XenMobile Server

Sep 18, 2017

Current release: XenMobile Server 10.7

XenMobile Server is an on-premises enterprise mobility management solution that offers mobile device management (MDM) and mobile application management (MAM) capabilities.

The cloud service version of XenMobile Server is called XenMobile Service.

The XenMobile Apps are productivity and communication apps that are offered as a part of the XenMobile solution.

For information specific to the XenMobile cloud offering, see XenMobile Service. For information about the XenMobile Apps, see XenMobile Apps.

For the XenMobile Server and apps, Citrix supports the current and prior two versions of XenMobile. For a list of new features, known and fixed issues in the prior two versions, see:

- What's new in XenMobile Server 10.6
- What's new in XenMobile Server 10.5

For PDFs of the documentation for all versions earlier than the most recent version, see the Archive List of Legacy Documents.

XenMobile 9. This version reached the End of Life (EOL) lifecycle status as of June 30, 2017. When a product release reaches EOL, you can use the product within the terms of your product licensing agreement, but the available support options are limited. Historical information appears in the Knowledge Center or other online resources. The documentation is no longer updated and is provided on an as-is basis. For more information about product lifecycle milestones, see the Product Matrix.

For five years beyond the EOL date, you can download a PDF of the XenMobile 9 documentation from the Archive List of Legacy Documents.

For more information about moving from XenMobile 9 to XenMobile 10.6 or earlier, or to XenMobile Service via Citrix Cloud, see this Citrix.com page.

Upgrades

Important

Before you upgrade to XenMobile 10.7 (on-premises)

1. If the virtual machine running the XenMobile Server to be upgraded has less than 4 GB of RAM, increase the RAM to at least 4 GB. Keep in mind that the recommended minimum RAM is 8 GB for production environments.
2. For upgrades from XenMobile 10.4 or earlier: Make a note about your configurations for the Passcode and Restrictions device policies for Windows tablets. Those policies are no longer based on WMI. As a result, the upgrade removes the existing configurations. After the upgrade, reconfigure the Passcode and Restrictions device policies for Windows tablets.

3. If you have the deprecated Enterprise Data Protection device policy configured, delete the policy before upgrading.
4. Recommendation: Before you install a XenMobile update, use the functionality in your virtual machine (VM) to take a snapshot of your system. Also, back up your system configuration database. If you experience issues during an upgrade, complete backups enable you to recover.

You can directly upgrade to XenMobile 10.7 from XenMobile 10.6 or 10.5. You have these options for upgrading to XenMobile 10.7:

- **To upgrade from XenMobile 10.6 or XenMobile 10.5 to XenMobile 10.7**. Use the **Release Management** page in the XenMobile console. You do not use the Upgrade Tool to upgrade XenMobile 10 installations.

  To perform the upgrade, you use xms_10.7.0.20.bin. In the XenMobile console, click the gear icon in the upper-right corner of the console and then click **Release Management**. Click **Upgrade** and then upload the BIN file. Upgrade files for supported hypervisors are:

  xms_10.7.0.20.xenserver.xva
  xms_10.7.0.20.HyperV.zip
  xms_10.7.0.20.vmware.ova

- **To upgrade from XenMobile 10.4 to XenMobile 10.7.** Use the **Release Management** page in the XenMobile console to upgrade in the following sequence. You do not use the Upgrade Tool for these installations.
  - Upgrade from XenMobile 10.4 to XenMobile 10.6.
  - Upgrade from XenMobile 10.6 to XenMobile 10.7.
- **To upgrade from XenMobile 10.3.6 to XenMobile 10.7.** Use the **Release Management** page in the XenMobile console to upgrade in the following sequence. You do not use the Upgrade Tool for these installations.
  - Upgrade from XenMobile 10.3.6 to XenMobile 10.5.
  - Upgrade from XenMobile 10.5 to XenMobile 10.7.
- **To upgrade from XenMobile 10 or 10.1 to XenMobile 10.7**. First, use the **Release Management** page in the XenMobile console to upgrade in the following sequence. You do not use the Upgrade Tool for these installations.
  - Upgrade from XenMobile 10 or 10.1 to XenMobile 10.3.5
  - Upgrade from XenMobile 10.3.5 to XenMobile 10.4.
  - Upgrade from XenMobile 10.4 to XenMobile 10.6.
  - Upgrade from XenMobile 10.6 to XenMobile 10.7.
- **To upgrade from XenMobile 9.0 to XenMobile 10.7**. Use the XenMobile Upgrade Tool that is built in to XenMobile 10.6. Verify that your XenMobile 10.6 environment is working and then upgrade from XenMobile 10.6 to XenMobile 10.7. The Upgrade Tool supports all XenMobile 9 editions: MDM, App, and Enterprise.

For information about upgrading, see Upgrade and its subarticles.

To complete a new installation of the latest release of XenMobile, see Install and configure.

Related information

> XenMobile Support Knowledge Center
> Citrix Blogs on XenMobile

What's new in XenMobile Server 10.7

Sep 06, 2017

For information about upgrading, see Upgrade.

> ## Important
>
> **After an upgrade to XenMobile 10.7:**
>
> If functionality involving outgoing connections stop working, and you haven't changed your connection configuration, check the XenMobile Server log for errors, such as the following: Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer.
>
> If you receive the certificate validation error, disable hostname verification on XenMobile Server. By default, hostname verification is enabled on outgoing connections except for the Microsoft PKI server. If hostname verification breaks your deployment, change the server property **disable.hostname.verification** to **true**. The default value of this property is **false**.

XenMobile Server 10.7 includes the following new features:

- Integrate with Apple Education features
- Deploy iBooks to iOS devices
- BitLocker device policy
- New restrictions for supervised devices running iOS 10.3 and later
- Restart or shut down a supervised iOS device
- Locate or ring a supervised iOS device that's in lost mode
- Enhanced Android for Work support
- More macros for enrollment templates
- Other improvements
- Public REST API changes

For information about bug fixes, see Fixed issues.

> ## Important
>
> TouchDown by Symantec reached End of Life on July 3, 2017, with End of Standard Support, End of Extended Support, and End of Support Life on July 2, 2018. For more information, see the Symantec support article, TouchDown End-of-Life, End-of-Availability, and End-of-Support announcement.

Integrate with Apple Education features

You can use XenMobile Server as your mobile device management (MDM) solution in an environment that uses Apple Education. XenMobile supports the Apple Education enhancements introduced in iOS 9.3, including Apple School Manager and Classroom app for iPad. The new XenMobile Education Configuration device policy configures instructor and student devices for use with Apple Education.

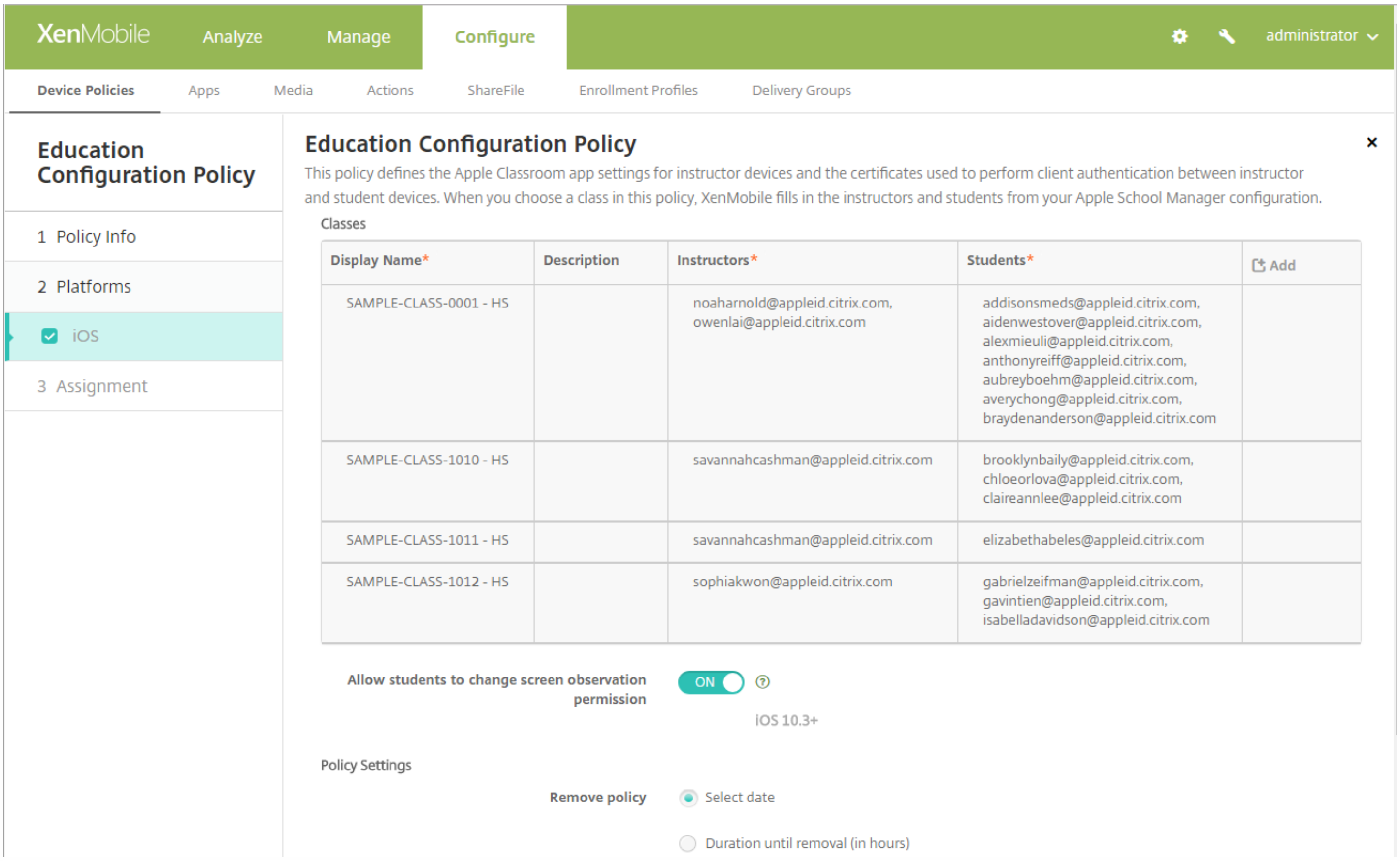
The following video provides a quick tour of the changes you make to Apple School Manager and XenMobile Server.

Citrix XenMobile Education Configuration: Integrate Apple Education features with XenMobile

You provide preconfigured and supervised iPads to instructors and students. That configuration includes:

- Apple School Manager DEP enrollment in XenMobile
- A Managed Apple ID account configured with a new password
- Required VPP apps and iBooks

For details about integrating with Apple Education features, see Integrate with Apple Education features and Education Configuration device policy.



Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Classes

Display Name*	Description	Instructors*	Students*	Add
SAMPLE-CLASS-0001 - HS		noaharnold@appleid.citrix.com, owenlai@appleid.citrix.com	addisonsmeds@appleid.citrix.com, aidenwestover@appleid.citrix.com, alexmieuli@appleid.citrix.com, anthonyreiff@appleid.citrix.com, aubreyboehm@appleid.citrix.com, averychong@appleid.citrix.com, braydenanderson@appleid.citrix.com	
SAMPLE-CLASS-1010 - HS		savannahcashman@appleid.citrix.com	brooklynbaily@appleid.citrix.com, chloeorlova@appleid.citrix.com, claireannlee@appleid.citrix.com	
SAMPLE-CLASS-1011 - HS		savannahcashman@appleid.citrix.com	elizabethabeles@appleid.citrix.com	
SAMPLE-CLASS-1012 - HS		sophiakwon@appleid.citrix.com	gabrielzeifman@appleid.citrix.com, gavintien@appleid.citrix.com, isabelladavidson@appleid.citrix.com	

Allow students to change screen observation permission: ON

iOS 10.3+

Policy Settings

Remove policy: ● Select date ○ Duration until removal (in hours)

Deploy iBooks to iOS devices

You can use XenMobile to deploy iBooks that you obtain through the Apple Volume Purchase Program (VPP). After you configure a VPP account in XenMobile, 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.

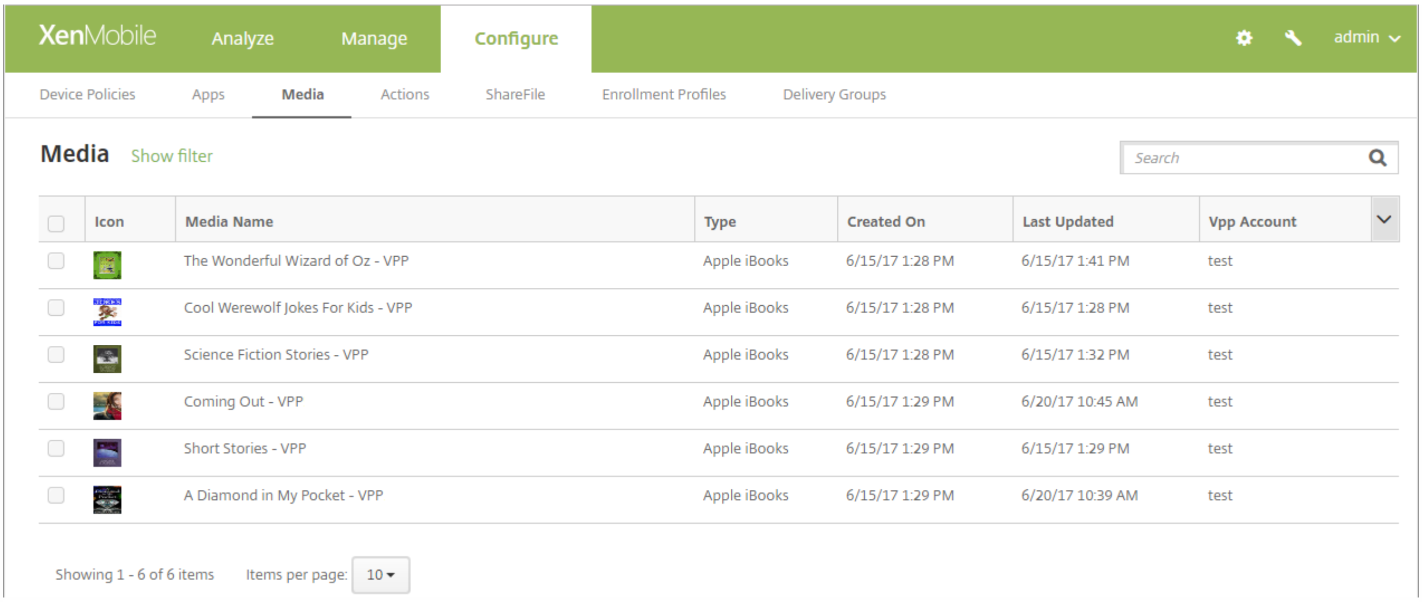
The first time that a user receives an iBook and accepts the VPP license, deployed books install on the device. The books appear in the Apple iBook app. You can't disassociate the book license from the user or remove the book from the device. XenMobile installs iBooks as required media. If a user deletes an installed book from their device, the book remains in the iBook app, ready for download.

Prerequisites

- iOS devices (minimum version iOS 8)
- Configure iOS VPP in XenMobile, as described in iOS Volume Purchase Plan.

Configure iBooks

iBooks obtained through VPP appear on the **Configure > Media** page. For more information, see Add media.



Media

□	Icon	Media Name	Type	Created On	Last Updated	Vpp Account
□		The Wonderful Wizard of Oz - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:41 PM	test
□		Cool Werewolf Jokes For Kids - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:28 PM	test
□		Science Fiction Stories - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:32 PM	test
□		Coming Out - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:45 AM	test
□		Short Stories - VPP	Apple iBooks	6/15/17 1:29 PM	6/15/17 1:29 PM	test
□		A Diamond in My Pocket - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:39 AM	test

Showing 1 - 6 of 6 items   Items per page: 10

BitLocker device policy

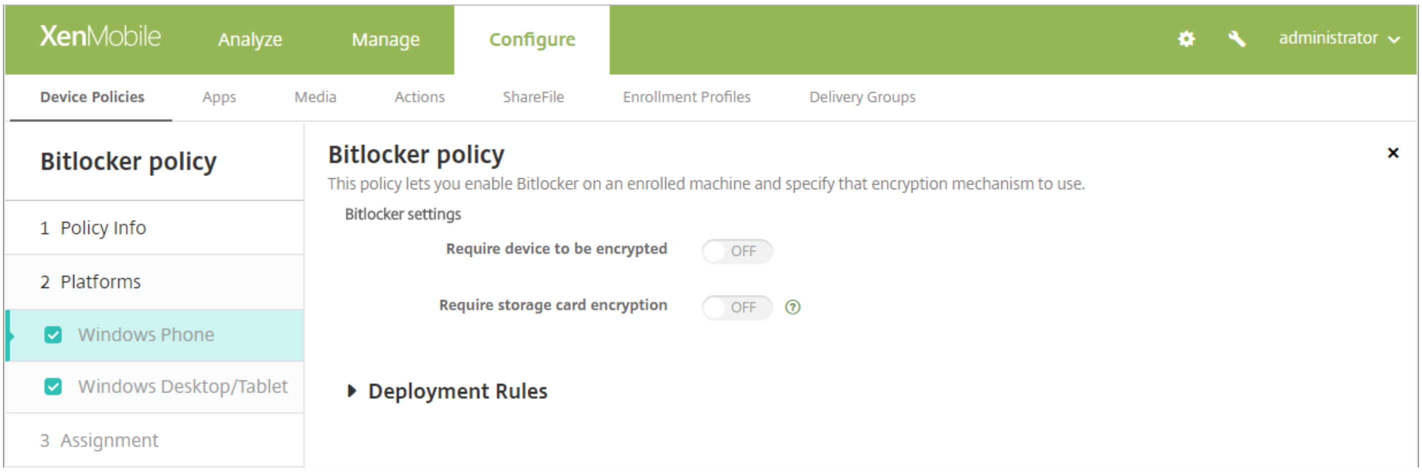
Windows 10 Enterprise includes a disk encryption feature called BitLocker, which provides extra file and system protections against unauthorized access of a lost or stolen device. For more protection, you can use BitLocker with Trusted Platform Module (TPM) chips, version 1.2 or later. A TPM chip handles 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 XenMobile to configure the settings available in the BitLocker wizard on Windows 10 devices. For example, on a device with BitLocker enabled, BitLocker can prompt users for:

- 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.



Bitlocker policy

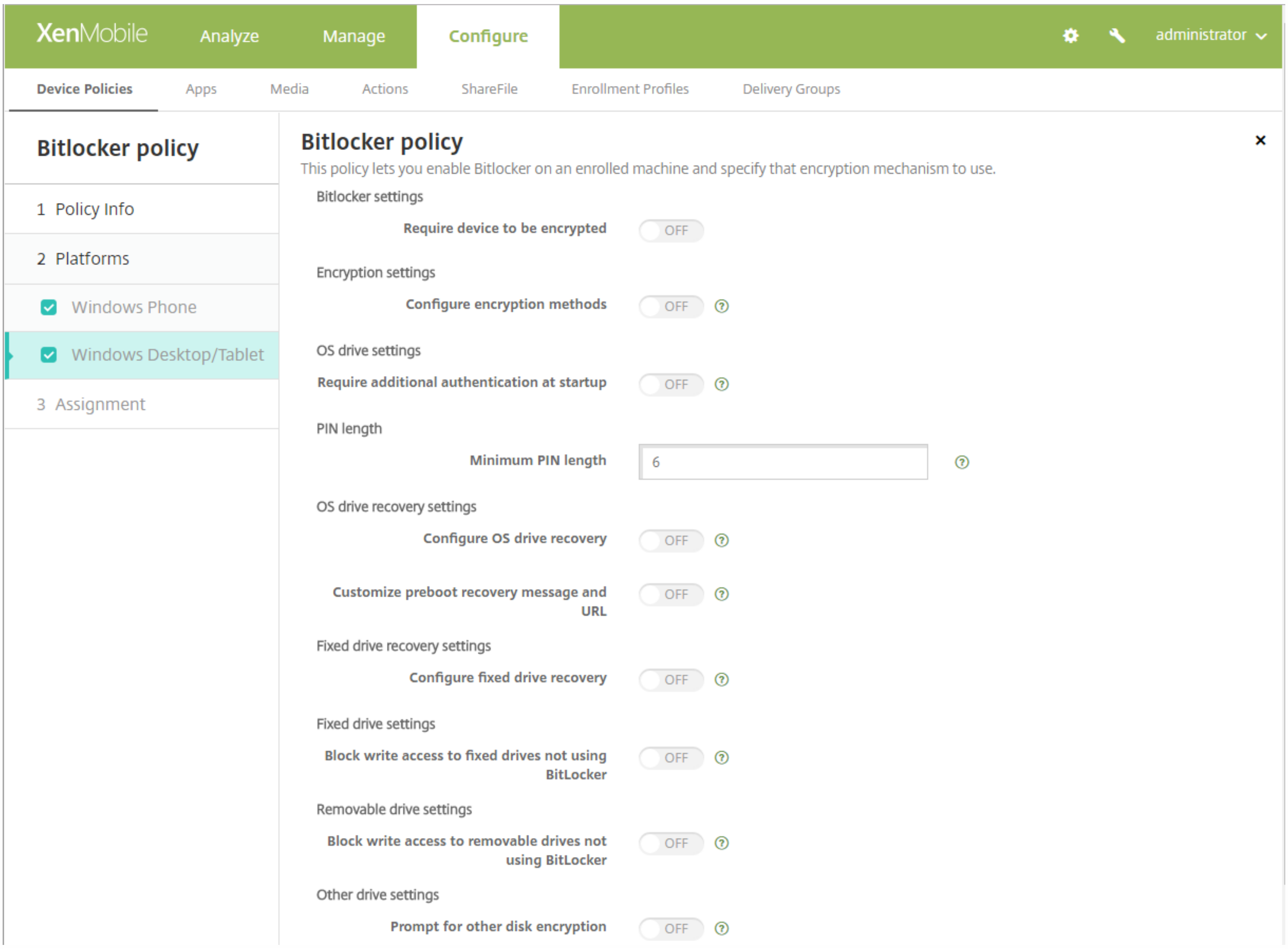
This policy lets you enable Bitlocker on an enrolled machine and specify that encryption mechanism to use.

Bitlocker settings

Require device to be encrypted: OFF

Require storage card encryption: OFF

Deployment Rules



Bitlocker policy

This policy lets you enable Bitlocker on an enrolled machine and specify that encryption mechanism to use.

Bitlocker settings

Require device to be encrypted: OFF

Encryption settings

Configure encryption methods: OFF

OS drive settings

Require additional authentication at startup: OFF

PIN length

Minimum PIN length: 6

OS drive recovery settings

Configure OS drive recovery: OFF

Customize preboot recovery message and URL: OFF

Fixed drive recovery settings

Configure fixed drive recovery: OFF

Fixed drive settings

Block write access to fixed drives not using BitLocker: OFF

Removable drive settings

Block write access to removable drives not using BitLocker: OFF

Other drive settings

Prompt for other disk encryption: OFF

For more information, see BitLocker device policy.

New restrictions for supervised devices running iOS 10.3 and later

Restrictions allow you to prevent users from performing certain actions on their devices and are implemented through device policies.

The following restrictions are now available for devices running iOS 10.3 and later, in supervised mode:

- **Allow Dictation**: Supervised only. If this restriction is set to **OFF**, dictation input is not allowed. The default setting is **ON**. For iOS 10.3 and later.
- **Force WiFi white listing**: 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**. For iOS 10.3 and later.

To set these restrictions:

1. In the XenMobile console, select **Configure > Device Policies**. The Device Policies page appears.

2. Select **Add**. The **Add a New Policy** page appears.

3. Click **Restrictions**. The restrictions **Policy information** page appears.

4. In the **Policy Information** pane, type the following information:

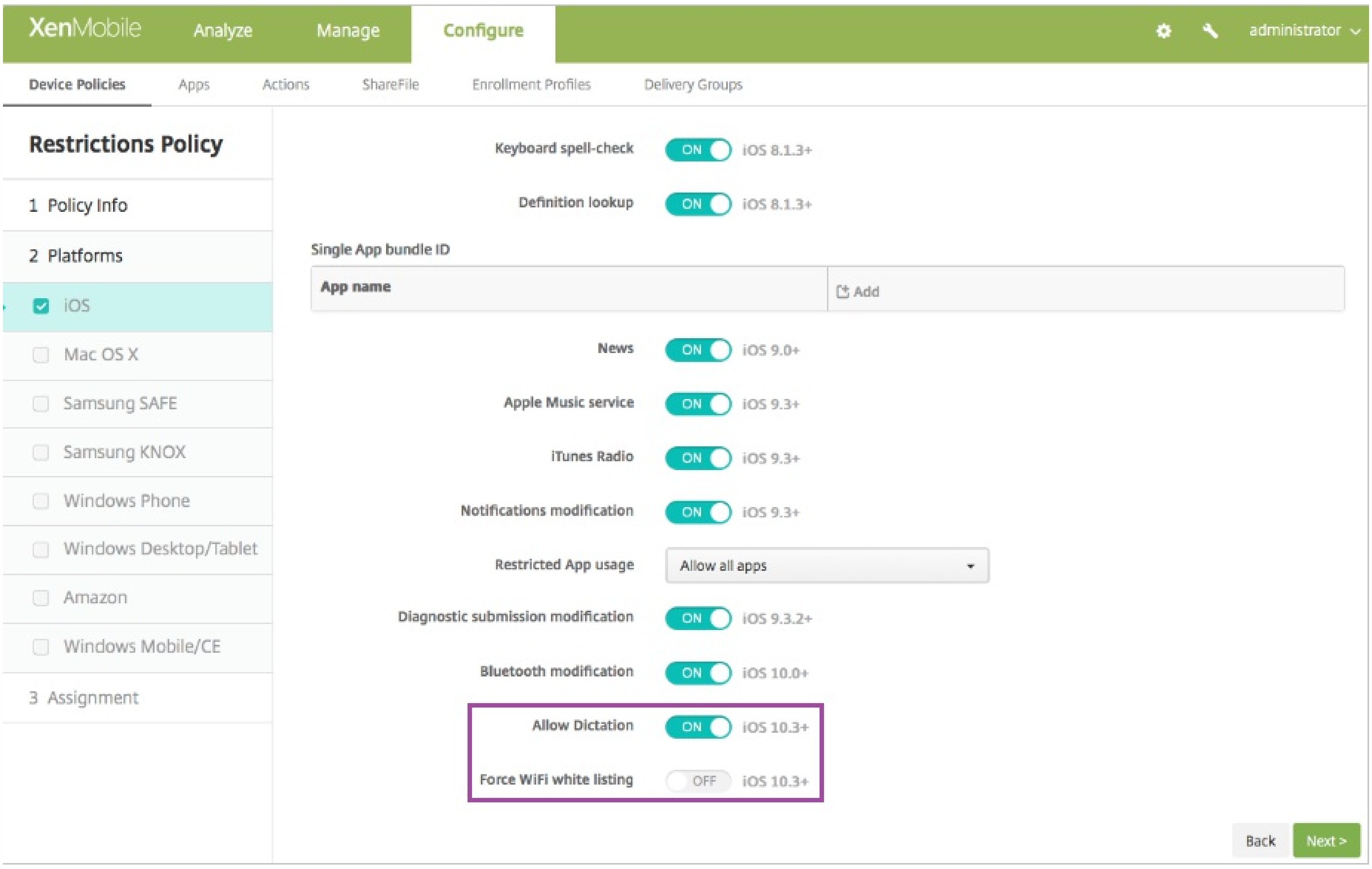
   Policy Name: Type a descriptive name for the policy.

   Description: Type an optional description of the policy.

5. Click **Next**. The **Policy Platforms** page appears.

6. Select **iOS**.

7. Click **Next** until the page showing the Single App bundle ID section appears. Set the restrictions.



XenMobile | Analyze | Manage | Configure | administrator

Device Policies | Apps | Actions | ShareFile | Enrollment Profiles | Delivery Groups

Restrictions Policy

1 Policy Info
2 Platforms
- ☑ iOS
- ☐ Mac OS X
- ☐ Samsung SAFE
- ☐ Samsung KNOX
- ☐ Windows Phone
- ☐ Windows Desktop/Tablet
- ☐ Amazon
- ☐ Windows Mobile/CE

3 Assignment

Setting	Value	
Keyboard spell-check	ON	iOS 8.1.3+
Definition lookup	ON	iOS 8.1.3+

Single App bundle ID

App name	Add

Setting	Value	
News	ON	iOS 9.0+
Apple Music service	ON	iOS 9.3+
iTunes Radio	ON	iOS 9.3+
Notifications modification	ON	iOS 9.3+
Restricted App usage	Allow all apps	
Diagnostic submission modification	ON	iOS 9.3.2+
Bluetooth modification	ON	iOS 10.0+
Allow Dictation	ON	iOS 10.3+
Force WiFi white listing	OFF	iOS 10.3+

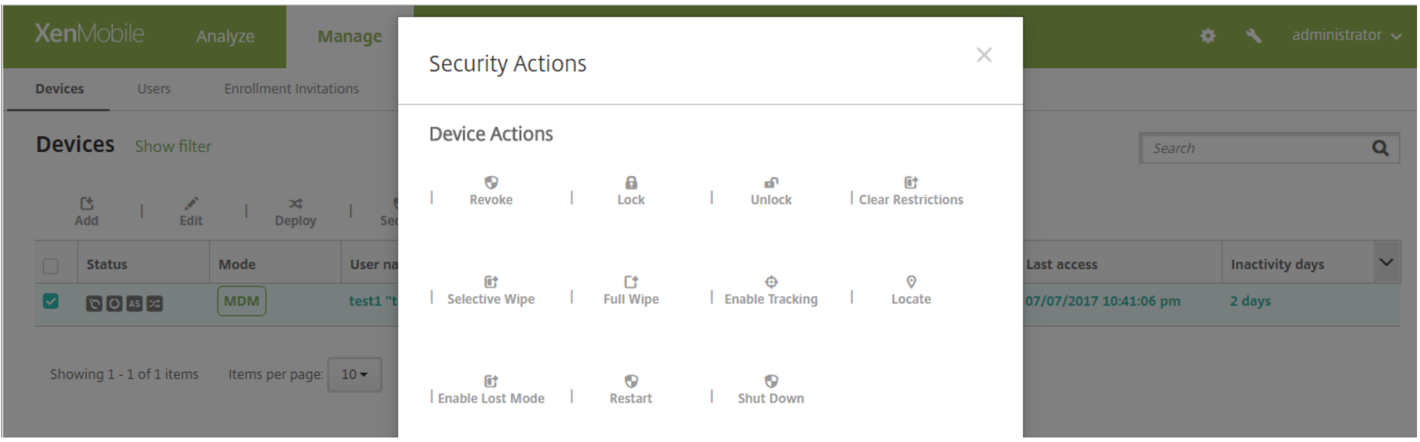
Back | Next >

For more information on setting restrictions, see Restrictions device policy.

Restart or shut down a supervised iOS device

You can use security actions to restart or shut down a supervised iOS device (minimum version 10.3). Go to **Manage > Devices**, select the device, click **Security**, and then click **Restart** or **Shut Down**.

A device restarts immediately when it receives the **Restart** command. Passcode-locked iOS devices don't rejoin WiFi networks after restarting, so they might not communicate with the server. A device shuts down immediately when it receives the **Shut Down** command.



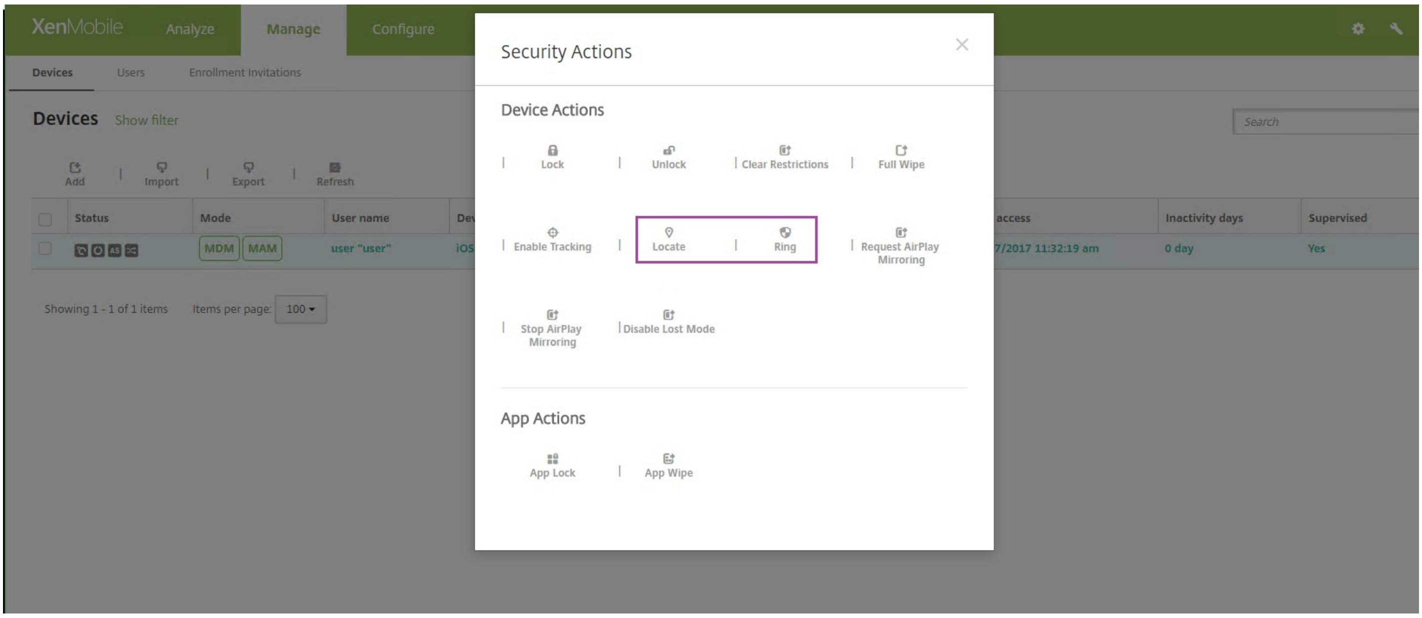
Security Actions

Device Actions

Revoke | Lock | Unlock | Clear Restrictions
Selective Wipe | Full Wipe | Enable Tracking | Locate
Enable Lost Mode | Restart | Shut Down

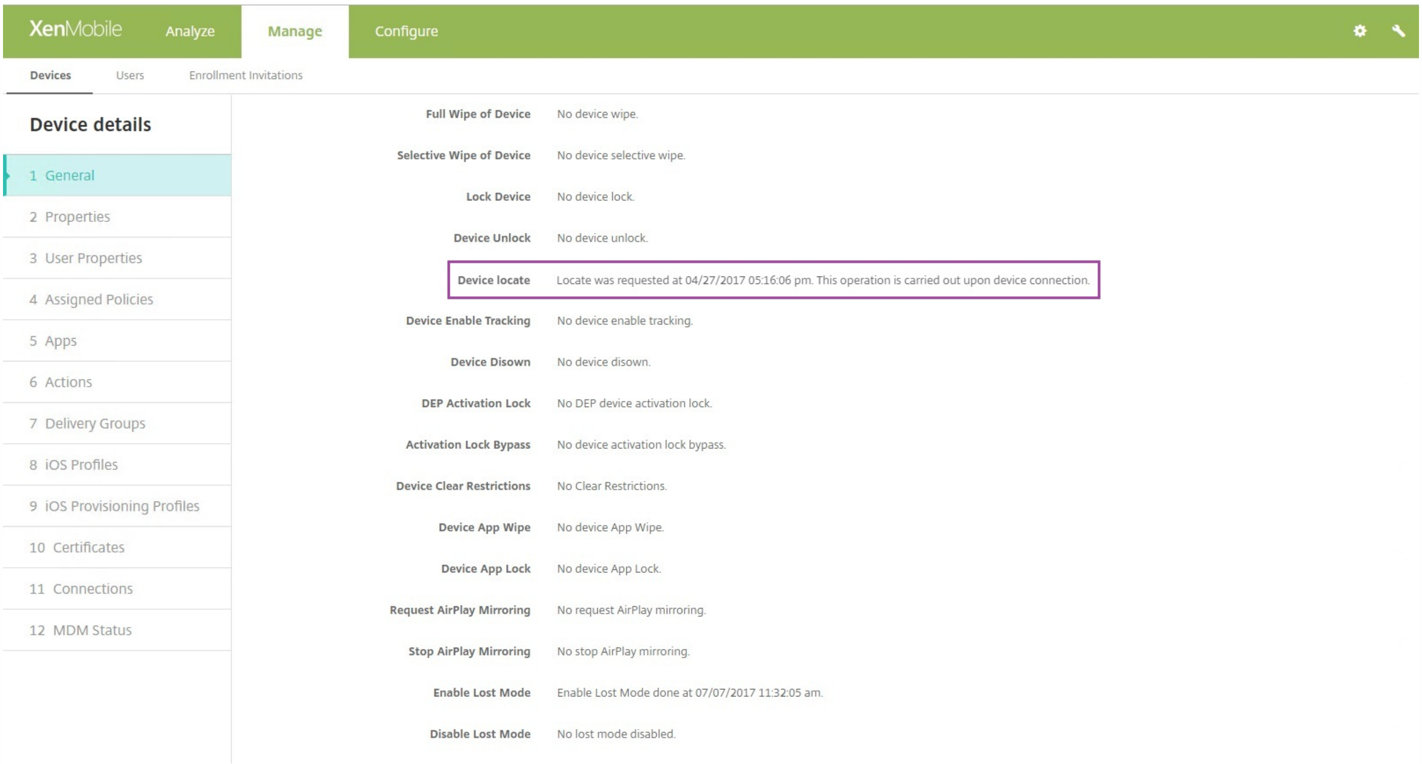
Locate or ring a supervised iOS device that's in lost mode

After you place a supervised iOS device in lost mode, you can use security actions to locate or ring the device. A "ring" is the lost mode sound that Apple defines for the device.



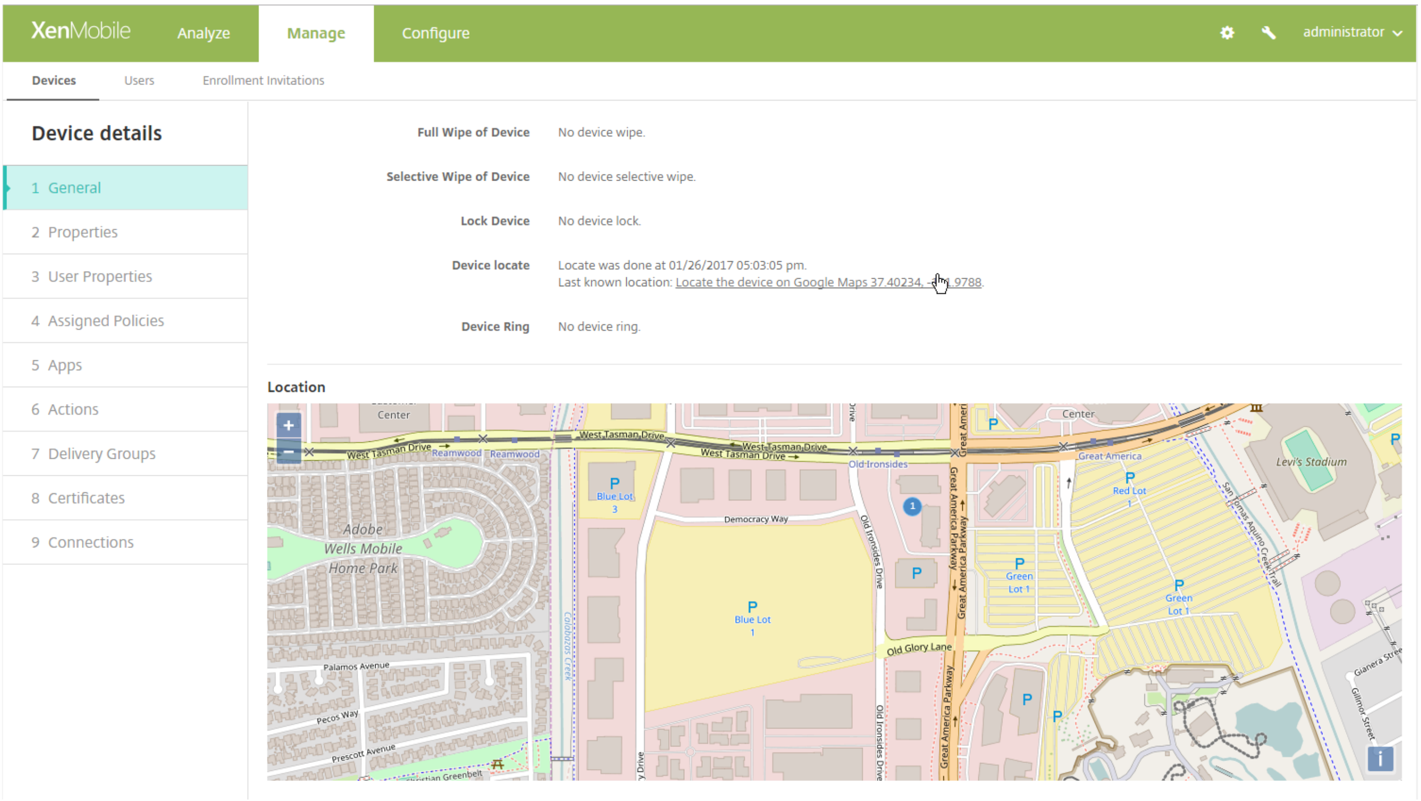
- To locate a device that's in lost mode:

  Go to **Manage > Devices**, select the device, click **Security**, and then click **Locate**. The **Device details** page provides a status of the location request.



Full Wipe of Device	No device wipe.
Selective Wipe of Device	No device selective wipe.
Lock Device	No device lock.
Device Unlock	No device unlock.
Device locate	Locate was requested at 04/27/2017 05:16:06 pm. This operation is carried out upon device connection.
Device Enable Tracking	No device enable tracking.
Device Disown	No device disown.
DEP Activation Lock	No DEP device activation lock.
Activation Lock Bypass	No device activation lock bypass.
Device Clear Restrictions	No Clear Restrictions.
Device App Wipe	No device App Wipe.
Device App Lock	No device App Lock.
Request AirPlay Mirroring	No request AirPlay mirroring.
Stop AirPlay Mirroring	No stop AirPlay mirroring.
Enable Lost Mode	Enable Lost Mode done at 07/07/2017 11:32:05 am.
Disable Lost Mode	No lost mode disabled.

If the device is located, the **Device details** page includes a map.



Full Wipe of Device	No device wipe.
Selective Wipe of Device	No device selective wipe.
Lock Device	No device lock.
Device locate	Locate was done at 01/26/2017 05:03:05 pm. Last known location: Locate the device on Google Maps 37.40234, -[illegible].9788.
Device Ring	No device ring.

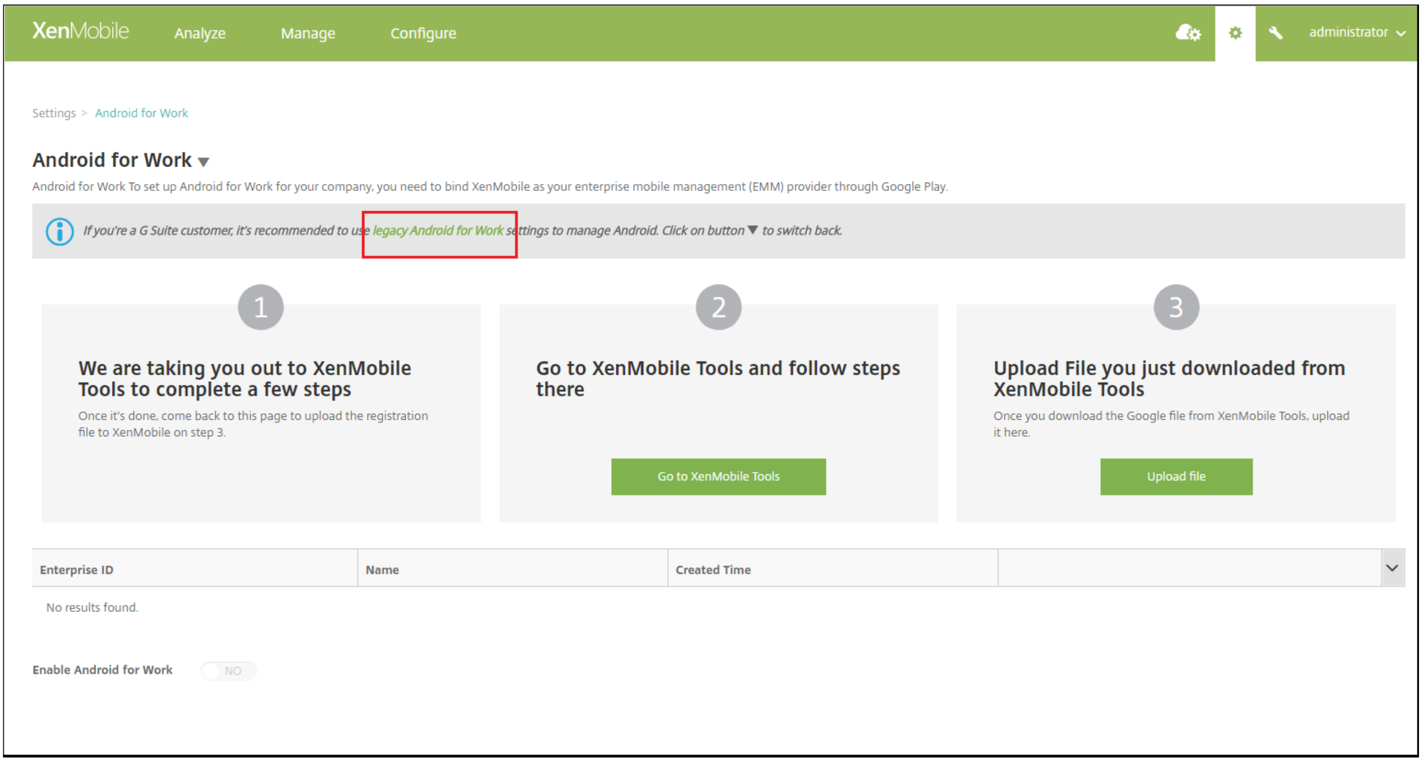
- To ring a device that's in lost mode (minimum version iOS 10.3):

  Go to **Manage > Devices**, select the device, click **Security**, and then click **Ring**. The next time that the device connects, it rings. To stop the ring, the user clicks the power button. To stop the ring from the XenMobile console, use the **Disable Lost Mode** security action.

Enhanced Android for Work support

XenMobile now provides a simple way to set up Android for Work for your organization. Using XenMobile Management Tools, you bind XenMobile as your enterprise mobility management provider through Google Play and create an enterprise for Android for Work.

> ## Note
>
> G Suite customers, use the legacy Android for Work settings to configure legacy Android for Work, as described in the Android for Work article. Click **legacy Android for Work** in the **Android for Work** page in XenMobile Settings.



Android for Work ▾

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

If you're a G Suite customer, it's recommended to use legacy Android for Work settings to manage Android. Click on button ▼ to switch back.

1 We are taking you out to XenMobile Tools to complete a few steps

Once it's done, come back to this page to upload the registration file to XenMobile on step 3.

2 Go to XenMobile Tools and follow steps there

3 Upload File you just downloaded from XenMobile Tools

Once you download the Google file from XenMobile Tools, upload it here.

Enterprise ID	Name	Created Time
No results found.		

Enable Android for Work: NO

You need:

- Your Citrix account credentials to sign in to XenMobile Tools
- Your corporate Google ID credentials to sign in to Google Play

For more information, see Android for Work.

Support for Device Health Attestation (DHA) on-

premises

You can now enable Device Health Attestation (DHA) for Windows 10 mobile devices through an on-premises Windows server. Previously, DHA for XenMobile may be enabled only through Microsoft Cloud.

To enable DHA on-premises, you first configure a DHA server. Then you create a XenMobile Server policy to enable the on-premises DHA service.
To configure a DHA, you need a machine running Windows Server 2016 Technical Preview 5 or later. You install DHA as a server role. For instructions, see this Microsoft TechNet article, Device Health Attestation.

To the XenMobile Server policy to enable the on-premises DHA service:

1. In the XenMobile console, click **Configure > Device Policies**. The Device Policies page appears.

2. If you have already created a policy to enable DHA through Microsoft Cloud, skip to step 8.

3. Click **Add** to add a new policy. The **Add a New Policy** dialog box appears.

4. Click **More**, and then under **Custom**, click **Device Health Attestation policy**. The **Device Health Attestation Policy** information page appears.

5. In the Policy Information pane, enter the following information:

   Policy Name: Type a descriptive name for the policy.

   Description: Type an optional description of the policy.

6. Click **Next**. The Policy Platforms page appears.

7. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.

8. For each platform that you choose:

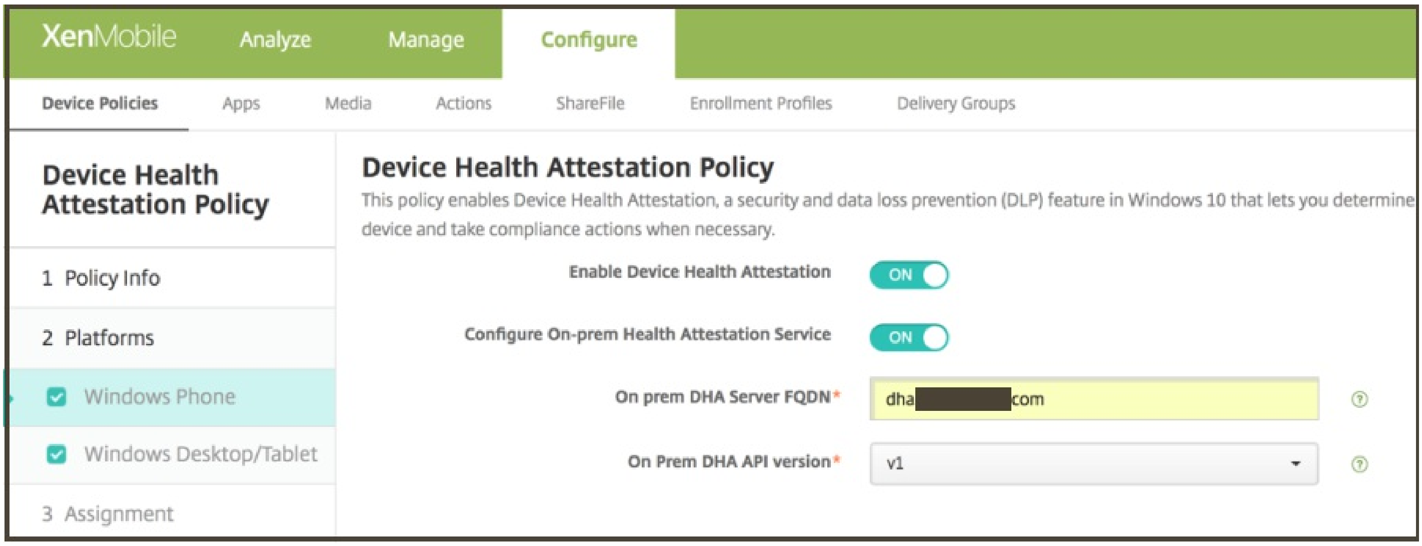
   a. Set **Enable Device Health Attestation** to **ON**.

   b. Set **Configure On-prem Health Attestation Service** to **ON**.

   c. In **On-prem DHA Service FQDN,** enter the fully qualified domain name of the DHA server you set up.

   d. In **On-prem DHA API version**, choose the version choose the version of the DHA service installed on the DHA server.

9. Configure deployment rules and choose delivery groups.



Device Health Attestation Policy

This policy enables Device Health Attestation, a security and data loss prevention (DLP) feature in Windows 10 that lets you determine device and take compliance actions when necessary.

Enable Device Health Attestation: ON

Configure On-prem Health Attestation Service: ON

On prem DHA Server FQDN*: dha[redacted]com

On Prem DHA API version*: v1

To confirm that the policy has been pushed to a Windows 10 Mobile device:

1. In the XenMobile console, click Manage > Device.

2. Select the device.

3. Select **Properties**.

4. Scroll down to see "Windows Device Health Attestation."

More macros for enrollment templates

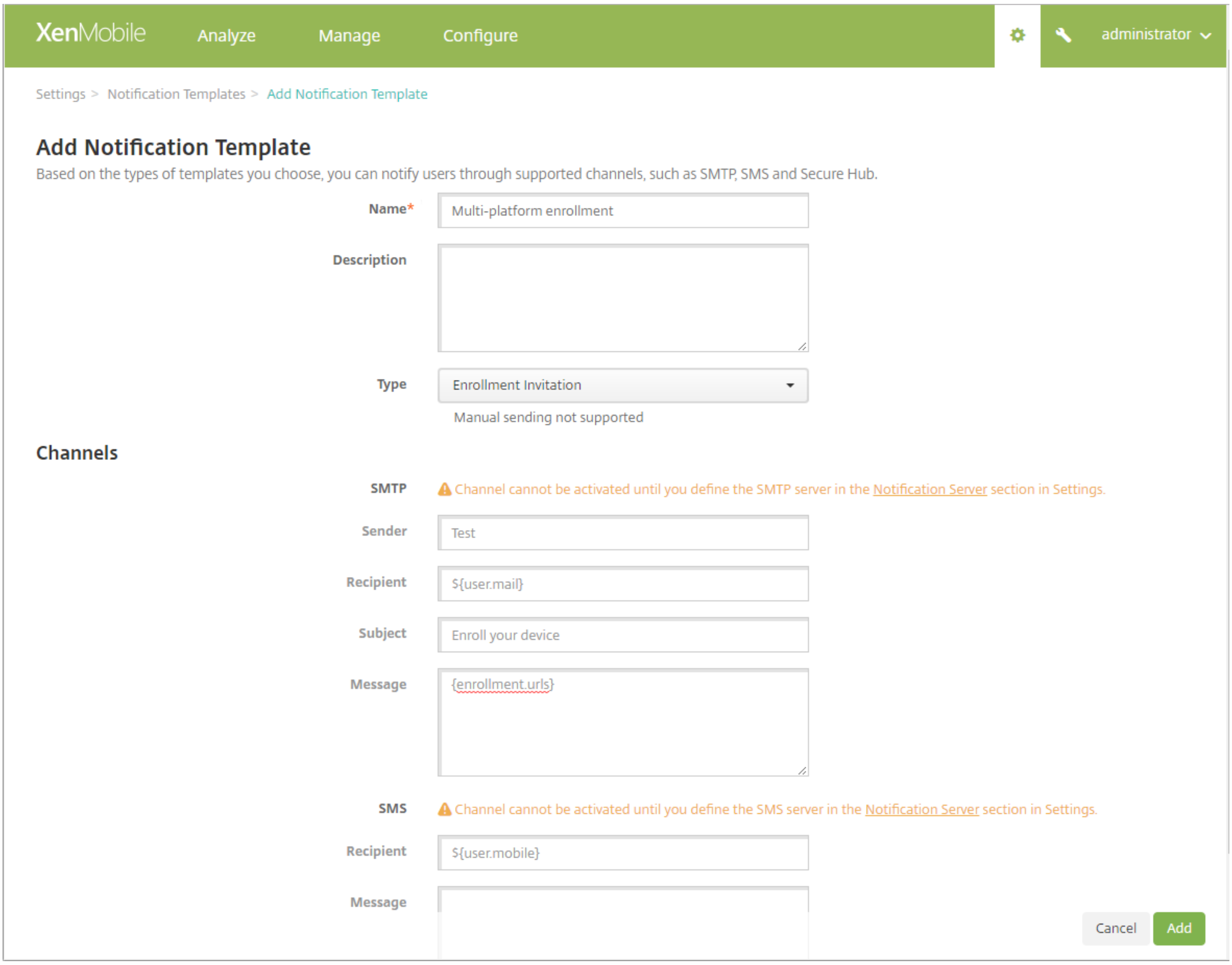
You can use these new macros when creating enrollment templates for device enrollment invitations:

${enrollment.urls}
${enrollment.ios.url}
${enrollment.macos.url}
${enrollment.android.url}
${enrollment.ios.platform}
${enrollment.macos.platform}
${enrollment.android.platform}
${enrollment.agent}

These macros allow you to create enrollment templates that contain enrollment URLs for multiple device platforms.

This example shows how to create a notification that includes enrollment URLs for multiple device platforms. The macro for the **Message** is:

${enrollment.urls}


XenMobile
Analyze
Manage
Configure
administrator
Settings > Notification Templates > Add Notification Template

Add Notification Template

Based on the types of templates you choose, you can notify users through supported channels, such as SMTP, SMS and Secure Hub.

Name*	Multi-platform enrollment
Description	
Type	Enrollment Invitation Manual sending not supported

Channels

SMTP	⚠ Channel cannot be activated until you define the SMTP server in the Notification Server section in Settings.
Sender	Test
Recipient	${user.mail}
Subject	Enroll your device
Message	{enrollment.urls}
SMS	⚠ Channel cannot be activated until you define the SMS server in the Notification Server section in Settings.
Recipient	${user.mobile}
Message	

These examples show how to create messages for notifications that prompt the users to click the enrollment URL for their device platforms:

Example 1:

To enroll, please click the link below that applies to your device platform:

${enrollment.ios.platform} - ${enrollment.ios.url}

${enrollment.macos.platform} - ${enrollment.macos.url}

${enrollment.android.platform} - ${enrollment.android.url}

Example 2:

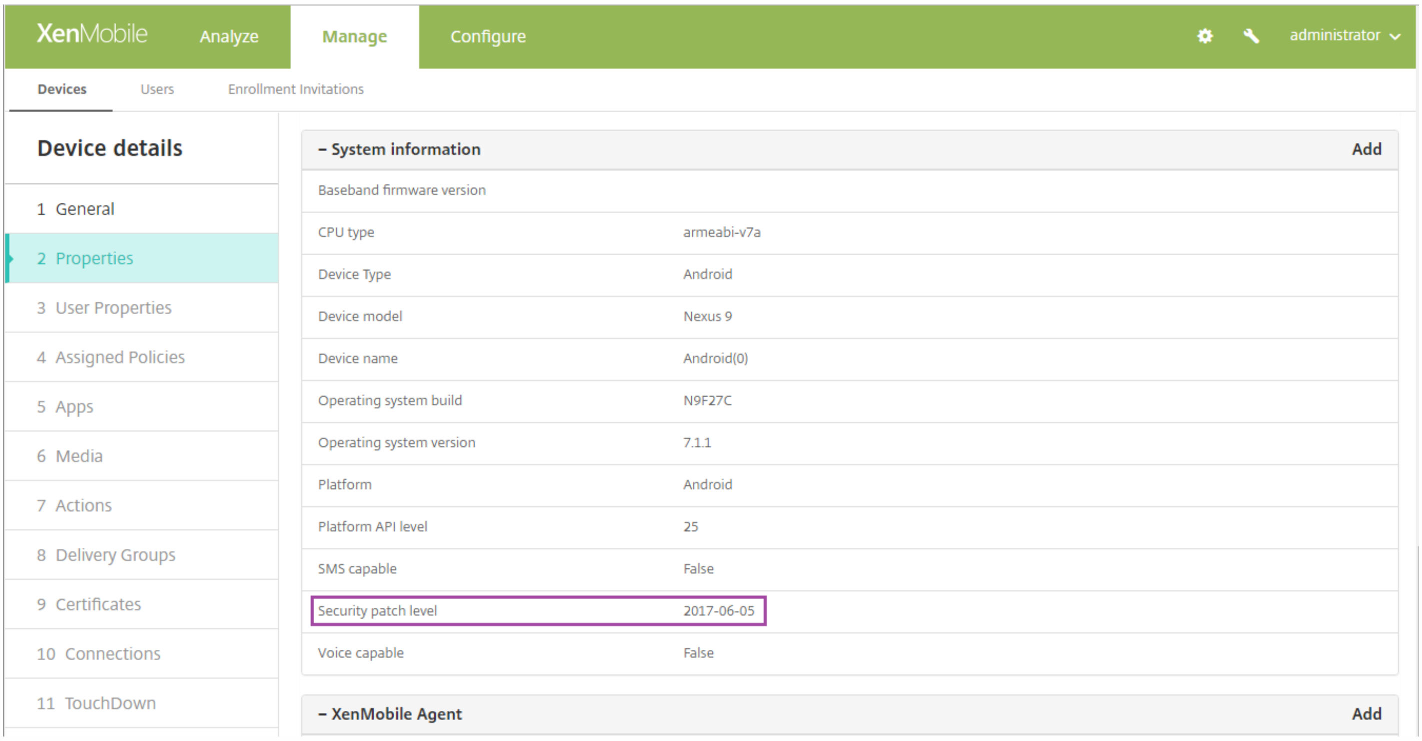
To enroll an iOS device, click the link ${enrollment.ios.url}.

To enroll a macOS device, click the link ${enrollment.macos.url}.

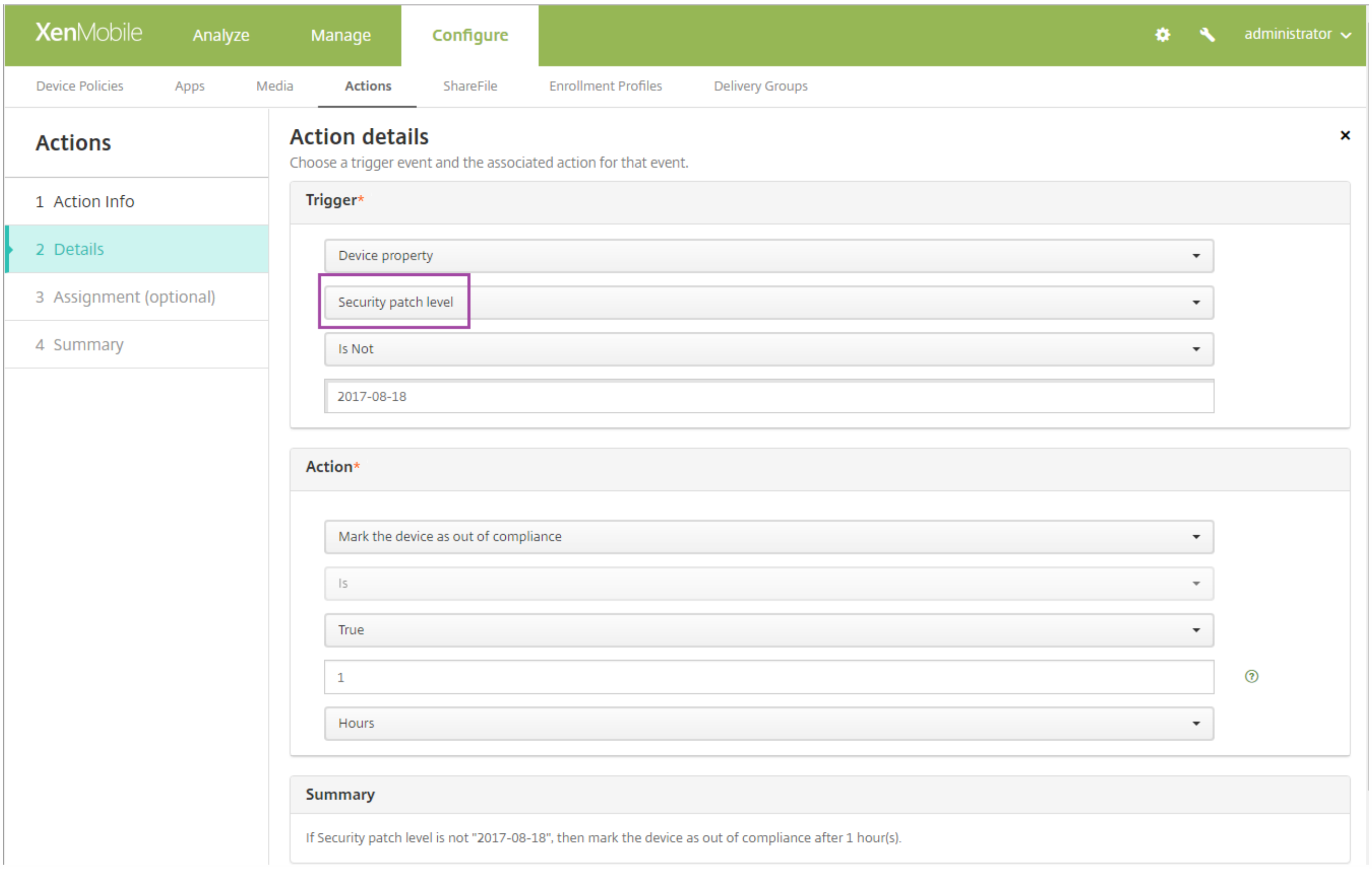
To enroll an Android device, click the link ${enrollment.android.url}.

Other improvements

- The XenMobile console and the Self Help Portal are now available in Spanish.
- **XenMobile now reports the Security patch level for Android devices**. You can view the **Security patch level** on the **Manage > Devices** page and in **Device details**. You can also use **Configure > Actions** to create an action that the security patch level triggers.



Baseband firmware version	
CPU type	armeabi-v7a
Device Type	Android
Device model	Nexus 9
Device name	Android(0)
Operating system build	N9F27C
Operating system version	7.1.1
Platform	Android
Platform API level	25
SMS capable	False
Security patch level	2017-06-05
Voice capable	False



Action details

Choose a trigger event and the associated action for that event.

Trigger*

- Device property
- Security patch level
- Is Not
- 2017-08-18

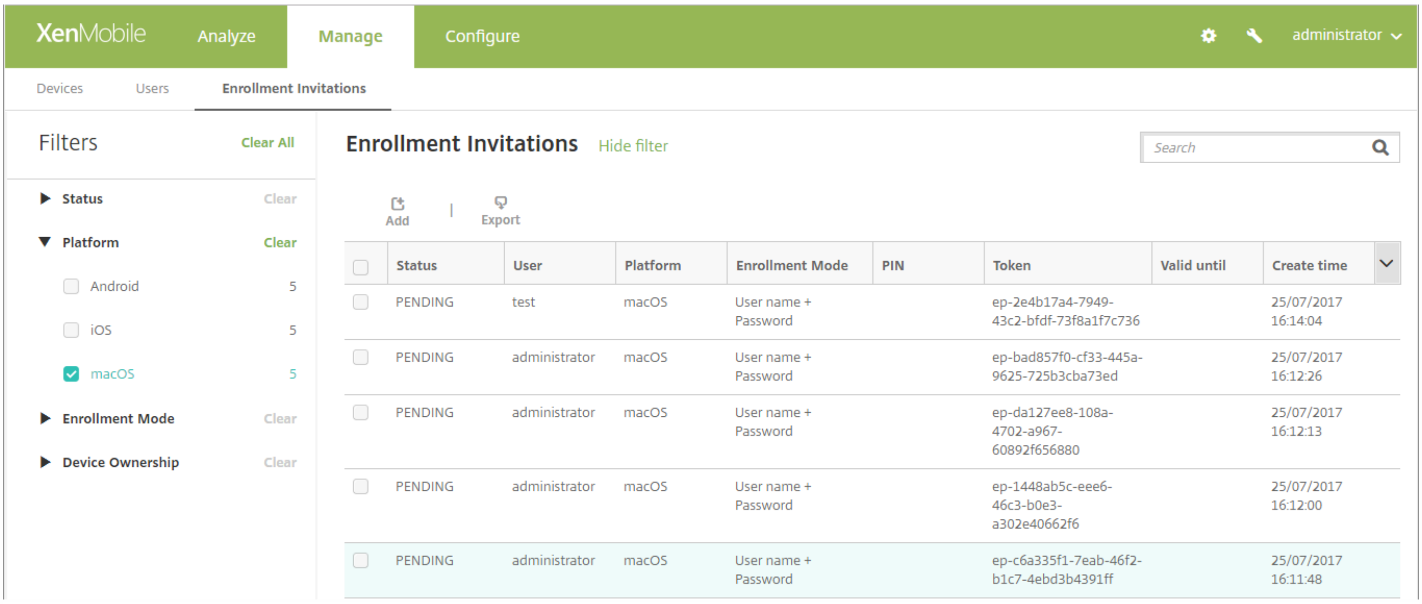
Action*

- Mark the device as out of compliance
- Is
- True
- 1
- Hours

Summary

If Security patch level is not "2017-08-18", then mark the device as out of compliance after 1 hour(s).

- **Filter enrollment invitations by macOS**. The Platform filter for **Manage > Enrollment Invitations** now includes **macOS**.



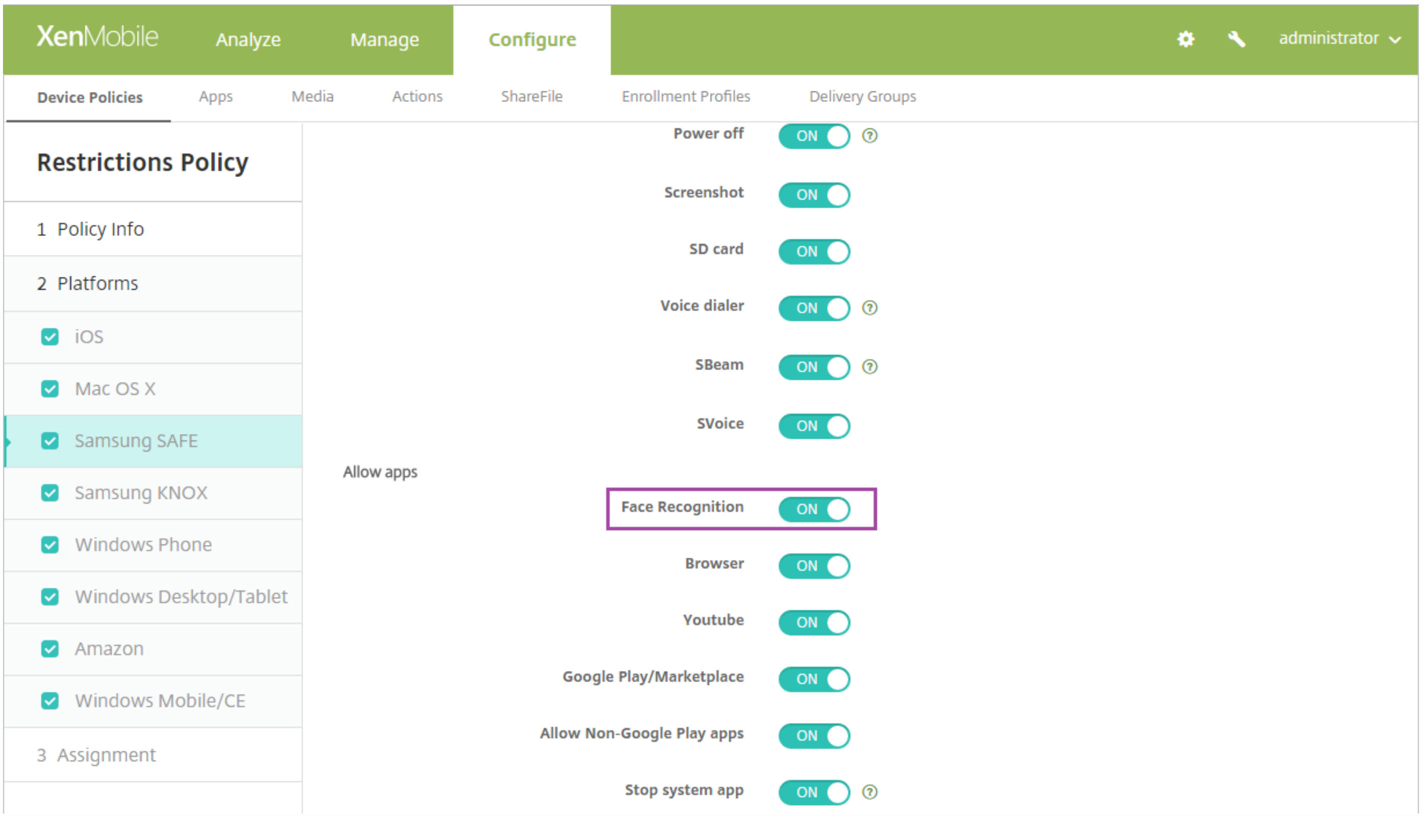
Platform	
□ Android	5
□ iOS	5
☑ macOS	5

Enrollment Invitations

□	Status	User	Platform	Enrollment Mode	PIN	Token	Valid until	Create time
□	PENDING	test	macOS	User name + Password		ep-2e4b17a4-7949-43c2-bfdf-73f8a1f7c736		25/07/2017 16:14:04
□	PENDING	administrator	macOS	User name + Password		ep-bad857f0-cf33-445a-9625-725b3cba73ed		25/07/2017 16:12:26
□	PENDING	administrator	macOS	User name + Password		ep-da127ee8-108a-4702-a967-60892f656880		25/07/2017 16:12:13
□	PENDING	administrator	macOS	User name + Password		ep-1448ab5c-eee6-46c3-b0e3-a302e40662f6		25/07/2017 16:12:00
□	PENDING	administrator	macOS	User name + Password		ep-c6a335f1-7eab-46f2-b1c7-4ebd3b4391ff		25/07/2017 16:11:48

- **Restrictions policy setting to block users from using face recognition to unlock Samsung Galaxy S8+ devices**. The Restrictions device policy for Samsung SAFE now includes the setting, **Face Recognition**. To block use of face recognition to unlock device access, go to **Configure > Device Policies** and edit the Restrictions policy to set **Face**

Recognition to **Off**.



Restrictions Policy

Allow apps

Power off ON

Screenshot ON

SD card ON

Voice dialer ON

SBeam ON

SVoice ON

Face Recognition ON

Browser ON

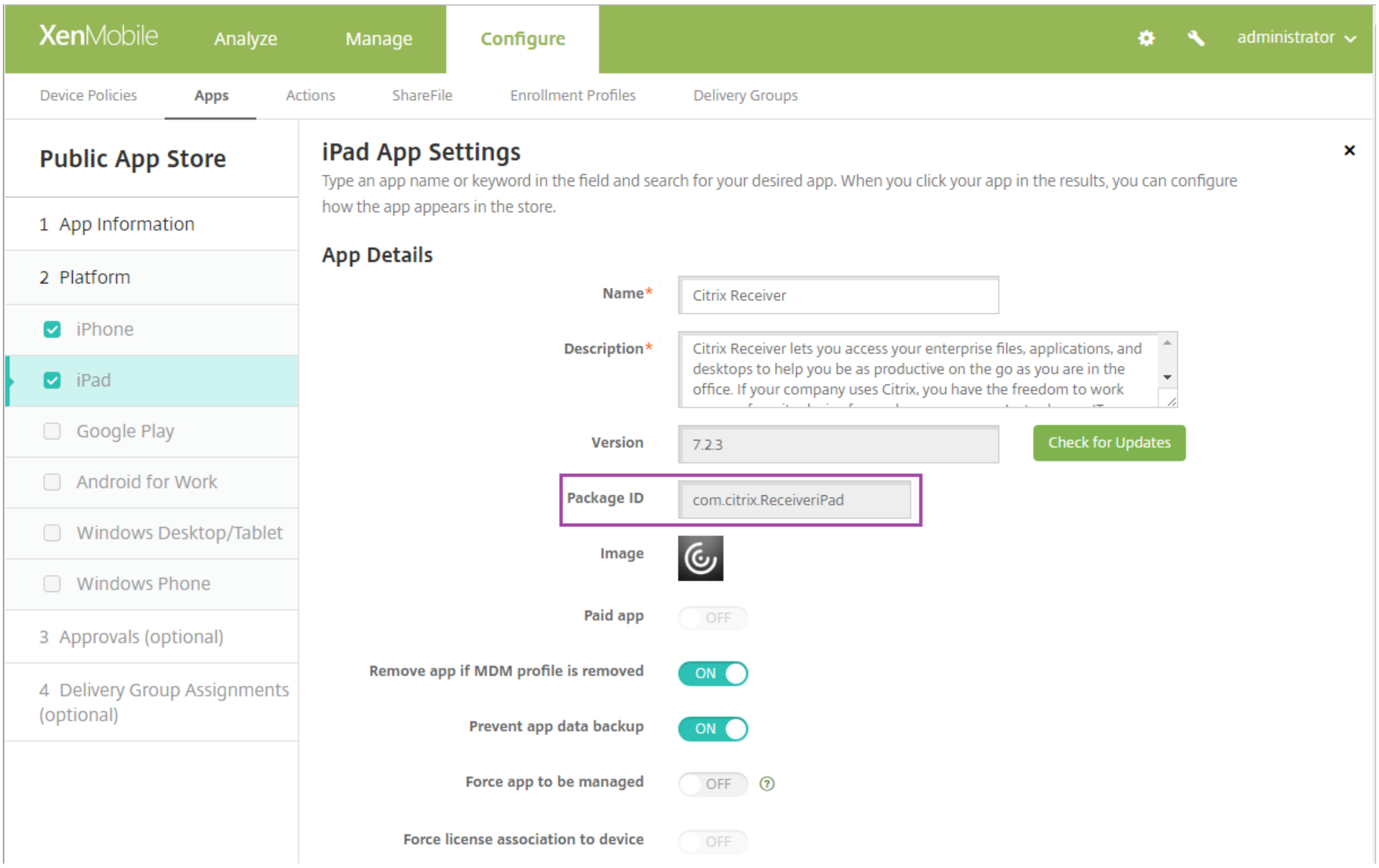
Youtube ON

Google Play/Marketplace ON

Allow Non-Google Play apps ON

Stop system app ON

- **Required macOS VPP apps now supported**. You can now deploy macOS VPP apps as required apps for both Active Directory and local users. You can view macOS VPP apps in **Configure > Apps**, where you can filter the apps by macOS VPP. On that page, the **Store Configuration** section doesn't appear for macOS VPP apps because there is no Secure Hub for macOS. In **Manage > Devices**, the **User Properties** include Retire VPP account for macOS VPP accounts.
- **Configure > Apps now shows the Package ID for public app store apps and enterprise apps**



Public App Store

1 App Information

2 Platform

- ☑ iPhone
- ☑ iPad
- □ Google Play
- □ Android for Work
- □ Windows Desktop/Tablet
- □ Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

iPad App Settings

Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

App Details

Name*: Citrix Receiver

Description*: Citrix Receiver lets you access your enterprise files, applications, and desktops to help you be as productive on the go as you are in the office. If your company uses Citrix, you have the freedom to work

Version: 7.2.3 [Check for Updates]

Package ID: com.citrix.ReceiveriPad

Image

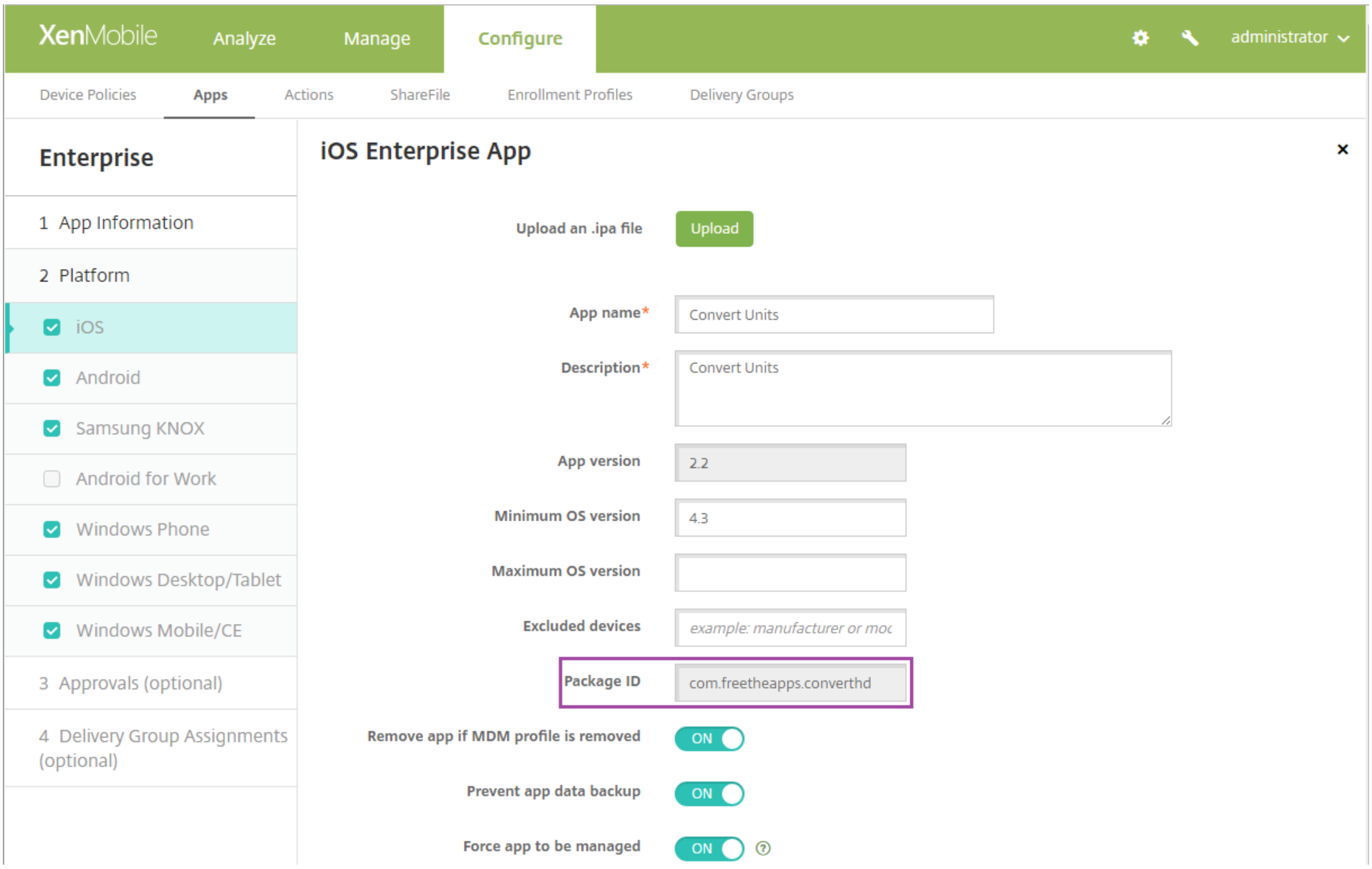
Paid app: OFF

Remove app if MDM profile is removed: ON

Prevent app data backup: ON

Force app to be managed: OFF

Force license association to device: OFF



Enterprise

1 App Information

2 Platform

- ☑ iOS
- ☑ Android
- ☑ Samsung KNOX
- □ Android for Work
- ☑ Windows Phone
- ☑ Windows Desktop/Tablet
- ☑ Windows Mobile/CE

3 Approvals (optional)

4 Delivery Group Assignments (optional)

iOS Enterprise App

Upload an .ipa file [Upload]

App name*: Convert Units

Description*: Convert Units

App version: 2.2

Minimum OS version: 4.3

Maximum OS version:

Excluded devices: *example: manufacturer or moc*

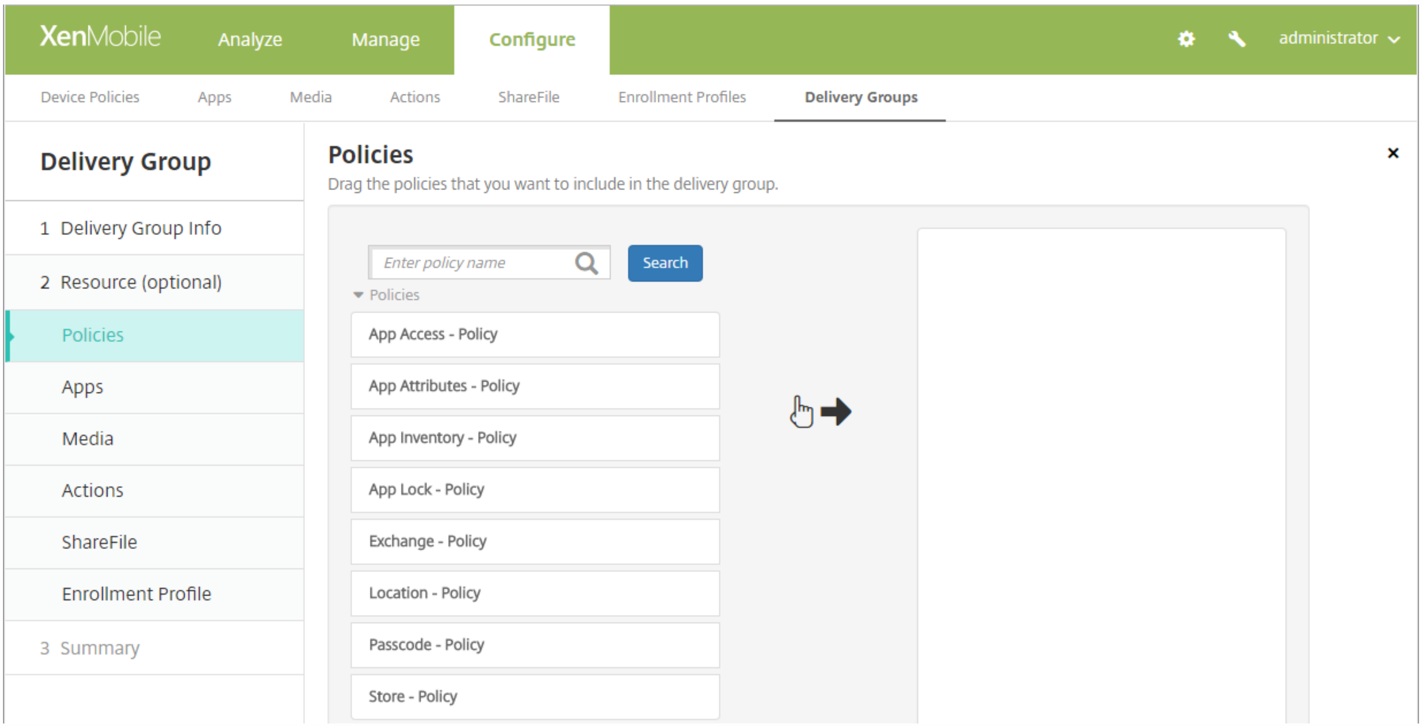
Package ID: com.freetheapps.converthd

Remove app if MDM profile is removed: ON

Prevent app data backup: ON

Force app to be managed: ON

- **Alphabetized resource lists for delivery groups.** In **Configure > Delivery Groups**, all resource lists and search results appear in alphabetical order.

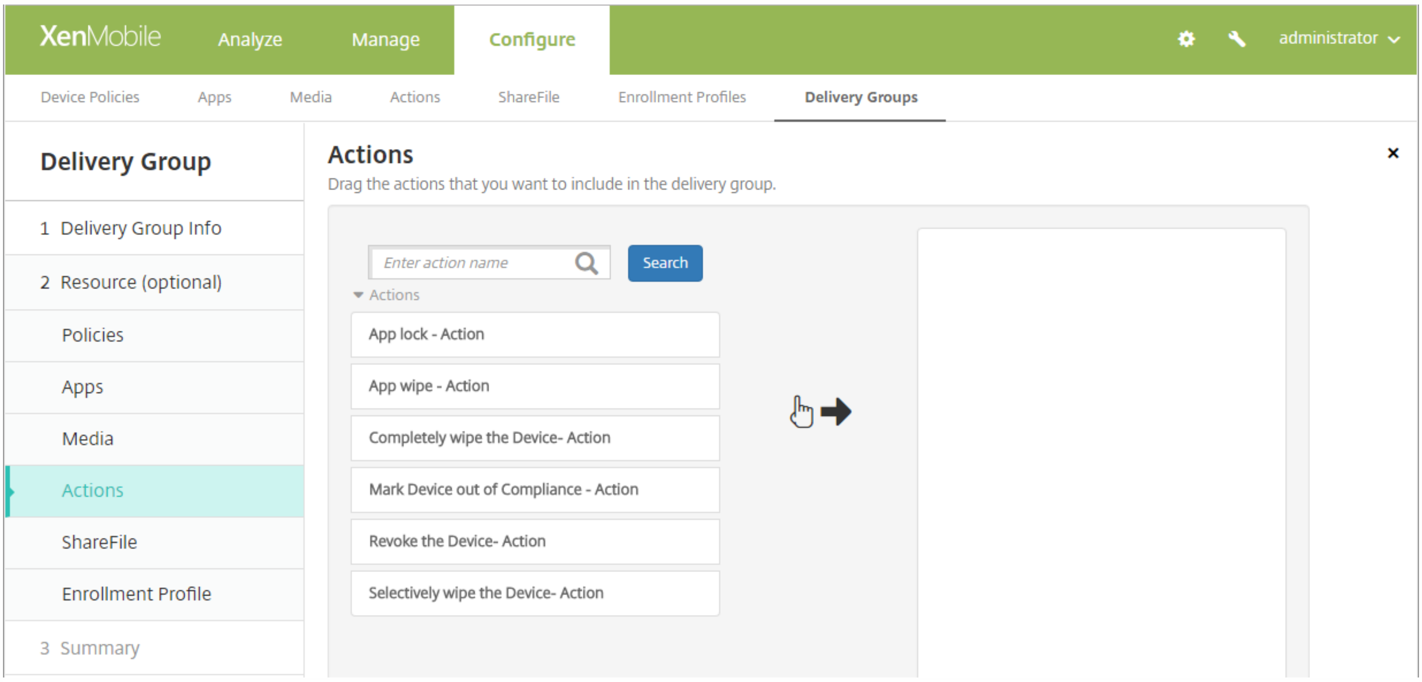


Policies

Drag the policies that you want to include in the delivery group.

Policies

- App Access - Policy
- App Attributes - Policy
- App Inventory - Policy
- App Lock - Policy
- Exchange - Policy
- Location - Policy
- Passcode - Policy
- Store - Policy



Actions

Drag the actions that you want to include in the delivery group.

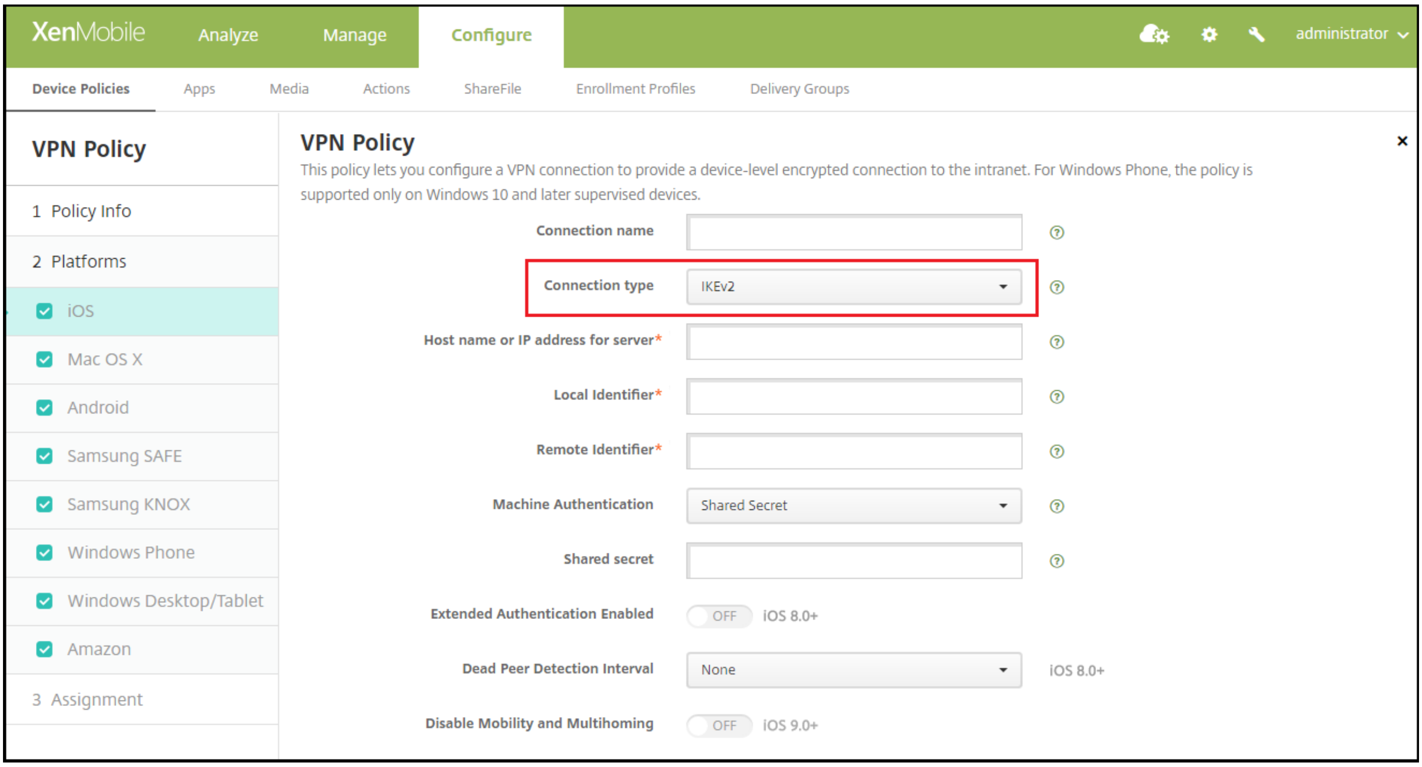
Actions

- App lock - Action
- App wipe - Action
- Completely wipe the Device- Action
- Mark Device out of Compliance - Action
- Revoke the Device- Action
- Selectively wipe the Device- Action

- On the **Manage > Devices** and **Manage > Users** pages, dates now appear in the 24-hour format, dd/mm/yyyy hh:mm:ss. Dates reflect the local time zone for devices and users.

- **The VPN policy for iOS devices now has a per-app VPN option for iKEv2 type VPN policies.** iOS 9.0 and later devices support per-app VPN for iKEv2 connections. The per-app VPN **Enable per-app VPN** options are:

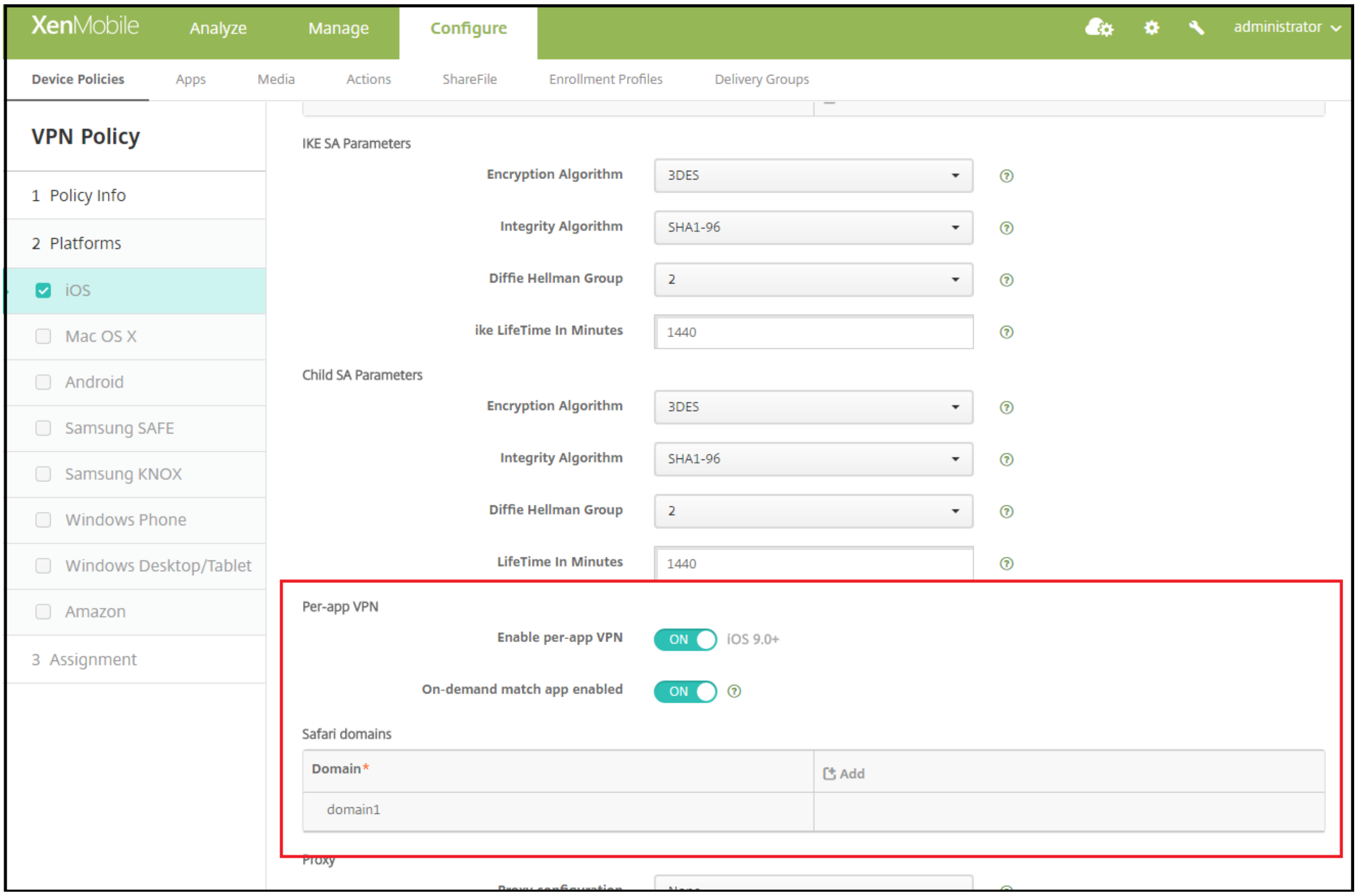
Enable per-app VPN
On-demand match app enabled
Safari domains



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name	
Connection type	IKEv2
Host name or IP address for server*	
Local Identifier*	
Remote Identifier*	
Machine Authentication	Shared Secret
Shared secret	
Extended Authentication Enabled	OFF iOS 8.0+
Dead Peer Detection Interval	None iOS 8.0+
Disable Mobility and Multihoming	OFF iOS 9.0+



IKE SA Parameters

Encryption Algorithm: 3DES

Integrity Algorithm: SHA1-96

Diffie Hellman Group: 2

ike LifeTime In Minutes: 1440

Child SA Parameters

Encryption Algorithm: 3DES

Integrity Algorithm: SHA1-96

Diffie Hellman Group: 2

LifeTime In Minutes: 1440

Per-app VPN

Enable per-app VPN: ON iOS 9.0+

On-demand match app enabled: ON

Safari domains

Domain*	
domain1	

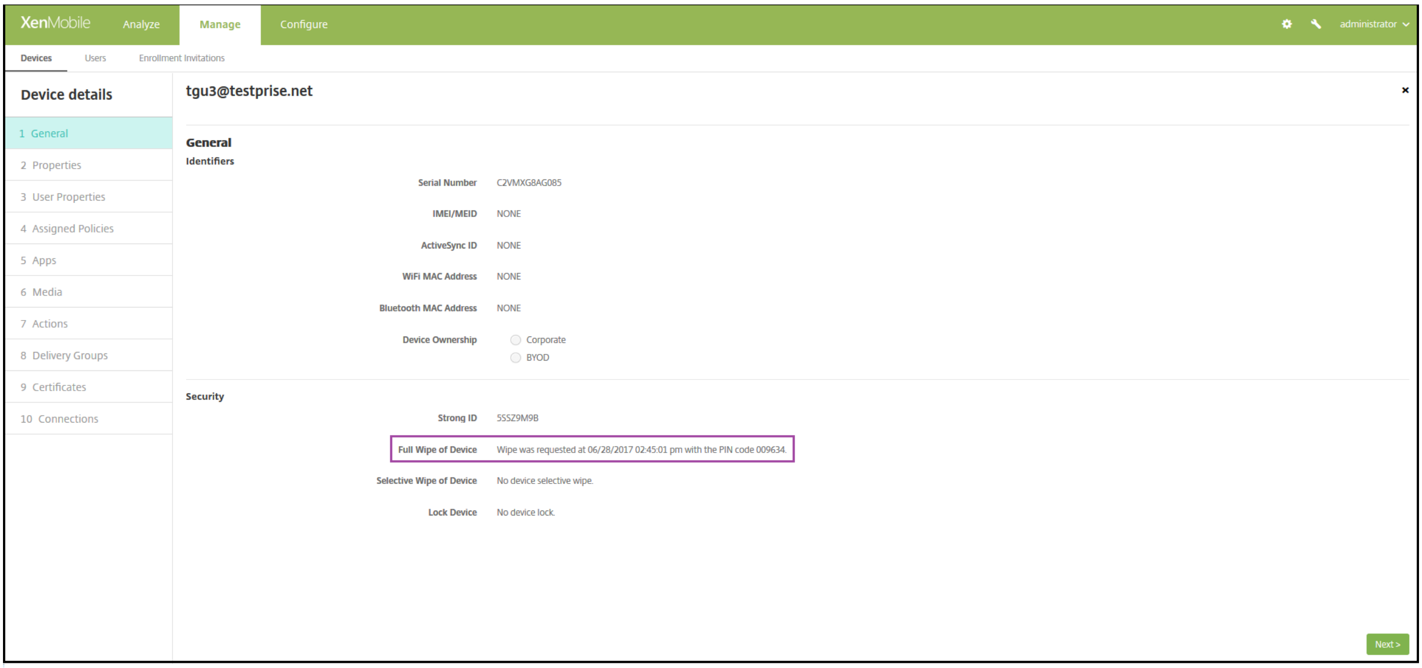
Under the "iOS" section, add to the iKEv2 connection type section:

Enable per-app VPN: Select whether to enable per-app VPN. The default is **OFF**. Available only on iOS 9.0 and later.

On-demand match app enabled: Select whether per-app VPN connections are triggered 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.

- **Wipe code for macOS devices shown in the XenMobile console.** macOS devices require the user to enter a PIN code after the device has been wiped. If the user does not remember this code, you can now look up the wipe code in the **Manage > Device** details page.



tgu3@testprise.net

General

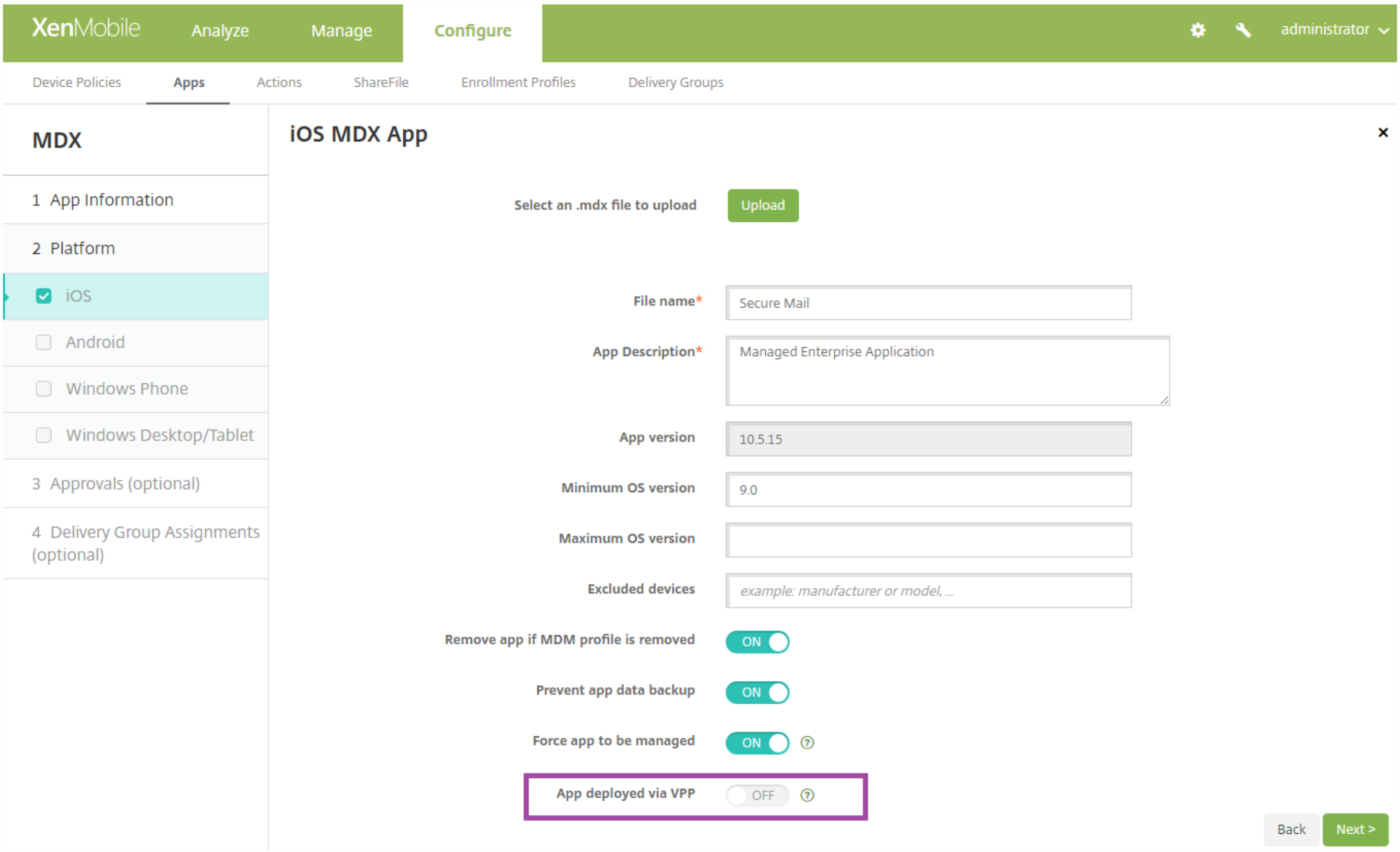
Identifiers

Serial Number	C2VMXG8AG085
IMEI/MEID	NONE
ActiveSync ID	NONE
WiFi MAC Address	NONE
Bluetooth MAC Address	NONE
Device Ownership	○ Corporate ○ BYOD

Security

Strong ID	5SSZ9M9B
Full Wipe of Device	Wipe was requested at 06/28/2017 02:45:01 pm with the PIN code 009634.
Selective Wipe of Device	No device selective wipe.
Lock Device	No device lock.

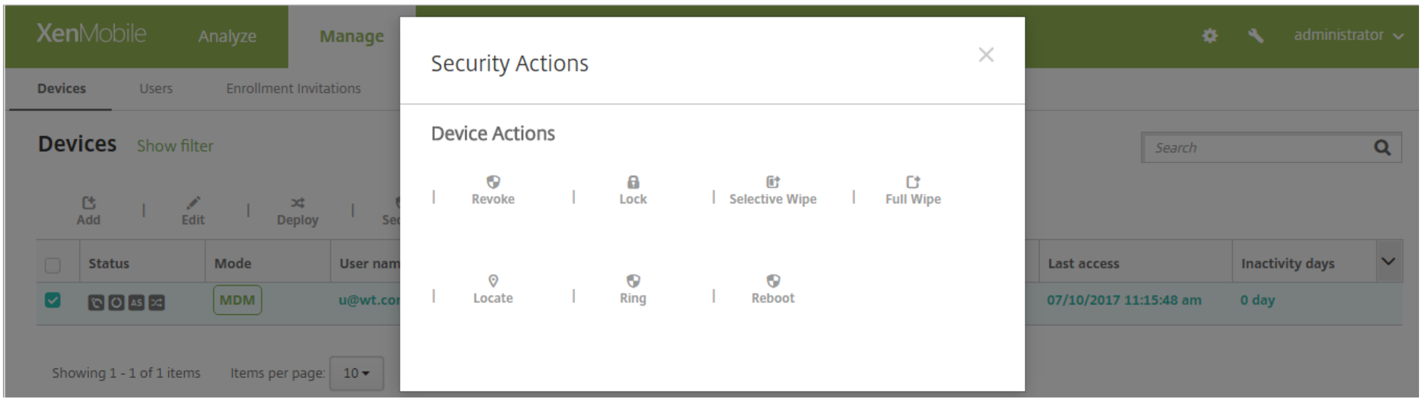
- **When you use VPP to deploy an MDX app, the Secure Hub store now shows only the VPP instance of the app**. Previously, both the VPP and MDX apps appeared in the store. This change prevents end users from installing the MDX version of the app, which requires the user to have an iTunes account. When you add an MDX app, there is a new setting, **App deployed via VPP**. Change that setting to **ON** if you plan to deploy the app by using VPP.



iOS MDX App

Select an .mdx file to upload	Upload
File name*	Secure Mail
App Description*	Managed Enterprise Application
App version	10.5.15
Minimum OS version	9.0
Maximum OS version	
Excluded devices	*example: manufacturer or model, ...*
Remove app if MDM profile is removed	ON
Prevent app data backup	ON
Force app to be managed	ON
App deployed via VPP	OFF

- **Improved performance when importing many VPP licenses**. This optimization uses multi-threading. A new XenMobile Server property, **MaxNumberOfWorker**, defaults to **3** (threads). If you need further optimization, you can increase the number of threads. However, with a larger number of threads, such as 6, a VPP import results in very high CPU usage.
- In the XenMobile console, all references to Mac OS X, OS X, OSX, MACOSX, and MacOS are now macOS.
- **Reboot a Windows 10 device**. You can now send a security action, Reboot, to reboot a device. For Windows Tablet and PCs, the message "System will reboot soon" appears and then the reboot occurs in five minutes. For Windows Phone, there is no warning message to users and the reboot occurs after a few minutes.



Public REST API changes

For the device notification REST services, you can now notify a device by using the device ID, without requiring XenMobile to send a token.

When using the XenMobile Public REST API to create enrollment invitations, you can now:

- **Specify a custom PIN**. If the enrollment mode requires a PIN, you can use a custom PIN instead of the one randomly generated by the XenMobile Server. The PIN length must match the setting configured for the enrollment mode. The PIN length defaults to 8. For example, a request might include: "pin": "12345678"
- **Select multiple platforms**. Previously, you could use the REST API to specify only one platform for an enrollment invitation. The "platform" field is deprecated and replaced with "platforms". For example, a request might include: "platforms": ["iOS", "MACOSX"]

The XenMobile Public API for REST Services now includes the following APIs:

- Get by Container ID
  - MDX mobile apps
  - Enterprise mobile apps
  - WebLink apps
  - Web/SaaS apps
  - Public store apps
- Upload app in new or existing container
  - MDX mobile apps
  - Enterprise mobile apps

- Update platform details inside the container for MDX mobile apps and public store apps
- Add or update app
  - WebLink apps
  - Web/SaaS apps
  - Public store apps
- Get all Web/SaaS connectors or get Web/Saas connectors by connector name
- Delete app container
  - MDX mobile apps
  - Enterprise mobile apps
  - WebLink apps
  - Web/SaaS apps

For details, see XenMobile Public API for REST Services.

What's new in XenMobile Server 10.6

Sep 29, 2017

> ## Note
>
> For the full set of product documentation for XenMobile Server 10.6, see the PDF.
>
> For updates and corrections to the XenMobile Server 10.6 PDF, see XenMobile Server 10.6 documentation errata.

For information about upgrading, see Upgrade. To access the XenMobile management console, use only the XenMobile Server fully qualified domain name or the IP addresses of the node.

XenMobile Server 10.6 includes the following new features and fixed issues.

> ## Important
>
> Touchdown by Symantec reached End of Life on July 3, 2017, with End of Standard Support, End of Extended Support, and End of Support Life on July 2, 2018. For more information, see the Symantec support article, Touchdown End-of-Life, End-of-Availability, and End-of- Support announcement.

Improved deployment of required apps

XenMobile now consistently and promptly installs required apps on managed iOS and Android devices. This improvement resolves deployment issues that occurred primarily for XenMobile configured in enterprise (XME) mode. Users more 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

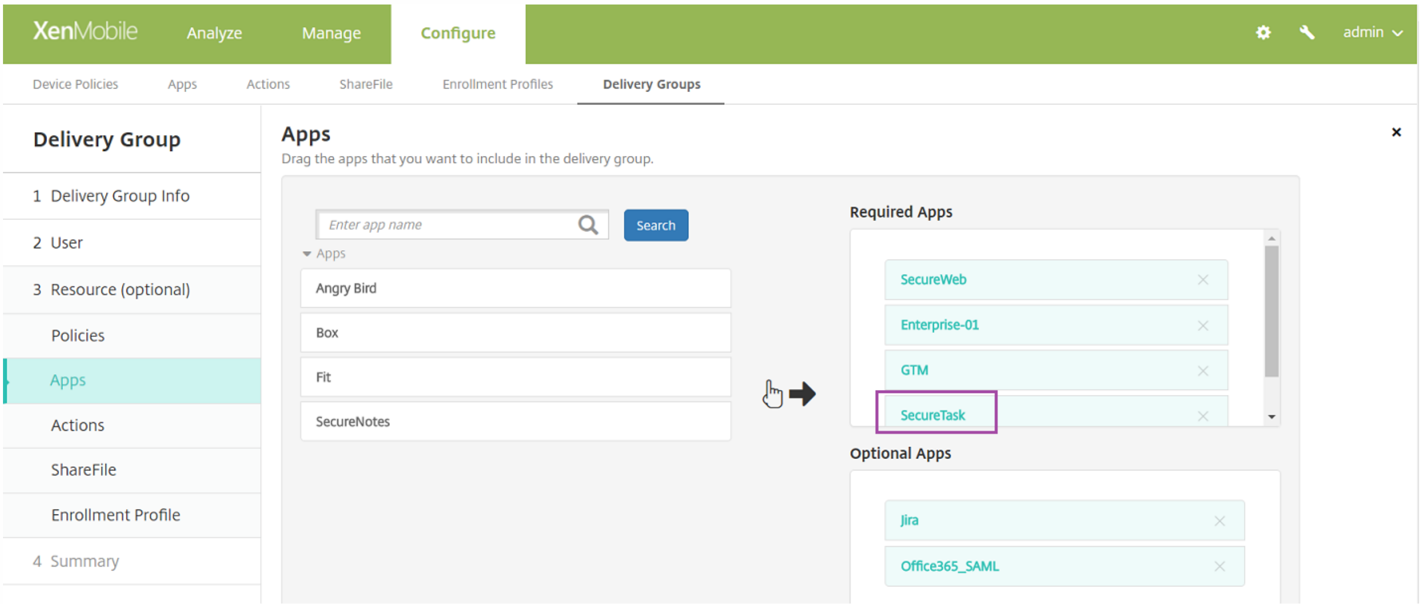
- XenMobile Server 10.6
- Secure Hub (minimum versions: 10.5.15 for iOS; 10.5.20 for Android)
- MDX Toolkit 10.6
- Custom server property, force.server.push.required.apps.

  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.apps** and set the **Value** to **true**.

- After you upgrade XenMobile Server 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.



Apps

Drag the apps that you want to include in the delivery group.

Apps:

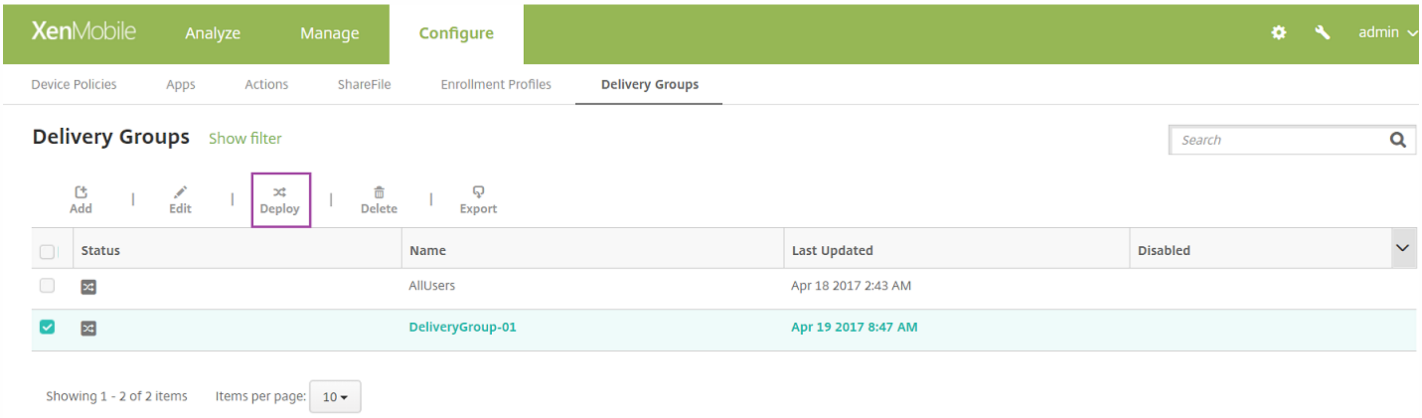
- Angry Bird
- Box
- Fit
- SecureNotes

Required Apps:

- SecureWeb
- Enterprise-01
- GTM
- SecureTask

Optional Apps:

- Jira
- Office365_SAML

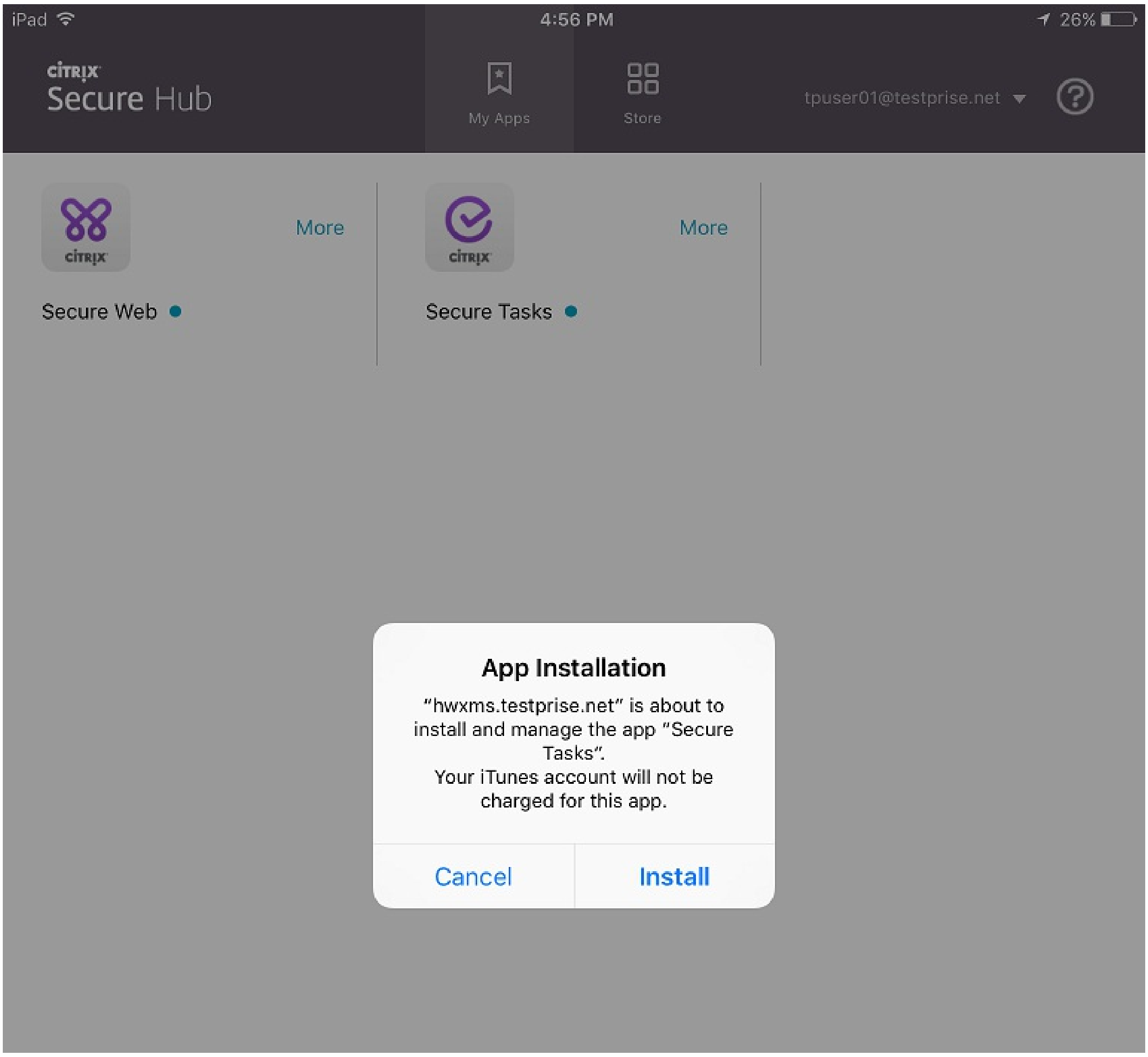


Delivery Groups

☐	Status	Name	Last Updated	Disabled
☐		AllUsers	Apr 18 2017 2:43 AM	
☑		DeliveryGroup-01	Apr 19 2017 8:47 AM	

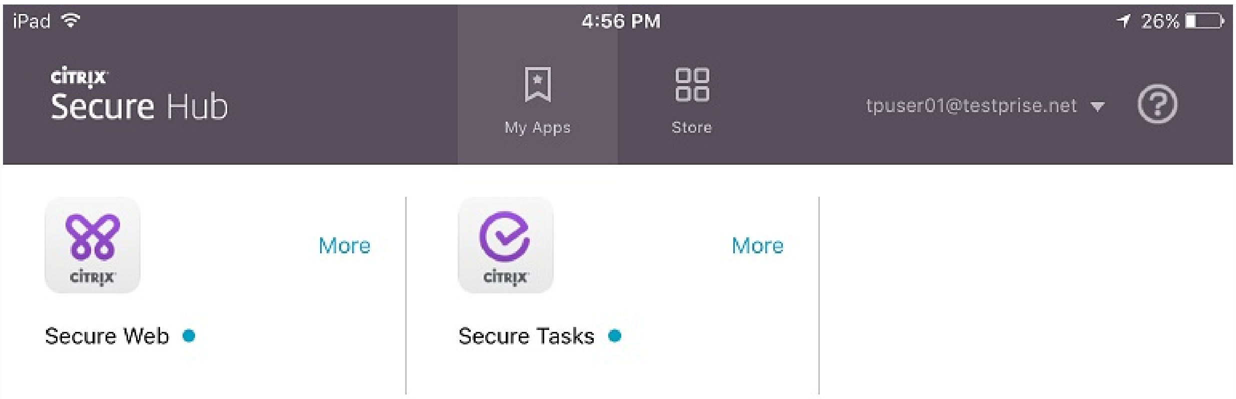
Showing 1 - 2 of 2 items Items per page: 10

After the sample app, Secure Tasks, deploys to the user device, Secure Hub prompts the user to install the app.



App Installation

"hwxms.testprise.net" is about to install and manage the app "Secure Tasks". Your iTunes account will not be charged for this app.



Important

MDX-enabled required apps, including enterprise apps and public app store apps, upgrade immediately, even if you configure an MDX policy for an app update grace period and the user chooses to upgrade the app later.

The following tables describe the administrator and user workflow for required apps. The tables describe the behavior in XenMobile Server versions earlier than version 10.6 as compared to the behavior in version 10.6.

The first table describes the workflow on iOS devices. The second table describes the workflow on Android devices.

iOS required app workflow

Enterprise apps		**Public app store apps**	
Earlier versions	**As of XenMobile Server 10.6**	**Earlier versions**	**As of XenMobile Server 10.6**
Deploy XenMobile App during initial enrollment. Required app is installed on device.	Same.	Deploy XenMobile App during initial enrollment. Required app is installed on device.	Same.
Update the app on the XenMobile console.	Same.	Update the app on the XenMobile console.	Same.
Open the Secure Hub Store on the device. The update icon appears in the store.	Click deploy in the XenMobile console to deploy required apps.	Open the Secure Hub Store on the device. The update icon appears in the store	Click deploy in the XenMobile console to deploy required apps.
The app on the springboard is updated.	The app on the springboard is updated.	The app on the springboard is updated. The upgrade starts automatically. Users are not prompted to update.	The app on the springboard is updated. The upgrade starts automatically. Users are not prompted to update.
Users open the app from the springboard. The app prompts users to upgrade in 7 days.	Users open the app from the springboard. Users are prompted to upgrade in 7 days. Actually, the app is upgraded even when users click Later.	Open the app on the device. The app is upgraded. Users are not prompted after a grace period.	Same.
Users click Later, the upgrade is not started. Users click Update now, the upgrade starts.	The app is upgraded.	Users click Later, the upgrade is not started. Users click Update now, the upgrade starts.	The app is upgraded.

Android required app workflow

Enterprise apps		**Public app store apps**	
Earlier versions	**As of XenMobile Server 10.6**	**Earlier versions**	**As of XenMobile Server 10.6**
Deploy XenMobile App during initial enrollment. Required app is installed on device.	Same.	Same.	Same.
Update the app on the XenMobile console	Click deploy in the XenMobile console to deploy required apps.	Update the app on the XenMobile console	Update the app on the XenMobile console
Open the Secure Hub Store on the device. The update icon appears in the store.	The app is upgraded. (Nexus devices prompt for install updates, but Samsung devices do a silent install.)	Open the Secure Hub Store on the device. The update icon appears in the store.	Click **Deploy** or enter the Secure Hub Store on the device. The update icon appears in the store.
No prompt or update appears on the device springboard.	Users open the app from the springboard. Users are prompted to upgrade in 7 days. In actuality, the app is upgraded even when users click **Later**.	Users must manually click the update icon in the Secure Hub Store to upgrade. (Nexus prompts users to install updates.)	App upgrade starts automatically. (Nexus devices prompt users to install the update.)
Users open the app from the springboard. The app prompts users to upgrade in 7 days.	App is upgraded.	Open the app on the springboard. The app is upgraded. Users are not prompted for a grace period.	Open the app on the springboard. The app is upgraded. Users are not prompted for a grace period.
Users click **Later**, the upgrade does not start. Users click **Update now**, the upgrade starts. (Users are not prompted to install on Samsung devices, but Nexus prompts for an update.)	The app is upgraded. (Samsung devices do a silent install.)	Users click **Later**, the upgrade does not start. Users click **Update now**. The upgrade starts.	The app is upgraded. (Samsung devices do a silent install.)

Configure an on-premises NetScaler Gateway for use with XenMobile Server

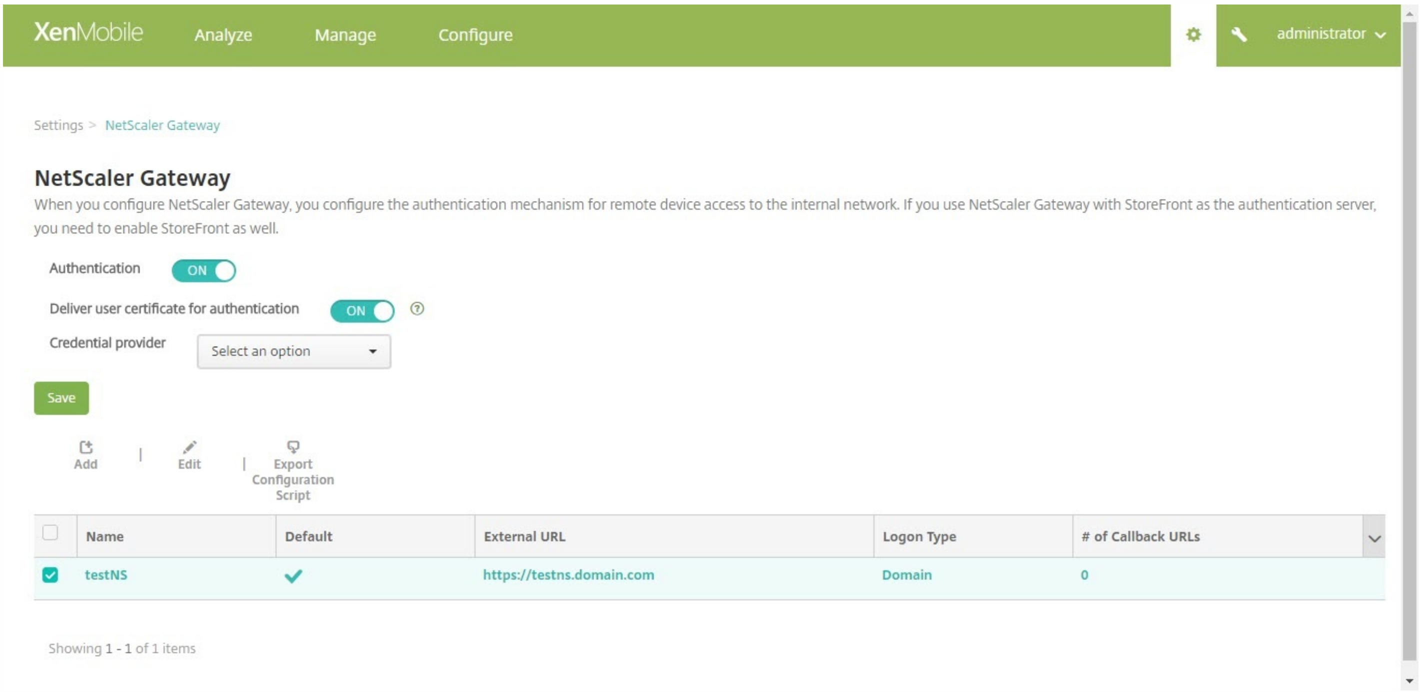
Starting with XenMobile 10.6, you configure NetScaler Gateway for use with XenMobile Server by exporting a script from XenMobile that you run on NetScaler Gateway. The script configures these NetScaler Gateway settings required by XenMobile:

- NetScaler Gateway virtual servers needed for MDM and MAM
- Session policies for the NetScaler Gateway virtual servers
- XenMobile Server details
- 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 NetScaler
- Other bindings: Service policy, CA certificate

The script doesn't handle the following configuration:

- Exchange load balancing
- ShareFile load balancing
- ICA Proxy configuration
- SSL Offload

If a NetScaler Gateway instance exists, the **Settings > NetScaler Gateway** page now has an **Export Configuration Script** button.



NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication: ON

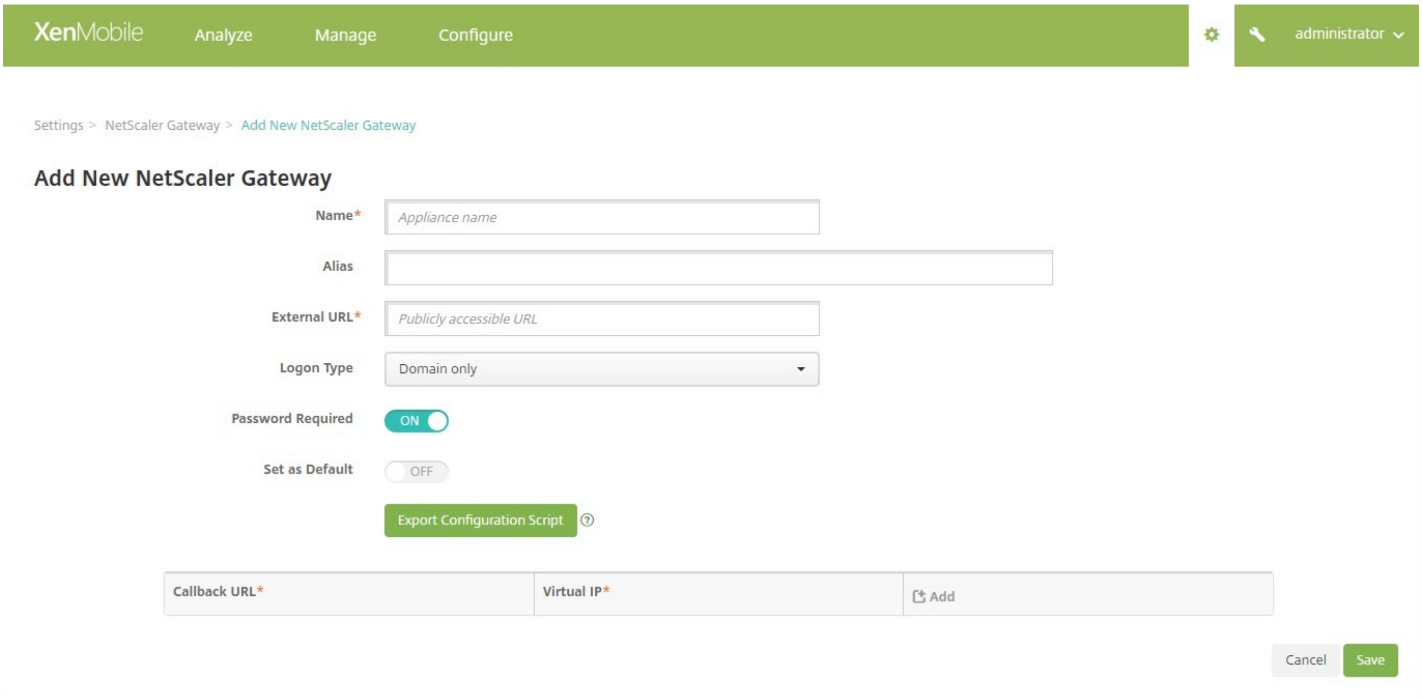
Deliver user certificate for authentication: ON

Credential provider: Select an option

☐	Name	Default	External URL	Logon Type	# of Callback URLs
☑	testNS	✓	https://testns.domain.com	Domain	0

Showing 1 - 1 of 1 items

The **Add New NetScaler Gateway** page also includes a link to export the configuration script.



Add New NetScaler Gateway

Name* Appliance name

Alias

External URL* Publicly accessible URL

Logon Type Domain only

Password Required ON

Set as Default OFF

Export Configuration Script

Callback URL*	Virtual IP*	Add

For more information, see NetScaler Gateway and XenMobile.

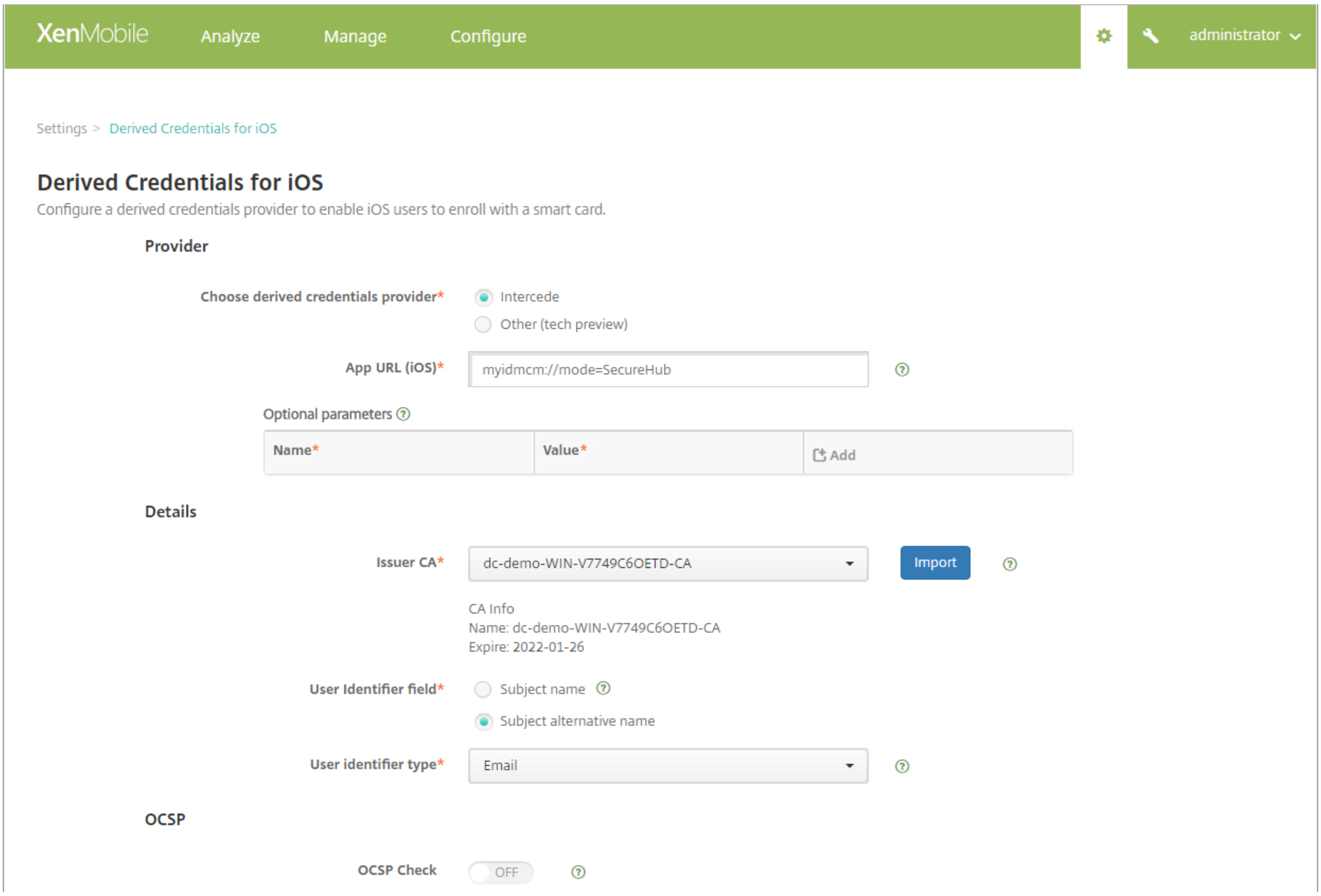
Derived credentials for iOS device enrollment

Derived credentials provide strong authentication for mobile devices. The credentials, derived from a smart card, reside in a mobile device instead of the card. The smart card is either a Personal Identity Verification (PIV) card or Common Access Card (CAC).

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

XenMobile can use derived credentials for iOS device enrollment. If configured for derived credentials, XenMobile doesn't support enrollment invitations or other enrollment modes for iOS devices. However, you can use the same XenMobile Server to enroll Android devices through enrollment invitations and other enrollment modes.

Configure derived credentials by using the **Settings > Derived Credentials for iOS** page. By default, the XenMobile console doesn't include **Settings > Derived Credentials**. To enable the interface for derived credentials, go to **Settings > Server Properties,** add the server property **derived.credentials.enable**, and set it to **true**.



Derived Credentials for iOS

Configure a derived credentials provider to enable iOS users to enroll with a smart card.

Provider

Choose derived credentials provider* ● Intercede ○ Other (tech preview)

App URL (iOS)* myidmcm://mode=SecureHub

Optional parameters

Name*	Value*

Details

Issuer CA* dc-demo-WIN-V7749C6OETD-CA

CA Info
Name: dc-demo-WIN-V7749C6OETD-CA
Expire: 2022-01-26

User Identifier field* ○ Subject name ● Subject alternative name

User identifier type* Email

OCSP

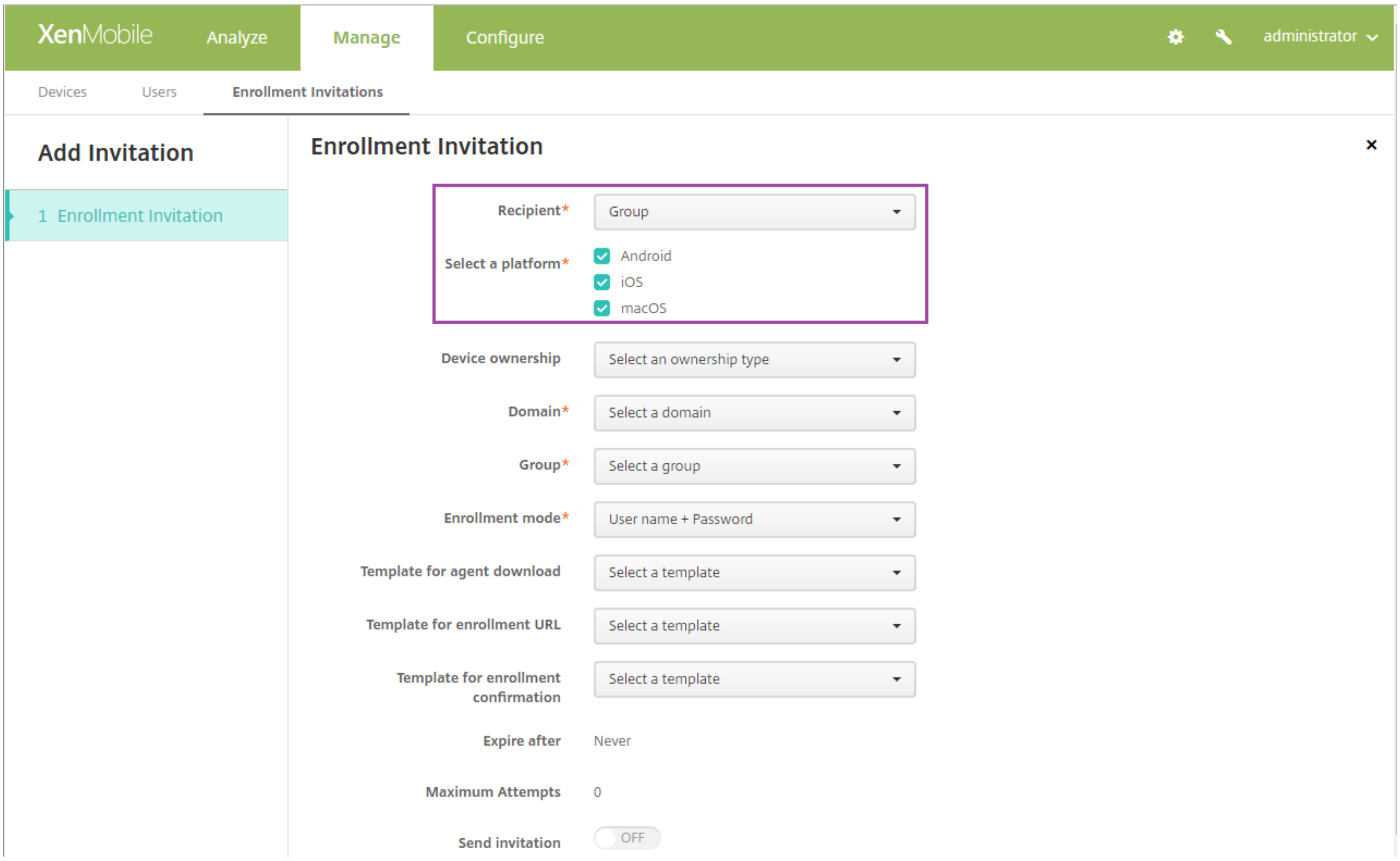
OCSP Check OFF

For more information, see Derived credentials for iOS. For information about the REST API for derived credentials, see the XenMobile REST API Reference PDF.

Select multiple device platforms for enrollment invitations

You can now select any combination of iOS, macOS, and Android device platforms for an enrollment invitation. The **Manage > Enrollment Invitations** page includes a **Select a platform** setting. The platforms selected determine the **Enrollment mode** options shown and whether some settings, such as **Device info**, appear.

If **Recipient** is **Group**, all platforms are selected by default.



Enrollment Invitation

Recipient*: Group

Select a platform*: ☑ Android ☑ iOS ☑ macOS

Device ownership: Select an ownership type

Domain*: Select a domain

Group*: Select a group

Enrollment mode*: User name + Password

Template for agent download: Select a template

Template for enrollment URL: Select a template

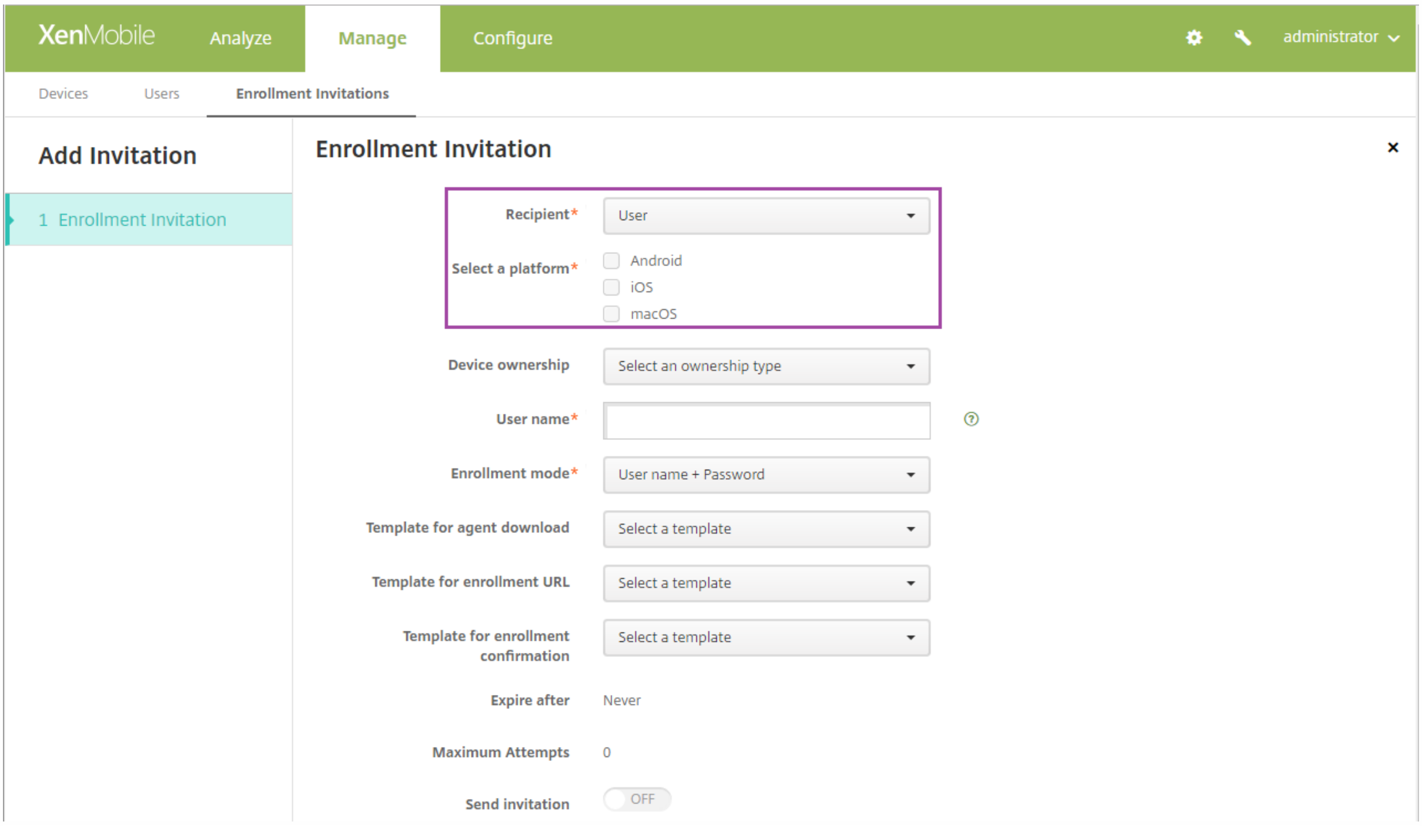
Template for enrollment confirmation: Select a template

Expire after: Never

Maximum Attempts: 0

Send invitation: OFF

If **Recipient** is **User**, no platforms are selected by default.



Enrollment Invitation

Recipient*: User

Select a platform*: □ Android □ iOS □ macOS

Device ownership: Select an ownership type

User name*:

Enrollment mode*: User name + Password

Template for agent download: Select a template

Template for enrollment URL: Select a template

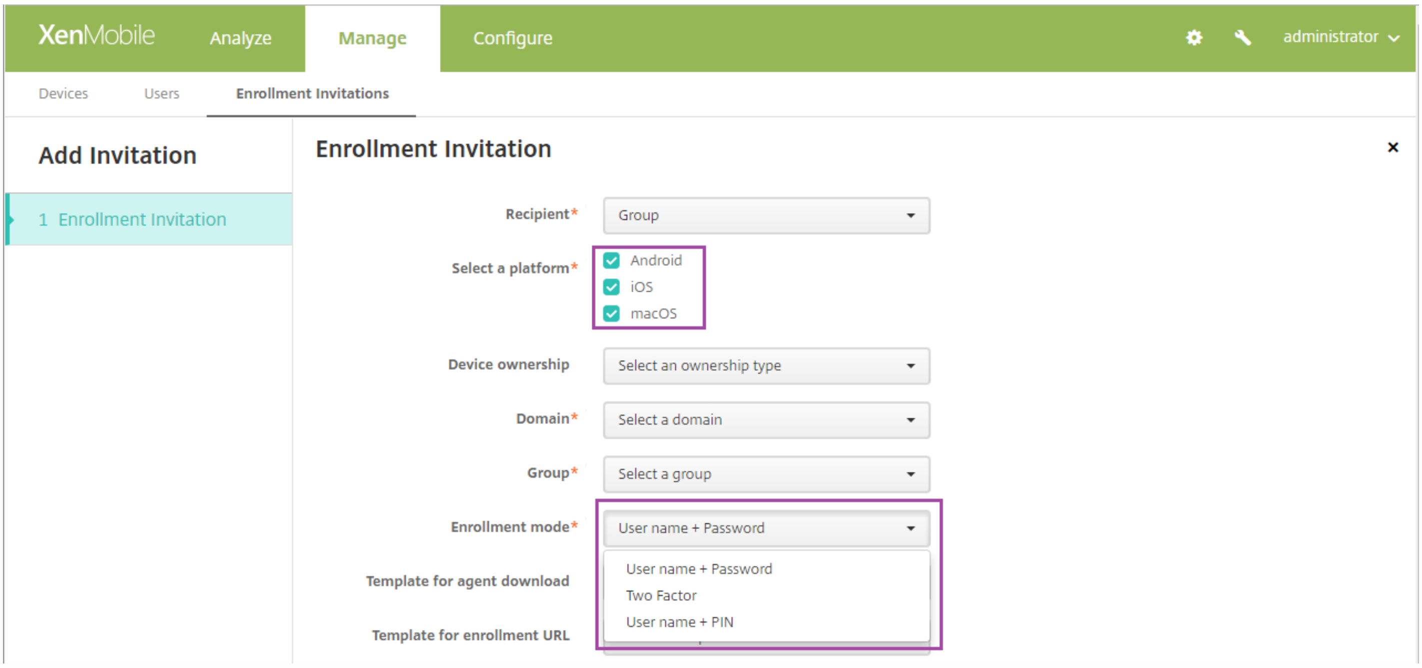
Template for enrollment confirmation: Select a template

Expire after: Never

Maximum Attempts: 0

Send invitation: OFF

Only the **Enrollment mode** options that are valid for each of the selected platforms appear. For example, if all platforms are selected, the valid enrollment modes for that combination are User name + Password, Two Factor, and User name + PIN.



Enrollment Invitation

Recipient*: Group

Select a platform*:
☑ Android
☑ iOS
☑ macOS

Device ownership: Select an ownership type

Domain*: Select a domain

Group*: Select a group

Enrollment mode*: User name + Password
- User name + Password
- Two Factor
- User name + PIN

Template for agent download

Template for enrollment URL

More enrollment options for macOS devices

In addition to enrolling macOS users by sending an enrollment link, you can now enroll macOS users by sending an enrollment invitation. Both methods enable macOS users to enroll over the air, directly from their devices.

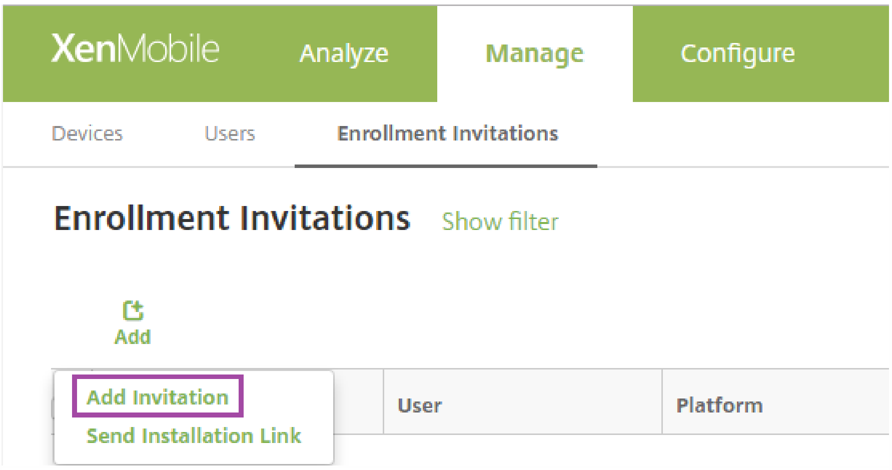
An enrollment invitation can use any of the following enrollment modes for macOS devices:

- User name + PIN
- User name + password
- Two Factor

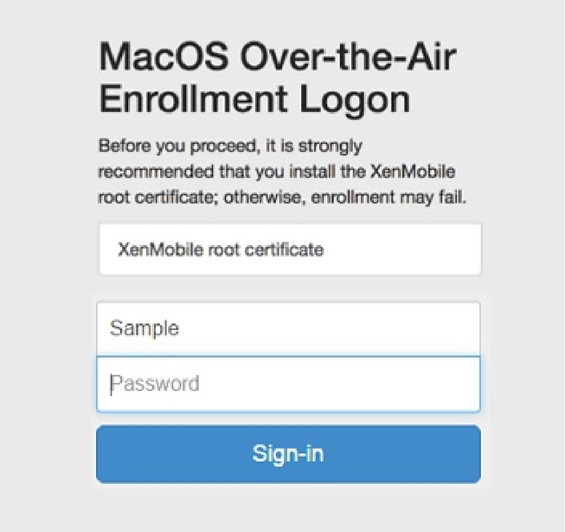
When the user follows the instructions in the enrollment invitation, a sign-on screen with the user name filled in appears.

To send macOS device users an enrollment invitation:

1. Add an invitation for macOS user enrollment. For more information, see Send users an enrollment invitation.



2. After users receive the invitation and click the link, the following screen appears in the Safari browser. XenMobile fills in the user name. If you chose **Two Factor** for the enrollment mode, an extra field appears.



MacOS Over-the-Air Enrollment Logon

Before you proceed, it is strongly recommended that you install the XenMobile root certificate; otherwise, enrollment may fail.

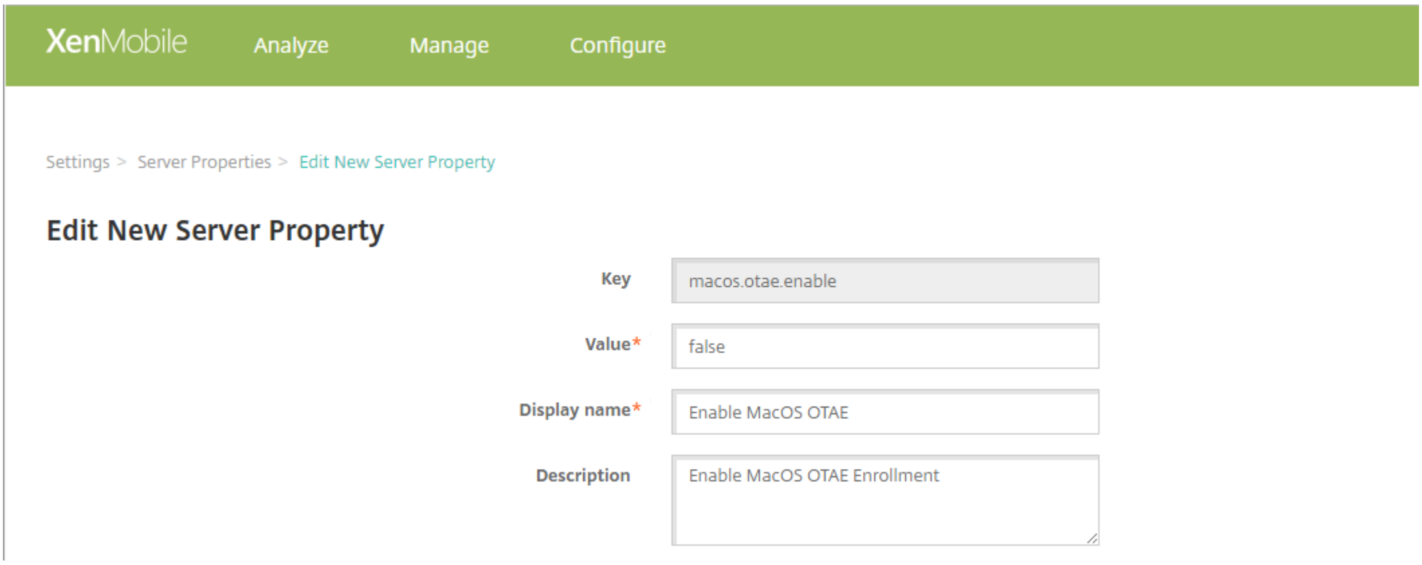
3. Users install certificates as necessary. If you configured a publicly trusted SSL certificate and a publicly trusted digital signing certificate for macOS, XenMobile doesn't prompt users to install a certificate. For more information about certificates, see Certificates and Authentication.

4. Users provide the requested credentials.

   You can now start managing Macs with XenMobile just as you manage mobile devices.

To prevent enrollment with an installation link on macOS devices:

You can prevent the use of an enrollment link for macOS devices by setting new server property, **Enable macOS OTAE** (**macos.otae.enable**), to **false**. As a result, macOS users can enroll only by using an enrollment invitation.



Settings > Server Properties > Edit New Server Property

Edit New Server Property

Key	macos.otae.enable
Value*	false
Display name*	Enable MacOS OTAE
Description	Enable MacOS OTAE Enrollment

Windows Information Protection device policy

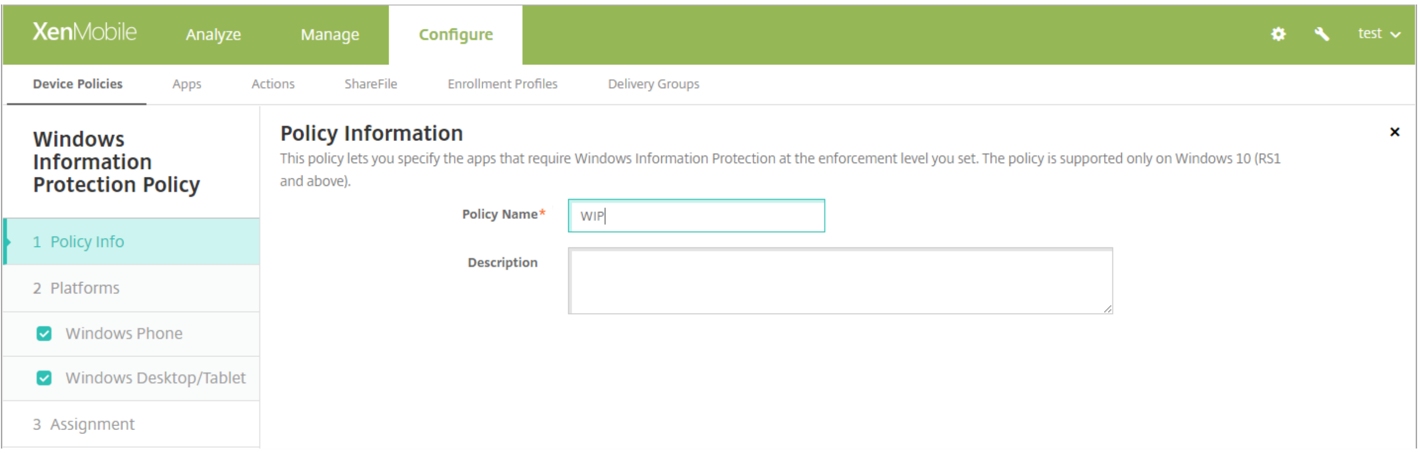
Windows Information Protection (WIP), previously known as enterprise data protection (EDP), is a Windows 10 technology that protects against the potential leakage of enterprise data. Data leakage can occur through sharing of enterprise data to non-enterprise protected apps, between apps, or outside of the network of your organization. For more information, see Protect your enterprise data using Windows Information Protection (WIP) on Microsoft TechNet.

You can create a device policy in XenMobile to specify the apps that require Windows Information Protection at the enforcement level you set. The policy, Windows Information Protection, is for Windows 10 version 1607 and later supervised Phone, Tablet, and Desktop.

You specify 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 create the policy, go to **Configure > Device Policies** and add the **Windows Information Protection** policy.



Windows Information Protection Policy

1 Policy Info

2 Platforms

☑ Windows Phone

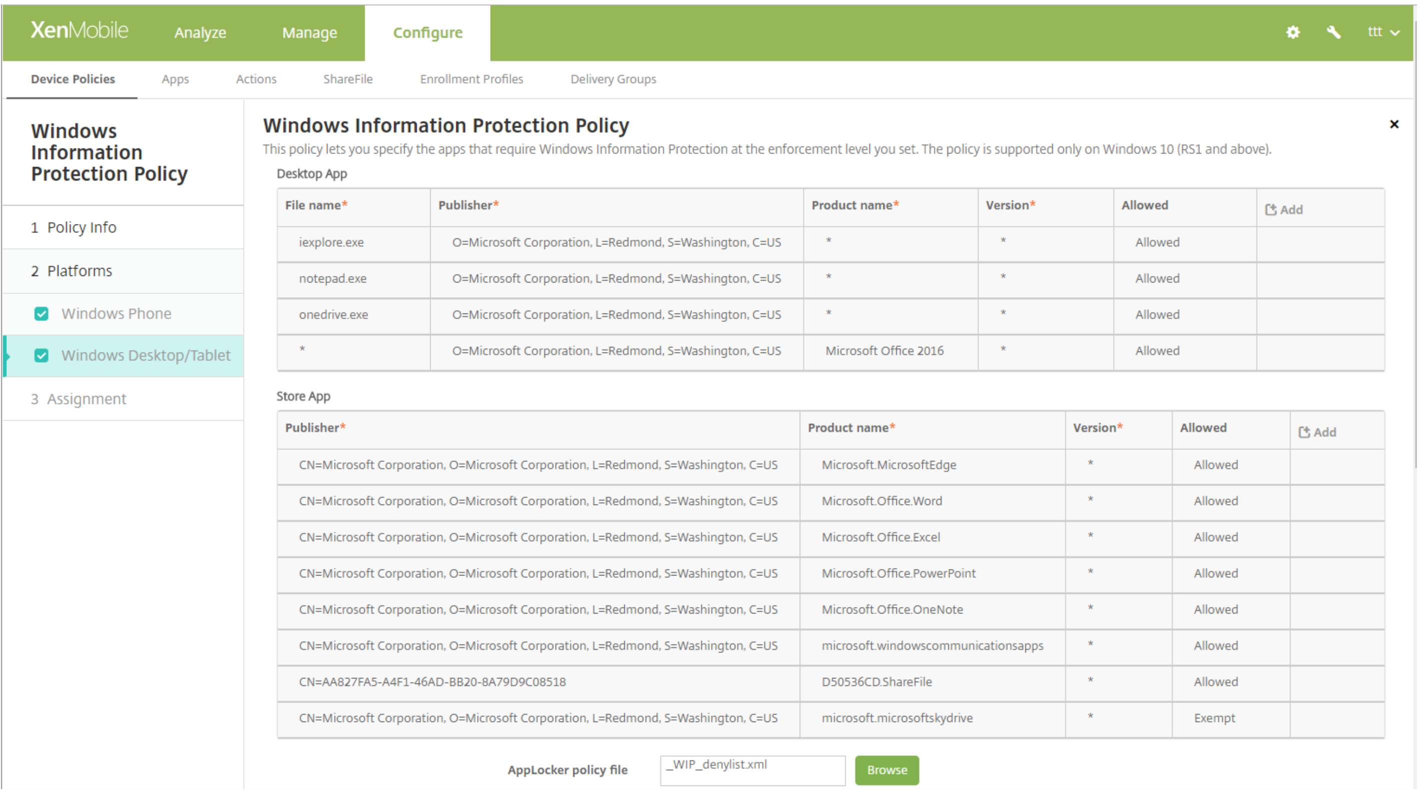
☑ Windows Desktop/Tablet

3 Assignment

Policy Information

This policy lets you specify the apps that require Windows Information Protection at the enforcement level you set. The policy is supported only on Windows 10 (RS1 and above).

Policy Name*	WIP
Description	



Windows Information Protection Policy

This policy lets you specify the apps that require Windows Information Protection at the enforcement level you set. The policy is supported only on Windows 10 (RS1 and above).

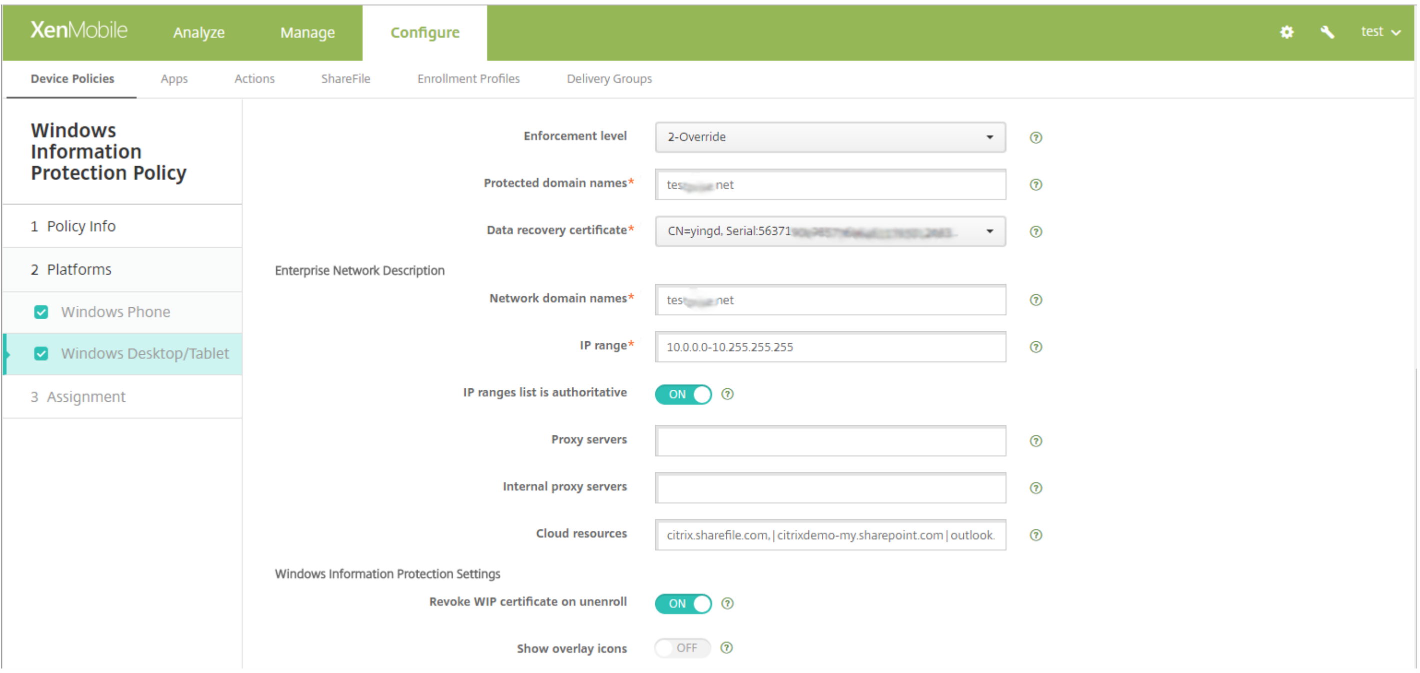
Desktop App

File name*	Publisher*	Product name*	Version*	Allowed	Add
iexplore.exe	O=Microsoft Corporation, L=Redmond, S=Washington, C=US	*	*	Allowed	
notepad.exe	O=Microsoft Corporation, L=Redmond, S=Washington, C=US	*	*	Allowed	
onedrive.exe	O=Microsoft Corporation, L=Redmond, S=Washington, C=US	*	*	Allowed	
*	O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft Office 2016	*	Allowed	

Store App

Publisher*	Product name*	Version*	Allowed	Add
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft.MicrosoftEdge	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft.Office.Word	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft.Office.Excel	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft.Office.PowerPoint	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft.Office.OneNote	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	microsoft.windowscommunicationsapps	*	Allowed	
CN=AA827FA5-A4F1-46AD-BB20-8A79D9C08518	D50536CD.ShareFile	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	microsoft.microsoftskydrive	*	Exempt	

AppLocker policy file: _WIP_denylist.xml



Enforcement level: 2-Override

Protected domain names*: tes[redacted]net

Data recovery certificate*: CN=yingd, Serial:56371[redacted]

Enterprise Network Description

Network domain names*: tes[redacted]net

IP range*: 10.0.0.0-10.255.255.255

IP ranges list is authoritative: ON

Proxy servers:

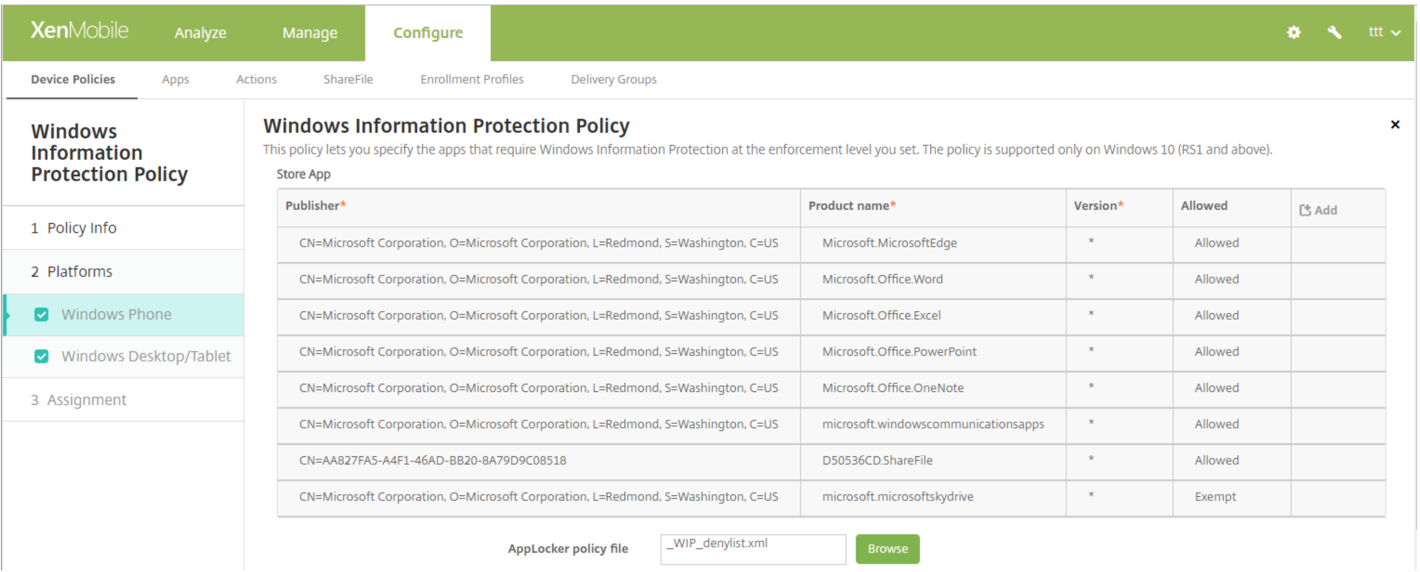
Internal proxy servers:

Cloud resources: citrix.sharefile.com,|citrixdemo-my.sharepoint.com|outlook.

Windows Information Protection Settings

Revoke WIP certificate on unenroll: ON

Show overlay icons: OFF



Windows Information Protection Policy

This policy lets you specify the apps that require Windows Information Protection at the enforcement level you set. The policy is supported only on Windows 10 (RS1 and above).

Store App

Publisher*	Product name*	Version*	Allowed	Add
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft.MicrosoftEdge	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft.Office.Word	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft.Office.Excel	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft.Office.PowerPoint	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Microsoft.Office.OneNote	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	microsoft.windowscommunicationsapps	*	Allowed	
CN=AA827FA5-A4F1-46AD-BB20-8A79D9C08518	D50536CD.ShareFile	*	Allowed	
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	microsoft.microsoftskydrive	*	Exempt	

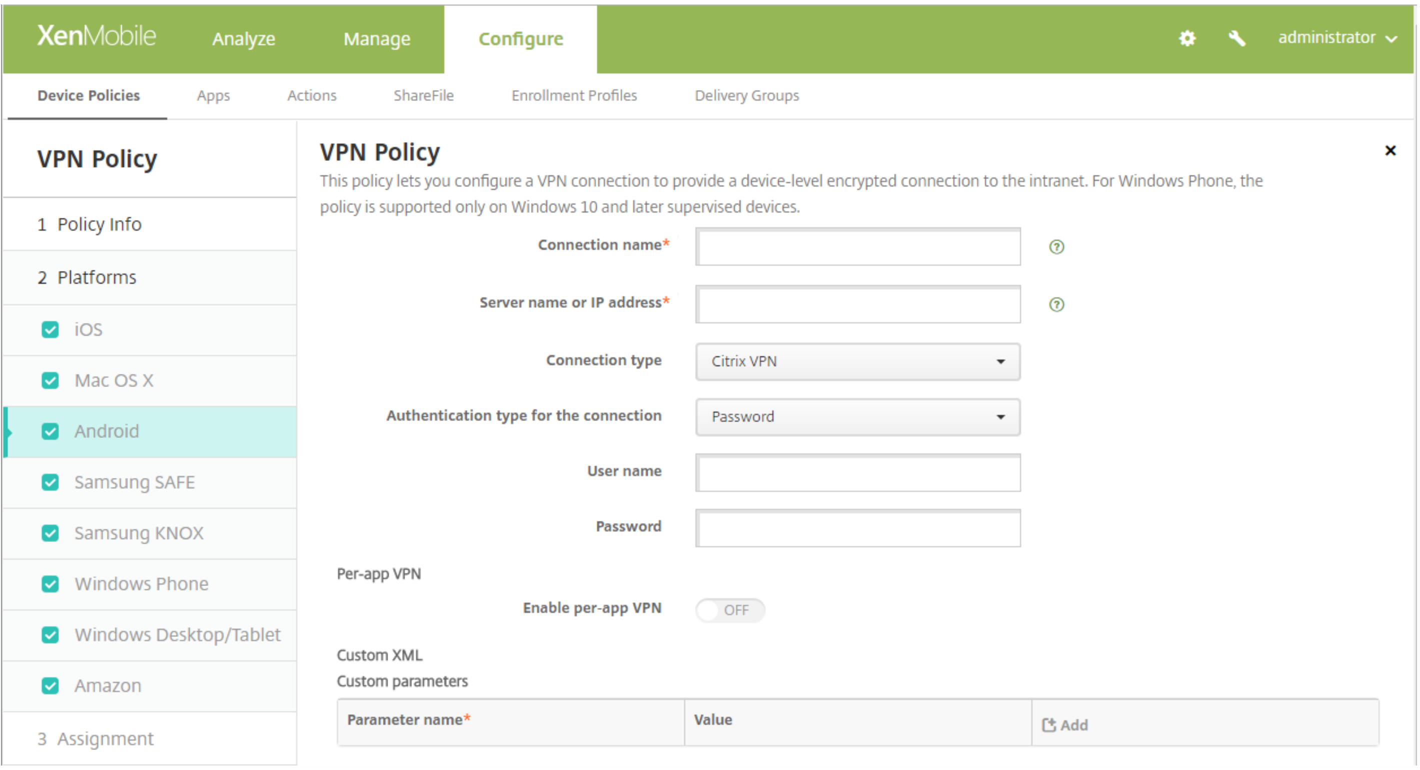
AppLocker policy file: _WIP_denylist.xml

For more information, see Windows Information Protection device policy.

Citrix VPN connection type for Android devices

The VPN device policy for Android now supports configuring Citrix VPN. Citrix VPN is a mobile application that connects to NetScaler Gateway in full VPN mode, as opposed to a clientless VPN or ICA proxy mode. This feature requires Secure Hub 10.6.

On the **Configure > Device Policies** page for Android, the **Connection type** menu now includes **Citrix VPN.**



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name*:

Server name or IP address*:

Connection type: Citrix VPN

Authentication type for the connection: Password

User name:

Password:

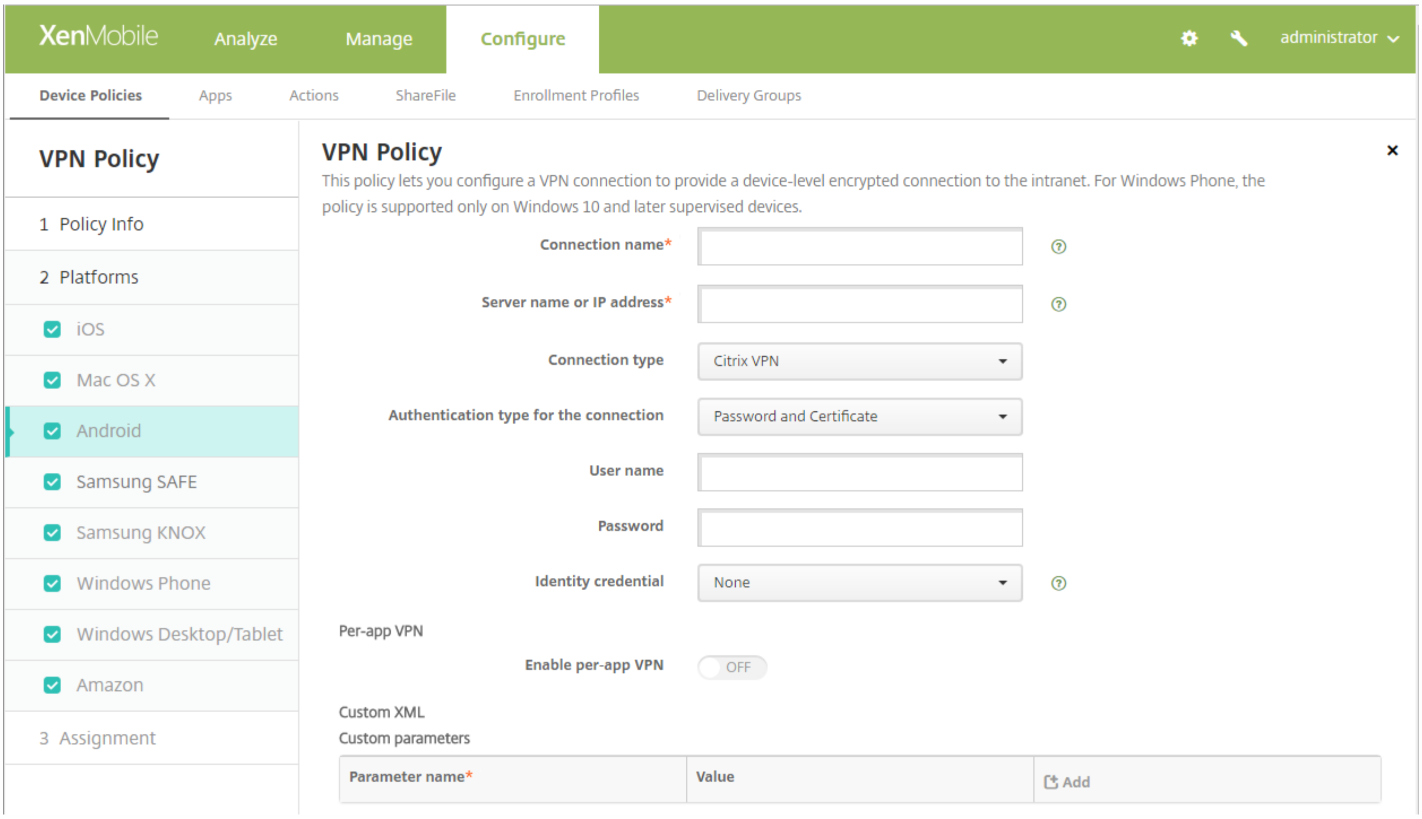
Per-app VPN

Enable per-app VPN: OFF

Custom XML

Custom parameters

Parameter name*	Value	Add



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name*

Server name or IP address*

Connection type: Citrix VPN

Authentication type for the connection: Password and Certificate

User name

Password

Identity credential: None

Per-app VPN

Enable per-app VPN: OFF

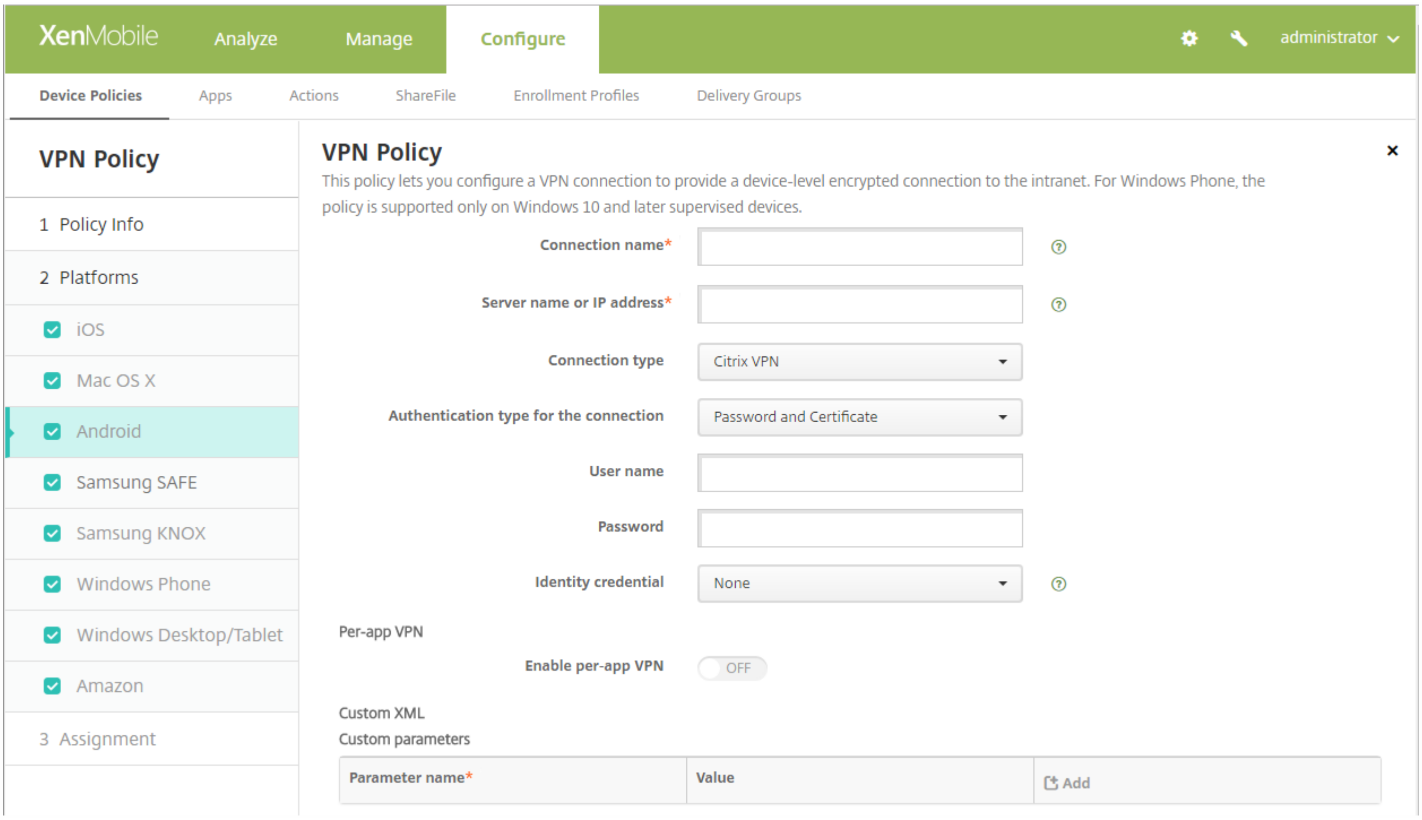
Custom XML

Custom parameters

Parameter name*	Value	Add

Settings for the Citrix VPN connection type:

- **Server name or IP address**: Type the FQDN or IP address of the NetScaler Gateway.
- **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**.
- **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**: Choose a setting. If **Whitelist**, all apps in the whitelist tunnel through this VPN. If **Blacklist**, all apps except any 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. XenMobile supports these parameters for Citrix VPN:
  - **disableL3Mode**: Optional. To enable this parameter, type **Yes** for the **Value**. If enabled, no user-added VPN connections are displayed and the user cannot add another connection. The restriction is global 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 is appended to the existing Citrix VPN user agent.



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name*

Server name or IP address*

Connection type: Citrix VPN

Authentication type for the connection: Password and Certificate

User name

Password

Identity credential: None

Per-app VPN

Enable per-app VPN: OFF

Custom XML

Custom parameters

Parameter name*	Value	

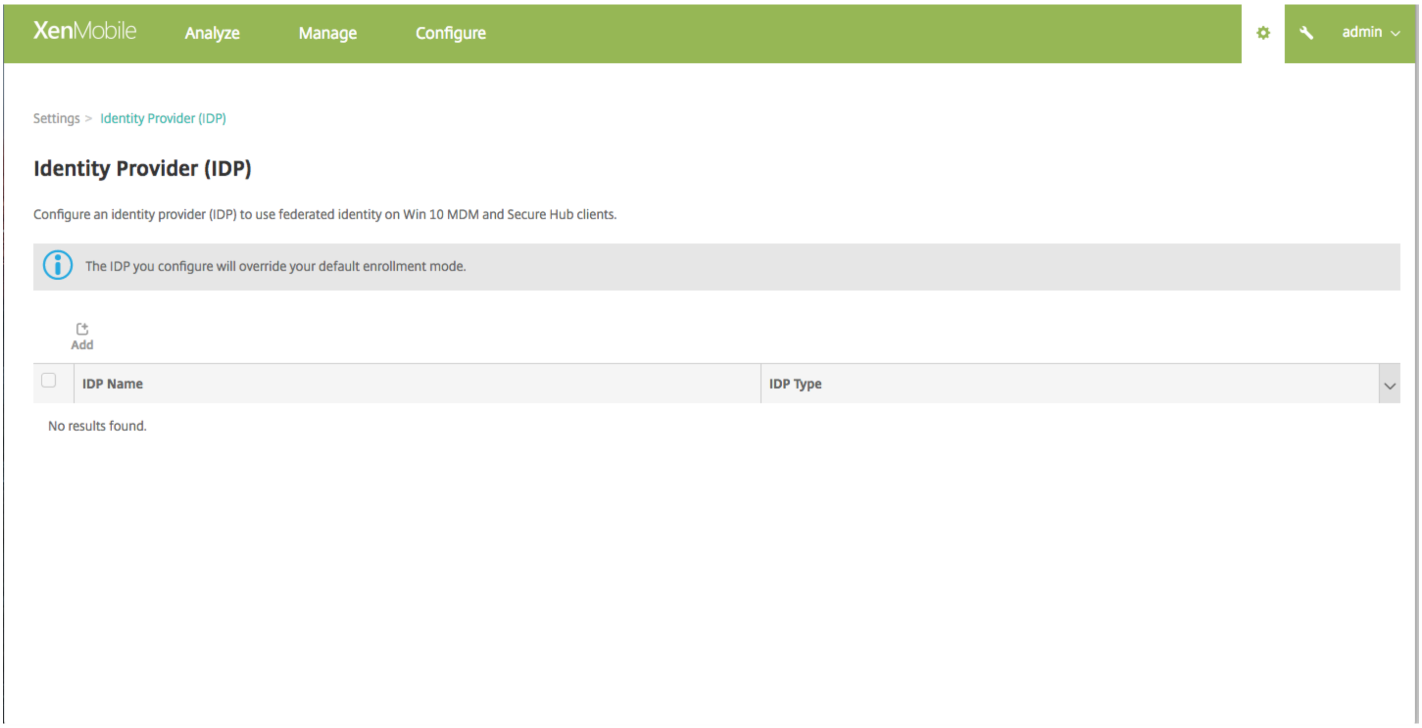
For more information, see VPN device policy.

XenMobile integration with Azure Active Directory as IDP

Configuring Azure Active Directory (AD) as your identity provider (IDP) lets users enroll in XenMobile using their Azure credentials.

iOS, Android, and Windows 10 devices are supported. iOS and Android devices enroll through Secure Hub.

You configure Azure as your IDP under **Settings > Authentication > IDP**. The **IDP** page is new to this version of XenMobile. In previous versions of XenMobile, you configured Azure under **Settings > Microsoft Azure**.



Settings > Identity Provider (IDP)

Identity Provider (IDP)

Configure an identity provider (IDP) to use federated identity on Win 10 MDM and Secure Hub clients.

The IDP you configure will override your default enrollment mode.

Add

□	IDP Name	IDP Type

No results found.

For more information, see XenMobile integration with Azure Active Directory as IDP.

Deploy device policies, apps, and smart actions based on app ID

You can now configure XenMobile to deploy device policies, apps, and smart actions based on app ID. To do that, you use a new deployment rule, **Installed app name**.

You can use this new feature to migrate from enterprise app store distribution to public app store distribution:

- Use the **Installed app name** rule with the App Uninstall device policy. Doing so triggers XenMobile to remove enterprise apps from user devices after the public app store version installs.
- This feature is available only for managed iOS devices connected to a XenMobile Server in enterprise mode (XME).

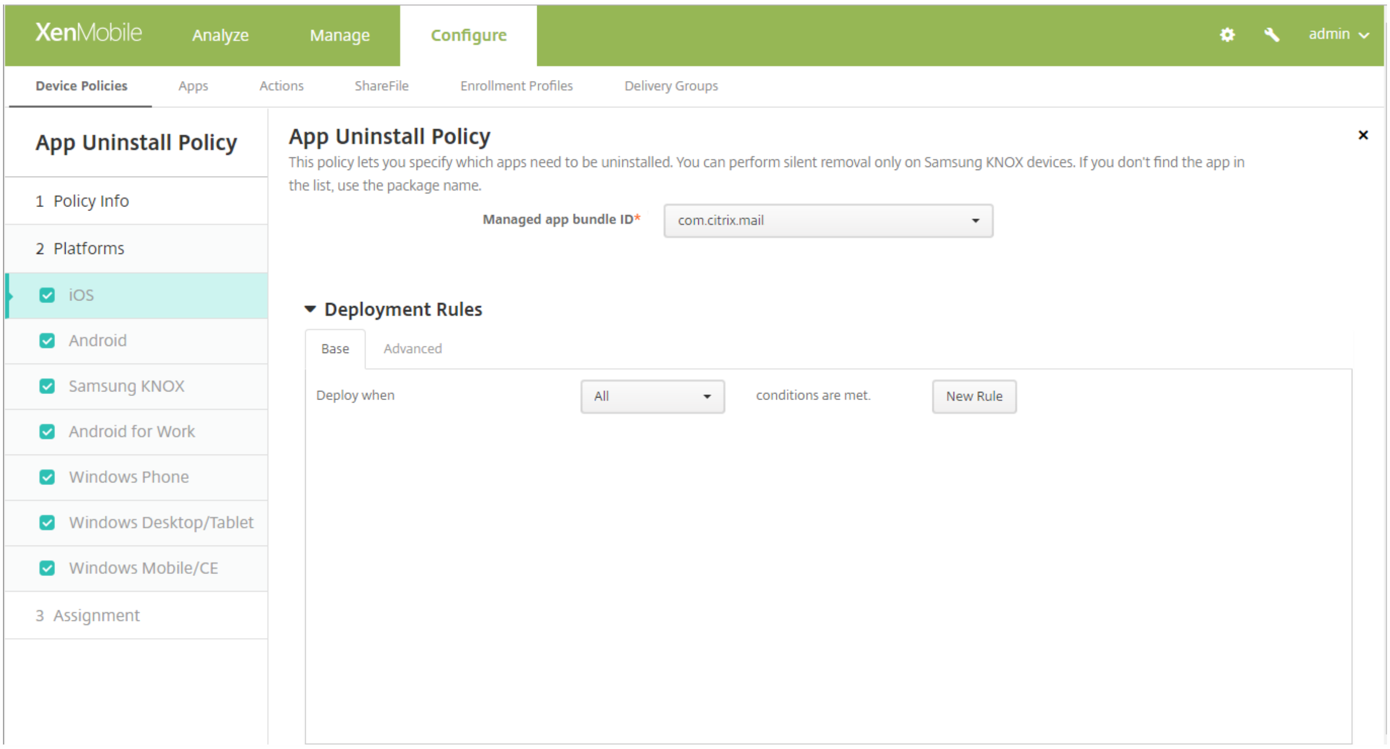
> ## Note
>
> Citrix requires that you use public app store versions of Citrix apps, instead of Enterprise versions, by the end of 2017.

To configure the App Uninstall device policy for an Enterprise app:

1. In **Configure > Device Policies**, click **Add**, and then click **App Uninstall**.

2. Name the policy and then remove the check boxes for all but the **iOS** platform.

3. On the **iOS** page, choose the app bundle ID for the old Enterprise app and then expand **Deployment Rules**.



App Uninstall Policy

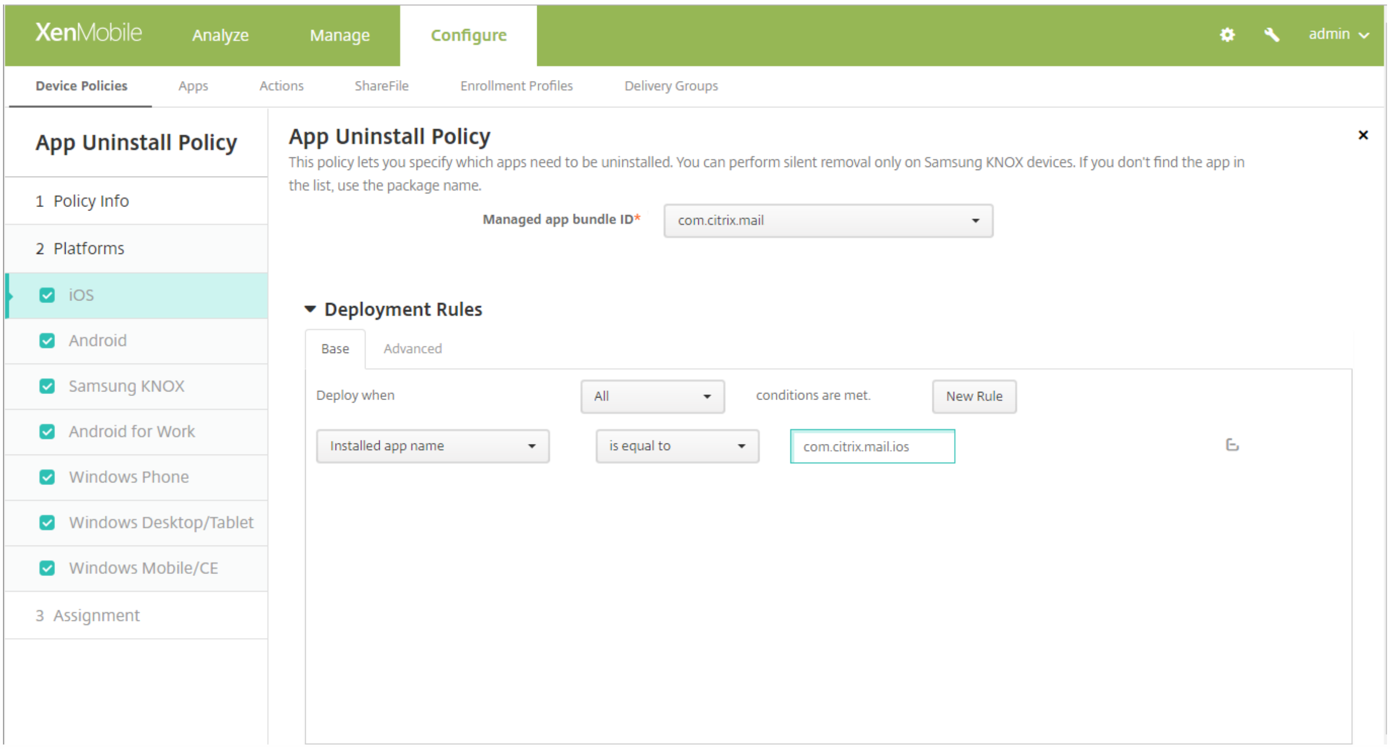
This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.

Managed app bundle ID* com.citrix.mail

Deployment Rules

Deploy when All conditions are met.

4. 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.



App Uninstall Policy

This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.

Managed app bundle ID* com.citrix.mail

Deployment Rules

Deploy when All conditions are met.

Installed app name is equal to com.citrix.mail.ios

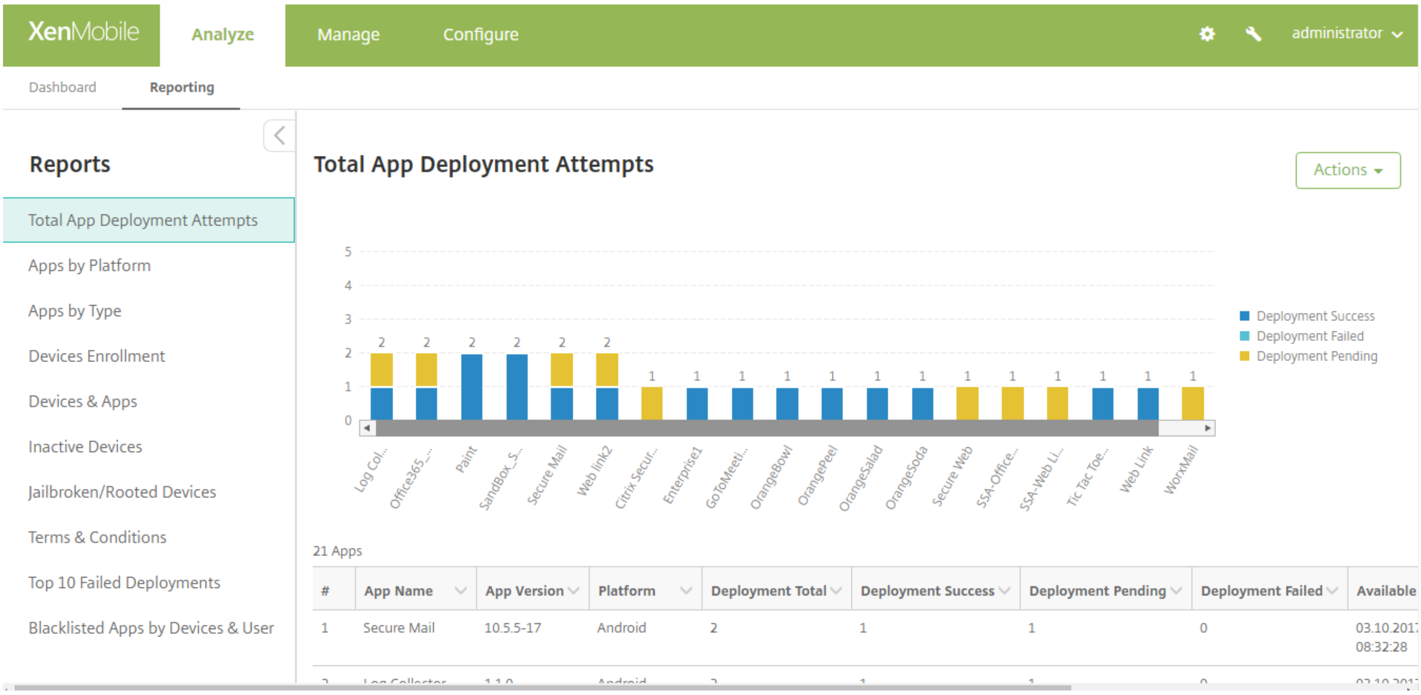
5. Compete the **Assignment** page and then click **Save**.

In the example, after the public app store app (com.citrix.mail.ios) installs on a device in the delivery groups specified, XenMobile removes the Enterprise version (com.citrix.mail).

Reporting improvements

The XenMobile **Analyze > Reporting** page has an improved design and more features for all pre-defined reports:

- Sorting and searching using device-based filters.
- Filtering reports by date
- Exporting reports in PDF format.
- Interactive charts that represent report data visually.
- The Top 25 Apps report is now called Total Apps Deployment Attempts. This report now lists all deployed apps and the percentage of users that have attempted to install them on their devices.



Total App Deployment Attempts

21 Apps

#	App Name	App Version	Platform	Deployment Total	Deployment Success	Deployment Pending	Deployment Failed	Available
1	Secure Mail	10.5.5-17	Android	2	1	1	0	03.10.201 08:32:28
2	Log Collector	1.1.0	Android	2	1	1	0	03.10.201

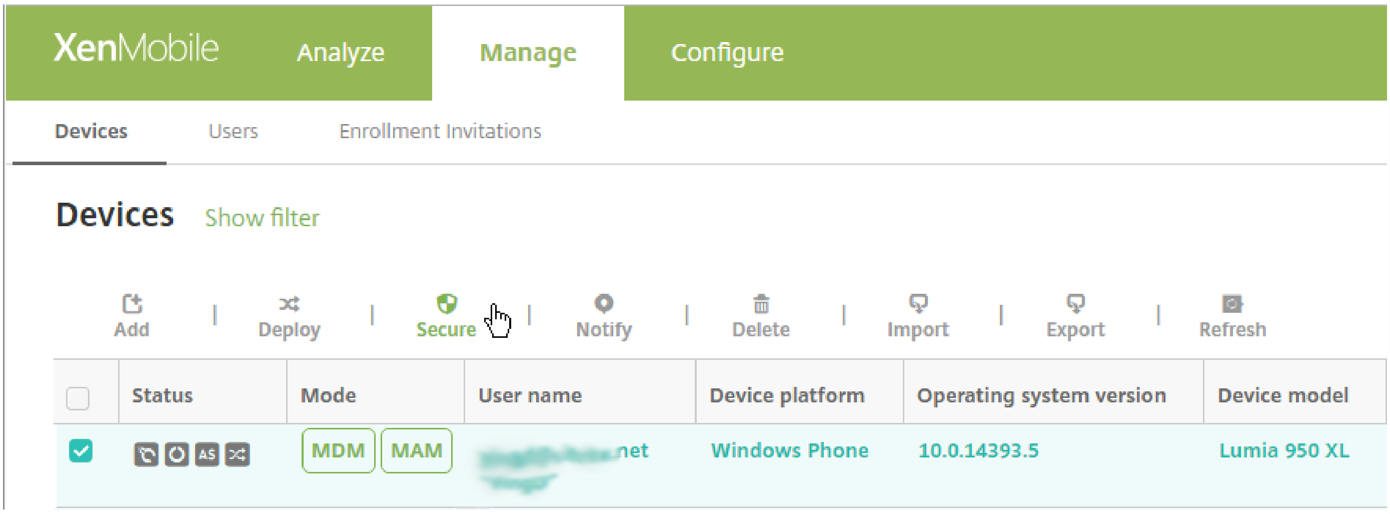
For more information, see Reports.

Locate Windows 10 devices

XenMobile console administrators and Self Help Portal users can now locate Windows 10 phones, desktops, and tablets. The locate feature is already available for iOS and Android devices. When you issue a locate command, the XenMobile Server communicates directly with the device.

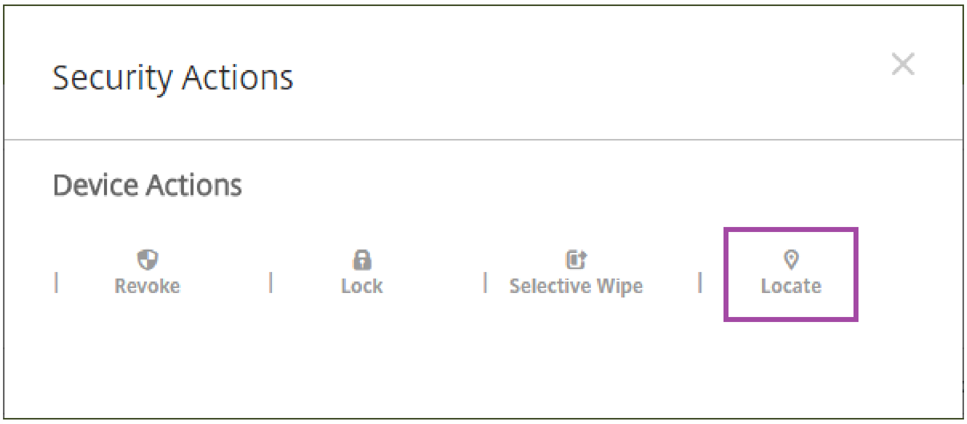
From the XenMobile console, send the Locate action to a device as follows.

1. On **Manage > Devices**, select the device, and then click **Secure**.

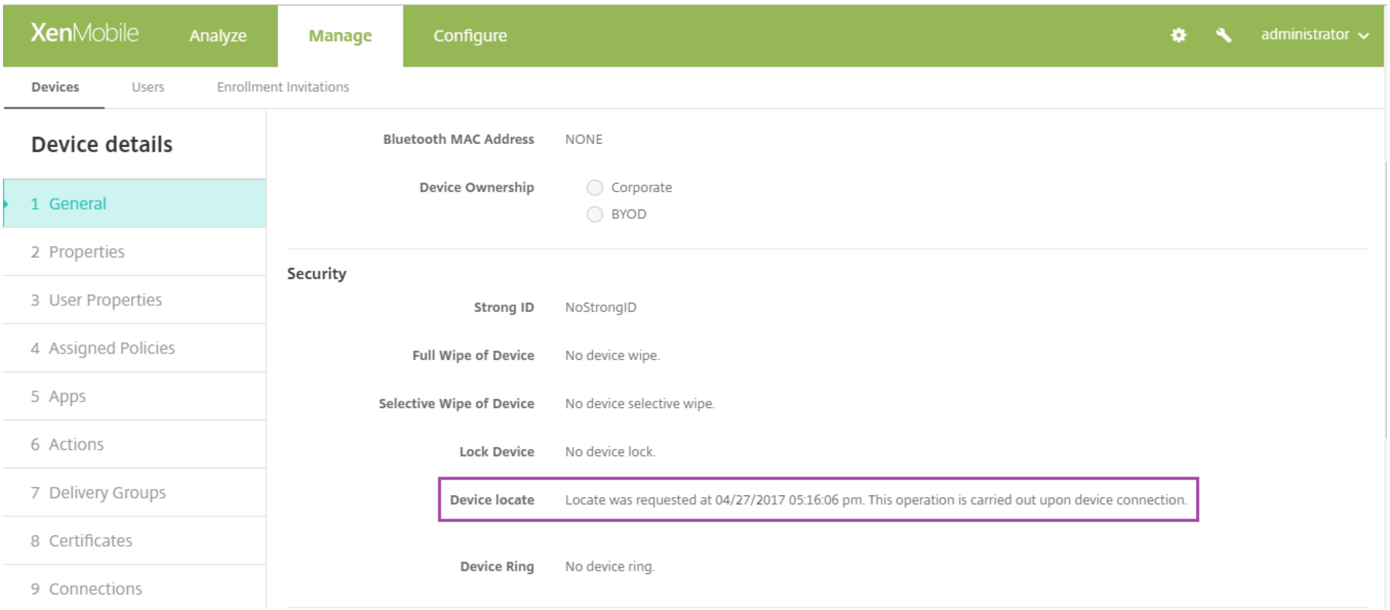


□	Status	Mode	User name	Device platform	Operating system version	Device model
☑		MDM MAM	[redacted]	Windows Phone	10.0.14393.5	Lumia 950 XL

2. In **Security Actions**, click **Locate**.



The **Device details** page provides a status of the location request and shows a map if the device is located.



Bluetooth MAC Address NONE

Device Ownership ○ Corporate ○ BYOD

Security

Strong ID NoStrongID

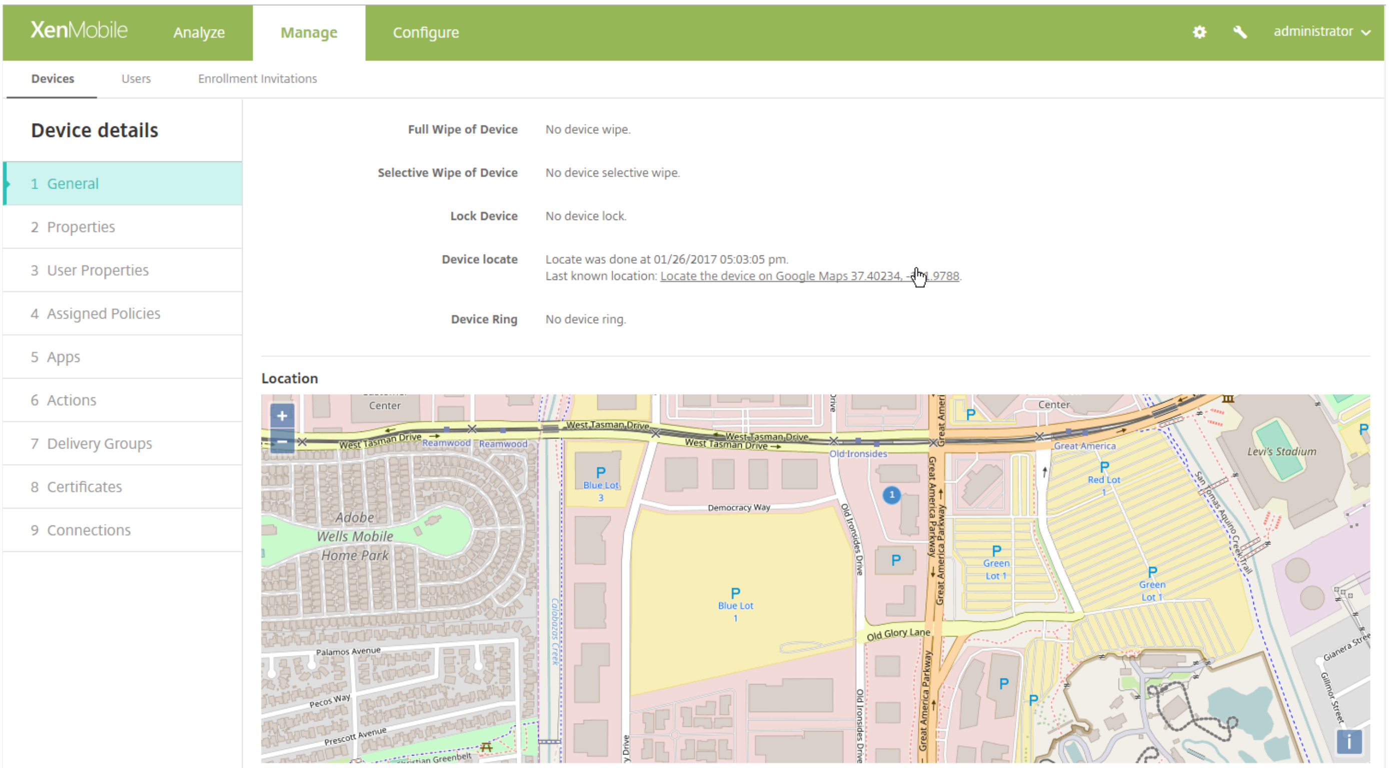
Full Wipe of Device No device wipe.

Selective Wipe of Device No device selective wipe.

Lock Device No device lock.

Device locate Locate was requested at 04/27/2017 05:16:06 pm. This operation is carried out upon device connection.

Device Ring No device ring.



Full Wipe of Device: No device wipe.

Selective Wipe of Device: No device selective wipe.

Lock Device: No device lock.

Device locate: Locate was done at 01/26/2017 05:03:05 pm.
Last known location: Locate the device on Google Maps 37.40234, -[illegible]1.9788.

Device Ring: No device ring.

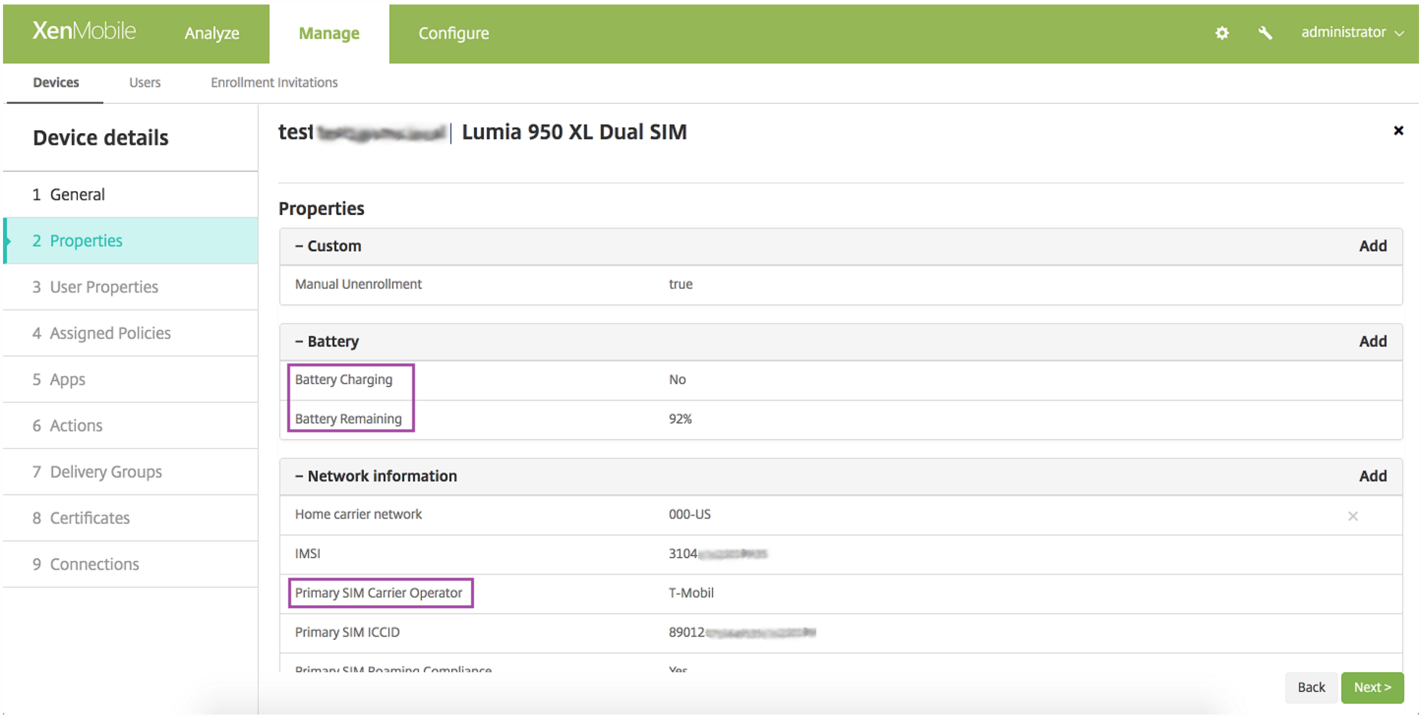
More device status properties for Windows 10 Phone and Tablet

The **Manage > Devices** page includes more device properties for Windows. The following properties, provided by the Windows 10 DeviceStatus configuration service provider (CSP), are available.

Antispyware Signature Status
Antispyware Status
Antivirus Signature Status
Antivirus Status
Battery Charging
Battery Remaining
Encryption Compliance
Firewall Status
IPV4 Address
IPV6 Address
MAC Address Network Connection
MAC Address Type
Operating System Edition
Primary SIM Carrier Operator
Primary SIM ICCID
Primary SIM Roaming compliance
Secure Boot status

TPM Version
User Account Control Status

For information about those properties, see the Microsoft article DeviceStatus CSP. The following sample shows a few of the added properties.



test[redacted] | Lumia 950 XL Dual SIM

Properties

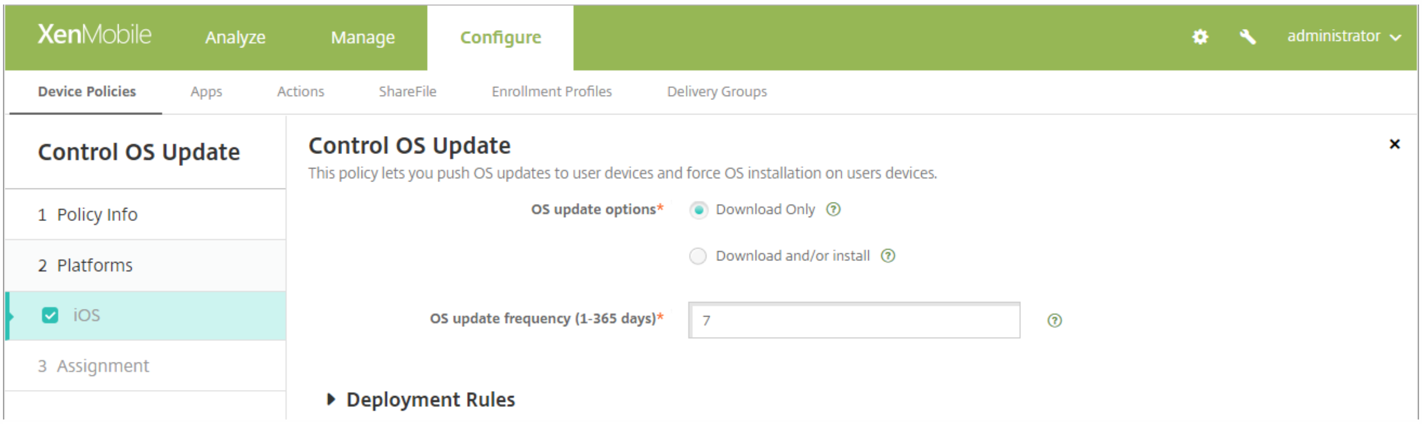
– Custom	Add
Manual Unenrollment	true

– Battery	Add
Battery Charging	No
Battery Remaining	92%

– Network information	Add
Home carrier network	000-US
IMSI	3104[redacted]
Primary SIM Carrier Operator	T-Mobil
Primary SIM ICCID	89012[redacted]
Primary SIM Roaming Compliance	Yes

Device policy to control OS updates on iOS devices

You can now configure XenMobile to send the latest OS updates to supervised iOS devices. You choose whether to deploy OS updates to devices so that users can install the updates manually, or to force installation on devices. To configure the new device policy, go to **Configure > Device Policies** and add **Control OS Update**.



Control OS Update

This policy lets you push OS updates to user devices and force OS installation on users devices.

OS update options* ● Download Only ○ Download and/or install

OS update frequency (1-365 days)* 7

Configure the options:

- **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 (1–365 days)**: Determines how frequently XenMobile checks and updates the device OS. The default is **7** days.

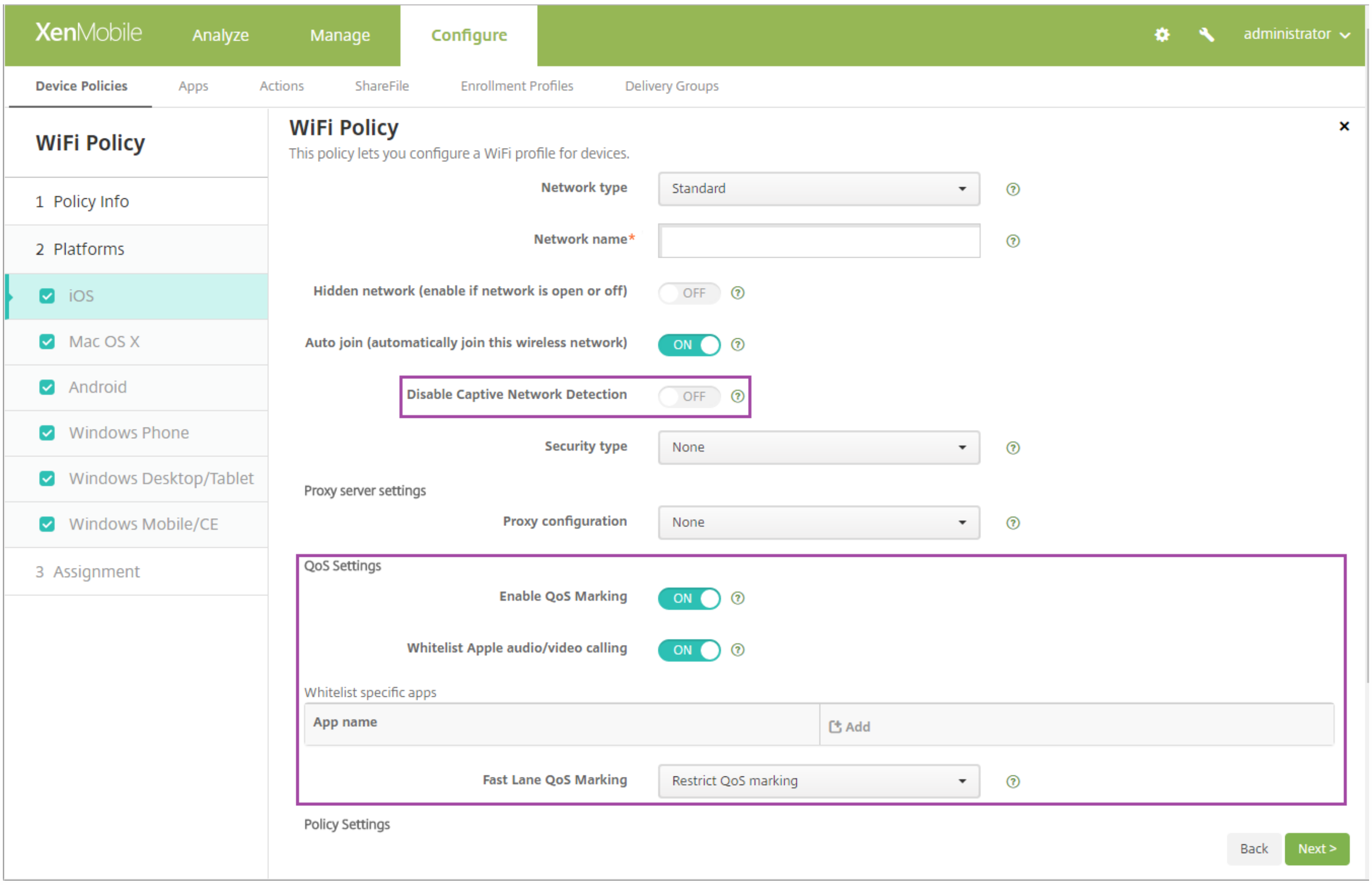
More WiFi policy options for iOS 10+

- **Disable Captive Network Detection**: If **ON**, users can't join networks that require agreements or other information before network access. Default is **OFF**.
- **Fast Lane QoS Marking**: Quality of Service (QoS) marking enables you to prioritize network bandwidth for specific business apps. Choose to restrict or not restrict Cisco Fast Lane QoS marking. If you don't restrict QoS marking for a WiFi network that supports Cisco Fast Lane QoS, all apps are whitelisted to use L2 and L3 marking. If you restrict QoS marking, specify the apps that can use L2 and L3 marking. Default is **Do not restrict QoS marking**.

If **Fast Lane QoS Marking** is **Restrict QoS marking**, the following options appear:

- **Enable QoS Marking**: Optional. If **OFF**, QoS marking is disabled. Default is **ON**.
- **Whitelist Apple audio/video calling**: Optional. If **OFF**, Apple audio and video calling aren't whitelisted, which means the traffic isn't prioritized. Default is **ON**.
- **Whitelist specific apps**: Specify the apps to use L2 and L3 marking.

For more information about WiFi policies for iOS, see Apple Configurator 2 Help.



WiFi Policy

This policy lets you configure a WiFi profile for devices.

Network type: Standard

Network name*:

Hidden network (enable if network is open or off): OFF

Auto join (automatically join this wireless network): ON

Disable Captive Network Detection: OFF

Security type: None

Proxy server settings

Proxy configuration: None

QoS Settings

Enable QoS Marking: ON

Whitelist Apple audio/video calling: ON

Whitelist specific apps

App name	Add

Fast Lane QoS Marking: Restrict QoS marking

Policy Settings

More per-app VPN policy options for iOS

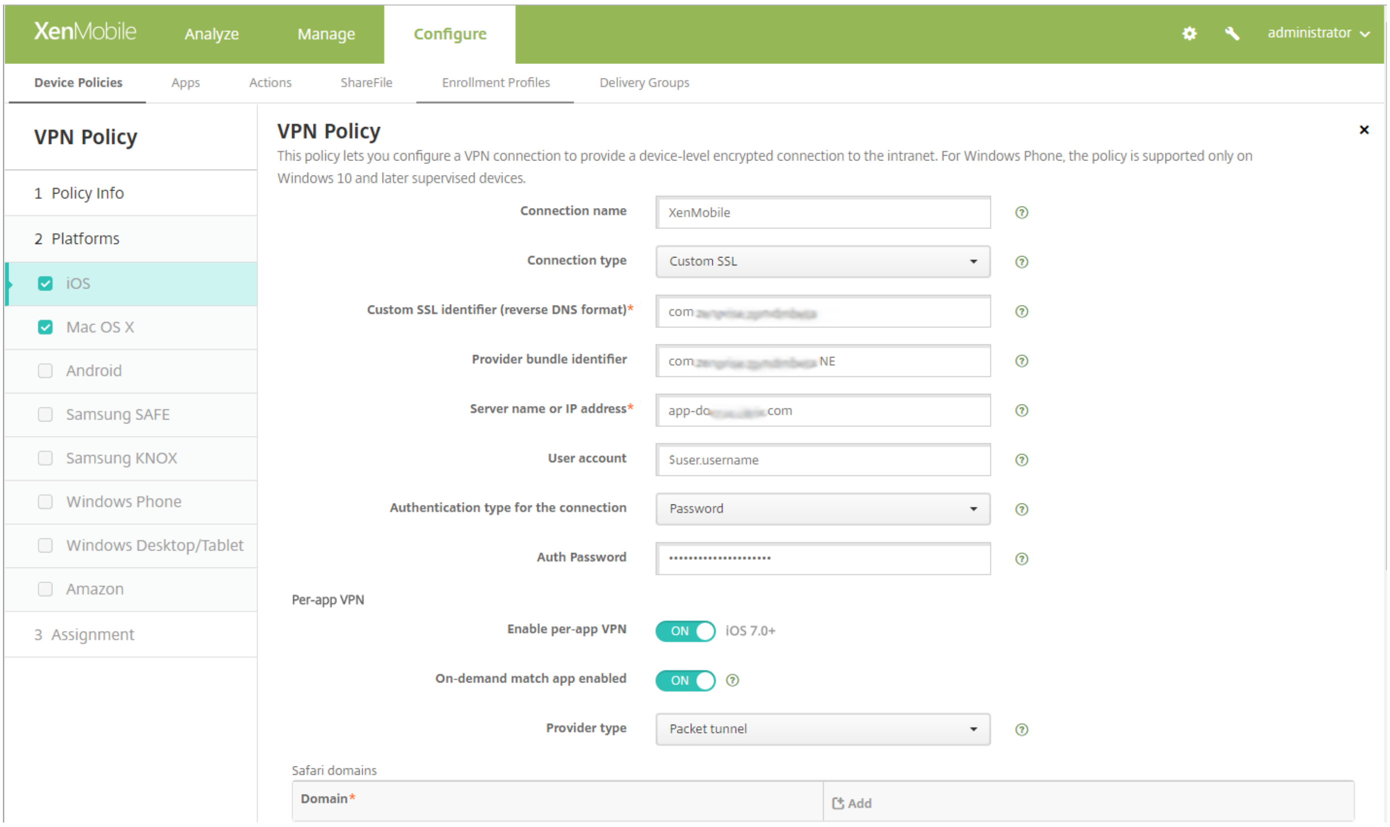
The VPN policy includes these new options, which are used when the VPN client on a device supports multiple VPN providers:

- **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.
- **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**. This option is visible when **Enable per-app VPN** is **ON**.

Per-app VPN options are available for these connection types: Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, and Custom SSL.

To configure a per-app VPN:

1. In **Configure > Device Policies**, create a VPN policy. For example:



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

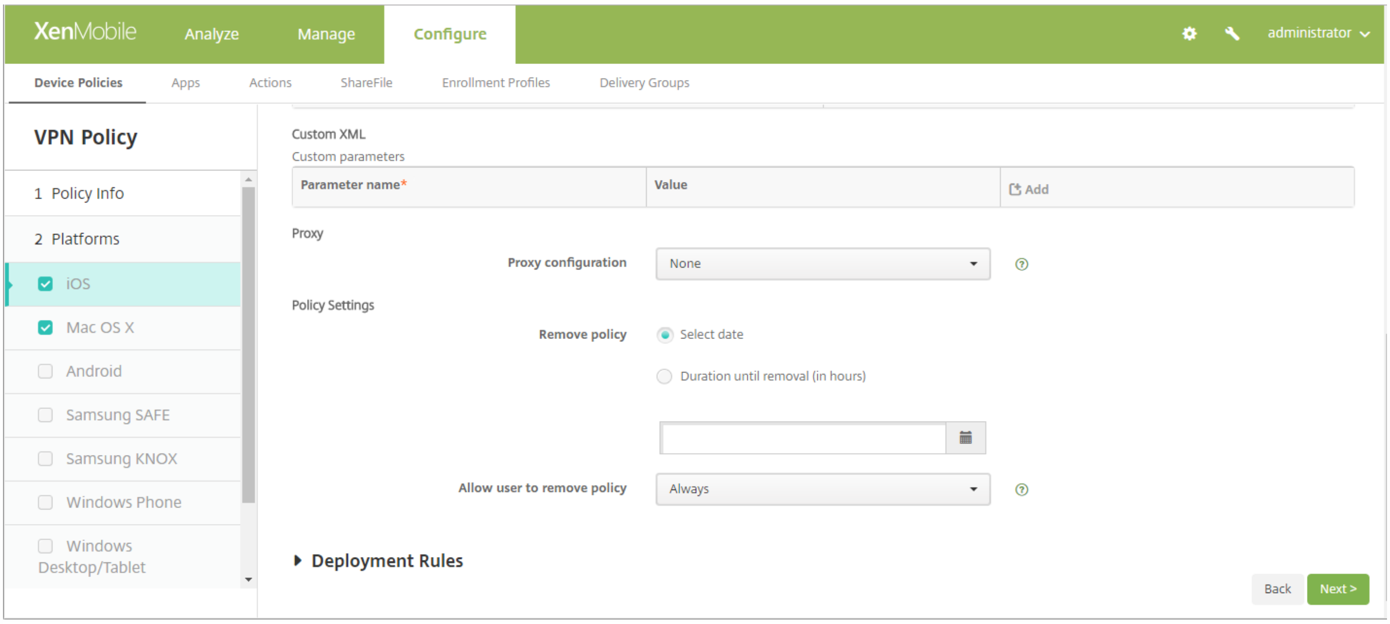
Connection name	XenMobile
Connection type	Custom SSL
Custom SSL identifier (reverse DNS format)*	com [redacted]
Provider bundle identifier	com [redacted] NE
Server name or IP address*	app-do [redacted] com
User account	$user.username
Authentication type for the connection	Password
Auth Password	••••••••••••••••••••

Per-app VPN

Enable per-app VPN	ON iOS 7.0+
On-demand match app enabled	ON
Provider type	Packet tunnel

Safari domains

Domain*	Add



Custom XML

Custom parameters

Parameter name*	Value	Add

Proxy

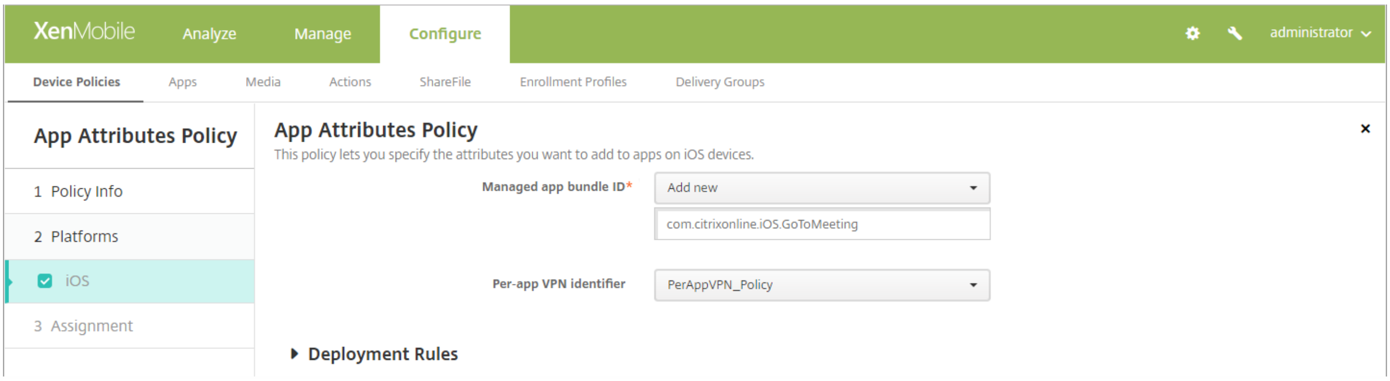
Proxy configuration	None

Policy Settings

Remove policy	● Select date ○ Duration until removal (in hours)
Allow user to remove policy	Always

Deployment Rules

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 enter the app bundle ID. (If you deploy an iOS App Inventory policy, the apps list contains apps.)



App Attributes Policy

This policy lets you specify the attributes you want to add to apps on iOS devices.

Managed app bundle ID*: Add new

com.citrixonline.iOS.GoToMeeting

Per-app VPN identifier: PerAppVPN_Policy

More feature restriction options for macOS devices

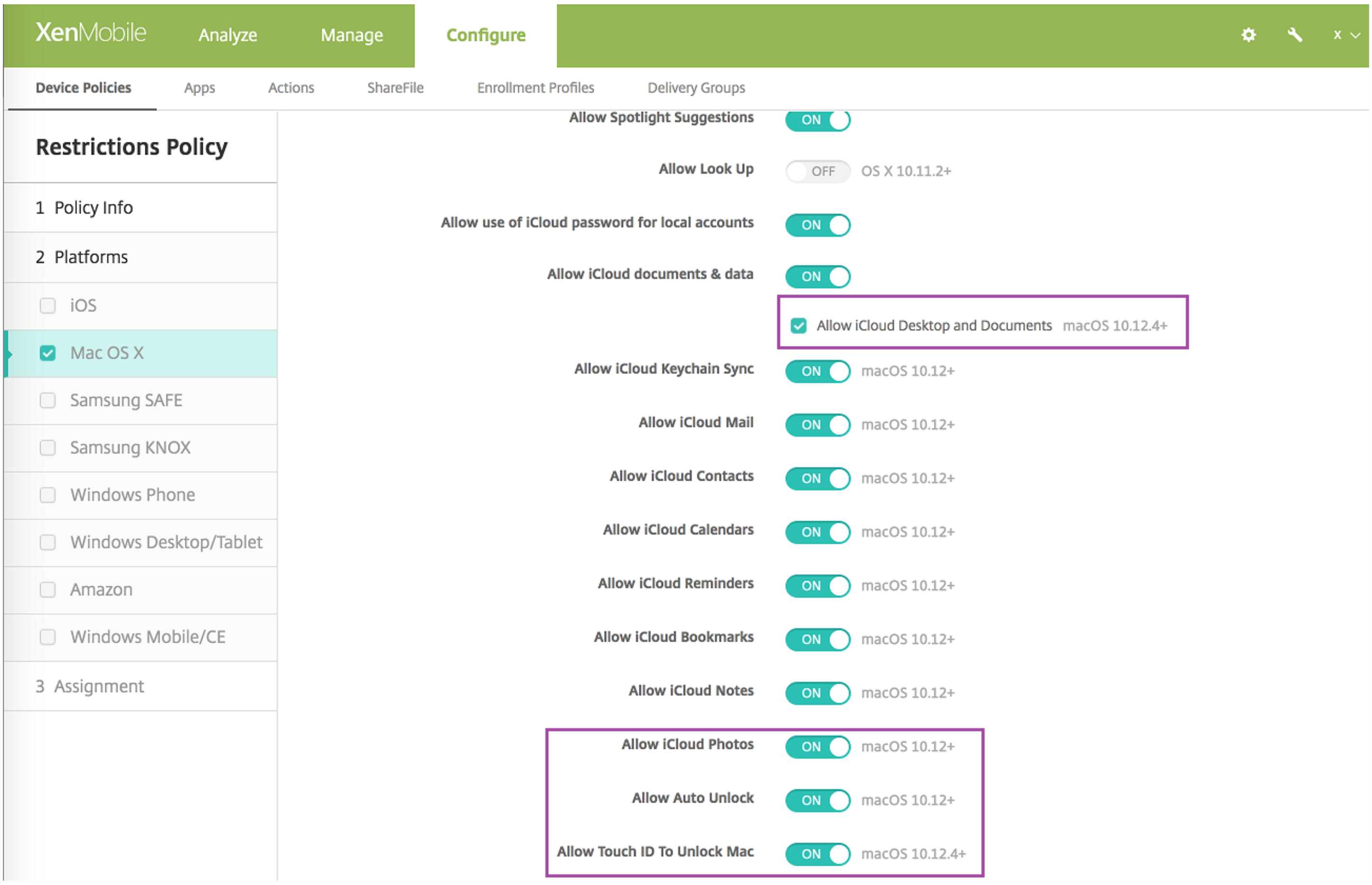
The Restrictions device policy has the following extra restriction options for macOS. By default, XenMobile allows all these features.

For macOS 10.12.4 and later:

- Allow Touch ID To Unlock Mac
- Allow iCloud Desktop and Documents

For macOS 10.12 and later:

- 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.
- Allow Auto Unlock
  For information about this option and Apple Watch, see https://support.apple.com/en-ie/HT206995.



Allow Spotlight Suggestions: ON

Allow Look Up: OFF OS X 10.11.2+

Allow use of iCloud password for local accounts: ON

Allow iCloud documents & data: ON

☑ Allow iCloud Desktop and Documents macOS 10.12.4+

Allow iCloud Keychain Sync: ON macOS 10.12+

Allow iCloud Mail: ON macOS 10.12+

Allow iCloud Contacts: ON macOS 10.12+

Allow iCloud Calendars: ON macOS 10.12+

Allow iCloud Reminders: ON macOS 10.12+

Allow iCloud Bookmarks: ON macOS 10.12+

Allow iCloud Notes: ON macOS 10.12+

Allow iCloud Photos: ON macOS 10.12+

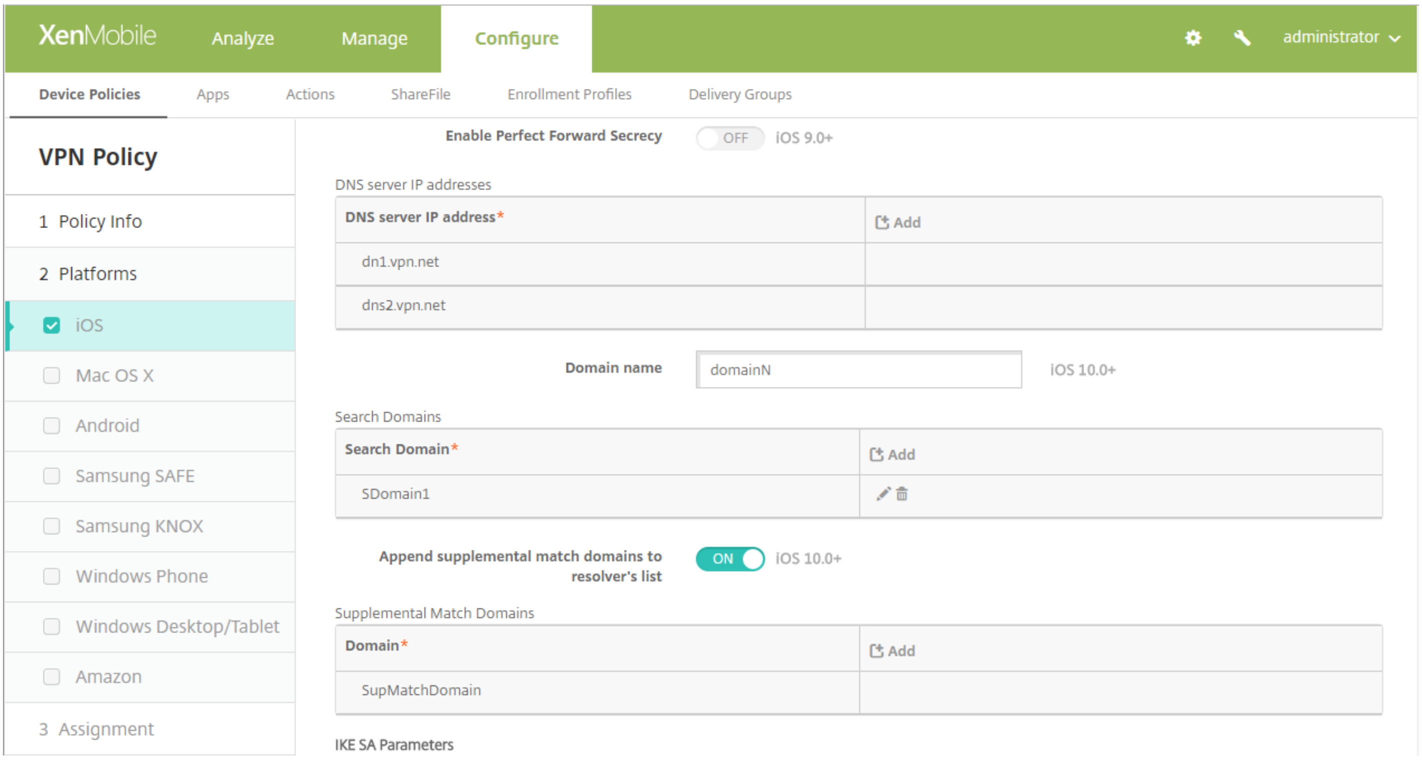
Allow Auto Unlock: ON macOS 10.12+

Allow Touch ID To Unlock Mac: ON macOS 10.12.4+

More IKEv2 parameters for the VPN device policy

iOS 10.0

The IKEv2, AlwaysOn IKEv2, and AlwaysOn IKEv2 Dual Configuration connection types have more parameters for iOS 10.0.



Enable Perfect Forward Secrecy: OFF iOS 9.0+

DNS server IP addresses

DNS server IP address*	Add
dn1.vpn.net	
dns2.vpn.net	

Domain name: domainN iOS 10.0+

Search Domains

Search Domain*	Add
SDomain1	

Append supplemental match domains to resolver's list: ON iOS 10.0+

Supplemental Match Domains

Domain*	Add
SupMatchDomain	

IKE SA Parameters

DNS server IP addresses: Optional. A list of DNS server IP addresses. These IP addresses can include a mixture of IPv4 and IPv6 addresses.

Domain name: Optional. The primary domain of the tunnel.

Search domains: Optional. A list of domains used to qualify single-label host names fully.

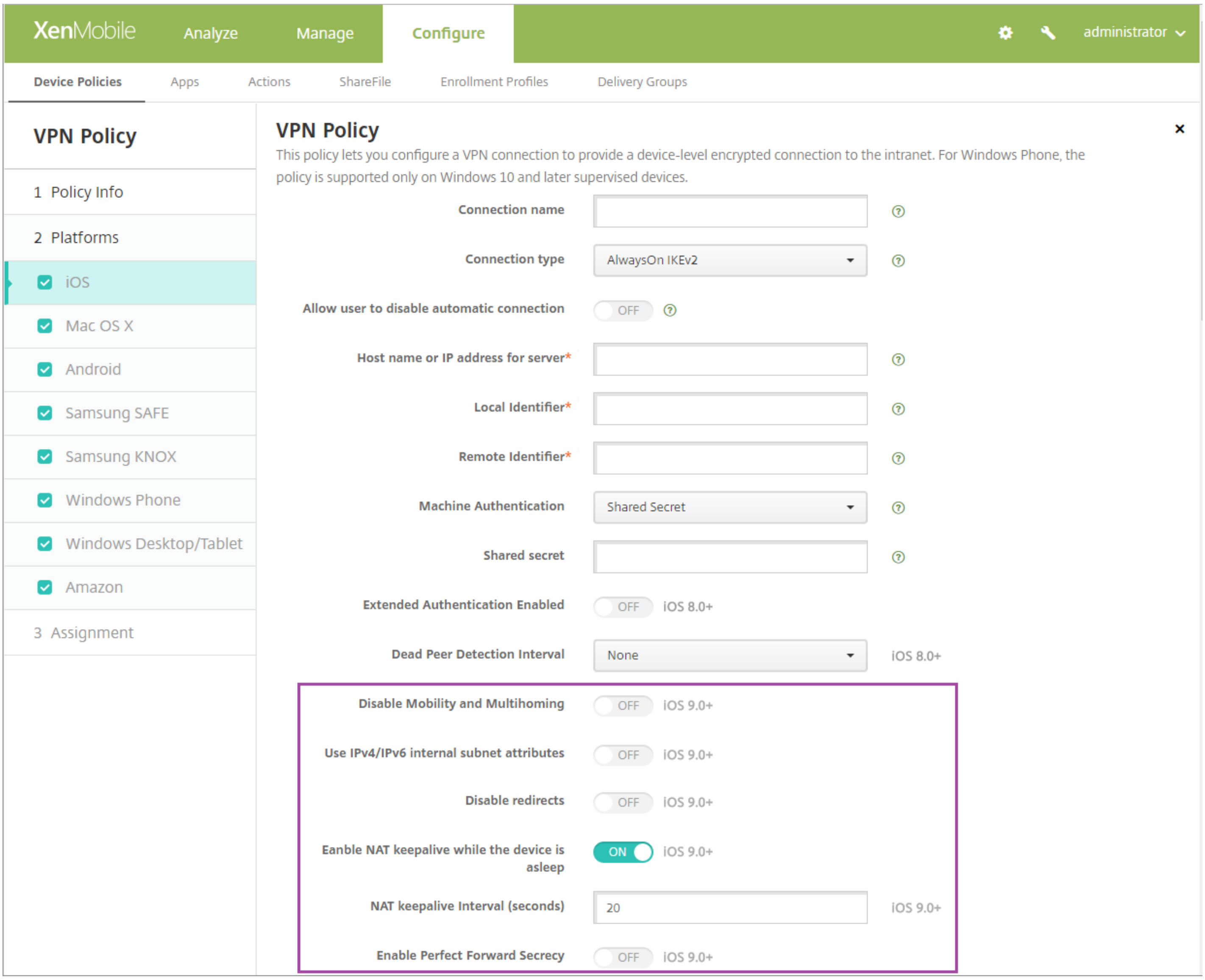
Append supplemental match domains to resolver's list: Optional. Determines whether to append the domains in Supplemental match domains to the Search domains for the resolver. **0** means append; **1** means don't append. Default is **0**.

Supplemental match domains: Optional. A list of domains 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 you save an empty string for this parameter, XenMobile uses that string as the default domain. This solution is how a split-tunnel configuration can direct all DNS queries first to the VPN DNS servers before the primary DNS servers. If the VPN tunnel becomes the default route of the network, the listed DNS servers become the default resolver. In that case, the supplemental match domains list is ignored.

iOS 9.0

The IKEv2, AlwaysOn IKEv2, and AlwaysOn IKEv2 Dual Configuration connection types have more parameters for iOS 9.0.



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name		
Connection type	AlwaysOn IKEv2	
Allow user to disable automatic connection	OFF	
Host name or IP address for server*		
Local Identifier*		
Remote Identifier*		
Machine Authentication	Shared Secret	
Shared secret		
Extended Authentication Enabled	OFF	iOS 8.0+
Dead Peer Detection Interval	None	iOS 8.0+
Disable Mobility and Multihoming	OFF	iOS 9.0+
Use IPv4/IPv6 internal subnet attributes	OFF	iOS 9.0+
Disable redirects	OFF	iOS 9.0+
Eanble NAT keepalive while the device is asleep	ON	iOS 9.0+
NAT keepalive Interval (seconds)	20	iOS 9.0+
Enable Perfect Forward Secrecy	OFF	iOS 9.0+

These parameters apply to all three IKEv2 connection types:

- **Disable Mobility and Multihoming**
- **Use IPv4/IPv6 internal subnet attributes**
- **Disable redirects**
- **Enable Perfect Forward Secrecy**

The two AlwaysOn IKEv2 connection types also include:

- **Enable NAT keepalive while the device is asleep**

  Keepalive packets maintain NAT mappings for IKEv2 connections. The chip sends these packets at regular interval 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 WiFi and 110 seconds over cellular. You can change the interval by using the **NAT keepalive interval** parameter.

- **NAT keepalive interval (seconds)**

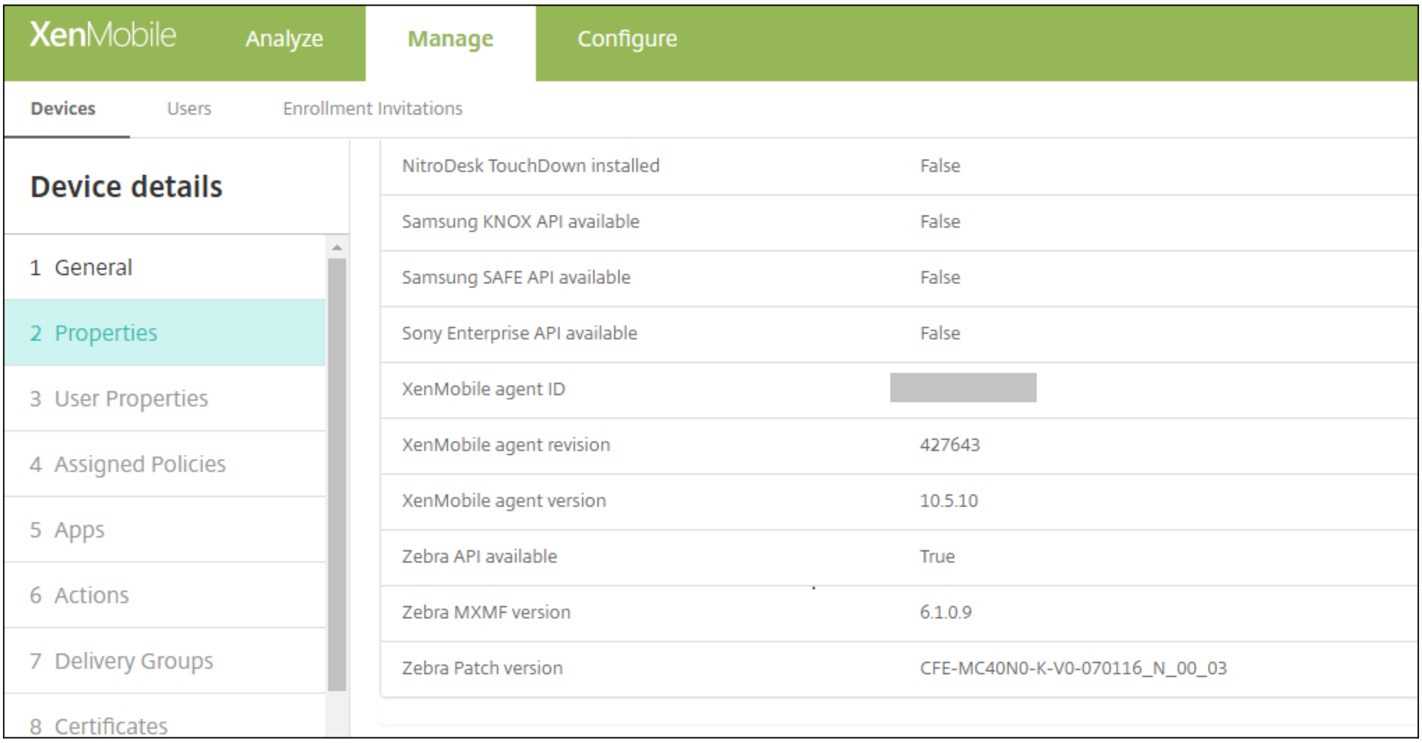
Defaults to **20** seconds.

Support for Zebra rugged Android-based mobile devices

XenMobile now supports users with Zebra Android devices.

Important: Zebra devices must install Secure Hub 10.5.10 to enroll in XenMobile.

In the XenMobile console, when you manage a Zebra device, several properties appear in **Manage > Devices**, in the **Device details**, **Properties** list.

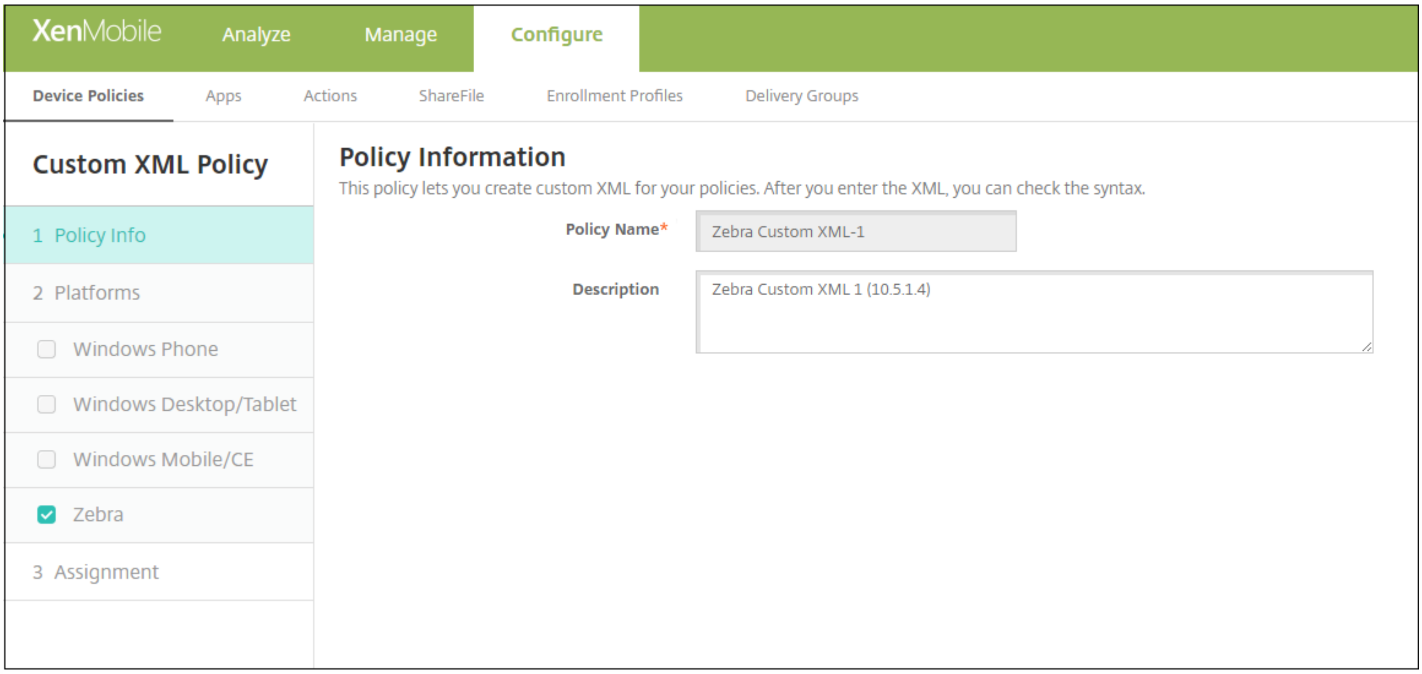


NitroDesk TouchDown installed	False
Samsung KNOX API available	False
Samsung SAFE API available	False
Sony Enterprise API available	False
XenMobile agent ID	[redacted]
XenMobile agent revision	427643
XenMobile agent version	10.5.10
Zebra API available	True
Zebra MXMF version	6.1.0.9
Zebra Patch version	CFE-MC40N0-K-V0-070116_N_00_03

- **Zebra API**: Indicates that the device contains the Zebra API.
- **Zebra MXMF version**: Indicates the MX Management Framework (MXMF) available for exposing APIs and configuring and managing Zebra Android-based devices.
- **Zebra patch version**: Indicates the patch version currently installed on the device.

For more details about Zebra devices, see the Zebra Technologies documentation.

The **Custom XML** MDM policy is also available for the Zebra platform.



Custom XML Policy

1 Policy Info

2 Platforms

- □ Windows Phone
- □ Windows Desktop/Tablet
- □ Windows Mobile/CE
- ☑ Zebra

3 Assignment

Policy Information

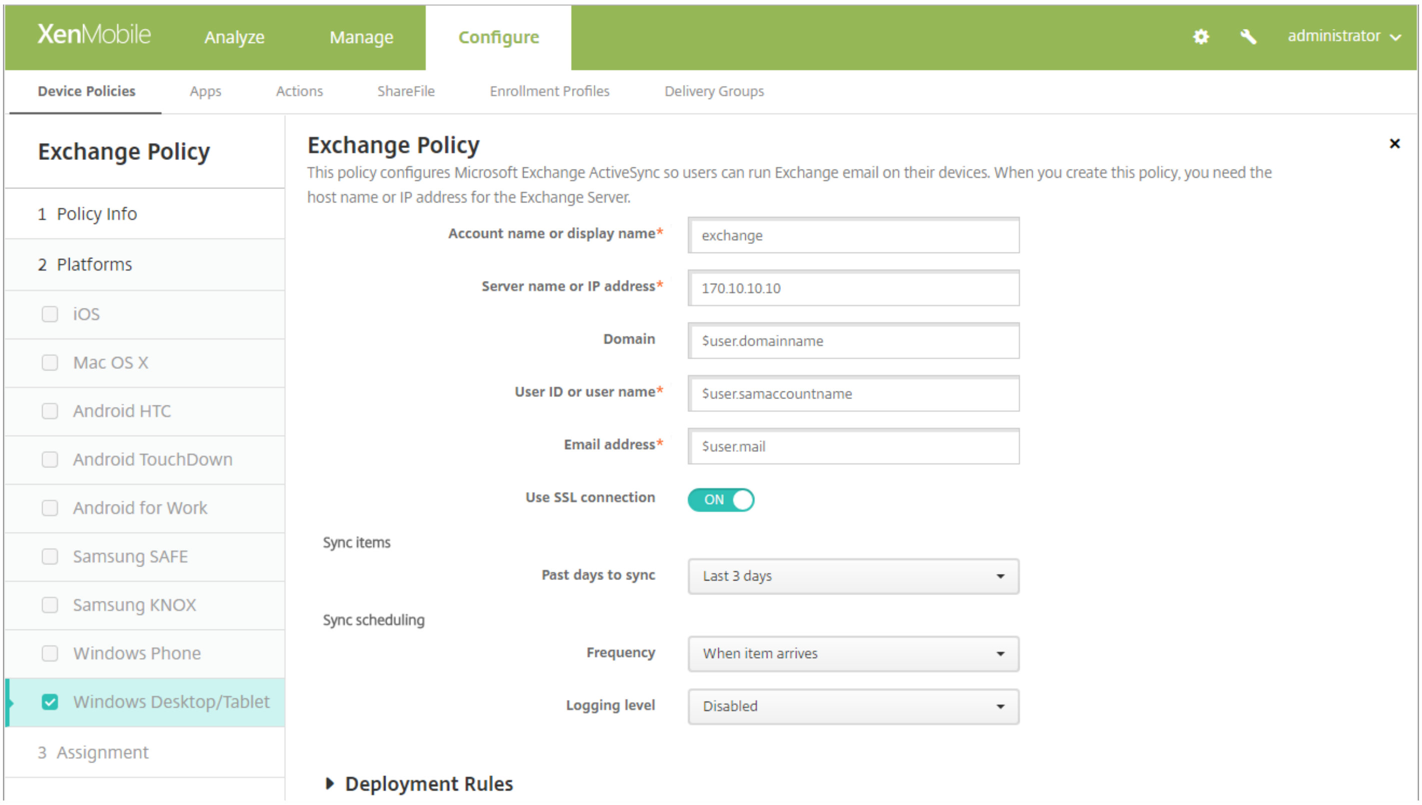
This policy lets you create custom XML for your policies. After you enter the XML, you can check the syntax.

Policy Name*: Zebra Custom XML-1

Description: Zebra Custom XML 1 (10.5.1.4)

Other improvements

- **Exchange policy now available for Windows 10 for Tablet.** To add the policy, go to **Configure > Device Policies**. The settings are the same as for Windows 10 Phone. For setting details, see Microsoft Exchange ActiveSync device policy.



Exchange Policy

1 Policy Info

2 Platforms

- □ iOS
- □ Mac OS X
- □ Android HTC
- □ Android TouchDown
- □ Android for Work
- □ Samsung SAFE
- □ Samsung KNOX
- □ Windows Phone
- ☑ Windows Desktop/Tablet

3 Assignment

Exchange Policy

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Account name or display name*: exchange

Server name or IP address*: 170.10.10.10

Domain: $user.domainname

User ID or user name*: $user.samaccountname

Email address*: $user.mail

Use SSL connection: ON

Sync items

Past days to sync: Last 3 days

Sync scheduling

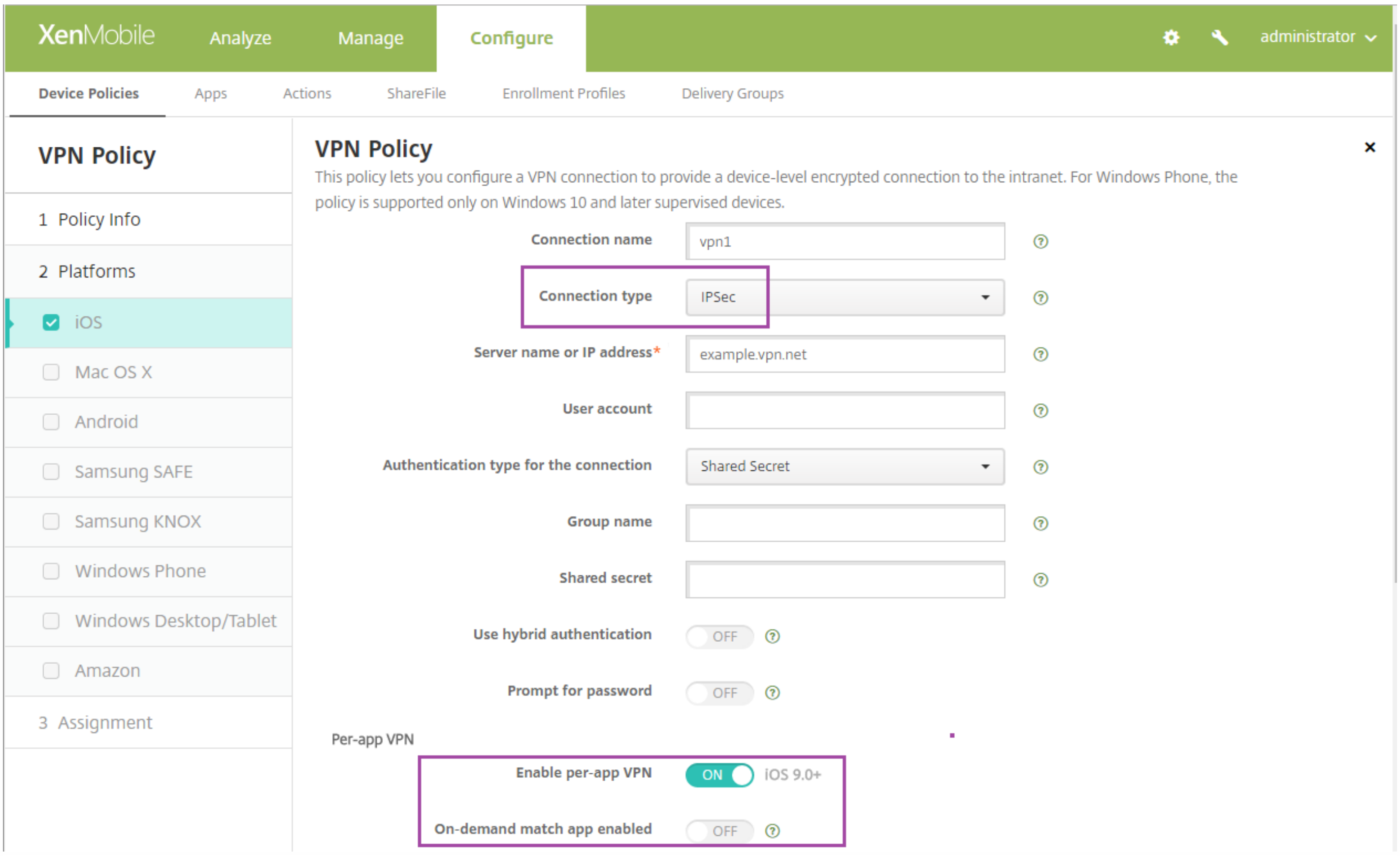
Frequency: When item arrives

Logging level: Disabled

▸ Deployment Rules

- **Active Directory user names now stored using lowercase letters.** As of this release, XenMobile stores all Active Directory user names using lowercase letters. This change applies to Active Directory users in the XenMobile database when it's upgraded and to new Active Directory users. This change doesn't apply to local user names.
- **Page loading, filtering, sorting, and searching device queries are now three times faster.** This optimization is a result of decoupling device count and query optimization while querying for a list of devices based on a given criteria. XenMobile Server can now fetch device counts dynamically.
- **The VPN policy for iOS devices now has per-app VPN options for the IPSec connection type.** iOS 9.0 and later devices support per-app VPN for IPSec connections. Netskope and other Cloud Access Security Brokers (CASBs) might recommend per-app VPN connections for IPSec.

  The per-app VPN options are **Enable per-app VPN**, **On-demand match app enabled**, and **Safari domains**.



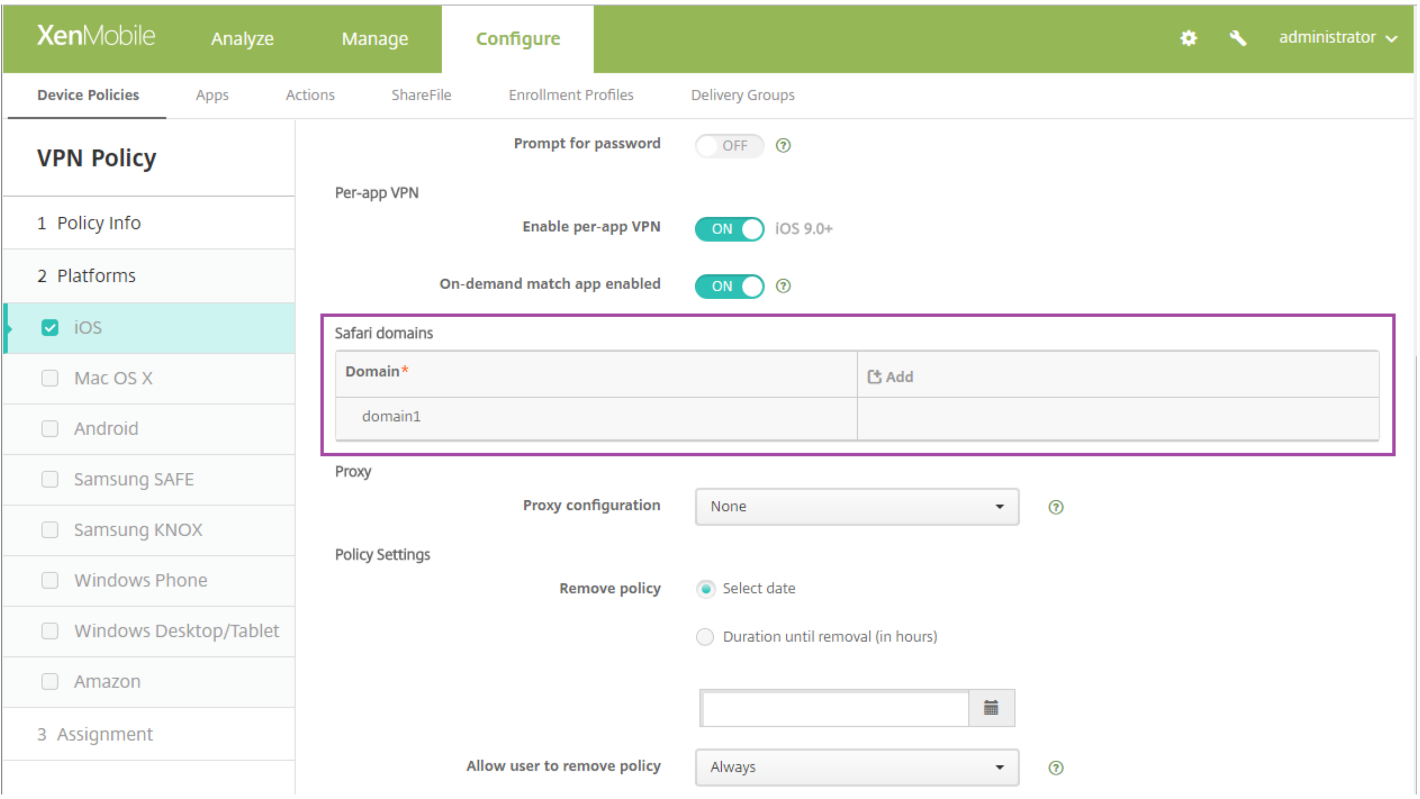
VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name	vpn1
Connection type	IPSec
Server name or IP address*	example.vpn.net
User account	
Authentication type for the connection	Shared Secret
Group name	
Shared secret	
Use hybrid authentication	OFF
Prompt for password	OFF

Per-app VPN

Enable per-app VPN	ON iOS 9.0+
On-demand match app enabled	OFF



XenMobile Analyze Manage Configure administrator

Device Policies | Apps | Actions | ShareFile | Enrollment Profiles | Delivery Groups

VPN Policy

1 Policy Info
2 Platforms
☑ iOS
□ Mac OS X
□ Android
□ Samsung SAFE
□ Samsung KNOX
□ Windows Phone
□ Windows Desktop/Tablet
□ Amazon
3 Assignment

Prompt for password: OFF

Per-app VPN

Enable per-app VPN: ON iOS 9.0+

On-demand match app enabled: ON

Safari domains

Domain*	Add
domain1	

Proxy

Proxy configuration: None

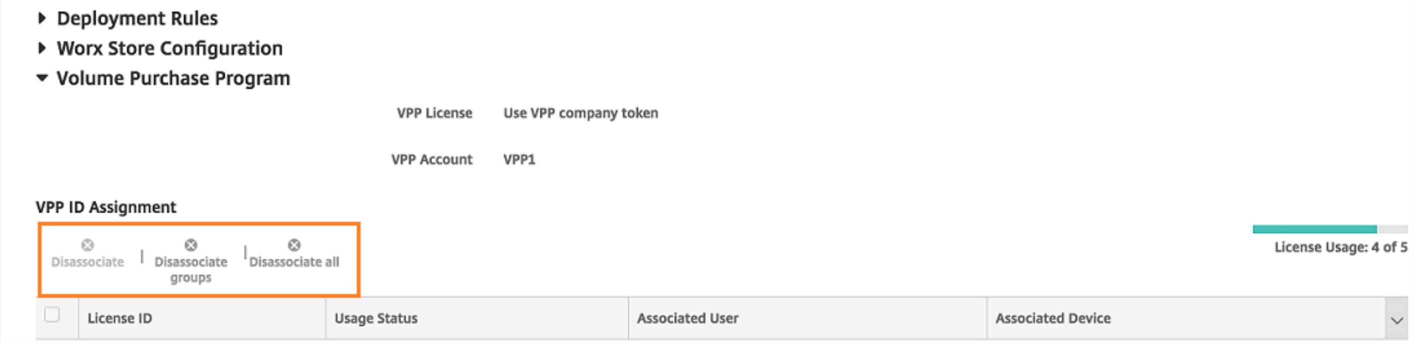
Policy Settings

Remove policy: ● Select date

○ Duration until removal (in hours)

Allow user to remove policy: Always

- **iOS Volume Purchase Program license revocation by user groups or in bulk**. You can now also disassociate Volume Purchase Program licenses for user groups or for all assignments to free licenses in bulk.



▸ Deployment Rules
▸ Worx Store Configuration
▾ Volume Purchase Program

VPP License: Use VPP company token

VPP Account: VPP1

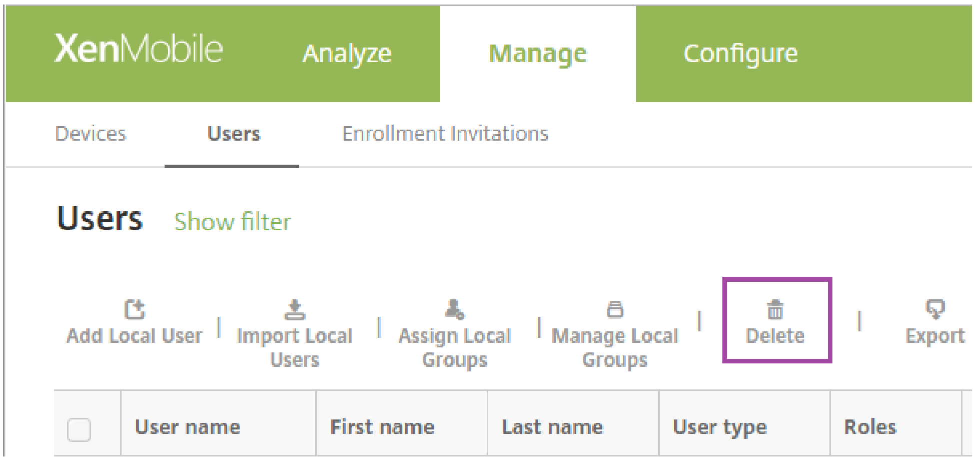
VPP ID Assignment

Disassociate | Disassociate groups | Disassociate all

License Usage: 4 of 5

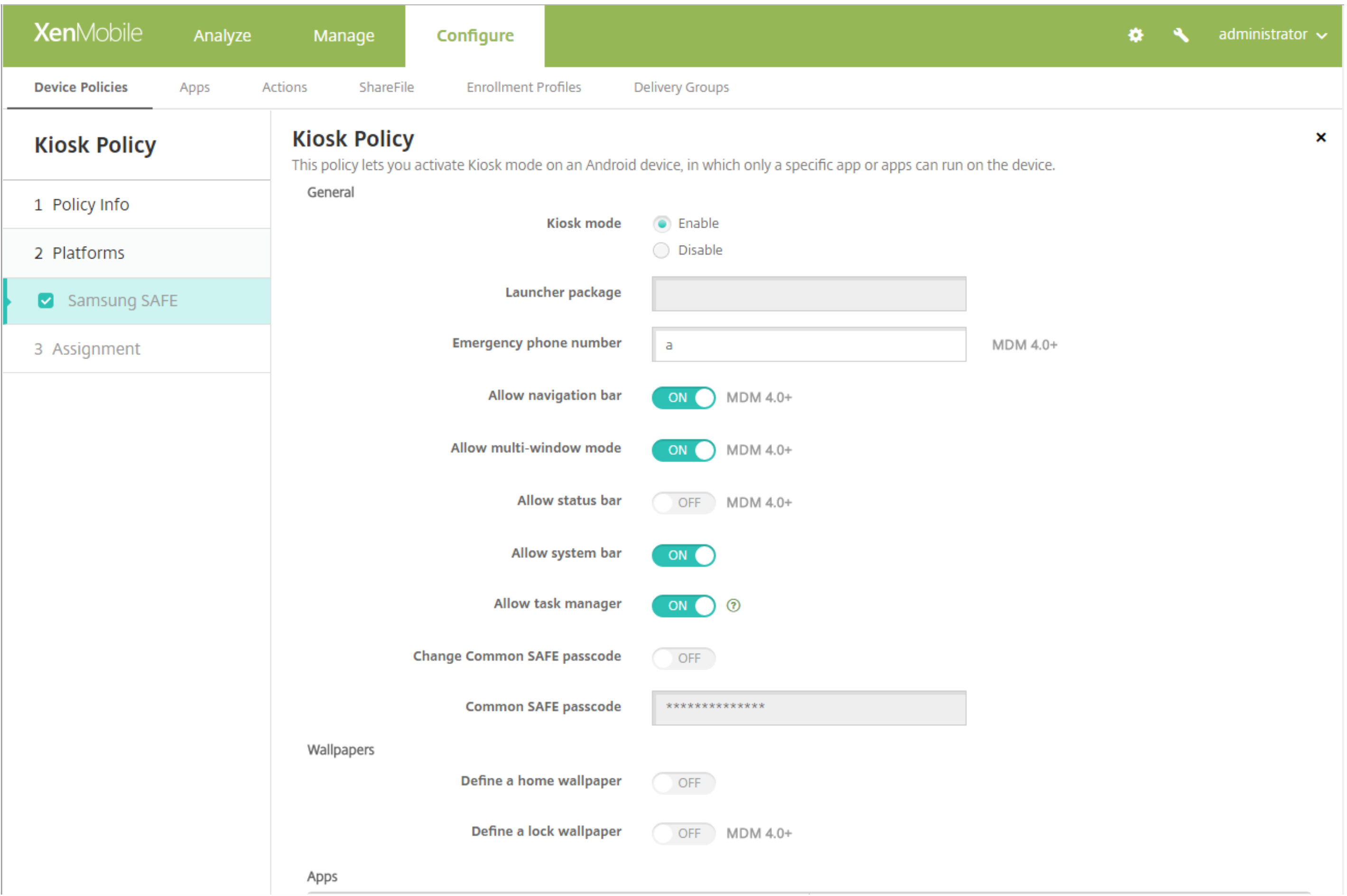
□	License ID	Usage Status	Associated User	Associated Device

- **Delete multiple Active Directory users at a time**. The menu bar that appears when you select one or more Active Directory users now includes the **Delete** command. Previously, the **Delete** command appeared only in the right-click menu for a single user.



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**.

- **Control whether the Common SAFE passcode field is editable**. To prevent inadvertent changes to the **Common SAFE passcode**, the Kiosk policy has a new setting, **Change Common SAFE passcode**. By default, the new setting is **OFF**. To change the passcode, set **Change Common SAFE passcode** to **ON** and then type a value for the passcode.



Kiosk Policy

This policy lets you activate Kiosk mode on an Android device, in which only a specific app or apps can run on the device.

General

Kiosk mode: ● Enable ○ Disable

Launcher package:

Emergency phone number: a — MDM 4.0+

Allow navigation bar: ON — MDM 4.0+

Allow multi-window mode: ON — MDM 4.0+

Allow status bar: OFF — MDM 4.0+

Allow system bar: ON

Allow task manager: ON

Change Common SAFE passcode: OFF

Common SAFE passcode: **************

Wallpapers

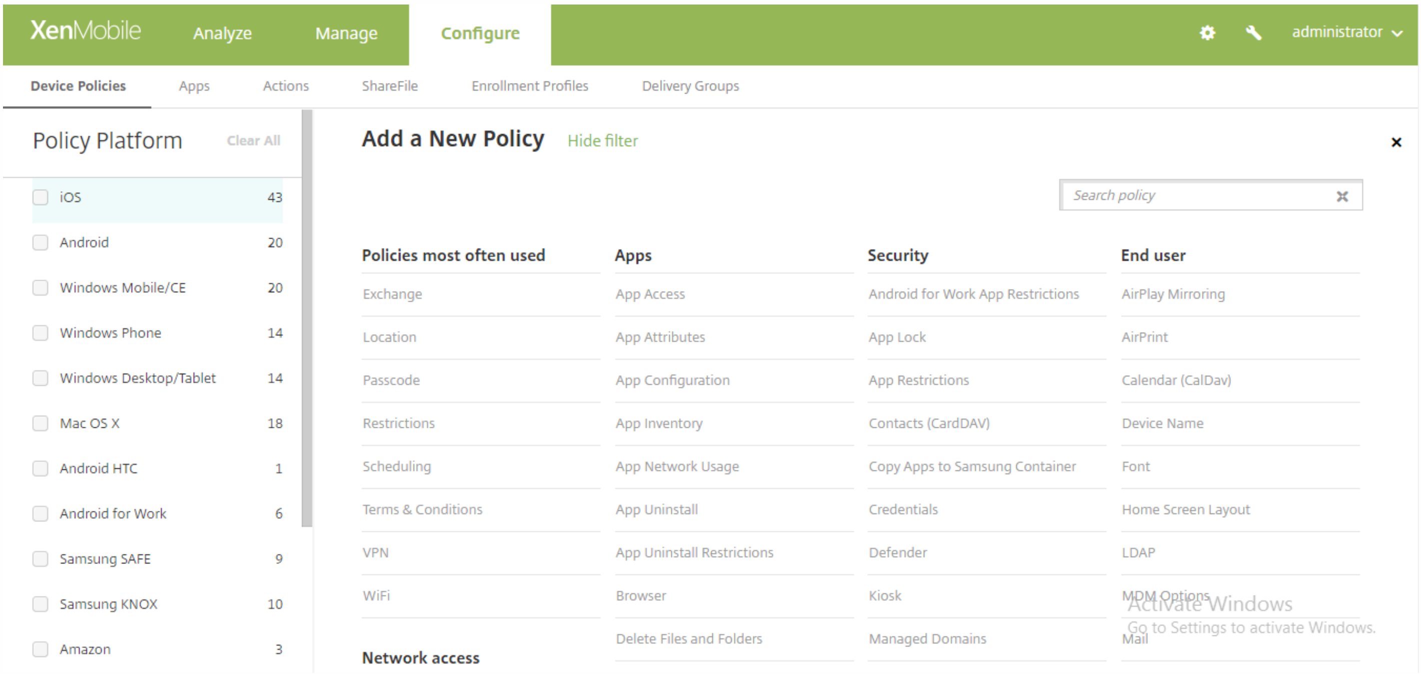
Define a home wallpaper: OFF

Define a lock wallpaper: OFF — MDM 4.0+

Apps

- **Filter the device policy list when adding a policy**. On the **Configure > Device Policies** page, when you click **Add**, the following page now appears. You can search for a policy by name, as before. You can also filter the list, to view the device policies for selected platforms.

The **Add a New Policy** page initially shows a list of device policies and platform filters.



Policy Platform

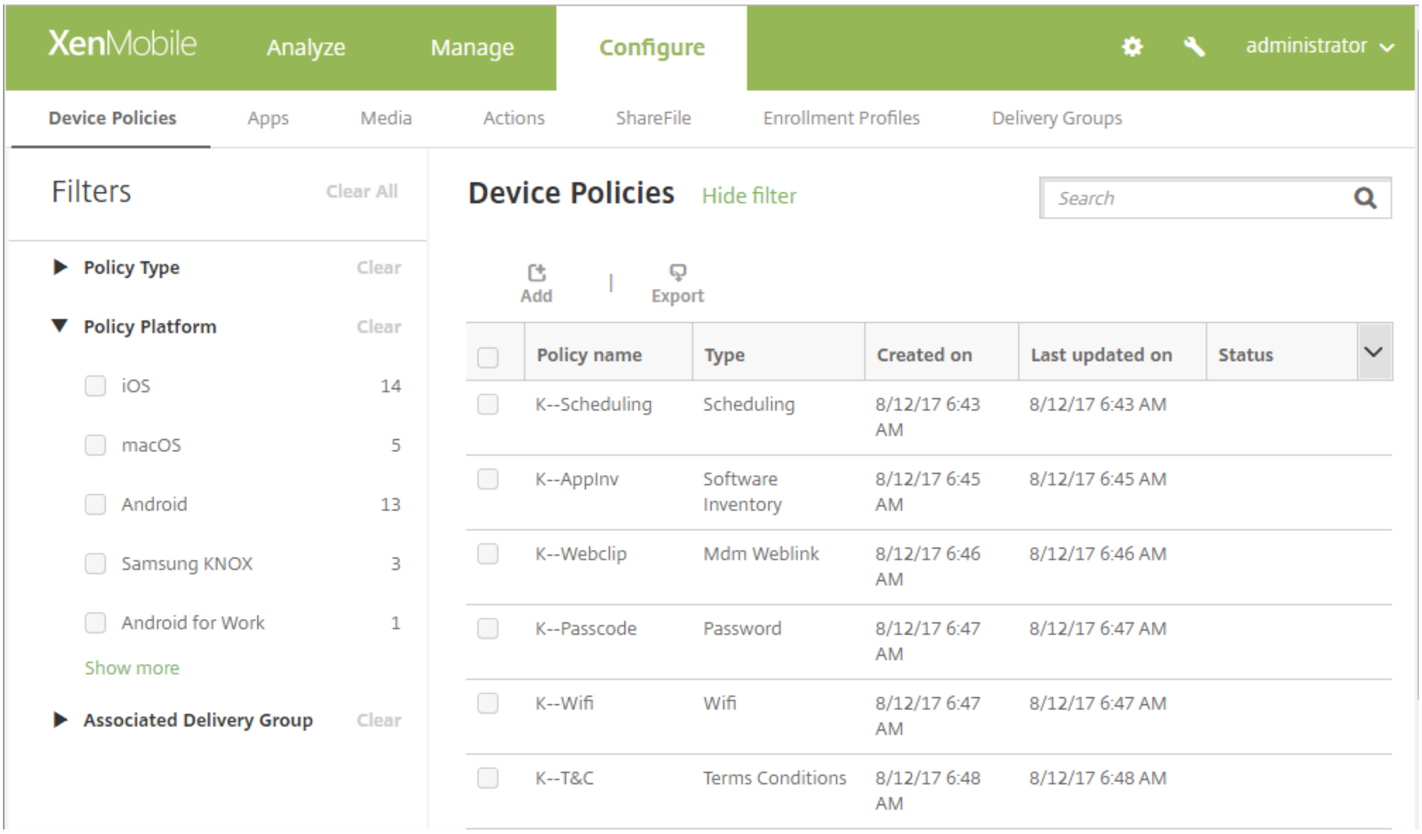
iOS	43
Android	20
Windows Mobile/CE	20
Windows Phone	14
Windows Desktop/Tablet	14
Mac OS X	18
Android HTC	1
Android for Work	6
Samsung SAFE	9
Samsung KNOX	10
Amazon	3

Add a New Policy

Policies most often used	Apps	Security	End user
Exchange	App Access	Android for Work App Restrictions	AirPlay Mirroring
Location	App Attributes	App Lock	AirPrint
Passcode	App Configuration	App Restrictions	Calendar (CalDav)
Restrictions	App Inventory	Contacts (CardDAV)	Device Name
Scheduling	App Network Usage	Copy Apps to Samsung Container	Font
Terms & Conditions	App Uninstall	Credentials	Home Screen Layout
VPN	App Uninstall Restrictions	Defender	LDAP
WiFi	Browser	Kiosk	MDM Options
	Delete Files and Folders	Managed Domains	Mail

Network access

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.



Filters

▶ Policy Type

▼ Policy Platform

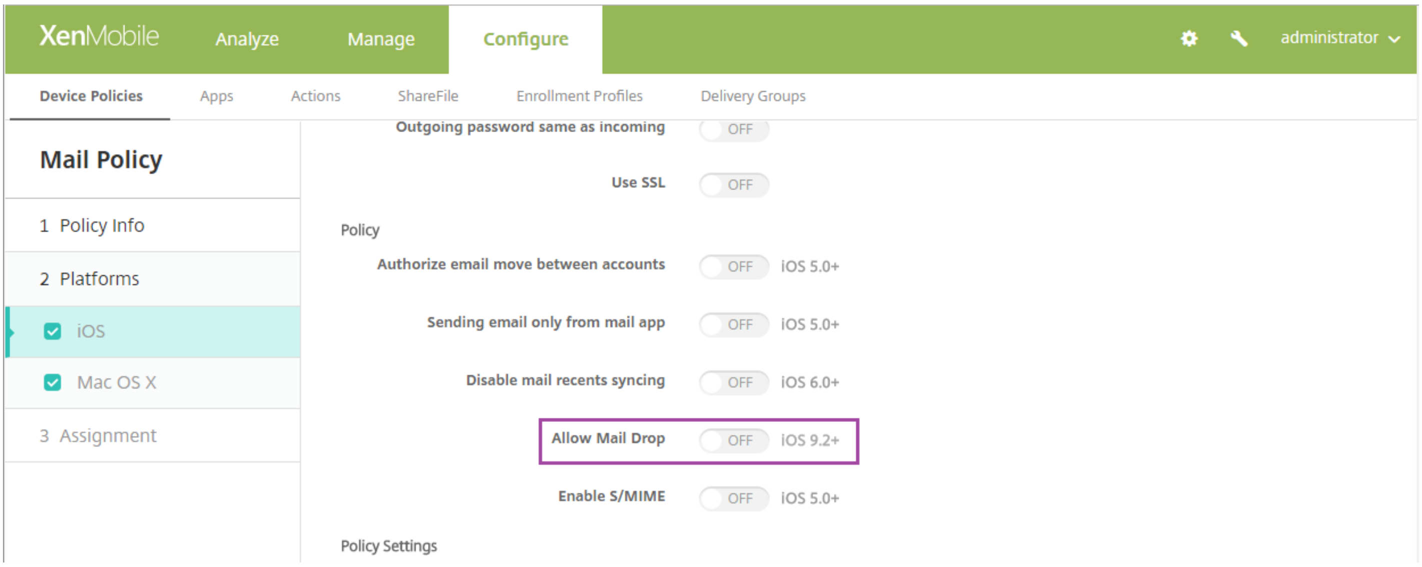
□ iOS	14
□ macOS	5
□ Android	13
□ Samsung KNOX	3
□ Android for Work	1

▶ Associated Delivery Group

Device Policies

□	Policy name	Type	Created on	Last updated on	Status
□	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM	
□	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM	
□	K--Webclip	Mdm Weblink	8/12/17 6:46 AM	8/12/17 6:46 AM	
□	K--Passcode	Password	8/12/17 6:47 AM	8/12/17 6:47 AM	
□	K--Wifi	Wifi	8/12/17 6:47 AM	8/12/17 6:47 AM	
□	K--T&C	Terms Conditions	8/12/17 6:48 AM	8/12/17 6:48 AM	

- **Apple Mail Drop support added to the Mail device policy**. You can now allow use of Apple Mail Drop for devices running iOS 9.2 and later. Mail Drop lets users upload files that are too large to send as an email attachment. Users can upload files up to 5 GB and then use the Mail app on their iOS device to send a link or preview to recipients.



Outgoing password same as incoming OFF

Use SSL OFF

Policy

Authorize email move between accounts OFF iOS 5.0+

Sending email only from mail app OFF iOS 5.0+

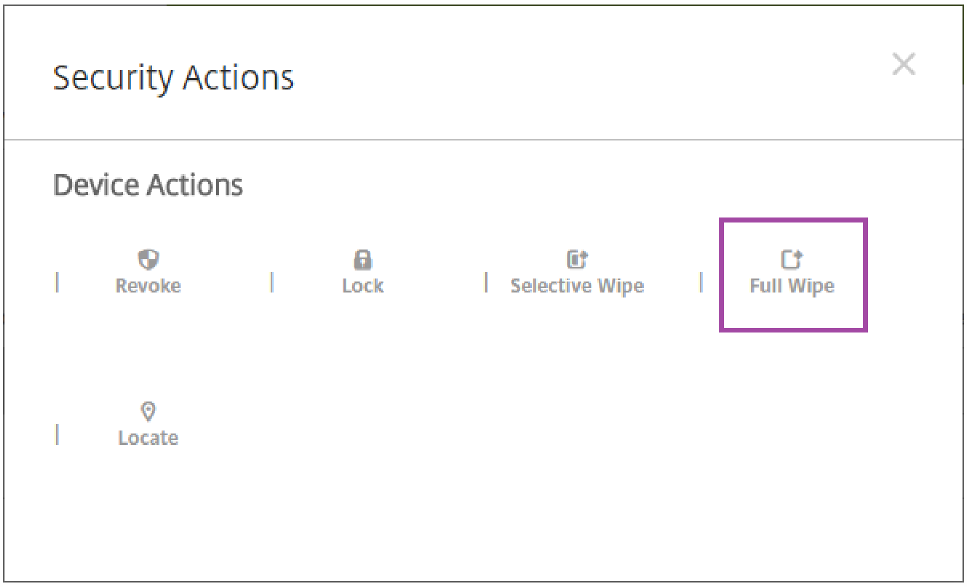
Disable mail recents syncing OFF iOS 6.0+

Allow Mail Drop OFF iOS 9.2+

Enable S/MIME OFF iOS 5.0+

Policy Settings

- **Device details logged for a wipe or lock of MAM-only devices**. When a MAM-only device gets wiped or locked, XenMobile logs now include the device ID and user name.
- **Support for Windows 10 RS2**. We certified XenMobile 10.5.3 and 10.5.2 with Windows 10 RS2 Phone and Tablet. XenMobile 10.5.1, 10.5.0, 10.4, and 10.3.x are compatible with Windows 10 RS2 Phone and Tablet.
- **Full wipe of Windows Desktop and Tablet devices**. You can now perform a full wipe to erase all personal and corporate data and apps from a Windows Desktop or Tablet device. From **Manage > Devices**, select a Windows Desktop/Tablet device, click **Secure**, and then click **Full Wipe**. On a desktop device, the remote wipe triggers the Windows **Reset this PC** command with the **Remove everything** option.

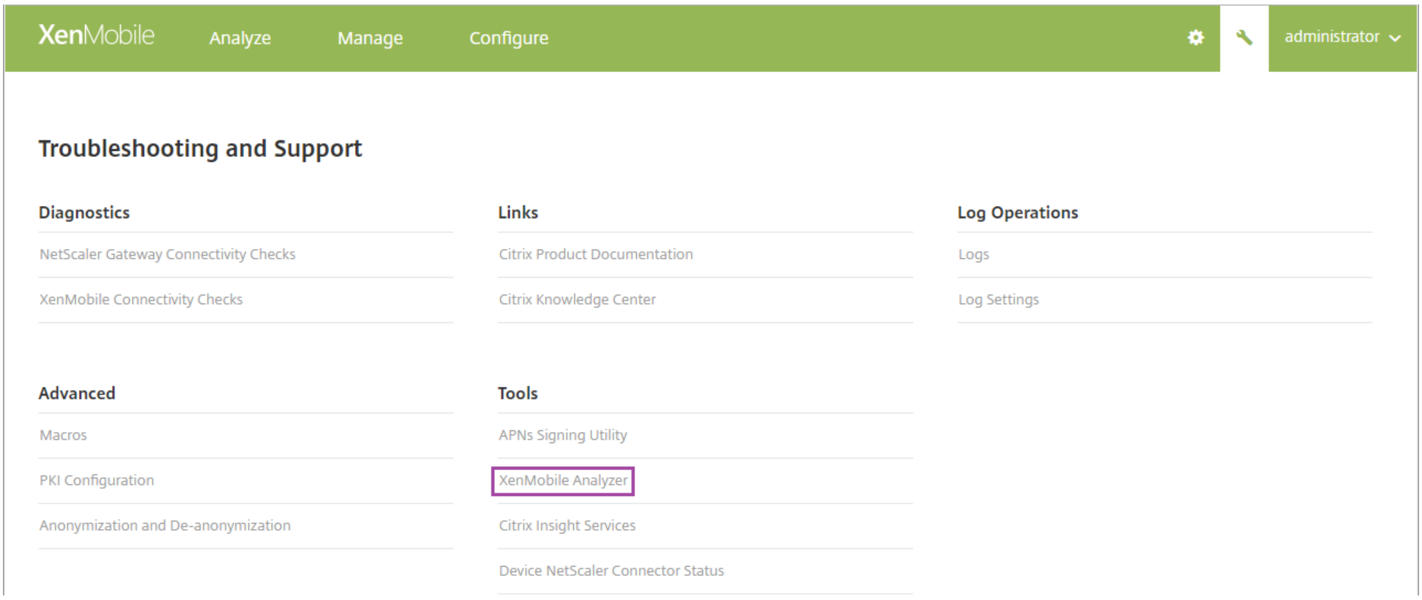


After you click **Full Wipe**, the **Device Actions** list includes **Cancel Wipe**. You can cancel a wipe before XenMobile deploys the wipe request.

Users can also wipe their Windows Desktop or Tablet device in the Self Help Portal.

XenMobile logs include wipe and cancel wipe events.

- The **Duration until removal option** for all iOS device policies has changed from days to hours. This latest version of XenMobile converts existing values to hours.
- **Improved performance of device queries and device filter expansion**. XenMobile now handles queries for device filter counts separately from device queries. When you expand a filter on the **Manage > Devices** page, spinners appear in place of filter counts until the counts are available.
- The **Troubleshooting and Support** page now includes a link to the XenMobile Analyzer.



Troubleshooting and Support

Diagnostics
- NetScaler Gateway Connectivity Checks
- XenMobile Connectivity Checks

Links
- Citrix Product Documentation
- Citrix Knowledge Center

Log Operations
- Logs
- Log Settings

Advanced
- Macros
- PKI Configuration
- Anonymization and De-anonymization

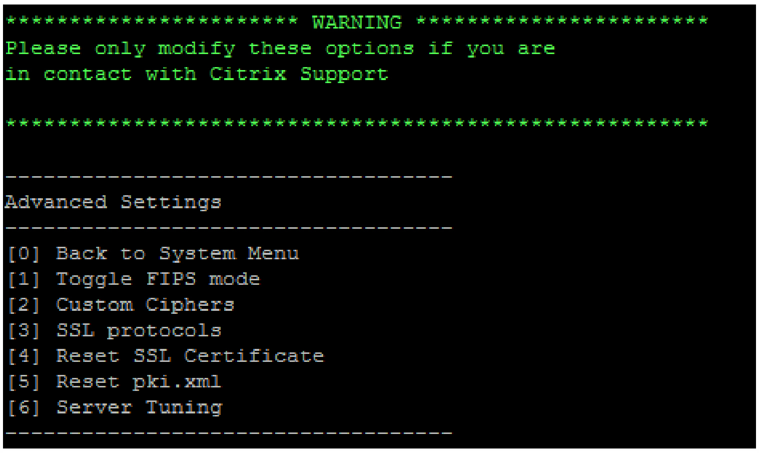
Tools
- APNs Signing Utility
- XenMobile Analyzer
- Citrix Insight Services
- Device NetScaler Connector Status

- **New XenMobile CLI option to specify SSL protocols**. You can now use the CLI to specify which SSL protocols XenMobile uses. The protocols allowed are:
  - TLSv1.2
  - TLSv1.1
  - TLSv1

  By default, XenMobile enables each of those SSL protocols. When you change the SSL protocol setting, you must restart XenMobile Server.

  To enable or disable protocols:

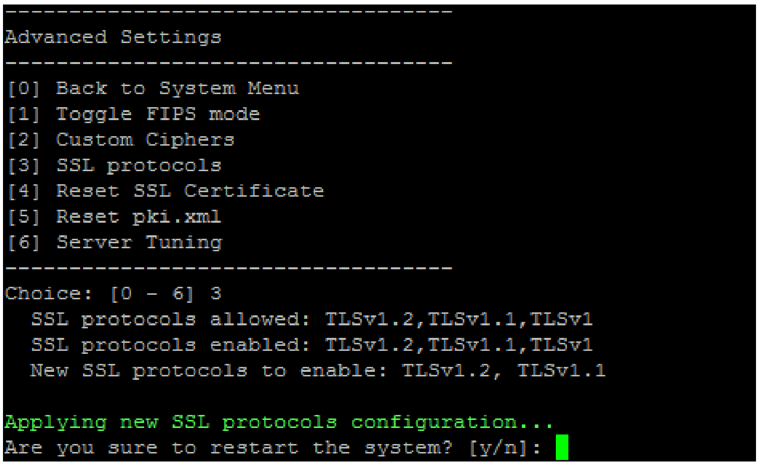
1. Open the XenMobile CLI, choose **[2] System**, and choose **[12] Advanced Settings**.



```
*********************** WARNING ***********************
Please only modify these options if you are
in contact with Citrix Support

*******************************************************

-----------------------------------
Advanced Settings
-----------------------------------
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] SSL protocols
[4] Reset SSL Certificate
[5] Reset pki.xml
[6] Server Tuning
-----------------------------------
```

2. Choose **[3] SSL protocols**.

3. After the prompt **New SSL protocols to enable**, type the protocols you want to enable. XenMobile disables any protocols that you don't include in your response. For example: To disable TLSv1, type **TLSv1.2,TLSv1.1** and then type **y** to restart XenMobile Server.



```
-----------------------------------
Advanced Settings
-----------------------------------
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] SSL protocols
[4] Reset SSL Certificate
[5] Reset pki.xml
[6] Server Tuning
-----------------------------------
Choice: [0 - 6] 3
  SSL protocols allowed: TLSv1.2,TLSv1.1,TLSv1
  SSL protocols enabled: TLSv1.2,TLSv1.1,TLSv1
  New SSL protocols to enable: TLSv1.2, TLSv1.1

Applying new SSL protocols configuration...
Are you sure to restart the system? [y/n]:
```

Fixed issues

XenMobile 10.6 includes the following fixed issues. Fixed issues for the Upgrade Tool appear in "XenMobile Upgrade Tool," later in this article.

For fixed issues related to XenMobile Apps, see Fixed issues.

When users enroll in XenMobile through an Azure Active Directory account, even after you wipe or revoke the device, they can enroll again without authorization. This issue is a third-party issue. [#628865, CXM-23203]

After upgrading to XenMobile Server 10.4:

- If you click the **ShareFile** tab, the page might not load and the information doesn't appear.

- If you attempt to add or edit a delivery group, the following error message might appear: 500 Internal Server error.

[#663344, #663788, CXM-19085]

If a table of users or enrollment invitations has multiple pages and you edit an item on the second or following page: After you save the change, XenMobile shows the first page of the table and discards the updates. [CXM-20209]

If you move a StorageZone Connector from delivery group A to delivery group B: ShareFile for iOS users in delivery group A can continue to use the connector. [CXM-21860]

When you integrate StoreFront with XenMobile and deploy HDX apps: After you change an Active Directory password, the HDX apps disappear from the XenMobile Store. [CXM-9859, CXM-22821]

If a table of users or enrollment invitations spans multiple pages and you edit an item on the second or following page: After you save the change, XenMobile shows the first page of the table and discards the updates. [CXM-20209]

If you move Active Directory users out of a group with permissions for StorageZone Connectors, ShareFile for iOS users can still access associated Network shares. To work around this issue, reinstall the ShareFile for iOS app. [CXM-21859]

You can't create a support bundle by using the XenMobile CLI. As a workaround, use the XenMobile console: Go to **Support > Create Support Bundles** and then click **Create**. [CXM-23091]

For a multi-page table of devices in the XenMobile console: After you save an edit to an item on the second or following page, XenMobile shows the first page of the table and discards the updates. [CXM-23143]

App downloads for MAM deployments to iOS and Android devices might fail. [CXM-23280]

If the server property **StorageZone Connectors supported** value is **NOT SUPPORTED** and you configure ShareFile in the XenMobile console: After you navigate to a different page and then return to **Configure > Sharefile**, the Sharefile page doesn't show the configuration although the configuration is saved. To work around this issue, change the server property, **Sharefile configuration type**, to **ENTERPRISE**. [CXM-23337]

When you configure a Windows Information Protection device policy and you enable the setting **Revoke WIP certificate on unenroll**: After you selectively wipe a Windows 10 tablet account, users are able to access a secure file. In addition, the file is not encrypted as expected. This condition is an issue with Windows 10 RS1 tablet. [CXM-23362]

For devices connecting to a cluster node: When you deploy policies and apps from a different cluster node, cluster issues occur. [CXM-23737]

When users whose sAMAccountName is different from the UPN prefix in Active Directory try to enroll their devices by using the invitation URL: XenMobile attempts to resolve the sAMAccountName@domainname as UPN and enrollment fails. As a workaround, in the XenMobile console, create invitations by user instead of by group. [CXM-24223]

When XenMobile queries Active Directory for a user group and receives an empty response with no errors: XenMobile interprets the response to mean that the group is deleted from Active Directory. XenMobile then deletes the user group from its database, causing users to lose access. [CXM-24228]

The Syslog server does not show the app name for app downloads. [CXM-24620]

If you create an RBAC role name that includes an ampersand (&), the symbol is encoded and you cannot edit the name. [CXM-24621]

For a XenMobile Webclip device policy: If the name and URL includes HTML special characters, such as ampersand (&), XenMobile encodes the characters. As a result, the URL breaks when you deploy the policy to managed devices. [CXM-

24622]

When adding a public Google Play Store app in the XenMobile console: The app search function doesn't pass through the proxy as expected and search fails to return the correct apps. [CXM-24894]

On the **Manage > Devices** page of the XenMobile console: Sorting by the **Inactivity Days** and **Last Access** columns in the table results in an error. [CXM-24895]

For Windows 10 devices enrolled through Azure Active Directory during initial setup of the device: You cannot perform a selective wipe on the device from the XenMobile console. This issue is a Microsoft limitation. [CXM-24899]

Issues might occur when uploading some VPP tokens to a new installation of XenMobile 10 or when migrating some VPP tokens from XenMobile 9 to 10.5. [CXM-25268]

If you include an ampersand (&) in a device policy or RBAC role name, XenMobile saves the name with **&amp;**instead of **&**. For example, **policya&b** is named **policya&amp;b**. [CXM-25630]

After you assign devices to a different DEP account, XenMobile removes those devices from its database. [CXM-25692]

In the **Configure > Device Policies** page for the VPN device policy, the following settings are optional, although the console page indicates that they are required (*): DNS server IP addresses, Search domains, Supplemental match domains. [CXM-25767]

If you add a VPP token to XenMobile, consume a VPP license with device association, delete the token, and then add the same token: In the **VPP ID Assignment** table on the **Configure > Apps** settings page, the **Associated Device** column might include **Hidden** instead of the device serial number. [CXM-25907]

All device properties for an enrolled macOS device get populated in XenMobile only if the following occurs: A delivery group is associated with the enrolled device and has a deployed resource, such as a policy. [CXM-25917]

After you click **Add** on the **Configure > Device Policies** page, XenMobile doesn't filter the policy list and search results by the selected platforms. Only the first five search results appear. [CXM-26354]

The General properties in the VMware console incorrectly show the Guest OS as a 32-bit OS, instead of 64-bit. This issue resolves when you install the updated VMware (.ova) file. [CXM-28048]

When users delete an app from the XenMobile console, the app remains in the database. As a result, the console doesn't sync with the database. [CXM-29613]

When filtering a report by date on the **Analyze > Reporting** page, the Calendar under the last access doesn't open after you click the calendar icon. As a workaround, click the **Value** field to open the date chooser. [CXM-29748]

In the XenMobile console, when you edit a delivery group role, the delivery group name and **Next** button intermittently do not appear. [CXM-30010]

After you aggregate and deploy XenApp and XenDesktop resources to Secure Hub, with the associated configuration on the XenMobile console: The HDX app icons don't appear in the store and an error message appears when users launch the apps. The message is: XenApp - Failed to get application detail. Please try again later. [CXM-30737]

When you configure and save an automated action in the XenMobile 10.5 console, the Base or Advanced Deployment Rules are not saved. The issue occurs on all platforms. [CXM-30742]

In some XenMobile Server environments in a clustered configuration, memory allocation issues occur on all nodes. When this issue occurs, the servers become unresponsive. [CXM-31283]

Exporting a CSV file for the **VPP apps license usage** Dashboard widget results in high CPU utilization on the database server. [CXM-31917]

Occasionally, a memory spike and out of memory error occurs on a XenMobile Server instance. When this issue occurs, the XenMobile Server becomes unresponsive. [CXM-31959]

In the **Settings > Apple Configurator Device Enrollment** page, after you change a setting and then click **Save**, an Internal Server Error message appears. XenMobile saves the changes. [CXM-32446]

On the XenMobile **Settings > Google Play Credentials** page: After you type the settings and click **Save**, the message "Email or password incorrect" appears intermittently. This error is due to an update from Google. [CXM-32847]

XenMobile Upgrade Tool

After you upgrade to XenMobile 10.4 from XenMobile 9, Windows devices are in MDM mode instead of in MAM+MDM mode. In addition, the XenMobile Store does not open. As a work-around, users can reenroll a migrated device. [CXM-18532]

Issues might occur when uploading some VPP tokens to a new installation of XenMobile 10 or when migrating some VPP tokens from XenMobile 9 to 10.5. [CXM-25268]

After an upgrade from XenMobile 9 to 10.x, a certificate might not renew because of an issue with the certificate renewal period conversion. [CXM-25637]

If you use PostgreSQL with XenMobile 9: Upgrading from XenMobile 9 to 10.x might fail intermittently because the PostgreSQL JDBC driver ignored the fetch size. [CXM-25638]

Known issues

XenMobile 10.6 includes the following known issues. Fixed issues for the Upgrade Tool appear under the heading "XenMobile Upgrade Tool" in this article.

For known issues related to XenMobile Apps, see Known issues.

Some Enterprise apps for Android don't upload to a XenMobile console configured in MDM or Enterprise (XME) mode. [CXM-22377]

When you configure a Windows Information Protection device policy and you enable the setting **Revoke WIP certificate on unenroll**: After you selectively wipe a Windows 10 tablet account, users are able to access a secure file. In addition, the file is not encrypted as expected. This issue is a Microsoft issue with Windows 10 RS1 tablet. [CXM-23362]

For Windows 10 devices enrolled through Azure Active Directory during initial setup of the device: You cannot revoke the device from the XenMobile console. This issue is a Microsoft limitation. [CXM-24897]

After you update the obfuscated APK file for some Android apps in the XenMobile console: The older version appears in the details and the updated version doesn't deploy to devices. [CXM-25629]

For Windows 10 RS2 Phone: When you issue a Ring device action from **Manage > Devices**, the ring command fails and doesn't deploy to the device. This is a third-party issue. [CXM-25888]

For Windows 10 RS2 Phone and Tablet: During re-enrollment, a user isn't prompted for the Server URL. To work around this issue, restart the device. Or, on the email address screen, tap the **X** across from **Connecting to a service** to go to the **Server URL** page. This is a third-party issue. [CXM-25900]

When XenMobile is in MAM-only mode, enrollment fails after the following steps: [CXM-26481]

1. A user enrolls an iOS device through a one-time PIN invitation.

2. The user removes their account from Secure Hub.

3. The user re-enrolls through a different type of one-time PIN invitation. For example, the first enrollment mode is High Security and the second enrollment mode is Invitation URL + PIN. Enrollment occurs within the NetScaler Enable Session Reuse timeout value, which defaults to two minutes.

When derived credentials are enabled on XenMobile Server, the Self Help Portal allows you to create enrollment invitations for iOS. [CXM-29679]

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. [CXM-30053]

On Windows 10 phones, if you deploy a Windows Information Protection device policy that has OneDrive configured as an allowed app, the following issue occurs. If you selectively wipe the device, OneDrive crashes when users open it. As a workaround, configure OneDrive as an exempt app in the Windows Information Protection device policy. [CXM-30618]

After XenMobile uses derived credentials for iOS device enrollment: If you later update **Settings > Derived Credentials** with a certificate that isn't from your provider, XenMobile continues to use derived credentials for iOS device enrollment. As a workaround, after you choose a different certificate in **Settings > Derived Credentials**, delete the derived credentials certificate from **Settings > Certificates**. [CXM-31540]

On a Windows RS2 tablet device that is enrolled with the XenMobile Server and logged in to a deployed Exchange account: If you use the XenMobile console to make the device unmanaged (except full wipe), the Exchange account remains on the enrolled device. [CXM-31697]

If the deprecated Enterprise Data Protection policy is configured and you upgrade to the latest version of XenMobile, the XenMobile console displays this error: "A configuration error has occurred. Please try again." As a workaround, delete the EDP policy before you upgrade XenMobile Server. [CXM-32132]

When searching for an app in the Google Play Store from the XenMobile console, the message "Error logging in with Google Play credentials" appears intermittently. You can close the error message and continue to search for apps. [CXM-32441]

For XenMobile cloud deployments outside of the U.S. only: When searching for an app in the Public App Store from the XenMobile console, the message "Error searching app from store platform: windows_phone" appears. [CXM-32444]

In the German, Korean, and Simplified Chinese versions of the XenMobile console: On the Android platform page for the VPN device policy, for the Citrix VPN connection type, the following labels aren't translated.

- Password and Certificate (an Authentication type option)
- Application List, App Package Name [CXM-33640]

XenMobile Server 10.6 documentation errata

The following items are errata found in the documentation since they were last published. Errata are content issues, such as errors or missing information, that could affect your use of XenMobile Server.

- XenMobile Server 10.6 supports VMWare ESXi 5.5.
- On page 106, under Port requirements, the following information should be included.

  The following port must be open for devices and apps to communicate with XenMobile 10.x.
  - **Port**: 30001
  - **Description**: Management API for initial staging of HTTPS service
  - **Source**: Internal LAN
  - **Destination**: XenMobile Server

Related information

> XenMobile Support Knowledge Center

What's new in XenMobile Server 10.5

Sep 27, 2017

> ## Note
>
> For the full set of product documentation for XenMobile Server 10.5, see the PDF.
>
> For updates and corrections to the XenMobile Server 10.5 PDF, see XenMobile Server 10.5 documentation errata.

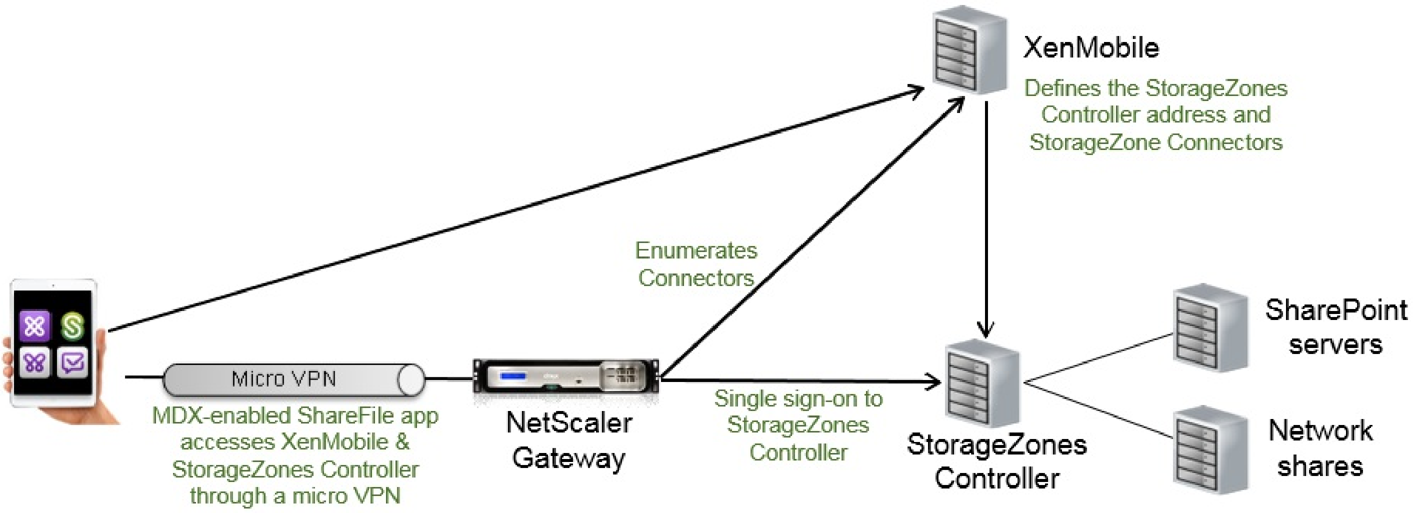
XenMobile Server 10.5 included the following new features. For information about known and fixed issues, see Known issues and Fixed issues later in this article.

Simplified management and deployment of ShareFile StorageZone Connectors

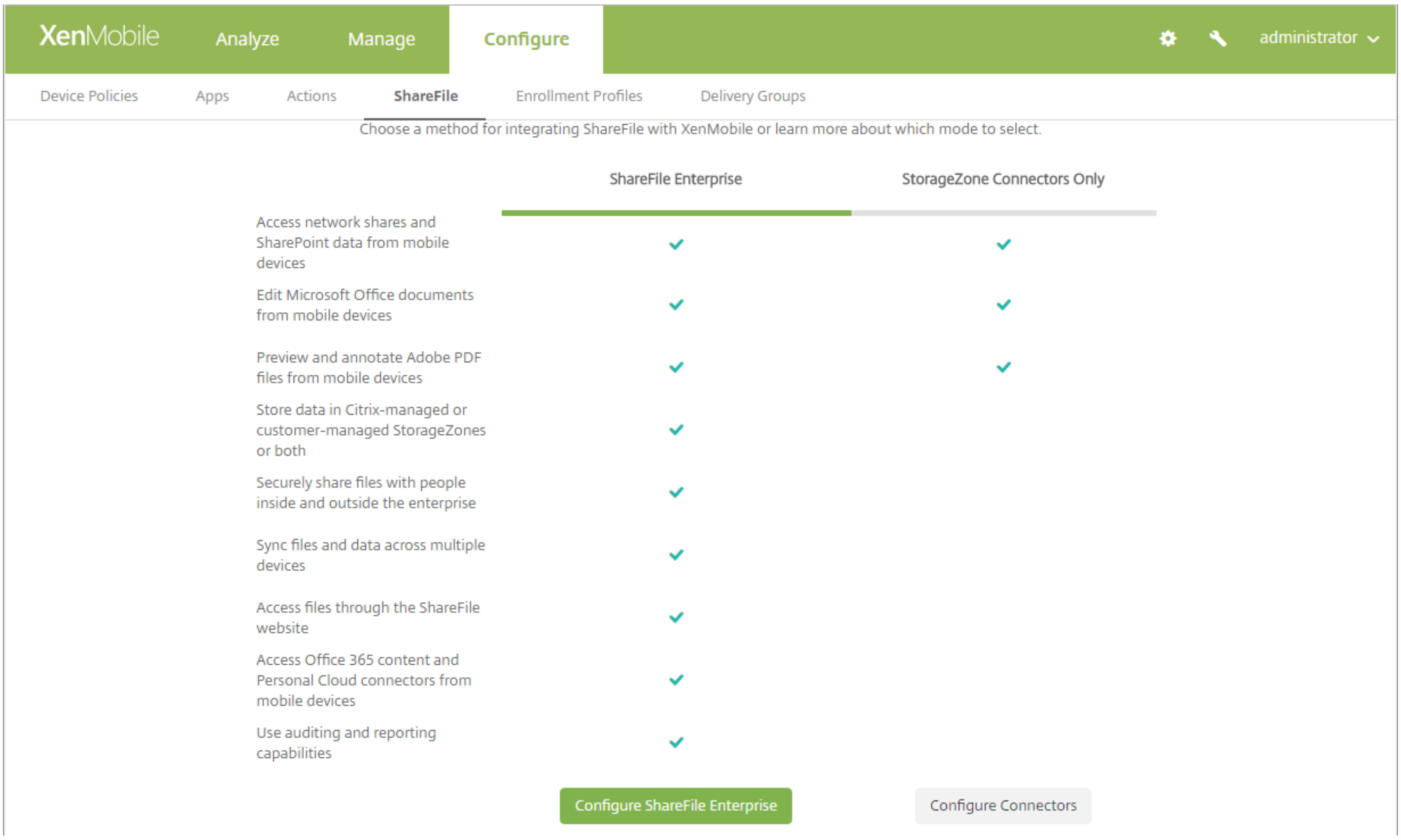
You can now use the XenMobile console to configure StorageZone Connectors. Offered as an alternative to using XenMobile with ShareFile Enterprise, the option to use XenMobile with StorageZone Connectors:

- Provides secure mobile access to existing on-premises storage repositories, such as SharePoint sites and network file shares. Doesn't require that you set up a ShareFile subdomain, provision users to ShareFile, or host ShareFile data.
- Provides users with mobile access to data through the ShareFile XenMobile Apps for iOS. Users can edit Microsoft Office documents. Users can also preview and annotate Adobe PDF files from mobile devices.
- File access is limited to the connectors. Users don't have access to other ShareFile functionality such as data sharing or syncing.
- Complies with security restrictions against leaking user information outside of the corporate network.
- Provides simple setup of StorageZone Connectors through the XenMobile console. If you later decide to use the full ShareFile functionality with XenMobile, you can change the configuration in the XenMobile console.
- Requires XenMobile Enterprise Edition.

The following diagram shows the high-level architecture for XenMobile use with StorageZone Connectors.


XenMobile
Defines the StorageZones Controller address and StorageZone Connectors
Enumerates Connectors
Micro VPN
MDX-enabled ShareFile app accesses XenMobile & StorageZones Controller through a micro VPN
NetScaler Gateway
Single sign-on to StorageZones Controller
StorageZones Controller
SharePoint servers
Network shares

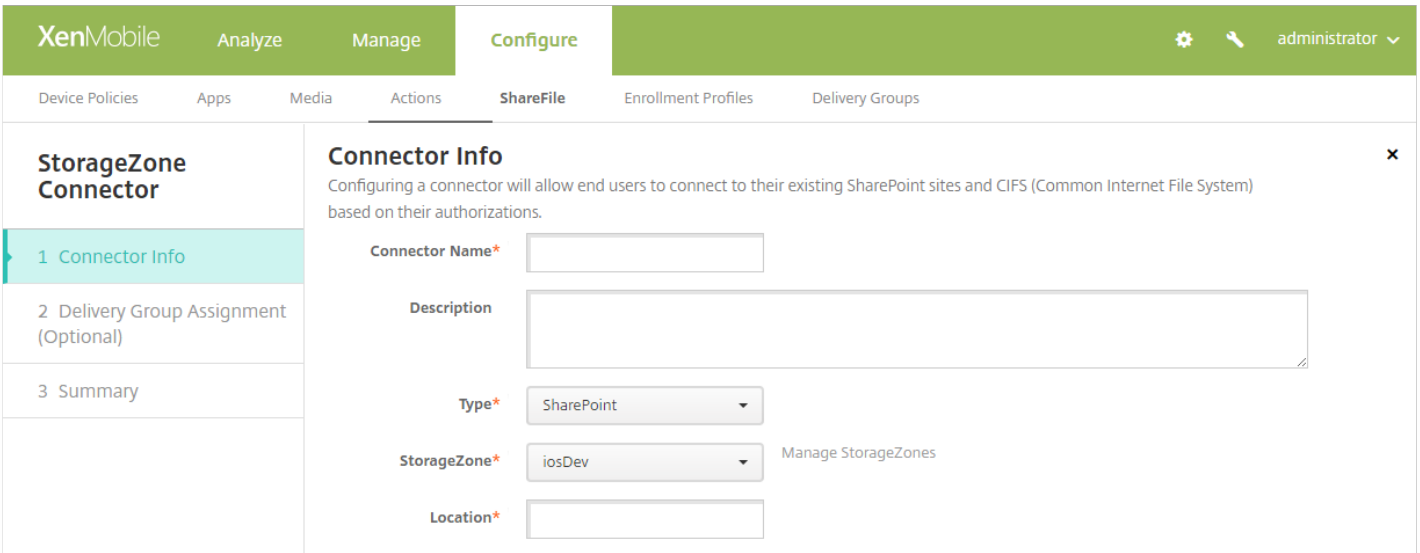
On your first visit to the **Configure > ShareFile** page, a description of the differences between using XenMobile with ShareFile Enterprise and with StorageZone Connectors appears.



Choose a method for integrating ShareFile with XenMobile or learn more about which mode to select.

	ShareFile Enterprise	StorageZone Connectors Only
Access network shares and SharePoint data from mobile devices	✓	✓
Edit Microsoft Office documents from mobile devices	✓	✓
Preview and annotate Adobe PDF files from mobile devices	✓	✓
Store data in Citrix-managed or customer-managed StorageZones or both	✓	
Securely share files with people inside and outside the enterprise	✓	
Sync files and data across multiple devices	✓	
Access files through the ShareFile website	✓	
Access Office 365 content and Personal Cloud connectors from mobile devices	✓	
Use auditing and reporting capabilities	✓	

If you click **Configure Connectors**, you provide information about the connectors and the StorageZones Controller.



Connector Info

Configuring a connector will allow end users to connect to their existing SharePoint sites and CIFS (Common Internet File System) based on their authorizations.

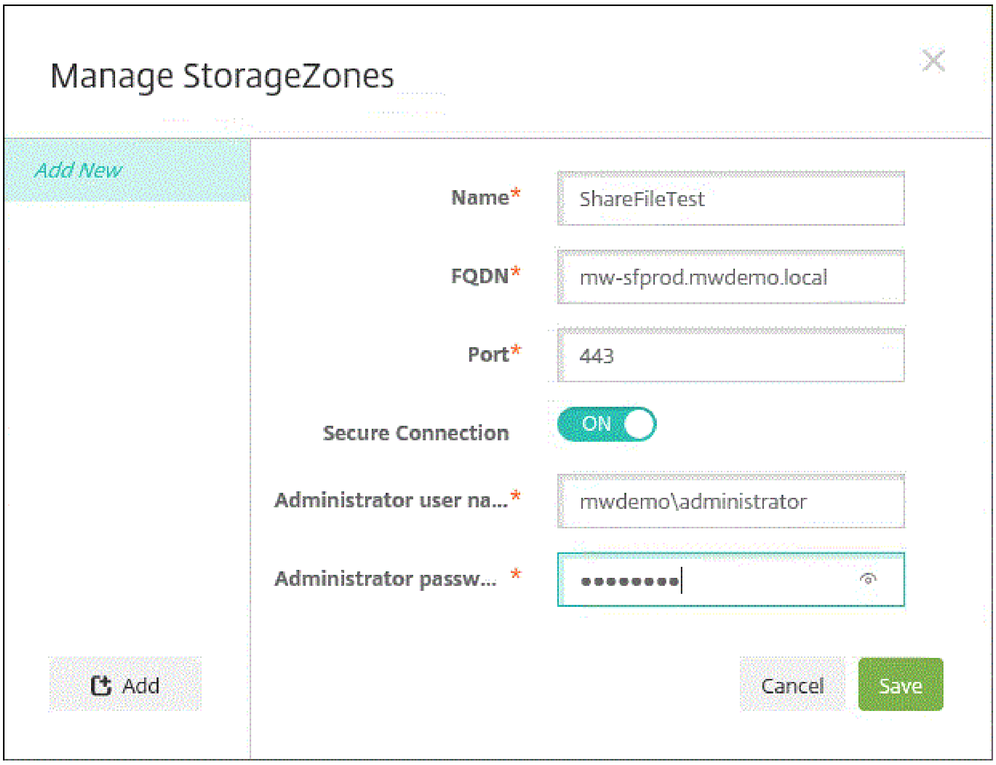
Connector Name*

Description

Type* SharePoint

StorageZone* iosDev

Location*



Manage StorageZones

Add New

Name* ShareFileTest

FQDN* mw-sfprod.mwdemo.local

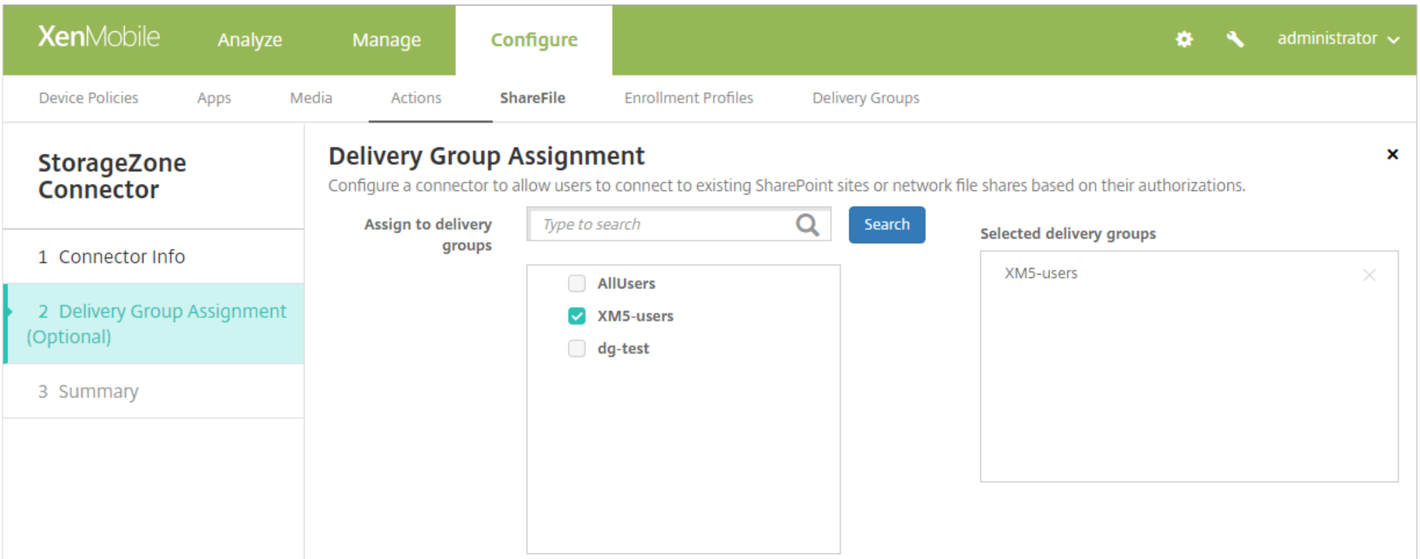
Port* 443

Secure Connection ON

Administrator user na...* mwdemo\administrator

Administrator passw... * ••••••••

You can associate connectors with delivery groups when you create the connector.



Delivery Group Assignment

Configure a connector to allow users to connect to existing SharePoint sites or network file shares based on their authorizations.

Assign to delivery groups: Type to search

□ AllUsers
☑ XM5-users
□ dg-test

Selected delivery groups: XM5-users

You can also associate connectors with delivery groups by using the **Configure > Delivery Groups** page.

For more information about integrating StorageZone Connectors with XenMobile, see ShareFile use with XenMobile.

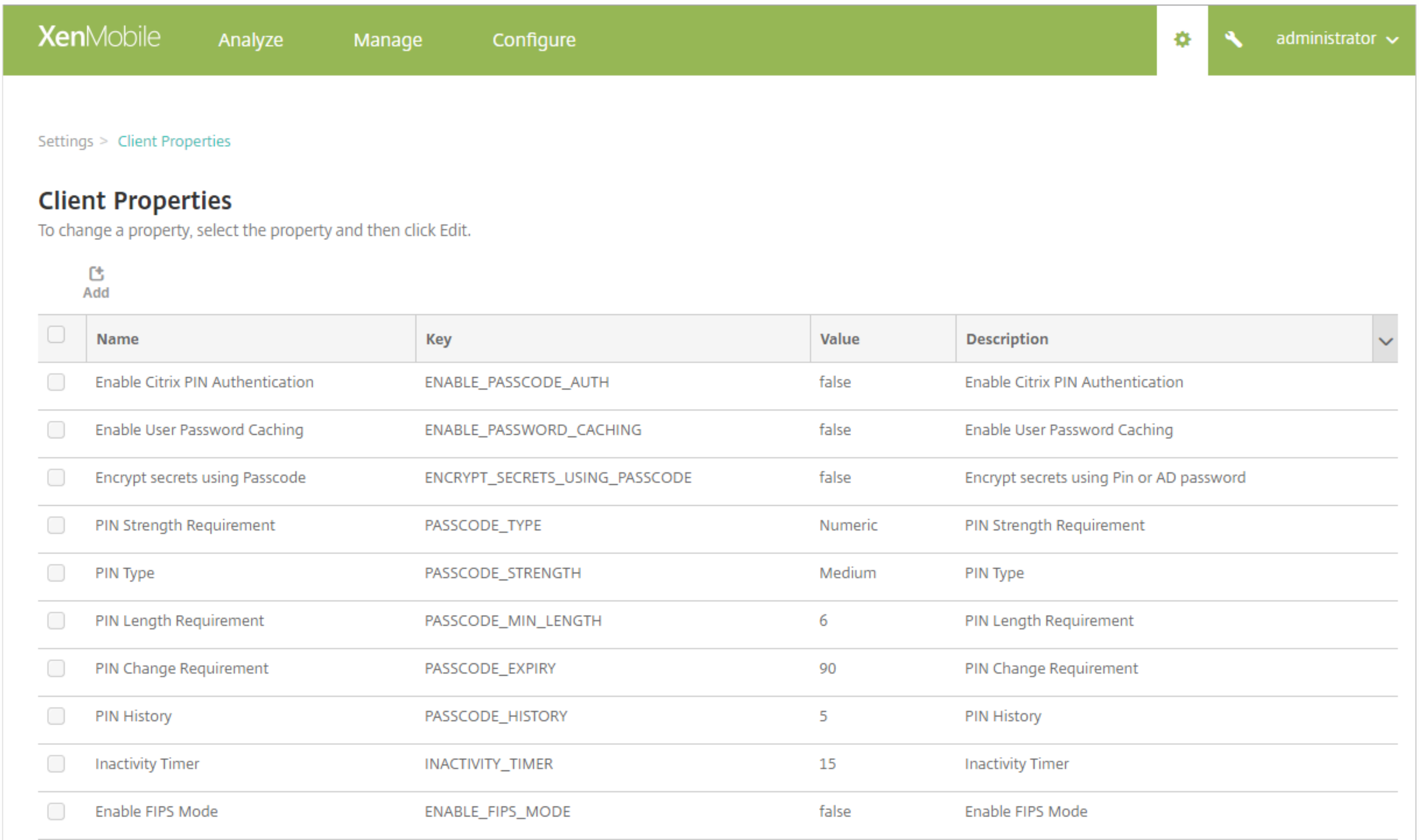
Renamed client properties

XenMobile client property names related to Citrix PIN have changed:

Old property name	New property name

Enable Worx PIN Authentication	Enable Citrix PIN Authentication
Worx PIN Type	PIN Type
PIN Strength Requirement	PIN Strength Requirement
Worx PIN Length Requirement	PIN Length Requirement
Worx PIN Change Requirement	PIN Change Requirement
Worx PIN History	PIN History

The property keys remain the same, as shown in the following sample:



Settings > Client Properties

Client Properties

To change a property, select the property and then click Edit.

	Name	Key	Value	Description
□	Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication
□	Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
□	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
□	PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
□	PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
□	PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement
□	PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
□	PIN History	PASSCODE_HISTORY	5	PIN History
□	Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
□	Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

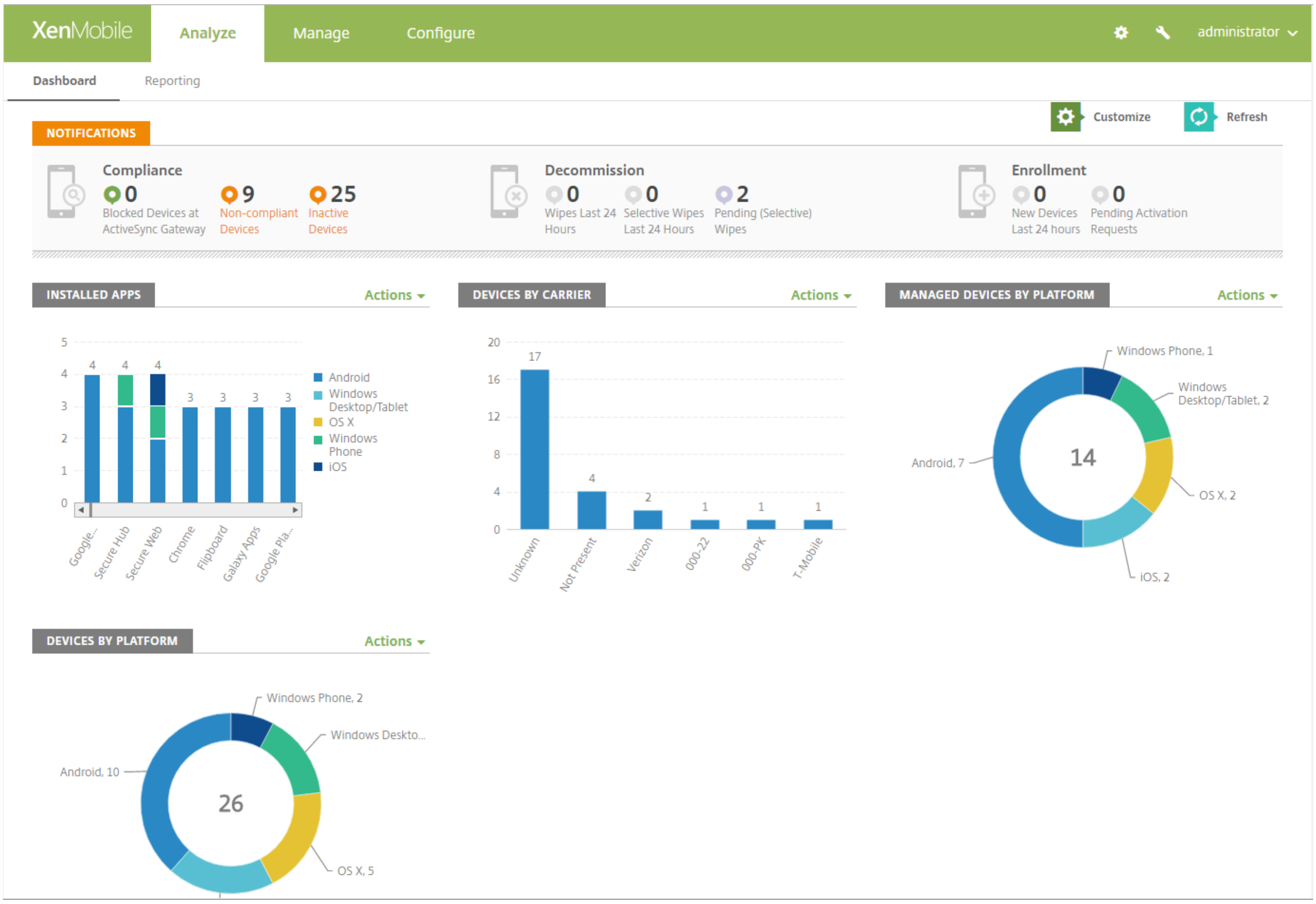
Dashboard improvements

The XenMobile **Analyze > Dashboard** page has a responsive design for improved viewing on smaller devices. Other improvements include:

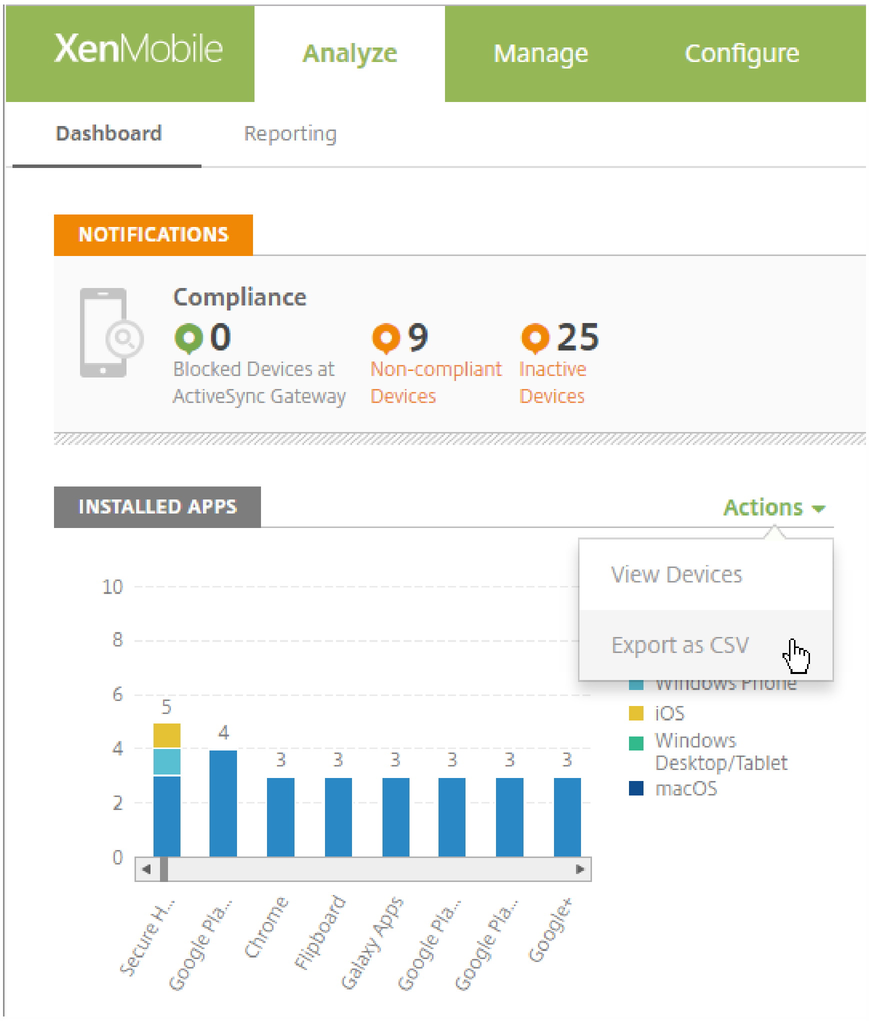
- The Installed Apps widget now shows the top 10 apps. To view other apps, use the search bar.
- To export Installed Apps as a CSV file:

- Choose an app and then export it to get a report for that app only.
- Choose no apps to get a report for all apps.
- The reports include the following information for an app: Name, Owner, Version, Size, ID, and Install time.

- The VPP Apps License Usage widgets now show all apps from the software inventory. You no longer have to search for an app.



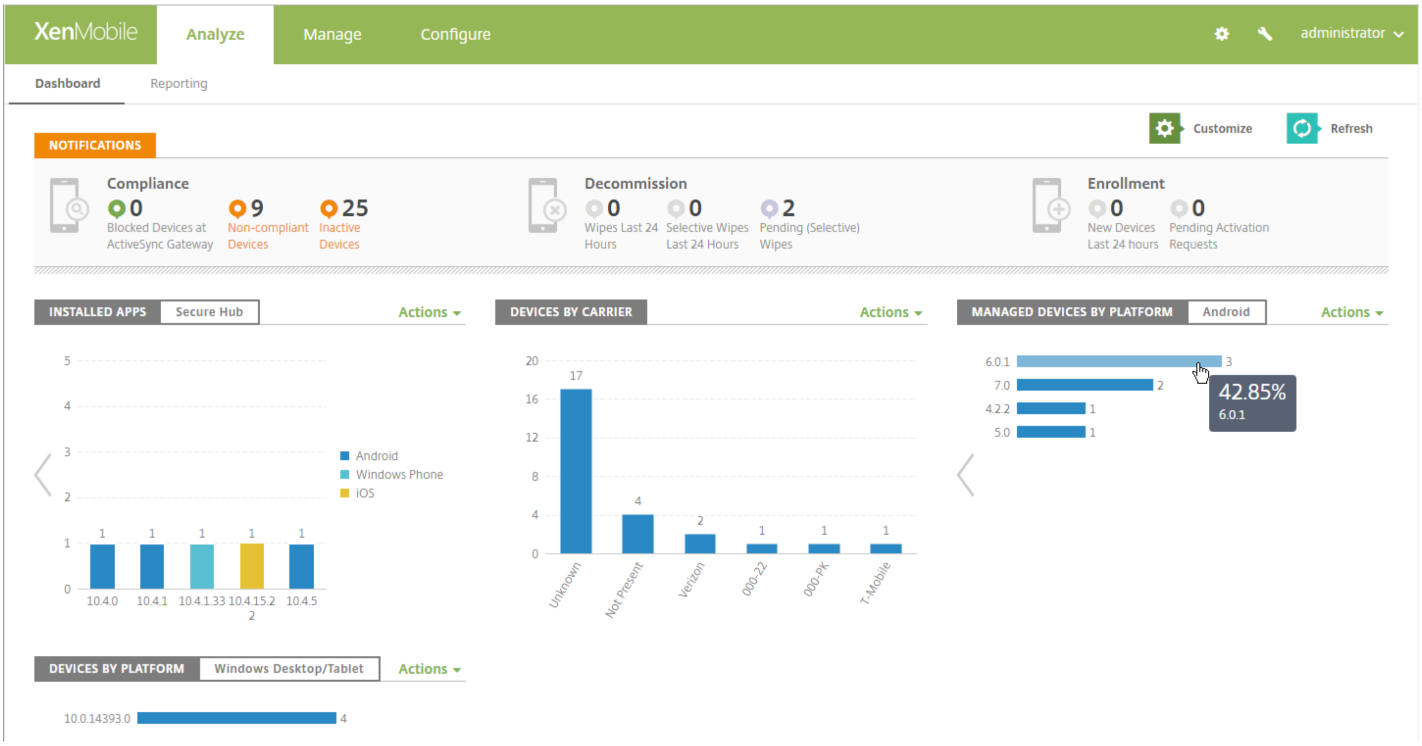
- The charts show counts in descending order.
- Each widget uses the best chart type for the information.
- The actions available for each widget appear in an **Actions** menu, which now includes only the actions most commonly performed from the dashboard:
  - **View Devices** - Opens the **Manage > Devices** page.
  - **Export as CSV** - Saves the data to a CSV file.



- The Export as CSV action exports the following information for each installed app:
  - Name
  - Version
  - Owner
  - Size
  - ID
  - Install time
- You can drill down to two levels of details for the following charts: Click a platform to see a bar chart for the version counts and then click a version to open the **Manage > Devices** page.
  Devices By Platform
  Managed Devices By Platform
  Unmanaged Devices By Platform
  Installed Apps

- To open the **Manage > Devices** page, click any of these charts:
  Devices By Carrier
  Devices By ActiveSync Gateway Status
  Devices By Ownership
  Android TouchDown License Status

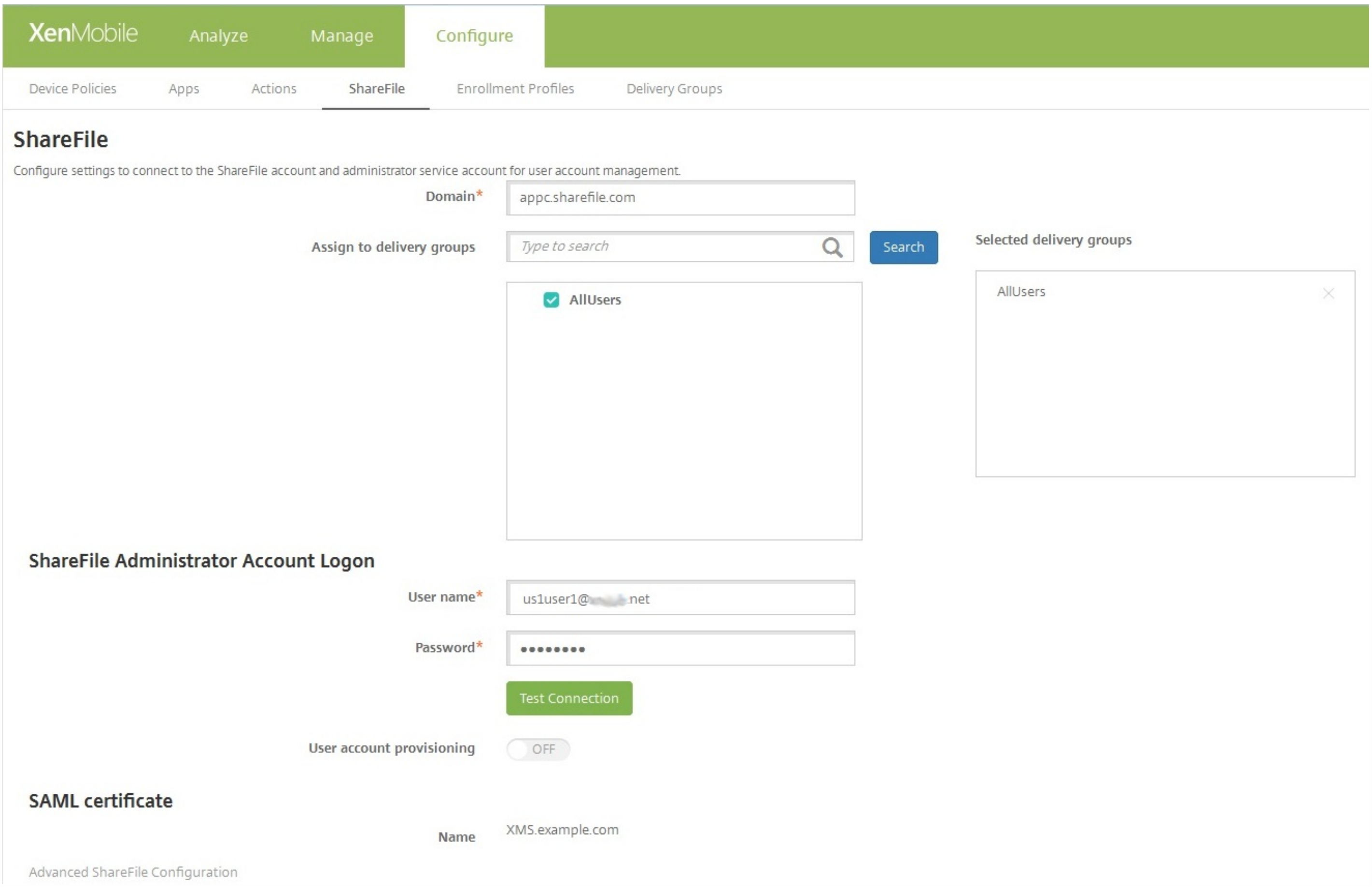
Failed Delivery Group Deployments
Devices By Blocked Reason
VPP Apps License Usage



Test Connection buttons added to XenMobile console

The XenMobile console now includes a **Test Connection** button on these pages:

- **Configure > ShareFile**: You can use the **Test Connection** button to verify that the user name and password for the ShareFile administrator account authenticate to the specified ShareFile account.



ShareFile

Configure settings to connect to the ShareFile account and administrator service account for user account management.

Domain* appc.sharefile.com

Assign to delivery groups: Type to search

☑ AllUsers

Selected delivery groups: AllUsers

ShareFile Administrator Account Logon

User name* us1user1@[redacted].net

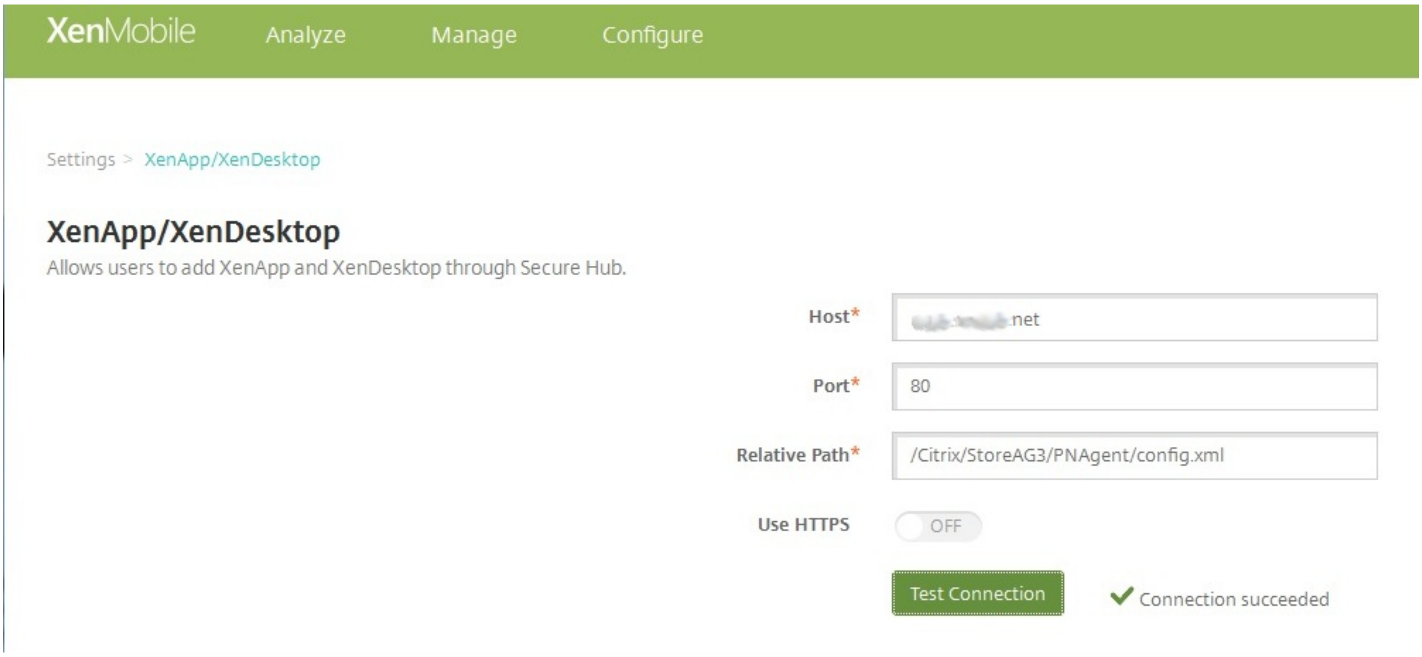
Password* ••••••••

User account provisioning: OFF

SAML certificate

Name: XMS.example.com

- **Settings > XenApp/XenDesktop**: You can use the **Test Connection** button to verify that XenMobile can connect to the specified XenApp and XenDesktop server.



XenApp/XenDesktop

Allows users to add XenApp and XenDesktop through Secure Hub.

Host* [redacted].net

Port* 80

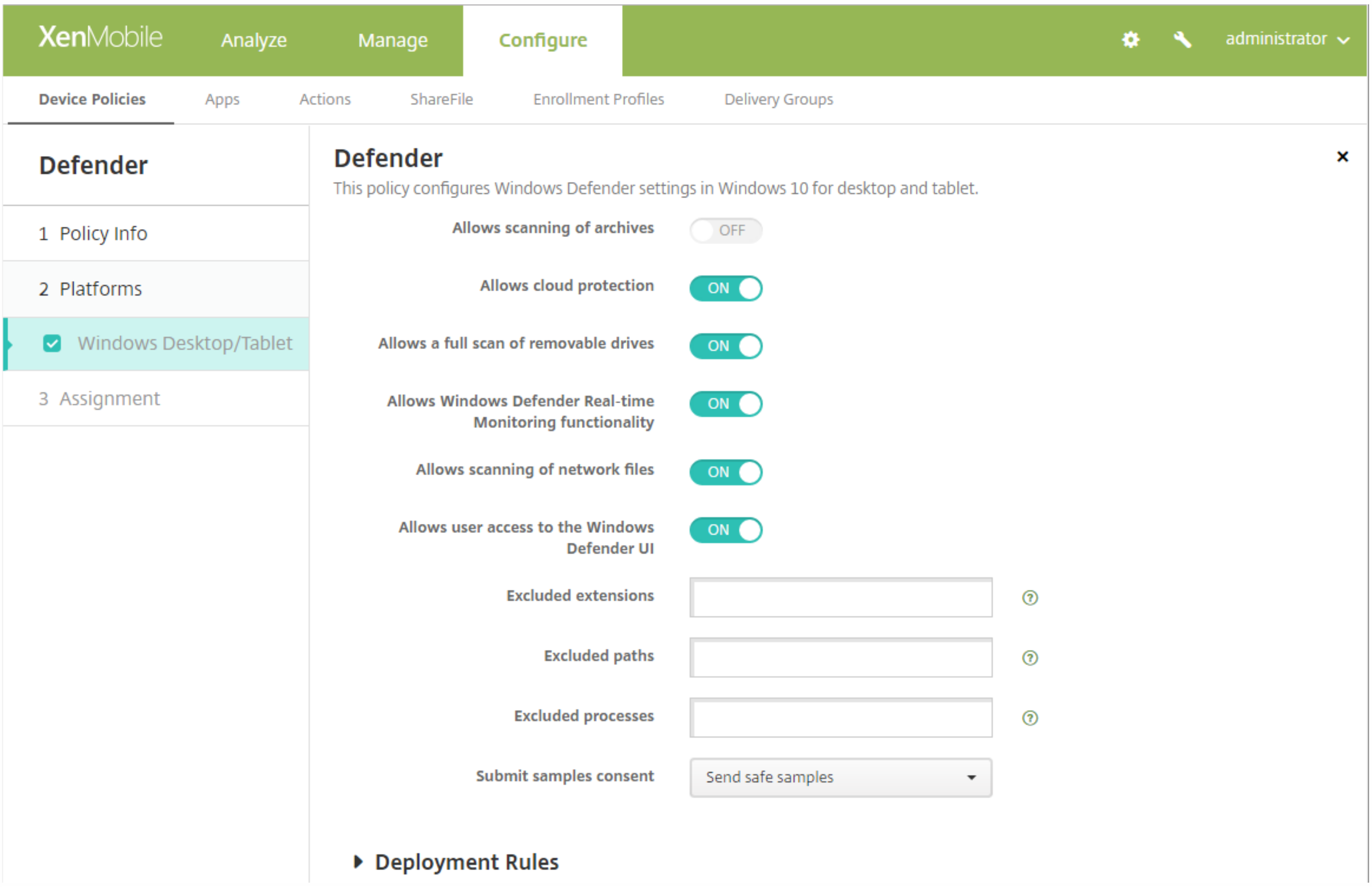
Relative Path* /Citrix/StoreAG3/PNAgent/config.xml

Use HTTPS: OFF

✓ Connection succeeded

Windows Defender device policy for Windows 10 for desktop and tablet

Windows Defender is malware protection included with Windows 10. You can use the XenMobile device policy, Defender, to configure the Microsoft Defender policy. To add the Defender policy, go to **Configure > Device Policies**, click **Add**, start typing **Defender**, and then click that name in the search results.



Defender

This policy configures Windows Defender settings in Windows 10 for desktop and tablet.

Allows scanning of archives: OFF

Allows cloud protection: ON

Allows a full scan of removable drives: ON

Allows Windows Defender Real-time Monitoring functionality: ON

Allows scanning of network files: ON

Allows user access to the Windows Defender UI: ON

Excluded extensions:

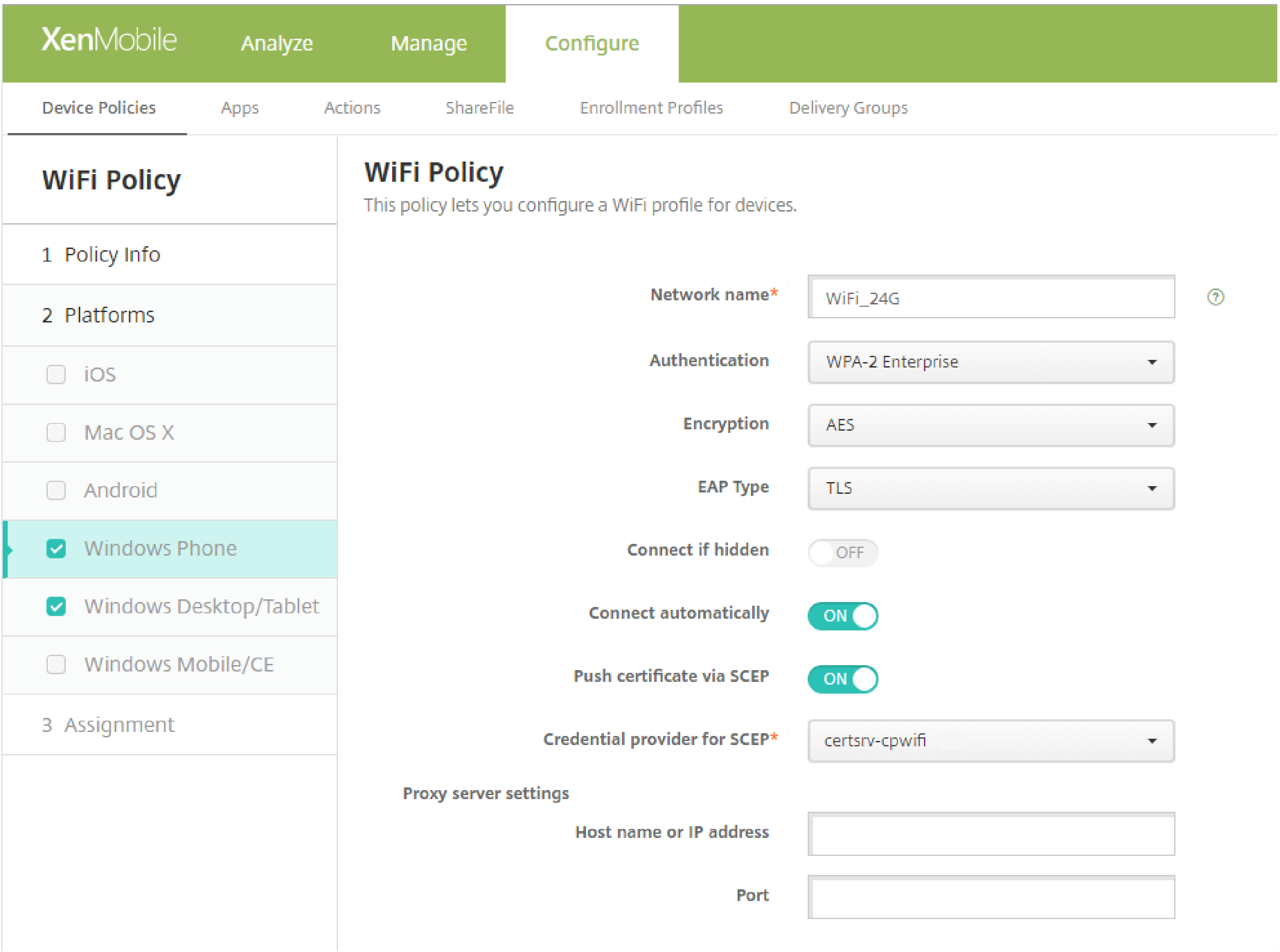
Excluded paths:

Excluded processes:

Submit samples consent: Send safe samples

WiFi device policy support for Windows 10

The WiFi device policy now includes support for Windows 10, enabling you to use client certificate authentication for your WiFi network. To update WiFi device policies, go to **Configure > Device Policies**.



WiFi Policy

This policy lets you configure a WiFi profile for devices.

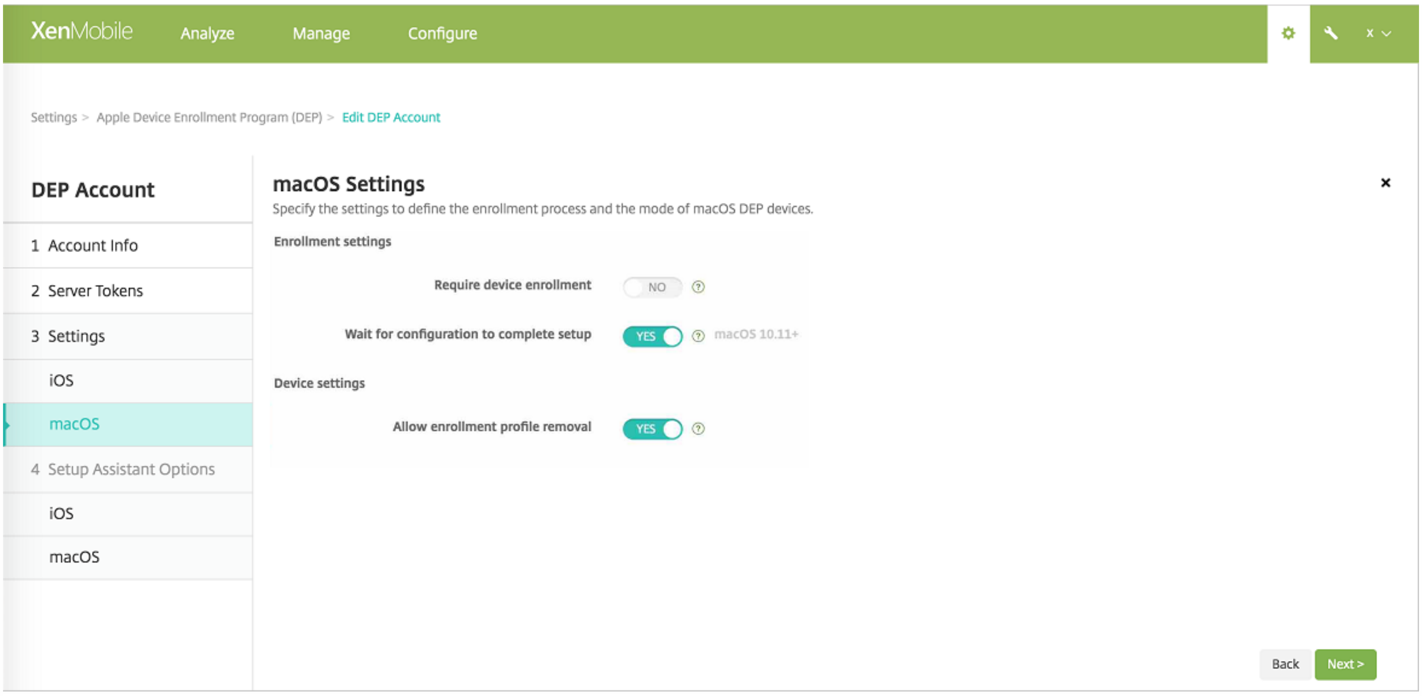
Network name*	WiFi_24G
Authentication	WPA-2 Enterprise
Encryption	AES
EAP Type	TLS
Connect if hidden	OFF
Connect automatically	ON
Push certificate via SCEP	ON
Credential provider for SCEP*	certsrv-cpwifi

Proxy server settings

Host name or IP address	
Port	

Bulk enrollment of macOS devices

The Apple Device Enrollment Program (DEP) setting in XenMobile now supports macOS devices running OS X 10.10 or later. You follow the same process as described in Bulk enrollment of iOS and macOS devices. If you add a DEP account from **Settings > Apple Device Enrollment Program (DEP)**, the **Settings** and **Setup Assistant Options** now includes a page for macOS.



macOS Settings

Specify the settings to define the enrollment process and the mode of macOS DEP devices.

Enrollment settings

Require device enrollment: NO

Wait for configuration to complete setup: YES (macOS 10.11+)

Device settings

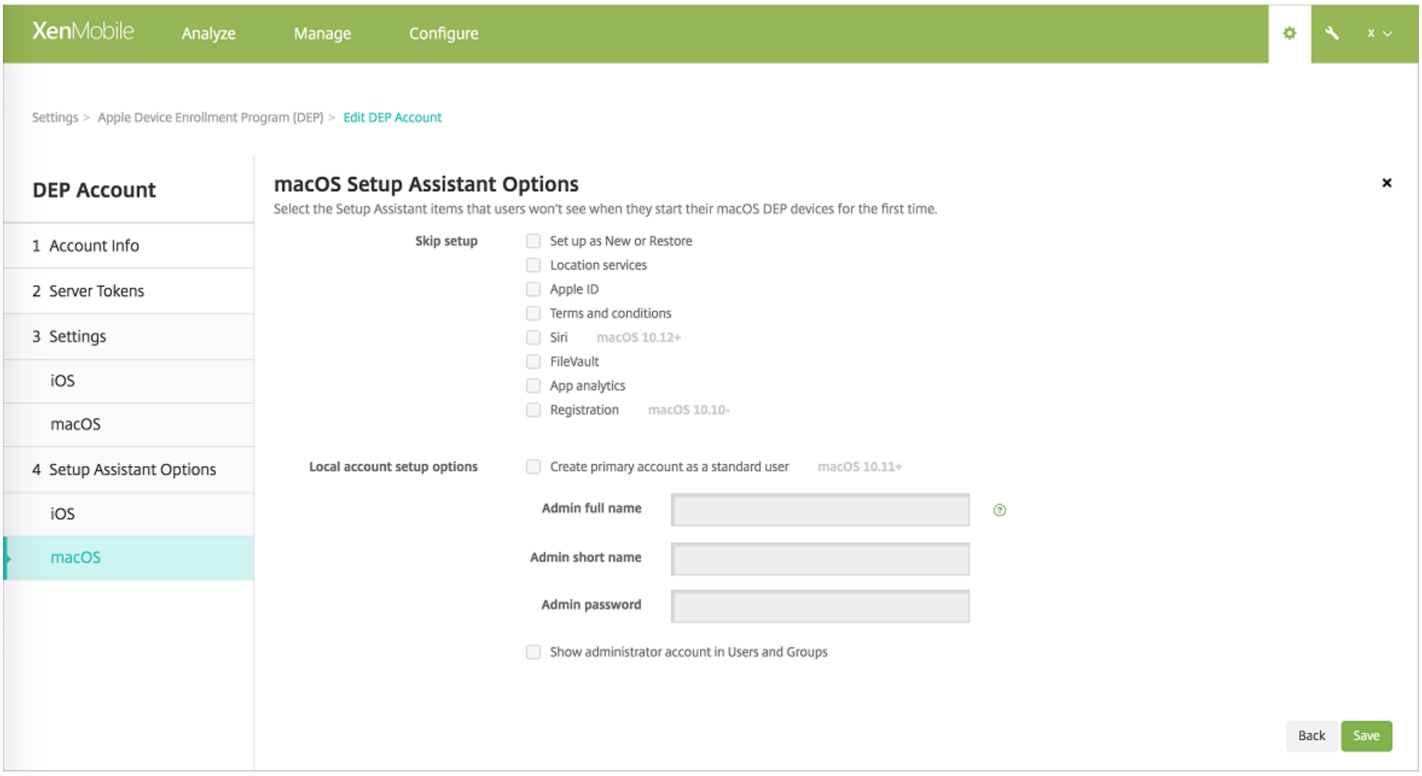
Allow enrollment profile removal: YES

Enrollment settings

- **Require device enrollment**: Whether to require users to enroll their devices. The default is **Yes**.
- **Wait for configuration to complete setup**: If you enable this setting, the macOS device doesn't continue in the Setup Assistant until the MDM resource passcode deploys to the device. The MDM resource passcode deployment occurs before the local account is created. This setting is available for macOS 10.11 and later 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**.



macOS Setup Assistant Options

Select the Setup Assistant items that users won't see when they start their macOS DEP devices for the first time.

Skip setup
- □ Set up as New or Restore
- □ Location services
- □ Apple ID
- □ Terms and conditions
- □ Siri macOS 10.12+
- □ FileVault
- □ App analytics
- □ Registration macOS 10.10-

Local account setup options
- □ Create primary account as a standard user macOS 10.11+

Admin full name

Admin short name

Admin password

□ Show administrator account in Users and Groups

- **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. XenMobile applies the FileVault setting only if the system has a single local user account that is signed in to iCloud.

  You can use the macOS FileVault Disk Encryption feature to protect the system volume by encrypting its contents. See the Apple support article, https://support.apple.com/en-us/HT204837. If you run the Setup Assistant on a late-model portable Mac on which FileVault is off, you might be prompted to turn on this feature. If the system meets the following requirements, the prompt appears on new systems and on systems upgraded to OS X 10.10 or 10.11:

  - The system has a single local administrator account
  - That account is signed in to 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 enabled you to send system registration information to Apple. This information associated your contact information with the Mac hardware. Apple primarily used the information to assist Apple support. If you previously specified an Apple ID, Setup Assistant optionally submitted the registration based on your Apple ID account. If you didn't specify an Apple ID, you can manually type your contact information.

- Under **Local account setup options**, specify the settings to create an administrator account, which is required for macOS. XenMobile creates the account, using the specified information.

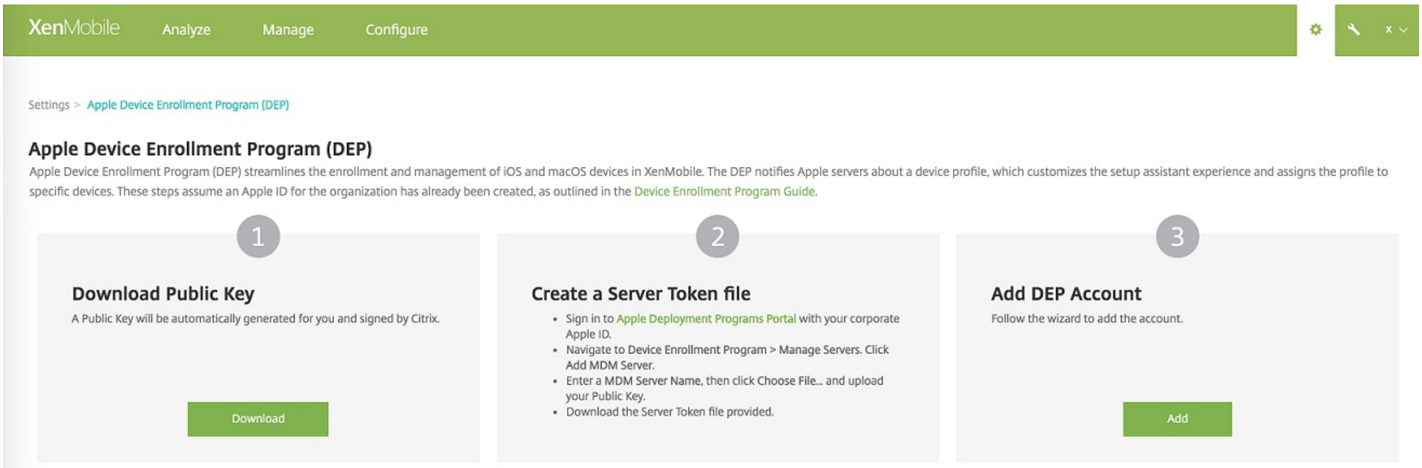
Support for multiple Apple Device Enrollment Program accounts for iOS and macOS devices

You can now define multiple Apple Device Enrollment Program (DEP) accounts. This feature enables you to use different enrollment settings, device settings, and Setup Assistant options. You can specify those settings and options by country, department, and other structures. You then associate DEP accounts with different device policies and different apps through deployment rules.

For example, you might centralize all your DEP accounts from different countries on the same XenMobile Server. You can then import and supervise all DEP devices. By customizing enrollment settings per country or other structure, you ensure that policies provide appropriate functionality across your organization. By customizing Setup Assistant options per country or other structure, you ensure that device users receive the appropriate setup assistance.

To accommodate support for multiple DEP accounts, the following pages replace **Settings > iOS Bulk Enrollment**:

- **Settings > Apple Device Enrollment Program (DEP)**: Use this page is to:
  - Create DEP accounts.
  - Configure enrollment settings, iOS and macOS device settings, and Setup Assistant options per each account.



Apple Device Enrollment Program (DEP)

Apple Device Enrollment Program (DEP) streamlines the enrollment and management of iOS and macOS devices in XenMobile. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. These steps assume an Apple ID for the organization has already been created, as outlined in the Device Enrollment Program Guide.

1 Download Public Key

A Public Key will be automatically generated for you and signed by Citrix.

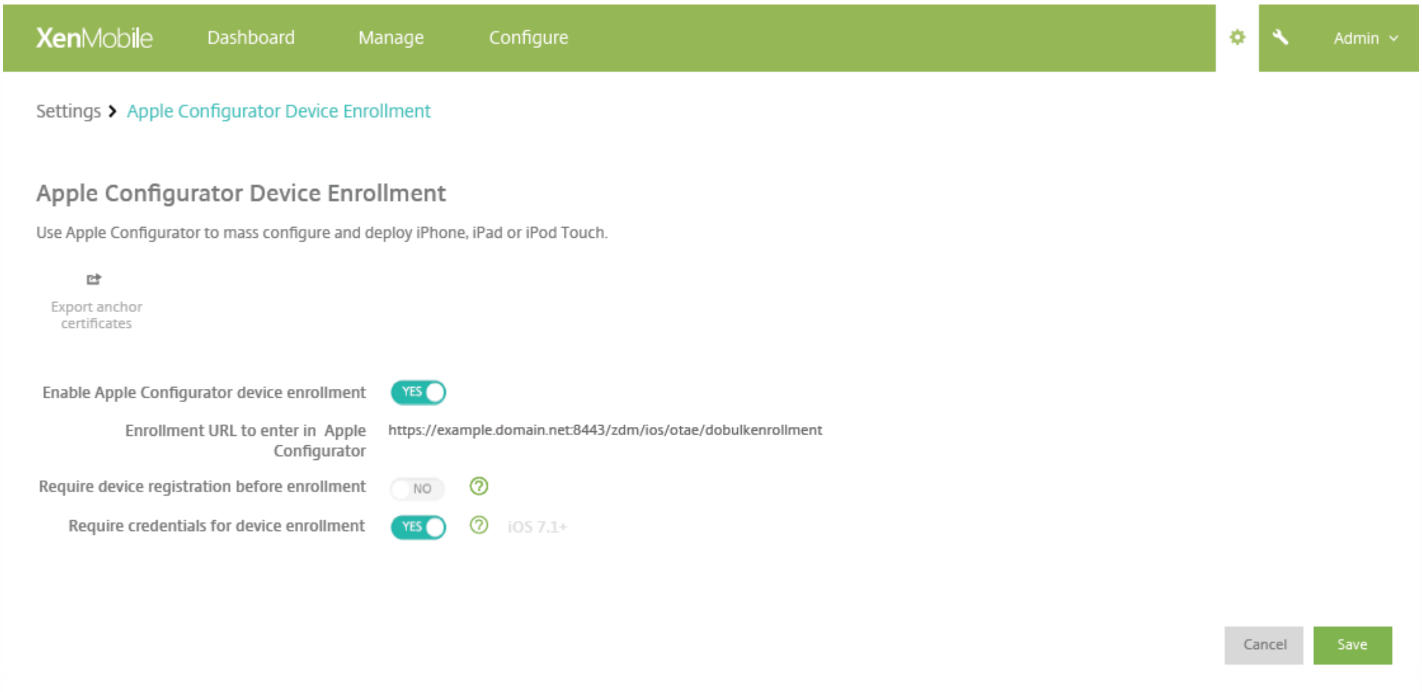
2 Create a Server Token file

- Sign in to Apple Deployment Programs Portal with your corporate Apple ID.
- Navigate to Device Enrollment Program > Manage Servers. Click Add MDM Server.
- Enter a MDM Server Name, then click Choose File... and upload your Public Key.
- Download the Server Token file provided.

3 Add DEP Account

Follow the wizard to add the account.

Settings > Apple Configurator Device Enrollment: Used to prepare iOS and macOS devices and to configure policies.



Settings > Apple Configurator Device Enrollment

Apple Configurator Device Enrollment

Use Apple Configurator to mass configure and deploy iPhone, iPad or iPod Touch.

Enable Apple Configurator device enrollment: YES

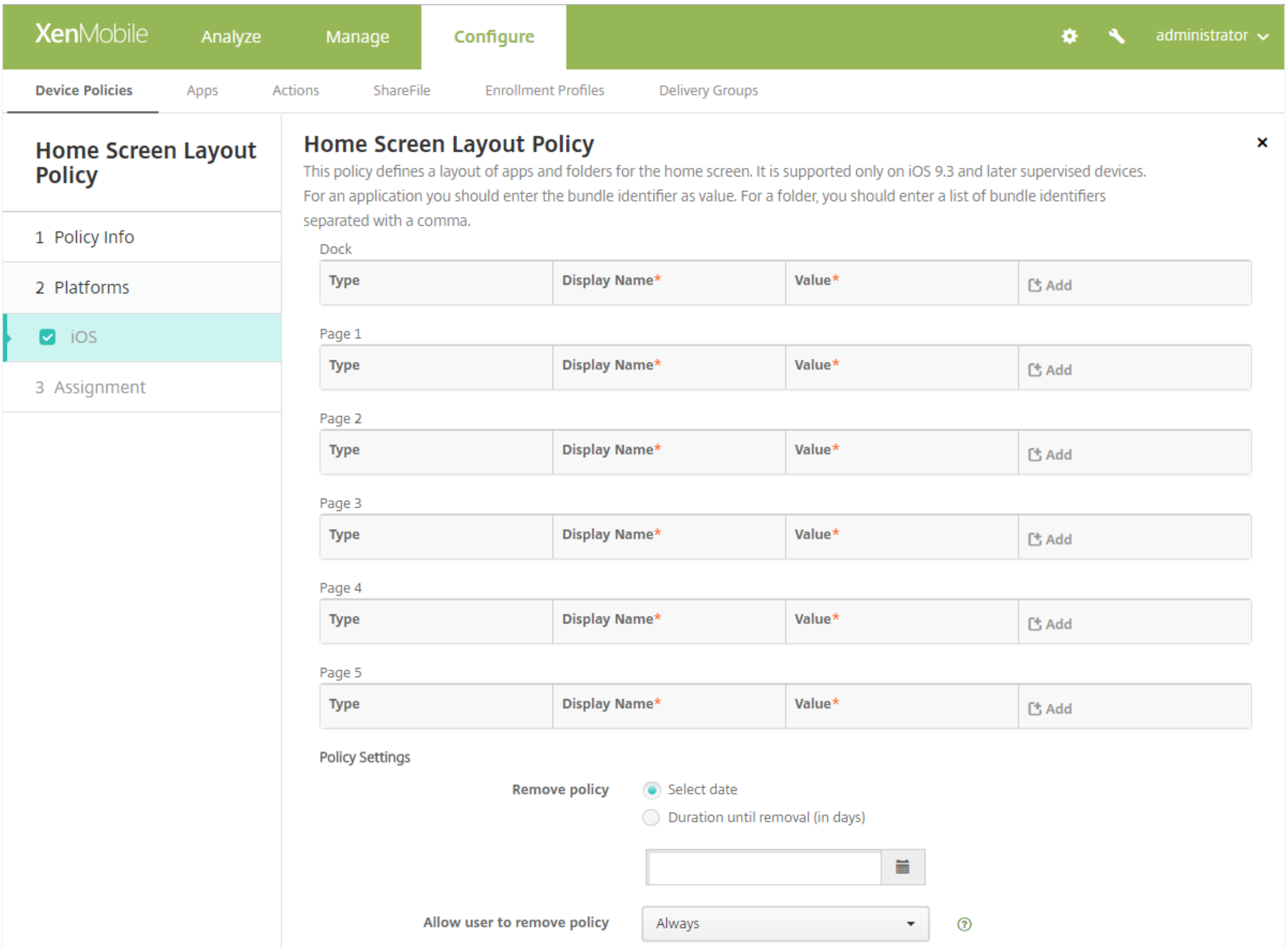
Enrollment URL to enter in Apple Configurator: https://example.domain.net:8443/zdm/ios/otae/dobulkenrollment

Require device registration before enrollment: NO

Require credentials for device enrollment: YES iOS 7.1+

iOS Home screen layout

Use the new Home Screen Layout device policy to specify the layout of apps and folders for the iOS Home screen. This policy is supported on iOS 9.3 and later supervised devices. To add the policy, go to **Configure > Device Policies**.



Home Screen Layout Policy

This policy defines a layout of apps and folders for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application you should enter the bundle identifier as value. For a folder, you should enter a list of bundle identifiers separated with a comma.

Dock

Type	Display Name*	Value*	Add

Page 1

Type	Display Name*	Value*	Add

Page 2

Type	Display Name*	Value*	Add

Page 3

Type	Display Name*	Value*	Add

Page 4

Type	Display Name*	Value*	Add

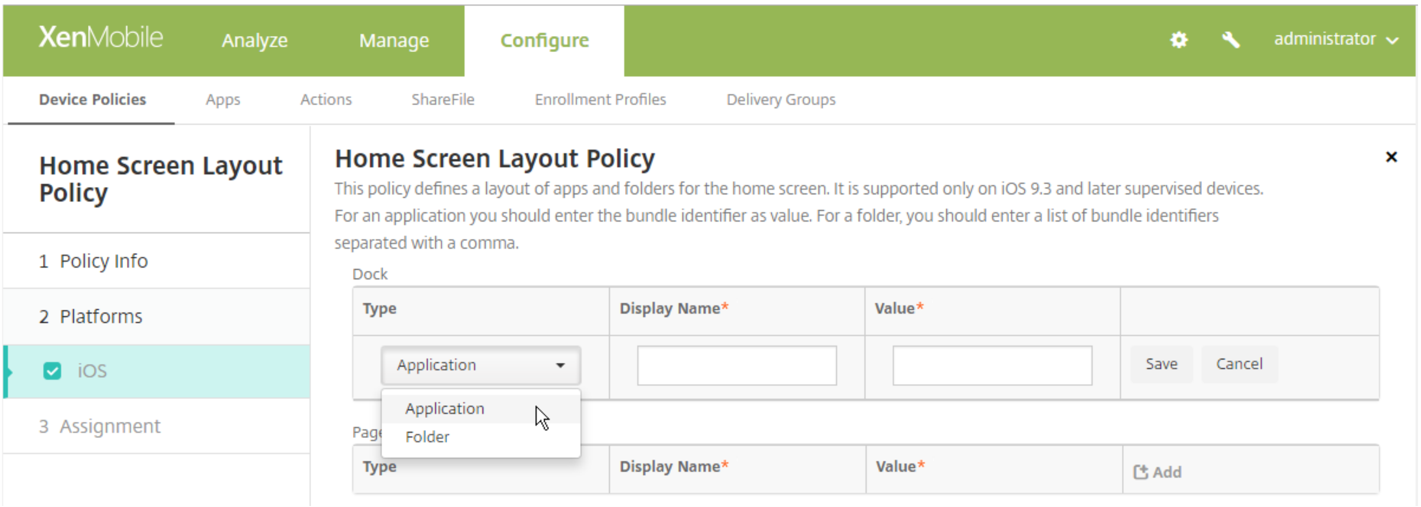
Page 5

Type	Display Name*	Value*	Add

Policy Settings

Remove policy: ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always



Home Screen Layout Policy

This policy defines a layout of apps and folders for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application you should enter the bundle identifier as value. For a folder, you should enter a list of bundle identifiers separated with a comma.

Dock

Type	Display Name*	Value*	
Application			Save Cancel

Page

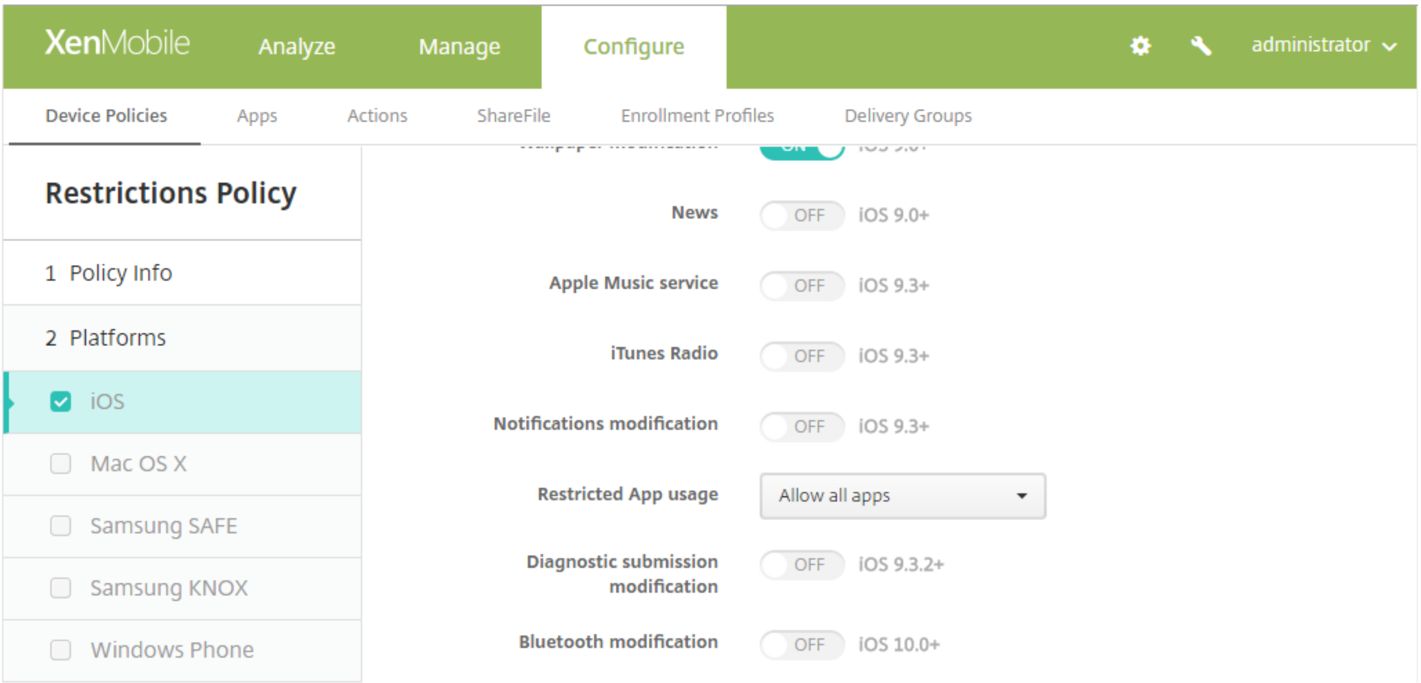
Type	Display Name*	Value*	Add

More feature restriction options for iOS devices

The Restrictions Policy for iOS now includes these additional restriction options:

- **News**: Allow users to use the News app (available in iOS 9.0 and later). Applies only to supervised devices.

- **Apple Music service**: Allow users to use the Apple Music service (available in iOS 9.3 and later). If you don't allow Apple Music service, the Music app runs in classic mode. Applies only to supervised devices.
- **iTunes Radio**: Allow users to use iTunes Radio (available in iOS 9.3 and later). Applies only to supervised devices.
- **Notifications modification**: Allow users to change notification settings (available in iOS 9.3 and later). Applies only to supervised devices.
- **Restricted App usage**: Allow users to use all apps or only the apps allowed or denied by bundle ID (available in iOS 9.3 and later). Applies only to supervised devices.
- **Diagnostic submission modification**: Allow users to change the diagnostic submission and app analytics settings in the Diagnostics & Usage pane in Settings (available in iOS 9.3.2 and later). Applies only to supervised devices.
- **Bluetooth modification**: Allow users to change Bluetooth settings (available in iOS 10.0 and later). Applies only to supervised devices.



Restrictions Policy

1 Policy Info

2 Platforms

☑ iOS

□ Mac OS X

□ Samsung SAFE

□ Samsung KNOX

□ Windows Phone

News OFF iOS 9.0+

Apple Music service OFF iOS 9.3+

iTunes Radio OFF iOS 9.3+

Notifications modification OFF iOS 9.3+

Restricted App usage Allow all apps

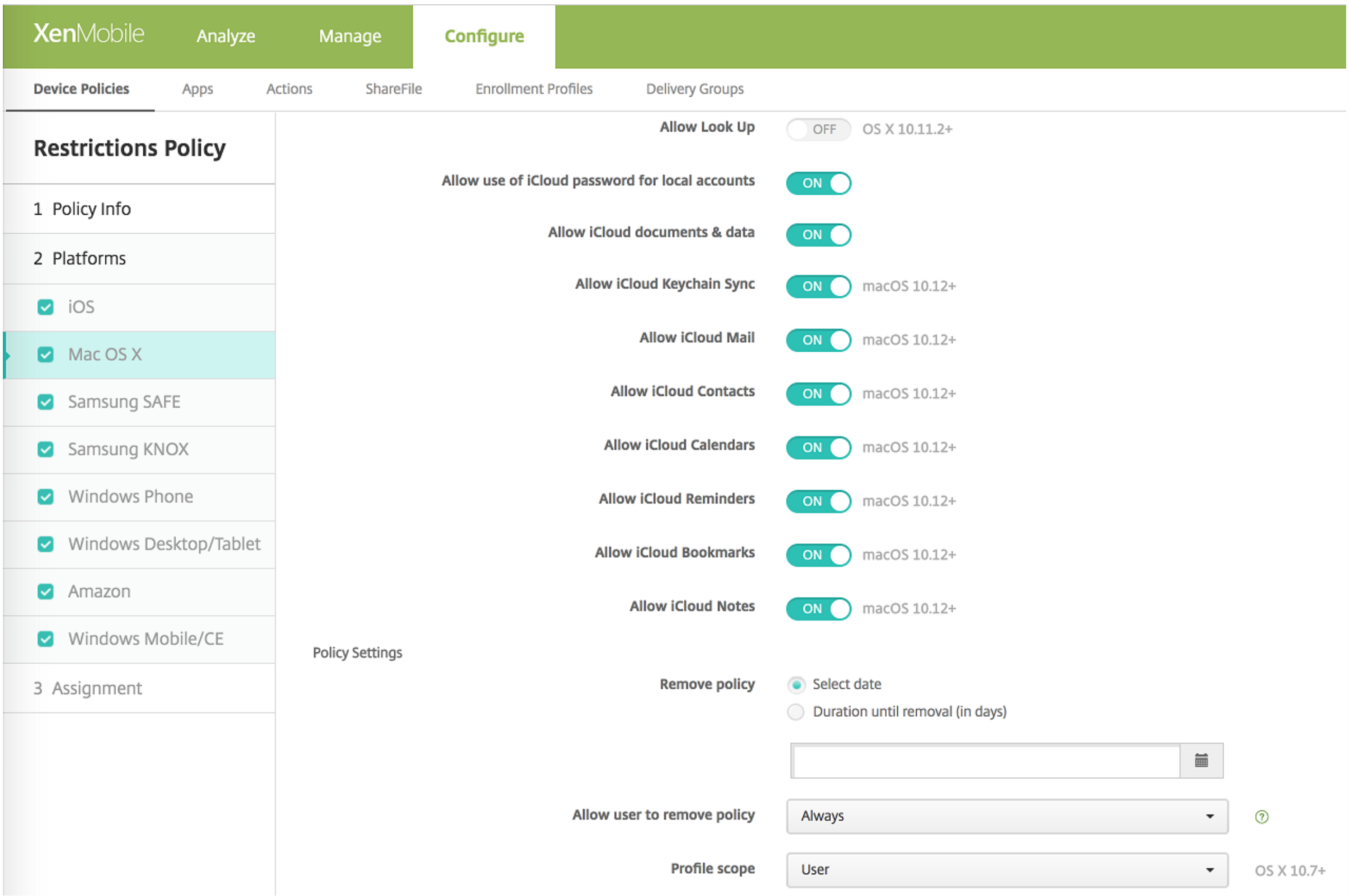
Diagnostic submission modification OFF iOS 9.3.2+

Bluetooth modification OFF iOS 10.0+

More feature restriction options for macOS devices

The Restrictions Policy has the following added restriction options for macOS 10.12 and later. By default, XenMobile allows these features.

- Allow Apple Music: If you don't allow Apple Music service, the Music app runs in classic mode. Applies only to supervised devices.
- Allow iCloud Keychain Sync
- Allow iCloud Mail
- Allow iCloud Contacts
- Allow iCloud Calendars
- Allow iCloud Reminders
- Allow iCloud Bookmarks
- Allow iCloud Notes



Allow Look Up: OFF — OS X 10.11.2+

Allow use of iCloud password for local accounts: ON

Allow iCloud documents & data: ON

Allow iCloud Keychain Sync: ON — macOS 10.12+

Allow iCloud Mail: ON — macOS 10.12+

Allow iCloud Contacts: ON — macOS 10.12+

Allow iCloud Calendars: ON — macOS 10.12+

Allow iCloud Reminders: ON — macOS 10.12+

Allow iCloud Bookmarks: ON — macOS 10.12+

Allow iCloud Notes: ON — macOS 10.12+

Policy Settings

Remove policy: ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always

Profile scope: User — OS X 10.7+

Support for iOS 9.3 Managed Lost Mode

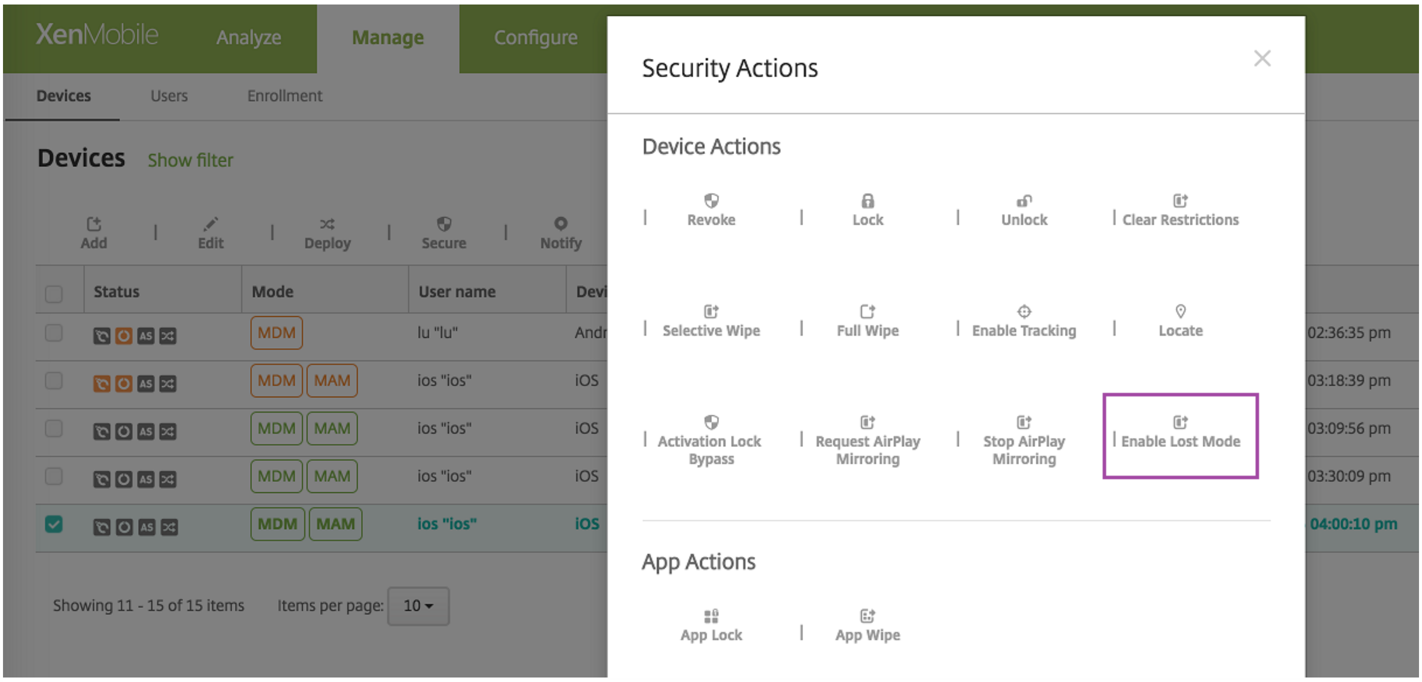
In iOS 9.3 or later, you can use Apple MDM to place a supervised device into Managed Lost Mode, a dedicated mode. You can use Managed Lost Mode to block or locate supervised devices that are lost or stolen.

XenMobile now has a Lost Mode device property. Unlike Apple Managed Lost Mode, XenMobile 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.

The XenMobile Lost Mode feature is similar to the XenMobile device lock feature. However, in XenMobile Lost Mode, only the XenMobile Server can unlock the device. By using device lock, users can unlock the device directly by using a PIN code provided by their administrator.

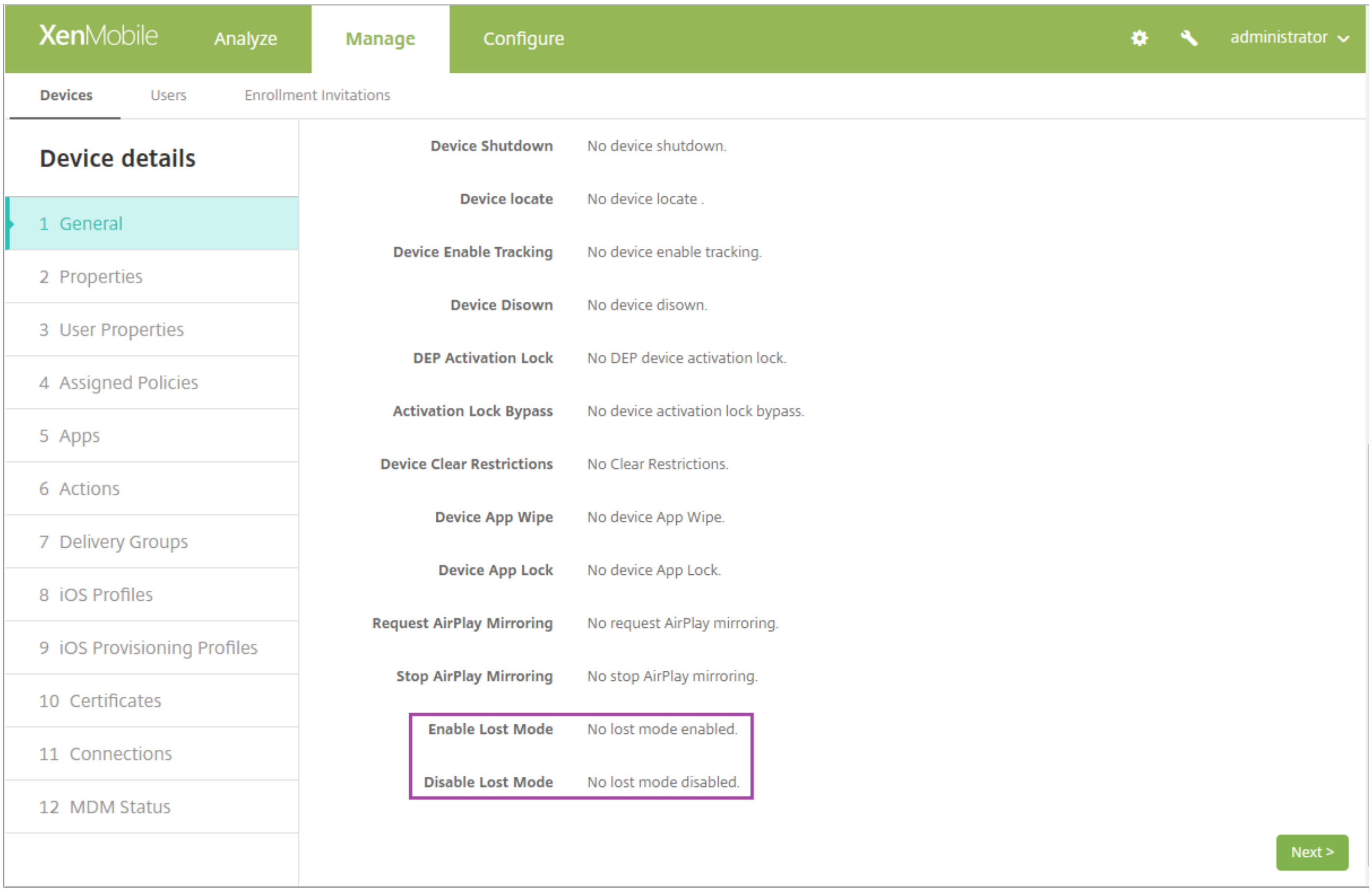
> ### Note
>
> In iOS 7 and later, you can also use iOS Device Lock to lock lost or stolen supervised or unsupervised devices remotely. Apple recommends that you avoid using iOS Device Lock for other purposes.

To enable or disable lost mode: Go to **Manage > Devices**, choose a supervised iOS device, and click **Secure**. Then, click **Enable Lost Mode** or **Disable Lost Mode**.



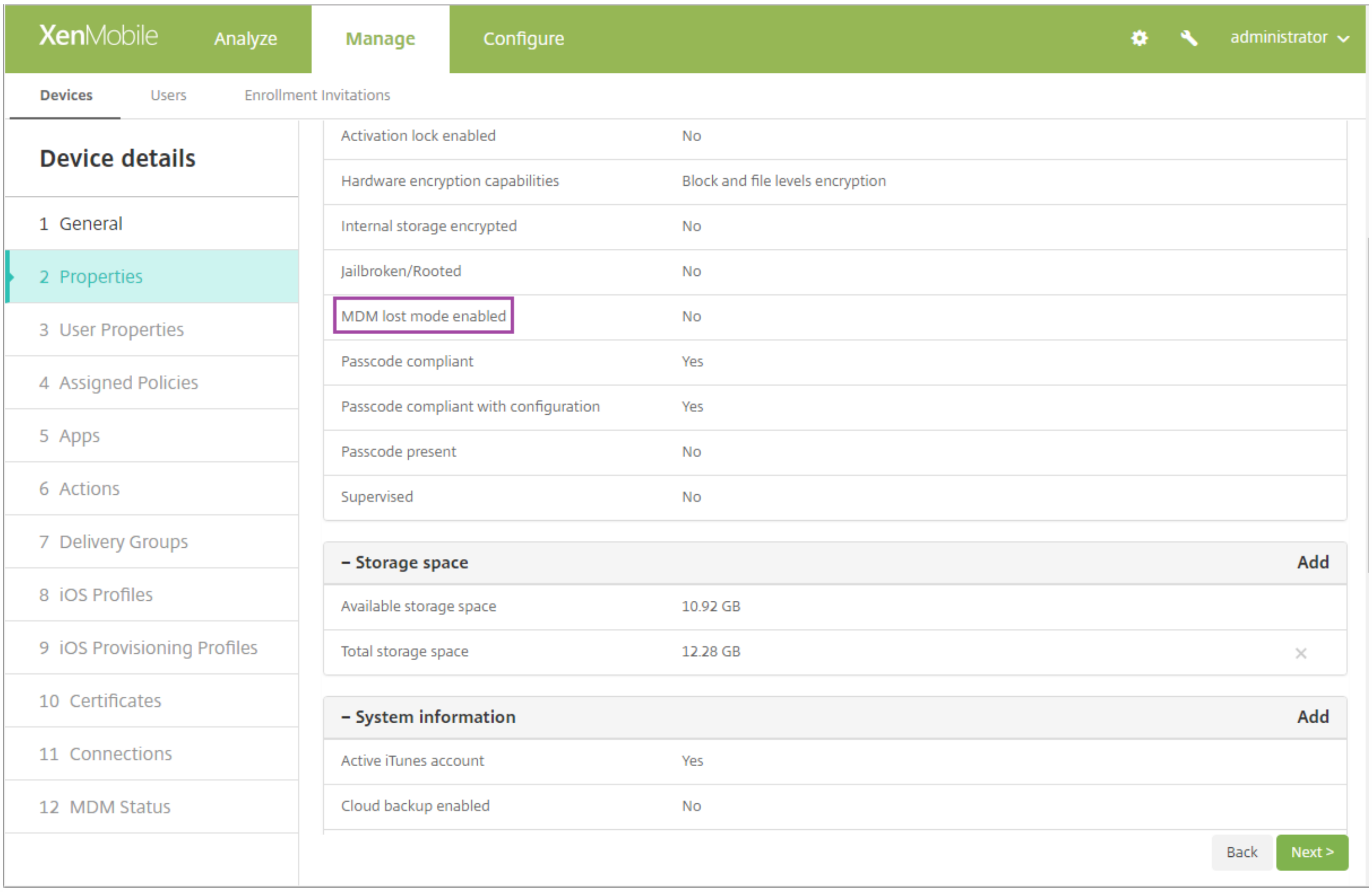
Use any of the following methods to check Lost Mode status:

- 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.



Device Shutdown	No device shutdown.
Device locate	No device locate .
Device Enable Tracking	No device enable tracking.
Device Disown	No device disown.
DEP Activation Lock	No DEP device activation lock.
Activation Lock Bypass	No device activation lock bypass.
Device Clear Restrictions	No Clear Restrictions.
Device App Wipe	No device App Wipe.
Device App Lock	No device App Lock.
Request AirPlay Mirroring	No request AirPlay mirroring.
Stop AirPlay Mirroring	No stop AirPlay mirroring.
Enable Lost Mode	No lost mode enabled.
Disable Lost Mode	No lost mode disabled.

- From **Manage > Devices**, on the **Properties** tab, verify the value of the setting **MDM lost mode enabled**.



Device details

Activation lock enabled	No
Hardware encryption capabilities	Block and file levels encryption
Internal storage encrypted	No
Jailbroken/Rooted	No
MDM lost mode enabled	No
Passcode compliant	Yes
Passcode compliant with configuration	Yes
Passcode present	No
Supervised	No

– Storage space

Available storage space	10.92 GB
Total storage space	12.28 GB

– System information

Active iTunes account	Yes
Cloud backup enabled	No

If you enable XenMobile Lost Mode on an iOS device, the XenMobile 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.

For iPads running iOS 7 and later: iOS appends the words "Lost iPad" to what you type in the **Message** box of the **Security Actions** dialog box. For iPhones running iOS 7 and later: If you leave the **Message** box empty and provide a phone number, Apple displays the message "Call owner" on the device lock screen.

SmartAccess for HDX apps

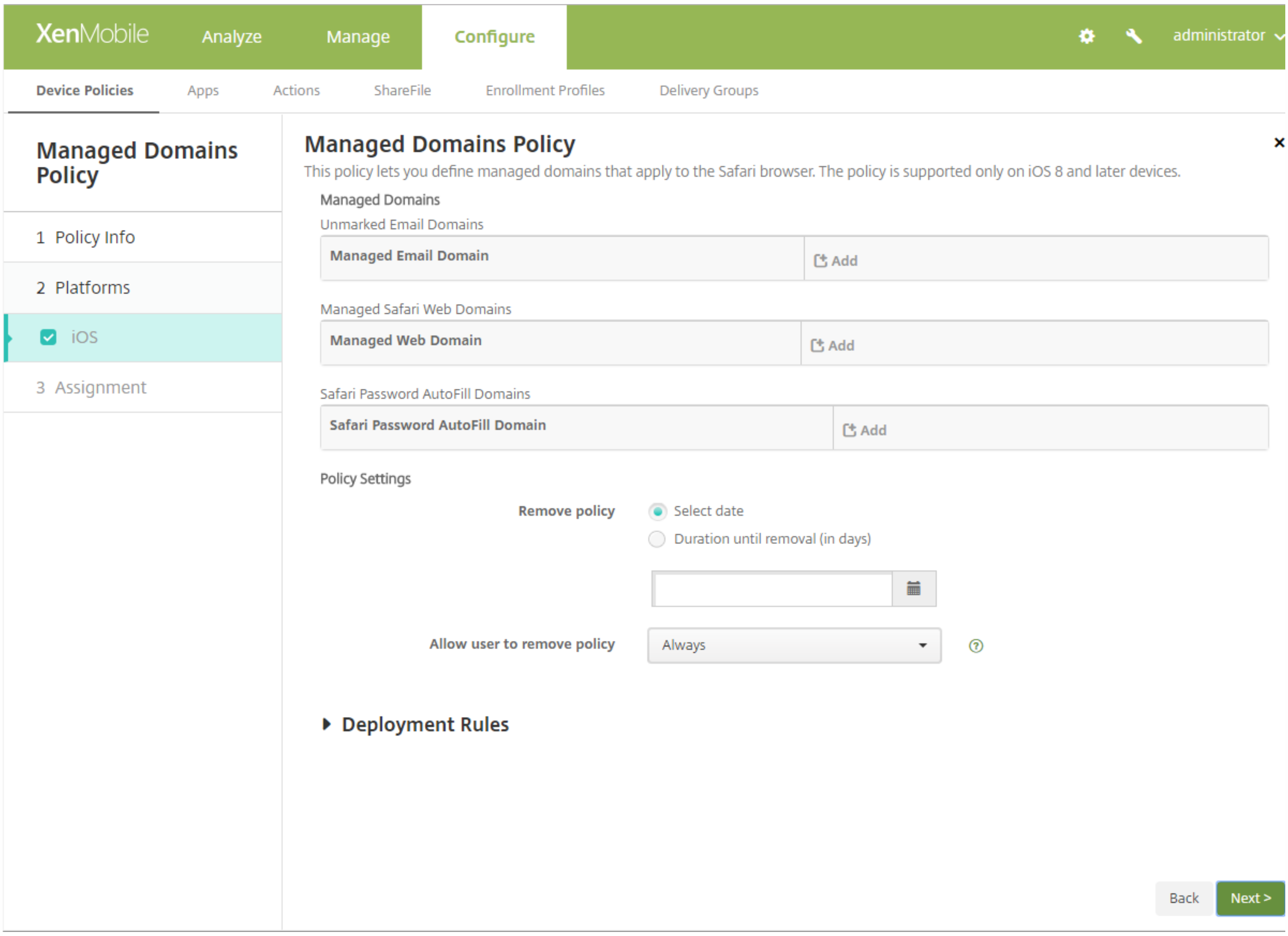
The SmartAccess feature allows you to control access to HDX apps based on device properties, user properties, or installed applications. You can control access by using automated actions to mark the device as out of compliance. To use SmartAccess, configure HDX apps in XenApp and XenDesktop with a SmartAccess policy that denies access to out-of-compliance devices. XenMobile communicates device status to StoreFront using a signed, encrypted tag. StoreFront allows or denies access based on the access control policy of the app.

Other improvements

- **More languages supported**. The XenMobile console is now available in Japanese. Secure Hub is now available in Arabic and Russian.
- **WiFi device policy**. The WiFi device policy now includes support for Windows 10, enabling you to use client certificate

authentication for your WiFi network. To update WiFi device policies, go to **Configure > Device Policies**.

- **Test Connection button added to the PKI Entities page**. When you add a Microsoft Certificate Services entity, you can test the connection to ensure that the server is reachable.
- **Improved stability** through database optimizations.
- **Last access time changes for MAM-only devices**. Previously, the device statistics for devices registered in MAM mode used the device registration time as the last access time. XenMobile now uses the most recent of the last online authentication or last activity for the last access time. The **Manage > Devices** page now includes the last access time.
- **Managed Domains policy now includes Safari password autofill domains**. For iOS 9.3 and later supervised devices, you can now specify the URLs from which users can save passwords in Safari. To do that, go to **Configure > Device Policies**. Then, add or open the **Managed Domains Policy**, and complete the settings under **Safari Password AutoFill Domain**.



Managed Domains Policy

This policy lets you define managed domains that apply to the Safari browser. The policy is supported only on iOS 8 and later devices.

Managed Domains

Unmarked Email Domains

Managed Email Domain

Managed Safari Web Domains

Managed Web Domain

Safari Password AutoFill Domains

Safari Password AutoFill Domain

Policy Settings

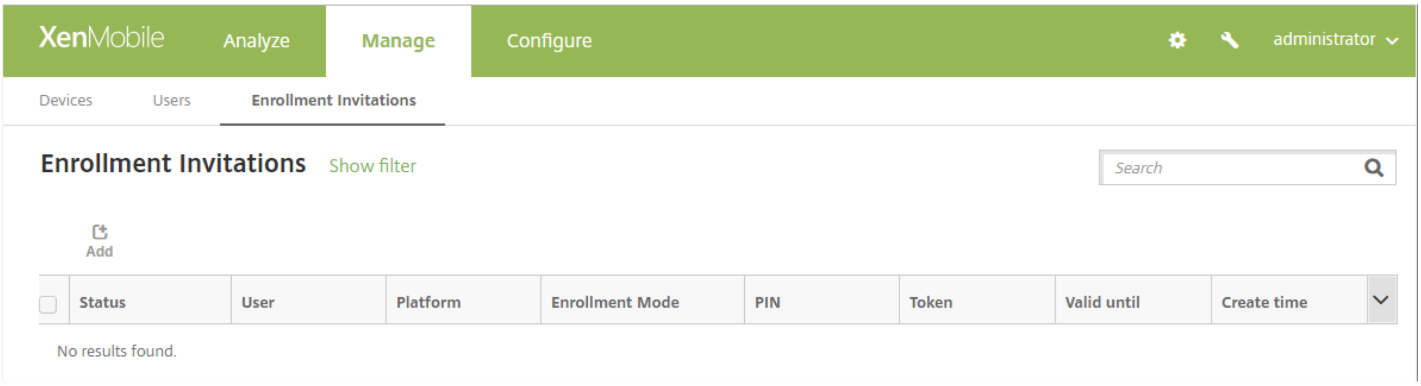
Remove policy: ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always

- **TLS 1.2 required for Secure Hub**. Apple now requires App Transport Security (ATS) for all apps submitted to the Apple App Store. ATS uses the Transport Layer Security (TLS) protocol version 1.2, which is now the required server protocol for Secure Hub.
- **Console interface improvements for managing enrollment invitations**. To clarify the terminology, the XenMobile console has the following improvements:
  - The page **Manage > Enrollments** changed to **Manage > Enrollment Invitations**.
  - The **Enrollment Status** column changed to **Status**. As before, that column contains enrollment invitation status, not

  enrollment status.

  - The terminology used when you manage an enrollment invitation now matches the terminology used when creating the invitation. We changed these labels:
    The **Type** column is now **Platform**.
    The **Mode** column is now **Enrollment Mode**.
    In the filter, the **Invitations Status** is now **Status**.
    In the filter, the **Invitations Mode** is now **Enrollment Mode**.
  - The value labels in the **Mode** column are now the same labels used when you create an invitation. For example, the **Mode** column now shows "User name" instead of "classic".



Enrollment Invitations

Status	User	Platform	Enrollment Mode	PIN	Token	Valid until	Create time

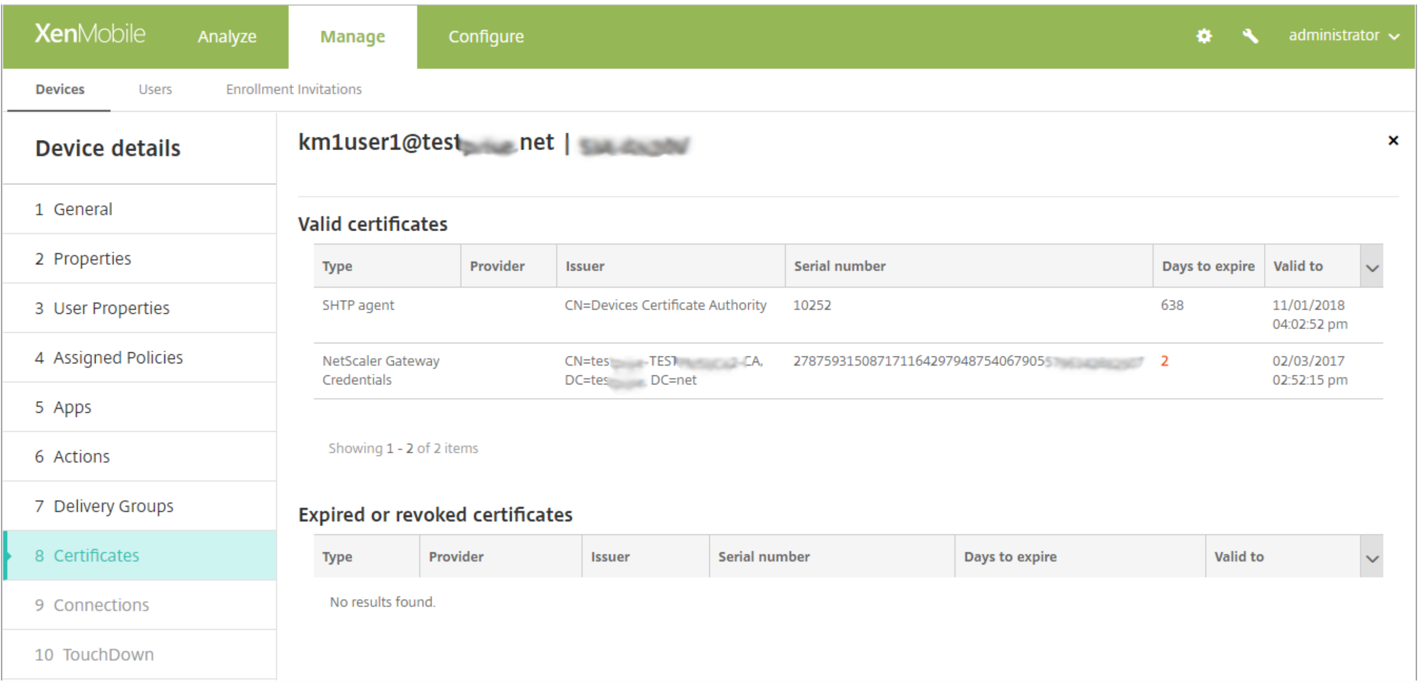
No results found.

- **New server property to set the VPP license baseline minimum interval**. XenMobile periodically reimports VPP licenses from Apple to ensure that the licenses reflect all changes. Such changes include when you manually delete an imported app from VPP. By default, XenMobile refreshes the VPP license baseline a minimum of every 720 minutes. You can now change the baseline interval through the new server property, **VPP baseline interval** (vpp.baseline).

  If you have more than 50,000 VPP licenses installed, Citrix recommends that you increase the baseline interval to reduce the frequency and overhead of importing licenses. If you expect frequent VPP license changes from Apple, Citrix recommends that you lower the value to keep XenMobile updated with the changes. The minimum interval between two baselines is 60 minutes.

  In addition, XenMobile performs a delta import every 60 minutes, to capture the changes since the last import. Setting the VPP baseline minimum interval to 60 minutes might delay the interval between baselines up to 119 minutes.

- The **Certificates** tab for **Manage > Devices** now includes the number of days before NetScaler Gateway certificates expire.



Device details

1 General
2 Properties
3 User Properties
4 Assigned Policies
5 Apps
6 Actions
7 Delivery Groups
8 Certificates
9 Connections
10 TouchDown

km1user1@test[redacted].net | [redacted]

Valid certificates

Type	Provider	Issuer	Serial number	Days to expire	Valid to
SHTP agent		CN=Devices Certificate Authority	10252	638	11/01/2018 04:02:52 pm
NetScaler Gateway Credentials		CN=tes[redacted]-TEST[redacted]-CA, DC=tes[redacted] DC=net	2787593150871711642979487540679055[redacted]	2	02/03/2017 02:52:15 pm

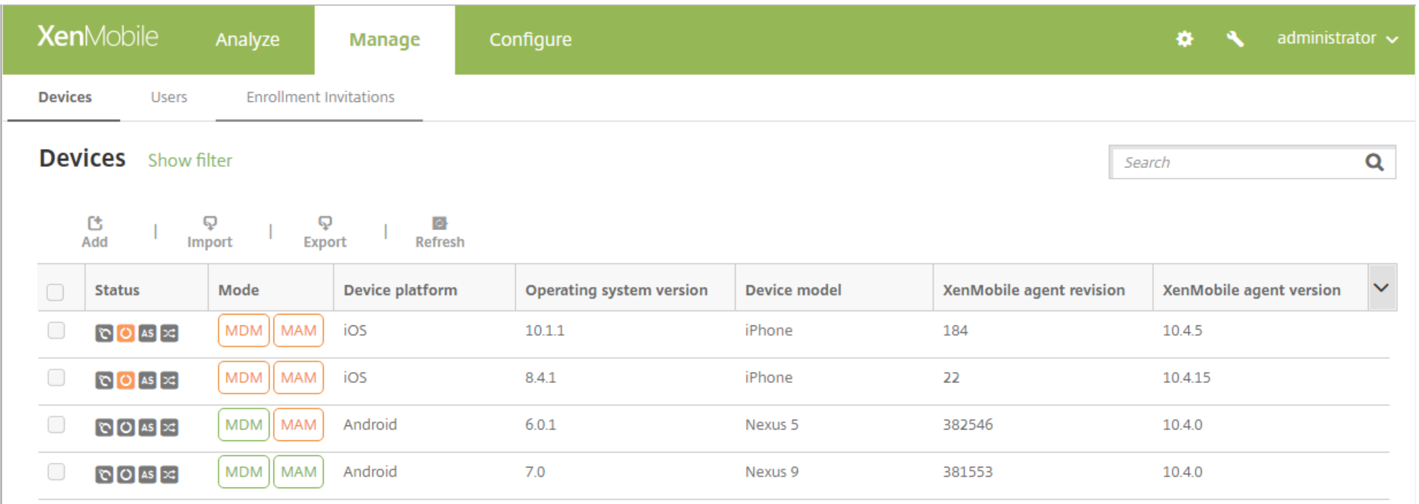
Showing 1 - 2 of 2 items

Expired or revoked certificates

Type	Provider	Issuer	Serial number	Days to expire	Valid to

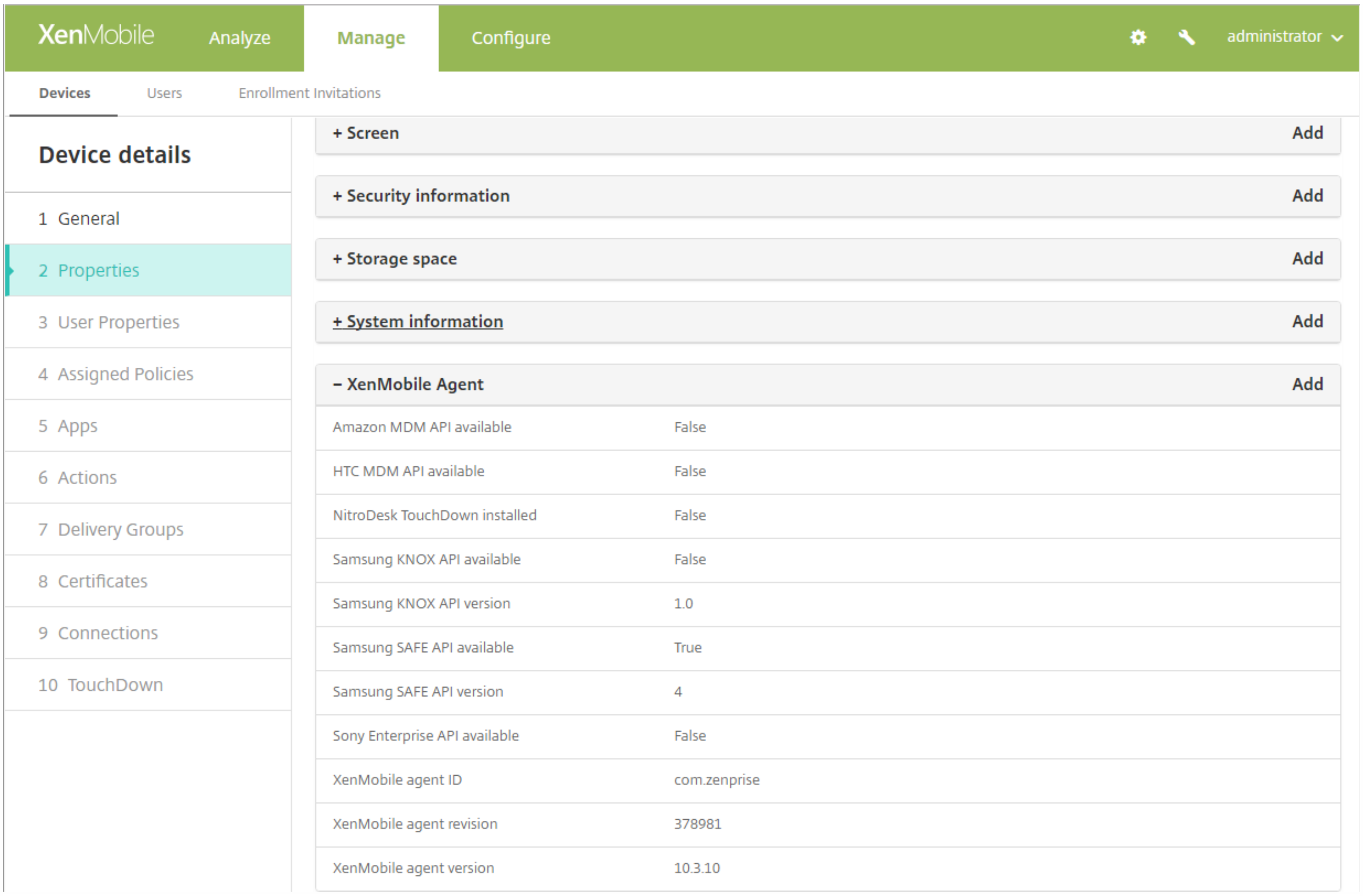
No results found.

- The **Manage > Devices** page and the **Properties** tab for devices now include the XenMobile agent revision and version numbers.



Devices

□	Status	Mode	Device platform	Operating system version	Device model	XenMobile agent revision	XenMobile agent version
□		MDM MAM	iOS	10.1.1	iPhone	184	10.4.5
□		MDM MAM	iOS	8.4.1	iPhone	22	10.4.15
□		MDM MAM	Android	6.0.1	Nexus 5	382546	10.4.0
□		MDM MAM	Android	7.0	Nexus 9	381553	10.4.0



Device details

1 General
2 Properties
3 User Properties
4 Assigned Policies
5 Apps
6 Actions
7 Delivery Groups
8 Certificates
9 Connections
10 TouchDown

+ Screen Add

+ Security information Add

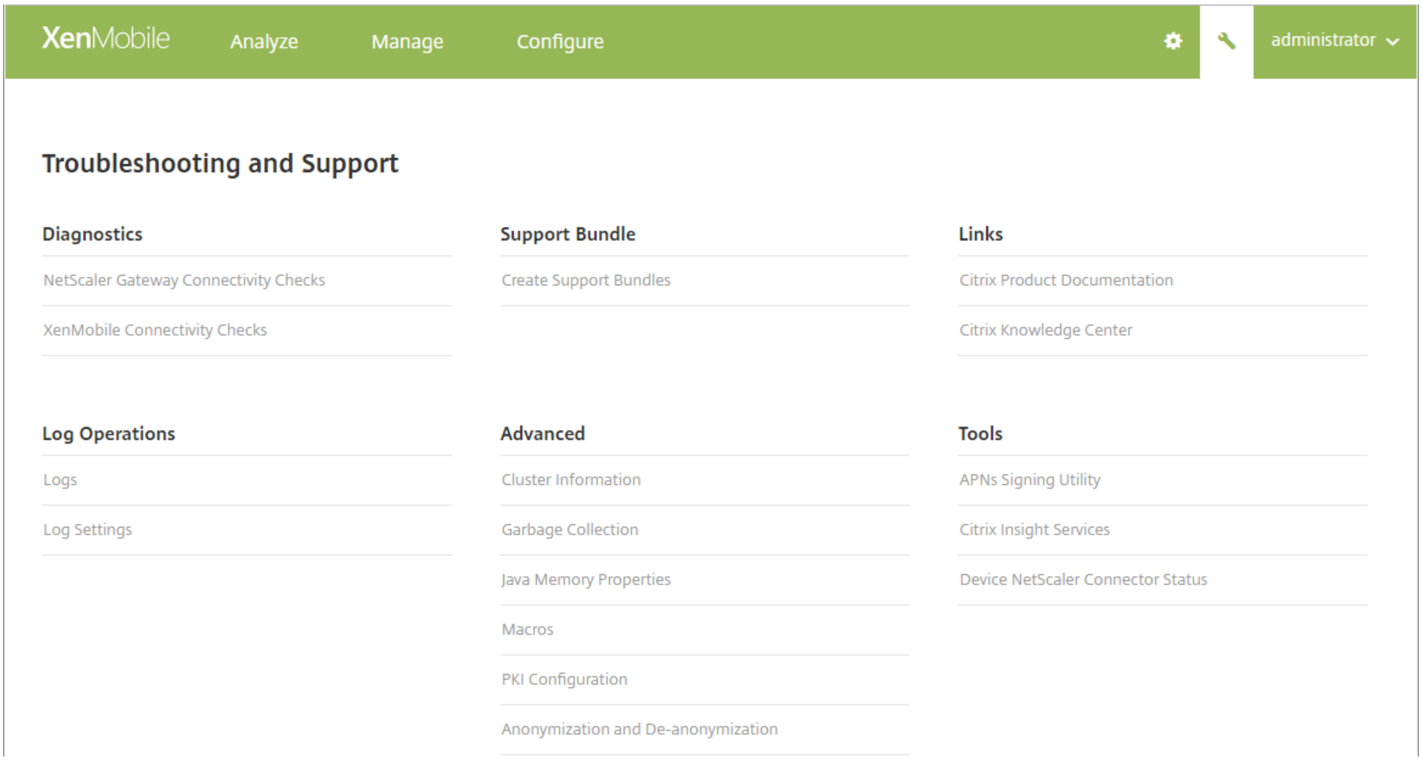
+ Storage space Add

+ System information Add

– XenMobile Agent Add

Amazon MDM API available	False
HTC MDM API available	False
NitroDesk TouchDown installed	False
Samsung KNOX API available	False
Samsung KNOX API version	1.0
Samsung SAFE API available	True
Samsung SAFE API version	4
Sony Enterprise API available	False
XenMobile agent ID	com.zenprise
XenMobile agent revision	378981
XenMobile agent version	10.3.10

- The **Troubleshooting and Support** page has been rearranged to improve usability.



Troubleshooting and Support

Diagnostics
- NetScaler Gateway Connectivity Checks
- XenMobile Connectivity Checks

Support Bundle
- Create Support Bundles

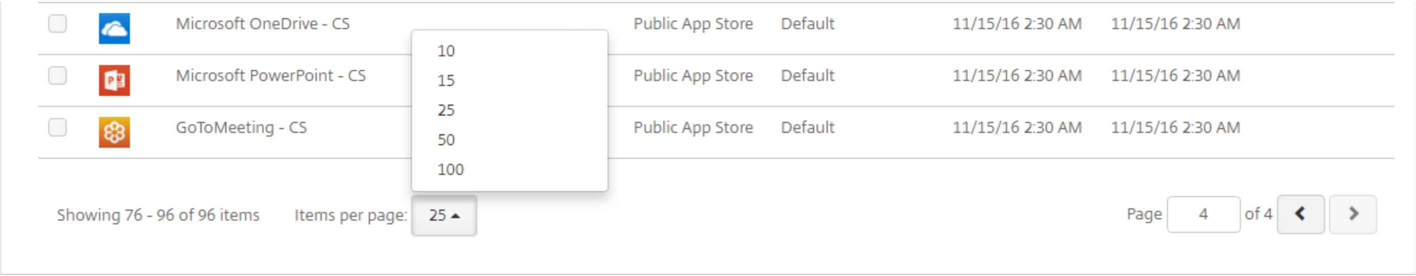
Links
- Citrix Product Documentation
- Citrix Knowledge Center

Log Operations
- Logs
- Log Settings

Advanced
- Cluster Information
- Garbage Collection
- Java Memory Properties
- Macros
- PKI Configuration
- Anonymization and De-anonymization

Tools
- APNs Signing Utility
- Citrix Insight Services
- Device NetScaler Connector Status

- **Log messages**. Log messages generated when a user can't be found now include the possible reasons. For example: Invalid credentials, LDAP configuration, or user missing from the LDAP domain or user base DN.
- **List pagination**. Lists on **Manage > Devices**, **Manage > Enrollment Invitations**, **Manage > Users**, **Configure > Device Policies**, **Configure > Apps**, **Configure > Actions**, **Configure > Enrollment Profiles**, and **Configure > Delivery Groups** are now paginated. You can choose the number of items to show on a page.



□	Microsoft OneDrive - CS		Public App Store	Default	11/15/16 2:30 AM	11/15/16 2:30 AM
□	Microsoft PowerPoint - CS		Public App Store	Default	11/15/16 2:30 AM	11/15/16 2:30 AM
□	GoToMeeting - CS		Public App Store	Default	11/15/16 2:30 AM	11/15/16 2:30 AM

Showing 76 - 96 of 96 items Items per page: 25 ▴ Page 4 of 4

- **New REST API parameter to support remove license servers.** The license REST API now has a new parameter, **serverPort**, to support remote license servers. For the full REST API reference, see this PDF. In addition, the documentation for the license API is updated. The documentation includes the license server and license notification response information for Save License Info. The documentation also includes other corrections.

- **Additions to the XenMobile Public API for REST Services.** The REST API now sends all device properties in a device call that uses a filter. The API wraps device properties in a JSON object and includes the properties as part of the response.

  The REST API now includes calls for ShareFile Enterprise, ShareFile StorageZones, and ShareFile StorageZone Connectors.

  For more information, see the XenMobile Public API for REST Services PDF.

Deprecated items

Windows 8.1 tablets are no longer supported. XenMobile Server no longer supports Windows 8.1 tablets.

Device policies for Windows 8.1 tablets are removed. The Sideloading key and Signing certificate device policies are deprecated.

Known issues in version 10.5

With NetScaler 12.0.41.16, when Secure Mail is configured with STA, mail sync fails on iOS and Android devices. The issue is fixed in NetScaler 12.0 build 41.22. For details and updates, see this Support Knowledge Center article. [#685075]

When you integrate StoreFront with XenMobile and deploy HDX apps, after you change an Active Directory password, the HDX apps disappear from the XenMobile Store. [CXM-9859]

After you upgrade to XenMobile 10.4.2, Android for Work apps don't appear on the device for a user in a nested Active Directory group. [CXM-19930]

An upgrade from XenMobile 10.3.6 to XenMobile 10.5 might change the device owner to "anonymous" for enrolled devices running Android for Work. [CXM-19933]

Users can renew certificates even if **Renew certificates when they expire** is **OFF** in your XenMobile configuration. [CXM-

20923]

For Active Directory users in a group with permissions for StorageZone Connectors: If you move users out of the group, ShareFile for iOS users can still access Network shares associated with those connectors. To work around this issue, reinstall the ShareFile for iOS app. [CXM-21859]

If you move a StorageZone Connector from delivery group A to B, ShareFile for iOS users in delivery group A can continue to use the connector. [CXM-21860]

If XenMobile uses self-signed certificates, users can't enroll iOS 10.3 devices into XenMobile. This limitation results from a change in iOS 10.3. To enroll devices running iOS 10.3 or later into XenMobile, you must use trusted SSL certificates in XenMobile. [CXM-24120]

When deploying apps, a prompt tells users to install the app if it is already installed on the device but has never been opened. As part of a fix for this issue, if an app is updated on the server, it is not updated on the user's device until they launch the app. [CXM-32193]

Upgrade Tool known issues

After you upgrade to XenMobile 10.4 from XenMobile 9, some policies for Windows devices appear in the XenMobile console, even after XenMobile deploys them. Specifically, the policies remain on the **Pending** tab of the **Assigned Policies** page of **Manage > Devices**. As a workaround, edit and then redeploy any policies shown as pending. That action clears the policies for Windows phones from the **Pending** tab. The Webclip policy for Windows tablets remains on the **Pending** tab although it works properly on the devices. [CXM-21769]

Fixed issues in version 10.5

XenMobile 10.5 includes the following fixed issues. Fixed issues for the Upgrade Tool appear in XenMobile Upgrade Tool in this article.

For iPhone6 devices, when users try to enroll devices using one-time password invitations that are bound to the device IMEI/MEID, the first profile installs successfully. The second MDM profile installation fails with the error message, "Profile Installation Fails. A connection to the server could not be established." On iPhone devices, the one-time password binds to the MEID number instead of the IMEI number. [#606162]

You cannot locate your Android ID by typing ***#*#8255#*#*** on your phone, as instructed on the **Settings > Google Play Credentials** page. Use a device ID app from the Google Play store to look up your device ID. [#633854]

After upgrading to XenMobile Server 10.4:

- If you open a **ShareFile** tab, the page might not load and the information does not appear.
- If you attempt to add or edit a delivery group, the following error message might appear: 500 Internal Server error. [663344, 663788, CXM-19085]

After using the MDX Toolkit to wrap an app that was developed using the Mowbly framework, the app navigation buttons no longer work. [#654962]

Accessing aggregated HDX apps in Secure Hub might fail with the error message, Failed to get application detail, please try again later. [#658058]

When Citrix Launcher is deployed to devices, apps don't appear under background tasks. [#680978]

If the web proxy JSON file for App Controller 9.0 includes an unescaped backslash character in the web proxy user name, XenMobile Server can't start. [CXM-13721]

In clustered XenMobile deployments managed by Hazelcast, a node in the cluster might intermittently fail to appear in the Hazelcast member list. [CXM-16537]

If you configure an IPsec VPN device policy, the group name and shared secret isn't saved and is missing on the device. [CXM-17002]

After an upgrade to 10.3.6, devices with multiple valid identities can't renew. If there are many renewal failures, XenMobile might crash repeatedly. [CXM-17358]

An issue might occur with an intermediate CA certificate used for client certificate authentication. The issue causes a network access error to appear on Android devices. [CXM-17401]

Issues might occur with SQL database configuration when updating XenMobile from version 10.3.5 to 10.3.6. [CXM-17565]

The on-premises version of XenMobile periodically synchronizes the license server with licenses that XenMobile checked out. The synchronization ensures that the count matches the number of devices and users. In this way, if XenMobile detects a mismatch, the issue is resolved within 24 hours. [CXM-18129]

The XenMobile console requires that you specify a password for the WiFi policy, although a password is optional. [CXM-18249]

XenMobile isn't deploying user profiles because the date format has the wrong format. [CXM-18250]

If using the XenMobile console with an Internet Explorer 11 browser, you cannot add or edit an LDAP configuration. [CXM-18324]

If you create an Exchange policy for all device types, and the policy includes a macro for the domain **$user.dnsroot**, the policy doesn't deploy. [CXM-18545]

If a delivery group name includes an ampersand (&), assigning a policy to that delivery group results in an error. [CXM-18768]

After configuring DEP settings for the first time in **Settings > iOS Bulk Enrollment**, this error appears when you click **Save**: Resources bag (container) with name 'Worx Home by Citrix' doesn't exist. To work around this issue, create a delivery group (**Configure > Delivery Groups**) after you configure the DEP settings and click **OK** on the error page. The delivery group must include the following:

- The user group named **Device Enrollment Program Group**
- The policy **DEP Software Inventory**
- The required app **Secure Hub by Citrix**

This issue doesn't affect existing enrollments if DEP was configured before Citrix Secure Hub appeared in the Apple Store on October 6, 2016. [CXM-19158]

For Enrollment Invitation or Enrollment PIN templates: If the message in a template includes certain macros, the message sent to users includes the macro instead of the user information. Those macros are enrollment URL (${enrollment.url}) and enrollment PIN (${enrollment.pin}). [CXM-19210]

Sometimes you can't upload an Enterprise app because XenMobile is unable to find the application icon although the icon is available. [CXM-19213]

In the **Settings > PKI Entities > Discretionary CA** page, you can view only the first page of CA certificates if there are multiple pages of certificates. [CXM-19736]

For a delivery group deployed to multiple devices: If you click a delivery group on **Configure > Delivery Groups**, and then click a button under **Deployment**, the **Manage > Devices** page shows an incorrect device list. [CXM-19737]

If a XenMobile App update is available in the iOS App Store or the Google Play Store: Prompts for app updates don't appear in the XenMobile Store after a user opens the app. [CXM-19927]

A XenMobile macro that includes $user.dnsroot does not resolve for domains where the parent and child domains are in a tree-root trust relationship. [CXM-20366]

If the sAMAccountName differs from the name portion of the UPN, macro resolution for the client property SEND_LDAP_ATTRIBUTES fails. For example: The sAMAccountName is **samplename** and the UPN is **sample@example.com**. [CXM-20414]

If XenMobile is in MDM mode and you're using DEP enrollment with user credentials supplied during the DEP phase: If a user removes Secure Hub from the device within a short interval after enrollment, the server gets into an inconsistent state. A short interval might be one hour. [CXM-20924]

A device doesn't automatically go into compliance after an automated action. [CXM-21006]

For RBAC administrators in a custom RBAC role that includes some user group restrictions: If Active Directory users in user groups have some devices enrolled, the **Manage > Devices** page opens slowly. [CXM-21007, CXM-21009]

After upgrading to XenMobile 10.3.6, administrators with custom RBAC role access can see enrolled devices from other domains even if the RBAC configuration restricts that access. [CXM-21008]

XenMobile cluster members might not respond to some HTTP requests, which prevents users from enrolling because of the **Company network not available** errors. [CXM-21010]

If the iOS bulk enrollment settings have **Require credentials for device enrollment** enabled, any type of invitation for a DEP enrollment causes XenMobile Server errors. The errors include error messages in Secure Hub, error messages in the XenMobile console, and loss of MDM functionality for all devices. To work around this issue, delete all enrollment invitations for the affected users on the **Manage > Enrollment** page. Then, restart the XenMobile Server. [CXM-21500]

Automatic actions that the XenMobile Lost Mode triggers fail for iOS devices configured with a passcode. This issue applies to all available actions triggered by Lost Mode: **App wipe**, **App lock**, **Mark the device as out of compliance**, and **Send notification**. [CXM-21579]

The Devices & Apps report generated from **Analyze > Reporting** shows an incorrect app install count for each device. [CXM-21773]

When you add the Skype for Business public app on XenMobile Console, the icon might not appear. However, you can search and add the app on the console and the app can be installed on the device. [CXM-21774, #668341]

Some Enterprise apps for Android don't upload to a XenMobile console configured in MDM or XME mode. [CXM-22377]

Deploying resources based on dynamic device properties, such as Current mobile country code, don't work. XenMobile ignores the rules and allows the resources (such as device policies, apps, and actions) to deploy on the device. [CXM-22565]

You can't create a support bundle by using the XenMobile CLI. As a workaround, use the XenMobile console: Go to **Support**

> Create Support Bundles and then click **Create**. [CXM-23091]

After an upgrade to XenMobile 10.3.6, Secure Hub no longer includes HDX apps. Logs include the entry, Unable to get the Config xml data Host name. [CXM-23177]

If you edit only the platform details for a device policy: The edits don't trigger a change to the **Last updated on** time on **Configure > Device Policies**. The last update time does change after you add or remove platforms. [CXM-23178]

If your browser language is set to French, you can't create or edit the WiFi device policy in the XenMobile console. [CXM-23180]

The **Manage > Devices** page shows iOS devices as inactive although the devices are active and communicating with XenMobile Server. This issue appears in logs as follows:

java.lang.IllegalStateException: Cannot load backing target entity: has been deleted. [CXM-23181]

If the server property **StorageZone Connectors supported value** is **NOT SUPPORTED** and you configure ShareFile: After you navigate to a different console page and then return to **Configure > ShareFile**, the **ShareFile** page doesn't show the configuration although the configuration is saved. To work around this issue, change the server property, **ShareFile configuration type**, to **ENTERPRISE**. [CXM-23337]

When a DEP device is deleted and then re-enrolled, the re-enrollment might fail with the error, Invalid profile. [CXM-24078]

This release contains a defense-in-depth measure for CVE-2016-5195, also known as Linux Dirty Cow.

Upgrade Tool fixed issues

If your deployment in XenMobile 9 includes a gpsstats.apk enterprise app, the upgrade to XenMobile 10.4 might fail. [CXM-17992]

After an upgrade from XenMobile 9 to XenMobile 10.4, Windows and iOS devices are in MDM mode instead of in MAM+MDM mode. In addition, the XenMobile Store does not open. As a workaround, users can reenroll a migrated device. [CXM-18532, CXM-23408]

After an upgrade from XenMobile 9 to XenMobile 10.4, XenMobile has duplicate, inactive MAM-only records from prior re-enrollments. That issue occurs even if XenMobile 9 required Device Manager enrollment. [CXM-18544]

During an upgrade from XenMobile 9.0 to XenMobile 10.4.x: The Upgrade tool doesn't update the device name in the device property table for devices that are enrolled in XME (MDM+MAM) mode. [CXM-20821]

If the App Controller database contains users in the data format **username**, an upgrade from XenMobile 9.0 to XenMobile 10.x fails. Instead, use the data format **domain\username** or **username@domain**. [CXM-21072]

If the case of the path to the .p12 server certificates differs for HTTP and HTTPS, an upgrade from XenMobile 9.0 to XenMobile 10.4.x fails. For example, if the HTTP path is Certificates\MDM.p12 and the HTTPS path is certificates\MDM.p12. [CXM-21581]

After an upgrade from XenMobile 9 to 10.x, XenMobile Store doesn't include apps. Also, XenMobile doesn't assign local groups to delivery groups. This issue occurs if a local user is part of a local group and the local user enrolls the device. [CXM-23375]

If Device Manager has two records for an Active Directory user and those records don't match as follows, an upgrade fails:

- The records have different UPNs. For example, one user record has a UPN of john.smith@eng.domain.com. The other record has john.smith@domain.com.
- The records have case differences in the sAMAccountName. For example, one user record has a sAMAccountName of johns. The other record has JOHNS. [CXM-23382]

After an upgrade from XenMobile 9 to XenMobile 10.x: You cannot edit in the upgraded XenMobile console a configuration policy that you customized in Device Manager by using the iPhone Configuration Utility or Apple Configurator. [CXM-23942]

XenMobile Server 10.5 documentation errata

The following items are errata found in the documentation since they were last published. Errata are content issues, such as errors or missing information, that could affect your use of XenMobile Server.

On page 49, under Port requirements, the following information should be included.

The following port must be open for devices and apps to communicate with XenMobile 10.x.

- **Port**: 30001
- **Description**: Management API for initial staging of HTTPS service
- **Source**: Internal LAN
- **Destination**: XenMobile Server

Fixed issues

Oct 06, 2017

XenMobile 10.7 includes the following fixed issues.

For fixed issues related to XenMobile Apps, see Fixed issues.

Delivery groups might show a pending deployment status even though the apps associated with the devices in those delivery groups are successfully installed. [#654162, CXM-21771]

After you update the obfuscated APK file for some Android apps in the XenMobile console, the older version appears in the details and the updated version doesn't deploy to devices. [CXM-25629]

When you create a Send Notification action that is set to repeat **0** times, iOS and Android users get spammed with notifications. [CXM-31790]

After an upgrade from XenMobile 10.4 to 10.5: When enrolling iOS and Android devices, MAM enrollment fails if LDAP is managed with Global Catalog and the client property SEND_LDAP_ATTRIBUTES is configured. MDM enrollment succeeds. [CXM-32408]

When you click **Export** on the **Manage > Users** page: If there are more than 10,000 users, the download takes a very long time. [CXM-32425]

If a VPN Connection name has a space, or other non-alphanumeric characters, XenMobile doesn't deploy the policy to devices. [CXM-32538]

After you enroll an iOS device in Secure Hub, XenApp or XenDesktop applications from a non-default category appear without an icon. If users click on such applications, the error message "Failed to get application details, please try again later" appears. [CXM-32575]

On the XenMobile **Settings > Google Play Credentials** page: After you type the settings and click **Save**, the message "Email or password incorrect" appears intermittently. This error is due to an update from Google. [CXM-32847]

On the Android platform page for the VPN device policy, for the Citrix VPN connection type: The following labels aren't translated in the German, Korean, and Simplified Chinese versions of the XenMobile console:

- Password and Certificate (an Authentication type option)
- Application List, App Package Name [CXM-33640]
- You might have intermittent difficulties accessing the XenMobile Server console because of high memory usage. [CXM-35069]

After saving edits to remove the Device Model property from an iOS device in **Manage > Devices** and then clicking **Export**, the "500 Internal Error"" message appears. [CXM-36495]

Over-the-air enrollment for iOS devices fails intermittently. The error message "Profile installation failed" appears. [CXM-37001]

The XenMobile REST API doesn't allow you to select multiple platforms when creating an enrollment invitation. [CXM-35853]

The Full Wipe security action fails on enrolled devices running macOS High Sierra (10.13 beta3) with the Apple File System

(APFS). [CXM-36397]

The enrollment URL link in an enrollment invitation might fail to resolve to the enrollment URL. To prevent this issue, ensure that the template you choose contains macros compatible with the platforms you selected when creating the enrollment invitation. Use these new macros when creating enrollment URL templates:

> ${enrollment.urls}, ${enrollment.ios.url}, ${enrollment.macos.url}, ${enrollment.android.url}, ${enrollment.ios.platform}, ${enrollment.macos.platform}, ${enrollment.android.platform}, and ${enrollment.agent}
>
> The older ${enrollment.url} still works for enrollment invitations that have only one platform selected. [CXM-37513]

After you use the XenMobile CLI to edit the proxy exclusion list and then restart the server, the list appears truncated in the CLI. This issue only affects the display of the list. [CXM-37812]

When you submit a macro on the **Troubleshooting and Support > Macros** page, the "Failed to get macro information" message appears. [CXM-37940]

Related information

> XenMobile Support Knowledge Center

Known issues

Feb 06, 2018

XenMobile 10.7 includes the following known issues.

For known issues related to XenMobile Apps, see Known issues.

Enrollment invitations to macOS devices refer to MACOSX instead of macOS. [CXM-32370]

Devices running iOS 11 might fail to enroll in Secure Hub when TLS 1.2 is not enabled in NetScaler, and when XenMobile is configured with either:

- LDAP and certificate authentication
- Certificate authentication
- Certificate authentication plus security token [CXM-33327]

After a user removes a book from the iBook app, the book doesn't reinstall automatically. To download the book again, press the download icon within iBooks. [CXM-34281]

On iOS 11, installed MDX apps begins to re-install when the next deployment happens. [CXM-34896]

If you send the Enable Lost Mode security action to a supervised iOS device without Secure Hub, the Locate button doesn't appear on the device. [CXM-36106]

RBAC administrators can assign the default admin role to new or existing users. Assigning the default admin role should be restricted to super admins. [CXM-37805]

For administrators who have only the PKI Entities and Credential Providers roles in RBAC: The administrator gets logged out of the XenMobile console while adding a PKI Entity or Credential Provider. To work around this issue, add the Certificates permission to the RBAC role of the administrator. [CXM-38713]

After upgrading to XenMobile Server 10.7 or later and enrolling a device: The license count shown in the XenMobile console is much greater than the actual number of enrolled devices. This issue is due to a third-party component. [CXM-40533]

Related information

> XenMobile Support Knowledge Center

Architecture

Nov 28, 2017

The XenMobile components in the XenMobile reference architecture you choose to deploy are based on the device or app management requirements of your organization. The components of XenMobile are modular and build on each other. For example, to give users in your organization remote access to mobile apps and to track user device types, you deploy XenMobile with NetScaler Gateway. XenMobile is where you manage apps and devices, and NetScaler Gateway enables users to connect to your network.

Deploying XenMobile components: You can deploy XenMobile to enable users to connect to resources in your internal network in the following ways:

- Connections to the internal network. If your users are remote, they can connect by using a VPN or micro VPN connection through NetScaler Gateway. That connection provides access to apps and desktops in the internal network.
- Device enrollment. Users can enroll mobile devices in XenMobile so you can manage the devices in the XenMobile console that connect to network resources.
- Web, SaaS, and mobile apps. Users can access their web, SaaS, and mobile apps from XenMobile through Secure Hub.
- Windows-based apps and virtual desktops. Users can connect with Citrix Receiver or a web browser to access Windows-based apps and virtual desktops from StoreFront or the Web Interface.

To achieve any of those capabilities for an on-premises XenMobile Server, Citrix recommends deploying XenMobile components in the following order:

- NetScaler Gateway. You can configure settings in NetScaler Gateway to enable communication with XenMobile, StoreFront, or the Web Interface by using the Quick Configuration wizard. Before using the Quick Configuration wizard in NetScaler Gateway, you must install one of the following components to set up communications: XenMobile, StoreFront, or the Web Interface.
- XenMobile. After you install XenMobile, you can configure policies and settings in the XenMobile console that allow users to enroll their mobile devices. You also can configure mobile, web, and SaaS apps. Mobile apps can include apps from the Apple App Store or Google Play. Users can also connect to mobile apps you wrap with the MDX Toolkit and upload to the console.
- MDX Toolkit. The MDX Toolkit can securely wrap mobile apps created within your organization or outside the company. After you wrap an app, you then use the XenMobile console to add the app to XenMobile and change the policy configuration as needed. You can also add app categories, apply workflows, and deploy apps to delivery groups. See About the MDX Toolkit.
- StoreFront (optional). You can provide access to Windows-based apps and virtual desktops from StoreFront through connections with Receiver.
- ShareFile Enterprise (optional). If you deploy ShareFile, you can enable enterprise directory integration through XenMobile, which acts as a Security Assertion Markup Language (SAML) identity provider. For more information about configuring identity providers for ShareFile, see the ShareFile support site.

XenMobile provides device management and app management through the XenMobile console. This section describes the reference architecture for the XenMobile deployment.

In a production environment, Citrix recommends deploying the XenMobile solution in a cluster configuration for both scalability and server redundancy. Also, using the NetScaler SSL Offload capability can further reduce the load on the XenMobile Server and increase throughput. For more information about how to set up clustering for XenMobile by configuring two load balancing virtual IP addresses on NetScaler, see Clustering.

For more information about configuring XenMobile for a disaster recovery deployment, see the Deployment Handbook Disaster Recovery article. That article includes an architecture diagram.

The following sections describe different reference architectures for the XenMobile deployment. For reference architecture diagrams, see the XenMobile Deployment Handbook articles, Reference Architecture for On-Premises Deployments and Reference Architecture for Cloud Deployments. For a complete list of ports, see Port requirements (on-premises) and Port requirements (cloud).

Mobile device management (MDM) mode

> ## Important
>
> If you configure MDM mode and later change to ENT mode, be sure to use the same (Active Directory) authentication. XenMobile doesn't support changing the authentication mode after user enrollment. For more information, see Upgrade from XenMobile 10 MDM Edition to Enterprise Edition.

XenMobile MDM Edition provides mobile device management. For platform support, see Supported device operating systems. If you plan to use only the MDM features of XenMobile, you deploy XenMobile in MDM mode. For example, if you want to do the following.

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

In the recommended model, the XenMobile Server is positioned in the DMZ with an optional NetScaler in front, which provides more protection for XenMobile.

Mobile app management (MAM) mode

MAM, also called MAM-only mode, provides mobile app management. For platform support, see Supported device operating systems. If you plan to use only the MAM features of XenMobile without having devices enroll for MDM, you deploy XenMobile in MAM mode. For example, if you want to do the following.

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

The devices cannot be MDM enrolled.

In this deployment model, XenMobile Server is positioned with NetScaler Gateway in front, which provides more protection for XenMobile.

MDM+MAM mode

Using MDM and MAM modes together provides mobile app and data management and mobile device management. For platform support, see Supported device operating systems. If you plan to use MDM+MAM features of XenMobile, you deploy XenMobile in ENT (enterprise) mode. For example, if you want to:

- 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

In the recommended deployment model, the XenMobile Server is positioned in the DMZ with NetScaler Gateway in front, which provides more protection for XenMobile.

XenMobile in the internal network - Another deployment option is to position an on-premises XenMobile Server in the internal network, rather than in the DMZ. This deployment is used if your security policy requires that only network appliances can be placed in the DMZ. In this deployment, the XenMobile Server is not in the DMZ. Therefore, there is no requirement to open ports on the internal firewall to allow access to SQL Server and PKI servers from the DMZ.

System requirements and compatibility

Dec 18, 2017

For more requirements and compatibility information, see the following articles:

- XenMobile compatibility
- Supported device operating systems
- Port requirements
- Scalability
- Licensing
- FIPS 140-2 compliance
- Language support

To run XenMobile 10.7, you need the following minimum system requirements:

- One of the following:
  - XenServer (supported versions: 6.5.x, 7.0, 7.1, 7.2); for details, see XenServer
  - VMware (supported versions: ESXi 5.5, ESXi 6.0, ESXi 6.5.0, or ESXi 6.5.0d); for details, see VMware
  - Hyper-V (supported versions: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016); for details, see Hyper-V
- Dual core processor
- Four virtual CPUs
- 8 GB of RAM for production environments; 4 GB of RAM for proof of concept and test environments
- 50 GB of disk space

XenMobile 10.7 requires Citrix License Server 11.12.1 or later.

NetScaler Gateway system requirements

To run NetScaler Gateway with XenMobile 10.7, you need the following minimum system requirements.

- NetScaler Gateway. Supported versions: 12.0, 11.1.x, 11.0.x, 10.5.x
- One of the following:
  - XenServer (supported versions: 6.5 or 7.0)
  - VMWare (supported versions: ESXi 4.1, ESXi 5.1, ESXi 5.5, ESXi 6.0)
  - Hyper-V (supported versions: Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2)
- Two virtual CPUs
- 2 GB of RAM
- 20 GB of disk space

You also must be able to communicate with Active Directory, which requires a service account. You only need query and read access.

XenMobile 10.7 Database Requirements

XenMobile requires one of the following databases:

- Microsoft SQL Server

The XenMobile repository supports a Microsoft SQL Server database running on one of the following supported versions. For more information about Microsoft SQL Server databases, see Microsoft SQL Server.

Microsoft SQL Server 2016
Microsoft SQL Server 2014
Microsoft SQL Server 2012
Microsoft SQL Server 2008 R2
Microsoft SQL Server 2008

XenMobile supports SQL Basic Availability Groups (Always On Availability Groups) and SQL Clustering for database high availability.

Citrix recommends using Microsoft SQL remotely.

Note: Ensure that the service account of the SQL Server to be used on XenMobile has the DBcreator role permission. For more information about SQL Server service accounts, see the following pages on the Microsoft Developer Network site. These links point to information for SQL Server 2014. If you are using a different version, choose your server version from the **Other Versions** list:

Server Configuration - Service Accounts

Configure Windows Service Accounts and Permissions

Server-Level Roles

- PostgreSQL (for test environments only). PostgreSQL is included with XenMobile. You can use it locally or remotely in test environments. Database migration is not supported. You can't move databases created in a test environment to a production environment.

  Note: All XenMobile editions support Remote PostgreSQL 9.5.2 and 9.3.11 for Windows with the following limitations: Support for up to 300 devices. Use on-premises SQL Server for more than 300 devices; No support for clustering.

StoreFront Compatibility

StoreFront 3.9
StoreFront 3.8
StoreFront 3.7
StoreFront 3.6
StoreFront 3.5
StoreFront 3.0
Web Interface 5.4
XenApp and XenDesktop 7.13
XenApp and XenDesktop 7.12
XenApp and XenDesktop 7.11
XenApp and XenDesktop 7.9
XenApp and XenDesktop 7.8
XenApp and XenDesktop 7.7
XenApp and XenDesktop Long Term Service Release (LTSR)
XenApp and XenDesktop 7.6
XenApp and XenDesktop 7.5

XenMobile compatibility

Feb 13, 2018

> ### Important
>
> Citrix ceased support of enterprise distribution for XenMobile productivity apps on December 31, 2017. For details, see the Citrix product matrix. Now, only public app store distribution is supported.
>
> The MDX Toolkit 10.7.10 is the final release that supports the wrapping of XenMobile Apps. Users access XenMobile Apps versions 10.7.5 and later from the public app stores. Users access ShareFile for XenMobile from the public app stores after version 6.5.

This article summarizes the versions of the supported XenMobile components that you can integrate. Those components include NetScaler Gateway and the version of the MDX Toolkit required to wrap, configure, and distribute apps.

Supported versions and upgrade paths

For the XenMobile Server and XenMobile Apps, Citrix supports the current and prior two versions of XenMobile. For example, if the current version is XenMobile Server 10.7, Citrix also supports versions 10.6 and 10.5. A version includes both releases and service packs. XenMobile 10.4, for example, was a service pack rather than a full release.

XenMobile 9. This version reached the End of Life (EOL) lifecycle status as of June 30, 2017. For more information about product lifecycle milestones, see the Product Matrix. Since the EOL date and for five years beyond the EOL date, you can download a PDF of the XenMobile 9 documentation from the Archive List of Legacy Documents. For more information about moving from XenMobile 9 XenMobile 10.x or to XenMobile Service via Citrix Cloud, see this Citrix.com page.

	Upgrade support statement	Latest version	Upgrade from
Public store apps (such as Secure Hub, Secure Mail, and Secure Web)	- Last two versions - Users who have automatic updates enabled receive the latest version from the app store. - The latest app supports the previous two MDX files.	- 10.7.30 (Secure Hub for Android) - 10.7.30 (Secure Hub for iOS) - 10.7.30 (Secure Mail for iOS) - 10.7.30 (Secure Mail for Android) - 10.7.30 (Secure Web for iOS) - 10.7.30 (Secure Web for Android)	- 10.7.25 or 10.7.20(Secure Hub) - 10.7.25 or 10.7.20 (Secure Mail) - 10.7.25 or 10.7.20 (Secure Web)
MDX	Previous version.	10.7.30	10.7.25
Server (on-premises)	All earlier 10.x versions and from XenMobile 9 with Rolling Patch 9	10.7	10.x, XenMobile 9 with Rolling Patch 9. For upgrade paths, see Upgrade.

XenMobile compatibility

To use new features, fixes, and policy updates, Citrix recommends that you install the most recent version of Secure Hub and XenMobile Apps.

Note: The MDX Toolkit 10.7.10 is the final release that supports the wrapping of XenMobile Apps. Users access XenMobile Apps versions 10.7.5 and later from the public app stores. Users access ShareFile for XenMobile from the public app stores after version 6.5.

- The latest version of the XenMobile Apps require the latest version of Secure Hub. The two previous versions of the apps are compatible with the latest Secure Hub.
- The latest versions of Secure Hub, MDX Toolkit, and XenMobile Apps are compatible with the latest version and the two prior versions of XenMobile Server.

Wrapping XenMobile Apps

The MDX Toolkit 10.7.10 is the final release that supports the wrapping of XenMobile Apps. Users access XenMobile Apps versions 10.7.5 and later from the public app stores.

The following table lists the final XenMobile App enterprise versions that you can wrap with the MDX Toolkit.

XenMobile App	Enterprise versions that you can wrap by using the MDX Toolkit 10.7.10
Secure Hub	10.0.3 and 10.0.0 available for Windows Phone
Secure Forms	10.7.0.13 available for iOS
Secure Mail	10.7.0 for iOS 10.6.20 for Android
Secure Notes	10.7.0 available for iOS 10.6.20 available for Android
Secure Tasks	10.7.0 available for iOS 10.6.20 available for Android
Secure Web	10.7.0 available for iOS 10.6.20 available for Android
QuickEdit	6.15 available for iOS 6.13 available for Android
ScanDirect	1.3.6 available for iOS
ShareConnect	3.5 available for iOS 3.5 available for Android
ShareFile	6.4 available for iOS 6.0 available for Android[1]

[1] It's possible that ShareFile might support an MDX Toolkit version following version 10.7.10.

Browser support

XenMobile 10.x supports the following browsers:

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

XenMobile 10.x is compatible with the most current version of the browser and one version before the current version.

Supported device operating systems

Jan 31, 2018

XenMobile supports devices running the following platforms and operating systems for enterprise mobility management, including app and device management. Because of platform restrictions and security features, XenMobile doesn't support all functionality on all platforms.

The supported device platform information in this article also applies to XenMobile Mail Manager and XenMobile NetScaler Connector.

> ### 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 XenMobile work on older platform releases. This article details what Citrix supports for each operating system. This article also includes device models that Citrix tested. For issues with other device models, contact Citrix support.

Android

With the release of Android O (version 8):

- Android 5 becomes the minimum version supported by XenMobile.
- Support ended for Android 4.4x as of the version 10.6.20 public app store release of XenMobile Apps.

XenMobile 10.x support for Android

Operating systems supported for all modes: Android 5.x, 6.x, 7.x, 8

Operating systems supported for MDM-only mode: Android 4.4, 5.x, 6.x, 7.x, 8

XenMobile 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.

Android devices and operating systems tested specifically on XenMobile 10.x in MDM+MAM (enterprise) mode

- Google Nexus 9 Tablet (operating system 7.0)
- Google Nexus 5 (operating system 6.0.1)
- Google Nexus 5X (operating system 7.1.1 and 8.0)
- Google Nexus 9 Tab (operating system 5.0.1)
- Google Nexus 9 Tab (operating system 5.1.1)
- Google Nexus 6P (operating system 7.1.1 and 8.0)
- Google Nexus 6 (operating systems 6.0.1 and 7.0)
- Google Nexus 5 (operating system 8.0)
- Google Pixel (operating system 7.0 and 8.0)
- Google Pixel C (operating system 8.0)
- Google Pixel XL (operating system 8.0)

- Google Pixel 2 (operating system 8.0)
- Google Pixel 2 XL (operating system 8.0)
- Galaxy S8 (operating system 7.1.1)
- Galaxy S7 (operating system 7.0)
- Galaxy S6 (operating system 6.0.1, 5.0)
- Galaxy Tab A (operating system 6.0)
- Galaxy Note3 model SM-N900 (operating system 5.0)
- Galaxy S6 Edge, SM-G925F (operating system 6.0.1)
- Galaxy S5 SM-G900F (operating system 6.0.1)
- Galaxy S5 SM-G900H (operating system 6.0.1)
- Huawei P10 Lite
- Huawei P10
- Huawei P8 Lite 2017
- Moto Turbo (operating system 6.0.1)
- OnePlus (operating systems 5, 6, 7, and 8)
- Sony Xperia, Model: SGP311 (operating system 5.0.1)
- Zebra (all models and operating systems)

Android devices and operating systems tested specifically on XenMobile 10.x in MDM-only mode

- Google Nexus 7 tablet (operating system 4.4.4)
- Google Nexus 9 tablet (operating system 7.0)
- Google Nexus 5 (operating system 6.0.1)
- Google Nexus 5X (operating system 7.1.1 and 8.0)
- Google Pixel (operating system 7.0 and 8.0)
- Google Pixel C (operating system 8.0)
- Google Pixel XL (operating system 8.0)
- Google Pixel 2 (operating system 8.0)
- Galaxy S7 (operating system 7.0)
- Galaxy S8 (operating system 7.1.1)
- Galaxy S6 (operating system 6.0.1, 5.0)
- Galaxy Tab A (operating system 6.0)
- Galaxy Note3 model SM-N900 (operating system 5.0)
- Galaxy S6 Edge, SM-G925F (operating system 6.0.1)
- Galaxy S5 SM-G900F (operating system 6.0.1)
- Galaxy S5 SM-G900H (operating system 6.0.1)
- Huawei Nexus 6 (operating systems 6.0.1 and 7.0)
- Huawei P10 Lite
- Huawei P10
- Huawei P8 Lite 2017
- Nexus 9 Tab (operating system 5.0.1)
- Nexus 9 Tab (operating system 5.1.1)
- Nexus 7 (operating system 4.4)
- Nexus 5 (operating system 8.0)
- OnePlus (operating systems 5, 6, 7, and 8)
- Sony Xperia, Model: SGP311 (operating system 5.0.1)
- Zebra (all models and operating systems)

In addition, the following device types are tested with Secure Mail.

Device type	Operating system
Google Pixel	7.0 and 8.0
Samsung S8	7.0
Samsung S7	7.0
Samsung S6	6.0.1
Samsung S5	5
Samsung Tab A	6.0.1
Google Pixel 2	8.0

SAFE and KNOX

On compatible Samsung devices, XenMobile 10.x supports and extends both Samsung for Enterprise (SAFE) and Samsung KNOX policies. XenMobile 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.

For HTC-specific policies, XenMobile supports HTC API version 0.5.0. For Sony-specific policies, XenMobile supports Sony Enterprise SDK 2.0.

iOS

With the release of iOS 11:

- XenMobile support for iOS 8 devices ended.
- XenMobile support for iOS 9 devices running XenMobile Apps ended October 31, 2017.
- XenMobile support continues for iOS 9 devices in MDM mode.
- Secure Hub no longer supports SHA-1 certificates on devices running iOS 11. To avoid related issues, users must update to Secure Hub 10.6.10 or later before upgrading their devices to iOS 11. For more information about anticipating this change, see the Knowledge Center article on XenMobile iOS 11 and Android O Support.

XenMobile 10.6 and 10.7 for iOS

- iOS 11.x
- iOS 10.x
- iOS 9.x (MDM only)

Some iOS devices that XenMobile 10.6 and 10.7 support:

- iPhone X
- iPhone 8, 8 Plus
- iPhone 7 Plus 10.2.1 (XenMobile 10.5 and later)
- iPhone 6, 6 Plus, 6S Plus, 6S+, 5s
- iPhone 5, 5c (iOS 9.x only)
- iPad 2, 3
- iPad Air, iPad Air-2, iPad Mini-4, Mini-3, Mini-2
- iPad Pro

macOS

XenMobile 10.7

- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra

XenMobile 10.6

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra

Windows Phone and Tablet

XenMobile 10.5, 10.6, and 10.7

- Windows 10 RS1, RS2, and RS3 Phone and Tablet
  - Not supported when XenMobile is in MAM-only mode.
- Windows Phone 10
- Windows Phone 8.1
  - For MDM mode only
- Windows Mobile/CE
  - Not supported if XenMobile is in MAM-only mode.

Symbian

XenMobile 10.6 and 10.7

The following list includes some of the Symbian devices that XenMobile 10.6 and 10.7 support.

- 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

BlackBerry

Management of BlackBerry devices is provided through XenMobile Mail Manager. For details, see Installing XenMobile Mail Manager.

Port requirements

Jan 29, 2018

To enable devices and apps to communicate with XenMobile, you open specific ports in your firewalls. The following tables list the ports that must be open. For port requirements for XenMobile Service, see Port requirements.

Open ports for NetScaler Gateway and XenMobile to manage apps

Open the following ports to allow user connections from Citrix Secure Hub, Citrix Receiver, and the NetScaler Gateway Plug-in through NetScaler Gateway to the following components:

- XenMobile
- StoreFront
- XenDesktop
- XenMobile NetScaler Connector
- Other internal network resources, such as intranet websites

To enable traffic to Launch Darkly from NetScaler, you can use the IP addresses noted in this Support Knowledge Center article.

For more information about NetScaler Gateway, see Configuration Settings for your XenMobile Environment in the NetScaler Gateway documentation. For more information about IP addresses owned by NetScaler, see How a NetScaler Communicates with Clients and Servers in the NetScaler documentation. That section includes information about NetScaler IP (NSIP) virtual server IP (VIP) and subnet IP (SNIP) addresses.

TCP port	Description	Source	Destination
21 or 22	Used to send support bundles to an FTP or SCP server.	XenMobile	FTP or SCP server
3 (TCP and UDP)	Used for DNS connections.	NetScaler Gateway XenMobile	DNS Server
80	NetScaler Gateway passes the VPN connection to the internal network resource through the second firewall. This situation typically occurs if users log on with the NetScaler Gateway Plug-in.	NetScaler Gateway	Intranet websites
80 or 8080 443	XML and Secure Ticket Authority (STA) port used for enumeration, ticketing, and authentication. Citrix recommends using port 443.	StoreFront and Web Interface XML network traffic NetScaler Gateway STA	XenDesktop or XenApp
123 (TCP	Used for Network Time Protocol (NTP) services.	NetScaler Gateway	NTP server

TCP port	Description	Source	Destination
389	Used for insecure LDAP connections	NetScaler Gateway XenMobile	LDAP authentication server or Microsoft Active Directory
443	Each item below corresponds to the same item in the right-hand columns. • Used for connections to StoreFront from Citrix Receiver or Receiver for Web to XenApp and XenDesktop. • Used for connections to XenMobile for web, mobile, and SaaS app delivery. • Used for general device communication to XenMobile Server • Used for connections from mobile devices to XenMobile for enrollment. • Used for connections from XenMobile to XenMobile NetScaler Connector. • Used for connections from XenMobile NetScaler Connector to XenMobile. • Used for Callback URL in deployments without certificate authentication.	• Internet • Internet • XenMobile • Internet • XenMobile • XenMobile NetScaler Connector • XenMobile	• NetScaler Gateway • NetScaler Gateway • XenMobile • XenMobile • XenMobile NetScaler Connector • XenMobile • NetScaler Gateway
514	Used for connections between XenMobile and a syslog server.	XenMobile	Syslog server
636	Used for secure LDAP connections.	NetScaler Gateway XenMobile	LDAP authentication server or Active Directory
1494	Used for ICA connections to Windows-based applications in the internal network. Citrix recommends keeping this port open.	NetScaler Gateway	XenApp or XenDesktop
1812	Used for RADIUS connections.	NetScaler Gateway	RADIUS authentication server
2598	Used for connections to Windows-based applications in the internal network using session reliability. Citrix recommends keeping this port open.	NetScaler Gateway	XenApp or XenDesktop
3268	Used for Microsoft Global Catalog insecure LDAP connections.	NetScaler Gateway XenMobile	LDAP authentication server or Active Directory
3269	Used for Microsoft Global Catalog secure LDAP connections.	NetScaler Gateway XenMobile	LDAP authentication server or Active Directory
9080	Used for HTTP traffic between NetScaler and the XenMobile NetScaler	NetScaler	XenMobile NetScaler

TCP port	Description	Source	Destination
30001	Management API for initial staging of HTTPS service	Internal LAN	XenMobile Server
9443	Used for HTTPS traffic between NetScaler and the XenMobile NetScaler Connector.	NetScaler	XenMobile NetScaler Connector
45000 80	Used for communication between two XenMobile VMs when deployed in a cluster. Port 80 is for internode communication and for SSL offload.	XenMobile	XenMobile
8443	Used for enrollment, XenMobile Store, and mobile app management (MAM).	• XenMobile • NetScaler Gateway • Devices • Internet	XenMobile
4443	• Used for accessing the XenMobile console by an administrator through the browser. • Used for downloading logs and support bundles for all XenMobile cluster nodes from one node.	• Access point (browser) • XenMobile	XenMobile
27000	Default port used for accessing the external Citrix License Server.	XenMobile	Citrix License Server
7279	Default port used for checking Citrix licenses in and out.	XenMobile	Citrix Vendor Daemon

Open XenMobile ports to manage devices

Open the following ports to allow XenMobile to communicate in your network.

TCP port	Description	Source	Destination
25	Default SMTP port for the XenMobile notification service. If your SMTP server uses a different port, ensure that your firewall does not block that port.	XenMobile	SMTP server
80 and 443	Enterprise App Store connection to Apple iTunes App Store (ax.itunes.apple.com), Google Play (must use 80), or Windows Phone Store. Used for publishing apps from the app stores through Citrix Mobile Self-Serve on iOS, Secure Hub for Android, or Secure Hub for Windows Phone.	XenMobile	• Apple iTunes App Store (ax.itunes.apple.com and *.mzstatic.com) • Apple Volume Purchase Program (vpp.itunes.apple.com) • For Windows Phone: login.live.com and *.notify.windows.com

(play.google.com)

TCP port	Description	Source	Destination
80 or 443	Used for outbound connections between XenMobile and Nexmo SMS Notification Relay.	XenMobile	Nexmo SMS Relay Server
389	Used for insecure LDAP connections.	XenMobile	LDAP authentication server or Active Directory
443	• Used for enrollment and agent setup for Android and Windows Mobile. • Used for enrollment and agent setup for Android and Windows devices, the XenMobile web console, and MDM Remote Support Client.	• Internet • Internet LAN and Wi-Fi	XenMobile
1433	Used by default for connections to a remote database server (optional).	XenMobile	SQL Server
2195	Used for Apple Push Notification service (APNs) outbound connections to gateway.push.apple.com for iOS device notifications and device policy push.	XenMobile	Internet (APNs hosts using the public IP address 17.0.0.0/8)
2196	Used for APNs outbound connections to feedback.push.apple.com for iOS device notification and device policy push.		
5223	Used for APNs outbound connections from iOS devices on Wi-Fi networks to *.push.apple.com.	iOS devices on Wi-Fi networks	Internet (APNs hosts using the public IP address 17.0.0.0/8)
8081	Used for app tunnels from the optional MDM Remote Support Client. Defaults to 8081.	Remote Support Client	XenMobile
8443	Used for enrollment of iOS and Windows Phone devices.	• Internet • LAN and Wi-Fi	

Port requirement for Auto Discovery Service connectivity

This port configuration ensures that Android devices connecting from Secure Hub for Android can access the Citrix Auto Discovery 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, do the following prerequisites:

- **Collect XenMobile 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 the environment in which the device is enrolling. For Secure Hub to enroll a device, the device must reach the ADS. Therefore, opening up 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:

FQDN	IP address	Port	IP and port usage
discovery.mdm.zenprise.com	52.5.138.94	443	Secure Hub - ADS Communication
discovery.mdm.zenprise.com	52.1.30.122	443	Secure Hub - ADS Communication
ads.xm.cloud.com*	34.194.83.188	443	Secure Hub - ADS Communication
ads.xm.cloud.com*	34.193.202.23	443	Secure Hub - ADS Communication

* SecureHub version 10.6.15 and later uses ads.xm.cloud.com.

Scalability and performance

Sep 06, 2017

Understanding the scale of your XenMobile infrastructure plays a significant role in how you decide to deploy and configure XenMobile. This article contains data from scalability tests and guidance on determining infrastructure requirements for performance and scalability for small- to large-scale, on-premises XenMobile enterprise deployments.

Scalability is defined here in terms of the ability of devices already enrolled in the deployment to reconnect to the deployment at the same time.

- *Scalability* is defined as the maximum number of devices enrolled in the deployment.
- *Login Rate* is defined maximum rate at which existing devices can reconnect to the deployment.

The data in this article are derived from testing on deployments ranging in size from 10,000 to 75,000 devices. The tests comprised mobile device using known workloads.

All testing was done on XenMobile Enterprise edition.

Testing was done using the NetScaler Gateway 8200. NetScaler appliance with similar or greater capacity can be expected to produce similar or greater scalability and performance.

This table summarizes the scalability test results:

Scalability	**Up to 75,000 devices**	
Login rate	Reconnection rate of existing users	Up to 9,375 devices per hour
Configuration	NetScaler Gateway	MPX 8200
	XenMobile Enterprise Edition	XenMobile Server 7-node cluster
	Database	Microsoft SQL Server external database

Test results by device population and hardware configuration

This table provides scalability test results for deployment device populations and hardware configurations tested.

Number of devices	12,500	30,000	60,000	75,000
Reconnection rate of	1,250	3,750	7,500	9,375

existing devices per hour				
XenMobile Server – mode	Standalone	Cluster	Cluster	Cluster
XenMobile Server – cluster	N/A	3	5	7

XenMobile Server – virtual appliance	Memory = 8 GB RAM
	vCPUs = 4
		Memory = 16 GB RAM
		vCPUs = 6
			Memory = 24 GB RAM
			vCPUs = 8
				Memory = 24 GB RAM
				vCPUs = 8

Active Directory	Memory = 4 GB RAM
	vCPUs = 2
		Memory = 8 GB RAM
		vCPUs = 4
			Memory = 16 GB RAM
			vCPUs = 4
				Memory = 16 GB RAM
				vCPUs = 4

Microsoft SQL Server external database	Memory = 8 GB RAM
	vCPUs = 4
		Memory = 16 GB RAM
		vCPUs = 8
			Memory = 24 GB RAM
			vCPUs = 16
				Memory = 24 GB RAM
				vCPUs = 16

Scalability profile

These tables summarize the test profile used derive the data in this article:

Active Directory Configuration	Profile used
Users	100,000
Groups	200,000
Levels of nesting	5

XenMobile Server Configuration	Total	Per user
Policies	20	20
Apps	270	50

Public app	200	0
MDX	50	30
Web and SaaS	20	20
Actions	50	
Delivery groups	20	
Active Directory groups per delivery group	10	

SQL	
Number of databases	1

Device connections and app activities

These scalability tests collected data on the ability of devices enrolled in a deployment to reconnect over an 8-hour period.

The tests simulated a reconnect interval during which reconnecting devices obtain all entitled security policies, subjecting XenMobile Server nodes to higher than normal load conditions. During subsequent reconnections, only changed or new policies are pushed to iOS devices, lessening the load on the XenMobile Server nodes.

These tests used a mix of 50 percent iOS devices and 50 percent Android devices.

These tests assume the reconnecting Android devices have received prior GCM notifications.

During the 8-hour test interval, the following app-related activities occurred:

- Secure Hub was opened once to enumerate entitled apps
- 2 SAML web apps were opened
- 4 MAM apps were downloaded
- 1 STA was generated for use by Secure Mail
- 240 STA ticket validations, one for each Secure Mail reconnect event over a micro-VPN, were performed.

Reference architecture

For the reference architecture for deployments used in these scalability tests, see "Core MAM+MDM Reference Architecture" in Reference Architecture for On-Premises Deployments.

Caveats and limitations

Note the following when considering the scalability test results in this article:

- Windows platform was not tested.
- Policy push was tested for iOS and Android devices.
- Each XenMobile Server node supports a maximum of 12,000 devices simultaneously.

Licensing

Sep 06, 2017

Licensing differs for XenMobile Service and XenMobile Server:

- Citrix Cloud Ops handles licensing for XenMobile Service.
- XenMobile Server and NetScaler Gateway require licenses.

  For more information about NetScaler Gateway licensing, see Licensing in the NetScaler Gateway documentation. XenMobile uses Citrix Licensing to manage licenses. For more information about Citrix Licensing, see The Citrix Licensing System.

  When you purchase XenMobile Server, you receive an order confirmation email message containing instructions for activating your licenses. New customers must register for a license program before placing an order. For more information about XenMobile licensing models and programs, see XenMobile licensing.

For a data sheet that shows which XenMobile features are available in each XenMobile edition, see this PDF.

You must install Citrix Licensing before downloading your XenMobile licenses. The name of the server on which you installed Citrix Licensing is required to generate the license file. When you install XenMobile, Citrix Licensing is installed on the server by default. Alternatively, you can use an existing Citrix Licensing deployment to manage your XenMobile licenses. For more information about installing, deploying, and managing Citrix Licensing, see Licensing Your Product.

> ## Note
>
> The latest version of XenMobile requires the 11.12.1 Citrix License Server or later. Older license server versions do not work with the latest version of XenMobile.

> ## Important
>
> If you intend to cluster nodes, or instances, of XenMobile, you must use Citrix Licensing on a remote server.

Citrix recommends that you retain local copies of all license files you receive. When you save a back-up copy of the configuration file, all license files are included in the backup. If, however, you reinstall XenMobile without first backing up the configuration file, you need the original license files.

XenMobile licensing considerations

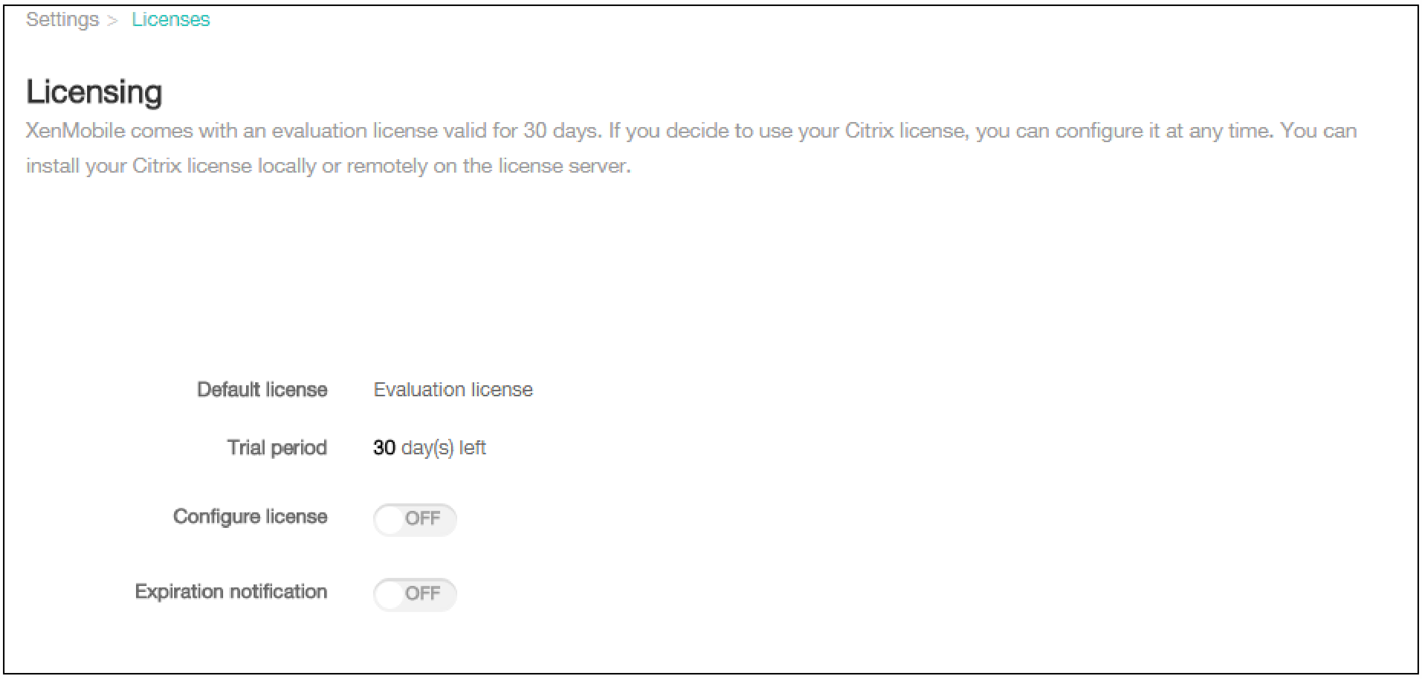
In the absence of a license, XenMobile operates fully featured in trial mode for a grace period of 30 days. This trial mode can be used only one time, with the 30-day period beginning when you install XenMobile. Access to the XenMobile web console is never blocked, regardless of whether a valid XenMobile license is available. In the XenMobile console, you can see how many days are left in your trial period.

Although XenMobile allows you to upload multiple licenses, only one license can be activated at a time.

When a XenMobile license expires, you can no longer perform any device management functions. For example, new users or devices cannot be enrolled, and apps and configurations deployed to enrolled devices cannot be updated. For more information about XenMobile licensing models and programs, see XenMobile licensing.

To find the Licensing page on the XenMobile console

When the **Licensing** page first appears after you install XenMobile, the license is set for the default 30-day trial mode and is not yet configured. You can add and configure licenses on this page.



Settings > Licenses

Licensing

XenMobile comes with an evaluation license valid for 30 days. If you decide to use your Citrix license, you can configure it at any time. You can install your Citrix license locally or remotely on the license server.

Default license Evaluation license

Trial period 30 day(s) left

Configure license OFF

Expiration notification OFF

1. On the XenMobile console, click the gear icon in the upper right-hand corner. The **Settings** page appears.

2. Click **Licensing**. The **Licensing** page appears.

To add a local license

When adding new licenses, they appear in the table. The first license added is automatically activated. If you add multiple licenses of the same category, such as Enterprise and type, these licenses appear in a single row of the table. In these cases, the **Total number of licenses** and **Number used** reflect the combined amount for the common licenses. The **Expires on** date shows the latest expiration date among the common licenses.

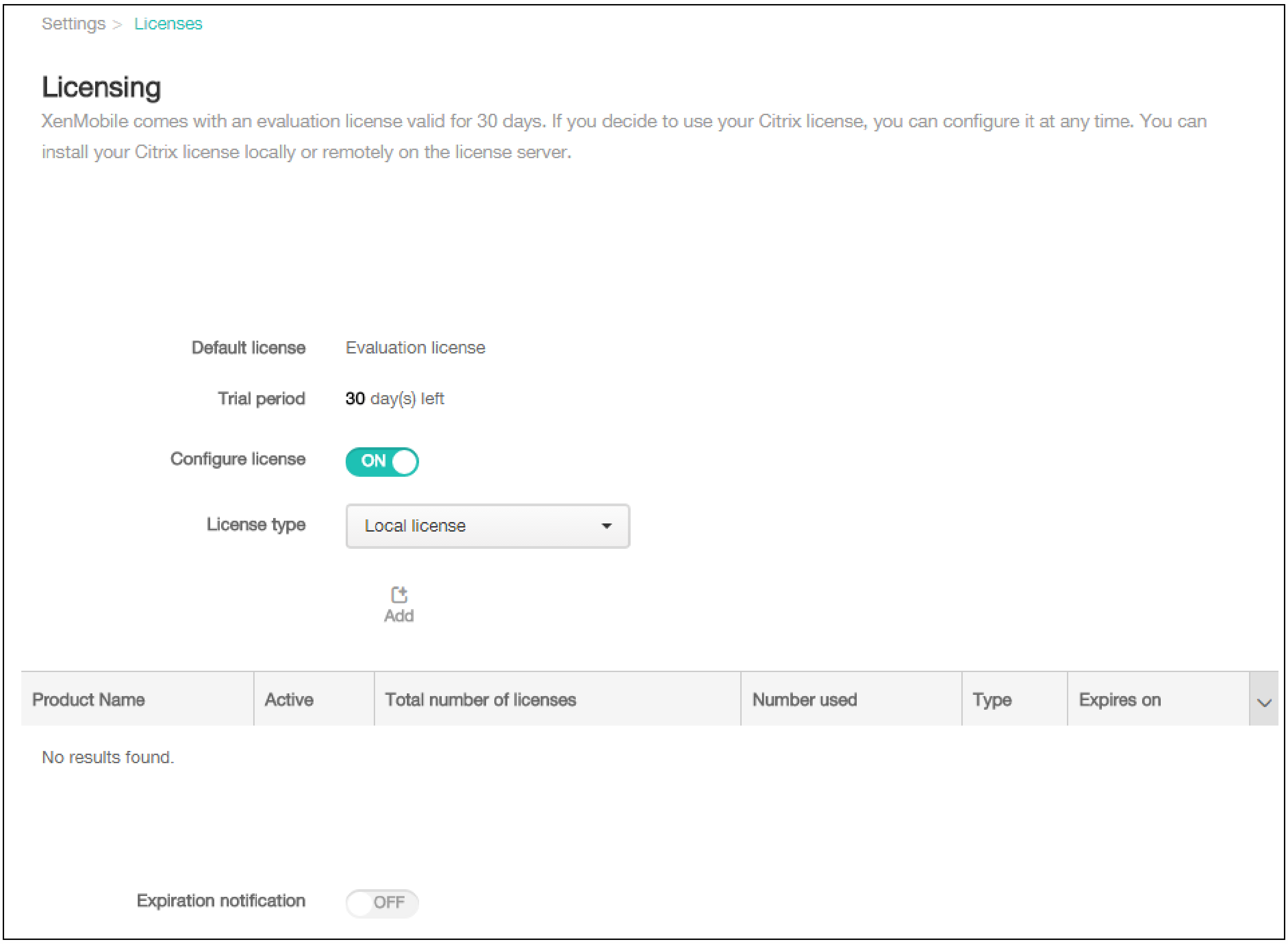
You manage all local licenses through the XenMobile console.

1. Get a license file from the Simple License Service, through the License Administration Console, or directly from your account on Citrix.com. For details, see Obtain your license files.

2. On the XenMobile console, click the gear icon in the upper right-hand corner. The **Settings** page appears.

3. Click **Licensing**. The **Licensing** page appears.

4. Set **Configure license** to **On**. The **License type** list, the **Add** button, and the **Licensing** table appear. The **Licensing** table contains licenses you have used with XenMobile. If you have not added a Citrix license yet, the table is empty.



Settings > Licenses

Licensing

XenMobile comes with an evaluation license valid for 30 days. If you decide to use your Citrix license, you can configure it at any time. You can install your Citrix license locally or remotely on the license server.

Default license Evaluation license

Trial period 30 day(s) left

Configure license ON

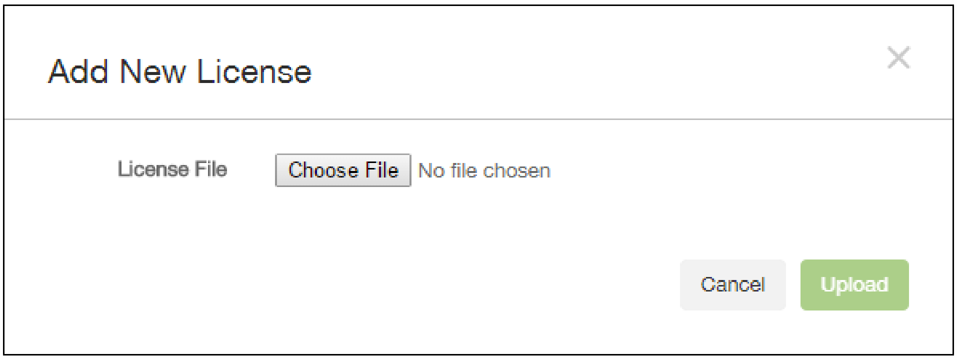
License type Local license

Product Name	Active	Total number of licenses	Number used	Type	Expires on

No results found.

Expiration notification OFF

5. Ensure that **License type** is set to **Local license** and then click **Add**. The **Add New License** dialog box appears.

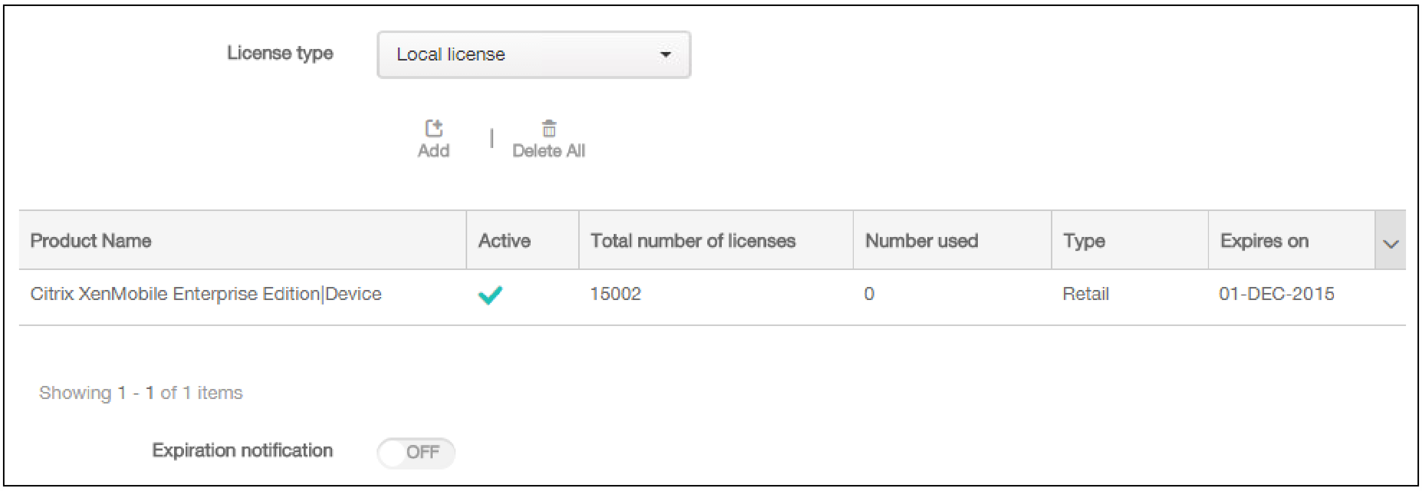


Add New License

License File Choose File No file chosen

6. In the **Add New License** dialog box, click **Choose File** and then browse to your license file location.

7. Click **Upload**. The license is uploaded locally and appears in the table.



License type: Local license

Product Name	Active	Total number of licenses	Number used	Type	Expires on
Citrix XenMobile Enterprise Edition|Device	✓	15002	0	Retail	01-DEC-2015

Showing 1 - 1 of 1 items

Expiration notification: OFF

8. When the license appears in the table on the **Licensing** page, activate it. If the license is first in the table, the license is activated automatically.

To add a remote license

If you are using the remote Citrix Licensing server, you use the Citrix Licensing server to manage *all* licensing activity. For details, see Licensing Your Product.

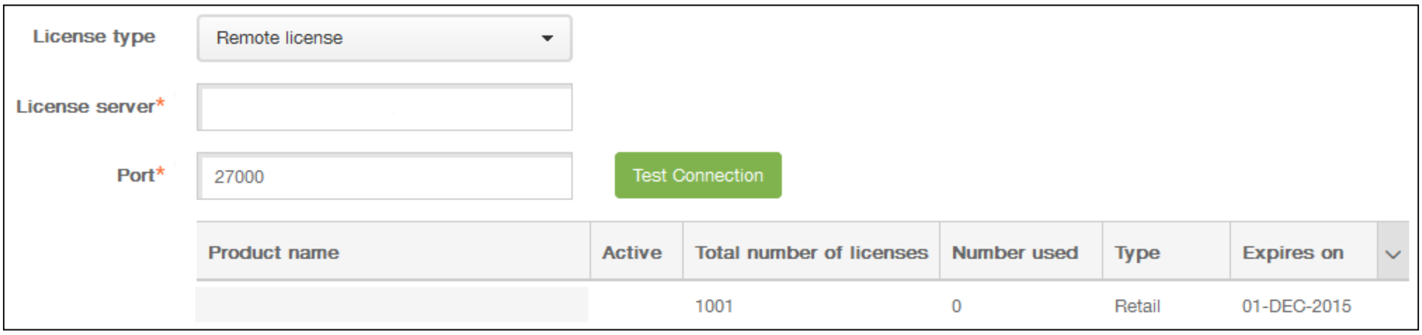
1. Import the License server certificate into XenMobile Server (**Settings > Certificates**).

2. By default, hostname verification is enabled on outgoing connections except for the Microsoft PKI server. If hostname verification breaks your deployment, change the server property **disable.hostname.verification** to **true**. The default value of this property is **false**.

When hostname verification fails, the server log includes errors such as: "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer"

3. On the **Licensing** page, set **Configure license** to **On**. The **License type** list, the **Add** button, and the **Licensing** table appear. The **Licensing** table contains licenses you have used with XenMobile. If you have not added a Citrix license yet, the table is empty.

4. Set **License type** to **Remote license**. The **License server** and **Port** fields and the **Test Connection** button replace the **Add** button.



License type: Remote license

License server*:

Port*: 27000

Product name	Active	Total number of licenses	Number used	Type	Expires on
		1001	0	Retail	01-DEC-2015

5. Configure these settings:

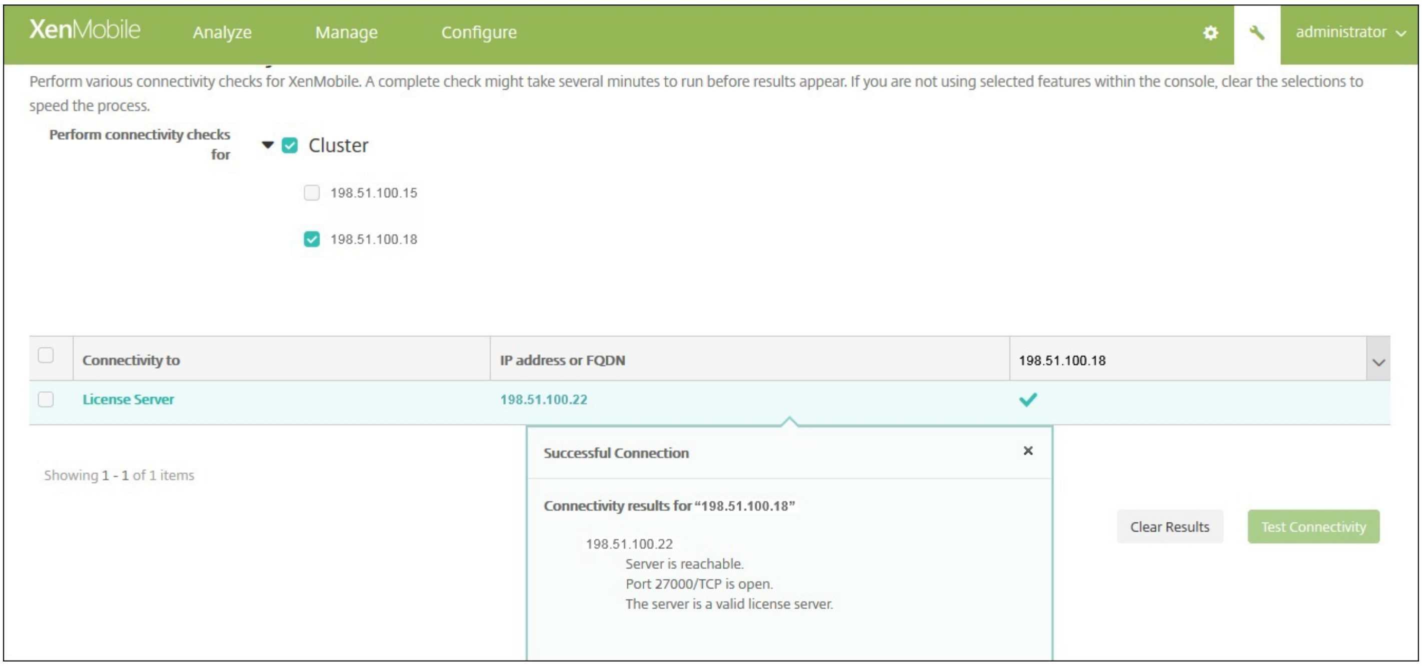
- **License server**: Type the IP address or fully qualified domain name (FQDN) of your remote licensing server.
- **Port**: Accept the default port or type the port number used to communicate with the licensing server.

6. Click **Test Connection**. If the connection is successful, XenMobile connects with the Licensing server and the Licensing table is filled with available licenses. If there is only one license, it is activated automatically.

When you click **Text Connection**, XenMobile confirms the following:

- XenMobile can communicate with the license server.
- Licenses on the license server are valid.
- The license server is compatible with XenMobile.

If the connection is unsuccessful, review the displayed error message, make the necessary corrections, and then click **Test Connection**.



Perform various connectivity checks for XenMobile. A complete check might take several minutes to run before results appear. If you are not using selected features within the console, clear the selections to speed the process.

Perform connectivity checks for ☑ Cluster

□ 198.51.100.15

☑ 198.51.100.18

□	Connectivity to	IP address or FQDN	198.51.100.18
□	License Server	198.51.100.22	✓

Showing 1 - 1 of 1 items

Successful Connection ×

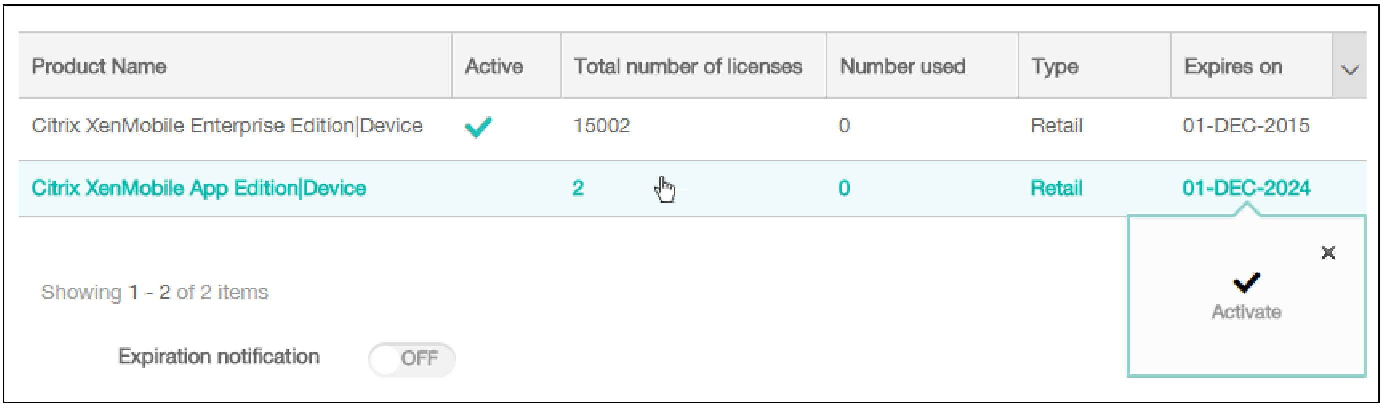
Connectivity results for "198.51.100.18"

198.51.100.22
Server is reachable.
Port 27000/TCP is open.
The server is a valid license server.

To activate a different license

If you have multiple licenses, you can choose the license you want to activate. You can have only one license active at a time, however.

1. On the **Licensing** page, in the **Licensing table**, click the row of the license you want to activate. An **Activate** confirmation dialog appears next to the row.



Product Name	Active	Total number of licenses	Number used	Type	Expires on
Citrix XenMobile Enterprise Edition|Device	✓	15002	0	Retail	01-DEC-2015
Citrix XenMobile App Edition|Device		2	0	Retail	01-DEC-2024

Showing 1 - 2 of 2 items

Expiration notification: OFF

2. Click **Activate**. The **Activate** dialog box appears.

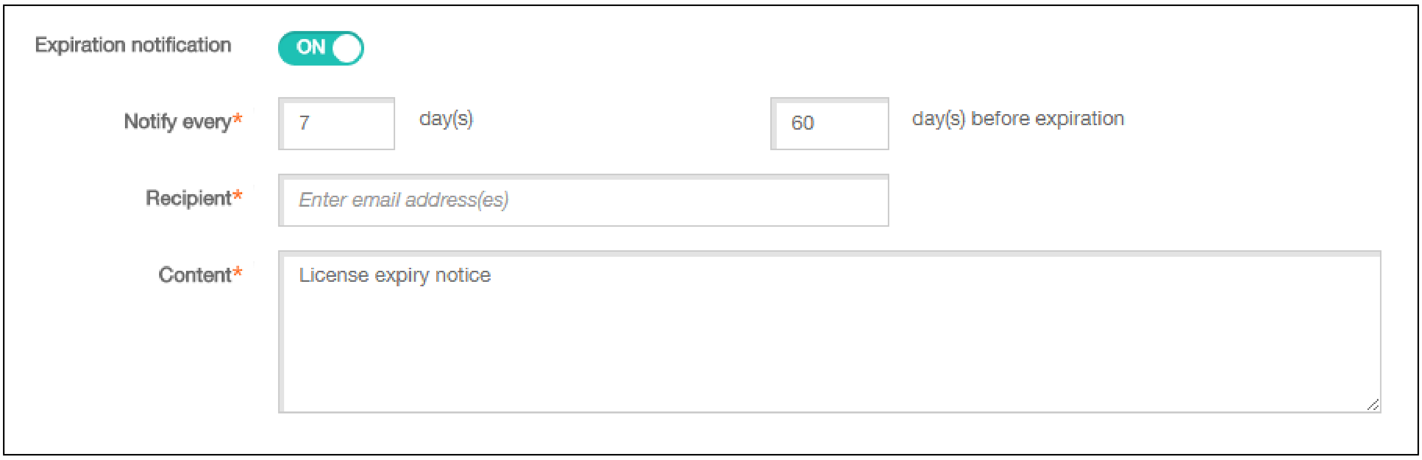
3. Click **Activate**. The selected license is activated.

> ## Important
>
> If you activate the selected license, the currently active license is deactivated.

To automate an expiration notification

After you have activated remote or local licenses, you can configure XenMobile to notify you or a designate when the license expiration date approaches.

1. On the **Licensing** page, set **Expiration notification** to **On**. New notification-related fields appear.



Expiration notification: ON

Notify every*: 7 day(s) 60 day(s) before expiration

Recipient*: Enter email address(es)

Content*: License expiry notice

2. Configure these settings:

- **Notify every**: Type:
  - The frequency with which the notifications are sent, such as every **7** days.
  - When to begin sending the notification, such as 60 days before the license expires.
- **Recipient**: Type your email address or the email address of the person responsible for the license.
- **Content**: Type an expiration notification message that the recipient sees in the notification.

3. Click **Save**. Based on your settings, XenMobile begins sending email messages containing the text you typed in **Content** to the recipient you typed in **Recipient**. The notifications are sent with the frequency you set.

FIPS 140-2 compliance

Sep 06, 2017

The Federal Information Processing Standard (FIPS), issued by the US National Institute of Standards and Technologies (NIST), specifies the security requirements for cryptographic modules used in security systems. FIPS 140-2 is the second version of this standard. For more information about NIST-validated FIPS 140 modules, see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf.

Important: FIPS support is available only for on-premises installations of XenMobile Server. You can enable XenMobile FIPS mode only during initial installation.
Note: XenMobile mobile device management-only, XenMobile mobile app management-only, and XenMobile Enterprise are all FIPS compliant as long as no HDX apps are used.
All data-at-rest and data-in-transit cryptographic operations on iOS use FIPS-certified cryptographic modules provided by the OpenSSL and Apple. On Android, all data-at-rest cryptographic operations and all data-in-transit cryptographic operations from the mobile device to NetScaler Gateway use FIPS-certified cryptographic modules provided by OpenSSL.

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

All data-at-rest and data-in-transit cryptographic operations at XenMobile Device Manager use FIPS-certified cryptographic modules provided by OpenSSL. Combined with the cryptographic operations described above for mobile devices, and between mobile devices and NetScaler Gateway, all data-at-rest and data-in-transit for MDM flows use FIPS-compliant cryptographic modules end-to-end.

All data-in-transit cryptographic operations between iOS, Android, and Windows mobile devices and NetScaler Gateway use FIPS-certified cryptographic modules. XenMobile uses a DMZ-hosted NetScaler FIPS Edition appliance equipped with a certified FIPS module to secure these data. For more information, see the NetScaler FIPS documentation.

MDX apps are supported on Windows Phone and use cryptographic libraries and APIs that are FIPS-compliant on Windows Phone. All data-at-rest for MDX apps on Windows Phone and all data-in-transit between the Windows Phone device and NetScaler Gateway are encrypted using these libraries and APIs.

The MDX Vault encrypts MDX-wrapped apps and associated data-at-rest on both iOS and Android devices using FIPS-certified cryptographic modules provided by the OpenSSL.

For the full XenMobile FIPS 140-2 compliance statement, including the specific modules used in each case, contact your Citrix representative.

Language support

Sep 06, 2017

XenMobile Apps and the XenMobile 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 http://support.citrix.com/article/CTX119253.

This article lists the supported languages in the latest release of XenMobile.

XenMobile console and the Self Help Portal

- French
- German
- Spanish
- Japanese
- Korean
- Portuguese
- Simplified Chinese

XenMobile Apps

An X indicates that the app is available in that particular language. The Secure Forms app is currently available in English only.

Note: As of the release of version 10.4, Worx Mobile Apps are renamed to XenMobile Apps. Most of the individual XenMobile Apps are also renamed. For details, see About XenMobile Apps.

iOS and Android

	Secure Hub	**Secure Mail**	**Secure Web**	**Secure Notes**	**Secure Tasks**	**QuickEdit**
Japanese	X	X	X	X	X	X
Simplified Chinese	X	X	X	X	X	X
Traditional Chinese	X	X	X	X	X	X
French	X	X	X	X	X	X
German	X	X	X	X	X	X
Spanish	X	X	X	X	X	X

Korean	X	X	X	X	X	X
Portuguese	X	X	X	X	X	X
Dutch	X	X	X	X	X	X
Italian	X	X	X	X	X	X
Danish	X	X	X	X	X	X
Swedish	X	X	X	X	X	X
Hebrew	X	X	X	X	X	iOS only
Arabic	X	X	X	X	X	X
Russian	X	X	X	X	X	X
Turkish	X	X	Android only			

Windows

	Secure Hub	**Secure Mail**	**Secure Web**
French	X	X	X
German	X	X	X
Spanish	X	X	X
Italian	X	X	X
Danish	X	X	X
Swedish	X	X	X

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.

	iOS	**Android**
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
Secure Tasks	X	X
Secure Notes	X	X
QuickEdit	X	X

Install and configure

Dec 01, 2017

Before you start:

You can use the following preinstallation checklist to note the prerequisites and settings for installing XenMobile. Each task or note includes a column indicating the component or function for which the requirement applies.

Planning a XenMobile deployment involves many considerations. For recommendations, common questions, and use cases for your complete XenMobile environment, see the XenMobile Deployment Handbook.

For installation steps, see the Install XenMobile section later in this article.

Preinstallation checklist

Basic Network Connectivity

The following are the network settings you need for the XenMobile solution.

✓	Prerequisite or setting	Component or function	Note the setting
	Note the fully qualified domain name (FQDN) to which remote users connect.	XenMobile NetScaler Gateway	
	Note the public and local IP address. You need these IP addresses to configure the firewall to set up network address translation (NAT).	XenMobile NetScaler Gateway	
	Note the subnet mask.	XenMobile NetScaler Gateway	
	Note the DNS IP addresses.	XenMobile NetScaler Gateway	
	Write down the WINS server IP addresses (if applicable).	NetScaler Gateway	

	Identify and write down the NetScaler Gateway host name. Note: This item is not the FQDN. The FQDN is contained in the signed server certificate that is bound to the virtual server and to which users connect. You can configure the host name by using the Setup Wizard in NetScaler Gateway.	NetScaler Gateway	
	Note the IP address of XenMobile. Reserve one IP address if you install one instance of XenMobile. If you configure a cluster, note all IP addresses that you need.	XenMobile	
	• One public IP address configured on NetScaler Gateway • One external DNS entry for NetScaler Gateway	NetScaler Gateway	
	Note the web proxy server IP address, port, proxy host list, and the administrator user name and password. These settings are optional if you deploy a proxy server in your network (if applicable). Note: You can use either the sAMAccountName or the User Principal Name (UPN) when configuring the user name for the web proxy.	XenMobile NetScaler Gateway	
	Note the default gateway IP address.	XenMobile NetScaler Gateway	
	Note the system IP (NSIP) address and subnet mask.	NetScaler Gateway	
	Note the subnet IP (SNIP) address and subnet mask.	NetScaler Gateway	
	Note the NetScaler Gateway virtual server IP address and FQDN from the certificate. To configure multiple virtual servers, note all virtual IP addresses and FQDNs from the certificates.	NetScaler Gateway	
	Note the internal networks that users can access through NetScaler Gateway. Example: 10.10.0.0/24 Enter all internal networks and network segments that users need access to in these cases: When users connect with Secure Hub or the NetScaler Gateway Plug-in when split tunneling is set to On.	NetScaler Gateway	

	Make sure that the network connectivity between the XenMobile server, NetScaler Gateway, the external Microsoft SQL Server, and the DNS server are reachable.	XenMobile NetScaler Gateway	

Licensing

XenMobile requires you to purchase licensing options for NetScaler Gateway and XenMobile. For more information about Citrix Licensing, see The Citrix Licensing System.

✓	Prerequisite	Component	Note the location
	Obtain Universal licenses from the Citrix web site. For details, see Licensing in the NetScaler Gateway documentation.	NetScaler Gateway XenMobile Citrix License Server	

Certificates

XenMobile and NetScaler Gateway require certificates to enable connections with other Citrix products and app and from user devices. For details, see the Certificates and Authentication section in the XenMobile documentation.

✓	Prerequisite	Component	Notes
	Obtain and install required certificates.	XenMobile NetScaler Gateway	

Ports

Open ports to allow communication with the XenMobile components.

✓	Prerequisite	Component	Notes
	Open ports for XenMobile	XenMobile NetScaler Gateway	

Database

XenMobile requires database connection configuration. The XenMobile repository requires a Microsoft SQL Server database running on one of the supported versions noted in System requirements and compatibility. Citrix recommends using Microsoft SQL remotely. PostgreSQL is included with XenMobile and should be used locally or remotely only in test environments.

By default, XenMobile uses the jDTS database driver. To use the Microsoft JDBC driver for on-premises installations of XenMobile Server, see SQL Server drivers.

∘	Prerequisite	Component	Note the setting
	Microsoft SQL Server IP address and port. Make sure the service account of the SQL Server to be used on XenMobile has the DBcreator role permission.	XenMobile	

Active Directory Settings

∘	Prerequisite	Component	Note the setting
	Note the Active Directory IP address and port for the primary and secondary servers. If you use port 636, install a root certificate from a CA on XenMobile, and change the Use secure connections option to Yes.	XenMobile NetScaler Gateway	
	Note the Active Directory domain name.	XenMobile NetScaler Gateway	
	Note the Active Directory service account, which requires a user ID, password, and domain alias. The Active Directory service account is the account that XenMobile uses to query Active Directory.	XenMobile NetScaler Gateway	
	Note the User Base DN. The directory level under which users are located; for example, cn=users,dc=ace,dc=com. NetScaler Gateway and XenMobile use this to DN query Active Directory.	XenMobile NetScaler Gateway	
	Note the Group Base DN. The directory level under which groups are located. NetScaler Gateway and XenMobile use this DN to query Active Directory.	XenMobile NetScaler Gateway	

Connections between XenMobile and NetScaler Gateway

✓	Prerequisite	Component	Note the setting
	Note the XenMobile host name.	XenMobile	
	Note the FQDN or IP address of XenMobile.	XenMobile	
	Identify the apps users can access.	NetScaler Gateway	
	Note the Callback URL.	XenMobile	

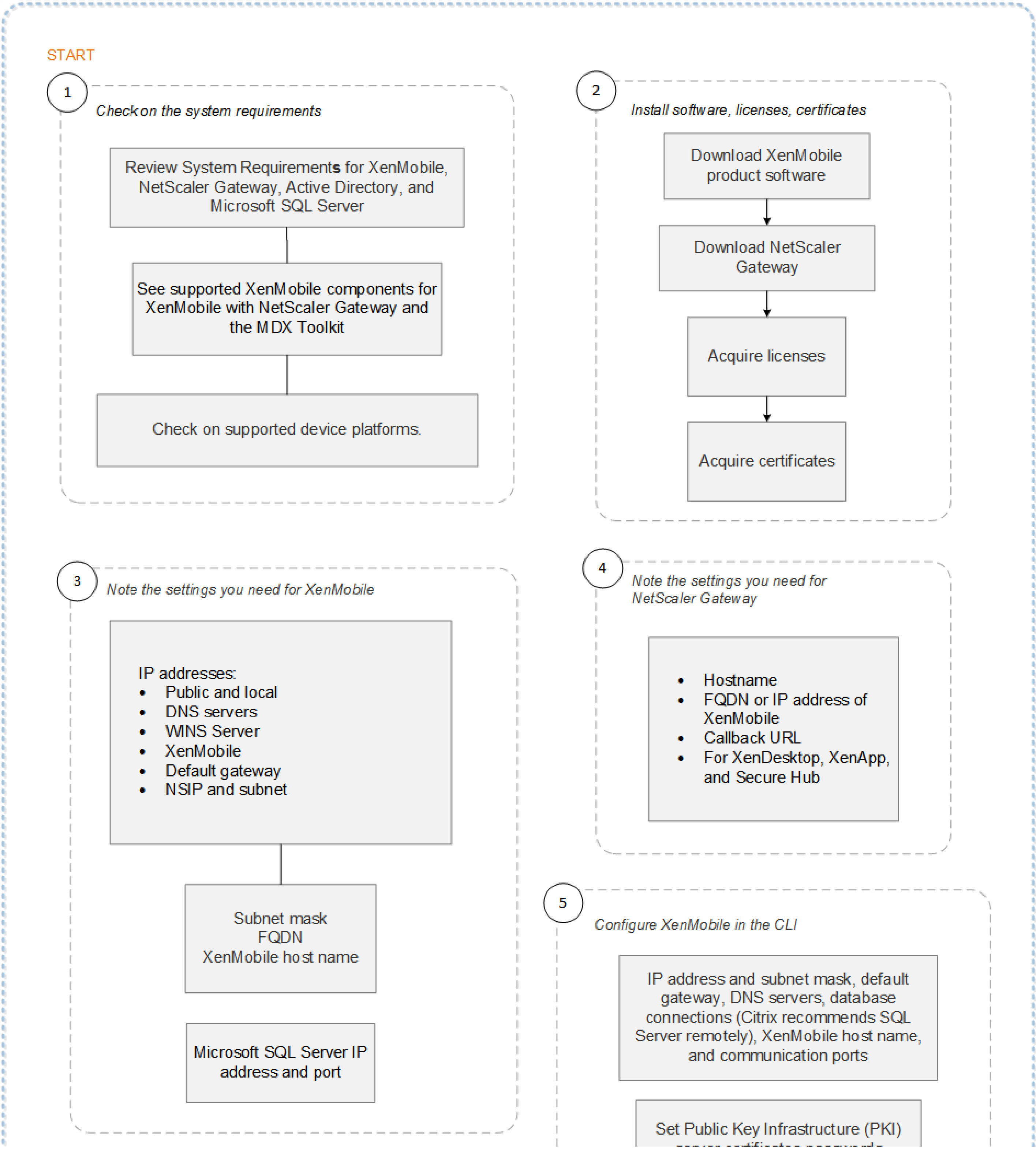
User Connections: Access to XenDesktop, XenApp, and Citrix Secure Hub

Citrix recommends that you use the Quick Configuration wizard in NetScaler to configure connection settings between XenMobile and NetScaler Gateway and between XenMobile and Secure Hub. You create a second virtual server to enable user connections from Citrix Receiver and web browsers. Those connections are to Windows-based applications and virtual desktops in XenApp and XenDesktop. Citrix recommends that you also use the Quick Configuration wizard in NetScaler to configure these settings.

∘	Prerequisite	Component	Note the setting
	Note the NetScaler Gateway host name and external URL. The external URL is the web address with which users connect.	XenMobile	
	Note the NetScaler Gateway callback URL.	XenMobile	
	Note the IP addresses and subnets masks for the virtual server.	NetScaler Gateway	
	Note the path for Program Neighborhood Agent or a XenApp Services site.	NetScaler Gateway XenMobile	
	Note the FQDN or IP address of the XenApp or XenDesktop server running the Secure Ticket Authority (STA) (for ICA connections only).	NetScaler Gateway	
	Note the public FQDN for XenMobile.	NetScaler Gateway	
	Note the public FQDN for Secure Hub.	NetScaler Gateway	

Flowchart for XenMobile deployment

You can use this flowchart to guide you through the main steps for deploying XenMobile. Links to topics on each step follow the figure.



START

1 *Check on the system requirements*

Review System Requirements for XenMobile, NetScaler Gateway, Active Directory, and Microsoft SQL Server

See supported XenMobile components for XenMobile with NetScaler Gateway and the MDX Toolkit

Check on supported device platforms.

2 *Install software, licenses, certificates*

Download XenMobile product software

Download NetScaler Gateway

Acquire licenses

Acquire certificates

3 *Note the settings you need for XenMobile*

IP addresses:
- Public and local
- DNS servers
- WINS Server
- XenMobile
- Default gateway
- NSIP and subnet

Subnet mask
FQDN
XenMobile host name

Microsoft SQL Server IP address and port

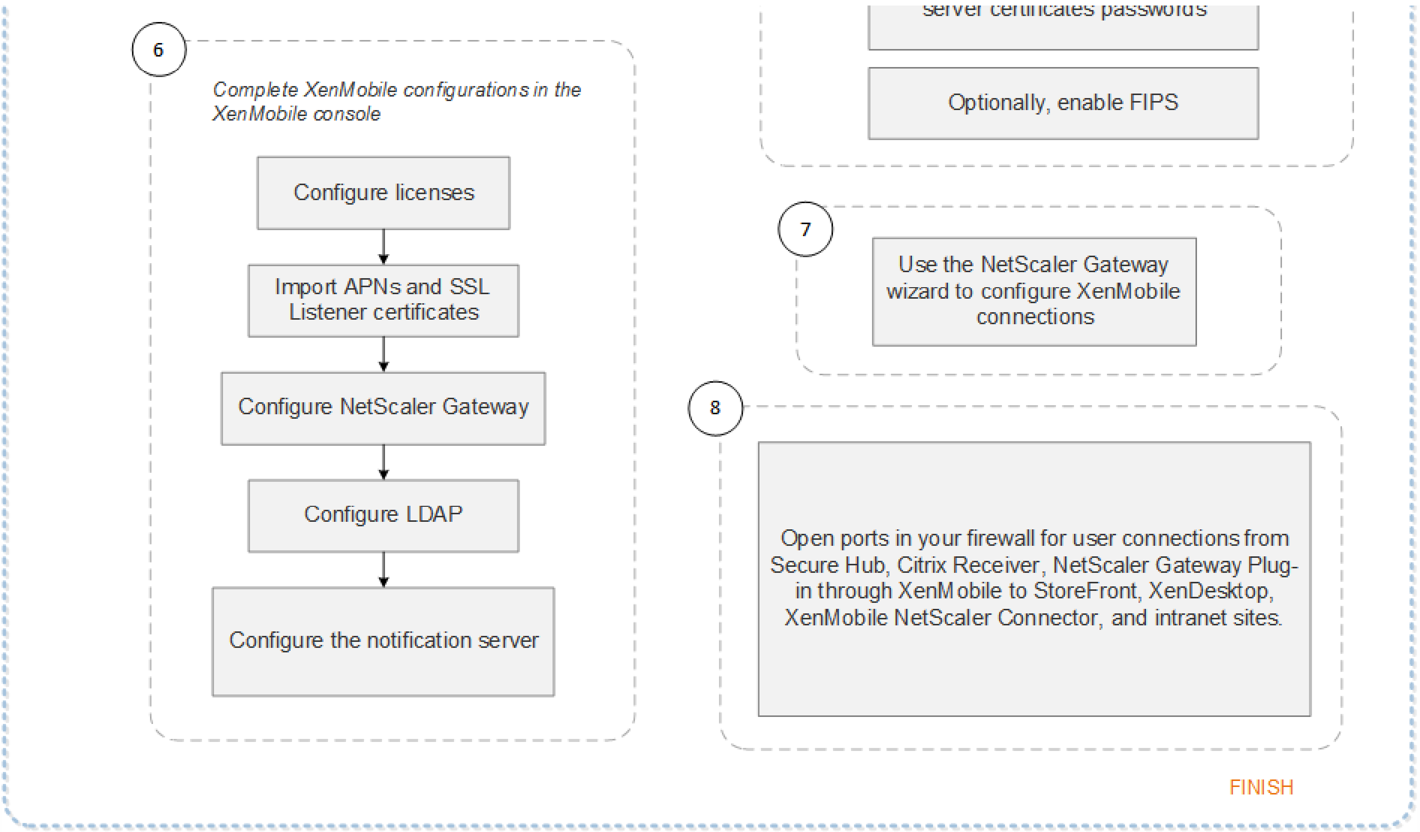
4 *Note the settings you need for NetScaler Gateway*

- Hostname
- FQDN or IP address of XenMobile
- Callback URL
- For XenDesktop, XenApp, and Secure Hub

5 *Configure XenMobile in the CLI*

IP address and subnet mask, default gateway, DNS servers, database connections (Citrix recommends SQL Server remotely), XenMobile host name, and communication ports

Set Public Key Infrastructure (PKI)


server certificates passwords
Optionally, enable FIPS
6
Complete XenMobile configurations in the XenMobile console
Configure licenses
Import APNs and SSL Listener certificates
Configure NetScaler Gateway
Configure LDAP
Configure the notification server
7
Use the NetScaler Gateway wizard to configure XenMobile connections
8
Open ports in your firewall for user connections from Secure Hub, Citrix Receiver, NetScaler Gateway Plug-in through XenMobile to StoreFront, XenDesktop, XenMobile NetScaler Connector, and intranet sites.
FINISH

1: System requirements and compatibility

2: Install and configure

3 and 4: Preinstallation checklist (this article)

5: Configure XenMobile in the Command Prompt Window (this article)

6: Configure XenMobile in a web browser (this article)

7: Configuring Settings for Your XenMobile Environment

8: Port requirements

The flowchart is also available in PDF format.

PDF Flowchart for Deploying XenMobile

Install XenMobile

The XenMobile virtual machine (VM) runs on Citrix XenServer, VMware ESXi, or Microsoft Hyper-V. You can use XenCenter or vSphere management consoles to install XenMobile.

> ### Note
>
> Ensure that the hypervisor is configured with the correct time – either using an NTP server or a manual configuration - because

> XenMobile uses that time. If you have time zone issues when syncing XenMobile time with a hypervisor, you can avoid the issues by pointing XenMobile to an NTP server. To do that, use the XenMobile CLI, as described in Command-line interface options.

XenServer or VMware ESXi prerequisites: Before installing XenMobile on XenServer or VMware ESXi, you must do the following. For details, refer to your XenServer or VMware documentation.

- Install XenServer or VMware ESXi on a computer with adequate hardware resources.
- Install XenCenter or vSphere on a separate computer. The computer that hosts XenCenter or vSphere connects to the XenServer or VMware ESXi host through the network.

Hyper-V prerequisites: Before installing XenMobile on Hyper-V, you must do the following. For details, refer to your Hyper-V documentation.

- Install Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 with Hyper-V enabled, role enabled, on a computer with adequate system resources. While installing the Hyper-V role, be sure to specify the network interface cards (NICs) on the server that Hyper-V will use to create the virtual networks. You can reserve some NICs for the host.
- - Delete the file Virtual Machines/<build-specific UUID>.xml
  - Move the file Legacy/<build-specific UUID>.exp into Virtual Machines

If you install Windows Server 2008 R2 or Windows Server 2012, do the following:

These steps are necessary because there are two different versions of the Hyper-V manifest file representing the VM configuration (.exp and .xml). The Windows Server 2008 R2 and Windows Server 2012 releases support only .exp. For these releases, you must have only the .exp manifest file in place before installation.

Windows Server 2012 R2 does not require these extra steps.

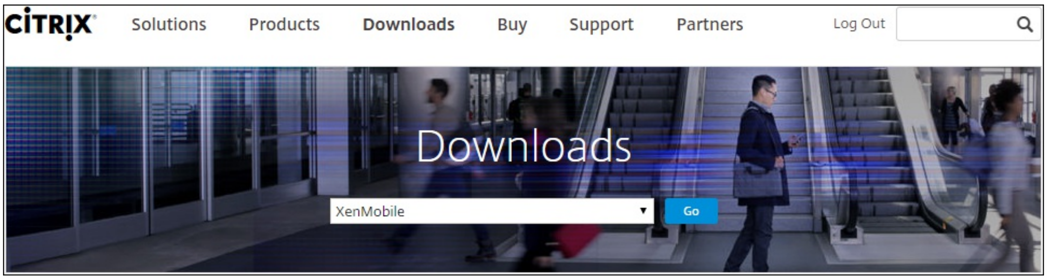
FIPS 140-2 mode: If you plan to install XenMobile server in FIPS mode, you need to complete a prerequisite group, as discussed in Configuring FIPs.

Download XenMobile product software

You can download product software from the Citrix web site. You need to log on to the site first and then use the Downloads link on the Citrix web page to navigate to the page containing the software you want to download.

To download the software for XenMobile

1. Go to the Citrix web site.
2. Next to the Search box, click Log On and log on to your account.
3. Click the Downloads tab.
4. On the Downloads page, from the select product list, click XenMobile.



5. Click **Go**. The XenMobile page appears.
6. Expand **XenMobile Server**.
7. Expand **Product Software**.
8. Click **XenMobile Server 10**.
9. Click the **Jump to Download** menu and choose the appropriate virtual image to use to install XenMobile.. Alternatively, scroll down the page to locate the **Download File** button for the image you want to install.
10. Follow the instructions on your screen to download the software.

To download the software for NetScaler Gateway

You can use this procedure to download the NetScaler Gateway virtual appliance or software upgrades to your existing NetScaler Gateway appliance.

1. Go to the Citrix web site.
2. If you are not already logged on to the Citrix web site, next to the Search box, click Log On and log on to your account.
3. Click the Downloads tab.
4. On the Downloads page, from the select product list, click NetScaler Gateway.
5. Click Go. The NetScaler Gateway page appears.
6. On the NetScaler Gateway page, expand the version of NetScaler Gateway you are running.
7. Under Firmware, click the appliance software version you want to download.
   Note: You can also click Virtual Appliances to download NetScaler VPX. When you select this option, you receive a list of software for the virtual machine for each hypervisor.
8. Click the appliance software version you want to download.
9. On the appliance software page for the version you want to download, click Download for the appropriate virtual appliance.
10. Follow the instructions on your screen to download the software.

Configure XenMobile for First-Time Use

1. Configure the IP address and subnet mask, default gateway, DNS servers, and so on for XenMobile by using the XenCenter or vSphere command-line console.

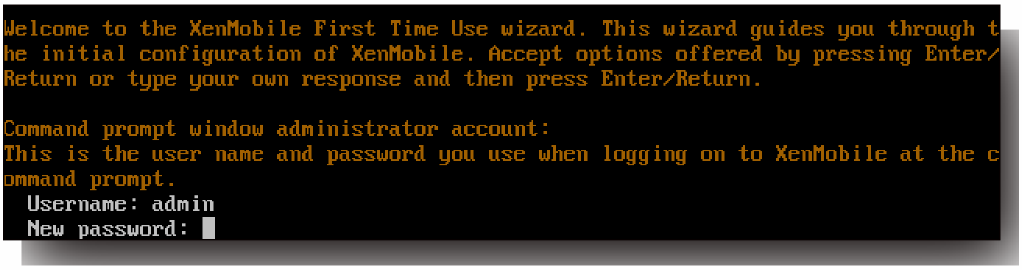
> ### Note
>
> When you use a vSphere web client: We recommend that you don't configure networking properties during the time you deploy the OVF template on the **Customize template** page. By doing so in a high availability configuration: You avoid an issue with the IP address that occurs when you clone and then restart the second XenMobile virtual machine.

2. Access the XenMobile management console only through the XenMobile Server fully qualified domain name or the IP addresses of the node.

3. Log on and then follow the steps in the initial logon screens.

Configure XenMobile in the Command Prompt Window

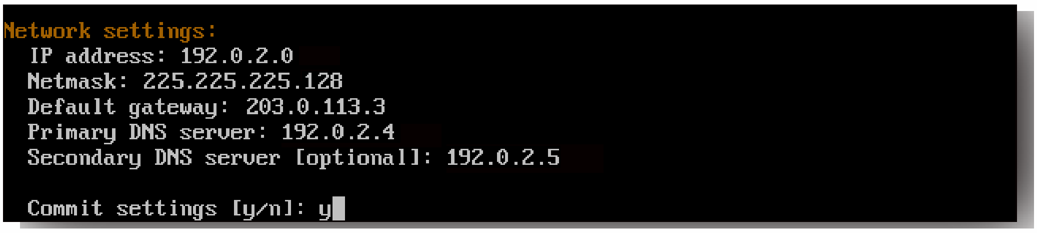
1. Import the XenMobile virtual machine into Citrix XenServer, Microsoft Hyper-V, or VMware ESXi. For details, see XenServer, Hyper-V, or VMware documentation.
2. In your hypervisor, select the imported XenMobile virtual machine and start the command prompt view. For details, see the documentation for your hypervisor.
3. From the hypervisor console page, create an administrator account for XenMobile in the command prompt window by typing the administrator user name and password.
   Important:
   When you create or changed passwords for the command prompt administrator account, Public Key Infrastructure (PKI) server certificates, and FIPS: XenMobile enforces the following rules for all users except Active Directory users whose passwords are managed outside of XenMobile.
   - The password must be at least eight characters long and must meet at least three of the following complexity criteria:
     - Uppercase letters (A through Z)
     - Lowercase letters (a through z)
     - Numerals (0 through 9)
     - Special characters (such as, !, #, $, %)



```
Welcome to the XenMobile First Time Use wizard. This wizard guides you through t
he initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
  Username: admin
  New password: 
```

   Note: No characters, such as asterisks, are shown when you type the new password. Nothing appears.

4. Provide the following network information and then, type y to commit the settings:
   1. IP address of the XenMobile server
   2. Netmask
   3. Default gateway, which is the IP address of the default gateway in the DMZ
   4. Primary DNS server, which is the IP address of the DNS server
   5. Secondary DNS server (optional)

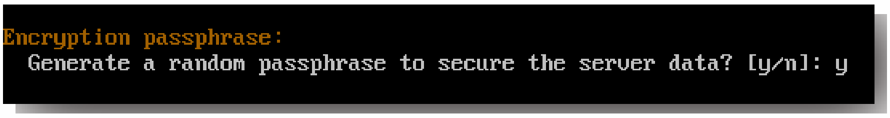


```
Network settings:
  IP address: 192.0.2.0
  Netmask: 225.225.225.128
  Default gateway: 203.0.113.3
  Primary DNS server: 192.0.2.4
  Secondary DNS server [optional]: 192.0.2.5

  Commit settings [y/n]: y
```

Note: The addresses shown in this and following images are non-working and are provided as examples only.

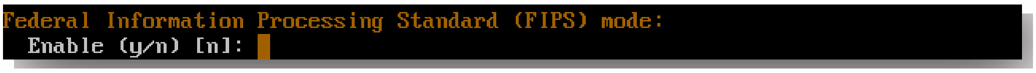
5. Type y to increase security by generating a random encryption passphrase or n to provide your own passphrase. Citrix recommends typing y to generate a random passphrase. The passphrase is used as part of the protection of the encryption keys used to secure your sensitive data. A hash of the passphrase, stored in the server file system, is used to retrieve the keys during the encryption and decryption of data. The passphrase cannot be viewed.

   > **Note:** If you intend to extend your environment and configure more servers, provide your own passphrase. If you select a random passphrase, you can't view it.



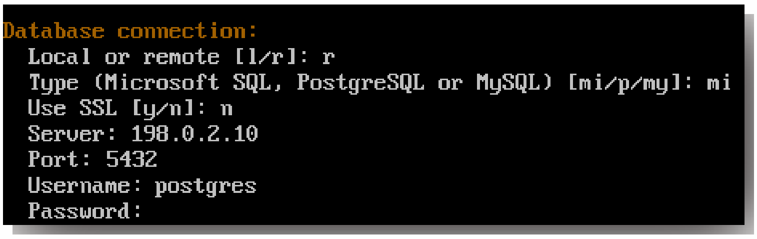
```
Encryption passphrase:
  Generate a random passphrase to secure the server data? [y/n]: y
```

6. Optionally, enable Federal Information Processing Standard (FIPS). For details about FIPS, see FIPS. Also, be sure to complete a prerequisite group, as discussed in Configuring FIPs.



```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

7. Provide the following information to configure the database connection.

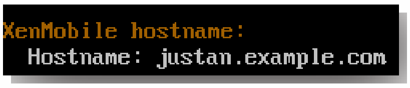


```
Database connection:
  Local or remote [l/r]: r
  Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi
  Use SSL [y/n]: n
  Server: 198.0.2.10
  Port: 5432
  Username: postgres
  Password:
```

   1. Your database can be local or remote. Type l for local or r for remote.
   2. Select the database type. Type mi for Microsoft SQL or type p for PostgreSQL.
      Important:
      - Citrix recommends using Microsoft SQL remotely. PostgreSQL is included with XenMobile and should be used locally or remotely only in test environments.
      - Database migration is not supported. Databases created in a test environment cannot be moved to a production environment.
   3. Optionally, type y to use SSL authentication for your database.
   4. Provide the fully qualified domain name (FQDN) for the server hosting XenMobile. This one host server provides both device management and app management services.
   5. Type your database port number if it is different from the default port number. The default port for Microsoft SQL is 1433 and the default port for PostgreSQL is 5432.
   6. Type your database administrator user name.
   7. Type your database administrator password.
   8. Type the database name.
   9. Press **Enter** to commit the database settings.
8. Optionally, type y to enable clustering XenMobile nodes, or instances.

Important: If you enable a XenMobile cluster, after system configuration completes, open port 80 to enable real-time communication between cluster members. Complete that setup on all cluster nodes.

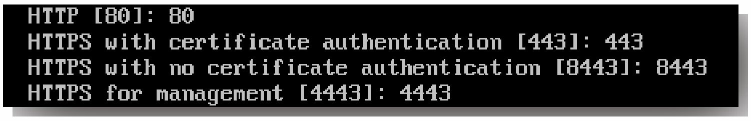
9. Type the XenMobile server fully qualified domain name (FQDN).



```
XenMobile hostname:
  Hostname: justan.example.com
```

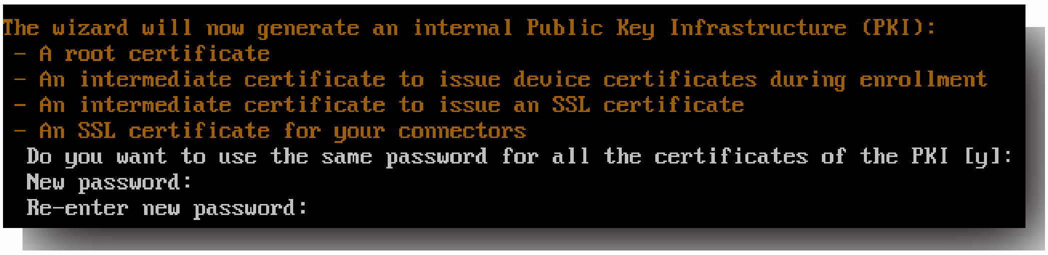
10. Press **Enter** to commit the settings.
11. Identify the communication ports. For details on ports and their uses, see Port Requirements.

    Note: Accept the default ports by pressing **Enter** (Return on a Mac).



```
  HTTP [80]: 80
  HTTPS with certificate authentication [443]: 443
  HTTPS with no certificate authentication [8443]: 8443
  HTTPS for management [4443]: 4443
```

12. Skip the next question about upgrading from a previous XenMobile release because you are installing XenMobile for the first time.
13. Type y if you want to use the same password for each Public Key Infrastructure (PKI) certificate. For details on the XenMobile PKI feature, see Uploading Certificates.

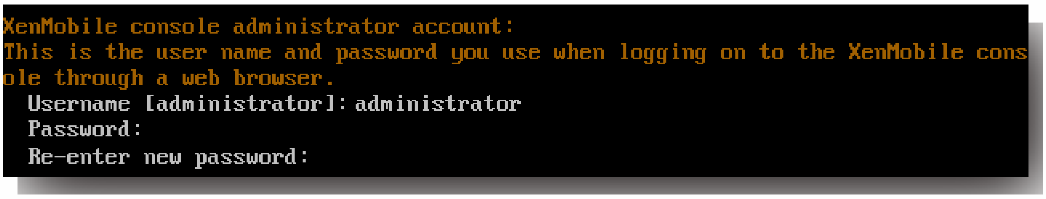


```
The wizard will now generate an internal Public Key Infrastructure (PKI):
 - A root certificate
 - An intermediate certificate to issue device certificates during enrollment
 - An intermediate certificate to issue an SSL certificate
 - An SSL certificate for your connectors
  Do you want to use the same password for all the certificates of the PKI [y]:
  New password:
  Re-enter new password:
```

Important: If you intend to cluster nodes, or instances, of XenMobile together, you must provide the identical passwords for subsequent nodes.

14. Type the new password and then, reenter the new password to confirm it.

    Note: No characters, such as asterisks, are shown when you type the new password. Nothing appears.
15. Press **Enter** to commit the settings.
16. Create an administrator account for logging on to the XenMobile console with a web browser. Be sure to remember these credentials for later use.

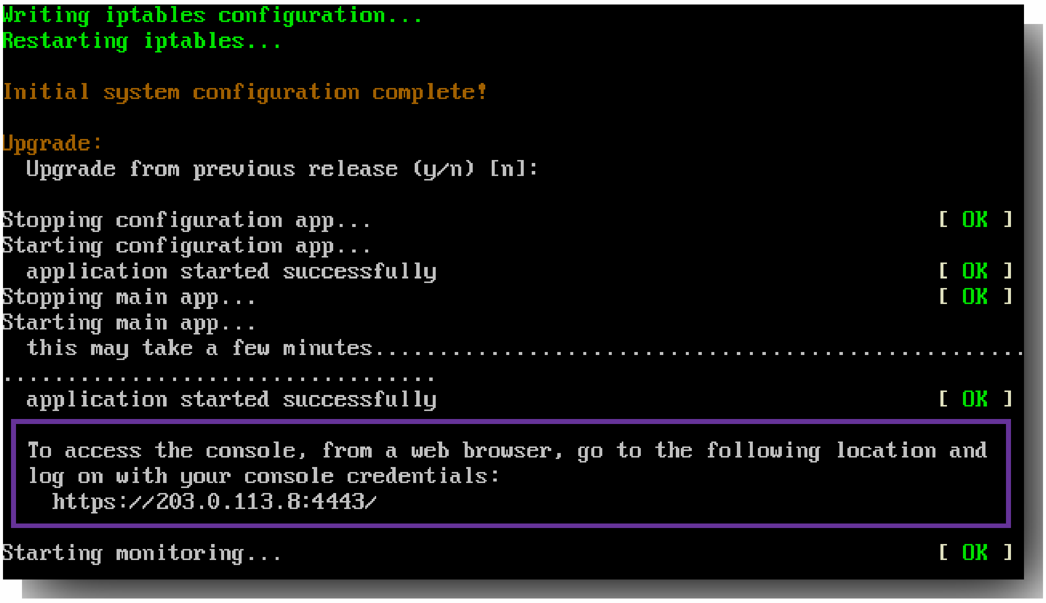


```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile cons
ole through a web browser.
  Username [administrator]: administrator
  Password:
  Re-enter new password:
```

Note: No characters, such as asterisks, are shown when you type the new password. Nothing appears.

17. Press **Enter** to commit the settings. The initial system configuration is saved.
18. When asked if this is an upgrade, type n because it is a new installation.

19. Copy the complete URL that appears on the screen and continue this initial XenMobile configuration in your web browser.



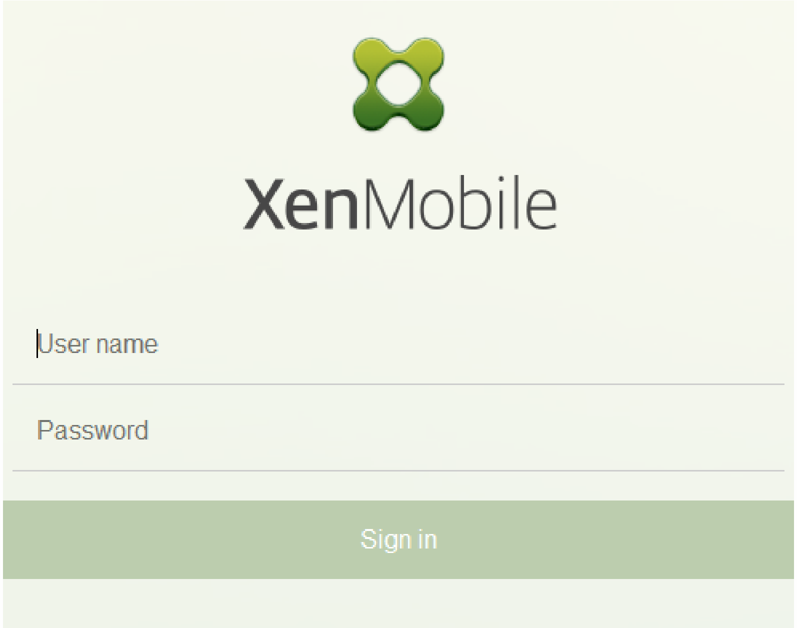
```
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!

Upgrade:
  Upgrade from previous release (y/n) [n]:

Stopping configuration app...                                          [ OK ]
Starting configuration app...
  application started successfully                                     [ OK ]
Stopping main app...                                                   [ OK ]
Starting main app...
  this may take a few minutes............................................
..................................
  application started successfully                                     [ OK ]

  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://203.0.113.8:4443/

Starting monitoring...                                                 [ OK ]
```

Configure XenMobile in a web browser

After completing the initial portion of the XenMobile configuration in your hypervisor command prompt window, complete the process in your web browser.

1. In your web browser, navigate to the location provided at the conclusion of the command prompt window configuration.

2. Type the XenMobile console administrator account user name and password you created in the command prompt window.



3. On the Get Started page, click Start. The Licensing page appears.
4. Configure the license. If you don't upload a license, you use an evaluation license valid for 30 days. For details on adding and configuring licenses and configuring expiration notifications, see Licensing.

Important: If you intend to use XenMobile clustering by adding cluster nodes, or instances, of XenMobile, you must use the Citrix Licensing on a remote server.
5. On the Certificate page, click Import. The Import dialog box appears.

6. Import your APNs and SSL Listener certificate. If you manage iOS devices, you need an APNs certificate. For details on working with certificates, see Certificates.

Note: This step requires restarting the server.
7. If appropriate to the environment, configure NetScaler Gateway. For details on configuring NetScaler Gateway, see NetScaler Gateway and XenMobile and Configuring Settings for Your XenMobile Environment.

Note:
- You can deploy NetScaler Gateway at the perimeter of your internal network (or intranet). That deployment provides a secure single point of access to the servers, apps, and other network resources that reside in the internal network. In this deployment, all remote users must connect to NetScaler Gateway before they can access any resources in the internal network.
- Although NetScaler Gateway is an optional setting: After you enter data on the page, you must clear or complete the required fields before you can leave the page.

8. Complete the LDAP configuration to access users and groups from Active Directory. For details on configuring the LDAP connection, see LDAP Configuration.

9. Configure the notification server to be able to send messages to users. For details on notification server configuration, see Notifications.

Post-requisite: Restart the XenMobile server to activate your certificates.

Configure FIPS with XenMobile

Jan 09, 2018

> ## Note
>
> XenMobile Service server-side components are not FIPS 140-2 compliant.

Federal Information Processing Standards (FIPS) mode in XenMobile supports U.S. federal government customers by configuring the server to use only FIPS 140-2 certified libraries for all encryption operations. Installing your XenMobile server with FIPS mode ensures that all data at rest and data in transit for both the XenMobile client and server are fully compliant with FIPS 140-2.

Before installing a XenMobile Server in FIPS mode, you need to complete the following prerequisites.

- You must use an external SQL Server 2012 or SQL Server 2014 for the XenMobile database. The SQL Server also must be configured for secure SSL communication. For instructions on configuring secure SSL communication to SQL Server, see the SQL Server Books Online.
- Secure SSL communication requires that an SSL certificate be installed on your SQL Server. The SSL certificate can either be a public certificate from a commercial CA or a self-signed certificate from an internal CA. Note that SQL Server 2014 cannot accept a wildcard certificate. Citrix recommends, therefore, that you request an SSL certificate with the FQDN of the SQL Server.
- If you use a self-signed certificate for SQL Server, you will need a copy of the root CA certificate that issued your self-signed certificate. The root CA certificate must be imported to the XenMobile server during installation.

Configuring FIPS mode

You can enable FIPS mode only during the initial setup of XenMobile server. It is not possible to enable FIPS after installation is complete. Therefore, if you plan on using FIPS mode, you must install the XenMobile server with FIPS mode from the start. In addition, if you have a XenMobile cluster, all cluster nodes must have FIPS enabled; you cannot have a mix of FIPS and non-FIPS XenMobile servers in the same cluster.

There is a **Toggle FIPS mode** option in the XenMobile command-line interface that is not for production use. This option is intended for non-production, diagnostic use and is not supported on a production XenMobile server.

1. During initial setup, enable **FIPS mode**.

2. Upload the root CA certificate for your SQL Server. If you used a self-signed SSL certificate rather than a public certificate on your SQL Server, choose **Yes** for this option and then do one of the following:

    a. Copy and paste the CA certificate.

    b. Import the CA certificate. To import the CA certificate, you must post the certificate to a website that is accessible from the XenMobile server via an HTTP URL. For details, see Uploading the certificate to XenMobile.

3. Specify the server name and port of your SQL Server, the credentials for logging into SQL Server, and the database name to create for XenMobile.

Note: You can use either a SQL logon or an Active Directory account to access SQL Server, but the logon you use must have the DBcreator role.

4. To use an Active Directory account, enter the credentials in the format domain\username.

5. Once these steps are complete, proceed with the XenMobile initial setup.

To confirm that the configuration of FIPS mode is successful, log on to the XenMobile command-line interface. The phrase **In FIPS Compliant Mode** appears in the logon banner.

Importing Certificates

The following procedure describes how to configure FIPS on XenMobile by importing the certificate, which is required when you use a VMware hypervisor.

SQL Prerequisites

1. The connection to the SQL instance from XenMobile needs to be secure and must be SQL Server version 2012 or SQL Server 2014. To secure the connection, see How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console.

2. If the service does not restart properly, check the following:Open **Services.msc**.

a. Copy the logon account information used for the SQL Server service.

b. Open MMC.exe on the SQL Server.

c. Go to **File** > **Add/Remove Snap-in** and then double-click the certificates item to add the certificates snap-in. Select the computer account and local computer in the two pages on the wizard.

d. Click **OK**.

e. Expand **Certificates (Local Computer)** > **Personal** > **Certificates** and find the imported SSL certificate.

f. Right-click the imported certificate (selected in the SQL Server Configuration Manager) and then click **All Tasks** > **Manage Private Keys**.

g. Under **Group or User names**, click **Add**.

h. Enter the SQL service account name you copied in the earlier step.

i. Clear the **Allow Full Control** option. By default the service account will be given both Full control and Read permissions, but it only needs to be able to read the private key.

j. Close **MMC** and start the SQL service.

3. Ensure the SQL service is started correctly.

Internet Information Services (IIS) Prerequisites

1. Download the rootcert (base 64).

2. Copy the rootcert to the default site on the IIS server, C:\inetpub\wwwroot.

3. Check the **Authentication** check box for the default site.

4. Set **Anonymous** to **enabled**.

5. Select the **Failed Request Tracking** rules check box.

6. Ensure that .cer is not blocked.

7. Browse to the location of the .cer in an Internt Explorer browser from the local server, http://localhost/certname.cer. The root cert text should appear in the browser.

8. If the root cert does not appear in the Internet Explorer browser, make sure that ASP is enabled on the IIS server as follows.

   a. Open Server Manager**.**

   b. Navigate to the wizard in **Manage** > **Add Roles and Features**.

   c. In the server roles, expand **Web Server (IIS)**, expand **Web Server**, expand **Application Development** and then select **ASP**.

   d. Click **Next** until the install completes.

9. Open Internet Explorer and browse to http://localhost/cert.cer.

For more information, see Web Server (IIS).

> Note
>
> You can use the use the IIS instance of the CA for this procedure.

Importing the Root Certificate During Initial FIPS Configuration

When you complete the steps to configure XenMobile for the first time in the command-line console, you must complete these settings to import the root certificate. For details on the installation steps, see Installing XenMobile.

- Enable FIPS: Yes
- Upload Root Certificate: Yes
- Copy(c) or Import(i): i
- Enter HTTP URL to import: http://*FQDN of IIS server*/cert.cer
- Server: *FQDN of SQL Server*
- Port: 1433
- User name: Service account which has the ability to create the database (domain\username).
- Password: The password for the service account.
- Database Name: This is a name you choose.

Enable FIPS mode on mobile devices

By default, FIPS mode is disabled on mobile devices. To enable FIPS mode, go to **Settings > Client Properties**, edit the **Enable FIPS Mode** property, and set the value to **true**. For more information, see Client properties.

Configure clustering

Jan 02, 2018

In XenMobile versions earlier than version 10, you configured Device Manager as a cluster and App Controller as a high availability pair. XenMobile 10 integrated XenMobile 9 Device Manager and App Controller. As of version 10, high availability is no longer applicable to XenMobile. To configure clustering, therefore, you need to configure the following two load balancing virtual IP addresses on NetScaler.

- **Mobile device management (MDM) load balancing virtual IP address**: An MDM load balancing virtual IP address is required to communicate with the XenMobile nodes that are configured in a cluster. This load balancing is done in SSL Bridge mode.
- **Mobile app management (MAM) load balancing virtual IP address**: MAM load balancing virtual IP addresses are required for NetScaler Gateway to communicate with XenMobile nodes that are configured in a cluster. In XenMobile 10, by default, all traffic from NetScaler Gateway routes to the load balancing virtual IP address on port 8443.

The procedures in this article explain the method of creating a new XenMobile virtual machine (VM) and joining the new VM to an existing VM, thereby creating a cluster setup.

Prerequisites

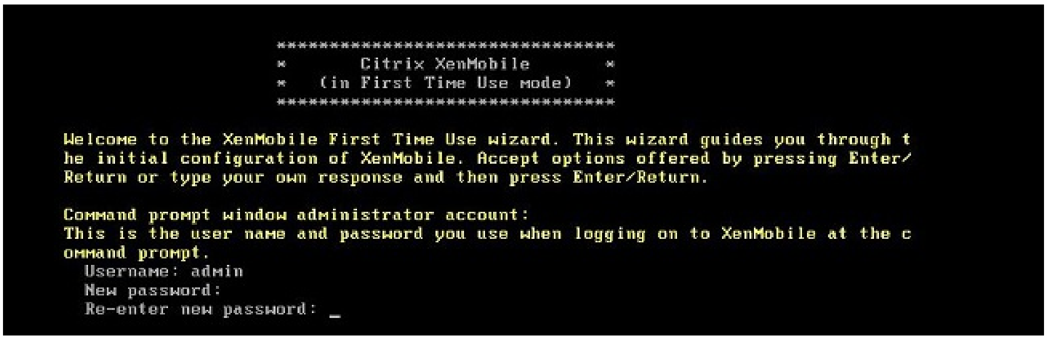
- You have fully configured the required XenMobile node.
- Configure NTP on all cluster nodes and the XenMobile database. Clustering doesn't work properly unless all of those servers have the same time.
- One public IP address for MDM load balancer and one private IP address for MAM.
- Server certificates.
- One free IP for NetScaler Gateway virtual IP address.
- With XenMobile deployed in a cluster setup and in MDM-only or Enterprise mode (MDM+MAM): You must modify your NetScaler load balancer configuration to use **Source IP persistence** for all NetScaler MDM load balancers, that is, virtual servers set up for ports 8443 and 443. Complete that configuration before user devices upgrade to iOS 11. For more information, see this Citrix Knowledge Center article: https://support.citrix.com/article/CTX227406.

For reference architectural diagrams for XenMobile 10.x in clustered configurations, see Architecture.

Installing the XenMobile Cluster Nodes

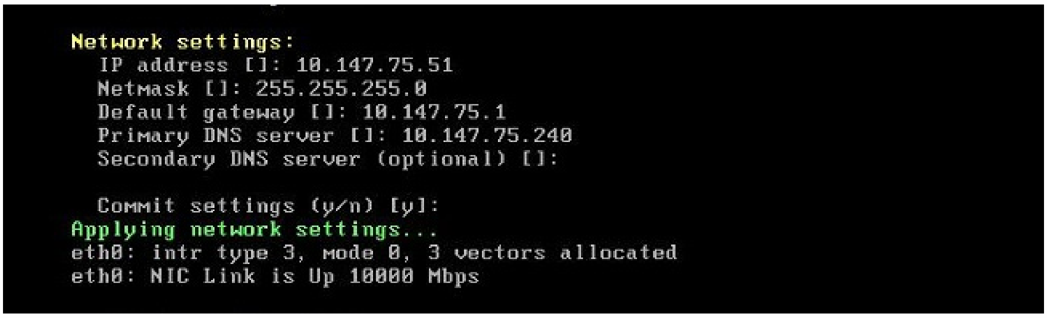
Based on the number of nodes you require, you create new XenMobile VMs. You point the new VMs to the same database and provide the same PKI certificate passwords.

1. Open the command-line console of the new VM and enter the new password for the administrator account.



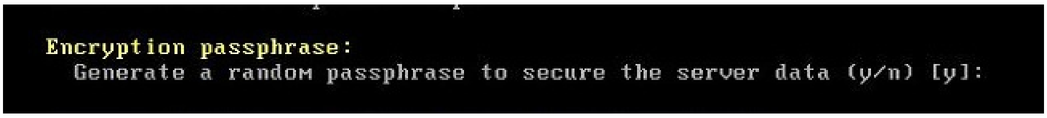
```
                    **********************************
                    *        Citrix XenMobile        *
                    *    (in First Time Use mode)    *
                    **********************************

Welcome to the XenMobile First Time Use wizard. This wizard guides you through t
he initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
  Username: admin
  New password:
  Re-enter new password: _
```

2. Provide the network configuration details as shown in the following figure.



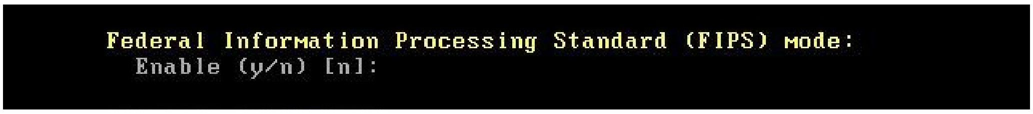
```
Network settings:
  IP address []: 10.147.75.51
  Netmask []: 255.255.255.0
  Default gateway []: 10.147.75.1
  Primary DNS server []: 10.147.75.240
  Secondary DNS server (optional) []:

  Commit settings (y/n) [y]:
Applying network settings...
eth0: intr type 3, mode 0, 3 vectors allocated
eth0: NIC Link is Up 10000 Mbps
```

3. If you want to use the default password for data protection, type y; or, type n and enter a new password.



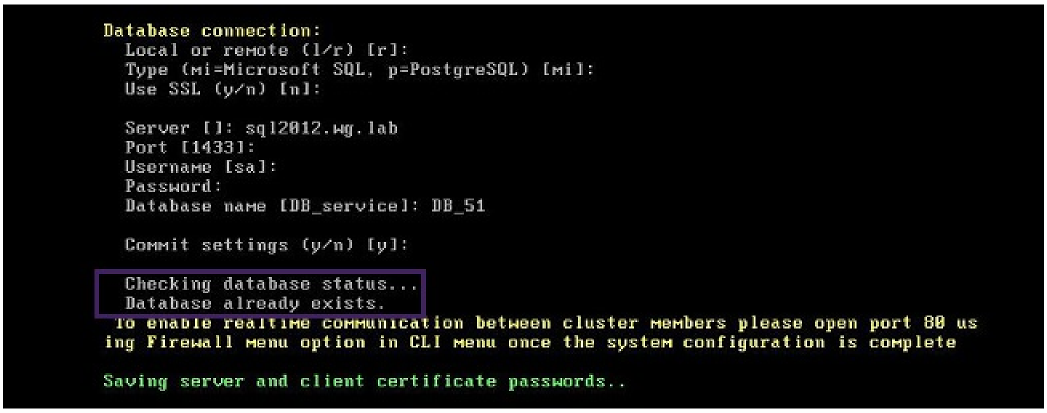
```
Encryption passphrase:
  Generate a random passphrase to secure the server data (y/n) [y]:
```

4. If you want to use FIPS, type y; or, type n.



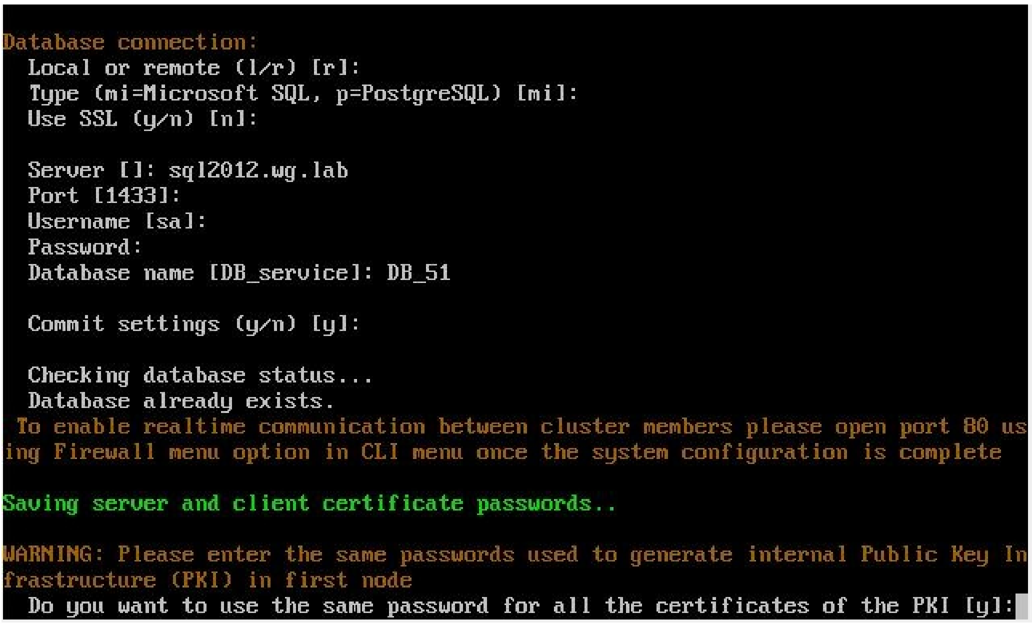
```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

5. Configure the database so that you point to same database that the earlier fully configured VM pointed to. You will see the message: Database already exists.



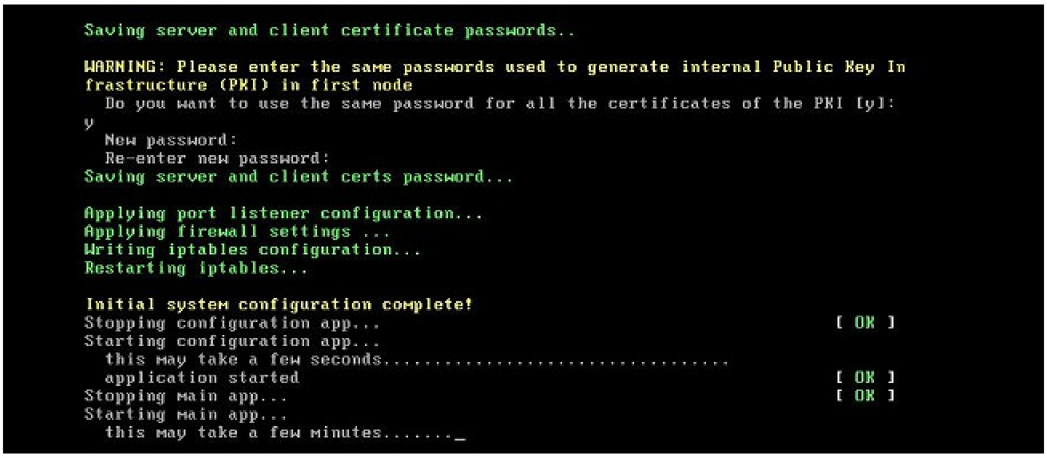
```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

  Server []: sql2012.wg.lab
  Port [1433]:
  Username [sa]:
  Password:
  Database name [DB_service]: DB_51

  Commit settings (y/n) [y]:

  Checking database status...
  Database already exists.
 To enable realtime communication between cluster members please open port 80 us
ing Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..
```

6. Enter the same passwords for the certificates that you provided for the first VM.



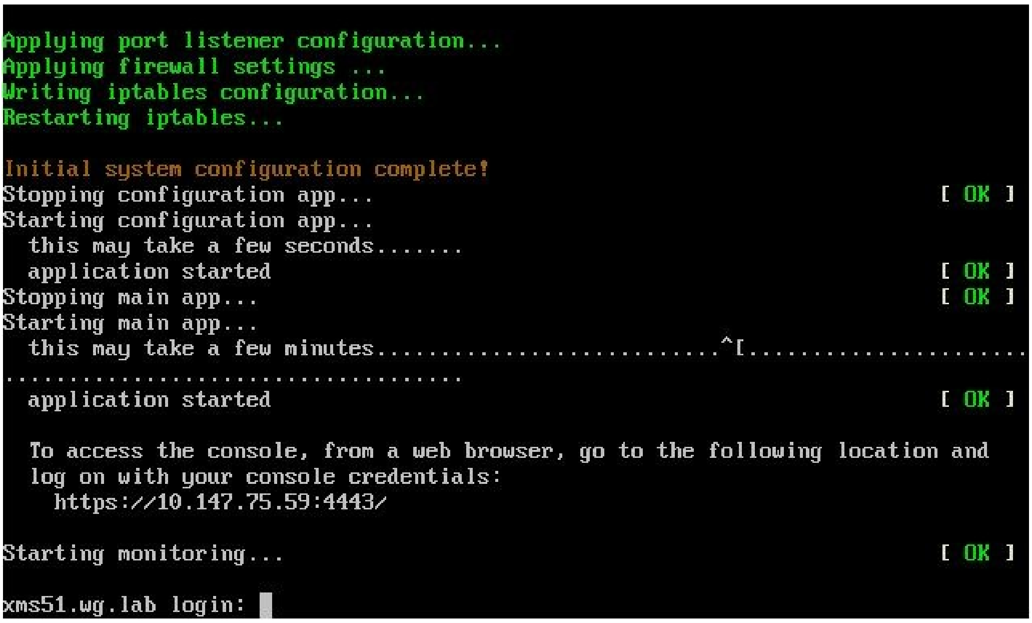
```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

  Server []: sql2012.wg.lab
  Port [1433]:
  Username [sa]:
  Password:
  Database name [DB_service]: DB_51

  Commit settings (y/n) [y]:

  Checking database status...
  Database already exists.
 To enable realtime communication between cluster members please open port 80 us
ing Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key In
frastructure (PKI) in first node
  Do you want to use the same password for all the certificates of the PKI [y]:
```

After you have entered the password, the initial configuration on second node will complete.



```
Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key In
frastructure (PKI) in first node
  Do you want to use the same password for all the certificates of the PKI [y]:
y
  New password:
  Re-enter new password:
Saving server and client certs password...

Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app...                                          [ OK ]
Starting configuration app...
  this may take a few seconds.................................
  application started                                                  [ OK ]
Stopping main app...                                                   [ OK ]
Starting main app...
  this may take a few minutes......._
```

7. When the configuration is complete, the server restarts and the logon dialog box appears.

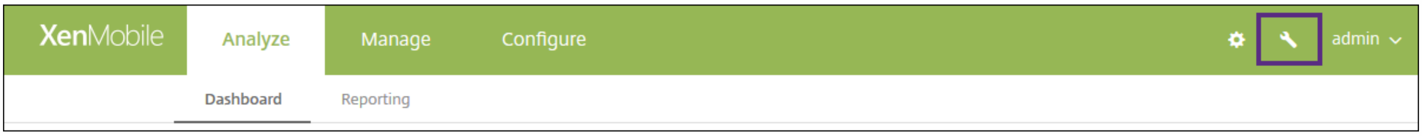


```
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app...                                      [ OK ]
Starting configuration app...
  this may take a few seconds.......
  application started                                              [ OK ]
Stopping main app...                                               [ OK ]
Starting main app...
  this may take a few minutes...........................^[.......................
......................................
  application started                                              [ OK ]

  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://10.147.75.59:4443/

Starting monitoring...                                             [ OK ]

xms51.wg.lab login:
```

Note: The logon dialog box is identical to the logon dialog box of the first VM. The match is a way for you to confirm that both VMs are using the same database server.

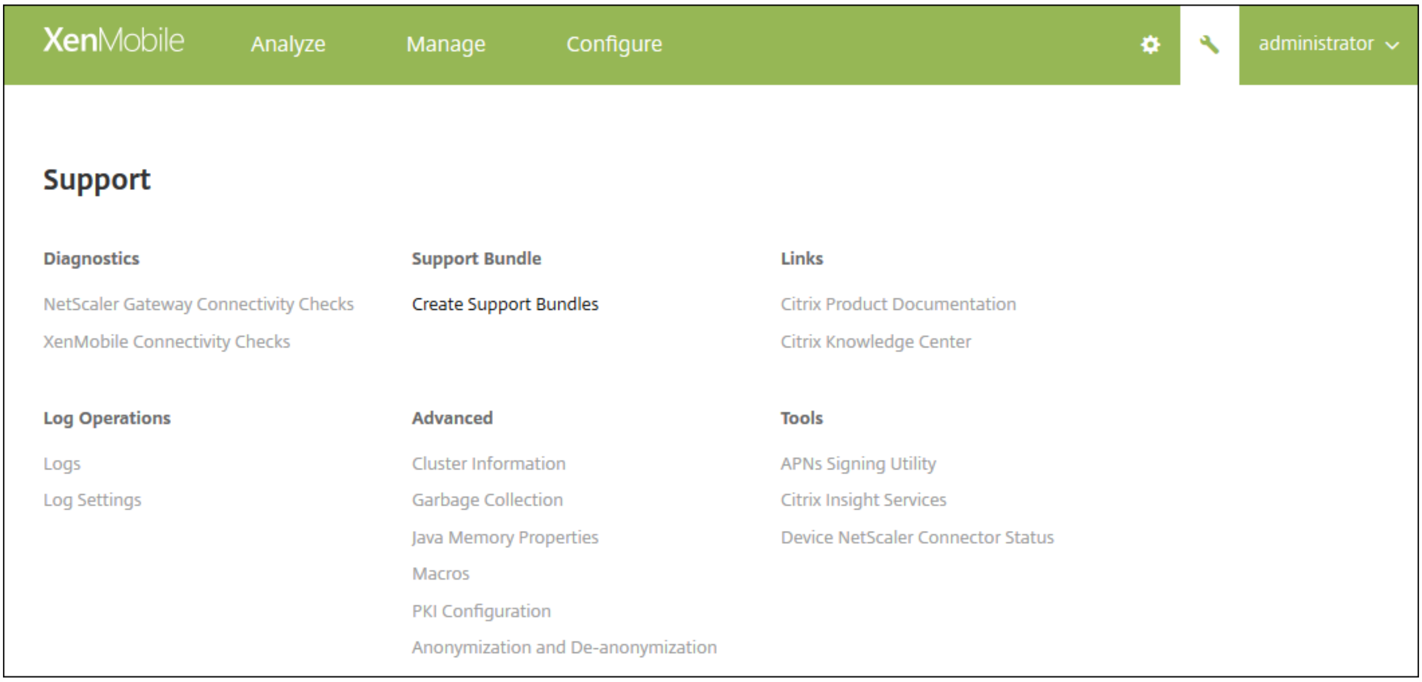
8. Use the fully qualified domain name (FQDN) of XenMobile to open the XenMobile console in a web browser.

9. In the XenMobile console, click the wrench icon in the upper-right corner of the console.



The **Support** page opens.

10. Under **Advanced**, click **Cluster Information**.



Support

Diagnostics
NetScaler Gateway Connectivity Checks
XenMobile Connectivity Checks

Support Bundle
Create Support Bundles

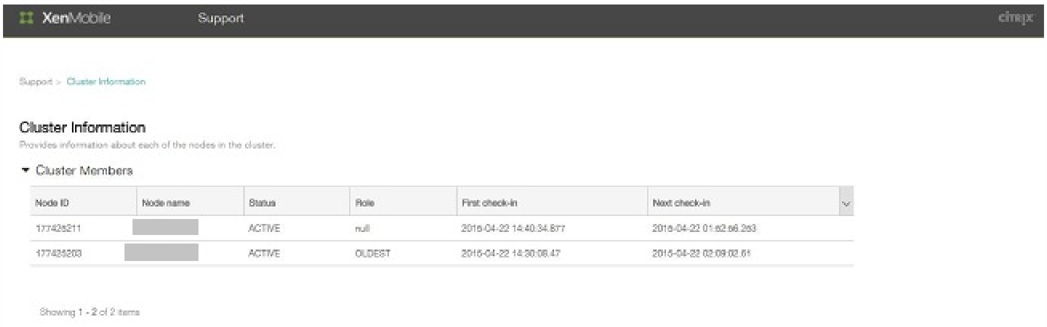
Links
Citrix Product Documentation
Citrix Knowledge Center

Log Operations
Logs
Log Settings

Advanced
Cluster Information
Garbage Collection
Java Memory Properties
Macros
PKI Configuration
Anonymization and De-anonymization

Tools
APNs Signing Utility
Citrix Insight Services
Device NetScaler Connector Status

All of the information about the cluster, including cluster member, device connection information, tasks, and so on, appear. The new node is now a member of the cluster.



Support > Cluster Information

Cluster Information

Provides information about each of the nodes in the cluster.

▾ Cluster Members

Node ID	Node name	Status	Role	First check-in	Next check-in
177426211	[redacted]	ACTIVE	null	2016-04-22 14:40:34.877	2016-04-22 01:52:56.263
177426203	[redacted]	ACTIVE	OLDEST	2016-04-22 14:30:08.47	2016-04-22 02:09:02.61

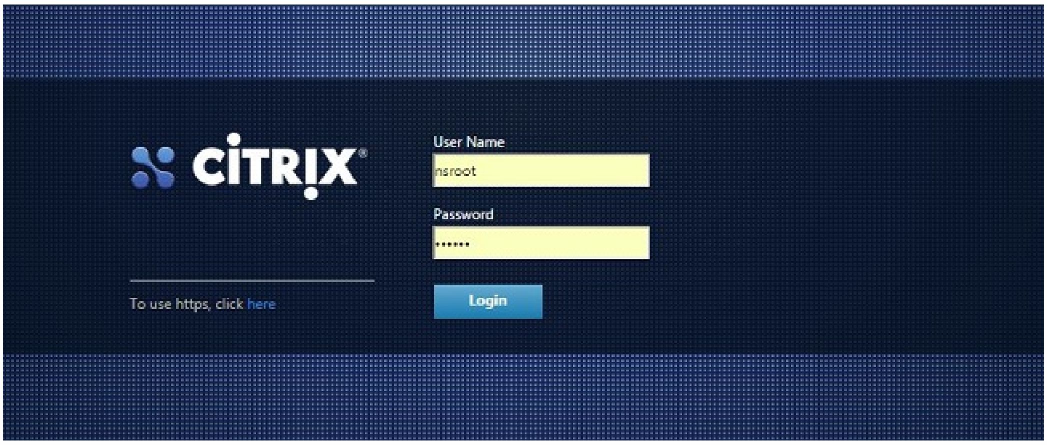
Showing 1 - 2 of 2 items

You can add other nodes by following the same steps. The first cluster added to the node has a Role of **OLDEST**. Clusters added after that will show a Role of **NONE** or **null**.

To configure load balancing for the XenMobile cluster in NetScaler

After you add the required nodes as members of the XenMobile cluster, you need to load balance the nodes to be able to access the clusters. Load balancing is done by running XenMobile Wizard available in NetScaler 10.5.x. You can following the steps in this procedure to load balance XenMobile by running the wizard.

1. Log on to NetScaler.

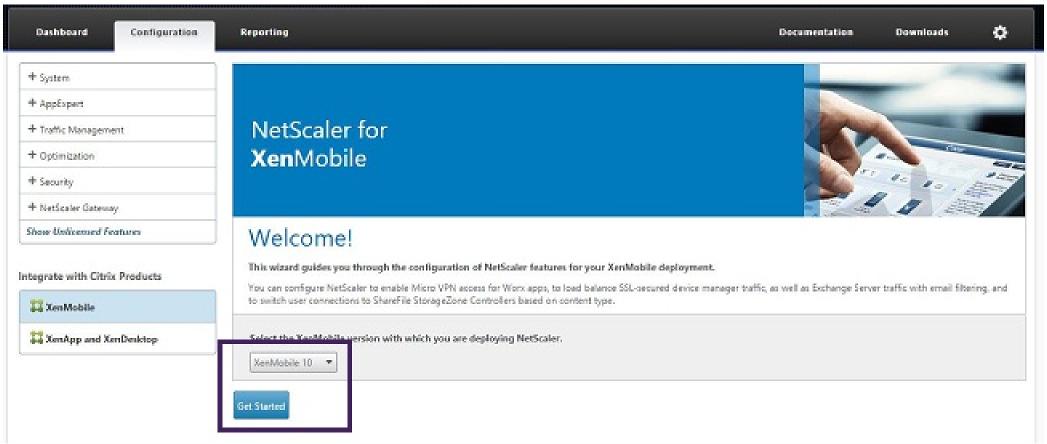


User Name: nsroot

Password: ••••••

To use https, click here

2. On the Configuration tab, click XenMobile and then click Get Started.



NetScaler for XenMobile

Welcome!

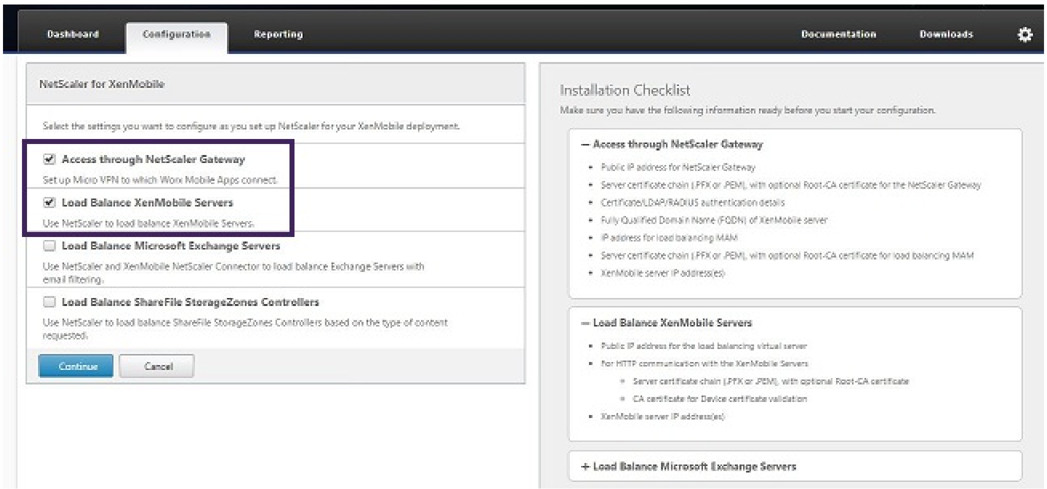
This wizard guides you through the configuration of NetScaler features for your XenMobile deployment.

You can configure NetScaler to enable Micro VPN access for Worx apps, to load balance SSL-secured device manager traffic, as well as Exchange Server traffic with email filtering, and to switch user connections to ShareFile StorageZone Controllers based on content type.

Select the XenMobile version with which you are deploying NetScaler.

XenMobile 10

3. Select the Access through NetScaler Gateway check box and the Load Balance XenMobile Servers check box and then click Continue.



NetScaler for XenMobile

Select the settings you want to configure as you set up NetScaler for your XenMobile deployment.

☑ Access through NetScaler Gateway
Set up Micro VPN to which Worx Mobile Apps connect.

☑ Load Balance XenMobile Servers
Use NetScaler to load balance XenMobile Servers.

□ Load Balance Microsoft Exchange Servers
Use NetScaler and XenMobile NetScaler Connector to load balance Exchange Servers with email filtering.

□ Load Balance ShareFile StorageZones Controllers
Use NetScaler to load balance ShareFile StorageZones Controllers based on the type of content requested.

Installation Checklist

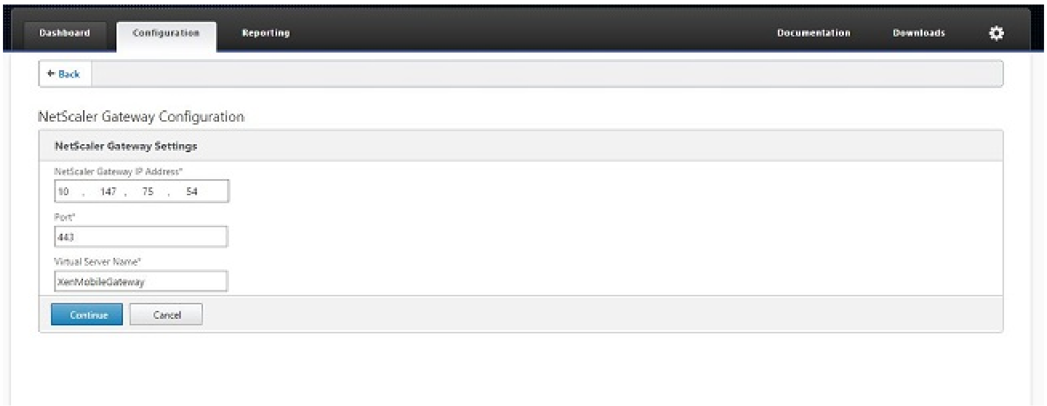
Make sure you have the following information ready before you start your configuration.

– Access through NetScaler Gateway
- Public IP address for NetScaler Gateway
- Server certificate chain (.PFX or .PEM), with optional Root-CA certificate for the NetScaler Gateway
- Certificate/LDAP/RADIUS authentication details
- Fully Qualified Domain Name (FQDN) of XenMobile server
- IP address for load balancing MAM
- Server certificate chain (.PFX or .PEM), with optional Root-CA certificate for load balancing MAM
- XenMobile server IP address(es)

– Load Balance XenMobile Servers
- Public IP address for the load balancing virtual server
- For HTTP communication with the XenMobile Servers
  - Server certificate chain (.PFX or .PEM), with optional Root-CA certificate
  - CA certificate for Device certificate validation
- XenMobile server IP address(es)

+ Load Balance Microsoft Exchange Servers

4. Enter the IP address for NetScaler Gateway and then click Continue.



NetScaler Gateway Configuration

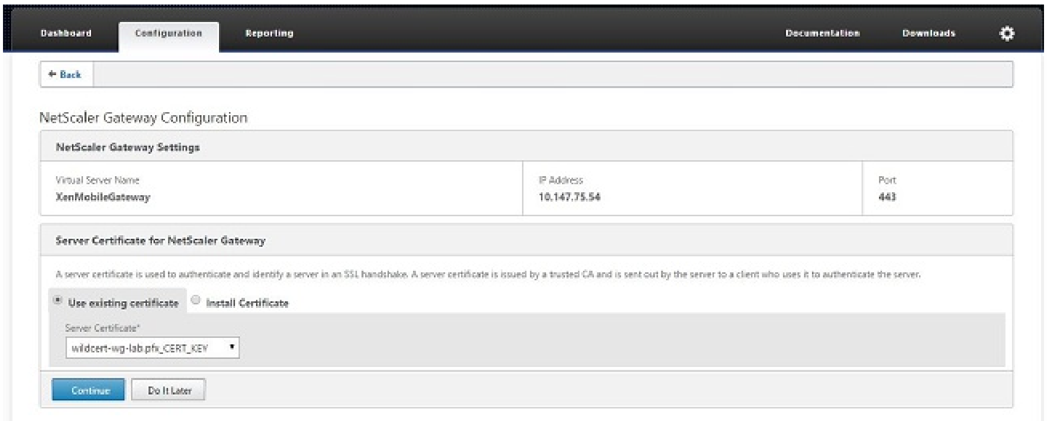
NetScaler Gateway Settings

NetScaler Gateway IP Address*: 10 . 147 . 75 . 54

Port*: 443

Virtual Server Name*: XenMobileGateway

5. Bind the server certificate to the NetScaler Gateway virtual IP address by doing one of the following and then click Continue.
   - In Use existing certificate, choose the server certificate from the list.
   - Click the Install Certificate tab to upload a new server certificate.



NetScaler Gateway Configuration

NetScaler Gateway Settings

Virtual Server Name: XenMobileGateway
IP Address: 10.147.75.54
Port: 443

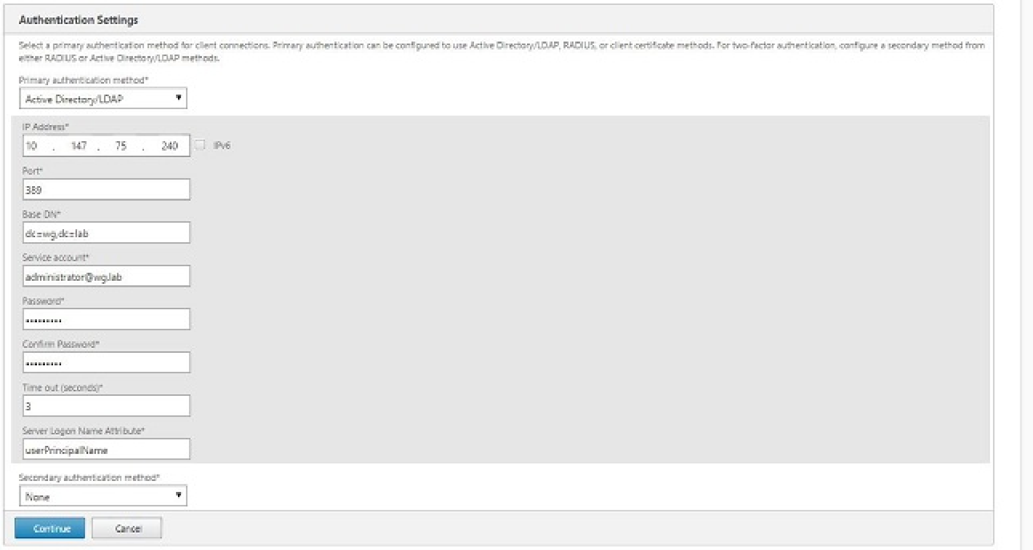
Server Certificate for NetScaler Gateway

A server certificate is used to authenticate and identify a server in an SSL handshake. A server certificate is issued by a trusted CA and is sent out by the server to a client who uses it to authenticate the server.

● Use existing certificate ○ Install Certificate

Server Certificate*: wildcert-wg-lab.pfx_CERT_KEY

6. Enter the Authentication server details and then click Continue.



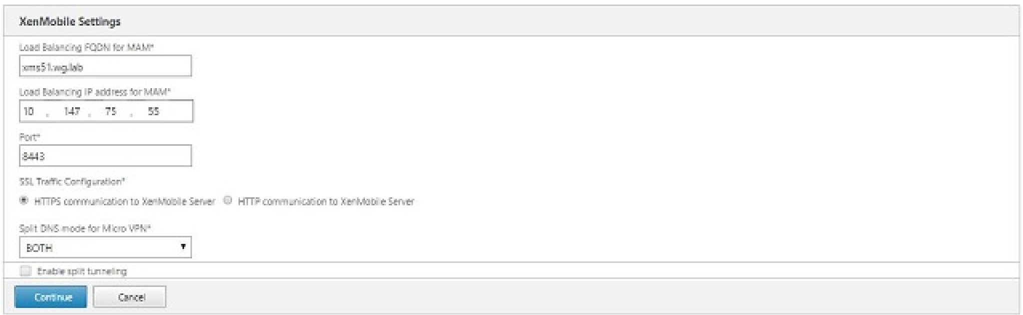
Authentication Settings

Select a primary authentication method for client connections. Primary authentication can be configured to use Active Directory/LDAP, RADIUS, or client certificate methods. For two-factor authentication, configure a secondary method from either RADIUS or Active Directory/LDAP methods.

Primary authentication method*: Active Directory/LDAP
IP Address*: 10 . 147 . 75 . 240 □ IPv6
Port*: 389
Base DN*: dc=wg,dc=lab
Service account*: administrator@wg.lab
Password*: ••••••••••
Confirm Password*: ••••••••••
Time out (seconds)*: 3
Server Logon Name Attribute*: userPrincipalName
Secondary authentication method*: None

Note: Make sure the Server Logon Name Attribute is same as you provided in the XenMobile LDAP configuration.

7. Under XenMobile settings, enter the Load Balancing FQDN for MAM and then click Continue.

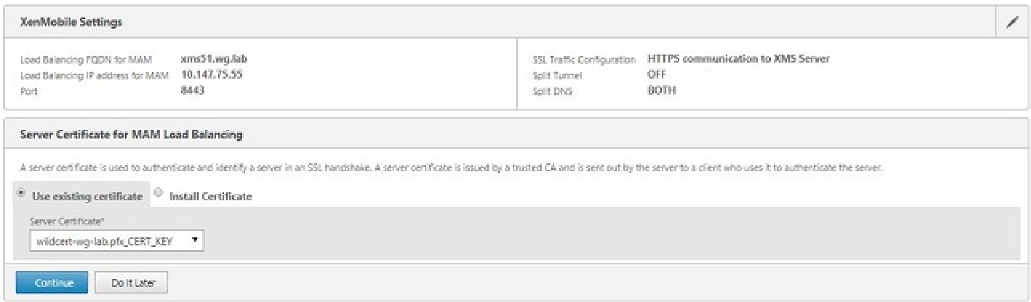


XenMobile Settings

Load Balancing FQDN for MAM*: xms51.wg.lab
Load Balancing IP address for MAM*: 10 . 147 . 75 . 55
Port*: 8443
SSL Traffic Configuration*: ● HTTPS communication to XenMobile Server ○ HTTP communication to XenMobile Server
Split DNS mode for Micro VPN*: BOTH
□ Enable split tunneling

Note: Make sure the FQDN of the MAM load balancing virtual IP address and the FQDN of XenMobile are the same.

8. If you want to use SSL Bridge mode (HTTPS), select HTTPS communication to XenMobile Server. However, if you want to use SSL offload, select HTTP communication to XenMobile Server, as shown in the preceding figure. For the purposes of this article, the choice is SSL Bridge mode (HTTPS).
9. Bind the server certificate for the MAM load balancing virtual IP address and then click Continue.



XenMobile Settings

Load Balancing FQDN for MAM xms51.wg.lab
Load Balancing IP address for MAM 10.147.75.55
Port 8443

SSL Traffic Configuration HTTPS communication to XMS Server
Split Tunnel OFF
Split DNS BOTH

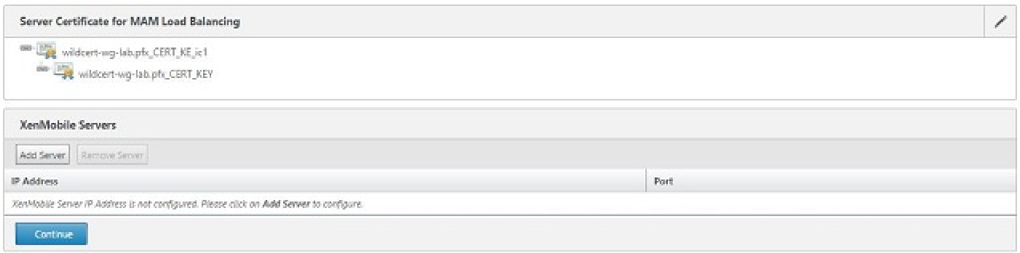
Server Certificate for MAM Load Balancing

A server certificate is used to authenticate and identify a server in an SSL handshake. A server certificate is issued by a trusted CA and is sent out by the server to a client who uses it to authenticate the server.

● Use existing certificate ○ Install Certificate

Server Certificate*: wildcert-wg-lab.pfx_CERT_KEY

10. Under XenMobile Servers, click Add Server to add the XenMobile nodes.



Server Certificate for MAM Load Balancing

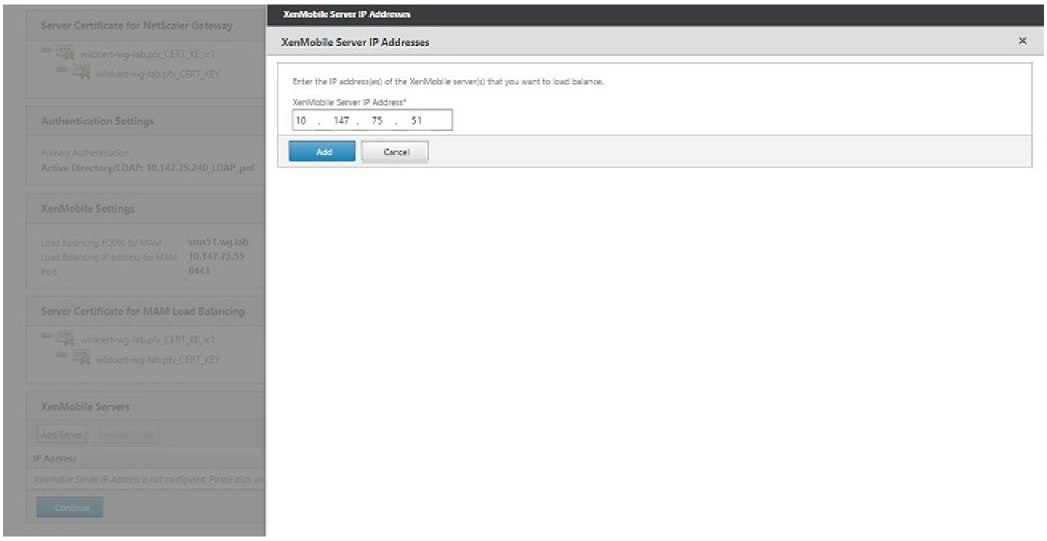
wildcert-wg-lab.pfx_CERT_KE_ic1
wildcert-wg-lab.pfx_CERT_KEY

XenMobile Servers

IP Address	Port

*XenMobile Server IP Address is not configured. Please click on **Add Server** to configure.*

11. Enter the IP address of the XenMobile node and then click Add.

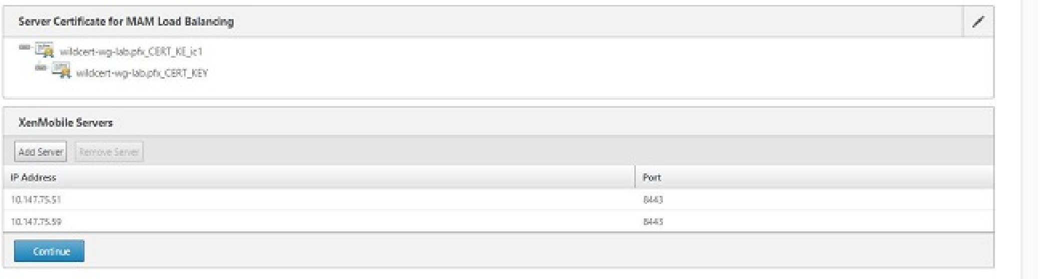


XenMobile Server IP Addresses

Enter the IP address(es) of the XenMobile server(s) that you want to load balance.

XenMobile Server IP Address*: 10 . 147 . 75 . 51

12. Repeat steps 10 and 11 to add additional XenMobile nodes that are part of the XenMobile cluster. You will see all the XenMobile nodes that you have added. Click Continue.



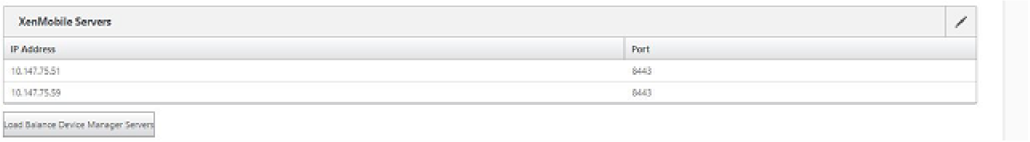
Server Certificate for MAM Load Balancing

wildcert-wg-lab.pfx_CERT_KE_ic1
wildcert-wg-lab.pfx_CERT_KEY

XenMobile Servers

IP Address	Port
10.147.75.51	8443
10.147.75.59	8443

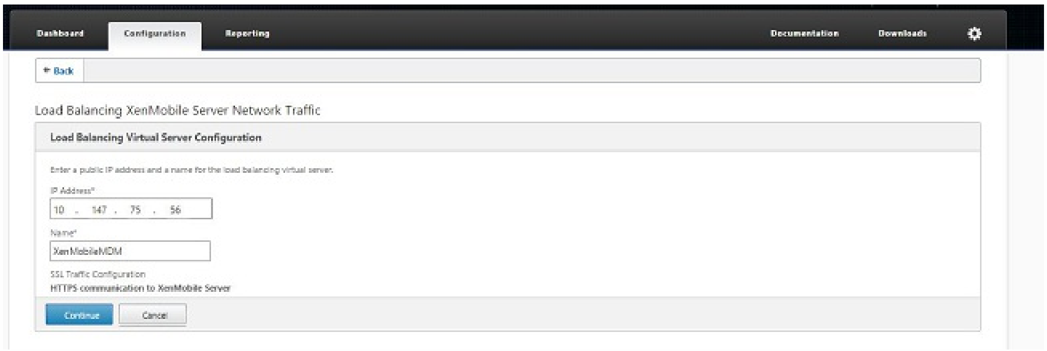
13. Click Load Balance Device Manager Servers to continue with the MDM load balancing configuration.



XenMobile Servers

IP Address	Port
10.147.75.51	8443
10.147.75.59	8443

14. Enter the IP address to be used for MDM load balancing IP address and then click Continue.



Load Balancing XenMobile Server Network Traffic

Load Balancing Virtual Server Configuration

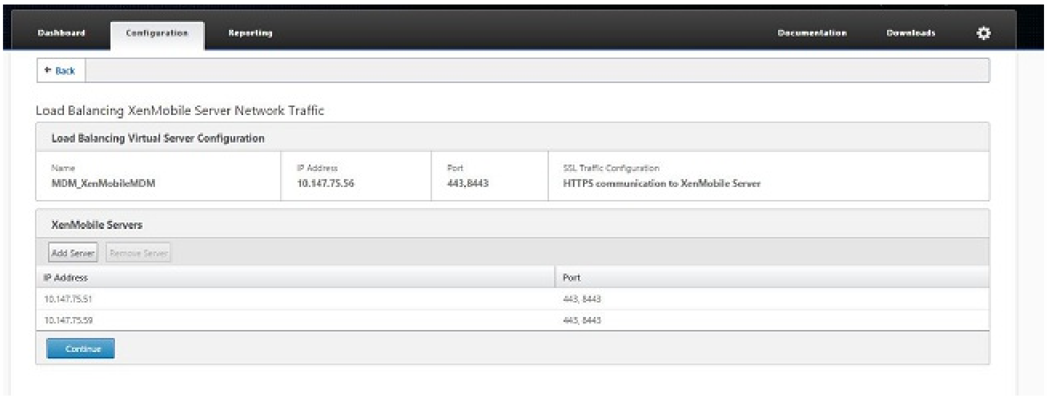
Enter a public IP address and a name for the load balancing virtual server.

IP Address*: 10 . 147 . 75 . 56

Name*: XenMobileMDM

SSL Traffic Configuration: HTTPS communication to XenMobile Server

15. Once you see the XenMobile nodes in the list, click Continue and then click Done to finish the process.



Load Balancing XenMobile Server Network Traffic

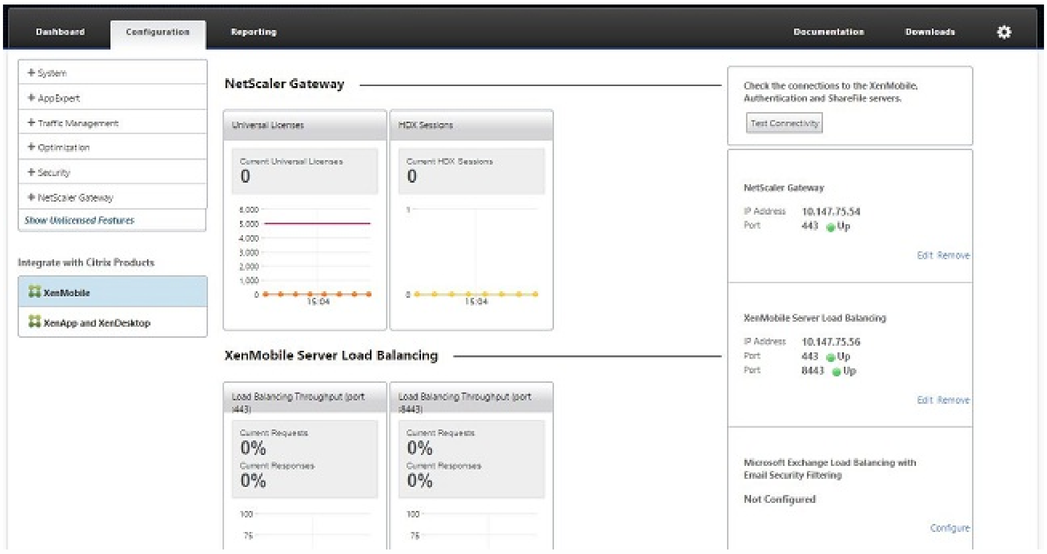
Load Balancing Virtual Server Configuration

Name	IP Address	Port	SSL Traffic Configuration
MDM_XenMobileMDM	10.147.75.56	443,8443	HTTPS communication to XenMobile Server

XenMobile Servers

IP Address	Port
10.147.75.51	443, 8443
10.147.75.59	443, 8443

You will see the virtual IP address status on the XenMobile page.



Check the connections to the XenMobile, Authentication and ShareFile servers.

NetScaler Gateway

IP Address 10.147.75.54
Port 443 ● Up

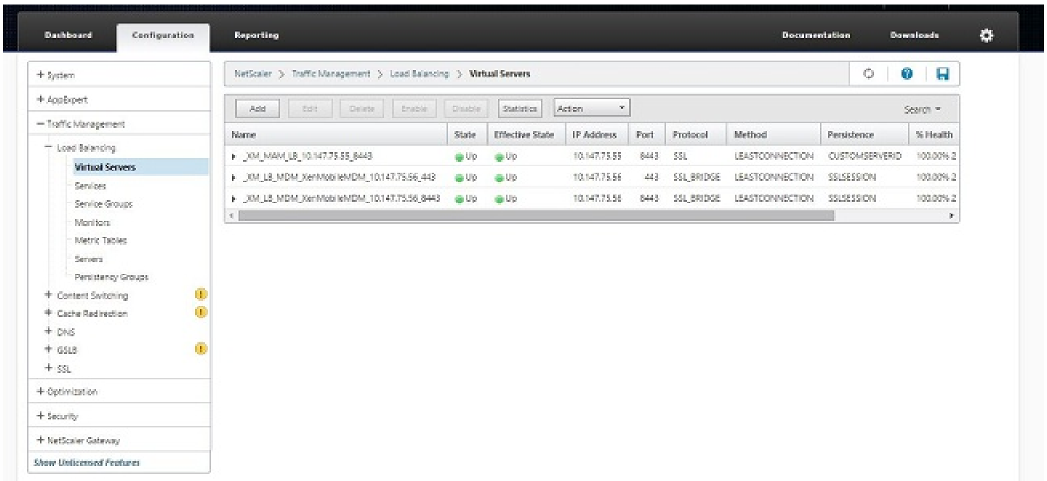
XenMobile Server Load Balancing

IP Address 10.147.75.56
Port 443 ● Up
Port 8443 ● Up

Microsoft Exchange Load Balancing with Email Security Filtering

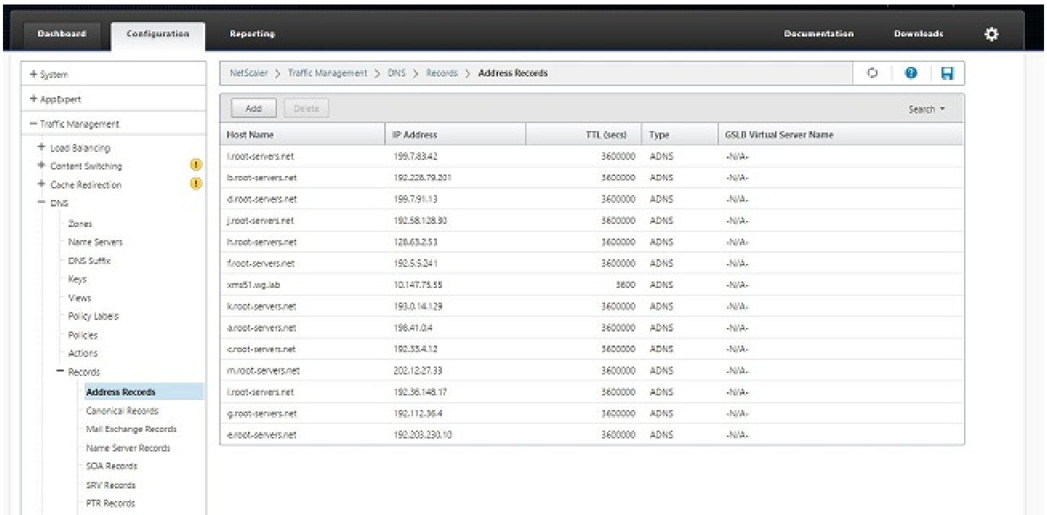
Not Configured

16. To confirm if the virtual IP addresses are up and running, click the Configuration tab and then navigate to Traffic Management > Load Balancing > Virtual Servers.



Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health
_XM_MAM_LB_10.147.75.55_8443	● Up	● Up	10.147.75.55	8443	SSL	LEASTCONNECTION	CUSTOMSERVERID	100.00% 2
_XM_LB_MDM_XenMobileMDM_10.147.75.56_443	● Up	● Up	10.147.75.56	443	SSL_BRIDGE	LEASTCONNECTION	SSLSESSION	100.00% 2
_XM_LB_MDM_XenMobileMDM_10.147.75.56_8443	● Up	● Up	10.147.75.56	8443	SSL_BRIDGE	LEASTCONNECTION	SSLSESSION	100.00% 2

You will also see that the DNS entry in NetScaler points to the MAM load balancing virtual IP address.



Host Name	IP Address	TTL (secs)	Type	GSLB Virtual Server Name
l.root-servers.net	199.7.83.42	3600000	ADNS	-N/A-
b.root-servers.net	192.228.79.201	3600000	ADNS	-N/A-
d.root-servers.net	199.7.91.13	3600000	ADNS	-N/A-
j.root-servers.net	192.58.128.30	3600000	ADNS	-N/A-
h.root-servers.net	128.63.2.53	3600000	ADNS	-N/A-
f.root-servers.net	192.5.5.241	3600000	ADNS	-N/A-
xms51.wg.lab	10.147.75.55	3600	ADNS	-N/A-
k.root-servers.net	193.0.14.129	3600000	ADNS	-N/A-
a.root-servers.net	198.41.0.4	3600000	ADNS	-N/A-
c.root-servers.net	192.33.4.12	3600000	ADNS	-N/A-
m.root-servers.net	202.12.27.33	3600000	ADNS	-N/A-
i.root-servers.net	192.36.148.17	3600000	ADNS	-N/A-
g.root-servers.net	192.112.36.4	3600000	ADNS	-N/A-
e.root-servers.net	192.203.230.10	3600000	ADNS	-N/A-

Disaster recovery guide

Sep 06, 2017

You can architect and configure XenMobile deployments that include multiple sites for disaster recovery using an active-passive failover strategy. For details, see the XenMobile Deployment Handbook Disaster Recovery article.

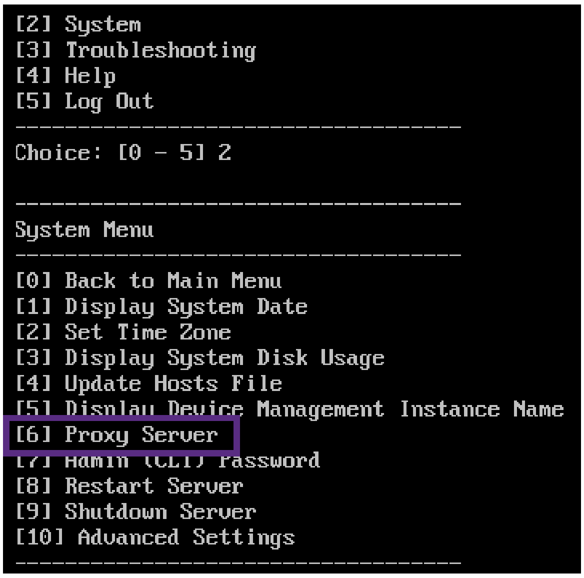
Enable proxy servers

Sep 06, 2017

When you want to control outbound internet traffic, you can set up a proxy server in XenMobile to carry that traffic. To do this, you need to set up the proxy server through the command-line interface (CLI). Note that setting up the proxy server requires restarting your system.

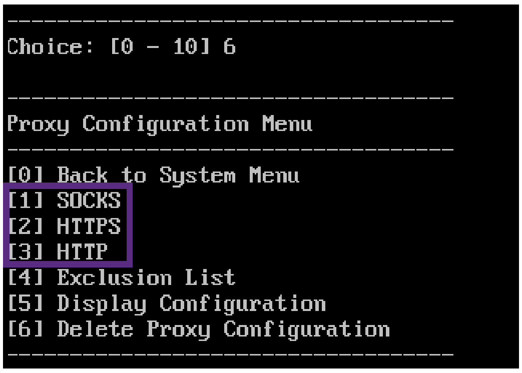
1. In the XenMobile CLI main menu, type **2** to select the System Menu.

2. In the System Menu, type **6** to select the Proxy Server Menu.



```
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----------------------------------
Choice: [0 - 5] 2

-----------------------------------
System Menu
-----------------------------------
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Display System Disk Usage
[4] Update Hosts File
[5] Display Device Management Instance Name
[6] Proxy Server
[7] Admin (CLI) Password
[8] Restart Server
[9] Shutdown Server
[10] Advanced Settings
-----------------------------------
```

3. In the Proxy Configuration Menu, type **1** to select SOCKS, **2** to select HTTPS, or **3** to select HTTP.

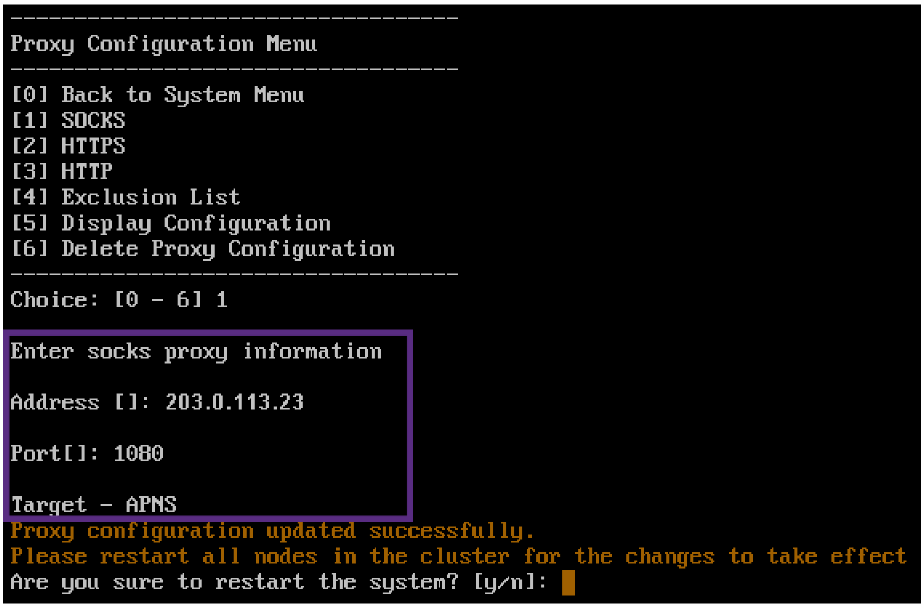


```
-----------------------------------
Choice: [0 - 10] 6

-----------------------------------
Proxy Configuration Menu
-----------------------------------
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----------------------------------
```

4. Type your proxy server IP address, port number, and target. See the following table for supported target types for each proxy server type.

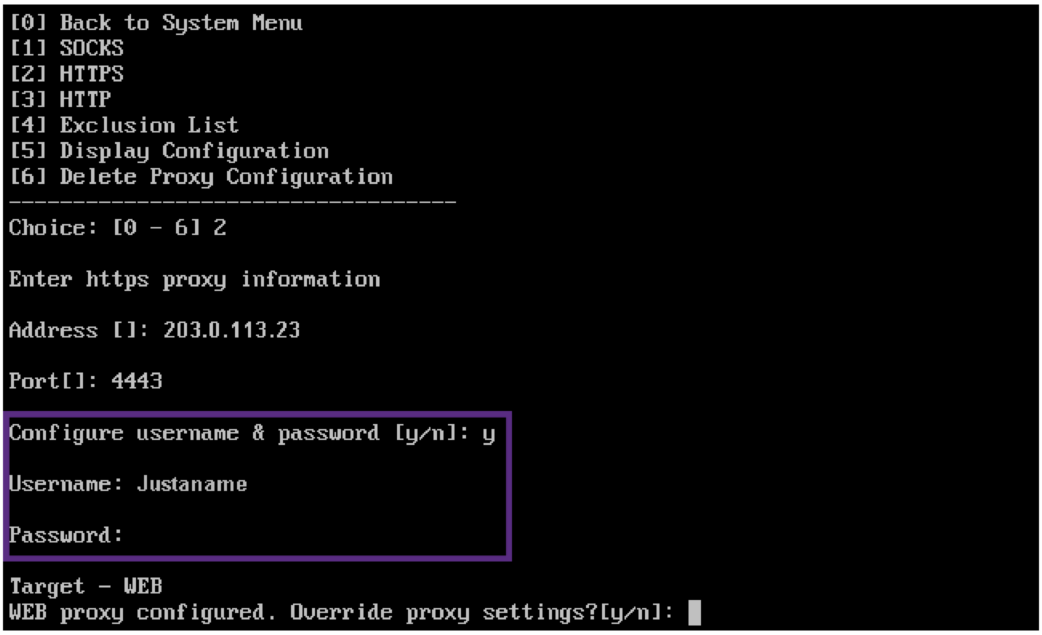
Proxy type	**Supported targets**
SOCKS	APNS

HTTP	APNS, Web. PKI
HTTPS	Web, PKI
HTTP with authentication	Web, PKI
HTTPS with authentication	Web, PKI



```
-----------------------------------
Proxy Configuration Menu
-----------------------------------
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----------------------------------
Choice: [0 - 6] 1

Enter socks proxy information

Address []: 203.0.113.23

Port[]: 1080

Target - APNS
Proxy configuration updated successfully.
Please restart all nodes in the cluster for the changes to take effect
Are you sure to restart the system? [y/n]:
```

5. If you choose to configure a user name and password for authentication on your HTTP or HTTPS proxy server, type **y**, and then type the user name and password.



```
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----------------------------------
Choice: [0 - 6] 2

Enter https proxy information

Address []: 203.0.113.23

Port[]: 4443

Configure username & password [y/n]: y

Username: Justaname

Password:

Target - WEB
WEB proxy configured. Override proxy settings?[y/n]:
```

6. Type **y** to finish setting up your proxy server.

SQL Server drivers

Jan 29, 2018

XenMobile Service uses the jTDS driver for connections to SQL Server.

As of XenMobile Server 10.7 RP 2: For connections to SQL Server from an on-premises XenMobile Server, you can use the default driver, jTDS, or the Microsoft Java Database Connectivity (JDBC) driver. The jTDS driver is the default driver when you install XenMobile Server on-premises or upgrade from a XenMobile Server that's configured to use the jTDS driver.

For both drivers, XenMobile supports SQL Server authentication or Windows authentication. For those combinations of authentication and driver, SSL can be on or off.

When you use Windows authentication with the Microsoft JDBC driver, the driver uses integrated authentication with Kerberos. XenMobile contacts Kerberos to obtain the Kerberos Key Distribution Center (KDC) details. If the required details aren't available, the XenMobile CLI prompts for the IP address of the Active Directory server.

To switch from the jTDS driver to the JDBC driver, SSH to all your XenMobile Server nodes and use the XenMobile CLI for configuration. The steps vary according to your current jTDS driver configuration, as follows.

Switch to Microsoft JDBC (SSL is off; SQL Server authentication)

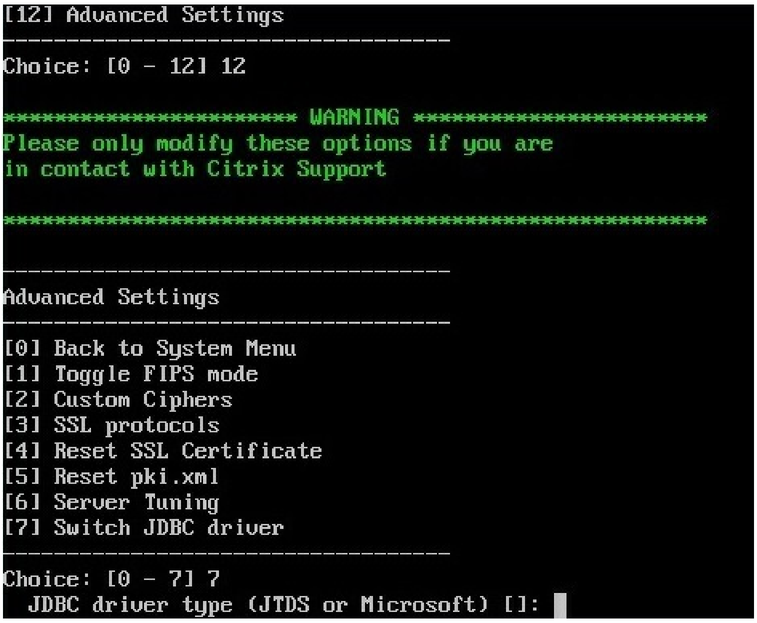
To complete these steps, you need the SQL Server user name and password.

1. SSH to all XenMobile Server nodes.

2. In the XenMobile CLI main menu, type **2** to select the System Menu.

3. Type **12** to select Advanced Settings.

4. Type **7** to select Switch JDBC driver, and then type **m** for Microsoft.



```
[12] Advanced Settings
-----------------------------------
Choice: [0 - 12] 12

*********************** WARNING ***********************
Please only modify these options if you are
in contact with Citrix Support

*******************************************************

-----------------------------------
Advanced Settings
-----------------------------------
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] SSL protocols
[4] Reset SSL Certificate
[5] Reset pki.xml
[6] Server Tuning
[7] Switch JDBC driver
-----------------------------------
Choice: [0 - 7] 7
  JDBC driver type (JTDS or Microsoft) []:
```

5. When prompted, type **y** to choose SQL authentication and then type the SQL Server user name and password.

6. Repeat the steps for each XenMobile Server node.

7. Restart each XenMobile Server node.

Switch to Microsoft JDBC (SSL is off; Windows authentication)

To complete these steps, you need the Active Directory user name and password, the Kerberos KDC realm, and the KDC user name.

1. SSH to all XenMobile Server nodes.
2. In the XenMobile CLI main menu, type **2** to select the System Menu.
3. Type **12** to select Advanced Settings.
4. Type **7** to select Switch JDBC driver, and then type **m**.
5. When prompted whether to use SQL Server authentication, type **n**.
6. When prompted, type the Active Directory user name and password configured for the SQL server.
7. If XenMobile doesn't auto-discover the Kerberos KDC realm, it prompts for the KDC details, including the SQL server FQDN.
8. When prompted whether to use SSL, type **n**. XenMobile saves the configuration. If XenMobile can't save the configuration because of errors, it shows an error message and the details that you entered.
9. Repeat the steps for each XenMobile Server node.
10. Restart each XenMobile Server node.

Server properties

Jan 29, 2018

XenMobile has many properties that apply to server-wide operations. This article describes many of the server properties and details how to add, edit, or delete server properties.

Some properties are Custom Keys. To add a custom key, click **Add** and then, from **Key**, choose **Custom Key**.

For information about the properties typically configured, see Server Properties in the XenMobile virtual handbook.

Server Property Definitions

Add Device Always:

- If **true**, XenMobile adds a device to the XenMobile console, even if it fails enrollment, so 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 XenMobile from generating multiple certificates for a device in a short time period. Citrix recommends that you not change this value. Defaults to **30** minutes.

Audit Log Cleanup Execution Time:

- The time to start the audit log cleanup, formatted as HH:MM AM/PM. Example: 04:00 AM. Defaults to **02:00 AM**.

Audit Log Cleanup Interval (in Days):

- The number of days that XenMobile retains the audit log. Defaults to **1**.

Audit Logger:

- If **False**, does not log user interface (UI) events. Defaults to **False**.

Audit Log Retention (in Days):

- The number of days that XenMobile retains the audit log. Defaults to **7**.

auth.ldap.connect.timeout and **auth.ldap.read.timeout**:

- To compensate for slow LDAP responses, Citrix recommends that you add server properties for the following Custom Keys.

  Key: **Custom Key**
  Key: **auth.ldap.connect.timeout**
  Value: **60000**
  Display name: **auth.ldap.connect.timeout=60000**
  Description: LDAP connection timeout

  Key: **Custom Key**

Key: **auth.ldap.read.timeout**
Value: **60000**
Display name: **auth.ldap.read.timeout=60000**
Description: LDAP read timeout

Certificate Renewal in Seconds:

- The number of seconds before a certificate expires that XenMobile 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, XenMobile attempts to renew the certificate. Defaults to **2592000** seconds (30 days).

Connection Timeout:

- The session inactivity timeout, in minutes, after which XenMobile closes the TCP connection to a device. The session remains open. Applies to Android and Windows CE devices and Remote Support. Defaults to **5** minutes.

Connection Timeout to Microsoft Certification Server:

- The number of seconds that XenMobile waits for a response from the certificate server. If the certificate server is slow and has much traffic, 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).

Default deployment channel:

- Determines how XenMobile deploys a resource to a device: At the user-level (**DEFAULT_TO_USER**) or device-level. Defaults to **DEFAULT_TO_DEVICE**.

Deploy Log Cleanup (in Days):

- The number of days that XenMobile retains the deployment log. Defaults to **7**.

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 VPP 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 your XenMobile Server

  - The Microsoft CA server is the certificate issuer

  - An internal CA, whose root XenMobile Server doesn't trust, signed your certificate.

  Defaults to **True**.

Enable Console:

- If **true**, enables user access to the Self Help Portal Console. Defaults to **true**.

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 XenMobile 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. XenMobile 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**.

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, 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 XenMobile pulls a complete list (baseline) of ActiveSync allowed and denied users. Defaults to **28800** seconds.

hibernate.c3p0.max_size:

- This Custom Key determines the maximum number of connections that XenMobile can open to the SQL Server database. XenMobile uses the value you specify for this custom key as an upper limit. The connections open only if you need them. Base your settings on the capacity of your database server. For more information, see Tuning XenMobile Operations. Configure the key as follows. Default is **1000**.

Key: **hibernate.c3p0.max_size**
Value: **500**
Display name: **hibernate.c3p0.max_size=*nnn***
Description: DB connections to SQL

hibernate.c3p0.timeout:

- This Custom Key determines the idle time-out. Default is **300**.

  Key: **Custom Key**
  Key: **hibernate.c3p0.timeout**
  Value: **30**
  Display name: **hibernate.c3p0.timeout=30**
  Description: Database idle timeout

Identifies if telemetry is enabled or not:

- Identifies if telemetry (Customer Experience Improvement Program, or CEIP) is enabled. You can opt in to CEIP when you install or upgrade XenMobile. If XenMobile has 15 consecutive failed uploads, it disables telemetry. Defaults to **false**.

Inactivity Timeout in Minutes:

- If the **WebServices timeout type** server property is **INACTIVITY_TIMEOUT:** This property defines the number of minutes after which XenMobile logs out an inactive administrator who did the following:
  - Used the XenMobile Public API for REST Services to access the XenMobile console
  - Used the XenMobile Public API for REST Services to access any third-party app. A timeout of **0** means that an inactive user remains logged in.

    Defaults to **5**.

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 First Step Delayed:

- After a user enters their credentials during device enrollment, this value specifies how long to wait before prompting for the root CA. 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 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 XenMobile 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 XenMobile iOS agent identities. Defaults to **1024**.

iOS Device Management Identity Renewal Days:

- Specifies the number of days before the certificate expiration that XenMobile 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, XenMobile issues a new certificate. Defaults to **30** days.

iOS MDM APNS Private Key Password:

- This property contains the APNs password, which is required for XenMobile to push notifications to Apple servers.

Length of Inactivity Before Device Is Disconnected:

- Specifies how long a device can remain inactive, including the last authentication, before XenMobile 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 a large number of VPP licenses. Defaults to **3**. If you need further optimization, you can increase the number of threads. However, be aware that with a larger number of threads, such as 6, a VPP import results in very high CPU usage.

NetScaler Single Sign-On:

- If **False**, disables the XenMobile callback feature during single signon from NetScaler to XenMobile. If the NetScaler Gateway configuration includes a callback URL, XenMobile uses the callback feature to verify the NetScaler Gateway session ID. Defaults to **False**.

Number of consecutive failed uploads:

- Displays the number of consecutive failures during Customer Experience Improvement Program (CEIP) uploads. XenMobile increments the value when an upload fails. After 15 upload failures, XenMobile disables CEIP, also called telemetry. For more information, see the server property **Identifies if telemetry is enabled or not**. XenMobile 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 XenMobile 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 XenMobile 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**.

Session Log Cleanup (in Days):

- The number of days that XenMobile retains the session log. Defaults to **7**.

Server Mode:

- Determines whether XenMobile runs in MAM, MDM, or ENT (enterprise) mode, corresponding to app management, device management, or app and device management. Set the Server Mode property according to how you want devices to register, as noted in the table below. Server Mode defaults to **ENT**, regardless of license type.

  If you have a XenMobile MDM Edition license, the effective server mode is always MDM regardless of how you set the server mode in Server Properties. If you have an MDM Edition license, you cannot enable app management by setting the server mode to either MAM or ENT.

Your licenses are this Edition	You want devices to register in this mode	Set Server Mode property to
Enterprise / Advanced	MDM mode	MDM
Enterprise / Advanced	MDM+MAM mode	ENT
MDM	MDM mode	MDM

The effective server mode is a combination of the license type and server mode. For an MDM license, the effective server mode is always MDM, regardless of the server mode setting. For Enterprise and Advanced licenses, the effective server mode matches the server mode, if the server mode is **ENT** or **MDM**. If the server mode is **MAM**, the effective server mode is ENT.

XenMobile adds the server mode to the server log for each of these activities: A license is activated, a license is deleted, and you change the server mode in Server Properties. For information about creating and viewing log files, see Logs and View and analyze log files in XenMobile.

ShareFile configuration type:

- Specifies the ShareFile storage type. **ENTERPRISE** enables ShareFile Enterprise mode. **CONNECTORS** provides access only to StorageZone Connectors that you create through the XenMobile console. Defaults to **NONE**, which shows the initial view of the **Configure > ShareFile** screen where you choose between ShareFile Enterprise and Connectors. Defaults to **NONE**.

Static Timeout in Minutes:

- If the **WebServices timeout type** server property is **STATIC_TIMEOUT**: This property defines the number of minutes after which XenMobile logs out an administrator after using the following:
  - The XenMobile Public API for REST Services to access the XenMobile console.
  - The XenMobile 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 for Work. XenMobile needs this property if the Android for Work 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 XenMobile to Windows devices. Defaults to **False**.

Use ActiveSync ID to Conduct an ActiveSync Wipe Device:

- If **true**, XenMobile Mail Manager uses the ActiveSync identifier as an argument for the asWipeDevice method. Defaults to **false**.

User-Defined Device Properties N:

- 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 XenMobile database, you can create deployment rules based on the value of the properties.

  Key: **Custom Key**
  Key: **device.properties.userDefinedN**
  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**.

VPP baseline interval:

- The minimum interval that XenMobile reimports VPP licenses from Apple. Refreshing license information ensures that XenMobile reflects all changes, such as when you manually delete an imported app from VPP. By default, XenMobile refreshes the VPP license baseline a minimum of every **720** minutes.

  If you have many VPP 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 VPP license changes from Apple: Citrix recommends that you lower the value to keep XenMobile updated with the changes. The minimum interval between two baselines is 60 minutes. In addition, XenMobile performs a delta import every 60 minutes, to capture the changes since the last import. Therefore, if the VPP baseline interval is 60 minutes, the interval between baselines could be delayed up to 119 minutes.

WebServices Timeout Type:

- Specifies how to expire an authentication token retrieved from the public API. If **STATIC_TIMEOUT**, XenMobile considers an authentication token as expired after the value specified in the server property **Static Timeout in Minutes**.

  If **INACTIVITY_TIMEOUT**, XenMobile considers an authentication token as expired after the token is inactive for the value specified in 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 XenMobile 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 works with the properties **Unauthenticated App download for Android** and **Unauthenticated App download for Windows**. Those properties specify whether to allow unauthenticated app downloads. Defaults to **3600000**.

XenMobile MDM Self Help Portal console max inactive interval (minutes):

- The number of minutes after which XenMobile logs out an inactive user from the XenMobile Self Help Portal. A timeout of **0** means that an inactive user remains logged in. Defaults to **30**.

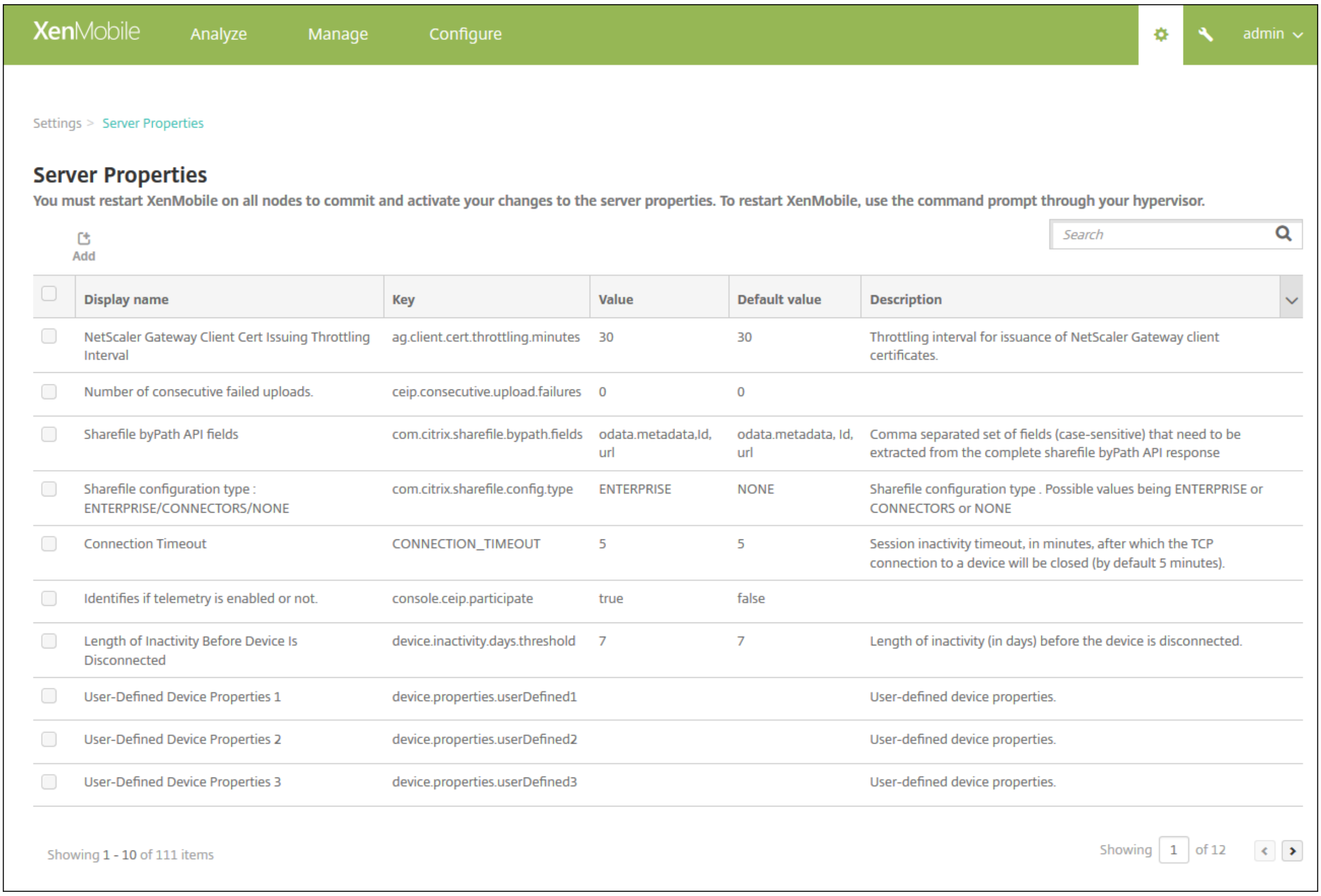
Adding, Editing, or Deleting Server Properties

In XenMobile, you can apply properties to the server. After making changes, ensure that you restart XenMobile on all nodes to commit and activate changes.

> ## Note
>
> To restart XenMobile, use the command prompt through your hypervisor.

1. In the XenMobile 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.



Server Properties

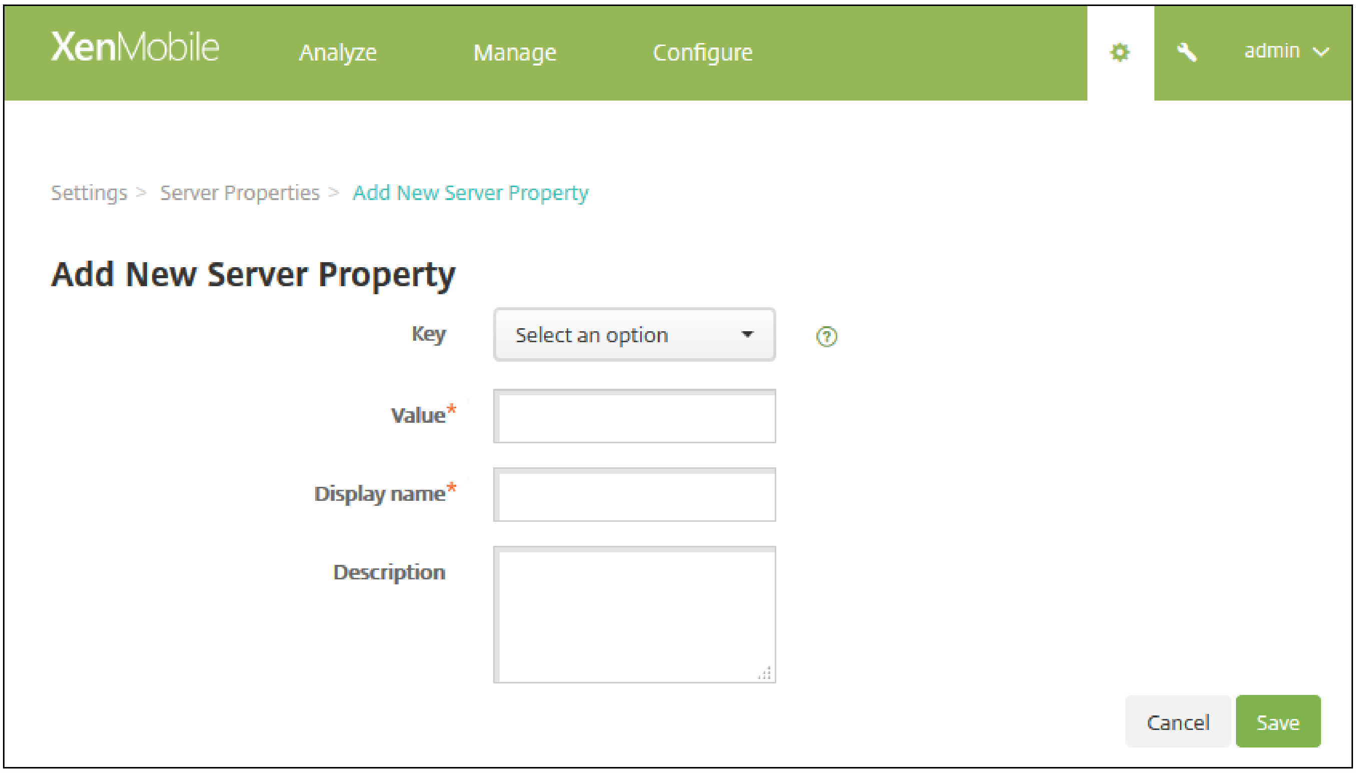
You must restart XenMobile on all nodes to commit and activate your changes to the server properties. To restart XenMobile, use the command prompt through your hypervisor.

□	Display name	Key	Value	Default value	Description
□	NetScaler Gateway Client Cert Issuing Throttling Interval	ag.client.cert.throttling.minutes	30	30	Throttling interval for issuance of NetScaler Gateway client certificates.
□	Number of consecutive failed uploads.	ceip.consecutive.upload.failures	0	0	
□	Sharefile byPath API fields	com.citrix.sharefile.bypath.fields	odata.metadata,Id, url	odata.metadata, Id, url	Comma separated set of fields (case-sensitive) that need to be extracted from the complete sharefile byPath API response
□	Sharefile configuration type : ENTERPRISE/CONNECTORS/NONE	com.citrix.sharefile.config.type	ENTERPRISE	NONE	Sharefile configuration type . Possible values being ENTERPRISE or CONNECTORS or NONE
□	Connection Timeout	CONNECTION_TIMEOUT	5	5	Session inactivity timeout, in minutes, after which the TCP connection to a device will be closed (by default 5 minutes).
□	Identifies if telemetry is enabled or not.	console.ceip.participate	true	false	
□	Length of Inactivity Before Device Is Disconnected	device.inactivity.days.threshold	7	7	Length of inactivity (in days) before the device is disconnected.
□	User-Defined Device Properties 1	device.properties.userDefined1			User-defined device properties.
□	User-Defined Device Properties 2	device.properties.userDefined2			User-defined device properties.
□	User-Defined Device Properties 3	device.properties.userDefined3			User-defined device properties.

Showing 1 - 10 of 111 items

Showing 1 of 12

1. Click **Add**. The **Add New Server Property** page appears.



Add New Server Property

Key: Select an option

Value*

Display name*

Description

2. Configure these settings:

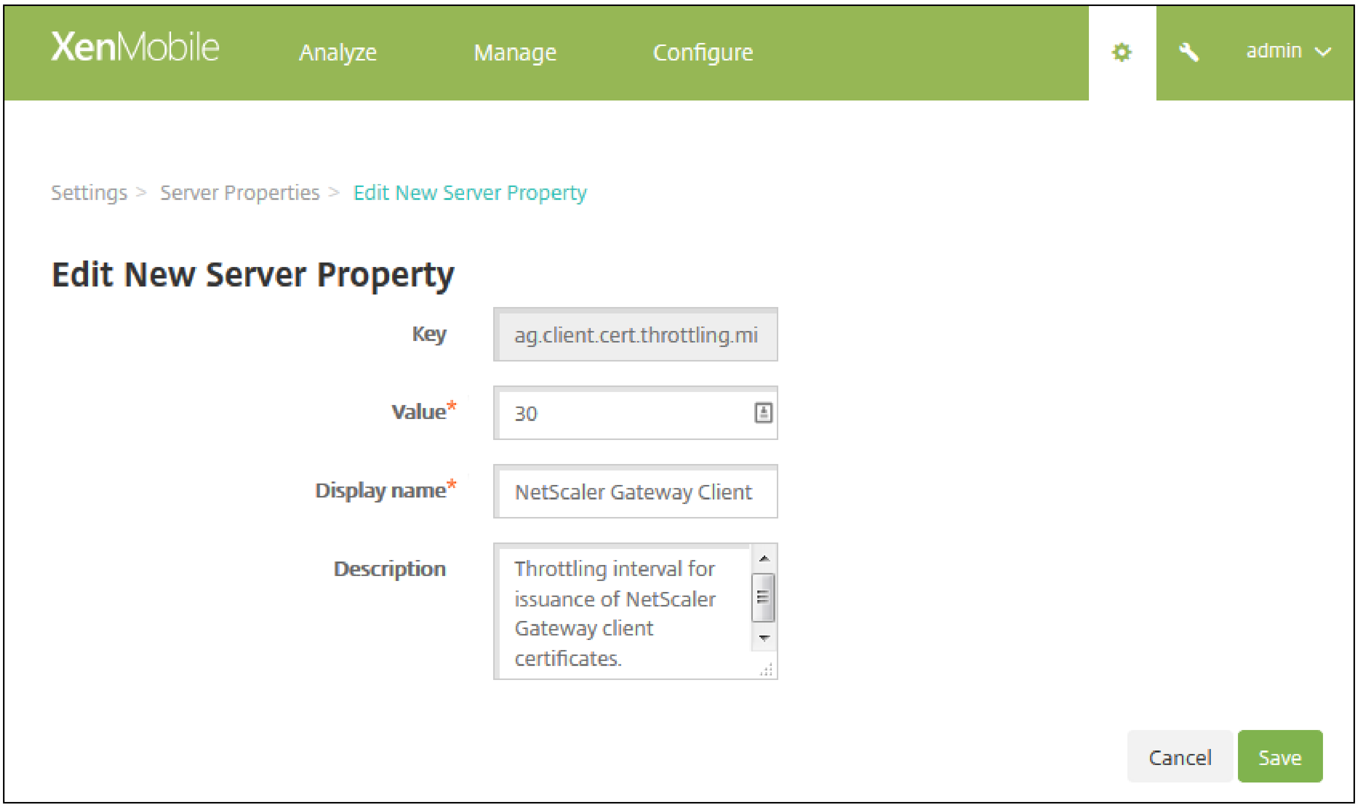
- **Key**: In the list, select the appropriate key. Keys are case-sensitive. Contact Citrix Support before you edit property values or to request a special key.
- **Value**: Enter a value depending on the key you selected.
- **Display name**: Enter a name for the new property value that appears in the **Server Properties** table.
- **Description**: Optionally, type a description for the new server property.

3. Click **Save**.

1. In the **Server Properties** table, select the server property you want to edit.

> **Note**: When you select the check box next to a server property, the options menu appears above the server 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 New Server Property** page appears.



Settings > Server Properties > Edit New Server Property

Edit New Server Property

Key: ag.client.cert.throttling.mi

Value*: 30

Display name*: NetScaler Gateway Client

Description: Throttling interval for issuance of NetScaler Gateway client certificates.

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.

1. In the **Server Properties** table, select the server property you want to delete.

   Note: 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.

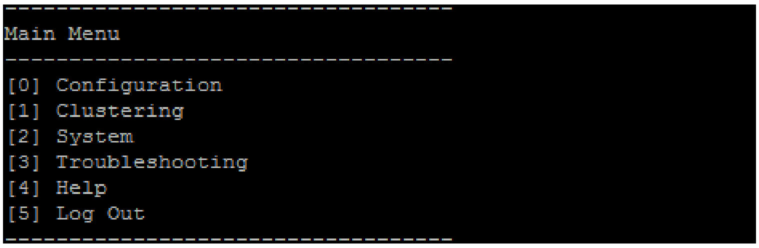
Command-line interface options

Dec 01, 2017

For an on-premises installation of XenMobile Server, you can access the CLI options at any time as follows:

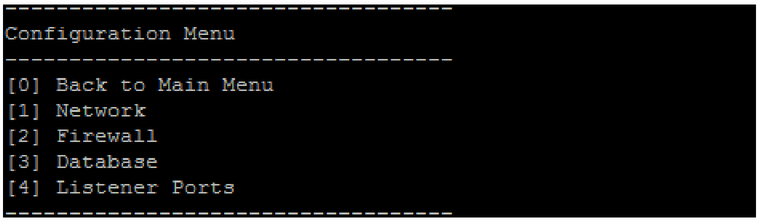
- **From the hypervisor on which you installed XenMobile**: In your hypervisor, select the imported XenMobile virtual machine, start the command prompt view, and log on to your administrator account for XenMobile. For details, see the documentation for your hypervisor.
- **If SSH is enabled in your firewall, by using SSH**. Log on to your administrator account for XenMobile.

You can perform various configuration and troubleshooting tasks using the CLI. Following is the top-level menu for the CLI.



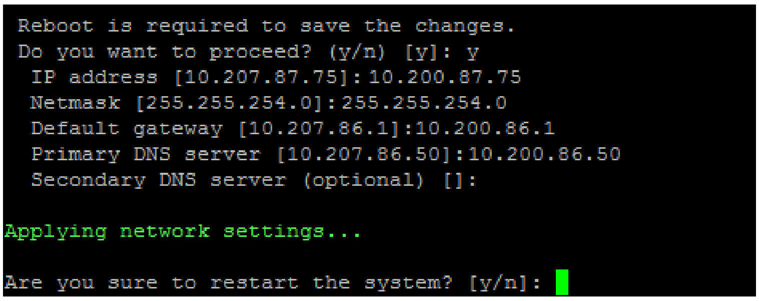
```
-----------------------------------
Main Menu
-----------------------------------
[0] Configuration
[1] Clustering
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----------------------------------
```

Following are samples of the **Configuration Menu** and the settings displayed for each option.



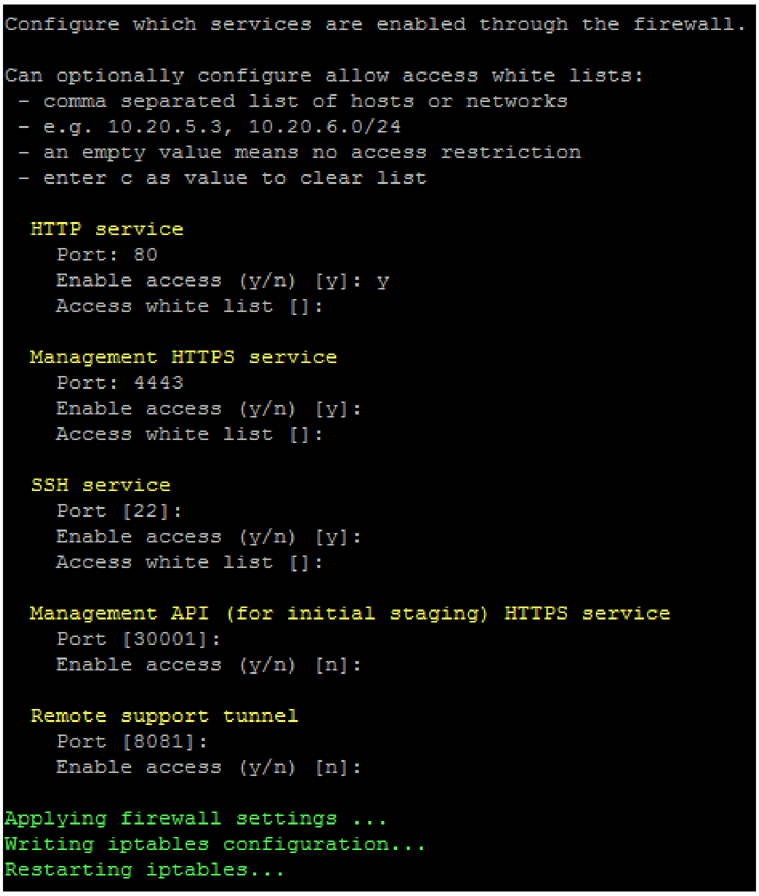
```
-----------------------------------
Configuration Menu
-----------------------------------
[0] Back to Main Menu
[1] Network
[2] Firewall
[3] Database
[4] Listener Ports
-----------------------------------
```

[1] Network



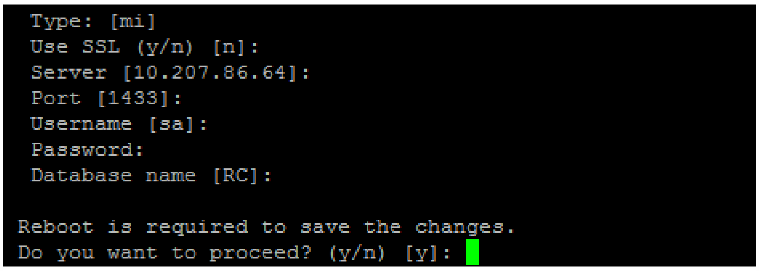
```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  IP address [10.207.87.75]:10.200.87.75
  Netmask [255.255.254.0]:255.255.254.0
  Default gateway [10.207.86.1]:10.200.86.1
  Primary DNS server [10.207.86.50]:10.200.86.50
  Secondary DNS server (optional) []:

Applying network settings...

Are you sure to restart the system? [y/n]:
```

[2] Firewall



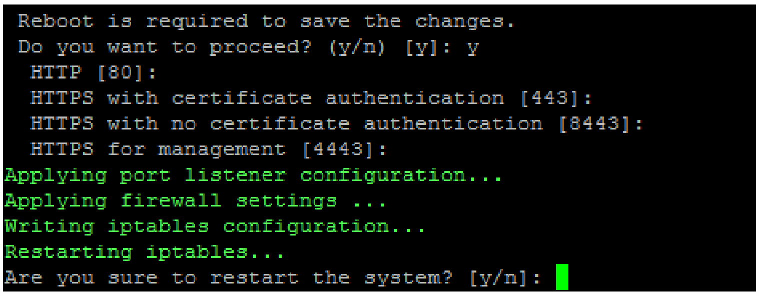
```
Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:
 - comma separated list of hosts or networks
 - e.g. 10.20.5.3, 10.20.6.0/24
 - an empty value means no access restriction
 - enter c as value to clear list

  HTTP service
    Port: 80
    Enable access (y/n) [y]: y
    Access white list []:

  Management HTTPS service
    Port: 4443
    Enable access (y/n) [y]:
    Access white list []:

  SSH service
    Port [22]:
    Enable access (y/n) [y]:
    Access white list []:

  Management API (for initial staging) HTTPS service
    Port [30001]:
    Enable access (y/n) [n]:

  Remote support tunnel
    Port [8081]:
    Enable access (y/n) [n]:

Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
```

[3] Database



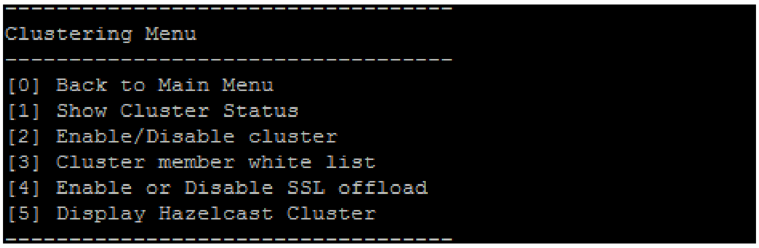
```
  Type: [mi]
  Use SSL (y/n) [n]:
  Server [10.207.86.64]:
  Port [1433]:
  Username [sa]:
  Password:
  Database name [RC]:

 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]:
```

[4] Listener Ports



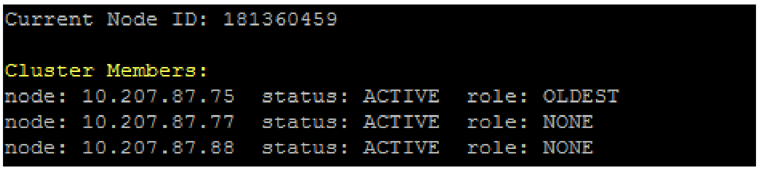
```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  HTTP [80]:
  HTTPS with certificate authentication [443]:
  HTTPS with no certificate authentication [8443]:
  HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]:
```

Following are samples of the **Clustering Menu** and the settings displayed for each option.



```
-----------------------------------
Clustering Menu
-----------------------------------
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----------------------------------
```

[1] Show Cluster Status



```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75  status: ACTIVE  role: OLDEST
node: 10.207.87.77  status: ACTIVE  role: NONE
node: 10.207.87.88  status: ACTIVE  role: NONE
```

[2] Enable/Disable cluster

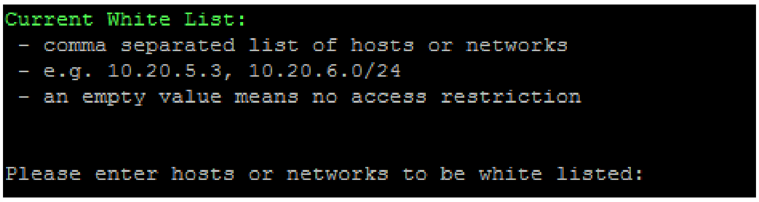
When you choose to enable clustering, the following message appears:

> To enable real-time communication between cluster members, please open port 80 using the Firewall menu option in CLI menu. Also configure Access white list under Firewall settings for restricted access.

When you choose to disable clustering, the following message appears:

> You have chosen to disable clustering. Access to port 80 is not needed. Please disable it.

[3] Cluster member white list



```
Current White List:
 - comma separated list of hosts or networks
 - e.g. 10.20.5.3, 10.20.6.0/24
 - an empty value means no access restriction


Please enter hosts or networks to be white listed:
```

[4] Enable or disable SSL offload

When you select to enable or disable SSL offloading, the following message appears:

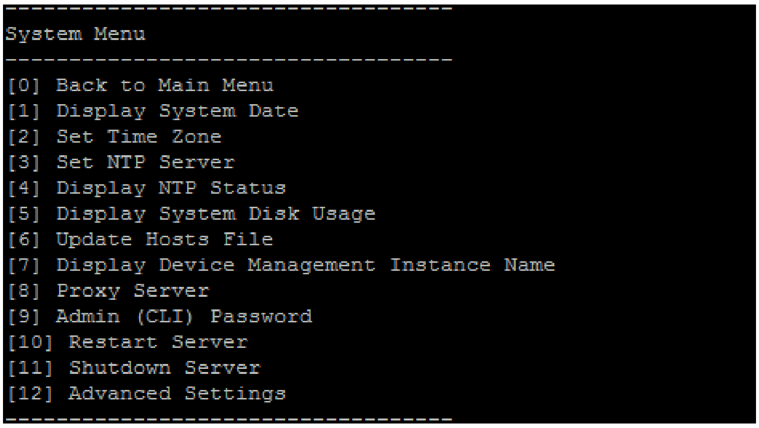
> Enabling SSL offload opens port 80 for everyone. Please configure Access white list under Firewall settings for restricted access.

[5] Display Hazelcast Cluster

When you select to display the Hazelcast Cluster, the following options appear:

> Hazelcast Cluster Members:
>
> [IP addresses listed]
>
> NOTE: If a configured node is not part of the cluster, please reboot that node.

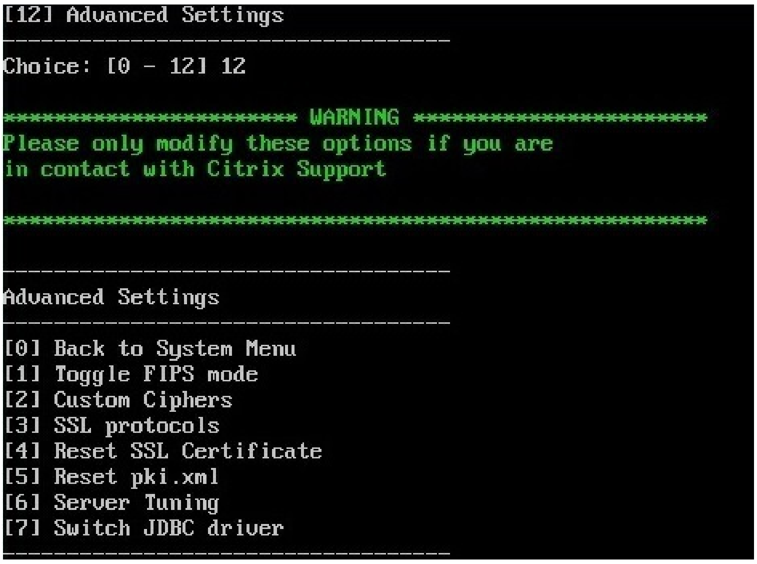
From the **System Menu**, you can display or set system-level information, restart or shut down the server, or access **Advanced Settings**.



```
-----------------------------------
System Menu
-----------------------------------
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Set NTP Server
[4] Display NTP Status
[5] Display System Disk Usage
[6] Update Hosts File
[7] Display Device Management Instance Name
[8] Proxy Server
[9] Admin (CLI) Password
[10] Restart Server
[11] Shutdown Server
[12] Advanced Settings
-----------------------------------
```

Set NTP Server enables you to specify NTP server information. If you have time zone issues when syncing XenMobile time with a hypervisor, you can avoid the issues by pointing XenMobile to an NTP server. Restart all cluster servers after changing this option.

[12] Advanced Settings



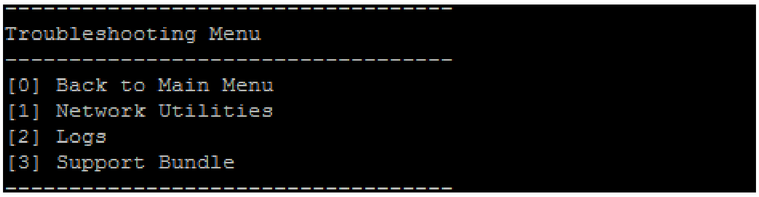
```
[12] Advanced Settings
-----------------------------------
Choice: [0 - 12] 12

*********************** WARNING ***********************
Please only modify these options if you are
in contact with Citrix Support

*******************************************************

-----------------------------------
Advanced Settings
-----------------------------------
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] SSL protocols
[4] Reset SSL Certificate
[5] Reset pki.xml
[6] Server Tuning
[7] Switch JDBC driver
-----------------------------------
```

SSL protocols options default to all allowed protocols. After the prompt **New SSL protocols to enable**, type the protocols you want to enable. XenMobile disables any protocols that you don't include in your response. For example: To disable TLSv1, type **TLSv1.2,TLSv1.1** and then type **y** to restart XenMobile Server.

Server Tuning options include the server connection timeout, maximum connections (by port), and maximum threads (by port).

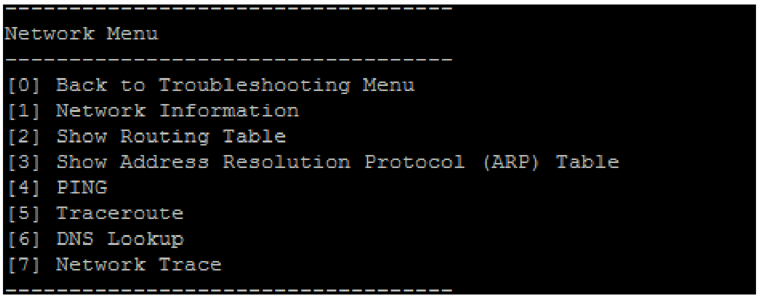
Switch JDBC driver options are **jTDS** and **Microsoft** JDBC. The default driver is jTDS. For information about switching to the Microsoft JDBC driver, see SQL Server drivers.

Following are samples of the **Troubleshooting Menu** and the settings displayed for each option.



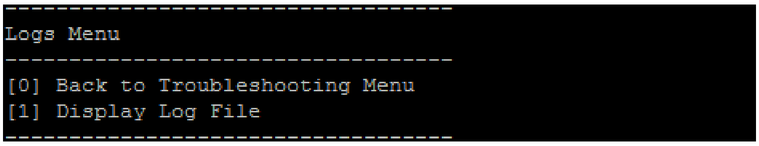
```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----------------------------------
```

[1] Network Utilities



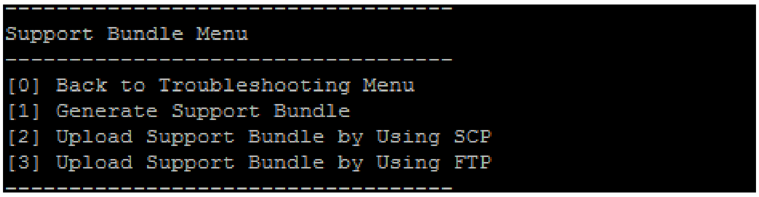
```
-----------------------------------
Network Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Network Information
[2] Show Routing Table
[3] Show Address Resolution Protocol (ARP) Table
[4] PING
[5] Traceroute
[6] DNS Lookup
[7] Network Trace
-----------------------------------
```

[2] Logs



```
-----------------------------------
Logs Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Display Log File
-----------------------------------
```

[3] Support Bundle



```
-----------------------------------
Support Bundle Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----------------------------------
```

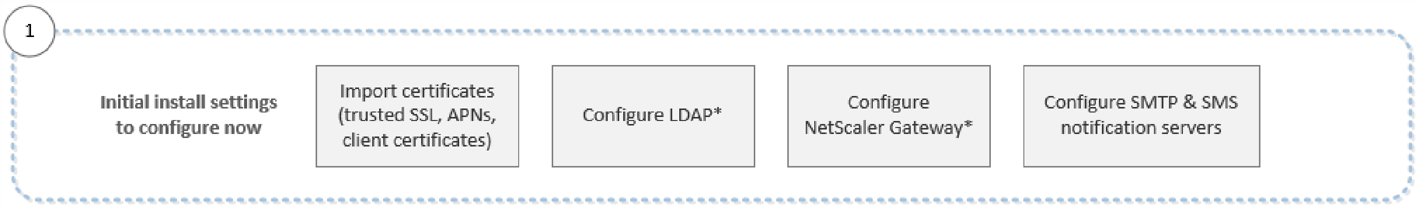
Getting started workflows for XenMobile console

Sep 06, 2017

The XenMobile console is the unified management tool in XenMobile. This article assumes you've installed XenMobile and are ready to work in the console. If you have yet to install XenMobile, see Installing XenMobile. For details on browser support for the XenMobile console, the XenMobile Compatibility article.

After you finish configuring XenMobile first in the command-line console and next in the XenMobile console, the dashboard opens. You cannot return to the initial configuration screens. If you skipped some install configurations, you can configure the following settings in the console. Before you start adding users, apps, and devices, you consider completing these install settings. To start, click the gear icon in the upper-right corner of the console.

Note: The items with an asterisk are optional.


1
Initial install settings to configure now
Import certificates (trusted SSL, APNs, client certificates)
Configure LDAP*
Configure NetScaler Gateway*
Configure SMTP & SMS notification servers

For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and sections:

- Authentication
- NetScaler Gateway and XenMobile
- Notifications

To support Android, iOS, and Windows platforms, you must have the following account-related setup.

Android

- Create Google Play credentials. For details, see Google Play Launch.
- Create an Android for Work administrator account. For details, see Android for Work.
- Verify your domain name with Google. For details, see Verify your domain for G Suite.
- Enable APIs and create a service account for Android for Work. For details, see Android enterprise Help.

iOS

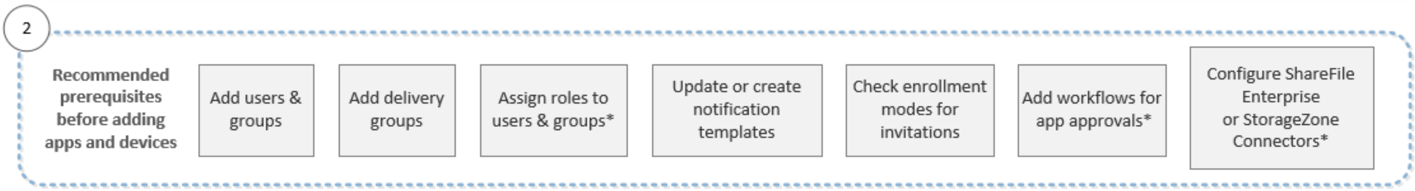
- Create an Apple ID and developer account. For details, see the Apple Developer Program website.
- Create an Apple Push Notification Service (APNs) certificate. If you plan to manage iOS devices with your XenMobile Service (cloud) deployment, you need an Apple APNs certificate. If you use push notification for your WorxMail deployment, you also need an Apple APNs certificate. For details about obtaining Apple APNs certificates, see the Apple Push Certificates Portal. For more information about XenMobile and APNs, see APNs certificates and Push Notifications for WorxMail for iOS.
- Create a Volume Purchase Program (VPP) company token. For details, see Apple Volume Purchasing Program.

Windows

- Create a Microsoft Windows Store developer account. For details, see the Microsoft Windows Dev Center.
- Obtain a Microsoft Windows Store Publisher ID. For details, see the Microsoft Windows Dev Center.
- Acquire an enterprise certificate from Symantec. For details, see the Microsoft Windows Dev Center.
- Ensure that you have a public SSL certificate available if you plan to use XenMobile autodiscovery for your Windows Phone enrollment. For details, see XenMobile Autodiscovery Service.
- Create an Application Enrollment Token (AET). For details, see the Microsoft Windows Dev Center.

This workflow shows prerequisites for you to configure before you add apps and devices.

Note: The items with an asterisk are optional.

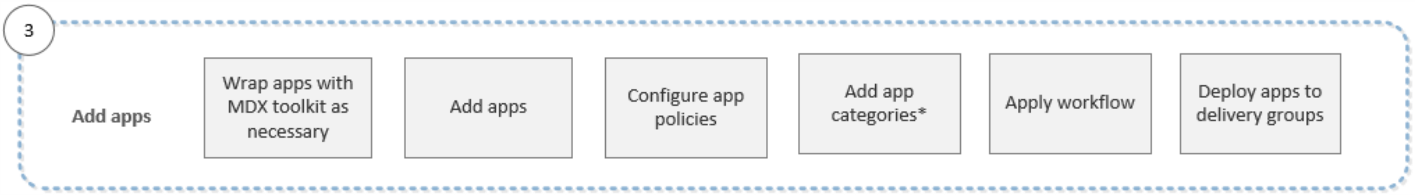

2
Recommended prerequisites before adding apps and devices
Add users & groups
Add delivery groups
Assign roles to users & groups*
Update or create notification templates
Check enrollment modes for invitations
Add workflows for app approvals*
Configure ShareFile Enterprise or StorageZone Connectors*

For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and sections:

- User accounts, roles, and enrollment
- Deploy resources
- Configure roles with RBAC
- Notifications
- Create and manage workflows
- ShareFile use with XenMobile

This workflow shows a recommended order to follow when adding apps to XenMobile.

Note: The items with an asterisk are optional.



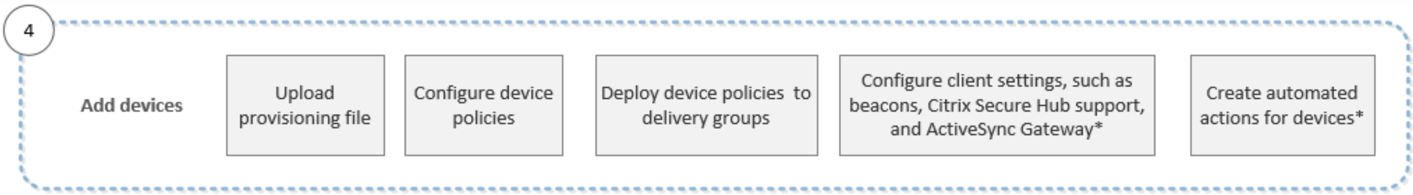
For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and sections:

- About the MDX Toolkit
- Add apps
- MDX Policies at a Glance

- Create and manage workflows
- Deploy resources

This workflow shows a recommended order to follow when adding and registering devices in XenMobile.

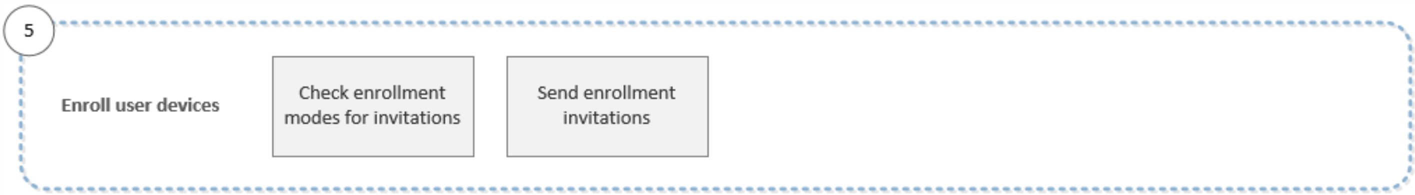
Note: The items with an asterisk are optional.


4
Add devices
Upload provisioning file
Configure device policies
Deploy device policies to delivery groups
Configure client settings, such as beacons, Citrix Secure Hub support, and ActiveSync Gateway*
Create automated actions for devices*

For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and sections:

- Devices
- Supported device operating systems
- Deploy resources
- Monitor and support
- Automated actions

This workflow shows a recommended order to follow when enrolling user devices in XenMobile.

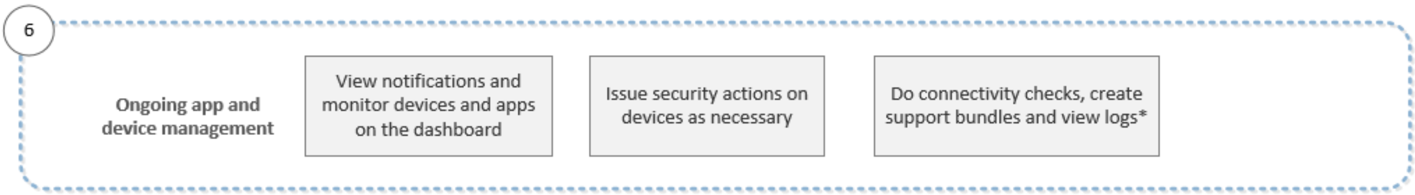

5
Enroll user devices
Check enrollment modes for invitations
Send enrollment invitations

For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles:

- User accounts, roles, and enrollment
- Notifications

This workflow shows app and device management activities that you can do in the console.

Note: The items with an asterisk are optional.


6
Ongoing app and device management
View notifications and monitor devices and apps on the dashboard
Issue security actions on devices as necessary
Do connectivity checks, create support bundles and view logs*

For more information about the support options found from clicking the wrench icon in the upper-right corner of the console, see Monitor and support.

Certificates and authentication

Feb 15, 2018

Several components play a role in authentication during XenMobile operations:

- **XenMobile Server**: The XenMobile 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 and whether to require two-factor authentication or three-factor authentication. Through client properties in XenMobile, you can enable Citrix PIN authentication and configure the complexity and expiration time of the PIN.
- **NetScaler**: NetScaler provides termination for micro VPN SSL sessions. NetScaler 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 works with XenMobile Server in enrollment operations. Secure Hub is the entity on a device that talks to NetScaler: When a session expires, Secure Hub gets an authentication ticket from NetScaler 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 the section on certificate pinning in the Secure Hub article.

  Secure Hub also facilitates the MDX security container: Secure Hub pushes policies, creates a session with NetScaler 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 NetScaler, enforce offline mode restrictions, and enforce client policies, such as time-outs.

For more information about the considerations on how to configure authentication, including an overview of single-factor, and two-factor authentication methods, see the Deployment Handbook Authentication article.

You use certificates in XenMobile 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
- SAML for single sign-on with ShareFile
- Microsoft Azure Active Directory server settings

Certificates

By default, XenMobile comes with a self-signed Secure Sockets Layer (SSL) certificate that is generated during installation to secure the communication flows to the server. Citrix recommends that you replace the SSL certificate with a trusted SSL certificate from a well-known certificate authority (CA).

> ## Note
>
> iOS 10.3 devices don't support self-signed certificates. If XenMobile uses self-signed certificates, users can't enroll iOS 10.3 devices

> into XenMobile. To enroll devices running iOS 10.3 or later into XenMobile, you must use trusted SSL certificates in XenMobile.

XenMobile 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 XenMobile-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 XenMobile, 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 XenMobile component:

XenMobile component	Certificate format	Required certificate type
NetScaler Gateway	PEM (BASE64), PFX (PKCS#12)	SSL, Root; NetScaler Gateway converts PFX to PEM automatically.
XenMobile Server	.p12 (.pfx on Windows-based computers)	SSL, SAML, APNs; XenMobile also generates a full PKI during the installation process. **Important**: XenMobile Server 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 the XenMobile server.
StoreFront	PFX (PKCS#12)	SSL, Root

XenMobile supports SSL listener certificates and client certificates with bit lengths of 4096, 2048, and 1024. Note that 1024-bit certificates are easily compromised.

For NetScaler Gateway and the XenMobile Server, 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 NetScaler Gateway or the XenMobile configuration utility. After you create the CSR, you submit it to the CA for signing. When the CA returns the signed certificate, you can install the certificate on NetScaler Gateway or XenMobile.

Each certificate you upload has an entry in the Certificates table, summarizing 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 XenMobile 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

XenMobile may or may not possess the private key for a given certificate. Likewise, XenMobile 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.

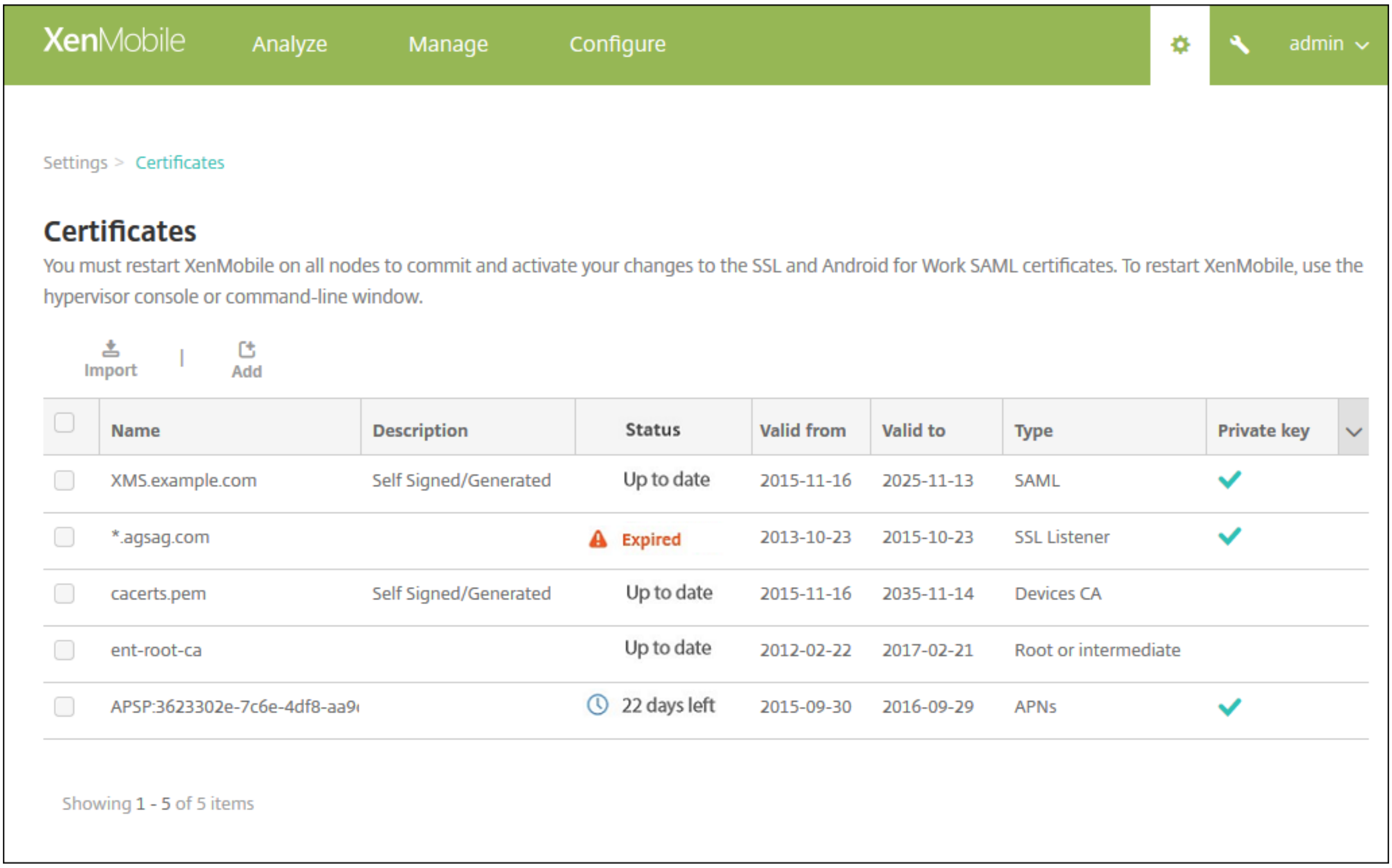
When configuring the Microsoft CA entity, you specify the CA certificate. You select the CA certificate from a list of all server certificates that are CA certificates. Likewise, when configuring client authentication, you can select from a list of all the server certificates for which XenMobile has 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 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 XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.

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



Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

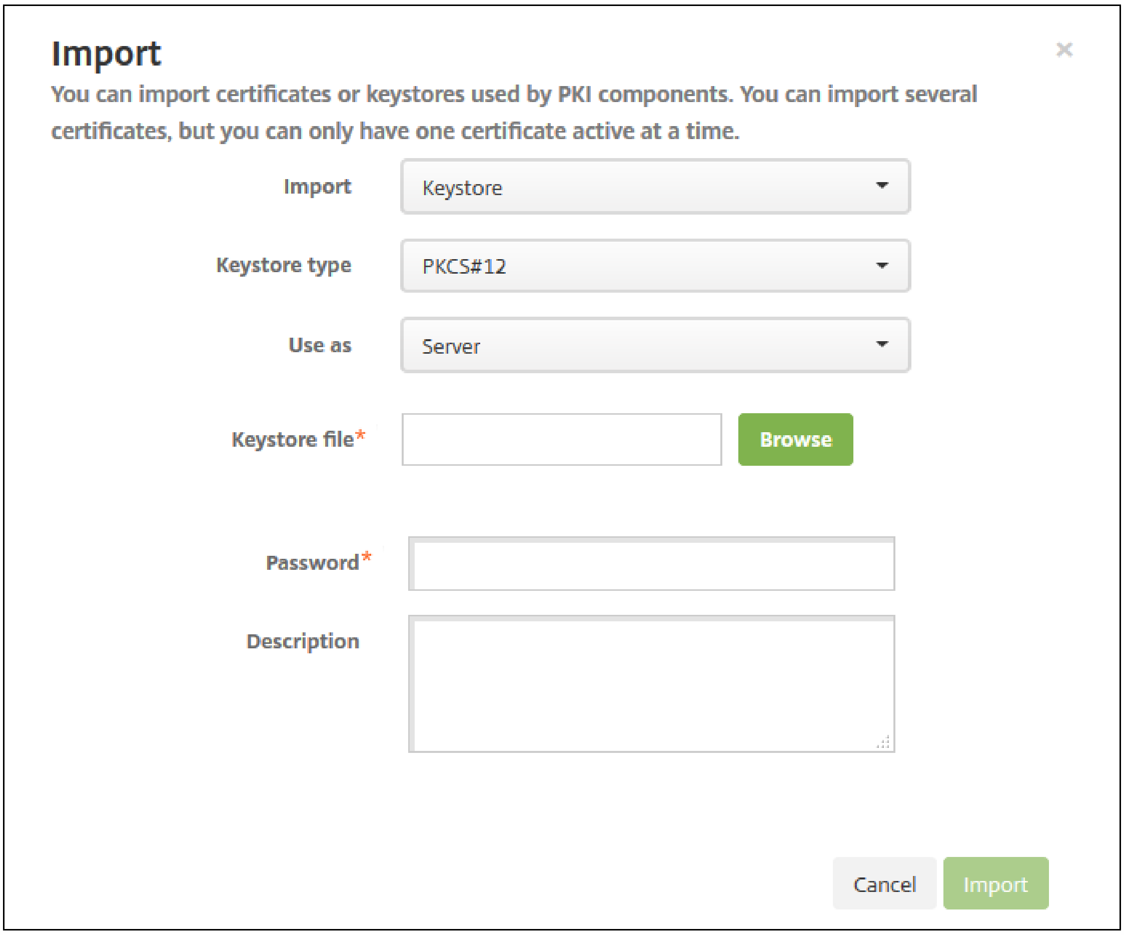
□	Name	Description	Status	Valid from	Valid to	Type	Private key
□	XMS.example.com	Self Signed/Generated	Up to date	2015-11-16	2025-11-13	SAML	✓
□	*.agsag.com		Expired	2013-10-23	2015-10-23	SSL Listener	✓
□	cacerts.pem	Self Signed/Generated	Up to date	2015-11-16	2035-11-14	Devices CA	
□	ent-root-ca		Up to date	2012-02-22	2017-02-21	Root or intermediate	
□	APSP:3623302e-7c6e-4df8-aa9		22 days left	2015-09-30	2016-09-29	APNs	✓

Showing 1 - 5 of 5 items

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.



Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import: Keystore

Keystore type: PKCS#12

Use as: Server

Keystore file*

Password*

Description

- **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 the XenMobile Server that are uploaded to the XenMobile web console. They 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 XenMobile 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, XenMobile attempts to construct a certificate chain from the input, and imports all certificates in that chain (creating 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 for heuristic purposes. The description only attaches to the first certificate in the chain. You can update the description of the remaining certificates later.

1. In the XenMobile 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**, click how you will use the keystore. The available options are:

- **Server**. Server certificates are certificates used functionally by the XenMobile Server that are uploaded to the XenMobile web console. They 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 XenMobile 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

XenMobile only allows one certificate per public key to exist in the system at any given 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 to delete the entry.

To most effectively update your certificates, in the XenMobile 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.

XenMobile Certificate Administration

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

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

XenMobile Server
SSL Certificate for MDM FQDN
SAML Certificate (For ShareFile)
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 XenMobile Server Secure Hub Notifications
PKI User Certificate for connectivity to PKI

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

NetScaler
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

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 XenMobile resources.

> ## Note
>
> The Certification Authority (CA) prompts you to renew your SSL certificate prior to the expiration date.

Because the Apple Push Notification Service (APNs) certificates expire every year, 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.

To enroll and manage iOS devices with XenMobile, set up and create an APNs certificate from Apple. If the certificate expires, users cannot enroll in XenMobile 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. You must 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 with the following information:

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.

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.

Thank You,

Apple Push Notification Service

An app that runs on a physical iOS device (other than apps in the Apple App Store) must be signed with a provisioning profile. The app must also be signed 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 the MDX Toolkit. An example of an acceptable App ID is: com.CompanyName.ProductName.
2. From the Apple Enterprise Developer portal, go to **Provisioning Profiles** > **Distribution** and create an in-house provisioning profile. Repeat this step for each App ID created in the previous step.
3. Download all provisioning profiles. For details, see Wrapping iOS Mobile Apps.

To confirm that all XenMobile Server certificates are valid, do the following:

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

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.

Symantec 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 Symantec Code Signing Certificates for Windows Phone in the Symantec 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.

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

An expired NetScaler 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 NetScaler certificates. The Center notifies you when the certificate expires. These tools assist to monitor the following NetScaler certificates:

- SSL Certificate for MDM FQDN
- SSL Certificate for Gateway FQDN
- SSL Certificate for ShareFile SZC FQDN
- SSL Certificate for Exchange Load Balancing (offload configuration)
- SSL Certificate for StoreFront Load Balancing
- Root and Intermediate CA Certificates for the preceding certificates

NetScaler Gateway and XenMobile

Sep 06, 2017

When you configure NetScaler Gateway using XenMobile, you establish the authentication mechanism for remote device access to the internal network. This functionality enables apps on a mobile device to access corporate servers located in the intranet. XenMobile creates a micro VPN from the apps on the device to NetScaler Gateway.

You configure NetScaler Gateway for use with XenMobile Server by exporting a script from XenMobile that you run on NetScaler Gateway. This article contains the following sections:

Prerequisites for using the NetScaler Gateway configuration script

Configure authentication for remote device access to the internal network

Add a NetScaler Gateway instance

Configure NetScaler Gateway for use with XenMobile Server

Add a callback URL and NetScaler Gateway VPN virtual IP

Prerequisites for using the NetScaler Gateway configuration script

NetScaler requirements:

- NetScaler (minimum version 11.0, Build 70.12).
- NetScaler IP address is configured and has connectivity to the LDAP server, unless LDAP is load balanced.
- NetScaler Subnet (SNIP) IP address is configured, has connectivity to the necessary back end servers, and has public network access over port 8443/TCP.
- DNS can resolve public domains.
- NetScaler is licensed with Platform/Universal or Trial licenses. For information, see https://support.citrix.com/article/CTX126049.
- A NetScaler Gateway SSL certificate is uploaded and installed on the NetScaler. For information see, https://support.citrix.com/article/CTX136023.

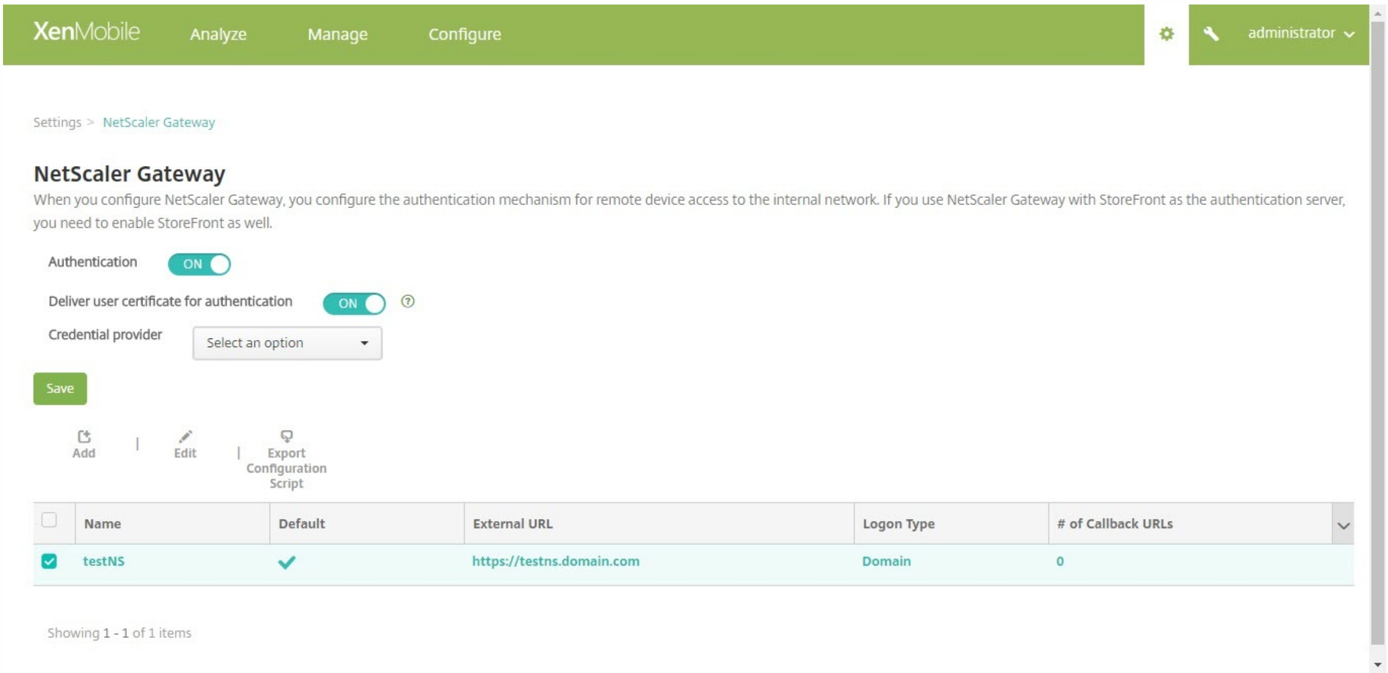
XenMobile requirements:

- XenMobile Server (minimum version 10.6).
- LDAP server is configured.

Configure authentication for remote device access to the internal network

1. In the XenMobile web console, click the gear icon in the upper-right corner of the console. The `Settings` page appears.

2. Under **Server**, click **NetScaler Gateway**. The **NetScaler Gateway** page appears. In the following example, a NetScaler Gateway instance exists.



NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication: ON

Deliver user certificate for authentication: ON

Credential provider: Select an option

Save

☐	Name	Default	External URL	Logon Type	# of Callback URLs
☑	testNS	✓	https://testns.domain.com	Domain	0

Showing 1 - 1 of 1 items

3. Configure these settings:

- **Authentication**: Select whether to enable authentication. The default is **ON**.
- **Deliver user certificate for authentication**: Select whether you want XenMobile to share the authentication certificate with Secure Hub so that the NetScaler Gateway handles 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**.

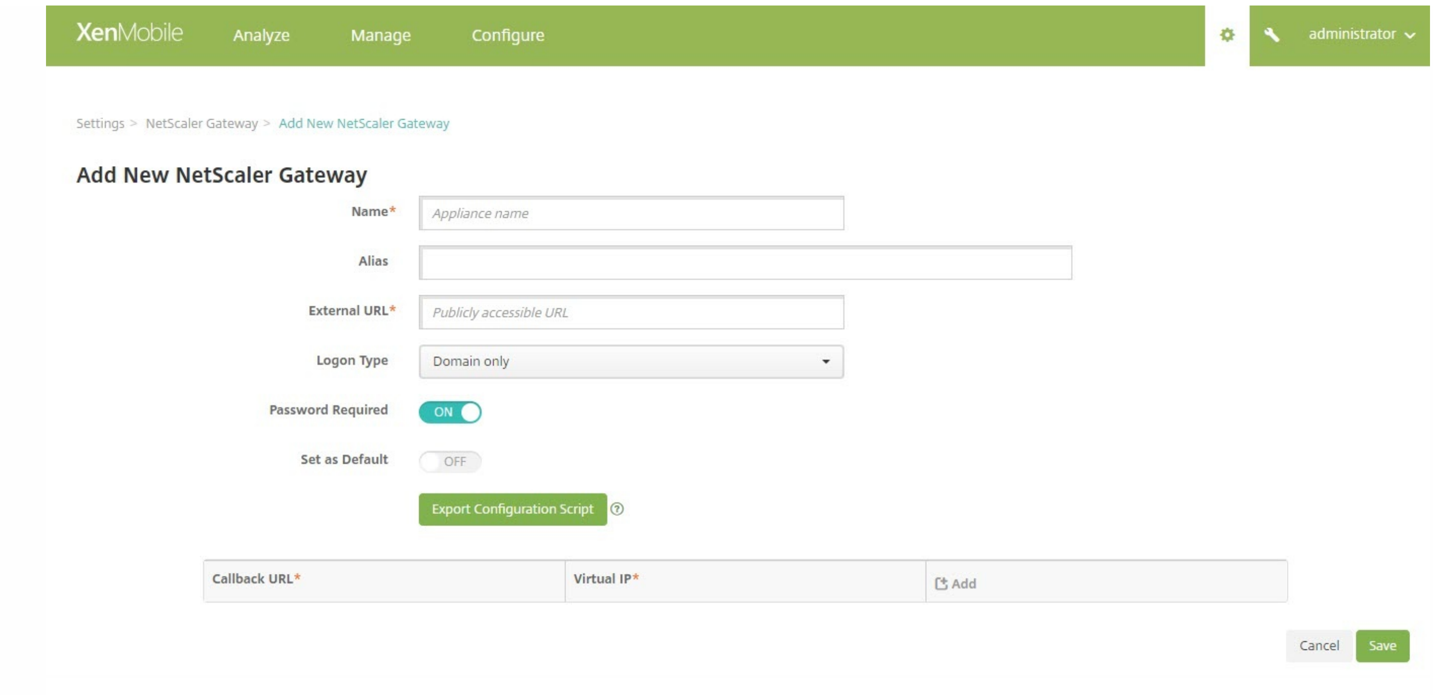
Add a NetScaler Gateway instance

After you save the authentication settings, you add a NetScaler Gateway instance to XenMobile.

1. In the XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page opens.

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

3. Click **Add**. The **Add New NetScaler Gateway** page appears.



Settings > NetScaler Gateway > Add New NetScaler Gateway

Add New NetScaler Gateway

Name* Appliance name

Alias

External URL* Publicly accessible URL

Logon Type Domain only

Password Required ON

Set as Default OFF

4. Configure these settings:

- **Name**: Type a name for the NetScaler Gateway instance.
- **Alias**: Optionally include an alias name for the NetScaler Gateway.
- **External URL**: Type the publicly accessible URL for NetScaler Gateway. For example, https://receiver.com.
- **Logon Type**: Choose a logon type. Types include **Domain only**, **Security token only**, **Domain and security token**, **Certificate**, **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**.

If you use **Certificate and security token**, some additional configuration is required on NetScaler Gateway to support Secure Hub. For information, see Configuring XenMobile for Certificate and Security Token Authentication.

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 NetScaler Gateway as the default. The default is **OFF**.
- **Export Configuration Script**: Click the button to export a configuration bundle that you upload to NetScaler Gateway to configure it with XenMobile settings. For information, see "Configure an on-premises NetScaler Gateway for use with XenMobile Server" after these steps.
- **Callback URL** and **Virtual IP**: Save your settings before adding these fields. For information, see "Add a callback URL and NetScaler Gateway VPN virtual IP" later in this article.

5. Click **Save**. The new NetScaler Gateway is added and appears in the table. You can edit or delete an instance by clicking the name in the list.

Configure NetScaler Gateway for use with XenMobile

Server

To configure an on-premises NetScaler Gateway for use with XenMobile Server, you perform the following general steps, detailed in this article:

1. Download a script and related files from XenMobile Server. See the readme file provided with the script for the latest detailed instructions.

2. Verify that your environment meets the prerequisites.

3. Update the script for your environment.

4. Run the script on NetScaler.

5. Test the configuration.

The script configures these NetScaler Gateway settings required by XenMobile:

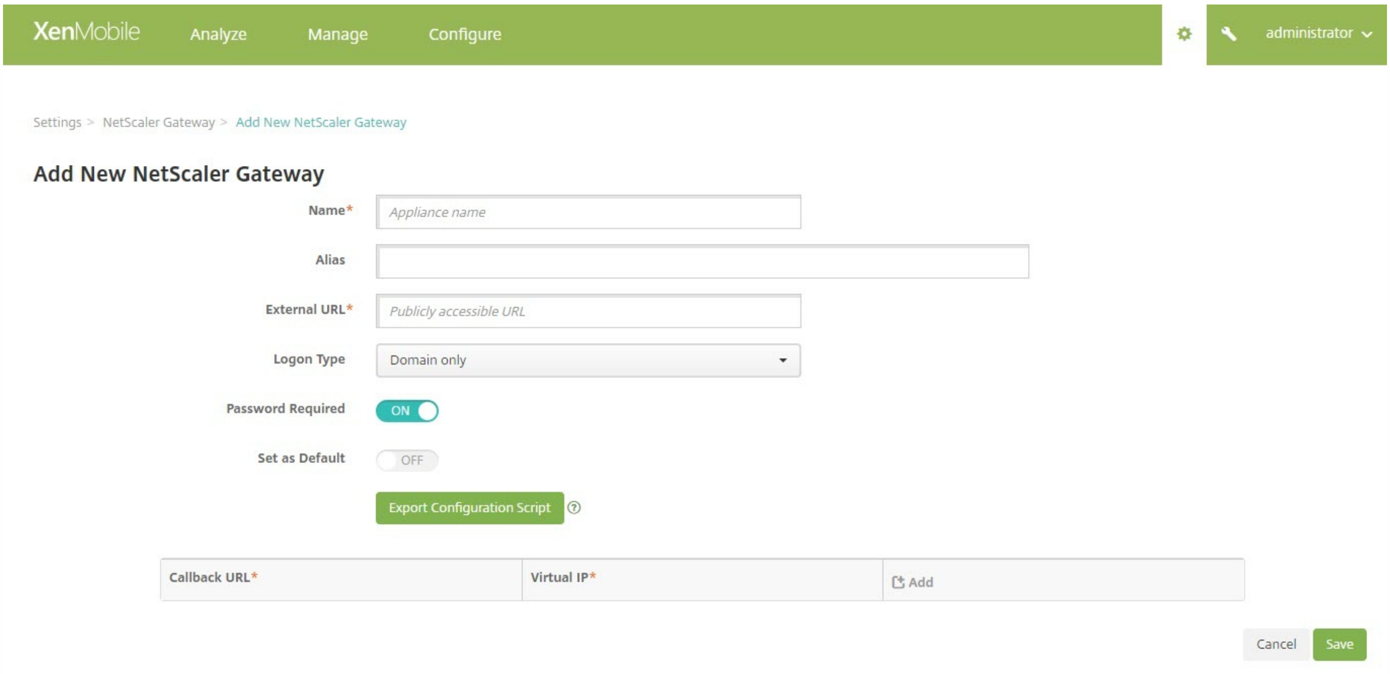
- NetScaler Gateway virtual servers needed for MDM and MAM
- Session policies for the NetScaler Gateway virtual servers
- XenMobile Server details
- Authentication Policies and Actions for the NSG virtual server.
  The script describes the LDAP configuration settings.
- Traffic actions and policies for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

The script doesn't handle the following configuration:

- Exchange load balancing
- ShareFile load balancing
- ICA Proxy configuration
- SSL Offload

To download, update, and run the script:

1. If you're adding a NetScaler Gateway, click **Export Configuration Script** on the **Add New NetScaler Gateway** page.



Settings > NetScaler Gateway > Add New NetScaler Gateway

Add New NetScaler Gateway

Name* Appliance name

Alias

External URL* Publicly accessible URL

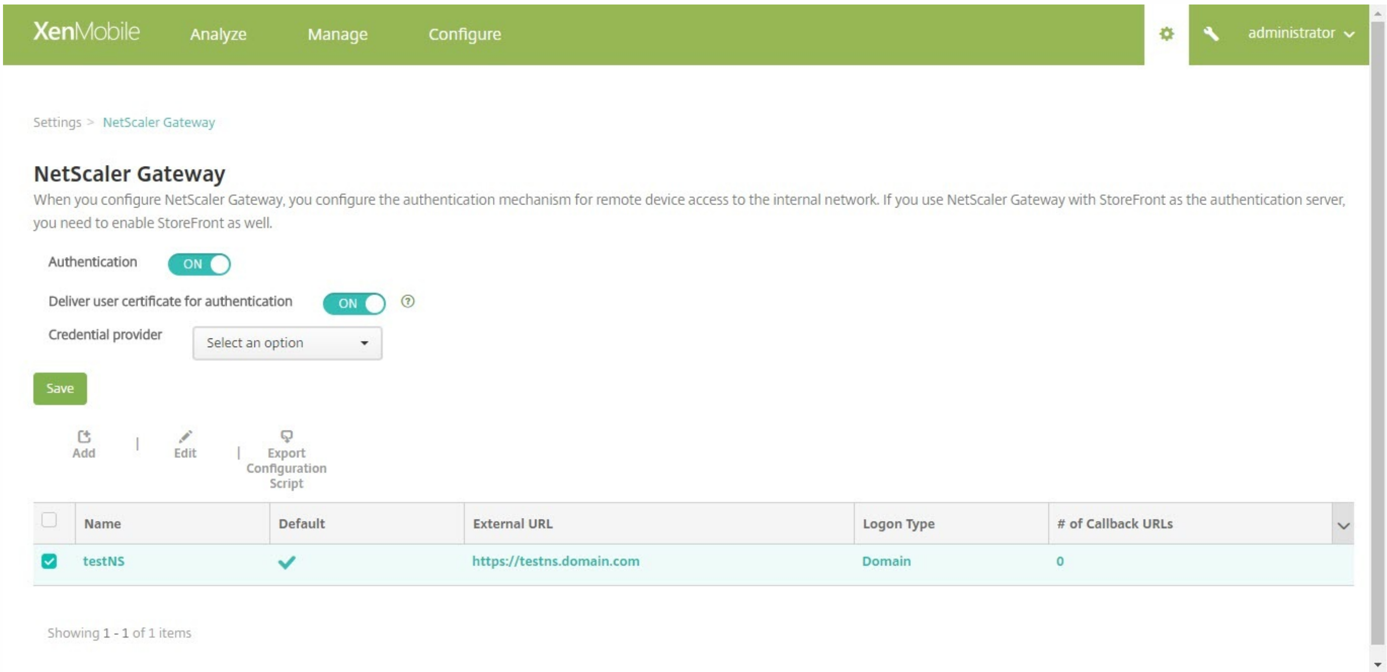
Logon Type: Domain only

Password Required: ON

Set as Default: OFF

Callback URL*	Virtual IP*	Add

Or, if you add a NetScaler Gateway instance and click **Save** before you export the script: Return to **Settings** > **NetScaler Gateway**, select the NetScaler, click **Export Configuration Script**, and then click **Download**.



Settings > NetScaler Gateway

NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication: ON

Deliver user certificate for authentication: ON

Credential provider: Select an option

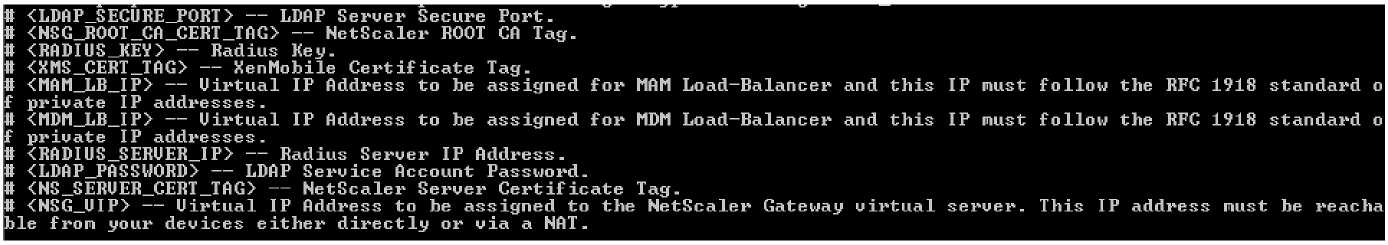
☐	Name	Default	External URL	Logon Type	# of Callback URLs
☑	testNS	✓	https://testns.domain.com	Domain	0

Showing 1 - 1 of 1 items

After you click **Export Configuration Script**, XenMobile creates a .tar.gz script bundle. The script bundle includes:

- 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 of XenMobile Server (these certificates, for SSL offload, are not needed for the current release)
- Script that contains the NetScaler CLI commands used to remove the NetScaler configuration

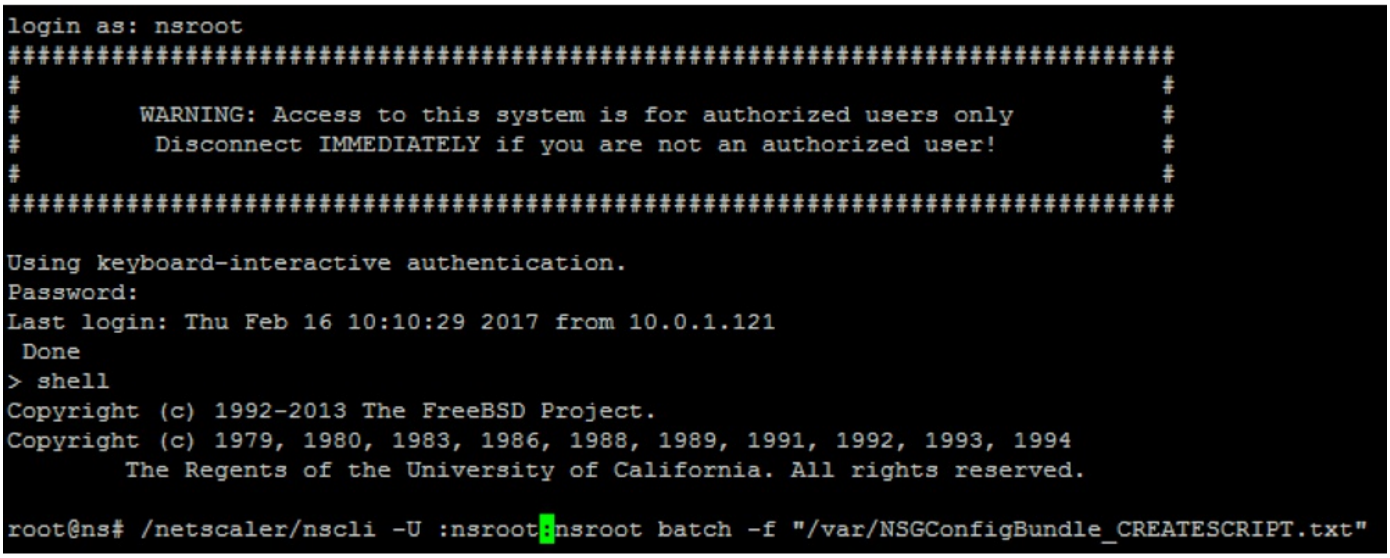
2. Edit the script (NSGConfigBundle_CREATESCRIPT.txt) to replace all placeholders with details from your environment.



```
# <LDAP_SECURE_PORT> -- LDAP Server Secure Port.
# <NSG_ROOT_CA_CERT_TAG> -- NetScaler ROOT CA Tag.
# <RADIUS_KEY> -- Radius Key.
# <XMS_CERT_TAG> -- XenMobile Certificate Tag.
# <MAM_LB_IP> -- Virtual IP Address to be assigned for MAM Load-Balancer and this IP must follow the RFC 1918 standard o
f private IP addresses.
# <MDM_LB_IP> -- Virtual IP Address to be assigned for MDM Load-Balancer and this IP must follow the RFC 1918 standard o
f private IP addresses.
# <RADIUS_SERVER_IP> -- Radius Server IP Address.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <NS_SERVER_CERT_TAG> -- NetScaler Server Certificate Tag.
# <NSG_VIP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reacha
ble from your devices either directly or via a NAT.
```

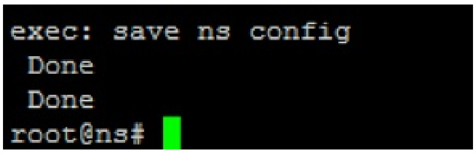
3. Run your edited script in the NetScaler bash shell, as described in the readme file included in the script bundle. For example:

   /netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"



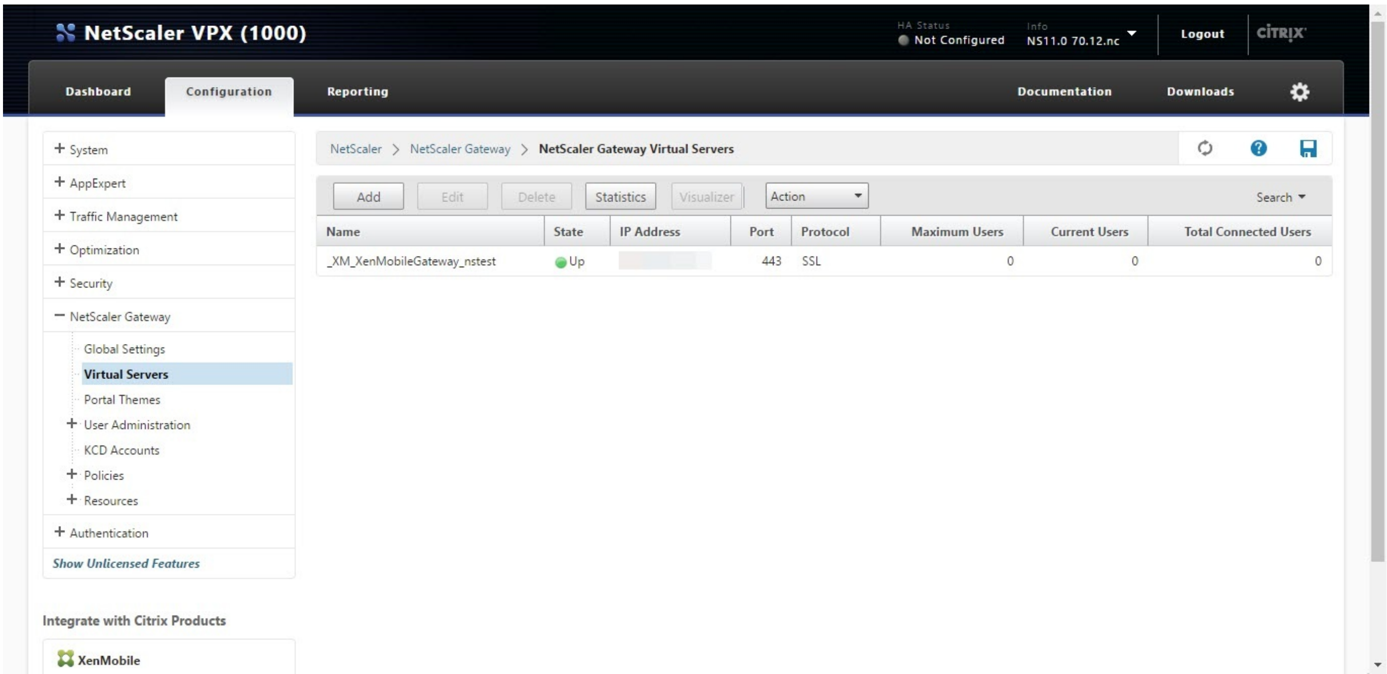
```
login as: nsroot
##############################################################################
#                                                                            #
#        WARNING: Access to this system is for authorized users only         #
#         Disconnect IMMEDIATELY if you are not an authorized user!          #
#                                                                            #
##############################################################################

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

   When the script completes, the following lines appear.



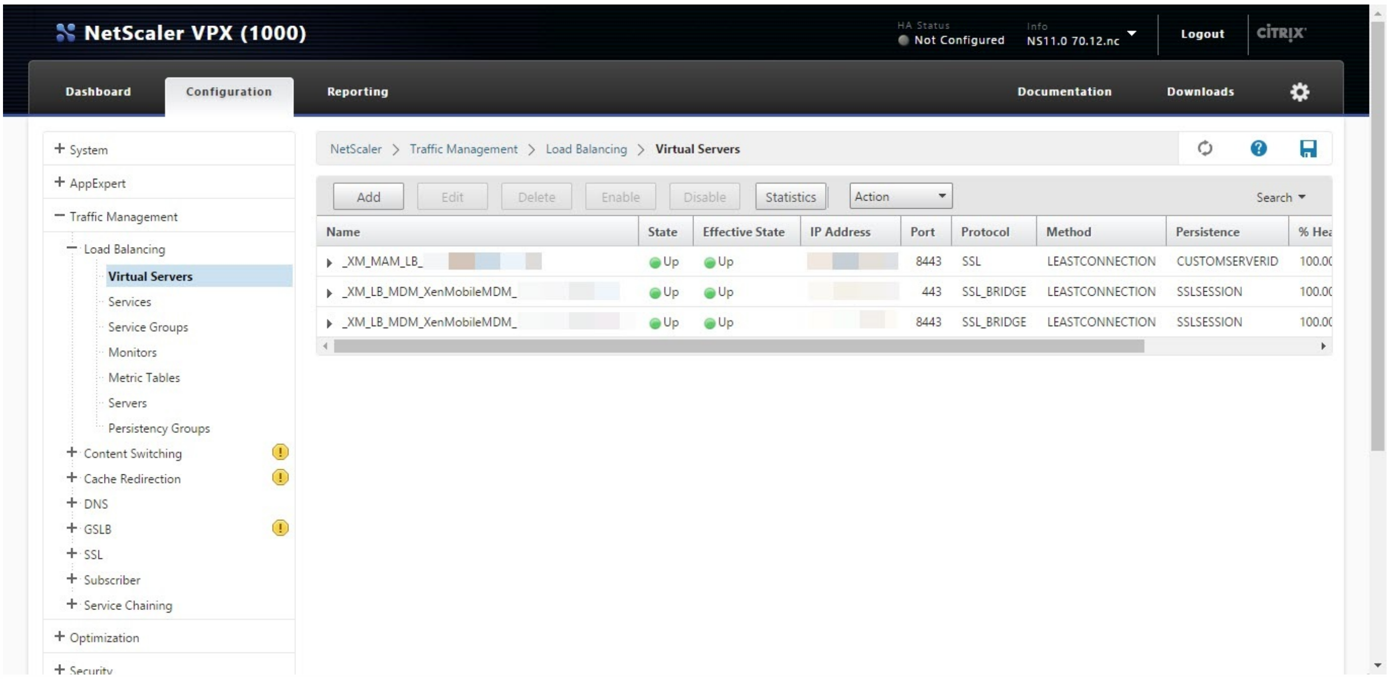
```
exec: save ns config
 Done
 Done
root@ns#
```

1. Validate that the NetScaler Gateway Virtual Server shows a state of **UP**.



Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
_XM_XenMobileGateway_nstest	Up	[redacted]	443	SSL	0	0	0

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



Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Hea
_XM_MAM_LB_[redacted]	Up	Up	[redacted]	8443	SSL	LEASTCONNECTION	CUSTOMSERVERID	100.0
_XM_LB_MDM_XenMobileMDM_[redacted]	Up	Up	[redacted]	443	SSL_BRIDGE	LEASTCONNECTION	SSLSESSION	100.0
_XM_LB_MDM_XenMobileMDM_[redacted]	Up	Up	[redacted]	8443	SSL_BRIDGE	LEASTCONNECTION	SSLSESSION	100.0

3. Open a web browser, connect to the NetScaler Gateway URL, and attempt to authenticate. If the authentication fails, this message appears: HTTP Status 404 - Not Found

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

Add a callback URL and NetScaler Gateway VPN virtual

IP

After adding the NetScaler Gateway instance, you can add a callback URL and specify a NetScaler Gateway virtual IP address. **Note**: These settings are optional, but can be configured for extra security, especially when the XenMobile Server is in the DMZ.

1. In **Settings > NetScaler Gateway**, select the NetScaler Gateway and then click **Edit**.
2. In the table, click **Add**.
3. For **Callback URL** type the fully qualified domain name (FQDN). The callback URL verifies that a request originated from NetScaler Gateway. Ensure that the callback URL resolves to an IP address that is reachable from XenMobile Server. The callback URL can be an external NetScaler Gateway URL or some other URL.
4. Type the NetScaler Gateway **Virtual IP** address and then click **Save**.

Domain or domain plus security token authentication

Nov 28, 2017

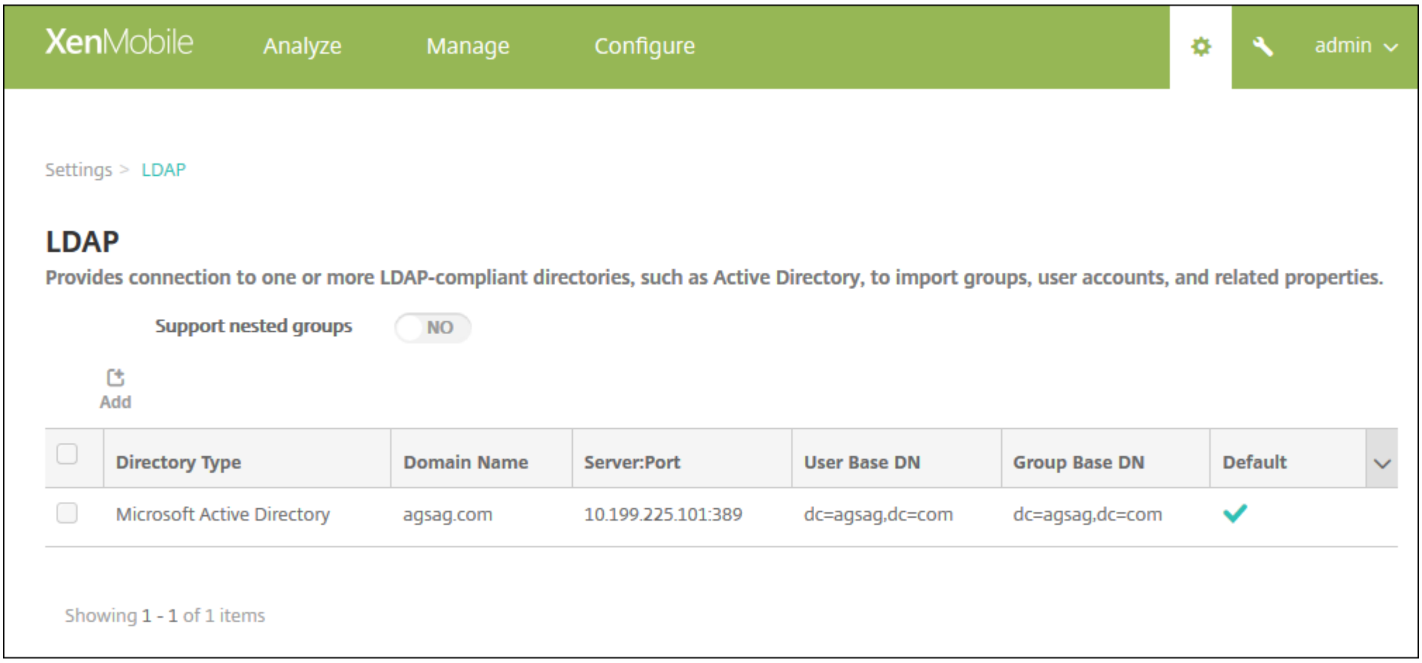
XenMobile supports domain-based authentication against one or more directories, such as Active Directory, that are compliant with the Lightweight Directory Access Protocol (LDAP). You can configure a connection in XenMobile to one or more directories and then use the LDAP configuration to import groups, 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, enabling a user to log on one time to a company website, and then be automatically logged into the corporate intranet.

A client starts an LDAP session by connecting to an LDAP server, referred to 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
>
> XenMobile doesn't support changing the authentication mode from domain authentication to a different authentication mode after users have enrolled devices in XenMobile.

1. In the XenMobile 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 from this page.



LDAP

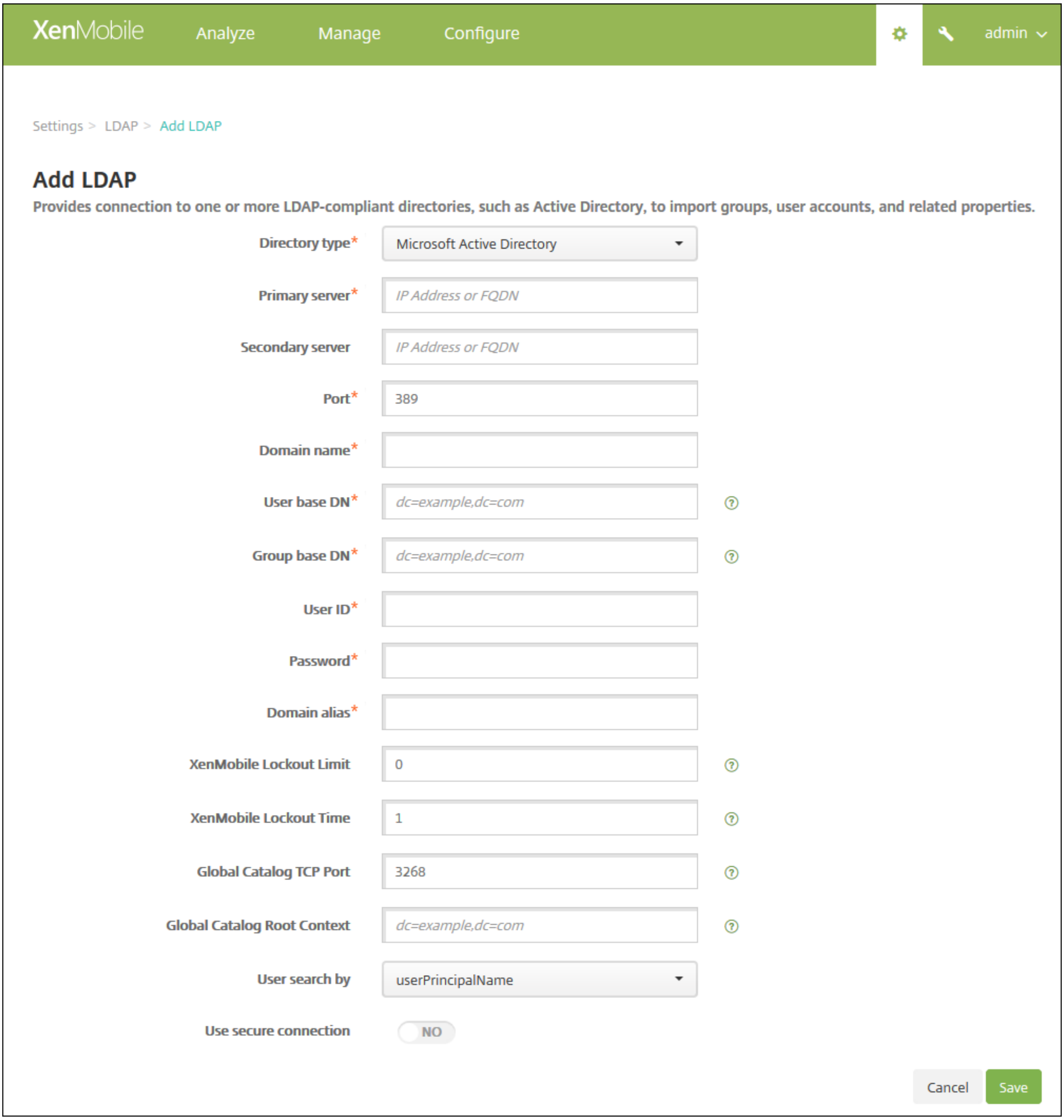
Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Support nested groups NO

□	Directory Type	Domain Name	Server:Port	User Base DN	Group Base DN	Default
□	Microsoft Active Directory	agsag.com	10.199.225.101:389	dc=agsag,dc=com	dc=agsag,dc=com	✓

Showing 1 - 1 of 1 items

1. On the **LDAP** page, click **Add**. The **Add LDAP** page appears.



Add LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory
Primary server*	IP Address or FQDN
Secondary server	IP Address or FQDN
Port*	389
Domain name*	
User base DN*	dc=example,dc=com
Group base DN*	dc=example,dc=com
User ID*	
Password*	
Domain alias*	
XenMobile Lockout Limit	0
XenMobile Lockout Time	1
Global Catalog TCP Port	3268
Global Catalog Root Context	dc=example,dc=com
User search by	userPrincipalName
Use secure connection	NO

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).

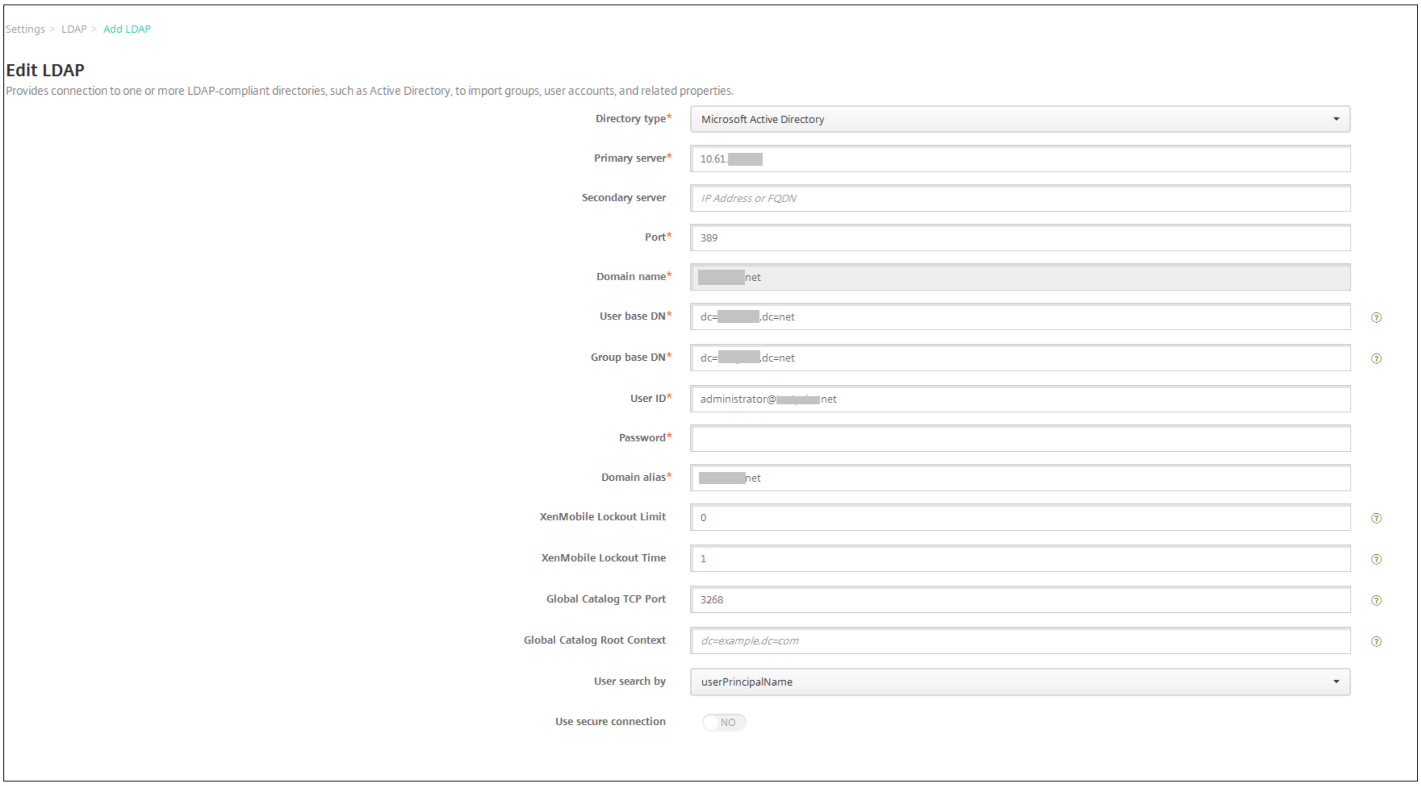
- **Secondary server**: Optionally, if a secondary server has been configured, enter the IP address or FQDN for the secondary server. This server is a failover server used if the primary server cannot be reached.
- **Port**: Type the port number used by the LDAP server. By default, the port number is 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.
- **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.
- **XenMobile Lockout Limit**: Type a number between 0 and 999 for the number of failed logon attempts. Setting this field to 0 means that XenMobile will never lock out the user based on failed logon attempts.
- **XenMobile Lockout Time**: Type a number between 0 and 99999 representing the number of minutes a user must wait after exceeding the lockout limit. Setting this field to 0 means that the user will not be 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**: In the list, click either **userPrincipalName**, or **sAMAccountName**. The default is **userPrincipalName**.
- **Use secure connection**: Select whether to use secure connections. The default is **NO**.

3. Click **Save**.

1. In the **LDAP** table, select the directory you want to edit.

> **Note**: When you select the check box next to a directory, the options menu appears above the LDAP 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 LDAP** page appears.



Settings > LDAP > Add LDAP

Edit LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory
Primary server*	10.61.[redacted]
Secondary server	IP Address or FQDN
Port*	389
Domain name*	[redacted]net
User base DN*	dc=[redacted],dc=net
Group base DN*	dc=[redacted],dc=net
User ID*	administrator@[redacted]net
Password*	
Domain alias*	[redacted]net
XenMobile Lockout Limit	0
XenMobile Lockout Time	1
Global Catalog TCP Port	3268
Global Catalog Root Context	dc=example,dc=com
User search by	userPrincipalName
Use secure connection	NO

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 represents 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.
- **XenMobile Lockout Limit**: Type a number between 0 and 999 for the number of failed logon attempts. Setting this field to 0 means that XenMobile will never lock out the user based on failed logon attempts.
- **XenMobile Lockout Time**: Type a number between 0 and 99999 representing the number of minutes a user must wait after exceeding the lockout limit. Setting this field to 0 means that the user will not be 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**: In the list, click either **userPrincipalName**, or **sAMAccountName**.
- **Use secure connection**: Select whether to use secure connections.

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

1. In the **LDAP** table, select the directory you want to delete.

> **Note**: 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

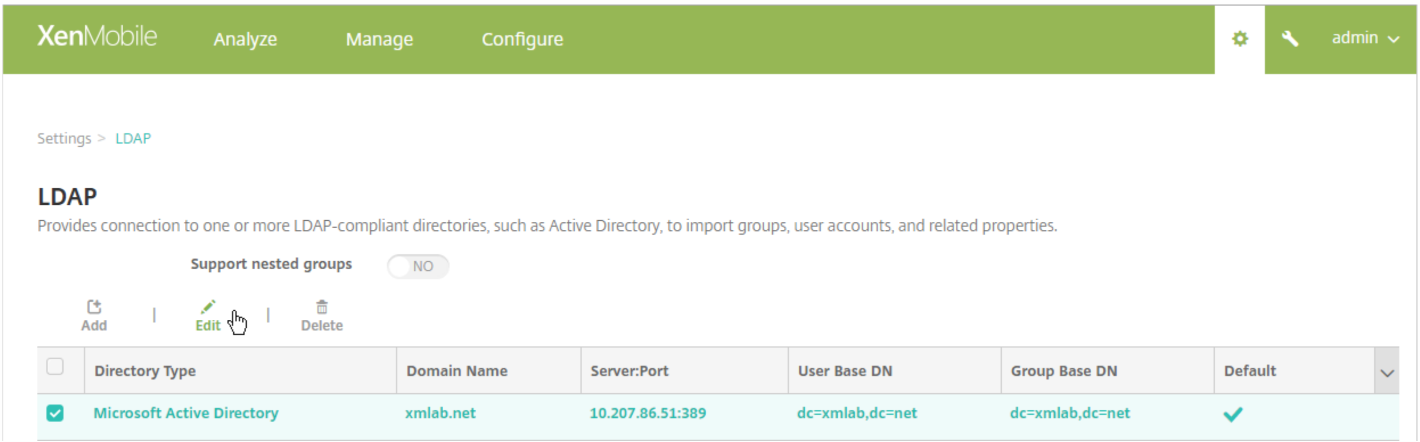
You can configure XenMobile to require users to authenticate with their LDAP credentials plus a one-time password, using the RADIUS protocol.

For optimal usability, you can combine this configuration with Citrix PIN and Active Directory password caching so users do not have to repeatedly enter their Active Directory user names and passwords. Users will need to enter user names and passwords for enrollment, password expiration, and account lockout.

Use of LDAP for authentication requires that you install an SSL certificate from a Certificate Authority on XenMobile. For information, see Uploading certificates in XenMobile.

1. In **Settings**, click **LDAP**.

2. Select **Microsoft Active Directory** and then click **Edit**.



LDAP

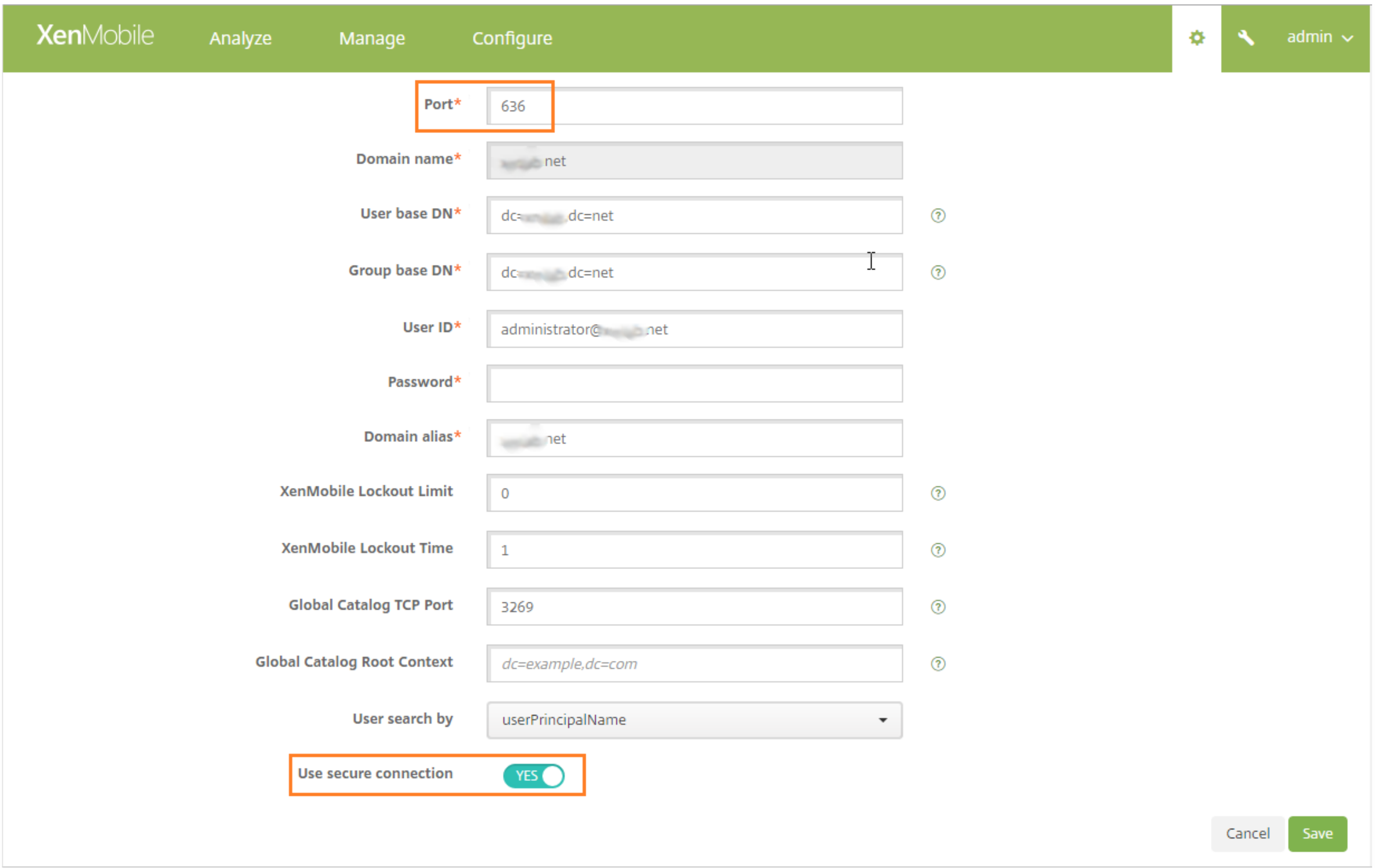
Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Support nested groups: NO

□	Directory Type	Domain Name	Server:Port	User Base DN	Group Base DN	Default
☑	Microsoft Active Directory	xmlab.net	10.207.86.51:389	dc=xmlab,dc=net	dc=xmlab,dc=net	✓

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**.



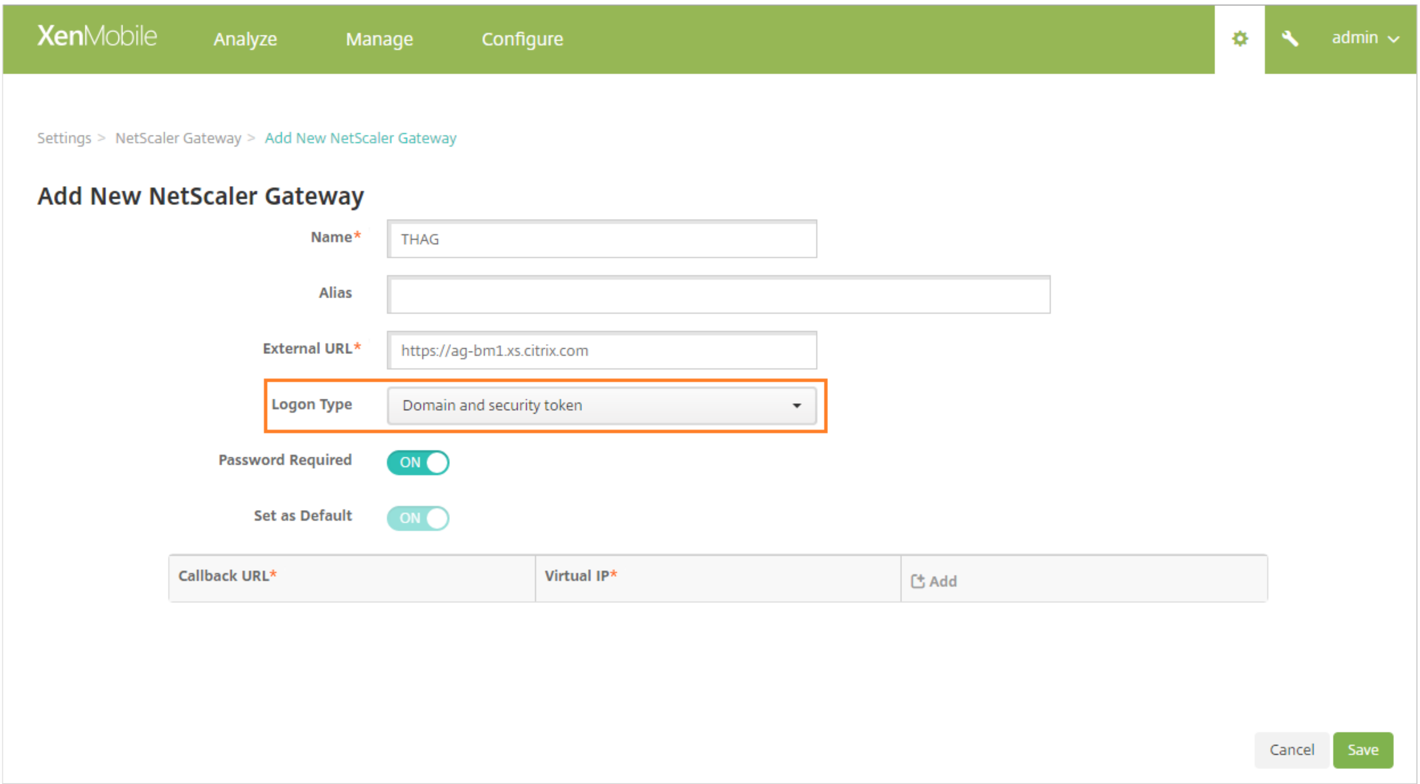
Port*	636
Domain name*	[redacted] net
User base DN*	dc=[redacted] dc=net
Group base DN*	dc[redacted] dc=net
User ID*	administrator@[redacted] net
Password*	
Domain alias*	[redacted] net
XenMobile Lockout Limit	0
XenMobile Lockout Time	1
Global Catalog TCP Port	3269
Global Catalog Root Context	dc=example,dc=com
User search by	userPrincipalName
Use secure connection	YES

The following steps assume that you already have added a NetScaler Gateway instance to XenMobile. To add a NetScaler Gateway instance, see To configure a new NetScaler Gateway instance.

1. In **Settings**, click **NetScaler Gateway**.

2. Select the **NetScaler Gateway** and then click **Edit**.

3. From **Logon Type**, select **Domain and security token**.



Add New NetScaler Gateway

Name* THAG

Alias

External URL* https://ag-bm1.xs.citrix.com

Logon Type Domain and security token

Password Required ON

Set as Default ON

Callback URL*	Virtual IP*	Add

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 NetScaler Gateway session profiles and policies for your virtual servers used with XenMobile. For information, see Configuring Domain and Security Token Authentication for XenMobile in the NetScaler Gateway documentation.

Client certificate or certificate plus domain authentication

Nov 28, 2017

The default configuration for XenMobile is user name and password authentication. To add another layer of security for enrollment and access to XenMobile environment, consider using certificate-based authentication. In the XenMobile 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 NetScaler.

For optimal usability, you can combine this configuration with Citrix PIN and Active Directory password caching so users do not have to repeatedly enter their Active Directory user names and passwords. Users will need to enter user names and passwords for enrollment, password expiration, and account lockout.

> ## Important
>
> XenMobile doesn't support changing the authentication mode from domain authentication to some other authentication mode after users have enrolled devices in XenMobile.

If you don't allow LDAP and use smart cards or similar methods, configuring certificates allows you to represent a smart card to XenMobile. Users then enroll using a unique PIN that XenMobile generates for them. After a user has access, XenMobile creates and deploys the certificate subsequently used to authenticate to the XenMobile environment.

You can use the NetScaler for XenMobile wizard to perform the configuration required for XenMobile when using NetScaler certificate-only authentication or certificate plus domain authentication. You can run the NetScaler for XenMobile wizard one time only.

In highly secure environments where usage of LDAP credentials outside of an organization in public or insecure networks is considered a prime security threat for the organization, two-factor authentication using a client certificate and a security token is an option. For information, see Configuring XenMobile for Certificate and Security Token Authentication.

Client certificate authentication is available for XenMobile MAM mode (MAM-only) and ENT mode (when users enroll into MDM). Client certificate authentication isn't available for XenMobile ENT mode when users enroll into legacy MAM mode. To use client certificate authentication for XenMobile ENT and MAM modes, you must configure the Microsoft server, the XenMobile server, and then NetScaler Gateway. Follow these general steps, as described in this article.

On the Microsoft server:

1. Add a certificate snap-in to the Microsoft Management Console.
2. Add the template to Certificate Authority (CA).
3. Create a PFX certificate from the CA server.

On the XenMobile server:

1. Upload the certificate to XenMobile.
2. Create the PKI entity for certificate-based authentication.
3. Configure credentials providers.

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

On NetScaler Gateway, configure as described in Configuring Client Certificate or Client Certificate and Domain Authentication in the NetScaler Gateway documentation.

Prerequisites

- When you create a Microsoft Certificate Services Entity template, to avoid possible authentication issues with enrolled devices, avoid using special characters, such as :, !, $, (), #, % , +, *, ~, ?, |, {}, and [] in the template name.
- For Windows Phone 8.1 devices using client certificate authentication and SSL Offload, you must disable SSL session reuse for port 443 on both load balancing virtual servers in NetScaler. To do that, Run the following command on the vservers for port 443:

  set ssl vserver <ssl lb vserver> sessReuse DISABLE

  Note: Disabling SSL session reuse disables some of the optimizations that NetScaler provides, which can result in a performance decrease on the NetScaler.

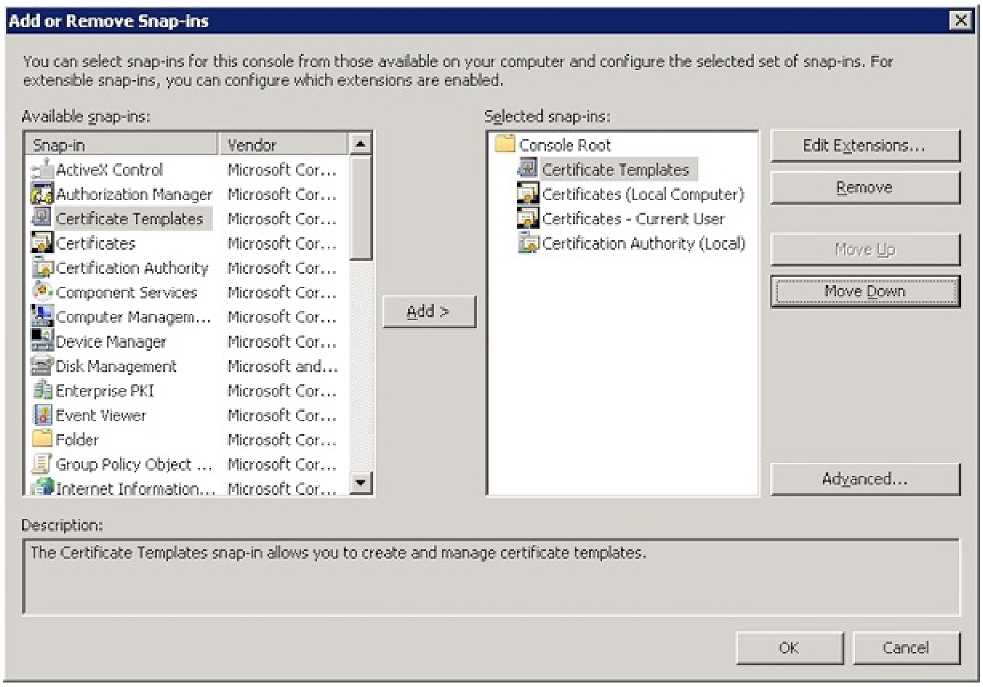
- To configure Certificate-based Authentication for Exchange ActiveSync, see this Microsoft blog.
- If you are using private server certificates to secure the ActiveSync traffic to the Exchange Server, ensure that the mobile devices have all of the Root/Intermediate certificates. Otherwise, certificate-based authentication will fail during the mailbox setup in Secure Mail. In the Exchange IIS Console, you must:
  - Add a website for XenMobile 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**.
- Make sure that Secure Mail is wrapped with the latest MDX Toolkit, if required for your deployment method.

Add a certificate snap-in to the Microsoft Management Console

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

2. Add the following snap-ins:

   Certificate Templates
   Certificates (Local Computer)
   Certificates - Current User
   Certificate Authority (Local)



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Enterprise PKI	Microsoft Cor...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Information...	Microsoft Cor...

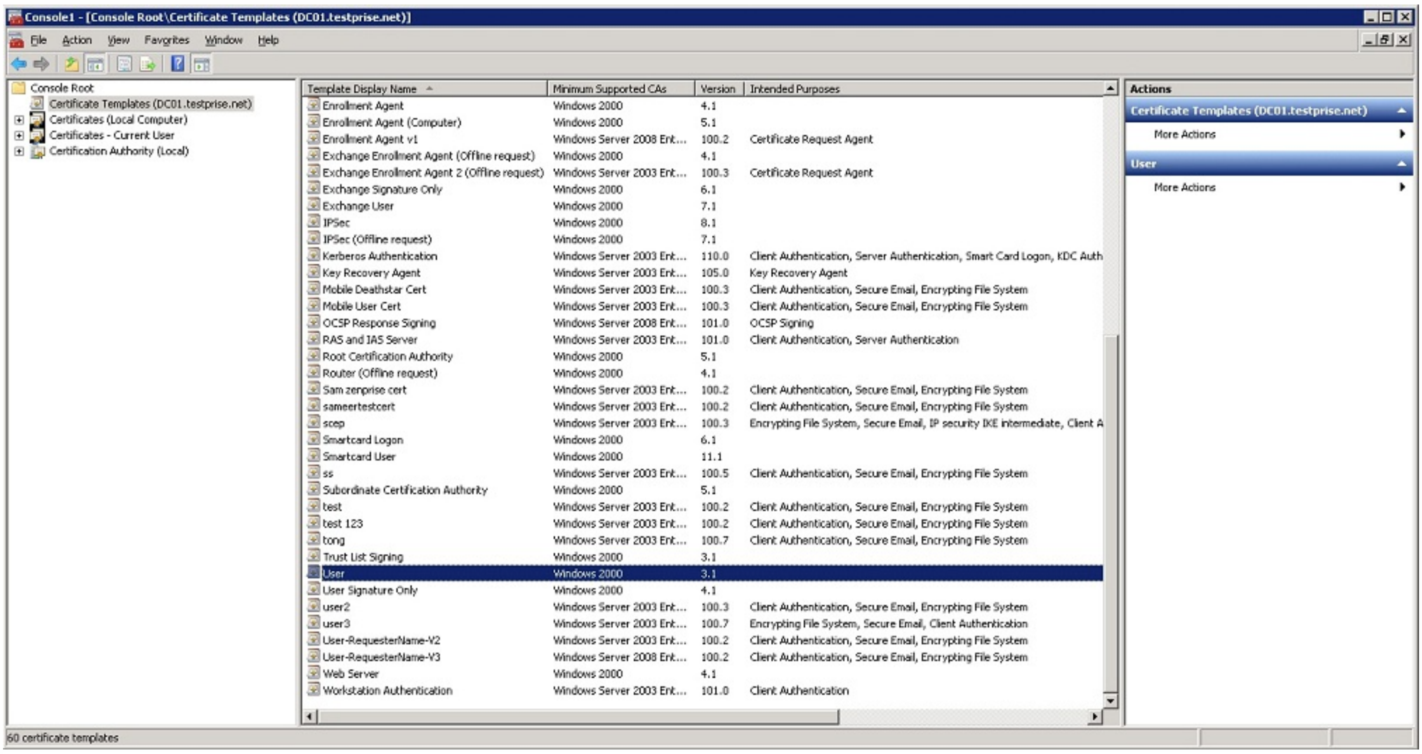
Selected snap-ins:

- Console Root
  - Certificate Templates
  - Certificates (Local Computer)
  - Certificates - Current User
  - Certification Authority (Local)

Description:

The Certificate Templates snap-in allows you to create and manage certificate templates.

3. Expand **Certificate Templates**.



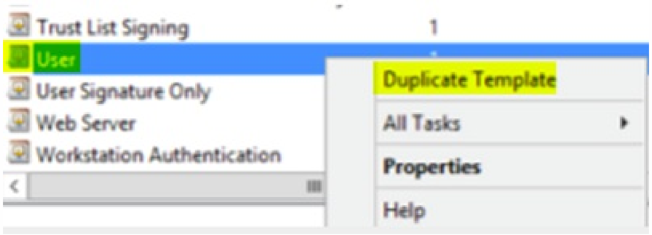
Console1 - [Console Root\Certificate Templates (DC01.testprise.net)]
File
Action
View
Favorites
Window
Help

- Console Root
  - Certificate Templates (DC01.testprise.net)
  - Certificates (Local Computer)
  - Certificates - Current User
  - Certification Authority (Local)

Template Display Name	Minimum Supported CAs	Version	Intended Purposes
Enrollment Agent	Windows 2000	4.1	
Enrollment Agent (Computer)	Windows 2000	5.1	
Enrollment Agent v1	Windows Server 2008 Ent...	100.2	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Windows 2000	4.1	
Exchange Enrollment Agent 2 (Offline request)	Windows Server 2003 Ent...	100.3	Certificate Request Agent
Exchange Signature Only	Windows 2000	6.1	
Exchange User	Windows 2000	7.1	
IPSec	Windows 2000	8.1	
IPSec (Offline request)	Windows 2000	7.1	
Kerberos Authentication	Windows Server 2003 Ent...	110.0	Client Authentication, Server Authentication, Smart Card Logon, KDC Auth
Key Recovery Agent	Windows Server 2003 Ent...	105.0	Key Recovery Agent
Mobile Deathstar Cert	Windows Server 2003 Ent...	100.3	Client Authentication, Secure Email, Encrypting File System
Mobile User Cert	Windows Server 2003 Ent...	100.3	Client Authentication, Secure Email, Encrypting File System
OCSP Response Signing	Windows Server 2008 Ent...	101.0	OCSP Signing
RAS and IAS Server	Windows Server 2003 Ent...	101.0	Client Authentication, Server Authentication
Root Certification Authority	Windows 2000	5.1	
Router (Offline request)	Windows 2000	4.1	
Sam zenprise cert	Windows Server 2003 Ent...	100.2	Client Authentication, Secure Email, Encrypting File System
sameertestcert	Windows Server 2003 Ent...	100.2	Client Authentication, Secure Email, Encrypting File System
scep	Windows Server 2003 Ent...	100.3	Encrypting File System, Secure Email, IP security IKE intermediate, Client A
Smartcard Logon	Windows 2000	6.1	
Smartcard User	Windows 2000	11.1	
ss	Windows Server 2003 Ent...	100.5	Client Authentication, Secure Email, Encrypting File System
Subordinate Certification Authority	Windows 2000	5.1	
test	Windows Server 2003 Ent...	100.2	Client Authentication, Secure Email, Encrypting File System
test 123	Windows Server 2003 Ent...	100.2	Client Authentication, Secure Email, Encrypting File System
tong	Windows Server 2003 Ent...	100.7	Client Authentication, Secure Email, Encrypting File System
Trust List Signing	Windows 2000	3.1	
User	Windows 2000	3.1	
User Signature Only	Windows 2000	4.1	
user2	Windows Server 2003 Ent...	100.3	Client Authentication, Secure Email, Encrypting File System
user3	Windows Server 2003 Ent...	100.7	Encrypting File System, Secure Email, Client Authentication
User-RequesterName-V2	Windows Server 2003 Ent...	100.2	Client Authentication, Secure Email, Encrypting File System
User-RequesterName-V3	Windows Server 2008 Ent...	100.2	Client Authentication, Secure Email, Encrypting File System
Web Server	Windows 2000	4.1	
Workstation Authentication	Windows Server 2003 Ent...	101.0	Client Authentication

60 certificate templates

4. Select the **User** template and **Duplicate Template**.

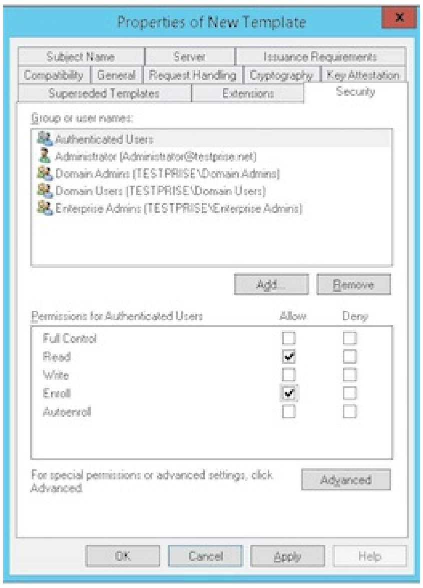


5. Provide the Template display name.

> **Important:** Do not select the **Publish certificate in Active Directory** check box unless required. If this option is selected, all user client certificates will be pushed/created in Active Directory, which might clutter your Active Directory database.

6. Select **Windows 2003 Server** for the template type. In Windows 2012 R2 server, under **Compatibility**, select **Certificate authority** and set the recipient as **Windows 2003**.

7. Under **Security**, select the **Enroll** option in the **Allow** column for the authenticated users.

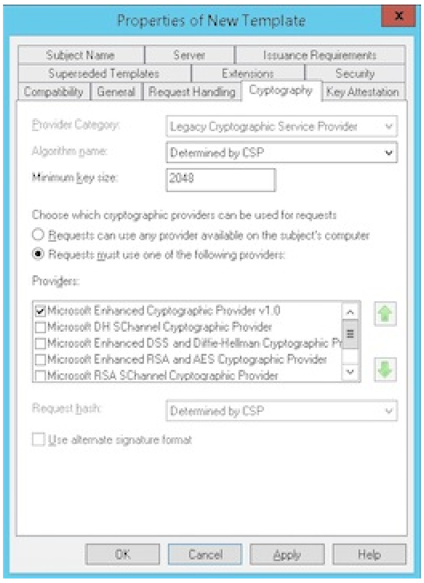


Authenticated Users
Administrator (Administrator@testprise.net)
Domain Admins (TESTPRISE\Domain Admins)
Domain Users (TESTPRISE\Domain Users)
Enterprise Admins (TESTPRISE\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.

8. Under **Cryptography**, make sure you provide the key size, which you will need to enter during XenMobile configuration.



Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

○ Requests can use any provider available on the subject's computer

● Requests must use one of the following providers:

Providers:

☑ Microsoft Enhanced Cryptographic Provider v1.0

□ Microsoft DH SChannel Cryptographic Provider

□ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr

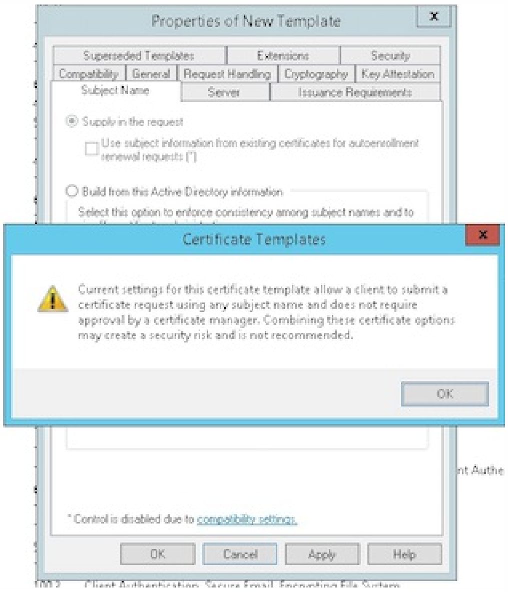
□ Microsoft Enhanced RSA and AES Cryptographic Provider

□ Microsoft RSA SChannel Cryptographic Provider

Request hash: Determined by CSP

□ Use alternate signature format

9. Under **Subject Name**, select **Supply in the request**. Apply the changes and then save.



● Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to

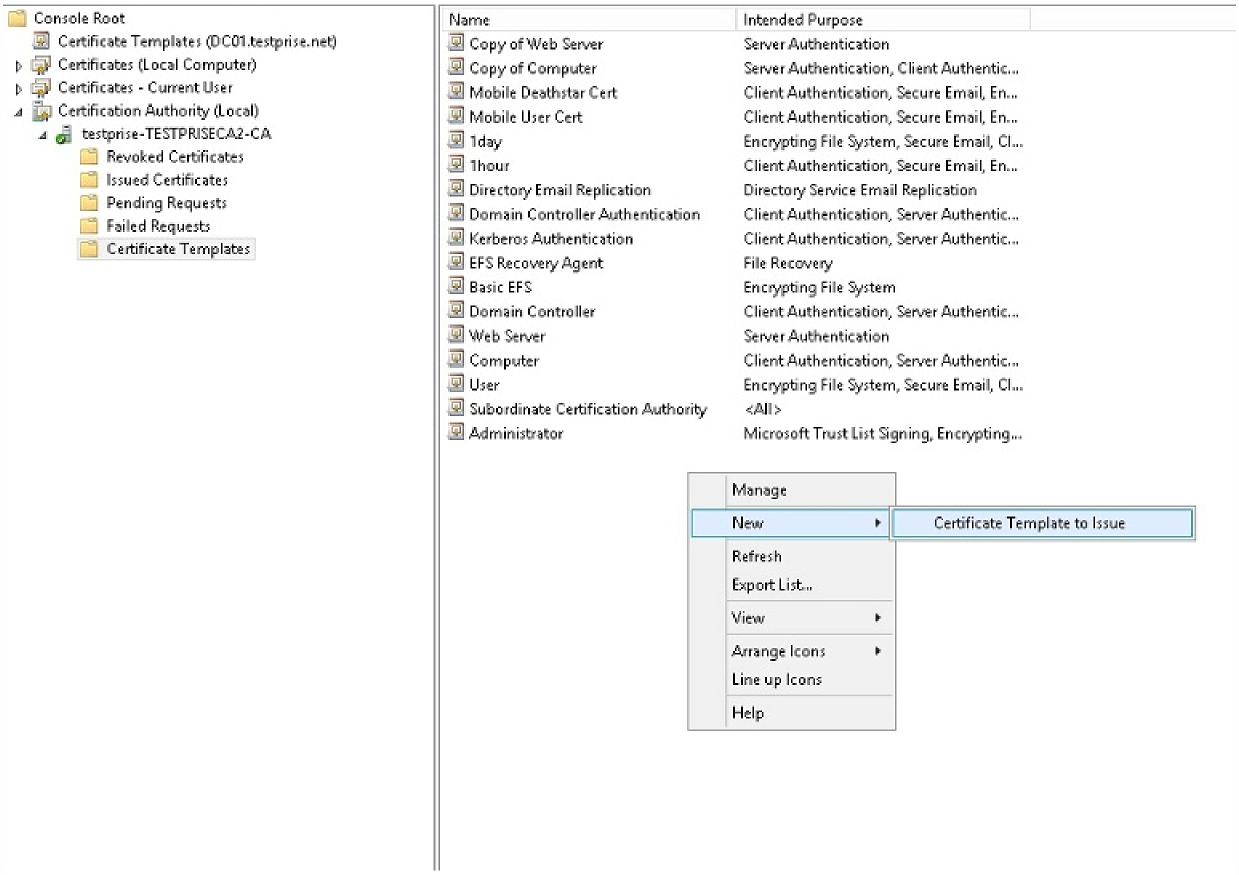
Current settings for this certificate template allow a client to submit a certificate request using any subject name and does not require approval by a certificate manager. Combining these certificate options may create a security risk and is not recommended.

* Control is disabled due to compatibility settings.

Adding the template to Certificate Authority

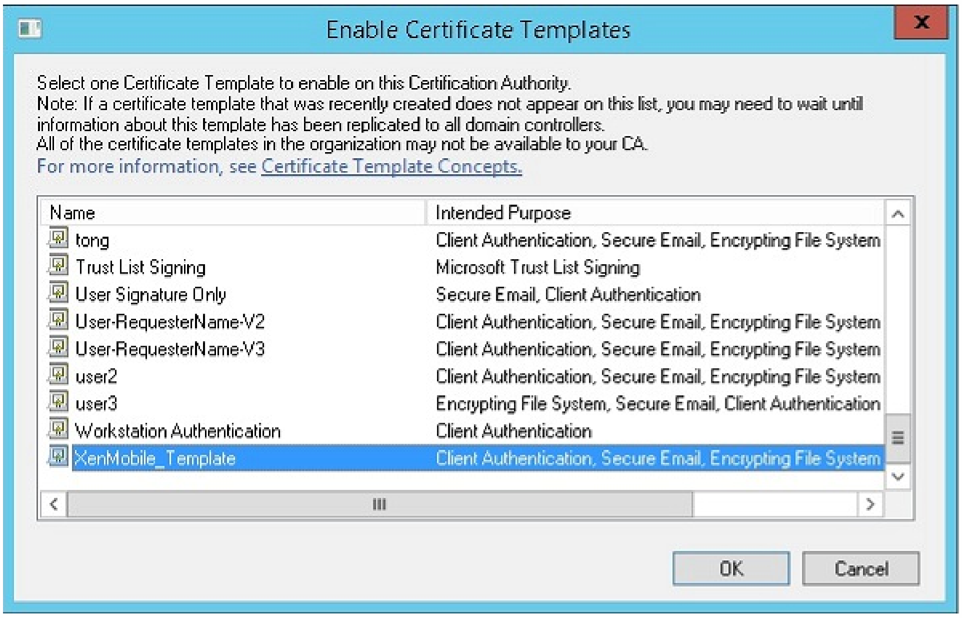
1. Go to **Certificate Authority** and select **Certificate Templates**.

2. Right-click in the right pane and then select **New > Certificate Template to Issue**.


Console Root
Certificate Templates (DC01.testprise.net)
Certificates (Local Computer)
Certificates - Current User
Certification Authority (Local)
testprise-TESTPRISECA2-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Manage
New
Certificate Template to Issue
Refresh
Export List...
View
Arrange Icons
Line up Icons
Help

Name	Intended Purpose
Copy of Web Server	Server Authentication
Copy of Computer	Server Authentication, Client Authentic...
Mobile Deathstar Cert	Client Authentication, Secure Email, En...
Mobile User Cert	Client Authentication, Secure Email, En...
1day	Encrypting File System, Secure Email, Cl...
1hour	Client Authentication, Secure Email, En...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

3. Select the template you created in the previous step and then click **OK** to add it into the **Certificate Authority**.



Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
tong	Client Authentication, Secure Email, Encrypting File System
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication
User-RequesterName-V2	Client Authentication, Secure Email, Encrypting File System
User-RequesterName-V3	Client Authentication, Secure Email, Encrypting File System
user2	Client Authentication, Secure Email, Encrypting File System
user3	Encrypting File System, Secure Email, Client Authentication
Workstation Authentication	Client Authentication
XenMobile_Template	Client Authentication, Secure Email, Encrypting File System

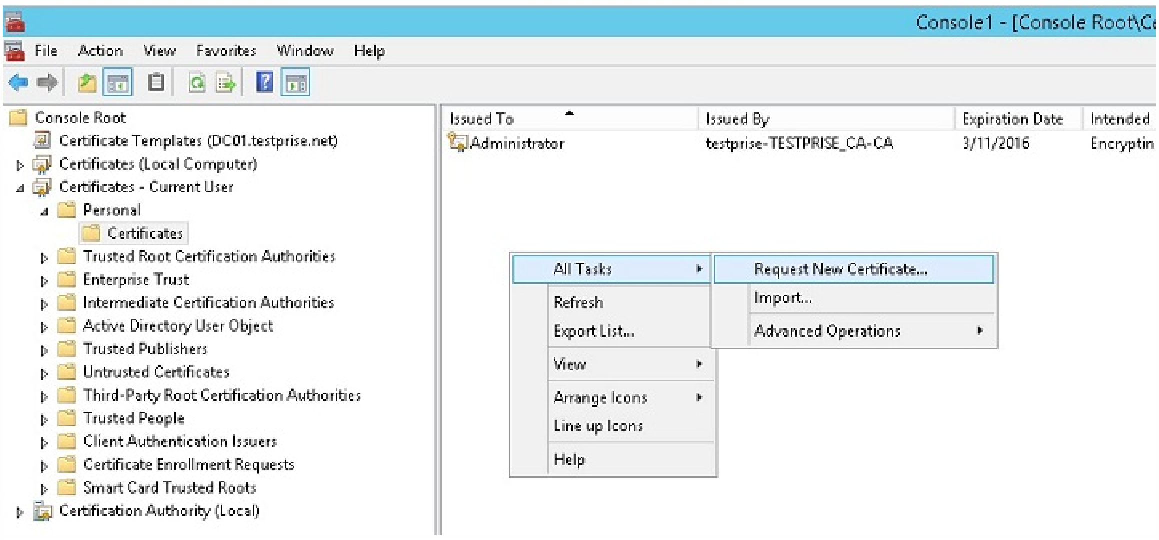
Creating a PFX certificate from the CA server

1. Create a user .pfx cert using the service account with which you logged in. This .pfx will be uploaded into XenMobile,

which will request a user certificate on behalf of the users who enroll their devices.

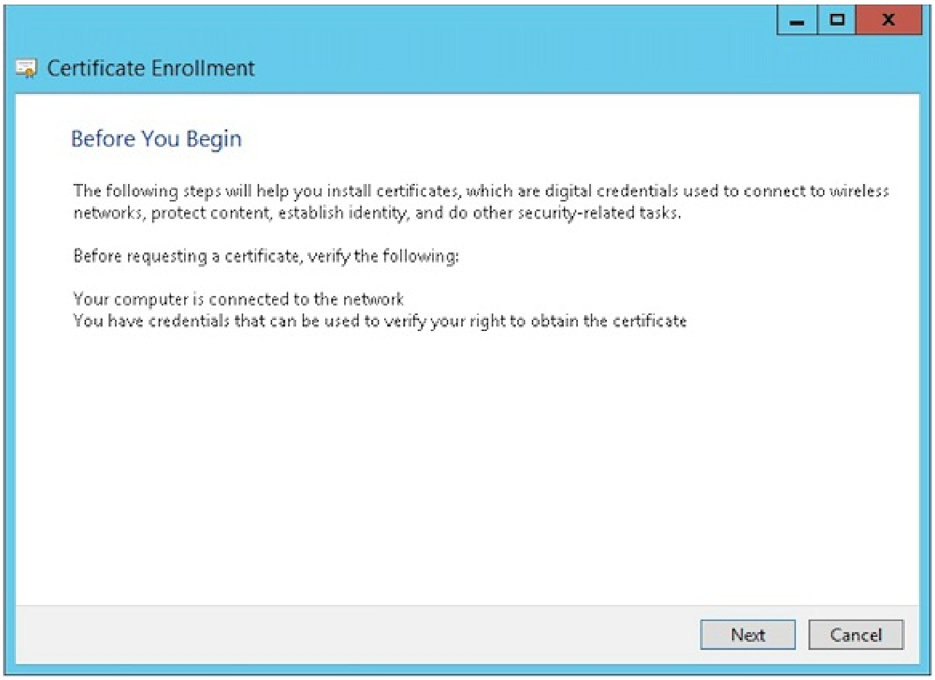
2. Under **Current User**, expand **Certificates**.

3. Right-click in the right pane and then click **Request New Certificate**.


Console1 - [Console Root\C
File
Action
View
Favorites
Window
Help
Console Root
Certificate Templates (DC01.testprise.net)
Certificates (Local Computer)
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots
Certification Authority (Local)
All Tasks
Refresh
Export List...
View
Arrange Icons
Line up Icons
Help
Request New Certificate...
Import...
Advanced Operations

Issued To	Issued By	Expiration Date	Intended
Administrator	testprise-TESTPRISE_CA-CA	3/11/2016	Encryptin

4. The **Certificate Enrollment** screen appears. Click **Next**.



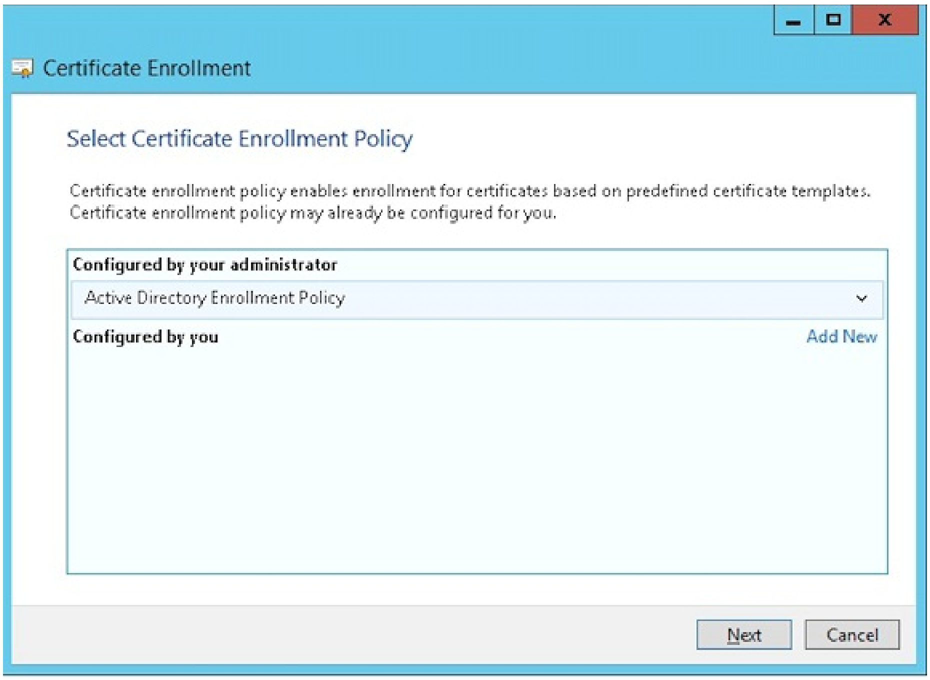
Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

5. Select **Active Directory Enrollment Policy** and then click **Next**.



Certificate Enrollment

Select Certificate Enrollment Policy

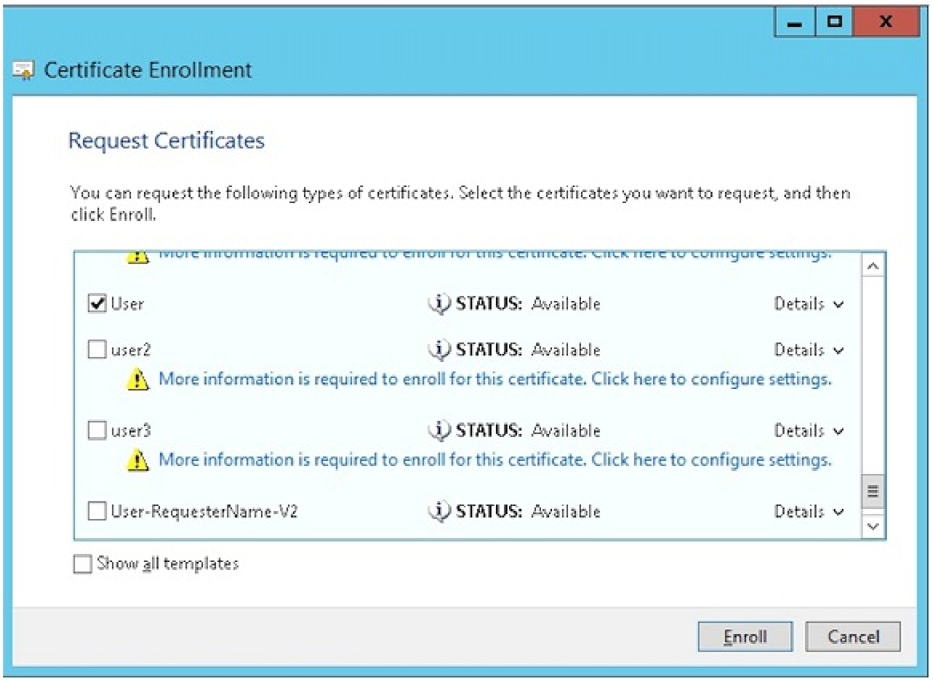
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

Configured by you

6. Select the **User** template and then click **Enroll**.



Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

More information is required to enroll for this certificate. Click here to configure settings.

☑ User — **STATUS:** Available — Details

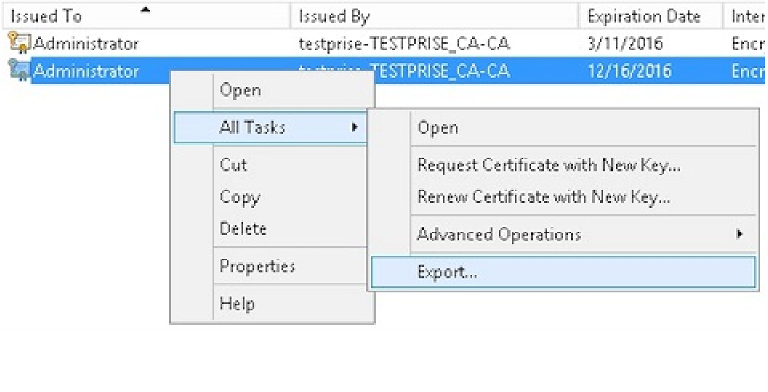
□ user2 — **STATUS:** Available — Details
More information is required to enroll for this certificate. Click here to configure settings.

□ user3 — **STATUS:** Available — Details
More information is required to enroll for this certificate. Click here to configure settings.

□ User-RequesterName-V2 — **STATUS:** Available — Details

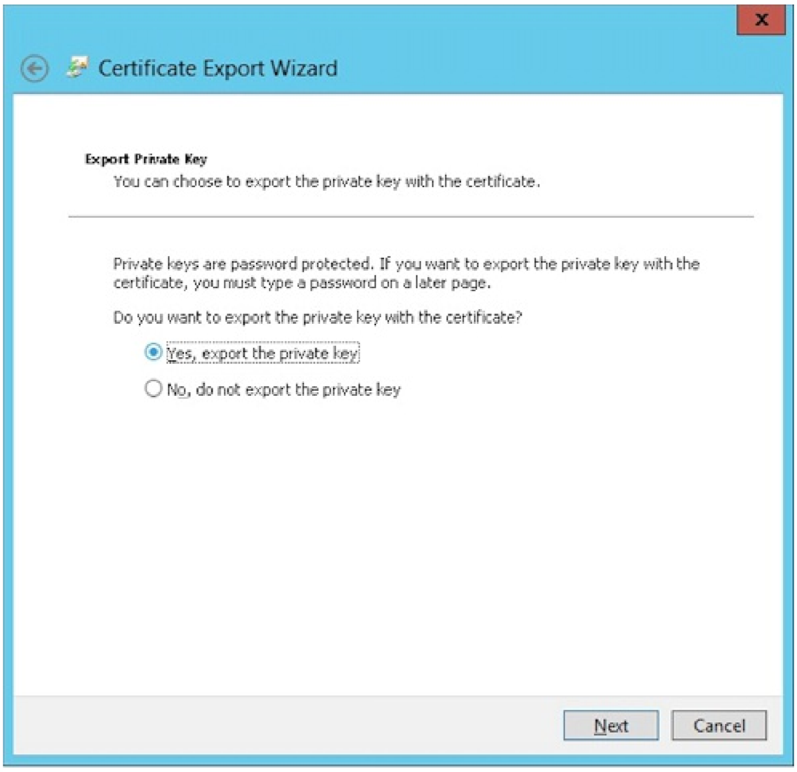
□ Show all templates

7. Export the .pfx file that you created in the previous step.



Issued To	Issued By	Expiration Date	Inter
Administrator	testprise-TESTPRISE_CA-CA	3/11/2016	Encr
Administrator	TESTPRISE_CA-CA	12/16/2016	Encr

8. Click **Yes, export the private key**.



Export Private Key

You can choose to export the private key with the certificate.

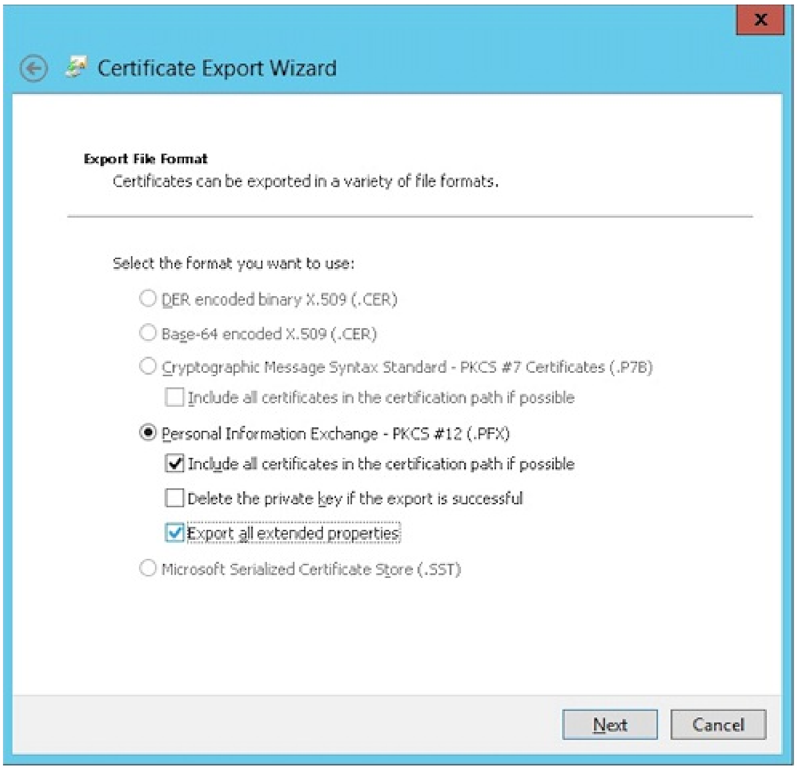
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

9. Select **Include all certificates in the certification path if possible** and select the **Export all extended properties** check box.

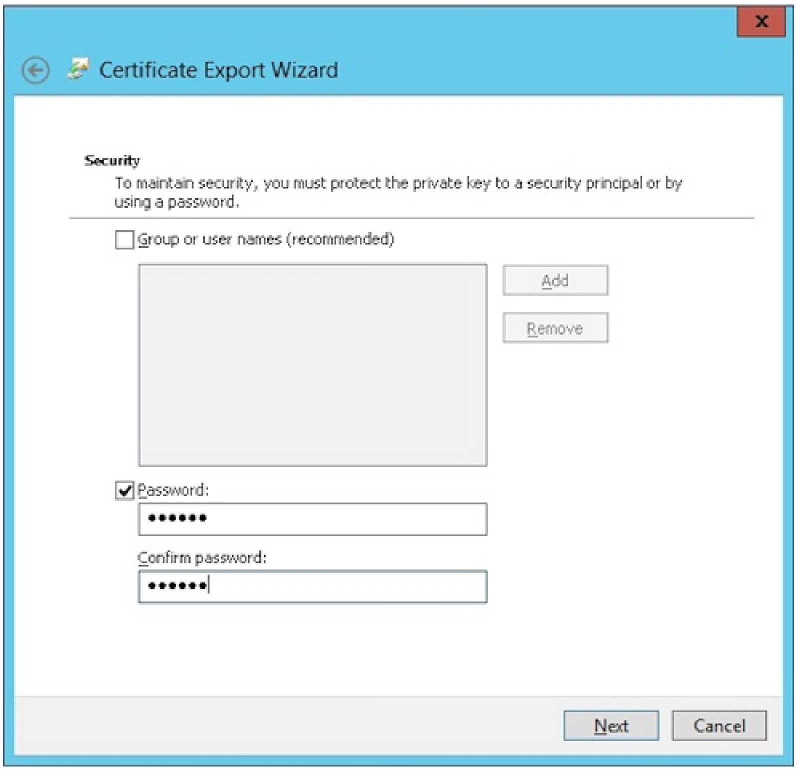

Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
● Personal Information Exchange - PKCS #12 (.PFX)
☑ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
☑ Export all extended properties
○ Microsoft Serialized Certificate Store (.SST)

10. Set a password that you'll use when uploading this certificate into XenMobile.


Certificate Export Wizard

Security
To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

☑ Password:
••••••

Confirm password:
••••••

11. Save the certificate onto your hard drive.

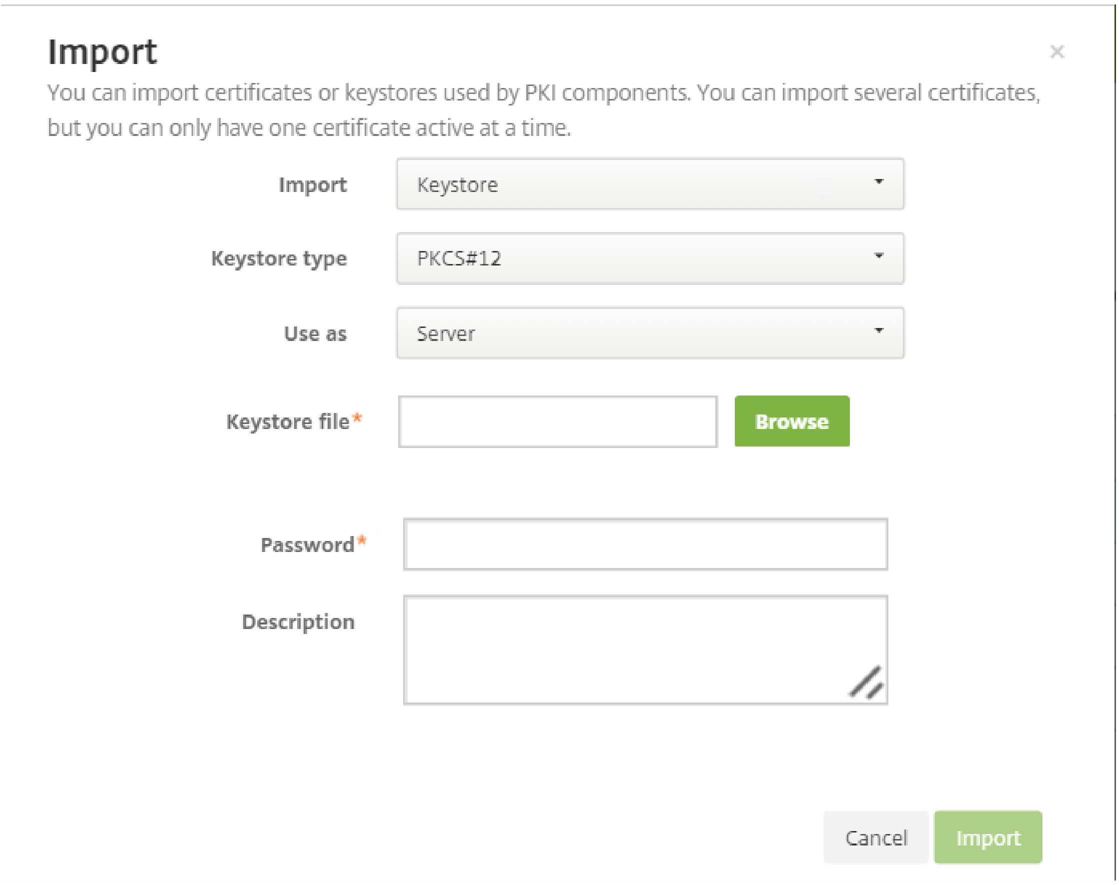
Uploading the certificate to XenMobile

1. In the XenMobile 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.



Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import: Keystore

Keystore type: PKCS#12

Use as: Server

Keystore file*

Password*

Description

4. Click **Import**.

5. Verify that the certificate installed correctly. It should display as a User certificate.

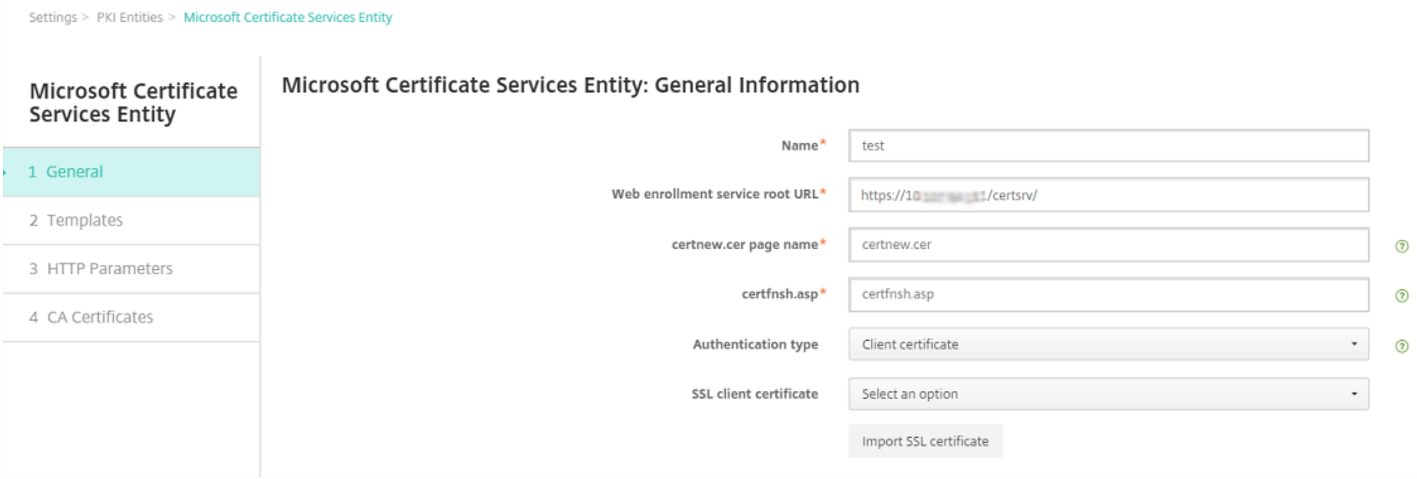
Creating the PKI entity for certificate-based authentication

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 XenMobile client certificate.



Settings > PKI Entities > Microsoft Certificate Services Entity

Microsoft Certificate Services Entity

1 General
2 Templates
3 HTTP Parameters
4 CA Certificates

Microsoft Certificate Services Entity: General Information

Name*: test

Web enrollment service root URL*: https://10[redacted]/certsrv/

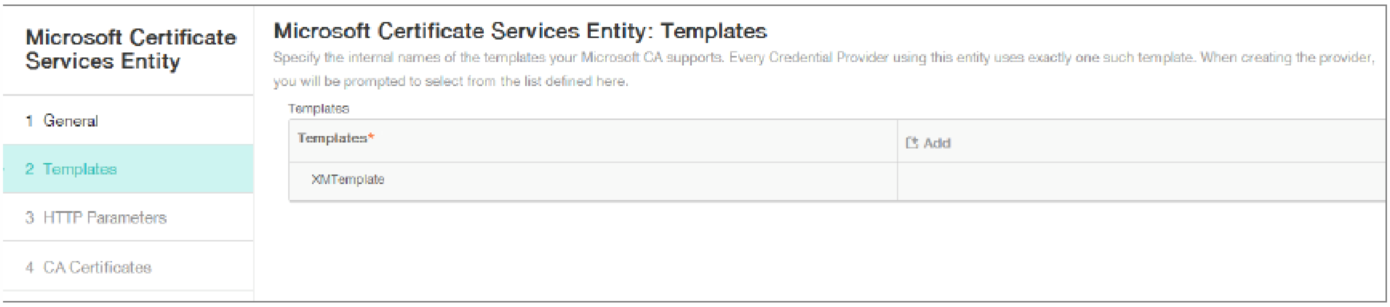
certnew.cer page name*: certnew.cer

certfnsh.asp*: certfnsh.asp

Authentication type: Client certificate

SSL client certificate: Select an option

4. Under **Templates**, add the template that you created when configuring the Microsoft certificate. Be sure not to add spaces.



Microsoft Certificate Services Entity

1 General
2 Templates
3 HTTP Parameters
4 CA Certificates

Microsoft Certificate Services Entity: Templates

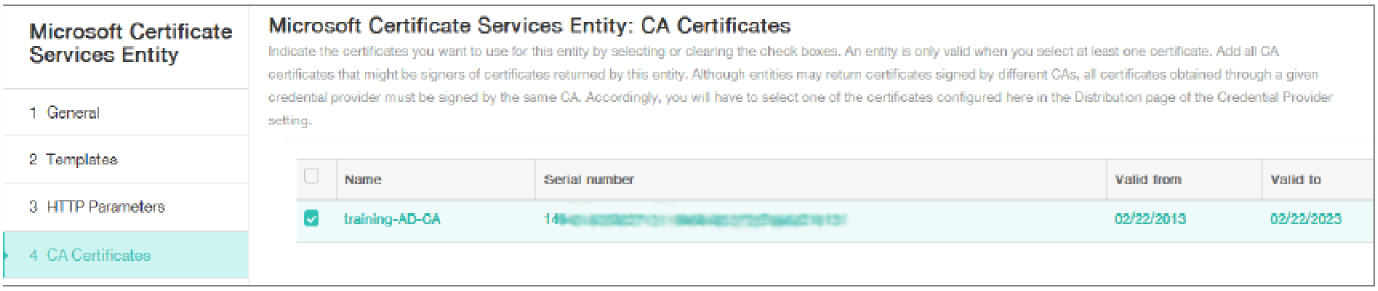
Specify the internal names of the templates your Microsoft CA supports. Every Credential Provider using this entity uses exactly one such template. When creating the provider, you will be prompted to select from the list defined here.

Templates

Templates*	Add
XMTemplate	

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 XenMobile client certificate.



Microsoft Certificate Services Entity

1 General
2 Templates
3 HTTP Parameters
4 CA Certificates

Microsoft Certificate Services Entity: CA Certificates

Indicate the certificates you want to use for this entity by selecting or clearing the check boxes. An entity is only valid when you select at least one certificate. Add all CA certificates that might be signers of certificates returned by this entity. Although entities may return certificates signed by different CAs, all certificates obtained through a given credential provider must be signed by the same CA. Accordingly, you will have to select one of the certificates configured here in the Distribution page of the Credential Provider setting.

□	Name	Serial number	Valid from	Valid to
☑	training-AD-CA	14[redacted]	02/22/2013	02/22/2023

7. Click **Save**.

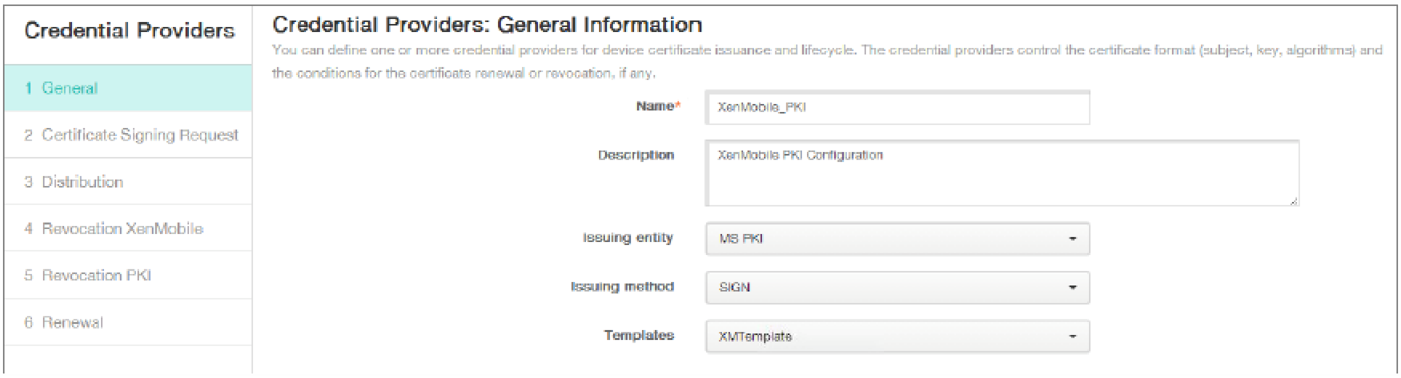
Configuring credentials providers

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.



Credential Providers

1 General
2 Certificate Signing Request
3 Distribution
4 Revocation XenMobile
5 Revocation PKI
6 Renewal

Credential Providers: General Information

You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.

Name*: XenMobile_PKI

Description: XenMobile PKI Configuration

Issuing entity: MS PKI

Issuing method: SIGN

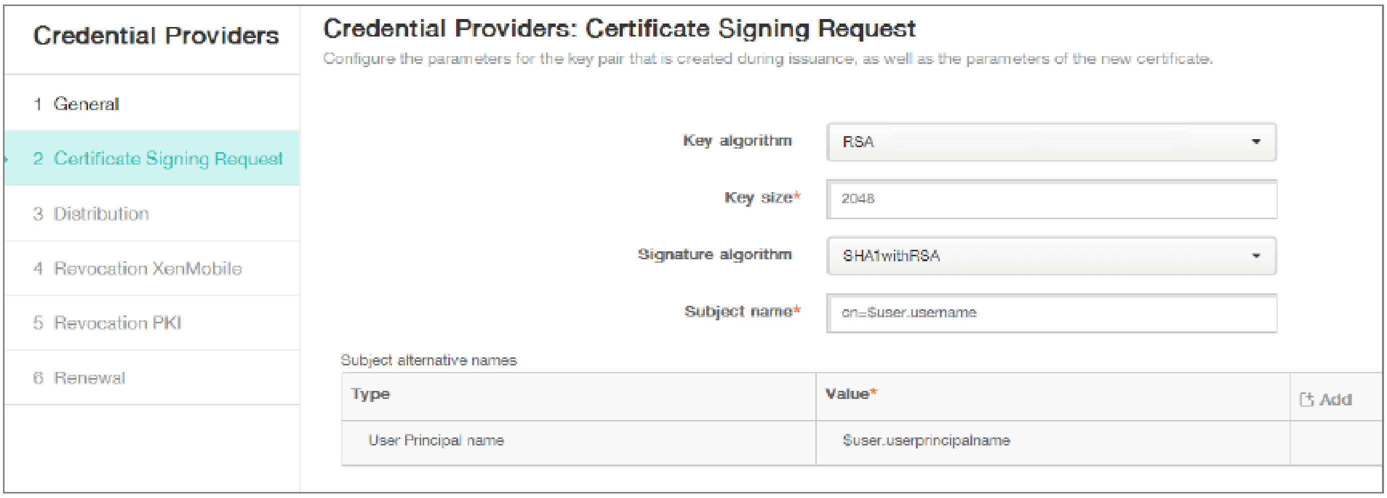
Templates: XMTemplate

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



Credential Providers

1 General
2 Certificate Signing Request
3 Distribution
4 Revocation XenMobile
5 Revocation PKI
6 Renewal

Credential Providers: Certificate Signing Request

Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.

Key algorithm: RSA

Key size*: 2048

Signature algorithm: SHA1withRSA

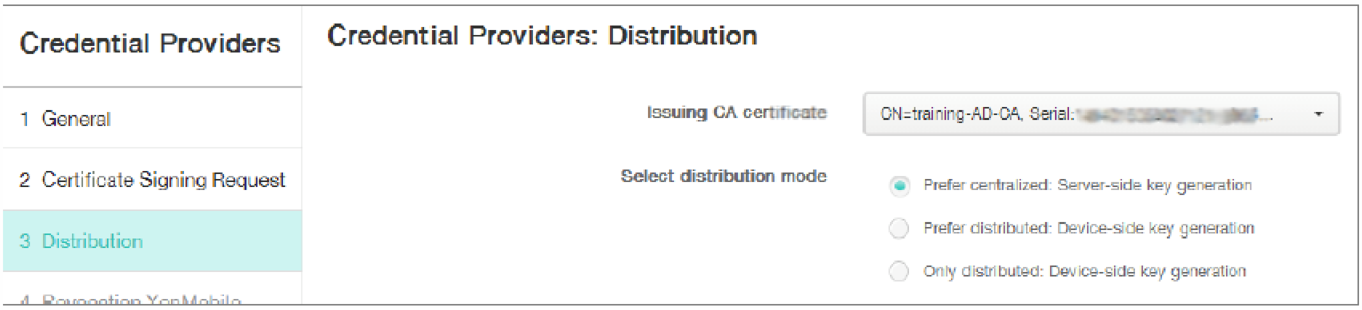
Subject name*: cn=$user.username

Subject alternative names

Type	Value*	Add
User Principal name	$user.userprincipalname	

5. Click **Distribution** and enter the following parameters:

- **Issuing CA certificate**: Select the Issuing CA that signed the XenMobile Client Certificate.
- **Select distribution mode**: Select **Prefer centralized: Server-side key generation**.



Credential Providers

1 General
2 Certificate Signing Request
3 Distribution
4 Revocation XenMobile

Credential Providers: Distribution

Issuing CA certificate: CN=training-AD-CA, Serial: [redacted]...

Select distribution mode:

● Prefer centralized: Server-side key generation

○ Prefer distributed: Device-side key generation

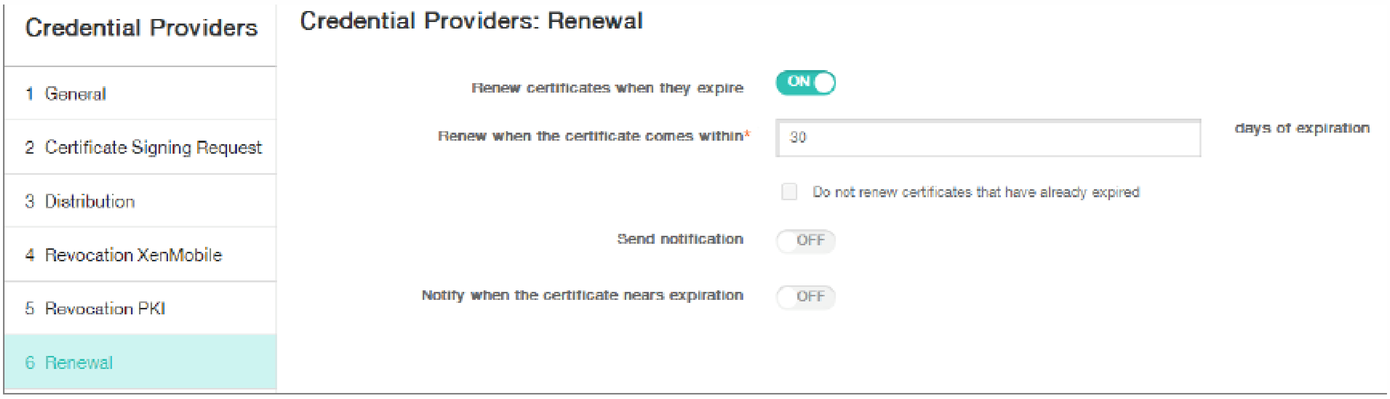
○ Only distributed: Device-side key generation

6. For the next two sections -- **Revocation XenMobile** and **Revocation PKI** -- set the parameters as required. For the purpose of this article, 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.



Credential Providers

1 General
2 Certificate Signing Request
3 Distribution
4 Revocation XenMobile
5 Revocation PKI
6 Renewal

Credential Providers: Renewal

Renew certificates when they expire: ON

Renew when the certificate comes within*: 30 days of expiration

□ Do not renew certificates that have already expired

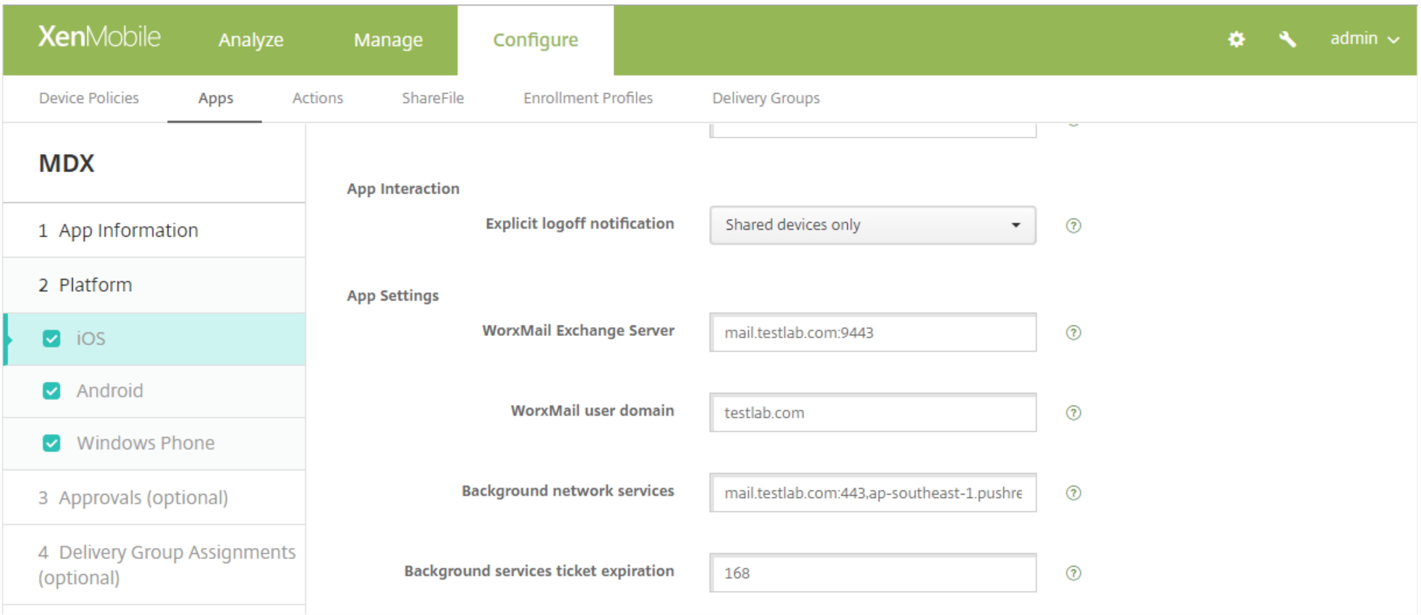
Send notification: OFF

Notify when the certificate nears expiration: OFF

10. Click **Save**.

Configuring Secure Mail to use certificate-based authentication

When you add Secure Mail to XenMobile, be sure to configure the Exchange settings under **App Settings**.



App Interaction

Explicit logoff notification: Shared devices only

App Settings

WorxMail Exchange Server: mail.testlab.com:9443

WorxMail user domain: testlab.com

Background network services: mail.testlab.com:443,ap-southeast-1.pushre

Background services ticket expiration: 168

Configuring NetScaler certificate delivery in XenMobile

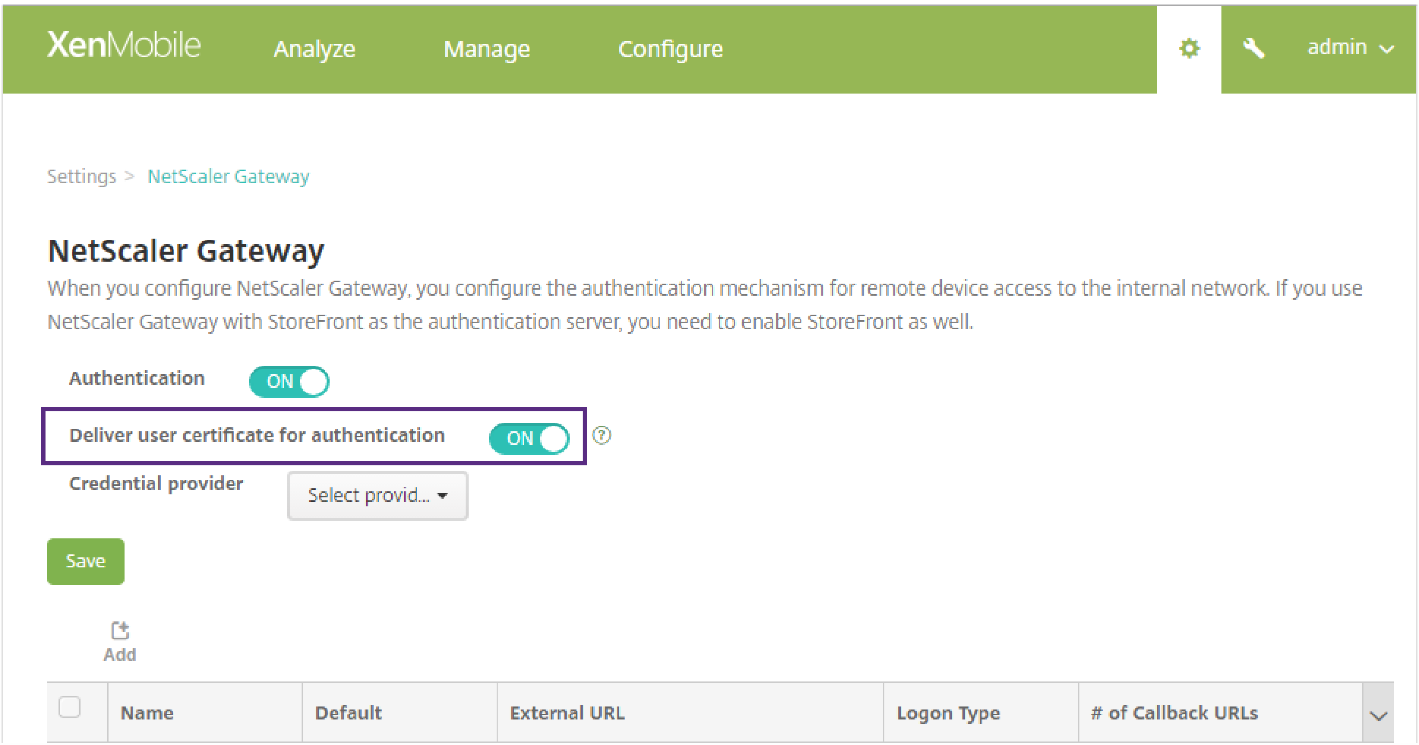
1. Log on to the XenMobile console and click the gear icon in the upper-right corner. The **Settings** screen appears.

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

3. If NetScaler Gateway isn't already added, click **Add** and specify the settings:

- **External URL**: https://YourNetScalerGatewayURL
- **Logon Type**: Certificate
- **Password Required**: OFF
- **Set as Default**: ON

4. For **Deliver user certificate for authentication**, select **On**.



NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication: ON

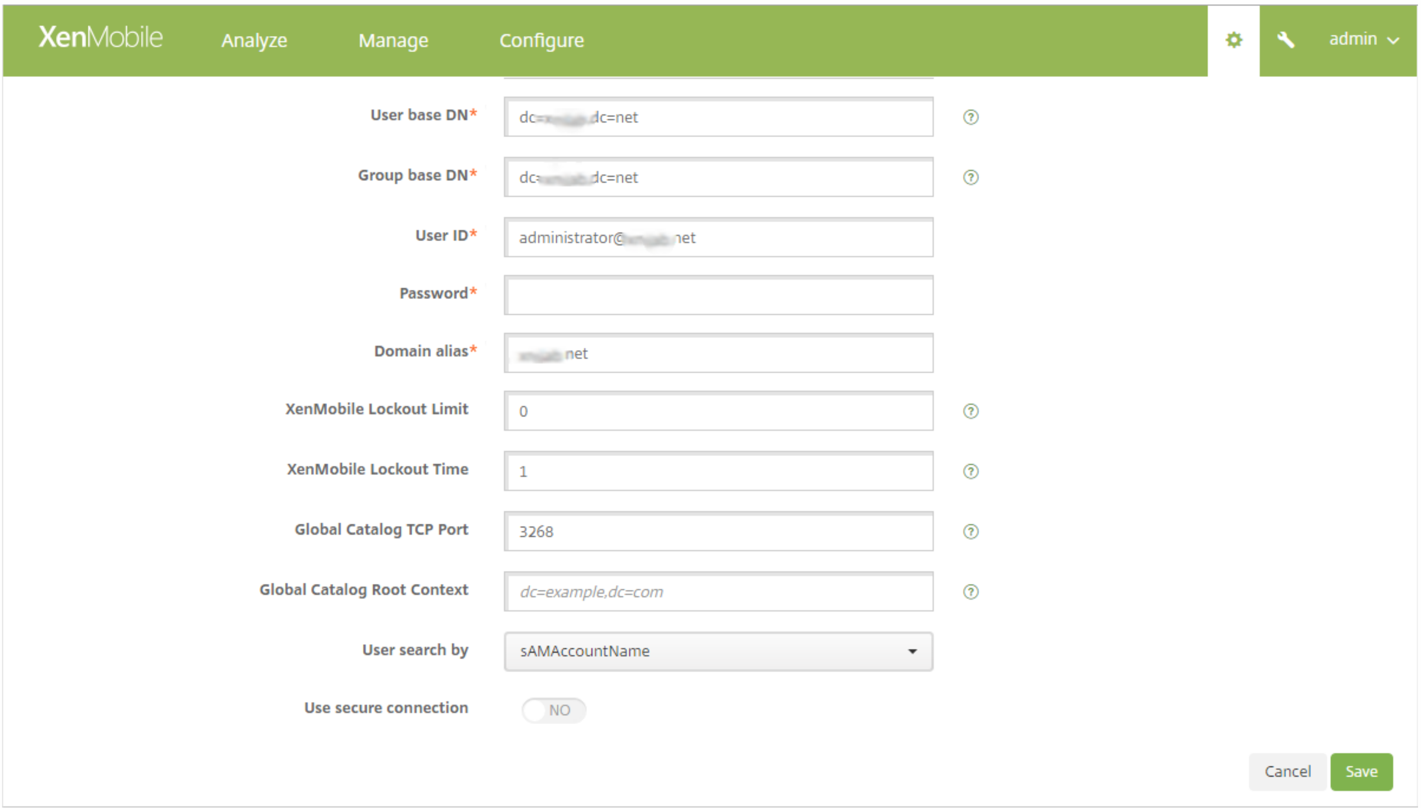
Deliver user certificate for authentication: ON

Credential provider: Select provid...

□	Name	Default	External URL	Logon Type	# of Callback URLs

5. For **Credential Provider**, select a provider and then click **Save**.

6. If you will use sAMAccount attributes in the user certificates as an alternative to User Principal Name (UPN), configure the LDAP connector in XenMobile as follows: Go to **Settings > LDAP**, select the directory and click **Edit**, and select **sAMAccountName** in **User search by**.



User base DN*: dc=[redacted],dc=net

Group base DN*: dc=[redacted],dc=net

User ID*: administrator@[redacted].net

Password*:

Domain alias*: [redacted].net

XenMobile Lockout Limit: 0

XenMobile Lockout Time: 1

Global Catalog TCP Port: 3268

Global Catalog Root Context: dc=example,dc=com

User search by: sAMAccountName

Use secure connection: NO

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

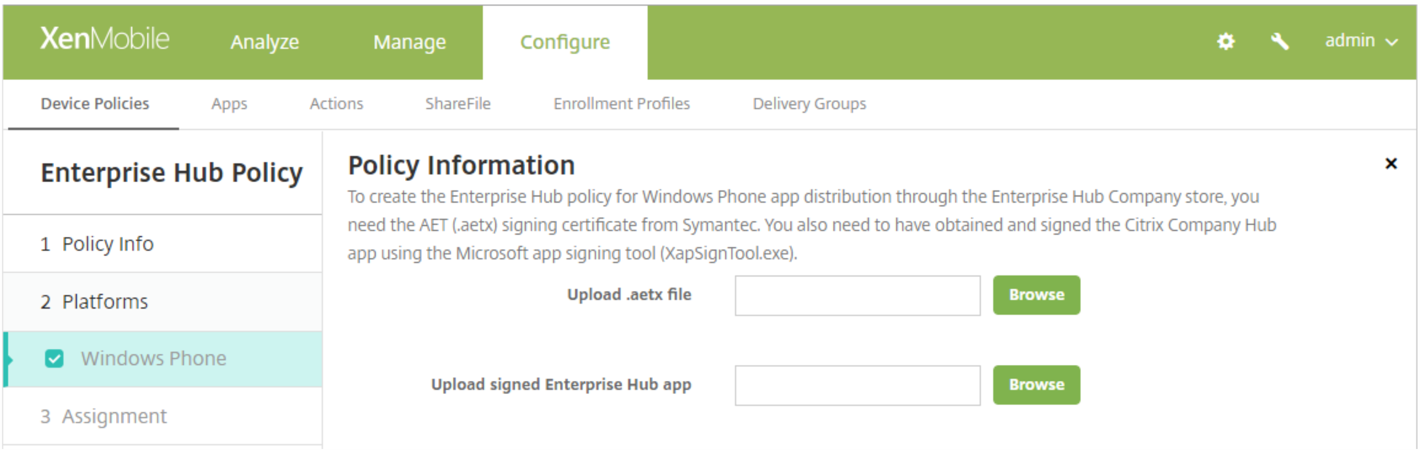
For Windows Phone devices, you must create an Enterprise Hub device policy to deliver the AETX file and the Secure Hub client.

> **Note**
>
> Ensure that both the AETX and Secure Hub files were using the same enterprise certificate from the certificate provider and the same Publisher ID from the Windows Store developer account.

1. In the XenMobile console, click **Configure** > **Device Policies**.

2. Click **Add** and then, under **More** > **XenMobile 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.



Policy Information

To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe).

Upload .aetx file

Upload signed Enterprise Hub app

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 NetScaler Gateway configuration, the user workflow is as follows:

1. Users enroll their mobile device.

2. XenMobile prompts users to create a Citrix PIN.

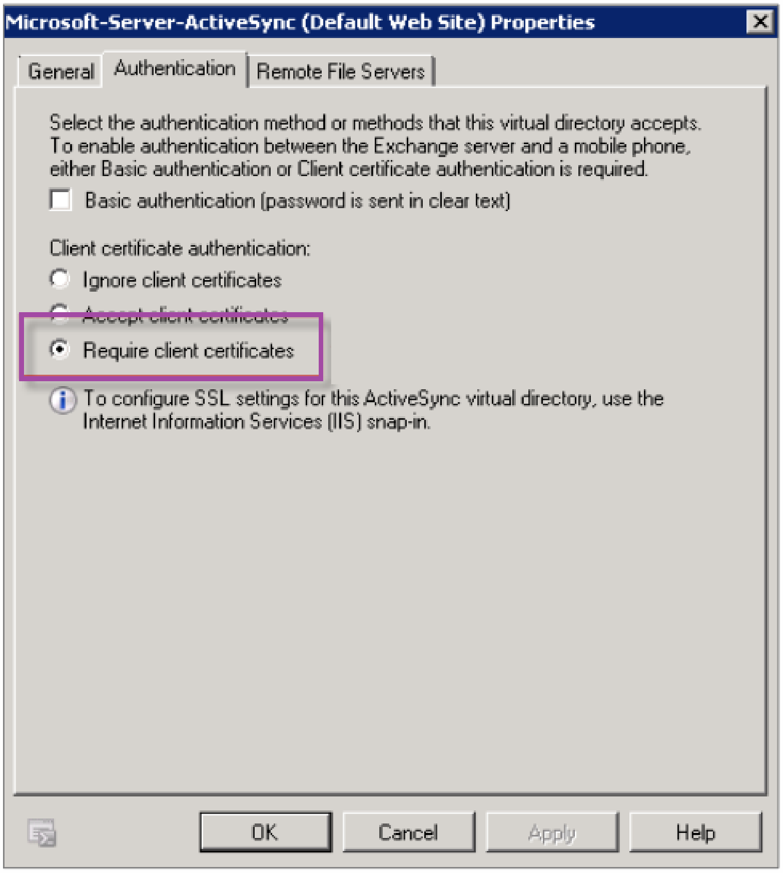
3. Users are then redirected to the XenMobile Store.

4. When users start Secure Mail, XenMobile will not prompt them for user credentials in order to configure their mailbox. Instead, Secure Mail requests the client certificate from Secure Hub and submits it to Microsoft Exchange Server for authentication. If XenMobile 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 is using private SSL server certificates to secure the traffic, verify that the Root/Intermediate certificates are installed on the mobile device.

2. Verify that the authentication type selected for ActiveSync is **Require client certificates**.



Select the authentication method or methods that this virtual directory accepts. To enable authentication between the Exchange server and a mobile phone, either Basic authentication or Client certificate authentication is required.

□ Basic authentication (password is sent in clear text)

Client certificate authentication:

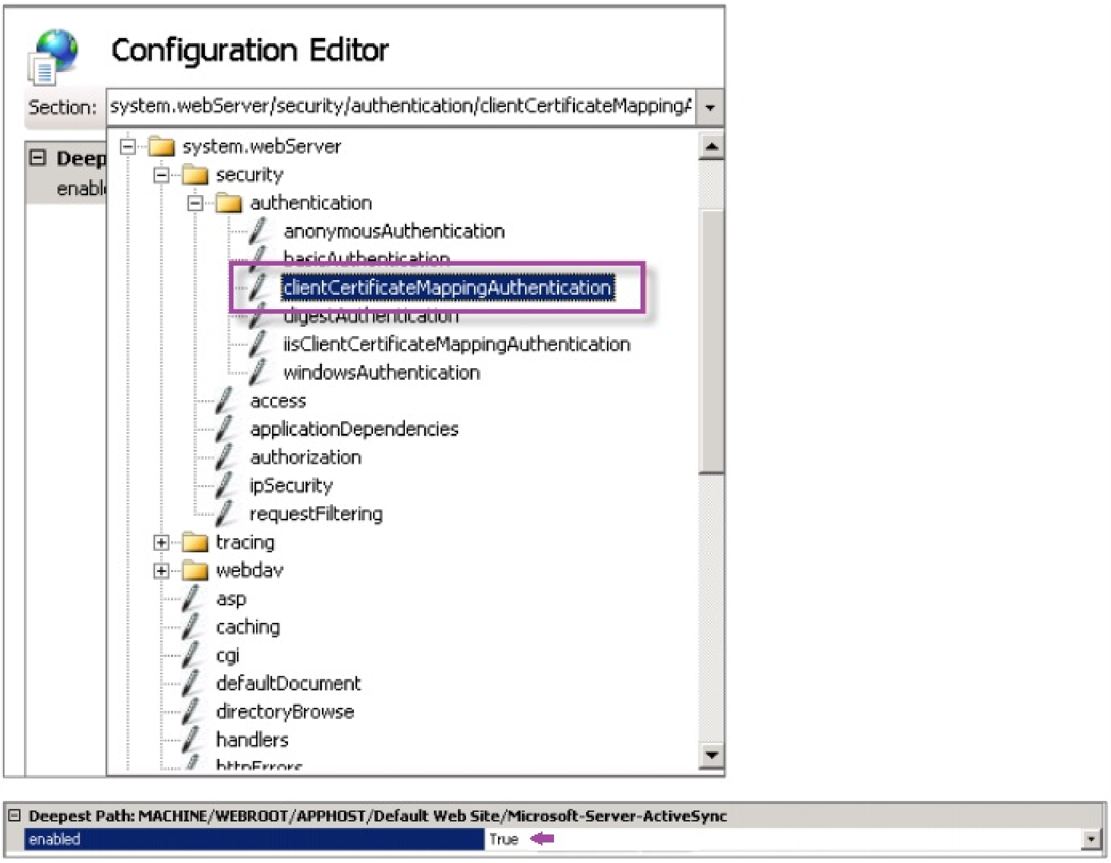
○ Ignore client certificates

○ Accept client certificates

● Require client certificates

To configure SSL settings for this ActiveSync virtual directory, use the Internet Information Services (IIS) snap-in.

3. On Microsoft Exchange Server, check the **Microsoft-Server-ActiveSync** site to have client certificate mapping authentication enabled (by default it is disabled). The option is under **Configuration Editor** > **Security** > **Authentication**.



Section: system.webServer/security/authentication/clientCertificateMappingA

Deepest Path: MACHINE/WEBROOT/APPHOST/Default Web Site/Microsoft-Server-ActiveSync

enabled True

Note: After selecting **True**, be sure to click **Apply** for the changes take effect.

4. Check the NetScaler Gateway settings in the XenMobile console: Ensure that **Deliver user certificate for authentication** is **ON** and that **Credential provider** has the correct profile selected, as described earlier in "To configure NetScaler certificate delivery in XenMobile."

To determine if the client certificate was delivered to a mobile device:

1. In the XenMobile console, go to **Manage** > **Devices** and select the device.

2. Click **Edit** or **Show More**.

3. Go to the **Delivery Groups** section, and search for this entry:

    NetScaler Gateway Credentials : Requested credential, CertId=

To validate whether client certificate negotiation is enabled:

1. Run this netsh command to show the SSL Certificate configuration that is bound on the IIS website:

```
netsh http show sslcert
```

2. If the value for **Negotiate Client Certificate** is **Disabled**, run the following command to enable it:

```
netsh http delete sslcert ipport=0.0.0.0:443
netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={app_id} certstorename=store_name verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

For Example:

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c5435c94e05da appid={4dc3e181-e14b-4a21-b022-59fc669b0914} 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 XenMobile:

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

If Secure Mail won't install successfully on Windows Phone 8.1:

- Verify that the Application Enrollment Token (.AETX) file is delivered through XenMobile using the Enterprise Hub device policy.
- Verify that 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.
- Verify that the same Publisher ID is being used to sign and wrap Secure Hub, Secure Mail, and the Application Enrollment Token.

PKI entities

Oct 02, 2017

A XenMobile 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 XenMobile. Internal components are referred to as discretionary. External components are part of your corporate infrastructure.

XenMobile supports the following types of PKI entities:

- Generic PKIs (GPKIs)

  XenMobile Server GPKI support includes Symantec Managed PKI.

- Microsoft Certificate Services
- Discretionary Certificate Authorities (CAs)

XenMobile 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.

When you configure a PKI entity, indicate to XenMobile 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 XenMobile 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, to avoid possible authentication issues with enrolled devices, avoid using special characters in the template name. For example: ! : $ ( ) # % + * ~ ? | { } [ ]

Generic PKI

The Generic PKI (GPKI) protocol is a proprietary XenMobile 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 XenMobile with that WSDL definition, either through a URL or by uploading the file itself.

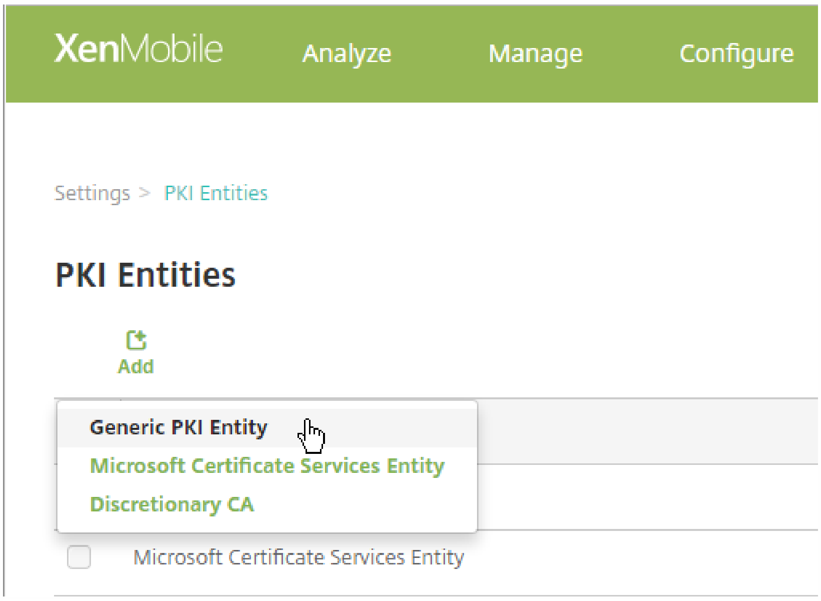
Support for each of the PKI operations in an adapter is optional. If an adapter supports a given operation, the adapter is said to have the corresponding capability (sign, fetch, or revoke). Each of these capabilities may be associated with a set of user parameters.

User parameters are parameters that the GPKI adapter defines for a specific operation and for which you must provide values to XenMobile. XenMobile 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 XenMobile and the GPKI adapter.

1. In the XenMobile console, click **Settings** > **PKI Entities**.

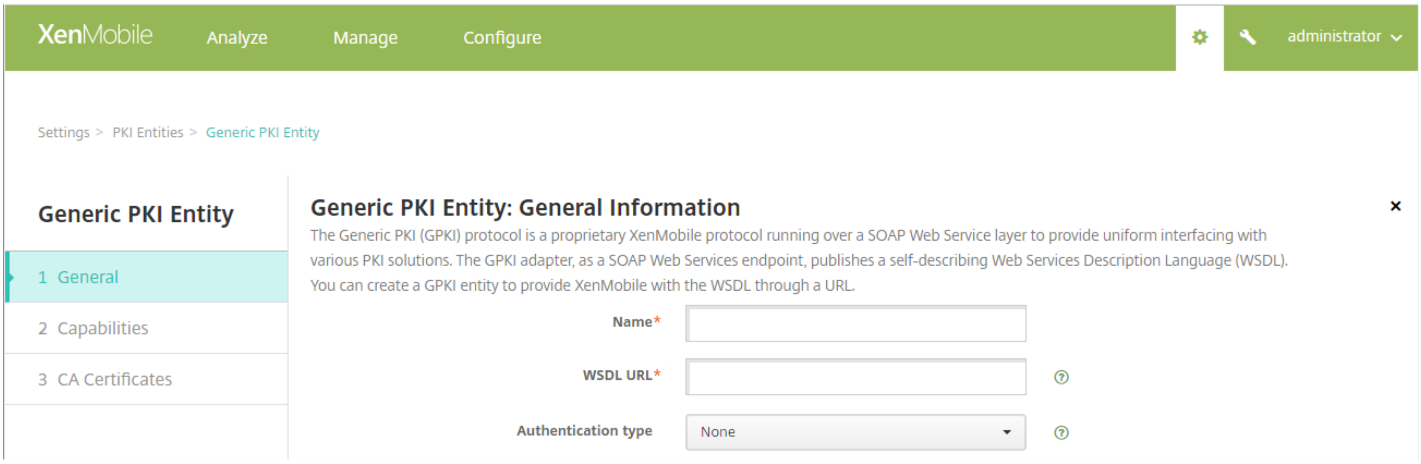
2. On the **PKI Entities** page, click **Add**.

A menu of PKI entity types appears.



3. Click **Generic PKI Entity**.

The Generic PKI Entity: General Information page appears.



Generic PKI Entity: General Information

The Generic PKI (GPKI) protocol is a proprietary XenMobile protocol running over a SOAP Web Service layer to provide uniform interfacing with various PKI solutions. The GPKI adapter, as a SOAP Web Services endpoint, publishes a self-describing Web Services Description Language (WSDL). You can create a GPKI entity to provide XenMobile with the WSDL through a URL.

Name*

WSDL URL*

Authentication type: None

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.

Note: 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.

Symantec Managed PKI

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

Prerequisites

- Access to Symantec Managed PKI Infrastructure

- Windows Server 2012 R2 server with the following components installed:
  - Java
  - Apache Tomcat
  - Symantec PKI Client
  - Portecle

  For information about installing those components, see "Set up Windows Server," next.
- Access to the XenMobile downloads site

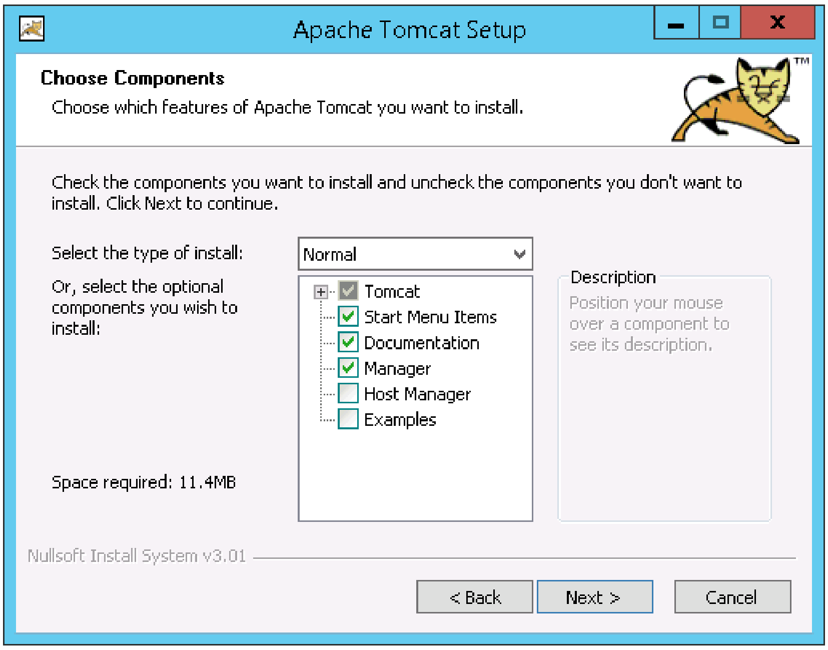
This section assists you in setting up Windows Server so that it meets the XenMobile requirements for GPKI support.

Install Java on Windows Server

Download Java from https://java.com/en/download/faq/java_win64bit.xml and then install it. In the Security Warning dialog box, be sure to 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, be sure to click **Run**. Complete the Apache Tomcat setup, using the following examples as a guide.



Apache Tomcat Setup

Choose Components

Choose which features of Apache Tomcat you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Normal

Or, select the optional components you wish to install:

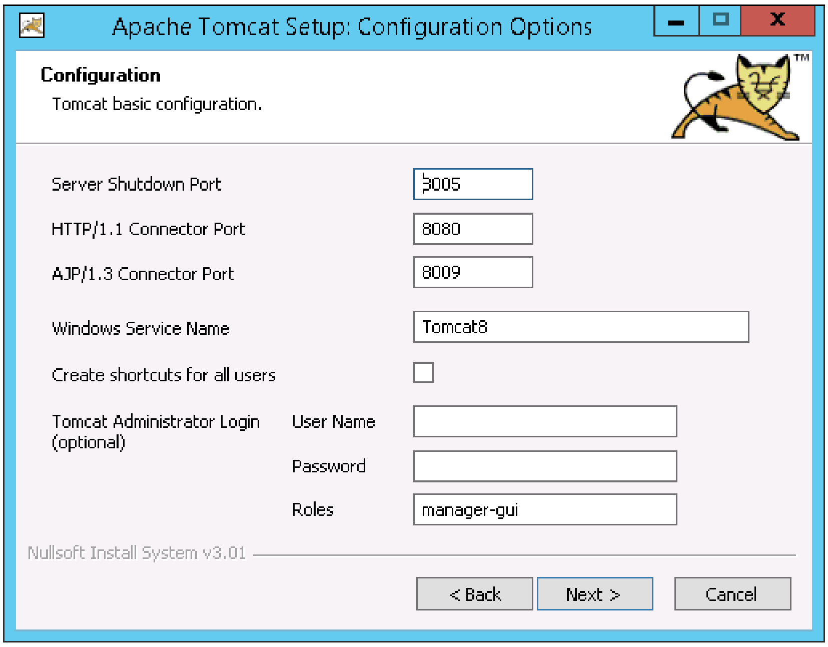
- ☑ Tomcat
  - ☑ Start Menu Items
  - ☑ Documentation
  - ☑ Manager
  - ☐ Host Manager
  - ☐ Examples

Description

Position your mouse over a component to see its description.

Space required: 11.4MB

Nullsoft Install System v3.01


Apache Tomcat Setup: Configuration Options

Configuration

Tomcat basic configuration.

Server Shutdown Port: 8005

HTTP/1.1 Connector Port: 8080

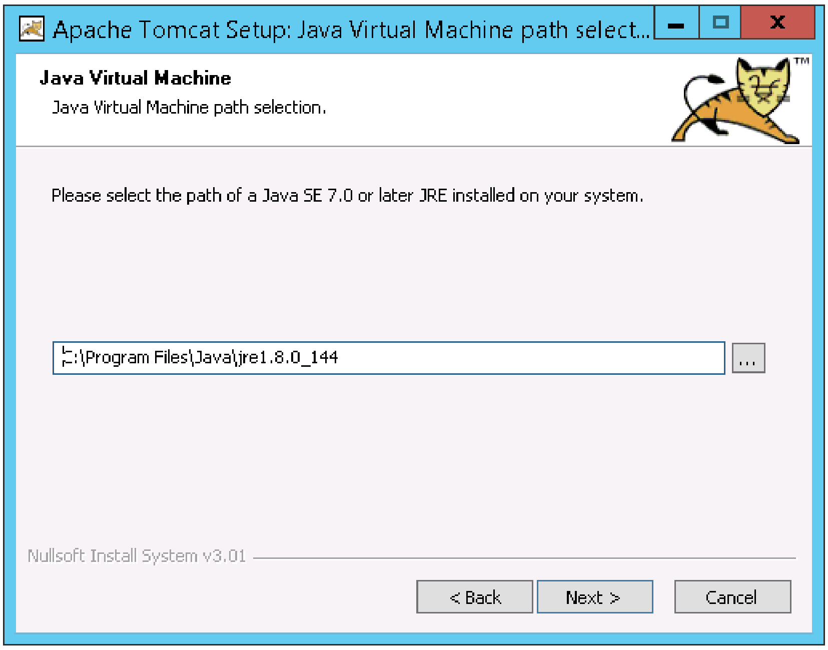
AJP/1.3 Connector Port: 8009

Windows Service Name: Tomcat8

Create shortcuts for all users: □

Tomcat Administrator Login (optional)
- User Name:
- Password:
- Roles: manager-gui

Nullsoft Install System v3.01


Apache Tomcat Setup: Java Virtual Machine path select...

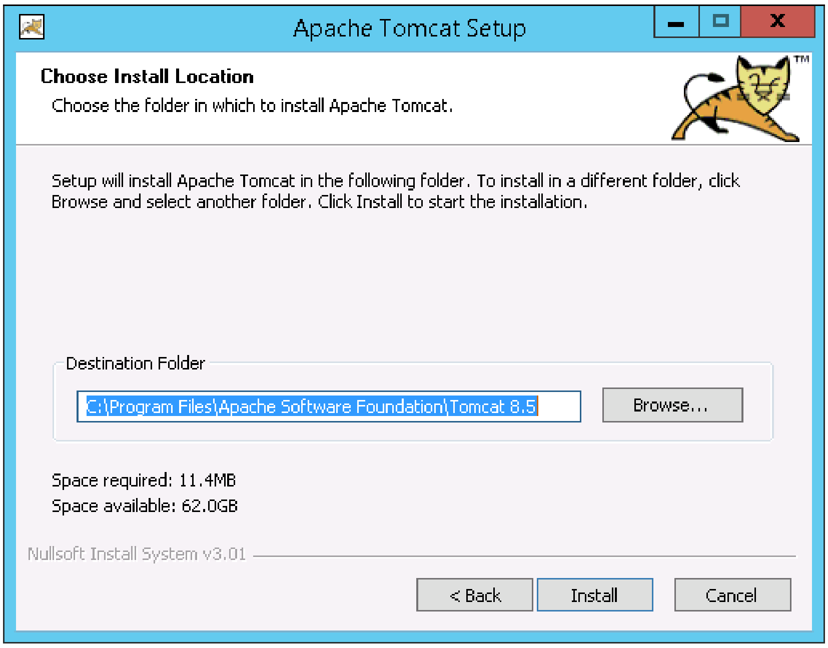
Java Virtual Machine

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

Nullsoft Install System v3.01



Apache Tomcat Setup

Choose Install Location

Choose the folder in which to install Apache Tomcat.

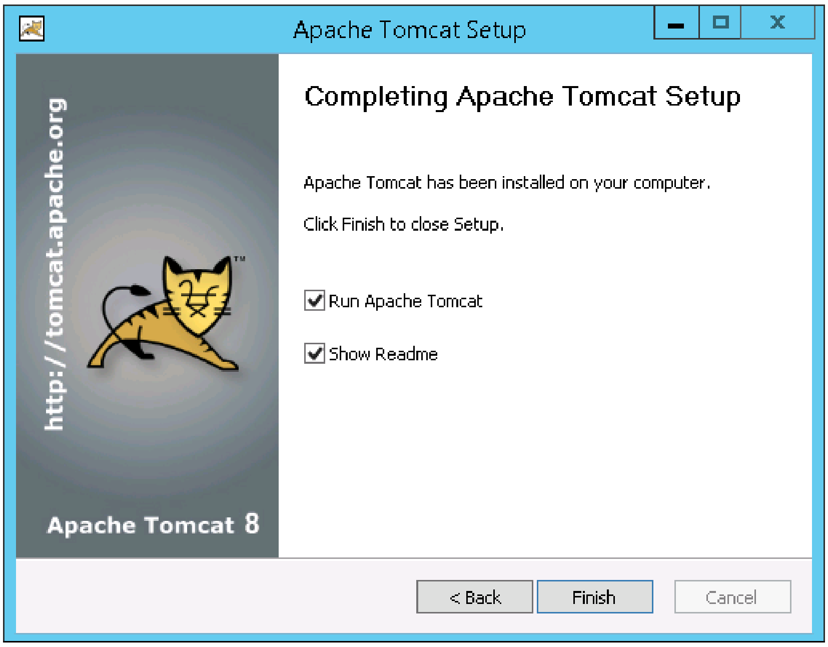
Setup will install Apache Tomcat in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

C:\Program Files\Apache Software Foundation\Tomcat 8.5

Space required: 11.4MB

Space available: 62.0GB



Apache Tomcat Setup

Completing Apache Tomcat Setup

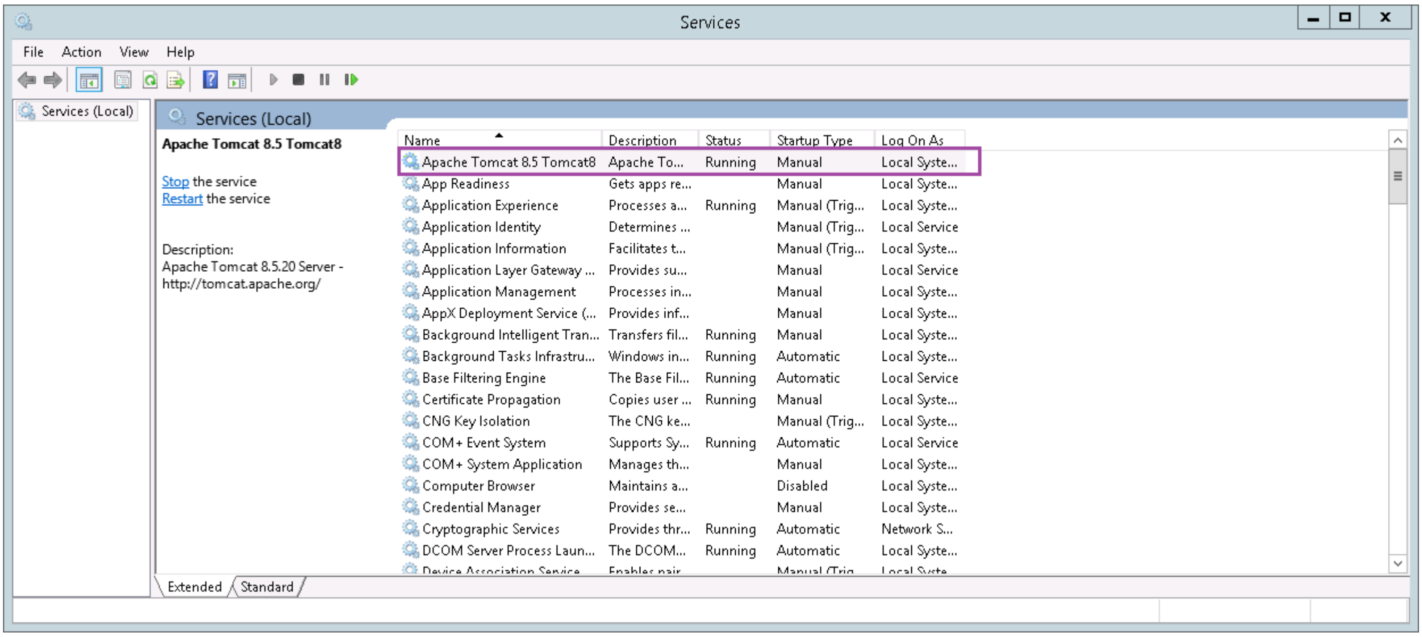
Apache Tomcat has been installed on your computer.

Click Finish to close Setup.

☑ Run Apache Tomcat

☑ Show Readme

Next, go to Windows Services and change **Startup Type** from **Manual** to **Automatic**.



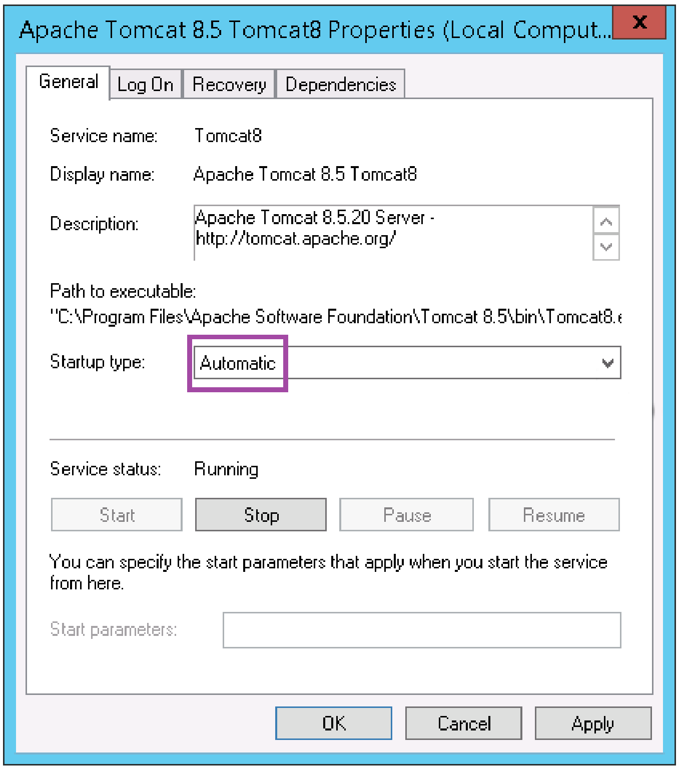
Services (Local)

Apache Tomcat 8.5 Tomcat8

Stop the service
Restart the service

Description:
Apache Tomcat 8.5.20 Server - http://tomcat.apache.org/

Name	Description	Status	Startup Type	Log On As
Apache Tomcat 8.5 Tomcat8	Apache To...	Running	Manual	Local Syste...
App Readiness	Gets apps re...		Manual	Local Syste...
Application Experience	Processes a...	Running	Manual (Trig...	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...		Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...		Manual	Local Syste...
Background Intelligent Tran...	Transfers fil...	Running	Manual	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Certificate Propagation	Copies user ...	Running	Manual	Local Syste...
CNG Key Isolation	The CNG ke...		Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...		Manual	Local Syste...
Computer Browser	Maintains a...		Disabled	Local Syste...
Credential Manager	Provides se...		Manual	Local Syste...
Cryptographic Services	Provides thr...	Running	Automatic	Network S...
DCOM Server Process Laun...	The DCOM...	Running	Automatic	Local Syste...
Device Association Service	Enables pair...		Manual (Trig...	Local Syste...


Apache Tomcat 8.5 Tomcat8 Properties (Local Comput...

Service name: Tomcat8

Display name: Apache Tomcat 8.5 Tomcat8

Description: Apache Tomcat 8.5.20 Server - http://tomcat.apache.org/

Path to executable:
"C:\Program Files\Apache Software Foundation\Tomcat 8.5\bin\Tomcat8.e

Startup type: Automatic

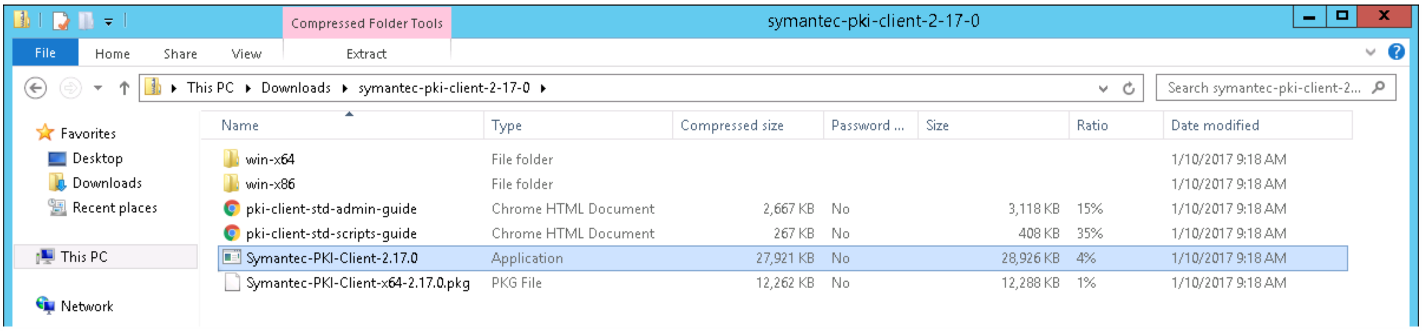
Service status: Running

You can specify the start parameters that apply when you start the service from here.

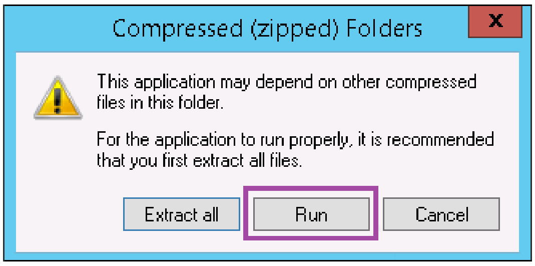
Start parameters:

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.


Compressed Folder Tools
symantec-pki-client-2-17-0
File
Home
Share
View
Extract
This PC ▸ Downloads ▸ symantec-pki-client-2-17-0 ▸
Search symantec-pki-client-2...
Favorites
Desktop
Downloads
Recent places
This PC
Network

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
win-x64	File folder					1/10/2017 9:18 AM
win-x86	File folder					1/10/2017 9:18 AM
pki-client-std-admin-guide	Chrome HTML Document	2,667 KB	No	3,118 KB	15%	1/10/2017 9:18 AM
pki-client-std-scripts-guide	Chrome HTML Document	267 KB	No	408 KB	35%	1/10/2017 9:18 AM
Symantec-PKI-Client-2.17.0	Application	27,921 KB	No	28,926 KB	4%	1/10/2017 9:18 AM
Symantec-PKI-Client-x64-2.17.0.pkg	PKG File	12,262 KB	No	12,288 KB	1%	1/10/2017 9:18 AM



This application may depend on other compressed files in this folder.

For the application to run properly, it is recommended that you first extract all files.

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

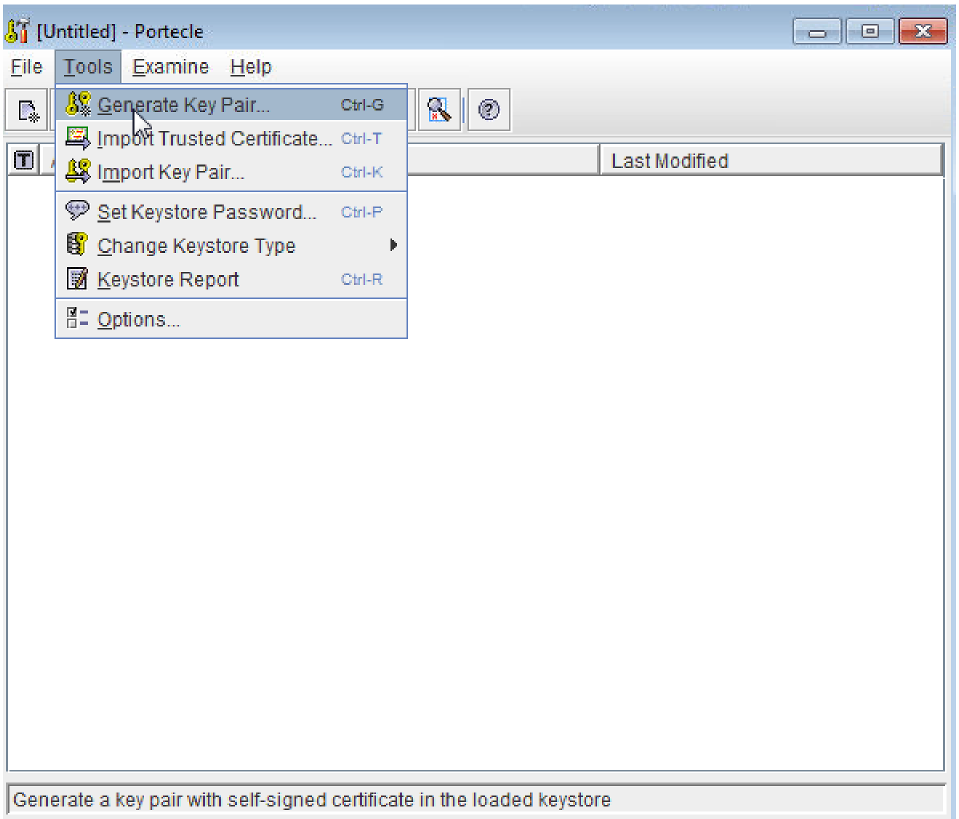
Download the installer from https://sourceforge.net/projects/portecleinstall/files/ and then unzip and run the installer.

Generate the registration authority (RA) certificate for Symantec 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.

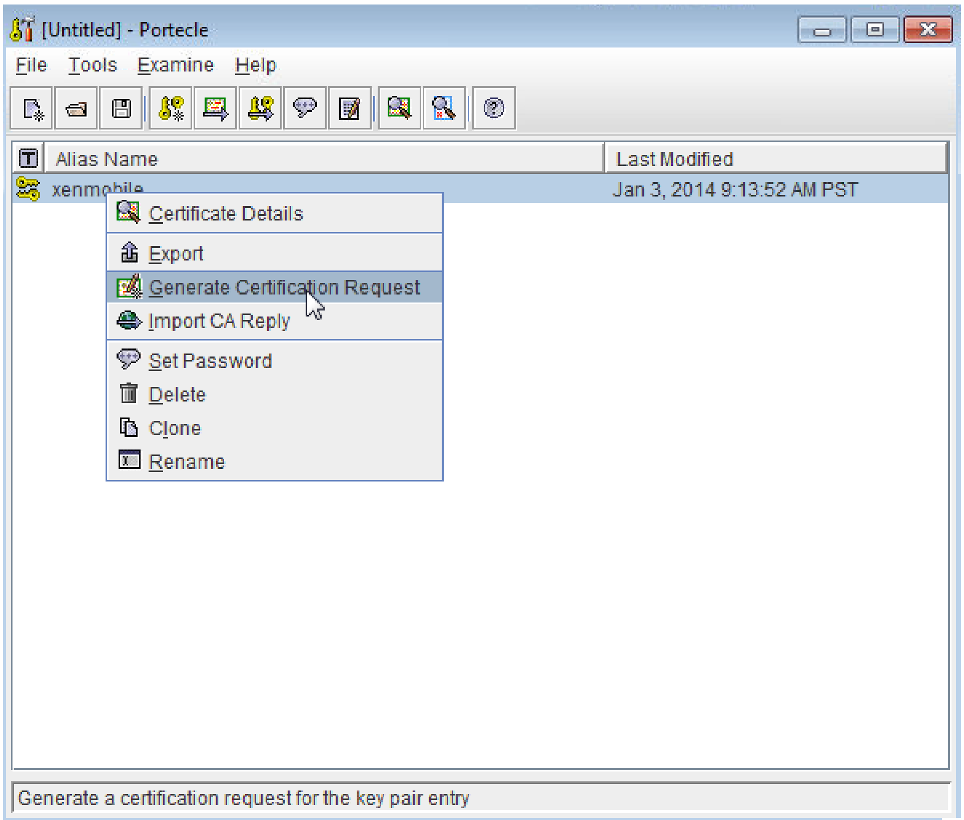
This article also describes how to upload the RA and public certificates.

1. In Portecle, go to **Tools** > **Generate Key Pair**, provide the required information, and generate the key pair.


[Untitled] - Portecle
File
Tools
Examine
Help
Generate Key Pair... Ctrl-G
Import Trusted Certificate... Ctrl-T
Import Key Pair... Ctrl-K
Set Keystore Password... Ctrl-P
Change Keystore Type
Keystore Report Ctrl-R
Options...
Last Modified

Generate a key pair with self-signed certificate in the loaded keystore

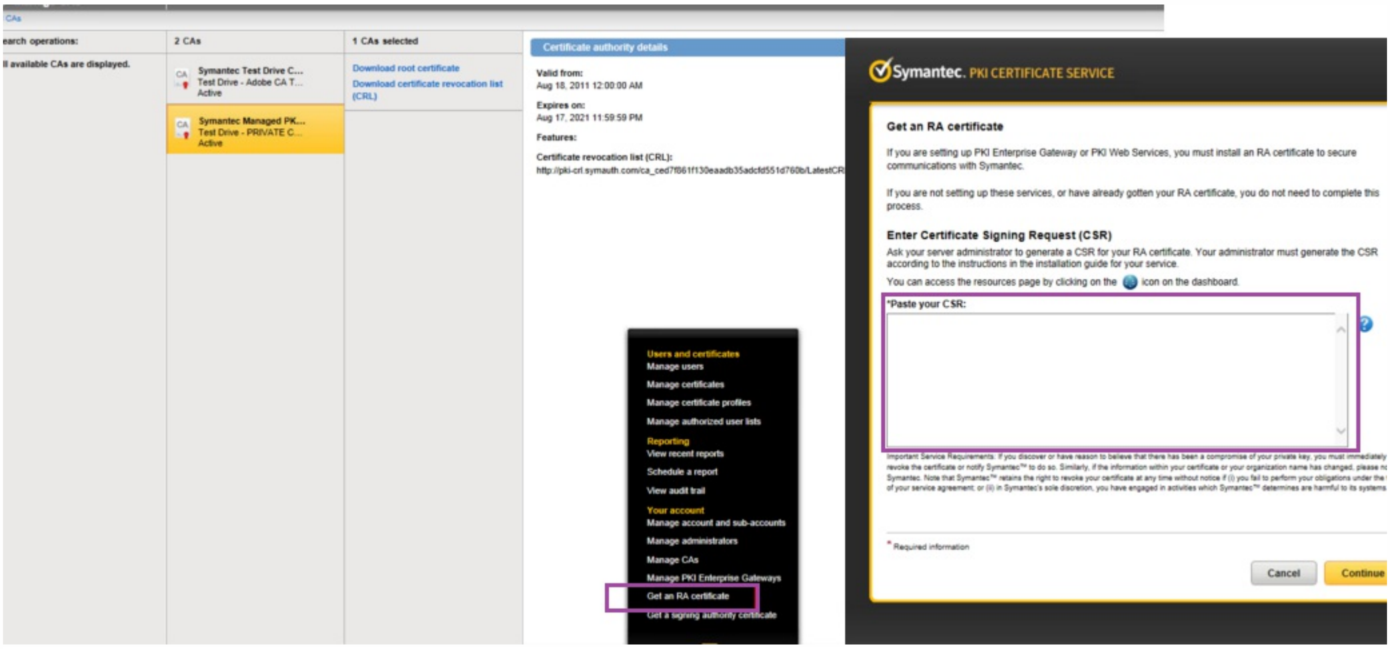
2. Right-click the key pair and then click **Generate Certification Request**.



Generate a certification request for the key pair entry

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**.


CAs
earch operations:
ll available CAs are displayed.
2 CAs
Symantec Test Drive C...
Test Drive - Adobe CA T...
Active
Symantec Managed PK...
Test Drive - PRIVATE C...
Active
1 CAs selected
Download root certificate
Download certificate revocation list (CRL)
Certificate authority details
Users and certificates
Manage users
Manage certificates
Manage certificate profiles
Manage authorized user lists
Reporting
View recent reports
Schedule a report
View audit trail
Your account
Manage account and sub-accounts
Manage administrators
Manage CAs
Manage PKI Enterprise Gateways
Get an RA certificate
Get a signing authority certificate
Symantec. PKI CERTIFICATE SERVICE
Cancel
Continue

Valid from:
Aug 18, 2011 12:00:00 AM

Expires on:
Aug 17, 2021 11:59:59 PM

Features:

Certificate revocation list (CRL):
http://pki-crl.symauth.com/ca_ced7f861f130eaadb35adcfd551d760b/LatestCR

Get an RA certificate

If you are setting up PKI Enterprise Gateway or PKI Web Services, you must install an RA certificate to secure communications with Symantec.

If you are not setting up these services, or have already gotten your RA certificate, you do not need to complete this process.

Enter Certificate Signing Request (CSR)

Ask your server administrator to generate a CSR for your RA certificate. Your administrator must generate the CSR according to the instructions in the installation guide for your service.

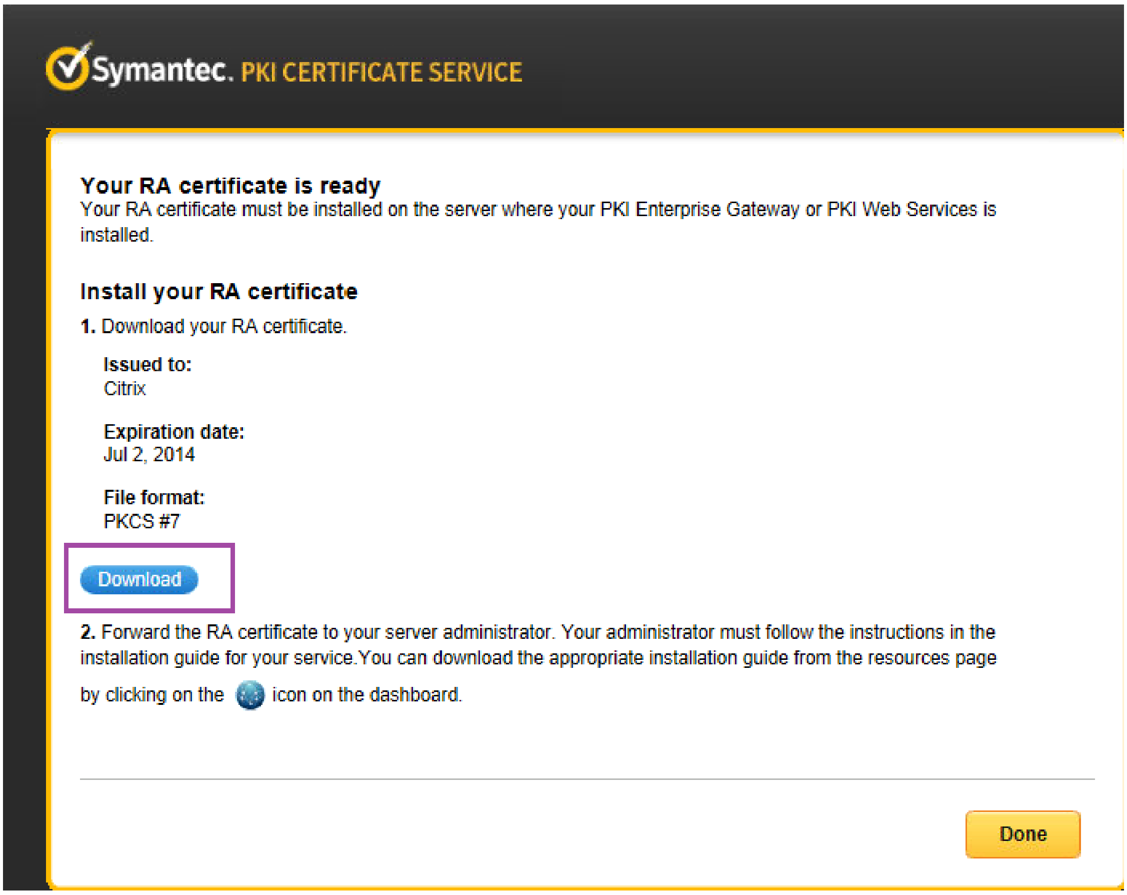
You can access the resources page by clicking on the 🌐 icon on the dashboard.

*Paste your CSR:

Important Service Requirements: If you discover or have reason to believe that there has been a compromise of your private key, you must immediately revoke the certificate or notify Symantec™ to do so. Similarly, if the information within your certificate or your organization name has changed, please no Symantec. Note that Symantec™ retains the right to revoke your certificate at any time without notice if (i) you fail to perform your obligations under the of your service agreement; or (ii) in Symantec's sole discretion, you have engaged in activities which Symantec™ determines are harmful to its systems.

* Required information

5. Click **Download** to download the generated RA certificate.



Your RA certificate is ready

Your RA certificate must be installed on the server where your PKI Enterprise Gateway or PKI Web Services is installed.

Install your RA certificate

1. Download your RA certificate.

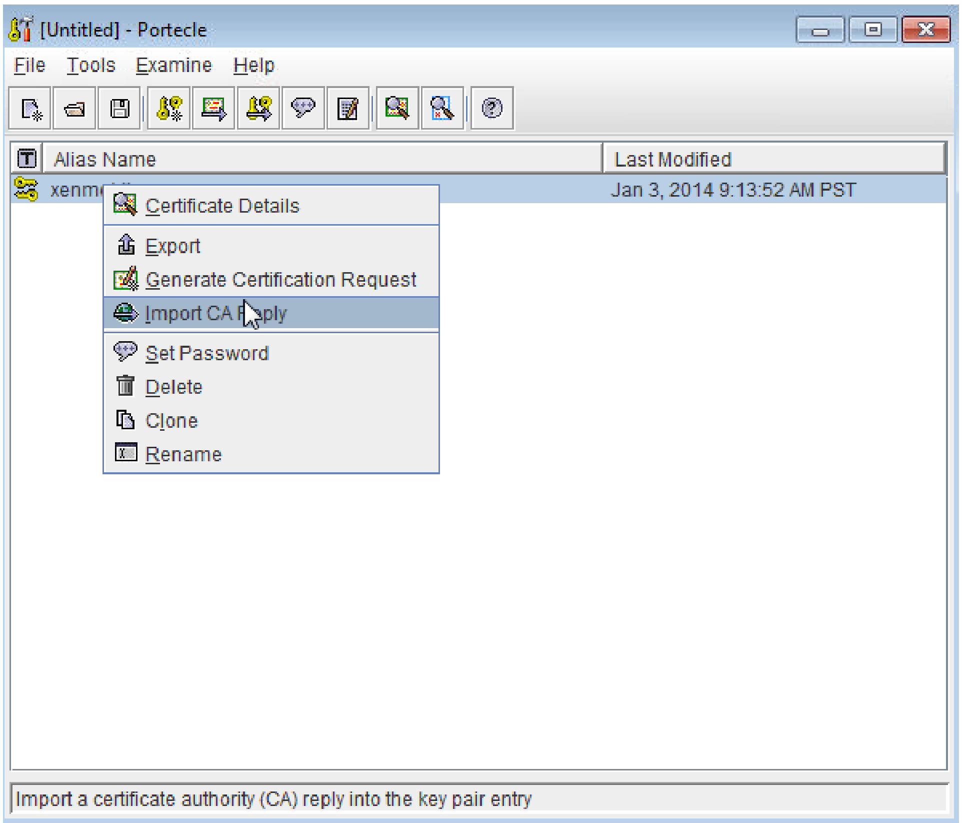
Issued to:
Citrix

Expiration date:
Jul 2, 2014

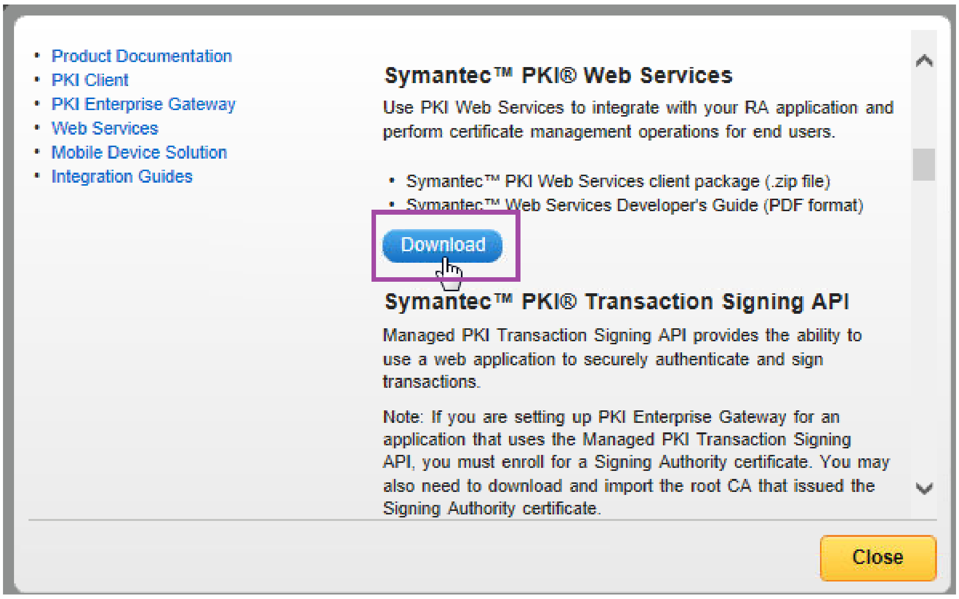
File format:
PKCS #7

2. Forward the RA certificate to your server administrator. Your administrator must follow the instructions in the installation guide for your service.You can download the appropriate installation guide from the resources page by clicking on the 🌐 icon on the dashboard.

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.



Symantec™ PKI® Web Services

Use PKI Web Services to integrate with your RA application and perform certificate management operations for end users.

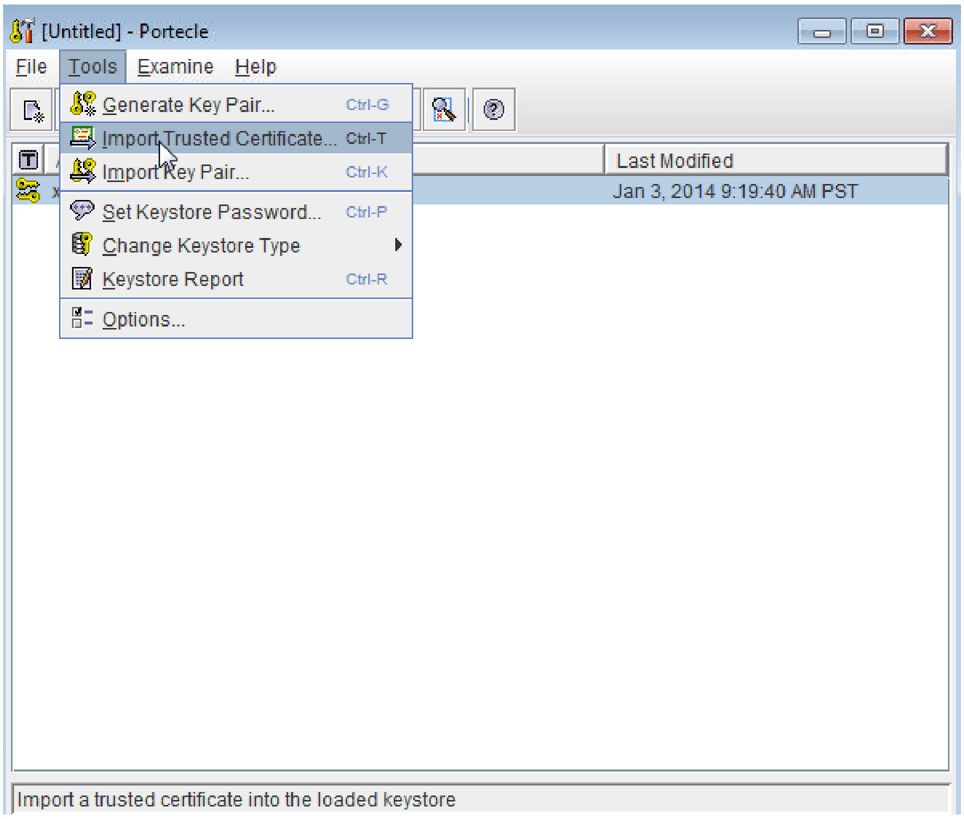
- Symantec™ PKI Web Services client package (.zip file)
- Symantec™ Web Services Developer's Guide (PDF format)

Symantec™ PKI® Transaction Signing API

Managed PKI Transaction Signing API provides the ability to use a web application to securely authenticate and sign transactions.

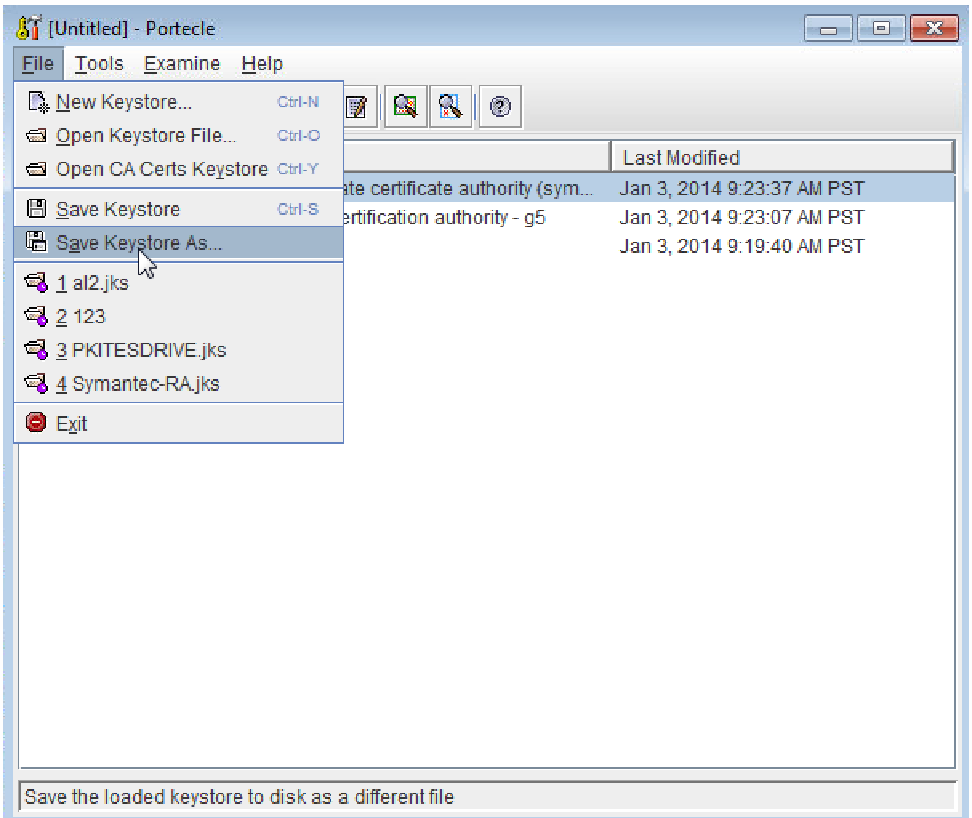
Note: If you are setting up PKI Enterprise Gateway for an application that uses the Managed PKI Transaction Signing API, you must enroll for a Signing Authority certificate. You may also need to download and import the root CA that issued the Signing Authority certificate.

8. In Portecle, import the RA intermediate and root certificates into the keystore: Go to **Tools > Import Trusted Certificates**.


[Untitled] - Portecle
File
Tools
Examine
Help
Generate Key Pair... Ctrl-G
Import Trusted Certificate... Ctrl-T
Import Key Pair... Ctrl-K
Set Keystore Password... Ctrl-P
Change Keystore Type
Keystore Report Ctrl-R
Options...
Last Modified
Jan 3, 2014 9:19:40 AM PST

Import a trusted certificate into the loaded keystore

9. After importing the CAs, save the keystore as RA.jks under the C:\Symantec folder on the Windows server.


[Untitled] - Portecle
File
Tools
Examine
Help
New Keystore... Ctrl-N
Open Keystore File... Ctrl-O
Open CA Certs Keystore Ctrl-Y
Save Keystore Ctrl-S
Save Keystore As...
1 al2.jks
2 123
3 PKITESDRIVE.jks
4 Symantec-RA.jks
Exit
Last Modified
ate certificate authority (sym...
ertification authority - g5
Jan 3, 2014 9:23:37 AM PST
Jan 3, 2014 9:23:07 AM PST
Jan 3, 2014 9:19:40 AM PST

Save the loaded keystore to disk as a different file

Configure Symantec PKI Adapter on Windows Server

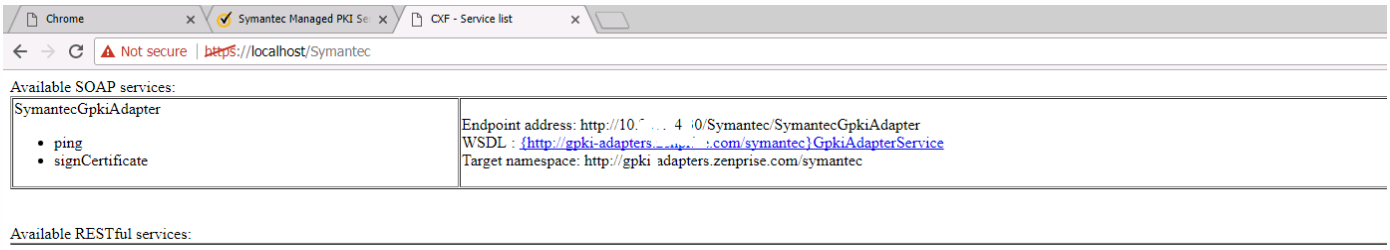
1. Log in to Windows Server as an administrator.
2. Upload the RA.jks file that you generated in the preceding section. Also upload the public certificates (cacerts.jks) for your Symantec MPKI server.
3. From the XenMobile Server 10 download page, expand **Tools**, and download the Symantec PKI Adapter file. The filename is XenMobile_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:

   ```
   Gpki.CaSvc.Url=https://<managed PKI URL>


   # keystore for client-cert auth

   keyStore=C:\\Symantec\\RA.jks


   # truststore for server with self-signed root CA

   trustStore=C:\\Symantec\\cacerts.jks
   ```

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 http://localhost/Symantec.
7. Navigate to the folder <tomcat dir>\webapps\Symantec\WEB-INF\classes and edit the 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 http://localhost/Symantec, and then copy the endpoint address. In the next section, you paste that address when configuring the PKI adapter.



Available SOAP services:

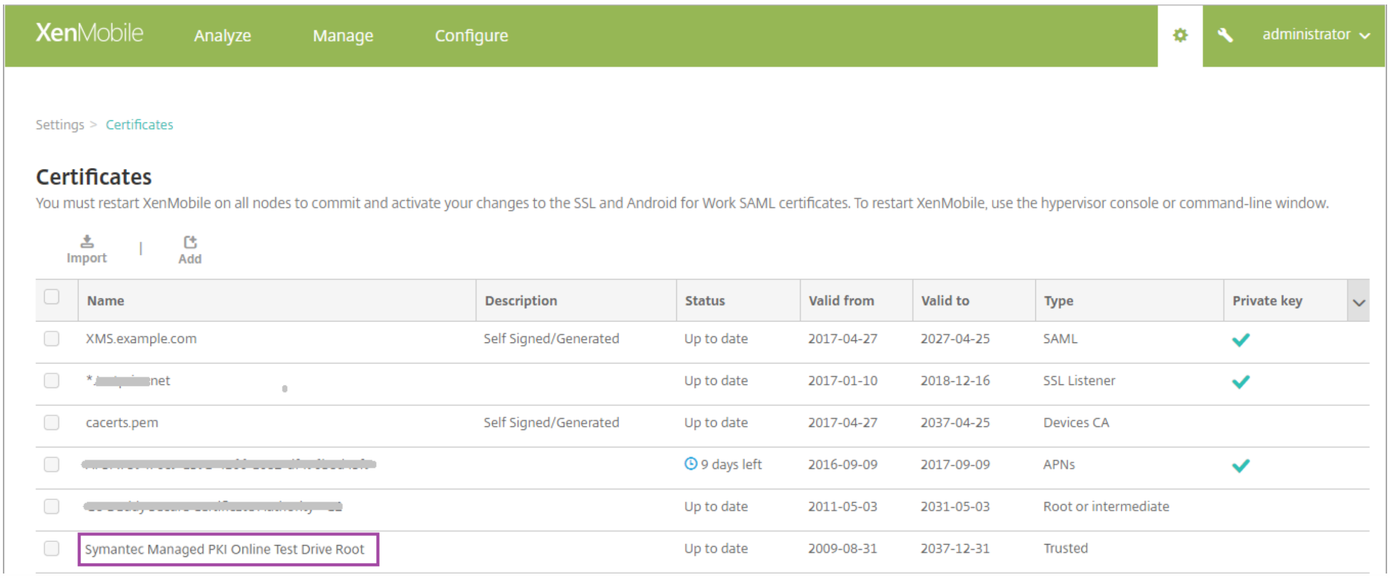
SymantecGpkiAdapter • ping • signCertificate	Endpoint address: http://10.[illegible] 4 [illegible]0/Symantec/SymantecGpkiAdapter WSDL : {http://gpki-adapters.[illegible].com/symantec}GpkiAdapterService Target namespace: http://gpki adapters.zenprise.com/symantec

Available RESTful services:

Complete the Windows Server setup before performing the following XenMobile Server 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 XenMobile Server console, go to **Settings > Certificates** and click **Import**.



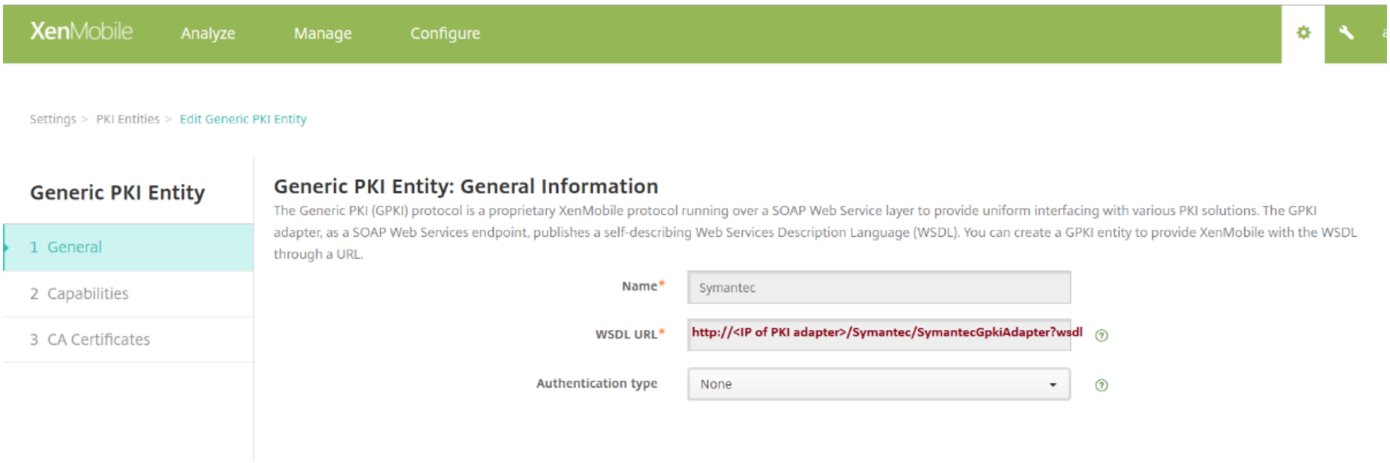
Settings > Certificates

Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

□	Name	Description	Status	Valid from	Valid to	Type	Private key
□	XMS.example.com	Self Signed/Generated	Up to date	2017-04-27	2027-04-25	SAML	✓
□	*.[redacted]net		Up to date	2017-01-10	2018-12-16	SSL Listener	✓
□	cacerts.pem	Self Signed/Generated	Up to date	2017-04-27	2037-04-25	Devices CA	
□	[redacted]		9 days left	2016-09-09	2017-09-09	APNs	✓
□	[redacted]		Up to date	2011-05-03	2031-05-03	Root or intermediate	
□	Symantec Managed PKI Online Test Drive Root		Up to date	2009-08-31	2037-12-31	Trusted	

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 below.



Settings > PKI Entities > Edit Generic PKI Entity

Generic PKI Entity

1 General
2 Capabilities
3 CA Certificates

Generic PKI Entity: General Information

The Generic PKI (GPKI) protocol is a proprietary XenMobile protocol running over a SOAP Web Service layer to provide uniform interfacing with various PKI solutions. The GPKI adapter, as a SOAP Web Services endpoint, publishes a self-describing Web Services Description Language (WSDL). You can create a GPKI entity to provide XenMobile with the WSDL through a URL.

Name*: Symantec

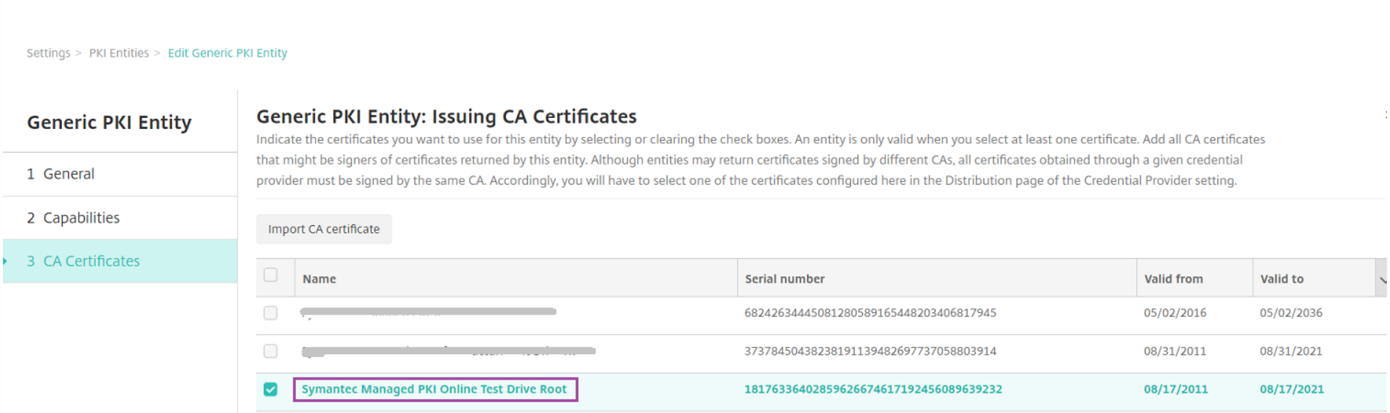
WSDL URL*: http://<IP of PKI adapter>/Symantec/SymantecGpkiAdapter?wsdl

Authentication type: None

3. Click **Next**. XenMobile populates the parameter names from the WSDL.

Settings > PKI Entities > Edit Generic PKI Entity

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



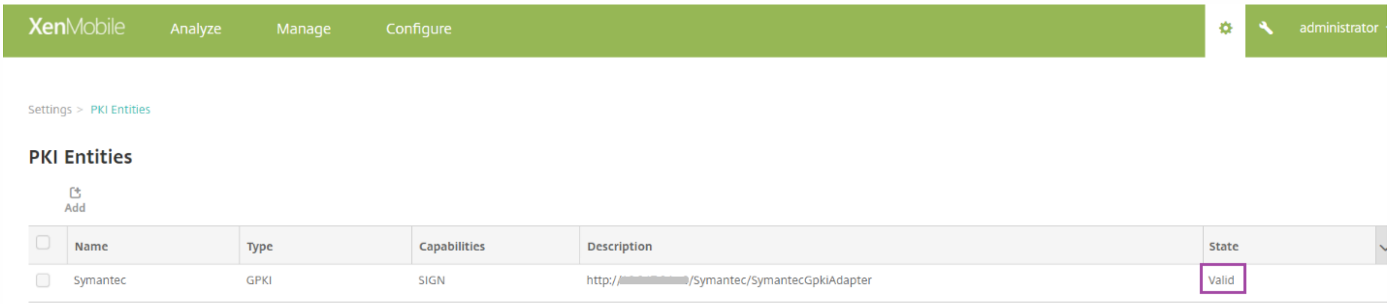
Settings > PKI Entities > Edit Generic PKI Entity

Generic PKI Entity: Issuing CA Certificates

Indicate the certificates you want to use for this entity by selecting or clearing the check boxes. An entity is only valid when you select at least one certificate. Add all CA certificates that might be signers of certificates returned by this entity. Although entities may return certificates signed by different CAs, all certificates obtained through a given credential provider must be signed by the same CA. Accordingly, you will have to select one of the certificates configured here in the Distribution page of the Credential Provider setting.

☐	Name	Serial number	Valid from	Valid to
☐	[redacted]	68242634445081280589165448203406817945	05/02/2016	05/02/2036
☐	[redacted]	37378450438238191139482697737058803914	08/31/2011	08/31/2021
☑	Symantec Managed PKI Online Test Drive Root	18176336402859626674617192456089639232	08/17/2011	08/17/2021

5. On the **Settings > PKI Entities** page, verify that the **State** of the PKI Entity you added is **Valid**.



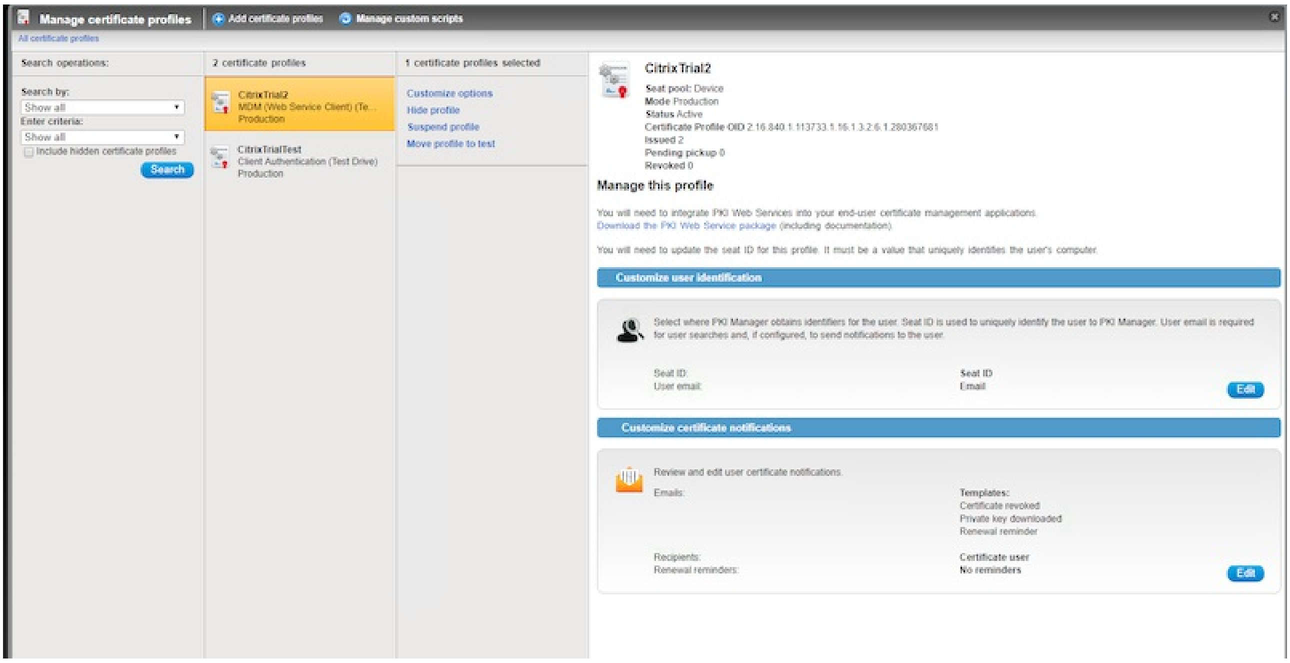
Settings > PKI Entities

PKI Entities

☐	Name	Type	Capabilities	Description	State
☐	Symantec	GPKI	SIGN	http://[redacted]/Symantec/SymantecGpkiAdapter	Valid

To create the credential provider for Symantec Managed PKI

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



CitrixTrial2
MDM (Web Service Client) (Te...
Production

CitrixTrialTest
Client Authentication (Test Drive)
Production

Citrix Trial2
Seat pool: Device
Mode Production
Status Active
Certificate Profile OID 2.16.840.1.113733.1.16.1.3.2.6.1.280367681
Issued 2
Pending pickup 0
Revoked 0

Manage this profile

You will need to integrate PKI Web Services into your end-user certificate management applications.
Download the PKI Web Service package (including documentation).

You will need to update the seat ID for this profile. It must be a value that uniquely identifies the user's computer.

Select where PKI Manager obtains identifiers for the user. Seat ID is used to uniquely identify the user to PKI Manager. User email is required for user searches and, if configured, to send notifications to the user.

Seat ID: Seat ID
User email: Email

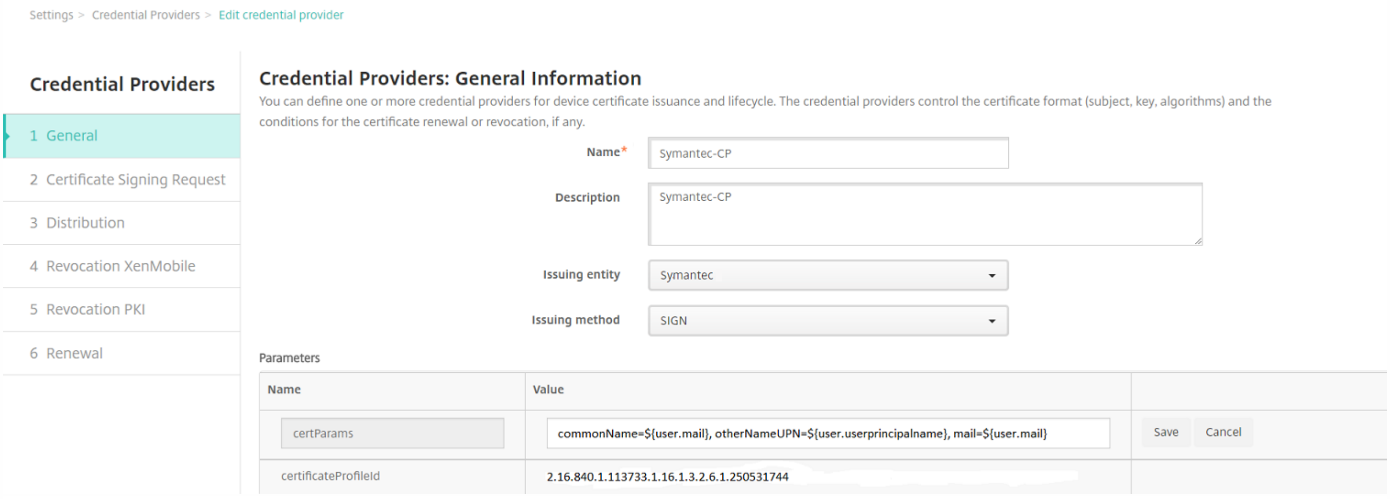
Review and edit user certificate notifications.

Emails: Templates:
Certificate revoked
Private key downloaded
Renewal reminder

Recipients: Certificate user
Renewal reminders: No reminders

2. In the XenMobile Server 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 XenMobile 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.



Credential Providers: General Information

You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.

Name*: Symantec-CP

Description: Symantec-CP

Issuing entity: Symantec

Issuing method: SIGN

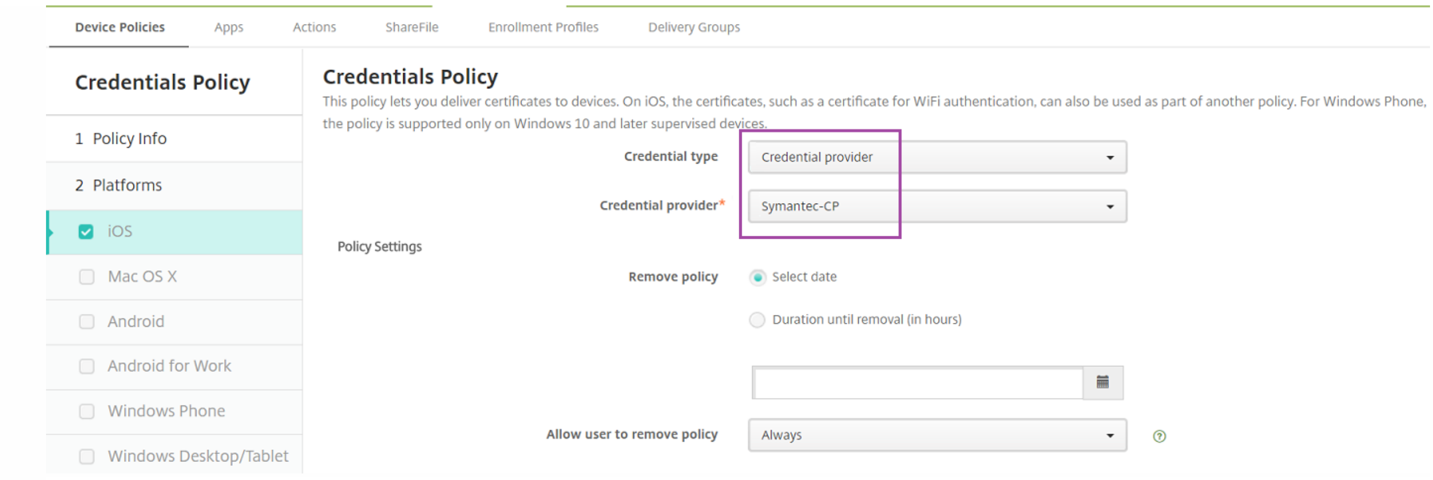
Parameters

Name	Value	
certParams	commonName=${user.mail}, otherNameUPN=${user.userprincipalname}, mail=${user.mail}	Save Cancel
certificateProfileId	2.16.840.1.113733.1.16.1.3.2.6.1.250531744	

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.



Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Credential type: Credential provider

Credential provider*: Symantec-CP

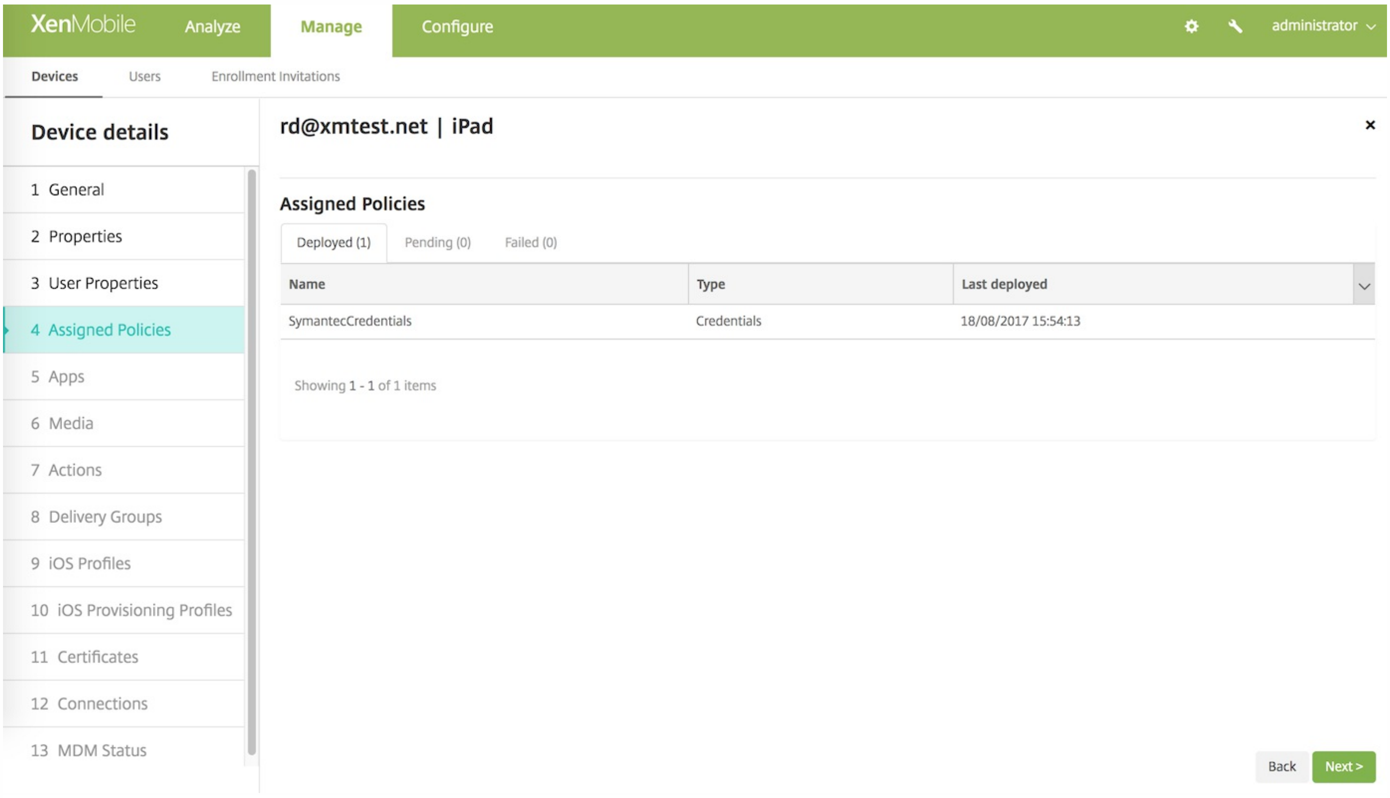
Policy Settings

Remove policy: ● Select date ○ Duration until removal (in hours)

Allow user to remove policy: Always

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.



rd@xmtest.net | iPad

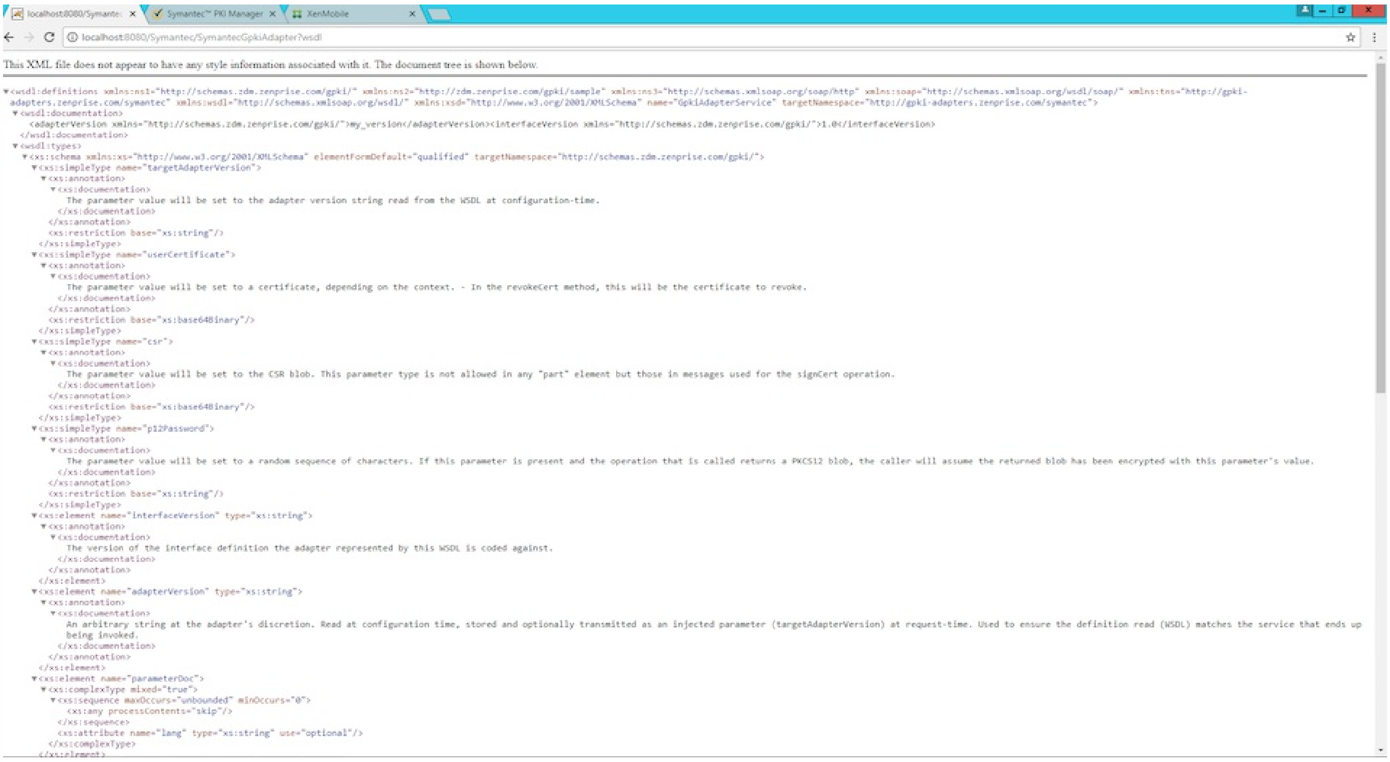
Assigned Policies

Deployed (1) Pending (0) Failed (0)

Name	Type	Last deployed
SymantecCredentials	Credentials	18/08/2017 15:54:13

Showing 1 - 1 of 1 items

If the policy didn't deploy, log in to the Windows Server and check if the WSDL is loading properly.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<wsdl:definitions xmlns:ns1="http://schemas.zdm.zenprise.com/gpki/" xmlns:ns2="http://zdm.zenprise.com/gpki/sample" xmlns:ns3="http://schemas.xmlsoap.org/soap/http" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:tns="http://gpki-
 adapters.zenprise.com/symantec" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" name="GpkiAdapterService" targetNamespace="http://gpki-adapters.zenprise.com/symantec">
  ▼<wsdl:documentation>
     <adapterVersion xmlns="http://schemas.zdm.zenprise.com/gpki/">my_version</adapterVersion><interfaceVersion xmlns="http://schemas.zdm.zenprise.com/gpki/">1.0</interfaceVersion>
   </wsdl:documentation>
  ▼<wsdl:types>
    ▼<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" targetNamespace="http://schemas.zdm.zenprise.com/gpki/">
      ▼<xs:simpleType name="targetAdapterVersion">
        ▼<xs:annotation>
          ▼<xs:documentation>
             The parameter value will be set to the adapter version string read from the WSDL at configuration-time.
           </xs:documentation>
         </xs:annotation>
         <xs:restriction base="xs:string"/>
       </xs:simpleType>
      ▼<xs:simpleType name="userCertificate">
        ▼<xs:annotation>
          ▼<xs:documentation>
             The parameter value will be set to a certificate, depending on the context. - In the revokeCert method, this will be the certificate to revoke.
           </xs:documentation>
         </xs:annotation>
         <xs:restriction base="xs:base64Binary"/>
       </xs:simpleType>
      ▼<xs:simpleType name="csr">
        ▼<xs:annotation>
          ▼<xs:documentation>
             The parameter value will be set to the CSR blob. This parameter type is not allowed in any "part" element but those in messages used for the signCert operation.
           </xs:documentation>
         </xs:annotation>
         <xs:restriction base="xs:base64Binary"/>
       </xs:simpleType>
      ▼<xs:simpleType name="p12Password">
        ▼<xs:annotation>
          ▼<xs:documentation>
             The parameter value will be set to a random sequence of characters. If this parameter is present and the operation that is called returns a PKCS12 blob, the caller will assume the returned blob has been encrypted with this parameter's value.
           </xs:documentation>
         </xs:annotation>
         <xs:restriction base="xs:string"/>
       </xs:simpleType>
      ▼<xs:element name="interfaceVersion" type="xs:string">
        ▼<xs:annotation>
          ▼<xs:documentation>
             The version of the interface definition the adapter represented by this WSDL is coded against.
           </xs:documentation>
         </xs:annotation>
       </xs:element>
      ▼<xs:element name="adapterVersion" type="xs:string">
        ▼<xs:annotation>
          ▼<xs:documentation>
             An arbitrary string at the adapter's discretion. Read at configuration time, stored and optionally transmitted as an injected parameter (targetAdapterVersion) at request-time. Used to ensure the definition read (WSDL) matches the service that ends up
             being invoked.
           </xs:documentation>
         </xs:annotation>
       </xs:element>
      ▼<xs:element name="parameterDoc">
        ▼<xs:complexType mixed="true">
          ▼<xs:sequence maxOccurs="unbounded" minOccurs="0">
             <xs:any processContents="skip"/>
           </xs:sequence>
           <xs:attribute name="lang" type="xs:string" use="optional"/>
         </xs:complexType>
       </xs:element>
```

For more troubleshooting information, check the Tomcat logs in <tomcat dir>\logs\catalina.<current date>.

Microsoft Certificate Services

XenMobile interfaces with Microsoft Certificate Services through its web enrollment interface. XenMobile only supports the issuing of new certificates through that interface (the equivalent of the GPKI sign capability). If the Microsoft CA generates a NetScaler Gateway user certificate, NetScaler Gateway supports renewal and revocation for those certificates.

To create a Microsoft CA PKI entity in XenMobile, you must specify the base URL of the Certificate Services web interface. If you choose, use SSL client authentication to secure the connection between XenMobile and the Certificate Services web interface.

1. In the XenMobile 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://192.0.2.13/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.

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, refer to the Microsoft documentation for your Microsoft Server version. XenMobile 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 that XenMobile should inject in 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 XenMobile of the signers of the certificates that the system obtains through this entity. When your CA certificate is renewed, update it in XenMobile and then the change is applied to the entity transparently.

10. On the **Microsoft Certificate Services Entity: CA Certificates** page, select the certificates you want to use for this entity.

11. Click **Save**.

The entity appears on the PKI Entities table.

NetScaler Certificate Revocation List (CRL)

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

When you configure client certificate-based authentication, consider whether to configure the NetScaler 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. XenMobile 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 XenMobile with a CA certificate and the associated private key. XenMobile 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 XenMobile 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: id-kp-OCSPSigning extendedKeyUsage.

The XenMobile 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).

1. In the XenMobile console, click the gear icon in the upper-right corner of the console and then click **More** > **PKI Entities**.

2. On the **PKI Entities** page, click **Add**.

A menu of PKI entity types appears.

3. Click **Discretionary CA**.

The **Discretionary CA: General Information** page appears.

4. On the **Discretionary CA: General Information** page, do the following:

- **Name**: Type a descriptive name for the discretionary CA.
- **CA certificate to sign certificate requests**: Click a certificate for the discretionary CA to use to sign certificate requests. This list of certificates is generated from the CA certificates with private keys you uploaded at XenMobile at

Configure > **Settings** > **Certificates**.

5. Click **Next**.

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

6. On the **Discretionary CA: Parameters** page, do the following:

- **Serial number generator**: The discretionary CA generates serial numbers for the certificates it issues. From this list, click **Sequential** or **Non-sequential** to determine how the numbers are generated.
- **Next serial number**: Type a value to determine the next number issued.
- **Certificate valid for**: Type the number of days the certificate is valid.
- **Key usage**: Identify the purpose of the certificates issued by the discretionary CA by setting the appropriate keys to **On**. Once set, the CA is limited 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 and an RA signing certificate with the KeyUsage digitalSignature. 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 OSCP signing CA certificate. This list of certificates is generated from the CA certificates you uploaded to XenMobile.

10. Click **Save**.

The discretionary CA appears on the PKI Entities table.

Credential providers

Sep 06, 2017

Credential providers are the actual certificate configurations you use in the various parts of the XenMobile system. They define the sources, parameters, and life cycles of your certificates, 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, XenMobile does not issue certificates before enrollment, although XenMobile 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, then 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.

With this in mind, the credential provider configuration in XenMobile does the following:

- Determines the source of certificates.
- Determines the method in which certificates are obtained: Signing a new certificate or fetching (recovering) an existing certificate and key pair.
- Determines the parameters for issuance or recovery. For example, Certificate Signing Request (CSR) parameters, such as key size, key algorithm, distinguished name, certificate extensions, and so on.
- Determines the manner in which certificates are delivered to the device.
- Determines revocation conditions. Although all certificates are revoked in XenMobile when the management relationship is severed, the configuration may specify an earlier revocation; for instance, when the associated device configuration is deleted. In addition, under some conditions, the revocation of the associated certificate in XenMobile may be sent to the back-end public key infrastructure (PKI); that is, its revocation in XenMobile may cause its revocation on the PKI.
- Determines renewal settings. Certificates obtained through a given credential provider may be automatically renewed when they near expiration, or, separately from that situation, notifications may be issued when that expiration approaches.

To what extent various configuration options are available mainly depends on the type of PKI Entity and issuance method that you select for a credential provider.

You can obtain a certificate, which is referred to 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. XenMobile 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 XenMobile, is a recovery of an existing key pair. XenMobile supports the fetch method only for Generic PKI.

A credential provider uses either 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.

Two modes of certificate delivery are available in XenMobile: 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, XenMobile acts like a delegate (a registrar) to the actual certificate authority. XenMobile 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 XenMobile.

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 must upload the certificates to XenMobile 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 mandates 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 XenMobile:

Context	SCEP supported	SCEP required
iOS Profile Service	Yes	Yes
iOS mobile device management enrollment	Yes	No
iOS configuration profiles	Yes	No
SHTP enrollment	No	No
SHTP configuration	No	No
Windows Phone and Tablet enrollment	No	No

Context	SCEP supported	SCEP required
Windows Phone and Tablet configuration	No except for the Wifi device policy, which is supported for Windows Phone 8.1 and the latest Windows 10 release	No

There are three types of revocation.

- **Internal revocation**. Internal revocation affects the certificate status as maintained by XenMobile. This status is taken into account when XenMobile evaluates a certificate presented to it, or when XenMobile has to provide OCSP status information for some certificate. The credential provider configuration determines how this status is affected under various conditions. For instance, the credential provider may specify that certificates obtained through the certificate provider should be flagged as revoked when the certificates have been deleted from the device.
- **Externally propagated revocation**. Also known as Revocation XenMobile, this type of revocation applies to certificates obtained from an external PKI. The certificate is revoked on the PKI when the certificate is internally revoked by XenMobile, 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 XenMobile evaluates a given certificate status, XenMobile queries the PKI as to that status. If the certificate is revoked, XenMobile internally revokes the certificate. This mechanism uses the OCSP protocol.

These three types are not exclusive, but rather apply together: The internal revocation is caused either by an external revocation or by independent findings, and in turn the internal revocation potentially effects an external revocation.

A certificate renewal is the combination of a revocation of the existing certificate and an issuance of another certificate.

Note that XenMobile first attempts to obtain the new certificate before revoking the previous certificate, in order to avoid discontinuation of service if the issuance fails. If distributed (SCEP-supported) delivery is used, 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 and independently of the success or failure of its 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 it is, a renewal is attempted.

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 XenMobile, is an internal entity. The issuing method for a discretionary entity is always sign, meaning that with each issuing operation, XenMobile 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 Symantec Managed PKI, including creating the credential provider, see "Symantec

Managed PKI" in PKI entities.

1. In the XenMobile web console, click the gear icon in the upper-right corner of the console and then click **More** > **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 refer to the configuration in other parts of the XenMobile console.
- **Description**: Describe the credential provider. Although this is an optional field, a description can be useful in the future to help you remember 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.

4. Click **Next**.

Note: These templates become available when Microsoft Certificate Services Entities are added at **Settings** > **PKI Entities**.

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 is a required field.
  Note: The permissible values depend on the key type; for instance, the maximum size for DSA keys is 1024 bits. To avoid false negatives, which will depend on the underlying hardware and software, XenMobile does not enforce key sizes. You should always test credential provider configurations in a test environment before activating them in production.

- **Signature algorithm**: Click a value for the new certificate. Values are dependent on the key algorithm.
- **Subject name**: Required. Type the Distinguished Name (DN) of the new certificate subject. For example:
  CN=${user.username}, OU=${user.department}, O=${user.companyname},C=${user.c}\endquotation

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

  Key algorithm: RSA
  Key size: 2048
  Signature algorithm: SHA1withRSA
  Subject name: cn=$user.username

6. To add a new 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

Note: As with Subject name, you can use XenMobile macros in the value field.

7. Click **Next**.

The **Credential Providers: Distribution** page appears.

8. 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 be the CA certificate configured on the entity itself; it will be 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 XenMobile and is required when using NetScaler Gateway authentication. The private keys are generated and stored on the server and distributed to user devices.
  - **Prefer distributed: Device-side key generation**. The private keys are generated and stored on the user devices. This distributed mode uses SCEP and requires an RA encryption certificate with the keyUsage keyEncryption and an RA signing certificate with the KeyUsage digitalSignature. The same certificate can be used for both encryption and signing.
  - **Only distributed: Device-side key generation**. This option works the same as Prefer distributed: Device-side key generation, except that since it is "Only," rather than "Prefer," no option is available if device-side key generation fails or is unavailable.

If you selected **Prefer distributed: Device-side key generation** or **Only distributed: Device-side key generation**, click the RA signing certificate and RA encryption certificate. The same certificate can be used for both. New fields appear for these certificates.

9. Click **Next**.

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

12. On the **Credential Providers: Revocation XenMobile** page, do the following:

- In **Revoke issued certificates**, select one of the options indicating when certificates should be revoked.
- If you would like XenMobile to send a notification when the certificate is revoked, set the value of **Send notification** to **On** and choose a notification template.

- If you would like to revoke the certificate on PKI when the certificate has been revoked from XenMobile, set **Revoke certificate on PKI** to **On** and, in the **Entity list**, click a template. The Entity list shows all the available GPKI entities with revocation capabilities. When the certificate is revoked from XenMobile, a revocation call is sent to the PKI selected from the Entity list.

13. 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.

14. 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**. Additional fields related to revocation PKI appear.
- In the **OCSP responder CA certificate** list, click the distinguished name (DN) of the certificate's subject. **Note**: You can use XenMobile macros for the DN field values. For example: CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation
- In the **When certificate is revoked** list, click one of the following actions to take on the PKI entity when the certificate is revoked:

  Do nothing.

  Renew the certificate.

  Revoke and wipe the device.

- If you would like XenMobile 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.

15. Click **Next**.

The **Credential Providers: Renewal** page appears. On this page, you can configure XenMobile to do the following:

- Renew the certificate, optionally sending a notification when this is done (notification on renewal), and optionally excluding already expired certificates from the operation.
- Issue a notification for certificates that near expiration (notification before renewal).

16. 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**.

Additional fields appear.

- In the **Renew when the certificate comes within** field, type how many days prior to expiration the renewal should be made.
- Optionally, select **Do not renew certificates that have already expired**. **Note**: In this case, "already expired" means that the certificate's NotAfter date is in the past, not that it has been revoked. XenMobile will not renew certificates once they have been internally revoked.

17. If you want XenMobile to send a notification when the certificate has been renewed, set **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.

18. If you want XenMobile to send a notification when the certification nears expiration, set **Notify when certificate nears expiration** 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.

19. In the **Notify when the certificate comes within** field, type how many days prior to the certificate's expiration the notification should be sent.

20. Click **Save**.

The credential provider is added to the Credential Provider table.

APNs certificates

Dec 14, 2017

In order to enroll and manage iOS devices with XenMobile, you need to set up and create an Apple Push Notification service (APNs) certificate from Apple. This section outlines the following basic steps for requesting the APNs certificate:

- Use a Windows Server 2012 R2 or Windows 2008 R2 Server and Microsoft Internet Information Server (IIS) or a Mac computer to generate a Certificate Signing Request (CSR).
- Have Citrix sign the CSR.
- Request an APNs certificate from Apple.
- Import the certificate to XenMobile.

Note:

- The APNs certificate from Apple enables mobile device management via the Apple Push Network. If you accidentally or intentionally revoke the certificate, you will lose the ability to manage your devices.
- If you used the iOS Developer Enterprise Program to create a mobile device manager push certificate, you may need to take action due to the migration of existing certificates to the Apple Push Certificates Portal.

The topics that outline the step-by-step procedures are listed in order in this section as follows:

Step 1: For Windows, generate a CSR with a Windows Server 2012 R2 or Windows 2008 R2 Server and Microsoft IIS. For Mac, generate a CSR on a Mac computer. Citrix recommends this method.

- To create a CSR by using Microsoft IIS
- To create a CSR on a Mac computer

Step 2: Submit the CSR to Citrix at the XenMobile APNs CSR Signing website (MyCitrix ID required). Citrix signs the CSR with its mobile device management signing certificate and returns the signed file in a .plist format. For more information, see To sign the CSR

Step 3: Submit the signed CSR to Apple at Apple Push Certificate Portal (Apple ID required) and then download the APNs certificate from Apple. For more information, see Submit Signed CSR to Apple.

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

- To create a .pfx APNs certificate by using Microsoft IIS
- To create a .pfx APNs certificate on a Mac computer
- Create a .pfx APNs certificate by using OpenSSL

Step 5: Import an APNs certificate into XenMobile.

Mobile device management (MDM) push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificates Portal. This migration affects the creation of new MDM push certificates and the renewal, revocation, and downloading of existing MDM push certificates. The migration does not affect other (non-MDM) APNs certificates.

If your MDM push certificate was created in the iOS Developer Enterprise Program, the following situations apply:

- The certificate has been migrated for you automatically.
- You can renew the certificate in the Apple Push Certificates Portal without affecting your users.
- You need to use the iOS Developer Enterprise Program to revoke or download a preexisting certificate.

If none of your MDM push certificates is near expiration, you don't need to do anything. If you do have an MDM push certificate that is approaching expiration, contact your MDM solution provider. Then, have your iOS Developer Program Agent log on to the Apple Push Certificates Portal with their Apple ID.

All new MDM push certificates must be created in the Apple Push Certificates Portal. The iOS Developer Enterprise Program will no longer allow the creation of an App ID with a Bundle Identifier (APNs topic) that contains com.apple.mgmt.

Note: You must keep track of the Apple ID used to create the certificate. In addition, the Apple ID should be a corporate ID and not a personal ID.

The first step for generating an APNs certificate request for iOS devices is to create a Certificate Signing Request (CSR). On a Windows 2012 R2 or Windows 2008 R2 Server, you can 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**.

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.
4. On the **Keychain Access** menu, click **Certificate Assistant** > **Request a Certificate From a Certificate Authority**.
5. The Certificate Assistant prompts you to enter the following information:
   1. **Email Address**. Email address of the individual or role account who is responsible for managing the certificate.
   2. **Common Name**. Common name of the individual or a role account who is responsible for managing the certificate.
   3. **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 by selecting 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.

If you cannot use a Windows 2012 R2 or Windows 2008 R2 Server and Microsoft Internet Information Server (IIS) or a Mac computer to generate a Certificate Signing Request (CSR) to submit to Apple for the Apple Push Notification service (APNs) certificate, you can use OpenSSL.

Note: In order to use OpenSSL to create a CSR, you need to 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.
   ```
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [AU]:US
   State or Province Name (full name) [Some-State]:CA
   Locality Name (eg, city) []:RWC
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer
   Organizational Unit Name (eg, section) []:Marketing
   Common Name (eg, YOUR name) []:John Doe
   Email Address []:john.doe@customer.com
   ```

3. At the next message, enter a password for the CSR private key.
   ```
   Please enter the following 'extra' attributes
   to be sent with your certificate request
   A challenge password []:
   An optional company name []:
   ```

4. Send the resulting CSR to Citrix.

Citrix prepares the signed CSR and returns the file to you through email.

Before you can submit the certificate to Apple, it needs to be signed by Citrix so it can be used with XenMobile.

1. In your browser, go to the XenMobile APNs CSR Signing website.
2. Click **Upload the CSR**.
3. Browse to and select the certificate.
   Note: The certificate must be in .pem/txt format.

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

After receiving your signed Certificate Signing Request (CSR) from Citrix, you need to 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 (http://developer.apple.com/devcenter/ios/index.action) before going to the identity.apple.com link in

Step 1.

1. In a browser, go to https://identity.apple.com/pushcert.
2. Click **Create a Certificate**.
3. If this is the first time you are creating 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 should appear stating that the upload is successful.
5. Click **Download** to retrieve the .pem certificate.
   Note: If you are using Internet Explorer and the file extension is missing, click **Cancel** two times and then download from the next window.

To use the APNs certificate from Apple with XenMobile, you need to complete the certificate request in Microsoft IIS, export the certificate as a PCKS #12 (.pfx) file and then import the APNs certificate into XenMobile.

Important: You need to 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**.
   Note: You will need the password for the certificate during the installation of XenMobile.
7. Copy the .pfx certificate to the server on which XenMobile will be installed.
8. Sign on to the XenMobile console as an administrator.
9. In the XenMobile 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**.

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 will appear 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 XenMobile 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 will prompt 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 XenMobile server.
   Note: If you don't plan to keep and preserve the computer and user account that you originally used to generate the CSR and complete the certificate 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 will be voided and you will have to repeat the entire CSR and APNs process.

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.

```
openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12
```

2. Enter a password for the .pfx certificate file. Remember this password because you need to use the password again when you upload the certificate to XenMobile.
3. Note the location for the .pfx certificate file and then copy the file to the XenMobile server, so you can use the XenMobile console to upload the file.

After you have requested and received a new APNs certificate, you import the APNs certificate into XenMobile to either add the certificate for the first time or to replace an existing certificate.

1. In the XenMobile 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 .p12 file on your computer.
7. Enter a password and then click **Import**.

For more information about certificates in XenMobile, see the Certificates section.

To renew an APNs certificate, you need to perform the same steps you would if you were creating a new certificate. Then, you visit the Apple Push Certificates Portal and upload the new certificate. After logging on, you see your existing certificate or you may see a certificate that was imported from your previous Apple Developers account. 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 in order to access the site. When you are renewing your certificate, ensure that you use the same organisation name and Apple ID.

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

1. Generate a CSR using Microsoft Internet Information Services (IIS).
2. At the XenMobile APNs CSR Signing website, upload the new CSR and then click **Sign**.
3. Submit the signed CSR to Apple at Apple Push Certificate Portal.
4. Click **Renew**.
5. Generate a PCKS #12 (.pfx) APNs certificate using Microsoft IIS.
6. Update the new APNs certiificate in the XenMobile console. Click the gear icon in the upper-right corner of the console. The **Settings** page appears.
7. Click **Certificates**. The **Certificates** page appears.
8. Click **Import**. The **Import** dialog box appears.
9. From the **Import** menu, choose **Keystore**.
10. From **Use as**, choose **APNs**.
11. Browse to the .p12 file on your computer.
12. Enter a password and then click **Import**.

SAML for single sign-on with ShareFile

Jan 03, 2018

You can configure XenMobile and ShareFile to use Security Assertion Markup Language (SAML) to provide single sign-on (SSO) access to ShareFile mobile apps. This functionality includes ShareFile apps that are wrapped with the MDX Toolkit and non-wrapped ShareFile clients, such as the web site, Outlook plugin, or sync clients.

- **For wrapped ShareFile apps**. Users who log on to ShareFile through the ShareFile mobile app are redirected to Secure Hub for user authentication and to acquire a SAML token. After successful authentication, the ShareFile mobile app sends the SAML token to ShareFile. After the initial logon, users can access the ShareFile mobile app through SSO. They can also attach documents from ShareFile to Secure Mail mails without logging on each time.
- **For non-wrapped ShareFile clients**. Users who log on to ShareFile using a web browser or other ShareFile client are redirected to XenMobile for user authentication and to acquire a SAML token. After successful authentication, the SAML token is sent to ShareFile. After the initial log on, users can access ShareFile clients through SSO without logging on each time.

To use XenMobile as a SAML identity provider (IdP) to ShareFile, you must configure XenMobile to use ShareFile Enterprise, as described in this article. Alternatively, you can configure XenMobile to work only with StorageZone Connectors. For more information, see ShareFile use with XenMobile.

For a detailed reference architecture diagram, see the XenMobile Deployment Handbook article, Reference Architecture for On-Premises Deployments.

You must complete the following prerequisites before you can configure SSO with XenMobile and ShareFile apps:

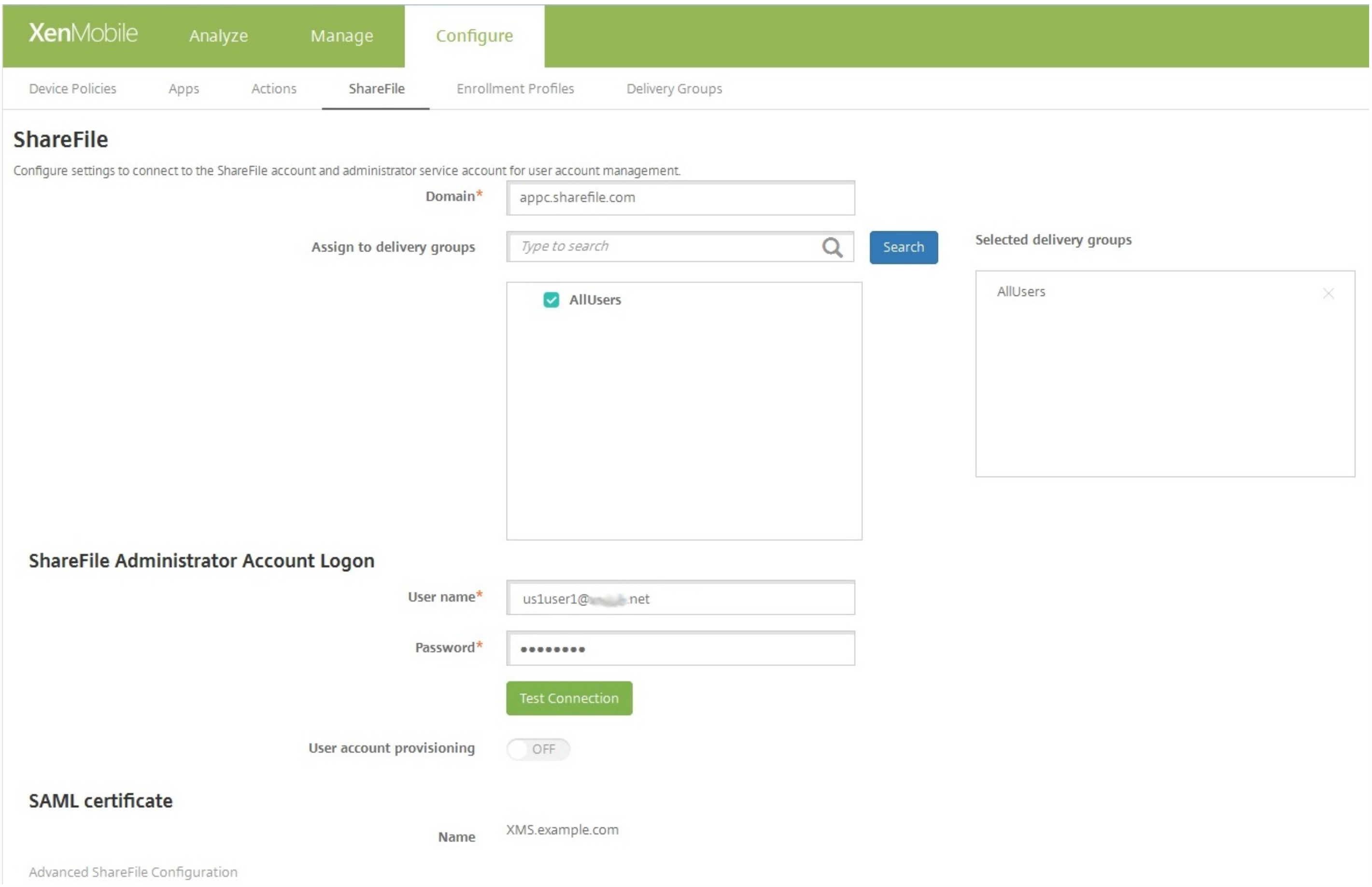
- The MDX Service or a compatible version of the MDX Toolkit (for ShareFile mobile apps).

  For more information, see XenMobile compatibility.

- A compatible version of ShareFile mobile apps and Secure Hub.
- ShareFile administrator account.
- Connectivity verified between XenMobile and ShareFile.

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

1. In the XenMobile web console, click **Configure** > **ShareFile**. The **ShareFile** configuration page appears.



ShareFile

Configure settings to connect to the ShareFile account and administrator service account for user account management.

Domain*: appc.sharefile.com

Assign to delivery groups: Type to search

☑ AllUsers

Selected delivery groups: AllUsers

ShareFile Administrator Account Logon

User name*: us1user1@[redacted].net

Password*: ••••••••

User account provisioning: OFF

SAML certificate

Name: XMS.example.com

2. Configure these settings:

- **Domain**: Type your ShareFile subdomain name; for example example.sharefile.com.
- **Assign to delivery groups**: Select or search for the delivery groups that you want to be able to use SSO with ShareFile.
- **ShareFile Administrator Account Logon**
  - **User name**: Type the ShareFile administrator user name. This user must have administrator privileges.
  - **Password**: Type the ShareFile administrator password.
  - **User account provisioning**: Turn on this option if you want to enable user provisioning in XenMobile; leave it disabled if you plan to use the ShareFile User Management Tool for user provisioning.

    Note: If a user without a ShareFile account is included in the selected roles, XenMobile automatically provisions a ShareFile account for that user if you enable User account provisioning. Citrix recommends that you use a role with a small membership for testing the configuration. Doing so avoids the potential of a large number of users without ShareFile accounts.

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

4. Click **Save**. XenMobile syncs with ShareFile and updates the ShareFile settings **ShareFile Issuer/Entity ID** and **Login URL**.

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

1. With the MDX Toolkit, wrap the ShareFile mobile app. For more information about wrapping apps with the MDX Toolkit, see Wrapping Apps with the MDX Toolkit.

2. In the XenMobile console, upload the wrapped ShareFile mobile app. For information about uploading MDX apps, see To add an MDX app to XenMobile.

3. Verify the SAML settings by logging on to ShareFile with the administrator user name and password you configured above.

4. Verify that ShareFile and XenMobile are configured for the same time zone.

Note: Make sure that XenMobile shows the correct time with regard to the configured time zone. If not, SSO failure may occur.

Validate the ShareFile mobile app

1. On the user device, if it has not already been done, install and configure Secure Hub.

2. From the XenMobile Store, download and install the ShareFile mobile app.

3. Start the ShareFile mobile app. ShareFile 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 XenMobile 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.

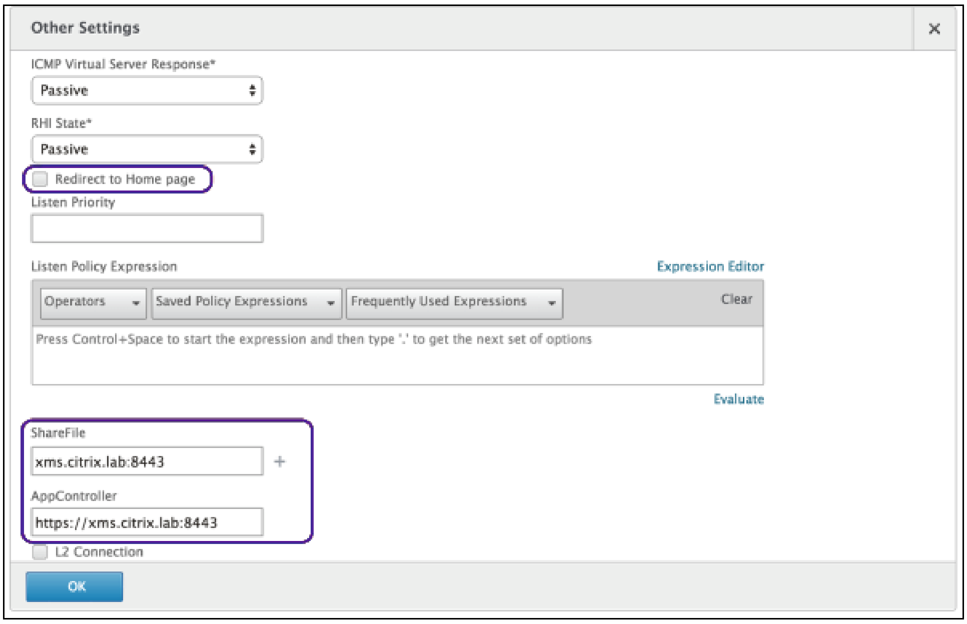
If you want to configure access for non-wrapped ShareFile clients, such as the web site, Outlook plugin, or the sync clients, you must configure NetScaler Gateway to support the use of XenMobile as a SAML identity provider as follows:

- Disable home page redirection.
- Create a ShareFile session policy and profile.
- Configure policies on the NetScaler Gateway virtual server.

Disable home page redirection

You must disable the default behavior for requests that come through the /cginfra path so that the user sees the original requested internal URL instead of the configured home page.

1. Edit the settings for the NetScaler Gateway virtual server that is used for XenMobile logons. In NetScaler 10.5, go to **Other Settings** and then clear the check box labeled **Redirect to Home Page**.



ICMP Virtual Server Response*: Passive

RHI State*: Passive

□ Redirect to Home page

Listen Priority:

Listen Policy Expression: Press Control+Space to start the expression and then type '.' to get the next set of options

ShareFile: xms.citrix.lab:8443

AppController: https://xms.citrix.lab:8443

□ L2 Connection

2. Under **ShareFile**, type your XenMobile internal server name and port number.

3. Under **AppController**, type your XenMobile URL.

This configuration authorizes requests to the URL you entered through the /cginfra path.

Create a ShareFile session policy an request profile

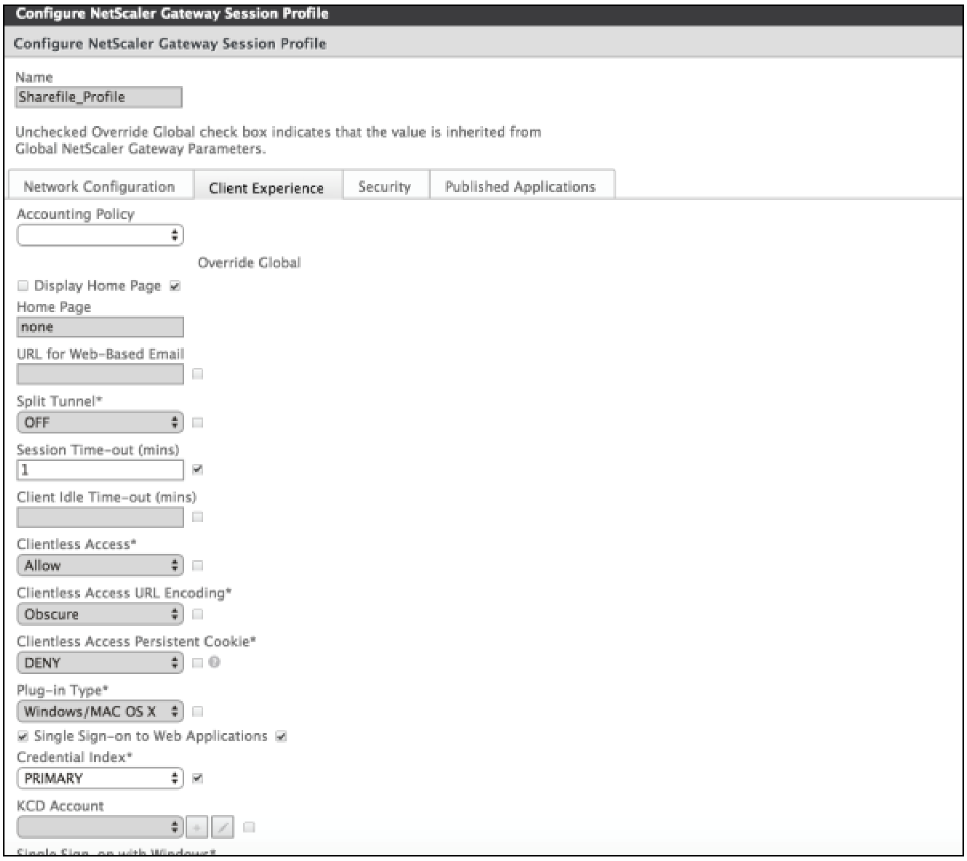
Configure these settings to create a ShareFile session policy and request profile:

1. In the NetScaler Gateway configuration utility, in the left-hand navigation pane, click **NetScaler Gateway** > **Policies** > **Session**.

2. Create a new session policy. On the **Policies** tab, click **Add**.

3. In the **Name** field, type **ShareFile_Policy**.

4. Create a new action by clicking the **+** button. The **Create NetScaler Gateway Session Profile** page appears.



Configure NetScaler Gateway Session Profile

Configure NetScaler Gateway Session Profile

Name: Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Accounting Policy:

Override Global

□ Display Home Page ☑

Home Page: none

URL for Web-Based Email: □

Split Tunnel*: OFF □

Session Time-out (mins): 1 ☑

Client Idle Time-out (mins): □

Clientless Access*: Allow □

Clientless Access URL Encoding*: Obscure □

Clientless Access Persistent Cookie*: DENY □

Plug-in Type*: Windows/MAC OS X □

☑ Single Sign-on to Web Applications ☑

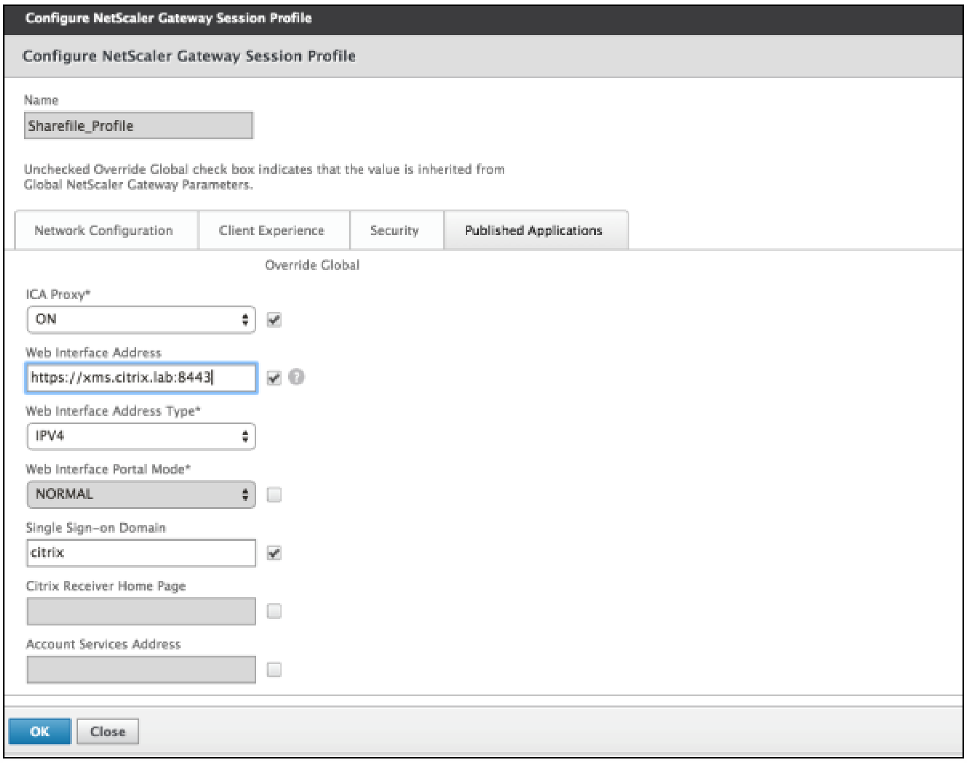
Credential Index*: PRIMARY ☑

KCD Account: □

Single Sign-on with Windows*

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**: In the list, click PRIMARY.
- Click the **Published Applications** tab.


Configure NetScaler Gateway Session Profile

Configure NetScaler Gateway Session Profile

Name: Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Override Global

ICA Proxy*: ON ☑

Web Interface Address: https://xms.citrix.lab:8443 ☑

Web Interface Address Type*: IPV4

Web Interface Portal Mode*: NORMAL □

Single Sign-on Domain: citrix ☑

Citrix Receiver Home Page: □

Account Services Address: □

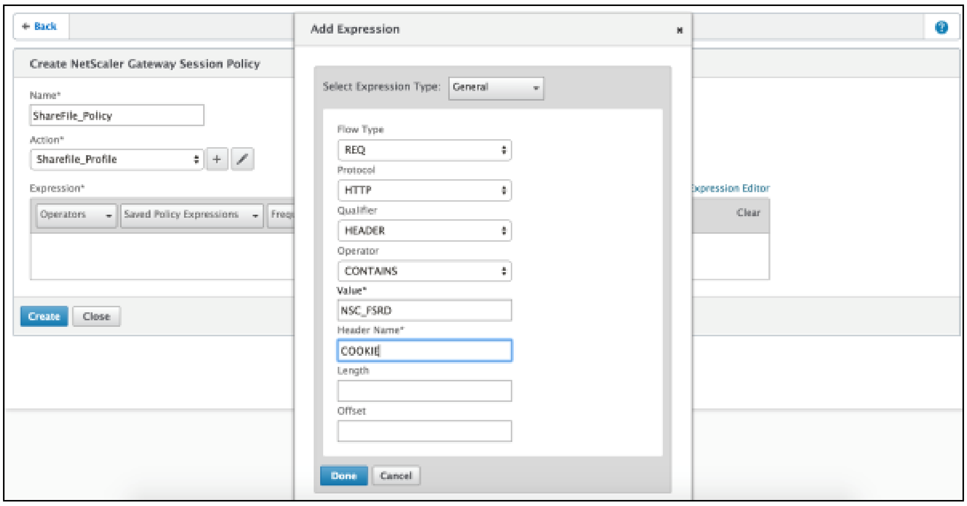
Configure these settings:

- **ICA Proxy**: In the list, click **ON**.
- **Web Interface Address**: Type your XenMobile server URL.
- **Single Sign-on Domain**: Type your Active Directory domain name.

> **Note**: When configuring the NetScaler Gateway Session Profile, the domain suffix for **Single Sign-on Domain** must match the XenMobile domain alias defined in LDAP.

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

6. Click **Expression Editor**.


Create NetScaler Gateway Session Policy

Name*: ShareFile_Policy

Action*: Sharefile_Profile

Expression*

Add Expression

Select Expression Type: General

Flow Type: REQ

Protocol: HTTP

Qualifier: HEADER

Operator: CONTAINS

Value*: NSC_FSRD

Header Name*: COOKIE

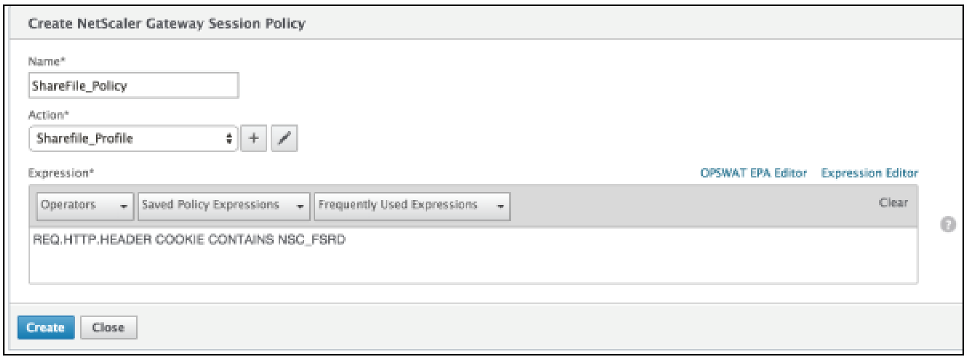
Length:

Offset:

Configure these settings:

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

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



Create NetScaler Gateway Session Policy

Name*: ShareFile_Policy

Action*: Sharefile_Profile

Expression*: REQ.HTTP.HEADER COOKIE CONTAINS NSC_FSRD

Configure policies on the NetScaler Gateway virtual server

Configure these settings on the NetScaler Gateway virtual server.

1. In the NetScaler Gateway configuration utility, in the left-hand navigation pane, click **NetScaler Gateway** > **Virtual Servers**.

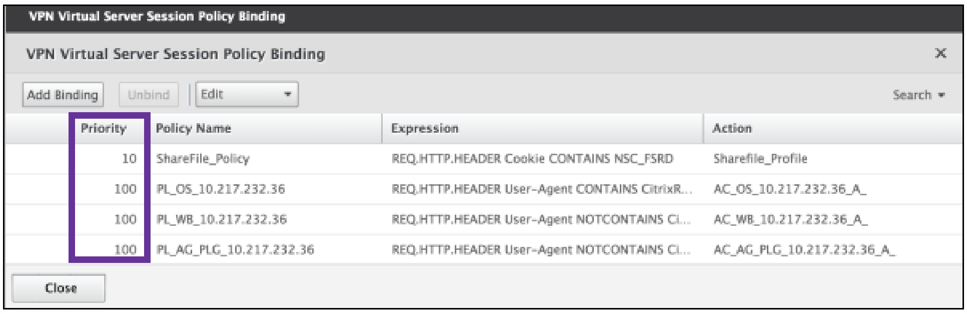
2. In the **Details** pane, click your NetScaler Gateway virtual server.

3. Click **Edit**.

4. Click **Configured policies** > **Session policies** and then click **Add binding**.

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, as shown in the following figure.



VPN Virtual Server Session Policy Binding

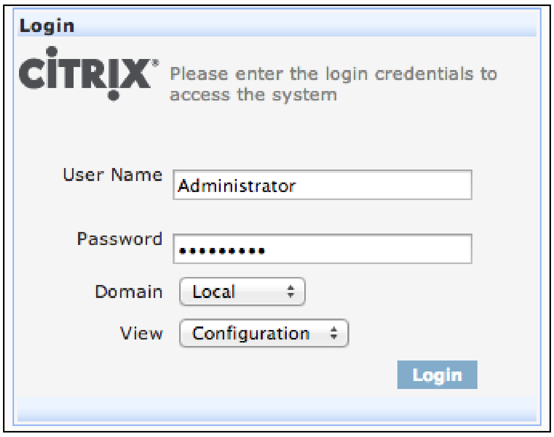
Priority	Policy Name	Expression	Action
10	ShareFile_Policy	REQ.HTTP.HEADER Cookie CONTAINS NSC_FSRD	Sharefile_Profile
100	PL_OS_10.217.232.36	REQ.HTTP.HEADER User-Agent CONTAINS CitrixR...	AC_OS_10.217.232.36_A_
100	PL_WB_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Ci...	AC_WB_10.217.232.36_A_
100	PL_AG_PLG_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Ci...	AC_AG_PLG_10.217.232.36_A_

7. Click **Done** and then save the running NetScaler configuration.

Use the following steps to find the internal app name for your ShareFile configuration.

1. Log on to the XenMobile administrator tool using the URL **https://<XenMobile server>:4443/OCA/admin/**. Be sure to enter "OCA" in uppercase letters.

2. In the **View** list, click **Configuration**.



Login

Please enter the login credentials to access the system

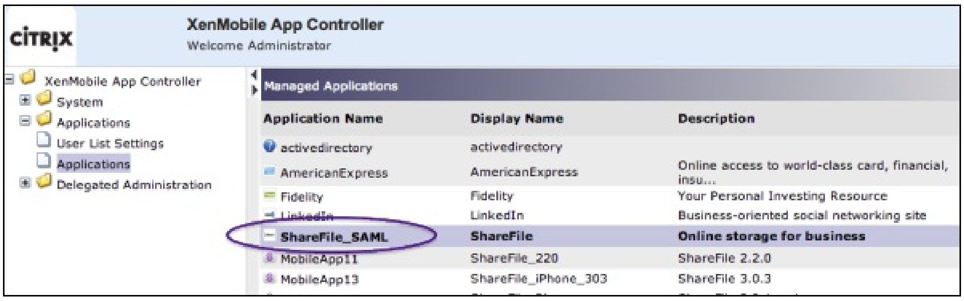
User Name: Administrator

Password: •••••••••

Domain: Local

View: Configuration

3. Click **Applications > Applications** and note the **Application Name** for the app with the **Display Name** "ShareFile".



XenMobile App Controller

Welcome Administrator

Managed Applications

Application Name	Display Name	Description
activedirectory	activedirectory	
AmericanExpress	AmericanExpress	Online access to world-class card, financial, insu...
Fidelity	Fidelity	Your Personal Investing Resource
LinkedIn	LinkedIn	Business-oriented social networking site
ShareFile_SAML	ShareFile	Online storage for business
MobileApp11	ShareFile_220	ShareFile 2.2.0
MobileApp13	ShareFile_iPhone_303	ShareFile 3.0.3

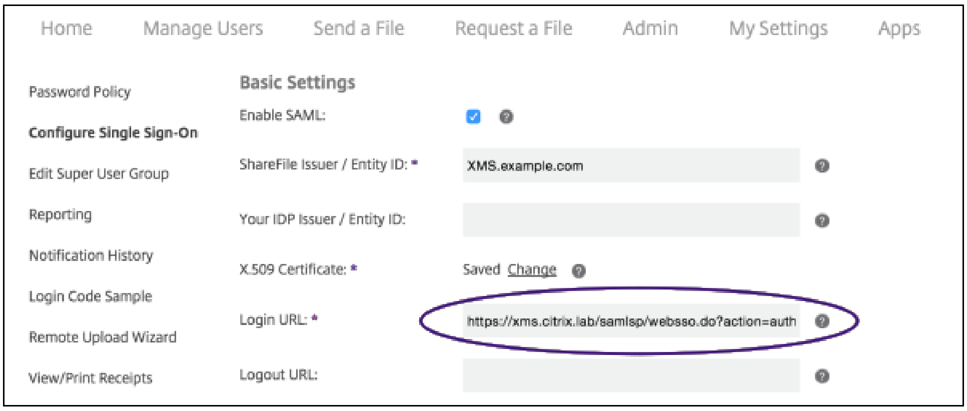
Modify the ShareFile.com SSO settings

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

2. In the ShareFile web interface, click **Admin** and then select **Configure Single Sign-on**.

3. Edit the **Login URL** as follows:

The **Login URL** should look similar to: https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.



Home | Manage Users | Send a File | Request a File | Admin | My Settings | Apps

- Password Policy
- **Configure Single Sign-On**
- Edit Super User Group
- Reporting
- Notification History
- Login Code Sample
- Remote Upload Wizard
- View/Print Receipts

Basic Settings

Enable SAML:	☑
ShareFile Issuer / Entity ID: *	XMS.example.com
Your IDP Issuer / Entity ID:	
X.509 Certificate: *	Saved Change
Login URL: *	https://xms.citrix.lab/samlsp/websso.do?action=auth
Logout URL:	

- Insert the NetScaler Gateway virtual server external FQDN plus "/cginfra/https/" in front of the XenMobile server FQDN and then add "8443" after the XenMobile FQDN.

  The URL should now look similar to this: 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 ShareFile application name from step 3 in SAML for single sign-on with ShareFile. 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).

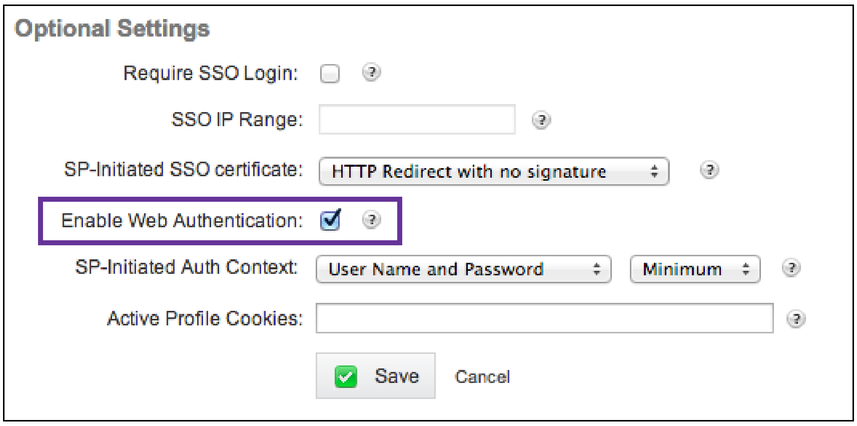
  The URL should now look similar to this: https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**&app=ShareFile_SAML**&reqtype=1

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

  The modified URL should now look similar to: https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**.

  Important: Each time you edit or recreate the ShareFile app or change the ShareFile settings in the XenMobile console, a new number is appended the internal application name, which means you must also update the Login URL in the ShareFile web site to reflect the updated app name.

4. Under **Optional Settings**, select the **Enable Web Authentication** check box.



Optional Settings

Require SSO Login:	□
SSO IP Range:	
SP-Initiated SSO certificate:	HTTP Redirect with no signature
Enable Web Authentication:	☑
SP-Initiated Auth Context:	User Name and Password / Minimum
Active Profile Cookies:	

Do the following to validate the configuration.

1. Point your browser to https://<subdomain>sharefile.com/saml/login.

You are redirected to the NetScaler Gateway logon form. If you are not redirected, verify the preceding configuration settings.

2. Enter the user name and password for the NetScaler Gateway and XenMobile environment you configured.

Your ShareFile folders at <subdomain>.sharefile.com appear. If you do not see your ShareFile folders, make sure you entered the proper logon credentials.

Azure Active Directory as IDP

Dec 27, 2017

Configuring Azure Active Directory (AD) as your identity provider (IDP) lets users enroll in XenMobile using their Azure credentials.

iOS, Android, and Windows 10 devices are supported. iOS and Android devices enroll through Secure Hub.

You configure Azure as your IDP under **Settings** > **Authentication** > **IDP**. The **IDP** page is new to this version of XenMobile. In previous versions of XenMobile, you configured Azure under **Settings** > **Microsoft Azure**.

Requirements

Versions and licenses

- To enroll iOS or Android devices, you need Secure Hub 10.5.5.
- To enroll Windows 10 devices, you need Microsoft Azure Premium licenses.

Directory services and authentication

- XenMobile Server must be configured for certificate-based authentication.
- If you are using NetScaler for authentication, NetScaler must be configured for certificate-based authentication.
- Secure Hub authentication uses Azure AD and honors the authentication mode defined on Azure AD.
- XenMobile Server must connect to Windows Active Directory (AD) using LDAP. Configure your local LDAP server to sync with Azure AD.

Authentication flow

When device enrolls through Secure Hub and XenMobile is configured to use Azure as its IDP:

1. Users enter a user name and password, on their device, in the Azure AD login screen shown in Secure Hub.

2. Azure AD validates the user and sends an ID token.

3. Secure Hub shares the ID token with XenMobile Server.

4. XenMobile validates the ID token and the user information present in the ID token. XenMobile returns a session ID.

Azure account setup

To use Azure AD as your IDP, first log in to your Azure account and make these changes:

1. Register your custom domain and verify the domain. For details, see Add your own domain name to Azure Active Directory.

2. Extend your on-premises directory to Azure Active Directory using directory integration tools. For details, see Directory

Integration.

To use Azure AD to enroll Windows 10 devices, make the following changes to your Azure account:

1. Make the MDM a reliable party of Azure AD. To do so, click **Azure Active Directory** > **Applications** and then click **Add**.

2. Select **Add an application** from the gallery. Go to **MOBILE DEVICE MANAGEMENT** and then select **on-premises MDM application**. Save the settings.
   Note: You choose on-premises application even if you signed up for Citrix XenMobile cloud because in Microsoft terminology, any non-multi-tenant application is an on-premises MDM application.

3. In the application, configure XenMobile Server discovery, terms of use endpoints, and APP ID URI:
   • **MDM Discovery URL**: https://<FQDN>:8443/*instanceName*/wpe
   • **MDM Terms of Use URL**: https://<FQDN>:8443/*instanceName*/wpe/tou
   • **APP ID URI**: https://<FQDN>:8443/

4. Select the on-premises MDM application that you created in step 2. Enable the option, **Manage devices for these users**, to enable MDM management for all users or any specific user group.

   For more information about using Azure AD to Windows 10 devices, see the Microsoft article Azure Active Directory integration with MDM.

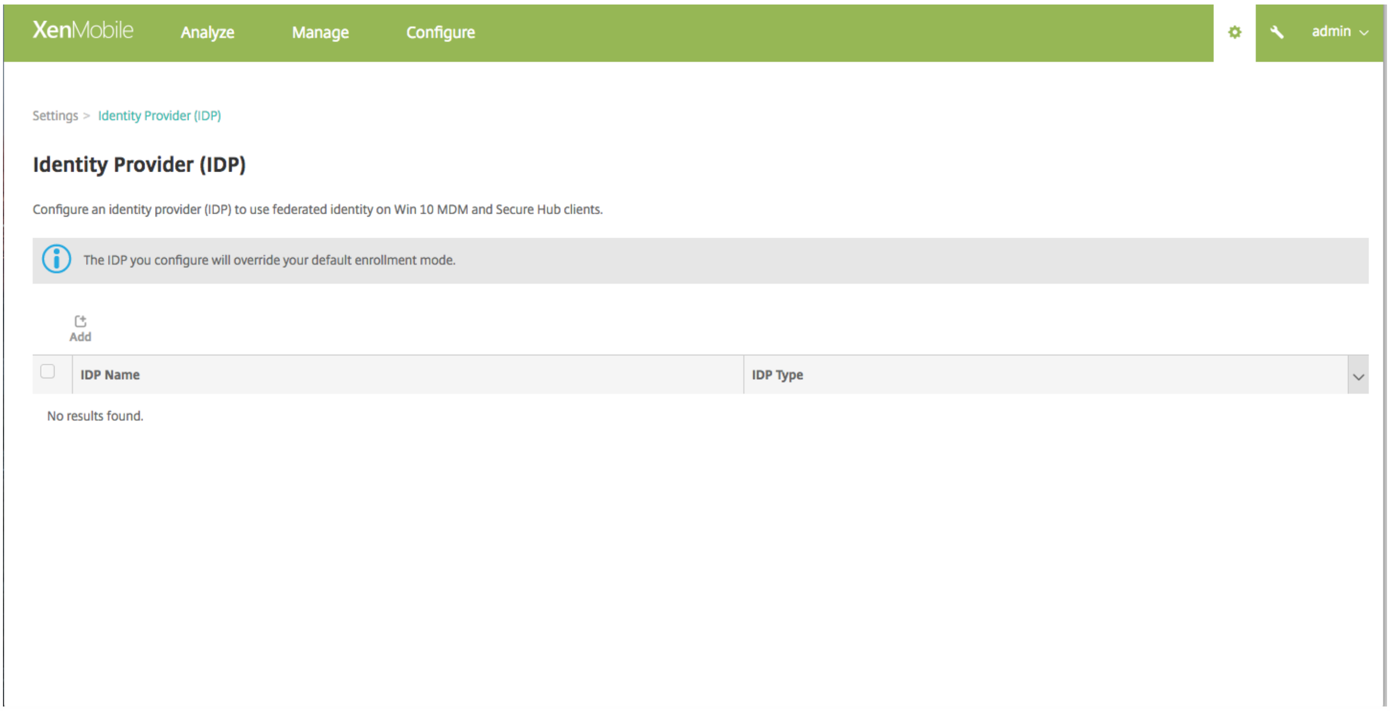
Configure Azure AD as your IDP

1. Locate or make note of the information you need from your Azure account:

   - Tenant ID from the Azure application settings page.
   - If you want to use Azure AD to enroll Windows 10 devices, you also need:
     - **App ID URI**: The URL for the server running XenMobile.
     - **Client ID**: The unique identifier for your app from the Azure Configure page.
     - **Key**: From the Azure application settings page.

2. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.

3. Under **Authentication**, click **Identity Provider (IDP)**. The **Identity Provider** page appears.



Identity Provider (IDP)

Configure an identity provider (IDP) to use federated identity on Win 10 MDM and Secure Hub clients.

The IDP you configure will override your default enrollment mode.

IDP Name	IDP Type

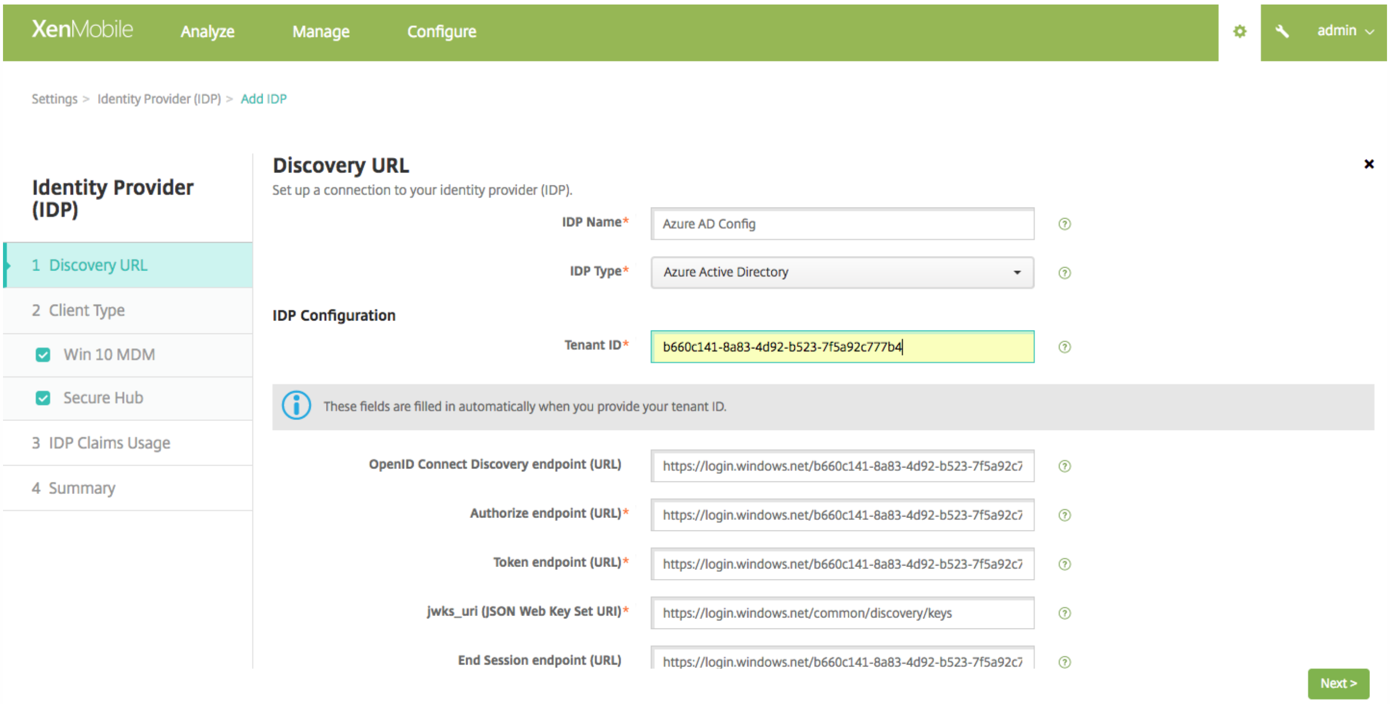
No results found.

4. Click **Add**. The **IDP configuration** page appears.

5. Configure the following information about your IDP:

   - **IDP Name**: Type a name for IDP connection you are creating.
   - **IDP Type**: Choose Azure Active Directory as your IDP type.
   - **Tenant ID**: Copy this value from the Azure application settings page. In the browser address bar, copy the section made up of numbers and letters.

   For example, in https://manage.windowszaure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem ..., the tenant ID is: abc123-abc123-abc123.



Discovery URL

Set up a connection to your identity provider (IDP).

IDP Name*: Azure AD Config

IDP Type*: Azure Active Directory

IDP Configuration

Tenant ID*: b660c141-8a83-4d92-b523-7f5a92c777b4

These fields are filled in automatically when you provide your tenant ID.

OpenID Connect Discovery endpoint (URL): https://login.windows.net/b660c141-8a83-4d92-b523-7f5a92c7

Authorize endpoint (URL)*: https://login.windows.net/b660c141-8a83-4d92-b523-7f5a92c7

Token endpoint (URL)*: https://login.windows.net/b660c141-8a83-4d92-b523-7f5a92c7

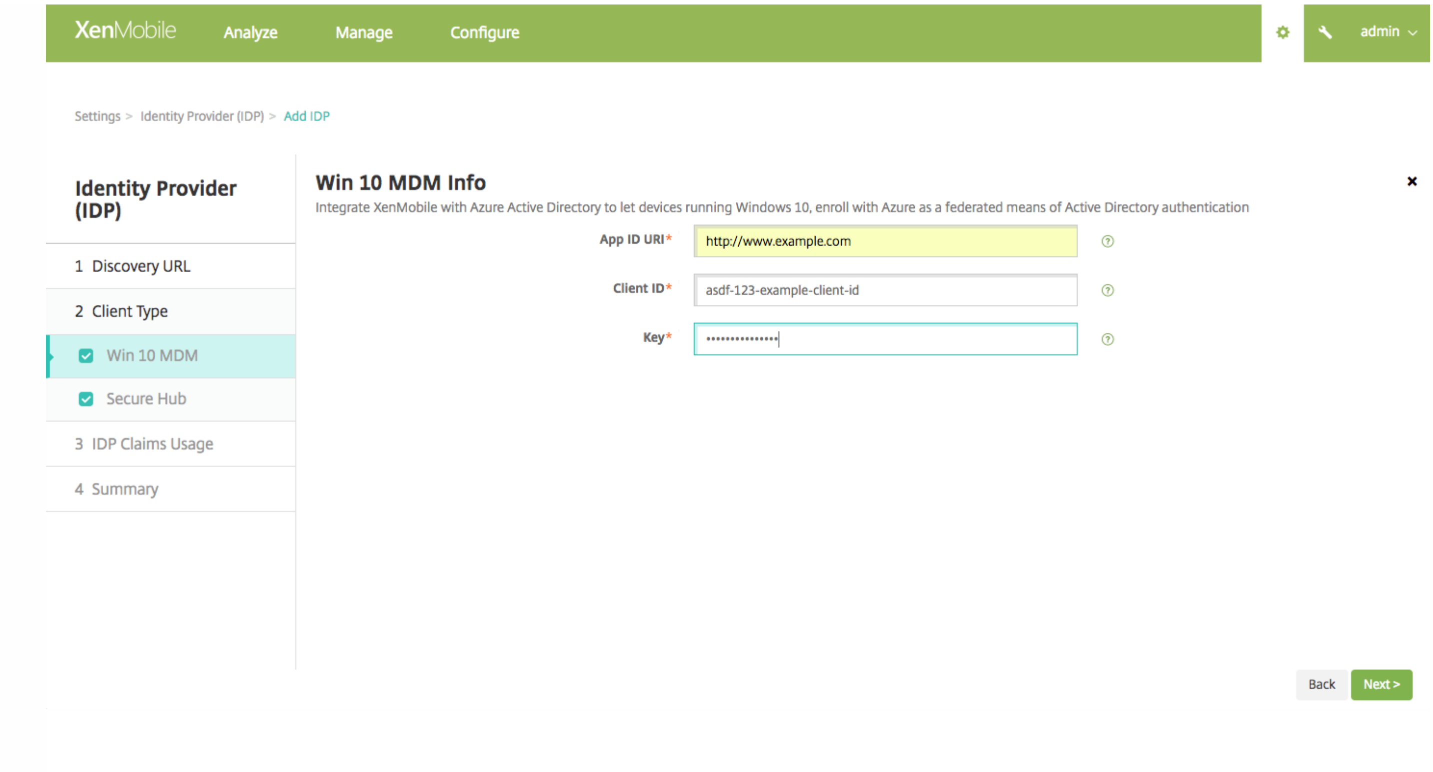
jwks_uri (JSON Web Key Set URI)*: https://login.windows.net/common/discovery/keys

End Session endpoint (URL): https://login.windows.net/b660c141-8a83-4d92-b523-7f5a92c7

6. The rest of the fields automatically fill. When they are filled, click **Next**.

7. To configure XenMobile to enroll Windows 10 devices using Azure AD for MDM enrollment, configure the following settings. To skip this optional step, clear **Win 10 MDM**.

   - **App ID URI**: Type the URL for the XenMobile Server that you entered when you configured your Azure settings.
   - **Client ID**: Copy and paste this value from the Azure Configure page. The client ID is the unique identifier for your app.
   - **Key**: Copy this value from the Azure application settings page. Under keys, select a duration in the list and then save the setting. You can then copy the key and paste it into this field. A key is required when apps read or write data in Microsoft Azure AD.



Win 10 MDM Info

Integrate XenMobile with Azure Active Directory to let devices running Windows 10, enroll with Azure as a federated means of Active Directory authentication

App ID URI* http://www.example.com

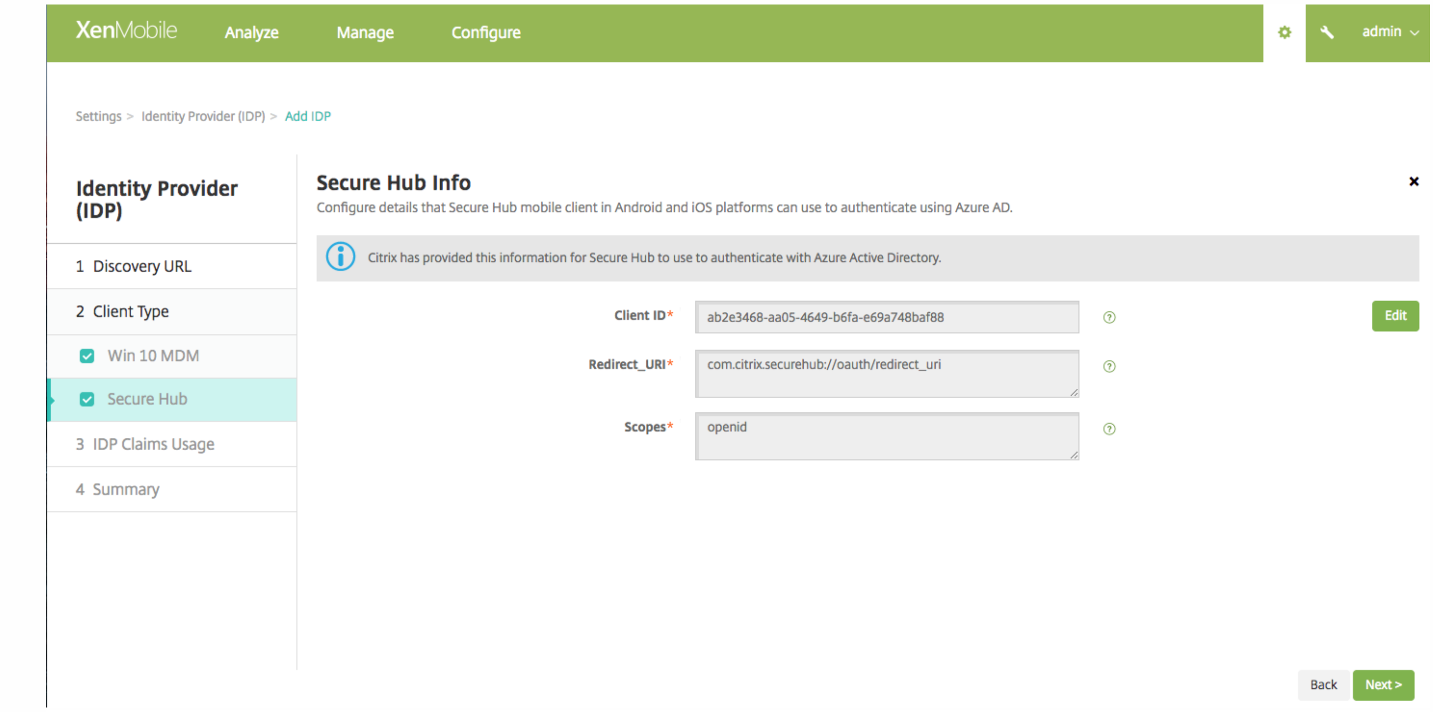
Client ID* asdf-123-example-client-id

Key* •••••••••••••••

8. Click **Next**.

   Citrix has registered Secure Hub with Microsoft Azure and maintains the information. This screen shows the details used by Secure Hub to communicate with Azure Active Directory. This page will be used in the future if any of this information needs a change. Edit this page only if Citrix advises you to.

9. Click **Next**.



Secure Hub Info

Configure details that Secure Hub mobile client in Android and iOS platforms can use to authenticate using Azure AD.

Citrix has provided this information for Secure Hub to use to authenticate with Azure Active Directory.

Client ID* ab2e3468-aa05-4649-b6fa-e69a748baf88

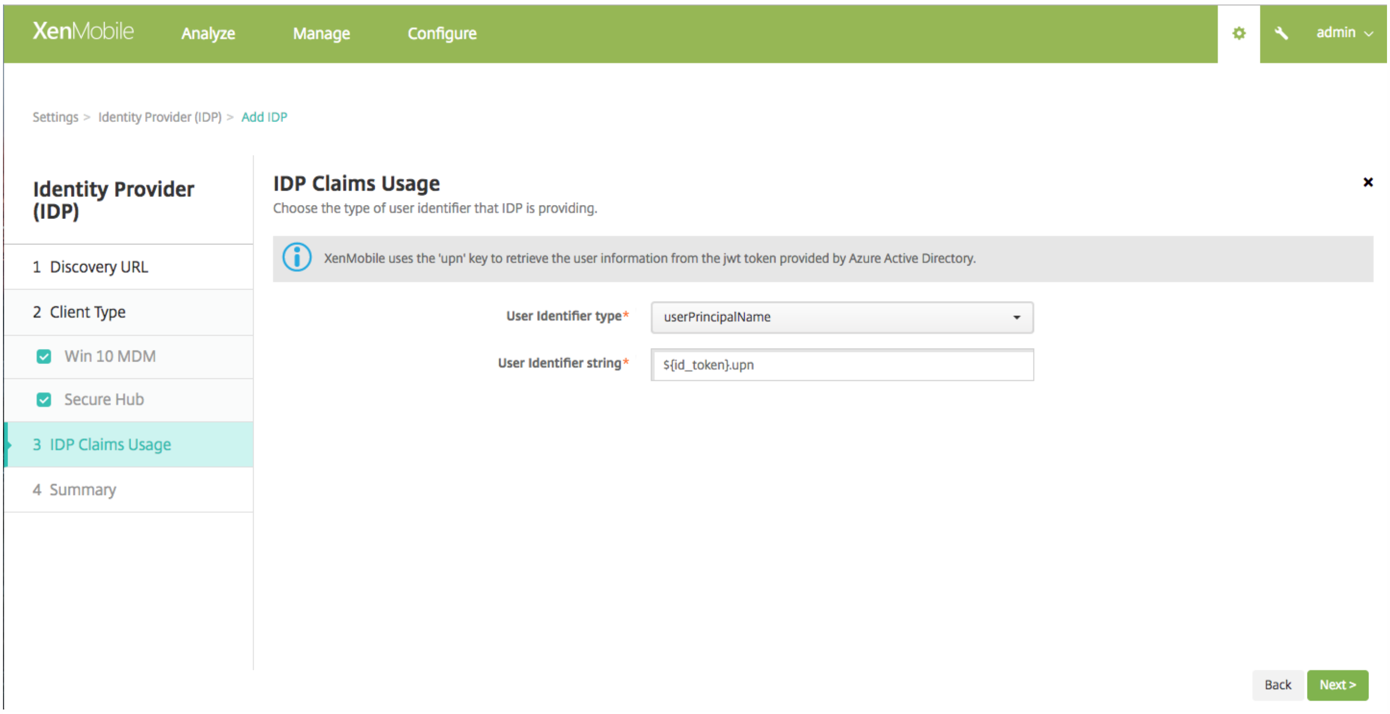
Redirect_URI* com.citrix.securehub://oauth/redirect_uri

Scopes* openid

10. Configure the type of user identifier your IDP is providing:

- **User Identifier type**: Choose **userPrincipalName** from the drop-down list.
- **User Identifier string**: This field is automatically filled.

11. Click **Next**.



IDP Claims Usage

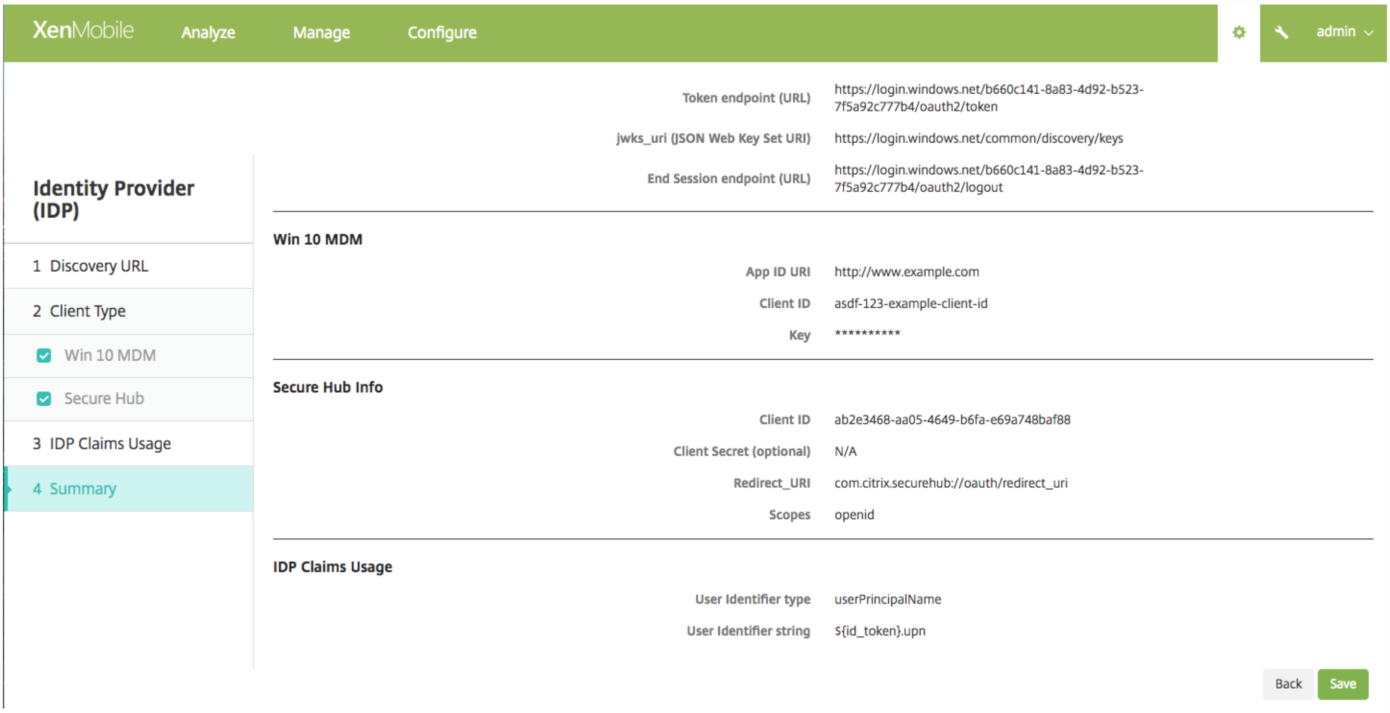
Choose the type of user identifier that IDP is providing.

XenMobile uses the 'upn' key to retrieve the user information from the jwt token provided by Azure Active Directory.

User Identifier type*: userPrincipalName

User Identifier string*: ${id_token}.upn

12. Review the **Summary** page and click **Save**.



Token endpoint (URL)	https://login.windows.net/b660c141-8a83-4d92-b523-7f5a92c777b4/oauth2/token
jwks_uri (JSON Web Key Set URI)	https://login.windows.net/common/discovery/keys
End Session endpoint (URL)	https://login.windows.net/b660c141-8a83-4d92-b523-7f5a92c777b4/oauth2/logout

Win 10 MDM

App ID URI	http://www.example.com
Client ID	asdf-123-example-client-id
Key	**********

Secure Hub Info

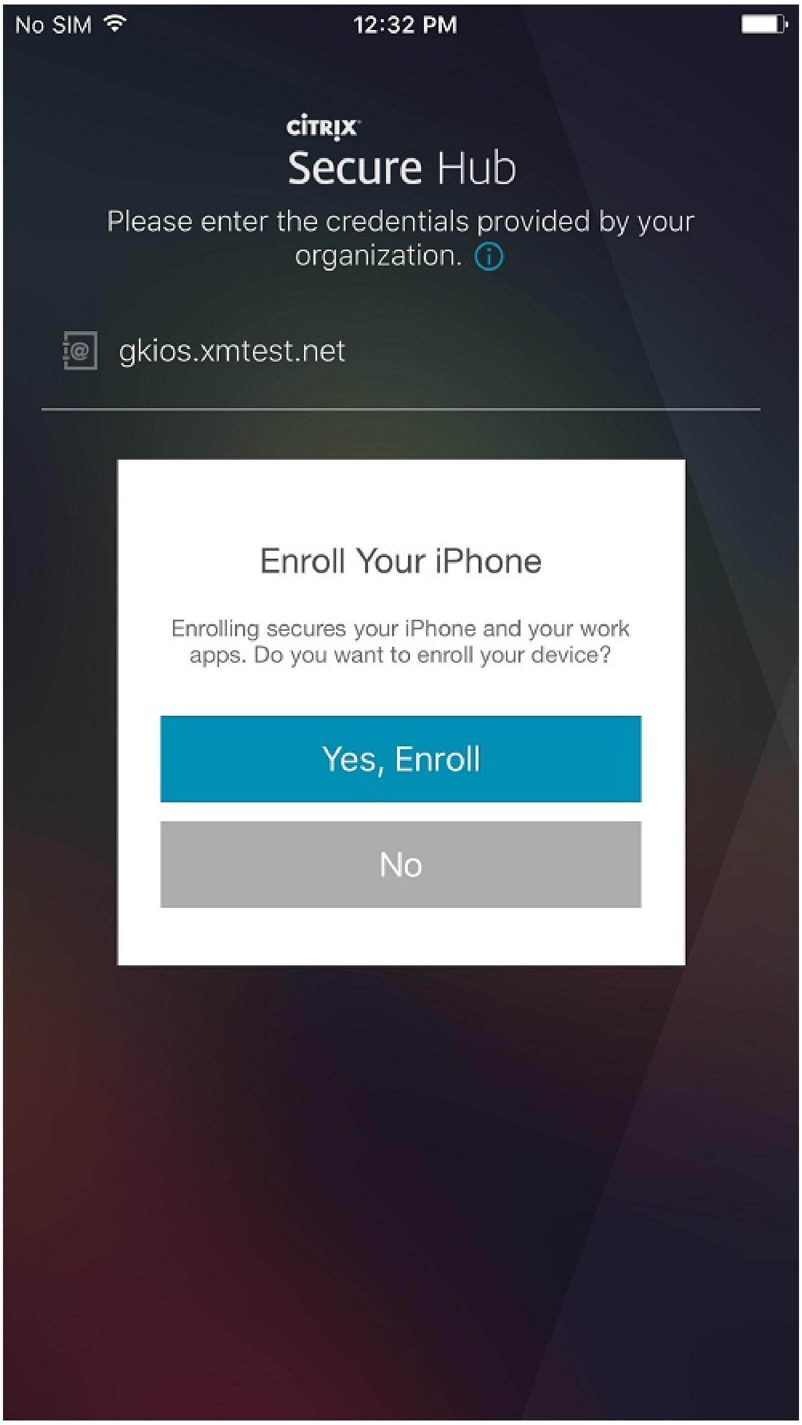
Client ID	ab2e3468-aa05-4649-b6fa-e69a748baf88
Client Secret (optional)	N/A
Redirect_URI	com.citrix.securehub://oauth/redirect_uri
Scopes	openid

IDP Claims Usage

User Identifier type	userPrincipalName
User Identifier string	${id_token}.upn

What users experience

1. Users start Secure Hub. Users then enter the XenMobile Server Fully Qualified Domain Name (FQDN), a User Principle Name (UPN), or email address.



No SIM 12:32 PM

CITRIX Secure Hub

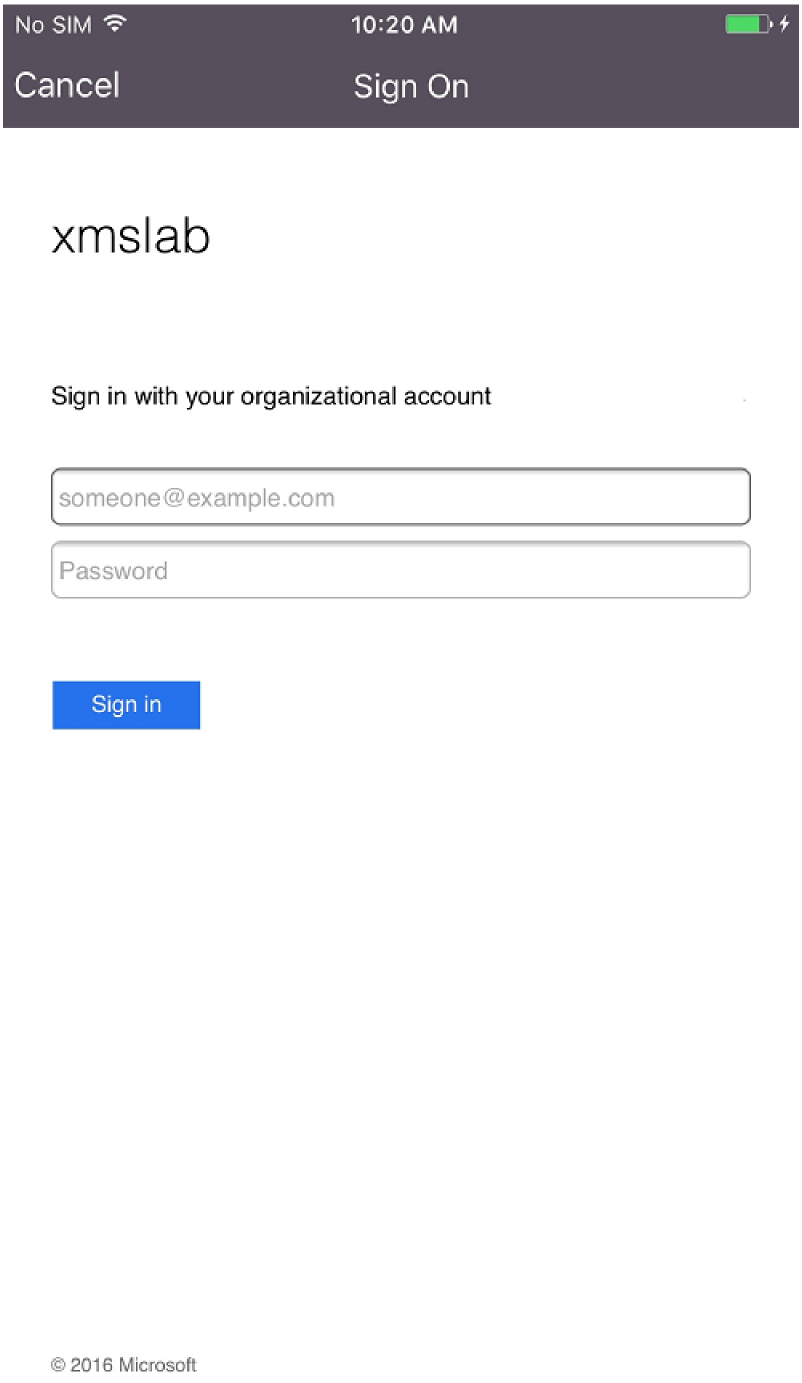
Please enter the credentials provided by your organization.

gkios.xmtest.net

Enroll Your iPhone

Enrolling secures your iPhone and your work apps. Do you want to enroll your device?

2. Users then click **Yes, Enroll**.


No SIM 10:20 AM

Cancel Sign On

xmslab

Sign in with your organizational account

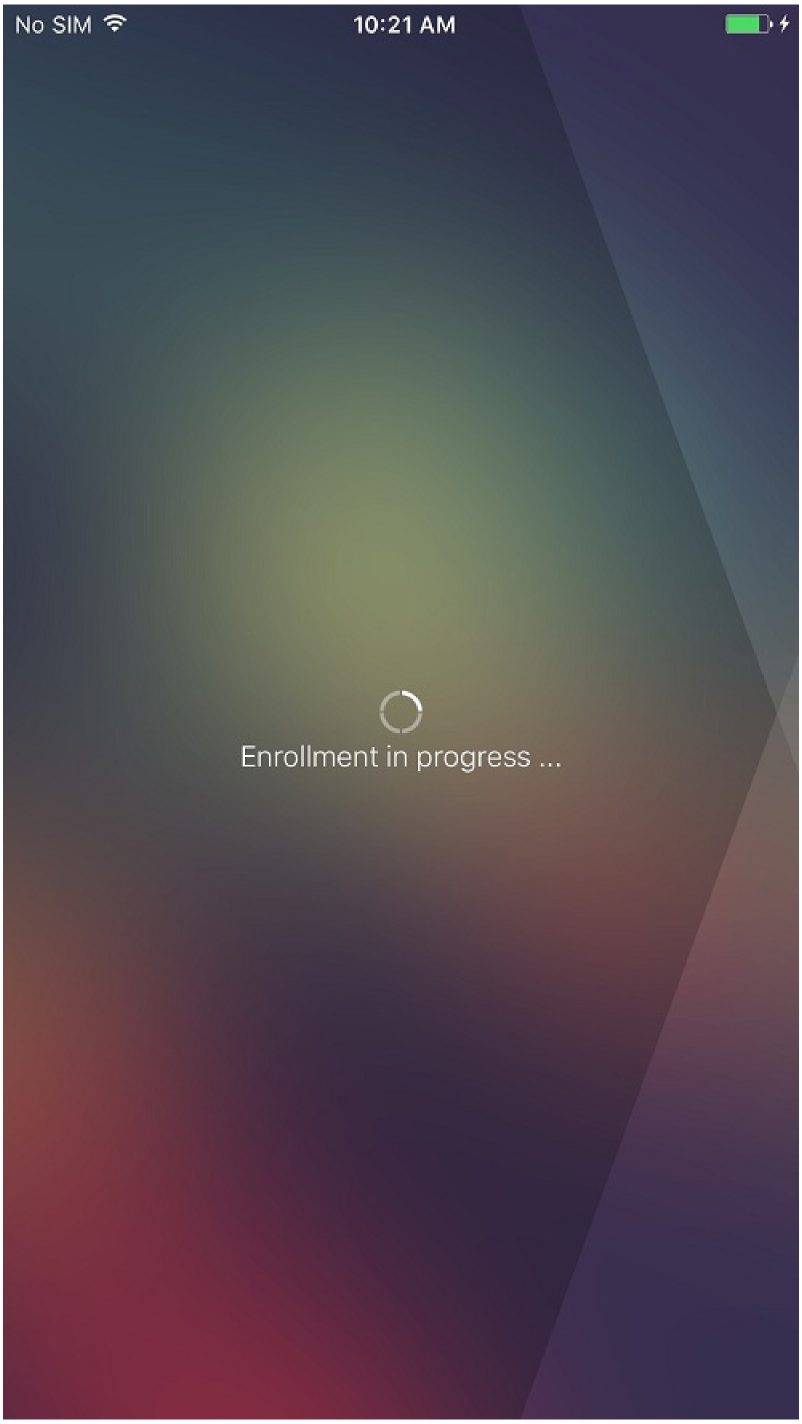
someone@example.com

Password

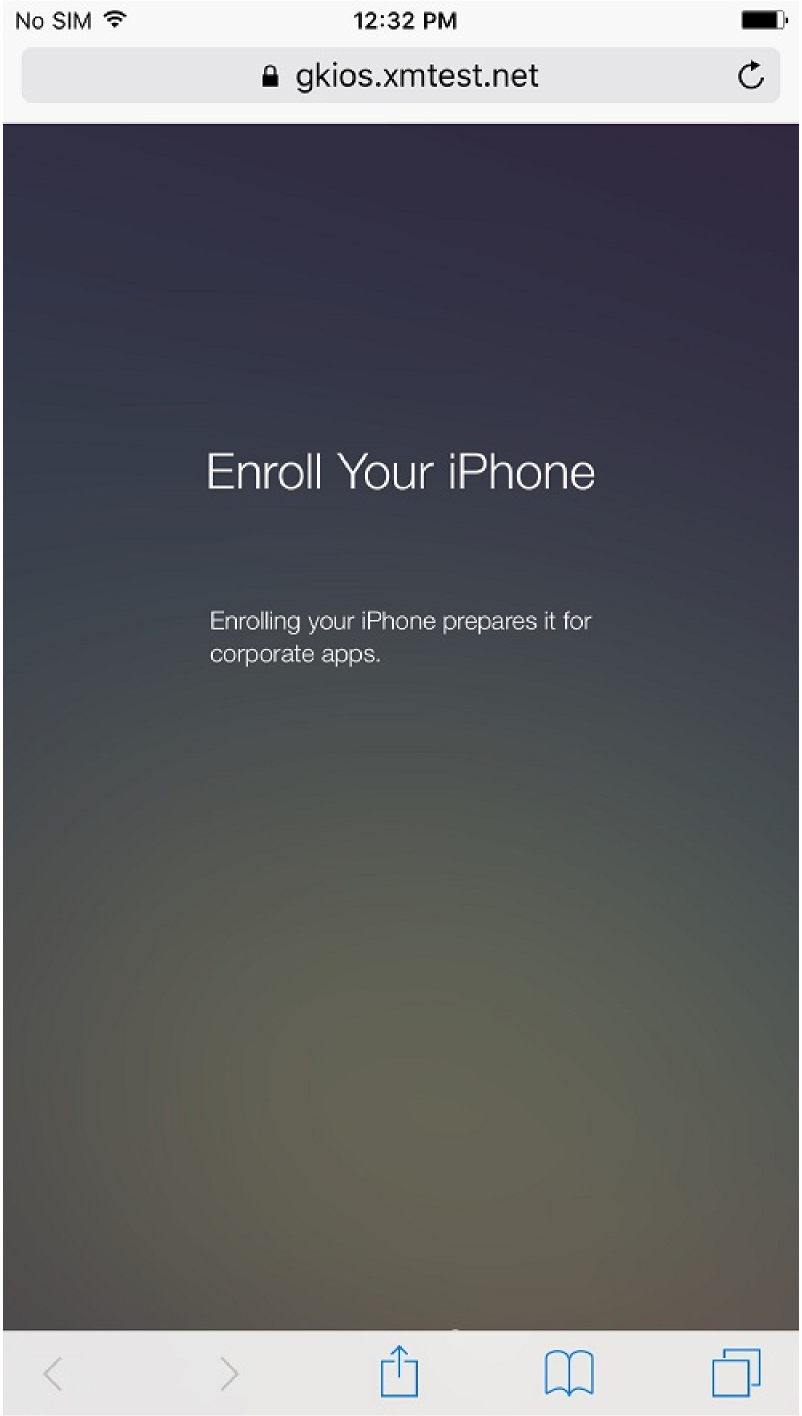
Sign in

© 2016 Microsoft

3. Users log on by using their Azure AD credentials.

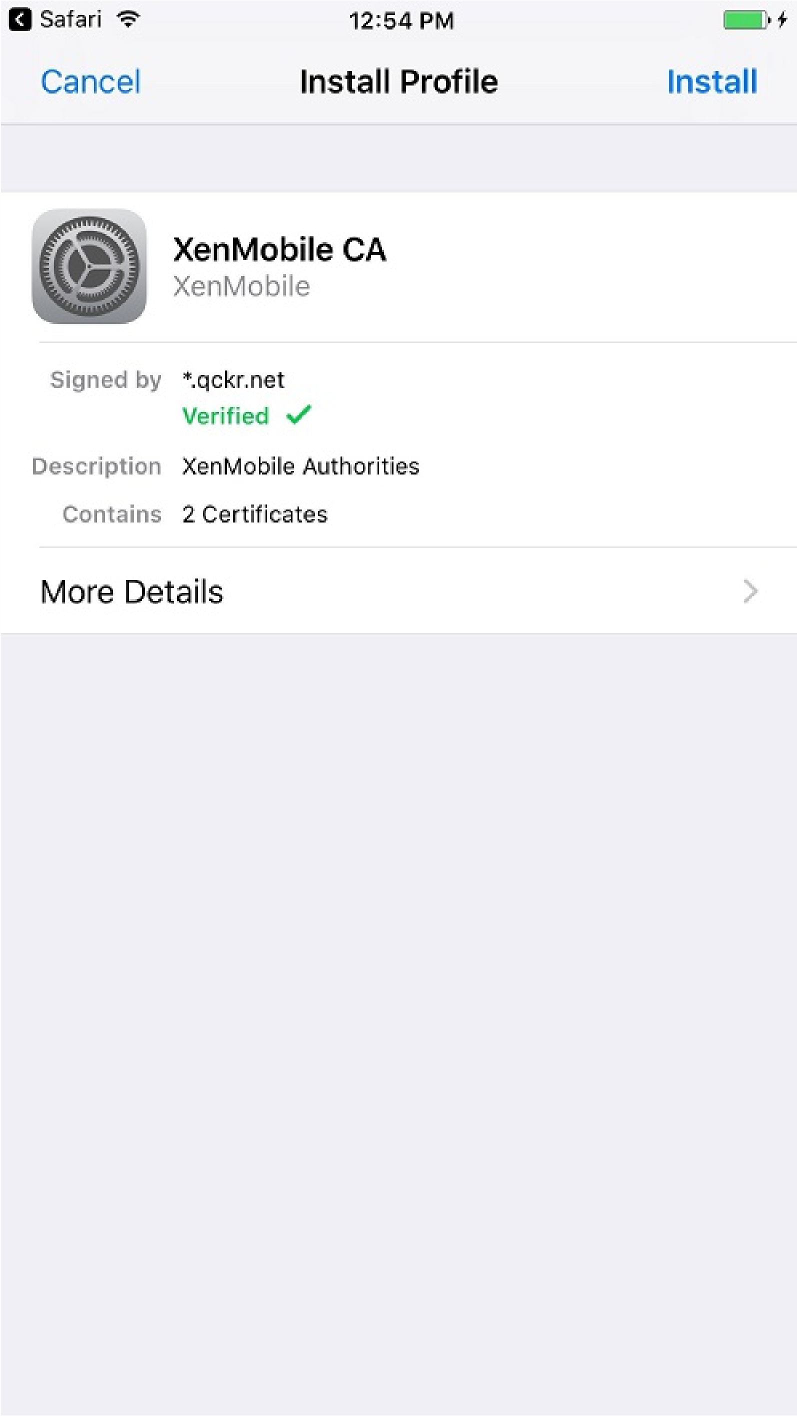


Enrollment in progress ...



Enroll Your iPhone

Enrolling your iPhone prepares it for corporate apps.



XenMobile CA
XenMobile

Signed by *.qckr.net
Verified ✓

Description XenMobile Authorities

Contains 2 Certificates

4. Users complete the enrollment steps in the same way as any other enrollment through Secure Hub.

   Note: XenMobile doesn't support authentication through Azure AD for enrollment invitations. If you send users an enrollment invitation containing an enrollment URL, users authenticate through LDAP instead of Azure AD.

Derived credentials for iOS

Dec 18, 2017

Derived credentials provide strong authentication for mobile devices. The credentials, derived from a smart card, reside in a mobile device instead of the card. The smart card is either a Personal Identity Verification (PIV) card or Common Access Card (CAC).

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

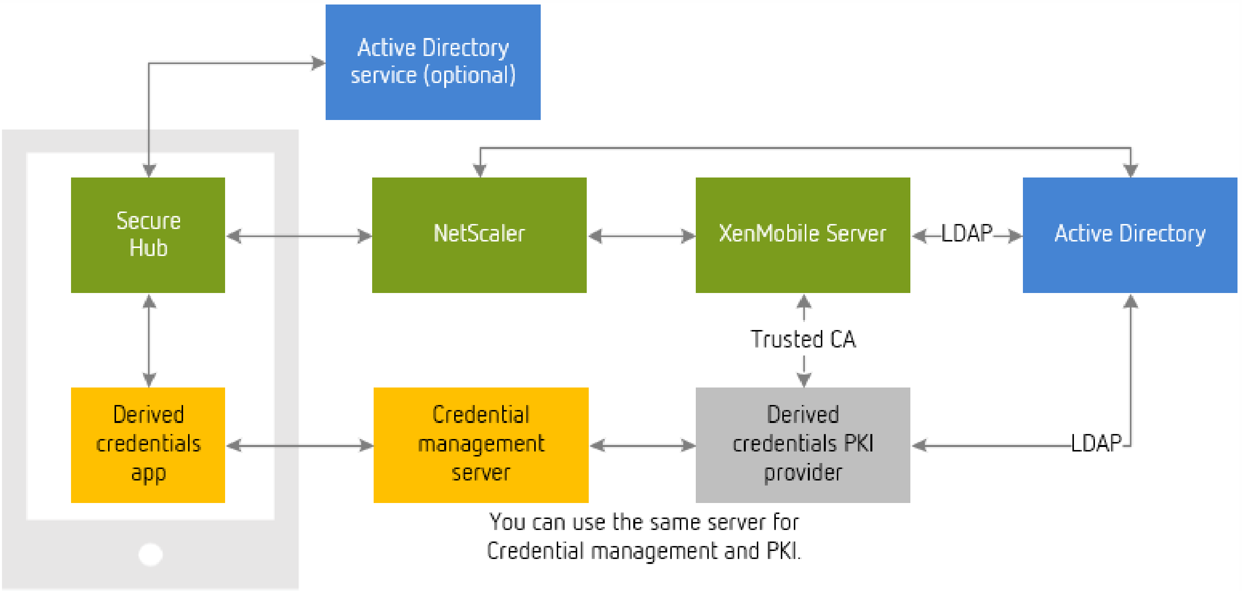
XenMobile can use derived credentials for iOS device enrollment. If configured for derived credentials, XenMobile doesn't support enrollment invitations or other enrollment modes for iOS devices. However, you can use the same XenMobile Server to enroll Android devices through enrollment invitations and other enrollment modes.

Requirements

- One of the following derived credential solutions:
  - Intercede 3.12
    Citrix has validated that XenMobile works with the Intercede derived credential solution. The app name in the Apple App Store is MyID for Citrix.
    Note: Users must install MyID for Citrix on their devices *before* enrolling in XenMobile.
- Other derived credential solutions
  While it's likely that most other credential solutions are compatible with XenMobile, test the integration before deploying it to production.
- XenMobile Server 10.6 (minimum version)
  - Configured for Enterprise (XME) mode
  - Must have the root certificate of the authority that issues certificates to the Credentials Provider server. That setup enables XenMobile 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 myID.com and the LDAP domain name is sample.com, set **Domain alias** to **sample.com, myID.com**.
  - You can't use derived credentials with shared devices.
- User identity certificates:
  - The username in the Subject alternative name field must be formatted as 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.
  - User identity in the Subject field in either Email or CN is not currently supported.
- NetScaler Gateway configured for certificate authentication or certificate plus security token authentication
  For information about PKI configuration, see PKI entities.
- Secure Hub 10.6 (minimum version)
- XenMobile Apps 10.6 (minimum version)
  - Secure Mail doesn't use derived credentials and continues to work as before.
  - Use the same developer certificate to sign all apps in the Apple App Store.

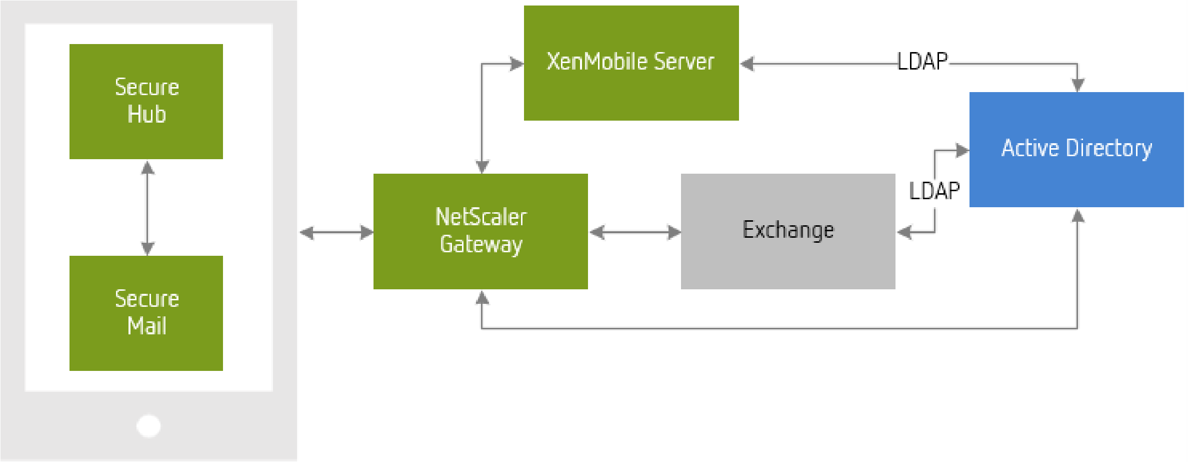
Architecture

For enrollment, XenMobile Server connects to the components described in the "Requirements" section, as shown in the following diagram.


Active Directory service (optional)
Secure Hub
NetScaler
XenMobile Server
LDAP
Active Directory
Trusted CA
Derived credentials app
Credential management server
Derived credentials PKI provider
LDAP
You can use the same server for Credential management and PKI.

- 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.
- XenMobile Server connects to your third-party PKI server to obtain certificates.

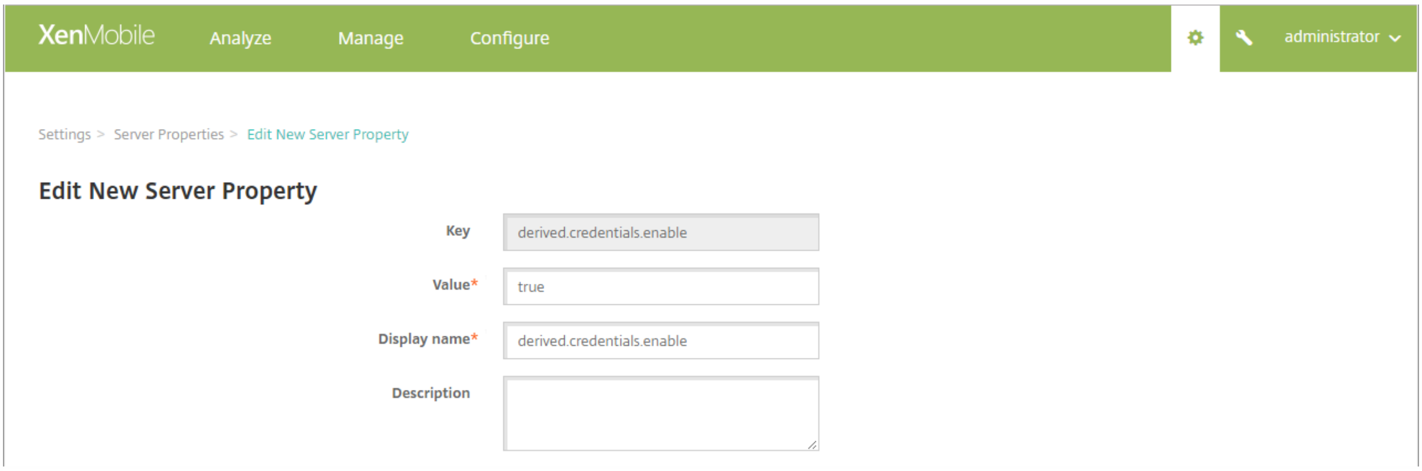
After enrollment, the components connect as shown in the following diagram.



The following sections describe how to configure XenMobile with a derived credentials provider, enable derived credentials for enrollment, and manage devices that use derived credentials.

Enable derived credentials

By default, the XenMobile console doesn't include the **Settings** > **Derived Credentials** page. To enable the interface for derived credentials, go to **Settings** > **Server Properties**, add the server property **derived.credentials.enable**, and set it to **true**.



Edit New Server Property

Key: derived.credentials.enable

Value*: true

Display name*: derived.credentials.enable

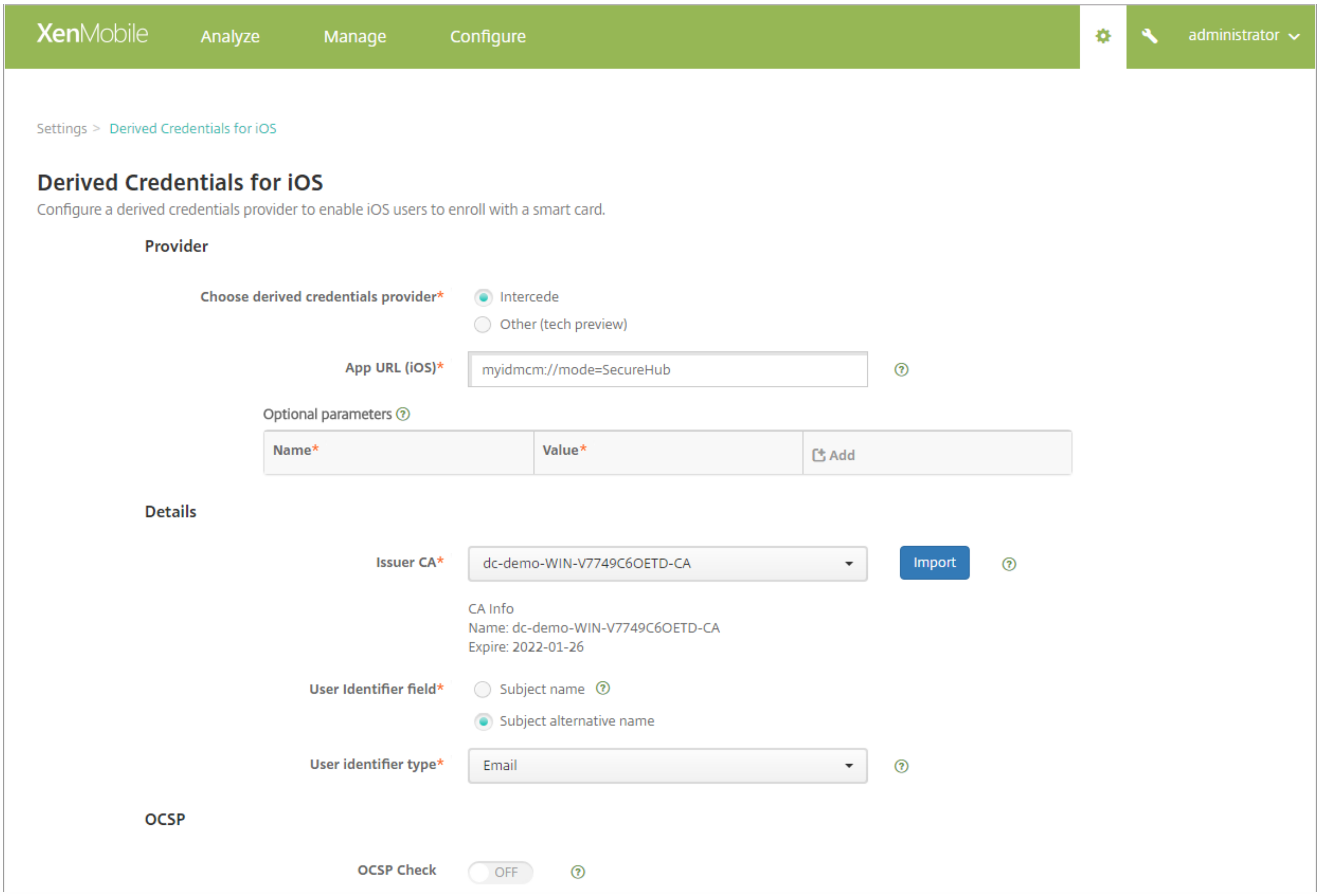
Description:

Configure derived credentials

These instructions assume that you have a working configuration for the derived credentials provider that you plan to integrate with XenMobile. You can then configure XenMobile to communicate with that server. You also choose a derived credentials CA certificate already added to XenMobile 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 XenMobile console, go to **Settings** > **Derived Credentials for iOS**.



Settings > Derived Credentials for iOS

Derived Credentials for iOS

Configure a derived credentials provider to enable iOS users to enroll with a smart card.

Provider

Choose derived credentials provider* ● Intercede ○ Other (tech preview)

App URL (iOS)* myidmcm://mode=SecureHub

Optional parameters

Name*	Value*	Add

Details

Issuer CA* dc-demo-WIN-V7749C6OETD-CA

CA Info
Name: dc-demo-WIN-V7749C6OETD-CA
Expire: 2022-01-26

User Identifier field* ○ Subject name ● Subject alternative name

User identifier type* Email

OCSP

OCSP Check OFF

2. Under **Provider**:

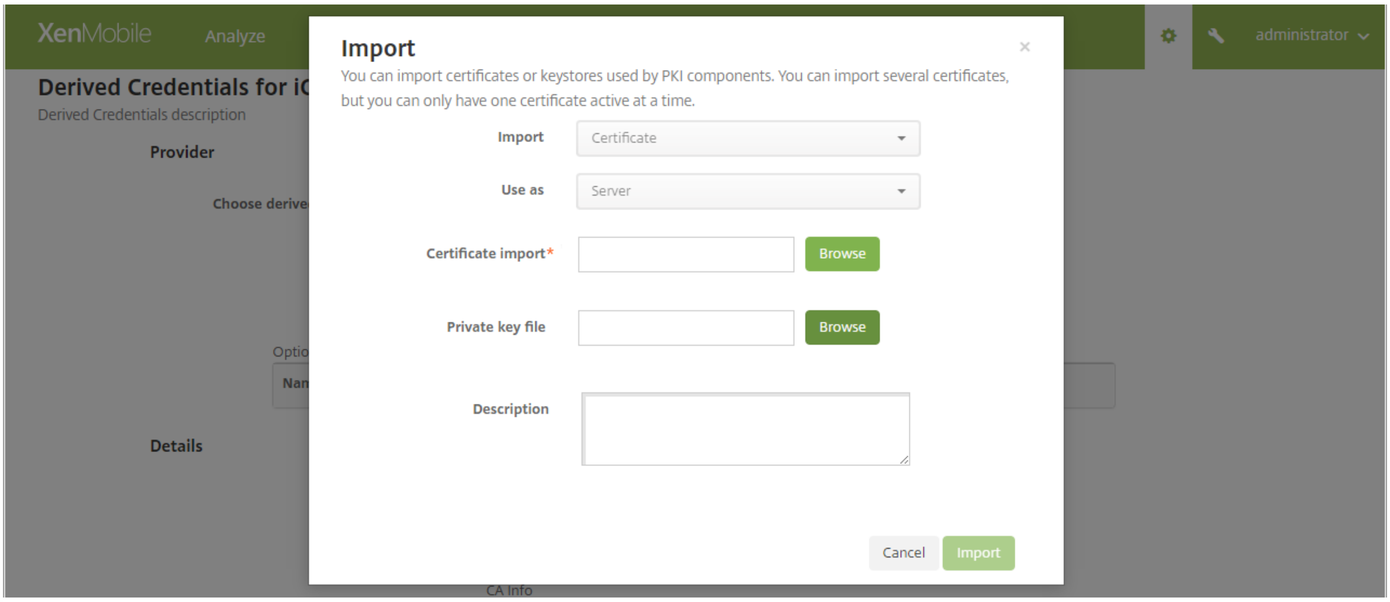
   - **Choose derived credentials provider**. Citrix validated that XenMobile works with **Intercede**. If you choose **Other** for the provider, test the integration before putting your server into production.
   - **App URL (iOS)**: If you choose **Intercede** as the provider, XenMobile fills in the **App URL**. If you choose **Other** as the provider, obtain the App URL from your derived credentials provider.

     Note: If a device can't contact your provider, verify the App URL with the provider. You might need to change it.

   - **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.

3. Specify a certificate for derived credentials: If the certificate is already uploaded to XenMobile, choose that certificate from **Issuer CA**. Otherwise, click **Import** to add a certificate. The **Import Certificate** dialog box appears.

4. In the **Import Certificate** dialog box, click **Browse** to navigate to the certificate. Then click **Browse** to navigate to the private key file.



Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import: Certificate

Use as: Server

Certificate import*: Browse

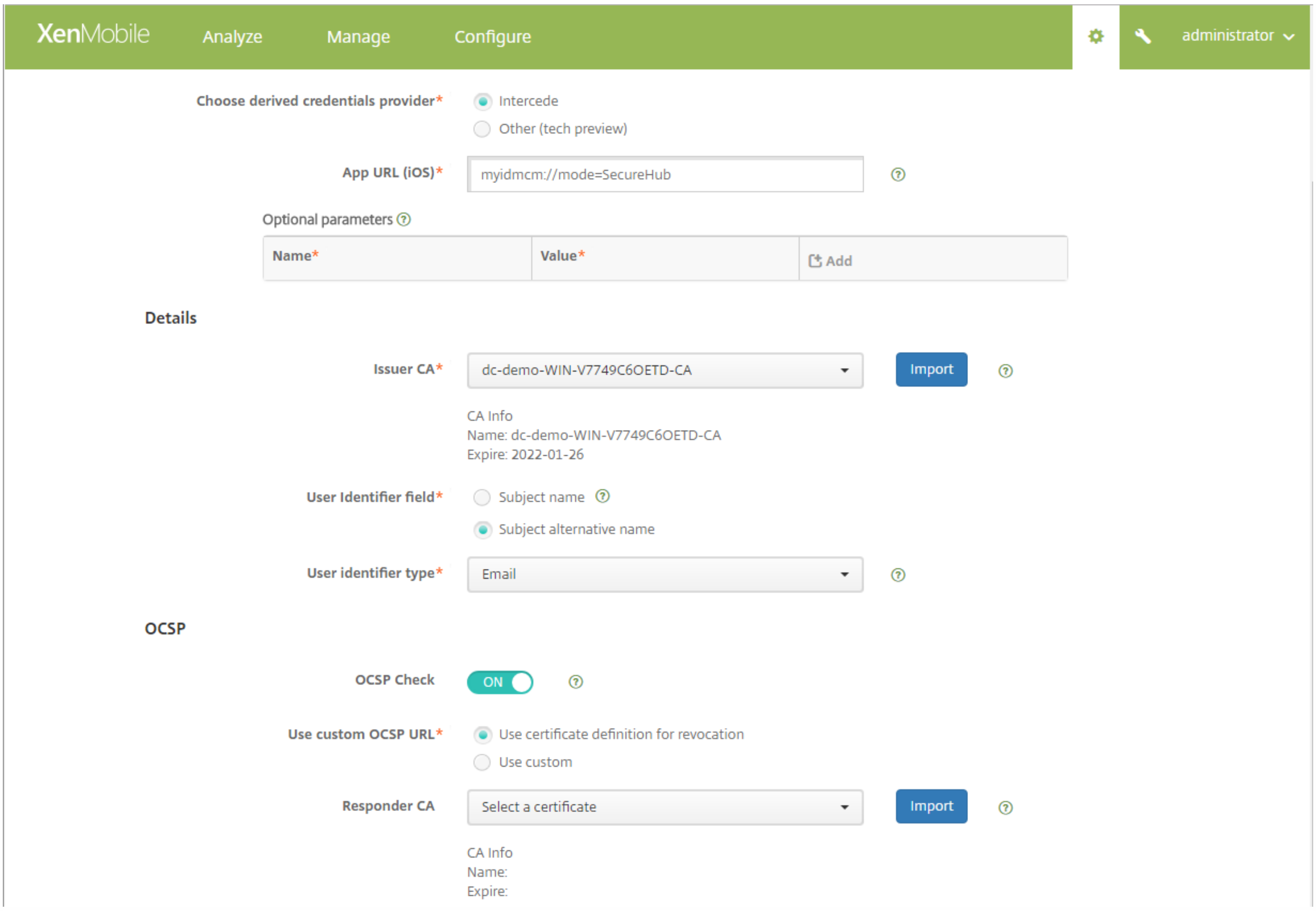
Private key file: Browse

Description:

5. If you choose **Intercede** as the provider, XenMobile fills in the **User Identifier field** and the **User Identifier type**. For Intercede, the **User Identifier field** is **Subject alternative name**, and the **User Identifier type** is **userPrincipalName**. Contact other derived credential providers for their information and configure the settings.

6. You can optionally use an OCSP responder for certificate revocation checking. By default, OSP checking is off. To activate OCSP support for the CA certificate:

   - Set **OCSP check** to **ON**.



Choose derived credentials provider* ● Intercede ○ Other (tech preview)

App URL (iOS)* myidmcm://mode=SecureHub

Optional parameters

Name*	Value*

Details

Issuer CA* dc-demo-WIN-V7749C6OETD-CA

CA Info
Name: dc-demo-WIN-V7749C6OETD-CA
Expire: 2022-01-26

User Identifier field* ○ Subject name ● Subject alternative name

User identifier type* Email

OCSP

OCSP Check ON

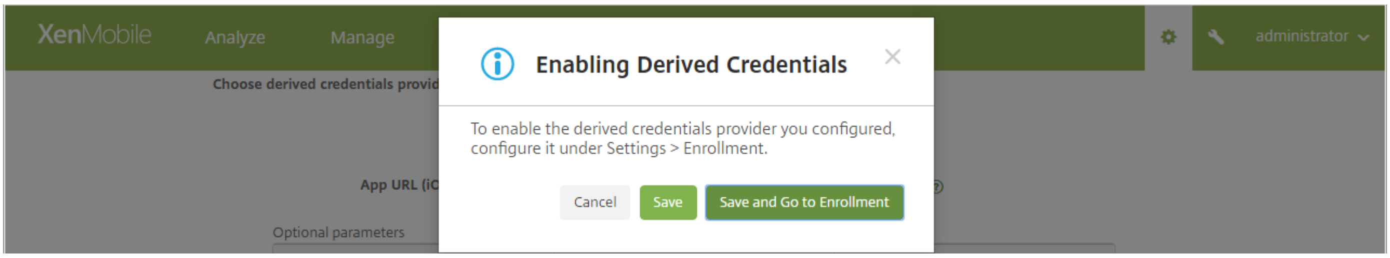
Use custom OCSP URL* ● Use certificate definition for revocation ○ Use custom

Responder CA Select a certificate

CA Info
Name:
Expire:

- Choose an option for **Use custom OCSP URL**. By default, XenMobile extracts the OCSP URL from the certificate (the **Use certificate definition for revocation** option). To specify a responder URL, click **Use custom** and 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.

7. Click **Save**. The **Derived Credentials** dialog box appears.

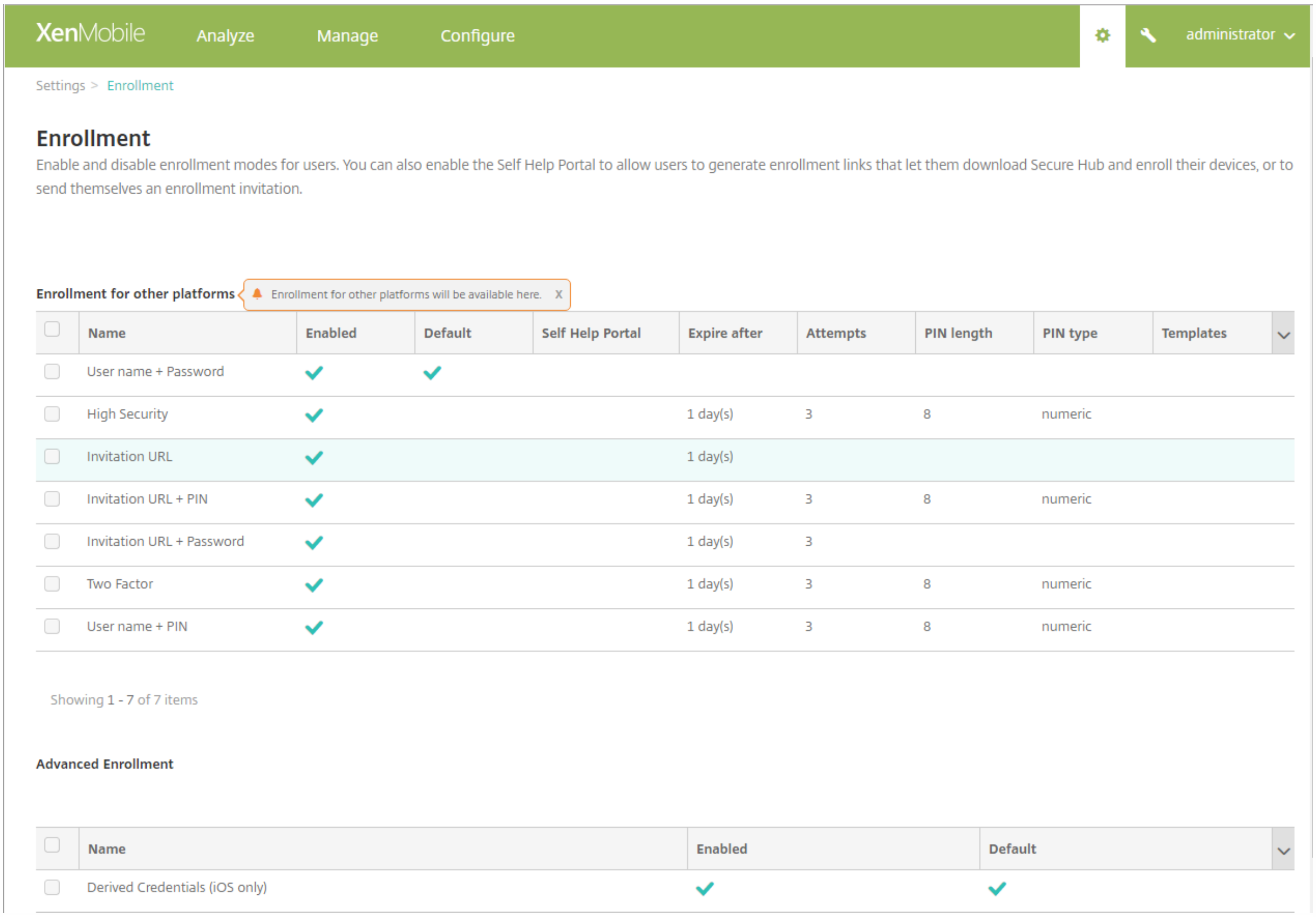


Enabling Derived Credentials

To enable the derived credentials provider you configured, configure it under Settings > Enrollment.

- 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**.

8. To enable derived credentials for enrollment: On the **Settings > Enrollment** page, under **Advanced Enrollment**, select **Derived Credentials (iOS only)** and then click **Enable**.



Settings > Enrollment

Enrollment

Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Secure Hub and enroll their devices, or to send themselves an enrollment invitation.

Enrollment for other platforms Enrollment for other platforms will be available here. X

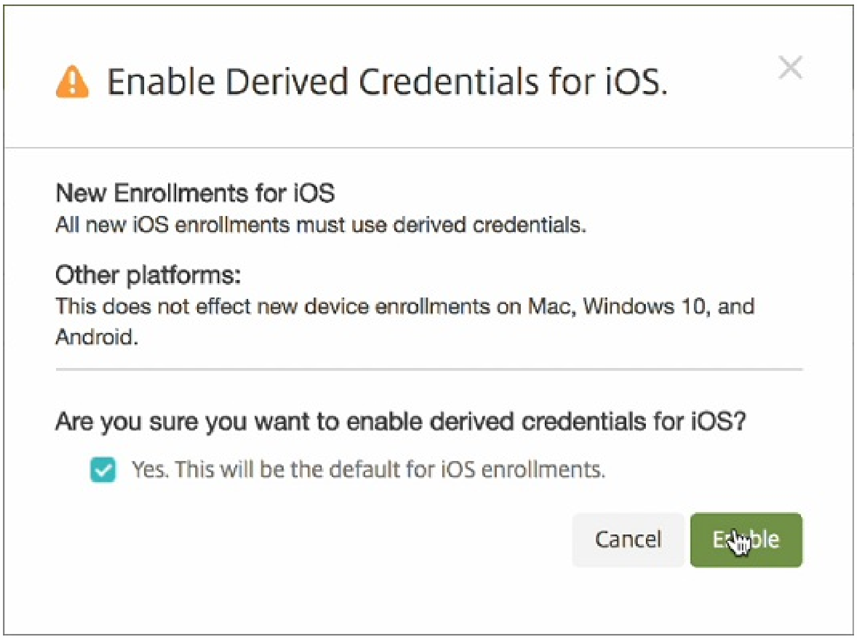
□	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates
□	User name + Password	✓	✓						
□	High Security	✓			1 day(s)	3	8	numeric	
□	Invitation URL	✓			1 day(s)				
□	Invitation URL + PIN	✓			1 day(s)	3	8	numeric	
□	Invitation URL + Password	✓			1 day(s)	3			
□	Two Factor	✓			1 day(s)	3	8	numeric	
□	User name + PIN	✓			1 day(s)	3	8	numeric	

Showing 1 - 7 of 7 items

Advanced Enrollment

□	Name	Enabled	Default
□	Derived Credentials (iOS only)	✓	✓

9. A confirmation dialog box appears. To enable derived credentials, select the check box, and click **Enable**.



Enable Derived Credentials for iOS.

New Enrollments for iOS
All new iOS enrollments must use derived credentials.

Other platforms:
This does not effect new device enrollments on Mac, Windows 10, and Android.

Are you sure you want to enable derived credentials for iOS?

☑ Yes. This will be the default for iOS enrollments.

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**.

For enrollment steps when using derived credentials, see iOS devices using derived credentials.

Log messages for derived credentials

Log messages during Secure Hub communication with XenMobile Server indicate success or failure, as follows.

Messages from XenMobile Server (SessionCreate SUCCESS)

```
2017-05-11T23:23:28.537+0000 | D88973753C718B23  |  INFO | http-nio-10080-exec-47 |
com.sparus.nps.ios.agent.V9AgentUtils | Derived Credential: User extracted from certificate: XXXXXXX@XMTEST.NET

2017-05-11T23:23:28.728+0000 | D88973753C718B23  |  INFO | http-nio-10080-exec-47 |
com.sparus.nps.ios.agent.V9AgentUtils | Derived Credential: Using user XXXXXX@XMTEST.NET' from cert and converted to
XXXXXXX with certid 60000001a95b7fecbbbf2821dd0000000001a9

2017-05-11T23:23:28.883+0000 | D88973753C718B23  |  INFO | http-nio-10080-exec-47 |
com.citrix.cg.bo.spring.impl.InternalUserServiceImpl | Input params for addUser. UserName XXXXXXX@auster.ctx' and
Domain Name 'auster.ctx'

2017-05-11T23:23:29.94+0000 | D88973753C718B23  |  INFO | http-nio-10080-exec-47 |
com.citrix.xms.oca.imil.service.impl.GroupServiceImpl | No.of groups:0 retrieved by UserID:40

2017-05-11T23:23:29.95+0000 | D88973753C718B23  |  WARN | http-nio-10080-exec-47 |
com.sparus.nps.ldap.LdapCredentialHandlerImpl | No groups found for user XXXXXX@auster.ctx'

2017-05-11T23:23:34.244+0000 | 21829910a6438ef5  |  INFO | http-nio-10080-exec-60 |
com.sparus.nps.ios.agent.V7ContextBuilder | No matching identity found in request from 172.16.1.57 to
/zdm/ios/agent;jsessionid=D88973753C718B23ADDEA26B46E5FBB2

2017-05-11T23:23:59.118+0000 | 21829910a6438ef5  |  INFO | http-nio-10080-exec-52 |
com.sparus.nps.ios.enroll.ProfileServiceServlet | New enrollment initiated for serialNumber=CCQLQNKPFMJF, imei=null,
udid=4a621749b64f7d915849ebcef3ded9cf7f460406, meid=null
```

Messages from XenMobile Server (SessionCreate FAIL)

```
2017-05-11T23:06:46.168+0000 | 40DA582380D50C72  |  INFO | http-nio-10080-exec-42 |
com.sparus.nps.ios.agent.V9AgentUtils | Derived Credential: User extracted from certificate: XXXXXXXX@XMTEST.NET

2017-05-11T23:06:46.233+0000 | 40DA582380D50C72  |  WARN | http-nio-10080-exec-42 | com.citrix.cg.util.CGUtil | No
default Domain found redirecting to 'local' domain.

2017-05-11T23:06:46.253+0000 | 40DA582380D50C72  |  WARN | http-nio-10080-exec-42 | com.citrix.cg.util.CGUtil |
local domain. Directory service not managed for IDP local
```

```
2017-05-11T23:06:46.253+0000 | 40DA582380D50C72  | ERROR | http-nio-10080-exec-42 |
com.sparus.nps.ios.agent.V9AgentUtils | dc ecxeption

com.citrix.xms.oca.imil.exception.OperationFailedException: Could not log on. Incorrect user name or password
```

Messages from Secure Hub (SessionCreate SUCCESS)

```
start request with id 6 and value (redacted) https://*****/zdm/ios/agent?action=sessioncreate&h=dc

Handling the client cert challenge for h=dc

Cred length is 3405

Passing the credentials in DC client cert challenge

Credentials parsed successfully

received challenge NSURLAuthenticationMethodServerTrust

request with id 6 succeeded with httpResponse code 200
```

Messages from Secure Hub (SessionCreate FAIL)

```
start request with id 6 and value (redacted) https://*****/zdm/ios/agent?action=sessioncreate&h=dc

Handling the client cert challenge for h=dc

Item found.

Cred length is 3434

Passing the credentials in DC client cert challenge

Credentials parsed successfully

request with id 6 failed with httpResponse code 500
```

Messages related to NetScaler

```
User is enrolled with Derived Credential and transientCredential is NOT nil. //Derived credential certificate is passed to NetScaler.

User is enrolled with Derived Credential and transientCredential is nil. ////Derived credential certificate isn't found and isn't passed to NetScaler.

User is enrolled with Derived Credential and the certificate has expired. Displaying message to the user to renew the certificate.
```

Upgrade

Nov 29, 2017

Important

Before you upgrade to XenMobile 10.7 (on-premises)

1. If the virtual machine running the XenMobile Server to be upgraded has less than 4 GB of RAM, increase the RAM to at least 4 GB. Keep in mind that the recommended minimum RAM is 8 GB for production environments.
2. For upgrades from XenMobile 10.4 or earlier: Make a note about your configurations for the Passcode and Restrictions device policies for Windows tablets. Those policies are no longer based on WMI. As a result, the upgrade removes the existing configurations. After the upgrade, reconfigure the Passcode and Restrictions device policies for Windows tablets.
3. If you have the deprecated Enterprise Data Protection device policy configured, delete the policy before upgrading.
4. Recommendation: Before you install a XenMobile update, use the functionality in your VM to take a snapshot of your system. Also, back up your system configuration database. If you experience issues during an upgrade, complete backups enable you to recover.

After you upgrade to XenMobile 10.7 (on-premises)

- If functionality involving outgoing connections stop working, and you haven't changed your connections configuration, check the XenMobile Server log for errors such as the following: “Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer”

  The certificate validation error indicates that you need to disable hostname verification on XenMobile Server. By default, hostname verification is enabled on outgoing connections except for the Microsoft PKI server. If hostname verification breaks your deployment, change the server property **disable.hostname.verification** to **true**. The default value of this property is **false**.

Citrix publishes new versions or important updates of XenMobile to Citrix.com. At the same time, a notice is sent to the contact on record for each customer.

You have these options for upgrading XenMobile:

- **To upgrade from XenMobile 10.6 or 10.5 to XenMobile 10.7**. Use the **Release Management** page in the XenMobile console. You do not use the Upgrade Tool to upgrade XenMobile 10 installations.
- **To upgrade from XenMobile 10.4 to XenMobile 10.7.** Use the **Release Management** page in the XenMobile console to upgrade in the following sequence. You do not use the Upgrade Tool for these installations.
  - Upgrade from XenMobile 10.4 to XenMobile 10.6.
  - Upgrade from XenMobile 10.6 to XenMobile 10.7.
- **To upgrade from XenMobile 10.3.6 to XenMobile 10.7**. Use the **Release Management** page in the XenMobile console to upgrade in the following sequence. You do not use the Upgrade Tool for these installations.
  - Upgrade from XenMobile 10.3.6 to XenMobile 10.5.
  - Upgrade from XenMobile 10.5 to XenMobile 10.7.
- **To upgrade from XenMobile 10 or 10.1 to XenMobile 10.7**. Use the **Release Management** page in the XenMobile console to upgrade in the following sequence. You do not use the Upgrade Tool for these installations.
  - Upgrade from XenMobile 10 or 10.1 to XenMobile 10.3.5.
  - Upgrade from XenMobile 10.3.5 to XenMobile 10.4.

  - Upgrade from XenMobile 10.4 to XenMobile 10.6.
  - Upgrade from XenMobile 10.6 to XenMobile 10.7.
- **To upgrade from XenMobile 9.0 to the latest XenMobile release.**
  Use the XenMobile Upgrade Tool that is built in to XenMobile 10.6. Verify that your XenMobile 10.6 environment is working and then upgrade from XenMobile 10.6 to XenMobile 10.7. See the articles in this section for details. The Upgrade Tool supports all XenMobile 9 editions: MDM, App, and Enterprise.

This article details the versions to use for upgrades, how to use the **Release Management** page, and how to upgrade clustered XenMobile deployments. This article also describes how to upgrade from MDM to Enterprise Edition.

Current XenMobile Server version	Release number	Upgrade to	Release number	Upgrade path	Update location
XenMobile Server 9 with App Controller Rolling Patch 9 installed	9.0.0_97106	XenMobile Server 10.6	10.6.0	XenMobile Server 9 upgrade to XenMobile Server 10.6. Then, XenMobile Server 10.6 upgrade to XenMobile 10.7	Download the App Controller rolling patch prerequisite. • The Upgrade Tool for XenMobile 10.6 is built into XenMobile Server 10.6. • After upgrading to XenMobile Server 10.6, test the XenMobile 10.6 environment. Then, upgrade from XenMobile Server 10.6 to XenMobile Server 10.7. • For more information, see Upgrade Tool prerequisites.
XenMobile Server 10 or XenMobile 10.1	10.1.0.63030	XenMobile Server 10.3.5	10.3.5	XenMobile 10 or XenMobile 10.1 upgrade to XenMobile 10.3.5	Download
XenMobile Server 10.3.5	10.3.5	XenMobile Server 10.4	10.4.0.116	XenMobile 10.3.5 upgrade to XenMobile 10.4	Download
XenMobile Server 10.4	10.4.0.116	XenMobile Server 10.6	10.6.0	XenMobile 10.4 upgrade to XenMobile 10.6	Download
XenMobile Server 10.5	10.5.x	XenMobile Server 10.7	10.7.0	XenMobile 10.5 upgrade to XenMobile 10.7	Download
XenMobile Server 10.6	10.6.x	XenMobile Server 10.7	10.7.0	XenMobile 10.6 upgrade to XenMobile 10.7	Download

Use the **Release Management** page to upgrade from supported XenMobile 10 versions (indicated in the preceding table) to the latest version of XenMobile Server.

Prerequisites:

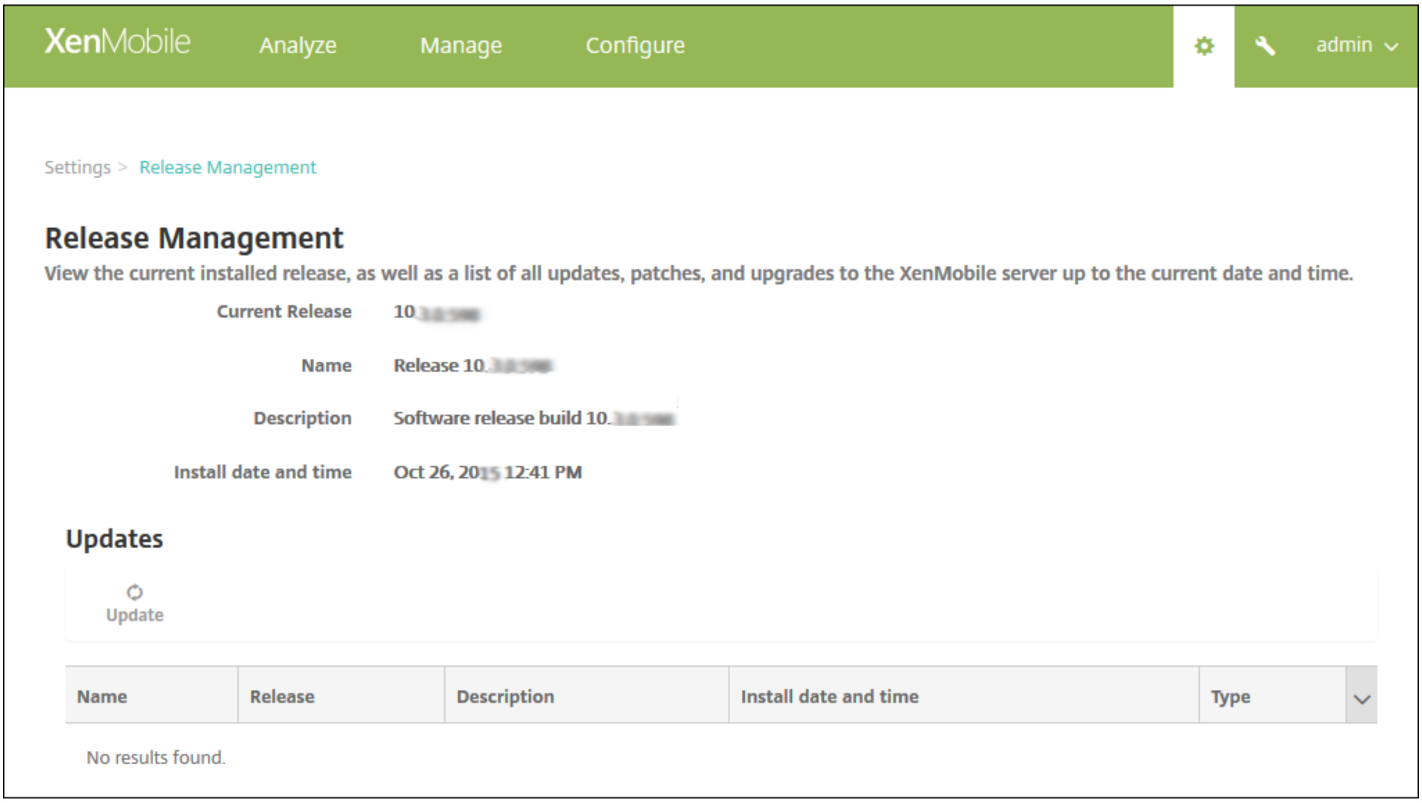
- Review the System Requirements.

If you have a clustered deployment, see the instructions at the end of this article.

1. Log on to your account on the Citrix website and download the XenMobile Upgrade (.bin) file to an appropriate location.

2. In the XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.

3. Click **Release Management**. The **Release Management** page appears.



Release Management

View the current installed release, as well as a list of all updates, patches, and upgrades to the XenMobile server up to the current date and time.

Current Release: 10.[redacted]

Name: Release 10.[redacted]

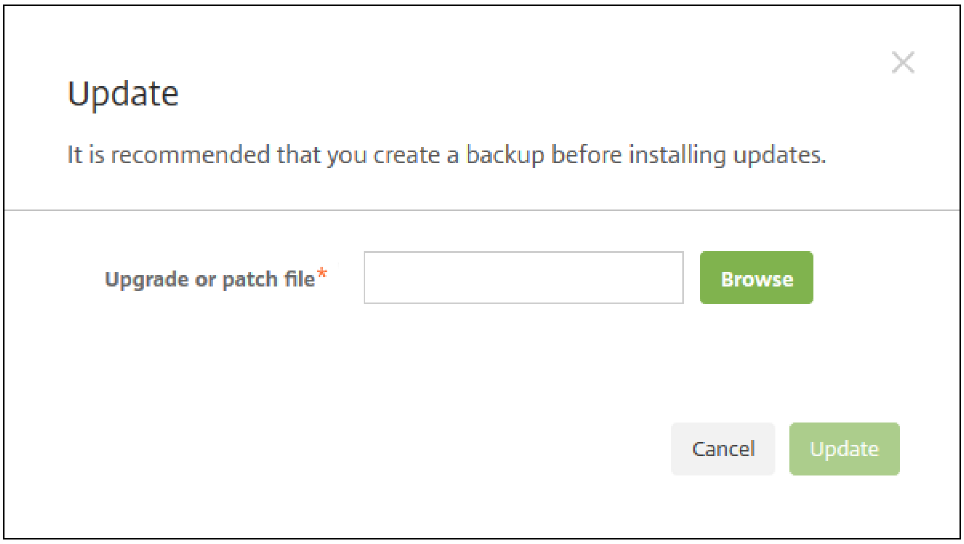
Description: Software release build 10.[redacted]

Install date and time: Oct 26, 20[redacted] 12:41 PM

Updates

Name	Release	Description	Install date and time	Type
No results found.				

4. Under **Updates**, click **Update**. The **Update** dialog box appears.


Update

It is recommended that you create a backup before installing updates.

5. Select the XenMobile upgrade file you downloaded from Citrix.com by clicking **Browse** and navigating to the file location.

6. Click **Update** and then if prompted, restart XenMobile.

If for some reason the update cannot be completed successfully, an error message appears indicating the problem. The system is reverted to its state previous to the update attempt.

Note: After an upgrade, XenMobile requires a restart. Use the XenMobile CLI to restart XenMobile Server. It's important that you clear your browser cache after the system restarts.

Important

Before you install a XenMobile update, use the functionality in your virtual machine (VM) to take a snapshot of your system. Also, back up your system configuration database. If you experience issues during an upgrade, complete backups enable you to recover.

If your system is configured in cluster mode, follow these steps to update each node from a XenMobile 10 release:

1. Upload the .bin file on all nodes from **Settings > Release Management**.

2. Shut down all the nodes from the **System Menu** in the CLI.

3. Bring up one node, from the **System Menu** in the CLI, and check that the service is running.

4. Bring up other nodes one after the other.

If XenMobile can't complete the update successfully, an error message appears indicating the problem. XenMobile then reverts the system to its state previous to the update attempt.

You can upgrade XenMobile 10 MDM Edition to XenMobile 10 Enterprise Edition for iOS and Android devices.

Prerequisites:

- The correct Enterprise license.
- NetScaler Gateway is configured.

To upgrade:

1. Go to **Settings** > **Licensing** and verify that the correct Enterprise Edition license type is uploaded.
2. Go to **Settings** > **Server Properties** and change the **Server Mode** property from **MDM** to **ENT**.
3. Go to **Settings** > **Netscaler Gateway** and configure the NetScaler Gateway details. Set the authentication mode to the same as the MDM Edition, that is, domain (Active Directory) authentication. XenMobile doesn't support changing the authentication mode after user enrollment.
4. Optional: Go to **Settings** > **Client Properties** and enable Citrix PIN authentication.

After you complete those steps, users must perform the following steps to switch a device into Enterprise mode.

iOS users:

1. Close Secure Hub: Tap the device home button twice (quickly) and slide up the Secure Hub app.
2. Open Secure Hub.

Android users:

1. Open Secure Hub.
2. Go to **Preferences** > **Device Information**.
3. Click **Refresh Policy**.

If you enabled Citrix PIN authentication, Secure Hub prompts users to create a PIN. After a user creates a PIN, XenMobile configures the device in Enterprise mode. In the XenMobile console, the **Manage** > **Devices** page then shows both MDM and MAM as active for the device.

Upgrade Tool prerequisites

Sep 06, 2017

> ## Note
>
> XenMobile 9 reached the End of Life (EOL) lifecycle status as of June 30, 2017. When a product release reaches EOL, you can use the product within the terms of your product licensing agreement, but the available support options are limited. Historical information appears in the Knowledge Center or other online resources. The documentation is no longer updated and is provided on an as-is basis. For more information about product lifecycle milestones, see the Product Matrix.
>
> For five years beyond the EOL date, you can download a PDF of the XenMobile 9 documentation from the Archive List of Legacy Documents.
>
> For more information about moving from XenMobile 9 to XenMobile 10.6 or earlier, or to XenMobile Service via Citrix Cloud, see this Citrix.com page.

To upgrade from XenMobile 9.0 to XenMobile 10.6, you use the XenMobile built-in Upgrade Tool.

The Upgrade Tool supports:

- iOS and Android devices enrolled in all XenMobile Server Modes (ENT, MAM, MDM)
- Windows phones and tablets enrolled in MDM mode
- Windows phones enrolled in Enterprise mode
- Windows CE devices in MDM mode

If Multi-Tenant Console (MTC) is enabled on XenMobile 9.0, you can migrate MTC to a stand-alone deployment of the latest version of XenMobile. XenMobile 10 does not support MTC, so you must manage these upgraded instances on an individual basis. After you complete the prerequisites in this article, see Upgrade the MTC tenant server to XenMobile.

The latest version of XenMobile supports NetScaler Gateway versions 12.0, 11.1.x, 11.0.x, and 10.5.x.

The Upgrade Tool built in to XenMobile also supports NetScaler Gateway version 10.1.x. Citrix doesn't support NetScaler Gateway 10.1 for use with the latest version of XenMobile. However, you can upgrade a NetScaler Gateway 10.1 deployment using the Upgrade Tool built in to XenMobile. After that, Citrix recommends that you upgrade NetScaler Gateway to the latest supported version.

> ## Important
>
> The upgrade process is complex. Before starting an upgrade, be sure to review the Known issues, plan your upgrade, and complete all prerequisites, as described in this article. In addition, this blog includes prerequisite checklists that can help you plan your upgrade.
>
> After you run the Upgrade Tool, be sure you complete all post-requisites.
>
> If you don't complete a prerequisite, the upgrade can fail. You must then configure a new instance of the latest version of XenMobile in the command-line console and start the Upgrade Tool again.

Citrix recommends that you upgrade in the following stages.

1. Do a test drive in a staging environment, completing all prerequisite and Upgrade Tool steps. Citrix recommends that you do an upgrade test drive first to get a feel for how the process works and what you can expect to see after you do a full production upgrade. A test drive upgrade tests the upgrade of your configuration data, not user data.

In NetScaler (minimum version NetScaler 10.5), Citrix recommends that you use the NetScaler for XenMobile Wizard to set up a fresh NetScaler with NetScaler Gateway and NetScaler load balancing virtual servers.

2. Verify that the test drive correctly upgraded your configuration data, such as LDAP, policies, and apps. Verify test devices.

3. Do a production upgrade in your production environment and go live. Plan for downtime while running the upgrade.

About test drives and production upgrades

With the XenMobile Upgrade Tool, you first test the ugprade and then perform the full production upgrade.

When you choose Test Drive:
The Upgrade Tool does an upgrade test drive with production configuration data to compare XenMobile 9.0 and the latest version of XenMobile without affecting your production environment. The test drive upgrade tests only configuration data; it does not test device data (in the case of XenMobile Enterprise Edition deployments) or user data.

The results of an upgrade test drive are for testing only. You cannot upgrade a test drive deployment. Instead, you must begin again for a production upgrade. An upgrade test drive works with any XenMobile 9.0 edition.

When you choose Upgrade:
The Upgrade Tool at first copies all configuration, device, and user data from XenMobile 9.0 to a new instance of the latest version of XenMobile with the same fully qualified domain name (FQDN). Everything in XenMobile 9.0 remains intact until you move the new XenMobile server instance into production.

When you log on to the console for the new XenMobile server instance after the upgrade, you see all the user and device data that the upgrade moved from XenMobile 9.0.

What the Upgrade Tool does not do

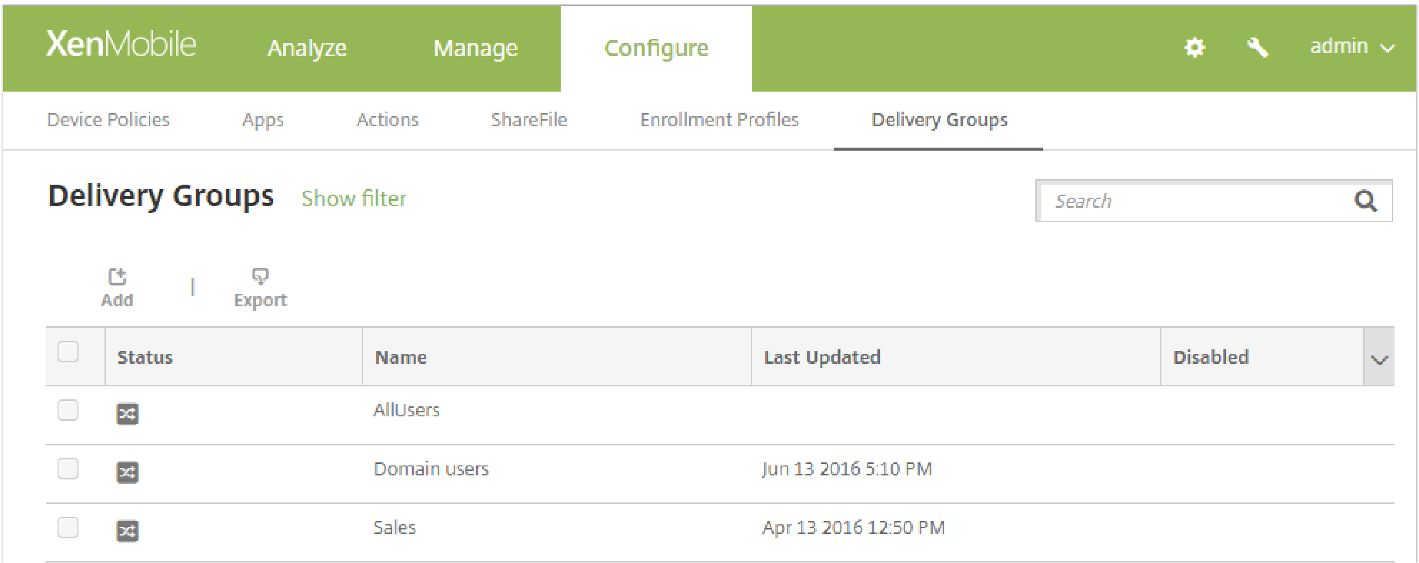
The following information isn't upgraded to the latest version of XenMobile when you use the Upgrade Tool:

- Licensing information.
- Reports data.
- Server group policies and associated deployments (not supported in the latest version of XenMobile).
- Managed Service Provider (MSP) group.
- Policies and packages related to Windows 8.0.
- Deployment packages not in use; for example, when no users or groups are assigned to a deployment package.
- Any other configuration or user data as described in the upgrade log file.
- CXM Web (replaced by Citrix Secure Web).
- DLP policies (replaced by Citrix Sharefile).
- Custom Active Directory attributes.
- If you have configured multiple branding policies in XenMobile 9.0, the branding policy is not upgraded. Later versions of XenMobile support one branding policy; you have to leave one branding policy in XenMobile 9.0 to successfully upgrade to the latest version of XenMobile.

- Any settings in the auth.jsp file in XenMobile 9.0 that are used to restrict access to the console. Console access restrictions in the latest version of XenMobile are firewall settings that you can configure in the command-line interface.
- Sys log server configurations.
- Form-fill connectors configured on XenMobile 9.0 (not supported in later versions of XenMobile).

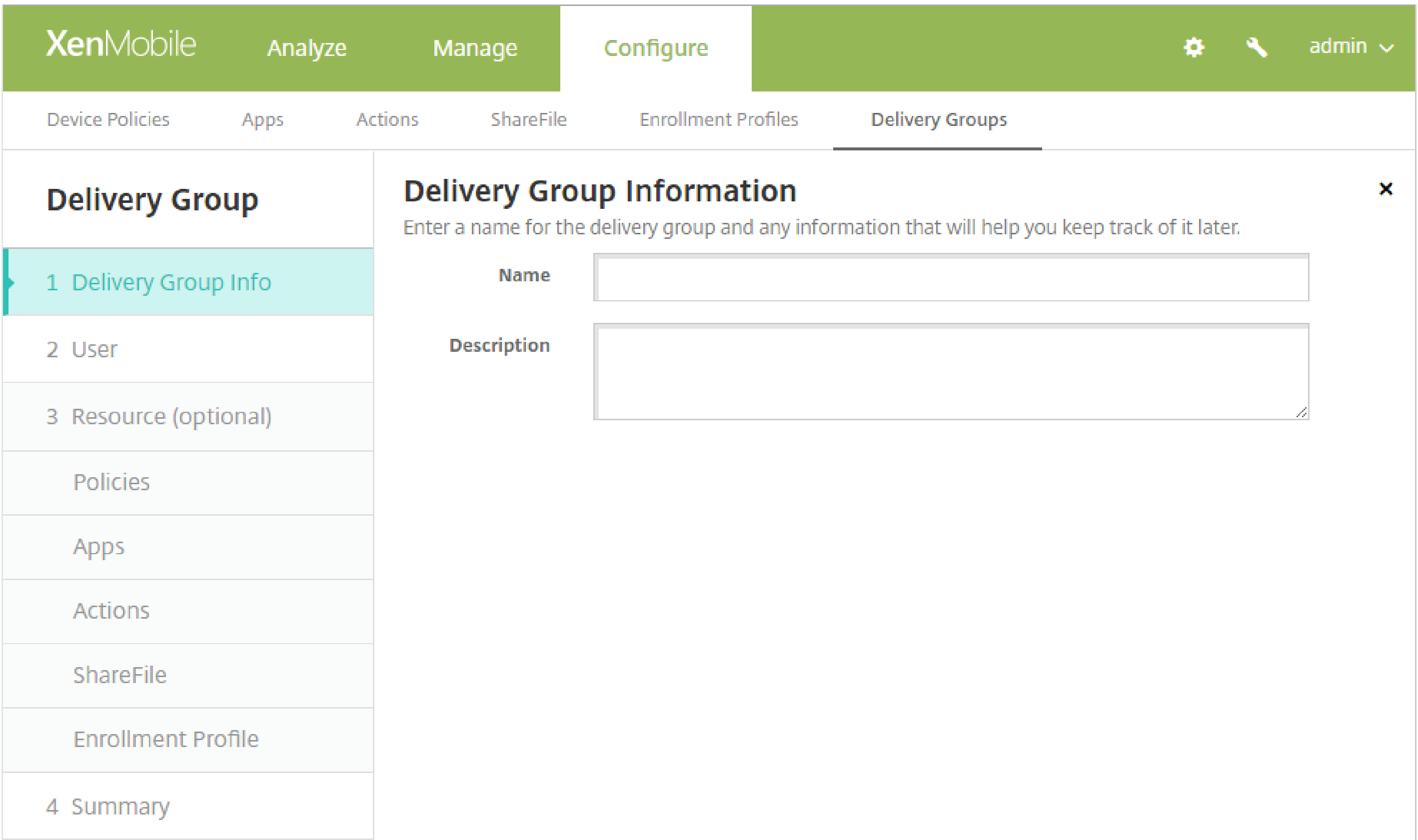
XenMobile changes

- The Upgrade Tool doesn't upgrade Active Directory users who are assigned to local groups. You can subsequently assign Active Directory users to local groups.
- XenMobile 10 doesn't support nested local groups. An upgrade from XenMobile 9 flattens the local groups hierarchy.
- Deployment packages in Device Manager are referred to as delivery groups in XenMobile, as shown in the following figure. For more information, see Deploy resources.



	Status	Name	Last Updated	Disabled
□		AllUsers		
□		Domain users	Jun 13 2016 5:10 PM	
□		Sales	Apr 13 2016 12:50 PM	

Inside the delivery group, you can view the policies, actions, and apps required for the group of users who require the resources.



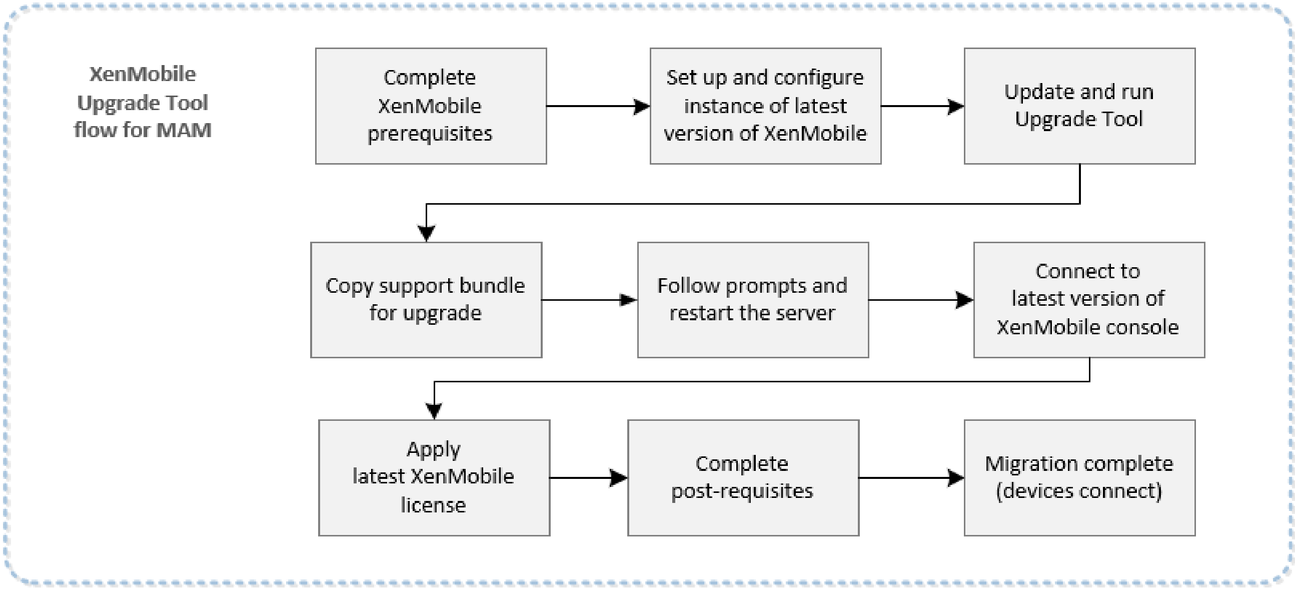
Delivery Group Information

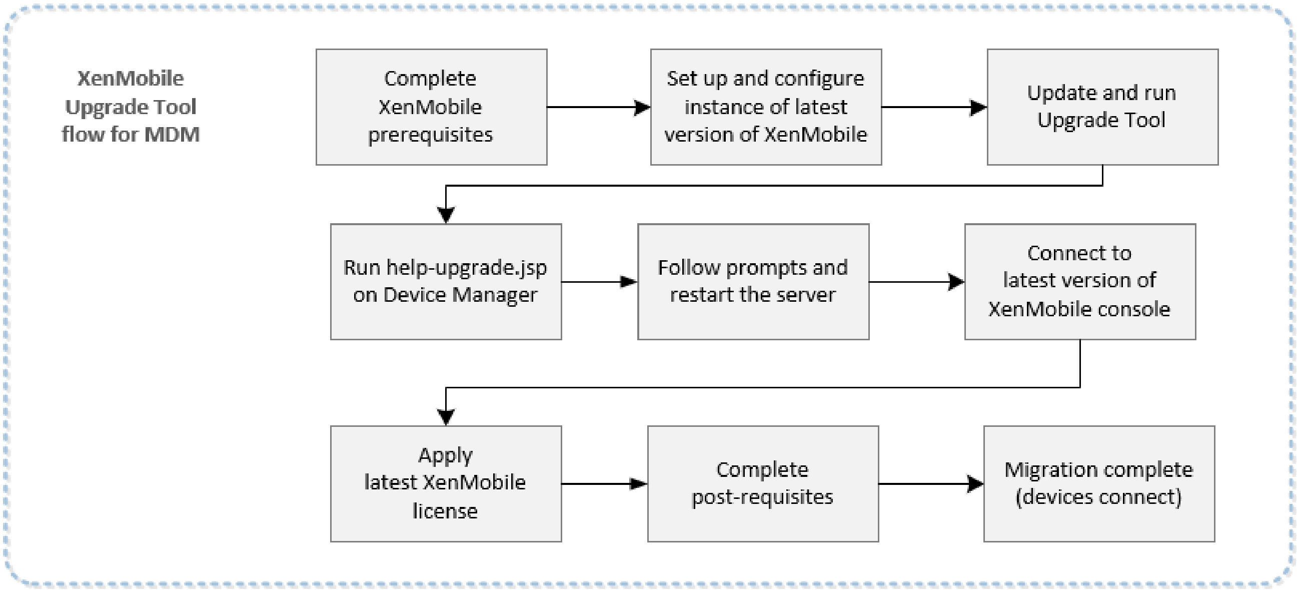
Enter a name for the delivery group and any information that will help you keep track of it later.

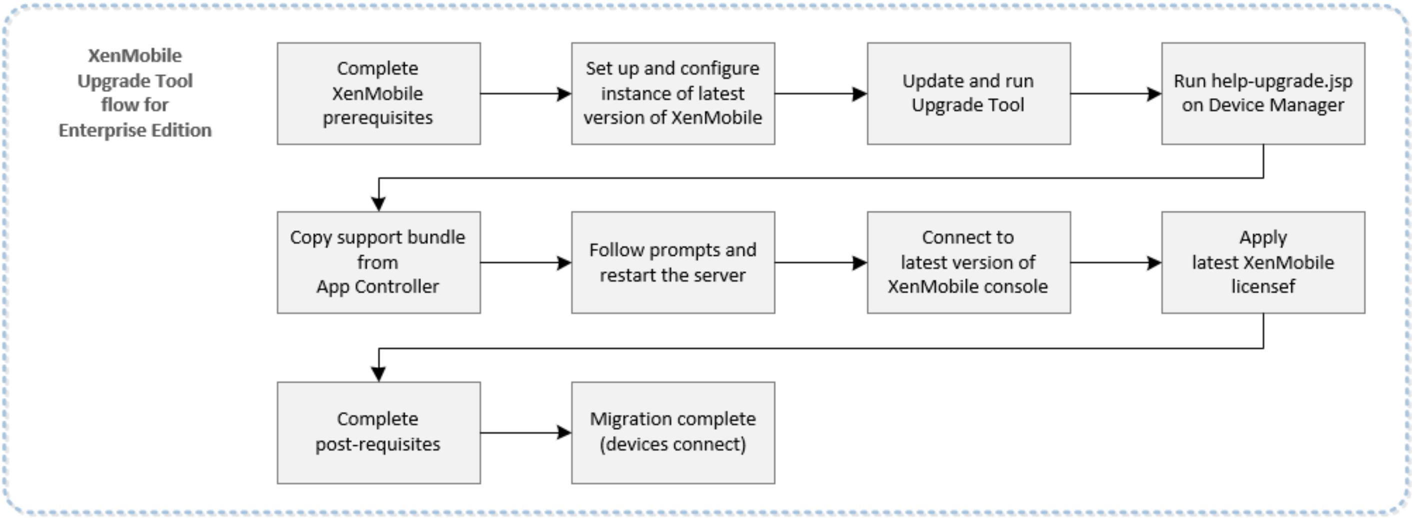
Name

Description

The following figures illustrate the basic steps you take to upgrade from XenMobile 9.0.


XenMobile Upgrade Tool flow for MAM
Complete XenMobile prerequisites
Set up and configure instance of latest version of XenMobile
Update and run Upgrade Tool
Copy support bundle for upgrade
Follow prompts and restart the server
Connect to latest version of XenMobile console
Apply latest XenMobile license
Complete post-requisites
Migration complete (devices connect)


XenMobile Upgrade Tool flow for MDM
Complete XenMobile prerequisites
Set up and configure instance of latest version of XenMobile
Update and run Upgrade Tool
Run help-upgrade.jsp on Device Manager
Follow prompts and restart the server
Connect to latest version of XenMobile console
Apply latest XenMobile license
Complete post-requisites
Migration complete (devices connect)


XenMobile Upgrade Tool flow for Enterprise Edition
Complete XenMobile prerequisites
Set up and configure instance of latest version of XenMobile
Update and run Upgrade Tool
Run help-upgrade.jsp on Device Manager
Copy support bundle from App Controller
Follow prompts and restart the server
Connect to latest version of XenMobile console
Apply latest XenMobile licensef
Complete post-requisites
Migration complete (devices connect)

Citrix recommends the following steps for upgrading a XenMobile 9.0 Enterprise environment, with Windows Phones enrolled in Enterprise mode and using Worx Home 9.x, to the latest version of XenMobile.

1. Upgrade Worx Home on Device Manager to Worx Home 10.2 or later and then deploy Worx Home 10.2.

2. Manually uninstall Worx Home 9.x from user devices.

3. Instruct users to go to the Download Hub on their phone to install Worx Home 10.2 or later, which you deployed from Device Manager.

4. After you complete the prerequisites described in this article, upgrade to the latest version of XenMobile as described in Enable and run the XenMobile Upgrade Tool.

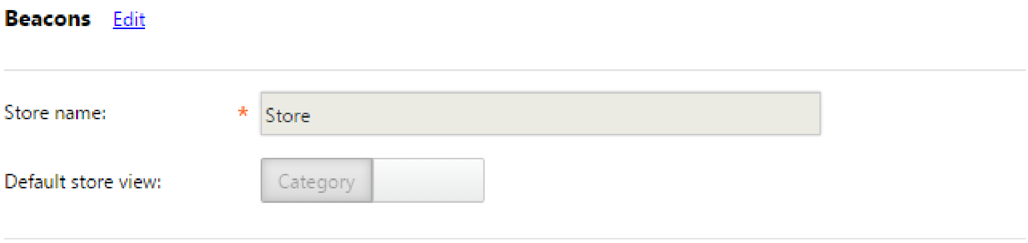
5. Make NetScaler changes for devices to connect back, as described in Upgrade Tool post-requisites.

Download XenMobile 9.0 App Controller Rolling Patch 9 from https://support.citrix.com/article/CTX218552.

In the App Controller management console, go to **Settings > Release Management**. Click **Update** and then select the patch file you downloaded. Click **Upload** and then restart App Controller.

Before you upgrade XenMobile 9 to the latest version of XenMobile, you must change a custom store name back to its default value so that enrolled Windows devices continue to work after the upgrade. For more information, see http://support.citrix.com/article/CTX214553.

In a MAM or Enterprise mode upgrade, if the store name has been changed to from the default Store on App Controller, restore the name back to the default setting of **Store** before generating a support bundle for the upgrade.



Beacons Edit

Store name: * Store

Default store view: Category

For the required versions of related components such as Citrix License Server, see System requirements and its sub-articles.

- **NetScaler**: Before you upgrade NetScaler, be sure to save a copy of your Netscaler configuration file (ns.conf). Current Netscaler releases include an easy-to-use quick deployment utility, the NetScaler for XenMobile wizard, that guides you through the steps to integrate NetScaler and XenMobile. For more information, see Configuring Settings for Your XenMobile Environment and FAQ: XenMobile 10 and NetScaler 10.5 Integration.
- **Firewall Ports**: Open firewall ports for the new XenMobile Server IP similar to the ports opened for the XenMobile 9.0 IP server. For XenMobile port requirements, see Port requirements.
- **LDAP Server**: Make sure that the new XenMobile Server connects to one or more LDAP servers. You must have an active route to LDAP servers after you upgrade, when you restart the server.

To migrate using an existing database, the database service account password in the old and new infrastructures must match.

The following table lists the possible database migration options. For system requirements, see XenMobile Database Requirements.

From XenMobile 9.0	To the latest version of XenMobile
Enterprise Edition	

App Controller	MDM	
Local PostgreSQL	Local PostgreSQL	Local PostgreSQL
Local PostgreSQL	MS SQL	MS SQL
Local PostgreSQL	Remote PostgreSQL	Remote PostgreSQL
App Edition		
Local PostgreSQL		Local PostgreSQL
Local PostgreSQL		Remote PostgreSQL
Local PostgreSQL		MS SQL
MDM Edition		
Local PostgreSQL		Local PostgreSQL
MS SQL		MS SQL
Remote PostgreSQL		Remote PostgreSQL

During the database migration process, XenMobile needs the ability to access the database solution implemented on XenMobile 9.0 Device Manager. For example, the following ports must be open:

- For Microsoft SQL Server, the default port is 1433.
- For PostgreSQL, the default port is 5432.

To allow remote connections to PostgreSQL, you must complete the following steps:

1. Open the file pg_hba.conf and then locate the following line:

```
host all all 127.0.0.1/32 md5
```

2. To allow all IP addresses, change the line to:

```
host all all 0.0.0.0/0 md5
```

Alternatively, add another host entry to allow connections to the XenMobile server IP address:

```
host all all 10.x.x.x/32 md5
```

3. Save the file.

4. Stop and start the service.

5. Open the postgresql.conf file and then locate the following line:

```
#listen_addresses = 'localhost'
```

6. Change the line to:

```
listen_addresses = '*'
```

7. Stop and start the PostgreSQL service to apply the changes.

If the database solution has a custom port assigned, you must ensure that the port is allowed and open in the firewall protecting XenMobile 9.0 Device Manager. Doing so enables the new instance of XenMobile to connect to the database and migrate the required information.

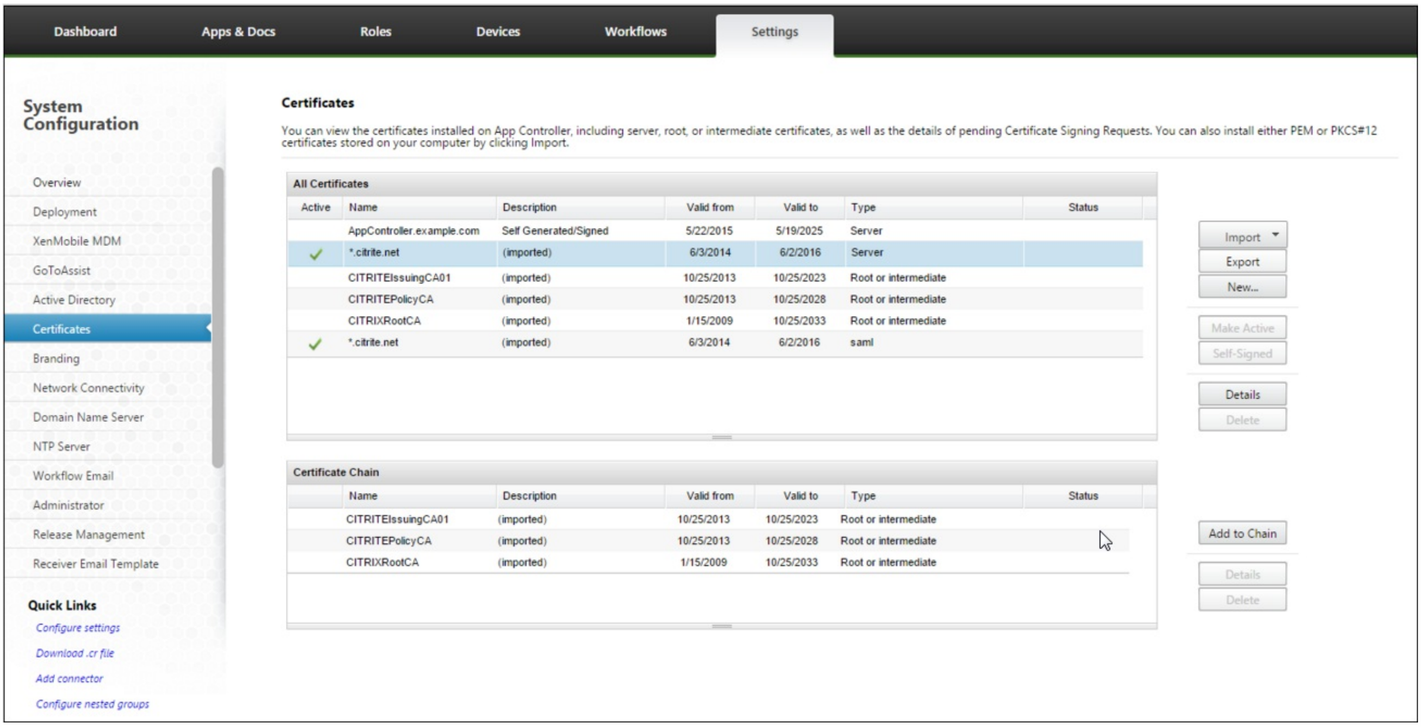
Deployment package names in XenMobile 9.0 that contain special characters (!, $, (), #, % , +, *, ~, ?, |, {}, and []) upgrade, however you can't edit the delivery groups in new instance of XenMobile after the upgrade. In addition, local users and local groups created in XenMobile 9.0 that contain an open square bracket ([) cause problems in new instance of XenMobile with creating enrollment invitations. Before an upgrade, remove all special characters from deployment package names as well as open square brackets from local user and local group names.

External SSL certificates must meet the conditions outlined in the Citrix Support article How to Configure an External SSL Certificate. Be sure to review your pki.xml before starting the upgrade to ensure that the SSL certificate meets those conditions.

If you are upgrading a XenMobile 9.0 Enterprise Edition deployment, you must export the App Controller server certificate. Later, when you are handling the upgrade post-requisites, you must import the server certificate into NetScaler Gateway. Follow these steps to export the server certificate:

1. Log on to the XenMobile 9.0 App Controller and click **Certificates**.

2. In the certificate list, click the server certificate you want to export and then click **Export**.



System Configuration

- Overview
- Deployment
- XenMobile MDM
- GoToAssist
- Active Directory
- Certificates
- Branding
- Network Connectivity
- Domain Name Server
- NTP Server
- Workflow Email
- Administrator
- Release Management
- Receiver Email Template

Quick Links

- *Configure settings*
- *Download .cr file*
- *Add connector*
- *Configure nested groups*

Certificates

You can view the certificates installed on App Controller, including server, root, or intermediate certificates, as well as the details of pending Certificate Signing Requests. You can also install either PEM or PKCS#12 certificates stored on your computer by clicking Import.

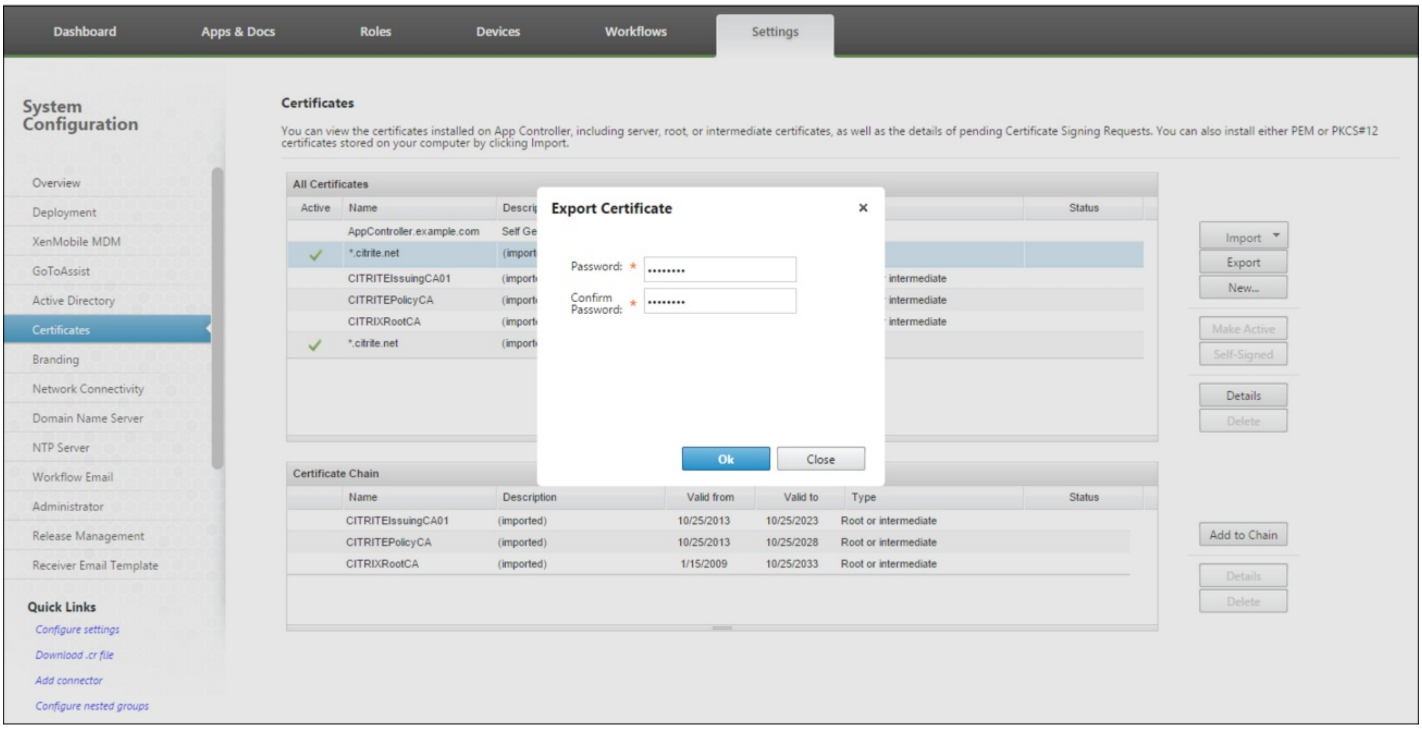
All Certificates

Active	Name	Description	Valid from	Valid to	Type	Status
	AppController.example.com	Self Generated/Signed	5/22/2015	5/19/2025	Server	
✓	*.citrite.net	(imported)	6/3/2014	6/2/2016	Server	
	CITRITEIssuingCA01	(imported)	10/25/2013	10/25/2023	Root or intermediate	
	CITRITEPolicyCA	(imported)	10/25/2013	10/25/2028	Root or intermediate	
	CITRIXRootCA	(imported)	1/15/2009	10/25/2033	Root or intermediate	
✓	*.citrite.net	(imported)	6/3/2014	6/2/2016	saml	

Certificate Chain

Name	Description	Valid from	Valid to	Type	Status
CITRITEIssuingCA01	(imported)	10/25/2013	10/25/2023	Root or intermediate	
CITRITEPolicyCA	(imported)	10/25/2013	10/25/2028	Root or intermediate	
CITRIXRootCA	(imported)	1/15/2009	10/25/2033	Root or intermediate	

3. In the **Export Certificate** dialog box, type your certificate password in both fields and then click **OK**.



System Configuration

- Overview
- Deployment
- XenMobile MDM
- GoToAssist
- Active Directory
- Certificates
- Branding
- Network Connectivity
- Domain Name Server
- NTP Server
- Workflow Email
- Administrator
- Release Management
- Receiver Email Template

Quick Links

- *Configure settings*
- *Download .cr file*
- *Add connector*
- *Configure nested groups*

Certificates

You can view the certificates installed on App Controller, including server, root, or intermediate certificates, as well as the details of pending Certificate Signing Requests. You can also install either PEM or PKCS#12 certificates stored on your computer by clicking Import.

All Certificates

Active	Name	Descri	Status
	AppController.example.com	Self Ge	
✓	*.citrite.net	(import	
	CITRITEIssuingCA01	(import intermediate	
	CITRITEPolicyCA	(import intermediate	
	CITRIXRootCA	(import intermediate	
✓	*.citrite.net	(import	

Export Certificate ×

Password: * ••••••••

Confirm Password: * ••••••••

Certificate Chain

Name	Description	Valid from	Valid to	Type	Status
CITRITEIssuingCA01	(imported)	10/25/2013	10/25/2023	Root or intermediate	
CITRITEPolicyCA	(imported)	10/25/2013	10/25/2028	Root or intermediate	
CITRIXRootCA	(imported)	1/15/2009	10/25/2033	Root or intermediate	

Prepare a server where you can upload the encrypted support bundle from the XenMobile command-line interface using either the File Transfer Protocol (FTP) or Secure Copy Protocol (SCP).

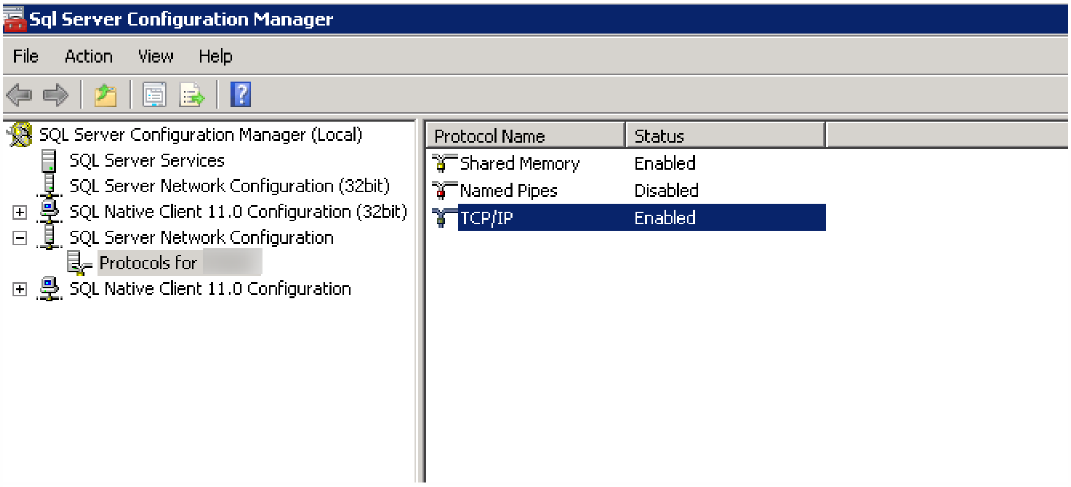
Enable and run the XenMobile Upgrade Tool

Sep 06, 2017

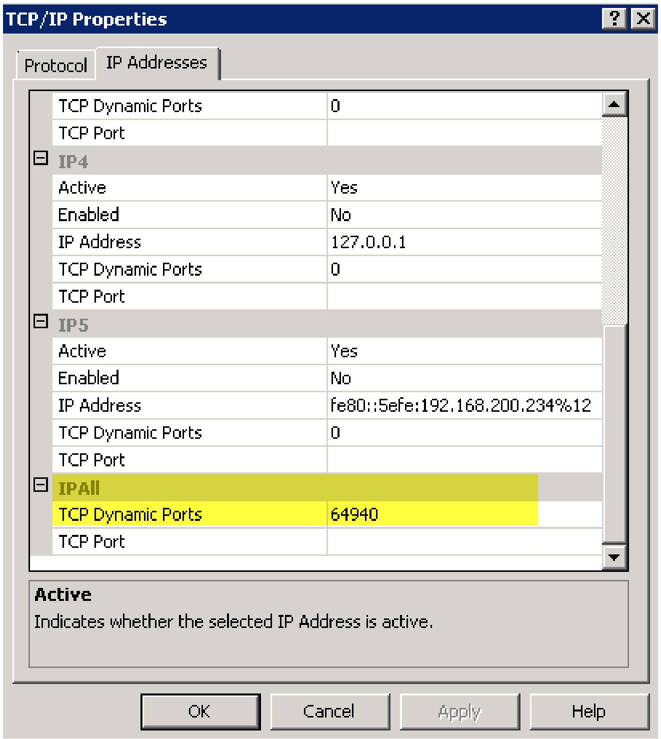
If your XenMobile 9 environment meets the following prerequisites, follow the steps in this section before proceeding with the upgrade.

- XenMobile 9 MDM Edition or Enterprise Edition has an external SQL Server database.
- SQL Server database runs on a non-default named instance.
- SQL Server named instance listens on a static or dynamic TCP port. You can confirm this prerequisite by looking at the IP addresses of the TCP/IP protocol of the named instance as shown in the following figures.

> ## Note
>
> Citrix recommends that the SQL server database instance always runs on a static port, because the XenMobile server needs continuing access to the database. This connection generally traverses through a firewall. As a result, you must open the appropriate port in the firewall. Therefore, ensure that the database instance is running on a static port.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 11.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for [redacted]
SQL Native Client 11.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled



TCP/IP Properties

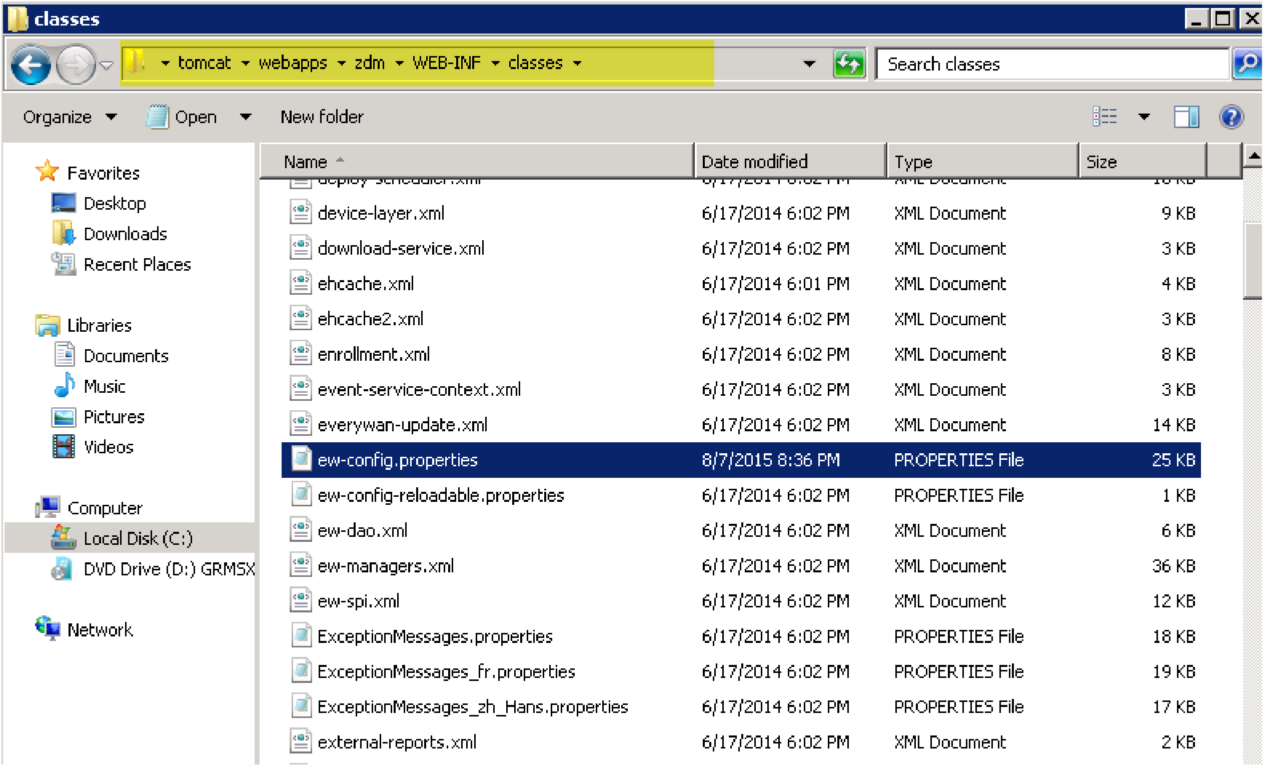
Protocol | IP Addresses

TCP Dynamic Ports	0
TCP Port	
IP4	
Active	Yes
Enabled	No
IP Address	127.0.0.1
TCP Dynamic Ports	0
TCP Port	
IP5	
Active	Yes
Enabled	No
IP Address	fe80::5efe:192.168.200.234%12
TCP Dynamic Ports	0
TCP Port	
IPAll	
TCP Dynamic Ports	64940
TCP Port	

Active
Indicates whether the selected IP Address is active.

Pre-upgrade steps

1. Go to the Device Manager installation directory and open the ew-config.properties file. This file is available in tomcat\webapps\zdm\WEB-INF\classes.



classes

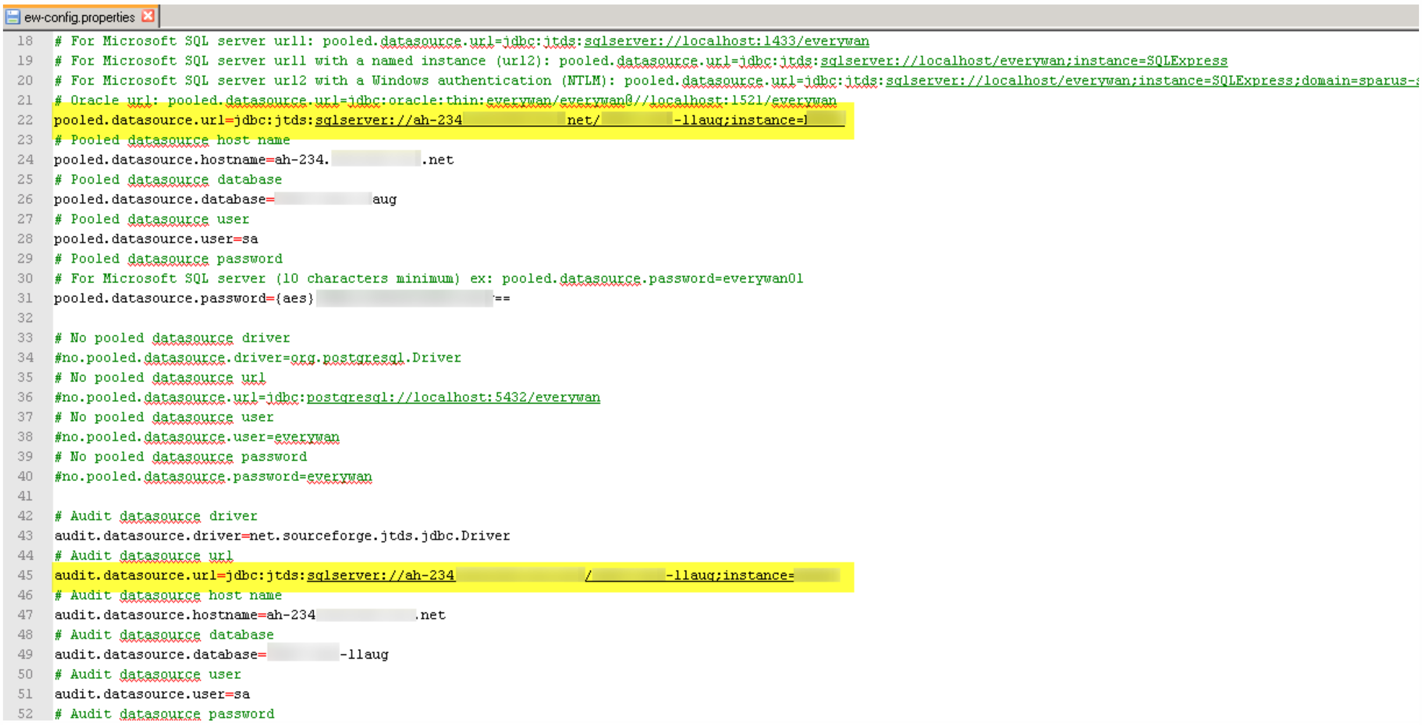
tomcat ▸ webapps ▸ zdm ▸ WEB-INF ▸ classes ▸

Name	Date modified	Type	Size
device-layer.xml	6/17/2014 6:02 PM	XML Document	9 KB
download-service.xml	6/17/2014 6:02 PM	XML Document	3 KB
ehcache.xml	6/17/2014 6:01 PM	XML Document	4 KB
ehcache2.xml	6/17/2014 6:02 PM	XML Document	3 KB
enrollment.xml	6/17/2014 6:02 PM	XML Document	8 KB
event-service-context.xml	6/17/2014 6:02 PM	XML Document	3 KB
everywan-update.xml	6/17/2014 6:02 PM	XML Document	14 KB
ew-config.properties	8/7/2015 8:36 PM	PROPERTIES File	25 KB
ew-config-reloadable.properties	6/17/2014 6:02 PM	PROPERTIES File	1 KB
ew-dao.xml	6/17/2014 6:02 PM	XML Document	6 KB
ew-managers.xml	6/17/2014 6:02 PM	XML Document	36 KB
ew-spi.xml	6/17/2014 6:02 PM	XML Document	12 KB
ExceptionMessages.properties	6/17/2014 6:02 PM	PROPERTIES File	18 KB
ExceptionMessages_fr.properties	6/17/2014 6:02 PM	PROPERTIES File	19 KB
ExceptionMessages_zh_Hans.properties	6/17/2014 6:02 PM	PROPERTIES File	17 KB
external-reports.xml	6/17/2014 6:02 PM	XML Document	2 KB

2. In the ew-config.properties file, search for the following URLs in the DATASOURCE Configuration section:

pooled.datasource.url= jdbc:jtds:sqlserver://<SQLserver_FQDN>/<DB_Name>;instance=<Instance_Name>

audit.datasource.url= jdbc:jtds:sqlserver://<SQLserver_FQDN>/<DB_Name>;instance=<Instance_Name>



```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-s
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234[redacted]net/[redacted]-1laug;instance=[redacted]
# Pooled datasource host name
pooled.datasource.hostname=ah-234.[redacted].net
# Pooled datasource database
pooled.datasource.database=[redacted]aug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}[redacted]==

# No pooled datasource driver
#no.pooled.datasource.driver=org.postgresql.Driver
# No pooled datasource url
#no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
# No pooled datasource user
#no.pooled.datasource.user=everywan
# No pooled datasource password
#no.pooled.datasource.password=everywan

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://ah-234[redacted]/[redacted]-1laug;instance=[redacted]
# Audit datasource host name
audit.datasource.hostname=ah-234[redacted].net
# Audit datasource database
audit.datasource.database=[redacted]-1laug
# Audit datasource user
audit.datasource.user=sa
# Audit datasource password
```

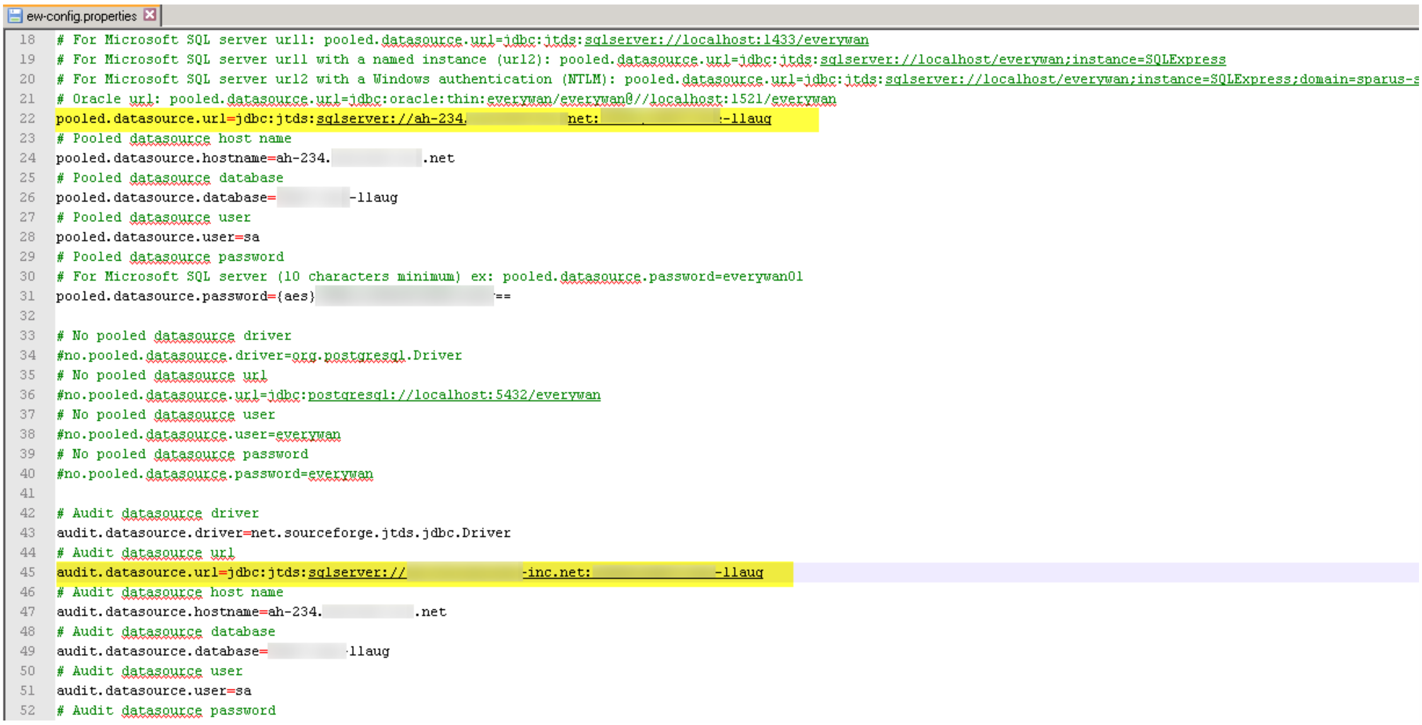
3. Remove the instance name in the preceding URLs, then add the port and SQL Server FQDN. In this case, 64940 is the required port.

pooled.datasource.url=jdbc:jtds:sqlserver:// <SQLserver_FQDN>:64940/<DB_Name>

audit.datasource.url=jdbc:jtds:sqlserver:// <SQLserver_FQDN>:64940/<DB_Name>

Note

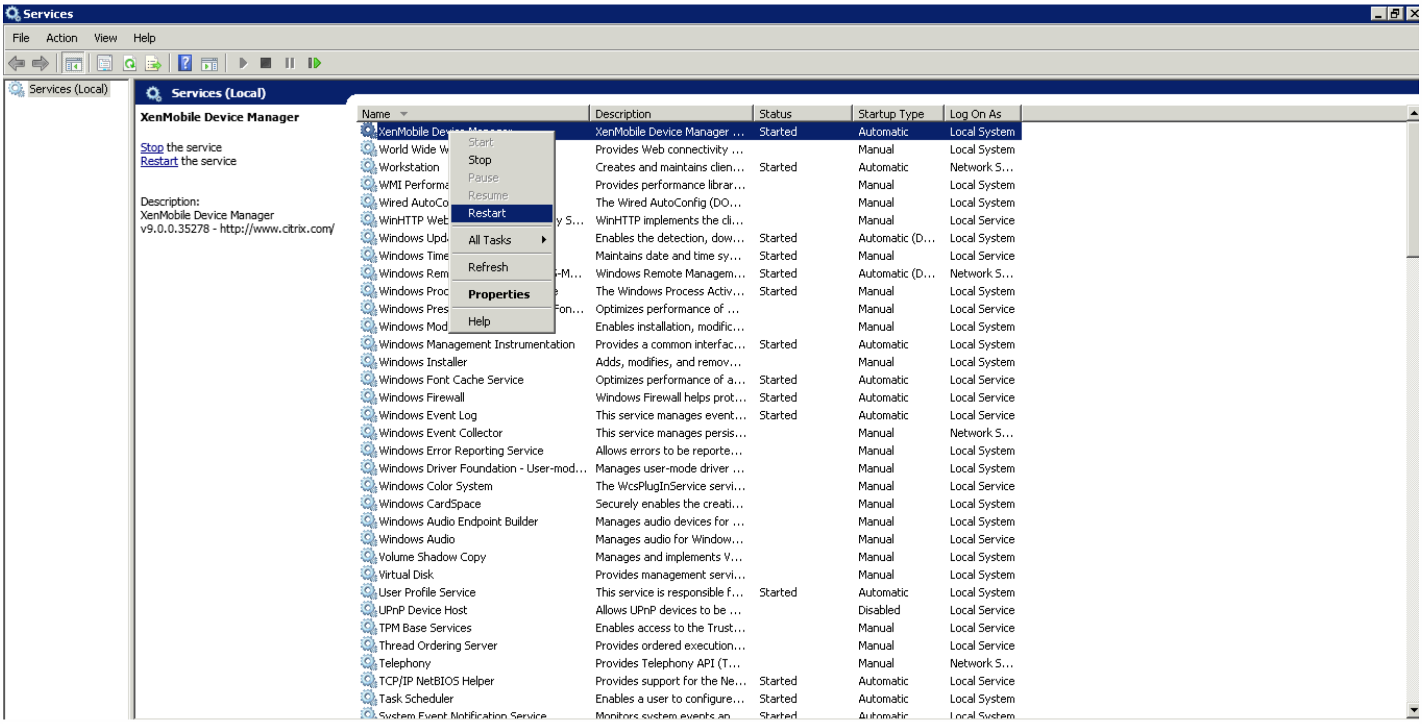
Citrix recommends that you make a backup, copy, or note of the changes you make in the ew-config.properties file. This information is helpful in case the upgrade fails.



ew-config.properties

```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-s
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234.[redacted]net:[redacted]-llaug
# Pooled datasource host name
pooled.datasource.hostname=ah-234.[redacted].net
# Pooled datasource database
pooled.datasource.database=[redacted]-llaug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}[redacted]==

# No pooled datasource driver
#no.pooled.datasource.driver=org.postgresql.Driver
# No pooled datasource url
#no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
# No pooled datasource user
#no.pooled.datasource.user=everywan
# No pooled datasource password
#no.pooled.datasource.password=everywan

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://[redacted]-inc.net:[redacted]-llaug
# Audit datasource host name
audit.datasource.hostname=ah-234.[redacted].net
# Audit datasource database
audit.datasource.database=[redacted]llaug
# Audit datasource user
audit.datasource.user=sa
# Audit datasource password
```

4. Restart the Device Manager service. Refresh the device connections after the Device Manager instance restarts.



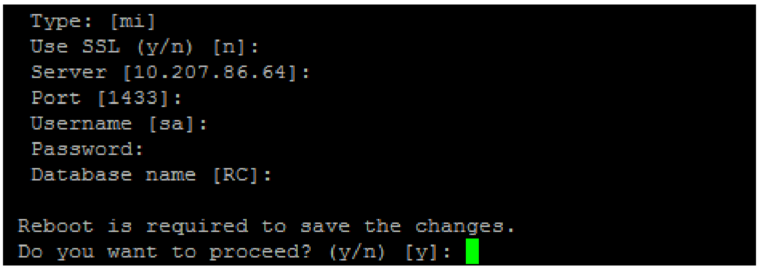
XenMobile Device Manager

Stop the service
Restart the service

Description:
XenMobile Device Manager v9.0.0.35278 - http://www.citrix.com/

Name	Description	Status	Startup Type	Log On As
XenMobile Dev	XenMobile Device Manager …	Started	Automatic	Local System
World Wide W	Provides Web connectivity …		Manual	Local System
Workstation	Creates and maintains clien…	Started	Automatic	Network S…
WMI Performa	Provides performance librar…		Manual	Local System
Wired AutoCo	The Wired AutoConfig (DO…		Manual	Local System
WinHTTP Web y S…	WinHTTP implements the cli…		Manual	Local Service
Windows Upd	Enables the detection, dow…	Started	Automatic (D…	Local System
Windows Time	Maintains date and time sy…	Started	Manual	Local Service
Windows Rem -M…	Windows Remote Managem…	Started	Automatic (D…	Network S…
Windows Proc	The Windows Process Activ…	Started	Manual	Local System
Windows Pres Fon…	Optimizes performance of …		Manual	Local Service
Windows Mod	Enables installation, modific…		Manual	Local System
Windows Management Instrumentation	Provides a common interfac…	Started	Automatic	Local System
Windows Installer	Adds, modifies, and remov…		Manual	Local System
Windows Font Cache Service	Optimizes performance of a…	Started	Automatic	Local Service
Windows Firewall	Windows Firewall helps prot…	Started	Automatic	Local Service
Windows Event Log	This service manages event…	Started	Automatic	Local Service
Windows Event Collector	This service manages persis…		Manual	Network S…
Windows Error Reporting Service	Allows errors to be reporte…		Manual	Local System
Windows Driver Foundation - User-mod…	Manages user-mode driver …		Manual	Local System
Windows Color System	The WcsPlugInService servi…		Manual	Local Service
Windows CardSpace	Securely enables the creati…		Manual	Local System
Windows Audio Endpoint Builder	Manages audio devices for …		Manual	Local System
Windows Audio	Manages audio for Window…		Manual	Local Service
Volume Shadow Copy	Manages and implements V…		Manual	Local System
Virtual Disk	Provides management servi…		Manual	Local System
User Profile Service	This service is responsible f…	Started	Automatic	Local System
UPnP Device Host	Allows UPnP devices to be …		Disabled	Local Service
TPM Base Services	Enables access to the Trust…		Manual	Local Service
Thread Ordering Server	Provides ordered execution…		Manual	Local Service
Telephony	Provides Telephony API (T…		Manual	Network S…
TCP/IP NetBIOS Helper	Provides support for the Ne…	Started	Automatic	Local Service
Task Scheduler	Enables a user to configure…	Started	Automatic	Local System
System Event Notification Service	Monitors system events an…	Started	Automatic	Local System

5. Determine if the new XenMobile 10.x server must also work with named SQL instance. If so, identify the port on which the named instance is running. If the port is a dynamic port, Citrix recommends that you convert the port to a static port. Later, when you reach the following portion of the database setup during the upgrade, configure the static port on the new XenMobile server.



```
  Type: [mi]
  Use SSL (y/n) [n]:
  Server [10.207.86.64]:
  Port [1433]:
  Username [sa]:
  Password:
  Database name [RC]:

 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]:
```

You can now proceed with the upgrade.

If your system is configured in cluster mode:

1. Shut down all nodes other than the one you plan to upgrade first. To shut down a node, use `Settings` in the command-line interface.

2. Upgrade the node that's still running, as described in the next section, "To enable and run the Upgrade Tool."

3. After you've ensured that the first upgrade has upgraded as expected, rejoin each of the remaining nodes, one at a time. To rejoin:

    a. Restart the node.

    b. Do not upgrade the node if prompted.

    c. Join the node to the cluster database.

    XenMobile will automatically upgrade a node after you rejoin it to the cluster.

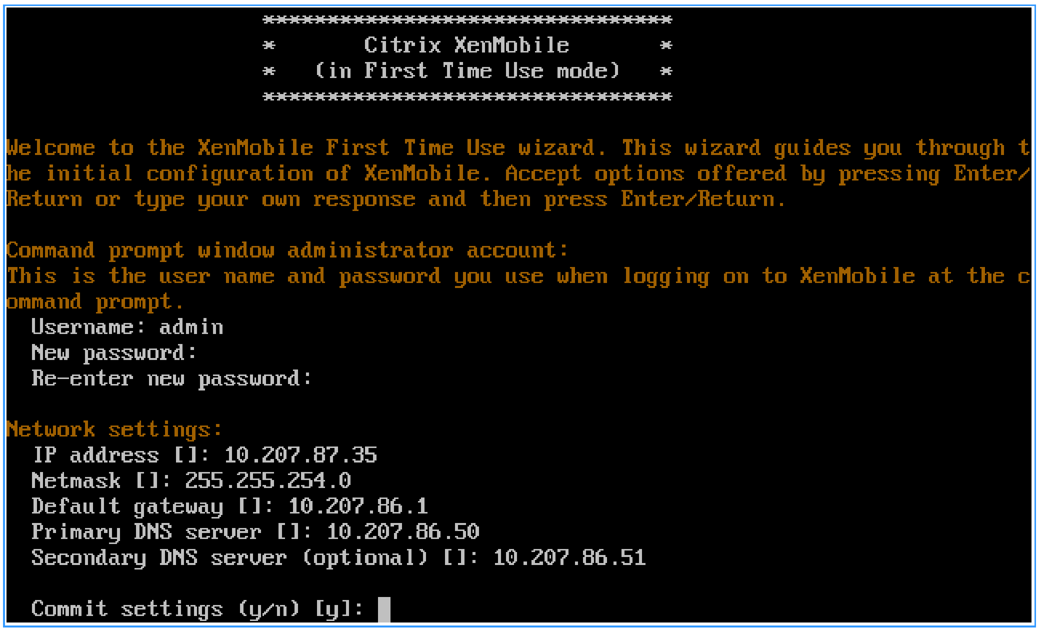
4. Perform all post-requisite tasks on each node after you rejoin it to the cluster.

Enable the Upgrade Tool through the command-line interface (CLI) when you first install the latest version of XenMobile.

> ## Important
>
> If you want to take a snapshot of your system, first complete the initial configuration of the latest version of XenMobile and use the Upgrade Tool.

1. In the CLI, type your administrator user name and password and then enter your network settings.

2. Type **y** to commit the settings.



```
                    *********************************
                    *       Citrix XenMobile        *
                    *    (in First Time Use mode)   *
                    *********************************

Welcome to the XenMobile First Time Use wizard. This wizard guides you through t
he initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
  Username: admin
  New password:
  Re-enter new password:

Network settings:
  IP address []: 10.207.87.35
  Netmask []: 255.255.254.0
  Default gateway []: 10.207.86.1
  Primary DNS server []: 10.207.86.50
  Secondary DNS server (optional) []: 10.207.86.51

  Commit settings (y/n) [y]:
```

3. Type **y** to upgrade.

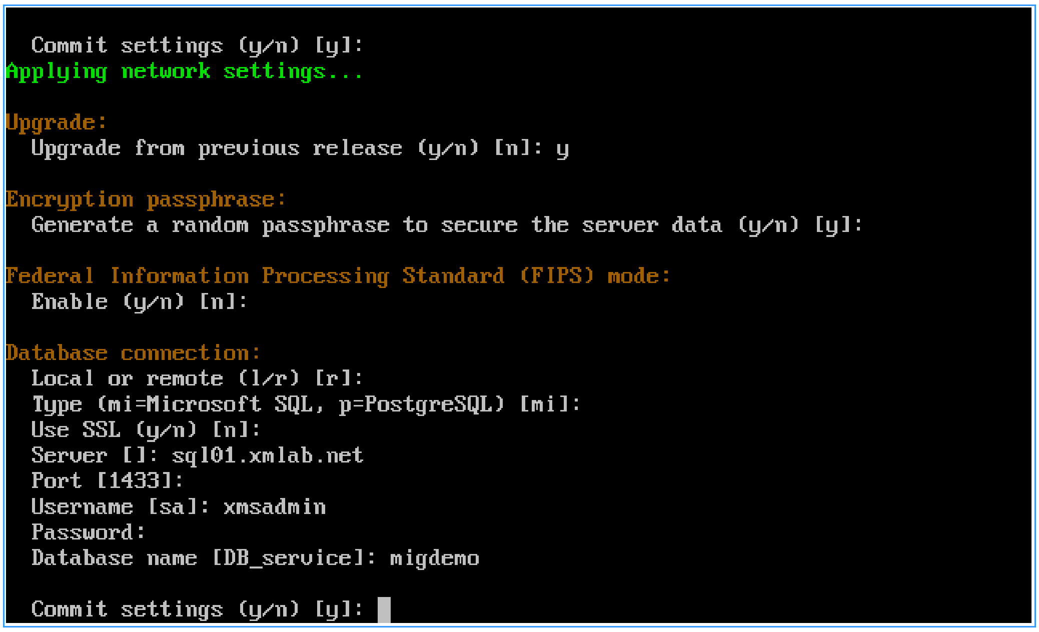
Note

If you do not select **y** here, you must configure a new instance of the latest version of XenMobile in the command-line console. Then, start the Upgrade Tool again.

4. Complete these settings:

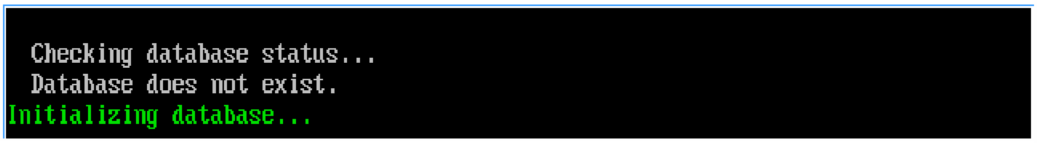
- Citrix recommends typing **y** to generate a random passphrase. XenMobile uses the passphrase as part of the protection of the encryption keys which secure your sensitive data. XenMobile uses a hash of the passphrase, stored in the server file system, to retrieve the keys during the encryption and decryption of data. The passphrase isn't viewable.
- Optionally, enable FIPS.
- Type your database connection information.

5. Type **y** to commit the settings.



```
  Commit settings (y/n) [y]:
Applying network settings...

Upgrade:
  Upgrade from previous release (y/n) [n]: y

Encryption passphrase:
  Generate a random passphrase to secure the server data (y/n) [y]:

Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:

Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:
  Server []: sql01.xmlab.net
  Port [1433]:
  Username [sa]: xmsadmin
  Password:
  Database name [DB_service]: migdemo

  Commit settings (y/n) [y]:
```

XenMobile initializes the database.



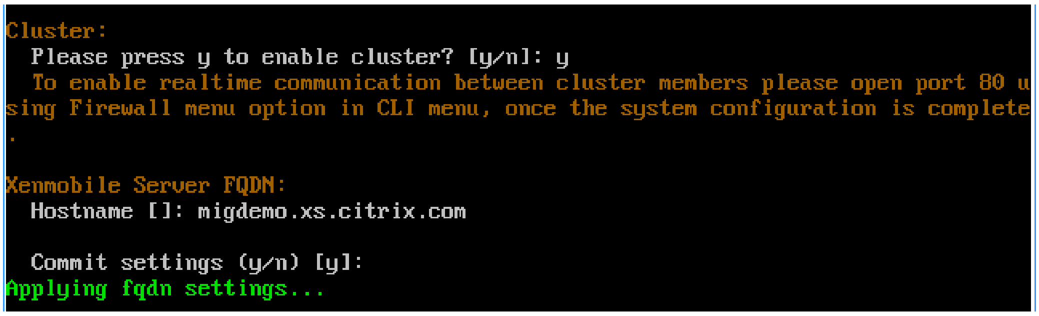
```
  Checking database status...
  Database does not exist.
Initializing database...
```

6. Select whether to enable clustered servers. Type the XenMobile fully qualified domain name (FQDN). Note the following:

- For XenMobile Enterprise Edition deployments, the FQDN is the same as the XenMobile 9.0 MDM FQDN.
- For MAM deployments, the FQDN is the same as the XenMobile 9.0 App Controller FQDN.
- For MDM deployments, the FQDN is the same as the XenMobile 9.0 Device Manager FQDN.

Important

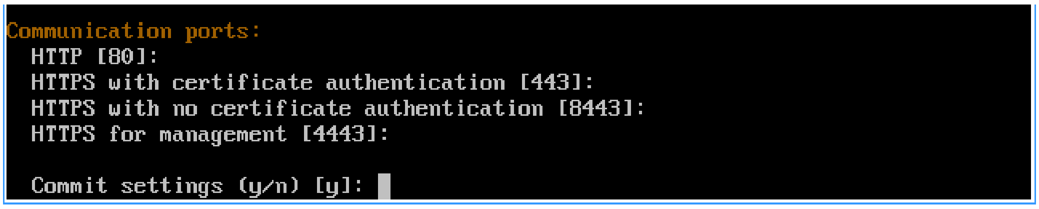
The FQDN for the 9.0 environment and for the new environment must match.



```
Cluster:
  Please press y to enable cluster? [y/n]: y
  To enable realtime communication between cluster members please open port 80 u
sing Firewall menu option in CLI menu, once the system configuration is complete
.

Xenmobile Server FQDN:
  Hostname []: migdemo.xs.citrix.com

  Commit settings (y/n) [y]:
Applying fqdn settings...
```

7. Type **y** to commit the settings.

8. Set communication ports.

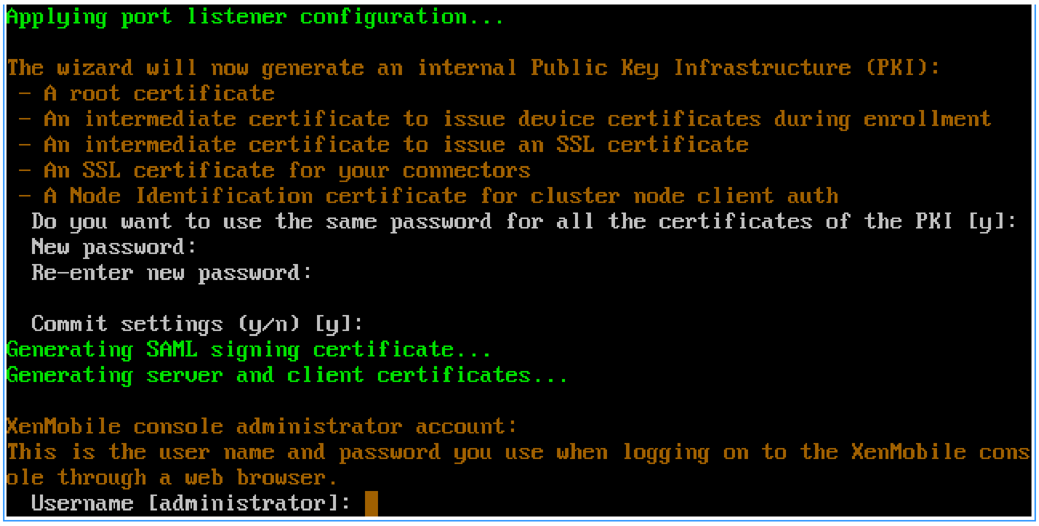


```
Communication ports:
  HTTP [80]:
  HTTPS with certificate authentication [443]:
  HTTPS with no certificate authentication [8443]:
  HTTPS for management [4443]:

  Commit settings (y/n) [y]:
```

9. Type **y** to commit the settings.

10. Select whether to use the same password for all certificates and type the password to be used for certificates.

11. Type **y** to commit the settings.

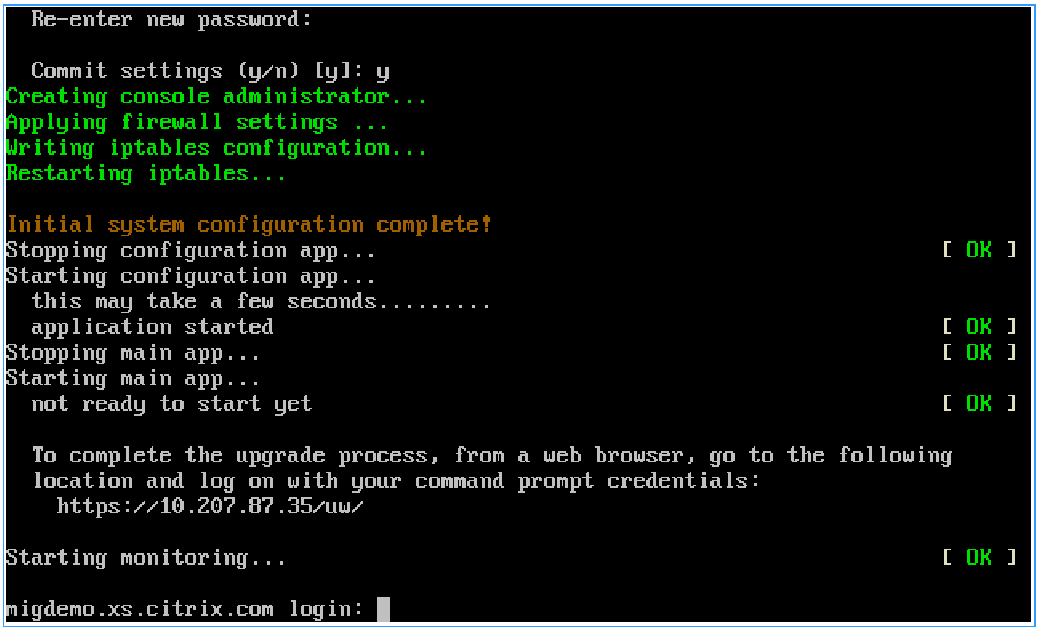


```
Applying port listener configuration...

The wizard will now generate an internal Public Key Infrastructure (PKI):
 - A root certificate
 - An intermediate certificate to issue device certificates during enrollment
 - An intermediate certificate to issue an SSL certificate
 - An SSL certificate for your connectors
 - A Node Identification certificate for cluster node client auth
  Do you want to use the same password for all the certificates of the PKI [y]:
  New password:
  Re-enter new password:

  Commit settings (y/n) [y]:
Generating SAML signing certificate...
Generating server and client certificates...

XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile cons
ole through a web browser.
  Username [administrator]:
```

12. Type the user name and password for the XenMobile console administrator.

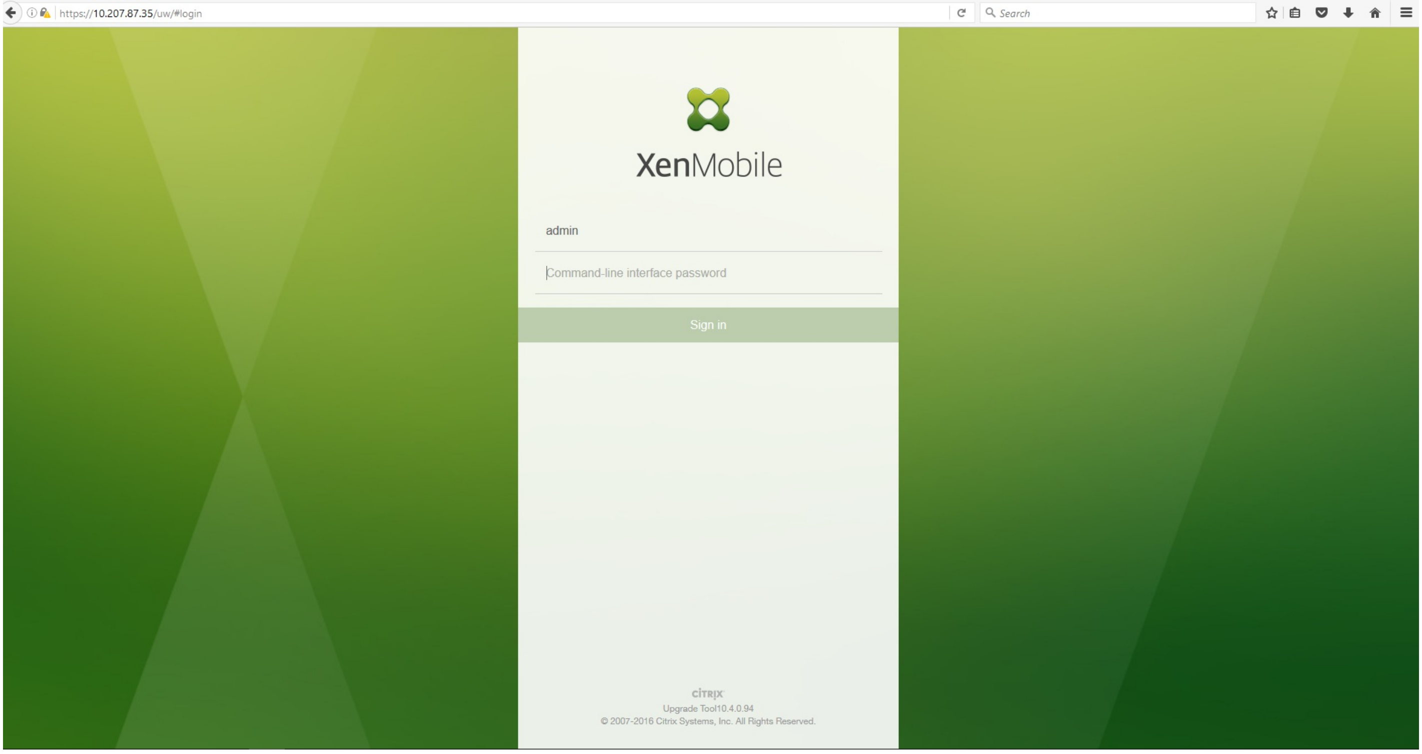
13. Type **y** to commit the settings.

XenMobile enables the one-time-only Upgrade Tool.

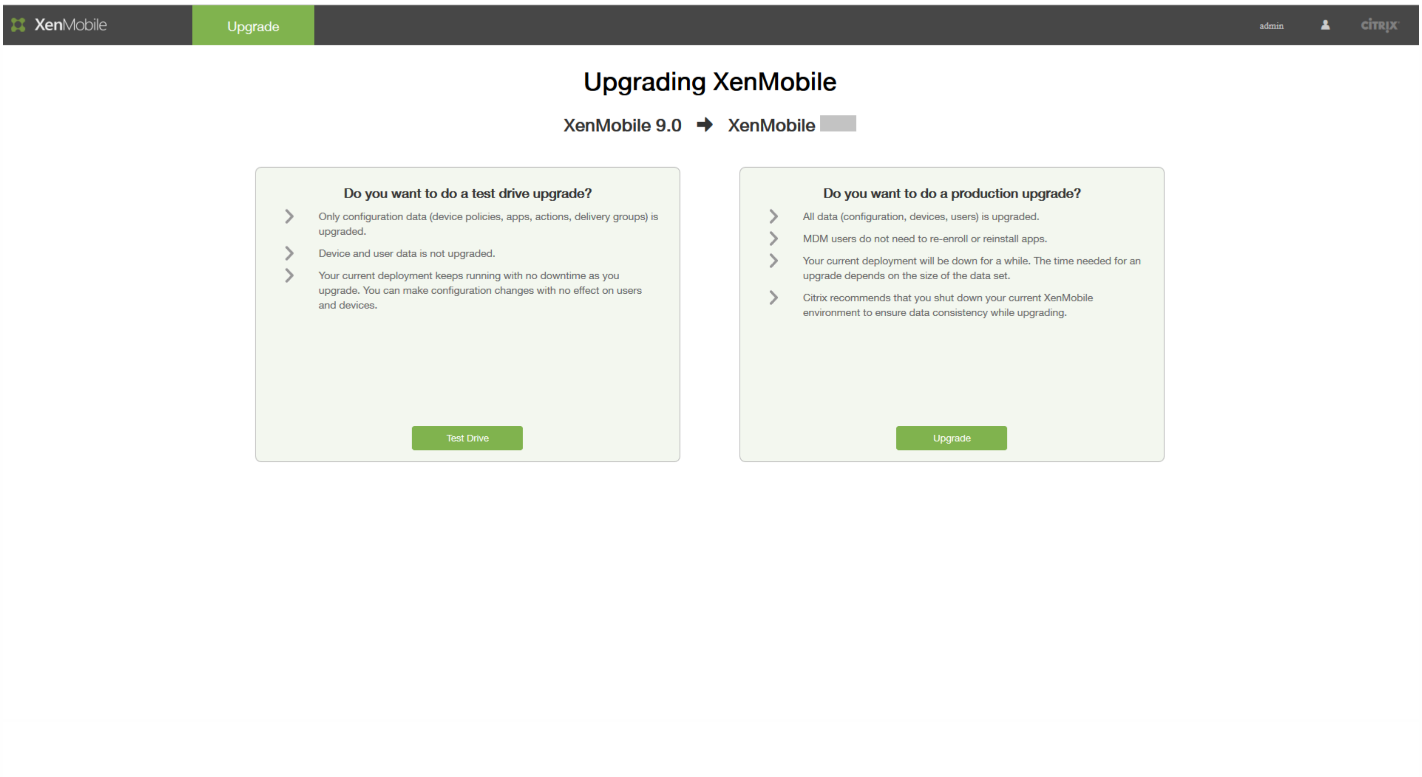


```
  Re-enter new password:

  Commit settings (y/n) [y]: y
Creating console administrator...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app...                                          [ OK ]
Starting configuration app...
  this may take a few seconds.........
  application started                                                  [ OK ]
Stopping main app...                                                   [ OK ]
Starting main app...
  not ready to start yet                                               [ OK ]

  To complete the upgrade process, from a web browser, go to the following
  location and log on with your command prompt credentials:
    https://10.207.87.35/uw/

Starting monitoring...                                                 [ OK ]

migdemo.xs.citrix.com login: 
```

14. Access the Upgrade Tool on a web browser through https://<XenMobile-Server-IPAddress>/uw/ and log in using the credentials you specified using the CLI.


https://10.207.87.35/uw/#login
Search
XenMobile
admin
Command-line interface password
Sign in
citrix
Upgrade Tool10.4.0.94
© 2007-2016 Citrix Systems, Inc. All Rights Reserved.

15. You can now choose between a test drive and a production upgrade. These instructions are for a production upgrade. In the **Upgrading XenMobile** page, click **Upgrade**.



Upgrading XenMobile

XenMobile 9.0 ➜ XenMobile

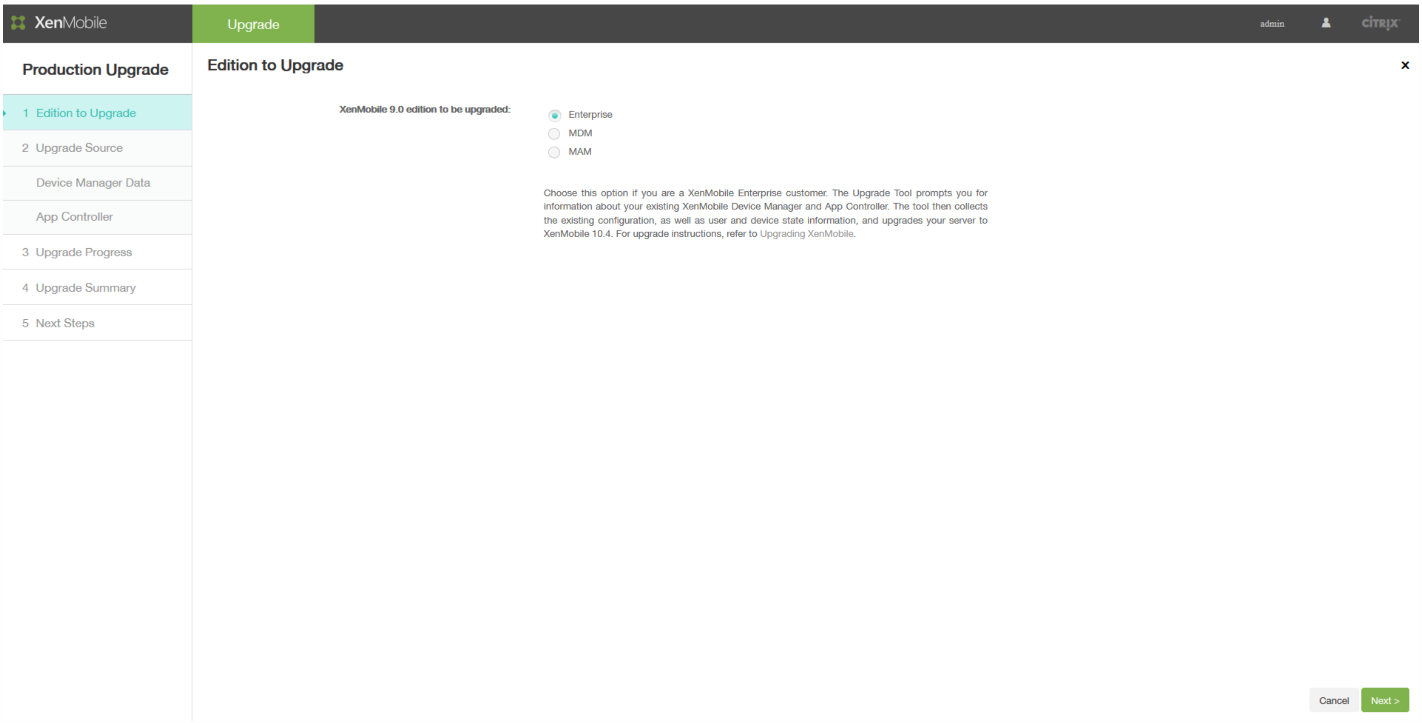
Do you want to do a test drive upgrade?

- Only configuration data (device policies, apps, actions, delivery groups) is upgraded.
- Device and user data is not upgraded.
- Your current deployment keeps running with no downtime as you upgrade. You can make configuration changes with no effect on users and devices.

Do you want to do a production upgrade?

- All data (configuration, devices, users) is upgraded.
- MDM users do not need to re-enroll or reinstall apps.
- Your current deployment will be down for a while. The time needed for an upgrade depends on the size of the data set.
- Citrix recommends that you shut down your current XenMobile environment to ensure data consistency while upgrading.

16. In the **Edition to Upgrade** page, select your edition. The example screen below shows Enterprise edition selected.



Edition to Upgrade

XenMobile 9.0 edition to be upgraded: ● Enterprise ○ MDM ○ MAM

Choose this option if you are a XenMobile Enterprise customer. The Upgrade Tool prompts you for information about your existing XenMobile Device Manager and App Controller. The tool then collects the existing configuration, as well as user and device state information, and upgrades your server to XenMobile 10.4. For upgrade instructions, refer to Upgrading XenMobile.

17. Click **Next**.

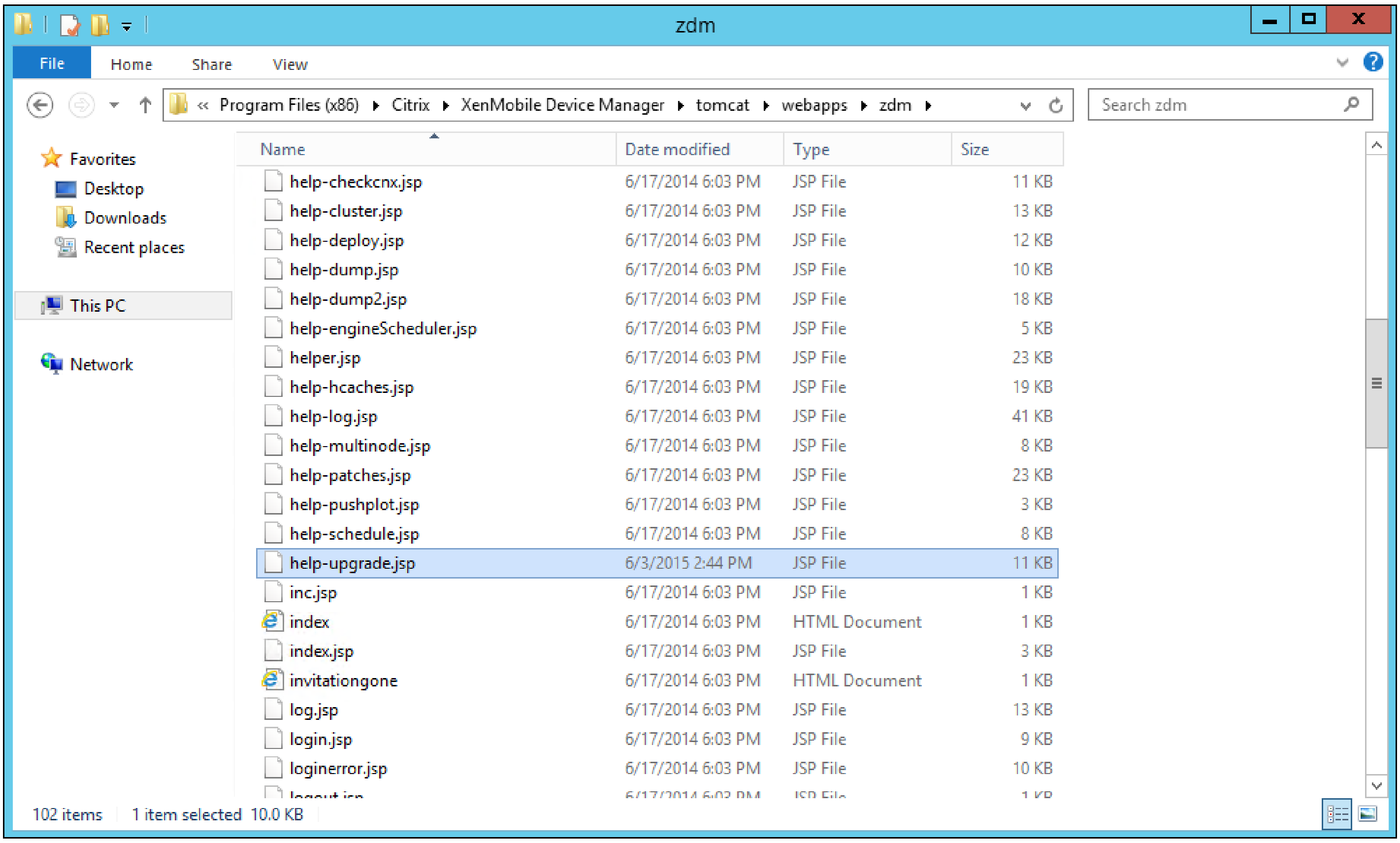
If you are upgrading an Enterprise or MDM edition, the **Device Manager** page appears. Follow steps 18 through 22 to complete this page.

If you are upgrading a MAM edition, skip to step 23 to complete the **App Controller** page.

18. Collect the files required to migrate your existing XenMobile 9.0 Device Manager data. During this process, you get access to the database URL and user name that you then copy to the **Device Manager** page.

a. Click the link in step 1 of the **Device Manager** page and save the downloaded help-upgrade.zip file.

b. Extract the help-upgrade.jsp file to <MDM-Install-Path>\tomcat\webapps\zdm on your existing XenMobile 9.0 Device Manager.

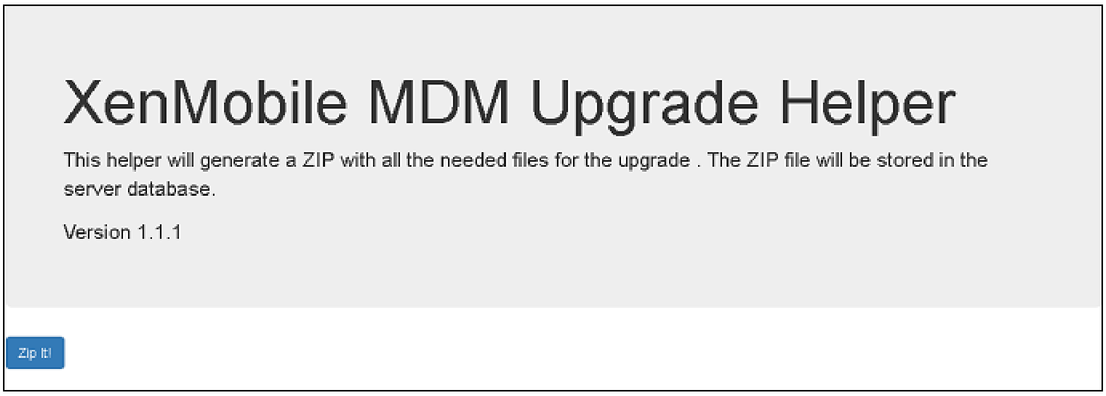


Name	Date modified	Type	Size
help-checkcnx.jsp	6/17/2014 6:03 PM	JSP File	11 KB
help-cluster.jsp	6/17/2014 6:03 PM	JSP File	13 KB
help-deploy.jsp	6/17/2014 6:03 PM	JSP File	12 KB
help-dump.jsp	6/17/2014 6:03 PM	JSP File	10 KB
help-dump2.jsp	6/17/2014 6:03 PM	JSP File	18 KB
help-engineScheduler.jsp	6/17/2014 6:03 PM	JSP File	5 KB
helper.jsp	6/17/2014 6:03 PM	JSP File	23 KB
help-hcaches.jsp	6/17/2014 6:03 PM	JSP File	19 KB
help-log.jsp	6/17/2014 6:03 PM	JSP File	41 KB
help-multinode.jsp	6/17/2014 6:03 PM	JSP File	8 KB
help-patches.jsp	6/17/2014 6:03 PM	JSP File	23 KB
help-pushplot.jsp	6/17/2014 6:03 PM	JSP File	3 KB
help-schedule.jsp	6/17/2014 6:03 PM	JSP File	8 KB
help-upgrade.jsp	6/3/2015 2:44 PM	JSP File	11 KB
inc.jsp	6/17/2014 6:03 PM	JSP File	1 KB
index	6/17/2014 6:03 PM	HTML Document	1 KB
index.jsp	6/17/2014 6:03 PM	JSP File	3 KB
invitationgone	6/17/2014 6:03 PM	HTML Document	1 KB
log.jsp	6/17/2014 6:03 PM	JSP File	13 KB
login.jsp	6/17/2014 6:03 PM	JSP File	9 KB
loginerror.jsp	6/17/2014 6:03 PM	JSP File	10 KB
logout.jsp	6/17/2014 6:03 PM	JSP File	1 KB

c. In a browser window, log on to the XenMobile 9.0 server.

d. In a separate browser tab, enter this URL to open the **XenMobile MDM Upgrade Helper** page: https://localhost/zdm/help-upgrade.jsp. That page includes a zip of all XenMobile 9.0 files that are needed for the upgrade. The zip file is stored in the server database from where it is extracted.

e. Click **Zip it** and then follow the on-screen steps to collect the files needed for the upgrade.

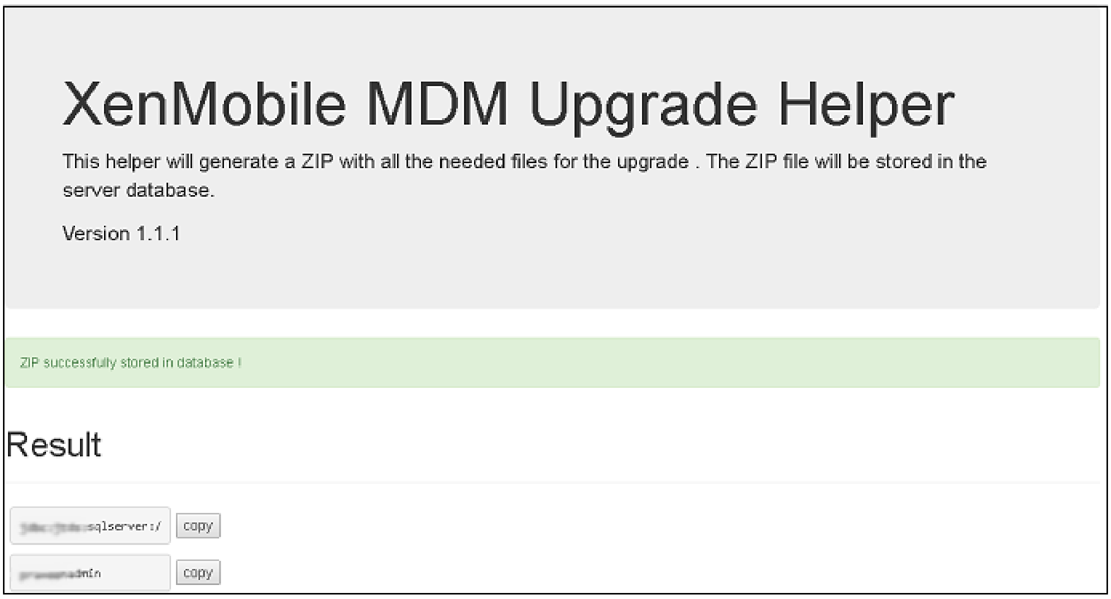


XenMobile MDM Upgrade Helper

This helper will generate a ZIP with all the needed files for the upgrade . The ZIP file will be stored in the server database.

Version 1.1.1

19. Under **Result**, copy the URL and paste it in the **Database URL** field in the Upgrade Tool **Device Manager** page. Then copy the user name and copy it to the **Device Manager** page.



XenMobile MDM Upgrade Helper

This helper will generate a ZIP with all the needed files for the upgrade . The ZIP file will be stored in the server database.

Version 1.1.1

ZIP successfully stored in database !

Result

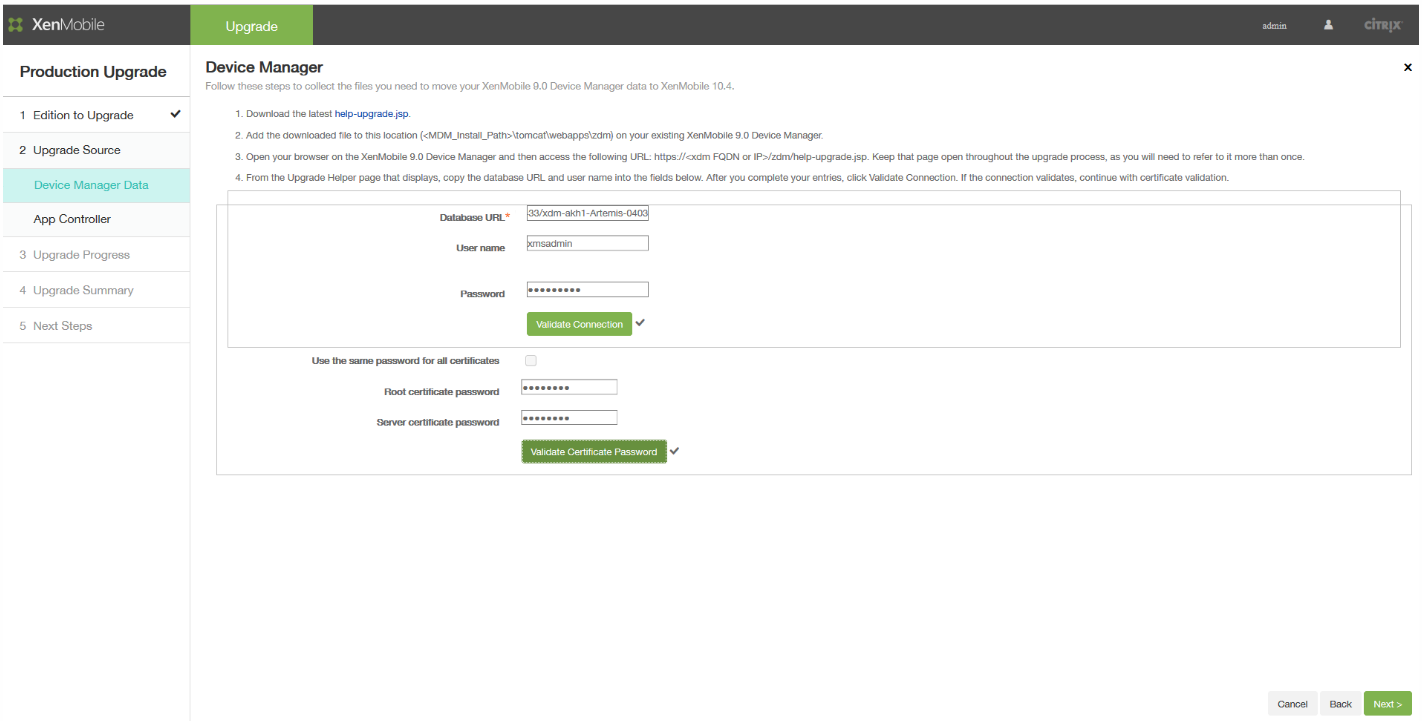
[redacted]sqlserver:/ copy

[redacted]admin copy

20. In the Upgrade Tool:

a. Enter the password and then click **Validate Connection**.

b. Enter the password for each certificate and then click **Validate Password**.



Device Manager

Follow these steps to collect the files you need to move your XenMobile 9.0 Device Manager data to XenMobile 10.4.

1. Download the latest help-upgrade.jsp.
2. Add the downloaded file to this location (<MDM_Install_Path>\tomcat\webapps\zdm) on your existing XenMobile 9.0 Device Manager.
3. Open your browser on the XenMobile 9.0 Device Manager and then access the following URL: https://<xdm FQDN or IP>/zdm/help-upgrade.jsp. Keep that page open throughout the upgrade process, as you will need to refer to it more than once.
4. From the Upgrade Helper page that displays, copy the database URL and user name into the fields below. After you complete your entries, click Validate Connection. If the connection validates, continue with certificate validation.

Database URL* 33/xdm-akh1-Artemis-0403

User name xmsadmin

Password ••••••••••

Validate Connection ✓

Use the same password for all certificates □

Root certificate password ••••••••

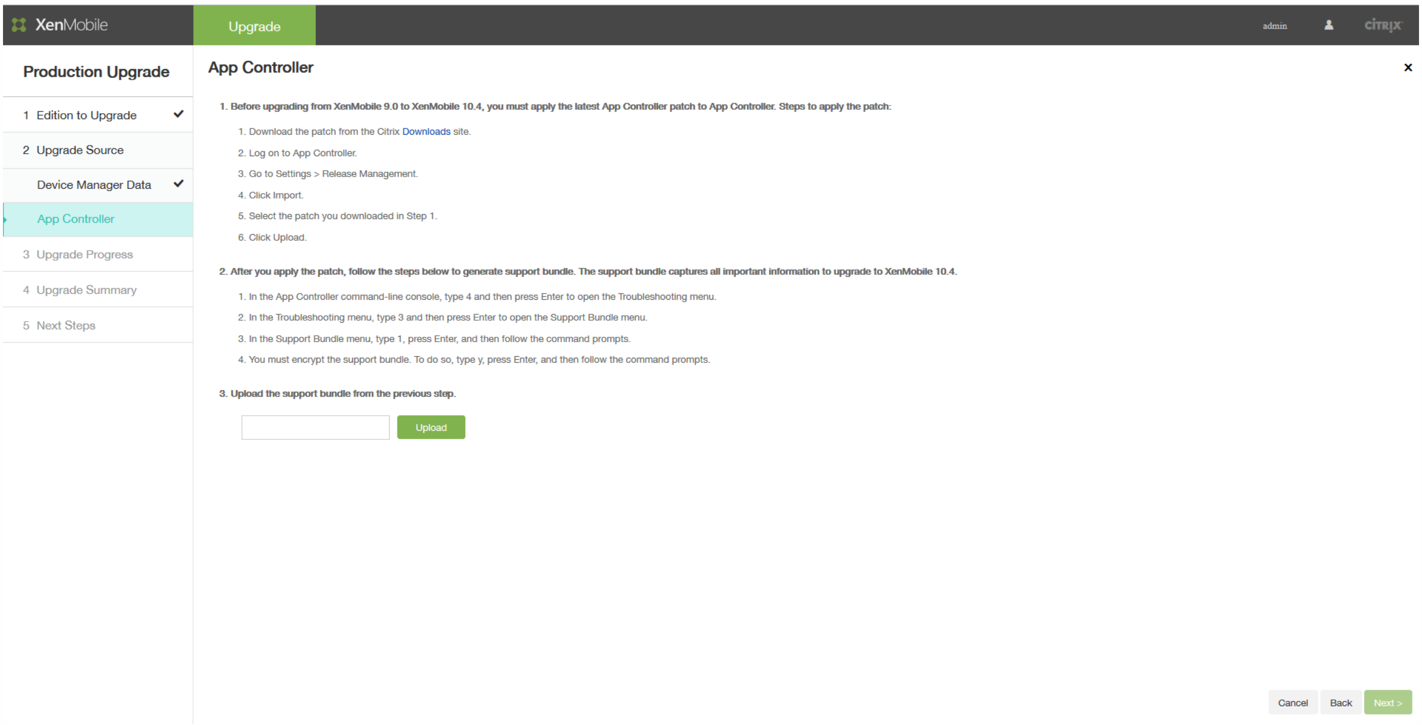
Server certificate password ••••••••

Validate Certificate Password ✓

21. Click **Next**.

22. If you changed the ew-config.properties file, restart the xdm service on XenMobile 9 MDM and then go to https://localhost/zdm/help-upgrade.jsp to run the zip again. Doing so re-reads the ew-config.properties file and saves it to the XenMobile MDM 9 database to prepare for migration.

23. Next you apply an upgrade patch to App Controller and then generate and upload a support bundle. Start by following the instructions in section 1 of the **App Controller** page to upgrade App Controller.



App Controller

1. Before upgrading from XenMobile 9.0 to XenMobile 10.4, you must apply the latest App Controller patch to App Controller. Steps to apply the patch:

1. Download the patch from the Citrix Downloads site.
2. Log on to App Controller.
3. Go to Settings > Release Management.
4. Click Import.
5. Select the patch you downloaded in Step 1.
6. Click Upload.

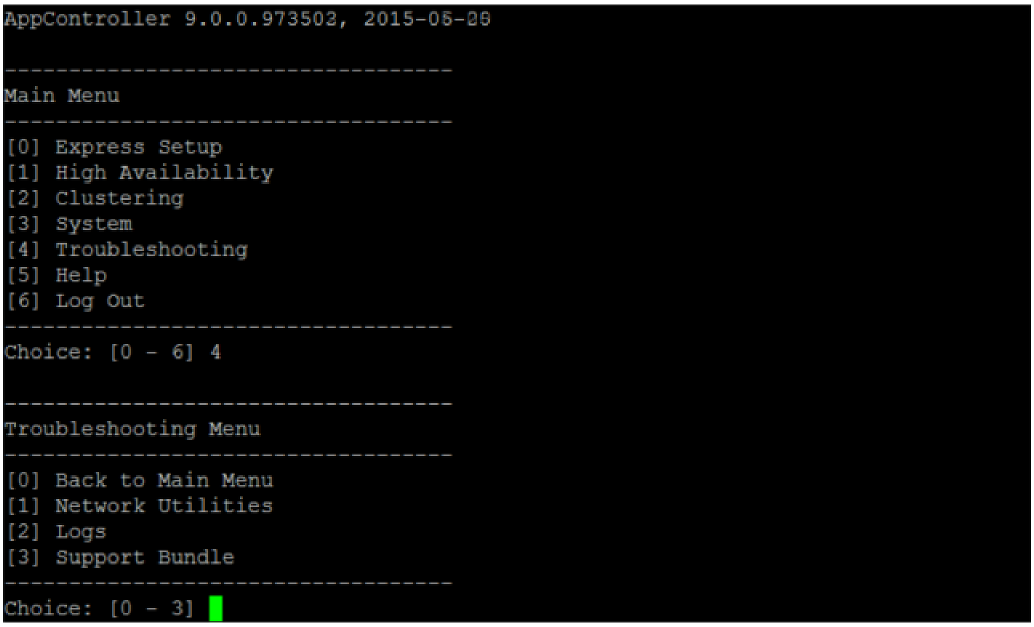
2. After you apply the patch, follow the steps below to generate support bundle. The support bundle captures all important information to upgrade to XenMobile 10.4.

1. In the App Controller command-line console, type 4 and then press Enter to open the Troubleshooting menu.
2. In the Troubleshooting menu, type 3 and then press Enter to open the Support Bundle menu.
3. In the Support Bundle menu, type 1, press Enter, and then follow the command prompts.
4. You must encrypt the support bundle. To do so, type y, press Enter, and then follow the command prompts.

3. Upload the support bundle from the previous step.

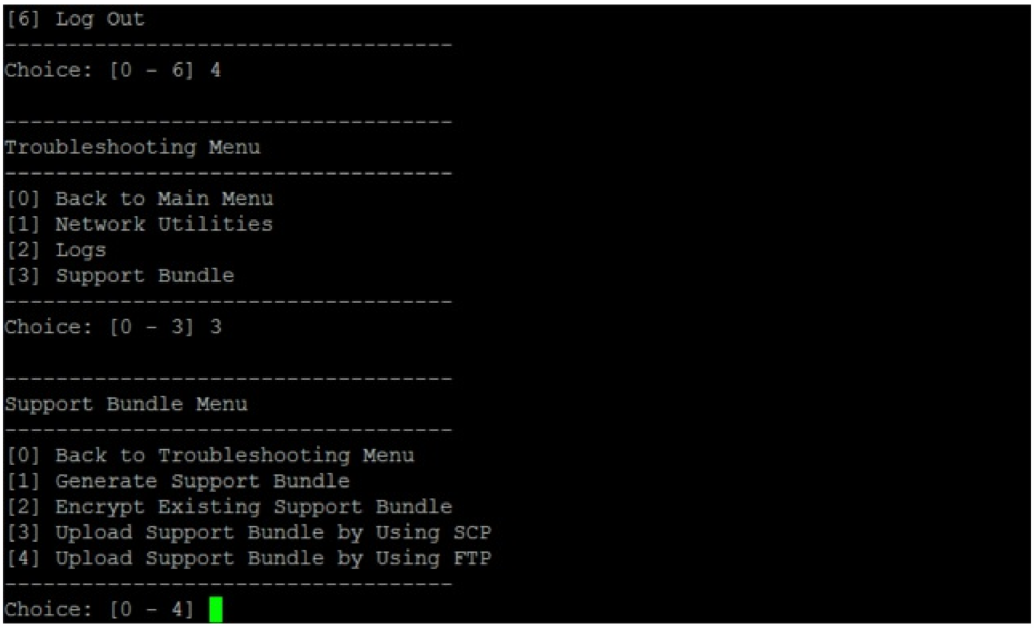
25. Continue to the instructions in section 2 of the **App Controller** page:

a. In the App Controller command-line console, type **4** and then press ENTER to open the Troubleshooting menu.



```
AppController 9.0.0.973502, 2015-05-29

-----------------------------------
Main Menu
-----------------------------------
[0] Express Setup
[1] High Availability
[2] Clustering
[3] System
[4] Troubleshooting
[5] Help
[6] Log Out
-----------------------------------
Choice: [0 - 6] 4

-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----------------------------------
Choice: [0 - 3] 
```

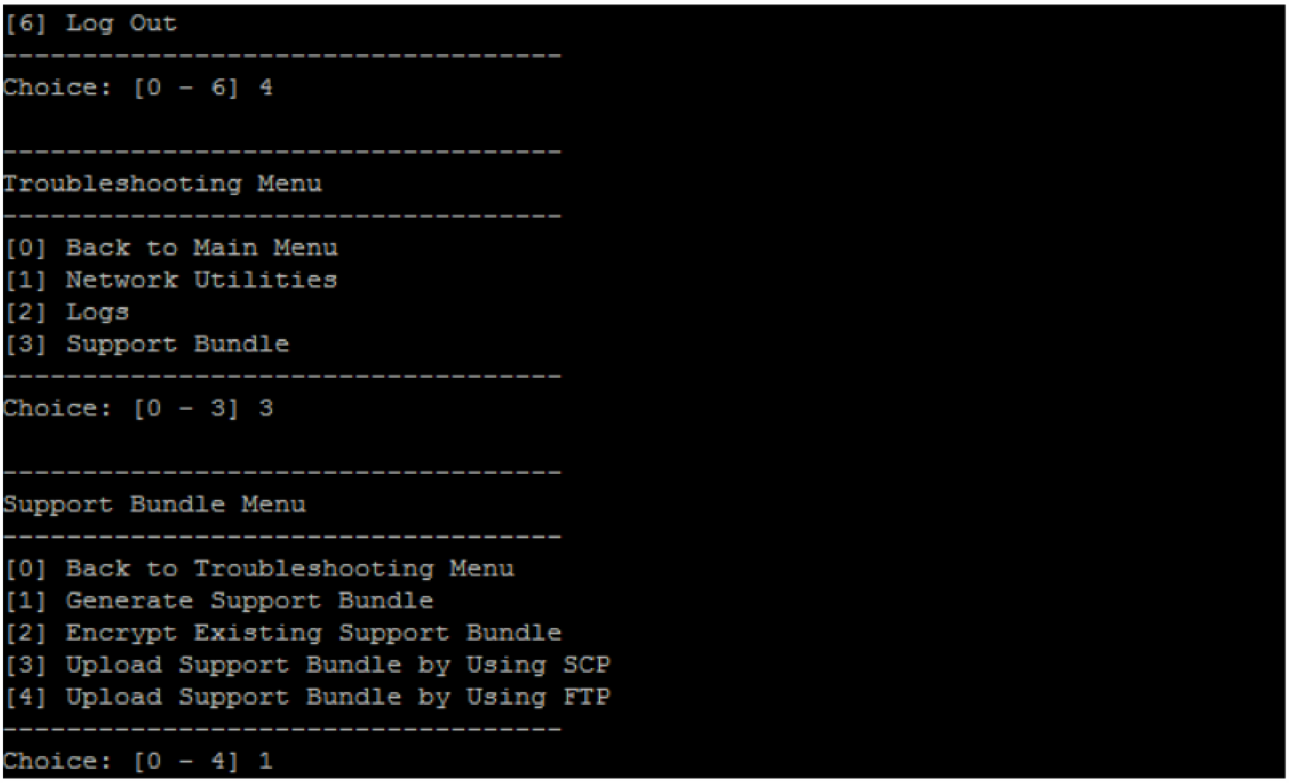
b. In the Troubleshooting menu, type **3** and then press ENTER to open the Support Bundle menu.



```
[6] Log Out
-----------------------------------
Choice: [0 - 6] 4

-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----------------------------------
Choice: [0 - 3] 3

-----------------------------------
Support Bundle Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
-----------------------------------
Choice: [0 - 4]
```

c. In the Support Bundle menu, type **1**, press ENTER, and then follow the command prompts.

Note: Ensure that you encrypt the support bundle.

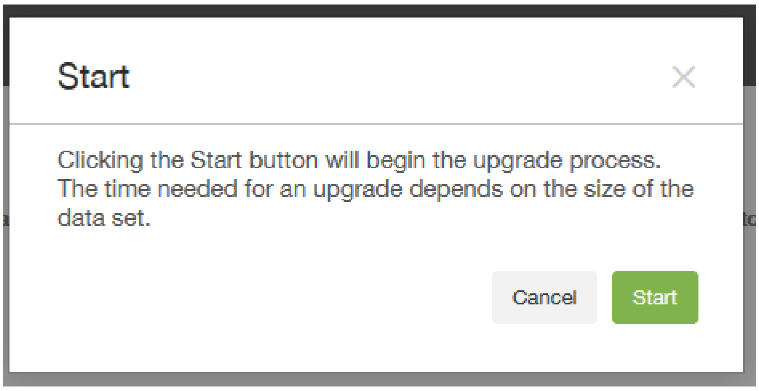


```
[6] Log Out
-----------------------------------
Choice: [0 - 6] 4

-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----------------------------------
Choice: [0 - 3] 3

-----------------------------------
Support Bundle Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
-----------------------------------
Choice: [0 - 4] 1
```

26. In section 3 of the **App Controller** page, specify the support bundle and then click **Upload**.

The Upgrade Tool processes the collected files (for XenMobile Enterprise and MAM editions) and the support bundle. This step may take more than 15 minutes if you are migrating many users.

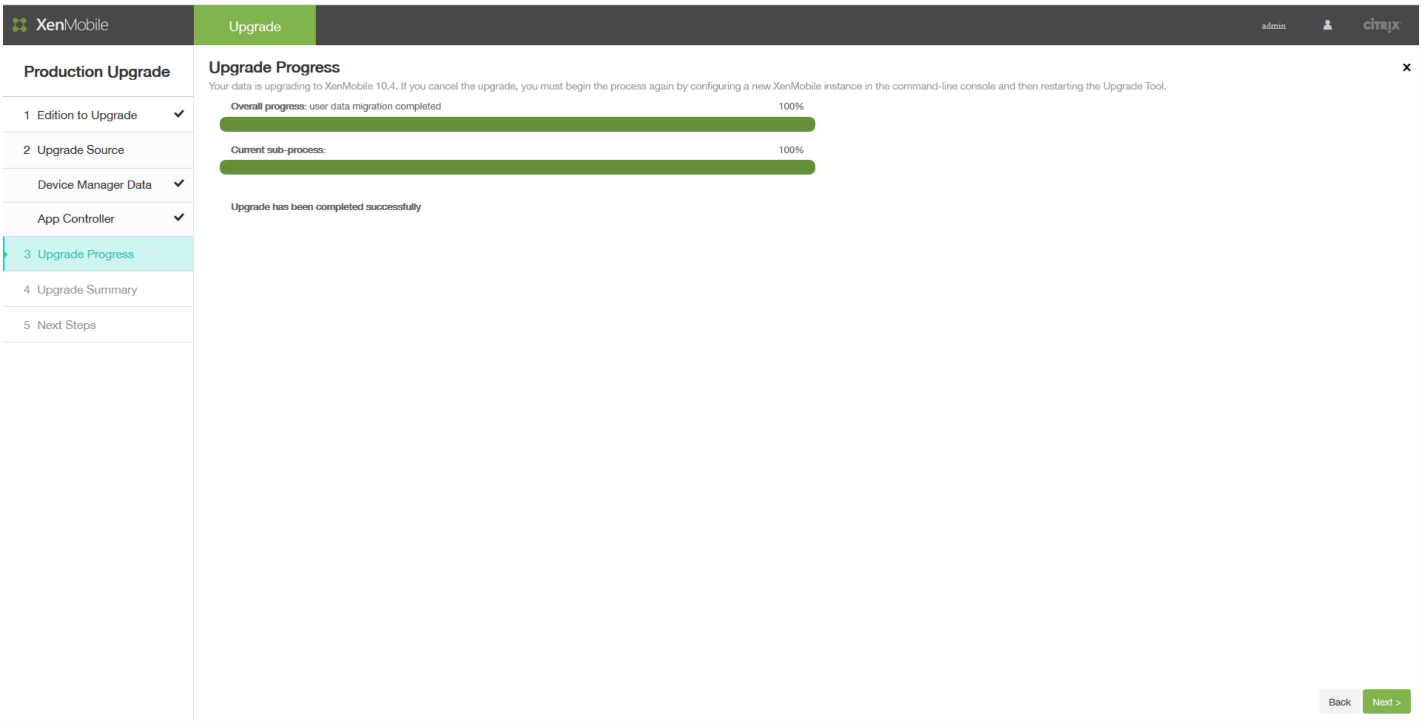
27. Click **Next**. The **Start** confirmation dialog box appears.



Start

Clicking the Start button will begin the upgrade process. The time needed for an upgrade depends on the size of the data set.

28. Click **Start**. The **Upgrade Progress** page appears with progress indicators to let you track the data upgrade from XenMobile 9.0. When the upgrade is complete, the progress indicators are at 100% and the **Next** button is enabled.



Upgrade Progress

Your data is upgrading to XenMobile 10.4. If you cancel the upgrade, you must begin the process again by configuring a new XenMobile instance in the command-line console and then restarting the Upgrade Tool.

Overall progress: user data migration completed 100%

Current sub-process: 100%

Upgrade has been completed successfully

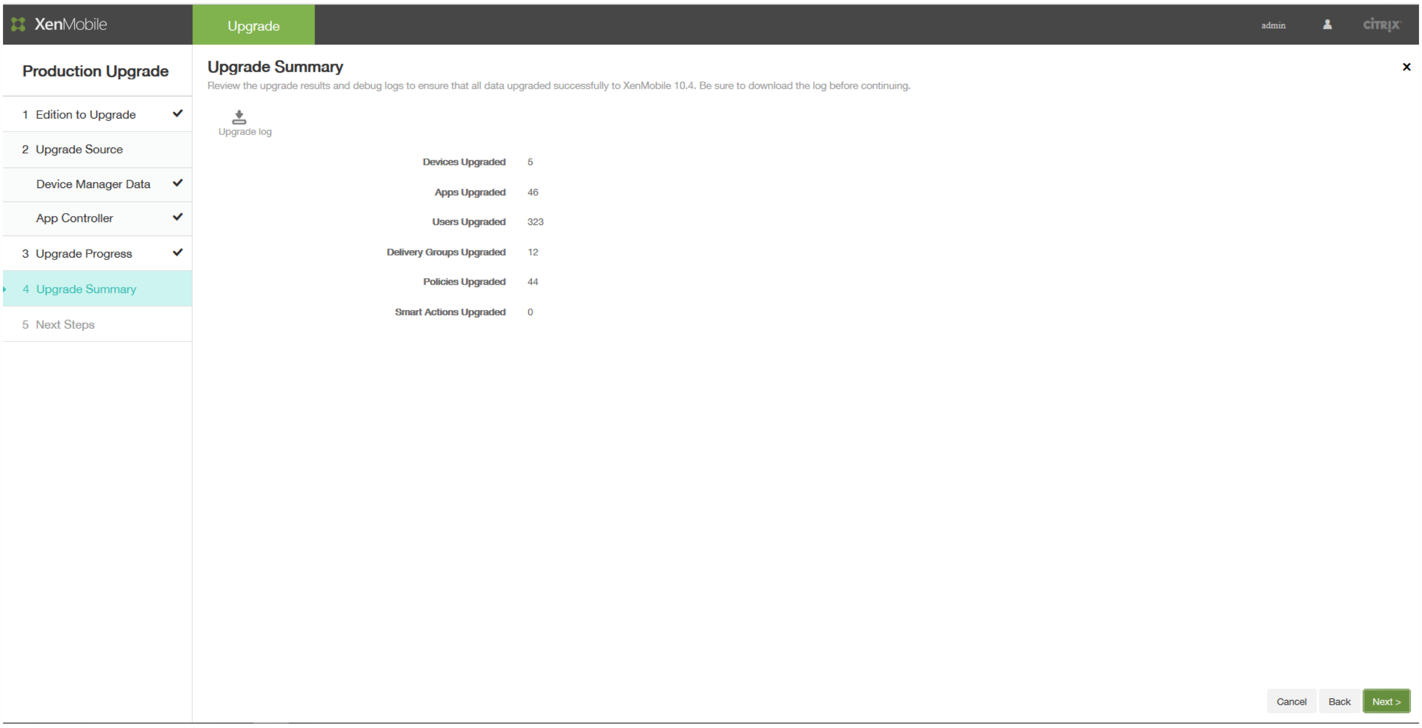
Note

If the upgrade fails, you can view the logs to understand the reason for the error. Then, import a new XenMobile instance and restart the upgrade process. You cannot use the Back button in the browser to return to earlier pages and correct information.

The Upgrade Progress page lets you know when the upgrade has completed successfully.

29. Click **Next**. The **Upgrade Summary** page appears.

If you are upgrading an Enterprise or MAM edition, the **Upgrade Summary** page might look like the following:

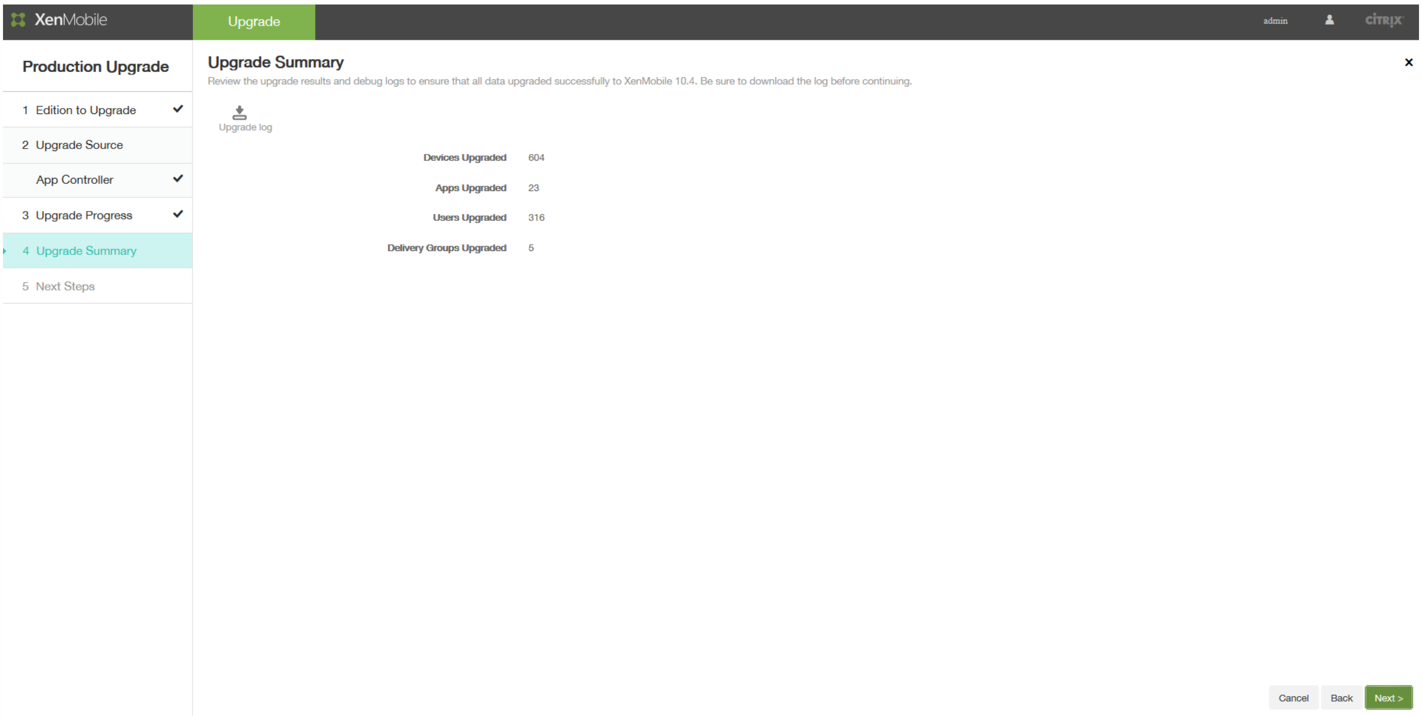


Upgrade Summary

Review the upgrade results and debug logs to ensure that all data upgraded successfully to XenMobile 10.4. Be sure to download the log before continuing.

Devices Upgraded	5
Apps Upgraded	46
Users Upgraded	323
Delivery Groups Upgraded	12
Policies Upgraded	44
Smart Actions Upgraded	0

If you are upgrading an MDM edition, the **Upgrade Summary** page might look like the following:



Upgrade Summary

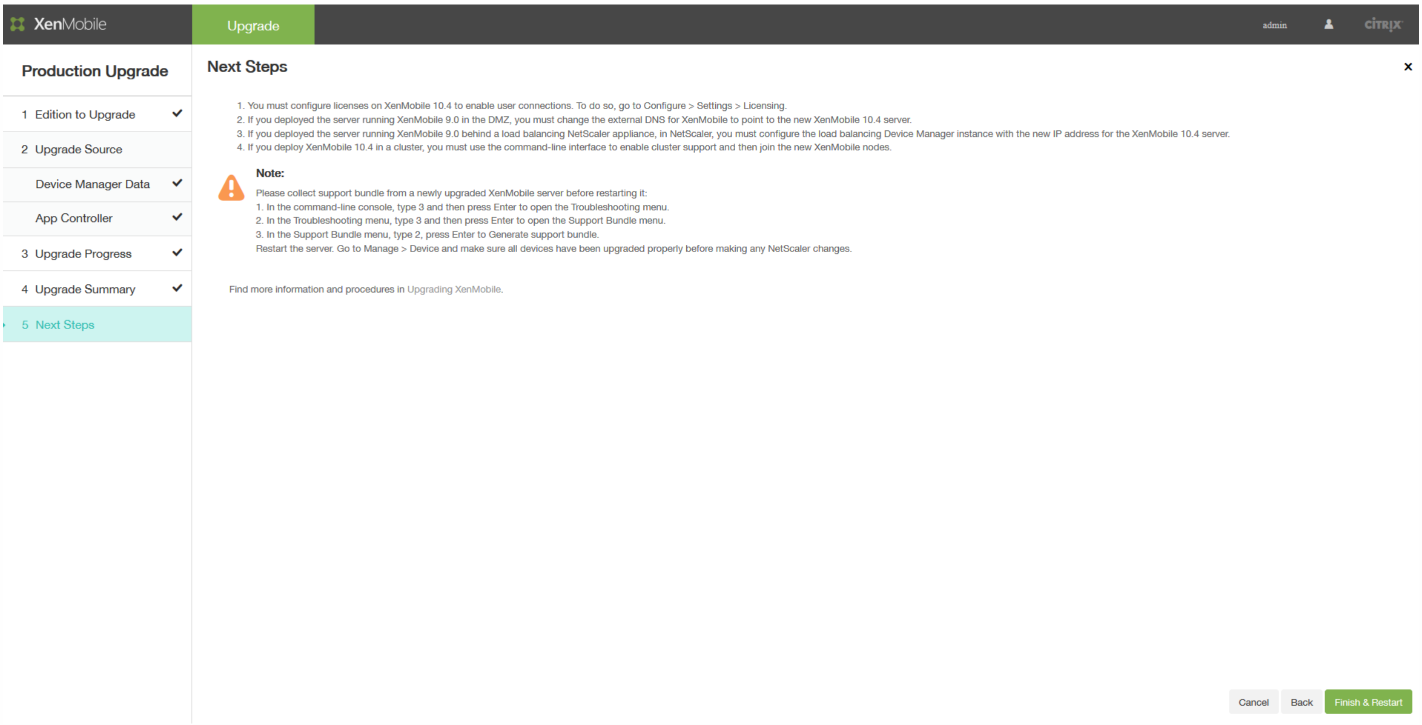
Review the upgrade results and debug logs to ensure that all data upgraded successfully to XenMobile 10.4. Be sure to download the log before continuing.

Devices Upgraded	604
Apps Upgraded	23
Users Upgraded	316
Delivery Groups Upgraded	5

30. Click the **Upgrade log** icon to download the log. Be sure to download the log before leaving this page.

Citrix recommends that you review the log to determine whether any items weren't upgraded to the latest version of XenMobile. Such items include policies, settings, user data, and so on.

31. After you download the upgrade log, click **Next**. The **Next Steps** page appears.



Next Steps

1. You must configure licenses on XenMobile 10.4 to enable user connections. To do so, go to Configure > Settings > Licensing.
2. If you deployed the server running XenMobile 9.0 in the DMZ, you must change the external DNS for XenMobile to point to the new XenMobile 10.4 server.
3. If you deployed the server running XenMobile 9.0 behind a load balancing NetScaler appliance, in NetScaler, you must configure the load balancing Device Manager instance with the new IP address for the XenMobile 10.4 server.
4. If you deploy XenMobile 10.4 in a cluster, you must use the command-line interface to enable cluster support and then join the new XenMobile nodes.

Note:

Please collect support bundle from a newly upgraded XenMobile server before restarting it:
1. In the command-line console, type 3 and then press Enter to open the Troubleshooting menu.
2. In the Troubleshooting menu, type 3 and then press Enter to open the Support Bundle menu.
3. In the Support Bundle menu, type 2, press Enter to Generate support bundle.
Restart the server. Go to Manage > Device and make sure all devices have been upgraded properly before making any NetScaler changes.

Find more information and procedures in Upgrading XenMobile.

For instructions related to those steps, see Upgrade Tool Post-Requisites.

Upgrade Tool post-requisites

Sep 06, 2017

After the Upgrade Tool completes, the tool provides a general list of next steps. The post-requisite tasks for your environment can vary, based on your installed NetScaler version, whether you used the NetScaler for XenMobile wizard to configure NetScaler, and your XenMobile Edition.

Be sure to review the following list of post-requisite tasks and complete all that apply to your environment.

1. Configure licenses on XenMobile to enable user connections. For details, see this procedure.

2. If you deployed the server running XenMobile 9.0 in the DMZ, change the external DNS for XenMobile to point to the new XenMobile server instance.

3. If you deployed the server running XenMobile 9.0 behind a load balancing NetScaler appliance, make the following changes on NetScaler:

    a. Configure a new load balancing virtual server for the upgrade. For details, see this procedure.

    b. Configure an address record to point the App Controller server FQDN to the new load balancer for the upgrade. For details, see this procedure.

    c. Change the Device Manager load balancing virtual server to point to the new XenMobile server IP address. For details, see this procedure.

    d. Change the NetScaler Gateway to point to the new XenMobile server FQDN. For details, see this procedure.

    e. The following tasks are required only in these cases:

        - If you used the NetScaler for XenMobile wizard 9 with NetScaler 11.1, 11.0, or 10.5; or

        - If you're using NetScaler Gateway 10.1 (which is not recommended); or

        - If you didn't use the NetScaler for XenMobile wizard when configuring NetScaler 10.5 or later for XenMobile.

    For the procedures that you should follow for the preceding cases, see the following articles in XenMobile Upgrade Tool 10.1 documentation:

        Create a new MAM Load Balancing Virtual Server Based on an SSL Bridge MDM Configuration
        Create a new MAM Load Balancing Virtual Server Based on an SSL Offload MDM Configuration

4. If you deploy the latest version of XenMobile in a cluster, you must use the XenMobile command-line interface (CLI) to enable cluster support and then join the new XenMobile nodes. For help with the XenMobile CLI, see Clustering Menu Options.

5. Complete the remaining post-requisites, as required for your environment.

This article also covers post-requisites for settings related to Secure Ticket Authority, Network Time Protocol (NTP) server, XenMobile server host name, update information that did not upgrade, custom store name, and XenMobile device enrollment after upgrade.

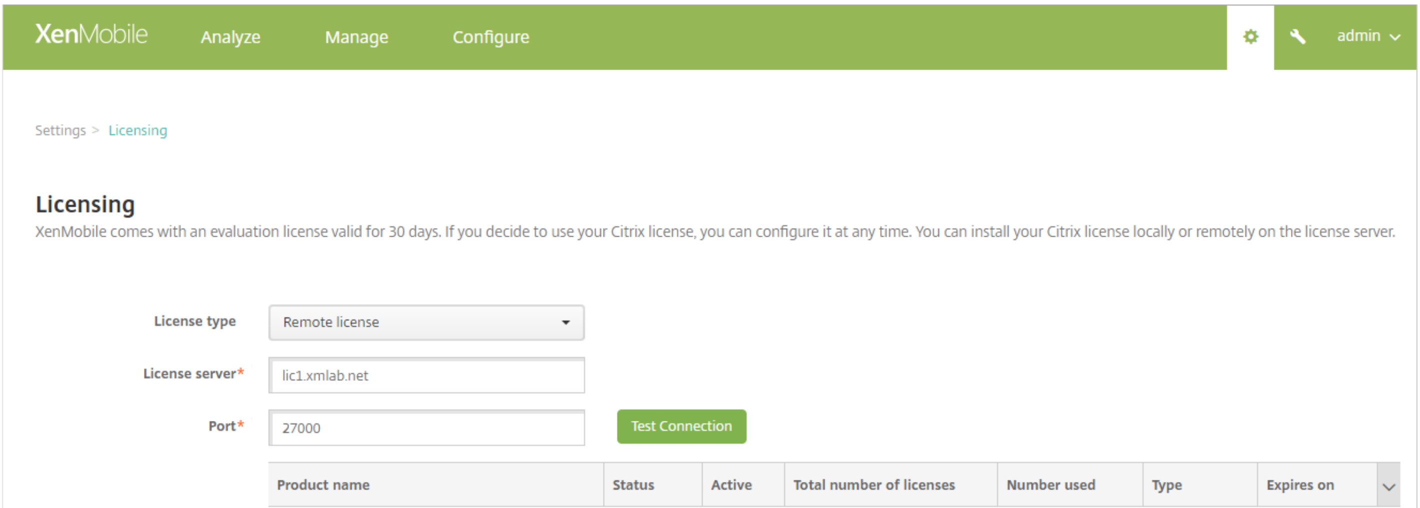
The latest versions of XenMobile only support Citrix V6 licensing. You must set the local or remote license configuration in the new XenMobile console to enable user connections, as follows.

1. Download the license file. To do so, see Citrix Licensing.

2. Log on to the new XenMobile console: Go to https://<XenMobile-server-IP-address>:4443.

- For MDM or ENT upgrades, log on with your XenMobile 9.0 Device Manager administrator credentials.
- For MAM upgrades, log on with your XenMobile 9.0 App Controller administrator credentials.

3. Go to **Settings > Licensing**.



Licensing

XenMobile comes with an evaluation license valid for 30 days. If you decide to use your Citrix license, you can configure it at any time. You can install your Citrix license locally or remotely on the license server.

License type: Remote license

License server*: lic1.xmlab.net

Port*: 27000

Test Connection

Product name	Status	Active	Total number of licenses	Number used	Type	Expires on

For more details about adding local and remote licenses, see Licensing.

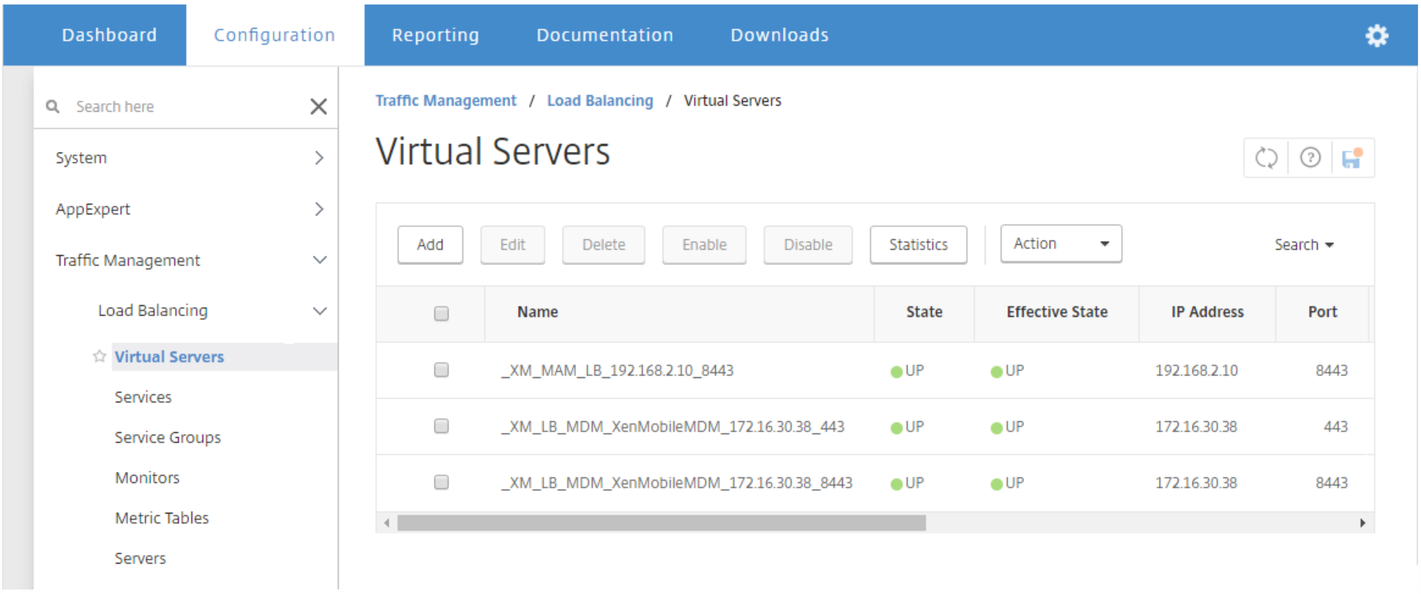
Important

This post-requisite is required *only* when you upgrade a XenMobile Enterprise Edition production upgrade; it is not required for MAM or MDM upgrades.

After a XenMobile Enterprise Edition production upgrade to the latest version of XenMobile, you must configure a new load balancing virtual server for the XenMobile 9.0 App Controller FQDN. To do that, you use the NetScaler Gateway configuration tool.

The example screens in this section, for NetScaler Gateway 11.1, are similar to NetScaler Gateway versions 11.0 and 10.5.

1. Click **Traffic Management > Load Balancing > Virtual Servers**.



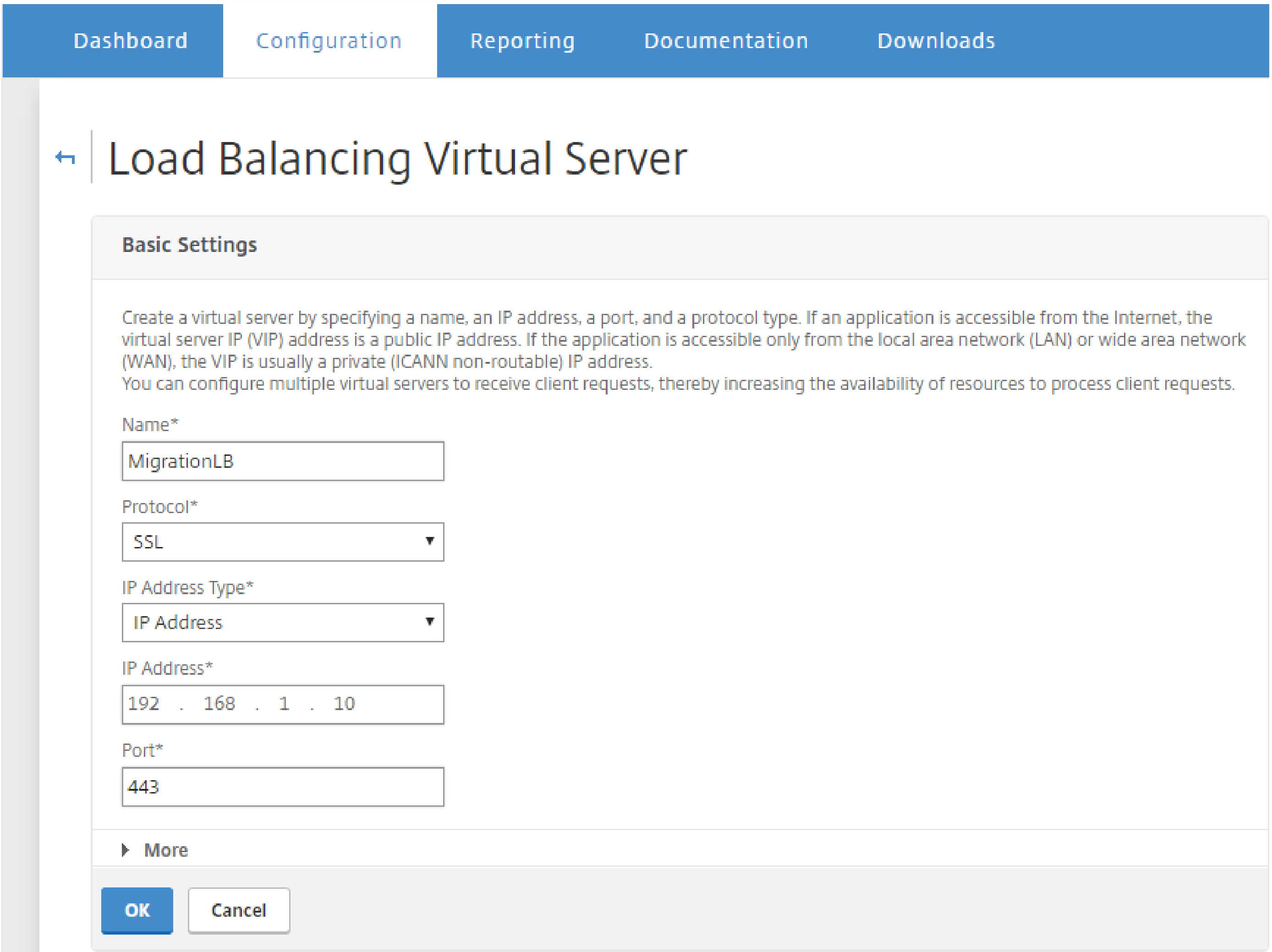
Traffic Management / Load Balancing / Virtual Servers

Virtual Servers

□	Name	State	Effective State	IP Address	Port
□	_XM_MAM_LB_192.168.2.10_8443	● UP	● UP	192.168.2.10	8443
□	_XM_LB_MDM_XenMobileMDM_172.16.30.38_443	● UP	● UP	172.16.30.38	443
□	_XM_LB_MDM_XenMobileMDM_172.16.30.38_8443	● UP	● UP	172.16.30.38	8443

2. Click **Add**.

3. On the **Load Balancing Virtual Server** page, configure the following settings and then click **OK**.



Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.
You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name*
MigrationLB

Protocol*
SSL

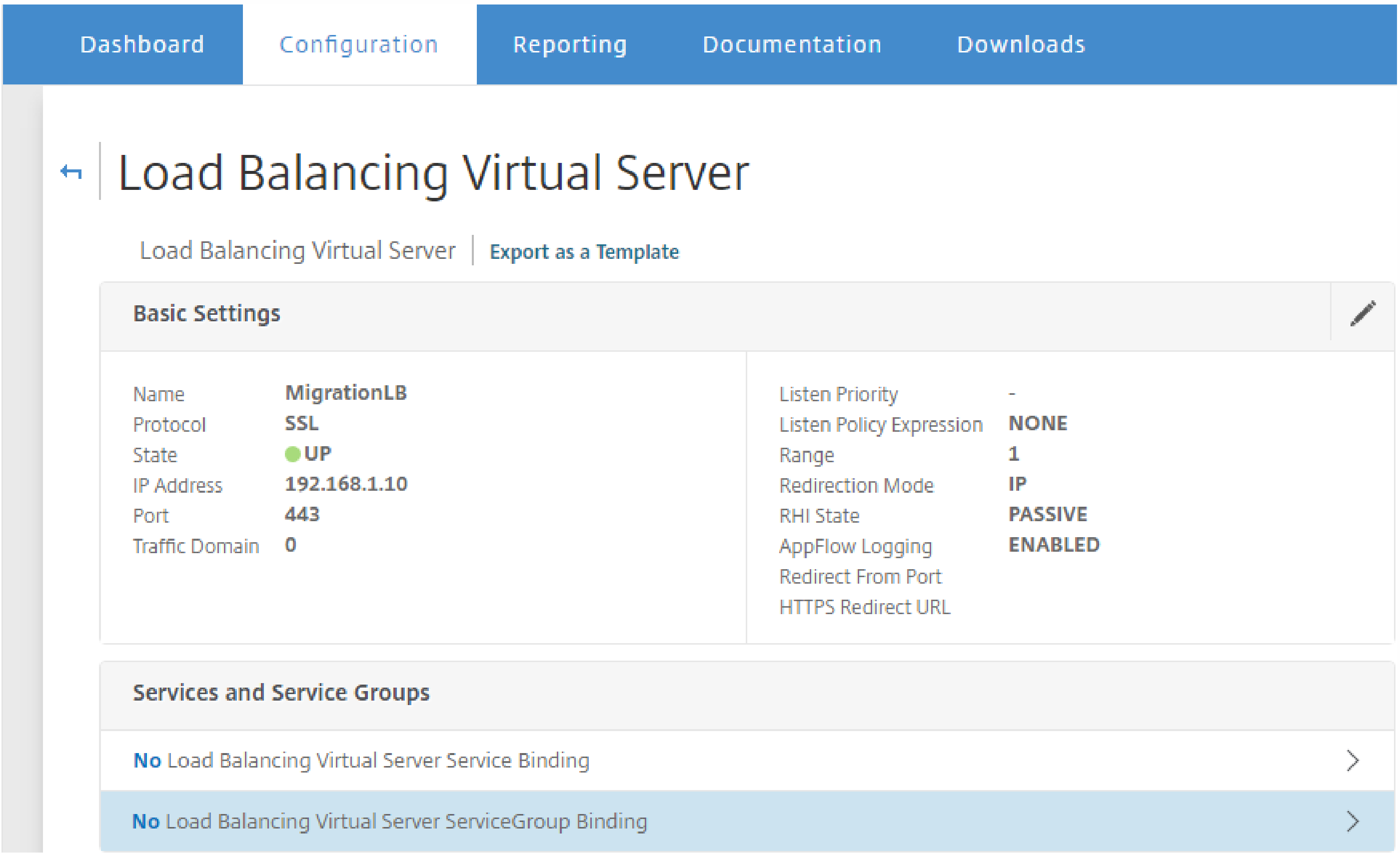
IP Address Type*
IP Address

IP Address*
192 . 168 . 1 . 10

Port*
443

- **Name**: Type a name for the new load balancer.
- **Protocol**: Set to **SSL**. The default is **HTTP**.
- **IP Address**: Enter an IP address for the new load balancer, which follows RFC 1918; for example 192.168.1.10.
- **Port**: Set to **443**.

4. Under **Services and Service Groups**, click **No Load Balancing Virtual Server Service Group Binding**.



Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

Basic Settings

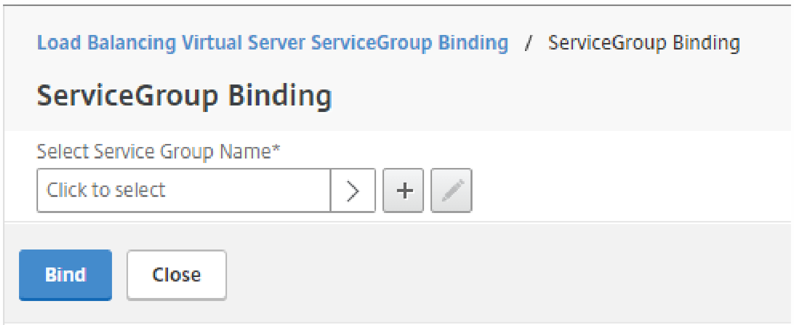
Name	MigrationLB	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	● UP	Range	1
IP Address	192.168.1.10	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED
		Redirect From Port	
		HTTPS Redirect URL	

Services and Service Groups

No Load Balancing Virtual Server Service Binding

No Load Balancing Virtual Server ServiceGroup Binding

5. Under **Select Service Group Name**, click **Click to Select**.

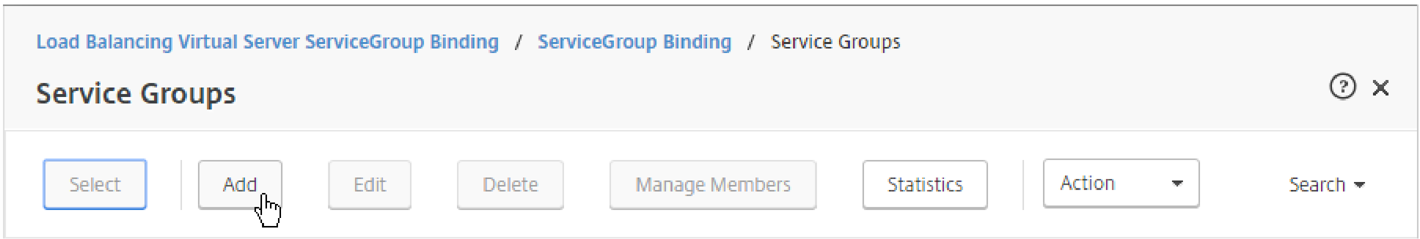

Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding

ServiceGroup Binding

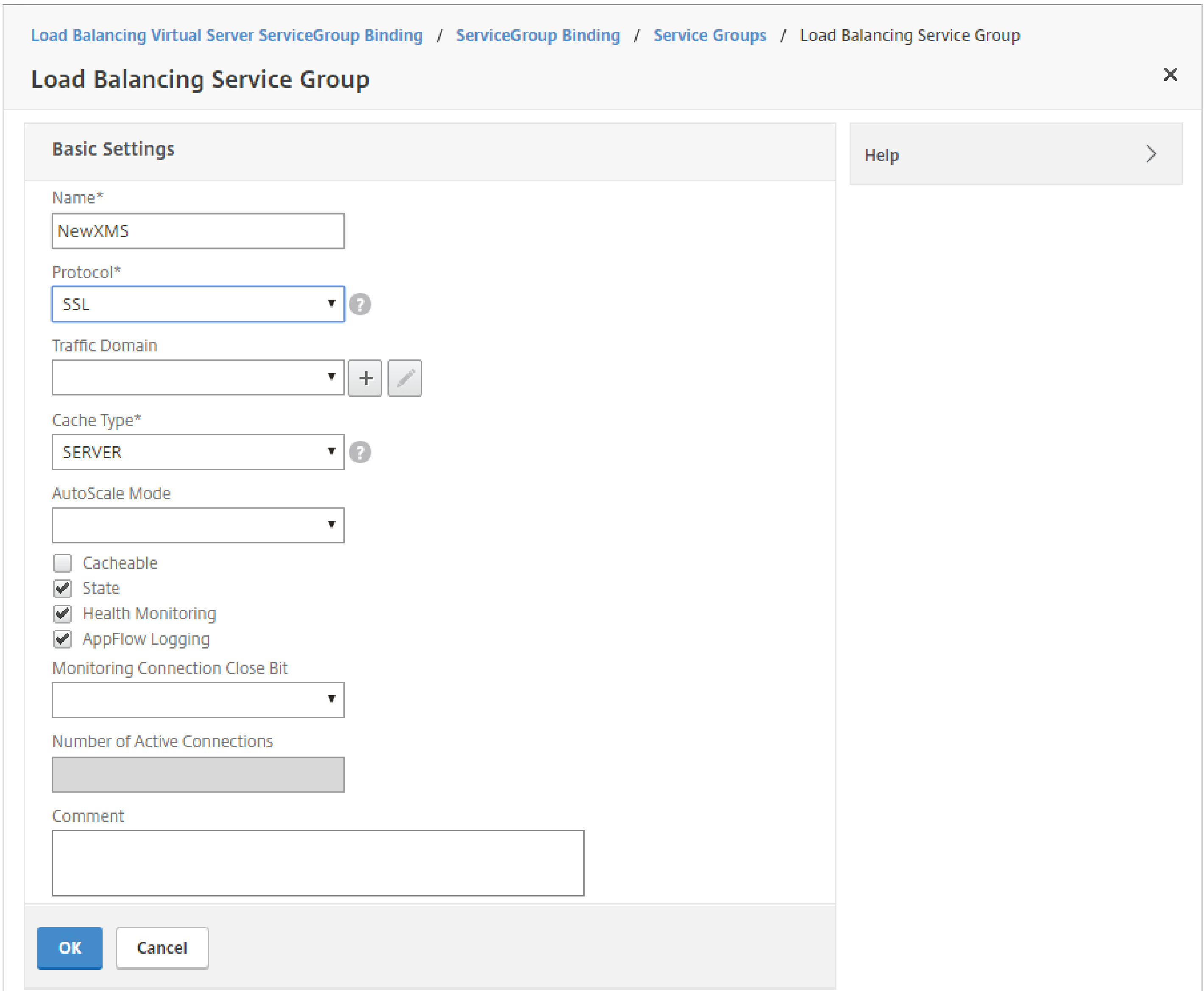
Select Service Group Name*

Click to select

6. Click **Add** to create a new service group.


Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding / Service Groups
Service Groups
Select
Add
Edit
Delete
Manage Members
Statistics
Action
Search

7. On the **Load Balancing Service Group** page, type a name for the new service group, make sure the protocol is set to **SSL**, and then click **OK**.


Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding / Service Groups / Load Balancing Service Group
Load Balancing Service Group
Help
OK
Cancel

Basic Settings

Name*: NewXMS

Protocol*: SSL

Traffic Domain:

Cache Type*: SERVER

AutoScale Mode:

□ Cacheable

☑ State

☑ Health Monitoring

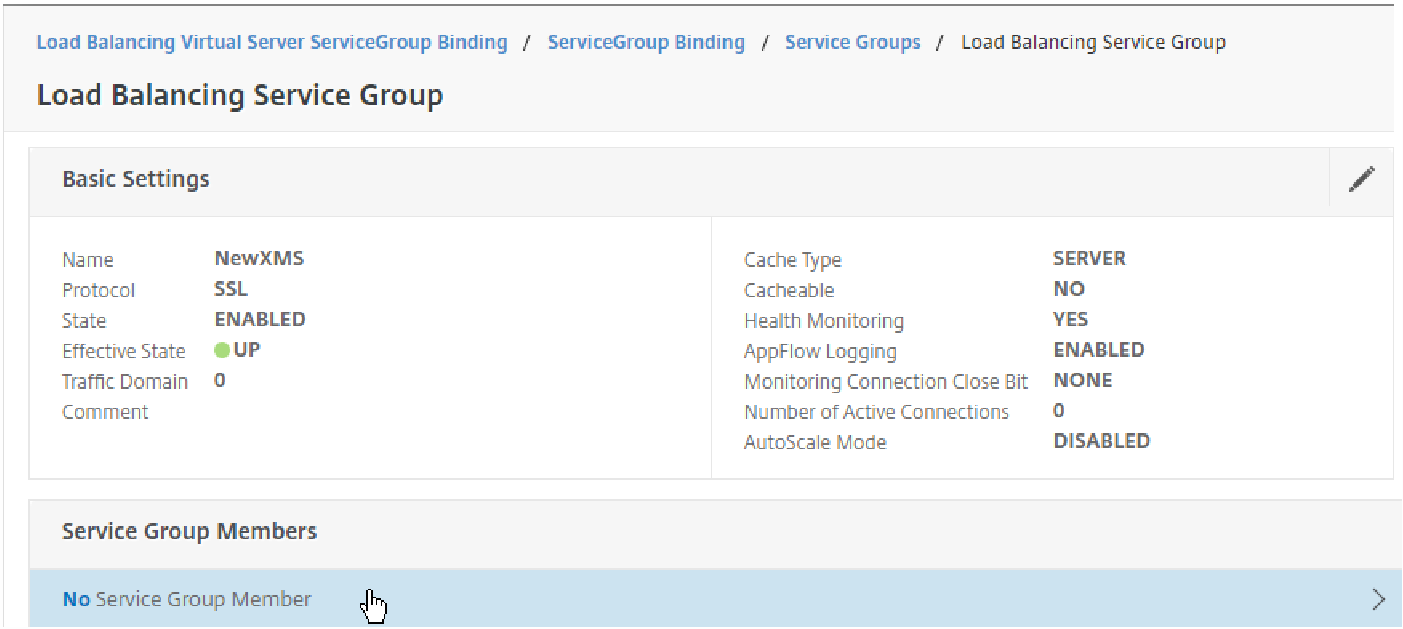
☑ AppFlow Logging

Monitoring Connection Close Bit:

Number of Active Connections:

Comment:

8. Click **No Service Group Member**.



Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding / Service Groups / Load Balancing Service Group

Load Balancing Service Group

Basic Settings

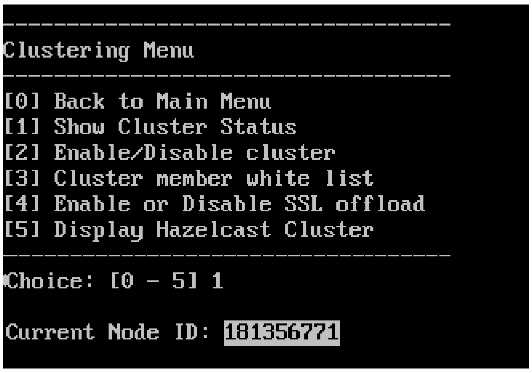
Name	NewXMS	Cache Type	SERVER
Protocol	SSL	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Effective State	● UP	AppFlow Logging	ENABLED
Traffic Domain	0	Monitoring Connection Close Bit	NONE
Comment		Number of Active Connections	0
		AutoScale Mode	DISABLED

Service Group Members

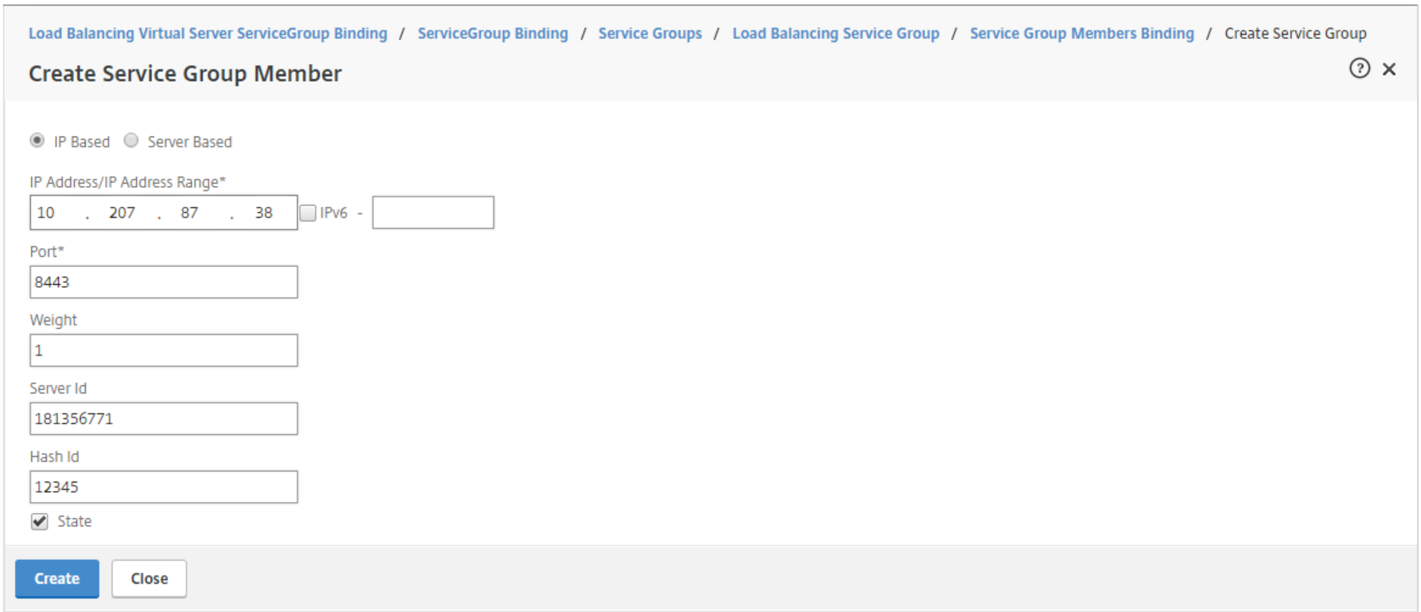
No Service Group Member

9. On the **Create Service Group Member** page, configure the following settings:

- **IP Address/IP Address Range**: Enter the IP address for the new XenMobile server instance.
- **Port**: Set to **8443**.
- **Server ID**: If you are migrating from a clustered XenMobile 9.0 environment to a new XenMobile clustered environment, enter the server node ID for the current XenMobile server. To obtain the server node ID, log on to the XenMobile server command-line interface (CLI) and type **1** to go to the **Clustering** menu. The server node ID in the CLI is labelled **Current Node ID**.



```
-----------------------------------
Clustering Menu
-----------------------------------
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----------------------------------
Choice: [0 - 5] 1

Current Node ID: 181356771
```


Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding / Service Groups / Load Balancing Service Group / Service Group Members Binding / Create Service Group

Create Service Group Member

● IP Based ○ Server Based

IP Address/IP Address Range*: 10 . 207 . 87 . 38 □ IPv6 -

Port*: 8443

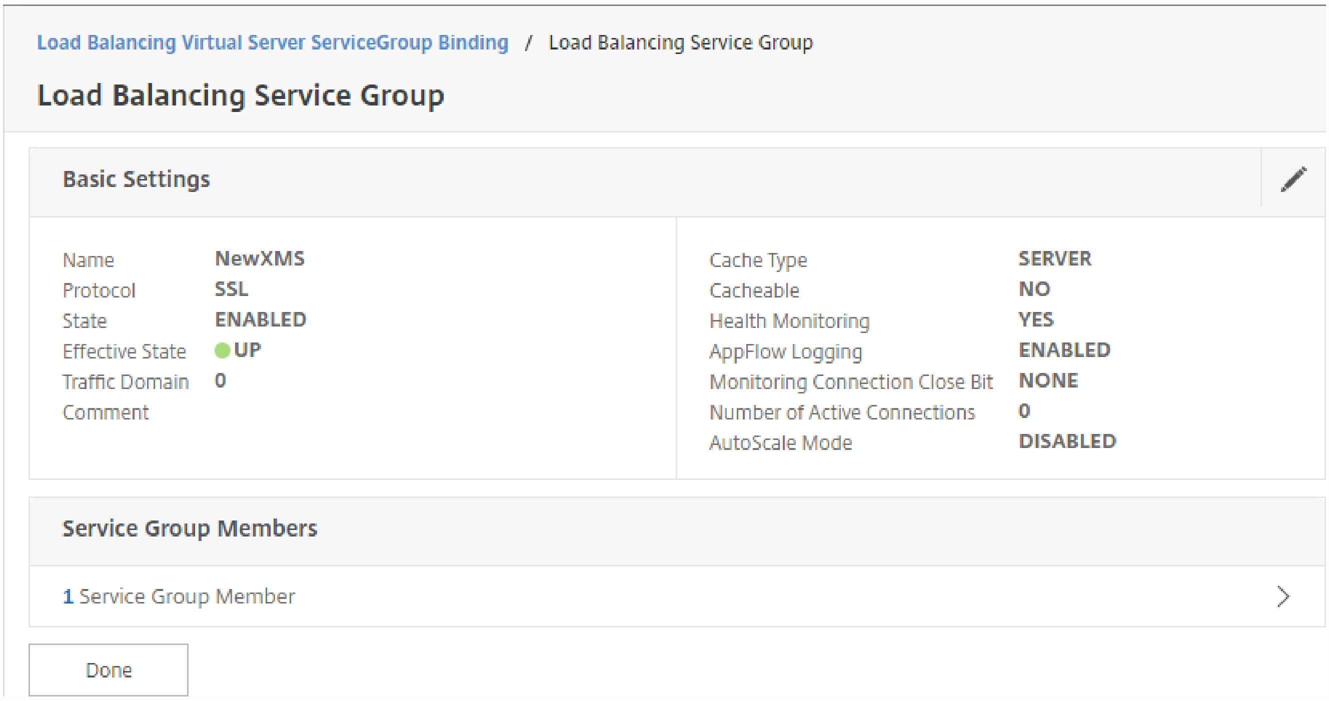
Weight: 1

Server Id: 181356771

Hash Id: 12345

☑ State

10. Click **Create** and then click **Done**.


Load Balancing Virtual Server ServiceGroup Binding / Load Balancing Service Group

Load Balancing Service Group

Basic Settings

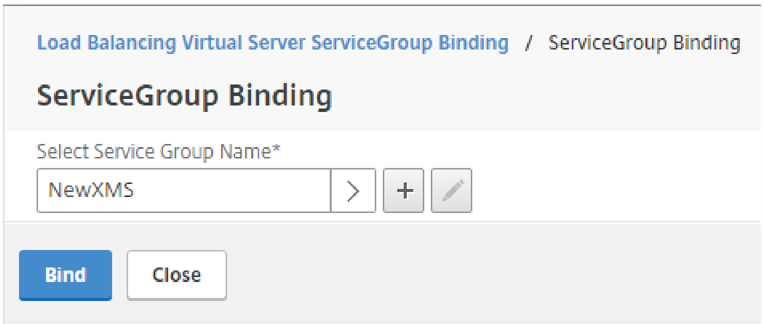
Name	NewXMS	Cache Type	SERVER
Protocol	SSL	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Effective State	● UP	AppFlow Logging	ENABLED
Traffic Domain	0	Monitoring Connection Close Bit	NONE
Comment		Number of Active Connections	0
		AutoScale Mode	DISABLED

Service Group Members

1 Service Group Member

11. Click **Done** and then **OK**.

12. Click **Bind** and then on the next screen, click **Done**.



Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding

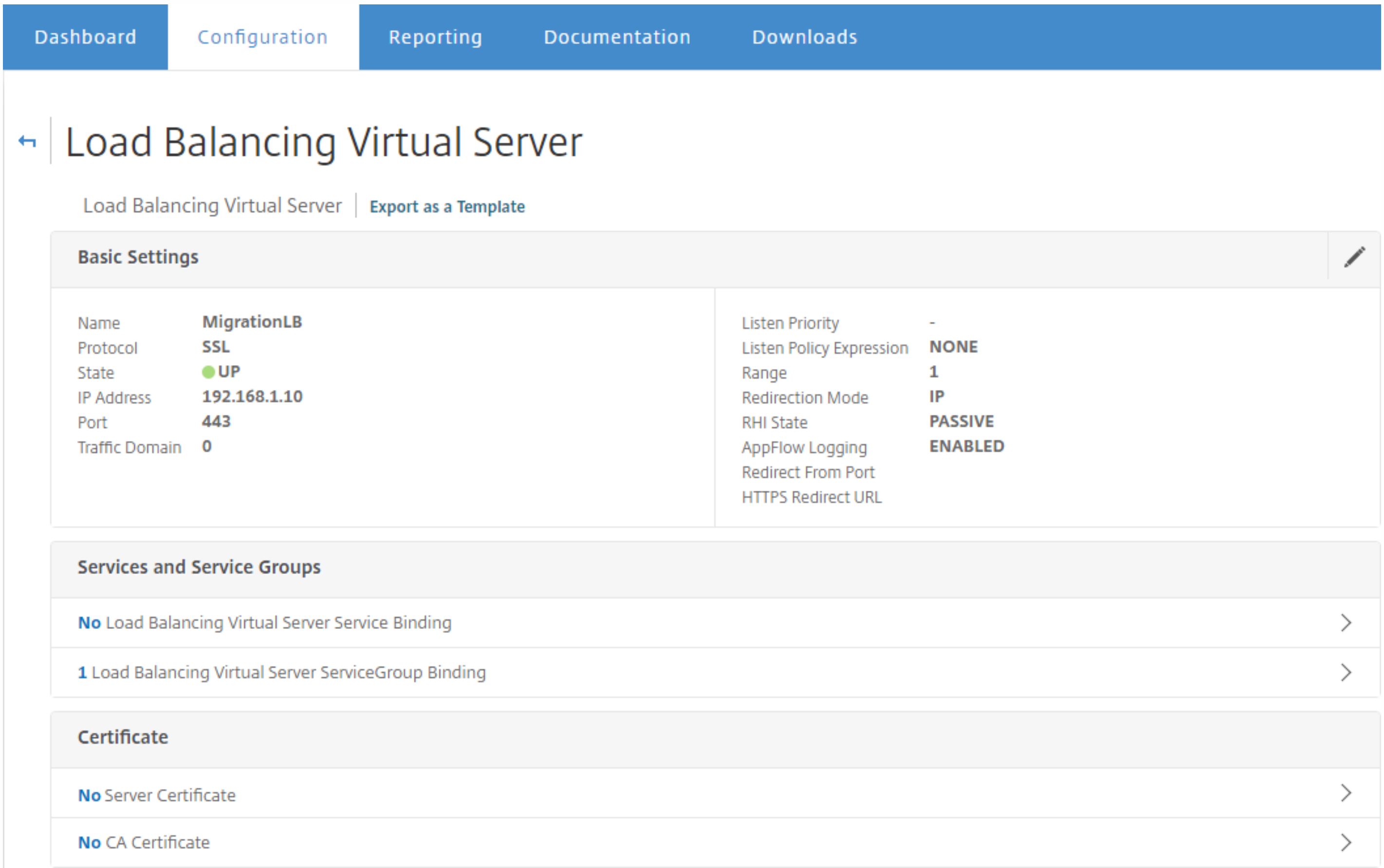
ServiceGroup Binding

Select Service Group Name*

NewXMS

Bind Close

13. Under **Certificates**, click **No Server Certificate**.



Dashboard | Configuration | Reporting | Documentation | Downloads

Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

Basic Settings

Name	MigrationLB	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	● UP	Range	1
IP Address	192.168.1.10	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED
		Redirect From Port	
		HTTPS Redirect URL	

Services and Service Groups

No Load Balancing Virtual Server Service Binding

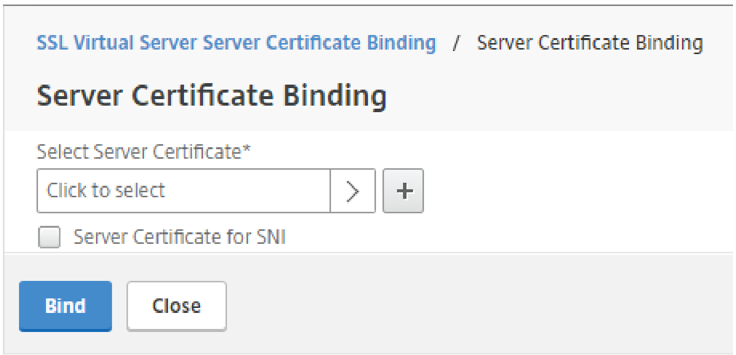
1 Load Balancing Virtual Server ServiceGroup Binding

Certificate

No Server Certificate

No CA Certificate

14. Under **Server Certificate Binding**, click **Click to Select**.



SSL Virtual Server Server Certificate Binding / Server Certificate Binding

Server Certificate Binding

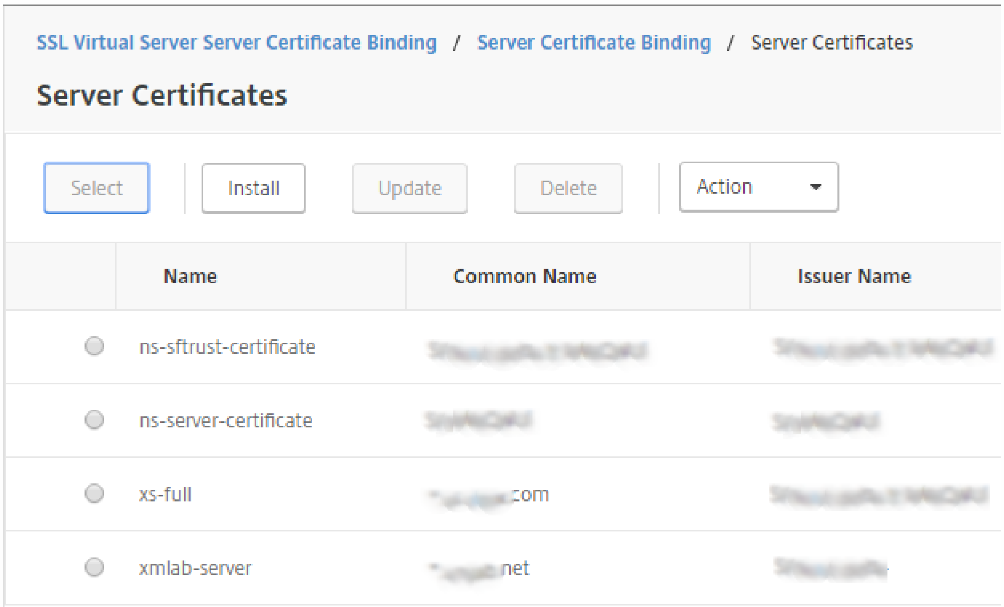
Select Server Certificate*

Click to select

□ Server Certificate for SNI

Bind Close

15. Under **Certificates**, click the XenMobile 9.0 server certificate you exported in Upgrade Tool prerequisites and then click **OK**.

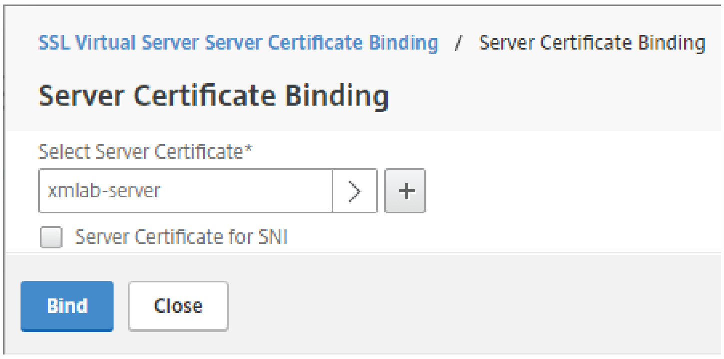


SSL Virtual Server Server Certificate Binding / Server Certificate Binding / Server Certificates

Server Certificates

	Name	Common Name	Issuer Name
○	ns-sftrust-certificate	[redacted]	[redacted]
○	ns-server-certificate	[redacted]	[redacted]
○	xs-full	*[redacted].com	[redacted]
○	xmlab-server	*[redacted].net	[redacted]

16. Click **Bind** and then on the next screen, click **Done**.

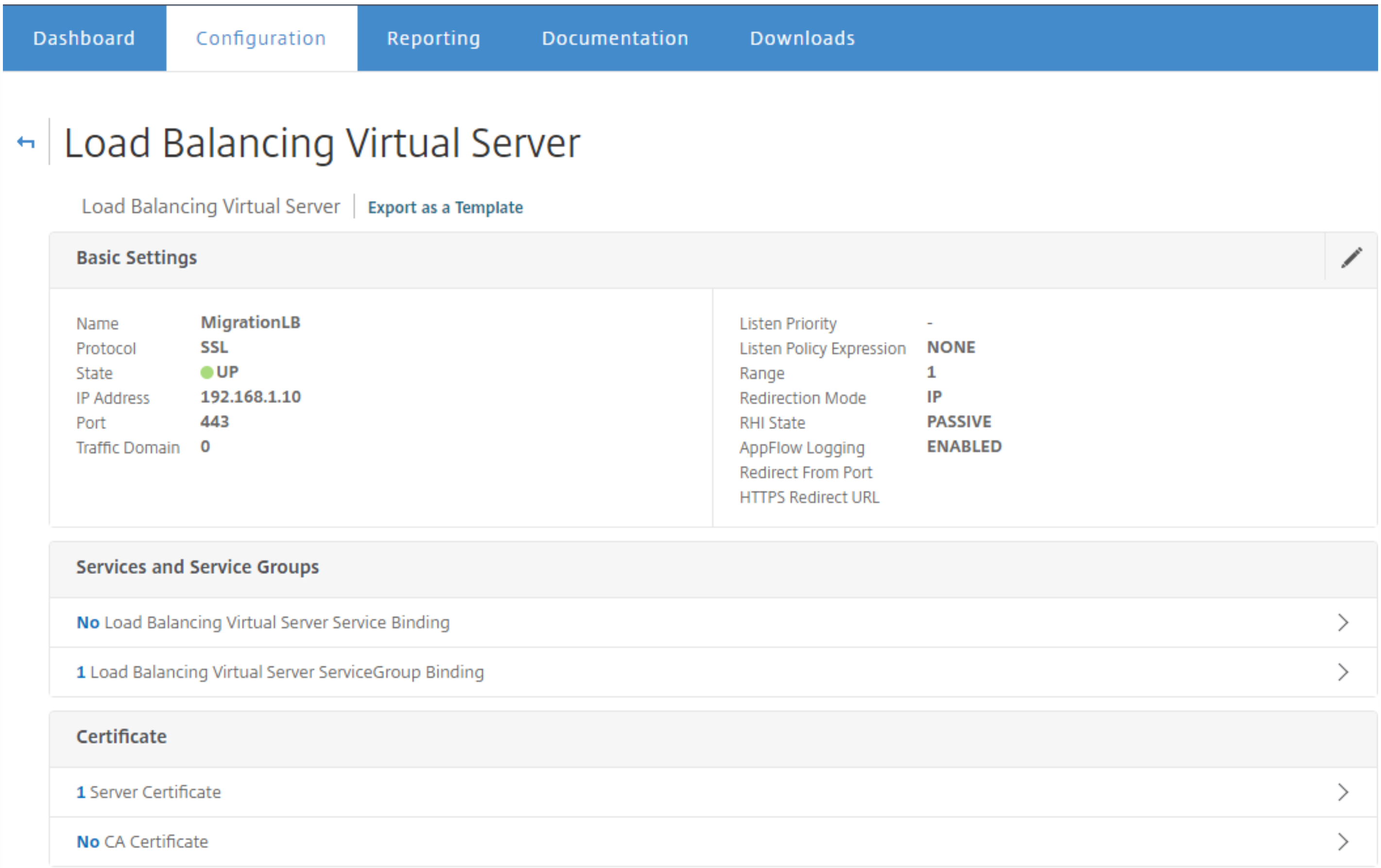


SSL Virtual Server Server Certificate Binding / Server Certificate Binding

Server Certificate Binding

Select Server Certificate*: xmlab-server

□ Server Certificate for SNI



Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

Basic Settings

Name MigrationLB
Protocol SSL
State ● UP
IP Address 192.168.1.10
Port 443
Traffic Domain 0

Listen Priority -
Listen Policy Expression NONE
Range 1
Redirection Mode IP
RHI State PASSIVE
AppFlow Logging ENABLED
Redirect From Port
HTTPS Redirect URL

Services and Service Groups

No Load Balancing Virtual Server Service Binding

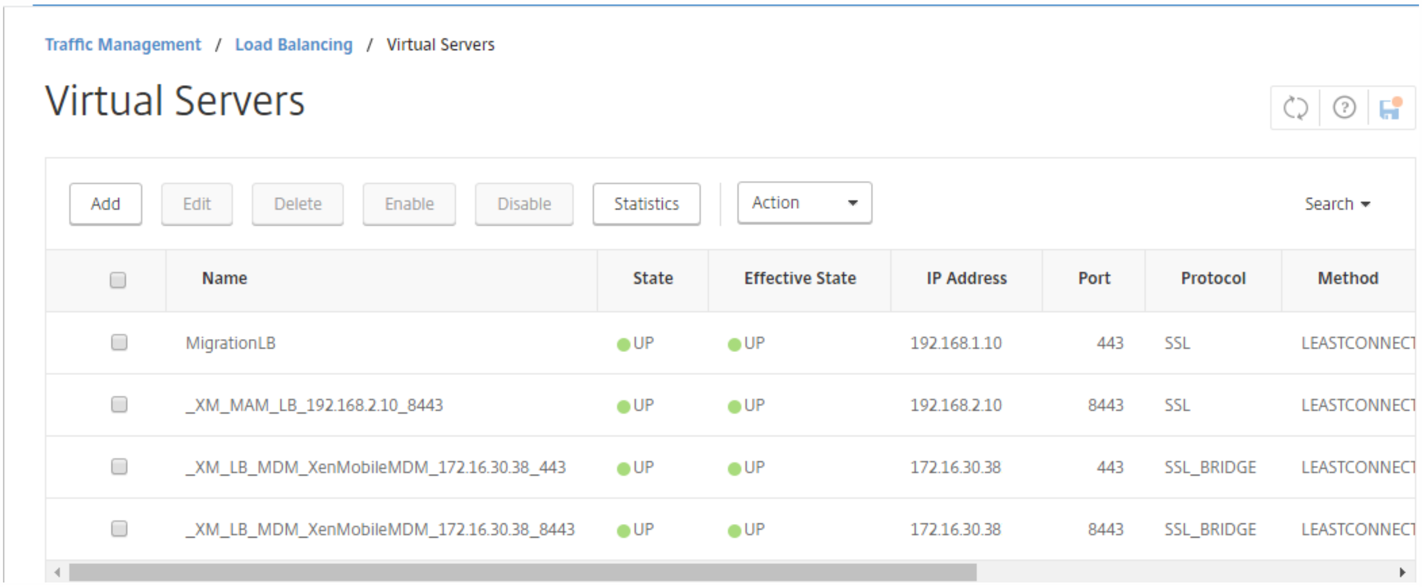
1 Load Balancing Virtual Server ServiceGroup Binding

Certificate

1 Server Certificate

No CA Certificate

17. Click the refresh button to confirm that the server is up.



Traffic Management / Load Balancing / Virtual Servers

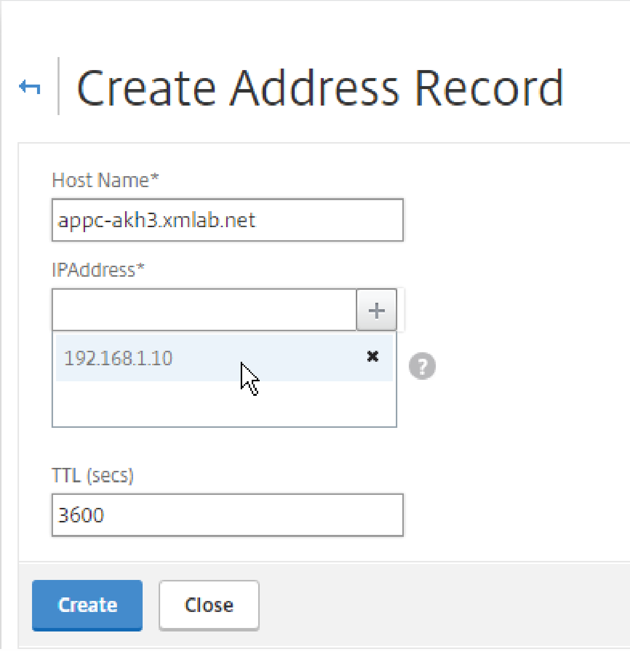
Virtual Servers

□	Name	State	Effective State	IP Address	Port	Protocol	Method
□	MigrationLB	● UP	● UP	192.168.1.10	443	SSL	LEASTCONNECT
□	_XM_MAM_LB_192.168.2.10_8443	● UP	● UP	192.168.2.10	8443	SSL	LEASTCONNECT
□	_XM_LB_MDM_XenMobileMDM_172.16.30.38_443	● UP	● UP	172.16.30.38	443	SSL_BRIDGE	LEASTCONNECT
□	_XM_LB_MDM_XenMobileMDM_172.16.30.38_8443	● UP	● UP	172.16.30.38	8443	SSL_BRIDGE	LEASTCONNECT

1. Log on to NetScaler, click **Traffic Management > DNS > Records > Address Records**, and then click **Add**.

Note

If you have a Global Server Load Balancing configuration, adding an address record causes the Global Server Load Balancing system to respond authoritatively for that server with the local IP address.



Create Address Record

Host Name*: appc-akh3.xmlab.net

IPAddress*: 192.168.1.10

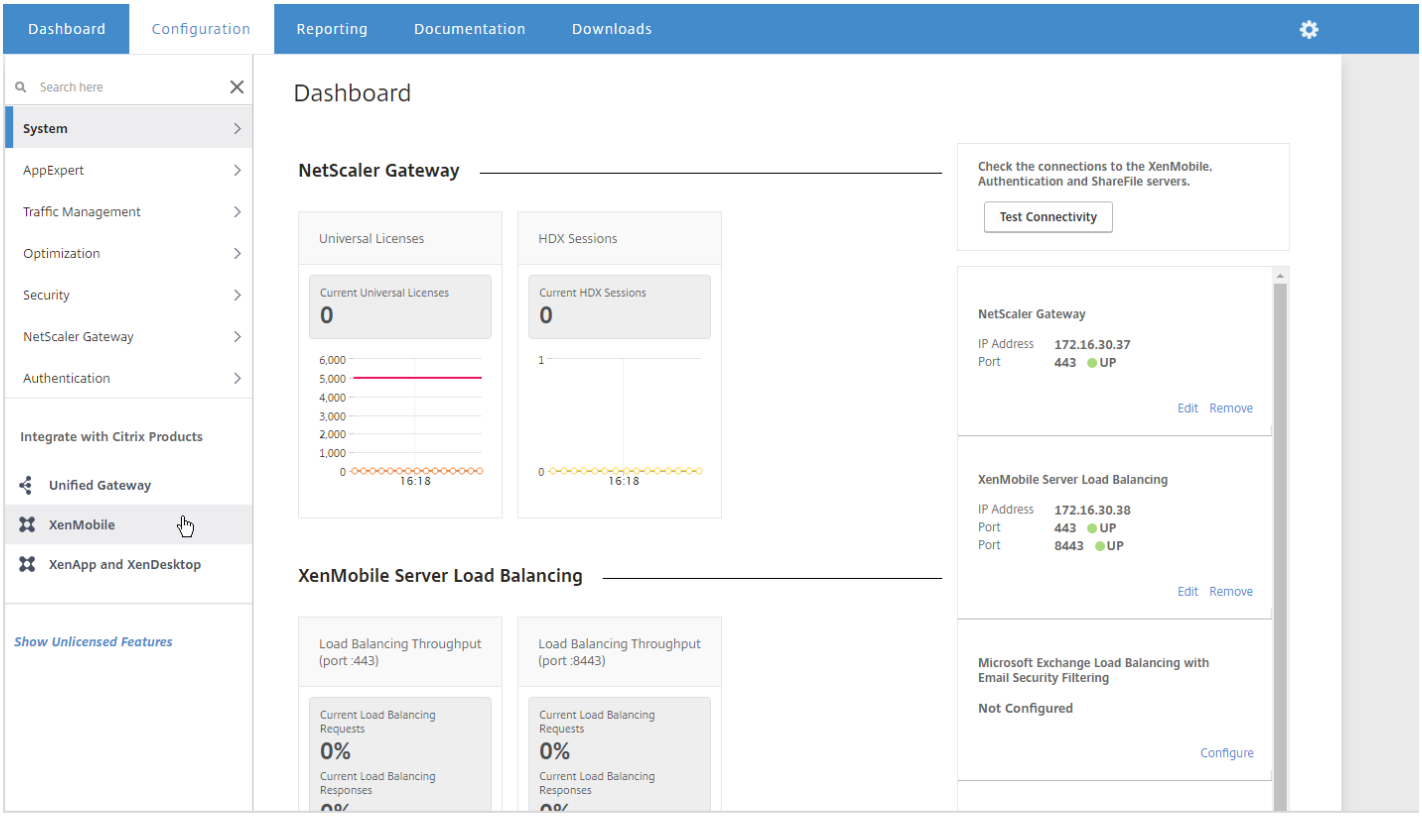
TTL (secs): 3600

If you deployed the server running XenMobile 9.0 behind a load balancing NetScaler appliance, you must configure the load balancing XenMobile 9.0 Device Manager instance in NetScaler with the new IP address for the new XenMobile server instance.

The procedure differs depending on whether you're using NetScaler 11.1 or NetScaler versions 11.0 or 10.5.

For NetScaler 11.1

1. Under **Integrate with Citrix Products**, click **XenMobile**.



Dashboard

NetScaler Gateway

Current Universal Licenses 0

Current HDX Sessions 0

XenMobile Server Load Balancing

Current Load Balancing Requests 0%

Current Load Balancing Responses 0%

Current Load Balancing Requests 0%

Current Load Balancing Responses 0%

Check the connections to the XenMobile, Authentication and ShareFile servers.

NetScaler Gateway

IP Address	172.16.30.37
Port	443 ● UP

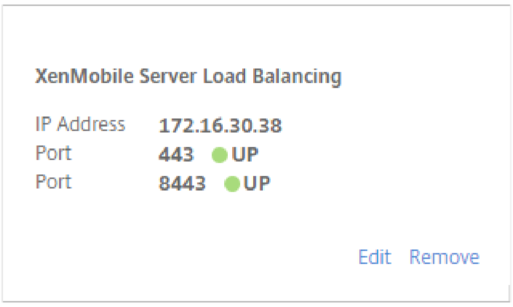
XenMobile Server Load Balancing

IP Address	172.16.30.38
Port	443 ● UP
Port	8443 ● UP

Microsoft Exchange Load Balancing with Email Security Filtering

Not Configured

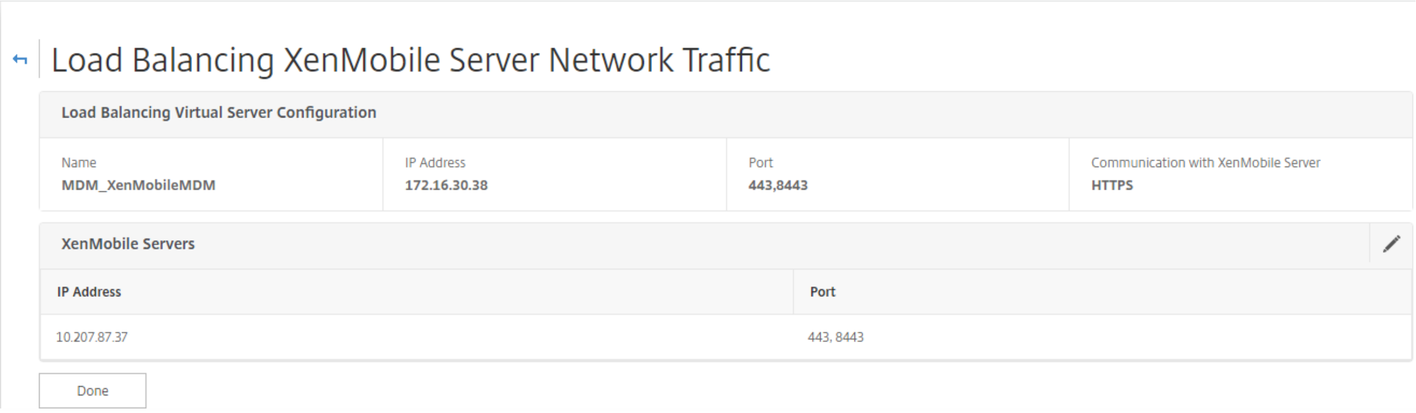
2. On the right side of the screen, under **XenMobile Server Load Balancing**, click **Edit**.



XenMobile Server Load Balancing

IP Address	172.16.30.38
Port	443 ● UP
Port	8443 ● UP

The **Load Balancing XenMobile Server Network Traffic** page appears.



Load Balancing XenMobile Server Network Traffic

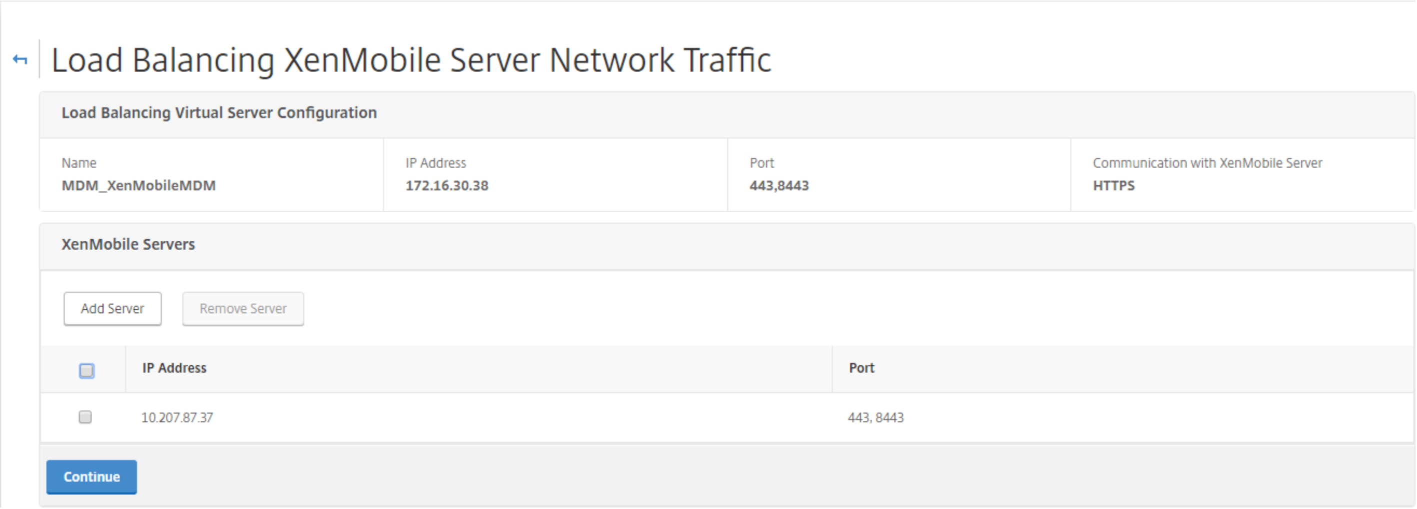
Load Balancing Virtual Server Configuration

Name	IP Address	Port	Communication with XenMobile Server
MDM_XenMobileMDM	172.16.30.38	443,8443	HTTPS

XenMobile Servers

IP Address	Port
10.207.87.37	443, 8443

3. Click the pen icon for XenMobile Servers to open those settings.



Load Balancing XenMobile Server Network Traffic

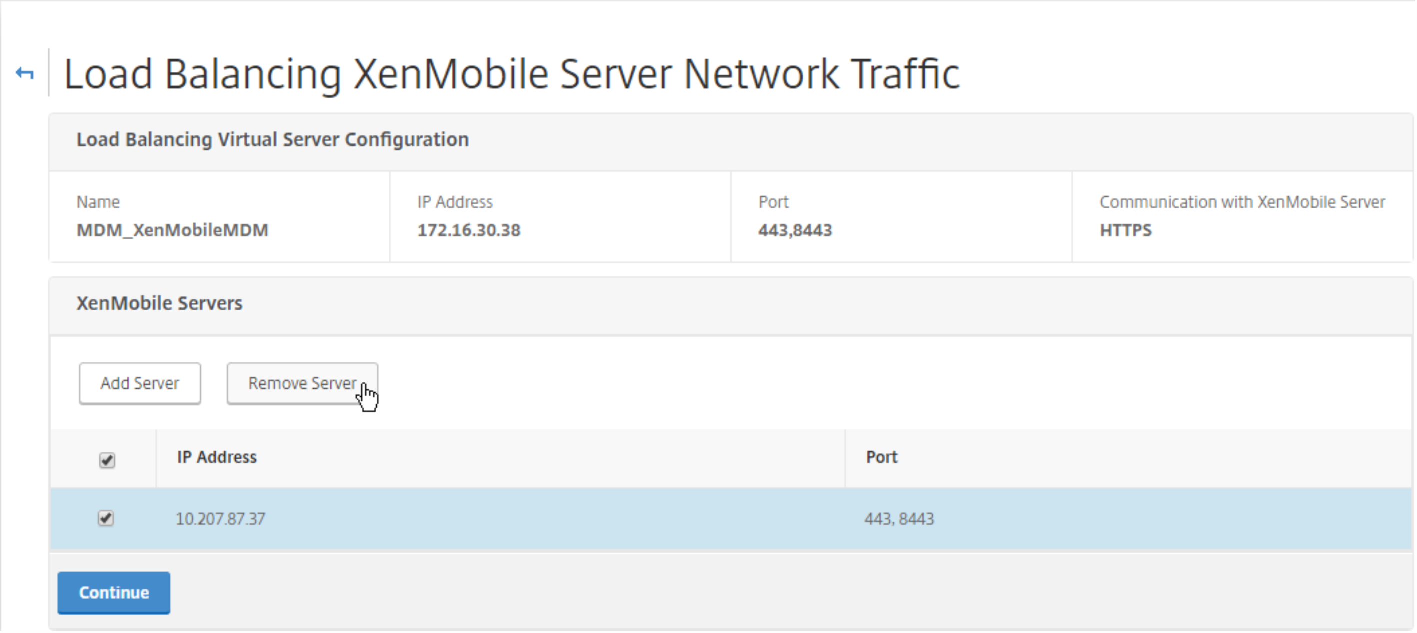
Load Balancing Virtual Server Configuration

Name	IP Address	Port	Communication with XenMobile Server
MDM_XenMobileMDM	172.16.30.38	443,8443	HTTPS

XenMobile Servers

□	IP Address	Port
□	10.207.87.37	443, 8443

4. Select the 9.0 Device Manager server IP address and then click **Remove Server**.



Load Balancing XenMobile Server Network Traffic

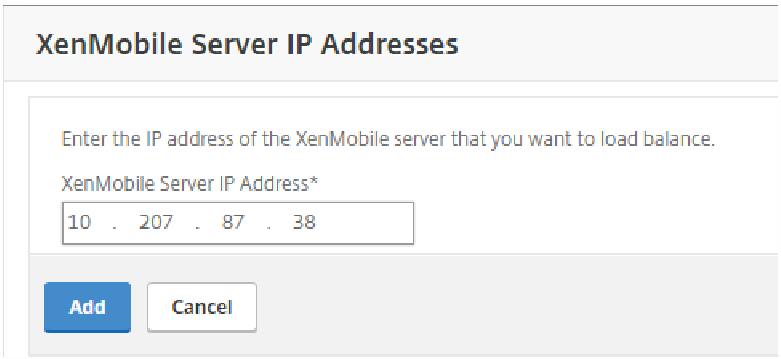
Load Balancing Virtual Server Configuration

Name	IP Address	Port	Communication with XenMobile Server
MDM_XenMobileMDM	172.16.30.38	443,8443	HTTPS

XenMobile Servers

☑	IP Address	Port
☑	10.207.87.37	443, 8443

5. Click **Add Server** and then add the new XenMobile server IP address.



XenMobile Server IP Addresses

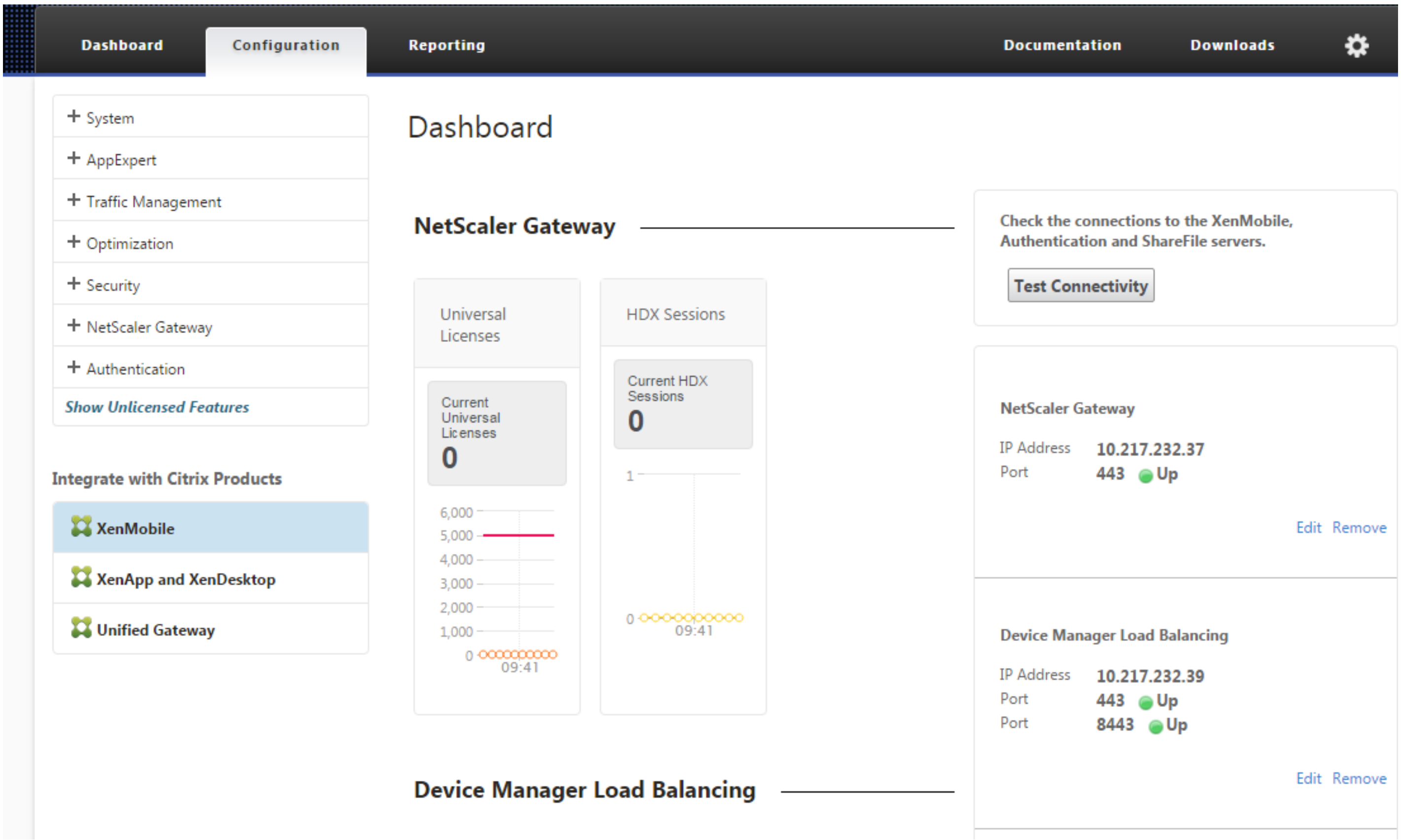
Enter the IP address of the XenMobile server that you want to load balance.

XenMobile Server IP Address*

10 . 207 . 87 . 38

For NetScaler versions 11.0 or 10.5

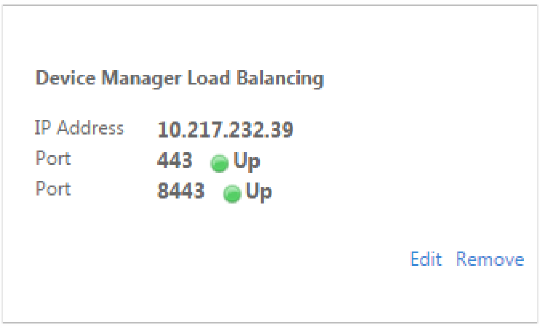
1. Under **Integrate with Citrix Products**, click **XenMobile**.



NetScaler Gateway
IP Address 10.217.232.37
Port 443 Up

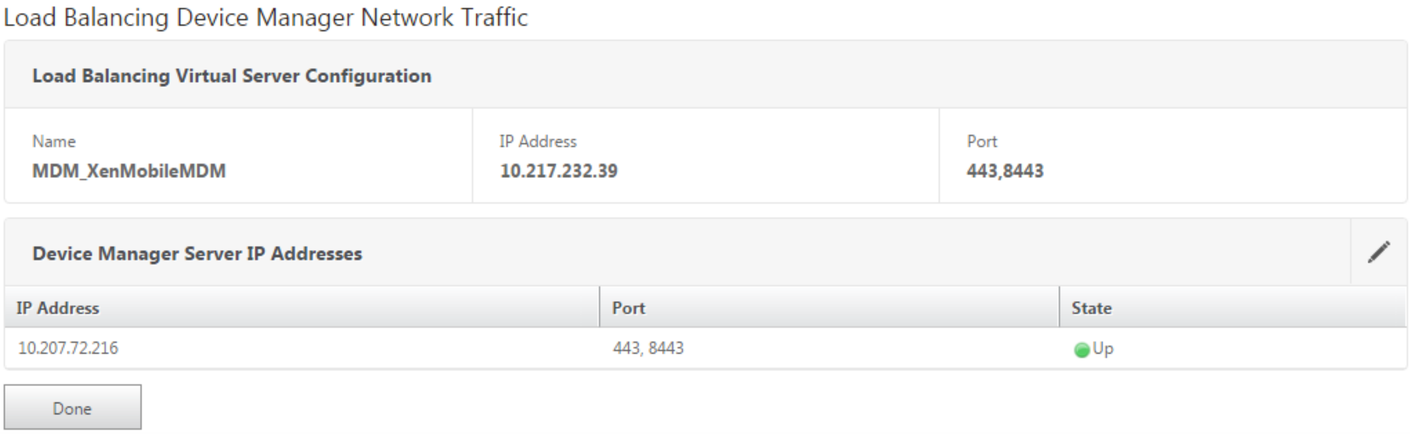
Device Manager Load Balancing
IP Address 10.217.232.39
Port 443 Up
Port 8443 Up

2. On the right side of the screen, under **Device Manager Load Balancing**, click **Edit**.



Device Manager Load Balancing
IP Address 10.217.232.39
Port 443 Up
Port 8443 Up

The **Load Balancing Device Manager Network Traffic** page appears.



Load Balancing Device Manager Network Traffic

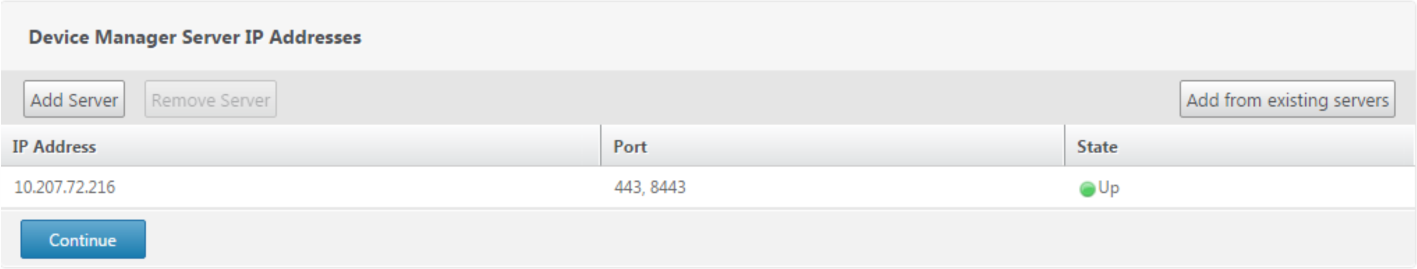
Load Balancing Virtual Server Configuration

Name	IP Address	Port
MDM_XenMobileMDM	**10.217.232.39**	**443,8443**

Device Manager Server IP Addresses

IP Address	Port	State
10.207.72.216	443, 8443	● Up

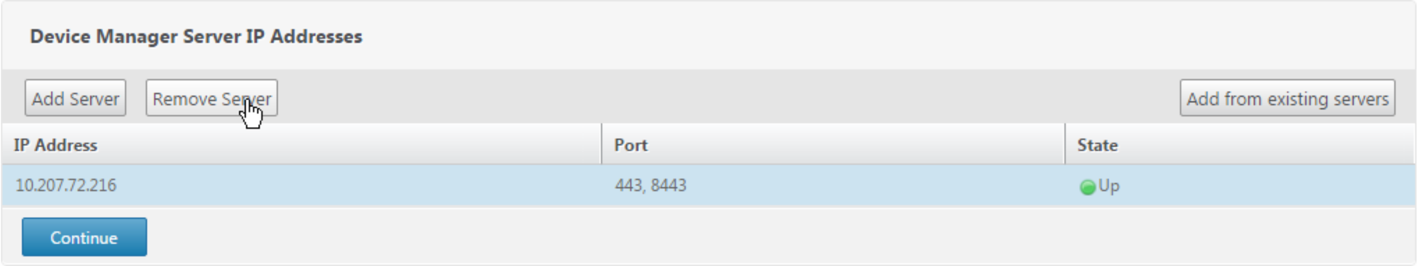
3. Click the pen icon for **Device Manager Server IP Addresses** to open those settings.



Device Manager Server IP Addresses

IP Address	Port	State
10.207.72.216	443, 8443	● Up

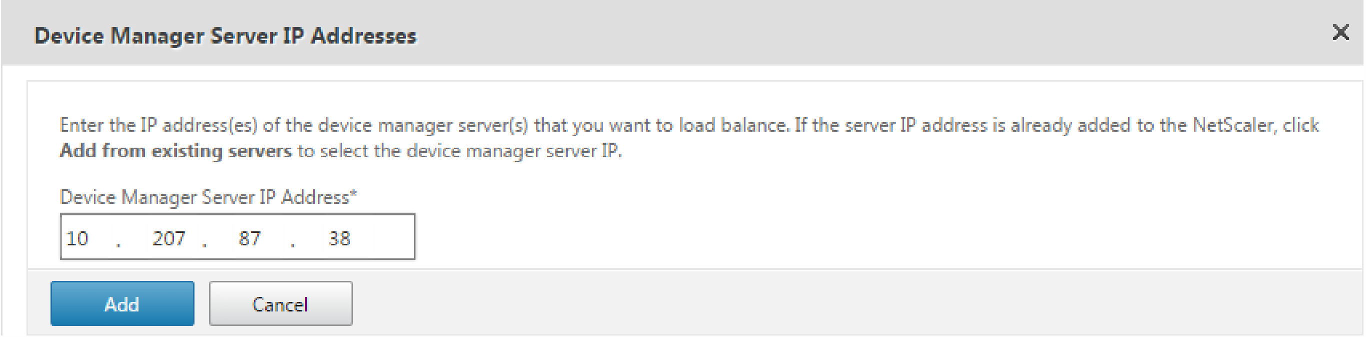
4. Select the 9.0 Device Manager server IP address and then click **Remove Server**.



Device Manager Server IP Addresses

IP Address	Port	State
10.207.72.216	443, 8443	● Up

5. Click **Add Server** and then add the new XenMobile server IP address.



Device Manager Server IP Addresses

Enter the IP address(es) of the device manager server(s) that you want to load balance. If the server IP address is already added to the NetScaler, click **Add from existing servers** to select the device manager server IP.

Device Manager Server IP Address*

10 . 207 . 87 . 38

At this point, NetScaler Gateway points to the App Controller FQDN. You must change NetScaler to point to the new XenMobile FQDN. The latest versions of XenMobile listen on port 8443 instead of port 443. If you used the NetScaler for XenMobile wizard 9 to set up your NetScaler, you must include the port number with the FQDN, as shown in the examples in the following tables.

XenMobile Enterprise Edition

Change the App Controller FQDN to point to the new XenMobile FQDN, which is the XenMobile 9.0 Device Manager FQDN followed by port 8443. The following table shows an example.

XenMobile 9.0 Component	Component FQDN	New XenMobile Enterprise Edition FQDN
Device Manager	enroll.example.com	enroll.example.com:8443
App Controller	appc.example.net	N/A
NetScaler Gateway	access.example.com	N/A

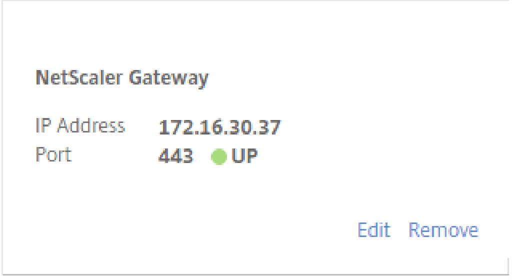
XenMobile App Edition

Change the App Controller FQDN to point to the new XenMobile FQDN, which is the XenMobile 9.0 App Controller FQDN followed by port 8443. The following table shows an example.

XenMobile 9.0 Component	Component FQDN	New XenMobile Enterprise Edition FQDN
App Controller	appc.example.net	appc.example.net:8443
NetScaler Gateway	access.example.com	N/A

1. Under **Integrate with Citrix Products**, click **XenMobile**.

2. Under **NetScaler Gateway**, click **Edit**.

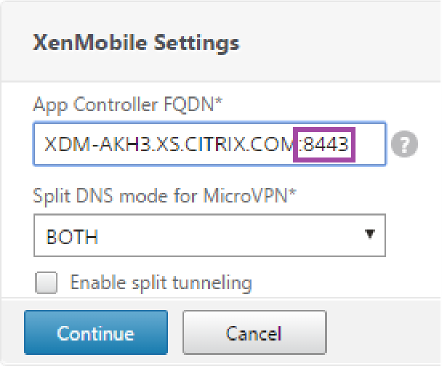


NetScaler Gateway

IP Address 172.16.30.37

Port 443 ● UP

3. Click the pen icon next to **XenMobile Settings** and then change the App Controller FQDN to the XenMobile server FQDN and append **:8443** to the FQDN. For example, *SAMPLE-XENMOBILE.FQDN*.COM:**8443**.



XenMobile Settings

App Controller FQDN*: XDM-AKH3.XS.CITRIX.COM:8443

Split DNS mode for MicroVPN*: BOTH

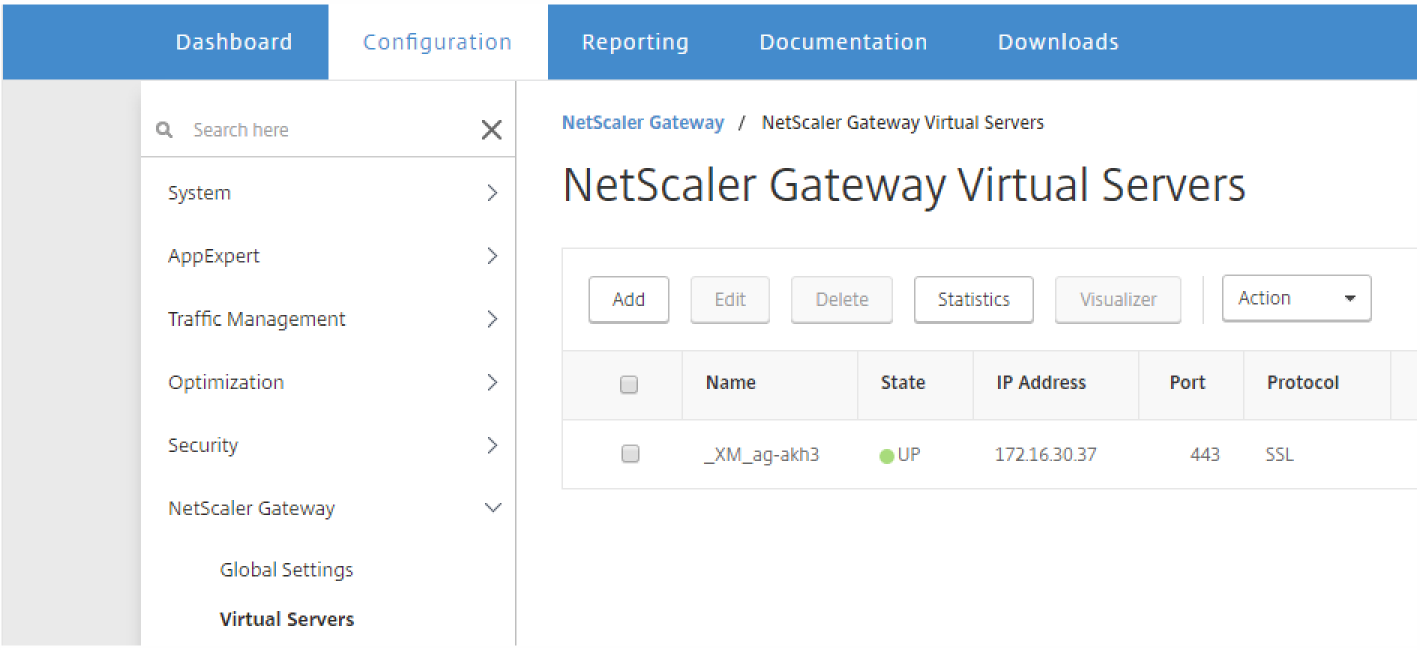
☐ Enable split tunneling

4. Click **Continue** and **Finish**.

Next, you must update your DNS to resolve the FQDN of the server running Secure Ticket Authority to the IP address of the new XenMobile Server instance. Sometimes after the post-requisite changes, the Secure Ticket Authority Server isn't bound in NetScaler, although it appears in the **VPN Virtual Server STA Server Binding** list.

In NetScaler Gateway, you add the IP address or FQDN of the server running the Secure Ticket Authority, as follows:

1. Click **Netscaler Gateway > Virtual Servers**.

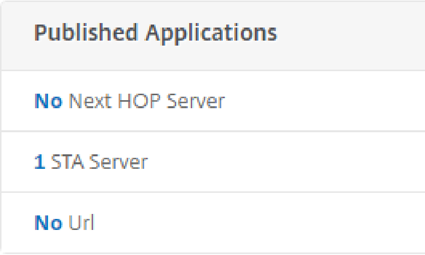


NetScaler Gateway Virtual Servers

☐	Name	State	IP Address	Port	Protocol
☐	_XM_ag-akh3	● UP	172.16.30.37	443	SSL

2. Make sure that the NetScaler Gateway virtual server is in the **Up** state. Select the configured Netscaler Gateway Virtual Server and then click **Edit**.

3. Under **Published Applications**, click **STA server**.



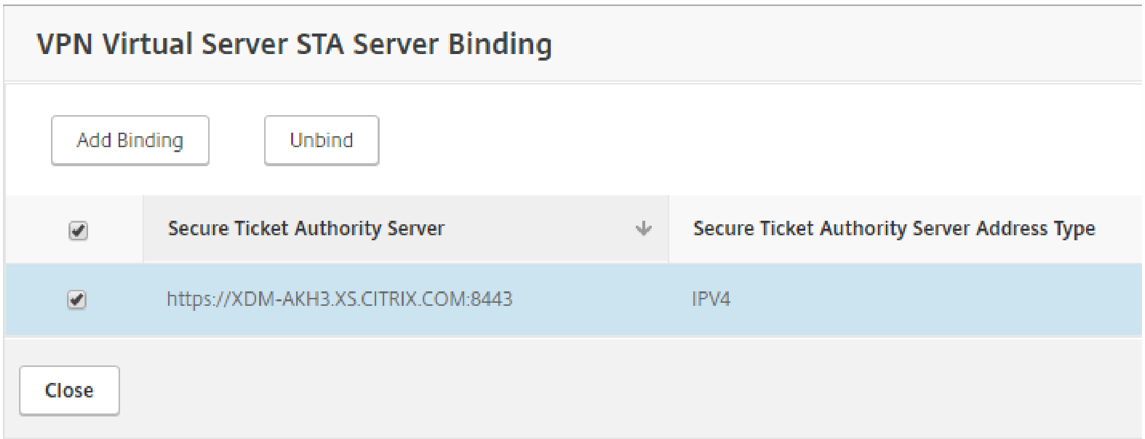
Published Applications

No Next HOP Server

1 STA Server

No Url

4. Note the **Secure Ticket Authority Server** URL, which you will enter in step 6. Then select the Secure Ticket Authority Server in the list.



VPN Virtual Server STA Server Binding

☑	Secure Ticket Authority Server	Secure Ticket Authority Server Address Type
☑	https://XDM-AKH3.XS.CITRIX.COM:8443	IPV4

5. Click **Unbind** and then click **Add Binding**.

6. In the **Secure Ticket Authority Server** field, type the URL that you noted in step 4.

7. Click **Bind**, click **Close**, and then click **Done**.

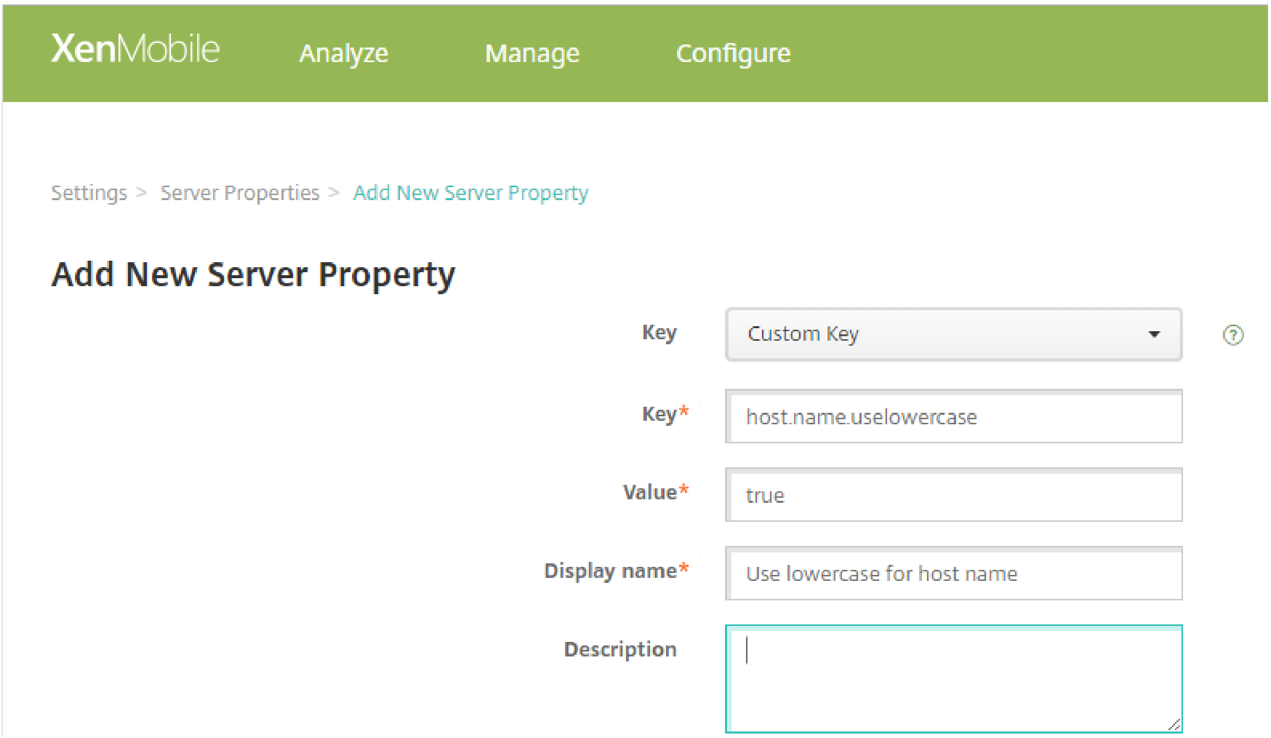
Make sure to sync the time on NetScaler and on XenMobile server. If possible, point NetScaler and XenMobile server to the same public Network Time Protocol (NTP) server.

If your XenMobile 9.0 host name includes uppercase letters, complete the following steps so that mobile devices can access Citrix Store:

1. In the new XenMobile console, go to **Settings** > **Server Properties**.

2. Click **Add** and complete the fields as follows:

- **Key**: Select **Custom Key**.
- **Key**: Enter **host.name.uselowercase**.
- **Value**: Enter **true**.
- **Display name**: Enter a description for the key.



Add New Server Property

Key	Custom Key
Key*	host.name.uselowercase
Value*	true
Display name*	Use lowercase for host name
Description	

3. Restart the XenMobile server.

Update the following as necessary:

- Managed Service Provider (MSP) group
- Custom Active Directory attributes
- RBAC roles
  For an on-premises upgrade, RBAC settings have issues. For information, see Known issues.
- Log settings
- Any configuration or user data listed in the migration.log file
- Any sys log server configuration

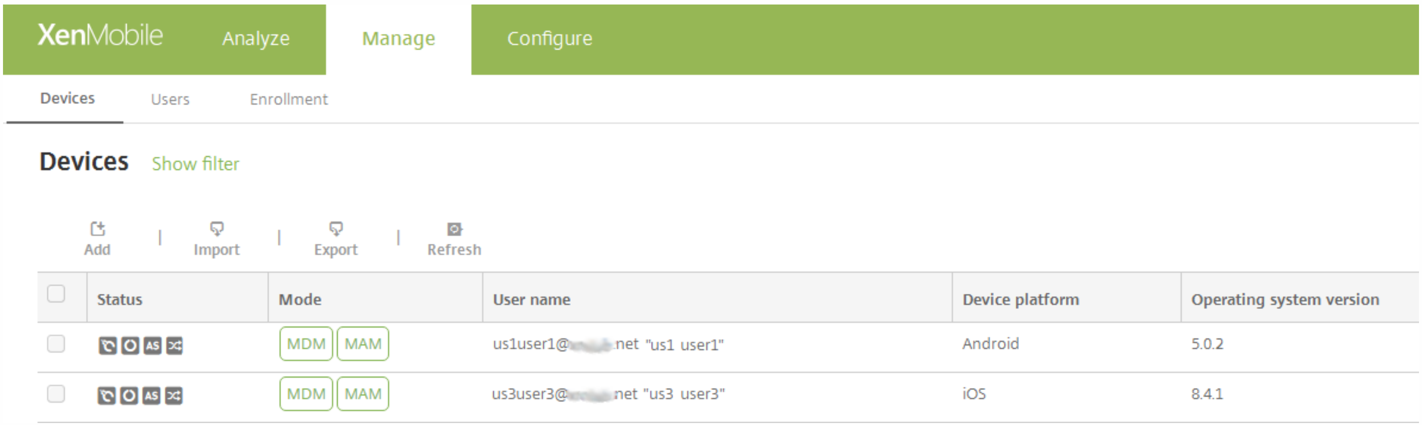
Before you upgraded, one of the prerequisite steps was to change a custom Citrix Store name back to its default value. If you did not complete that prerequisite, you must follow one of these post-requisite steps before using the latest version of XenMobile Server:

- If you have a large population of Windows devices, change the store name to the default value. After that, end users enrolled with iOS and Android devices must sign off from Citrix Secure Hub (previously Worx Home) and then sign in again.
- If you have fewer Windows devices than iOS and Android devices, the recommendation is to have the Windows users re-enroll their devices.

For more information about this issue, see http://support.citrix.com/article/CTX214553.

Users do not need to re-enroll their devices after you do a production upgrade to the latest version of XenMobile. The devices should connect automatically to the new XenMobile Server based on the heartbeat interval. Users may, however, be asked to re-authenticate before the device can reconnect.

After the user devices connect, check to make sure you see the devices in the XenMobile console, as shown in the following figure.



□	Status	Mode	User name	Device platform	Operating system version
□		MDM MAM	us1user1@[redacted]net "us1 user1"	Android	5.0.2
□		MDM MAM	us3user3@[redacted]net "us3 user3"	iOS	8.4.1

Upgrade the MTC tenant server to XenMobile

Nov 15, 2017

If XenMobile 9.0 MDM or Enterprise Edition has Multi-Tenant Console (MTC) enabled, you can migrate MTC-managed XenMobile 9 instances to standalone instances of the latest version of XenMobile. XenMobile 10.x does not support MTC, so you must manage these upgraded instances on an individual basis.

1. Make sure that you configure network address translation (NAT) in front of all of the MTC clients.

2. Install an instance of the latest version of XenMobile.

3. If no port mapping is enabled on the MTC tenant, do the following:

> a. Make sure that, for the new XenMobile instance, the server port that allows HTTPS communication with certificates (typically, port 443) and that allows HTTPS communication without certificates (8443) matches the port used for the XenMobile instance.
>
> b. Configure a new port for management.
>
> c. If port mapping is enabled, use the port that is mapped to and not the port that the XenMobile server listens on.

4. During the XenMobile server startup, use the instance name, **zdm**.

5. When you are enabling the Upgrade Tool through the XenMobile command-line interface, you must respond **Yes** to the upgrade prompt.

6. From the server from which you are upgrading, copy the following files from C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\webapps\tenant-name\WEB-INF\classes:

- ew-config.properties
- pki.xml
- variables.xml

7. Copy the following files from C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name:

- cacerts.pem.jks
- https.p12
- pki-ca-devices.p12
- pki-ca-root.p12
- pki-ca-servers.p12

8. Make a copy of C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\server.xml and modify it as described in the following steps.

9. Remove all of the port connectors in use by the other tenant in server xml, except keep port 80.

10. On the used port connector, remove the instance name from all file paths within the following range:

keystoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name\https.p12" to:

keystoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\https.p12"

11. Repeat step 10 for the file paths from:

truststoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name\cacerts.pem.jks"

to:

truststoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\cacerts.pem.jks"

12. Create a .zip file with the files you copied in steps 6 - 8.

13. Open the IP address of the new XenMobile Server, as follows: https://*ipAddress:port*/uw/?cloudMode, where *port* is the HTTPS connection with a certificate. The upgrade wizard opens.

14. Using the steps described in the upgrade wizard, select **MDM** or **Enterprise**.

For **MDM** upgrades, the wizard prompts you to upload the .zip file. You must also validate that the database is correct and enter the password for the CA certificate.

For **Enterprise** upgrades, the wizard prompts you to upload the support bundle for App Controller.

15. After the XenMobile server restarts, sign on to the XenMobile console by using the IP address of your XenMobile server followed by the management port number.

16. Change the NAT to point to a new server.

17. Make necessary firewall changes to allow ports used by XenMobile server.

User accounts, roles, and enrollment

Sep 06, 2017

You configure the following items in the XenMobile console on the **Manage** tab and the **Settings** page:

- User accounts and groups
- Roles for user accounts and groups
- Enrollment mode and invitations

From the **Manage tab**, you can do the following:

- Click **Users** to add user accounts manually or use a .csv provisioning file to import the accounts and to manage local groups. For details, see:
  - To add, edit, or delete local user accounts
  - To import user accounts by using a .csv provisioning file and Provisioning file formats
  - To add or remove groups in XenMobile

  You can also use workflows to manage the creation and removal of user accounts, as described later in this article in Create and manage workflows.

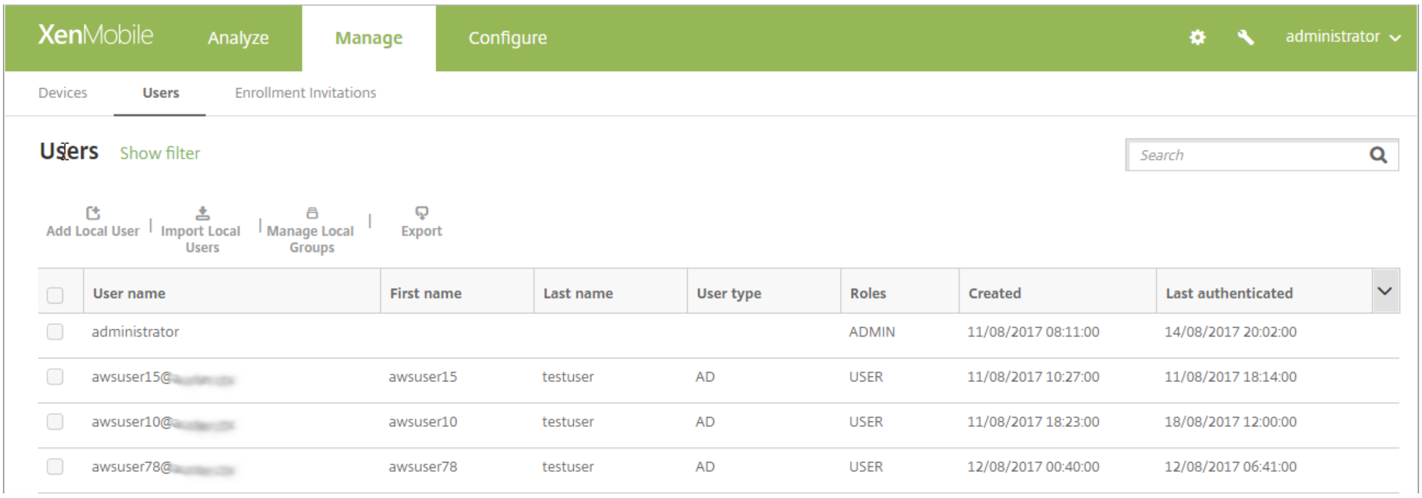
- Click **Enrollment** to configure up to seven modes and to send enrollment invitations. Each enrollment mode its own level of security and number of steps users must take to enroll their devices. For details, see:
  - To configure enrollment modes and enable the Self Help Portal
  - Enable autodiscovery in XenMobile for user enrollment

From the **Settings** page, you can do the following:

- Click **Role-Based Access Control** to assign predefined roles, or sets of permissions, to users and groups. These permissions control the level of access users have to system functions. For details, see:
  - Configuring Roles with RBAC
- Click **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 details, see:
  - Creating and updating Notification Templates

You can add local user accounts to XenMobile manually or you can use a provisioning file to import the accounts. For the steps to import user accounts from a provisioning file, see To import user accounts by using a .csv provisioning file.

1. In the XenMobile console, click **Manage** > **Users**. The **Users** page appears.

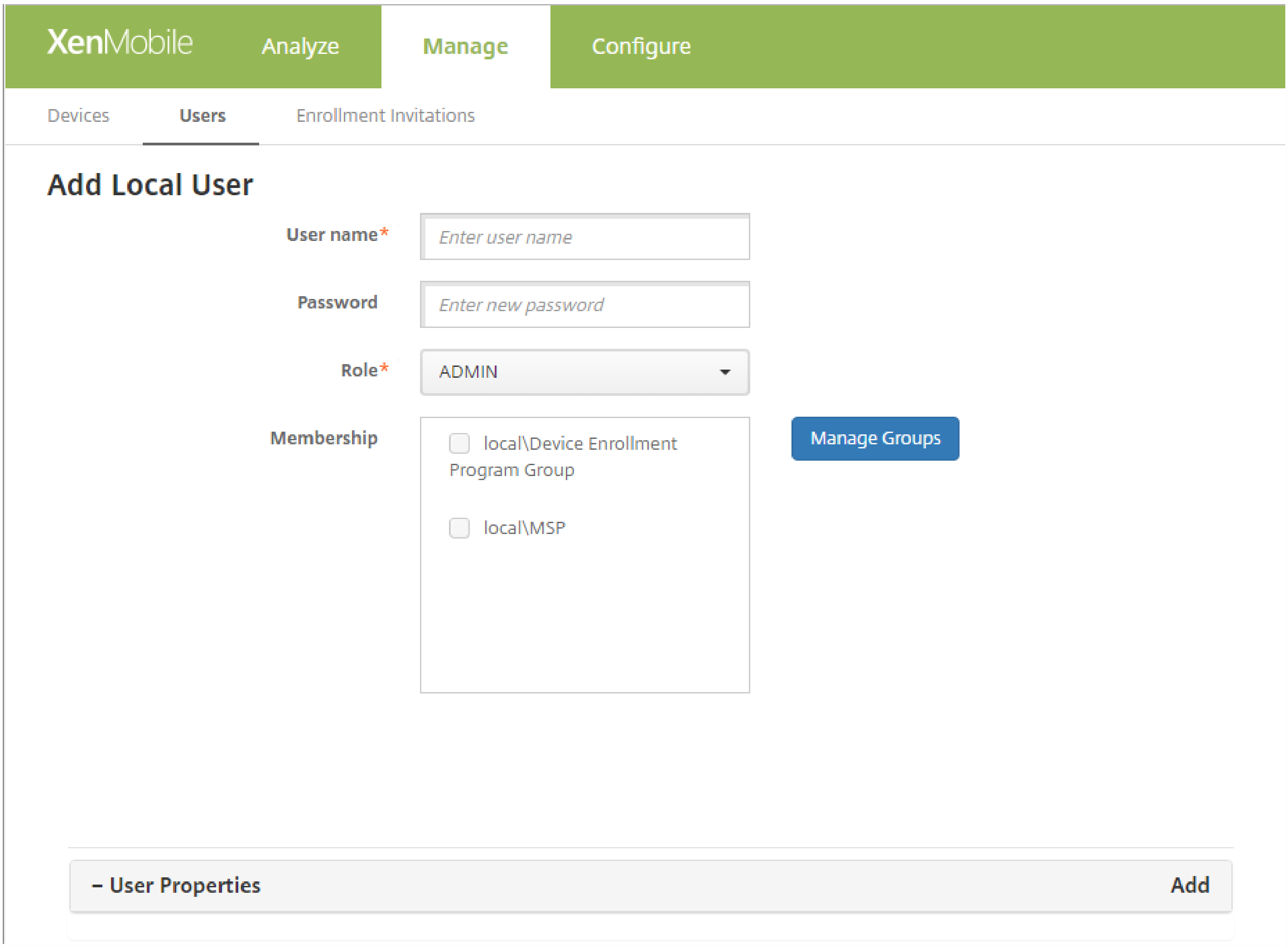


☐	User name	First name	Last name	User type	Roles	Created	Last authenticated
☐	administrator				ADMIN	11/08/2017 08:11:00	14/08/2017 20:02:00
☐	awsuser15@[redacted]	awsuser15	testuser	AD	USER	11/08/2017 10:27:00	11/08/2017 18:14:00
☐	awsuser10@[redacted]	awsuser10	testuser	AD	USER	11/08/2017 18:23:00	18/08/2017 12:00:00
☐	awsuser78@[redacted]	awsuser78	testuser	AD	USER	12/08/2017 00:40:00	12/08/2017 06:41:00

2. Click **Show filter** to filter the list.

To add a local user account

1. On the **Users** page, click **Add Local User**. The **Add Local User** page appears.



Add Local User

User name* Enter user name

Password Enter new password

Role* ADMIN

Membership
☐ local\Device Enrollment Program Group
☐ local\MSP

2. Configure these settings:

- **User name**: Type the name, a required field. You can include spaces in names, as well as upper and lowercase letters.
- **Password**: Type an optional user password.
- **Role**: In the list, click the user role. For more information about roles, see Configuring 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**.

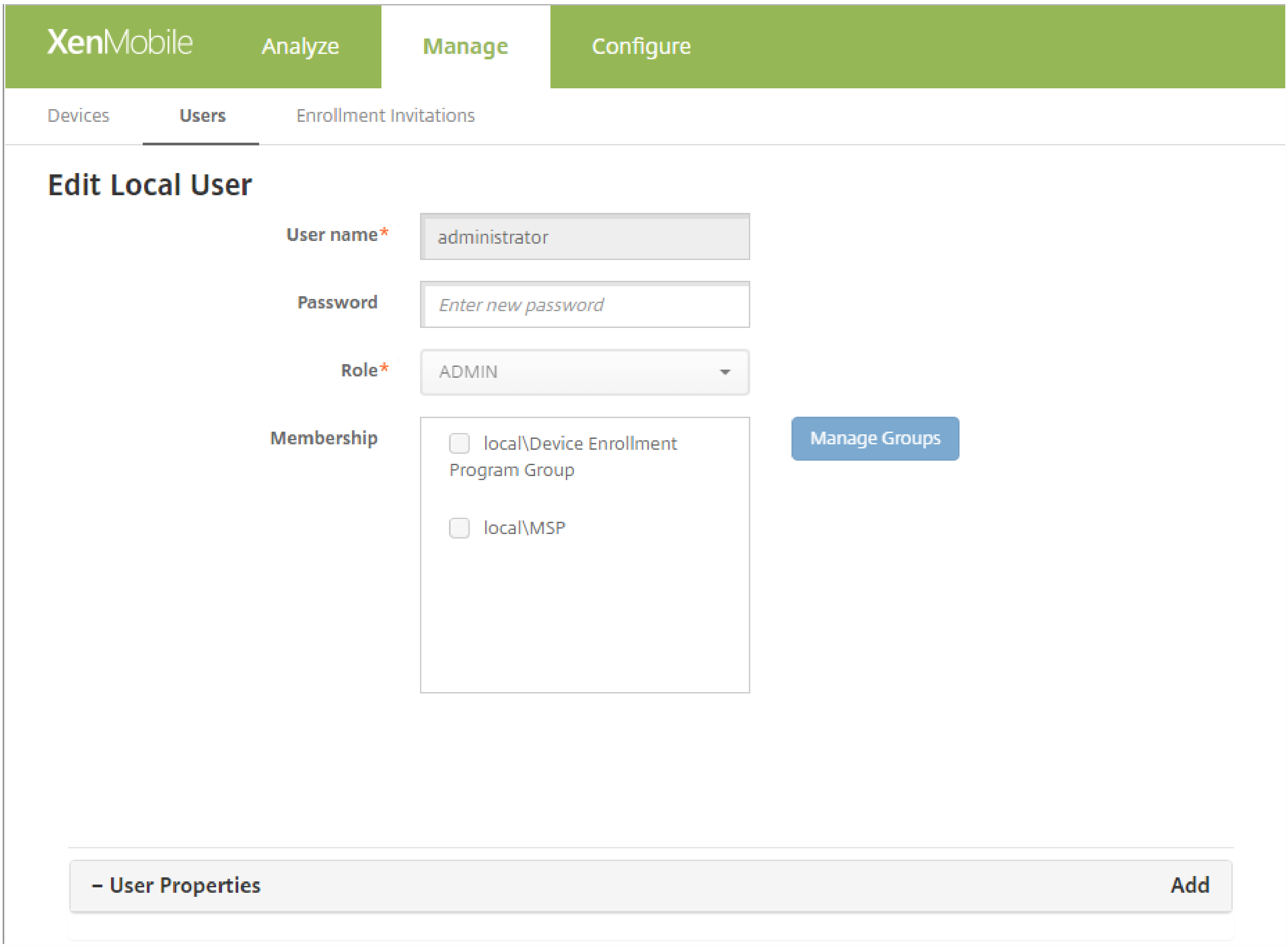
Note: To delete an existing user property, hover over the line containing the property and then click the X on the right side. The property is deleted immediately.

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.



Edit Local User

User name* administrator

Password *Enter new password*

Role* ADMIN

Membership
□ local\Device Enrollment Program Group
□ local\MSP

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.

Note: 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**.

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.

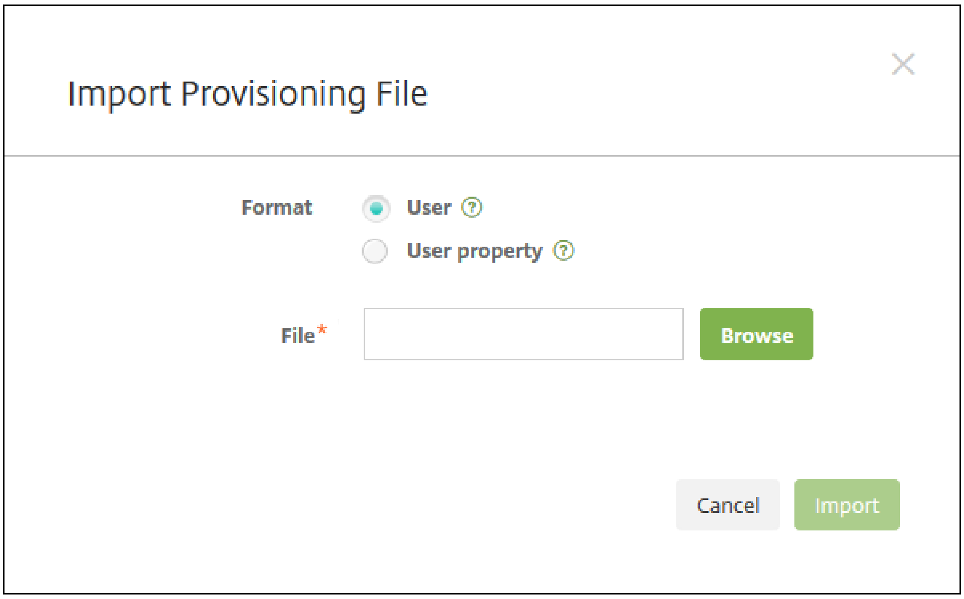
Note:

- 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 XenMobile, the user cannot enroll by using the corresponding LDAP credentials.
- If importing user accounts to the XenMobile internal user directory, disable the default domain to speed up the import process. Keep in mind that disabling the domain affects enrollments, so you should 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 XenMobile.

1. In the XenMobile console, click **Manage** > **Users**. The **Users** page appears.

2. Click **Import Local Users**. The **Import Provisioning File** dialog box appears.



Import Provisioning File

Format ● User ○ User property

File*

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**.

A provisioning file that you create manually and use to import user accounts and properties to XenMobile must be in one of the following formats:

- **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 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

This entry, user01;pwd\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01, means:

- **User**: user01
- **Password**: pwd;01
- **Role**: USER
- **Groups**:
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

As another example, AUser0;1.password;USER;ActiveDirectory.test.net, means:

- **User**: AUser0
- **Password**: 1.password
- **Role**: USER
- **Group**: ActiveDirectory.test.net

Example of user attribute provisioning content

This 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

You configure device enrollment modes to allow users to enroll their devices in XenMobile. XenMobile 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. Users can log on to the portal and generate enrollment links that allow them to enroll their devices or choose to send themselves an enrollment invitation. You configure enrollment modes in the XenMobile console from the **Settings** > **Enrollment** page.

You send enrollment invitations from the **Manage** > **Enrollment Invitations** page. For information, see Send an enrollment invitation.

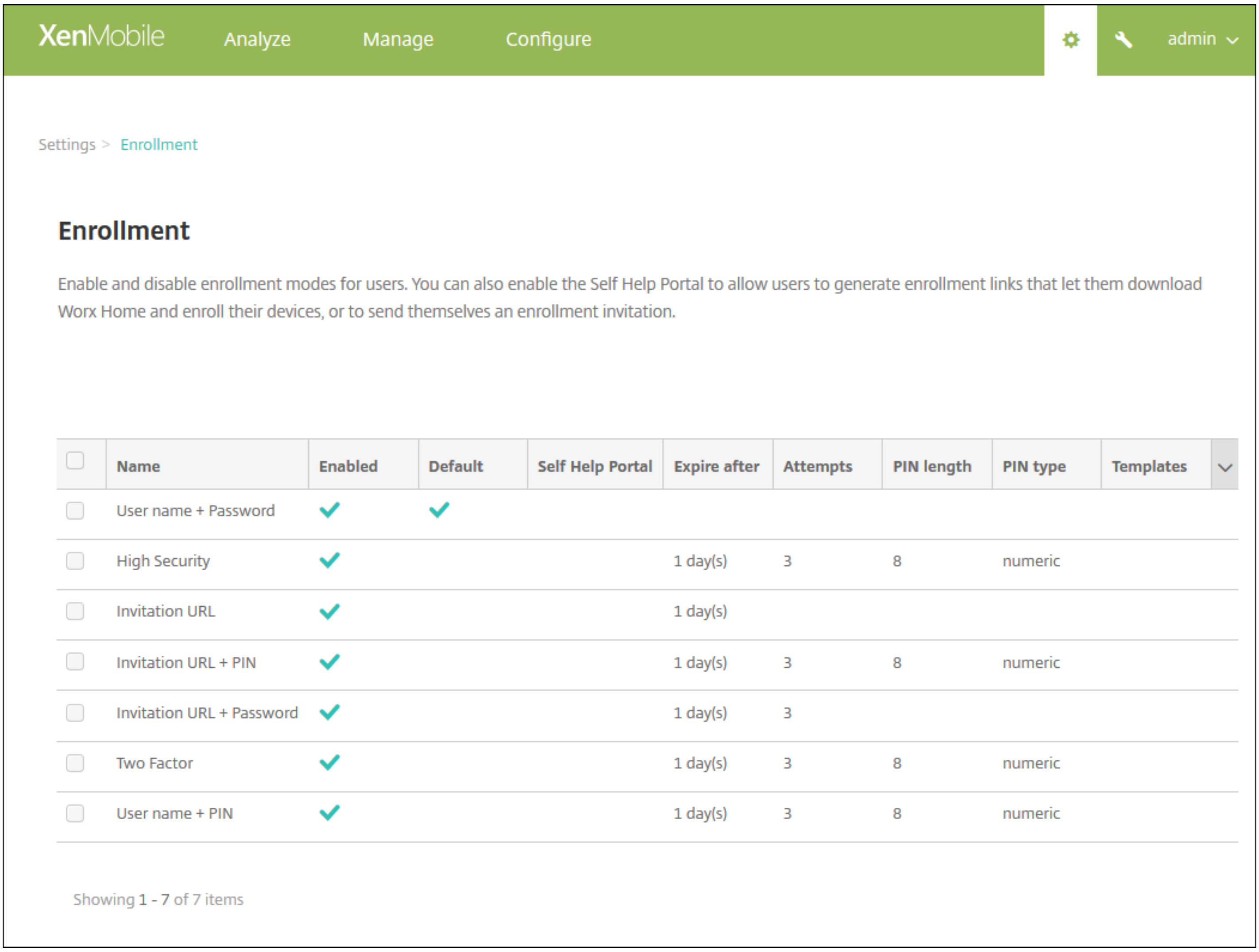
Note: If you plan to use custom notification templates, you must set up the templates before you configure enrollment modes. For more information about notification templates, see Creating or Updating Notification Templates.

1. On the XenMobile 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.

Note: When you select the check box next to an enrollment mode, the options menu appears above the enrollment mode list. When you click anywhere else in the list, the options menu appears on the right side of the listing.



Enrollment

Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Worx Home and enroll their devices, or to send themselves an enrollment invitation.

□	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates
□	User name + Password	✓	✓						
□	High Security	✓			1 day(s)	3	8	numeric	
□	Invitation URL	✓			1 day(s)				
□	Invitation URL + PIN	✓			1 day(s)	3	8	numeric	
□	Invitation URL + Password	✓			1 day(s)	3			
□	Two Factor	✓			1 day(s)	3	8	numeric	
□	User name + PIN	✓			1 day(s)	3	8	numeric	

Showing 1 - 7 of 7 items

Choose from these enrollment modes:

- User name + Password
- High Security
- Invitation URL
- Invitation URL + PIN
- Invitation URL + Password
- Two Factor
- User name + PIN

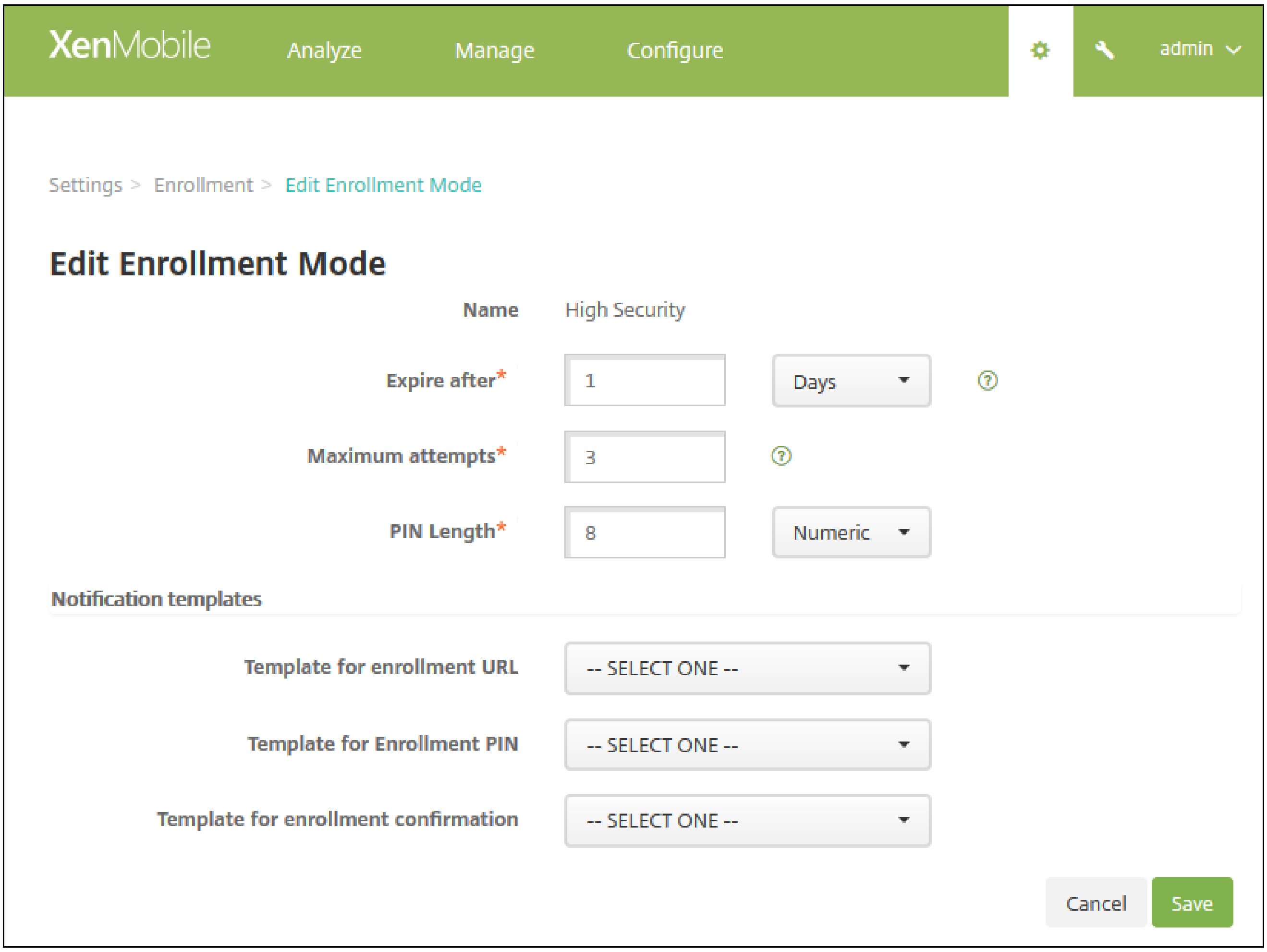
You can use enrollment invitations to restrict enrollment to users with an invitation only.

You can use one-time PIN (OTP) enrollment invitations as a two-factor solution. OTP enrollment invitations 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.

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 may see different options.



Edit Enrollment Mode

Name	High Security	
Expire after*	1	Days
Maximum attempts*	3	
PIN Length*	8	Numeric

Notification templates

Template for enrollment URL	-- SELECT ONE --
Template for Enrollment PIN	-- SELECT ONE --
Template for enrollment confirmation	-- SELECT ONE --

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.
  Note: 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.
  Note: 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 XenMobile. For more information on notification templates, see Creating or updating 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

When you set an enrollment mode as the default, the 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 a request for enrollment 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**.

Note: 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 may change how you allow users to enroll their devices by disabling one enrollment mode and enabling another.

1. Select an enrollment mode.

Note: 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 XenMobile individually.

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. Select an enrollment mode.

2 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.

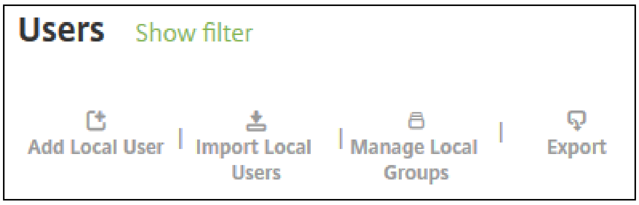
You manage groups in the **Manage Groups** dialog box in the XenMobile console on these pages: **Users**, **Add Local User**, or **Edit Local User**. There is no group edit command.

If you remove a group, keep in mind that removing the group has no effect on user accounts. Removing a group simply removes user association with that group. Users also lose access to apps or profiles provided by the Delivery Groups that are associated with that group; any other group associations, however, remain intact. If users are not associated with any other local groups, they are associated at the top level.

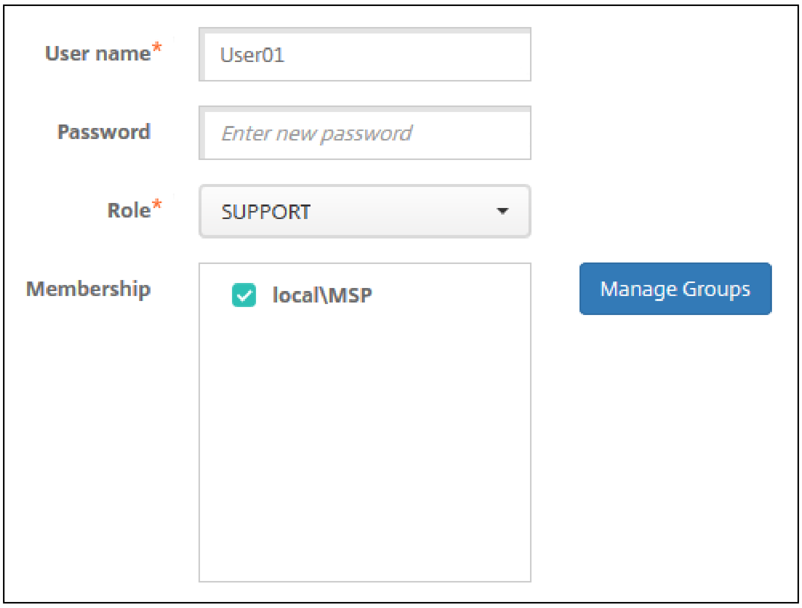
To add a local group

1. Do one of the following:

- On the **Users** page, click **Manage Local Groups**.



- On either the **Add Local User** page or the **Edit Local User** page, click **Manage Groups**.

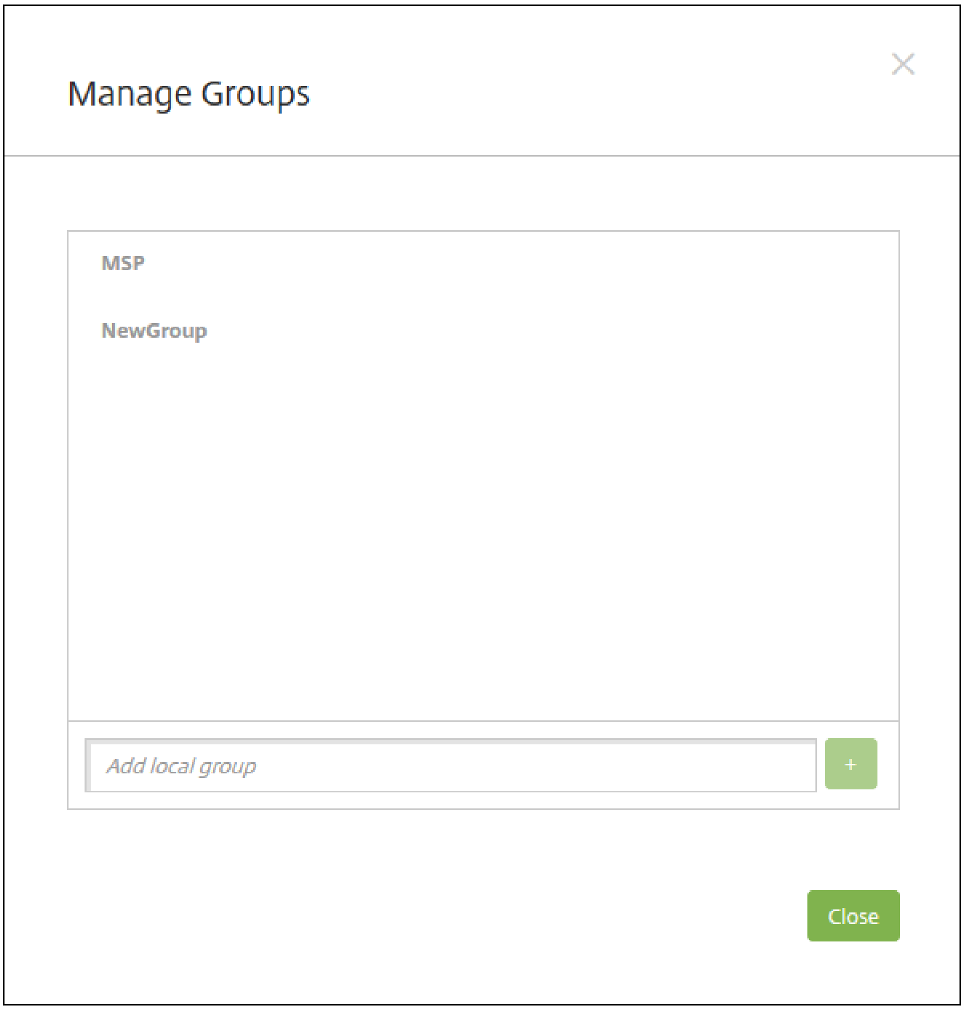

User name* User01

Password Enter new password

Role* SUPPORT

Membership ☑ local\MSP

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**.

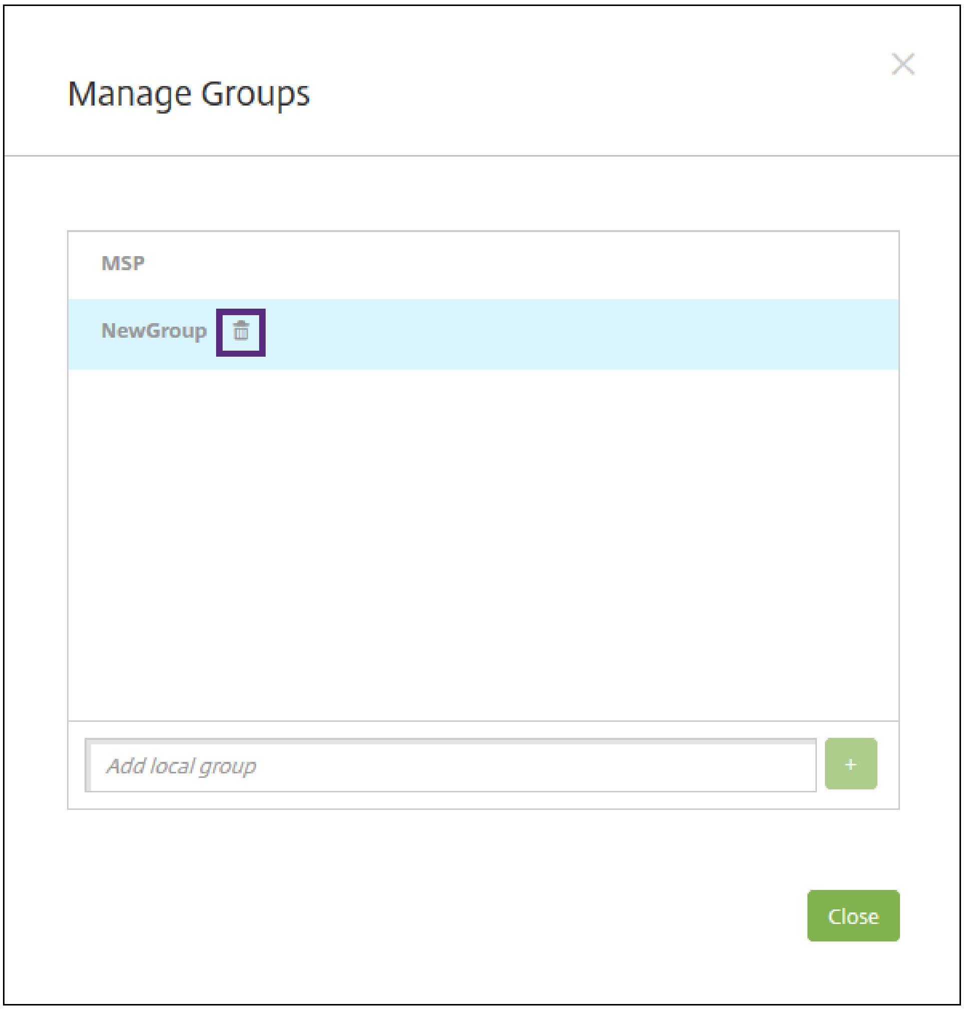
To remove a group

Note: Removing a group has no effect on user accounts. Removing a group simply removes the users' association with that group. Users also lose access to apps or profiles provided by the Delivery Groups that are associated with that group; any other group associations, however, remain intact. If users are not 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**.

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 XenMobile 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 XenMobile:

- In the **Workflows** page in the XenMobile 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.

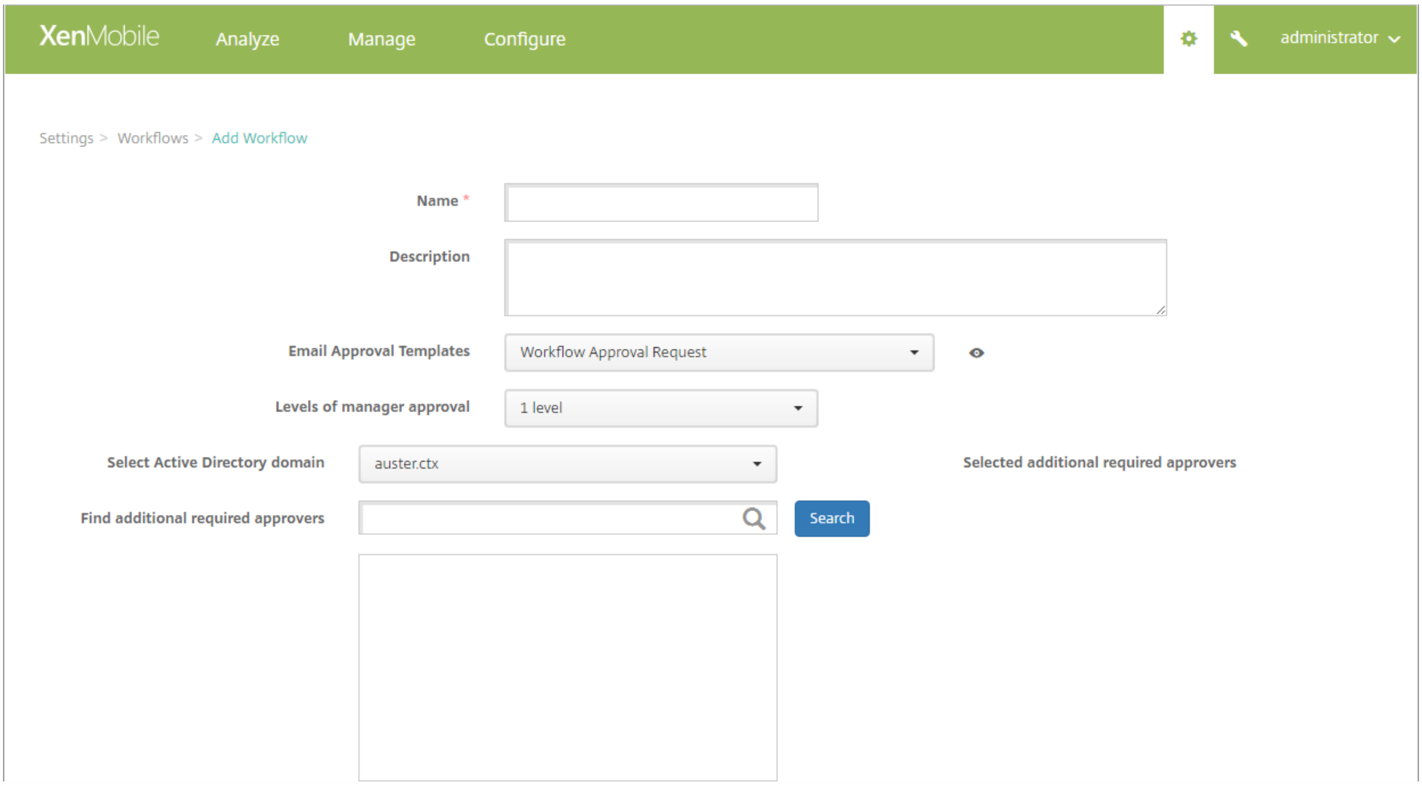
- When you configure an application connector in the app, you provide a workflow name and then configure the individuals who can approve the user account request. See Adding Apps to XenMobile.

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 XenMobile 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 XenMobile 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.



Name *

Description

Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level

Select Active Directory domain: auster.ctx

Find additional required approvers

Selected additional required approvers

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 XenMobile 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.

Configure roles with RBAC

Dec 14, 2017

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. Note that 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.

This article contains the following sections:

- Admin Role
- Device Provisioning Role
- Support Role
- User Role
- Configure roles with RBAC

Admin Role

Users with the predefined Admin role have access or do not have access to the following features in XenMobile. By default, **Authorized access** (except Self-Help Portal), **Console features**, and **Apply permissions** are enabled.

Authorized access

Admin console access	Administrators have access to all features on the XenMobile console.
Self-Help Portal access	Administrators do not have Self-Help Portal access.
Shared devices enroller	Administrators do not have Shared devices enroller access. This feature is intended for users who need to enroll shared devices.
Remote Support access	Administrators own Remote Support access.*
Public API access	Administrators have access to the public API to perform actions programmatically that are available on the XenMobile console. The actions include administering certificates, apps, devices, delivery groups, and local users.

* Remote support isn't available to XenMobile Service customers. For on-premises XenMobile Server deployments: Remote support enables your help desk representatives to take remote control of managed Windows CE and Android mobile

devices. Screen cast is supported on Samsung KNOX devices only. Remote support isn't available for clustered on-premises XenMobile Server deployments.

Console features

Administrators have unrestricted access to the XenMobile console.

Dashboard	The **Dashboard** is the first page that administrators see after logging on to the XenMobile 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 XenMobile.
Policies	The **Configure > Device Policies** page is where you manage device polices, such as VPN and WiFi.
Apps	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.
Enrollment Profiles	The **Configure > Enrollment Profiles** page is where you configure enrollment profiles (modes) to allow users to enroll their devices.
Delivery Groups	The **Configure > Delivery Groups** page is where you manage delivery groups and the resources associated with them.

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.

Devices

Administrators access device features throughout the console by setting device restrictions, setting up and sending notifications to devices, administering apps on the devices, and so on.

Full Wipe device	Erase all data and apps from a device, including memory cards if the device has one.
Clear Restriction	Remove one or more device restriction.
Selective Wipe device	Erase all corporate data and apps from a device, leaving personal data and apps in place.
View locations	See the location of and set geographic restrictions on a device. Includes: Locate device, See the location of a device, Track device, Track a device's location over time.
Lock device	Remotely lock a device so that users cannot use the device.
Unlock device	Remotely unlock a device so that users can use the device.
Lock container	Remotely lock the corporate container on a device.
Unlock container	Remotely unlock the corporate container on a device.
Reset container password	Reset the corporate container password.
Enable ASM DEP/Bypass activation lock	Store a bypass code on a supervised iOS device when Activation Lock is enabled. If you need to erase the device, use this code to clear the Activation Lock automatically.
Rings the device	Remotely ring a Windows device at full volume for 5 minutes.
Reboot the device	Restart Windows devices from the XenMobile console.

Deploy to device	Send apps, notifications, restrictions, and so on to a device.
Edit device	Change settings on the device.
Notification to device	Send a notification to a device.
Add/Delete device	Add or remove devices from XenMobile.
Devices import	Import a group of devices from a file into XenMobile.
Export device table	Collect device information from the Device page and export it to a .csv file.
Revoke device	Prohibit a device from connecting to XenMobile.
App lock	Deny access to all apps on a device. On Android, users will not be able to log into XenMobile at all. On iOS, users will still be able to log in, but they will be unable to access apps.
App wipe	On Android, this deletes the user's XenMobile account. On iOS, this deletes the encryption key users need to be able to access XenMobile features.
View software inventory	See what software is installed on a device.
Request AirPlay mirroring	Request to start AirPlay streaming.
Stop AirPlay mirroring	Stop AirPlay streaming.
Enable lost mode	On the Manage page, in Devices, you can put a supervised device in lost mode to block a supervised device on the lock screen and locate the device when the device is lost or stolen.
Disable lost mode	On the Manage page, in Devices, you can disable lost mode for a device that is set to lost mode.
OS Update device	You can deploy a Control OS Updates device policy to devices.
Shut down device	Shut down iOS devices from the XenMobile console.

Restart device	Restart iOS devices from the XenMobile console.

Local Users and Groups

Administrators manage local users and local user groups on the **Manage > Users** page in XenMobile.

Add/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

Add/Delete policy	Add or remove a device or app policy.
Edit policy	Change a device or app policy.
Upload Policy	Upload a device or app policy.
Clone Policy	Copy a device or app policy.
Disable Policy	Disable an existing app policy.

Export Policy	Collect device policy information from the Device Policies page and export it to a .csv file.
Assign Policy	Assign a device policy to one or more delivery groups.

App

Administrators manage apps on the **Configure > Apps** page in XenMobile.

Add/Delete app store or enterprise app	Add or remove a public app store app or an app not wrapped with the MDX Toolkit.
Edit app store or enterprise app	Make changes to a public app store app or an app not wrapped with the MDX Toolkit.
Add/Delete MDX, Web and SaaS app	Add or remove an app wrapped with the MDX Toolkit (MDX app), an app from your internal network (Web app), or an app from a public network (SaaS) to XenMobile.
Edit MDX, Web and SaaS app	Make changes to an app wrapped with the MDX Toolkit (MDX app), an app from your internal network (Web app), or an app from a public network (SaaS) to XenMobile.
Add/Delete category	Add or delete a category in which apps can appear in the XenMobile Store.
Assign public/enterprise app to delivery group	Assign a public app store app or an app not wrapped with the MDX Toolkit to a delivery group for deployment.
Assign MDX/WebLink/SaaS app to delivery group	Assign an app wrapped with the MDX Toolkit (MDX app), an app that does not require single sign-on (WebLink), or an app from a public network (SaaS) to a delivery group for deployment to user devices.
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 VPP license.

Add/Delete app store or enterprise books

Assign public/enterprise books to delivery group
Edit app store or enterprise books

Smart action

Add/delete smart action	Add or remove an action that is defined by a trigger (event, device or user property, or installed app name) and associated response.
Edit smart action	Change an action that is defined by a trigger (event, device or user property, or installed app name) and associated response.
Assign smart action to delivery group	Assign an action to a delivery group for deployment to user devices.
Export smart action	Collect action information from the Actions page and export it to a .csv file.

Delivery group

Administrators manage delivery groups from the **Configure > Delivery Groups** page.

Add/delete delivery group	Create or remove a delivery group, which adds specified users and optional policies, apps, and actions.
Edit delivery group	Change an existing delivery group, which modifies users and optional policies, apps, and actions.
Deploy delivery group	Make delivery group available for use.
Export delivery group	Collect delivery group information from the Delivery group page and export it to a .csv file.

Enrollment profile

Manage enrollment profiles.

Add/delete enrollment profile
Edit enrollment profile

Assign enrollment profile to delivery group

Settings

Administrators configure various settings on the **Settings** pages.

RBAC	RBAC Assignment, Assign roles
LDAP	Administer one or more LDAP-compliant directory, such as Active Directory, to import groups, user accounts, and related properties.
License	For on-premises XenMobile Server. Administer your Citrix licenses.
Enrollment	Enable enrollment modes for users as well as the Self-Help Portal.
Release Management	View the current installed release. Includes: Release Management Update
Certificates	Edit APNS certificate, Certificates SSL Listener
Notification Templates	Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.
Workflows	Manage the creation, approval, and removal of user accounts for use with app configurations.
Credential Providers	Add one or more credential providers authorized to issue device certificates. The credential providers control the certificate format and the conditions for renewing or revoking the certificate.
PKI Entities	Manage public key infrastructure entities (generic, Microsoft Certificate Services, or discretionary CA).
Test PKI Connection	Use the Test Connection button on the **Settings > PKI Entities** page to ensure that the server is accessible.
Client Properties	Manage various properties on user devices, such as passcode type, strength, expiration, and so on.
Client Support	Set the ways in which users can contact your support services (email, phone, or support ticket email).

Client Branding	Create a custom store name and default store views for the XenMobile Store. Add a custom logo that appears on XenMobile Store or Secure Hub.
Carrier SMS Gateway	Set up carrier SMS gateways to configure notifications that XenMobile sends through carrier SMS gateways.
Notification Server	Set up a SMTP gateway server to send email to users.
ActiveSync Gateway	Manage user access to users and devices through rules and properties.
Google Play Credentials	Set up user name, password, and device ID to allow access to Google Play.
Apple Device Enrollment Program (DEP)	Add an Apple DEP account to XenMobile.
Apple Configurator Device Enrollment	Configure Apple Configurator settings in XenMobile.
iOS/VPP Settings	Add Apple Volume Purchase Program accounts.
Mobile Service Provider	Use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and to issue operations.
NetScaler Gateway	For on-premises XenMobile Server. Add a NetScaler Gateway. Choose whether to enable authentication and whether to push user certificate for authentication. Choose a credential provider.
Network Access Control	Set the conditions that determine a device is non-compliant and therefore denied access to the network.
Samsung KNOX	Enable or disable XenMobile to query Samsung KNOX attestation server REST APIs.
Server Properties	Add or modify server properties. Requires restarting XenMobile on all nodes.
Syslog	For on-premises XenMobile Server. Send log files to a system log (syslog) server using the server host name or IP address.
XenApp/XenDesktop	Allow users to add XenApp and XenDesktop through Secure Hub.

ShareFile	When using XenMobile with ShareFile Enterprise: Configure settings to connect to the ShareFile account and administrator service account to manage user accounts. Requires existing ShareFile domain and administrator credentials. When using XenMobile with StorageZone Connectors: Configure XenMobile to point to network shares and SharePoint locations defined in ShareFile StorageZones Connectors.
Experience Improvement Program	For on-premises XenMobile Server. Opt into or out of sending anonymous statistics and usage information to Citrix.
Microsoft Azure	For on-premises XenMobile Server. Integrate XenMobile with Microsoft Azure.
Android for Work	Configure Android for Work server settings.
Identity Provider (IDP)	Configure an identity provider.
Derived Credentials	Configure derived credentials for iOS device enrollment.

Support

Administrators can perform various support tasks.

NetScaler Gateway Connectivity Checks	Perform various connectivity checks for NetScaler Gateway by IP address. Requires a user name and password.
XenMobile Connectivity Checks	Perform connectivity checks for selected XenMobile features, such as database, DNS, Google Plan, and so on.
Create Support Bundles	For on-premises XenMobile Server. Create a file to send to Citrix Support for troubleshooting. Contains system information, logs, database information, core information, trace files, and the latest configuration information for XenMobile or NetScaler Gateway.
Citrix Product Documentation	Access the public Citrix XenMobile documentation site.
Citrix Knowledge Center	Access the Citrix Support site to search for knowledge base articles.
Logs	Access and analyze log file details for debug, admin audit, and user audit.
Cluster Information	For on-premises XenMobile Server. Access information about each of the nodes in a

	clustered environment.
Garbage Collection	For on-premises XenMobile Server. Access information about memory objects no longer in use.
Java Memory Properties	For on-premises XenMobile Server. Access a snapshot of Java memory usage, memory details, and memory pool details.
Macros	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.
PKI Configuration	Import and export PKI configuration information.
APNS Signing Utility	Submit a request for Apple Push Network signing (APNs) certificates, or upload Secure Mail APNs certificate for iOS.
Citrix Insight Services	Upload logs to Citrix Insight Services (CIS) for assistance with various issues.
Device NetScaler Connector Status	Query XenMobile for the status of a device as sent to XenMobile NetScaler Connector based on the device ActiveSync ID.
Anonymization and de-anonymization	For on-premises XenMobile Server. When you create support bundles in XenMobile, sensitive user, server, and network data is made anonymous by default. You can change this behavior on the Anonymization and De-anonymization page in Support under Advanced.
Log Settings	Customize the log level or add a custom logger.

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

Device provisioning users have the following restricted access to the XenMobile console. By default, each of the following features is enabled.

Devices

Edit device	Change settings on the device.
Add/Delete device	Add or remove devices from XenMobile.

Settings

Device provisioning users can access the **Settings** page, but do not have the rights to configure the features.

Support Role

Users with the Support role have access to remote support; their permissions apply to all users by default and they cannot edit this setting.

User Role

Users with the User role have the following limited access to XenMobile.

Authorized access

Self-Help Portal	Users have access only to the Self-Help Portal in XenMobile.

Console features

Users have the following restricted access to the XenMobile console.

Devices

Full Wipe device	Erase all data and apps from a device, including memory cards if the device has one.
Selective Wipe device	Erase all corporate data and apps from a device, leaving personal data and apps in place.
View locations	See the location of and set geographic restrictions on a device. Included: Locate

	device, See the location of a device, Track device, Track device location over time
Lock device	Remotely lock a device so that it cannot be used.
Unlock device	Remotely unlock a device so that It can be used.
Lock container	Remotely lock the corporate container on a device.
Unlock container	Remotely unlock the corporate container on a device.
Reset container password	Reset the corporate container password.
Enable ASM DEP/Bypass activation lock	Store a bypass code on a supervised iOS device when Activation Lock is enabled. If you need to erase the device, use this code to clear the Activation Lock automatically.
Rings the device	Remotely ring a Windows device at full volume for 5 minutes.
Reboot the device	Restart a Windows device.
View software inventory	See what software is installed on a device.

Enrollment

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.

Restrict Group Access

For all four default roles, this permission is set by default and can be applied to all user groups. You cannot edit the role.

Configure roles with RBAC

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

XenMobile implements four 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.

- **Support**. Grants access to remote support.
- **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 new user roles with permissions to access specific system functions beyond the functions defined by the default roles.

Roles can be assigned 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 are merged together to define the permissions for that user. For example, if ADGroupA users can locate manager devices, and ADGroupB users can wipe employee devices, then a user who belongs to both groups can locate and wipe devices of managers and employees.

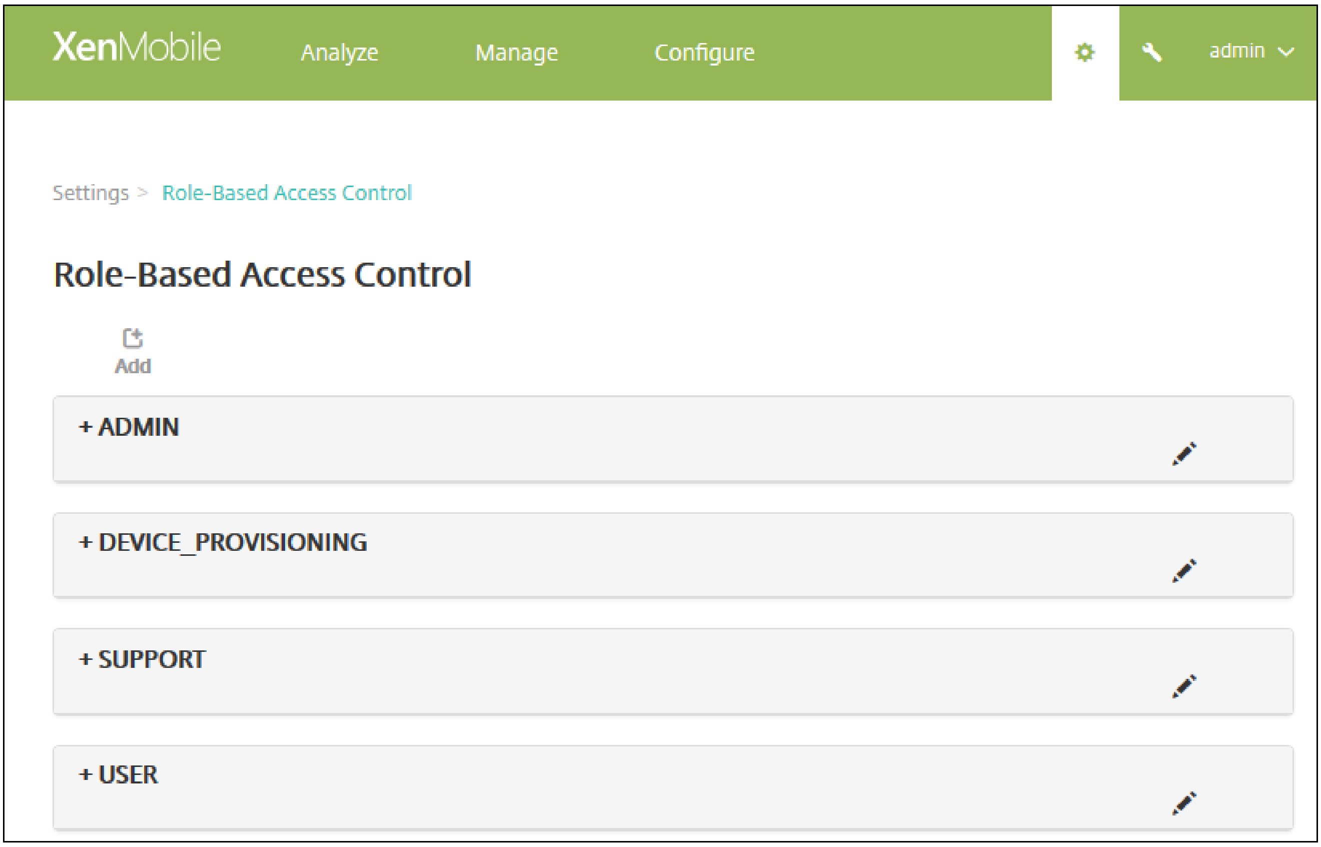
Note: Local users may have only one role assigned to them.

You can use the RBAC feature in XenMobile to do the following:

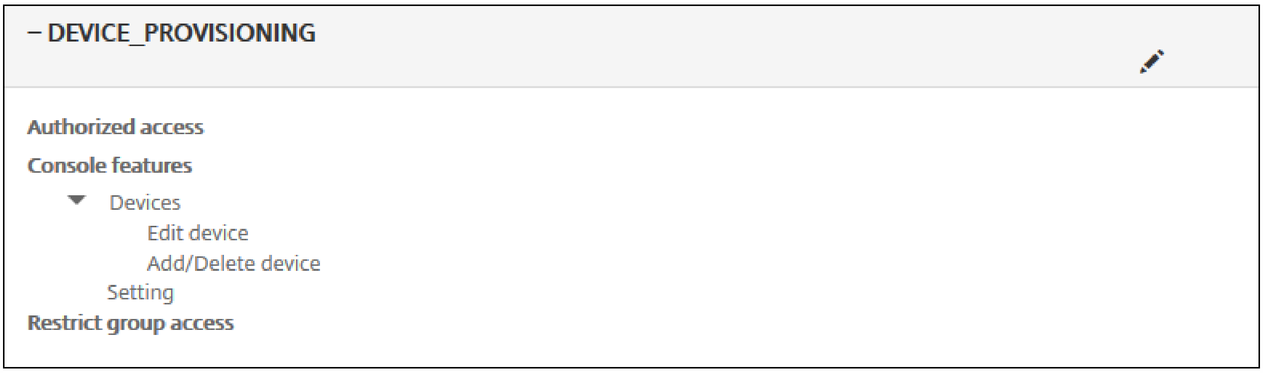
- Create a new role.
- Add groups to a role.
- Associate local users to roles.

1. In the XenMobile 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.



If you click the plus sign (+) next to a role, the role expands to show all the permissions for that role, as shown in the following figure.



– DEVICE_PROVISIONING

Authorized access

Console features

- Devices
  - Edit device
  - Add/Delete device
- Setting

Restrict group access

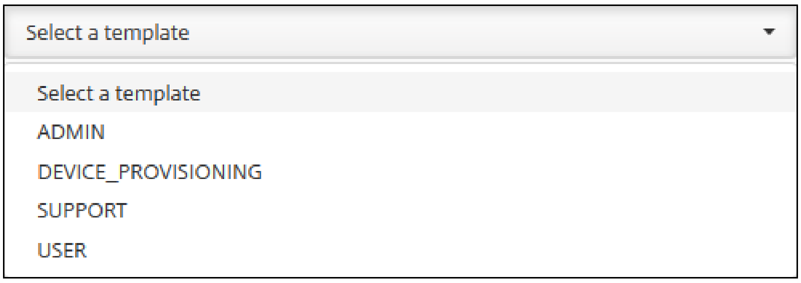
3. Click **Add** to add a new user role, click the pen icon to the right of an existing role to edit the role, or click the trash can icon to the right of a role you previously defined to delete the role. You cannot delete the default user roles.

- 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.

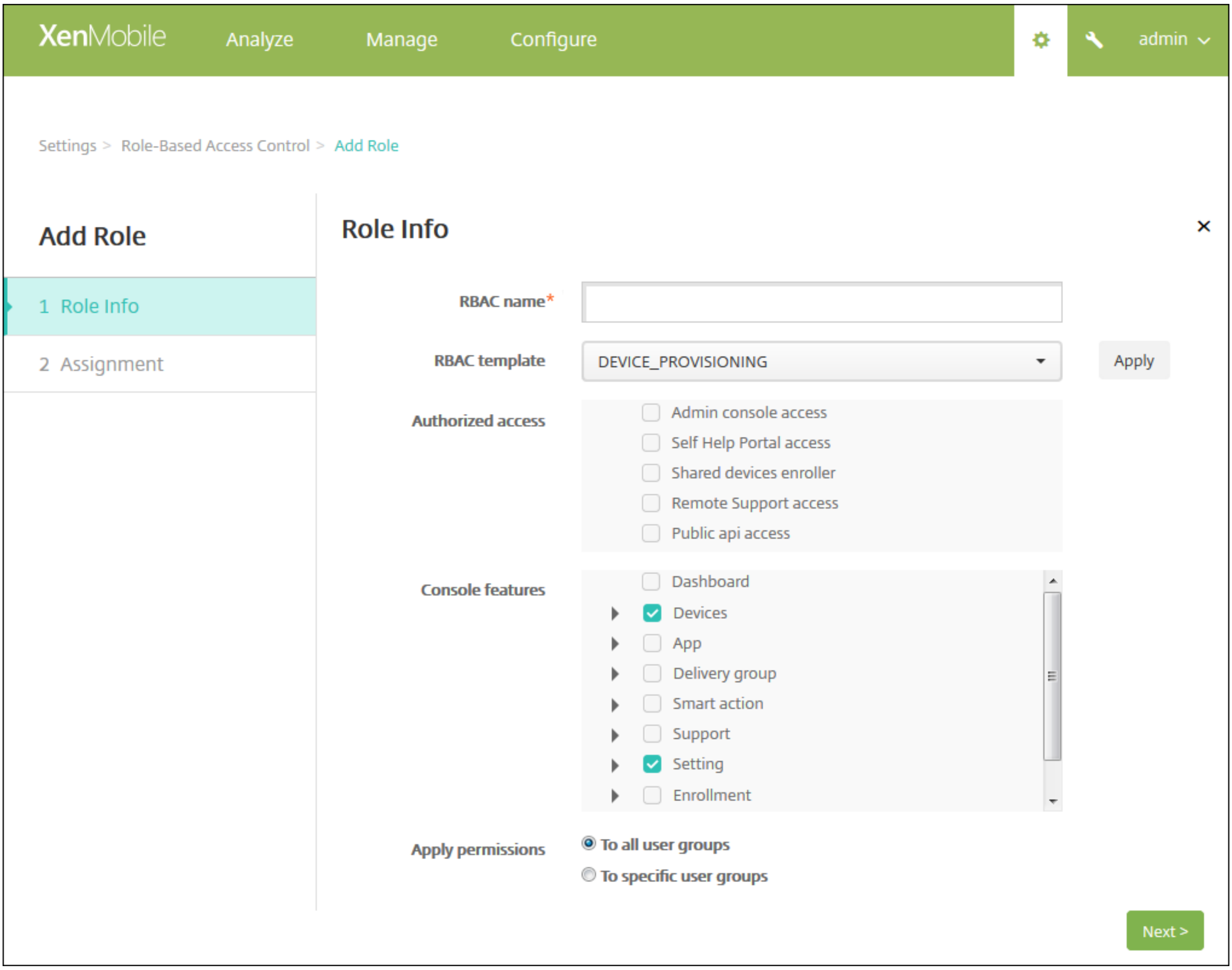
4. Enter the following information to create a new user role or to edit an existing user role:

- **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. You cannot select a template if you are editing an existing role.

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 with the pre-defined access and feature permissions for the selected template.



Role Info

RBAC name*

RBAC template: DEVICE_PROVISIONING

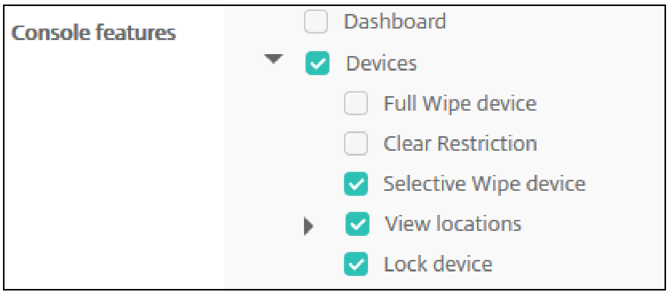
Authorized access
- □ Admin console access
- □ Self Help Portal access
- □ Shared devices enroller
- □ Remote Support access
- □ Public api access

Console features
- □ Dashboard
- ☑ Devices
- □ App
- □ Delivery group
- □ Smart action
- □ Support
- ☑ Setting
- □ Enrollment

Apply permissions
- ● To all user groups
- ○ To specific user groups

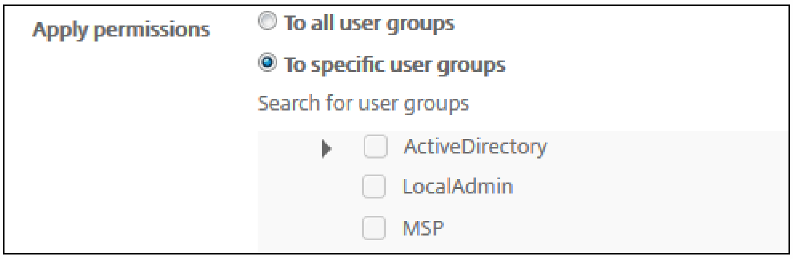
6. Select and clear the check boxes in **Authorized access** and **Console features** to customize the role.

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; you must select individual options below the top level to enable those options. For example, in the following figure, the **Full Wipe device** and **Clear Restrictions** options do not appear on the console for users assigned to the role, but the checked options do appear.



Console features
- □ Dashboard
- ☑ Devices
  - □ Full Wipe device
  - □ Clear Restriction
  - ☑ Selective Wipe device
  - ☑ View locations
  - ☑ Lock device

7. **Apply permissions**: Select the groups to which you want to apply the selected permissions. If you click **To specific user groups**, a list of groups appears from which you can select one or more groups.



Apply permissions

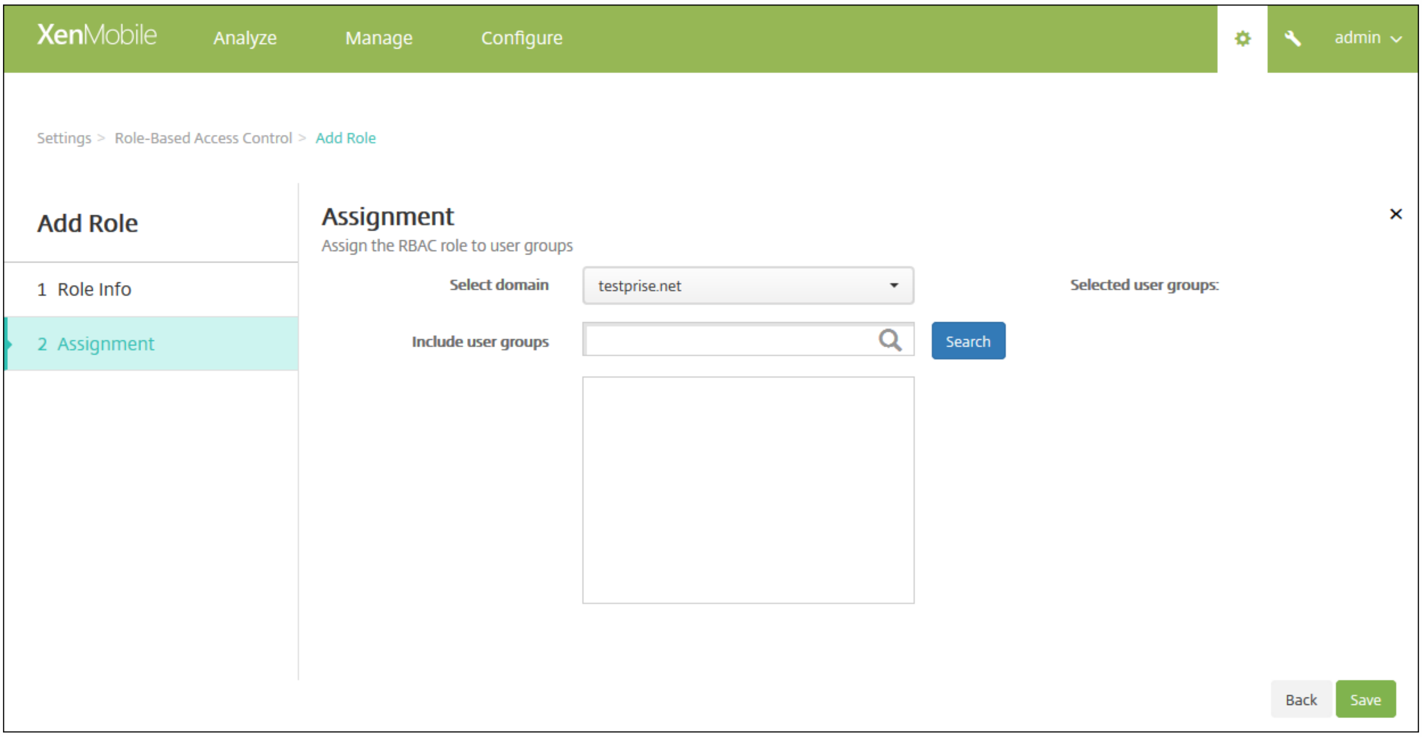
○ To all user groups

● To specific user groups

Search for user groups

- □ ActiveDirectory
- □ LocalAdmin
- □ MSP

8. Click **Next**. The **Assignment** page appears.



Settings > Role-Based Access Control > Add Role

Add Role

1 Role Info

2 Assignment

Assignment

Assign the RBAC role to user groups

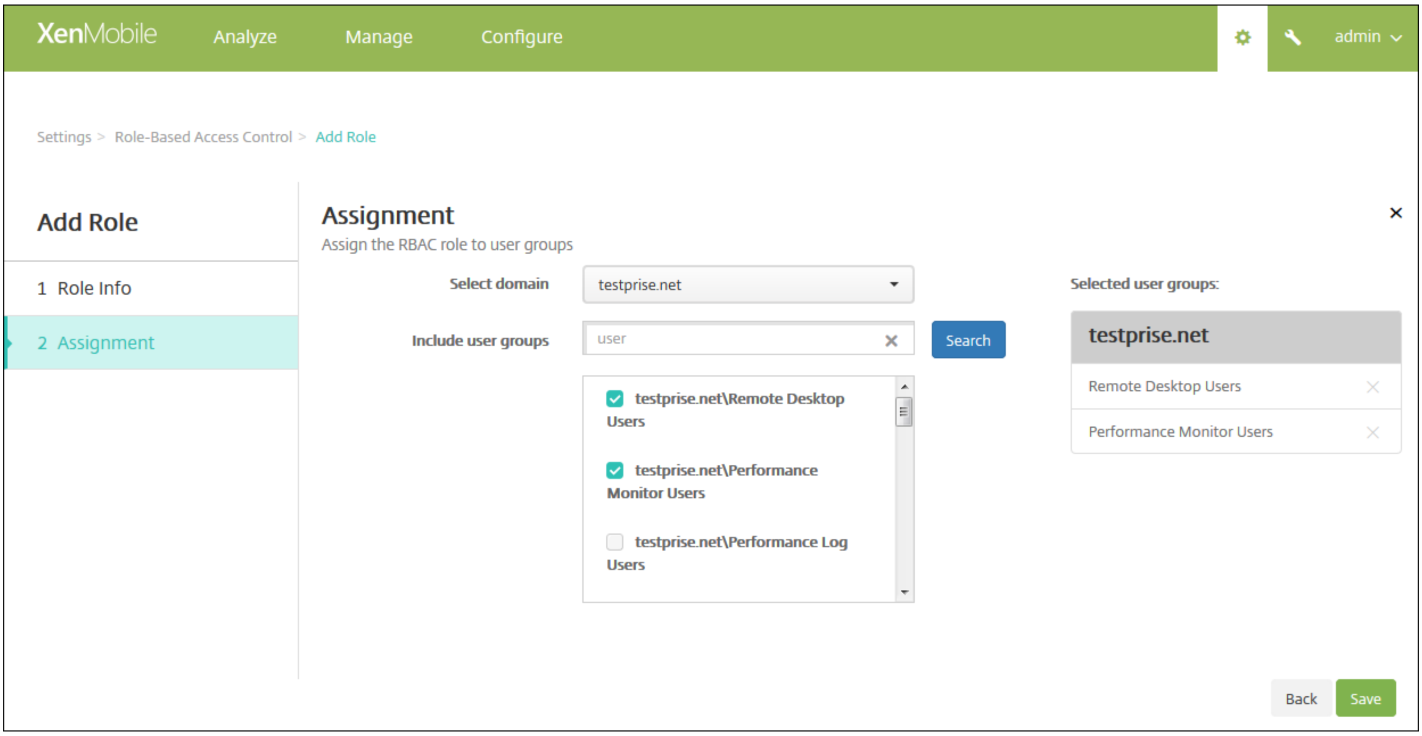
Select domain: testprise.net

Include user groups

Selected user groups:

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.


XenMobile
Analyze
Manage
Configure
admin
Settings > Role-Based Access Control > Add Role
Add Role
1 Role Info
2 Assignment
Assignment
Assign the RBAC role to user groups
Select domain
testprise.net
Include user groups
user
Search
☑ testprise.net\Remote Desktop Users
☑ testprise.net\Performance Monitor Users
□ testprise.net\Performance Log Users
Selected user groups:
testprise.net
Remote Desktop Users
Performance Monitor Users
Back
Save

Note: To remove a user group from the **Selected user groups** list, click the X next to the user group name.

10. Click **Save**.

Notifications

Sep 06, 2017

You can use notifications in XenMobile 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 XenMobile, you must configure a gateway and a notification server. You can set up a notification server in XenMobile 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 XenMobile to configure notifications that are sent through a 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.

This article explain how to:

Add an SMTP server

Add an SMS gateway

Add a carrier SMS gateway

Create and update notification templates

Prerequisites

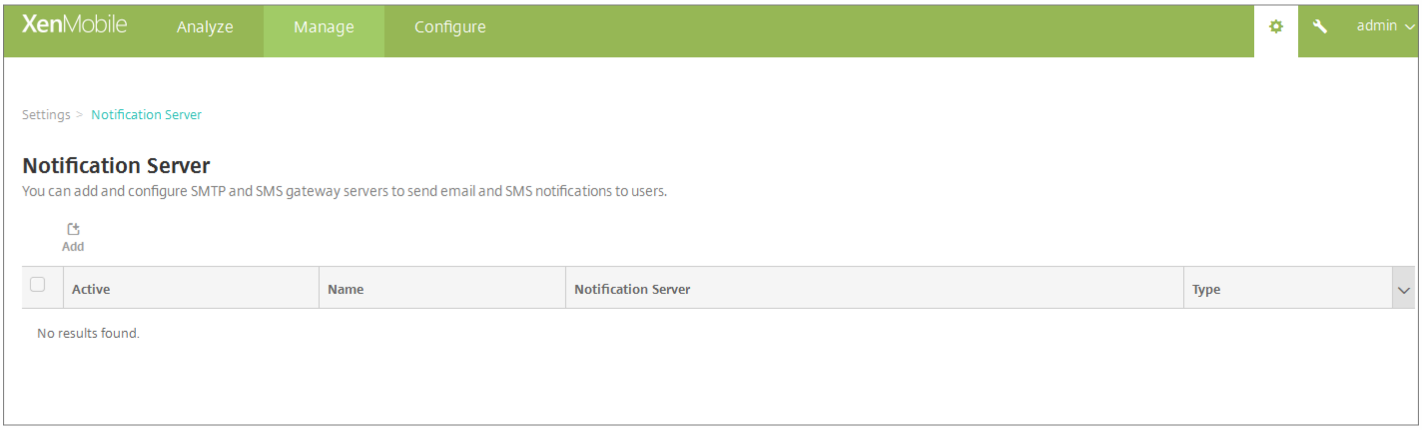
- Before configuring the SMS gateway, consult your system administrator to determine the server information. It's important to know whether the SMS server is hosted on an internal corporate server, or whether the server is part of a hosted email service. In that case, you need information from the website 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 XenMobile located in your network DMZ to point back to the SMTP server on your internal network. That enables XenMobile to send notifications successfully.

Configure an SMTP server and SMS gateway

1. In the XenMobile 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.



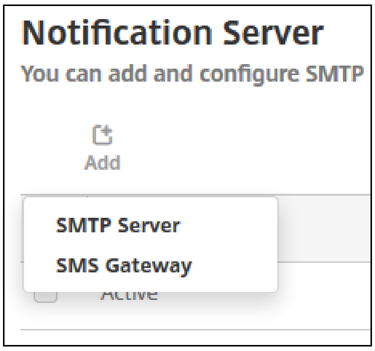
Notification Server

You can add and configure SMTP and SMS gateway servers to send email and SMS notifications to users.

□	Active	Name	Notification Server	Type

No results found.

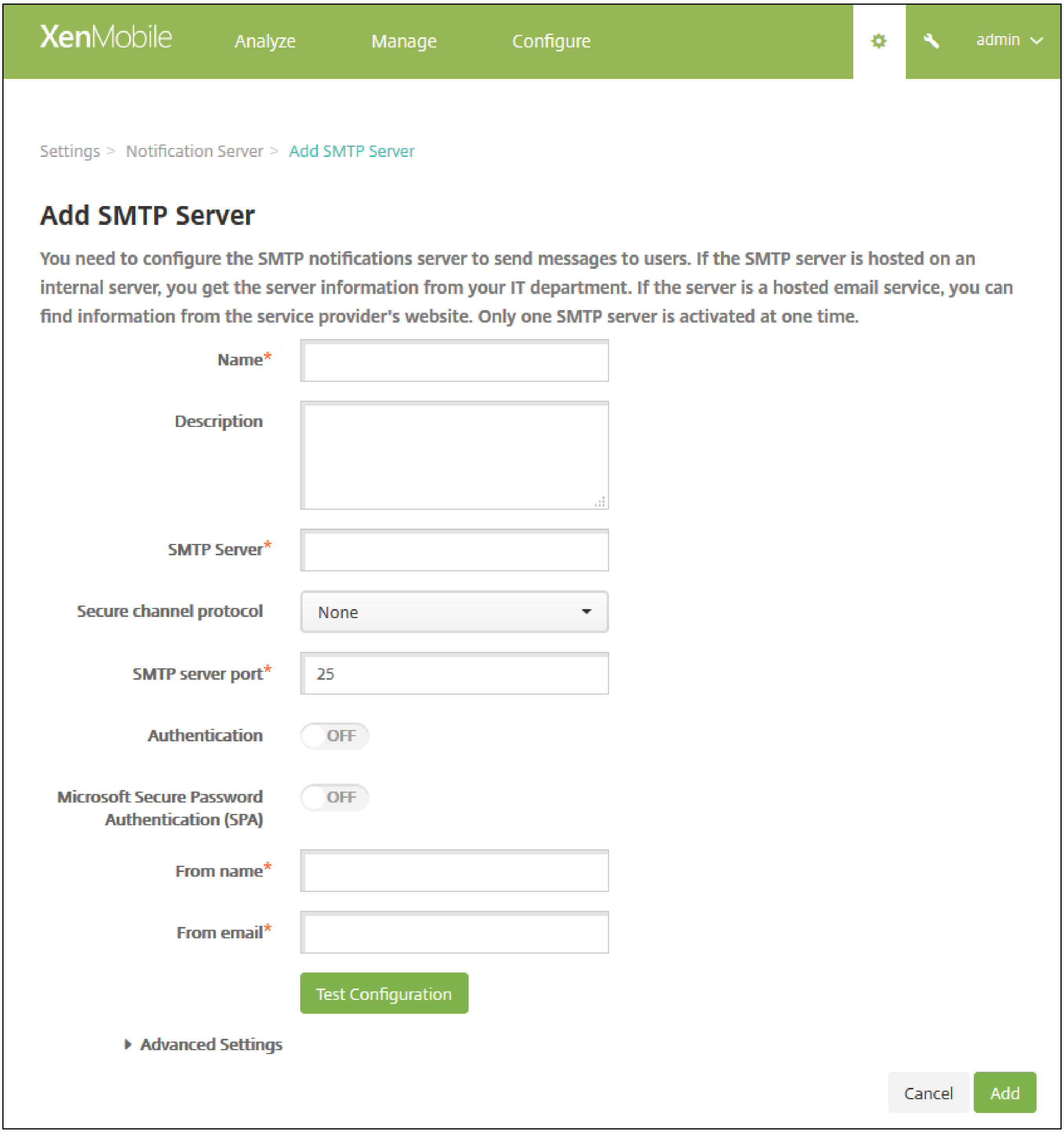
2. Click **Add**. A menu appears with options to configure an SMTP server or an SMS gateway.


Notification Server

You can add and configure SMTP

- To add an SMTP server, click **SMTP Server** and then see To add an SMTP server for the steps to configure this setting.
- To an SMS gateway, click **SMS Gateway** and then see To add an SMS gateway for the steps to configure this setting.

Add an SMTP server



Add SMTP Server

You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP server is activated at one time.

Name*

Description

SMTP Server*

Secure channel protocol: None

SMTP server port*: 25

Authentication: OFF

Microsoft Secure Password Authentication (SPA): OFF

From name*

From email*

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.

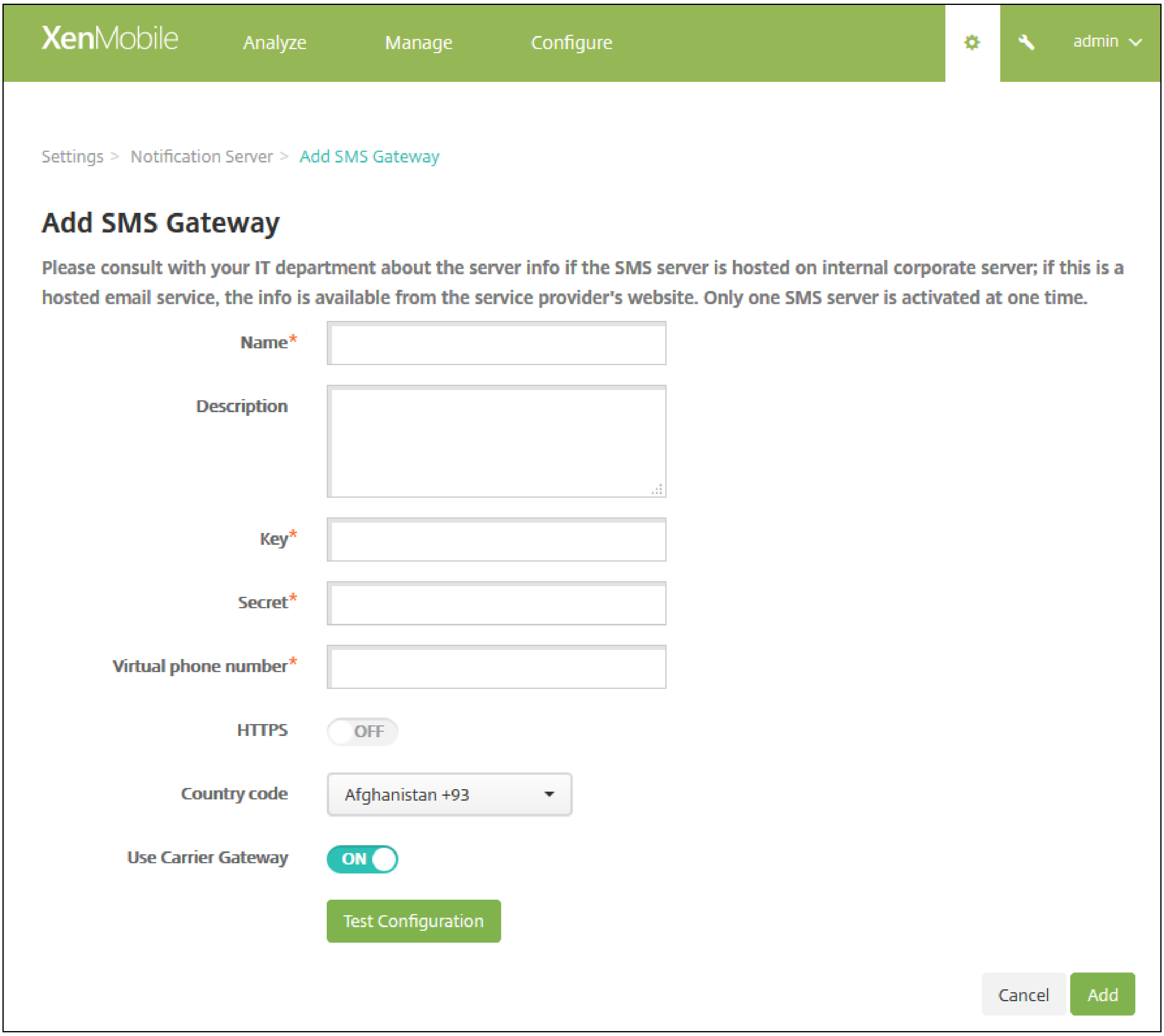
2. Click **Test Configuration** to send a test email notification.

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



Settings > Notification Server > Add SMS Gateway

Add SMS Gateway

Please consult with your IT department about the server info if the SMS server is hosted on internal corporate server; if this is a hosted email service, the info is available from the service provider's website. Only one SMS server is activated at one time.

Name*	
Description	
Key*	
Secret*	
Virtual phone number*	
HTTPS	OFF
Country code	Afghanistan +93
Use Carrier Gateway	ON

Note

XenMobile only supports Nexmo SMS messaging. If you do not already have an account to use Nexmo messaging, visit their website to create one.

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 **OFF**.

  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.

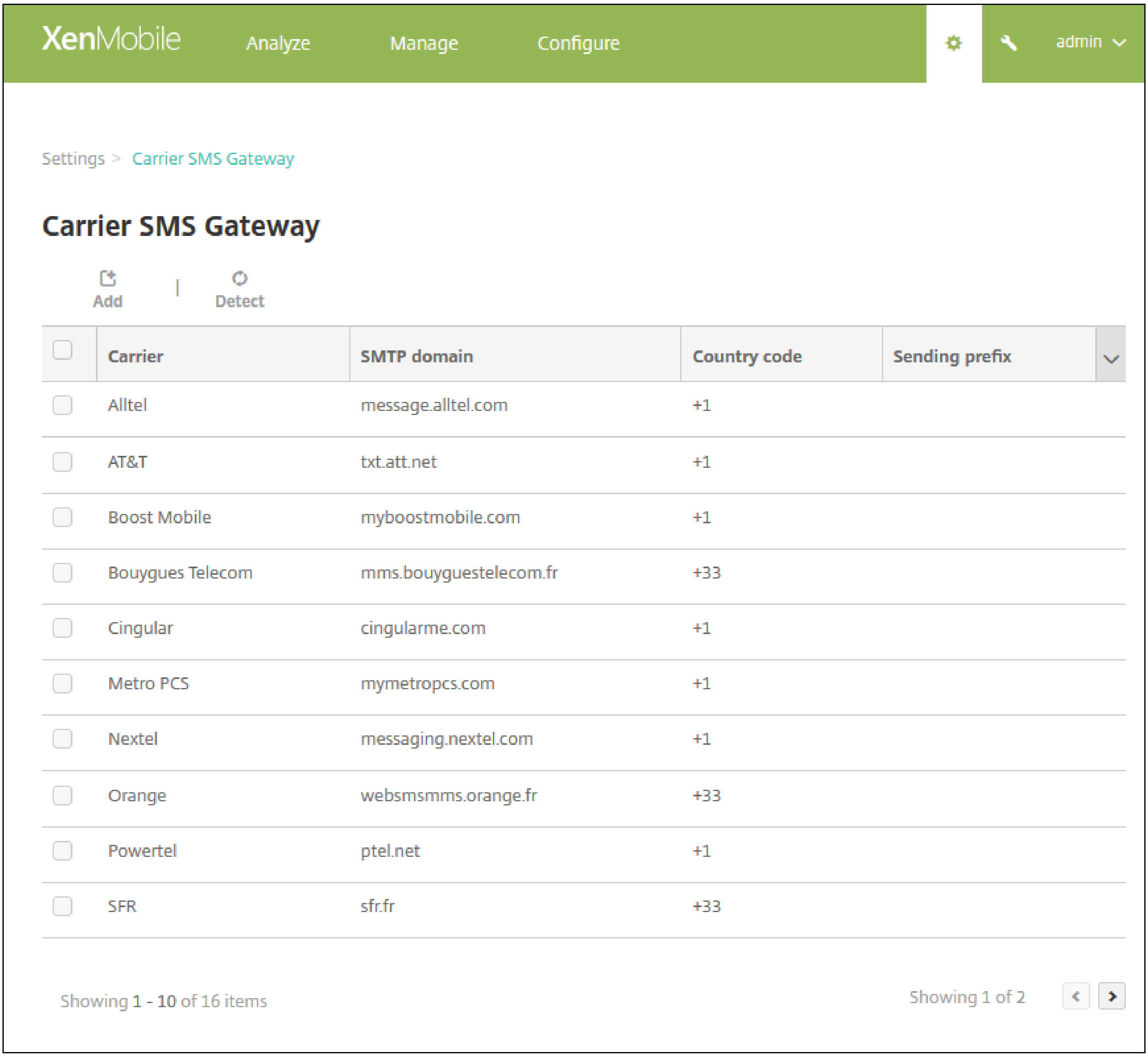
2. Click **Add**.

Add a carrier SMS gateway

You can set up a Carrier SMS Gateway in XenMobile 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 XenMobile 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.



Settings > Carrier SMS Gateway

Carrier SMS Gateway

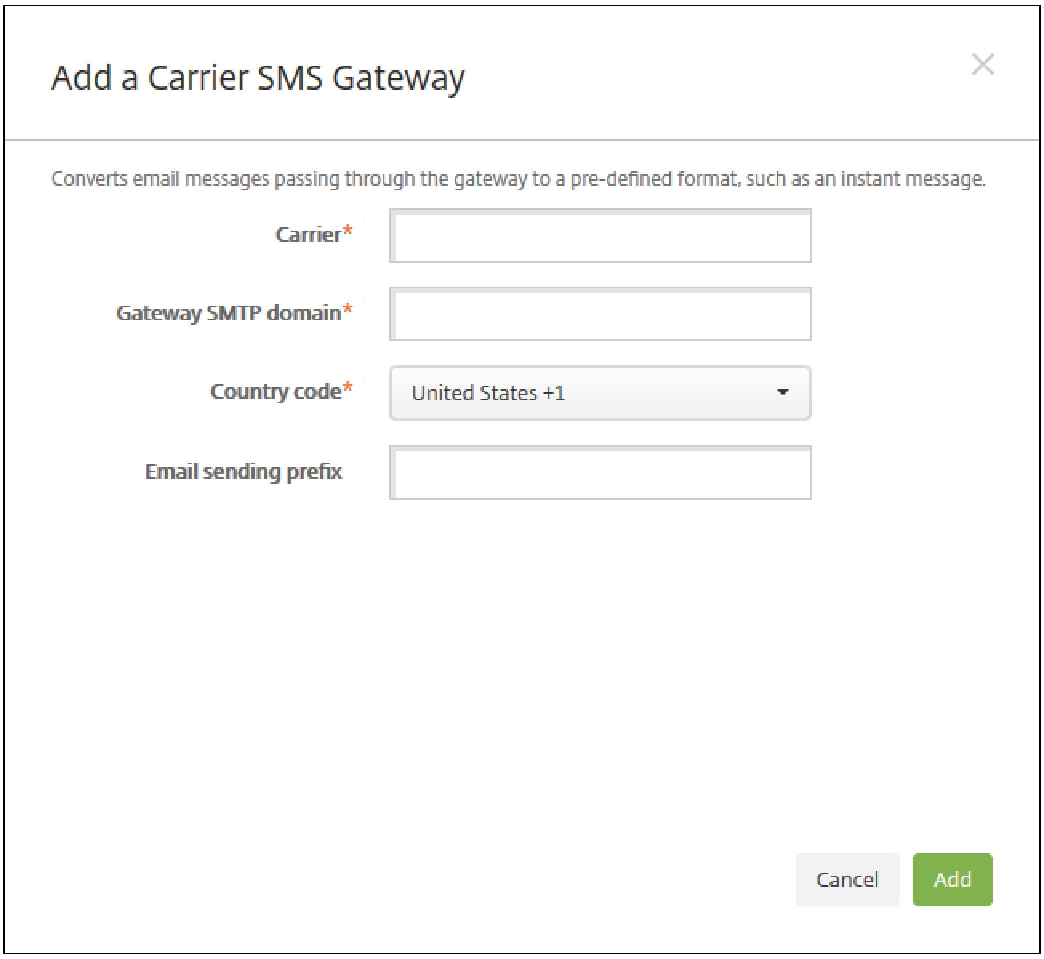
□	Carrier	SMTP domain	Country code	Sending prefix
□	Alltel	message.alltel.com	+1	
□	AT&T	txt.att.net	+1	
□	Boost Mobile	myboostmobile.com	+1	
□	Bouygues Telecom	mms.bouyguestelecom.fr	+33	
□	Cingular	cingularme.com	+1	
□	Metro PCS	mymetropcs.com	+1	
□	Nextel	messaging.nextel.com	+1	
□	Orange	websmsmms.orange.fr	+33	
□	Powertel	ptel.net	+1	
□	SFR	sfr.fr	+33	

Showing 1 - 10 of 16 items

Showing 1 of 2

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.


Add a Carrier SMS Gateway

Converts email messages passing through the gateway to a pre-defined format, such as an instant message.

Carrier*

Gateway SMTP domain*

Country code* United States +1

Email sending prefix

Note: XenMobile only supports Nexmo SMS messaging. If you do not already have an account to use Nexmo messaging, visit their website to create one.

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

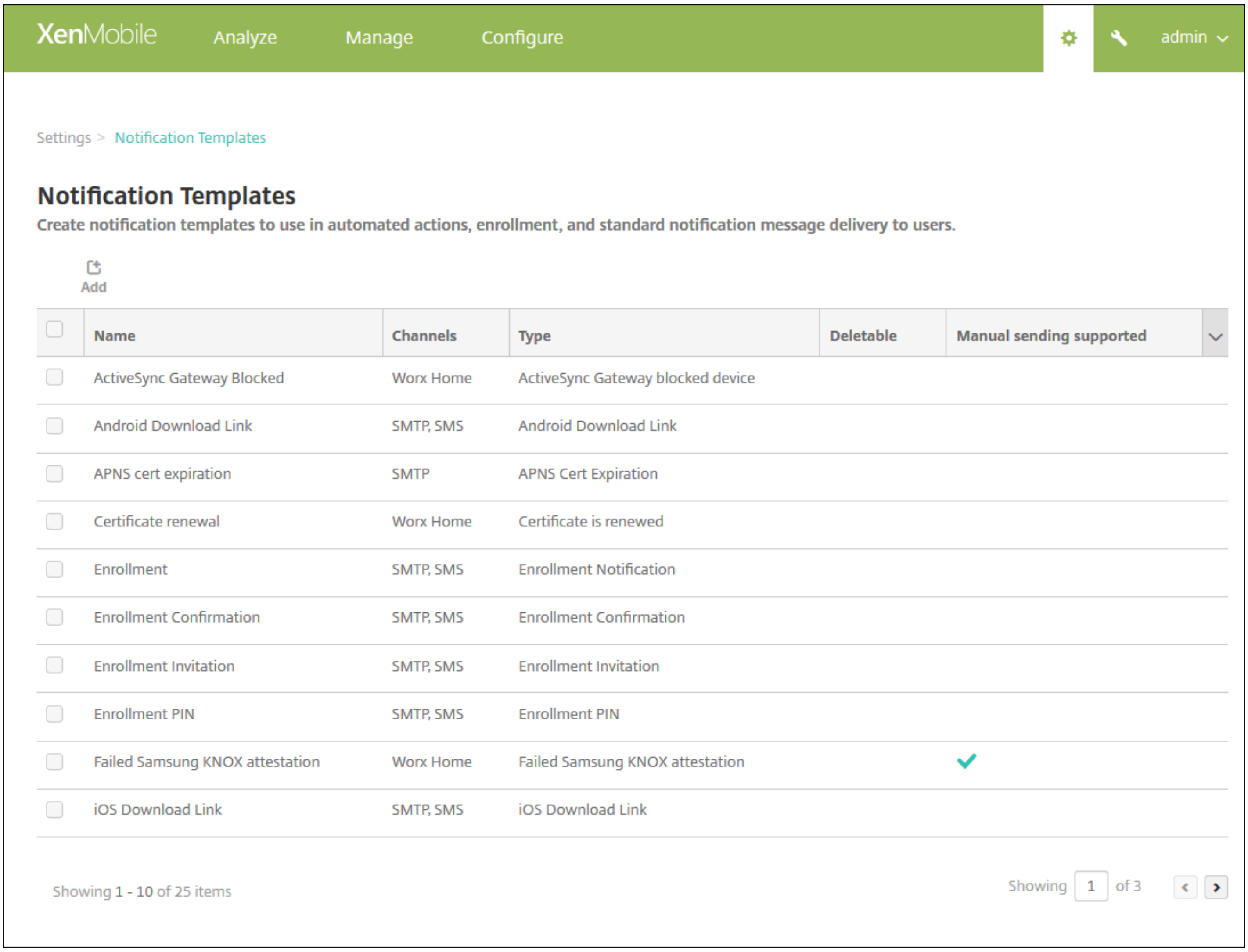
You can create or update notification templates in XenMobile to be used in automated actions, enrollment, and standard notification messages sent to users. You configure the notification templates to send messages over three different channels: Secure Hub, SMTP, or SMS.

XenMobile includes many predefined notification templates that reflect the distinct types of events that XenMobile 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. XenMobile prompts you to set up the channels when you add notification templates if they are not already set up.

1. In the XenMobile 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.



Settings > Notification Templates

Notification Templates

Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.

□	Name	Channels	Type	Deletable	Manual sending supported
□	ActiveSync Gateway Blocked	Worx Home	ActiveSync Gateway blocked device		
□	Android Download Link	SMTP, SMS	Android Download Link		
□	APNS cert expiration	SMTP	APNS Cert Expiration		
□	Certificate renewal	Worx Home	Certificate is renewed		
□	Enrollment	SMTP, SMS	Enrollment Notification		
□	Enrollment Confirmation	SMTP, SMS	Enrollment Confirmation		
□	Enrollment Invitation	SMTP, SMS	Enrollment Invitation		
□	Enrollment PIN	SMTP, SMS	Enrollment PIN		
□	Failed Samsung KNOX attestation	Worx Home	Failed Samsung KNOX attestation		✓
□	iOS Download Link	SMTP, SMS	iOS Download Link		

Showing 1 - 10 of 25 items

Showing 1 of 3

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.

  Important: You are only able to activate the SMTP notification if you have already 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.

> **Important**: You are only able to activate the SMS notification if you have already set up the SMS gateway.

- **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. For information about using macros in a message, see Macros.

5. 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

Note: 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.

2. Click **Delete** to delete the notification template or click **Cancel** to cancel deleting the notification template.

Devices

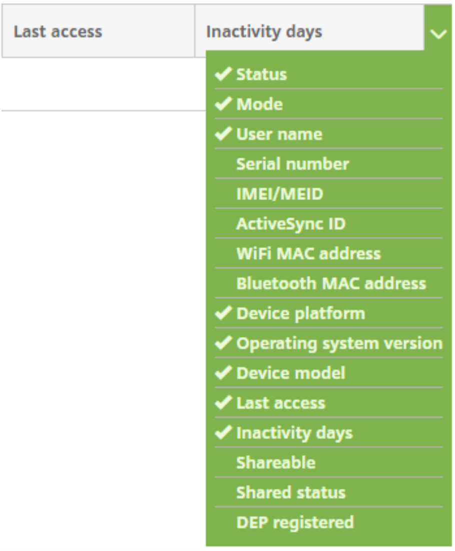
Dec 14, 2017

The XenMobile server 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 XenMobile console with your devices, you can add the devices manually or you can import a list of devices from a file. See Device provisioning file formats, for information about device provisioning file formats.

The **Devices** page in the XenMobile console lists each device and the following information:

- **Status** (icons indicate whether the device is jailbroken, is managed, whether Active Sync Gateway is available, and the deployment state)
- **Mode** (whether the device mode is MDM, MAM, or both)
- Other information about the device, such as **User name**, **Device platform**, **Operating system version**, **Device model**, **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.



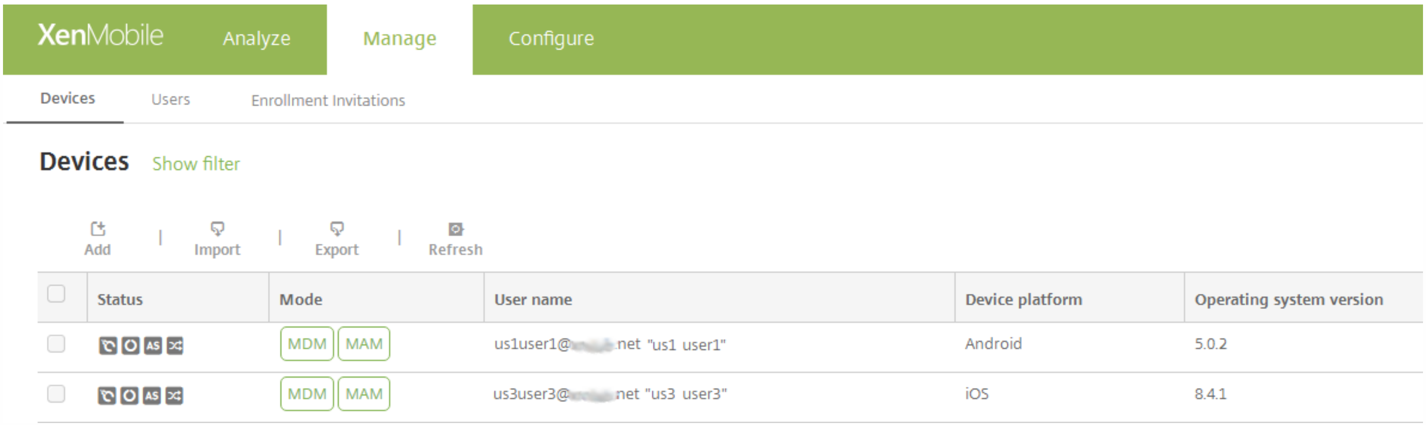
You can add devices manually, import devices from a device provisioning file, edit device details, perform security actions, and send notifications to devices. You can also export all device table data to a .csv file to create a custom report. The server exports all device attributes. If you apply filters, XenMobile uses the filters when creating the .csv file.

See the following sections for details about managing devices:

- Add a device manually
- Import devices from a device provisioning file
- Perform security actions
- Send a notification to devices
- Export the Devices table
- Tag user devices manually
- Device provisioning file formats
- Device property names and values

Add a device manually

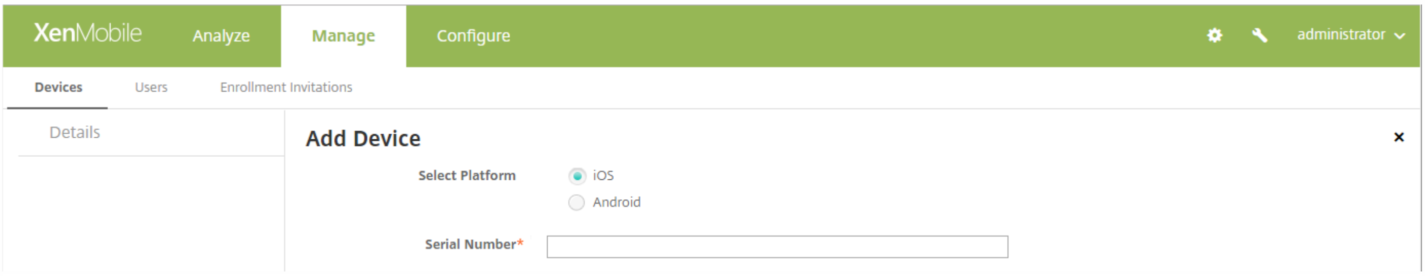
1. In the XenMobile console, click **Manage > Devices**. The **Devices** page appears.



Devices Show filter

□	Status	Mode	User name	Device platform	Operating system version
□		MDM MAM	us1user1@[redacted]net "us1 user1"	Android	5.0.2
□		MDM MAM	us3user3@[redacted]net "us3 user3"	iOS	8.4.1

2. Click **Add**. The **Add Device** page appears.



Add Device

Select Platform ● iOS ○ Android

Serial Number*

3. Configure these settings:

- **Select platform**: Click either **iOS** or **Android**.
- **Serial Number**: Type the device serial number.
- **IMEI/MEID**: Optionally, for Android devices only, type the device IMEI/MEID information.

4. Click **Add**. The **Devices** table appears with the device added to the bottom of the list. Choose the device you added and then in the menu that appears, click **Edit** to view and confirm the device details.

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.

- XenMobile Server configured in Enterprise (XME) or MDM mode
- LDAP configured

- If using local groups and local users:

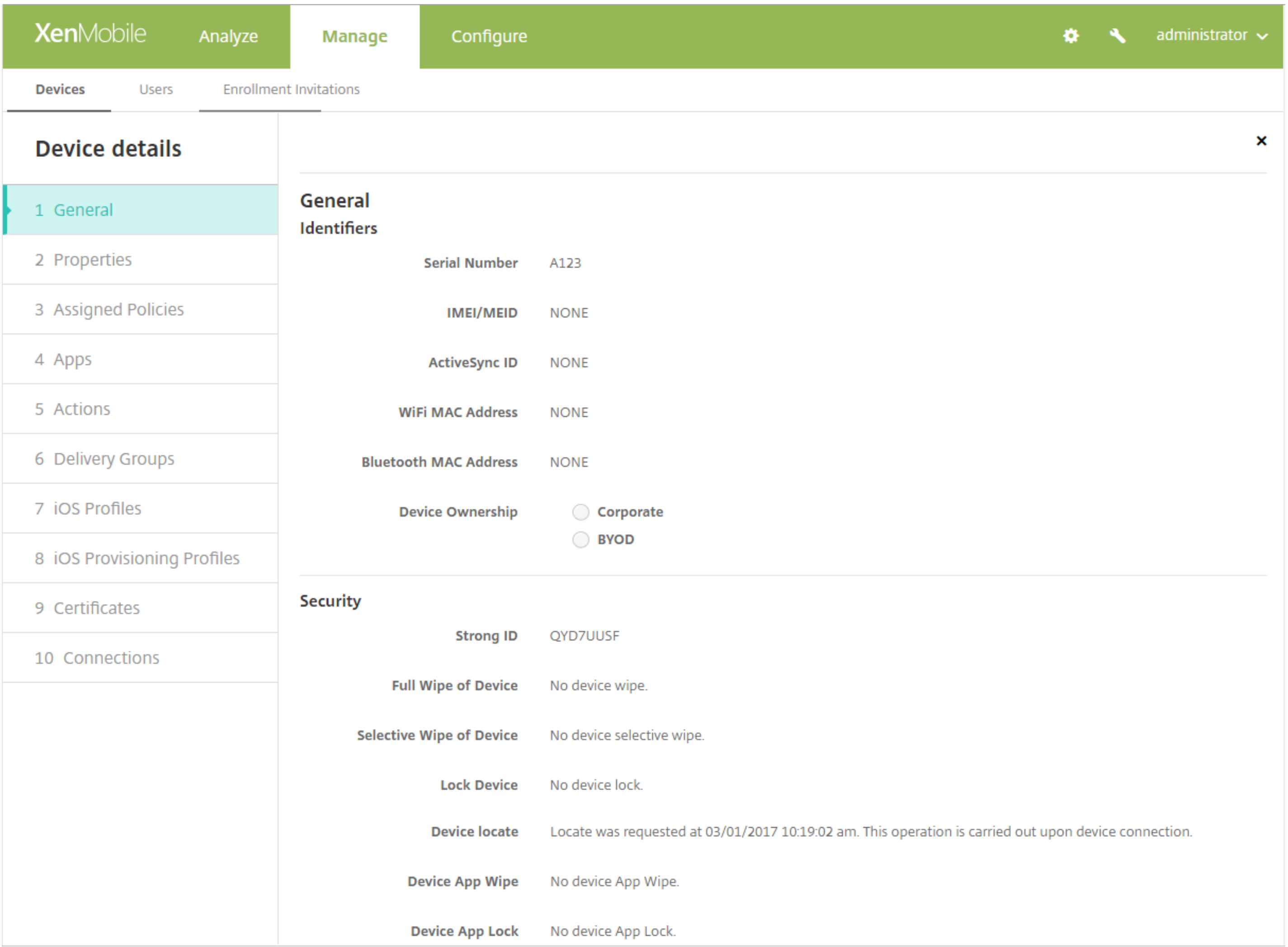
  - One or more local groups.

  - 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.



General

Identifiers

Serial Number	A123
IMEI/MEID	NONE
ActiveSync ID	NONE
WiFi MAC Address	NONE
Bluetooth MAC Address	NONE
Device Ownership	○ Corporate ○ BYOD

Security

Strong ID	QYD7UUSF
Full Wipe of Device	No device wipe.
Selective Wipe of Device	No device selective wipe.
Lock Device	No device lock.
Device locate	Locate was requested at 03/01/2017 10:19:02 am. This operation is carried out upon device connection.
Device App Wipe	No device App Wipe.
Device App Lock	No device App Lock.

5. The **General** page lists device **Identifiers**, such as the serial number, ActiveSync ID, 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 XenMobile 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 Device property names and values in this article.

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. XenMobile deletes the item immediately.

7. The remaining **Device Details** sections contain summary information for the device.

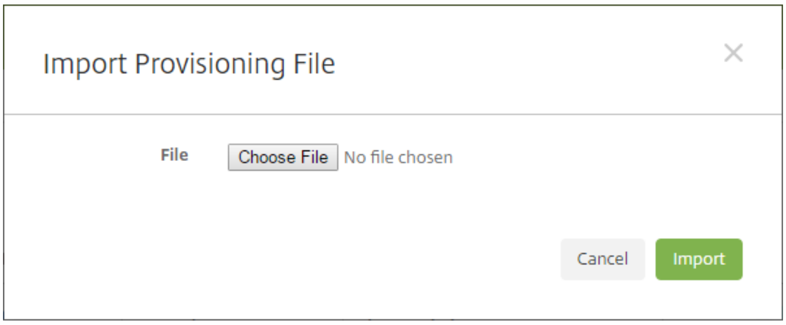
- **Assigned Policies**: Displays the number of assigned policies including the number of deployed, pending, and failed policies. Provides the policy name, type and last deployed information for each policy.
- **Apps**: Displays, for the last inventory, the number of installed, pending, and failed apps. Provides the app name, identifier, type, and other information.
- **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 whether it is managed.
- **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.
- **TouchDown** (Android devices only): Displays information about the last device authentication and the last user authenticated. Provides each applicable policy name and policy value.

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 more information, see Device provisioning file formats in this article.

1. Go to **Manage > Devices** and 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.

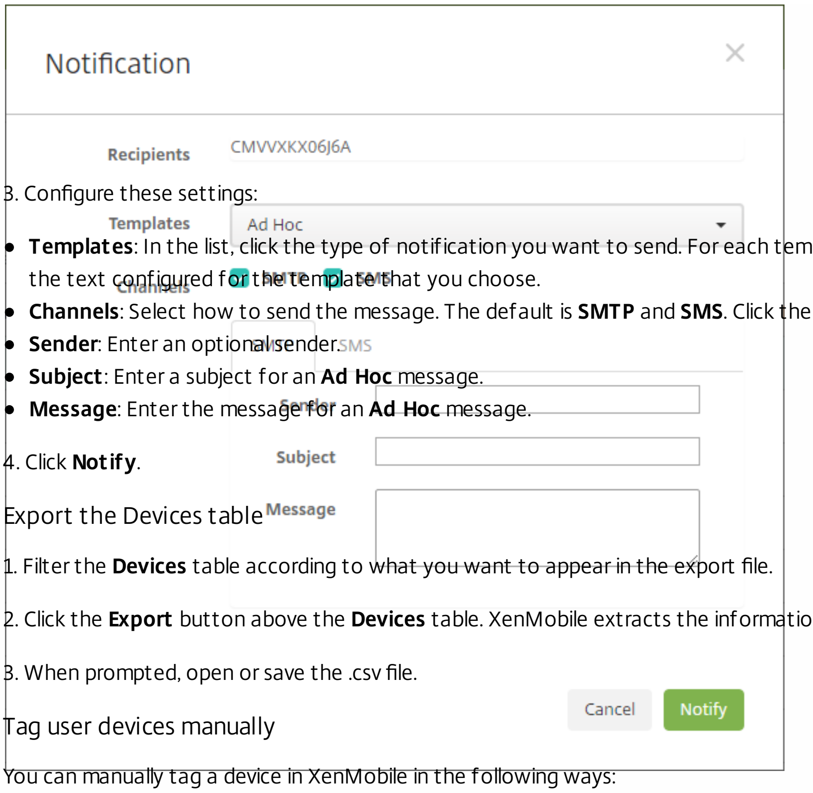
4. To edit the device information, select it and then click **Edit**. For information about the **Device details** pages, see Add a device manually.

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.



Notification

Recipients CMVVXKX06J6A

Templates Ad Hoc

Channels ☑ SMTP ☑ SMS

SMS

Sender

Subject

Message

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**.

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. XenMobile extracts the information in the filtered **Devices** table and converts it to a .csv file.

3. When prompted, open or save the .csv file.

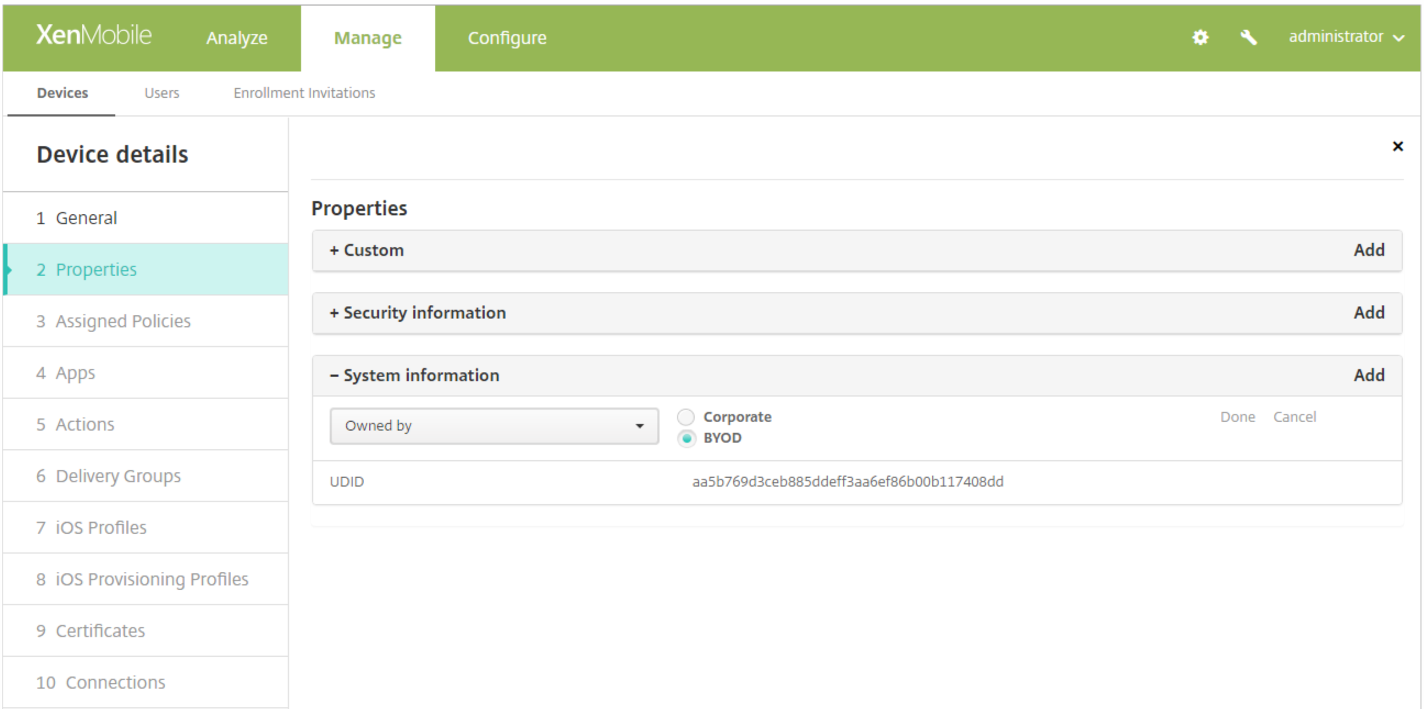
Tag user devices manually

You can manually tag a device in XenMobile 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 XenMobile console.
2. Add the property named **Owned by** and choose either **Corporate** or **BYOD** (employee-owned).



Device details

Properties

+ Custom Add

+ Security information Add

– System information Add

Owned by ○ Corporate ● BYOD Done Cancel

UDID aa5b769d3ceb885ddeff3aa6ef86b00b117408dd

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. XenMobile supports an import file format that is common to all three supported device types: Android, iOS, and Windows.

A provisioning file that you create manually and use to import devices to XenMobile must be in the following format:

SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; ... propertyNameN;propertyValueN

Notes:

- For property names and values, see "Device property names and values" in the next section.
- 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:
  propertyV;test;1;2

  Escape it as follows:
  propertyV\;test\;1\;2
- The serial number is required for iOS devices because the serial number is the iOS device identifier.
- For other device platforms, you must include either the serial number or the IMEI.
- Valid values for **OperatingSystemFamily** are **WINDOWS**, **ANDROID**, or **iOS**.

Example of a device provisioning file

COPY

```
1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyN;propertyV$*&&ééétest

3050BF3F517301081610065510590393;35244201625379903;iOS;test;

4050BF3F517301081610065510590393;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;
```

Each line in the file describes a device. The first entry in the above sample means the following:

- SerialNumber: 1050BF3F517301081610065510590391
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS
- ProertyName: propertyN
- PropertyValue: propertyV\;test\;1\;2;prop 2

Device property names and values

Property name in Manage > Devices page	Name and values for device provisioning file	Values (meaning)	Value type
AIK Present?	WINDOWS_HAS_AIK_PRESENT		String

Account Suspended?	GOOGLE_AW_DIRECTORY_SUSPENDED		String
Activation lock bypass code	ACTIVATION_LOCK_BYPASS_CODE		String
Activation lock enabled	ACTIVATION_LOCK_ENABLED	1 (Yes), 0 (No)	Boolean
Active iTunes account	ACTIVE_ITUNES	1 (Yes), 0 (No)	Boolean
ActiveSync ID	EXCHANGE_ACTIVESYNC_ID		String
ActiveSync device known by MSP	AS_DEVICE_KNOWN_BY_ZMSP	1 (True), 0 (False)	Boolean
Administrator disabled	ADMIN_DISABLED	1 (Yes), 0 (No)	Boolean
Amazon MDM API available	AMAZON_MDM	1 (True), 0 (False)	Boolean
Android for Work Device ID	GOOGLE_AW_DEVICE_ID		String
Android for Work Enabled Device?	GOOGLE_AW_ENABLED_DEVICE		String
Android for Work Install Type	GOOGLE_AW_INSTALL_TYPE	DeviceAdministrator (Device Owner), AvengerManagedProfile (Work Managed Device), ManagedProfile (Work Profile)	String
Antispyware Signature Status (Windows 10)	ANTI_SPYWARE_SIGNATURE_STATUS		Boolean
Antispyware Status (Windows 10)	ANTI_SPYWARE_STATUS		Boolean
Antivirus Signature Status (Windows 10)	ANTI_VIRUS_SIGNATURE_STATUS	Not recent version, Most recent version. N/A	String
Antivirus Status (Windows 10)	ANTI_VIRUS_STATUS	ON and monitoring, Disabled, OFF or not monitoring, Temporarily not monitoring, N/A	String
Asset tag	ASSET_TAG		String
Autoupdate Status	AUTOUPDATE_STATUS		String
Available RAM	MEMORY_AVAILABLE		Integer

Available storage space	TOTAL_DISK_SPACE		Integer
BIOS Info	BIOS_INFO		String
Backup battery	BACKUP_BATTERY_PERCENT		Integer
Baseband firmware version	MODEM_FIRMWARE_VERSION		String
Battery Status	BATTERY_STATUS		String
Battery charging (Windows 8.1 Phone)	BATTERY_CHARGING	1 (True), 0 (False)	Boolean
Battery Charging (Windows 10)	BATTERY_CHARGING_STATUS	1 (True), 0 (False)	Boolean
Battery Remaining (Windows 10)	BATTERY_ESTIMATED_CHARGE_REMAINING		Integer
Bes device known by MSP	BES_DEVICE_KNOWN_BY_ZMSP	1 (True), 0 (False)	Boolean
BES PIN	BES_PIN		String
BES server agent ID	ENROLLMENT_AGENT_ID		String
BES server name	BES_SERVER		String
BES server version	BES_VERSION		String
Bit Locker Status	WINDOWS_HAS_BIT_LOCKER_STATUS		String
Bluetooth MAC address	BLUETOOTH_MAC		String
Boot Debugging Enabled?	WINDOWS_HAS_BOOT_DEBUGGING_ENABLED		String
Boot Manager Rev List Version	WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION		String
CPU clock speed	CPU_CLOCK_SPEED		Integer
CPU type	CPU_TYPE		String
Carrier settings version	CARRIER_SETTINGS_VERSION		String
Cellular latitude	GPS_LATITUDE_FROM_CELLULAR		String
Cellular longitude	GPS_LONGITUDE_FROM_CELLULAR		String

Cellular technology	CELLULAR_TECHNOLOGY		Integer
Cellular timestamp	GPS_TIMESTAMP_FROM_CELLULAR		Date
Change Password at Next Login?	GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN		String
Client device ID	CLIENT_DEVICE_ID		String
Cloud backup enabled	CLOUD_BACKUP_ENABLED	1 (Yes), 0 (No)	Boolean
Code Integrity Enabled?	WINDOWS_HAS_CODE_INTEGRITY_ENABLED		String
Code Integrity Rev List Version	WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION		String
Color	COLOR		String
Creation Time	GOOGLE_AW_DIRECTORY_CREATION_TIME		String
Current carrier network	CURRENT_CARRIER_NETWORK		String
Current mobile country code	CURRENT_MCC		Integer
Current mobile network code	CURRENT_MNC		String
DEP account name	BULK_ENROLLMENT_DEP_ACCOUNT_NAME		String
DEP Policy	WINDOWS_HAS_DEP_POLICY		String
Data roaming allowed	DATA_ROAMING_ENABLED	1 (Yes), 0 (No)	Boolean
Date of the last iCloud backup	LAST_CLOUD_BACKUP_DATE		Date
Description	DESCRIPTION		String
Device Enrollment Program profile assigned	PROFILE_ASSIGN_TIME		Date
Device Enrollment Program profile pushed	PROFILE_PUSH_TIME		Date
Device Enrollment Program profile removed	PROFILE_REMOVE_TIME		Date
Device Enrollment Program registration by	DEVICE_ASSIGNED_BY		String
Device Enrollment Program registration date	DEVICE_ASSIGNED_DATE		Date

Device Type	DEVICE_TYPE		String
Device model	MODEL_ID		String
Device name	DEVICE_NAME		String
Do Not Disturb activated	DO_NOT_DISTURB	1 (Yes), 0 (No)	Boolean
ELAM Driver Loaded?	WINDOWS_HAS_ELAM_DRIVER_LOADED		String
Encryption Compliance (Windows 10)	ENCRYPTION_COMPLIANCE	Encrypted, Not Encrypted	String
ENROLLMENT_KEY_GENERATION_DATE	ENROLLMENT_KEY_GENERATION_DATE		Date
Enterprise ID	ENTERPRISE_ID		String
External storage 1: available space	EXTERNAL_STORAGE1_FREE_SPACE		Integer
External storage 1: name	EXTERNAL_STORAGE1_NAME		String
External storage 1: total space	EXTERNAL_STORAGE1_TOTAL_SPACE		Integer
External storage 2: available space	EXTERNAL_STORAGE2_FREE_SPACE		Integer
External storage 2: name	EXTERNAL_STORAGE2_NAME		String
External storage 2: total space	EXTERNAL_STORAGE2_TOTAL_SPACE		Integer
External storage encrypted	EXTERNAL_ENCRYPTION	1 (Yes), 0 (No)	Boolean
Firewall Status (Windows 8.1 Phone)	FIREWALL_STATUS		String
Firewall Status (Windows 10)	DEVICE_FIREWALL_STATUS	On and monitoring, Disabled, Off or not monitoring, Temporarily not monitoring, N/A	String
Firmware version	FIRMWARE_VERSION		String
First synchronization	ZMSP_FIRST_SYNC		Date
GPS altitude	GPS_ALTITUDE_FROM_GPS		String
GPS latitude	GPS_LATITUDE_FROM_GPS		String

GPS longitude	GPS_LONGITUDE_FROM_GPS		String
GPS timestamp	GPS_TIMESTAMP_FROM_GPS		Date
Google Directory Alias	GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS		String
Google Directory Family Name	GOOGLE_AW_DIRECTORY_FAMILY_NAME		String
Google Directory Name	GOOGLE_AW_DIRECTORY_NAME		String
Google Directory Primary Email	GOOGLE_AW_DIRECTORY_PRIMARY		String
Google Directory User ID	GOOGLE_AW_DIRECTORY_USER_ID		String
HAS_CONTAINER	HAS_CONTAINER	1 (Yes), 0 (No)	Boolean
HTC API version	HTC_MDM_VERSION		String
HTC MDM API available	HTC_MDM	1 (Yes), 0 (No)	Boolean
Hardware encryption capabilities	HARDWARE_ENCRYPTION_CAPS		Integer
Hash of the iTunes store account currently logged on	ITUNES_STORE_ACCOUNT_HASH		String
Home carrier network	SIM_CARRIER_NETWORK		String
Home mobile country code	SIM_MCC		Integer
Home mobile network code	SIM_MNC		String
ICCID	ICCID		String
IMEI/MEID number	IMEI		String
IMSI	IMSI		String
IP location	IP_LOCATION		String
Identity	AS_DEVICE_IDENTITY		String
Internal storage encrypted	LOCAL_ENCRYPTION	1 (True), 0 (False)	Boolean
IPV4 Address (Windows 10)	IP_ADDRESSV4		String
IPV6 Address (Windows 10)	IP_ADDRESSV6		String

Issued At	WINDOWS_HAS_ISSUED_AT		String
Jailbroken/Rooted	ROOT_ACCESS	1 (Yes), 0 (No)	Boolean
Kernel Debugging Enabled?	WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED		String
Kiosk mode	IS_KIOSK	1 (True), 0 (False)	Boolean
Last known IP address	LAST_IP_ADDR		String
Last policy update time	LAST_POLICY_UPDATE_TIME		Date
Last synchronization	ZMSP_LAST_SYNC		Date
Locator service enabled	DEVICE_LOCATOR	1 (Yes), 0 (No)	Boolean
MAC Address Network Connection (Windows 10)	MAC_NETWORK_CONNECTION	1 (Yes), 0 (No)	Boolean
MAC Address Type (Windows 10)	MAC_ADDRESS_TYPE	Unknown, LAN, WLAN	String
MDX_SHARED_ENCRYPTION_KEY	MDX_SHARED_ENCRYPTION_KEY		String
MEID	MEID		String
Mailbox Setup	GOOGLE_AW_DIRECTORY_MAILBOX_SETUP		String
Main battery	MAIN_BATTERY_PERCENT		Integer
Mobile phone number	TEL_NUMBER		String
Model ID	SYSTEM_OEM		String
Network Adapter Type	NETWORK_ADAPTER_TYPE		String
NitroDesk TouchDown installed	TOUCHDOWN_FIND	1 (True), 0 (False)	Boolean
NitroDesk TouchDown licensed via MDM	TOUCHDOWN_LICENSED_VIA_MDM	1 (True), 0 (False)	Boolean
Operating system build	SYSTEM_OS_BUILD		String
Operating System Edition (Windows 10)	OS_EDITION		String
Operating system language (locale)	SYSTEM_LANGUAGE		String

Operating system version	SYSTEM_OS_VERSION		String
Organization address	ORGANIZATION_ADDRESS		String
Organization e-mail	ORGANIZATION_EMAIL		String
Organization magic	ORGANIZATION_MAGIC		String
Organization name	ORGANIZATION_NAME		String
Organization phone number	ORGANIZATION_PHONE		String
Other	OTHER		String
Out of Compliance	OUT_OF_COMPLIANCE	1 (True), 0 (False)	Boolean
Owned by	CORPORATE_OWNED	1 (Corporate), 0 (BYOD)	Boolean
PCR0	WINDOWS_HAS_PCR0		String
PIN code for geofence	PIN_CODE_FOR_GEO_FENCE		String
Passcode compliant	PASSCODE_IS_COMPLIANT	1 (Yes), 0 (No)	Boolean
Passcode compliant with configuration	PASSCODE_IS_COMPLIANT_WITH_CFG	1 (Yes), 0 (No)	Boolean
Passcode present	PASSCODE_PRESENT	1 (Yes), 0 (No)	Boolean
Perimeter breach	GPS_PERIMETER_BREACH	1 (Yes), 0 (No)	Boolean
Personal Hotspot activated	PERSONAL_HOTSPOT_ENABLED	1 (Yes), 0 (No)	Boolean
Platform	SYSTEM_PLATFORM		String
Platform API level	API_LEVEL		Integer
Policy name	POLICY_NAME		String
Primary Phone Number	IDENTITY1_PHONENUMBER		String
Primary SIM Carrier Operator (Windows 10)	IDENTITY1_CARRIER_NETWORK_OPERATOR		String
Primary SIM ICCID (Windows 10)	IDENTITY1_ICCID		String
Primary SIM IMEI	IDENTITY1_IMEI		String

Primary SIM IMSI	IDENTITY1_IMSI		String
Primary SIM Roaming	IDENTITY1_ROAMING	1 (True), 0 (False)	Boolean
Primary SIM Roaming Compliance (Windows 10)	IDENTITY1_ROAMING_COMPLIANCE	1 (True), 0 (False)	Boolean
Product name	PRODUCT_NAME		String
Publisher Device ID	PUBLISHER_DEVICE_ID		String
Reset Count	WINDOWS_HAS_RESET_COUNT		String
Restart Count	WINDOWS_HAS_RESTART_COUNT		String
SBCP Hash	WINDOWS_HAS_SBCP_HASH		String
SMS capable	IS_SMS_CAPABLE	1 (True), 0 (False)	Boolean
Safe Mode Enabled?	WINDOWS_HAS_SAFE_MODE		String
Samsung KNOX API available	SAMSUNG_KNOX	1 (True), 0 (False)	Boolean
Samsung KNOX API version	SAMSUNG_KNOX_VERSION		String
Samsung KNOX attestation	SAMSUNG_KNOX_ATTESTED	1 (Passed), 0 (Failed)	Boolean
Samsung KNOX attestation updated date	SAMSUNG_KNOX_ATT_UPDATED_TIME		Date
Samsung SAFE API available	SAMSUNG_MDM	1 (True), 0 (False)	Boolean
Samsung SAFE API version	SAMSUNG_MDM_VERSION		String
Screen: X-axis resolution	SCREEN_XDPI		Integer (PPI)
Screen: Y-axis resolution	SCREEN_YDPI		Integer (PPI)
Screen: height	SCREEN_HEIGHT		Integer (pixels)
Screen: number of colors	SCREEN_NB_COLORS		Integer
Screen: size	SCREEN_SIZE		Decimal (inches)

Screen: width	SCREEN_WIDTH		Integer (pixels)
Secondary Phone Number	IDENTITY2_PHONENUMBER		String
Secondary SIM IMEI	IDENTITY2_IMEI		String
Secondary SIM IMSI	IDENTITY2_IMSI		String
Secondary SIM Roaming	IDENTITY2_ROAMING	1 (True), 0 (False)	Boolean
Secure Boot Enabled? (Windows 8.1 Phone)	WINDOWS_HAS_SECURE_BOOT_ENABLED		String
Secure Boot Status (Windows 10)	SECURE_BOOT_STATE	Not supported, Enabled, Disabled	String
SecureContainer Enabled	WINDOWS_HAS_BIT_LOCKER_STATUS		String
Serial number	SERIAL_NUMBER		String
Sony Enterprise API available	SONY_MDM	1 (True), 0 (False)	Boolean
Sony Enterprise API version	SONY_MDM_VERSION		String
Supervised	Supervised	1 (Yes), 0 (No)	Boolean
Suspension Reason	GOOGLE_AW_DIRECTORY_SUSPENTION_REASON		String
Tampered Status	TAMPERED_STATUS		String
Terms & Conditions	TERMS_AND_CONDITIONS		String
Terms And Agreement Accepted?	GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS		String
Test Signing Enabled?	WINDOWS_HAS_TEST_SIGNING_ENABLED		String
Total RAM	MEMORY		Integer
Total storage space	FREEDISK		Integer
TPM Version (Windows 10)	TPM_VERSION		String
UDID	UDID		String
User Account Control Status	UAC_STATUS	Not supported,	String

(Windows 10)		Enabled, Disabled	
User agent	USER_AGENT		String
User defined #1	USER_DEFINED_1		String
User defined #2	USER_DEFINED_2		String
User defined #3	USER_DEFINED_3		String
User language (locale)	USER_LANGUAGE		String
VSM Enabled?	WINDOWS_HAS_VSM_ENABLED		String
Vendor	VENDOR		String
Voice capable	IS_VOICE_CAPABLE	1 (True), 0 (False)	Boolean
Voice roaming allowed	VOICE_ROAMING_ENABLED	1 (Yes), 0 (No)	Boolean
WINDOWS_ENROLLMENT_KEY	WINDOWS_ENROLLMENT_KEY		String
WNS Notification Status	WNS_PUSH_STATUS		String
WNS Notification URL	PROPERTY_WNS_PUSH_URL		String
WNS Notification URL expiry date	PROPERTY_WNS_PUSH_URL_EXPIRY		String
WiFi MAC address	WIFI_MAC		String
WinPE Enabled?	WINDOWS_HAS_WINPE		String
XenMobile agent ID	AGENT_ID		String
XenMobile agent revision	EW_REVISION		String
XenMobile agent version	EW_VERSION		String

ActiveSync Gateway

Sep 06, 2017

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 XenMobile. Based on these rules, you can allow or deny devices access to ActiveSync data. For example, if you activate the rule Missing Required Apps, XenMobile 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**.

For more information about the App Access device policy, see App access device policies.

XenMobile supports the following rules:

Anonymous Devices: Checks if a device is in anonymous mode. This check is available if XenMobile 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, XenMobile 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 XenMobile 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 XenMobile 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.

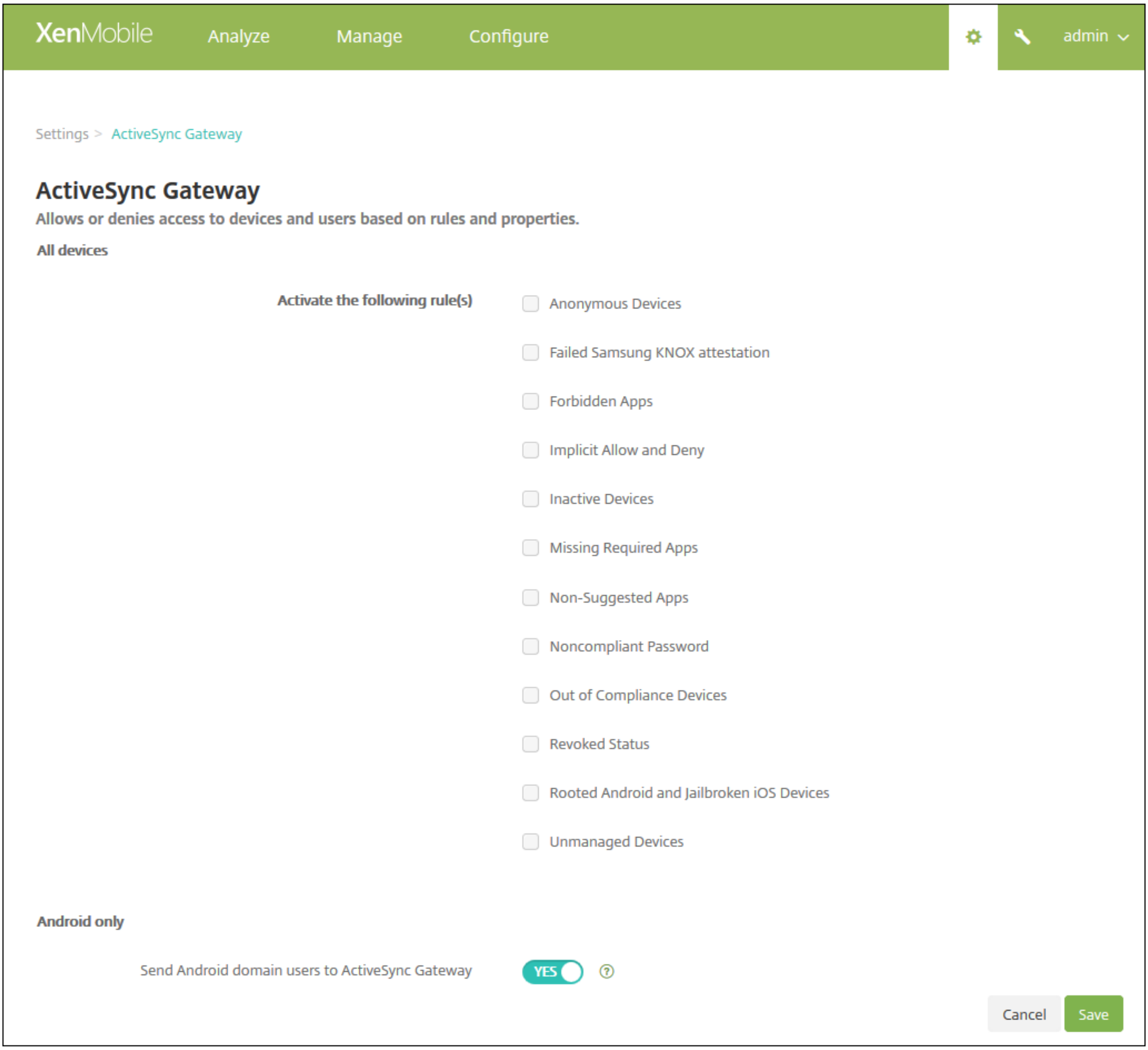
Unmanaged Devices: Check whether a device is still in a managed state, under XenMobile control. For example, a device running in MAM mode or an un-enrolled device is not managed.

Send Android domain users to ActiveSync Gateway: Click **YES** to ensure that XenMobile sends Android device information to the ActiveSync Gateway.

To configure the ActiveSync Gateway settings

1. In the XenMobile 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.



Settings > ActiveSync Gateway

ActiveSync Gateway

Allows or denies access to devices and users based on rules and properties.

All devices

Activate the following rule(s)

□ Anonymous Devices
□ Failed Samsung KNOX attestation
□ Forbidden Apps
□ Implicit Allow and Deny
□ Inactive Devices
□ Missing Required Apps
□ Non-Suggested Apps
□ Noncompliant Password
□ Out of Compliance Devices
□ Revoked Status
□ Rooted Android and Jailbroken iOS Devices
□ Unmanaged Devices

Android only

Send Android domain users to ActiveSync Gateway: YES

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 XenMobile sends Android device information to the ActiveSync Gateway.

5. Click **Save**.

Android for Work

Jan 09, 2018

Android for Work is a secure workspace available on Android devices running Android 5.0 and later. The workspace isolates business accounts, apps, and data from personal accounts, apps, and data. In XenMobile, you manage both bring your own device (BYOD) and company-owned Android devices by having user create a separate work profile on their devices. By combining hardware encryption and the policies you deploy, you securely separate the corporate and personal areas on a device. You can remotely manage or wipe all corporate policies, apps, and data without affecting the personal area of the user. For more information about supported Android devices, see the Google Android Enterprise website.

You use Google Play to add, buy, and approve apps for deployment to the Android for Work workspace on a device. You can use Google Play to deploy your private Android apps, in addition to public and third-party apps. When you add a paid public app store app to XenMobile for Android for Work, you can review the Bulk Purchase licensing status. That status is the total number of licenses available, the number now in use, and the email address of each user consuming the licenses. For details about adding an app to XenMobile, see To add a public app store app to XenMobile.

Setting up Android for Work

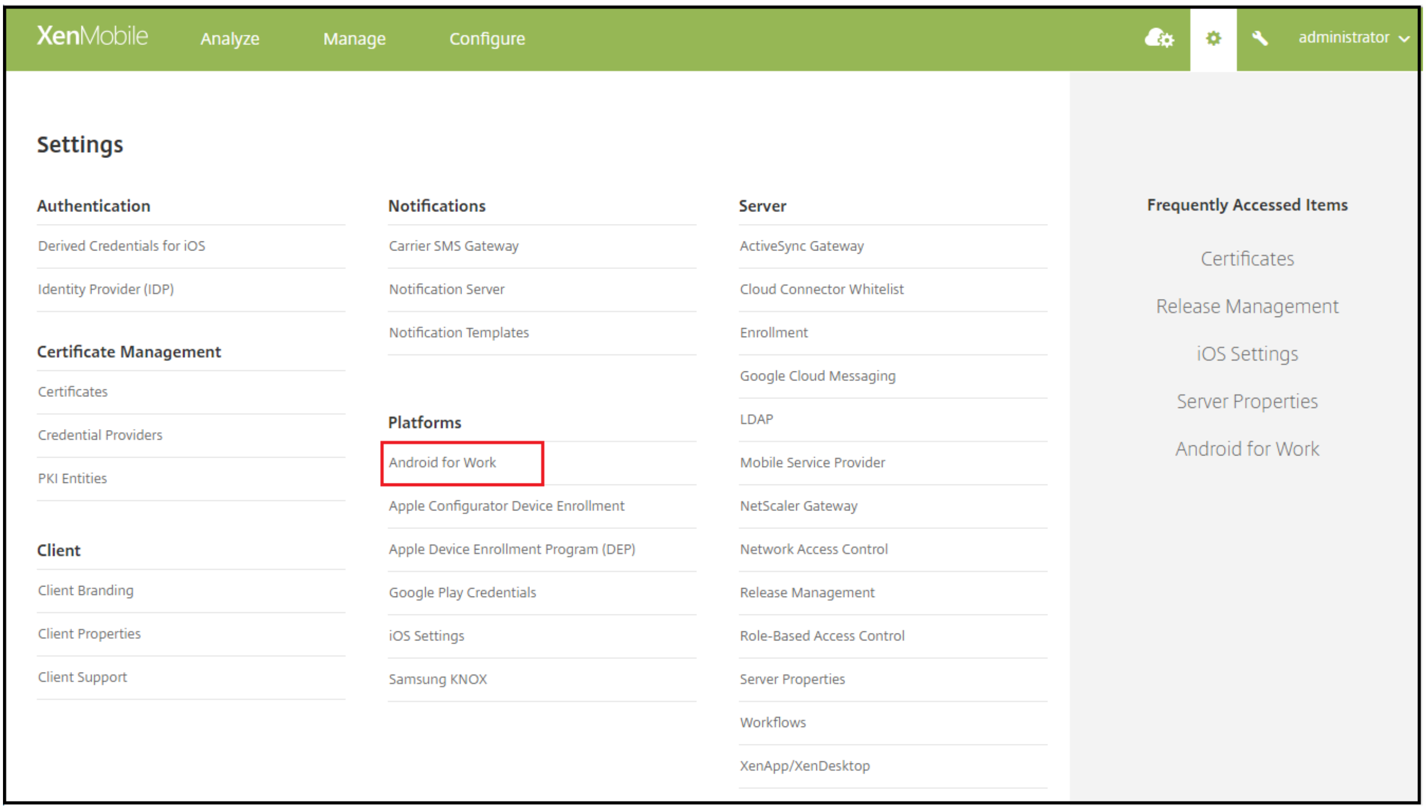
XenMobile provides a simple way to set up Android for Work for your organization. Using XenMobile Management Tools, you bind XenMobile as your enterprise mobility management provider through Google Play and create an enterprise for Android for Work.

Note: G Suite customers, see "Legacy Android for Work for G Suite" customers.

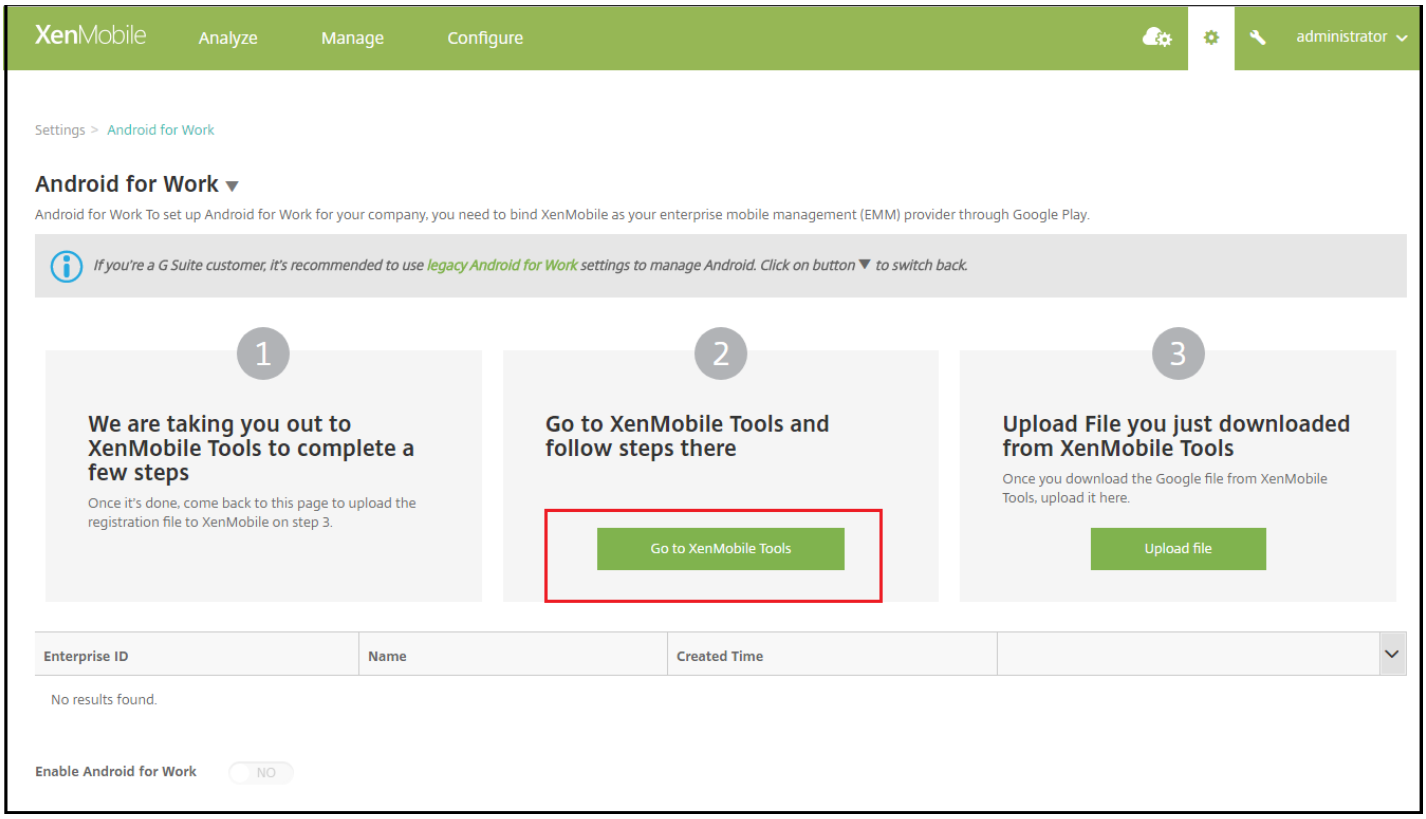
You'll need:
• Your Citrix account credentials to sign in to XenMobile Tools
• You corporate Google ID credentials to sign in to Google Play

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

2. On the Settings page, click **Android for Work**.



3. On the Android for Work page in XenMobile Settings, click **Go to XenMobile Tools.**



Settings > Android for Work

Android for Work ▾

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

If you're a G Suite customer, it's recommended to use legacy Android for Work settings to manage Android. Click on button ▼ to switch back.

1 We are taking you out to XenMobile Tools to complete a few steps

Once it's done, come back to this page to upload the registration file to XenMobile on step 3.

2 Go to XenMobile Tools and follow steps there

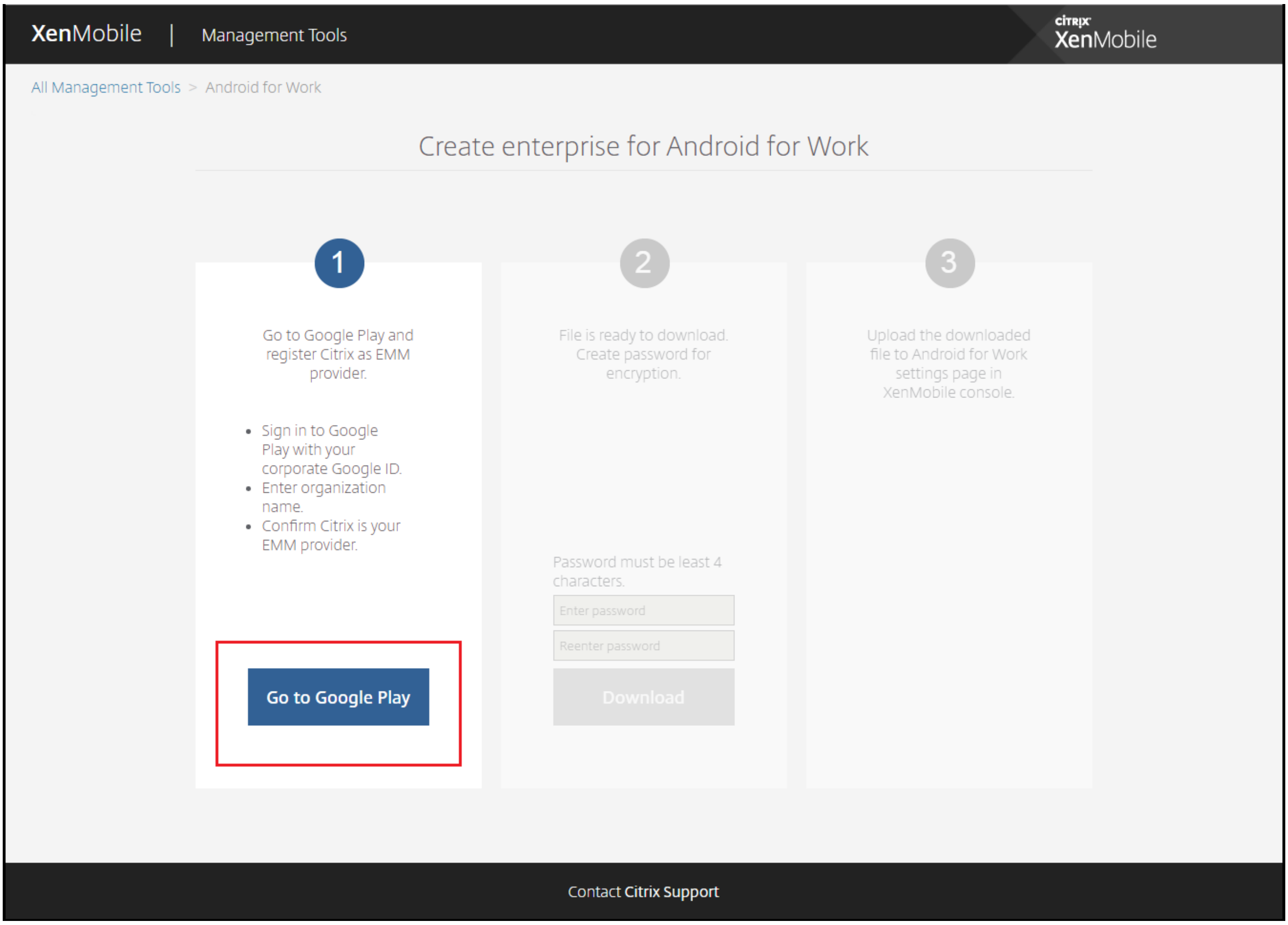
3 Upload File you just downloaded from XenMobile Tools

Once you download the Google file from XenMobile Tools, upload it here.

Enterprise ID	Name	Created Time	
No results found.			

Enable Android for Work: NO

4. Sign in to your Citrix account if prompted.
5. In the Android for Work page in XenMobile Tools Management, click **Go to Google Play**.



XenMobile | Management Tools

All Management Tools > Android for Work

Create enterprise for Android for Work

1 Go to Google Play and register Citrix as EMM provider.

- Sign in to Google Play with your corporate Google ID.
- Enter organization name.
- Confirm Citrix is your EMM provider.

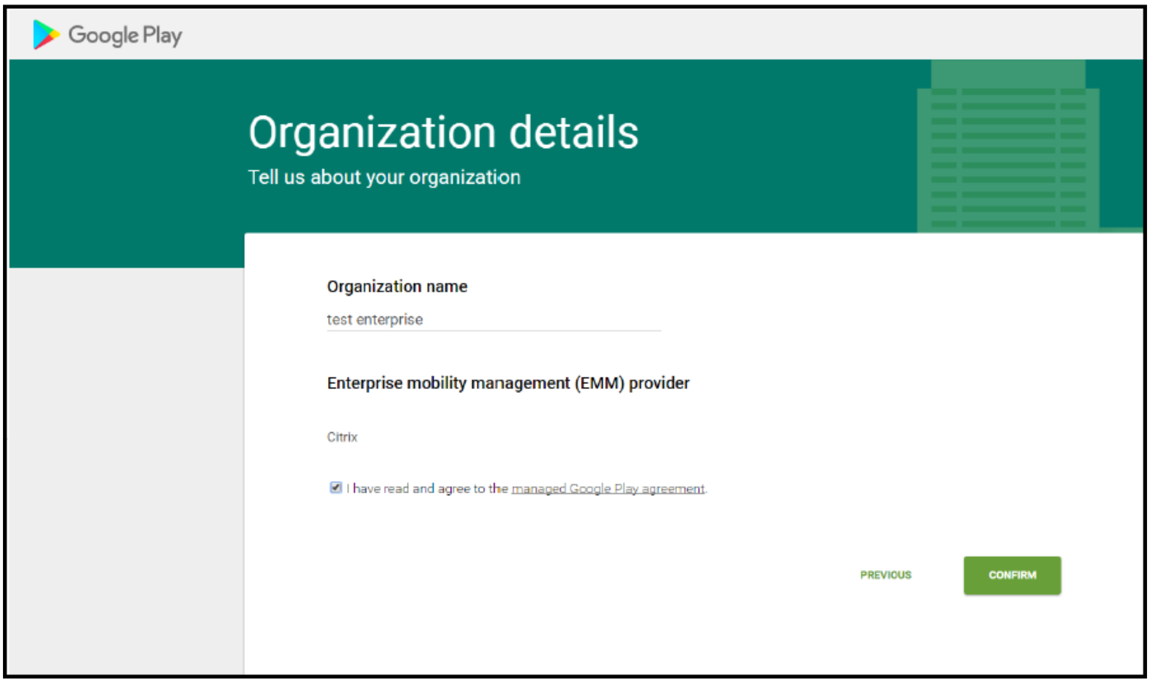
2 File is ready to download. Create password for encryption.

Password must be least 4 characters.

3 Upload the downloaded file to Android for Work settings page in XenMobile console.

6. In Google Play, register Citrix as your organization enterprise mobility management:

   a. Enter your organizations name.
   b. Ensure that Citrix is shown as you enterprise mobility management.
   c. Accept the terms.
   d. Click **Confirm**.



Organization details

Tell us about your organization

Organization name

test enterprise

Enterprise mobility management (EMM) provider

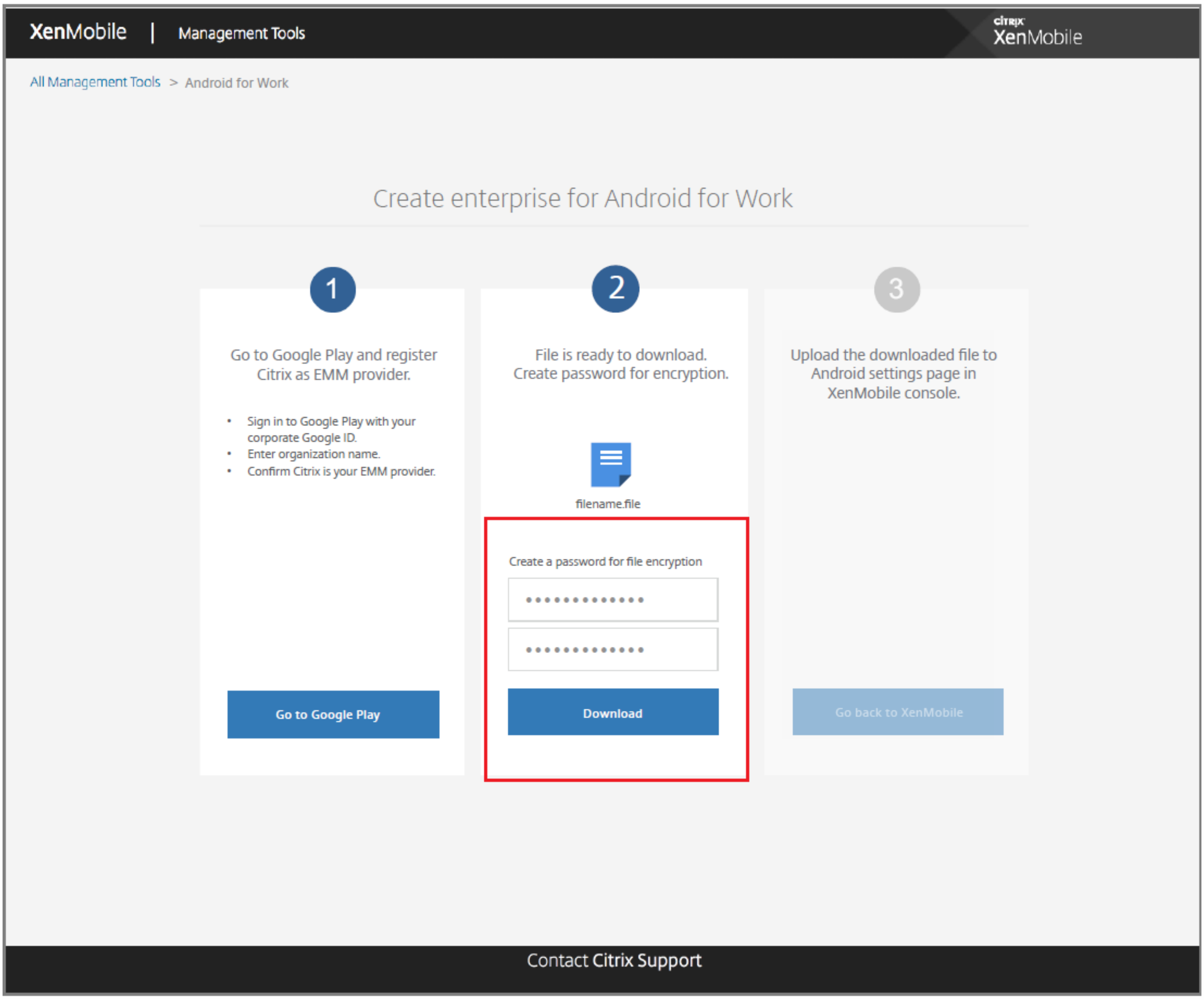
Citrix

☑ I have read and agree to the managed Google Play agreement.

e. In the page that appears, click **Complete Registration**.

This creates a file for you to download and then upload to XenMobile.

7. In the Android for Work page in XenMobile Tools Management, click **Download**.
8. Create a password for file encryption. You'll need this again when you upload the file.



XenMobile | Management Tools
CITRIX XenMobile
All Management Tools > Android for Work

Create enterprise for Android for Work

1 Go to Google Play and register Citrix as EMM provider.

- Sign in to Google Play with your corporate Google ID.
- Enter organization name.
- Confirm Citrix is your EMM provider.

2 File is ready to download. Create password for encryption.

filename.file

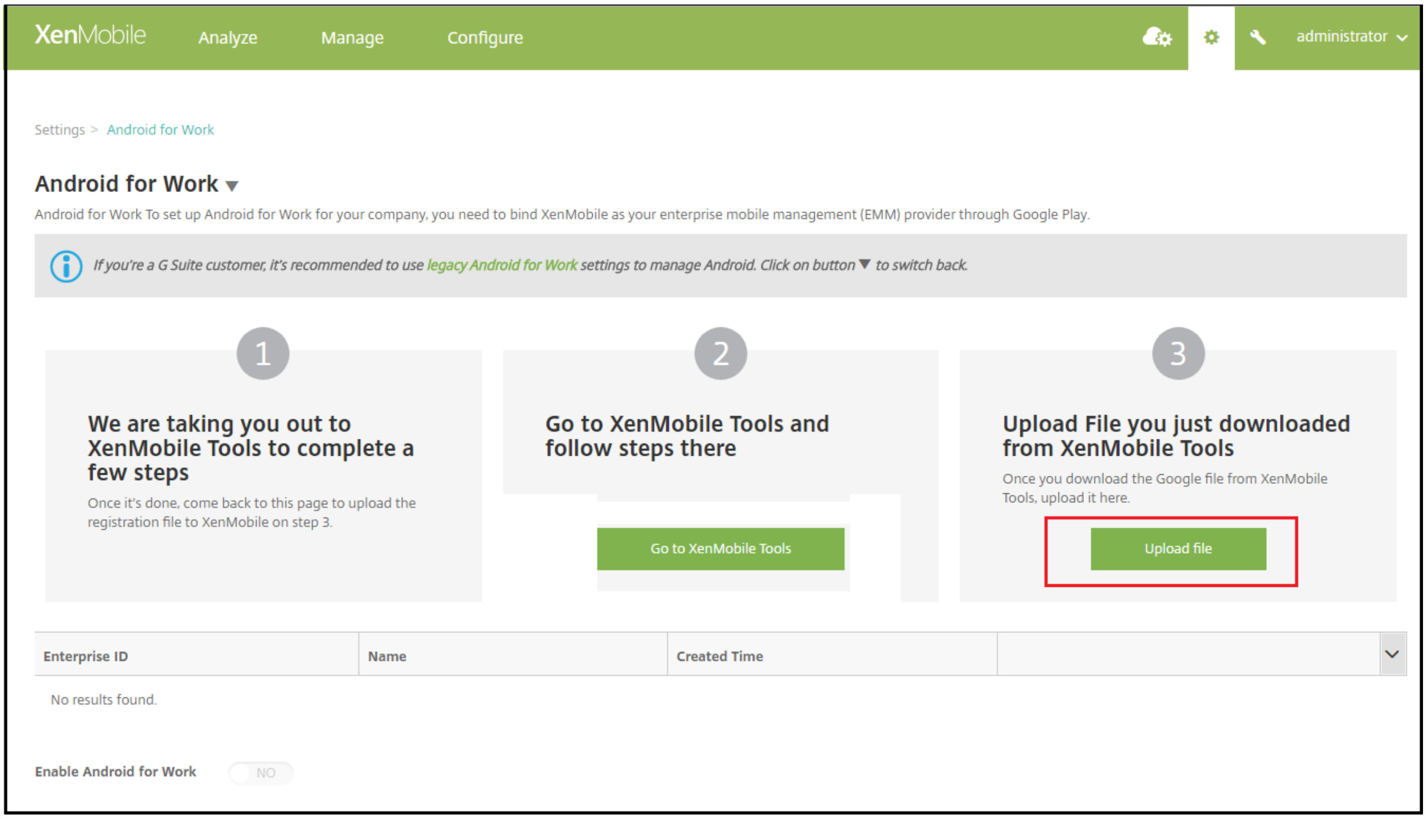
Create a password for file encryption

•••••••••••••

•••••••••••••

3 Upload the downloaded file to Android settings page in XenMobile console.

9. Click **Go back to XenMobile**.
10. In Android for Work page in XenMobile Settings, click **Upload file**.



Settings > Android for Work

Android for Work ▾

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

If you're a G Suite customer, it's recommended to use legacy Android for Work settings to manage Android. Click on button ▼ to switch back.

1 We are taking you out to XenMobile Tools to complete a few steps

Once it's done, come back to this page to upload the registration file to XenMobile on step 3.

2 Go to XenMobile Tools and follow steps there

Go to XenMobile Tools

3 Upload File you just downloaded from XenMobile Tools

Once you download the Google file from XenMobile Tools, upload it here.

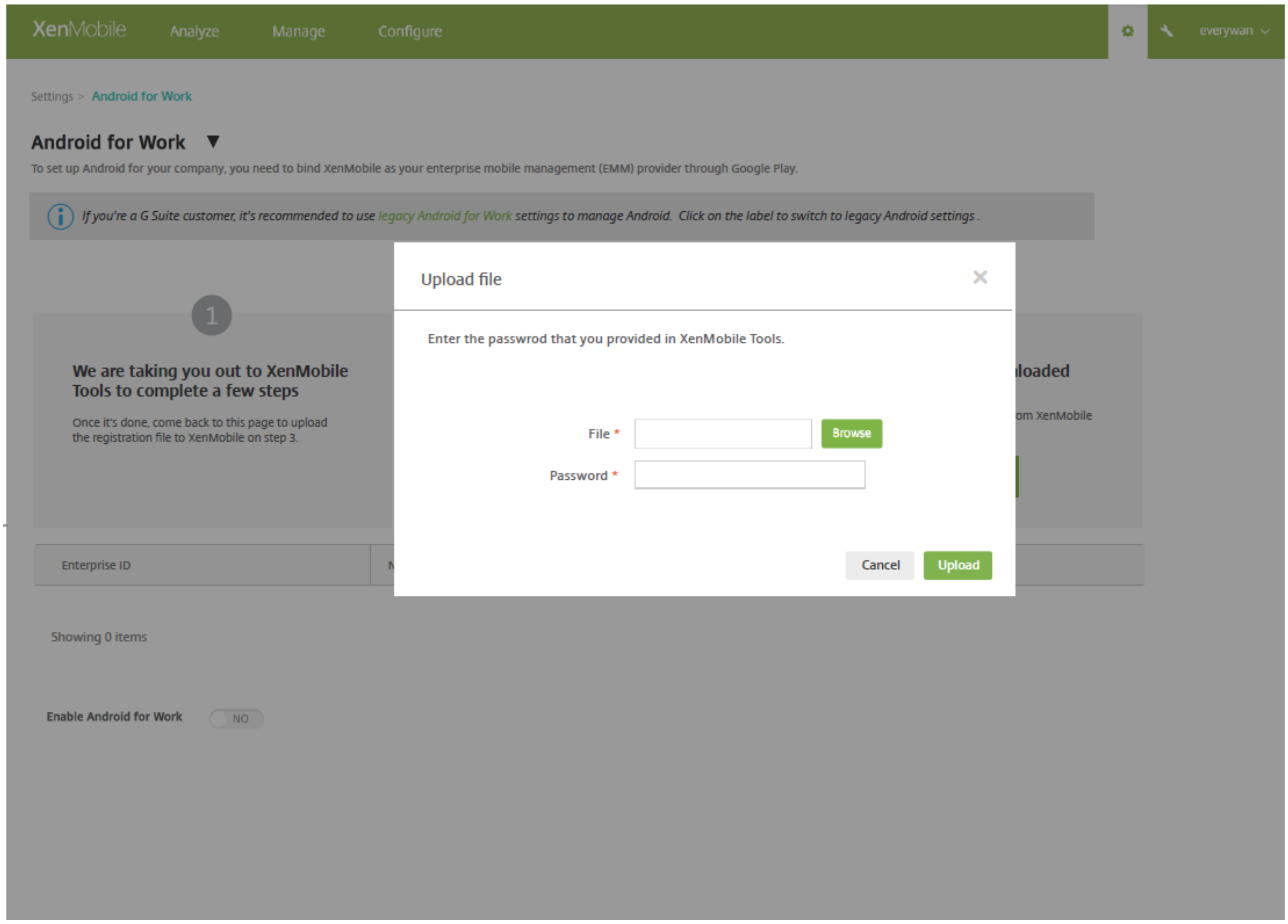
Upload file

Enterprise ID	Name	Created Time

No results found.

Enable Android for Work NO

11. Browse to the file you downloaded and enter the password you created. Click **Upload**.



Android for Work

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

If you're a G Suite customer, it's recommended to use legacy Android for Work settings to manage Android. Click on the label to switch to legacy Android settings .

1

We are taking you out to XenMobile Tools to complete a few steps

Once it's done, come back to this page to upload the registration file to XenMobile on step 3.

Upload file

Enter the passwrod that you provided in XenMobile Tools.

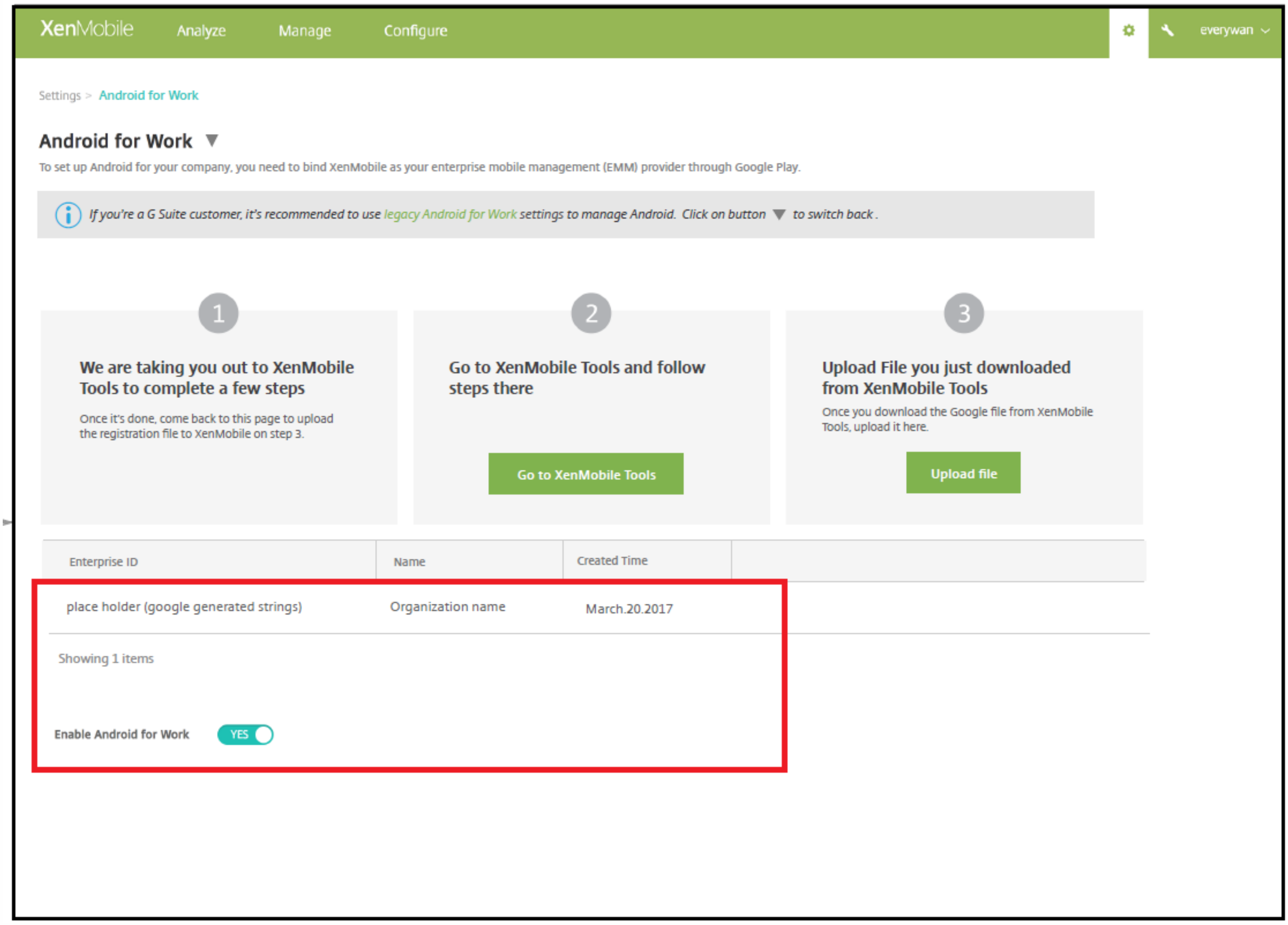
File *

Password *

Showing 0 items

Enable Android for Work NO

12. An enterprise ID has been added for Android for Work. To enable Android of Work, slide **Enable Android for Work** to **Yes**.



Android for Work ▼

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

If you're a G Suite customer, it's recommended to use legacy Android for Work settings to manage Android. Click on button ▼ to switch back .

1 We are taking you out to XenMobile Tools to complete a few steps

Once it's done, come back to this page to upload the registration file to XenMobile on step 3.

2 Go to XenMobile Tools and follow steps there

Go to XenMobile Tools

3 Upload File you just downloaded from XenMobile Tools

Once you download the Google file from XenMobile Tools, upload it here.

Upload file

Enterprise ID	Name	Created Time
place holder (google generated strings)	Organization name	March.20.2017

Showing 1 items

Enable Android for Work YES

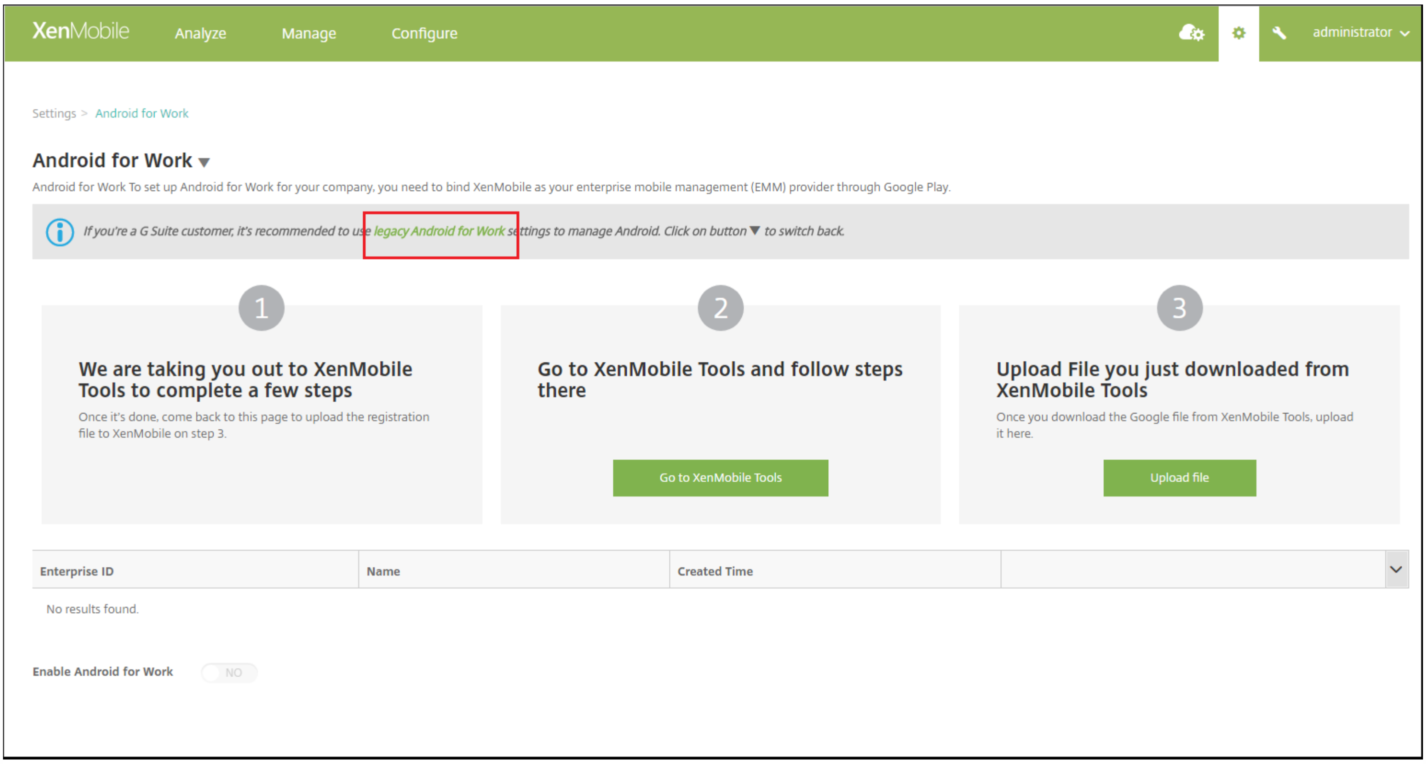
Legacy Android for Work for G Suite Customers

G Suite customers should use the legacy Android for Work settings to legacy Android for Work.

Requirements for legacy Android for Work:

- A publicly accessible domain
- A Google administrator account
- Devices that have managed profile support and that are running Android 5.0+ Lollipop
- A Google account that has Google Play installed
- A Work profile set up on the device

To start configuring legacy Android for Work, click **legacy Android for Work** in the Android for Work page in XenMobile Settings.



XenMobile Analyze Manage Configure administrator

Settings > Android for Work

Android for Work ▾

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

If you're a G Suite customer, it's recommended to use legacy Android for Work settings to manage Android. Click on button ▾ to switch back.

1 We are taking you out to XenMobile Tools to complete a few steps

Once it's done, come back to this page to upload the registration file to XenMobile on step 3.

2 Go to XenMobile Tools and follow steps there

Go to XenMobile Tools

3 Upload File you just downloaded from XenMobile Tools

Once you download the Google file from XenMobile Tools, upload it here.

Upload file

Enterprise ID	Name	Created Time	
No results found.			

Enable Android for Work NO

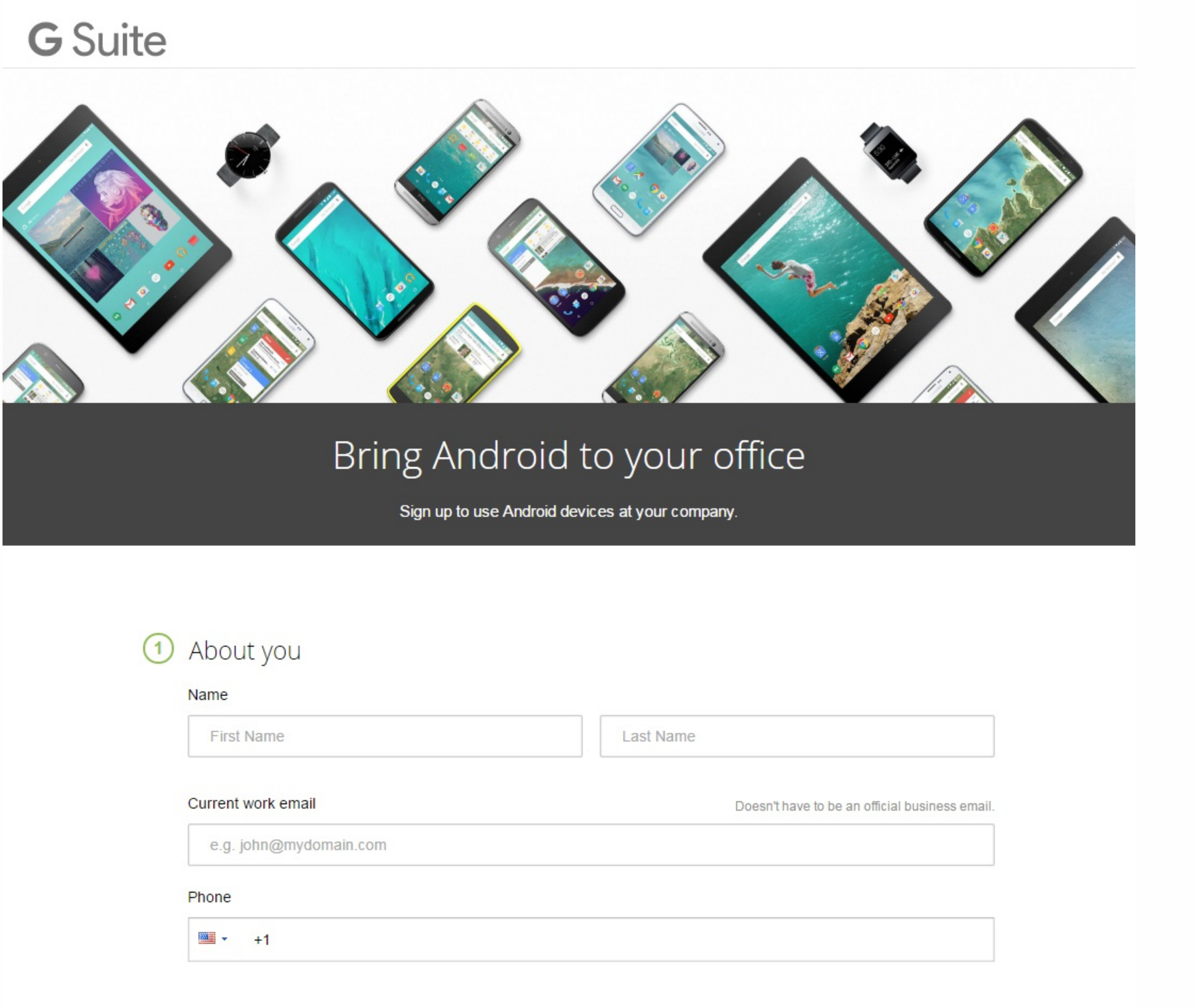
Create an Android for Work Account

Meet the following prerequisites before you can set up an Android for Work account:

If you have already verified your domain name with Google, you can skip to this step: Set up an Android for Work service account and download an Android for Work certificate.

1. Navigate to https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

The following page displays where you type your administrator and company information.



G Suite

Bring Android to your office

Sign up to use Android devices at your company.

1 About you

Name

First Name | Last Name

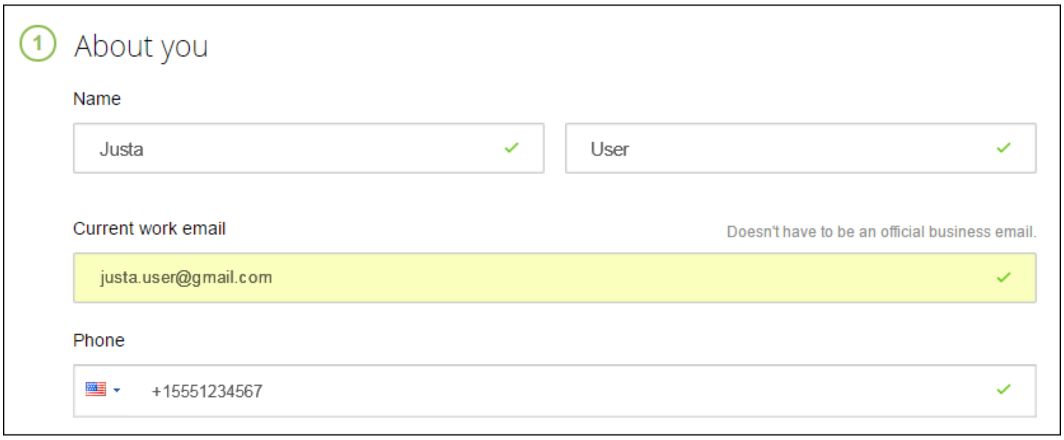
Current work email — Doesn't have to be an official business email.

e.g. john@mydomain.com

Phone

+1

2. Type your administrator user information.



1 About you

Name

Justa ✓ | User ✓

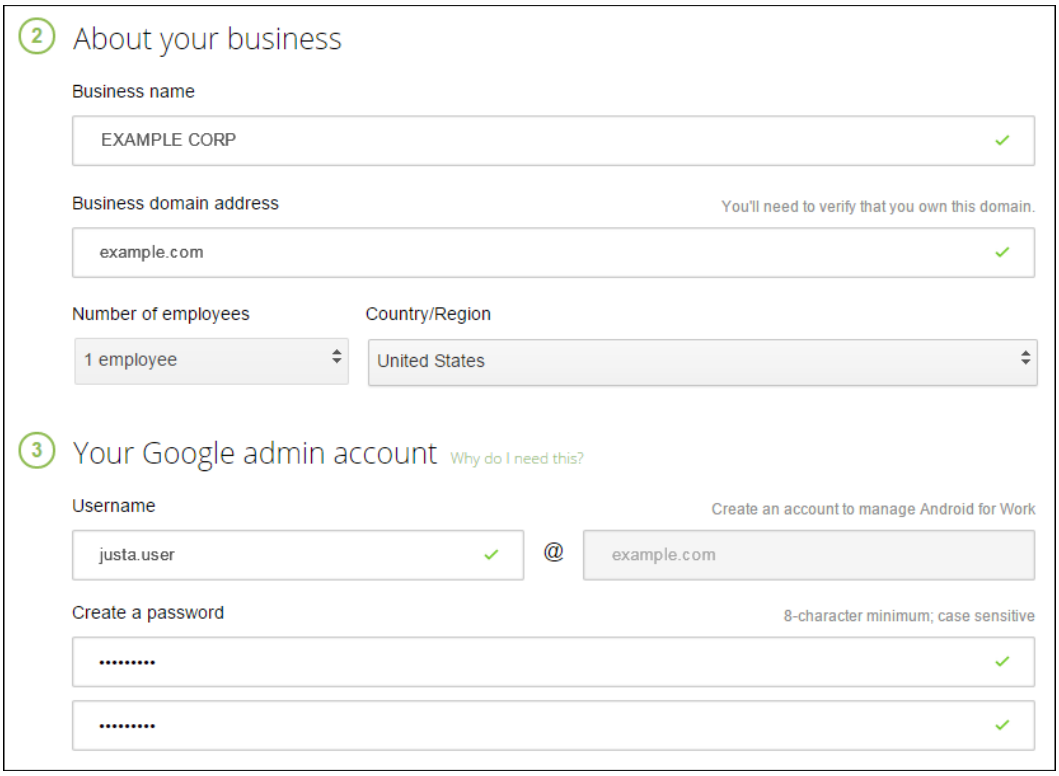
Current work email — Doesn't have to be an official business email.

justa.user@gmail.com ✓

Phone

+15551234567 ✓

2. Type your company information, in addition to your administrator account information.



2 About your business

Business name

EXAMPLE CORP ✓

Business domain address — You'll need to verify that you own this domain.

example.com ✓

Number of employees: 1 employee

Country/Region: United States

3 Your Google admin account

Username — Create an account to manage Android for Work

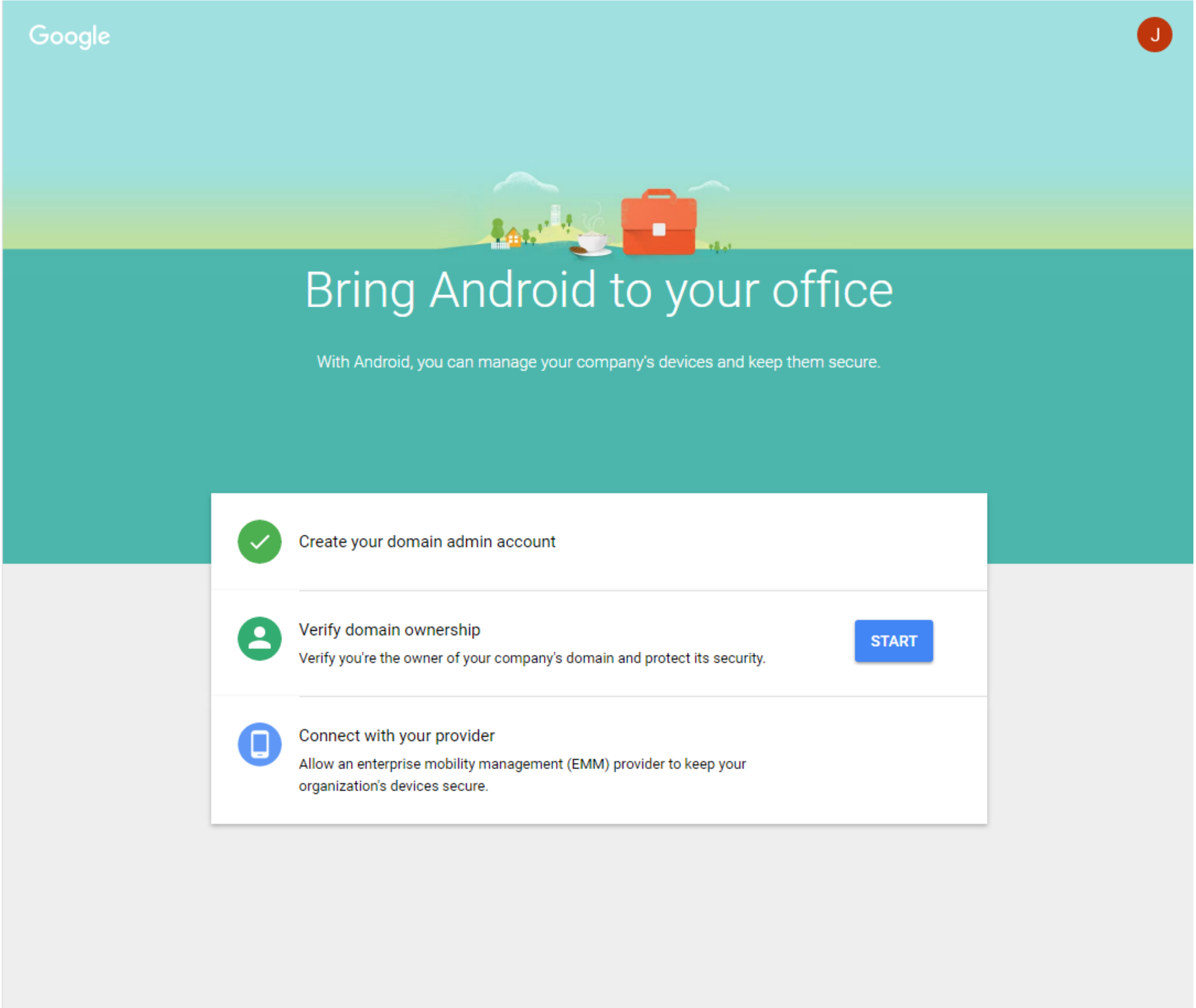
justa.user ✓ @ example.com

Create a password — 8-character minimum; case sensitive

••••••••• ✓

••••••••• ✓

The first step in the process is complete and you see the following page.



Bring Android to your office

With Android, you can manage your company's devices and keep them secure.

Create your domain admin account

Verify domain ownership
Verify you're the owner of your company's domain and protect its security.

Connect with your provider
Allow an enterprise mobility management (EMM) provider to keep your organization's devices secure.

Verify domain ownership

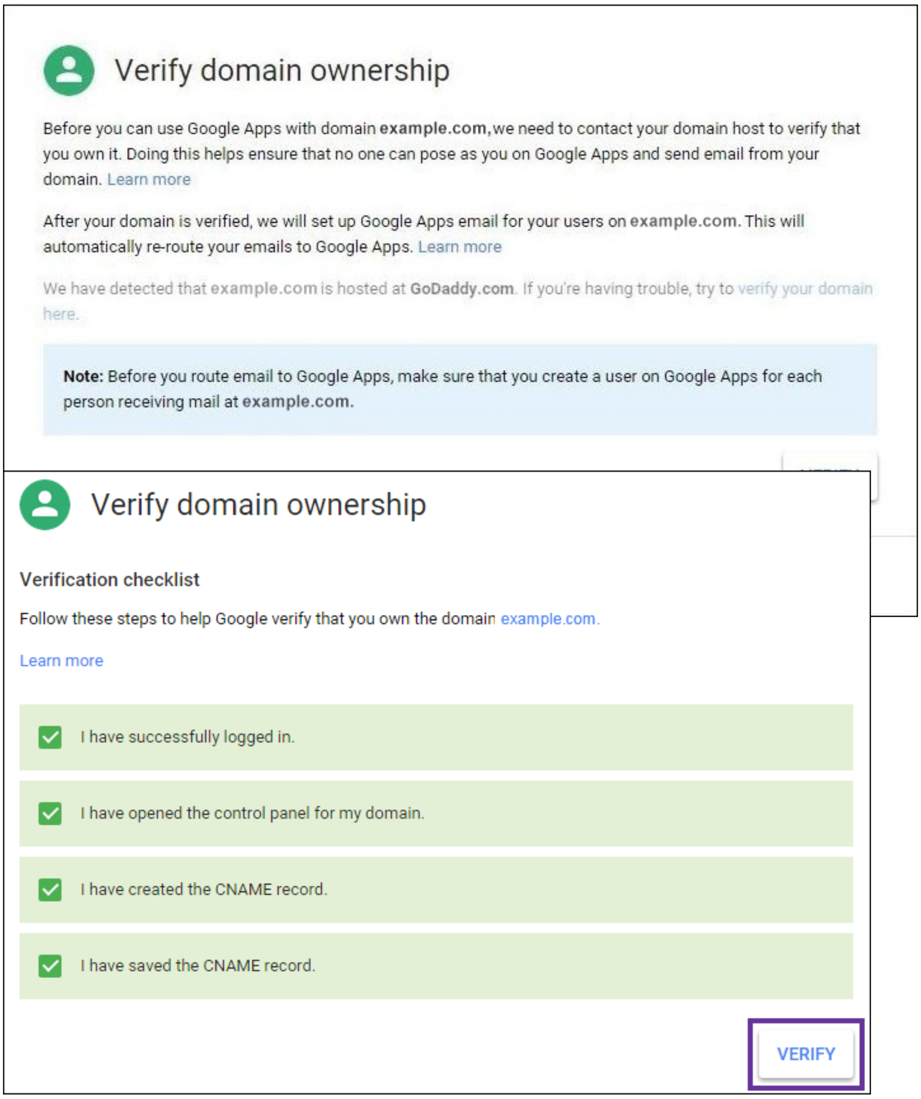
Allow Google to verify your domain in one of the following ways:

- 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/6095407/.

1. Click **Start** to begin the verification of your domain.

The **Verify domain ownership** page displays. Follow the instructions on the page to verify your domain.

2. Click **Verify**.



Verify domain ownership

Before you can use Google Apps with domain **example.com,** we need to contact your domain host to verify that you own it. Doing this helps ensure that no one can pose as you on Google Apps and send email from your domain. Learn more

After your domain is verified, we will set up Google Apps email for your users on **example.com**. This will automatically re-route your emails to Google Apps. Learn more

We have detected that **example.com** is hosted at **GoDaddy.com**. If you're having trouble, try to verify your domain here.

Note: Before you route email to Google Apps, make sure that you create a user on Google Apps for each person receiving mail at **example.com**.

Verify domain ownership

Verification checklist

Follow these steps to help Google verify that you own the domain example.com.

Learn more

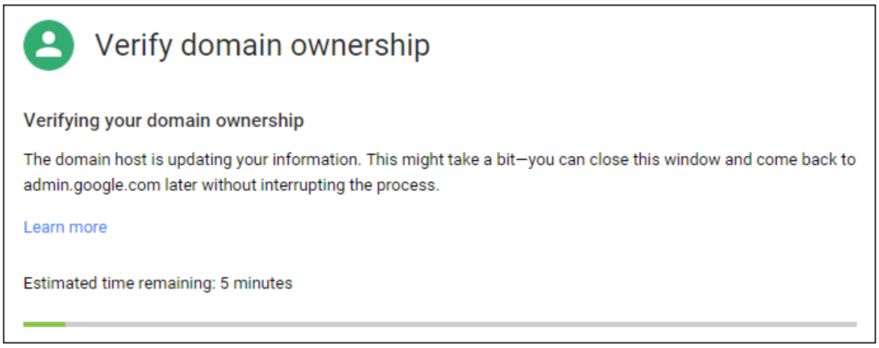
☑ I have successfully logged in.

☑ I have opened the control panel for my domain.

☑ I have created the CNAME record.

☑ I have saved the CNAME record.

3. Google verifies your domain ownership.



Verify domain ownership

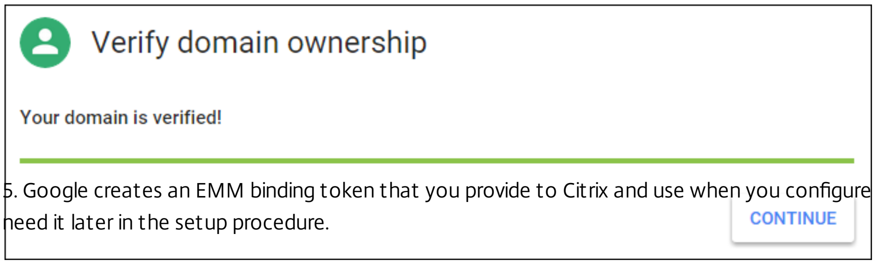
Verifying your domain ownership

The domain host is updating your information. This might take a bit—you can close this window and come back to admin.google.com later without interrupting the process.

Learn more

Estimated time remaining: 5 minutes

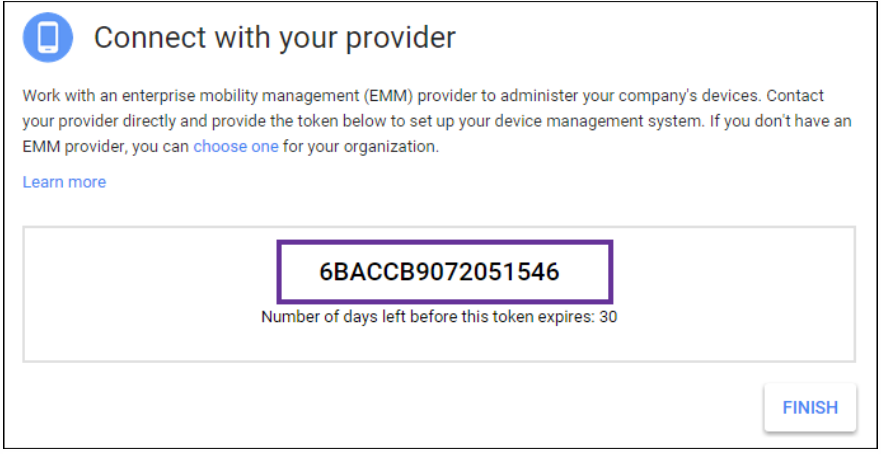
4. After successful verification, the following page displays. Click **Continue**.



Verify domain ownership

Your domain is verified!

5. Google creates an EMM binding token that you provide to Citrix and use when you configure Android for Work settings. Copy and save the token; you need it later in the setup procedure.



Connect with your provider

Work with an enterprise mobility management (EMM) provider to administer your company's devices. Contact your provider directly and provide the token below to set up your device management system. If you don't have an EMM provider, you can choose one for your organization.

Learn more

6BACCB9072051546

Number of days left before this token expires: 30

6. Click **Finish** to complete setting up Android for Work. A page appears, indicating that you've successfully verified your domain.

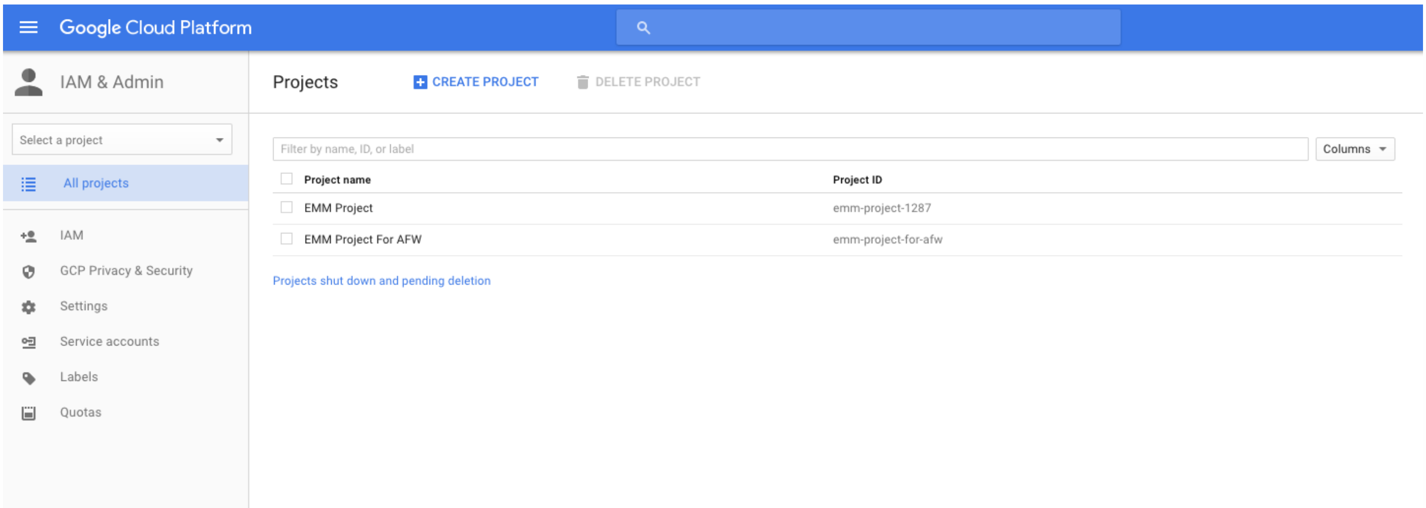
After you create an Android for Work service account, you can sign in to the Google Admin console to manage your mobility management settings.

Set up an Android for Work service account and download an Android for Work certificate

To allow XenMobile 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 XenMobile and Google services for Android. For more information about the authentication protocol being used, go to https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

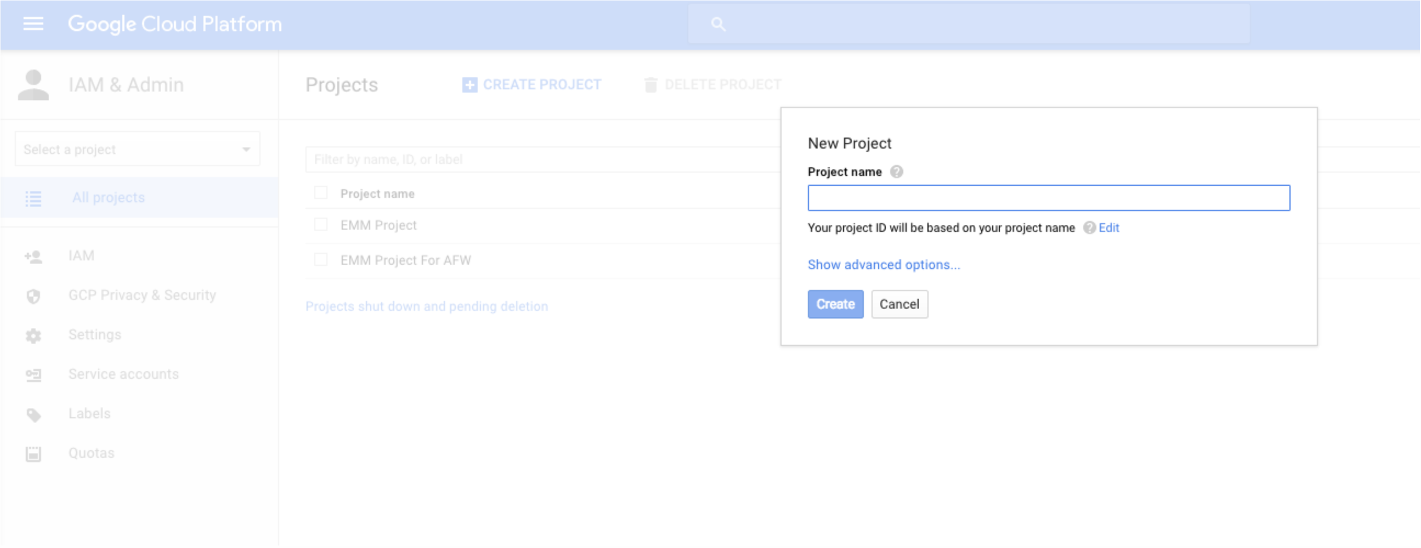
1. In a web browser, go to https://console.cloud.google.com/project and sign in with your Google administrator credentials

2. In the **Projects** list, click **Create Project.**



□ Project name	Project ID
□ EMM Project	emm-project-1287
□ EMM Project For AFW	emm-project-for-afw

3. In **Project name**, type a name for the project.



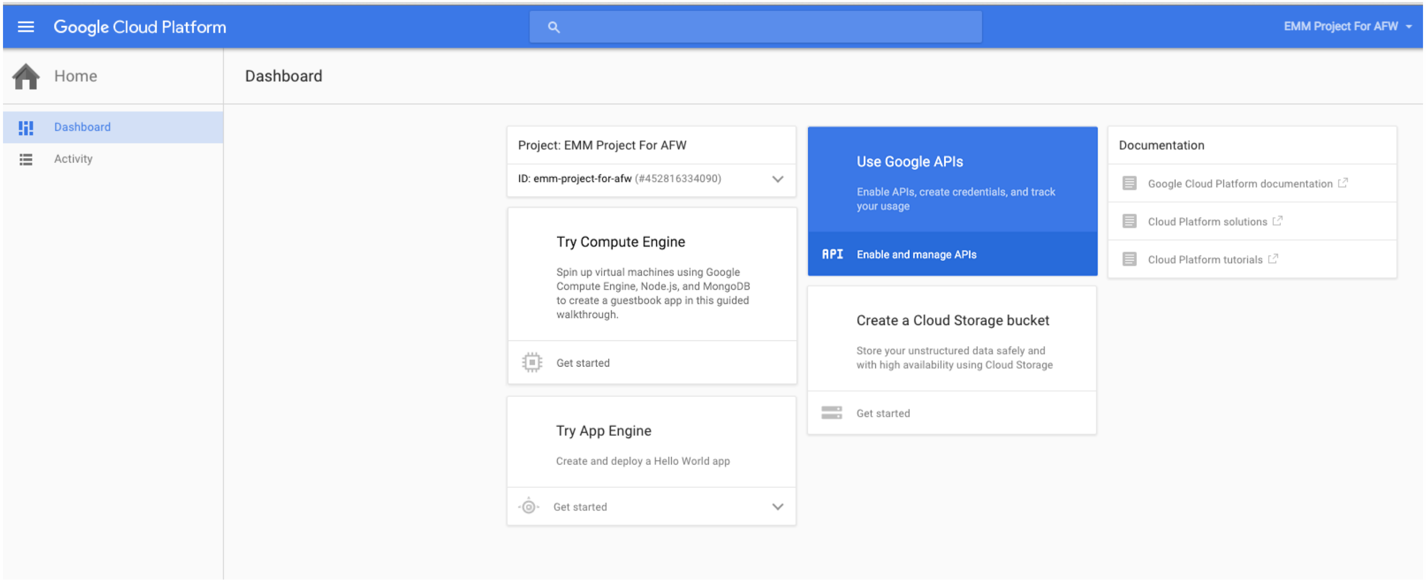
New Project

Project name

Your project ID will be based on your project name Edit

Show advanced options...

4. On the Dashboard, click **Use Google APIs**.



Project: EMM Project For AFW

ID: emm-project-for-afw (#452816334090)

Try Compute Engine

Spin up virtual machines using Google Compute Engine, Node.js, and MongoDB to create a guestbook app in this guided walkthrough.

Get started

Try App Engine

Create and deploy a Hello World app

Get started

Use Google APIs

Enable APIs, create credentials, and track your usage

API Enable and manage APIs

Create a Cloud Storage bucket

Store your unstructured data safely and with high availability using Cloud Storage

Get started

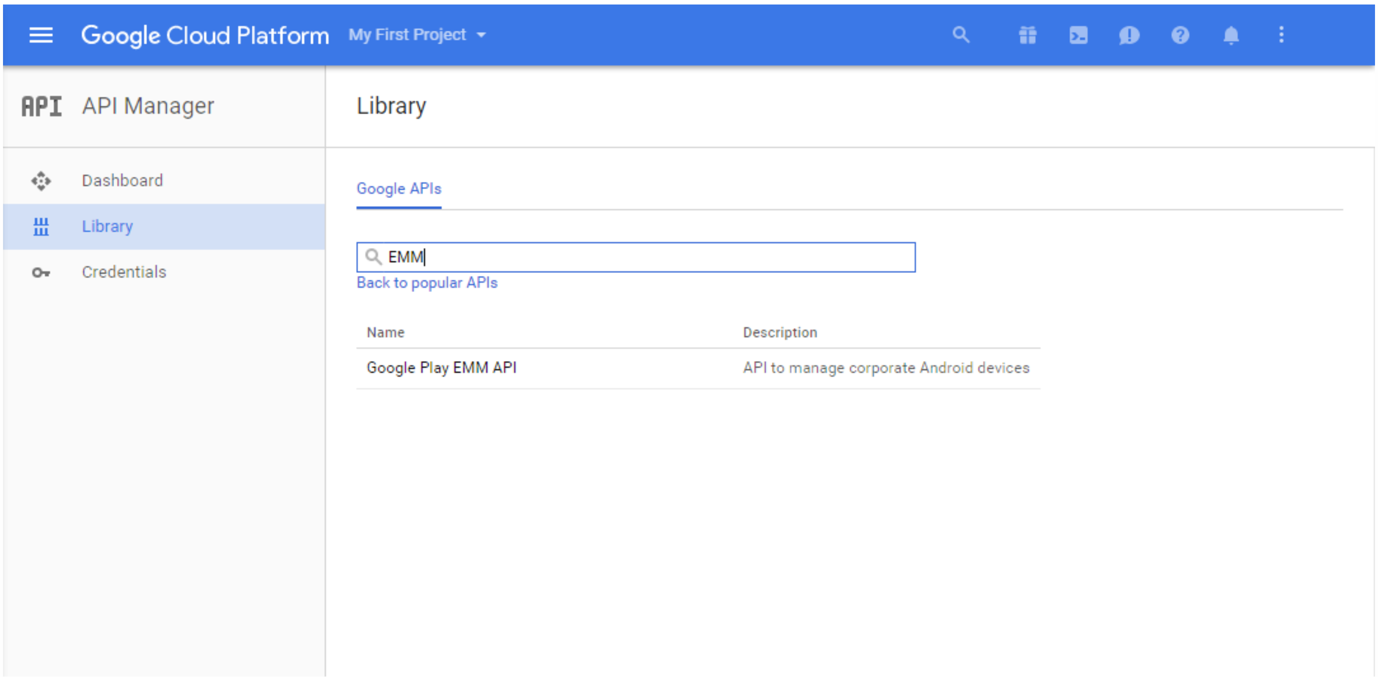
Documentation

Google Cloud Platform documentation

Cloud Platform solutions

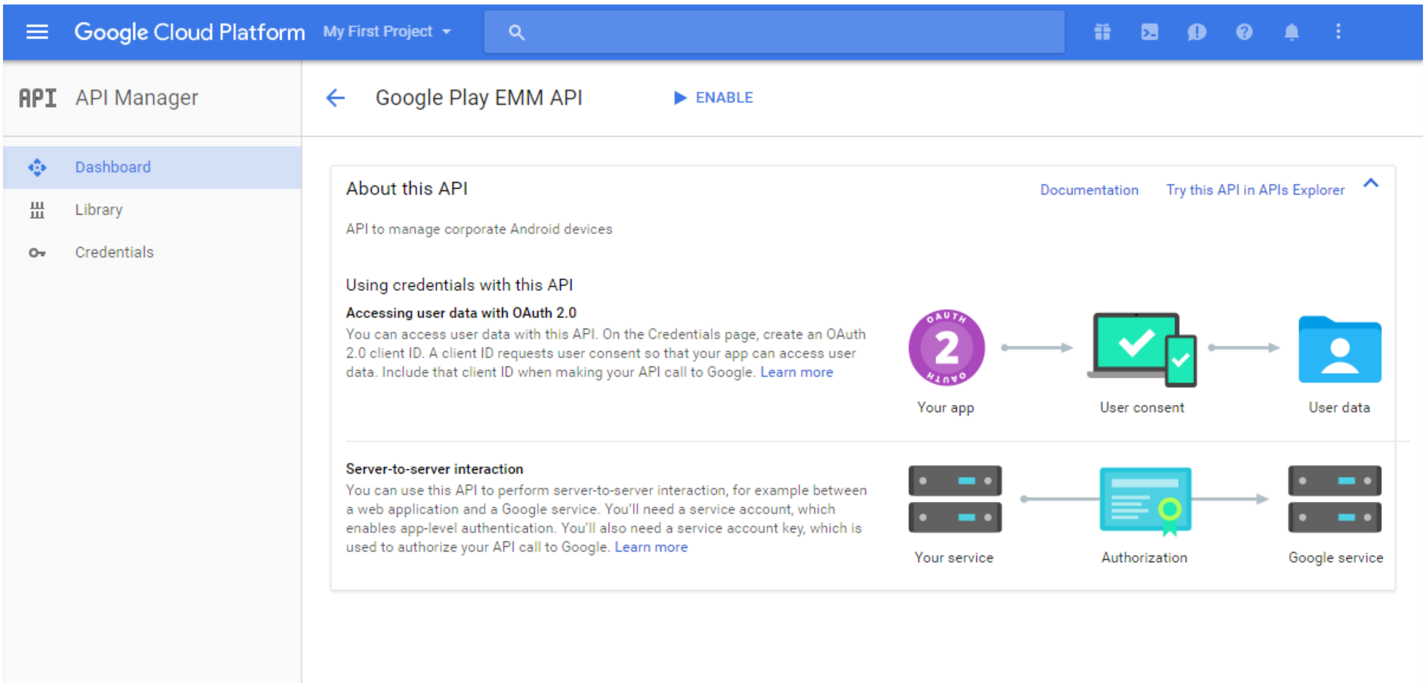
Cloud Platform tutorials

5. Click **Library**, in **Search**, type **EMM** and then click the search result.



Name	Description
Google Play EMM API	API to manage corporate Android devices

6. On the **Overview** page, click **Enable**.



About this API

API to manage corporate Android devices

Using credentials with this API

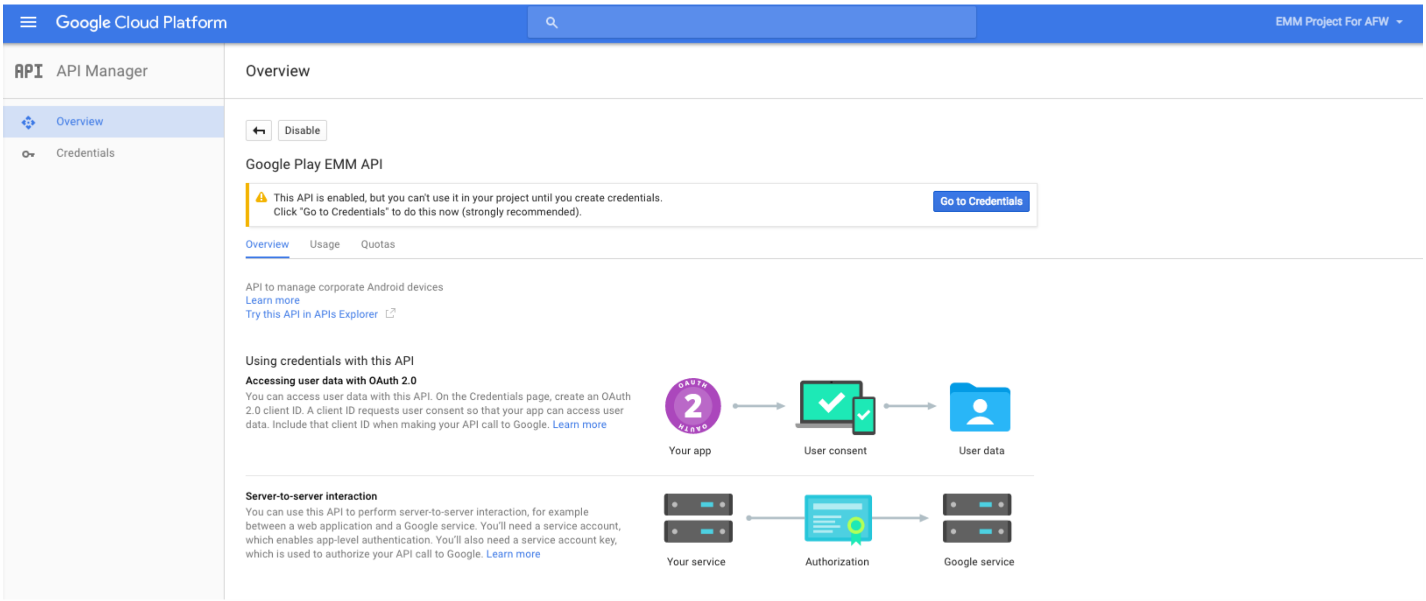
Accessing user data with OAuth 2.0

You can access user data with this API. On the Credentials page, create an OAuth 2.0 client ID. A client ID requests user consent so that your app can access user data. Include that client ID when making your API call to Google. Learn more

Server-to-server interaction

You can use this API to perform server-to-server interaction, for example between a web application and a Google service. You'll need a service account, which enables app-level authentication. You'll also need a service account key, which is used to authorize your API call to Google. Learn more

7. Next to **Google Play EMM API**, click **Go to Credentials**.



Google Cloud Platform

EMM Project For AFW

API API Manager

Overview

Credentials

Overview

Disable

Google Play EMM API

This API is enabled, but you can't use it in your project until you create credentials.
Click "Go to Credentials" to do this now (strongly recommended).

Go to Credentials

Overview Usage Quotas

API to manage corporate Android devices
Learn more
Try this API in APIs Explorer

Using credentials with this API

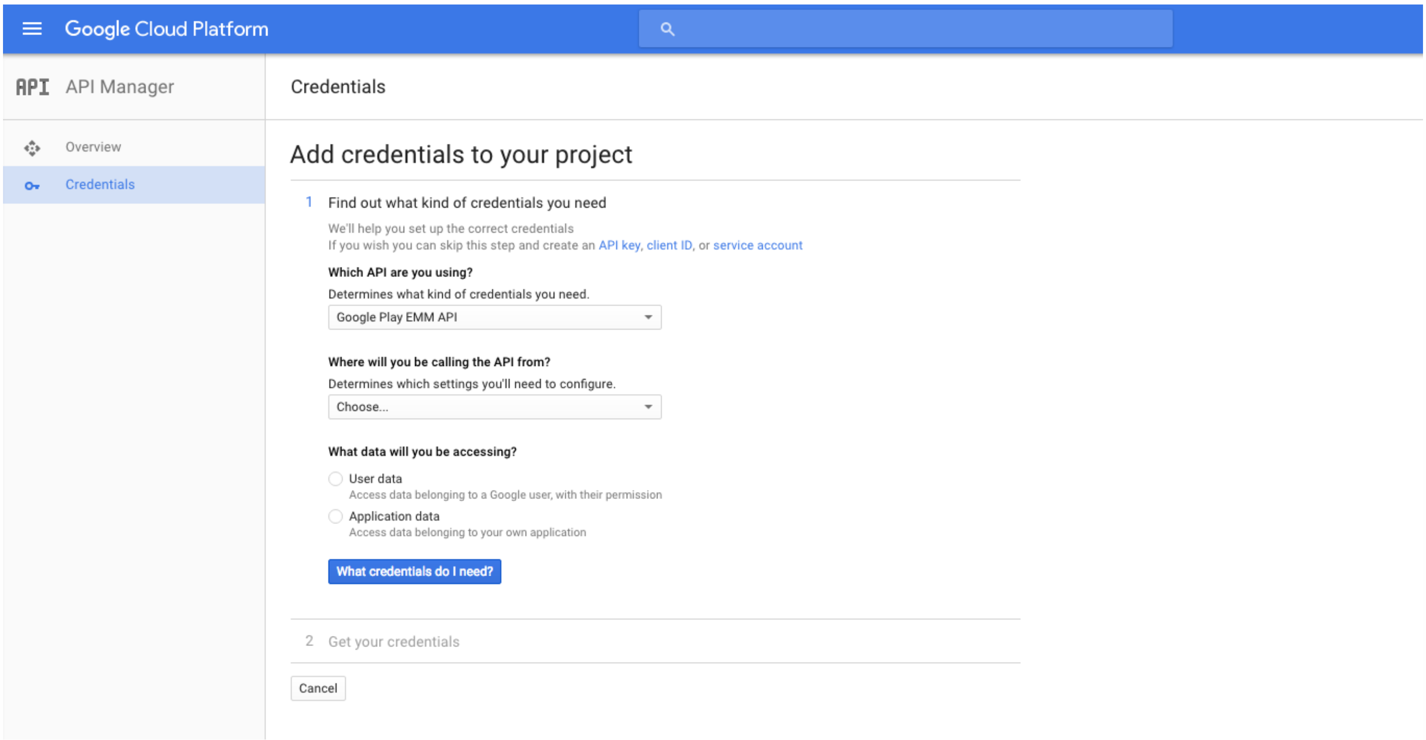
Accessing user data with OAuth 2.0

You can access user data with this API. On the Credentials page, create an OAuth 2.0 client ID. A client ID requests user consent so that your app can access user data. Include that client ID when making your API call to Google. Learn more

Server-to-server interaction

You can use this API to perform server-to-server interaction, for example between a web application and a Google service. You'll need a service account, which enables app-level authentication. You'll also need a service account key, which is used to authorize your API call to Google. Learn more

8. In the **Add credentials to our project** list, in step 1, click **service account**.



Google Cloud Platform

API API Manager

Overview

Credentials

Credentials

Add credentials to your project

1 Find out what kind of credentials you need

We'll help you set up the correct credentials
If you wish you can skip this step and create an API key, client ID, or service account

Which API are you using?

Determines what kind of credentials you need.

Google Play EMM API

Where will you be calling the API from?

Determines which settings you'll need to configure.

Choose...

What data will you be accessing?

○ User data
Access data belonging to a Google user, with their permission

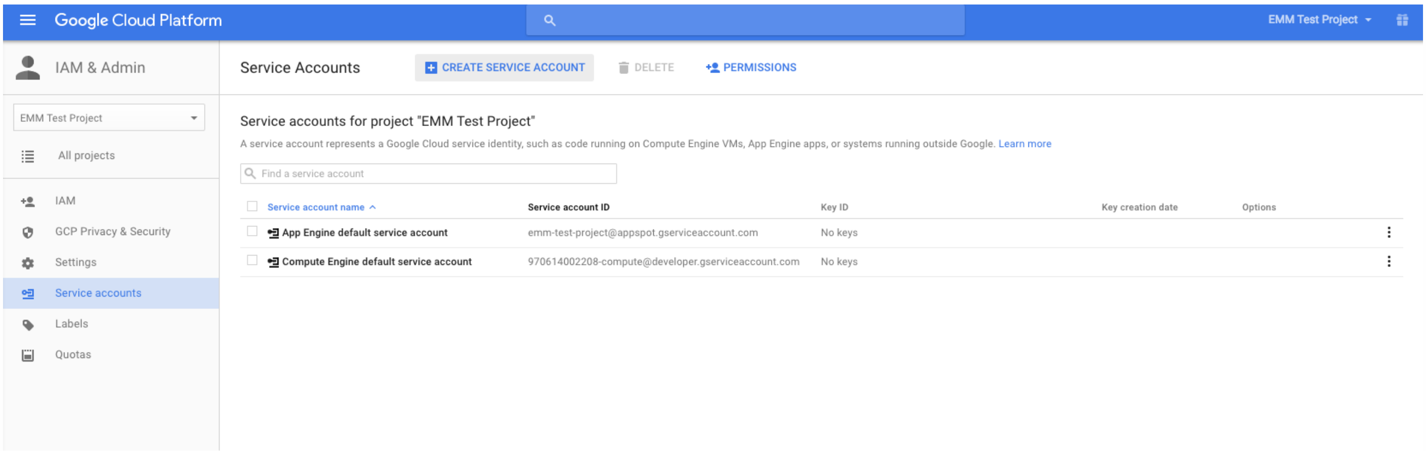
○ Application data
Access data belonging to your own application

What credentials do I need?

2 Get your credentials

Cancel

9. On the **Service Accounts** page, click **Create Service Account**.

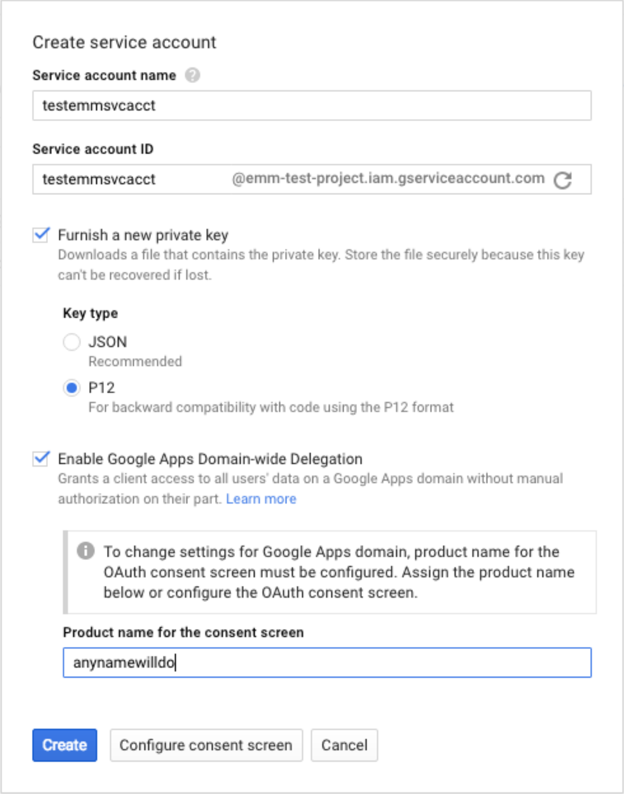


Service accounts for project "EMM Test Project"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more

Service account name	Service account ID	Key ID	Key creation date	Options
App Engine default service account	emm-test-project@appspot.gserviceaccount.com	No keys		⋮
Compute Engine default service account	970614002208-compute@developer.gserviceaccount.com	No keys		⋮

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.**



Create service account

Service account name

testemmsvcacct

Service account ID

testemmsvcacct @emm-test-project.iam.gserviceaccount.com

☑ Furnish a new private key
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

○ JSON
Recommended

● P12
For backward compatibility with code using the P12 format

☑ Enable Google Apps Domain-wide Delegation
Grants a client access to all users' data on a Google Apps domain without manual authorization on their part. Learn more

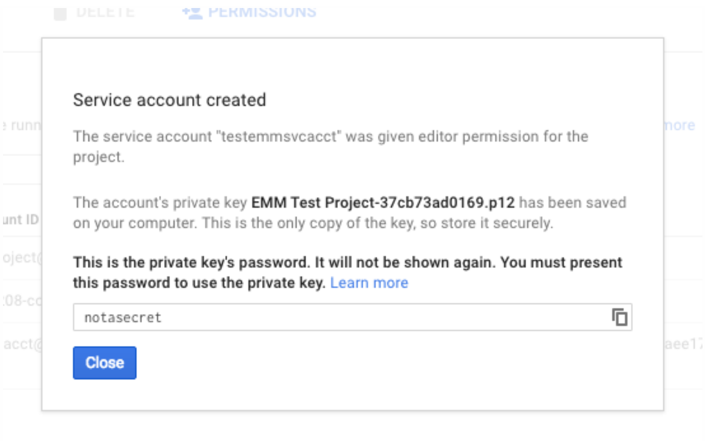
To change settings for Google Apps domain, product name for the OAuth consent screen must be configured. Assign the product name below or configure the OAuth consent screen.

Product name for the consent screen

anynamewilldo

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**.



Service account created

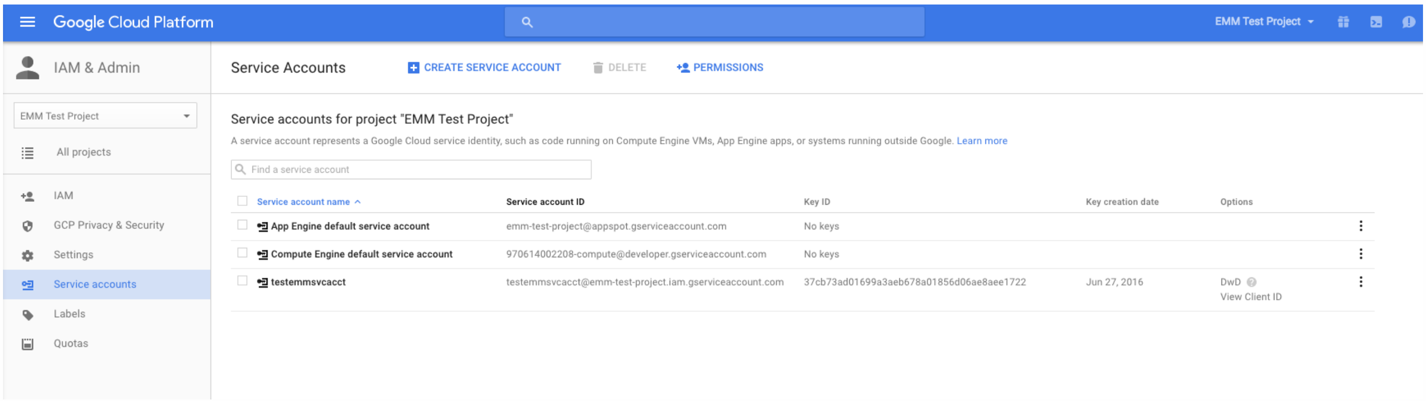
The service account "testemmsvcacct" was given editor permission for the project.

The account's private key **EMM Test Project-37cb73ad0169.p12** has been saved on your computer. This is the only copy of the key, so store it securely.

This is the private key's password. It will not be shown again. You must present this password to use the private key. Learn more

```
notasecret
```

12. In **Permissions**, click **Service accounts** and then under **Options** for your service account, click **View Client ID**.



Service Accounts

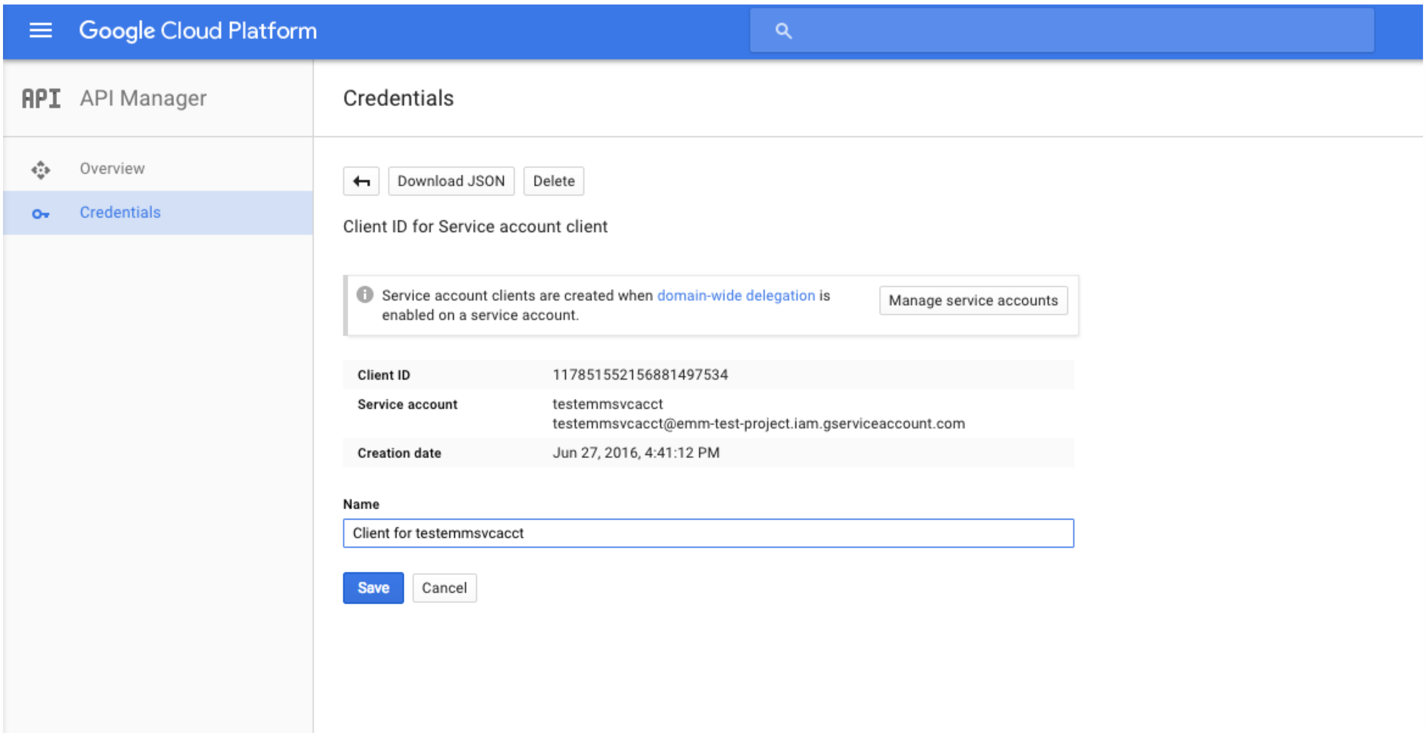
Service accounts for project "EMM Test Project"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more

Find a service account

□ Service account name	Service account ID	Key ID	Key creation date	Options
□ App Engine default service account	emm-test-project@appspot.gserviceaccount.com	No keys		
□ Compute Engine default service account	970614002208-compute@developer.gserviceaccount.com	No keys		
□ testemmsvcacct	testemmsvcacct@emm-test-project.iam.gserviceaccount.com	37cb73ad01699a3aeb678a01856d06ae8aee1722	Jun 27, 2016	DwD 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.



Credentials

Client ID for Service account client

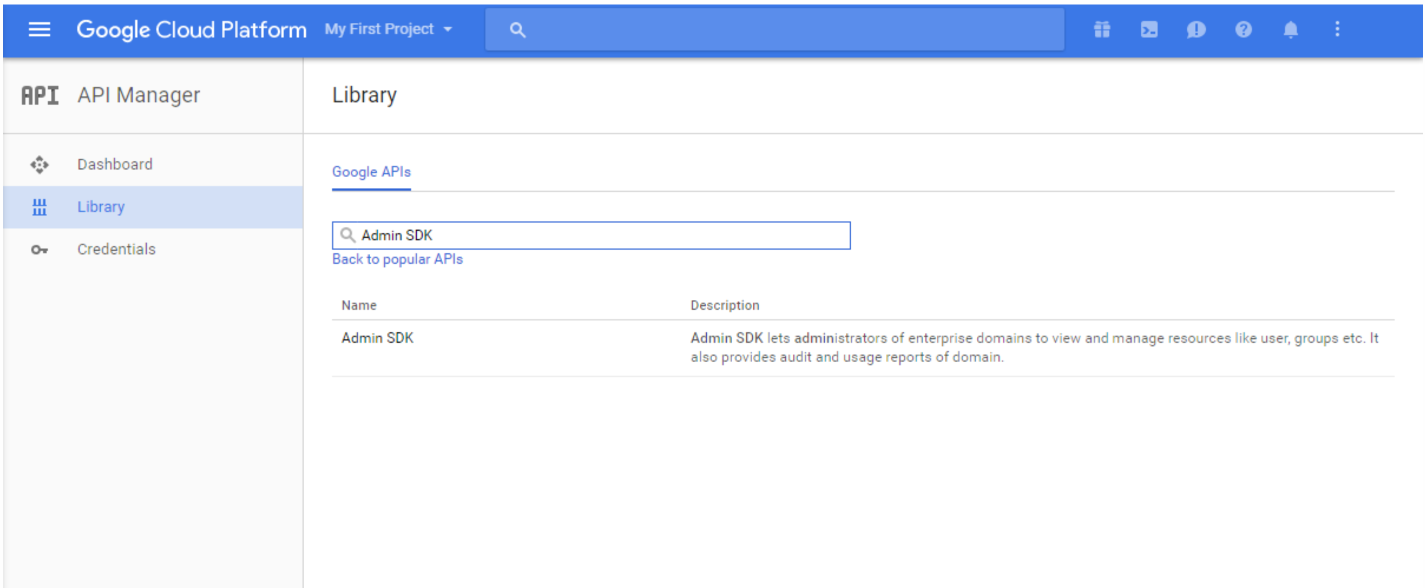
Service account clients are created when domain-wide delegation is enabled on a service account.

Client ID	117851552156881497534
Service account	testemmsvcacct testemmsvcacct@emm-test-project.iam.gserviceaccount.com
Creation date	Jun 27, 2016, 4:41:12 PM

Name

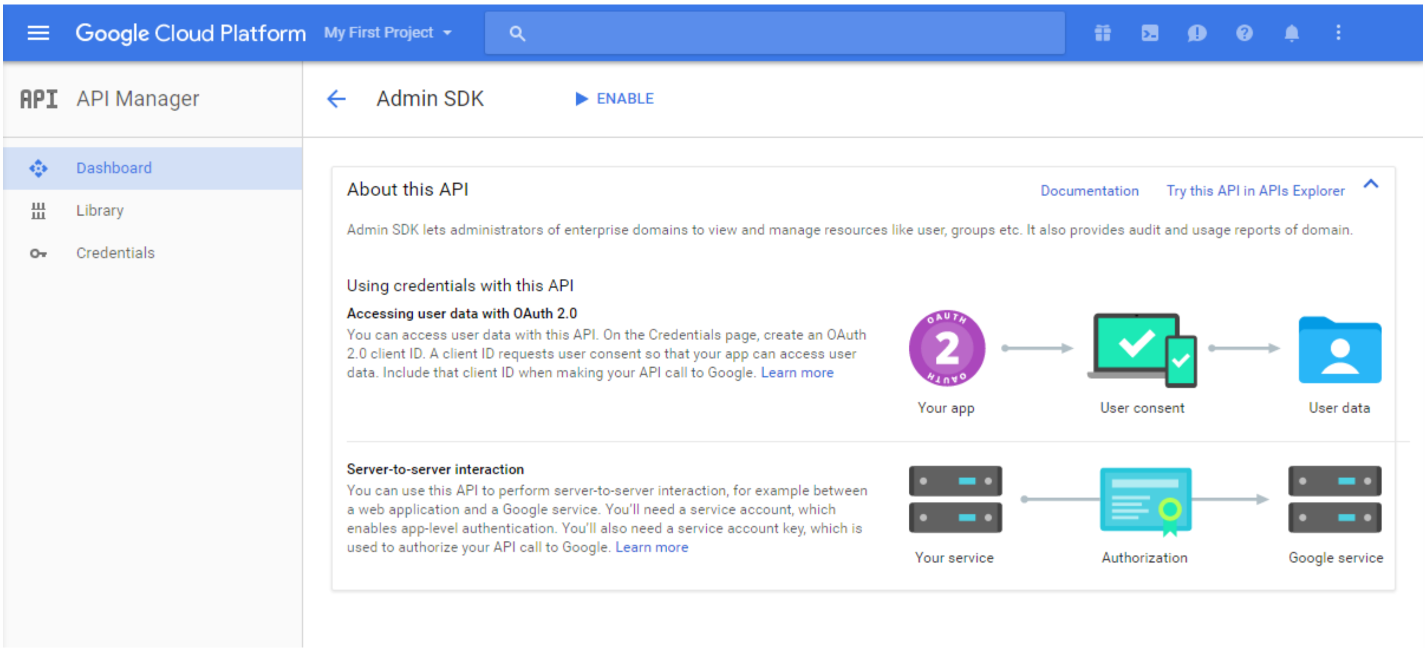
Client for testemmsvcacct

14. On the **Library** page, search for **Admin SDK** and then click the search result.



Name	Description
Admin SDK	Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.

15. On the **Overview** page, click **Enable**.



About this API

Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.

Using credentials with this API

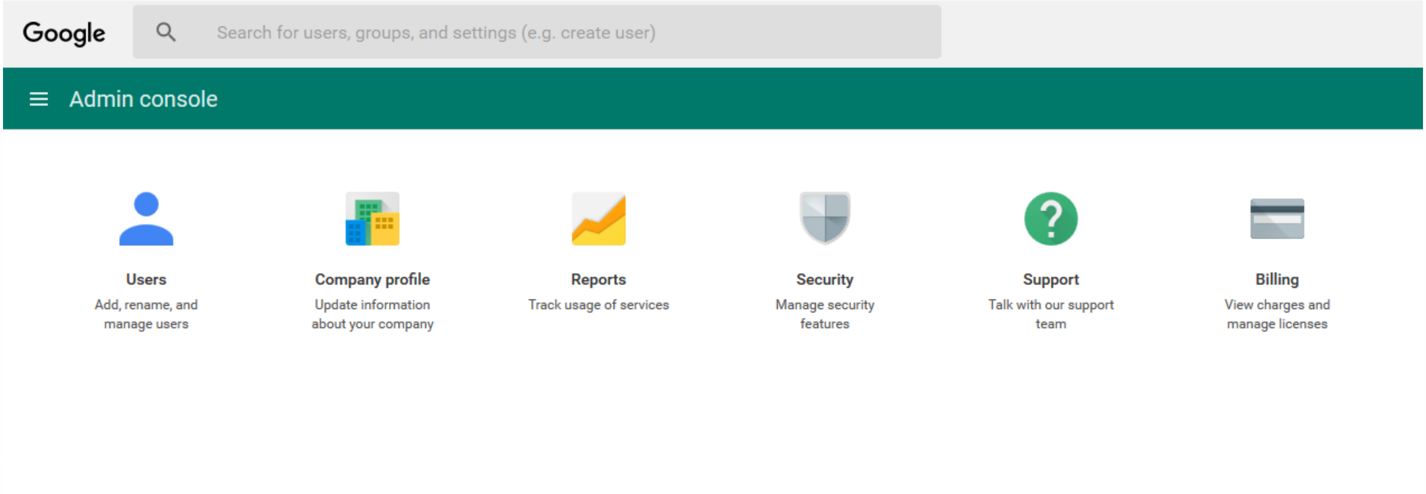
Accessing user data with OAuth 2.0

You can access user data with this API. On the Credentials page, create an OAuth 2.0 client ID. A client ID requests user consent so that your app can access user data. Include that client ID when making your API call to Google. Learn more

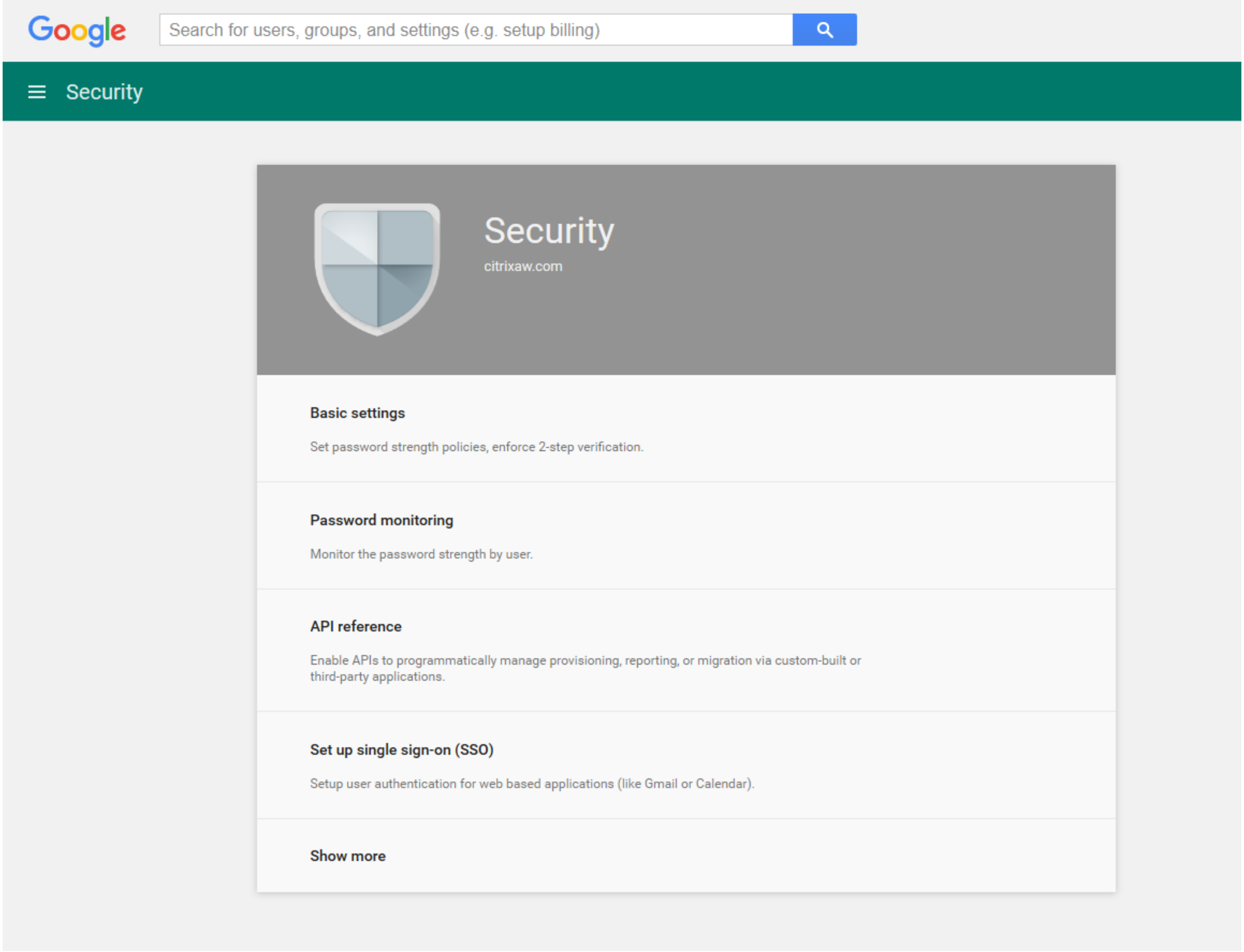
Server-to-server interaction

You can use this API to perform server-to-server interaction, for example between a web application and a Google service. You'll need a service account, which enables app-level authentication. You'll also need a service account key, which is used to authorize your API call to Google. Learn more

16. Open the Google admin console for your domain and then click **Security**.


Google
Search for users, groups, and settings (e.g. create user)
Admin console
Users
Add, rename, and manage users
Company profile
Update information about your company
Reports
Track usage of services
Security
Manage security features
Support
Talk with our support team
Billing
View charges and manage licenses

17. On the **Settings** page, click **Show more** and then click **Advanced settings**.



Basic settings

Set password strength policies, enforce 2-step verification.

Password monitoring

Monitor the password strength by user.

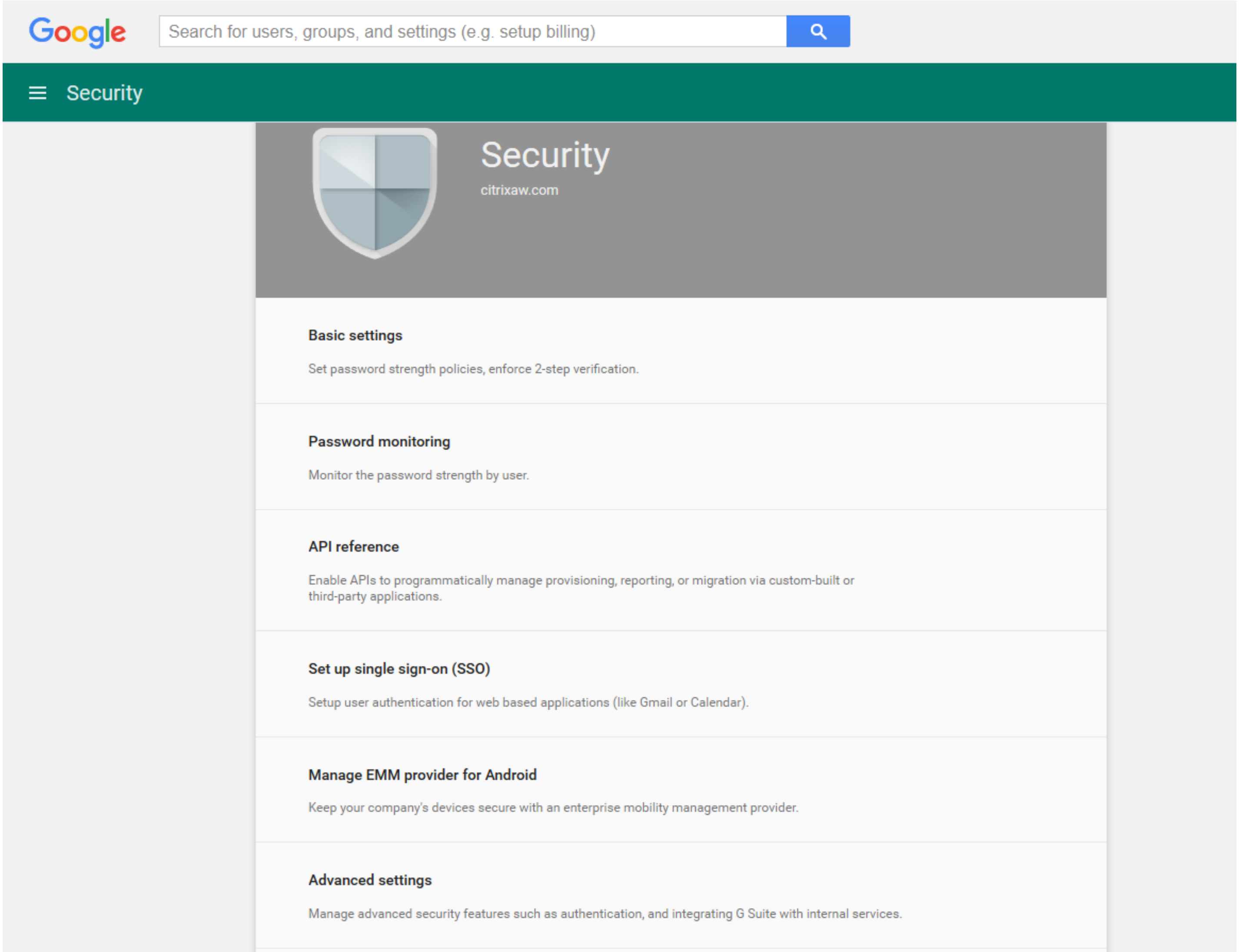
API reference

Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

Show more



Security

citrixaw.com

Basic settings

Set password strength policies, enforce 2-step verification.

Password monitoring

Monitor the password strength by user.

API reference

Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

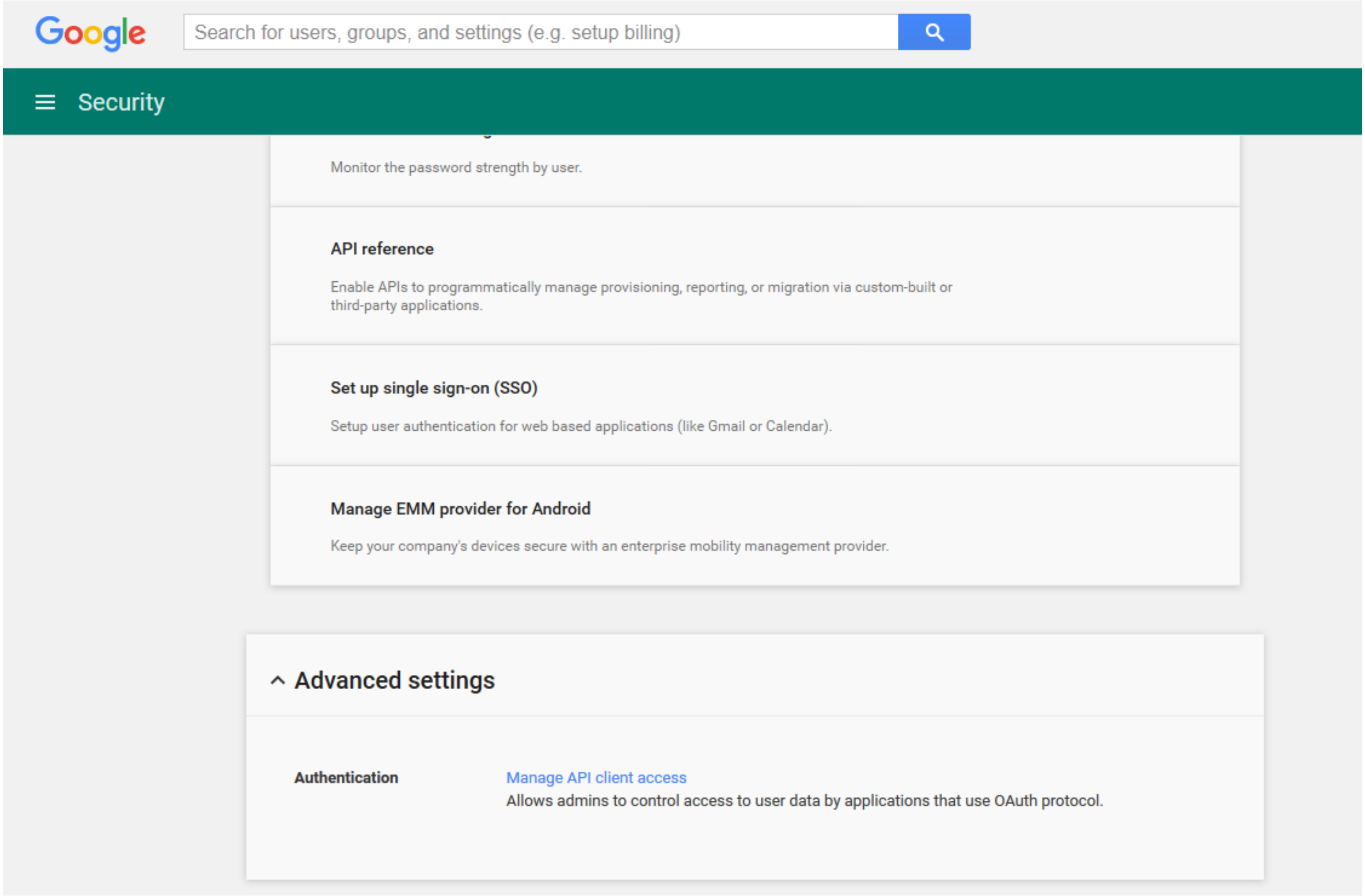
Manage EMM provider for Android

Keep your company's devices secure with an enterprise mobility management provider.

Advanced settings

Manage advanced security features such as authentication, and integrating G Suite with internal services.

18. Click **Manage API client access**.



Monitor the password strength by user.

API reference

Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

Manage EMM provider for Android

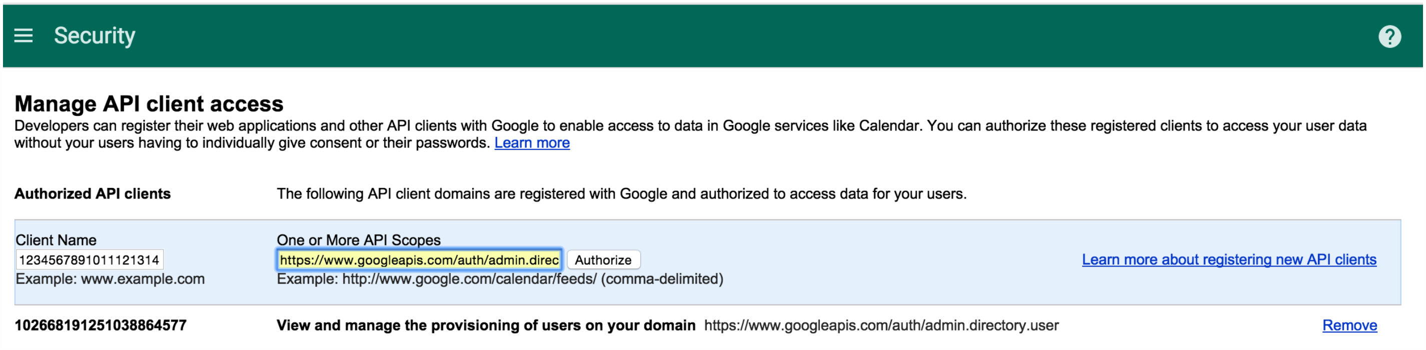
Keep your company's devices secure with an enterprise mobility management provider.

Advanced settings

Authentication — Manage API client access

Allows admins to control access to user data by applications that use OAuth protocol.

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**.



Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. Learn more

Authorized API clients The following API client domains are registered with Google and authorized to access data for your users.

Client Name: 1234567891011121314
Example: www.example.com

One or More API Scopes: https://www.googleapis.com/auth/admin.direc
Example: http://www.google.com/calendar/feeds/ (comma-delimited)

102668191251038864577	**View and manage the provisioning of users on your domain** https://www.googleapis.com/auth/admin.directory.user	Remove

Binding to EMM

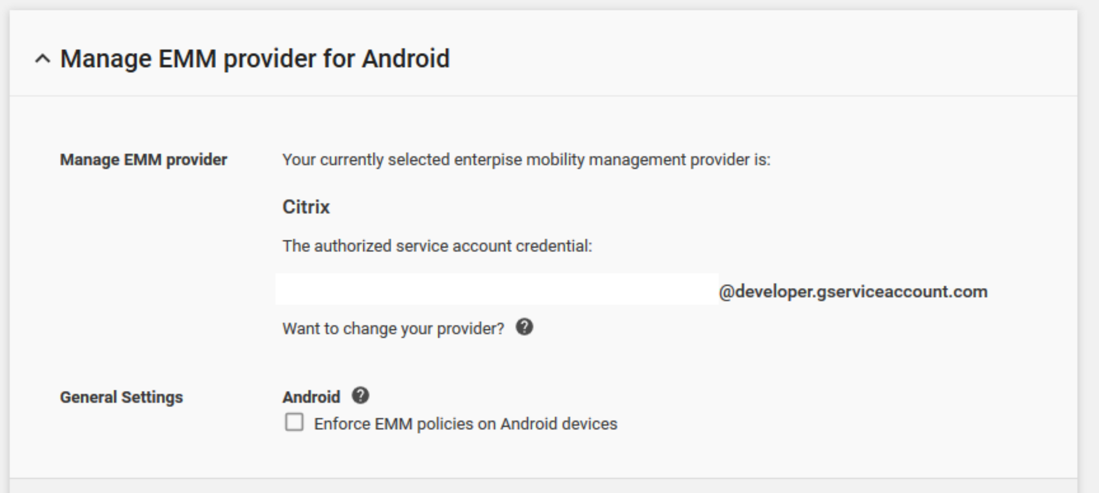
Before you can use XenMobile to manage your Android devices, you must contact Citrix Technical Support and provide your domain name, service account, and binding token. Citrix binds the token to XenMobile as your enterprise mobility management (EMM) provider. For contact information for Citrix Technical 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 for Work account is bound to Citrix as your EMM provider.

After you confirm the token binding, you can start using the XenMobile console to manage your Android devices. Import the P12 certificate you generated in step 14. Set up Android for Work server settings, enable SAML-based single-sign-on (SSO), and define at least one Android for Work device policy.



^ Manage EMM provider for Android

Manage EMM provider Your currently selected enterprise mobility management provider is:

Citrix

The authorized service account credential:

@developer.gserviceaccount.com

Want to change your provider?

General Settings Android

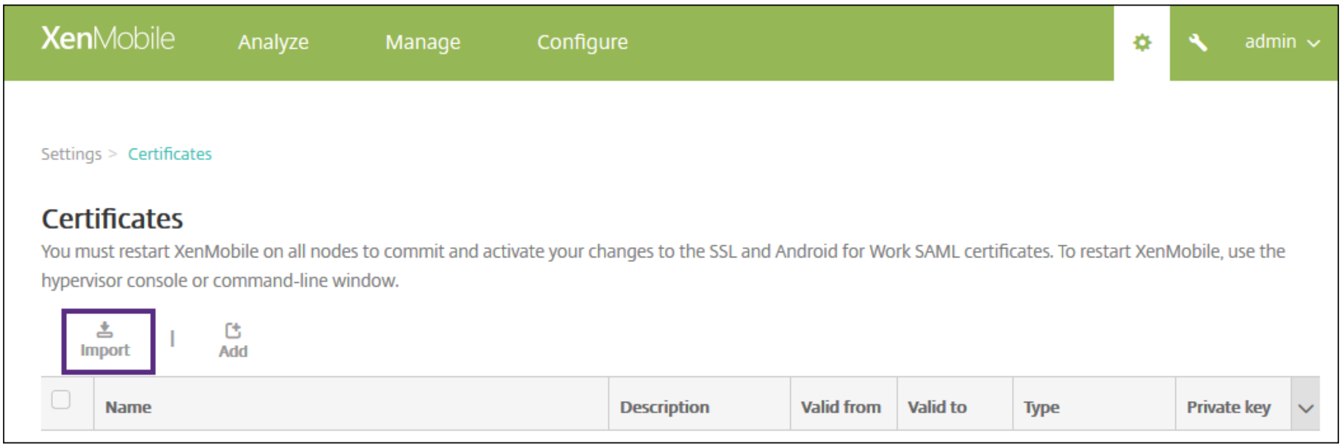
□ Enforce EMM policies on Android devices

Import the P12 certificate

Follow these steps to import your Android for Work P12 certificate:

1. Sign in to the XenMobile 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 displays.



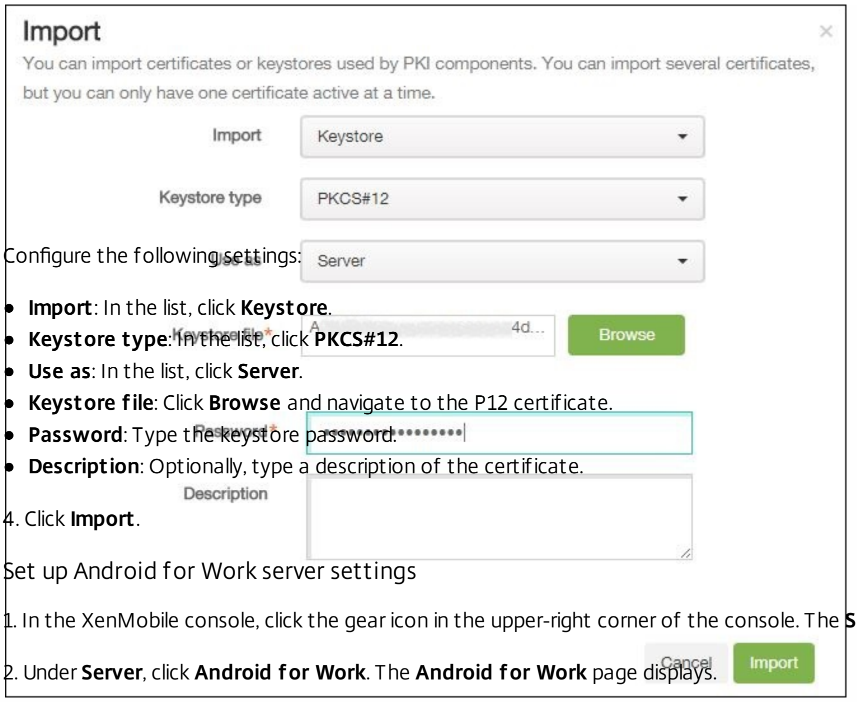
Settings > Certificates

Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

□	Name	Description	Valid from	Valid to	Type	Private key

3. Click **Import**. The **Import** dialog box displays.



Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import: Keystore

Keystore type: PKCS#12

Use as: Server

Keystore file*: A…4d...

Password*: •••••••••

Description

Configure the following settings:

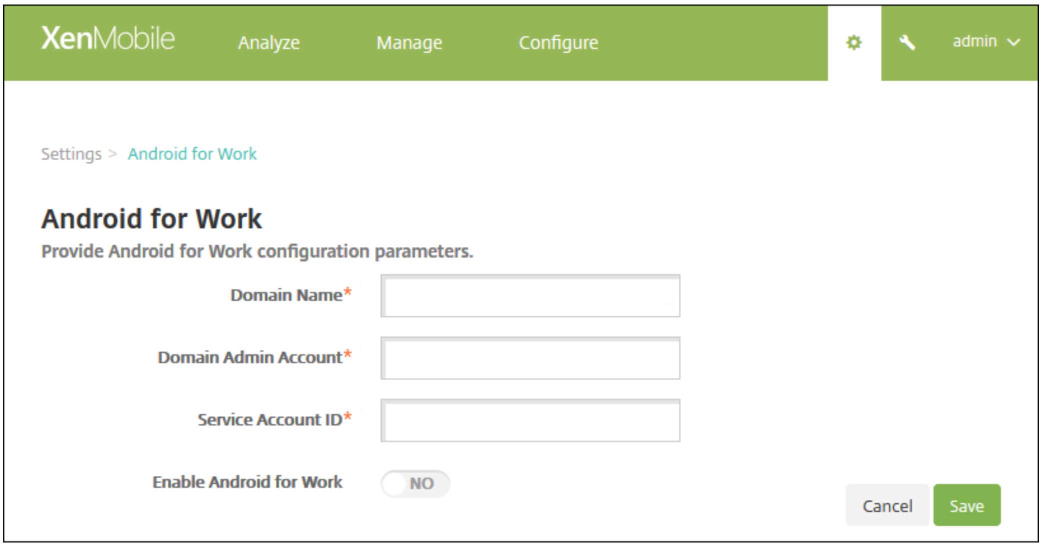
- **Import**: In the list, click **Keystore**.
- **Keystore type**: In the list, click **PKCS#12**.
- **Use as**: In the list, click **Server**.
- **Keystore file**: Click **Browse** and navigate to the P12 certificate.
- **Password**: Type the keystore password.
- **Description**: Optionally, type a description of the certificate.

4. Click **Import**.

Set up Android for Work server settings

1. In the XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page displays.

2. Under **Server**, click **Android for Work**. The **Android for Work** page displays.



Settings > Android for Work

Android for Work

Provide Android for Work configuration parameters.

Domain Name*

Domain Admin Account*

Service Account ID*

Enable Android for Work: NO

Configure the following settings:

- **Domain name**: Type your Android for Work 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).
- **Enable Android for Work**: Click to enable or disable Android for Work.

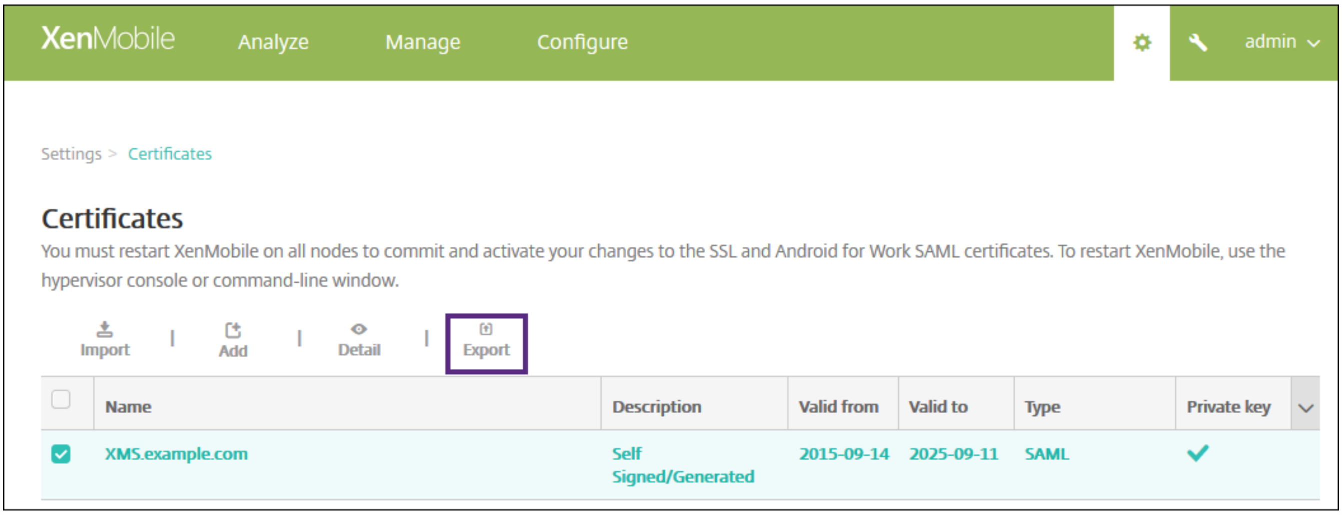
3. Click **Save**.

Enable SAML-based single-sign-on

1. Sign in to the XenMobile console.

2. Click the gear icon in the upper-right corner of the console. The **Settings** page displays.

3. Click **Certificates**. The **Certificates** page dispalyspens.



Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

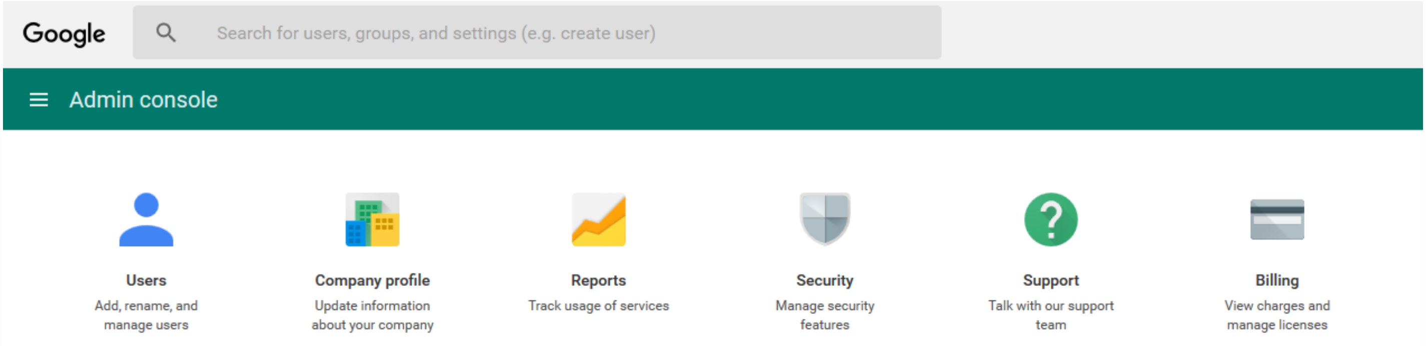
□	Name	Description	Valid from	Valid to	Type	Private key
☑	XMS.example.com	Self Signed/Generated	2015-09-14	2025-09-11	SAML	✓

3. In the list of certificates, click the SAML certificate.

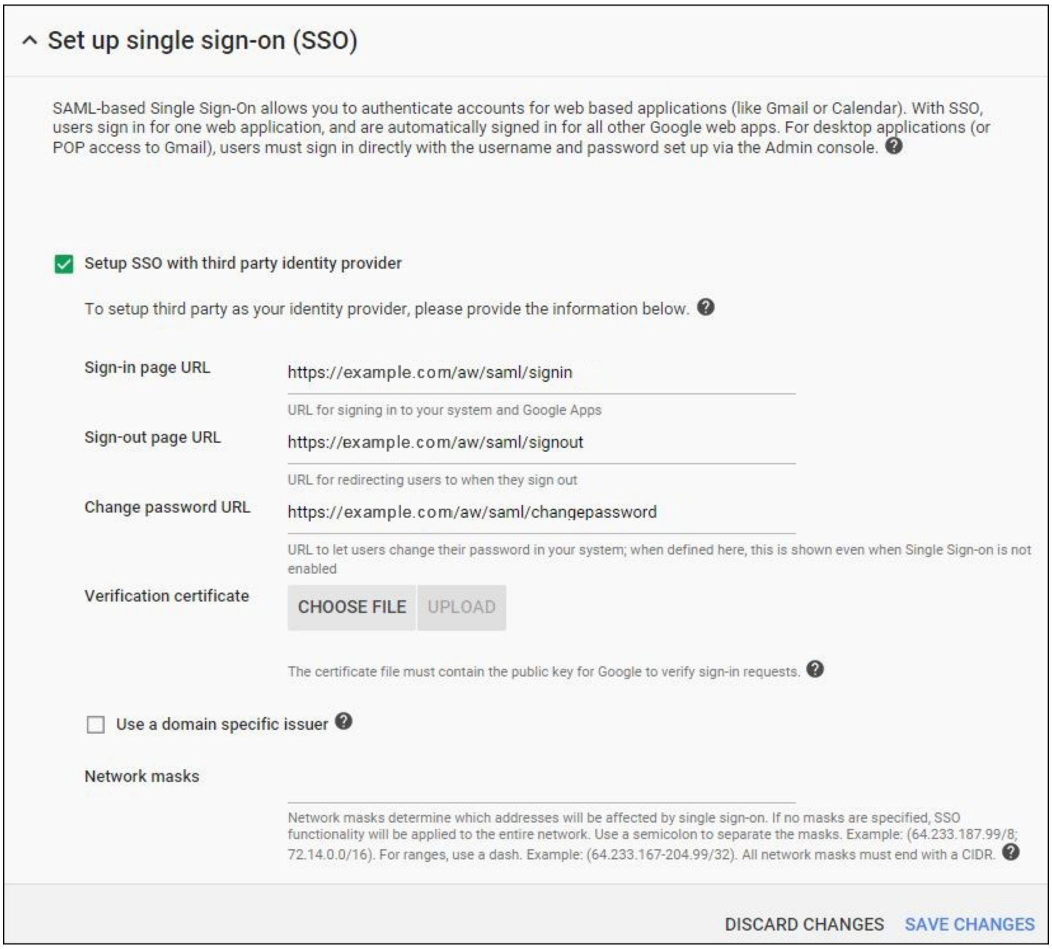
4. Click **Export** and save the certificate to your computer.

5. Sign in to the Google Admin portal by using your Android for Work administrator credentials. For access to the portal, see Google Admin portal.

6. Click **Security**.


Google
Search for users, groups, and settings (e.g. create user)
Admin console
Users
Add, rename, and manage users
Company profile
Update information about your company
Reports
Track usage of services
Security
Manage security features
Support
Talk with our support team
Billing
View charges and manage licenses

7. Under **Security**, click **Set up single sign-on (SSO)** and then configure the following settings.



^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console.

☑ Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below.

Sign-in page URL: https://example.com/aw/saml/signin

URL for signing in to your system and Google Apps

Sign-out page URL: https://example.com/aw/saml/signout

URL for redirecting users to when they sign out

Change password URL: https://example.com/aw/saml/changepassword

URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate: CHOOSE FILE UPLOAD

The certificate file must contain the public key for Google to verify sign-in requests.

□ Use a domain specific issuer

Network masks

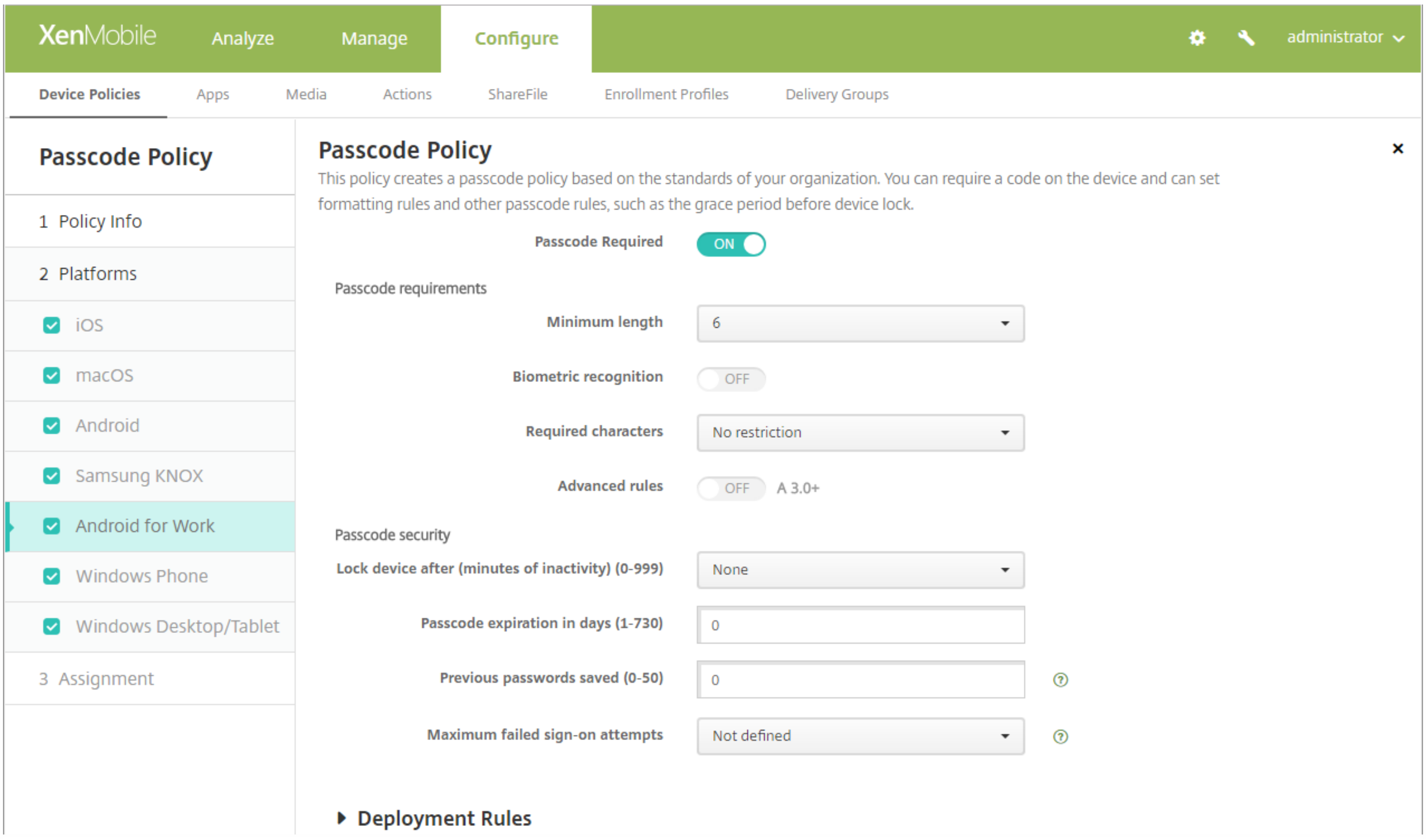
Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR.

- **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 XenMobile.

8. Click **SAVE CHANGES**.

Set up an Android for Work device policy

Set up a Passcode policy so that users must establish a passcode on their devices when they first enroll.



Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode Required: ON

Passcode requirements

Minimum length: 6

Biometric recognition: OFF

Required characters: No restriction

Advanced rules: OFF A 3.0+

Passcode security

Lock device after (minutes of inactivity) (0-999): None

Passcode expiration in days (1-730): 0

Previous passwords saved (0-50): 0

Maximum failed sign-on attempts: Not defined

The basic steps to setting up any device policy are as follows.

1. Sign on to the XenMobile 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 for Work** and then configure the settings for the policy.

6. Assign the policy to a Delivery Group.

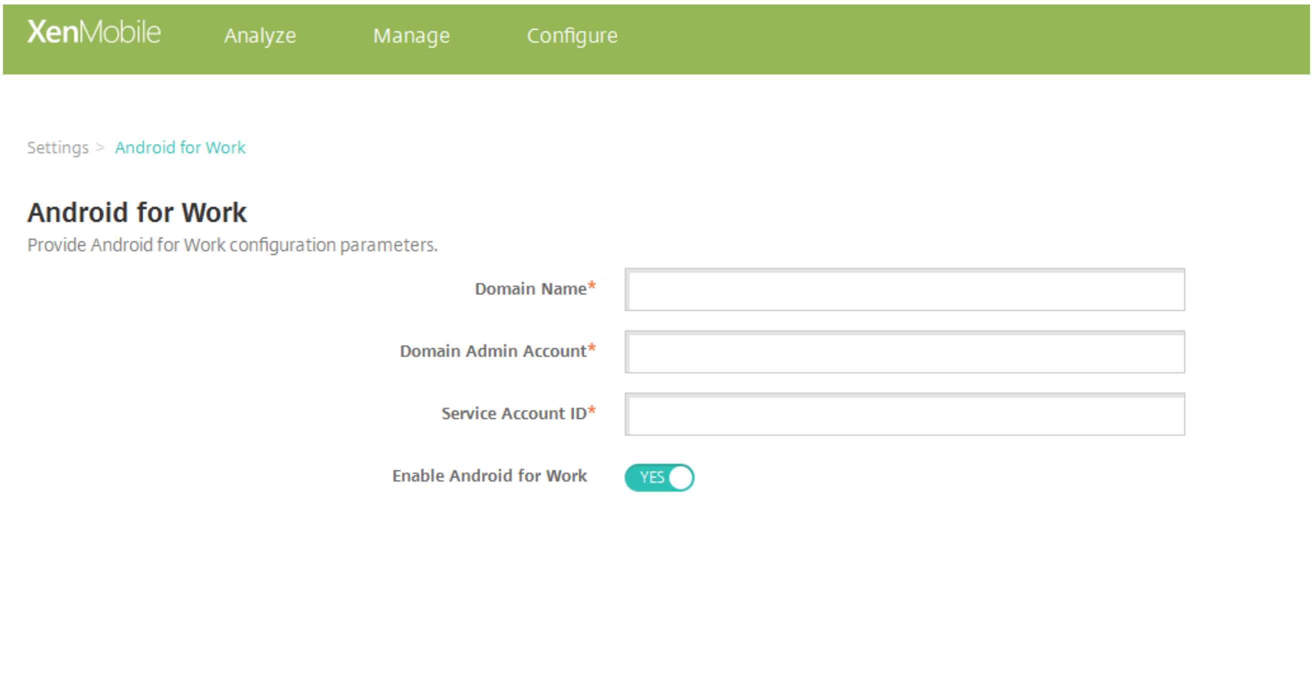
For more information about setting up other device policies that are available for Android for Work, see XenMobile Device Policies by Platform.

Configure Android for Work account settings

Before you can start managing Android apps and policies on devices, you must set up an Android for Work domain and account information in XenMobile. First, complete Android for Work setup tasks on Google to set up a domain administrator and to obtain a service account ID and a binding token.

1. In the XenMobile web console, click the gear icon in the upper-right corner. The **Settings** page displays.

2. Under **Server**, click **Android for Work**. The **Android for Work** configuration page displays.



Android for Work

Provide Android for Work configuration parameters.

Domain Name*

Domain Admin Account*

Service Account ID*

Enable Android for Work YES

3. On the **Android for Work** 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.
- **Enable Android for Work**: Select whether to enable Android for Work or not.

4.Click **Save**.

Enrolling Android for Work devices

If your device enrollment process requires users to enter a username or user ID, the format accepted depends on how the XenMobile server is configured to search for users by User Principal Name (UPN) or SAM account name.

If the XenMobile server is configured to search for users by UPN, users must enter a UPN in the format:

- *username@domain*

If the XenMobile server is configured to search for users by SAM users must enter a SAM in one of these formats:

- *username@domain*
- *domain\username*

To determine which type of user name your XenMobile server is configured for:

1. In the XenMobile server console click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **LDAP** to view the configuration of the LDAP connection.
3. Near the bottom of the page, view the **User search by** field:

- If it is set to **userPrincipalName**, the XenMobile server is set for UPN.
- If it is set to **sAMAccountName**, the XenMobile server is set for SAM.

Provisioning work-managed device mode in Android for Work

Work-managed device mode for Android for Work is available for corporate-owned devices only. XenMobile supports two methods of enrollment in work-managed device mode:

- **Near field communication (NFC) bump.** The NFC bump enrollment method can be used on fleet devices that have been reset to their factory settings.

A 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.

- **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 work-managed device mode by scanning a QR code from the setup wizard.

NFC bump

To enroll a device in device mode using NFC bumps requires two devices: one that has been reset to its factory settings and one running the XenMobile Provisioning Tool.

Prerequisites

- A XenMobile Server version 10.4 that is enabled for Android for Work.
- A factory-reset device, provisioned for Android for Work in work-managed device mode. 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 10.4 or on the Citrix downloads page.

Each device can have only one Android for Work profile, managed by an enterprise mobility management (EMM) app. In XenMobile, 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.

You can start work-managed device mode on new devices or on devices restored to factory settings. You manage the entire device by using XenMobile.

Data transferred through the NFC bump

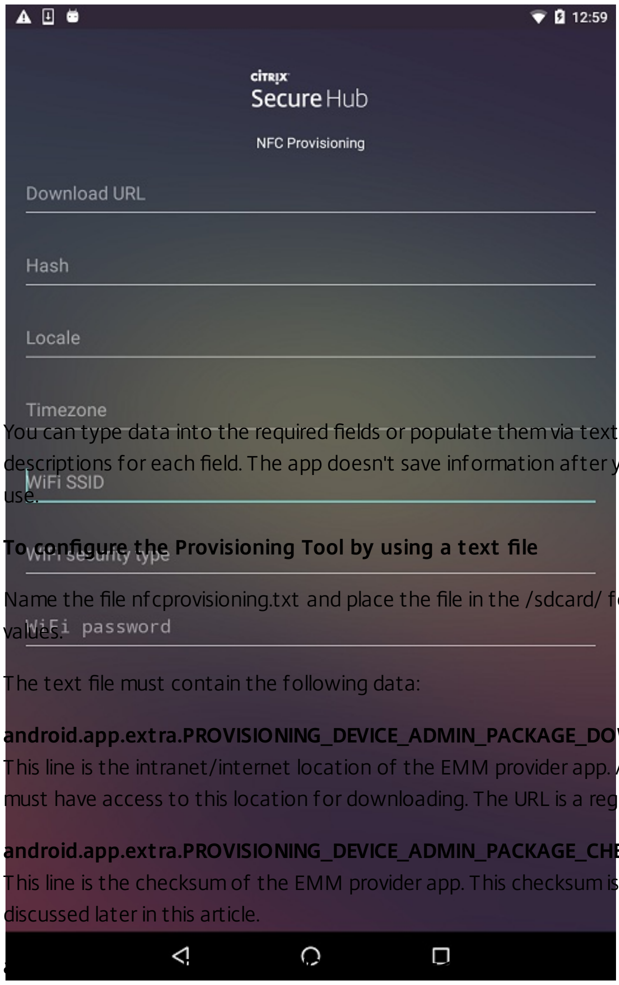
Provisioning a factory-reset device requires you to send the following data through an NFC bump to initialize Android for Work:

- 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 XenMobile 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 use.

To configure the Provisioning Tool by using a text file

Name the file nfcprovisioning.txt and place the file in the /sdcard/ folder on the SD card of the device. The app can then read the text file and populate the values.

The text file must 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.

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.

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=http://www.somepublicurlhere.com/path/to/securehub.apk
>
> android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\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=http://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\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

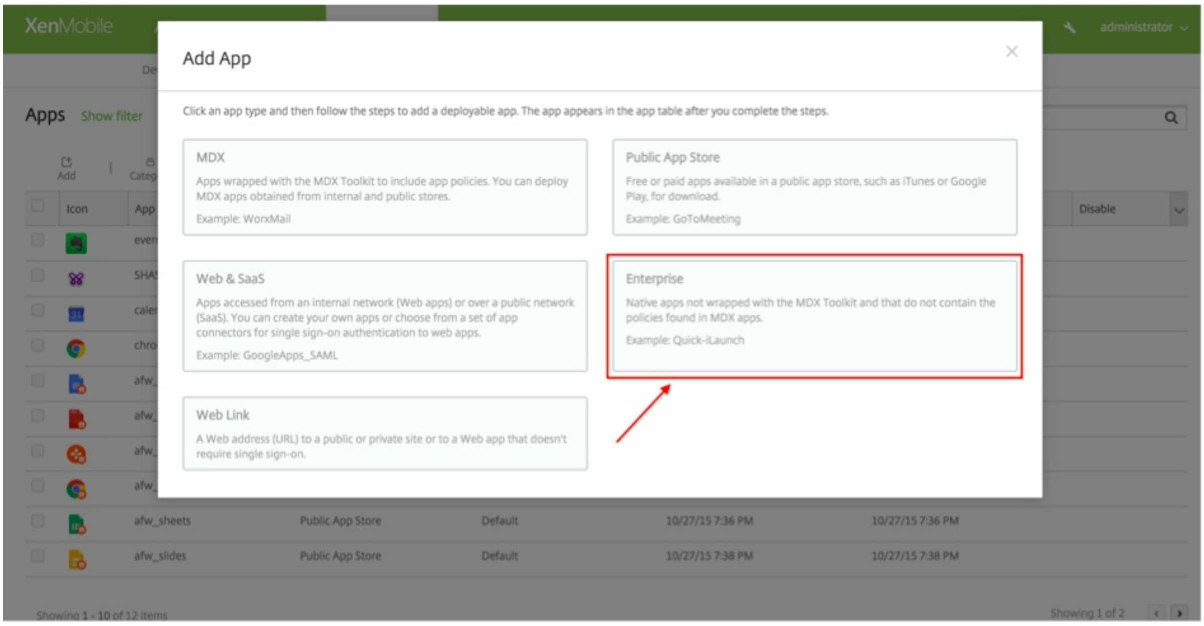
To get the checksum of any app, add the app as an enterprise app.

1. In the XenMobile console, go to **Configure > Apps** and then click **Add**.

The **Add Apps** window appears.

2. Click **Enterprise**.

The **App information** page displays.



Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
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 web apps.
Example: GoogleApps_SAML

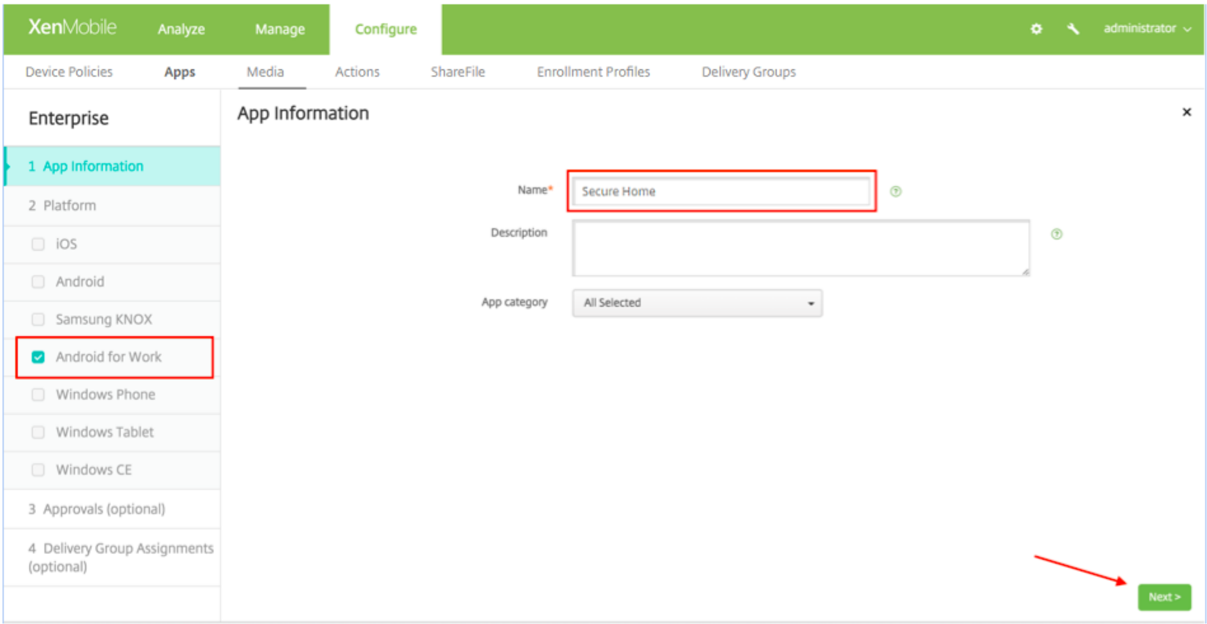
Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

XenMobile
administrator
Apps
Show filter
Add
Categ
Icon
App
Disable
afw_sheets Public App Store Default 10/27/15 7:36 PM 10/27/15 7:36 PM
afw_slides Public App Store Default 10/27/15 7:38 PM 10/27/15 7:38 PM
Showing 1 - 10 of 12 items
Showing 1 of 2

3. Select the following configuration and then click **Next**.

The **Android for Work Enterprise App** page displays.



App Information

Name* Secure Home

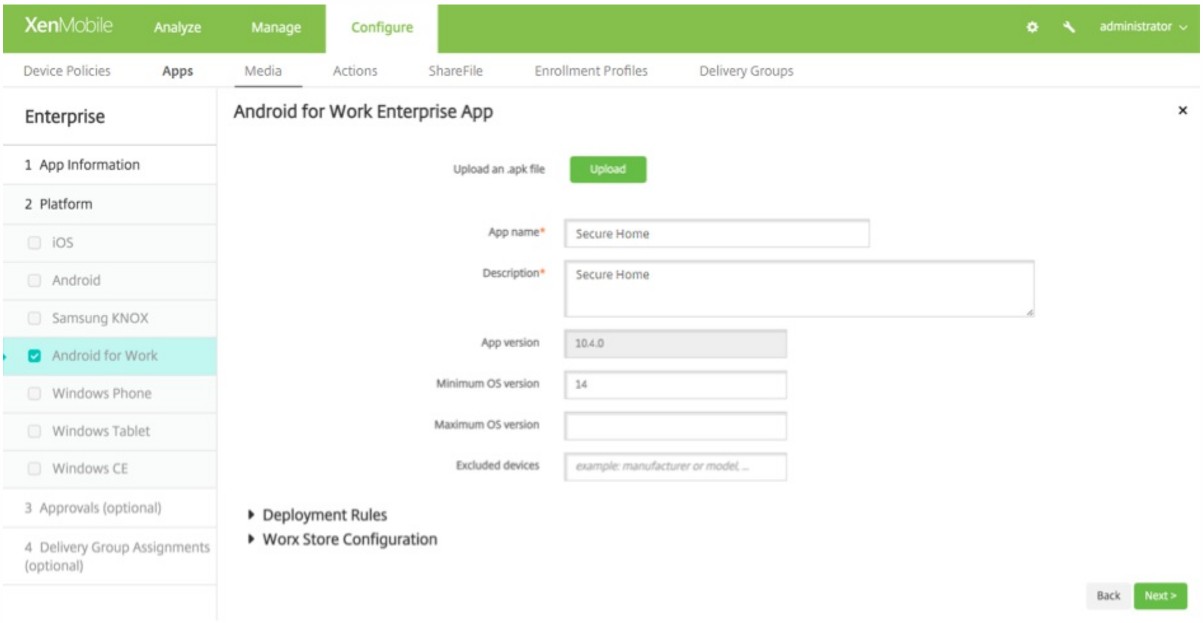
Description

App category All Selected

☐ iOS
☐ Android
☐ Samsung KNOX
☑ Android for Work
☐ Windows Phone
☐ Windows Tablet
☐ Windows CE

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 display.



Android for Work Enterprise App

Upload an .apk file

App name* Secure Home

Description* Secure Home

App version 10.4.0

Minimum OS version 14

Maximum OS version

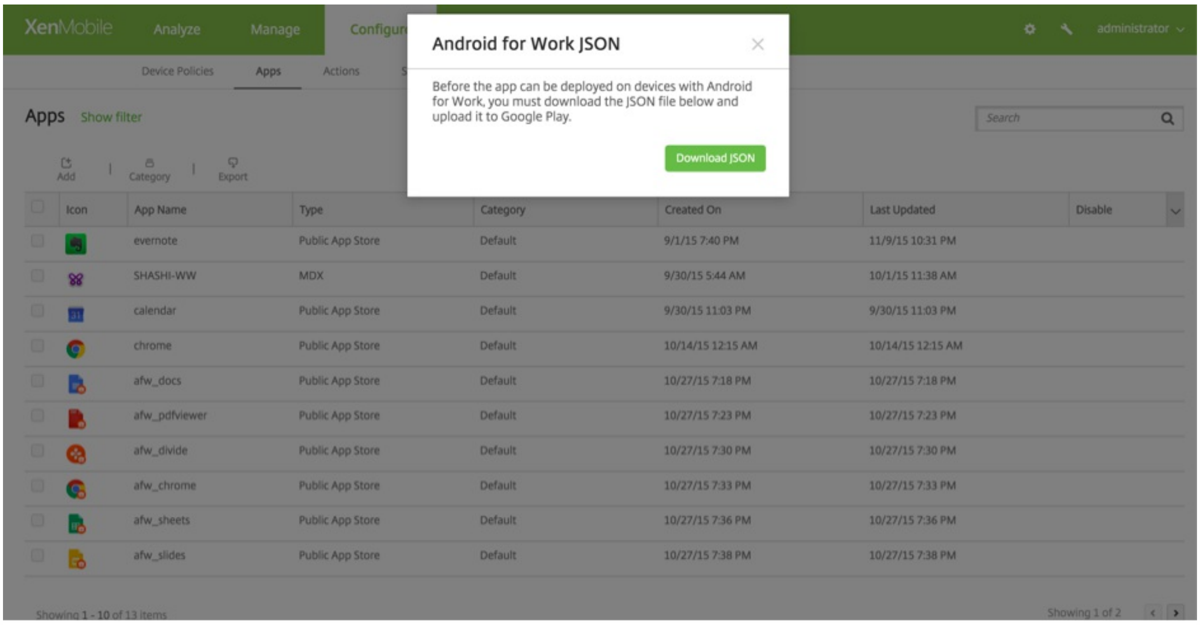
Excluded devices *example: manufacturer or model, ...*

▸ Deployment Rules

▸ Worx Store Configuration

☐ iOS
☐ Android
☐ Samsung KNOX
☑ Android for Work
☐ Windows Phone
☐ Windows Tablet
☐ Windows CE

5. Click **Next** to bring up a 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.



Android for Work JSON

Before the app can be deployed on devices with Android for Work, you must download the JSON file below and upload it to Google Play.

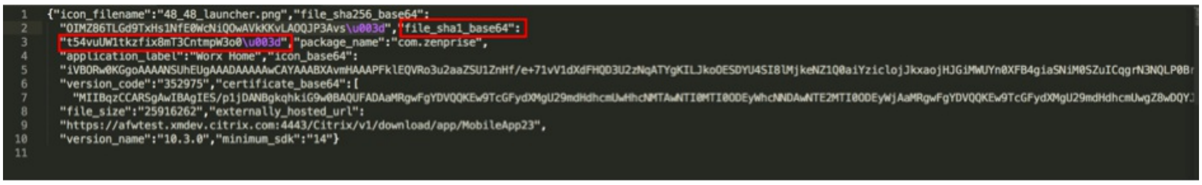
Download JSON

□	Icon	App Name	Type	Category	Created On	Last Updated	Disable
□		evernote	Public App Store	Default	9/1/15 7:40 PM	11/9/15 10:31 PM	
□		SHASHI-WW	MDX	Default	9/30/15 5:44 AM	10/1/15 11:38 AM	
□		calendar	Public App Store	Default	9/30/15 11:03 PM	9/30/15 11:03 PM	
□		chrome	Public App Store	Default	10/14/15 12:15 AM	10/14/15 12:15 AM	
□		afw_docs	Public App Store	Default	10/27/15 7:18 PM	10/27/15 7:18 PM	
□		afw_pdfviewer	Public App Store	Default	10/27/15 7:23 PM	10/27/15 7:23 PM	
□		afw_divide	Public App Store	Default	10/27/15 7:30 PM	10/27/15 7:30 PM	
□		afw_chrome	Public App Store	Default	10/27/15 7:33 PM	10/27/15 7:33 PM	
□		afw_sheets	Public App Store	Default	10/27/15 7:36 PM	10/27/15 7:36 PM	
□		afw_slides	Public App Store	Default	10/27/15 7:38 PM	10/27/15 7:38 PM	

Showing 1 - 10 of 13 items

Showing 1 of 2

A typical JSON file looks like the following:



```
{"icon_filename":"48_48_launcher.png","file_sha256_base64":
  "OIMZ86TLGd9TxHs1NfE0WcNiQOwAVkKKvLAOQJP3Avs\u003d","file_sha1_base64":
  "t54vuUW1tkzfix8mT3CntmpW3o0\u003d","package_name":"com.zenprise",
  "application_label":"Worx Home","icon_base64":
  "iVBORw0KGgoAAAANSUhEUgAAADAAAAAwCAYAAABXAvmHAAAPFklEQVRo3u2aaZSU1ZnHf/e+71vV1dXdFHQD3U2zNqATYgKILJkoOESDYU4SI8lMjkeNZ1Q0aiYziclojJkxaojHJGGiMWUYn0XFB4giaSNiM0SZuICqgrN3NQLP0B
  "version_code":"352975","certificate_base64":[
    "MIIBqzCCARSgAwIBAgIES/p1jDANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQKEw9TcGFydXMgU29mdHdhcmUwHhcNMTAwNTI0MTI0ODEyWhcNNDAwNTE2MTI0ODEyWjAaMRgwFgYDVQQKEw9TcGFydXMgU29mdHdhcmUwgZ8wDQYJ
  "file_size":"25916262","externally_hosted_url":
  "https://afwtest.xmdev.citrix.com:4443/Citrix/v1/download/app/MobileApp23",
  "version_name":"10.3.0","minimum_sdk":"14"}
```

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 by Google under Apache license 2.0
- Design support library by Google under Apache license 2.0
- v7 Palette library by Google under Apache license 2.0
- Butter Knife by Jake Wharton under Apache license 2.0

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. The QR code is scanned by the devices camera to enroll the device.

Prerequisites

Provisioning work-managed device mode using QR code is supported on all Android devices running Android 7.0 and above.

Creating a QR code from a JSON

Create a JSON with the following fields.

These fields are required:

Key: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Value: com.zenprise/com.zenprise.configuration.AdminFunction

Key: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Value: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Key: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Value: https://path/to/securehub.apk

NOTE: If Secure Hub is uploaded onto Citrix XenMobile server as an enterprise app, it can be downloaded from https://<fqdn>:4443/*instanceName*/worxhome.apk. The path to Secure Hub APK that is used as the value above, should be accessible over the Wi-Fi connection that the device would be connected 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.

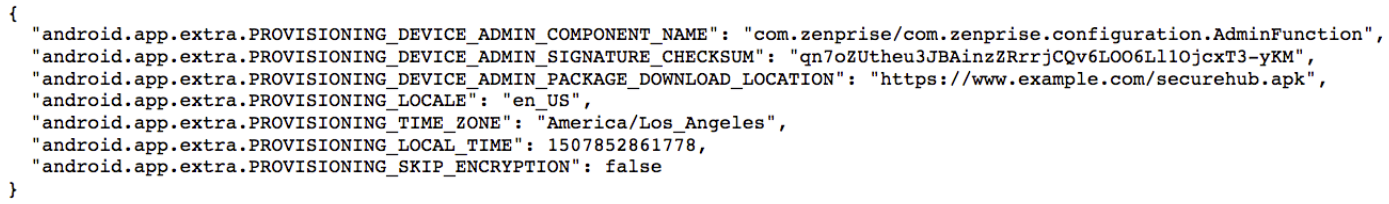
android.app.extra.PROVISIONING_LOCAL_TIME

Time in milliseconds since the Epoch. The Unix epoch (or Unix time or POSIX time or Unix timestamp) is the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT), not counting leap seconds (in ISO 8601: 1970-01-01T00:00:00Z)

android.app.extra.PROVISIONING_SKIP_ENCRYPTION

Set this to true to skip encryption during profile creation. Set to false to force encryption during profile creation.

A typical JSON looks like this:



```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

Validate the JSON that is created using any JSON validation tool (for example, https://jsonlint.com) and convert that JSON string to a QR code using any online QR code generator (for example, http://goqr.me).

This QR code is scanned by a factory-reset device to enroll the device in work-managed device mode.

Enroll the device

To enroll a device in work-managed device mode, the device must be in factory reset state.

To enroll the device:

1. Tap the screen 6 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.

More information

For more information, see this Google guide for Android EMM developers: https://developers.google.com/android/work/prov-devices#qr_code_method .

Provisioning work profile mode in Android for Work

Work profile mode for Android for Work is available for devices on which you securely separate the corporate and personal areas on a device (for example, BYOD devices). The enrollment experience for work profile mode is similar to Android enrollment in XenMobile, with the user downloading Secure Hub from Google Play and enrolling the device. For information about enrolling Android devices, see Enroll devices.

> **Tip**
>
> When enrolling devices in Android for Work in work profile mode, always go to Google Play. From there, enable Secure Hub to appear in the user's personal profile.

Bulk enrollment of iOS and macOS devices

Sep 06, 2017

You can enroll large numbers of iOS and macOS devices in XenMobile in two ways.

- You can use the Apple Device Enrollment Program (DEP) to enroll the iOS and macOS devices that you buy directly from Apple, a participating Apple Authorized Reseller, or a carrier. XenMobile supports the Device Enrollment Program for Business and Apple School Manager for Education. This article describes integrating with Business DEP accounts. For information about Apple School Manager DEP accounts, see Integrate with Apple Education features.

  For DEP enrollment of macOS devices, XenMobile requires that the devices run macOS 10.10 or later.

- Or you can use the Apple Configurator to enroll iOS devices whether or not you purchased them directly from Apple.

With Business DEP, you do not have to touch or prepare the devices. Instead, you submit device serial numbers or purchase order numbers through DEP to configure and enroll the devices. After XenMobile 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 DEP, 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 DEP, see the Apple Device Enrollment Program page.

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 XenMobile, the devices receive policies from XenMobile. You can then start managing the devices. For more information about using Apple Configurator, see the Apple Configurator help.

> Important
>
> You must open required ports for connectivity between XenMobile and Apple. For more information, see Port requirements.

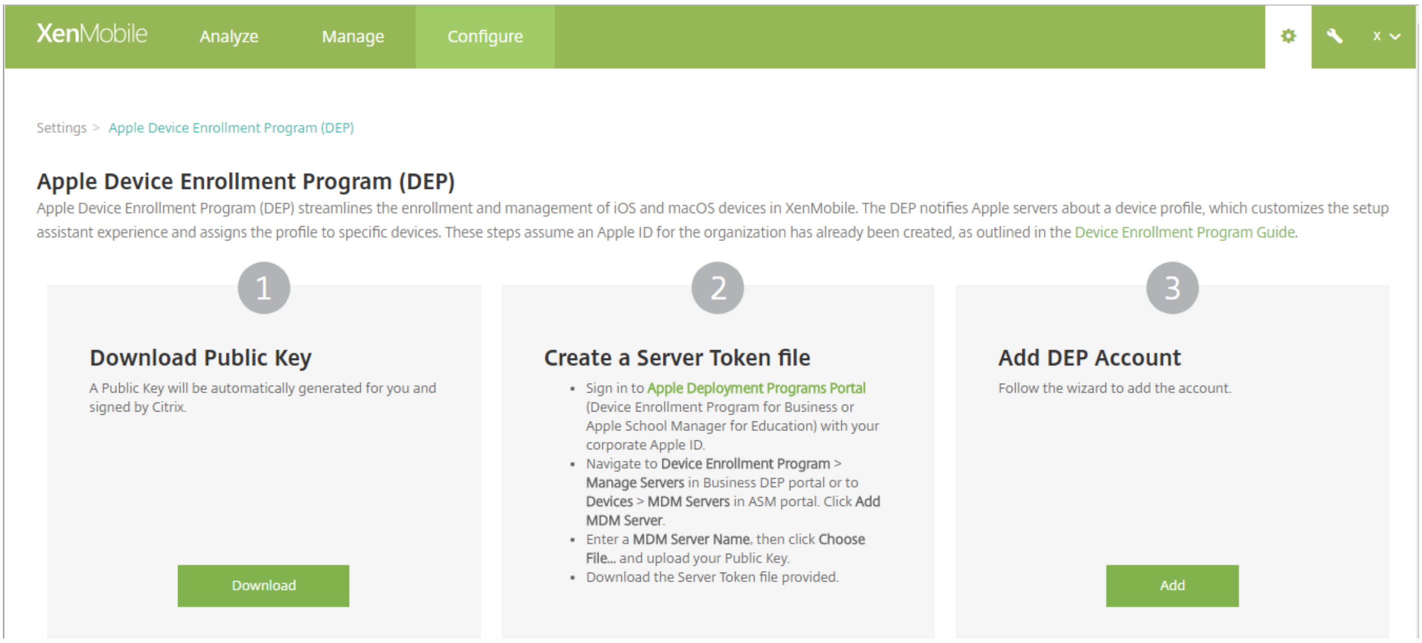
Integrate your Business Apple DEP account with XenMobile

If you do not have an Apple Business DEP account, see Deploy iOS and macOS devices through Apple DEP.

To connect your Apple Business DEP account with your XenMobile server deployment, you enter information in the XenMobile console and the Apple DEP Portal, as described in the following steps.

Step 1: Download a public key from your XenMobile server

1. Log on to the XenMobile console and go to **Settings > Apple Device Enrollment Program (DEP)**.



Settings > Apple Device Enrollment Program (DEP)

Apple Device Enrollment Program (DEP)

Apple Device Enrollment Program (DEP) streamlines the enrollment and management of iOS and macOS devices in XenMobile. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. These steps assume an Apple ID for the organization has already been created, as outlined in the Device Enrollment Program Guide.

1 Download Public Key

A Public Key will be automatically generated for you and signed by Citrix.

Download

2 Create a Server Token file

- Sign in to Apple Deployment Programs Portal (Device Enrollment Program for Business or Apple School Manager for Education) with your corporate Apple ID.
- Navigate to Device Enrollment Program > Manage Servers in Business DEP portal or to Devices > MDM Servers in ASM portal. Click Add MDM Server.
- Enter a MDM Server Name, then click Choose File... and upload your Public Key.
- Download the Server Token file provided.

3 Add DEP Account

Follow the wizard to add the account.

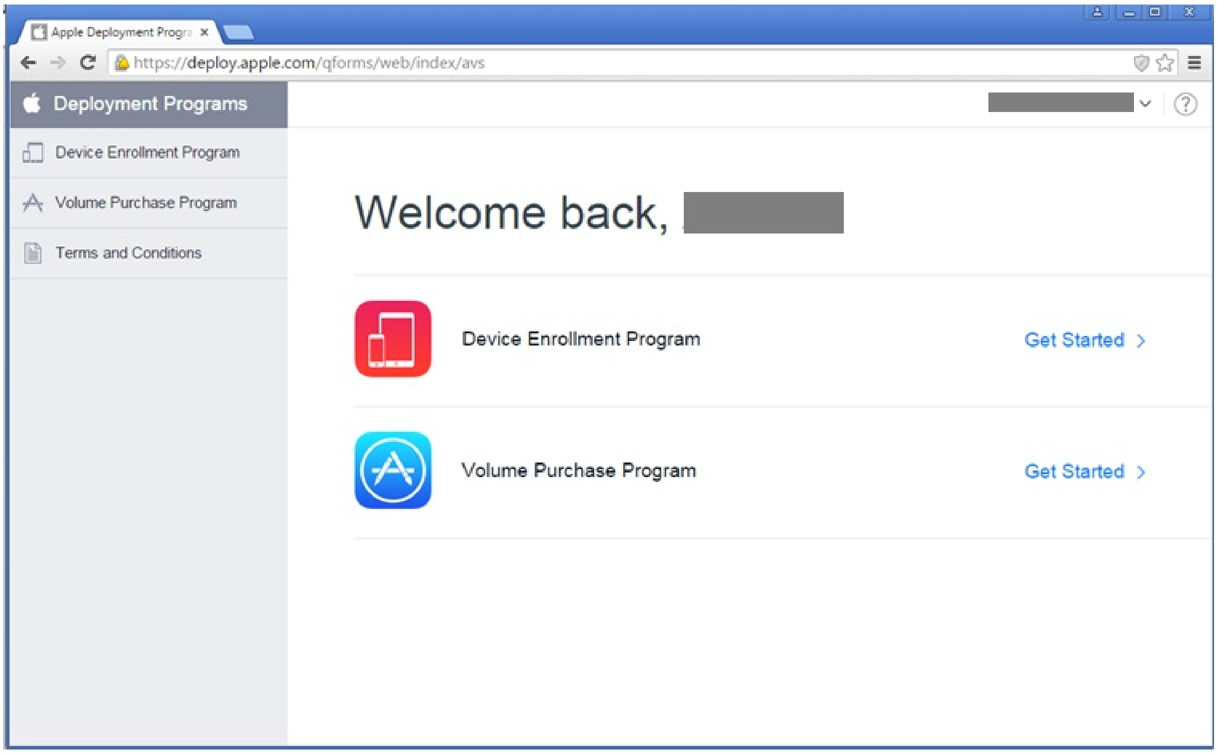
Add

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.

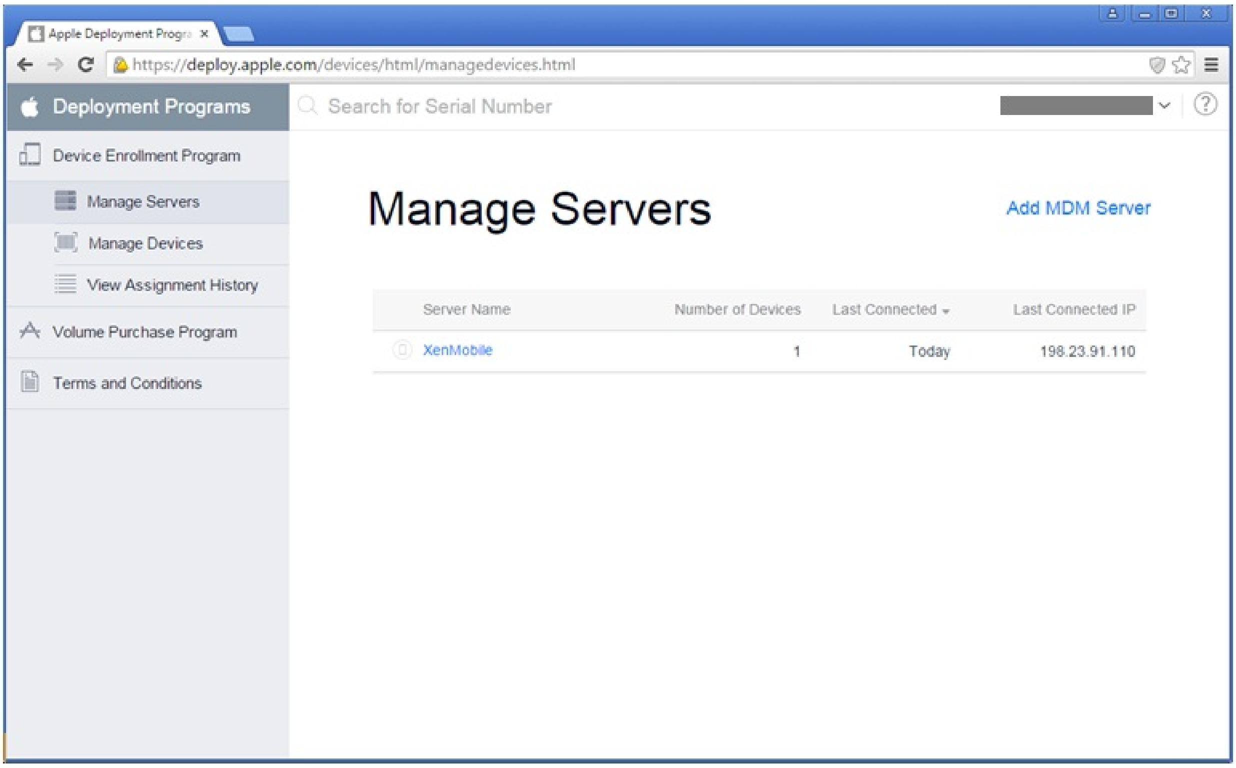
2. In the Apple DEP Portal, click **Device Enrollment Program**.



[redacted]

Welcome back, [redacted]

3. Click **Manage Servers** and then on the right side, click **Add MDM Server**.


Apple Deployment Progra ×

https://deploy.apple.com/devices/html/managedevices.html

Deployment Programs

Search for Serial Number

[redacted]

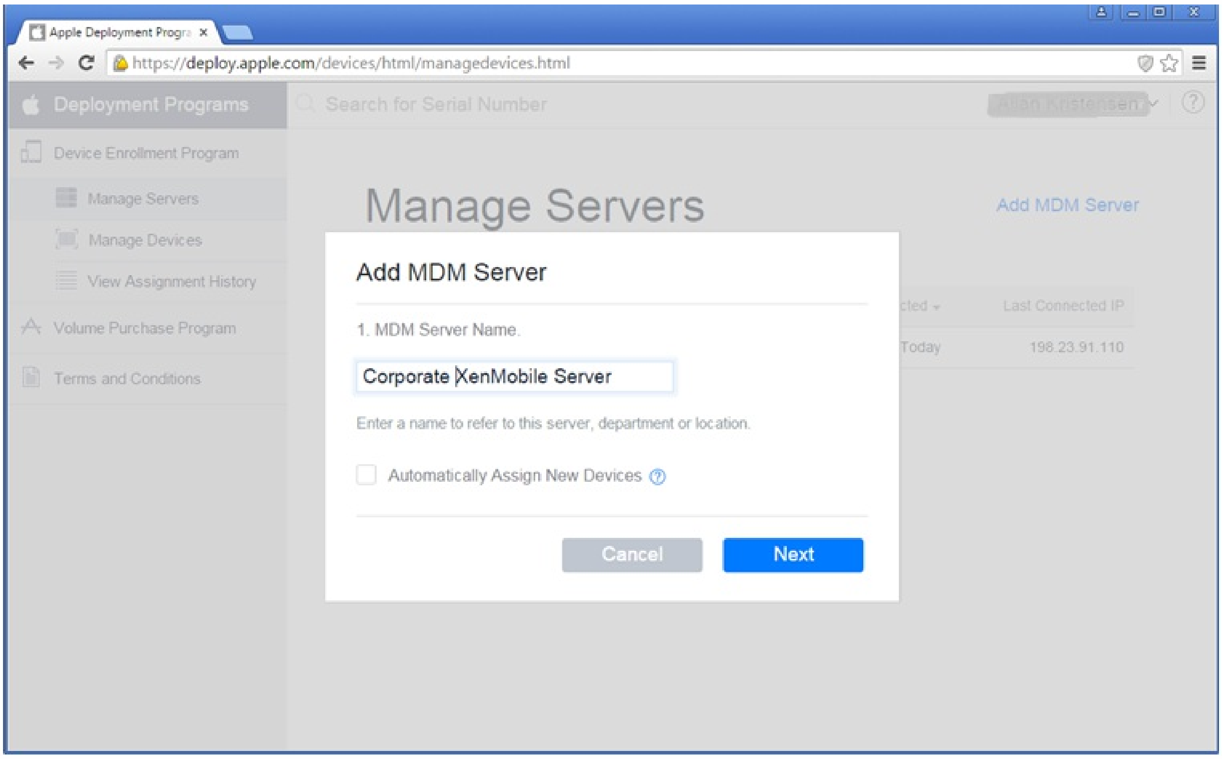
- Device Enrollment Program
  - Manage Servers
  - Manage Devices
  - View Assignment History
- Volume Purchase Program
- Terms and Conditions

Manage Servers

Add MDM Server

Server Name	Number of Devices	Last Connected	Last Connected IP
XenMobile	1	Today	198.23.91.110

4. In **Add MDM Server**, enter a name for your XenMobile server and then click **Next**.


Add MDM Server

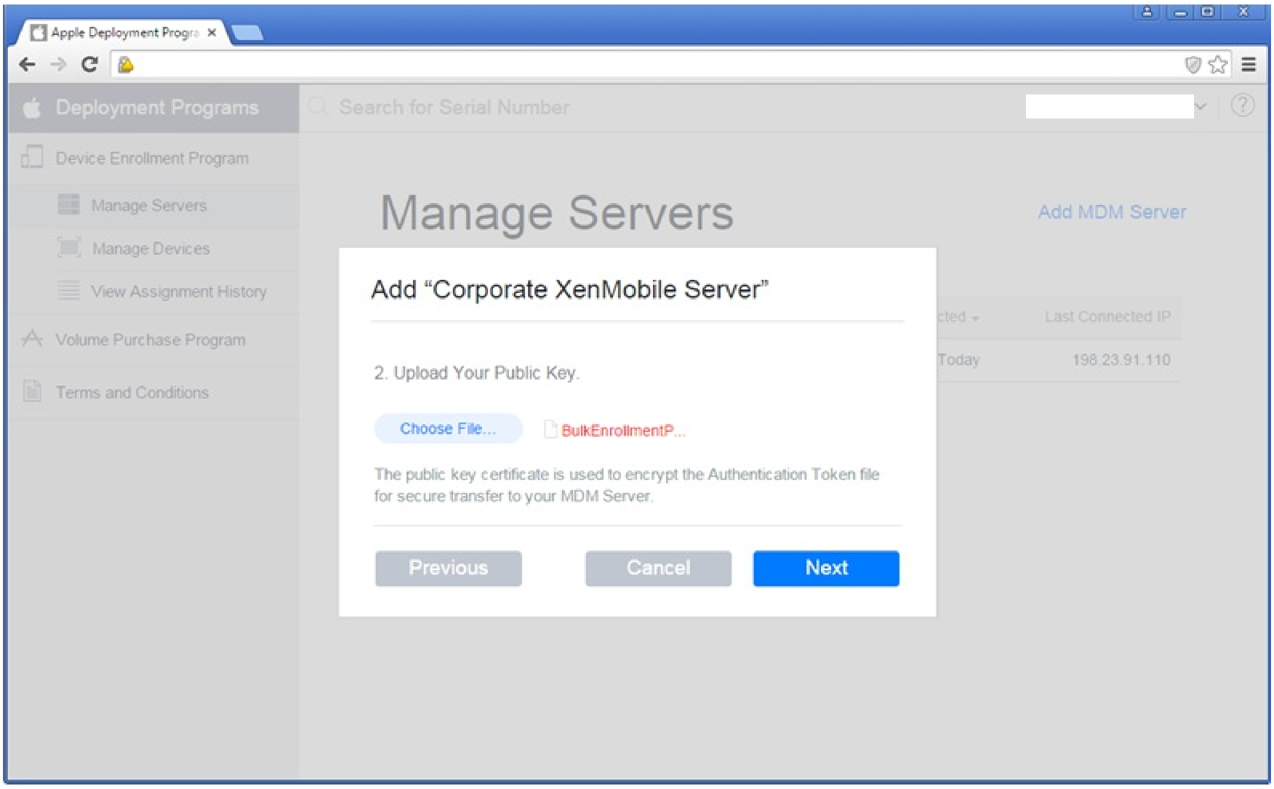
1. MDM Server Name.

Corporate XenMobile Server

Enter a name to refer to this server, department or location.

□ Automatically Assign New Devices

5. On the Apple DEP Portal, click **Choose file**, choose the public key you downloaded from XenMobile, and click **Next**.

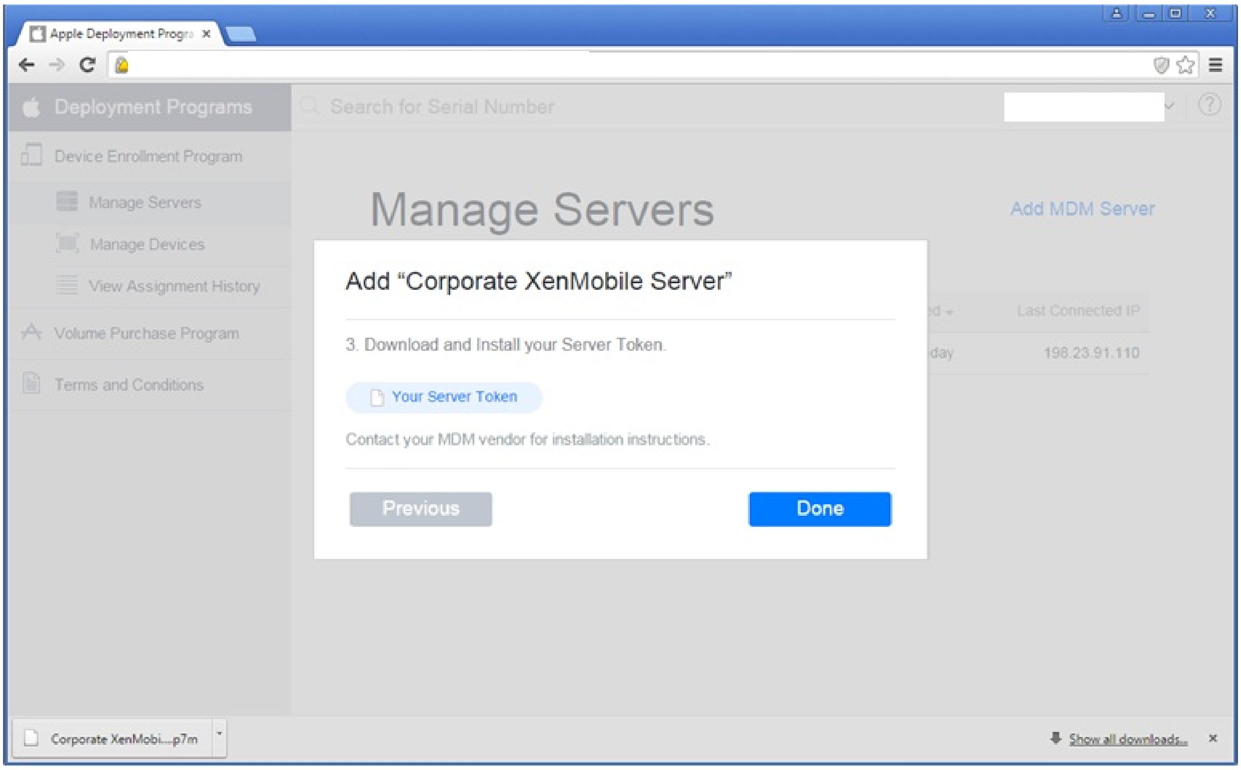


Add "Corporate XenMobile Server"

2. Upload Your Public Key.

The public key certificate is used to encrypt the Authentication Token file for secure transfer to your MDM Server.

6. Click **Your Server Token** to generate a server token, which downloads from the browser, and then click **Done**.



Add "Corporate XenMobile Server"

3. Download and Install your Server Token.

Contact your MDM vendor for installation instructions.

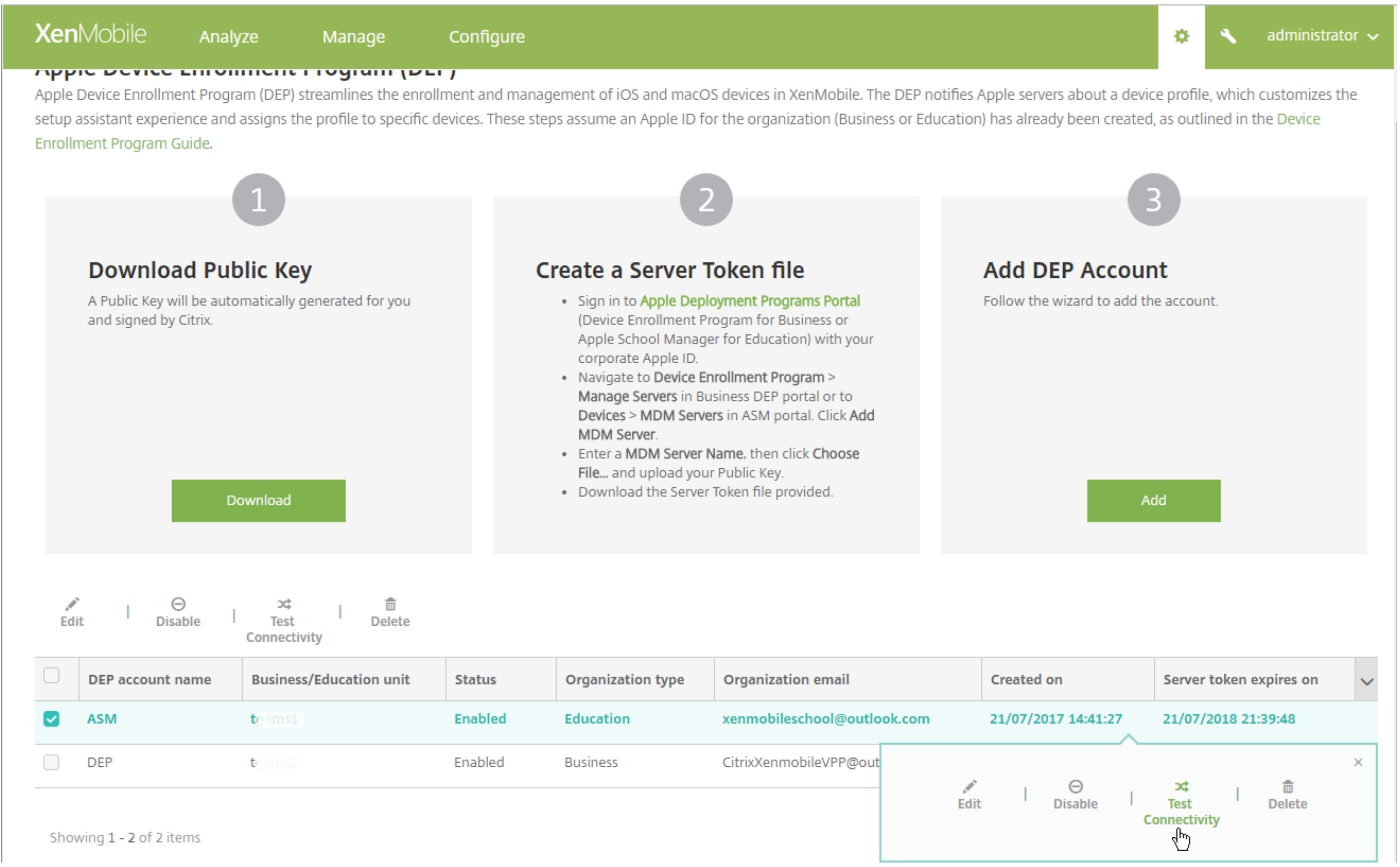
Your Apple DEP token information appears in the XenMobile console after you import the token file. You will upload the server token file when adding the DEP account to XenMobile.

Step 3: Add a DEP account to XenMobile

You can add multiple DEP accounts to XenMobile. This feature enables you to use different enrollment settings and setup assistant options by country, department, and so on. You then associate DEP accounts with different device policies.

For example, you might centralize all of your DEP accounts from different countries on the same XenMobile server, to import and supervise all DEP 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 XenMobile console, go to **Settings > Apple Device Enrollment Program (DEP)** and, under **Add DEP Account**, click **Add**.



Apple Device Enrollment Program (DEP)

Apple Device Enrollment Program (DEP) streamlines the enrollment and management of iOS and macOS devices in XenMobile. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. These steps assume an Apple ID for the organization (Business or Education) has already been created, as outlined in the Device Enrollment Program Guide.

1 **Download Public Key**

A Public Key will be automatically generated for you and signed by Citrix.

Download

2 **Create a Server Token file**

- Sign in to Apple Deployment Programs Portal (Device Enrollment Program for Business or Apple School Manager for Education) with your corporate Apple ID.
- Navigate to Device Enrollment Program > Manage Servers in Business DEP portal or to Devices > MDM Servers in ASM portal. Click Add MDM Server.
- Enter a MDM Server Name, then click Choose File... and upload your Public Key.
- Download the Server Token file provided.

3 **Add DEP Account**

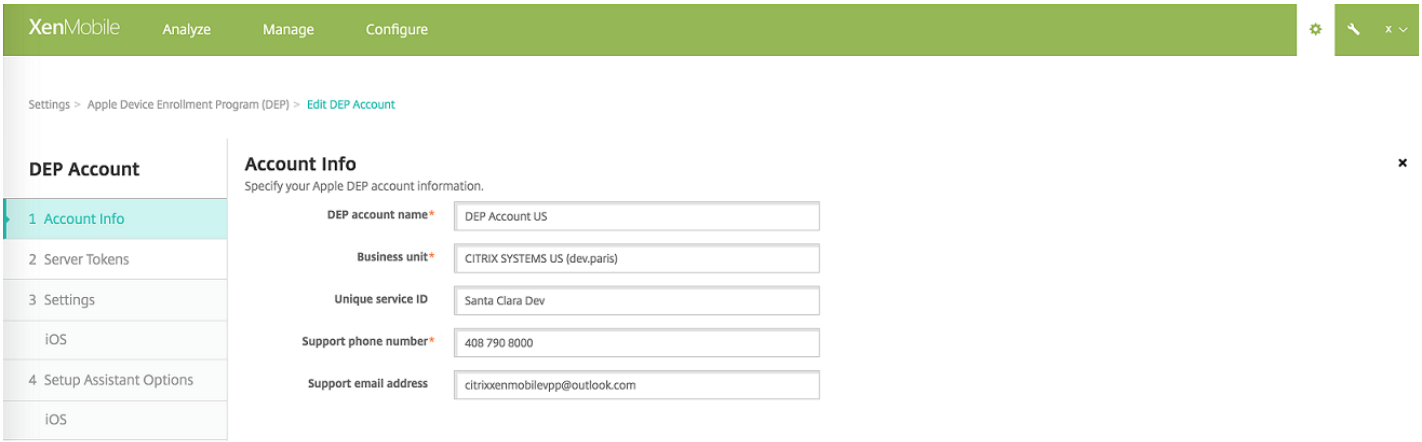
Follow the wizard to add the account.

Add

☐	DEP account name	Business/Education unit	Status	Organization type	Organization email	Created on	Server token expires on
☑	ASM	t[redacted]	Enabled	Education	xenmobileschool@outlook.com	21/07/2017 14:41:27	21/07/2018 21:39:48
☐	DEP	t[redacted]	Enabled	Business	CitrixXenmobileVPP@out		

Showing 1 - 2 of 2 items

2. In the **Account Info** page, specify these settings:


XenMobile
Analyze
Manage
Configure
Settings > Apple Device Enrollment Program (DEP) > Edit DEP Account
DEP Account
1 Account Info
2 Server Tokens
3 Settings
iOS
4 Setup Assistant Options
iOS

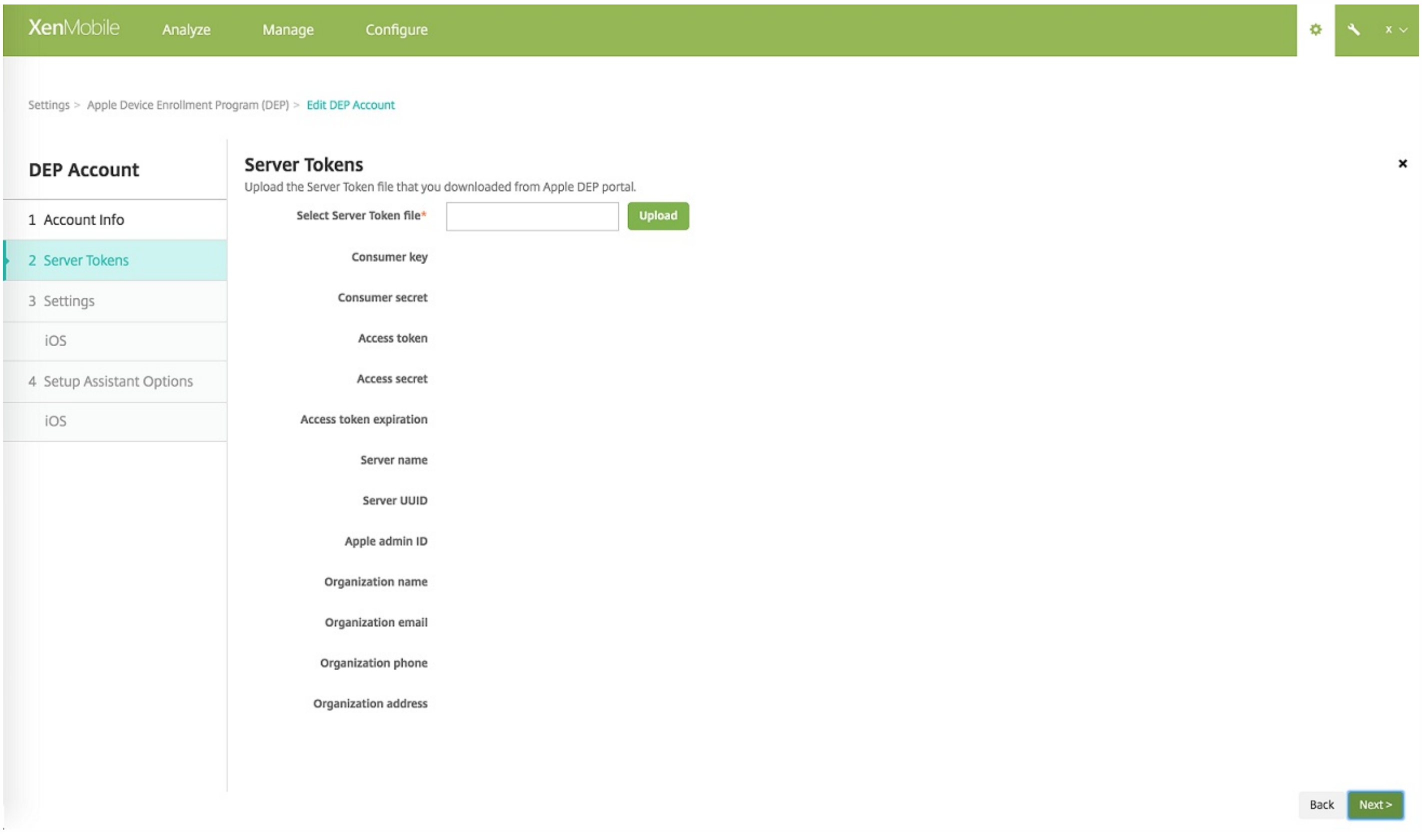
Account Info

Specify your Apple DEP account information.

DEP account name*	DEP Account US
Business unit*	CITRIX SYSTEMS US (dev.paris)
Unique service ID	Santa Clara Dev
Support phone number*	408 790 8000
Support email address	citrixxenmobilevpp@outlook.com

- **DEP account name**: A unique name for this DEP account. Use names that reflect how you organize DEP 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 may call for help during setup. This field is required.
- **Support email address**: An optional support email address available to end users.

3. In the **Server Tokens** page, specify your server token file and then click **Upload**.



Server Tokens

Upload the Server Token file that you downloaded from Apple DEP portal.

Select Server Token file*

Consumer key

Consumer secret

Access token

Access secret

Access token expiration

Server name

Server UUID

Apple admin ID

Organization name

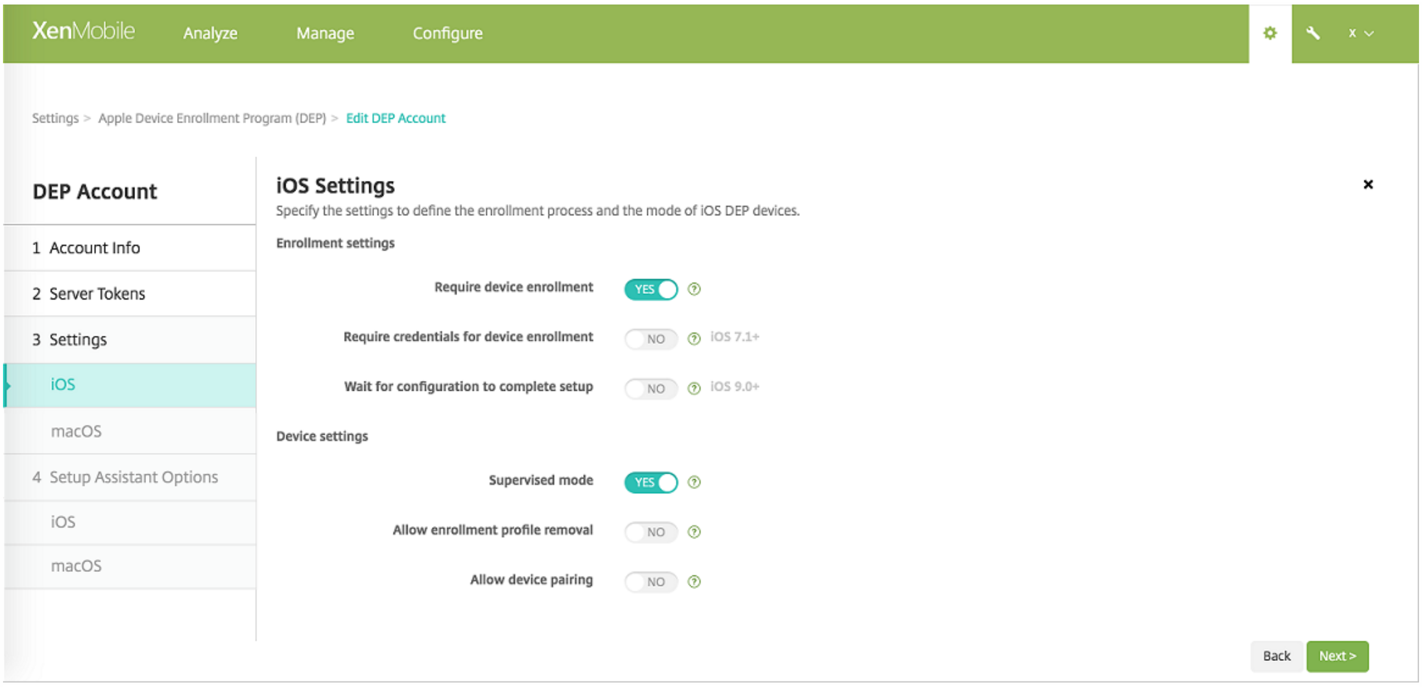
Organization email

Organization phone

Organization address

Your server token information appears.

4. In **iOS Settings**, specify these settings:



iOS Settings

Specify the settings to define the enrollment process and the mode of iOS DEP devices.

Enrollment settings

Require device enrollment: YES

Require credentials for device enrollment: NO (iOS 7.1+)

Wait for configuration to complete setup: NO (iOS 9.0+)

Device settings

Supervised mode: YES

Allow enrollment profile removal: NO

Allow device pairing: NO

Enrollment settings

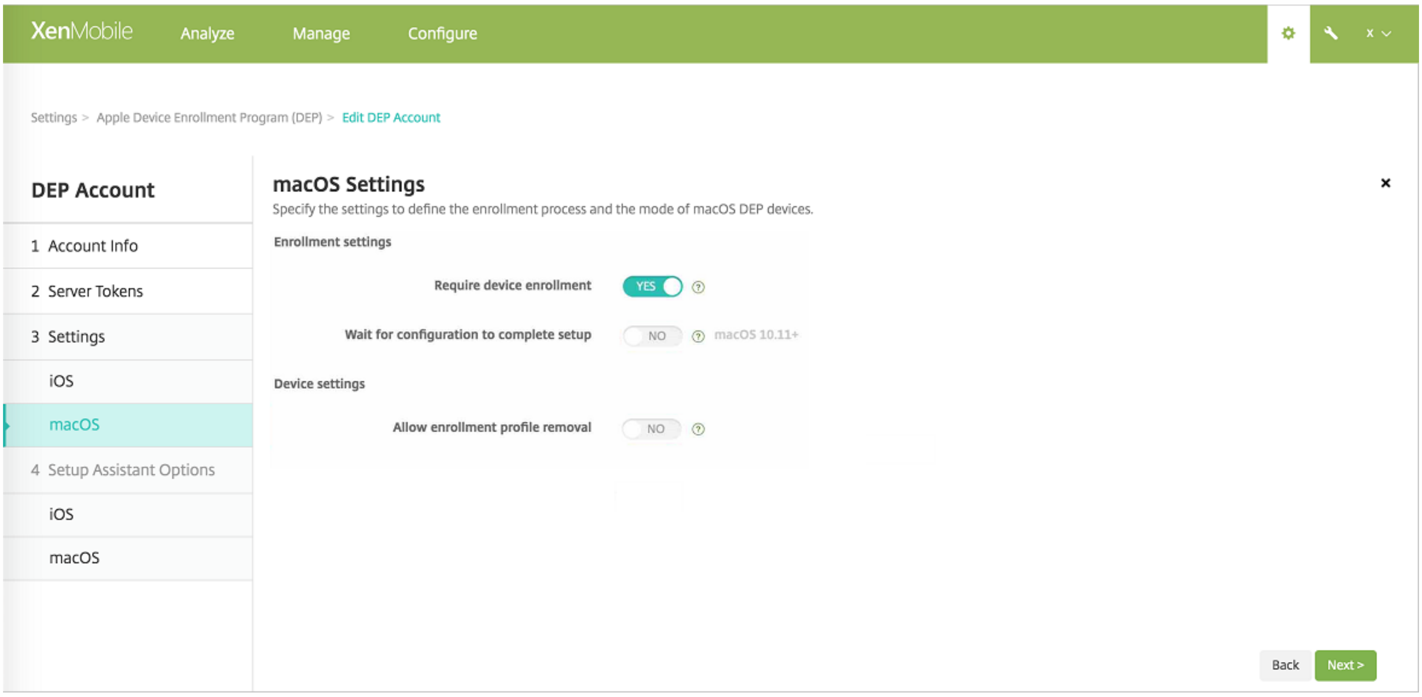
- **Require device enrollment**: Whether to require users to enroll their devices. The default is **Yes**.
- **Require credentials for device enrollment**: Whether to require users to enter their credentials during DEP set up. This feature is available for iOS 7.1 and higher. The default is **No**.
  Note: When DEP is on for the first time setup and you don't select this option, the DEP components, such as DEP user, Secure Hub, software inventory, and DEP deployment group, are created. If you do select this option, XenMobile doesn't create the components. As a result, if you later clear this option, users who have not entered their credentials cannot perform the DEP enrollment because these DEP components do not exist. To add DEP components, in that case, you should disable and enable the DEP 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 iOS 9.0 and higher 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 DEP 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 DEP, whether you can manage them through iTunes and the Apple

Configurator. The default is **No**.

5. In **macOS Settings**, specify these settings:



macOS Settings

Specify the settings to define the enrollment process and the mode of macOS DEP devices.

Enrollment settings

Require device enrollment: YES

Wait for configuration to complete setup: NO macOS 10.11+

Device settings

Allow enrollment profile removal: NO

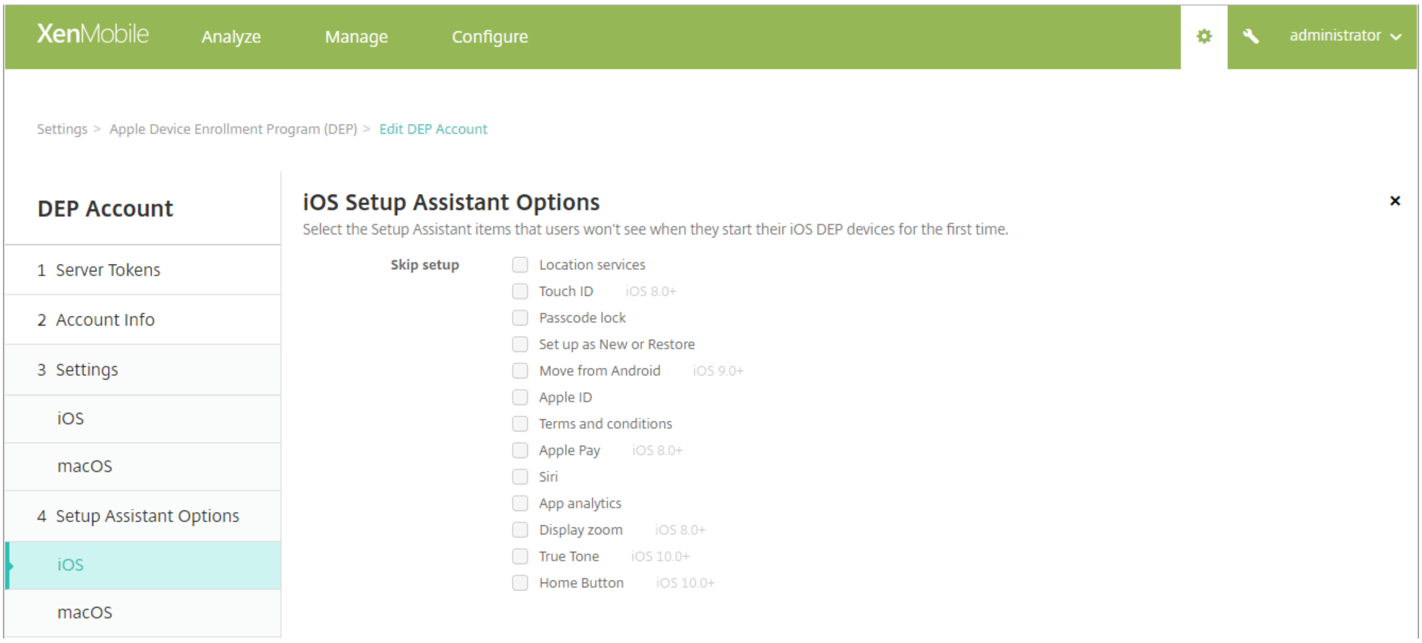
Enrollment settings

- **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 **iOS Setup Assistant Options**, select the iOS Setup Assistant steps that your users will not have to take (that is, steps that are skipped) when they start their devices the first time. The default for all items is unchecked.



iOS Setup Assistant Options

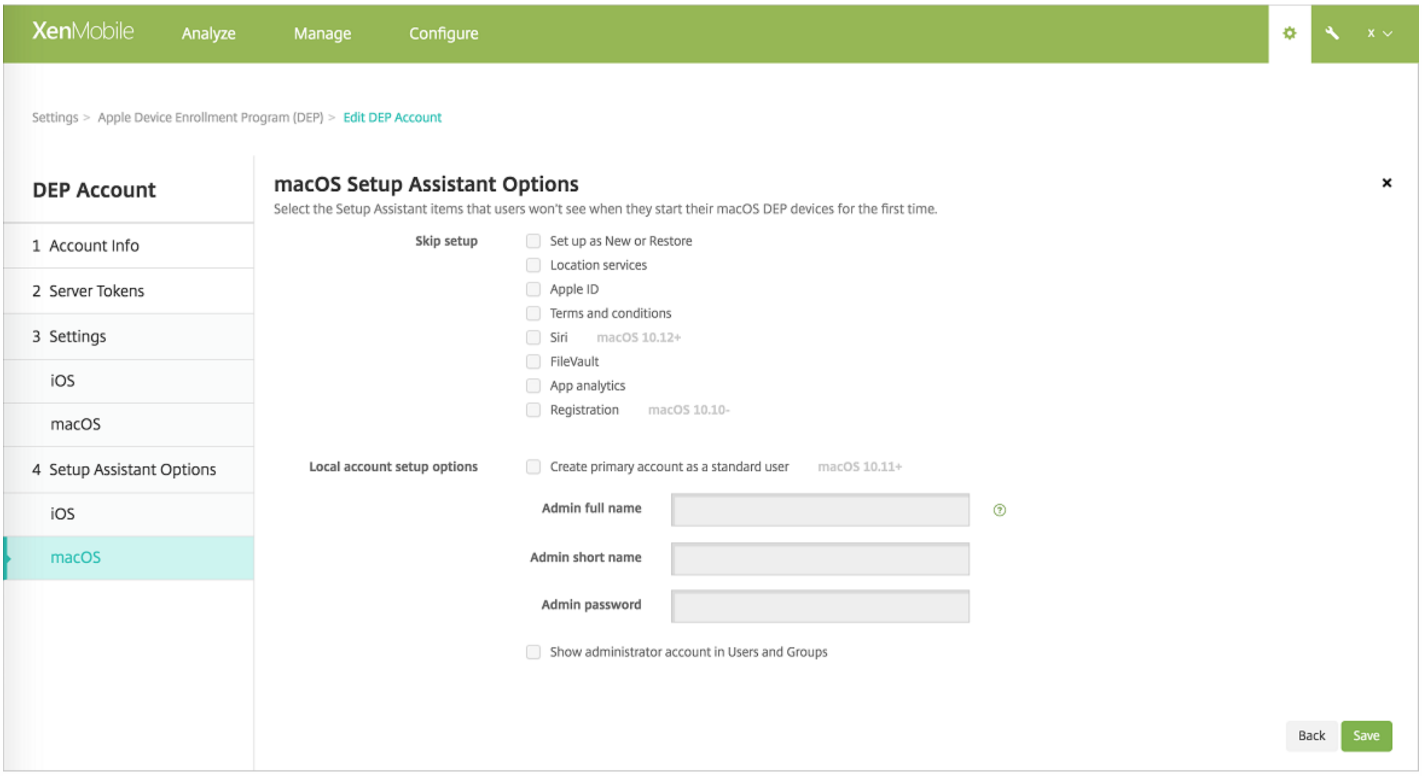
Select the Setup Assistant items that users won't see when they start their iOS DEP devices for the first time.

Skip setup
- ☐ Location services
- ☐ Touch ID iOS 8.0+
- ☐ Passcode lock
- ☐ Set up as New or Restore
- ☐ Move from Android iOS 9.0+
- ☐ Apple ID
- ☐ Terms and conditions
- ☐ Apple Pay iOS 8.0+
- ☐ Siri
- ☐ App analytics
- ☐ Display zoom iOS 8.0+
- ☐ True Tone iOS 10.0+
- ☐ Home Button iOS 10.0+

- **Location services**: Set up the location service on the device.
- **Touch ID**: Set up Touch ID on iOS 8.0 and later 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 9 or later 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 8.0 and later 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 8.0 or later devices.
- **True Tone**: Set up the True Tone Display on iOS 10.0 devices (minimum version).
- **Home Button**: Set up the Home Button screen sensitivity on iOS 10.0 devices (minimum version).

The DEP account appears on **Settings > Apple Device Enrollment Program (DEP)**.

7. In **macOS Setup Assistant Options**, select the macOS Setup Assistant steps that your users will not have to take (that is, steps that are skipped) when they start their devices the first time. The default for all items is unchecked.



Settings > Apple Device Enrollment Program (DEP) > Edit DEP Account

DEP Account

1 Account Info
2 Server Tokens
3 Settings
iOS
macOS
4 Setup Assistant Options
iOS
macOS

macOS Setup Assistant Options

Select the Setup Assistant items that users won't see when they start their macOS DEP devices for the first time.

Skip setup
□ Set up as New or Restore
□ Location services
□ Apple ID
□ Terms and conditions
□ Siri macOS 10.12+
□ FileVault
□ App analytics
□ Registration macOS 10.10-

Local account setup options
□ Create primary account as a standard user macOS 10.11+

Admin full name

Admin short name

Admin password

□ Show administrator account in Users and Groups

- **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. XenMobile applies the FileVault setting only if the system has a single local user account and that account is signed into iCloud.

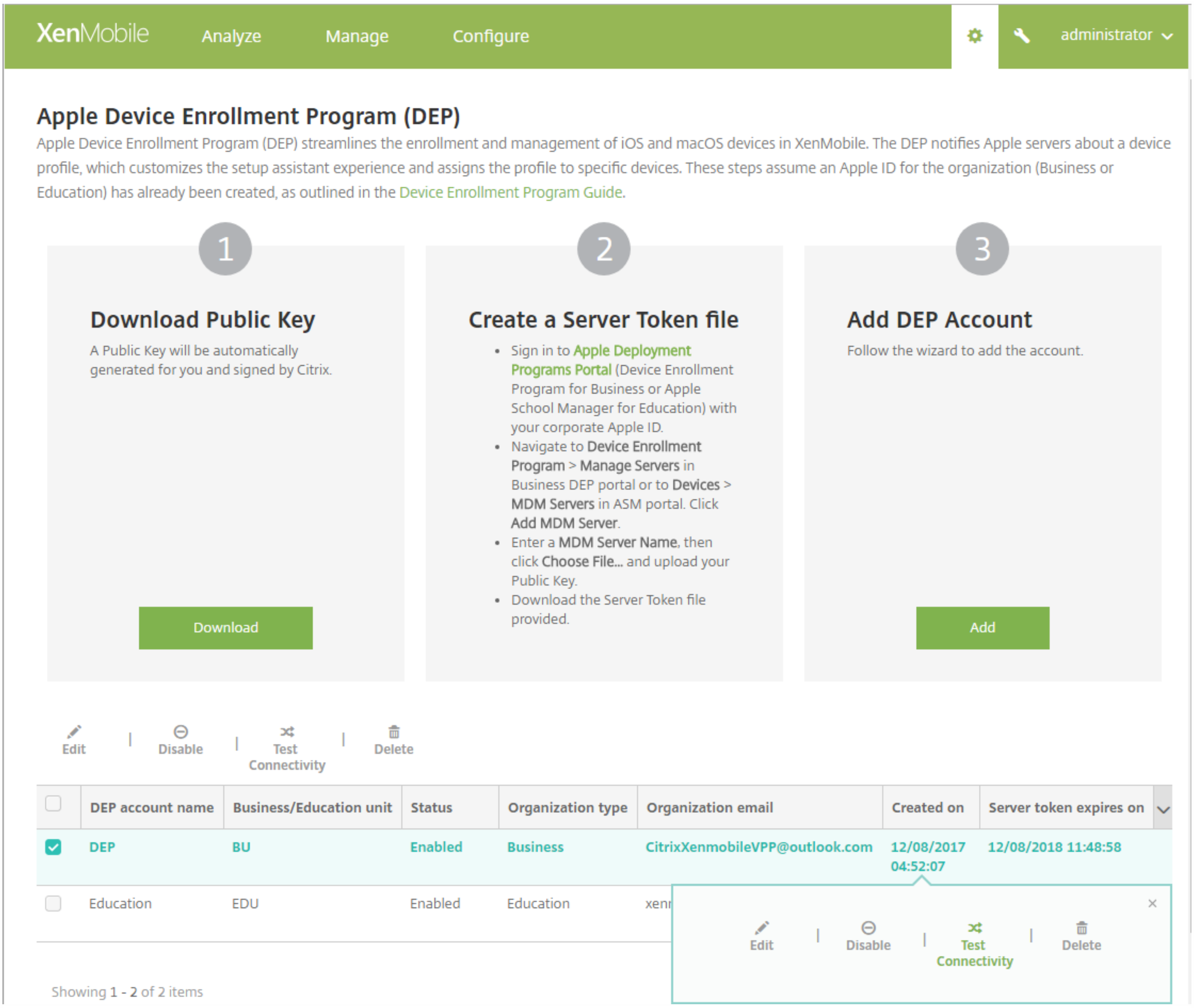
  Note: You can use the macOS FileVault Disk Encryption feature to protect the system volume by encrypting its contents (https://support.apple.com/en-us/HT204837). If you run the Setup assistant on a late-model portable Mac that doesn't have FileVault turned on, you might be prompted to turn on this feature. 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. XenMobile creates the account, using the specified information.

8. To test connectivity between XenMobile and Apple, select the account and click **Test Connectivity**.



Apple Device Enrollment Program (DEP)

Apple Device Enrollment Program (DEP) streamlines the enrollment and management of iOS and macOS devices in XenMobile. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. These steps assume an Apple ID for the organization (Business or Education) has already been created, as outlined in the Device Enrollment Program Guide.

1 Download Public Key

A Public Key will be automatically generated for you and signed by Citrix.

Download

2 Create a Server Token file

- Sign in to Apple Deployment Programs Portal (Device Enrollment Program for Business or Apple School Manager for Education) with your corporate Apple ID.
- Navigate to Device Enrollment Program > Manage Servers in Business DEP portal or to Devices > MDM Servers in ASM portal. Click Add MDM Server.
- Enter a MDM Server Name, then click Choose File... and upload your Public Key.
- Download the Server Token file provided.

3 Add DEP Account

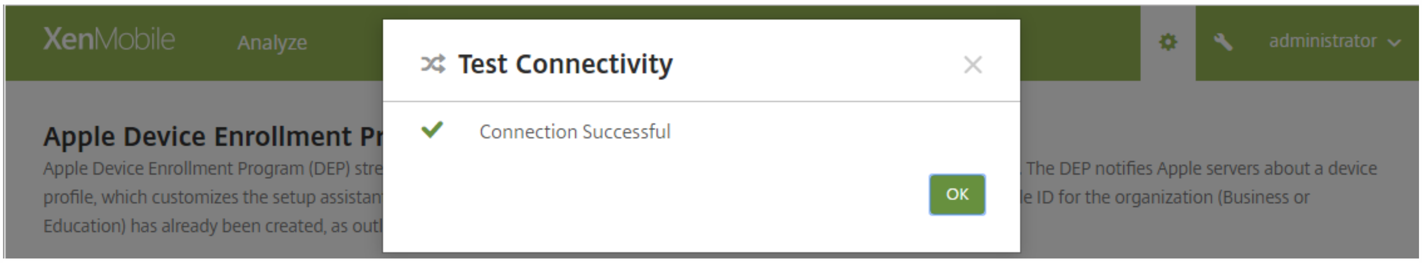
Follow the wizard to add the account.

Add

☐	DEP account name	Business/Education unit	Status	Organization type	Organization email	Created on	Server token expires on
☑	DEP	BU	Enabled	Business	CitrixXenmobileVPP@outlook.com	12/08/2017 04:52:07	12/08/2018 11:48:58
☐	Education	EDU	Enabled	Education	xenr		

Showing 1 - 2 of 2 items

A status message appears.



Test Connectivity

✓ Connection Successful

OK

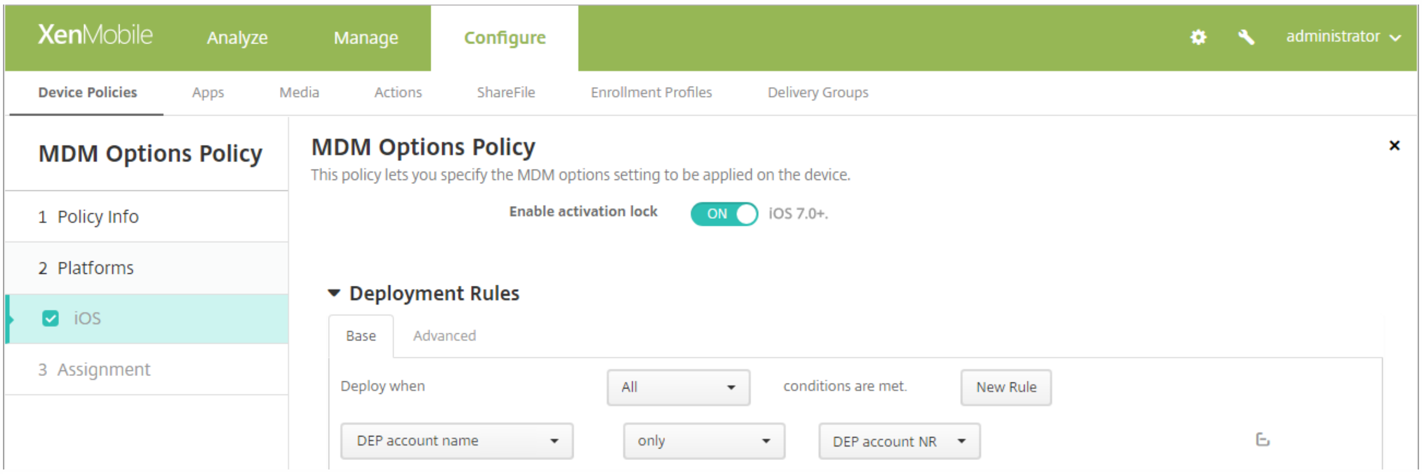
Configure deployment rules of device policies and apps for DEP accounts

You can associate DEP 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 Apple DEP account.
- Deploys for all Apple DEP accounts except the one selected.

The list of DEP accounts includes only those accounts with a status of enabled or disabled. If the DEP account is disabled, the DEP device doesn't belong to this account. Therefore, XenMobile doesn't deploy the app or policy to the device.

In the following example, a device policy deploys only for devices with the Apple DEP account name "DEP Account NR".



MDM Options Policy

This policy lets you specify the MDM options setting to be applied on the device.

Enable activation lock: ON iOS 7.0+.

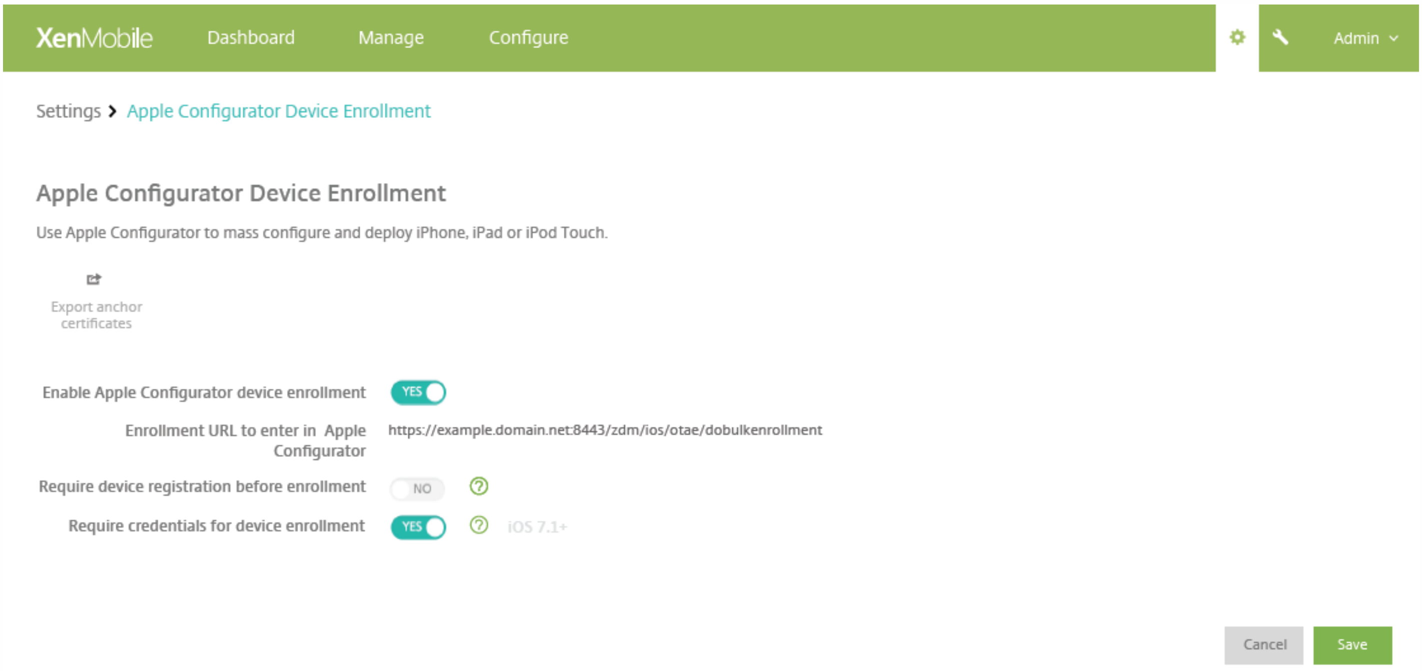
Deployment Rules

Deploy when All conditions are met.

DEP account name | only | DEP account NR

Configure Apple Configurator settings

1. In the XenMobile console, go to **Settings > Apple Configurator Device Enrollment**.


XenMobile
Dashboard
Manage
Configure
Admin
Settings > Apple Configurator Device Enrollment
Export anchor certificates
Cancel
Save

Apple Configurator Device Enrollment

Use Apple Configurator to mass configure and deploy iPhone, iPad or iPod Touch.

Enable Apple Configurator device enrollment: YES

Enrollment URL to enter in Apple Configurator: https://example.domain.net:8443/zdm/ios/otae/dobulkenrollment

Require device registration before enrollment: NO

Require credentials for device enrollment: YES iOS 7.1+

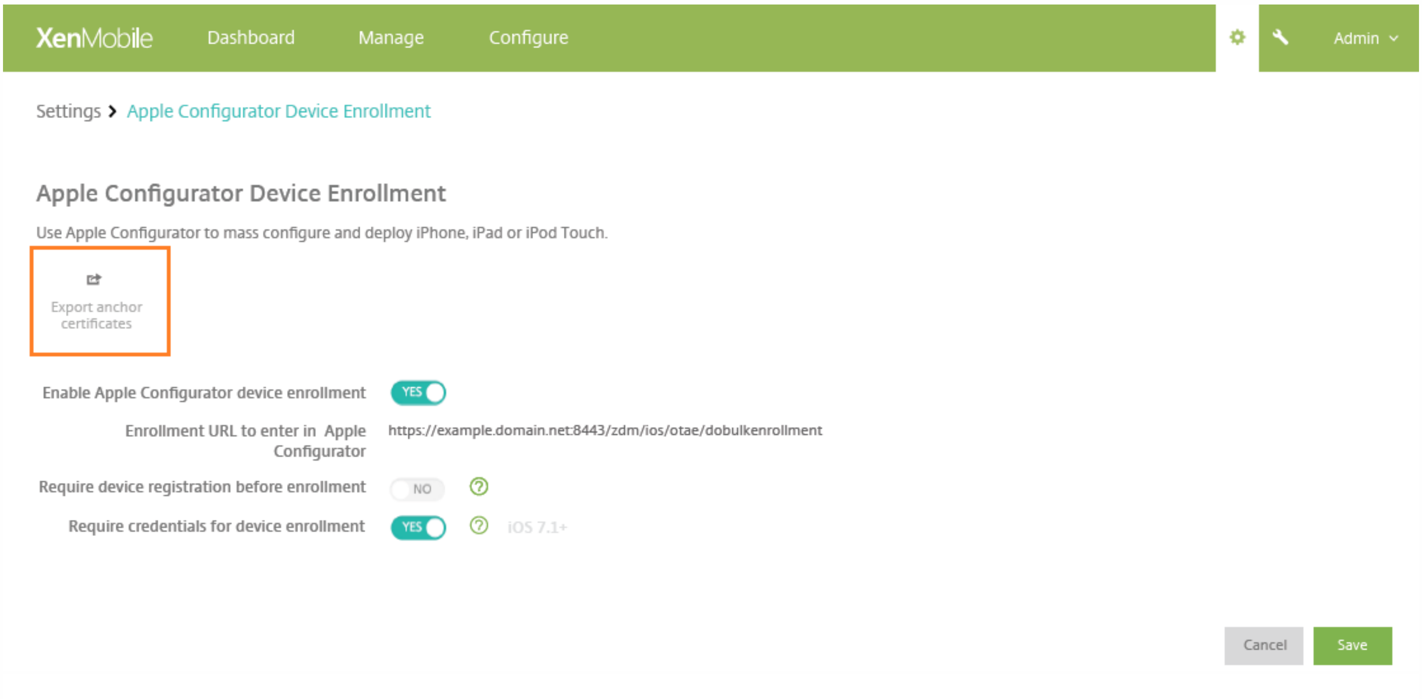
2. Set **Enable Apple Configurator device enrollment** to **Yes**.

3. The **Enrollment URL to enter in Apple Configurator** is a read-only field. This is the URL for the XenMobile 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 XenMobile 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 XenMobile manually or through a CSV file before before enrollment.

5. To require users of iOS 7.1 and later 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 XenMobile 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).


XenMobile
Dashboard
Manage
Configure
Admin
Settings > Apple Configurator Device Enrollment
Export anchor certificates
Cancel
Save

Apple Configurator Device Enrollment

Use Apple Configurator to mass configure and deploy iPhone, iPad or iPod Touch.

Enable Apple Configurator device enrollment: YES

Enrollment URL to enter in Apple Configurator: https://example.domain.net:8443/zdm/ios/otae/dobulkenrollment

Require device registration before enrollment: NO

Require credentials for device enrollment: YES iOS 7.1+

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 XenMobile 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.

To renew or update certificates when using the Apple DEP

When the XenMobile Secure Sockets Layer (SSL) certificate is renewed, you upload a new certificate in the XenMobile 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, XenMobile uses the new SSL certificate. For more information about certificates in XenMobile, see Uploading Certificates in XenMobile.

It is not necessary to reestablish the trust relationship between Apple DEP and XenMobile 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 DEP, see the Apple documentation.

To place an iOS device in Supervised mode by using the Apple Configurator

> **Important**
>
> Placing a device into Supervised mode will install the selected version of iOS on the device, completely wiping the device of any previously stored user data or apps.

1. Install Apple Configurator from iTunes.

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:

a. 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.

b. Optionally, provide a name for the device.

c. 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**.

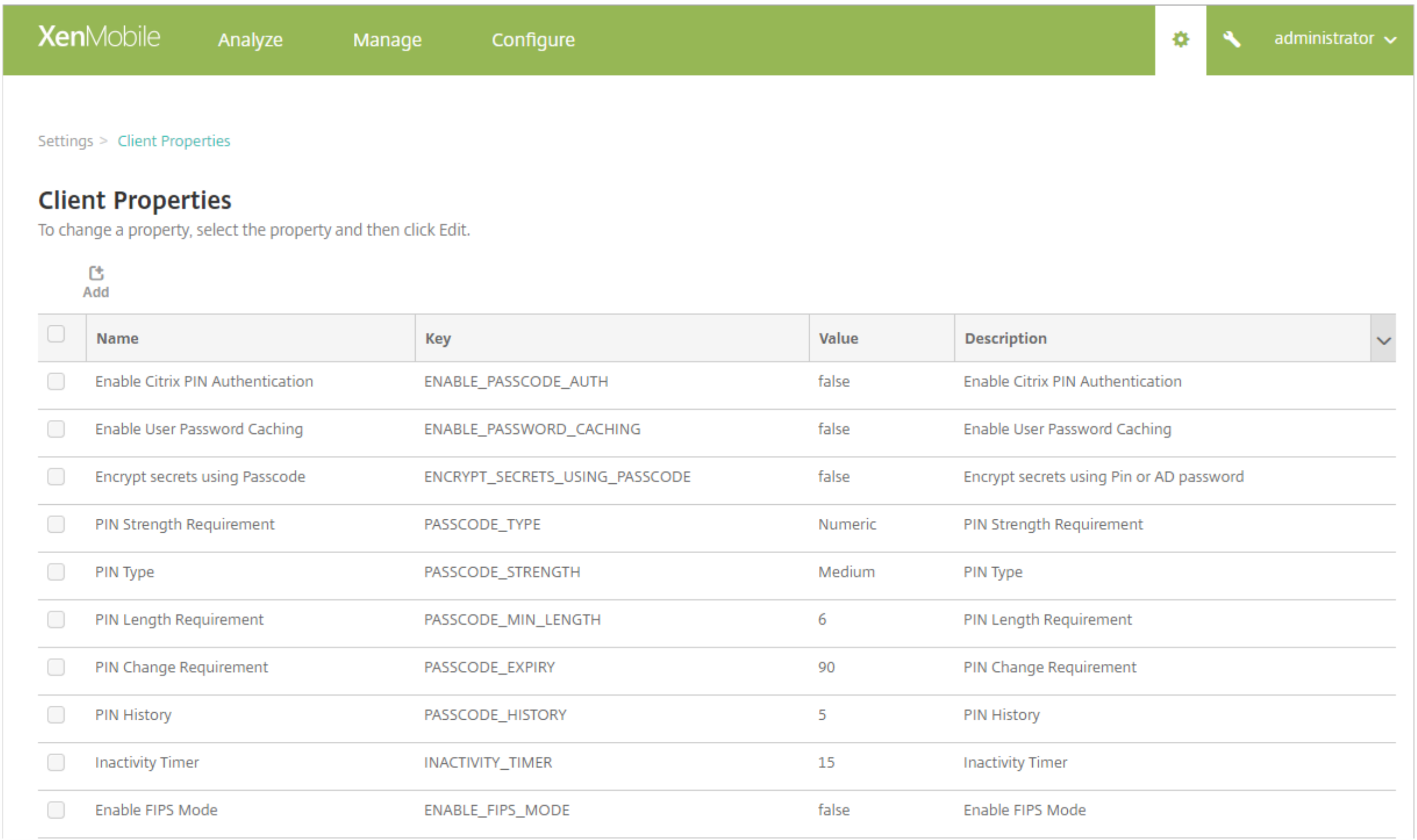
Client properties

Dec 28, 2017

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 occassionally for client apps. For details about more commonly configured client properties, see Client property reference, later in this article.

1. In the XenMobile 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.



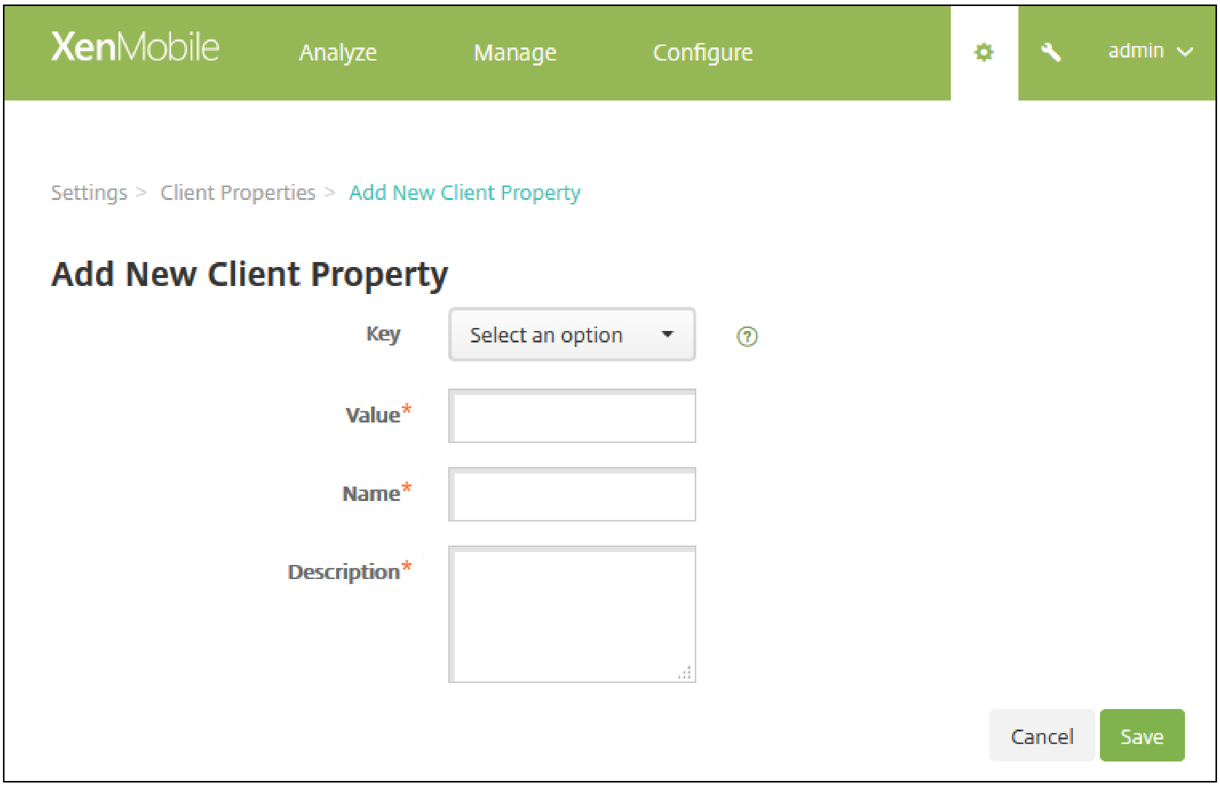
Client Properties

To change a property, select the property and then click Edit.

□	Name	Key	Value	Description
□	Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication
□	Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
□	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
□	PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
□	PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
□	PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement
□	PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
□	PIN History	PASSCODE_HISTORY	5	PIN History
□	Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
□	Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

To add a client property

1. Click **Add**. The **Add New Client Property** page appears.



Settings > Client Properties > Add New Client Property

Add New Client Property

Key: Select an option

Value*

Name*

Description*

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.

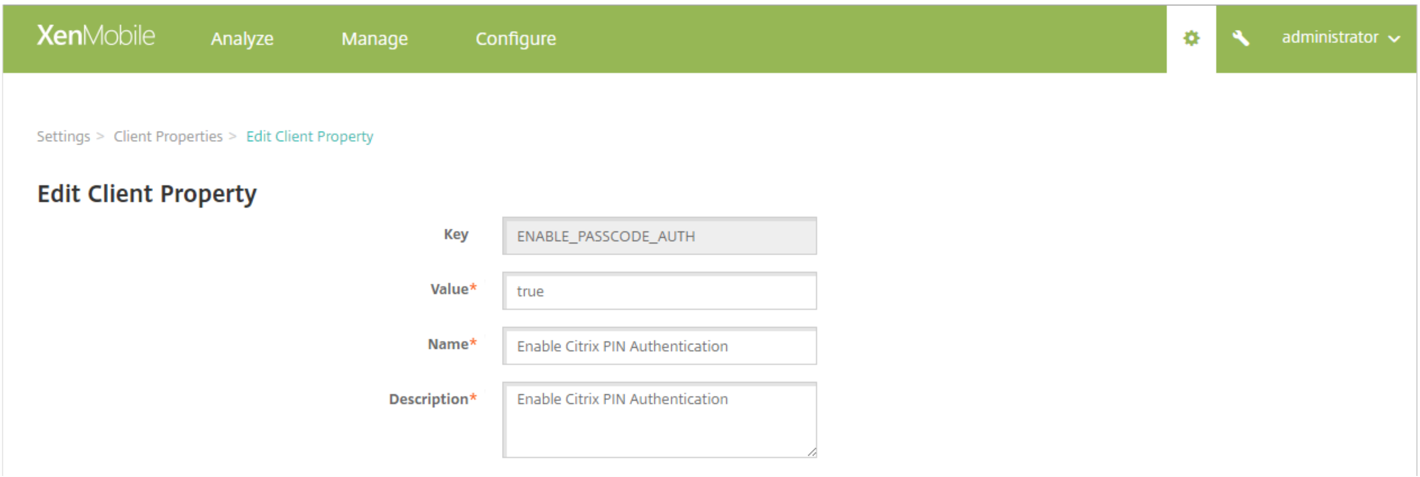
3. Click **Save**.

To edit a client property

1. In the **Client Properties** table, select the client property you want to edit.

Note: 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.



Settings > Client Properties > Edit Client Property

Edit Client Property

Key: ENABLE_PASSCODE_AUTH

Value*: true

Name*: Enable Citrix PIN Authentication

Description*: Enable Citrix PIN Authentication

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.

> **Note**: 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 XenMobile 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 XenMobile 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 XenMobile 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. XenMobile 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, XenMobile 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_FIPS_MODE:

- Display name: Enable FIPS Mode
- This property enables or disables FIPS mode on mobile devices. After you change the value, Secure Hub passes the new value to the device when Secure Hub does the next online authentication.
- Possible values: **true** or **false**
- Default value: **false**

ENABLE_NETWORK_EXTENSION:

- Display name: ENABLE_NETWORK_EXTENSION
- By default, XenMobile enables the Apple Network Extension framework when Secure Hub installs. To disable Network Extension, go to **Settings > Client Properties**, add the custom key **ENABLE_NETWORK_EXTENSION**, and set the **Value** to **false**.
- Default value: **true**

ENABLE_PASSCODE_AUTH:

- Display name: Enable Citrix PIN Authentication
- This property allows you to turn on Citrix PIN functionality. With the Citrix PIN or passcode, users are prompted to define a PIN to use instead of their Active Directory password. This setting is automatically enabled when ENABLE_PASSWORD_CACHING is enabled or when XenMobile 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 XenMobile.

  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, XenMobile 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, XenMobile 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 XenMobile.
- 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.

  Note: 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: **1** through **99**
- 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:

Passcode strength	**Rules for numeric passcode type**	**Allowed**	**Not allowed**
Low	All numbers, any sequence allowed	444444, 123456, 654321	
Medium (default setting)	All numbers cannot be the same or consecutive.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321

High	Same as for the Medium Passcode strength.		
Strong	Same as for the Medium Passcode strength.		

Rules for alphanumeric passcodes:

Passcode strength	**Rules for alphanumeric passcode type**	**Allowed**	**Not allowed**
Low	Must contain at least one number and one letter	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef
Medium (default setting)	In addition to the rules for Low passcode strength, letters and all numbers cannot be the same. Letters cannot be consecutive and numbers cannot be consecutive.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, or aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, or cba123
High	Include at least one capital letter and one small letter.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Strong	Include at least one number, one special symbol, one capital letter, and one small letter.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

PASSCODE_TYPE:

- Display name: PIN Type
- This property defines whether users are able to define a numerical Citrix PIN or an alphanumeric passcode. When you select **Numeric**, users can use numbers only (Citrix PIN). When you select **Alphanumeric**, users can use a combination of letters and numbers (passcode).

  Note: If you change this setting, users must set a new Citrix PIN or passcode the next time that they are prompted to authenticate.

- Possible values: **Numeric** or **Alphanumeric**
- Default value: **Numeric**

REFRESHINTERVAL:

- Display name: REFRESHINTERVAL
- By default, XenMobile pings the Auto Discovery Server (ADS) for pinned certificates every 3 days. To change the refresh interval, go to **Settings > Client Properties**, add the custom key **REFRESHINTERVAL**, and set the **Value** to the number of hours.
- Default value: **72** hours (3 days)

SEND_LDAP_ATTRIBUTES:

- For MAM-only deployments of Android, iOS, or macOS devices: You can configure XenMobile 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.
- To configure this global client policy, go to **Settings > Client Properties**, add the custom key **SEND_LDAP_ATTRIBUTES**, and set the **Value** as follows.
- Value: userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}
- The attribute values are specified as macros, similar to MDM policies.
- Here is a sample account service response for this property:

  <property value="userPrincipalName=eng1@xmslab.com,sAMAccountName=eng1,displayName=eng1\, test1,email=eng1@xmslab.com\,eng1@xmslab.com" name="SEND_LDAP_ATTRIBUTES"/>
- Note: For this property, XenMobile 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 XenMobile 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_EXCLUDE_DOMAINS**, 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:

  app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream,launchdarkly.com, crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net,mobile.launchdarkly.com, pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com

Deploy iOS and macOS devices through Apple DEP

Sep 06, 2017

Apple has device enrollment programs for business and education accounts. For business accounts, you enroll in the Apple Deployment Program to use the Apple Device Enrollment Program (DEP) for device enrollment and management in XenMobile. That program is for iOS and macOS devices. For information about signing up for a business Apple Deployment Program account, see this PDF from Apple.

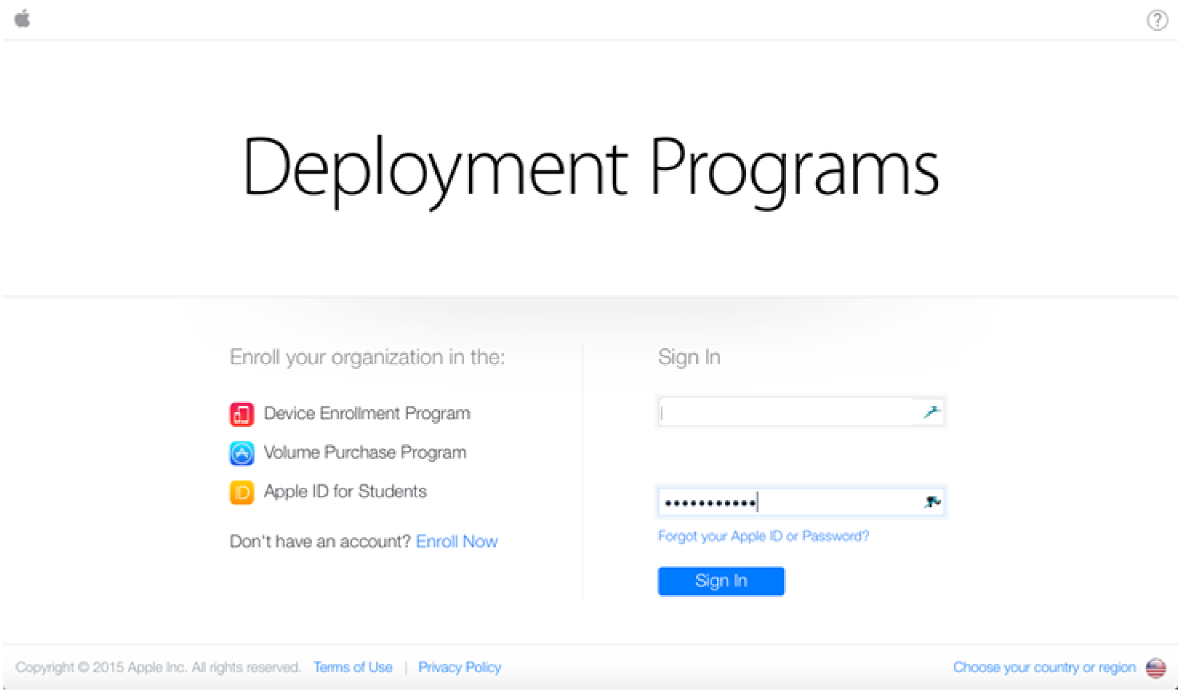
Be aware that the Apple Deployment Program is available for organizations and not individuals. You must provide a considerable amount of corporate details and information to create an Apple Deployment Program account. Thus, it could take time to request and receive approval for accounts.

For education accounts, you create an Apple School Manager account. Apple School Manager unifies the Device Enrollment Program (DEP) and Volume Purchase Program (VPP). Apple School Manager is a type of Education DEP. To create an Apple School Manager account, go to https://school.apple.com/.

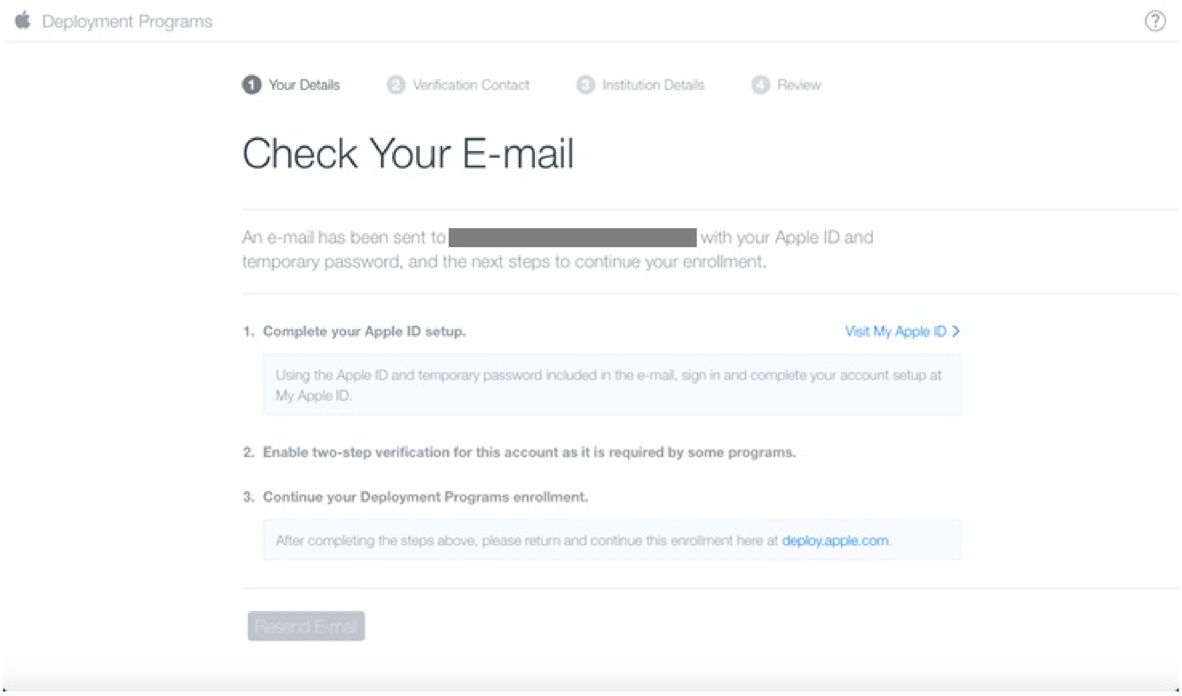
Enroll in the Apple Deployment Program

1. Go to deploy.apple.com to apply for an Apple Deployment Program account. When applying for a DEP account, the best practice is to use an email address for the organization, such as dep@company.com.

Note: For education accounts, go to https://school.apple.com/.


Deployment Programs
Enroll your organization in the:
Device Enrollment Program
Volume Purchase Program
Apple ID for Students
Don't have an account? Enroll Now
Sign In
••••••••••••
Forgot your Apple ID or Password?
Sign In
Copyright © 2015 Apple Inc. All rights reserved.
Terms of Use
Privacy Policy
Choose your country or region

2. After you type your organization information, Apple emails you a temporary password for the new Apple ID.



Check Your E-mail

An e-mail has been sent to [redacted] with your Apple ID and temporary password, and the next steps to continue your enrollment.

1. Complete your Apple ID setup. Visit My Apple ID >

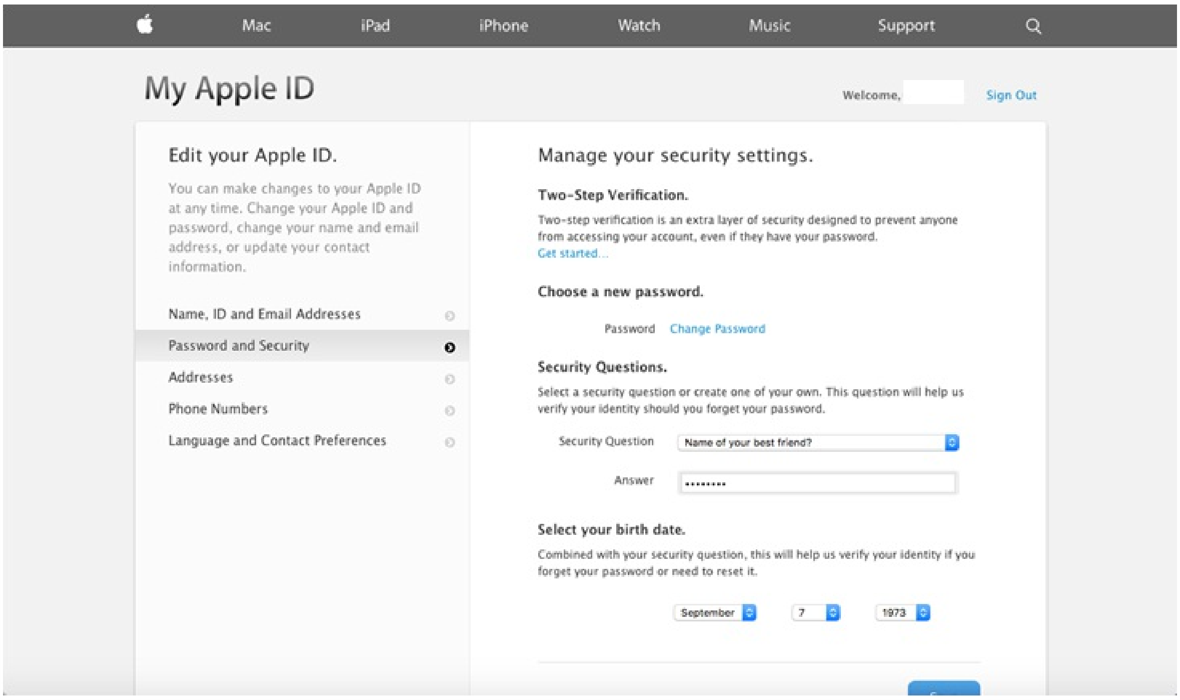
Using the Apple ID and temporary password included in the e-mail, sign in and complete your account setup at My Apple ID.

2. Enable two-step verification for this account as it is required by some programs.

3. Continue your Deployment Programs enrollment.

After completing the steps above, please return and continue this enrollment here at deploy.apple.com.

3. You then sign in with your Apple ID and complete the security settings for the account.



My Apple ID

Welcome, Sign Out

Edit your Apple ID.

You can make changes to your Apple ID at any time. Change your Apple ID and password, change your name and email address, or update your contact information.

Name, ID and Email Addresses
Password and Security
Addresses
Phone Numbers
Language and Contact Preferences

Manage your security settings.

Two-Step Verification.

Two-step verification is an extra layer of security designed to prevent anyone from accessing your account, even if they have your password.
Get started...

Choose a new password.

Password Change Password

Security Questions.

Select a security question or create one of your own. This question will help us verify your identity should you forget your password.

Security Question: Name of your best friend?

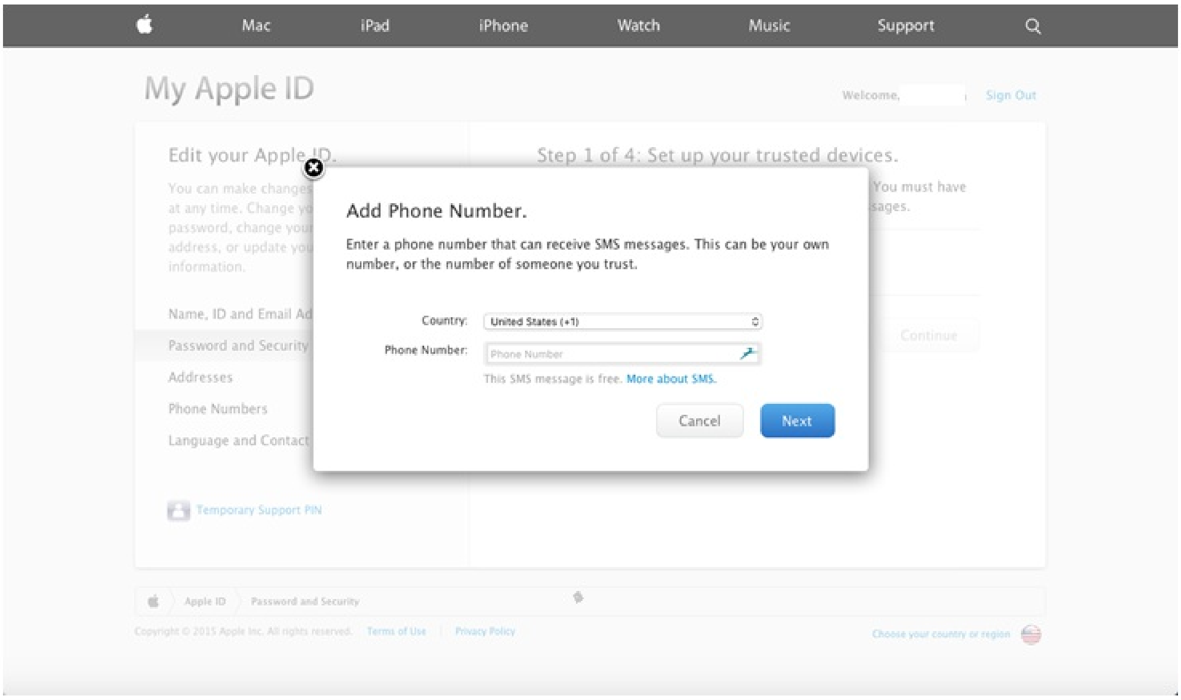
Answer: ••••••••

Select your birth date.

Combined with your security question, this will help us verify your identity if you forget your password or need to reset it.

September 7 1973

4. Configure and enable two-step verification, which is required for use with the DEP Portal. During these steps, after you add a phone number, you receive the 4-digit PIN for the two-step verification.



My Apple ID

Welcome,

Edit your Apple ID.

You can make changes at any time. Change yo password, change you address, or update yo information.

Step 1 of 4: Set up your trusted devices.

You must have sages.

Add Phone Number.

Enter a phone number that can receive SMS messages. This can be your own number, or the number of someone you trust.

Country: United States (+1)

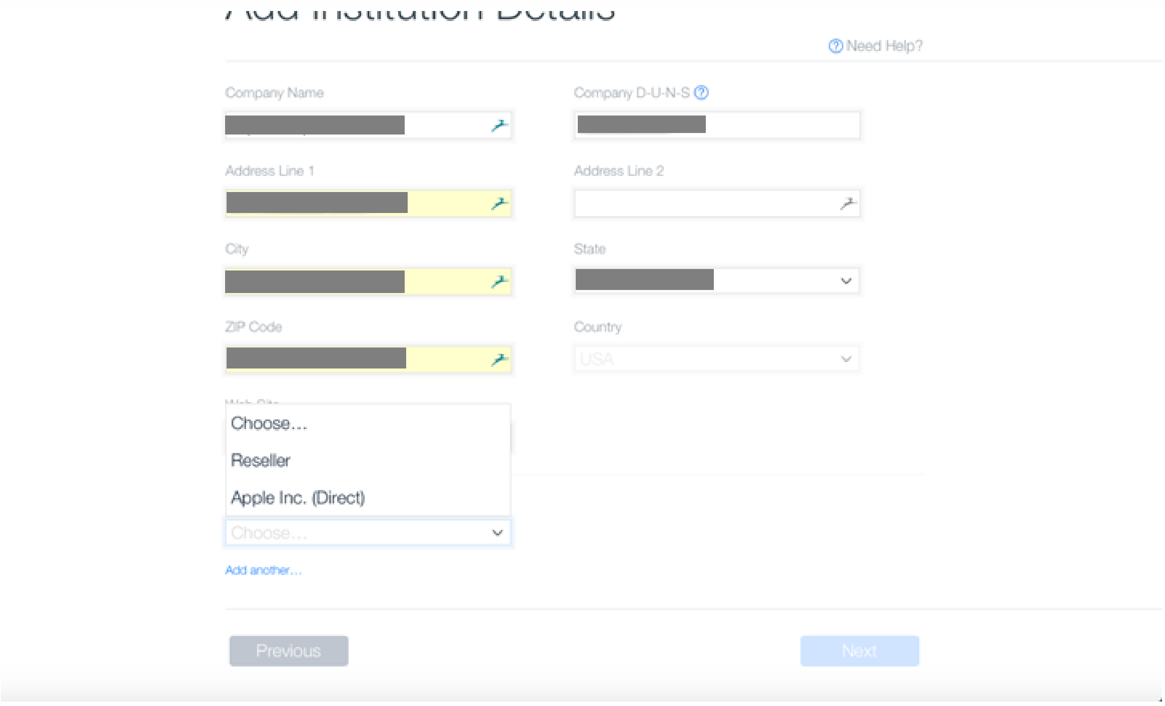
Phone Number: Phone Number

This SMS message is free. More about SMS.

Copyright © 2015 Apple Inc. All rights reserved.

5. Log in to the DEP Portal to complete the account configuration using the two-step verification that you set up.

6. Add your company details and then select from where you purchase devices. For details on purchasing options, see the next section, Ordering DEP-enabled devices.



Company Name: [redacted]

Company D-U-N-S: [redacted]

Address Line 1: [redacted]

Address Line 2:

City: [redacted]

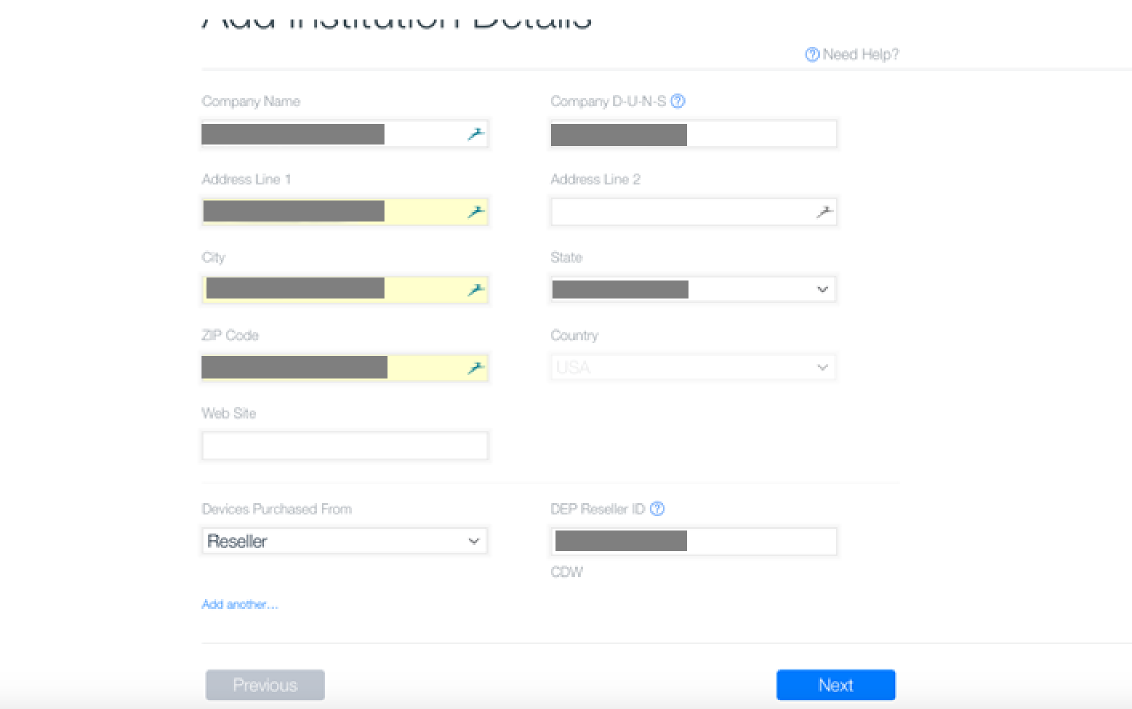
State: [redacted]

ZIP Code: [redacted]

Country: USA

Web Site

7. Add the Apple Customer Number or the DEP Reseller ID. Then verify your enrollment details and wait for Apple to approve your account.



Add Institution Details

Company Name: [redacted]

Company D-U-N-S: [redacted]

Address Line 1: [redacted]

Address Line 2:

City: [redacted]

State: [redacted]

ZIP Code: [redacted]

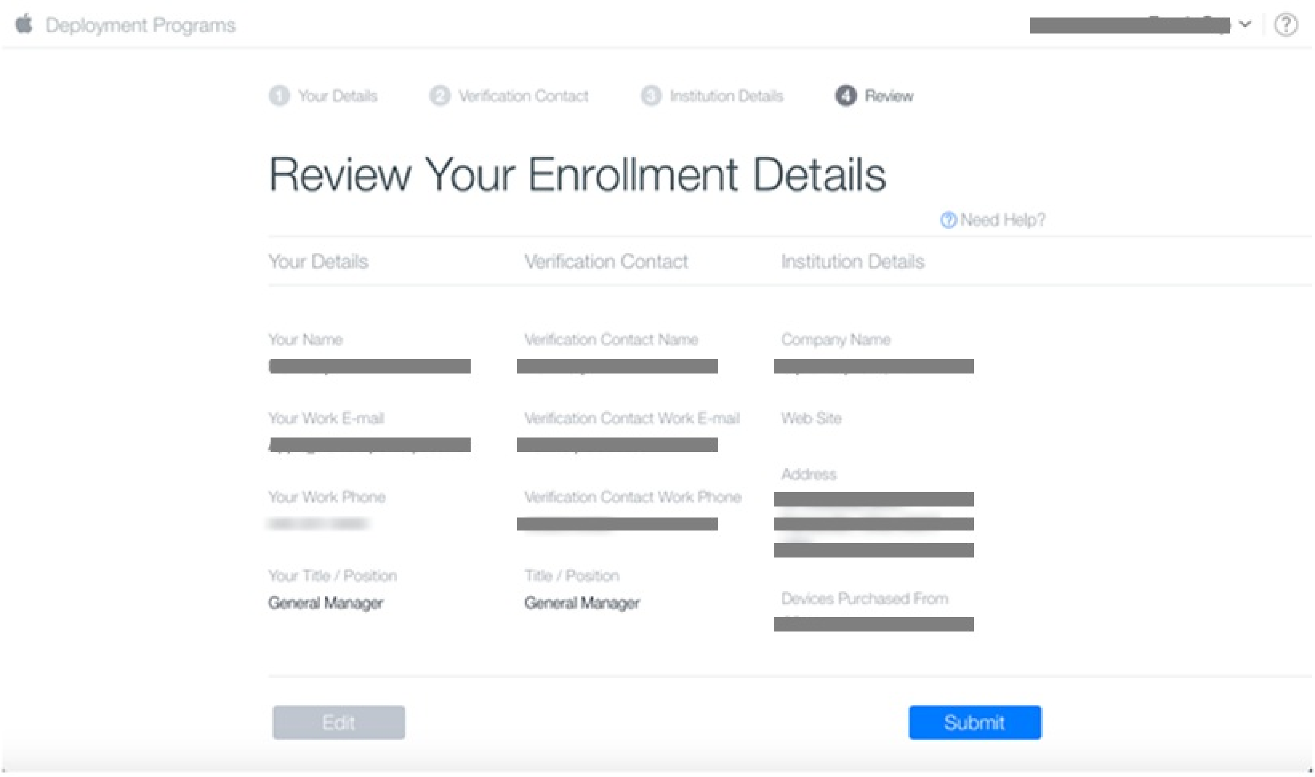
Country: USA

Web Site:

Devices Purchased From: Reseller

DEP Reseller ID: [redacted]

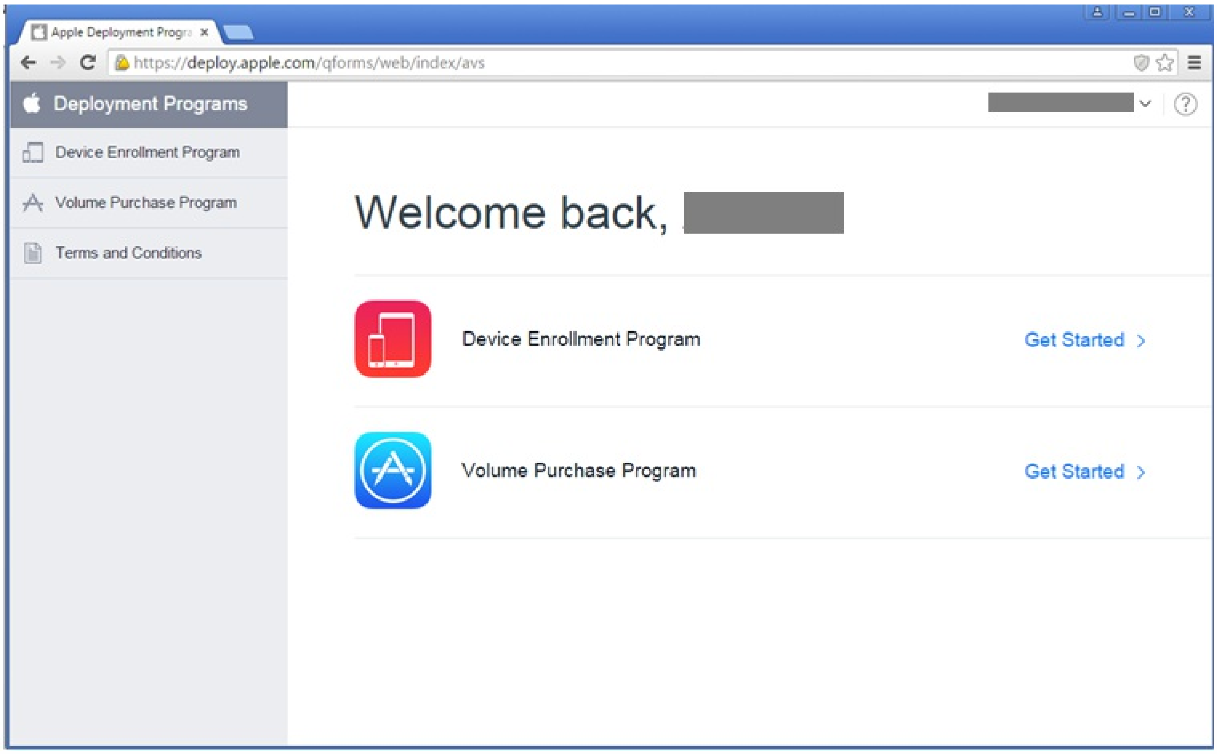
CDW



Review Your Enrollment Details

Your Details	Verification Contact	Institution Details
Your Name [redacted]	Verification Contact Name [redacted]	Company Name [redacted]
Your Work E-mail [redacted]	Verification Contact Work E-mail [redacted]	Web Site
Your Work Phone [redacted]	Verification Contact Work Phone [redacted]	Address [redacted]
Your Title / Position General Manager	Title / Position General Manager	Devices Purchased From [redacted]

8. After you receive your logon credentials from Apple, log in to the Apple DEP Portal.



To connect your account to XenMobile, see "Integrate your Apple DEP account with XenMobile" in Bulk enrollment of iOS and macOS devices.

Order DEP-enabled devices

You can order DEP-enabled devices directly from Apple or DEP-enabled authorized resellers or carriers. To order from Apple, provide your Apple Customer ID in the Apple DEP Portal. Your Customer ID enables Apple to associate your purchased devices with your Apple DEP account.

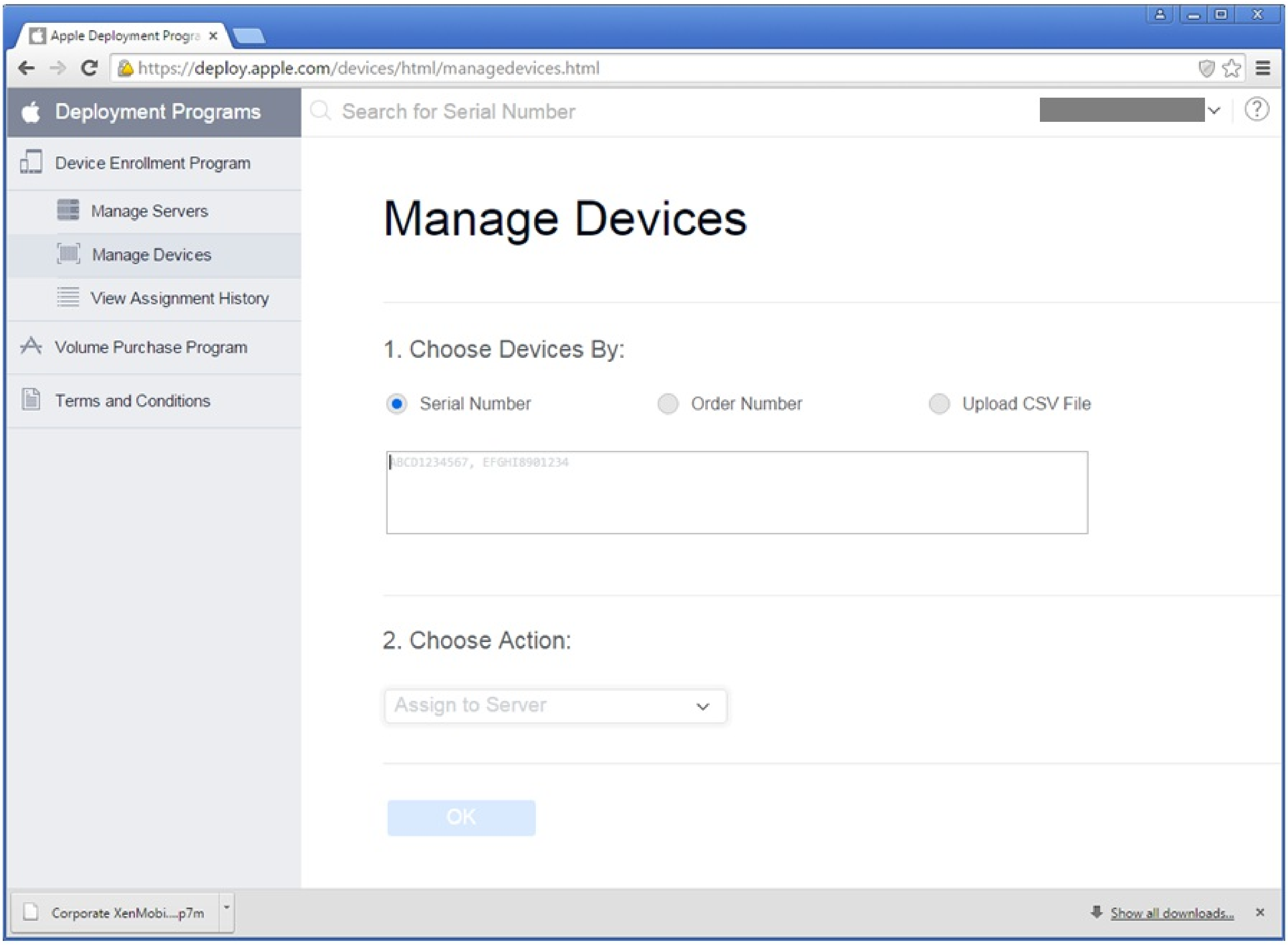
To order from your reseller or carrier, contact your Apple reseller or carrier to check if they participate in the Apple DEP. Ask for the Apple DEP ID of the reseller when purchasing devices. Apple requires that information when you add your Apple DEP reseller to your Apple DEP account. After you add the Apple DEP ID for the reseller, you receive a DEP customer ID. Provide the DEP customer ID to the reseller, who uses the ID to submit information about your device purchases to Apple. For more information, see this Apple website.

Manage DEP-enabled devices

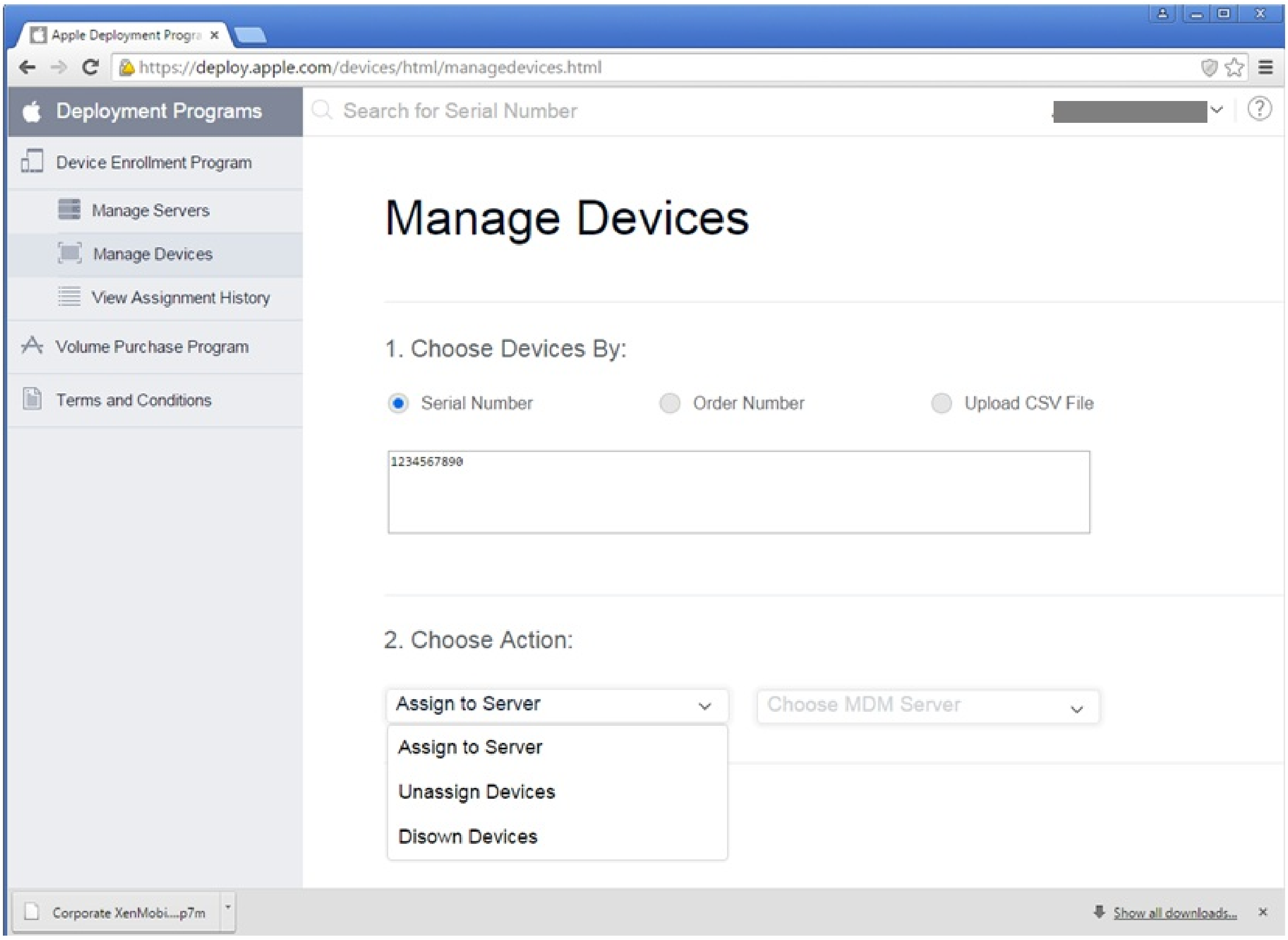
Follow these steps to associate devices with your XenMobile Server by using the DEP Portal to update your Apple DEP account.

1. Log on to the Apple DEP Portal.

2. Click **Device Enrollment Program** and then click **Manage Devices**. In **Choose Devices By**, choose the option for which you want to upload and define your Apple DEP-enabled devices: **Serial Number**, **Order Number**, or **Upload CSV File**.



3. To assign your devices to a XenMobile Server, under **Choose Action**, choose **Assign to Server**. Then, in the list, choose the name of your XenMobile Server. Click **OK**.



Manage Devices

1. Choose Devices By:

● Serial Number ○ Order Number ○ Upload CSV File

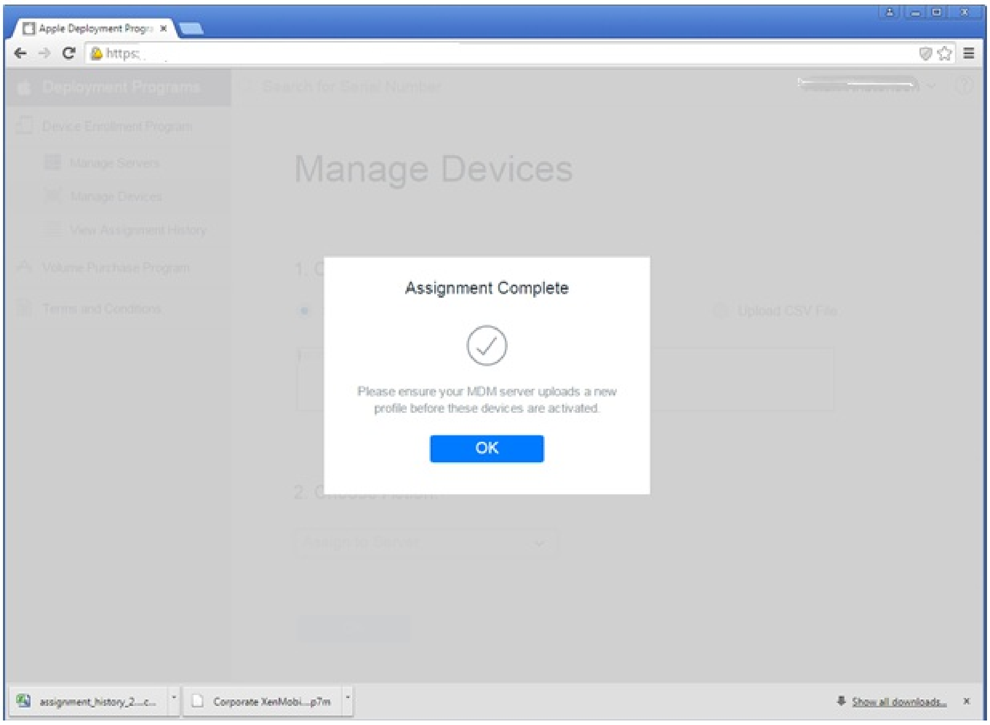
1234567890

2. Choose Action:

Assign to Server

Choose MDM Server

Your Apple DEP devices are now associated with the selected XenMobile Server.



Assignment Complete

Please ensure your MDM server uploads a new profile before these devices are activated.

OK

User experience when enrolling an Apple DEP-enabled device

When users enroll an Apple DEP-enabled device, their experience is as follows.

1. Users start their Apple DEP-enabled device.

2. XenMobile delivers the Apple DEP configuration that you configured in the XenMobile console to the Apple DEP-enabled device.

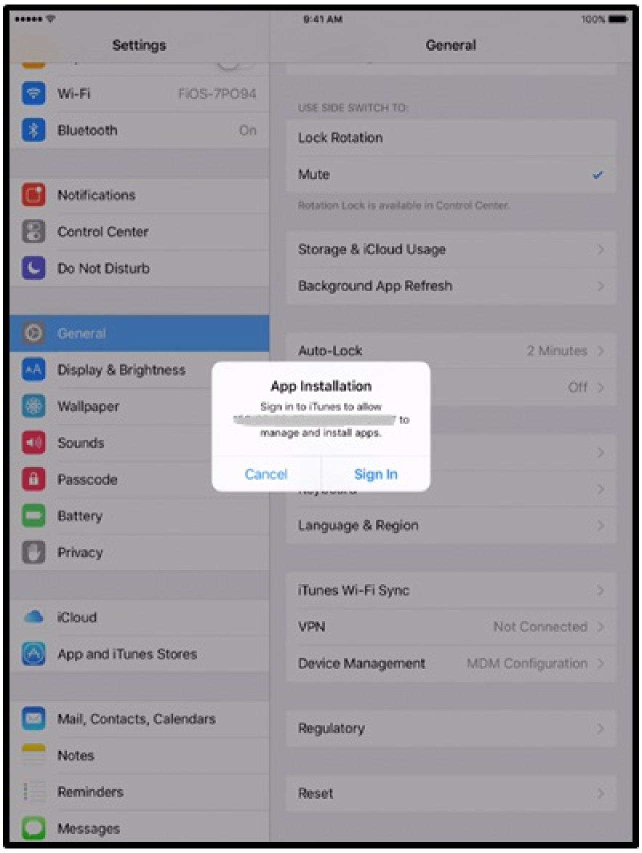
3. Users configure the initial settings on their device.

4. The device automatically starts the XenMobile device enrollment process.

5. Users continue to configure the other initial settings on their device.

6. In the home screen, users might be prompted to sign in to iTunes so that they can download Citrix Secure Hub.

> ### Note
>
> This step is optional if XenMobile is configured to deploy the Secure Hub app using the device-based Volume Purchase Program (VPP) app assignment. In this case, you don't need to create an iTunes account or use an existing account.



App Installation

Sign in to iTunes to allow [redacted] to manage and install apps.

7. Users open Secure Hub and type their credentials. If required by the policy, users might be prompted to create and verify a Citrix PIN.

XenMobile deploys any remaining required apps to the device.

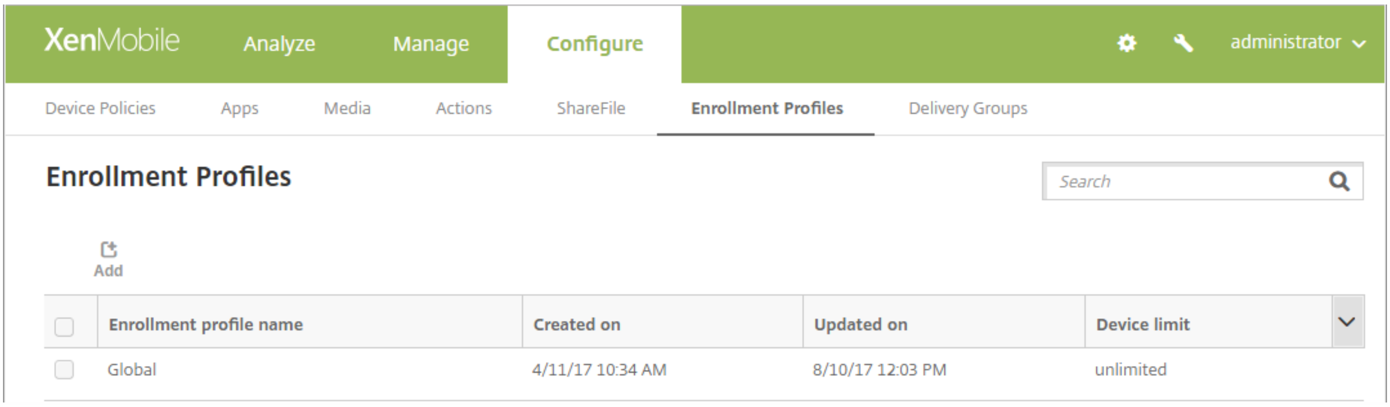
Device enrollment limit

Sep 06, 2017

XenMobile 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.

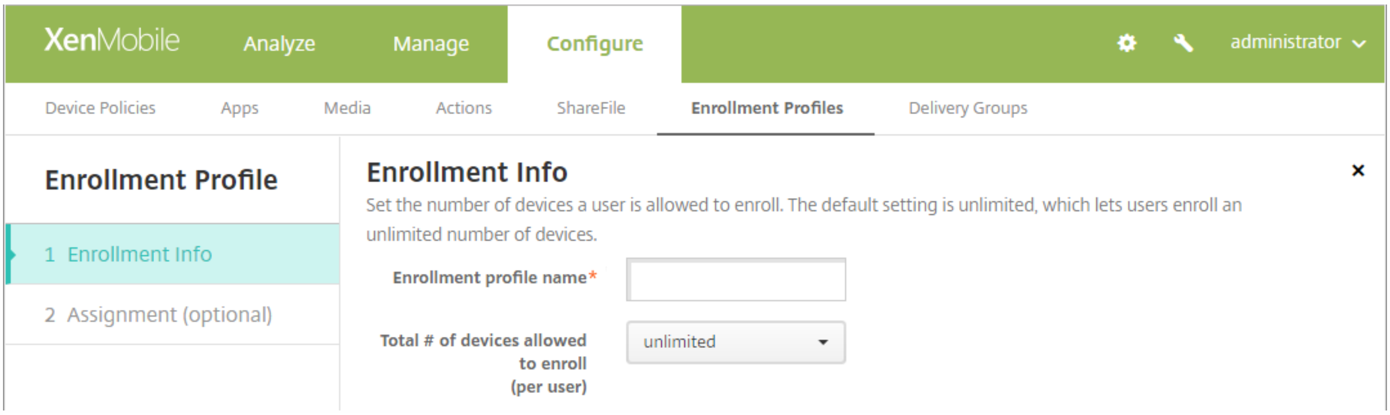
The device enrollment limit applies to the ENT, MDM, and MAM server modes. This feature is available for iOS and Android devices only.

1. Go to **Configure > Enrollment Profiles**. The default Global profile appears.



□	Enrollment profile name	Created on	Updated on	Device limit
□	Global	4/11/17 10:34 AM	8/10/17 12:03 PM	unlimited

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.



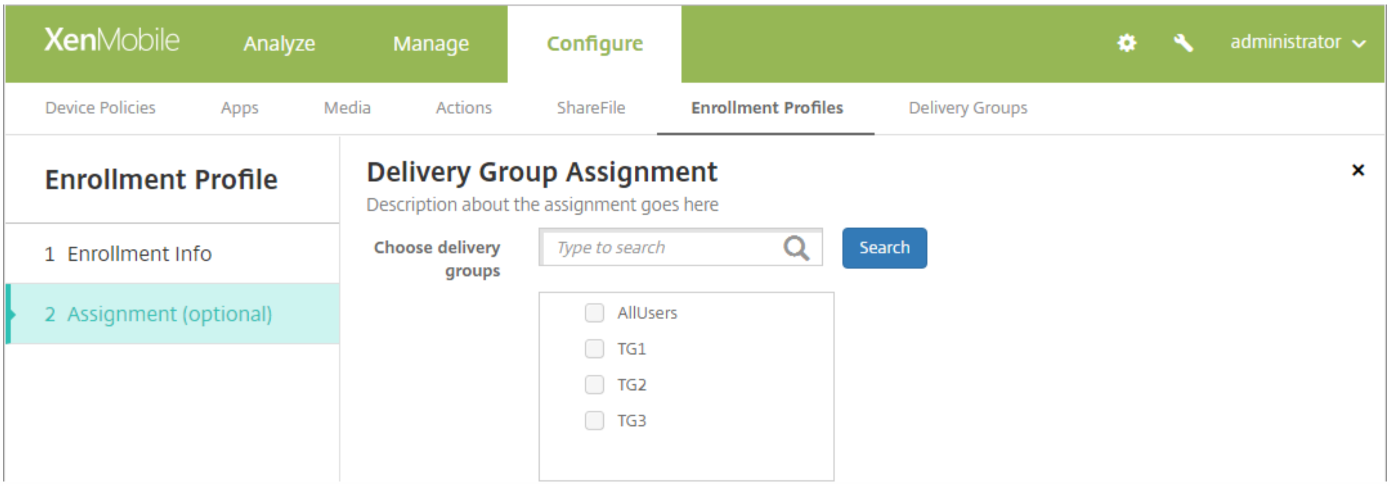
Enrollment Info

Set the number of devices a user is allowed to enroll. The default setting is unlimited, which lets users enroll an unlimited number of devices.

Enrollment profile name*

Total # of devices allowed to enroll (per user): unlimited

3. Click **Next**. The **Delivery Group Assignment** screen appears.

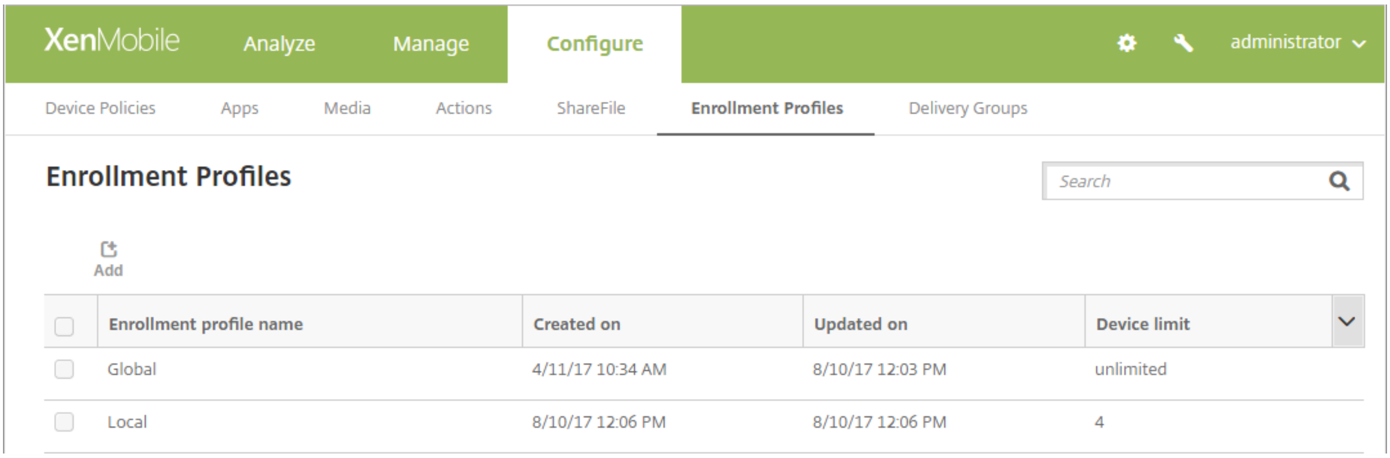


Delivery Group Assignment

Description about the assignment goes here

4. Select the delivery groups for this enrollment profile and then click **Save**.

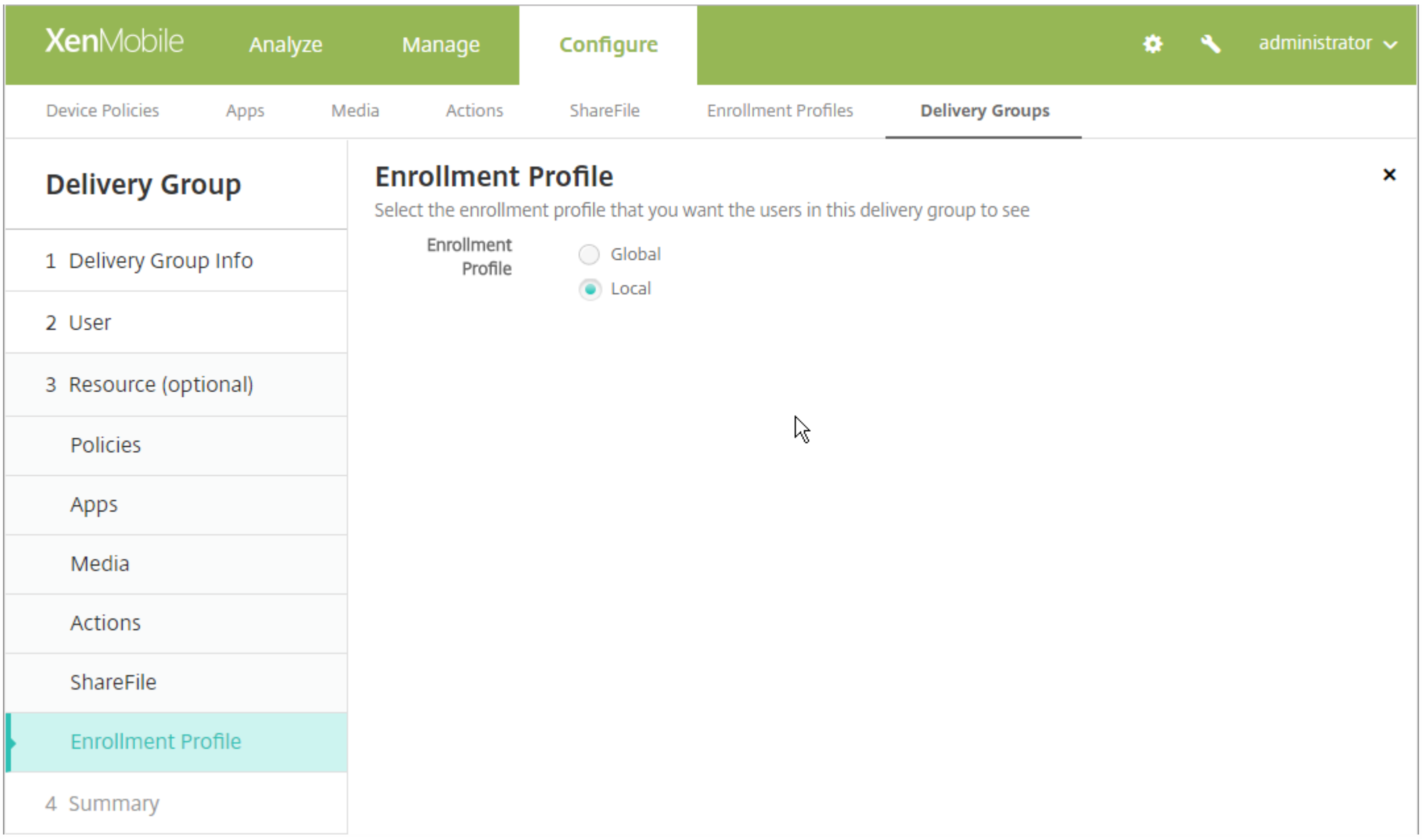
   The **Delivery Groups** page appears.



Enrollment Profiles

□	Enrollment profile name	Created on	Updated on	Device limit
□	Global	4/11/17 10:34 AM	8/10/17 12:03 PM	unlimited
□	Local	8/10/17 12:06 PM	8/10/17 12:06 PM	4

To change the enrollment profiles associated with a delivery group, go to **Configure > Delivery Groups** and then click **Enrollment Profiles**.



Enrollment Profile

Select the enrollment profile that you want the users in this delivery group to see

Enrollment Profile ○ Global ● Local

User experience with a device enrollment limit

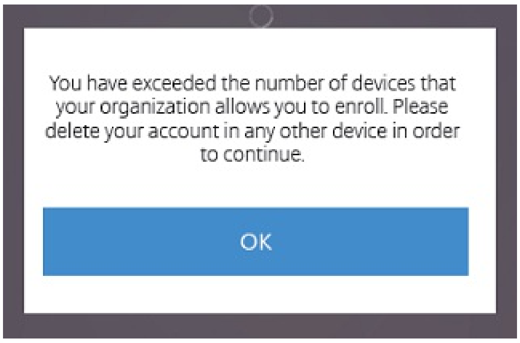
When you set the device enrollment limit and users try to enroll a new device, they follow these steps:

1. Sign on to Secure Hub.

2. Enter a server address to enroll.

3. Enter 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.

Enroll devices

Dec 27, 2017

To manage user devices remotely and securely, you enroll user devices in XenMobile. The XenMobile client software is installed on the user device and the user identity is authenticated. Then, XenMobile and the user profile are installed. Next, in the XenMobile console, you can perform device management tasks. You can apply policies, deploy apps, push data to the device, and lock, wipe, and locate lost or stolen devices.

Azure Active Directory enrollment is supported for iOS, Android, and Windows 10 devices. For more information about configuring Azure as your identity provider (IDP), see XenMobile Integration with Azure Active Directory as IDP.

Note: Before you can enroll iOS device users, you must request an APNs certificate. For details, see Certificates and authentication.

To update configuration options for users and devices, go to the **Manage > Enrollment Invitations** page. For details, see Send an enrollment invitation in this article.

This article has the following sections:

Android devices

iOS devices that use user-provided credentials

iOS devices that use derived credentials

macOS devices

Windows devices

Send an enrollment invitation

Android devices

> ## Note
>
> For information about enrolling Android for Work devices, see Android for Work.

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. Enter your corporate credentials, such as your XenMobile Server name, User Principal Name (UPN), or email address. Then, click **Next**.
5. In the **Activate device administrator** screen, tap **Activate**.
6. Enter your corporate password and then tap **Sign On**.
7. Depending on the way XenMobile is configured, you may be asked to create a Citrix PIN. You can use the PIN to sign on to Secure Hub and other XenMobile-enabled apps, such as Secure Mail and ShareFile. You enter your Citrix PIN twice. On

the **Create Citrix PIN** screen, enter a PIN.
8. Reenter the PIN. Secure Hub opens. You can then access the XenMobile Store to view the apps you can install on your Android device.
9. If you configured XenMobile to push apps to devices automatically after enrollment, users are prompted to install the apps. In addition, policies that you configure in XenMobile 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 XenMobile console. You cannot perform actions on the device, however. You cannot track the device, and you cannot monitor the 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:

a. Swipe from the left of the screen to open a settings pane.

b. Tap **Preferences**, tap **Accounts**, and then tap **Delete Account**.

On a tablet:

a. Tap the arrow next to your email address on the upper-right corner.

b. Tap **Preferences**, tap **Accounts**, and then tap **Delete Account**.

3. Tap **Re-Enroll**. A message appears to confirm you want to reenroll your device.

4. Tap **OK**.

Your device is unenrolled.

5. Follow the on-screen instructions to reenroll your device.

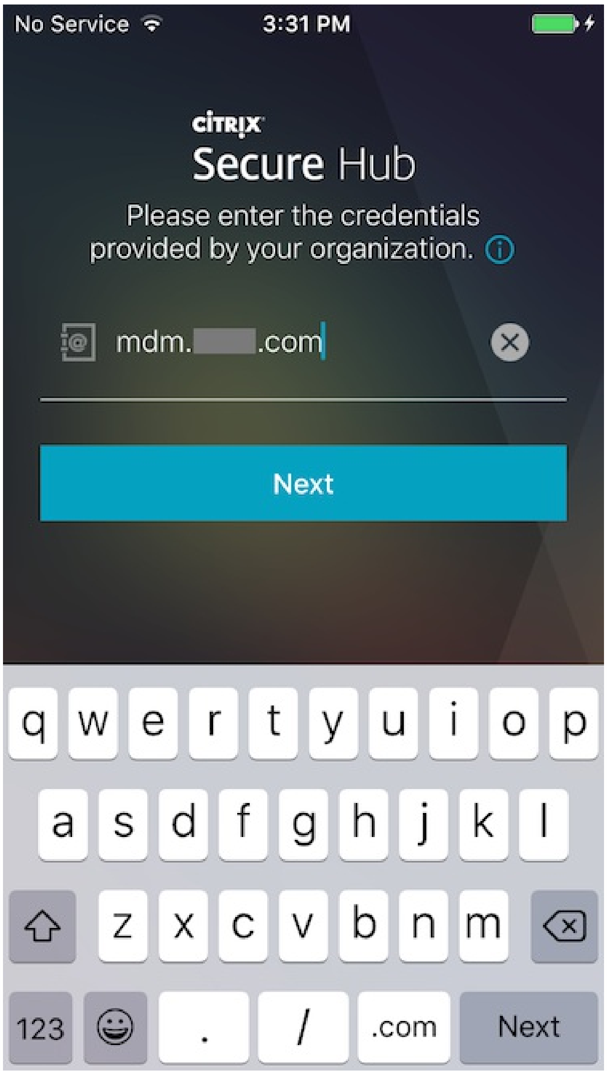
iOS devices that use user-provided credentials

1. Download the Secure Hub app from the Apple iTunes App Store on the device and then install the app on the device.

2. On the iOS device Home screen, tap the Secure Hub app.

3. When the Secure Hub app opens, enter the server address that your help desk provided.

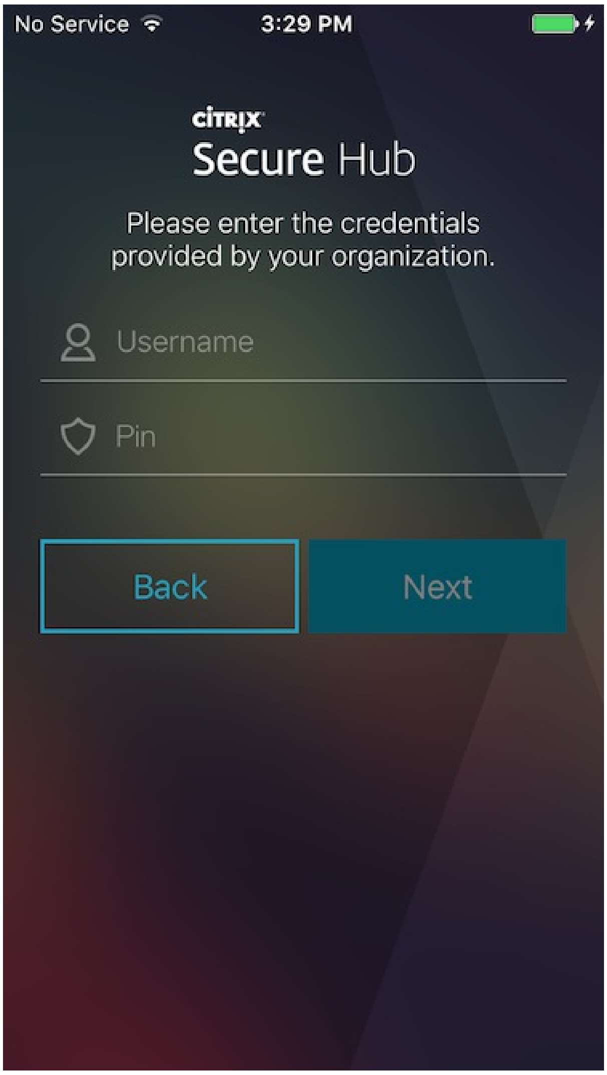
The screens presented might differ from these examples, depending on how XenMobile is configured.



Please enter the credentials provided by your organization.

mdm.[redacted].com

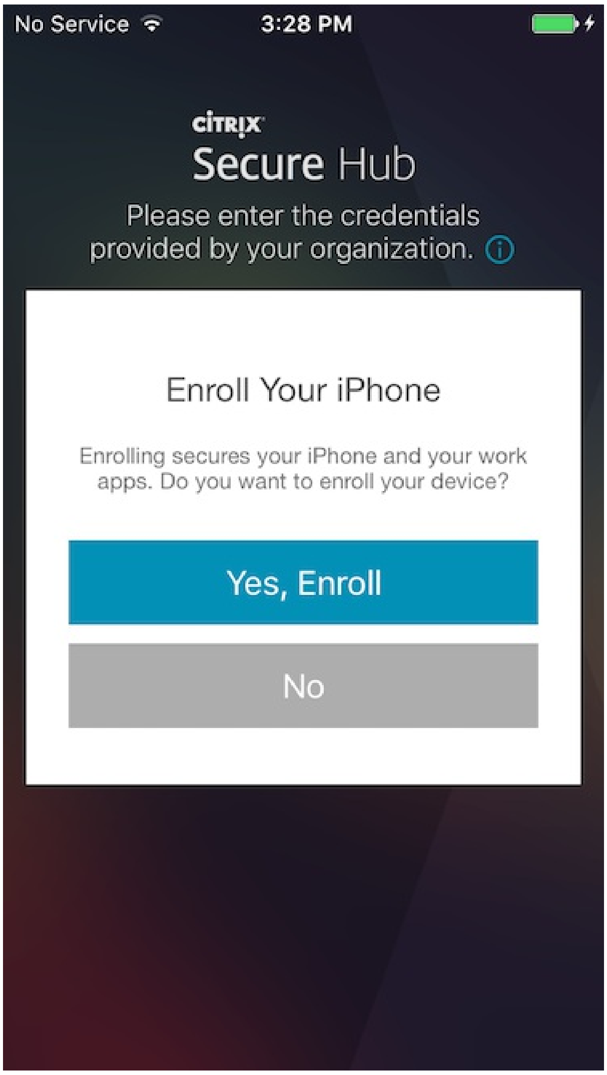
4. When prompted, enter your user name and password or PIN. Click **Next**.


No Service 3:29 PM

Secure Hub

Please enter the credentials provided by your organization.

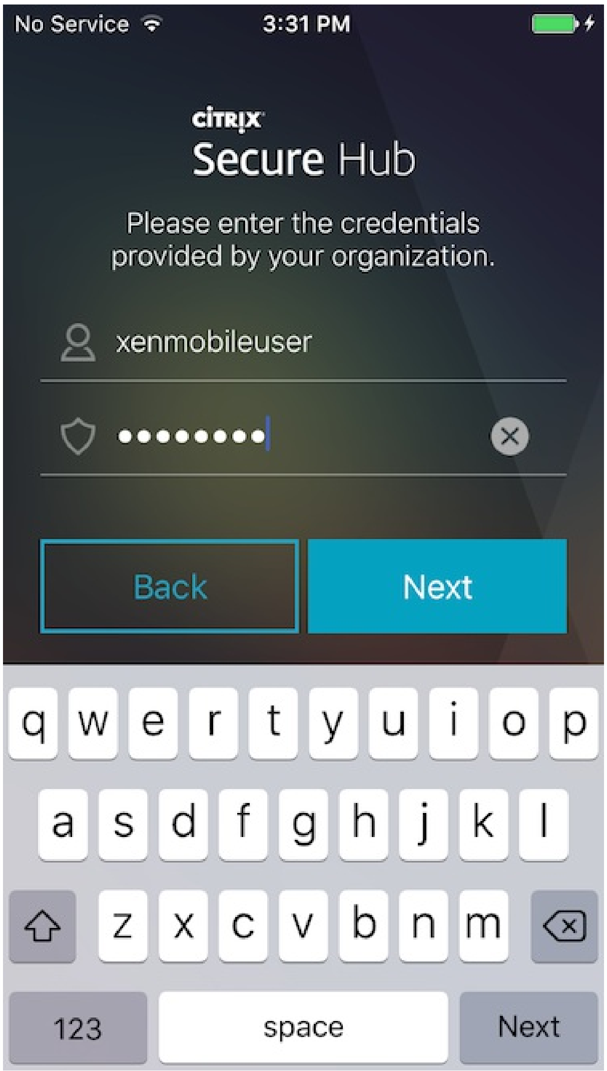
5. When prompted to enroll, click **Yes, Enroll** and then enter your credentials when prompted.



Please enter the credentials provided by your organization.

Enroll Your iPhone

Enrolling secures your iPhone and your work apps. Do you want to enroll your device?

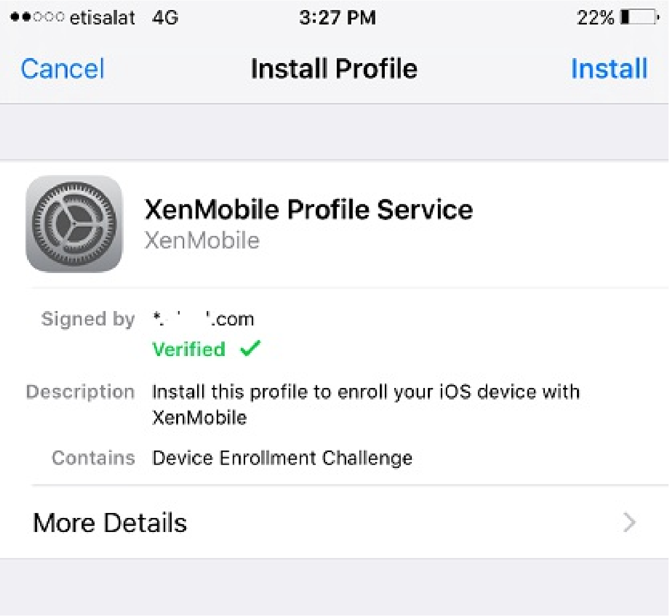


Please enter the credentials provided by your organization.

xenmobileuser

••••••••

6. Tap **Install** to install the Citrix Profile Services.



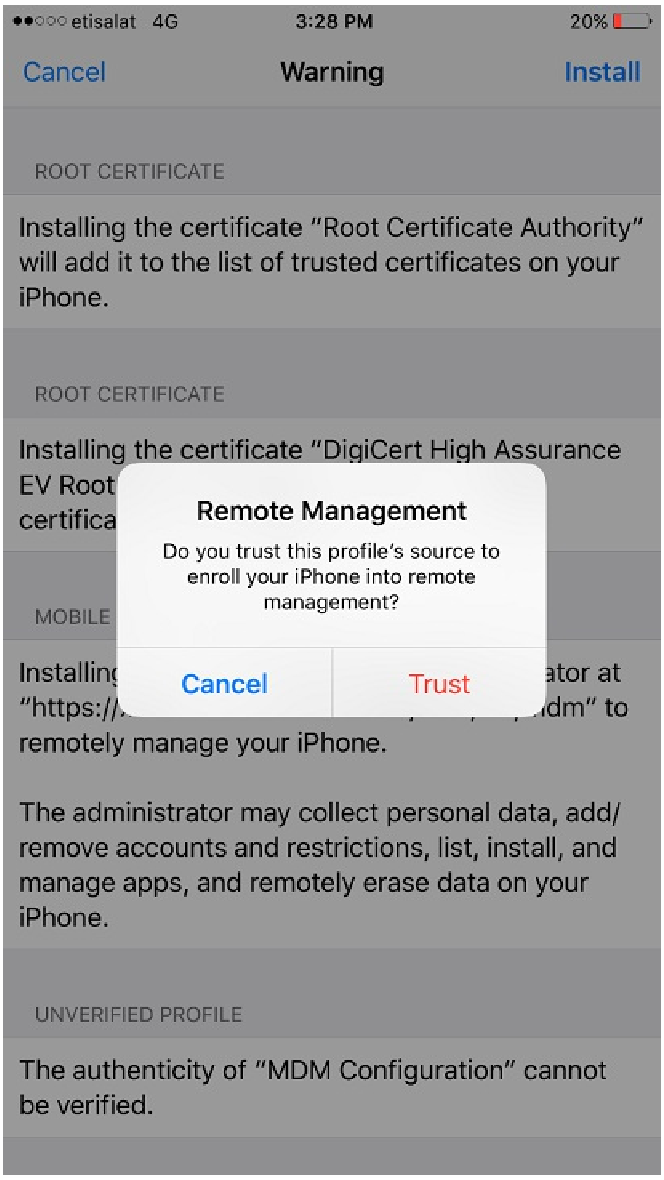
XenMobile Profile Service
XenMobile

Signed by *. '   '.com
Verified ✓

Description Install this profile to enroll your iOS device with XenMobile

Contains Device Enrollment Challenge

7. Tap **Trust**.



●●○○○ etisalat 4G 3:28 PM 20%

Cancel Warning Install

ROOT CERTIFICATE

Installing the certificate "Root Certificate Authority" will add it to the list of trusted certificates on your iPhone.

ROOT CERTIFICATE

Installing the certificate "DigiCert High Assurance EV Root certifica

MOBILE

Installing "https://   dm" to remotely manage your iPhone.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPhone.

UNVERIFIED PROFILE

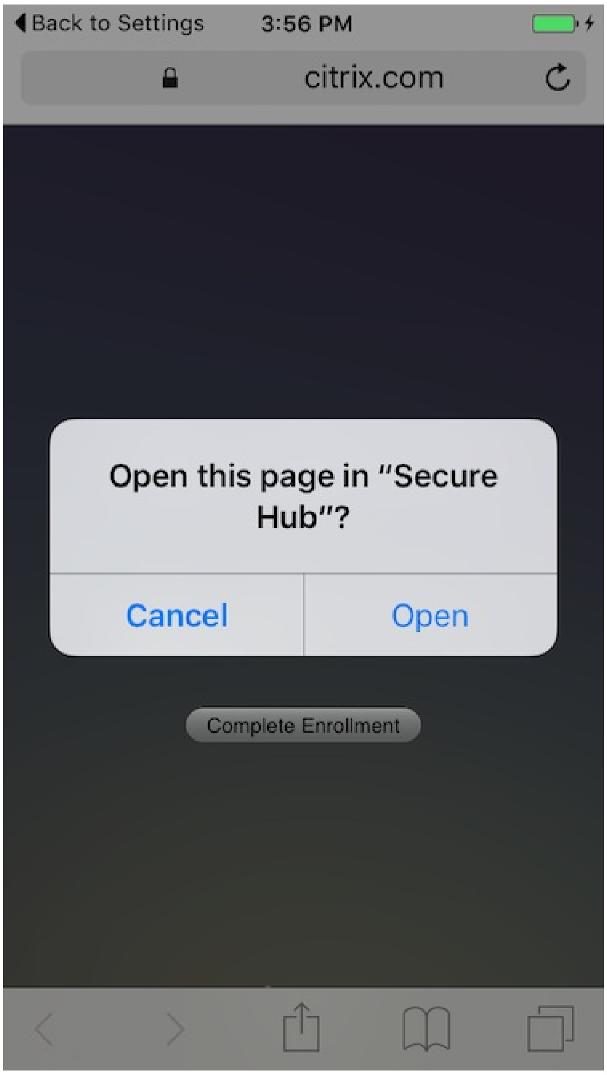
The authenticity of "MDM Configuration" cannot be verified.

Remote Management

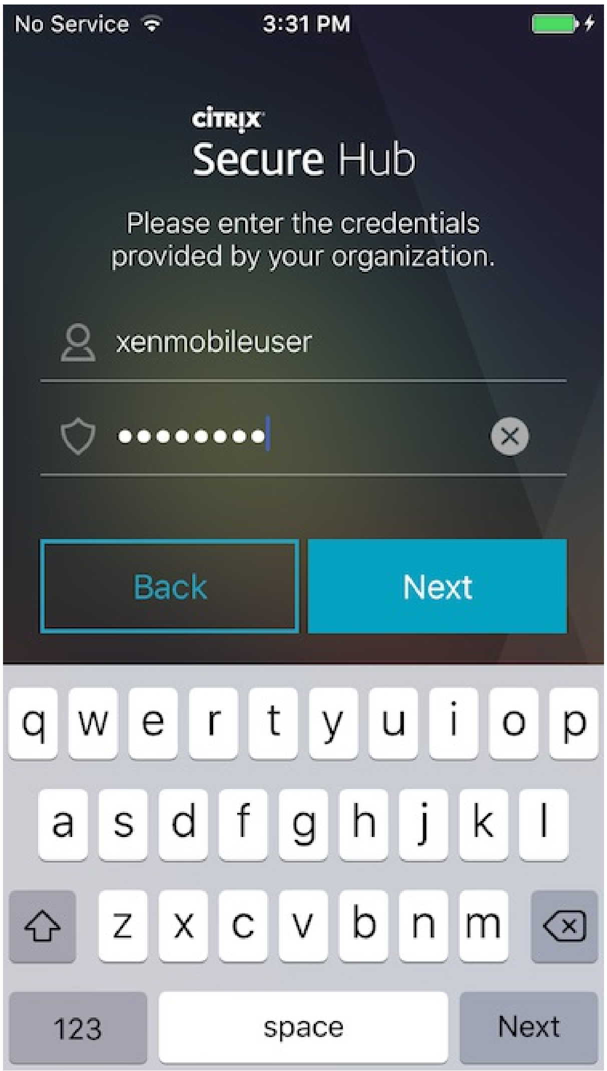
Do you trust this profile's source to enroll your iPhone into remote management?

Cancel Trust

8. Tap **Open** and then enter your credentials.



Open this page in "Secure Hub"?



No Service 3:31 PM

CITRIX

Secure Hub

Please enter the credentials provided by your organization.

xenmobileuser

••••••••

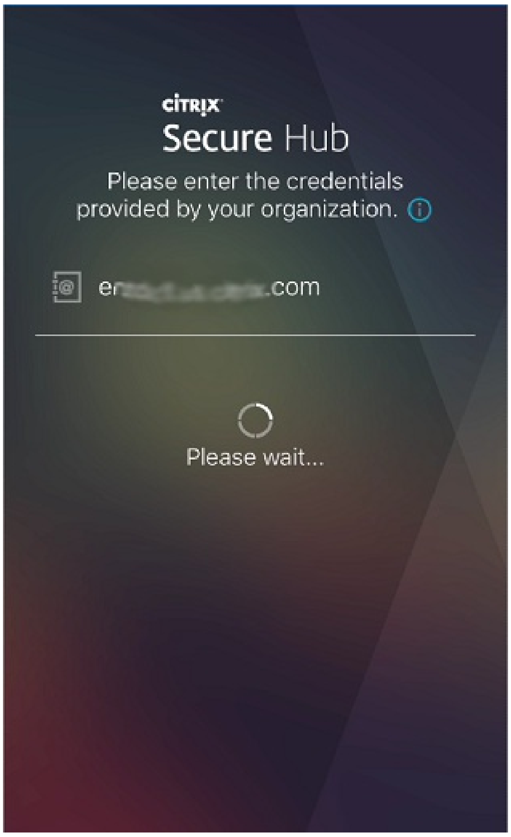
iOS devices that use derived credentials

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

1. The user installs Secure Hub and the app from your derived credential provider.

   The identity provider app for Intercede is MyID for Citrix. The logo for that app follows.

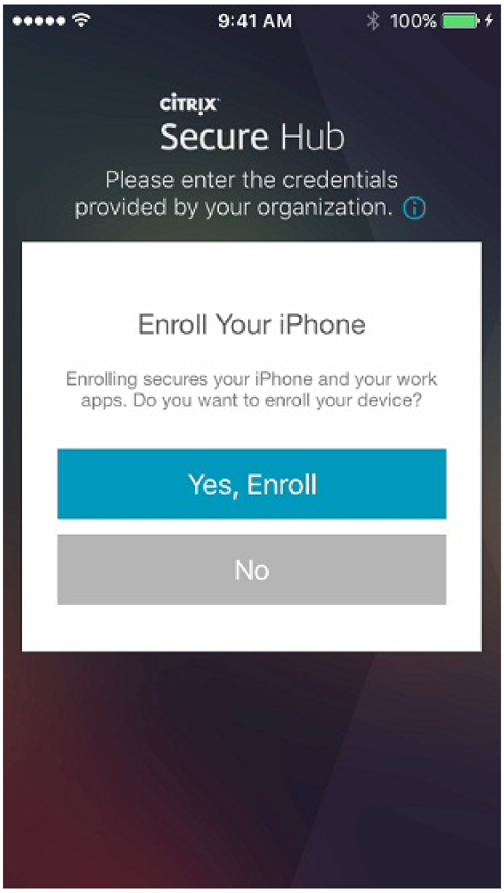
2. The user starts Secure Hub. When prompted, the user types the XenMobile Server fully qualified domain name and then clicks **Next**. Enrollment in Secure Hub starts. If the XenMobile Server supports derived credentials, Secure Hub prompts the user to create a Citrix PIN.



Please enter the credentials provided by your organization.

er[redacted].com

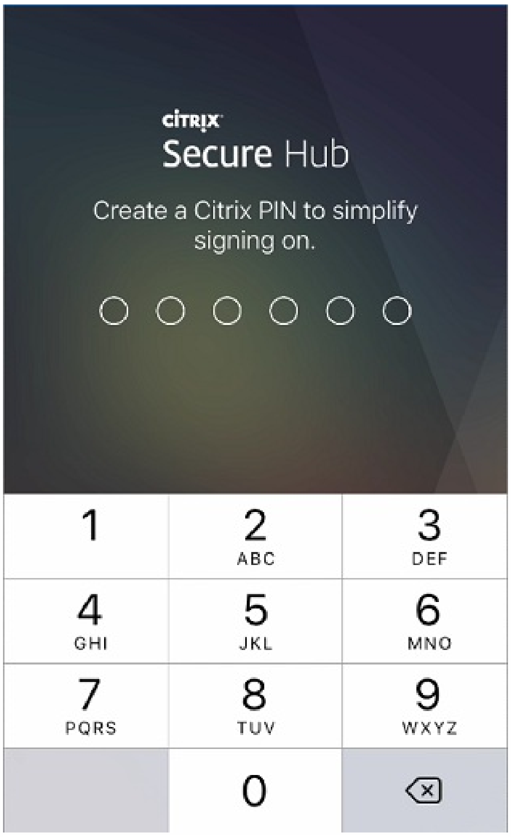
Please wait...



Please enter the credentials provided by your organization.

Enroll Your iPhone

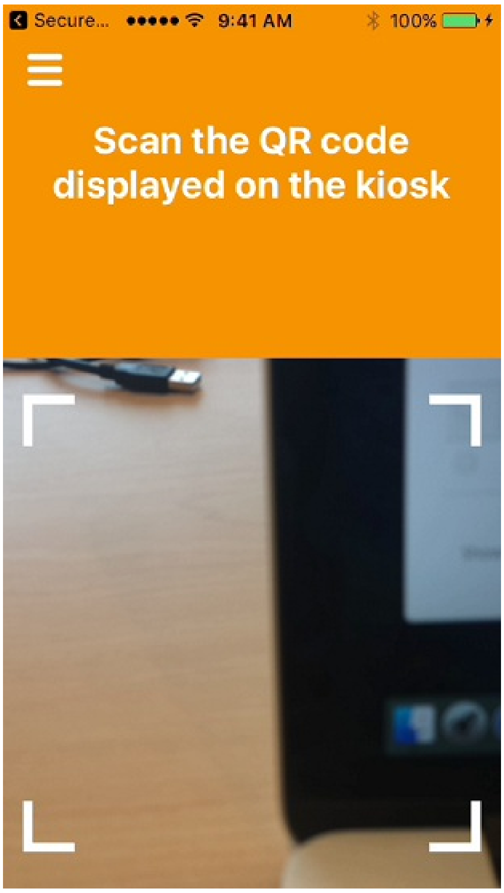
Enrolling secures your iPhone and your work apps. Do you want to enroll your device?



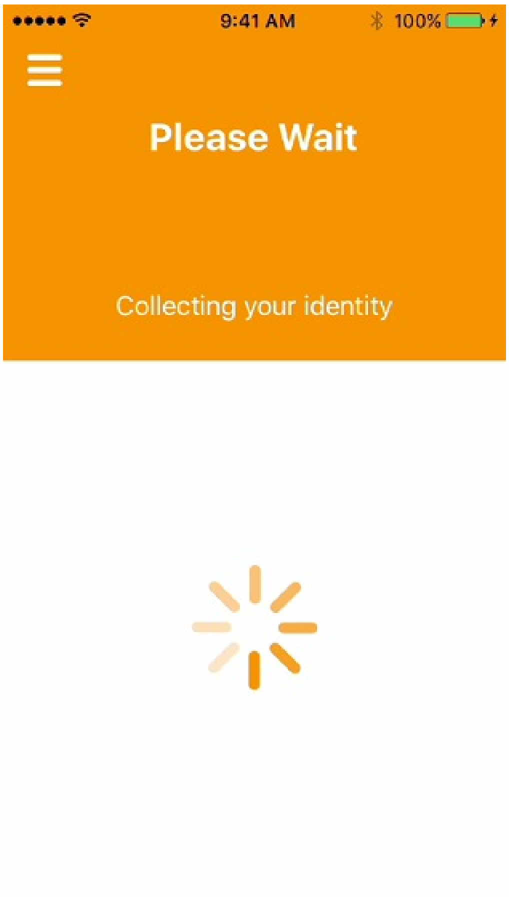
Secure Hub

Create a Citrix PIN to simplify signing on.

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



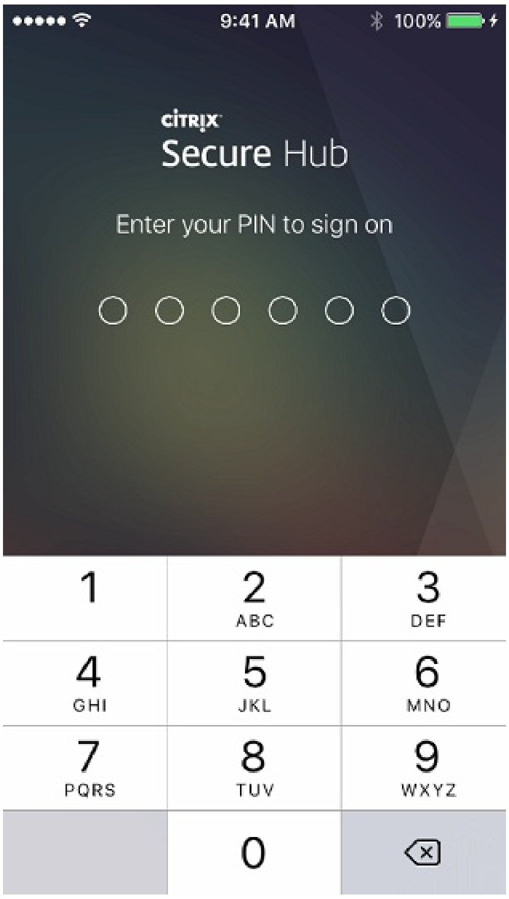
4. The user inserts their card into the smart card reader that's attached to their desktop. The desktop app then displays a QR code and prompts the user to scan the code using their mobile device.



Please Wait

Collecting your identity

5. The user enters their Secure Hub PIN when prompted.



6. After authenticating the PIN, Secure Hub downloads the certificates. The user then follows the prompts to complete enrollment.

To view device information in the XenMobile console:

- Go to **Manage > Devices** and then select a device to display a command box. Click **Show more**.
- Go to **Analyze > Dashboard**.

macOS devices

XenMobile 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 installation link**. This enrollment method for macOS devices sends users an enrollment link, which they open in Safari. A user then enrolls by providing their user name and password.

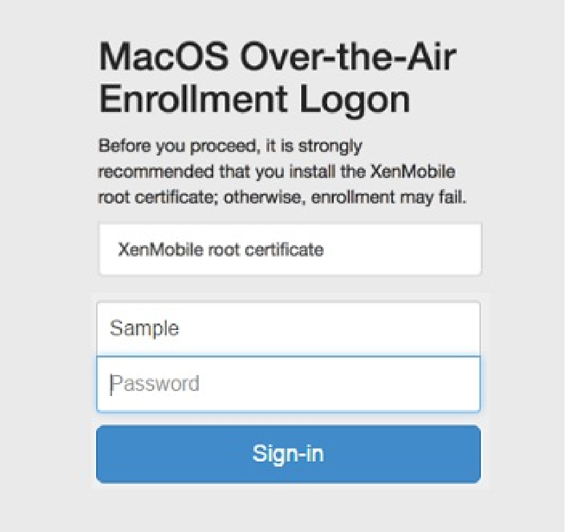
  To prevent the use of an enrollment link for macOS devices, set the server property, **Enable macOS OTAE** to **false**. As a result, macOS users can enroll only by using an enrollment invitation.

Send users an enrollment invitation

1. Optionally set up macOS device policies in the XenMobile console. For more information about device policies, see Device Policies. To find out which device policies you can configure for macOS, see Device policies by platform.

2. Add an invitation for macOS user enrollment. For more information, see Send an enrollment invitation in this article.

3. After users receive the invitation and click the link, the following screen appears in the Safari browser. XenMobile fills in the user name. If you chose **Two Factor** for the enrollment mode, another field appears.



MacOS Over-the-Air Enrollment Logon

Before you proceed, it is strongly recommended that you install the XenMobile root certificate; otherwise, enrollment may fail.

4. 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 more information about certificates, see Certificates and authentication.

5. Users provide the requested credentials.

   The Mac device policies install. You can now start managing Macs with XenMobile just as you manage mobile devices.

Send users an installation link

1. Optionally set up macOS device policies in the XenMobile console. For more information about device policies, see Device Policies. To find out which device policies you can configure for macOS, see Device policies by platform.

2. Send the enrollment link https://*serverFQDN*:8443/*instanceName*/macos/otae, which users open in Safari.

   - ***serverFQDN*** is the fully qualified domain name (FQDN) of the server running XenMobile.
   - 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.

3. 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 more information about certificates, see Certificates and authentication.

4. Users sign on to their Macs.

   The Mac device policies install. You can now start managing Macs with XenMobile just as you manage mobile devices.

Windows devices

> ### Note
>
> This section includes references to Windows Phone 8.1 devices, which Microsoft moved to End of Support on July 11, 2017. XenMobile currently supports Windows Phone 8.1 devices for MDM enrollment only.

Devices running Windows 10 enroll with Azure as a federated means of Active Directory authentication. 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 out-of-the-box the first time the device is powered on.
- Enroll in MDM as part of Azure AD Join from the Windows Settings page after the device is configured.

You can enroll devices in XenMobile that are running the following Windows operating systems:

- Windows 10 phone and tablet
- Windows Phone 8.1

Users can enroll directly through their devices.

Note for Windows 10 RS2 Phone and Tablet: During re-enrollment, a user isn't prompted for the Server URL. To work around this issue, restart the device. Or, on the email address screen, tap the X across from "Connecting to a service" to go to the Server URL page. This is a third-party issue.

You must configure autodiscovery and the Windows discovery service for user enrollment to enable the management of supported Windows devices.

Before Windows device users can enroll by using Azure, you must configure the Microsoft Azure server settings in XenMobile. For details, see Microsoft Azure Active Directory server settings.

> ### Note
>
> In order for Windows devices to enroll, the SSL listener certificate must be a public certificate. Enrollment fails if you've uploaded a self-signed SSL certificate.

To enroll Windows devices with self-discovery

To enable management of Windows devices, Citrix recommends you configure autodiscovery and the Windows discovery service. For details, see Enable autodiscovery.

1. On the device, check for and install all available Windows Updates.

2. For Windows 10: In the charms menu, tap **Settings** and then tap **Accounts > Access work or school > Connect to work or school**. For Windows 8.1 phones: Tap **PC Settings > Network > Workplace**.

3. Enter your corporate email address and then tap **Continue** on Windows 10 or tap **Turn on device management** on Windows 8.1. To enroll as a local user, enter a nonexistent email address with the correct domain name (for example, foo@mydomain.com). This permits you to bypass a known Microsoft limitation where enrollment is performed by the built-in Device Management on Windows; in the **Connecting to a service** dialog box, enter the user name and password associated with the local user. The device automatically discovers a XenMobile 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 XenMobile.

5. For Windows 10: In the **Terms of use** dialog box, indicate that you agree to have your device managed and then tap **Accept**. For Windows 8.1: In the **Allow apps and services from IT admin** dialog box, indicate that you agree to have your device managed and then tap **Turn on**.

To enroll Windows devices without self-discovery

It is possible to enroll Windows devices without autodiscovery. Citrix, however, recommends that you configure autodiscovery. Enrollment without autodiscovery results in a call to port 80 before connecting to the desired URL, so it is not considered best practice for production deployment. Citrix recommends that you use this process only in test environments and proof of concept deployment.

1. On the device, check for and install all available Windows Updates.

2. For Windows 10: In the charms menu, tap **Settings** and then tap **Accounts > Access work or school > Connect to work or school**. For Windows 8.1: Tap **PC Settings > Network > Workplace**.

3. Enter your corporate email address.

4. For Windows 10: If autodiscovery is not configured, an option appears where you can enter the server details, as described in step 5. For Windows 8.1: If **Automatically detect server address** is set to **on**, tap to turn the option **off**.

5. For Windows 10: In the **Enter server address** field, type the address:
https://serverfqdn:8443/serverInstance/wpe.
If a port other than 8443 is used for unauthenticated SSL connections, use that port number in place of 8443 in this address.

For Windows 8.1: Type the server address in the following format:
https://serverfqdn:8443/serverInstance/Discovery.svc.
If a port other than 8443 is used for unauthenticated SSL connections, use that port number in place of 8443 in this address.

6. Type your password.
7. For Windows 10: In the **Terms of use** dialog box, indicate that you agree to have your device managed and then tap **Accept**. For Windows 8.1: In the **Allow apps and services from IT admin** dialog box, indicate that you agree to have your device managed and then tap **Turn on**.

To enroll Windows Phone devices

To enroll Windows Phone devices in XenMobile, 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 XenMobile 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, ensure that you have configured an Enterprise Hub policy (with a signed Secure Hub, Windows Phone app for each platform you support).

1. On the main screen of the Windows phone, tap the **Settings** icon.

- For Windows 10: 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**.
- For Windows 8.1: Tap **PC Settings > Network > Workplace**, and then tap **Add Account**.

2. 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 Step 8.

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). This permits you to bypass a known Microsoft limitation; in the **Connecting to a service** dialog box, enter the user name and password associated with the local user.

3. On the next screen, type the web address of the XenMobile Server, such as: https://<xenmobile_server>:<portnumber>/<instancename>/wpe. For example, https://mycompany.mdm.com:8443/zdm/wpe. **Note**: The port number has to be adapted to your implementation. It must be the same port that you used for an iOS enrollment.

4. Enter the user name and domain if authentication is validated through a user name and domain and then tap **sign in**.

5. If a screen appears noting 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**.

6. On Windows Phone 8.1, when the account is added, you have the option of selecting **Install company app**. If your administrator has configured a Company App store, select this option and then tap **done**. If you clear this option, you will need to re-enroll your device to receive the Company app store.

7. On Windows Phone 8.1, on the **Account Added** screen, tap **done**.

8. To force a connection to the server, tap the refresh icon. If the device does not manually connect to the server, XenMobile attempts to reconnect. XenMobile connects to the device every 3 minutes 5 successive times, then every 2 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.

Send an enrollment invitation

In the XenMobile 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.

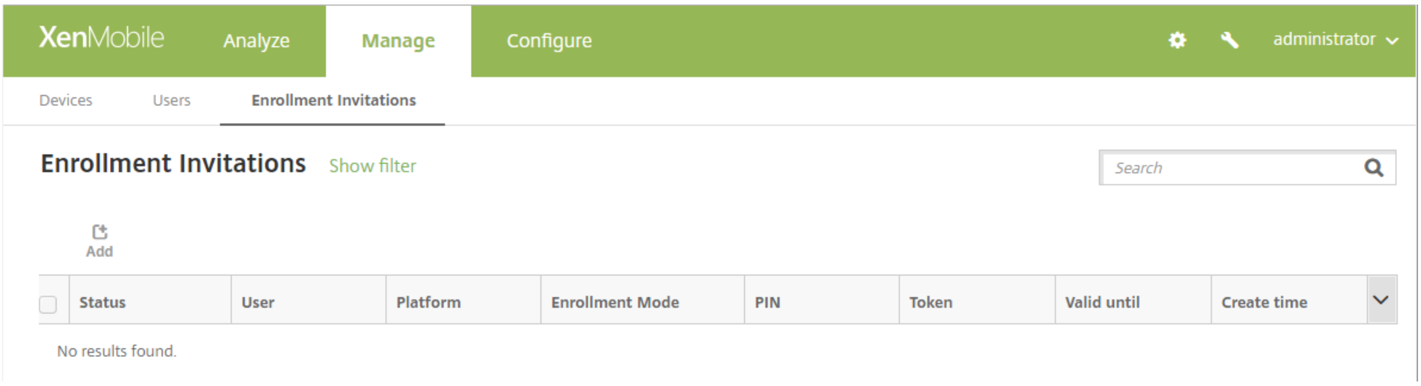
After users enroll, their devices appear as managed on **Manage > Devices**. The status of the invitation URL is shown as **Redeemed**.

Prerequisites

- XenMobile Server configured in Enterprise (XME) or MDM mode
- 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

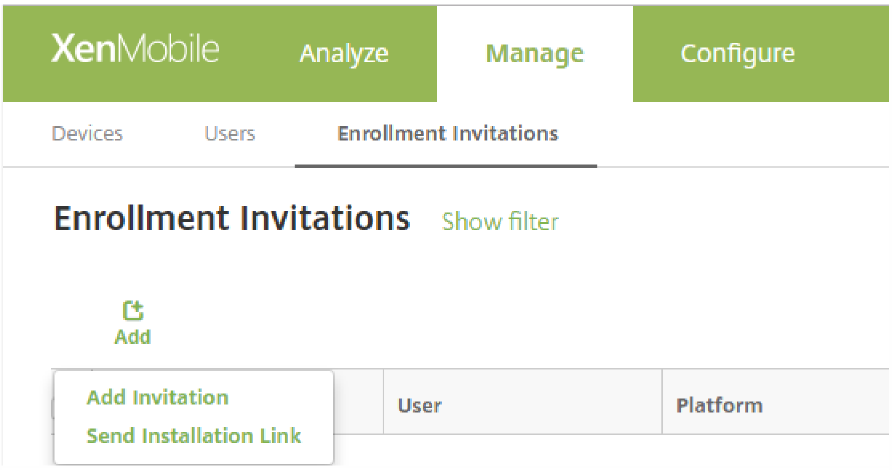
1. In the XenMobile console, click **Manage** > **Enrollment Invitations**. The **Enrollment Invitations** page appears.



□	Status	User	Platform	Enrollment Mode	PIN	Token	Valid until	Create time

No results found.

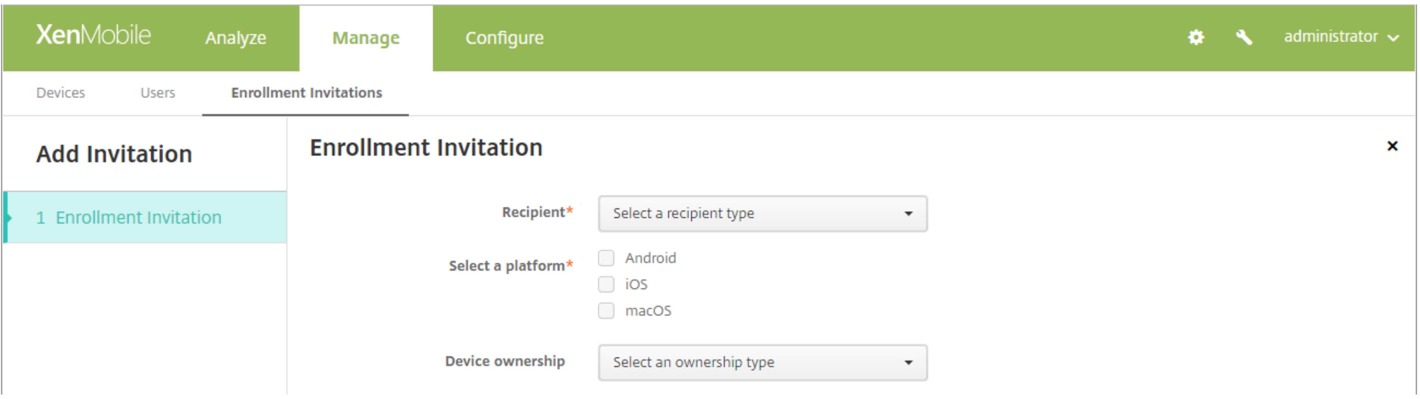
2. Click **Add**. A menu of enrollment options appears.



- 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.

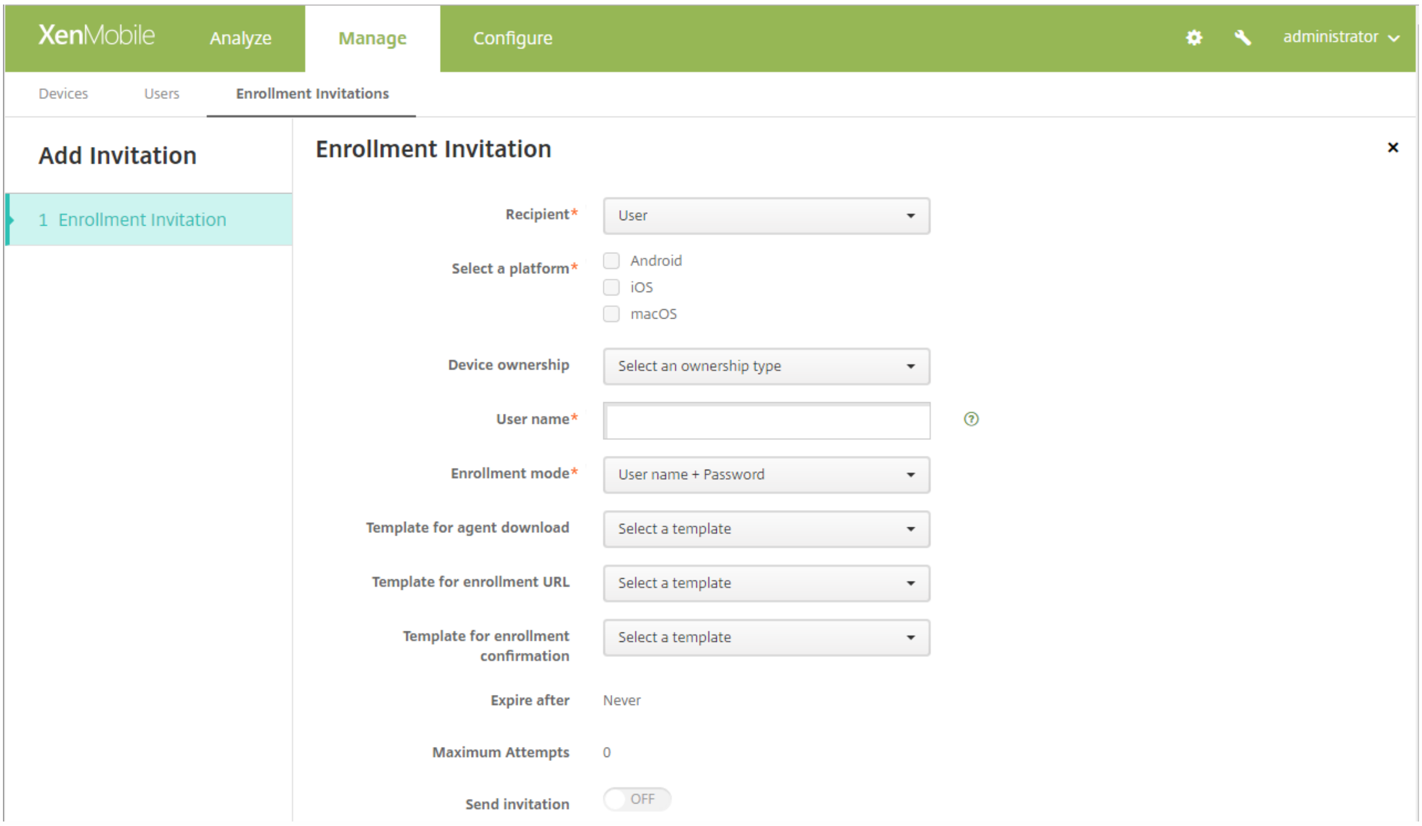


4. Configure these settings:

- **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



Enrollment Invitation

Recipient*: User

Select a platform*: □ Android □ iOS □ macOS

Device ownership: Select an ownership type

User name*:

Enrollment mode*: User name + Password

Template for agent download: Select a template

Template for enrollment URL: Select a template

Template for enrollment confirmation: Select a template

Expire after: Never

Maximum Attempts: 0

Send invitation: OFF

1. Configure these **User** settings:

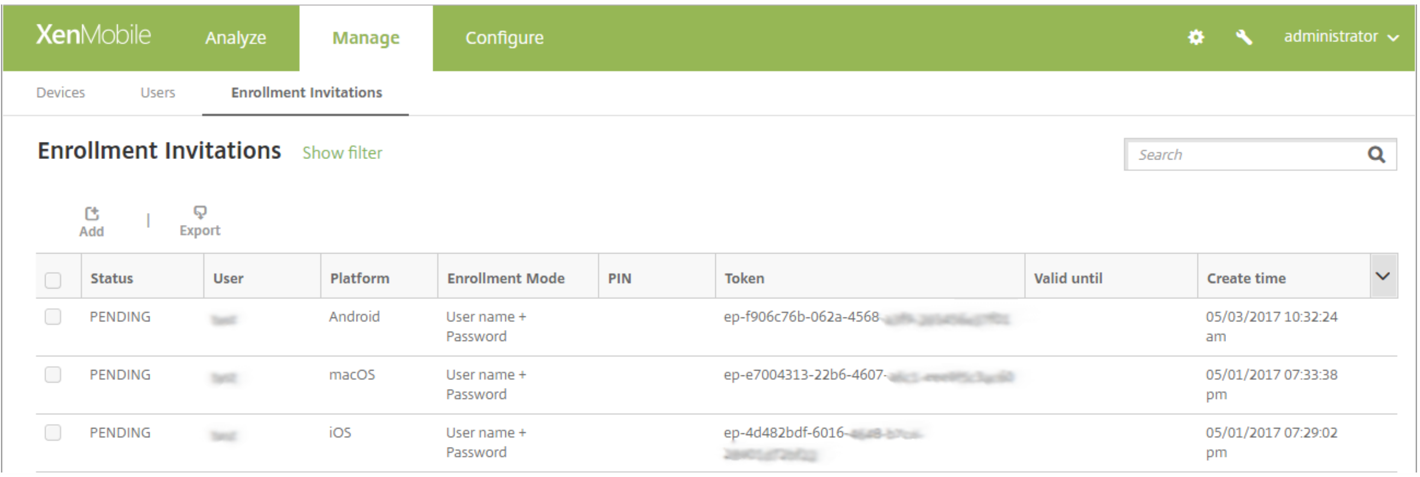
- **User name**: Type a user name. The user must exist in the XenMobile Server as a local user or as a user in Active Directory. If the user is local, ensure that the email property of the user is set so you can send that user notifications. If the user is in Active Directory, ensure that LDAP is configured.
- **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, where you 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 To 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. For more information about configuring enrollment modes, see To configure enrollment modes.
- **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.

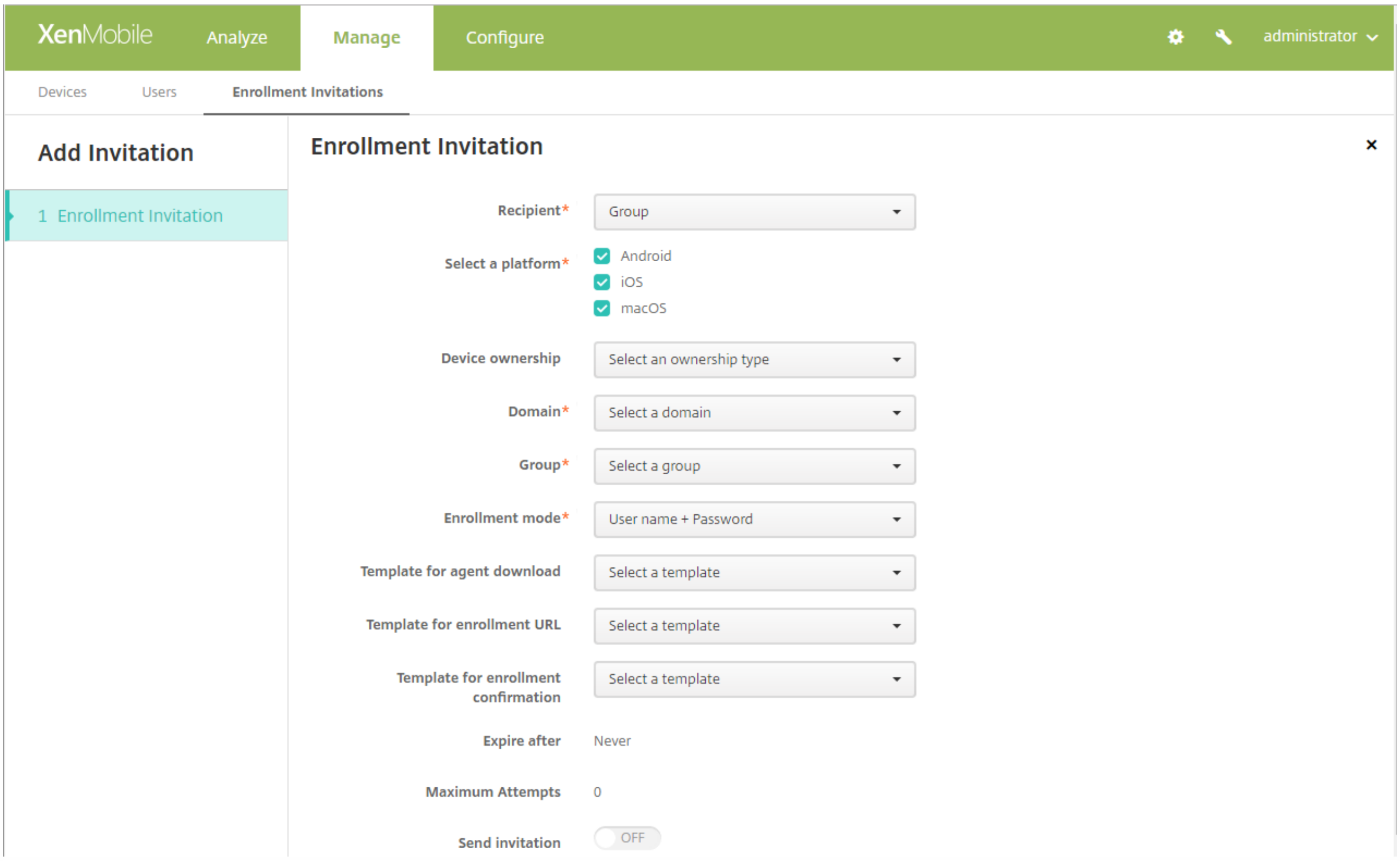
2. Click **Save and Send** if you enabled **Send invitation**. Otherwise, click **Save**. The invitation appears in the table on the **Enrollment Invitations** page.



Enrollment Invitations

□	Status	User	Platform	Enrollment Mode	PIN	Token	Valid until	Create time
□	PENDING	[redacted]	Android	User name + Password		ep-f906c76b-062a-4568-[redacted]		05/03/2017 10:32:24 am
□	PENDING	[redacted]	macOS	User name + Password		ep-e7004313-22b6-4607-[redacted]		05/01/2017 07:33:38 pm
□	PENDING	[redacted]	iOS	User name + Password		ep-4d482bdf-6016-[redacted]		05/01/2017 07:29:02 pm

To send an enrollment invitation to a group



Enrollment Invitation

Recipient*: Group

Select a platform*: ☑ Android ☑ iOS ☑ macOS

Device ownership: Select an ownership type

Domain*: Select a domain

Group*: Select a group

Enrollment mode*: User name + Password

Template for agent download: Select a template

Template for enrollment URL: Select a template

Template for enrollment confirmation: Select a template

Expire after: Never

Maximum Attempts: 0

Send invitation: OFF

1. Configure these settings:

- **Domain**: Choose the domain of the group to receive the invitation.
- **Group**: Choose the group to receive the invitation.
- **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

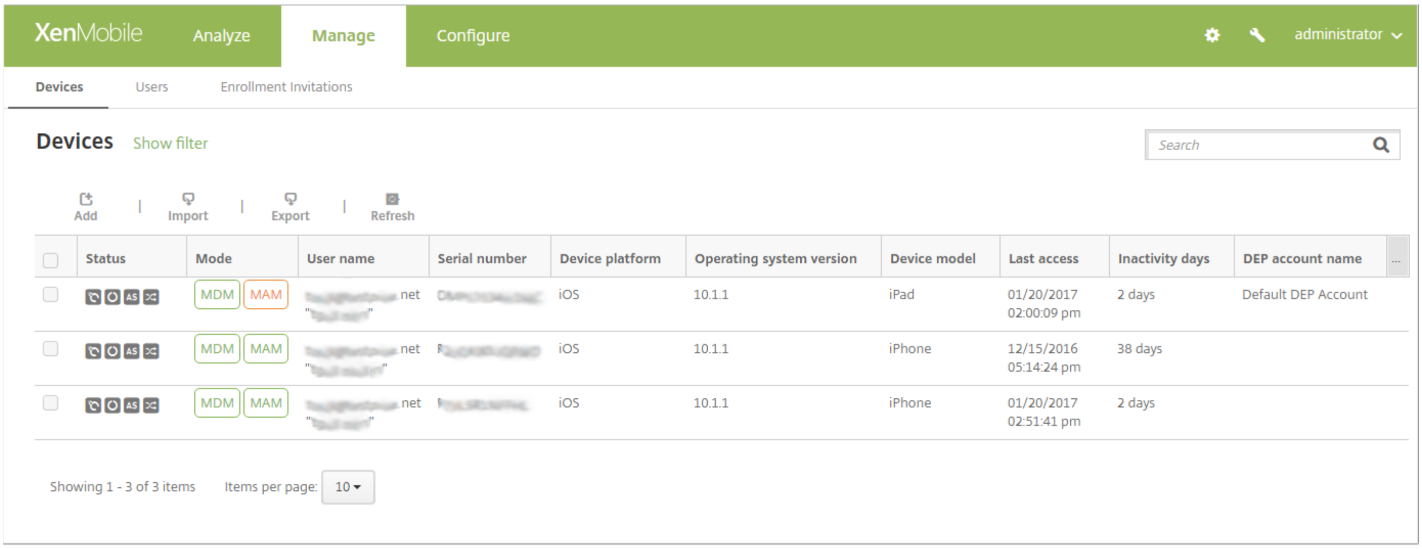
  Only the enrollment modes that are valid for each of the selected platforms appear.

  Note: When you select any enrollment mode that includes a PIN, the **Template for enrollment PIN** field appears, where you 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 To 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. For more information about configuring enrollment modes, see To configure enrollment modes.
- **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.

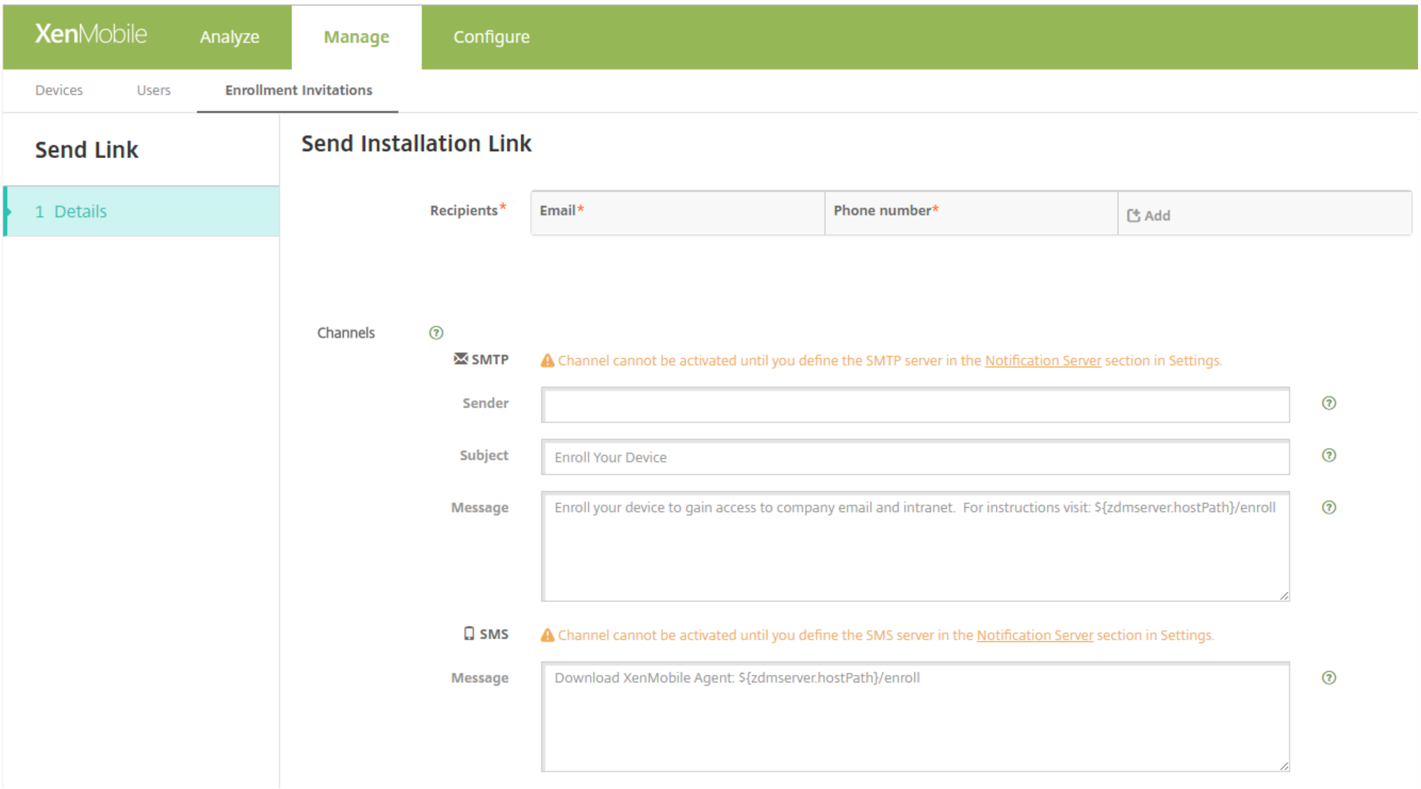


Devices Show filter

□	Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP account name
□		MDM MAM	[redacted].net "[redacted]"	[redacted]	iOS	10.1.1	iPad	01/20/2017 02:00:09 pm	2 days	Default DEP Account
□		MDM MAM	[redacted].net "[redacted]"	[redacted]	iOS	10.1.1	iPhone	12/15/2016 05:14:24 pm	38 days	
□		MDM MAM	[redacted].net "[redacted]"	[redacted]	iOS	10.1.1	iPhone	01/20/2017 02:51:41 pm	2 days	

Showing 1 - 3 of 3 items Items per page: 10

To send an installation link



Send Installation Link

Recipients* Email* Phone number* Add

Channels

SMTP ⚠ Channel cannot be activated until you define the SMTP server in the Notification Server section in Settings.

Sender

Subject: Enroll Your Device

Message: Enroll your device to gain access to company email and intranet. For instructions visit: ${zdmserver.hostPath}/enroll

SMS ⚠ Channel cannot be activated until you define the SMS server in the Notification Server section in Settings.

Message: Download XenMobile Agent: ${zdmserver.hostPath}/enroll

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:

- **Recipient**: For each recipient that you want to add, click Add and 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.
  - Click **Save**.

    Note: To delete an existing 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 an existing recipient, hover over the line containing the listing and then click the pen icon on the right-hand 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.

      Note: 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.

Firebase Cloud Messaging

Sep 06, 2017

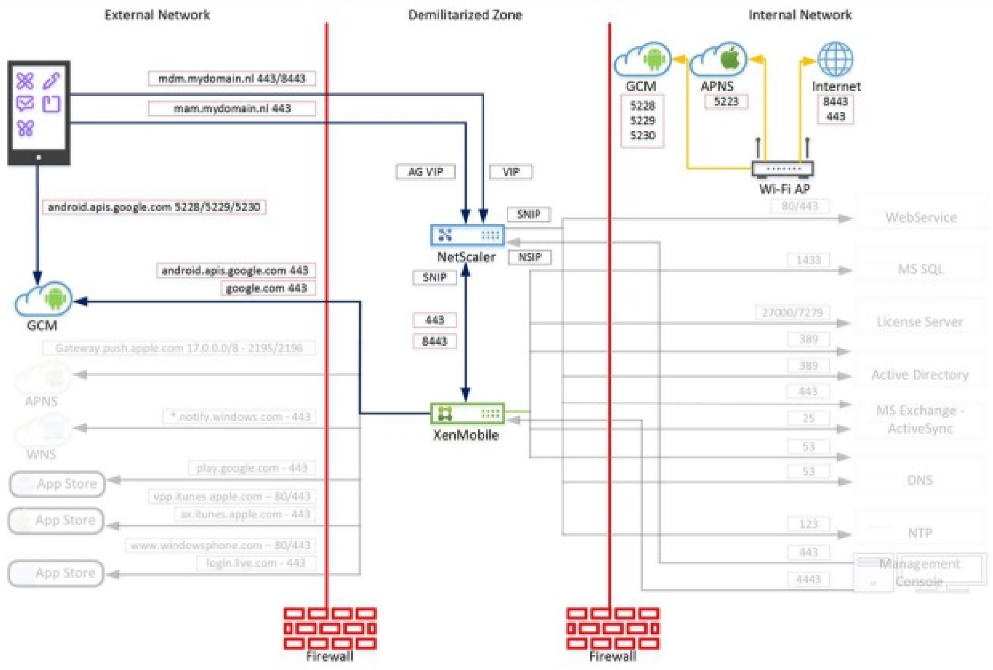
Alternative to the **Active poll period** policy, you can use Firebase Cloud Messaging (FCM) to control how and when Android devices connect to XenMobile. By using the following configuration, any security action or deploy command triggers a push notification to prompt the user to reconnect to the XenMobile Server.

Prerequisites

- XenMobile 10.3.x
- Latest Secure Hub client
- Google developer account credentials
- Open port 443 on XenMobile to Android.apis.google.com and Google.com

Architecture

This diagram shows the communication flow for FCM in the external and internal network.

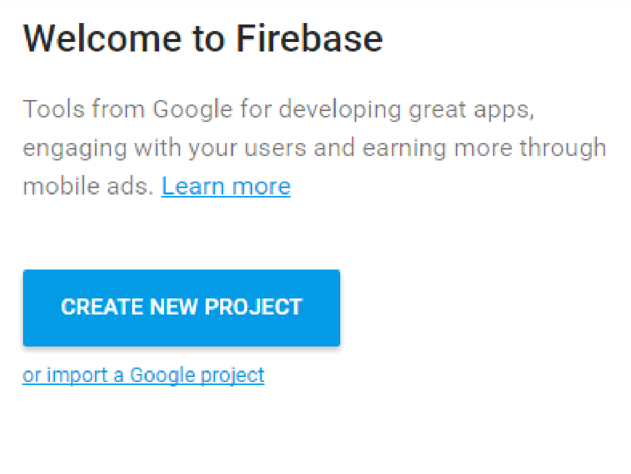


To configure your Google account for GCM

1. Sign in to the following URL using your Google developer account credentials:

   https://console.firebase.google.com/?pli=1

2. Click **Create a project**.



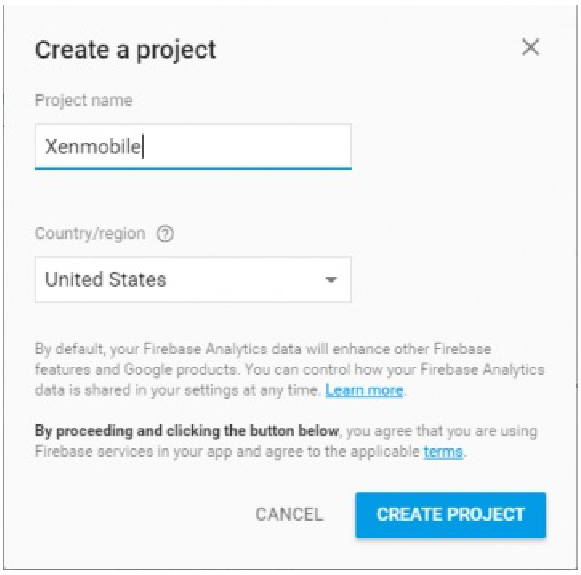
Welcome to Firebase

Tools from Google for developing great apps, engaging with your users and earning more through mobile ads. Learn more

CREATE NEW PROJECT

or import a Google project

3. Type a **Project name** and then click **Create Project**.



Create a project

Project name

Xenmobile

Country/region

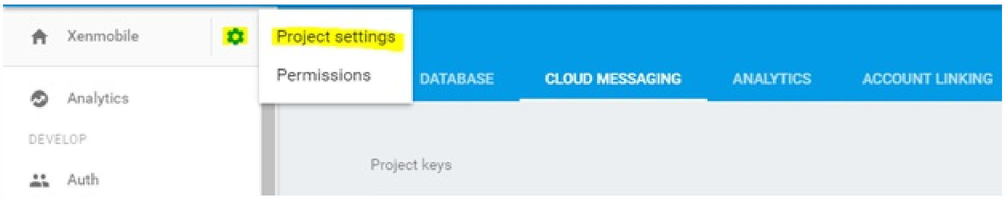
United States

By default, your Firebase Analytics data will enhance other Firebase features and Google products. You can control how your Firebase Analytics data is shared in your settings at any time. Learn more.

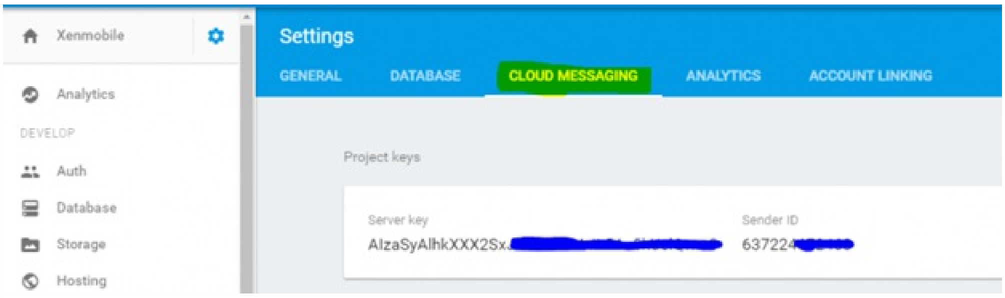
By proceeding and clicking the button below, you agree that you are using Firebase services in your app and agree to the applicable terms.

CANCEL CREATE PROJECT

4. Click the gear icon next to your project name in the top left and click **Project Settings**.



5. Select the **Cloud Messaging** tab. You can find your sender ID and Server Key on this page. Copy these values because you must provide them in XenMobile Server. It is important to note that any Server Keys created after September 2016 must be created in the Firebase console.



Project keys

Server key: AlzaSyAlhkXXX2Sx.[redacted]

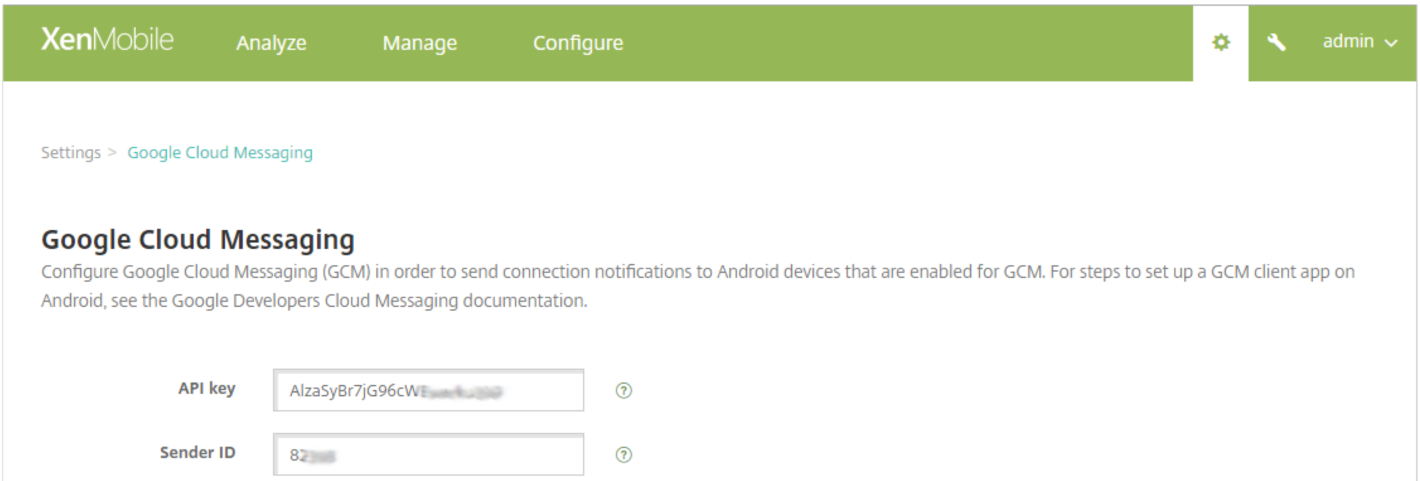
Sender ID: 637224[redacted]

To configure XenMobile for GCM

1. Sign in to XenMobile console and then click **Settings > Server Properties**. In the search bar, type **GCM** and click search.

   a. Edit **GCM API key**, and type the Firebase Cloud Messaging API key that you copied in the last step of Firebase Cloud Messaging configuration.

   b. Edit **GCM Sender ID**, and type the Sender ID value you noted in the previous procedure.



Google Cloud Messaging

Configure Google Cloud Messaging (GCM) in order to send connection notifications to Android devices that are enabled for GCM. For steps to set up a GCM client app on Android, see the Google Developers Cloud Messaging documentation.

API key: AlzaSyBr7jG96cWE[redacted]

Sender ID: 82[redacted]

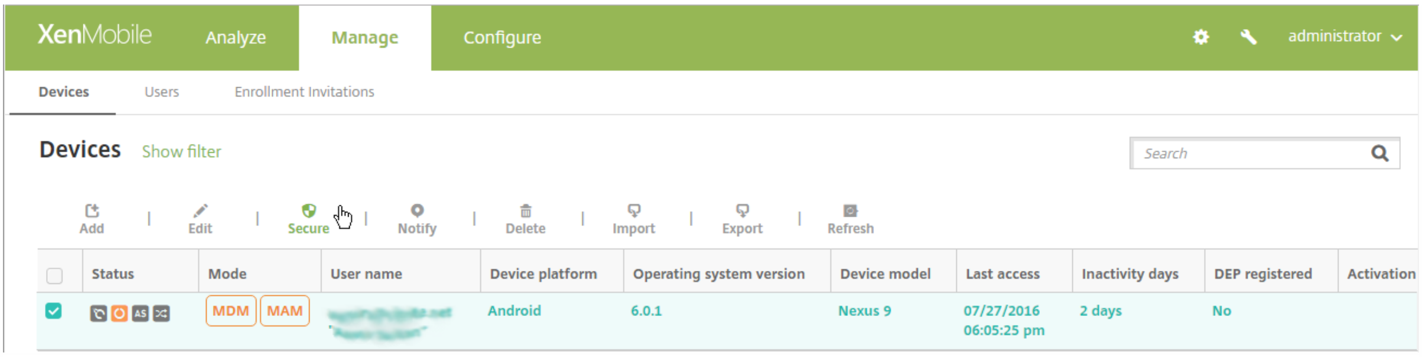
To test your configuration

As a prerequisite to test your FCM configuration, do not have a **Scheduling** policy configured. Alternatively, do not set the policy to **Always Connect**. For more information about configuring the **Scheduling** policy, see Scheduling device policy.

1. Enroll an Android device.

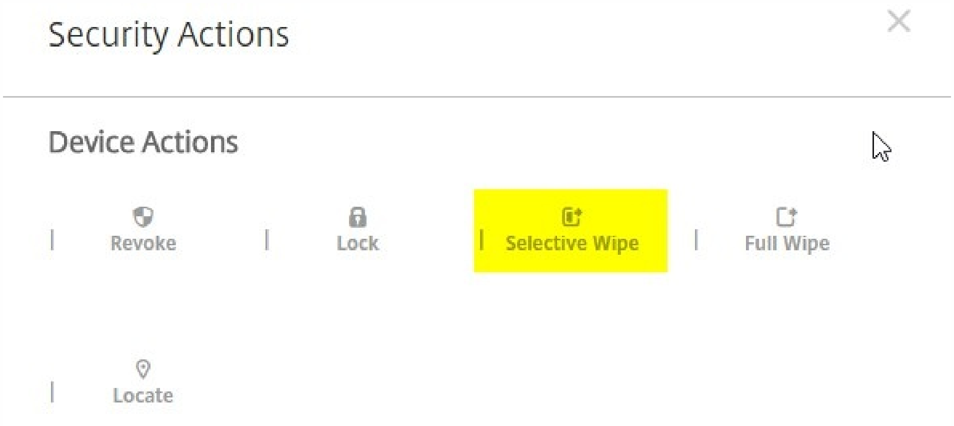
2. Leave the device idle for some time, so that it disconnects from XenMobile Server.

3. Sign in to the XenMobile console, click **Manage**, select the Android device, and then click **Secure**.



☐	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP registered	Activation
☑	AS	MDM MAM	[redacted]	Android	6.0.1	Nexus 9	07/27/2016 06:05:25 pm	2 days	No	

4. Under **Device Actions**, click **Selective Wipe**.



In a successful configuration, selective wipe occurs on the device.

Google Play credentials

Sep 06, 2017

XenMobile uses Google Play credentials to extract app information for the device.

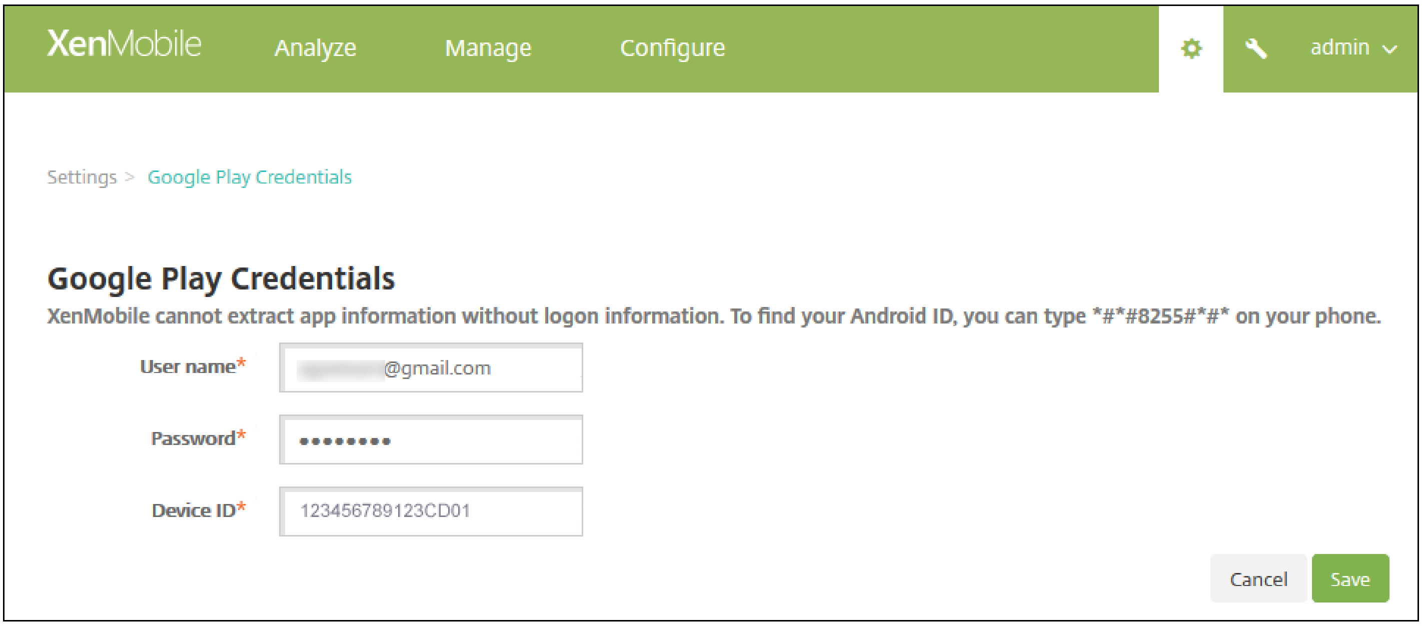
To locate your Android ID, enter *#*#8255#*#* on your phone. If the code does not reveal the device ID on your device type, it might be possible to use a third-party app to derive the device ID. The ID to retrieve is the Google Services Framework ID with the label GSF ID.

> ## Note
>
> When searching for Google Play Store apps in the XenMobile console, the search returns apps based on the Android operating system of the device. For example, a Samsung S6 Edge is running an operating system version 6.0.1. When you search for apps, the only apps that appear in the search result are apps that are compatible with Android version 6.0.1.

> ## Important
>
> To enable XenMobile to extract app information, you might need to configure your Gmail account to permit unsecure connections. For steps, see the Google support site.

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

2. Under **Platforms**, click **Google Play Credentials**. The Google Play Credentials page appears.



Settings > Google Play Credentials

Google Play Credentials

XenMobile cannot extract app information without logon information. To find your Android ID, you can type *#*#8255#*#* on your phone.

User name*	[redacted]@gmail.com
Password*	••••••••
Device ID*	123456789123CD01

3. Configure these settings:

- **User name**: Type the name associated with the Google Play account.

- **Password**: Type the user password.
- **Device ID**: Type your Android ID.
  See the Note earlier in the article for steps on obtaining your Android ID.

3. Click **Save**.

Integrate with Apple Education features

Feb 19, 2018

You can use XenMobile Server as your mobile device management (MDM) solution in an environment that uses Apple Education. XenMobile supports the Apple Education enhancements introduced in iOS 9.3, including Apple School Manager and Classroom app for iPad. The XenMobile 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 Apple School Manager DEP enrollment in XenMobile, a Managed Apple ID account configured with a new password, and required VPP apps and iBooks.

The following video provides a quick tour of the changes you make to Apple School Manager and XenMobile Server.

Citrix XenMobile Education Configuration: Integrate Apple Education features with XenMobile

Here are highlights of XenMobile support for Apple Education features.

Apple School Manager

Apple School Manager is a service that lets you set up, deploy, and manage iOS devices and macOS laptops used in educational institutions. Apple School Manager includes a web-based portal that lets IT administrators:

- Assign DEP devices to different MDM servers.
- Purchase VPP 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.

Apple School Manager is a type of Education DEP. XenMobile supports both Business DEP and Apple School Manager enrollment.

You can add multiple Apple School Manager DEP accounts to XenMobile Server. For example, this feature enables you to use different enrollment settings and Setup Assistant options by Education unit or department. You then associate DEP accounts with different device policies.

After you add an Apple School Manager DEP account to the XenMobile console, XenMobile retrieves class and roster information. During device setup, XenMobile Server:

- 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 VPP.

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 XenMobile 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.

Prerequisites

- NetScaler Gateway
- XenMobile Server configured in Enterprise mode (XME, also referred to as MDM+MAM) or MDM mode. If you already have a XenMobile Server configured in XME or MDM mode, you can use it with Apple School Manager.
- Apple iPad 3rd generation (minimum version) or iPad Mini, with iOS 9.3 (minimum version)

Notes:

- XenMobile currently supports the one-to-one model of Apple Education. You can assign one iPad to only one Apple School Manager user.
- XenMobile Server doesn't validate Apple School Manager user accounts against LDAP or Active Directory. However, you can connect XenMobile Server to LDAP or Active Directory for management of users and devices not related to Apple School Manager instructors or students. For example, you can use Active Directory to provide Secure Mail and Secure Web to other Apple School Manager members, such as IT administrators and managers.
- Because Apple School Manager instructors and students are local users, there is no need to deploy Citrix Secure Hub to their devices.
- MAM enrollment that includes NetScaler Gateway authentication doesn't support local users (only Active Directory users). Therefore, XenMobile deploys only required VPP apps and iBooks to instructor and student devices.

Configure Apple School Manager and XenMobile Server

After you purchase iPads from Apple or from Apple Authorized Resellers or carriers: Follow the workflow in this section to set up your Apple School Manager account and devices. This workflow includes steps that you perform in the Apple School Manager portal and in the XenMobile console.

Step 1: Create your Apple School Manager account and complete the Setup Assistant

If you plan to upgrade from Apple Deployment Programs, see the Apple Support article, Prepare to upgrade to Apple School Manager. To create your Apple School Manager account, go to https://school.apple.com/ and follow the instructions to enroll. The first time that you log in to Apple School Manager, the Setup Assistant opens.

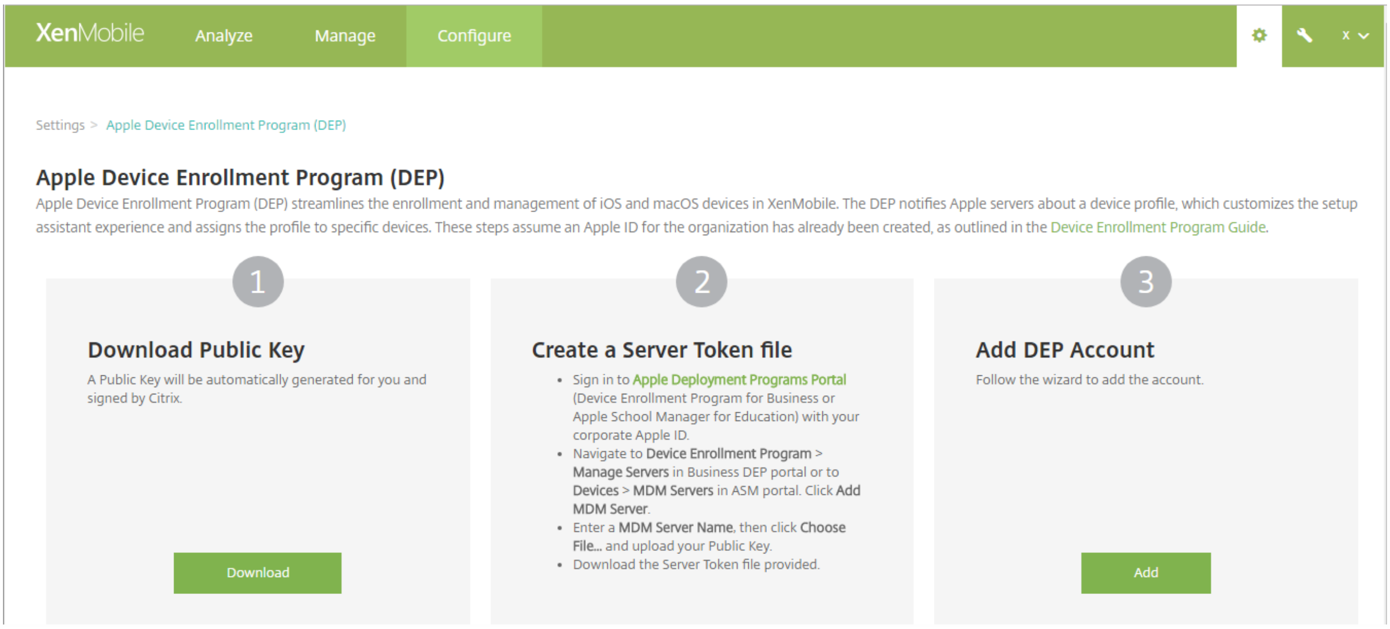
- For information about Apple School Manager prerequisites, the Setup Assistant, and management tasks, see the Apple School Manager help.
- When setting up an Apple School Manager, use a domain name that differs from the domain name for Active Directory. For example, prefix the domain name for Apple School Manager with something like **appleid**.
- When you connect Apple School Manager to your roster data, Apple School Manager creates Managed Apple IDs for instructors and students. Your roster data includes instructors, students, and classes. For information about adding roster data to Apple School Manager, see the articles under "Find staff, students and classes" in the Apple School Manager help.
- You can customize the Managed Apple ID format for your institution, as described under "Managed Apple IDs" in the Apple School Manager help.

  Important: Don't change Managed Apple IDs after you import Apple School Manager information into XenMobile Server.
- If you purchased devices through resellers or carriers, link those devices to Apple School Manager. For information, see the articles under "Manage devices" in the Apple School Manager help.

Step 2: Configure XenMobile Server as the MDM Server for Apple School Manager and configure device assignments

The Apple School Manager portal includes an **MDM Servers** tab. You need the public key file from XenMobile Server to complete that setup.

1. Download the public key for your XenMobile Server to your local computer: Log on to the XenMobile console and go to **Settings > Apple Device Enrollment Program (DEP)**.



Apple Device Enrollment Program (DEP)

Apple Device Enrollment Program (DEP) streamlines the enrollment and management of iOS and macOS devices in XenMobile. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. These steps assume an Apple ID for the organization has already been created, as outlined in the Device Enrollment Program Guide.

Download Public Key

A Public Key will be automatically generated for you and signed by Citrix.

Create a Server Token file

- Sign in to Apple Deployment Programs Portal (Device Enrollment Program for Business or Apple School Manager for Education) with your corporate Apple ID.
- Navigate to Device Enrollment Program > Manage Servers in Business DEP portal or to Devices > MDM Servers in ASM portal. Click Add MDM Server.
- Enter a MDM Server Name, then click Choose File... and upload your Public Key.
- Download the Server Token file provided.

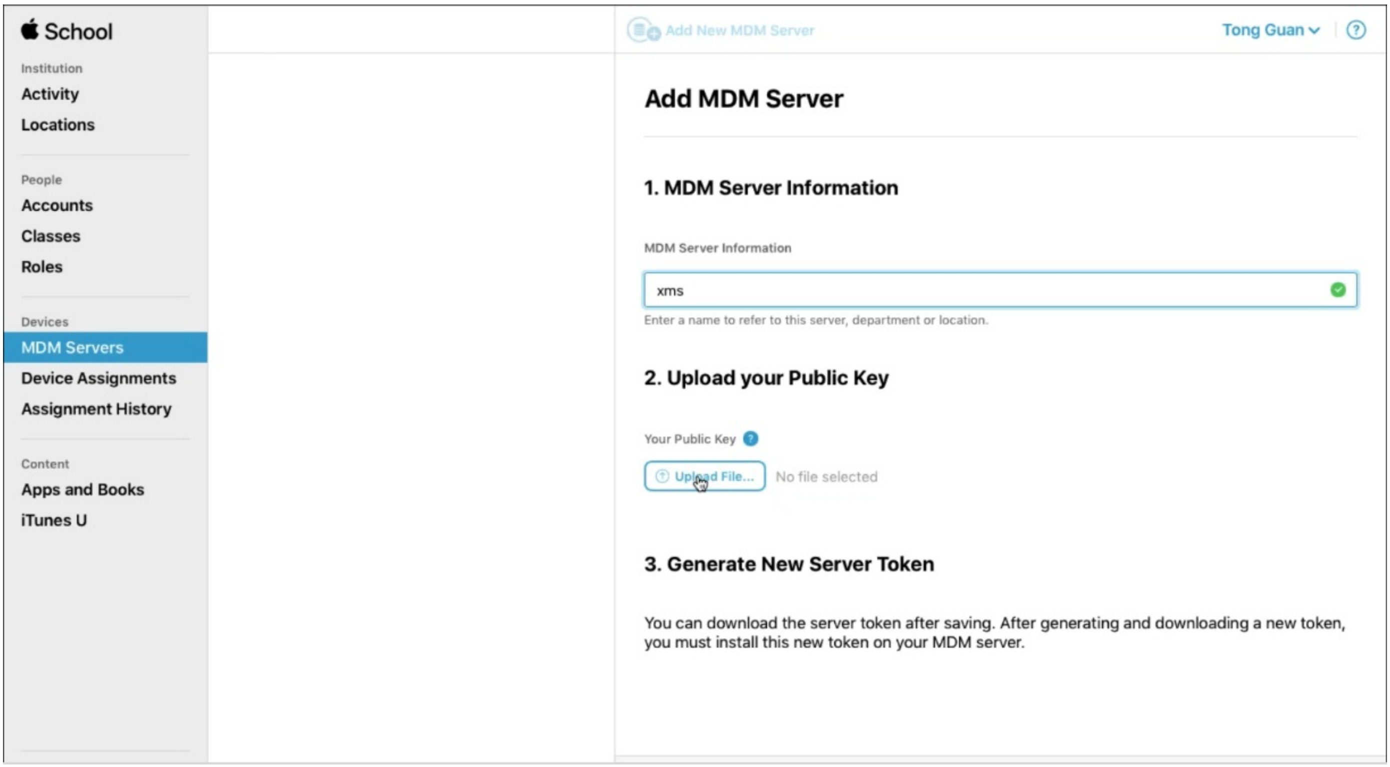
Add DEP Account

Follow the wizard to add the account.

2. Under **Download Public Key**, click **Download** and then save the PEM file.

3. In Apple School Manager portal, click **MDM Servers**, and type a name for XenMobile Server. The server name that you type is for your reference and is not the server URL or name.

4. Under **Upload your Public Key**, click **Upload File**.



Add MDM Server

1. MDM Server Information

MDM Server Information: xms

Enter a name to refer to this server, department or location.

2. Upload your Public Key

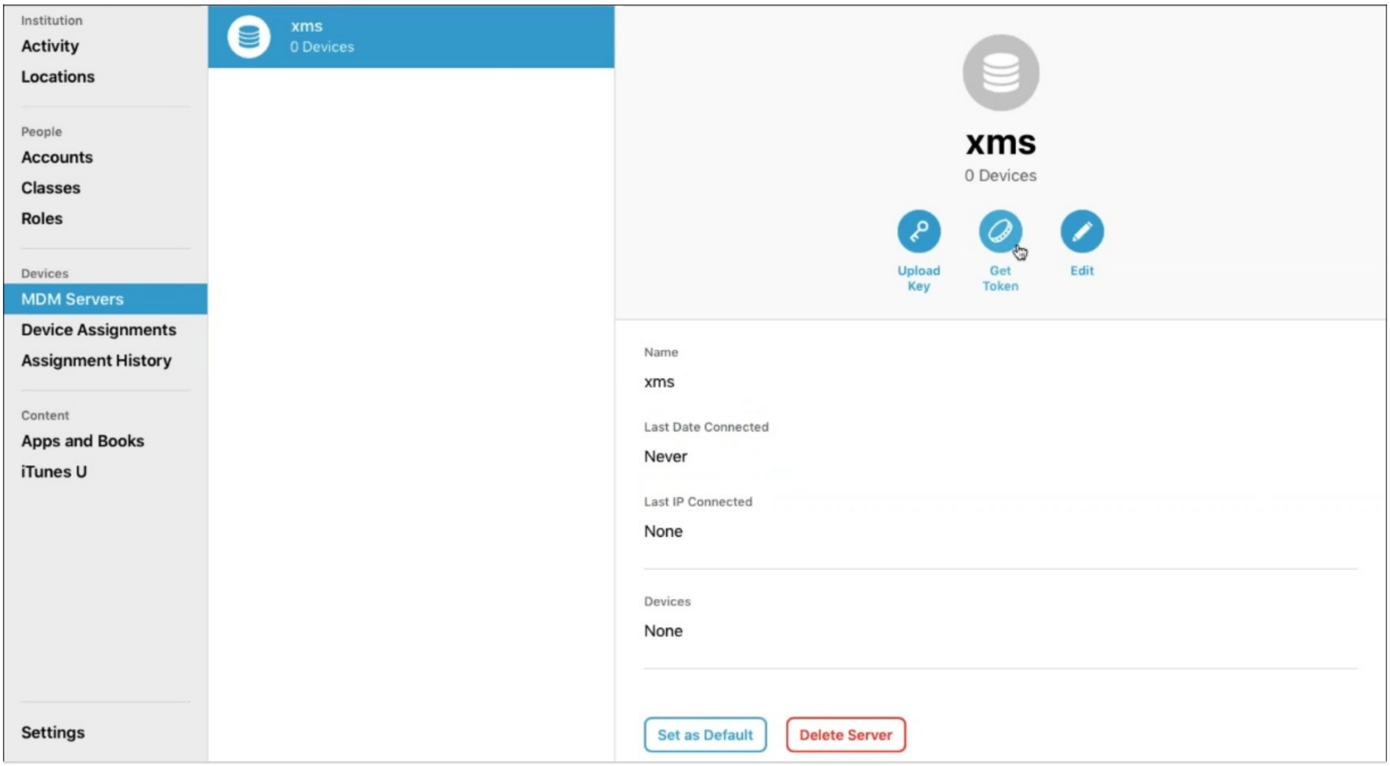
Your Public Key: No file selected

3. Generate New Server Token

You can download the server token after saving. After generating and downloading a new token, you must install this new token on your MDM server.

5. Upload the server key that you downloaded from XenMobile Server and then click **Save**.

6. Generate a server token: Click **Get Token** and then download the server token file to your computer.



Institution
Activity
Locations

People
Accounts
Classes
Roles

Devices
MDM Servers
Device Assignments
Assignment History

Content
Apps and Books
iTunes U

Settings

xms
0 Devices

xms
0 Devices

Upload Key
Get Token
Edit

Name
xms

Last Date Connected
Never

Last IP Connected
None

Devices
None

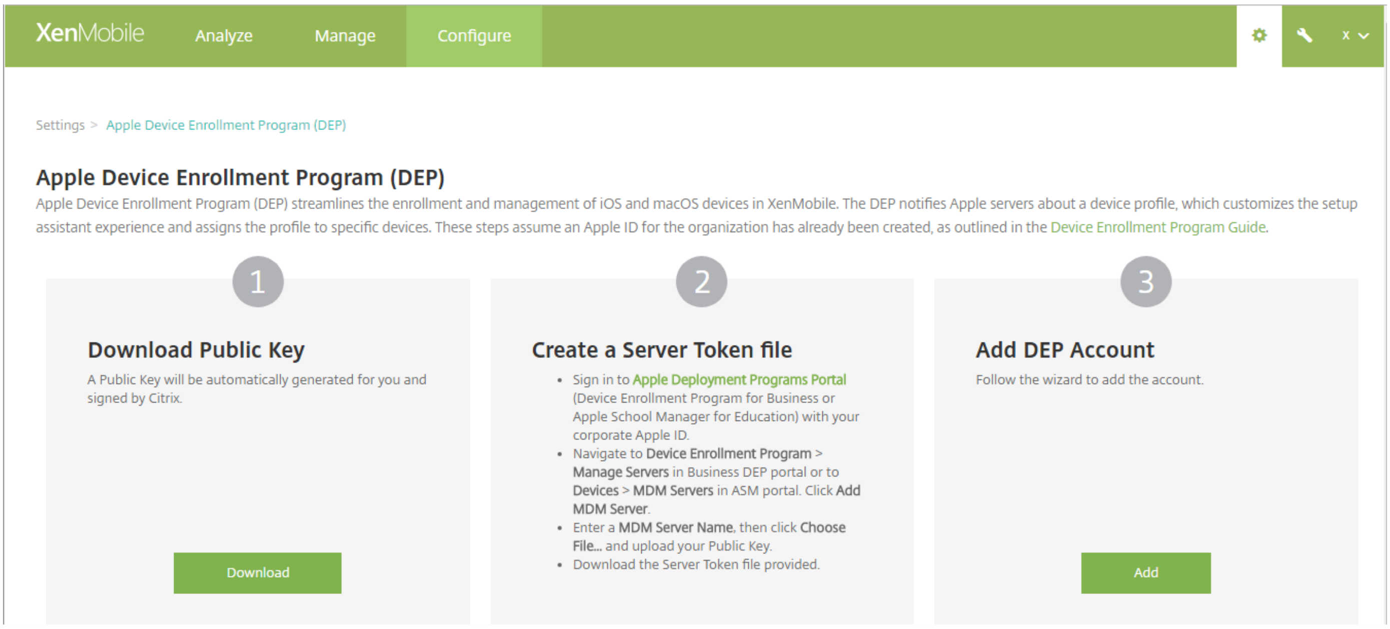
Set as Default
Delete Server

7. Click **Device Assignments**, choose how you want to assign devices and then provide the information requested. For information, see Assign devices in the Apple School Manager help.

8. Under **Choose Action**, in the **Perform Action** menu, click **Assign to Server**. Then, in the **MDM Server** menu, click the XenMobile Server to manage the devices and then click **Done**.

Step 3: Add the Apple School Manager account to XenMobile Server

1. In XenMobile console, go to **Settings > Apple Device Enrollment Program (DEP)** and under **Add DEP Account**, click **Add**.



XenMobile Analyze Manage Configure

Settings > Apple Device Enrollment Program (DEP)

Apple Device Enrollment Program (DEP)

Apple Device Enrollment Program (DEP) streamlines the enrollment and management of iOS and macOS devices in XenMobile. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. These steps assume an Apple ID for the organization has already been created, as outlined in the Device Enrollment Program Guide.

1

Download Public Key

A Public Key will be automatically generated for you and signed by Citrix.

Download

2

Create a Server Token file

- Sign in to Apple Deployment Programs Portal (Device Enrollment Program for Business or Apple School Manager for Education) with your corporate Apple ID.
- Navigate to Device Enrollment Program > Manage Servers in Business DEP portal or to Devices > MDM Servers in ASM portal. Click Add MDM Server.
- Enter a MDM Server Name, then click Choose File... and upload your Public Key.
- Download the Server Token file provided.

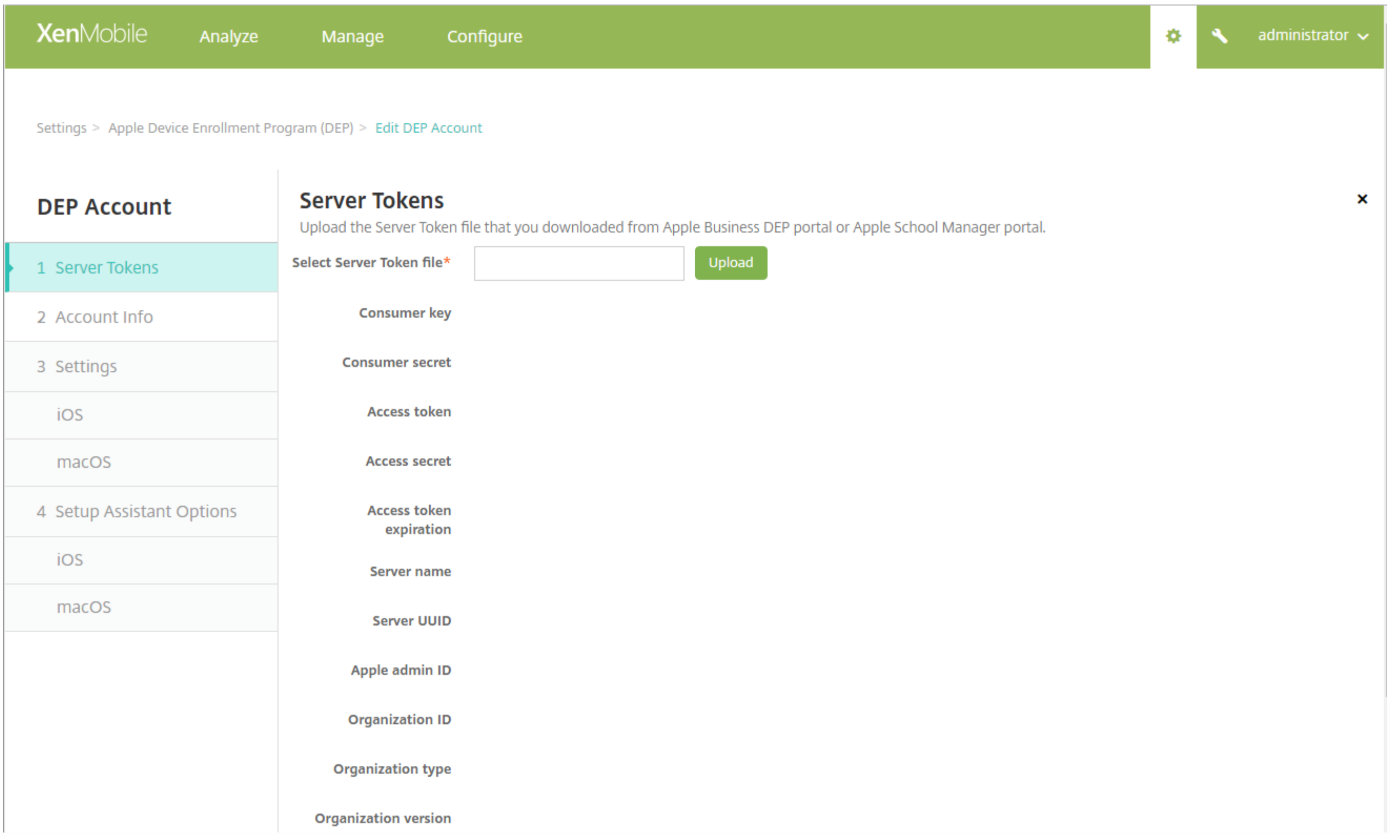
3

Add DEP Account

Follow the wizard to add the account.

Add

2. In the **Server Tokens** page, click **Upload** and choose the server token (.p7m) file that you downloaded from the Apple School Manager portal. The token information appears.



Settings > Apple Device Enrollment Program (DEP) > Edit DEP Account

Server Tokens

Upload the Server Token file that you downloaded from Apple Business DEP portal or Apple School Manager portal.

Select Server Token file*

Consumer key

Consumer secret

Access token

Access secret

Access token expiration

Server name

Server UUID

Apple admin ID

Organization ID

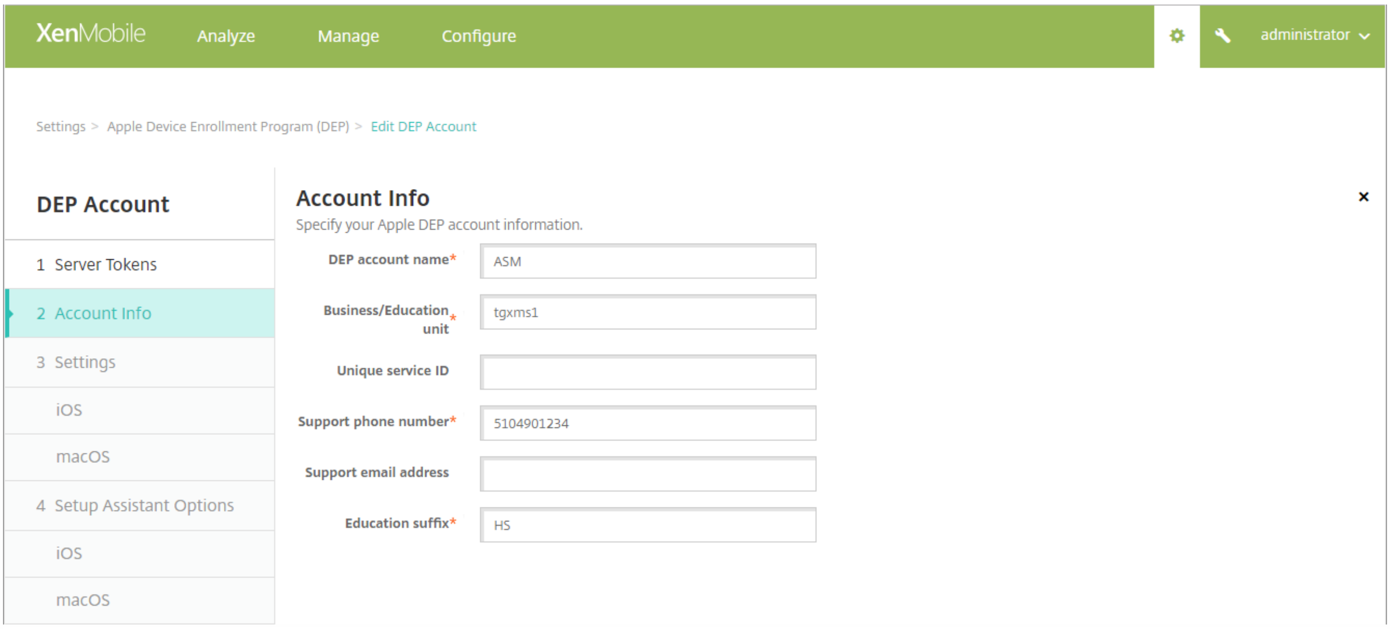
Organization type

Organization version

Notes:

- **Organization ID** is your customer ID for DEP.
- Apple School Manager accounts have an **Organization type** of **Education** and an **Organization version** of **v2**.

3. In the **Account Info** page, specify the following settings.



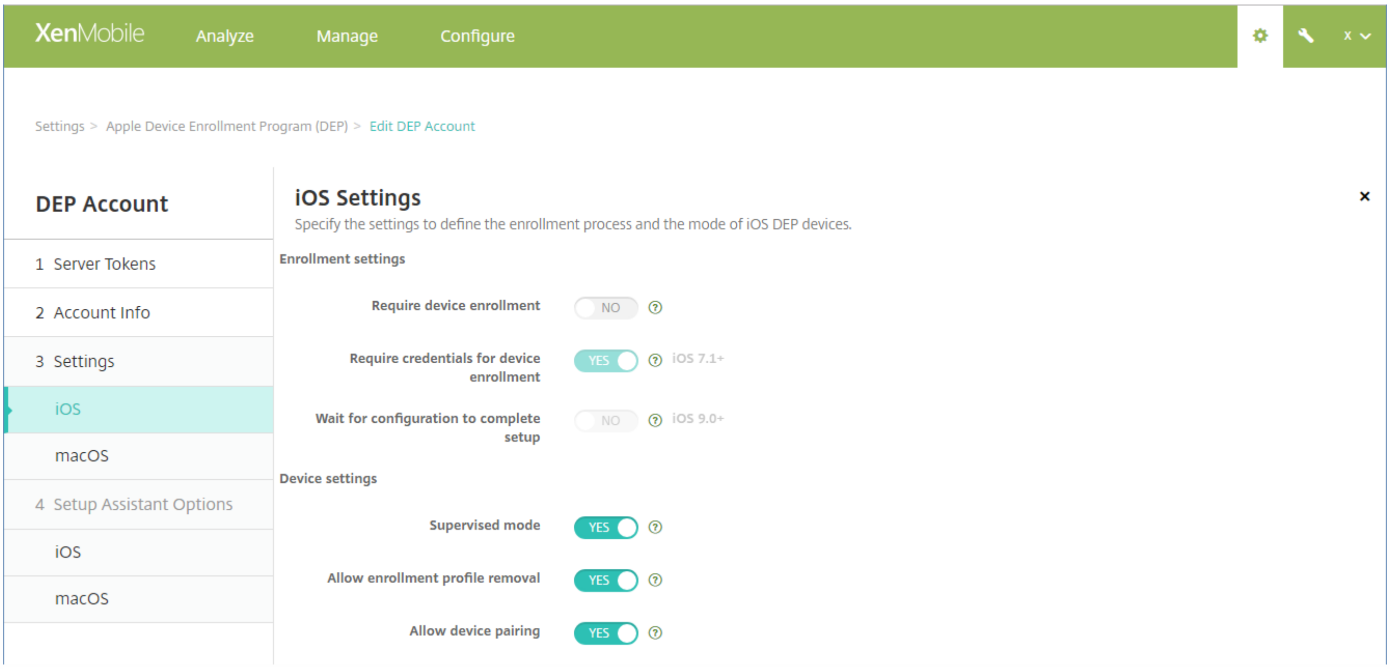
Account Info

Specify your Apple DEP account information.

DEP account name*	ASM
Business/Education unit*	tgxms1
Unique service ID	
Support phone number*	5104901234
Support email address	
Education suffix*	HS

- **DEP account name**: A unique name for this DEP account. Use names that reflect how you organize DEP 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 may 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 Apple School Manager DEP account. (The VPP suffix flags apps and iBooks for a given VPP account.) The recommendation is to use the same suffix for both accounts, Apple School Manager DEP and Apple School Manager VPP.

4. Click **Next**. In **iOS Settings**, specify the following settings.



iOS Settings

Specify the settings to define the enrollment process and the mode of iOS DEP devices.

Enrollment settings

Require device enrollment: NO

Require credentials for device enrollment: YES iOS 7.1+

Wait for configuration to complete setup: NO iOS 9.0+

Device settings

Supervised mode: YES

Allow enrollment profile removal: YES

Allow device pairing: YES

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 DEP setup. For Apple School Manager integration with XenMobile Server, this setting is **Yes** by default.

- **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 Apple School Manager integration with XenMobile Server, 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.

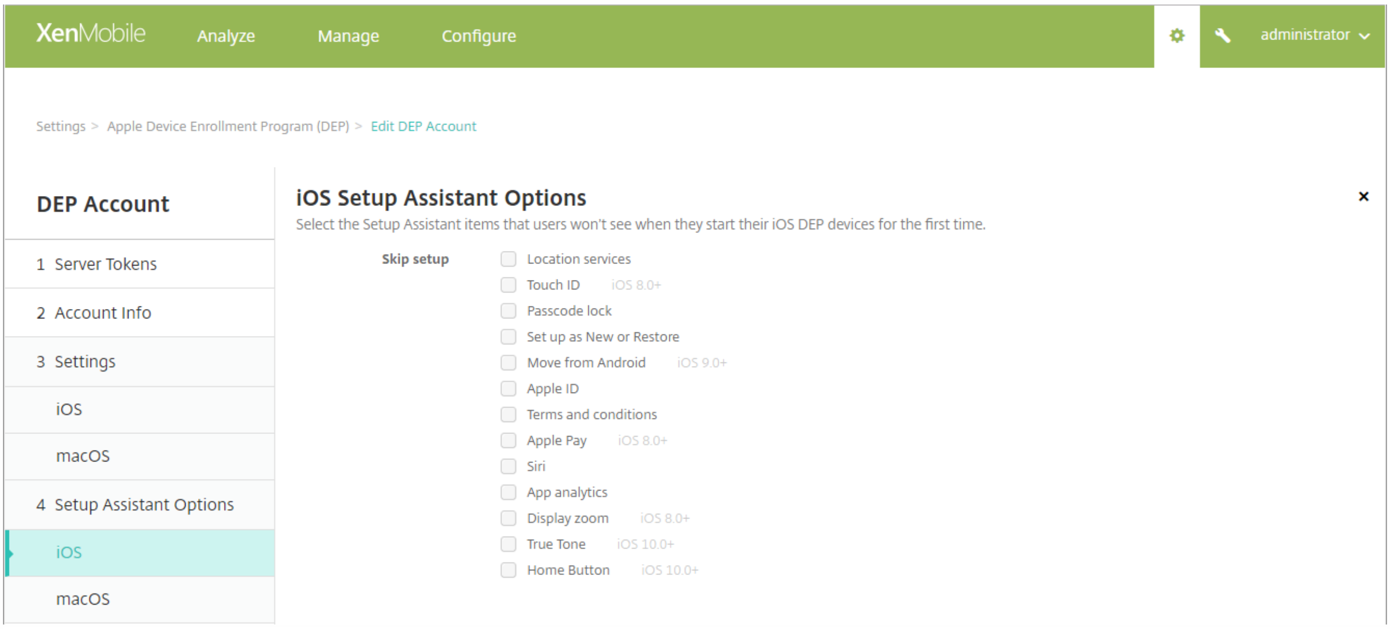
- **Allow enrollment profile removal**: For Apple School Manager integration, allow devices to use a profile that you can remove remotely. Change this setting to **Yes**.

- **Allow device pairing**: For Apple School Manager 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.



Settings > Apple Device Enrollment Program (DEP) > Edit DEP Account

DEP Account

1 Server Tokens

2 Account Info

3 Settings

iOS

macOS

4 Setup Assistant Options

iOS

macOS

iOS Setup Assistant Options

Select the Setup Assistant items that users won't see when they start their iOS DEP devices for the first time.

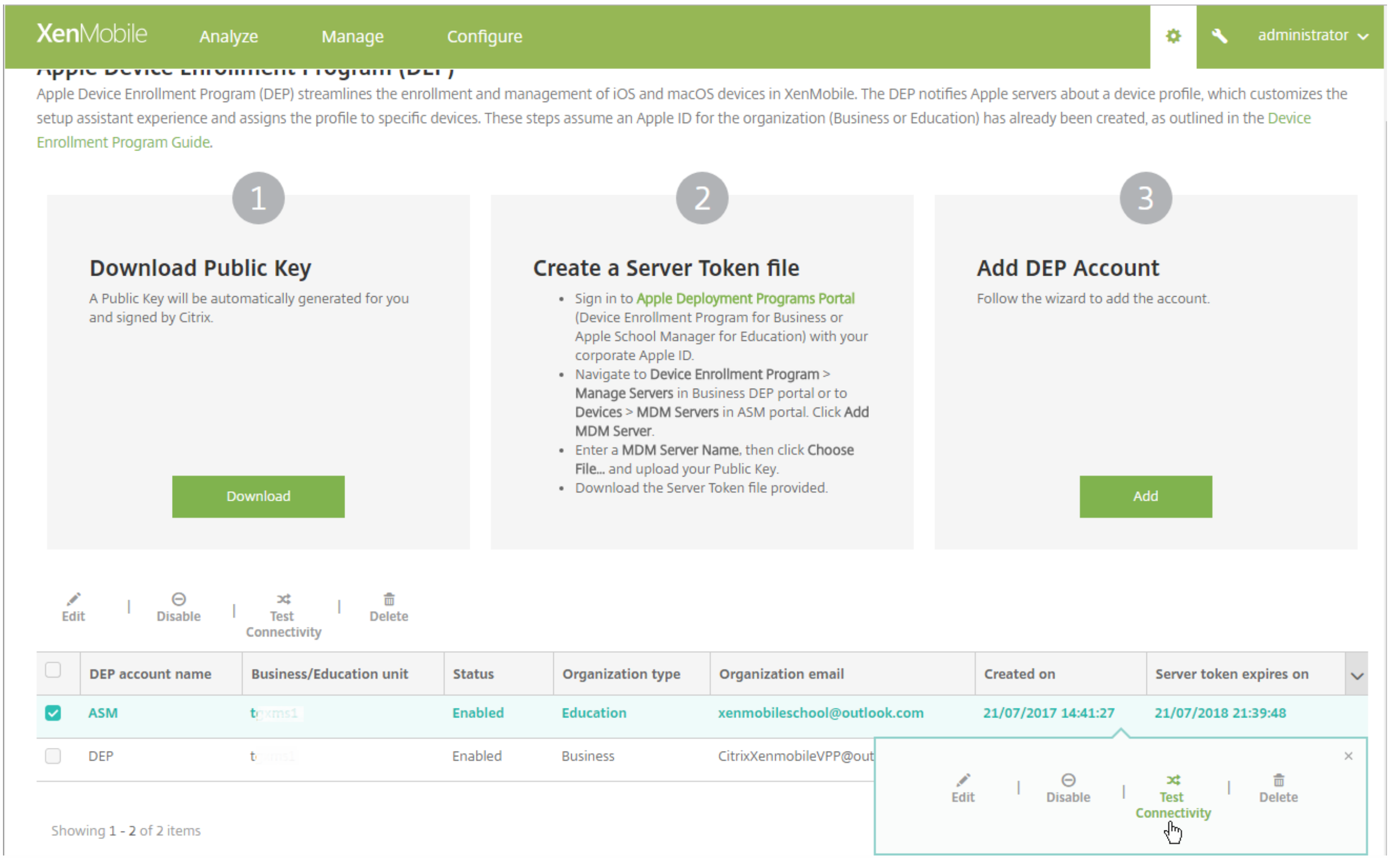
Skip setup

- □ Location services
- □ Touch ID iOS 8.0+
- □ Passcode lock
- □ Set up as New or Restore
- □ Move from Android iOS 9.0+
- □ Apple ID
- □ Terms and conditions
- □ Apple Pay iOS 8.0+
- □ Siri
- □ App analytics
- □ Display zoom iOS 8.0+
- □ True Tone iOS 10.0+
- □ Home Button iOS 10.0+

- **Location services**: Set up the location service on the device.
- **Touch ID**: Set up Touch ID on iOS 8.0 and later 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 9 or later 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 8.0 and later 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 8.0 or later devices.
- **True Tone**: Set up the True Tone Display on iOS 10.0 devices (minimum version).

- **Home Button**: Set up the Home Button screen sensitivity on iOS 10.0 devices (minimum version).

6. The DEP account appears on **Settings > Apple Device Enrollment Program (DEP)**. To test connectivity between XenMobile Server and your Apple School Manager account, select the account and click **Test Connectivity**.



Apple Device Enrollment Program (DEP)

Apple Device Enrollment Program (DEP) streamlines the enrollment and management of iOS and macOS devices in XenMobile. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. These steps assume an Apple ID for the organization (Business or Education) has already been created, as outlined in the Device Enrollment Program Guide.

1 **Download Public Key**

A Public Key will be automatically generated for you and signed by Citrix.

Download

2 **Create a Server Token file**

- Sign in to Apple Deployment Programs Portal (Device Enrollment Program for Business or Apple School Manager for Education) with your corporate Apple ID.
- Navigate to **Device Enrollment Program** > **Manage Servers** in Business DEP portal or to **Devices** > **MDM Servers** in ASM portal. Click **Add MDM Server**.
- Enter a **MDM Server Name**, then click **Choose File...** and upload your Public Key.
- Download the Server Token file provided.

3 **Add DEP Account**

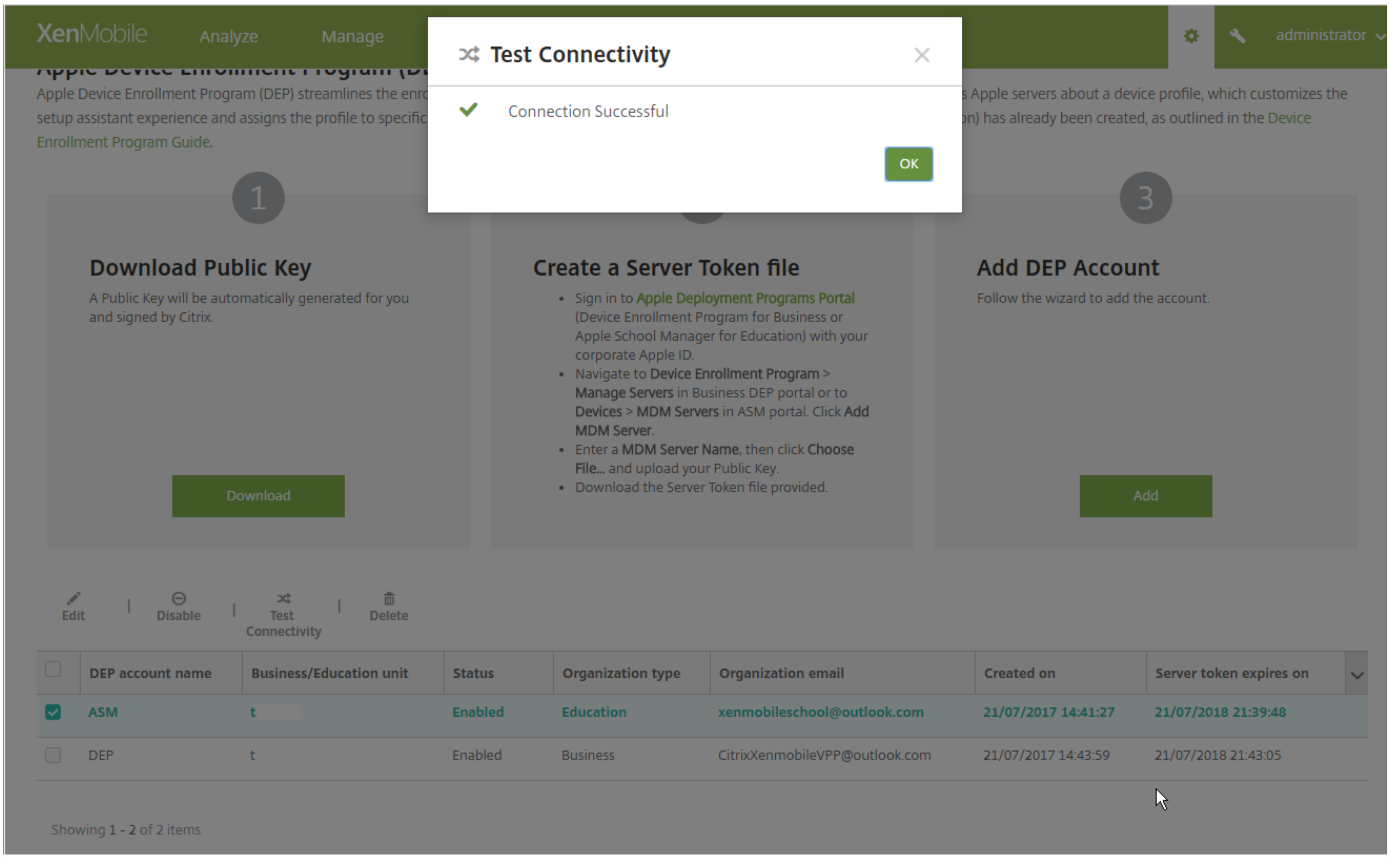
Follow the wizard to add the account.

Add

☐	DEP account name	Business/Education unit	Status	Organization type	Organization email	Created on	Server token expires on
☑	ASM	t[redacted]	Enabled	Education	xenmobileschool@outlook.com	21/07/2017 14:41:27	21/07/2018 21:39:48
☐	DEP	t[redacted]	Enabled	Business	CitrixXenmobileVPP@out		

Showing 1 - 2 of 2 items

A status message appears.



Test Connectivity

✓ Connection Successful

OK

Apple Device Enrollment Program (DEP) streamlines the enro… s Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific… n) has already been created, as outlined in the Device Enrollment Program Guide.

1 Download Public Key

A Public Key will be automatically generated for you and signed by Citrix.

Download

Create a Server Token file

- Sign in to Apple Deployment Programs Portal (Device Enrollment Program for Business or Apple School Manager for Education) with your corporate Apple ID.
- Navigate to **Device Enrollment Program > Manage Servers** in Business DEP portal or to **Devices > MDM Servers** in ASM portal. Click **Add MDM Server**.
- Enter a **MDM Server Name**, then click **Choose File...** and upload your Public Key.
- Download the Server Token file provided.

3 Add DEP Account

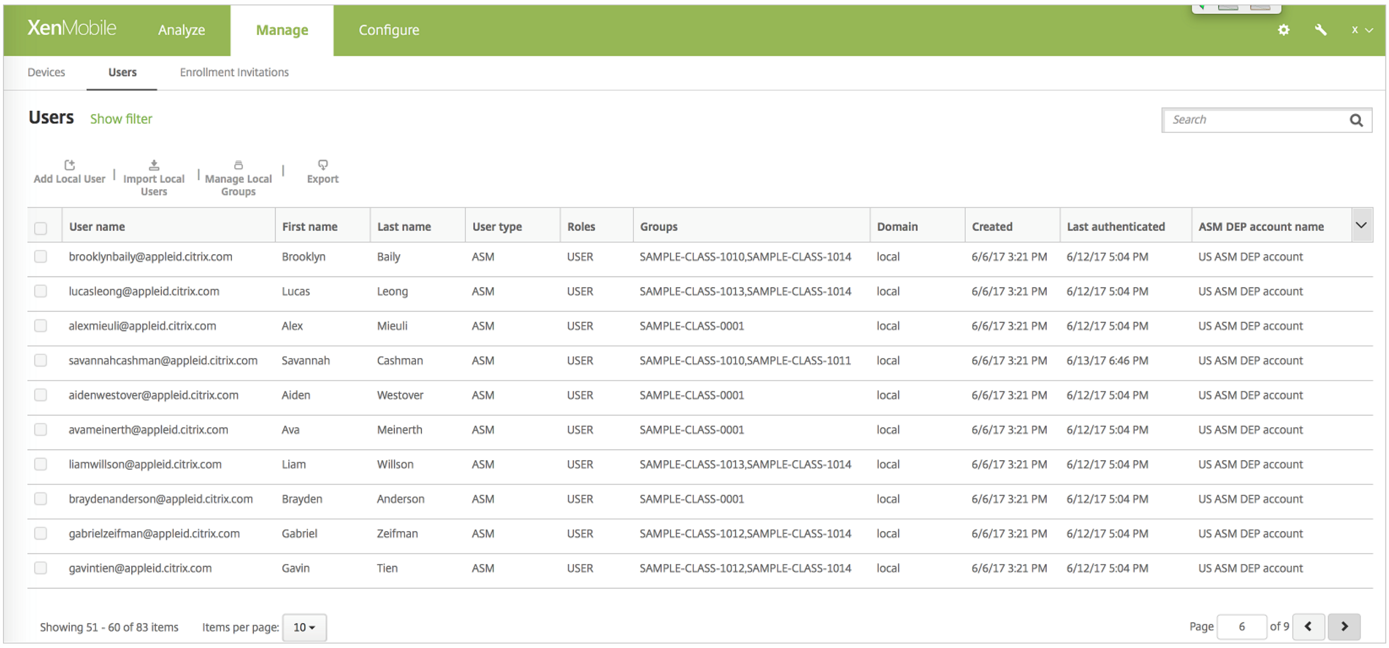
Follow the wizard to add the account.

Add

□	DEP account name	Business/Education unit	Status	Organization type	Organization email	Created on	Server token expires on
☑	ASM	t [redacted]	Enabled	Education	xenmobileschool@outlook.com	21/07/2017 14:41:27	21/07/2018 21:39:48
□	DEP	t	Enabled	Business	CitrixXenmobileVPP@outlook.com	21/07/2017 14:43:59	21/07/2018 21:43:05

Showing 1 - 2 of 2 items

After a few minutes, the user accounts from Apple School Manager appear on **Manage > Users** page. XenMobile Server 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**.



Users Show filter

□	User name	First name	Last name	User type	Roles	Groups	Domain	Created	Last authenticated	ASM DEP account name
□	brooklynbaily@appleid.citrix.com	Brooklyn	Baily	ASM	USER	SAMPLE-CLASS-1010,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
□	lucasleong@appleid.citrix.com	Lucas	Leong	ASM	USER	SAMPLE-CLASS-1013,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
□	alexmieuli@appleid.citrix.com	Alex	Mieuli	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
□	savannahcashman@appleid.citrix.com	Savannah	Cashman	ASM	USER	SAMPLE-CLASS-1010,SAMPLE-CLASS-1011	local	6/6/17 3:21 PM	6/13/17 6:46 PM	US ASM DEP account
□	aidenwestover@appleid.citrix.com	Aiden	Westover	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
□	avameinerth@appleid.citrix.com	Ava	Meinerth	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
□	liamwillson@appleid.citrix.com	Liam	Willson	ASM	USER	SAMPLE-CLASS-1013,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
□	braydenanderson@appleid.citrix.com	Brayden	Anderson	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
□	gabrielzeifman@appleid.citrix.com	Gabriel	Zeifman	ASM	USER	SAMPLE-CLASS-1012,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
□	gavintien@appleid.citrix.com	Gavin	Tien	ASM	USER	SAMPLE-CLASS-1012,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account

Showing 51 - 60 of 83 items Items per page: 10

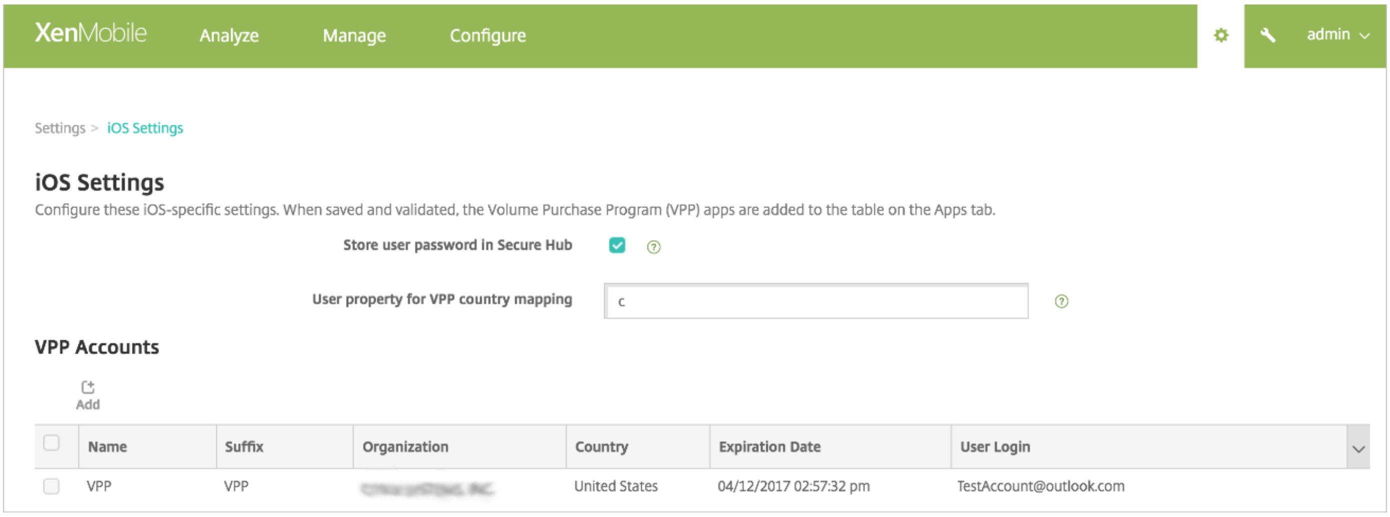
Page 6 of 9

To find all users for a given Apple School Manager DEP account, type the account name in the user search filter.

Step 4: Configure an Education VPP account for Apple School Manager

In this section, you point XenMobile to the VPP account that you use to purchase VPP licenses for apps and iBooks.

1. To configure an Education VPP account for Apple School Manager, follow the instructions in iOS Volume Purchase Program. The Add a VPP account screen requires that you supply a Company Token. Download your token directly from your Education VPP account (https://volume.itunes.apple.com/us/store) and paste it into the **Add a VPP account** screen.



iOS Settings

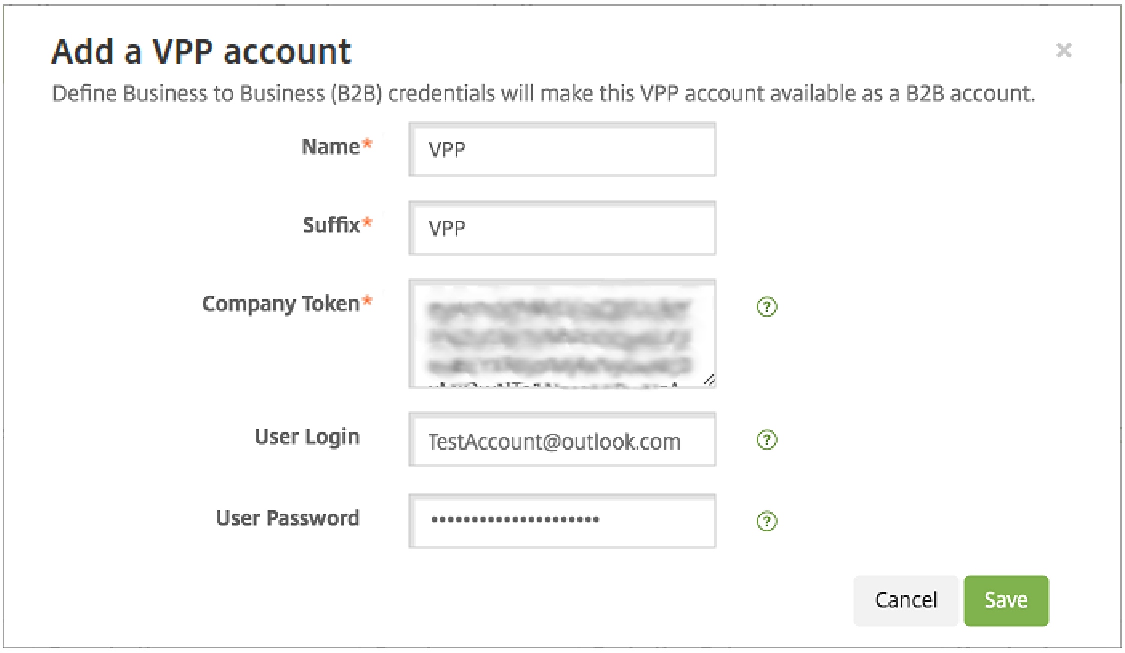
Configure these iOS-specific settings. When saved and validated, the Volume Purchase Program (VPP) apps are added to the table on the Apps tab.

Store user password in Secure Hub ☑

User property for VPP country mapping: c

VPP Accounts

□	Name	Suffix	Organization	Country	Expiration Date	User Login
□	VPP	VPP	[redacted]	United States	04/12/2017 02:57:32 pm	TestAccount@outlook.com



Add a VPP account

Define Business to Business (B2B) credentials will make this VPP account available as a B2B account.

Name*	VPP
Suffix*	VPP
Company Token*	[redacted]
User Login	TestAccount@outlook.com
User Password	••••••••••••••••••••••

2. Wait a few minutes for the VPP licenses to import into XenMobile Server.

Step 5: Add passwords for Apple School Manager users

After you add an Apple School Manager DEP account, XenMobile Server imports classes and users from Apple School Manager. XenMobile treats classes as local groups and uses the term "group" in the console. If a class has a group name in Apple School Manager, XenMobile assigns the group name to the class. Otherwise, XenMobile uses the source system ID for the group name. XenMobile doesn't use the course name for the class name because course names in Apple School Manager aren't unique.

XenMobile uses the Managed Apple IDs to create local users with the user type **ASM**. The users are local because Apple School Manager creates the credentials independently of all external data sources. As a result, XenMobile doesn't use a directory server to authenticate these new users.

Apple School Manager doesn't send temporary user passwords to XenMobile Server. You can import them from a CSV file or add them manually. To import temporary user passwords:

1. Obtain the CSV file generated by Apple School Manager 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 XenMobile Server. There is no constraint on the password type for this purpose.

   The format of an entry in the CSV file is as follows: elizabethabeles@appleid.citrix.com,Elizabeth,Anne,Abeles,password

   Where:

   User: elizabethabeles@appleid.citrix.com

   First name: Elizabeth

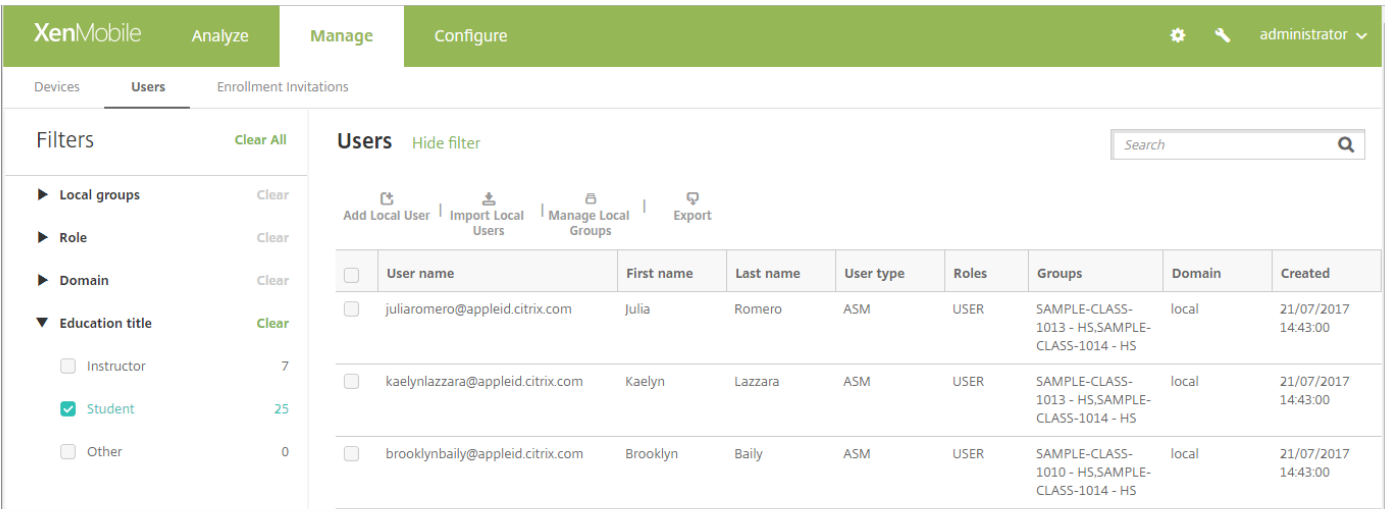
   Middle name: Anne

   Last name: Abeles

   Password: password
3. In the XenMobile console, click **Manage > Users**. The **Users** page appears.

   The following **Manage > Users** screen sample shows a list of users imported from Apple School Manager. In the **Users** list:

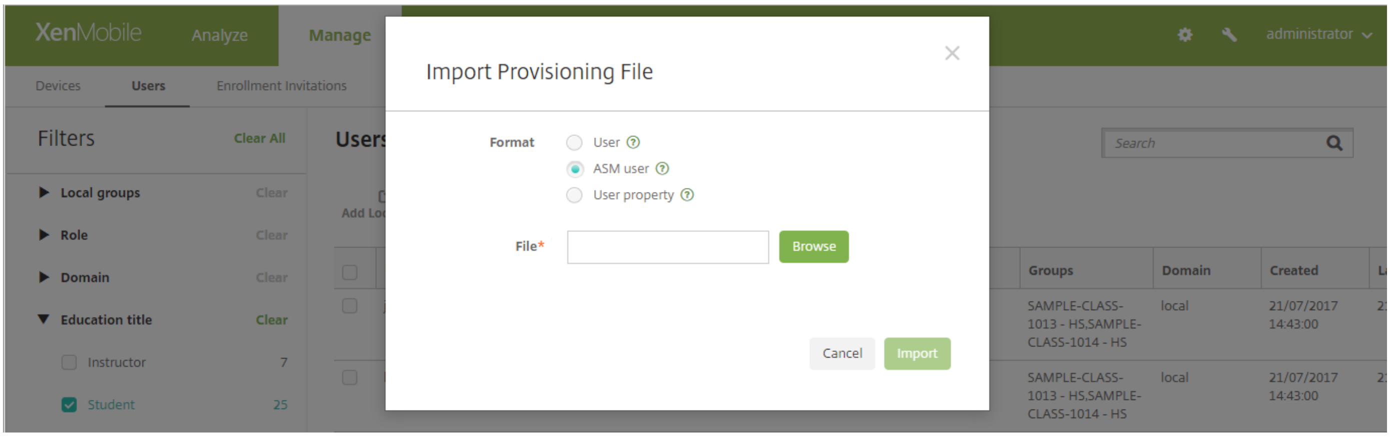
   - **User name** shows the managed Apple ID.
   - User type is **ASM**, to indicate the account originated from Apple School Manager.
   - **Groups** show the classes.



□	User name	First name	Last name	User type	Roles	Groups	Domain	Created
□	juliaromero@appleid.citrix.com	Julia	Romero	ASM	USER	SAMPLE-CLASS-1013 - HS,SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00
□	kaelynlazzara@appleid.citrix.com	Kaelyn	Lazzara	ASM	USER	SAMPLE-CLASS-1013 - HS,SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00
□	brooklynbaily@appleid.citrix.com	Brooklyn	Baily	ASM	USER	SAMPLE-CLASS-1010 - HS,SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00

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**.

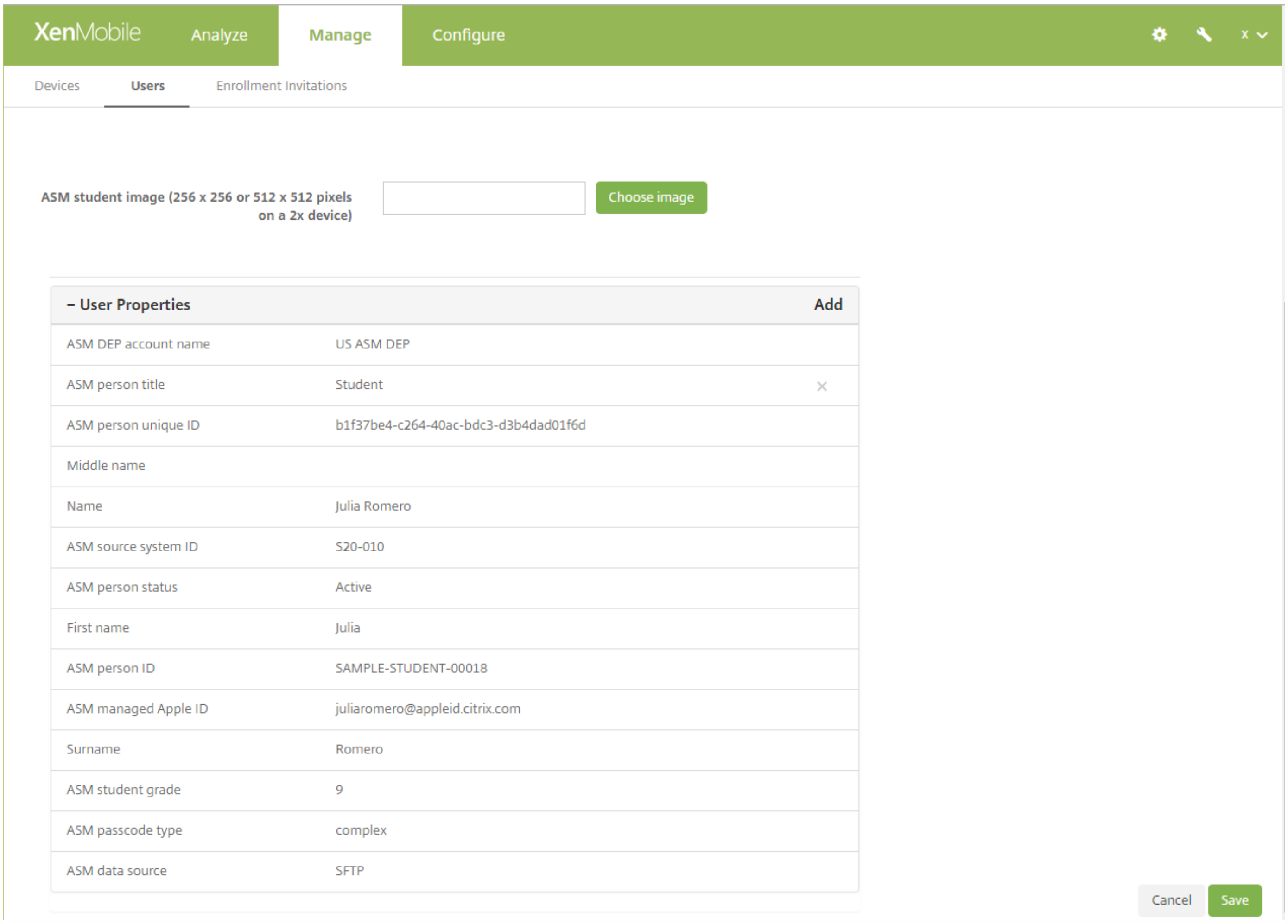


Import Provisioning File

Format: ○ User ● ASM user ○ User property

File*

6. To view the properties for a local user, select the user and then click **Edit**.



ASM student image (256 x 256 or 512 x 512 pixels on a 2x device)

– User Properties

ASM DEP account name	US ASM DEP
ASM person title	Student
ASM person unique ID	b1f37be4-c264-40ac-bdc3-d3b4dad01f6d
Middle name	
Name	Julia Romero
ASM source system ID	S20-010
ASM person status	Active
First name	Julia
ASM person ID	SAMPLE-STUDENT-00018
ASM managed Apple ID	juliaromero@appleid.citrix.com
Surname	Romero
ASM student grade	9
ASM passcode type	complex
ASM data source	SFTP

In addition to the name properties, these Apple School Manager properties appear:

- **ASM DEP account**: The name you gave the account in XenMobile Server.
- **ASM person title**: Either Instructor, Student or Other.
- **ASM person unique ID**: Unique identifier for the user.
- **ASM source system ID**: An identifier configured by your organization 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 managed Apple ID**: A Managed Apple ID might include your institution name and **appleid**. For example, the ID might resemble johnappleseed@appleid.myschool.edu. XenMobile Server requires a Managed Apple ID for authentication.
- **ASM student grade**: Student grade information (not used by instructors).
- **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 data source**: The data source of the class, such as **CSV** or **SFTP**.

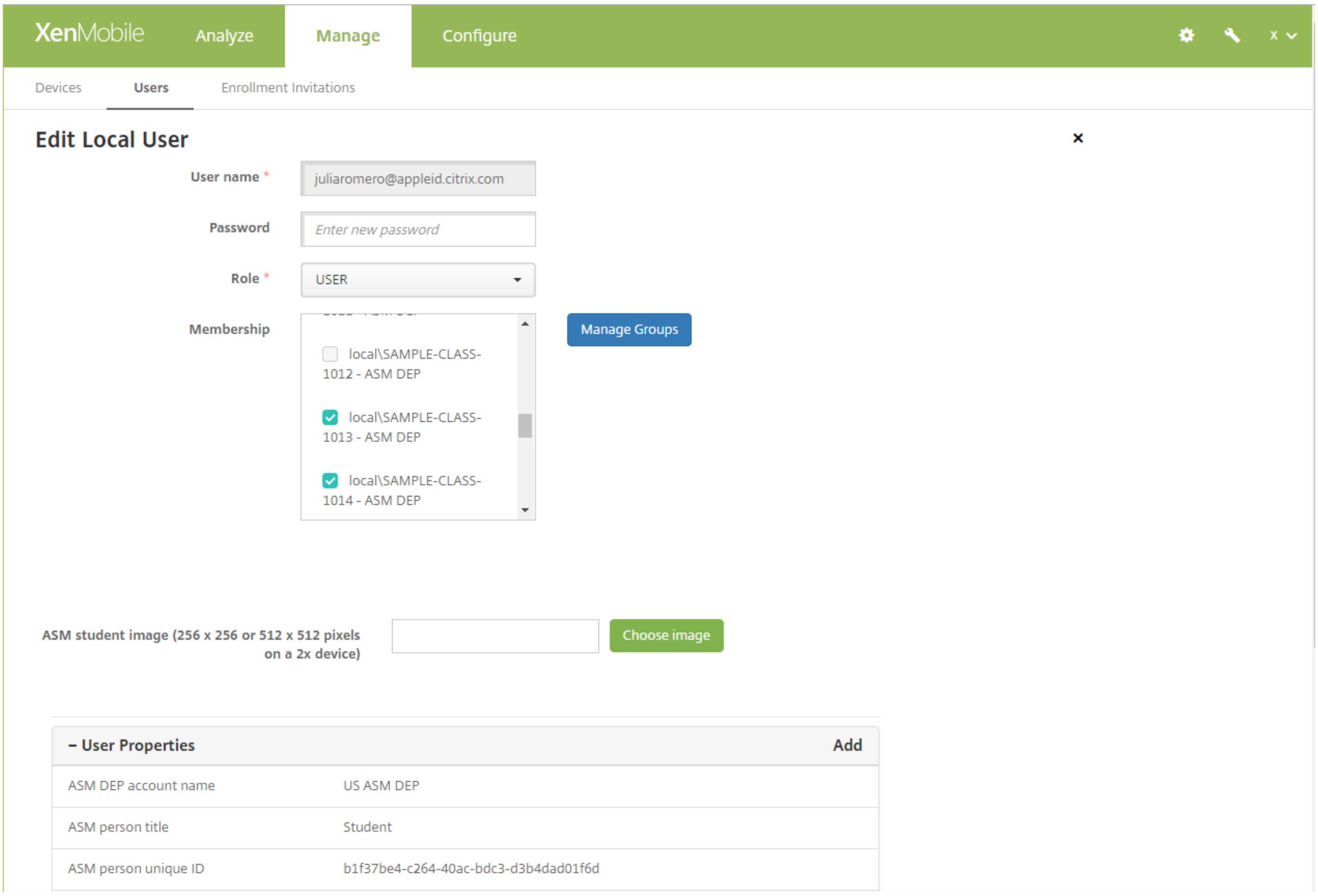
Step 6: Optionally add photos of students

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**.



Edit Local User

User name * juliaromero@appleid.citrix.com

Password Enter new password

Role * USER

Membership

□ local\SAMPLE-CLASS-1012 - ASM DEP

☑ local\SAMPLE-CLASS-1013 - ASM DEP

☑ local\SAMPLE-CLASS-1014 - ASM DEP

ASM student image (256 x 256 or 512 x 512 pixels on a 2x device)

– User Properties

ASM DEP account name	US ASM DEP
ASM person title	Student
ASM person unique ID	b1f37be4-c264-40ac-bdc3-d3b4dad01f6d

Step 7: Plan and add resources and delivery groups to XenMobile Server

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, VPP 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.

- VPP apps:

  XenMobile requires that you deploy VPP apps as required apps for education users. XenMobile Server currently doesn't support deploying such VPP apps as optional.

  If you use the Apple Classroom app, deploy it only to instructor devices.

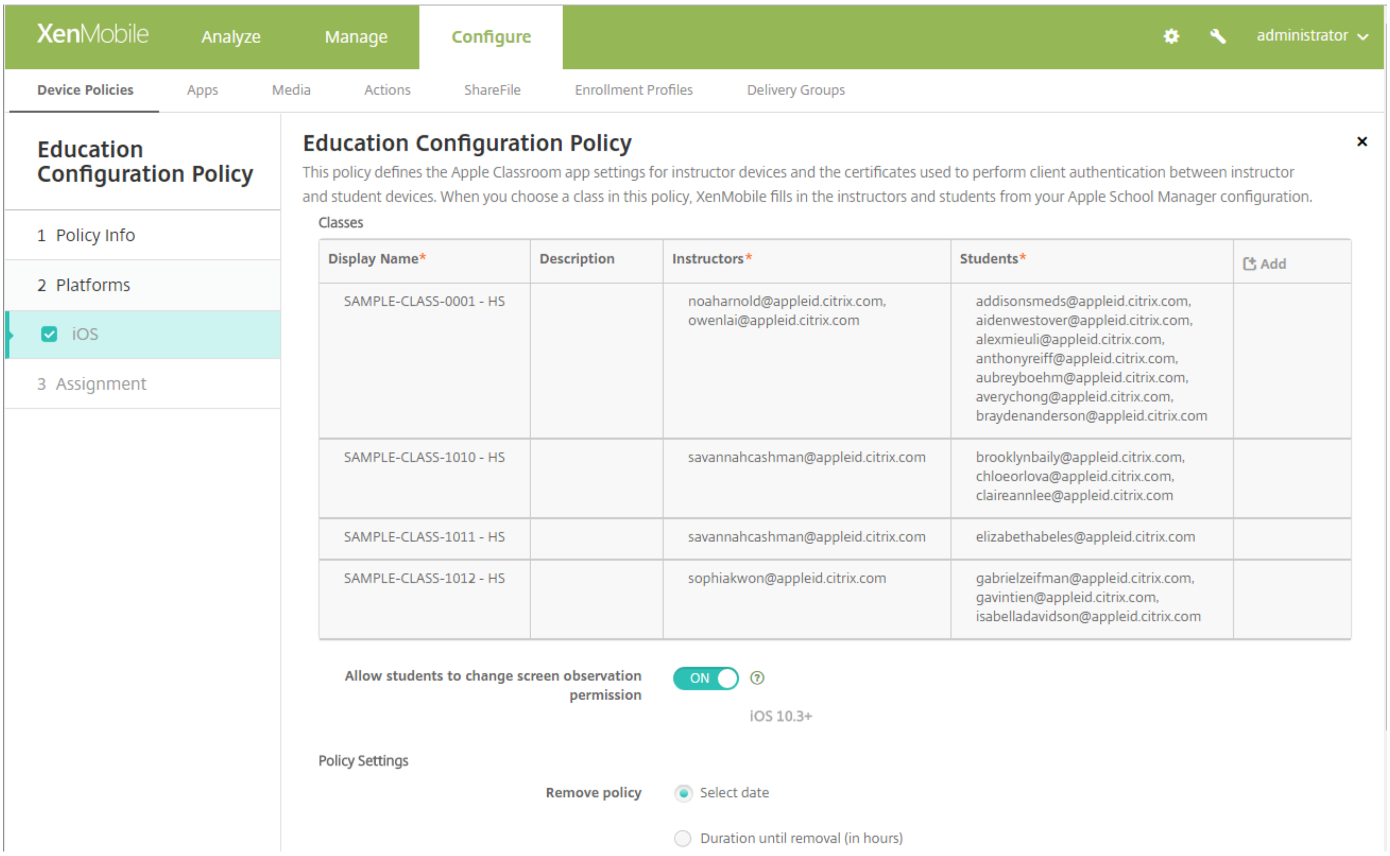
  Deploy any other apps that you want to provide to instructors or students. This solution doesn't use Citrix Secure Hub app, so there's no need to deploy it to instructors or students.

- VPP iBooks:

  After XenMobile Server connects to your Apple School Manager VPP account, your purchased iBooks appear in the XenMobile console, in **Configure > Media**. The iBooks listed on that page are available to add to delivery groups. Currently, XenMobile Server 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 XenMobile 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.

   Education Configuration Policy

   This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

   Classes

Display Name*	Description	Instructors*	Students*
SAMPLE-CLASS-0001 - HS		noaharnold@appleid.citrix.com, owenlai@appleid.citrix.com	addisonsmeds@appleid.citrix.com, aidenwestover@appleid.citrix.com, alexmieuli@appleid.citrix.com, anthonyreiff@appleid.citrix.com, aubreyboehm@appleid.citrix.com, averychong@appleid.citrix.com, braydenanderson@appleid.citrix.com
SAMPLE-CLASS-1010 - HS		savannahcashman@appleid.citrix.com	brooklynbaily@appleid.citrix.com, chloeorlova@appleid.citrix.com, claireannlee@appleid.citrix.com
SAMPLE-CLASS-1011 - HS		savannahcashman@appleid.citrix.com	elizabethabeles@appleid.citrix.com
SAMPLE-CLASS-1012 - HS		sophiakwon@appleid.citrix.com	gabrielzeifman@appleid.citrix.com, gavintien@appleid.citrix.com, isabelladavidson@appleid.citrix.com

   Allow students to change screen observation permission: ON

   iOS 10.3+

   Policy Settings

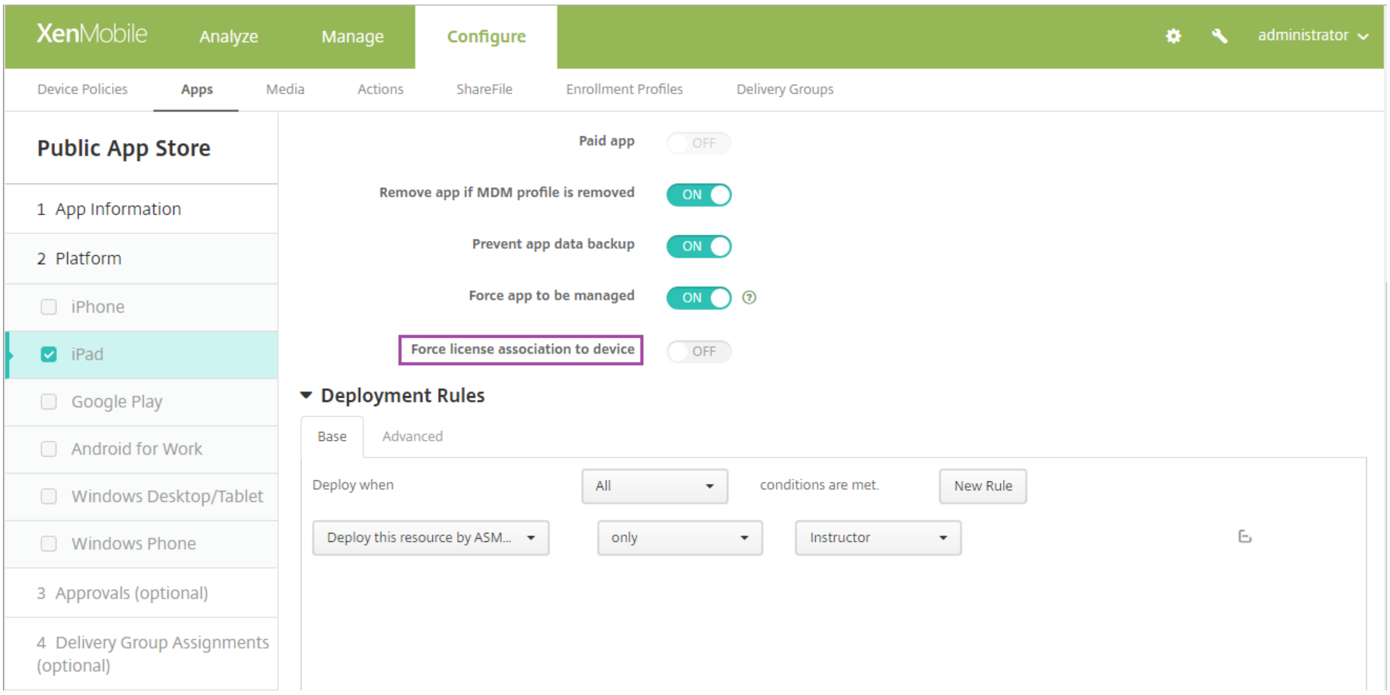
   Remove policy: ● Select date ○ Duration until removal (in hours)

   For information about device policies, see Device policies and the individual policy articles.

2. Configure apps (**Configure > Apps**) and iBooks (**Configure > Media**):

   - By default, XenMobile assigns apps and iBooks at the user level. During first-time deployment, instructors and students receive a prompt to register to VPP. After accepting the invitation, users receive their VPP apps and iBooks at the next deployment (within six hours). Citrix recommends that you force the deployment of apps and iBooks to new VPP 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 VPP program.



Paid app: OFF

Remove app if MDM profile is removed: ON

Prevent app data backup: ON

Force app to be managed: ON

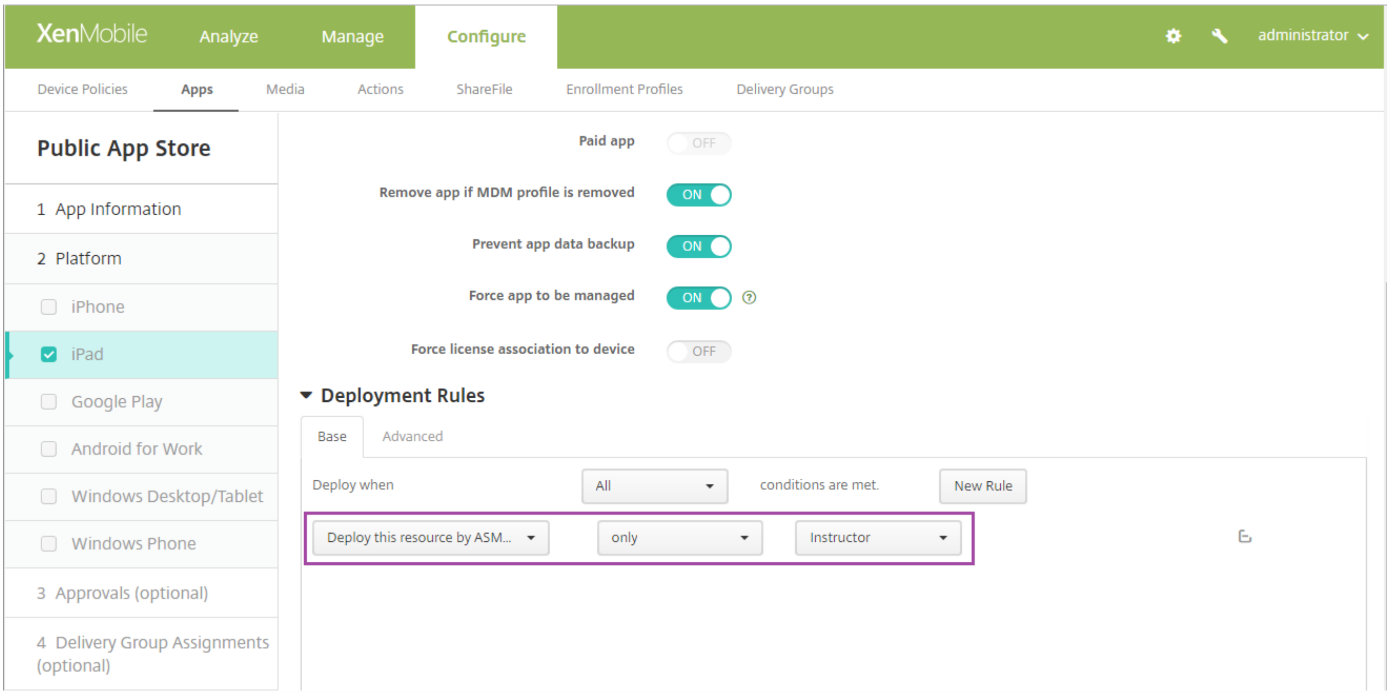
Force license association to device: OFF

☐ iPhone ☑ iPad ☐ Google Play ☐ Android for Work ☐ Windows Desktop/Tablet ☐ Windows Phone

Deploy when All conditions are met.

Deploy this resource by ASM... only Instructor

- To deploy an app only to instructors, select a delivery group that includes only instructors or use the following deployment rule:
  Deploy this resource by ASM DEP device type
  only
  Instructor



Paid app: OFF

Remove app if MDM profile is removed: ON

Prevent app data backup: ON

Force app to be managed: ON

Force license association to device: OFF

☐ iPhone ☑ iPad ☐ Google Play ☐ Android for Work ☐ Windows Desktop/Tablet ☐ Windows Phone

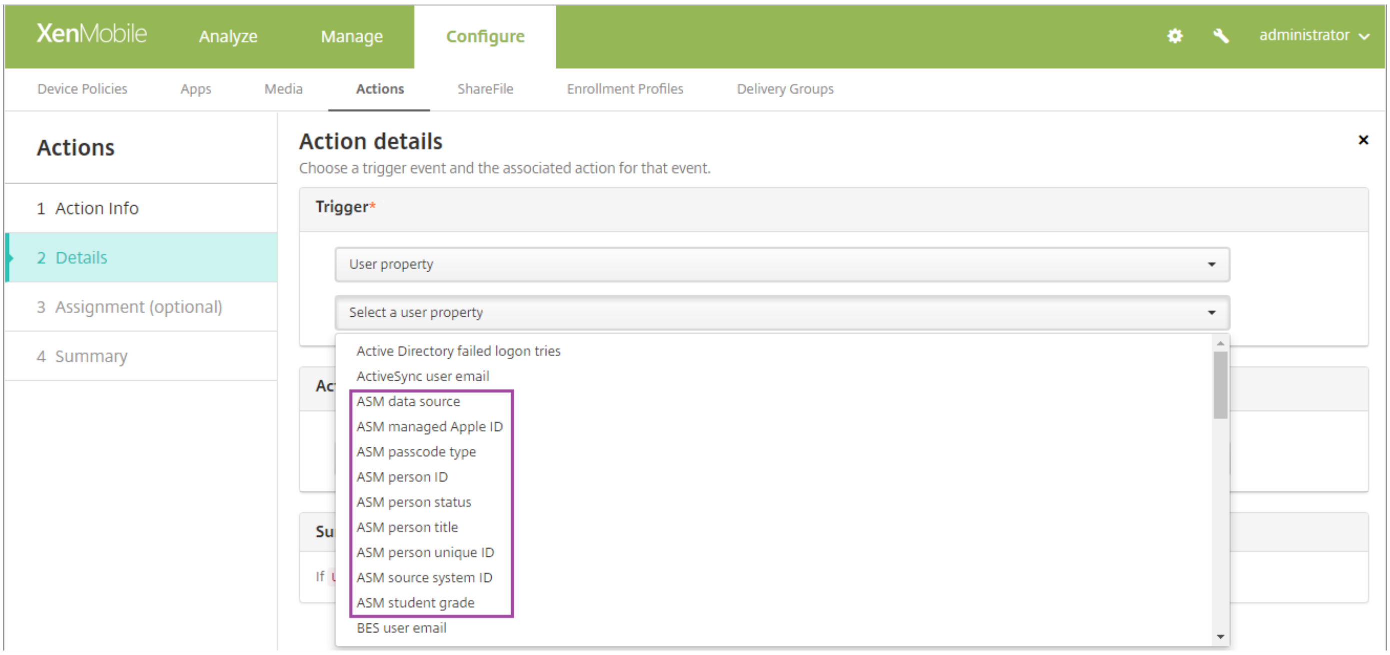
Deploy when All conditions are met.

Deploy this resource by ASM... only Instructor

- For help with adding VPP apps, see Add a Public App Store app.

3. Optional. Create actions based on Apple School Manager user properties. For example, you might create an action to

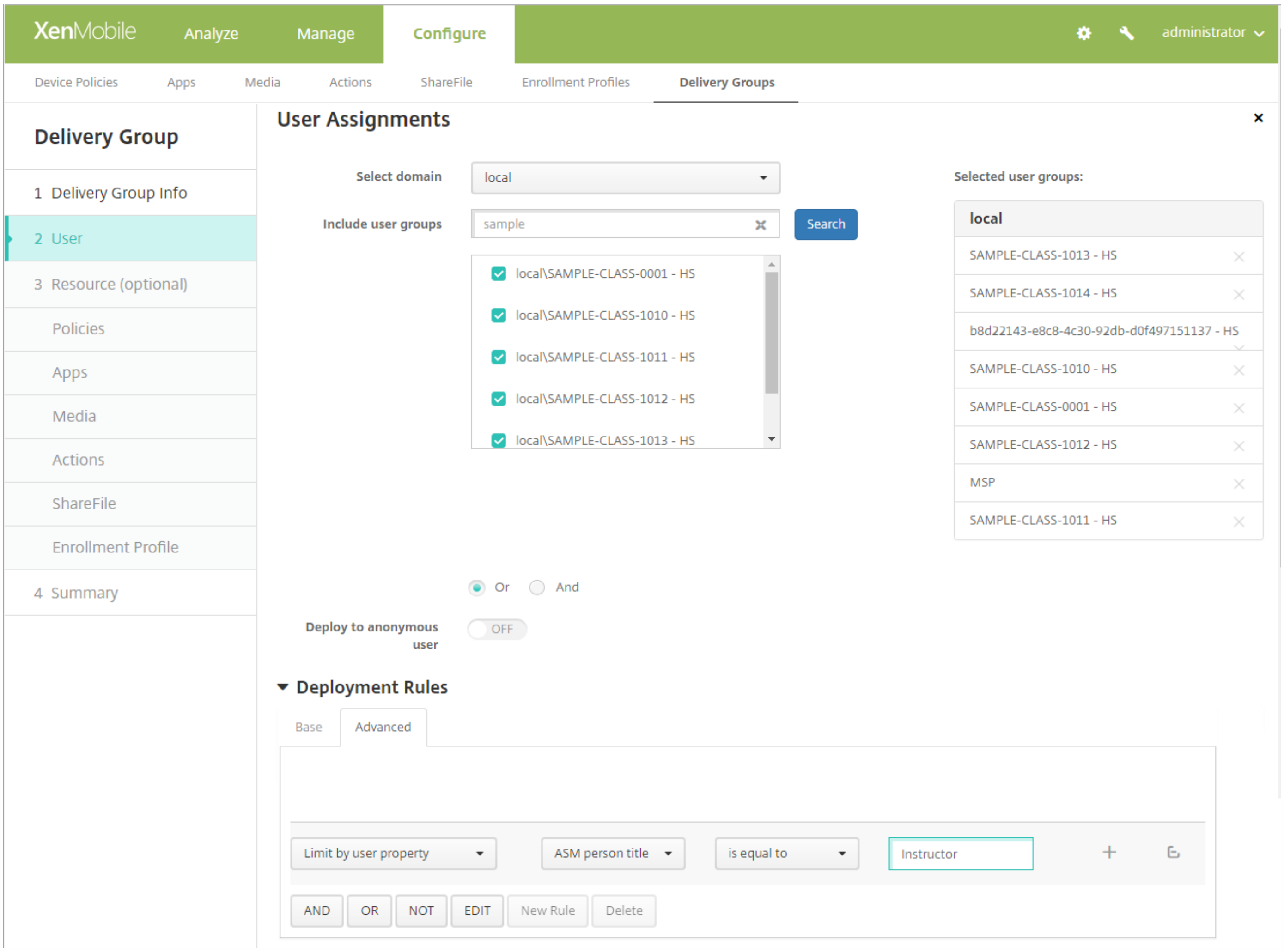
send a notification to student devices when a new app installs. Alternatively, you can create an action that a user property triggers, as shown in the following example.



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 Apple School Manager. Also, create a deployment rule for instructors and students.

   For example, the following user assignments are for instructors. The deployment rule is:
   Limit by user property
   ASM person title
   is equal to
   Instructor



User Assignments

Select domain: local

Include user groups: sample

Search

☑ local\SAMPLE-CLASS-0001 - HS
☑ local\SAMPLE-CLASS-1010 - HS
☑ local\SAMPLE-CLASS-1011 - HS
☑ local\SAMPLE-CLASS-1012 - HS
☑ local\SAMPLE-CLASS-1013 - HS

Selected user groups:

local
SAMPLE-CLASS-1013 - HS
SAMPLE-CLASS-1014 - HS
b8d22143-e8c8-4c30-92db-d0f497151137 - HS
SAMPLE-CLASS-1010 - HS
SAMPLE-CLASS-0001 - HS
SAMPLE-CLASS-1012 - HS
MSP
SAMPLE-CLASS-1011 - HS

● Or ○ And

Deploy to anonymous user: OFF

Deployment Rules

Base | Advanced

Limit by user property | ASM person title | is equal to | Instructor

AND | OR | NOT | EDIT | New Rule | Delete

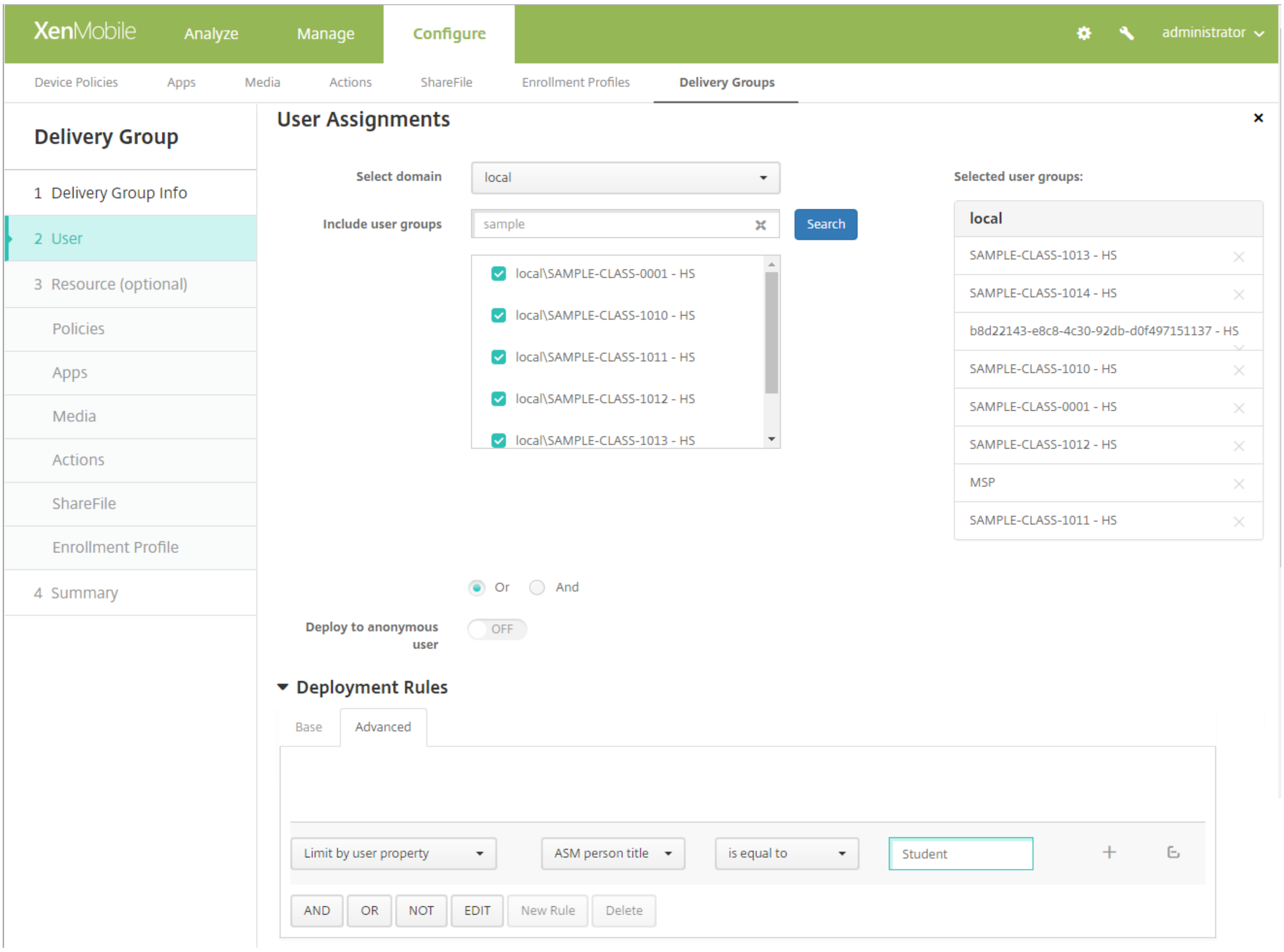
The following user assignments are for students. The deployment rule is:

Limit by user property

ASM person title

is equal to

Student



User Assignments

Select domain: local

Include user groups: sample

☑ local\SAMPLE-CLASS-0001 - HS
☑ local\SAMPLE-CLASS-1010 - HS
☑ local\SAMPLE-CLASS-1011 - HS
☑ local\SAMPLE-CLASS-1012 - HS
☑ local\SAMPLE-CLASS-1013 - HS

Selected user groups:

local
- SAMPLE-CLASS-1013 - HS
- SAMPLE-CLASS-1014 - HS
- b8d22143-e8c8-4c30-92db-d0f497151137 - HS
- SAMPLE-CLASS-1010 - HS
- SAMPLE-CLASS-0001 - HS
- SAMPLE-CLASS-1012 - HS
- MSP
- SAMPLE-CLASS-1011 - HS

● Or ○ And

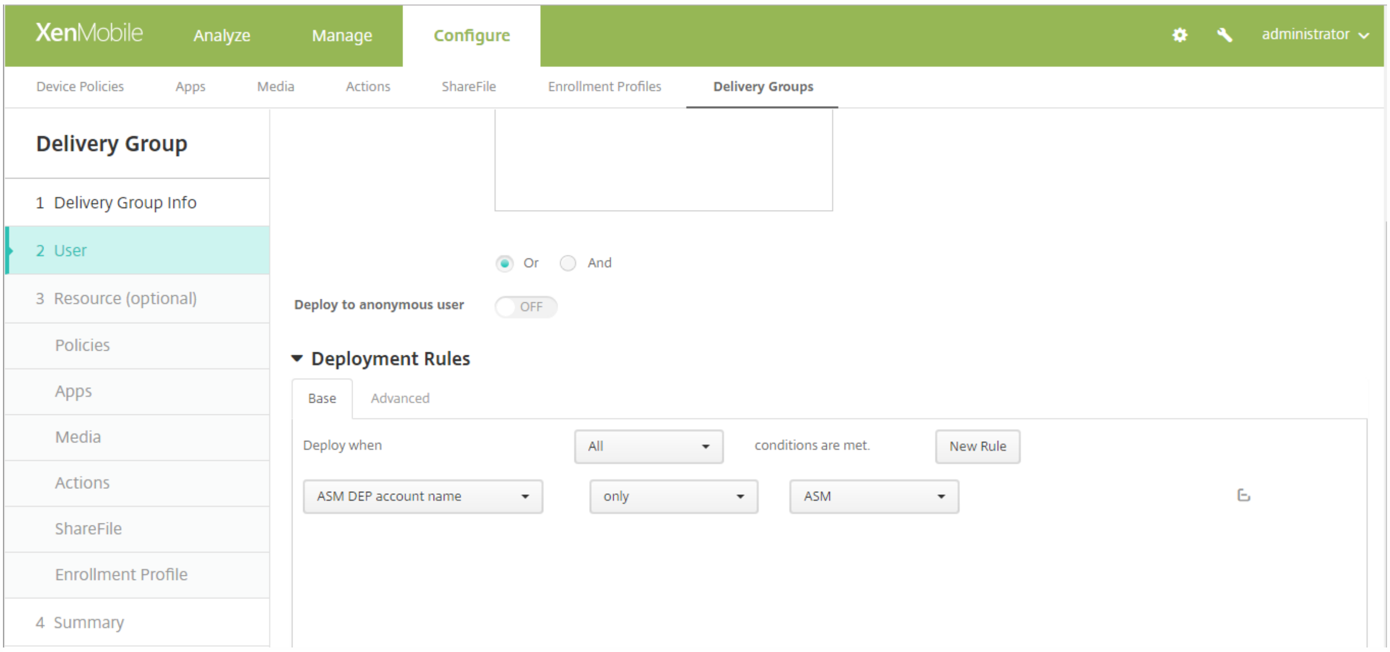
Deploy to anonymous user: OFF

Deployment Rules

Base | Advanced

Limit by user property | ASM person title | is equal to | Student

You can also filter a delivery group by using a deployment rule based on the Apple School Manager DEP account name.



● Or ○ And

Deploy to anonymous user: OFF

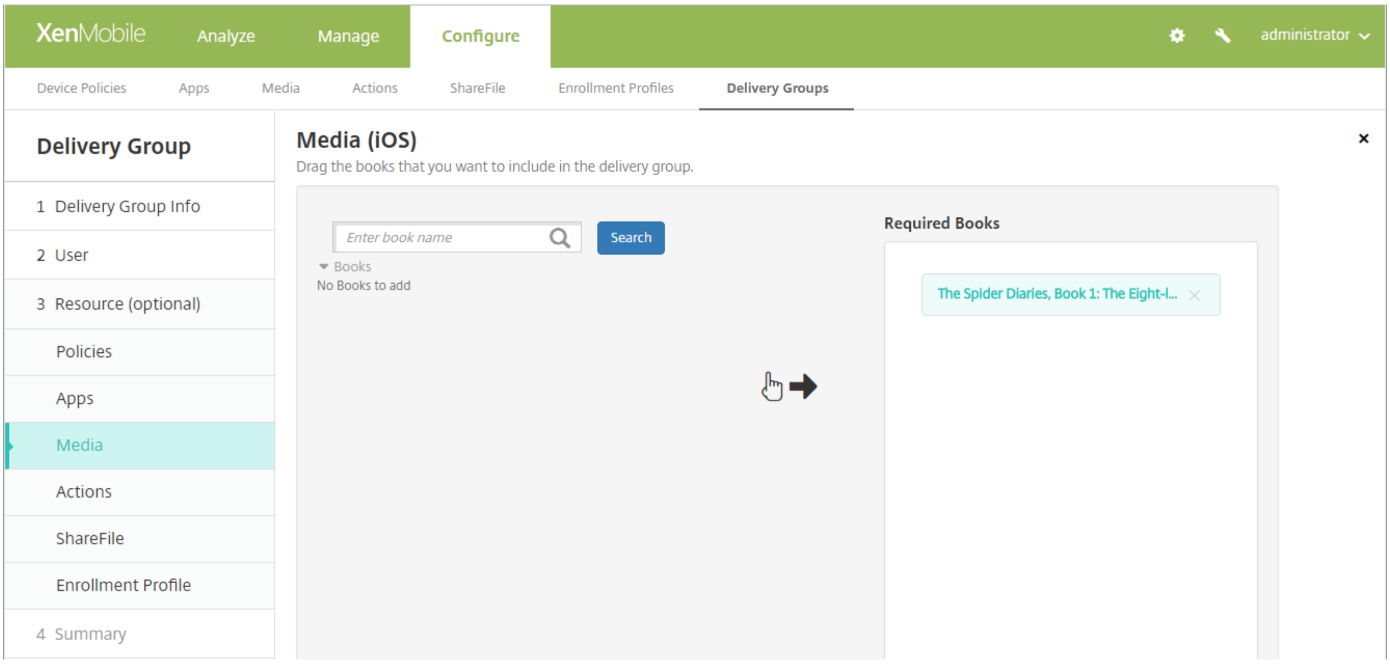
Deployment Rules

Base | Advanced

Deploy when All conditions are met.

ASM DEP account name | only | ASM

5. Assign the resources to delivery groups. The following example shows an iBook contained in a delivery group.



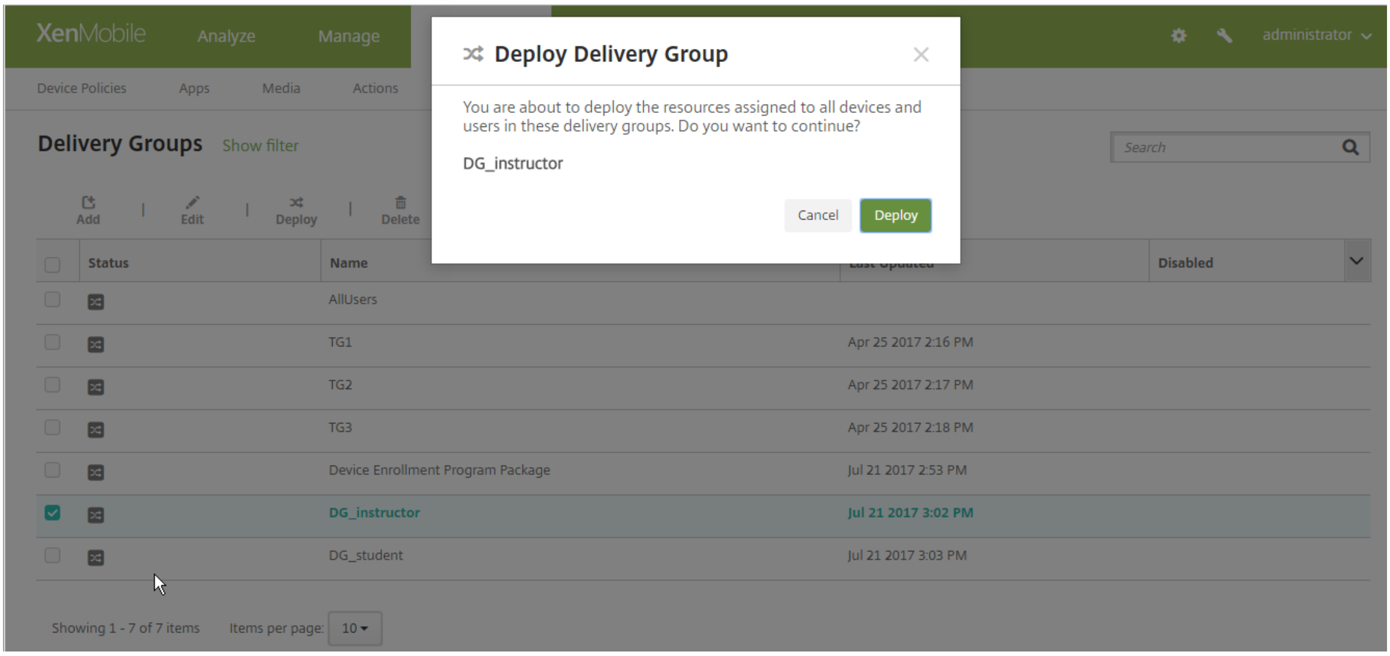
Media (iOS)

Drag the books that you want to include in the delivery group.

No Books to add

The Spider Diaries, Book 1: The Eight-l...

The following example shows the confirmation dialog that appears when you select a delivery group and click **Deploy**.



Deploy Delivery Group

You are about to deploy the resources assigned to all devices and users in these delivery groups. Do you want to continue?

DG_instructor

☐	Status	Name	Last Updated	Disabled
☐		AllUsers		
☐		TG1	Apr 25 2017 2:16 PM	
☐		TG2	Apr 25 2017 2:17 PM	
☐		TG3	Apr 25 2017 2:18 PM	
☐		Device Enrollment Program Package	Jul 21 2017 2:53 PM	
☑		DG_instructor	Jul 21 2017 3:02 PM	
☐		DG_student	Jul 21 2017 3:03 PM	

Showing 1 - 7 of 7 items Items per page: 10

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:

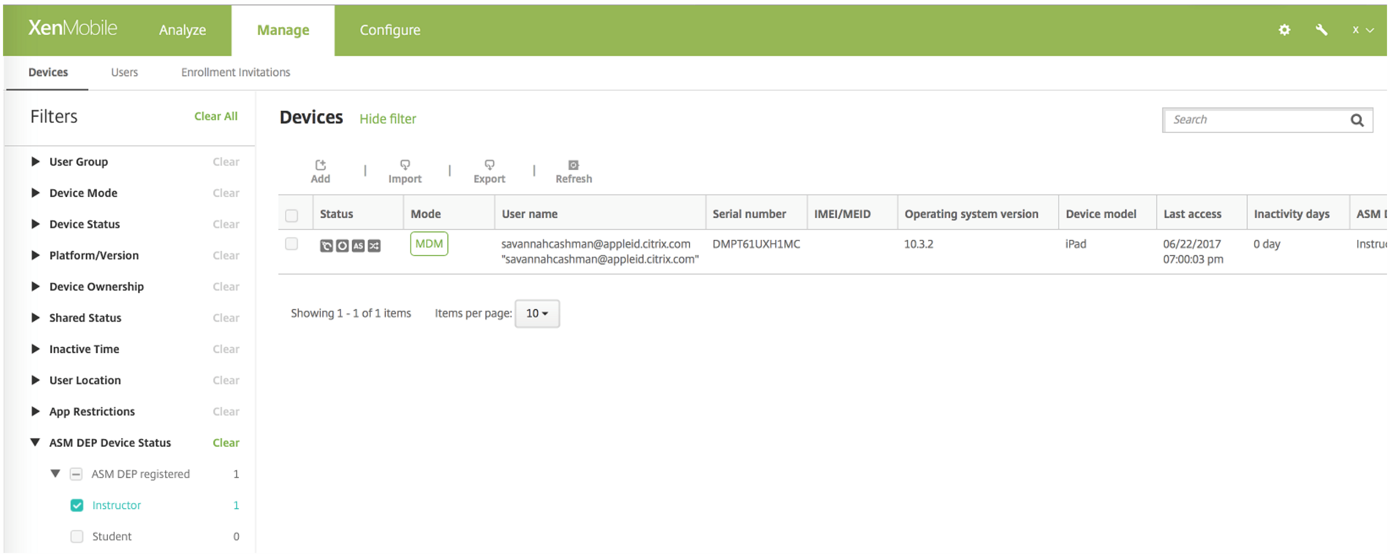
- A school administrator can enroll instructor and student devices by using the user password you can set in the XenMobile console. As a result, you can provide users with devices that are already set up with apps and media.

- When users receive the devices, they enroll using the user password that you provide to them. After enrollment completes, XenMobile Server sends device policies, apps, and media to the devices.

To test enrollment, use DEP devices that are linked to Apple School Manager.

1. If the devices aren't linked to Apple School Manager, erase the device contents and settings by performing a hard reset.
2. Enroll an Apple School Manager DEP device with an instructor. Then, enroll an Apple School Manager DEP device with a student.
3. In the **Manage > Devices** page, check that both Apple School Manager DEP devices are enrolled in MDM only.

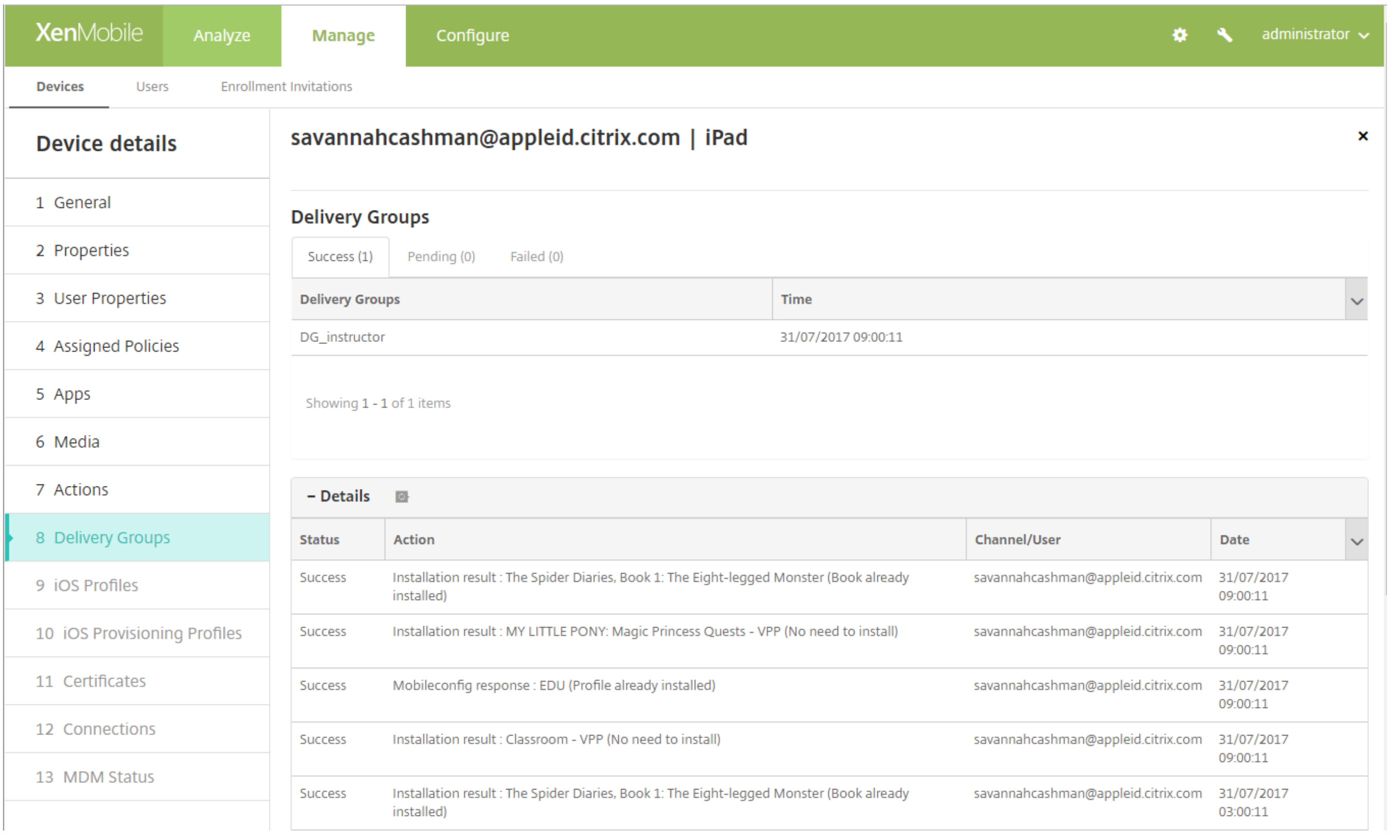
   You can filter the **Devices** page by the Apple School Manager DEP device status: **ASM DEP registered**, **Instructor**, and **Student**.



- ▶ User Group Clear
- ▶ Device Mode Clear
- ▶ Device Status Clear
- ▶ Platform/Version Clear
- ▶ Device Ownership Clear
- ▶ Shared Status Clear
- ▶ Inactive Time Clear
- ▶ User Location Clear
- ▶ App Restrictions Clear
- ▼ ASM DEP Device Status Clear
  - ▼ ⊟ ASM DEP registered 1
    - ☑ Instructor 1
    - □ Student 0

□	Status	Mode	User name	Serial number	IMEI/MEID	Operating system version	Device model	Last access	Inactivity days	ASM I
□		MDM	savannahcashman@appleid.citrix.com "savannahcashman@appleid.citrix.com"	DMPT61UXH1MC		10.3.2	iPad	06/22/2017 07:00:03 pm	0 day	Instru

4. To verify that MDM resources deployed correctly for each device: Select the device, click **Edit**, and check the various pages.



savannahcashman@appleid.citrix.com | iPad

Delivery Groups

Delivery Groups	Time
DG_instructor	31/07/2017 09:00:11

Status	Action	Channel/User	Date
Success	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster (Book already installed)	savannahcashman@appleid.citrix.com	31/07/2017 09:00:11
Success	Installation result : MY LITTLE PONY: Magic Princess Quests - VPP (No need to install)	savannahcashman@appleid.citrix.com	31/07/2017 09:00:11
Success	Mobileconfig response : EDU (Profile already installed)	savannahcashman@appleid.citrix.com	31/07/2017 09:00:11
Success	Installation result : Classroom - VPP (No need to install)	savannahcashman@appleid.citrix.com	31/07/2017 09:00:11
Success	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster (Book already installed)	savannahcashman@appleid.citrix.com	31/07/2017 03:00:11

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:

- XenMobile Server passwords for DEP enrollment
- Apple School Manager 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, XenMobile prompts them in the DEP enrollment screen to enroll their device.
2. The user provides their Managed Apple ID and XenMobile Server password used to authenticate to the XenMobile Server.
3. In the Apple ID setup step, the device prompts the user to provide their Managed Apple ID and Apple School Manager 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, XenMobile Server 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 VPP. After accepting the invitation, users receive their VPP apps and iBooks at the next deployment (within six hours).

Manage instructor, student, and class data

When managing instructor, student, and class data, note the following:

- Don't change Managed Apple IDs after you import Apple School Manager information into XenMobile Server. XenMobile also uses Apple School Manager user identifiers to identify users.
- If you add or change class data in Apple School Manager 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 XenMobile console and then redeploy the policy.
- If you update user properties in the Apple School Manager portal, XenMobile also updates those properties in the console. However, XenMobile 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 Apple School Manager, complete the following steps to reflect that change in XenMobile.

  1. In the Apple School Manager 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 XenMobile 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 Apple School Manager portal, XenMobile Server also deletes that user from the XenMobile 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 Apple School Manager administrator. The administrator can provide the temporary password or generate a new one.

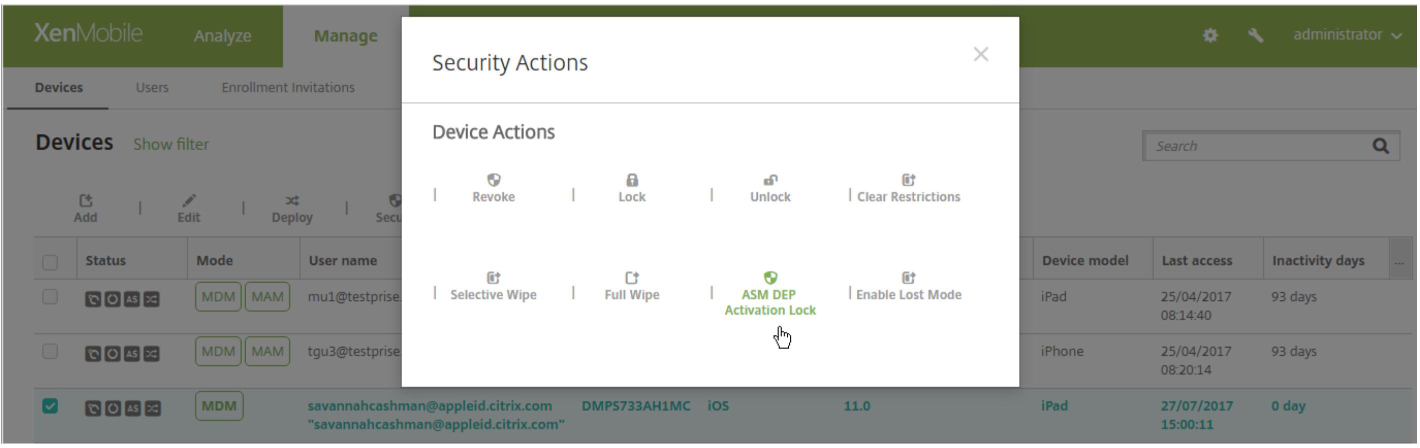
Manage a lost or stolen device that's enrolled in Apple School Manager DEP

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 DEP. XenMobile Server includes an **ASM DEP Activation Lock** security action that enables you to send a lock code to an Apple School Manager DEP-enrolled device.

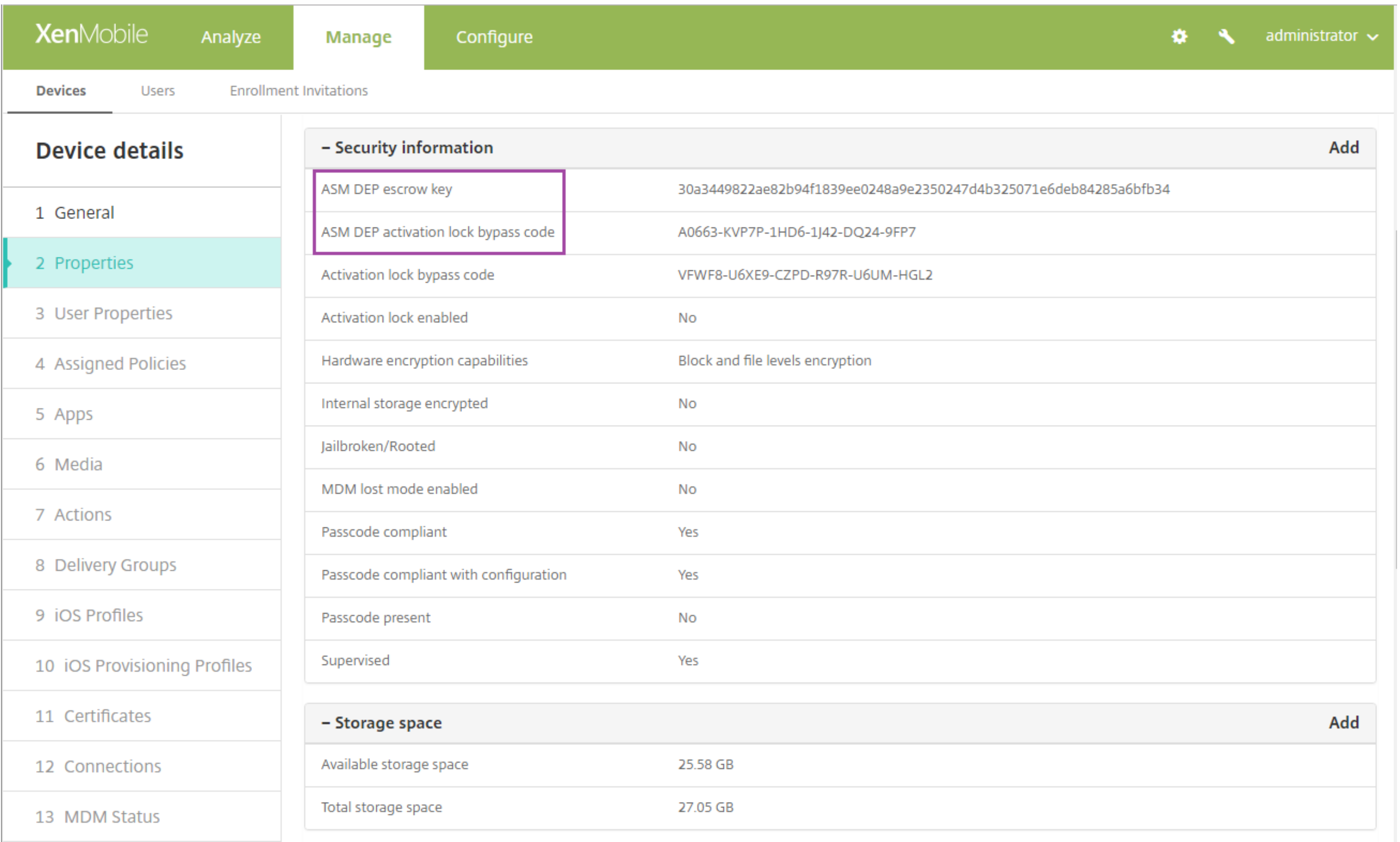
When you use the **ASM DEP Activation Lock** security action, XenMobile can locate devices without requiring users to enable the Find My iPhone/iPad service. When an Apple School Manager device is hard-reset or fully wiped, the user provides their Managed Apple ID and password to unlock the device.

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 in the Security actions article. The user also can leave the login blank and type the **ASM DEP 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 DEP Activation Lock**.



The properties, **ASM DEP escrow key** and **ASM DEP activation lock bypass code**, appear in **Device details**.



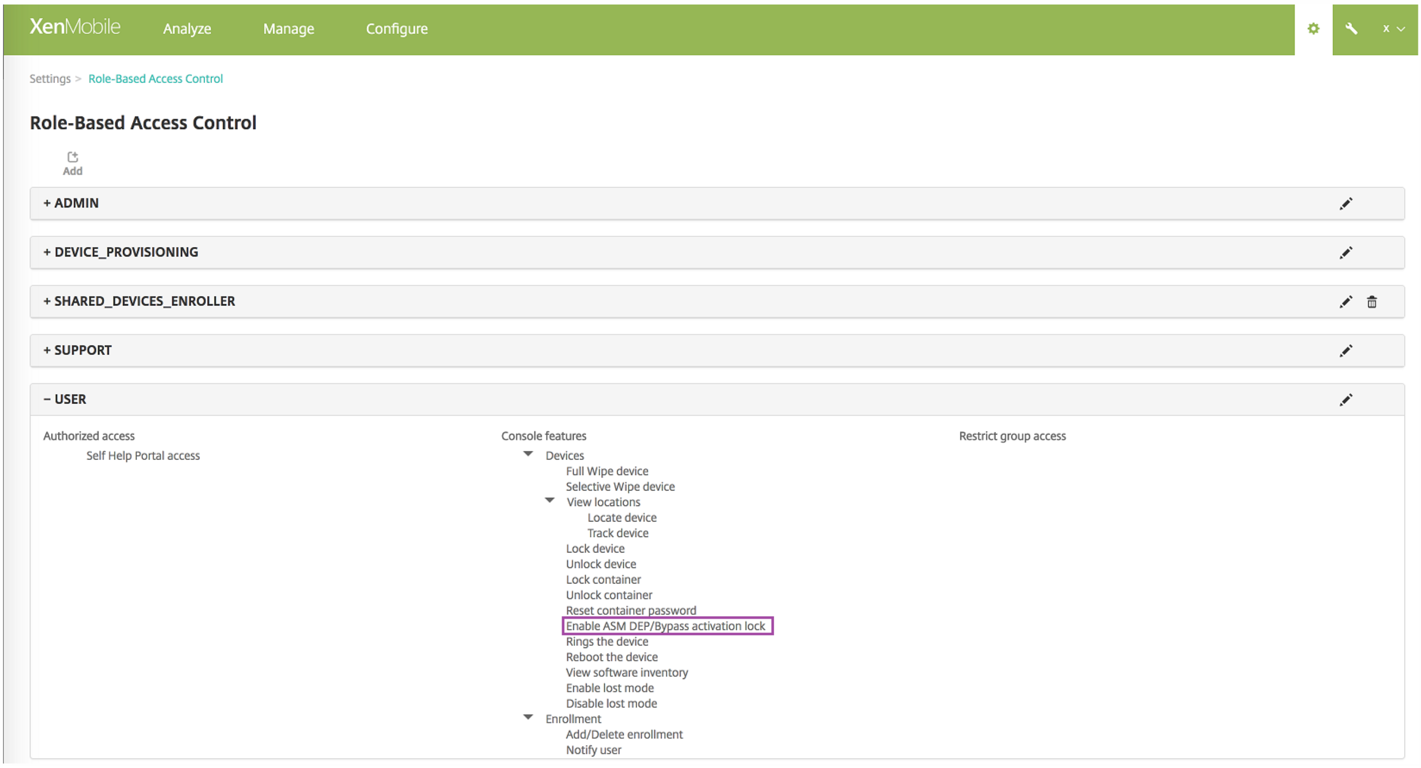
– Security information

ASM DEP escrow key	30a3449822ae82b94f1839ee0248a9e2350247d4b325071e6deb84285a6bfb34
ASM DEP activation lock bypass code	A0663-KVP7P-1HD6-1J42-DQ24-9FP7
Activation lock bypass code	VFWF8-U6XE9-CZPD-R97R-U6UM-HGL2
Activation lock enabled	No
Hardware encryption capabilities	Block and file levels encryption
Internal storage encrypted	No
Jailbroken/Rooted	No
MDM lost mode enabled	No
Passcode compliant	Yes
Passcode compliant with configuration	Yes
Passcode present	No
Supervised	Yes

– Storage space

Available storage space	25.58 GB
Total storage space	27.05 GB

The RBAC permission for an ASM DEP Activation Lock is **Devices > Enable ASM DEP/Bypass activation lock**.



Role-Based Access Control

+ ADMIN

+ DEVICE_PROVISIONING

+ SHARED_DEVICES_ENROLLER

+ SUPPORT

− USER

Authorized access
- Self Help Portal access

Console features
- Devices
  - Full Wipe device
  - Selective Wipe device
  - View locations
    - Locate device
    - Track device
  - Lock device
  - Unlock device
  - Lock container
  - Unlock container
  - Reset container password
  - Enable ASM DEP/Bypass activation lock
  - Rings the device
  - Reboot the device
  - View software inventory
  - Enable lost mode
  - Disable lost mode
- Enrollment
  - Add/Delete enrollment
  - Notify user

Restrict group access

Network Access Control

Sep 06, 2017

If you have a Network Access Control (NAC) appliance set up in your network, such as a Cisco ISE, in XenMobile, you can enable filters to set devices as compliant or not compliant for NAC, based on rules or properties. If a managed device in XenMobile does not meet the specified criteria, and as a result is marked Not Compliant, the NAC appliance will block the device on your network.

In the XenMobile console, you select one or more criterion in the list to set a device as not compliant.

XenMobile supports the following NAC compliance filters:

Anonymous Devices: Checks if a device is in anonymous mode. This check is available if XenMobile 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. 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, XenMobile 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 XenMobile 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 third party making use of XenMobile 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.

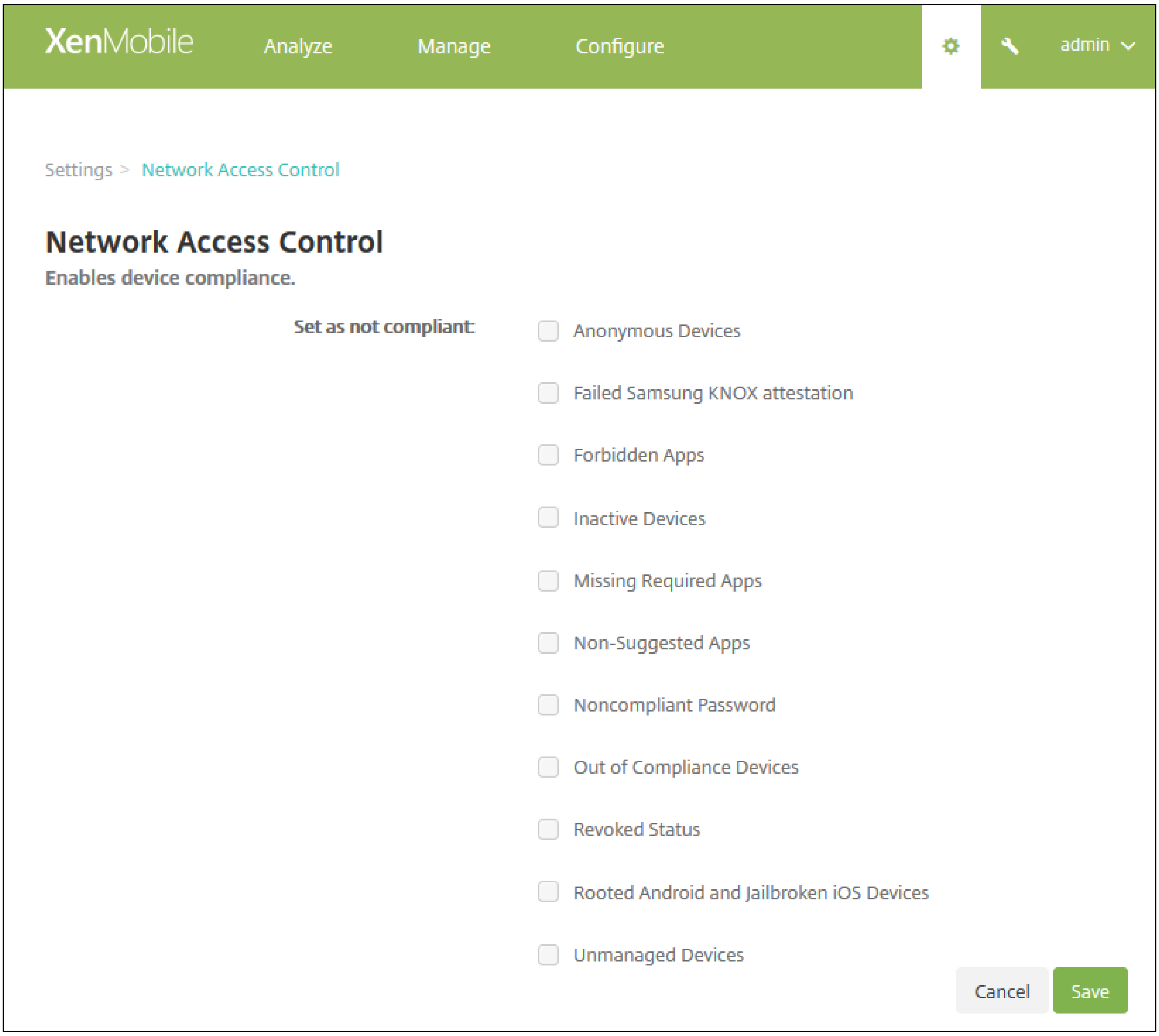
Unmanaged Devices: Check whether a device is still in a managed state, under XenMobile control. For example, a device running in MAM mode or an un-enrolled device is not managed.

> ## Note
>
> The Implicit Compliant/Not Compliant filter sets the default value only on devices that are managed by XenMobile. For example, any devices that have a blacklisted app installed or are not enrolled, are marked as Not-Compliant and will be blocked from your network by the NAC appliance.

Configure Network Access Control

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

2. Under **Server**, click **Network Access Control**. The **Network Access Control** page appears.



Settings > Network Access Control

Network Access Control

Enables device compliance.

Set as not compliant:

□ Anonymous Devices

□ Failed Samsung KNOX attestation

□ 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

3. Select the check boxes for the **Set as not compliant** filters you want to enable.

4. Click **Save**.

Samsung KNOX

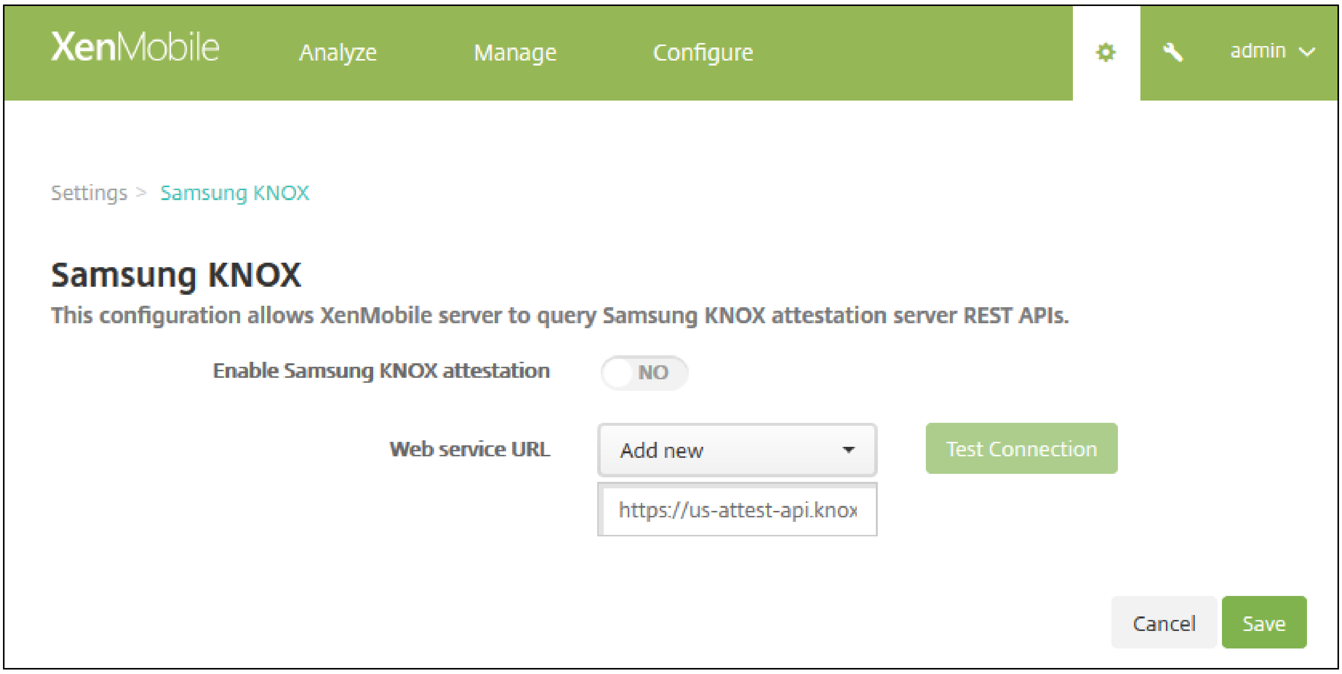
Sep 06, 2017

You can configure XenMobile to query the Samsung KNOX attestation server REST APIs.

Samsung KNOX leverages 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 trusted boot.

1. In the XenMobile web console, click the gear icon in the upper-right corner. The **Settings** page appears.

2. Under **Platforms**, click **Samsung KNOX**. The **Samsung KNOX** page appears.



Samsung KNOX

This configuration allows XenMobile server to query Samsung KNOX attestation server REST APIs.

Enable Samsung KNOX attestation: NO

Web service URL: Add new

https://us-attest-api.knox

3. In **Enable Samsung KNOX attestation,** select whether to enable Samsung KNOX attestation. The default is **NO**.

4. When you set **Enable Samsung KNOX attestation**, to **YES**, the **Web service URL** option is enabled. Then, in the list, do one of the following:

   a. Click the appropriate attestation server.

   b. Click **Add new** and then enter the Web service URL.

5. Click **Test Connection** to verify the connection. A success or failure message appears.

6. Click **Save**.

> ## Note
>
> You can use Samsung KNOX Mobile Enrollment to enroll multiple Samsung KNOX devices into XenMobile (or any mobile device

> manager) without manually configuring each device. For information, see Samsung KNOX Bulk Enrollment.

Security actions

Oct 26, 2017

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 XenMobile. On iOS, users can sign in, but they can't access apps.
- **App wipe**: On Android, an app wipe deletes the user account from XenMobile. On iOS, deletes a user account in Secure Hub.
- **ASM DEP Activation Lock**: Creates an Activation Lock bypass code for iOS devices enrolled in Apple School Manager DEP.
- **Clear restrictions**: On supervised iOS devices, this command allows XenMobile Server 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.
- **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 and macOS devices, the wipe occurs immediately, even if the device is locked.
  - For Windows Phone devices, a full wipe removes all XenMobile information and all user data, including personal content such as apps, emails, contacts, and media.
  - For Windows Mobile devices that are running Windows Mobile 6 or earlier: After the wipe, you might need to send the device back to the manufacturer to reload the original operating system, software, or both.
  - 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**.
- **Lock**: Remotely locks a device, which is useful if a device is lost but you aren't sure if it's stolen. XenMobile 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 XenMobile console
- **Lock and Reset Password**: Remotely locks a device and resets the password.
- **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 iOS devices.
- **Revoke**: Prohibits a device from connecting to XenMobile Server.
- **Revoke/Authorize (iOS, macOS)**: 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 XenMobile to install apps on the device. The wipe also removes all XenMobile certificates and configurations deployed to the device. You can't reenroll a selectively wiped Windows Phone device.
- **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.

The remainder of this article covers these topics:

- Security actions for Android devices
- Security actions for iOS and macOS devices
- Security actions for Windows devices
- Lock iOS devices
- Remove a device from the XenMobile console
- Selectively wipe a device
- Delete a device
- Lock, unlock, wipe, or unwipe apps
- Put iOS devices in Lost Mode

- Bypass an iOS activation lock

Security actions for Android devices

Security action	Android[1]	Android for Work (BYOD)	Android for Work (corporate-owned)
App Lock	Yes	No	No
App Wipe	Yes	No	No
Full Wipe	Yes	No	Yes
Locate	Yes[2]	Yes[2]	Yes[2]
Lock	Yes	Yes	Yes
Lock and Reset Password	Yes	No	Yes
Notify (Ring)	Yes	Yes	Yes
Revoke	Yes	Yes	Yes
Selective Wipe	Yes	Yes	No

[1] Except for Android for Work devices.

[2] For devices running Android 6.0+, Locate 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, XenMobile again requests location permission when sending the Locate command.

Security actions for iOS and macOS devices

Security action	iOS	macOS
Activation Lock Bypass	Yes	No

App Lock	Yes	No
App Wipe	Yes	No
ASM DEP Activation Lock	Yes	No
Clear Restrictions	Yes	No
Enable/Disable Lost Mode	Yes	No
Enable/Disable Tracking	Yes	No
Full Wipe	Yes	Yes
Locate	Yes	No
Lock	Yes	Yes
Ring	Yes	Yes
Request/Stop AirPlay Mirroring	Yes	No
Restart/Shut Down	Yes	No
Revoke/Authorize	Yes	Yes
Selective Wipe	Yes	Yes
Unlock	Yes	No

Security actions for Windows devices

Security action	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
Locate	Yes	Yes	No
Lock	Yes	Yes	Yes

Lock and Reset Password	Yes	No	Yes
Reboot	Yes	Yes	No
Revoke	Yes	Yes	Yes
Ring	Yes	No	Yes
Selective Wipe	Yes	Yes	Yes
Wipe	Yes	No	Yes

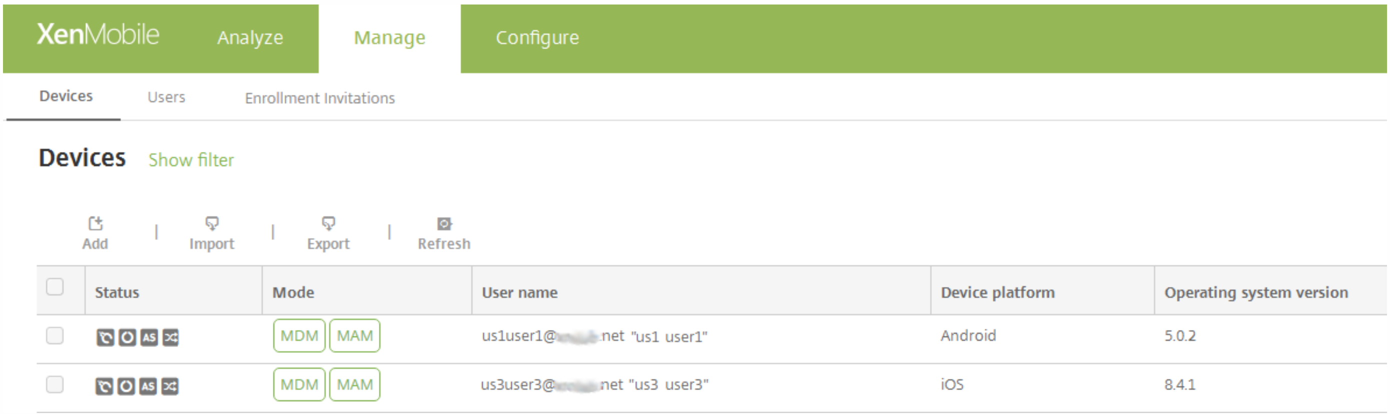
The remainder of this article provides the steps for performing various security actions. You can also automate some actions. For more information, see Automated actions.

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. This feature is supported on devices running iOS 7 and above.

To display a message and phone number on a locked device, set the Passcode policy to true in the XenMobile console. Alternatively, users can enable the passcode on the device manually.

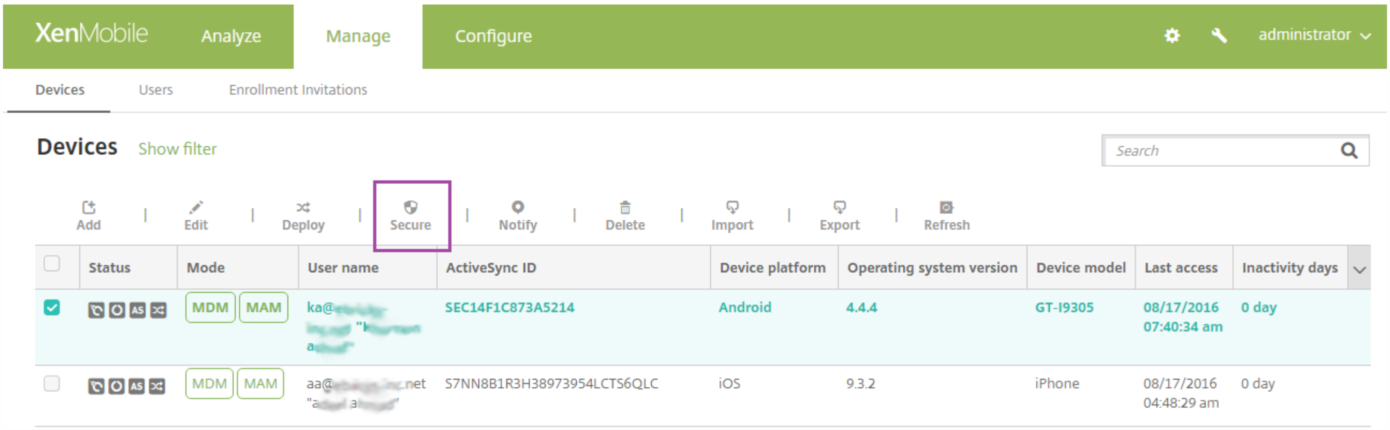
1. Click **Manage > Devices**. The **Devices** page displays.



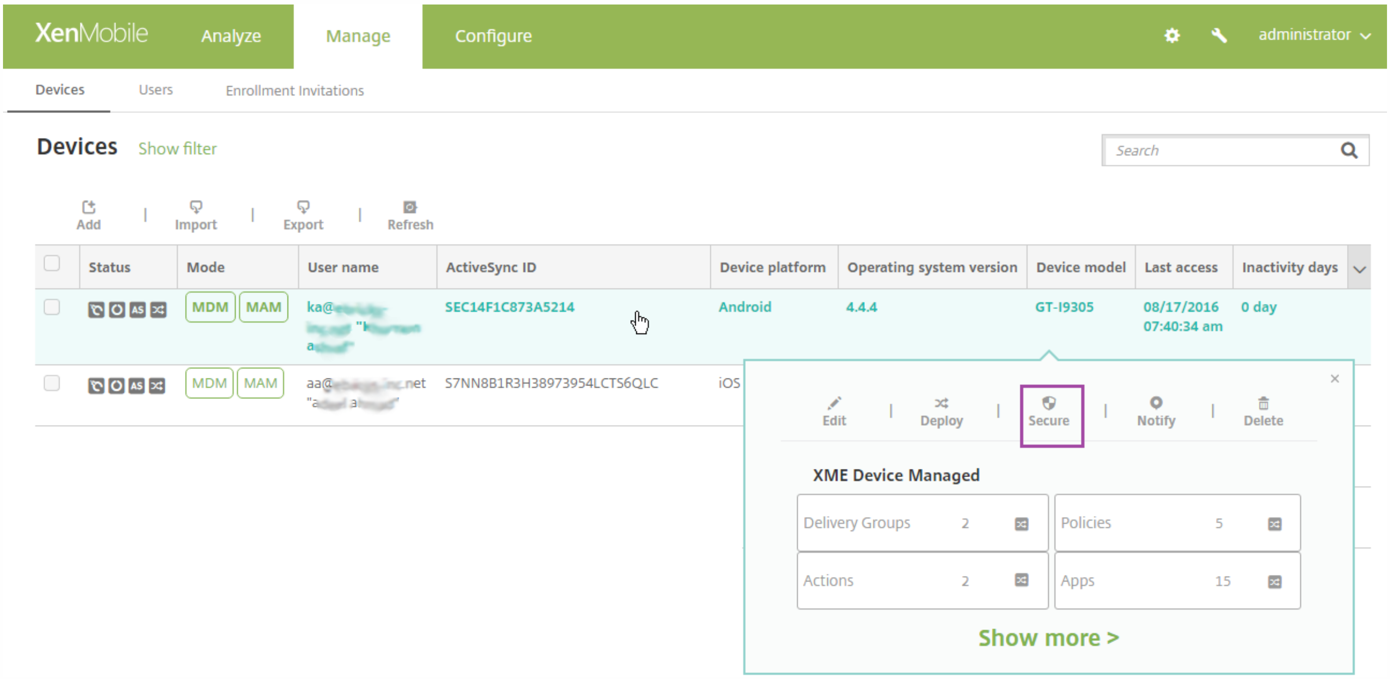
☐	Status	Mode	User name	Device platform	Operating system version
☐		MDM MAM	us1user1@[redacted].net "us1 user1"	Android	5.0.2
☐		MDM MAM	us3user3@[redacted].net "us3 user3"	iOS	8.4.1

2. Select the iOS device you want to lock.

   When you select the check box next to a device, the options menu displays above the device list. When you click anywhere else in the list, the options menu displays on the right side of the listing.



☐	Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
☑	AS	MDM MAM	ka@[redacted]	SEC14F1C873A5214	Android	4.4.4	GT-I9305	08/17/2016 07:40:34 am	0 day
☐	AS	MDM MAM	aa@[redacted].net "[redacted]"	S7NN8B1R3H38973954LCTS6QLC	iOS	9.3.2	iPhone	08/17/2016 04:48:29 am	0 day



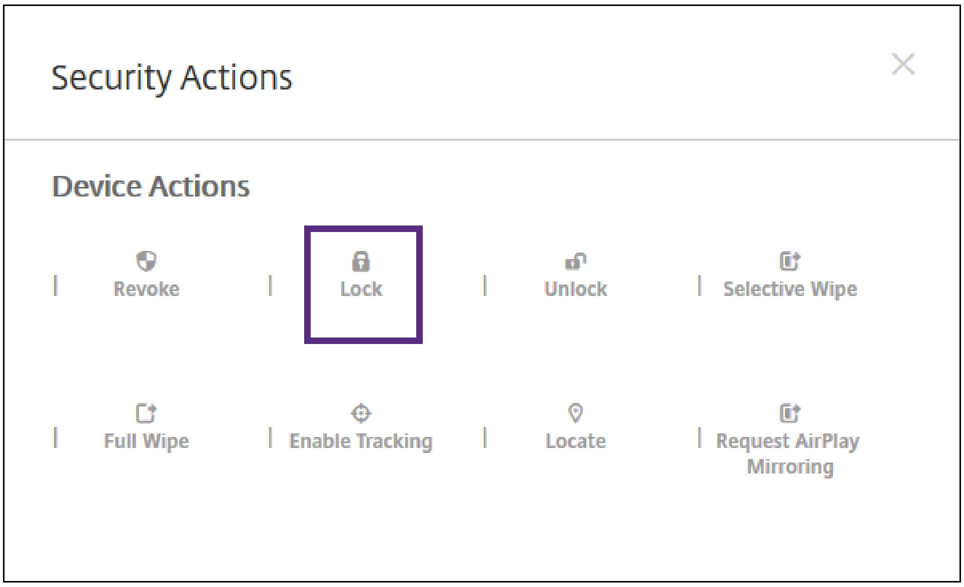
☐	Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
☐	AS	MDM MAM	ka@[redacted]	SEC14F1C873A5214	Android	4.4.4	GT-I9305	08/17/2016 07:40:34 am	0 day
☐	AS	MDM MAM	aa@[redacted].net "[redacted]"	S7NN8B1R3H38973954LCTS6QLC	iOS				

XME Device Managed

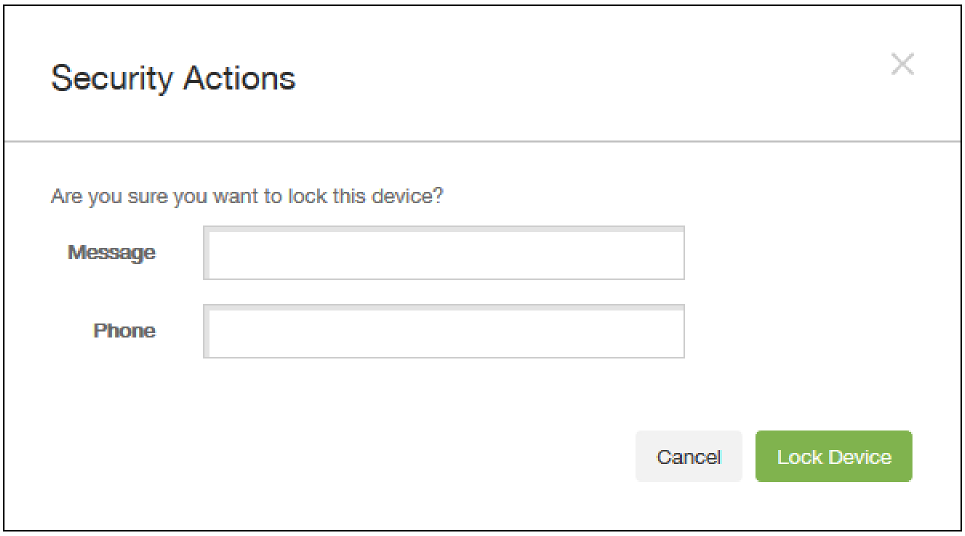
Delivery Groups	2	Policies	5
Actions	2	Apps	15

Show more >

3. In the options menu, click **Secure**. The **Security Actions** dialog box displays.



4. Click **Lock**. The **Security Actions** confirmation dialog box displays.



Are you sure you want to lock this device?

Message

Phone

5. Optionally, type a message and phone number that appears on the lock screen of the device.

   For iPads running iOS 7 and later: iOS appends the words “Lost iPad” to what you type in the **Message** field.

   For iPhones running iOS 7 and later: If you leave the **Message** field empty and provide a phone number, Apple displays the message “Call owner” on the device lock screen.

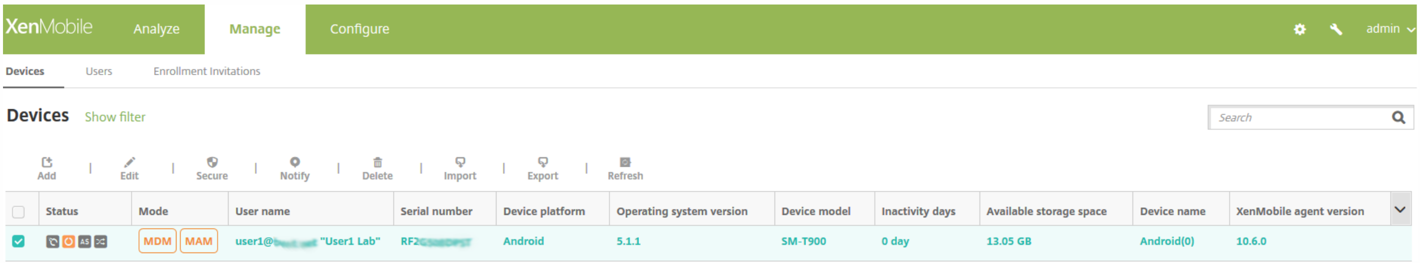
6. Click **Lock Device**.

Remove a device from the XenMobile console

Important

> When you remove a device from the XenMobile 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 XenMobile console, go to **Manage > Devices**, select a managed device, and then click **Delete**.



☐	Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version
☑	AS	MDM MAM	user1@[redacted] "User1 Lab"	RF2[redacted]	Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0

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**.

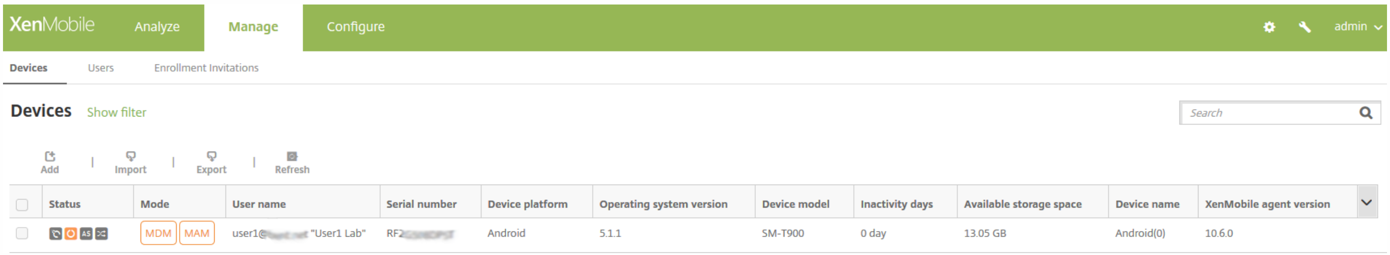
Delete a device

This procedure removes managed apps and data from the device and deletes the device from the Devices list in the XenMobile 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.



☐	Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version
☐	AS	MDM MAM	user1@[redacted] "User1 Lab"	RF2[redacted]	Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0

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.

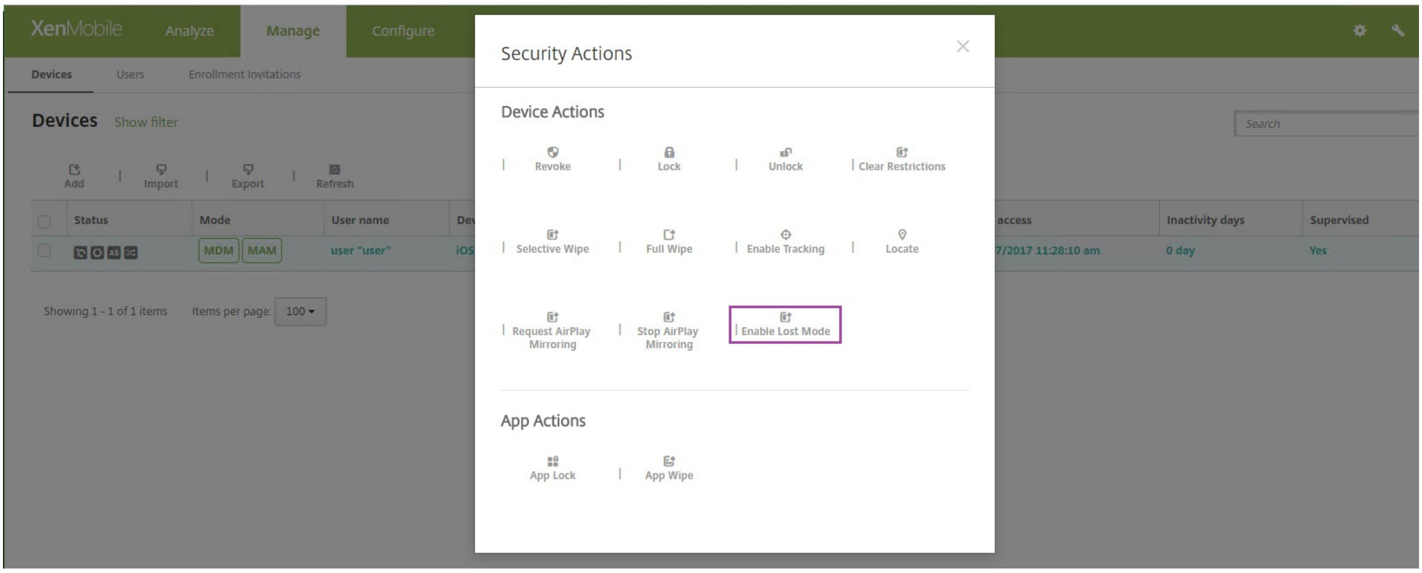
   You can also use the **Security Actions** box to check the device status for a user whose account is disabled or deleted from Active Directory. The presence of the App Unlock or App Unwipe actions indicate apps that are locked or wiped.

Put iOS devices in Lost Mode

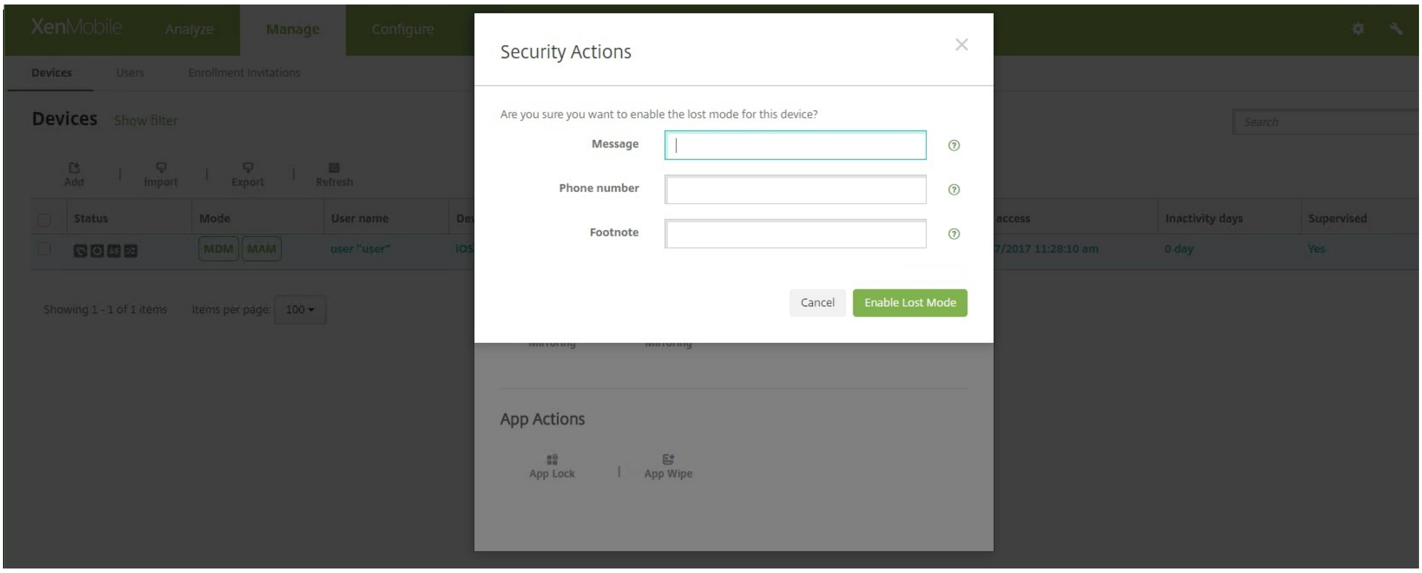
The XenMobile Lost Mode device property puts an iOS device in Lost Mode. Unlike Apple Managed Lost Mode, XenMobile Lost Mode doesn't require a user to perform either of the following actions to enable locating their device: Configure the Find My iPhone/iPad setting or enable the Location Services for Citrix Secure Hub.

In XenMobile Lost Mode, only the XenMobile Server can unlock the device. (In contrast, if you use the XenMobile 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 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.



Security Actions

Are you sure you want to enable the lost mode for this device?

Message

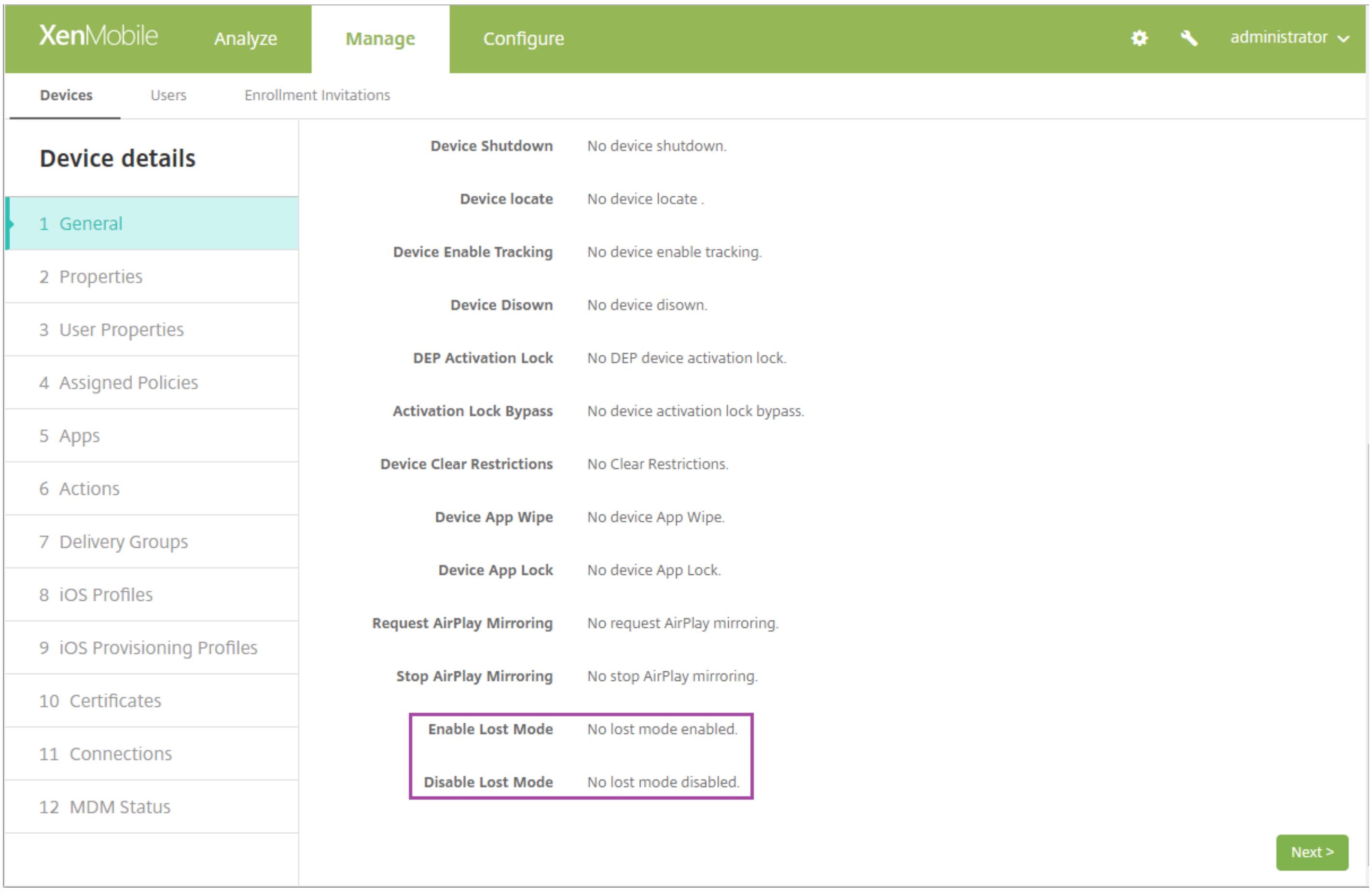
Phone number

Footnote

Cancel | Enable Lost Mode

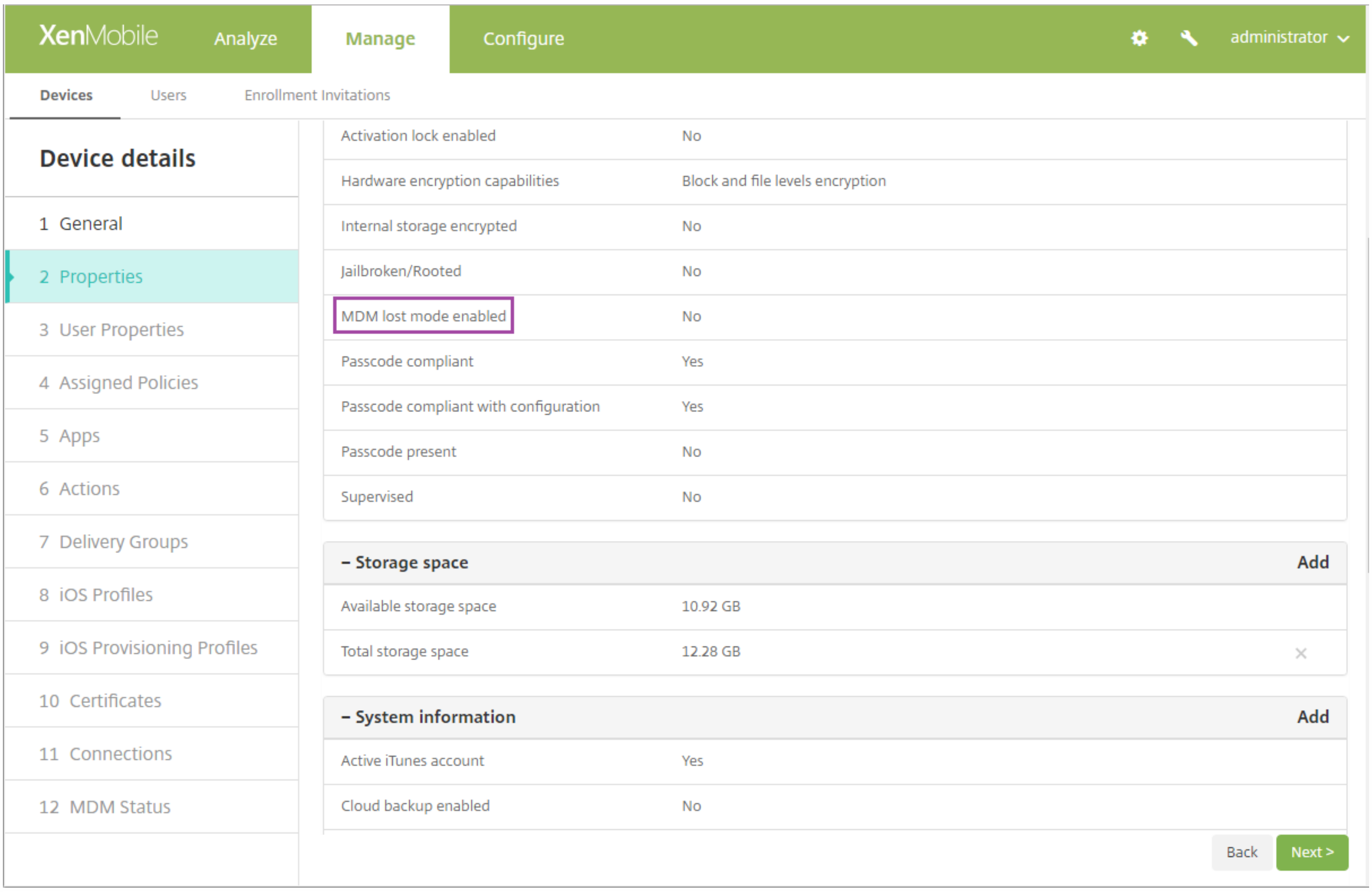
Use any of the following methods to check Lost Mode status:

- 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.



Device Shutdown	No device shutdown.
Device locate	No device locate .
Device Enable Tracking	No device enable tracking.
Device Disown	No device disown.
DEP Activation Lock	No DEP device activation lock.
Activation Lock Bypass	No device activation lock bypass.
Device Clear Restrictions	No Clear Restrictions.
Device App Wipe	No device App Wipe.
Device App Lock	No device App Lock.
Request AirPlay Mirroring	No request AirPlay mirroring.
Stop AirPlay Mirroring	No stop AirPlay mirroring.
Enable Lost Mode	No lost mode enabled.
Disable Lost Mode	No lost mode disabled.

- From **Manage > Devices**, on the **Properties** tab, verify that the value of the **MDM lost mode enabled** setting is correct.



Activation lock enabled	No
Hardware encryption capabilities	Block and file levels encryption
Internal storage encrypted	No
Jailbroken/Rooted	No
MDM lost mode enabled	No
Passcode compliant	Yes
Passcode compliant with configuration	Yes
Passcode present	No
Supervised	No

– Storage space Add

Available storage space	10.92 GB
Total storage space	12.28 GB

– System information Add

Active iTunes account	Yes
Cloud backup enabled	No

If you enable XenMobile Lost Mode on an iOS device, the XenMobile 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.

For iPads running iOS 7 and later: iOS appends the words "Lost iPad" to what you type in the **Message** in the **Security Actions** screen.

For iPhones running iOS 7 and later: 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 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 XenMobile MDM Options device policy. You can then manage a device from the XenMobile 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 XenMobile 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 XenMobile console.

Device requirements for activation lock bypass

- iOS 7.1 (minimum version)
- Supervised through Apple Configurator or Apple DEP
- Configured with an iCloud account
- Find My iPhone/iPad enabled
- Enrolled in XenMobile
- 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.

> Note
>
> - 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 XenMobile. Either you or the user can contact Apple support to unblock the device directly.
> - During a hardware inventory, XenMobile queries a device for an Activation lock bypass code. If a bypass code is available, the device sends it to XenMobile. Then, to remove the bypass code from the device, send the Activation Lock Bypass security action from the XenMobile console.
>   At that point, XenMobile Server 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 username 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**.

Shared devices

Dec 05, 2017

XenMobile 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 may also want shift workers in fields like law enforcement, retail, and manufacturing to share devices to reduce equipment costs.

Key Points About Shared Devices

MDM mode

- Available on both iOS and Android tablets and phones. Basic device enrollment program (DEP) enrollment is not supported for a XenMobile Enterprise shared device. You must use an authorized DEP to enroll a shared device in this mode.
- Client certificate authentication, Citrix PIN, Touch ID, User Entropy, and two-factor authentication are not supported.

MDM+MAM mode

- Available only on iOS and Android tablets.
- Supported on XenMobile 10.3.x and later.
- Only Active Directory username and password authentication is supported.
- Client certificate authentication, Worx PIN, 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 ShareFile 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 can share XenMobile apps and MDX-wrapped apps only; they cannot share native apps on the devices.
- Once downloaded during first-time enrollment, XenMobile 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, the **Disallow rooted devices** policy in the XenMobile console should be **On**.

Prerequisites for Enrolling Shared Devices

Before you can enroll shared devices, you must do the following:

- Create a shared device enrollment user role. See Configuring Roles with RBAC.
- Create a shared device user. See To add, edit, or delete local users in XenMobile.
- 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 Managing Delivery Groups.

Pre-requisites for MDM+MAM Mode

1. Create an Active Directory group named something like **Shared Device Enrollers**.
2. Add to this group Active Directory users who will 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.

Shared Device Requirements

For the best user experience, including silent installation and removal of apps, Citrix recommends configuring shared devices on the following platforms:

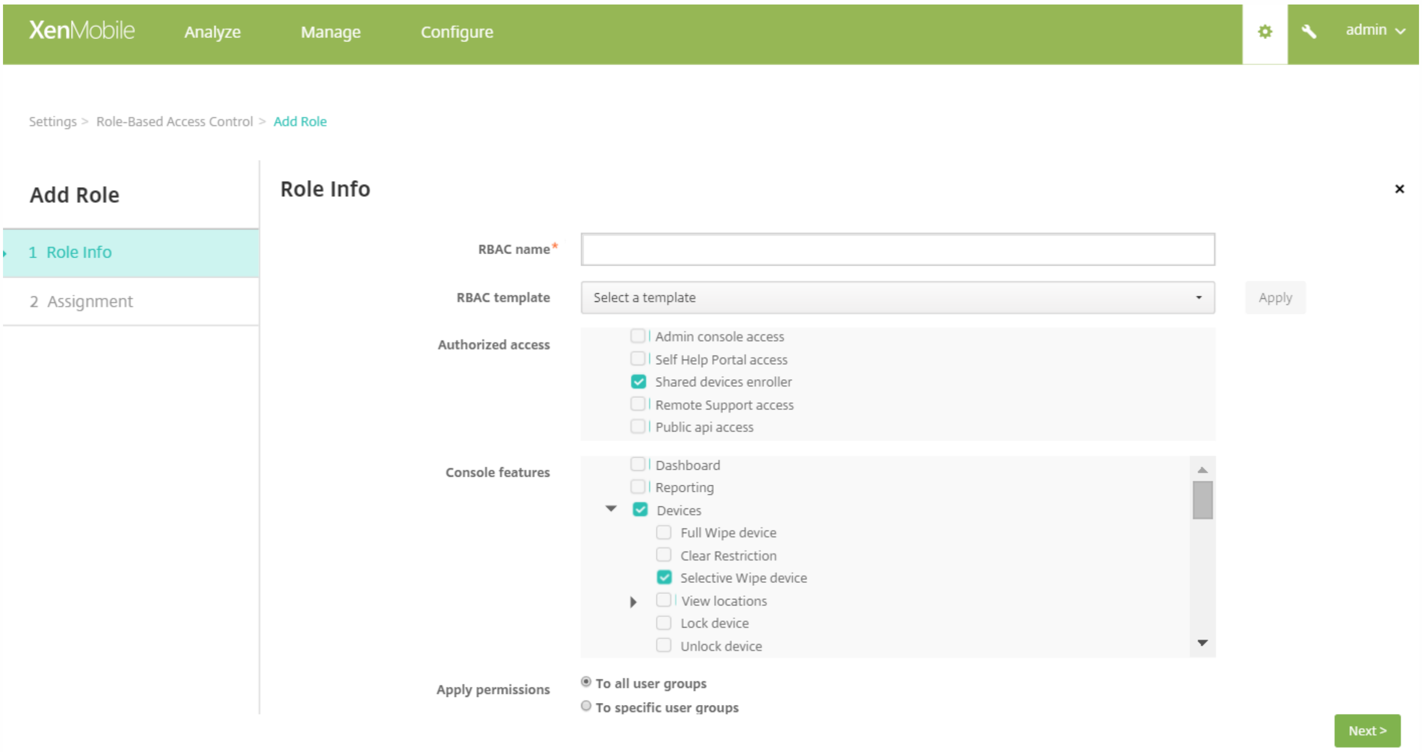
- iOS 9 (MDM only) and iOS 10
- Android M
- Android 5.x
- Android 4.4.x (MDM only)
- Android 4.0.x (MDM only)

Configuring a Shared Device

Follow these steps to configure a shared device.

1. From the XenMobile 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 is displayed.
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 un-enrolled.

   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**.



Role Info

RBAC name*

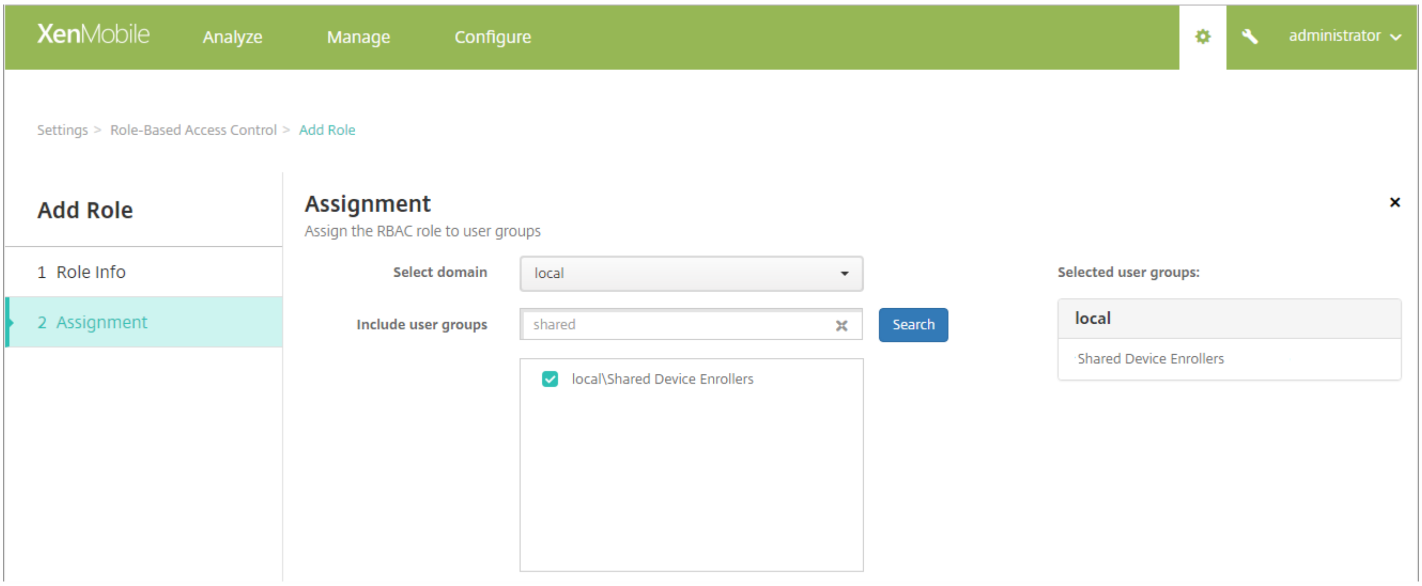
RBAC template: Select a template

Authorized access:
- □ Admin console access
- □ Self Help Portal access
- ☑ Shared devices enroller
- □ Remote Support access
- □ Public api access

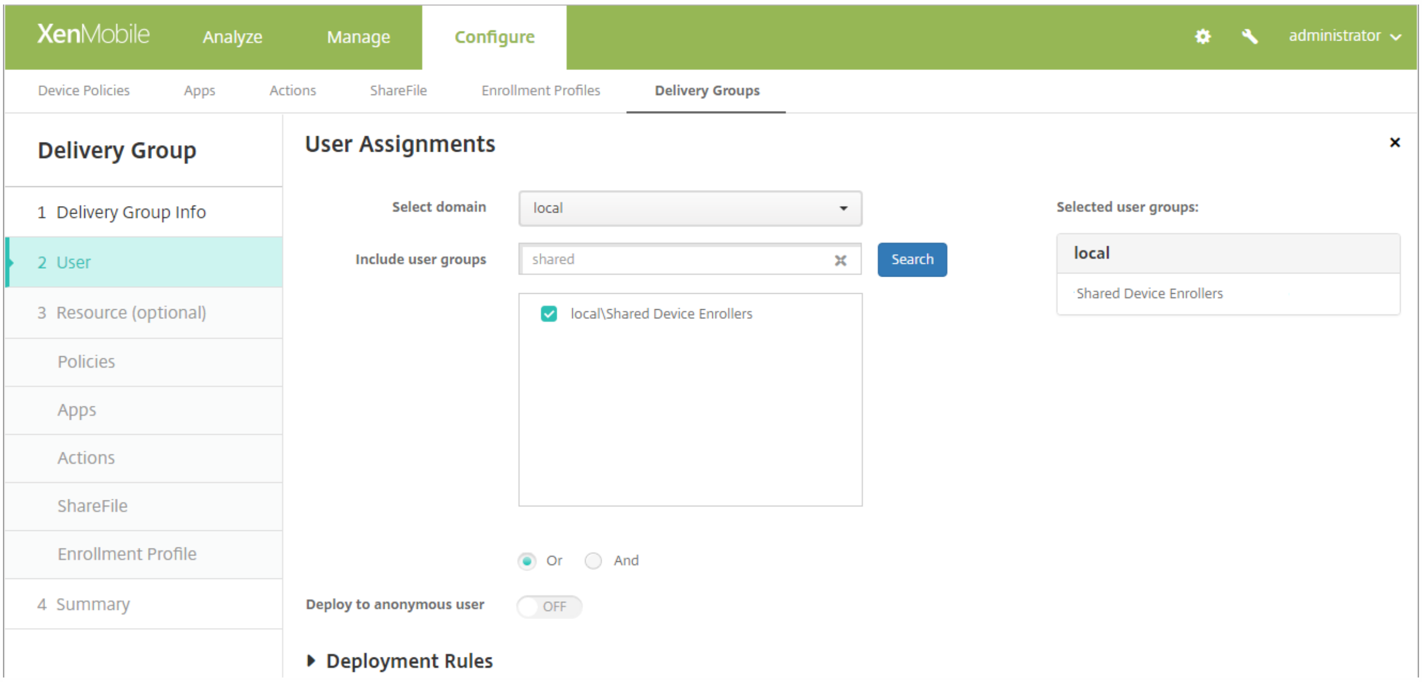
Console features:
- □ Dashboard
- □ Reporting
- ☑ Devices
  - □ Full Wipe device
  - □ Clear Restriction
  - ☑ Selective Wipe device
  - □ View locations
  - □ Lock device
  - □ Unlock device

Apply permissions:
- ● To all user groups
- ○ To specific user groups

Click **Next** to move to the **Assignment** screen. Assign the shared-device enrollment role you just created to the Active Directory group you created for shared device enrollment users in Step 1 under Pre-requisites. In the image below, **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 XenMobile using the shared device enrollment user account. You can now view and manage the device through the XenMobile console. For more information, see Enrolling Devices.

6. To apply different policies or to provide additional 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 Configuring Deployment Rules.

7. To stop sharing the device, perform a selective wipe to remove the shared device enrollment user account from the device, along with any apps and policies deployed to it.

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, while 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 that will share the device. Allowing unlimited sync is not recommended.

Number of users sharing device	Recommended max sync period
21 to 25	1 week or less
6 to 20	2 weeks or less
5 or fewer	1 month or less

- 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 will be common across users who share the device:

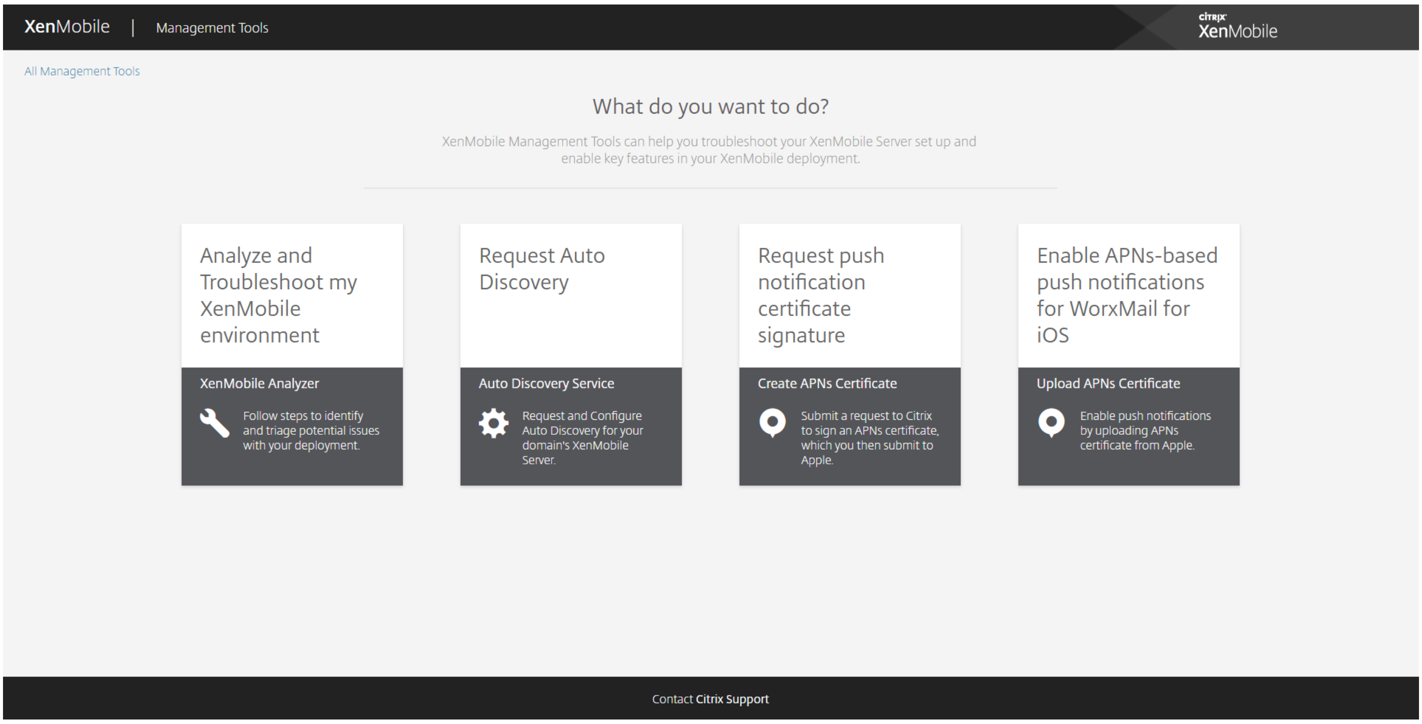
  Notifications
  Signature
  Out of Office
  Sync Mail Period
  S/MIME
  Check Spelling

XenMobile Autodiscovery Service

Jan 30, 2018

Autodiscovery is an important part of many XenMobile deployments. Autodiscovery simplifies the enrollment process for users. They can use their network user names and Active Directory passwords to enroll their devices, rather than having to also enter details about the XenMobile server. Users enter their user name in user principal name (UPN) format; for example, user@mycompany.com. The XenMobile AutoDiscovery Service enables you to create or edit an autodiscovery record without assistance from Citrix support.

To access the XenMobile AutoDiscovery Service, navigate to https://tools.xm.cloud.com and the click **Request Auto Discovery**.



What do you want to do?

XenMobile Management Tools can help you troubleshoot your XenMobile Server set up and enable key features in your XenMobile deployment.

Analyze and Troubleshoot my XenMobile environment

XenMobile Analyzer

Follow steps to identify and triage potential issues with your deployment.

Request Auto Discovery

Auto Discovery Service

Request and Configure Auto Discovery for your domain's XenMobile Server.

Request push notification certificate signature

Create APNs Certificate

Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.

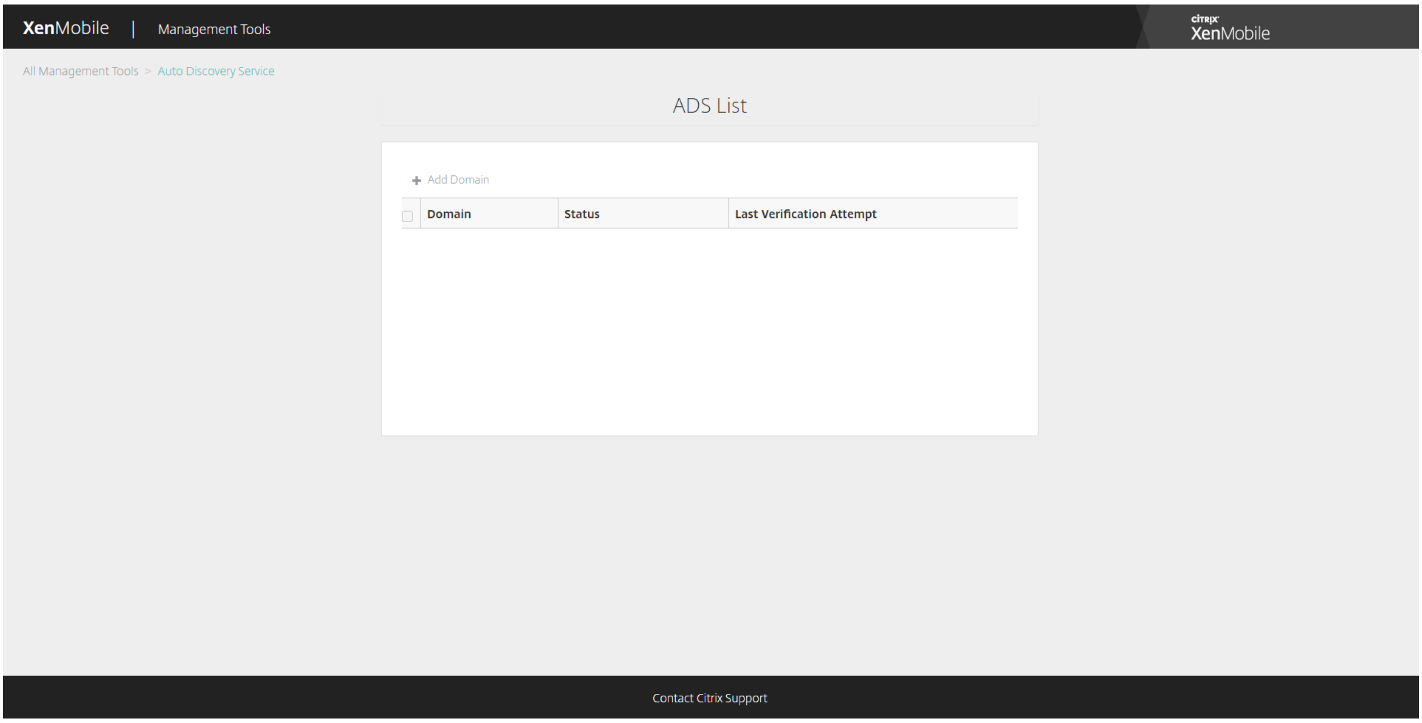
Enable APNs-based push notifications for WorxMail for iOS

Upload APNs Certificate

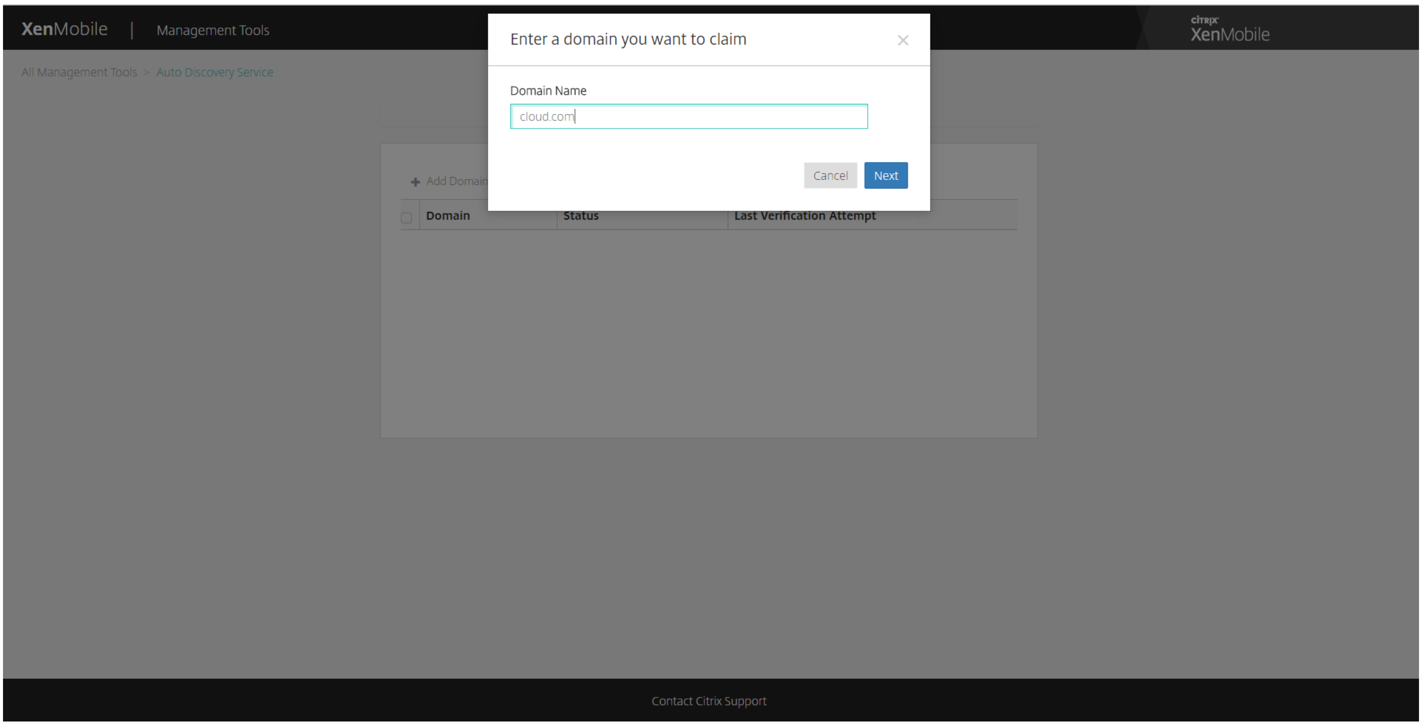
Enable push notifications by uploading APNs certificate from Apple.

Requesting AutoDiscovery

1. On the AutoDiscovery Service page, you need to first claim a domain. Click **Add Domain**.


XenMobile | Management Tools
citrix XenMobile
All Management Tools > Auto Discovery Service
ADS List
+ Add Domain
Domain
Status
Last Verification Attempt
Contact Citrix Support

2. In the dialog box that opens, enter the domain name of your XenMobile environment and then click **Next**.


XenMobile | Management Tools
citrix XenMobile
All Management Tools > Auto Discovery Service
+ Add Domain
Domain
Status
Last Verification Attempt
Contact Citrix Support

Enter a domain you want to claim

Domain Name: cloud.com

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

a. Copy the DNS token provided in the XenMobile Tools Portal.

b. Create a DNS TXT record in the zone file for your domain in your domain hosting provider portal.

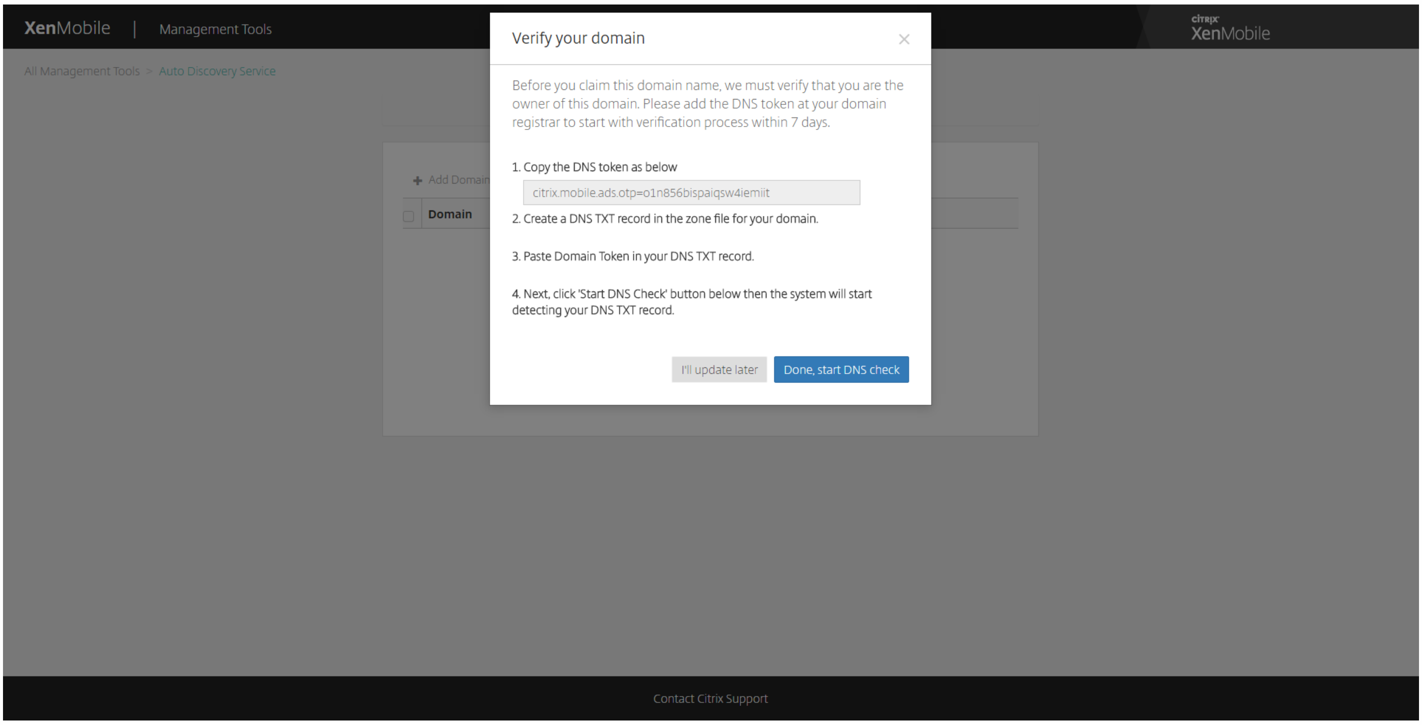
To create a DNS TXT record you need to log into the Domain Hosting Provider portal for the domain you have added in step 2 above. In the Domain Hosting portal you can edit your Domain Name Server Records and add a custom TXT record. An example below of a adding a DNS TXT entry in a hosting portal for sample domain domain.com.

c. Paste the Domain Token in your DNS TXT record and save your Domain name Server record.

d. Back in the XenMobile Tools Portal, click Done, start DNS check.

The system detects your DNS TXT record. Alternatively, you can click I'll update later, and the record is saved. The DNS check won't start until you select the Waiting record and click DNS Check.

This check ideally takes about an hour, but it can take up to two days to return a response. In addition, you may need to leave the portal and return to see the status change.


XenMobile | Management Tools
All Management Tools > Auto Discovery Service
citrix XenMobile
+ Add Domain
Domain
Contact Citrix Support

Verify your domain

Before you claim this domain name, we must verify that you are the owner of this domain. Please add the DNS token at your domain registrar to start with verification process within 7 days.

1. Copy the DNS token as below

citrix.mobile.ads.otp=o1n856bispaiqsw4iemiit

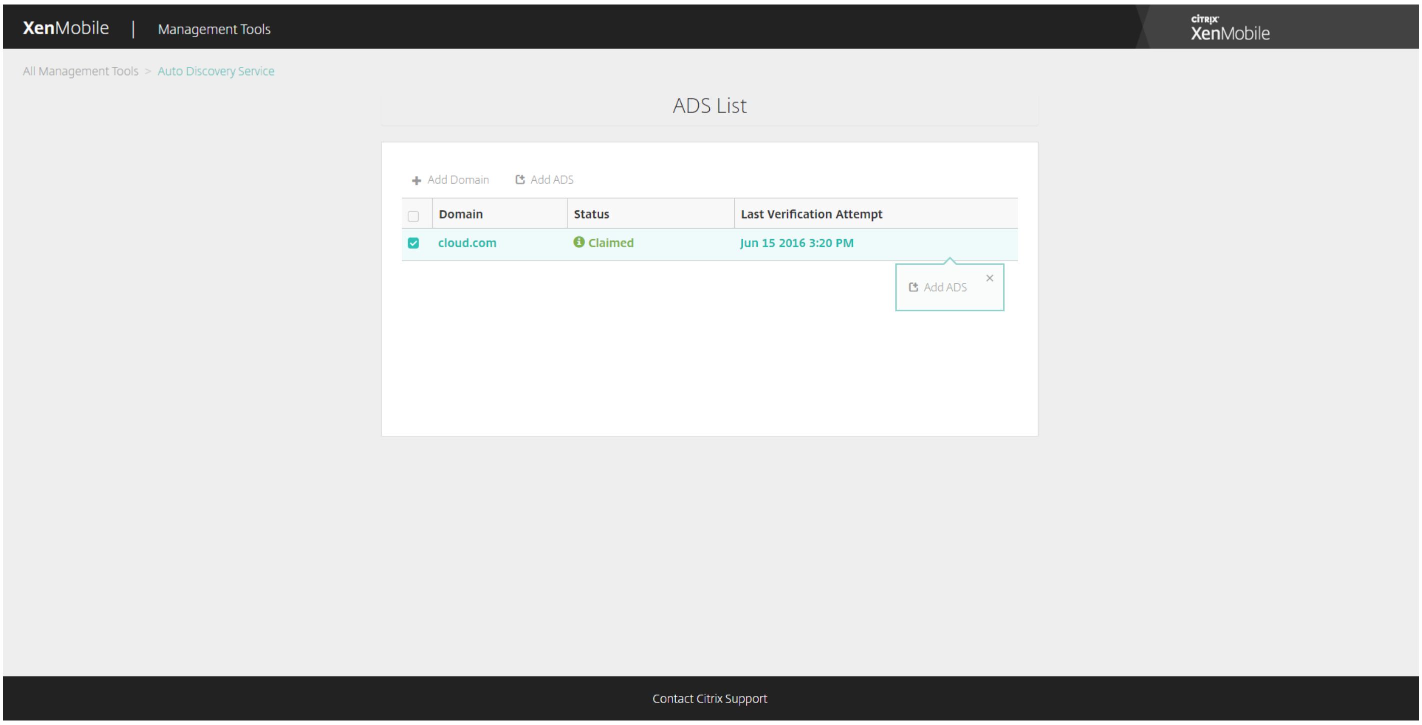
2. Create a DNS TXT record in the zone file for your domain.

3. Paste Domain Token in your DNS TXT record.

4. Next, click 'Start DNS Check' button below then the system will start detecting your DNS TXT record.

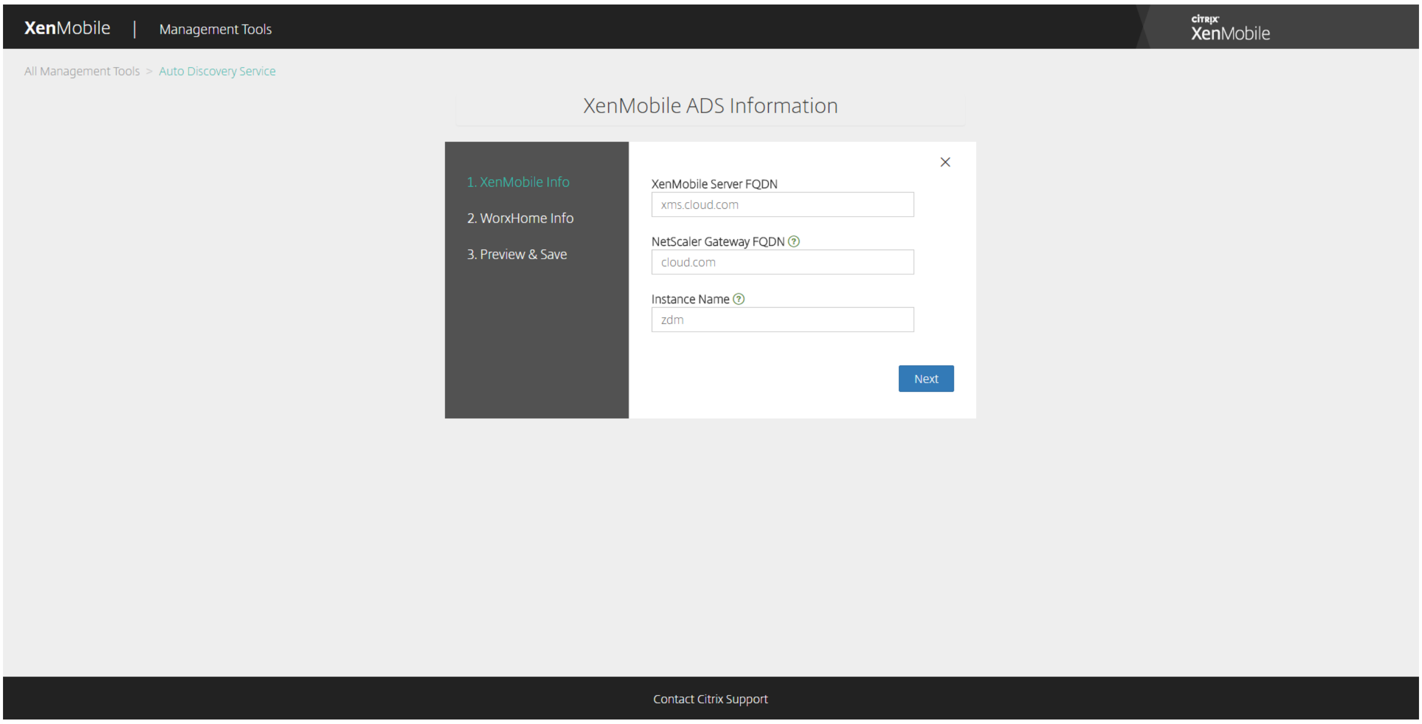
4. After you claim your domain, you can enter AutoDiscovery Service information. Right-click the domain record for which you want to request autodiscovery and then click **Add ADS**.

If your domain already has an AutoDiscovery record, please log a case with Citrix Technical Support to modify details as required.



□	Domain	Status	Last Verification Attempt
☑	cloud.com	Claimed	Jun 15 2016 3:20 PM

5. Enter your **XenMobile Server FQDN**, **NetScaler Gateway FQDN**, and **Instance Name** and then click **Next**. If you are unsure, add a default instance of "zdm".


XenMobile | Management Tools
citrix XenMobile
All Management Tools > Auto Discovery Service
XenMobile ADS Information
1. XenMobile Info
2. WorxHome Info
3. Preview & Save
×
Next
Contact Citrix Support

XenMobile Server FQDN: xms.cloud.com

NetScaler Gateway FQDN: cloud.com

Instance Name: zdm

In the screenshot above, please note that Worx Home is now called Secure Hub.

6. Enter the following information for Secure Hub and then click **Next**.

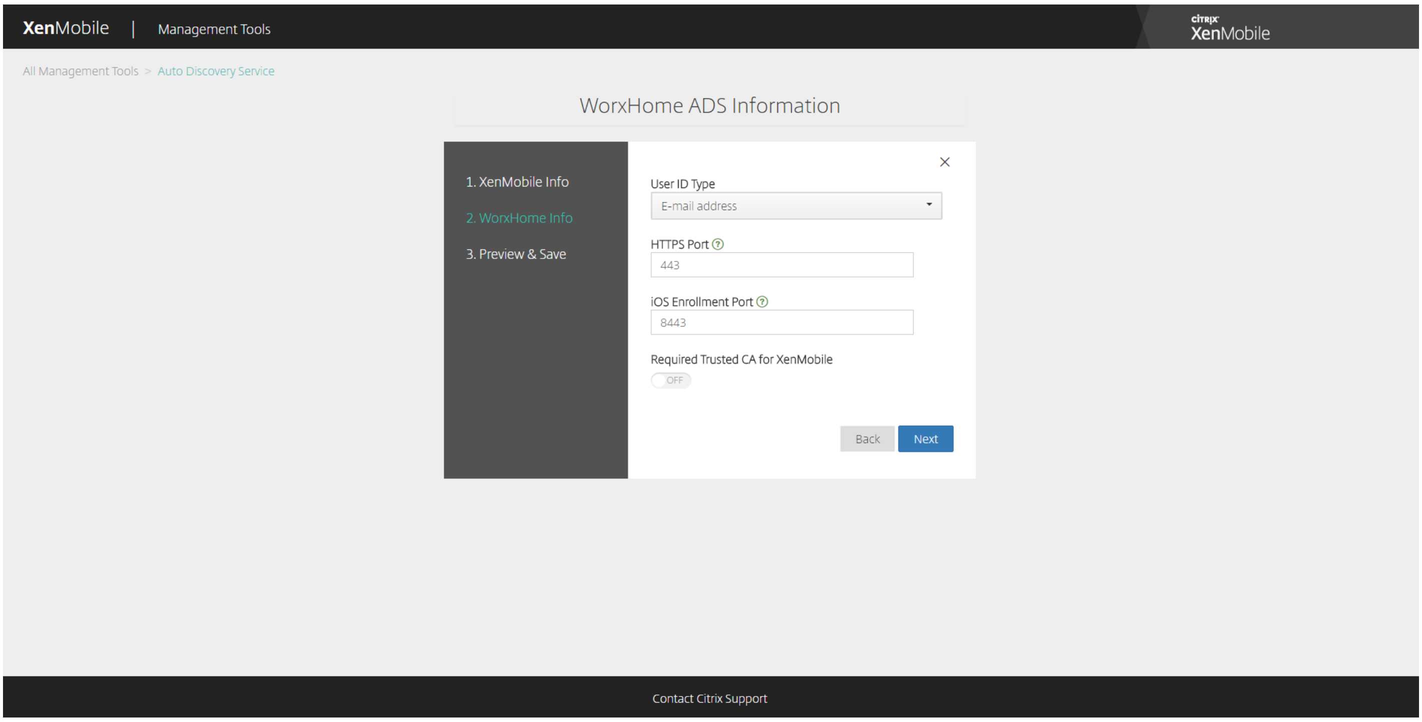
   a. **User ID Type**: Select the type of ID with which users sign on as either **E-mail address** or **UPN**.

UPN is used when the user's UPN (User Principal Name) is the same as their e-mail address. Both methods use the domain entered to find the server address. With **E-mail address** the user will be asked to enter their user name and password and with **UPN**, they will be asked to enter their password.

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

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

d. **Required Trusted CA for XenMobile**: Indicate whether a trusted certificate is required to access XenMobile or not. This option can be **OFF** or **ON**. Currently, the ability to upload a certificate for this feature does not exist. If you want to use this feature, you need to call Citrix Support, and have autodiscovery set up through them. To learn more about certificate pinning, see the section on certificate pinning in Secure Hub in the XenMobile Apps documentation. To read about the ports required for certificate pinning to work, see the support article on XenMobile Port Requirements for ADS Connectivity.



User ID Type: E-mail address

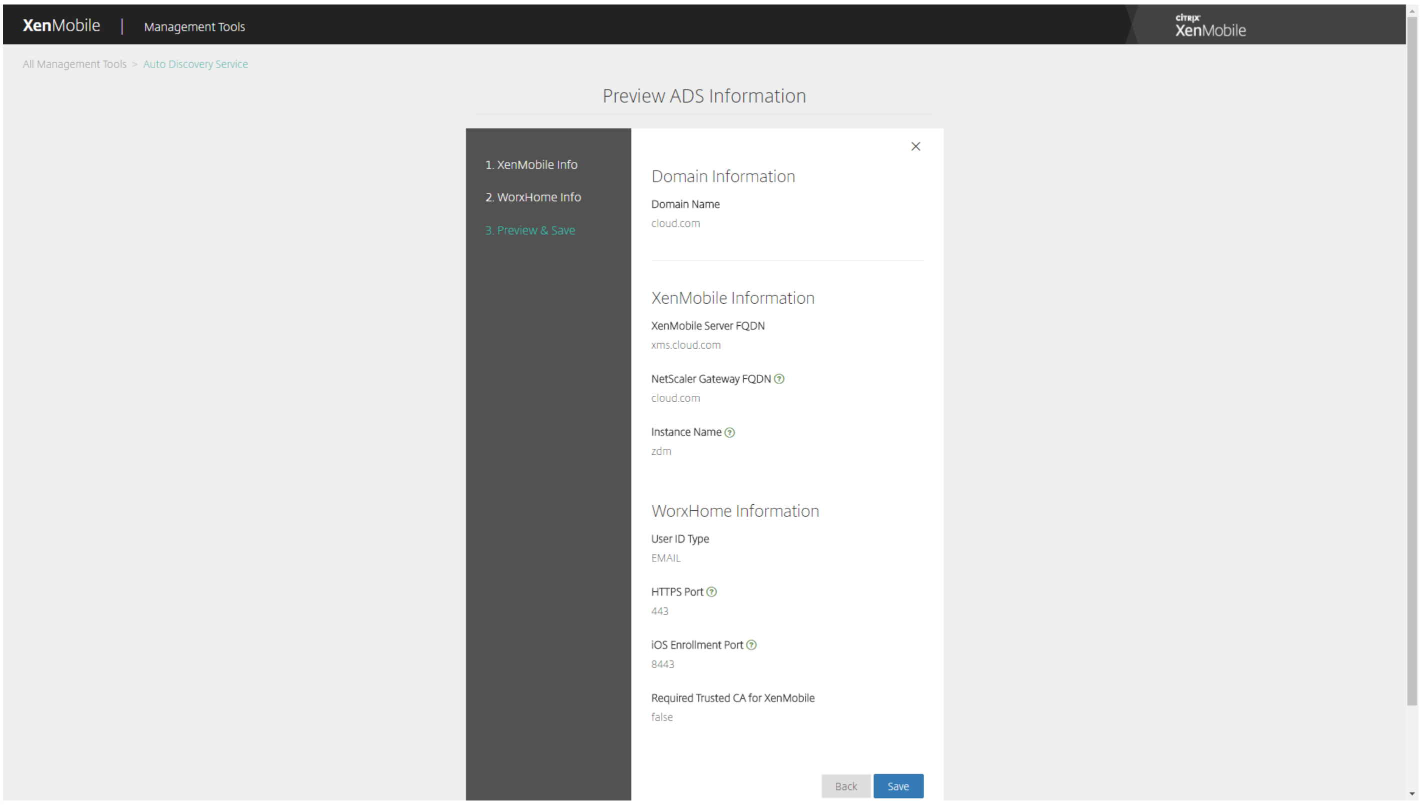
HTTPS Port: 443

iOS Enrollment Port: 8443

Required Trusted CA for XenMobile: OFF

In the screenshot above, please note that Worx Home is now called Secure Hub.

7. A summary page displays all the information you entered in the preceding steps. Verify that the data is correct then click **Save**.



Preview ADS Information

Domain Information

Domain Name
cloud.com

XenMobile Information

XenMobile Server FQDN
xms.cloud.com

NetScaler Gateway FQDN
cloud.com

Instance Name
zdm

WorxHome Information

User ID Type
EMAIL

HTTPS Port
443

iOS Enrollment Port
8443

Required Trusted CA for XenMobile
false

In the screenshot above, please note that Worx Home is now called Secure Hub.

Enable autodiscovery

Autodiscovery simplifies the enrollment process for users. They can use their network user names and Active Directory passwords to enroll their devices, rather than having to also enter details about the XenMobile server. Users enter their user name in user principal name (UPN) format; for example, user@mycompany.com.

To enable autodiscovery, you can access the Autodiscovery Service portal at https://tools.xm.cloud.com.

There may be some limited cases in which you need to contact Citrix Support to enable autodiscovery. To do so you can follow the procedures below to communicate your deployment information and, in the case of Windows devices, an SSL certificate to the Citrix Technical Support team. After Citrix receives this information, when users enroll their devices, the domain information is extracted and mapped to a server address. This information is maintained in the XenMobile database, so that the information is always accessible and available when users enroll.

1. If you are unable to enable autodiscovery using the Autodiscovery Service portal at https://tools.xm.cloud.com, open a Technical Support case using the Citrix Support portal and then provide the following information:

- The domain containing the accounts with which users will enroll.
- The XenMobile server fully qualified domain name (FQDN).
- The XenMobile instance name. By default, the instance name is zdm and is case-sensitive.
- User ID Type, which can be either UPN or Email. By default, the type is UPN.
- The port used for iOS enrollment if you changed the port number from the default port 8443.
- The port through which the XenMobile server accepts connections if you changed the port number from the default

port 443.
- Optionally, an email address for your XenMobile administrator.

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

- Obtain a publicly signed, non-wildcard SSL certificate for enterpriseenrollment.mycompany.com, where mycompany.com is the domain containing the accounts with which users will enroll. Attach the SSL certificate in .pfx format and its password to your request.
- Create a canonical name (CNAME) record in your DNS and map the address of your SSL certificate (enterpriseenrollment.mycompany.com) to autodisc.zc.zenprise.com. When a Windows device user enrolls using a UPN, in addition to providing the details of your XenMobile server, the Citrix enrollment server instructs the device to request a valid certificate from the XenMobile server.

Your Technical Support case will be updated when your details and certificate, if applicable, have been added to the Citrix servers. At this point, users can start enrolling with autodiscovery.

Note: You can also use a multi-domain certificate if you want to enroll using more than one domain. The multi-domain certificate should have the following structure:

- A SubjectDN with a CN that specifies the primary domain it serves (for example, enterpriseenrollment.mycompany1.com).
- The appropriate SANs for the remaining domains (for example, enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com, and so on).

Device policies

Dec 28, 2017

You can configure how XenMobile 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.

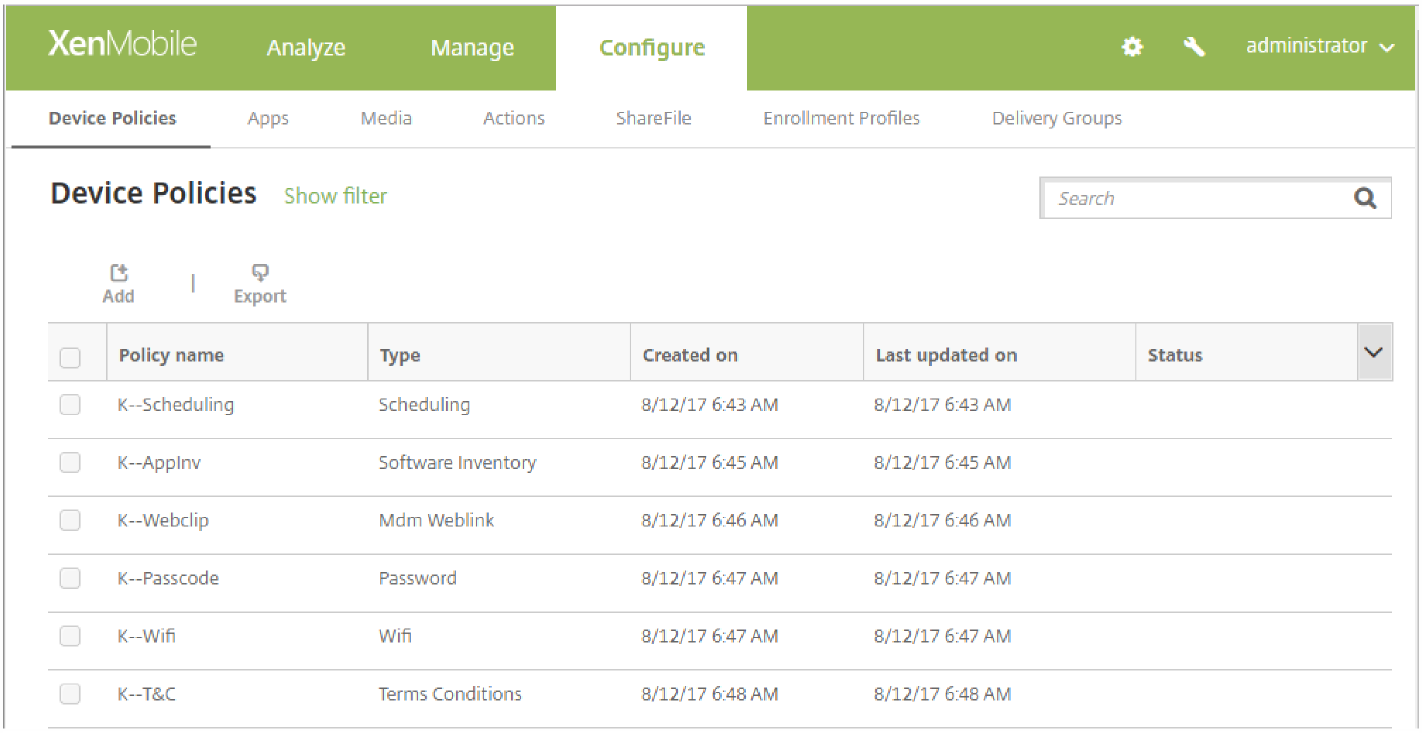
For the policies per platform matrix, download the Device Policies by Platform Matrix PDF. For a summary description of each device policy, see Device policy summaries in this article.

> ## Important
>
> Before you create a policy, complete these requirements: Create any delivery groups you plan to use. Install any necessary CA certificates.

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).

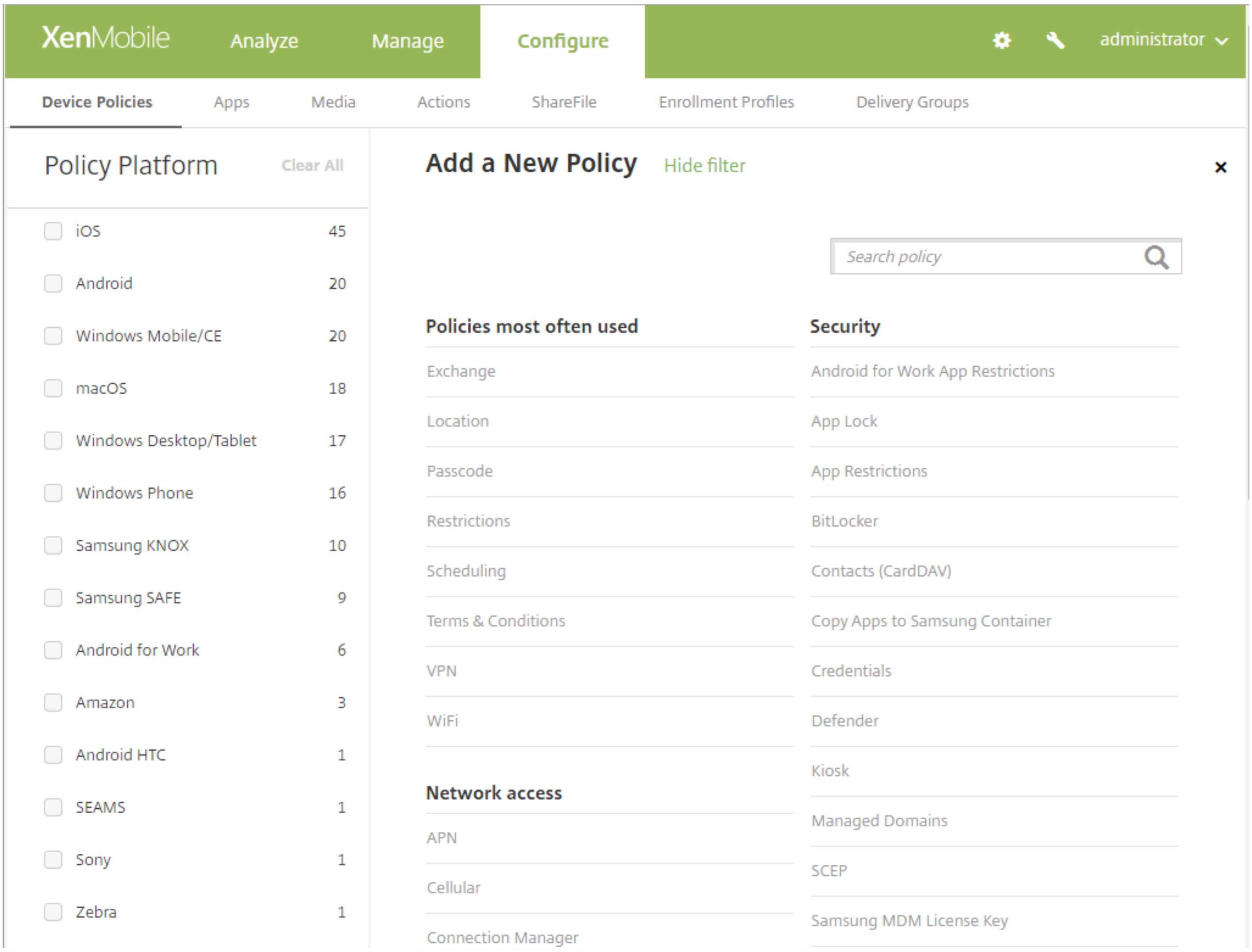
To create and manage device policies, go to **Configure > Device Policies**.



□	Policy name	Type	Created on	Last updated on	Status
□	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM	
□	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM	
□	K--Webclip	Mdm Weblink	8/12/17 6:46 AM	8/12/17 6:46 AM	
□	K--Passcode	Password	8/12/17 6:47 AM	8/12/17 6:47 AM	
□	K--Wifi	Wifi	8/12/17 6:47 AM	8/12/17 6:47 AM	
□	K--T&C	Terms Conditions	8/12/17 6:48 AM	8/12/17 6:48 AM	

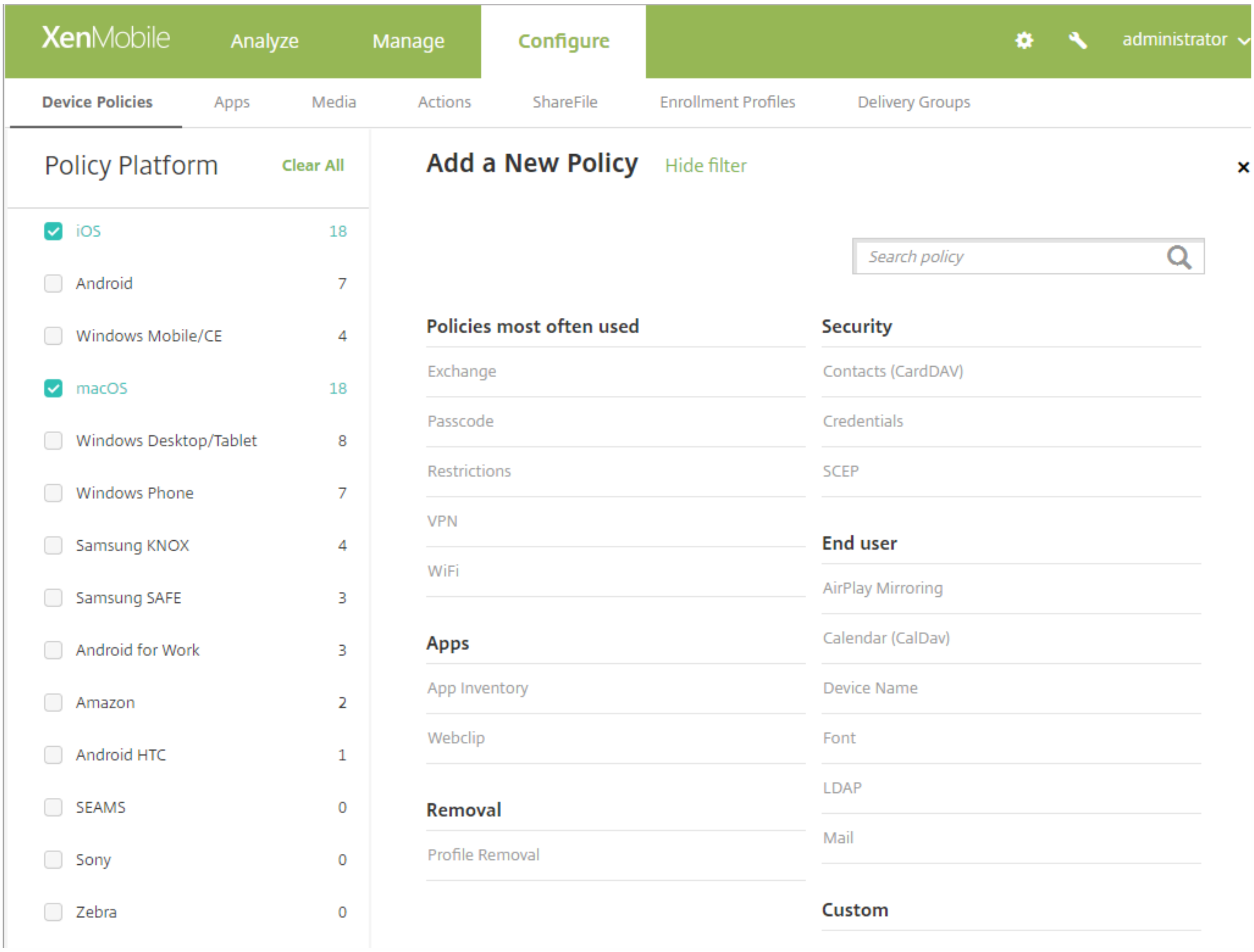
Add a device policy

1. On the **Device Policies** page, click **Add**. The **Add a New Policy** page appears.



□ iOS	45
□ Android	20
□ Windows Mobile/CE	20
□ macOS	18
□ Windows Desktop/Tablet	17
□ Windows Phone	16
□ Samsung KNOX	10
□ Samsung SAFE	9
□ Android for Work	6
□ Amazon	3
□ Android HTC	1
□ SEAMS	1
□ Sony	1
□ Zebra	1

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.



Policy Platform

☑	iOS	18
□	Android	7
□	Windows Mobile/CE	4
☑	macOS	18
□	Windows Desktop/Tablet	8
□	Windows Phone	7
□	Samsung KNOX	4
□	Samsung SAFE	3
□	Android for Work	3
□	Amazon	2
□	Android HTC	1
□	SEAMS	0
□	Sony	0
□	Zebra	0

Add a New Policy

Policies most often used
- Exchange
- Passcode
- Restrictions
- VPN
- WiFi

Apps
- App Inventory
- Webclip

Removal
- Profile Removal

Security
- Contacts (CardDAV)
- Credentials
- SCEP

End user
- AirPlay Mirroring
- Calendar (CalDav)
- Device Name
- Font
- LDAP
- Mail

Custom

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.

To configure deployment rules:

Note: For more information about configuring deployment rules, see Deploy resources.

a. Expand **Deployment Rules** and then configure the following settings. The **Base** tab appears by default.

- In the lists, click options to determine when the policy should be deployed. 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.

b. Click the **Advanced** tab to combine the rules with Boolean options. The conditions you chose on the **Base** tab appear.

c. 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.

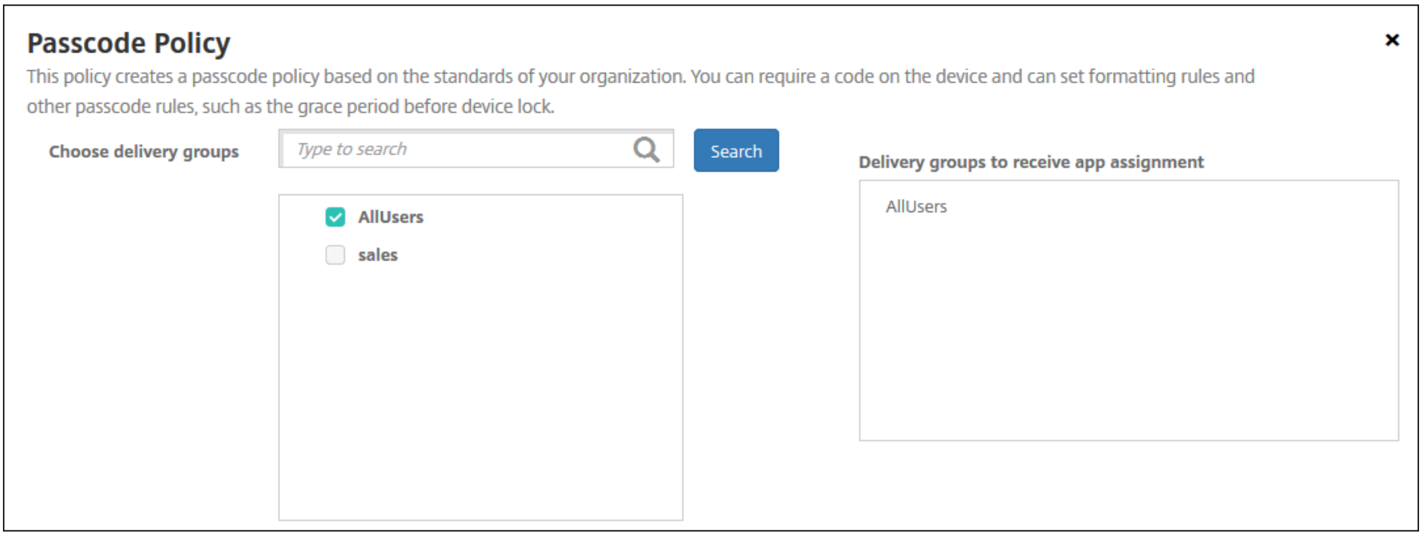
At any time, you can click to select a condition and then click **EDIT** to change the condition or **Delete** to remove the condition.

- Click **New Rule** to add another condition.

6. Click **Next** to move to the next platform page or, when all the platform pages are complete, to the **Assignments** page.

7. 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.

Note: **Delivery groups to receive app assignment** doesn't appear until you select a delivery group.



Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

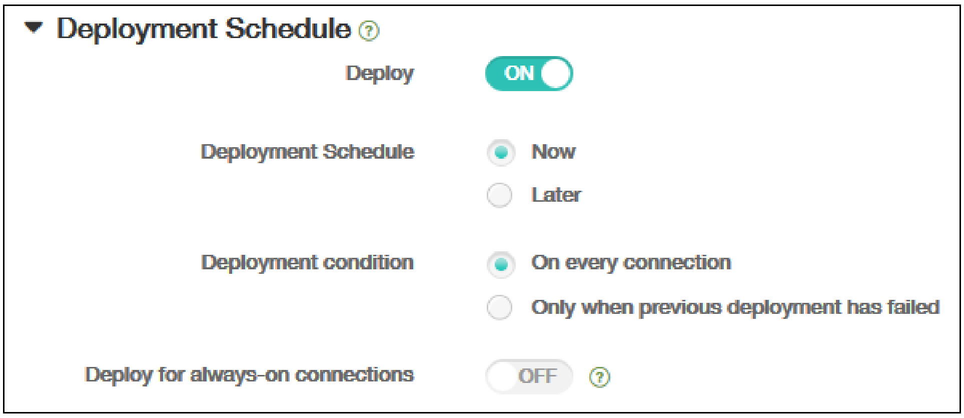
8. On the **Assignments** page, expand **Deployment Schedule** and then configure the following settings:

- 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.

- 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**, which does not apply to iOS.



Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

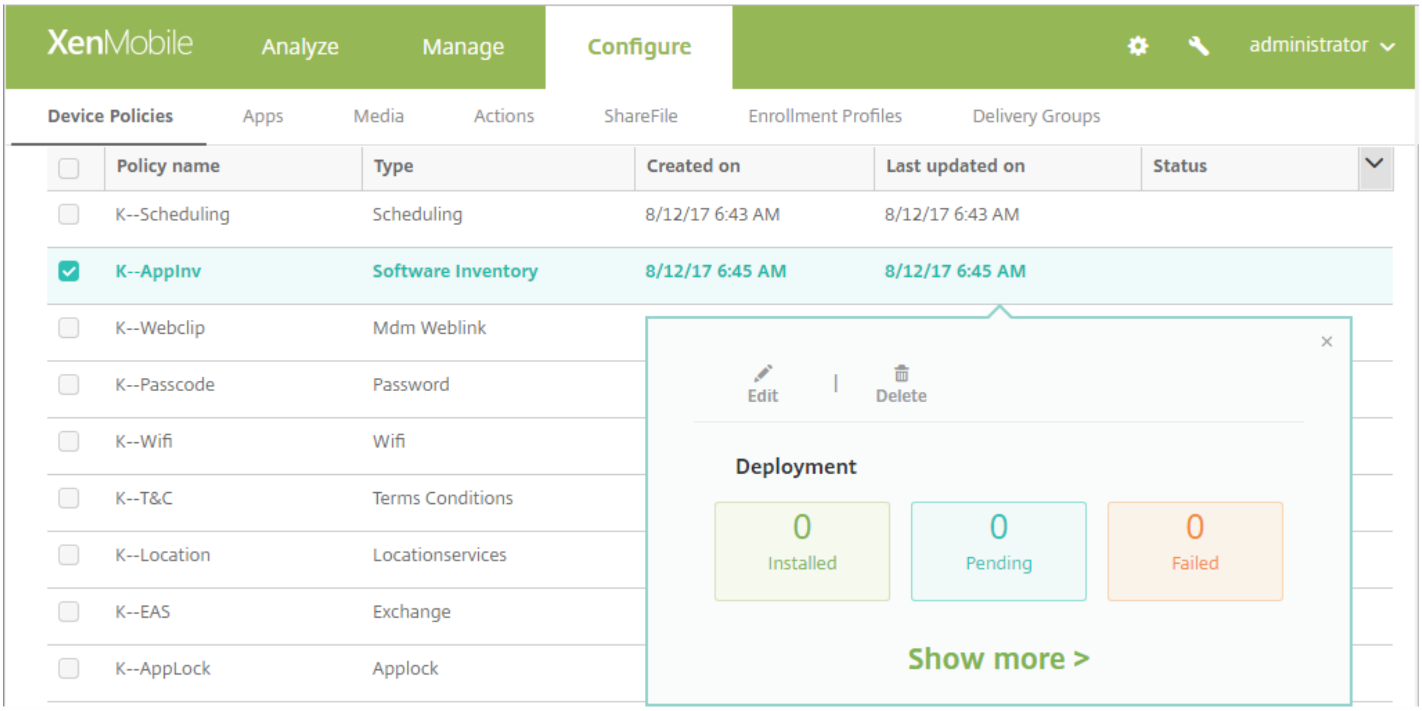
Deploy for always-on connections: OFF

9. 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 to show the options menu above the policy list. Or, click a policy in the list to show the options menu to the right of the listing.



	Policy name	Type	Created on	Last updated on	Status
□	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM	
☑	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM	
□	K--Webclip	Mdm Weblink			
□	K--Passcode	Password			
□	K--Wifi	Wifi			
□	K--T&C	Terms Conditions			
□	K--Location	Locationservices			
□	K--EAS	Exchange			
□	K--AppLock	Applock			

Edit | Delete

Deployment

0 Installed	0 Pending	0 Failed

Show more >

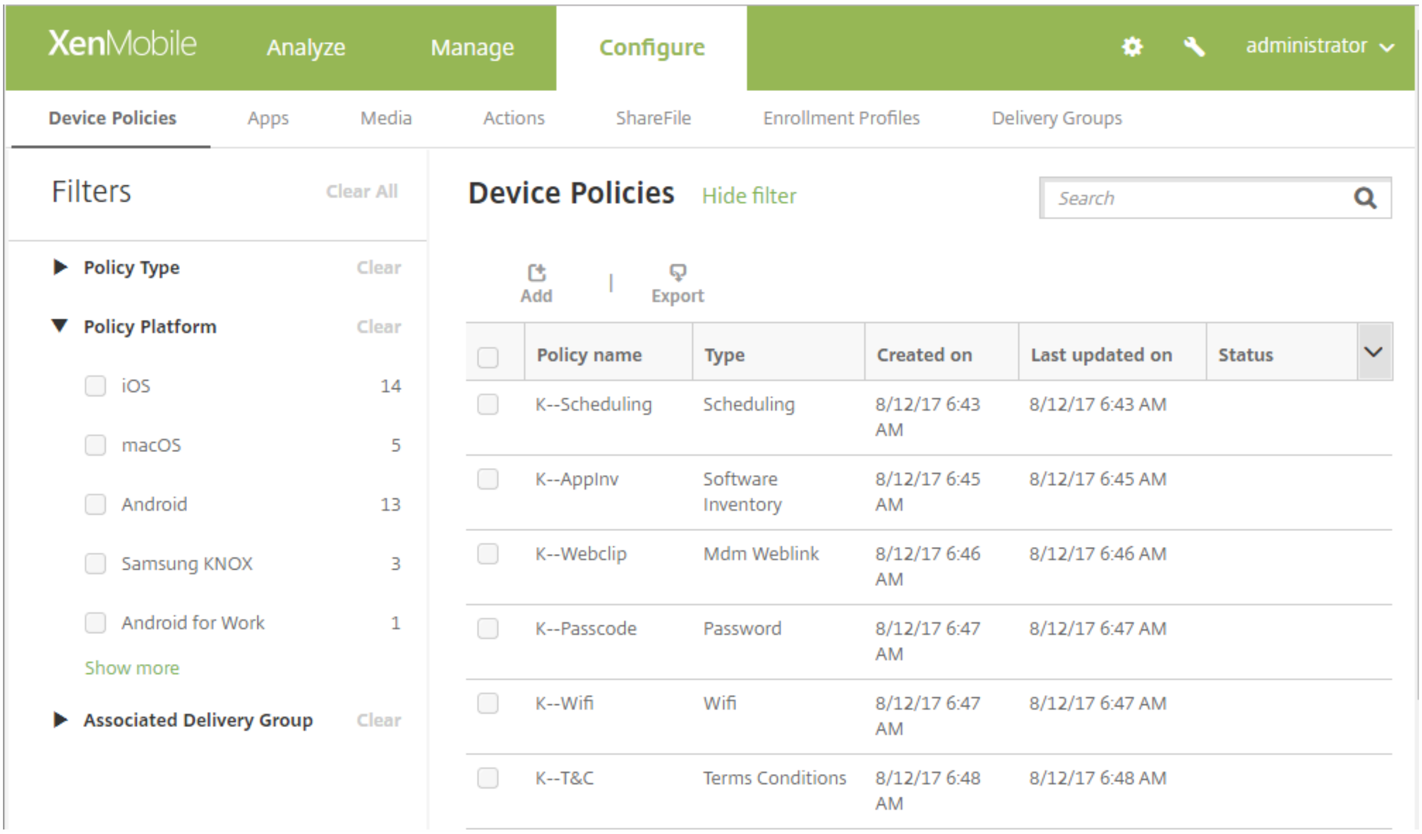
To view policy details, click **Show more**.

To edit all settings for a device policy, click **Edit**.

If you click **Delete**, a confirmation dialog box appears. Click **Delete** again.

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.



□	iOS	14
□	macOS	5
□	Android	13
□	Samsung KNOX	3
□	Android for Work	1

□	Policy name	Type	Created on	Last updated on	Status
□	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM	
□	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM	
□	K--Webclip	Mdm Weblink	8/12/17 6:46 AM	8/12/17 6:46 AM	
□	K--Passcode	Password	8/12/17 6:47 AM	8/12/17 6:47 AM	
□	K--Wifi	Wifi	8/12/17 6:47 AM	8/12/17 6:47 AM	
□	K--T&C	Terms Conditions	8/12/17 6:48 AM	8/12/17 6:48 AM	

Click **SAVE THIS VIEW** to save a filter. The name of the filter then appears in a button below the **SAVE THIS VIEW** button.

Device policy summaries

Device Policy Name	Device Policy Description
AirPlay Mirroring	Adds specific AirPlay devices (such as Apple TV or another Mac computer) to iOS devices. You also have the option of adding devices to a whitelist for supervised devices, which limits users to only the AirPlay devices on the whitelist.
AirPrint	Adds AirPrint printers to the AirPrint printer list on iOS devices. This policy makes it easier to support environments where the printers and the devices are on different subnets. Available for iOS 7.0 and later. Note: Be sure to have the IP address and resource path for each printer.

Android for Work App Restrictions	Updates the restrictions associated with Android apps.
APN	Determines the settings used to connect your devices to the General Packet Radio Service (GPRS) of a specific phone carrier. This setting is already defined in most newer phones. Use this policy if your organization doesn't use a consumer APN to connect to the internet from a mobile device.
App Access	Defines a list of the apps that are required to be installed on the device, that can be installed on the device, or that 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.
App Attributes	Specifies attributes, such as a managed app bundle ID or per-app VPN identifier, for iOS devices.
App Configuration	Remotely configures various settings and behaviors of apps that support managed configuration. To do that, you deploy an XML configuration file (called a property list, or plist) to iOS devices. Or, you deploy key/value pairs to Windows 10 phone, desktop, or tablet devices.
App Inventory	Collects an inventory of the apps on managed devices. XenMobile 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.
App Lock	Defines a list of apps that users either can or can't run on iOS or certain Android devices.
App Network Usage	Sets network usage rules to specify how managed apps use networks, such as cellular data networks, on iOS devices. The rules only apply to managed apps. Managed apps are apps that you deploy to user devices through XenMobile.
App Restrictions	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.
App Uninstall	Remove apps from user devices.
App Uninstall Restrictions	Specifies the apps that users can or can't uninstall.
BitLocker	Configures the settings available in the BitLocker interface on Windows 10 devices.
Browser	Defines whether user devices can use the browser or which browser functions the devices can use.
Calendar	Adds a calendar (CalDAV) account to iOS or macOS devices. The CalDAV account enables users to

(CalDav)	synchronize scheduling data with any server that supports CalDAV.
Cellular	Configures cellular network settings.
Connection Manager	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.
Contacts (CardDAV)	Adds an iOS contact (CardDAV) account to iOS or macOS devices. The CardDAV account enables users to synchronize contact data with any server that supports CardDAV.
Control OS Updates	Deploys the latest OS updates to supported, supervised devices.
Copy apps to Samsung Container	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.
Credentials	Enables integrated authentication with your PKI configuration in XenMobile. For example, with a PKI entity, a keystore, a credential provider, or a server certificate. For information about credentials, see Certificates and authentication.
Custom XML	Customizes features such as device provisioning, device feature enablement, device configuration, and fault management.
Defender	Configures Windows Defender settings for Windows 10 for desktop and tablet.
Delete Files and Folders	Deletes specific files or folders from Windows Mobile/CE devices.
Delete Registry Keys and Values	Deletes specific registry keys and values from Windows Mobile/CE devices.
Device Health Attestation	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 XenMobile. When XenMobile receives the Health Attestation Certificate, based on the contents of that certificate, it can deploy automatic actions that you configured.
Device Name	Sets the names on iOS and macOS devices so that you can identify the devices. You can use macros, text, or a combination of both to define a device name. For information about macros, see Macros.
Education	Configures instructor and student devices for use with Apple Education. If instructors use the

Configuration	Classroom app, the Education Configuration device policy is required.
Enterprise Hub	Distributes apps to Windows Phones through the Enterprise Hub Company store. XenMobile 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 XenMobile Enterprise Edition. You can deploy the initial Enterprise Hub policy only during device enrollment.
Exchange	Enables ActiveSync email for the native email client on the device.
Files	Adds script files to XenMobile 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.
Font	Adds fonts to iOS and macOS devices. Fonts must be TrueType (.TTF) or OpenType (.OFT) fonts. Font collections (.TTC or .OTC) are not supported.
Home screen layout	Specifies the layout of apps and folders for the iOS Home screen on iOS 9.3 and later supervised devices.
Import iOS & macOS Profile	Imports device configuration XML files for iOS and macOS devices into XenMobile. The file contains device security policies and restrictions that you prepare by using the Apple Configurator. For more information about using the Apple Configurator to create a configuration file, see the Apple Configurator Help page.
Kiosk	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.
Launcher Configuration	Specifies the following for Citrix Launcher on Android devices: The apps allowed, a custom logo image for the Citrix Launcher icon, a custom background image for Citrix Launcher, and password requirements to exit the launcher.
LDAP	Provides information about an LDAP server to use for iOS devices, including any necessary account information such as the LDAP server host name. The policy also provides a set of LDAP search policies to use when querying the LDAP server.
Location	Lets you geo-locate devices on a map, assuming that the device has GPS enabled for Secure Hub. After deploying this policy to the device, you can send a locate command from the XenMobile Server. The device then responds with its location coordinates. XenMobile also supports geofencing and tracking policies.
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 8 and later supervised devices, you can specify URLs or subdomains to control how users can open documents, attachments, and downloads from the browser.
MDM Options	Manages Find My Phone and iPad Activation Lock on supervised iOS 7.0 and later phone devices. For the steps on putting an iOS device in supervised mode, see Bulk enrollment of iOS and macOS devices.
Organization Info	Specifies organization information for alert messages that XenMobile deploys to iOS devices.
Passcode	Enforces a PIN code or password on a managed device. You can set the complexity and timeouts for the passcode on the device.
Personal Hotspot	Allows users to connect to the internet when they are not in range of a WiFi network. Users connect through the cellular data connection on their iOS device, using personal hotspot functionality.
Profile Removal	Removes the app profile from iOS or macOS devices.
Provisioning Profile	Specifies an enterprise distribution provisioning profile to send to devices. When you develop and code sign an iOS enterprise app, you usually include a provisioning profile. Apple requires the profile for the app to run on an iOS device. If a provisioning profile is missing or has expired, the app crashes when a user taps to open it.
Provisioning Profile Removal	Removes iOS provisioning profiles.
Proxy	Specifies global HTTP proxy settings for devices running Windows Mobile/CE and iOS. You can deploy only one global HTTP proxy policy per device.
Registry	Defines the registry keys and values that let you administer Windows Mobile/CE devices. The Windows Mobile/CE registry stores data about apps, drivers, user preferences, and configuration settings.
Remote Support	Provides you with remote access to Samsung KNOX devices.
Restrictions	Provides hundreds of options to lock down and control features and functionality on managed devices. Examples of restriction options: Disable the camera or microphone, enforce roaming rules,

	and enforce access to third-party services, such as app stores.
Roaming	Configures whether to allow voice and data roaming on iOS and Windows Mobile/CE devices. If voice roaming is disabled, data roaming is automatically disabled.
Samsung SAFE Firewall	Configures the firewall settings for Samsung devices. You provide the IP addresses, ports, and host names that you want to allow devices to access or that you want to block devices from accessing. You can also configure the proxy and proxy reroute settings.
Samsung MDM License Key	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. XenMobile supports and extends both Samsung for Enterprise (SAFE) and Samsung KNOX policies.
Scheduling	Required for Android and Windows Mobile devices to connect back in to the XenMobile Server 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.
SCEP	Configures iOS and macOS devices to retrieve a certificate from an external SCEP server. You can also deliver a certificate to the device using SCEP from a PKI that is connected to XenMobile. To do that, create a PKI entity and a PKI provider in distributed mode. For details, see PKI entities.
SSO Account	Creates single sign-on (SSO) accounts so users sign on one-time only to access XenMobile and your internal company resources. 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 compatible with Kerberos authentication. Available for iOS.
Storage Encryption	Encrypts internal and external storage. For some devices, this policy prevents users from using a storage card on their devices.
Subscribed Calendars	Adds 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. Ensure that you subscribe to a calendar before you add it to the subscribed calendars list on user devices.
Terms and Conditions	Requires that users accept the specific policies of your company that govern connections to the corporate network. When users enroll their devices with XenMobile, they must accept the terms and conditions to enroll their devices. Declining the terms and conditions cancels the enrollment process.
Tunnel	Used only for Remote Support. For information about Remote Support, see Support options and Remote Support. This policy increases service continuity and data transfer reliability for your mobile apps.
VPN	Provides access to back end systems that use legacy VPN gateway technology. This policy provides VPN gateway connection details that you can deploy to devices. XenMobile supports several VPN providers, including Cisco AnyConnect, Juniper, and Citrix VPN. If your VPN gateway supports this

	option, you can link this policy to a CA and enable VPN on-demand.
Wallpaper	Adds a .png or .jpg file to set wallpaper on an iOS device lock screen, home screen, or both. To use different wallpaper on iPads and iPhones, create different wallpaper policies and deploy them to the appropriate users.
Web Content Filter	Filters web content on iOS devices. XenMobile uses the Apple auto-filter function and the sites that you add to whitelists and blacklists. Available only for iOS supervised devices. For information about placing an iOS device in Supervised mode, see Place an iOS device in Supervised mode by using the Apple Configurator.
Webclip	Places shortcuts, or webclips, to websites so that they appear alongside apps on user 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.
WiFi	Allows administrators to deploy WiFi router details to managed devices. The router details include SSID, authentication data, and configuration data.
Windows CE Certificate	Creates and delivers Windows Mobile/CE certificates from an external PKI to user devices. For more information about certificates and PKI entities, see Certificates and authentication.
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.
XenMobile Store	Specifies whether a XenMobile Store webclip appears on the home screen of user devices.
XenMobile Options	Configures the Secure Hub behavior when connecting to XenMobile from Android and Windows Mobile/CE devices.
XenMobile Uninstall	Uninstalls XenMobile from Android and Window Mobile/CE devices. When deployed, this policy removes XenMobile from all devices in the deployment group.

Device policies by platform

Sep 13, 2017

To view the policies per platform, download the Device Policies by Platform Matrix PDF. You add and configure the device policies in the XenMobile console from **Configure > Device Policies**.

The latest release of XenMobile supports device policies for the following platforms:

- Amazon
- iOS
- macOS
- Android HTC
- Android TouchDown
- Android for Work
- Android
- Android Sony
- Android Zebra
- Samsung SAFE
- Samsung KNOX
- Samsung SEAMS
- Windows 10 Phone
- Windows 10 Desktop/Tablet
- Windows Phone 8.1
- Windows Mobile/CE

For details on supported devices in the latest release of XenMobile, see Supported device platforms.

> ## Note
>
> If your environment is configured with Group Policy Objects (GPOs):
>
> When you configure XenMobile device policies for Windows 10, keep the following rule in mind. If a policy on one or more enrolled Windows 10 devices conflicts, the policy aligned with the GPO takes precedence.

AirPlay mirroring device policy

Sep 06, 2017

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 XenMobile to add specific AirPlay devices (such as Apple TV or another Mac computer) to users' 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.

1. In the XenMobile 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 **End user**, click **AirPlay Mirroring**. The **AirPlay Mirroring Policy** page appears.

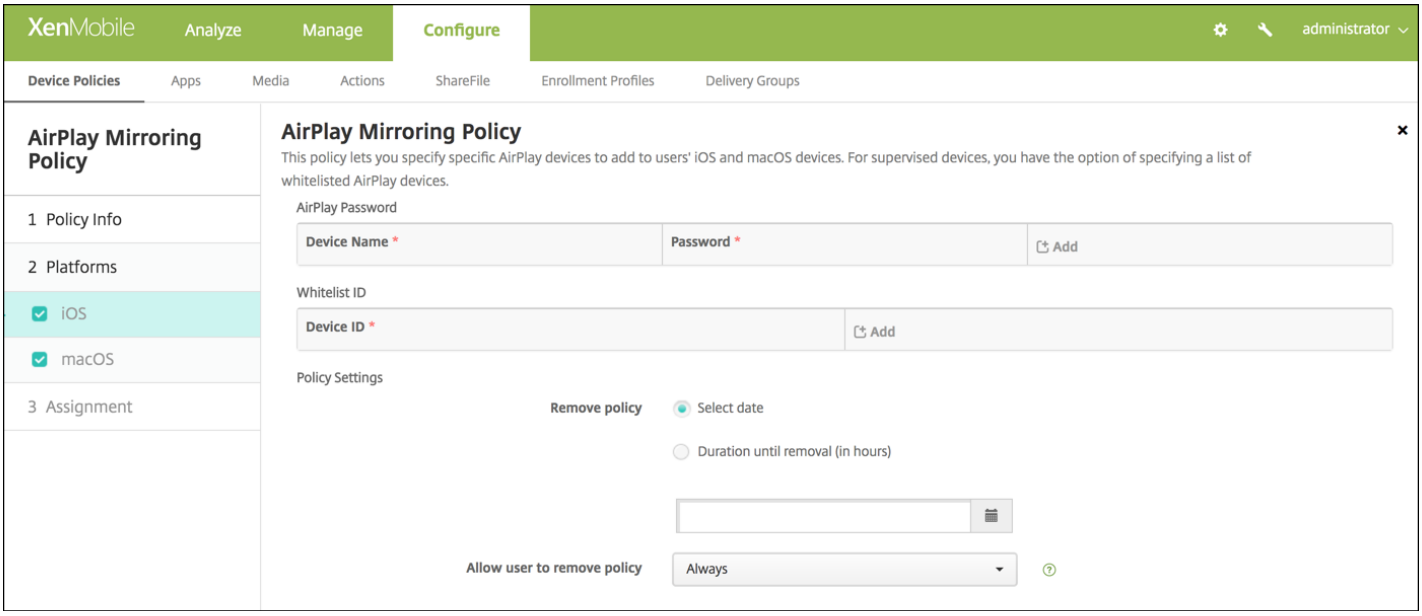
4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.



AirPlay Mirroring Policy

This policy lets you specify specific AirPlay devices to add to users' iOS and macOS devices. For supervised devices, you have the option of specifying a list of whitelisted AirPlay devices.

AirPlay Password

Device Name *	Password *	Add

Whitelist ID

Device ID *	Add

Policy Settings

Remove policy: ● Select date ○ Duration until removal (in hours)

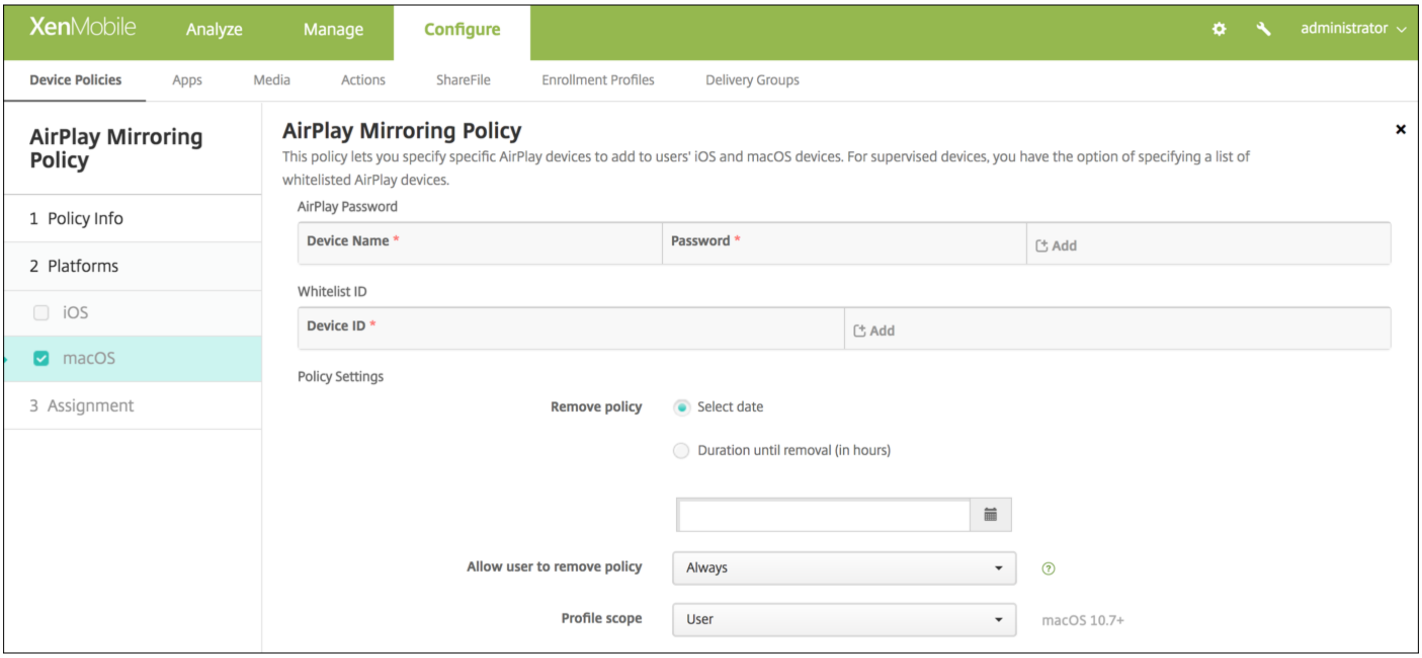
Allow user to remove policy: Always

Configure these 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.

  Note: To delete an existing device, hover over the line containing the listing and click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

  To edit an existing device, hover over the line containing the listing and click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.
- **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.



AirPlay Mirroring Policy

This policy lets you specify specific AirPlay devices to add to users' iOS and macOS devices. For supervised devices, you have the option of specifying a list of whitelisted AirPlay devices.

AirPlay Password

Device Name *	Password *

Whitelist ID

Device ID *

Policy Settings

Remove policy ● Select date ○ Duration until removal (in hours)

Allow user to remove policy: Always

Profile scope: User — macOS 10.7+

Configure these 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.

  Note: To delete an existing device, hover over the line containing the listing and click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

  To edit an existing device, hover over the line containing the listing and click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- **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**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

AirPrint device policy

Sep 06, 2017

You can add a device policy in XenMobile to add AirPrint printers to the AirPrint printer list on users' iOS devices. This policy makes it easier to support environments where the printers and the devices are on different subnets.

Note:

- This policy applies to iOS 7.0 and later.
- Be sure to have the IP address and resource path for each printer.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More** and then, under **End user**, click **AirPrint**. The **AirPrint Policy** 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 **iOS Platform Information** page appears.

6. Configure these 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.
  - Click **Save** to add the printer or click **Cancel** to cancel adding the printer.

    Note: To delete an existing printer, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing.

    To edit an existing printer, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click Save to save the changed listing or Cancel to leave the listing unchanged.

- **Policy Settings**
  - 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.
  - 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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Android for Work app restriction policy

Sep 06, 2017

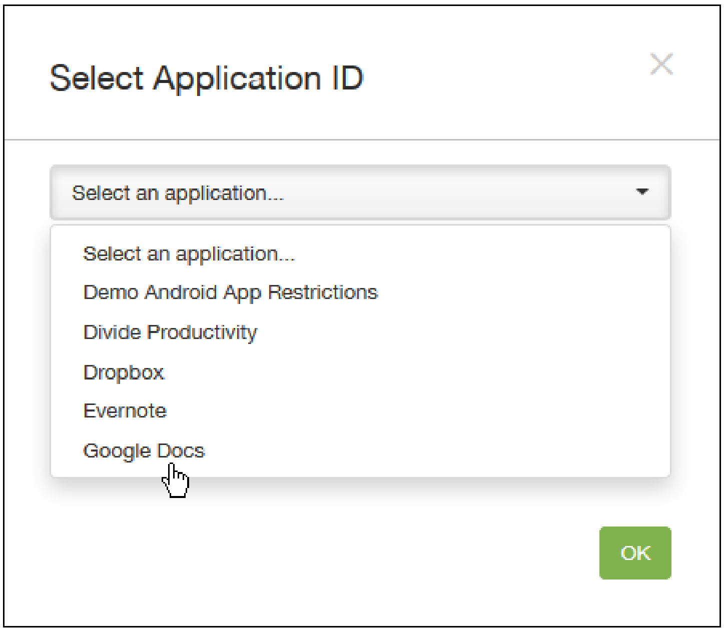
You can modify the restrictions associated with Android for Work apps, but before you can do so, you must meet the following prerequisites:

- Complete Android for Work setup tasks on Google. For more information, see Managing Devices with Android for Work.
- Create an Android for Work account. For more information, see Create an Android for Work account.
- Add Android for Work apps to XenMobile. For more information, see Adding Apps to XenMobile.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

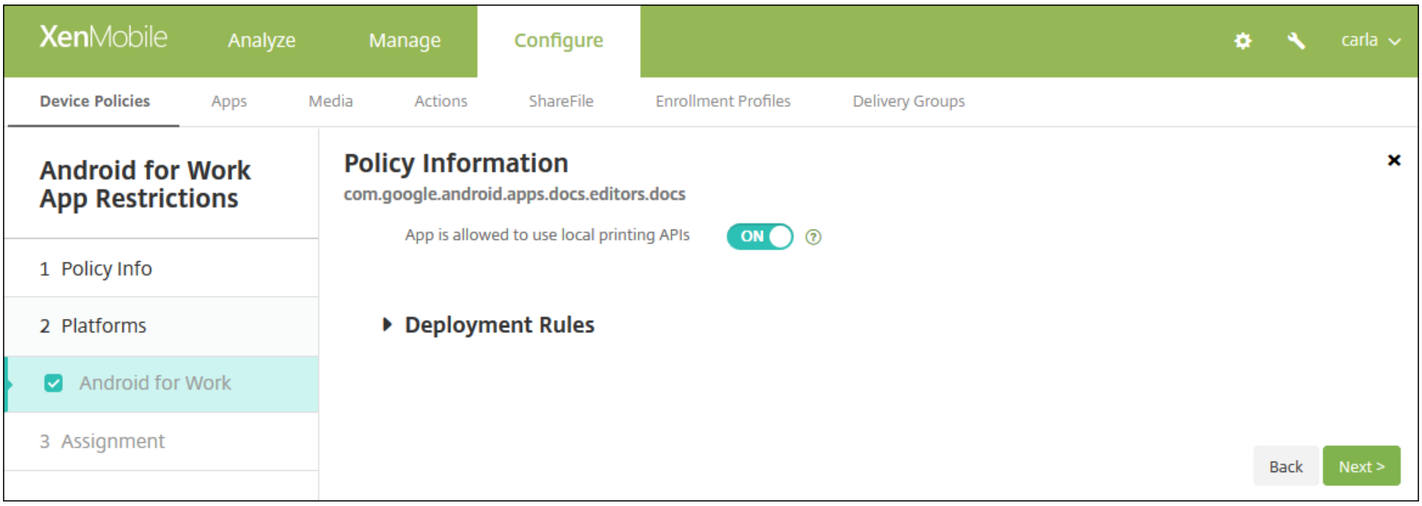
2. Click **Add** to add a new policy. The **Add a New Policy** page appears.

3. Expand **More** and then under **Security**, click **Android for Work App Restrictions**. A dialog box appears asking you to select an app.



4. In the list, select the app to which you want to apply restrictions and then click **OK**.

- If there are no Android for Work apps added to XenMobile, you cannot proceed. For more information about adding apps to XenMobile, see Adding Apps to XenMobile.
- If the app has no restrictions associated with it, a notification to that effect appears. Click **OK** to dismiss the dialog box.
- If the app has restrictions associated with it, the **Android for Work App Restrictions Policy** information page appears.



Policy Information

com.google.android.apps.docs.editors.docs

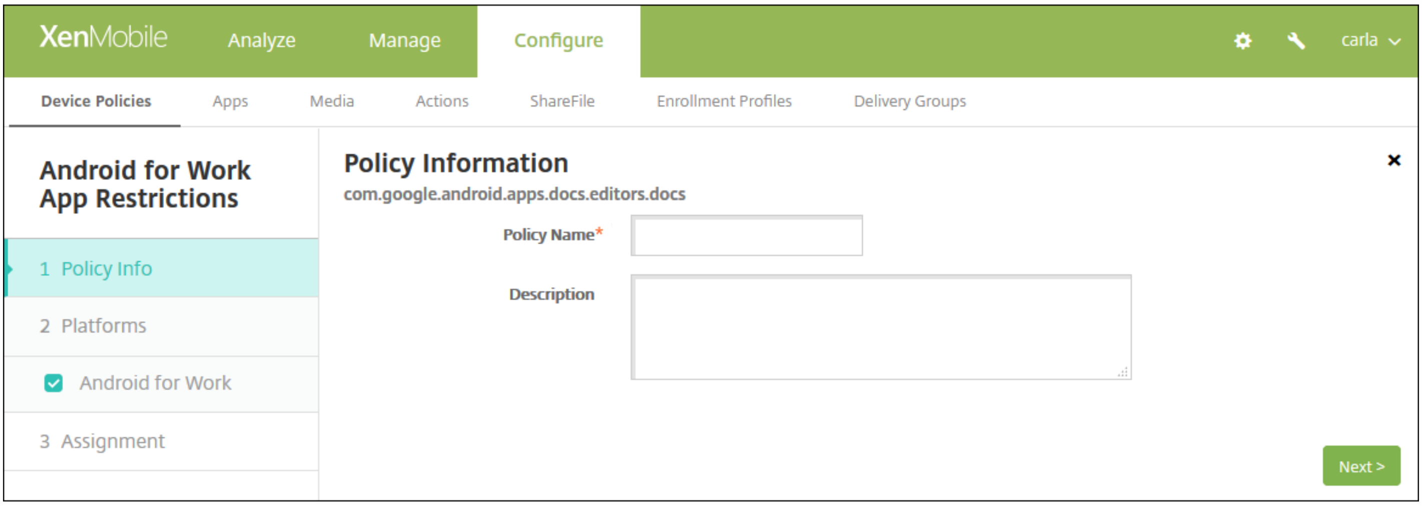
App is allowed to use local printing APIs: ON

Deployment Rules

5. 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.

6. Click **Next**. The **Android for Work Platform** page appears.



Policy Information

com.google.android.apps.docs.editors.docs

Policy Name*

Description

7. Configure the settings for the app you selected. The settings you see depend on the restrictions associated with the selected app.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

APN device policy

Sep 06, 2017

You can add a custom Access Point Name (APN) device policy for iOS, Android, and Windows Mobile/CE 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.

iOS settings

Android settings

Windows Mobile/CE settings

1. In the XenMobile console, click **Configure** > **Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More**, and then under **Network Access**, click **APN**. The **APN Policy** information page appears.

4. In the **Policy Information** pane, enter the following information:

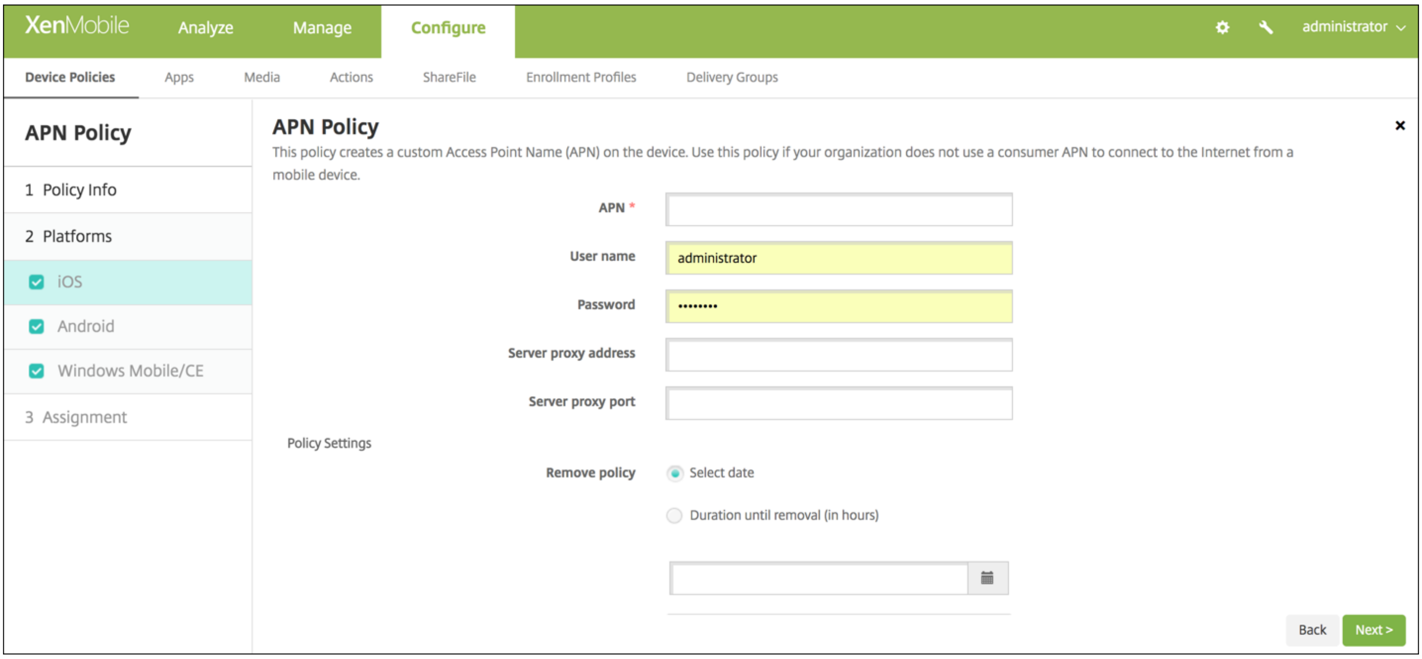
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

5. Click **Next**. The **Policy Platforms** page appears.

Note: When the **Policy Platforms** page appears, all platforms are selected and you see the iOS platform first.

6. Under **Platforms**, select the platforms you want to add.

When you finish configuring the settings for a platform, refer to Step 7 for how to set that platform's deployment rules.



APN Policy

This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN *

User name: administrator

Password: ••••••••

Server proxy address

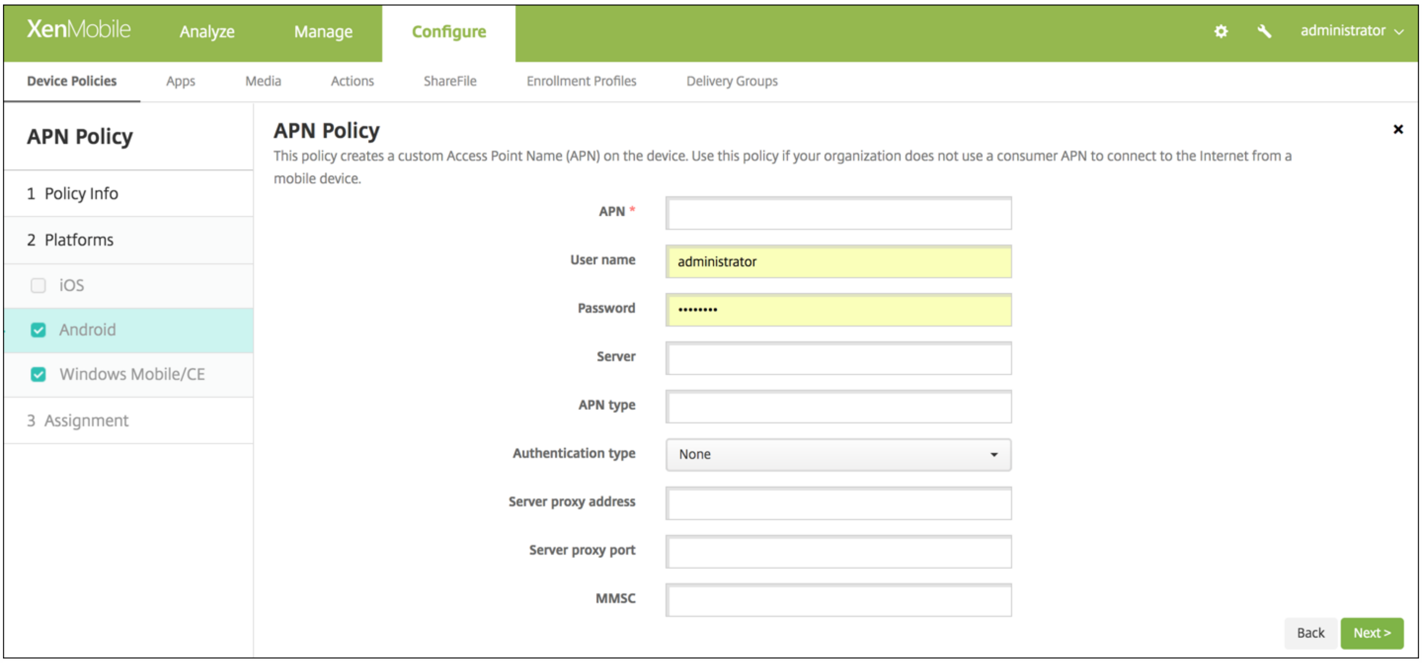
Server proxy port

Policy Settings

Remove policy: ● Select date ○ Duration until removal (in hours)

Configure these 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.
  - 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.



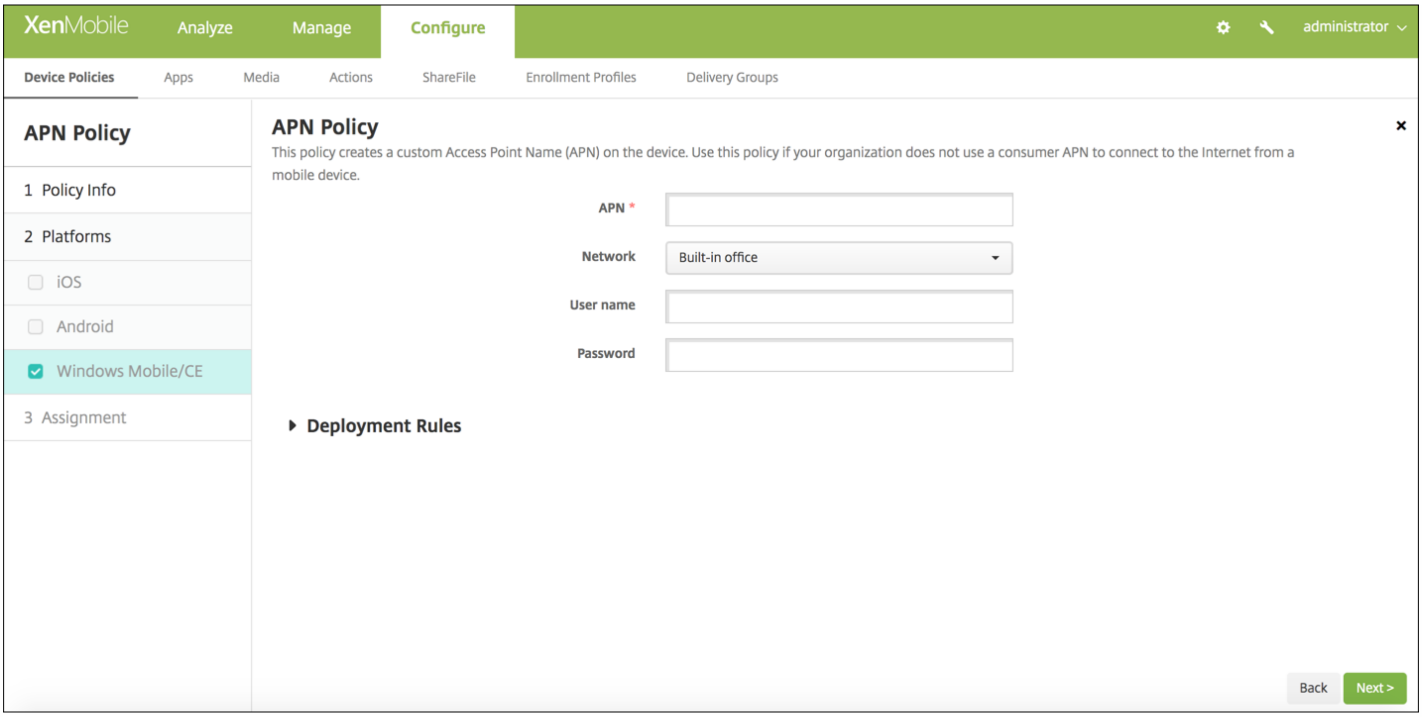
APN Policy

This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN *	
User name	administrator
Password	••••••••
Server	
APN type	
Authentication type	None
Server proxy address	
Server proxy port	
MMSC	

Configure these 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 standardweb 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.



APN Policy

This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN *	
Network	Built-in office
User name	
Password	

Configure the following settings:

- **APN**: Type the name of the access point. This must match an accepted Android APN or the policy will fail.
- **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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

App access device policy

Sep 06, 2017

The app access device policy in XenMobile 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 create app access policies for iOS, Android, and Windows Mobile/CE devices.

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, it is recommended that you name each policy carefully, so you know which policy in XenMobile applies to which list of apps.

1. In the XenMobile console, click **Configure > Device Policies**.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Expand **More**, and then under **Apps**, click **App Access**. The **App Access Policy** information page appears.

4. On the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy Platforms** page appears.

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, refer to Step 7 for how to set that platform's deployment rules.

6. Configure the following settings for each platform you select.

- **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.

    Note: To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing app, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

App attributes device policy

Sep 06, 2017

The App attributes device policy lets you specify attributes, such as a managed app bundle ID or per-app VPN identifier, for iOS devices.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

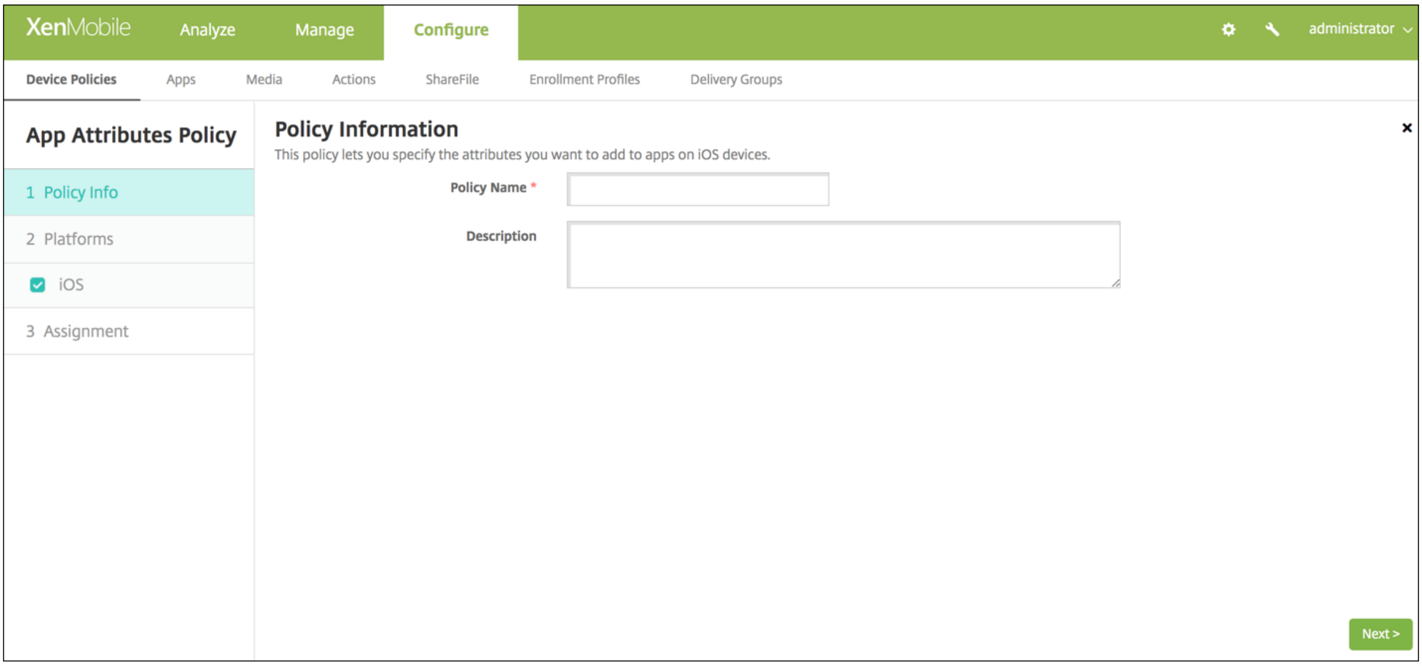
2. Click **Add**. The **Add a New Policy** page appears.

3. Expand **More**, and then under **Apps**, click **App Attributes**. The **App Attributes 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 **App Attributes** platform information page appears.



Policy Information

This policy lets you specify the attributes you want to add to apps on iOS devices.

Policy Name *

Description

6. Configure these 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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

App configuration device policy

Sep 06, 2017

You can remotely configure apps that support managed configuration by deploying an XML configuration file (called a property list, or plist) to users' iOS devices or key/value pairs for Windows 10 phone, tablet, or desktop devices. The configuration specifies various settings and behaviors in the app. XenMobile 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.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** page appears.

3. Expand **More**, and then under **Apps**, click **App Configuration**. The **App Configuration 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.

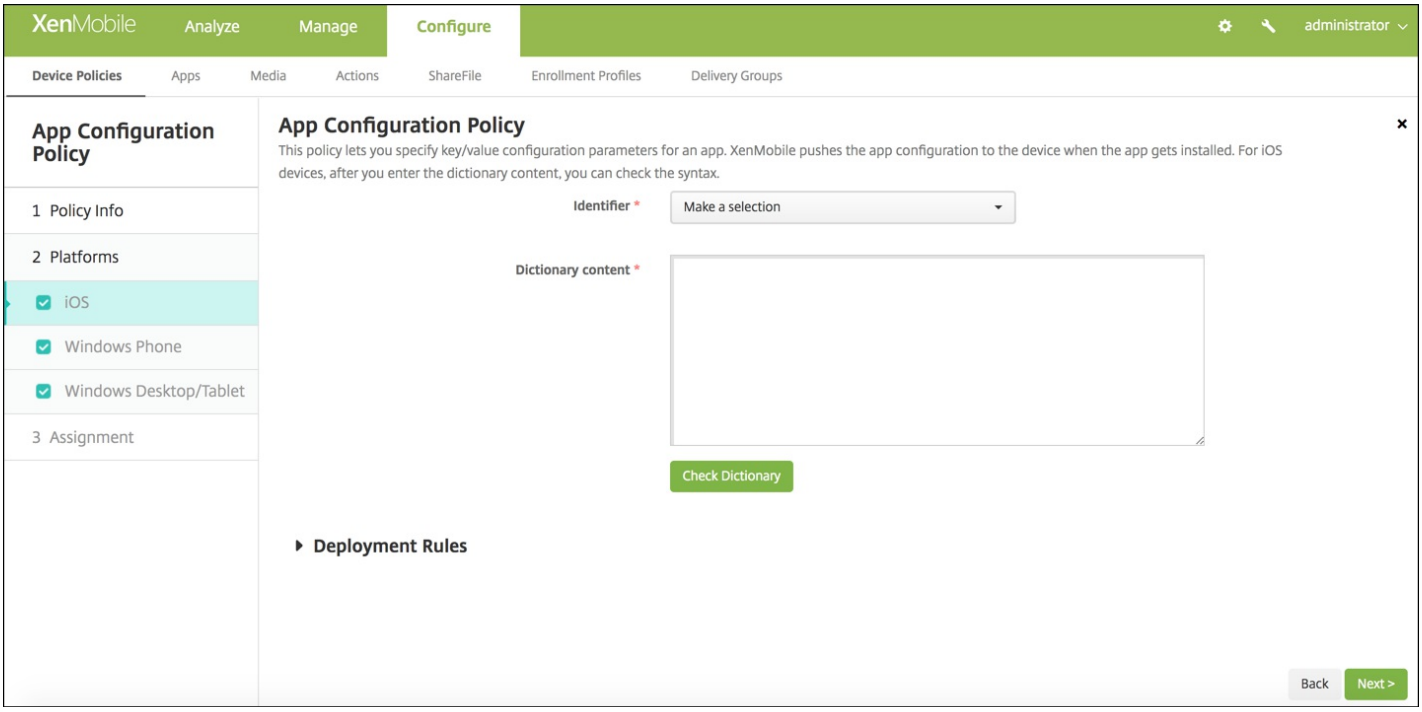
5. Click **Next**. The **Policy Platforms** page appears.

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, refer to Step 6 for how to set that platform's deployment rules.

Configure 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**. XenMobile 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.

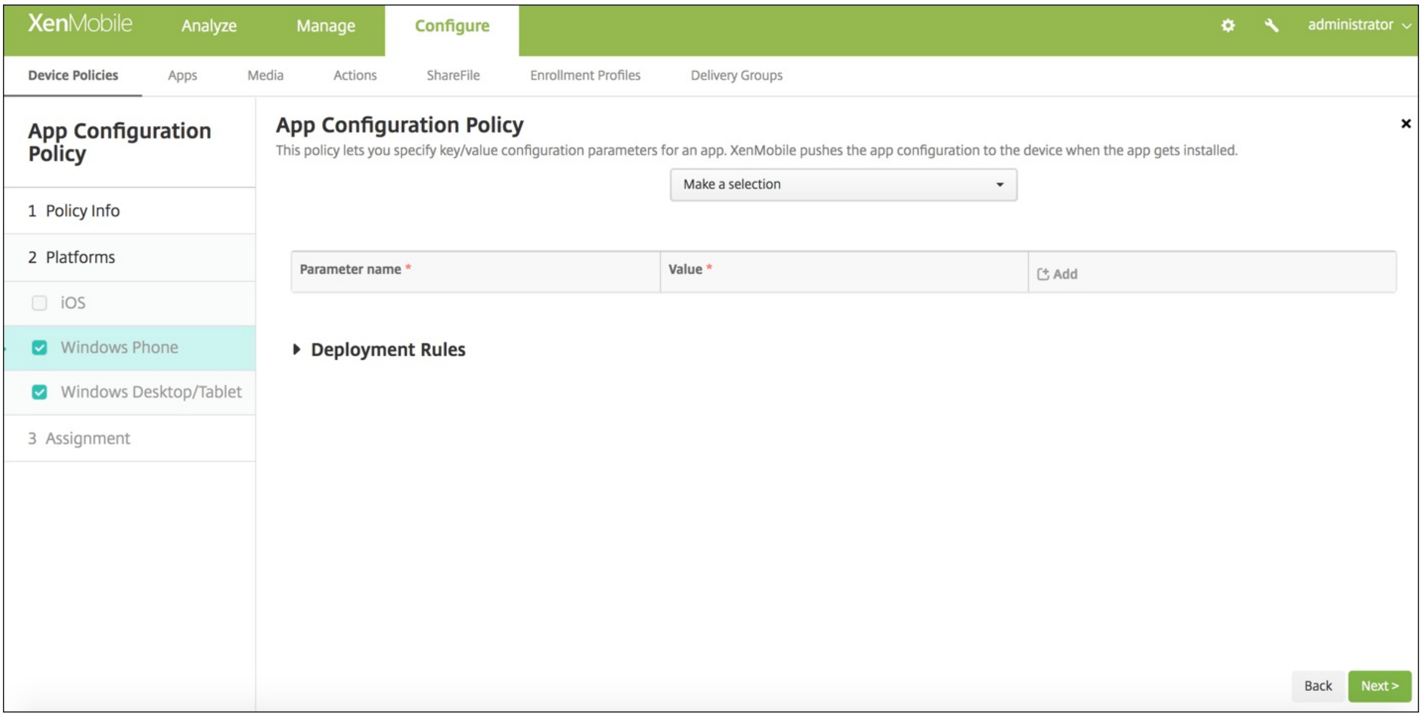


App Configuration Policy

This policy lets you specify key/value configuration parameters for an app. XenMobile pushes the app configuration to the device when the app gets installed. For iOS devices, after you enter the dictionary content, you can check the syntax.

Configure Windows Phone or Desktop/Tablet 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.



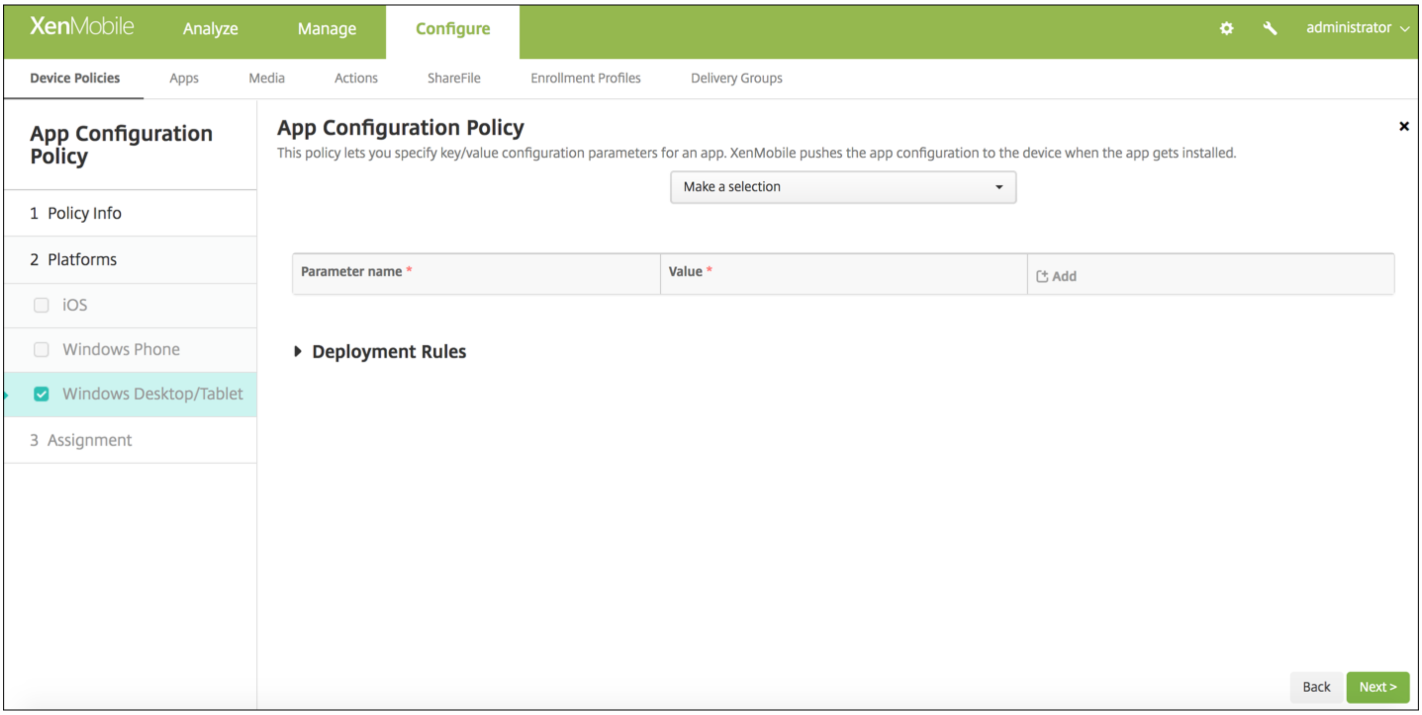
App Configuration Policy

This policy lets you specify key/value configuration parameters for an app. XenMobile pushes the app configuration to the device when the app gets installed.

Make a selection

Parameter name *	Value *

□ iOS
☑ Windows Phone
☑ Windows Desktop/Tablet



App Configuration Policy

This policy lets you specify key/value configuration parameters for an app. XenMobile pushes the app configuration to the device when the app gets installed.

Make a selection

Parameter name *	Value *

□ iOS
□ Windows Phone
☑ Windows Desktop/Tablet

6. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

App inventory device policy

Sep 06, 2017

An app inventory policy in XenMobile lets you collect an inventory of the apps on managed devices, and then the inventory is compared 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. You can create app access policies for iOS, macOS, Android (including for devices enabled for Android for Work), Windows desktop/tablet, Windows phone, or Windows Mobile/CE devices.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

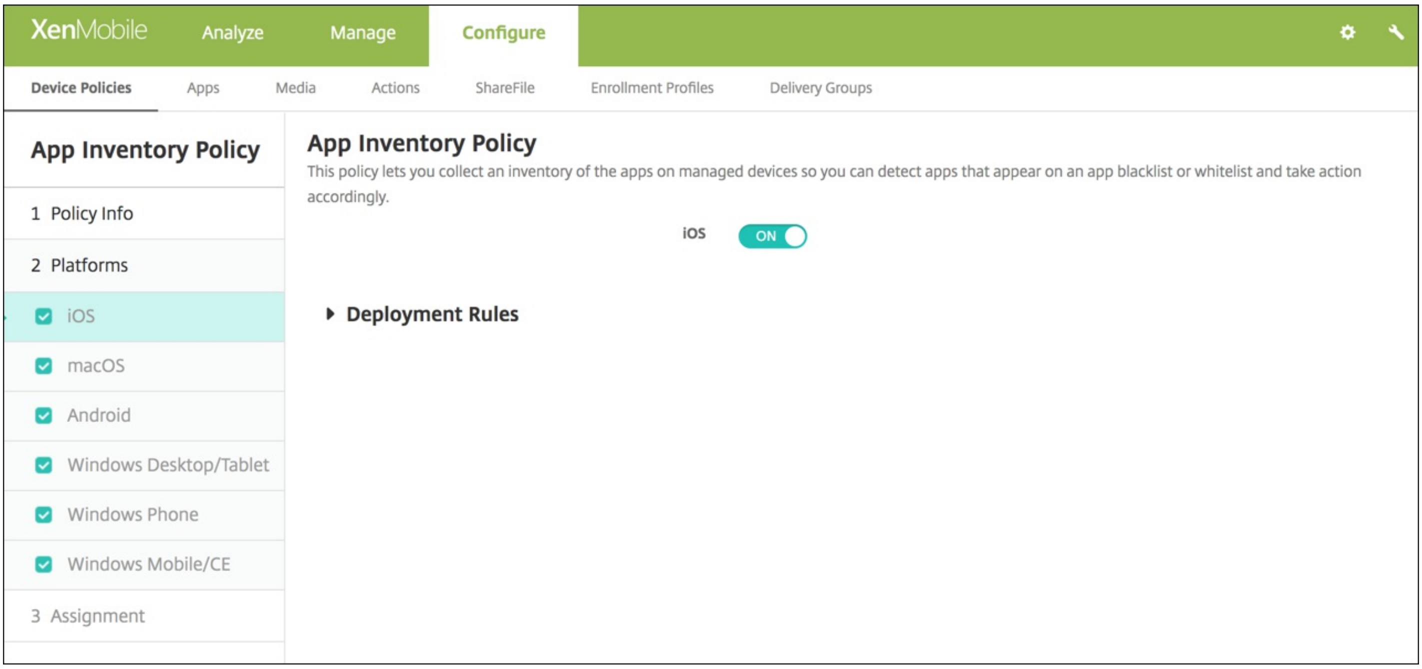
2. Click **Add**. The **Add a New Policy** page appears.

3. Expand **More**, and under **Apps**, click **App Inventory**. The **App Inventory Policy** page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy Platforms** page appears.



App Inventory Policy

This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.

iOS ON

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, refer to Step 7 for how to set that platform's deployment rules.

6. For each platform you select, leave the default setting or change the setting to **OFF**. The default is **ON**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

App lock device policy

Sep 06, 2017

You can create a policy in XenMobile to define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device. You can configure this policy for both iOS and Android devices, but the exact way the policy works differs for each 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 due to the deprecation of the required API by Google.

iOS settings

Android settings

1. In the XenMobile 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 **App Lock**. The **App Lock Policy** page appears.

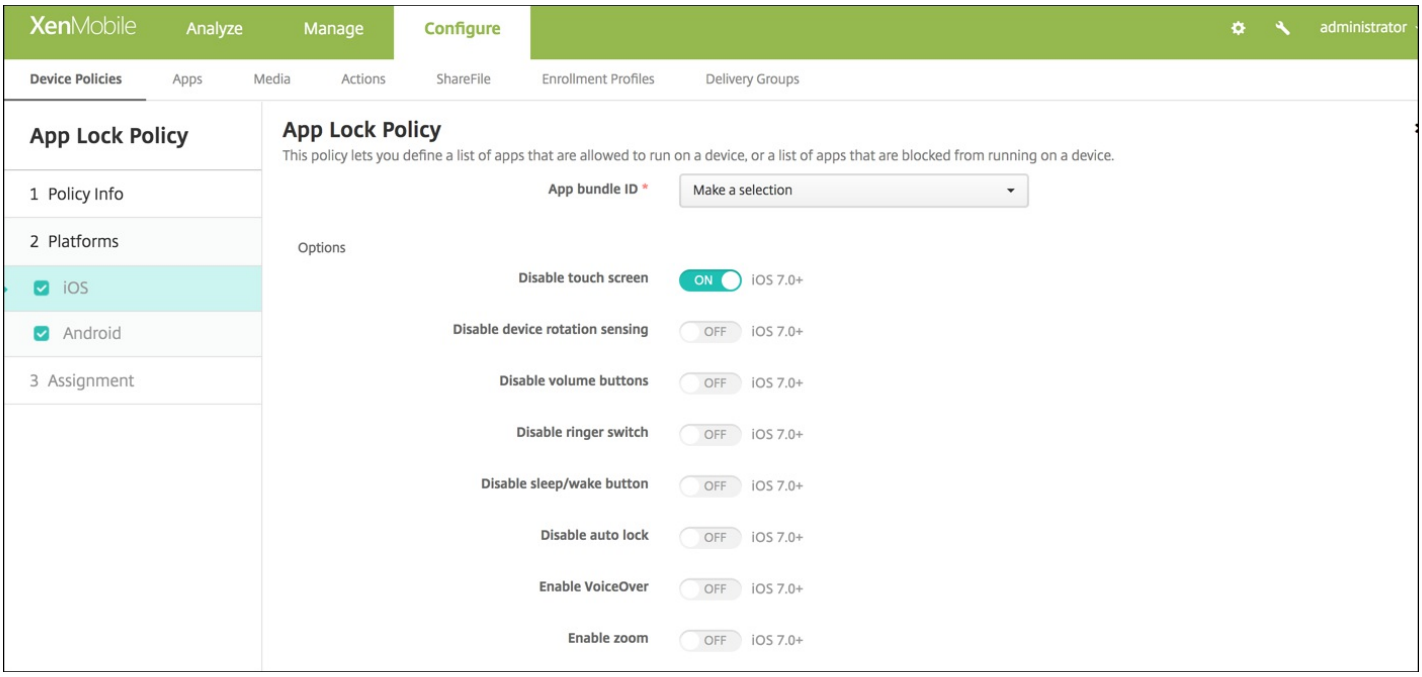
4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: If desired, type a description of the policy.

5. Click **Next**. The **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, refer to Step 7 for how to set that platform's deployment rules.



App Lock Policy

This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.

App bundle ID * Make a selection

Options

Disable touch screen ON iOS 7.0+

Disable device rotation sensing OFF iOS 7.0+

Disable volume buttons OFF iOS 7.0+

Disable ringer switch OFF iOS 7.0+

Disable sleep/wake button OFF iOS 7.0+

Disable auto lock OFF iOS 7.0+

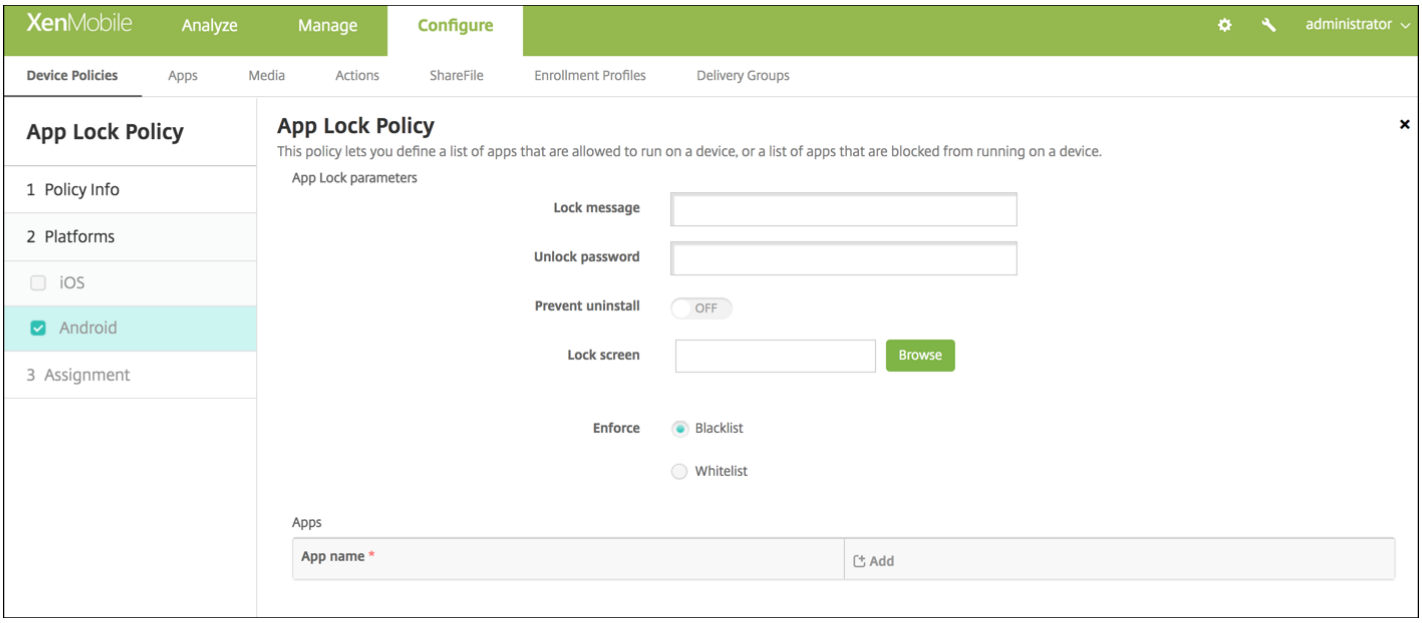
Enable VoiceOver OFF iOS 7.0+

Enable zoom OFF iOS 7.0+

Configure these 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**: Each of the following options applies only to iOS 7.0 or later. 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 - **Note**: When this option is disabled, 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**: Each of the following options applies only to iOS 7.0 or later. For each option, the default is **OFF**.
  - Allow VoiceOver adjustment
  - Allow zoom adjustment
  - Allow invert colors adjustment
  - Allow AssitiveTouch adjustment
- **Policy Settings**
  - o Next to **Remove policy**, click either **Select date** or **Duration until removal (in hours)**.
  - o If you click **Select date**, click the calendar to select the specific date for removal.
  - o In the **Allow user to remove policy** list, click **Always**, **Password required**, or **Never**.

- o If you click **Password required**, next to **Removal password**, type the necessary password.



App Lock Policy

This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.

App Lock parameters

Lock message

Unlock password

Prevent uninstall: OFF

Lock screen

Enforce: ● Blacklist ○ Whitelist

Apps

App name *	Add

Configure these settings:

- **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.

    Note: To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing app, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

App network usage device policy

Sep 06, 2017

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 XenMobile. They do not include apps that users have downloaded directly to their devices without being deployed through XenMobile or those already installed on the devices when the devices were enrolled in XenMobile.

1. In the XenMobile console, click **Configure > Device Policies**.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Expand **More**, and then under **Apps**, click **App Network Usage**. The **App Network Usage Policy** information page appears.

4. On the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy Platforms** page appears.

6. Configure these 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.

    Note: To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing app, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

App restrictions device policy

Sep 06, 2017

You can create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

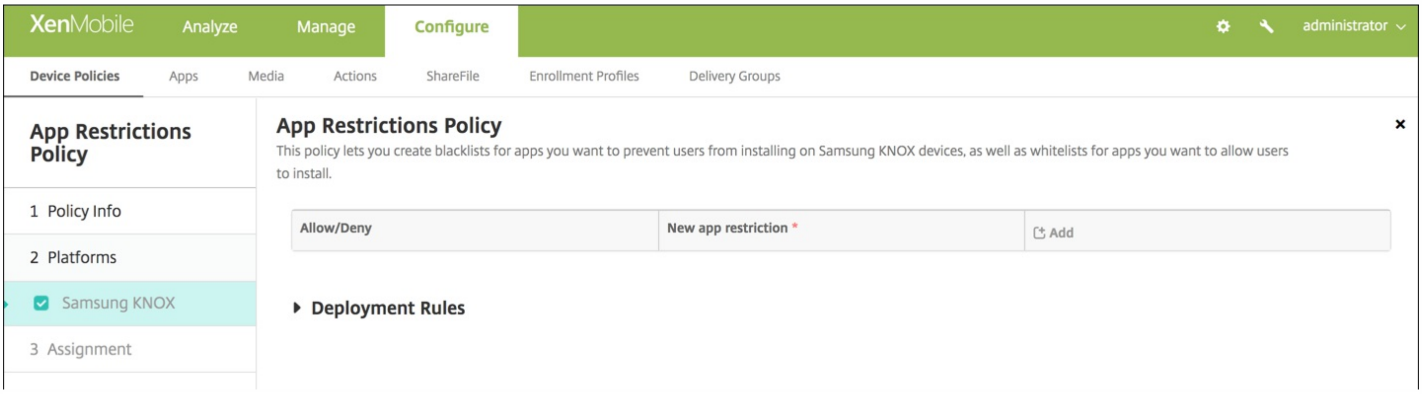
2. Click **Add**. The **Add New Policy** dialog box appears.

3. Expand **More** and then, under **Security**, click **App Restrictions**. The **App Restrictions Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Samsung KNOX Platform** page appears.



This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.

6. 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.

> **Note**: To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.
>
> To edit an existing app, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

App tunneling device policy

Nov 29, 2017

> ## Note
>
> The App tunneling policy is used only for Remote Support. For information about Remote Support, see Support options and Remote Support.

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 also use app tunnels to create remote support tunnels to a device for management support. You can configure the app tunneling policy for Android and Windows Mobile/CE devices.

Note: Any app traffic sent through a tunnel that you define in this policy goes through XenMobile before being redirected to the server running the app.

Android settings

Windows Mobile/CE settings

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More** and then, under **Network access**, click **Tunnel**. The **Tunnel Policy** page appears.

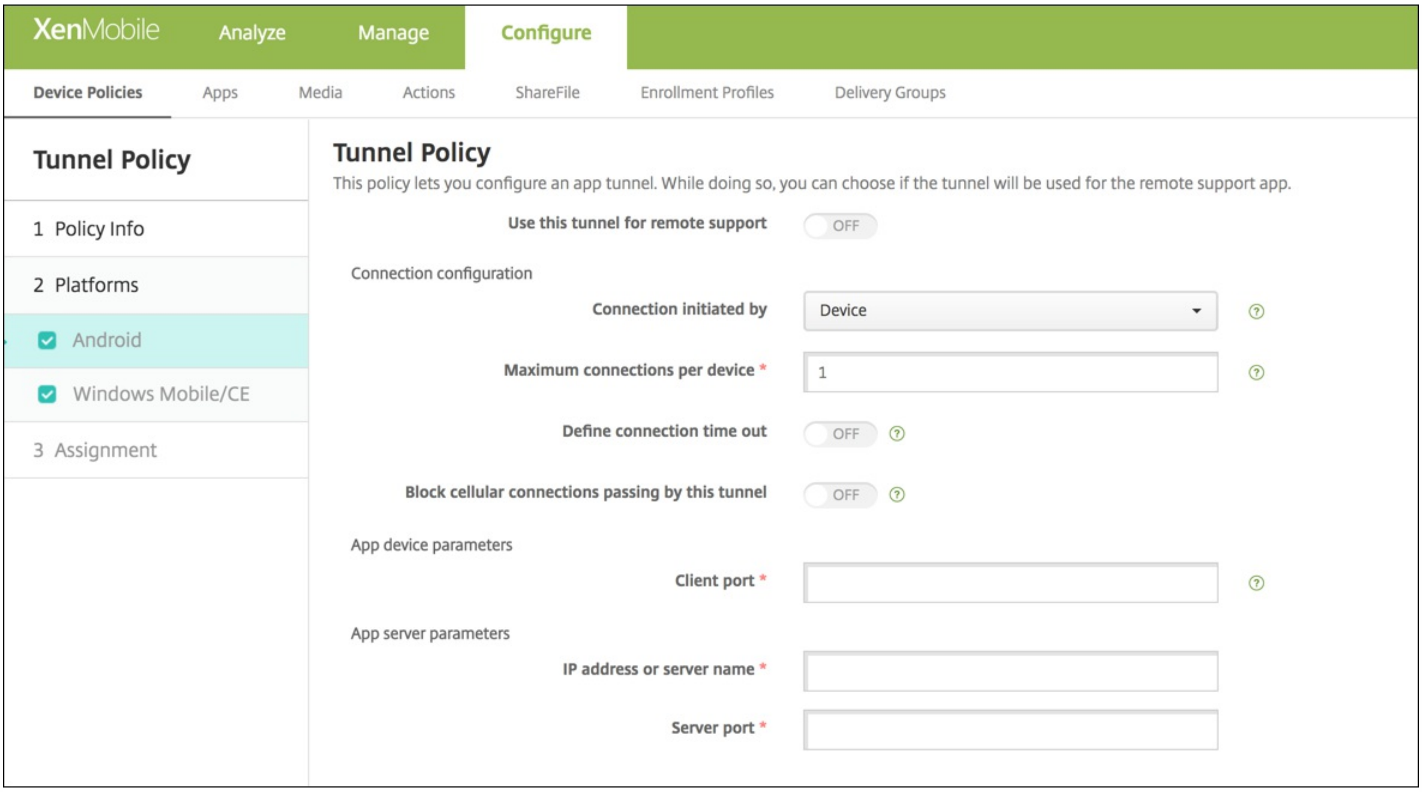
4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.



Tunnel Policy

This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.

Use this tunnel for remote support: OFF

Connection configuration

Connection initiated by: Device

Maximum connections per device *: 1

Define connection time out: OFF

Block cellular connections passing by this tunnel: OFF

App device parameters

Client port *

App server parameters

IP address or server name *

Server port *

Configure these settings:

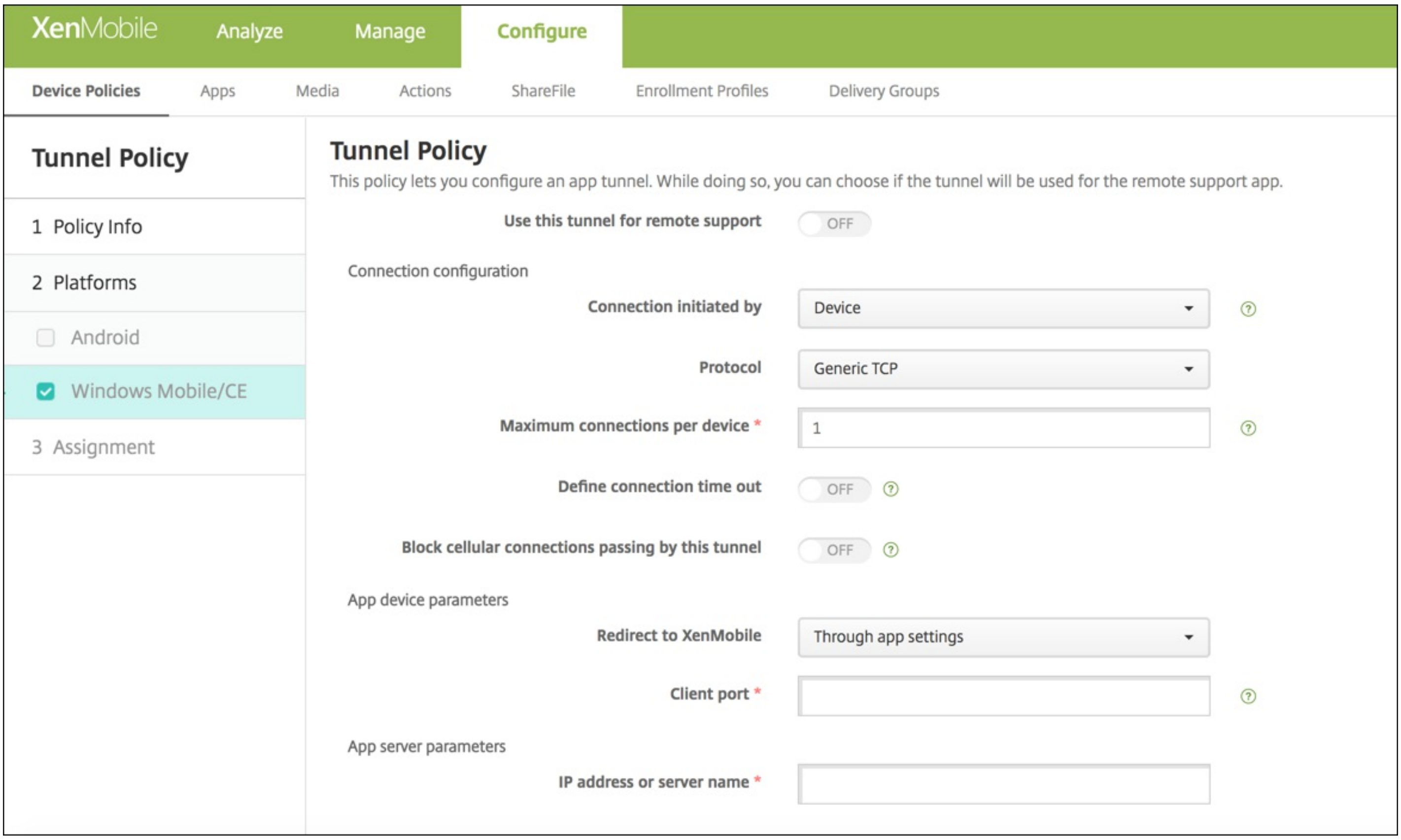
- **Use this tunnel for remote support:** Select whether the tunnel will be used for remote support.

  Note: The configuration steps are different depending on whether you select remote support.

- If you do not select remote support, do the following:
  - **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. **Note**: WiFi and USB connections will not be 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.
- If you do select remote support, do the following:
  - **Use this tunnel for remote support**: Set to **On**.
  - **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.
  - **Use SSL connection**: Select whether to use a secure SSL connection for this tunnel.

- **Block cellular connections passing by this tunnel**: Select whether this tunnel is blocked while roaming.
  Note: WiFi and USB connections will not be blocked.



Tunnel Policy

This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.

Use this tunnel for remote support: OFF

Connection configuration

Connection initiated by: Device

Protocol: Generic TCP

Maximum connections per device *: 1

Define connection time out: OFF

Block cellular connections passing by this tunnel: OFF

App device parameters

Redirect to XenMobile: Through app settings

Client port *:

App server parameters

IP address or server name *:

Configure these settings:

- **Use this tunnel for remote support**: Select whether the tunnel will be used for remote support.

  Note: The configuration steps are different depending on whether you select remote support.

- If you do not select remote support, do the following:
  - **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**: 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.
    Note: WiFi and USB connections will not be blocked.

  - **Redirect to XenMobile**: In the list, click how the device connects to XenMobile. 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** and type the to IP address in **IP address** range to.

  - **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.
- If you do select remote support, do the following:
  - **Use this tunnel for remote support**: Set to **On**.
  - **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.
  - **Use SSL connection**: Select whether to use a secure SSL connection for this tunnel.
  - **Block cellular connections passing by this tunnel**: Select whether this tunnel is blocked while roaming.
    Note: WiFi and USB connections will not be blocked.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

App uninstall device policy

Sep 06, 2017

You can create an app uninstall policy for iOS, Android, Samsung KNOX, Android for Work, Windows desktop/tablet, and Windows Mobile/CE platforms. An app uninstall policy lets you remove apps from users' 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 your users' 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.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

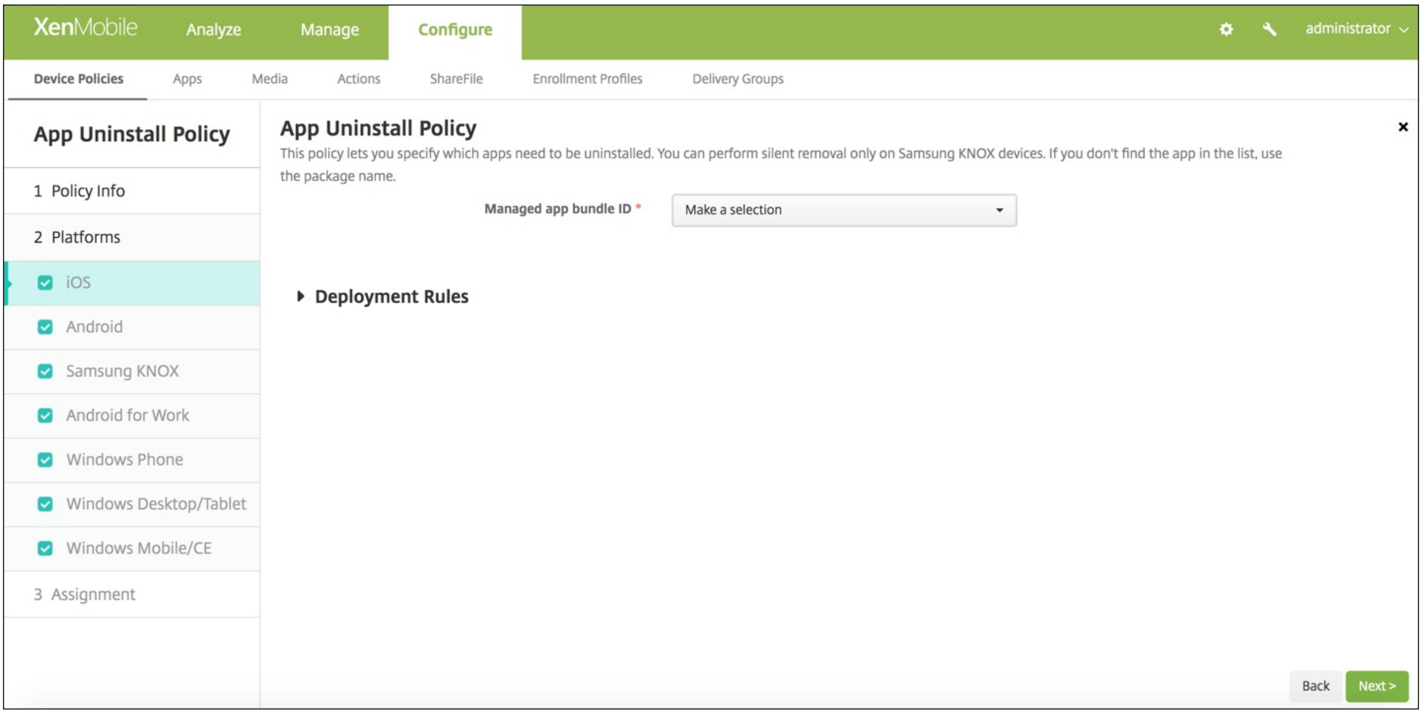
3. Expand **More** and then, under **Apps**, click **App Uninstall**. The **App Uninstall Policy** page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy Platforms** page appears.

6. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.



App Uninstall Policy

This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.

Managed app bundle ID * Make a selection

When you finish configuring the settings for a platform, refer to Step 7 for how to set that platform's deployment rules.

Configure this setting:

- **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.

Configure this setting:

- **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 will be empty and you must add new apps.
  - Click **Add** to add the app or click **Cancel** to cancel adding the app.

    Note: To delete an existing app from the uninstall policy, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing app, hover over the line containing the listing and click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

You can configure XenMobile 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 XenMobile to remove older apps from user devices upon installation of the new version. This feature is available only for managed iOS devices connected to a XenMobile 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, XenMobile removes the Enterprise version (com.citrix.mail).

App uninstall restrictions device policy

Sep 06, 2017

You can specify the apps users can or cannot uninstall on a Samsung SAFE or Amazon device.

1. In the XenMobile console, click **Configure > Device Policies**.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Expand **More**, and then under **Apps**, click **App Uninstall Restrictions**. The **App Uninstall Restrictions Policy** information page appears.

4. On the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.

7. Configure these settings for each platform you selected:

- **App Uninstall Restrictions Settings**: For each app rule you want to adds, click **Add** and then do the following:
  - **App Name**: 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**.

  Note: To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

  To edit an existing app, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

8. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

BitLocker device policy

Sep 06, 2017

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 XenMobile to configure the settings available in the BitLocker wizard on Windows 10 devices. For example, on a device with BitLocker enabled, BitLocker can prompt users for how they want to unlock their drive at startup, how to back up their recovery key, and 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.

Requirements

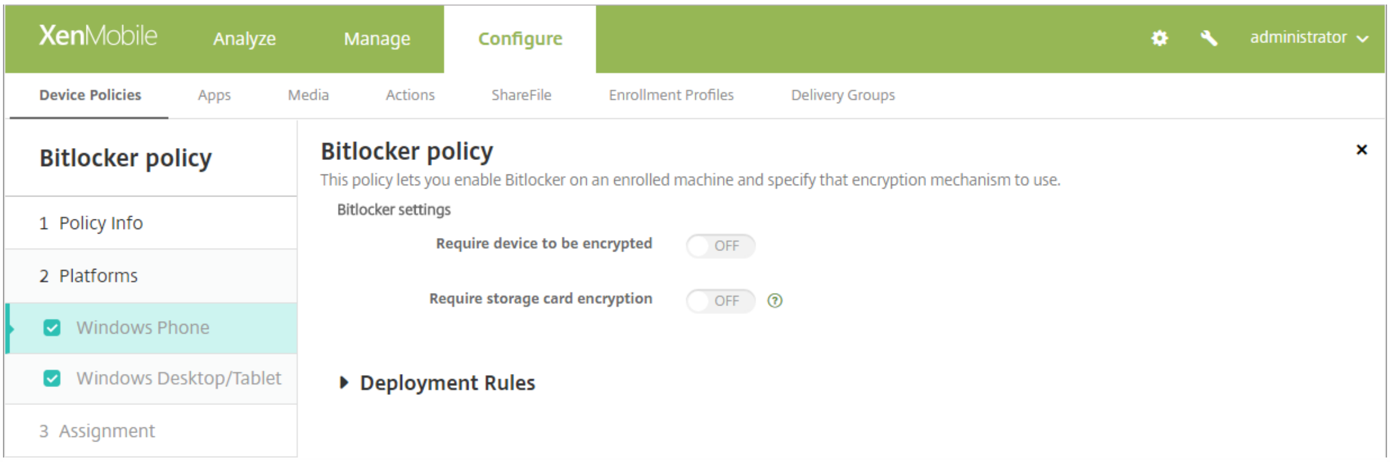
Before deploying the BitLocker device policy, prepare your environment for BitLocker use. For detailed information from Microsoft, including BitLocker system requirements and setup, see BitLocker and the articles under that node.

Configure Windows 10 settings

After BitLocker encryption starts on a device, you can't subsequently change the BitLocker settings on the device by deploying an updated policy.

1. Click **Configure > Device Policies**. The **Device Policies** page appears.
2. Click **Add**. The **Add a New Policy** dialog box appears.
3. Start typing **BitLocker** and then click that name in the search results. The BitLocker **Policy information** page appears.
4. In the **Policy information** page, enter the following information:
   - **Policy Name**: Type a descriptive name for the policy.
   - **Description**: Optionally, type a description of the policy.
5. Click **Next** and then configure the settings for each platform that you choose.

   ### Windows Phone settings



Bitlocker policy

This policy lets you enable Bitlocker on an enrolled machine and specify that encryption mechanism to use.

Bitlocker settings

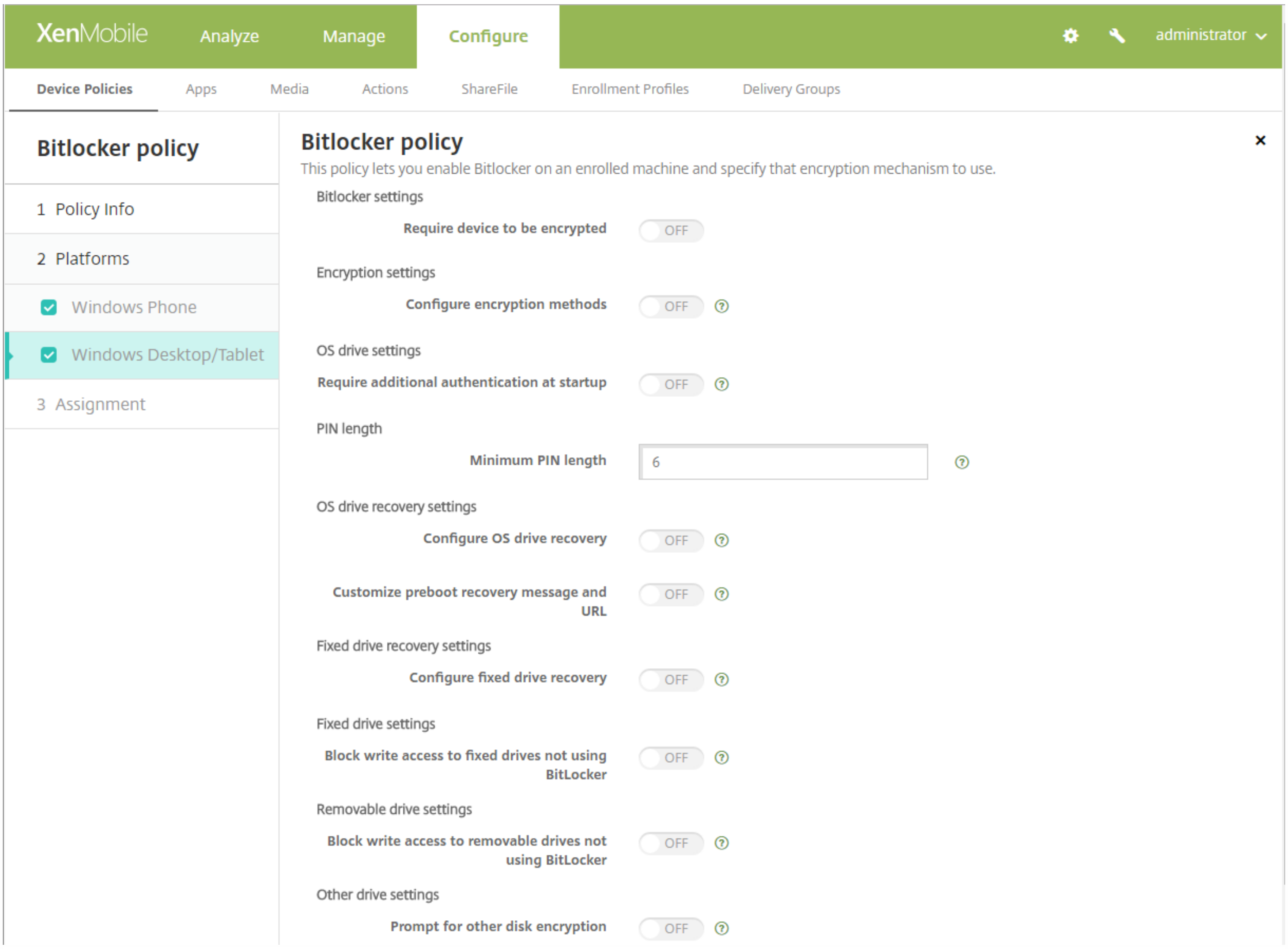
Require device to be encrypted: OFF

Require storage card encryption: OFF

Deployment Rules

- **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 that encryption mechanism to use.

Bitlocker settings

Require device to be encrypted: OFF

Encryption settings

Configure encryption methods: OFF

OS drive settings

Require additional authentication at startup: OFF

PIN length

Minimum PIN length: 6

OS drive recovery settings

Configure OS drive recovery: OFF

Customize preboot recovery message and URL: OFF

Fixed drive recovery settings

Configure fixed drive recovery: OFF

Fixed drive settings

Block write access to fixed drives not using BitLocker: OFF

Removable drive settings

Block write access to removable drives not using BitLocker: OFF

Other drive settings

Prompt for other disk encryption: OFF

- **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**.

- **Configure encryption methods**: Determines the encryption methods to use for specific drive types. If **Off**, the BitLocker wizard prompts the 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**.

- **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 TPM chip**: On a device with no TPM chip, BitLocker requires users to create a 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 additional 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. If the unlock fails, the device enters recovery mode.

- **Minimum PIN length**: The minimum length of the TPM startup PIN. Defaults to **6**.
- **Configure 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 Basic Deployment. Default is **Off**.
  - **Create 48-digit recovery password for OS drive recovery**: 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-digit password**.
  - **Create 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 AD DS**: Specifies whether to save the recovery options to Active Directory Domain Services. Default is **Off**.
  - **Configure recovery info stored in AD DS**: 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 AD DS**: 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**.
- **Customize 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**, and **Use custom recovery URL**. If **Off**, the default recovery message and URL display. Default is **Off**.

- **Configure fixed drive recovery**: Configures the recovery options to 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**.

- **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**.

- **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**.

- **Prompt for other disk encryption**: Allows you to disable the warning prompt for other disk encryption on devices. Defaults to **Off**.

6. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

> ## Note
>
> After BitLocker encryption starts on a device, you can't subsequently change the BitLocker settings on the device by deploying an updated BitLocker device policy.

Browser device policy

Sep 06, 2017

You can create browser device polices for Samsung SAFE or Samsung KNOX devices to define whether users' 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.

Samsung SAFE and Samsung KNOX settings

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add** to add a new policy. The **Add a New Policy** dialog box appears.

3. Click **More**, and then under **Apps**, click **Browser**. The **Browser Policy** information page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.

Configure these 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.

8. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Calendar (CalDav) device policy

Sep 06, 2017

You can add a device policy in XenMobile 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.

1. In the XenMobile 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 **End user**, click **Calendar (CalDAV)**. The **Calendar (CalDAV) Policy** 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 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, refer to Step 7 for how to set that platform's deployment rules.

Configure the following settings:

- **Account description**: Type an account description. This field is required.
- **Host name**: Type the address of the CalDAV server. This field is required.
- **Port**: Type the port on which to connect to the CalDAV server. This field is required. The default is **8443**.
- **Principal URL**: Type the base URL to the user's calendar.
- **User name**: Type the user's logon name. This field is required.
- **Password**: Type an optional user password.
- **Use SSL**: Select whether to use a Secure Socket Layer connection to the CalDAV server. The default is **ON**.
- Policy Settings
  - 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.

Configure the following settings:

- **Account description**: Type an account description. This field is required.
- **Host name**: Type the address of the CalDAV server. This field is required.
- **Port**: Type the port on which to connect to the CalDAV server. This field is required. The default is **8443**.
- **Principal URL**: Type the base URL to the user's calendar.
- **User name**: Type the user's logon name. This field is required.
- **Password**: Type an optional user password.

- **Use SSL**: Select whether to use a Secure Socket Layer connection to the CalDAV server. The default is **ON**.
- **Policy Settings**
  - 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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Cellular device policy

Sep 06, 2017

This policy allows you to configure cellular network settings on an iOS device.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** page appears.

3. Expand **More**, and then, under **Network Access**, click **Cellular**. The **Cellular Network 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 **iOS Platform** information page appears.

6. Configure these settings:

- Attach APN
  - **Name**: Type 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**: Type a user name used for authentication.
- APN
  - **Name**: Type a name for the Access Point Name (APN) configuration.
  - **Authentication type**: In the list, click **CHAP** or **PAP**. The default is **PAP**.
  - **User name**: Type a user name used for authentication.
  - **Password**: Type a password used for authentication.
  - **Proxy server**: Type the proxy server network address.
- 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.

8. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Connection manager device policy

Sep 06, 2017

In XenMobile, 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.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More**, and then, under **Network Access**, click **Connection manager**. The **Connection Manager** policy information page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Windows Mobile/CE Platform** page appears.

6. Configure these settings.

Note: **Built-in office** means all connections are to your company's intranet and **Built-in Internet** means 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**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Connection scheduling device policy

Sep 06, 2017

You create connection scheduling policies to control how and when users' devices connect to XenMobile. Note that you can configure this policy for devices enabled for Android for Work as well.

You can specify that users connect their devices manually, that devices stay connected permanently, or that devices connect within a defined time frame.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **Scheduling**. The **Connection Scheduling Policy** information page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 8 for how to set that platform's deployment rules.

7. Configure the following settings for each of the platforms you selected:

- **Require devices to connect**: Click the option you want to set for this schedule.
  - **Always**: Keep the connection alive permanently. XenMobile on the user's device attempts to reconnect to the XenMobile server after a network connection loss and will monitor 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 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. You must 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 XenMobile on their devices. Citrix doesn't recommend this option for production deployments because it prevents you from deploying security policies to devices, thus users will never 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, XenMobile 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 is **20**.
  - **Define schedule**: When enabled, XenMobile on the user's device attempts to reconnect to the XenMobile server after a network connection loss and monitors the connection by transmitting control packets at regular intervals within the time frame you define. See Defining a connection time frame 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

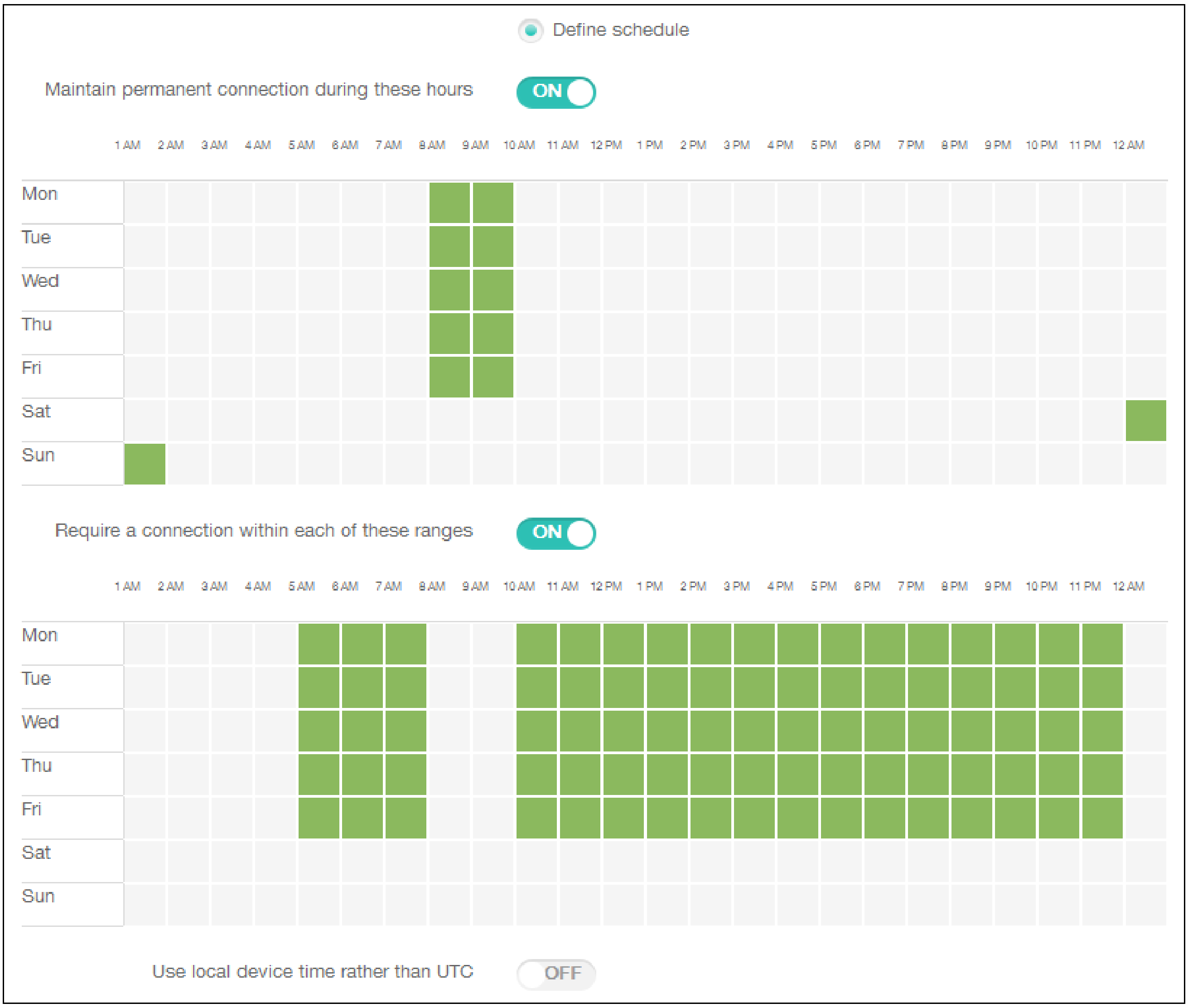
defined time frames.

- **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, so if you want a connection between 8:00 AM and 9:00 AM every weekday, you 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, and at least one connection every weekday between 5:00 AM and 8:00 AM or between 10:00 AM and 11:00 PM.



● Define schedule

Maintain permanent connection during these hours ON

	1 AM	2 AM	3 AM	4 AM	5 AM	6 AM	7 AM	8 AM	9 AM	10 AM	11 AM	12 PM	1 PM	2 PM	3 PM	4 PM	5 PM	6 PM	7 PM	8 PM	9 PM	10 PM	11 PM	12 AM
Mon								🟩	🟩															
Tue								🟩	🟩															
Wed								🟩	🟩															
Thu								🟩	🟩															
Fri								🟩	🟩															
Sat																								🟩
Sun	🟩																							

Require a connection within each of these ranges ON

	1 AM	2 AM	3 AM	4 AM	5 AM	6 AM	7 AM	8 AM	9 AM	10 AM	11 AM	12 PM	1 PM	2 PM	3 PM	4 PM	5 PM	6 PM	7 PM	8 PM	9 PM	10 PM	11 PM	12 AM
Mon					🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Tue					🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Wed					🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Thu					🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Fri					🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Sat																								
Sun																								

Use local device time rather than UTC OFF

8. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Contacts (CardDAV) device policy

Sep 06, 2017

You can add a device policy in XenMobile 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.

1. In the XenMobile 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 **Contacts CardDAV**. The **CardDAV Policy** page appears.

4. In the **Policy Information** pane, type 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 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, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS settings

Configure these settings:

- **Account description**: Type an account description. This field is required.
- **Host name**: Type the address of the CardDAV server. This field is required.
- **Port**: Type the port on which to connect to the CardDAV server. This field is required. The default is **8443**.
- **Principal URL**: Type the base URL to the user's calendar.
- **User name**: Type the user's logon name. This field is required.
- **Password**: Type an optional user password.
- **Use SSL**: Select whether to use a Secure Socket Layer connection to the CardDAV server. The default is **ON**.
- **Policy Settings**
  - 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.

Configure macOS settings

Configure these settings:

- **Account description**: Type an account description. This field is required.
- **Host name**: Type the address of the CardDAV server. This field is required.
- **Port**: Type the port on which to connect to the CardDAV server. This field is required. The default is **8443**.
- **Principal URL**: Type the base URL to the user's calendar.
- **User name**: Type the user's logon name. This field is required.
- **Password**: Type an optional user password.

- **Use SSL**: Select whether to use a Secure Socket Layer connection to the CardDAV server. The default is **ON**.
- **Policy Settings**
  - 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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Control OS Updates device policy

Oct 13, 2017

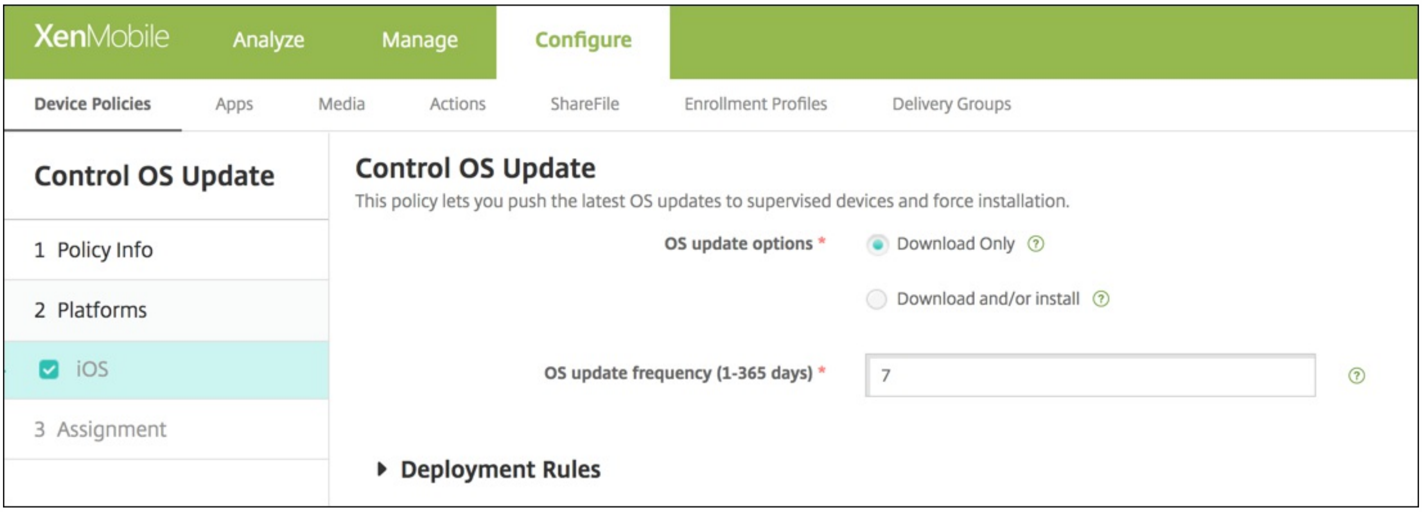
The Control OS Update device policy lets you deploy the latest OS updates to supervised iOS and Samsung SAFE devices.

iOS options

Note: For devices running iOS 10.3 and later, Control OS Updates works on supervised devices. For devices running a version prior to iOS 10.3, Control OS Updates works on devices that are both supervised and DEP-enrolled.

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 XenMobile checks and updates the device OS. The default is **7** days.



Control OS Update

This policy lets you push the latest OS updates to supervised devices and force installation.

OS update options * ● Download Only ○ Download and/or install

OS update frequency (1-365 days) * 7

Note

For general information about configuring policies, see Add a device policy.

Copy Apps to Samsung Container device policy

Sep 06, 2017

You can specify apps that are already installed on a device be copied to a SEAMS container or to a KNOX container on supported Samsung devices (for information about supported devices, see Samsung's Samsung KNOX Supported Devices page). 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.

Prerequisites:

- Device must be enrolled on XenMobile.
- The Samsung MDM keys (ELM and KLM) must be deployed (for how to do this, see Samsung MDM License Key device policies).
- Apps are already installed on device
- Initialize KNOX on the device to copy apps to the KNOX container.

1. In the XenMobile console, click **Configure > Device Policies**.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Expand **More**, and then under **Security**, click **Copy Apps to Samsung Container**. The **Copy Apps to Samsung Container Policy** information page appears.

4. On the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 8 for how to set that platform's deployment rules.

7. Configure the following setting for each platform you select.

- **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 fo the LacingArt app.
  - Click **Save** or **Cancel**.

    Note: To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing app, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

8. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Credentials device policy

Sep 06, 2017

You can create credentials device policies in XenMobile to enable integrated authentication with your PKI configuration in XenMobile, such as a PKI entity, a keystore, a credential provider, or a server certificate. For more information about credentials, see Certificates.

You can create credential policies for iOS, macOS, Android, Android for Work, Windows desktop/tablet, Windows Mobile/CE, and Windows Phone devices. Each platform requires a different set of values, which are described in this article.

iOS settings

macOS settings

Android and Android for Work settings

Windows desktop/tablet settings

Windows Mobile/CE settings

Windows Phone settings

Before you can create this policy, you need the credential information you plan to use for each platform, plus any certificates and passwords.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add New Policy** dialog box appears.

3. Expand **More** and then, under **Security**, click **Credentials**. The **Credentials Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

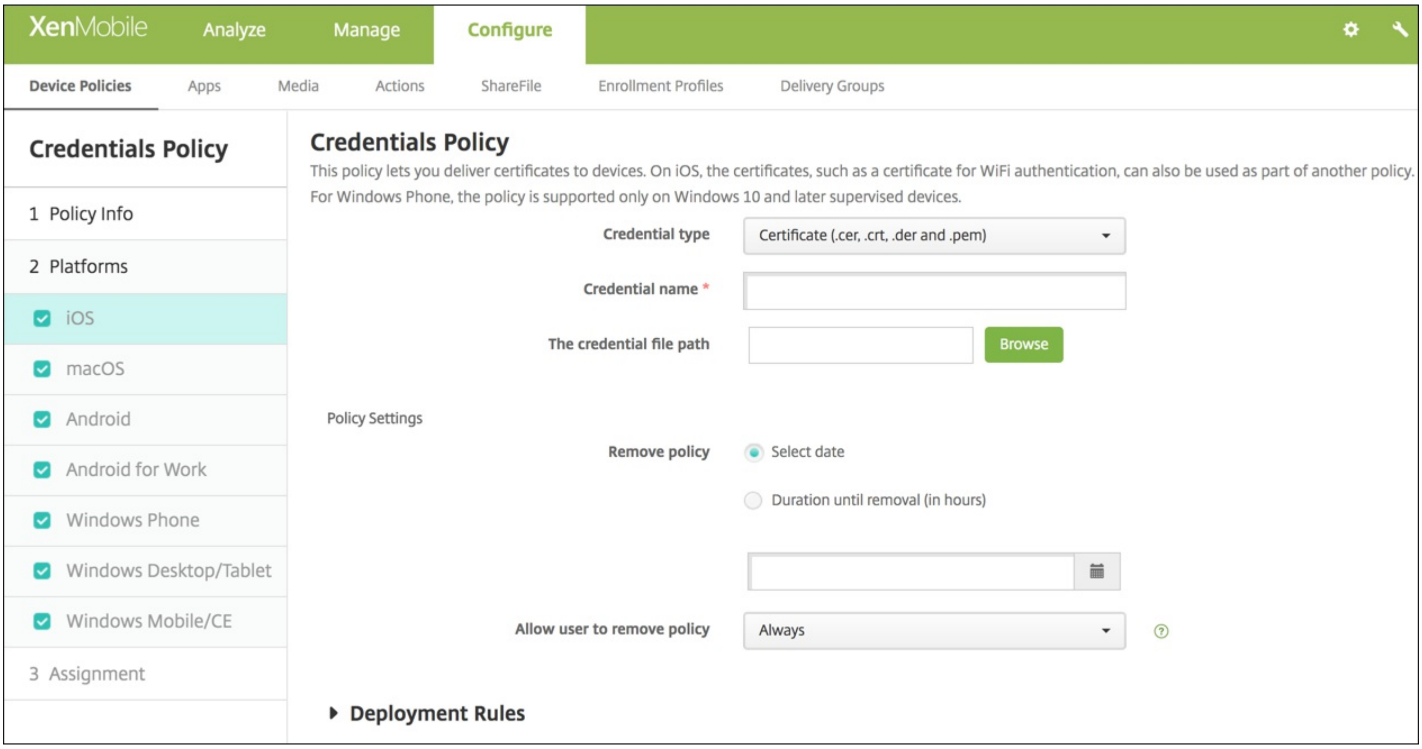
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS settings



Credentials Policy

1 Policy Info

2 Platforms

☑ iOS

☑ macOS

☑ Android

☑ Android for Work

☑ Windows Phone

☑ Windows Desktop/Tablet

☑ Windows Mobile/CE

3 Assignment

Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Credential type: Certificate (.cer, .crt, .der and .pem)

Credential name *

The credential file path [Browse]

Policy Settings

Remove policy: ● Select date ○ Duration until removal (in hours)

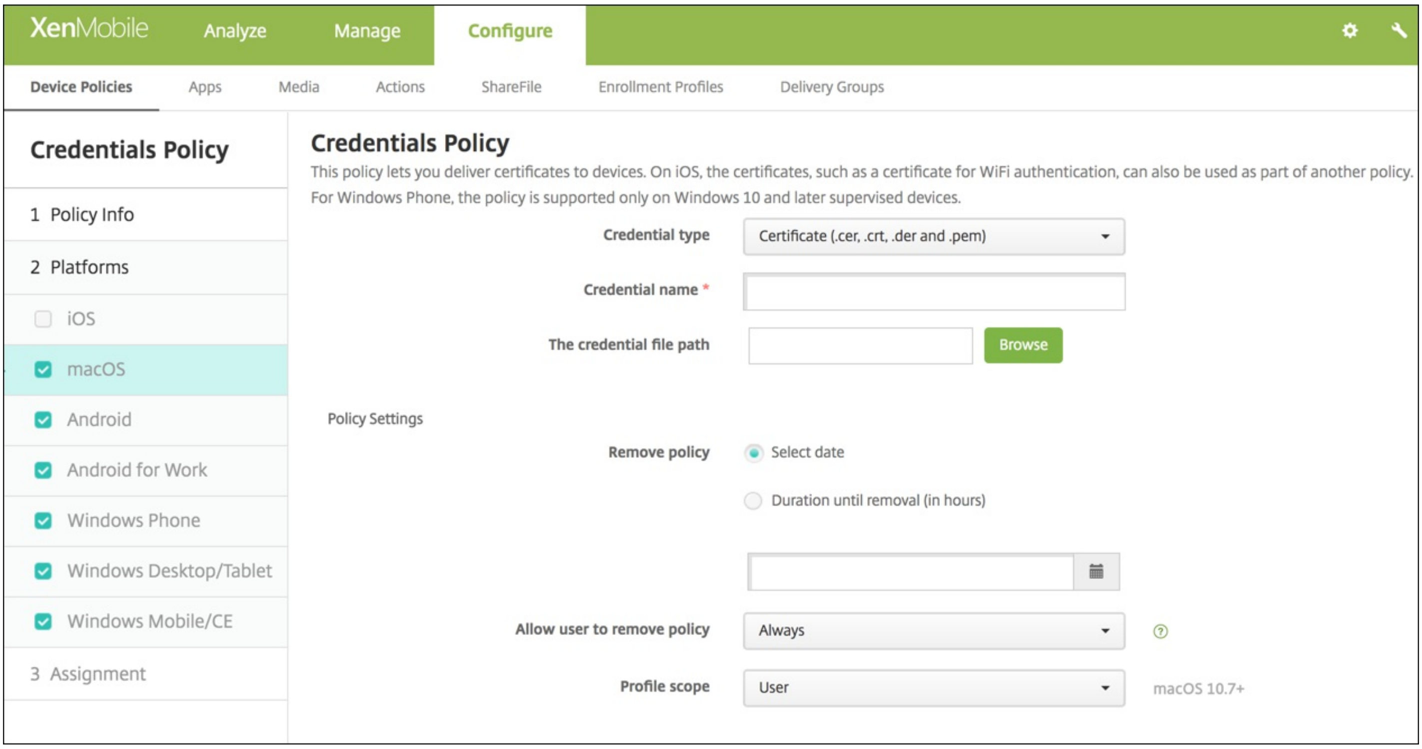
Allow user to remove policy: Always

Deployment Rules

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.
- **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.

Configure macOS settings



Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Credential type: Certificate (.cer, .crt, .der and .pem)

Credential name *

The credential file path

Policy Settings

Remove policy: ● Select date ○ Duration until removal (in hours)

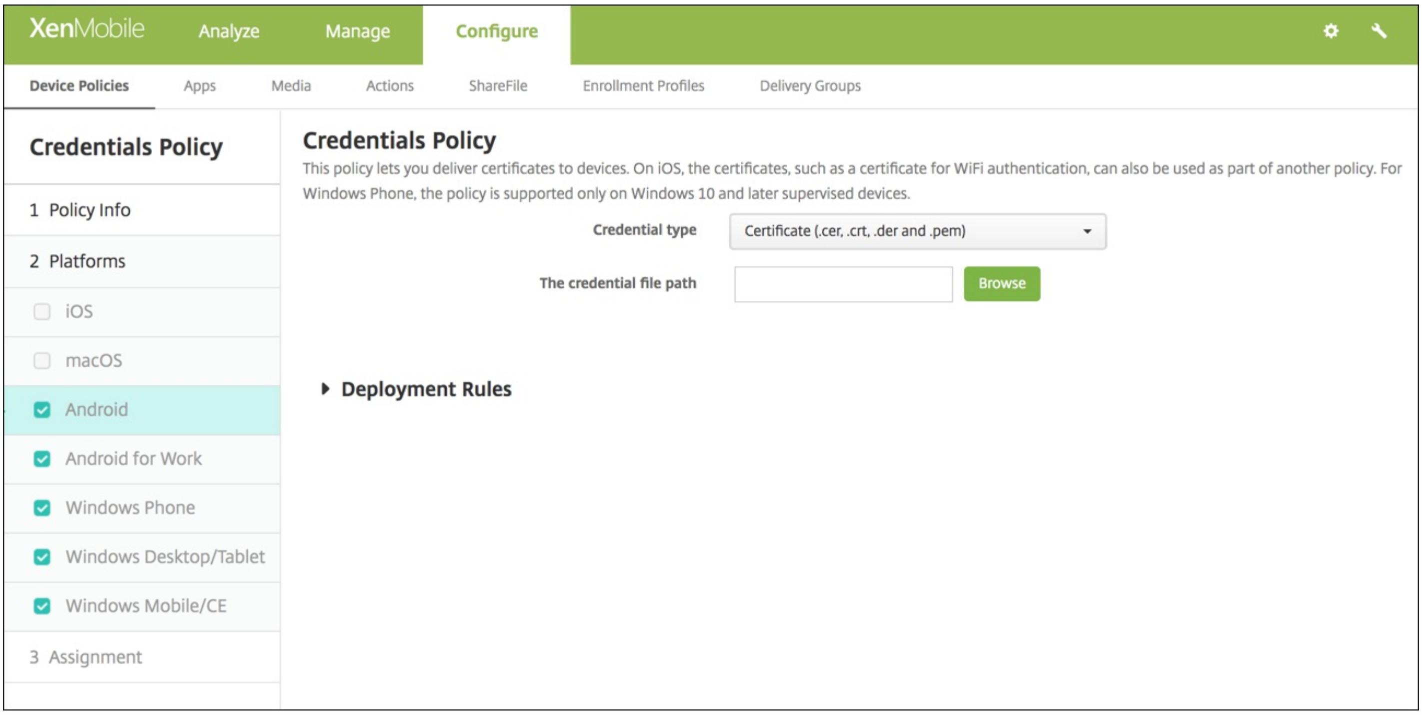
Allow user to remove policy: Always

Profile scope: User — macOS 10.7+

Configure the following settings:

- **Credential type**: In the list, click the type of credential to use with this policy and the, 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.
- **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 **Policy scope**, click either **User** or **System**. The default is **User**. This option is available only on macOS 10.7 and later.

Configure Android and Android for Work settings



Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

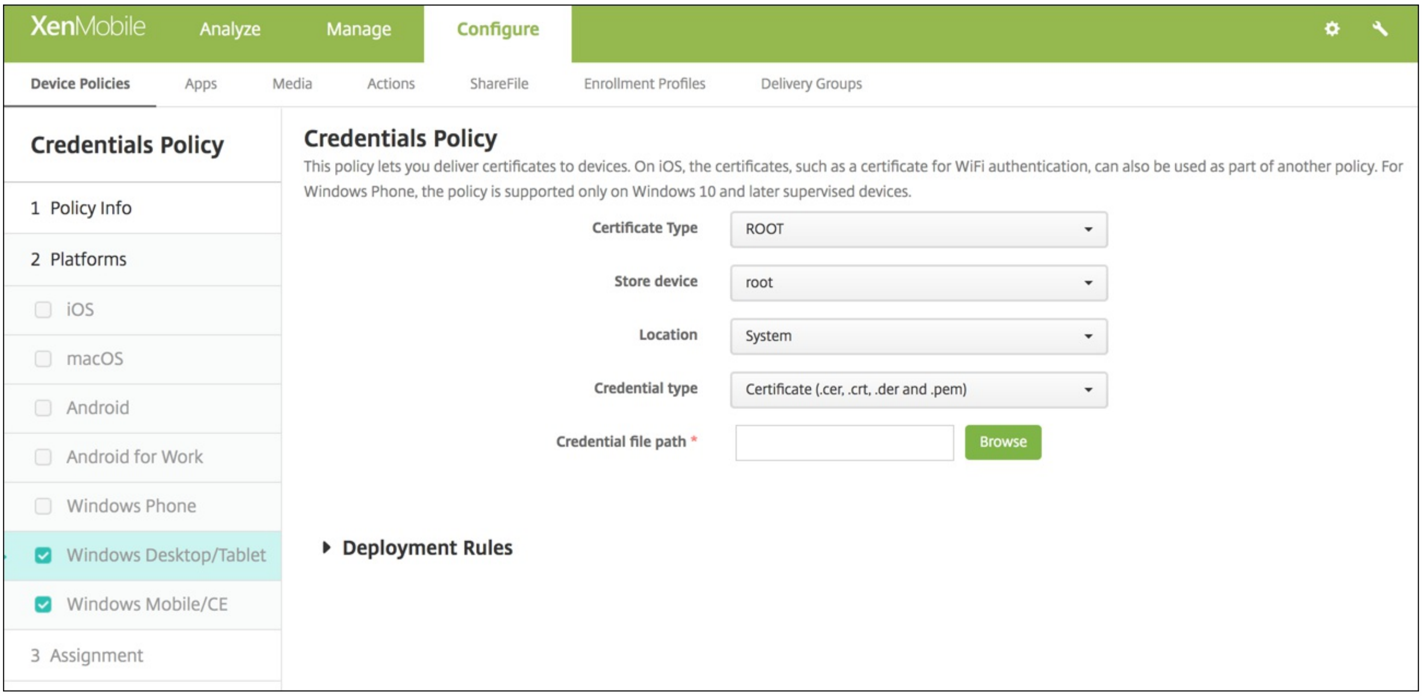
Credential type: Certificate (.cer, .crt, .der and .pem)

The credential file path:

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 Windows Desktop/Tablet settings



Credentials Policy

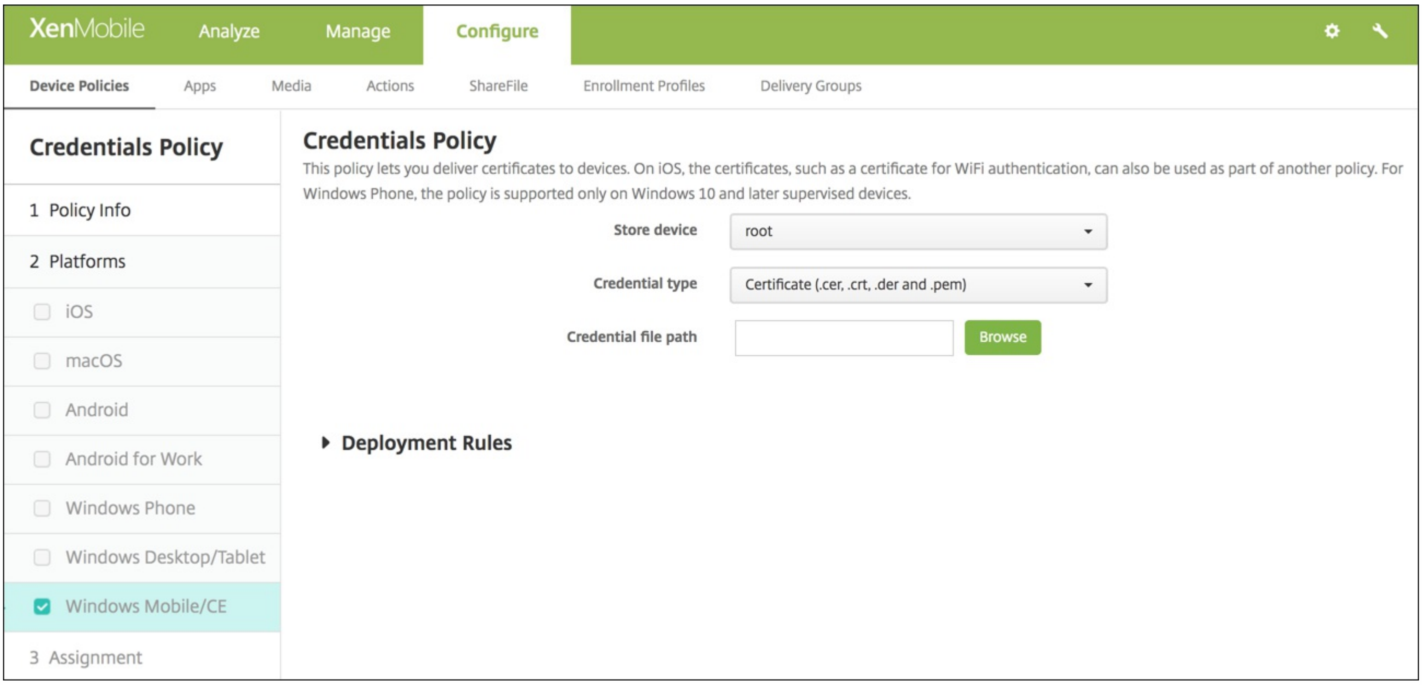
This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Certificate Type	ROOT
Store device	root
Location	System
Credential type	Certificate (.cer, .crt, .der and .pem)
Credential file path *	

Configure the following 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**: **System** is the only location for Windows 10 tablets.
  - **Credential type**: **Certificate** is the only credential type for Windows 10 tablets.
  - **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**: **System** is the only location for Windows 10 tablets.
- **Credential type**: **Keystore** is the only credential type for Windows 10 tablets.
- **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.

Configure Windows Mobile/CE settings



Credentials Policy

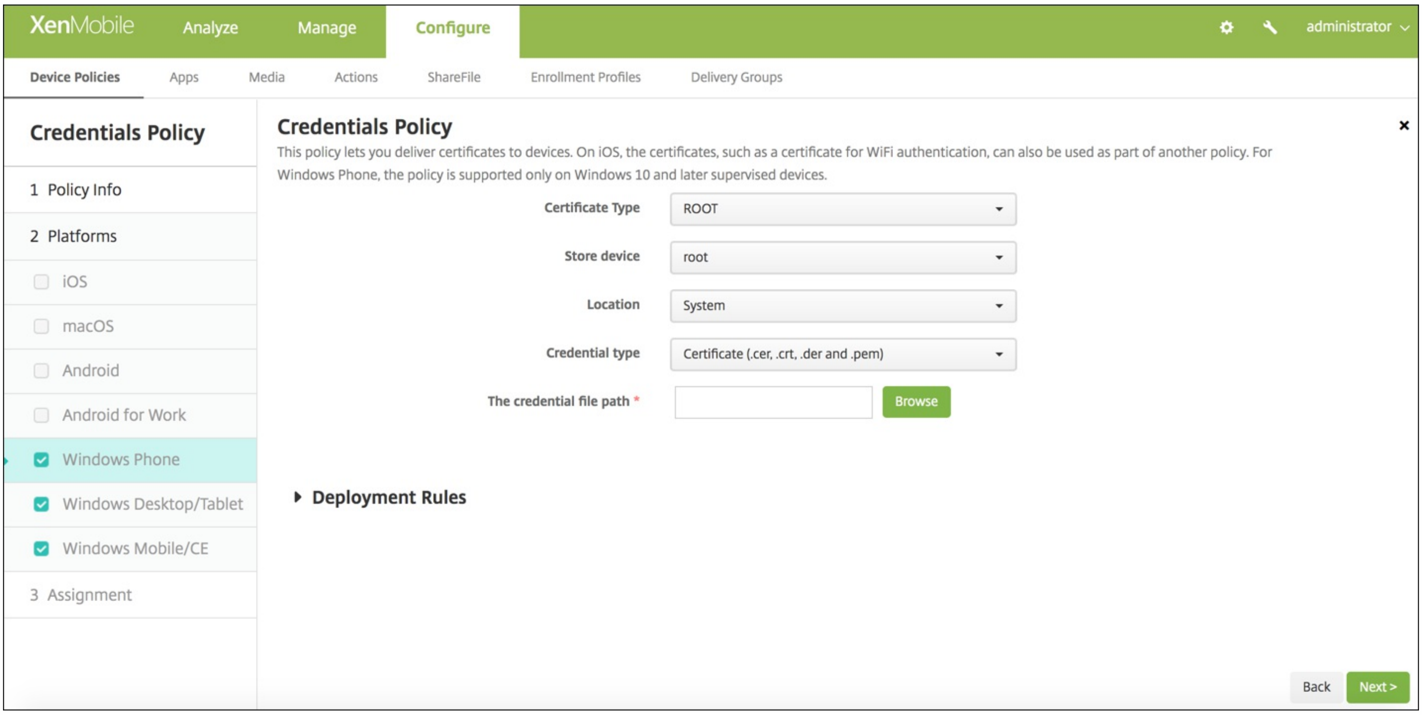
This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Store device	root
Credential type	Certificate (.cer, .crt, .der and .pem)
Credential file path	

Configure the following 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 will run with privileged trust level.
  - **Unprivileged execution trust authorities** - Applications signed with a certificate belonging to this store will run 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.

Configure Windows Phone settings



Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Certificate Type: ROOT
Store device: root
Location: System
Credential type: Certificate (.cer, .crt, .der and .pem)
The credential file path *

Configure the following 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**: System 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**: **System** is the only location for Windows phones.
  - **Credential type**: **Keystore** is the only credential type for Windows phones.
  - **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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Custom XML device policy

Sep 06, 2017

You can create custom XML policies in XenMobile to customize the following features on supported Windows and Zebra Android 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.

For Zebra Android 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 About MX on the Zebra 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.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add New Policy** dialog box appears.

3. Expand **More** and then under **Custom**, click **Custom XML**. The **Custom XML Policy** information page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy Platforms** page appears.

6. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.

7. Configure the following setting for each platform you selected:

- **XML content**: Type, or cut and paste, the custom XML code you want to add to the policy.

8. Configure deployment rules. For more information, see Add a device policy.

9. Click **Next**. XenMobile checks the XML content syntax. Any syntax errors appear below the content box. Fix any errors before you continue.

If there are no syntax errors, the **Custom XML Policy** assignment page appears.

10. Next to **Choose delivery groups**, type to find a delivery group. Or, select a group or groups in the list to which you want to assign the policy. The groups you select appear in the **Delivery groups to receive app assignment** list.

11. 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 deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms.

12. Click **Save**.

Defender device policy

Sep 06, 2017

Windows Defender is malware protection included with Windows 10. You can use the XenMobile device policy, Defender, to configure the Microsoft Defender policy for Windows 10 for desktop and tablet.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

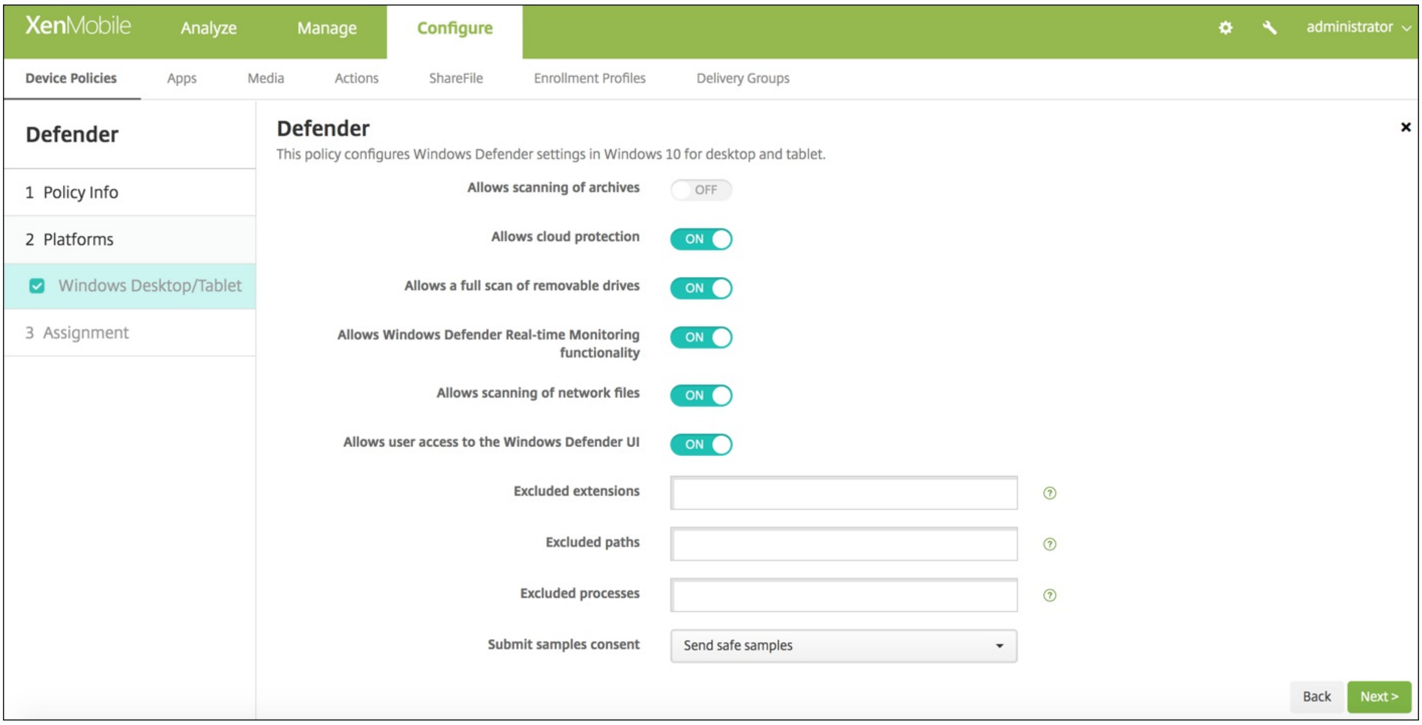
2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Start typing **Defender** and then click that name in the search results. The **Defender Policy information** page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

5. Click **Next**. The **Policy Platforms** page appears.



Defender

This policy configures Windows Defender settings in Windows 10 for desktop and tablet.

Allows scanning of archives: OFF

Allows cloud protection: ON

Allows a full scan of removable drives: ON

Allows Windows Defender Real-time Monitoring functionality: ON

Allows scanning of network files: ON

Allows user access to the Windows Defender UI: ON

Excluded extensions:

Excluded paths:

Excluded processes:

Submit samples consent: Send safe samples

Configure these 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**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Delete files and folders device policy

Sep 06, 2017

You can create a policy in XenMobile to delete specific files or folders from Windows Mobile/CE devices.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add New Policy** dialog box appears.

3. Expand **More** and then, under **Apps**, click **Delete Files and Folders**. The **Delete Files and Folders Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Windows Mobile/CE Platform** page appears.

6. Configure these 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** to not save the file or folder.

    Note: To delete an existing listing, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing listing, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Delete registry keys and values device policy

Sep 06, 2017

You can create a policy in XenMobile to delete specific registry keys and values from Windows Mobile/CE devices.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add New Policy** dialog box appears.

3. Expand **More** and then, under **Apps**, click **Delete Registry Keys and Values**. The **Delete Registry Keys and Values Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Windows Mobile/CE Platform** page appears.

6. Configure these settings:

- **Registry keys and values to delete**: for each registry key and value you want to delete, click **Add** and then do the following:
  - **Key**: Type the registry key path. This is a required field.The registry key path should either start with HKEY_CLASSES_ROOT\ or HKEY_CURRENT_USER\ or HKEY_LOCAL_MACHINE\ or HKEY_USERS\.
  - **Value**: Type the value name to be deleted or leave this field blank to delete the entire registry key.
  - Click **Save** to save the key and value, or click **Cancel** to not save the key and value.

    Note: To delete an existing listing, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing listing, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Device Health Attestation device policy

Oct 20, 2017

In XenMobile, you can require Windows 10 devices to report the state of their health by having those 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 XenMobile. When XenMobile receives the Health Attestation Certificate, based on the contents of the Health Attestation Certificate, it can deploy automatic actions that you have set up previously.

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
- DEP 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.

To configure DHA using Microsoft Cloud

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add** to add a new policy. The **Add a New Policy** dialog box appears.

3. Click **More**, and then under **Custom**, click **Device Health Attestation policy**. The **Device Health Attestation Policy** information page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.

Configure this setting for each platform that you choose:

- **Enable Device Health Attestation**: Select whether to require Device Health Attestation. The default is **OFF**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

To configure DHA using an on-premises Windows DHA server

To enable DHA on-premises, you first configure a DHA server. Then you create a XenMobile Server policy to enable the on-premises DHA service.

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 configure DHA using an on-premises Windows DHA server:

1. In the XenMobile console, click **Configure > Device Policies**. The Device Policies page appears.

2. If you have already created a policy to enable DHA through Microsoft Cloud, skip to step 8.

3. Click **Add** to add a new policy. The **Add a New Policy** dialog box appears.

4. Click **More**, and then under **Custom**, click **Device Health Attestation policy**. The **Device Health Attestation Policy** information page appears.

5. In the Policy Information pane, enter the following information:

   Policy Name: Type a descriptive name for the policy.

   Description: Type an optional description of the policy.

6. Click **Next**. The **Policy Platforms** page appears.

7. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.

8. For each platform that you choose:

   a. Set **Enable Device Health Attestation** to **ON**.

   b. Set **Configure On-prem Health Attestation Service** to **ON**.

   c. In **On-prem DHA Service FQDN**, enter the fully qualified domain name of the DHA server you set up.

   d. In **On-prem DHA API version**, choose the version of the DHA service installed on the DHA server.

9. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Device name device policy

Sep 19, 2017

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 XenMobile.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** page appears.

3. Expand **More**, and under **End User**, click **Device name**. The **Device Name Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

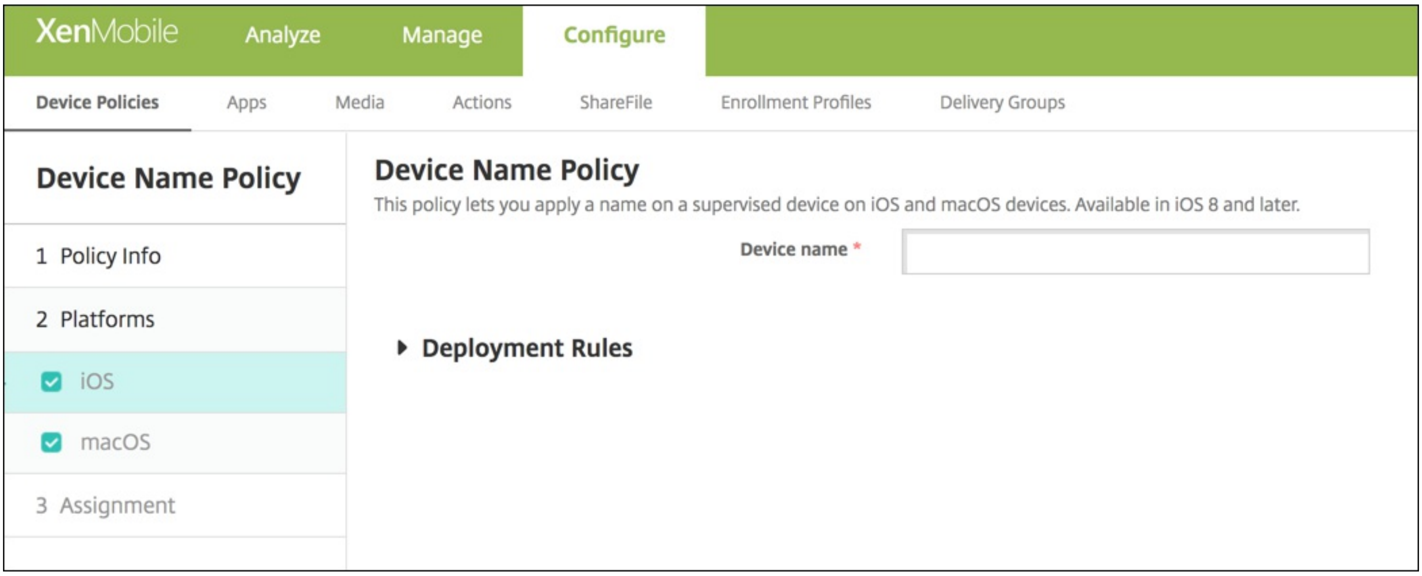
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS and macOS settings



Device Name Policy

This policy lets you apply a name on a supervised device on iOS and macOS devices. Available in iOS 8 and later.

Device name *

▸ Deployment Rules

Configure this setting for the platforms you choose:

- **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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Education Configuration device policy

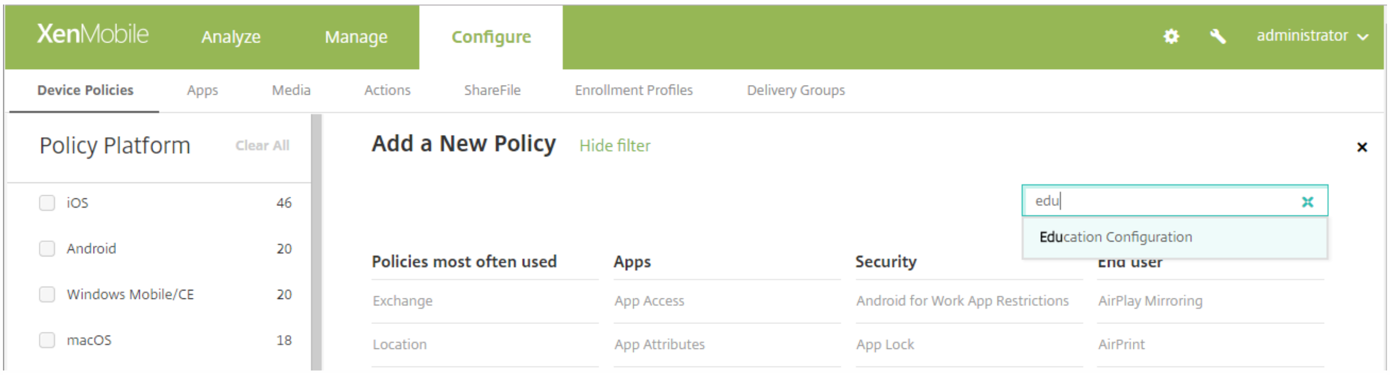
Sep 06, 2017

The Education Configuration device policy defines:

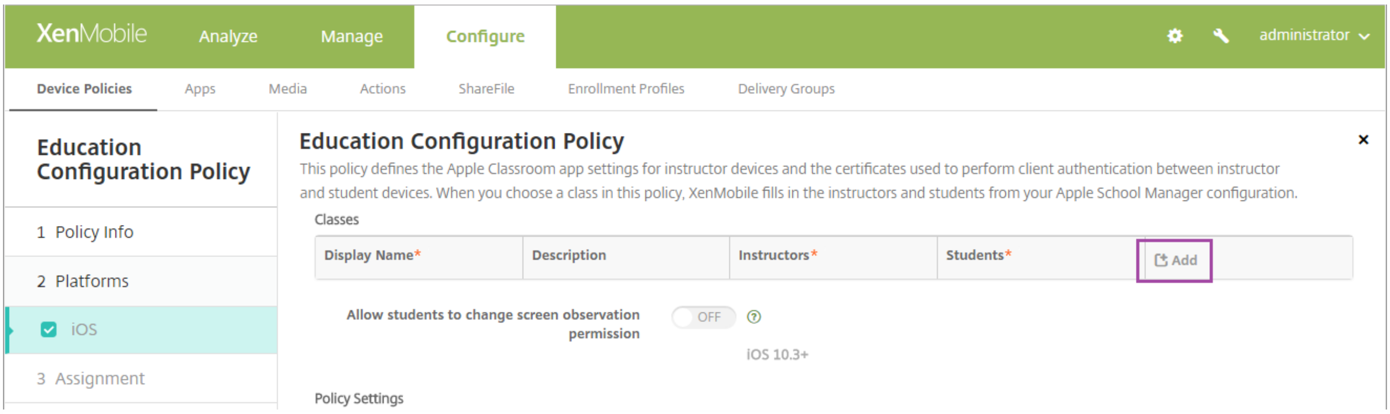
- The Apple Classroom app settings for instructor devices.
- The certificates used to perform client authentication between instructor and student devices.

When you choose a class in this policy, the XenMobile 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.

1. In the XenMobile console, go to **Configure > Device Policies** and then click **Add**.
2. In the search box, start typing **education** and then click **Education Configuration**.



3. On the **Policy Information** page, type a **Policy Name** to identify the policy in XenMobile.
4. On the **Education Configuration Policy** page, click **Add**.



Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Classes

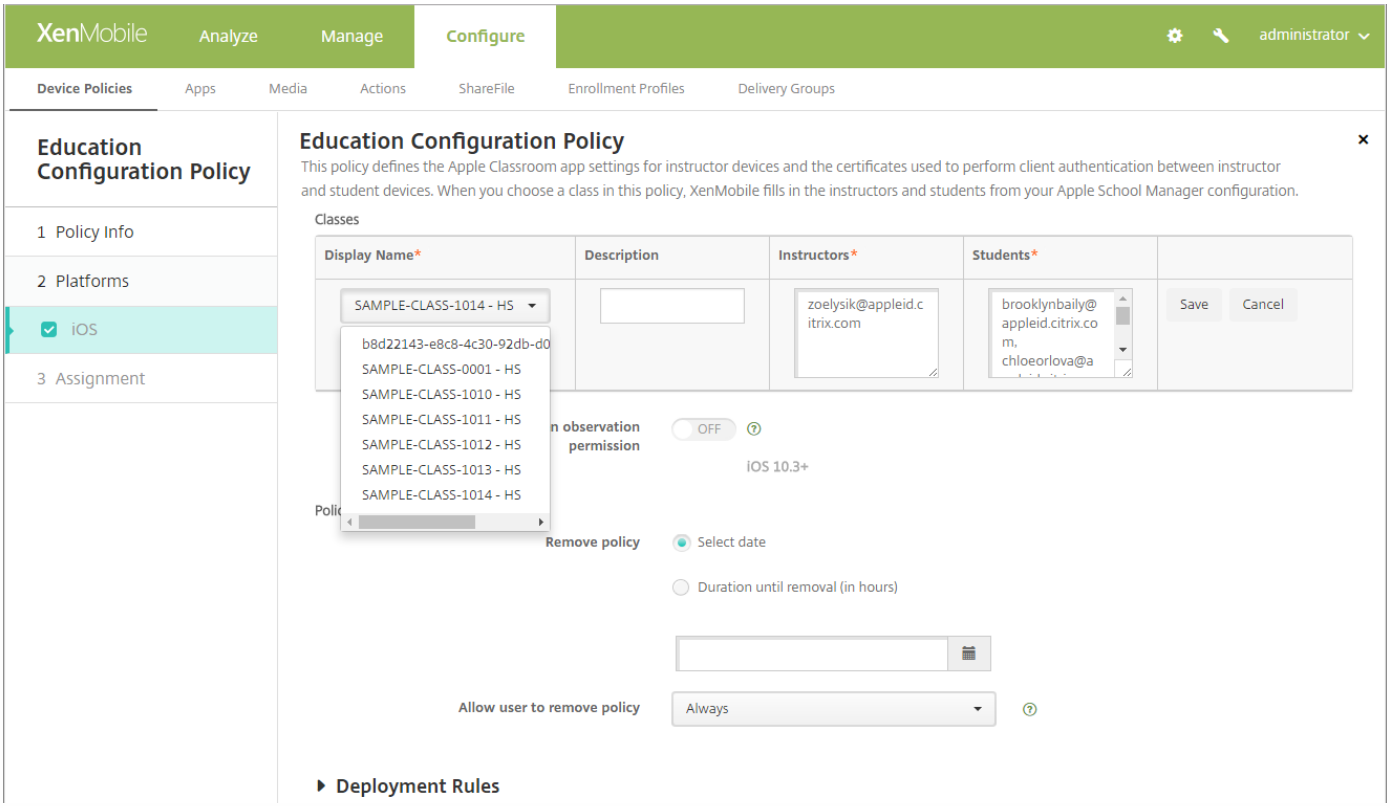
Display Name*	Description	Instructors*	Students*	Add

Allow students to change screen observation permission: OFF

iOS 10.3+

Policy Settings

5. Click the **Display Name** list. A list of classes obtained from your connected Apple School Manager account appears.



Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Classes

Display Name*	Description	Instructors*	Students*	
SAMPLE-CLASS-1014 - HS		zoelysik@appleid.citrix.com	brooklynbaily@appleid.citrix.com, chloeorlova@a	Save Cancel

n observation permission OFF

iOS 10.3+

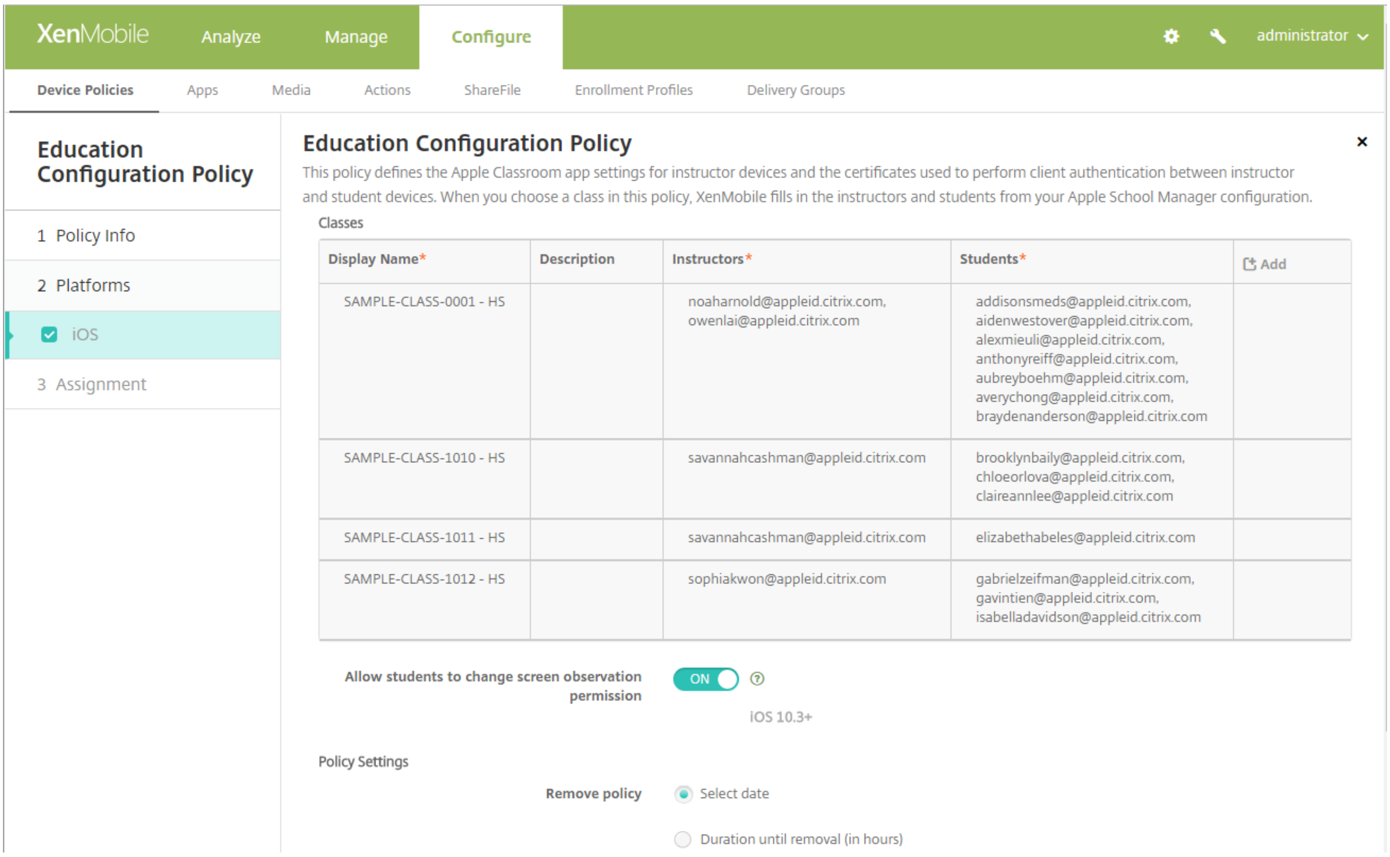
Remove policy ● Select date

○ Duration until removal (in hours)

Allow user to remove policy: Always

Deployment Rules

When you choose a class from **Display Name**, XenMobile fills in the instructors and students. Continue adding classes.



Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Classes

Display Name*	Description	Instructors*	Students*	Add
SAMPLE-CLASS-0001 - HS		noaharnold@appleid.citrix.com, owenlai@appleid.citrix.com	addisonsmeds@appleid.citrix.com, aidenwestover@appleid.citrix.com, alexmieuli@appleid.citrix.com, anthonyreiff@appleid.citrix.com, aubreyboehm@appleid.citrix.com, averychong@appleid.citrix.com, braydenanderson@appleid.citrix.com	
SAMPLE-CLASS-1010 - HS		savannahcashman@appleid.citrix.com	brooklynbaily@appleid.citrix.com, chloeorlova@appleid.citrix.com, claireannlee@appleid.citrix.com	
SAMPLE-CLASS-1011 - HS		savannahcashman@appleid.citrix.com	elizabethabeles@appleid.citrix.com	
SAMPLE-CLASS-1012 - HS		sophiakwon@appleid.citrix.com	gabrielzeifman@appleid.citrix.com, gavintien@appleid.citrix.com, isabelladavidson@appleid.citrix.com	

Allow students to change screen observation permission ON

iOS 10.3+

Policy Settings

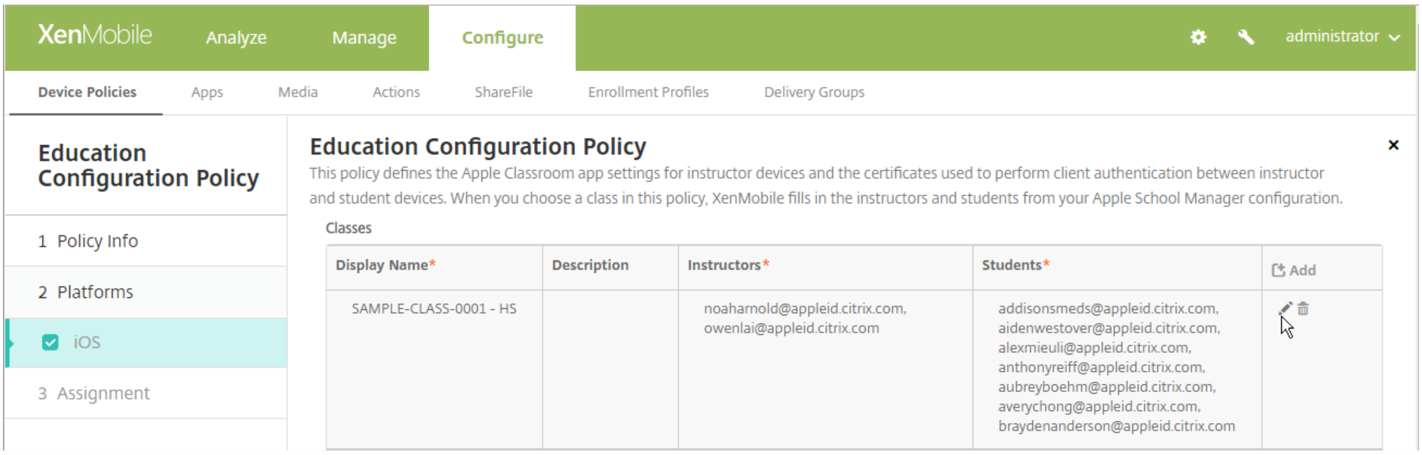
Remove policy ● Select date

○ Duration until removal (in hours)

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. XenMobile Server 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.



Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Classes

Display Name*	Description	Instructors*	Students*	Add
SAMPLE-CLASS-0001 - HS		noaharnold@appleid.citrix.com, owenlai@appleid.citrix.com	addisonsmeds@appleid.citrix.com, aidenwestover@appleid.citrix.com, alexmieuli@appleid.citrix.com, anthonyreiff@appleid.citrix.com, aubreyboehm@appleid.citrix.com, averychong@appleid.citrix.com, braydenanderson@appleid.citrix.com	

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.

Enterprise Hub device policy

Sep 06, 2017

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 Symantec
- The Citrix Company Hub app signed by using the Microsoft app signing tool (XapSignTool.exe)

Note: XenMobile supports only one Enterprise Hub policy for one mode of Windows Phone Secure Hub. For example, to upload Windows Phone Secure Hub for XenMobile Enterprise Edition, you should not create multiple Enterprise Hub policies with different versions of Work Home for XenMobile Enterprise Edition. You can only deploy the initial Enterprise Hub policy during device enrollment.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

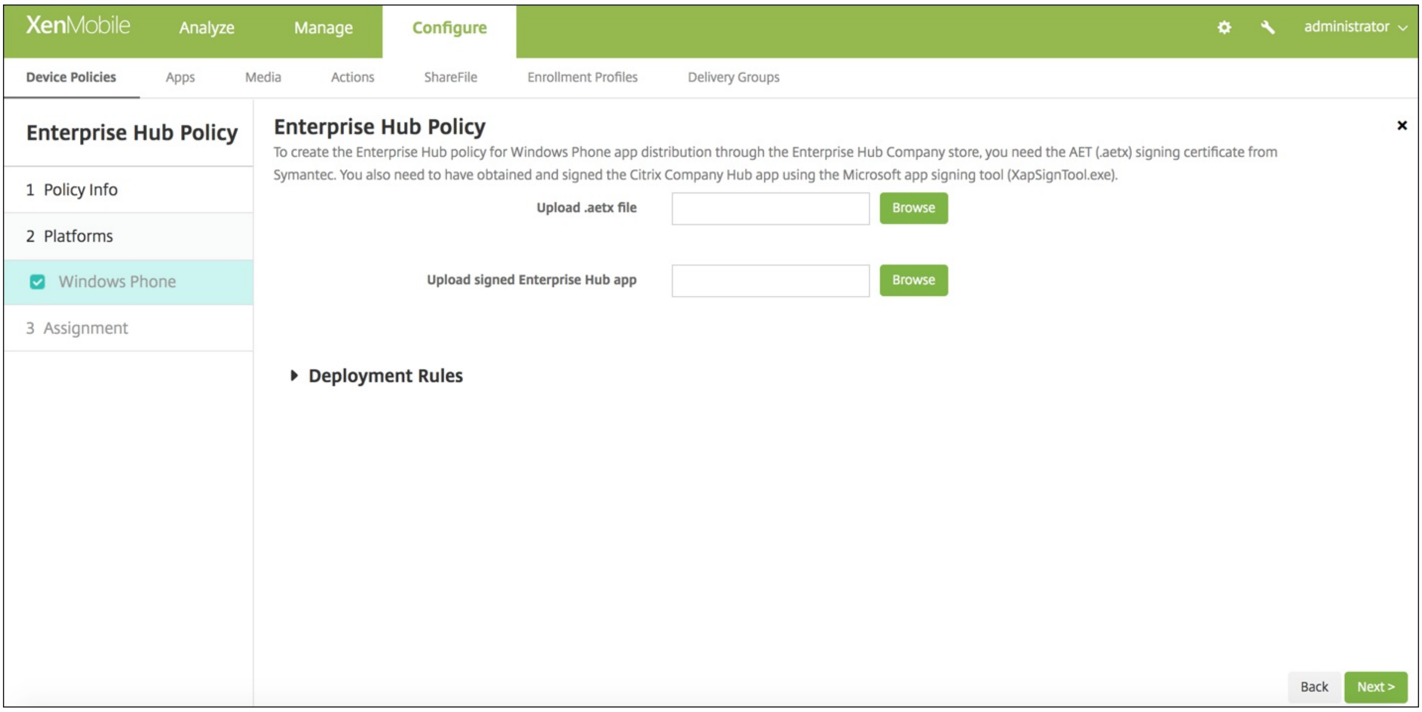
2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Expand **More** and then, under **XenMobile agent**, click **Enterprise Hub**. The **Enterprise Hub Policy** page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Windows Phone** platform page appears.



Enterprise Hub Policy

To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe).

Upload .aetx file

Upload signed Enterprise Hub app

6. Configure these settings:

- **Upload .aetx file**: Select the .aetx file by clicking **Browse** and navigating to the file's location.
- **Upload signed Enterprise Hub app**: Select the Enterprise Hub app by clicking **Browse** and navigating to the app's location.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Exchange device policy

Sep 06, 2017

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 TouchDown, Android for Work, 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.

iOS

macOS

Android HTC

Android TouchDown

Android for Work

Samsung SAFE and Samsung KNOX

Windows Phone and Windows Desktop/Tablet

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.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **Exchange**. The **Exchange Policy** information page appears.

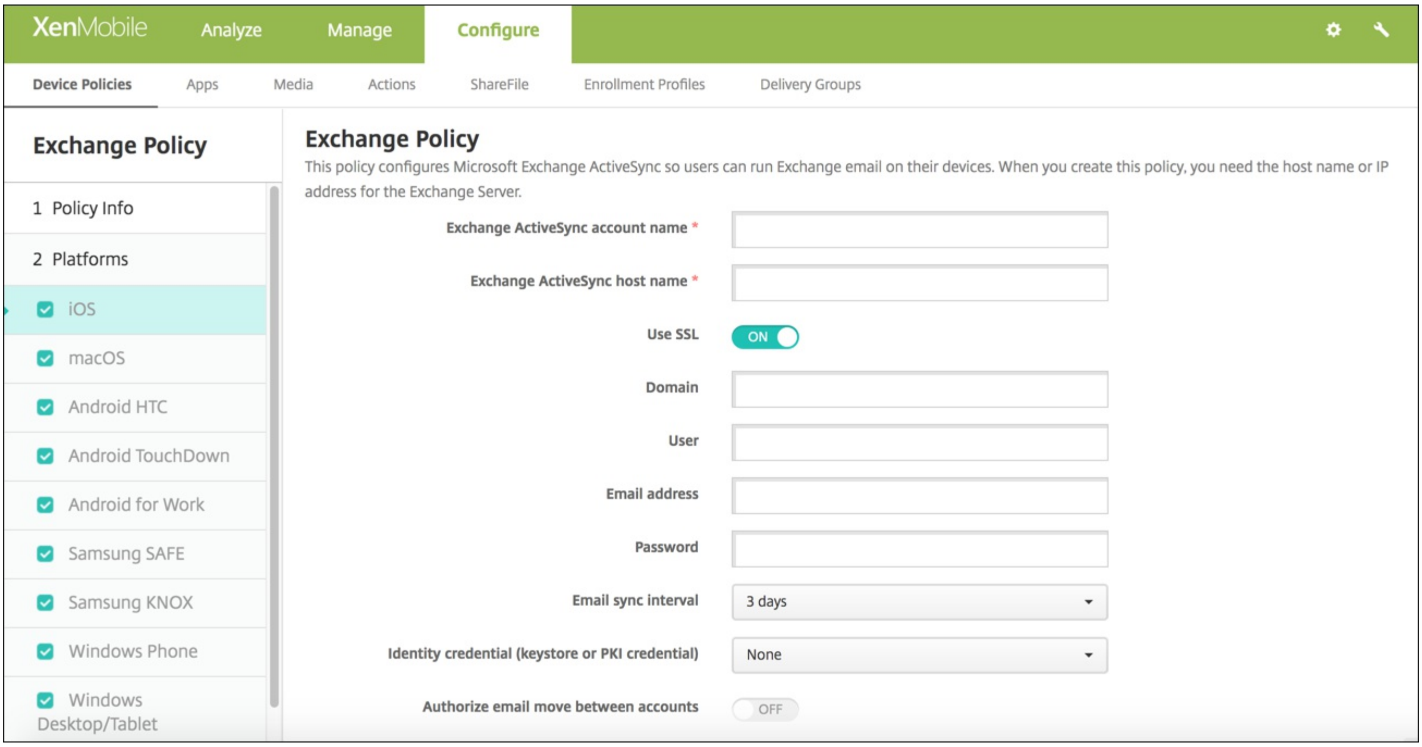
4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. 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, refer to Step 7 for how to set deployment rules.

Configure iOS settings



Exchange Policy

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

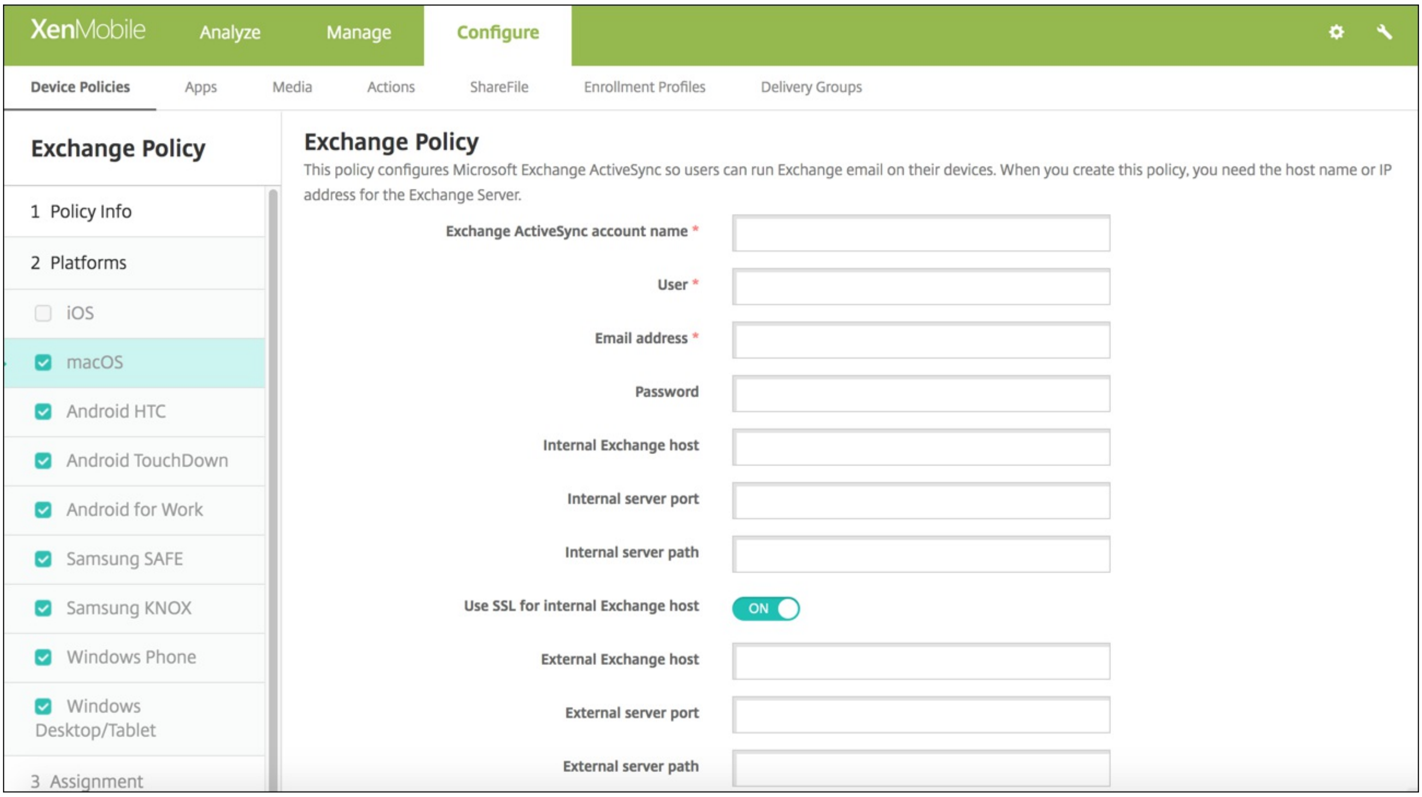
Exchange ActiveSync account name *	
Exchange ActiveSync host name *	
Use SSL	ON
Domain	
User	
Email address	
Password	
Email sync interval	3 days
Identity credential (keystore or PKI credential)	None
Authorize email move between accounts	OFF

Configure these 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.
- **Password**: Enter an optional password for the Exchange user account.
- **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 XenMobile. 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**. This option applies only to iOS 6.0 and later.
- **Enable S/MIME**: Select whether this account supports S/MIME authentication and encryption. The default is **OFF**. When set to **ON**, the following two fields appear:
  - **Signing identity credential**. The default is **None**.
  - **Encryption identity credential**. The default is **None**.

- **Enable per message S/MIME switch**: Select whether to allow users to encrypt outgoing email on a per-message basis. The default is **OFF**.

Configure macOS settings



Exchange Policy

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Exchange ActiveSync account name *

User *

Email address *

Password

Internal Exchange host

Internal server port

Internal server path

Use SSL for internal Exchange host: ON

External Exchange host

External server port

External server path

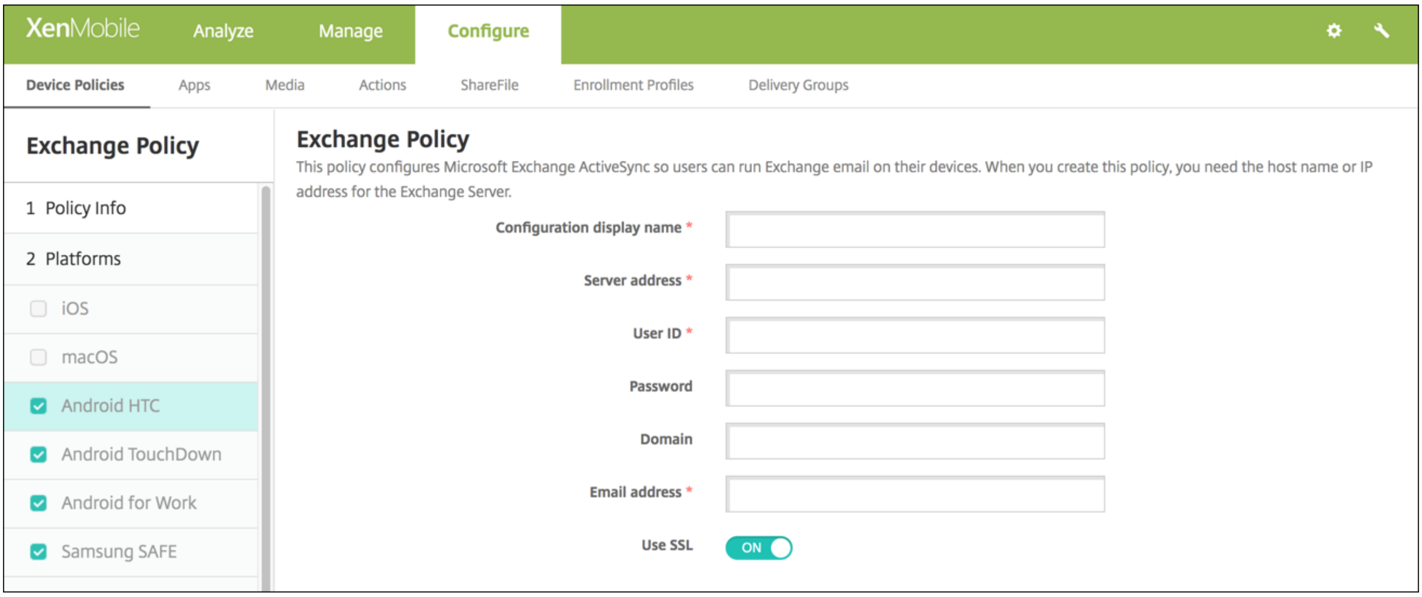
Configure these settings:

- **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.
- **Password**: Enter an optional password for the Exchange user account.
- **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 different, type an optional

external Exchange server path.

- **Use SSL for external Exchange host**: Select whether to secure connections between user devices and the internal Exchange host. The default is **ON**.
- **Allow Mail Drop**: Select whether to allow users to share files wirelessly between two Macs, without having to connect to an existing network. The default is **OFF**.

Configure Android HTC settings



Exchange Policy

1 Policy Info

2 Platforms

□ iOS

□ macOS

☑ Android HTC

☑ Android TouchDown

☑ Android for Work

☑ Samsung SAFE

Exchange Policy

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Configuration display name *

Server address *

User ID *

Password

Domain

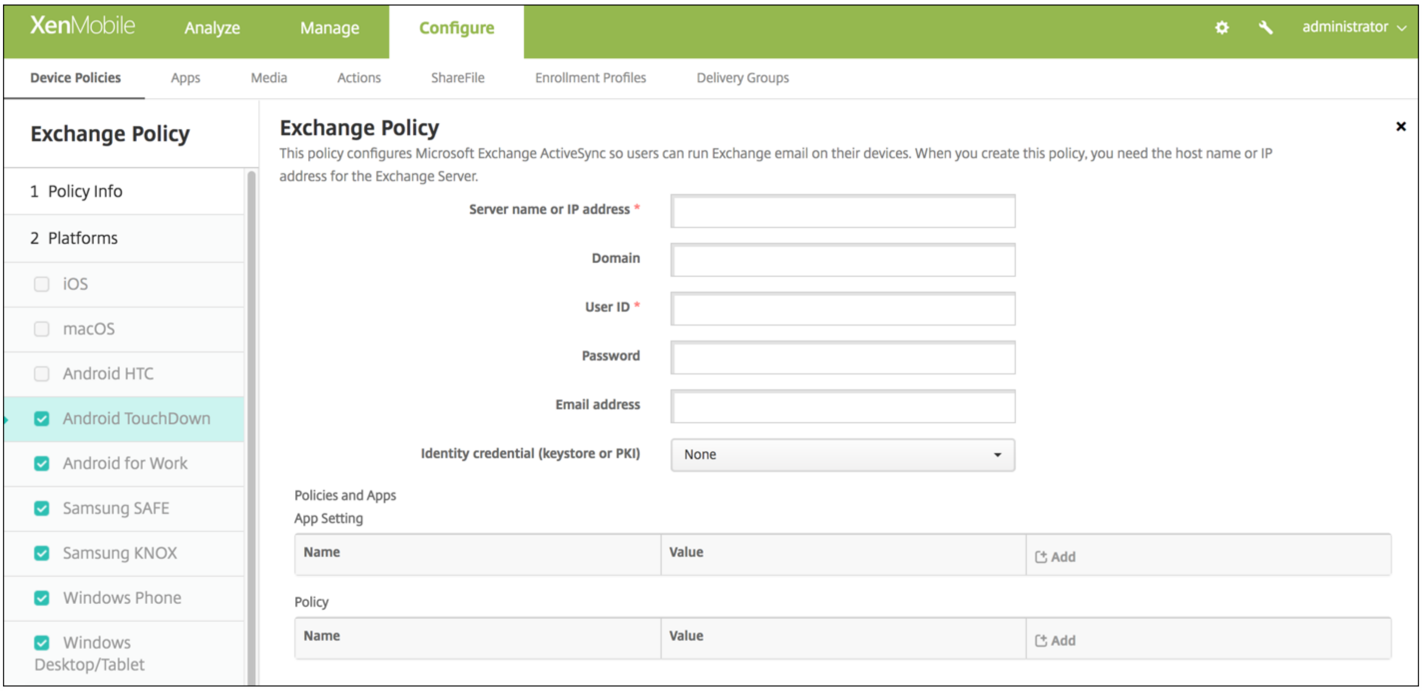
Email address *

Use SSL ON

Configure these settings:

- **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**.

Configure Android TouchDown settings



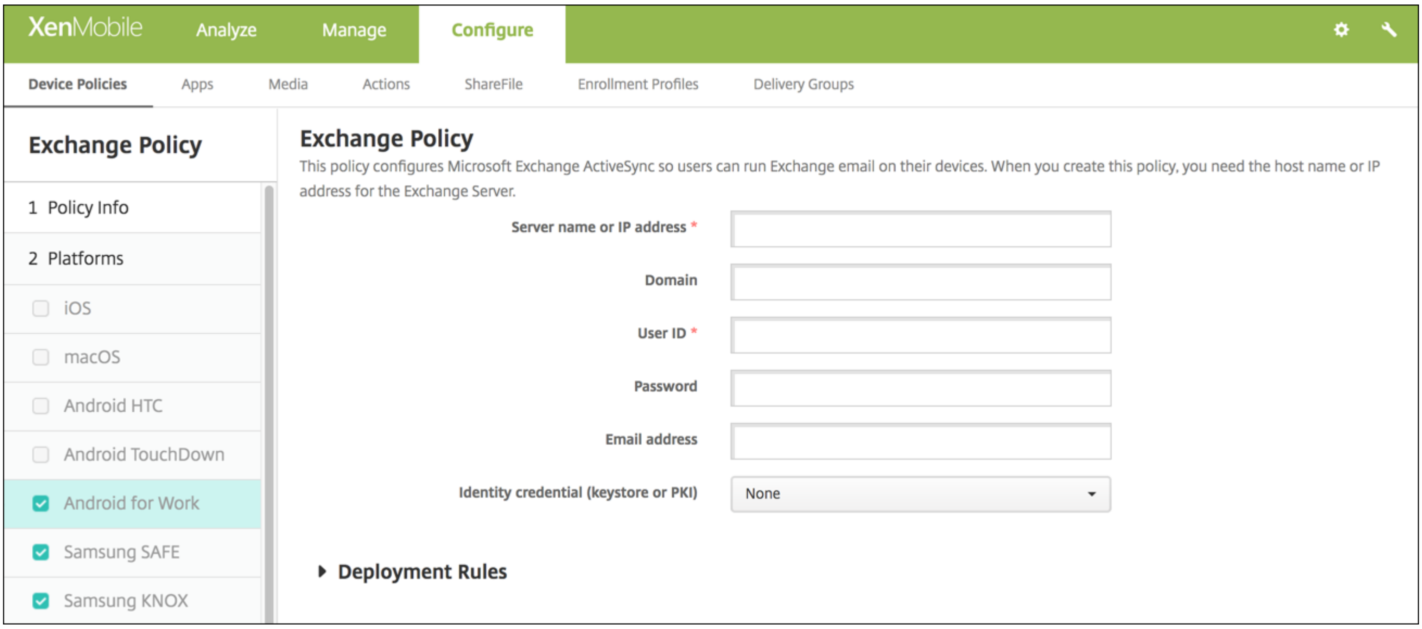
This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Identity credential (keystore or PKI): None

Configure these settings:

- **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 XenMobile. 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.

Configure Android for Work



Exchange Policy

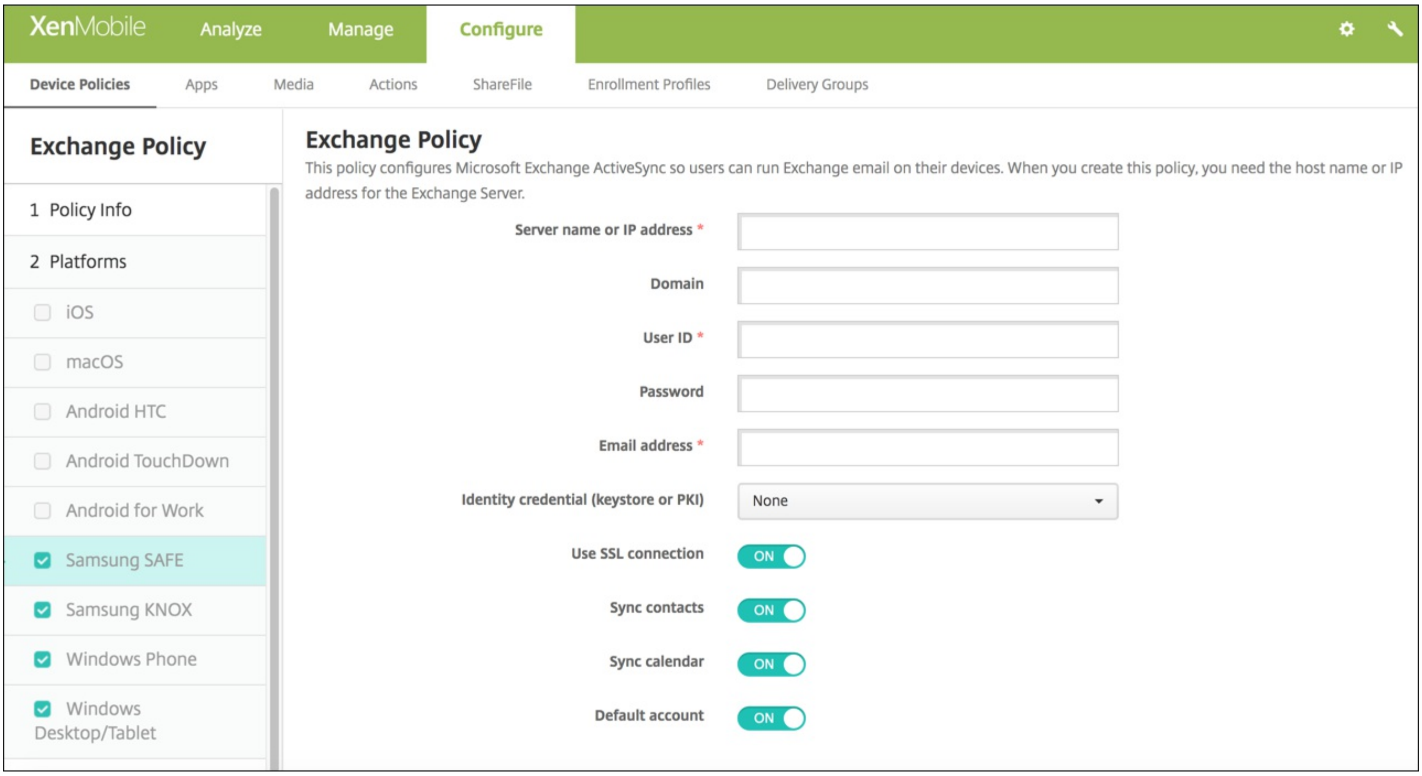
This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Server name or IP address *	
Domain	
User ID *	
Password	
Email address	
Identity credential (keystore or PKI)	None

Configure these settings:

- **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 XenMobile. This field is only required when Exchange requires a client certificate authentication. The default is **None**.

Configure Samsung SAFE and Samsung KNOX settings



Exchange Policy

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Server name or IP address *

Domain

User ID *

Password

Email address *

Identity credential (keystore or PKI): None

Use SSL connection: ON

Sync contacts: ON

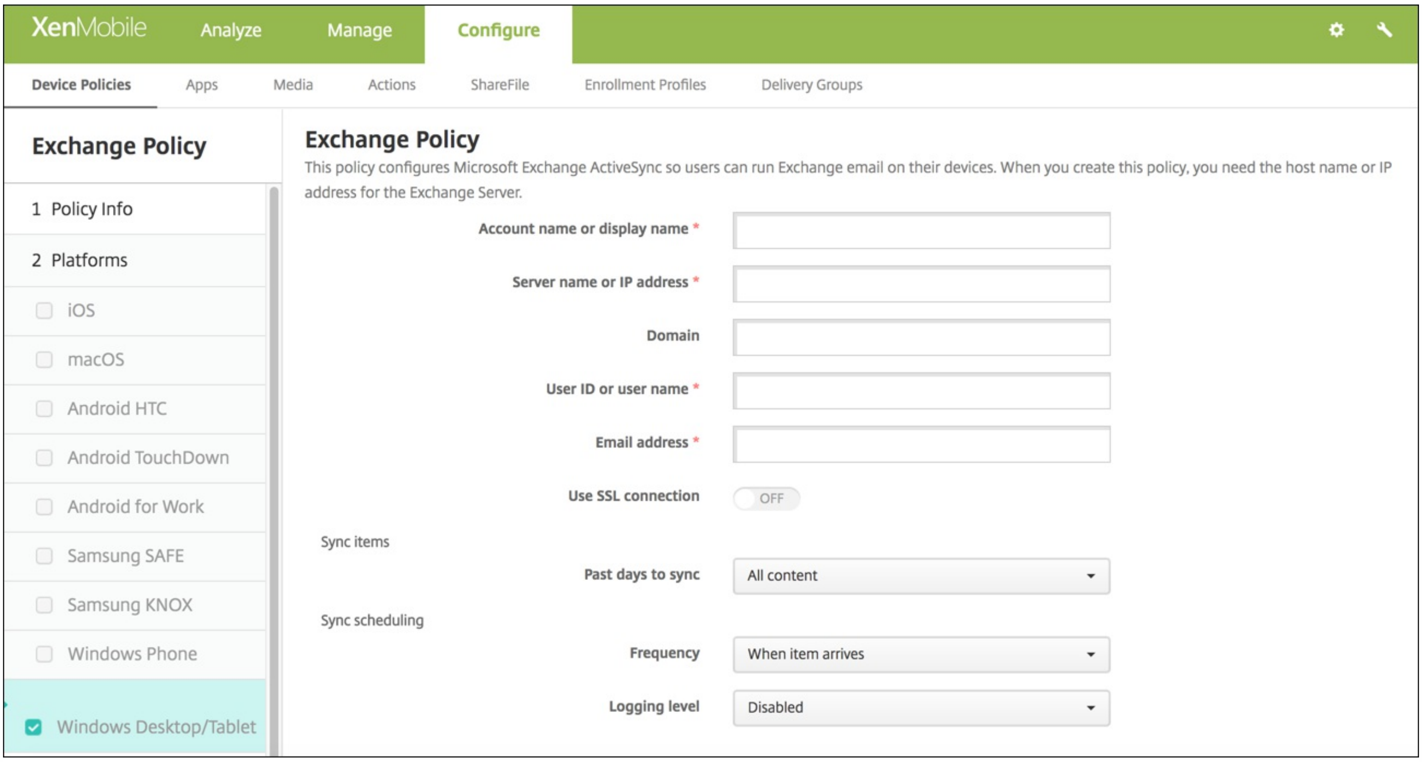
Sync calendar: ON

Default account: ON

Configure these settings:

- **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 XenMobile. 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**.

Configure Windows Phone and Windows Desktop/Tablet settings



Exchange Policy

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Account name or display name *	
Server name or IP address *	
Domain	
User ID or user name *	
Email address *	
Use SSL connection	OFF
Sync items	
Past days to sync	All content
Sync scheduling	
Frequency	When item arrives
Logging level	Disabled

Configure these settings:

Note: This policy does not allow you to set the user password. Users must set that parameter from their devices after you push the policy.

- **Account name or display name**: Type the Exchange ActiveSync account name.
- **Server name or IP address**: Type the Exchange Server host name or IP address.
- **Domain**: Enter the domain in which the Exchange Server 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 it 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**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Files device policy

Sep 06, 2017

You can add script files to XenMobile 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. 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
- For Windows Mobile and Windows CE only: Script files created with MortScript

1. In the XenMobile 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 **Apps**, click **Files**. The **Files 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 **Policy 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, refer to Step 7 for how to set that platform's deployment rules.

Configure Android settings

Configure the following settings:

- **File to be imported**: Select the file to import by clicking Browse and navigating to the file's location.
- **File type**: Select either **File** or **Script**. When you select **Script**, **Execute immediately** appears. Select whether the script is executed as soon as 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 the macros %XenMobile Folder%\ or %Flash Storage%\ as the start of a path identifier.
- **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.

Configure Windows Mobile/CE settings

Configure the following settings:

- **File to be imported**: Select the file to import by clicking Browse and navigating to the file's location.
- **File type**: Select either **File** or **Script**. When you select **Script**, **Execute immediately** appears. Select whether the script is executed as soon as 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%\
  - %XenMobile 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**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Font device policy

Sep 06, 2017

You can add a device policy in XenMobile to add additional fonts to users' iOS and macOS devices. Fonts must be TrueType (.ttf) or OpenType (.oft) fonts. Font collections (.ttc or .otc) are not supported.

Note: For iOS, this policy applies only to iOS 7.0 and later.

1. In the XenMobile 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 **End user**, click **Font**. The **Font Policy** 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 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, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS setting

Configure the following settings:

- **User-visible name**: Type the name that users see in their font lists.
- **Font file**: Select the font file to be added to users' devices by clicking **Browse** and then navigating to the file's location.
- **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.

Configure macOS settings

Configure the following settings:

- **User-visible name**: Type the name that users see in their font lists.
- **Font file**: Select the font file to be added to users' devices by clicking **Browse** and then navigating to the file's location.
- **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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Home screen layout device policy

Sep 06, 2017

You can specify the layout of apps and folders for the iOS Home screen. The Home screen layout device policy is for iOS 9.3 and later supervised devices.

> ## Note
>
> 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 XenMobile policy or through the Apple Configurator.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

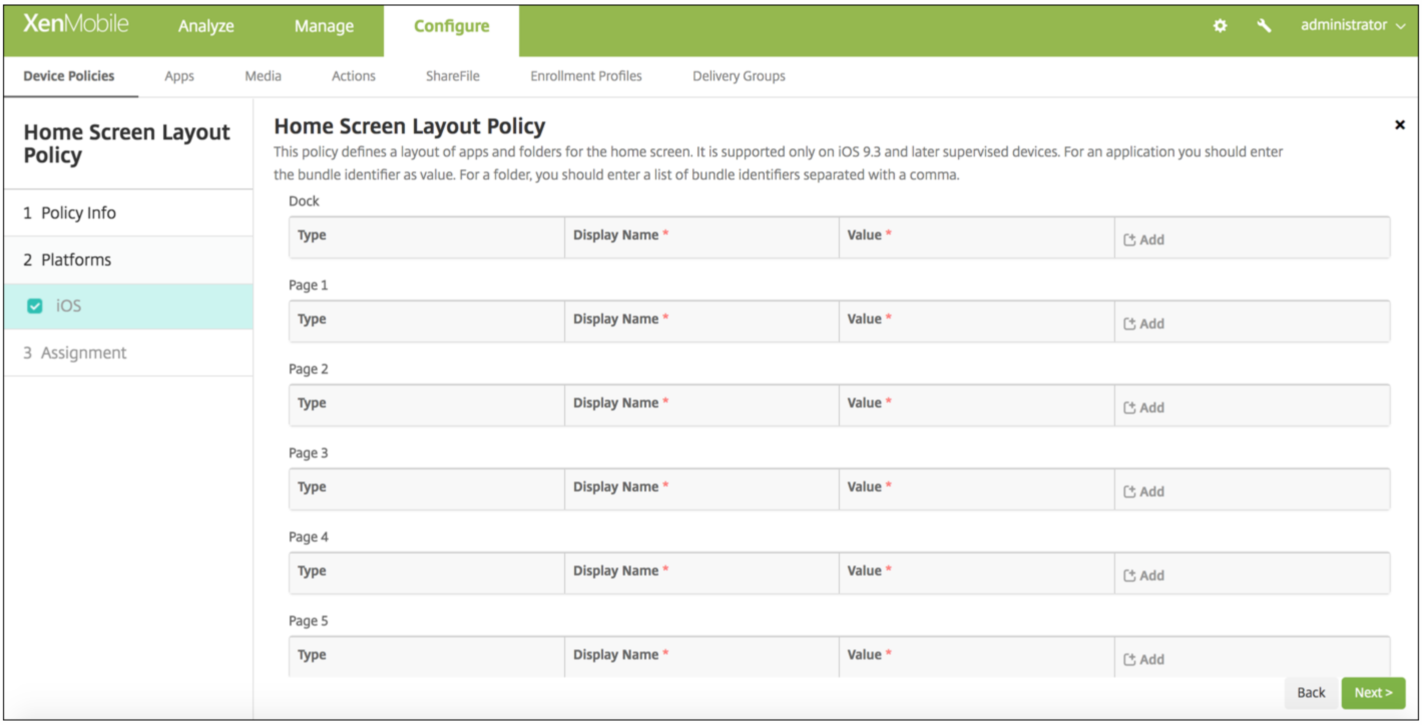
2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Start typing **Home Screen Layout** and then click that name in the search results. The **Home Screen Layout Policy information** page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

5. Click **Next**. The **iOS** pane appears.

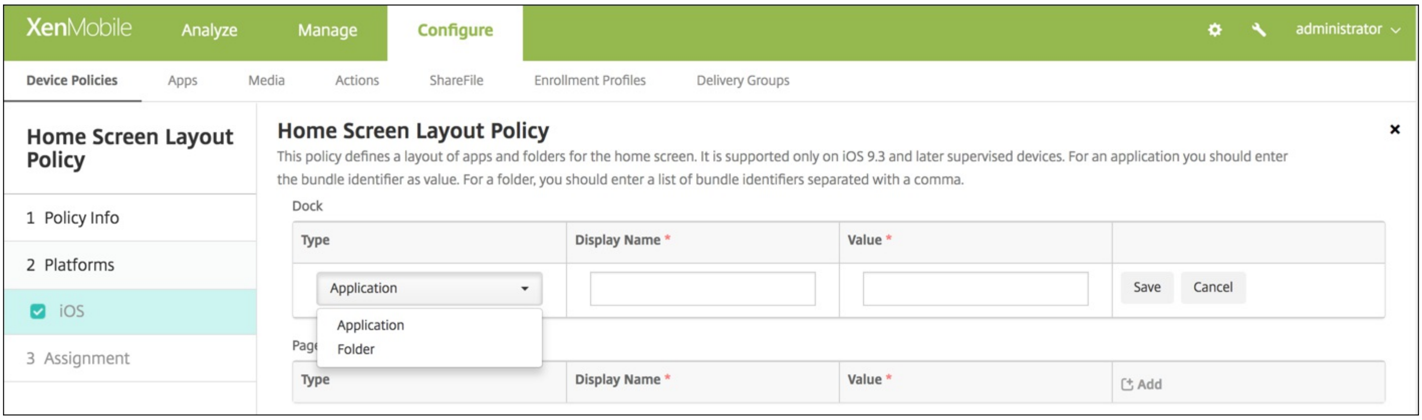


Home Screen Layout Policy

This policy defines a layout of apps and folders for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application you should enter the bundle identifier as value. For a folder, you should enter a list of bundle identifiers separated with a comma.

6. Configure the settings:

- For each of the screen areas you want to configure (such as **Dock** or **Page 1**), click **Add**.
- **Type**: Choose either **Application** or **Folder**.



Home Screen Layout Policy

This policy defines a layout of apps and folders for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application you should enter the bundle identifier as value. For a folder, you should enter a list of bundle identifiers separated with a comma.

- **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.

Policy Settings

- **Remove policy**: Either choose **Select date** and choose a date from the calendar, or choose **Duration until removal** and specify the number of days.
- **Allow user to remove policy**: Specify when to allow a user to remove the home screen definition: **Always**, **Passcode required** (only if they provide a passcode), or **Never**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Import iOS & macOS Profile device policy

Sep 06, 2017

You can import device configuration XML files for iOS and macOS devices into XenMobile. The file contains device security policies and restrictions that you prepare with the Apple Configurator.

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.

1. In the XenMobile console, click **Configure > Device Policies**.

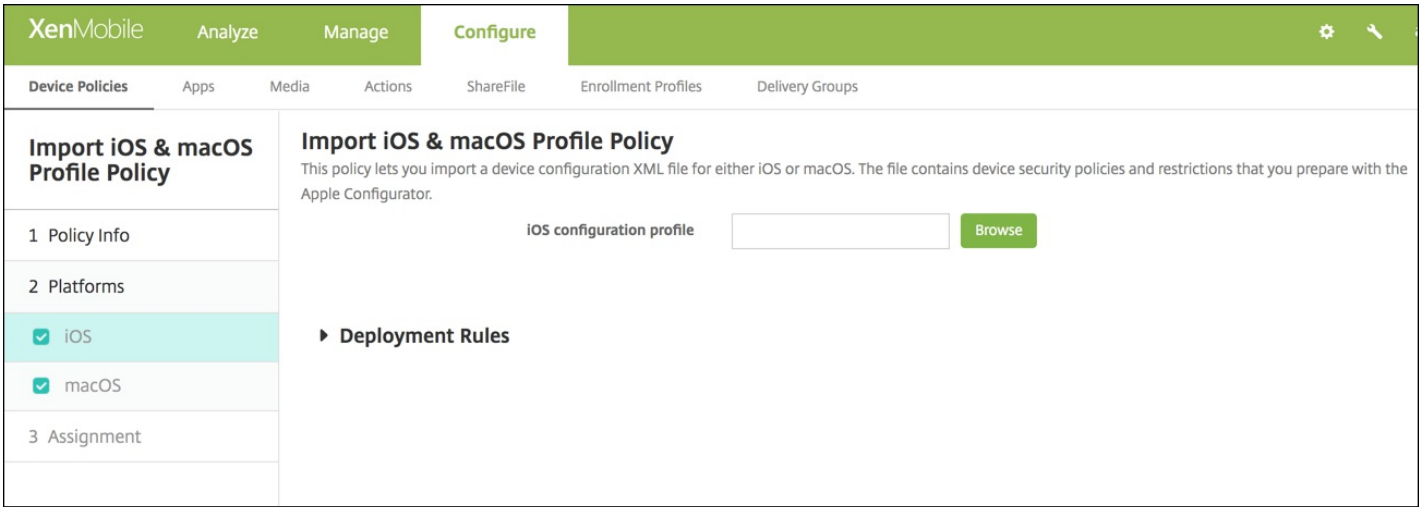
2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Expand **More**, and then under **Custom**, click **Import iOS & macOS Profile**. The **Import iOS & macOS Profile Policy** information page appears.

4. On the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy Platforms** page appears.



Import iOS & macOS Profile Policy

This policy lets you import a device configuration XML file for either iOS or macOS. The file contains device security policies and restrictions that you prepare with the Apple Configurator.

iOS configuration profile

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, refer to Step 8 for how to set that platform's deployment rules.

7. Configure this setting for each platform you selected:

- **iOS configuration profile** or **macOS configuration profile**: Select the configuration file to import by clicking **Browse** and navigating to the file's location.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

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 will install 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.

c. 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**.

Kiosk device policy for Samsung SAFE

Sep 06, 2017

You create a Kiosk policy in XenMobile to let you to specify that only a specific app or apps can be used on Samsung SAFE devices. 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.

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 the Connection Scheduling Policy for Android devices, as described in Connection scheduling device policies. This step enables Android devices connect back to XenMobile.

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

Note:

- 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.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Expand **More** and then, under **Security**, click **Kiosk**. The **Kiosk Policy** page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Samsung SAFE Platform** information page appears.

6. Configure these settings:

- **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.

> **Note**: To delete an existing app, 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 **Cancel** to keep the listing.
>
> To edit an existing app, hover over the line containing the listing and then click the pen icon on the right side. Update the listing and then click **Save**. Or, click **Cancel** to leave the listing unchanged.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Launcher configuration device policy for Android

Sep 06, 2017

Citrix Launcher lets you customize the user experience for Android devices deployed by XenMobile. You can add a 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 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, XenMobile installs it, replacing the default Android launcher.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

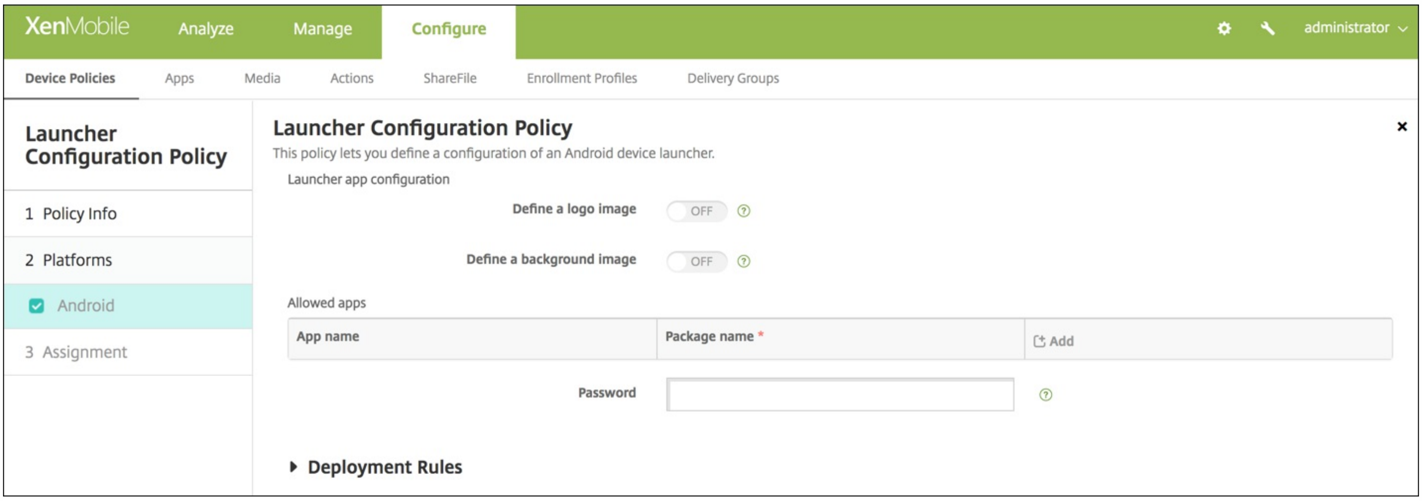
2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Start typing **Launcher** and then select **Launcher Configuration** from the list. The **Launcher Configuration Policy** 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 **Android Platform** information page appears.



Launcher Configuration Policy

This policy lets you define a configuration of an Android device launcher.

Launcher app configuration

Define a logo image: OFF

Define a background image: OFF

Allowed apps

Password:

6. Configure these 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.

    > **Note:** To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.
    >
    > To edit an existing app, hover over the line containing the listing and then click the pen icon on the right side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- **Password**: The password a user must enter to exit Citrix Launcher.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

LDAP device policy

Sep 06, 2017

You create an LDAP policy for iOS devices in XenMobile 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.

iOS settings

macOS settings

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add** to add a policy. The **Add a New Policy** dialog box appears.

3. Expand **More** and then, under **End user**, click **LDAP**. The **LDAP Policy** 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 **Policy Platforms** information 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, refer to Step 7 for how to set the deployment rules.

Configure iOS settings

Configure the following 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 leve**l, or **Subtree** to define how deeply into the LDAP tree to search. The default is **Base**.
    - **Base** searches the node pointed to by 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.

    > **Note**: To delete the search setting, hover over the line containing the listing and click the trash icon on the right side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing.
    >
    > To edit a search setting, hover over the line containing the listing and click the pen icon on the right side. Update the listing and then click **Save**. Or, click **Cancel** to leave the listing unchanged.

- 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.
- 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.

Configure macOS settings

Configure the following 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 leve**l, or **Subtree** to define how deeply into the LDAP tree to search. The default is **Base**.
    - **Base** searches the node pointed to by 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.

    > **Note**: To delete an existing search setting, hover over the line containing the listing and click the trash icon on the right side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.
    >
    > To edit an existing search setting, hover over the line containing the listing and 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.

- 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.
- 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.
- In **Profile scope**, click either **User** or **System**. The default is **User**. This option is available only on macOS 10.7 and later.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Location device policy

Sep 06, 2017

You create location device policies in XenMobile to enforce geographic boundaries. When users breach the defined boundary, also called a *geofence*, XenMobile 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 the Perform Security Actions section in Devices.

You can create location device policies for iOS and Android. Each platform requires a different set of values, which are described in this article.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **Location**. The **Location Policy** information page appears.

4. In the **Policy Information** pane, enter the following information:

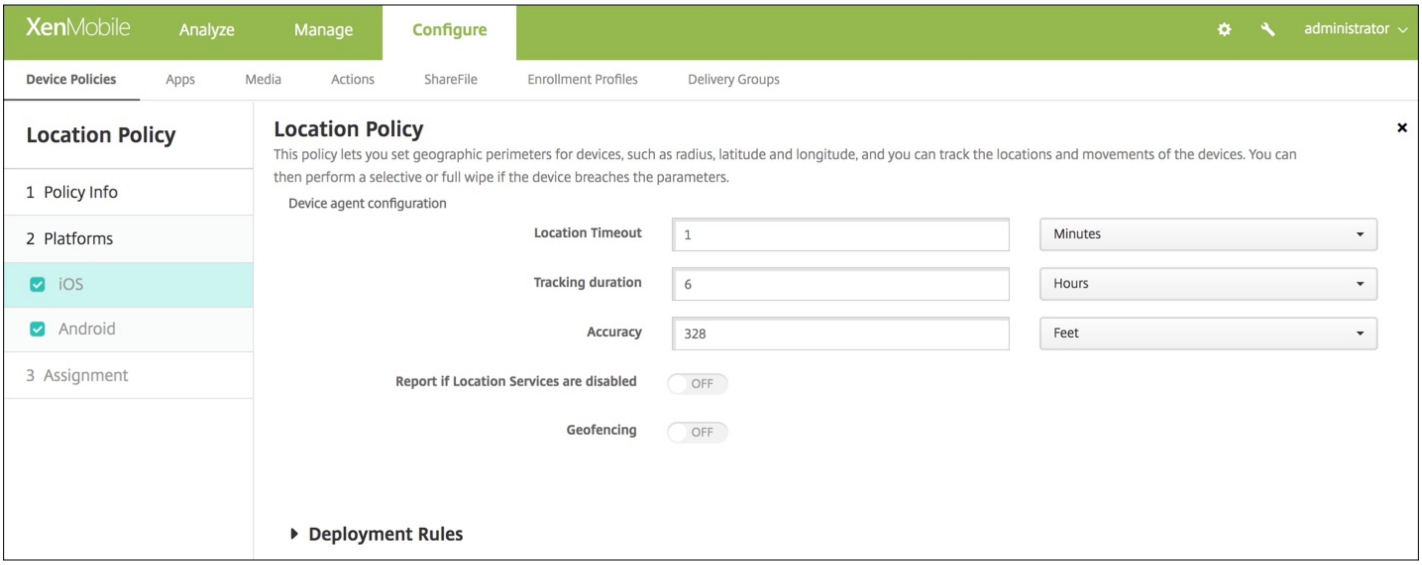
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **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, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS settings



Location Policy

This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.

Device agent configuration

Location Timeout: 1 Minutes

Tracking duration: 6 Hours

Accuracy: 328 Feet

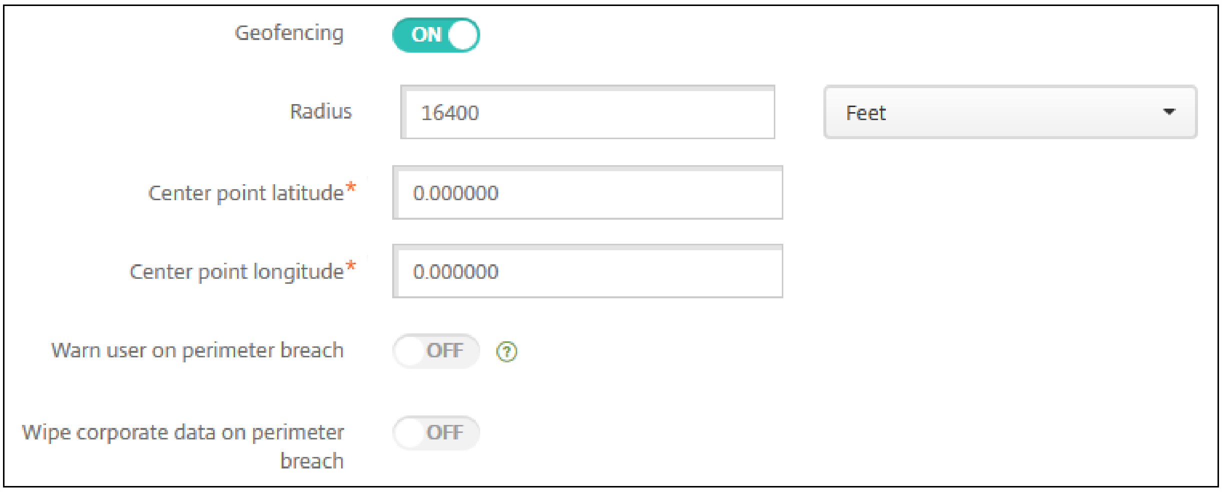
Report if Location Services are disabled: OFF

Geofencing: OFF

Configure these settings:

- **Location timeout**: Type a numeral and then, in the list, click **Seconds** or **Minutes** to set how often XenMobile 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, in the list, click **Hours** or **Minutes** to set how long XenMobile tracks the device. Valid values are 1-6 hours or 10-360 minutes. The default is 6 hours.
- **Accuracy**: Type a numeral and then, in the list, click **Meters**, **Feet**, or **Yards** to set how close to a device XenMobile tracks the device. Valid values are 10-5000 yards or meters, or 30-15000 feet. The default is 328 feet.
- **Report if Location Services are disabled**: Select whether the device sends a report to XenMobile when GPS is disabled. The default is **OFF**.
- **Geofencing**



Geofencing: ON

Radius: 16400 Feet

Center point latitude*: 0.000000

Center point longitude*: 0.000000

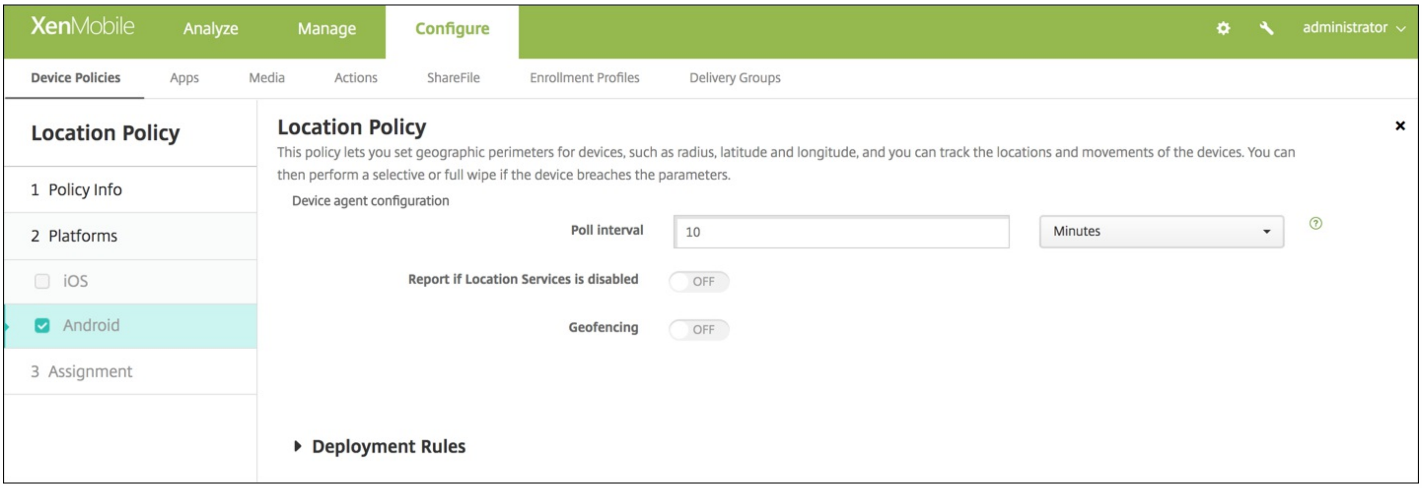
Warn user on perimeter breach: OFF

Wipe corporate data on perimeter breach: OFF

When you enable Geofencing, configure these settings:

- **Radius**: Type a numeral and then, in the list, click the units to be used to measure the radius. The default is 16,400 feet. Valid values for radius are:
  - 164-164000 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 XenMobile 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, in the list, click **Seconds** or **Minutes** to set the length of time to delay before wiping corporate data from users' devices. This gives users an opportunity to return to the allowed location before XenMobile selectively wipes their devices. The default is 0 seconds.

Configure Android settings



Location Policy

This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.

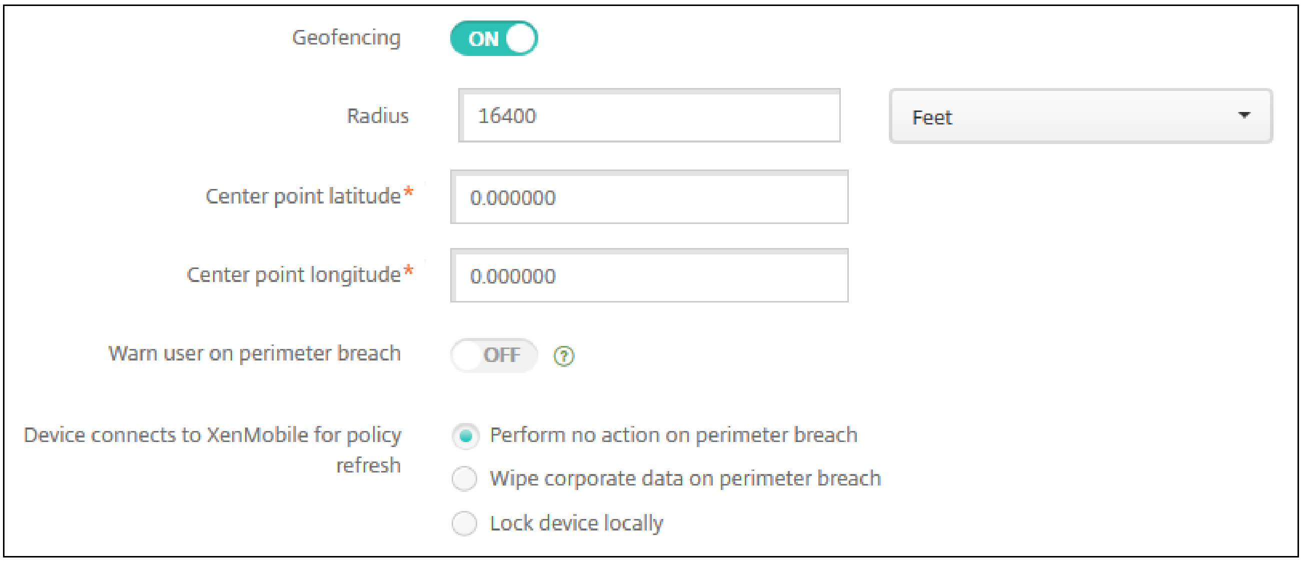
Device agent configuration

Poll interval: 10 Minutes

Report if Location Services is disabled: OFF

Geofencing: OFF

- **Poll interval**: Type a numeral and then, in the list, click **Minutes** or **Hours**, or **Days** to set how often XenMobile 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 may adversely affect the device's battery life.
- **Report if Location Services are disabled**: Select whether the device sends a report to XenMobile when GPS is disabled. The default is **OFF**.
- **Geofencing**



Geofencing: ON

Radius: 16400 Feet

Center point latitude*: 0.000000

Center point longitude*: 0.000000

Warn user on perimeter breach: OFF

Device connects to XenMobile for policy refresh:
● Perform no action on perimeter breach
○ Wipe corporate data on perimeter breach
○ Lock device locally

When you enable Geofencing, configure these settings:

- **Radius**: Type a numeral and then, in the list, click the units to be used to measure the radius. The default is 16,400 feet. 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 XenMobile is required to display the warning message.
- **Device connects to XenMobile 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, in the list, click Seconds or Minutes to set the length of time to delay before wiping corporate data from users' devices. This gives users an opportunity to return to the allowed location before XenMobile selectively wipes their devices. The default is 0 seconds.
  - **Delay on lock**: 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, in the list, click Seconds or Minutes to set the length of time to delay before locking users' devices. This gives users an opportunity to return to the allowed location before XenMobile locks their devices. The default is 0 seconds.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Mail device policy

Sep 06, 2017

You can add a mail device policy in XenMobile to configure an email account on iOS or macOS devices.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add** to add a policy. The **Add a New Policy** dialog box appears.

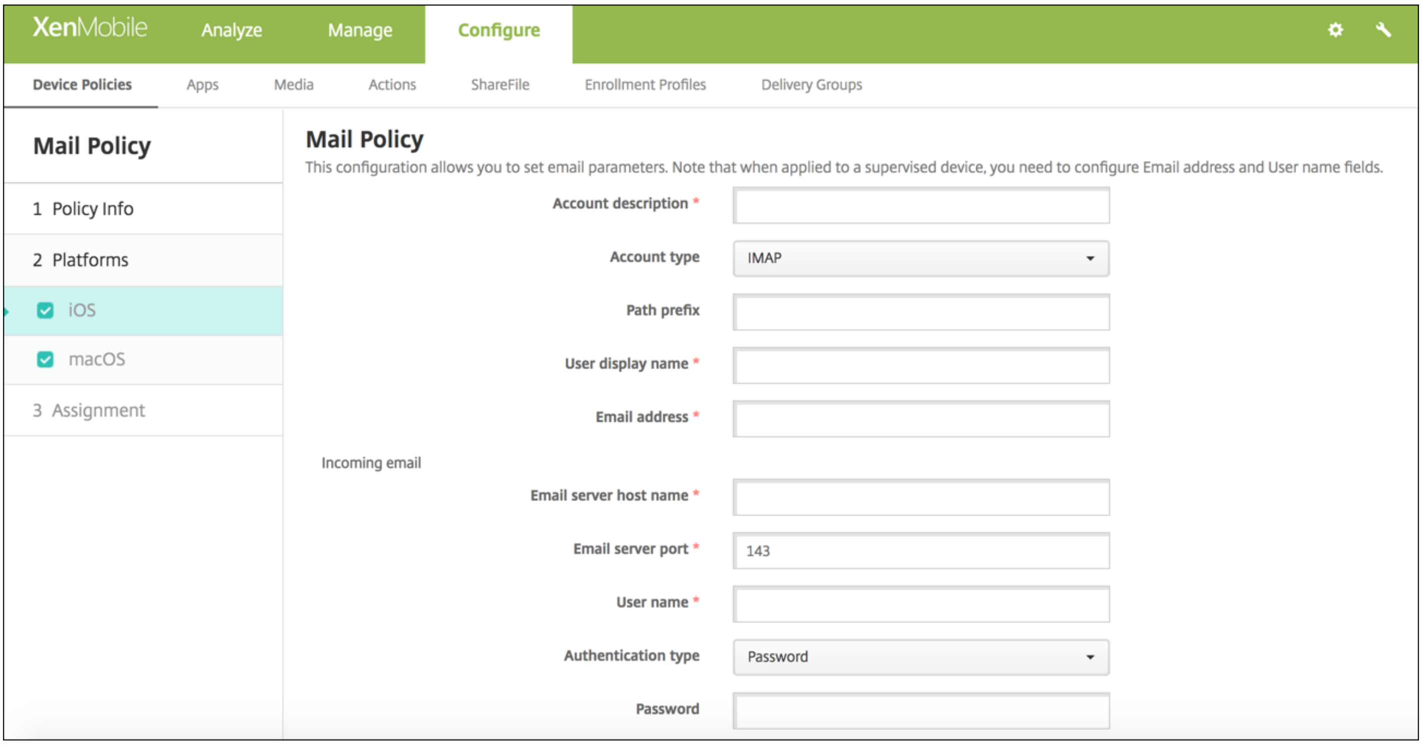
3. Click **More** and then, under **End user**, click **Mail**. The **Mail Policy** page appears.

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 **Mail Policy Platforms** page appears.

6. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the other.



Mail Policy

This configuration allows you to set email parameters. Note that when applied to a supervised device, you need to configure Email address and User name fields.

Account description *

Account type: IMAP

Path prefix

User display name *

Email address *

Incoming email

Email server host name *

Email server port *: 143

User name *

Authentication type: Password

Password

When you finish configuring the settings for a platform, refer to Step 8 for how to set platform deployment rules.

7. Configure the following settings for the platforms you selected.

- **Account description**: Type an account description that appears in the Mail and Settings apps. This field is required.
- **Account type**: Choose either **IMAP** or **POP** to select the protocol to be used for user accounts. The default is **IMAP**. When you select **POP**, the following **Path** prefix option disappears.
- **Path prefix**: Type **INBOX** or your IMAP mail account path prefix. This field is required.
- **User display name**: Type the full user name to be used for messages and other purposes. This field is required.

- **Email address**: Type the full email address for the account. This field is required.
- **Incoming email settings**
  - **Email server host name**: Type the incoming mail server host name or IP address. This field is required.
  - **Email server port**: Type the incoming mail server port number. The default is **143**. This field is required.
  - **User name**: Type the user name for the email account. This name is generally the same as the email address up to the @ character. This field is required.
  - **Authentication type**: Choose the authentication type to be used. The default is **Password**. When **None** is selected, the following **Password** field disappears.
  - **Password**: Type an optional password for the incoming mail server.
  - **Use SSL**: Select whether the incoming mail server uses Secure Socket Layer authentication. The default is **OFF**.
- **Outgoing email settings**
  - **Email server host name**: Type the outgoing mail server host name or IP address. This 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**
  - **Note**: For iOS settings, these options apply only to iOS 5.0 and later. There are no restrictions for macOS.
  - **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**: Select whether this account supports S/MIME authentication and encryption. The default is **OFF**. When set to ON, the following two fields appear.
    - **Signing identity credential**: Choose the signing credential to use.
    - **Encryption identity credential**: Choose the encryption credential to use.
- **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 password.
  - Next to **Profile scope**: Choose either **User** or **System**. The default is **User**. This option is available only on macOS 10.7 and later.

8. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Managed domains device policy

Sep 06, 2017

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 8 and later supervised devices, you specify URLs or subdomains to control how users can open documents, attachments, and downloads from the browser. For iOS 9.3 and later supervised devices, you can specify the 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.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add New Policy** dialog box appears.

3. Expand **More** and then, under **Security**, click **Managed domains**. The **Managed Domains Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **iOS Platform** page appears.

How to specify domains

6. Configure these 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.

      Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

      To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel**.

- **Policy Settings**
  - 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.
  - 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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

MDM options device policy

Oct 26, 2017

You can create a device policy in XenMobile to manage Find My Phone/iPad Activation Lock on supervised iOS 7.0 and later phone 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 XenMobile MDM Options device policy. You can then manage a device from the XenMobile 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 XenMobile 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 XenMobile console.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

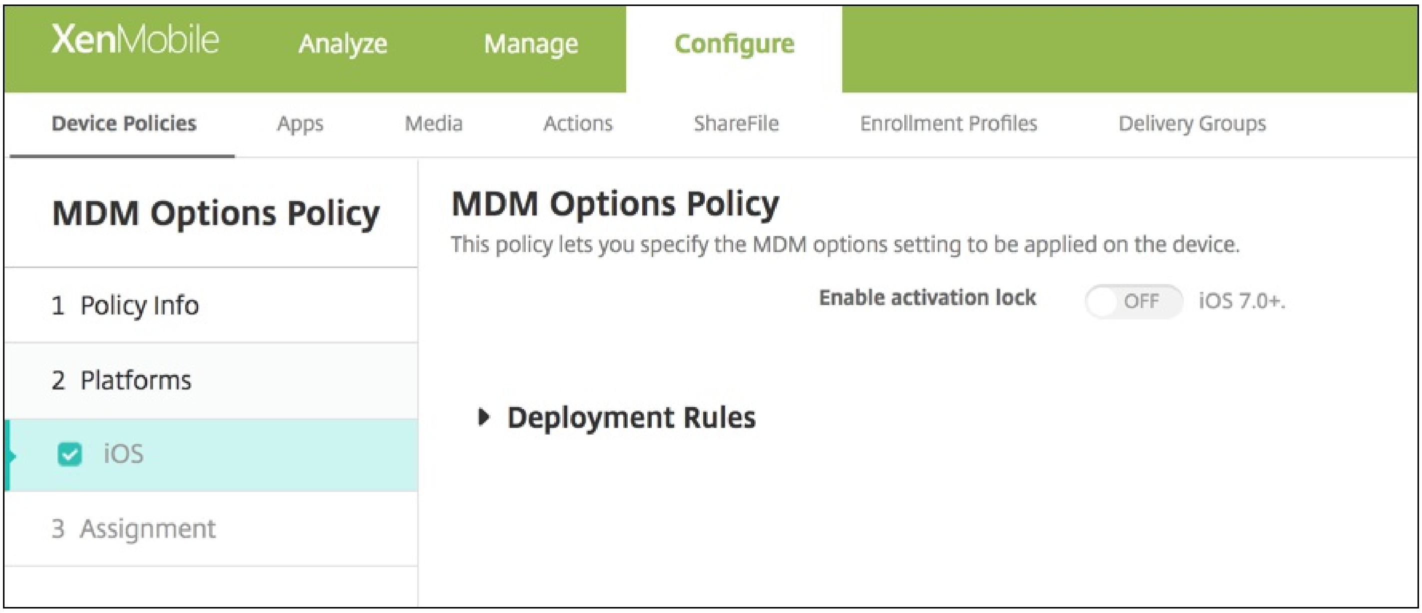
2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Expand **More** and then, under **End user**, click **MDM Options**. The **MDM Options Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **iOS MDM Policy Platform** page appears.



MDM Options Policy

This policy lets you specify the MDM options setting to be applied on the device.

Enable activation lock OFF iOS 7.0+.

6. Configure this setting:

- **Enable Activation Lock**: Select whether to enable Activation Lock on the devices to which you deploy this policy. The default is **OFF**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

After you enable Activation Lock by deploying the MDM options device policy: The Security action A**ctivation 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 in the Security actions article.

Organization information device policy

Sep 06, 2017

You can add a device policy in XenMobile to specify your organization's information for alert messages that are pushed from XenMobile to iOS devices. The policy is available for iOS 7 and later devices.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More** and then, under **End user**, click **Organization info**. The **Organization Info Policy** page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: If desired, type a description of the policy.

5. Click **Next**. The **iOS Platform Information** page appears.

Configure these settings:

- **Name**: Type the name of the organization running XenMobile.
- **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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Passcode device policy

Oct 13, 2017

You create a passcode policy in XenMobile 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 for Work, Windows Phone, and Windows desktop/tablet. Each platform requires a different set of values, which are described in this article.

iOS settings

macOS settings

Android settings

Samsung KNOX settings

Android for Work settings

Windows Phone settings

Windows Desktop/Tablet settings

1. In the XenMobile 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:

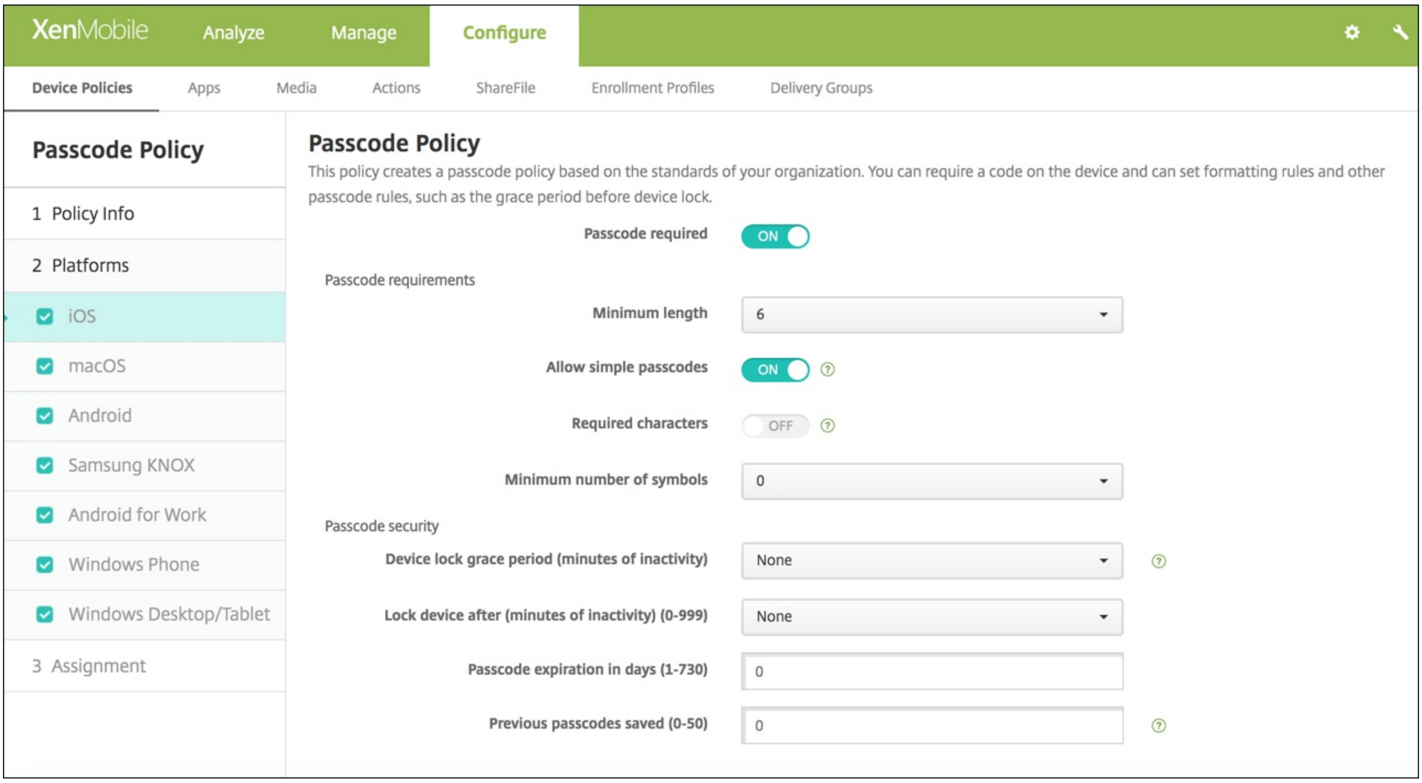
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

5. Click **Next**. The **Platforms** page appears.

6. Under **Platforms**, select 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, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS settings



Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode required: ON

Passcode requirements

Minimum length: 6

Allow simple passcodes: ON

Required characters: OFF

Minimum number of symbols: 0

Passcode security

Device lock grace period (minutes of inactivity): None

Lock device after (minutes of inactivity) (0-999): None

Passcode expiration in days (1-730): 0

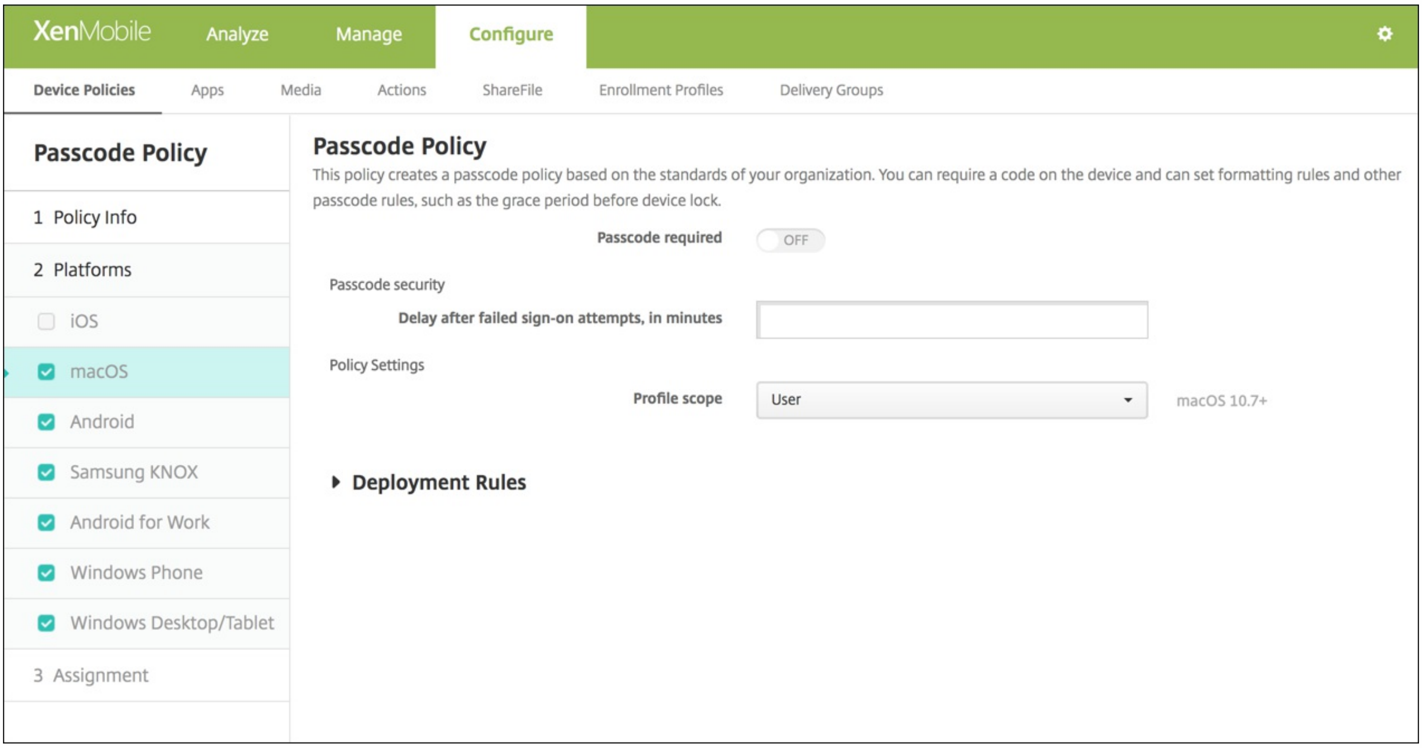
Previous passcodes saved (0-50): 0

Configure the following 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.
  - 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.

Configure macOS settings



Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode required: OFF

Passcode security

Delay after failed sign-on attempts, in minutes:

Policy Settings

Profile scope: User — macOS 10.7+

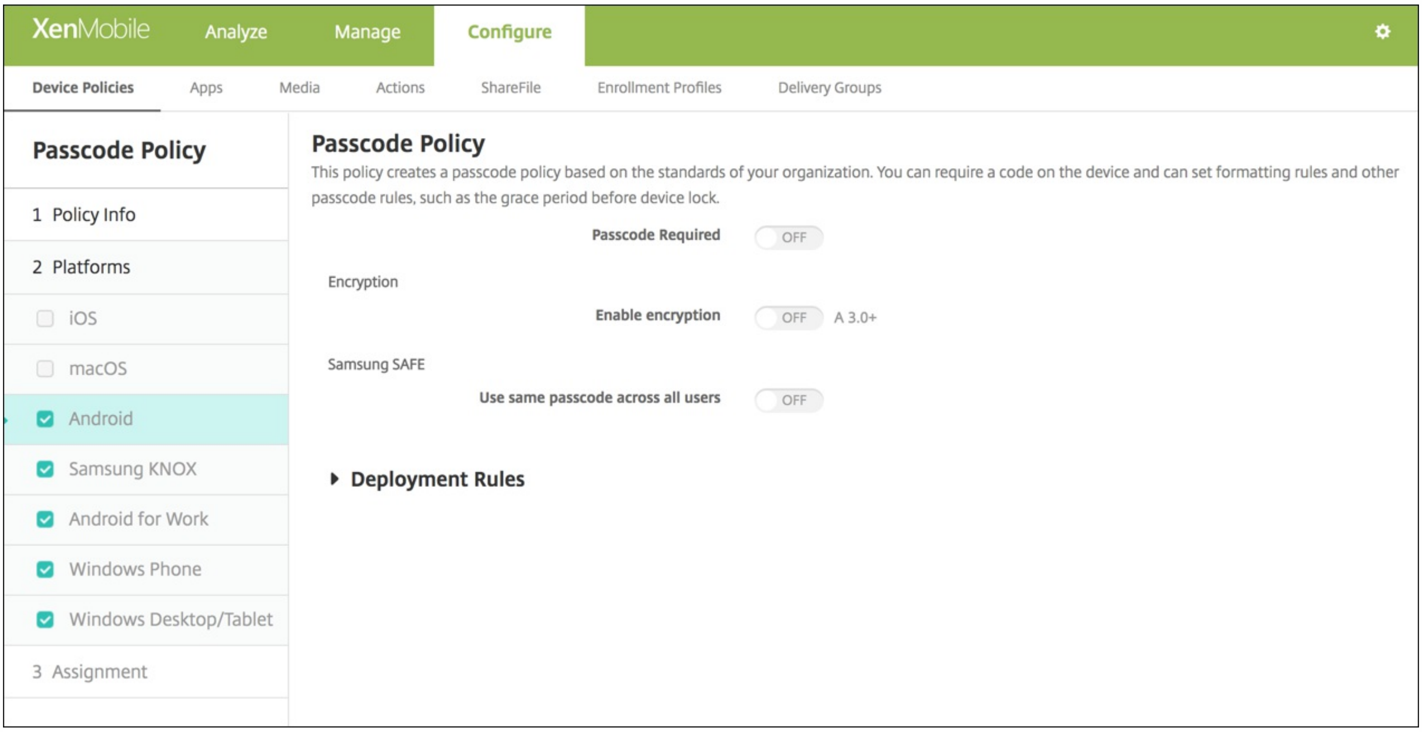
Configure these settings:

- **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.

Configure Android settings



Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode Required OFF

Encryption

Enable encryption OFF A 3.0+

Samsung SAFE

Use same passcode across all users OFF

Configure these settings:

Note: The default setting for Android is **OFF**.

- **Passcode required**: Select this option to require a passcode and to display the configuration options for an Android passcode device policy. The page expands to let you configure settings for passcode requirements, passcode security, 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. This option is available for Android 3.0 and later.

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. This option is available for Android 3.0 and later. The option is available regardless of the **Passcode required** setting.

    > **Note**: 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**
  - **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 authenicate using a fingerprint.
      - **Allow iris**. Select to allow users to authenicate 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

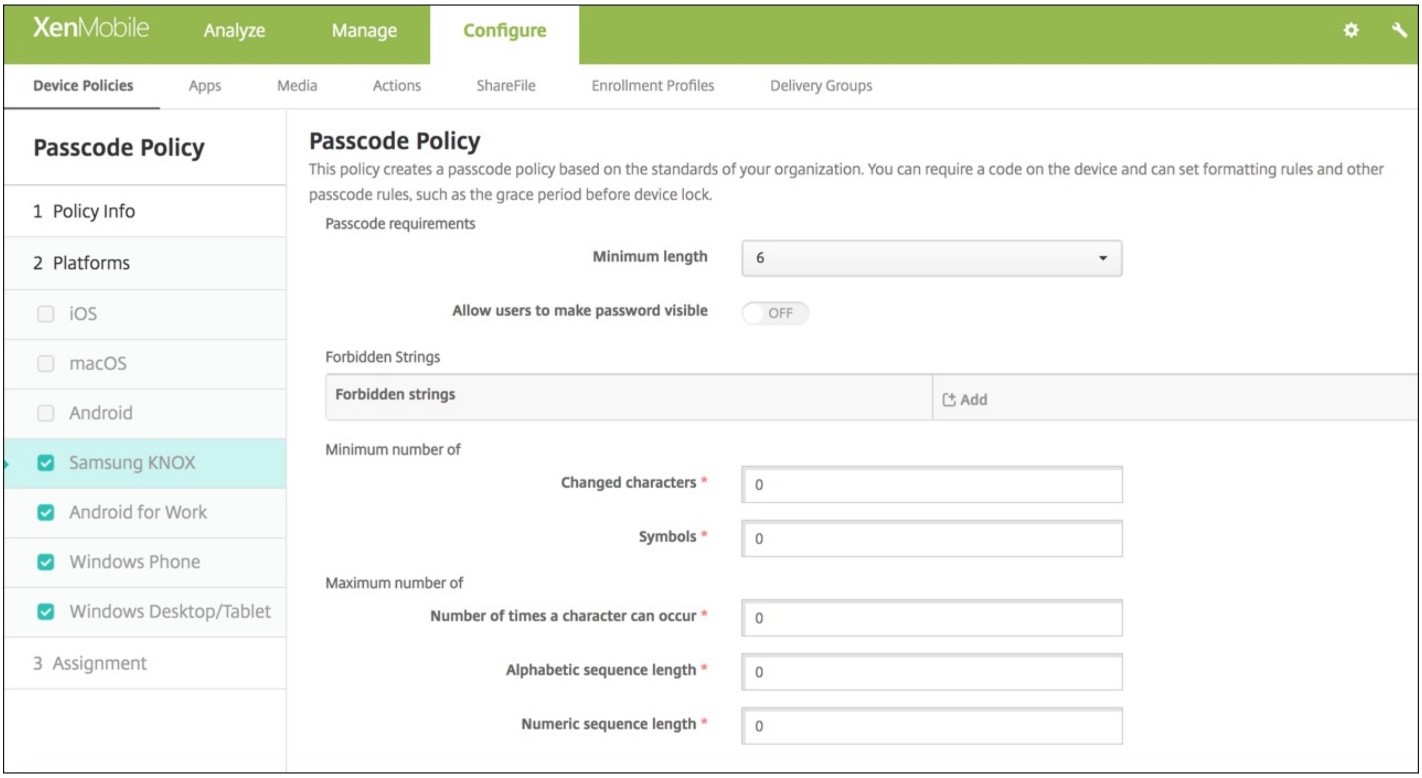
then do the following:

- **Forbidden strings**: Type the string users may not use.
- Click **Save** to add the string or click **Cancel** to cancel adding the string.

  Note: To delete an existing string, hover over the line containing the listing and click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

  To edit an existing string, hover over the line containing the listing and click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure Samsung KNOX settings



Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode requirements

Minimum length: 6

Allow users to make password visible: OFF

Forbidden Strings

Forbidden strings | Add

Minimum number of

Changed characters *: 0

Symbols *: 0

Maximum number of

Number of times a character can occur *: 0

Alphabetic sequence length *: 0

Numeric sequence length *: 0

Configure these settings:

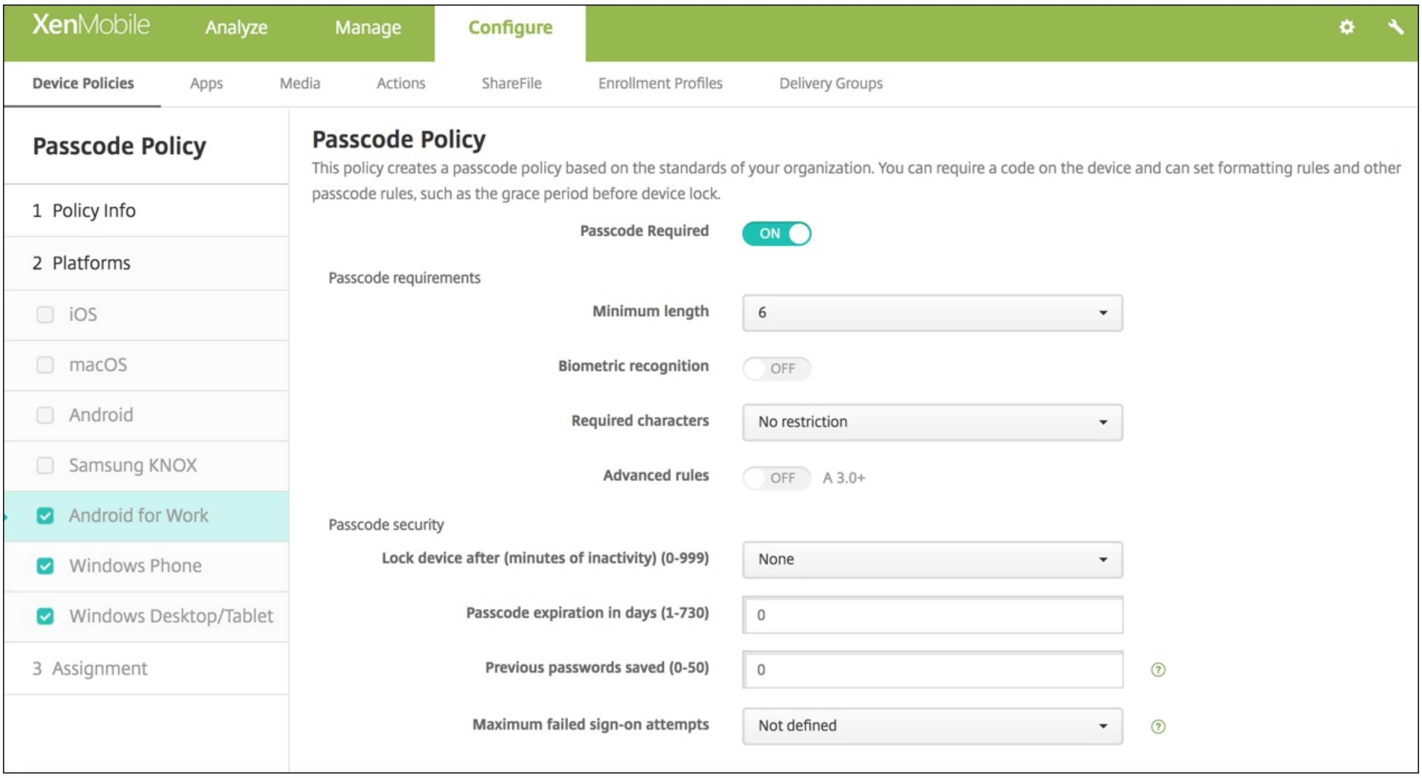
- **Passcode requirements**
  - **Minimum length**: In the list, click the minimum passcode length. The default is **6**.
  - **Allow users to make password visible**: Select whether to let users make the password visible.
  - **Forbidden strings**: You create forbidden strings to prevent users from 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.

      Note: To delete an existing string, hover over the line containing the listing and click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

To edit an existing string, hover over the line containing the listing and click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- **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**.
  - **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**.

Configure Android for Work settings



Passcode Policy

1 Policy Info

2 Platforms

□ iOS

□ macOS

□ Android

□ Samsung KNOX

☑ Android for Work

☑ Windows Phone

☑ Windows Desktop/Tablet

3 Assignment

Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode Required: ON

Passcode requirements

Minimum length: 6

Biometric recognition: OFF

Required characters: No restriction

Advanced rules: OFF A 3.0+

Passcode security

Lock device after (minutes of inactivity) (0-999): None

Passcode expiration in days (1-730): 0

Previous passwords saved (0-50): 0

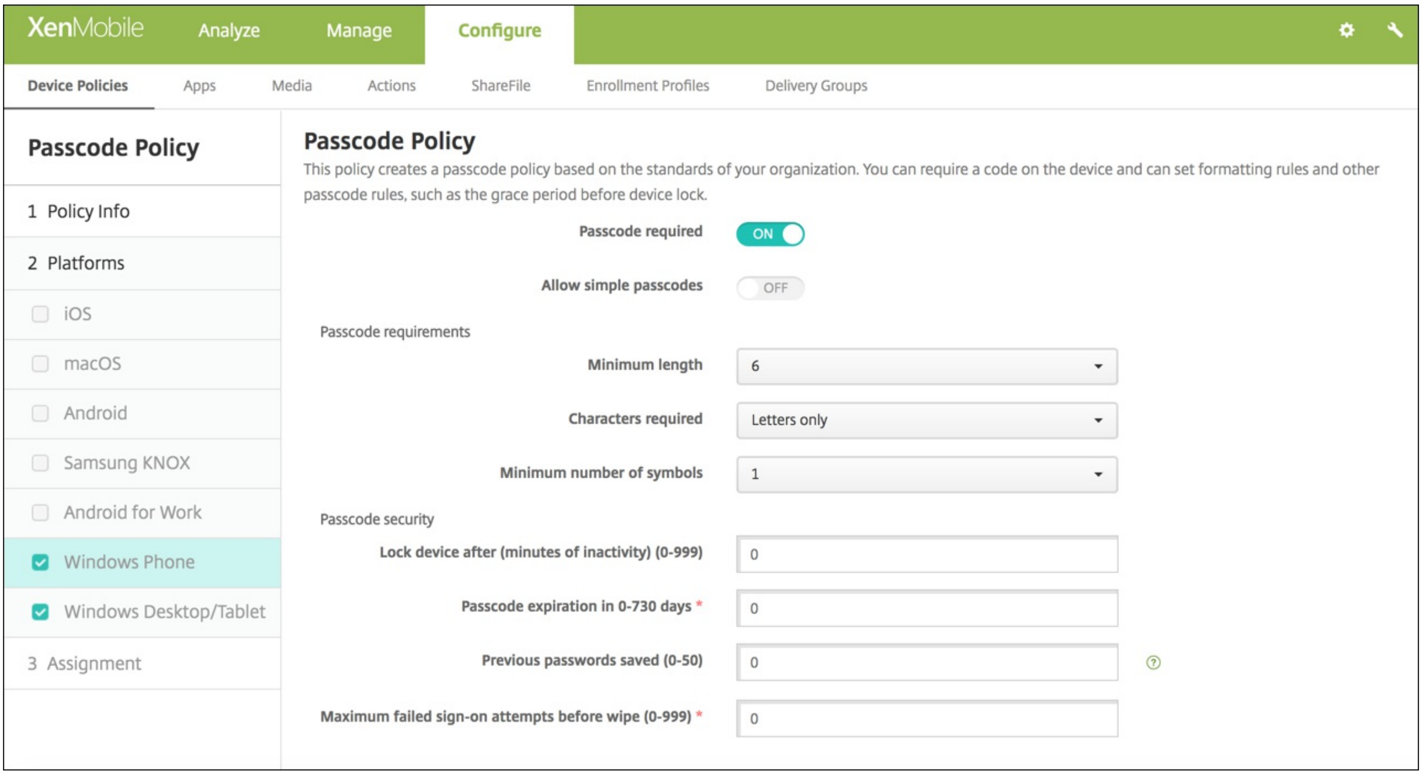
Maximum failed sign-on attempts: Not defined

Configure these settings:

- **Passcode required**: Select this option to require a passcode and to display the configuration options for an Android for Work passcode device policy. The page expands to let you configure settings for passcode requirements and passcode security.
- **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**. Note that this feature is not currently supported.
  - **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. This option is not available for Android devices earlier than Android 5.0. 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 number of minutes 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 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**.

Configure Windows Phone settings



Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode required: ON

Allow simple passcodes: OFF

Passcode requirements

Minimum length: 6

Characters required: Letters only

Minimum number of symbols: 1

Passcode security

Lock device after (minutes of inactivity) (0-999): 0

Passcode expiration in 0-730 days *: 0

Previous passwords saved (0-50): 0

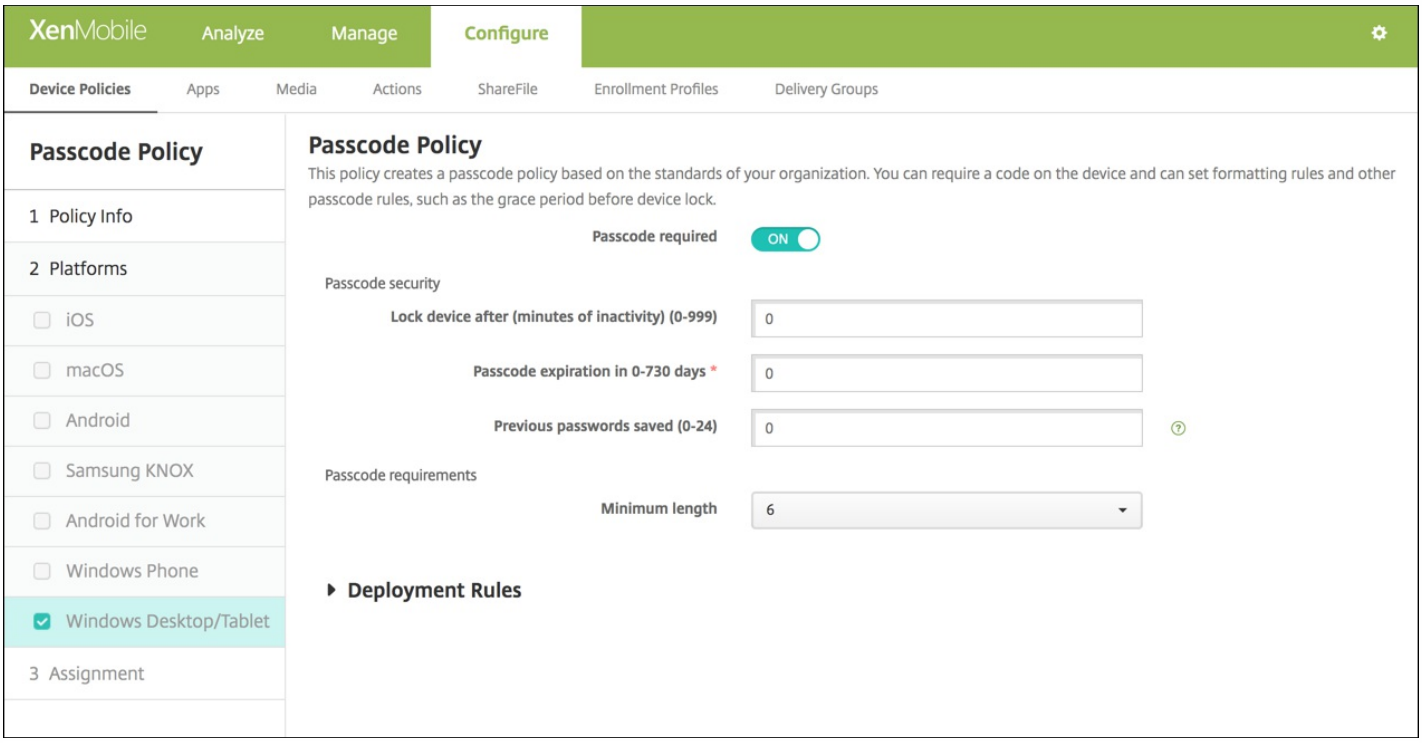
Maximum failed sign-on attempts before wipe (0-999) *: 0

Configure these 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 alphanumeric**, **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**.

Configure Windows Desktop/Tablet settings



Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode required: ON

Passcode security

Lock device after (minutes of inactivity) (0-999): 0

Passcode expiration in 0-730 days *: 0

Previous passwords saved (0-24): 0

Passcode requirements

Minimum length: 6

Configure these settings:

- **Disallow convenience logon**: Select whether to allow users to access their devices with picture passwords or biometric logons. The default is **OFF**.
- **Minimum passcode length**: In the list, click the minimum passcode length. The default is **6**.
- **Maximum passcode attempts before wipe**: In the list, click the number of times a user can fail to sign in successfully after which corporate data is wiped from the device. The default is **4**.
- **Passcode expiration in days (0-730)**: Type the number of days after which the passcode expires. Valid values are 0-730. The default is **0**, which means the passcode never expires.
- **Passcode history: (1-24)**: 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**.
- **Maximum inactivity before device lock in minutes (1-999)**: Type the length of time in minutes that a device can be inactive before it is locked. Valid values are 1-999. You must enter a number between 1 and 999 in this field. The default is **0**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Personal hotspot device policy

Sep 06, 2017

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. Available on iOS 7.0 and later.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** page appears.

3. Expand **More**, and then under **Network Access**, click **Personal Hotspot**. The **Personal Hotspot 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 **iOS Platform** information page appears.

6. Configure this setting:

- **Disable personal hotspot**: Select whether to disable the personal hotspot functionality on users' devices. The default is **OFF**, which switches off the personal hotspot on users devices. This policy does not disable the functionality; users can still use the personal hotspot on their devices, but when the policy is deployed, the personal hotspot is turned off so that it doesn't remain on by default.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Profile Removal device policy

Sep 06, 2017

You can create an app profile removal device policy in XenMobile. The policy, when deployed, removes the app profile from users' iOS or macOS devices.

1. In the XenMobile console, click **Configure > Device Policies**. The Device Policies page appears.

2. Click **Add**. The **Add New Policy** dialog box appears.

3. Expand **More** and then, under **Removal**, click **Profile Removal**. The **Profile Removal Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

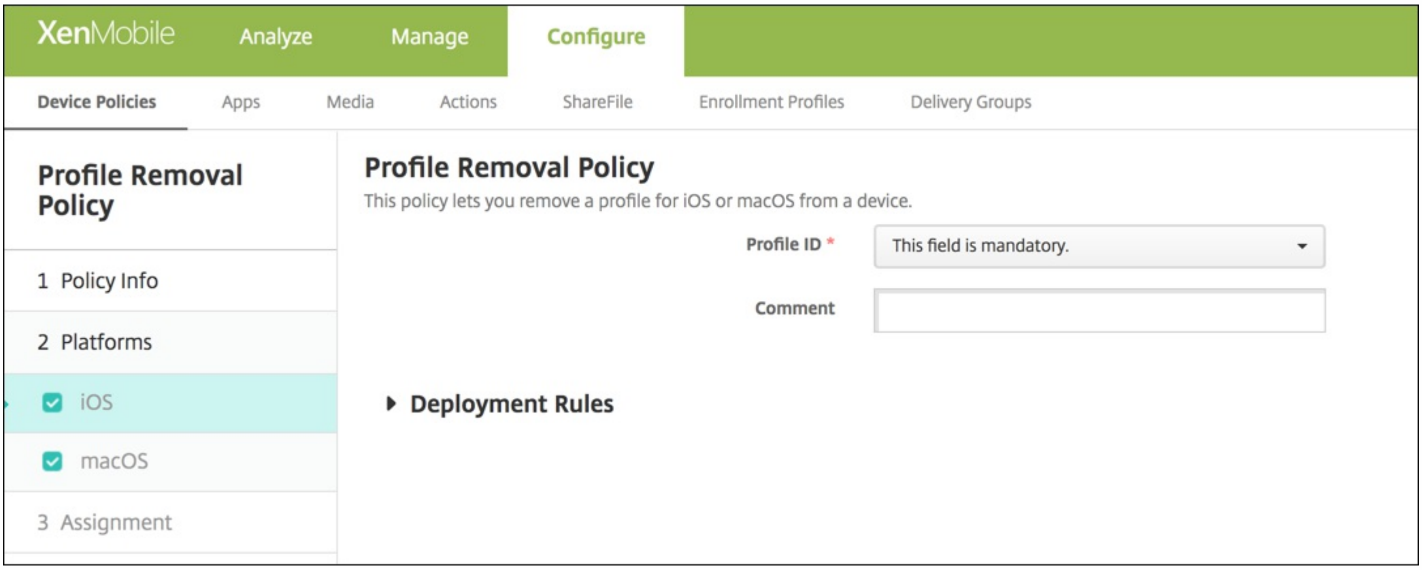
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **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, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS setting



Profile Removal Policy

This policy lets you remove a profile for iOS or macOS from a device.

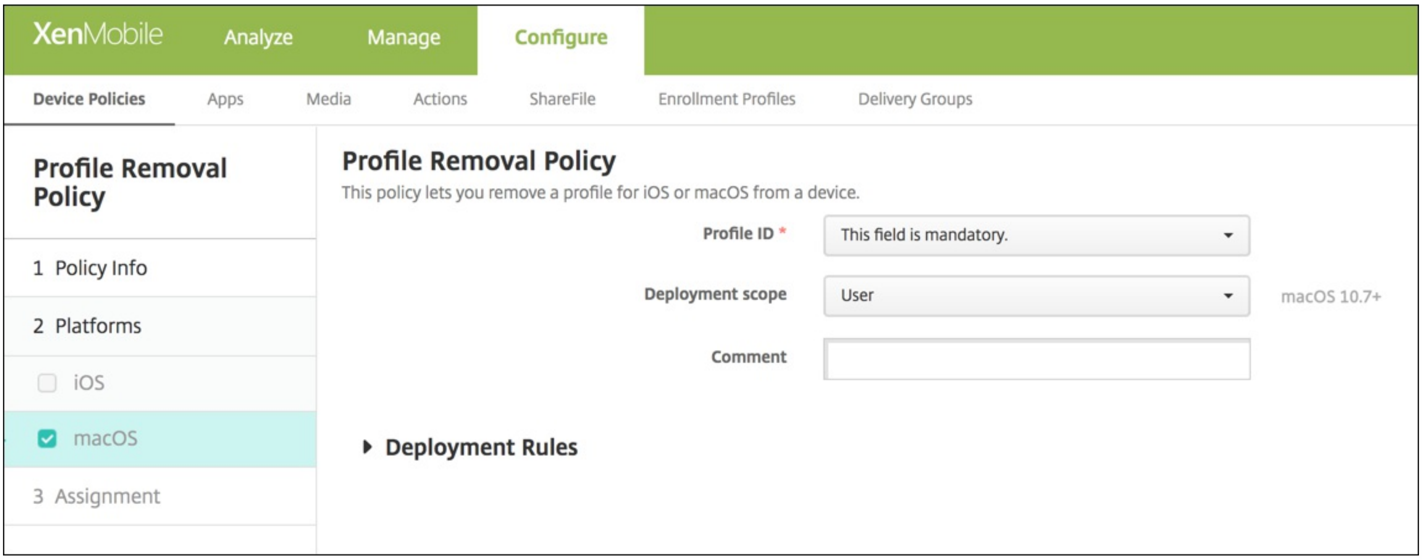
Profile ID * This field is mandatory.

Comment

Configure these settings:

- **Profile ID**: In the list, click the app profile ID. This field is required.
- **Comment**: Type an optional comment.

Configure macOS settings



Profile Removal Policy

This policy lets you remove a profile for iOS or macOS from a device.

Profile ID *: This field is mandatory.

Deployment scope: User — macOS 10.7+

Comment:

Configure these 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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Provisioning profile device policy

Sep 06, 2017

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 XenMobile 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 Creating Provisioning Profiles on the Apple Developer site.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

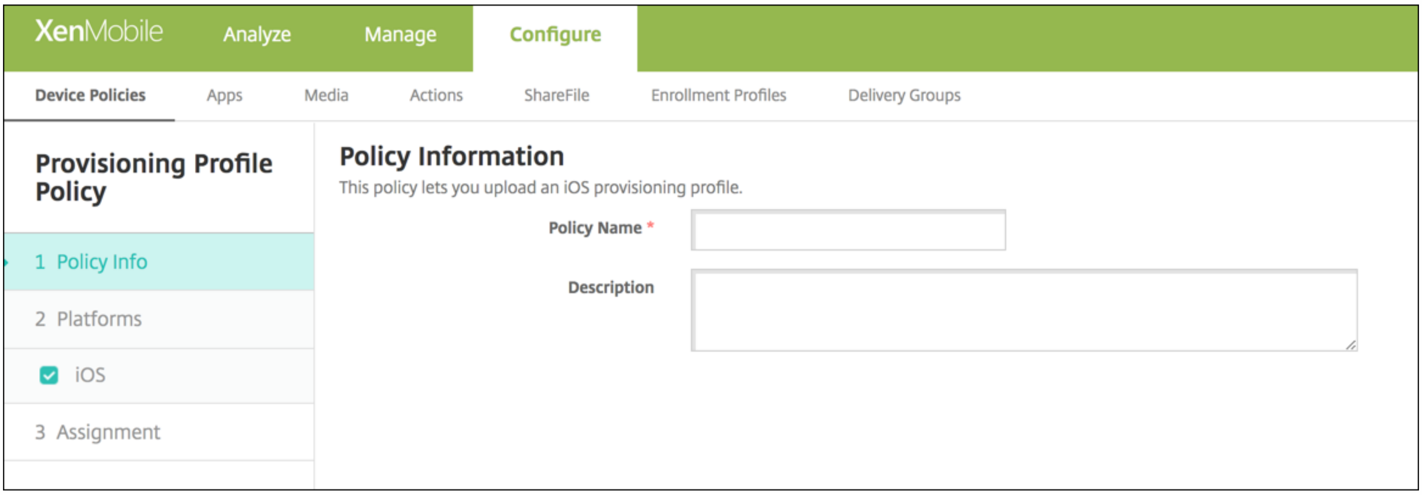
2. Click **Add**. The **Add a New Policy** page appears.

3. Expand **More** and then, under **Apps**, click **Provisioning Profile**. The **Provisioning Profile 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 **iOS Platform** information page appears.



Policy Information

This policy lets you upload an iOS provisioning profile.

Policy Name *

Description

6. Configure this setiing:

- **iOS provisioning profile**: Select the provisioning profile file to import by clicking **Browse** and then navigating to the file's location.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Provisioning profile removal device policy

Sep 06, 2017

You can remove iOS provisioning profiles with device policies. For more information on provisioning profiles, see adding a provisioning profile.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** page appears.

3. Expand **More** and then, under **Removal**, click **Provisioning Profile removal**. The **Provisioning Profile Removal 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 **iOS Platform** page appears.

6. Configure these settings:

- **iOS provisioning profile**: In the list, click the provisioning profile you want to remove.
- **Comment**: Optionally, add a comment.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Proxy device policy

Sep 06, 2017

You can add a device policy in XenMobile to specify global HTTP proxy settings for devices running Windows Mobile/CE andiOS 6.0 or later. 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.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appear

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More** and then, under **Network access**, click **Proxy**. The **Proxy Policy** page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Enter a descriptive name for the policy.
- **Description**: Optionally, enter a description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS settings

Configure these 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.
    - **User name**: Type an optional user name to authenticate to the proxy server.
    - **Password**: Type an optional password to authenticate to the proxy server.
  - If you click **Automatic**, configure these settings:
    - **Proxy PAC URL**: Type 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**. This option is available only on iOS 7.0 and later.
- **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.
  - 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.

Configure Windows Mobile/CE settings

Configure these 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**.
- **User name**: 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**.

7. Configure the deployment rules

8. Click **Next**. The **Proxy Policy** assignment page appears.

9. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand **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**. If you choose **OFF**, no other options need to be configured.
- 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.
- 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**, which does not apply to iOS.

11. Click **Save**.

Registry device policy

Sep 06, 2017

The Windows Mobile/CE registry stores data about apps, drivers, user preferences, and configuration settings. In XenMobile, you can define the registry keys and values that let you administer Windows Mobile/CE devices.

1. In the XenMobile 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 **Custom**, click **Registry**. The **Registry Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Windows Mobile/CE Platform** page appears.

6. Configure these 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\Microsoft\Windows* 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** to not save the registry key information.

  Note: To delete an existing registry key, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

  To edit an existing registry key, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Remote support device policy

Nov 29, 2017

> ### Note
>
> For on-premises XenMobile Server deployments: Remote support enables your help desk representatives to take remote control of managed Windows CE and Android mobile devices. Screen cast is supported on Samsung KNOX devices only.
>
> Remote support isn't available to XenMobile Service customers and isn't supported for clustered on-premises XenMobile Server deployments.
>
> For more information, see Support options and Remote Support.

You create a remote support policy in XenMobile to give you remote access to supported Windows and Android devices. You can configure two types of support:

- **Basic**, which lets you view diagnostic information about the device, such as system information, processes that are running, task manager (memory and CPU usage), installed software folder contents, and so on.
- **Premium**, which lets you remotely control the device's screen, including control over colors (in either the main window, or in a separate, floating window), the ability to establish a Voice-over-IP session (VoIP) between the help desk and the user, to configure settings, and to establish a chat session between the help desk and the user.

Note: To implement this policy, you must do the following:

- Install the XenMobile Remote Support app in your environment.
- Configure a remote support app tunnel. For details, see App tunneling device policies.
- Configure a Samsung KNOX remote support device policy as described in this topic.
- Deploy both the app tunnel remote support policy and the Samsung KNOX remote support policy to user devices.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

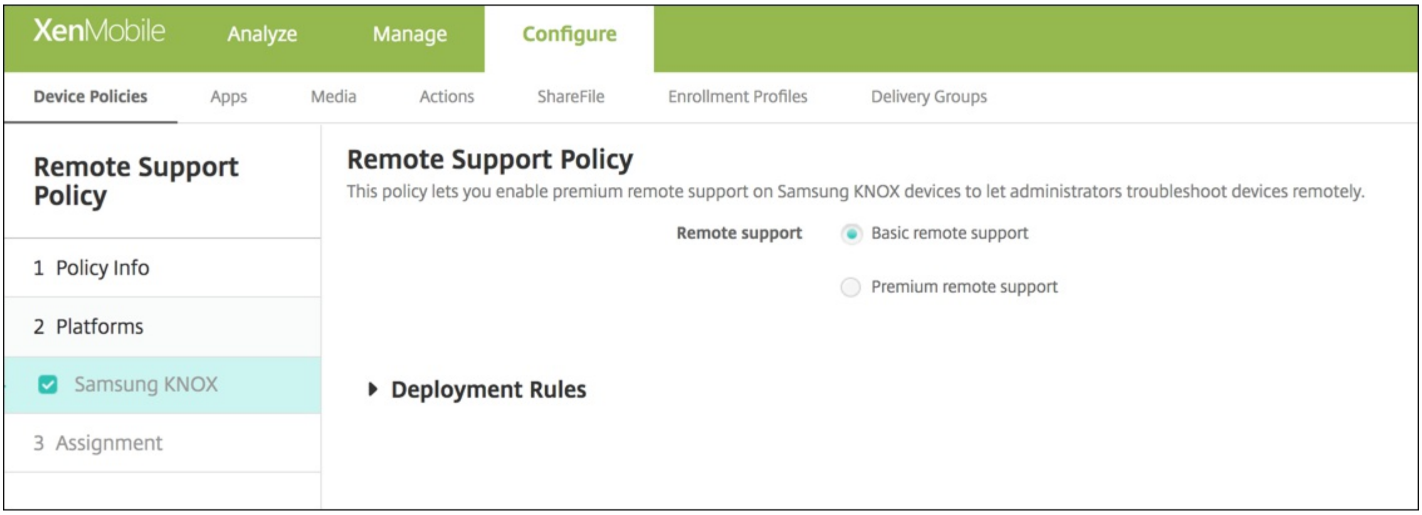
2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Start typing **Remote Support** and then click **Remote Support**. The **Remote Support Policy** 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 **Samsung KNOX** platform information page appears.



Remote Support Policy

This policy lets you enable premium remote support on Samsung KNOX devices to let administrators troubleshoot devices remotely.

Remote support ● Basic remote support
○ Premium remote support

6. Configure this setting:

- **Remote support**: Select **Basic remote support** or **Premium remote support**. The default is **Basic remote support**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Restrictions device policy

Feb 02, 2018

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*. The main exceptions are the iOS Security - Force feature and all Windows Tablet features, which default to **OFF**, or *restricts*.

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.
- **Screen shots**. If **ON**, the user can take screen shots on their device. If **OFF**, the user cannot take screen shots on their device.

> ## 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.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** page appears.

3. Click **Restrictions**. The restrictions **Policy information** page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

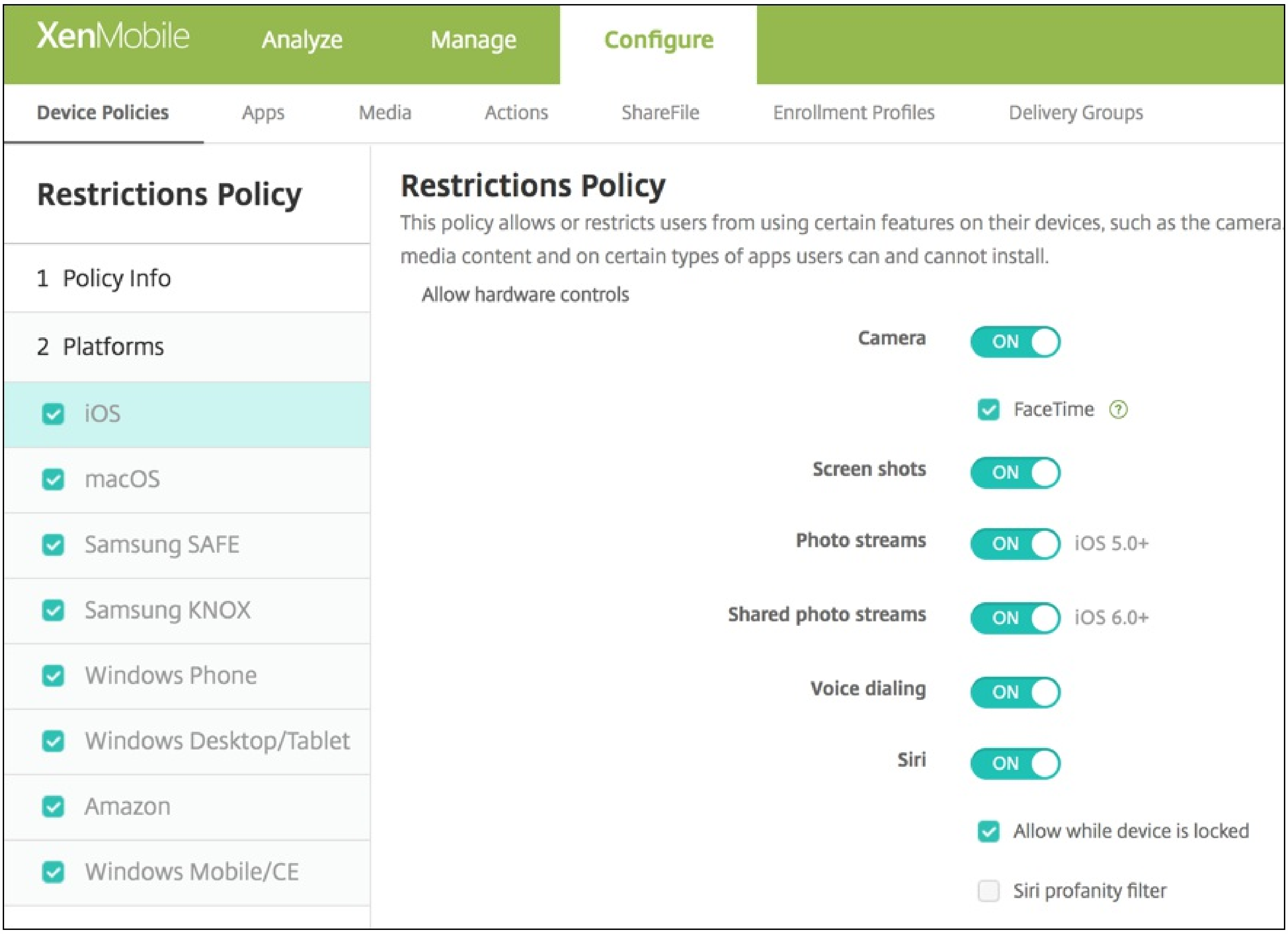
4. Click **Next**. The **Policy Platforms** page appears.

5. Under **Platforms**, select the platform or platforms you want to add. You can then change the policy information for each platform you selected. Click to restrict any of the features in the following sections, which changes the setting to **OFF**. Unless otherwise noted, the default setting is to enable the feature.

If you selected:
iOS
macOS
Samsung SAFE
Samsung KNOX
Windows Phone and Windows Desktop/Tablet
Amazon
Windows Mobile/CE

When you finish setting the restrictions for a platform, refer to Step 7 later in this article for how to set that platform's deployment rules.

iOS



Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera media content and on certain types of apps users can and cannot install.

Allow hardware controls

Camera ON

☑ FaceTime

Screen shots ON

Photo streams ON iOS 5.0+

Shared photo streams ON iOS 6.0+

Voice dialing ON

Siri ON

☑ Allow while device is locked

□ Siri profanity filter

iOS settings

Note: Some of the iOS restrictions options apply only to specific versions of iOS (and, where applicable, these versions are noted on the XenMobile console page). For example, the capability to allow or block AirDrop is only supported on devices running iOS 7 and later. The capability to allow or block Photo streams is supported on devices running iOS 5 and later. Also, some options only apply if the device is placed in supervised mode. 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.

- **Allow hardware controls**
  - **Camera**: Allow users to use the camera on their devices.
    - **FaceTime**: Allow users to use FaceTime on their devices. This restriction is deprecated on unsupervised iOS 10 devices.
  - **Screen shots**: Allow users to take screen shots on their devices.
  - **Photo streams**: Allow users to use MyPhotoStream to share photos through iCloud to all their iOS devices (iOS 5.0 and later).
  - **Shared photo streams**: Allow users to use iCloud Photo Sharing to share photos with coworkers, friends, and family (iOS 6.0 and later).
  - **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. This restriction is deprecated on unsupervised iOS 10 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. This restriction is deprecated on unsupervised iOS 10 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 (iOS 5.0 and later).
  - **Safari**: Allow users to access Safari. This restriction is deprecated on unsupervised iOS 10 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 (iOS 5.0 and later). This restriction is deprecated on unsupervised iOS 10 devices.
  - **iCloud backup**: Allow users to back up their devices to iCloud (iOS 5.0 and later).
  - **iCloud keychain**: Allow users to store passwords, WiFi network, credit card, and other information in the iCloud Keychain (iOS 7.0 and later).
  - **Cloud photo library**: Allow users to access their iCloud photo library (iOS 9.0 and later).
- **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 (iOS 7.0 and later).
  - **Passcode on first Airplay pairing**: Require that AirPlay-enabled devices are verified with a one-time onscreen code before they can use AirPlay (iOS 7.0 and later).
  - **Paired Apple Watch to use Wrist Detection**: Require a paired Apple Watch to use **Wrist Detection** (iOS 8.2 and later).
  - **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 (iOS 9.0 and later).
- **Security - Allow**
  - **Accepting untrusted SSL certificates**: Allow users to accept web sites' untrusted SSL certificates (iOS 5.0 and later).
  - **Automatic update to certificate trust settings**: Allow trusted certificates to be updated automatically (iOS 7.0 and later).
  - **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 (iOS 7.0 and later).
  - **Passbook notifications when locked**: Allow Passbook notifications to appear on the lock screen (iOS 6.0 and later).
  - **Handoff**: Allow users to transfer activities from one iOS device to another nearby iOS device (iOS 8.0 and later).
  - **iCloud sync for managed apps**: Allow users to sync managed apps to iCloud (iOS 8.0 and later).
  - **Backup for enterprise books**: Allow enterprise books to be backed up to iCloud (iOS 8.0 and later).
  - **Notes and highlights sync for enterprise books**: Allow notes and highlights users have added to enterprise books to be synced to iCloud (iOS 8.0 and later).
  - **Enterprise app trust**: Allow enterprise applications to be trusted (iOS 9.0 and later).
  - **Internet results in Spotlight**: Allow Spotlight to show search results from the Internet as well as the device (iOS 8.0 and

later).

- **Supervised only settings - Allow**

  These settings apply only to supervised devices. For the steps on setting an iOS device to supervised mode, see 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 (iOS 8.0 and later).
  - **Configuring restrictions**: Allow users to configure parental controls on their devices (iOS 8.0 and later).
  - **Podcasts**: Allow users to download and sync podcasts (iOS 8.0 and later).
  - **Installing configuration profiles**: Allow users to install a configuration profile other than that the one deployed by you (iOS 6.0 and later).
  - **Fingerprint modification**: Allow users to change or delete their Touch ID fingerprint (iOS 8.3 and later).
  - **Installing apps from device:** (iOS 9.0 and later).
  - **Keyboard shortcuts**: Allow users to create custom keyboard shortcuts for words or phrases that they use often (iOS 9.0 and later).
  - **Paired Apple watch**: Allow users to pair an Apple Watch to a supervised device (iOS 9.0 and later).
  - **Passcode modification**: Allow users to change the passcode on a supervised device (iOS 9.0 and later).
  - **Device name modification**: Allow users to change the name of their device.
  - **Wallpaper modification**: Allow user to change the wallpaper on their devices (iOS 9.0 and later).
  - **Automatically downloading apps**(iOS 9.0 and later).
  - **AirDrop**: Allow users to share photos, videos, websites, locations, and more with nearby iOS devices (iOS 7.0 and later).
  - **iMessage**: Allow users to text over Wi-Fi with iMessage (iOS 6.0 and later).
  - **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. (iOS 7.0 and later).
  - **iBooks**: Allow users to use the iBooks app (iOS 6.0 and later).
  - **Removing apps**: Allow users to remove apps from their devices (iOS 7.0 and later).
  - **Game Center**: Allow users to play online games through Game Center on their devices (iOS 6.0 and later).
    - **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 (iOS 7.0 and later).
  - **Modifying app cellular data settings**: Allow users to modify how apps use cellular data (iOS 7.0 and later).
  - **Modifying Find My Friends settings**: Allow users to change their Find My Friends settings (iOS 7.0 and later).
  - **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 (iOS 7.0 and later).
  - **Predictive keyboards**: Allow user devices to use the predictive keyboard for suggesting words as they type (iOS 8.1.3 and later). 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 (iOS 8.1.3 and later). 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 (iOS 8.1.3 and later). 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 (iOS 8.1.3 and later). 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 one or more apps, click **Add** and do the following:

    a. **App name**: Enter an app name.
    b. Click **Save** or **Cancel**.
    c. Repeat steps a and b for each app you want to add.

    Tip: To delete an existing app, hover over the line containing the app name and then click the trashcan icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

  To edit an existing app, hover over the line containing the app name and then click the pen icon on the right-hand side.

  - **News:** Allow users to use the News app (iOS 9.0 and later).
  - **Apple Music service**: Allow users to use the Apple Music service (iOS 9.3 and later). If you don't allow Apple Music service, the Music app runs in classic mode.
  - **iTunes Radio**: Allow users to use iTunes Radio (iOS 9.3 and later).
  - **Notifications modification**: Allow users to modify notification settings (iOS 9.3 and later).
  - **Restricted App usage**: Allow users to use all apps or to use or not use apps, based on the bundle IDs you provide (iOS 9.3 and later). Applies only to supervised devices.

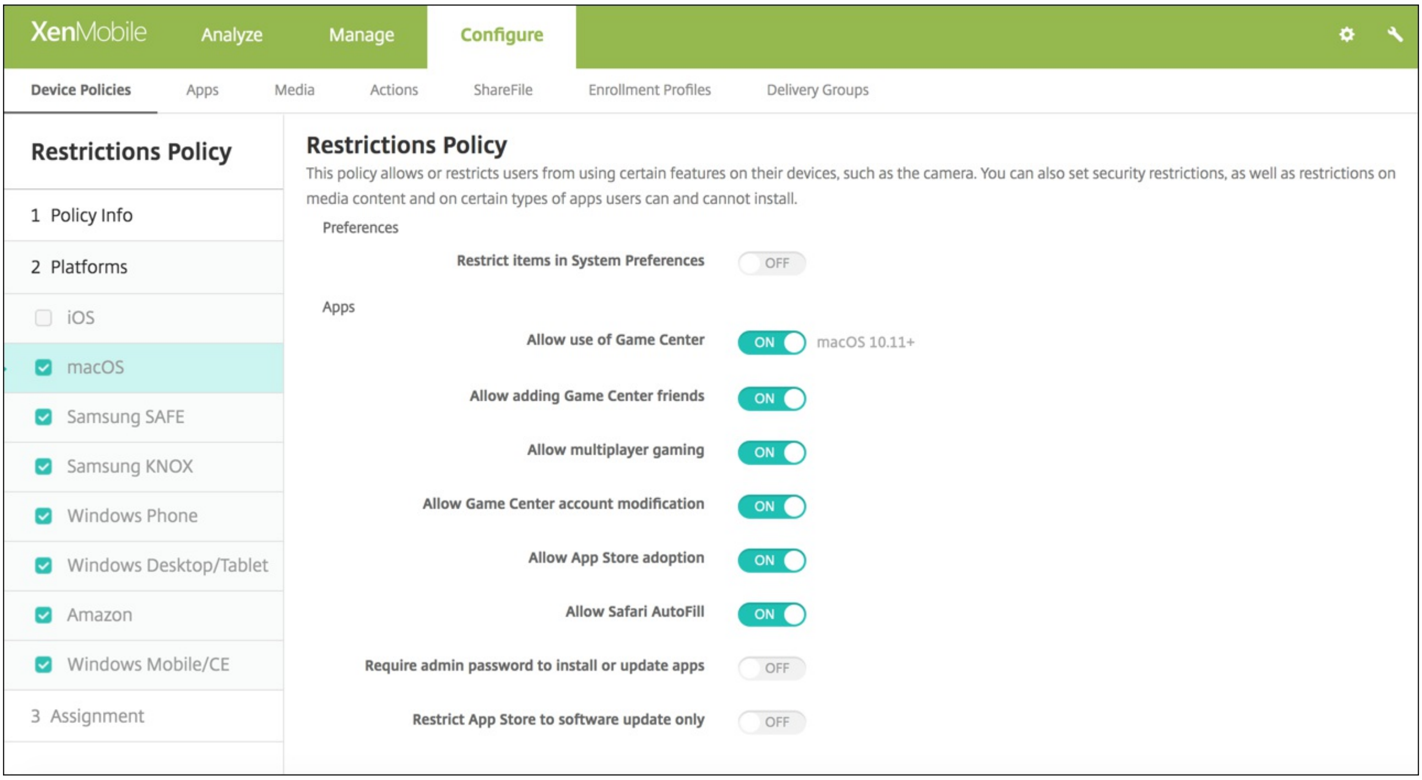
    After you configure the Restrictions device policy to block some apps and then deploy the policy: If you later want to allow some or all of those apps, changing and deploying the Restrictions device policy doesn't change the restrictions. In this case, iOS doesn't apply the changes to the iOS profile. 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 DEP 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.

- **Diagnostic submission modification**: Allow users to modify the diagnostic submission and app analytics settings in the Diagnostics & Usage pane in Settings (iOS 9.3.2 and later).
- **Bluetooth modification**: Allow users to modify Bluetooth settings (iOS 10.0 and later).
- **Allow Dictation**: Supervised only. If this restriction is set to **OFF**, dictation input is not allowed. The default setting is **ON**. For iOS 10..3 and later.
- **Force WiFi white listing**: 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**. For iOS 10.3 and later.

- **Security - Show in lock screen**
  - **Control Center**: Allow access to Control Center on the lock screen, which lets users easily modify Airplane Mode, WiFi, Bluetooth, Do Not Disturb Mode, and Lock Rotation settings (iOS 7.0 and later).
  - **Notification**: Allow notifications on the lock screen (iOS 7.0 and later).
  - **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 (iOS 6.0 and later).
  - **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 Allow all movies.
  - **TV Shows**: Set whether TV shows are allowed on users' devices. If TV shows are allowed, optionally set the ratings level for TV shows. In the list, click an option to allow or restrict TV shows on the device. The default is Allow all TV Shows.
  - **Apps**: Set whether apps are allowed on users' devices. If apps are allowed, optionally set the ratings level for apps. In the list, click an option to allow or restrict apps on the device. The default is Allow all apps.
- **Policy Settings**
  - 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.

macOS



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.

Preferences

Restrict items in System Preferences: OFF

Apps

Allow use of Game Center: ON macOS 10.11+

Allow adding Game Center friends: ON

Allow multiplayer gaming: ON

Allow Game Center account modification: ON

Allow App Store adoption: ON

Allow Safari AutoFill: ON

Require admin password to install or update apps: OFF

Restrict App Store to software update only: OFF

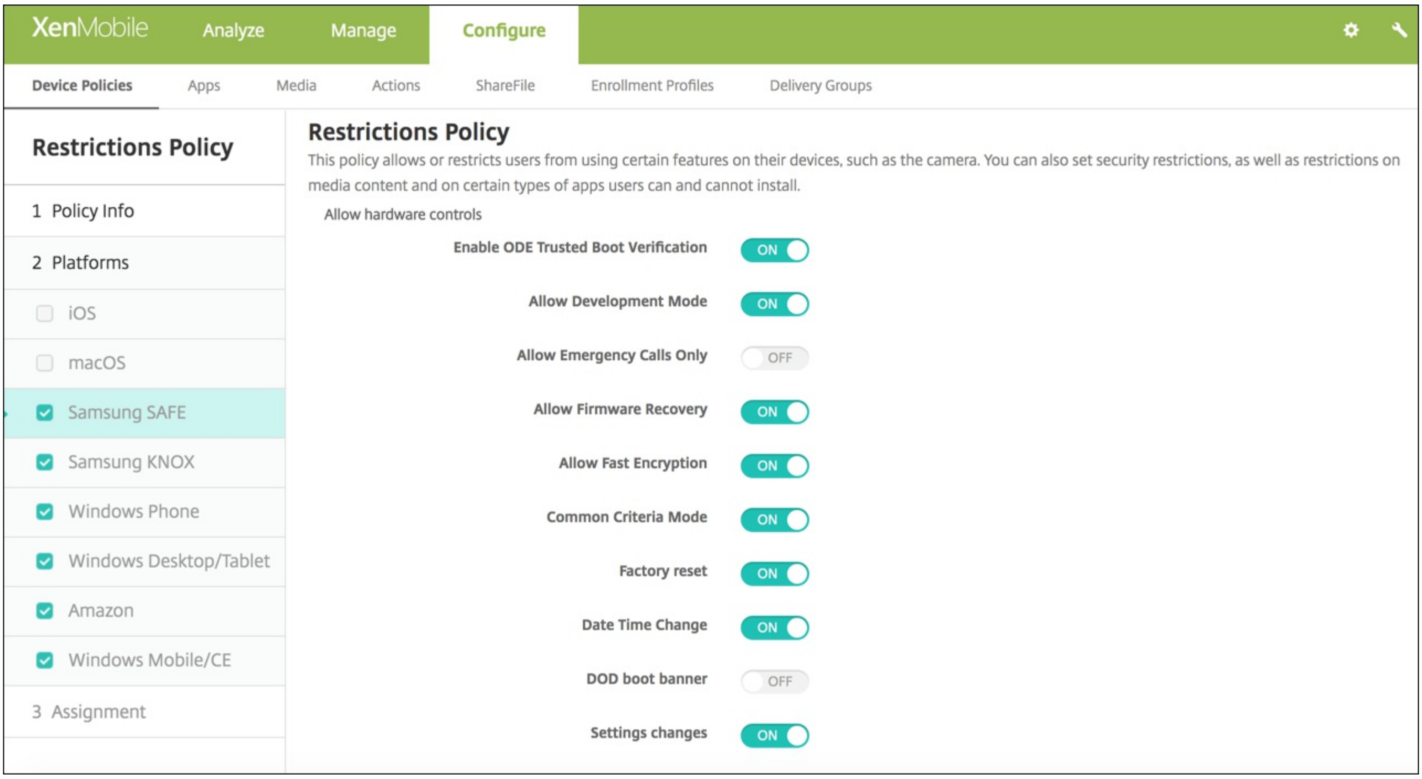
macOS settings

- **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 apps that preexist in OS X to be adopted by the App Store. 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, web sites, 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. For more information about Spotlight Suggestions, see Apple's Spotlight Suggestions page.
    - **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 means that user will 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. For more information, see Apple's iCloud documents and Data page.
        - **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 http://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**.
- **Policy Setting**
    - 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.
    - In the **Profile Scope** list, click **User** or **System** (macOS 10.7 and later).

Samsung SAFE



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 hardware controls

Enable ODE Trusted Boot Verification: ON

Allow Development Mode: ON

Allow Emergency Calls Only: OFF

Allow Firmware Recovery: ON

Allow Fast Encryption: ON

Common Criteria Mode: ON

Factory reset: ON

Date Time Change: ON

DOD boot banner: OFF

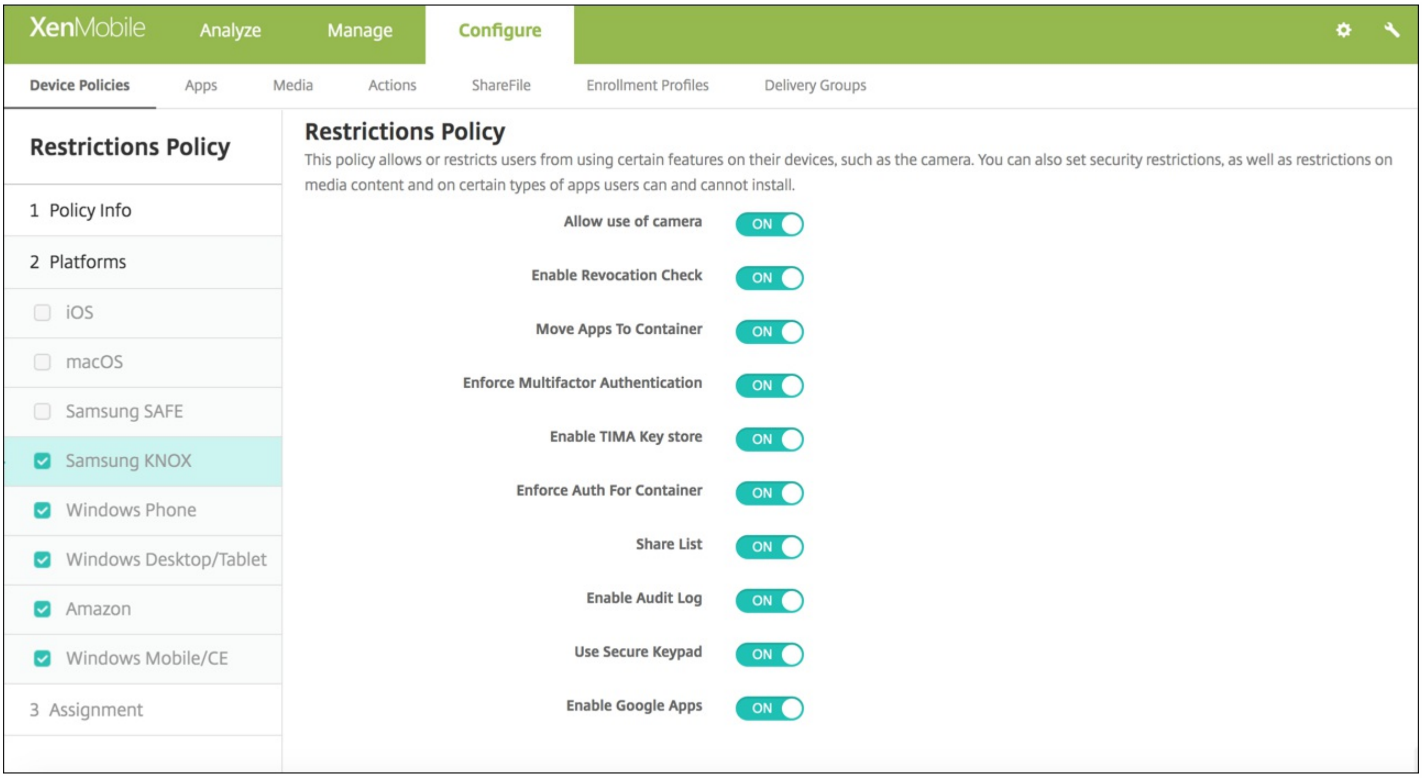
Settings changes: ON

Samsung SAFE settings

Note: Some options are available only under specific Samsung Mobile Device Management APIs; they 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.
  - **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 (Near Field Communication) 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 screen shots 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 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.
    - **Stop system app**: Allow users to disable pre-installed system apps (MDM 4.0 and later).
- **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 WiFi networks.
        - **Tethering**: Allow users to share a mobile data connection with another device using their WiFi connection.
        - **Direct**: Allow users to connect directly to another device through their WiFi connection (MDM 4.0 and later).
        - **State Change**: Allow apps to change WiFi connectivity state.
        - **User Policy Changes**: Allow users to change WiFi policies. If not selected, users can change only the WiFi user name and password. If selected, users can change all WiFi 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 web pages, 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.



Restrictions Policy

1 Policy Info

2 Platforms

□ iOS

□ macOS

□ Samsung SAFE

☑ Samsung KNOX

☑ Windows Phone

☑ Windows Desktop/Tablet

☑ Amazon

☑ Windows Mobile/CE

3 Assignment

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: ON

Enable Revocation Check: ON

Move Apps To Container: ON

Enforce Multifactor Authentication: ON

Enable TIMA Key store: ON

Enforce Auth For Container: ON

Share List: ON

Enable Audit Log: ON

Use Secure Keypad: ON

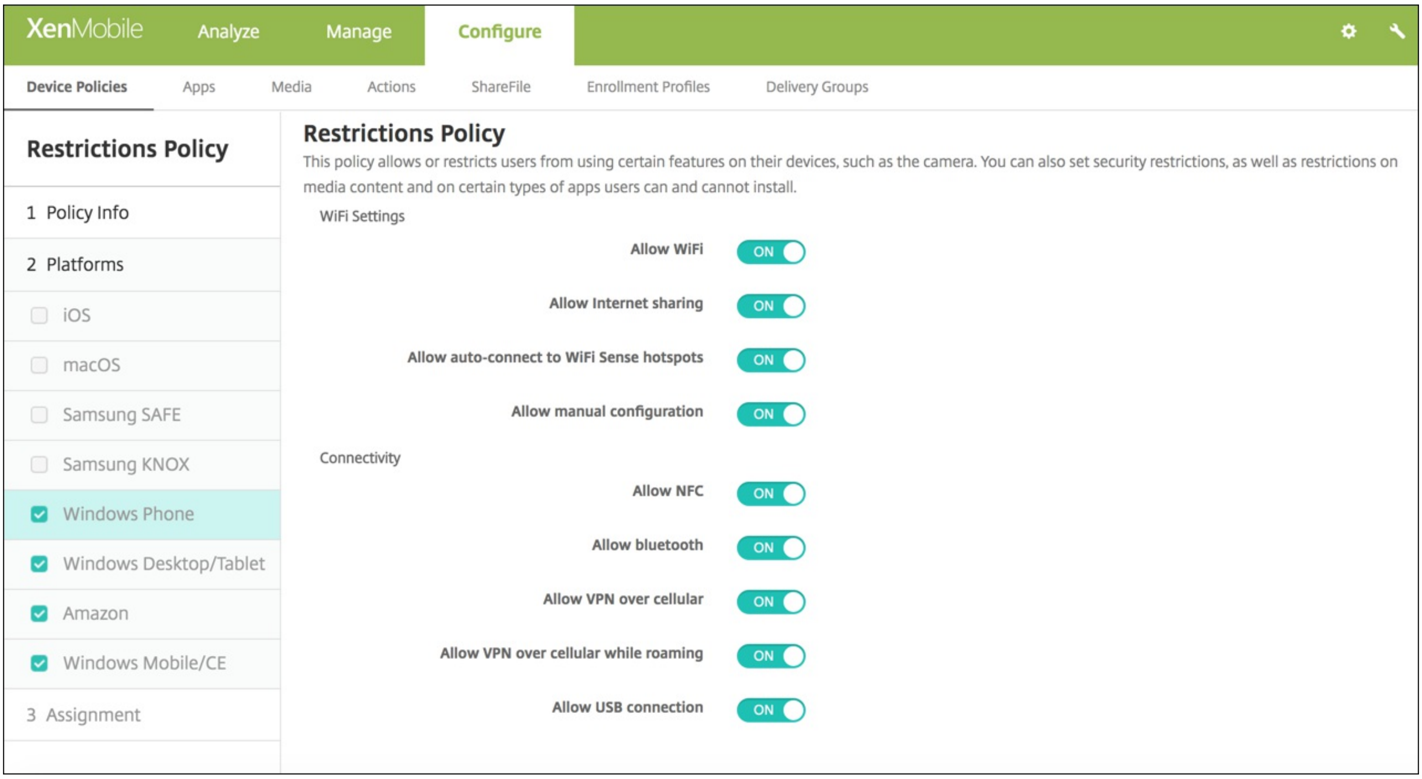
Enable Google Apps: ON

Samsung KNOX settings

Note: These options are available only under Samsung KNOX Premium (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 separate, and different, authentication to open the KNOX container from that used to unlock the device.
- **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.

Windows Phone and Windows Desktop/Tablet



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.

WiFi Settings

Allow WiFi: ON

Allow Internet sharing: ON

Allow auto-connect to WiFi Sense hotspots: ON

Allow manual configuration: ON

Connectivity

Allow NFC: ON

Allow bluetooth: ON

Allow VPN over cellular: ON

Allow VPN over cellular while roaming: ON

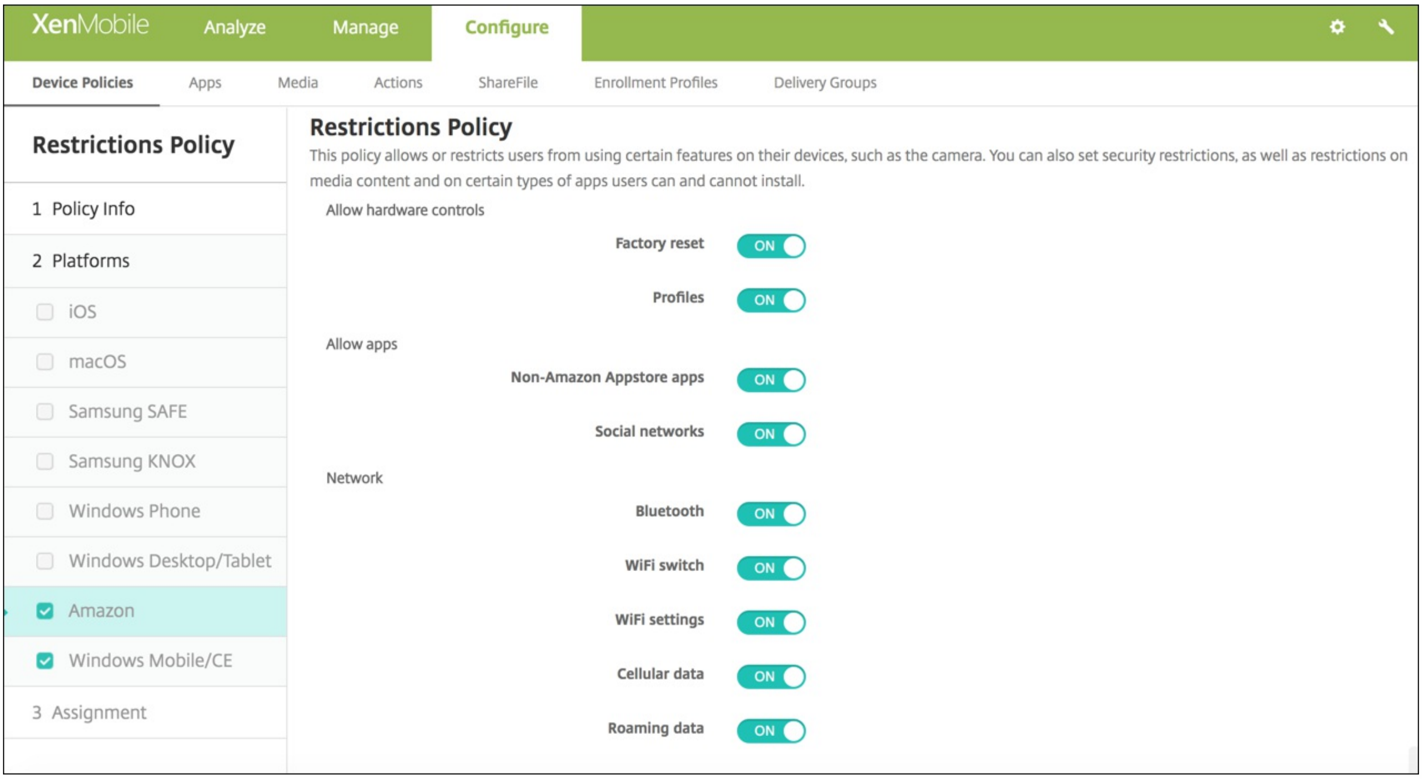
Allow USB connection: ON

Windows Phone and Windows Desktop/Tablet settings

- **WiFi Settings**
  - **Allow WiFi**: Allow a device to connect to a WiFI network. Windows Phone only.
  - **Allow Internet sharing**: Allow a device to share its internet connection with other devices by turning it into a WiFi hotspot.
  - **Allow auto-connect to WiFi Sense hotspots**: Allow a device to connect automatically to WiFi Sense hotspots. Location services must be enabled for this option to work. For more information about WiFi Sense, see the Windows Phone WiFi Sense FAQ.
  - **Allow manual configuration**: Allow users to manually configure WiFi connections. Windows Phone only.
- **Connectivity**
  - **Allow NFC**: Allow device to communicate with an NFC (Near Field Communication) 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. Note that 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 XenMobile 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 signin settings.
  - **Allow workplace:** Allows users to change workplace settings.
  - **Allow your account:** Allows users to change account settings.

Amazon



Restrictions Policy

1 Policy Info

2 Platforms

- ☐ iOS
- ☐ macOS
- ☐ Samsung SAFE
- ☐ Samsung KNOX
- ☐ Windows Phone
- ☐ Windows Desktop/Tablet
- ☑ Amazon
- ☑ Windows Mobile/CE

3 Assignment

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 hardware controls

Factory reset ON

Profiles ON

Allow apps

Non-Amazon Appstore apps ON

Social networks ON

Network

Bluetooth ON

WiFi switch ON

WiFi settings ON

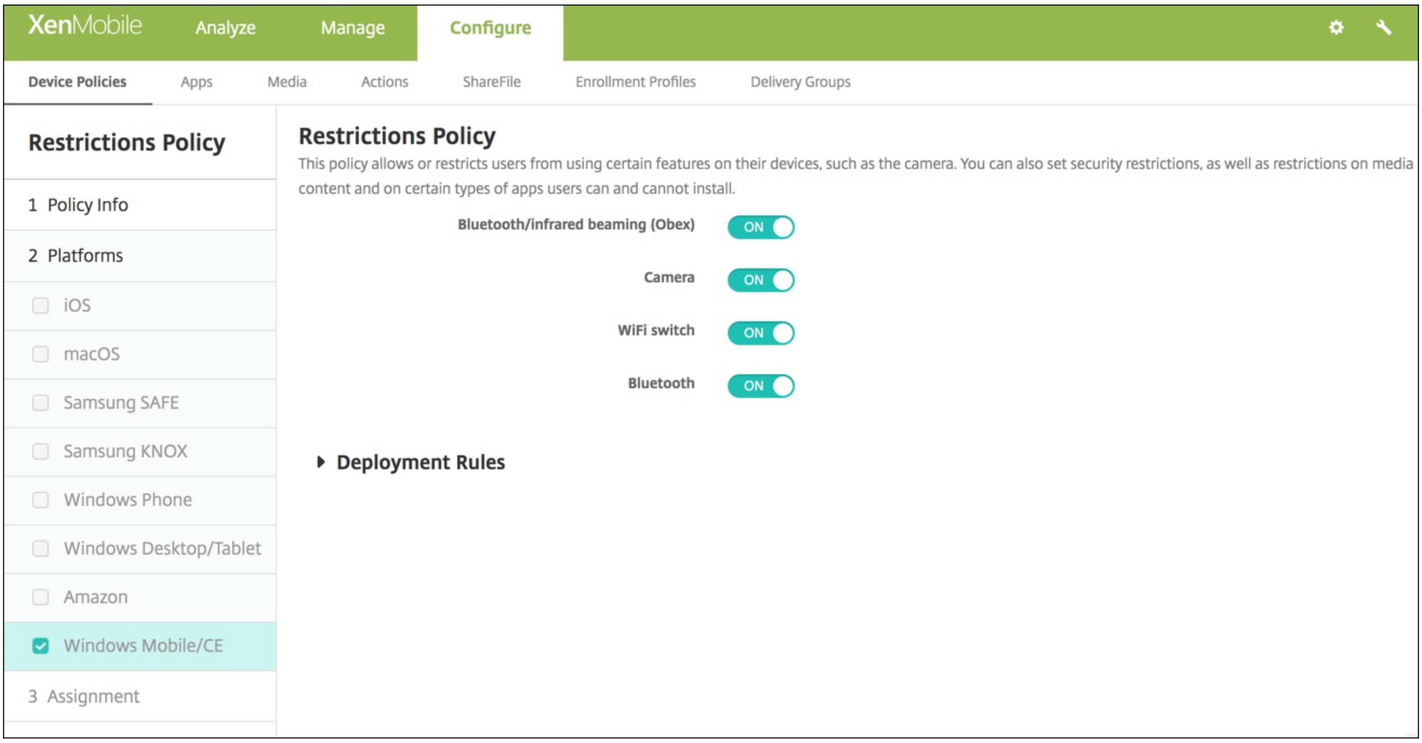
Cellular data ON

Roaming data ON

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 WiFi connectivity state.
  - **WiFi settings**: Allow users to change WiFi 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.

Windows Mobile/CE



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.

Bluetooth/infrared beaming (Obex) ON

Camera ON

WiFi switch ON

Bluetooth ON

Windows Mobile/CE settings

- **Bluetooth/infrared beaming (Obex)**: Enable OBEX (OBject EXchange protocol) over Bluetooth or infrared to exchange data between devices.
- **Camera:** Enable the camera on users' devices.
- **WiFi switch**: Allow users to switch WiFi networks.
- **Bluetooth**: Enable Bluetooth on users' devices.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Roaming device policy

Sep 06, 2017

You can add a device policy in XenMobile to configure whether to allow voice and data roaming on users' iOS and Windows Mobile/CE devices. When voice roaming is disabled, data roaming is automatically disabled. For iOS, this policy is available only on iOS 5.0 and later devices.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More** and then, under **Network access**, click **Roaming**. The **Roaming 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 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, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS settings

Configure these 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.

Configure Windows Mobile/CE settings

Configure these settings:

- **While roaming**
  - **Use on-demand connection only**: The device only connects to XenMobile if users manually trigger the connection on their devices, or if a mobile application requests a forced connection (such as a push mail request if the Exchange Server has been set accordingly). Note that this option temporarily disables the default device connection schedule policy.
  - **Block all cellular connections except the ones managed by XenMobile**: Except for the data traffic officially declared in a XenMobile application tunnel or other XenMobile 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 XenMobile**: All application data transiting through a XenMobile tunnel is blocked (including XenMobile Remote Support). The data traffic related to pure device management, however, is not blocked.
  - **Block all cellular connections to XenMobile**: In this case, until the device is either reconnected through USB, WiFi, or

its default mobile operator cellular network, there is no traffic transiting between the device and XenMobile.

- **While domestic roaming**
  - **Ignore domestic roaming**: No data is blocked while users roam domestically.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Samsung MDM license key device policy

Sep 06, 2017

XenMobile supports and extends both Samsung for Enterprise (SAFE) and Samsung KNOX policies. SAFE is a family of solutions that provides security and feature enhancements for business use through integration with mobile device management solutions. Samsung KNOX is a solution within the SAFE program that provides a more secure Android platform for enterprise use.

You must enable the SAFE APIs by deploying the built-in Samsung Enterprise License Management (ELM) key to a device before you can deploy SAFE policies and restrictions. To enable the Samsung KNOX API, you also need to purchase a Samsung KNOX Workspace license using the Samsung KNOX License Management System (KLMS), in addition to deploying the Samsung ELM key. The Samsung KLMS provisions valid licenses to mobile device management solutions to enable them to activate Samsung KNOX APIs on mobile devices. These licenses must be obtained from Samsung and are not provided by Citrix.

You must deploy Secure Hub along with the Samsung ELM key to enable the SAFE and Samsung KNOX APIs. You can verify that the SAFE APIs are enabled by checking the device properties. When the Samsung ELM key is deployed, the **Samsung MDM API available** setting is set to **True**.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog appears.

3. Click **More** and then, under **Security**, click **Samsung MDM License Key**. The **Samsung MDM License Key Policy** information page appears.

4. In the **Policy Information** pane, enter the following information:

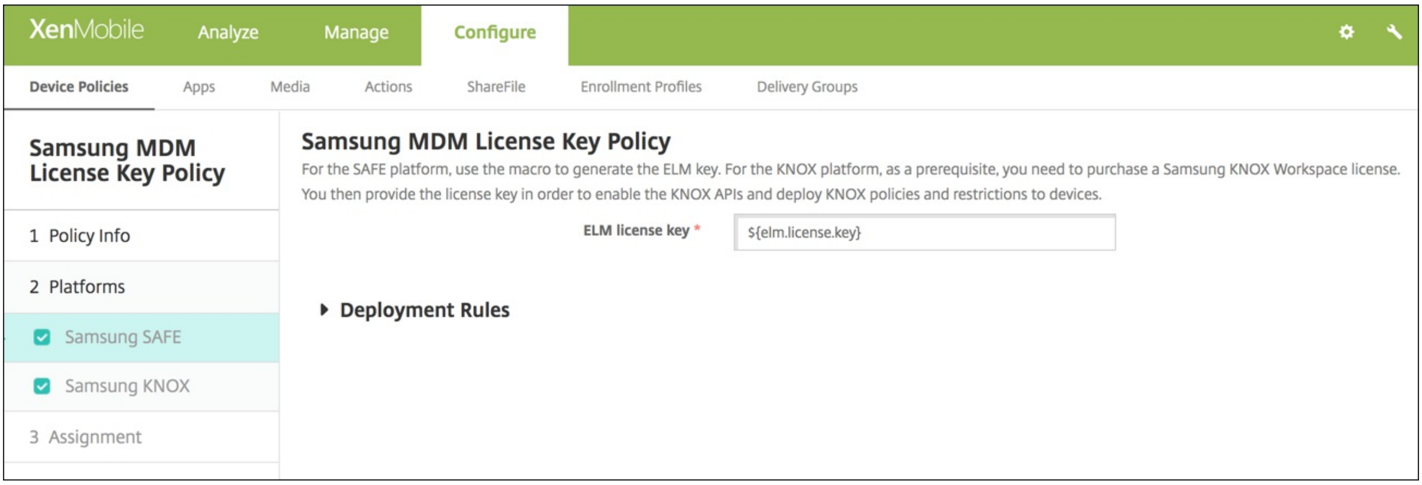
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **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, refer to Step 7 for how to set that platform's deployment rules.

Configure Samsung SAFE settings



Samsung MDM License Key Policy

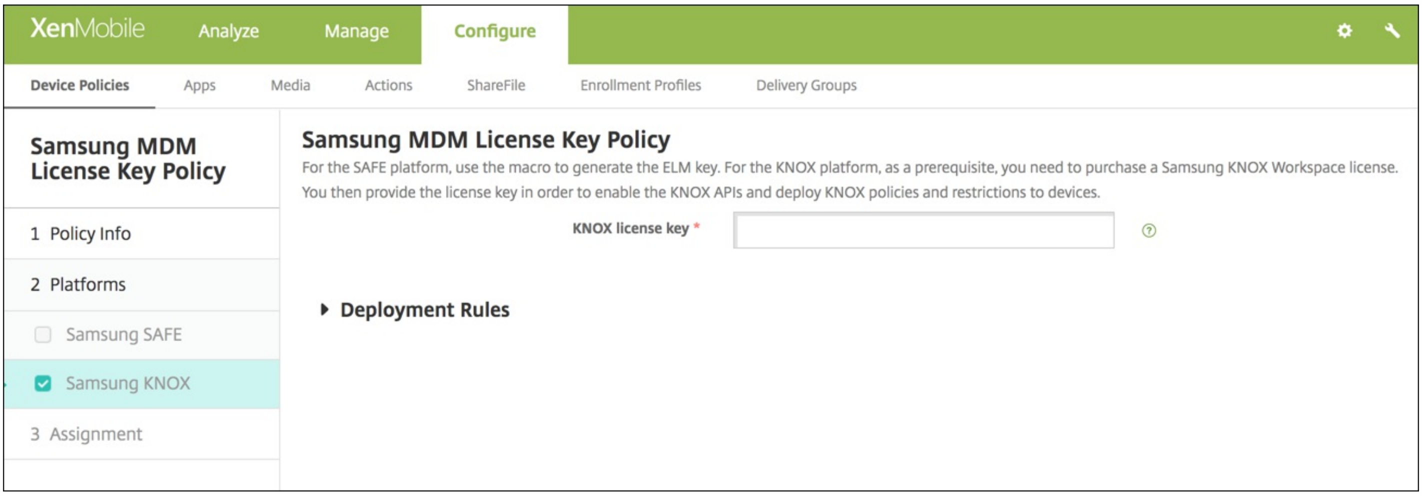
For the SAFE platform, use the macro to generate the ELM key. For the KNOX platform, as a prerequisite, you need to purchase a Samsung KNOX Workspace license. You then provide the license key in order to enable the KNOX APIs and deploy KNOX policies and restrictions to devices.

ELM license key * ${elm.license.key}

Configure this setting:

- **ELM License key**: This field should already contain the macro that generates the ELM license key. If the field is blank, type the macro ${elm.license.key}.

Configure Samsung KNOX settings



Samsung MDM License Key Policy

For the SAFE platform, use the macro to generate the ELM key. For the KNOX platform, as a prerequisite, you need to purchase a Samsung KNOX Workspace license. You then provide the license key in order to enable the KNOX APIs and deploy KNOX policies and restrictions to devices.

KNOX license key *

Configure this setting:

- **KNOX License key**: Type the KNOX license key that you obtained from Samsung.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Samsung SAFE firewall device policy

Sep 06, 2017

This policy lets you configure the firewall settings for Samsung devices. You enter IP addresses, ports, and host names that you want to allow devices to access or that you want to block devices from accessing. You can also configure proxy and proxy reroute settings.

1. In the XenMobile 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 **Network access**, click **Samsung Firewall**. The **Samsung Firewall Policy** 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 **Samsung SAFE** platform information page appears.

6. Configure these settings:

- **Allow/Deny hosts**
  - For each host to which you want to allow or deny access, click **Add** and do the following:
    - **Host name/IP range**: Type the host name or IP address range of the site you want to affect.
    - **Port/port range**: Type the port or port range.
    - **Allow/deny rule filter**: Select Whitelist to allow access or click Blacklist to deny access to the site.
    - Click **Save** or **Cancel**.
- **Reroute configuration**
  - For each proxy you want to configure, click **Add** and do the following:
    - **Host name/IP range**: Type the host name or IP address range for the proxy reroute.
    - **Port/port range**: Type the port or port range.
    - **Proxy IP**: Type the proxy IP address.
    - **Proxy port**: Type the proxy port.
    - Click **Save** or **Cancel**.

    Note: To delete an existing item, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing item, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- **Proxy Configuration**
  - **Proxy IP**: Type the IP address of the proxy server.
  - **Port**: Type the proxy server port.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

SCEP device policy

Sep 06, 2017

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 XenMobile, you should create a PKI entity and a PKI provider in distributed mode. For details, see PKI Entities.

iOS settings

macOS settings

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add New Policy** dialog box appears.

3. Expand **More** and then, under **Security**, click **SCEP**. The **SCEP Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

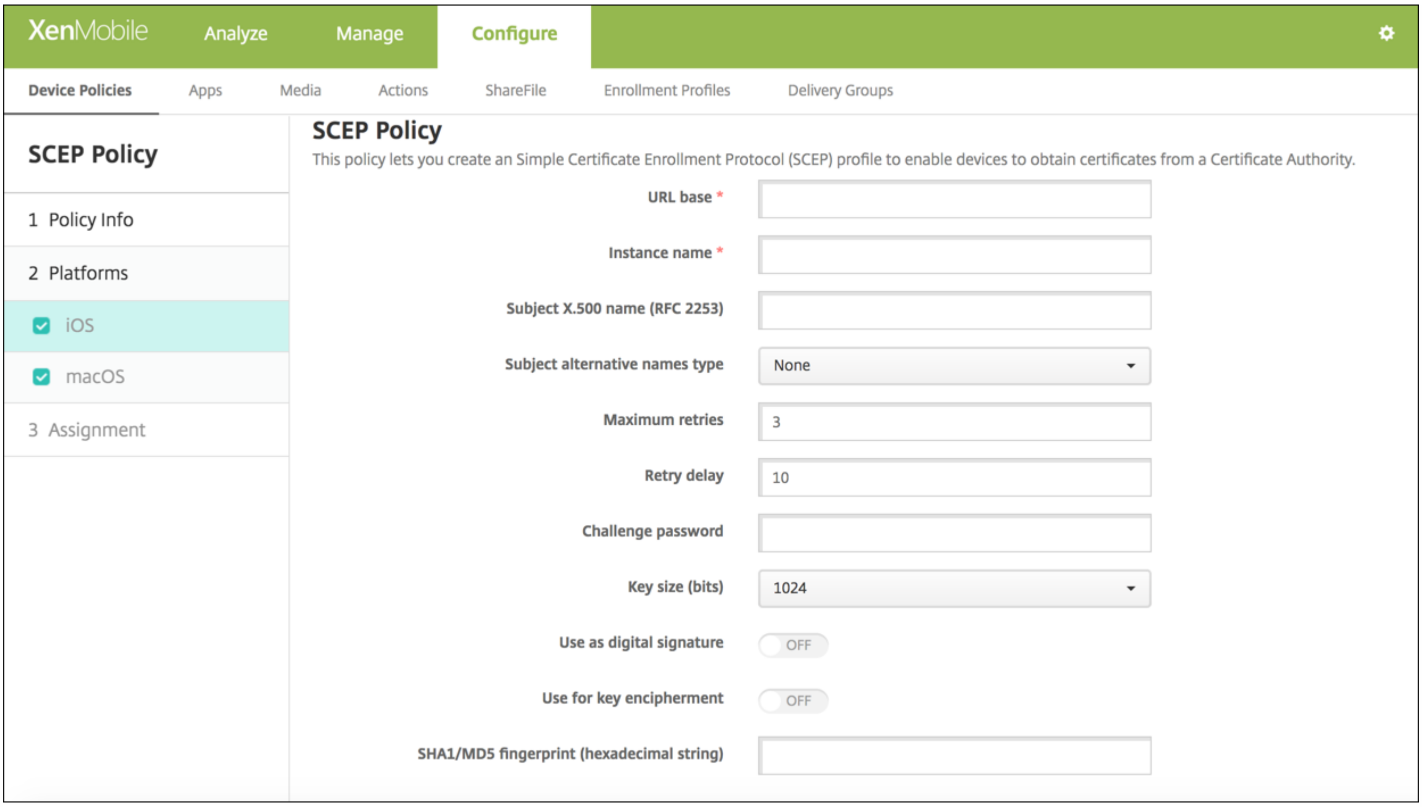
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **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, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS settings



SCEP Policy

This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.

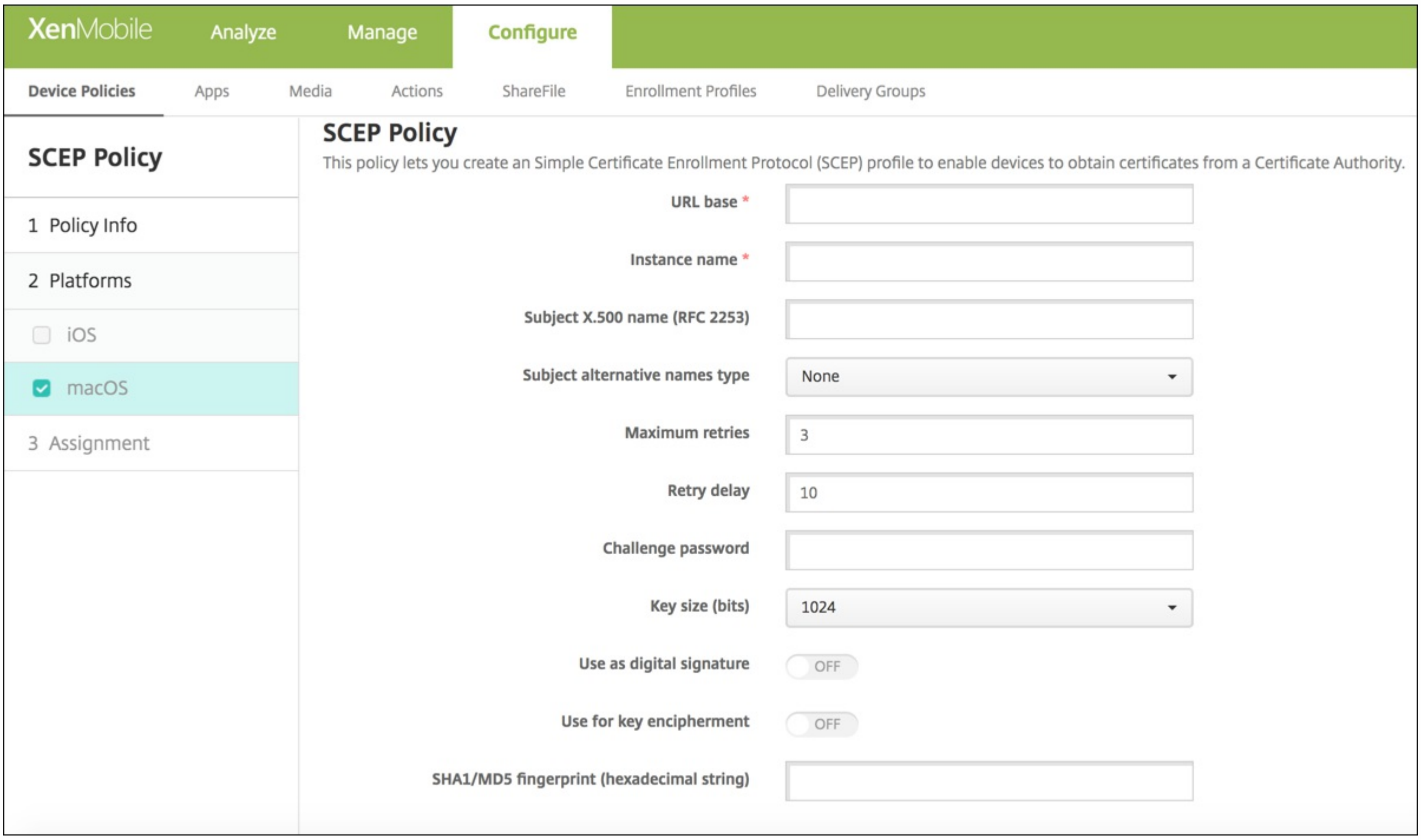
URL base *	
Instance name *	
Subject X.500 name (RFC 2253)	
Subject alternative names type	None
Maximum retries	3
Retry delay	10
Challenge password	
Key size (bits)	1024
Use as digital signature	OFF
Use for key encipherment	OFF
SHA1/MD5 fingerprint (hexadecimal string)	

Configure these 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**: 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.
- **Policy Settings**
  - 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.
  - 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.

Configure macOS settings



SCEP Policy

This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.

URL base *	
Instance name *	
Subject X.500 name (RFC 2253)	
Subject alternative names type	None
Maximum retries	3
Retry delay	10
Challenge password	
Key size (bits)	1024
Use as digital signature	OFF
Use for key encipherment	OFF
SHA1/MD5 fingerprint (hexadecimal string)	

Configure these 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.
- **Policy Settings**
  - 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.
  - 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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

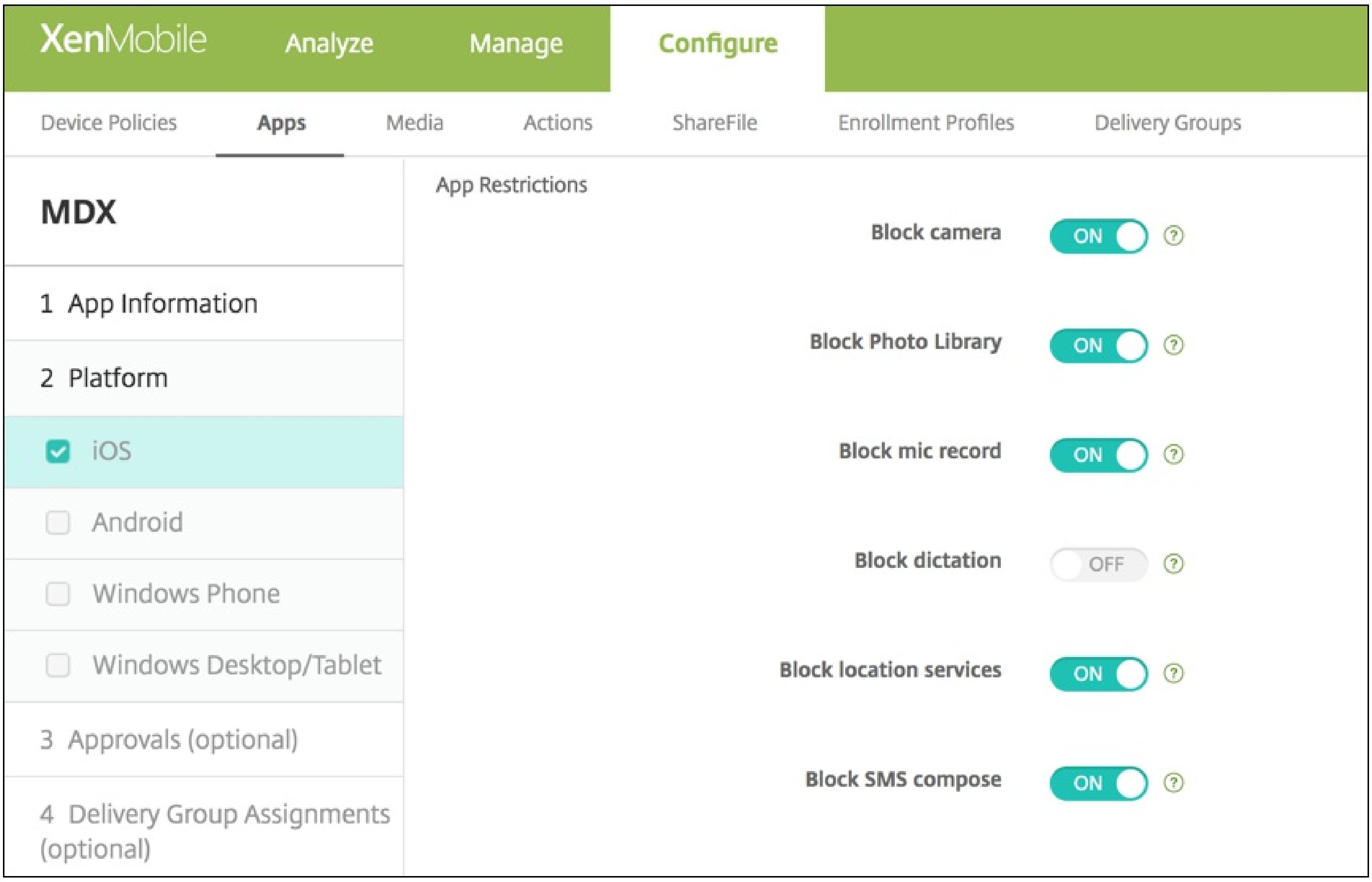
Siri and dictation policies

Sep 06, 2017

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 XenMobile container. The text that results from dictation, however, remains within the container.

XenMobile 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 XenMobile console at **Configure > Apps**. Select the app, click **Edit**, then click **iOS**.



App Restrictions

Block camera ON

Block Photo Library ON

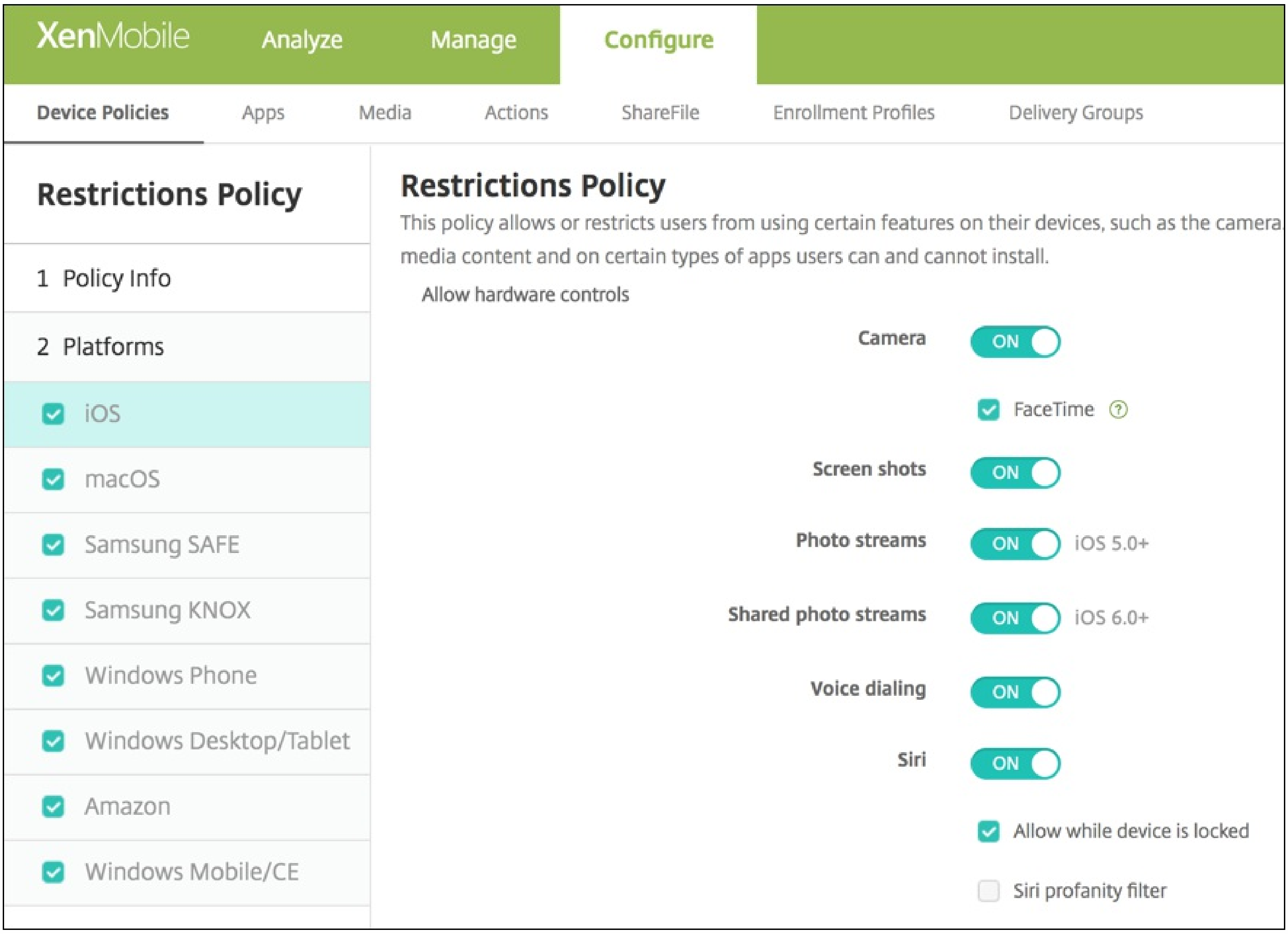
Block mic record ON

Block dictation OFF

Block location services ON

Block SMS compose ON

In MDM deployments, you can also disable Siri with the Siri policy at **Configure > Device Policies > Restrictions Policy > iOS**. The use of Siri is allowed by default.



Restrictions Policy

1 Policy Info

2 Platforms

☑ iOS

☑ macOS

☑ Samsung SAFE

☑ Samsung KNOX

☑ Windows Phone

☑ Windows Desktop/Tablet

☑ Amazon

☑ Windows Mobile/CE

Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera media content and on certain types of apps users can and cannot install.

Allow hardware controls

Camera ON

☑ FaceTime

Screen shots ON

Photo streams ON iOS 5.0+

Shared photo streams ON iOS 6.0+

Voice dialing ON

Siri ON

☑ Allow while device is locked

□ Siri profanity filter

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

Sep 06, 2017

You create single sign-on (SSO) accounts in XenMobile to let users sign on one-time only to access XenMobile 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.

Note: This policy applies only to iOS 7.0 and later.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More** and then, under **End user**, click **SSO Account**. The **SSO Account Policy** page appears.

4. In the **SSO Account 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 **iOS Platform** information page appears.

6. Configure these 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, http://shopping.apple.com is valid, but http://*.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.
  - Click **Add** to add the app identifier or click **Cancel** to cancel adding the app identifier.

  Note: To delete an existing URL or app identifier, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing.

To edit an existing URL or app identifier, hover over the line containing the listing and click the pen icon on the right-hand side. Make any changes to the listing and then click Save to save the changed listing or Cancel to leave the listing unchanged.

- **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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Storage encryption device policy

Sep 06, 2017

You create storage encryption device policies in XenMobile 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.

Samsung SAFE settings

Windows Phone settings

Android Sony settings

Note: For Samsung SAFE devices, before configuring this policy, make sure the following requirements are met:

- You must set the Screen Lock option on users' devices.
- Users' devices must be plugged in and 80% charged.
- The device must require a password containing both numbers and letters or symbols.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More** and then, under **Security**, click **Storage Encryption**. The **Storage Encryption Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.

Configure these 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**.

Configure these 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**.

Configure this setting:

- **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**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Store device policy

Sep 06, 2017

You can create a policy in XenMobile to specify whether iOS, Android, or Windows Tablet devices display a XenMobile Store webclip on the devices' home screen.

1. In the XenMobile 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 **Apps**, click **Store**. The **Store Policy** page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: If desired, type a description of the policy.

5. Click **Next**. The **Platforms** page appears.

6. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.

7. For each platform that you configure, select whether a XenMobile Store webclip appears on users' devices. The default is **ON**.

After you configure each platform, refer to Step 8 for how to set that platform's deployment rules.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Subscribed calendars device policy

Sep 06, 2017

You can add a device policy in XenMobile to add a subscribed calendar to the calendars list on users' iOS devices. The list of public calendars to which you can subscribe is available at www.apple.com/downloads/macosx/calendars.

Note: You must have subscribed to a calendar before you can add it to the subscribed calendars list on users' devices.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More** and then, under **End user**, click **Subscribed Calendars**. The **Subscribed Calendars Policy** 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 **iOS Platform Information** page appears.

6. Configure these 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 http:// link to an iCalendar file (.ics). This field is required.
- **User name**: Enter the user's logon name. This field is required.
- **Password**: Enter an optional user password.
- **Use SSL**: Select whether to use a Secure Socket Layer connection to the calendar. The default is Off.
- **Policy Settings**
  - 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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Terms and conditions device policy

Sep 06, 2017

You create terms and conditions device policies in XenMobile when you want users to accept your company's specific policies governing connections to the corporate network. When users enroll their devices with XenMobile, 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.

iOS and Android settings

Windows Phone and Windows Tablet settings

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **Terms & Conditions**. The **Terms & Conditions Policy** 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 **Terms & Conditions Platforms** information page appears.

Configure these 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**.

Configure these 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**.

6. Click **Next**. The **Terms & Conditions Policy** assignment page appears.

7. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand **Delivery groups to receive app assignment** list.

8. Click **Save**.

VPN device policy

Sep 06, 2017

You can add a device policy in XenMobile to configure virtual private network (VPN) settings that enable users' devices to connect securely to corporate resources. You can configure the VPN policy for the following platforms. Each platform requires a different set of values, which are described in detail in this article.

iOS settings

macOS settings

Android settings

Samsung SAFE settings

Samsung KNOX settings

Windows Phone settings

Windows Tablet settings

Amazon settings

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **VPN**. The **VPN Policy** page appears.

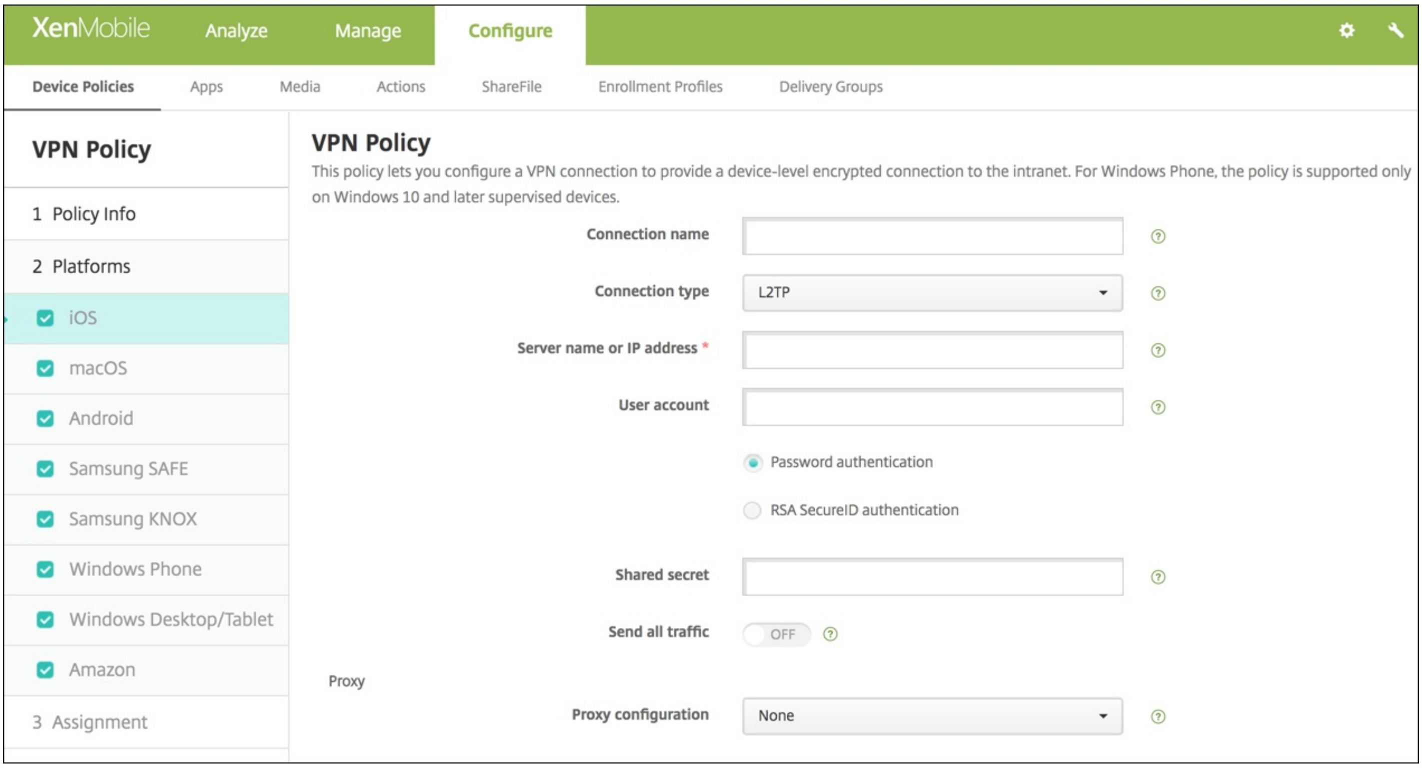
4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy Platforms** page appears. When the **Policy Platform** page appears, all platforms are selected and you see the iOS platform first.

6. Under **Platforms**, select the platform or platforms you want to add. Clear those platforms that you do not want to configure.

When you finish configuring the settings for a platform, refer to Step 7 for how to set that platform's deployment rules.



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name:

Connection type: L2TP

Server name or IP address *:

User account:

● Password authentication

○ RSA SecureID authentication

Shared secret:

Send all traffic: OFF

Proxy

Proxy configuration: None

Configure these settings

- **Connection name**: Type a name for the connection.
- **Connection type**: In the list, click 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. This connection type requires that the Cisco AnyConnect VPN client is installed on the user device.
  - **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.
  - **Citrix VPN**: Citrix VPN client for iOS.
  - **Custom SSL**: Custom Secure Socket Layer.

The following sections list the configuration options for each of the preceding connection types.

Configure L2TP Protocol

- **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 SecureID 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

- **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 SecureID authentication**.
- **Encryption level**: In the list, click 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

- **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, click 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, click 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.
- **Enable per-app VPN**: Select whether to enable per-app VPN. The default is **OFF**. Available only on iOS 9.0 and later.
- **On-demand match app enabled:** Select whether per-app VPN connections are triggered 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 AnyConnect Protocol

- **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, click 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, click 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.

- **Per-app VPN**: Select whether to enable per-app VPN. The default is **OFF**. Available only on iOS 7.0 and later. If you enable this option, configure these settings:
    - **On-demand match enabled**: Select whether per-app VPN connections are triggered 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.

            Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

            To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure Juniper SSL Protocol

- **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, click 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, click 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**. Available only on iOS 7.0 and later. If you enable this option, configure these settings:
    - **On-demand match enabled**: Select whether per-app VPN connections are triggered 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.

            Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

            To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure F5 SSL Protocol

- **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, click 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, click 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**. Available only on iOS 7.0 and later. If you enable this option, configure these settings:
  - **On-demand match enabled**: Select whether per-app VPN connections are triggered 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.

      Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

      To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure SonicWALL Protocol

- **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, click 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, click 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**. Available only on iOS 7.0 and later. If you set this option to ON, configure these settings:
  - **On-demand match enabled**: Select whether per-app VPN connections are triggered 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.

Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure Ariba VIA protocol

- **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, click 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, click 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**. Available only on iOS 7.0 and later. If you enable this option, configure these settings:
  - **On-demand match enabled**: Select whether per-app VPN connections are triggered 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.

Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure IKEv2 protocols

This section includes settings used for the IKEv2, AlwaysOn IKEv2, and AlwaysOn IKEv2 Dual Configuration protocols.

- **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**. (iOS 8.0 and later)
- **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: (iOS 8.0 and later)
  - **None**: Disable dead peer detection.
  - **Low**: Contact peer every 30 minutes.
  - **Medium**: Contact peer every 10 minutes.
  - **High**: Contact peer every 1 minute.
- **Disable Mobility and Multihoming**: Choose whether to disable this feature. (iOS 9.0+)
- **Use IPv4/IPv6 internal subnet attributes**: Choose whether to enable this feature. (iOS 9.0+)
- **Disable redirects**: Choose whether to disable redirects. (iOS 9.0+)
- **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 interval 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 WiFi and 110 seconds over cellular. You can change the interval by using the NAT keepalive interval parameter. (iOS 9.0+)
- **NAT keepalive Interval (seconds)**: Defaults to 20 seconds. (iOS 9.0+)
- **Enable Perfect Forward Secrecy**: Choose whether to enable this feature. (iOS 9.0+)
- **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. (iOS 10.0+)
- **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 append the domains in the supplemental match domains list to the list of search domains for the resolver. **0** means append; **1** means don't append. Default is **0**.
- **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, that string is used as the default domain. This is how a split-tunnel configuration can direct all DNS queries first to the VPN DNS servers before the primary DNS servers. If the VPN tunnel becomes the default route of the network, the DNS servers listed 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, click the IKE encryption algorithm to use. The default is **3DES**.
  - **Integrity Algorithm**: In the list, click the integrity algorithm to use. The default is **SHA1-96**.
  - **Diffie Hellman Group**: In the list, click the Diffie Hellman group number. The default is **2**.
  - **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, click how to handle the voice mail exception. The default is **Allow traffic via tunnel**.
  - **AirPrint**: In the list, click 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.

    Note: To delete an existing app bundle identifier, hover over the line containing the listing and then click the trashcan icon on the right side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing app bundle identifier, 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.
- **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**. Available only on iOS 9.0 and later.
  - **On-demand match app enabled:** Select whether per-app VPN connections are triggered 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 VPN protocol

The Citrix VPN client is available in the Apple Store 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, click 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, click 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**. Available only on iOS 7.0 and later. If you set this option to ON, configure the following settings:
  - **On-demand match enabled**: Select whether per-app VPN connections are triggered 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.

      Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

      To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.
- **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 NetScaler policies that are targeted to VPN plugin clients. The **Value** for this key is automatically appended to the VPN plugin for the requests initiated by the plugin.

  Note: To delete an existing parameter, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

  To edit an existing parameter, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure Custom SSL protocol

- **Custom SSL identifier (reverse DNS format)**: Set to the bundle identifier.
- **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.
- **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, click 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, click 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**. Available only on iOS 7.0 and later. If you set this option to ON, configure the following settings:
  - **On-demand match enabled**: Select whether per-app VPN connections are triggered 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**.
  - **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.

> **Note**: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.
>
> To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- **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.

> **Note**: To delete an existing parameter, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.
>
> To edit an existing parameter, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure Enable VPN on demand options

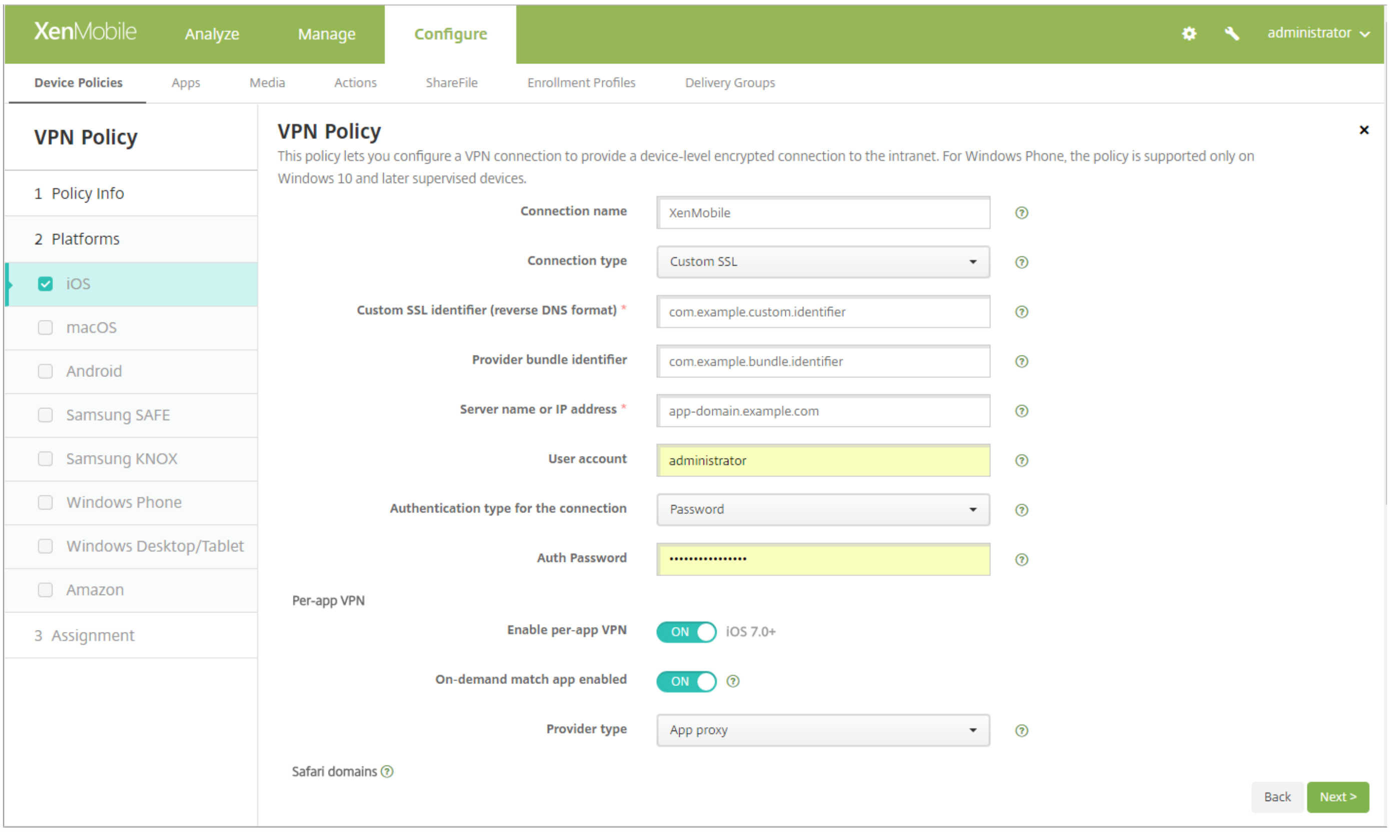
- Proxy
  - **Proxy configuration**: In the list, click how the VPN connection routes through a proxy server. The default is **None**.
    - If you enable **Manual**, configure these settings:
      - **Host name or IP address for the proxy server**: Type the host name or IP address for the proxy server. This field is required.
      - **Port for the proxy server**: Type the proxy server port number. This field is required.
      - **User name**: Type an optional proxy server user name.
      - **Password**: Type an optional proxy server password.
    - If you configure **Automatic**, configure this setting:
      - **Proxy server URL**: Type the URL for the proxy server. This field is required.
- Policy Settings
  - 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.
  - 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.

Configure a per-app VPN

Per-app VPN options for iOS are available for these connection types: Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, and Custom SSL.

To configure a per-app VPN:

1. In **Configure** > **Device Policies**, create a VPN policy. For example:



VPN Policy

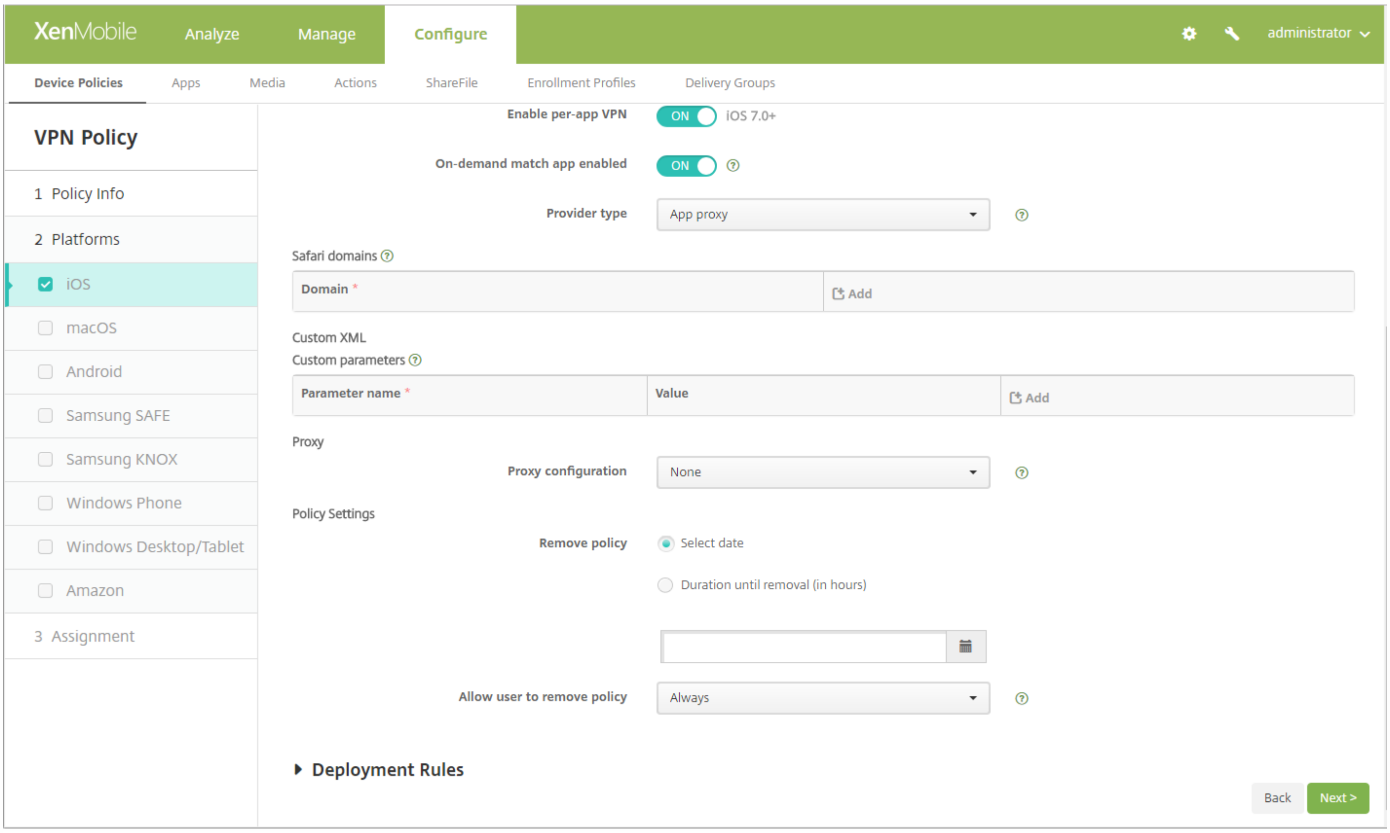
This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name	XenMobile
Connection type	Custom SSL
Custom SSL identifier (reverse DNS format) *	com.example.custom.identifier
Provider bundle identifier	com.example.bundle.identifier
Server name or IP address *	app-domain.example.com
User account	administrator
Authentication type for the connection	Password
Auth Password	•••••••••••••••••

Per-app VPN

Enable per-app VPN	ON iOS 7.0+
On-demand match app enabled	ON
Provider type	App proxy

Safari domains



Enable per-app VPN	ON iOS 7.0+
On-demand match app enabled	ON
Provider type	App proxy

Safari domains

Domain *	Add

Custom XML

Custom parameters

Parameter name *	Value	Add

Proxy

Proxy configuration	None

Policy Settings

Remove policy: ● Select date ○ Duration until removal (in hours)

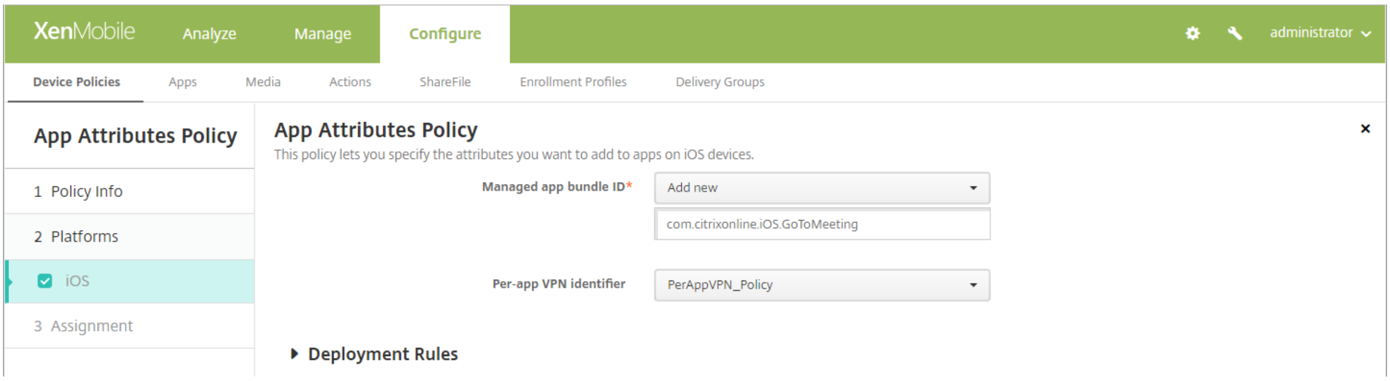
Allow user to remove policy	Always

Deployment Rules

A per-app VPN policy for Secure Hub has the following setting requirements:

- **Connection Name**: Set to **XenMobile**. XenMobile uses the Connection Name as the VPN provider localized description. Secure Hub uses the VPN localized description to differentiate the device-wide provider from the per-app provider.
- **Connection type**: Set to **Custom SSL**.
- **Custom SSL Identifier**: Set to the bundle identifier of Secure Hub.
- **Provider Bundle Identifier**: Set to the bundle identifier of the Secure Hub network extension. That bundle identifier is the Secure Hub bundle identifier, specified in **Custom SSL identifier**, with **.NE** appended.
- **Provider Type**: Set to **Packet tunnel**.

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.)



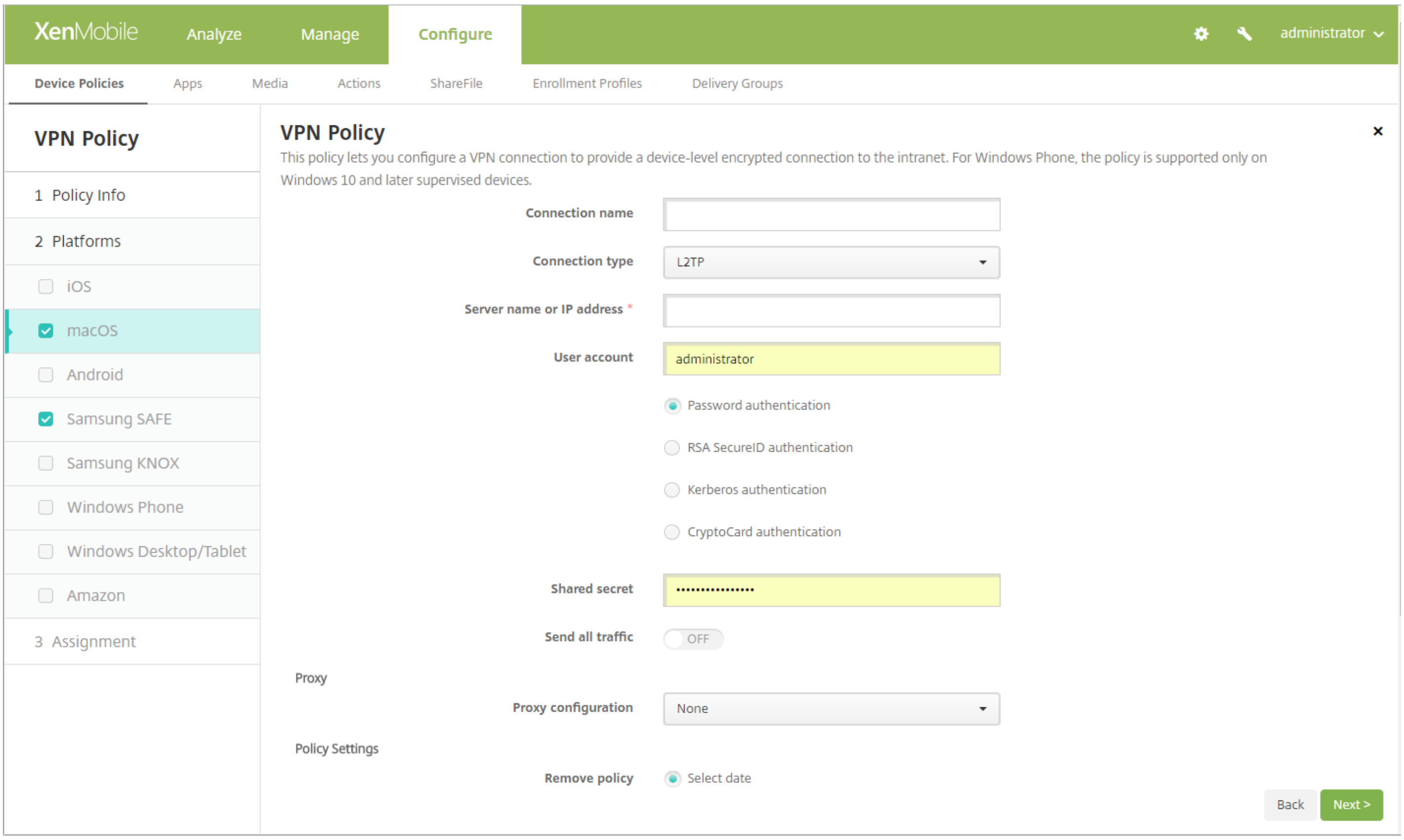
App Attributes Policy

This policy lets you specify the attributes you want to add to apps on iOS devices.

Managed app bundle ID*: Add new

com.citrixonline.iOS.GoToMeeting

Per-app VPN identifier: PerAppVPN_Policy



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name:

Connection type: L2TP

Server name or IP address *:

User account: administrator

● Password authentication
○ RSA SecureID authentication
○ Kerberos authentication
○ CryptoCard authentication

Shared secret: ••••••••••••••••

Send all traffic: OFF

Proxy

Proxy configuration: None

Policy Settings

Remove policy: ● Select date

Configure these settings:

- **Connection name**: Type a name for the connection.
- **Connection type**: In the list, click 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

- **Server name or IP address**: Type the server name or IP address for the VPN server.
- **User Account**: Type an optional user account.
- Select one of **Password authentication**, **RSA SecureID authentication**, **Kerberos authentication**, **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

- **Server name or IP address**: Type the server name or IP address for the VPN server.
- **User Account**: Type an optional user account.
- Select one of **Password authentication**, **RSA SecureID authentication**, **Kerberos authentication**, **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

- **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, click 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, click 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

- **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, click 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, click 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.

- **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 enabled**: Select whether per-app VPN connections are triggered 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.

      Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

      To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure Juniper SSL Protocol

- **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, click 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, click 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 the following settings:
  - **On-demand match enabled**: Select whether per-app VPN connections are triggered 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.

      Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

      To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure F5 SSL Protocol

- **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, click 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, click 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 enabled**: Select whether per-app VPN connections are triggered 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.

Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure SonicWALL Protocol

- **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, click 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, click 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 enabled**: Select whether per-app VPN connections are triggered 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.

Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure Ariba VIA protocol

- **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, click 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, click 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 enabled**: Select whether per-app VPN connections are triggered 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.

> **Note**: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.
>
> To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure Citrix VPN protocol

The Citrix VPN client is available in the Apple Store 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, click 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, click 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**. Available only on iOS 7.0 and later. If you enable this option, configure these settings:
  - **On-demand match enabled**: Select whether per-app VPN connections are triggered 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.

      Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

      To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- **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 NetScaler policies that are targeted to VPN plugin clients. The **Value** for this key is automatically appended to the VPN plugin for the requests initiated by the plugin.

    Note: To delete an existing parameter, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing parameter, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Configure Custom SSL protocol

- **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, click 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, click 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 enabled**: Select whether per-app VPN connections are triggered 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.

        Note: To delete an existing domain, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

        To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- **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.

    Note: To delete an existing parameter, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

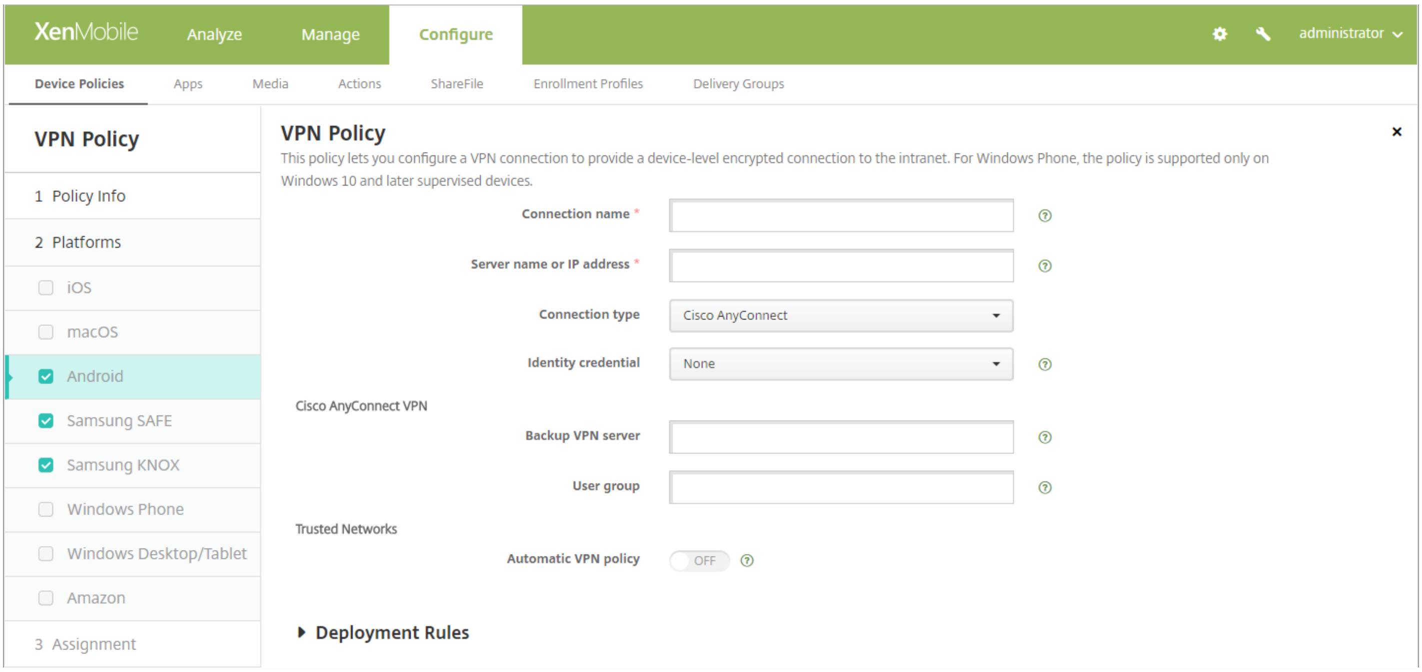
    To edit an existing parameter, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

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 click 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, such as 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, click 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 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 is the default.
    - **Ethernet**: Matches only Ethernet network interface hardware.
    - **WiFi**: Matches only WiFi 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 WiFi 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, click 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, such as when the DNS server cannot resolve the domain, redirects to a different server, or times out.
      - **NeverConnect**: The domain never triggers a VPN connection.
    - **Action Parameters: RequiredDNSServers**: For each DNS server 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 need not 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 hostname cannot be resolved, if the server is unreachable, or if the server does not respond with a 200 HTTP status code, a VPN connection is established in response. 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 will see Valid XML in green text below the XML content text box if the XML is valid; otherwise, you will see an error message in orange text describing the error.

- Proxy
  - **Proxy configuration**: In the list, click how the VPN connection routes through a proxy server. The default is **None**.
    - If you enable **Manual**, configure these settings:
      - **Host name or IP address for the proxy server**: Type the host name or IP address for the proxy server. This field is required.
      - **Port for the proxy server**: Type the proxy server port number. This field is required.
      - **User name**: Type an optional proxy server user name.
      - **Password**: Type an optional proxy server password.
    - If you configure **Automatic**, configure this setting:
      - **Proxy server URL**: Type the URL for the proxy server. This field is required.
- Policy Settings
  - 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.
  - 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.



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name *

Server name or IP address *

Connection type: Cisco AnyConnect

Identity credential: None

Cisco AnyConnect VPN

Backup VPN server

User group

Trusted Networks

Automatic VPN policy: OFF

Configure these settings for **Citrix VPN**:

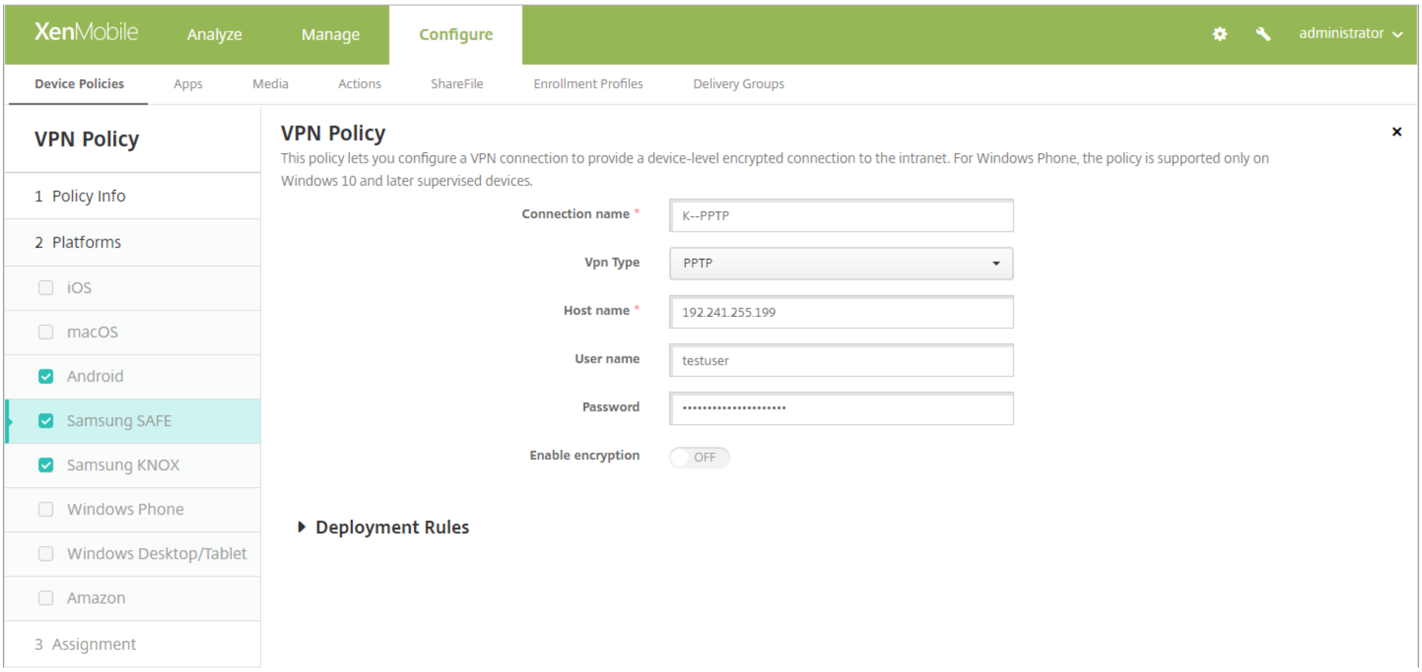
- **Connection name**: Type a name for the VPN connection. This field is required.
- **Server name or IP address**: Type the FQDN or IP address of the NetScaler Gateway.
- **Authentication type for the connection**: Choose an authentication type and complete any of these fields that appear for the type:
  - **User name** and **Password**: Type your VPN credentials for the **Authentication types** of **Password** or **Password and Certificate**. Optional. If you don't provide the VPN credentials, the Citrix VPN app prompts for a user name and password.
  - **Identity credential**: Appears for the **Authentication types** of **Certificate** or **Password and Certificate**.
- **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**: Choose a setting. If **Whitelist**, all apps in the whitelist tunnel through this VPN. If **Blacklist**, all apps except those 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. XenMobile supports these parameters for Citrix VPN:
  - **disableL3Mode**: Optional. To enable this parameter, type **Yes** for the **Value**. If enabled, XenMobile doesn't display user-added VPN connections and the user cannot add a new connection. This 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 these settings for **Cisco AnyConnect VPN**:

- **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.
- **Backup VPN server**: Type the backup VPN server information.
- **User group**: Type the user group information.
- **Identity credential**: In the list, select an identity credential.
- 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, click the desired policy. The default is **Disconnect**. Possible options are:
      - **Disconnect**: The client terminates the VPN connection in the trusted network. This is the default.
      - **Connect**: The client initiates a VPN connection in the trusted network.
      - **Do Nothing**: The client takes no action.
      - **Pause**: Suspends the VPN session (rather than disconnecting it) when a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user leaves the trusted network again, the session resumes. This eliminates the need to establish a new VPN session after leaving a trusted network.
    - **Untrusted network policy**: In the list, click the desired policy. The default is **Connect**. Possible options are:
      - **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 may have 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 may have 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.

      Note: To delete an existing server, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

      To edit an existing server, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.



VPN Policy

1 Policy Info

2 Platforms

- □ iOS
- □ macOS
- ☑ Android
- ☑ Samsung SAFE
- ☑ Samsung KNOX
- □ Windows Phone
- □ Windows Desktop/Tablet
- □ Amazon

3 Assignment

VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name *	K--PPTP
Vpn Type	PPTP
Host name *	192.241.255.199
User name	testuser
Password	••••••••••••••••••••••
Enable encryption	OFF

Configure these settings:

- **Connection name**: Type a name for the connection.
- **Vpn type**: In the list, click 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 is the default setting.
  - **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.

The following sections list the configuration options for each of the preceding VPN types.

Configure L2TP with pre-shared key protocol

- **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

- **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.
- **Identity credential**: In the list, click the identity credential to be used. The default is **None**.

Configure PPTP protocol

- **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.
- **Enable encryption**: Select whether to enable encryption on the VPN connection.

Configure Enterprise protocol

- **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:
  - **User name**: Type a user name.
  - **Password**: Type the user password.
- **Group name**: Type an optional group name.
- **Authentication method**: In the list, click the authentication method to be used. Possible options are:
  - **Certificate**: Use certificate authentication. This is the default. If selected, in the Identity credential list, click 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, click 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**.
- **Enable mobile option**: Select whether to enable mobile option. The default is **OFF**.
- **Diffie-Hellman group value (key strength)**: In the list, click the key strength to be used. The default is 0.
- **Split tunnel type**: In the list, click 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, click 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
  - **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

- **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, click 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.

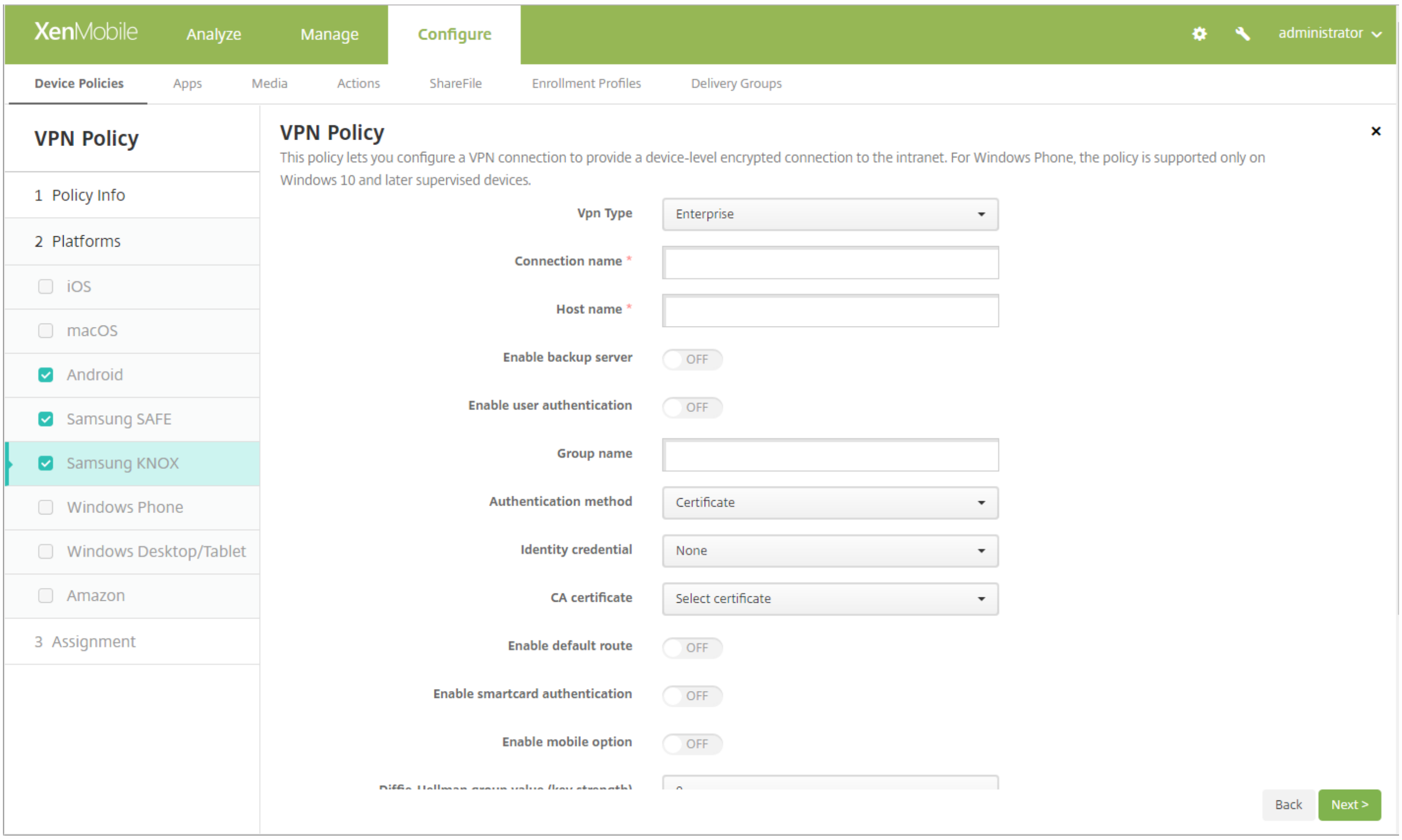
Configure IPSEC connection type settings

- **Identity**: Type an optional identifier for this configuration.
- **IPsec group ID type**: In the list, click 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, click the Internet Key Exchange version to use. The default is **IKEv1**.
- **Authentication method**: In the list, click the authentication method to be used. The default is **Certificate**. Possible options are:
  - **Certificate**: Use certificate authentication. If selected, in the **Identity credentia**l list, click 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 click the identity credential to use. The default is **None**.
- **CA certificate**: In the list, click 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).
- **Diffie-Hellman group value (key strength)**: In the list, click 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, click 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

- **Authentication method**: In the list, click 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, click the credential to use. The default is **None**.
  - **CAC based Authentication:** Use a Common Access Card (CAC) for authentication.
- **CA certificate**: In the list, click 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, click 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.



☐ iOS
☐ macOS
☑ Android
☑ Samsung SAFE
☑ Samsung KNOX
☐ Windows Phone
☐ Windows Desktop/Tablet
☐ Amazon

VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Vpn Type	Enterprise
Connection name *	
Host name *	
Enable backup server	OFF
Enable user authentication	OFF
Group name	
Authentication method	Certificate
Identity credential	None
CA certificate	Select certificate
Enable default route	OFF
Enable smartcard authentication	OFF
Enable mobile option	OFF
Diffie-Hellman group value (key strength)	0

Note: When you configure any policy for Samsung KNOX, it applies only inside the Samsung KNOX container.

Configure these settings:

- **Vpn Type**: In the list, click the type of VPN connection to configure, 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

- **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:
  - **User name**: Type a user name.
  - **Password**: Type the user password.
- **Group name**: Type an optional group name.
- **Authentication method**: In the list, click the authentication method to be used. Possible options are:
  - **Certificate**: Use certificate authentication. This is the default. If selected, in the Identity credential list, click 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, click 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, click the key strength to be used. The default is **0**.
- **Split tunnel type**: In the list, click 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, click the level of NSA Suite B encryption to use. Possible options are:
  - **GCM-128**: Use 128-bit AES-GCM encryption: This 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.

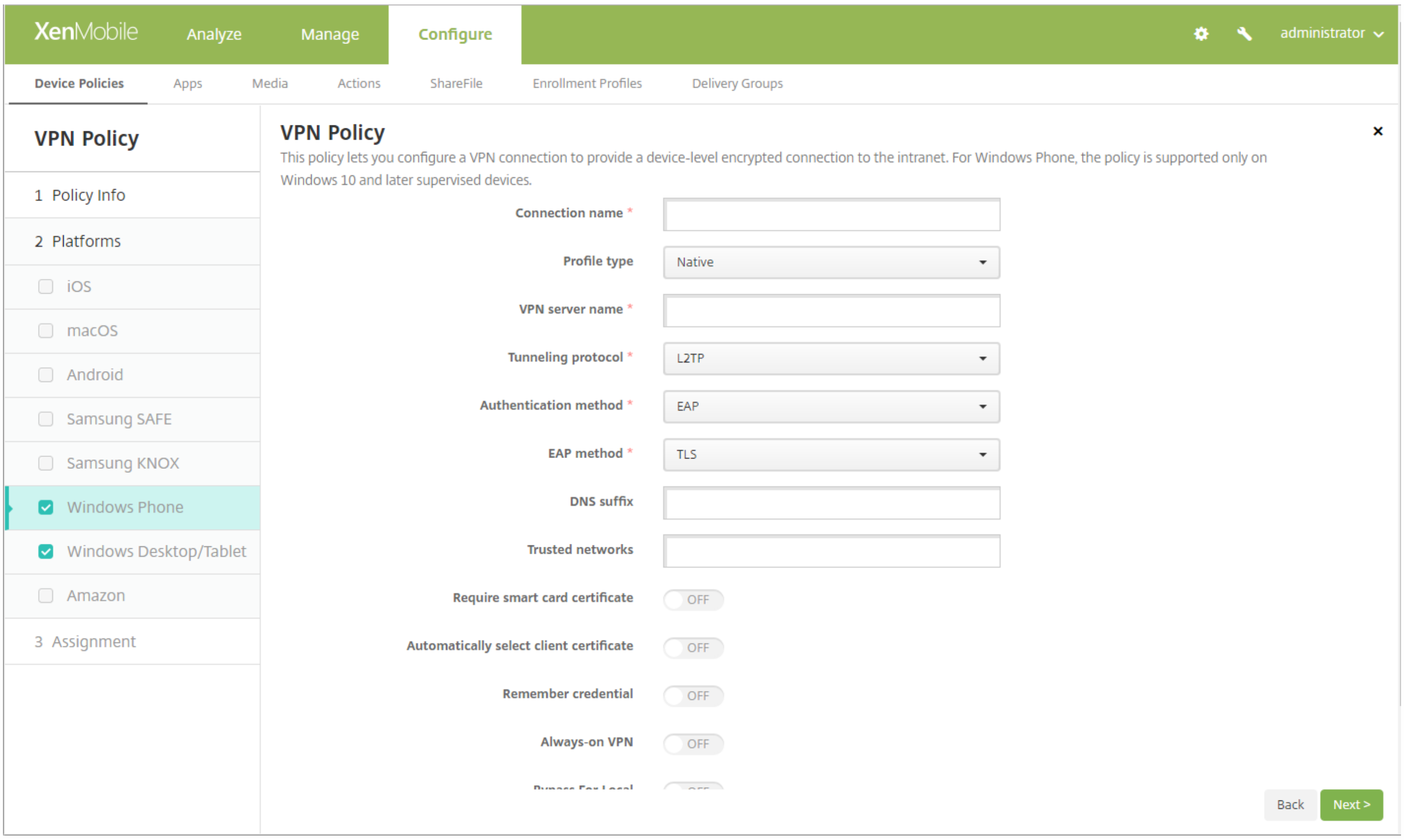
Configure generic protocol

- **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, click 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**
  - **Identity**: Type an optional identifier for this configuration.
  - **IPsec group ID type**: In the list, click 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, click the Internet Key Exchange version to use. The default is **IKEv1**.
  - **Authentication method**: In the list, click the authentication method to be used. The default is **Certificate**. Possible options are:
    - **Certificate**: Use certificate authenticationIf selected, in the **Identity credential** list, click 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.
  - **CA certificate**: In the list, click 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, click 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, click 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, click 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.
  - **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 is the default.
        - **Certificate**: Use certificate authentication. This is the default. If selected, in the Identity credential list, click the credential to use. The default is None.
        - **CAC based Authentication**: Use a Common Access Card (CAC) for authentication.
    - **CA certificate**: In the list, click 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, click 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, click 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.



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name *

Profile type: Native

VPN server name *

Tunneling protocol *: L2TP

Authentication method *: EAP

EAP method *: TLS

DNS suffix

Trusted networks

Require smart card certificate: OFF

Automatically select client certificate: OFF

Remember credential: OFF

Always-on VPN: OFF

Bypass For Local: OFF

Note: These settings are supported only on Window 10 and later supervised phones.

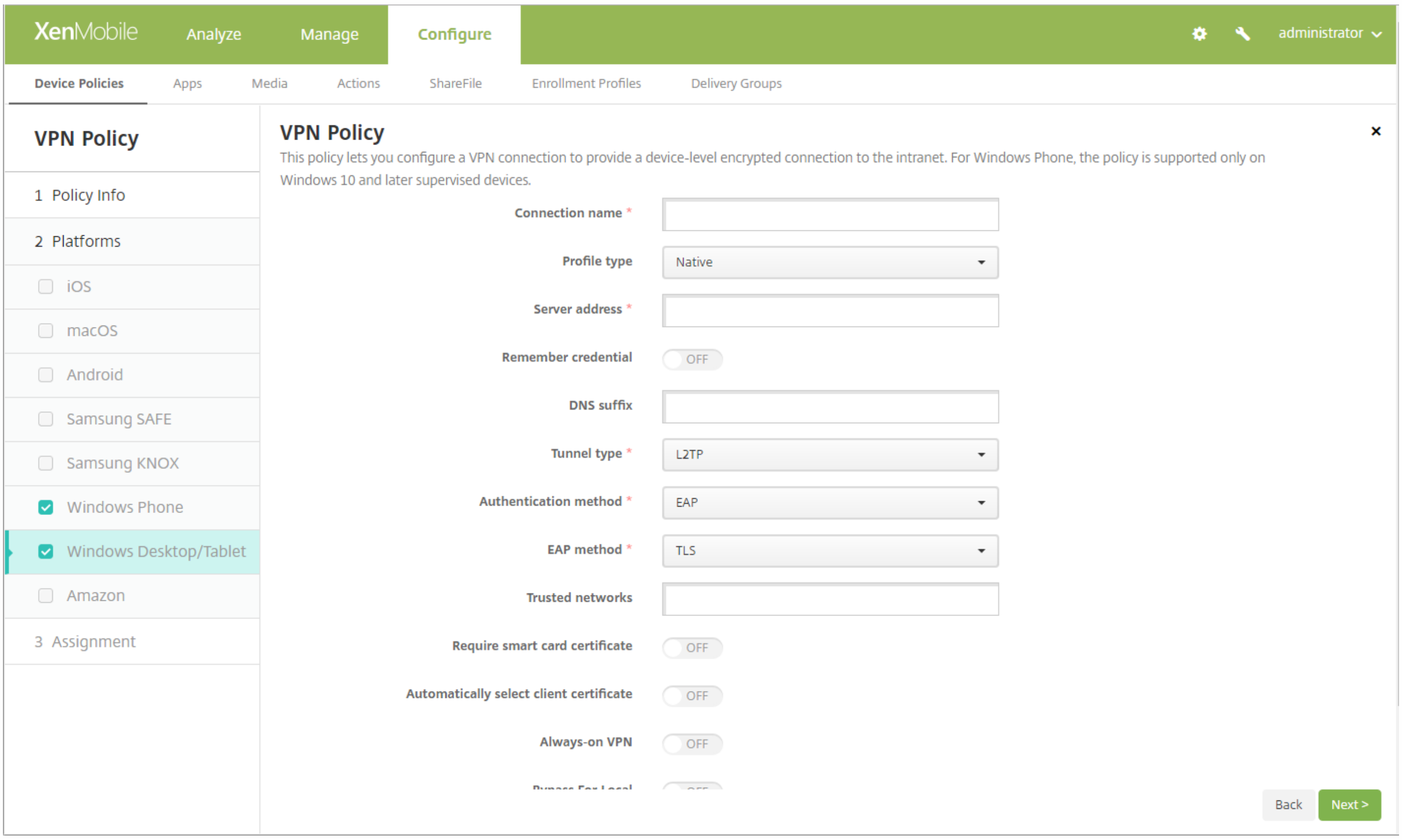
Configure these settings:

- **Connection name**: Enter a name for the connection. This field is required.
- **Profile type**: In the list, click 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, click 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, click 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, click 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 Windows 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 plugin profile to be used by clicking Browse and navigating to the file's location. Contact the plugin 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.



VPN Policy

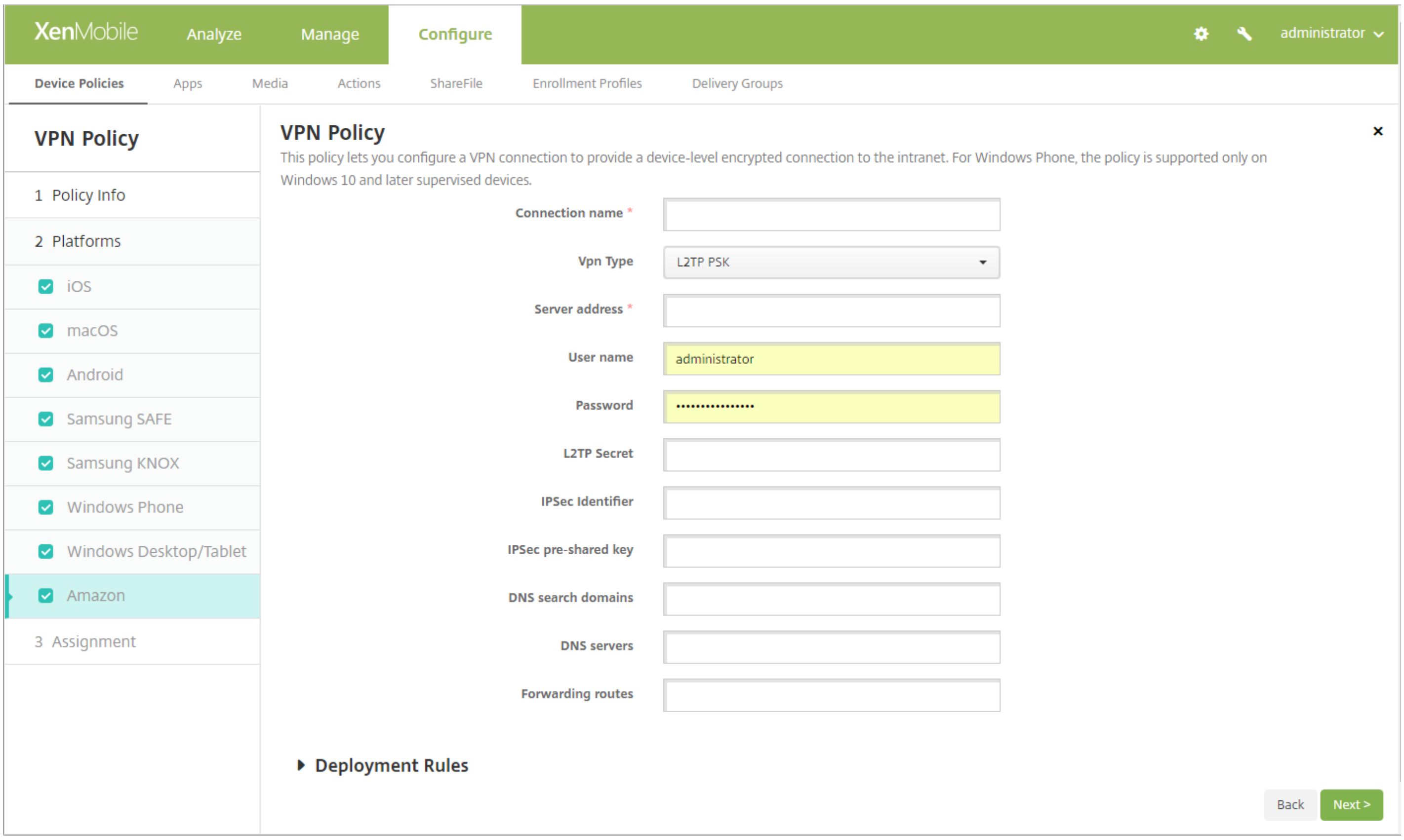
This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name *	
Profile type	Native
Server address *	
Remember credential	OFF
DNS suffix	
Tunnel type *	L2TP
Authentication method *	EAP
EAP method *	TLS
Trusted networks	
Require smart card certificate	OFF
Automatically select client certificate	OFF
Always-on VPN	OFF
Bypass For Local	OFF

Configure these settings:

Configure Windows 10 settings

- **Connection name**: Enter a name for the connection. This field is required.
- **Profile type**: In the list, click either **Native** or **Plugin**. The default is **Native**.
- **Configure Native profile type** - These setting 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, click 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, click 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, click 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 plugin profile to be used by clicking **Browse** and navigating to the file's location. Contact the plugin provider for format and details.
  - **Trusted networks**: Type a list of networks separated by commas that do not require a VPN connection for access. For example, when users are on your company wireless network, they can access protected resources directly.
  - **Always on VPN**: Select whether the VPN is always on. The default is **OFF**. When enabled, the VPN connection 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.



VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name *	
Vpn Type	L2TP PSK
Server address *	
User name	administrator
Password	•••••••••••••••••
L2TP Secret	
IPSec Identifier	
IPSec pre-shared key	
DNS search domains	
DNS servers	
Forwarding routes	

Configure these settings:

- **Connection name**: Enter a name for the connection.
- **Vpn type**: Click the connection type. Possible options are:
  - **L2TP PSK**: Layer 2 Tunneling Protocol with pre-shared key authentication. This 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

- **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

- **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, click the server certificate to be used.
- **CA certificate**: In the list, click the CA certificate to be used.
- **Identity credential**: In the list, click 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

- **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

- **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, click the server certificate to be used.
- **CA certificate**: In the list, click the CA certificate to be useg.
- **Identity credential**: In the list, click the identity credential to be useg.
- **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

- **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, click the server certificate to be used.
- **CA certificate**: In the list, click 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

- **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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Wallpaper device policy

Sep 06, 2017

You can add a .png or .jpg file to set wallpaper on an iOS device lock screen, home screen, or both. Available in iOS 7.1.2 and later. 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 Apple's recommended image dimensions for iOS devices.

Device		**Image dimensions in pixels**
iPhone	**iPad**	
4, 4s		640 x 960
5, 5c, 5s		640 x 1136
6, 6s		750 x 1334
6 Plus		1080 x 1920
	Air, 2	1536 x 2048
	4, 3	1536 x 2048
	Mini 2, 3	1536 x 2048
	Mini	768 x 1024

1. In the XenMobile 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 **End User**, click **Wallpaper**. The **Wallpaper Policy** page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy Platforms** page appears.

Configure these 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**: Select the wallpaper file by clicking **Browse** and navigating to the file's location.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Web content filter device policy

Sep 06, 2017

You can add a device policy in XenMobile to filter web content on iOS devices by using Apple's auto-filter function in conjunction with specific sites that you add to whitelists and blacklists. This policy is available only on iOS 7.0 and later devices in Supervised mode. For information about placing an iOS device into Supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **More** and then, under **Security**, click **Web Content Filter**. The **Web Content Filter Policy** 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 **iOS Platform** information page appears.

6. Configure these 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 settings

- **Web Content Filter**
  - **Auto filter enabled**: Select whether to use Apple's 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 regardless of whether 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 http:// or https:// 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 http:// or https:// before the web address.
    - Click **Save** to save the website to the blacklist or click **Cancel** not to save it.
- **Bookmark whitelist**
  - **Bookmark Whitelist**: Items in this list are the only sites accessible to users. For each web site you want to add to the bookmark whitelist, click **Add** and do the following:
    - **URL**: Type the URL of the website to be bookmarked. You must add http:// or https:// before the web address. This field is required.
    - **Bookmark folder**: Enter an optional bookmark folder name. If this field is left blank, the bookmark is added to the default bookmarks directory.
    - **Title**: Enter a descriptive title for the website. For example, type "Google" for the URL http://google.com.
    - Click **Save** to save the website to the blacklist or click **Cancel** not to save it.

Note: To delete an existing website, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

To edit an existing website, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

Plug-in filter type settings

- **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.

Note: To delete an existing key, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

To edit an existing key, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- 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.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Webclip device policy

Sep 06, 2017

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.

iOS settings

macOS settings

Android settings

Windows Desktop/Tablet settings

1. In the XenMobile 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 **Apps**, click **Webclip**. The **Webclip Policy** page appears.

4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.

Configure these 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, http://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's 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**.
- **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.

Configure these 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, http://server.
- **Icon to be updated**: Select the icon to be used for the webclip by clicking Browse and navigating to the file's location.
- 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.
  - In the **Profile scope** list, click **User** or **System**. This option is available on macOS 10.7 and later.

Configure these 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's location.

Configure these settings:

- **Name**: Type the label that is to appear with the webclip.
- **URL**: Type the URL associated with the webclip.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

8. Click **Next**. The **Webclip Policy** assignment page appears.

9. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. 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**. If you choose **OFF**, no other options need to be configured.
- 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.
- 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**, which does not apply

11. Click **Save** to save the policy.

WiFi device policy

Sep 06, 2017

You create new or edit existing WiFi device policies in XenMobile by using the **Configure > Device Policies** page. WiFi policies let 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

You can configure WiFi settings for users for the following platforms. Each platform requires a different set of values, which are described in detail in this article.

iOS settings

macOS settings

Android settings (includes devices enabled for Android for Work)

Windows Phone settings

Windows Desktop/Tablet settings

Important

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.

For more information, see Authentication and its subarticles.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add a New Policy** dialog box appears.

3. Click **WiFi**. The **WiFi Policy** page appears.

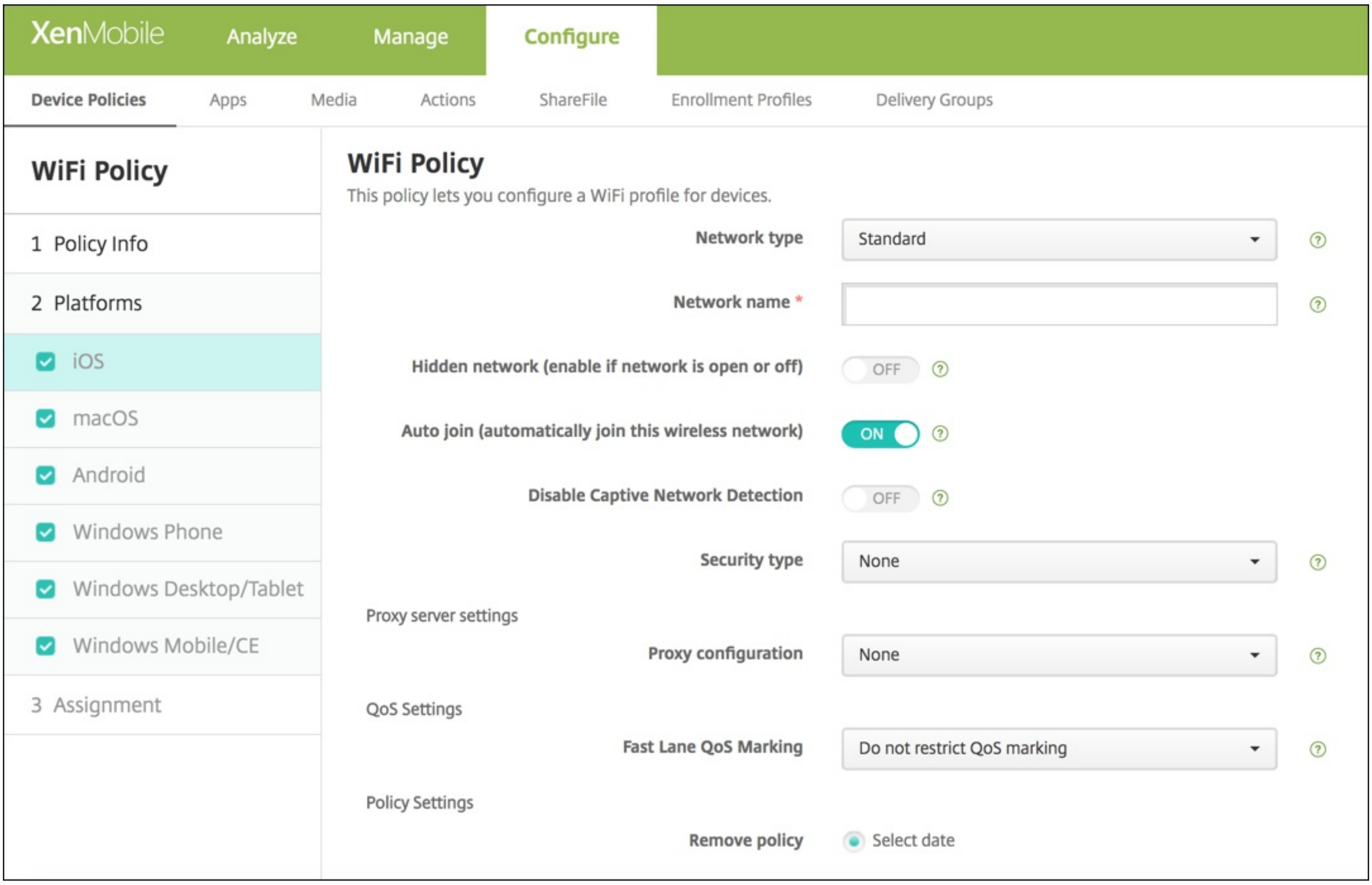
4. In the **Policy Information** pane, type the following information:

- **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 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, refer to Step 7 to set deployment rules for that platform.



WiFi Policy

This policy lets you configure a WiFi profile for devices.

Network type	Standard
Network name *	
Hidden network (enable if network is open or off)	OFF
Auto join (automatically join this wireless network)	ON
Disable Captive Network Detection	OFF
Security type	None
Proxy server settings	
Proxy configuration	None
QoS Settings	
Fast Lane QoS Marking	Do not restrict QoS marking
Policy Settings	
Remove policy	● Select date

Configure these 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. 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. XenMobile 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)

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)

Note: 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 XenMobile.
      - **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**.

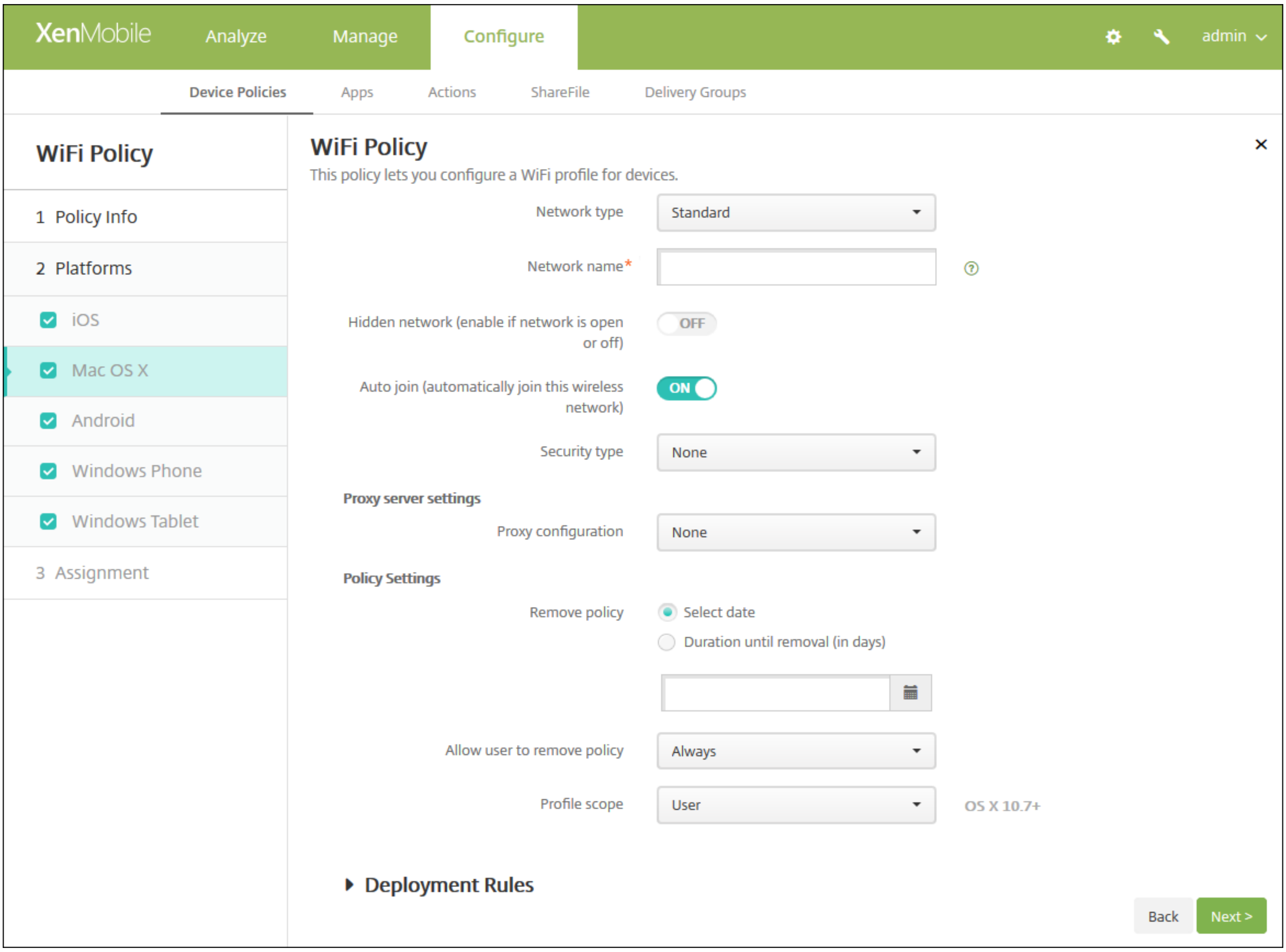
      To delete an item, hover over the line containing the listing and click the trash icon on the right side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

      To edit an item, hover over the line containing the listing and click the pen icon on the right side. Update the listing and then click **Save**.

- **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**. This option is available only on iOS 7.0 and later.

- Policy Settings
  - Next to **Remove policy**, choose either **Select date** or **Duration until removal (in hours)**.
  - If you choose **Select date**, click the calendar to choose the specific date for removal.
  - In the **Allow user to remove policy** list, choose **Always**, **Password required**, or **Never**.
  - If you choose **Password required**, next to **Removal password**, type the necessary password.



WiFi Policy

This policy lets you configure a WiFi profile for devices.

Network type: Standard

Network name*:

Hidden network (enable if network is open or off): OFF

Auto join (automatically join this wireless network): ON

Security type: None

Proxy server settings

Proxy configuration: None

Policy Settings

Remove policy: ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always

Profile scope: User OS X 10.7+

Configure these 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. 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)

- **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)

Note: 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 XenMobile.
      - **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**.

      To delete an item, hover over the line containing the listing and click the trash icon on the right side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

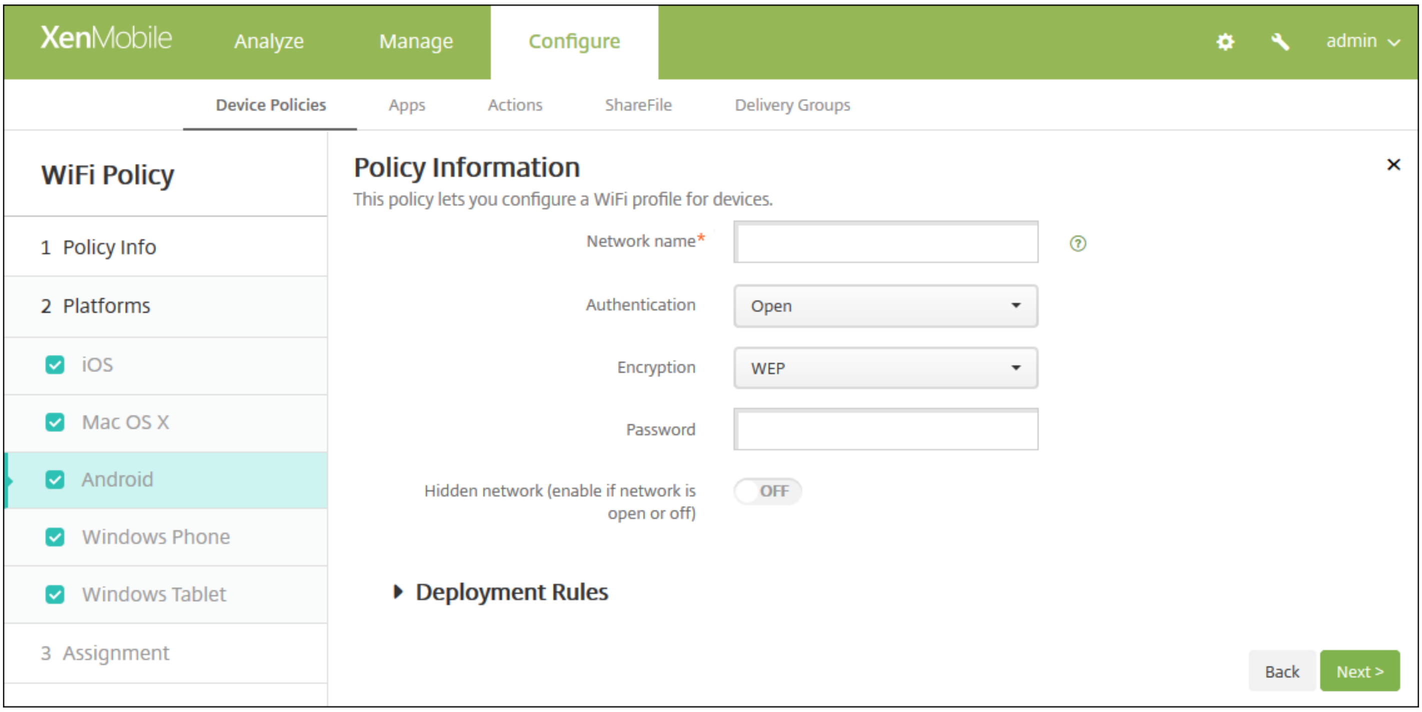
      To edit an item, hover over the line containing the listing and click the pen icon on the right side. Update the listing and then click **Save**.

- **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**. This option is available only on iOS 7.0 and later.

- Policy Settings
  - Next to **Remove policy**, choose either **Select date** or **Duration until removal (in hours)**.
  - If you choose **Select date**, click the calendar to choose the specific date for removal.
  - In the **Allow user to remove policy** list, choose **Always**, **Password required**, or **Never**.
  - If you choose **Password required**, next to **Removal password**, type the necessary password.
  - Next to **Profile scope**, choose either **User** or **System**. The default is **User**. This option is available only for macOS 10.7 and later.



Policy Information

This policy lets you configure a WiFi profile for devices.

Network name*

Authentication: Open

Encryption: WEP

Password

Hidden network (enable if network is open or off): OFF

Configure these 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.

Open, Shared

- **Encryption**: In the list, choose either **Disabled** or **WEP**. The default is **WEP**.
- **Password**: Type an optional password.

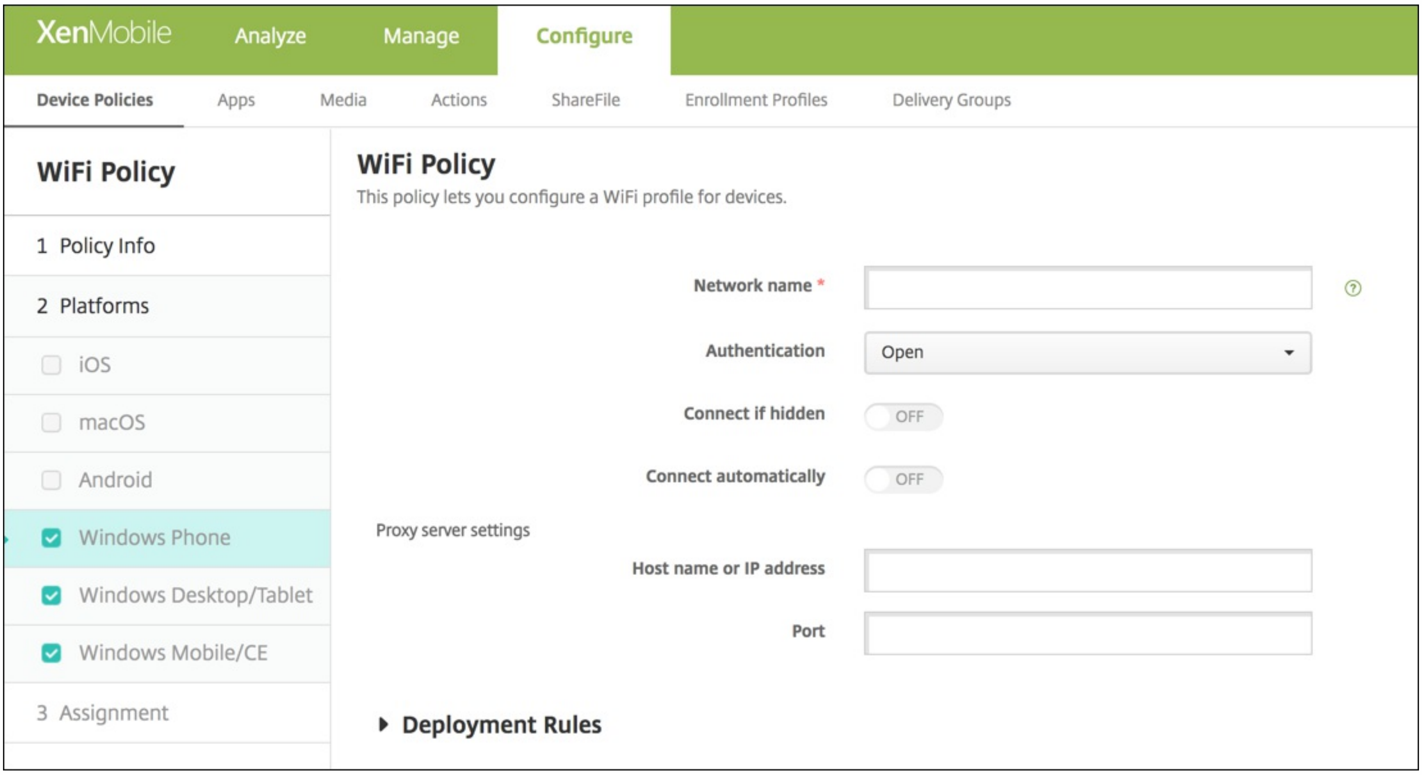
WPA, WPA-PSK, WPA2, WPA2-PSK

- **Encryption**: In the list, choose either **TKIP** or **AES**. The default is **TKIP**.
- **Password**: Type an optional password.

802.1x

- **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.



WiFi Policy

This policy lets you configure a WiFi profile for devices.

Network name *

Authentication: Open

Connect if hidden: OFF

Connect automatically: OFF

Proxy server settings

Host name or IP address

Port

Configure these 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 XenMobile 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

- **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

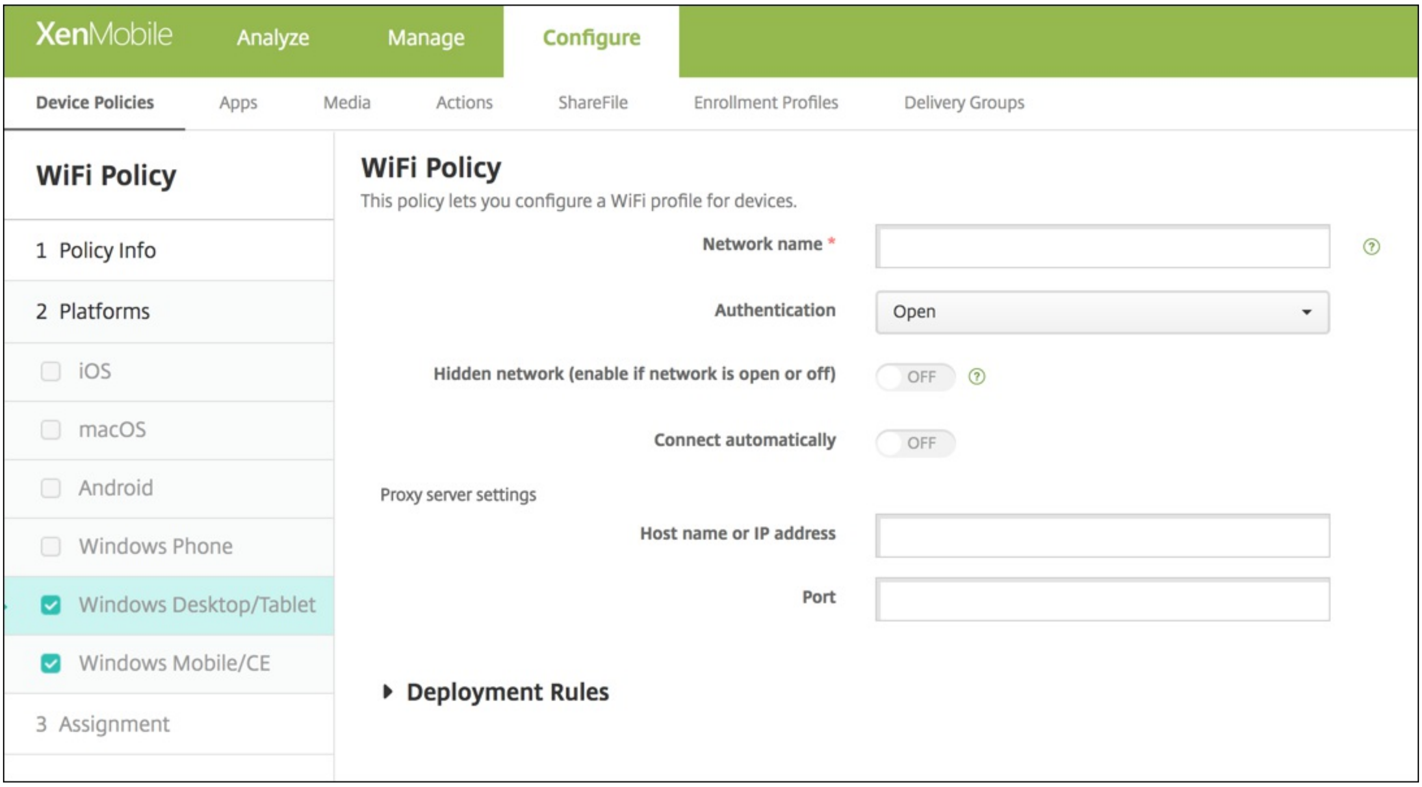
- **Encryption**: In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **Connect if hidden**: Choose whether to connect when the network is hidden.
- **Connect automatically**: Choose whether to connect to the network automatically.

WPA-2 Enterprise

- **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.



WiFi Policy

This policy lets you configure a WiFi profile for devices.

Network name *

Authentication: Open

Hidden network (enable if network is open or off): OFF

Connect automatically: OFF

Proxy server settings

Host name or IP address

Port

Configure the following settings:

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 XenMobile 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

- **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.

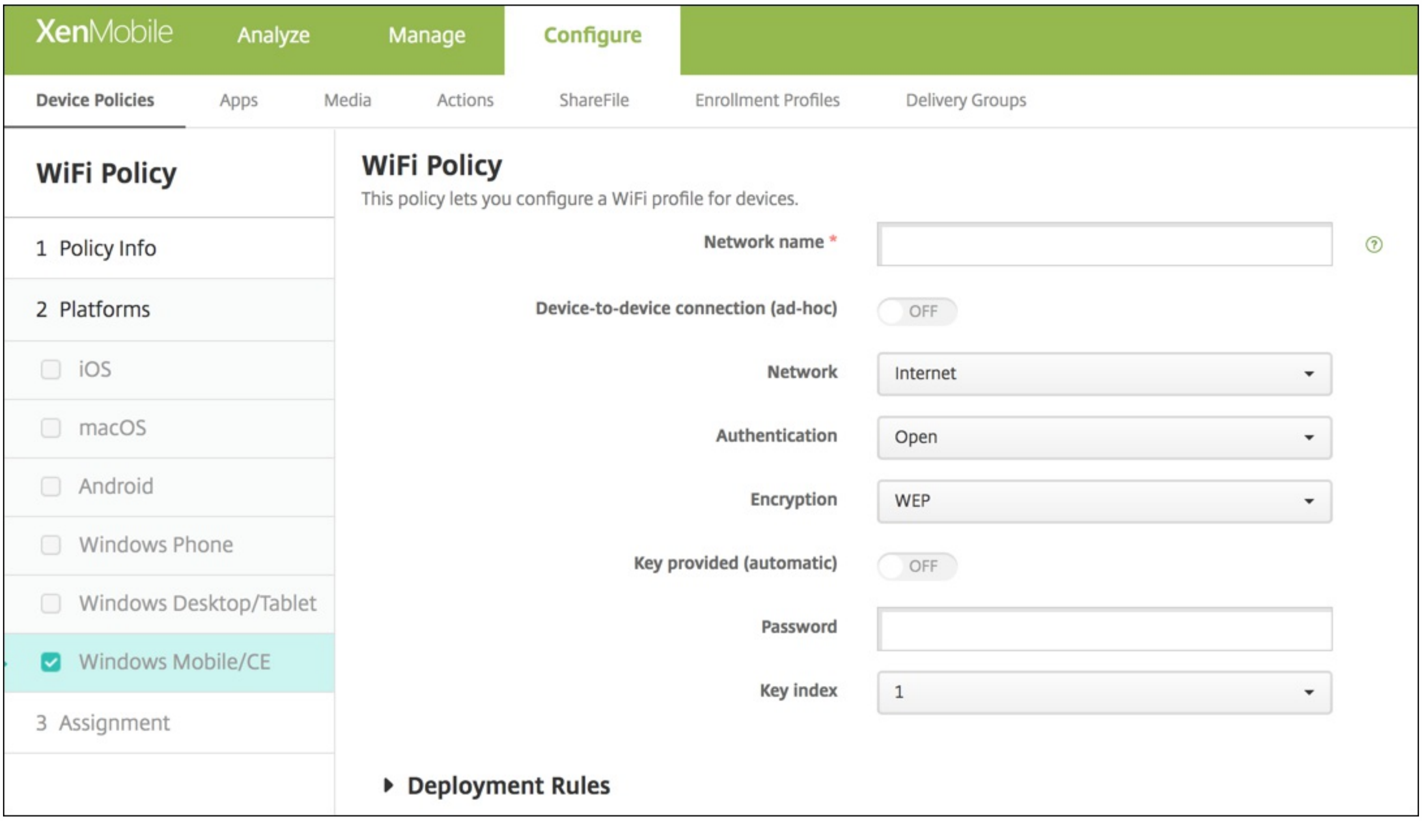
WPA Personal, WPA-2 Personal

- **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

- **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**.



WiFi Policy

This policy lets you configure a WiFi profile for devices.

Network name *	
Device-to-device connection (ad-hoc)	OFF
Network	Internet
Authentication	Open
Encryption	WEP
Key provided (automatic)	OFF
Password	
Key index	1

▸ Deployment Rules

Configure these 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 WiFi 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

- **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

- **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

- **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**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Windows CE certificate device policy

Sep 06, 2017

You can create a device policy in XenMobile to create and deliver Windows Mobile/CE certificates from an external PKI to users' devices. See Certificates for more information about Certificates and PKI entities.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add New Policy** dialog box appears.

3. Expand **More** and then, under **Security**, click **Windows CE Certificate**. The **Windows CE Certificate Policy** information page appears.

4. In the **Policy Information** pane, type the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Windows CE Certificate Policy Platform** information page appears.

6. Configure these 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%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name**: Type the name of the credential file.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

8. Click **Next**. The **Windows CE Certificate Policy** assignment page appears.

9. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. 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**. If you choose **OFF**, no other options need to be configured.
- 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.
- 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**, which does not apply to iOS.

11. Click **Save**.

Windows Information Protection device policy

Sep 06, 2017

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.

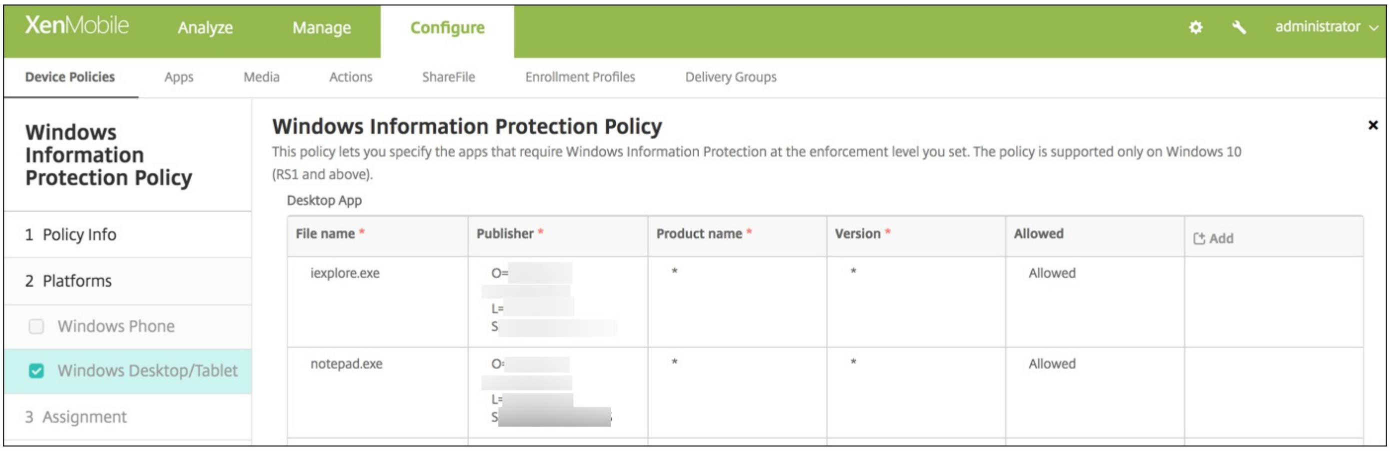
You can create a device policy in XenMobile to specify the apps that require Windows Information Protection at the enforcement level you set. The Windows Information Protection policy is for Windows 10 version 1607 and later supervised Phone, Tablet, and Desktop.

XenMobile 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 XenMobile.

1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.
2. Click **Add**. The **Add a New Policy** dialog box appears.
3. Start typing **Windows Information Protection** and then click that name in the search results. The Windows Information Protection **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 **Policy Platforms** pane appears.
6. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.



Windows Information Protection Policy

This policy lets you specify the apps that require Windows Information Protection at the enforcement level you set. The policy is supported only on Windows 10 (RS1 and above).

Desktop App

File name *	Publisher *	Product name *	Version *	Allowed

iexplore.exe	O=[redacted]
	L=[redacted]
	S[redacted]
		*	*	Allowed

notepad.exe	O=[redacted]
	L=[redacted]
	S[redacted]
		*	*	Allowed

Configure the settings for each platform that you choose:

- **Desktop App** (Windows 10 Tablet), **Store App** (Windows 10 Phone and Tablet): XenMobile 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. XenMobile 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:
  10.0.0.0-10.255.255.255, 2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff

- **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 WiFi 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:
  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. Defaults to **OFF**.

Note

For general information about configuring policies, see Add a device policy.

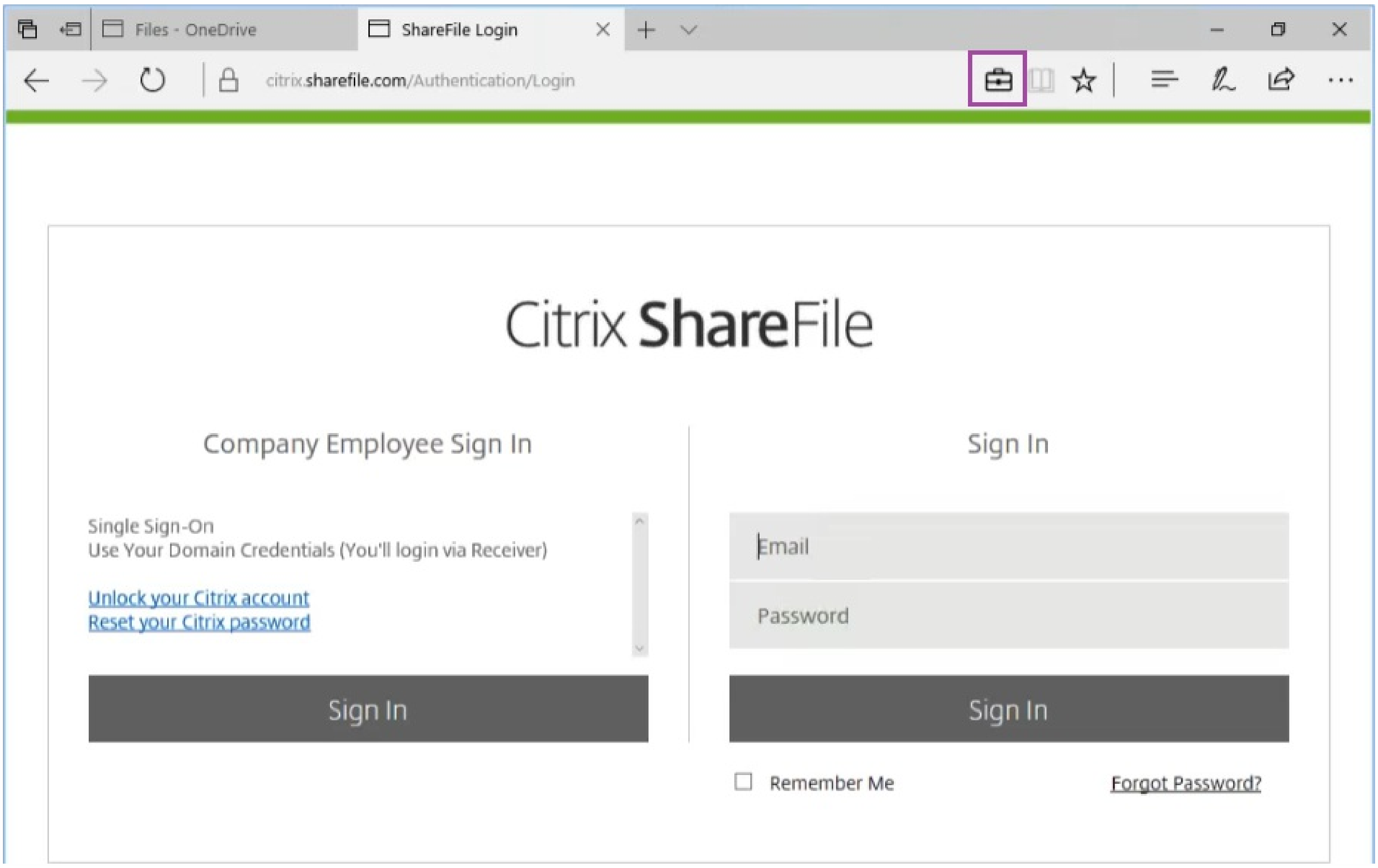
A data recover certificate is required to enable the **Windows Information Protection** policy.

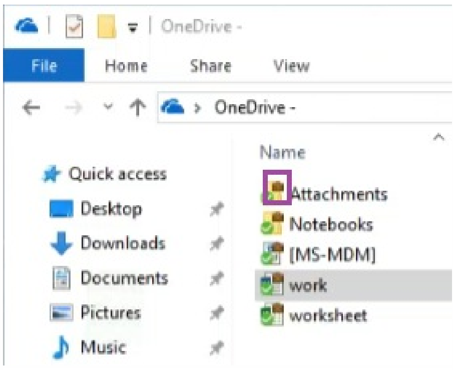
1. On the XenMobile Server, open a command prompt and navigate to a folder (other than Windows\System32) where you want to create a certificate.
2. Run this command:

   cipher /r:ESFDRA
3. When prompted, enter a password to protect the private key file.

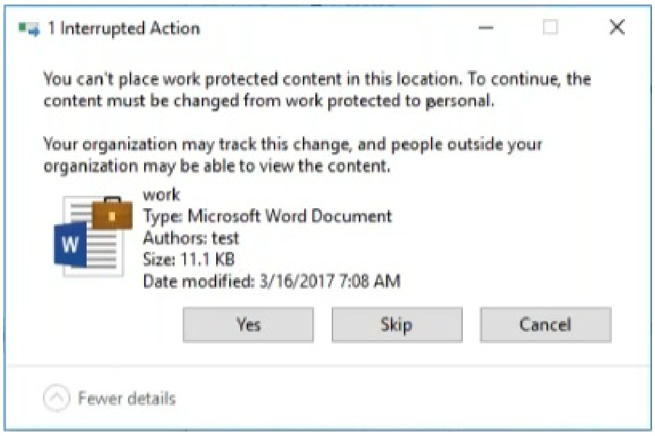
   The cipher command creates a .cer and a .pfx file.
4. In the XenMobile console, go to **Settings > Certificates** and import the .cer file, which applies to both Windows 10 tablets and phones.

When Windows Information Protection is in effect, apps and files include an icon:


Files - OneDrive
ShareFile Login
citrix.sharefile.com/Authentication/Login
Citrix ShareFile
Company Employee Sign In
Single Sign-On
Use Your Domain Credentials (You'll login via Receiver)
Unlock your Citrix account
Reset your Citrix password
Sign In
Sign In
Email
Password
Sign In
□ Remember Me
Forgot Password?



If a user copies or saves a protected file to a non-protected location, the following notification appears, depending on the enforcement level configured.



You can't place work protected content in this location. To continue, the content must be changed from work protected to personal.

Your organization may track this change, and people outside your organization may be able to view the content.

work
Type: Microsoft Word Document
Authors: test
Size: 11.1 KB
Date modified: 3/16/2017 7:08 AM

XenMobile options device policy

Sep 06, 2017

You add a XenMobile options policy to configure Secure Hub behavior when connecting to XenMobile from Android and Windows Mobile/CE devices.

1. In the XenMobile 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 **XenMobile agent**, click **XenMobile Options**. The **XenMobile Options Policy** page appears.

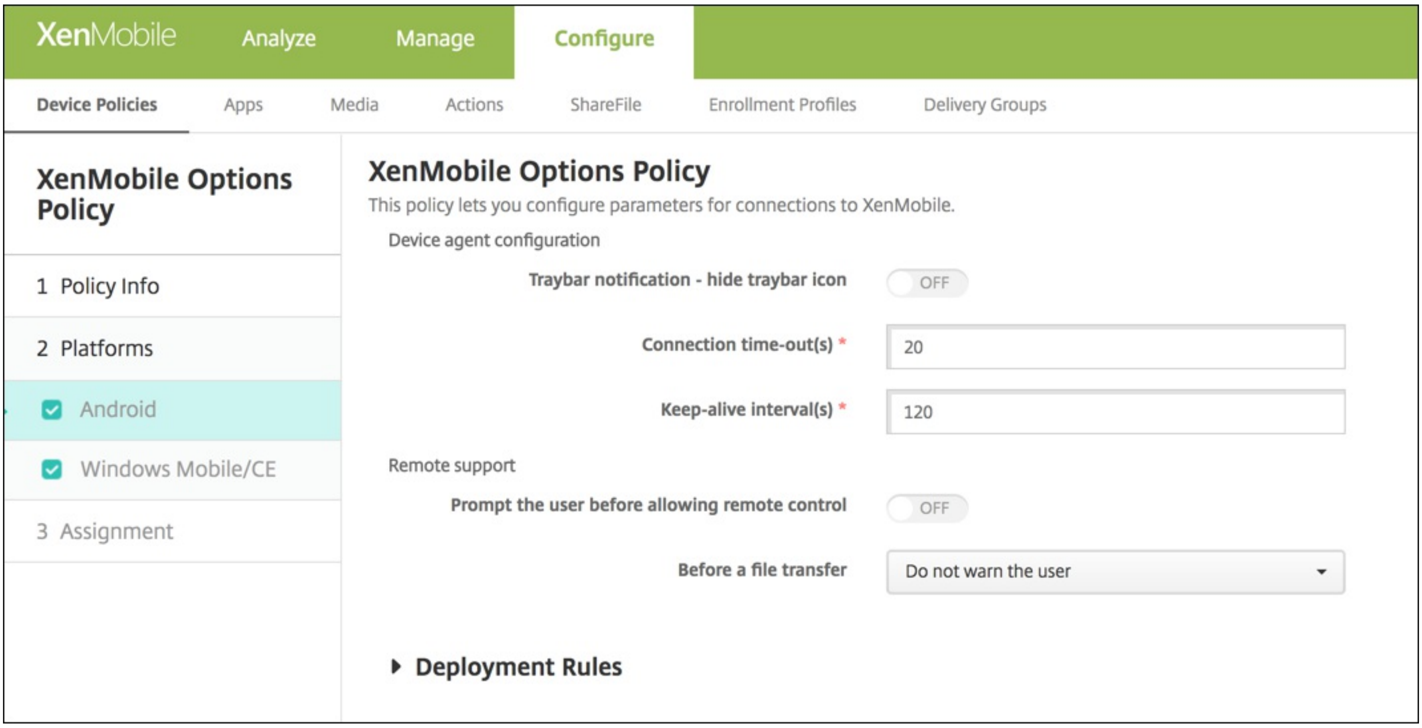
4. In the **Policy Information** pane, enter the following information:

- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

5. Click **Next**. The **Policy 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, refer to Step 7 for how to set that platform's deployment rules.



XenMobile Options Policy

This policy lets you configure parameters for connections to XenMobile.

Device agent configuration

Traybar notification - hide traybar icon: OFF

Connection time-out(s) *: 20

Keep-alive interval(s) *: 120

Remote support

Prompt the user before allowing remote control: OFF

Before a file transfer: Do not warn the user

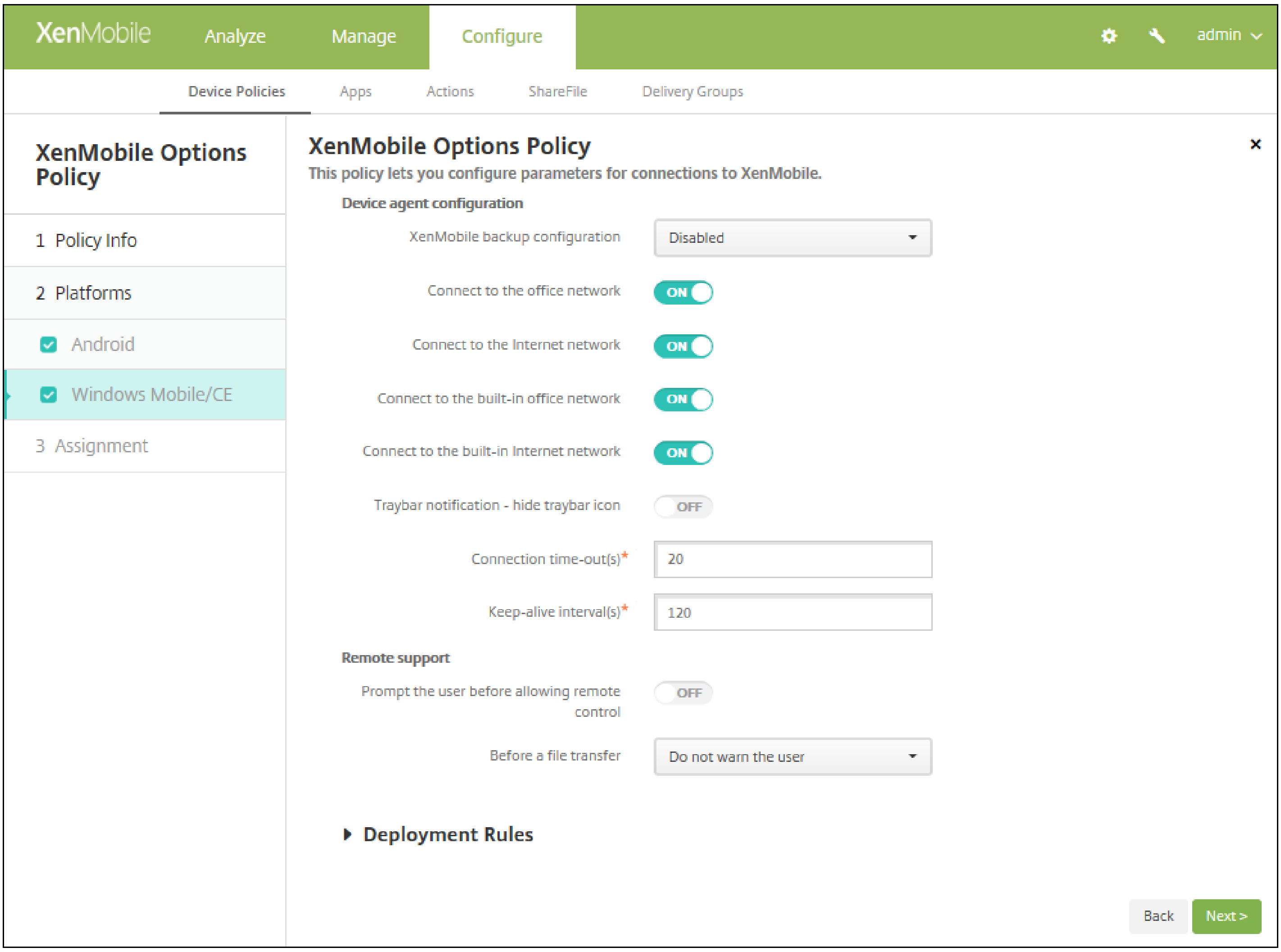
▸ Deployment Rules

Configure these 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**.



XenMobile Options Policy

This policy lets you configure parameters for connections to XenMobile.

Device agent configuration

XenMobile backup configuration: Disabled

Connect to the office network: ON

Connect to the Internet network: ON

Connect to the built-in office network: ON

Connect to the built-in Internet network: ON

Traybar notification - hide traybar icon: OFF

Connection time-out(s)*: 20

Keep-alive interval(s)*: 120

Remote support

Prompt the user before allowing remote control: OFF

Before a file transfer: Do not warn the user

Configure these settings:

- Device agent configuration
  - **XenMobile backup configuration**: In the list, click an option for backing up the XenMobile configuration on the users' devices. The default is **Disabled**. Available options are:
    - Disabled
    - At first connection after XenMobile installation
    - At 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**, XenMobile automatically detects the network.
  - **Connect to the built-in Internet network**: When set to **ON**, XenMobile automatically detects the network.
  - **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.
- 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**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

XenMobile uninstall device policy

Sep 06, 2017

You can add a device policy in XenMobile to uninstall XenMobile from Android and Window Mobile/CE devices. When deployed, this policy removes XenMobile from all devices in the deployment group.

1. In the XenMobile 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 **XenMobile agent**, click **XenMobile Uninstall**. The **XenMobile Uninstall Policy** 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 **Policy Platforms** information 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, refer to Step 7 for how to set that platform's deployment rules.

Configure this setting for each platform you choose:

- **Uninstall XenMobile from devices**: Select whether to uninstall XenMobile from every device to which you deploy this policy. The default is **OFF**.

7. Configure deployment rules and choose delivery groups. For more information, see Add a device policy.

Add apps

Nov 01, 2017

Important

The MDX 10.7.5 release is the final release that supports the wrapping of XenMobile Apps. You cannot use the MDX Toolkit or the MDX Service 10.7.10 and later to wrap 10.7.5 or later versions of the XenMobile Apps. You must access XenMobile Apps from the public app stores.

You add apps to XenMobile for management. You add the apps to the XenMobile 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 XenMobile:

- **MDX**. These apps are wrapped with the MDX 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 the MDX Toolkit 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.

Note

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.

Important

The MDX 10.7.5 release is the final release that supports the wrapping of XenMobile Apps. You cannot use the MDX Toolkit or the MDX Service 10.7.10 and later to wrap 10.7.5 or later versions of the XenMobile Apps. You must access XenMobile Apps from the public app stores.

XenMobile supports iOS, Android, and Windows apps, including XenMobile Apps, such as Secure Hub, Secure Mail and Secure Web, and the use of MDX policies. Using the XenMobile console, you can upload apps and then deliver the apps to user devices. In addition to the XenMobile 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 XenMobile Apps for iOS and Android, follow these general steps:

1. Download the public-store MDX files from https://www.citrix.com/downloads/xenmobile/product-software/xenmobile-enterprise-edition-worx-apps-and-mdx-toolkit.html.

2. Upload those files to the XenMobile 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.

To distribute XenMobile Apps for Windows, follow these general steps:

1. Download the app files from Citrix.

2. Wrap the app files using the MDX Toolkit.

3. Upload the wrapped apps to the XenMobile console, modifying the MDX policies as needed.

4. Deliver the apps to user devices through delivery groups. For details, see Public App Store Delivery of XenMobile Apps in the XenMobile Apps documentation.

The MDX Toolkit wraps apps for iOS, Android, and Windows 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.

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

- XenMobile Server 10.6 (minimum version)
- Secure Hub 10.5.15 for iOS and 10.5.20 for Android (minimum versions)
- MDX Toolkit 10.6 (minimum version)
- Custom server property, force.server.push.required.apps

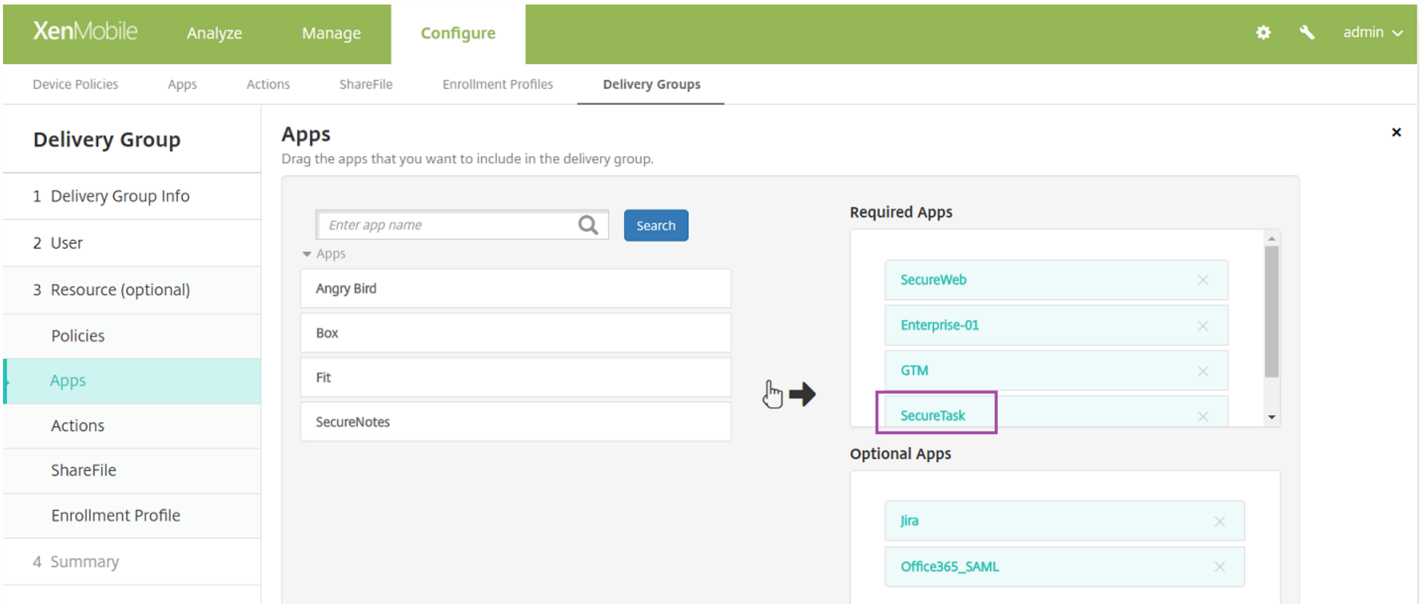
  The forced deployment of required apps is disabled by default. To enable the feature, create a Custom Key server property. Set the **Key** and **Display name** to **force.server.push.required.apps** and set the **Value** to **true**.

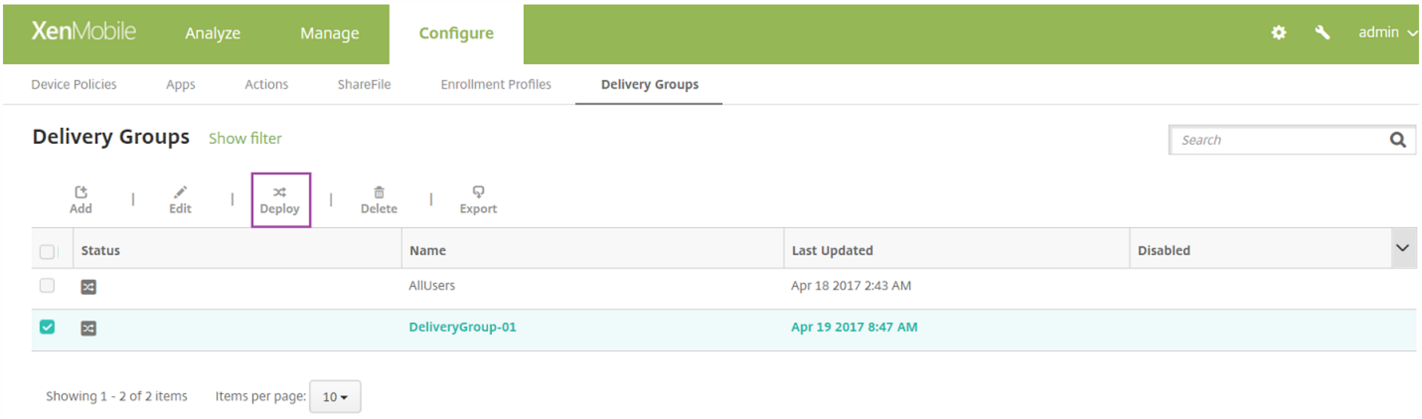
- After you upgrade XenMobile Server and Secure Hub: Users with enrolled devices must sign off and then sign on to

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.

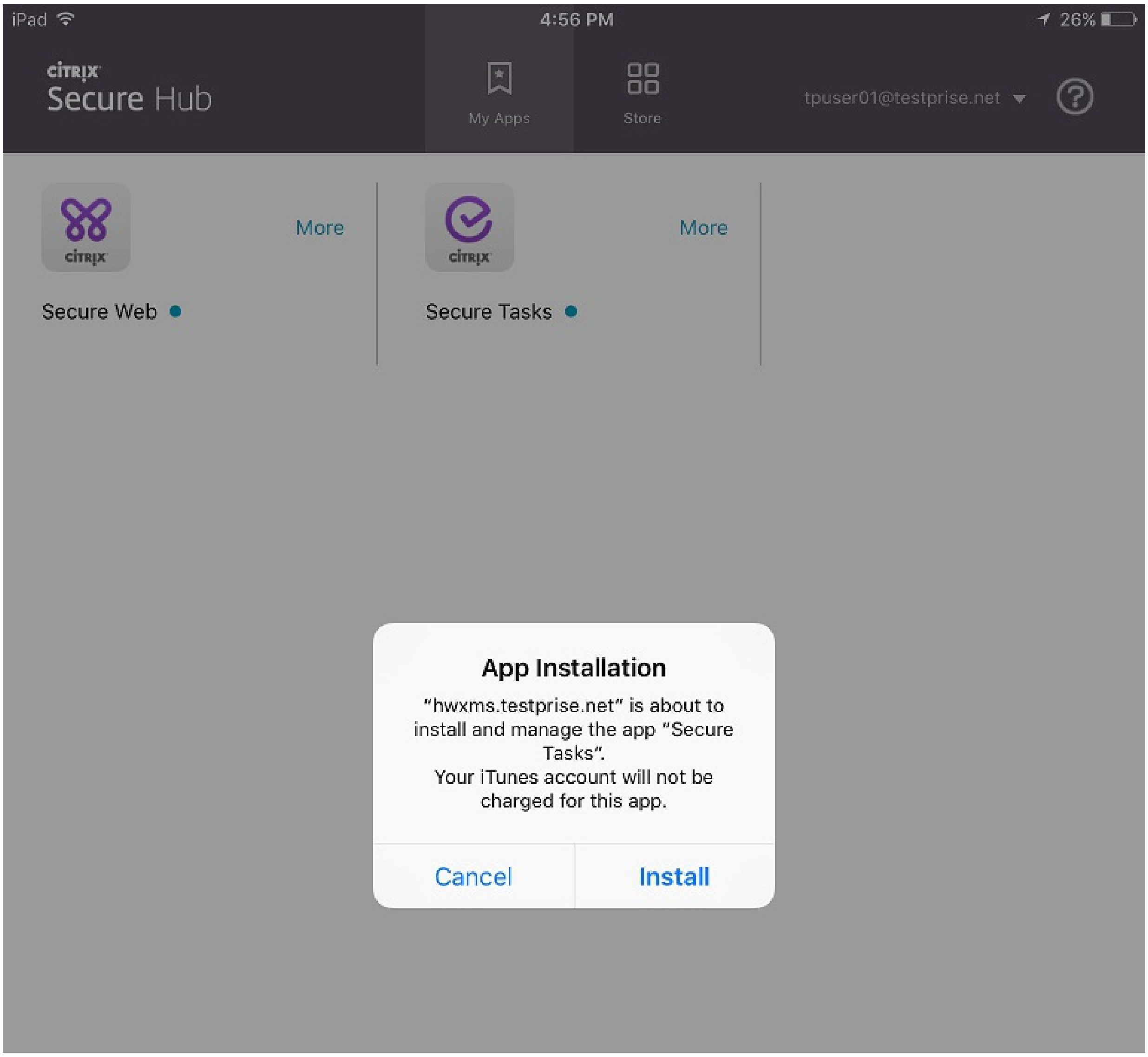




□	Status	Name	Last Updated	Disabled
□	☒	AllUsers	Apr 18 2017 2:43 AM	
☑	☒	DeliveryGroup-01	Apr 19 2017 8:47 AM	

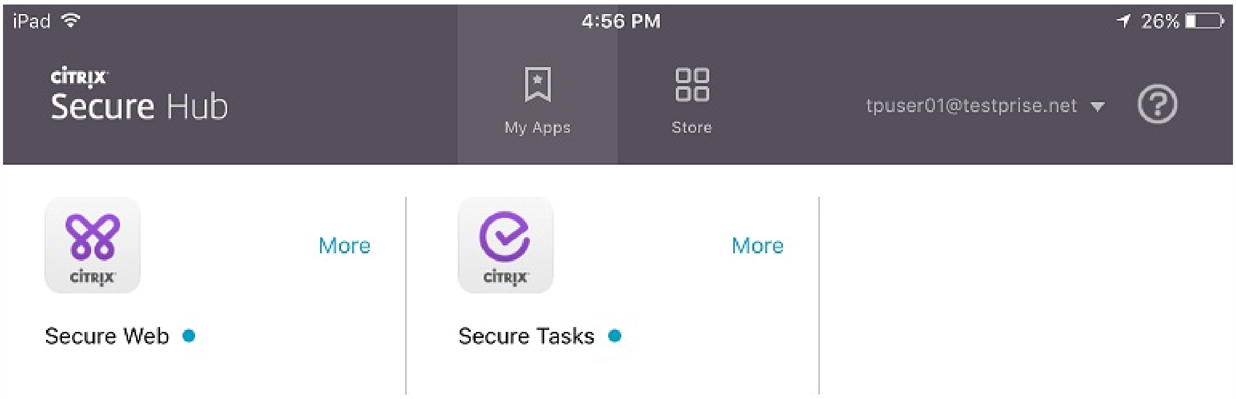
Showing 1 - 2 of 2 items Items per page: 10

After the sample app, Secure Tasks, deploys to the user device, Secure Hub prompts the user to install the app.



App Installation

"hwxms.testprise.net" is about to install and manage the app "Secure Tasks".
Your iTunes account will not be charged for this app.



Important

MDX-enabled required apps, including enterprise apps and public app store apps, upgrade immediately, 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 XenMobile App during initial enrollment. The required app is installed on the device.
2. Update the app on the XenMobile console.
3. Use the XenMobile 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 XenMobile App during initial enrollment. The required app is installed on the device.
2. Use the XenMobile 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 XenMobile App during initial enrollment. The required app is installed on the device.
2. Update the app on the XenMobile console.
3. Use the XenMobile 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.)

XenMobile 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. XenMobile includes Security Assertion Markup Language (SAML) connectors. SAML connectors are used for web applications that support SAML protocol for SSO and user account management. XenMobile supports SAML 1.1 and SAML 2.0.

You can also build your own enterprise SAML connectors.

For more information, see Add a Web or SaaS app in this article.

Enterprise applications typically reside in your internal network. Users can connect to the apps by using Secure Hub. When you add an enterprise app, XenMobile creates the app connector for it. For more information, see Add an enterprise app in this article.

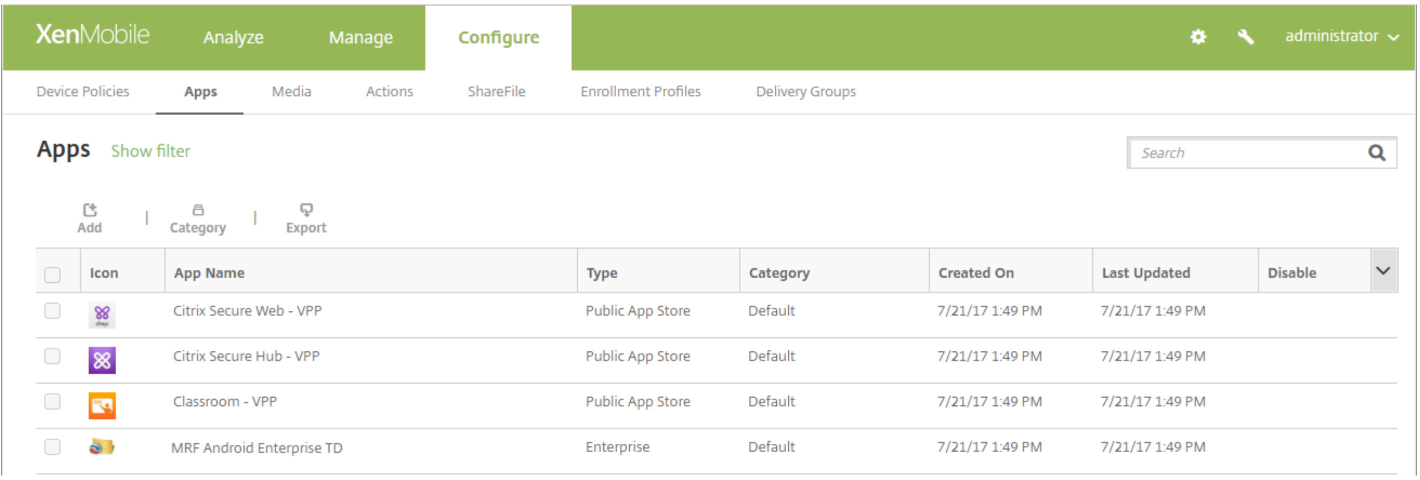
You can configure settings to retrieve app names and descriptions from the Apple App Store, Google Play, and the Windows Store. When you retrieve the app information from the store, XenMobile overwrites the existing name and description. For more information, see Add a public app store app in this article.

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 XenMobile Store. When users log on with Secure Hub, the link appears with the list of available apps and desktops. For more information, see Add a Web Link app in this article.

Add an MDX app

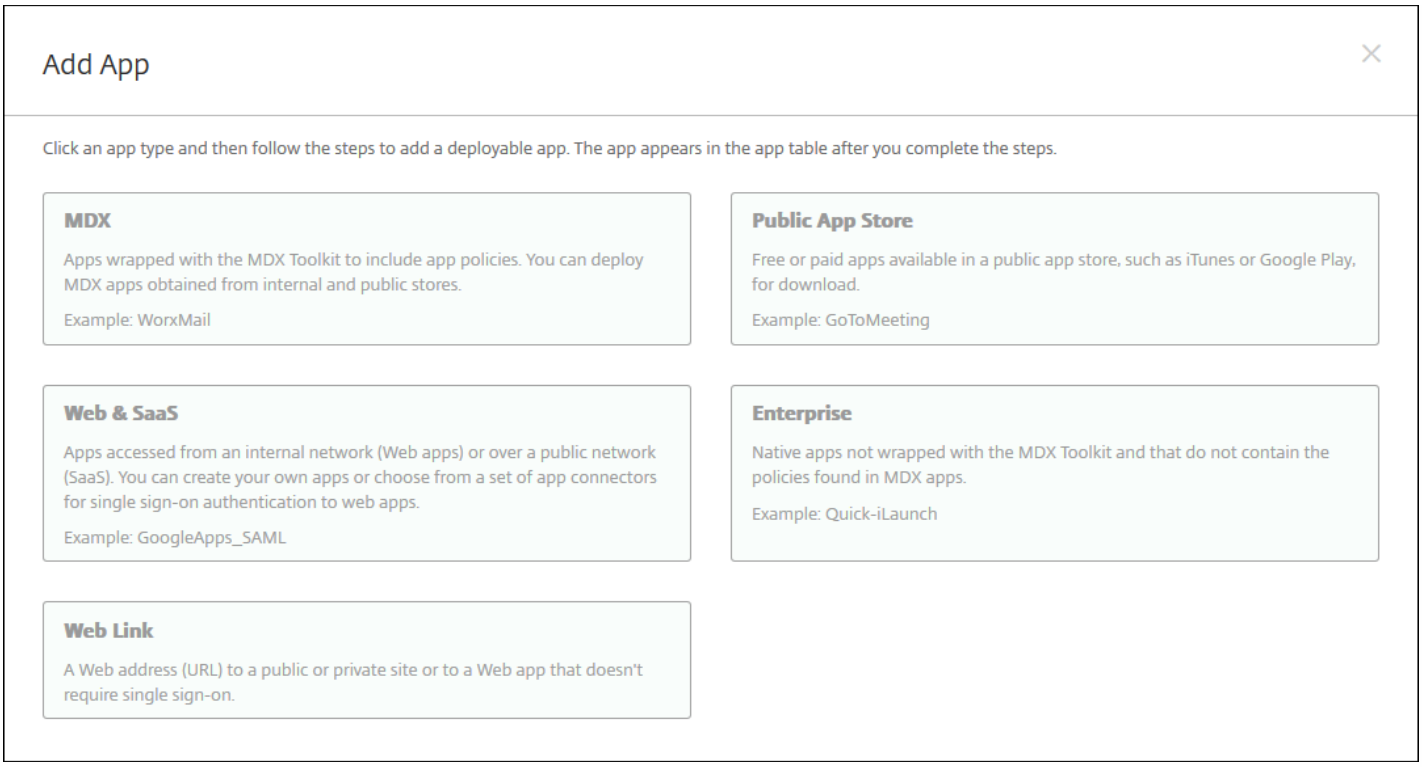
When you receive a wrapped MDX mobile app for an iOS, Android, or Windows Phone device, you can upload the app to XenMobile. After you upload the app, you can configure app details and policy settings. For more information about the app policies that are available for each device platform type, see MDX Policies at a Glance. Detailed policy descriptions also in that section.

1. In the XenMobile console, click **Configure** > **Apps**. The **Apps** page appears.



	Icon	App Name	Type	Category	Created On	Last Updated	Disable
□		Citrix Secure Web - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
□		Citrix Secure Hub - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
□		Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
□		MRF Android Enterprise TD	Enterprise	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	

2. Click **Add**. The **Add App** dialog box appears.



Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

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 web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

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 **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 11 for how to set the platform deployment rules.

7. Select an MDX file to upload by clicking **Upload** and navigating to the file location.

- If you are adding an iOS VPP B2B app, click **Your application is a VPP B2B application?**. Then, in the list, click the B2B VPP account to use.

8. Click **Next**. The app details page appears.

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.

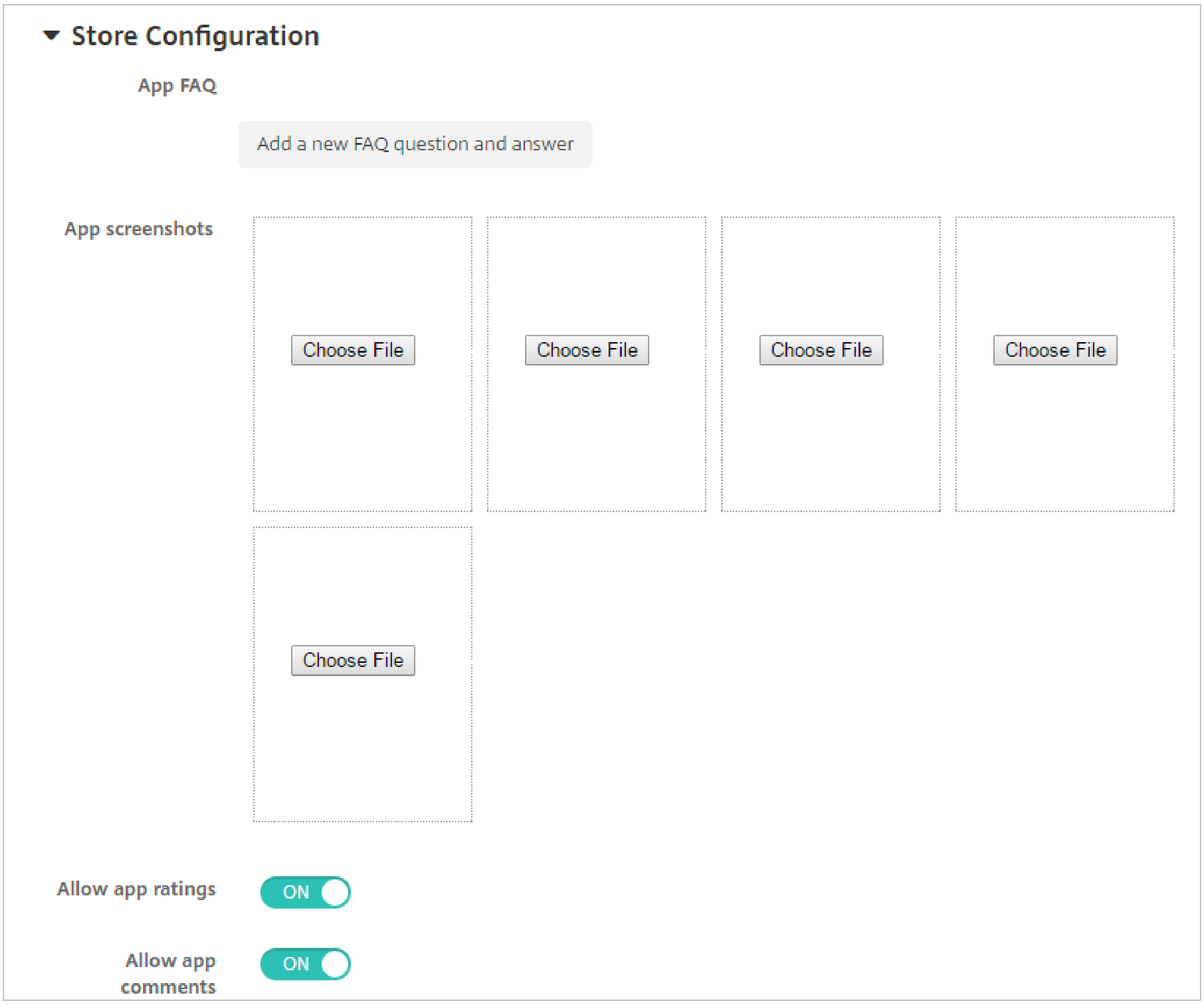
- **Excluded devices**: Optionally, type the manufacturer or models of devices that cannot run the app.
- **Remove app if MDM profile is removed**: Select whether to remove the app from a device when the MDM profile is removed. The default is **ON**.
- **Prevent app data backup**: Select whether to prevent users from backing up app data. The default is **ON**.
- **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**. Available in iOS 9.0 and later.
- **App deployed via VPP**: Select whether to deploy the app by using VPP. If **ON**, and you deploy an MDX version of the app and use VPP to deploy the app, Secure Hub shows only the VPP 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.

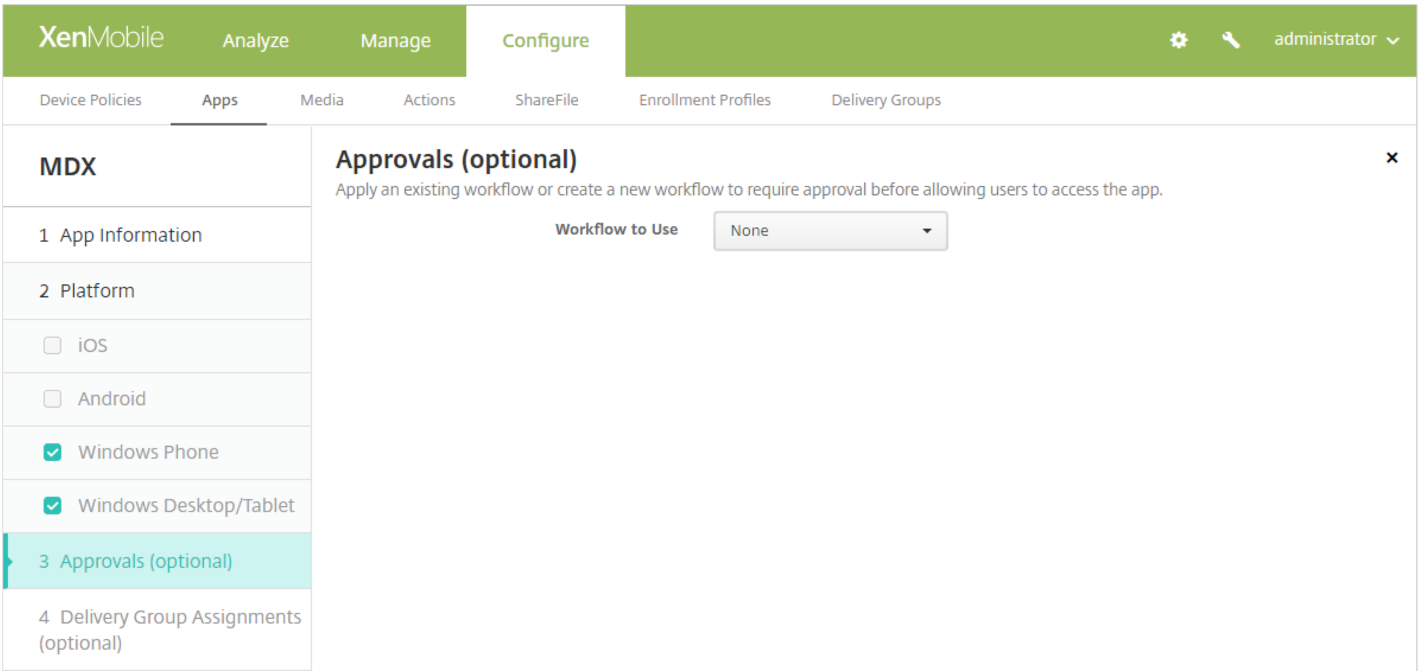
12. Expand **XenMobile Store Configuration**.



Optionally, you can add an FAQ for the app or screen captures that appear in the XenMobile 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 XenMobile 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.



Approvals (optional)

Apply an existing workflow or create a new workflow to require approval before allowing users to access the app.

Workflow to Use: None

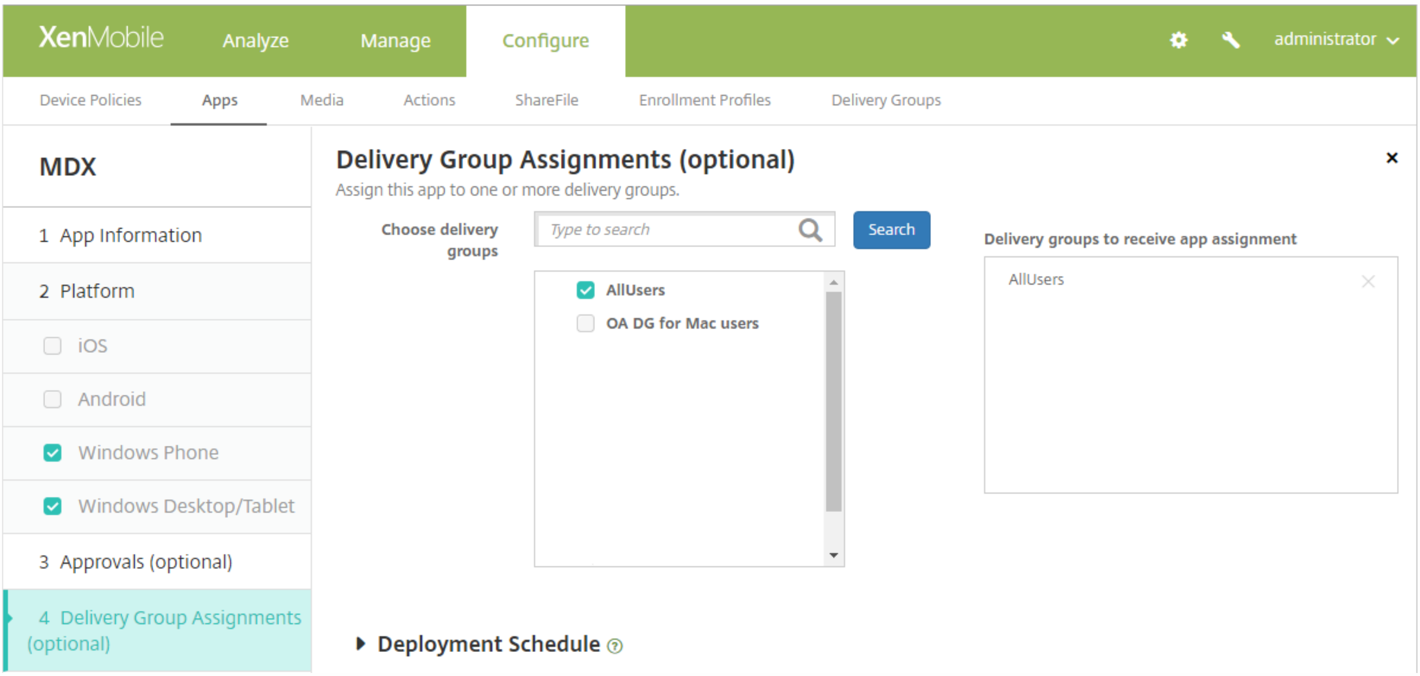
You use workflows when you need approval when creating user accounts. If you don't need to set up approval workflows, you can skip to Step 15.

Configure this setting if you need 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.



Delivery Group Assignments (optional)

Assign this app to one or more delivery groups.

Choose delivery groups

☑ AllUsers

□ OA DG for Mac users

Delivery groups to receive app assignment

AllUsers

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**.

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.

- 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**, which does not apply to iOS.

17. Click **Save**.

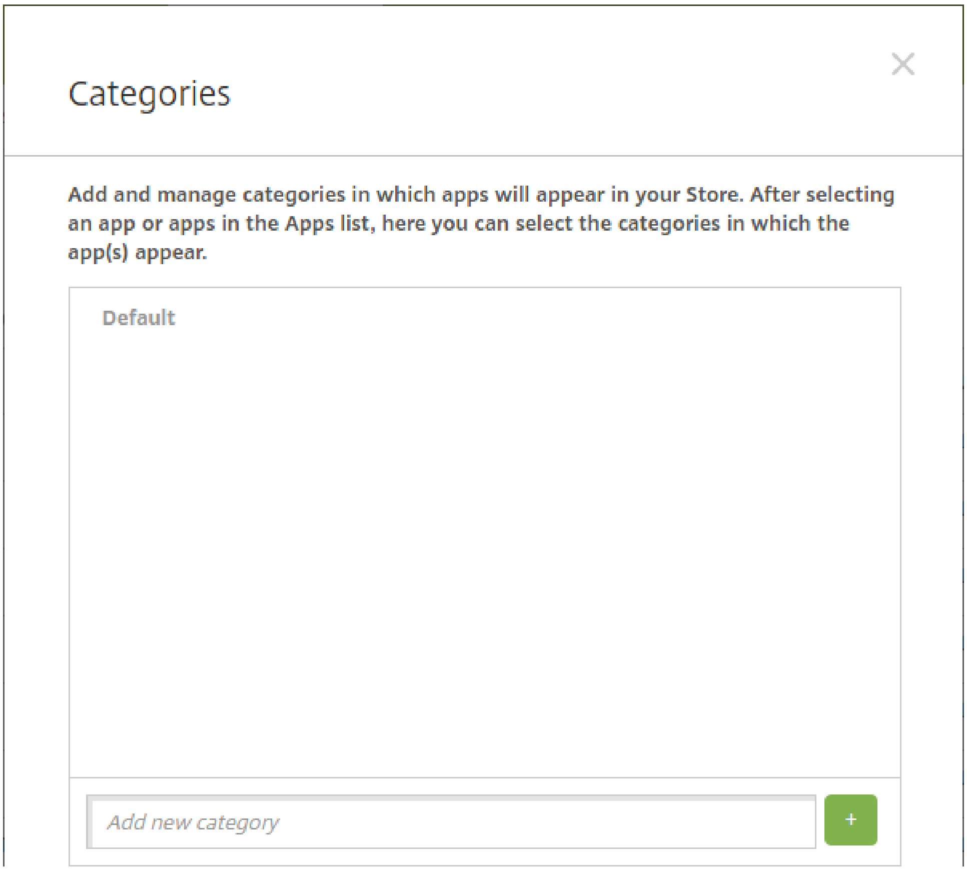
Create app categories

When users log on to Secure Hub, they receive a list of the apps, web links, and stores that you set up in XenMobile. 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 XenMobile 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 XenMobile console, click **Configure** > **Apps**. The **Apps** page appears.

2. Click **Category**. The **Categories** dialog box appears.



Categories

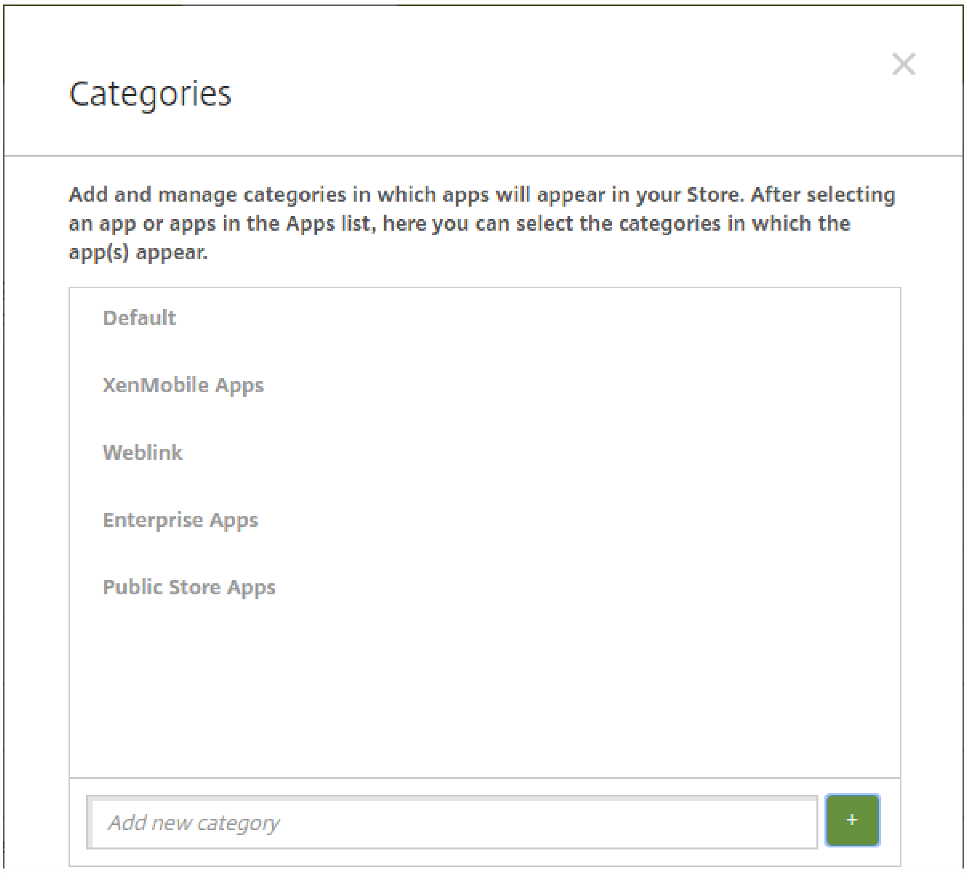
Add and manage categories in which apps will appear in your Store. After selecting an app or apps in the Apps list, here you can select the categories in which the app(s) appear.

Default

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.



Categories

Add and manage categories in which apps will appear in your Store. After selecting an app or apps in the Apps list, here you can select the categories in which the app(s) appear.

Default

XenMobile Apps

Weblink

Enterprise Apps

Public Store Apps

4. When you're done adding categories, close the **Categories** dialog box.

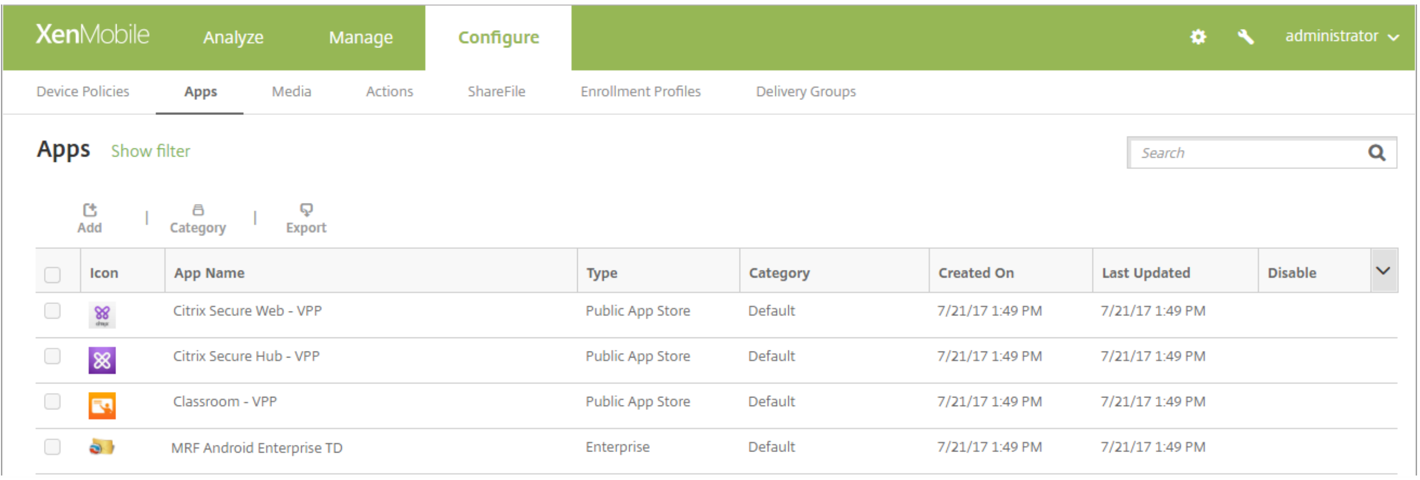
5. On the **Apps** page, you can place an existing app into a new category.

- 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

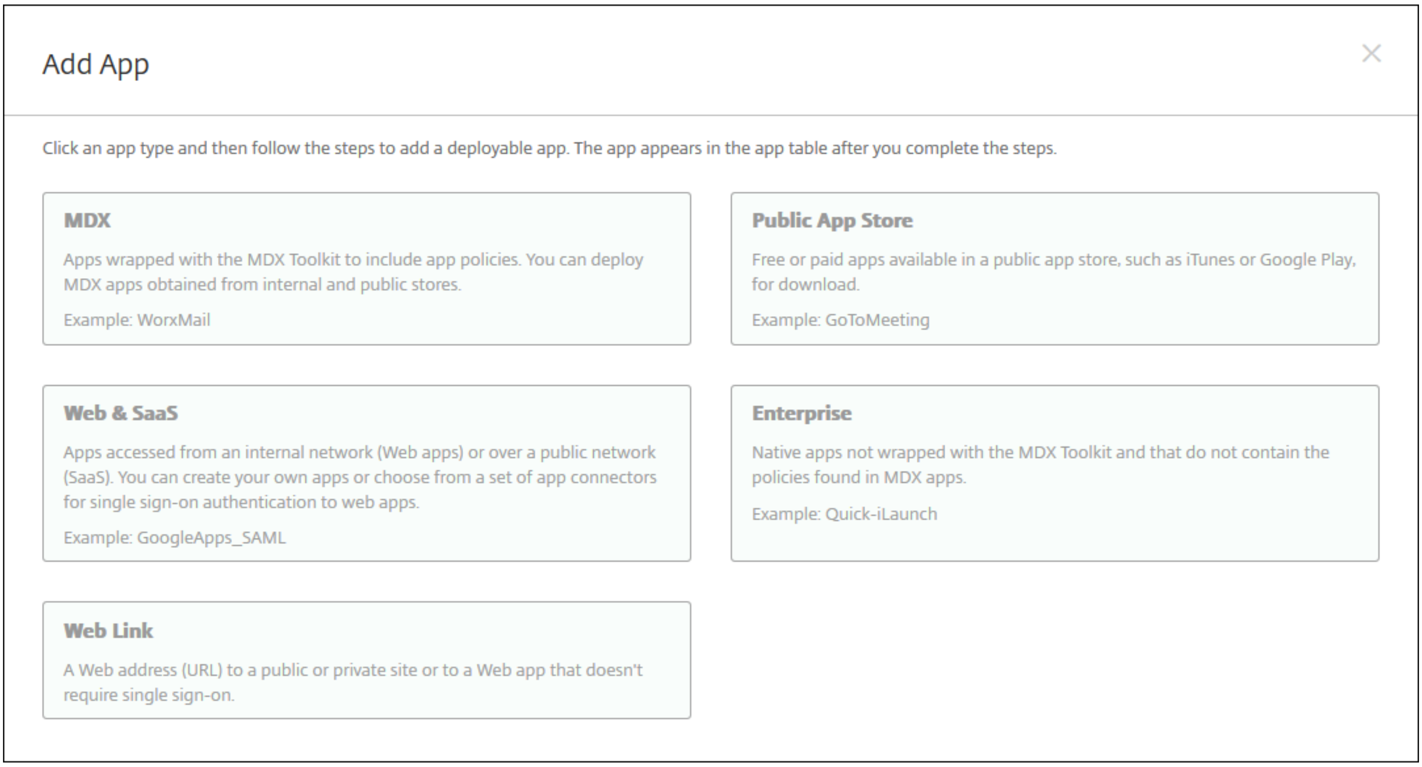
You can add free or paid apps to XenMobile that are available in a public app store, such as iTunes or Google Play. For example, GoToMeeting. Also, when you add a paid public app store app for an Android for Work, you can review the Bulk Purchase licensing status. That status is the total number of licenses available, the number currently in use, and the email address of each user consuming the licenses. The Bulk Purchase plan for Android for Work simplifies the process of finding, buying, and distributing apps and other data in bulk for an organization.

1. In the XenMobile console, click **Configure** > **Apps**. The **Apps** page appears.



☐	Icon	App Name	Type	Category	Created On	Last Updated	Disable
☐		Citrix Secure Web - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
☐		Citrix Secure Hub - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
☐		Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
☐		MRF Android Enterprise TD	Enterprise	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	

2. Click **Add**. The **Add App** dialog box appears.



Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

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 web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Click **Public App Store**. The **App Information** page appears.

4. On the **App Information** pane, type the following information:

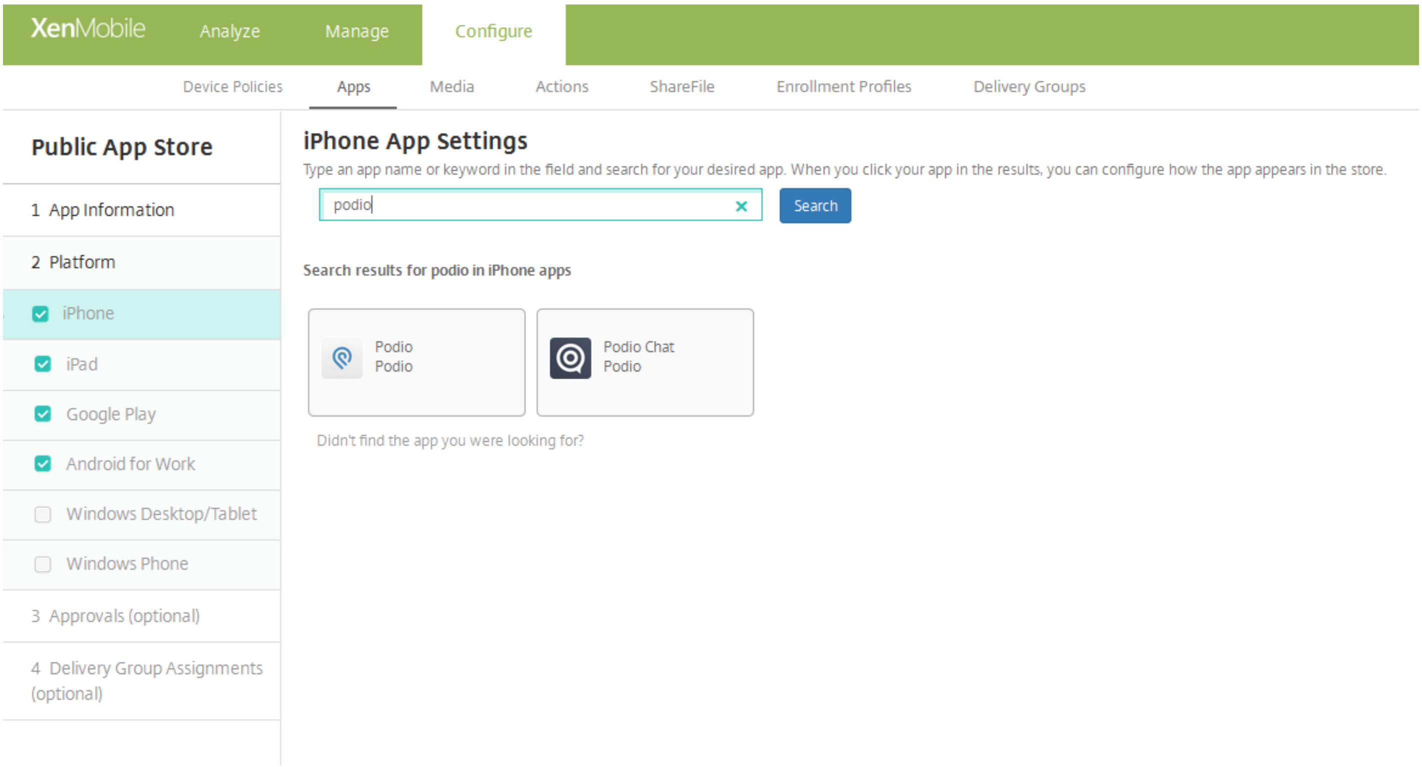
- **Name**: Type a descriptive name for the app. This name appears under **App Name** on the **Apps** table.
- **Description**: Type an optional description of the app.
- **App category**: Optionally, in the list, click the category to which you want to add the app. For more information about app categories, 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.

When you finish configuring the settings for a platform, see Step 10 for how to set the platform deployment rules.

7. Select an app to add by typing the app name in the search box and clicking **Search**. Apps matching the search criteria appear. The following figure shows the result of searching for **podio**.



Public App Store

1 App Information

2 Platform

- ☑ iPhone
- ☑ iPad
- ☑ Google Play
- ☑ Android for Work
- □ Windows Desktop/Tablet
- □ Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

iPhone App Settings

Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

podio ✕ Search

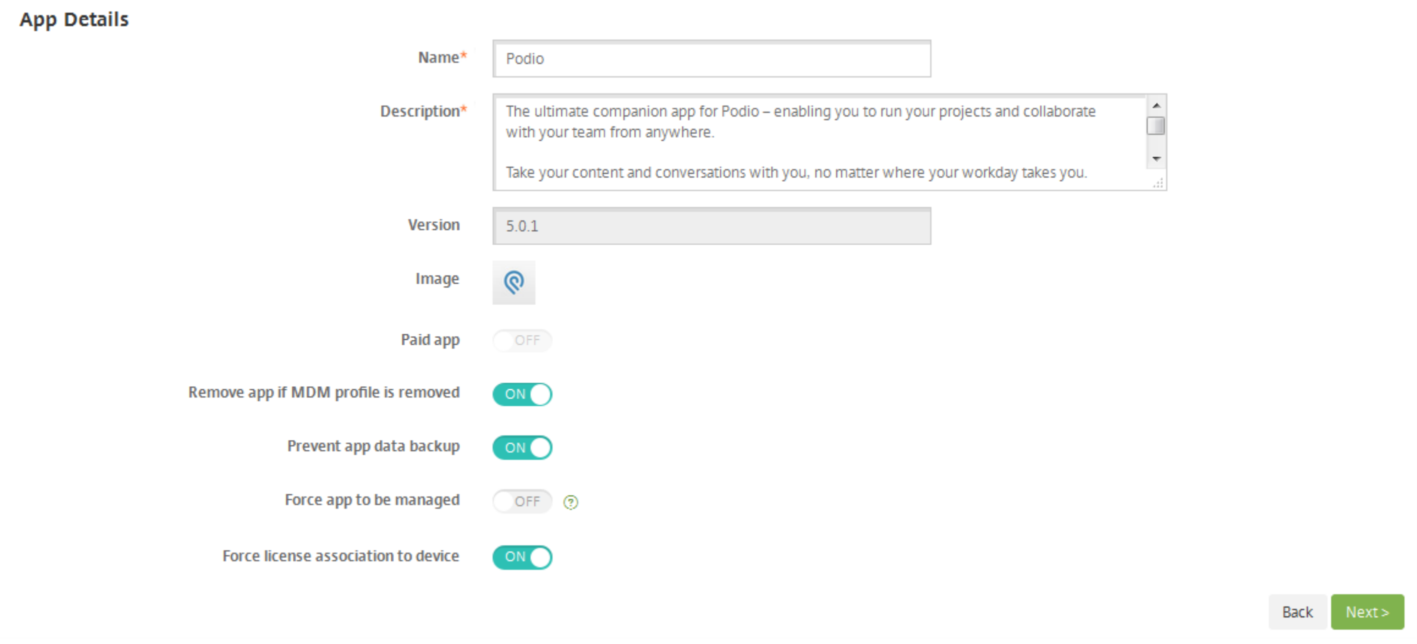
Search results for podio in iPhone apps

Podio
Podio

Podio Chat
Podio

Didn't find the app you were looking for?

8. Click the app you want to add. The **App Details** fields are pre-populated with information related to the chosen app (including the name, description, version number, and associated image).



App Details

Name*: Podio

Description*: The ultimate companion app for Podio – enabling you to run your projects and collaborate with your team from anywhere.

Take your content and conversations with you, no matter where your workday takes you.

Version: 5.0.1

Image

Paid app: OFF

Remove app if MDM profile is removed: ON

Prevent app data backup: ON

Force app to be managed: OFF

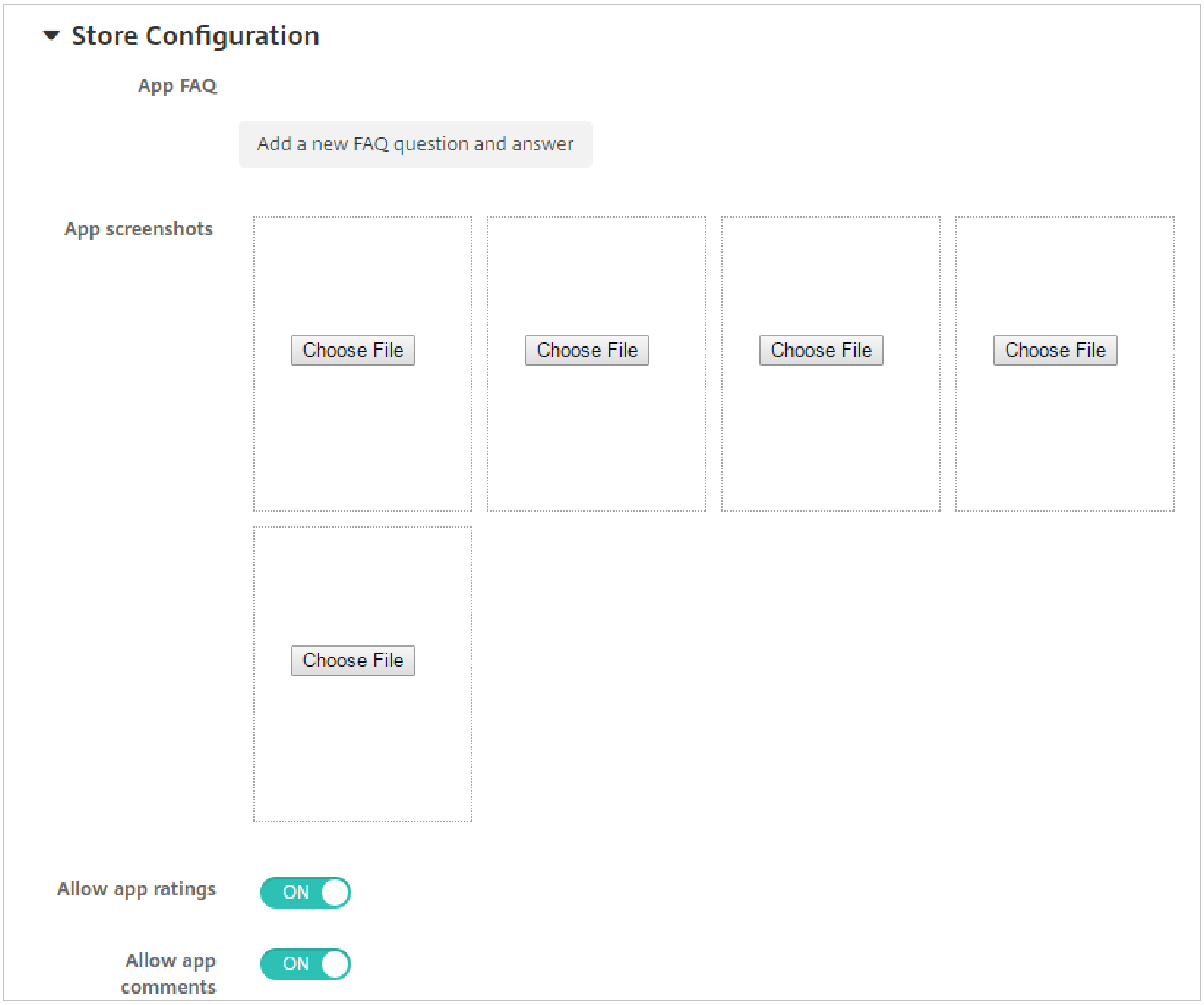
Force license association to device: ON

9. Configure these settings:

- If necessary, change the name and description for the app.
- **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**.
- **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**. Available in iOS 9.0 and later.
- **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. Available in iOS 9 and later. If the app you chose does not support assignment to a device, this field can't be changed.

10. Configure the deployment rules. For information, see Deploy resources.

11. Expand **XenMobile Store Configuration**.



Optionally, you can add an FAQ for the app or screen captures that appear in the XenMobile 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 XenMobile 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.

12. Expand **Volume Purchase Program** or, for Android for Work, expand **Bulk Purchase**.

For the Volume Purchase Program, complete the following steps.

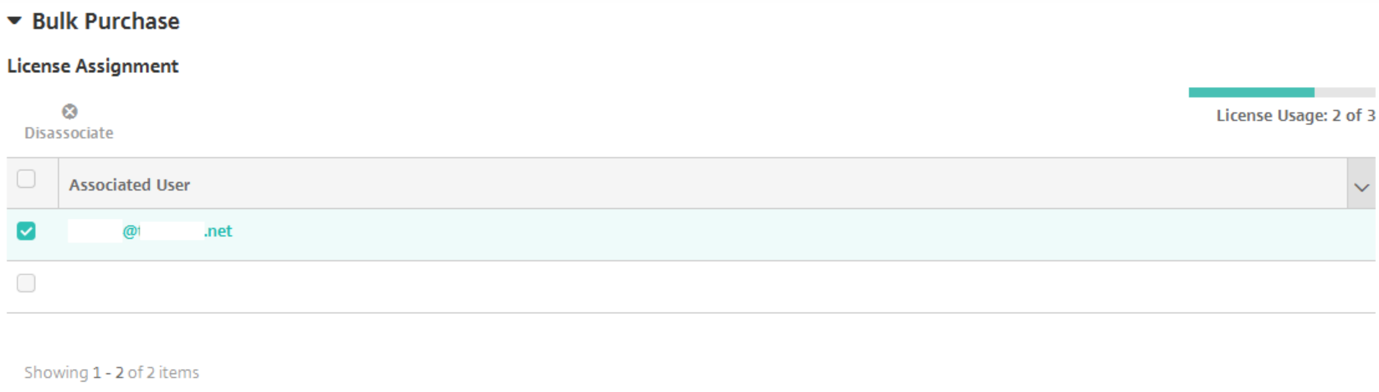
a. In the **VPP license** list, click **Upload a VPP license** file if you want to enable XenMobile to apply a VPP license for the app.

b. In the dialog box that appears, import the license.

For Android for Work 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 for Work, 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.



▾ Bulk Purchase

License Assignment

⊗ Disassociate

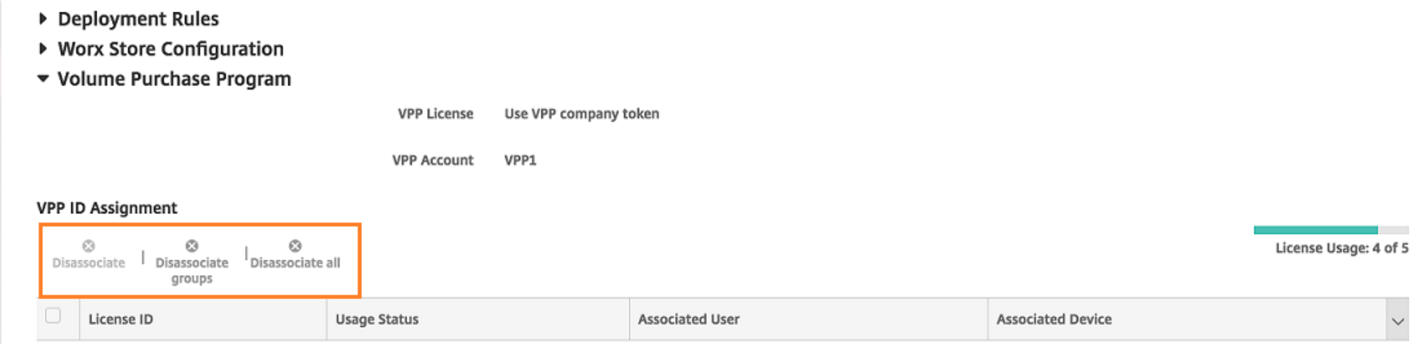
License Usage: 2 of 3

□	Associated User
☑	[redacted]@[redacted].net
□	

Showing 1 - 2 of 2 items

For Android for Work, 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 Program licenses for an individual user, user groups, or for all assignments. Doing so ends the license assignments and frees licenses.



VPP License: Use VPP company token

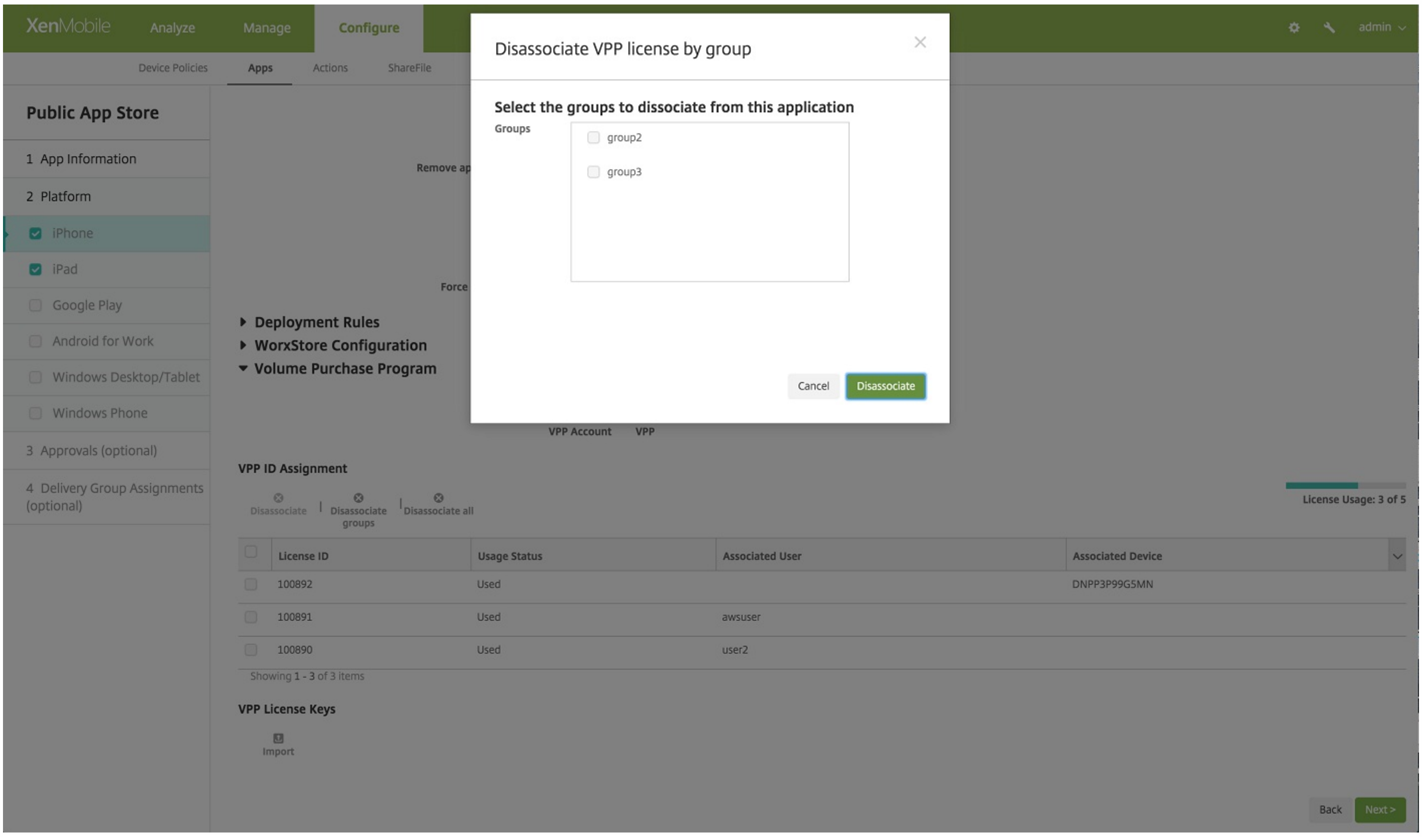
VPP Account: VPP1

VPP ID Assignment

License Usage: 4 of 5

□	License ID	Usage Status	Associated User	Associated Device

Clicking **Disassociate groups** opens a dialog box where you select groups.



Disassociate VPP license by group

Select the groups to dissociate from this application

Groups
- □ group2
- □ group3

VPP Account: VPP

VPP ID Assignment

License Usage: 3 of 5

□	License ID	Usage Status	Associated User	Associated Device
□	100892	Used		DNPP3P99G5MN
□	100891	Used	awsuser	
□	100890	Used	user2	

Showing 1 - 3 of 3 items

VPP License Keys

13. After you complete the **Volume Purchase Program** 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 to set up approval workflows, you can skip to the next step.

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.

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**.

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.
- 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**, which does not apply to iOS.

17. Click **Save**.

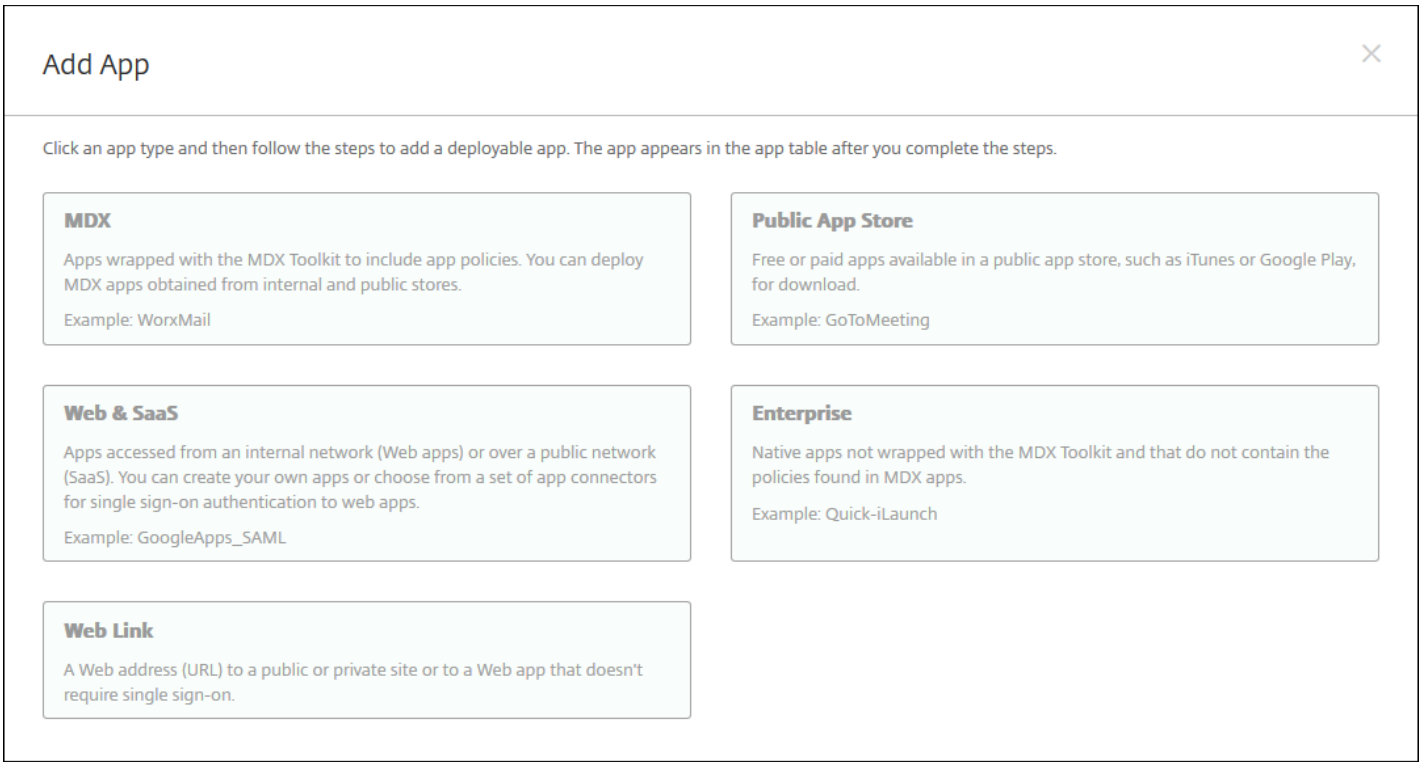
Add a Web or SaaS app

Using the XenMobile console, you can give users single sign-on (SSO) authorization to your mobile, enterprise, web, and SaaS apps. You can enable apps for SSO by using application connector templates. For a list of connector types available in XenMobile, see Application connector types. You can also you build your own connector in XenMobile 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 XenMobile console.

1. In the XenMobile console, click **Configure** > **Apps**. The **Apps** page opens.

2. Click **Add**. The **Add App** dialog box appears.



Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

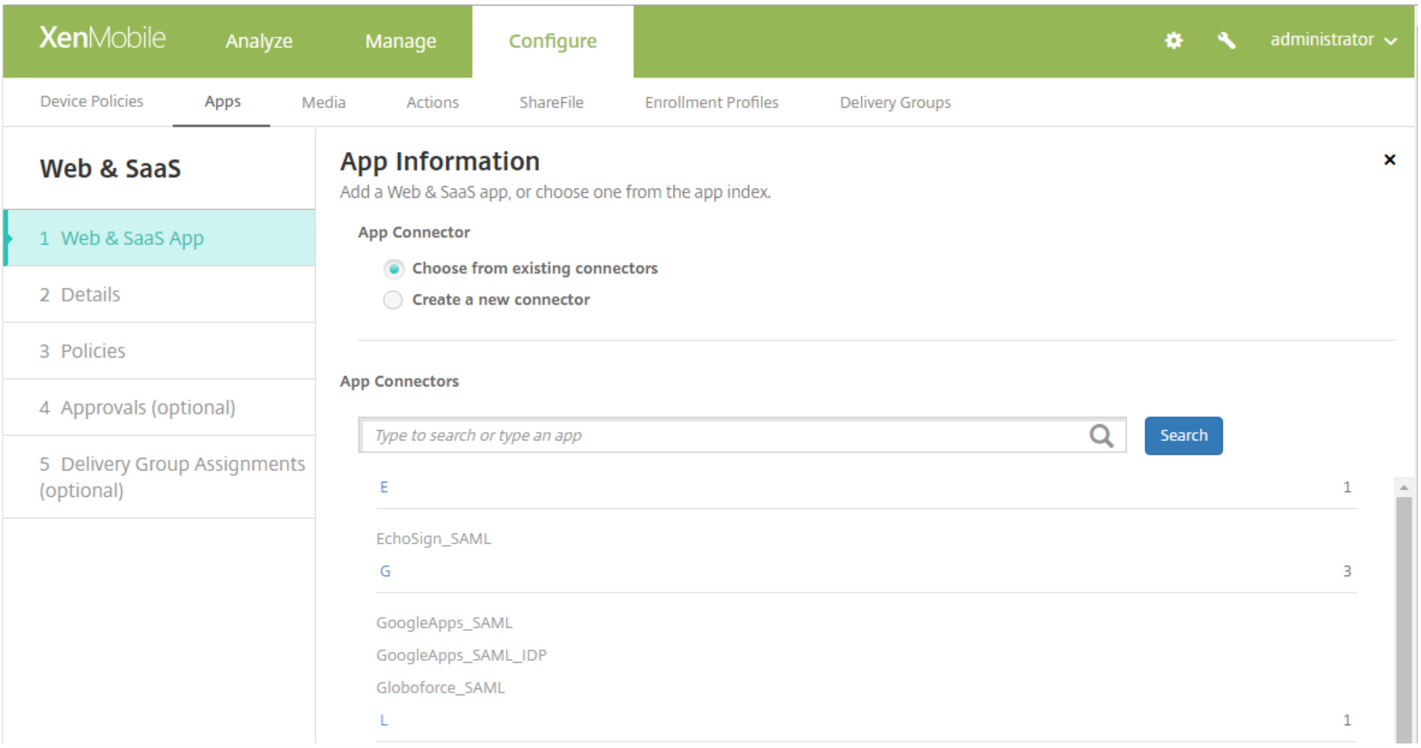
Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
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 web apps.
Example: GoogleApps_SAML

Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Click **Web & SaaS**. The **App Information** page appears.



App Information
Add a Web & SaaS app, or choose one from the app index.

App Connector
● Choose from existing connectors
○ Create a new connector

App Connectors

Type to search or type an app Search

E 1
EchoSign_SAML
G 3
GoogleApps_SAML
GoogleApps_SAML_IDP
Globoforce_SAML
L 1

4. Configure an existing or new app connector, as follows.

To configure an existing app connector

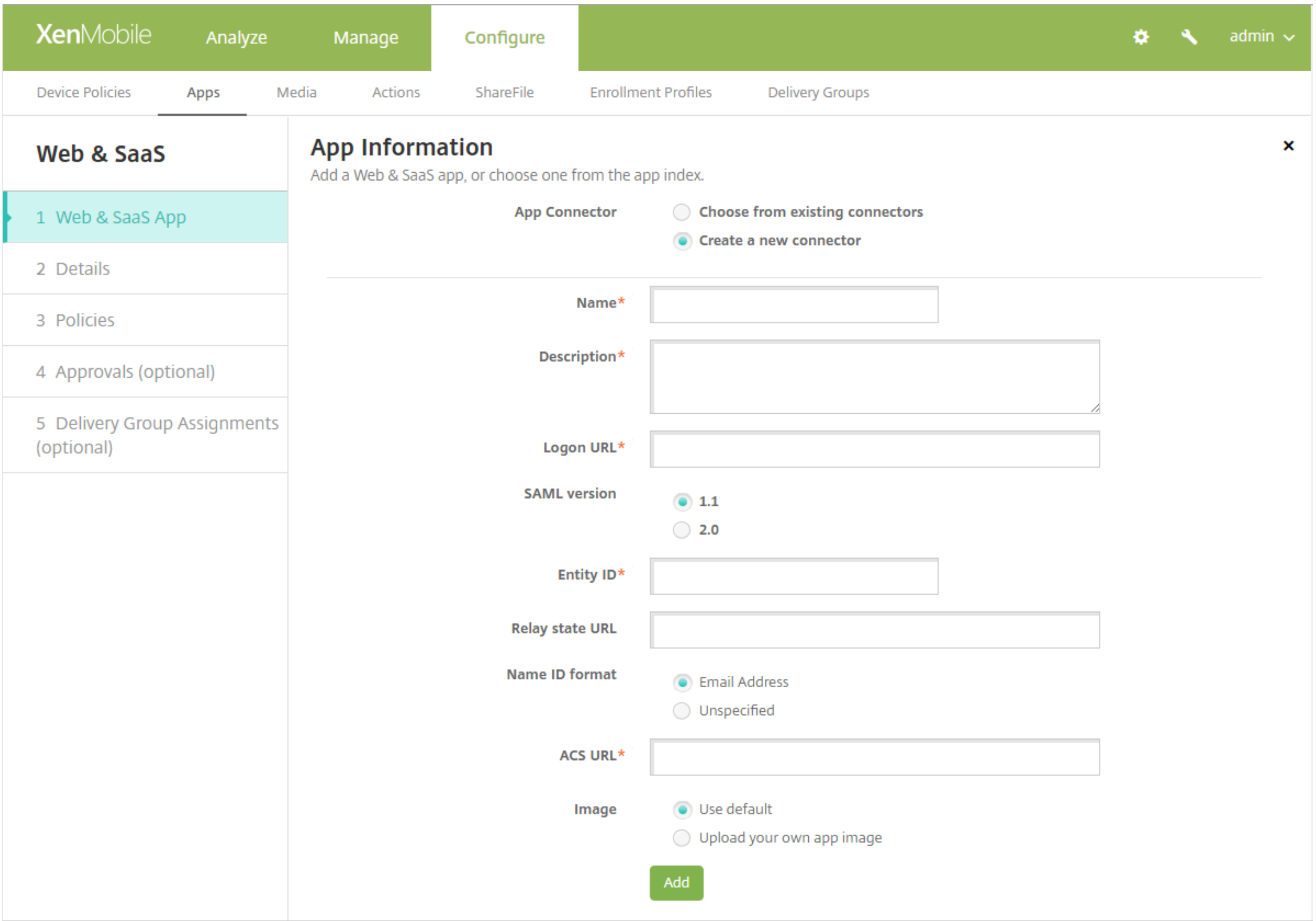
In the **App Information** page, **Choose from existing connectors** is already selected, as shown above. Click the connector you want to use in the **App Connectors** list. The app connector information appears.

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.
- **Domain name**: If applicable, type the domain name of the app. This field is required.
- **App is hosted in internal network**: Select whether the app is running on a server in your internal network. If users connect from a remote location to the internal app, they must connect through NetScaler Gateway. Setting this option to **ON** adds the VPN keyword to the app and allows users to connect through NetScaler Gateway. The default is **OFF**.
- **App category**: 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. Possible options are:
      - Disable account
      - Keep account
      - Remove 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

In the **App Information** page, select **Create a new connector**. The app connector fields appear.



App Information

Add a Web & SaaS app, or choose one from the app index.

App Connector ○ Choose from existing connectors ● Create a new connector

Name*

Description*

Logon URL*

SAML version ● 1.1 ○ 2.0

Entity ID*

Relay state URL

Name ID format ● Email Address ○ Unspecified

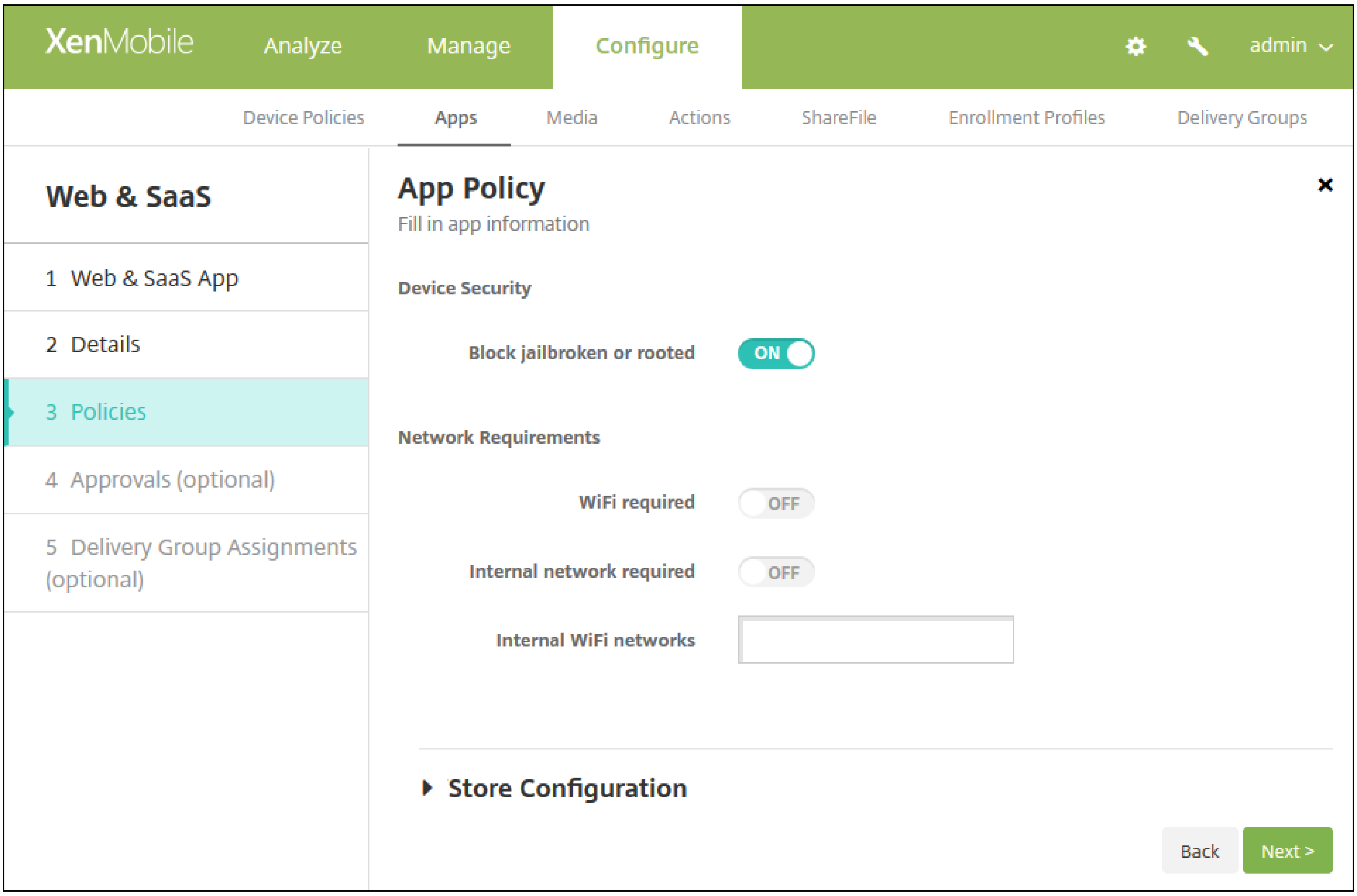
ACS URL*

Image ● Use default ○ Upload your own app image

Configure these settings:

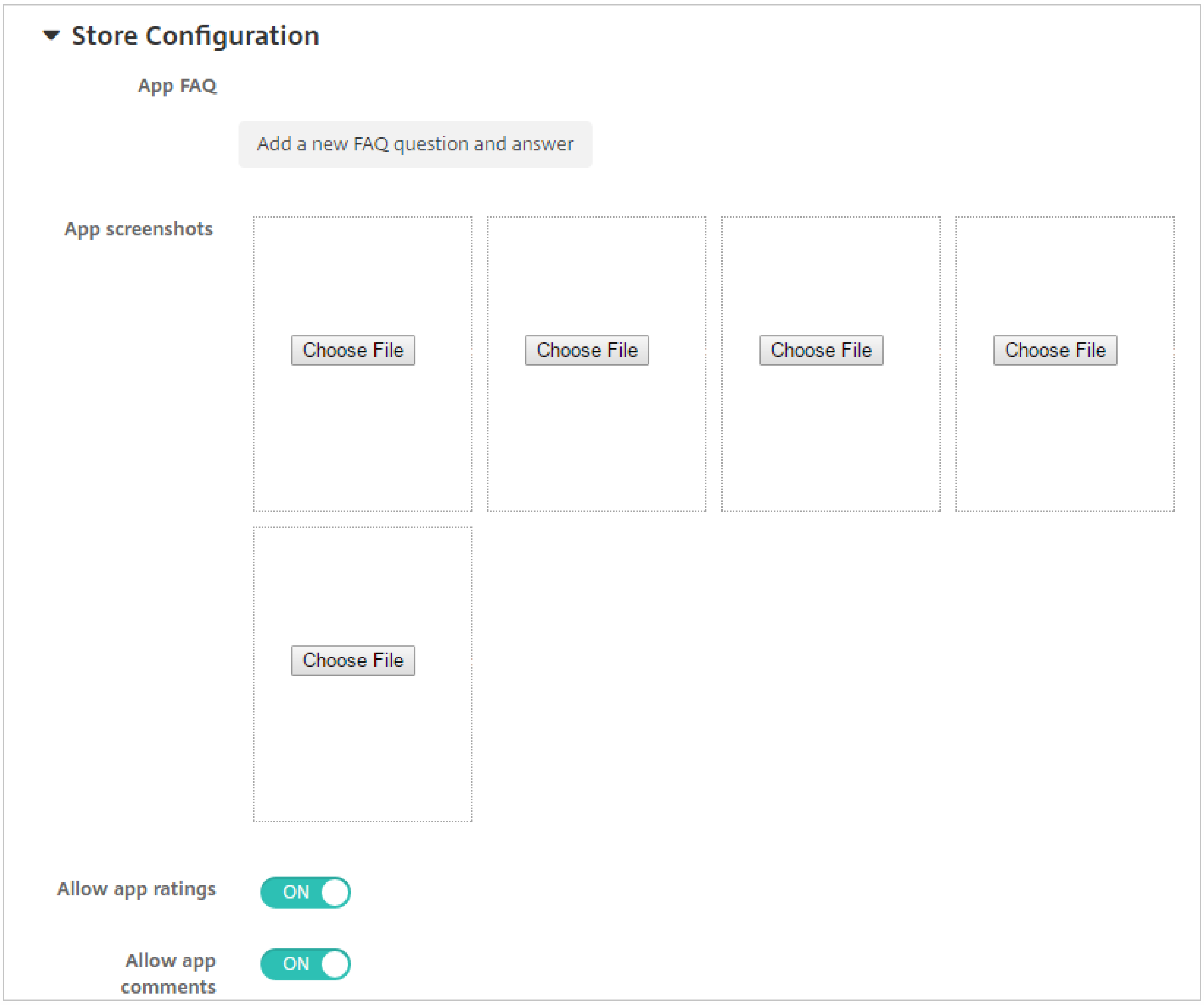
- **Name**: Type a name for the connector. This field is required.
- **Description**: Type a description for the connector. This field is required.
- **Logon URL**: Type, or copy and paste, the URL where users log on to the site. For example, if the app you want to add has a logon page, open a web browser and go to the logon page for the app. For example, it might be http://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 you own app image. The default is Use default.
  - If you want to upload your own image, select it by clicking **Browse** and navigating 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.
  - When you're finished, click **Add**. The **Details** page appears.

5. Click **Next**. The **App Policy** page appears.



- 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 WiFi 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 WiFi required, type the internal WiFi networks to use.

6. Expand **XenMobile Store Configuration**.


Store Configuration

App FAQ

App screenshots

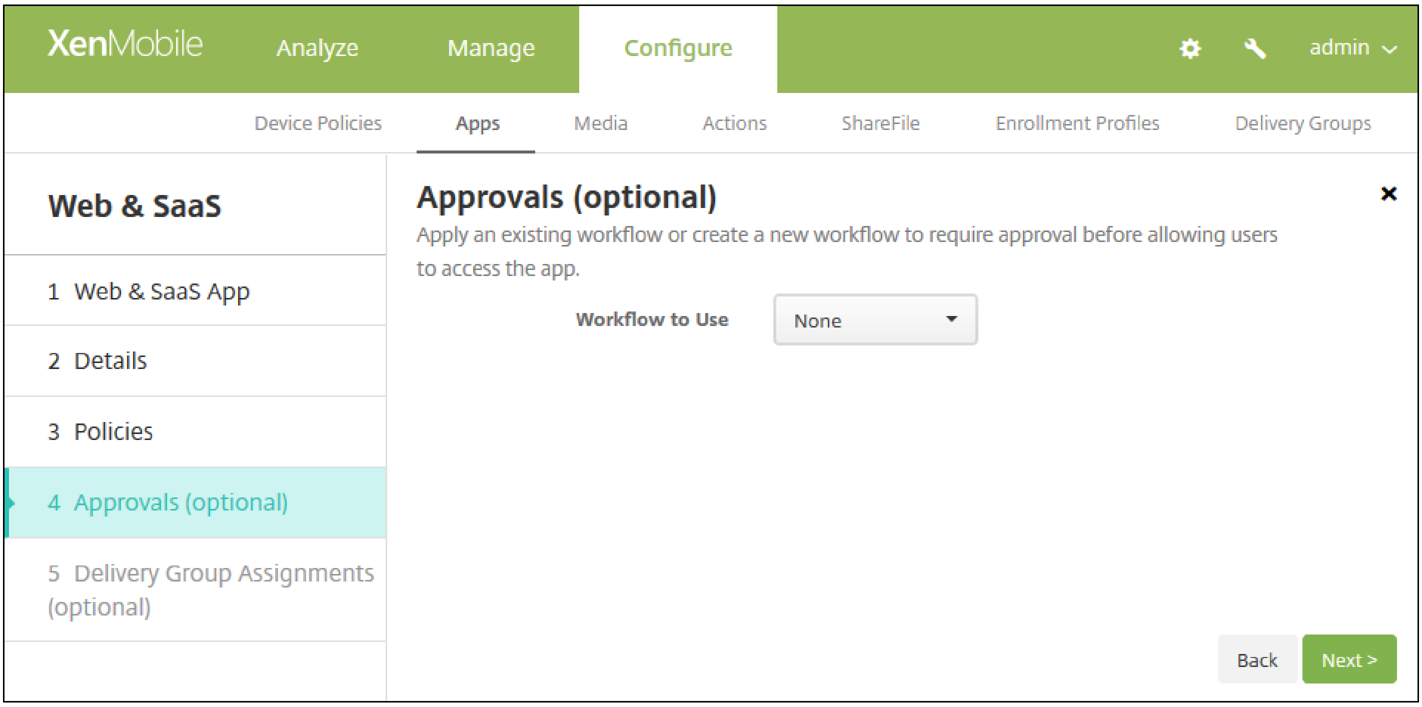
Allow app ratings: ON

Allow app comments: ON

Optionally, you can add an FAQ for the app or screen captures that appear in the XenMobile 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 XenMobile 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.



Approvals (optional)

Apply an existing workflow or create a new workflow to require approval before allowing users to access the app.

Workflow to Use: None

You use workflows when you need approval when creating user accounts. If you don't need to set up 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**.

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.
- 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**, which does not apply to iOS.

11. Click **Save**.

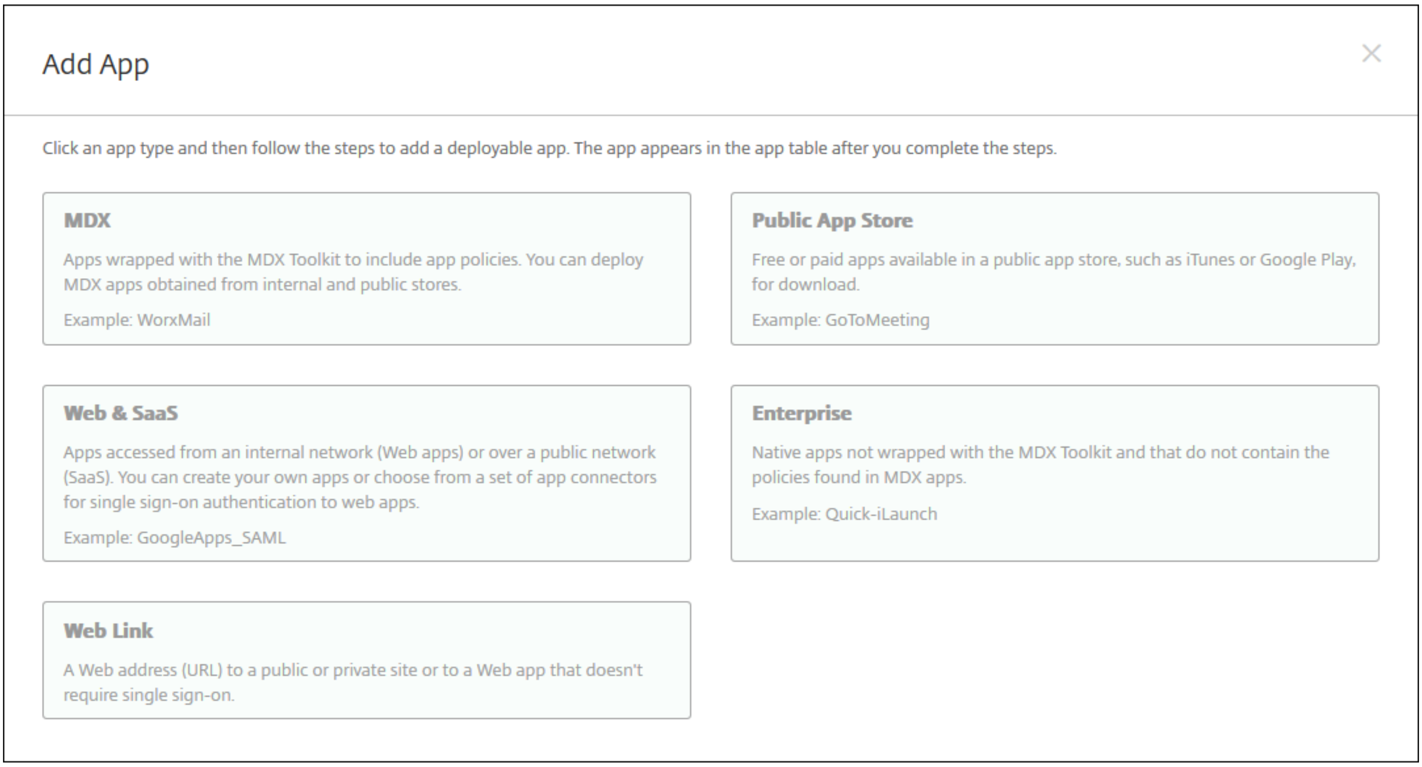
Add an enterprise app

Enterprise apps in XenMobile 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 XenMobile console. Enterprise apps support the following platforms (and corresponding file types):

- iOS (.ipa file)
- Android (.apk file)
- Samsung KNOX (.apk file)
- Android for Work (.apk file)
- Windows Phone (.xap or .appx file)
- Windows Tablet (.appx file)
- Windows Mobile/CE (.cab file)

1. In the XenMobile console, click **Configure** > **Apps**. The **Apps** page opens.

2. Click **Add**. The **Add App** dialog box appears.



Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

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 web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

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 **Browse** and navigating to the file location.

8. Click **Next**. The app information page for the platform appears.

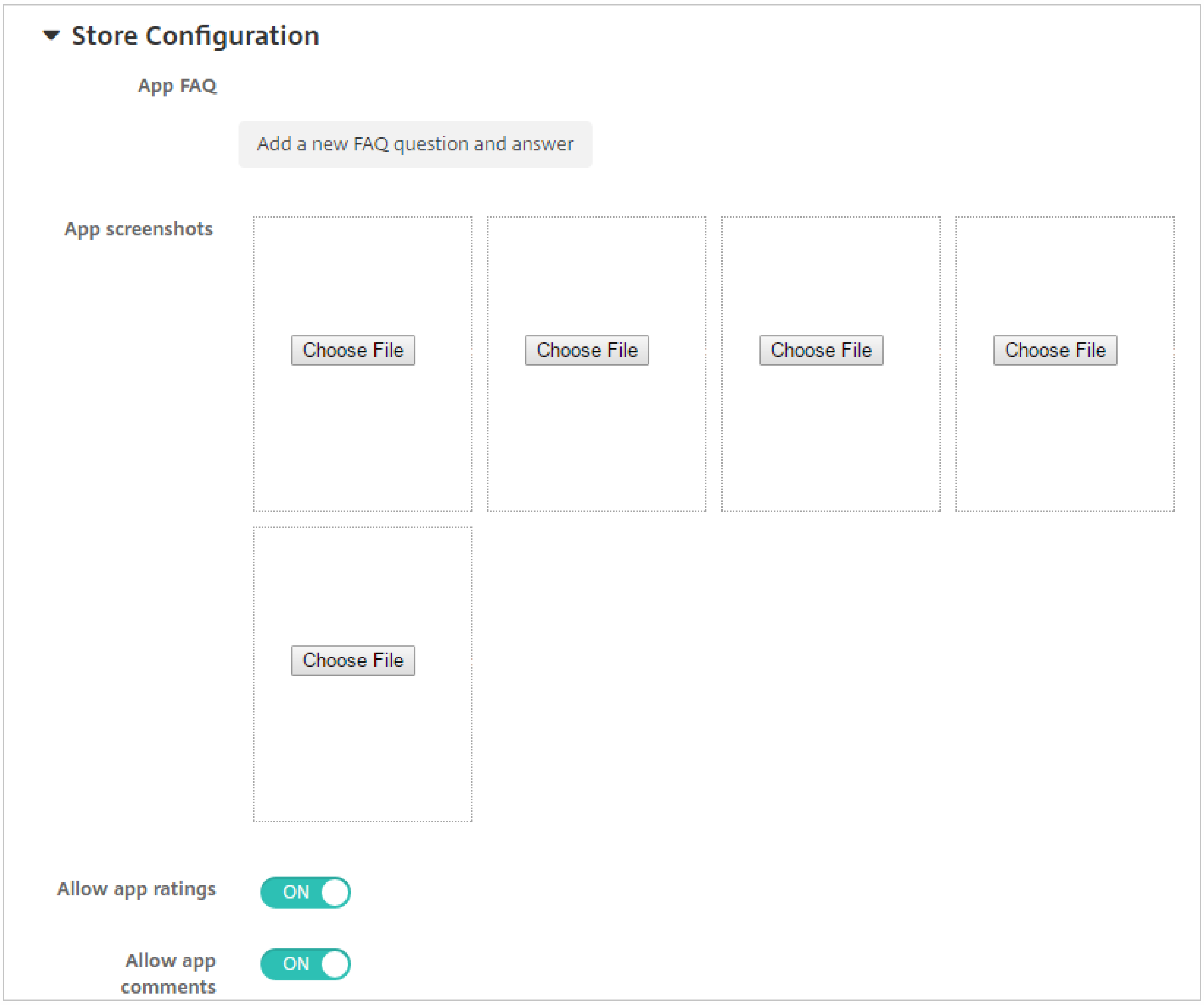
9. Configure the settings for the platform type, such as:

- **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. This setting applies to iOS 9.x devices.

10. Configure the deployment rules. For information, see Deploy resources.

11. Expand **XenMobile Store Configuration**.



Optionally, you can add an FAQ for the app or screen captures that appear in the XenMobile 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 XenMobile 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 to set up approval workflows, you can skip to Step 13.

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.

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**.

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.
- 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**, which does not apply to iOS.

16. Click **Save**.

Add a Web link

In XenMobile, 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).

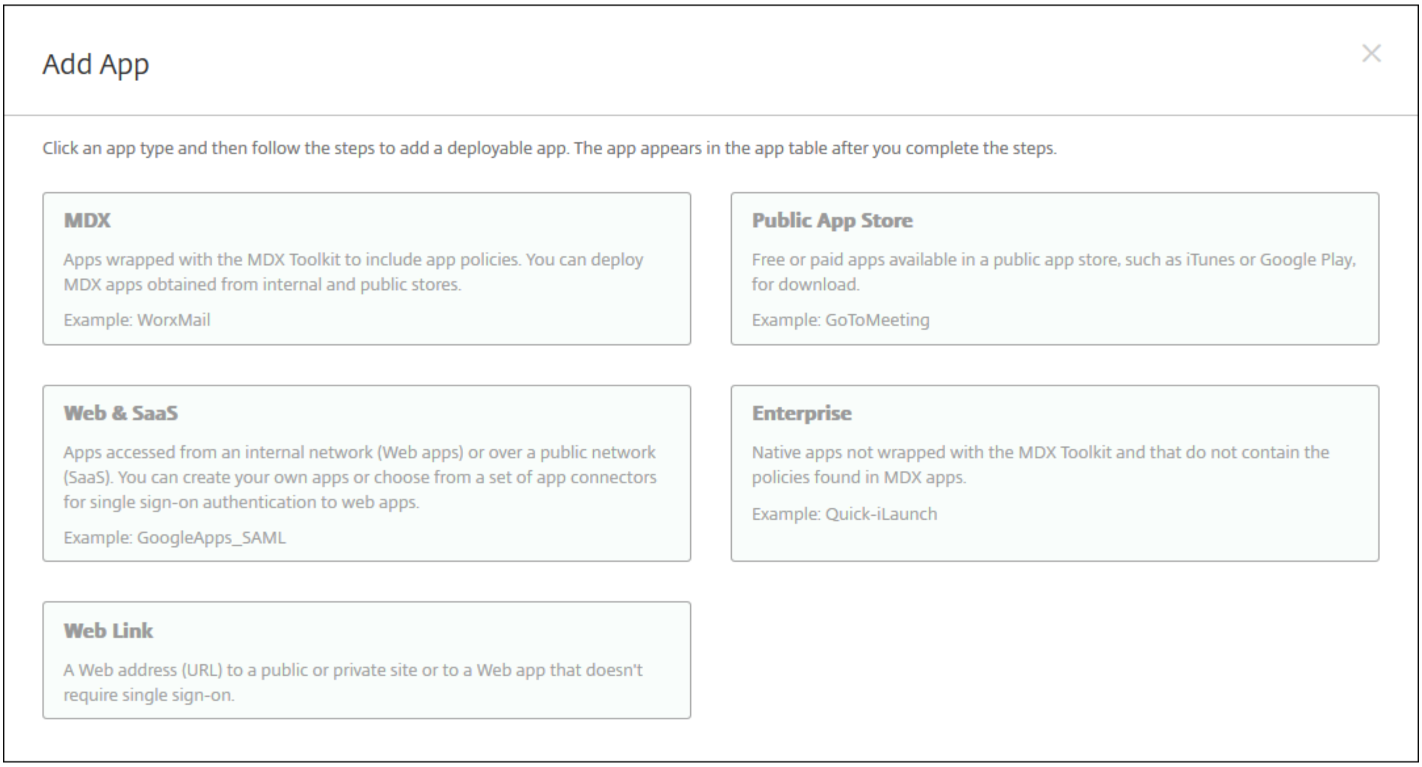
You can configure web links from the **Apps** tab in the XenMobile console. When you finish configuring the web link, the link appears as a link icon in the list in the **Apps** table. When users log on with Secure Hub, the link appears with the list of available apps and desktops.

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 XenMobile console, click **Configure** > **Apps**. The **Apps** page appears.

2. Click **Add**. The **Add App** dialog box appears.



Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
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 web apps.
Example: GoogleApps_SAML

Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

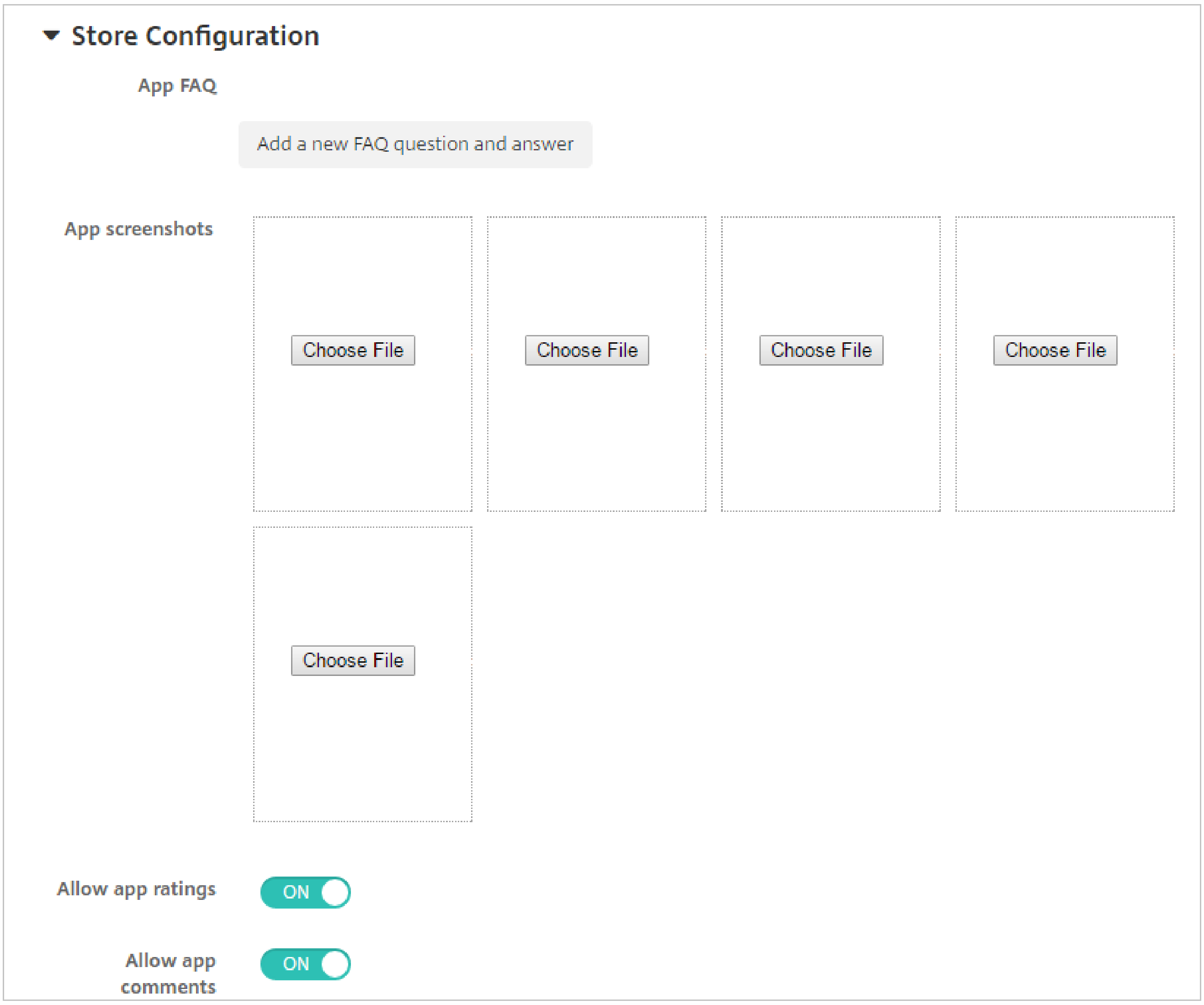
Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

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 NetScaler Gateway. Setting this option to **ON** adds the VPN keyword to the app and allows users to connect through NetScaler Gateway. The default is **OFF**.
- **App category**: In the list, click an optional category to apply to the app.
- **Image**: Select whether to use the default Citrix image or to upload you own app image. The default is Use default.
  - If you want to upload your own image, select it by clicking **Browse** and navigating 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 **XenMobile Store Configuration**.



Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings: ON

Allow app comments: ON

Optionally, you can add an FAQ for the app or screen captures that appear in the XenMobile 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 XenMobile 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**.

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.
- 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**, which does not apply to iOS.

9. Click **Save**.

Enable Microsoft 365 apps

You can open the MDX container to allow Secure Mail, Secure Web, and ShareFile 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 XenMobile 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 XenMobile:

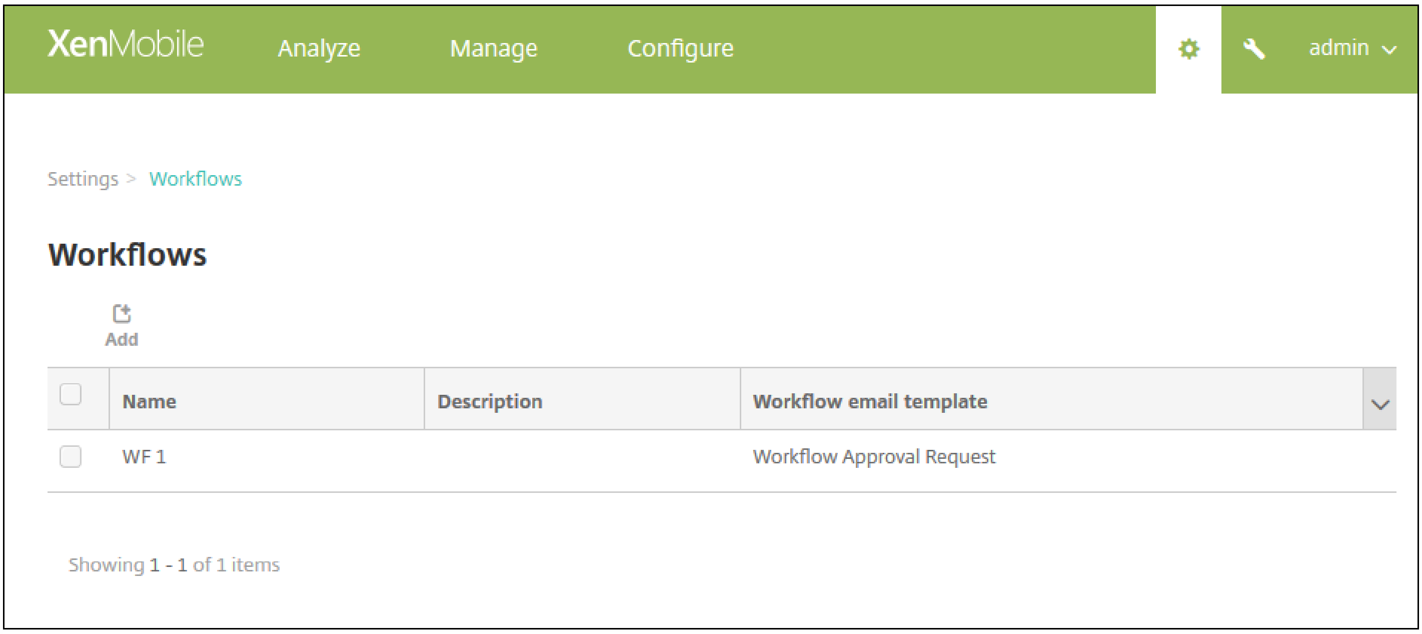
- In the Workflows page in the XenMobile console. On the Workflows page, you can configure multiple workflows for use with app configurations. When you configure workflows on the Workflows page, you can select the workflow when you configure the app.

- 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 XenMobile 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 XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.

2. Click **Workflows**. The **Workflows** page appears.

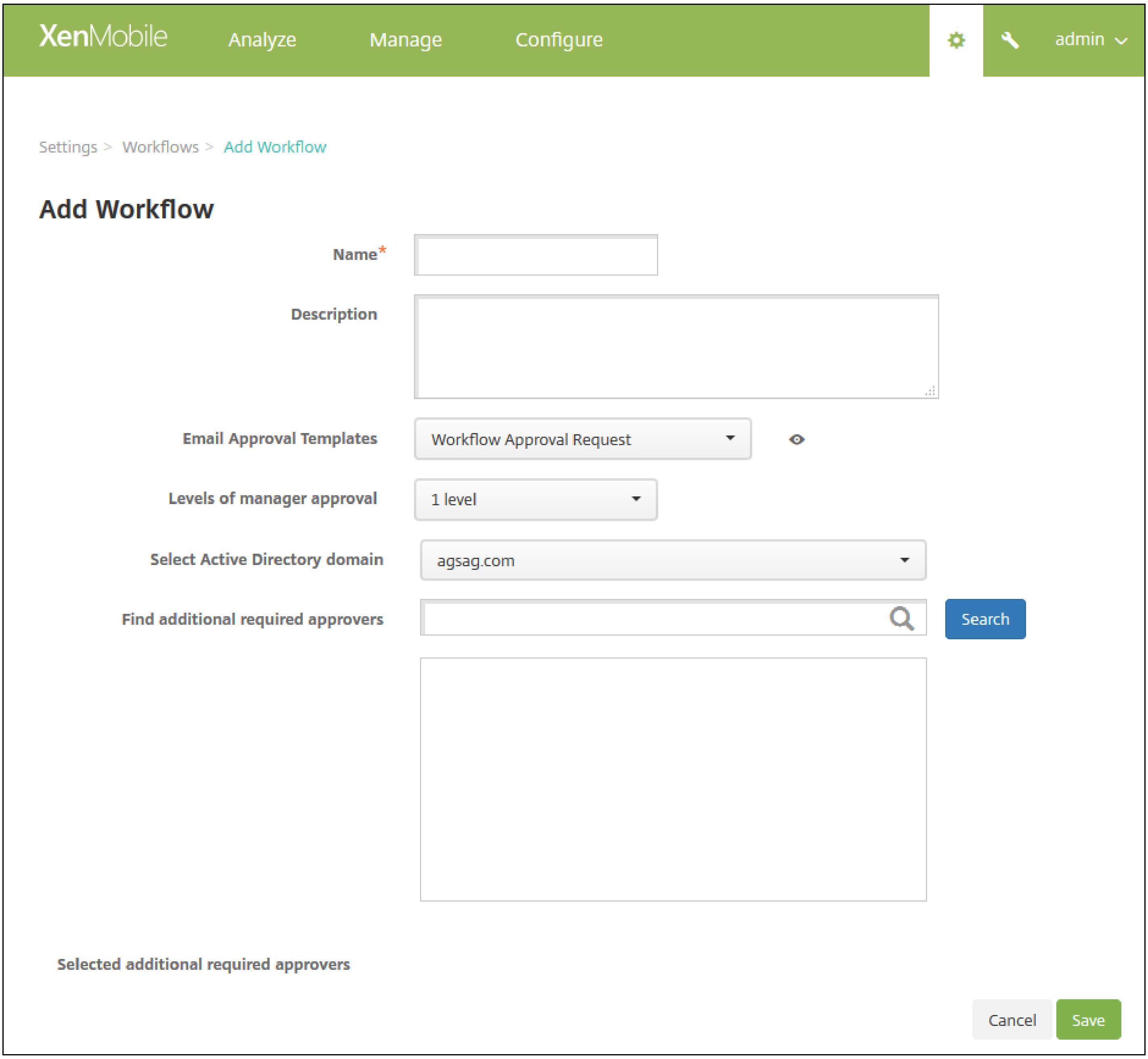


Workflows

□	Name	Description	Workflow email template
□	WF 1		Workflow Approval Request

Showing 1 - 1 of 1 items

3. Click **Add**. The **Add Workflow** page appears.



Add Workflow

Name*:

Description:

Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level

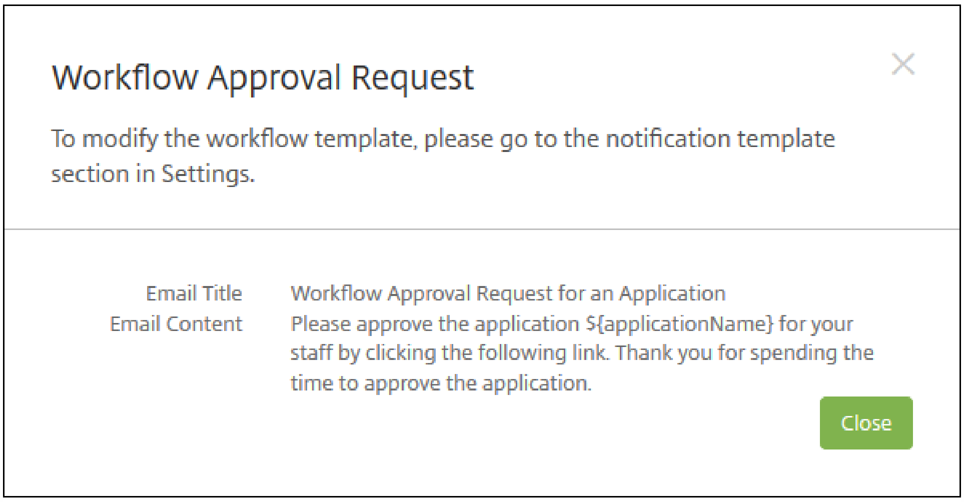
Select Active Directory domain: agsag.com

Find additional required approvers:

Selected additional required approvers

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 XenMobile console. When you click the eye icon to the right of this field, the following dialog box appears.



Workflow Approval Request

To modify the workflow template, please go to the notification template section in Settings.

Email Title Workflow Approval Request for an Application

Email Content Please approve the application ${applicationName} for your staff by clicking the following link. Thank you for spending the time to approve the application.

- **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.

Important: You cannot undo this operation.

App connector types

Sep 06, 2017

The following table lists the connectors and the types of connectors that are available in XenMobile when you add a Web or SaaS app. You can also add a new connector to XenMobile 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.

Connector name	SSO SAML	Supports user account management
EchoSign_SAML	Y	Y
Globoforce_SAML		**Note**: When using this connector, you must enable User Management for Provisioning to ensure seamless SSO integration.
GoogleApps_SAML	Y	Y
GoogleApps_SAML_IDP	Y	Y
Lynda_SAML	Y	Y
Office365_SAML	Y	Y
Salesforce_SAML	Y	Y
Salesforce_SAML_SP	Y	Y
SandBox_SAML	Y	
SuccessFactors_SAML	Y	
ShareFile_SAML	Y	
ShareFile_SAML_SP	Y	
WebEx_SAML_SP	Y	Y

Upgrade MDX or enterprise apps

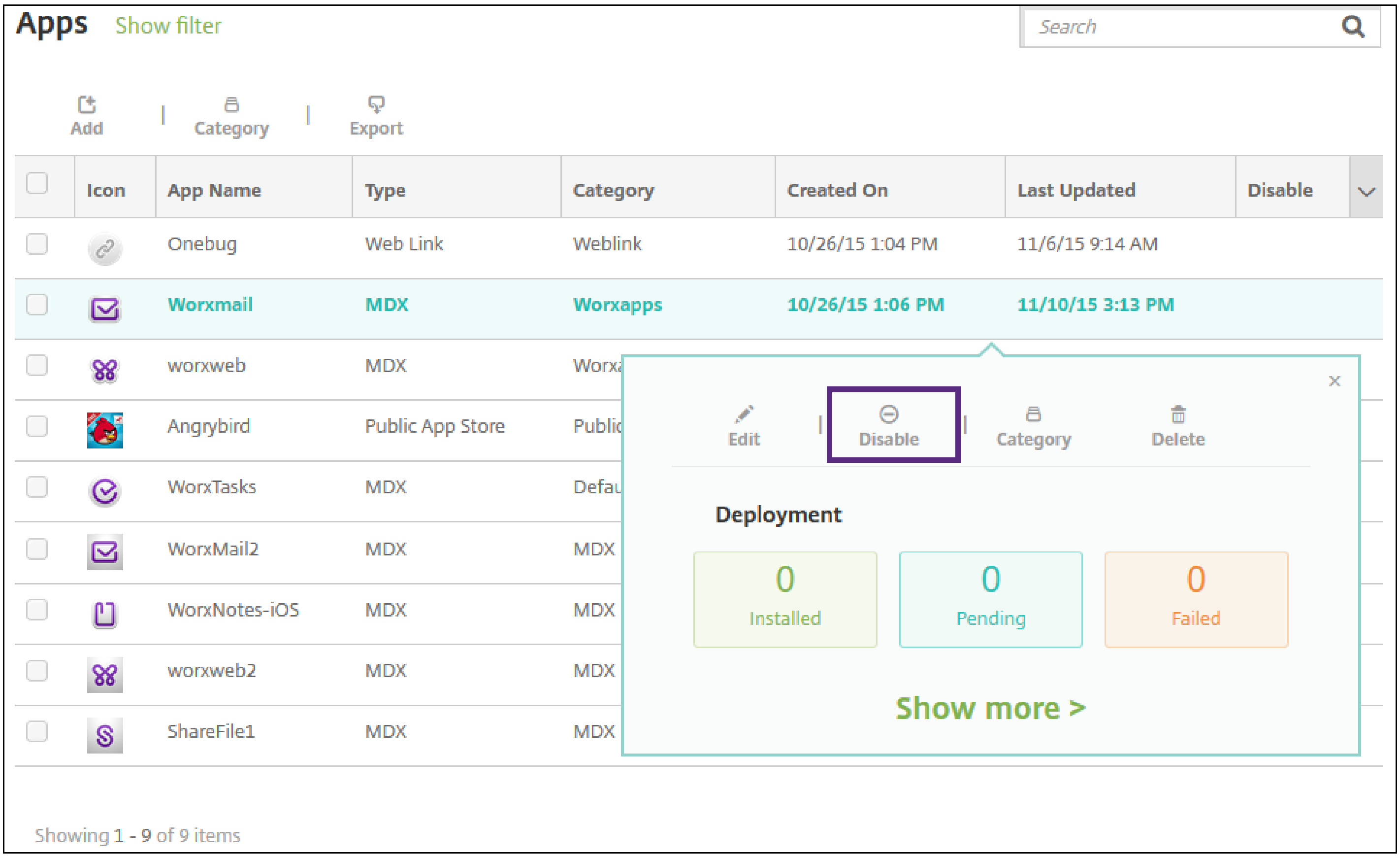
Sep 06, 2017

To upgrade an MDX or Enterprise app in XenMobile, disable the app in the XenMobile console, and then upload the new version of the app.

1. In the XenMobile console, click **Configure** > **Apps**. The **Apps** page appears.

2. For managed devices (devices enrolled in XenMobile for mobile device management), skip to Step 3. For unmanaged devices (devices enrolled in XenMobile 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.



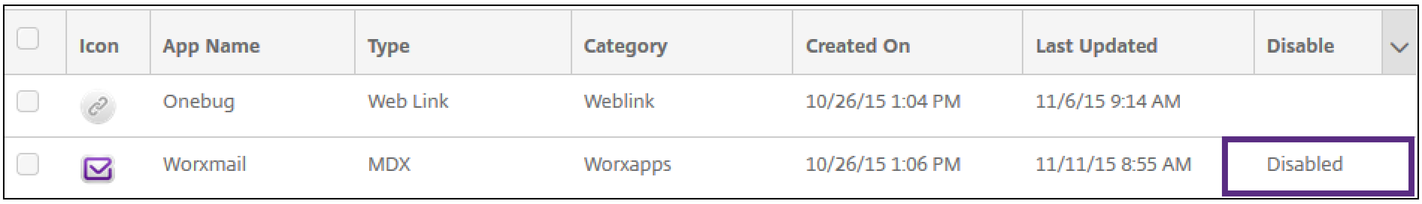
□	Icon	App Name	Type	Category	Created On	Last Updated	Disable
□		Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
□		Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/10/15 3:13 PM	
□		worxweb	MDX	Worx			
□		Angrybird	Public App Store	Public			
□		WorxTasks	MDX	Defau			
□		WorxMail2	MDX	MDX			
□		WorxNotes-iOS	MDX	MDX			
□		worxweb2	MDX	MDX			
□		ShareFile1	MDX	MDX			

Deployment

0	0	0
Installed	Pending	Failed

Showing 1 - 9 of 9 items

- Click **Disable** in the confirmation dialog box. *Disabled* appears in the **Disable** column for the app.



□	Icon	App Name	Type	Category	Created On	Last Updated	Disable
□		Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
□		Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/11/15 8:55 AM	Disabled

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 XenMobile.

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.
- **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 XenMobile.
- Optionally, change the app details and policy settings for the platform.
- Optionally, configure deployment rules and XenMobile Store configurations. For information, see "Add an MDX app" in Add apps.

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.

MDX app policies at a glance

Sep 06, 2017

For a table listing the MDX app policies for iOS, Android, and Windows with notes on restrictions and Citrix recommendations, see MDX Apps Policies at a Glance in the MDX Toolkit documentation.

XenMobile Store and Citrix Secure Hub branding

Sep 06, 2017

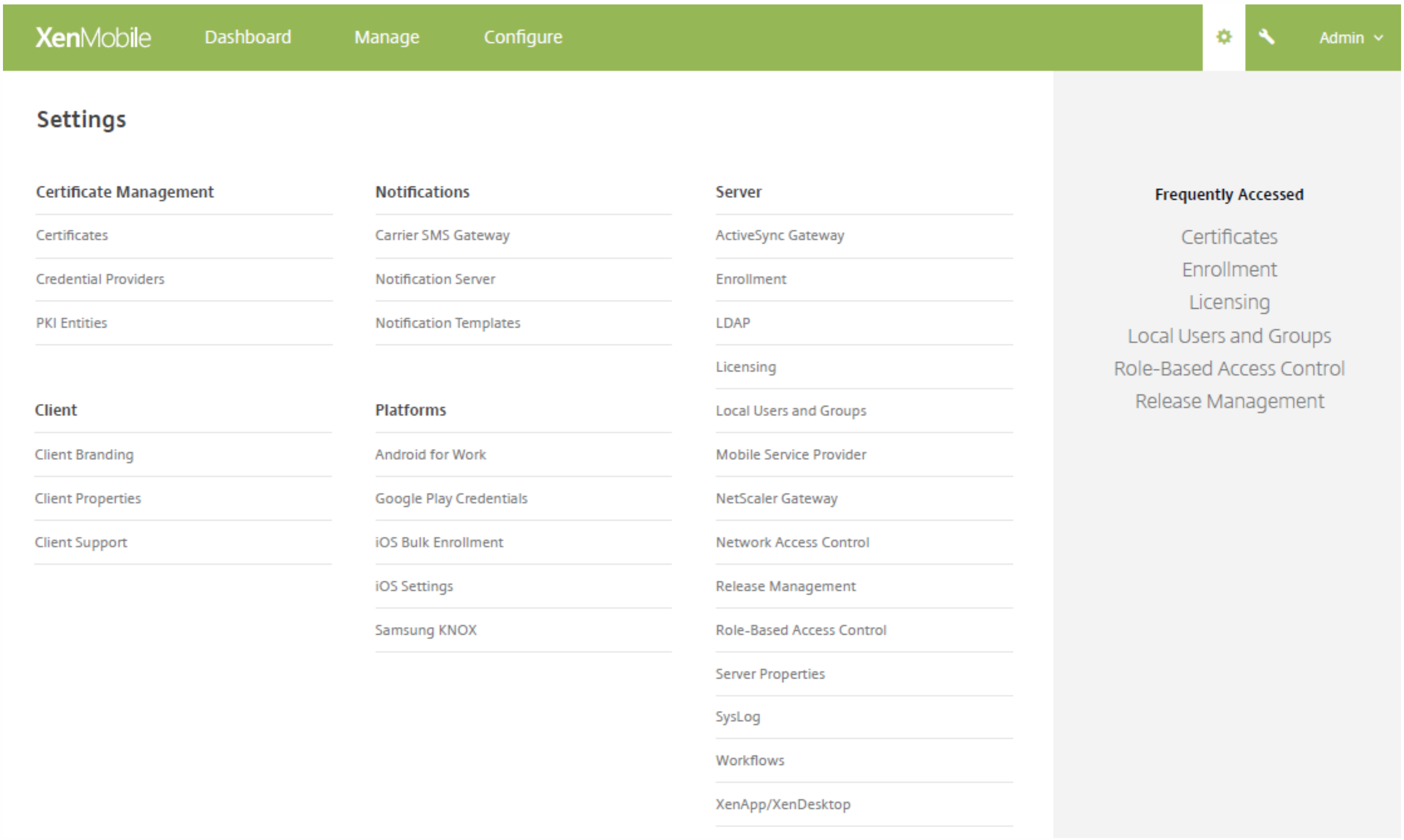
You can set how apps appear in the store and add a logo to brand Secure Hub and the XenMobile Store. These branding features are available for iOS and Android devices.

Note: Before you begin, make sure you have your custom image ready and accessible.

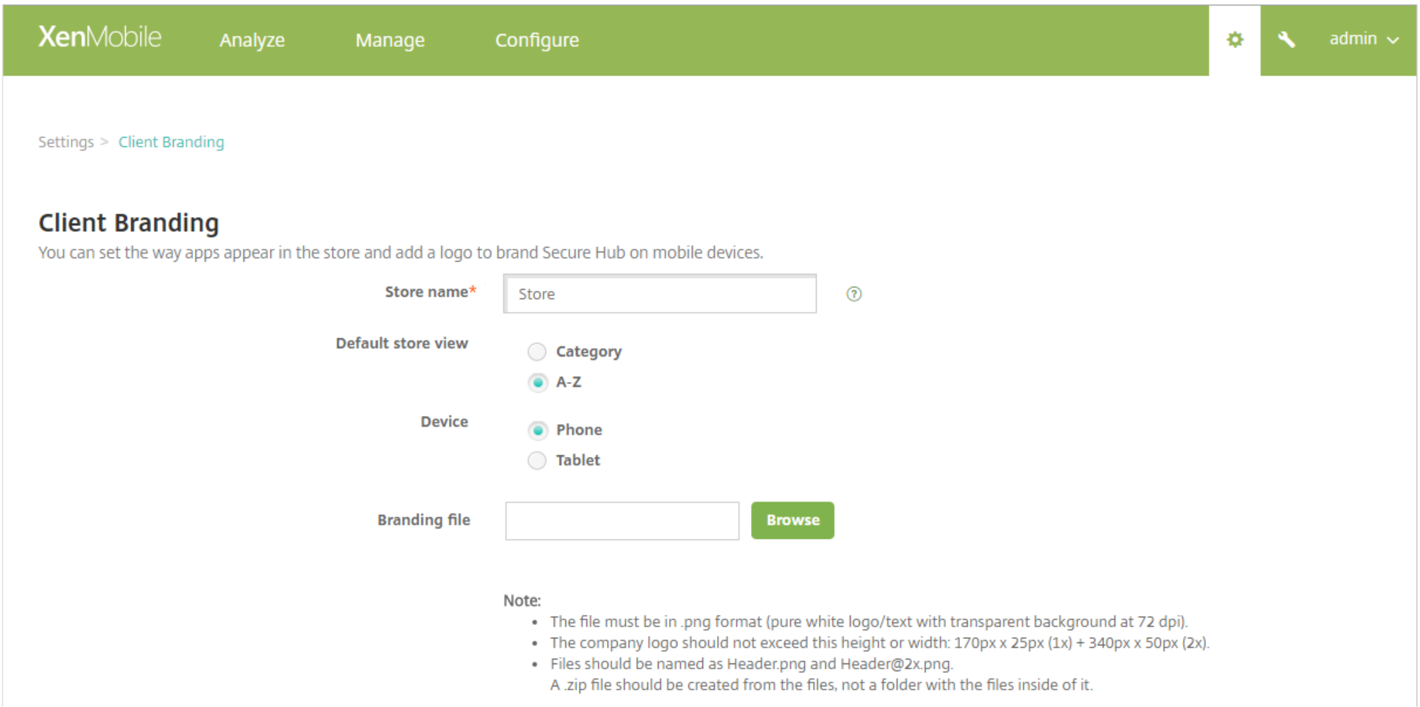
The custom image must meet these requirements:

- The file must be in .png format
- Use a pure white logo or text with a transparent background at 72 dpi.
- The company logo should 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 XenMobile 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

You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.

Store name*: Store

Default store view: ○ Category ● A-Z

Device: ● Phone ○ Tablet

Branding file:

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.
  A .zip file should be created from the files, not a folder with the files inside of it.

Configure the following settings:

- **Store name**: The store name appears on the 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.
- **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 users' devices, you need to create a deployment package and deploy the package to users' devices.

Citrix Launcher

Sep 06, 2017

Citrix Launcher lets you customize the user experience for Android devices deployed by XenMobile. The minimum Android version supported for Secure Hub management of Citrix Launcher is Android 4.0.3. You can add the **Launcher Configuration Policy** to control these Citrix Launcher features:

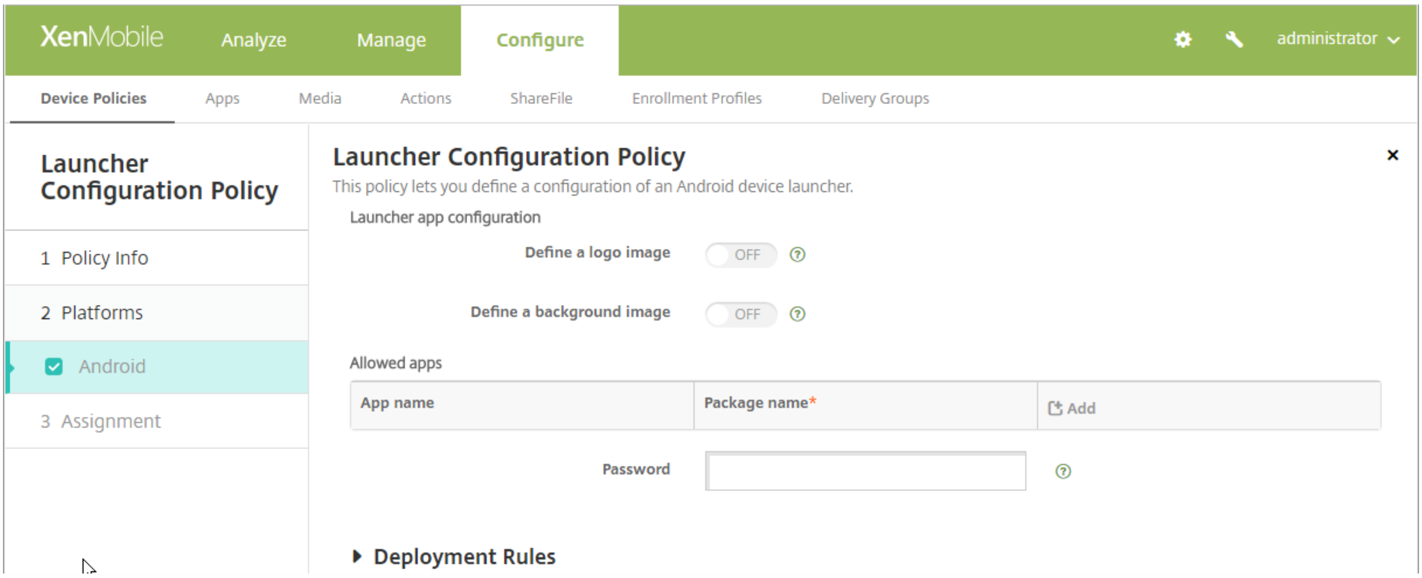
- Manage Android devices so that users can access only the apps that you specify.
- Optionally specify a custom logo image for the Citrix Launcher icon and a custom background image for Citrix Launcher.
- Specify a password that users must enter to exit the launcher.

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 downloads page for your XenMobile edition. The file name is CitrixLauncher.apk. The file is ready for uploading into XenMobile 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.



Launcher Configuration Policy

This policy lets you define a configuration of an Android device launcher.

Launcher app configuration

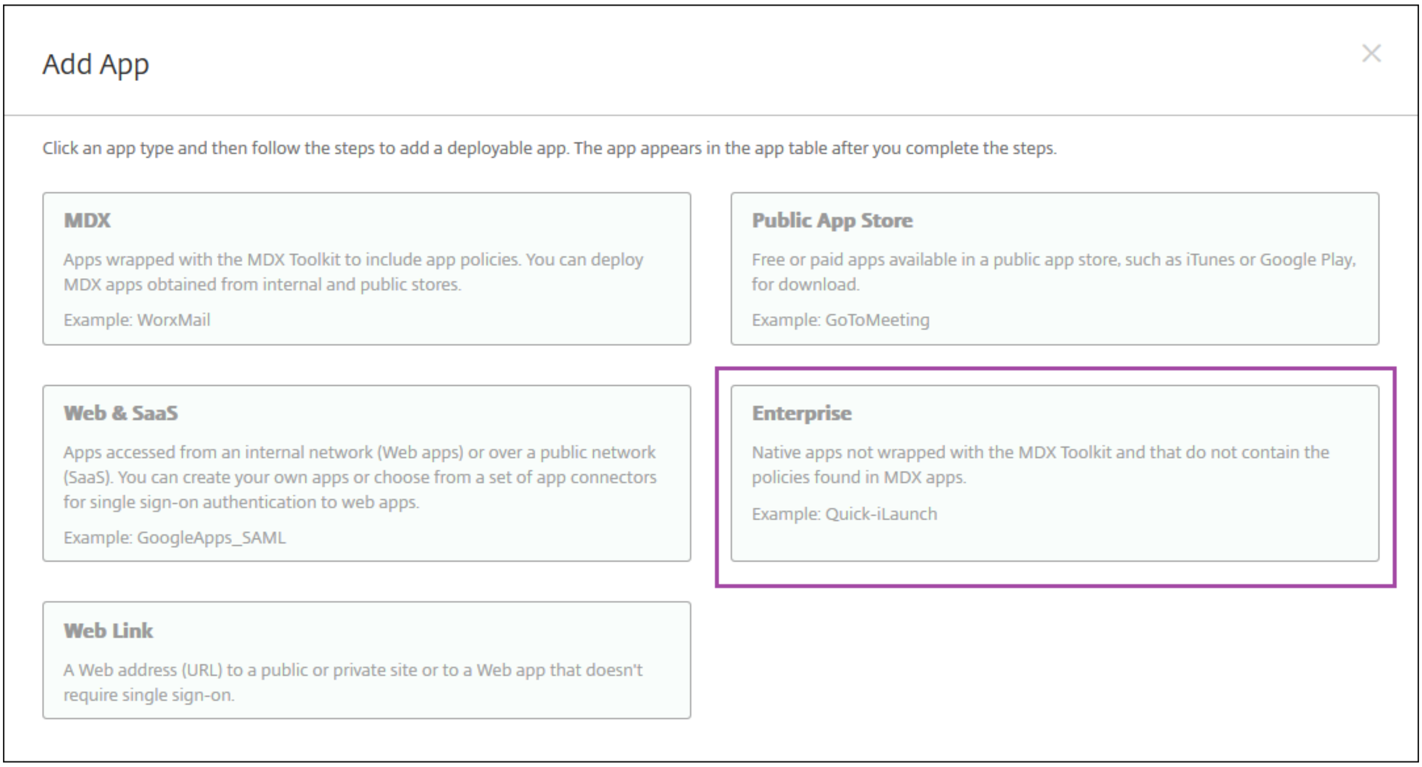
Define a logo image: OFF

Define a background image: OFF

Allowed apps

Password

3. Add the Citrix Launcher app to XenMobile as an enterprise app. In **Configure** > **Apps**, click **Add** and then click **Enterprise**. For more information, see Add an enterprise app.



Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

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 web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

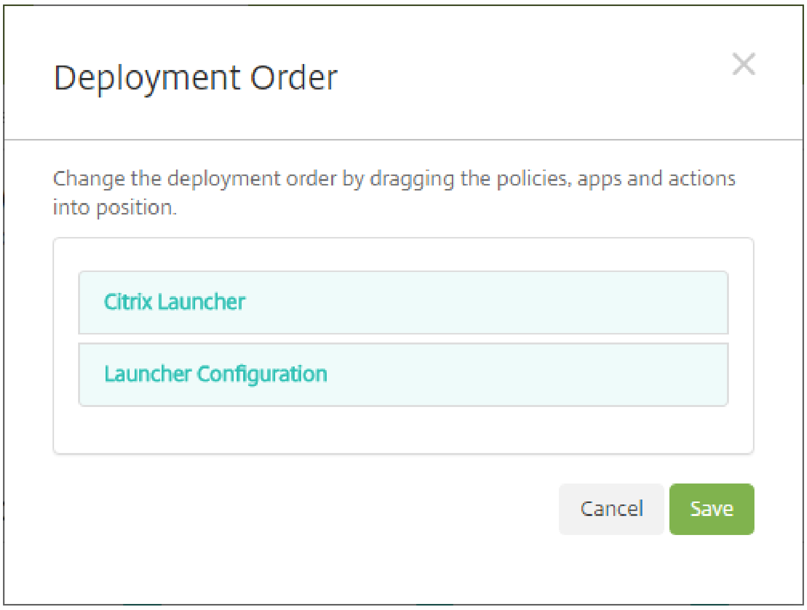
Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

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.



Deployment Order

Change the deployment order by dragging the policies, apps and actions into position.

Citrix Launcher

Launcher Configuration

For more information, see Deploy resources.

iOS Volume Purchase Program

Sep 06, 2017

You can manage iOS app licensing by using the Apple iOS Volume Purchase Program (VPP). The VPP solution simplifies the process to find, buy, and distribute apps and other data in bulk for an organization.

With VPP, you can use XenMobile to distribute public app store apps. VPP is not supported for XenMobile Apps or for apps wrapped by using the MDX Toolkit. Although you can distribute the XenMobile public store apps with VPP, the deployment is not optimal. Further enhancements to the XenMobile Server and the Secure Hub store are required to address the limitations. For a list of known issues with deploying the XenMobile public store apps via VPP and potential workarounds, see this article in the Citrix knowledge center.

With VPP, 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 VPP in XenMobile.

XenMobile periodically reimports VPP licenses from Apple to ensure that the licenses reflect all changes. Such changes include when you manually delete an imported app from VPP. By default, XenMobile refreshes the VPP license baseline a minimum of every 720 minutes. You can change the baseline interval through the server property, VPP baseline interval (vpp.baseline). For information, see Server properties.

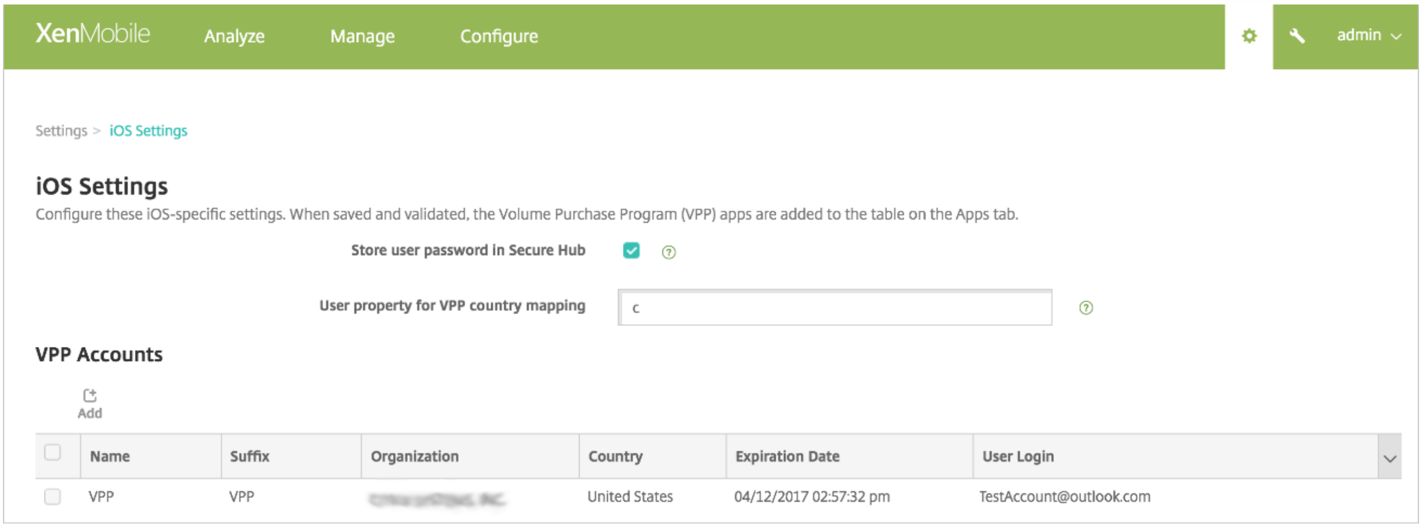
This article focuses on using VPP with managed licenses, which enables you to use XenMobile to distribute apps. If you currently use redemption codes and want to change to managed distribution, see this Apple Support document: Migrate from redemption codes to managed distribution with the Volume Purchase Program.

For information about the iOS VPP, see http://www.apple.com/business/vpp/. To enroll in VPP, go to https://deploy.apple.com/qforms/open/register/index/avs. To access your VPP store in iTunes, go to https://vpp.itunes.apple.com/?l=en.

After you save these iOS VPP settings in XenMobile, the purchased apps appear on the **Configure > Apps** page in the XenMobile console.

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

2. Under **Platform**, click **iOS Settings**. The **iOS Settings** configuration page appears.



Settings > iOS Settings

iOS Settings

Configure these iOS-specific settings. When saved and validated, the Volume Purchase Program (VPP) apps are added to the table on the Apps tab.

Store user password in Secure Hub ☑

User property for VPP country mapping: c

VPP Accounts

□	Name	Suffix	Organization	Country	Expiration Date	User Login
□	VPP	VPP	[redacted]	United States	04/12/2017 02:57:32 pm	TestAccount@outlook.com

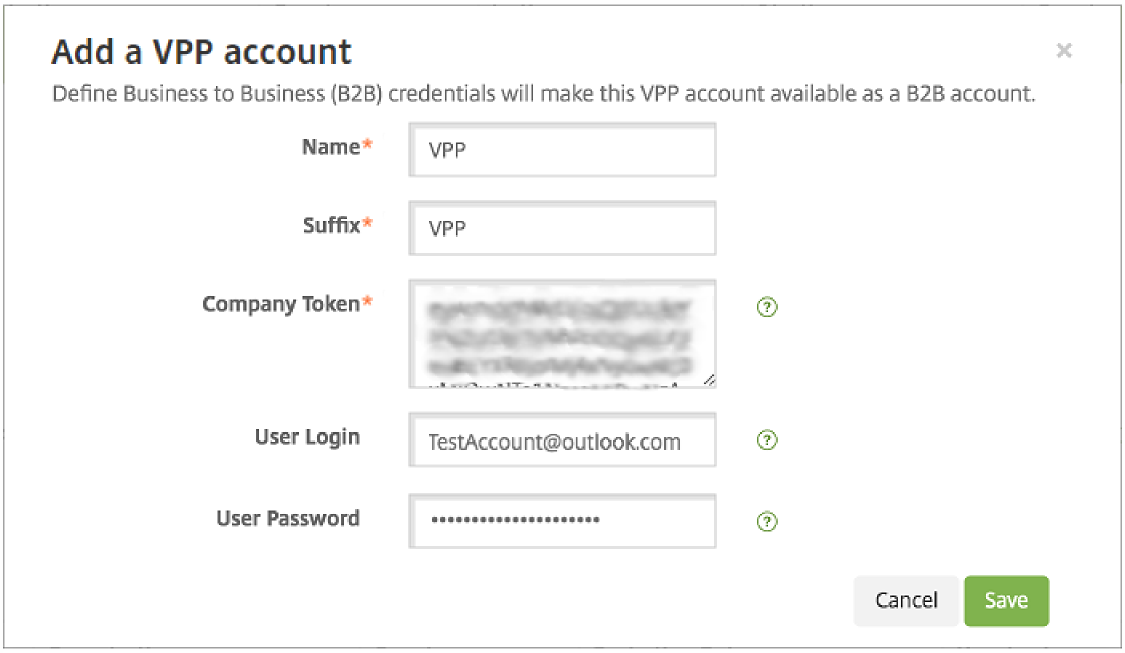
3. Configure these settings:

- **Store user password in Secure Hub**: Select whether to store a user name and password in Secure Hub for XenMobile authentication. The default is to store the information by using this secure method.
- **User property for VPP country mapping**: Type a code to allow users to download apps from country-specific app stores.

  XenMobile uses this mapping to choose the property pool of the VPP. For example, if the user property is United States, that user cannot download apps if the VPP code for the app is for the United Kingdom. Contact your VPP plan administrator for more information about the country mapping code.

VPP Accounts

- For each VPP account you want to add, click **Add**. The **Add VPP account** dialog box appears.



Add a VPP account

Define Business to Business (B2B) credentials will make this VPP account available as a B2B account.

Name* VPP

Suffix* VPP

Company Token* [redacted]

User Login TestAccount@outlook.com

User Password ••••••••••••••••••••

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 Program**.

- **Name**: Type the VPP account name.
- **Suffix**: Type the suffix to appear with the names of apps obtained through the VPP account. For example, if you enter **VPP**, the Secure Mail app appears in the apps list as **Secure Mail - VPP**.
- **Company Token**: Copy and paste the VPP service token obtained from Apple. To obtain the token: In the **Account Summary** page of the Apple VPP portal, click the **Download** button to generate and download the VPP 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 VPP account administrator name used to import custom B2B apps.
- **User Password**: Type the VPP account administrator password.

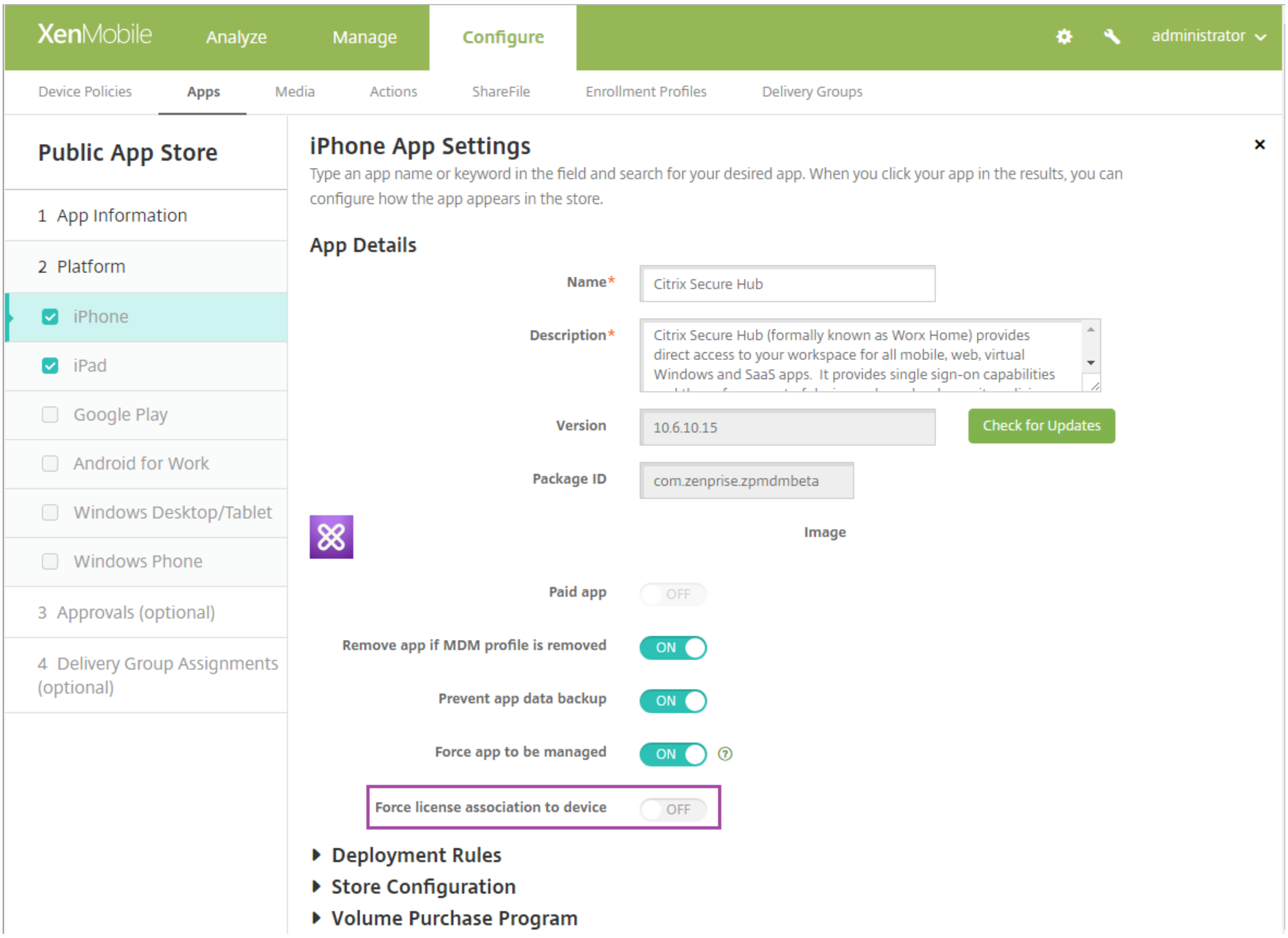
5. Click **Save** to close the dialog box.

6. Click **Save** to save the iOS settings.

A message appears stating that XenMobile adds the apps to the list on the **Configure > Apps** page. On that page, notice that the app names from your VPP account include the suffix you provided in the preceding configuration.

You can now configure the VPP app settings and then tune your delivery group and device policy settings for VPP apps. After you complete those configurations, users can enroll their devices. The following notes provide considerations for those processes.

- When configuring VPP app settings (**Configure > Apps**), enable **Force license association to device**. An advantage of using Apple VPP and DEP with supervised devices: The ability to use XenMobile 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 VPP program. Users can also download the apps without signing into their iTunes account.



Public App Store

1 App Information

2 Platform

☑ iPhone

☑ iPad

□ Google Play

□ Android for Work

□ Windows Desktop/Tablet

□ Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

iPhone App Settings

Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

App Details

Name*: Citrix Secure Hub

Description*: Citrix Secure Hub (formally known as Worx Home) provides direct access to your workspace for all mobile, web, virtual Windows and SaaS apps. It provides single sign-on capabilities

Version: 10.6.10.15

Package ID: com.zenprise.zpmdmbeta

Paid app: OFF

Remove app if MDM profile is removed: ON

Prevent app data backup: ON

Force app to be managed: ON

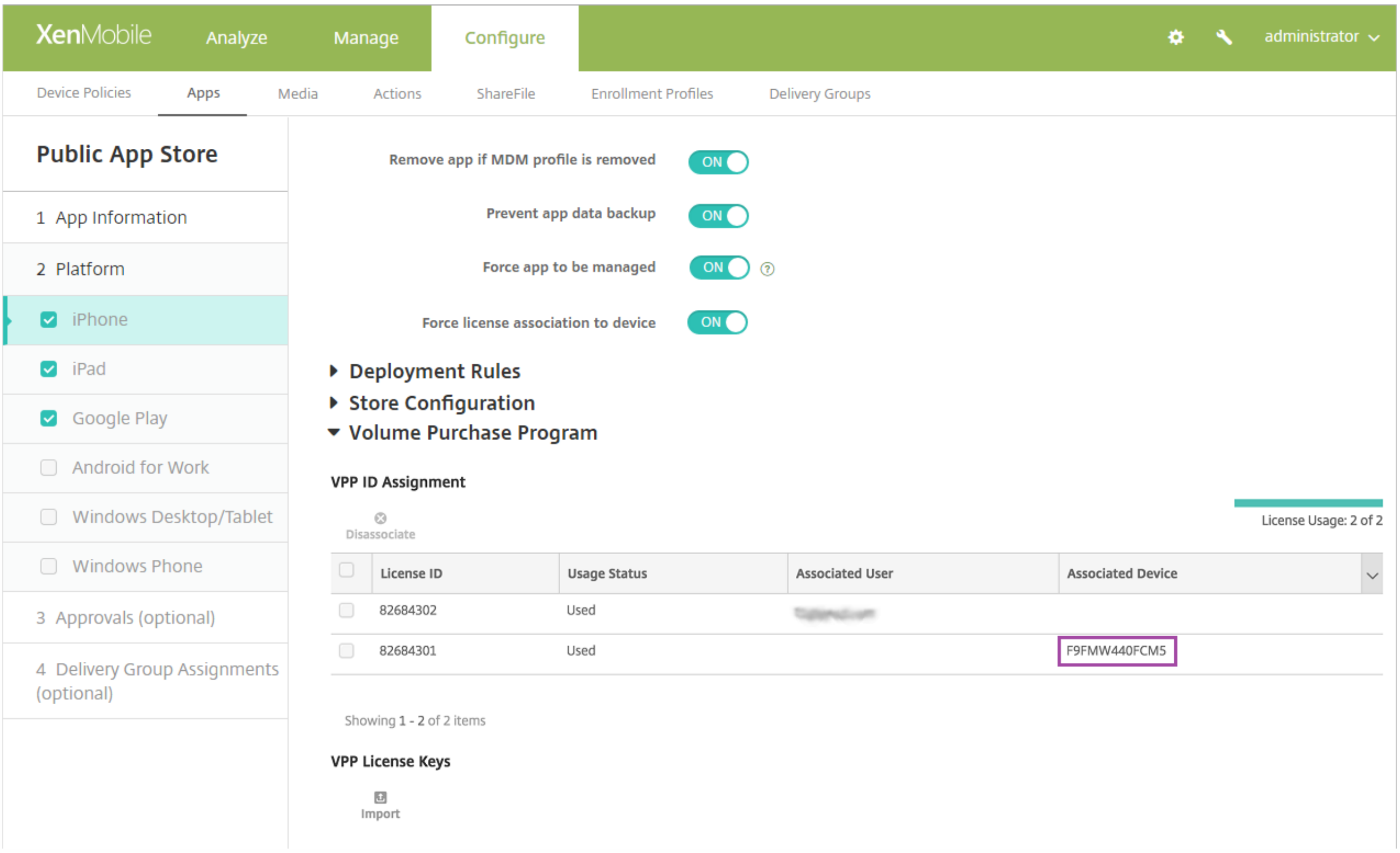
Force license association to device: OFF

▸ Deployment Rules

▸ Store Configuration

▸ Volume Purchase Program

To view the VPP info for that app, expand **Volume Purchase Program**. Notice in the **VPP ID Assignment** table, the license is associated with a device. The device serial number appears in the **Associated Device** column. 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.



Public App Store

1 App Information

2 Platform

- ☑ iPhone
- ☑ iPad
- ☑ Google Play
- □ Android for Work
- □ Windows Desktop/Tablet
- □ Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

Remove app if MDM profile is removed: ON

Prevent app data backup: ON

Force app to be managed: ON

Force license association to device: ON

- Deployment Rules
- Store Configuration
- Volume Purchase Program

VPP ID Assignment

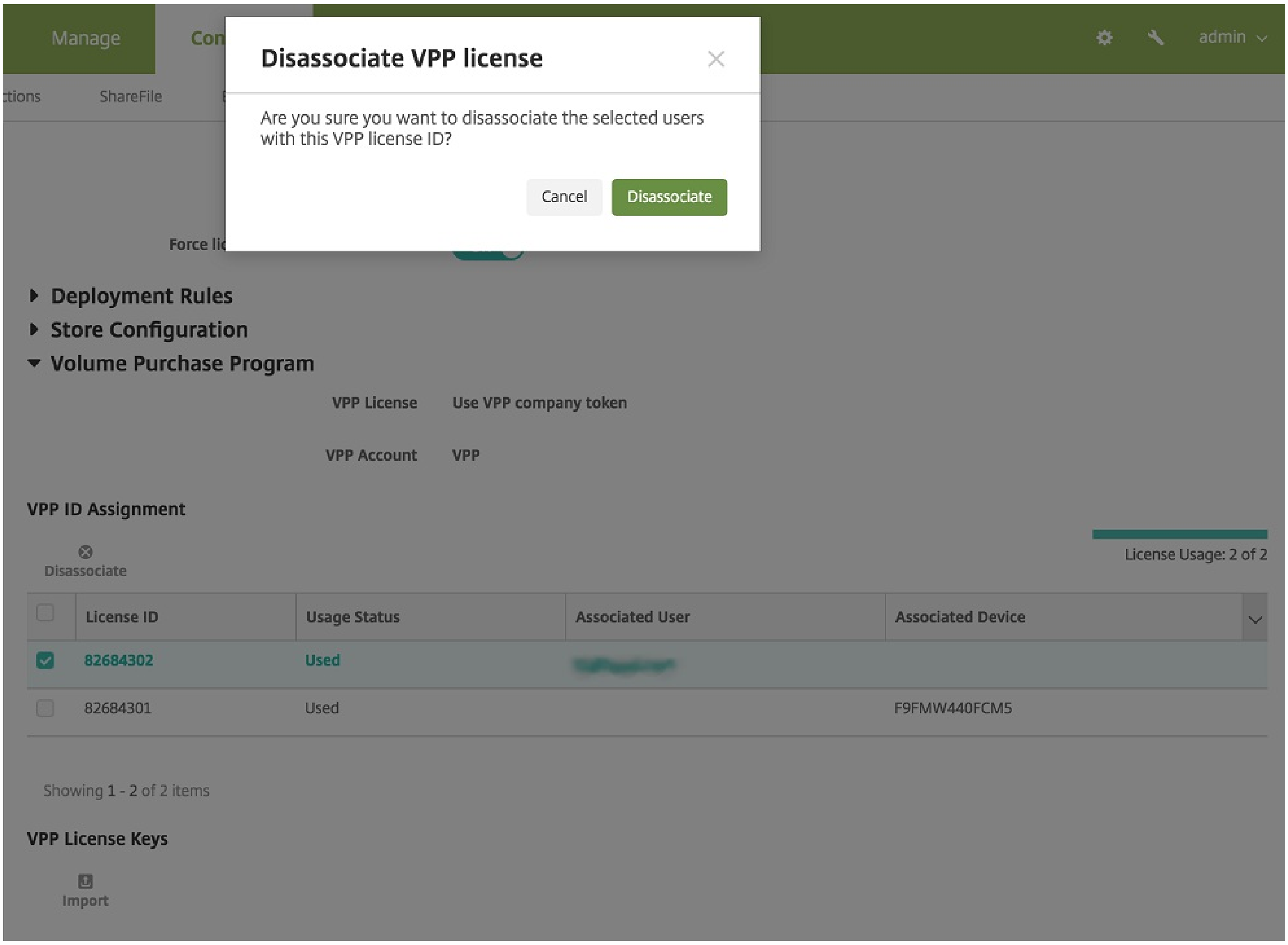
License Usage: 2 of 2

□	License ID	Usage Status	Associated User	Associated Device
□	82684302	Used	[redacted]	
□	82684301	Used		F9FMW440FCM5

Showing **1 - 2** of 2 items

VPP License Keys

To disassociate a license, click the row for the license and then click **Disassociate**.



Disassociate VPP license

Are you sure you want to disassociate the selected users with this VPP license ID?

Cancel | Disassociate

- Deployment Rules
- Store Configuration
- Volume Purchase Program

VPP License: Use VPP company token

VPP Account: VPP

VPP ID Assignment

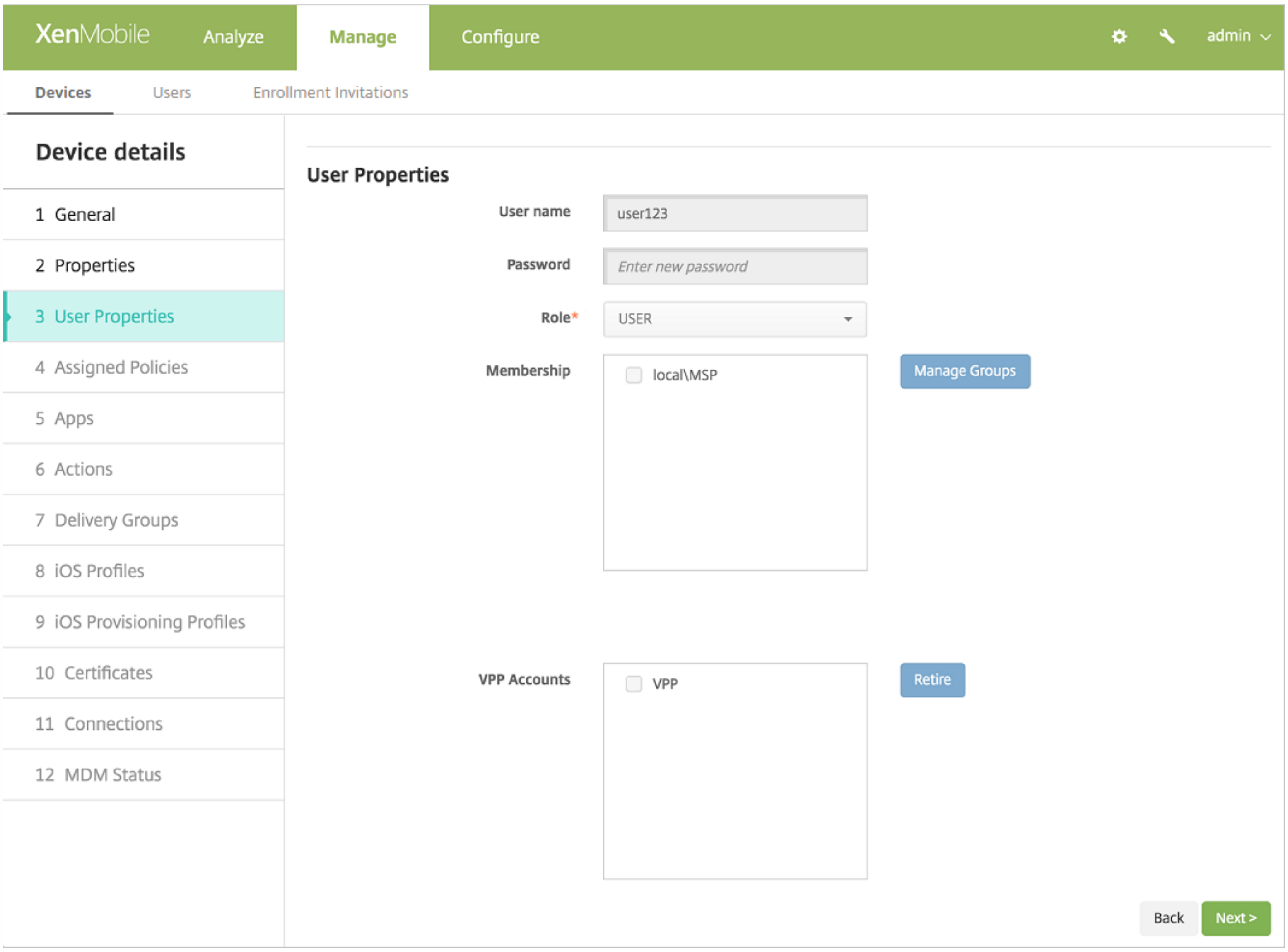
License Usage: 2 of 2

	License ID	Usage Status	Associated User	Associated Device
☑	82684302	Used	[redacted]	
□	82684301	Used		F9FMW440FCM5

Showing 1 - 2 of 2 items

VPP License Keys

If you associate VPP licenses with users, XenMobile integrates users into your VPP account and associates their iTunes ID with the VPP account. The iTunes ID of users is never visible to your company or to the XenMobile Server. Apple transparently creates the association to retain user privacy. You can retire a user from the VPP program, to disassociate all licenses from the user account. To retire a user, go to **Manage > Devices**.



User Properties

User name: user123

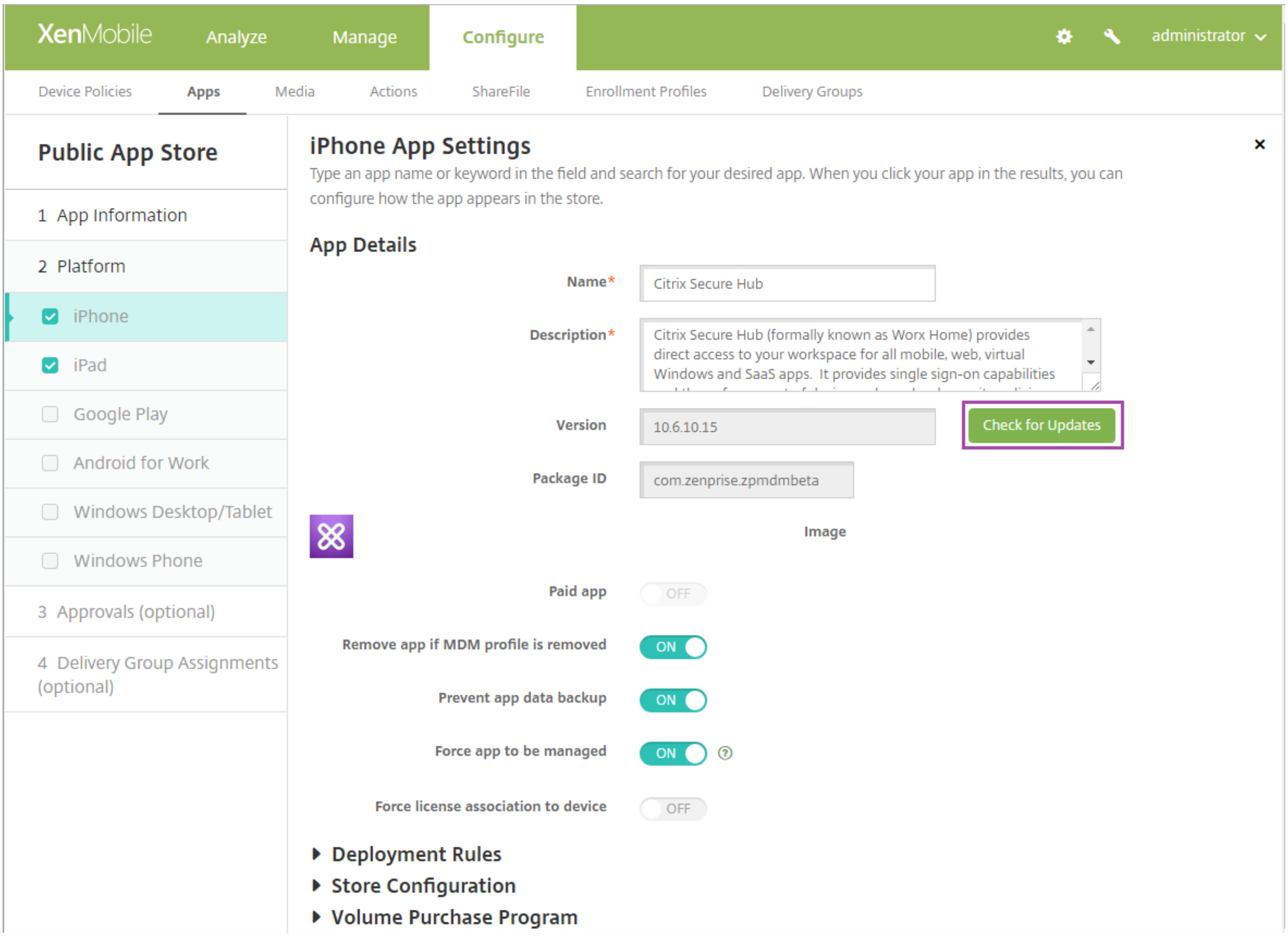
Password: *Enter new password*

Role*: USER

Membership: □ local\MSP

VPP Accounts: □ VPP

- When you assign an app to a delivery group, by default XenMobile identifies the app as an optional app. To ensure that XenMobile 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 VPP pushes the app, the app doesn't automatically update on devices until you check for updates and apply them. 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.



iPhone App Settings

Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

App Details

Name* Citrix Secure Hub

Description* Citrix Secure Hub (formally known as Worx Home) provides direct access to your workspace for all mobile, web, virtual Windows and SaaS apps. It provides single sign-on capabilities

Version 10.6.10.15

Package ID com.zenprise.zpmdmbeta

Paid app OFF

Remove app if MDM profile is removed ON

Prevent app data backup ON

Force app to be managed ON

Force license association to device OFF

XenApp and XenDesktop through Citrix Secure Hub

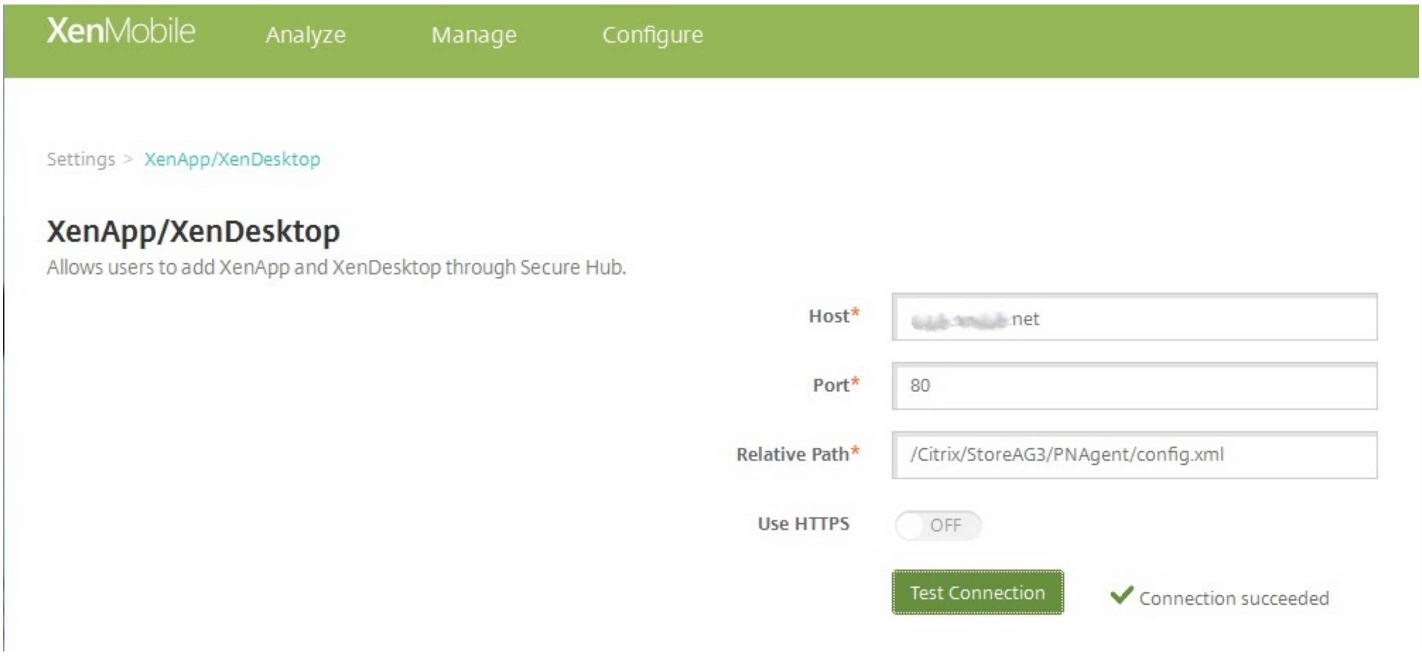
Sep 06, 2017

XenMobile can collect apps from XenApp and XenDesktop and make them available to mobile device users in the XenMobile Store. Users subscribe to the apps directly inside XenMobile Store and launch them from Secure Hub. Citrix Receiver must be installed on users' devices to launch the apps, but it does not need to be configured.

To configure this setting, you need the fully qualified domain name (FQDN) or IP address and port number for the Web Interface site or StoreFront.

1. In the XenMobile web console, click the gear icon in the upper-right corner. The **Settings** page appears.

2. Click **XenApp/XenDesktop**. The **XenApp/XenDesktop** page appears.



Settings > XenApp/XenDesktop

XenApp/XenDesktop

Allows users to add XenApp and XenDesktop through Secure Hub.

Host* [redacted]net

Port* 80

Relative Path* /Citrix/StoreAG3/PNAgent/config.xml

Use HTTPS OFF

✓ Connection succeeded

3. Configure these settings:

- **Host:** Type the fully qualified domain name (FQDN) or IP address for the Web Interface site or StoreFront.
- **Port:** Type the port number for the Web Interface site or 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 the Web Interface site or StoreFront and the client device. The default is **OFF**.

4. Click **Test Connection** to verify that XenMobile can connect to the specified XenApp and XenDesktop server.

5. Click **Save**.

ShareFile use with XenMobile

Oct 19, 2017

XenMobile has two options for integrating with ShareFile: ShareFile Enterprise and StorageZone Connectors. Integration with ShareFile Enterprise or StorageZone Connectors requires XenMobile Enterprise Edition.

ShareFile Enterprise

If you have XenMobile Enterprise Edition, you can configure XenMobile to provide access to your ShareFile Enterprise account. That configuration:

- Gives mobile users access to the full ShareFile feature set, such as file sharing, file sync, and StorageZone Connectors.
- Can provide ShareFile with single sign-on authentication of XenMobile App users, AD-based user account provisioning, and comprehensive access control policies.
- Provides ShareFile configuration, service level monitoring, and license usage monitoring through the XenMobile console.

For more information about configuring XenMobile for ShareFile Enterprise, see SAML for single sign-on with ShareFile.

StorageZone Connectors

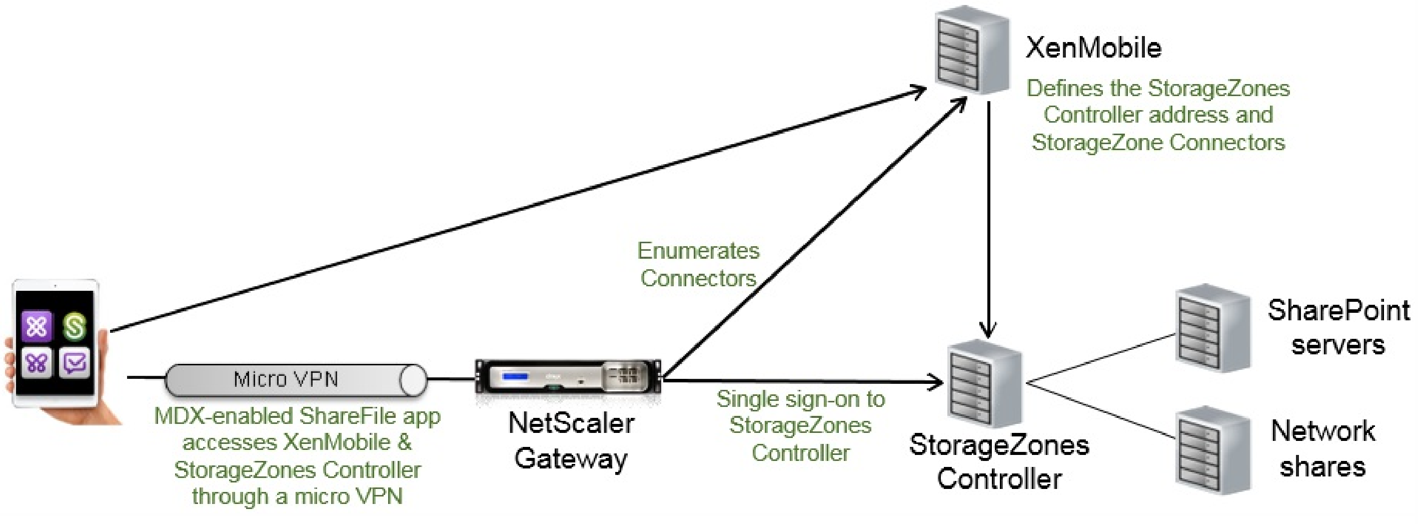
You can configure XenMobile to provide access only to StorageZone Connectors that you create through the XenMobile console. That configuration:

- Provides secure mobile access to existing on-premises storage repositories, such as SharePoint sites and network file shares.
- Doesn't require that you set up a ShareFile subdomain, provision users to ShareFile, or host ShareFile data.
- Provides users with mobile access to data through the ShareFile XenMobile Apps 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 StorageZone Connectors through the XenMobile console. If you later decide to use the full ShareFile functionality with XenMobile, you can change the configuration in the XenMobile console.
- Requires XenMobile Enterprise Edition.

For a XenMobile integration with StorageZone Connectors only:

- ShareFile uses your single sign-on configuration to NetScaler Gateway to authenticate with StorageZones Controller.
- XenMobile doesn't authenticate through SAML because the ShareFile control plane isn't used.

The following diagram shows the high-level architecture for XenMobile use with StorageZone Connectors.


XenMobile
Defines the StorageZones Controller address and StorageZone Connectors
Enumerates Connectors
SharePoint servers
Micro VPN
MDX-enabled ShareFile app accesses XenMobile & StorageZones Controller through a micro VPN
NetScaler Gateway
Single sign-on to StorageZones Controller
StorageZones Controller
Network shares

- Minimum component versions:
  - XenMobile Server 10.5 (on-premises)
  - ShareFile for iOS (MDX) 5.3
  - ShareFile for Android (MDX) 5.3
  - ShareFile StorageZones Controller 5.0

    This article contains instructions for how to configure ShareFile StorageZones Controller 5.0
- Ensure that the server to run StorageZones Controller meets the system requirements. For requirements, see the following sections in "System requirements" in the ShareFile StorageZones Controller documentation:
  - StorageZones Controller
  - StorageZone Connector for SharePoint
  - StorageZone Connector for Network File Shares

    The requirements for StorageZones for ShareFile Data and for Restricted StorageZones don't apply to a XenMobile integration with StorageZone Connectors only.

    XenMobile doesn't support Documentum connectors.
- To run PowerShell scripts:
  - Run the scripts in the 32-bit (x86) version of PowerShell.

Complete the following tasks, in the order presented, to install and set up StorageZones Controller. These steps are specific to XenMobile integration with StorageZone Connectors only. Some of these articles are in the StorageZones Controller documentation.

1. Configure NetScaler for StorageZones Controller

   You can use NetScaler as a DMZ proxy for StorageZones Controller.

2. Install an SSL certificate

   A StorageZones Controller that hosts standard zones requires an SSL certificate. A StorageZones 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 StorageZone Connectors.

4. Install StorageZones Controller

5. Prepare StorageZones Controller for use with StorageZone Connectors-only

6. Specify a proxy server for StorageZones

   The StorageZones Controllers console enables you to specify a proxy server for StorageZones Controllers. You can also specify a proxy server using other methods.

7. Configure the domain controller to trust the StorageZones Controller for delegation

   Configure the domain controller to support NTLM or Kerberos authentication on network shares or SharePoint sites.

8. Join a secondary StorageZones Controller to a StorageZone

   To configure a StorageZone for high availability, connect at least two StorageZones Controllers to it.

1. Download and install the StorageZones Controller software:

   a. From the ShareFile download page at http://www.citrix.com/downloads/sharefile.html, log on and download the latest StorageZones Controller installer.

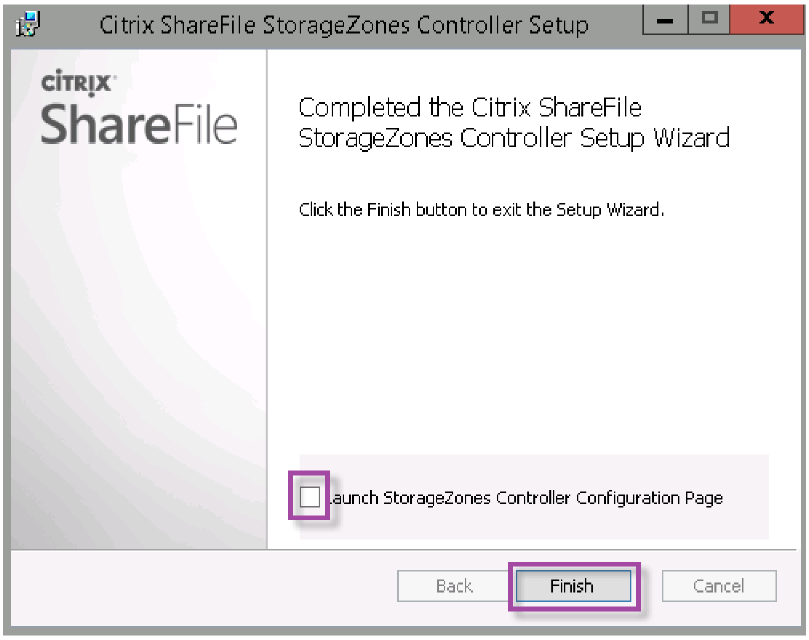
   b. Installing StorageZones Controller changes the default website on the server to the installation path of the controller. Enable **Anonymous Authentication** on the default website.

2. On the server where you want to install StorageZones Controller, run StorageCenter.msi.

   The ShareFile StorageZones 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 StorageZones Controller Configuration Page** and then click **Finish**.



Completed the Citrix ShareFile StorageZones Controller Setup Wizard

Click the Finish button to exit the Setup Wizard.

□ Launch StorageZones Controller Configuration Page

4. When prompted, restart the StorageZones Controller.

5. To test that the installation was successful, navigate to http://localhost/. If the installation is successful, the ShareFile logo appears.

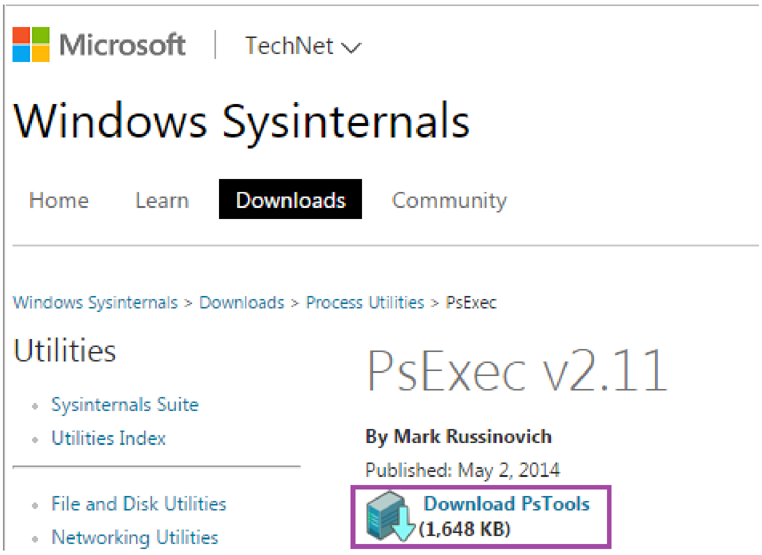
If the ShareFile logo does not appear, clear the browser cache and try again.

> ## Important
>
> If you plan to clone the StorageZones Controller, capture the disk image before you proceed with configuring the StorageZones Controller.

For an integration only with StorageZone Connectors, you don't use the StorageZones Controller administrative console. That interface requires a ShareFile administrator account, which isn't necessary for this solution. As a result, you run a PowerShell script to prepare the StorageZones Controller for use without the ShareFile control plane. The script does the following:

- Registers the current StorageZones Controller as a primary StorageZones Controller. You can later join secondary StorageZones Controllers to the primary controller.
- Creates a zone and sets the passphrase for it.

1. From your StorageZone 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.



Microsoft | TechNet

Windows Sysinternals

Home Learn Downloads Community

Windows Sysinternals > Downloads > Process Utilities > PsExec

Utilities

- Sysinternals Suite
- Utilities Index

- File and Disk Utilities
- Networking Utilities

PsExec v2.11

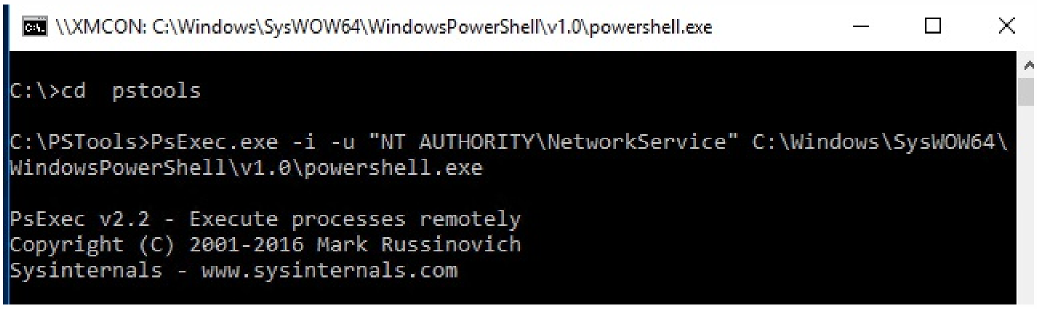
By Mark Russinovich

Published: May 2, 2014

Download PsTools (1,648 KB)

2. Run the PsExec tool: Open the Command Prompt as the Administrator User and then type the following:

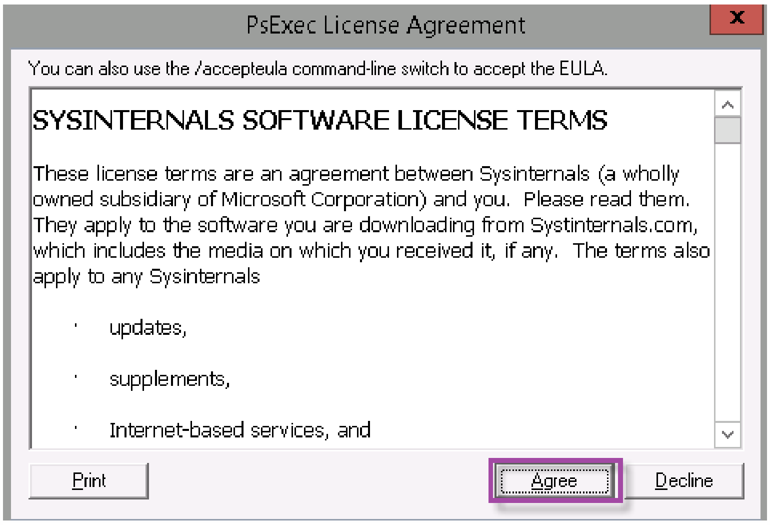
```
cd c:\pstools

PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



\\XMCON: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

```
C:\>cd  pstools

C:\PSTools>PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\
WindowsPowerShell\v1.0\powershell.exe

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

3. When prompted, click **Agree** to run the Sysinternals tool.



You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

A PowerShell widow opens.

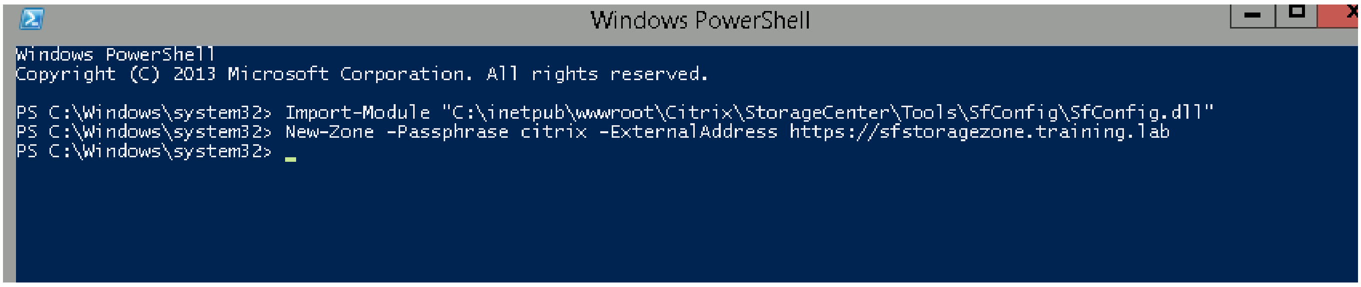
4. In the PowerShell window, type the following:

```
Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

New-Zone  -Passphrase passphrase -ExternalAddress https://szcfqdn.com
```

Where:

Passphrase: Is the passphrase 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 StorageZones, join more StorageZones Controllers to the StorageZone, or recover the StorageZone if the server fails.

ExternalAddress: Is the external fully qualified domain name of the StorageZones Controller server.



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"
PS C:\Windows\system32> New-Zone -Passphrase citrix -ExternalAddress https://sfstoragezone.training.lab
PS C:\Windows\system32> _
```

Your primary StorageZones Controller is now ready.

Before you log in to XenMobile to create StorageZone Connectors: Complete the following configuration, if applicable:

Specify a proxy server for StorageZones

Configure the domain controller to trust the StorageZones Controller for delegation

Join a secondary StorageZones Controller to a StorageZone

To create StorageZone Connectors, see Define StorageZones Controller connections in XenMobile.

To configure a StorageZone for high availability, connect at least two StorageZones Controllers to it. To join a secondary StorageZones Controller to a zone, install StorageZones Controller on a second server. Then join that controller to the zone of the primary controller.

1. Open a PowerShell window on the StorageZones Controller server that you want to join to the primary server.

2. In the PowerShell window, type the following:

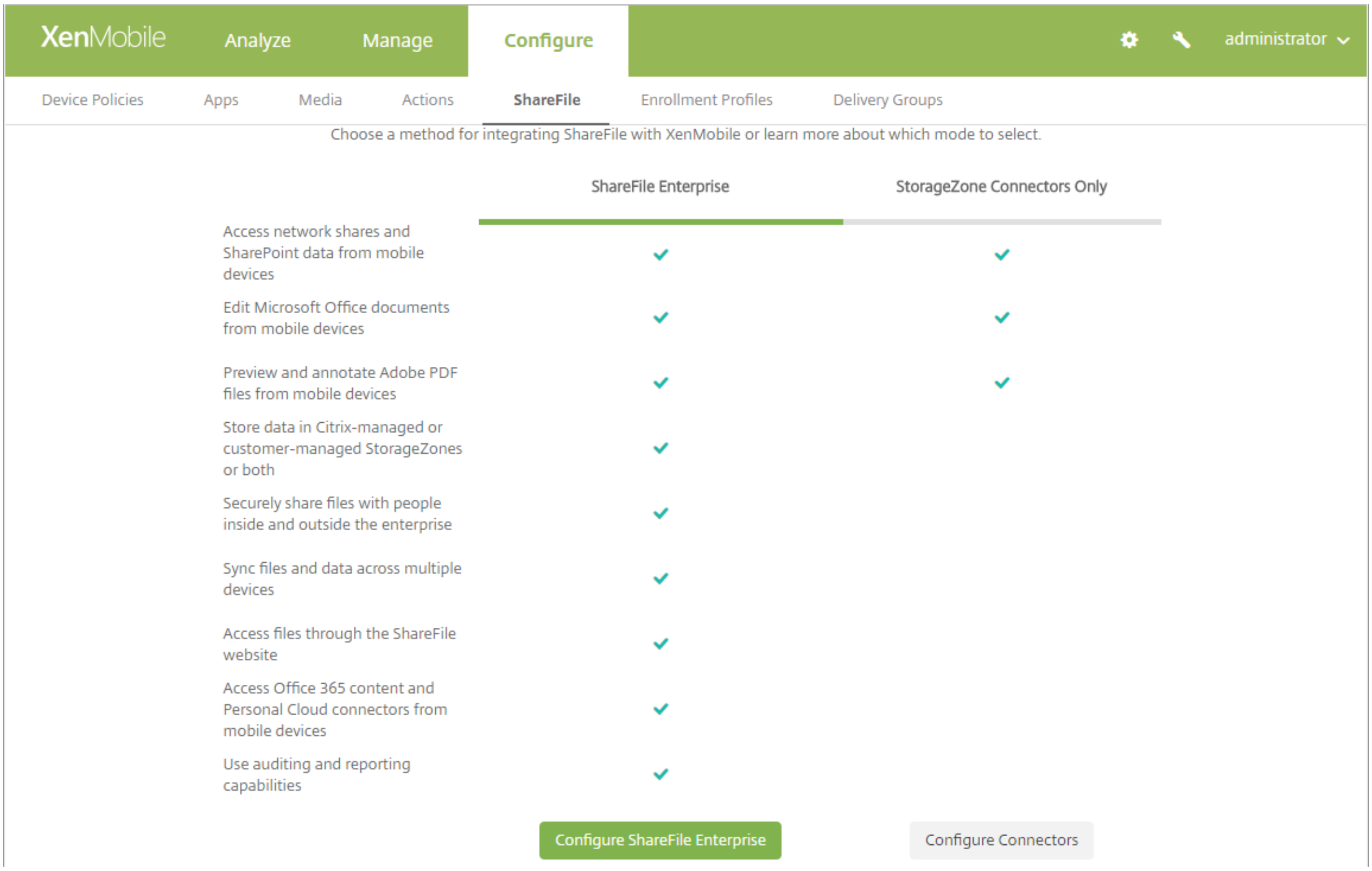
```
Join-Zone -Passphrase <passphrase> -PrimaryController <HostnameOrIP>
```

For example:

```
Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
```

Before you add StorageZone Connectors, you configure connection information for each StorageZones Controller enabled for StorageZone Connectors. You can define StorageZones Controllers as described in this section, or when you add a connector.

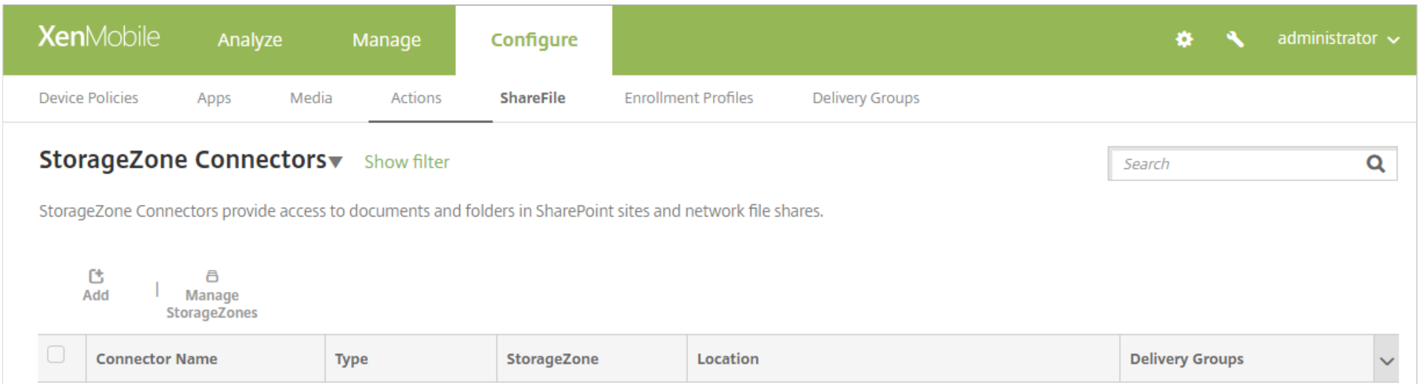
On your first visit to the **Configure > ShareFile** page, the page summarizes the differences between using XenMobile with ShareFile Enterprise and with StorageZone Connectors.



Choose a method for integrating ShareFile with XenMobile or learn more about which mode to select.

	ShareFile Enterprise	StorageZone Connectors Only
Access network shares and SharePoint data from mobile devices	✓	✓
Edit Microsoft Office documents from mobile devices	✓	✓
Preview and annotate Adobe PDF files from mobile devices	✓	✓
Store data in Citrix-managed or customer-managed StorageZones or both	✓	
Securely share files with people inside and outside the enterprise	✓	
Sync files and data across multiple devices	✓	
Access files through the ShareFile website	✓	
Access Office 365 content and Personal Cloud connectors from mobile devices	✓	
Use auditing and reporting capabilities	✓	

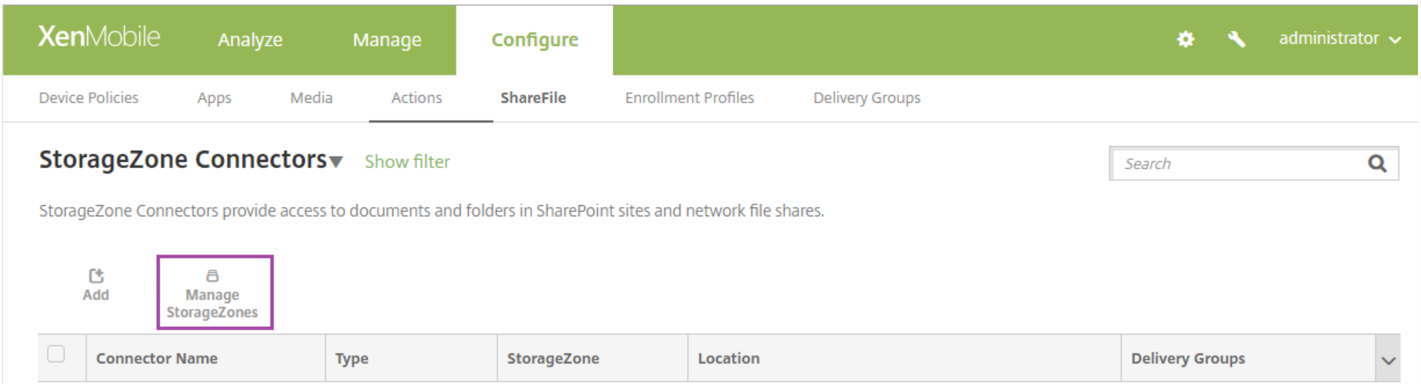
Click **Configure Connectors** to continue with the configuration steps in this article.



StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

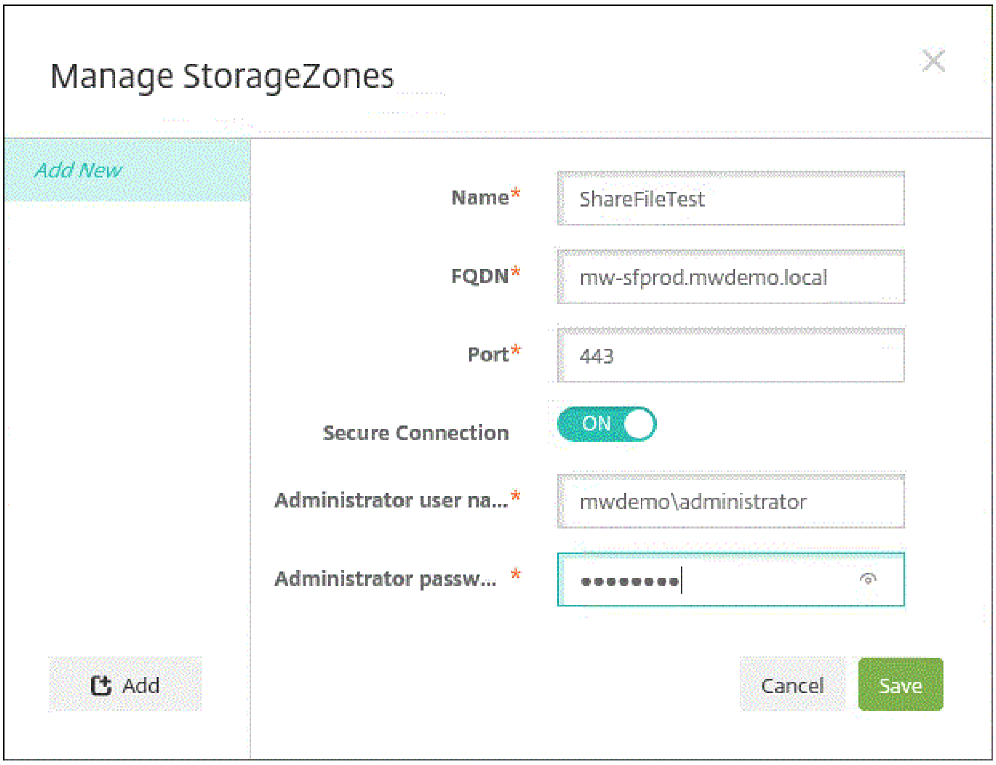
□	Connector Name	Type	StorageZone	Location	Delivery Groups

1. In **Configure > ShareFile**, click **Manage StorageZones**.



StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

2. In **Manage StorageZones**, add the connection information.



Manage StorageZones

Add New

Name*	ShareFileTest
FQDN*	mw-sfprod.mwdemo.local
Port*	443
Secure Connection	ON
Administrator user na...*	mwdemo\administrator
Administrator passw... *	••••••••

- **Name**: A descriptive name for the StorageZone, used to identify the StorageZone in XenMobile. Don't include a space or special characters in the name.
- **FQDN and Port**: The fully qualified domain name and port number for a StorageZones Controller that is reachable from the XenMobile Server.
- **Secure Connection**: If you use SSL for connections to StorageZones 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 StorageZones Controllers.

3. Click **Save**.

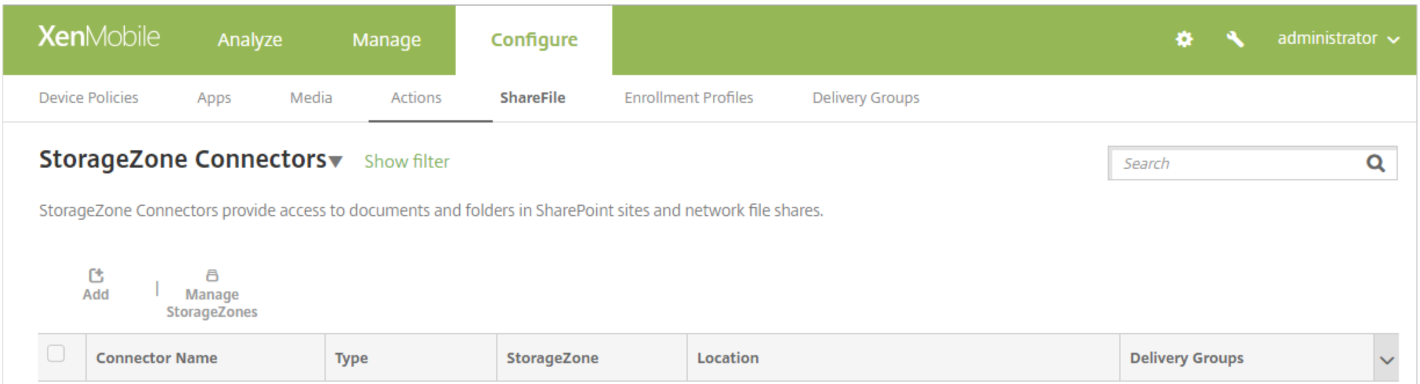
4. To test the connection, verify that XenMobile Server can reach the fully qualified domain name of the StorageZones

Controller on port 443.

5. To define another StorageZones Controller connection, click the **Add** button in **Manage StorageZones**.

To edit or delete the information for a StorageZones Controller connection, select the connection name in **Manage StorageZones**. Then, click **Edit** or **Delete**.

1. Go to **Configure** > **ShareFile** and then click **Add**.

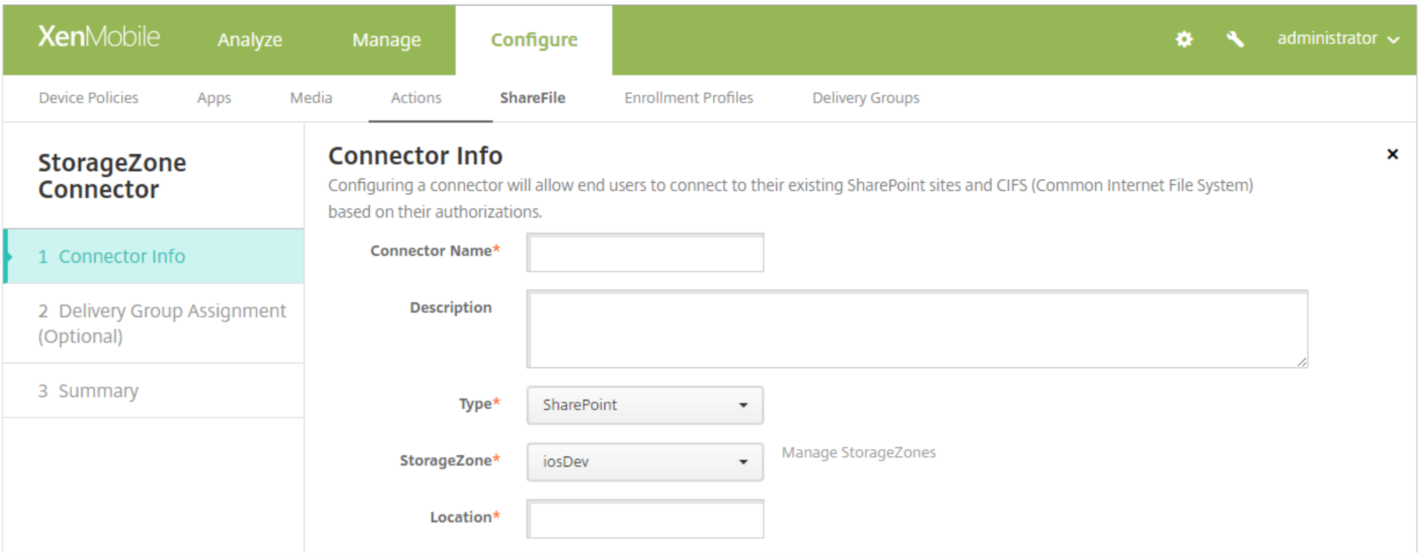


StorageZone Connectors

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

□	Connector Name	Type	StorageZone	Location	Delivery Groups

2. On the **Connector Info** page, configure these settings:



Connector Info

Configuring a connector will allow end users to connect to their existing SharePoint sites and CIFS (Common Internet File System) based on their authorizations.

Connector Name*

Description

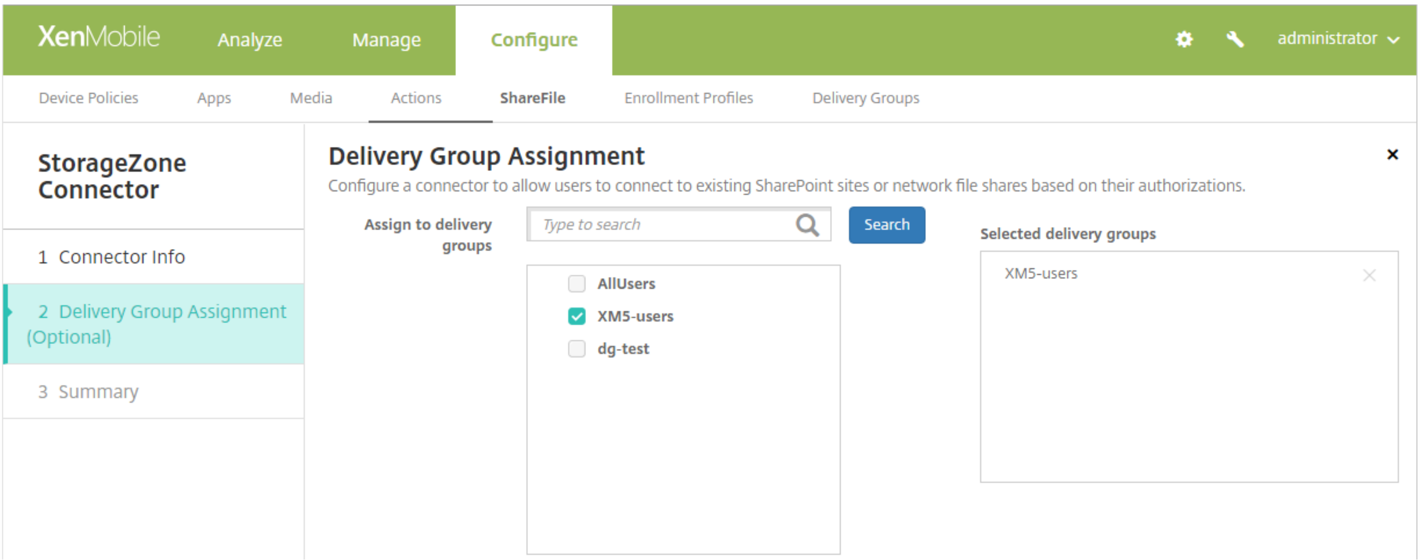
Type* SharePoint

StorageZone* iosDev

Location*

- **Connector Name**: A name that identifies the StorageZone Connector in XenMobile.
- **Description**: Optional notes about this Connector.
- **Type**: Choose either **SharePoint** or **Network**.
- **StorageZone**: Choose the StorageZone associated with the Connector. If the StorageZone isn't listed, click **Manage StorageZones** to define the StorageZones 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**.



Delivery Group Assignment

Configure a connector to allow users to connect to existing SharePoint sites or network file shares based on their authorizations.

Assign to delivery groups

☐ AllUsers
☑ XM5-users
☐ dg-test

Selected delivery groups: XM5-users

4. On the **Summary** page, you can review the options you configured. To adjust the configuration, click **Back**.

5. Click **Save** to save the Connector.

6. Test the connector:

a. When you wrap the ShareFile clients, do the following:

- Set the Network access policy to **Tunneled to the internal network**.

  In this mode of operation, the XenMobile MDX framework intercepts all network traffic from the ShareFile client. The traffic redirects through NetScaler Gateway by using an app-specific micro VPN.

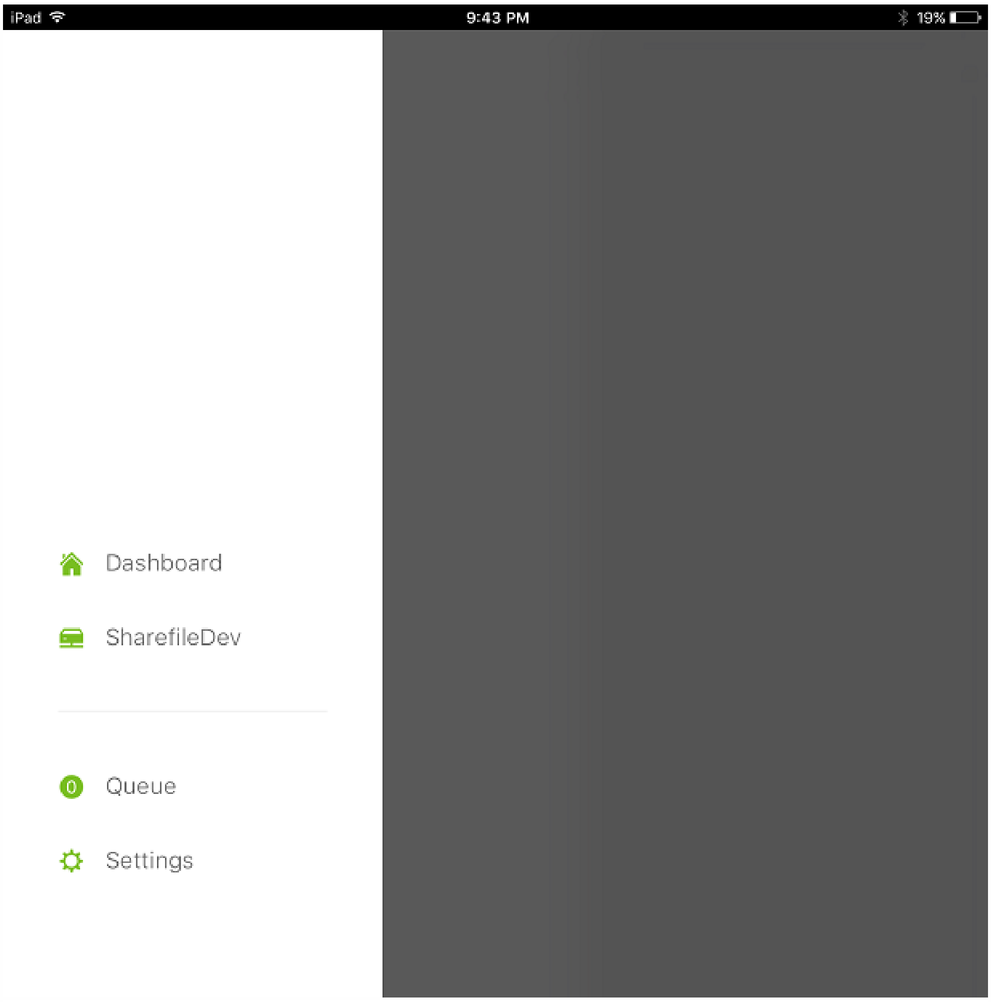
- Set the Preferred VPN mode policy to **Secure browse**.

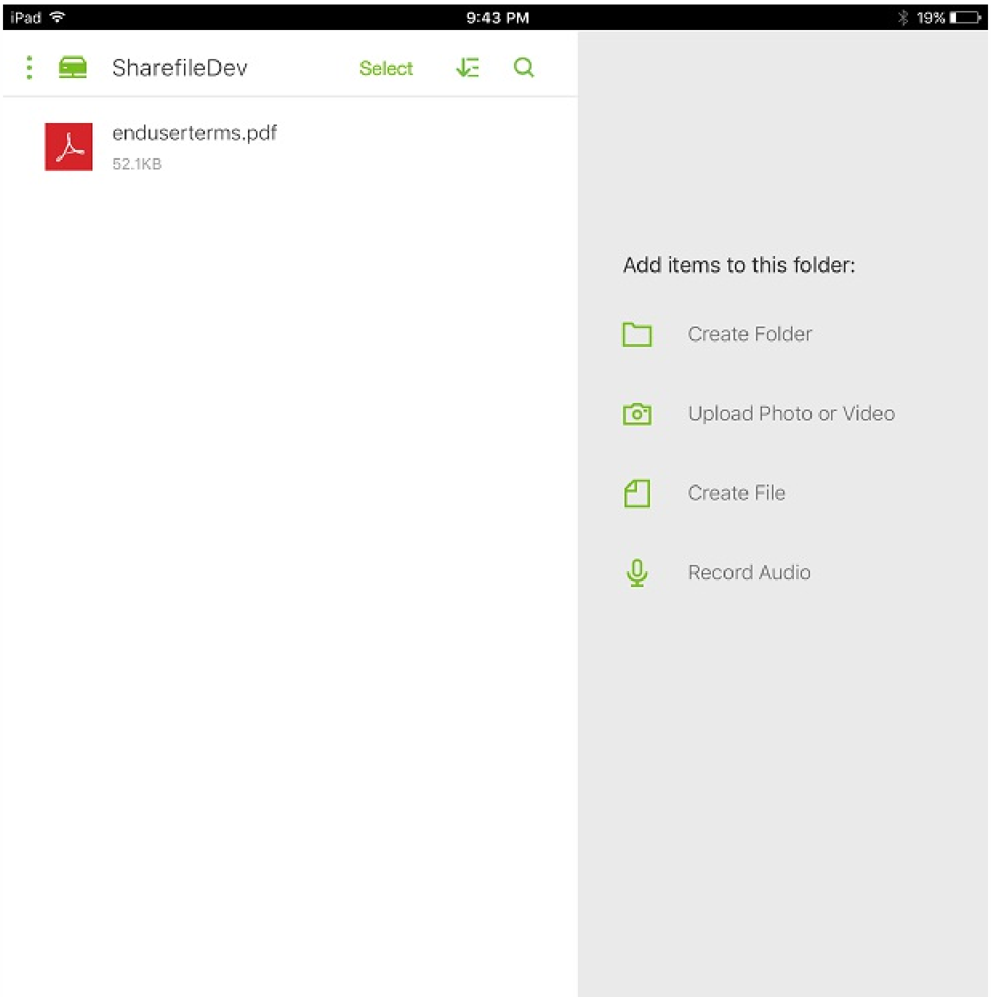
  In this mode of tunneling, the MDX framework terminates SSL/HTTP traffic from an MDX app. MDX then initiates new connections to internal connections on behalf of the user. This policy setting enables the MDX framework to detect and respond to authentication challenges issued by web servers.

b. Add the ShareFile clients to XenMobile. For details, see To add ShareFile clients to XenMobile.

c. From a supported device, verify single sign-on to ShareFile and connectors.

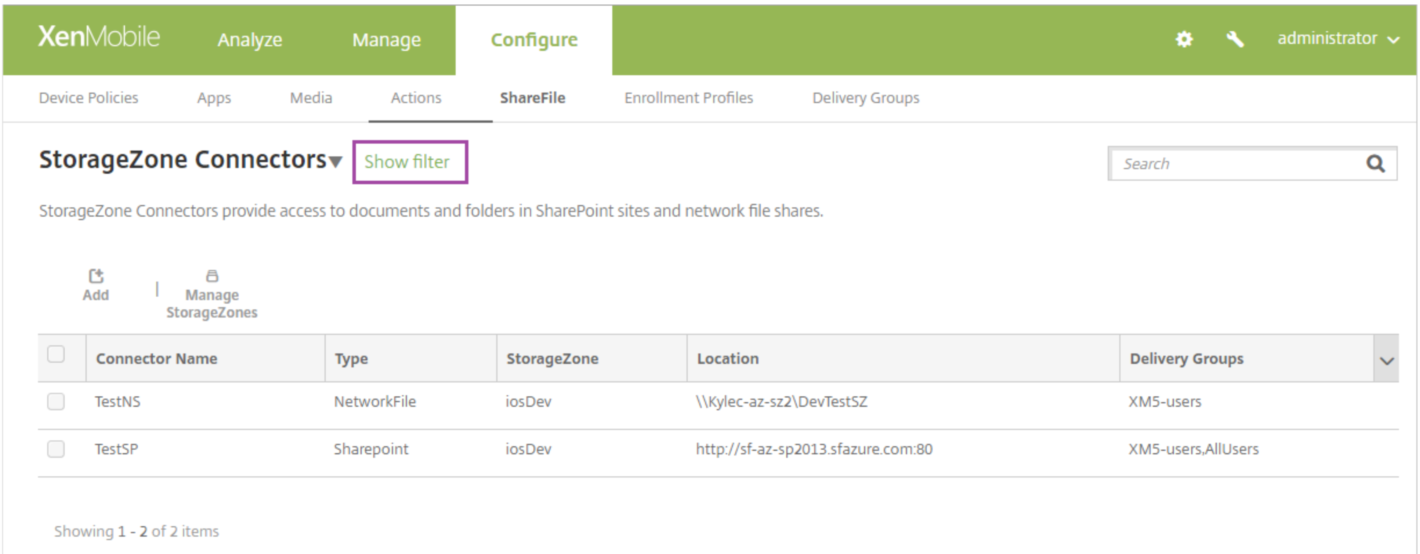
In the following samples, SharefileDev is the name of a connector.


iPad
9:43 PM
19%
Dashboard
SharefileDev
0
Queue
Settings



You can filter the list of StorageZone Connectors by Connector type, assigned delivery groups, and StorageZone.

1. Go to **Configure > ShareFile** and then click **Show filter**.

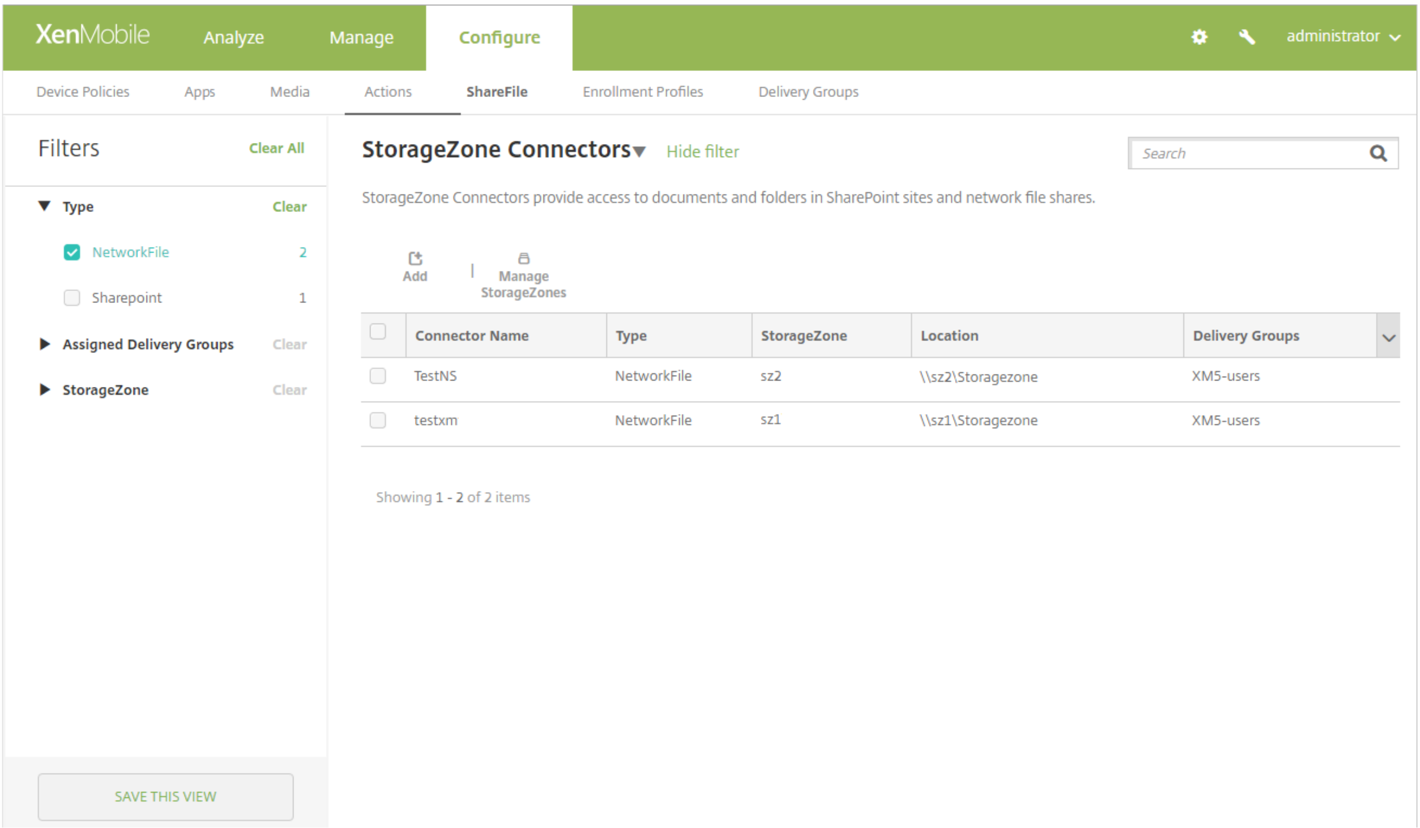


StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

	Connector Name	Type	StorageZone	Location	Delivery Groups
□	TestNS	NetworkFile	iosDev	\\Kylec-az-sz2\DevTestSZ	XM5-users
□	TestSP	Sharepoint	iosDev	http://sf-az-sp2013.sfazure.com:80	XM5-users,AllUsers

Showing 1 - 2 of 2 items

2. Expand the filter headings to make selections. To save a filter, click **Save This View**, type the filter name, and click **Save**.

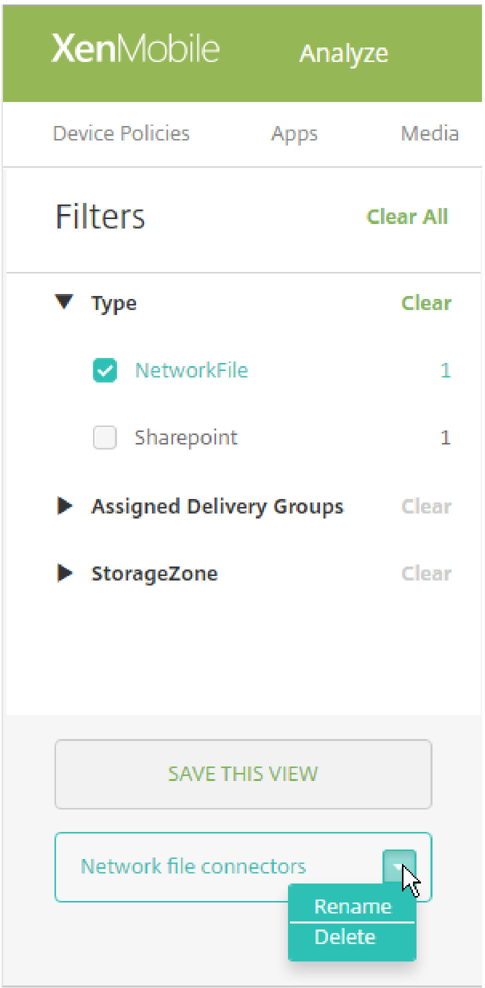


StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

□	Connector Name	Type	StorageZone	Location	Delivery Groups
□	TestNS	NetworkFile	sz2	\\sz2\Storagezone	XM5-users
□	testxm	NetworkFile	sz1	\\sz1\Storagezone	XM5-users

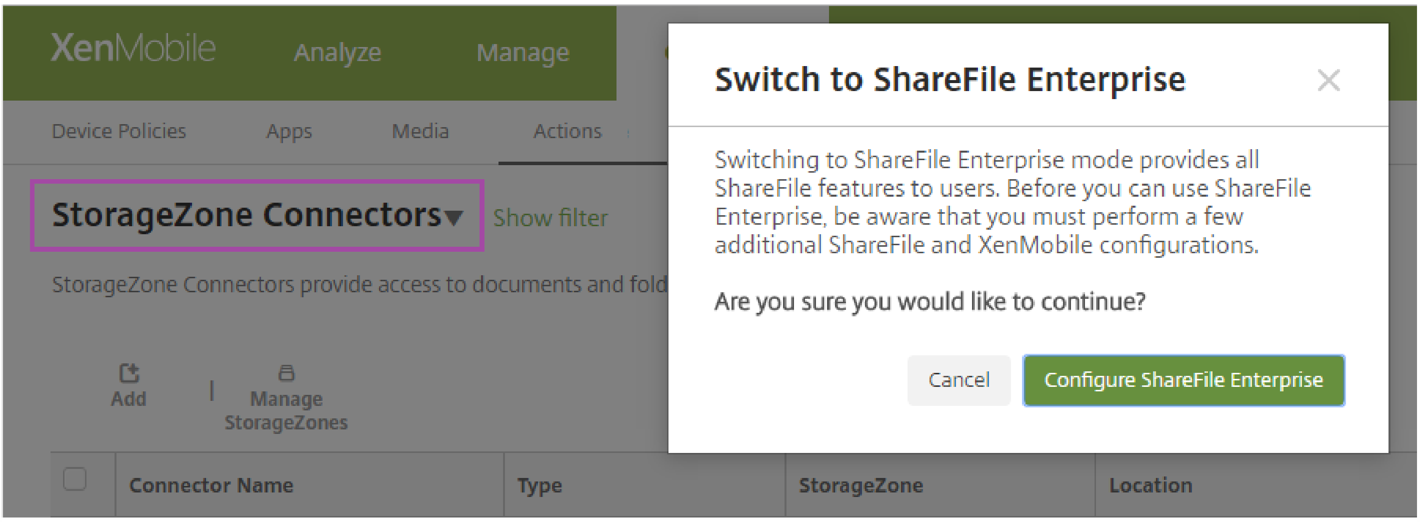
Showing 1 - 2 of 2 items

3. To rename or delete a filter, click the arrow icon beside the filter name.



After integrating StorageZone Connectors with XenMobile, you can later switch to the full ShareFile Enterprise feature set. Use of the ShareFile Enterprise feature set requires XenMobile Enterprise Edition. XenMobile retains your existing StorageZone Connector integration settings.

Go to **Configure > ShareFile**, click the **StorageZone Connectors** drop-down menu, and then click **Configure ShareFile Enterprise**.



Switch to ShareFile Enterprise

StorageZone Connectors provide access to documents and fold

Switching to ShareFile Enterprise mode provides all ShareFile features to users. Before you can use ShareFile Enterprise, be aware that you must perform a few additional ShareFile and XenMobile configurations.

Are you sure you would like to continue?

For information about configuring ShareFile Enterprise, see SAML for single sign-on with ShareFile.

SmartAccess for HDX apps

Sep 06, 2017

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 XenApp and XenDesktop by using a SmartAccess policy that denies access to out-of-compliance devices. XenMobile 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:

- XenApp and XenDesktop 7.6
- StoreFront 3.7 or 3.8
- XenMobile Server configured aggregate HDX apps from a StoreFront server
- XenMobile Server configured with a SAML certificate to be used for signing and encrypting tags. The same certificate without private key is uploaded on StoreFront server.

To start using this feature:

- Configure the XenMobile Server certificate to the StoreFront store
- Configure at least one XenApp and XenDesktop delivery group with the required SmartAccess policy
- Set the automated action in XenMobile

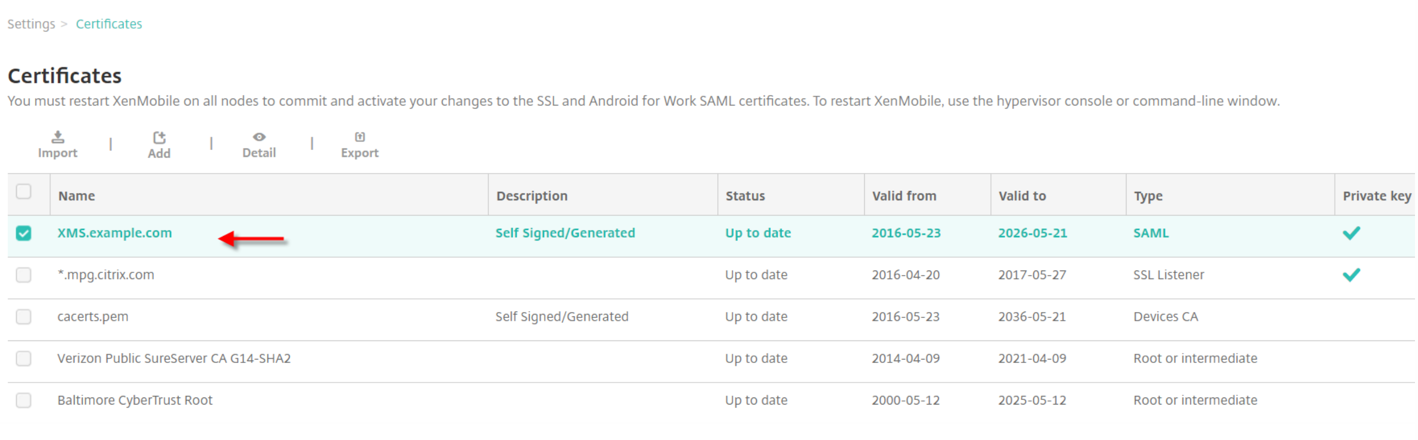
Export and configure the XenMobile Server certificate and upload it to the StoreFront store

SmartAccess uses signed and encrypted tags to communicate between the XenMobile and StoreFront servers. To enable that communication, you add the XenMobile Server certificate to the StoreFront store.

For more information about integrating StoreFront and XenMobile when XenMobile is enabled with domain and certificate-based authentication, see the Support Knowledge Center.

1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears. Click **Certificates**.

2. Locate the SAML certificate for XenMobile Server.



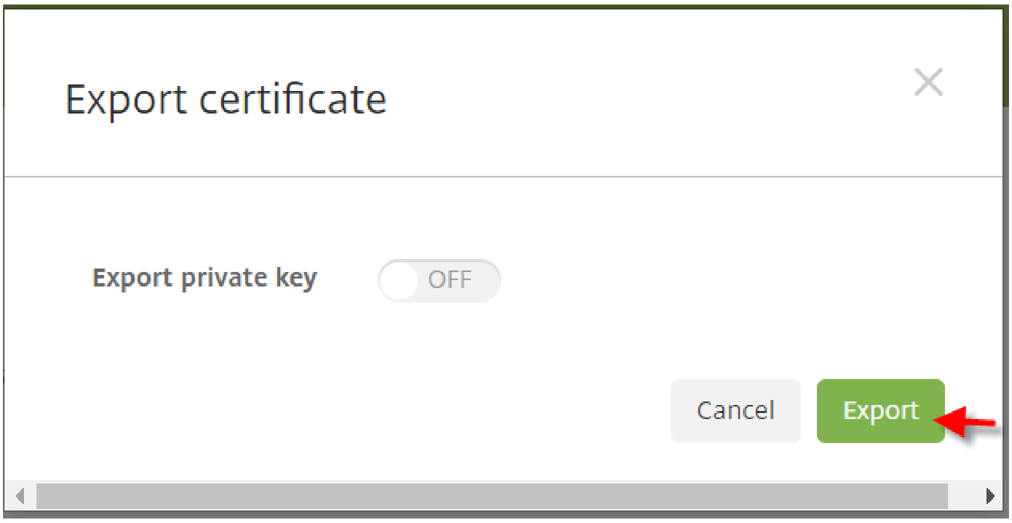
Settings > Certificates

Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

	Name	Description	Status	Valid from	Valid to	Type	Private key
☑	XMS.example.com	Self Signed/Generated	Up to date	2016-05-23	2026-05-21	SAML	✓
□	*.mpg.citrix.com		Up to date	2016-04-20	2017-05-27	SSL Listener	✓
□	cacerts.pem	Self Signed/Generated	Up to date	2016-05-23	2036-05-21	Devices CA	
□	Verizon Public SureServer CA G14-SHA2		Up to date	2014-04-09	2021-04-09	Root or intermediate	
□	Baltimore CyberTrust Root		Up to date	2000-05-12	2025-05-12	Root or intermediate	

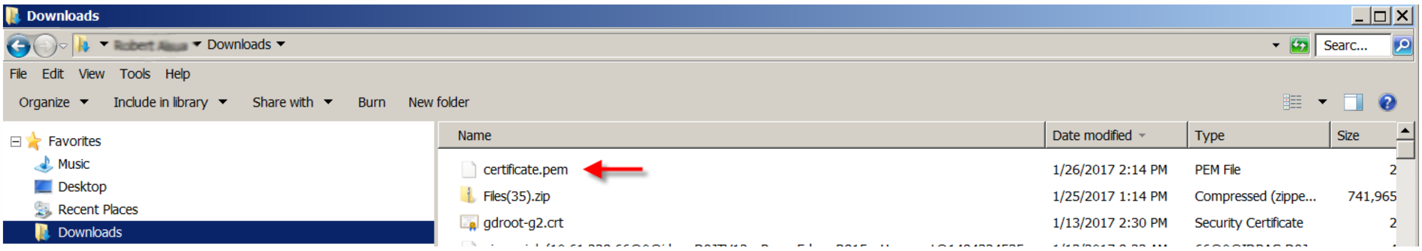
3. Ensure that **Export private key** is set to **Off**. Click **Export** to export the certificate to your download directory.



Export certificate

Export private key: OFF

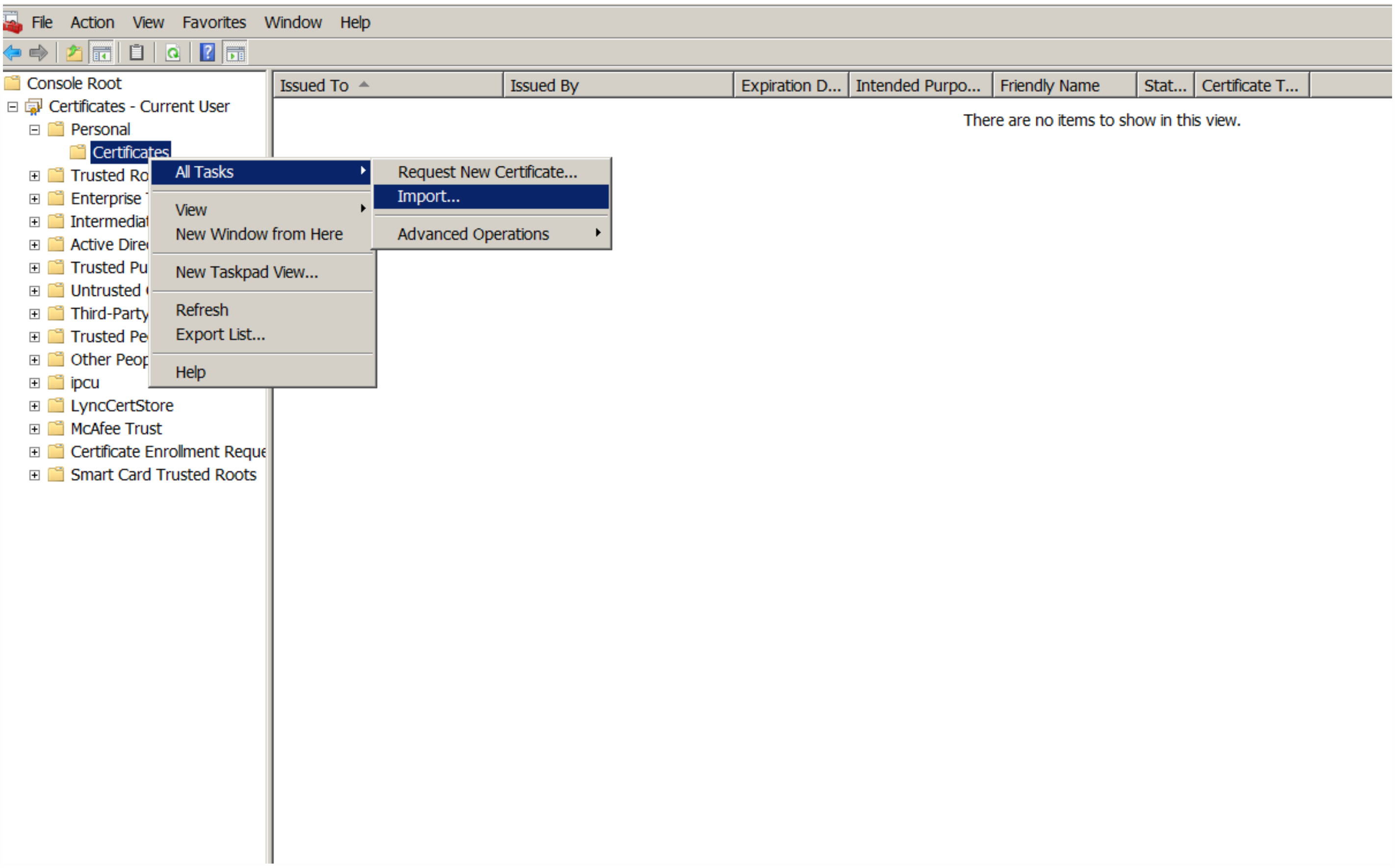
4. Locate the certificate in your download directory. The certificate is in PEM format.



Downloads
[redacted] ▸ Downloads ▸
Searc...
File Edit View Tools Help
Organize ▾ Include in library ▾ Share with ▾ Burn New folder
Favorites
Music
Desktop
Recent Places
Downloads

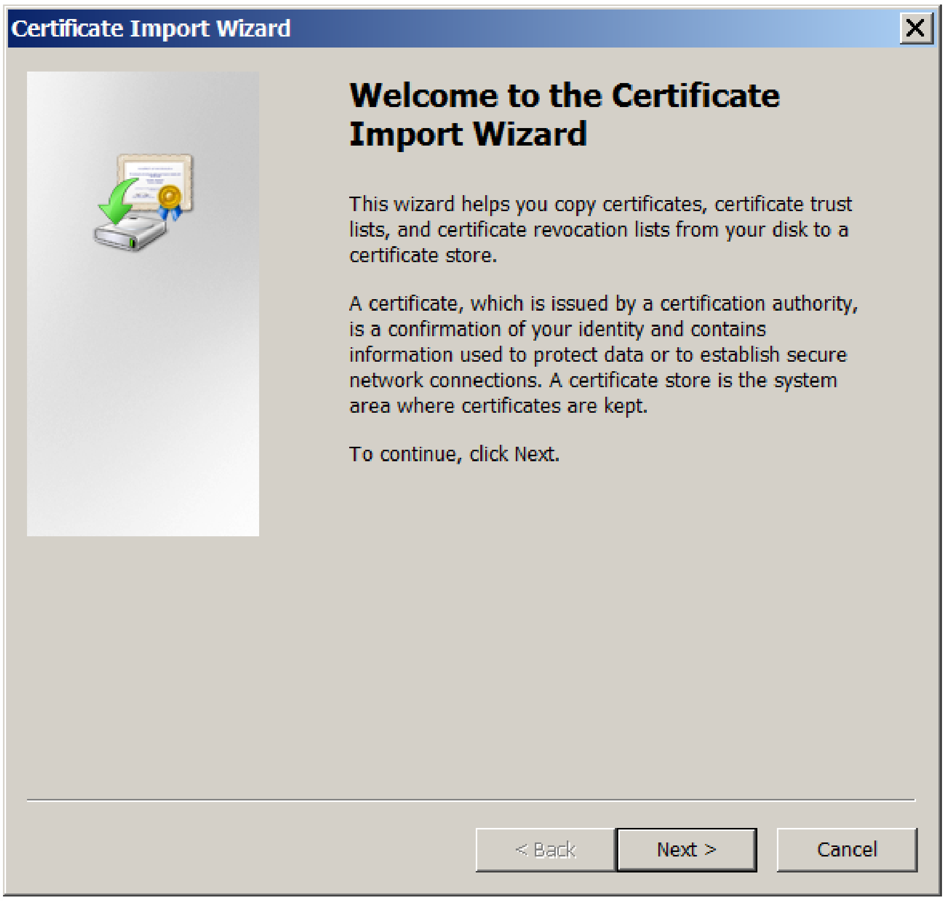
Name	Date modified	Type	Size
certificate.pem	1/26/2017 2:14 PM	PEM File	2
Files(35).zip	1/25/2017 1:14 PM	Compressed (zippe...	741,965
gdroot-g2.crt	1/13/2017 2:30 PM	Security Certificate	2

1. Open the Microsoft Management Console (MMC) and right-click **Certificates > All Tasks > Import**.



There are no items to show in this view.

2. When the certificate import wizard appears, click **Next**.



Certificate Import Wizard

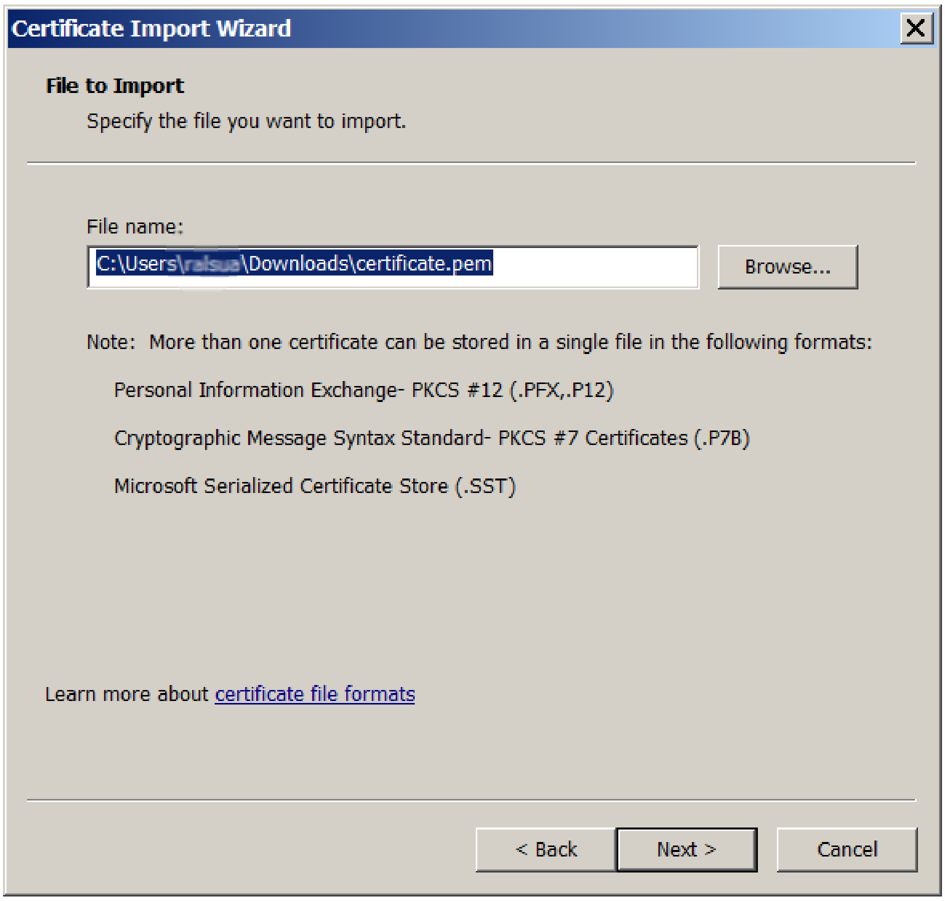
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

3. Browse to the certificate in the download directory.



File to Import

Specify the file you want to import.

File name:

C:\Users\[redacted]\Downloads\certificate.pem

Note: More than one certificate can be stored in a single file in the following formats:

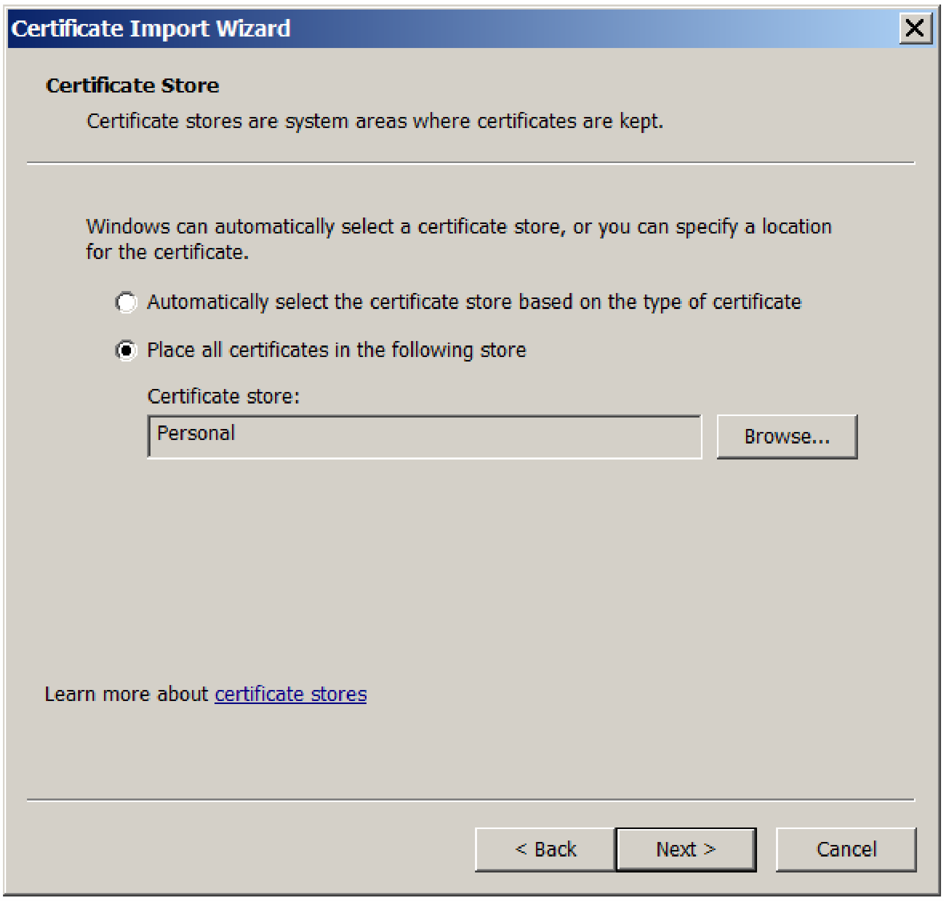
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

4. Select **Place all certificates in the following store** and select **Personal** as the certificate store. Click **Next**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

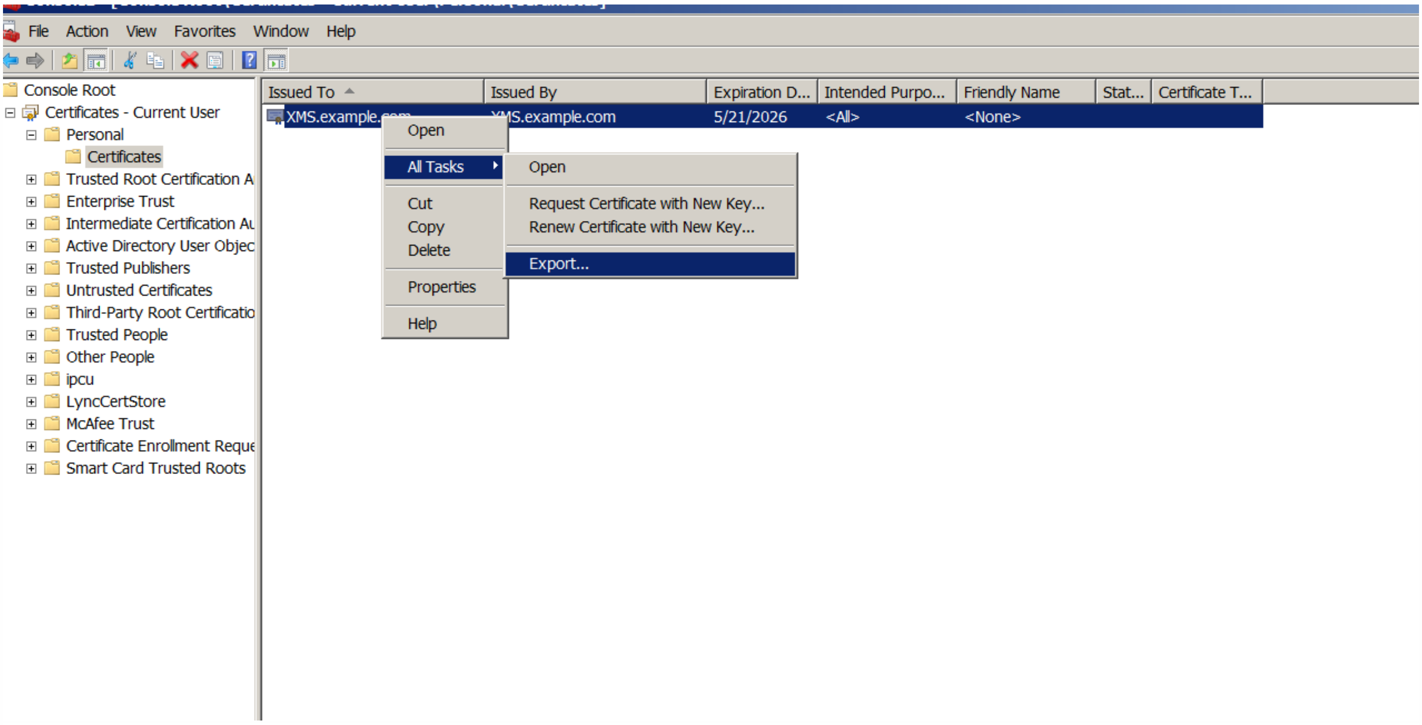
Certificate store:

Personal

Learn more about certificate stores

5. Review your selections and click **Finish**. Click **OK** to dismiss the confirmation window.

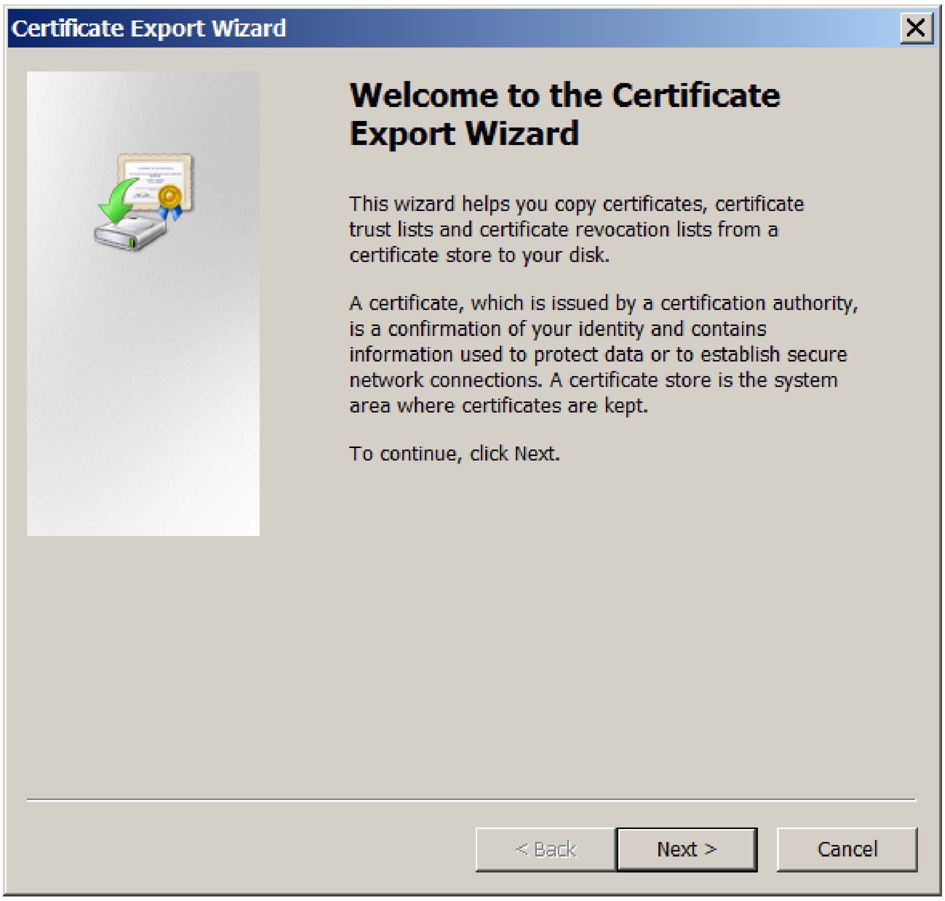
6. In the MMC, right-click the certificate and then choose **All Tasks > Export**.



Console Root
- Certificates - Current User
  - Personal
    - Certificates
  - Trusted Root Certification A
  - Enterprise Trust
  - Intermediate Certification Au
  - Active Directory User Objec
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certificatio
  - Trusted People
  - Other People
  - ipcu
  - LyncCertStore
  - McAfee Trust
  - Certificate Enrollment Reque
  - Smart Card Trusted Roots

Issued To	Issued By	Expiration D...	Intended Purpo...	Friendly Name	Stat...	Certificate T...
XMS.example.com	XMS.example.com	5/21/2026	<All>	<None>		

7. When the certificate export wizard appears, click **Next**.



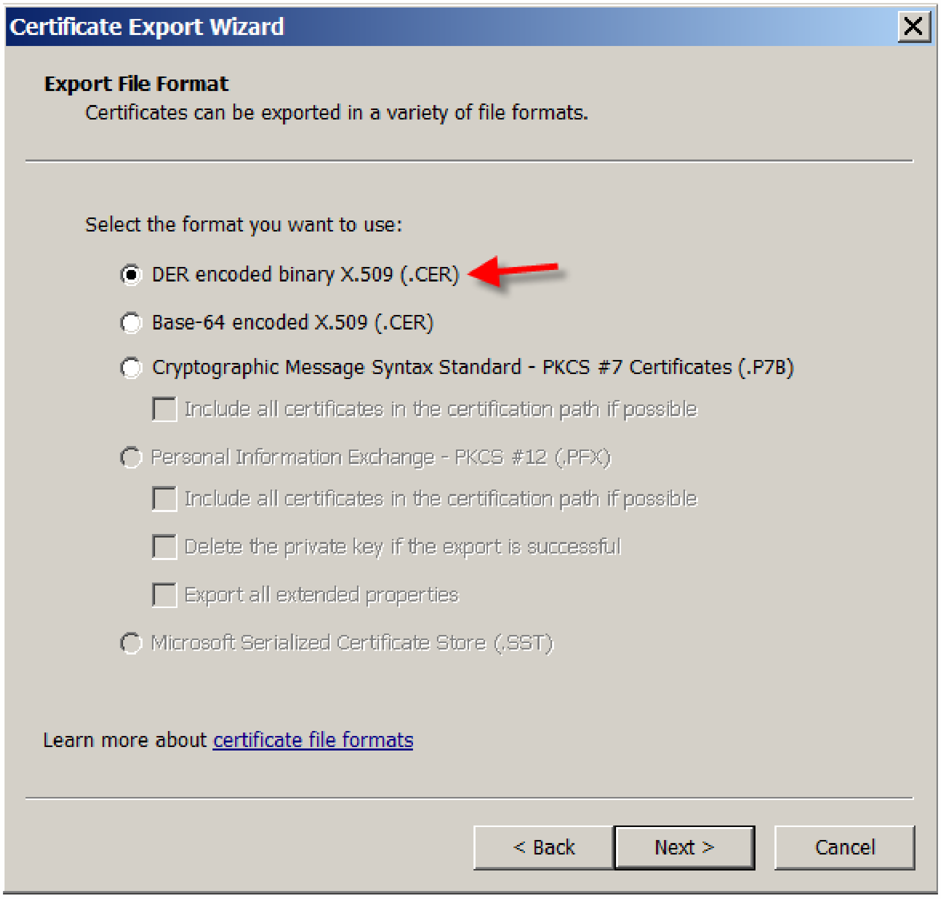
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

8. Choose the format **DER encoded binary X.509 (.CER)**. Click **Next**.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

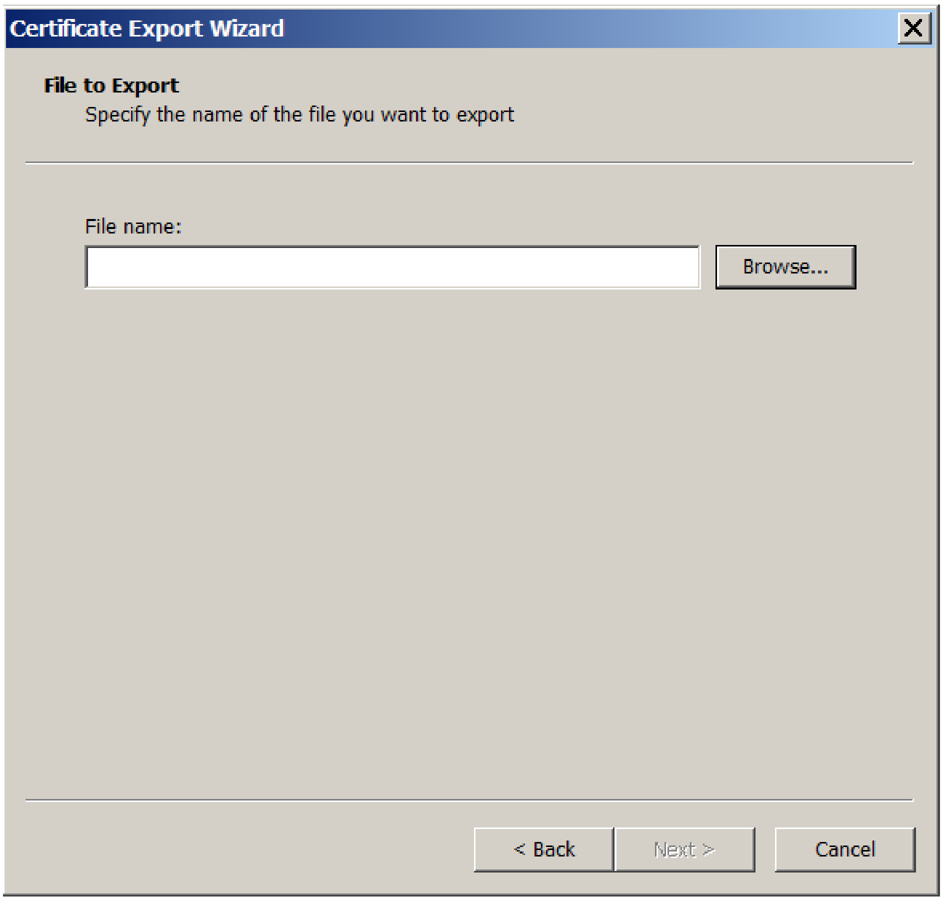
□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

9. Browse to the certificate. Type a name for the certificate and then click **Next**.



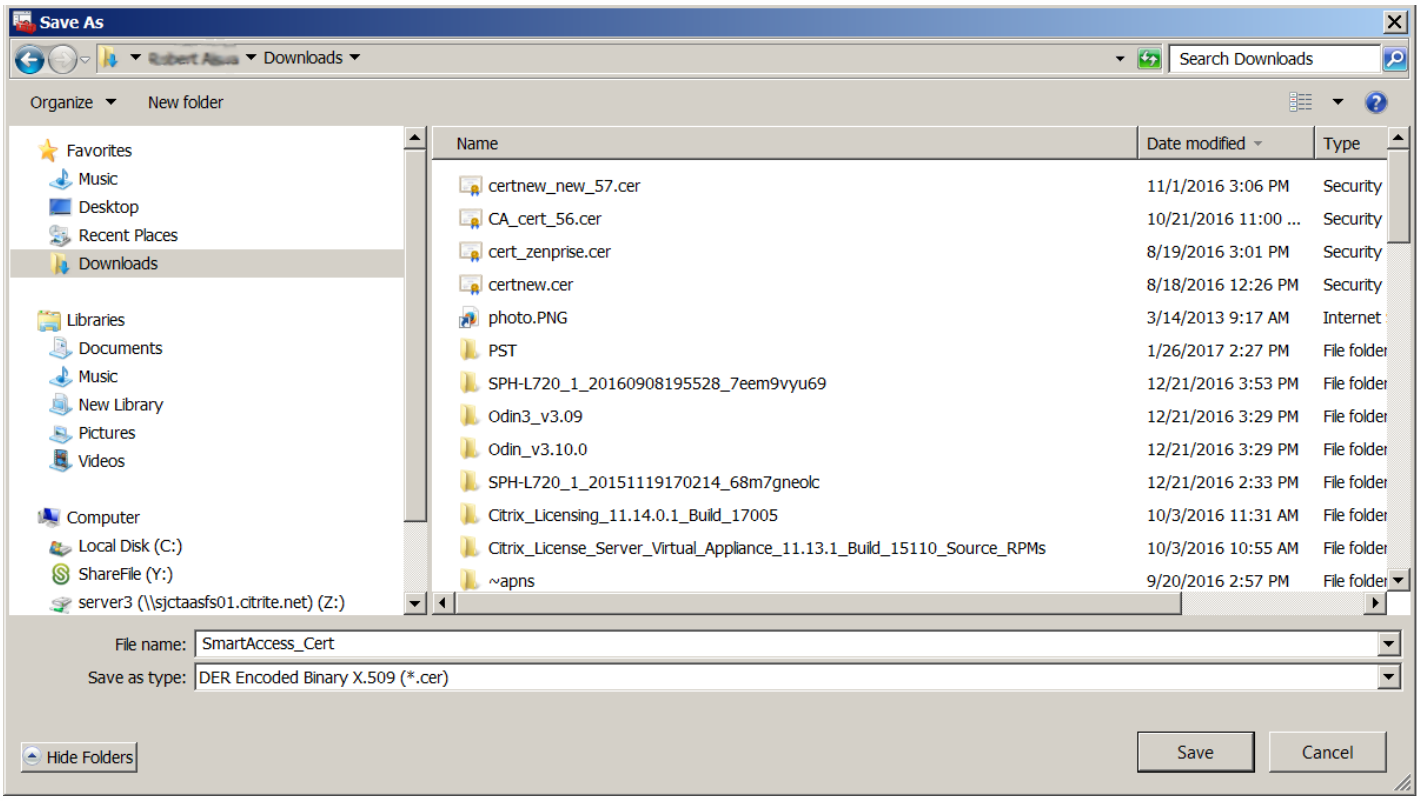
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

10. Save the certificate.



Save As

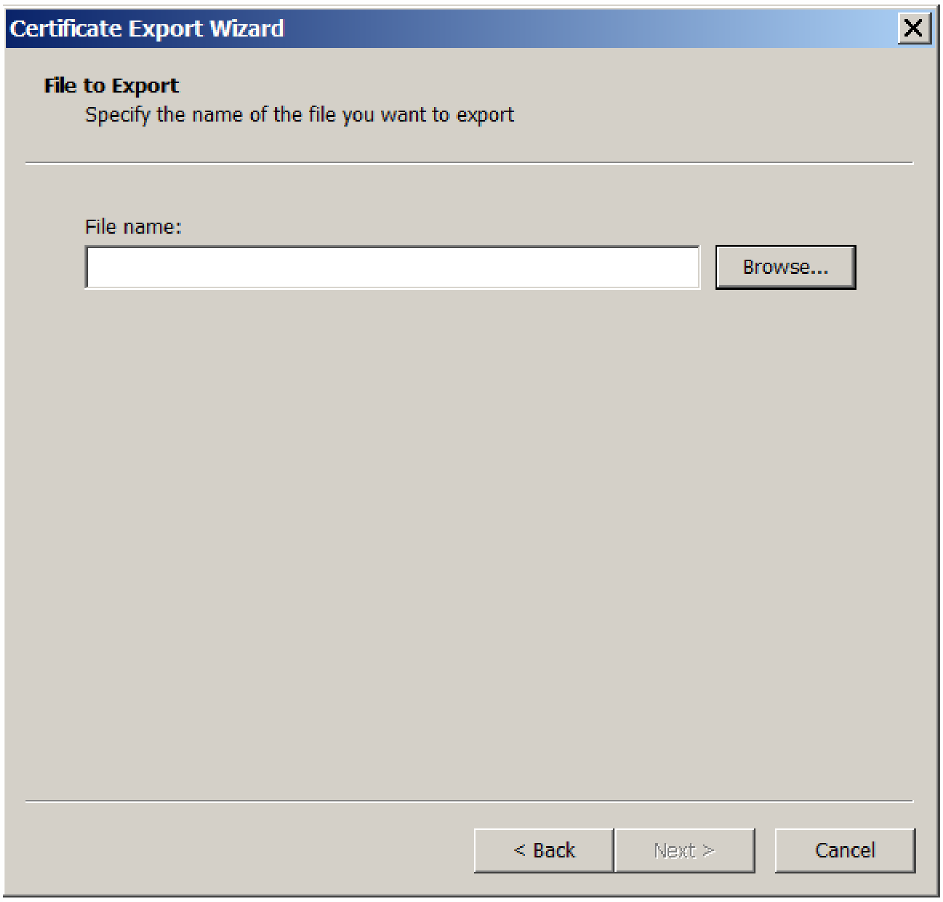
[redacted] ▸ Downloads ▸

Name	Date modified	Type
certnew_new_57.cer	11/1/2016 3:06 PM	Security
CA_cert_56.cer	10/21/2016 11:00 ...	Security
cert_zenprise.cer	8/19/2016 3:01 PM	Security
certnew.cer	8/18/2016 12:26 PM	Security
photo.PNG	3/14/2013 9:17 AM	Internet
PST	1/26/2017 2:27 PM	File folder
SPH-L720_1_20160908195528_7eem9vyu69	12/21/2016 3:53 PM	File folder
Odin3_v3.09	12/21/2016 3:29 PM	File folder
Odin_v3.10.0	12/21/2016 3:29 PM	File folder
SPH-L720_1_20151119170214_68m7gneolc	12/21/2016 2:33 PM	File folder
Citrix_Licensing_11.14.0.1_Build_17005	10/3/2016 11:31 AM	File folder
Citrix_License_Server_Virtual_Appliance_11.13.1_Build_15110_Source_RPMs	10/3/2016 10:55 AM	File folder
~apns	9/20/2016 2:57 PM	File folder

File name: SmartAccess_Cert

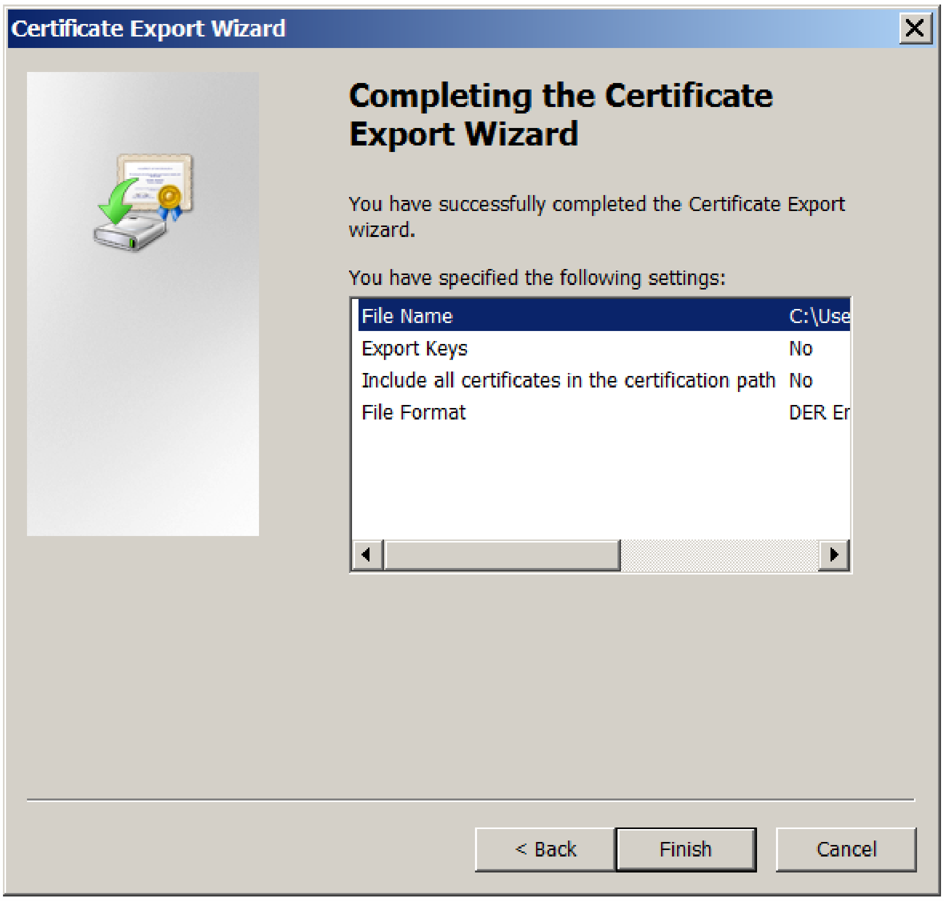
Save as type: DER Encoded Binary X.509 (*.cer)

11. Browse to the certificate and click **Next**.



Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
Browse...
< Back
Next >
Cancel

12. Review your selections and click **Finish**. Click **OK** to dismiss the confirmation window.



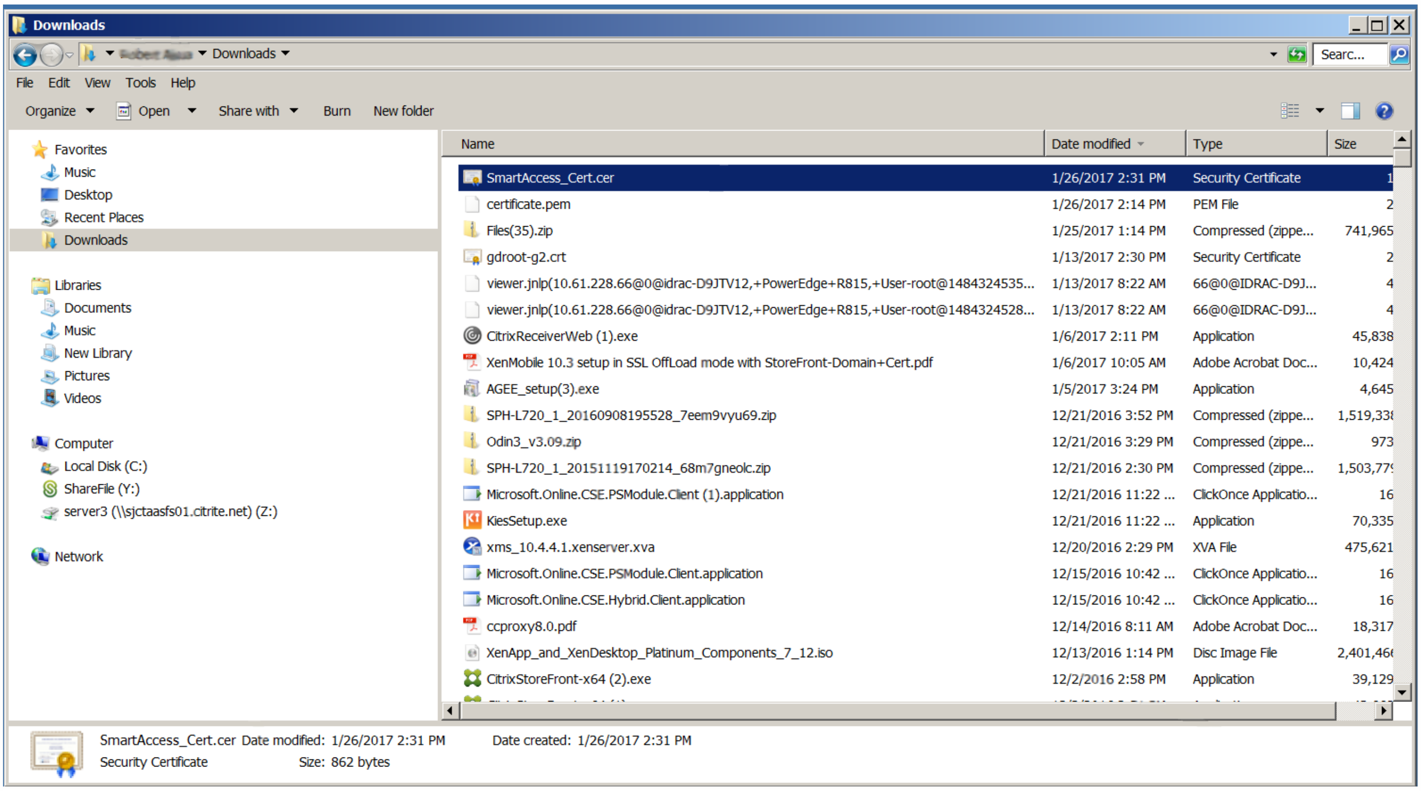
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Use
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Er

13. Locate the certificate in your download directory. Note that the certificate is in CER format.

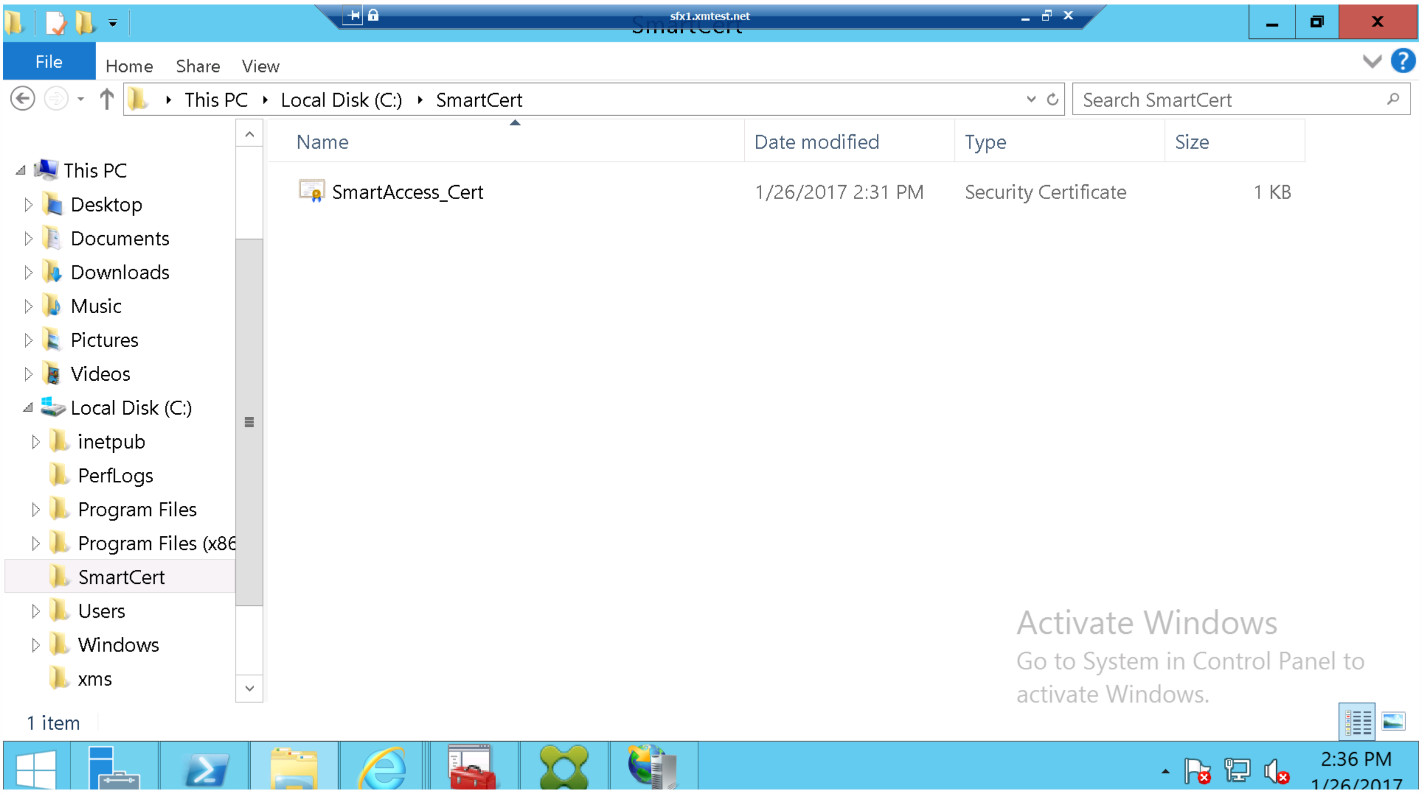


Name	Date modified	Type	Size
SmartAccess_Cert.cer	1/26/2017 2:31 PM	Security Certificate	1
certificate.pem	1/26/2017 2:14 PM	PEM File	2
Files(35).zip	1/25/2017 1:14 PM	Compressed (zippe...	741,965
gdroot-g2.crt	1/13/2017 2:30 PM	Security Certificate	2
viewer.jnlp(10.61.228.66@0@idrac-D9JTV12,+PowerEdge+R815,+User-root@1484324535...	1/13/2017 8:22 AM	66@0@IDRAC-D9J...	4
viewer.jnlp(10.61.228.66@0@idrac-D9JTV12,+PowerEdge+R815,+User-root@1484324528...	1/13/2017 8:22 AM	66@0@IDRAC-D9J...	4
CitrixReceiverWeb (1).exe	1/6/2017 2:11 PM	Application	45,838
XenMobile 10.3 setup in SSL OffLoad mode with StoreFront-Domain+Cert.pdf	1/6/2017 10:05 AM	Adobe Acrobat Doc...	10,424
AGEE_setup(3).exe	1/5/2017 3:24 PM	Application	4,645
SPH-L720_1_20160908195528_7eem9vyu69.zip	12/21/2016 3:52 PM	Compressed (zippe...	1,519,33
Odin3_v3.09.zip	12/21/2016 3:29 PM	Compressed (zippe...	973
SPH-L720_1_20151119170214_68m7gneolc.zip	12/21/2016 2:30 PM	Compressed (zippe...	1,503,77
Microsoft.Online.CSE.PSModule.Client (1).application	12/21/2016 11:22 ...	ClickOnce Applicatio...	16
KiesSetup.exe	12/21/2016 11:22 ...	Application	70,335
xms_10.4.4.1.xenserver.xva	12/20/2016 2:29 PM	XVA File	475,621
Microsoft.Online.CSE.PSModule.Client.application	12/15/2016 10:42 ...	ClickOnce Applicatio...	16
Microsoft.Online.CSE.Hybrid.Client.application	12/15/2016 10:42 ...	ClickOnce Applicatio...	16
ccproxy8.0.pdf	12/14/2016 8:11 AM	Adobe Acrobat Doc...	18,317
XenApp_and_XenDesktop_Platinum_Components_7_12.iso	12/13/2016 1:14 PM	Disc Image File	2,401,46
CitrixStoreFront-x64 (2).exe	12/2/2016 2:58 PM	Application	39,129

SmartAccess_Cert.cer Date modified: 1/26/2017 2:31 PM Date created: 1/26/2017 2:31 PM
Security Certificate Size: 862 bytes

1. On the StoreFront server, create a folder called **SmartCert**.

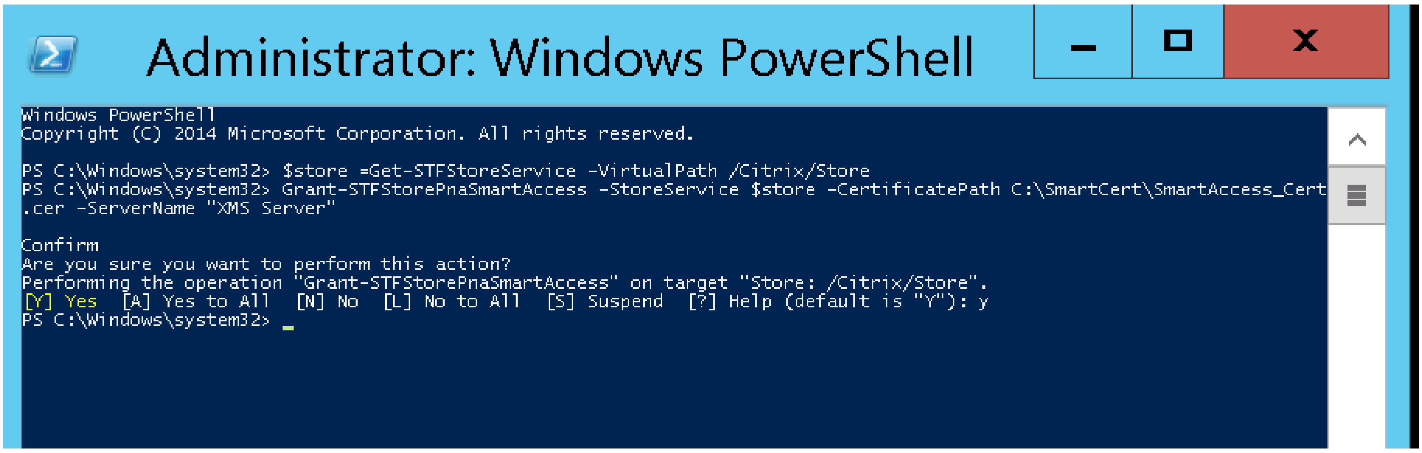
2. Copy the certificate to the **SmartCert** folder.



Name	Date modified	Type	Size
SmartAccess_Cert	1/26/2017 2:31 PM	Security Certificate	1 KB

On the StoreFront server, run this PowerShell command to configure the converted XenMobile Server certificate on the store:

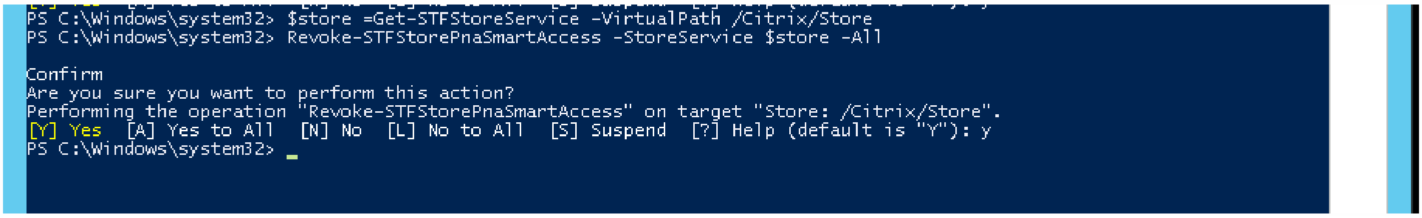
```
Grant-STFStorePnaSmartAccess –StoreService $store –CertificatePath “C:\xms\xms.cer” –ServerName “XMS server”
```



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> $store =Get-STFStoreService -VirtualPath /Citrix/Store
PS C:\Windows\system32> Grant-STFStorePnaSmartAccess -StoreService $store -CertificatePath C:\SmartCert\SmartAccess_Cert
.cer -ServerName "XMS Server"

Confirm
Are you sure you want to perform this action?
Performing the operation "Grant-STFStorePnaSmartAccess" on target "Store: /Citrix/Store".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y
PS C:\Windows\system32> _
```

If there are any existing certificates on the StoreFront store, run this PowerShell command to revoke them:

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```



```
PS C:\Windows\system32> $store =Get-STFStoreService -VirtualPath /Citrix/Store
PS C:\Windows\system32> Revoke-STFStorePnaSmartAccess -StoreService $store -All

Confirm
Are you sure you want to perform this action?
Performing the operation "Revoke-STFStorePnaSmartAccess" on target "Store: /Citrix/Store".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y
PS C:\Windows\system32> _
```

Alternatively, you can run any of these PowerShell commands on the StoreFront server to revoke existing certificates on the StoreFront store:

- Revoke by name:

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

 Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM Server”
```

- Revoke by thumbprint:

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

 Revoke-STFStorePnaSmartAccess –StoreService $store –CertificateThumbprint “1094821dec7834d5d42 bb456329efe4fca86c60b”
```

- Revoke by server object:

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

 $access = Get-STFStorePnaSmartAccess –StoreService $store

 Revoke-STFStorePnaSmartAccess –StoreService $store –SmartAccess $access.AccessConditionsTrusts[0]
```

Configure the SmartAccess policy for XenApp and XenDesktop

To add the required SmartAccess policy to the delivery group delivering the HDX app:

1. On the XenApp and XenDesktop server, open Citrix Studio.

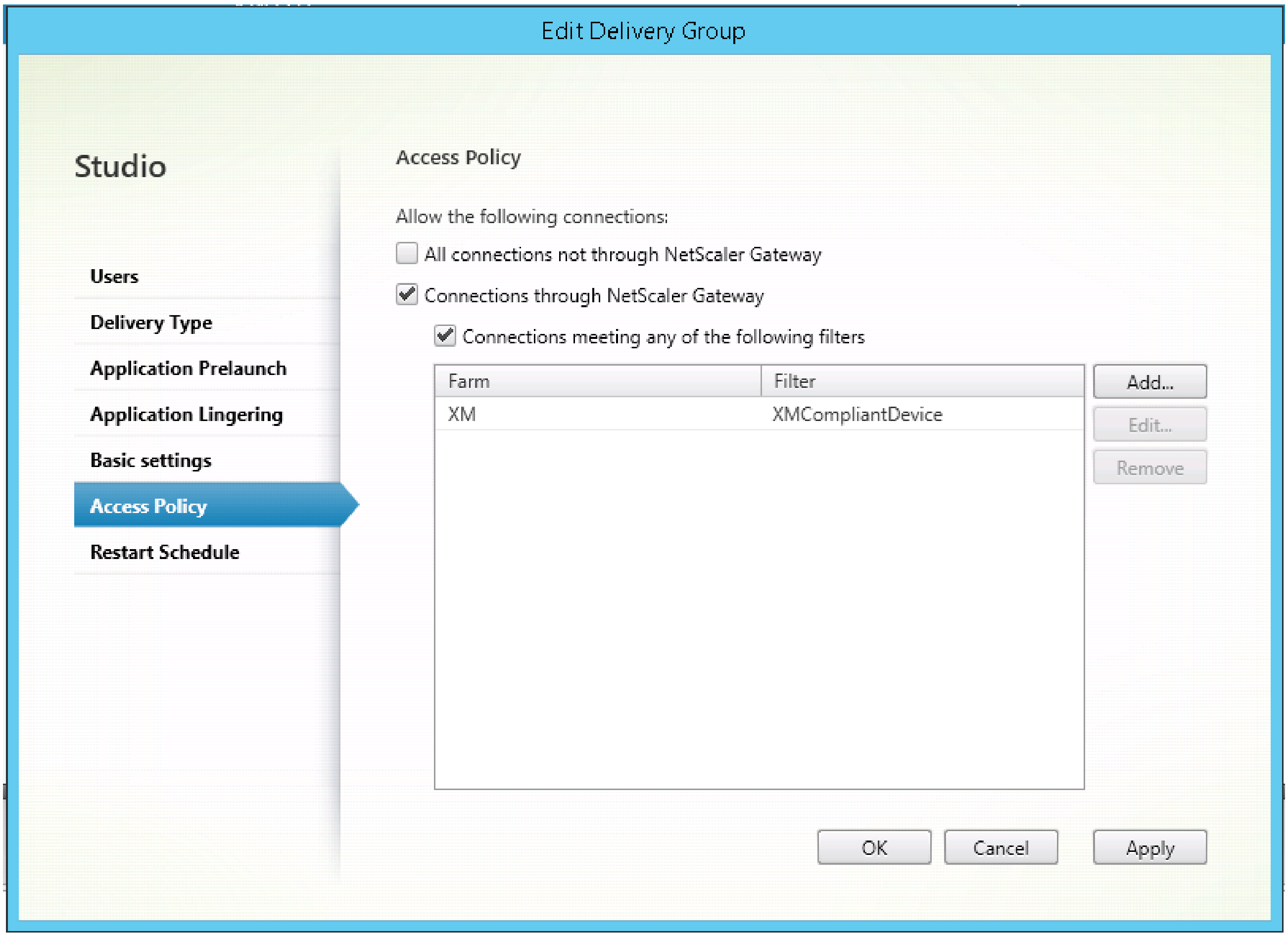
2. Select **Delivery Groups** in the Studio navigation pane.

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 NetScaler Gateway** and **Connection meeting any of the following**.

5. Click **Add**.

6. Add an access policy where **Farm** is **XM** and **Filter** is **XMCompliantDevice**.



Edit Delivery Group

Access Policy

Allow the following connections:

☐ All connections not through NetScaler Gateway

☑ Connections through NetScaler Gateway

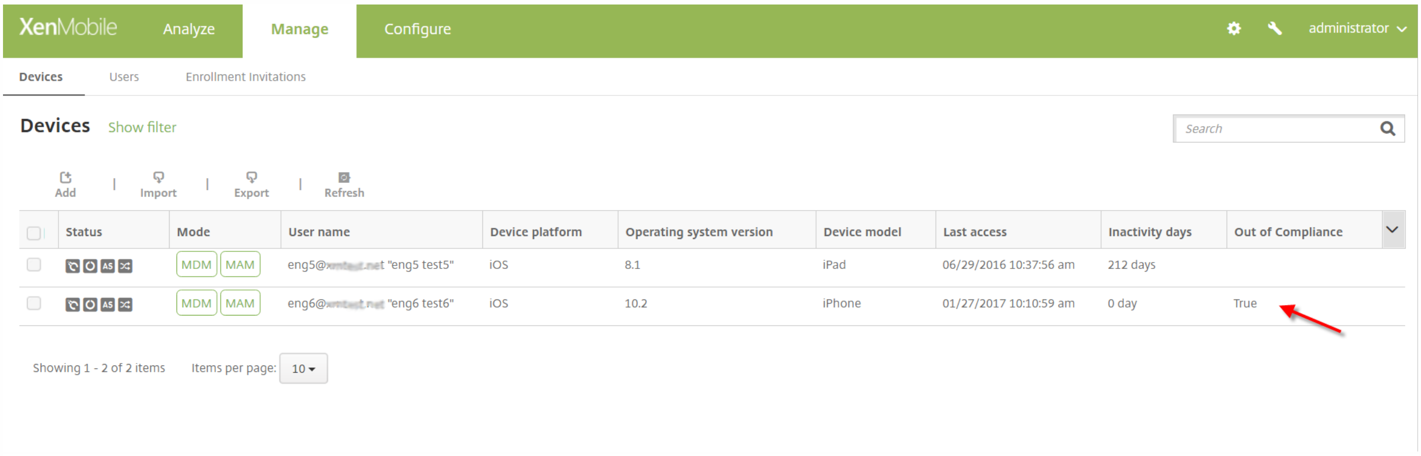
☑ Connections meeting any of the following filters

Farm	Filter
XM	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 XenMobile

The SmartAccess policy that you set in the delivery group for an HDX app denies access to a device when the device in out of compliance. Use automated actions to mark the device as out of compliance.



☐	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	Out of Compliance
☐		MDM MAM	eng5@[redacted] "eng5 test5"	iOS	8.1	iPad	06/29/2016 10:37:56 am	212 days	
☐		MDM MAM	eng6@[redacted] "eng6 test6"	iOS	10.2	iPhone	01/27/2017 10:10:59 am	0 day	True

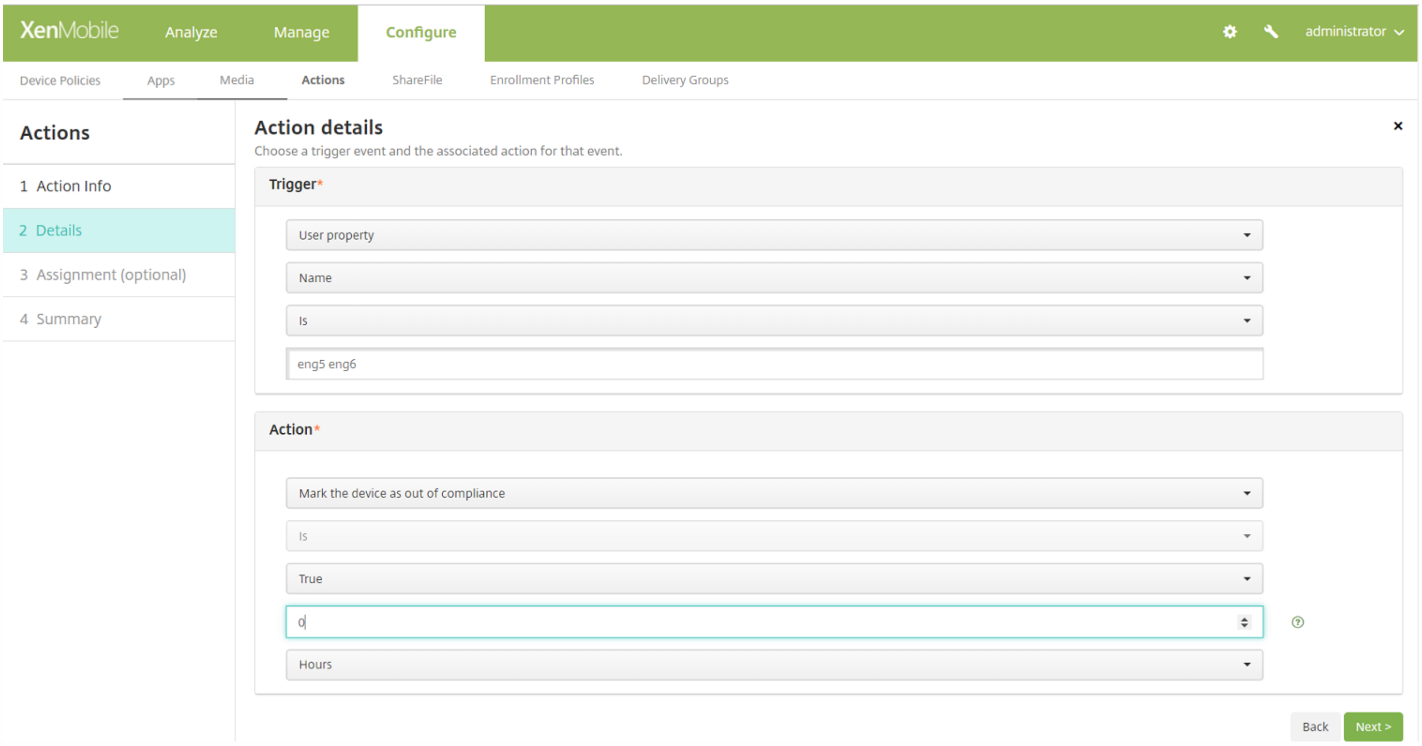
Showing 1 - 2 of 2 items Items per page: 10

1. From the XenMobile 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**.



Action details

Choose a trigger event and the associated action for that event.

Trigger*

User property

Name

Is

eng5 eng6

Action*

Mark the device as out of compliance

Is

True

0

Hours

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 XenMobile delivery group or groups to apply this action to.

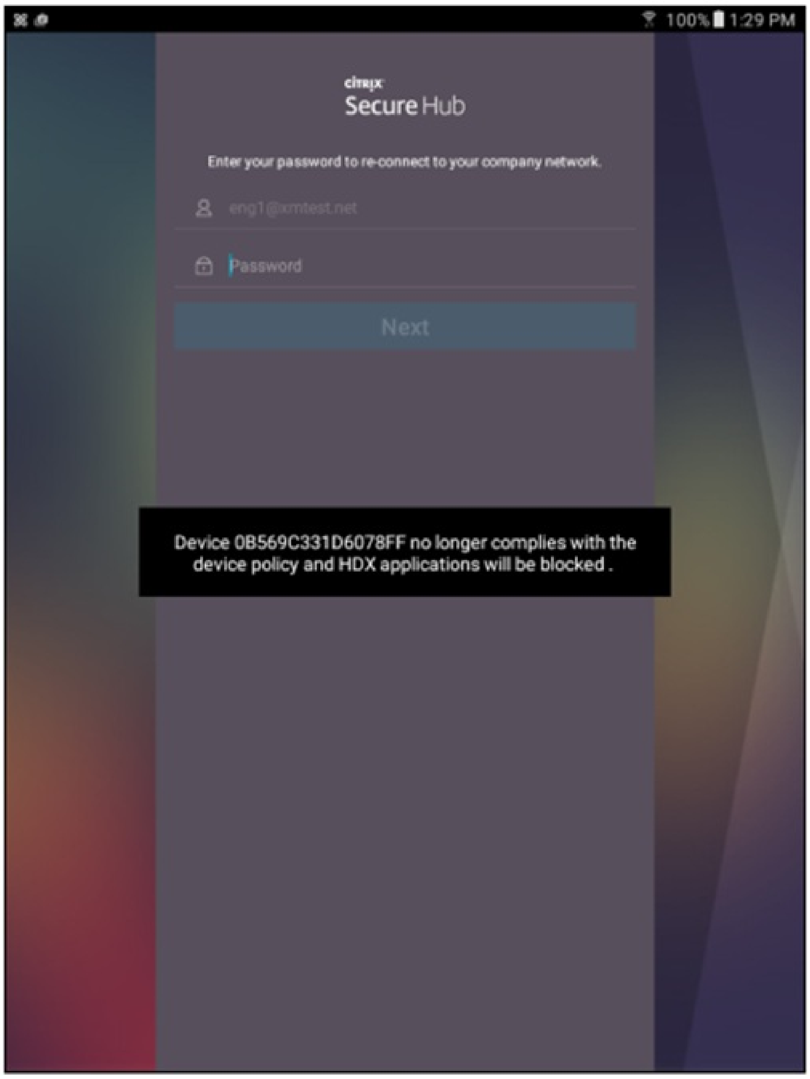
8. Review the summary of the action.

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."



Enter your password to re-connect to your company network.

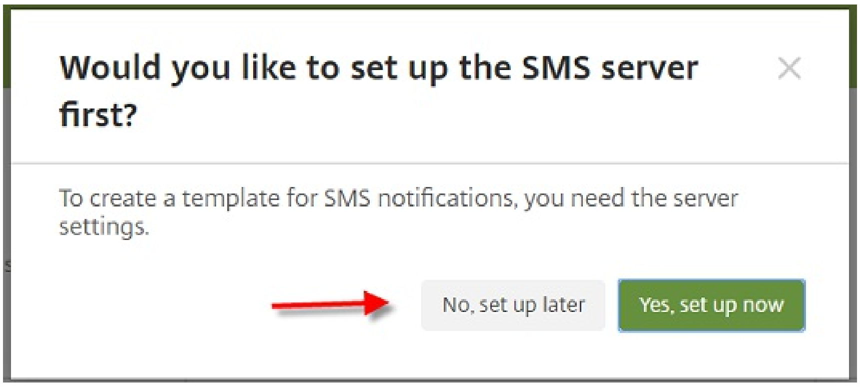
Device 0B569C331D6078FF no longer complies with the device policy and HDX applications will be blocked .

1. In the XenMobile 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**.

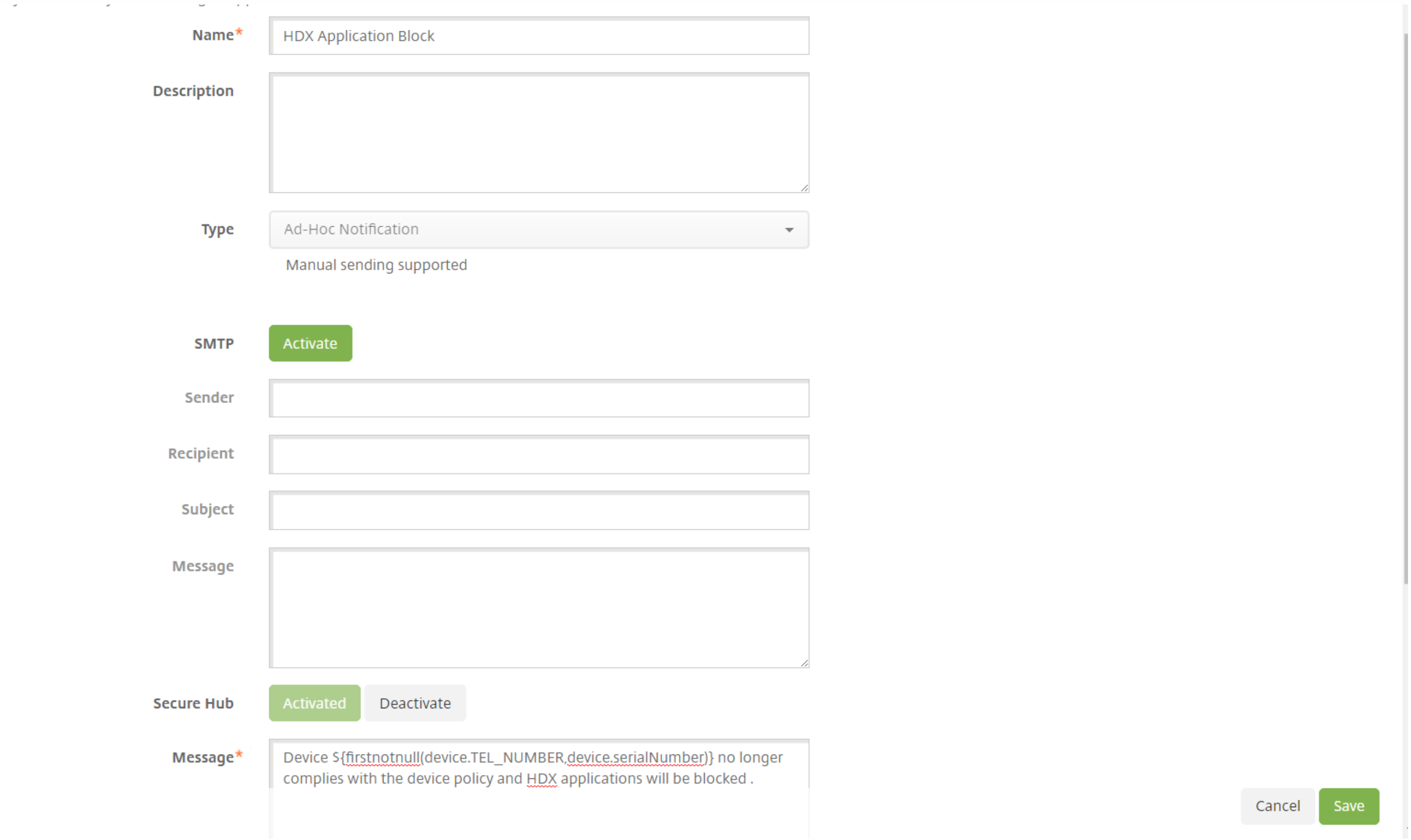


Would you like to set up the SMS server first?

To create a template for SMS notifications, you need the server settings.

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 ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.



Name*: HDX Application Block

Description:

Type: Ad-Hoc Notification

Manual sending supported

SMTP: Activate

Sender:

Recipient:

Subject:

Message:

Secure Hub: Activated | Deactivate

Message*: Device ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked .

6. Click **Save**.

1. From the XenMobile console, click **Configure > Actions**. The **Actions** page appears.

2. Click **Add** to add an action. The **Action Information** page appears.

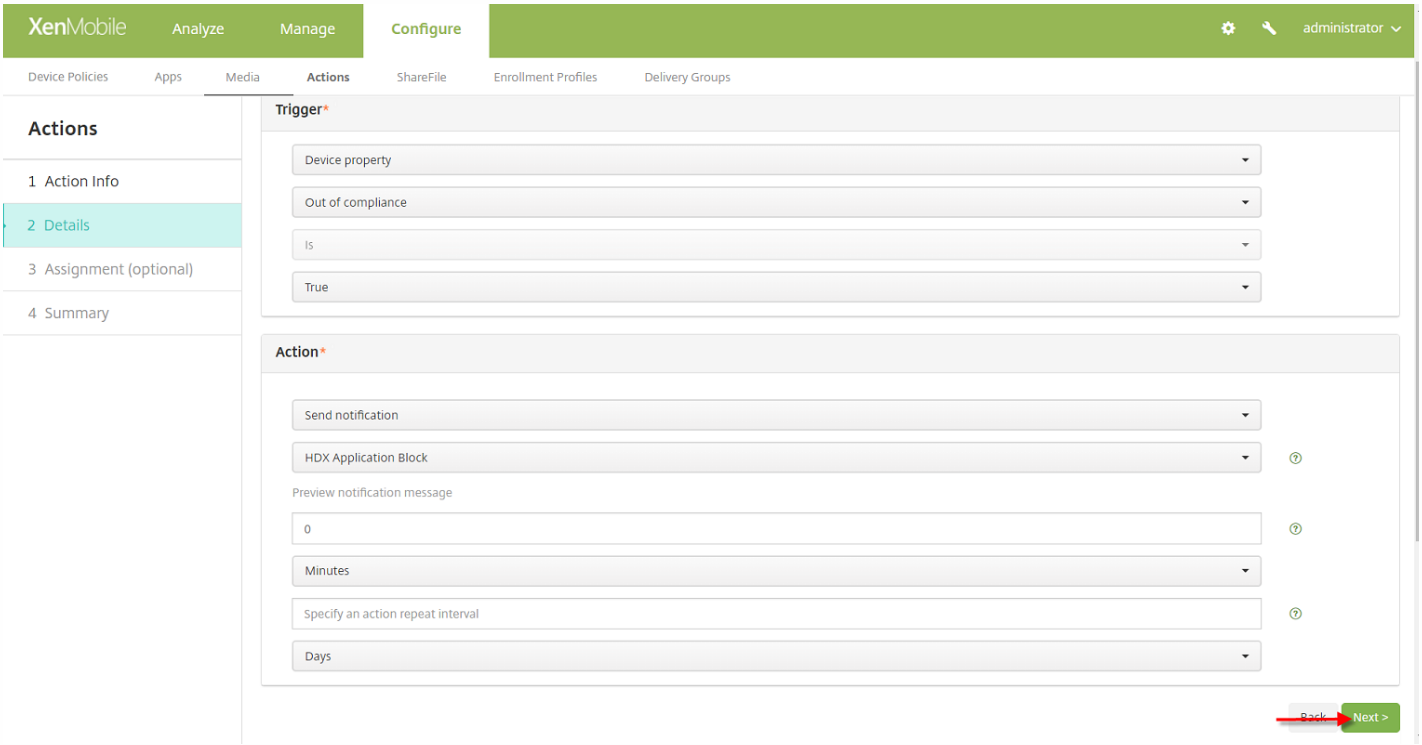
3. On the **Action Information** page, enter a name and description for the action:

- 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**.



Trigger*

Device property

Out of compliance

Is

True

Action*

Send notification

HDX Application Block

Preview notification message

0

Minutes

Specify an action repeat interval

Days

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 XenMobile 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**.

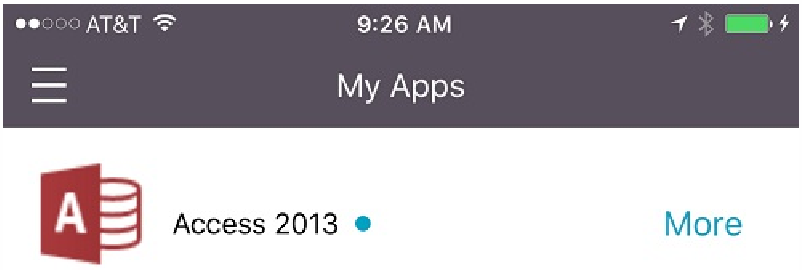
For more information on setting automated actions, see Automated actions.

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.



Add media

Sep 06, 2017

You add media to XenMobile so you can deploy the media to user devices. You can use XenMobile to deploy iBooks that you obtain through the Apple Volume Purchase Program (VPP).

After you configure a VPP account in XenMobile, 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.

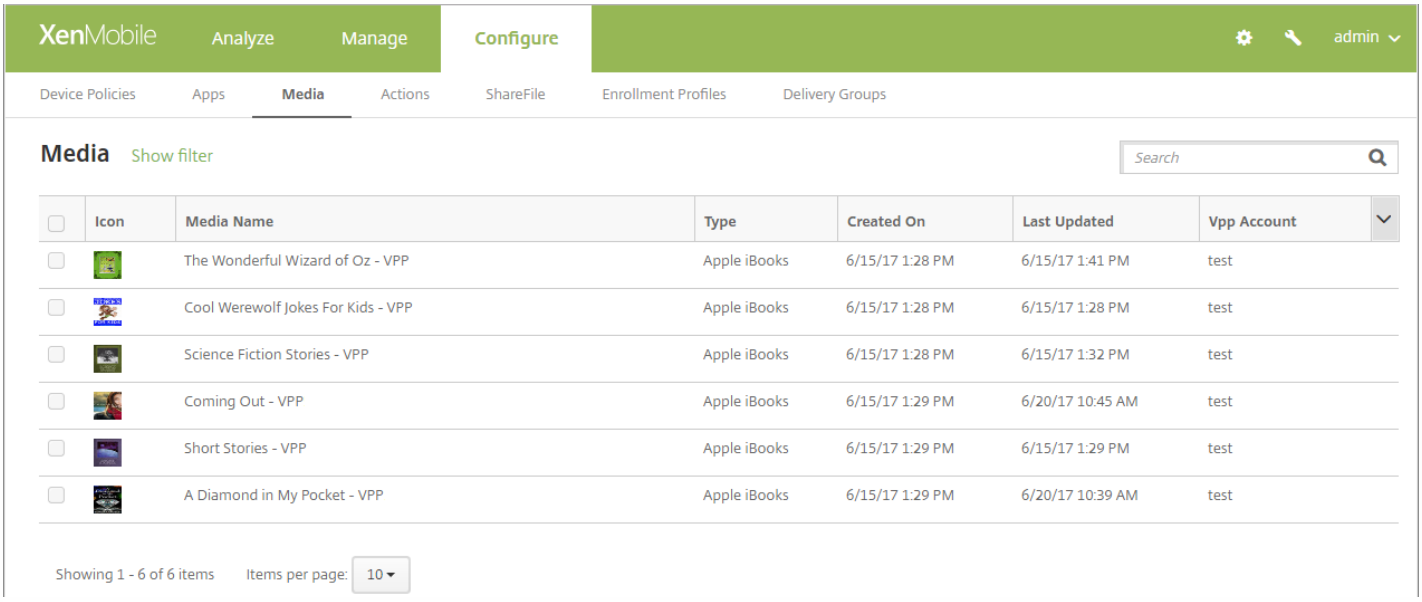
The first time that a user receives an iBook and accepts the VPP license, deployed books install on the device. The books appear in the Apple iBook app. You can't disassociate the book license from the user or remove the book from the device. XenMobile installs iBooks as required media. If a user deletes an installed book from their device, the book remains in the iBook app, ready for download.

Prerequisites

- iOS devices (minimum version iOS 8)
- Configure iOS VPP in XenMobile, as described in iOS Volume Purchase Plan.

Configure iBooks

iBooks obtained through VPP appear on the **Configure > Media** page.

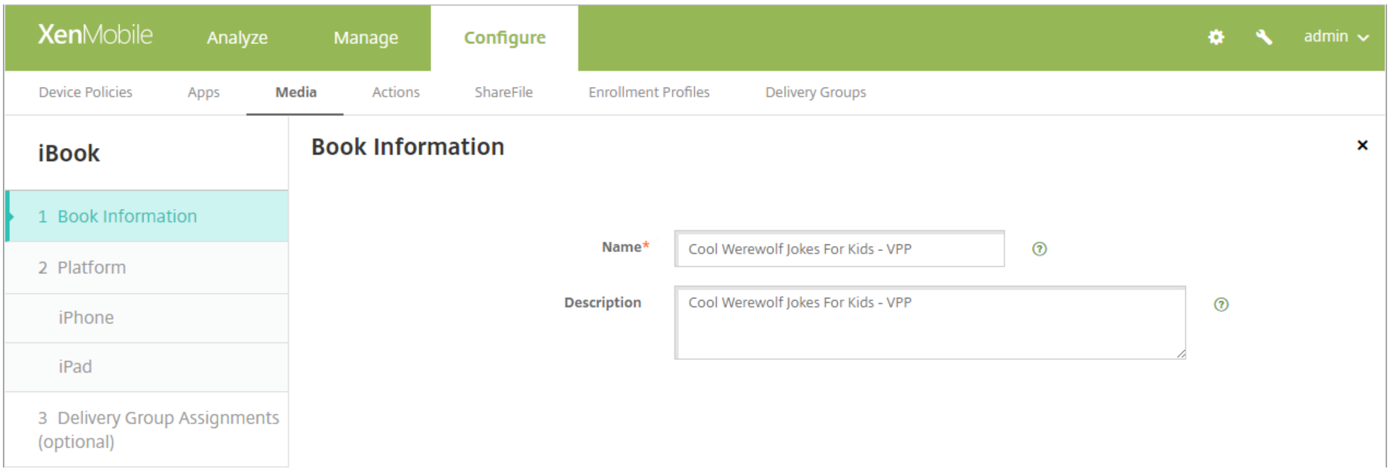


□	Icon	Media Name	Type	Created On	Last Updated	Vpp Account
□		The Wonderful Wizard of Oz - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:41 PM	test
□		Cool Werewolf Jokes For Kids - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:28 PM	test
□		Science Fiction Stories - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:32 PM	test
□		Coming Out - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:45 AM	test
□		Short Stories - VPP	Apple iBooks	6/15/17 1:29 PM	6/15/17 1:29 PM	test
□		A Diamond in My Pocket - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:39 AM	test

Showing 1 - 6 of 6 items Items per page: 10

To configure an iBook for deployment:

1. In **Configure > Media**, select an iBook and click **Edit**. The **Book Information** page appears.



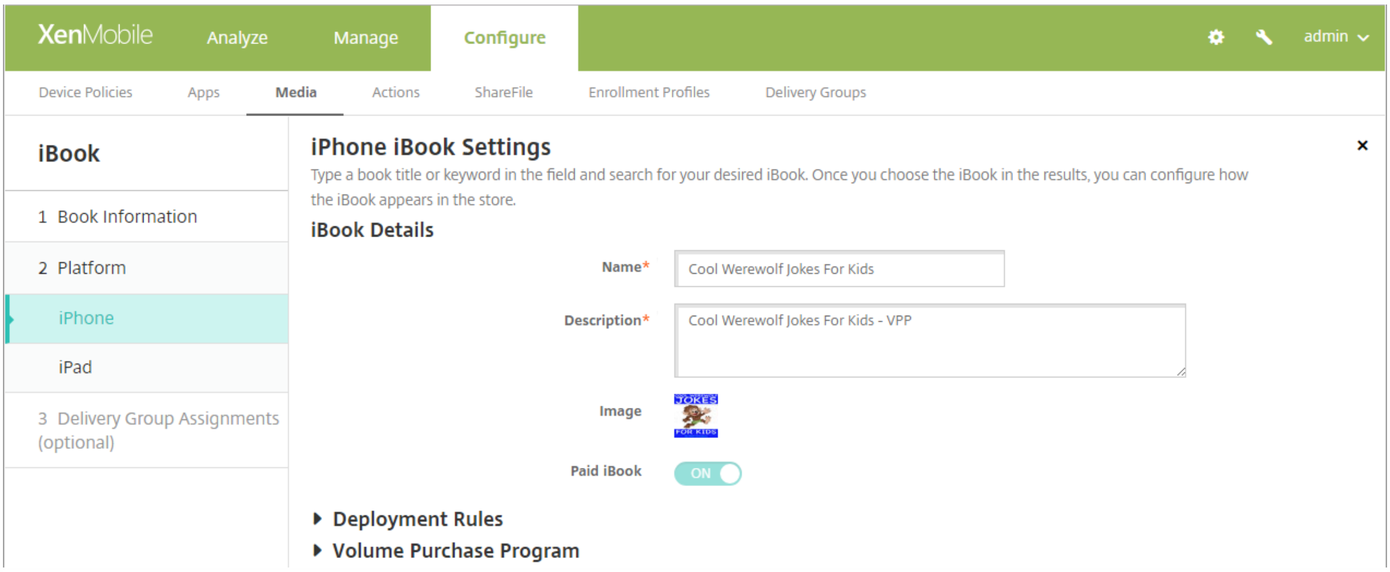
Book Information

Name*: Cool Werewolf Jokes For Kids - VPP

Description: Cool Werewolf Jokes For Kids - VPP

The **Name** and **Description** appear only in the XenMobile 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 VPP.



iPhone iBook Settings

Type a book title or keyword in the field and search for your desired iBook. Once you choose the iBook in the results, you can configure how the iBook appears in the store.

iBook Details

Name*: Cool Werewolf Jokes For Kids

Description*: Cool Werewolf Jokes For Kids - VPP

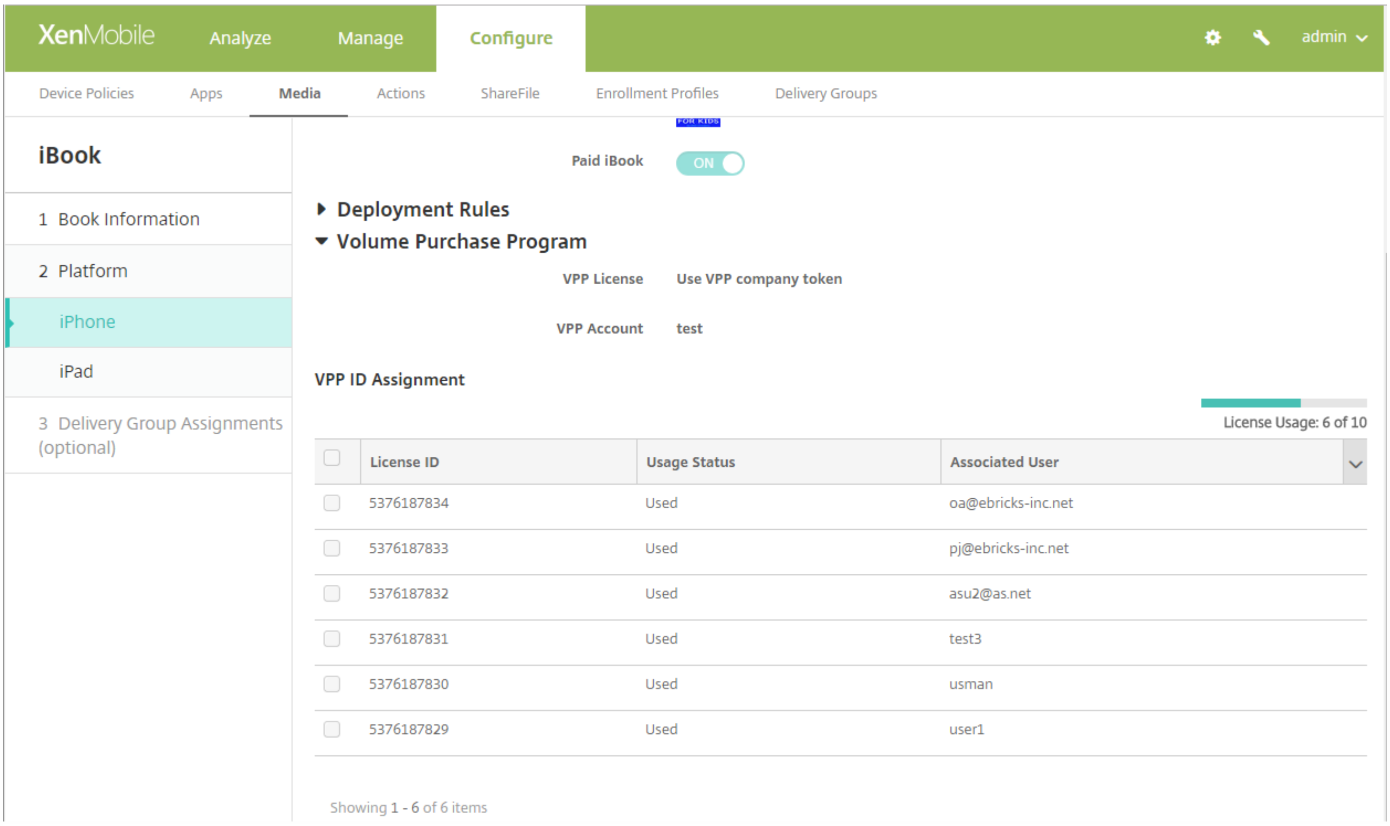
Image

Paid iBook: ON

▸ Deployment Rules

▸ Volume Purchase Program

You can also specify deployment rules or view VPP information.



Paid iBook: ON

VPP License: Use VPP company token

VPP Account: test

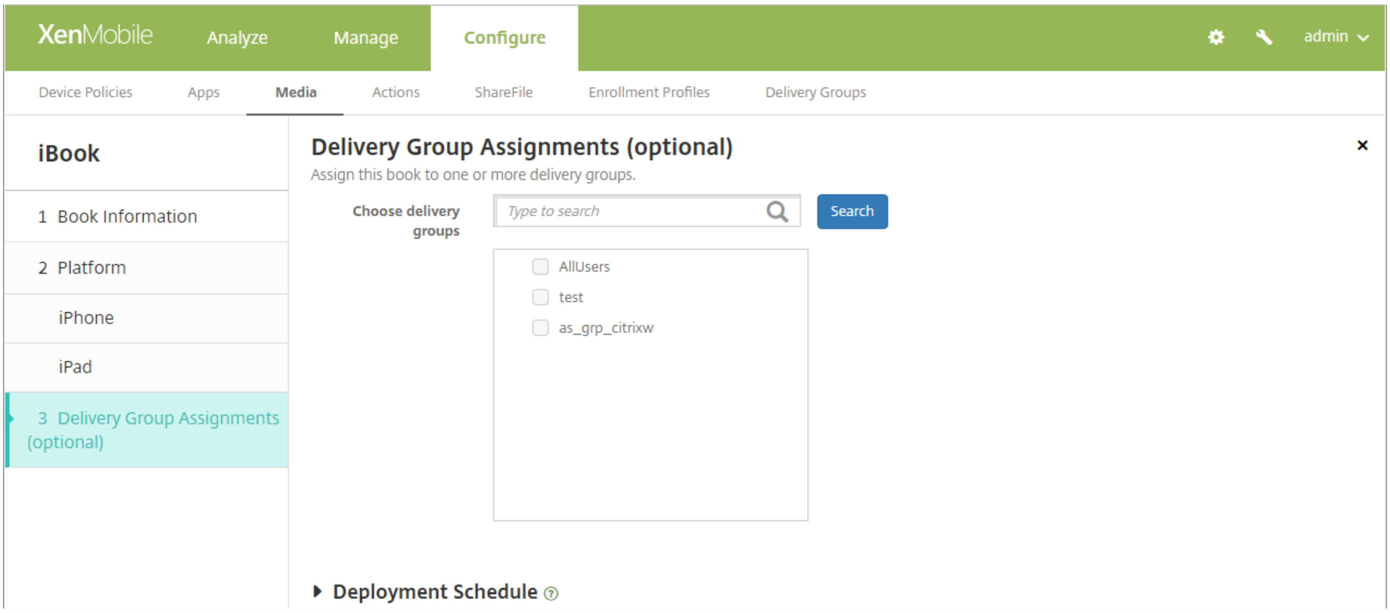
VPP ID Assignment

License Usage: 6 of 10

□	License ID	Usage Status	Associated User
□	5376187834	Used	oa@ebricks-inc.net
□	5376187833	Used	pj@ebricks-inc.net
□	5376187832	Used	asu2@as.net
□	5376187831	Used	test3
□	5376187830	Used	usman
□	5376187829	Used	user1

Showing 1 - 6 of 6 items

3. Optionally, assign the iBook to delivery groups and set a deployment schedule.



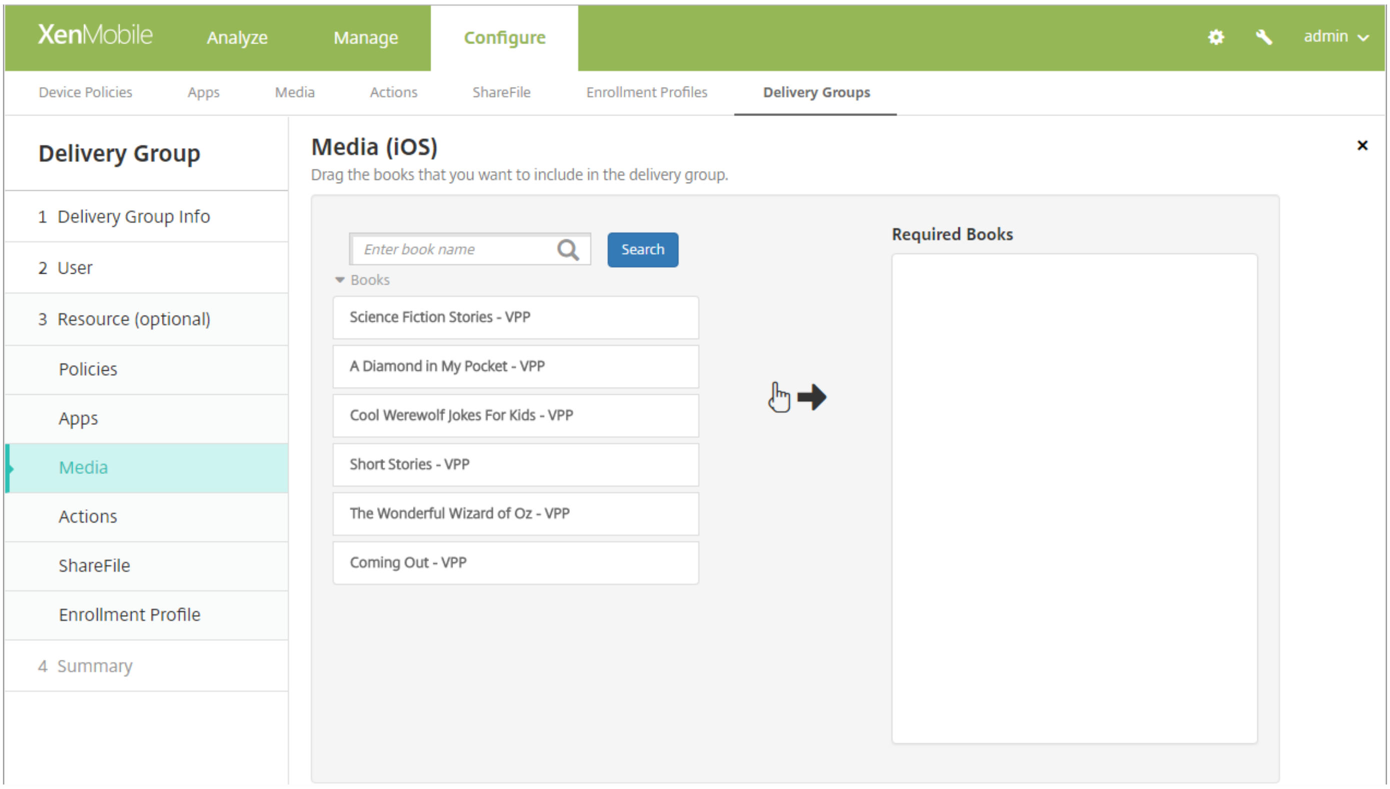
Delivery Group Assignments (optional)

Assign this book to one or more delivery groups.

Choose delivery groups: Type to search

□ AllUsers
□ test
□ as_grp_citrixw

You can also assign iBooks to delivery groups from the **Media** tab for **Configure > Delivery Groups**. XenMobile currently supports required book deployment only.


XenMobile | Analyze | Manage | Configure | admin

Device Policies | Apps | Media | Actions | ShareFile | Enrollment Profiles | Delivery Groups

Delivery Group

1 Delivery Group Info
2 User
3 Resource (optional)
Policies
Apps
Media
Actions
ShareFile
Enrollment Profile
4 Summary

Media (iOS)

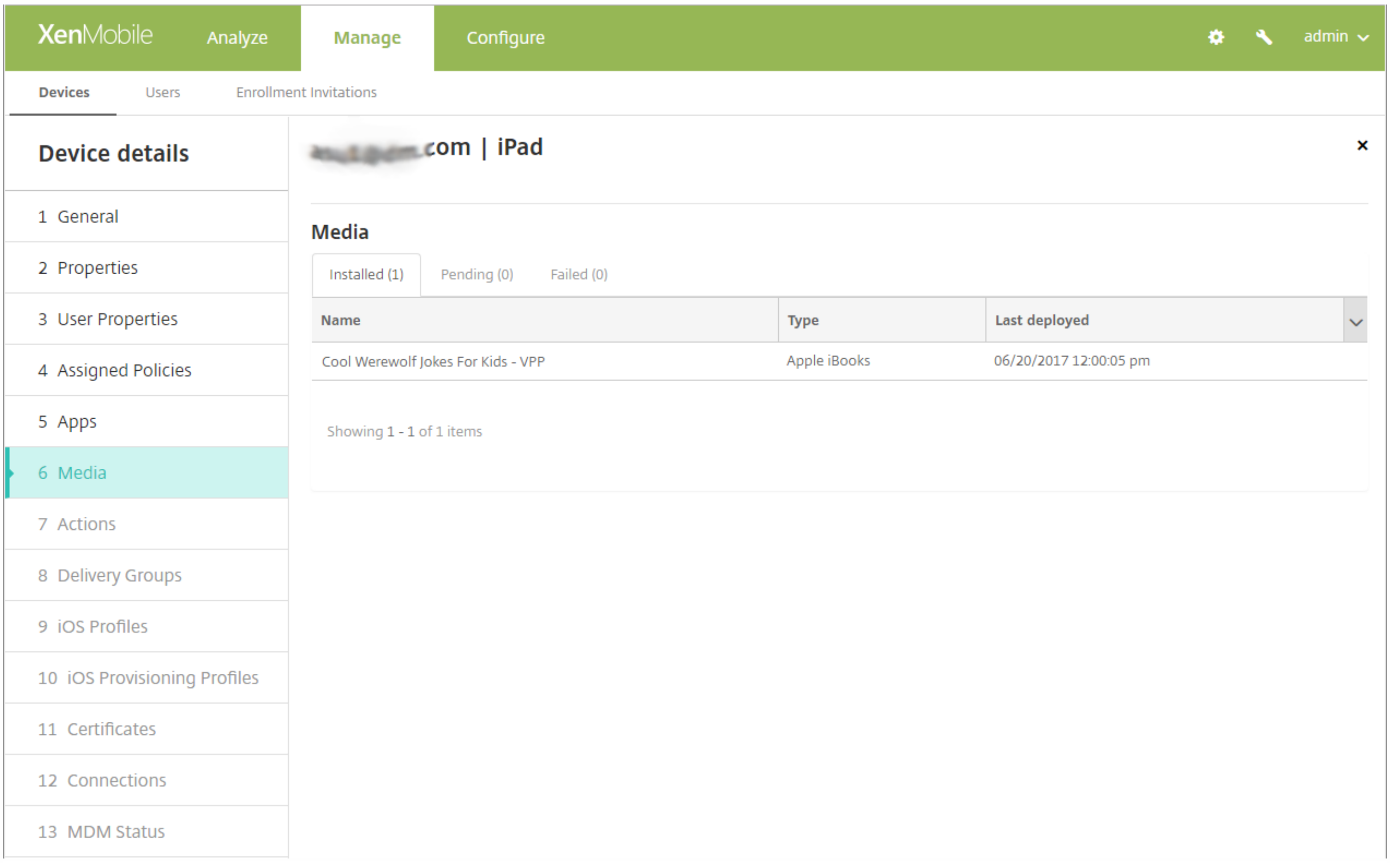
Drag the books that you want to include in the delivery group.

Enter book name | Search

Books
- Science Fiction Stories - VPP
- A Diamond in My Pocket - VPP
- Cool Werewolf Jokes For Kids - VPP
- Short Stories - VPP
- The Wonderful Wizard of Oz - VPP
- Coming Out - VPP

Required Books

4. Use the **Media** tab for **Manage** > **Devices** to view deployment status.


XenMobile | Analyze | Manage | Configure | admin

Devices | Users | Enrollment Invitations

Device details

1 General
2 Properties
3 User Properties
4 Assigned Policies
5 Apps
6 Media
7 Actions
8 Delivery Groups
9 iOS Profiles
10 iOS Provisioning Profiles
11 Certificates
12 Connections
13 MDM Status

[redacted].com | iPad

Media

Installed (1) | Pending (0) | Failed (0)

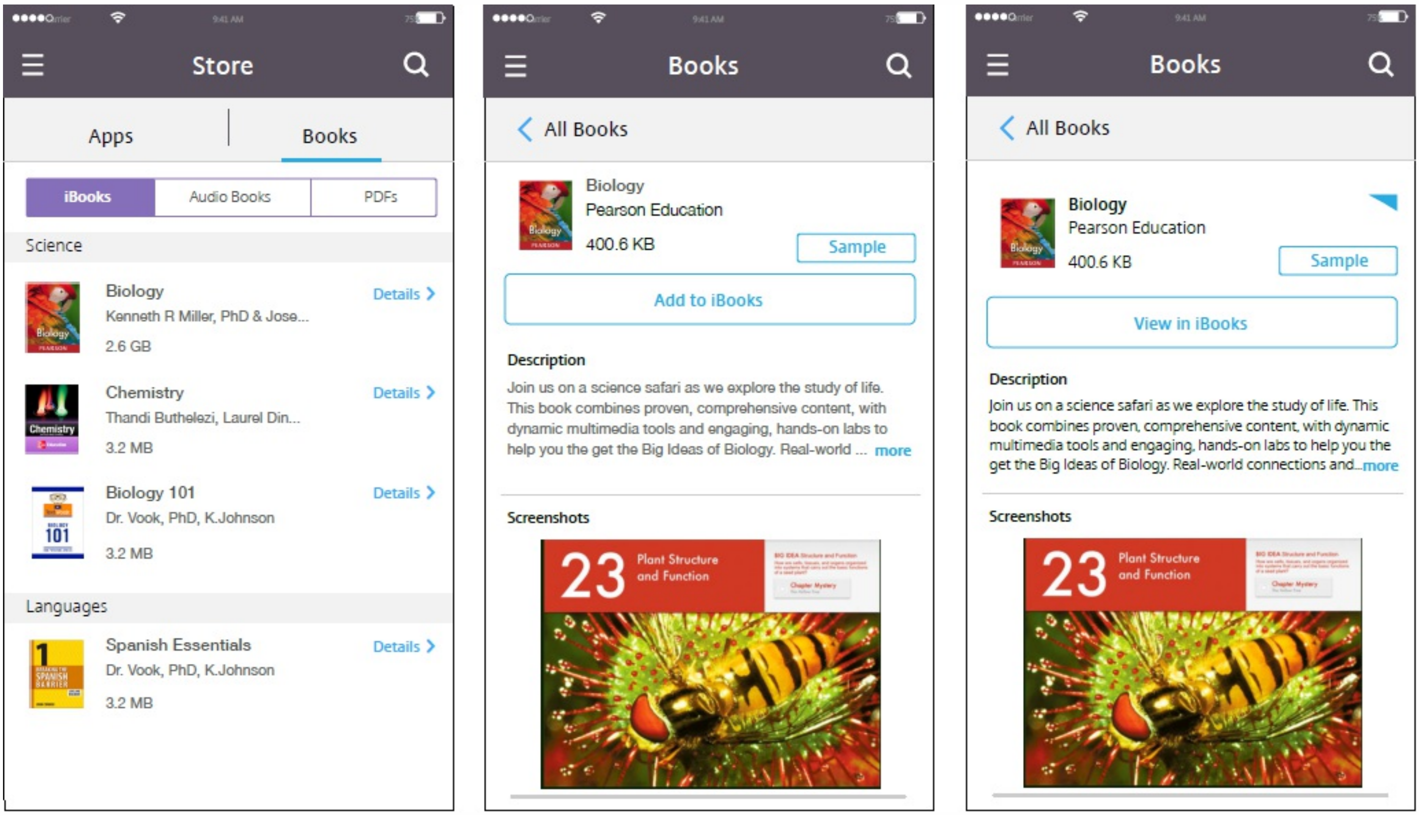
Name	Type	Last deployed
Cool Werewolf Jokes For Kids - VPP	Apple iBooks	06/20/2017 12:00:05 pm

Showing 1 - 1 of 1 items

Note

On the **Configure** > **Media** page, if you select a book and click **Delete**, XenMobile removes the book from the list. However, the next time XenMobile syncs with VPP, the book reappears on the list unless it has been removed from VPP. Deleting a book from the list doesn't remove the book from devices.

iBooks appear on user devices as shown in these samples.



Join us on a science safari as we explore the study of life. This book combines proven, comprehensive content, with dynamic multimedia tools and engaging, hands-on labs to help you the get the Big Ideas of Biology. Real-world ... more

Join us on a science safari as we explore the study of life. This book combines proven, comprehensive content, with dynamic multimedia tools and engaging, hands-on labs to help you the get the Big Ideas of Biology. Real-world connections and...more

Deploy resources

Dec 14, 2017

Device configuration and management typically involve creating resources (policies, apps, and media) and actions in the XenMobile console and then packaging them using delivery groups. The order in which XenMobile pushes resources and actions in a delivery group to devices is referred to as 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
- XenMobile 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.

Deploying to a delivery group means sending a push notification to all users with supported iOS and Windows devices. Those users must belong to the delivery group to reconnect to XenMobile. In this way, you can reevaluate the devices and deploy policies, apps, media, and actions. For users with Android devices: If they are already connected, they receive the resources immediately. Otherwise, based on their scheduling policy, they receive resources the next time that they connect.

The default AllUsers delivery group is created when you install and configure XenMobile. 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 XenMobile pushes resources to devices. Deployment order is supported only for MDM mode.

When determining deployment order, XenMobile 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 XenMobile 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 XenMobile deploys the resources.
- **Deployment rules:** XenMobile 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:** XenMobile 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.

Object/Resource	Device platform	Deployment rule	Deployment schedule	User/groups
Device policy	Y	Y	Y	-
App	Y	Y	Y	-
Media	Y	Y	Y	-
Action	-	Y	Y	-
Delivery group	-	Y	-	Y

It is very 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, XenMobile 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.

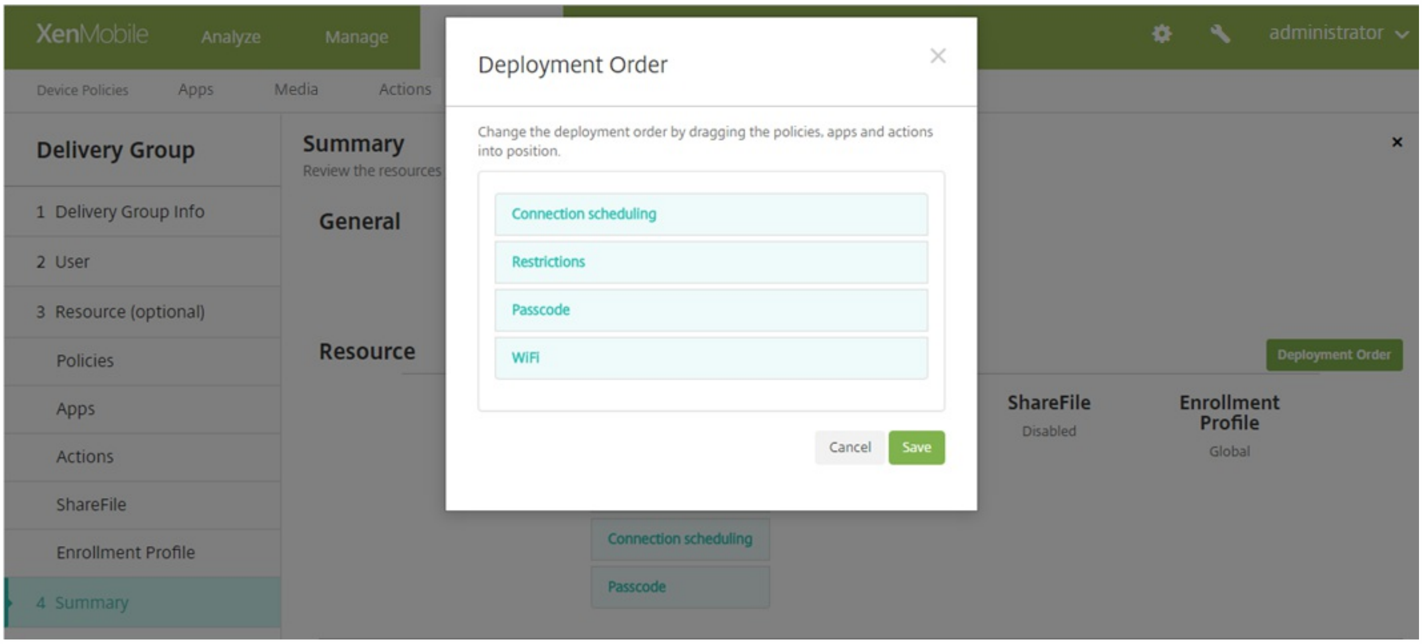
   c. While sorting, if a user-defined deployment order is specified for resources of a delivery group, maintain that order. Otherwise, sort the resources within that delivery group by resource name.

   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, XenMobile enforces the order defined by the XenMobile 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.



Deployment Order

Change the deployment order by dragging the policies, apps and actions into position.

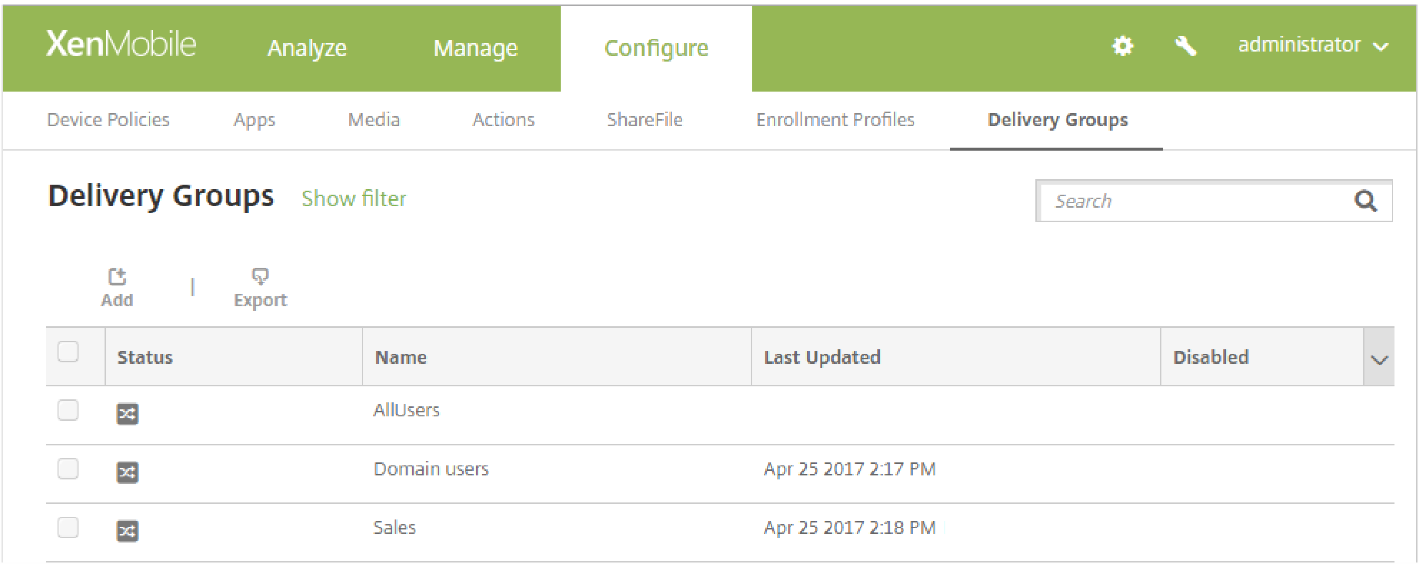
Connection scheduling
Restrictions
Passcode
WiFi

Cancel Save

If the calculation algorithm ordered deployment groups only by name, XenMobile would perform the deployment in this order, starting with the delivery group Account Managers 1: **WiFi**, **Passcode**, **Connection scheduling**, and **Restrictions**. XenMobile 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, XenMobile deploys the policies in this order: **Connection scheduling**, **Restrictions**, **Passcode**, and **WiFi**. XenMobile 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 XenMobile administrator.

1. In the XenMobile console, click **Configure** > **Delivery Groups**. The **Delivery Groups** page appears.

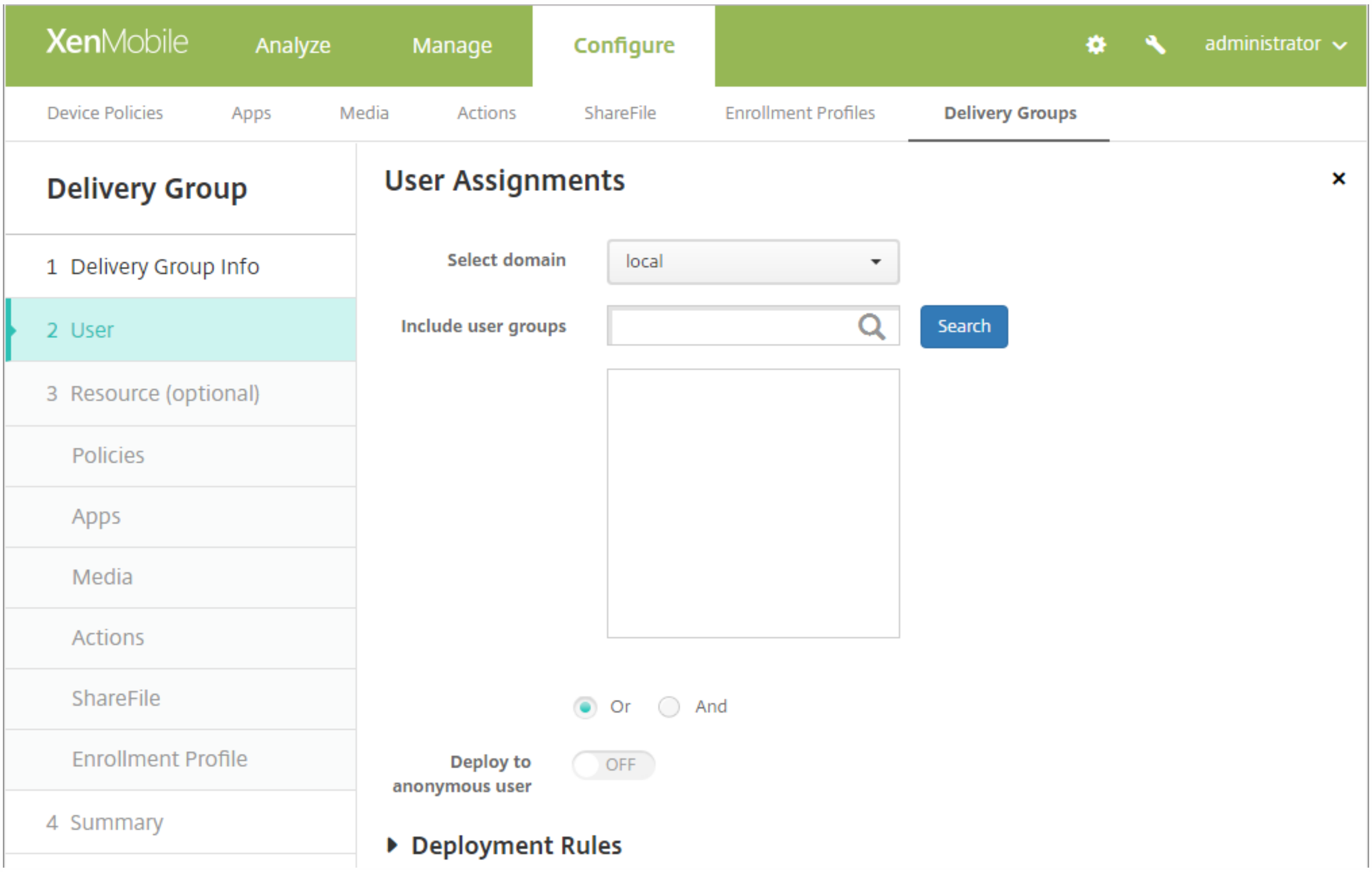


□	Status	Name	Last Updated	Disabled
□		AllUsers		
□		Domain users	Apr 25 2017 2:17 PM	
□		Sales	Apr 25 2017 2:18 PM	

2. From the **Delivery Groups** page, click **Add**. When the **Delivery Group Information** page appears, enter the following information:

- **Name**: Type a descriptive name for the delivery group.
- **Description**: Type an optional description of the delivery group.

3. Click **Next**. The **User Assignments** page appears.



Select domain: local

Include user groups:

● Or ○ And

Deploy to anonymous user: OFF

4. Configure these settings:

- **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 may 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.

  Note: Unauthenticated users are users whom you were not able to authenticate, but you allowed their devices to connect to XenMobile anyway.

5. Configure the deployment rules

a. 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 if you want to add conditions. You can add as many conditions as you would like.

b. Click the **Advanced** tab to combine the rules with Boolean options. The conditions you chose on the **Base** tab appear.

c. 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 that you want 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.

d. 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.

> **Note**: To skip a resource, under **Resources (optional)**, click the resource you want to add and follow the steps for that resource.

You can add optional resources to delivery groups to:

- Apply specific policies
- Provide required and optional apps
- Add automatic actions
- Enable ShareFile for single-sign on to content and data

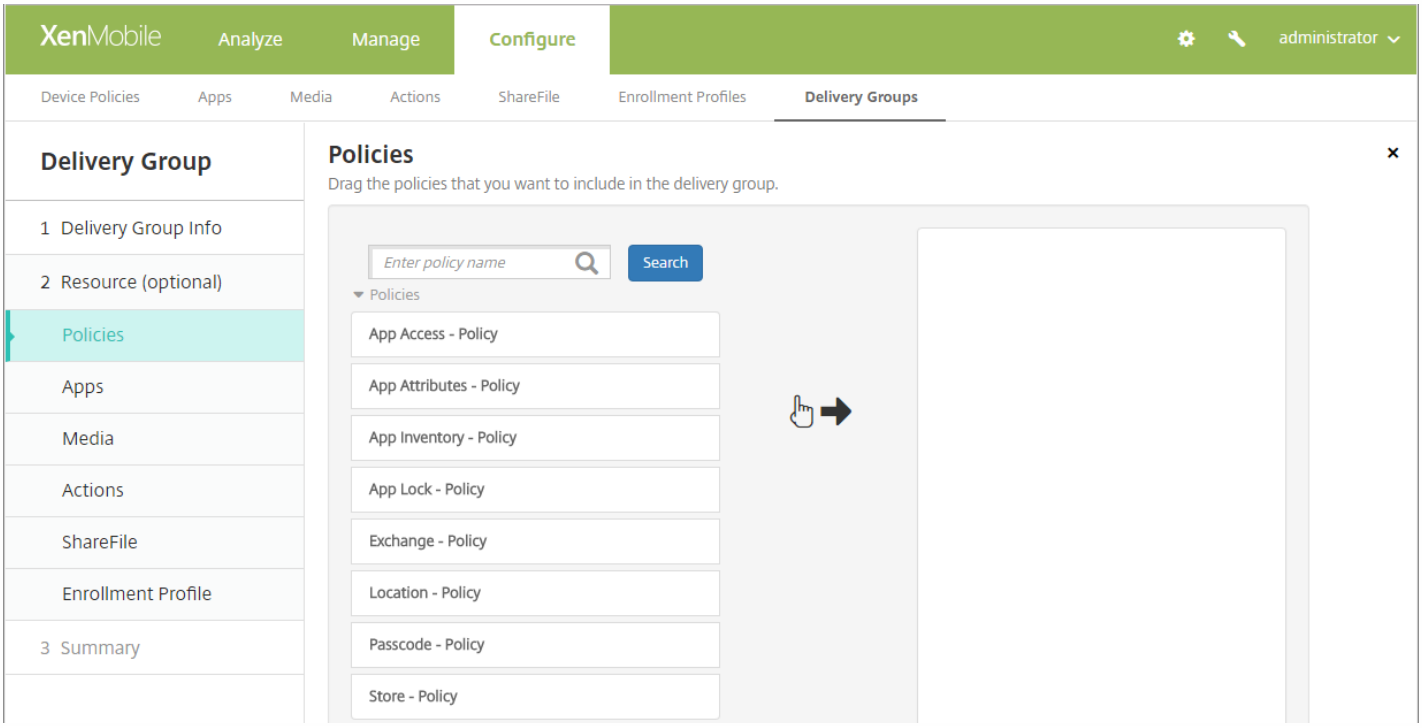
The following sections describe how to add policies, apps, actions, and how to enable ShareFile. You can add any, all, or none of these resources to the delivery group. To skip adding a resource, click **Summary**.

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.

Note: To remove a policy, click the **X** next to the policy name in the box on the right.



Policies

Drag the policies that you want to include in the delivery group.

2. Click **Next**. The **Apps** page appears.

It is very 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, XenMobile 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:

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:

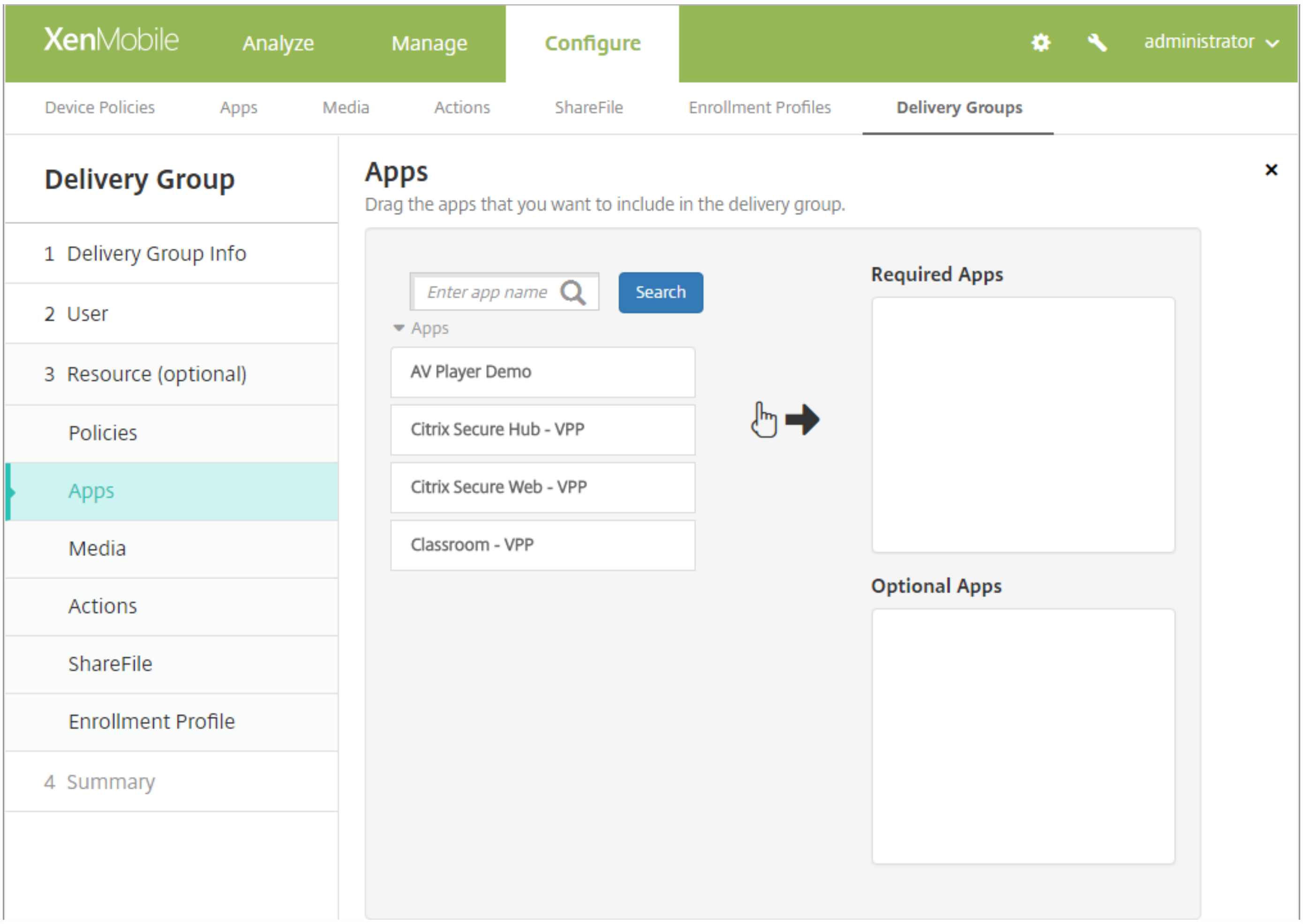
- You upload a new app and mark it as required.

- 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.

Add media

1. For each book you want to add, do the following:

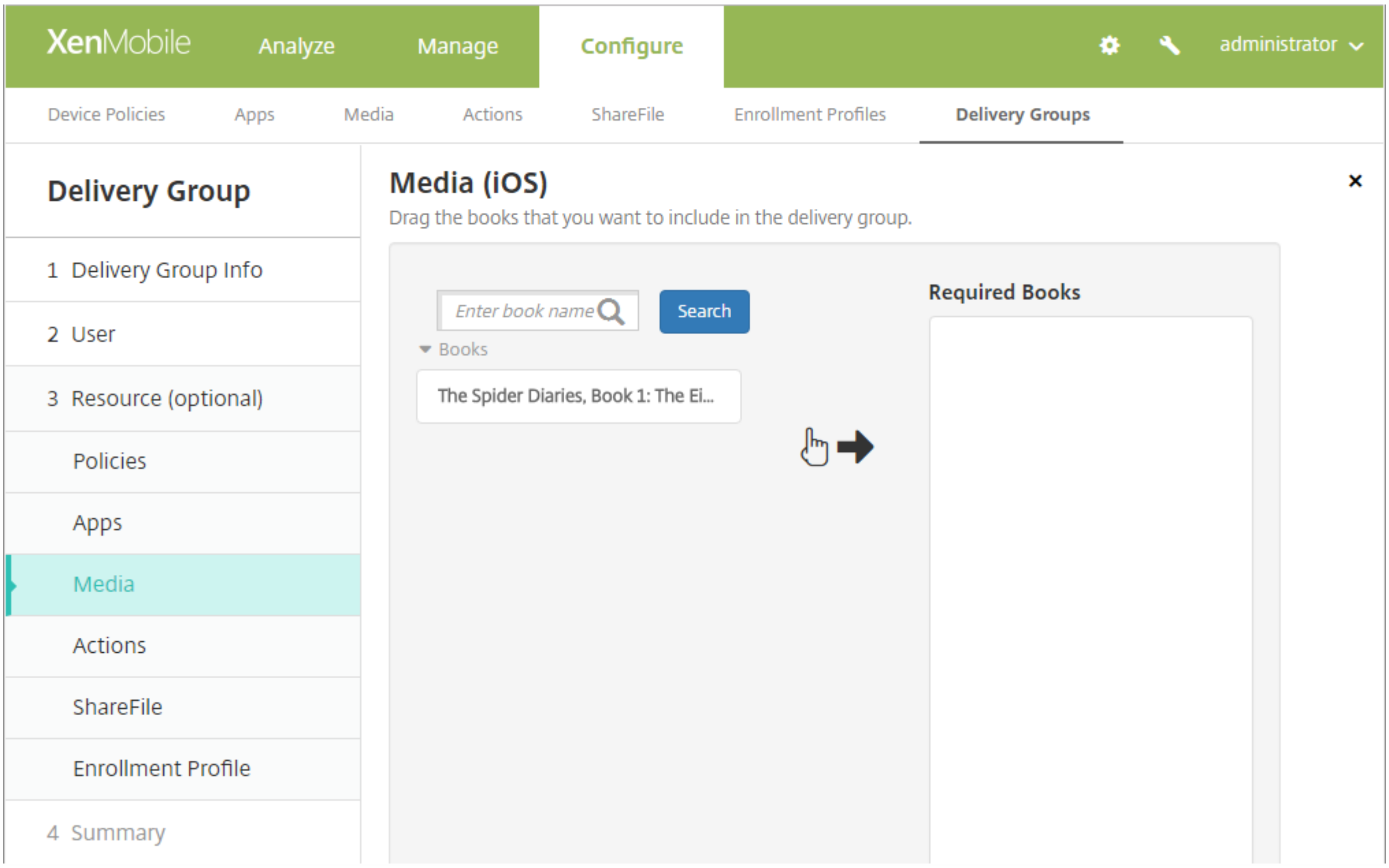
- Scroll through the list of available books to find the book you want to add.
- Or, to limit the list of books, type a full or partial book name in the search box, and then click **Search**.
- Click the book you want to add and drag it into the **Required Books** box.

It is very 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, XenMobile 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:



It is very 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, XenMobile 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:

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.

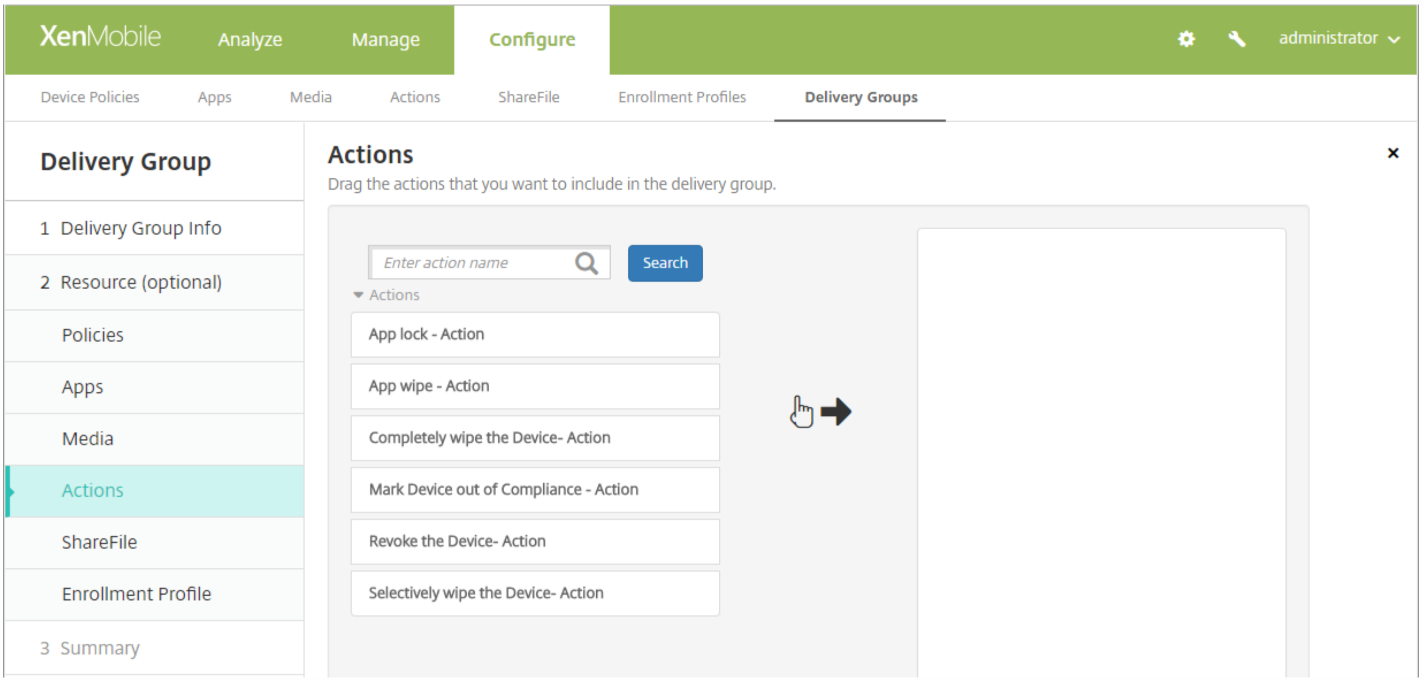
2. Click **Next**. The **Actions** page appears.

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.

Note: To remove an action, click the **X** next to the action name in the box on the right.

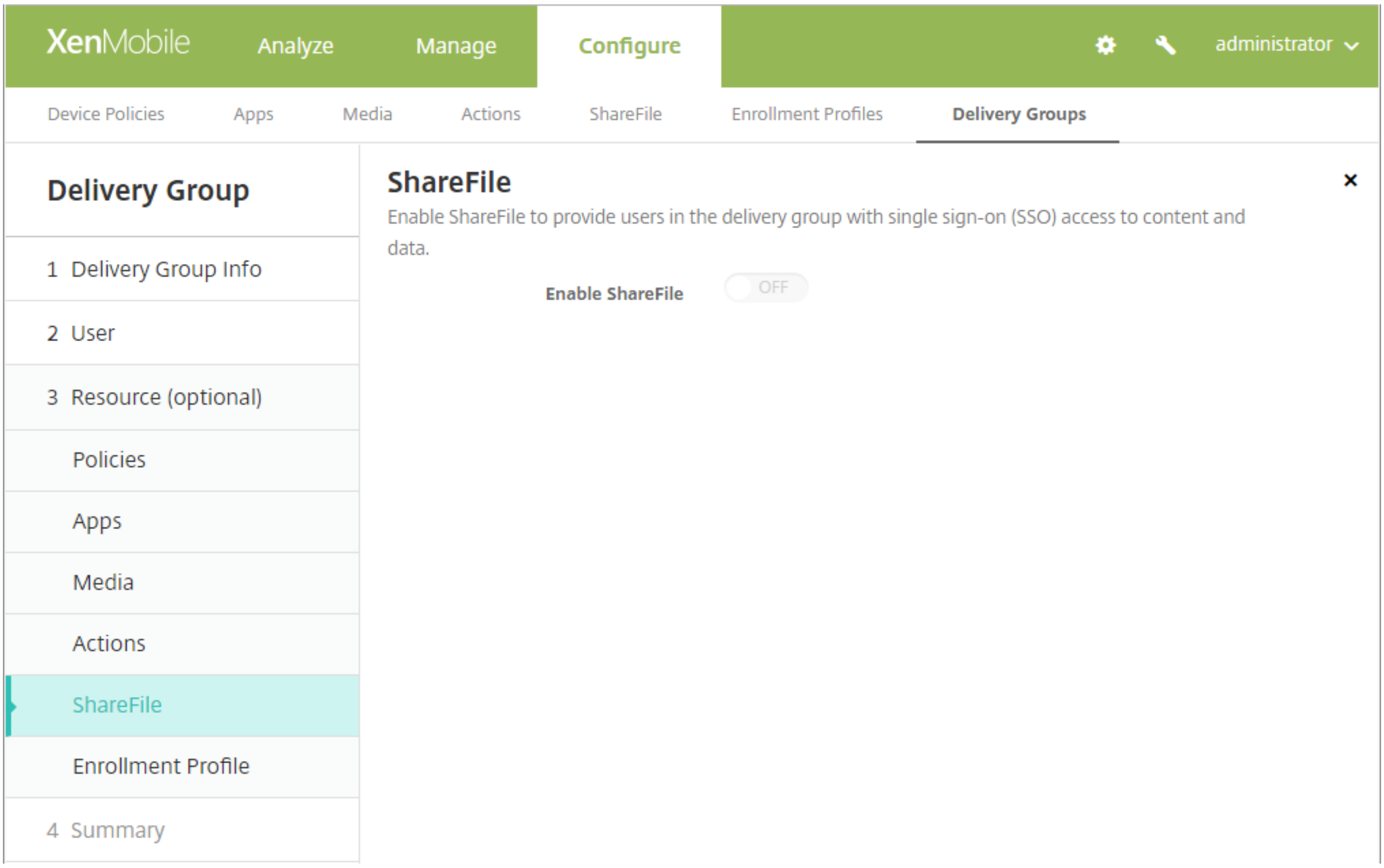


2. Click **Next**. The **ShareFile** page appears.

Apply the ShareFile configuration

The ShareFile page differs depending on whether you configured XenMobile (**Configure > ShareFile**) for ShareFile Enterprise or for StorageZone Connectors.

If you configured ShareFile Enterprise for use with XenMobile: Set **Enable ShareFile** to **ON** to provide the delivery group single sign-on access to ShareFile content and data.

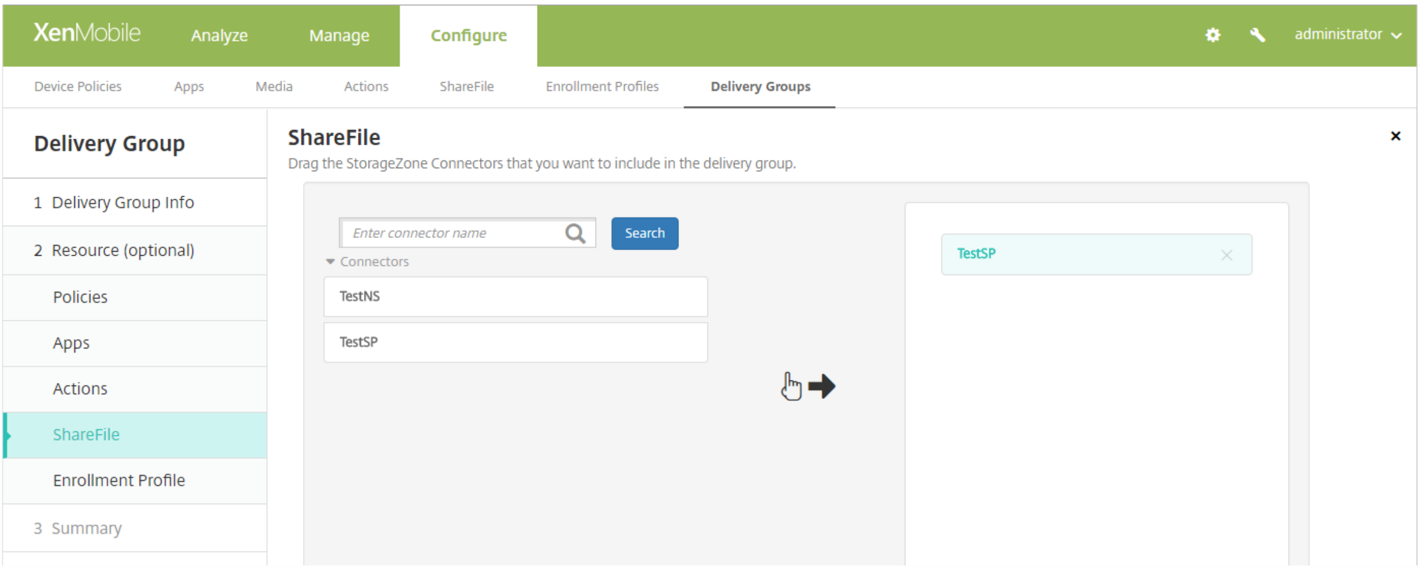


ShareFile

Enable ShareFile to provide users in the delivery group with single sign-on (SSO) access to content and data.

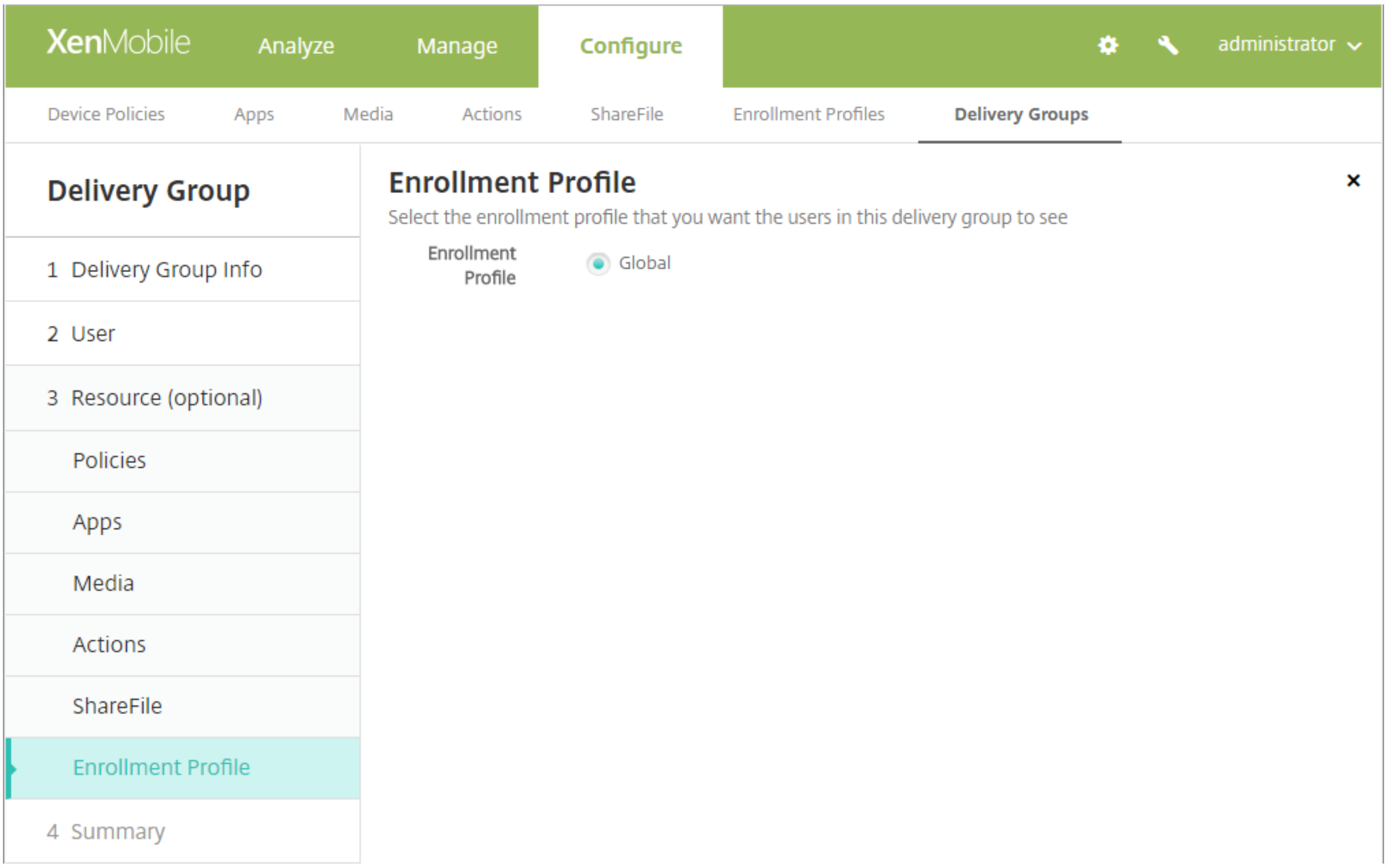
Enable ShareFile OFF

If you configured StorageZone Connectors for use with XenMobile, select the StorageZone Connectors to include in the delivery group.



ShareFile

Drag the StorageZone Connectors that you want to include in the delivery group.



Enrollment Profile

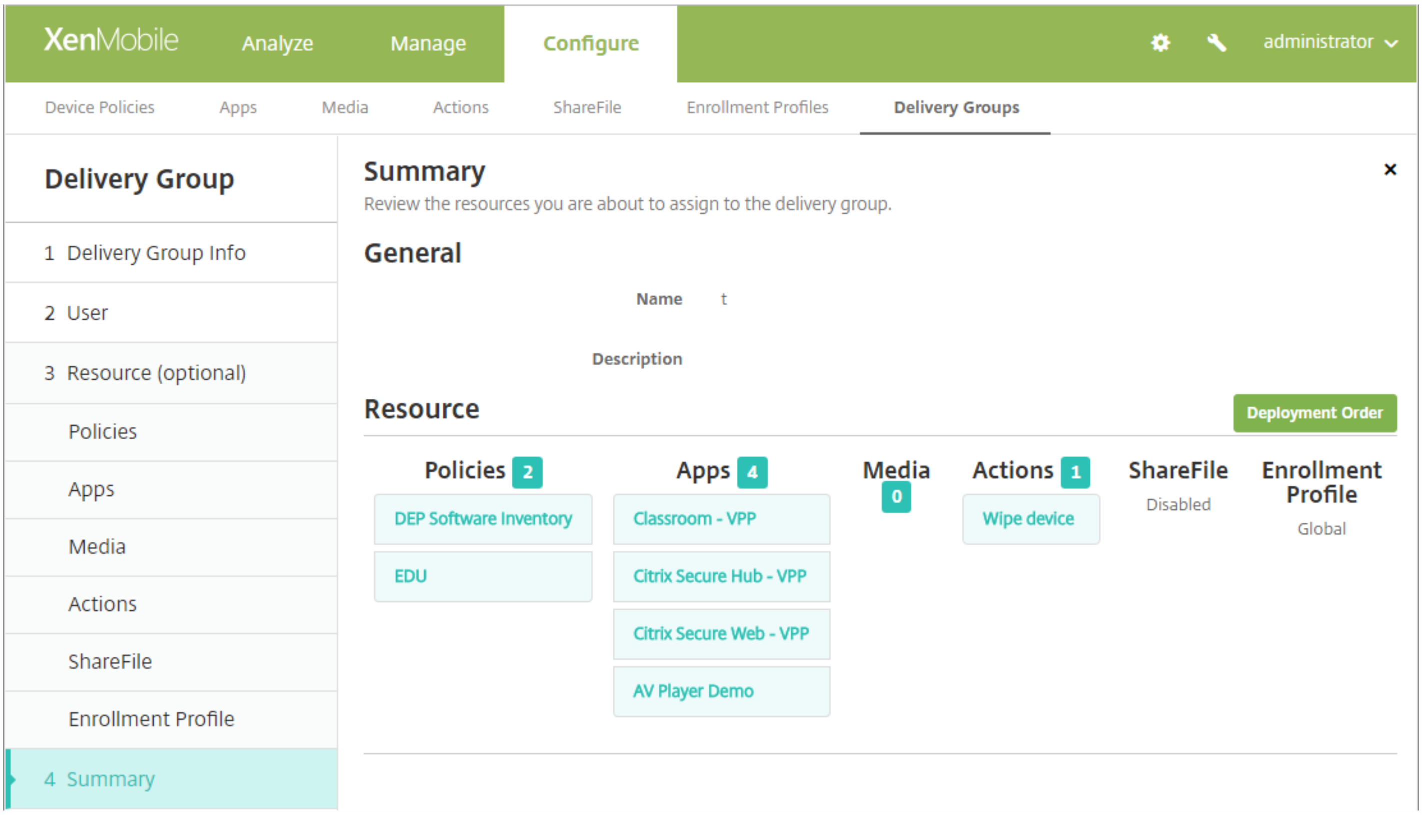
Select the enrollment profile that you want the users in this delivery group to see

Enrollment Profile ● Global

1. Configure this setting:

- **Enrollment Profile**: Select an Enrollment Profile. To create an enrollment profile, see Device enrollment limit.

2. Click **Next**. The **Summary** page appears.



Summary

Review the resources you are about to assign to the delivery group.

General

Name t

Description

Resource

Policies 2	Apps 4	Media 0	Actions 1	ShareFile	Enrollment Profile
DEP Software Inventory	Classroom - VPP		Wipe device	Disabled	Global
EDU	Citrix Secure Hub - VPP				
	Citrix Secure Web - VPP				
	AV Player Demo				

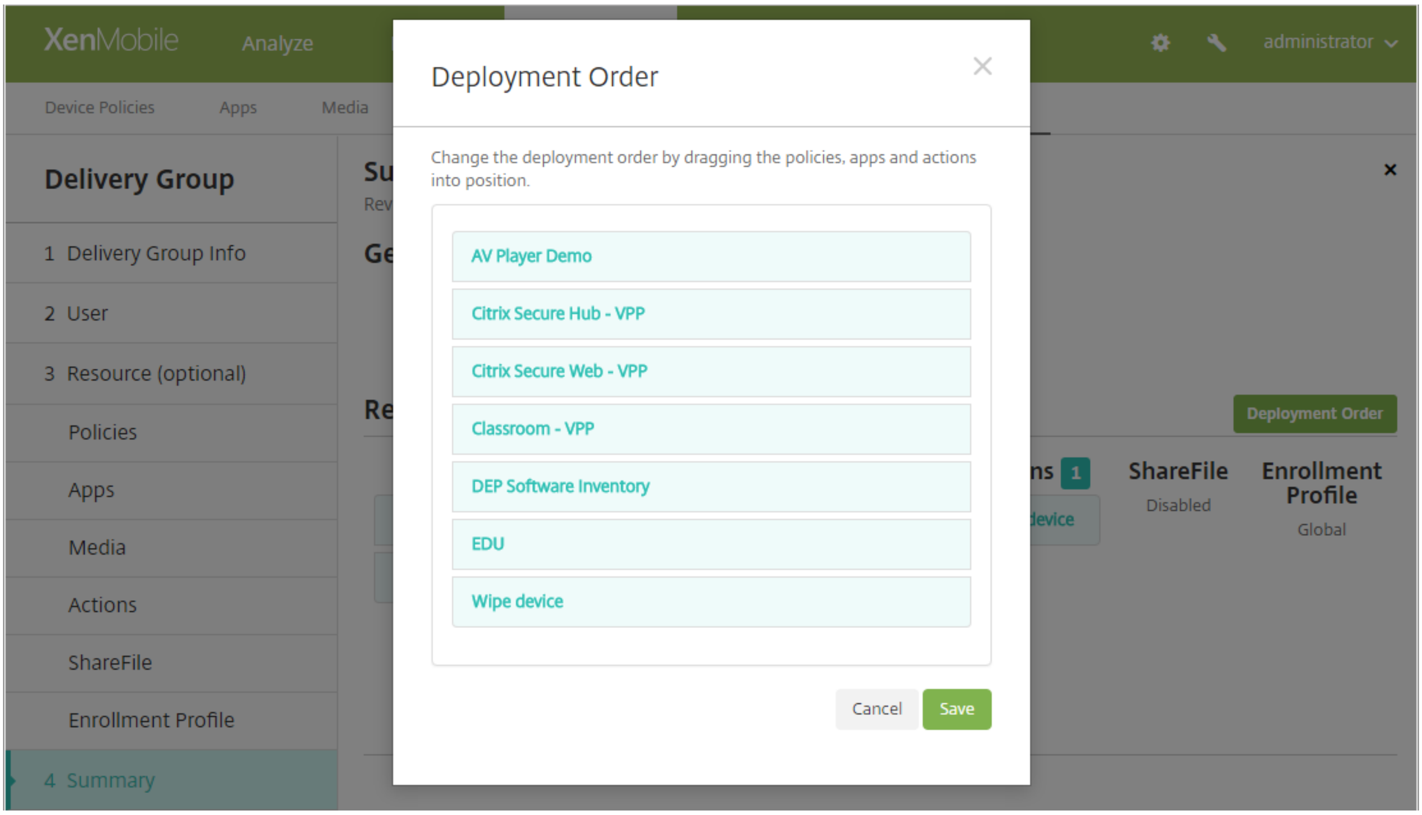
On the **Summary** page, you can review the options you have configured for the delivery group and change the deployment order of resources. The Summary page shows your resources by category. The Summary page doesn't reflect the deployment order.

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.

3. Click **Save** to save the delivery group.

1. Click the **Deployment Order** button. The **Deployment Order** dialog box appears.



Deployment Order

Change the deployment order by dragging the policies, apps and actions into position.

- AV Player Demo
- Citrix Secure Hub - VPP
- Citrix Secure Web - VPP
- Classroom - VPP
- DEP Software Inventory
- EDU
- Wipe device

2. Click on a resource and drag it to the location from which you want it deployed. After you change the deployment order, XenMobile deploys resources in the list from top to bottom.

3. Click **Save** to save the deployment order.

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**.

> ## Note
> AllUsers is the only delivery group that you can enable or disable.

1. 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:

Note: Depending on how you selected AllUsers, the **Enable** or **Disable** command appears above or to the right of the AllUsers delivery group.

- 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.

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 XenMobile. 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 XenMobile, they receive the resources immediately. Otherwise, based on their scheduling policy, they receive the resources the next time that they connect.

Note: For updated apps to appear in the Updated Available list in the XenMobile 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.

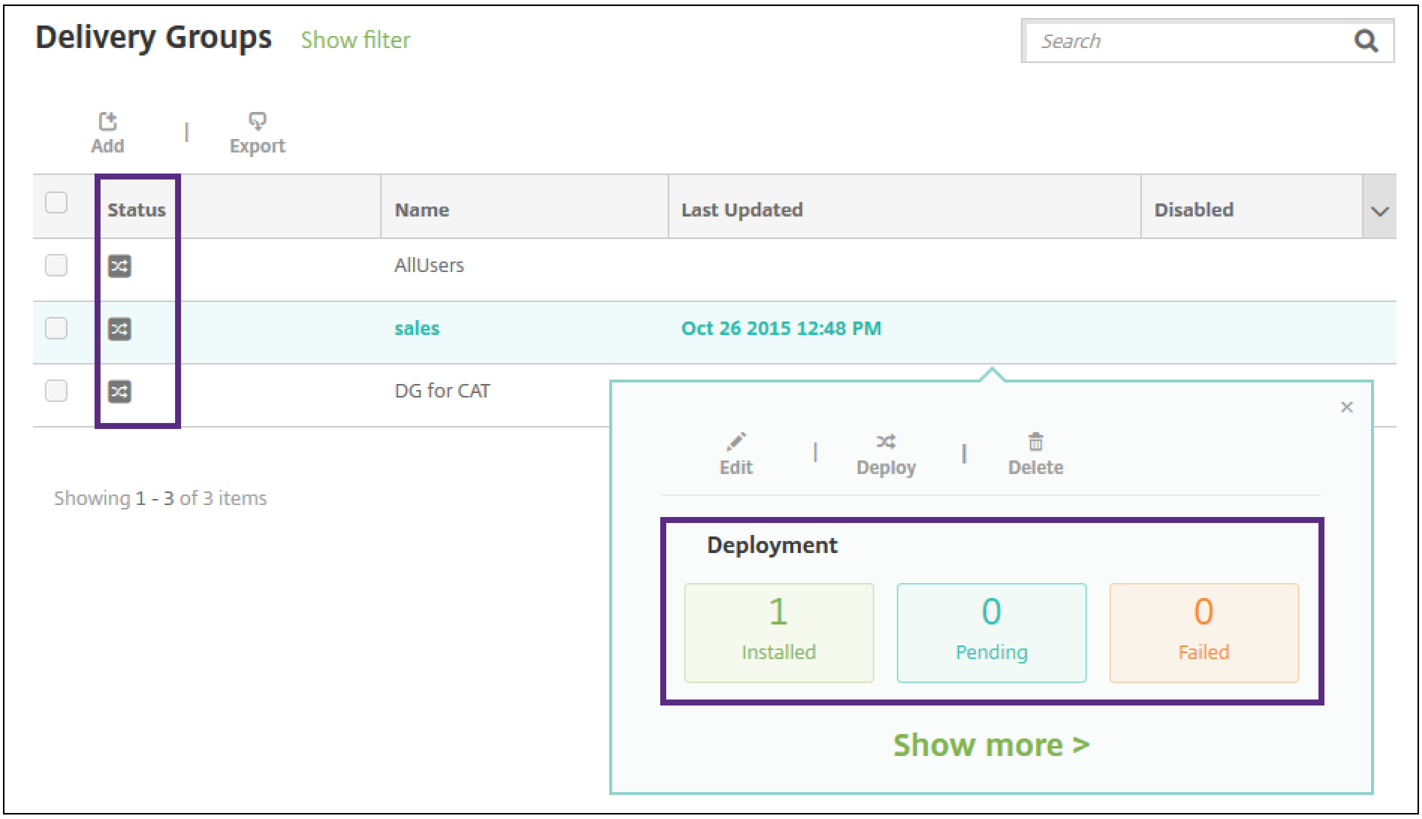
2. Click **Deploy**.

Note: 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 Show filter

Search

Add | Export

□	Status	Name	Last Updated	Disabled
□	⤨	AllUsers		
□	⤨	sales	Oct 26 2015 12:48 PM	
□	⤨	DG for CAT		

Showing 1 - 3 of 3 items

Deployment

1	0	0
Installed	Pending	Failed

Note

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.

Note: Depending on how you select a single delivery group, the **Delete** command appears above or to the right of the delivery group.

3. Click **Delete**.

Important

You cannot undo this action.

1. Click the **Export** button above the **Delivery Groups** table. XenMobile 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

Jan 18, 2018

XenMobile provides macros as a way to populate user or device property data within the text field of the following items:

- Policies
- Notifications
- Enrollment templates
- Automated actions
- Credential provider Certificate Signing Requests

XenMobile 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.

A macro can take the following form:

- ${type.PROPERTYNAME}
- ${type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]}

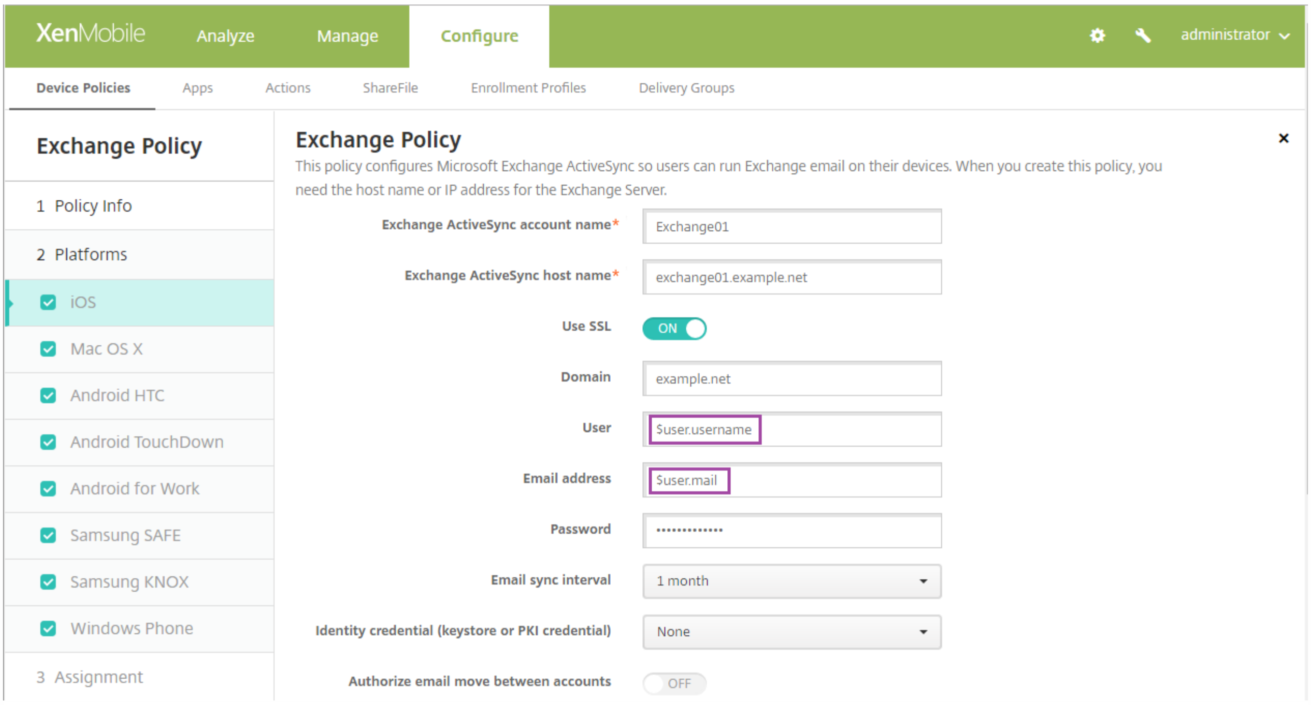
Enclose all syntax following the dollar sign ($) in curly brackets ({ }).

- Qualified property names reference either a user property, a device property, or a custom property.
- Qualified property names consist of a prefix, followed by the actual property name.
- User properties take the form ${user.[PROPERTYNAME] (prefix="user.")}.
- Device properties take the form ${device.[PROPERTYNAME] (prefix="device.")}.
- Property names are case-sensitive.
- A function can be a limited list or a link to a third-party reference that defines functions. This macro for a notification message includes the function **firstnotnull**:

  Device ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} has been blocked...

- For custom macros (properties that you define), the prefix is ${custom}. You can 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}**.



Exchange Policy

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Exchange ActiveSync account name* Exchange01

Exchange ActiveSync host name* exchange01.example.net

Use SSL ON

Domain example.net

User $user.username

Email address $user.mail

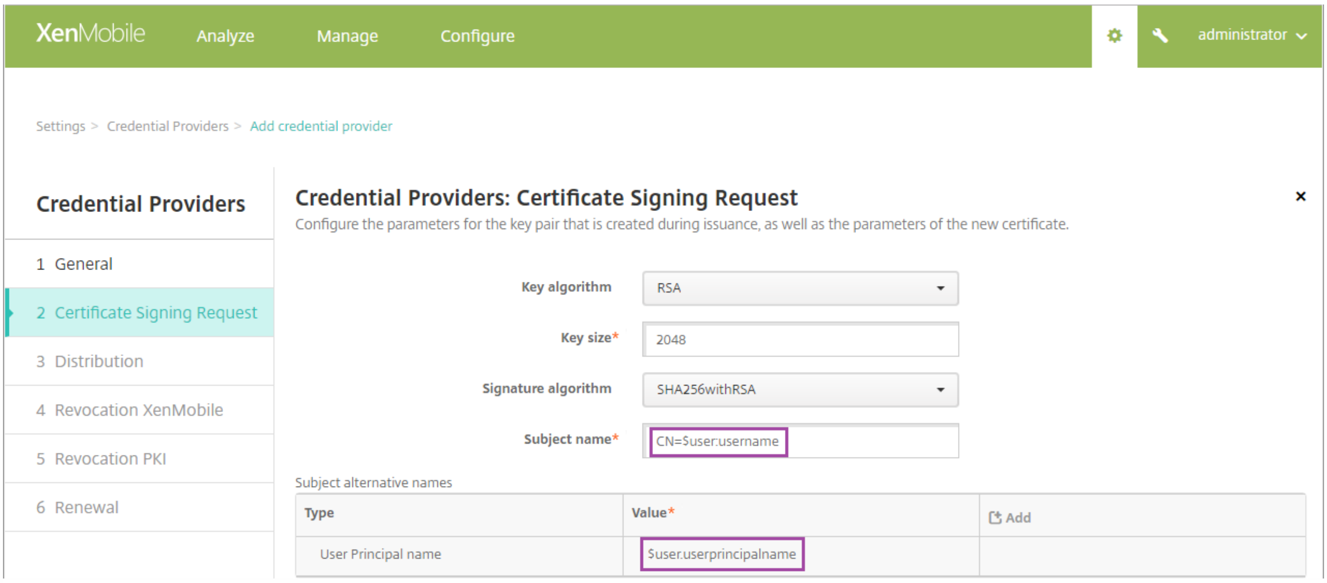
Password ••••••••••••••

Email sync interval 1 month

Identity credential (keystore or PKI credential) None

Authorize email move between accounts OFF

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**.



Credential Providers

1 General
2 Certificate Signing Request
3 Distribution
4 Revocation XenMobile
5 Revocation PKI
6 Renewal

Credential Providers: Certificate Signing Request

Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.

Key algorithm: RSA

Key size*: 2048

Signature algorithm: SHA256withRSA

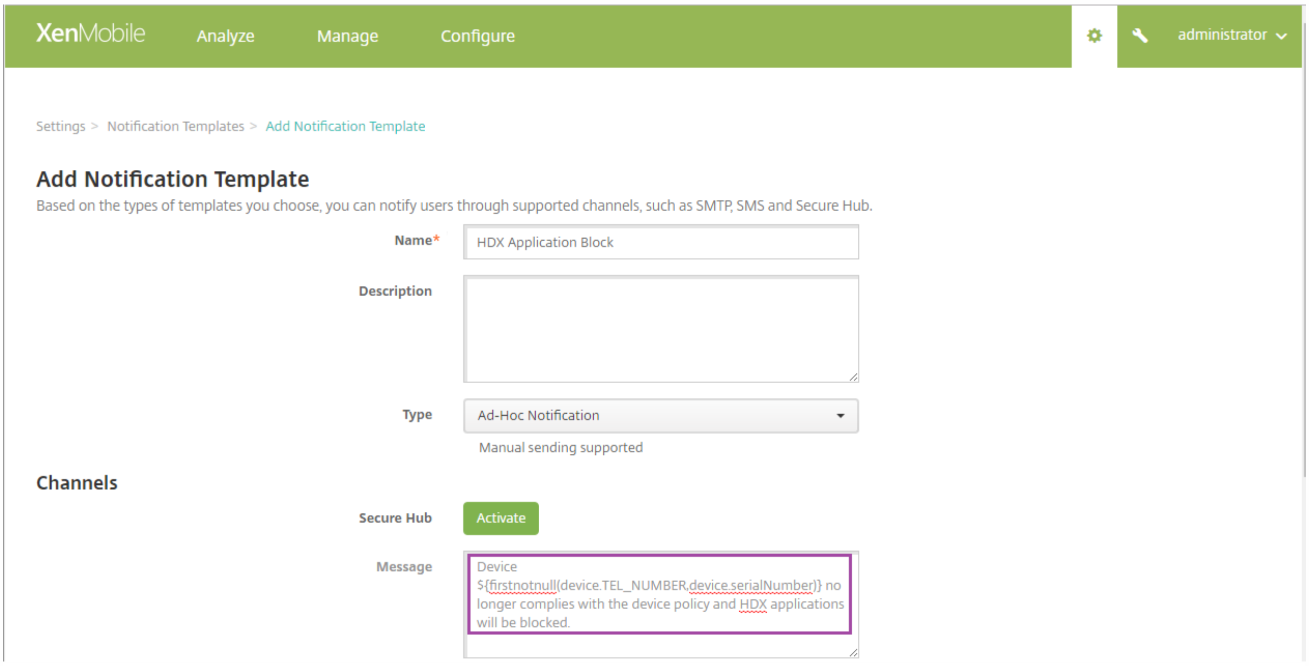
Subject name*: CN=$user.username

Subject alternative names

Type	Value*
User Principal name	$user.userprincipalname

The following example shows how to use macros in a notification template. The example template defines the message sent to a user when HDX applications are blocked because of a non-compliant device. The macro for the **Message** is:

Device ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.


XenMobile
Analyze
Manage
Configure
administrator
Settings > Notification Templates > Add Notification Template
Activate

Add Notification Template

Based on the types of templates you choose, you can notify users through supported channels, such as SMTP, SMS and Secure Hub.

Name*: HDX Application Block

Description:

Type: Ad-Hoc Notification

Manual sending supported

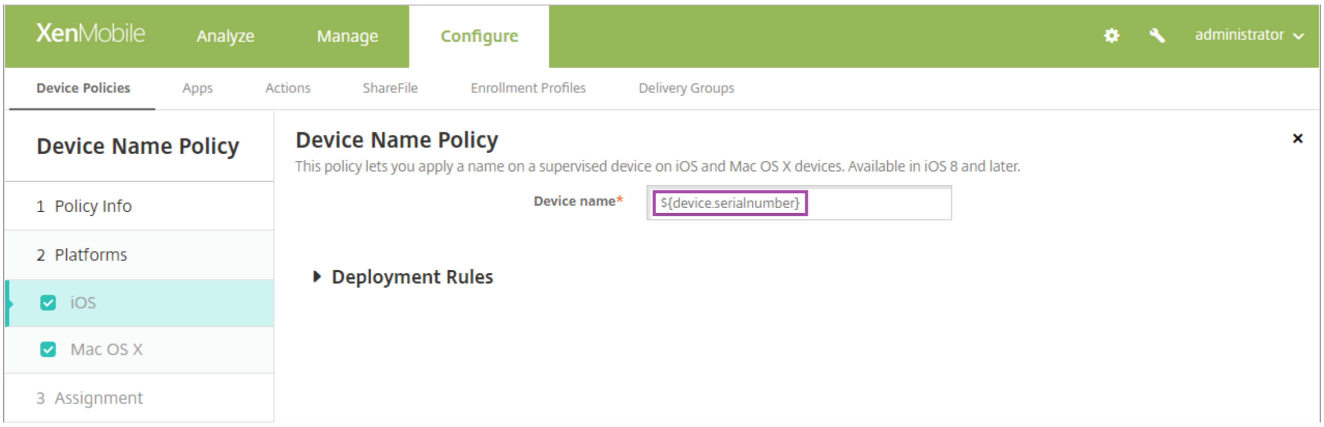
Channels

Secure Hub

Message: Device ${firstnotnull(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.



Device Name Policy

This policy lets you apply a name on a supervised device on iOS and Mac OS X devices. Available in iOS 8 and later.

Device name* ${device.serialnumber}

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

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 Webclip device policy, you can use this macro for the **URL**:

- ${webeas-url}

For the Samsung MDM License Key device policy, you can use this macro for the **ELM license key**:

- ${elm.license.key}

Display name	Macros
Device Id	$device.id
Device IMEI	$device.imei
OS Family	$device.OSFamily
Serial Number	$device.serialNumber

Display name	Web element	Macros
Account Suspended?	GOOGLE_AW_DIRECTORY_SUSPENDED	${device.GOOGLE_AW_DIRECTORY_SUSPENDED}
Activation lock bypass code	ACTIVATION_LOCK_BYPASS_CODE	${device.ACTIVATION_LOCK_BYPASS_CODE}
Activation lock enabled	ACTIVATION_LOCK_ENABLED	${device.ACTIVATION_LOCK_ENABLED}
Active iTunes account	ACTIVE_ITUNES	${device.ACTIVE_ITUNES}
ActiveSync device known by MSP	AS_DEVICE_KNOWN_BY_ZMSP	${device.AS_DEVICE_KNOWN_BY_ZMSP}
ActiveSync ID	EXCHANGE_ACTIVESYNC_ID	${device.EXCHANGE_ACTIVESYNC_ID}
Administrator disabled	ADMIN_DISABLED	${device.ADMIN_DISABLED}
AIK Present?	WINDOWS_HAS_AIK_PRESENT	${device.WINDOWS_HAS_AIK_PRESENT}
Amazon MDM API available	AMAZON_MDM	${device.AMAZON_MDM}
Android for Work Device ID	GOOGLE_AW_DEVICE_ID	${device.GOOGLE_AW_DEVICE_ID}
Android for Work Enabled Device?	GOOGLE_AW_ENABLED_DEVICE	${device.GOOGLE_AW_ENABLED_DEVICE}
Android for Work Install Type	GOOGLE_AW_INSTALL_TYPE	${device.GOOGLE_AW_INSTALL_TYPE}
Antispyware Signature tatus	ANTI_SPYWARE_SIGNATURE_STATUS	${device.ANTI_SPYWARE_SIGNATURE_STATUS}
Antispyware Status	ANTI_SPYWARE_STATUS	${device.ANTI_SPYWARE_STATUS}
Antivirus Signature Status	ANTI_VIRUS_SIGNATURE_STATUS	${device.ANTI_VIRUS_SIGNATURE_STATUS}
Antivirus Status	ANTI_VIRUS_STATUS	${device.ANTI_VIRUS_STATUS}
ASM DEP activation lock bypass code	DEP_ACTIVATION_LOCK_BYPASS_CODE	${device.DEP_ACTIVATION_LOCK_BYPASS_CODE}
ASM DEP escrow key	DEP_ESCROW_KEY	${device.DEP_ESCROW_KEY}
Asset tag	ASSET_TAG	${device.ASSET_TAG}
Automatically check software updates	AutoCheckEnabled	${device.AutoCheckEnabled}
Automatically download software updates in the background	BackgroundDownloadEnabled	${device.BackgroundDownloadEnabled}
Automatically install app updates	AutomaticAppInstallationEnabled	${device.AutomaticAppInstallationEnabled}
Automatically install OS updates	AutomaticOSInstallationEnabled	${device.AutomaticOSInstallationEnabled}
Automatically install security updates	AutomaticSecurityUpdatesEnabled	${device.AutomaticSecurityUpdatesEnabled}
Autoupdate Status	AUTOUPDATE_STATUS	${device.AUTOUPDATE_STATUS}
Available RAM	MEMORY_AVAILABLE	${device.MEMORY_AVAILABLE}
Available software updates	AVAILABLE_OS_UPDATE_HUMAN_READABLE	${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE}
Available storage space	FREEDISK	${device.FREEDISK}

Backup battery	BACKUP_BATTERY_PERCENT	${device.BACKUP_BATTERY_PERCENT}
Baseband firmware version	MODEM_FIRMWARE_VERSION	${device.MODEM_FIRMWARE_VERSION}
Battery Charging	BATTERY_CHARGING_STATUS	${device.BATTERY_CHARGING_STATUS}
Battery charging	BATTERY_CHARGING	${device.BATTERY_CHARGING}
Battery Remaining	BATTERY_ESTIMATED_CHARGE_REMAINING	${device.BATTERY_ESTIMATED_CHARGE_REMAINING}
Battery Runtime	BATTERY_RUNTIME	${device.BATTERY_RUNTIME}
Battery Status	BATTERY_STATUS	${device.BATTERY_STATUS}
Bes device known by MSP	BES_DEVICE_KNOWN_BY_ZMSP	${device.BES_DEVICE_KNOWN_BY_ZMSP}
BES PIN	BES_PIN	${device.BES_PIN}
BES server agent ID	AGENT_ID	${device.AGENT_ID}
BES server name	BES_SERVER	${device.BES_SERVER}
BES server version	BES_VERSION	${device.BES_VERSION}
BIOS Info	BIOS_INFO	${device.BIOS_INFO}
Bit Locker Status	WINDOWS_HAS_BIT_LOCKER_STATUS	${device.WINDOWS_HAS_BIT_LOCKER_STATUS}
Bluetooth MAC address	BLUETOOTH_MAC	${device.BLUETOOTH_MAC}
Boot Debugging Enabled?	WINDOWS_HAS_BOOT_DEBUGGING_ENABLED	${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED}
Boot Manager Rev List Version	WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION	${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION}
Carrier Code	CARRIER_CODE	${device.CARRIER_CODE}
Carrier settings version	CARRIER_SETTINGS_VERSION	${device.CARRIER_SETTINGS_VERSION}
Catalog URL	CatalogURL	${device.CatalogURL}
Cellular altitude	GPS_ALTITUDE_FROM_CELLULAR	${device.GPS_ALTITUDE_FROM_CELLULAR}
Cellular course	GPS_COURSE_FROM_CELLULAR	${device.GPS_COURSE_FROM_CELLULAR}
Cellular horizontal accuracy	GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR	${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR}
Cellular latitude	GPS_LATITUDE_FROM_CELLULAR	${device.GPS_LATITUDE_FROM_CELLULAR}
Cellular longitude	GPS_LONGITUDE_FROM_CELLULAR	${device.GPS_LONGITUDE_FROM_CELLULAR}
Cellular speed	GPS_SPEED_FROM_CELLULAR	${device.GPS_SPEED_FROM_CELLULAR}
Cellular technology	CELLULAR_TECHNOLOGY	${device.CELLULAR_TECHNOLOGY}
Cellular timestamp	GPS_TIMESTAMP_FROM_CELLULAR	${device.GPS_TIMESTAMP_FROM_CELLULAR}
Cellular vertical accuracy	GPS_VERTICAL_ACCURACY_FROM_CELLULAR	${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}
Change Password at Next Login?	GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN	${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

Client device ID	CLIENT_DEVICE_ID	${device.CLIENT_DEVICE_ID}
Cloud backup enabled	CLOUD_BACKUP_ENABLED	${device.CLOUD_BACKUP_ENABLED}
Code Integrity Enabled?	WINDOWS_HAS_CODE_INTEGRITY_ENABLED	${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED}
Code Integrity Rev List Version	WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION	${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION}
Color	COLOR	${device.COLOR}
CPU clock speed	CPU_CLOCK_SPEED	${device.CPU_CLOCK_SPEED}
CPU type	CPU_TYPE	${device.CPU_TYPE}
Creation Time	GOOGLE_AW_DIRECTORY_CREATION_TIME	${device.GOOGLE_AW_DIRECTORY_CREATION_TIME}
Critical software updates	AVAILABLE_OS_UPDATE_IS_CRITICAL	${device.AVAILABLE_OS_UPDATE_IS_CRITICAL}
Current carrier network	CARRIER	${device.CARRIER}
Current mobile country code	CURRENT_MCC	${device.CURRENT_MCC}
Current mobile network code	CURRENT_MNC	${device.CURRENT_MNC}
Data roaming allowed	DATA_ROAMING_ENABLED	${device.DATA_ROAMING_ENABLED}
Date of the last iCloud backup	LAST_CLOUD_BACKUP_DATE	${device.LAST_CLOUD_BACKUP_DATE}
Default catalog	IsDefaultCatalog	${device.IsDefaultCatalog}
DEP account name	BULK_ENROLLMENT_DEP_ACCOUNT_NAME	${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME}
DEP Policy	WINDOWS_HAS_DEP_POLICY	${device.WINDOWS_HAS_DEP_POLICY}
DEP profile assigned	PROFILE_ASSIGN_TIME	${device.PROFILE_ASSIGN_TIME}
DEP profile pushed	PROFILE_PUSH_TIME	${device.PROFILE_PUSH_TIME}
DEP profile removed	PROFILE_REMOVE_TIME	${device.PROFILE_REMOVE_TIME}
DEP registration by	DEVICE_ASSIGNED_BY	${device.DEVICE_ASSIGNED_BY}
DEP registration date	DEVICE_ASSIGNED_DATE	${device.DEVICE_ASSIGNED_DATE}
Description	DESCRIPTION	${device.DESCRIPTION}
Device model	SYSTEM_OEM	${device.SYSTEM_OEM}
Device name	DEVICE_NAME	${device.DEVICE_NAME}
Device Type	DEVICE_TYPE	${device.DEVICE_TYPE}
Do Not Disturb activated	DO_NOT_DISTURB	${device.DO_NOT_DISTURB}
ELAM Driver Loaded?	WINDOWS_HAS_ELAM_DRIVER_LOADED	${device.WINDOWS_HAS_ELAM_DRIVER_LOADED}
Encryption Compliance	ENCRYPTION_COMPLIANCE	${device.ENCRYPTION_COMPLIANCE}
ENROLLMENT_KEY_GENERATION_DATE	ENROLLMENT_KEY_GENERATION_DATE	${device.ENROLLMENT_KEY_GENERATION_DATE}
Enterprise ID	ENTERPRISEID	${device.ENTERPRISEID}

External storage 1: available space	EXTERNAL_STORAGE1_FREE_SPACE	${device.EXTERNAL_STORAGE1_FREE_SPACE}
External storage 1: name	EXTERNAL_STORAGE1_NAME	${device.EXTERNAL_STORAGE1_NAME}
External storage 1: total space	EXTERNAL_STORAGE1_TOTAL_SPACE	${device.EXTERNAL_STORAGE1_TOTAL_SPACE}
External storage 2: available space	EXTERNAL_STORAGE2_FREE_SPACE	${device.EXTERNAL_STORAGE2_FREE_SPACE}
External storage 2: name	EXTERNAL_STORAGE2_NAME	${device.EXTERNAL_STORAGE2_NAME}
External storage 2: total space	EXTERNAL_STORAGE2_TOTAL_SPACE	${device.EXTERNAL_STORAGE2_TOTAL_SPACE}
External storage encrypted	EXTERNAL_ENCRYPTION	${device.EXTERNAL_ENCRYPTION}
FileVault Enabled	IS_FILEVAULT_ENABLED	${device.IS_FILEVAULT_ENABLED}
Firewall Status	DEVICE_FIREWALL_STATUS	${device.DEVICE_FIREWALL_STATUS}
Firewall Status	FIREWALL_STATUS	${device.FIREWALL_STATUS}
Firmware version	FIRMWARE_VERSION	${device.FIRMWARE_VERSION}
First synchronization	ZMSP_FIRST_SYNC	${device.ZMSP_FIRST_SYNC}
Google Directory Alias	GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS	${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}
Google Directory Family Name	GOOGLE_AW_DIRECTORY_FAMILY_NAME	${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}
Google Directory Name	GOOGLE_AW_DIRECTORY_NAME	${device.GOOGLE_AW_DIRECTORY_NAME}
Google Directory Primary Email	GOOGLE_AW_DIRECTORY_PRIMARY	${device.GOOGLE_AW_DIRECTORY_PRIMARY}
Google Directory User ID	GOOGLE_AW_DIRECTORY_USER_ID	${device.GOOGLE_AW_DIRECTORY_USER_ID}
GPS altitude	GPS_ALTITUDE_FROM_GPS	${device.GPS_ALTITUDE_FROM_GPS}
GPS course	GPS_COURSE_FROM_GPS	${device.GPS_COURSE_FROM_GPS}
GPS horizontal accuracy	GPS_HORIZONTAL_ACCURACY_FROM_GPS	${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS}
GPS latitude	GPS_LATITUDE_FROM_GPS	${device.GPS_LATITUDE_FROM_GPS}
GPS longitude	GPS_LONGITUDE_FROM_GPS	${device.GPS_LONGITUDE_FROM_GPS}
GPS speed	GPS_SPEED_FROM_GPS	${device.GPS_SPEED_FROM_GPS}
GPS timestamp	GPS_TIMESTAMP_FROM_GPS	${device.GPS_TIMESTAMP_FROM_GPS}
GPS vertical accuracy	GPS_VERTICAL_ACCURACY_FROM_GPS	${device.GPS_VERTICAL_ACCURACY_FROM_GPS}
Hardware Device ID	HW_DEVICE_ID	${device.HW_DEVICE_ID}
Hardware encryption capabilities	HARDWARE_ENCRYPTION_CAPS	${device.HARDWARE_ENCRYPTION_CAPS}
HAS_CONTAINER	HAS_CONTAINER	${device.HAS_CONTAINER}
Hash of the iTunes store account currently logged on	ITUNES_STORE_ACCOUNT_HASH	${device.ITUNES_STORE_ACCOUNT_HASH}
Home carrier network	SIM_CARRIER_NETWORK	${device.SIM_CARRIER_NETWORK}

Home mobile country code	SIM_MCC	${device.SIM_MCC}
Home mobile network code	SIM_MNC	${device.SIM_MNC}
HTC API version	HTC_MDM_VERSION	${device.HTC_MDM_VERSION}
HTC MDM API available	HTC_MDM	${device.HTC_MDM}
ICCID	ICCID	${device.ICCID}
Identity	AS_DEVICE_IDENTITY	${device.AS_DEVICE_IDENTITY}
IMEI/MEID number	IMEI	${device.IMEI}
IMSI	SIM_ID	${device.SIM_ID}
Internal storage encrypted	LOCAL_ENCRYPTION	${device.LOCAL_ENCRYPTION}
IP location	IP_LOCATION	${device.IP_LOCATION}
IPV4 Address	IP_ADDRESSV4	${device.IP_ADDRESSV4}
IPV6 Address	IP_ADDRESSV6	${device.IP_ADDRESSV6}
Issued At	WINDOWS_HAS_ISSUED_AT	${device.WINDOWS_HAS_ISSUED_AT}
Jailbroken/Rooted	ROOT_ACCESS	${device.ROOT_ACCESS}
Kernel Debugging Enabled?	WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED	${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED}
Kiosk mode	IS_KIOSK	${device.IS_KIOSK}
Last known IP address	LAST_IP_ADDR	${device.LAST_IP_ADDR}
Last policy update time	LAST_POLICY_UPDATE_TIME	${device.LAST_POLICY_UPDATE_TIME}
Last scan date	PreviousScanDate	${device.PreviousScanDate}
Last scan result	PreviousScanResult	${device.PreviousScanResult}
Last scheduled software updates	AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME	${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}
Last scheduled software updates failure message	AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG	${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG}
Last scheduled software updates status	AVAILABLE_OS_UPDATE_INSTALL_STATUS	${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS}
Last synchronization	ZMSP_LAST_SYNC	${device.ZMSP_LAST_SYNC}
Locator service enabled	DEVICE_LOCATOR	${device.DEVICE_LOCATOR}
MAC Address	MAC_ADDRESS	${device.MAC_ADDRESS}
MAC Address Network Connection	MAC_NETWORK_CONNECTION	${device.MAC_NETWORK_CONNECTION}
MAC Address Type	MAC_ADDRESS_TYPE	${device.MAC_ADDRESS_TYPE}
Mailbox Setup	GOOGLE_AW_DIRECTORY_MAILBOX_SETUP	${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP}
Main battery	MAIN_BATTERY_PERCENT	${device.MAIN_BATTERY_PERCENT}

MDM lost mode enabled	IS_MDM_LOST_MODE_ENABLED	${device.IS_MDM_LOST_MODE_ENABLED}
MDX_SHARED_ENCRYPTION_KEY	MDX_SHARED_ENCRYPTION_KEY	${device.MDX_SHARED_ENCRYPTION_KEY}
MEID	MEID	${device.MEID}
Mobile phone number	TEL_NUMBER	${device.TEL_NUMBER}
Model ID	MODEL_ID	${device.MODEL_ID}
Model Number	MODEL_NUMBER	${device.MODEL_NUMBER}
Network Adapter Type	NETWORK_ADAPTER_TYPE	${device.NETWORK_ADAPTER_TYPE}
NitroDesk TouchDown installed	TOUCHDOWN_FIND	${device.TOUCHDOWN_FIND}
NitroDesk TouchDown licensed via MDM	TOUCHDOWN_LICENSED_VIA_MDM	${device.TOUCHDOWN_LICENSED_VIA_MDM}
Operating system build	SYSTEM_OS_BUILD	${device.SYSTEM_OS_BUILD}
Operating System Edition	OS_EDITION	${device.OS_EDITION}
Operating system language (locale)	SYSTEM_LANGUAGE	${device.SYSTEM_LANGUAGE}
Operating system version	SYSTEM_OS_VERSION	${device.SYSTEM_OS_VERSION}
Organization address	ORGANIZATION_ADDRESS	${device.ORGANIZATION_ADDRESS}
Organization e-mail	ORGANIZATION_EMAIL	${device.ORGANIZATION_EMAIL}
Organization magic	ORGANIZATION_MAGIC	${device.ORGANIZATION_MAGIC}
Organization name	ORGANIZATION_NAME	${device.ORGANIZATION_NAME}
Organization phone number	ORGANIZATION_PHONE	${device.ORGANIZATION_PHONE}
Out of Compliance	OUT_OF_COMPLIANCE	${device.OUT_OF_COMPLIANCE}
Owned by	CORPORATE_OWNED	${device.CORPORATE_OWNED}
Passcode compliant	PASSCODE_IS_COMPLIANT	${device.PASSCODE_IS_COMPLIANT}
Passcode compliant with configuration	PASSCODE_IS_COMPLIANT_WITH_CFG	${device.PASSCODE_IS_COMPLIANT_WITH_CFG}
Passcode present	PASSCODE_PRESENT	${device.PASSCODE_PRESENT}
PCR0	WINDOWS_HAS_PCR0	${device.WINDOWS_HAS_PCR0}
Perimeter breach	GPS_PERIMETER_BREACH	${device.GPS_PERIMETER_BREACH}
Periodic check	PerformPeriodicCheck	${device.PerformPeriodicCheck}
Personal Hotspot activated	PERSONAL_HOTSPOT_ENABLED	${device.PERSONAL_HOTSPOT_ENABLED}
PIN code for geofence	PIN_CODE_FOR_GEO_FENCE	${device.PIN_CODE_FOR_GEO_FENCE}
Platform	SYSTEM_PLATFORM	${device.SYSTEM_PLATFORM}
Platform API level	API_LEVEL	${device.API_LEVEL}

Policy name	POLICY_NAME	${device.POLICY_NAME}
Primary Phone Number	IDENTITY1_PHONENUMBER	${device.IDENTITY1_PHONENUMBER}
Primary SIM Carrier Operator	IDENTITY1_CARRIER_NETWORK_OPERATOR	${device.IDENTITY1_CARRIER_NETWORK_OPERATOR}
Primary SIM ICCID	IDENTITY1_ICCID	${device.IDENTITY1_ICCID}
Primary SIM IMEI	IDENTITY1_IMEI	${device.IDENTITY1_IMEI}
Primary SIM IMSI	IDENTITY1_IMSI	${device.IDENTITY1_IMSI}
Primary SIM Roaming	IDENTITY1_ROAMING	${device.IDENTITY1_ROAMING}
Primary SIM Roaming Compliance	IDENTITY1_ROAMING_COMPLIANCE	${device.IDENTITY1_ROAMING_COMPLIANCE}
Product name	PRODUCT_NAME	${device.PRODUCT_NAME}
Publisher Device ID	PUBLISHER_DEVICE_ID	${device.PUBLISHER_DEVICE_ID}
Reset Count	WINDOWS_HAS_RESET_COUNT	${device.WINDOWS_HAS_RESET_COUNT}
Restart Count	WINDOWS_HAS_RESTART_COUNT	${device.WINDOWS_HAS_RESTART_COUNT}
Safe Mode Enabled?	WINDOWS_HAS_SAFE_MODE	${device.WINDOWS_HAS_SAFE_MODE}
Samsung KNOX API available	SAMSUNG_KNOX	${device.SAMSUNG_KNOX}
Samsung KNOX API version	SAMSUNG_KNOX_VERSION	${device.SAMSUNG_KNOX_VERSION}
Samsung KNOX attestation	SAMSUNG_KNOX_ATTESTED	${device.SAMSUNG_KNOX_ATTESTED}
Samsung KNOX attestation updated date	SAMSUNG_KNOX_ATT_UPDATED_TIME	${device.SAMSUNG_KNOX_ATT_UPDATED_TIME}
Samsung SAFE API available	SAMSUNG_MDM	${device.SAMSUNG_MDM}
Samsung SAFE API version	SAMSUNG_MDM_VERSION	${device.SAMSUNG_MDM_VERSION}
SBCP Hash	WINDOWS_HAS_SBCP_HASH	${device.WINDOWS_HAS_SBCP_HASH}
Screen: height	SCREEN_HEIGHT	${device.SCREEN_HEIGHT}
Screen: number of colors	SCREEN_NB_COLORS	${device.SCREEN_NB_COLORS}
Screen: size	SCREEN_SIZE	${device.SCREEN_SIZE}
Screen: width	SCREEN_WIDTH	${device.SCREEN_WIDTH}
Screen: X-axis resolution	SCREEN_XDPI	${device.SCREEN_XDPI}
Screen: Y-axis resolution	SCREEN_YDPI	${device.SCREEN_YDPI}
Secondary Phone Number	IDENTITY2_PHONENUMBER	${device.IDENTITY2_PHONENUMBER}
Secondary SIM Carrier Operator	IDENTITY2_CARRIER_NETWORK_OPERATOR	${device.IDENTITY2_CARRIER_NETWORK_OPERATOR}
Secondary SIM ICCID	IDENTITY2_ICCID	${device.IDENTITY2_ICCID}
Secondary SIM IMEI	IDENTITY2_IMEI	${device.IDENTITY2_IMEI}
Secondary SIM IMSI	IDENTITY2_IMSI	${device.IDENTITY2_IMSI}

Secondary SIM Roaming	IDENTITY2_ROAMING	${device.IDENTITY2_ROAMING}
Secondary SIM Roaming Compliance	IDENTITY2_ROAMING_COMPLIANCE	${device.IDENTITY2_ROAMING_COMPLIANCE}
Secure Boot Enabled?	WINDOWS_HAS_SECURE_BOOT_ENABLED	${device.WINDOWS_HAS_SECURE_BOOT_ENABLED}
Secure Boot Status	SECURE_BOOT_STATE	${device.SECURE_BOOT_STATE}
SecureContainer Enabled	DLP_ACTIVE	${device.DLP_ACTIVE}
Security patch level	SYSTEM_SECURITY_PATCH_LEVEL	${device.SYSTEM_SECURITY_PATCH_LEVEL}
Serial number	SERIAL_NUMBER	${device.SERIAL_NUMBER}
SMS capable	IS_SMS_CAPABLE	${device.IS_SMS_CAPABLE}
Sony Enterprise API available	SONY_MDM	${device.SONY_MDM}
Sony Enterprise API version	SONY_MDM_VERSION	${device.SONY_MDM_VERSION}
Supervised	SUPERVISED	${device.SUPERVISED}
Suspension Reason	GOOGLE_AW_DIRECTORY_SUSPENTION_REASON	${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON}
Tampered Status	TAMPERED_STATUS	${device.TAMPERED_STATUS}
Terms & Conditions	TERMS_AND_CONDITIONS	${device.TERMS_AND_CONDITIONS}
Terms And Agreement Accepted?	GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS	${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS}
Test Signing Enabled?	WINDOWS_HAS_TEST_SIGNING_ENABLED	${device.WINDOWS_HAS_TEST_SIGNING_ENABLED}
Total RAM	MEMORY	${device.MEMORY}
Total storage space	TOTAL_DISK_SPACE	${device.TOTAL_DISK_SPACE}
TPM version	TPM_VERSION	${device.TPM_VERSION}
UDID	UDID	${device.UDID}
User Account Control Status	UAC_STATUS	${device.UAC_STATUS}
User agent	USER_AGENT	${device.USER_AGENT}
User defined #1	USER_DEFINED_1	${device.USER_DEFINED_1}
User defined #2	USER_DEFINED_2	${device.USER_DEFINED_2}
User defined #3	USER_DEFINED_3	${device.USER_DEFINED_3}
User language (locale)	USER_LANGUAGE	${device.USER_LANGUAGE}
Vendor	VENDOR	${device.VENDOR}
Voice capable	IS_VOICE_CAPABLE	${device.IS_VOICE_CAPABLE}
Voice roaming allowed	VOICE_ROAMING_ENABLED	${device.VOICE_ROAMING_ENABLED}
VSM Enabled?	WINDOWS_HAS_VSM_ENABLED	${device.WINDOWS_HAS_VSM_ENABLED}

WiFi MAC address	WIFI_MAC	${device.WIFI_MAC}
WINDOWS_ENROLLMENT_KEY	WINDOWS_ENROLLMENT_KEY	${device.WINDOWS_ENROLLMENT_KEY}
WinPE Enabled?	WINDOWS_HAS_WINPE	${device.WINDOWS_HAS_WINPE}
WNS Notification Status	PROPERTY_WNS_PUSH_STATUS	${device.PROPERTY_WNS_PUSH_STATUS}
WNS Notification URL	PROPERTY_WNS_PUSH_URL	${device.PROPERTY_WNS_PUSH_URL}
WNS Notification URL expiry date	PROPERTY_WNS_PUSH_URL_EXPIRY	${device.PROPERTY_WNS_PUSH_URL_EXPIRY}
XenMobile agent ID	ENROLLMENT_AGENT_ID	${device.ENROLLMENT_AGENT_ID}
XenMobile agent revision	EW_REVISION	${device.EW_REVISION}
XenMobile agent version	EW_VERSION	${device.EW_VERSION}
Zebra API available	ZEBRA_MDM	${device.ZEBRA_MDM}
Zebra MXMF version	ZEBRA_MDM_VERSION	${device.ZEBRA_MDM_VERSION}
Zebra Patch version	ZEBRA_PATCH_VERSION	${device.ZEBRA_PATCH_VERSION}

Display name	**Macros**
domainname (domain name; default domain)	${user.domainname}
loginname (user name plus domain name)	${user.loginname}
username (login name minus the domain, if any)	${user.username}

Display name	**Web element**	**Macros**
Active Directory failed logon tries	badpwdcount	${user.badpwdcount}
ActiveSync user email	asuseremail	${user.asuseremail}
ASM data source	asmpersonsource	${user.asmpersonsource}
ASM DEP account name	asmdepaccount	${user.asmdepaccount}
ASM managed Apple ID	asmpersonmanagedappleid	${user.asmpersonmanagedappleid}
ASM passcode type	asmpersonpasscodetype	${user.asmpersonpasscodetype}
ASM person ID	asmpersonid	${user.asmpersonid}
ASM person status	asmpersonstatus	${user.asmpersonstatus}
ASM person title	asmpersontitle	${user.asmpersontitle}
ASM person unique ID	asmpersonuniqueid	${user.asmpersonuniqueid}
ASM source system ID	asmpersonsourcesystemid	${user.asmpersonsourcesystemid}
ASM student grade	asmpersongrade	${user.asmpersongrade}

BES user email	besuseremail	${user.besuseremail}
Company	company	${user.company}
Company name	companyname	${user.companyname}
Country	c	${user.c}
Department	department	${user.department}
Description	description	${user.description}
Disabled user	disableduser	${user.disableduser}
Display name	displayname	${user.displayname}
Distinguished name	distinguishedname	${user.distinguishedname}
Domain name	domainname	${user.domainname}
Email	mail	${user.mail}
First name	givenname	${user.givenname}
Home address	homestreetaddress	${user.homestreetaddress}
Home city	homecity	${user.homecity}
Home country	homecountry	${user.homecountry}
Home fax	homefax	${user.homefax}
Home phone	homephone	${user.homephone}
Home state/region	homestate	${user.homestate}
Home zip or post code	homezip	${user.homezip}
IP phone	ipphone	${user.ipphone}
Middle initial	middleinitial	${user.middleinitial}
Middle name	middlename	${user.middlename}
Mobile	mobile	${user.mobile}
Name	cn	${user.cn}
Office address	physicaldeliveryofficename	${user.physicaldeliveryofficename}
Office city	l	${user.l}
Office fax number	facsimiletelephonenumber	${user.facsimiletelephonenumber}
Office state/province	st	${user.st}
Office street address	officestreetaddress	${user.officestreetaddress}
Office telephone number	telephonenumber	${user.telephonenumber}

Office zip or post code	postalcode	${user.postalcode}
P.O. box	postofficebox	${user.postofficebox}
Pager	pager	${user.pager}
Primary group ID	primarygroupid	${user.primarygroupid}
SAM account	samaccountname	${user.samaccountname}
Street address	streetaddress	${user.streetaddress}
Surname	sn	${user.sn}
Title	title	${user.title}
User logon name	userprincipalname	${user.userprincipalname}

Automated actions

Nov 06, 2017

You create automated actions in XenMobile to program a reaction to events, user or device properties, or the existence of apps on user devices. When you create an automated action, you establish the effect on the user's device when it is connected to XenMobile based on triggers in the action. 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, if you want to detect an app that you have previously blacklisted (for example, Words with Friends), you can specify a trigger that sets the user's device out of compliance when Words with Friends is detected on their device. The action then notifies them that they must remove the app to bring their device back into compliance. You can set a time limit for how long to wait for the user to comply before taking more serious action, such as selectively wiping the device.

In cases in which a user's device is put into an out of compliance state, and then the user fixes the device so that the device is in compliance, you will need to 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.

This article explains how to add, edit, and filter automated actions in XenMobile, as well as how to configure app lock and app wipe actions for MAM-only mode.

> ### Note
>
> Before you can notify users, you must have configured notification servers in Settings for SMTP and SMS so that XenMobile can send the messages, see Notifications in XenMobile. Also, set up any notification templates you plan to use before proceeding. For details about setting up notification templates, see To create or update notification templates in XenMobile.

1. From the XenMobile console, click **Configure** > **Actions**. The **Actions** page appears.

2. On the **Actions** page, do one of the following:

- Click **Add** to add a new action.
- Select an existing action to edit or delete. Click the option you want to use.

Note: When you select the check box next to an action, the options menu appears above the action list; when you click anywhere else in the list, the options menu appears on the right side of the listing.

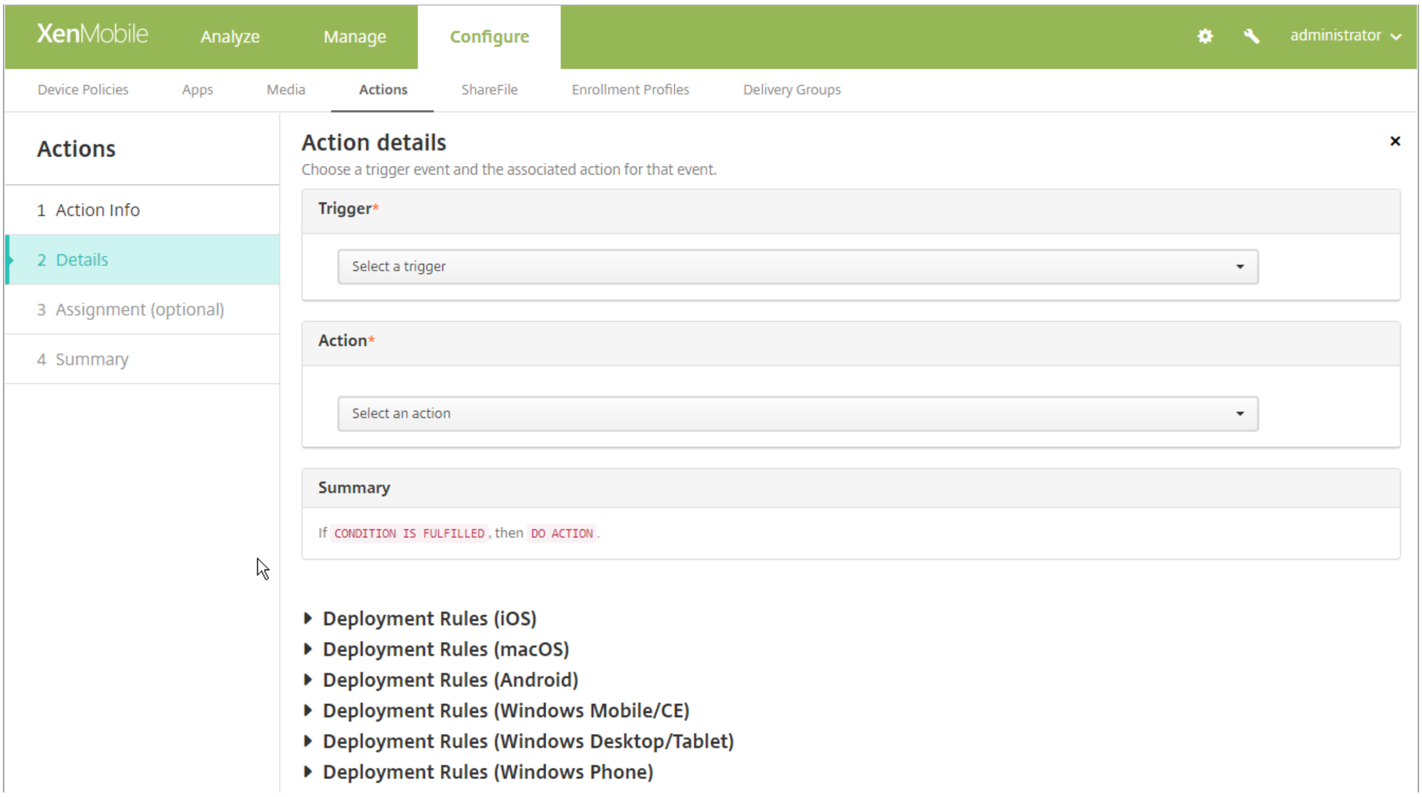
3. The **Action Information** page appears.

4. On the **Action Information** page, enter or modify the following information:

- **Name**: Type a name to uniquely identify the action. This field is required.
- **Description**: Describe what the action is meant to do.

5. Click **Next**. The **Action details** page appears.

Note: The following example shows how to set up an **Event** trigger. If you select a different trigger, the resulting options will be different from those shown here.



Choose a trigger event and the associated action for that event.

If CONDITION IS FULFILLED, then DO ACTION.

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 Device property names and values.
  - **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 To add an app inventory device policy.

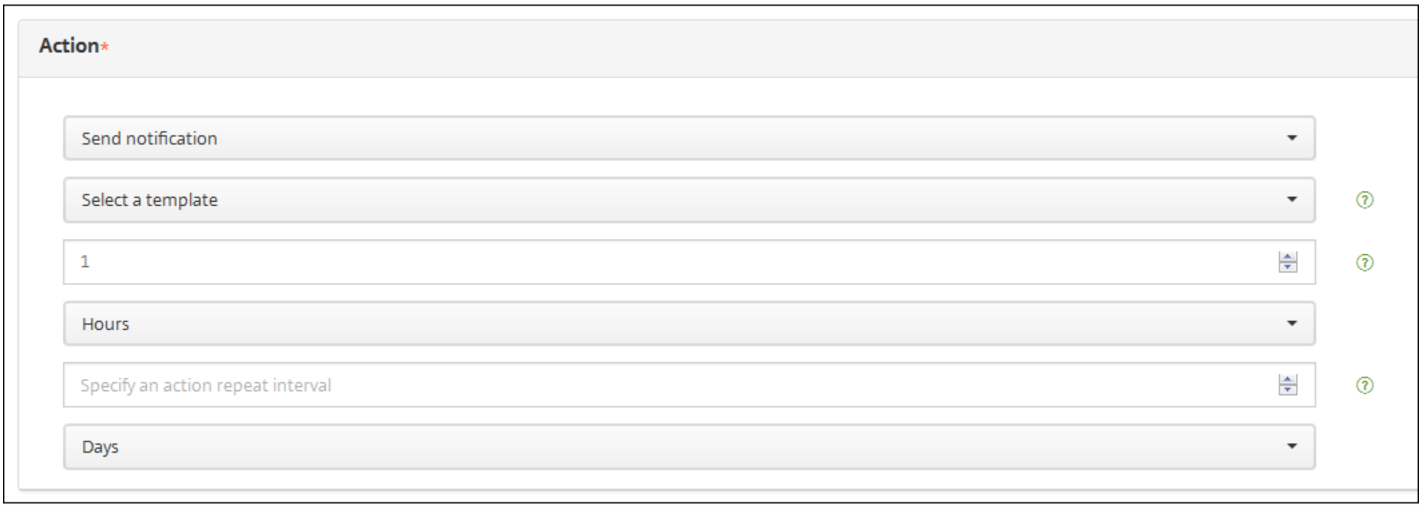
7. In the next list, click the response to the trigger.

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**, the remainder of this procedure explains how 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, unless a template doesn't yet exist for the notification type. In that case, you are prompted to configure a template with the message: No template for this event type. Create template using **Notification Template** in **Settings**.

Note: Before you can notify users, you must have configured notification servers in Settings for SMTP and SMS so that XenMobile can send the messages, see Notifications in XenMobile. Also, set up any notification templates you plan to use before proceeding. For details on setting up notification templates, see To create or update notification templates in XenMobile.



Action*

Send notification

Select a template

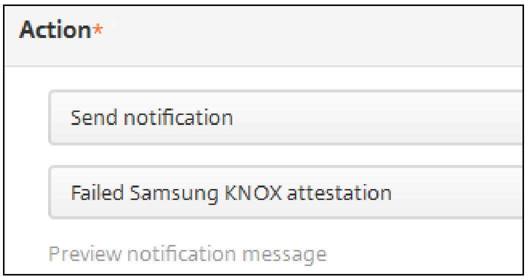
1

Hours

Specify an action repeat interval

Days

Note: After you select the template, you can preview the notification by clicking **Preview notification message**.



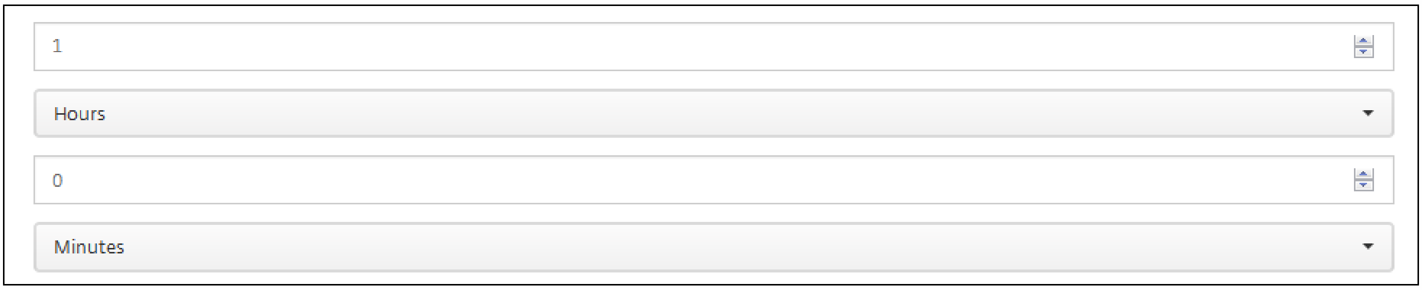
Action*

Send notification

Failed Samsung KNOX attestation

Preview notification message

10. In the following fields, set the delay in days, hours, or minutes before taking action and the interval at which the action repeats until the user addresses the triggering issue.



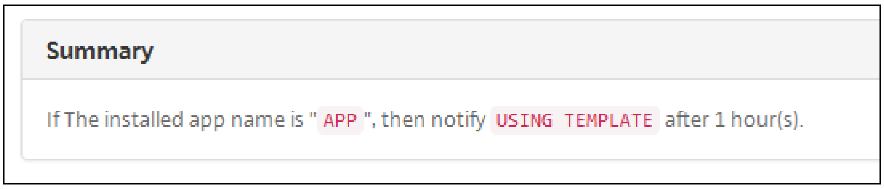
1

Hours

0

Minutes

11. In **Summary**, verify that you created the automated action as you intended.



Summary

If The installed app name is " APP ", then notify USING TEMPLATE after 1 hour(s).

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

- Expand Deployment Rules. The Base tab appears by default.
- In the lists, click options to determine when the action should be deployed.
  1. You can choose to deploy the action when all conditions are met or when any conditions are met. The default option is **All**.
  2. Click **New Rule** to define the conditions.
  3. In the lists, click the conditions, such as **Device ownership** and **BYOD**.
  4. Click **New Rule** again if you want to add more conditions. You can add as many conditions as you would like.
- Click the **Advanced** tab to combine the rules with Boolean options.
- The conditions you chose on the Base tab appear.
- You can use more advanced Boolean logic to combine, edit, or add rules.
  1. Click **AND**, **OR**, or **NOT**.
  2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
     At any time, you can click to select a condition and then click **EDIT** to change the condition or **Delete** to remove the condition.
  3. Click **New Rule** again if you want to add more conditions.
     In this example, the device ownership must be **BYOD**, the device local encryption must be **True**, the device must be passcode compliant, and the 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 a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand **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 need to be configured.
- 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.

Note: 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**, which does not apply to iOS.

17. Click **Next**. The **Summary** page appears, where you can verify the action configuration.

18. Click **Save** to save the action.

You can wipe or lock apps on a device in response to all four categories of triggers listed in the XenMobile console: event, device property, user property and installed app name.

To configure automatic app wipe or app lock

1. In the XenMobile 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.

5. In **Action**, select an action.

For this step, keep the following conditions in mind:

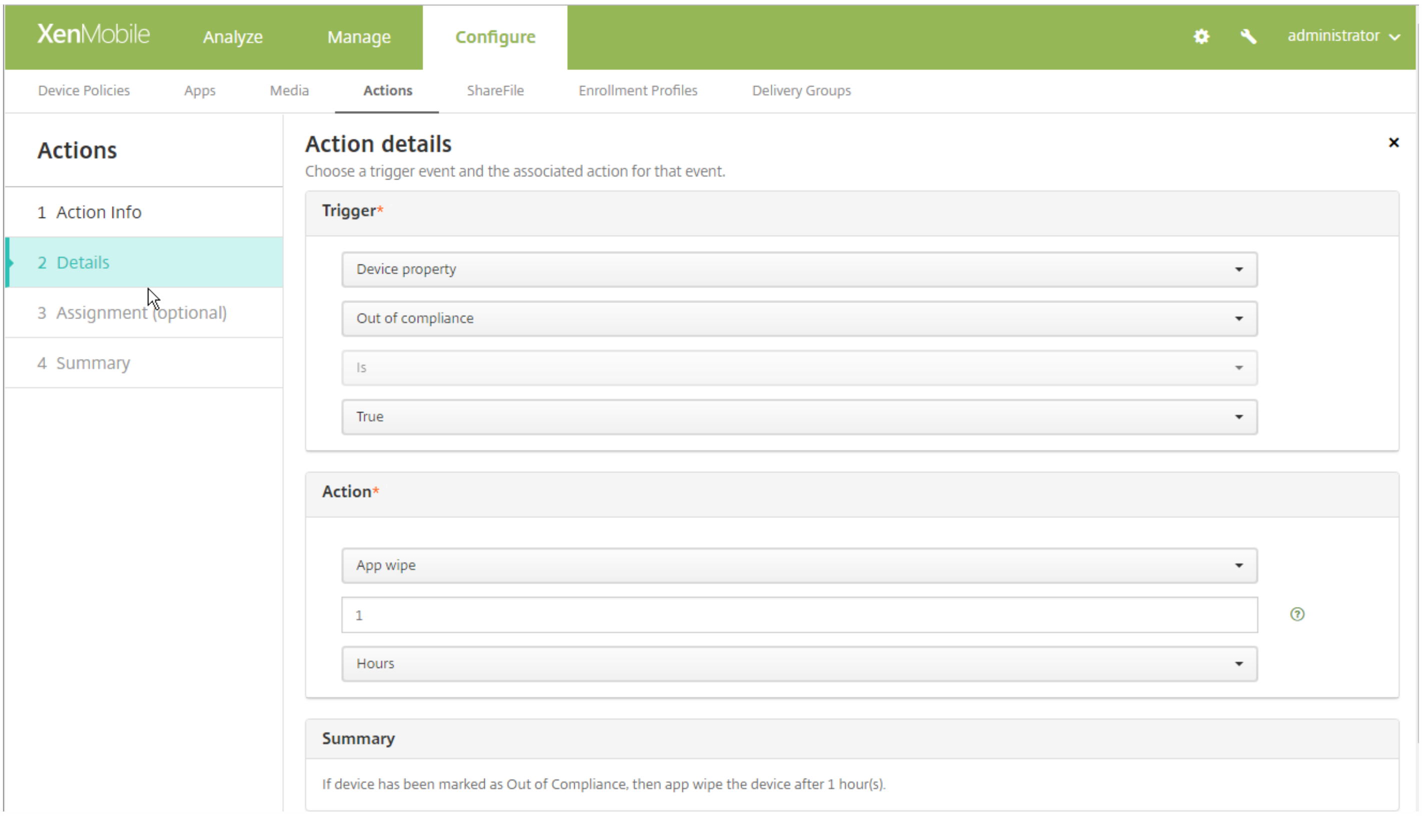
When the trigger type is **Event** and the value is not **Active Directory disabled user**, the **App wipe** and **App lock** actions will not appear.

When the trigger type is **Device property** and the value is **MDM lost mode enabled**, the following actions will not 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 delay gives users time to fix an issue if possible before the action is carried out. You can learn more about the App wipe and App lock actions in the topic on Configure roles with RBAC.

> ## 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 additional delay of approximately 1 hour may occur before any action is carried out, to allow the Active Directory database to synchronize with XenMobile.



Action details

Choose a trigger event and the associated action for that event.

Trigger*

Device property

Out of compliance

Is

True

Action*

App wipe

1

Hours

Summary

If device has been marked as Out of Compliance, then app wipe the device after 1 hour(s).

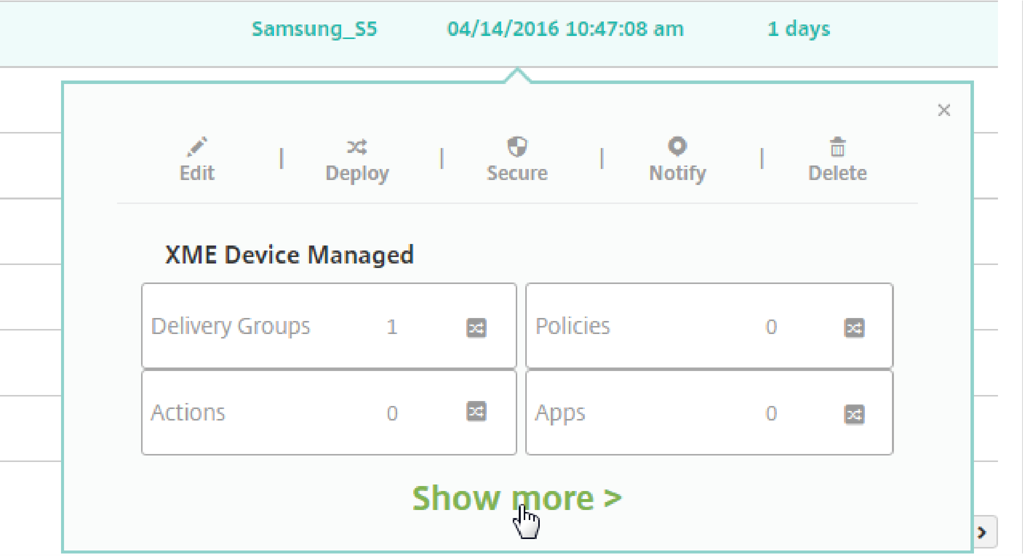
6. Configure deployment rules and then click **Next**.

7. Configure delivery group assignments and a deployment schedule and then click **Next**.

8. Click **Save**.

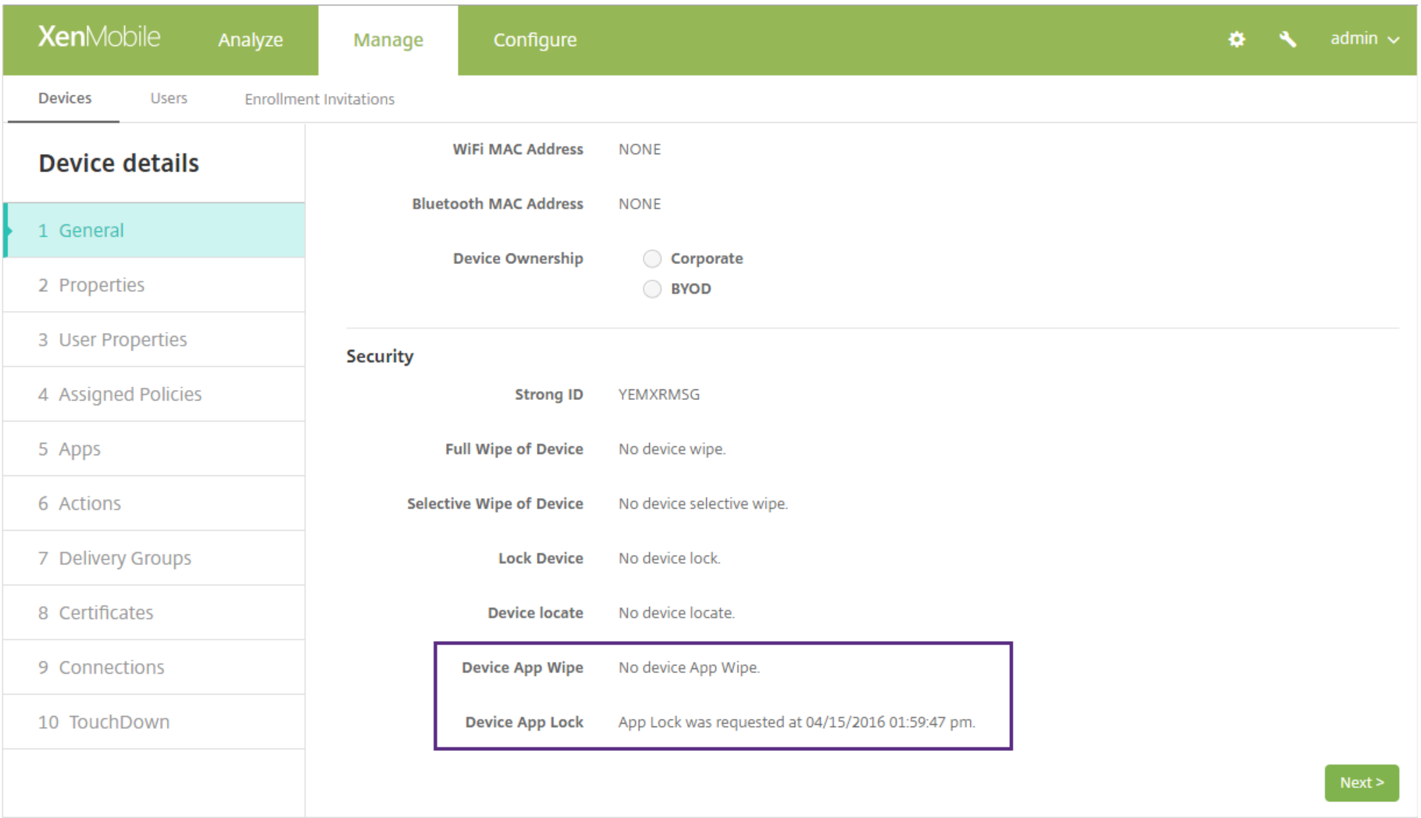
To check app lock or app wipe status

1. Go to **Manage > Devices**, click a device and then click **Show more**.



Delivery Groups	1	Policies	0
Actions	0	Apps	0

2. Scroll to **Device App Wipe** and **Device App Lock**.



Device details

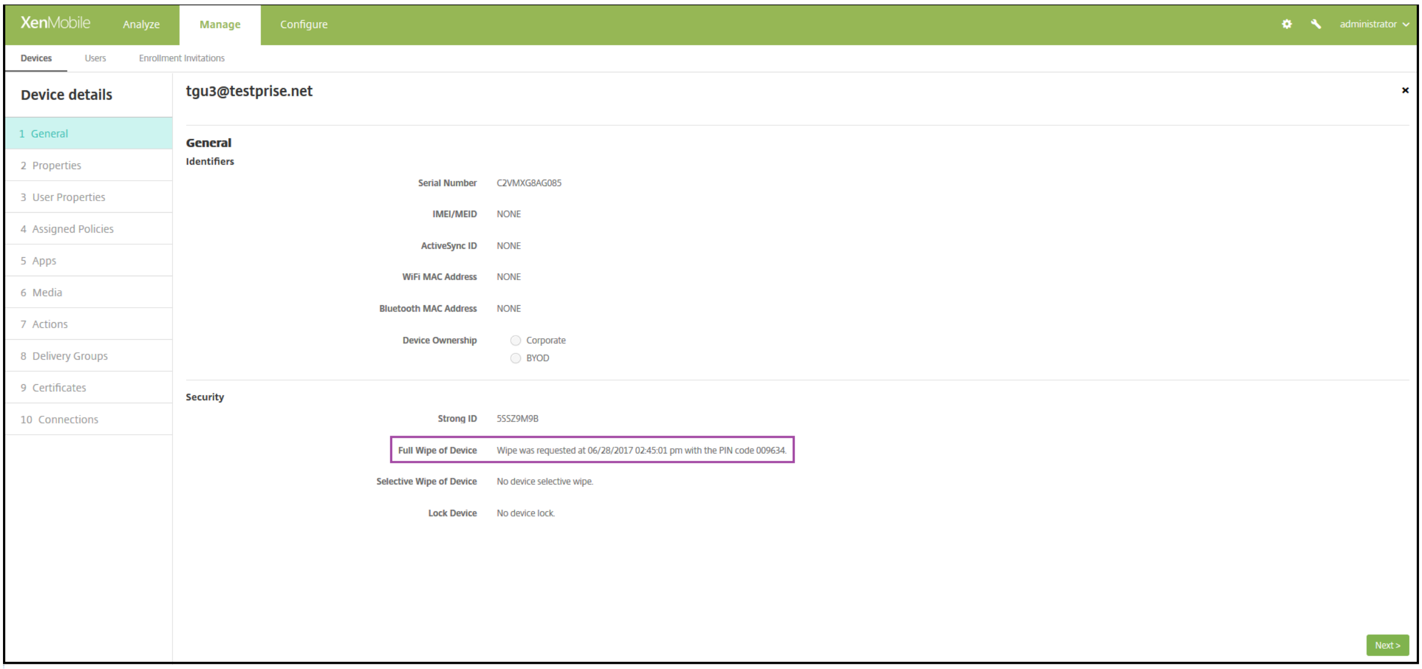
1 General
2 Properties
3 User Properties
4 Assigned Policies
5 Apps
6 Actions
7 Delivery Groups
8 Certificates
9 Connections
10 TouchDown

WiFi MAC Address	NONE
Bluetooth MAC Address	NONE
Device Ownership	○ Corporate ○ BYOD

Security

Strong ID	YEMXRMSG
Full Wipe of Device	No device wipe.
Selective Wipe of Device	No device selective wipe.
Lock Device	No device lock.
Device locate	No device locate.
Device App Wipe	No device App Wipe.
Device App Lock	App Lock was requested at 04/15/2016 01:59:47 pm.

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.



Device details

1 General
2 Properties
3 User Properties
4 Assigned Policies
5 Apps
6 Media
7 Actions
8 Delivery Groups
9 Certificates
10 Connections

tgu3@testprise.net

General

Identifiers

Serial Number	C2VMXG8AG085
IMEI/MEID	NONE
ActiveSync ID	NONE
WiFi MAC Address	NONE
Bluetooth MAC Address	NONE
Device Ownership	○ Corporate ○ BYOD

Security

Strong ID	5SSZ9M9B
Full Wipe of Device	Wipe was requested at 06/28/2017 02:45:01 pm with the PIN code 009634.
Selective Wipe of Device	No device selective wipe.
Lock Device	No device lock.

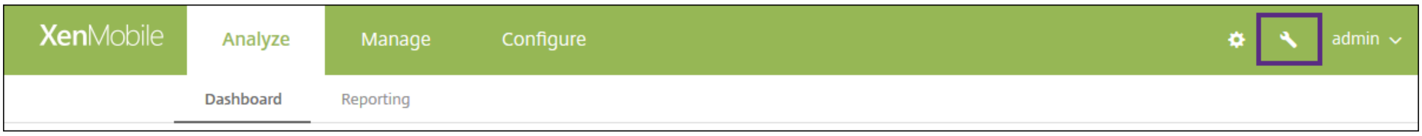
Monitor and support

Oct 25, 2017

You can use the XenMobile Dashboard and the XenMobile Support page to monitor and troubleshoot your XenMobile Server. Use the XenMobile Support page to access support-related information and tools.

For an on-premises XenMobile Server, you can also perform actions from the XenMobile CLI. For details, see Command-line interface options.

In the XenMobile console, click the wrench icon in the upper-right corner.

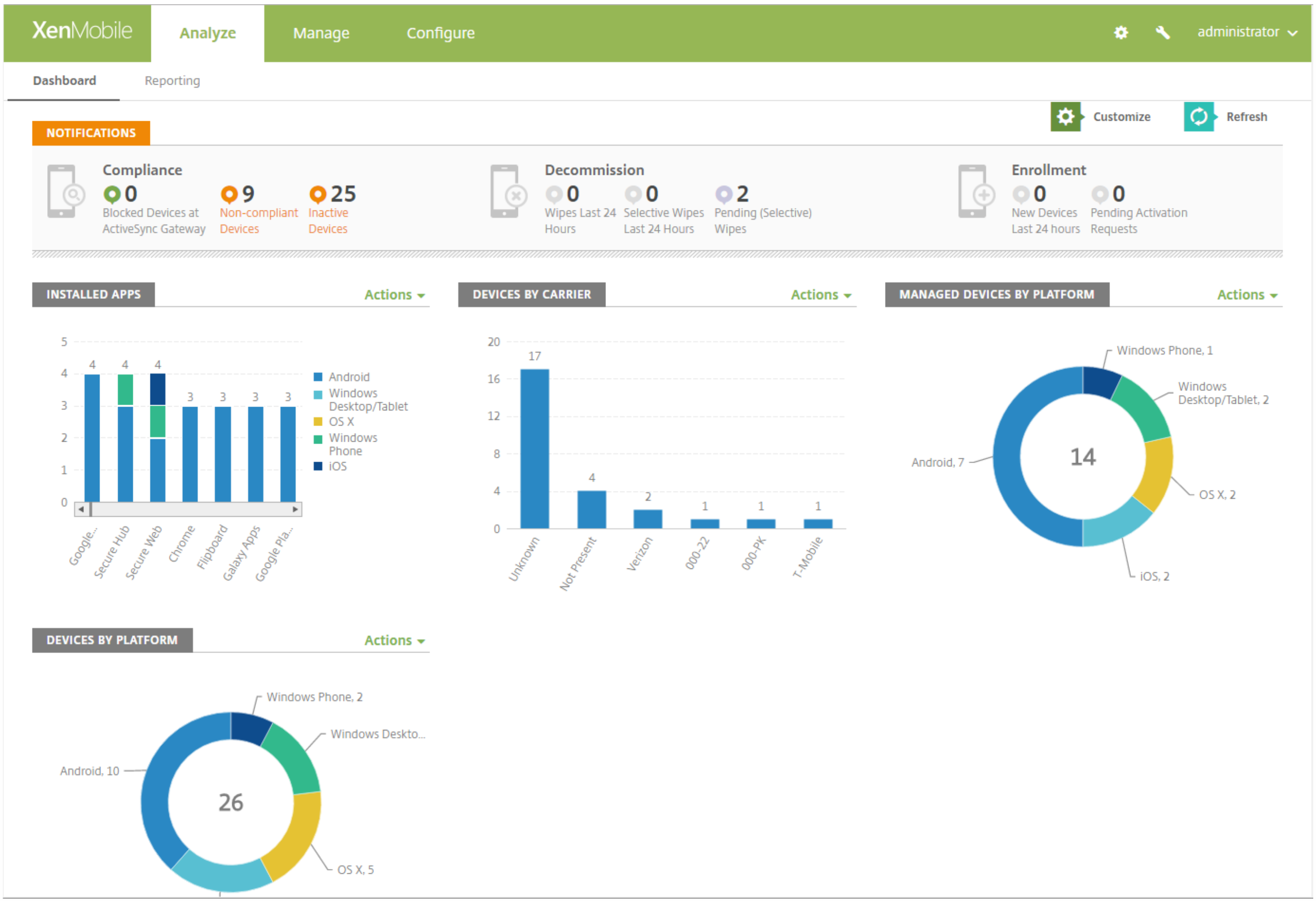


The Troubleshooting and Support page appears.

Use the XenMobile **Support** page to:

- Access diagnostics.
- Create support bundles (on-premises installations only).
- 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 XenMobile console dashboard. With this information, you can see issues and successes quickly by using widgets.

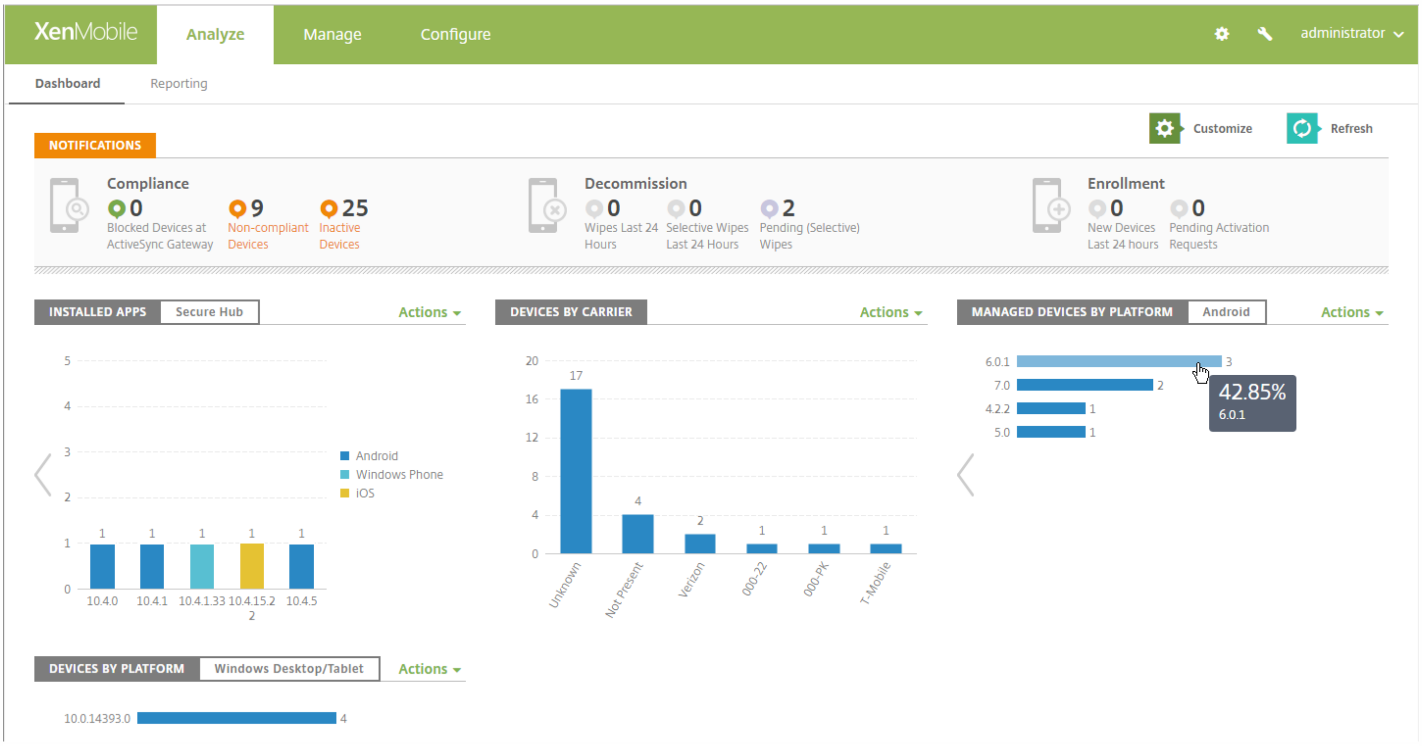


The dashboard is usually the page that first appears when you sign on to the XenMobile console. To access the dashboard from elsewhere in the console, click **Analyze**. Click **Customize** on the dashboard to edit the layout of the page and to edit the widgets that appear.

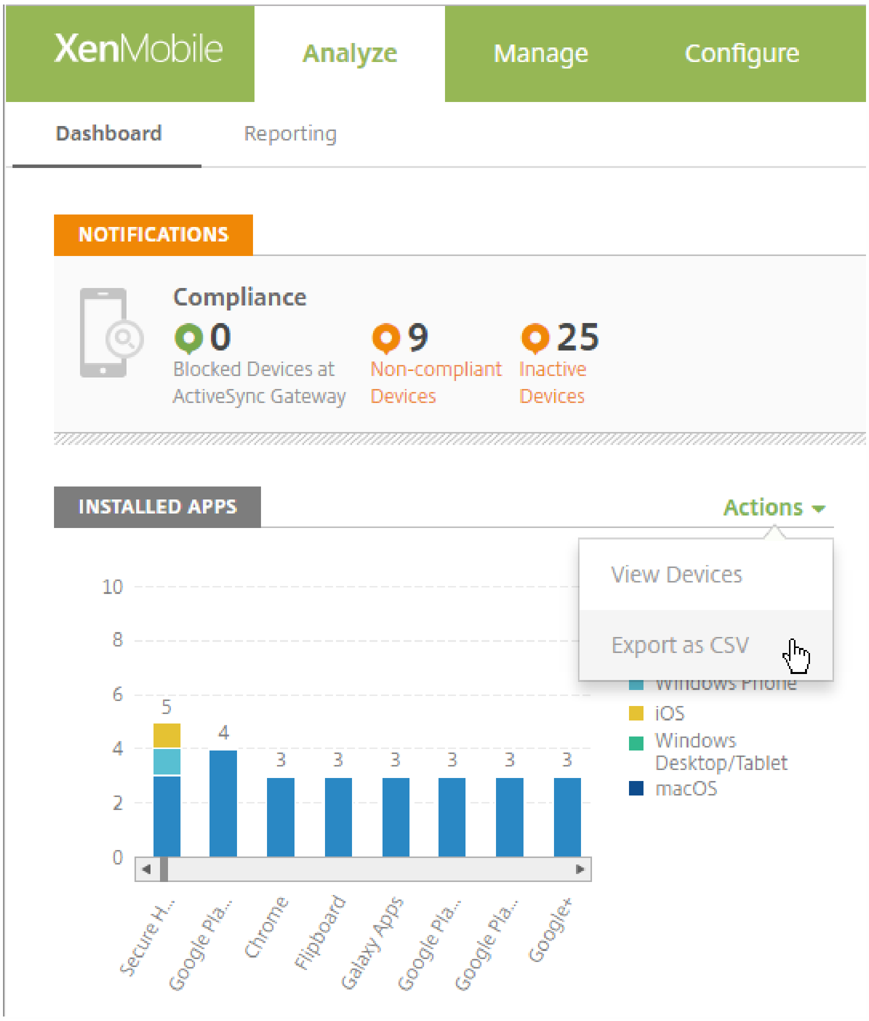
- **My Dashboards**: You can save up to four dashboards. You can edit these dashboards separately and view each one by selecting the saved dashboard.
- **Layout Style**: In this row, you can select how many widgets appear on your dashboard and how the widgets are laid out.
- **Widget Selection**: You 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 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.
  - **Android TouchDown License Status**: Displays the number of devices that have a TouchDown license.

- **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.
- **VPP Apps License Usage**: Displays license usage statistics for Apple Volume Purchase Program 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.


XenMobile
Analyze
Manage
Configure
Dashboard
Reporting
NOTIFICATIONS
Compliance
0
Blocked Devices at ActiveSync Gateway
9
Non-compliant Devices
25
Inactive Devices
INSTALLED APPS
Actions
View Devices
Export as CSV
Windows Phone
iOS
Windows Desktop/Tablet
macOS
10
8
6
4
2
0
5
4
3
3
3
3
3
3
Secure H...
Google Pla...
Chrome
Flipboard
Galaxy Apps
Google Pla...
Google Pla...
Google+

Reports

Oct 24, 2017

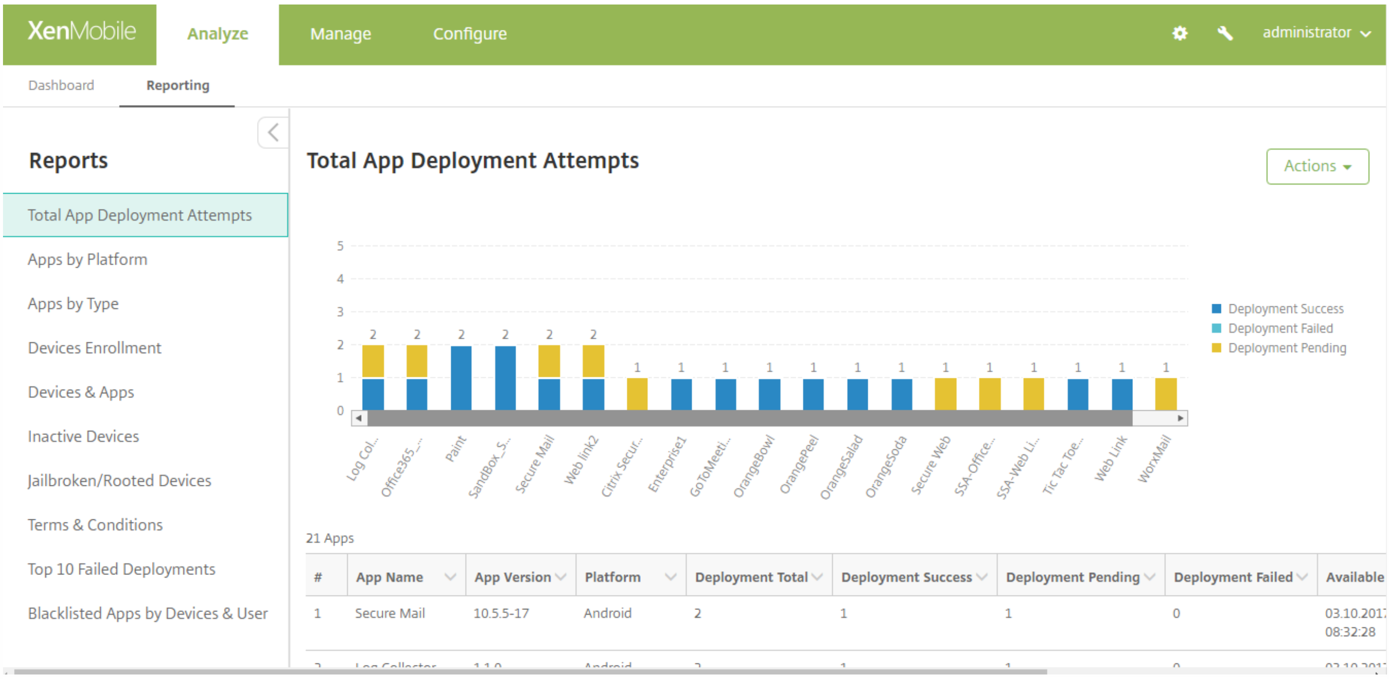
XenMobile provides the following pre-defined reports that let you analyze your app and device deployments. Each report appears as a table and a chart. You can sort and filter the tables by column. You can select elements in charts from more detailed information.

- **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 XenMobile 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 XenMobile console, click **Analyze > Reporting**. The **Reporting** page appears.
2. Click the report you want to generate.

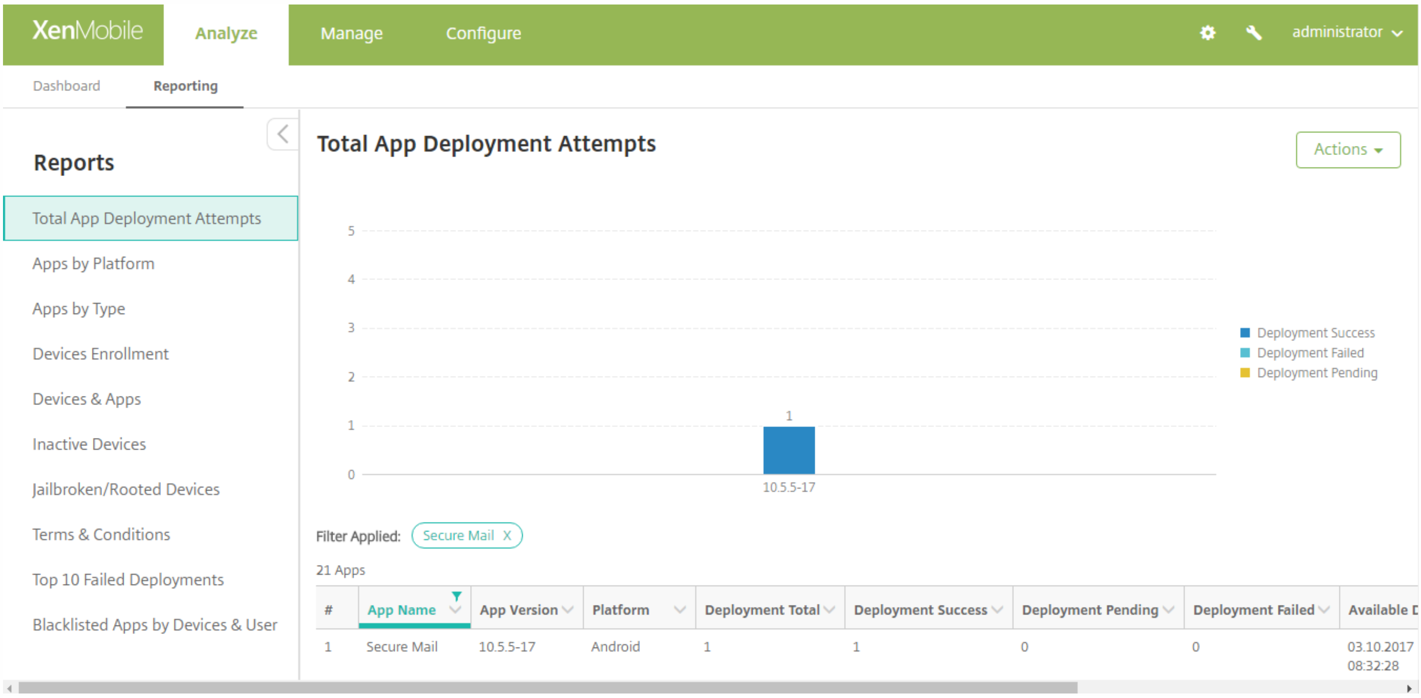


21 Apps

#	App Name	App Version	Platform	Deployment Total	Deployment Success	Deployment Pending	Deployment Failed	Available
1	Secure Mail	10.5.5-17	Android	2	1	1	0	03.10.201 08:32:28
2	Log Collector	1.1.0	Android	2	1	1	0	03.10.201

To view more details of a report:

- Click areas of the chart to drill down and see more details information.

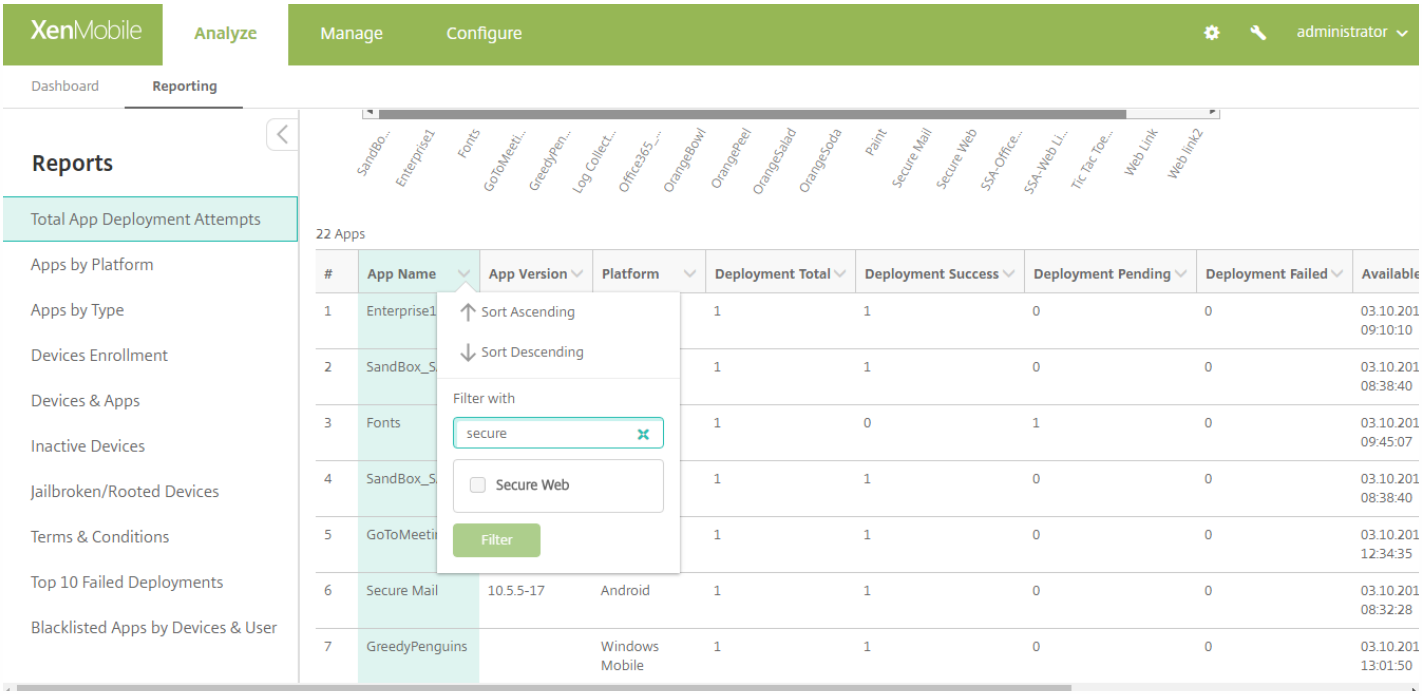


Filter Applied: Secure Mail X

21 Apps

#	App Name	App Version	Platform	Deployment Total	Deployment Success	Deployment Pending	Deployment Failed	Available D
1	Secure Mail	10.5.5-17	Android	1	1	0	0	03.10.2017 08:32:28

- To sort, filter, or search a table column, click the column heading.



Reports

- Total App Deployment Attempts
- Apps by Platform
- Apps by Type
- Devices Enrollment
- Devices & Apps
- Inactive Devices
- Jailbroken/Rooted Devices
- Terms & Conditions
- Top 10 Failed Deployments
- Blacklisted Apps by Devices & User

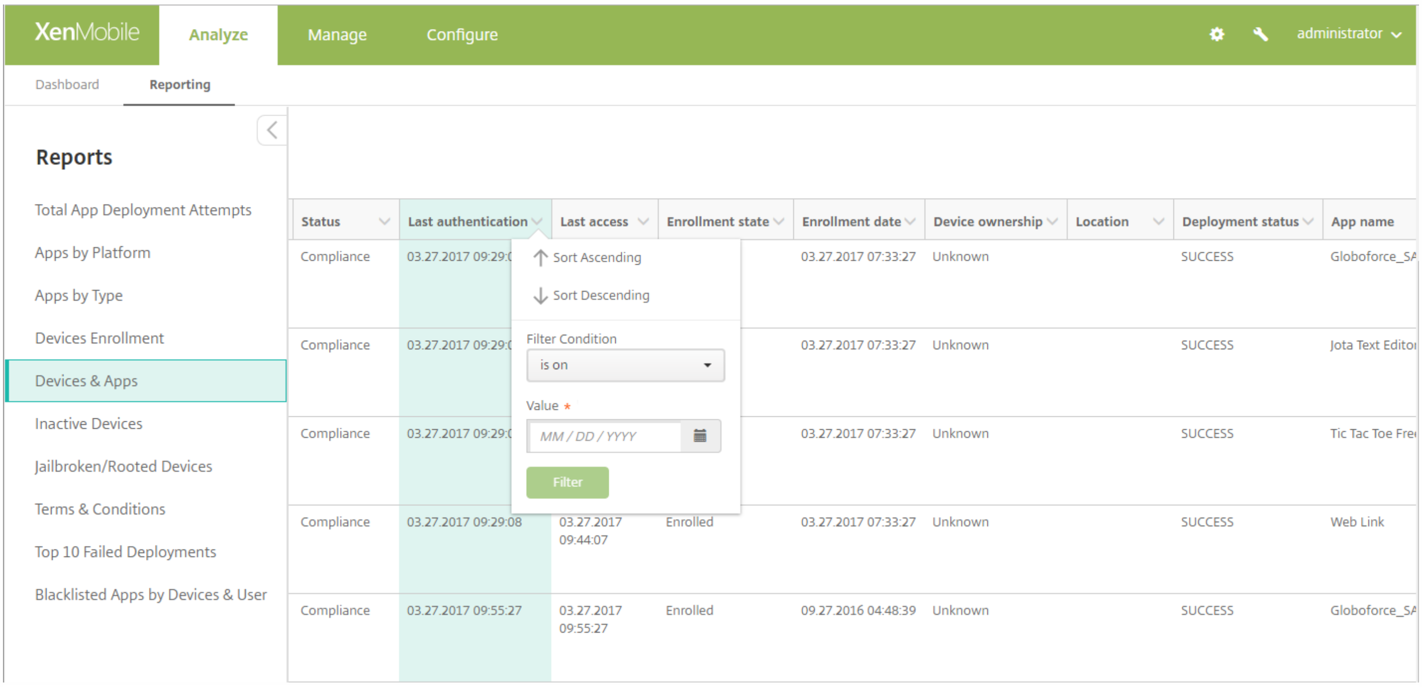
22 Apps

#	App Name	App Version	Platform	Deployment Total	Deployment Success	Deployment Pending	Deployment Failed	Available
1	Enterprise1			1	1	0	0	03.10.201 09:10:10
2	SandBox_S			1	1	0	0	03.10.201 08:38:40
3	Fonts			1	0	1	0	03.10.201 09:45:07
4	SandBox_S			1	1	0	0	03.10.201 08:38:40
5	GoToMeeti			1	1	0	0	03.10.201 12:34:35
6	Secure Mail	10.5.5-17	Android	1	1	0	0	03.10.201 08:32:28
7	GreedyPenguins		Windows Mobile	1	1	0	0	03.10.201 13:01:50

Sort Ascending
Sort Descending
Filter with
secure
□ Secure Web
Filter

- To filter the report by date:

  Click a column heading to view the filter settings.



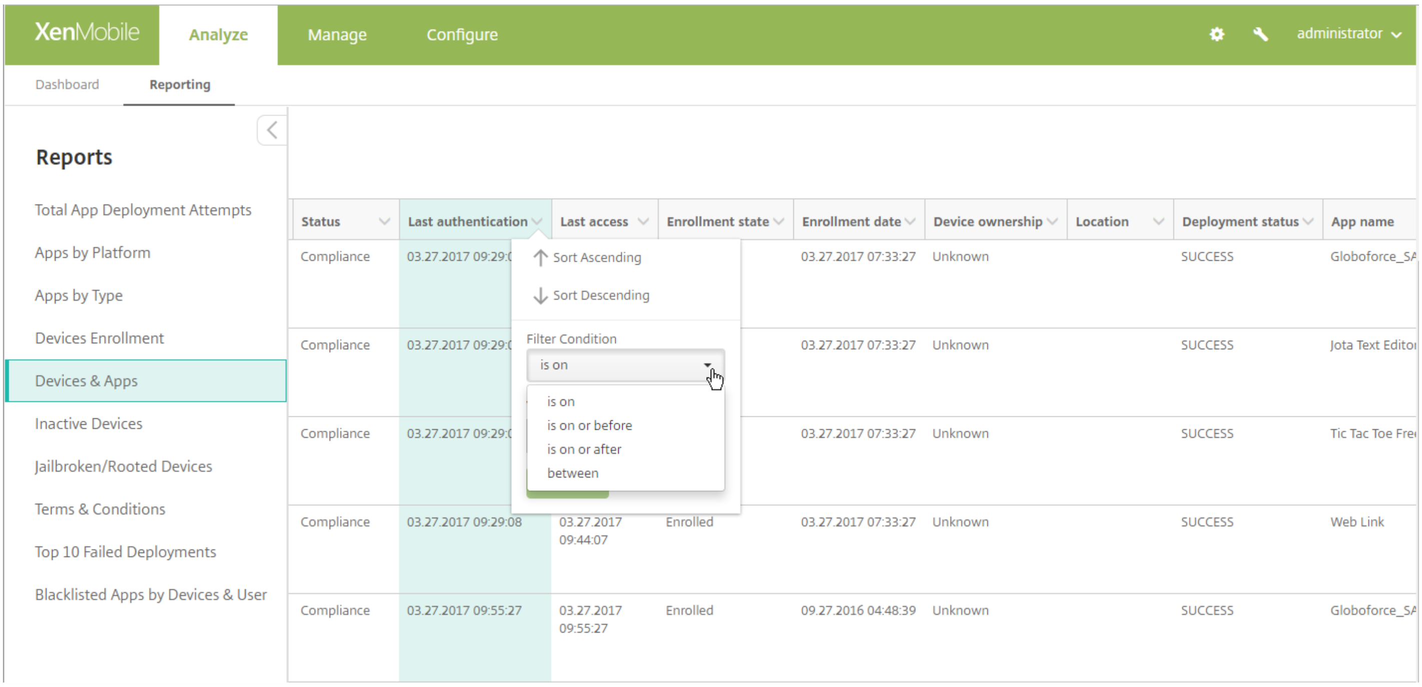
Reports

- Total App Deployment Attempts
- Apps by Platform
- Apps by Type
- Devices Enrollment
- Devices & Apps
- Inactive Devices
- Jailbroken/Rooted Devices
- Terms & Conditions
- Top 10 Failed Deployments
- Blacklisted Apps by Devices & User

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_SA
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Editor
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Free
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_SA

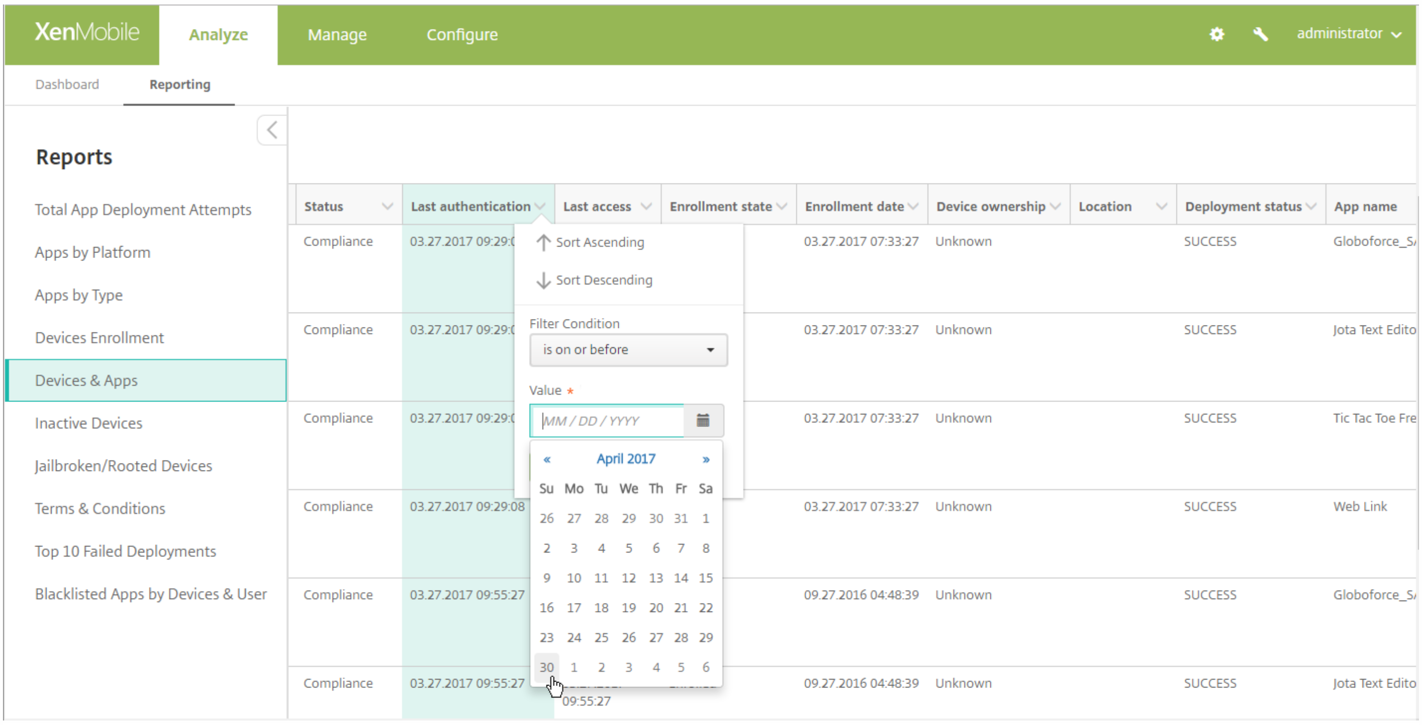
Sort Ascending
Sort Descending
Filter Condition
is on
Value *
MM / DD / YYYY
Filter

From **Filter Condition**, choose how you want to restrict the dates reported.



Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_SA
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Editor
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Free
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_SA

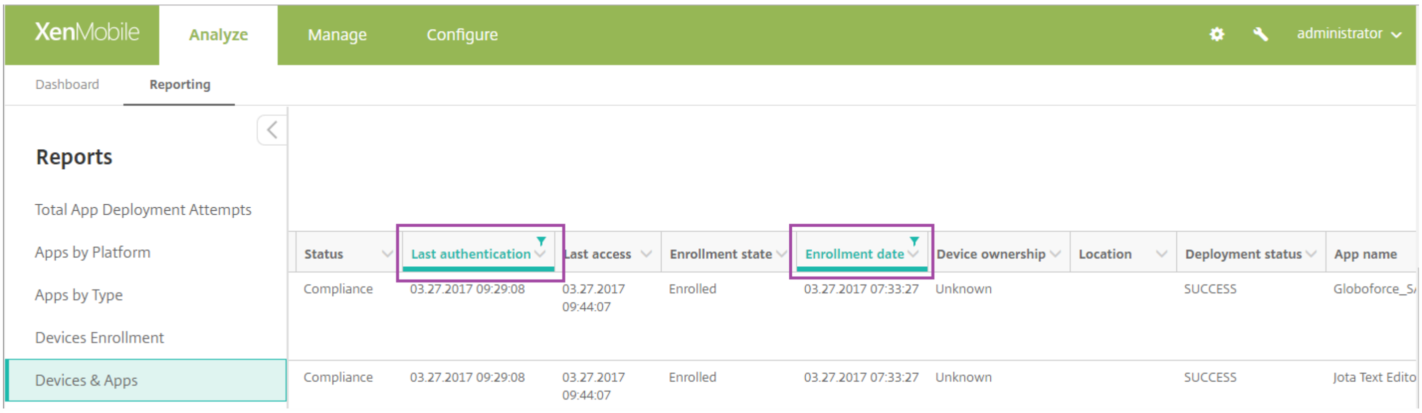
Use the date chooser to specify dates.



Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

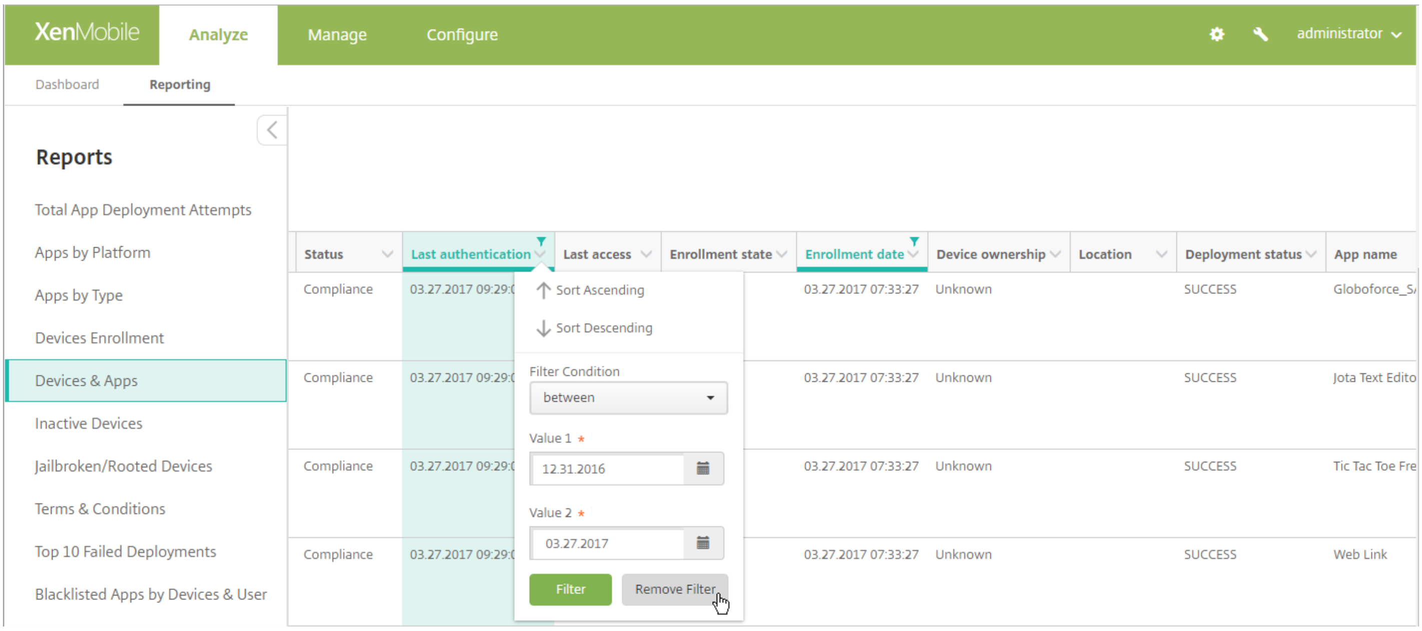
Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S/
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edito
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08			03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27			09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_S/
Compliance	03.27.2017 09:55:27	09:55:27		09.27.2016 04:48:39	Unknown		SUCCESS	Jota Text Edito

A column with a date filter displays as shown the following example.



Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S/
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edito

To remove a filter, click the column heading and then click **Remove Filter**.



Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S/
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edito
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:(			03.27.2017 07:33:27	Unknown		SUCCESS	Web Link

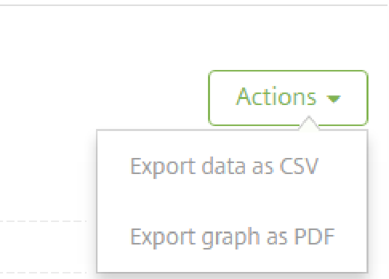
Filter Condition: between

Value 1 * 12.31.2016

Value 2 * 03.27.2017

To export a chart or table:

- To export the chart in PDF format, click **Action** > **Export graph as PDF**.
- To export the table data in CSV format, click **Action** > **Export data as CVS**.



Important

Although it is possible to use SQL Server to create custom reports, Citrix does not recommend this method. Citrix doesn't publish the schema and can change the schema without notification. If you do decide to pursue this method of reporting, ensure that SQL queries are run using a read-only account. Be aware that a query with multiple JOINs that takes some time to run will impact XenMobile Server performance during that time.

Mobile Service Provider

Sep 06, 2017

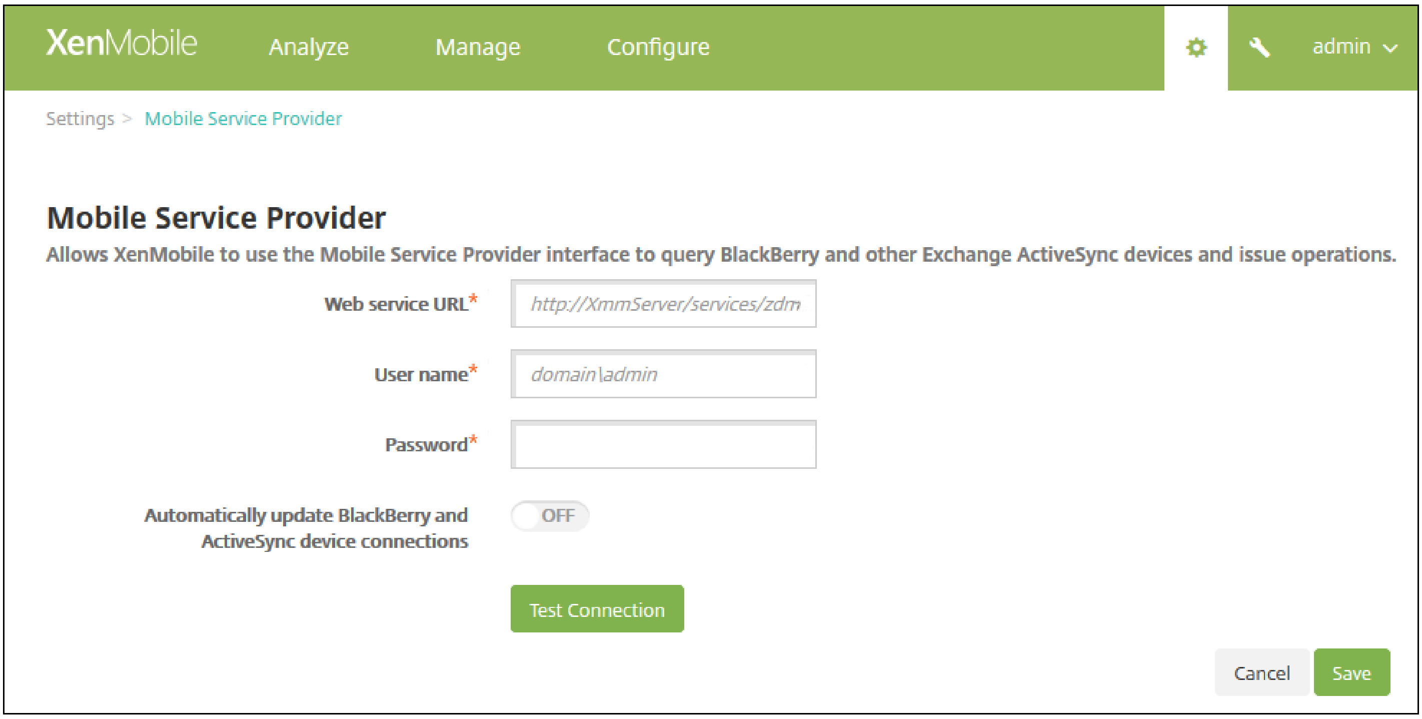
You can enable XenMobile to use the Mobile Service Provider interface to query BlackBerry and Exchange ActiveSync devices and issue operations.

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 XenMobile for management, the XenMobile 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 XenMobile 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.



Mobile Service Provider

Allows XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.

Web service URL*: http://XmmServer/services/zdm

User name*: domain\admin

Password*:

Automatically update BlackBerry and ActiveSync device connections: OFF

3. Configure these settings:

- **Web service URL**: Type the URL of the Web service; for example, http://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**.

SysLog

Sep 06, 2017

You can configure XenMobile Server (on-premises only) to send log files to a systems log (syslog) server. You need the server host name or IP address.

Syslog is a standard logging protocol with two components: an auditing module (which runs on the appliance) and a server, which can run on a remote system. The Syslog protocol uses the user data protocol (UDP) for data transfer. Admin events and User events are recorded.

You can configure the server to collect the following types of information:

- System logs that contain a record of actions taken by XenMobile.
- Audit logs that contain a chronological record of system activities for XenMobile.

The log information that a syslog server collects from an appliance is stored in a log file in the form of messages. These messages typically contain the following information:

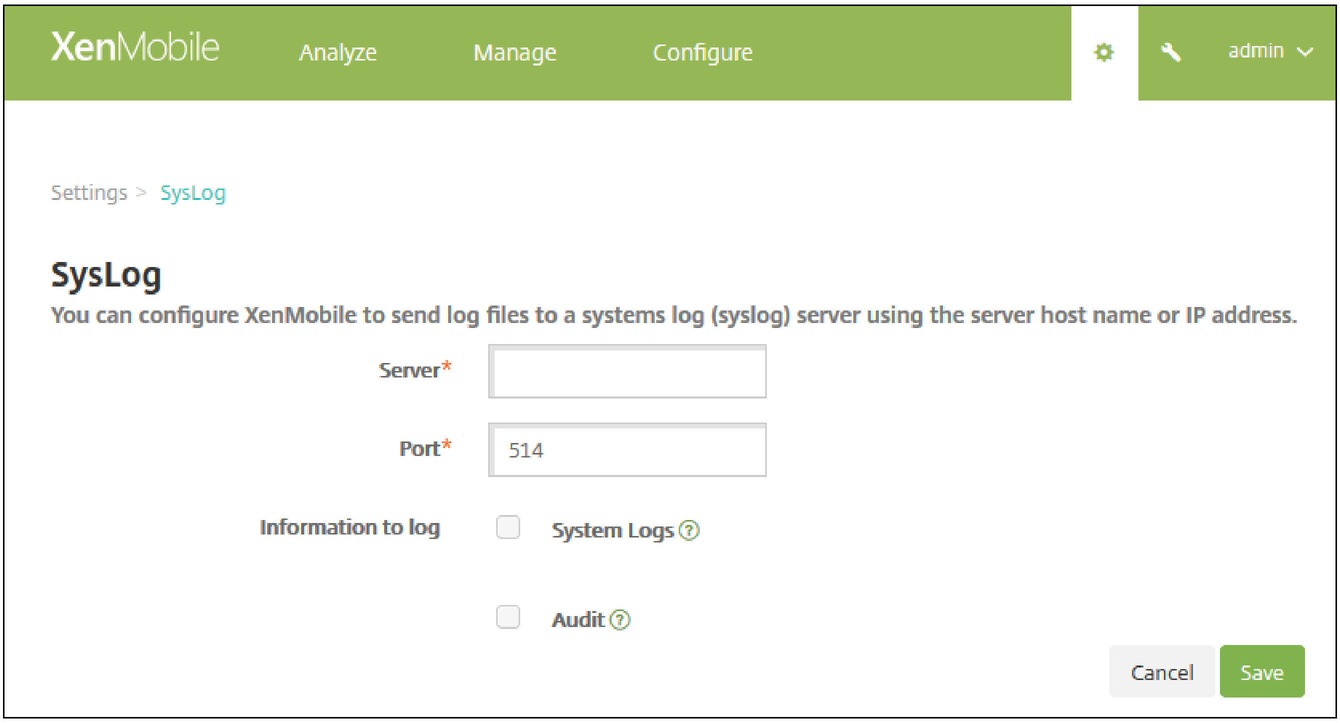
- The IP address of the appliance that generated the log message
- A time stamp
- The message type
- The log level associated with an event (Critical, Error, Notice, Warning, Informational, Debug, Alert, or Emergency)
- The message information

You can use this information to analyze the source of the alert and take corrective action if necessary.

> ## Note
>
> In XenMobile Service (cloud) deployments, Citrix does not support syslog integration with an on-premises syslog server. Instead, you can download the logs from the Support page in the XenMobile console. When doing so, you must click **Download All** to get system logs. For details, see View and analyze log files in XenMobile.

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

2. Click **Syslog**. The **Syslog** page appears.



Settings > SysLog

SysLog

You can configure XenMobile to send log files to a systems log (syslog) server using the server host name or IP address.

Server*

Port* 514

Information to log □ System Logs

□ Audit

3. Configure these settings:

- **Server**: Type either the IP address or the fully qualified domain name (FQDN) of your syslog server.
- **Port**: Type the port number. By default, the port is set to 514.
- **Information to log:** Select or clear **System Logs** and **Audit**.
  - System logs contain actions taken by XenMobile.
  - Audit logs contain a chronological record of system activities for XenMobile.

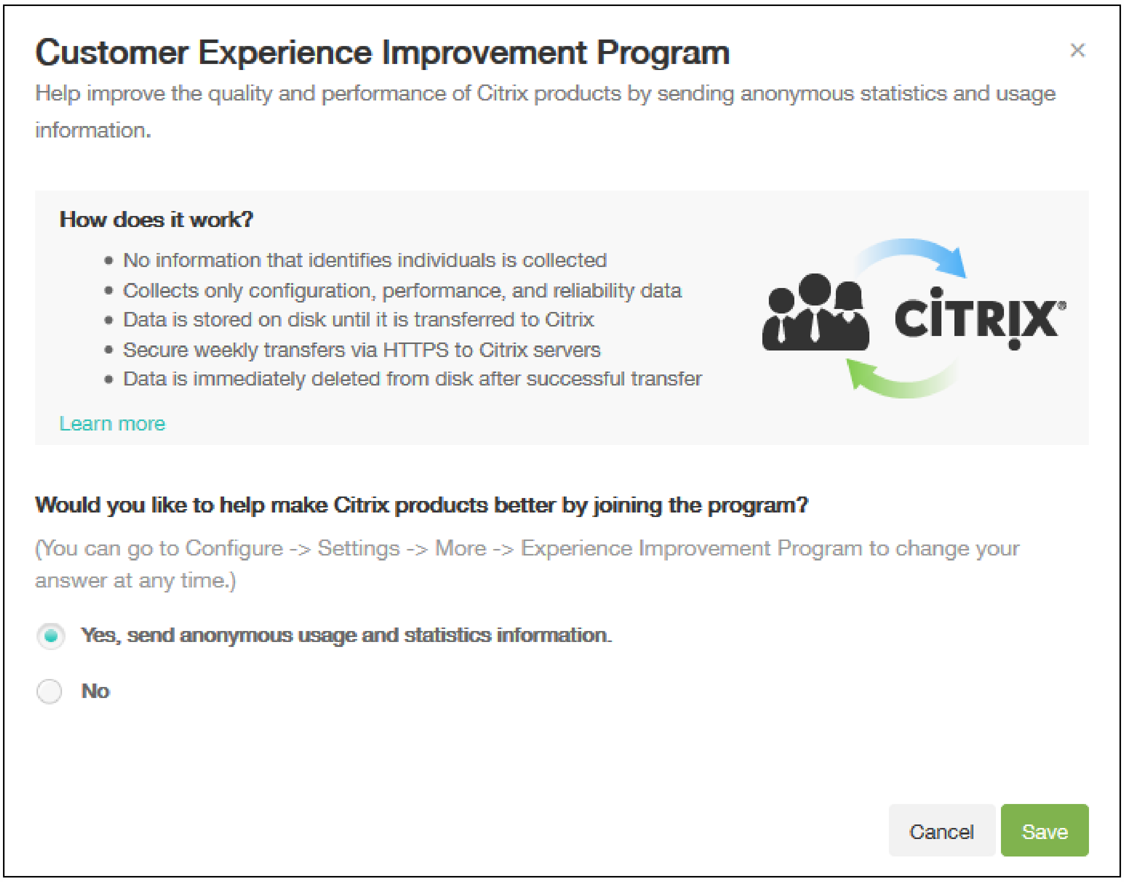
4. Click **Save**.

Customer Experience Improvement Program

Sep 06, 2017

The Citrix Customer Experience Improvement Program (CEIP) gathers anonymous configuration and usage data from XenMobile and automatically sends the data to Citrix. This data helps Citrix improve the quality, reliability, and performance of XenMobile. Participation in the CEIP is completely voluntary. When you first install XenMobile, or when you install an update, you have the option to participate in the CEIP. When you opt-in, data is typically collected on a weekly basis, and performance and usage data is collected hourly. The data is stored on disk and transferred securely via HTTPS to Citrix weekly. You can change whether you participate in the CEIP in the XenMobile console. For more information on the CEIP, see About the Citrix Customer Experience Improvement Program (CEIP).

The first time you install XenMobile or when you do an update, you see the following dialog box that prompts you to participate.



Customer Experience Improvement Program

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer

Learn more

Would you like to help make Citrix products better by joining the program?

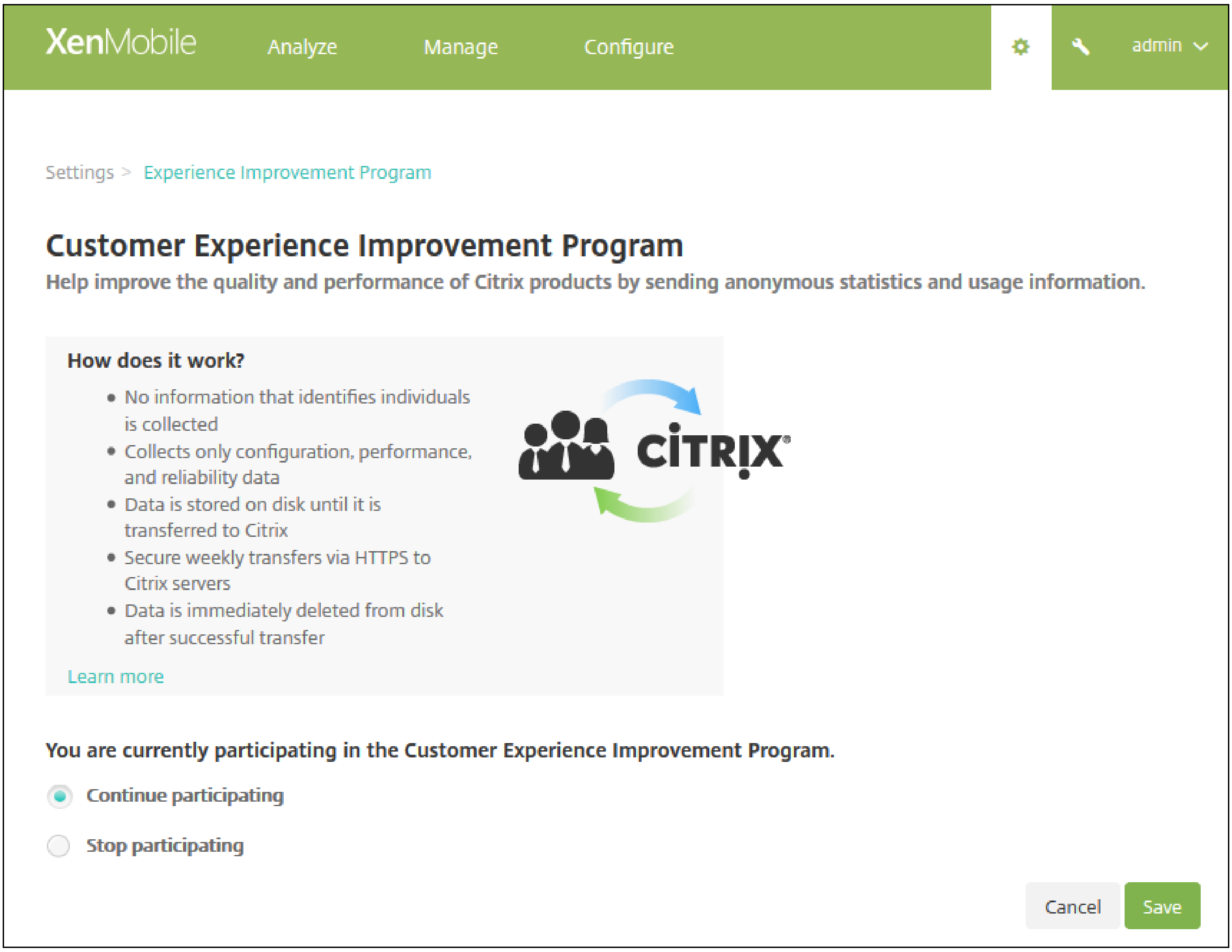
(You can go to Configure -> Settings -> More -> Experience Improvement Program to change your answer at any time.)

● Yes, send anonymous usage and statistics information.

○ No

1. To change your CEIP participation setting, in the XenMobile console, click the gear icon in the upper-right corner of the console to open the **Settings** page.

2. Under **Server**, click **Experience Improvement Program**. The **Customer Experience Improvement Program** page appears. The exact page you see depends on whether you are currently participating in the CEIP.



Settings > Experience Improvement Program

Customer Experience Improvement Program

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer

Learn more

You are currently participating in the Customer Experience Improvement Program.

● Continue participating

○ Stop participating

3. If you are currently participating in the CEIP and want to stop, click **Stop participating**.

4. If you are not currently participating in the CEIP and want to start, click **Start participating**.

5. Click **Save**.

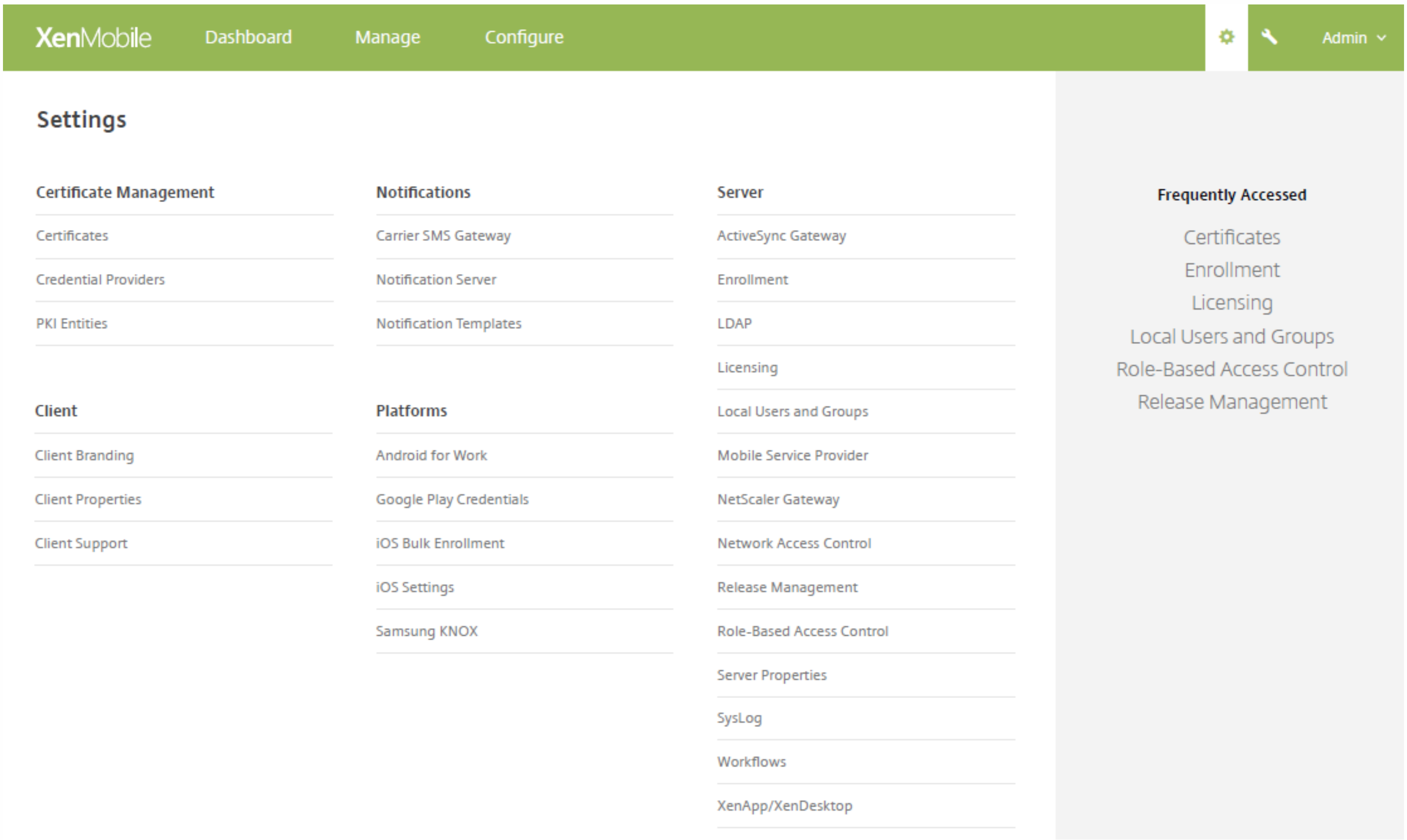
Support options and Remote Support

Nov 29, 2017

You can provide an email address for users to contact support staff. When users request assistance from their devices, they see the email address.

You can also configure how users send logs to the help desk from their devices. You can configure the logs to be sent directly or by email.

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



2. Under **Client**, click **Client Support**. The **Client Support** page appears.

3. Configure the following settings:

- **Support email (IT help desk)**: Type the email address for your IT help desk contact.
- **Send device logs to IT help desk**: Select whether device logs are sent **directly** or **by email**. The default is **by email**.
  - When you enable **directly**, settings for Store logs on ShareFile appear. If you enable Store logs on ShareFile, logs are sent directly to ShareFile. Otherwise, the logs are sent to XenMobile and then emailed to the help desk. In addition, the **If sending directly fails, use email** option appears, which is enabled by default. You can disable this option when you do not want to use the client email to send the logs for a server problem. When, however, you disable this option and a server problem occurs, the logs are not sent.
  - When you enable **by email**, the client email is always used to send the logs.

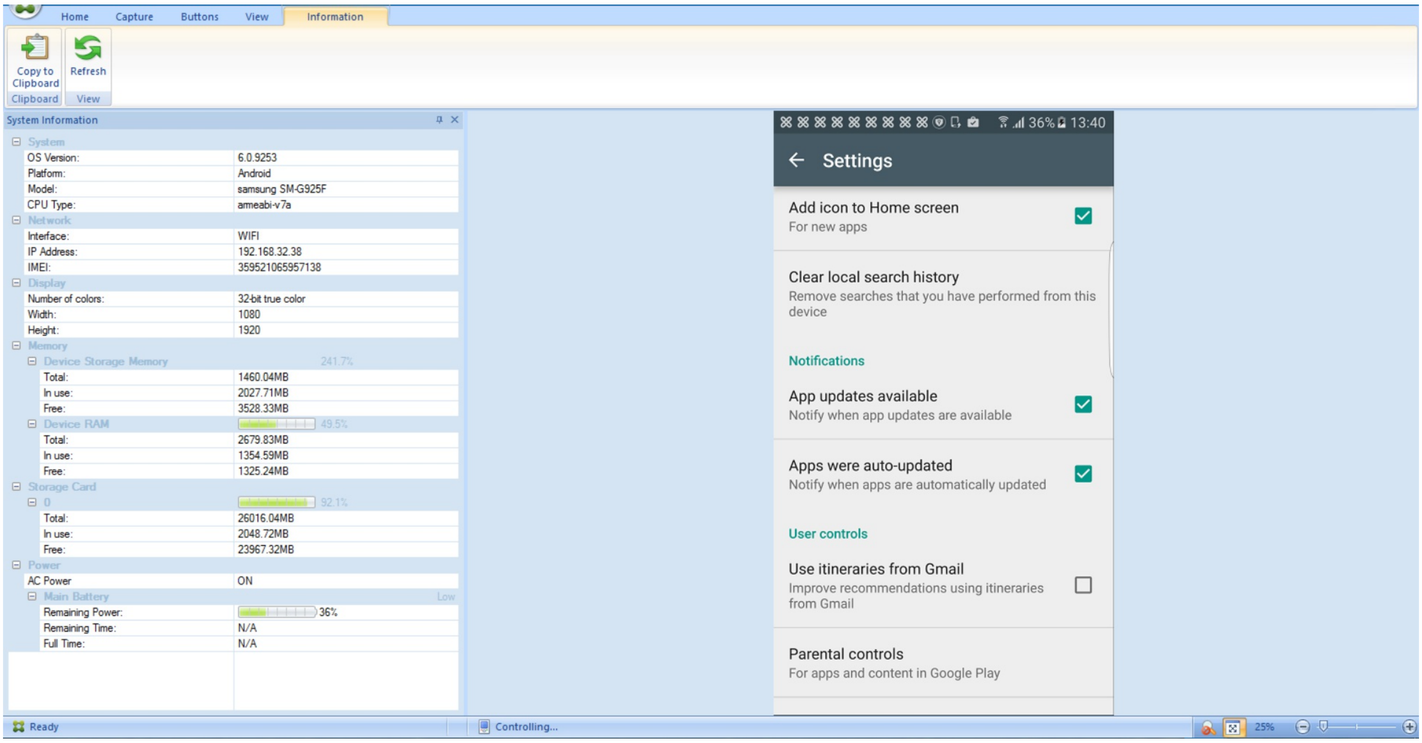
4. Click **Save**.

For on-premises XenMobile Server deployments: Remote support enables your help desk representatives to take remote control of managed Windows CE and Android mobile devices. Screen cast is supported on Samsung KNOX devices only.

Remote support isn't available to XenMobile Service customers and isn't supported for clustered on-premises XenMobile Server deployments.

During a remote control session:

- Users see on their mobile device an icon indicating a remote control session is active.
- Remote Support users see the Remote Support application window and a Remote Control window that shows a rendering of the controlled device.



System Information

System	
OS Version:	6.0.9253
Platform:	Android
Model:	samsung SM-G925F
CPU Type:	armeabi-v7a
Network	
Interface:	WIFI
IP Address:	192.168.32.38
IMEI:	359521065957138
Display	
Number of colors:	32-bit true color
Width:	1080
Height:	1920
Memory	
Device Storage Memory	241.7%
Total:	1460.04MB
In use:	2027.71MB
Free:	3528.33MB
Device RAM	49.5%
Total:	2679.83MB
In use:	1354.59MB
Free:	1325.24MB
Storage Card	
0	92.1%
Total:	26016.04MB
In use:	2048.72MB
Free:	23967.32MB
Power	
AC Power	ON
Main Battery	Low
Remaining Power:	36%
Remaining Time:	N/A
Full Time:	N/A

36% 13:40

Settings

Add icon to Home screen ☑
For new apps

Clear local search history
Remove searches that you have performed from this device

Notifications

App updates available ☑
Notify when app updates are available

Apps were auto-updated ☑
Notify when apps are automatically updated

User controls

Use itineraries from Gmail □
Improve recommendations using itineraries from Gmail

Parental controls
For apps and content in Google Play

By using Remote Support, you can do the following:

- Remotely sign on to a user device and control the screen. Users can watch you navigate their screen, which can also be helpful for training purposes.
- Navigate and repair a remote device in real time. You can change configurations, troubleshoot operating system issues, and disable or stop problematic apps or processes.
- Isolate and contain threats before they spread to other mobile devices by remotely disabling network access, stopping rogue processes, and removing apps or malware.
- Remotely enable the device ringer and call the phone, to help the user to locate the device. When a user can't find the device, you can wipe it to ensure that your sensitive data is not compromised.

Remote Support also enables support personnel to:

- Display a list of all connected devices within one or more instances of XenMobile.
- Display system information including device model, operating system level, International Mobile Station Equipment Identity (IMEI), serial number, memory and battery status, and connectivity.
- Display the users and groups for XenMobile.
- Run the device task manager where you can display active processes, end active processes, and restart the mobile device.
- Run remote file transfer that includes bidirectional file transfer between mobile devices and a central file server.
- Download and install software programs as a batch to one or more mobile devices.
- Configure remote registry key settings on the device.
- Optimize response time over low-bandwidth cellular networks by using real-time device screen remote control.
- Display the device skin for most mobile device brands and models. Display a skin editor to add new device models and map physical keys.
- Enable device screen capture, record, and replay with the ability to capture a sequence of interactions on the device that creates a video AVI file.
- Conduct live meetings by using a shared whiteboard, VoIP-based voice communications and chat among mobile users and support personnel.

Remote Support System Requirements

The Remote Support software installs on Windows-based computers which meet the following requirements. For port requirements, see Port Requirements.

Supported platforms:

- Intel Xeon/Pentium 4 -1 GHz minimum Workstation class
- 512-MB RAM minimum
- 100-MB free disk space minimum

Supported operating systems:

- Microsoft Windows 2003 Server Standard Edition or Enterprise Edition SP1 or later
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 or later
- Microsoft Windows Vista SP1 or later
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

To install the Remote Support software

1. To download the Remote Support installer, go to the XenMobile 10 download page and log on to your account.
2. Expand **Tools** and then download XenMobile Remote Support v9.
   The Remote Support file name is XenMobileRemoteSupport-9.0.0.35265.exe.
3. Double-click the Remote Support installer and then follow the instructions in the installation wizard.

To install Remote Support from the command line:

Run the following command:

```
RemoteSupport.exe /S
```

RemoteSupport is the name of the installation program. For example:

XenMobileRemoteSupport-9.0.0.35265.exe /S

You can use the following variables when installing the Remote Support software:

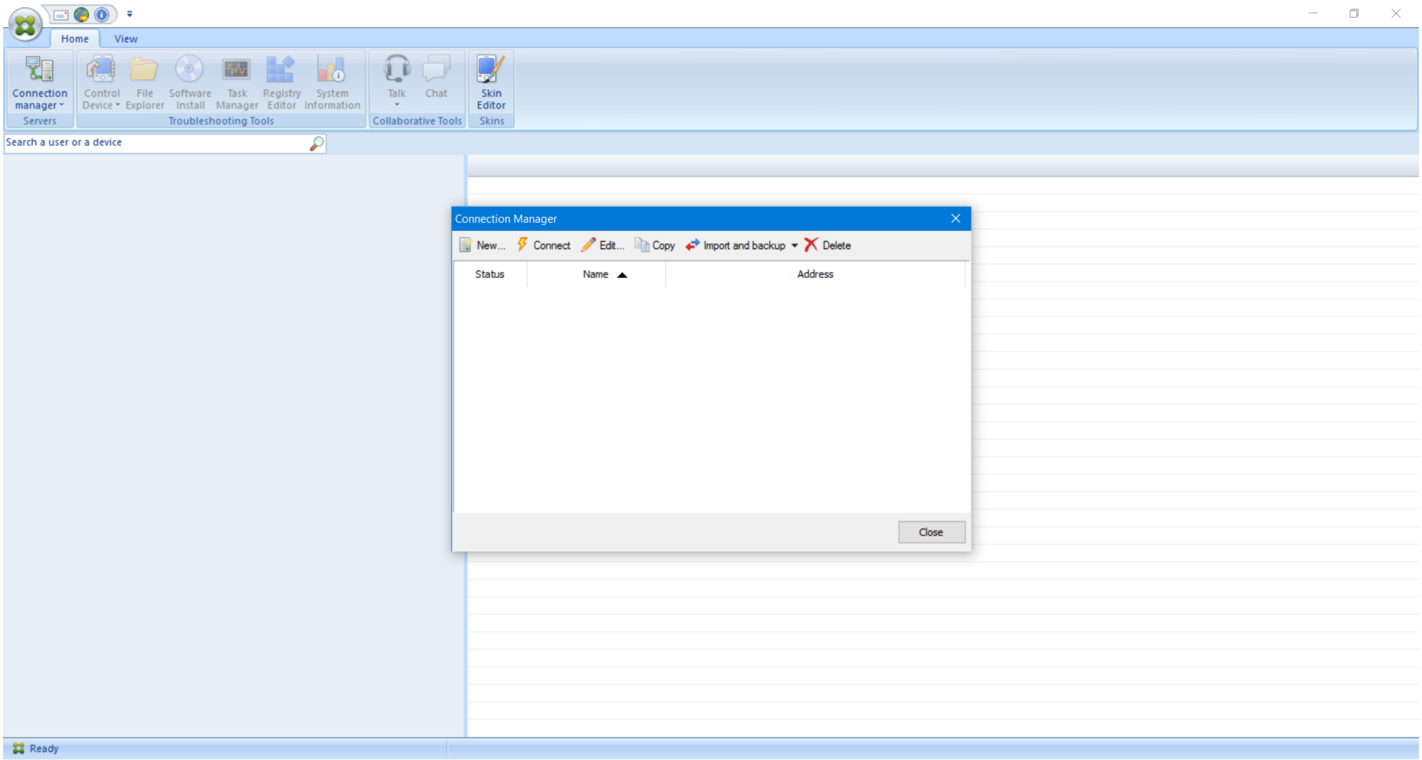
- /S: to install the Remote Support software silently with the default parameters.
- /D=dir: to specify a custom installation directory.

To connect Remote Support to XenMobile

To establish remote support connections to managed devices, you must add a connection from Remote Support to one or more XenMobile Servers that manage the devices. That connection runs over an app tunnel that you define in the Tunnel MDM policy, a device policy for Android and Windows Mobile/CE devices. Define the app tunnel before you can connect Remote Support to XenMobile. For details, see App tunneling device policies.

1. Start the Remote Support software and use your XenMobile credentials to sign on.

2. In **Connection Manager**, click **New**.



3. In the **Connection Configuration** dialog box, on the **Server** tab, type the following values:

a. In **Configuration name**, type a name for the configuration entry.

b. In **Server IP address or name**, type the IP address or the DNS name of the XenMobile Server.

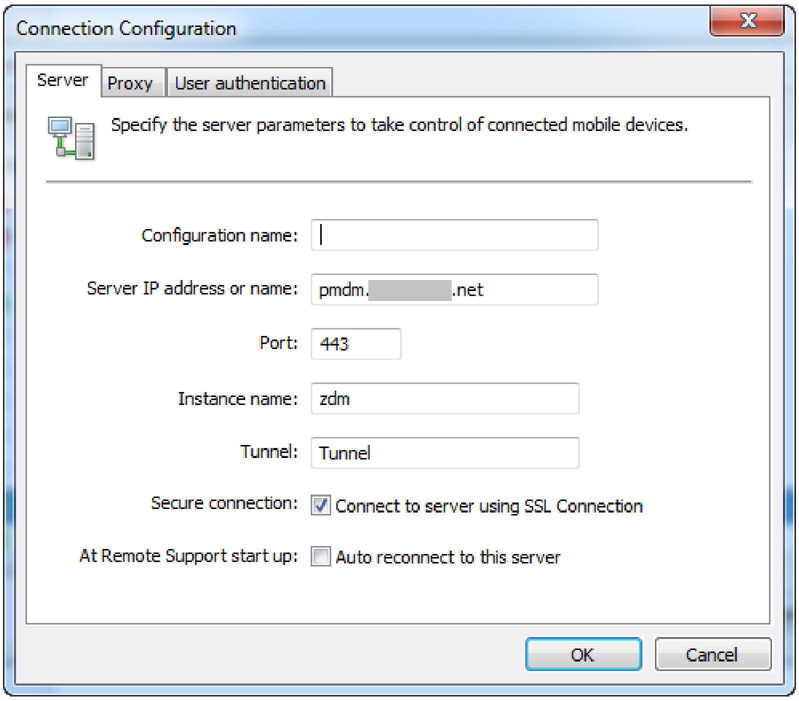
c. In **Port**, type a TCP port number, as defined in the XenMobile Server configuration.

d. In **Instance name**, when XenMobile is part of a multitenant deployment, type an instance name.

e. In **Tunnel**, type the name of the Tunnel policy.

f. Select the **Connect to server using SSL Connection** check box.

g. Select the **Auto reconnect to this server** check box to connect to the configured XenMobile Server each time the Remote Support application starts.



Connection Configuration

Server | Proxy | User authentication

Specify the server parameters to take control of connected mobile devices.

Configuration name:

Server IP address or name: pmdm.[redacted].net

Port: 443

Instance name: zdm

Tunnel: Tunnel

Secure connection: ☑ Connect to server using SSL Connection

At Remote Support start up: □ Auto reconnect to this server

4. On the **Proxy** tab, select **Use a http proxy server** and then type the following information:

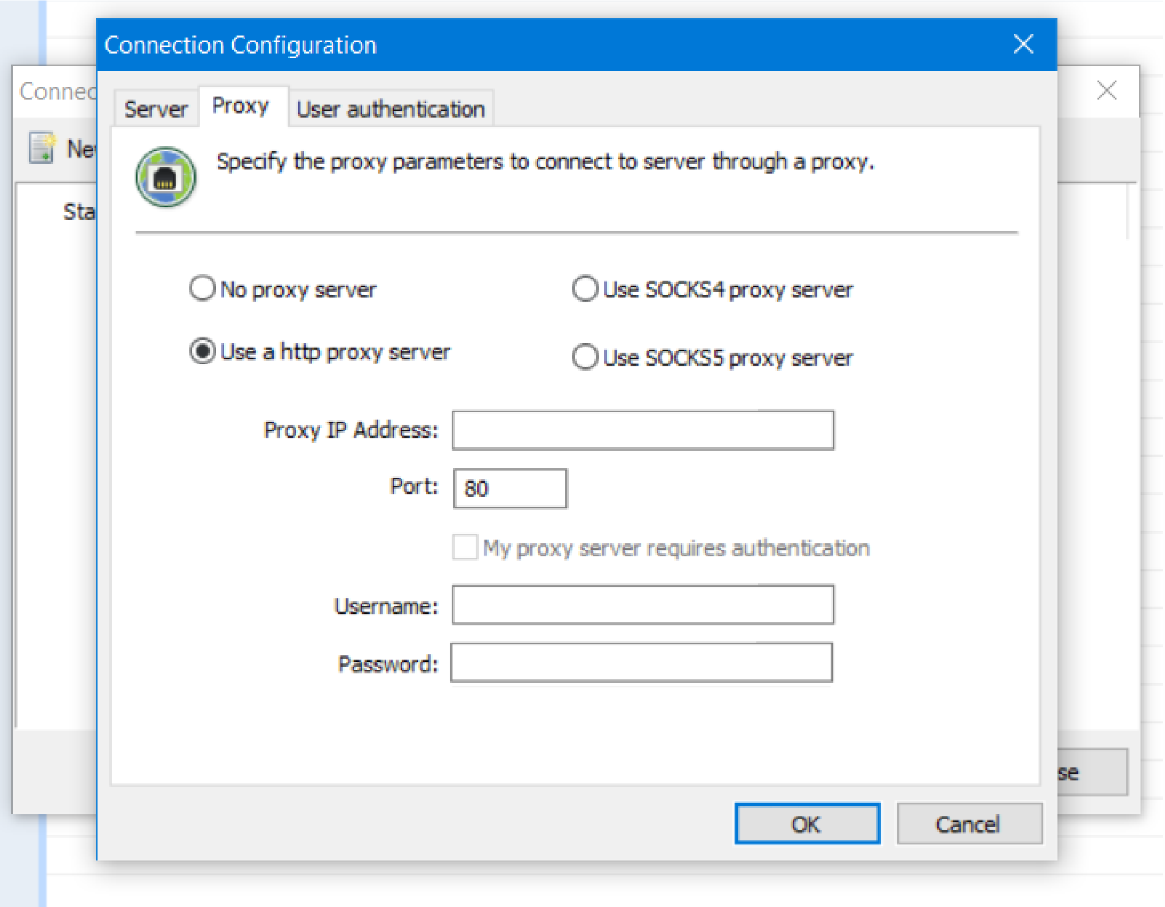
a. In **Proxy IP Address**, type the IP address of the proxy server.

b. In **Port**, type a TCP port number used by the proxy.

c. Select the **My proxy server requires authentication** check box when the proxy server requires authentication to allow traffic.

d. In **Username**, type the user name to be authenticated on the proxy server.

e. In **Password**, type the password to be authenticated on the proxy server.



Specify the proxy parameters to connect to server through a proxy.

○ No proxy server ○ Use SOCKS4 proxy server

● Use a http proxy server ○ Use SOCKS5 proxy server

Proxy IP Address:

Port: 80

□ My proxy server requires authentication

Username:

Password:

5. On the **User Authentication** tab, select the **Remember my login and password** check box and enter the credentials.

6. Click **OK**.

To connect to XenMobile, double-click the connection you created and then enter the user name and password you configured for the connection.

To enable remote support for Samsung KNOX devices

You create a Remote Support policy in XenMobile to give you remote access to Samsung KNOX devices. You can configure two types of support:

- **Basic**: Lets you view diagnostic information about the device. For example, system information, processes that are running, task manager (memory and CPU usage), and installed software folder contents.
- **Premium**: Lets you remotely control the device screen. For example, control window colors, establish a VoIP session between the help desk and user, and establish a chat session between the help desk and user.

  Premium support requires that you configure the Samsung MDM License Key device policy in the XenMobile console. When you configure this policy, select the **Samsung KNOX** platform only. For the Samsung SAFE platform, the ELM key automatically deploys on Samsung devices when they enroll in XenMobile. Therefore, don't select the Samsung SAFE platform for this policy. For details, see Samsung MDM license key.

For information about configuring the Remote Support Policy, see Remote support device policy.

To use a Remote Support session

After you start Remote Support, the left-side of the Remote Support application window presents XenMobile user groups as you defined in the XenMobile console. By default, only groups containing users who are currently connected appear. You can see the device for each user next to the user entry.

1. To see all users, expand each group from the left column.
   Those users currently connected to the XenMobile Server are indicated with a green icon.
2. To display all users, including those not currently connected, click **View** and select **Non-connected devices.**
   Non-connected users appear without the small green icon.

Devices connected to the XenMobile Server but not assigned to a user appear in Anonymous mode. (The string **Anonymous** appears in the list.) You can control these devices just like the device of a logged-in user.

To control a device, select the device by clicking its row and then clicking **Control Device**. A rendering of the device appears in the Remote Control window. You can interact with a controlled device in the following ways:

- Control the device screen, including control with colors, in either the main window, or in a separate, floating window.
- Establish a VoIP session between the help desk and the user. Configure VoIP settings.
- Establish a chat session with the user.
- Access the device task manager, to manage items such as memory usage, CPU usage, and running apps.
- Explore the mobile device local directories. Transfer files.
- Edit the device registry on Windows mobile devices.
- Display device system information and all installed software.
- Update the mobile device connection status with the XenMobile Server.

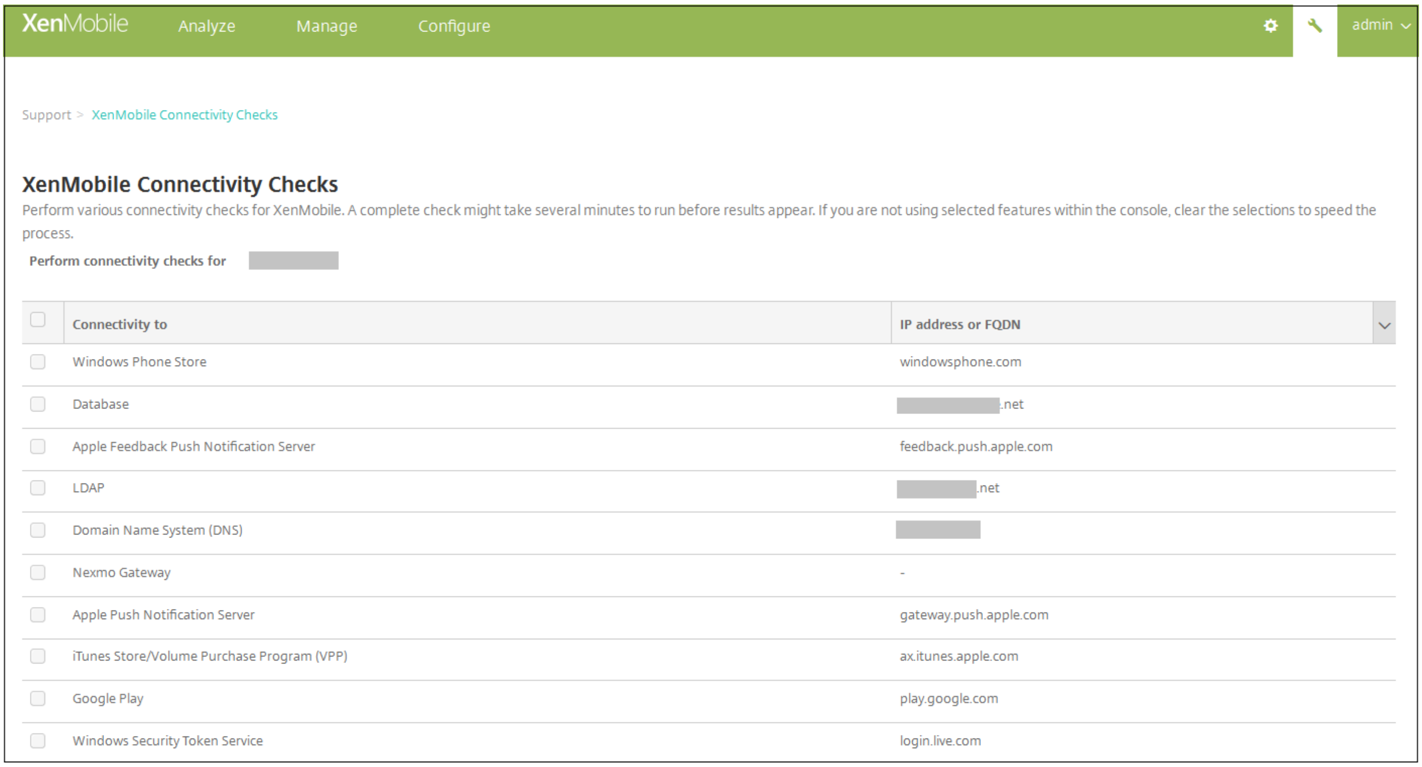
Connectivity checks

Sep 06, 2017

From the XenMobile **Support** page, you can check the XenMobile connection to NetScaler Gateway and to other servers and locations.

1. In the XenMobile console, click the wrench icon in the upper-right corner of the console. The **Support** page appears.

2. Under **Diagnostics**, click **XenMobile Connectivity Checks**. The **XenMobile Connectivity Checks** page appears. If your XenMobile environment contains clustered nodes, all nodes are shown.



Support > XenMobile Connectivity Checks

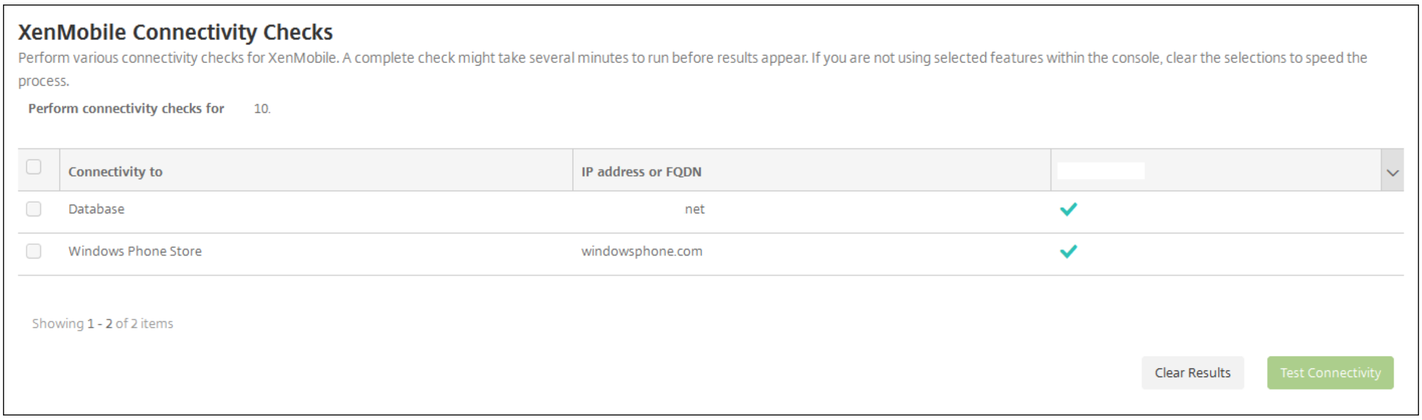
XenMobile Connectivity Checks

Perform various connectivity checks for XenMobile. A complete check might take several minutes to run before results appear. If you are not using selected features within the console, clear the selections to speed the process.

Perform connectivity checks for [redacted]

□	Connectivity to	IP address or FQDN
□	Windows Phone Store	windowsphone.com
□	Database	[redacted].net
□	Apple Feedback Push Notification Server	feedback.push.apple.com
□	LDAP	[redacted].net
□	Domain Name System (DNS)	[redacted]
□	Nexmo Gateway	-
□	Apple Push Notification Server	gateway.push.apple.com
□	iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
□	Google Play	play.google.com
□	Windows Security Token Service	login.live.com

2. Select the servers you want to include in the connectivity test and then click **Test Connectivity**. The test results page appears.



XenMobile Connectivity Checks

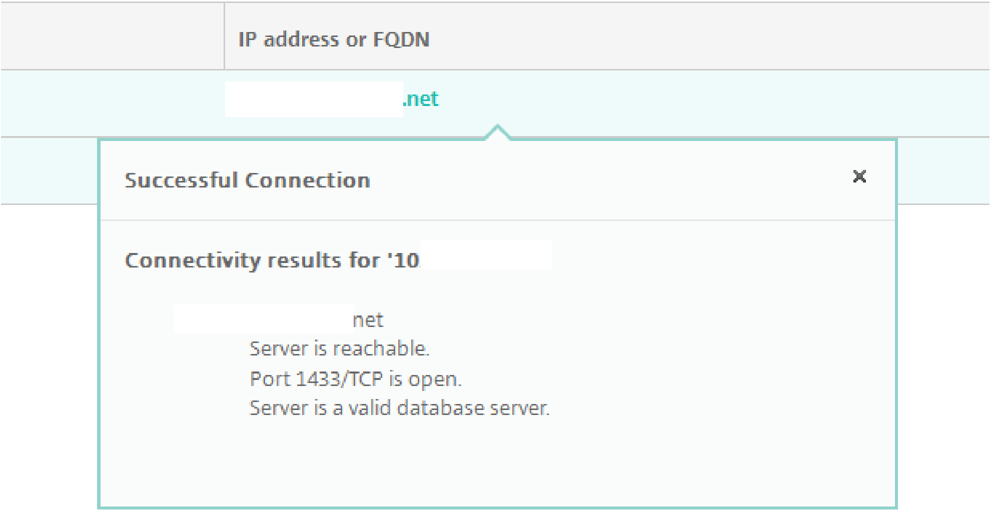
Perform various connectivity checks for XenMobile. A complete check might take several minutes to run before results appear. If you are not using selected features within the console, clear the selections to speed the process.

Perform connectivity checks for 10.

□	Connectivity to	IP address or FQDN	
□	Database	net	✓
□	Windows Phone Store	windowsphone.com	✓

Showing 1 - 2 of 2 items

3. Select a server in the test results table to see detailed results for that server.



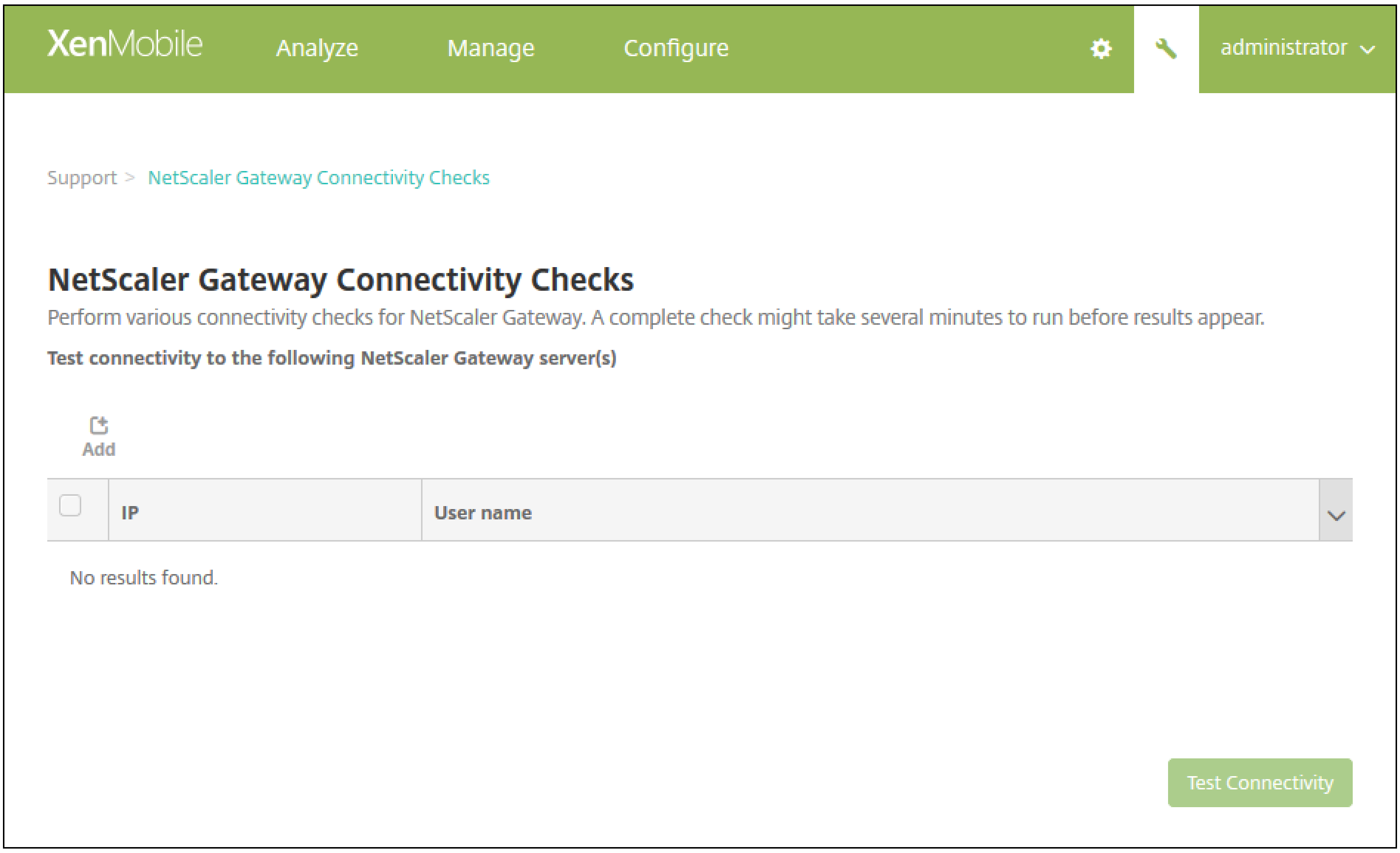
	IP address or FQDN
	[redacted].net

Successful Connection ×

Connectivity results for '10[redacted]

[redacted]net
Server is reachable.
Port 1433/TCP is open.
Server is a valid database server.

1. On the **Support** page, under **Diagnostics**, click **NetScaler Gateway Connectivity Checks**. The **NetScaler Gateway Connectivity Checks** page appears. The table is empty if you haven't added any NetScaler Gateway servers.



NetScaler Gateway Connectivity Checks

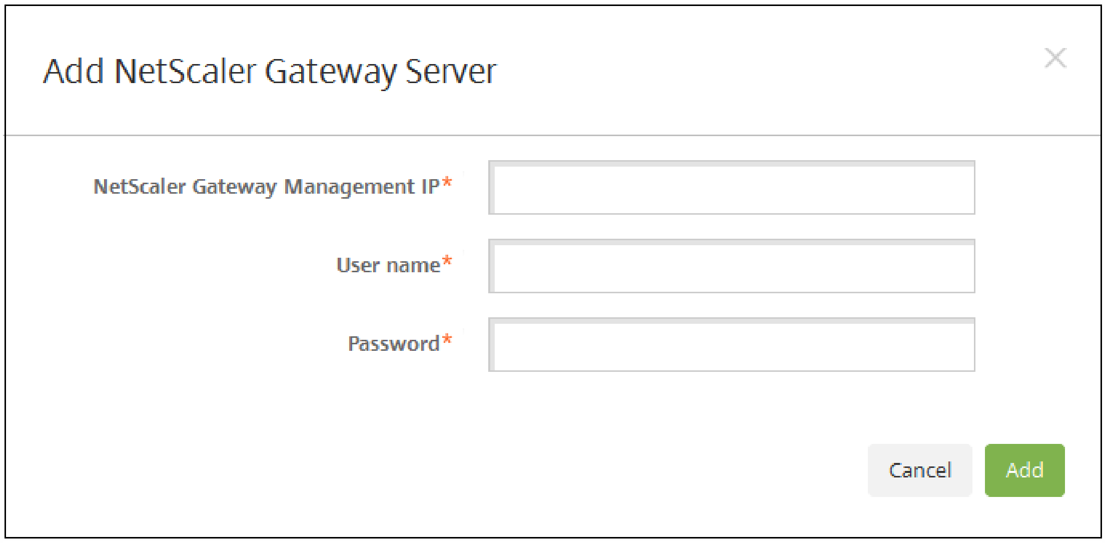
Perform various connectivity checks for NetScaler Gateway. A complete check might take several minutes to run before results appear.

Test connectivity to the following NetScaler Gateway server(s)

☐	IP	User name

No results found.

2. Click **Add**. The **Add NetScaler Gateway Server** dialog box appears.


Add NetScaler Gateway Server

NetScaler Gateway Management IP*

User name*

Password*

3. In **NetScaler Gateway Management IP**, type the management IP address for the server running NetScaler Gateway that you want to test.

Note: If you're conducting a connectivity check for a NetScaler Gateway server that has already been added before, the IP address is provided.

4. Type your administrator credentials for this NetScaler Gateway.

Note: If you're conducting a connectivity check for a NetScaler Gateway server that has already been added before, the user name is provided.

5. Click **Add**. The NetScaler Gateway is added to the table on the **NetScaler Gateway Connectivity Checks** page.

6. Select the NetScaler Gateway server and then click **Test Connectivity**. The results appear in a test results table.

7. Select a server in the test results table to see detailed results for that server.

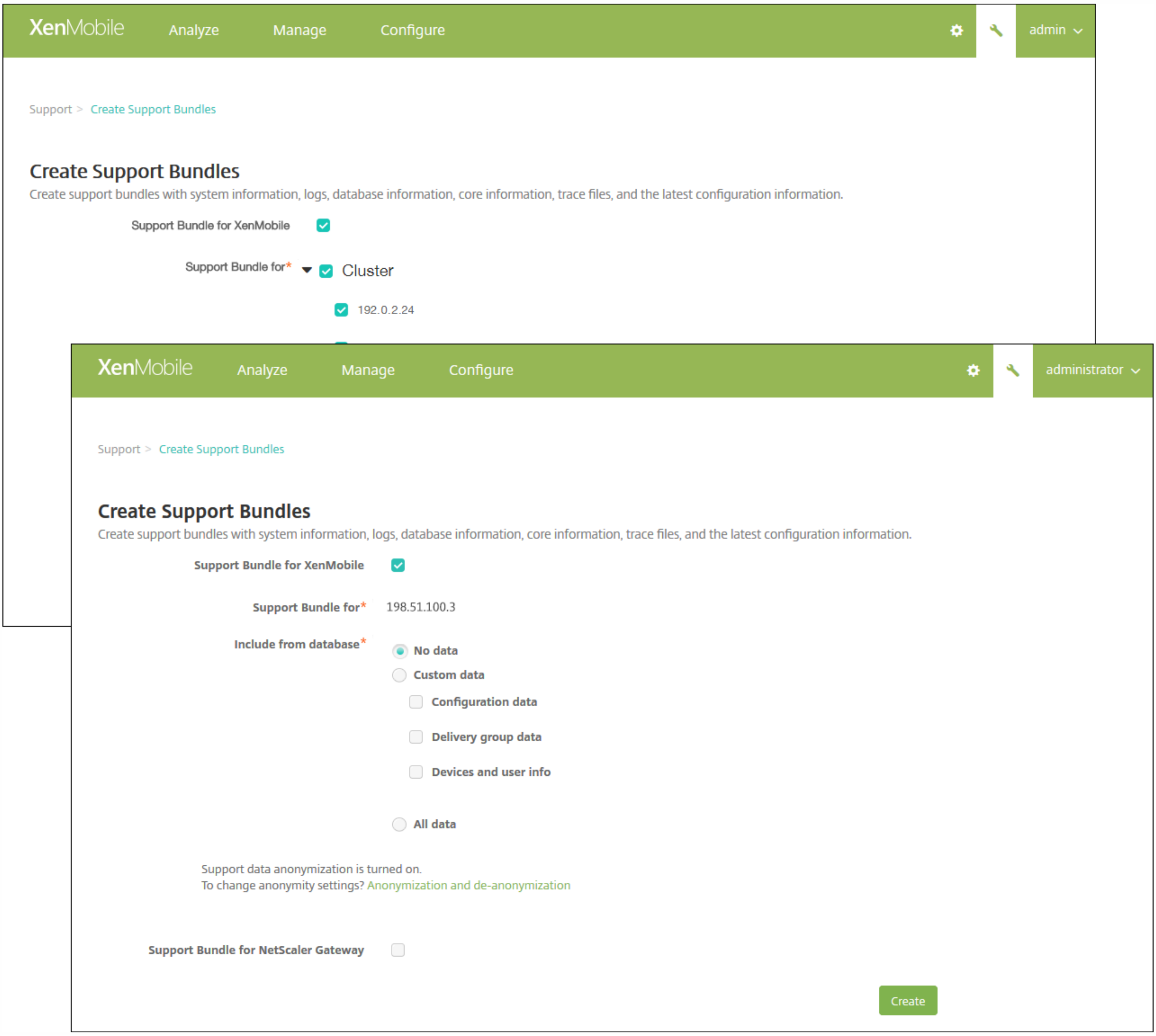
Support bundles

Sep 06, 2017

If you want to report an issue to Citrix or troubleshoot a problem, you can create a support bundle and then upload the support bundle to Citrix Insight Services (CIS).

1. In the XenMobile console, click the wrench icon in the right upper-hand corner. The **Support** page appears.

2. On the **Support** page, click **Create Support Bundles**. The **Create Support Bundles** page appears. If your XenMobile environment contains clustered nodes, all nodes are shown.



Create Support Bundles

Create support bundles with system information, logs, database information, core information, trace files, and the latest configuration information.

Support Bundle for XenMobile ☑

Support Bundle for* ☑ Cluster

☑ 192.0.2.24

Create Support Bundles

Create support bundles with system information, logs, database information, core information, trace files, and the latest configuration information.

Support Bundle for XenMobile ☑

Support Bundle for* 198.51.100.3

Include from database*
● No data
○ Custom data
□ Configuration data
□ Delivery group data
□ Devices and user info
○ All data

Support data anonymization is turned on.
To change anonymity settings? Anonymization and de-anonymization

Support Bundle for NetScaler Gateway □

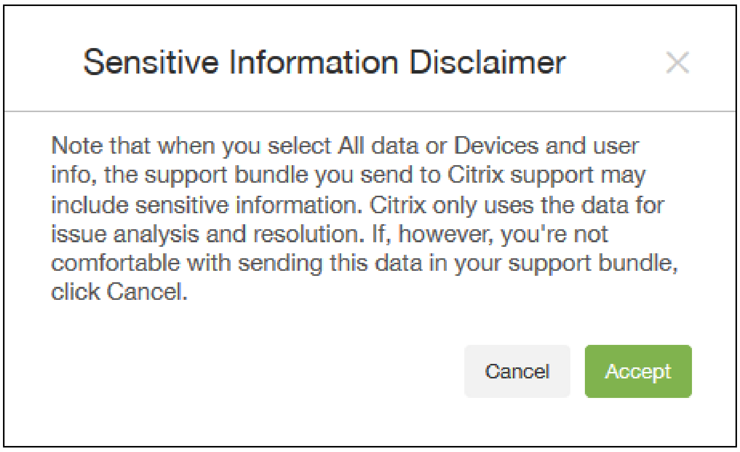
3. Make sure that the **Support Bundle for XenMobile** check box is selected.

4. If your XenMobile environment contains clustered nodes, in **Support Bundle for**, you can select all the nodes or any combination of nodes from which to draw data.

5. In **Include from database**, do one of the following:

- Click **No data**.
- Click **Custom data** and then select any or all of the following (by default, all options are selected):
  - **Configuration data**: Includes certificate configurations and device manager policies.
  - **Delivery group data**: Includes app delivery group information, containing app types and app delivery policy details.
  - **Devices and user info**: Includes device policies, apps, actions, and delivery groups.
- Click **All data**.

Note: If you choose **Devices and user info** or **All data**, and this is the first support bundle you have created, the **Sensitive Information Disclaimer** dialog box appears. Read the disclaimer and then click **Accept** or **Cancel**. If you click **Cancel**, the support bundle cannot be uploaded to Citrix. If you click **Accept**, you can upload the support bundle to Citrix and you will not see the disclaimer the next time you create a support bundle that includes device or user data.


Sensitive Information Disclaimer

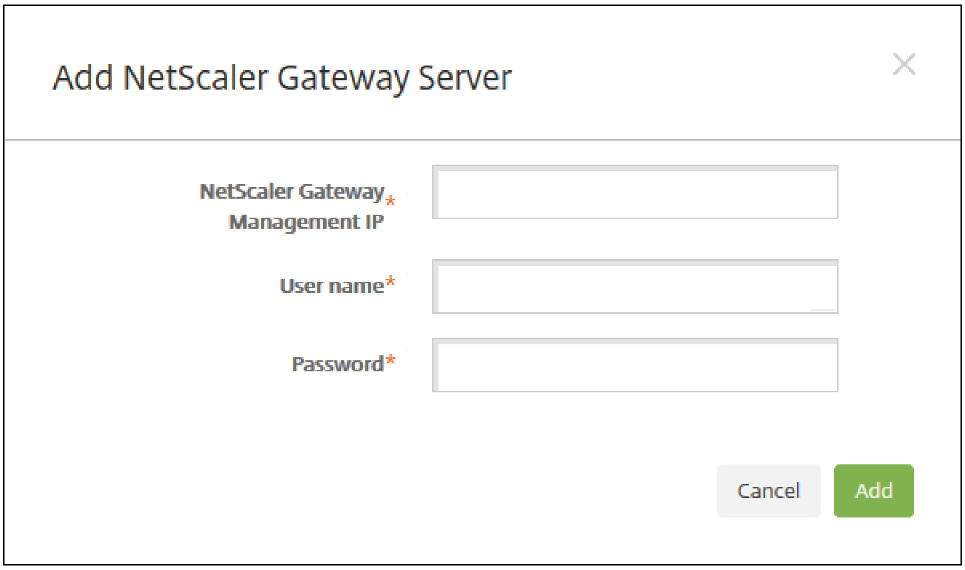
Note that when you select All data or Devices and user info, the support bundle you send to Citrix support may include sensitive information. Citrix only uses the data for issue analysis and resolution. If, however, you're not comfortable with sending this data in your support bundle, click Cancel.

6. The **Support data anonymization is turned on** option indicates that the default setting is to anonymize the data, which means that sensitive user, server, and network data is made anonymous in support bundles.

To change this setting, click **Anonymization and de-anonymization**. For more information about data anonymization, see Anonymizing data in support bundles.

7. Select the **Support Bundle for NetScaler Gateway** check box if you want to include support bundles from NetScaler Gateway and then do the following:

a. Click **Add**. The **Add NetScaler Gateway Server** dialog box appears.


Add NetScaler Gateway Server

NetScaler Gateway Management IP*

User name*

Password*

b. In **NetScaler Gateway Management IP**, type the NetScaler management IP address for the NetScaler Gateway from which you want to draw your support bundle data.

Note: If you are creating a bundle from a NetScaler Gateway server that is already added, the IP address is provided.

c. In **User name** and **Password**, type the user credentials needed to access the server running NetScaler Gateway.

Note: If you are creating a bundle from a NetScaler Gateway server that is already added, the user name is provided.

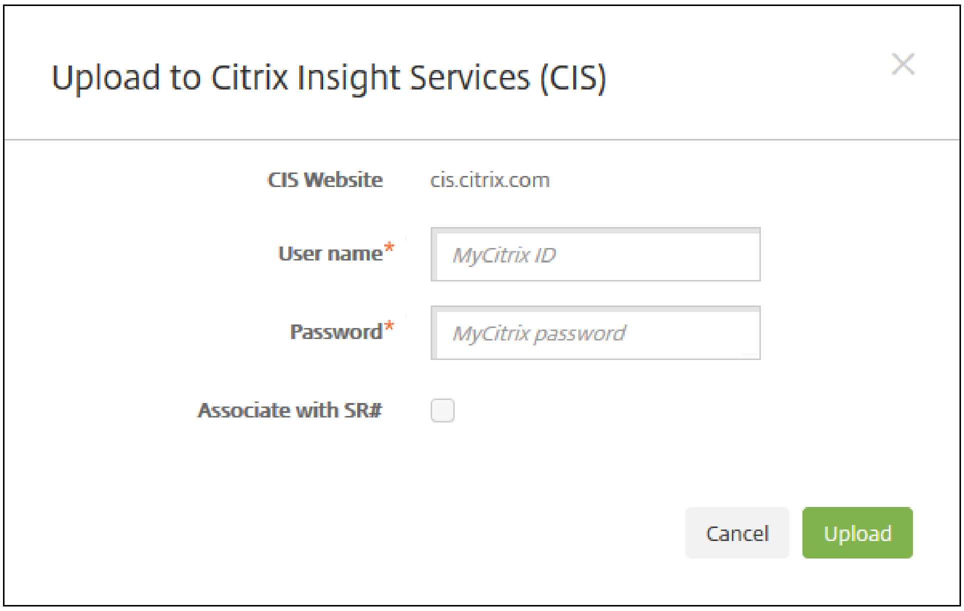
7. Click **Add**. The new NetScaler Gateway support bundle is added to the table.

8. Repeat Step 7 to add more NetScaler Gateway support bundles.

9. Click **Create**. The support bundle is created and two new buttons, **Upload to CIS** and **Download to Client**, appear.

After creating a support bundle, you can upload the bundle to Citrix Insight Services (CIS) or download the bundle to your computer. These steps show you how to upload the bundle to CIS. You need a MyCitrix ID and password to upload to CIS.

1. On the **Create Support Bundles** page, click **Upload to CIS**. The **Upload to Citrix Insight Services (CIS)** dialog box appears.



Upload to Citrix Insight Services (CIS)

CIS Website: cis.citrix.com

User name*: MyCitrix ID

Password*: MyCitrix password

Associate with SR#: □

2. In **User Name**, type your MyCitrix ID.

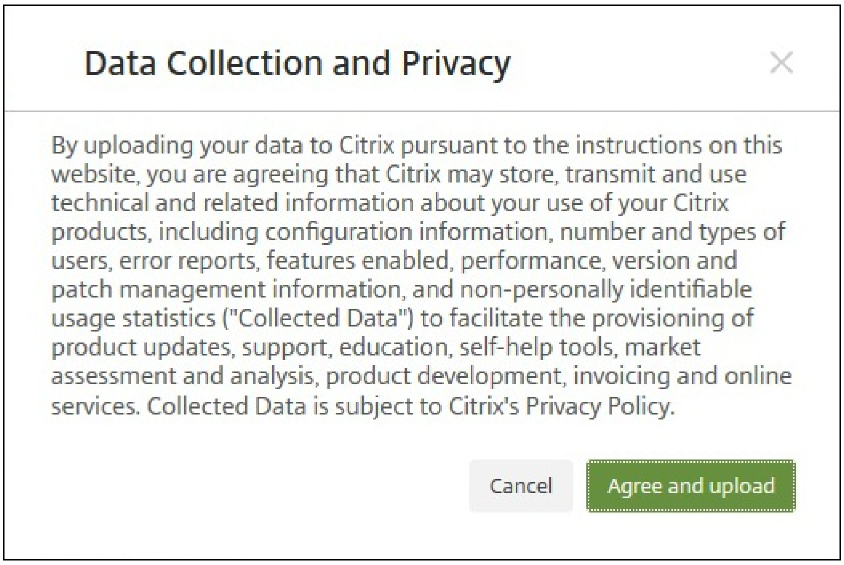
3. In **Password**, type your MyCitrix password.

4. If you want to connect this bundle with an existing service request number, select the **Associate with SR#** check box and in the two new fields that appear, do the following:

- In **SR#**, type the eight-digit service request number you want to associate this bundle with.
- In **SR Description**, type a description of the SR.

5. Click **Upload**.

If this is the first time you have uploaded a support bundle to CIS, and you haven't created an account on CIS through another product and accepted the Data Collection and Privacy agreement, the following dialog box appears; you must accept the agreement before the upload can begin. If you have an account on CIS and have previously accepted the agreement, the support bundle is uploaded immediately.



Data Collection and Privacy

By uploading your data to Citrix pursuant to the instructions on this website, you are agreeing that Citrix may store, transmit and use technical and related information about your use of your Citrix products, including configuration information, number and types of users, error reports, features enabled, performance, version and patch management information, and non-personally identifiable usage statistics ("Collected Data") to facilitate the provisioning of product updates, support, education, self-help tools, market assessment and analysis, product development, invoicing and online services. Collected Data is subject to Citrix's Privacy Policy.

6. Read the agreement and then click **Agree and upload**. The support bundle is uploaded.

After you create a support bundle, you can upload the bundle to CIS or download the bundle to your computer. If you would like to troubleshoot the problem on your own, download the support bundle to your computer.
On the Create Support Bundles page, click Download to Client. The bundle is downloaded to your computer.

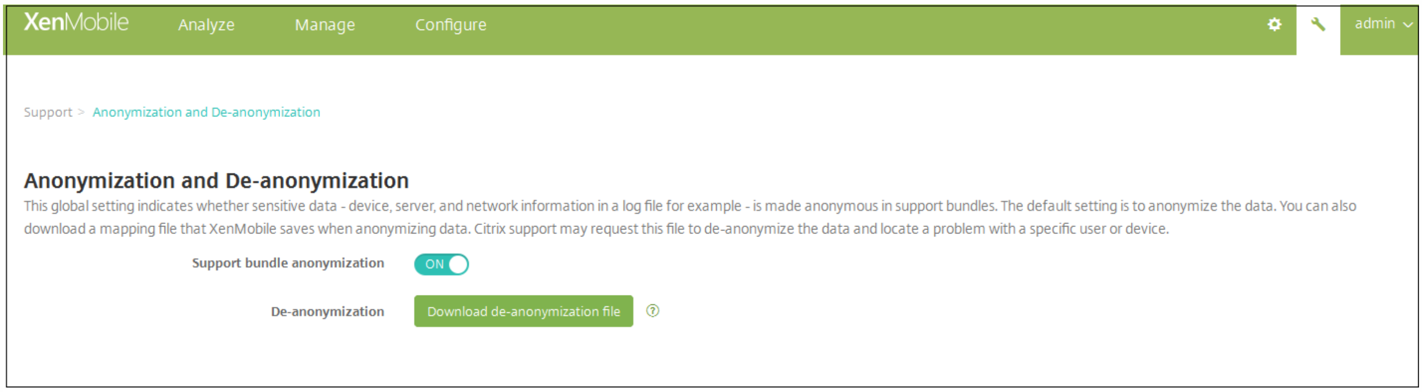
Anonymize data in support bundles

Sep 06, 2017

When you create support bundles in XenMobile, sensitive user, server, and network data is made anonymous by default. You can change this behavior on the Anonymization and De-anonymization page. You can also download a mapping file that XenMobile saves when anonymizing data. Citrix support may request this file to de-anonymize the data and locate a problem with a specific user or device.

1. In the XenMobile console, click the wrench icon in the right upper-hand corner. The **Support** page appears.

2. On the **Support** page, under **Advanced**, click **Anonymization and De-anonymization**. The **Anonymization and De-anonymization** page appears.



Anonymization and De-anonymization

This global setting indicates whether sensitive data - device, server, and network information in a log file for example - is made anonymous in support bundles. The default setting is to anonymize the data. You can also download a mapping file that XenMobile saves when anonymizing data. Citrix support may request this file to de-anonymize the data and locate a problem with a specific user or device.

Support bundle anonymization: ON

De-anonymization: Download de-anonymization file

3. In **Support bundle anonymization**, select whether data is anonymized. The default is **ON**.

4. Next to **De-anonymization**, click **Download de-anonymization file** to download the mapping file to send to Citrix support when they need specific device or user information to diagnose an issue.

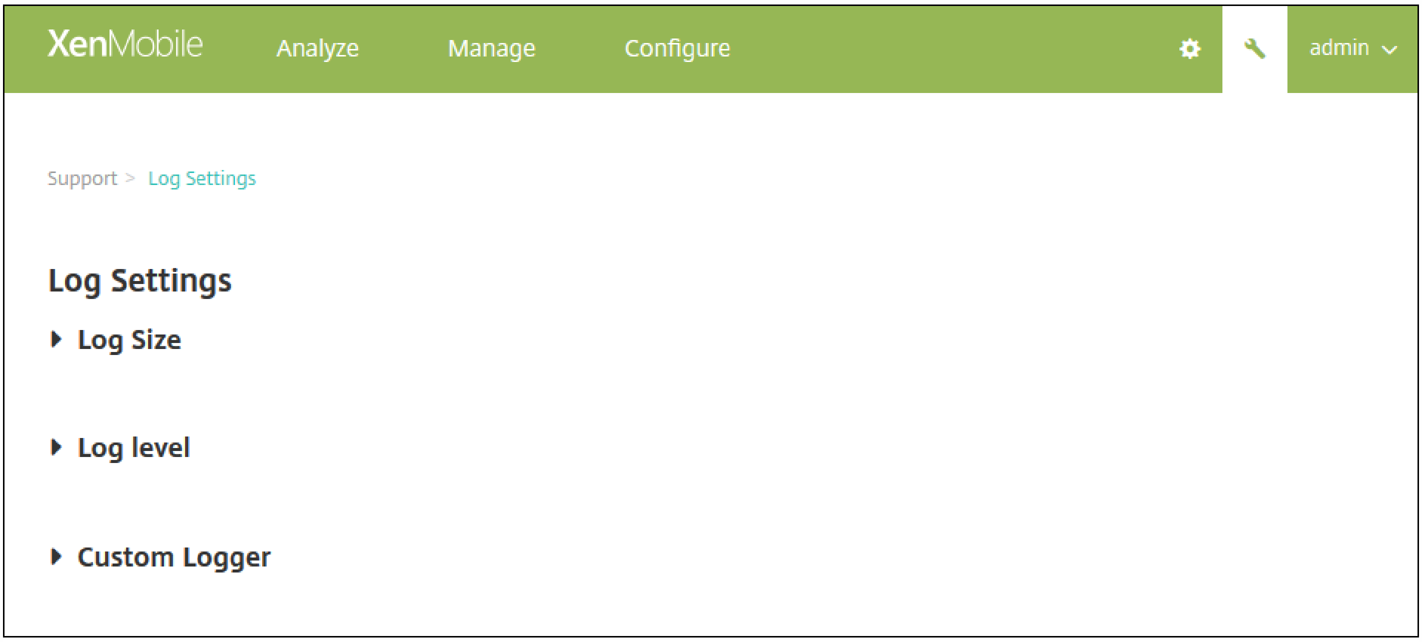
Logs

Sep 06, 2017

You can configure log settings to customize the output of logs that XenMobile generates. If you have clustered XenMobile servers, when you configure log settings in the XenMobile console, those settings are shared with all other servers in the cluster.

1. In the XenMobile console, click the wrench icon in the upper-right corner of the console. The **Support** page appears.

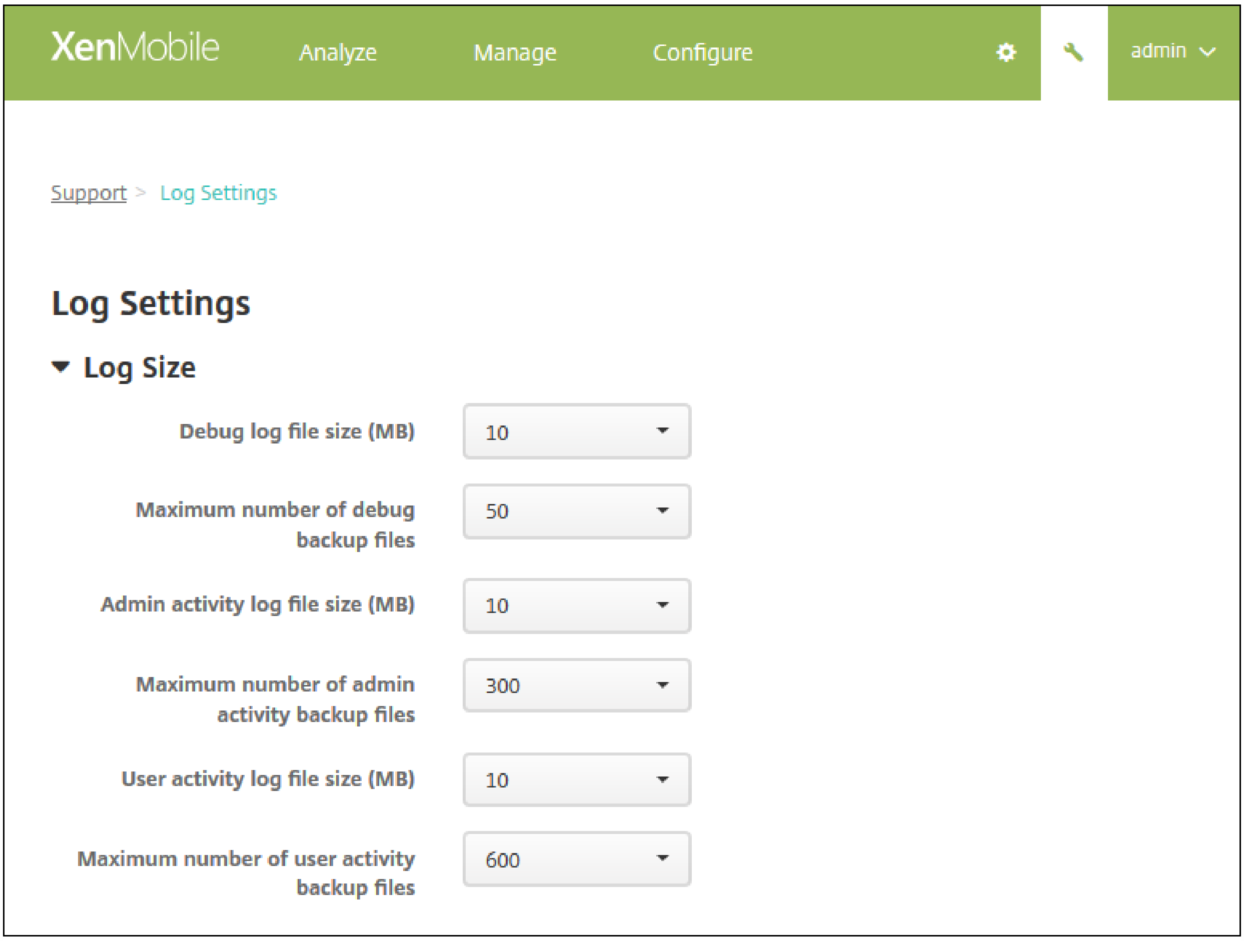
2. Under **Log Operations**, click **Log Settings**. The **Log Settings** page appears.



On the **Log Settings** page you can access the following options:

- **Log Size**. Use this option to control the size of the log file and the maximum number of log backup files retained in the database. Log size applies to each of the logs supported by XenMobile (debug log, Admin activity log, and user activity log).
- **Log level**. Use this option to change the log level or to persist settings.
- **Custom Logger**. Use this option to create a custom logger; custom logs require a class name and the log level.

1. On the **Log Settings** page, expand **Log Size**.



Support > Log Settings

Log Settings

Log Size

Debug log file size (MB): 10

Maximum number of debug backup files: 50

Admin activity log file size (MB): 10

Maximum number of admin activity backup files: 300

User activity log file size (MB): 10

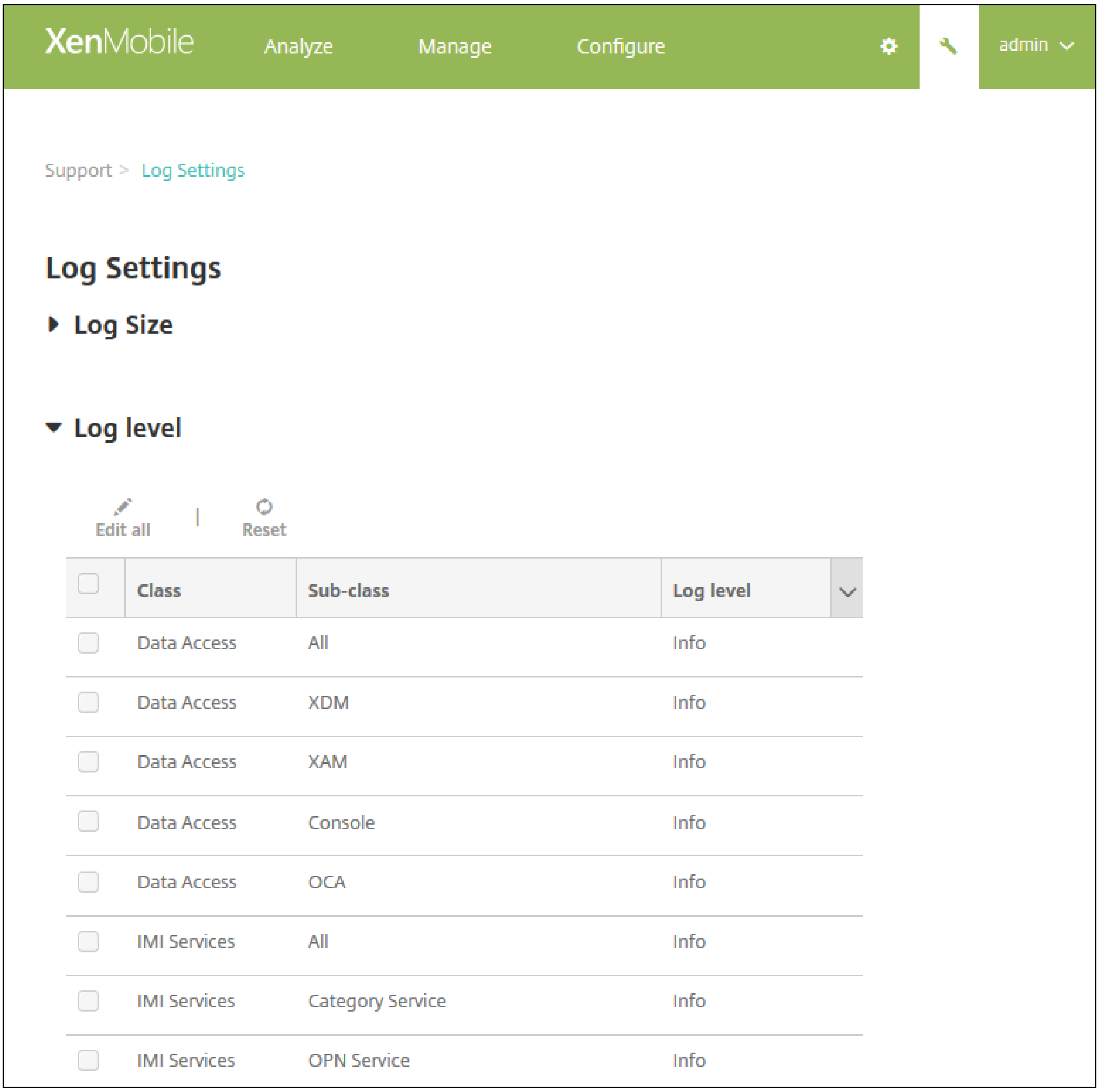
Maximum number of user activity backup files: 600

2. Configure these settings:

- **Debug log file size (MB)**: In the list, click a size between 5 MB and 20 MB to change the maximum size of the debug file. The default file size is **10 MB**.
- **Maximum number of debug backup files**: In the list, click the maximum number of debug files retained by the server. By default, XenMobile retains 50 backup files on the server.
- **Admin activity log file size (MB)**: in the list, click a size between 5 MB and 20 MB to change the maximum size of the admin activity file. The default file size is **10 MB**.
- **Maximum number of admin activity backup files**: In the list, click the maximum number of admin activity files retained by the server. By default, XenMobile retains 300 backup files on the server.
- **User activity log file size (MB)**: In the list, click a size between 5 MB and 20 MB to change the maximum size of the user activity file. The default file size is **10 MB**.
- **Maximum number of user activity backup files**: In the list, click the maximum number of user activity files retained by the server. By default, XenMobile retains 300 backup files on the server.

Log level lets you specify what type of information XenMobile collects in the log. You can set the same level for all classes or you can set individual classes to specific levels.

1. On the **Log Settings** page, expand **Log level**. The table of all log classes appears.



Log Settings

Log Size

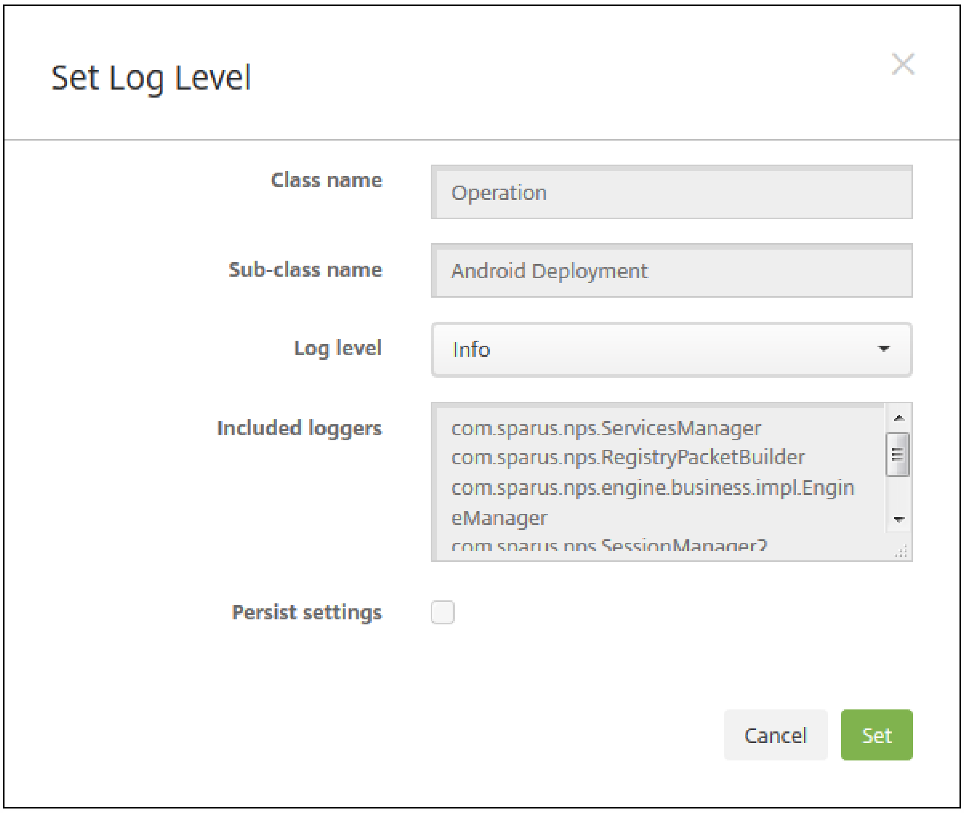
Log level

□	Class	Sub-class	Log level
□	Data Access	All	Info
□	Data Access	XDM	Info
□	Data Access	XAM	Info
□	Data Access	Console	Info
□	Data Access	OCA	Info
□	IMI Services	All	Info
□	IMI Services	Category Service	Info
□	IMI Services	OPN Service	Info

2. Do one of the following:

- Click the check box next to one Class and then, click **Set Level** to change just this class's log level.
- Click **Edit** all to apply the log level change to all classes in the table.

The **Set Log Level** dialog box appears where you can set the log level and select whether to have log level settings persist when you reboot the XenMobile server.



Set Log Level

Class name: Operation

Sub-class name: Android Deployment

Log level: Info

Included loggers:

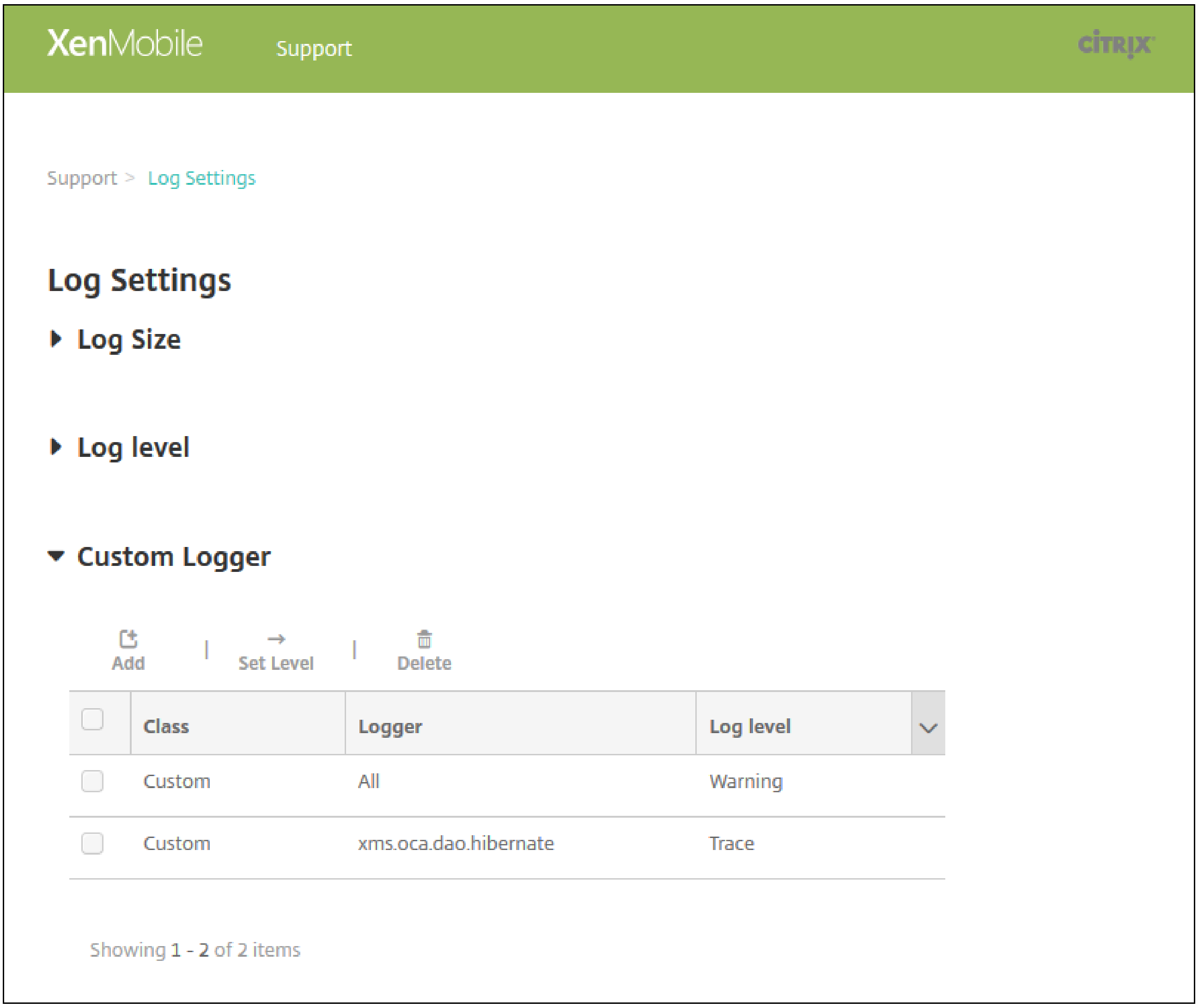
com.sparus.nps.ServicesManager
com.sparus.nps.RegistryPacketBuilder
com.sparus.nps.engine.business.impl.EngineManager
com.sparus.nps.SessionManager2

Persist settings: □

- **Class Name**: This field displays All when you are changing the log level for all classes or it displays the individual class name; it is not editable.
- **Sub-class name**: This field displays All when you are changing the log level for all classes or it displays the individual class sub-class name; it is not editable.
- **Log level**: In the list, click a log level. The supported log levels include:
  - Fatal
  - Error
  - Warning
  - Info
  - Debug
  - Trace
  - Off
- **Included Loggers**: This field is blank when you are changing the log level for all classes or it displays the currently configured loggers for an individual class; it is not editable.
- **Persist settings**: If you want the log level settings to persist when you reboot the server, select this check box. Not selecting this check box means that the log level settings revert to their defaults when you reboot the server.

3. Click **Set** to commit your changes.

1. On the **Log Settings** page, expand **Custom Logger**. The **Custom Logger** table appears. If you haven't added any custom loggers, the table is initially empty.



Log Settings

▸ Log Size

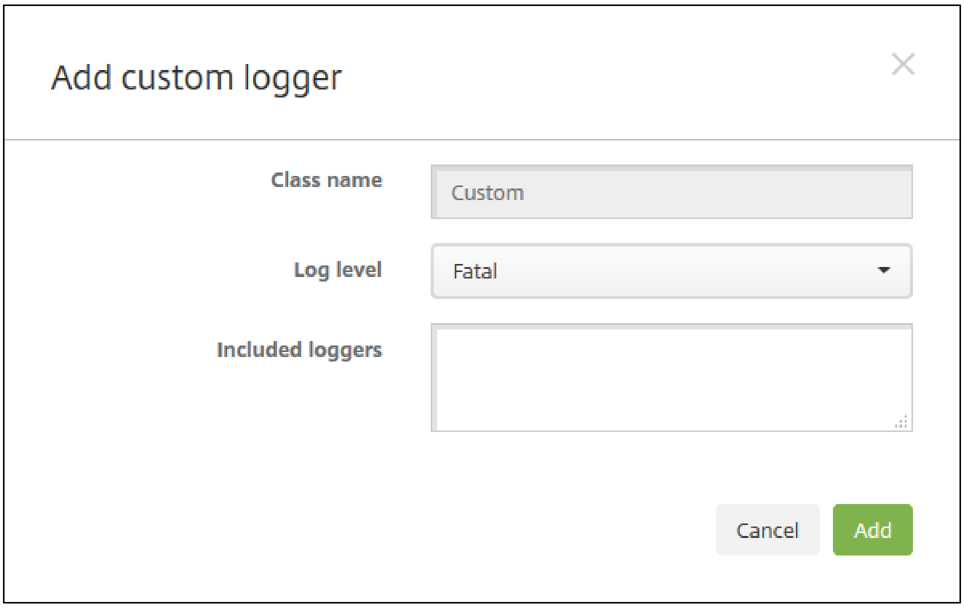
▸ Log level

▾ Custom Logger

□	Class	Logger	Log level
□	Custom	All	Warning
□	Custom	xms.oca.dao.hibernate	Trace

Showing 1 - 2 of 2 items

2. Click **Add**. The **Add custom logger** dialog box appears.



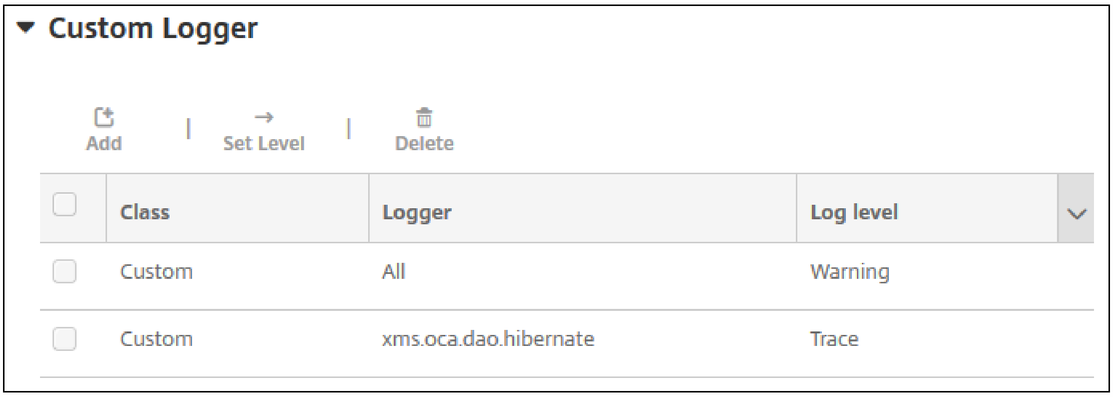
Add custom logger

Class name	Custom
Log level	Fatal
Included loggers	

3. Configure these settings:

- **Class Name**: This field displays **Custom**; it is not editable.
- **Log level**: In the list, click a log level. The supported log levels include:
  - Fatal
  - Error
  - Warning
  - Info
  - Debug
  - Trace
  - Off
- **Included Loggers**: Type the specific loggers you want to include in the custom logger or leave the field blank to include all loggers.

4. Click **Add**. The custom logger is added to the **Custom Logger** table.



☐	Class	Logger	Log level
☐	Custom	All	Warning
☐	Custom	xms.oca.dao.hibernate	Trace

1. On the **Log Settings** page, expand **Custom Logger**.

2. Select the custom logger you want to delete.

3. Click **Delete**. A dialog box appears asking whether you want to delete the custom logger. Click **OK**.

Important: You cannot undo this operation.

XenMobile Analyzer Tool

Jan 30, 2018

XenMobile Analyzer is a cloud-based tool that you can use to diagnose and troubleshoot XenMobile-related issues with configuration and other features. The tool checks for device or user enrollment and authentication issues within your XenMobile environment.

Configure the tool to point to your XenMobile 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 XenMobile Analyzer discovers issues, the tool provides recommendations to correct the issues.

In this article:

- Accessing and starting the XenMobile Analyzer
- Performing an environment check
- Performing a NetScaler check
- Adding a schedule to environment checks
- Performing other informative checks
- Known issues
- Fixed issues

Key features

- Secure, cloud-based micro-service to troubleshoot all XenMobile related issues.
- Accurate recommendations to resolve XenMobile configuration issues.
- Reduced support calls and accelerated troubleshooting of XenMobile environments.
- Zero-day support for XenMobile Server releases.
- Health check scheduling on a daily or weekly cadence.
- NetScaler configuration checks.
- Secure Web tests for reachability to intranet sites.
- Secure Mail autodiscovery service checks.
- ShareFile single sign-on (SSO) checks.

- The NetScaler Configuration Report displays a badge notification indicating the number of recommendations. The recommendations are based on the Essential Configuration checks on a particular NetScaler Gateway.
- The icons within the global navigation bar on the Test Environment List page have now been reordered for better user experience.

The following video highlights the navigation changes in the user interface.

Citrix XenMobile Analyzer: New Environment List UI

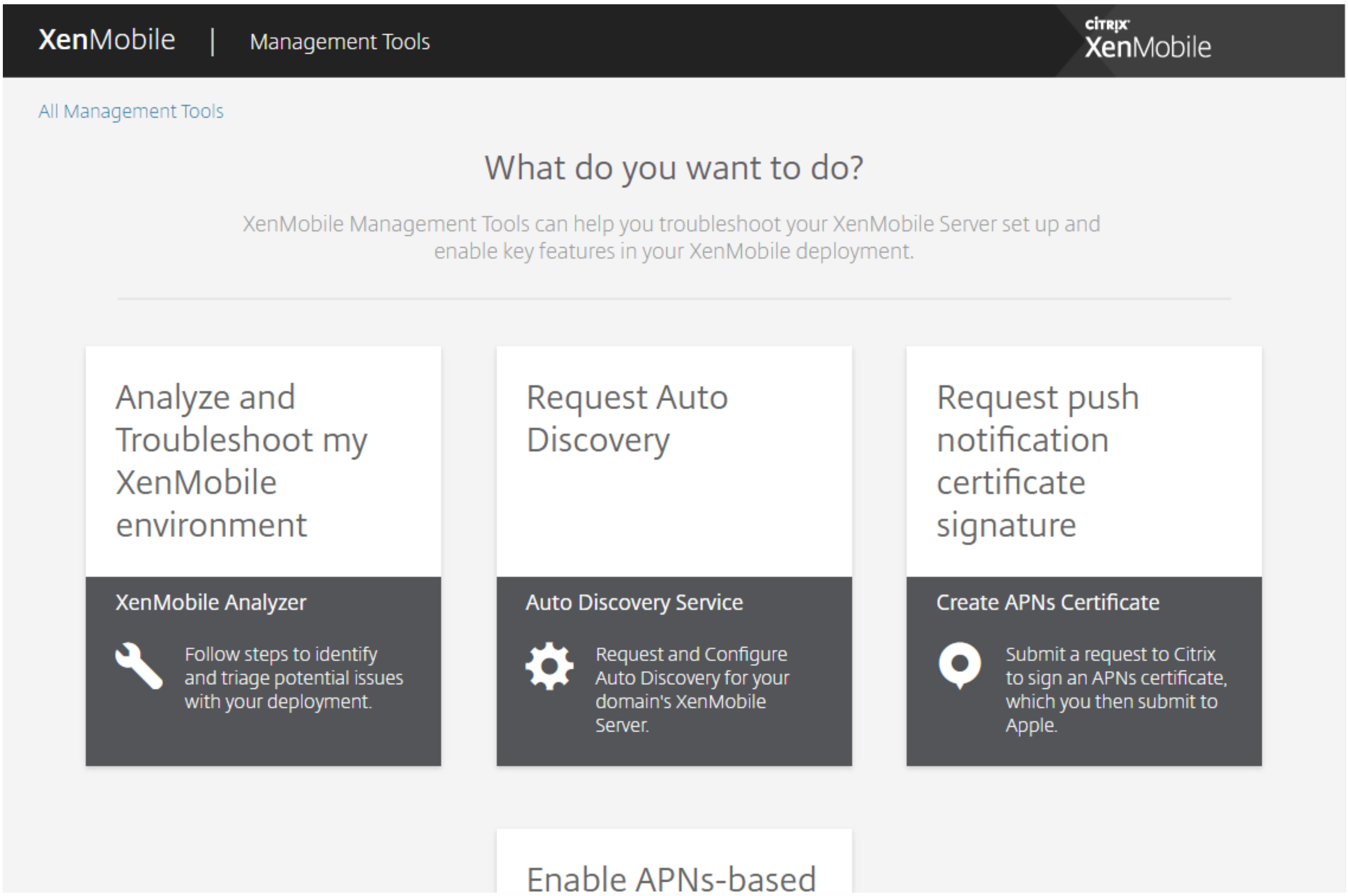
Note: This video contains no audio sound. It is best viewed in full screen mode.

Prerequisites

Product	Supported Version
XenMobile Server	10.3.0 and later
NetScaler Gateway	10.5 and later
Client Enrollment Simulation	iOS and Android

Access the XenMobile Analyzer by using either of these methods:

- In the XenMobile 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://tools.xm.cloud.com. On the XenMobile Management Tools page that appears, to start XenMobile Analyzer, click **Analyze and Troubleshoot my XenMobile Environment**.


XenMobile | Management Tools

All Management Tools

What do you want to do?

XenMobile Management Tools can help you troubleshoot your XenMobile Server set up and enable key features in your XenMobile deployment.

Analyze and Troubleshoot my XenMobile environment

XenMobile Analyzer

Follow steps to identify and triage potential issues with your deployment.

Request Auto Discovery

Auto Discovery Service

Request and Configure Auto Discovery for your domain's XenMobile Server.

Request push notification certificate signature

Create APNs Certificate

Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.

Enable APNs-based

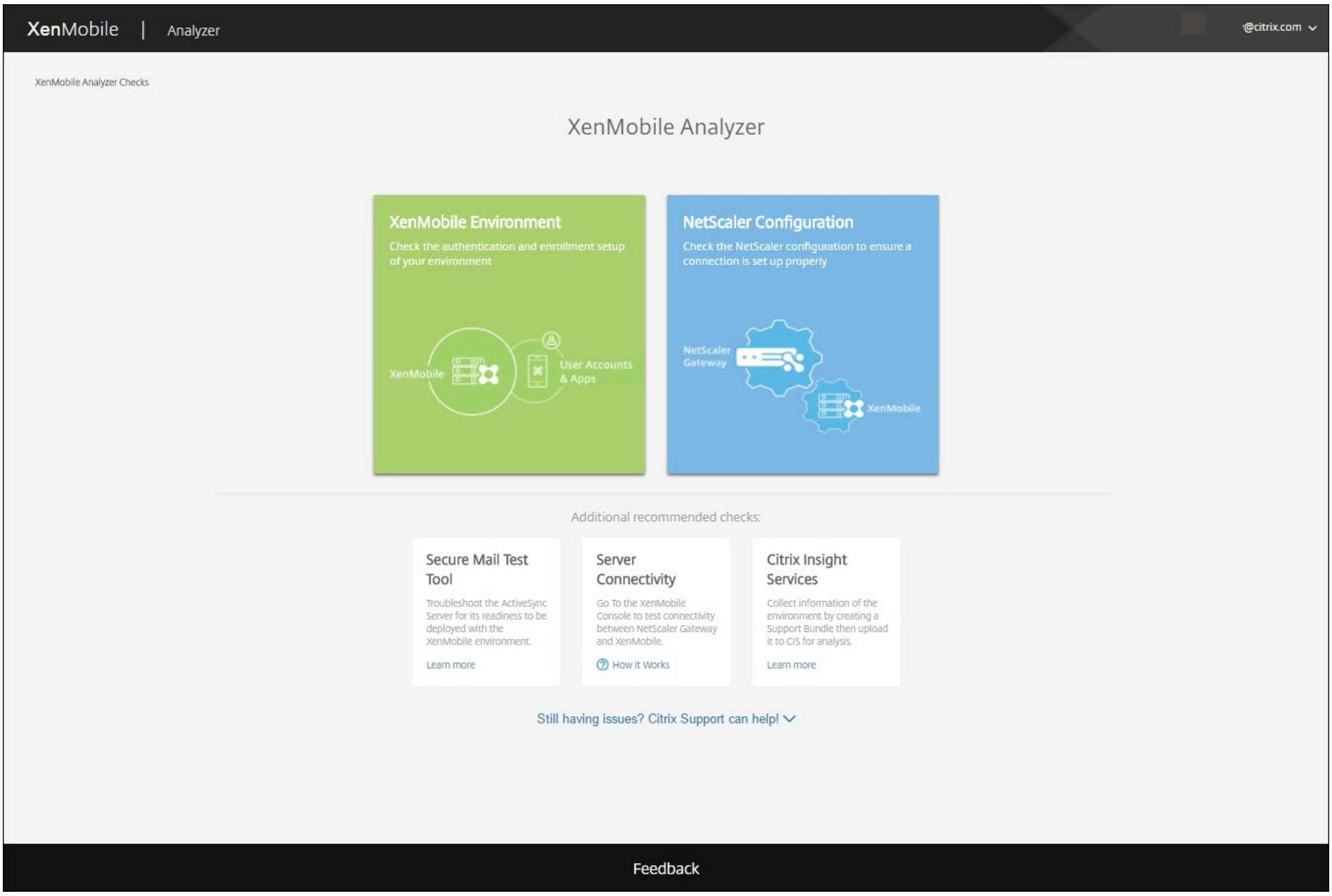
XenMobile Analyzer contains five options designed to lead you through the triage process and reduce the number of support tickets. The options can lower costs for everyone.

The options are as follows:

- **Environment Check** - This step guides you in setting up tests to check your setup for issues. The step also provides recommendations and solutions on device, user enrollment, and authentication issues.
- **NetScaler Check** - This step guides you in checking your NetScaler configurations for XenMobile deployment readiness.
- **Advanced Diagnostics** - This step provides information on using Citrix Insight Services to find further issues that the environment check might have missed.
- **Secure Mail Readiness** - This step directs you to download the XenMobile Exchange ActiveSync Test application. This tool helps troubleshoot the ActiveSync servers for their readiness to be deployed with a XenMobile environment.
- **Server Connectivity Checks** - This step instructs you to test the connectivity of your servers.
- **Contact Citrix support** - If you are still having issues, this step links you to the site where you can create a Citrix support case.

The following sections describe each option in more detail.

1. Log on to XenMobile Analyzer and click **XenMobile Environment**.



XenMobile Analyzer

XenMobile Environment

Check the authentication and enrollment setup of your environment

NetScaler Configuration

Check the NetScaler configuration to ensure a connection is set up properly

Additional recommended checks:

Secure Mail Test Tool

Troubleshoot the ActiveSync Server for its readiness to be deployed with the XenMobile environment.

Learn more

Server Connectivity

Go To the XenMobile Console to test connectivity between NetScaler Gateway and XenMobile.

How it Works

Citrix Insight Services

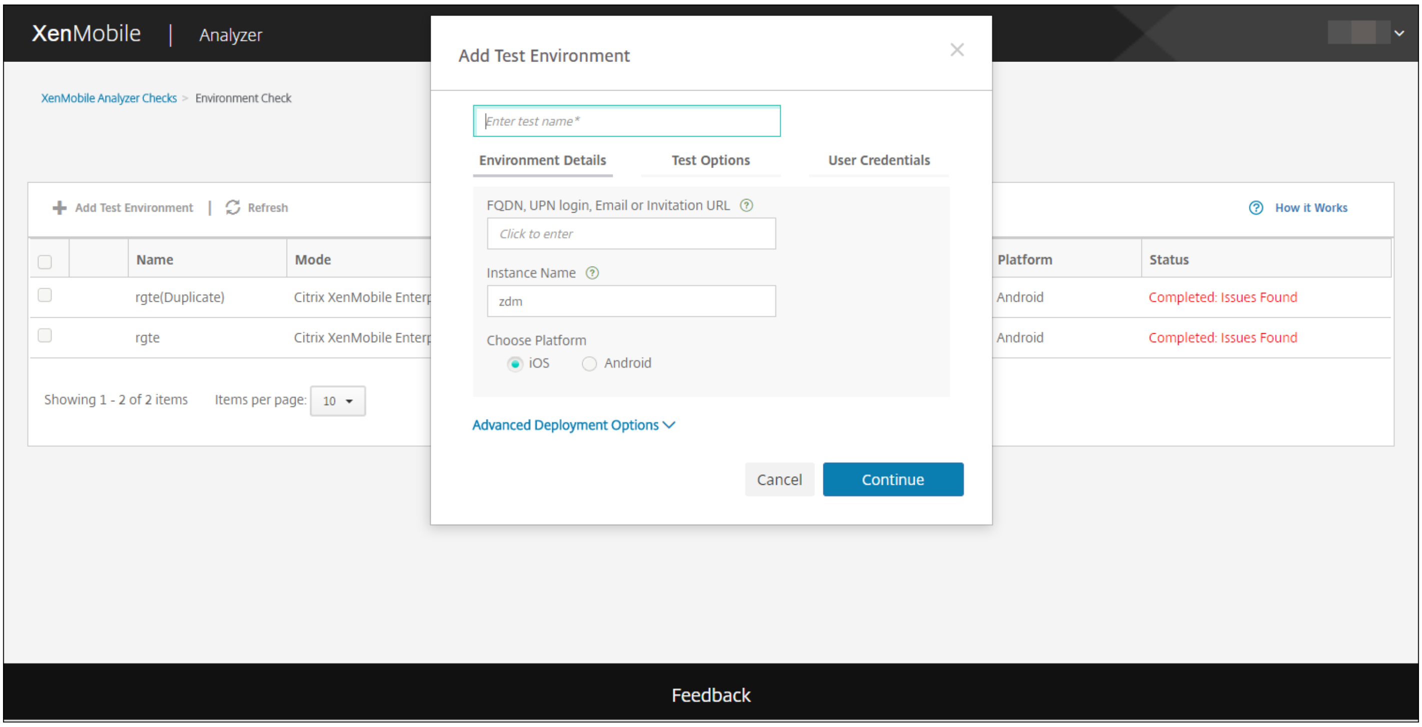
Collect information of the environment by creating a Support Bundle then upload it to CIS for analysis.

Learn more

Still having issues? Citrix Support can help!

2. Click **Add Test Environment**.

3. In the new **Add Test Environment** dialog box, do the following:



FQDN, UPN login, Email or Invitation URL: Click to enter

Instance Name: zdm

Choose Platform: ● iOS ○ Android

Name	Mode	Platform	Status
rgte(Duplicate)	Citrix XenMobile Enterp	Android	Completed: Issues Found
rgte	Citrix XenMobile Enterp	Android	Completed: Issues Found

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**, enter the information that is used to access the server.

c. In **Instance Name**, if you use a custom instance, you can provide that value.

d. In **Choose Platform**, select either **iOS** or **Android** as the platform for testing.

e. If you expand **Advanced Deployment Options**, in the **Deployment Mode** list, you can select your XenMobile deployment mode. Available options are **Enterprise (MDM + MAM)**, **App Management (MAM)**, or **Device Management (MDM)**.

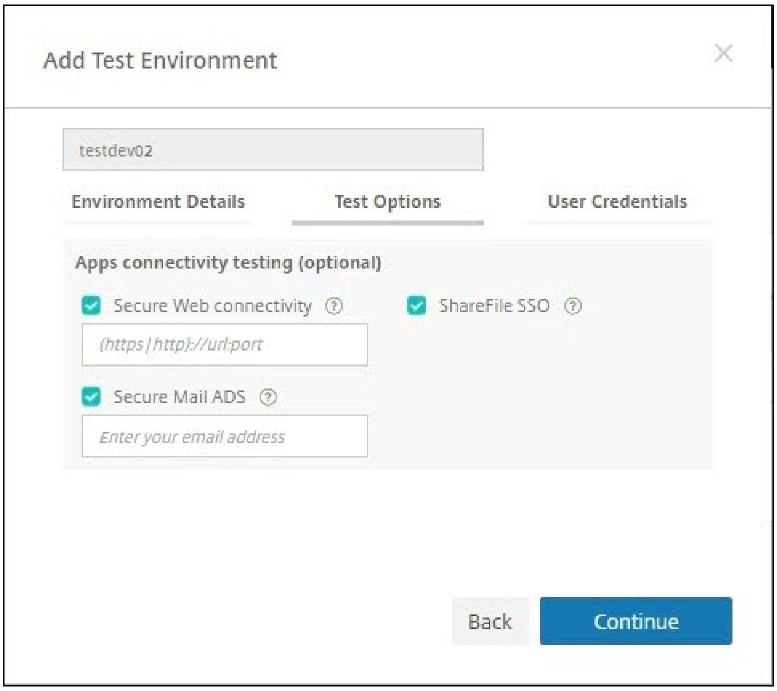
d. Click **Continue**.

4. On the **Test Options** tab, choose one or more of the following tests and then click **Continue**.

a. 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 the Secure Web app while trying to reach intranet URLs.

b. Secure Mail ADS. Provide a user email ID. This ID is used to test the autodiscovery of the Microsoft Exchange Server in your XenMobile environment. It detects if there are any issues related to Secure Mail Auto Discovery.

c. ShareFile SSO. If selected, XenMobile 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.



Add Test Environment

testdev02

Environment Details | Test Options | User Credentials

Apps connectivity testing (optional)

☑ Secure Web connectivity

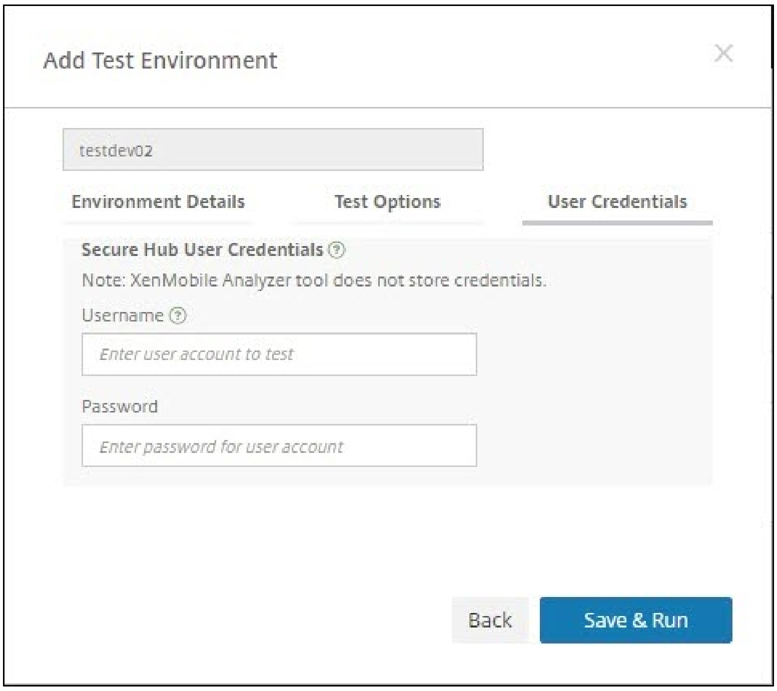
(https|http)://url:port

☑ ShareFile SSO

☑ Secure Mail ADS

Enter your email address

5. On the **User Credentials** tab, depending on your server setup, you see different fields. The possible fields are **Username**, **Username and Password**, or **Username, Password**, and **Enrollment PIN**.



Add Test Environment

testdev02

Environment Details | Test Options | User Credentials

Secure Hub User Credentials

Note: XenMobile Analyzer tool does not store credentials.

Username

Enter user account to test

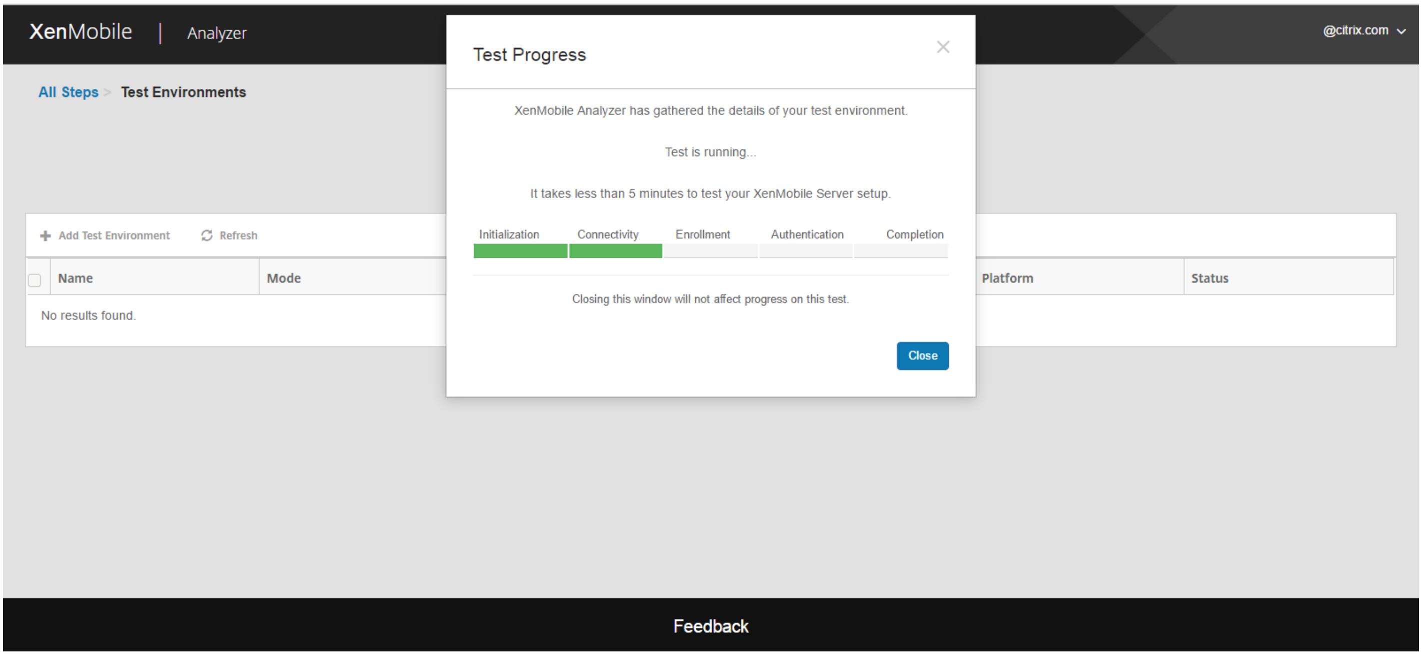
Password

Enter password for user account

6. 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 have passed appear in green. Tests that fail appear as red.



Test Progress

XenMobile Analyzer has gathered the details of your test environment.

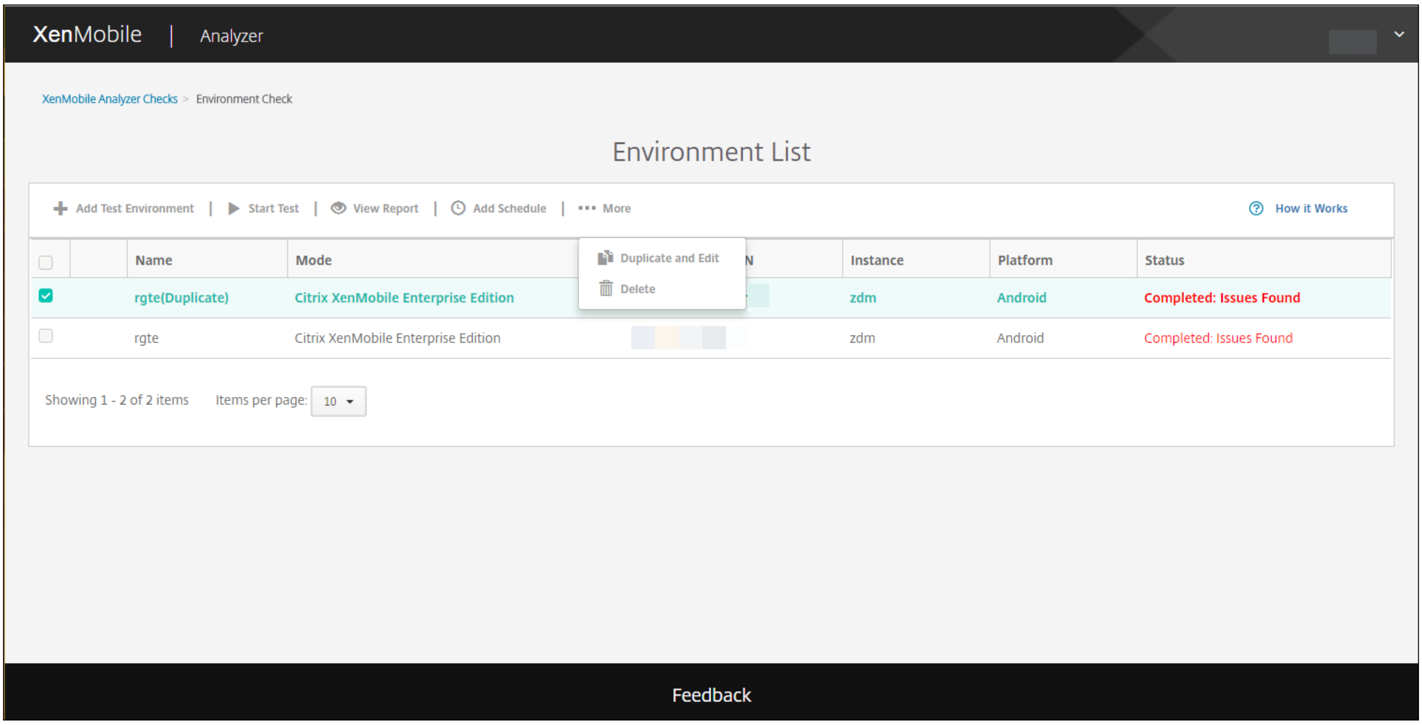
Test is running...

It takes less than 5 minutes to test your XenMobile Server setup.

Closing this window will not affect progress on this test.

No results found.

After closing the progress dialog box, you return to the **Environments List** page.



Environment List

	Name	Mode	N	Instance	Platform	Status
☑	rgte(Duplicate)	Citrix XenMobile Enterprise Edition		zdm	Android	Completed: Issues Found
□	rgte	Citrix XenMobile Enterprise Edition		zdm	Android	Completed: Issues Found

Showing 1 - 2 of 2 items   Items per page: 10

The **Results** page shows Test Details, Recommendations, and Results.

7. Click the **View Report** icon to see test results.

If recommendations have Citrix Knowledge Base articles associated with them, the articles are listed on this page.

8. Click the **Results** tab to display the individual Category and Tests that the tool performed, with their results.

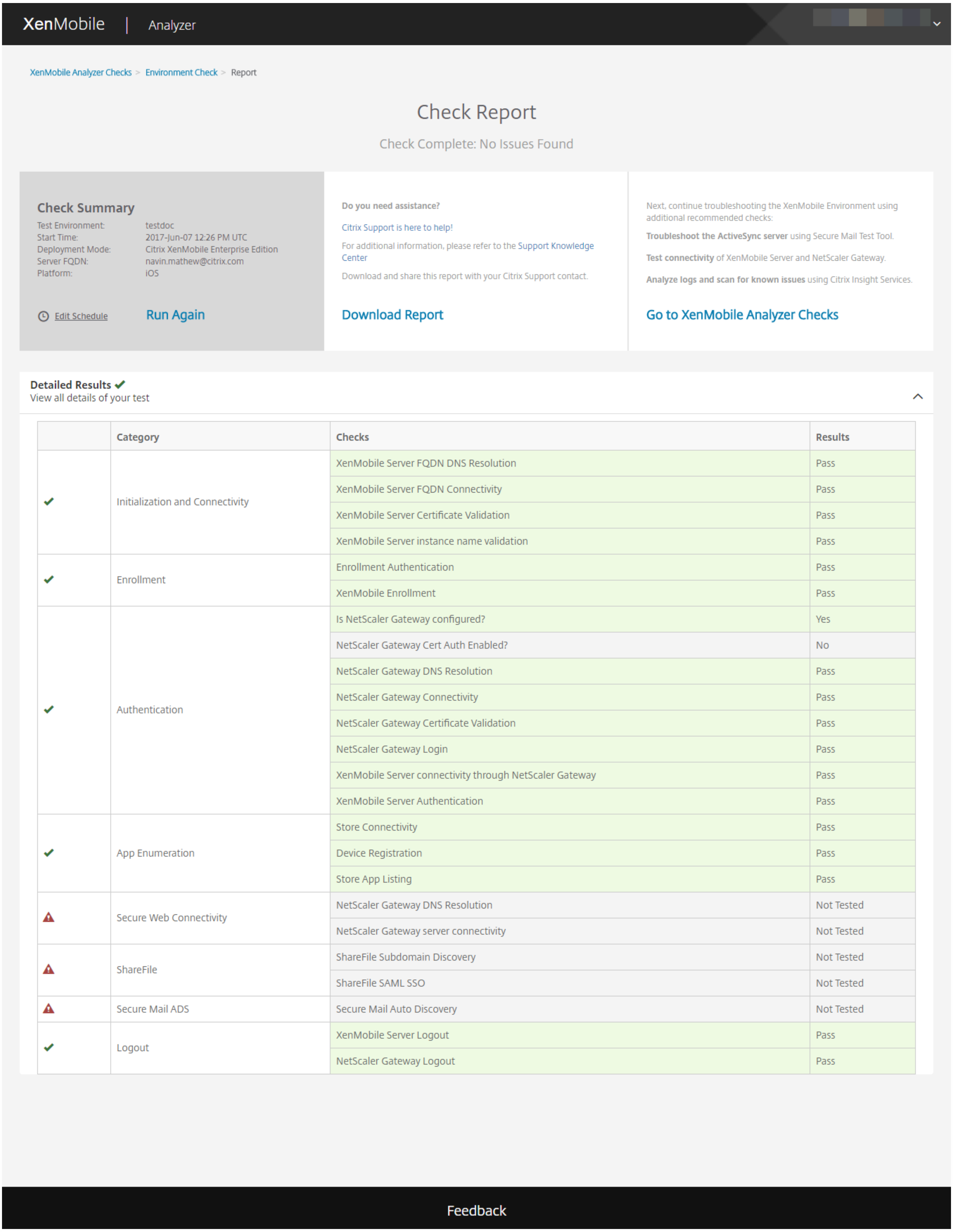
a. To download the report, click **Download Report**.

b. To return to the list of test environments, click **Environment Check**.

c. To rerun the same test, click **Run Again**.

d. If you want to rerun another test, go back to **Test Environments**, select the test, and click **Start Test**.

e. To select another XenMobile Analyzer option, click **Go To XenMobile Analyzer Checks**.



XenMobile | Analyzer [redacted]

XenMobile Analyzer Checks > Environment Check > Report

Check Report

Check Complete: No Issues Found

Check Summary

Test Environment: testdoc
Start Time: 2017-Jun-07 12:26 PM UTC
Deployment Mode: Citrix XenMobile Enterprise Edition
Server FQDN: navin.mathew@citrix.com
Platform: iOS

Edit Schedule   Run Again

Do you need assistance?

Citrix Support is here to help!

For additional information, please refer to the Support Knowledge Center

Download and share this report with your Citrix Support contact.

Download Report

Next, continue troubleshooting the XenMobile Environment using additional recommended checks:

Troubleshoot the ActiveSync server using Secure Mail Test Tool.

Test connectivity of XenMobile Server and NetScaler Gateway.

Analyze logs and scan for known issues using Citrix Insight Services.

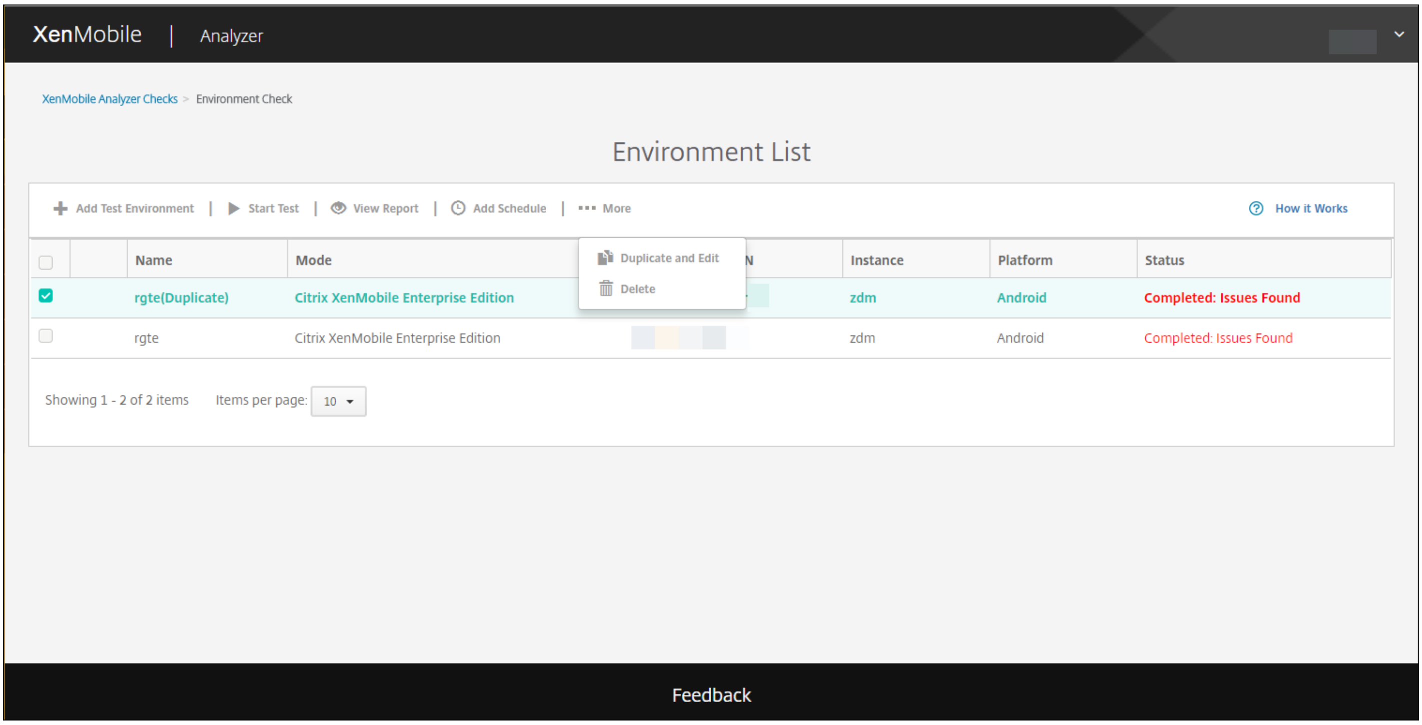
Go to XenMobile Analyzer Checks

Detailed Results ✓
View all details of your test

	Category	Checks	Results
✓	Initialization and Connectivity	XenMobile Server FQDN DNS Resolution	Pass
		XenMobile Server FQDN Connectivity	Pass
		XenMobile Server Certificate Validation	Pass
		XenMobile Server instance name validation	Pass
✓	Enrollment	Enrollment Authentication	Pass
		XenMobile Enrollment	Pass
✓	Authentication	Is NetScaler Gateway configured?	Yes
		NetScaler Gateway Cert Auth Enabled?	No
		NetScaler Gateway DNS Resolution	Pass
		NetScaler Gateway Connectivity	Pass
		NetScaler Gateway Certificate Validation	Pass
		NetScaler Gateway Login	Pass
		XenMobile Server connectivity through NetScaler Gateway	Pass
		XenMobile Server Authentication	Pass
✓	App Enumeration	Store Connectivity	Pass
		Device Registration	Pass
		Store App Listing	Pass
⚠	Secure Web Connectivity	NetScaler Gateway DNS Resolution	Not Tested
		NetScaler Gateway server connectivity	Not Tested
⚠	ShareFile	ShareFile Subdomain Discovery	Not Tested
		ShareFile SAML SSO	Not Tested
⚠	Secure Mail ADS	Secure Mail Auto Discovery	Not Tested
✓	Logout	XenMobile Server Logout	Pass
		NetScaler Gateway Logout	Pass

9. From the Test Environments page, you can copy and edit tests. To do so, select a test and then click **More** and select **Duplicate and Edit**.

A copy of the selected test is created and the Add Test Environment dialog opens, allowing you to modify the new test.



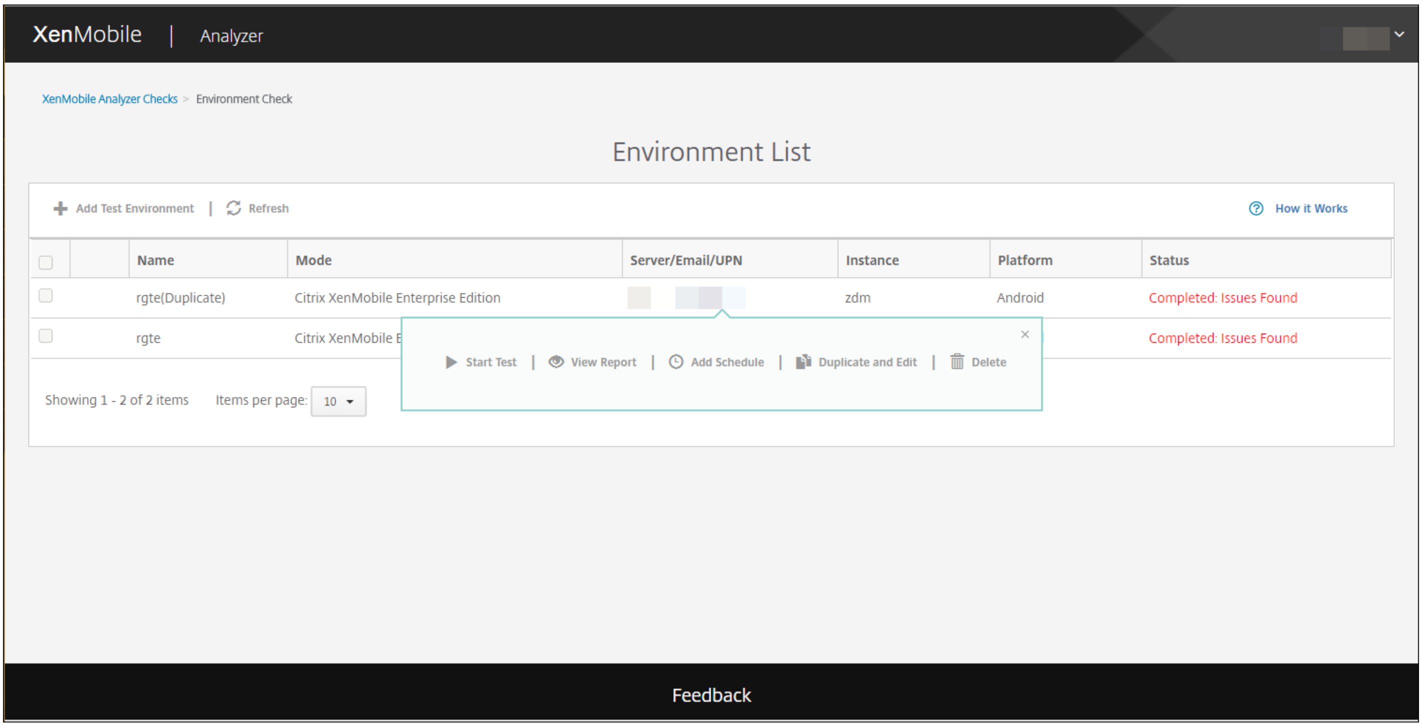
XenMobile | Analyzer
XenMobile Analyzer Checks > Environment Check

Environment List

+ Add Test Environment | ▶ Start Test | View Report | Add Schedule | ••• More
How it Works
Duplicate and Edit
Delete

□	Name	Mode	N	Instance	Platform	Status
☑	rgte(Duplicate)	Citrix XenMobile Enterprise Edition	[redacted]	zdm	Android	Completed: Issues Found
□	rgte	Citrix XenMobile Enterprise Edition	[redacted]	zdm	Android	Completed: Issues Found

Showing 1 - 2 of 2 items   Items per page: 10



XenMobile | Analyzer
XenMobile Analyzer Checks > Environment Check

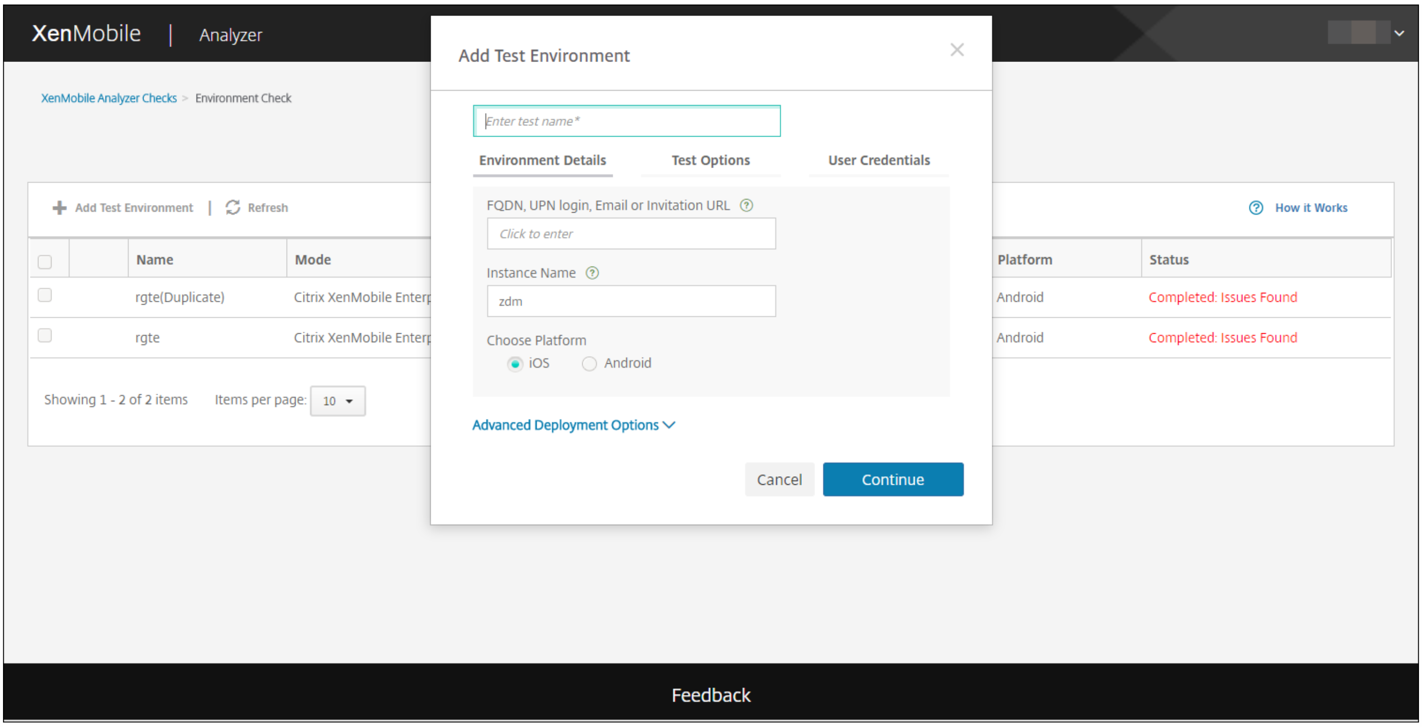
Environment List

+ Add Test Environment | Refresh
How it Works

□	Name	Mode	Server/Email/UPN	Instance	Platform	Status
□	rgte(Duplicate)	Citrix XenMobile Enterprise Edition	[redacted]	zdm	Android	Completed: Issues Found
□	rgte	Citrix XenMobile E				Completed: Issues Found

▶ Start Test | View Report | Add Schedule | Duplicate and Edit | Delete
×

Showing 1 - 2 of 2 items   Items per page: 10



XenMobile | Analyzer

XenMobile Analyzer Checks > Environment Check

Add Test Environment

Enter test name*

Environment Details | Test Options | User Credentials

FQDN, UPN login, Email or Invitation URL: Click to enter

Instance Name: zdm

Choose Platform: ● iOS ○ Android

Advanced Deployment Options

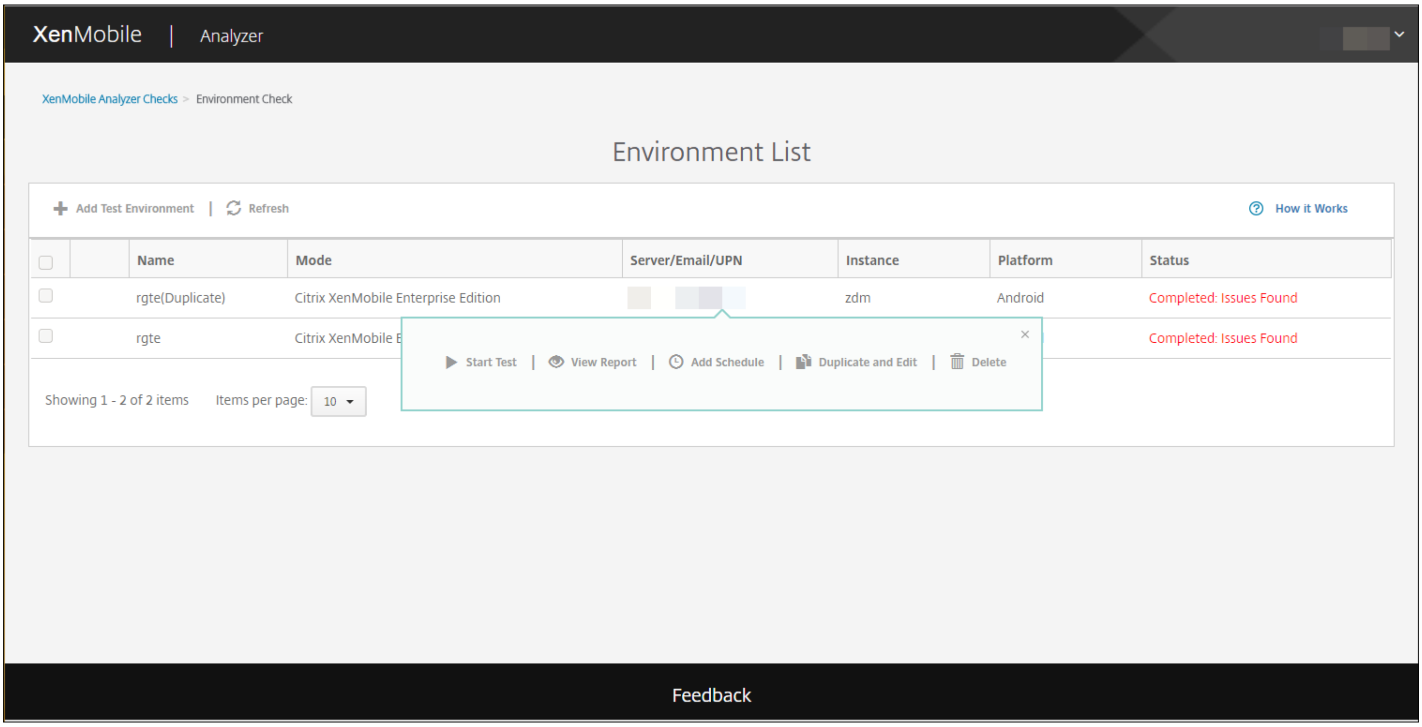
Cancel | Continue

□	Name	Mode	Platform	Status
□	rgte(Duplicate)	Citrix XenMobile Enterp	Android	Completed: Issues Found
□	rgte	Citrix XenMobile Enterp	Android	Completed: Issues Found

Showing 1 - 2 of 2 items Items per page: 10

You can configure tests to run on an automatic schedule with results sent to a list of users you configure.

1. On the **Environment List** page, select the environment for which you want to set up a schedule and click **Add Schedule**.



XenMobile | Analyzer

XenMobile Analyzer Checks > Environment Check

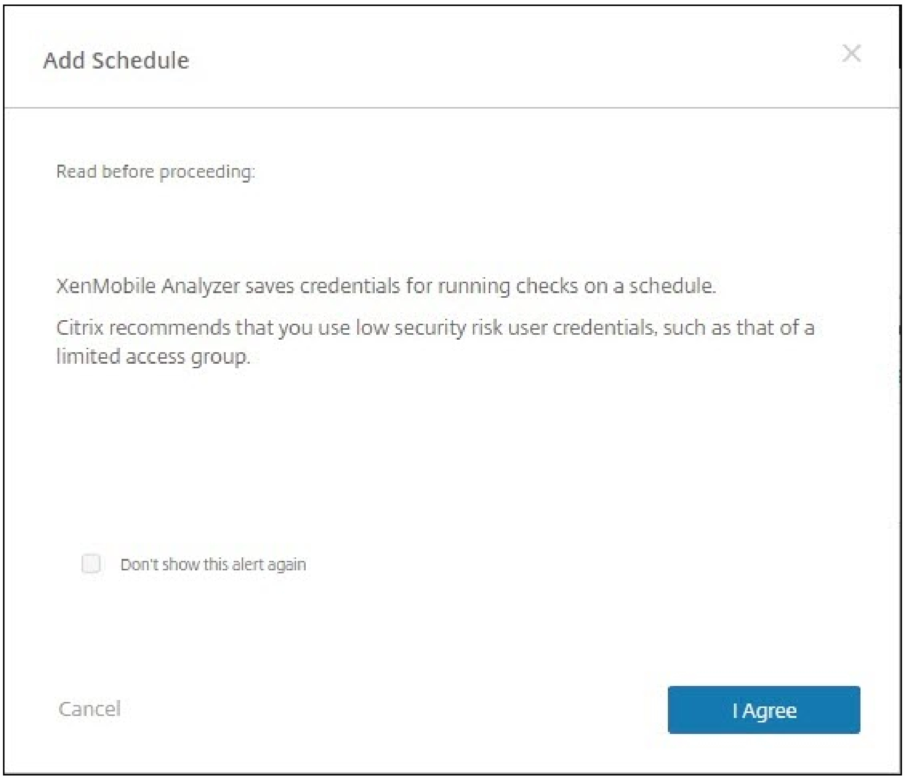
Environment List

□	Name	Mode	Server/Email/UPN	Instance	Platform	Status
□	rgte(Duplicate)	Citrix XenMobile Enterprise Edition		zdm	Android	Completed: Issues Found
□	rgte	Citrix XenMobile E				Completed: Issues Found

Showing 1 - 2 of 2 items Items per page: 10

2. The **Add Schedule** window displays a message warning you that XenMobile 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.



Add Schedule

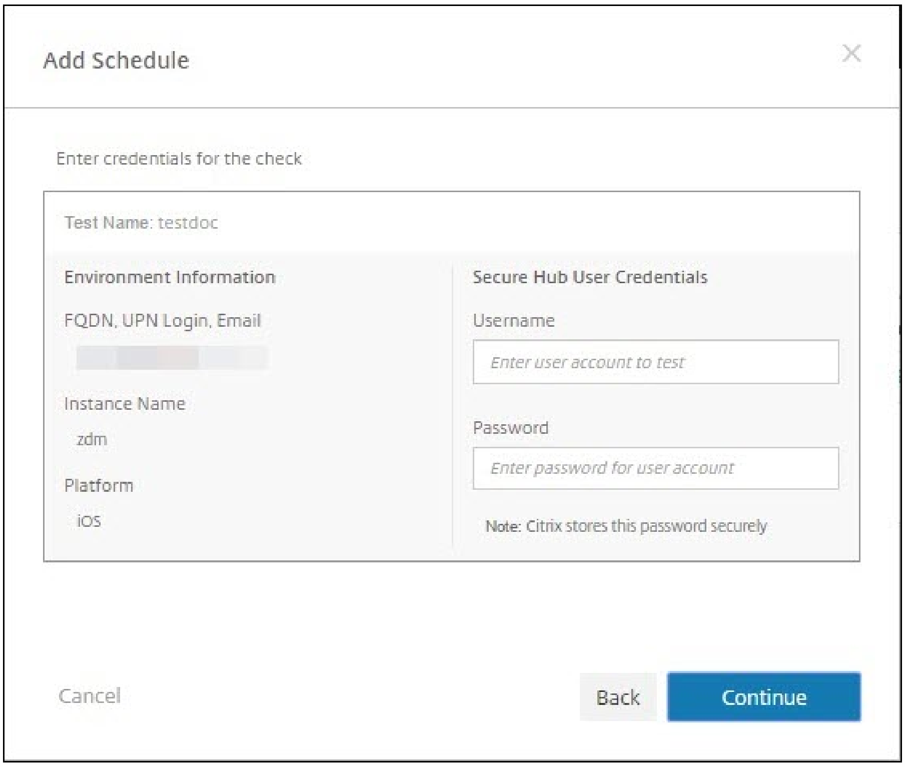
Read before proceeding:

XenMobile Analyzer saves credentials for running checks on a schedule.

Citrix recommends that you use low security risk user credentials, such as that of a limited access group.

□ Don't show this alert again

3. Enter a **Username** and **Password** for running the test.



Add Schedule

Enter credentials for the check

Test Name: testdoc

Environment Information

FQDN, UPN Login, Email
[redacted]

Instance Name
zdm

Platform
iOS

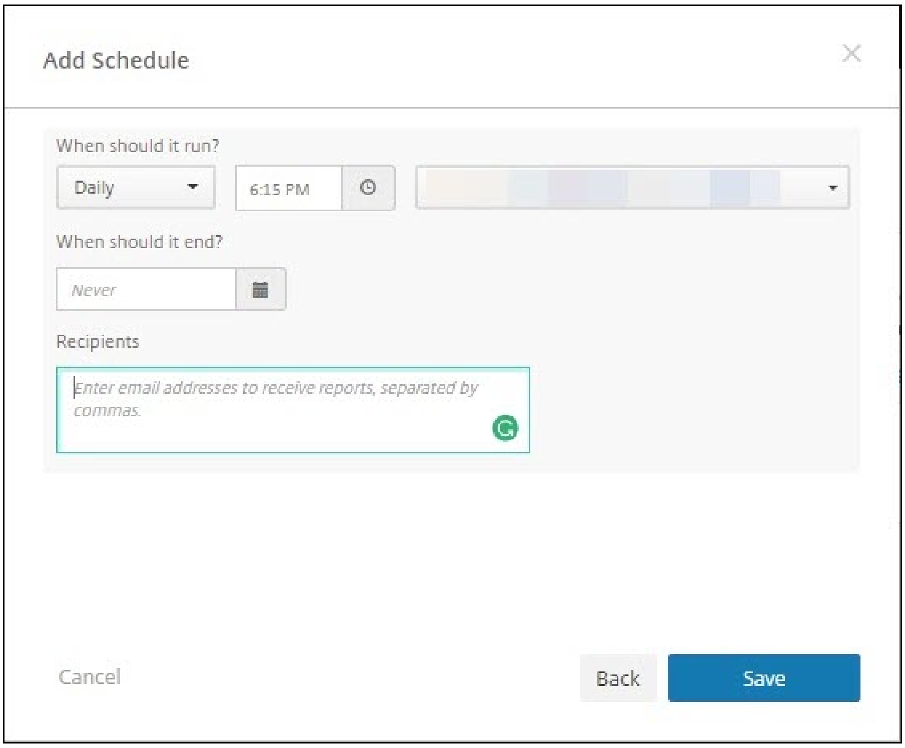
Secure Hub User Credentials

Username
Enter user account to test

Password
Enter password for user account

Note: Citrix stores this password securely

4. Configure a schedule for the test to run. You can select **Daily** or **Weekly** from the drop-down. Select a time of day for the test to run and a time zone. 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. Enter a list of email addresses to receive reports, separated by commas. Click **Save**.



Add Schedule

When should it run?

Daily | 6:15 PM

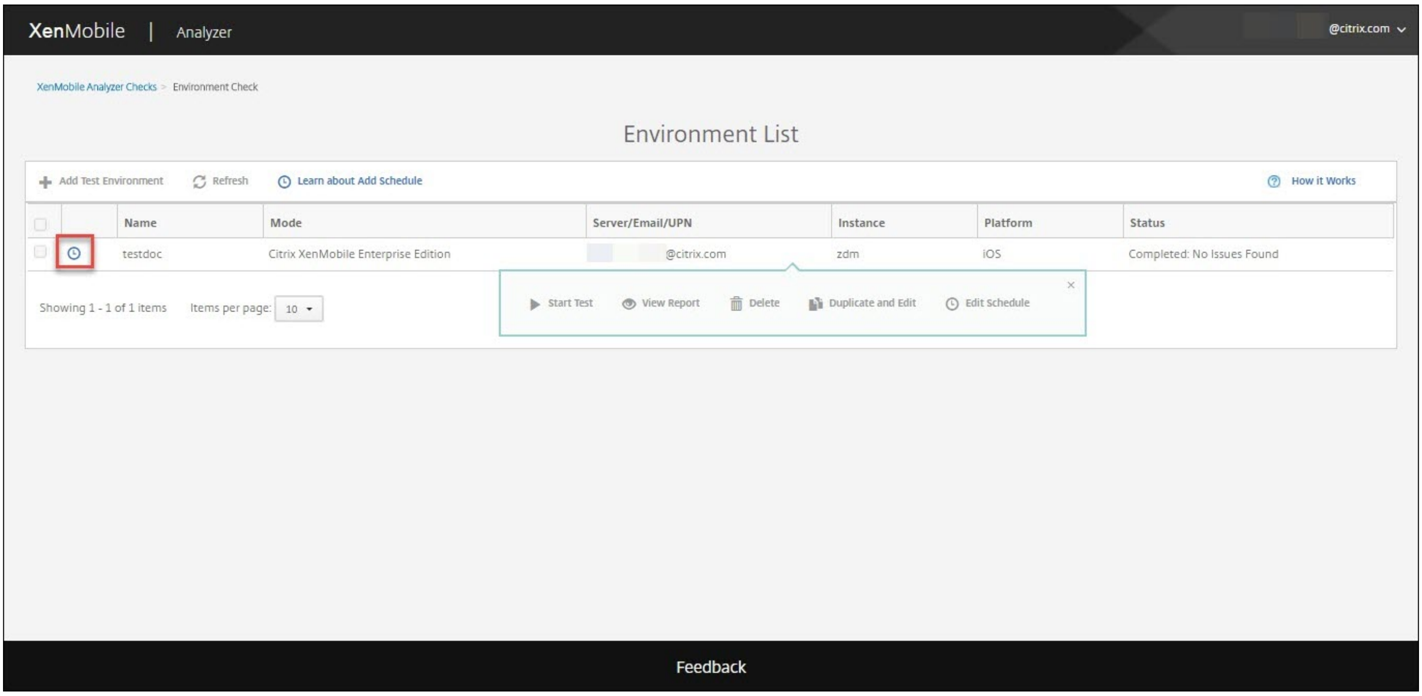
When should it end?

Never

Recipients

Enter email addresses to receive reports, separated by commas.

5. A clock symbol to the left of your test indicates that a schedule is configured. If you select your test, you can click **Edit Schedule** to change when the test runs.

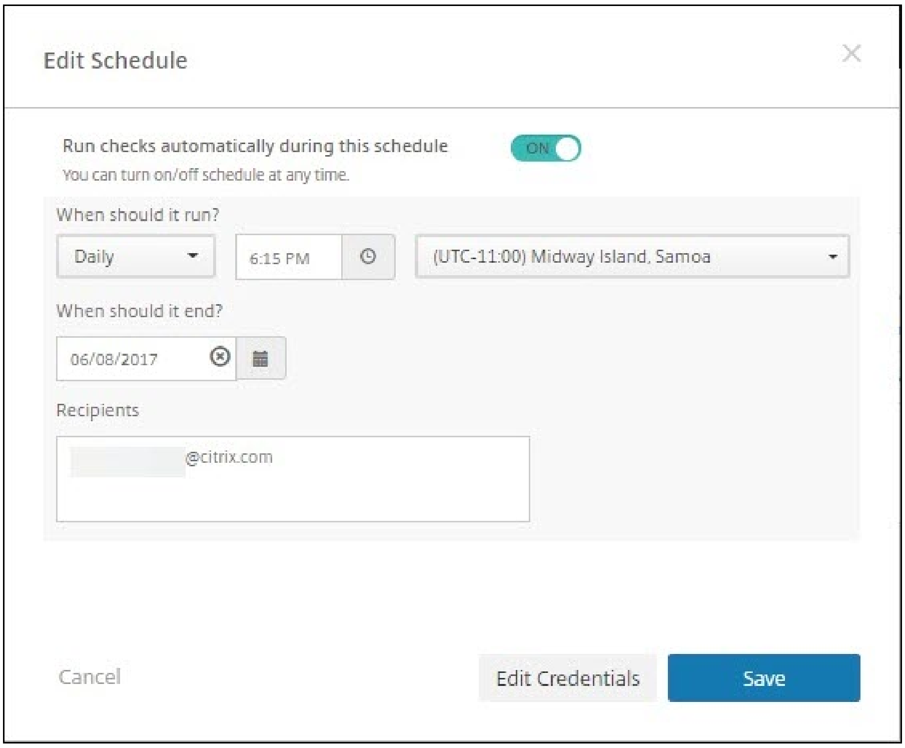


Environment List

		Name	Mode	Server/Email/UPN	Instance	Platform	Status
□		testdoc	Citrix XenMobile Enterprise Edition	@citrix.com	zdm	iOS	Completed: No Issues Found

Showing 1 - 1 of 1 items Items per page: 10

6. In this window, you can change when the test runs. You can also disable it, by clicking the switch at the top. Click **Save** when you're done.



Edit Schedule

Run checks automatically during this schedule ON

You can turn on/off schedule at any time.

When should it run?

Daily | 6:15 PM | (UTC-11:00) Midway Island, Samoa

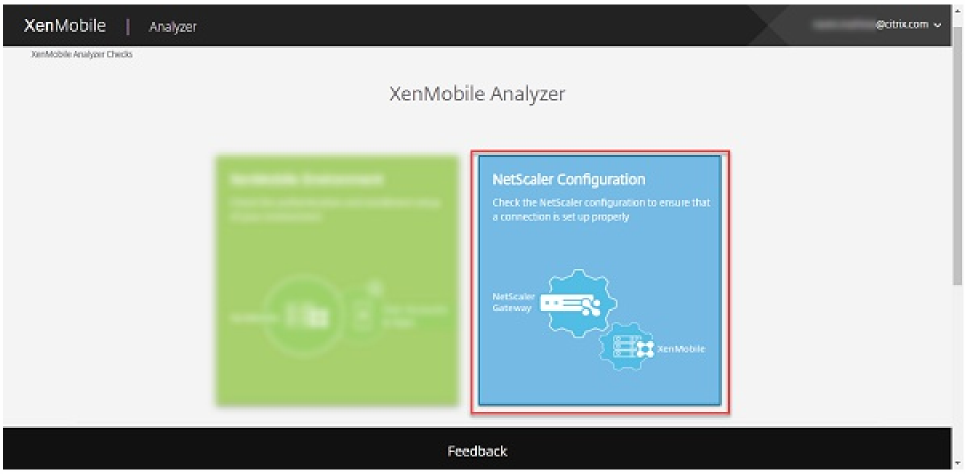
When should it end?

06/08/2017

Recipients

[redacted]@citrix.com

1. Log on to XenMobile Analyzer and then click **NetScaler Configuration**.



XenMobile | Analyzer

XenMobile Analyzer Checks

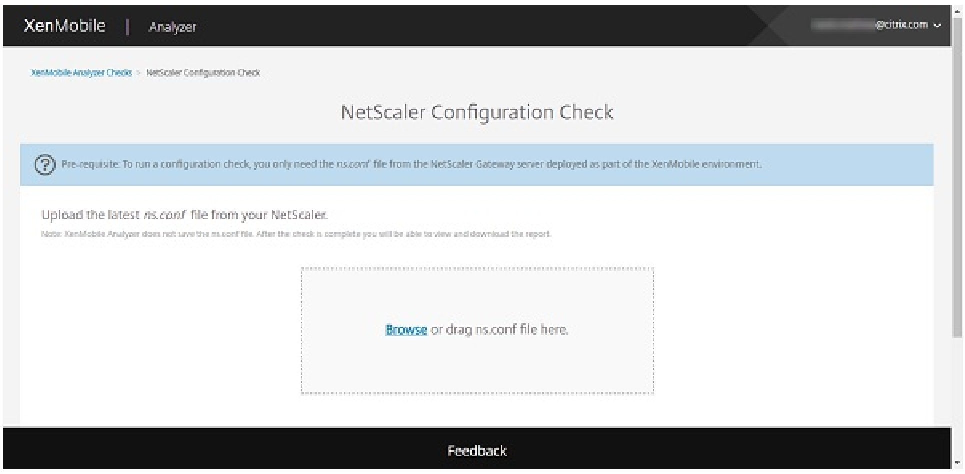
[redacted]@citrix.com

XenMobile Analyzer

NetScaler Configuration

Check the NetScaler configuration to ensure that a connection is set up properly

2. Upload the latest ns.conf file from your instance of NetScaler. 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.



XenMobile | Analyzer [redacted]@citrix.com

XenMobile Analyzer Checks > NetScaler Configuration Check

NetScaler Configuration Check

Pre-requisite: To run a configuration check, you only need the *ns.conf* file from the NetScaler Gateway server deployed as part of the XenMobile environment.

Upload the latest *ns.conf* file from your NetScaler.

Note: XenMobile Analyzer does not save the ns.conf file. After the check is complete you will be able to view and download the report.

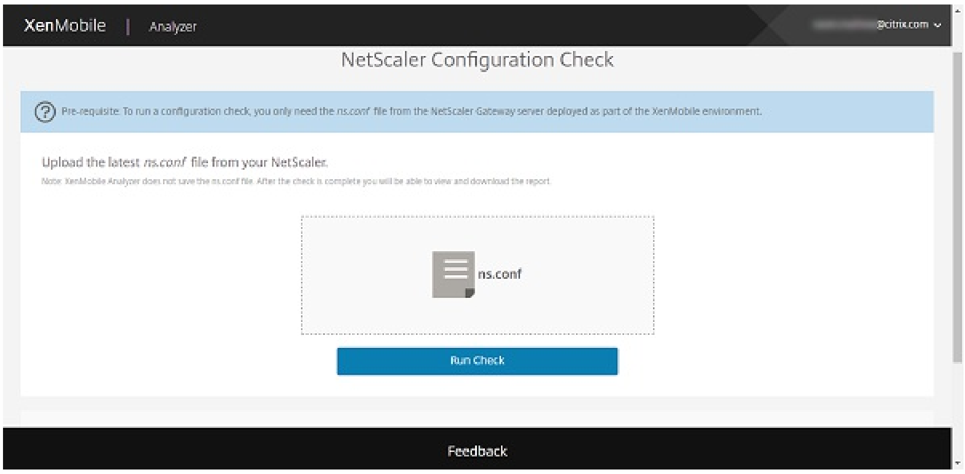
Browse or drag ns.conf file here.

Feedback

Note

XenMobile Analyzer does not save the ns.conf file. After the check is complete, you can view and download the report.

3. Click **Run Check**.



XenMobile | Analyzer [redacted]@citrix.com

NetScaler Configuration Check

Pre-requisite: To run a configuration check, you only need the *ns.conf* file from the NetScaler Gateway server deployed as part of the XenMobile environment.

Upload the latest *ns.conf* file from your NetScaler.

Note: XenMobile Analyzer does not save the ns.conf file. After the check is complete you will be able to view and download the report.

ns.conf

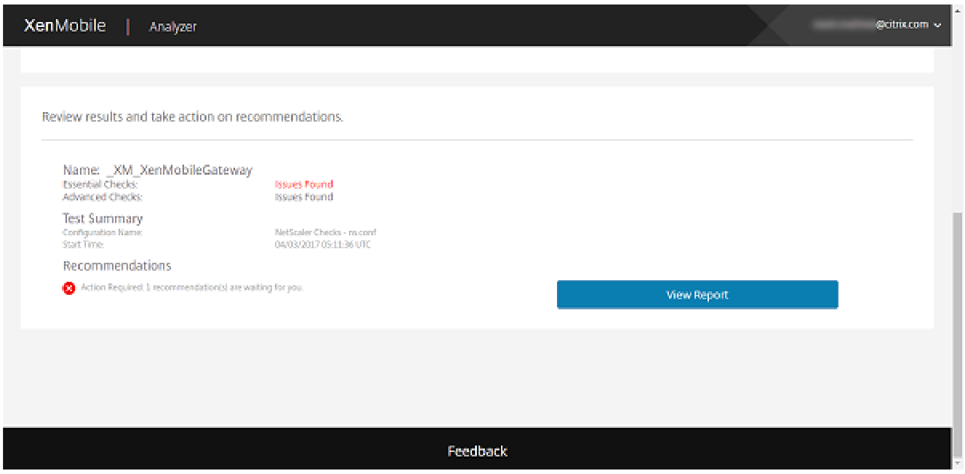
Run Check

Feedback

XenMobile Analyzer runs two types of configuration checks.

- Essential Checks looks for components that are critical for a successful XenMobile deployment.
- Advanced Checks looks for components that are not critical, but are complementary to XenMobile deployments.

4. To view recommendations on Essential and Advanced Checks for NetScaler, click **View Report**.



Review results and take action on recommendations.

Name: _XM_XenMobileGateway

Essential Checks:	Issues Found
Advanced Checks:	Issues Found

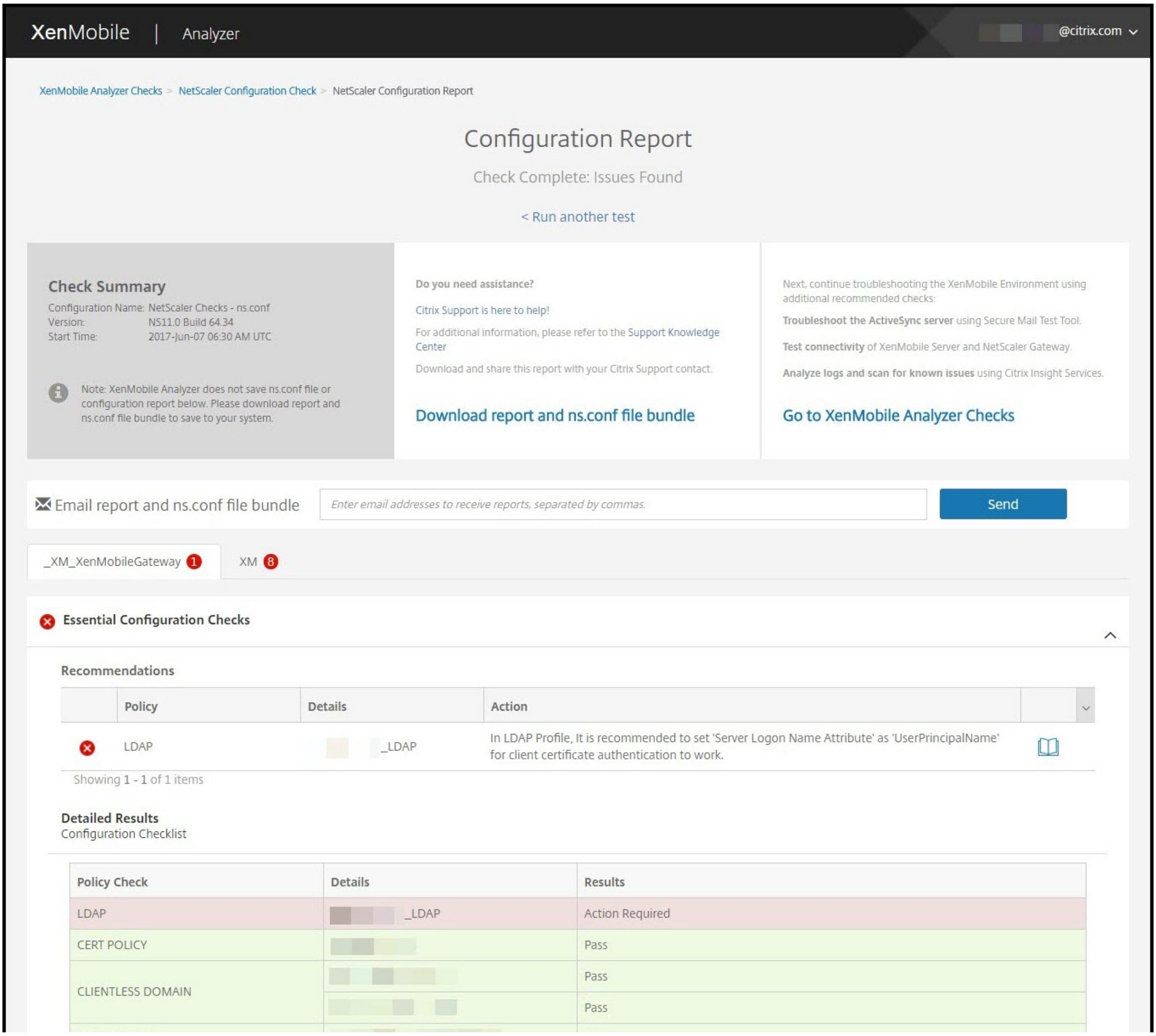
Test Summary

Configuration Name:	NetScaler Checks - ns.conf
Start Time:	04/03/2017 05:11:36 UTC

Recommendations

Action Required: 1 recommendation(s) are waiting for you.

The **Configuration Report** page appears.



XenMobile Analyzer Checks > NetScaler Configuration Check > NetScaler Configuration Report

Configuration Report

Check Complete: Issues Found

< Run another test

Check Summary

Configuration Name:	NetScaler Checks - ns.conf
Version:	NS11.0 Build 64.34
Start Time:	2017-Jun-07 06:30 AM UTC

Note: XenMobile Analyzer does not save ns.conf file or configuration report below. Please download report and ns.conf file bundle to save to your system.

Do you need assistance?

Citrix Support is here to help!

For additional information, please refer to the Support Knowledge Center

Download and share this report with your Citrix Support contact.

Download report and ns.conf file bundle

Next, continue troubleshooting the XenMobile Environment using additional recommended checks:

Troubleshoot the ActiveSync server using Secure Mail Test Tool.

Test connectivity of XenMobile Server and NetScaler Gateway.

Analyze logs and scan for known issues using Citrix Insight Services.

Go to XenMobile Analyzer Checks

Email report and ns.conf file bundle

Enter email addresses to receive reports, separated by commas.

Essential Configuration Checks

Recommendations

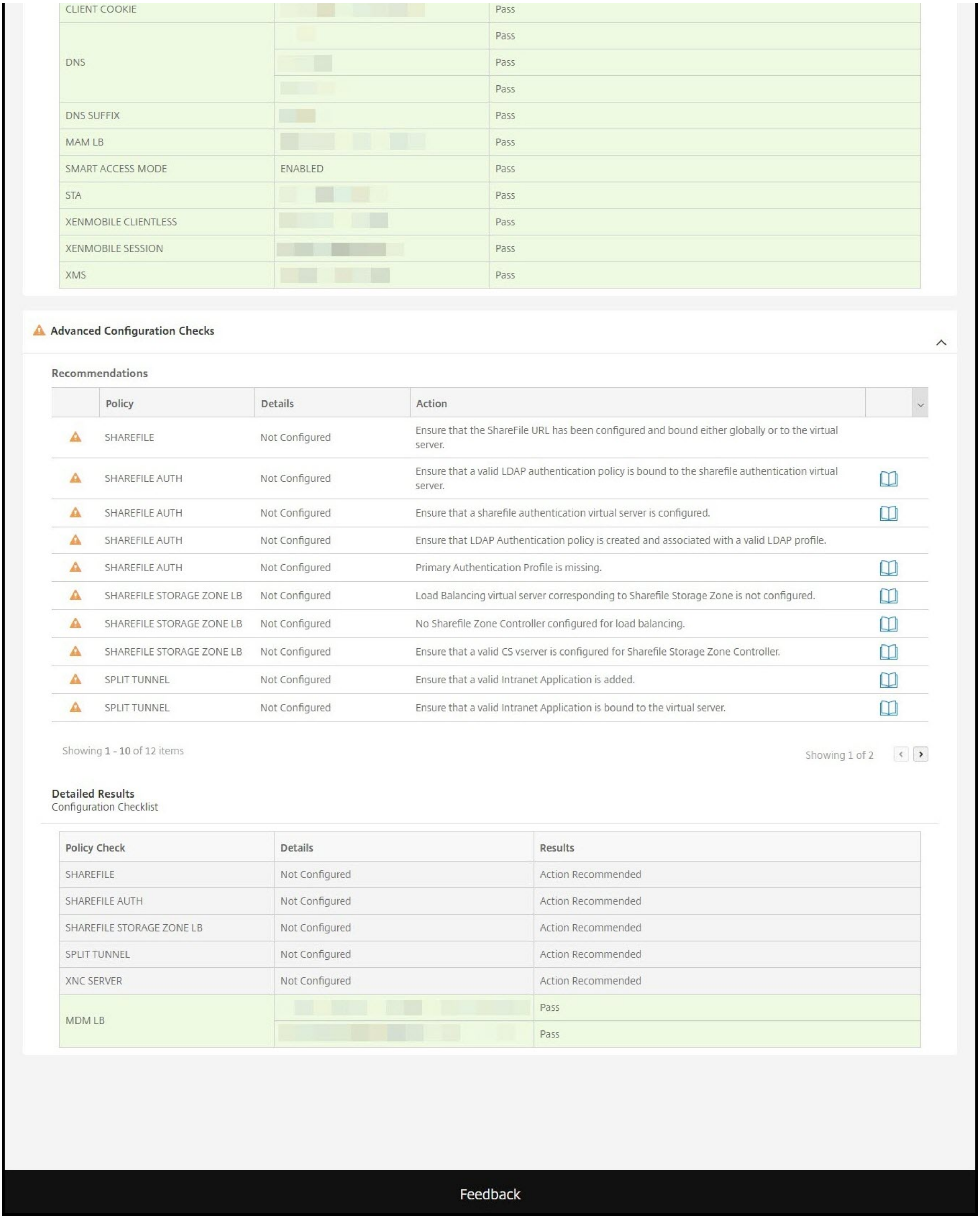
	Policy	Details	Action	
☒	LDAP	[redacted]_LDAP	In LDAP Profile, It is recommended to set 'Server Logon Name Attribute' as 'UserPrincipalName' for client certificate authentication to work.	📖

Showing 1 - 1 of 1 items

Detailed Results

Configuration Checklist

Policy Check	Details	Results
LDAP	[redacted]_LDAP	Action Required
CERT POLICY	[redacted]	Pass
CLIENTLESS DOMAIN	[redacted]	Pass
	[redacted]	Pass



CLIENT COOKIE	[redacted]	Pass
DNS	[redacted]	Pass
	[redacted]	Pass
	[redacted]	Pass
DNS SUFFIX	[redacted]	Pass
MAM LB	[redacted]	Pass
SMART ACCESS MODE	ENABLED	Pass
STA	[redacted]	Pass
XENMOBILE CLIENTLESS	[redacted]	Pass
XENMOBILE SESSION	[redacted]	Pass
XMS	[redacted]	Pass

⚠ **Advanced Configuration Checks**

Recommendations

	Policy	Details	Action	
⚠	SHAREFILE	Not Configured	Ensure that the ShareFile URL has been configured and bound either globally or to the virtual server.	
⚠	SHAREFILE AUTH	Not Configured	Ensure that a valid LDAP authentication policy is bound to the sharefile authentication virtual server.	📖
⚠	SHAREFILE AUTH	Not Configured	Ensure that a sharefile authentication virtual server is configured.	📖
⚠	SHAREFILE AUTH	Not Configured	Ensure that LDAP Authentication policy is created and associated with a valid LDAP profile.	
⚠	SHAREFILE AUTH	Not Configured	Primary Authentication Profile is missing.	📖
⚠	SHAREFILE STORAGE ZONE LB	Not Configured	Load Balancing virtual server corresponding to Sharefile Storage Zone is not configured.	📖
⚠	SHAREFILE STORAGE ZONE LB	Not Configured	No Sharefile Zone Controller configured for load balancing.	📖
⚠	SHAREFILE STORAGE ZONE LB	Not Configured	Ensure that a valid CS vserver is configured for Sharefile Storage Zone Controller.	📖
⚠	SPLIT TUNNEL	Not Configured	Ensure that a valid Intranet Application is added.	📖
⚠	SPLIT TUNNEL	Not Configured	Ensure that a valid Intranet Application is bound to the virtual server.	📖

Showing 1 - 10 of 12 items

Showing 1 of 2

Detailed Results
Configuration Checklist

Policy Check	Details	Results
SHAREFILE	Not Configured	Action Recommended
SHAREFILE AUTH	Not Configured	Action Recommended
SHAREFILE STORAGE ZONE LB	Not Configured	Action Recommended
SPLIT TUNNEL	Not Configured	Action Recommended
XNC SERVER	Not Configured	Action Recommended
MDM LB	[redacted]	Pass
	[redacted]	Pass

Feedback

Note

XenMobile Analyzer supports gateway servers configured through the NetScaler wizard. NetScaler 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**, **Details**, and **Results (Action Required)**.

When an Advanced Configuration check fails, the Recommendations table lists the **Policy**, **Details**, and **Results (Action Recommended)**.

The notification badge within the Configuration Report indicates the number of recommendations in the Essential Configuration check for gateway servers configured through the NetScaler wizard and user-configured Gateways.

On the **Configuration Report** page, the following options are available.

a. To view the details, click **Essential Configuration Checks/Advanced Configuration Checks** (or the expand icon).

b. To run another NetScaler configuration check, click **Run another test**.

c. To view other troubleshooting and analyzing tools, click **Go to XenMobile Analyzer Checks**.

d. To download a report of the results, click **Download report and ns.conf file bundle** or in **Email report and ns.conf bundle**, type your email address. Then, click **Send**.

You interact with the Environment Check step of XenMobile Analyzer directly to perform tests, whereas the other options are informative. Each of these options provides information concerning other support tools you can use to ensure that your XenMobile environment is set up correctly.

- **Advanced Diagnostics**: Instructs you to collect information on your environment and then upload the information to Citrix Insight Services. The tool analyzes your data and provides a personalized report with recommended resolutions.
- **Secure Mail Readiness:** Directs you to download and run the XenMobile Exchange ActiveSync Test application. The application troubleshoots ActiveSync servers for their readiness to be deployed with XenMobile environments. After the application runs, you can view reports or share them with others.
- **Server Connectivity Checks:** Provides you with instructions for checking your connections to XenMobile, Authentication, and ShareFile servers.
- **Contact Citrix support**: If all else fails, you can create a support ticket with Citrix support.

The following issues are known in the XenMobile 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.

The following issues with XenMobile Analyzer have been fixed:

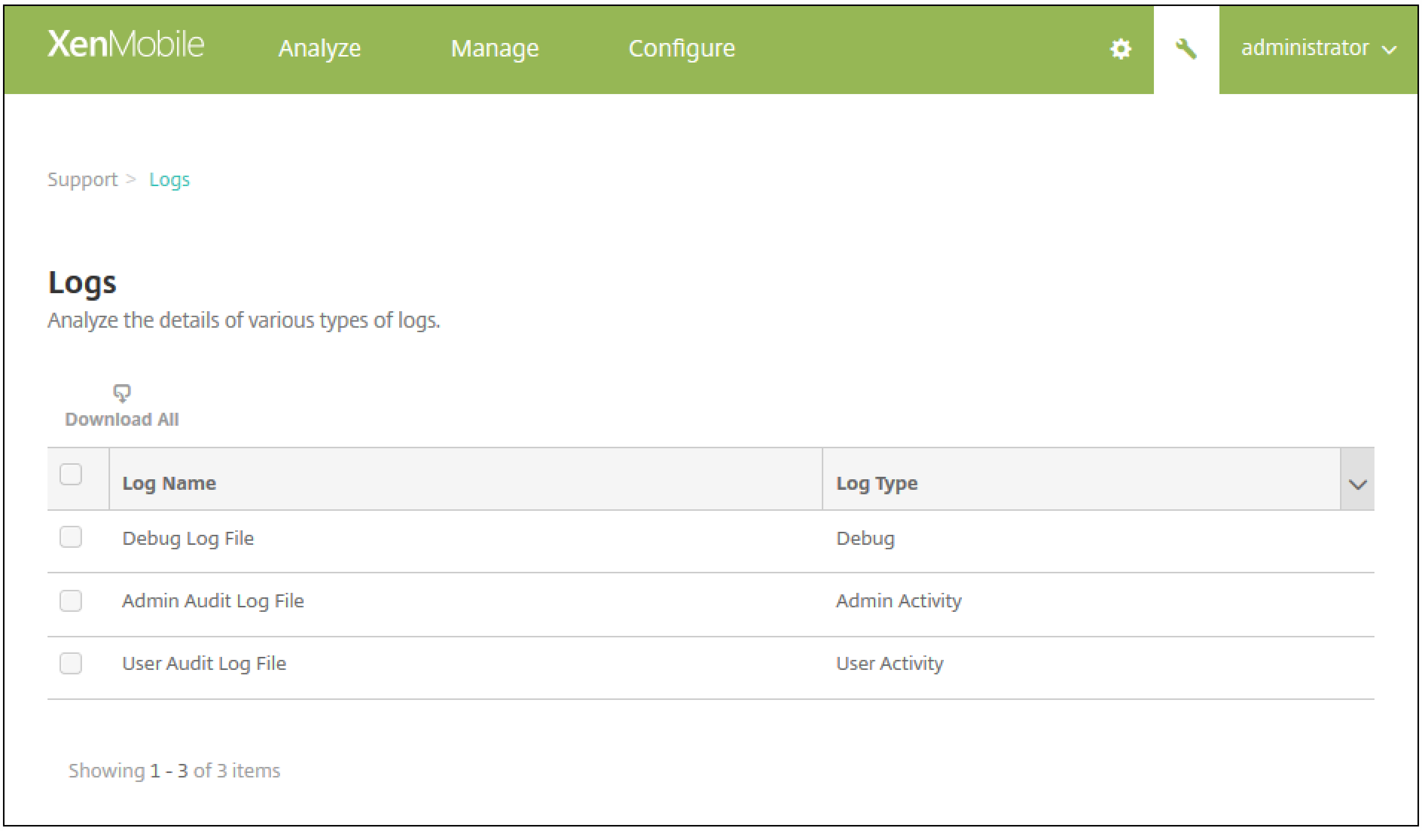
- When performing a check using enrollment invitation, the test passes but the enrollment invitation is not redeemed.

View and analyze log files in XenMobile

Sep 06, 2017

1. In the XenMobile console, click the wrench icon in the upper-right corner of the console. The **Support** page opens.

2. Under **Log Operations**, click **Logs**. The **Logs** page appears. Individual logs appear in a table.



Logs

Analyze the details of various types of logs.

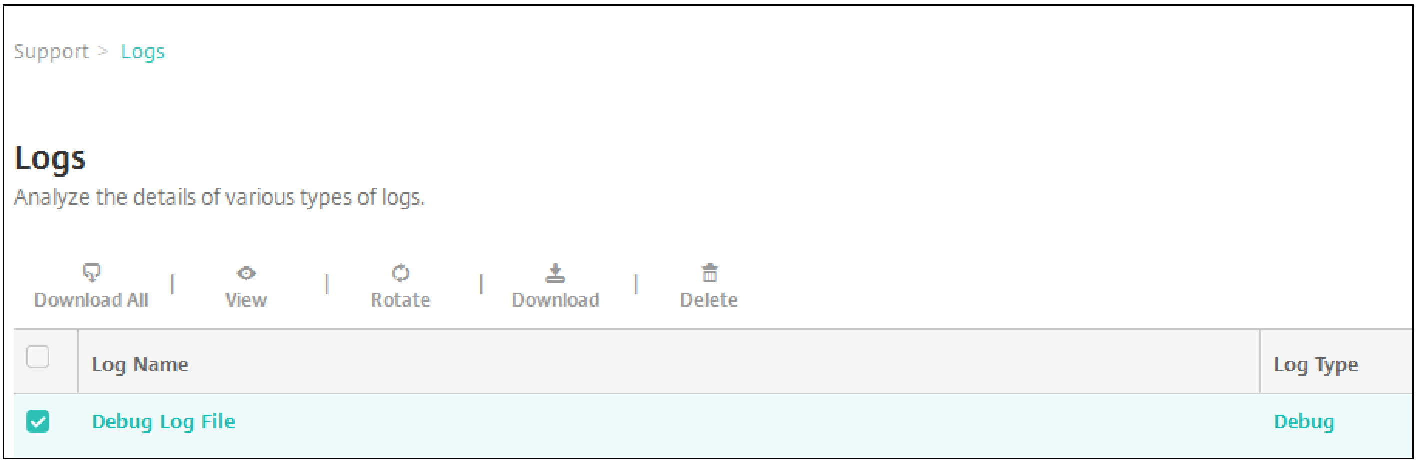
□	Log Name	Log Type
□	Debug Log File	Debug
□	Admin Audit Log File	Admin Activity
□	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

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 XenMobile 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, rotate, download a single log, or delete the selected log.



Logs

Analyze the details of various types of logs.

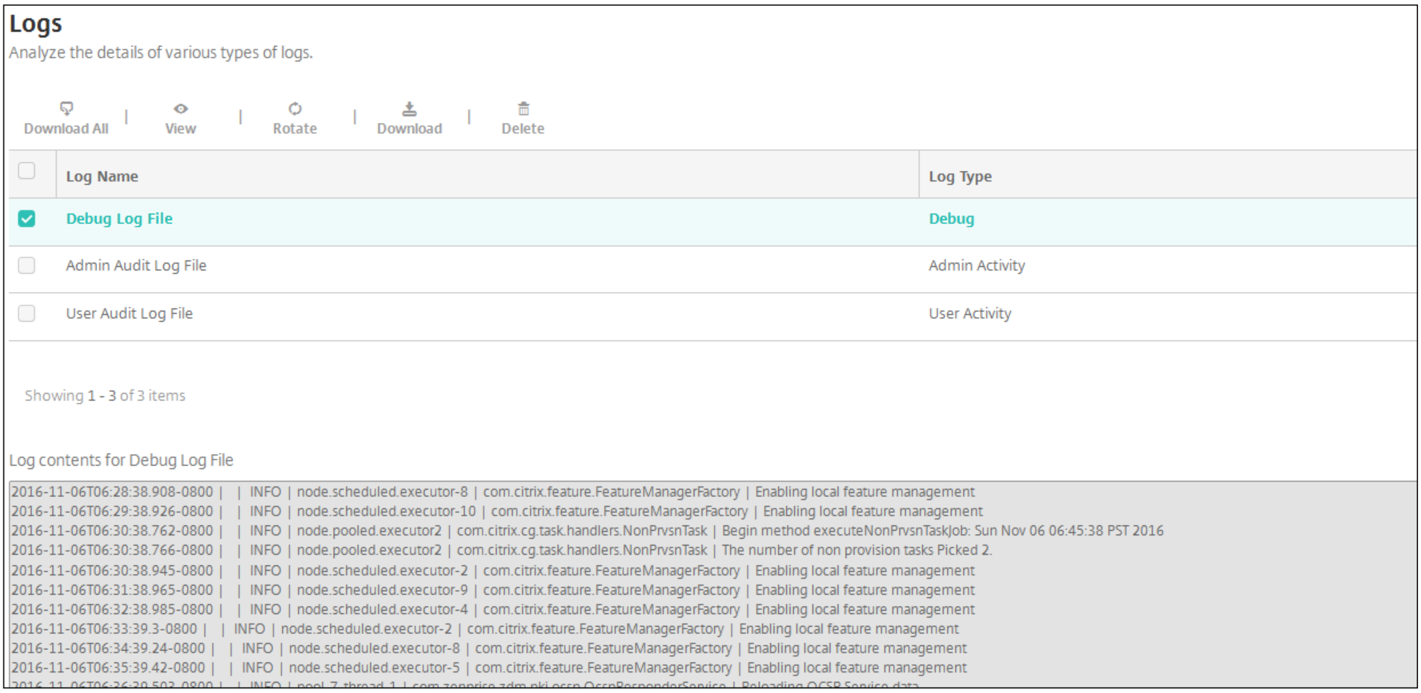
□	Log Name	Log Type
☑	Debug Log File	Debug

Note:

- If you select more than one log file, only **Download All** and **Rotate** are available.
- If you have clustered XenMobile servers, you can only view the logs for the server to which you are connected. To see logs for other servers, use one of the download options.

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.
- **Rotate**: Archives the current log file and creates a new file to capture log entries. A dialog box appears when archiving a log file; click Rotate to continue.
- **Download**: The console downloads only the single log file type selected; it also downloads any archived logs for that same type.
- **Delete**: Permanently removes the selected log files.


Logs

Analyze the details of various types of logs.

□	Log Name	Log Type
☑	Debug Log File	Debug
□	Admin Audit Log File	Admin Activity
□	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Debug Log File

```
2016-11-06T06:28:38.908-0800 |   | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:29:38.926-0800 |   | INFO | node.scheduled.executor-10 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:30:38.762-0800 |   | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | Begin method executeNonPrvsnTaskJob: Sun Nov 06 06:45:38 PST 2016
2016-11-06T06:30:38.766-0800 |   | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | The number of non provision tasks Picked 2.
2016-11-06T06:30:38.945-0800 |   | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:31:38.965-0800 |   | INFO | node.scheduled.executor-9 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:32:38.985-0800 |   | INFO | node.scheduled.executor-4 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:33:39.3-0800 |   | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:34:39.24-0800 |   | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:35:39.42-0800 |   | INFO | node.scheduled.executor-5 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:36:39.503-0800 |   | INFO | pool-7-thread-1 | com.zenprise.zdm.pki.ocsp.OcspResponderService | Reloading OCSP Service data
```

REST APIs

Sep 06, 2017

With the XenMobile REST API, you can call services that are exposed through the XenMobile console. You can call REST services by using any REST client. The API does not require you to sign on to the XenMobile console to call the services.

For the complete current set of available APIs, download the XenMobile Public API for REST Services PDF.

Permissions required to access the REST API

Access to the REST API requires one of the following permissions:

- Public API access permission set as part of role-based access configuration. For information on setting role-based access, 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.

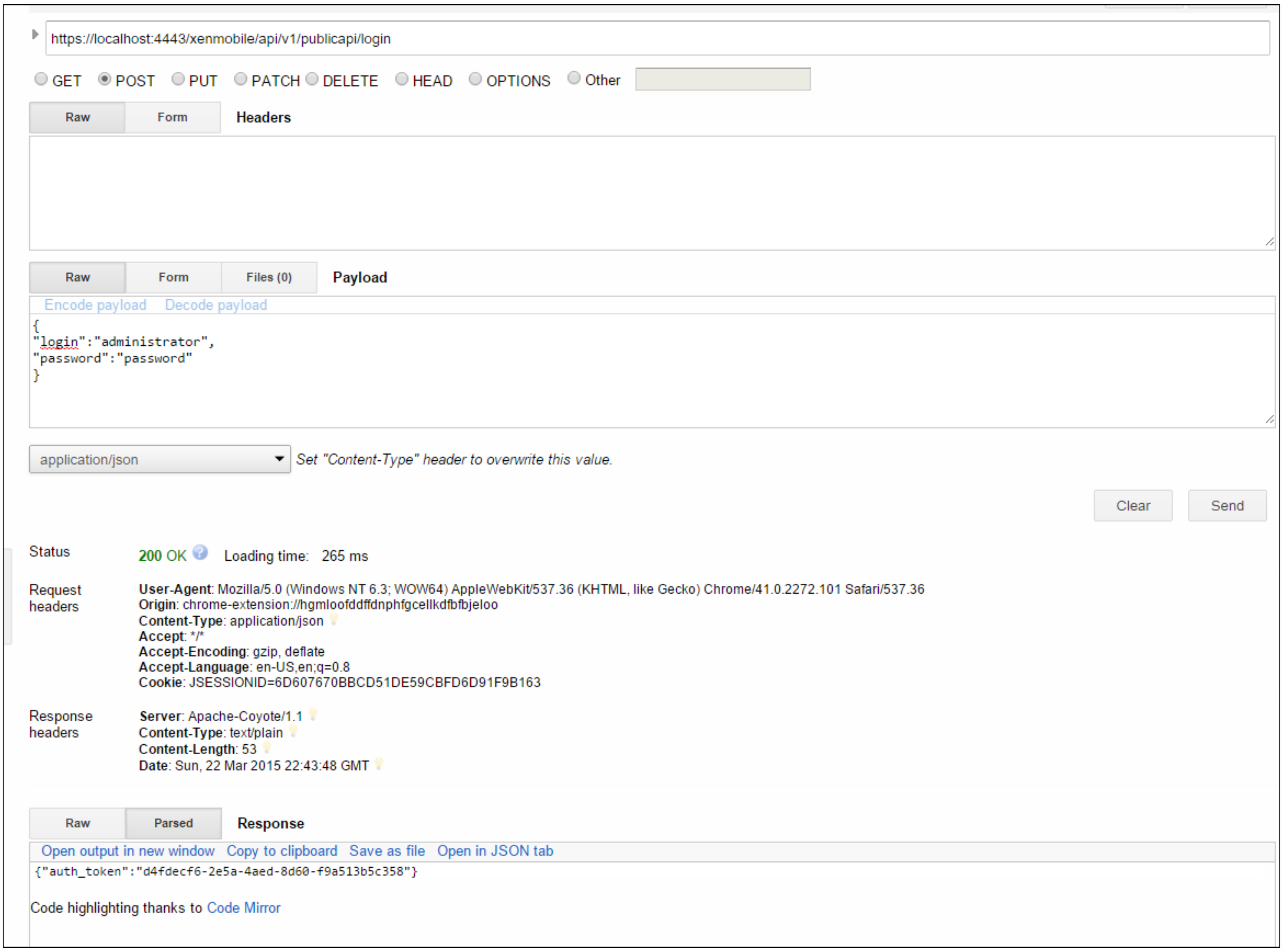
> ## Note
> In the following examples, change the host name and port number to match your environment.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login

Request: { "login":"administrator", "password":"password" }

Method type: POST

Content type: application/json



https://localhost:4443/xenmobile/api/v1/publicapi/login
○ GET ● POST ○ PUT ○ PATCH ○ DELETE ○ HEAD ○ OPTIONS ○ Other
Raw
Form
Headers
Raw
Form
Files (0)
Payload
Encode payload
Decode payload
Clear
Send
Raw
Parsed
Response
Open output in new window
Copy to clipboard
Save as file
Open in JSON tab

```
{
"login":"administrator",
"password":"password"
}
```

application/json Set "Content-Type" header to overwrite this value.

Status 200 OK Loading time: 265 ms

Request headers
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.101 Safari/537.36
Origin: chrome-extension://hgmloofddffdnphfgcellkdfbfbjeloo
Content-Type: application/json
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=6D607670BBCD51DE59CBFD6D91F9B163

Response headers
Server: Apache-Coyote/1.1
Content-Type: text/plain
Content-Length: 53
Date: Sun, 22 Mar 2015 22:43:48 GMT

```
{"auth_token":"d4fdecf6-2e5a-4aed-8d60-f9a513b5c358"}
```

Code highlighting thanks to Code Mirror

Related information

XenMobile REST API

XenMobile Mail Manager 10.x

Jan 22, 2018

XenMobile Mail Manager provides the functionality that extends the capabilities of XenMobile 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 XenMobile to access EAS device partnership information provided by Exchange.
- The ability for XenMobile to perform an EAS Wipe on a mobile device.
- The ability for XenMobile to access information about Blackberry devices, and to perform control operations such as Wipe and ResetPassword.

To download XenMobile Mail Manager, go to the Server Components section under XenMobile 10 Server on Citrix.com.

This article includes the following sections:

- What's new in version 10.1
- Fixed issues
- Architecture
- System requirements and prerequisites
- XenMobile Mail Manager prerequisites
- Requirements for Office 365 Exchange
- Install and configure
- Enforce email policies with ActiveSync IDs
- Access control rules
- Device monitoring
- Troubleshooting and diagnostics
- Troubleshooting Tools

Access Rules

The Rule Analysis window has a check box which, when selected, displays only those rules which are conflicts, overrides, redundancies, or supplements.

Default access (Allow, Block, or Unchanged) and ActiveSync command modes (PowerShell or Simulation) are set separately for each Microsoft Exchange environment configured in your XenMobile deployment.

Snapshots

You can configure the maximum number of snapshots shown in the snapshot history.

You can configure which errors to ignore during a major snapshot. When a major snapshot returns errors that are not configured as ignorable, the results of the snapshots are discarded.

To configure errors as ignorable, edit the config.xml file using an XML editor:

- If the Exchange Server is Office 365, navigate to the /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors node and add the text to be matched as a child element in the same format as the existing Error child element. Regular expressions are supported.
- If the Exchange Server is on-premises, navigate to the /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors node and add the text to be matched as a child element in the same format as the existing Error child element. Regular expressions

are supported.
- If there is more than one Exchange environment configured, navigate to the /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='ID Corresponding to the desired Exchange environment']/ExchangeServer/Specialists/PowerShell node. Add an IgnorableErrors child node to the PowerShell node for each error to be ignored. Add an Error child node to the IgnorableErrors node with the matching text contained in a CDATA section. Regular expressions are supported.

Save the config.xml and restart the XenMobile Mail Manager service.

PowerShell and Exchange

XenMobile Mail Manager now dynamically determines which cmdlets to use based on the version of Exchange it is connected to. For example, for Exchange 2010, it uses Get-ActiveSyncDevice, but for Exchange 2013 and Exchange 2016, it uses Get-MobileDevice.

Exchange Configuration

Exchange Server configurations can be edited and updated without restarting the XenMobile Mail Manager service.

Two new columns added to the Exchange environment summary tab display each environment's command mode (PowerShell or Simulation), and access mode (Allow, Block, or Unchanged).

Troubleshooting and Diagnostics

A set of PowerShell utilities for troubleshooting is available in the Support\PowerShell folder.

Testing connectivity to the Exchange service using the Test Connectivity button in the Configuration window of the console runs every read-only cmdlet used by the service, runs RBAC permissions tests against the Exchange Server for the configured user, and displays any errors or warnings in color-coded fashion (blue-yellow for warnings, red-orange for errors).

A new 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 cdmlets to a text file.

In support scenarios, all properties for all mailboxes on all devices managed by XenMobile Mail Manager can be saved by selecting a diagnostic check box in the console.

In support scenarios, trace-level logging is now supported.

Authentication

XenMobile Mail Manager supports Basic authentication for on-premises deployments. This enables XenMobile Mail Manager to be used when the XenMobile Mail Manager server is not a member of the domain in which the Exchange Server resides.

Access Rules

XenMobile Mail Manager applies local access control rules to all users in Active Directory (AD) groups, even if an AD group contains more than 1000 users. Previously, XenMobile Mail Manager applied local access control rules only to the first 1000 users of an AD group. [#548705]

The XenMobile Mail Manager console sometimes failed to respond when querying Active Directory groups containing 1000 users or more. [CXM-11729]

The LDAP Configuration window no longer displays an incorrect authentication mode. [CXM-5556]

Snapshots

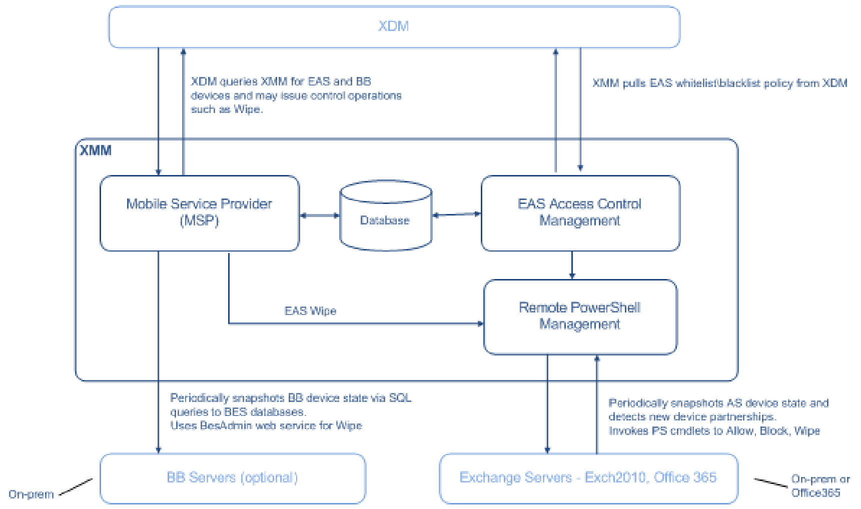
User names with apostrophes no longer cause minor snapshots to fail. [#617549]

In support scenarios where pipelining is disabled (the Disable Pipelining option is selected in the Configuration window of the XenMobile Mail Manager console), major snapshots no longer fail in on-premises Exchange environments. [#586083]

In support scenarios where pipelining is disabled (the Disable Pipelining option is selected in the Configuration window of the XenMobile Mail Manager console), data for deep snapshots is no longer collected regardless of whether the environment was configured for deep or shallow snapshots. Now data for deep snapshots is collected only when the environment is configured for deep snapshots. [#586092]

The first major snapshot after initial installation occasionally encountered an error that prevented XenMobile Mail Manager from running another major snapshot until the XenMobile Mail Manager service was restarted. This no longer occurs. [CXM-5536]

The following diagram shows the main components of XenMobile Mail Manager. For a detailed reference architecture diagram, see the XenMobile Deployment Handbook article, Reference Architecture for On-Premises Deployments.


XDM
XDM queries XMM for EAS and BB devices and may issue control operations such as Wipe.
XMM pulls EAS whitelist\blacklist policy from XDM
XMM
Mobile Service Provider (MSP)
Database
EAS Access Control Management
EAS Wipe
Remote PowerShell Management
Periodically snapshots BB device state via SQL queries to BES databases.
Uses BesAdmin web service for Wipe
Periodically snapshots AS device state and detects new device partnerships.
Invokes PS cmdlets to Allow, Block, Wipe
On-prem
BB Servers (optional)
Exchange Servers - Exch2010, Office 365
On-prem or Office365

The three main components are:

- **Exchange ActiveSync Access Control Management**. Communicates with XenMobile to retrieve an Exchange ActiveSync policy from XenMobile, 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 Provide**r. Provides a web service interface so that XenMobile can query Exchange ActiveSync and/or Blackberry devices, as well as issue control operations such as Wipe against them.

The following minimum system requirements are required to use XenMobile Mail Manager:

- Windows Server 2012 R2, Windows Server 2008 R2 (must be an English-based server)
- Microsoft SQL Server 2016, SQL Server 2012, SQL Server 2012 Express LocalDB, or SQL Server Express 2008
- Microsoft .NET Framework 4.5
- 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 SP2

Device email clients

Not all email clients consistently return the same ActiveSync ID for a device. Because XenMobile Mail Manager 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
- Touchdown for Smartphones

- Windows Management Framework must be installed.
  - PowerShell V5, V4, and V3
- The PowerShell execution policy must be set to RemoteSigned via Set-ExecutionPolicy RemoteSigned.
- TCP port 80 must be open between the computer running XenMobile Mail Manager and the remote Exchange Server.

Requirements for on-premises computer running Exchange

Permissions. 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.

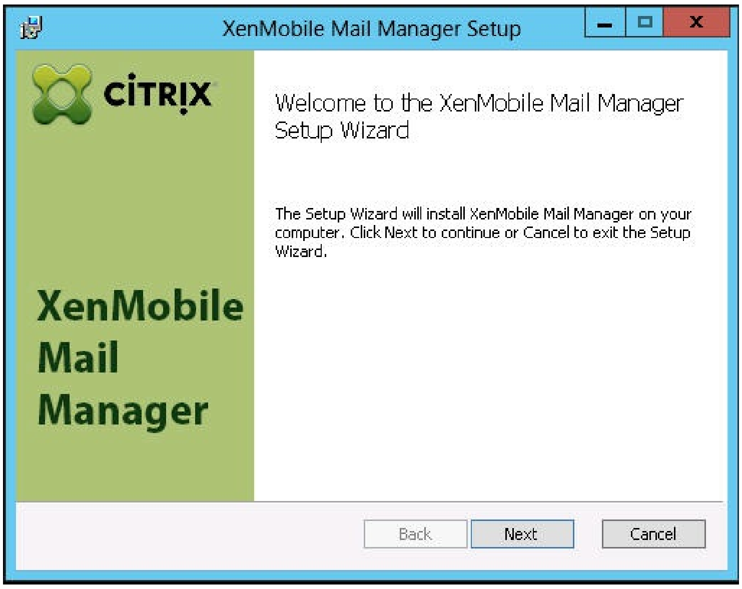
- **For Exchange Server 2010 SP2:**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **For Exchange Server 2013 and Exchange Server 2016:**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

- If XenMobile Mail Manager 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, in order to establish a remote connection and run remote commands, the credentials must correspond to a user who is an administrator on the remote machine. Per this blog post, You Don't Have to Be An Administrator to Run Remote PowerShell Commands, Set-PSSessionConfiguration can be used to eliminate the administrative requirement, but the support and discussion of the particulars of this command are beyond the scope of this document.
- 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, XenMobile Mail Manager 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.

- **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, XenMobile Mail Manager 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.

1. Click the XmmSetup.msi file and then follow the prompts in the installer to install XenMobile Mail Manager.

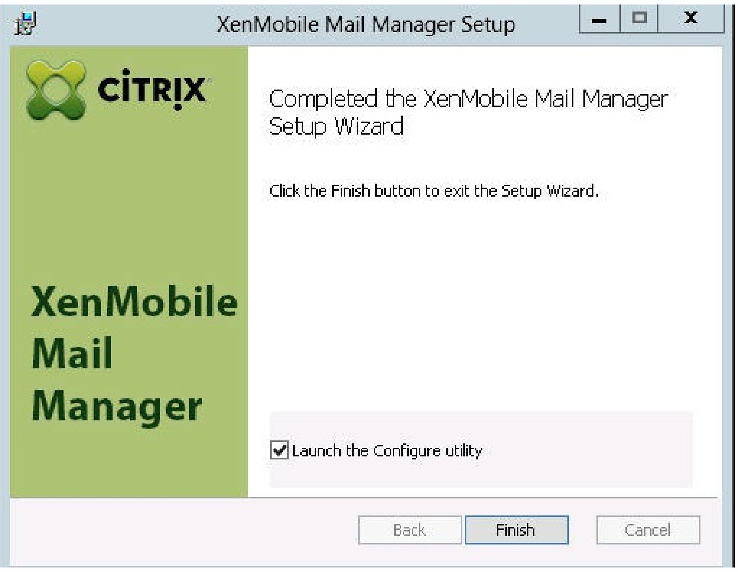


XenMobile Mail Manager Setup

Welcome to the XenMobile Mail Manager Setup Wizard

The Setup Wizard will install XenMobile Mail Manager on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

2. Leave **Launch the Configure utility** selected in the last screen of the set-up wizard. Or, from the **Start** menu, open **XenMobile Mail Manager.**



XenMobile Mail Manager Setup

Completed the XenMobile Mail Manager Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Launch the Configure utility

3. Configure the following database properties:

a. Select the **Configure** > **Database** tab.

b. Enter the name of the SQL Server (defaults to localhost).

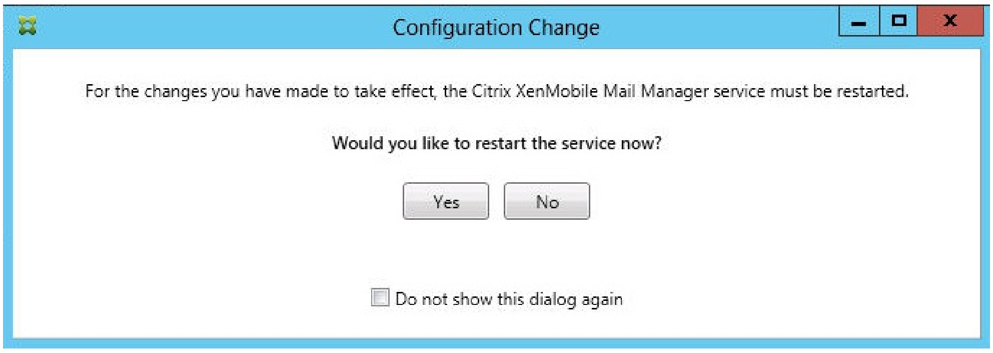
c. Keep the database as the default CitrixXmm.

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.
  Note: 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**.



Configuration Change

For the changes you have made to take effect, the Citrix XenMobile Mail Manager service must be restarted.

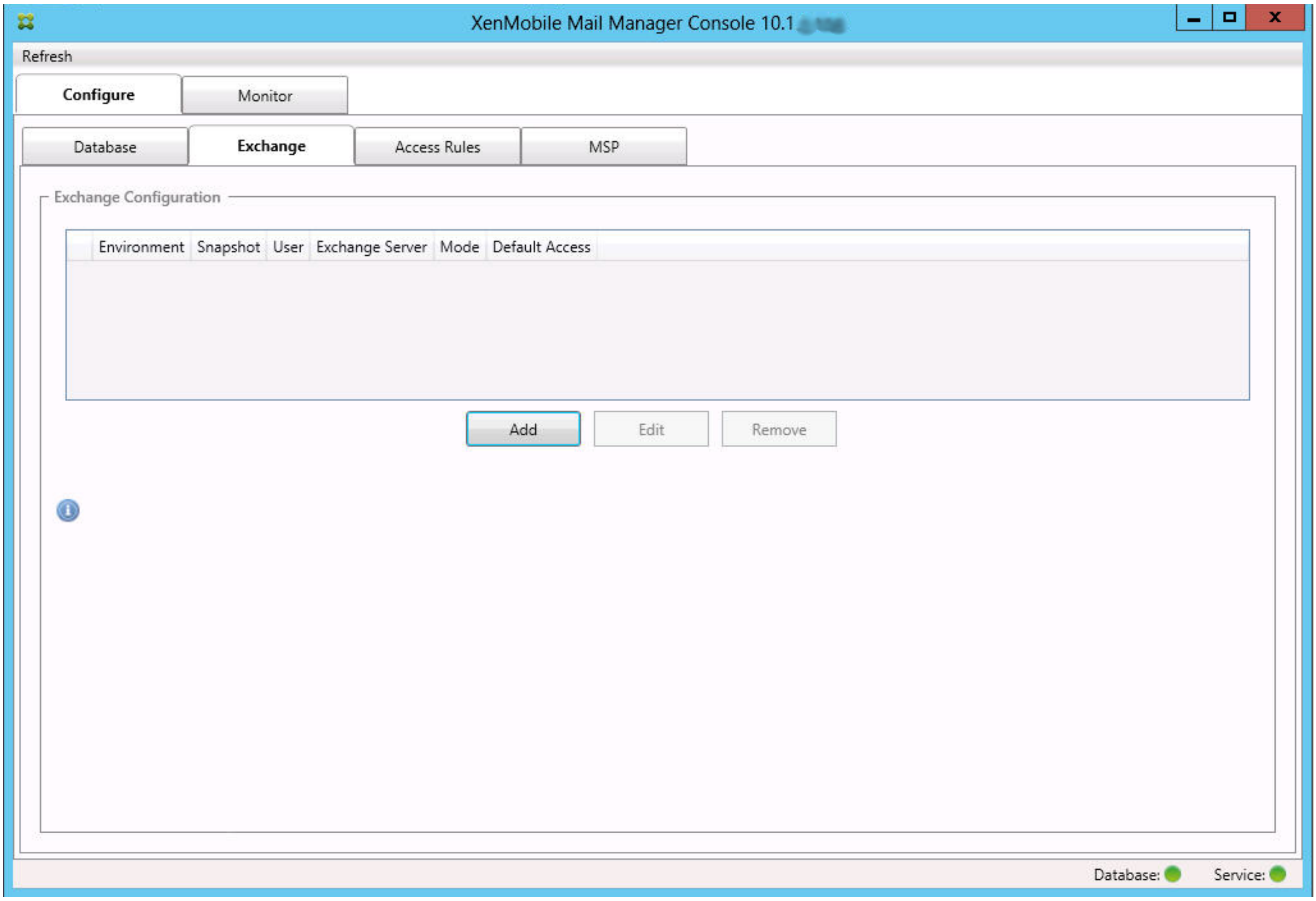
Would you like to restart the service now?

□ Do not show this dialog again

7. Configure one or more Exchange Servers:

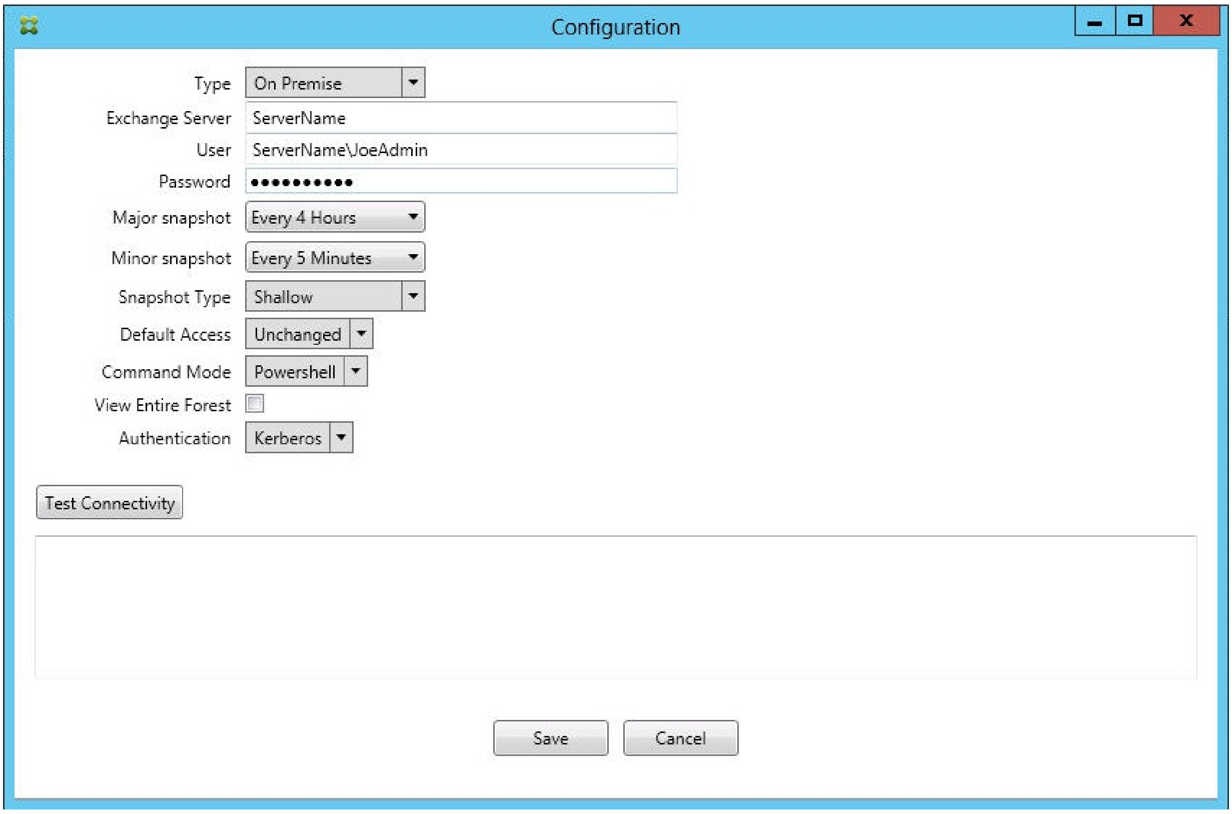
a. If managing a single Exchange environment, you only need a single server specified. If managing multiple Exchange environments, you need a single Exchange Server specified for each Exchange environment.

b. Select the **Configure** > **Exchange** tab.



c. Click **Add**.

d. Select the type of Exchange Server environment: **On Premise** or **Office 365**.



Type	On Premise
Exchange Server	ServerName
User	ServerName\JoeAdmin
Password	●●●●●●●●●●●
Major snapshot	Every 4 Hours
Minor snapshot	Every 5 Minutes
Snapshot Type	Shallow
Default Access	Unchanged
Command Mode	Powershell
View Entire Forest	□
Authentication	Kerberos

e. If you select **On Premise**, enter the name of the Exchange Server that will be used for Remote PowerShell commands.

f. Enter the user name of a Windows identity that has appropriate rights on the Exchange Server as specified within the **Requirements** section.

g. Enter the **Password** for the user.

h. Select the schedule for running Major snapshots. A major snapshot detects every Exchange ActiveSync partnership.

i. Select the schedule for running Minor snapshots. A minor snapshot detects newly created Exchange ActiveSync partnerships.

j. 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 XenMobile Mail Manager. Deep snapshots may take significantly longer and are only needed if the Mobile Service Provider is enabled for ActiveSync; this allows XenMobile to query for unmanaged devices.

k. Select the Default Access: **Allow**, **Block**, or **Unchanged**. This controls how all devices other than those identified by explicit XenMobile or Local rules are treated. If you select Allow, ActiveSync access to all such devices will be allowed; if you select Block, access will be denied; if you selectUnchanged, no change will be made.

l. Select the ActiveSync Command Mode: **PowerShell** or **Simulation**.

- In PowerShell mode, XenMobile Mail Manager will issue PowerShell commands to enact the desired access control.
- In Simulation mode, XenMobile Mail Manager will not issue PowerShell commands, but will log 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.

m. Select **View Entire Forest** to configure XenMobile Mail Manager to view the entire Active Directory forest in the Exchange environment.

n. Select the authenication protocol: **Kerberos** or **Basic**. XenMobile Mail Manager supports Basic authentication for on-premises deployments. This enables XenMobile Mail Manager to be used when the XenMobile Mail Manager server is not a member of the domain in which the Exchange server resides.

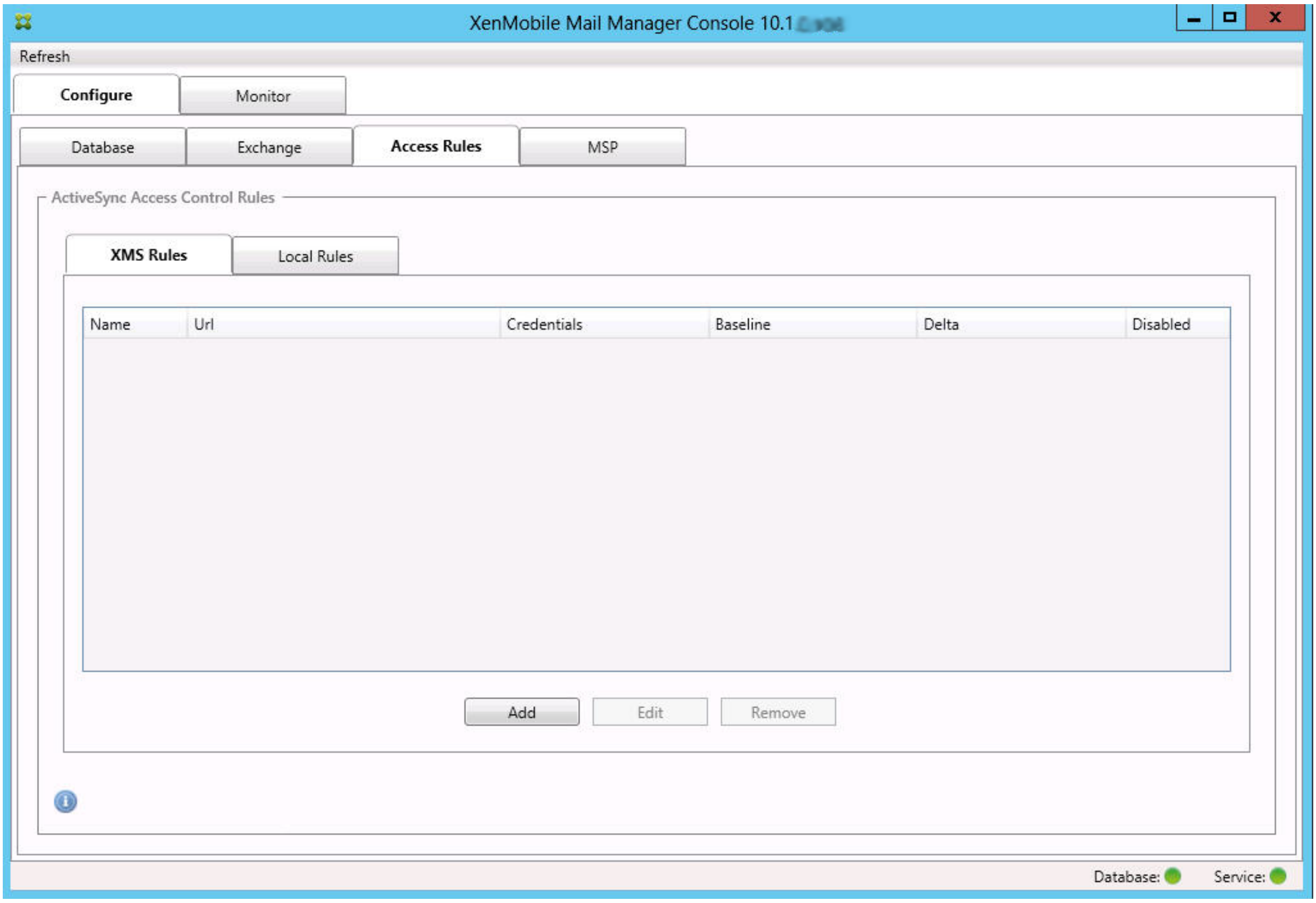
o. Click **Test Connectivity** to check that a connection can be made to the Exchange Server and then click **Save**.

p. A message prompts you to restart the service. Click **Yes**.

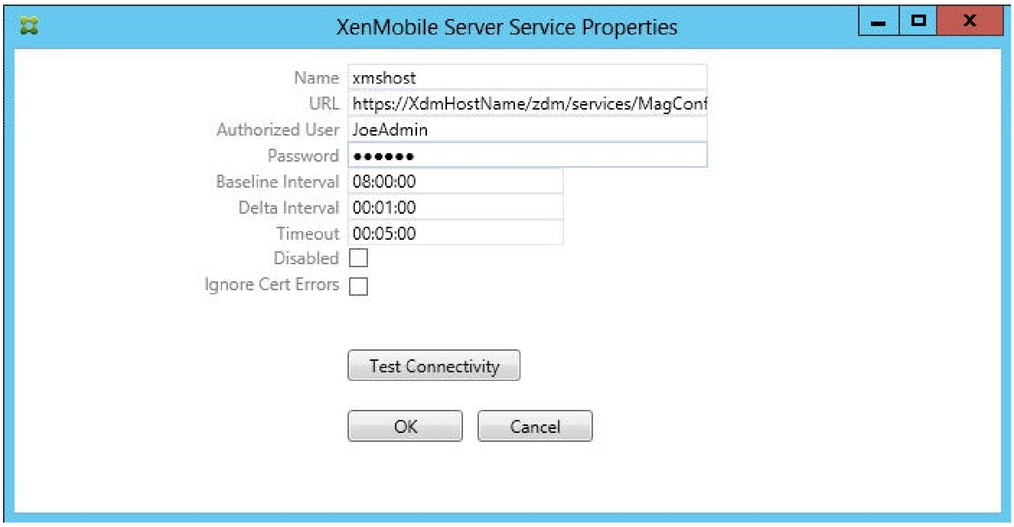
8. Configure the access rules:

a. Select the **Configure** > **Access Rules** tab.

b. Click the **XDM Rules** tab.



c. Click **Add**.



Name xmshost
URL https://XdmHostName/zdm/services/MagConf
Authorized User JoeAdmin
Password ●●●●●●
Baseline Interval 08:00:00
Delta Interval 00:01:00
Timeout 00:05:00
Disabled □
Ignore Cert Errors □

d. Enter a name for the XenMobile server rules, such as XdmHost.

e. Modify the URL string to refer to the XenMobile server; for example, if the server name is XdmHost and the instance name is zdm, enter http://XdmHostName/zdm/services/MagConfigService.

f. Enter an authorized user on the server.

g. Enter the password of the user.

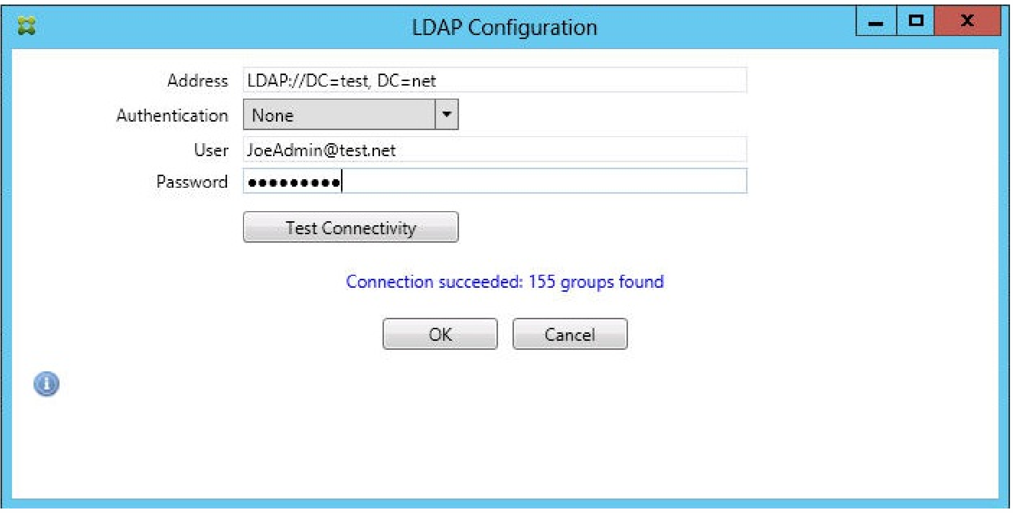
h. Keep the default values for the Baseline Interval, Delta Interval, and Timeout values.

i. Click **Test Connectivity** to check the connection to the server and then click **OK**.

Note: If the Disabled check box is checked, the XenMobile Mail Service will not collect policy from the XenMobile server.

9. Click the **Local Rules** tab.

a. If you want to construct local rules that operate on Active Directory Groups, click **Configure LDAP** and then configure the LDAP connection properties.



LDAP Configuration

Address LDAP://DC=test, DC=net

Authentication None

User JoeAdmin@test.net

Password ●●●●●●●●●

Connection succeeded: 155 groups found

b. 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. For details, see XenMobile Mail Manager Access Control Rules.

c. Enter text or text fragments in the text box. Optionally, click the query button to view the entities that match the fragment.

Note: 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 will be available.

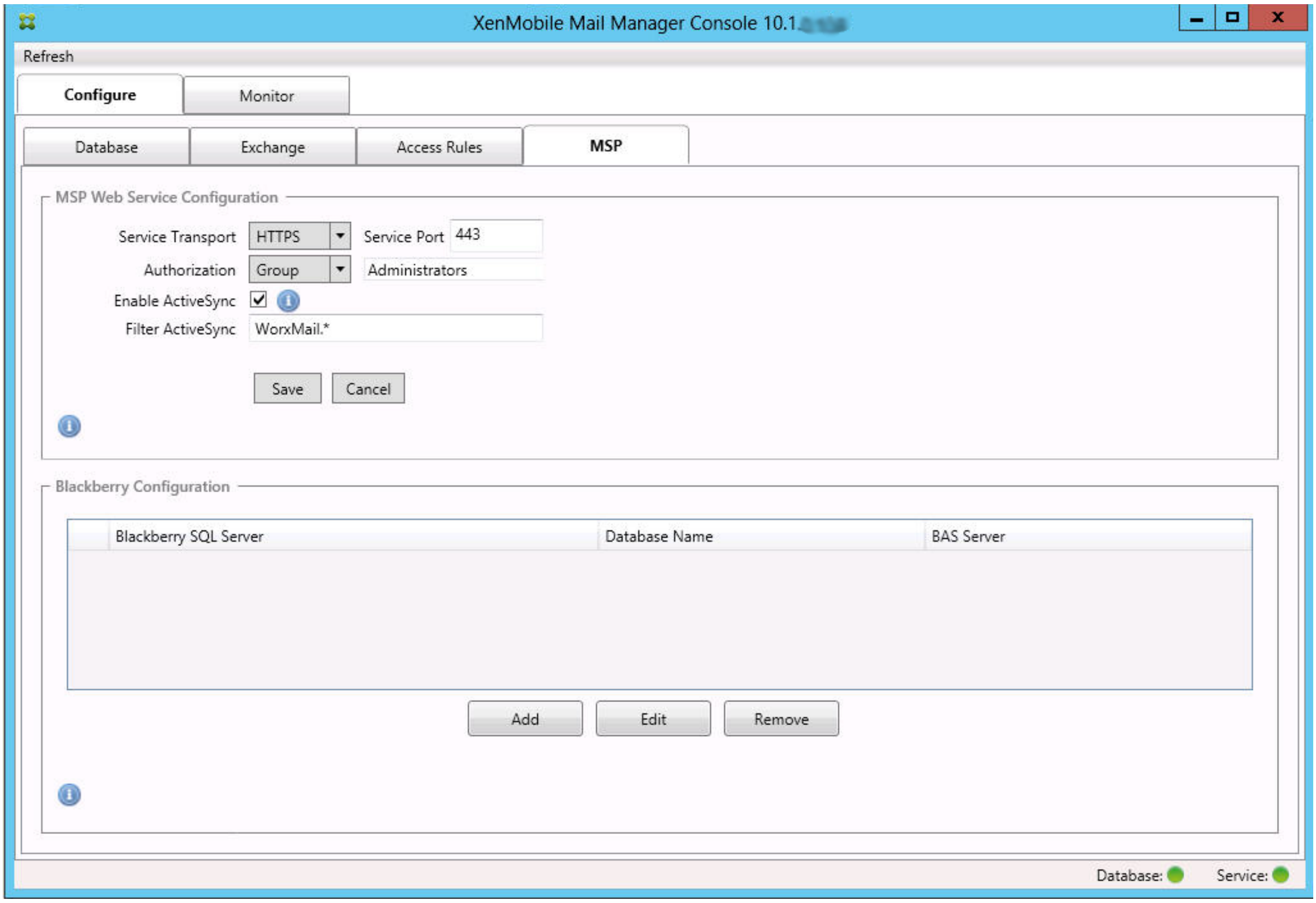
d. Select a text value and then click **Allow** or **Deny** to add it to the **Rule List** pane on the right side. You can change the order of rules or remove them using the buttons to the right of the **Rule List** pane. The order is important because, for a given user and device, rules are evaluated in the order shown and a match on a higher rule (nearer the top) will cause 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.

e. 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**.

10. Configure the Mobile Service Provider.

Note: The Mobile Service Provider is optional and is necessary only if XenMobile is also configured to use the Mobile Service Provider interface to query unmanaged devices.

a. Select the **Configure** > **MSP** tab.



MSP Web Service Configuration

Service Transport: HTTPS Service Port: 443

Authorization: Group Administrators

Enable ActiveSync: ☑

Filter ActiveSync: WorxMail.*

Blackberry Configuration

Blackberry SQL Server	Database Name	BAS Server

Database: ● Service: ●

b. Set the Service Transport type as HTTP or HTTPS for the Mobile Service Provider service.

c. Set the Service port (typically 80 or 443) for the Mobile Service Provider service.

Note: If you use port 443, the port requires an SSL certificate bound to it in IIS.

d. 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 XenMobile.

e. Set whether ActiveSync queries are enabled or not.

Note: if ActiveSync queries are enabled for the XenMobile server, the Snapshot type for one or more Exchange Servers must be set to **Deep**; this may have significant performance costs for taking snapshots.

f. By default, ActiveSync devices that match the regular expression Secure Mail.* will not be sent to XenMobile. To change this behavior, alter the Filter ActiveSync field as necessary.

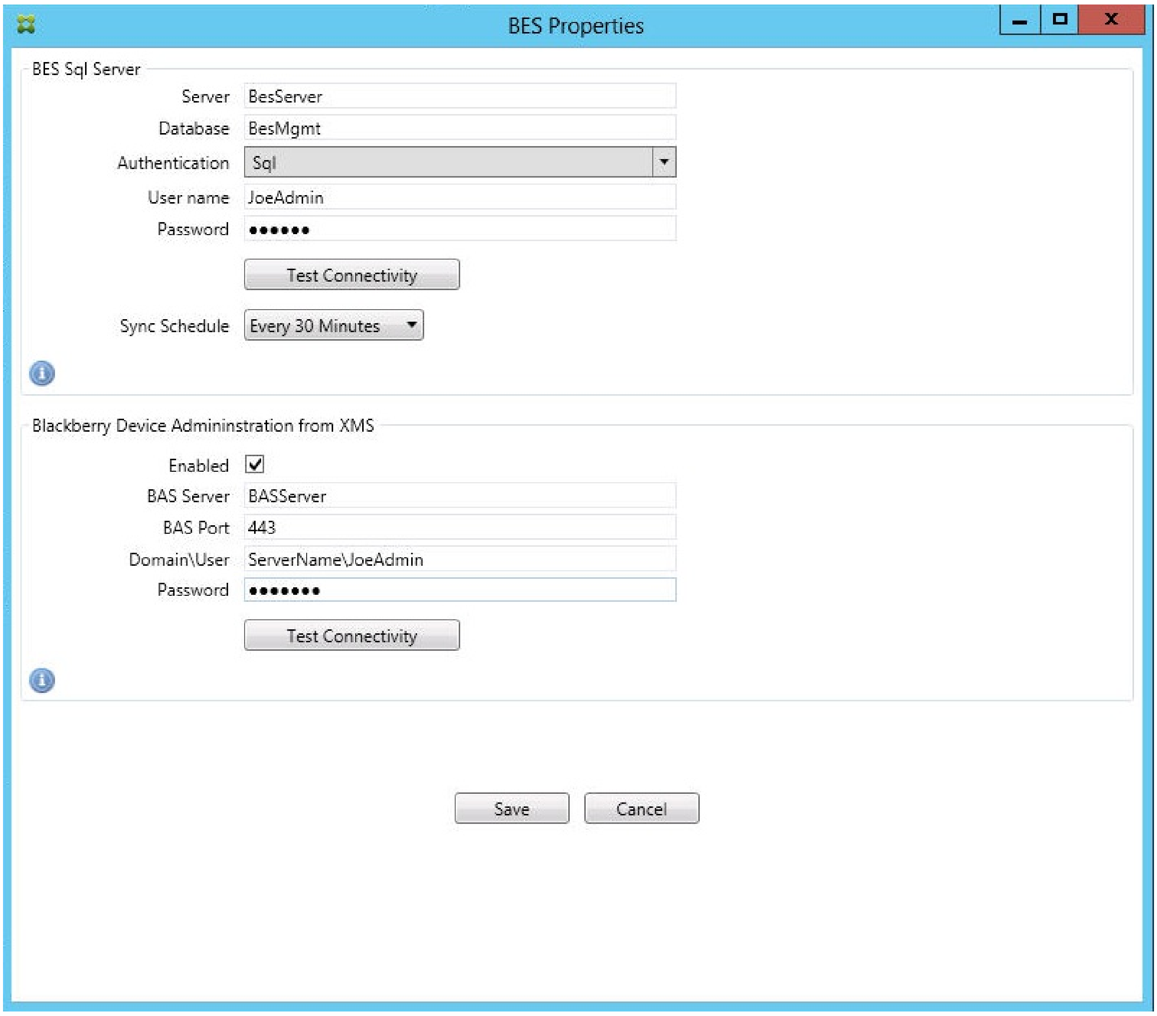
Note: Blank means that all devices will be forwarded to XenMobile.

g. Click **Save**.

11. Optionally, configure one or more BlackBerry Enterprise Server (BES):

a. Click **Add**.

b. Enter the server name of the BES SQL Server.



BES Properties

BES Sql Server

Server: BesServer

Database: BesMgmt

Authentication: Sql

User name: JoeAdmin

Password: ●●●●●●

Sync Schedule: Every 30 Minutes

Blackberry Device Admininstration from XMS

Enabled: ☑

BAS Server: BASServer

BAS Port: 443

Domain\User: ServerName\JoeAdmin

Password: ●●●●●●●

c. Enter the database name of the BES management database.

d. Select the Authentication mode. If you select Windows Integrated authentication, the user account of the XenMobile Mail Manager service is the account that is used to connect to the BES SQL Server.

Note: If you also choose Windows Integrated for the XenMobile Mail Manager database connection, the Windows account specified here must also be given access to the XenMobile Mail Manager database.

e. If you select SQL authentication, enter the user name and password.

f. Set the Sync Schedule. This is the schedule used to connect to the BES SQL Server and checks for any device updates.

g. Click **Test Connectivity** to check connectivity to the SQL Server.

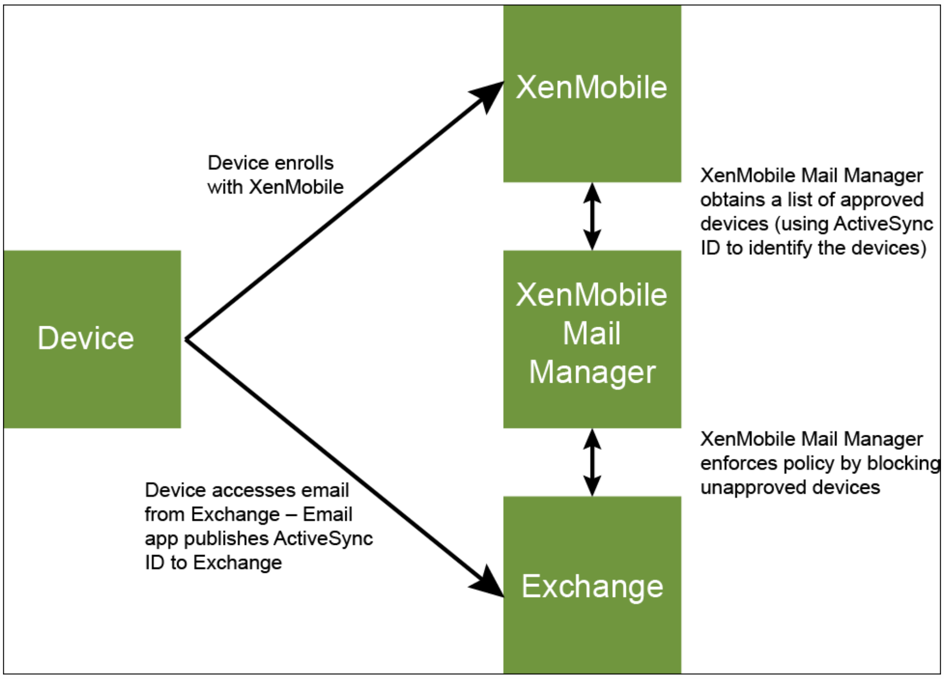
Note: If you select Windows Integrated, this test uses the current logged on user and not the XenMobile Mail Manager service user and therefore does not accurately test SQL authentication.

h. If you want to support remote Wipe and/or ResetPassword of BlackBerry devices from XenMobile, check 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.
- Click **Save**.

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. XenMobile Mail Manager and XenMobile work together to enforce such an email policy. XenMobile sets the policy for corporate email access and, when an unapproved device enrolls with XenMobile, XenMobile Mail Manager 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 uniquely identify the device. Secure Hub obtains a similar identifier and sends the identifier to XenMobile when the device is enrolled. By comparing the two device IDs, XenMobile Mail Manager can determine whether a specific device should have corporate email access. The following figure illustrates this concept:


XenMobile
Device enrolls with XenMobile
XenMobile Mail Manager obtains a list of approved devices (using ActiveSync ID to identify the devices)
Device
XenMobile Mail Manager
XenMobile Mail Manager enforces policy by blocking unapproved devices
Device accesses email from Exchange – Email app publishes ActiveSync ID to Exchange
Exchange

If XenMobile sends XenMobile Mail Manager an ActiveSync ID that is different from the ID the device publishes to Exchange, XenMobile Mail Manager 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 XenMobile.
- On all other Android platforms, push both the Touchdown app and the Touchdown ActiveSync configuration from XenMobile.

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 XenMobile Mail Manager 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.

XenMobile Mail Manager provides a rule-based approach for dynamically configuring access control for Exchange ActiveSync devices. A XenMobile Mail Manager 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 will revert 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.

XenMobile Mail Manager has three types of rules: local rules, XenMobile 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 XenMobile server rules nor the default access rule will be consulted. Local rules are configured locally to XenMobile Mail Manager 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 upon 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.

XenMobile server rules. XenMobile server rules are references to an external XenMobile server that provides rules about managed devices. The XenMobile server can be configured with its own high-level rules that identify the devices to be allowed or blocked based on properties known to XenMobile, such as whether the device is jailbroken or whether the device contains forbidden apps. XenMobile 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 XenMoble 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 XenMoble server rule will be allowed.
- **Default Access – Block**. Any device that is not matched by either a local or XenMoble server rule will be blocked.
- **Default Access - Unchanged**. Any device that is not matched by either a local or XenMoble server rule will not have its access state modified in any way by XenMobile Mail Manager. 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 XenMobile Mail Manager, the rules are evaluated in sequence, from highest to lowest priority as follows:

- Local rules
- XenMobile 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 XenMobile 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, as soon as the first match is encountered, evaluation stops.

XenMobile Mail Manager 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 XenMobile Mail Manager. Exchange may be configured with three levels of rules: personal exemptions, device rules, and organization settings. XenMobile Mail Manager 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, XenMobile Mail Manager 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 upon the field that is being matched, such as ActiveSync device ID, ActiveSync device type, User, User Agent, and so on.

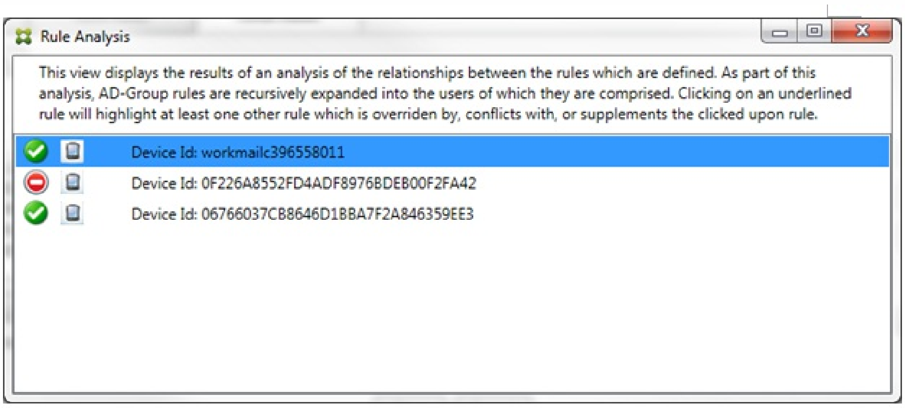
Rule terminology:

- **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 any time.
- **Ancillary rule**. An ancillary rule is related in some way to the primary rule either through override, conflict, or a supplementary relationship. The rules are indicated visually by a dashed border that surrounds them. For each primary rule, there can be 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 will be overridden by the primary rule, and/or the ancillary rule will conflict in its access with the primary rule, and/or the ancillary rule will supplement the primary rule.

The Appearance of the Types of Rules in the Rule Analysis Dialog Box

When there are no conflicts, overrides, or supplements, the Rule Analysis dialog box has no underlined entries. Clicking on any of the items has no impact; for example, normal selected item visuals will occur.

The Rule Analysis window has a check box which, when selected, displays only those rules which are conflicts, overrides, redundancies, or supplements.



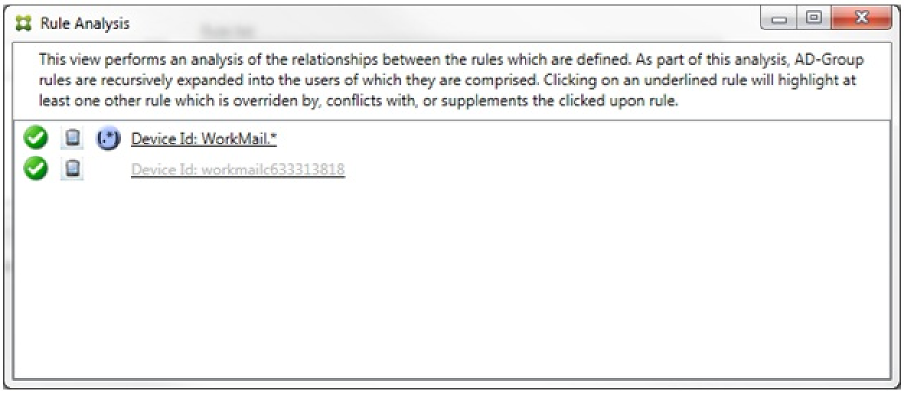
This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

✓ Device Id: workmailc396558011

⊖ Device Id: 0F226A8552FD4ADF8976BDEB00F2FA42

✓ Device Id: 06766037CB8646D1BBA7F2A846359EE3

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 will appear in a lighter font to indicate that the rule has been overridden by a higher priority rule. You can click on the overridden rule to find out which rule or rules have overriden 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 will appear next to it as a further visual indication that the rule is inactive. For example, before clicking on the rule, the dialog box appears as follows:



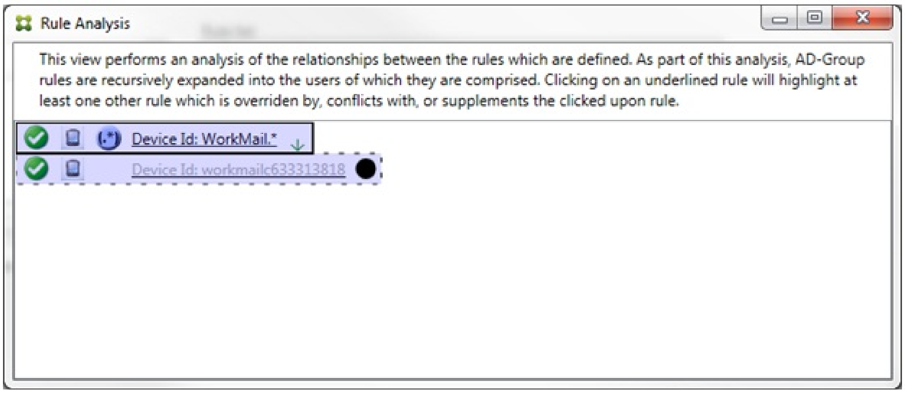
Rule Analysis

This view performs an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

Device Id: WorkMail.*

Device Id: workmailc633313818

When you click the highest-priority rule, the dialog box appears as follows:



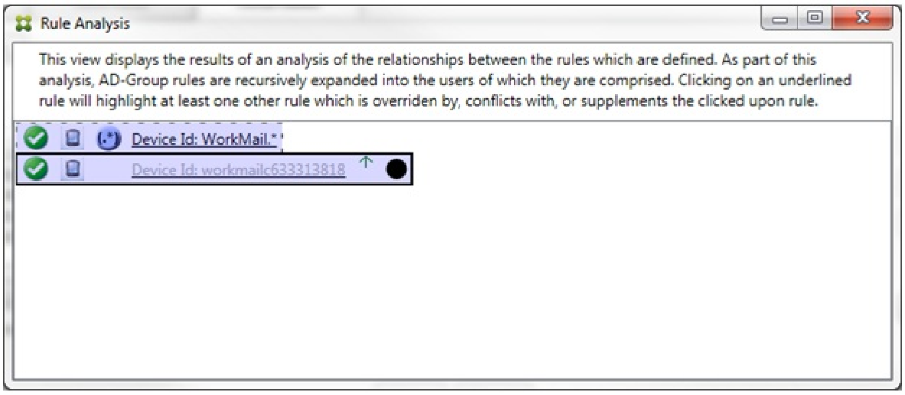
Rule Analysis

This view performs an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

Device Id: WorkMail.*

Device Id: workmailc633313818 ●

In this example, the regular expression rule WorkMail.* is the primary rule (indicated by the solid border) and the normal rule workmailc633313818 is an ancillary rule (indicated by the dashed border). The black dot next to the ancillary rule is a visual cue that further indicates that the rule is inactive (will never be evaluated) due to the higher-priority regular expression rule that precedes it. After clicking on the overridden rule, the dialog box appears as follows:



Rule Analysis

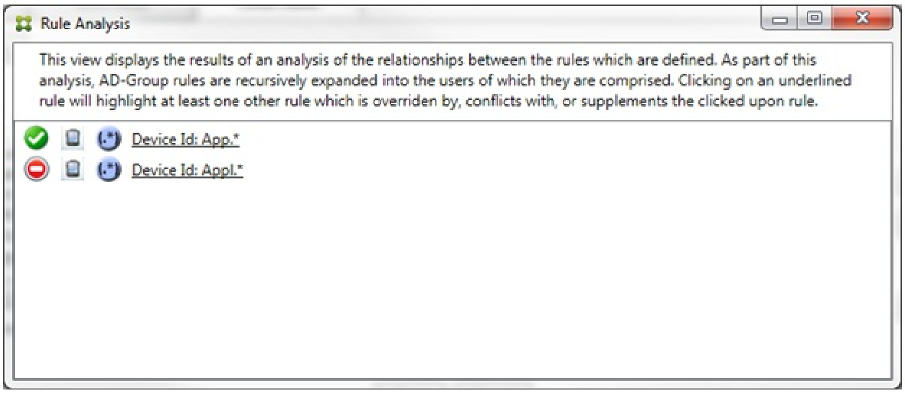
This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

Device Id: WorkMail.*

Device Id: workmailc633313818 ●

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 on either of the rules in a simple example, the dialog box appears as follows:

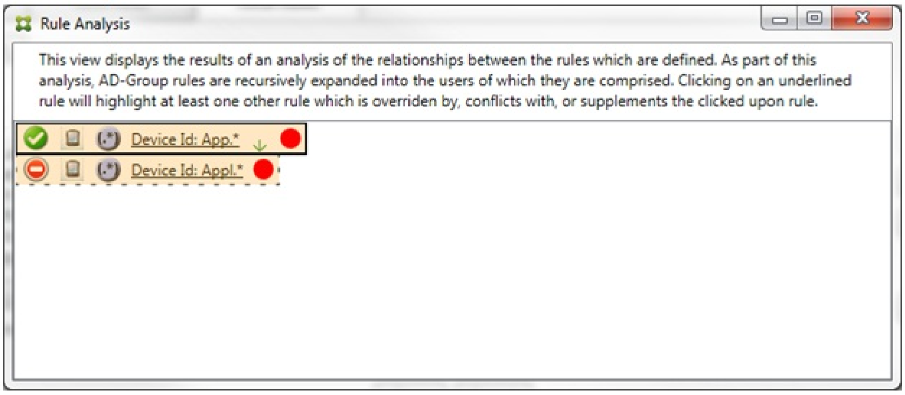


This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

Device Id: App.*

Device Id: Appl.*

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 on the first rule, the dialog box appears as follows:



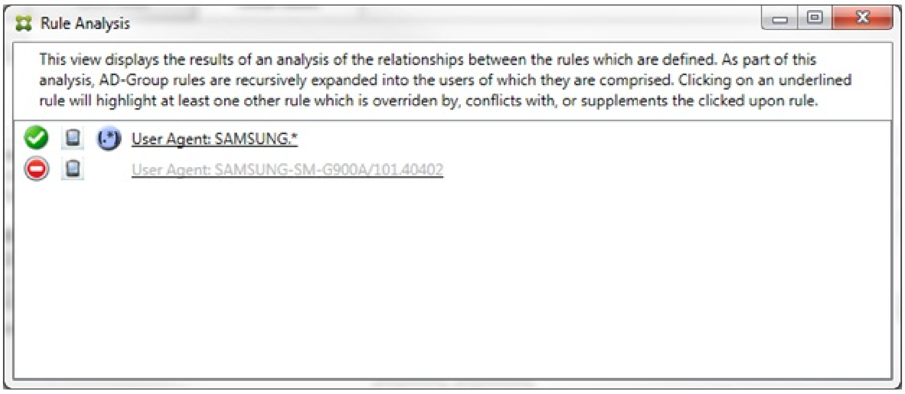
This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

Device Id: App.*

Device Id: Appl.*

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.



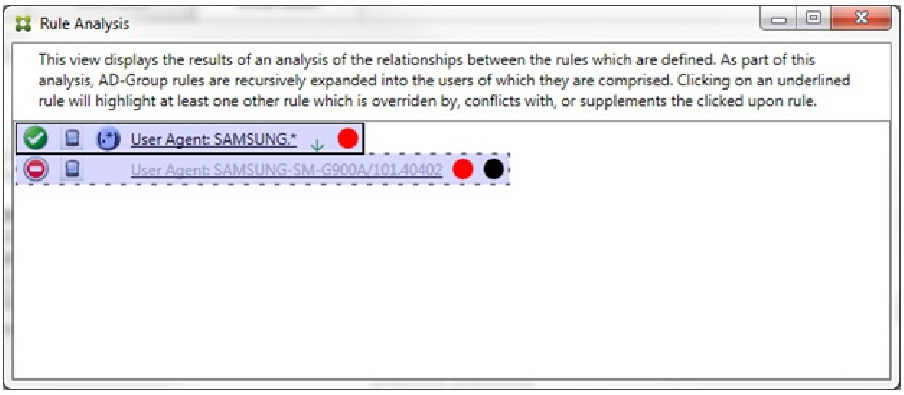
This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

User Agent: SAMSUNG.*

User Agent: SAMSUNG-SM-G900A/101.40402

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 on the regular expression rule, the dialog box appears as follows:



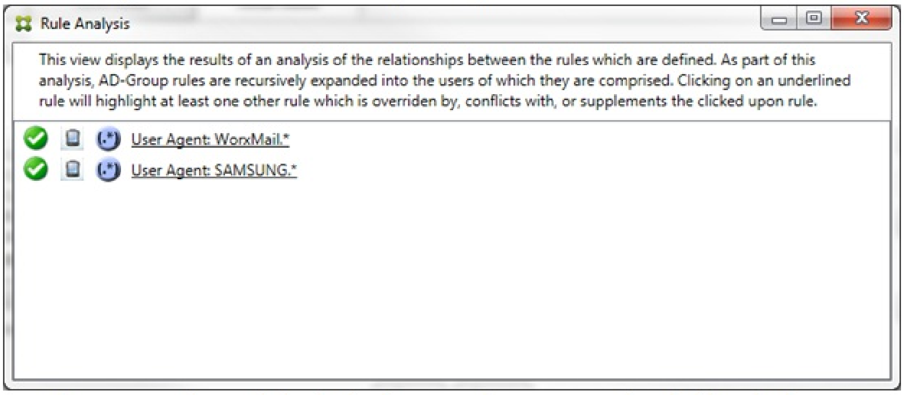
This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

✓ User Agent: SAMSUNG.* ●

⊖ User Agent: SAMSUNG-SM-G900A/101.40402 ● ●

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, as well as with a black dot to further indicate that it has been overridden and is 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 on either of the rules, in a simple example, the dialog box appears as follows:

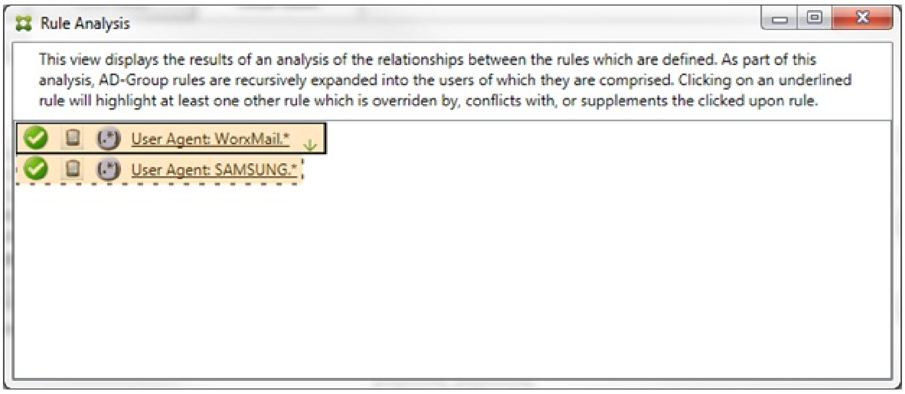


This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

✓ User Agent: WorxMail.*

✓ User Agent: SAMSUNG.*

Visual inspection easily reveals that both rules are regular expression rules which have both been applied to the ActiveSync device ID field in XenMobile Mail Manager. After clicking on the first rule, the dialog box looks as follows:



Rule Analysis

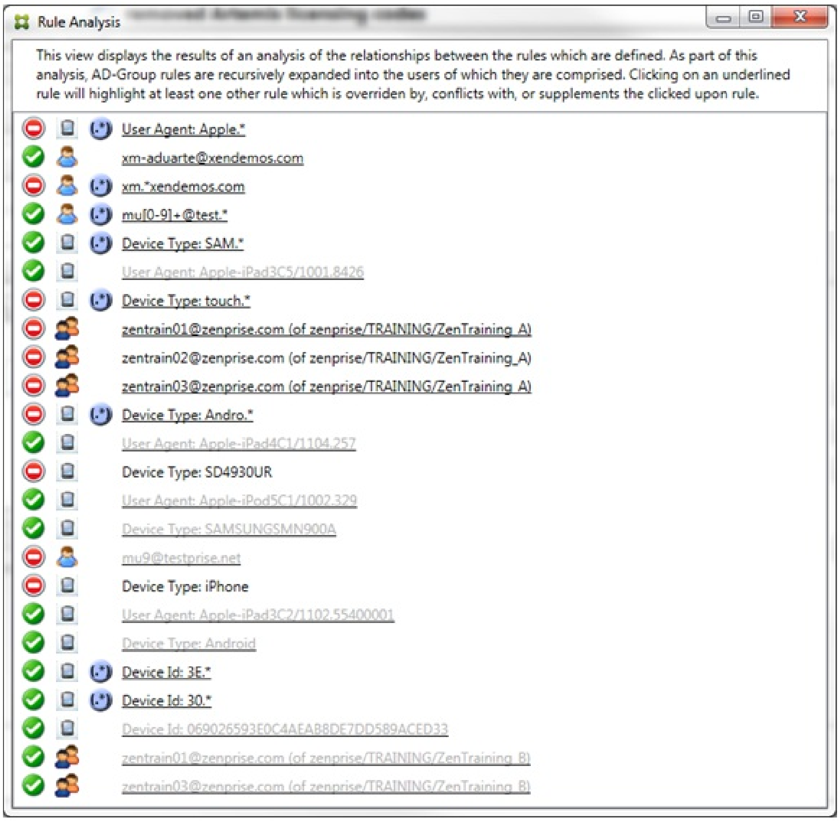
This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

✓ (.*) User Agent: WorxMail.*
✓ (.*) User Agent: SAMSUNG.*

The primary rule (regular expression rule WorkMail.*) is highlighted with a yellow overlay to indicate that there exists at least one additional 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 XenMobile Mail Manager; in this case, the ActiveSync device ID field.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.



Rule Analysis

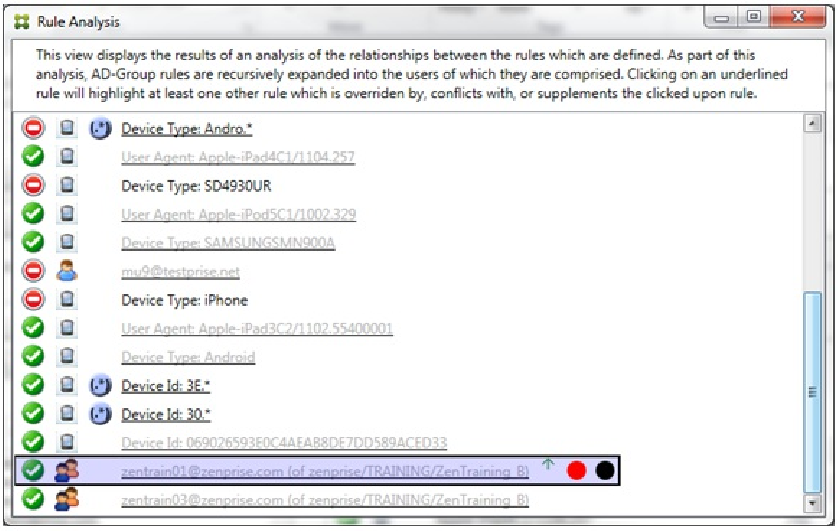
This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

⊖ (.*) User Agent: Apple.*
✓ xm-aduarte@xendemos.com
⊖ (.*) xm.*xendemos.com
✓ (.*) mu[0-9]+@test.*
✓ (.*) Device Type: SAM.*
✓ User Agent: Apple-iPad3C5/1001.8426
⊖ (.*) Device Type: touch.*
⊖ zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
⊖ zentrain02@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
⊖ zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
⊖ (.*) Device Type: Andro.*
✓ User Agent: Apple-iPad4C1/1104.257
⊖ Device Type: SD4930UR
✓ User Agent: Apple-iPod5C1/1002.329
✓ Device Type: SAMSUNGSMN900A
⊖ mu9@testprise.net
⊖ Device Type: iPhone
✓ User Agent: Apple-iPad3C2/1102.55400001
✓ Device Type: Android
✓ (.*) Device Id: 3E.*
✓ (.*) Device Id: 30.*
✓ Device Id: 069026593E0C4AEAB8DE7DD589ACED33
✓ zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining_B)
✓ zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining_B)

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.



Rule Analysis

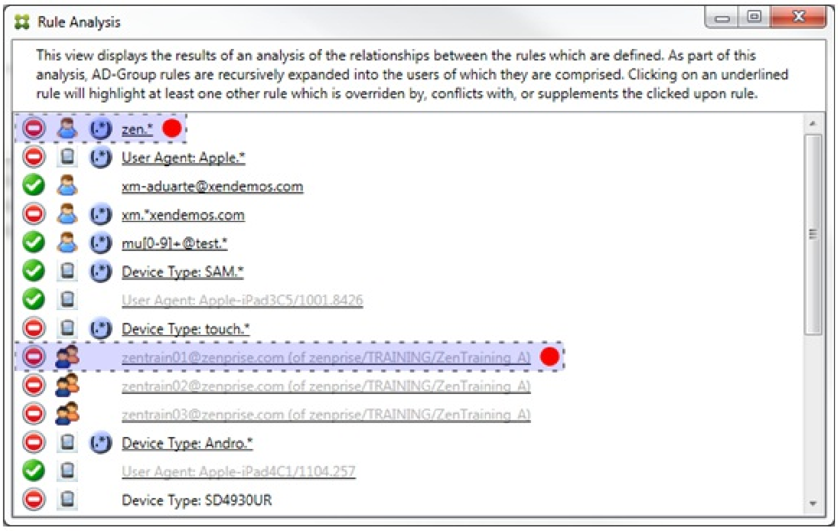
This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

Device Type: Andro.*
User Agent: Apple-iPad4C1/1104.257
Device Type: SD4930UR
User Agent: Apple-iPod5C1/1002.329
Device Type: SAMSUNGSMN900A
mu9@testprise.net
Device Type: iPhone
User Agent: Apple-iPad3C2/1102.55400001
Device Type: Android
Device Id: 3E.*
Device Id: 30.*
Device Id: 069026593E0C4AEAB8DE7DD589ACED33
zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining B) ↑ ● ●
zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining B)

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:



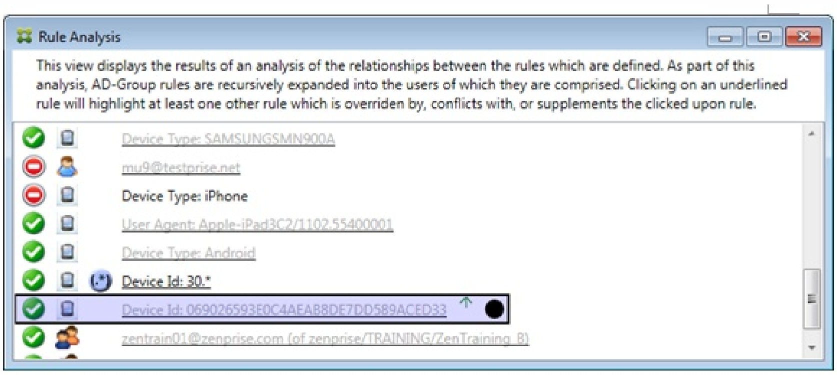
Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

zen.* ●
User Agent: Apple.*
xm-aduarte@xendemos.com
xm.*xendemos.com
mu[0-9]+@test.*
Device Type: SAM.*
User Agent: Apple-iPad3C5/1001.8426
Device Type: touch.*
zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining A) ●
zentrain02@zenprise.com (of zenprise/TRAINING/ZenTraining A)
zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining A)
Device Type: Andro.*
User Agent: Apple-iPad4C1/1104.257
Device Type: SD4930UR

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:

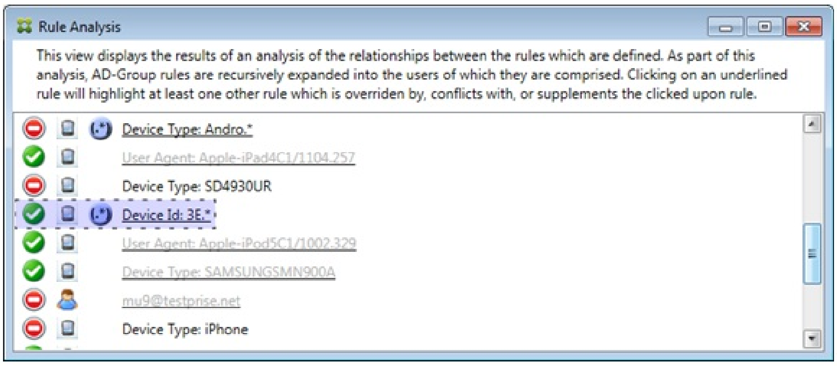


This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

✓ Device Type: SAMSUNGSMN900A
⊖ mu9@testprise.net
⊖ Device Type: iPhone
✓ User Agent: Apple-iPad3C2/1102.55400001
✓ Device Type: Android
✓ (.*) Device Id: 30.*
✓ Device Id: 069026593E0C4AEAB8DE7DD589ACED33 ↑ ●
✓ zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining_B)

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.



This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

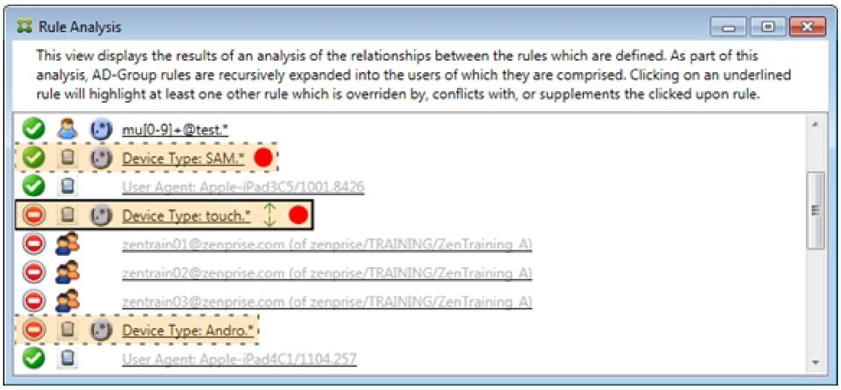
⊖ (.*) Device Type: Andro.*
✓ User Agent: Apple-iPad4C1/1104.257
⊖ Device Type: SD4930UR
✓ (.*) Device Id: 3E.*
✓ User Agent: Apple-iPod5C1/1002.329
✓ Device Type: SAMSUNGSMN900A
⊖ mu9@testprise.net
⊖ Device Type: iPhone

In this case, a single ancillary rule overrides the primary rule: the regular expression ActiveSynce device ID rule 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 SAM.* and the regular expression ActiveSync device type rule Andro.*
- Both of the ancillary rules are bordered with dashes to indicate that they are ancillary.
- Both of the ancillary rules are overlayed with yellow to indicate that they are supplementally being applied to the rule field of ActiveSync device type.
- You should ensure in such scenarios that their regular expression rules are not redundant.



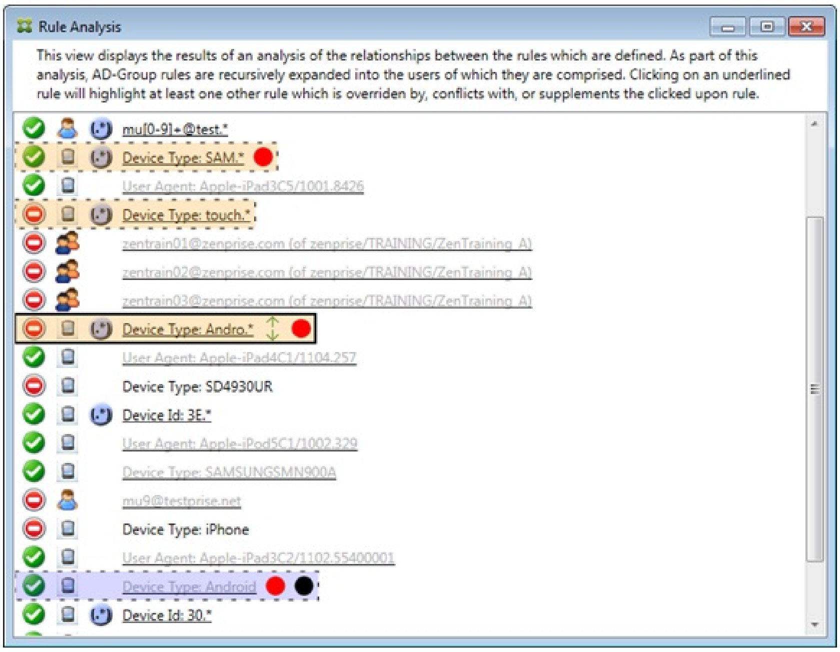
Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

mu[0-9]+@test.*
Device Type: SAM.* ●
User Agent: Apple-iPad3C5/1001.8426
Device Type: touch.* ↕ ●
zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining A)
zentrain02@zenprise.com (of zenprise/TRAINING/ZenTraining A)
zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining A)
Device Type: Andro.*
User Agent: Apple-iPad4C1/1104.257

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 on the regular expression rule applied to the rule field of device type with a value of touch.* Clicking on the ancillary rule Andro.* shows a different set of ancillary rules highlighted.



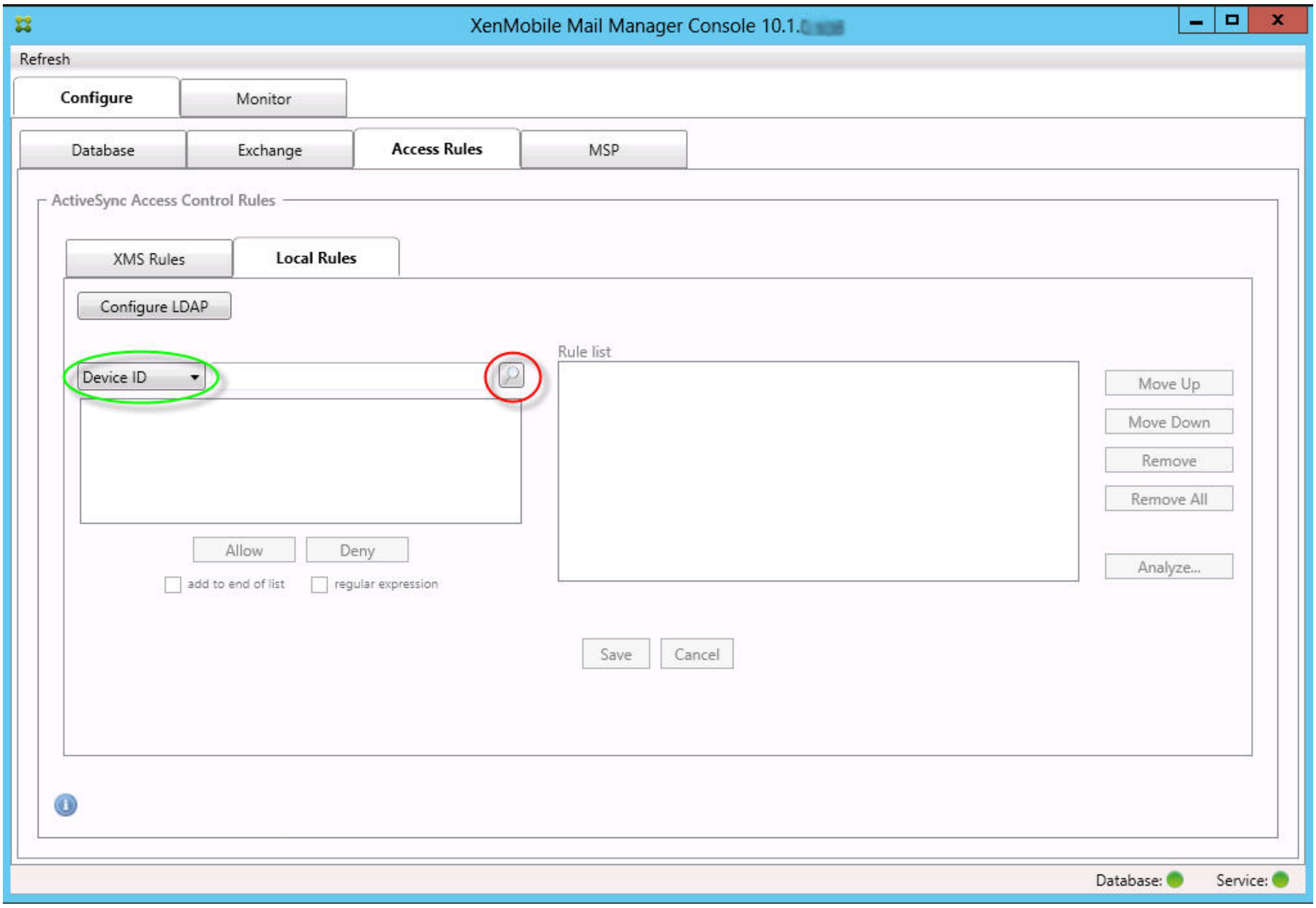
Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

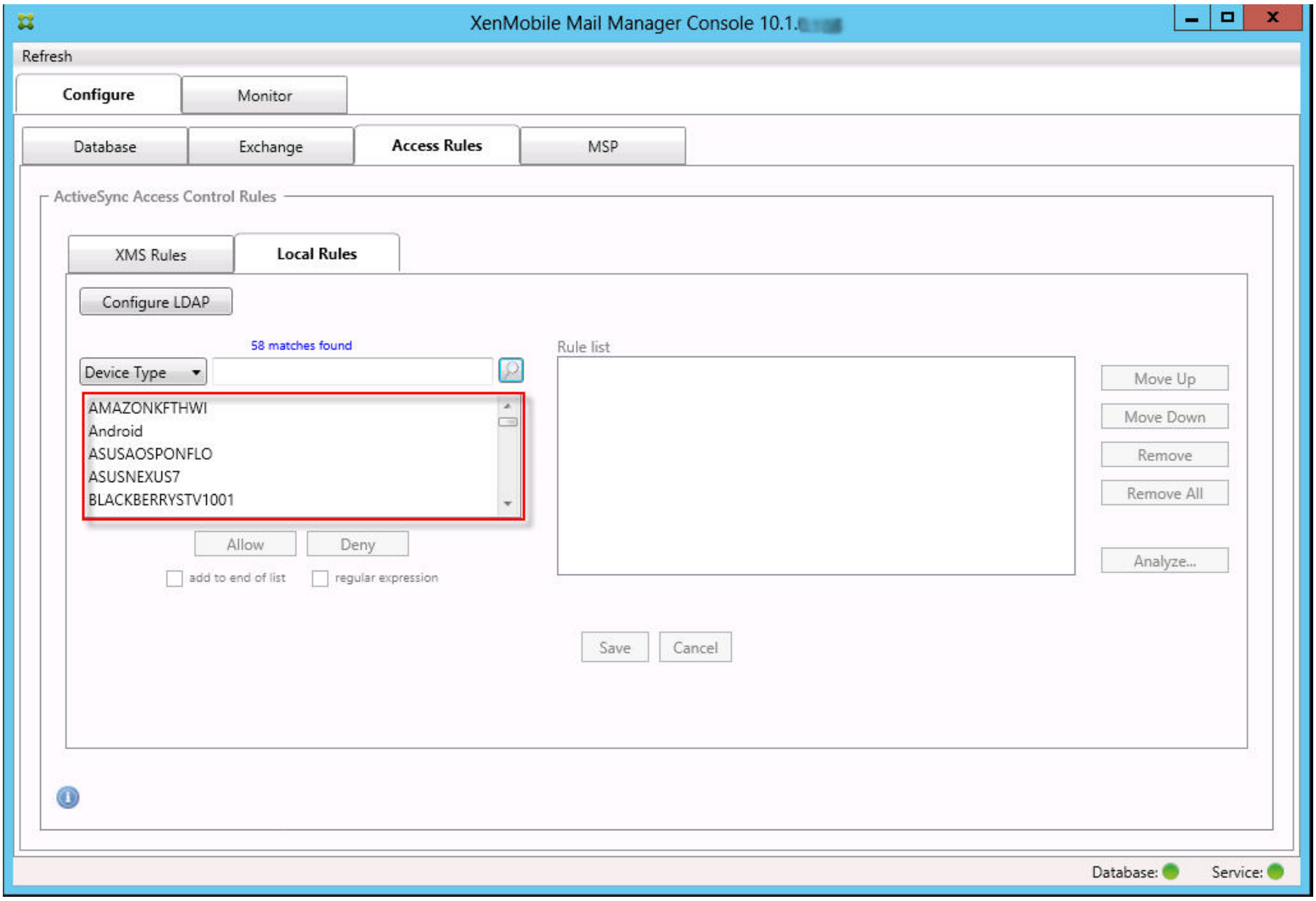
mu[0-9]+@test.*
Device Type: SAM.* ●
User Agent: Apple-iPad3C5/1001.8426
Device Type: touch.*
zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining A)
zentrain02@zenprise.com (of zenprise/TRAINING/ZenTraining A)
zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining A)
Device Type: Andro.* ↕ ●
User Agent: Apple-iPad4C1/1104.257
Device Type: SD4930UR
Device Id: 3E.*
User Agent: Apple-iPod5C1/1002.329
Device Type: SAMSUNGSMN900A
mu9@testprise.net
Device Type: iPhone
User Agent: Apple-iPad3C2/1102.55400001
Device Type: Android ● ●
Device Id: 30.*

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.

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 on 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.



XenMobile Mail Manager Console 10.1.[redacted]

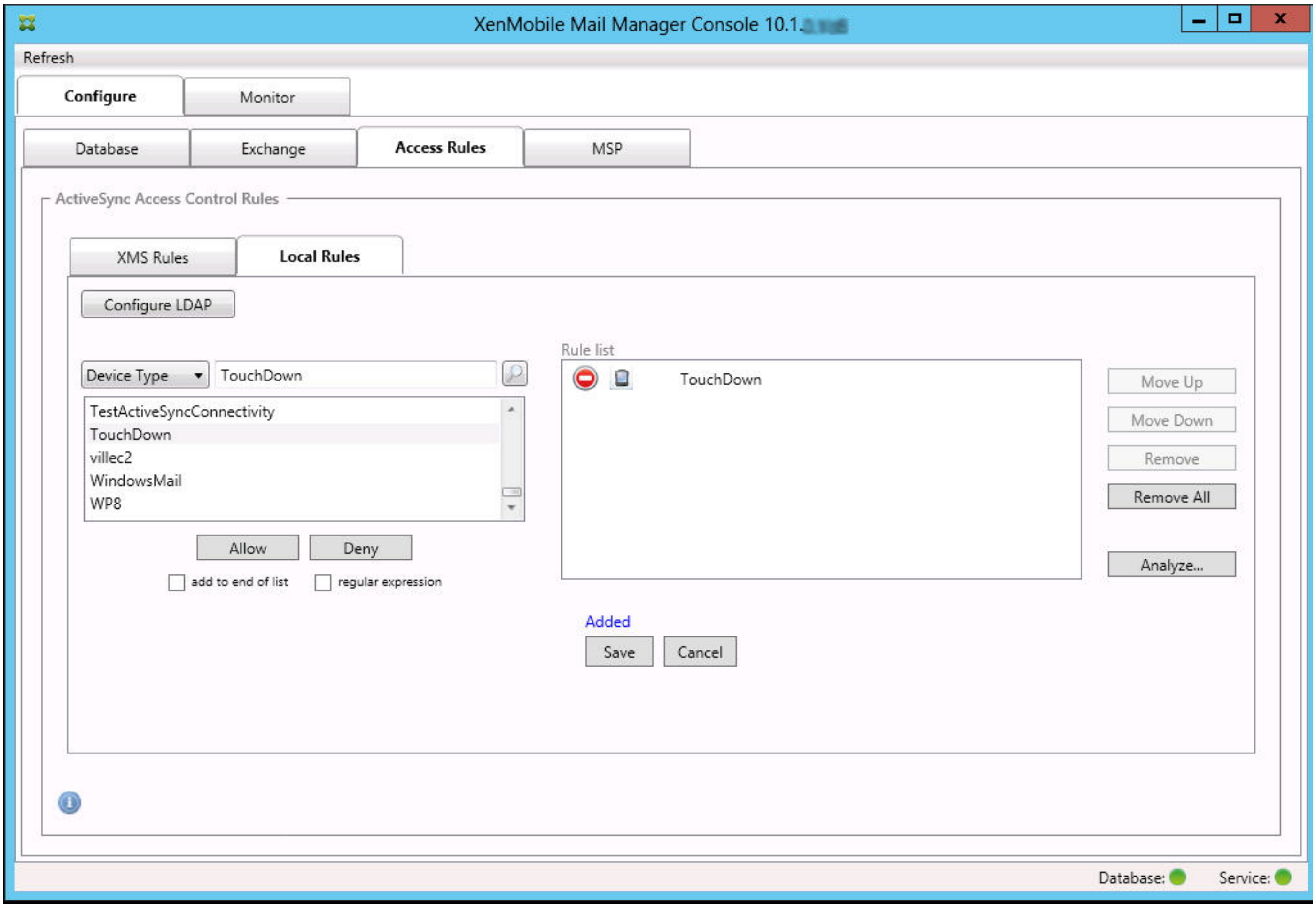
Device Type

58 matches found

AMAZONKFTHWI
Android
ASUSAOSPONFLO
ASUSNEXUS7
BLACKBERRYSTV1001

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.

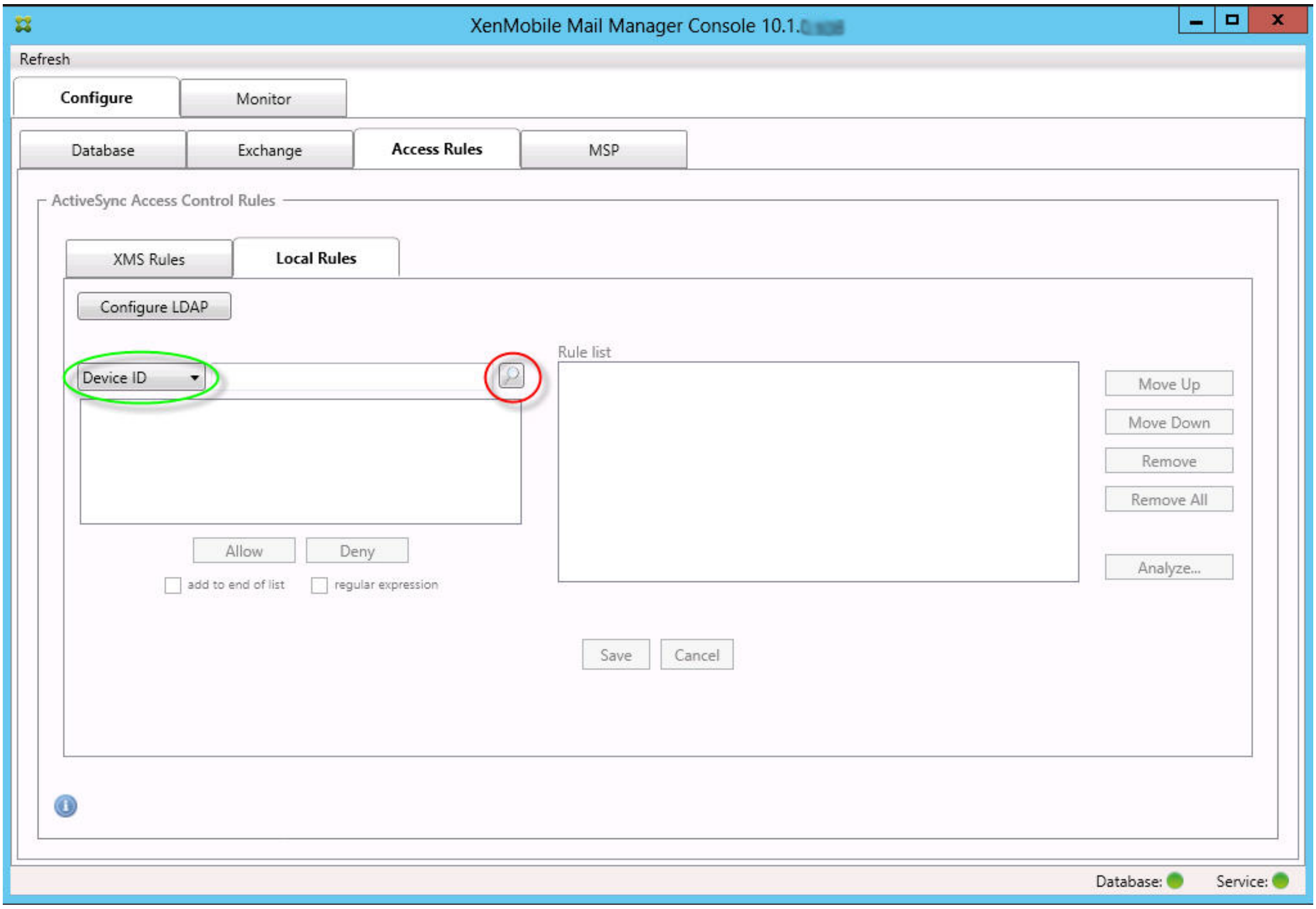
   In this example, all devices that have a device type of TouchDown are denied access.



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.

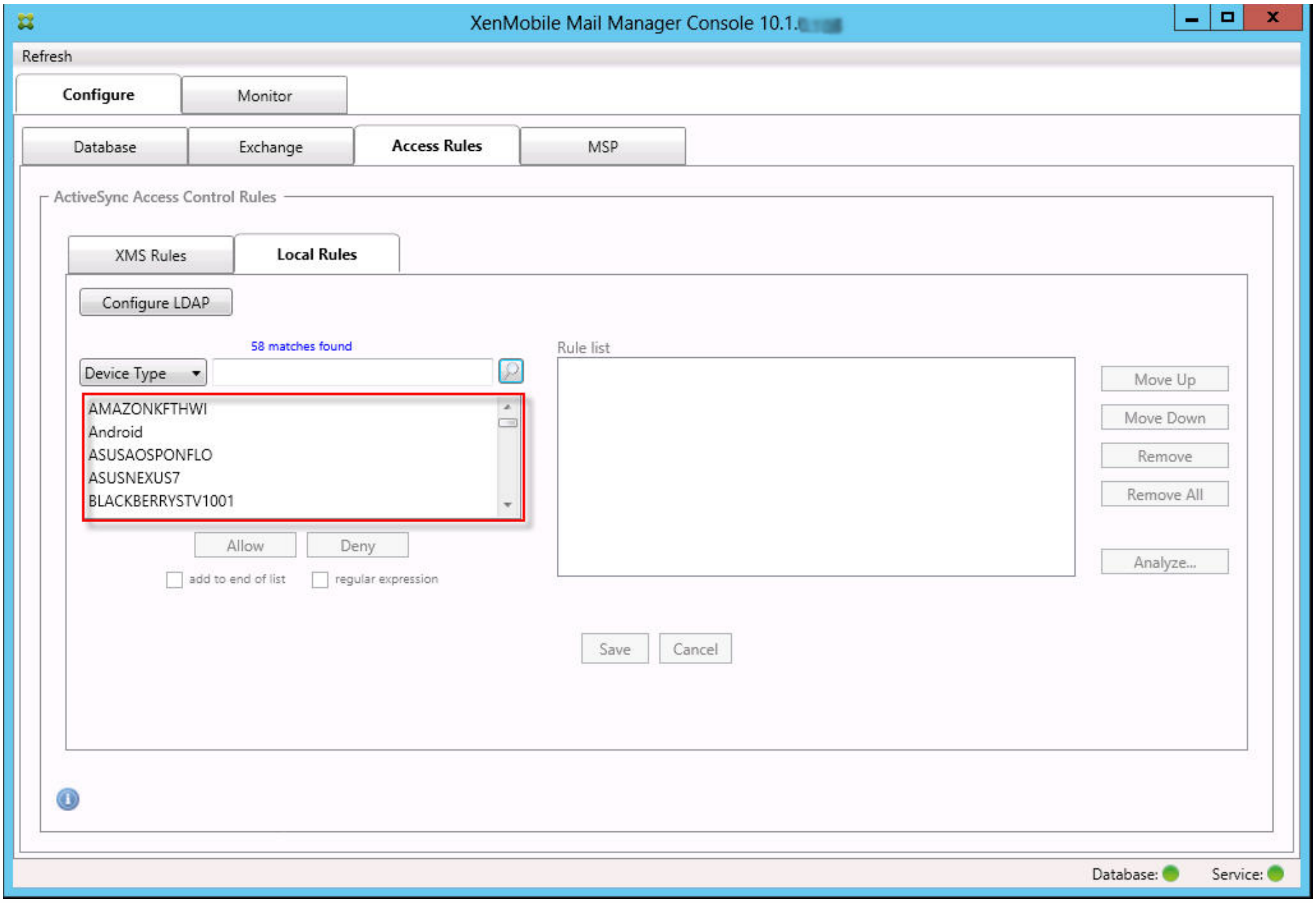
To build a regular expression from an existing field value

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 on 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.

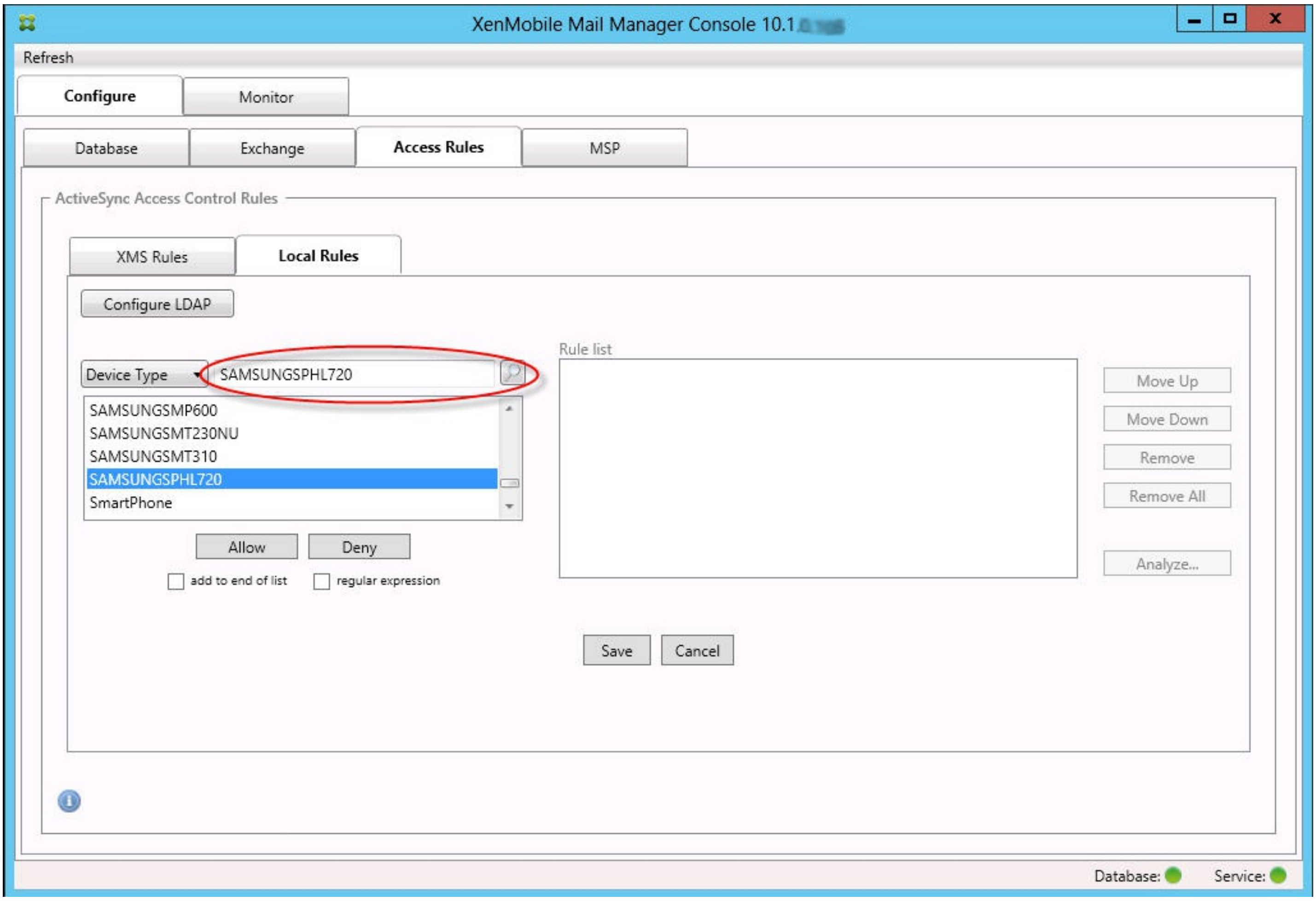


58 matches found

Device Type

AMAZONKFTHWI
Android
ASUSAOSPONFLO
ASUSNEXUS7
BLACKBERRYSTV1001

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**.



Device Type: SAMSUNGSPHL720

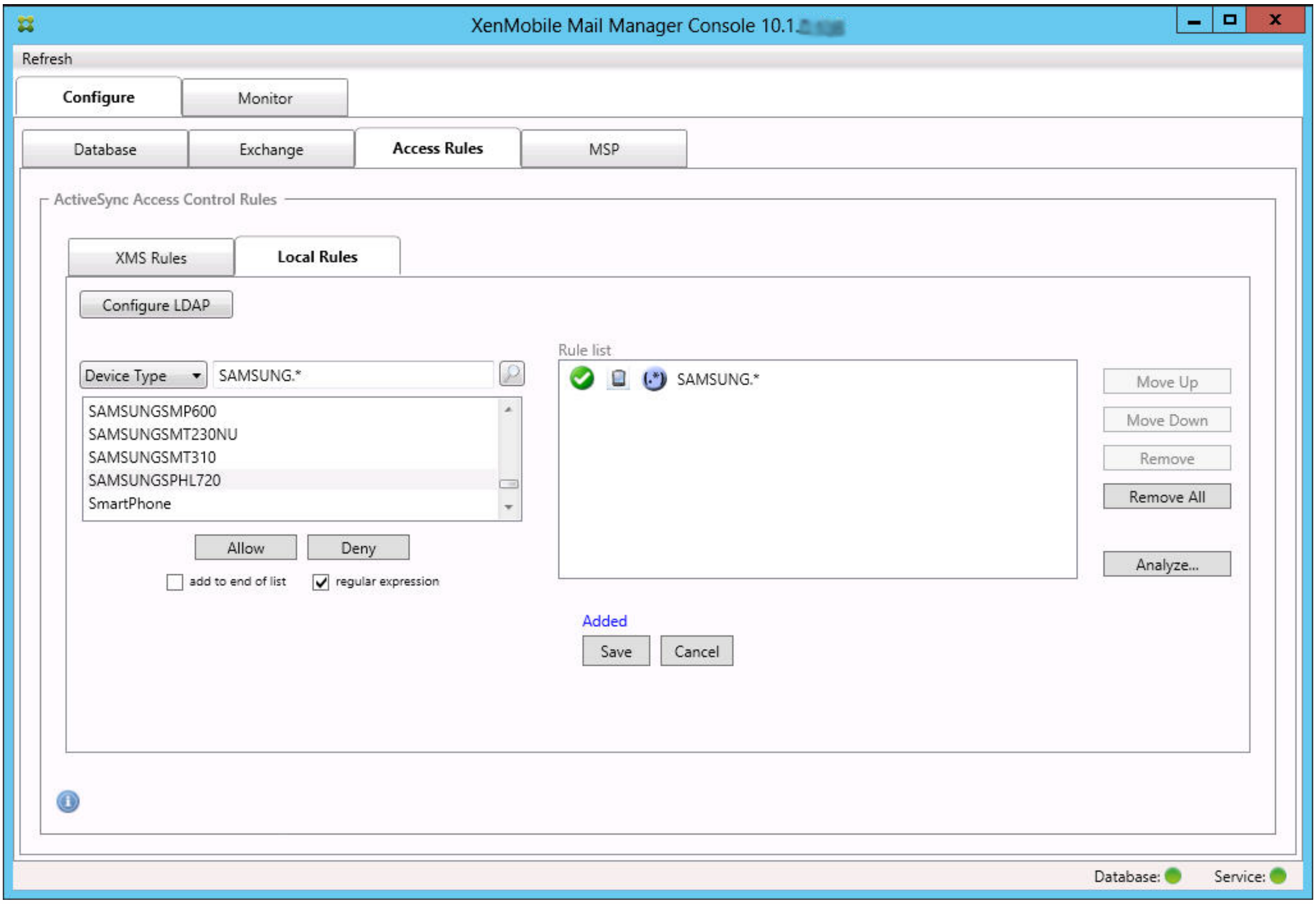
5. To allow all device types that have "Samsung" in their device type value, add a regular expression rule by following these steps:

a. Click within the selected item text box.

b. Change the text from SAMSUNGSPHL720 to SAMSUNG.*

c. Make sure that the regular expression check box is selected.

d. Click **Allow**.



Device Type SAMSUNG.*

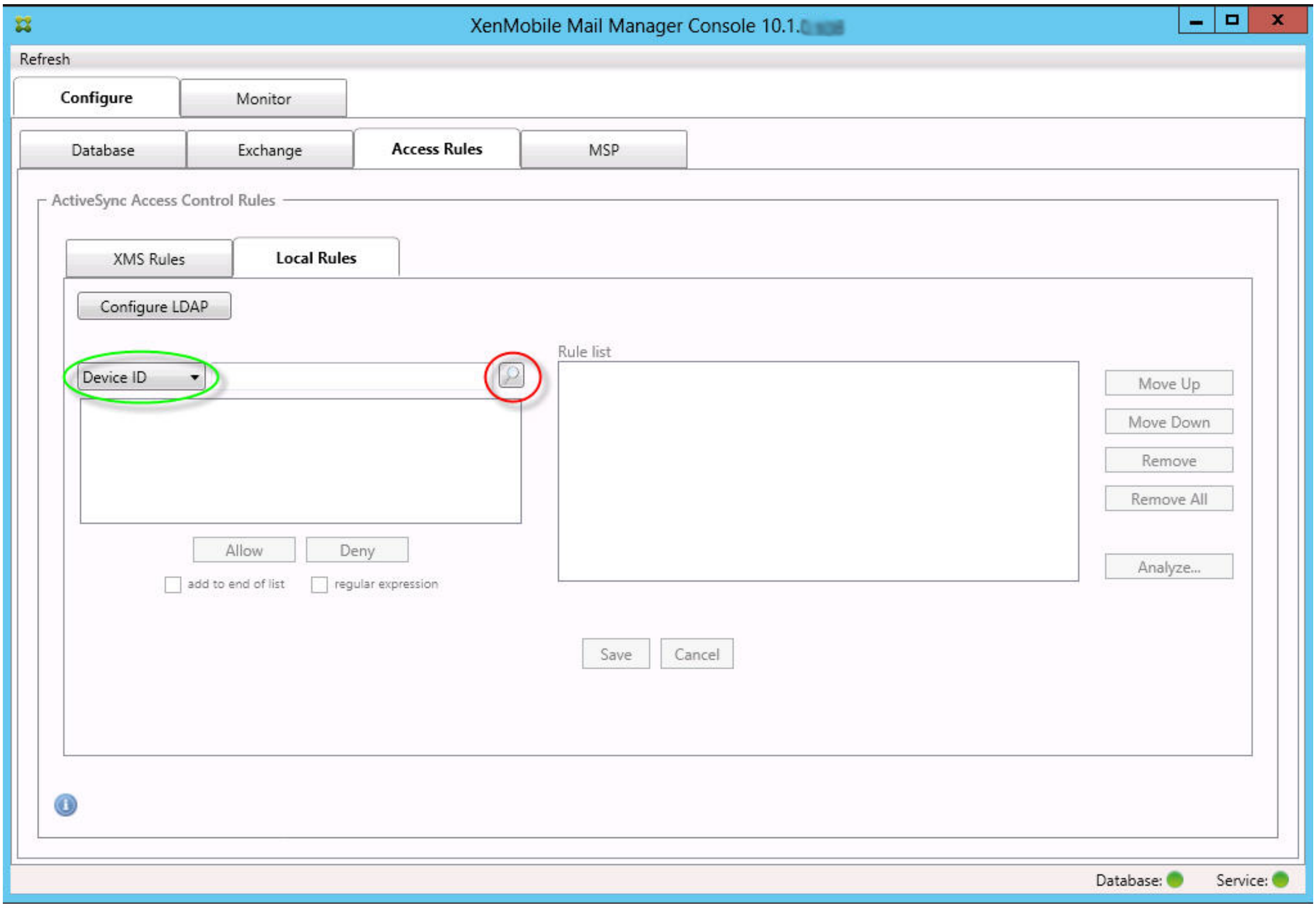
SAMSUNGSMP600
SAMSUNGSMT230NU
SAMSUNGSMT310
SAMSUNGSPHL720
SmartPhone

☐ add to end of list ☑ regular expression

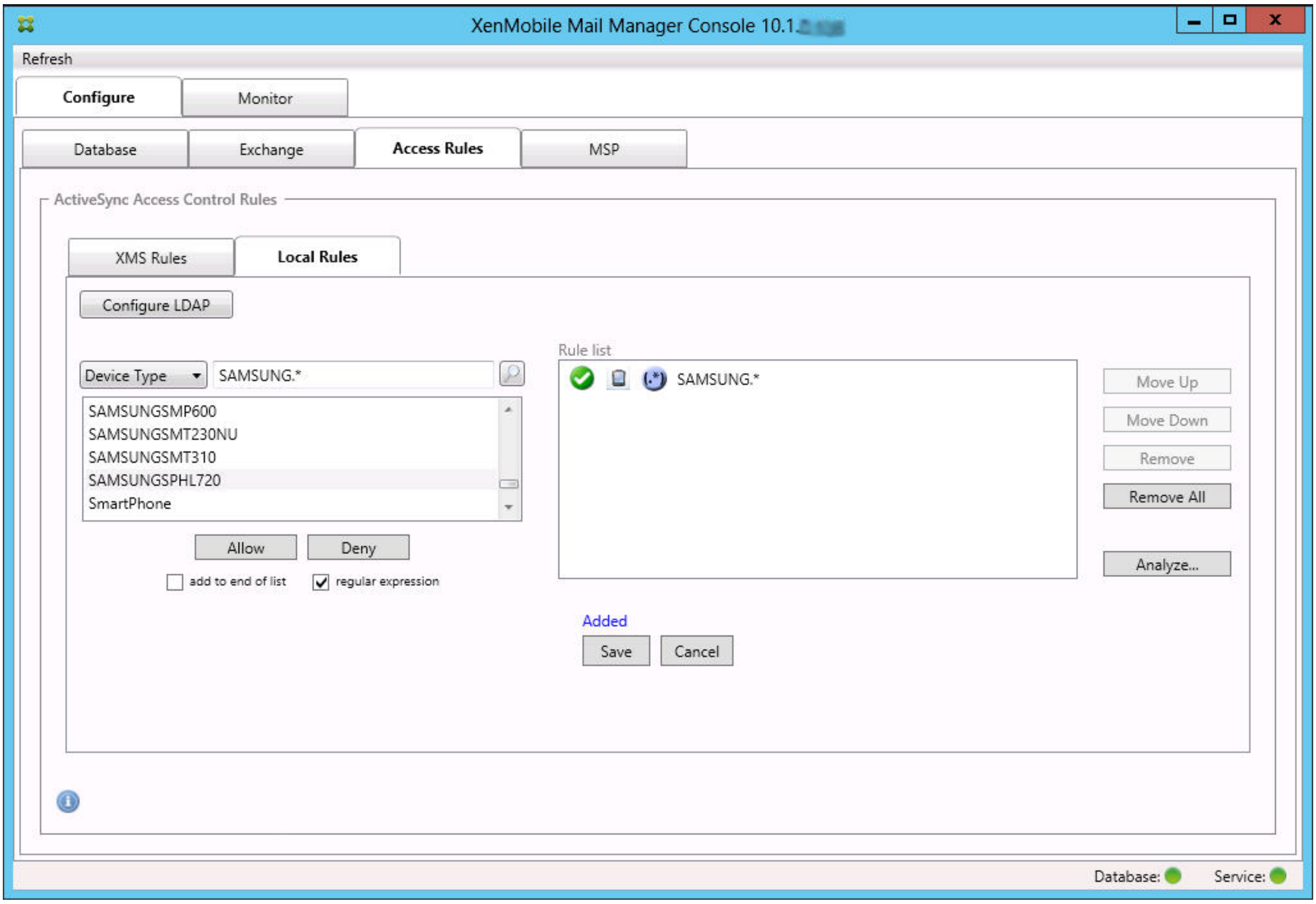
Rule list
✓ SAMSUNG.*

Added

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.

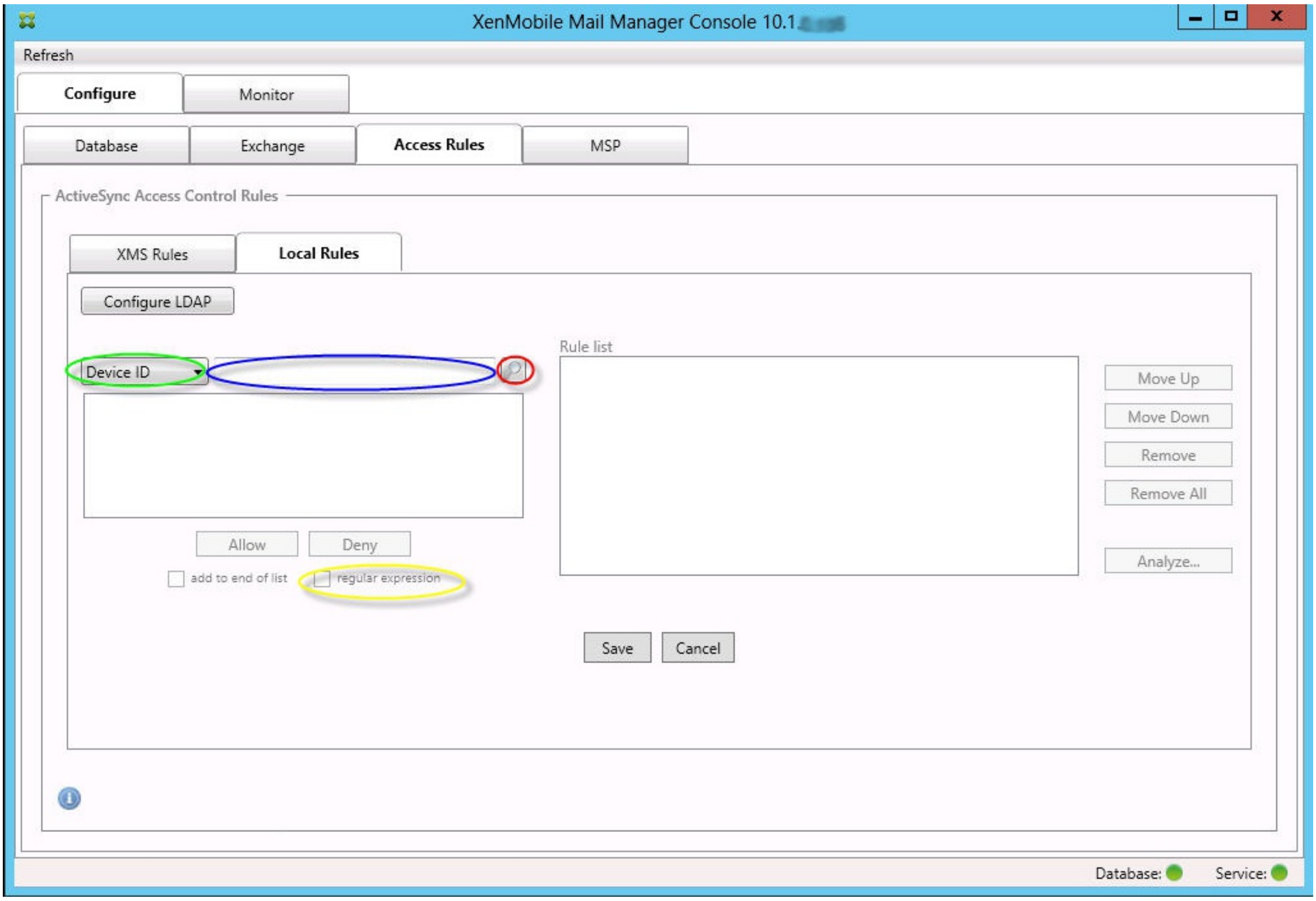


3. Select the field you want to match against. This example uses Device Type.
4. Type in the regular expression. This example uses samsung.*
5. Ensure that the regular expression check box is selected and then click Allow or Deny. In this example, the choice is Allow so that the final result is as follows:

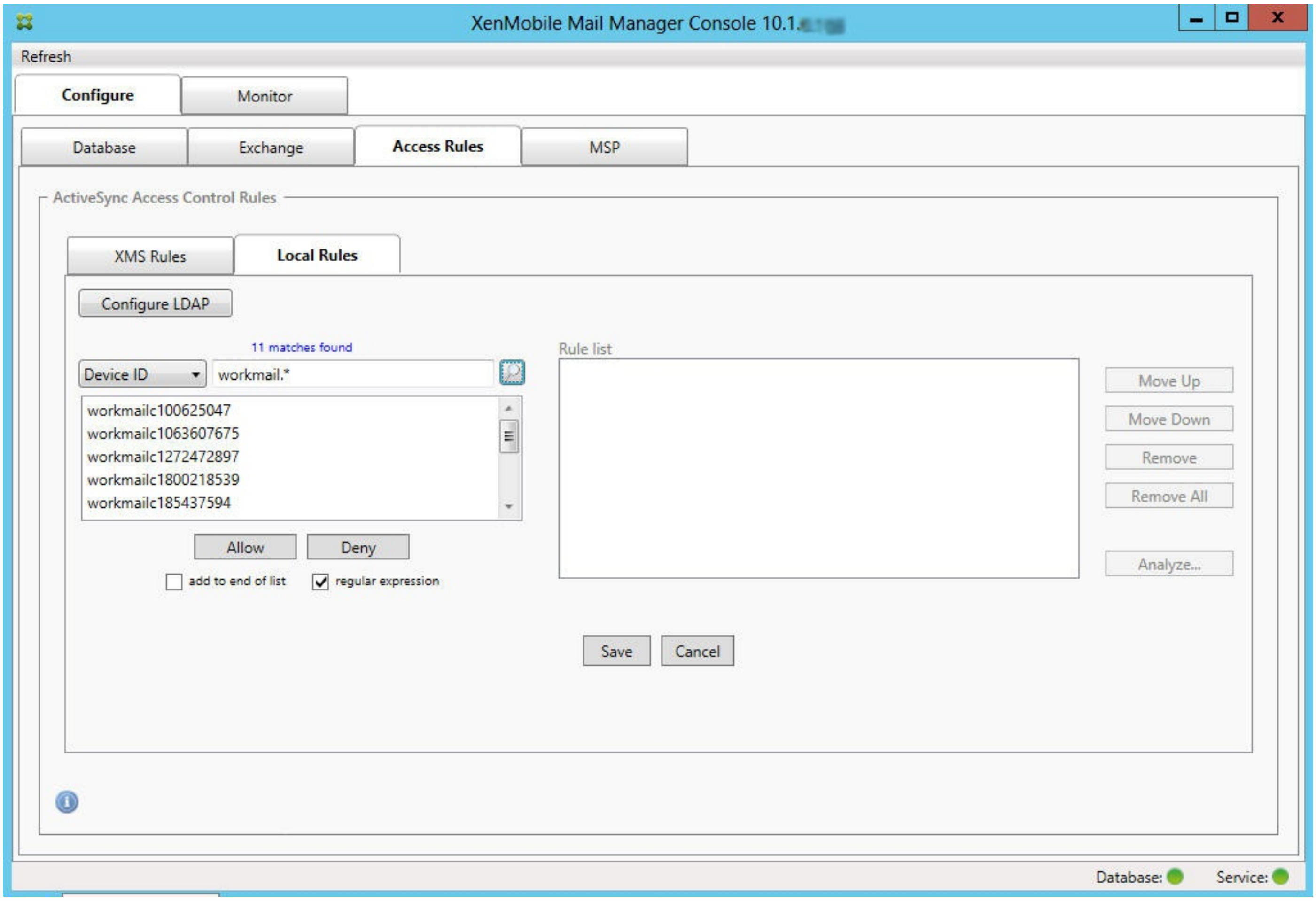


By selecting the regular expression check box, you can run searches for specific devices that match the given expression. This feature is only available if a major snapshot has successfully completed. You can use this feature even if there is no plan to use regular expression rules. For example, assume 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. Make sure the regular expression check box is selected and then click the magnifying glass icon to display matches as shown in the following figure.



11 matches found

Device ID ▾ workmail.*

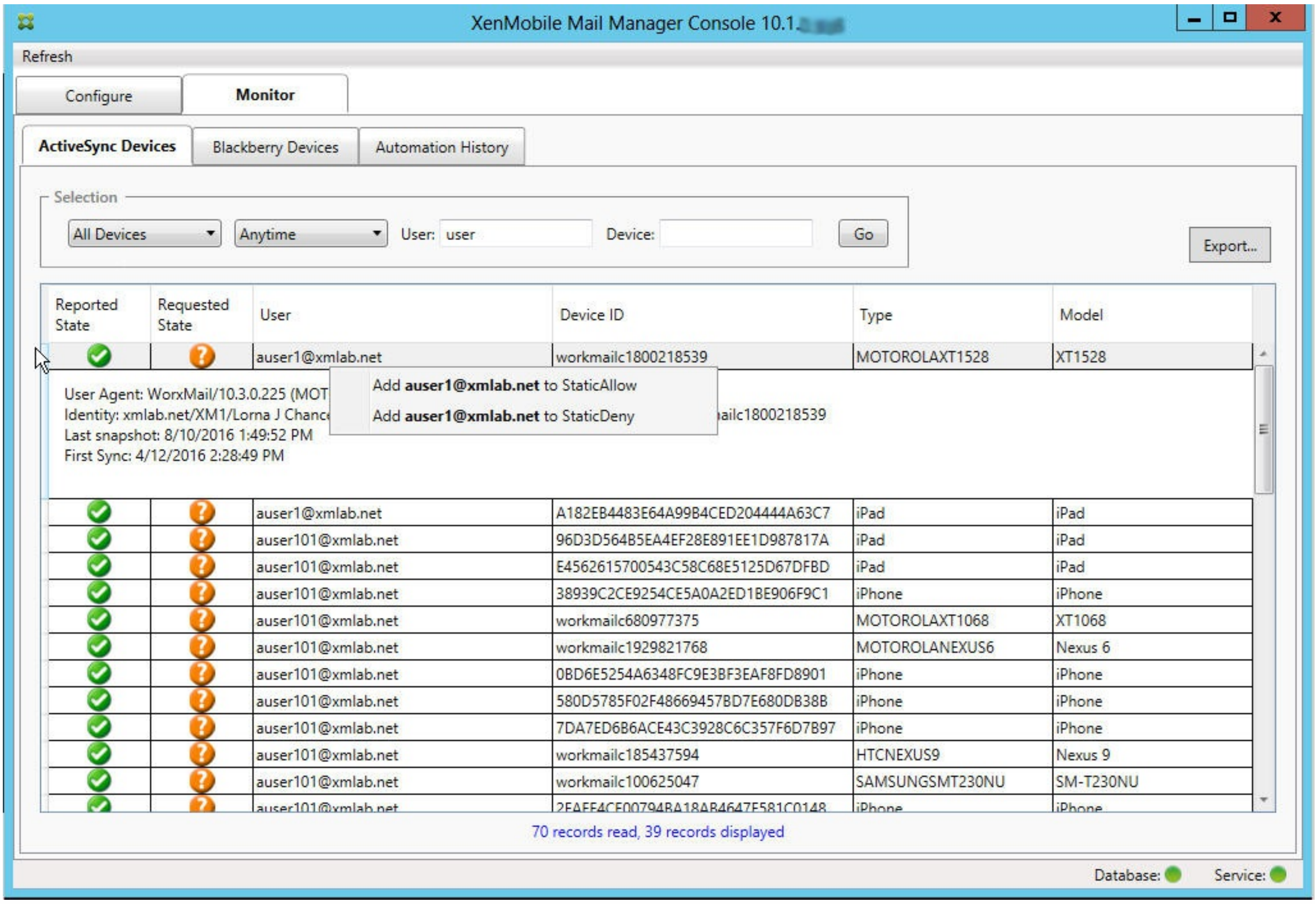
workmailc100625047
workmailc1063607675
workmailc1272472897
workmailc1800218539
workmailc185437594

□ add to end of list ☑ regular expression

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.



User: user

Device:

Reported State	Requested State	User	Device ID	Type	Model
✓	?	auser1@xmlab.net	workmailc1800218539	MOTOROLAXT1528	XT1528
✓	?	auser1@xmlab.net	A182EB4483E64A99B4CED204444A63C7	iPad	iPad
✓	?	auser101@xmlab.net	96D3D564B5EA4EF28E891EE1D987817A	iPad	iPad
✓	?	auser101@xmlab.net	E4562615700543C58C68E5125D67DFBD	iPad	iPad
✓	?	auser101@xmlab.net	38939C2CE9254CE5A0A2ED1BE906F9C1	iPhone	iPhone
✓	?	auser101@xmlab.net	workmailc680977375	MOTOROLAXT1068	XT1068
✓	?	auser101@xmlab.net	workmailc1929821768	MOTOROLANEXUS6	Nexus 6
✓	?	auser101@xmlab.net	0BD6E5254A6348FC9E3BF3EAF8FD8901	iPhone	iPhone
✓	?	auser101@xmlab.net	580D5785F02F48669457BD7E680DB38B	iPhone	iPhone
✓	?	auser101@xmlab.net	7DA7ED6B6ACE43C3928C6C357F6D7B97	iPhone	iPhone
✓	?	auser101@xmlab.net	workmailc185437594	HTCNEXUS9	Nexus 9
✓	?	auser101@xmlab.net	workmailc100625047	SAMSUNGSMT230NU	SM-T230NU
✓	?	auser101@xmlab.net	2FAFF4CF00794BA18AB4647F581C0148	iPhone	iPhone

User Agent: WorxMail/10.3.0.225 (MOT
Identity: xmlab.net/XM1/Lorna J Chanc ailc1800218539
Last snapshot: 8/10/2016 1:49:52 PM
First Sync: 4/12/2016 2:28:49 PM

Add **auser1@xmlab.net** to StaticAllow
Add **auser1@xmlab.net** to StaticDeny

70 records read, 39 records displayed

The **Monitor** tab in XenMobile Mail Manager 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.

XenMobile Mail Manager logs errors and other operational information to its log file: <Install Folder>\log\XmmWindowsService.log. XenMobile Mail Manager also logs significant events to the Windows Event Log.

The following list includes common errors:

XenMobile Mail Manager service doesn't start

Check the log file and the Windows Event Log for errors. Typical causes are as follows:

- The XenMobile Mail Manager 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 XenMobile Mail Manager service must be an allowed SQL logon. The account of the XenMobile Mail Manager 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.

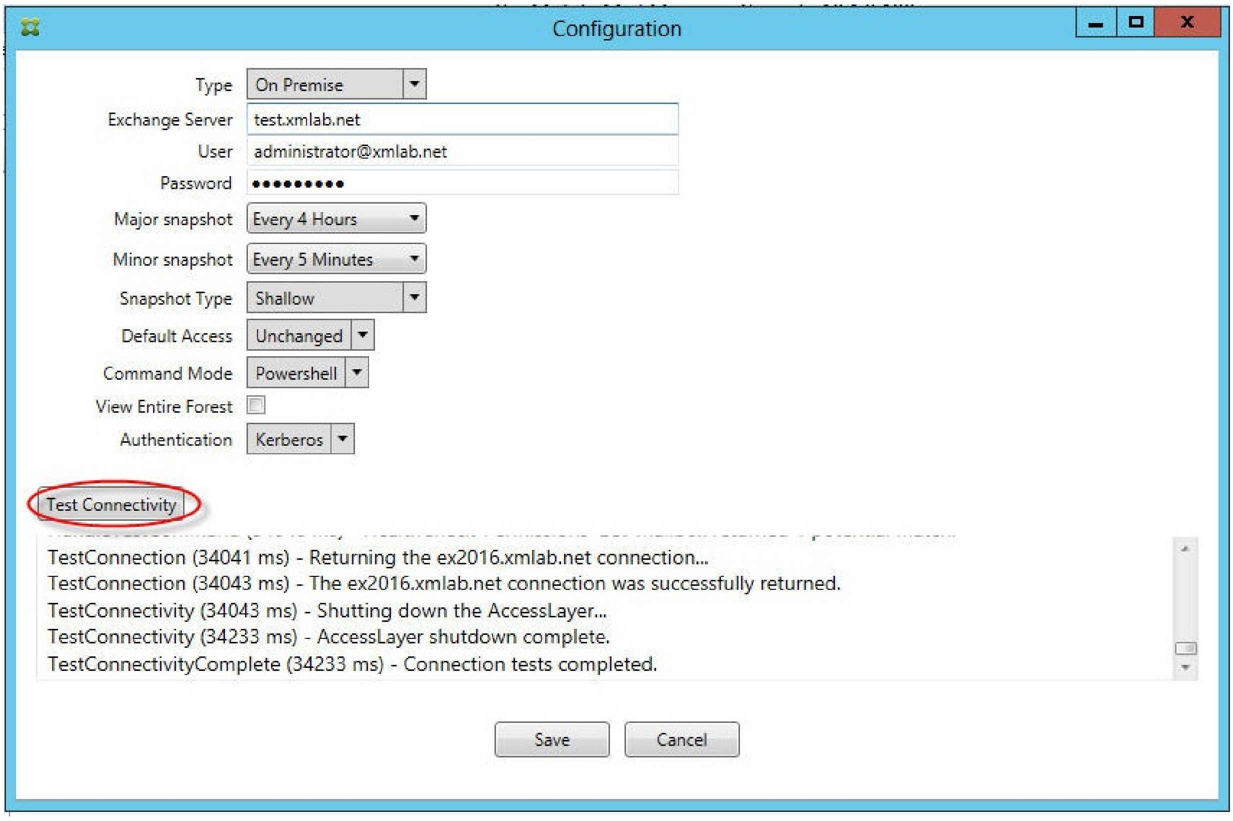
- The port configured for the Mobile Service Provider (MSP) is not available. A listening port must be selected that is not used by another process on the system.

XenMobile cannot connect to the MSP

Check that the MSP service port and transport is properly configured in the Configure> MSP tab of the XenMobile Mail Manager 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 http://msdn.microsoft.com/en-us/library/ms733791.aspx for details on installing certificates.

XenMobile Mail Manager 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 XenMobile and then click Test Connectivity. This simulates the web service requests that XenMobile service issues. Note that if HTTPS is configured, you must specify the actual host name of the server (the name specified in the SSL certificate).

Note: When using **Test Connectivity**, be sure to have at least one ActiveSyncDevice record or the test may fail.



Type	On Premise
Exchange Server	test.xmlab.net
User	administrator@xmlab.net
Password	●●●●●●●●●●
Major snapshot	Every 4 Hours
Minor snapshot	Every 5 Minutes
Snapshot Type	Shallow
Default Access	Unchanged
Command Mode	Powershell
View Entire Forest	□
Authentication	Kerberos

```
TestConnection (34041 ms) - Returning the ex2016.xmlab.net connection...
TestConnection (34043 ms) - The ex2016.xmlab.net connection was successfully returned.
TestConnectivity (34043 ms) - Shutting down the AccessLayer...
TestConnectivity (34233 ms) - AccessLayer shutdown complete.
TestConnectivityComplete (34233 ms) - Connection tests completed.
```

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 cdmlets to a text file.

XenMobile NetScaler Connector

Jan 02, 2018

XenMobile NetScaler Connector 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 XenMobile and by rules defined locally by XenMobile NetScaler Connector.

For more information, see ActiveSync Gateway in XenMobile.

For a detailed reference architecture diagram, see the XenMobile Deployment Handbook article, Reference Architecture for On-Premises Deployments.

This article includes the following sections:

- Monitoring XenMobile NetScaler Connector
- To simulate ActiveSync traffic with XenMobile NetScaler Connector
- Choosing filters for XenMobile NetScaler Connector
- To configure a connection to XenMobile NetScaler Connector
- To import a policy from XenMobile
- Configuring XenMobile NetScaler Connector policy mode
- Configuring XenMobile NetScaler Connector
- Choosing a Security Model for XenMobile NetScaler Connector
- Managing XenMobile NetScaler Connector
- Installing XenMobile NetScaler Connector
- XenMobile NetScaler Connector system requirements
- Deploying XenMobile NetScaler Connector

The XenMobile NetScaler Connector 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 XenMobile NetScaler Connector by NetScaler for authorization.

Also, to make sure the XenMobile NetScaler Connector web service is running, you can load the following URL into a browser on the XenMobile NetScaler Connector server http://<host:port>/services/ActiveSync/Version. If the URL returns the product version as a string, the web service is responsive.

You can use the XenMobile NetScaler Connector to simulate what ActiveSync traffic will look like in conjunction with your policies. In the XenMobile NetScaler Connector configuration utility, select the **Simulations** tab. The results show you how your policies will apply according to the rules you have configured.

The XenMobile NetScaler Connector 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 XenMobile NetScaler Connector within XenMobile.

- **Blacklisted Apps**. Allows or denies devices based on the Device List defined by blacklist policies and the presence of blacklisted apps.
- **Whitelisted Apps only**. Allows or denies devices based on the Device List defined by whitelist policies and the presence of non-whitelisted apps.
- **Unmanaged Devices**. Creates a Device List of all devices in the XenMobile database. The Mobile Application Gateway needs to be deployed in a Block Mode.
- **Rooted Android /Jailbroken iOS Devices**. Creates a Device List of all devices flagged as rooted and allows or denies based on rooted status.
- **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.
- **Noncompliant password**. Creates a Device List of all devices that do not have a passcode on the device.
- **Revoked Status**. Creates a Device List of all revoked devices and allows or denies based on revoked status.
- **Inactive devices**. Creates a Device List of devices that have not communicated with XenMobile within a specified period of time and are thus considered inactive and allows or denies the devices accordingly.
- **Anonymous Devices**. Allows or denies devices that are enrolled in XenMobile 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.
- **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 XenMobile NetScaler Connector status in the Devices tab is enabled and shows the XenMobile NetScaler Connector status for your devices. The Implicit Allow/Deny option also controls all of the other XenMobile NetScaler Connector filters that have not been selected. For example, Blacklists Apps will be denied (blocked) by XenMobile NetScaler Connector, whereas all other filters will be allowed because the Implicit Allow/Deny option is selected to Allow.

XenMobile NetScaler Connector communicates with XenMobile and other remote configuration providers through secure web services.

1. In the XenMobile NetScaler Connector 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 XenMobile Server.
3. In **Url**, enter the web address of the XenMobile 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 XenMobile server.
5. In **Managing Host**, enter the XenMobile NetScaler Connector 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 XenMobile NetScaler Connector to notify XenMobile when a device

is blocked. This option is required if you are using the XenMobile NetScaler Connector rules in any of your XenMobile 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, XenMobile NetScaler Connector 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.

1. In the XenMobile NetScaler Configuration 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 XenMobile Server and that has administrative privileges.
3. In **Url**, enter the web address of the XenMobile 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 XenMobile 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 XenMobile when multiple Forefront Threat Management Gateway (TMG) servers are configured in an array.

After you save the settings, open the GCS.

XenMobile NetScaler Connector can run in the following six modes:

- **Allow All**. This policy mode grants access for all traffic passing through XenMobile NetScaler Connector. No other filtering rules are used.
- **Deny All**. This policy mode blocks access for all traffic passing through XenMobile NetScaler Connector. 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. XenMobile NetScaler Connector 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 XenMobile NetScaler Connector.
- **Static + ZDM Rule**s: Block Mode. This policy mode executes static rules first, followed by dynamic rules from XenMobile 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 Rule**s: Permit Mode. This policy mode executes static rules first, followed by dynamic rules from XenMobile with an implicit permit or allow statement at the end. Devices are permitted or denied based on defined filters and XenMobile rules. Any devices that do not match on defined filters and rules are allowed.

The XenMobile NetScaler Connector process permits or blocks for dynamic rules based on unique ActiveSync IDs for iOS and Windows-based mobile devices received from XenMobile. Android devices differ in their behavior based on the manufacturer and some do not readily expose a unique ActiveSync ID. To compensate, XenMobile 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 XenMobile NetScaler Connector 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.

Enter static rules with values that the ISAPI filtering of the ActiveSync connection HTTP requests reads. Static rules enable XenMobile NetScaler Connector to permit or block traffic by the following criteria:

- **User**. XenMobile NetScaler Connector 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 XenMobile connected to Active Directory via LDAP. The **Log** tab within the XenMobile NetScaler Connector configuration utility shows the values that are passed through XenMobile NetScaler 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 XenMobile console. This value can also be screened from the Log tab in the XenMobile NetScaler Connector configuration utility.
- **DeviceType**. XenMobile NetScaler Connector 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 XenMobile NetScaler 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 XenMobile NetScaler Connector 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.

Device policies and properties in Device Manager define dynamic rules and can trigger a dynamic XenMobile NetScaler Connector filter. The triggers are based on the presence of a policy violation or property setting. The XenMobile NetScaler Connector 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 XenMobile NetScaler Connector.

Note: These dynamic rules must be configured in the XenMobile console.
1. In the XenMobile 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 XenMobile sends Android device information to the Secure Mobile Gateway. When this option is enabled, XenMobile sends Android device information to the XenMobile NetScaler Connector when XenMobile does not have the ActiveSync identifier for the Android device user.

You can view the basic policies in the default configuration on the **Policies** tab of the XenMobile NetScaler Connector configuration utility. If you want to create custom policies, you can edit the XenMobile NetScaler Connector 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.

The XenMobile NetScaler Connector uses an XML configuration file to dictate the actions of XenMobile NetScaler 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\.

The GroupRef nodes define the logical group names - by default, the AllowGroup and the DenyGroup.

Note: The order of the GroupRef nodes as they appear in the GroupRefList node is significant.
The ID value of a GroupRef node identifies a logical container or collection of members that are used for matching specific user accounts or devices. The action attributes 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.

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.

Note: In this release, only external XML files are supported.
The default installation implements two XML file in the configuration - allow.xml and deny.xml.

You can configure XenMobile NetScaler Connector 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. XenMobile NetScaler Connector connects the groups on a periodic basis. XenMobile can export groups of allowed and blocked devices and users to XenMobile NetScaler Connector.

Dynamic groups are maintained by an external source called a Gateway Configuration Provider and collected by XenMobile NetScaler Connector on a periodic basis. XenMobile can export groups of allowed and blocked devices and users to XenMobile NetScaler 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.

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 XenMobile NetScaler Connector with XenMobile 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.

You can use XenMobile NetScaler Connector 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.

By using the XenMobile NetScaler Connector 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.

1. Run XncInstaller.exe with an administrator account.
2. Follow the onscreen instructions to complete the uninstallation.

1. Run XncInstaller.exe with an administrator account to install XenMobile NetScaler Connector (XNC) or allow for upgrade or removal of an existing XenMobile NetScaler Connector.
2. Follow the onscreen instructions to complete the installation, upgrade, or uninstallation.

After you install XenMobile NetScaler Connector, you must manually restart the XenMobile configuration service and the notification service.

You can install XenMobile NetScaler Connector on its own server or on the same server where you installed XenMobile.

You can consider installing XenMobile NetScaler Connector on its own server (separate from XenMobile) for the following reasons:

- If your XenMobile Server is hosted remotely in the cloud (physical location).
- If you do not want XenMobile NetScaler Connector to be affected by restarts of the XenMobile Server (availability).
- If you want a server's system resources to be devoted entirely to XenMobile NetScaler Connector (performance).

The CPU load that XenMobile NetScaler Connector puts on a server depends on how many devices are managed. A general rule of thumb is to provision for one more CPU core if XenMobile NetScaler Connector is deployed on the same server as XenMobile. 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 XenMobile NetScaler Connector is not significant enough to warrant more memory.

XenMobile NetScaler Connector communicates with NetScaler over an SSL bridge configured on the NetScaler appliance. The bridge enables the appliance to bridge all secure traffic directly to XenMobile. XenMobile NetScaler Connector requires the following minimum system configuration:

Component	**Requirement**
Computer and processor	733 MHz Pentium III 733 MHz or higher processor. 2.0 GHz Pentium III or higher processor (recommended)
NetScaler	NetScaler appliance with software version 10
Memory	1 GB
Hard disk	NTFS-formatted local partition with 150 MB of available hard-disk space
Operating system	Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 SP2, Microsoft Windows Server 2012 R2
Other devices	Network adapter compatible with the host operating system for communication with the internal network
Display	VGA or higher-resolution monitor

The host computer for XenMobile NetScaler Connector 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 XenMobile NetScaler Connector, see Supported Device Platforms in XenMobile.

Device email clients

Not all email clients consistently return the same ActiveSync ID for a device. Because XenMobile NetScaler Connect 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
- TouchDown

XenMobile NetScaler Connector enables you to use NetScaler to proxy and load balance XenMobile server communication with XenMobile managed devices. XenMobile NetScaler Connector communicates periodically with XenMobile to synchronize policies. XenMobile NetScaler Connector and XenMobile can be clustered, together or independently, and can be load-balanced by NetScaler.

- **XenMobile NetScaler Connector 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.
- **XenMobile configuration service**. This service communicates with Device Manager to synchronize Device Manager policy changes with XenMobile NetScaler Connector.
- **XenMobile notification service**. This service sends notifications of unauthorized device access to Device Manager. In this way, Device Manager can take appropriate measures, such as notifying the user why the device was blocked.
- **XenMobile NetScaler configuration utility**. This application allows the administrator to configure and monitor XenMobile NetScaler Connector.

For XenMobile NetScaler Connector to receive requests from NetScaler to authorize ActiveSync traffic, do the following. Specify the port on which XenMobile NetScaler Connector listens to NetScaler web service calls.

1. From the **Start** menu, select the XenMobile NetScaler configuration utility.
2. Click the **Web Service** tab and then type the listening addresses for the XenMobile NetScaler Connector web service. You can select **HTTP** or **HTTPS** or both. If XenMobile NetScaler Connector is co-resident with XenMobile (installed on the same server), select port values that do not conflict with XenMobile.
3. After the values are configured, click **Save** and then click **Start Service** to start the web service.

To configure the access control policy you want to apply to your managed devices, do the following:

1. In the XenMobile NetScaler 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 XenMobile policies, select **Static + ZDM: Permit Mode or Static + ZDM: Block Mode**. These policies combine local (or, static) rules with the rules from XenMobile. 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**.

Specify the name and properties of the XenMobile Server (also known as a Config Provider) that you want to use with XenMobile NetScaler Connector and NetScaler.

Note: This task assumes that you have already installed and configured XenMobile.

1. In the XenMobile NetScaler Connector configuration utility, click the **Config Providers** tab and then click **Add**.
2. Enter the name and URL of the XenMobile Server you are using in this deployment. If youhave multiple XenMobile servers deployed in a multi-tenant deployment, this name must be unique for each server instance. For example, for **Name**, you could type **XMS**.

3. In **Url**, enter the Web address of the XenMobile 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 XenMobile web server.
5. In **Managing Host**, enter the server name where you installed XenMobile NetScaler Connector.
6. In **Baseline Interva**l, specify a time period for when a new refreshed dynamic ruleset is pulled from XenMobile.
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 XenMobile when a device is blocked. This option is required if you are using Secure Mobile Gateway rules in any of your Device Manager Automated Actions.
10. Once the server is configured, click **Test Connectivity** to test the connection to the XenMobile Server.
11. When connectivity has been established, click **Save**.

If you want to scale your XenMobile NetScaler Connector and XenMobile deployment, you can install instances of XenMobile NetScaler Connector on multiple Windows Servers, all pointing to the same XenMobile instance, and then you can use NetScaler to load balance the servers.

There are two modes for the XenMobile NetScaler Connector configuration:.

- In non-shared mode, each XenMobile NetScaler Connector instance communicates with a XenMobile server and keeps its own private copy of the resulting policy. For example, if you had a cluster of XenMobile servers, you could run a XenMobile NetScaler Connector instance on each XenMobile server and XenMobile NetScaler Connector would get policies from the local XenMobile instance.
- In shared mode, one XenMobile NetScaler Connector node is designated the primary node and it communicates with XenMobile. The resulting configuration is shared among the other nodes either by a Windows network share or by Windows (or third-party) replication.

The entire XenMobile NetScaler Connector configuration is in a single folder (consisting of a few XML files). The XenMobile NetScaler 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 XenMobile NetScaler Connector process.

Advanced Concepts

Dec 05, 2017

The XenMobile Advanced Concepts articles offer a deeper dive into product documentation on XenMobile. 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 XenMobile environment, also in this section, see the XenMobile Deployment Handbook.

For community support forums on XenMobile, see Citrix Discussions.

On-premises XenMobile interaction with Active Directory

XenMobile Deployment Handbook

Sending group enrollment invitations in XenMobile

Configuring an on-premises Device Health Attestation Server

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

On-premises XenMobile interaction with Active Directory

Siddartha Vuppala , Priyanka Joshi | Sep 06, 2017

This article explains the interaction between XenMobile Server and Active Directory. XenMobile Server interacts with Active Directory both inline and in the background. The following sections provide more information on the inline and the background operations that involve Active Directory interaction.

> ## Note
>
> This article is an overview of the interaction and does not cover the granular details. For more information about configuring Active Directory and LDAP in the XenMobile console, see Domain or domain plus security token authentication.

XenMobile Server communicates with Active Directory by using the LDAP settings that an administrator configures. The settings retrieve information about users and groups. Following are the operations that result in interaction between XenMobile Server and Active Directory.

1. **LDAP configuration.** Configuration of Active Directory itself results in an interaction with Active Directory. XenMobile Server attempts to validate the information by authenticating the information with Active Directory. The server does so by using the internet protocol, port, and service account credentials provided. A successful bind indicates that the connection is configured correctly.

2. **Group-based interactions.**

   a. Search for one or more groups during the Role-Based Access Control (RBAC) and delivery group definition creation. The XenMobile Server administrator inputs a search text string in the XenMobile console. XenMobile Server searches the selected domain for all groups that contain the substring that is provided. Then, XenMobile Server retrieves the objectGUID, sAMAccountName, and Distinguished Name attributes of the groups identified in the search.

   > ## Note
   >
   > This information is not stored in the XenMobile Server database.

   b. RBAC and deployment group definition add or update. The XenMobile Server administrator selects the Active Directory groups of interest based on the previous search and includes them in the deployment group definition. XenMobile Server searches for the specific group, one at a time, in Active Directory. XenMobile Server searches for the objectGUID attribute and retrieves selected attributes, including membership information. Group membership information helps determine membership between the group retrieved and existing users or groups in the XenMobile Server database. Changes to group membership result in the RBAC and deployment group derivation for the affected user members, which results in user entitlements.

> ### Note
>
> Changes to the deployment group definition can lead to change in app or policy entitlements for affected users.

c. **One-time PIN (OTP) invitations**. The XenMobile Server administrator selects a group from the list of Active Directory groups present in the XenMobile Server database. For this group, all the users, both direct and indirect, are retrieved from Active Directory. OTP invitations are sent to the users who were identified in the preceding step.

> ### Note
>
> The preceding three interactions imply that group-based interactions are triggered based on XenMobile Server configuration changes. When there are no changes to the configuration, the interactions imply that there are no interactions with Active Directory. They also imply that there are no requirement for background jobs to capture the group side of changes on a periodic basis.

3. **User-based interaction.**

a. User authentication. User authentication workflow results in two interactions with Active Directory:

- Used to authenticate the user with the credentials provided.
- Add or update select user attributes to the XenMobile Server database, including objectGUID, Distinguished Name, sAMAccountName, and direct membership to groups. Changes to group membership result in the re-evaluation of the app, policy, and access entitlements.

The user can authenticate either from the device or from the XenMobile Server console. In both the scenarios, interaction with Active Directory adheres to the same behavior.

b. App Store access and refresh. A refresh of the store results in a refresh of user attributes, including direct group memberships. This action allows for a re-evaluation of user entitlements.

c. Device check-ins. Administrators can configure in the XenMobile console the device check-ins on a periodic basis. Every time a device is checked-in, the corresponding user attributes are refreshed, including direct group memberships. These check-ins allow for a re-evaluation of user entitlements.

d. OTP invitations by Group. The XenMobile Server administrator selects a group from the list of Active Directory groups present in the XenMobile Server database. User members, both direct and indirect (due to nesting), are retrieved from Active Directory and saved in XenMobile Server database. OTP invitations are sent to the user members identified in the preceding step.

e. OTP invitations by user. The administrator inputs a search text string within the XenMobile console. XenMobile Server queries Active Directory and returns user records that match the input text string. The administrator then selects the user to send the OTP invitation. XenMobile Server retrieves the user details from Active Directory and updates the same details in the database before sending out the invitation to the user.

One conclusion from inline communication with Active Directory is that group-based interactions are triggered upon select changes to the XenMobile Server configuration. When there are no changes to the configuration, it implies that there are no interactions with Active Directory for groups.

This interaction requires background jobs that periodically sync with Active Directory and update relevant changes to the interested groups.

Following are the background jobs that interact with Active Directory.

1. **Group sync job**. The purpose of this job is to query Active Directory, one group at a time, on interested groups for changes to distinguished name or sAMAccountName attributes. The search query to Active Directory uses the objectGUID of the interested group to get the current values of distinguished name and sAMAccountName attributes. Changes in distinguished name or sAMAccountName values for interested groups are updated to the database.

   > ### Note
   >
   > This job does not update user to group membership information.

2. **Nested group sync job**. This job updates changes in the nesting hierarchy of interested groups. XenMobile Server allows both direct and indirect members of an interested group to get entitlements. The direct membership of the users is updated during user-based inline interactions. Running in the background, this job tracks indirect memberships. Indirect memberships are when a user is a member of a group that is a member of an interested group.

   This job gathers the list of Active Directory groups from XenMobile Server database. These groups are a part of either the deployment group or the RBAC definition. For each group in this list, XenMobile Server gets the members of the group. Members of a group are a list of distinguished names that represent both users and groups. XenMobile Server makes another query back to Active Directory to get only the user members of the interested group. The difference between the two lists gives only the group members for the interested group. Changes in member groups are updated to the database. The same process is repeated for all the groups in the hierarchy.

   Changes to nesting results in processing the affected users for entitlement changes.

3. **Disabled user check**. This job runs only when the XenMobile administrator creates an action to check for disabled users. The job runs within the scope of a group sync job. The job queries Active Directory to check for the disabled status of interested users, one user at a time.

XenMobile Deployment

Sep 06, 2017

There's a lot to consider when you're planning a XenMobile deployment. What devices should you choose? How should you manage them? How do you ensure that your network remains secure while still being user friendly? What hardware do you need in place and how do you troubleshoot it? This handbook aims to help answer those questions and more. Throughout the following pages, you'll find use cases and recommendations on topics that cover your deployment concerns, as well as questions you may have never thought to ask.

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 a XenMobile 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.

> ## Note
>
> Some of the sections in this handbook apply to XenMobile on-premises deployments only and some to both on-premises and XenMobile Service (cloud) deployments. A note indicates which deployment applies to the content in each section.

As with any deployment, assessing your needs should be your first priority. What is your primary need for XenMobile? Do you need to manage every device in your environment or just the apps? Maybe you need to manage both. How secure do you need your XenMobile environment to be? Let's look at common use cases and questions for you to consider when planning your deployment.

- Management modes
- Device requirements
- Security and user experience
- Apps
- User communities
- Email strategy
- XenMobile integration
- Multi-site requirements

Once you finish assessing your deployment needs, you can make decisions regarding the design and configuration of your environment. Choosing the hardware for your server, setting up policies for apps and devices, and getting users enrolled are just a few of the things you'll need to plan out. This section includes use cases and recommendations for each of these scenarios and more.

Note

The following articles in this section apply to XenMobile Service and XenMobile on-premises deployments.

- Integrating with NetScaler and NetScaler Gateway
- SSO and proxy considerations for MDX apps
- Authentication
- Reference architecture for on-premises deployments
- Reference architecture for cloud deployments
- Server properties
- Device and app policies
- User enrollment options
- Tuning XenMobile operations

After your XenMobile 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 XenMobile and its components generate, as well as how to read those logs. This section also includes a number of common troubleshooting steps you can follow to reduce customer support feedback time.

- App provisioning and deprovisioning
- Dashboard-based operations
- Role-based Access Control and XenMobile support
- Systems monitoring
- Disaster recovery
- Citrix support process

Management Modes

Dec 28, 2017

For each XenMobile instance (a single server or a cluster of nodes), you can choose whether to manage devices, apps, or both. XenMobile 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 (Enterprise mode)

Note: This section applies to XenMobile Service and XenMobile on-premises deployments.

Important

If you configure MDM mode and later change to ENT mode, be sure to use the same (Active Directory) authentication. XenMobile doesn't support changing the authentication mode after user enrollment. For more information, see Upgrade from XenMobile 10 MDM Edition to Enterprise Edition.

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.

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 XenMobile configured for MAM mode, you can use MDX-enabled mobile apps to provide per-app containerization and control. The term MAM mode is also called MAM-only mode. This term distinguishes this mode from a legacy MAM mode.

By leveraging MDX policies, XenMobile 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 XenMobile Apps. This support includes secure email delivery to Citrix Secure Mail, data sharing between the secured XenMobile Apps, and secure data storage in ShareFile. For details, see XenMobile Apps.

Note: Worx Mobile Apps are renamed to XenMobile Apps as of the 10.4 release. Most of the individual XenMobile Apps are renamed as well. For details, see About XenMobile 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 is a hybrid mode, also called Enterprise Mode, which enables all feature sets available in the XenMobile Enterprise Mobility Management (EMM) solution. Configuring XenMobile with MDM+MAM mode enables both MDM and MAM features.

XenMobile 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.

You specify the management mode for XenMobile Server through the Server Mode property. You configure the setting in the XenMobile console. The mode can be MDM, MAM, or ENT (for MDM+MAM).

The XenMobile edition for which you have a license determines the management modes and other features available, as shown in the following table.

XenMobile MDM Edition	XenMobile Advanced Edition	XenMobile Enterprise Edition
MDM features	MDM features	MDM features
-	MAM features	MAM features
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail

-	Secure Web	Secure Web
QuickEdit	QuickEdit	QuickEdit
-	Secure Tasks	Secure Tasks
-	-	ShareConnect
-	-	Secure Notes
-	-	ShareFile Enterprise Edition

Device Management and MDM Enrollment

A XenMobile 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 XenMobile 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.

Note: To specify whether you require users to enroll in MDM, use the XenMobile Server property **Enrollment Required** in the XenMobile console (**Settings** > **Server Properties**). That global server property applies to all users and devices for the XenMobile instance. The property applies only when the XenMobile Server Mode is ENT.

Following is a summary of the advantages and disadvantages (along with mitigations) of requiring MDM enrollment in a XenMobile Enterprise mode deployment.

Advantages:

- Users can access MAM resources without putting their devices under MDM management. This option can increase user adoption.
- Ability to secure access to MAM resources to protect enterprise data.
- MDX policies such as **App Passcode** can control app access for each MDX app.
- Configuring NetScaler, XenMobile Server, 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.
- A second XenMobile environment with MDM enrollment required is an option. When considering this option, keep in mind the additional overhead of managing two environments and the additional resources 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.

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 XenMobile actually manages on their devices and what information administrators can access.
- You can use a second XenMobile environment, with a Server Mode of MAM (also called MAM-only mode), for devices that don't need MDM management. When considering this option, keep in mind the additional overhead of managing two environments and the additional resources required.

About MAM and Legacy MAM Modes

XenMobile 10.3.5 introduced a new MAM-only server mode. To distinguish the prior and new MAM modes, the documentation uses these terms. The new mode is called MAM-only or MA, the prior MAM mode is called legacy MAM mode.

MAM-only mode is in effect when the Server Mode property of XenMobile is MAM. Devices register in MAM mode.

Legacy MAM functionality is in effect when the Server Mode property of XenMobile is ENT and users choose to opt out of device management. In that case, devices register in MAM mode. Users who opt out of MDM management continue to receive the legacy MAM functionality.

Note: Previously, setting the Server Mode property to MAM had the same effect as setting it to ENT: Users who opted out of MDM management received the legacy MAM functionality.

The following table summarizes the Server Mode setting to use for a particular license type and desired device mode:

Your licenses are for this	You want devices to register	Set the Server Mode property to

edition	in this mode	
Enterprise/ Advanced/MDM	MDM mode	MDM
Enterprise/Advanced	MAM mode (also called MAM-only mode)	MAM
Enterprise/Advanced	MDM+MAM mode	ENT (Users who opt out of device management operate under the legacy MAM mode.)

MAM-only mode supports the following features that were previously available only for ENT. These features are not available for Windows Phone.

- **Certificate-based authentication**: MAM-only mode supports certificate-based authentication. Users will experience continued access to their apps even when their Active Directory password expires. If you use certificate-based authentication for MAM devices, you must configure your NetScaler Gateway. By default, in **XenMobile Settings** > **NetScaler Gateway**, Deliver user certificate for authentication is set to **Off**, meaning that user name and password authentication is used. Change that setting to **On** to enable certificate authentication.
- **Self Help Portal**: To enable users to perform their own app lock and app wipe. Those actions apply to all apps on the device. You can configure the App Lock and App Wipe actions in **Configure** > **Actions**.
- **All enrollment modes**: Including High Security, Invitation URL, and Two Factor, configured through **Manage** > **Enrollment Invitations**.
- **Device registration limit for Android and iOS devices**: The Server Property **Number of Devices Per User** has moved to **Configure** > **Enrollment Profiles** and now applies to all server modes.
- **MAM-only APIs**: For MAM-only devices, you can call REST services by using any REST client and the XenMobile REST API to call services that the XenMobile console exposes.
- The MAM-only APIs enable you to:
  - Send an invitation URL and one-time PIN.
  - Issue app lock and wipe on devices.

The following table summarizes the differences between the legacy MAM and MAM-only functionality.

Enrollment Scenarios and Other Features	Legacy MAM (server mode is ENT)	MAM-only mode (server mode is MAM)
Certificate authentication	Not supported.	Supported. For certificate authentication, NetScaler Gateway is required.
Deployment requirement	XenMobile Server does not need to be directly accessible from devices.	XenMobile Server does not need to be directly accessible from devices.
Enrollment option	Use the NetScaler Gateway FQDN or, when using MDM	Use XenMobile Server FQDN.

	FQDN, opt not to enroll.	
Enrollment methods*	User name + Password	User name + Password, High Security, Invitation URL, Invitation URL+PIN, Invitation URL + Password, Two Factor, User name + PIN
App lock and wipe	Supported.	Supported.
Self Help Portal options for app lock and wipe	Not supported.	Supported.
App wipe behavior	Apps remain on the device but are not usable. XenMobile deletes the account on the client only.	Apps remain on the device but are not usable. XenMobile deletes the account on the client only.
Automated actions for MAM-only users.	Event, device property, user property actions are supported. Doesn't support installed app-based automated actions.	Supports event, device property, user property, and some app-based actions, including app wipe and app lock.
Built-in action when an Active Directory user is deleted	Supports app wipe.	Supports app wipe.
Enrollment limit	Supported; configured through an enrollment profile.	Supported; configured through an enrollment profile.
Software inventory	Supported. XenMobile lists apps installed on a device	Not supported.

***Regarding notifications**: SMTP is the only supported method for sending enrollment invitations.

Important: For MAM-only mode, previously enrolled users must re-enroll their devices. Be sure to provide users with the XenMobile Server FQDN they need for enrollment. In MAM-only mode, like the ENT mode, devices enroll using the XenMobile Server FQDN. (In the legacy MAM mode, devices enroll using the NetScaler Gateway FQDN.)

Device Requirements

Sep 06, 2017

> ## Note
>
> This section applies to XenMobile Service and XenMobile on-premises deployments.

An important point to consider for any deployment is the device you plan to roll out. On the iOS, Android, and Windows platforms, the options are numerous. For a list of devices that XenMobile 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, XenMobile 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 Device Enrollment Program (DEP) and Google Android for Work, 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

Jan 08, 2018

> ## Note
>
> This section applies to XenMobile Service and XenMobile on-premises deployments.

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 XenMobile.

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, NetScaler, 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, XenMobile 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 in the XenMobile documentation. 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 XenMobile, to assist with application delivery, software licensing, configuration, and application life cycle management. With XenMobile, 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. XenMobile provides organizations with the flexibility to deploy their solution as a MAM-only or a MDM-only environment, or to implement XenMobile as a unified XenMobile 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, XenMobile 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 Worx App 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. XenMobile 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 XenMobile. 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 Toolkit to wrap the app in order 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). XenMobile 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.

XenMobile Apps: These are Citrix-developed apps that are included with the XenMobile license. For details, see About XenMobile Apps. Citrix also offers other business-ready apps that ISVs develop by using the Worx App SDK.

HDX apps: These are Windows-hosted apps that you publish with StoreFront. If you have a Citrix XenApp and XenDesktop environment, you can integrate the apps with XenMobile to make the apps available to the enrolled users.

Depending of the type of mobile apps you plan to deploy and manage with XenMobile, 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 the Apple Volume Purchase Program (VPP). This option will require you to register for the VPP program and configure XenMobile VPP settings in the XenMobile console to distribute the apps with the VPP licenses. A variety of such use cases makes it important to assess and plan your MAM strategy prior to implementing the XenMobile 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, XenMobile 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 XenMobile 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 Worx App 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 to ensure that you create the right configurations when you install XenMobile server. 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 XenMobile 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 VPP to distribute and manage these apps via XenMobile. VPP 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.

Use Case

A healthcare organization plans to deploy XenMobile 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:

- **XenMobile Apps:** iOS and Android apps provided by Citrix.
- **Secure Mail:** Email, calendar, and contact app.
- **Secure Web:** Secure web browser that provides access to the Internet and intranet sites.
- **Secure Notes:** Secure note-taking app with email and calendar integration.
- **ShareFile:** 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 XenMobile. IT pushes security settings, configurations, and mobile apps to mobile devices via the Secure Hub client. Android and iOS devices enroll in XenMobile through Secure Hub.
- **Citrix Receiver:** Mobile app that allows users to open XenApp-hosted applications on mobile devices.
- **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 XenApp.

- **Epic Hyperspace:** Epic client application for electronic health record management.

ISV:

- **Vocera:** HIPAA compliant voice-over IP and messaging mobile app that extends the benefits of Vocera voice technology anytime, anywhere via iPhone and Android smartphones.

In-house apps:

- **HCMail:** App that helps compose encrypted messages, search address books on internal mail servers, and send the encrypted messages to the contacts using an email client.

In-house web apps:

- **PatientRounding:** Web application used to record patient health information by different departments.
- **Outlook Web Access:** Allows the access of email via a web browser.
- **SharePoint:** Used for organization-wide file and data sharing.

The following table lists the basic information required for MAM configuration.

App Name	App Type	MDX Wrapping	iOS	Android
Secure Mail	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Web	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Notes	XenMobile App	No for version 10.4.1 and later	Yes	Yes

ShareFile	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Hub	Public App	NA	Yes	Yes
Citrix Receiver	Public App	NA	Yes	Yes
GoToMeeting	Public App	NA	Yes	Yes
SalesForce1	Public App	NA	Yes	Yes
RSA SecurID	Public App	NA	Yes	Yes
Epic Haiku	Public App	NA	Yes	Yes
Epic Canto	Public App	NA	Yes	No
Epic Rover	Public App	NA	Yes	No
Epic Hyperspace	HDX App	NA	Yes	Yes
Vocera	ISV App	Yes	Yes	Yes
HCMail	In-House App	Yes	Yes	Yes
PatientRounding	Web App	NA	Yes	Yes
Outlook Web Access	Web App	NA	Yes	Yes
SharePoint	Web App	NA	Yes	Yes

The following tables list specific requirements you can consult when configuring MAM policies in XenMobile.

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Device Encryption
Secure Mail	Y	Selectively Allowed	Allowed	Not required

Secure Web	Y	Allowed	Allowed	Not required
Secure Notes	Y	Allowed	Allowed	Not required
ShareFile	Y	Allowed	Allowed	Not required
Secure Hub	Y	N/A	N/A	N/A
Citrix Receiver	Y	N/A	N/A	N/A
GoToMeeting	N	N/A	N/A	N/A
SalesForce1	N	N/A	N/A	N/A
RSA SecurID	N	N/A	N/A	N/A
Epic Haiku	Y	N/A	N/A	N/A
Epic Canto	Y	N/A	N/A	N/A
Epic Rover	Y	N/A	N/A	N/A
Epic Hyperspace	Y	N/A	N/A	N/A
Vocera	Y	Disallowed	Disallowed	Not required
HCMail	Y	Disallowed	Disallowed	Required
PatientRound-ing	Y	N/A	N/A	Required
Outlook Web Access	Y	N/A	N/A	Not required
SharePoint	Y	N/A	N/A	Not required

App Name	Proxy Filtering	Licensing	Geo-fencing	Worx App SDK	Minimum Operating System Version

Secure Mail	Required	N/A	Selectively Required	N/A	Enforced
Secure Web	Required	N/A	Not required	N/A	Enforced
Secure Notes	Required	N/A	Not required	N/A	Enforced
ShareFile	Required	N/A	Not required	N/A	Enforced
Secure Hub	Not required	VPP	Not required	N/A	Not enforced
Citrix Receiver	Not required	VPP	Not required	N/A	Not enforced
GoToMeeting	Not required	VPP	Not required	N/A	Not enforced
SalesForce1	Not required	VPP	Not required	N/A	Not enforced
RSA SecurID	Not required	VPP	Not required	N/A	Not enforced
Epic Haiku	Not required	VPP	Not required	N/A	Not enforced
Epic Canto	Not required	VPP	Not required	N/A	Not enforced
Epic Rover	Not required	VPP	Not required	N/A	Not enforced
Epic Hyperspace	Not required	N/A	Not required	N/A	Not enforced
Vocera	Required	N/A	Required	Required	Enforced
HCMail	Required	N/A	Required	Required	Enforced
PatientRound-ing	Required	N/A	Not required	N/A	Not enforced
Outlook Web Access	Required	N/A	Not required	N/A	Not enforced
SharePoint	Required	N/A	Not required	N/A	Not enforced

User Communities

Every organization consists of diverse user communities that operate in different functional roles. These user communities 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.

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 o.)
- 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 XenMobile, see Deploy resources.

Active Directory Organizational Units (OUs) and Groups

For OU = XenMobile 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

XenMobile Local Users and Groups

For Group= Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- ... Vendor 10

XenMobile Delivery Groups

- Clinical-Nurses
- Clinical-Physicians
- Clinical-Specialists
- Clinical-Outside Physicians
- Clinical-Home Health Services
- Clinical-Research Specialist
- Clinical-Education and Training
- Non-Clinical-Shared Services
- Non-Clinical-Physician Services
- Non-Clinical-Support Services

- Non-Clinical-Philanthropic Programs

Delivery Group and User Group mapping

Active Directory Groups	XenMobile Delivery Groups
XM-Nurses	Clinical-Nurses
XM-Physicians	Clinical-Physicians
XM-Specialists	Clinical-Specialists
XM-Outside Physicians	Clinical-Outside Physicians
XM-Home Health Services	Clinical-Home Health Services
XM-Research Specialist	Clinical-Research Specialist
XM-Education and Training	Clinical-Education and Training
XM-Shared Services	Non-Clinical-Shared Services
XM-Physician Services	Non-Clinical-Physician Services
XM-Support Services	Non-Clinical-Support Services
XM-Philanthropic Programs	Non-Clinical-Philanthropic Programs

Delivery Group and Resource mapping

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.

XenMobile Delivery Groups	Citrix Mobile Apps	Public Mobile Apps	HDX Mobile Apps
Clinical-Nurses	X		
Clinical-Physicians			

Clinical-Specialists			
Clinical-Outside Physicians	X		
Clinical-Home Health Services	X		
Clinical-Research Specialist	X		
Clinical-Education and Training		X	X
Non-Clinical-Shared Services		X	X
Non-Clinical-Physician Services		X	X
Non-Clinical-Support Services	X	X	X
Non-Clinical-Philanthropic Programs	X	X	X
Contractors	X	X	X

XenMobile Delivery Groups	Public App: RSA SecurID	Public App: EpicCare Haiku	HDX App: Epic Hyperspace	Passcode Policy	Device Restrictions	Automated Actions	WiFi Policy
Clinical-Nurses							X
Clinical-Physicians					X		
Clinical-Specialists							
Clinical-Outside Physicians							
Clinical-Home Health Services							
Clinical-Research Specialist							

Clinical-Education and Training		X	X				
Non-Clinical-Shared Services		X	X				
Non-Clinical-Physician Services		X	X				
Non-Clinical-Support Services		X	X				

Notes and considerations:

- XenMobile 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 XenMobile.
- XenMobile 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 XenMobile, that user cannot enroll. Likewise, if a user is a member of multiple groups, XenMobile will only categorize the user as being in the groups mapped to XenMobile.
- In order to make MDM enrollment mandatory, you must set the Enrollment Required option to True in Server Properties in the XenMobile console. For details, see Server Properties.
- You can delete a user group from a XenMobile delivery group by deleting the entry in the SQL Server database, under dbo.userlistgrps.
  Caution: Before you perform this action, create a backup of XenMobile and the database.

About Device Ownership in XenMobile

You can group users according to the owner of a users' 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 XenMobile console: in Deployment Rules and through XenMobile server properties on the Settings page. For details about deployment rules, see Configuring Deployment Rules in the XenMobile documentation. 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**, XenMobile 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 XenMobile.

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 XenMobile 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 XenMobile doesn't manage can install apps through the XenMobile 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 the XenMobile server routinely to confirm that the apps are still allowed to run.

Security Requirements

The amount of security considerations when deploying a XenMobile 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.

The following table specifies the deployment modes for each security level.

High Security	Higher Security	Highest Security
MAM and/or MDM	MDM+MAM	MDM+MAM; plus FIPS

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 XenMobile console.
- FIPS options for environments with the highest security needs, such as the federal government.

  If you enable FIPS mode, you must configure SQL Server to encrypt SQL traffic.

The following table specifies the NetScaler and NetScaler Gateway recommendations for each security level.

High Security	Higher Security	Highest Security
NetScaler is recommended. NetScaler Gateway is required for MAM and ENT; recommended for MDM	Standard NetScaler for XenMobile wizard configuration with SSL bridge if XenMobile is in the DMZ; or SSL offload if required to meet security standards when XenMobile server is in the internal network.	SSL Offload with end-to-end encryption

Notes:

- Exposing XenMobile 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 XenMobile server, but this choice poses a potential security risk.
- For high security environments, NetScaler with the default XenMobile configuration should meet or exceed security requirements.
- For MDM environments with the highest security needs, SSL termination at the NetScaler provides the ability to inspect traffic at the perimeter, while maintaining end-to-end SSL encryption.
- Options to define SSL/TLS ciphers.
- SSL FIPS NetScaler hardware is also available.
- For more information, see Integrating with NetScaler Gateway and NetScaler.

The following table specifies the NetScaler and NetScaler Gateway recommendations for each security level.

High Security	Higher Security	Highest Security
Active Directory Group membership only. All users Delivery Group disabled.	Invitation only enrollment 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 currently an option for Windows devices.)

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 MDM+MAM environments.
- 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

Nov 01, 2017

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 XenMobile, to assist with application delivery, software licensing, configuration, and application life cycle management.

With XenMobile, 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. XenMobile provides organizations with the flexibility to deploy their solution as a MAM-only or a MDM-only environment, or to implement XenMobile as a unified XenMobile 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, XenMobile 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 Worx App 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. XenMobile 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 XenMobile. 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 Toolkit to wrap the app in order 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). XenMobile 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.
- **Citrix XenMobile Apps**: These are Citrix-developed apps that are included with the XenMobile license. For details, see About XenMobile Apps. Citrix also offers other business-ready apps that ISVs develop by using the Worx App SDK.
- **HDX apps**: These are Windows-hosted apps that you publish with StoreFront. If you have a Citrix XenApp and XenDesktop environment, you can integrate the apps with XenMobile to make the apps available to the enrolled users.

Depending of the type of mobile apps you plan to deploy and manage with XenMobile, 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 the Apple Volume Purchase Program (VPP). This option will require you to register for the VPP program and configure XenMobile VPP settings in the XenMobile console to distribute the apps with the VPP licenses. A variety of such use cases makes it important to assess and plan your MAM strategy prior to implementing the XenMobile 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, Worx, 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 XenMobile 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 Worx App 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 to ensure that you create the right configurations when you install XenMobile server. 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. For details on security in XenMobile, see Security and User Experience.
- **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 XenMobile 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 VPP to distribute and manage these apps via XenMobile. VPP 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.

A healthcare organization plans to deploy XenMobile 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:

XenMobile Apps: iOS and Android apps provided by Citrix. For details, see XenMobile Apps.

Citrix Secure Hub: Client used by all mobile devices to communicate with XenMobile. IT pushes security settings, configurations, and mobile apps to mobile devices via Secure Hub. Android and iOS devices enroll in XenMobile through Secure Hub.

Citrix Receiver: Mobile app that allows users to open XenApp-hosted applications on mobile devices.

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 XenApp.

- **Epic Hyperspace:** Epic client application for electronic health record management.

ISV:

- **Vocera:** HIPAA compliant voice-over IP and messaging mobile app that extends the benefits of Vocera voice technology anytime, anywhere via iPhone and Android smartphones.

In-house apps:

- **HCMail:** App that helps compose encrypted messages, search address books on internal mail servers, and send the encrypted messages to the contacts using an email client.

In-house web apps:

- **PatientRounding:** Web application used to record patient health information by different departments.
- **Outlook Web Access:** Allows the access of email via a web browser.
- **SharePoint:** Used for organization-wide file and data sharing.

The following table lists the basic information required for MAM configuration.

App Name	App Type	MDX Wrapping	iOS	Android
Secure Mail	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Web	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Notes	XenMobile App	No for version 10.4.1 and later	Yes	Yes
ShareFile	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Hub	Public App	N/A	Yes	Yes
Citrix Receiver	Public App	N/A	Yes	Yes
GoToMeeting	Public App	N/A	Yes	Yes
SalesForce1	Public App	N/A	Yes	Yes
RSA SecurID	Public App	N/A	Yes	Yes
Epic Haiku	Public App	N/A	Yes	Yes
Epic Canto	Public App	N/A	Yes	No
Epic Rover	Public App	N/A	Yes	No
Epic Hyperspace	HDX App	N/A	Yes	Yes
Vocera	ISV App	Yes	Yes	Yes

HCMail	In-House App	Yes	Yes	Yes
PatientRounding	Web App	N/A	Yes	Yes
Outlook Web Access	Web App	N/A	Yes	Yes
SharePoint	Web App	N/A	Yes	Yes

The following table lists specific requirements you can consult configuring MAM policies in XenMobile.

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Device Encryption	Proxy Filtering	Licensing	Geo-fencing	Worx App SDK	Minimum Operating System Version
Secure Mail	Y	Selectively Allowed	Allowed	Not required	Required	N/A	Selectively Required	N/A	Enforced
Secure Web	Y	Allowed	Allowed	Not required	Required	N/A	Not required	N/A	Enforced
Secure Notes	Y	Allowed	Allowed	Not required	Required	N/A	Not required	N/A	Enforced
ShareFile	Y	Allowed	Allowed	Not required	Required	N/A	Not required	N/A	Enforced
Secure Hub	Y	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
Citrix Receiver	Y	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
GoToMeeting	N	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
SalesForce1	N	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
RSA SecurID	N	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
Epic Haiku	Y	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
Epic Canto	Y	N/A	N/A	N/A	Not	VPP	Not	N/A	Not

					required		required		enforced
Epic Rover	Y	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
Epic Hyperspace	Y	N/A	N/A	N/A	Not required	N/A	Not required	N/A	Not enforced
Vocera	Y	Disallowed	Disallowed	Not required	Required	N/A	Required	Required	Enforced
HCMail	Y	Disallowed	Disallowed	Required	Required	N/A	Required	Required	Enforced
PatientRounding	Y	N/A	N/A	Required	Required	N/A	Not required	N/A	Not enforced
Outlook Web Access	Y	N/A	N/A	Not required	Required	N/A	Not required	N/A	Not enforced
SharePoint	Y	N/A	N/A	Not required	Required	N/A	Not required	N/A	Not enforced

User Communities

Jan 08, 2018

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 XenMobile resources.

- XenMobile local users and groups

  For users who don't have an account in Active Directory, you can create the users as local XenMobile users. You can add local users to delivery groups and provision resources to them in the same manner as Active Directory users.

- XenMobile 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.

- 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.

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 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 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 XenMobile, see Deploy resources in the XenMobile product documentation.

Active Directory Organizational Units (OUs) and Groups

For OU = XenMobile 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

XenMobile Local Users and Groups

For Group= Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- ... Vendor 10

XenMobile Delivery Groups

- Clinical-Nurses
- Clinical-Physicians
- Clinical-Specialists
- Clinical-Outside Physicians
- Clinical-Home Health Services
- Clinical-Research Specialist
- Clinical-Education and Training
- Non-Clinical-Shared Services
- Non-Clinical-Physician Services
- Non-Clinical-Support Services
- Non-Clinical-Philanthropic Programs

Delivery Group and User Group mapping

Active Directory Groups	XenMobile Delivery Groups
XM-Nurses	Clinical-Nurses
XM-Physicians	Clinical-Physicians
XM-Specialists	Clinical-Specialists
XM-Outside Physicians	Clinical-Outside Physicians
XM-Home Health Services	Clinical-Home Health Services
XM-Research Specialist	Clinical-Research Specialist
XM-Education and Training	Clinical-Education and Training
XM-Shared Services	Non-Clinical-Shared Services
XM-Physician Services	Non-Clinical-Physician Services
XM-Support Services	Non-Clinical-Support Services
XM-Philanthropic Programs	Non-Clinical-Philanthropic Programs

Delivery Group and Resource Mapping of Apps

	Secure Mail	Secure Web	Secure Notes	ShareFile	Receiver	SalesForce1	RSA SecurID	EpicCare Haiku	Epic Hyperspace
Clinical-Nurses	X	X	X	X					
Clinical-Physicians									
Clinical-Specialists									
Clinical-Outside Physicians	X		X	X					
Clinical-Home Health Services	X		X	X					
Clinical-Research Specialist	X		X	X					
Clinical-Education and Training								X	X
Non-Clinical-Shared Services								X	X
Non-Clinical-Physician Services								X	X
Non-Clinical-Support Services	X		X	X				X	X

Non-Clinical-Philanthropic Programs	X		X	X				X	X
Contractors	X		X	X	X	X		X	X

Delivery Group and Resource Mapping of MDM Resources

	MDM: Passcode policy	MDM: Device Restrictions	MDM: Automated Actions	MDM: WiFi policy
Clinical-Nurses				X
Clinical-Physicians		X		
Clinical-Specialists				
Clinical-Outside Physicians				
Clinical-Home Health Services				
Clinical-Research Specialist				
Clinical-Education and Training				
Non-Clinical-Shared Services				
Non-Clinical-Physician Services				
Non-Clinical-Support Services				
Non-Clinical-Philanthropic Programs				
Contractors				X

Notes and considerations:

- XenMobile 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 XenMobile.
- XenMobile 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 XenMobile, that user cannot enroll. Likewise, if a user is a member of multiple groups, XenMobile only categorizes the user as being in the groups mapped to XenMobile.

- To make MDM enrollment mandatory, set the **Enrollment Required** option to **True** in **Server Properties** in the XenMobile console. For details, see Server Properties.
- To delete a user group from a XenMobile delivery group, delete the entry in the SQL Server database, under dbo.userlistgrps. **Caution:** Before you perform this action, create a backup of XenMobile and the database.

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 XenMobile console: in Deployment Rules and through XenMobile server properties on the **Settings** page. For details about deployment rules, see Deploy resources in the XenMobile documentation. For details about server properties, see Server Properties in this handbook.

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**, XenMobile 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 XenMobile 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 XenMobile doesn't manage can install apps through the XenMobile 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 the XenMobile server routinely to confirm that the apps are still allowed to run.

Email Strategy

Jan 22, 2018

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 XenMobile design. XenMobile 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.

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:

Topic	Secure Mail	Native (for example, iOS Mail)	Third-party mail (for example, TouchDown)
Minimum XenMobile Edition	Advanced	MDM	MDM
Configuration	Exchange account profiles configured via an MDX policy.	Exchange account profiles configured via an MDM policy. Android support is limited to: SAFE/KNOX, HTC, and Android for Work. All other clients are considered third-party clients.	Generally requires manual configuration by the user. Configuration of Exchange account profiles via an MDM policy for TouchDown only.
Security	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.	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.	Based on vendor/app feature set. Provides high security.
Integration	Allows interaction with managed (MDX) apps by default. Open web URLs with Citrix Secure Web. Save files to	Can only interact with other unmanaged (non-MDX) apps by default.	Can only interact with other unmanaged (non-MDX) apps by default.

	and attach files from ShareFile. Directly join and dial in to GoToMeeting.		
Deployment/ Licensing	You can push Secure Mail through MDM, directly from public app stores. Included with XenMobile Advanced and Enterprise licensing.	Client app included with platform operating system. No additional licensing requirements.	Can push via MDM, as an enterprise app or directly from public app stores. Associated licensing model/costs based on app vendor.
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.

This section discusses the three main scenarios and design considerations regarding the flow of mail (ActiveSync) traffic in the context of XenMobile.

Scenario 1: Exposed Exchange

Environments that support external clients commonly have Exchange ActiveSync services exposed to the internet. Mobile ActiveSync clients connect through this externally facing path through a reverse proxy (for example, NetScaler) 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 NetScaler (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 NetScaler 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 XenMobile, 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.

XenMobile 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 clients (native, such as TouchDown)
- ActiveSync filtering options with the use of XenMobile Mail Manager

As with most services exposed to the internet, you must secure the path and provide filtering for authorized access. The XenMobile solution includes two components designed specifically to provide ActiveSync filtering capabilities for native and third-party clients: XenMobile NetScaler Connector and XenMobile Mail Manager.

The use of XenMobile NetScaler Connector provides ActiveSync filtering at the perimeter, by using NetScaler 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. XenMobile NetScaler Connector acts an intermediary between NetScaler and the XenMobile Server. When a device communicates with Exchange through the ActiveSync virtual server on the NetScaler, NetScaler performs an HTTP callout to the XenMobile NetScaler Connector service. That service then checks the device status with XenMobile. Based on the status of the device, XenMobile NetScaler Connector replies to NetScaler 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 XenMobile NetScaler Connector component requires a Windows Server.
- Filtering rule set: XenMobile NetScaler Connector is designed for filtering based on device state and information, rather than user information. Although you may configure static rules to filter by user ID, no options exist for filtering based on Active Directory group membership, for example. If there is a requirement for Active Directory group filtering, you can use XenMobile Mail Manager instead.
- NetScaler scalability: Given the requirement to proxy ActiveSync traffic via NetScaler: Proper sizing of the NetScaler instance is critical to support the added workload of all ActiveSync SSL connections.
- NetScaler Integrated Caching: The XenMobile NetScaler Connector configuration on the NetScaler uses the Integrated Caching function to cache responses from XenMobile NetScaler Connector. As a result of that configuration, NetScaler doesn't need to issue a request to XenMobile NetScaler Connector for every ActiveSync transaction in a given session. That configuration is also critical for adequate performance and scale. Integrated Caching is available with the NetScaler Platinum Edition or you can license the feature separately for Enterprise Editions.
- Custom filtering policies: You might need to create custom NetScaler policies to restrict certain ActiveSync clients outside of the standard native mobile clients. This configuration requires knowledge on ActiveSync HTTP requests and NetScaler 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 NetScaler Gateway. If support for both native and third-party (with XenMobile NetScaler Connector) and Secure Mail clients is required: Citrix recommends that Secure Mail traffic does not flow via the NetScaler virtual server used for XenMobile NetScaler Connector. You can accomplish this traffic flow via DNS and keep the XenMobile NetScaler Connector policy from affecting Secure Mail clients.

For a diagram of XenMobile NetScaler Connector in a XenMobile deployment, see Reference Architecture for On-Premises Deployments.

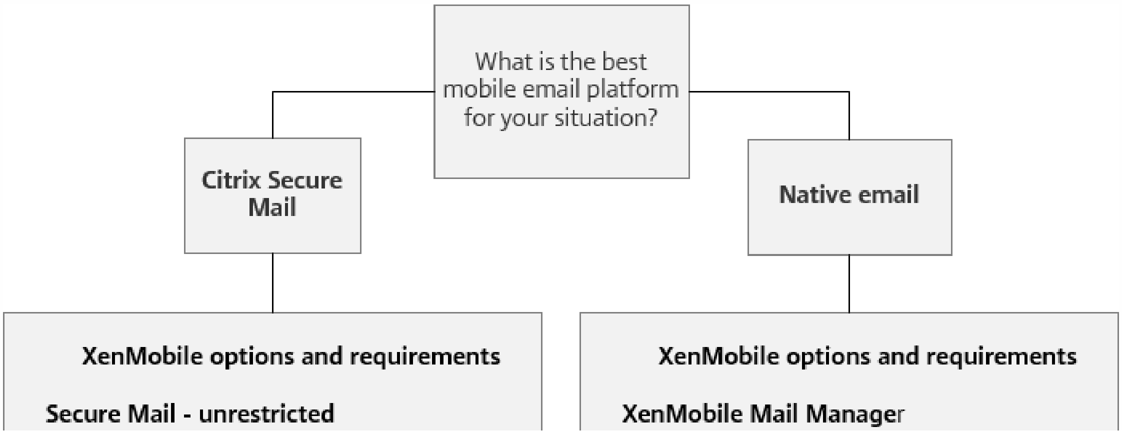
XenMobile Mail Manager is a XenMobile component that provides ActiveSync filtering at the Exchange service level. As a result, filtering only occurs once the mail reaches the exchange service, rather than when it enters the XenMobile environment. Mail Manager uses PowerShell to query Exchange ActiveSync for device partnership information and control access through device quarantine actions. Those action take devices in and out of quarantine based on XenMobile Mail Manager rule criteria. Similar to XenMobile NetScaler Connector, XenMobile Mail Manager checks the device status with XenMobile 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.

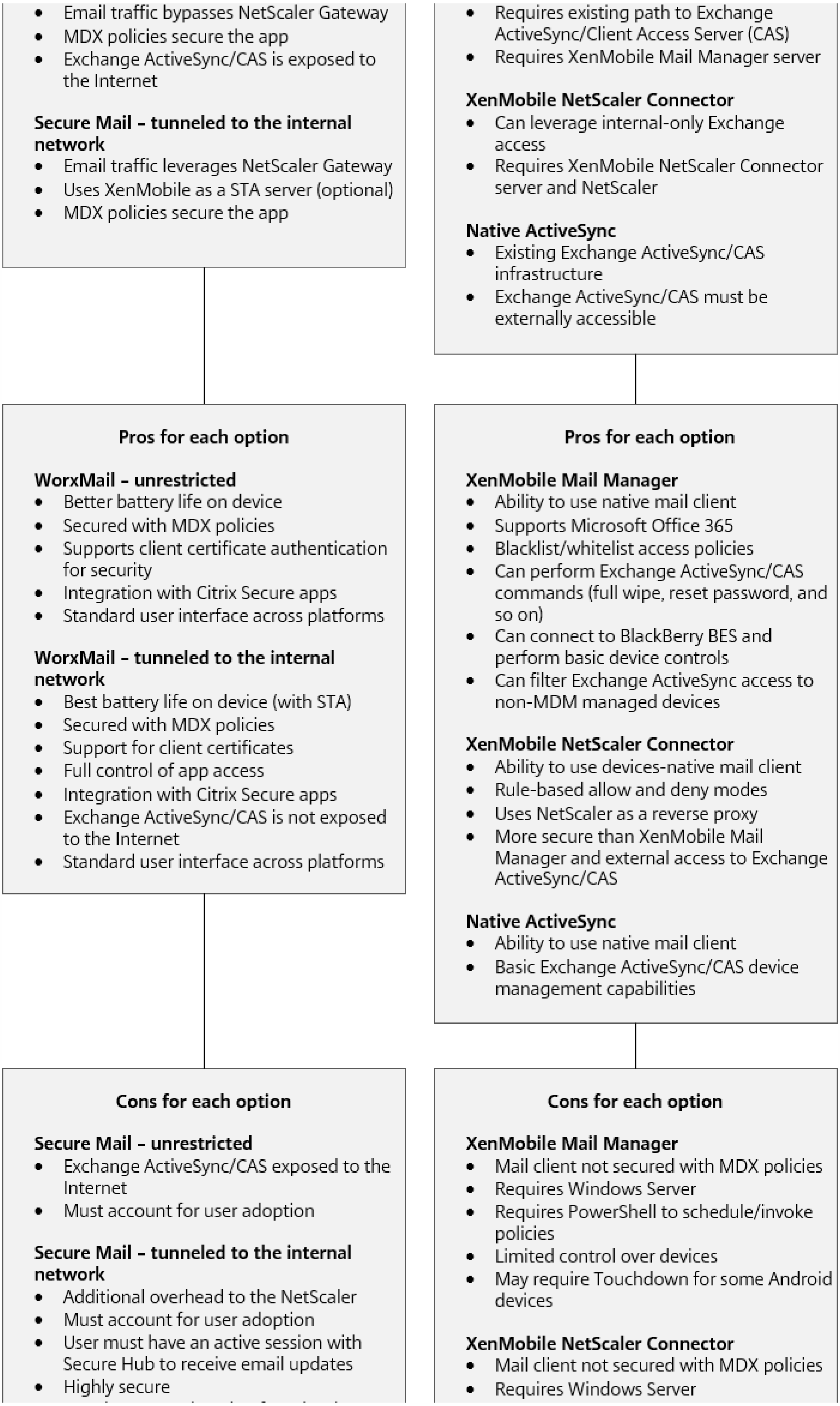
This solution does not require the use of NetScaler. You can deploy XenMobile Mail Manager without changes routing for the existing ActiveSync traffic. Design considerations include:

- Windows Server: The XenMobile Mail Manager component requires you to deploy Windows Server.
- Filtering rule set: Just like XenMobile NetScaler Connector, XenMobile Mail Manager includes filtering rules to evaluate device state. Additionally, XenMobile Mail Manager also supports static rules to filter based on Active Directory group membership.
- Exchange integration: XenMobile Mail Manager 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 XenMobile Mail Manager is filtering at the ActiveSync service level, consider other ActiveSync clients outside the XenMobile environment. You can configure XenMobile Mail Manager static rules to avoid unintended impact to other ActiveSync clients.
- Extended Exchange functions: Through direct integration with Exchange ActiveSync, XenMobile Mail Manager provides the ability for XenMobile to perform an Exchange ActiveSync wipe on a mobile device. XenMobile Mail Manager also allows XenMobile to access information about Blackberry devices and to perform other control operations.

For a diagram of XenMobile Mail Manager in a XenMobile deployment, see Reference Architecture for On-Premises Deployments.

The following figure helps you distinguish the pros and cons between using native email or Secure Mail solutions in your XenMobile deployment. Each choice allows for associated XenMobile 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
Native email
XenMobile options and requirements
Secure Mail - unrestricted
XenMobile options and requirements
XenMobile Mail Manager



- Email traffic bypasses NetScaler Gateway
- MDX policies secure the app
- Exchange ActiveSync/CAS is exposed to the Internet

Secure Mail – tunneled to the internal network

- Email traffic leverages NetScaler Gateway
- Uses XenMobile as a STA server (optional)
- MDX policies secure the app

- Requires existing path to Exchange ActiveSync/Client Access Server (CAS)
- Requires XenMobile Mail Manager server

XenMobile NetScaler Connector

- Can leverage internal-only Exchange access
- Requires XenMobile NetScaler Connector server and NetScaler

Native ActiveSync

- Existing Exchange ActiveSync/CAS infrastructure
- Exchange ActiveSync/CAS must be externally accessible

Pros for each option

WorxMail – unrestricted

- Better battery life on device
- Secured with MDX policies
- Supports client certificate authentication for security
- Integration with Citrix Secure apps
- Standard user interface across platforms

WorxMail – tunneled to the internal network

- Best battery life on device (with STA)
- Secured with MDX policies
- Support for client certificates
- Full control of app access
- Integration with Citrix Secure apps
- Exchange ActiveSync/CAS is not exposed to the Internet
- Standard user interface across platforms

Pros for each option

XenMobile Mail Manager

- 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-MDM managed devices

XenMobile NetScaler Connector

- Ability to use devices-native mail client
- Rule-based allow and deny modes
- Uses NetScaler as a reverse proxy
- More secure than XenMobile Mail Manager 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

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 NetScaler
- Must account for user adoption
- User must have an active session with Secure Hub to receive email updates
- Highly secure

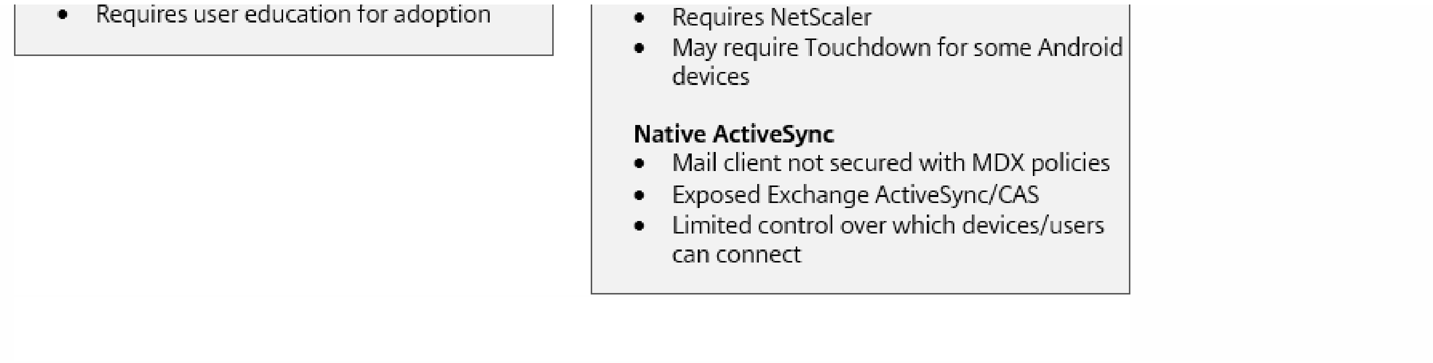
Cons for each option

XenMobile Mail Manager

- 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

XenMobile NetScaler Connector

- Mail client not secured with MDX policies
- Requires Windows Server



- Requires user education for adoption

- Requires NetScaler
- 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

XenMobile Integration

Jan 08, 2018

This article covers what to consider when planning how XenMobile is to integrate with your existing network and solutions. For example, if you're already using NetScaler for XenApp and XenDesktop:

- Should you use the existing NetScaler instance or a new, dedicated instance?
- Do you want to integrate with XenMobile the HDX apps that are published using StoreFront?
- Do you plan to use ShareFile with XenMobile?
- Do you have a Network Access Control solution that you want to integrate into XenMobile?
- Do you deploy web proxies for all outbound traffic from your network?

NetScaler Gateway required mandatory for XenMobile ENT and MAM modes. NetScaler Gateway provides a micro VPN path for access to all corporate resources and provides strong multi-factor authentication support. NetScaler load balancing is required for all XenMobile Server device modes:

- If you have multiple XenMobile Servers.
- Or, if the XenMobile Server is inside your DMZ or internal network (and therefore traffic flows from devices to NetScaler to XenMobile).

You can use existing NetScaler instances or set up new ones for XenMobile. The following sections note the advantages and disadvantages of using existing or new, dedicated NetScaler instances.

Shared NetScaler MPX with a NetScaler Gateway VIP created for XenMobile

Advantages:

- Uses a common NetScaler instance for all Citrix remote connections: XenApp, full VPN, and clientless VPN.
- Uses the existing NetScaler configurations, such as for certificate authentication and for accessing services like DNS, LDAP, and NTP.
- Uses a single NetScaler platform license.

Disadvantages:

- It is more difficult to plan for scale when you handle two very different use cases on the same NetScaler.
- Sometimes you need a specific NetScaler version for a XenApp use case. That same version might have known issues for XenMobile. Or XenMobile might have known issues for the NetScaler version.
- If a NetScaler Gateway exists, you cannot run the NetScaler for XenMobile wizard a second time to create the NetScaler configuration for XenMobile.
- Except when Platinum licenses are used for NetScaler Gateway 11.1 or later: User access licenses installed on NetScaler and required for VPN connectivity are pooled. Because those licenses are available to all NetScaler virtual servers, services other than XenMobile can potentially consume them.

Dedicated NetScaler VPX/MPX instance

Advantages:

Citrix recommends using a dedicated instance of NetScaler.

- Easier to plan for scale and separates XenMobile traffic from a NetScaler instance that might already be resource constrained.
- Avoids issues when XenMobile and XenApp need different NetScaler software versions. The recommendation generally is to use the latest compatible NetScaler version and build for XenMobile.
- Allows XenMobile configuration of NetScaler through the built-in NetScaler for XenMobile wizard.
- Virtual and physical separation of services.
- Except when Platinum licenses are used for NetScaler Gateway 11.1 or later: The user access licenses required for XenMobile are only available to XenMobile services on the NetScaler.

Disadvantages:

- Requires setup of extra services on NetScaler to support XenMobile configuration.
- Requires another NetScaler platform license. License each NetScaler instance for NetScaler Gateway.

For information about what to consider when integrating NetScaler and NetScaler Gateway with each XenMobile server mode, see Integrating with NetScaler and NetScaler Gateway.

If you have a Citrix XenApp and XenDesktop environment, you can integrate HDX applications with XenMobile using StoreFront. When you integrate HDX apps with XenMobile:

- The apps are available to users who are enrolled with XenMobile.
- The apps display in the XenMobile Store along with other mobile apps.
- XenMobile uses the legacy PNAgent (services) site on StoreFront.
- When Citrix Receiver is installed on a device, HDX apps start using the Receiver.

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 XenMobile.

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 XenMobile using the same NetScaler 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 Receiver and XenMobile Apps.

Integrate your existing StoreFront instance with XenMobile server

Advantages:

- Same store: No additional configuration of StoreFront is required for XenMobile, assuming that you use the same NetScaler VIP for HDX access. Suppose that you choose to use the same store and want to direct Receiver access to a new NetScaler VIP. In that case, add the appropriate NetScaler Gateway configuration to StoreFront.

- Same StoreFront server: Uses the existing StoreFront installation and configuration.

Disadvantages:

- Same store: Any reconfiguration of StoreFront to support XenApp and XenDesktop workloads may adversely affect XenMobile as well.
- Same StoreFront server: In large environments, consider the additional load from XenMobile usage of PNAgent for app enumeration and start-up.

Use a new, dedicated StoreFront instance for integration with XenMobile server

Advantages:

- New store: Any configuration changes of the StoreFront store for XenMobile should not affect existing XenApp and XenDesktop workloads.
- New StoreFront server: Server configuration changes should not affect XenApp and XenDesktop workflow. Additionally, load outside of XenMobile usage of PNAgent for app enumeration and launch should not affect scalability.

Disadvantages:

- New store: StoreFront store configuration.
- New StoreFront server: Requires new StoreFront installation and configuration.

For more information, see XenApp and XenDesktop through Citrix Secure Hub in the XenMobile documentation.

ShareFile enables users to access and sync all of their data from any device. With ShareFile, users can securely share data with people both inside and outside the organization. If you integrate ShareFile with XenMobile Advanced Edition or Enterprise Edition, XenMobile can provide ShareFile with:

- Single sign-on authentication for XenMobile App users.
- Active Directory-based user account provisioning.
- Comprehensive access control policies.

Mobile users can benefit from the full ShareFile Enterprise feature set.
Alternatively, you can configure XenMobile to integrate only with StorageZone Connectors. Through StorageZone Connectors, ShareFile provides access to:

- Ddocuments 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 XenDesktop and XenApp environments. You use the XenMobile console to configure the integration with ShareFile Enterprise or StorageZones Connectors. For more information, see ShareFile use with XenMobile.

The following sections note the questions to ask when making design decisions for ShareFile.

Integrate with ShareFile Enterprise or only StorageZone Connectors

Questions to ask:

- Do you need to store data in Citrix-managed StorageZones?
- Do you want to provide users with file sharing and sync capabilities?
- Do you want to enable users to access files on the ShareFile 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 ShareFile Enterprise.
- An integration with only StorageZone 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 ShareFile subdomain, provision users to ShareFile, or host ShareFile data. Using StorageZones Connectors with XenMobile complies with security restrictions against leaking user information outside of the corporate network.

ShareFile StorageZones Controller server location

Questions to ask:

- Do you require on-premises storage or features such as StorageZone Connectors?
- If using on-premises features of ShareFile, where will the ShareFile StorageZones Controllers sit in the network?

Design decision:

- Determine whether to locate the StorageZones Controller servers in the ShareFile cloud, in your on-premises single-tenant storage system, or in supported third-party cloud storage.
- StorageZones Controllers require some internet access to communicate with the Citrix ShareFile Control Plane. You can connect in several ways, including direct access, NAT/PAT configurations, or proxy configurations.

StorageZone Connectors

Questions to ask:

- What are the CIFS share paths?
- What are the SharePoint URLs?

Design decision:

- Determine if on-premises StorageZones Controllers are required to access those locations.
- Due to StorageZone Connector communication with internal resources such as file repositories, CIFS shares, and SharePoint: Citrix recommends that StorageZones Controllers reside in the internal network behind DMZ firewalls and fronted by NetScaler.

SAML integration with XenMobile Enterprise

Questions to ask:

- Is Active Directory authentication required for ShareFile?
- Does first time use of the ShareFile app for XenMobile 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:

XenMobile Enterprise environments may choose to use SAML as the authentication mechanism for ShareFile. The authentication options are:

- Use XenMobile server as the Identity Provider (IdP) for SAML

  This option can provide excellent user experience and automate ShareFile account creation, as well as enable mobile app SSO features.

- XenMobile server is enhanced for this process: It does not require the synchronization of Active Directory.
- Use the ShareFile 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 ShareFile 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 ShareFile SAML IdP.

Additionally, to satisfy both use cases, you can Configure and ADFS and XenMobile as a Dual IdP.

Mobile apps

Questions to ask:

- Which ShareFile mobile app do you plan to use (public, MDM, MDX)?

Design decision:

- You distribute XenMobile 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 ShareFile application may not be suitable. In an MDM-only environment, you can deliver the MDM version of the ShareFile app using XenMobile in MDM mode.
- For more information, see Apps and Citrix ShareFile for XenMobile.

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:

- ShareFile lets you manage employee permissions and device security. For information, see Employee Permissions and Managing Devices and Apps.
- Some ShareFile device security settings and MDX policies control the same features. In those cases, XenMobile policies take precedence, followed by the ShareFile device security settings. Examples: If you disable external apps in ShareFile,

but enable them in XenMobile, the external apps get disabled in ShareFile. You can configure the apps so that XenMobile doesn't require a PIN/passcode, but the ShareFile app requires a PIN/passcode.

Standard vs. Restricted StorageZones

Questions to ask:

- Do you require Restricted StorageZones?

Design decision:

- A standard StorageZone 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 StorageZone protects sensitive data: Only authenticated domain users can access the data stored in the zone.

The most likely scenario for routing XenMobile traffic through an HTTP(S)/SOCKS proxy is as follows: When the subnet that the XenMobile server resides in doesn't have outbound Internet access to the required Apple, Google, or Microsoft IP addresses. You can specify proxy server settings in XenMobile to route all Internet traffic to the proxy server. For more information, see Enable proxy servers.

The following table describes the advantages and disadvantages of the most common proxy used with XenMobile.

Option	Advantages	Disadvantages
Use an HTTP(S)/ SOCKS Proxy with XenMobile server.	In cases where policies do not permit outbound Internet connections from the XenMobile server subnet: You can configure an HTTP(S) or SOCKS proxy to provide Internet connectivity.	If the proxy server fails, APNs (iOS) or Google Cloud Messaging (Android) connectivity breaks. As a result, device notifications fail for all iOS and Android devices.
Use an HTTP(S) Proxy with Secure Web.	You can monitor HTTP/HTTPS traffic to ensure that Internet activity complies with your organization's standards.	This configuration requires all Secure Web Internet traffic to tunnel back to the corporate network before they are sent back out to the Internet. If your Internet connection constrains browsing: This configuration could affect Internet browsing performance.

Your NetScaler session profile configuration for split tunneling affects the traffic as follows.

When NetScaler Split Tunneling is **off**:

- If the MDX **Network access** policy is **Tunneled to the internal network:** All traffic is forced to use the micro VPN or clientless VPN (cVPN) tunnel back to the NetScaler Gateway.
- Configure NetScaler traffic policies/profiles for the proxy server and bind them to the NetScaler Gateway VIP.

Important: Be sure to exclude Secure Hub cVPN traffic from the proxy.

- For more information, see XenMobile Secure Hub Traffic Through Proxy Server in Secure Browse Mode.

When **NetScaler Split Tunneling** is **on**:

- When apps are configured with the MDX **Network access** policy set to **Tunneled to the internal network**: The apps first attempt to get the web resource directly. If the web resource is not publicly available, those apps then fall back to NetScaler Gateway.
- Configure NetScaler traffic policies and profiles for the proxy server. Then, bind those policies and profiles to the NetScaler Gateway VIP.

> **Important:** Be sure to exclude Secure Hub cVPN traffic from the proxy.

Your NetScaler session profile configuration for **Split DNS** (under **Client experience**) functions similarly to Split Tunneling.

With **Split DNS** enabled and set to **Both**:

- The client first attempts to resolve the FQDN locally and then falls back to NetScaler for DNS resolution during failure.

With **Split DNS** set to **Remote**:

- DNS resolution occurs only on NetScaler.

With **Split DNS** set to **Local**:

- The client attempts to resolve the FQDN locally. NetScaler isn't used for DNS resolution.

Enterprises can now manage mobile devices inside and outside of networks. Enterprise Mobility Management solutions such as XenMobile 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 XenMobile device security assessment through your NAC solution. Your NAC solution then can use the XenMobile security assessment to facilitate and handle authentication decisions. Citrix has validated NAC integration with XenMobile for Cisco Identity Services Engine (ISE) or ForeScout. Citrix doesn't guarantee integration for other NAC solutions.

Advantages of a NAC solution integration with XenMobile 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 XenMobile 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 XenMobile, see Network Access Control.

Multi-Site Requirements

Sep 06, 2017

You can architect and configure XenMobile deployments that include multiple sites for high availability and disaster recovery. This article provides an overview of the high availability and disaster recovered models used in XenMobile deployments.

- For XenMobile cluster nodes, NetScaler handles the load balancing.
- XenMobile server nodes operate in an active/active configuration.
- Additional XenMobile server nodes are added to a high availability cluster as capacity is required. One node can handle up to approximately 8,500 user devices (see Scalability and performance for additional detail).
- Citrix recommends configuring "n+1" XenMobile servers: one server for every 8,500 user devices and one extra server for redundancy.
- Citrix recommends high availability for all NetScaler instances wherever possible to allow the configurations to sync with a second NetScaler.
- The standard NetScaler high availability pair operates in an active/passive configuration.

A typical high availability XenMobile deployment typically includes:

- Two NetScaler instances (VPX or MPX). If the NetScaler SDX platform is used, high availability should also be considered.
- Two or more XenMobile servers configured with the same database settings.

You can configure XenMobile for disaster recovery across two data centers with one active data center and one passive data center. NetScaler and Global Server Load Balancing (GSLB) are used to create an active/active data path so that the user experience is that of an active/active setup.

For disaster recovery, a XenMobile deployment includes:

- Two data centers; each contains one or more NetScaler instances, XenMobile servers, and SQL Server databases.
- A GSLB server to direct traffic to the data centers. The GSLB server is configured for both the XenMobile enrollment URL and NetScaler Gateway URL handling traffic to the site.
- When you use the NetScaler for XenMobile wizard to configure NetScaler Gateway, by default, the GSLB is not enabled to resolve traffic to the XenMobile enrollment server and traffic to the NetScaler Gateway, en route to the MAM load-balancing server; as a result, additional steps are required. For more information on preparing for and implementing these steps, see Disaster Recovery.
- Clustered SQL Servers of Always On Availability Groups.
- Latency between the XenMobile servers and SQL Server must be less than 5 ms.

Note

The disaster recovery methods described in this handbook provide only automated disaster recovery for the access layer. You must manually start all XenMobile server nodes and the SQL Server database at the failover site before devices can connect the XenMobile server.

Integrating with NetScaler Gateway and NetScaler

Jan 08, 2018

When integrated with XenMobile, NetScaler Gateway provides an authentication mechanism for remote device access to the internal network for MAM devices. The integration enables XenMobile Apps to connect to corporate servers in the intranet through a micro VPN created from the apps on the mobile device to NetScaler Gateway.

NetScaler load balancing is required for all XenMobile server device modes if you have multiple XenMobile servers or if the XenMobile server is inside your DMZ or internal network (and therefore traffic flows from devices to NetScaler to XenMobile).

The integration requirements for NetScaler Gateway and NetScaler differ based on the XenMobile Server modes: MAM, MDM, and ENT.

MAM

With XenMobile Server in MAM mode:

- **NetScaler Gateway** is required. NetScaler Gateway provides a micro VPN path for access to all corporate resources and provides strong multi-factor authentication support.
- **NetScaler** is recommended for load balancing.

    Citrix recommends that you deploy XenMobile in a high availability configuration, which requires a load balancer in front of XenMobile. For details, see About MAM and Legacy MAM Modes.

MDM

With XenMobile Server in MDM mode:

- NetScaler Gateway isn't required. For MDM deployments, Citrix recommends NetScaler Gateway for mobile device VPN.
- NetScaler is recommended for security and load balancing.

    Citrix recommends that you deploy a NetScaler appliance in front of XenMobile server, for security and load balancing. For standard deployments with XenMobile server in the DMZ, Citrix recommends the NetScaler for XenMobile wizard along with XenMobile server load balancing in SSL Bridge mode. You can also consider SSL Offload for deployments where XenMobile server resides in the internal network rather than the DMZ and/or where security requires such configurations.

    While you might consider exposing XenMobile server to the Internet via NAT or existing third-party proxies or load-balancers for MDM provided that the SSL traffic terminates on XenMobile server (SSL Bridge), Citrix does not recommend that approach due to the potential security risk.

    For high security environments, NetScaler with the default XenMobile configuration should meet or exceed security requirements.

    For MDM environments with the highest security needs, SSL termination at the NetScaler provides the ability to inspect traffic at the perimeter, while maintaining end-to-end SSL encryption. For more information, see Security Requirements. NetScaler offers options to define SSL/TLS ciphers and SSL FIPS NetScaler hardware.

ENT (MAM+MDM)

With XenMobile Server in ENT mode:

- NetScaler Gateway is required. NetScaler Gateway provides a micro VPN path for access to all corporate resources and provides strong multi-factor authentication support.

  When the XenMobile server mode is ENT and a user opts out of MDM enrollment, the device operates in the legacy MAM mode. In the legacy MAM mode, devices enroll using the NetScaler Gateway FQDN. For details, see About MAM and Legacy MAM Modes.

- NetScaler is recommended for load balancing. For more information, see the NetScaler point above under "MDM."

> ## Important
>
> Be aware that for initial enrollment, the traffic from user devices authenticates on the XenMobile server whether you configure load balancing virtual servers to SSL Offload or SSL Bridge.

The following sections summarize the many design decisions to consider when planning a NetScaler Gateway integration with XenMobile.

Licensing and edition

Decision detail:

- What edition of NetScaler will you use?
- Have you applied Platform licenses to NetScaler?
- If you require MAM functionality, have you applied the NetScaler Universal Access Licenses?

Design guidance:

Ensure that you apply the proper licenses to the NetScaler Gateway. If you are using XenMobile NetScaler Connector, integrated caching might be required; therefore, you must ensure that the appropriate NetScaler Edition is in place.

The license requirements to enable NetScaler features are as follows.

- XenMobile MDM load balancing requires a NetScaler standard platform license at a minimum.
- ShareFile load balancing with StorageZones Controller requires a NetScaler standard platform license at a minimum.
- The XenMobile Enterprise edition includes the required NetScaler Gateway Universal licenses for MAM.
- Exchange load balancing requires a NetScaler Platinum platform license or a NetScaler Enterprise platform license with the addition of an Integrated Caching license.

NetScaler version for XenMobile

Decision detail:

- What version is the NetScaler running in the XenMobile environment?

- Will a separate instance be required?

Design guidance:

Citrix recommends using a dedicated instance of NetScaler for your NetScaler Gateway virtual server. Be sure that the minimum required NetScaler version and build is in use for the XenMobile environment. It is usually best to use the latest compatible NetScaler version and build for XenMobile. If upgrading NetScaler Gateway would affect your existing environments, a second dedicated instance for XenMobile might be appropriate.

If you plan to share a NetScaler instance for XenMobile and other apps that use VPN connections, be sure that you have enough VPN licenses for both. Keep in mind that XenMobile test and production environments cannot share a NetScaler instance.

Certificates

Decision detail:

- Do you require a higher degree of security for enrollments and access to the XenMobile environment?
- Is LDAP not an option?

Design guidance:

The default configuration for XenMobile is user name and password authentication. To add another layer of security for enrollment and access to XenMobile 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 XenMobile. Users then enroll using a unique PIN that XenMobile generates for them. After a user has access, XenMobile creates and deploys the certificate subsequently used to authenticate to the XenMobile environment.

XenMobile supports Certificate Revocation List (CRL) only for a third party Certificate Authority. If you have a Microsoft CA configured, XenMobile uses NetScaler to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the NetScaler 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; XenMobile 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.

Networking topology

Decision detail:

- What NetScaler topology is required?

Design guidance:

Citrix recommends using a NetScaler instance for XenMobile. However, if you don't want traffic going from the inside network out to the DMZ, you might consider setting up an additional instance of NetScaler, so that you're using one NetScaler instance for internal users and one for external users. Be aware that when users switch between the internal and external networks, DNS record caching can result in an increase in logon prompts in Secure Hub.

Note that XenMobile does not currently support NetScaler Gateway double hop.

Dedicated or shared NetScaler Gateway VIPs

Decision detail:

- Do you currently use NetScaler Gateway for XenApp and XenDesktop?
- Will XenMobile leverage the same NetScaler Gateway as XenApp and XenDesktop?
- What are the authentication requirements for both traffic flows?

Design guidance:

When your Citrix environment includes XenMobile, plus XenApp and XenDesktop, you can use the same NetScaler instance and NetScaler Gateway virtual server for both. Due to potential versioning conflicts and environment isolation, a dedicated NetScaler instance and NetScaler Gateway are recommend for each XenMobile environment. However, if a dedicated NetScaler instance is not an option, Citrix recommends using a dedicated NetScaler Gateway vServer rather than a vServer shared between XenMobile and XenApp and XenDesktop, to separate the traffic flows for Secure Hub.

If you use LDAP authentication, Receiver and Secure Hub can authenticate to the same NetScaler Gateway with no issues. If you use certificate-based authentication, XenMobile pushes a certificate in the MDX container and Secure Hub uses the certificate to authenticate with NetScaler Gateway. Receiver is separate from Secure Hub and can't use the same certificate as Secure Hub to authenticate to the same NetScaler Gateway.

You might consider this work around, which allows you to use the same FQDN for two NetScaler Gateway VIPs. You can create two NetScaler Gateway VIPs with the same IP address, but the one for Secure Hub uses the standard 443 port and the one for XenApp and XenDesktop (which deploy Receiver) uses port 444. Then, one FQDN resolves to the same IP address. For this work around, you might need to configure StoreFront to return an ICA file for port 444, instead of the default, port 443. This workaround doesn't require users to enter a port number.

NetScaler Gateway time-outs

Decision detail:

- How do you want to configure the NetScaler Gateway time-outs for XenMobile traffic?

Design guidance:

NetScaler Gateway includes the settings Session time-out and Forced time-out. For details, see Recommended Configurations in this handbook. Keep in mind that there are different time-out values for background services, NetScaler, and for accessing applications while offline.

XenMobile load balancer IP address for MAM

Decision detail:

- Are you using internal or external IP addresses for VIPs?

Design guidance:

In environments where you can use public IP addresses for NetScaler Gateway VIPs, assigning the XenMobile load balancing VIP and address in this manner will cause enrollment failures.

Ensure that the load balancing VIP uses an internal IP to avoid enrollment failures in this scenario. This virtual IP address must follow the RFC 1918 standard of private IP addresses. If you use a non-private IP address for this virtual server, NetScaler will not be able to contact the XenMobile server successfully during the authentication process. For details, see http://support.citrix.com/article/CTX200430.

MDM load balancing mechanism

Decision detail:

- How will the XenMobile servers be load balanced by NetScaler Gateway?

Design guidance:

Use SSL Bridge if XenMobile is in the DMZ. Use SSL Offload, if required to meet security standards, when XenMobile server is in the internal network.

- When you load balance XenMobile server with NetScaler VIPs in SSL Bridge mode, Internet traffic flows directly to XenMobile server, where connections terminate. SSL Bridge mode is the simplest mode to set up and troubleshoot.
- When you load balance XenMobile server with NetScaler VIPs in SSL Offload mode, Internet traffic flows directly to NetScaler, where connections terminate. NetScaler then establishes new sessions from NetScaler to XenMobile server. SSL Offload mode involves additional complexity during setup and troubleshooting.

Service port for MDM load balancing with SSL Offload

Decision detail:

- If you will use SSL Offload mode for Load Balancing, What port will the back-end service use?

Design guidance:

For SSL Offload, choose port 80 or 8443 as follows:

- Leverage port 80 back to XenMobile server, for true offloading.
- End-to-end encryption, that is, re-encryption of traffic, isn't supported. For details, see the Citrix support article, Supported Architectures Between NetScaler and XenMobile Server.

Enrollment FQDN

Decision detail:

- What will be the FQDN for enrollment and XenMobile instance/load balancing VIP?

Design guidance:

Initial configuration of the first XenMobile server in a cluster requires that you enter the XenMobile server FQDN. That FQDN must match your MDM VIP URL and your Internal MAM LB VIP URL. (An internal NetScaler address record resolves the MAM LB VIP.) For details, see "Enrollment FQDN for each deployment type" later in this article.

In addition, you must use the same certificate as the XenMobile SSL listener certificate, Internal MAM LB VIP certificate, and MDM VIP certificate (if using SSL Offload for MDM VIP).

Important: After you configure the enrollment FQDN, you cannot change it. A new enrollment FQDN will require a new SQL Server database and XenMobile server re-build.

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, NetScaler Gateway configuration is straightforward, assuming that Secure Web can 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. Because IT generally views enrolled devices (using the MDX container) as an extension of the corporate network, IT typically wants Secure Web connections to come back to NetScaler, go through a proxy server, and then go out to Internet. By default, Secure Web access tunnels to the internal network, which means that Secure Web uses a per-application VPN tunnel back to the internal network for all network access and NetScaler uses split tunnel settings.

For a discussion of Secure Web connections, see Configuring User Connections in the XenMobile Apps documentation.

Push Notifications for Secure Mail

Decision detail:

- Will you use push notifications?

Design guidance for iOS:

If your NetScaler Gateway configuration includes Secure Ticket Authority (STA) and split tunneling is off, NetScaler Gateway must allow traffic from Secure Mail to the Citrix listener service URLs specified in Push Notifications for Secure Mail for iOS.

Design guidance for Android:

As an alternative to the MDX policy, Active poll period, you can use Google Cloud Messaging (GCM) to control how and when Android devices need to connect to XenMobile. With GCM configured, any security action or deploy command triggers a push notification to Secure Hub to prompt the user to reconnect to the XenMobile 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 XenApp/XenDesktop farm.

ShareFile

Decision detail:

- Will you use ShareFile StorageZone Controllers in the environment?
- What ShareFile VIP URL will you use?

Design guidance:

If you will include ShareFile StorageZone Controllers in your environment, ensure that you correctly configure the following: ShareFile Content Switch VIP (used by the ShareFile Control Plane to communicate with the StorageZone Controller servers), ShareFile Load Balancing VIPs, and all required policies and profiles. For information, see Configure NetScaler for StorageZones Controller in the Citrix StorageZones documentation.

SAML IdP

Decision detail:

- If SAML is required for ShareFile, do you want to use XenMobile as the SAML IdP?

Design guidance:

The recommended best practice is to integrate ShareFile with XenMobile Advanced Edition or XenMobile Enterprise Edition, a simpler alternative to configuring SAML-based federation. When you use ShareFile with those XenMobile editions, XenMobile provides ShareFile with single sign-on (SSO) authentication of XenMobile Apps users, user account provisioning based on Active Directory, and comprehensive access control policies. The XenMobile console enables you to perform ShareFile configuration and to monitor service levels and license usage.

Note that there are two types of ShareFile clients: ShareFile Worx clients (also referred to as wrapped ShareFile) and ShareFile mobile clients (also referred to as unwrapped ShareFile). To understand the differences, see How ShareFile Worx Clients Differ from ShareFile Mobile Clients.

You can configure XenMobile and ShareFile to use SAML to provide SSO access to ShareFile mobile apps you wrap with the MDX toolkit, as well as to non-wrapped ShareFile clients, such as the web site, Outlook plugin, or sync clients.

If you want to use XenMobile as the SAML IdP for ShareFile, ensure that the proper configurations are in place. For details, see SAML for SSO with ShareFile.

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, XenMobile uses NetScaler Gateway to provide secure access to resources outside of the local network. For configuration details, see ShareConnect.

Enrollment FQDN for each deployment type

Deployment type	Enrollment FQDN
Enterprise (MDM+MAM) with mandatory MDM enrollment	XenMobile server FQDN

Enterprise (MDM+MAM) with optional MDM enrollment	XenMobile server FQDN or NetScaler Gateway FQDN
MDM only	XenMobile server FQDN
MAM-only (legacy)	NetScaler Gateway FQDN
MAM-only (for XenMobile 10.3.5 and higher)	XenMobile server FQDN

The XenMobile product documentation includes a Flowchart for Deploying XenMobile with NetScaler Gateway along with links to related articles, such as system requirements, gathering required information, configuring XenMobile for NetScaler Gateway, and using the NetScaler for XenMobile wizard to configure XenMobile connections.

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 XenMobile instances, such as for test, development, and production environments, you must configure NetScaler for the additional environments manually. When you have a working environment, take note of the settings before attempting to configure NetScaler manually for XenMobile.

The key decision you make when using the wizard is whether to use HTTPS or HTTP for communication to the XenMobile server. HTTPS provides secure back-end communication, as traffic between NetScaler and XenMobile is encrypted; the re-encryption impacts XenMobile server performance. HTTP provides better XenMobile server performance; traffic between NetScaler and XenMobile is not encrypted. The following tables show the HTTP and HTTPS port requirements for NetScaler and XenMobile server.

HTTPS

Citrix typically recommends SSL Bridge for NetScaler MDM virtual server configurations. For NetScaler SSL Offload use with MDM virtual servers, XenMobile supports only port 80 as the backend service.

Deployment type	NetScaler load balancing method	SSL re-encryption	XenMobile server port
MDM	SSL Bridge	N/A	443, 8443
MAM	SSL Offload	Enabled	8443
Enterprise	MDM: SSL Bridge	N/A	443, 8443
Enterprise	MAM: SSL Offload	Enabled	8443

HTTP

Deployment type	NetScaler load balancing method	SSL re-encryption	XenMobile server port
MDM	SSL Offload	Not supported	80
MAM	SSL Offload	Enabled	8443
Enterprise	MDM: SSL Offload	Not supported	80
Enterprise	MAM: SSL Offload	Enabled	8443

For diagrams of NetScaler Gateway in XenMobile deployments, see Reference Architecture for On-Premises Deployments and Reference Architecture for Cloud Deployments.

SSO and Proxy Considerations for MDX Apps

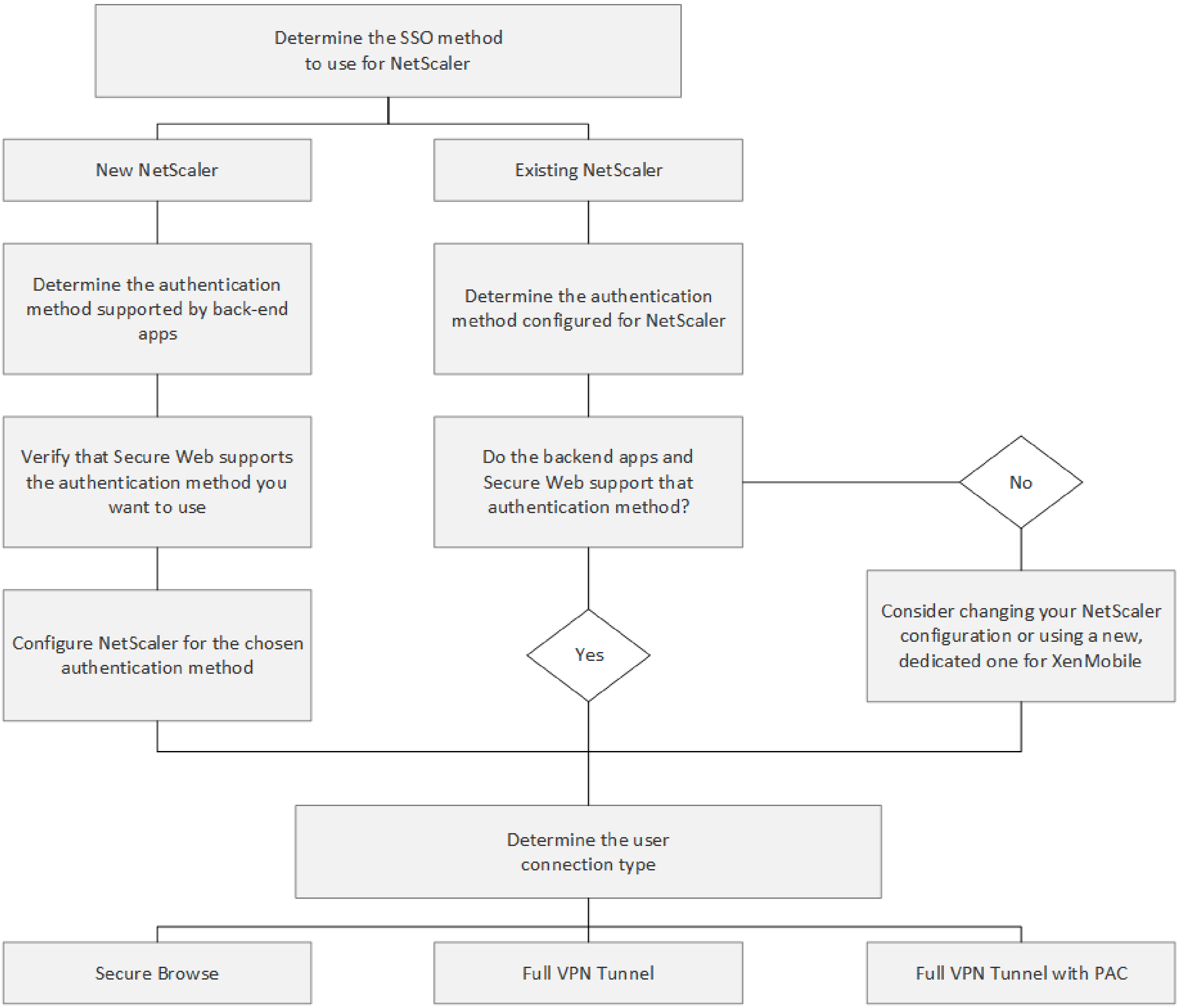
Jan 22, 2018

XenMobile integration with NetScaler 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, which is a type of clientless VPN
- Full VPN Tunnel

If NetScaler 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.


Determine the SSO method to use for NetScaler
New NetScaler
Existing NetScaler
Determine the authentication method supported by back-end apps
Determine the authentication method configured for NetScaler
Verify that Secure Web supports the authentication method you want to use
Do the backend apps and Secure Web support that authentication method?
No
Configure NetScaler for the chosen authentication method
Yes
Consider changing your NetScaler configuration or using a new, dedicated one for XenMobile
Determine the user connection type
Secure Browse
Full VPN Tunnel
Full VPN Tunnel with PAC

Secure Browse

- Recommended
- Provides SSO through NetScaler Gateway to HTTP and HTTPS sites.
- Secure Web does not prompt for credentials.

Full VPN Tunnel

- Required if end-to-end connections from Secure Web to an app server is required, such as for certificate authentication to an internal web server.
- Provides SSO through NetScaler Gateway to HTTP and HTTPS sites.
- Secure Web does not prompt for credentials.

Full VPN Tunnel with PAC

Applies only to Secure Web on iOS and Android devices.

- Provides SSO to the proxy server through NetScaler.
- Secure Web does not prompt for credentials.
- For authentication to HTTPS web sites, use the Secure Web MDX policy, **Enable web password caching**. Secure Web will prompt for credentials on first access of a website or after a password changes.

This section provides general information about the authentication methods supported by NetScaler.

SAML authentication

When you configure NetScaler for Security Assertion Markup Language (SAML), users can connect to web apps that support the SAML protocol for single sign-on. NetScaler Gateway supports the identity provider (IdP) single sign-on for SAML web apps.

Required configuration:

- Configure SAML SSO in the NetScaler Traffic profile.
- Configure the SAML iDP for the requested service.

NTLM authentication

If SSO to web apps is enabled in the session profile, NetScaler performs NTLM authentication automatically.

Required configuration:

- Enable SSO in the NetScaler Session or Traffic profile.

Kerberos impersonation

XenMobile supports Kerberos for Secure Web only. When you configure NetScaler for Kerberos SSO, NetScaler uses impersonation when a user password is available to NetScaler. Impersonation means that NetScaler uses user credentials to get the ticket required to gain access to services, such as Secure Web.

Required configuration:

- Configure the NetScaler "Worx" Session policy to allow it to identify the Kerberos Realm from your connection.
- Configure a Kerberos Constrained Delegation (KCD) account on NetScaler. Configure that account with no password and bind it to a traffic policy on your XenMobile gateway.
- For those and other configuration details, see the Citrix blog: WorxWeb and Kerberos Impersonation SSO.

Kerberos Constrained Delegation

XenMobile supports Kerberos for Secure Web only. When you configure NetScaler for Kerberos SSO, NetScaler uses constrained delegation when a user password is not available to NetScaler.

With constrained delegation, NetScaler 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 NetScaler.
- Enable SSO in the NetScaler 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 NetScaler 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 Secure Browse or Full VPN modes.

Required configuration:

- Configure Form-based SSO in the NetScaler Traffic profile.

Digest HTTP authentication

If you enable SSO to web apps in the session profile, NetScaler performs digest HTTP authentication automatically. This authentication method applies to apps that use Secure Browse or Full VPN modes.

Required configuration:

- Enable SSO in the NetScaler Session or Traffic profile.

Basic HTTP authentication

If you enable SSO to web apps in the session profile, NetScaler performs basic HTTP authentication automatically. This authentication method applies to apps that use Secure Browse or Full VPN modes.

Required configuration:

- Enable SSO in the NetScaler Session or Traffic profile.

The following sections describe the user connection types for Secure Web. For more information, see this Secure Web article in the Citrix documentation, Configuring User Connections.

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, NetScaler does not have visibility inside an HTTPS session.

Secure Browse

Connections that tunnel to the internal network can use a variation of a clientless VPN, referred to as Secure Browse. Secure Browse is the default configuration specified for the Secure Web **Preferred VPN mode** policy. Citrix recommends Secure Browse for connections that require single sign-on (SSO).

In Secure Browse mode, NetScaler breaks the HTTPS session into two parts:

- From the client to NetScaler
- From NetScaler to the back-end resource server.

In this manner, NetScaler 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 secure browse mode. For details, see the blog XenMobile 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. XenMobile supports proxy authentication provided by NetScaler. 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 NetScaler Gateway. NetScaler Gateway is unaware of the PAC file or proxy server.

For authentication to HTTPS web sites: The Secure Web MDX policy, **Enable web password caching**, enables Secure Web to authenticate and provide SSO to the proxy server through MDX.

When planning your SSO and proxy configuration, you must also decide whether to use NetScaler split tunneling. Citrix recommends that you use NetScaler split tunneling only if needed. This section provides a high-level look at how split tunneling works: NetScaler determines the traffic path based on its routing table. When NetScaler 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 NetScaler 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 NetScaler split tunneling. As a result, all traffic goes through the VPN tunnel.
- If you use Full VPN Tunnel with PAC, you must disable NetScaler Gateway split tunneling. If split tunneling is on and you configure a PAC file, the PAC file rules override the NetScaler split tunneling rules. A proxy server configured in a traffic policy does not override NetScaler 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 NetScaler split tunnel settings. The **Network access** policy default differs for some other XenMobile Apps.

NetScaler Gateway also has a micro VPN reverse split tunnel mode. This configuration supports an exclusion list of IP addresses that aren't tunneled to the NetScaler. Instead, those addresses are sent by using the device internet connection. For more information about reverse split tunneling, see Configuring Split Tunneling in the NetScaler Gateway documentation.

XenMobile includes a **Reverse split tunnel exclusion list.** To prevent certain websites from tunneling through NetScaler Gateway: Add a comma-separated list of fully qualified domain names (FQDN) or DNS suffixes that connect by using the local area network (LAN) instead. This list applies only to Secure Browse mode with NetScaler Gateway configured for reverse split tunneling.

Authentication

Sep 06, 2017

In a XenMobile 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, XenMobile client properties and NetScaler Gateway settings involved with authentication.
- The ways these policies, client properties, and settings interact.
- The tradeoffs of each choice.

This article also includes three examples of recommended configurations for increasing degrees of security.

Broadly speaking, stronger security results in a less-optimal user experience, because users have to authenticate more often. How you balance those concerns depends on your organization's needs and priorities. 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 XenMobile environment.

Online authentication: Allows users into the XenMobile 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.

Single Factor

LDAP: You can configure a connection in XenMobile 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 in the XenMobile documentation.

Client certificate: XenMobile can integrate with industry-standard certificate authorities to use certificates as the sole method of online authentication. XenMobile 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.

XenMobile supports Certificate Revocation List (CRL) only for a third-party Certificate Authority. If you have a Microsoft CA configured, XenMobile uses NetScaler to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the NetScaler 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; XenMobile 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 Reference Architecture for On-Premises Deployments.

Two Factor

LDAP + Client Certificate: In the XenMobile 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 NetScaler. 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 XenMobile 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.

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 XenMobile 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.

Note: If you select Secure offline for the Encryption keys policy, this policy is automatically enabled.

Online 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 XenMobile. When you set the Maximum offline period, if Secure Hub for iOS has a valid NetScaler Gateway token, the app retrieves new policies for MDX apps from XenMobile without any interruption to users. If Secure Hub does not have a valid NetScaler token, users must authenticate through Secure Hub in order for app policies to update. The NetScaler token may become invalid due to a NetScaler 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.

Note: Keep in mind that in a scenario in which users travel often and may use international roaming, the default of 72 hours (3 days) may be too short.

Background services ticket expiration: The time period that a background network service ticket remains valid. When Secure Mail connects through NetScaler Gateway to an Exchange Server running ActiveSync, XenMobile 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.

Online session required grace period: Determines how many minutes a user can use the app offline before the Online 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 XenMobile MDX Policies for iOS and XenMobile MDX Policies for Android.

XenMobile client properties

Note: Client properties are a global setting that apply to all devices that connect to XenMobile.

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 XenMobile console.

Following is a summary of a few important properties. For more information, see Client properties in the XenMobile documentation.

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 XenMobile 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**

NetScaler Settings

Session time-out: If you enable this setting, NetScaler Gateway disconnects the session if NetScaler detects no network activity for the specified interval. This setting is enforced for users who connect with the NetScaler Gateway Plug-in, Citrix Receiver, Secure Hub, or through a web browser. Default is **1440 minutes**. If you set this value to zero, the setting is disabled.

Forced time-out: If you enable this setting, NetScaler Gateway disconnects the session after the time-out interval elapses no matter what the user is doing. When the time-out interval elapses, there is no action the user can take to prevent the disconnection. This setting is enforced for users who connect with the NetScaler Gateway Plug-in, Citrix Receiver, Secure Hub, or through a web browser. If Secure Mail is using STA, a special NetScaler mode, the Forced time-out setting does not apply to Secure Mail sessions. Default is **1440 minutes**. If you leave this value blank, the setting is disabled.

For more information about time-out settings in NetScaler Gateway, see Configuring Time-Out Settings in the NetScaler documentation.

For more information on the scenarios that prompt users to authenticate with XenMobile by entering credentials on their devices, see Authentication Prompt Scenarios in the XenMobile Apps documentation.

Default Configuration Settings

These settings are the defaults provided by the NetScaler for XenMobile wizard, by the MDX Toolkit, and in the XenMobile console.

Setting	Where to Find the Setting	Default Setting
Session time-out	NetScaler Gateway	1440 minutes
Force time-out	NetScaler Gateway	1440 minutes
Maximum offline period	MDX Policies	72 hours
Background services ticket expiration	MDX Policies	168 hours (7 days)
Online session required	MDX Policies	Off
Online session required grace period	MDX Policies	0
App passcode	MDX Policies	On
Encrypt secrets using passcode	XenMobile client properties	false
Enable Citrix PIN Authentication	XenMobile client properties	false
PIN Strength Requirement	XenMobile client properties	Medium
PIN Type	XenMobile client properties	Numeric
Enable User Password Caching	XenMobile client properties	false
Inactivity Timer	XenMobile client properties	15
Enable Touch ID Authentication	XenMobile client properties	false

This section gives examples of three XenMobile 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.

High Security

This configuration, the most convenient to users, provides base-level security.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Session time-out	NetScaler Gateway	10080	Users enter their Secure Hub credentials only when online authentication is required - every 7 days
Force time-out	NetScaler Gateway	No value	Sessions will be extended if there's any activity.
Maximum offline period	MDX Policies	167	Requires policy refresh every week (every 7 days). The hour difference is to allow for refresh ahead of session time-out.
Background services ticket expiration	MDX Policies	240	Time out for STA, which allows for long-lived sessions without a NetScaler Gateway session token. 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.
Online session required	MDX Policies	Off	Ensures a valid network connection and NetScaler Gateway session to use apps.
Online session required grace period	MDX Policies	0	No grace period (if you enabled Online Session required).
App passcode	MDX Policies	On	Require passcode for application.
Encrypt secrets using passcode	XenMobile client properties	false	Do not require user entropy to encrypt the vault.
Enable Citrix PIN Authentication	XenMobile client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength Requirement	XenMobile client properties	Low	No password complexity requirements
PIN Type	XenMobile client properties	Numeric	PIN is a numeric sequence.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Password Caching	client properties		
Inactivity Timer	XenMobile client properties	90	If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.
Enable Touch ID Authentication	XenMobile client properties	true	Enables Touch ID for offline authentication use cases in iOS.

Higher Security

A more middle-of-the-road approach, this configuration requires users to authenticate more often - every 3 days, at most, instead of 7 - and stronger security. The increased number of authentications lock the container more often, ensuring data security when devices aren't in use.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Session time-out	NetScaler Gateway	4320	Users enter their Secure Hub credentials only when online authentication is required - every 3 days
Force time-out	NetScaler Gateway	No value	Sessions will be extended if there's any activity.
Maximum offline period	MDX Policies	71	Requires policy refresh every 3 days. The hour difference is to allow for refresh ahead of session time-out.
Background services ticket expiration	MDX Policies	168 hours	Time out for STA, which allows for long-lived sessions without a NetScaler Gateway session token. 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.
Online session required	MDX Policies	Off	Ensures a valid network connection and NetScaler Gateway session to use apps.
Online session required grace period	MDX Policies	0	No grace period (if you enabled Online Session required).
App passcode	MDX Policies	On	Require passcode for application.
Encrypt secrets using passcode	XenMobile client properties	false	Do not require user entropy to encrypt the vault.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
PIN Authentication	client properties		
PIN Strength Requirement	XenMobile client properties	Medium	Enforces medium password complexity rules.
PIN Type	XenMobile client properties	Numeric	PIN is a numeric sequence.
Enable Password Caching	XenMobile client properties	true	The user PIN caches and protects the Active Directory password.
Inactivity Timer	XenMobile client properties	30	If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.
Enable Touch ID Authentication	XenMobile client properties	true	Enables Touch ID for offline authentication use cases in iOS.

Highest Security

This configuration offers the highest level of security but contains significant usability trade-offs.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Session time-out	NetScaler Gateway	1440	Users enter their Secure Hub credentials only when online authentication is required-every 24 hours.
Force time-out	NetScaler Gateway	1440	Online authentication will be strictly required every 24 hours. Activity doesn't extend session life.
Maximum offline period	MDX Policies	23	Requires policy refresh every day.
Background services ticket expiration	MDX Policies	72 hours	Time out for STA, which allows for long-lived sessions without a NetScaler Gateway session token. 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.
Online session required	MDX Policies	Off	Ensures a valid network connection and NetScaler Gateway session to use apps.
Online session required grace	MDX	0	No grace period (if you enabled Online Session required).

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
App passcode	MDX Policies	On	Require passcode for application.
Encrypt secrets using passcode	XenMobile client properties	true	A key derived from user entropy protects the vault.
Enable Citrix PIN Authentication	XenMobile client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength Requirement	XenMobile client properties	Strong	High password complexity requirements.
PIN Type	XenMobile client properties	Alphanumeric	PIN is an alphanumeric sequence.
Enable Password Caching	XenMobile client properties	false	Active Directory password is not cached and Citrix PIN will be used for offline authentications.
Inactivity Timer	XenMobile client properties	15	If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.
Enable Touch ID Authentication	XenMobile client properties	false	Disables Touch ID for offline authentication use cases in iOS.

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 NetScaler appliances).

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Alternate NetScaler Gateway	MDX Policies	Requires the FQDN and port of the secondary NetScaler appliance.	Allows for enhanced authentication controlled by the secondary NetScaler appliance authentication and session policies.

If a user opens an app that logs on to the alternate NetScaler Gateway instance, all other apps will use that NetScaler Gateway instance for communicating with the internal network. The session will only switch back to the lower security NetScaler Gateway instance when the session times out from the NetScaler Gateway instance with enhanced security.

Using Online 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.

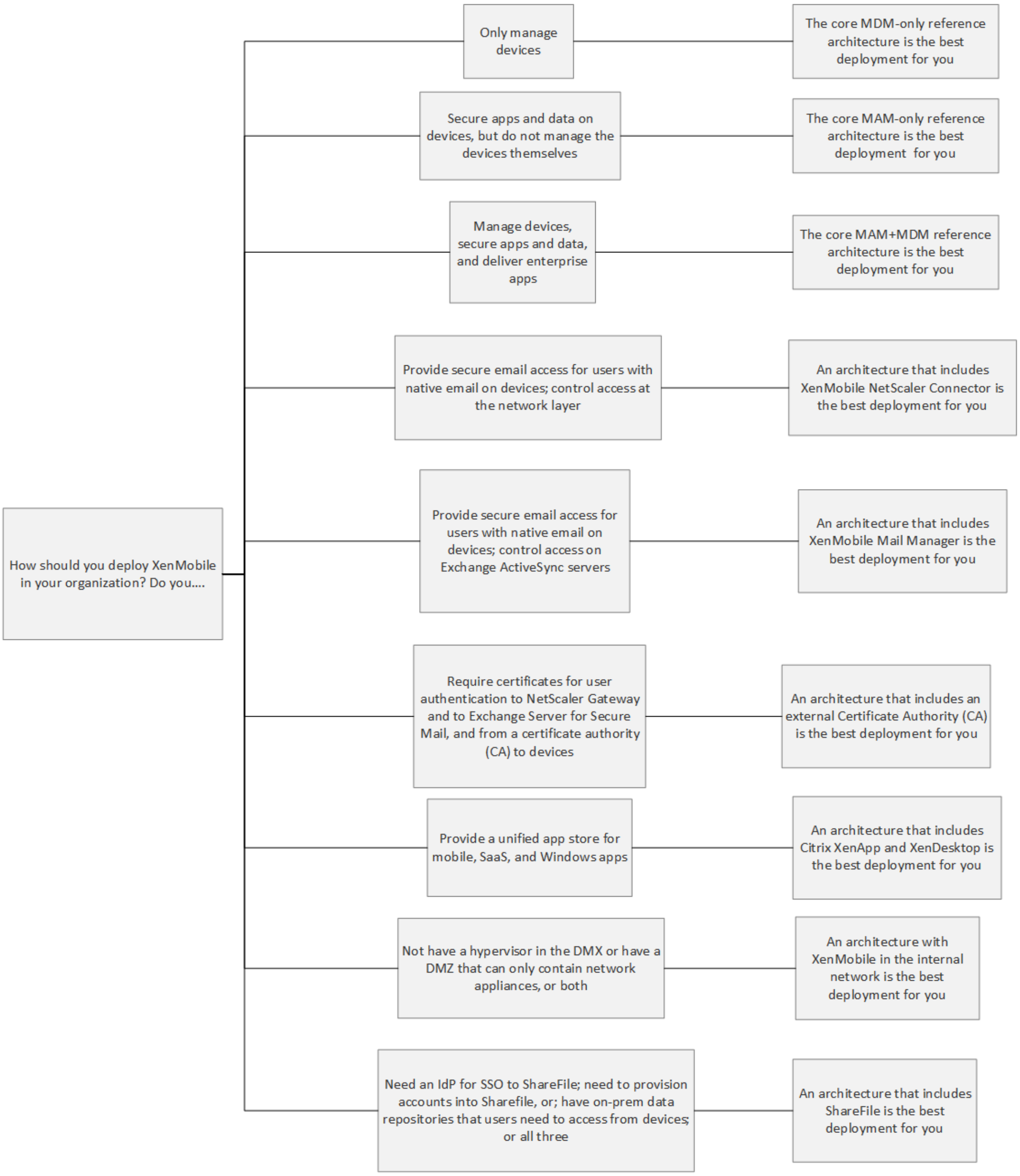
Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Online session required	MDX Policies	On	Ensures device is online and has a valid authentication token.
Online session required grace period	MDX Policies	15	Allows a 15-minute grace period before the user can no longer use apps

Reference Architecture for On-Premises Deployments

Sep 06, 2017

The figures in this article illustrate the reference architectures for the XenMobile deployment on premises. The deployment scenarios include MDM-only, MAM-only, and MDM+MAM as the core architectures, as well as those that include components, such as XenMobile NetScaler Connector, XenMobile Mail Manager, and XenApp and XenDesktop. The figures show the minimal components required for XenMobile.

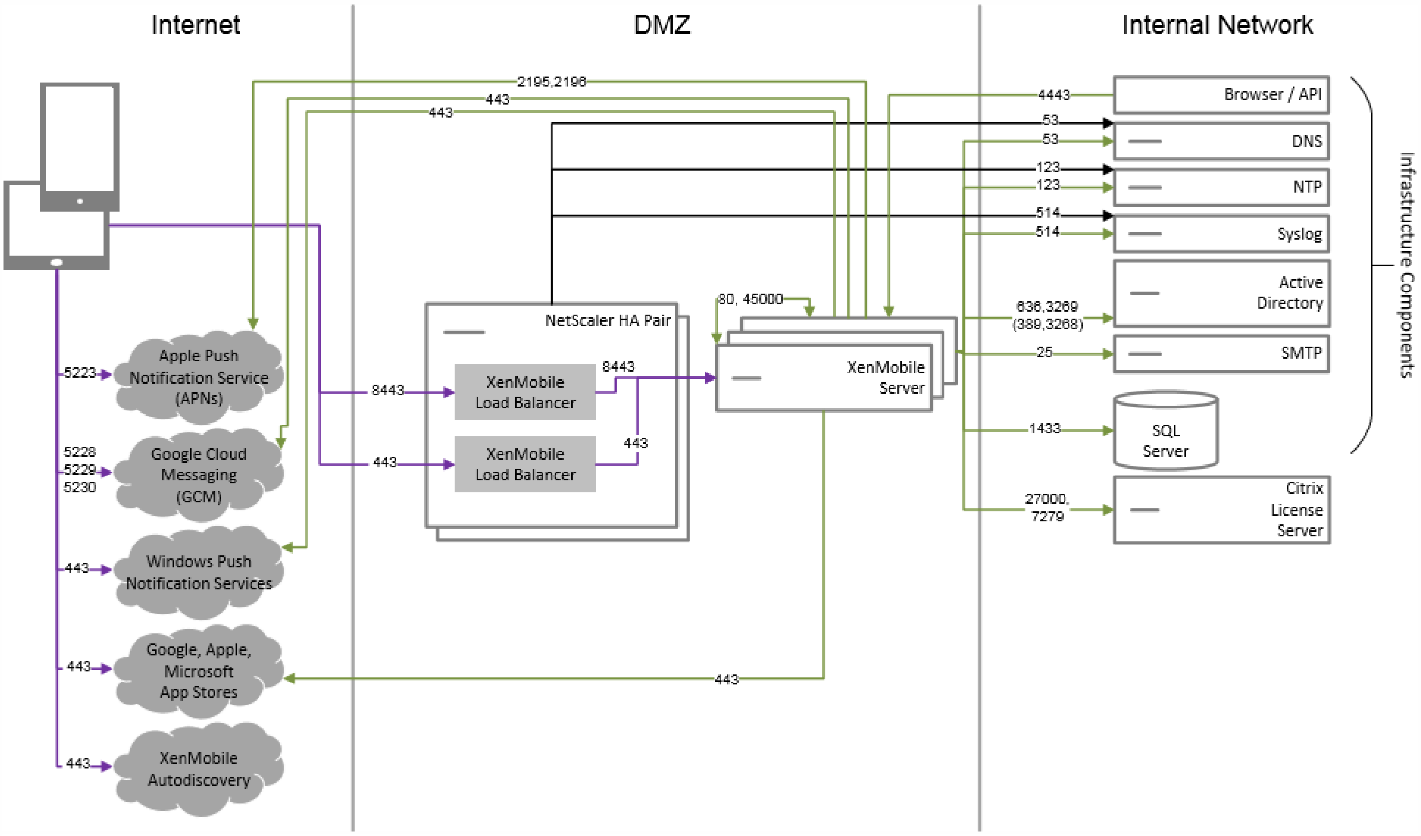
Use this chart as a general guide for your deployment decisions.


How should you deploy XenMobile in your organization? Do you....
Only manage devices
The core MDM-only reference architecture is the best deployment for you
Secure apps and data on devices, but do not manage the devices themselves
The core MAM-only reference architecture is the best deployment for you
Manage devices, secure apps and data, and deliver enterprise apps
The core MAM+MDM reference architecture is the best deployment for you
Provide secure email access for users with native email on devices; control access at the network layer
An architecture that includes XenMobile NetScaler Connector is the best deployment for you
Provide secure email access for users with native email on devices; control access on Exchange ActiveSync servers
An architecture that includes XenMobile Mail Manager is the best deployment for you
Require certificates for user authentication to NetScaler Gateway and to Exchange Server for Secure Mail, and from a certificate authority (CA) to devices
An architecture that includes an external Certificate Authority (CA) is the best deployment for you
Provide a unified app store for mobile, SaaS, and Windows apps
An architecture that includes Citrix XenApp and XenDesktop is the best deployment for you
Not have a hypervisor in the DMX or have a DMZ that can only contain network appliances, or both
An architecture with XenMobile in the internal network is the best deployment for you
Need an IdP for SSO to ShareFile; need to provision accounts into Sharefile, or; have on-prem data repositories that users need to access from devices; or all three
An architecture that includes ShareFile is the best deployment for you

In the figures, the numbers on the connectors represent ports that you must open to allow connections between the components. For a complete list of ports, see Port requirements in the XenMobile documentation.

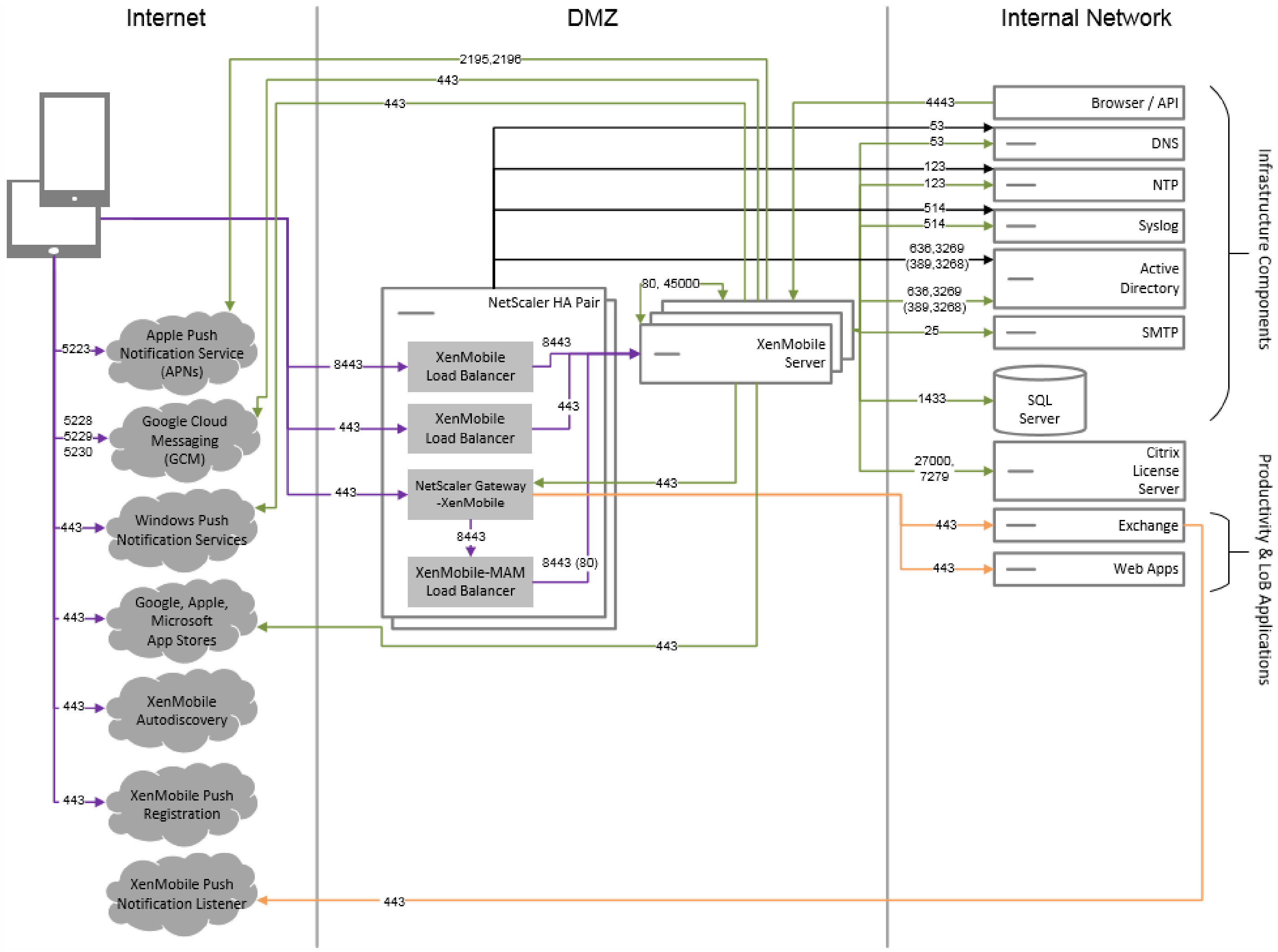
Core MDM-Only Reference Architecture

Deploy this architecture if you plan to use only the MDM features of XenMobile. For example, you need to manage a corporate-issued device through MDM in order to deploy device policies, apps and to retrieve asset inventories and be able to carry out actions on devices, such as a device wipe.



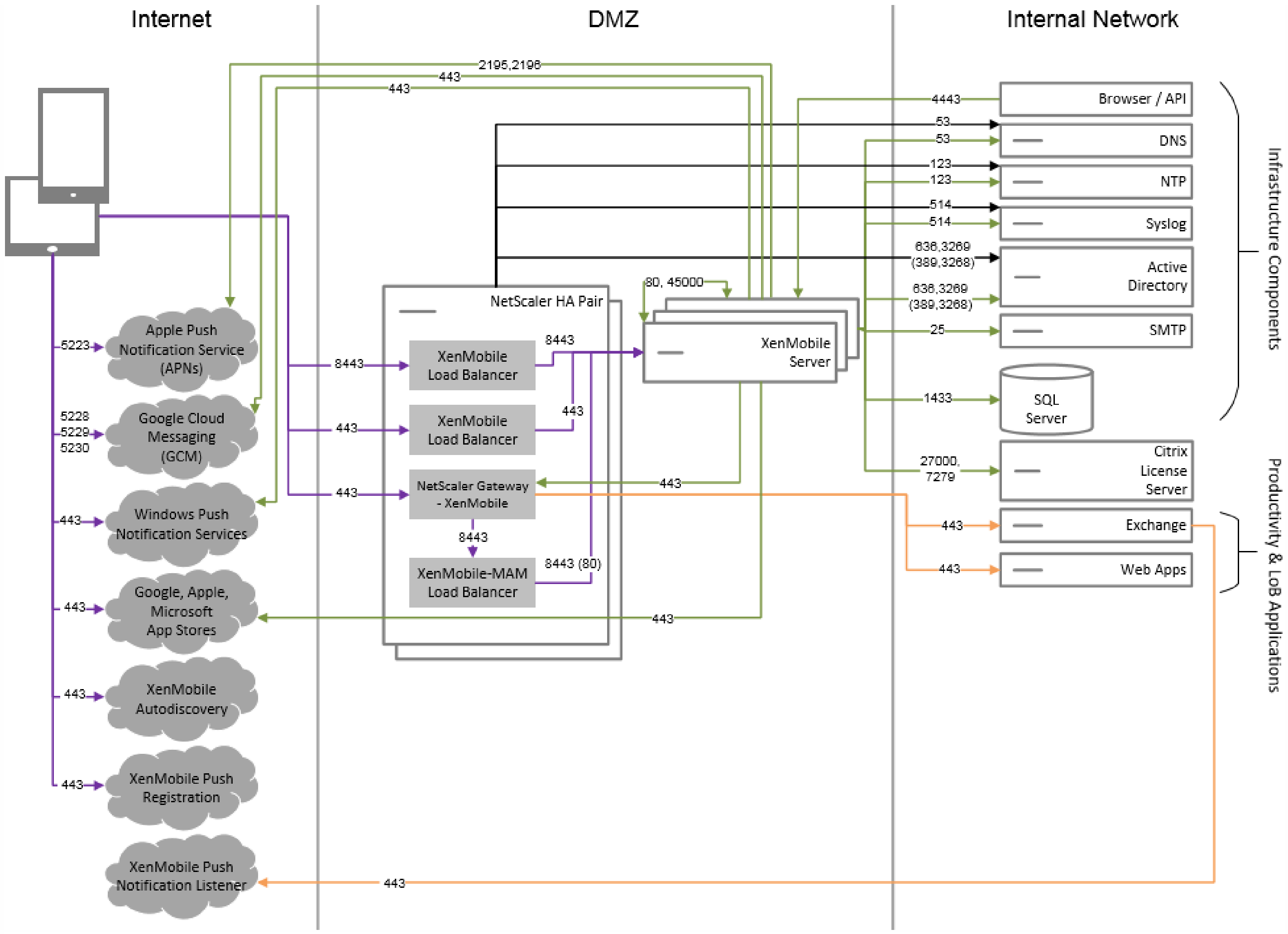
Core MAM-Only Reference Architecture

Deploy this architecture if you plan to use only the MAM features of XenMobile without having devices enroll for MDM. For example, you want to secure apps and data on BYO mobile devices; you want to deliver enterprise mobile apps and be able to lock apps and wipe their data. The devices cannot be MDM enrolled.



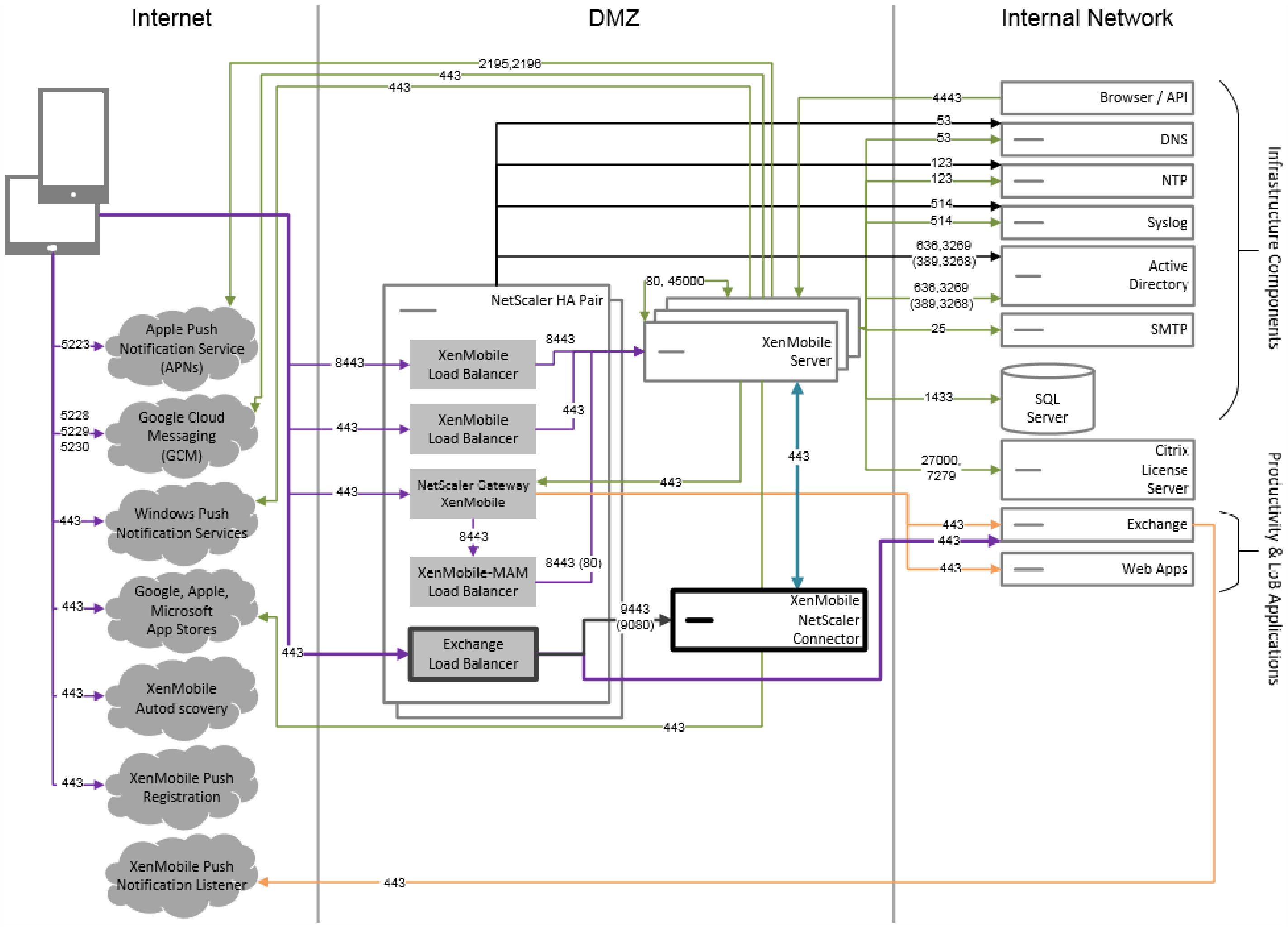
Core MAM+MDM Reference Architecture

Deploy this architecture if you plan to use MDM+MAM features of XenMobile. For example, you want to manage a corporate-issued device via MDM; you want to deploy device policies and apps, retrieve an asset inventory and be able to wipe devices. You also want to deliver enterprise mobile apps and be able to lock apps and wipe the data on devices.



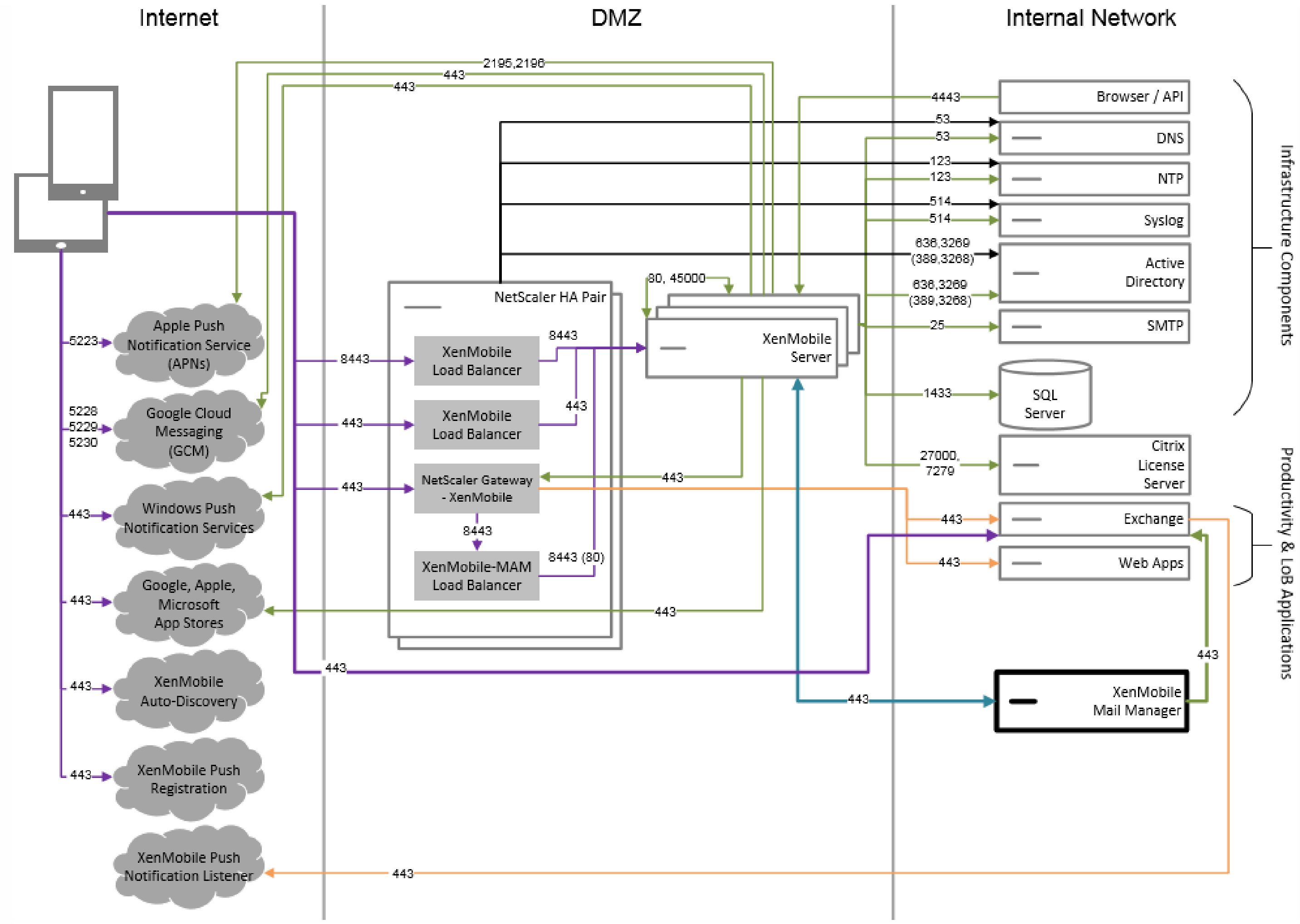
Reference Architecture with XenMobile NetScaler Connector

Deploy this architecture if you plan to use XenMobile NetScaler Connector with XenMobile. For example, you need to provide secure email access to users who use native mobile email apps. These users will continue accessing email via a native app or you may transition them over time to Citrix Secure Mail. Access control needs to occur at the network layer before traffic hits the Exchange Active Sync servers. Even though the diagram shows XenMobile NetScaler Connector deployed in a MDM and MAM architecture, you can also deploy XenMobile NetScaler Connector in the same manner as part of an MDM-only architecture.



Reference Architecture with XenMobile Mail Manager

Deploy this architecture if you plan to use XenMobile Mail Manager with XenMobile. For example, you want to provide secure email access to users who use native mobile email apps. These users will continue accessing email via a native app or you may transition users over time to Secure Mail. You can achieve access control on the Exchange ActiveSync servers. Although the diagram shows XenMobile Mail Manager deployed in a MDM and MAM architecture, you can also deploy XenMobile Mail Manager in the same manner as part of an MDM-only architecture.

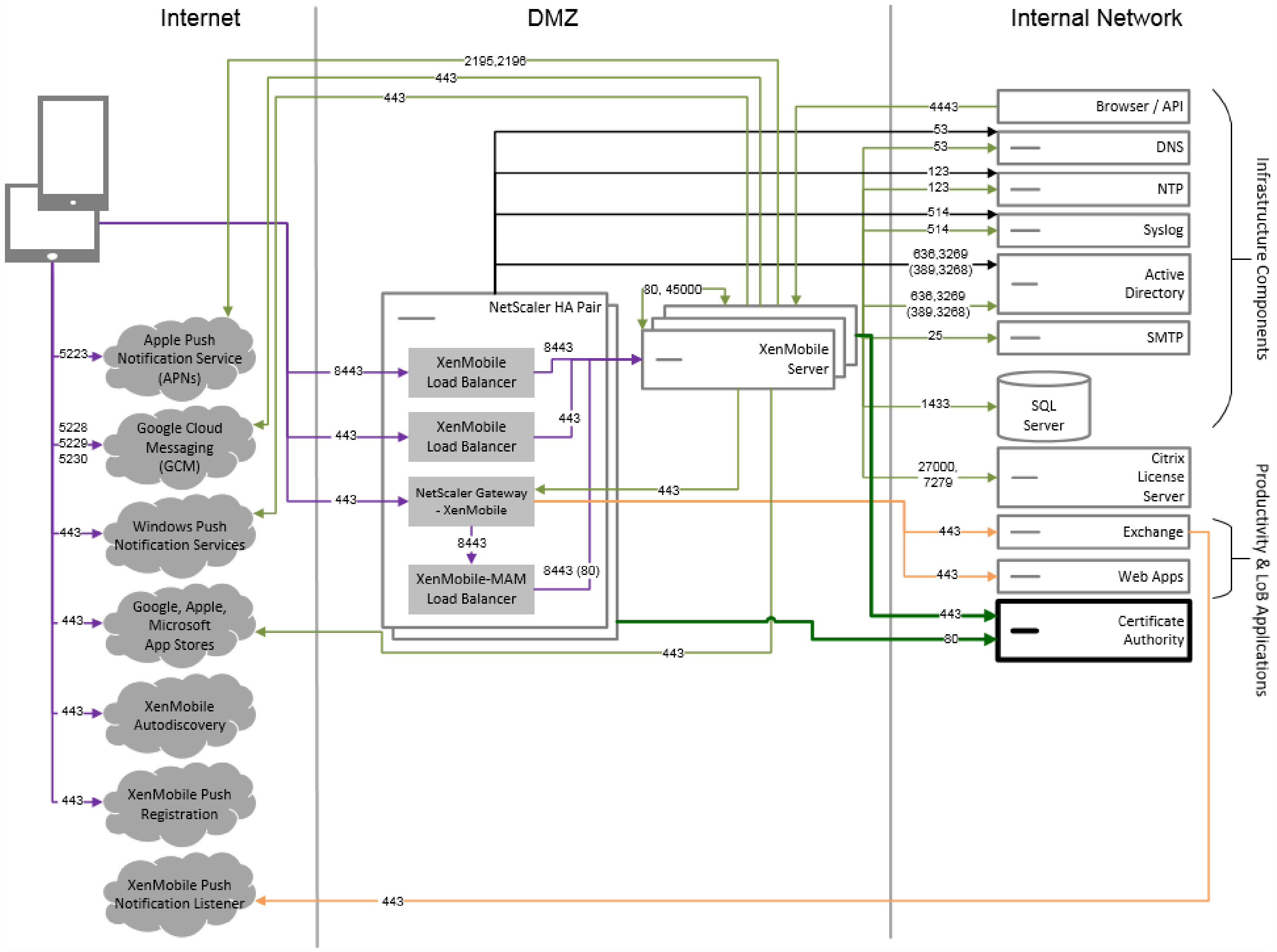


Reference Architecture with External Certificate Authority

A deployment that includes an external certificate authority is recommended to meet one or more of the following requirements:

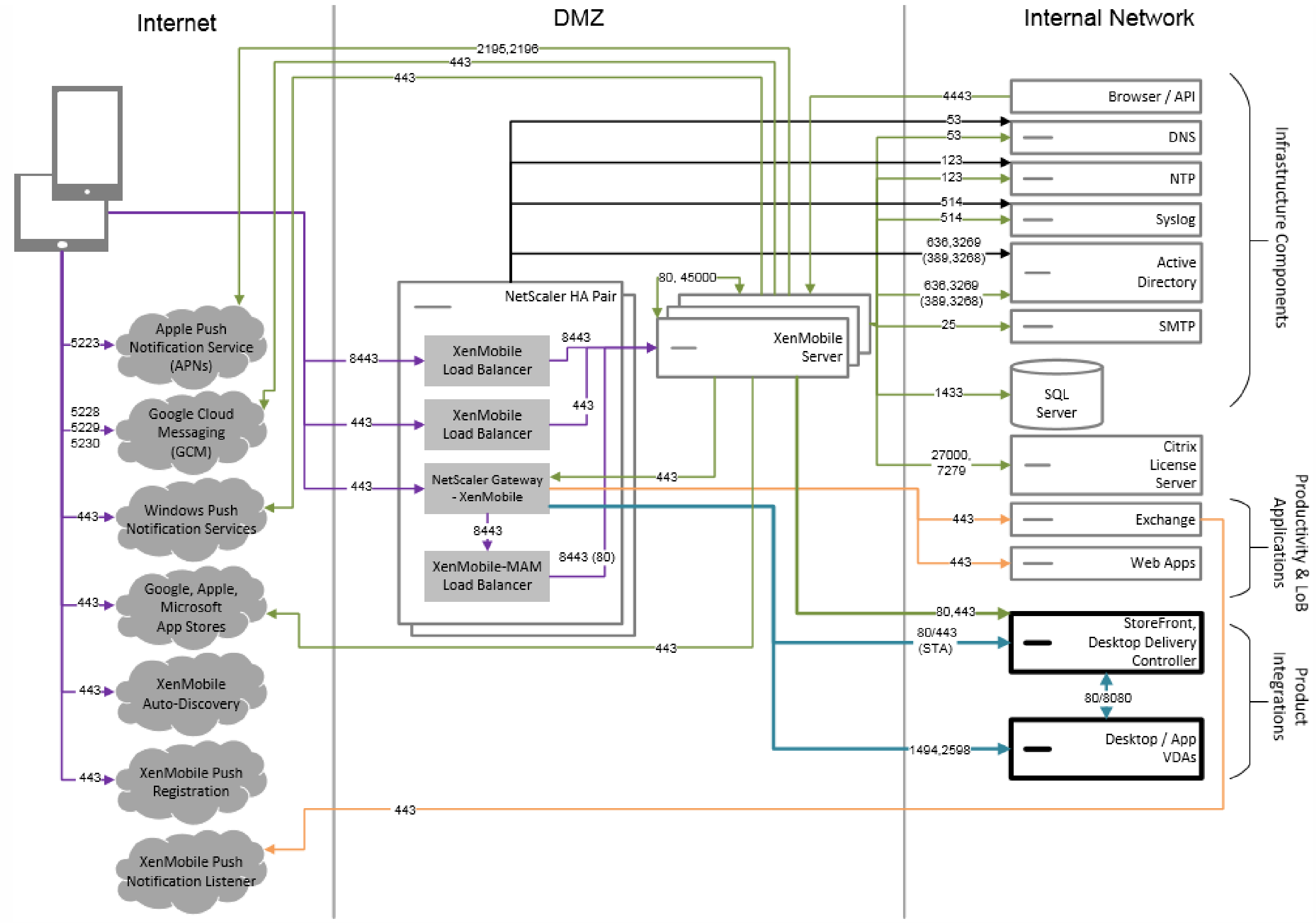
- You require user certificates for user authentication to NetScaler Gateway (for intranet access).
- You require Secure Mail users to authenticate to Exchange Server by using a user certificate.
- You need to push certificates issued by your corporate Certificate Authority to mobile devices for WiFi access, for example.

Although the diagram shows an external certificate authority deployed in an MDM+MAM architecture, you can also deploy an external Certificate Authority in the same manner as part of an MDM-only or MAM-only architecture.



Reference Architecture with XenApp and XenDesktop

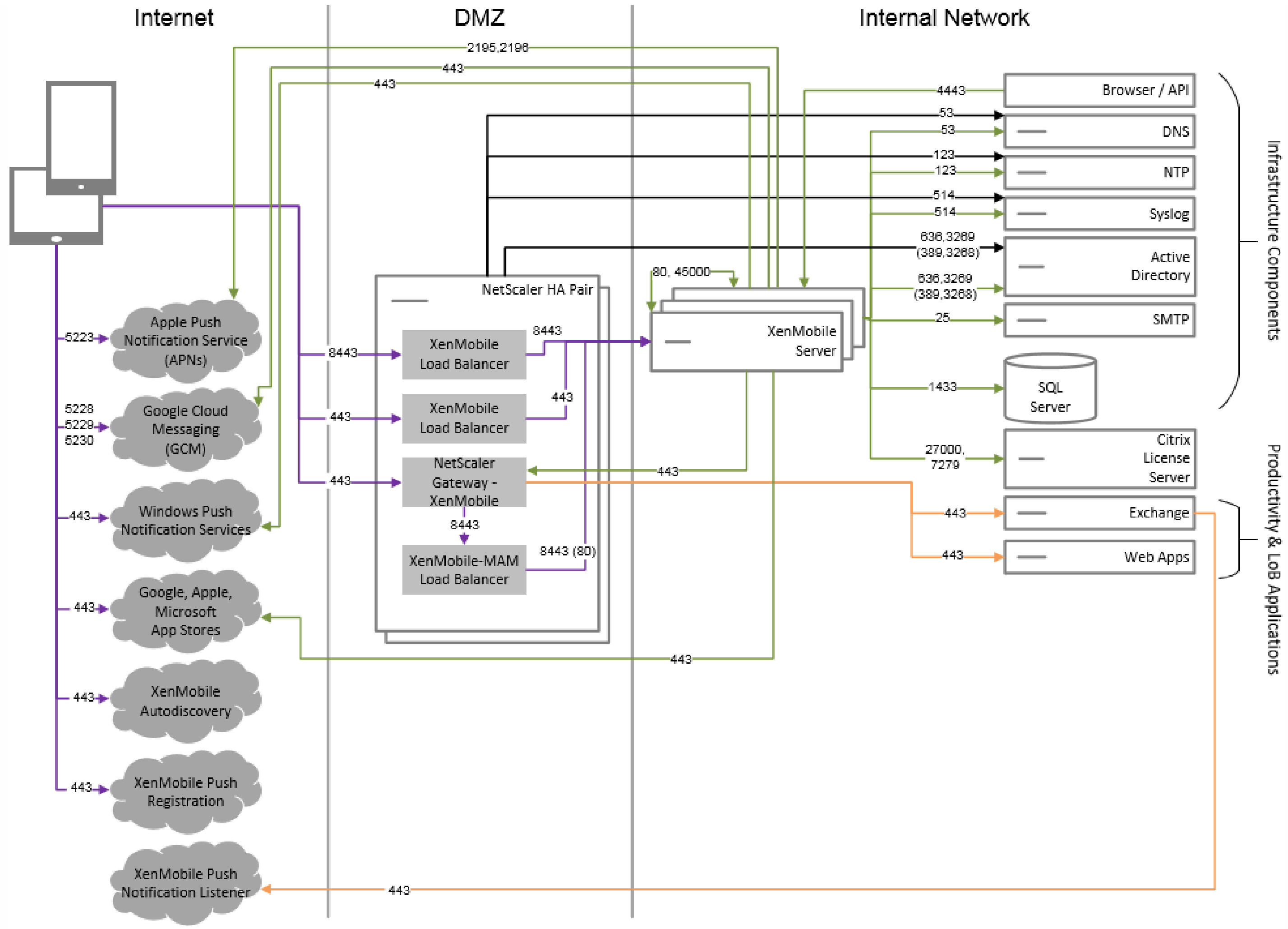
Deploy this architecture if you plan to integrate XenApp and XenDesktop with XenMobile. For example, you need to provide a unified app store to mobile users for all types of applications (mobile, SaaS and Windows). Although the diagram shows XenDesktop deployed in a MDM and MAM architecture, you can also deploy XenDesktop in the same manner as part of a MAM-only architecture.



Reference Architecture with XenMobile in the Internal Network

You can deploy an architecture with XenMobile in the internal network to meet one or more of the following requirements:

- You do not have or are not allowed to have a hypervisor in the DMZ.
- Your DMZ can only contain network appliances.
- Your security requirements require the use of SSL Offload.



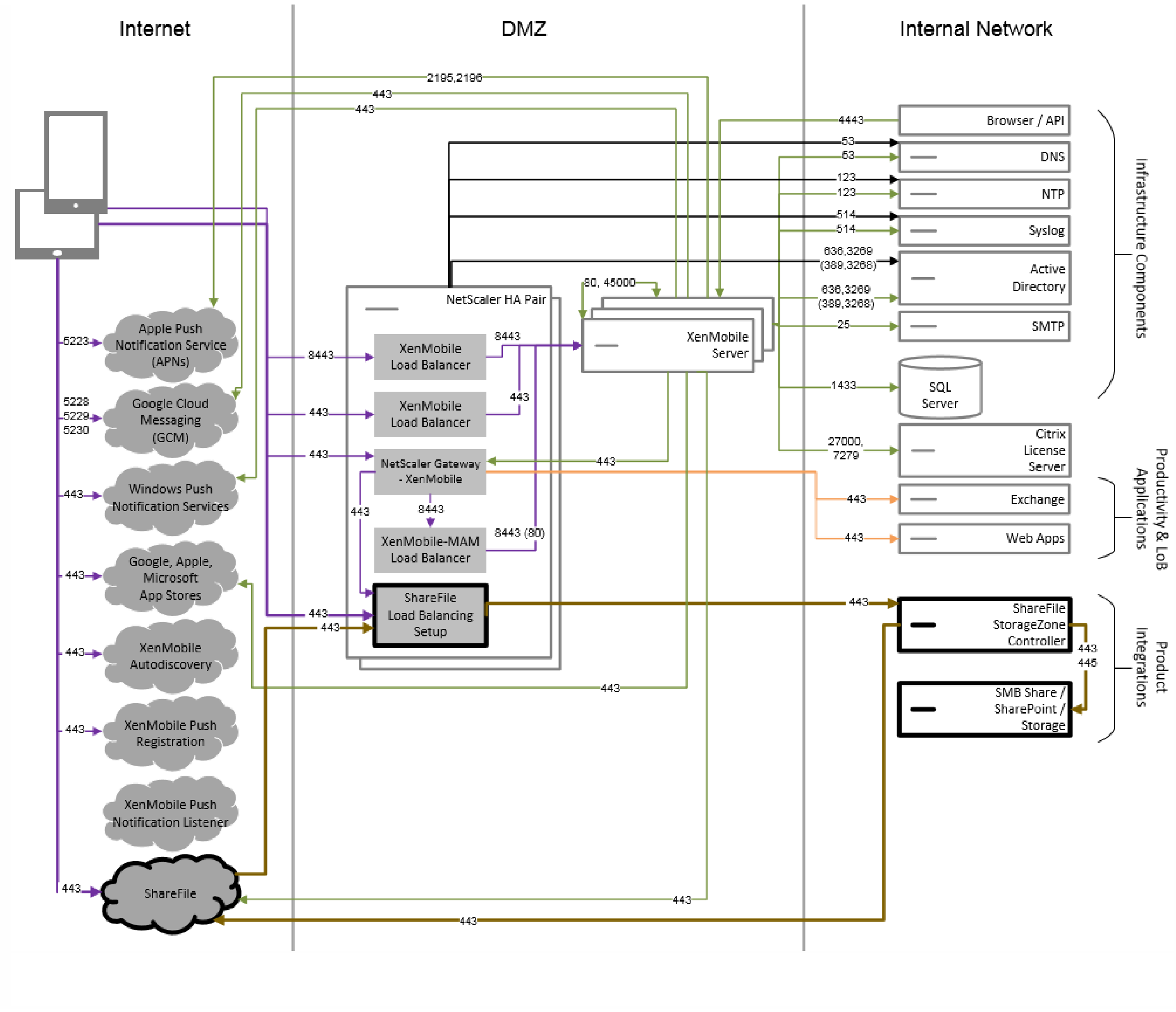
Reference Architecture with ShareFile

Deploy this architecture if you want to integrate ShareFile Enterprise or only StorageZone Connectors with XenMobile. ShareFile Enterprise integration enables you to meet one or more of the following requirements:

- You need an IDP to give users single sign-on (SSO) to ShareFile.com.
- You need a way to provision accounts into ShareFile.com.
- You have on-premises data repositories that need to be accessed from mobile devices.

An integration with only StorageZone Connectors gives users secure mobile access to existing on-premises storage repositories, such as SharePoint sites and network file shares. In this configuration, you don't need to set up a ShareFile subdomain, provision users to ShareFile, or host ShareFile data.

Although the diagram shows ShareFile deployed in a MDM+MAM architecture, you can also deploy ShareFile in the same manner as part of a MAM-only architecture.



Internet
DMZ
Internal Network
2195,2196
443
443
4443
Browser / API
53
53
DNS
123
123
NTP
514
514
Syslog
636,3269
(389,3268)
636,3269
(389,3268)
Active
Directory
25
SMTP
1433
SQL
Server
27000,
7279
Citrix
License
Server
Infrastructure Components
443
Exchange
443
Web Apps
Productivity & LoB
Applications
443
ShareFile
StorageZone
Controller
443
445
SMB Share /
SharePoint /
Storage
Product
Integrations
80, 45000
XenMobile
Server
NetScaler HA Pair
8443
XenMobile
Load Balancer
8443
443
XenMobile
Load Balancer
443
443
NetScaler Gateway
- XenMobile
443
443
8443
XenMobile-MAM
Load Balancer
8443 (80)
443
443
ShareFile
Load Balancing
Setup
443
5223
Apple Push
Notification Service
(APNs)
5228
5229
5230
Google Cloud
Messaging
(GCM)
443
Windows Push
Notification Services
443
Google, Apple,
Microsoft
App Stores
443
XenMobile
Autodiscovery
443
XenMobile Push
Registration
XenMobile Push
Notification Listener
443
ShareFile
443
443

Reference Architecture for Cloud Deployments

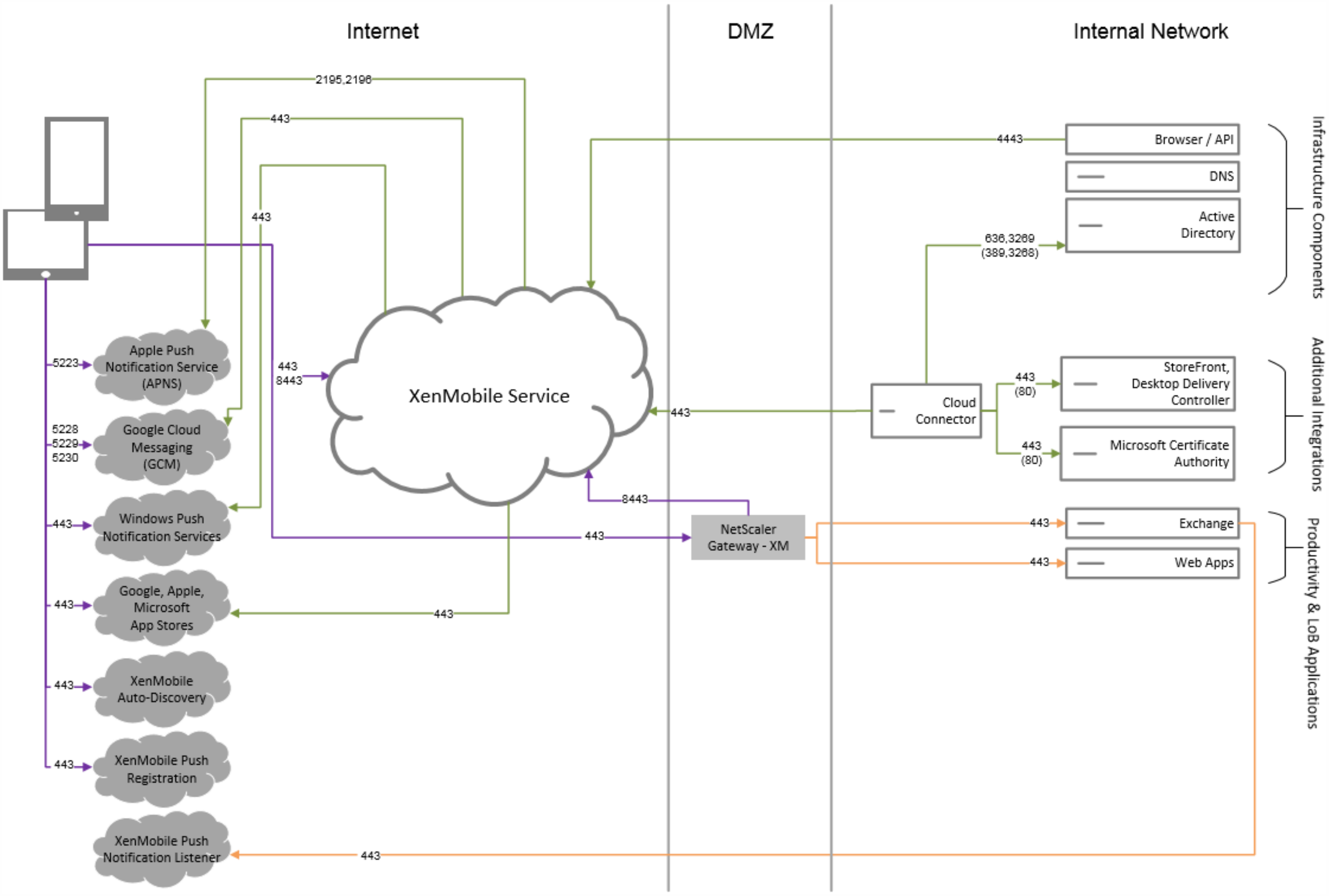
Sep 06, 2017

Note

This article applies to XenMobile Service deployments only.

The diagram in this article shows how XenMobile Service integrates with your data center. The other component integrations, such as ShareFile, Certificate Authority, and XenApp and XenDesktop, are available as shown in the preceding core architectures. For details, see Reference Architecture for On-Premises Deployments.

Use of Cloud Connector eliminates the need to set up complex networking or infrastructure configuration, such as VPNs or IPsec tunnels. If you require a micro VPN, you must use an on-premises NetScaler with Cloud Connector. The following diagram shows NetScaler Gateway hosted on your site.


Internet
DMZ
Internal Network
2195,2196
443
443
4443
Browser / API
DNS
Active Directory
636,3269 (389,3268)
Infrastructure Components
5223
Apple Push Notification Service (APNS)
443 8443
XenMobile Service
443
Cloud Connector
443 (80)
StoreFront, Desktop Delivery Controller
443 (80)
Microsoft Certificate Authority
Additional Integrations
5228 5229 5230
Google Cloud Messaging (GCM)
8443
443
Windows Push Notification Services
443
NetScaler Gateway - XM
443
Exchange
443
Web Apps
Productivity & LoB Applications
443
Google, Apple, Microsoft App Stores
443
443
XenMobile Auto-Discovery
443
XenMobile Push Registration
XenMobile Push Notification Listener
443

Server Properties

Sep 06, 2017

Server properties are global properties that apply to operations, users, and devices across an entire XenMobile 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.

Be aware that a change to some server properties requires a restart of each XenMobile server node. XenMobile notifies you when a restart is required.

Server Property	Notes
Block Enrollment of Rooted Android and Jailbroken iOS Devices	When this property is **True**, XenMobile blocks enrollments for rooted Android devices and jailbroken iOS devices. Default is **False**. Recommended setting is **True** for all security levels.
Enrollment required	This property, which applies only when the XenMobile Server Mode is ENT, specifies whether you require users to enroll in MDM. The property applies to all users and devices for the XenMobile 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. When this property is **False**, users can decline enrollment, but may still access apps on their devices through the XenMobile Store. When this property is **True**, any user who declines enrollment is denied access to apps. If you change this property after users enroll, the users must re-enroll. For a discussion about whether to require MDM enrollment, see Device Management and MDM Enrollment.
XenMobile MDM Self Help Portal console max inactive interval (minutes) **Note**: This property name reflects the older XenMobile versions. The property controls the XenMobile console max inactive interval.	The number of minutes after which XenMobile logs an inactive user out of the XenMobile console. A time-out of 0 means an inactive user remains logged in. Default is **30**.
Inactivity Timeout in Minutes	The number of minutes after which XenMobile logs out an inactive user who used the XenMobile server Public API to access the XenMobile 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**.

iOS Device Management Enrollment Install Root CA if Required	When this property is **True**, XenMobile checks if the user has the root CA installed on the device and, if the root certificate is missing, installs it. A third-party public certificate trusted by iOS is required. Default is **True**. If you are using trusted certificates and the iOS device trusts the issuer, setting this property to False improves the MDM user enrollment experience because Secure Hub doesn't prompt the user to install another certificate and enter their PIN. However, we don't recommend setting the property to **False** if you are using a self-signed SSL Listener certificate on the XenMobile server.
VPP baseline interval	The **VPP baseline interval** sets the minimum interval that XenMobile re-imports VPP licenses from Apple. Refreshing license information ensures that XenMobile reflects all changes, such as when you manually delete an imported app from VPP. By default, XenMobile refreshes the VPP license baseline a minimum of every **720** minutes. If you have a large number of VPP 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 VPP license changes from Apple, Citrix recommends that you lower the value to keep XenMobile updated with the changes. The minimum interval between two baselines is 60 minutes. Because the cron job runs in the background every 60 minutes, if the VPP baseline interval is 60 minutes, the interval between baselines could be delayed up to 119 minutes.

Some server properties help improve performance and stability. For details, see Tuning XenMobile Operations.

Device and App Policies

Jan 12, 2018

> ### Note
>
> This section applies to XenMobile Service and XenMobile on-premises deployments.

XenMobile 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

XenMobile 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.
- 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 XenMobile Protects Data at Rest

Data stored on mobile devices is referred to as data at rest. The mobile application management (MAM) capabilities in XenMobile enable complete management, security, and control over XenMobile Apps, MDX-enabled apps, and their associated data. The Worx App SDK, which enables apps for XenMobile 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, XenMobile also includes app-level encryption. XenMobile 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 Worx App 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. XenMobile 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 Worx App SDK uses FIPS 140-2 compliant AES 256- bit encryption with keys stored in a protected Citrix Secret Vault.

How XenMobile Protects Data in Transit

Data on the move between your user's mobile devices and your internal network is referred to as data in transit. MDX app container technology provides application-specific VPN access to your internal network through NetScaler Gateway.

Consider the situation where an employee wants to access the following resources 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 NetScaler Gateway policy, used for authentication and for micro VPN sessions with an app. You can use an Alternate NetScaler Gateway with the Online 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 XenMobile 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 XenMobile operation in sync with enterprise or industry changes, such as new corporate security policies or compliance regulations.
- When a new version of MDX Toolkit 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 XenMobile. 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.

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, for iOS 9 devices, 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 Client Properties in your XenMobile Server Settings. 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 XenMobile.

User example: When opening the Citrix Secure Web application on the device, the user must enter their Citrix PIN before they can browse web sites if the inactivity period is expired.

Online session required

Why use this policy: If an application requires access to a web app (web service) to run, enable this policy so that XenMobile 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 Online session required policy enabled, they can't use the app until they connected to the network using a cellular or wifi 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 XenMobile.

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 wifi service and reauthenticate, if prompted.

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 XenMobile 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 travelling internationally.

User example: You load a new version of Secure Mail in the XenMobile 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 expires. When the 6 hours expires, Secure Hub routes users to the XenMobile Store.

Active poll period (minutes)

Why use this policy: The active poll period is the interval at which XenMobile 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 XenMobile to the device, the lock occurs within 60 minutes of when the last poll took place.

Why use these policies: XenMobile includes a secret vault with a strong encryption layer that Secure Hub and other XenMobile 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 XenMobile 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.

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 ShareFile or Quick Edit but can't open the attached document in their own personal file viewing apps that are outside the container.

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.

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 NetScaler 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.

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.

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 NetScaler 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 XenMobile 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 XenMobile 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 XenMobile 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 Android and Windows Mobile devices can connect back to XenMobile for MDM management, app push, and policy deployment. If you do not deploy this policy and have not enabled Google Firebase Cloud Messaging (FCM), devices will not connect back to XenMobile. It is important to deploy this policy in the base package for enrolling devices. The Scheduling options are as follows:

Always - Keeps the connection alive permanently. Citrix recommends this option for optimized security. When you choose **Always**, also use the Connection timer policy to ensure that the connection is not draining the battery. By keeping the connection alive, you can push security commands like wipe or lock to the device on-demand. You must also select the Deployment Schedule option **Deploy for always-on connection** in each policy you deploy to the device.

Never - Connects manually. Citrix does not recommend this option for production deployments because the **Never** option prevents you from deploying security policies to devices; thus, users never receive any new apps or policies.

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, XenMobile processes the policy on the device the next time the device connects.

Define schedule - When enabled, XenMobile attempts to reconnect the user's device to the XenMobile 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 XenMobile, 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 XenMobile Store.

Native emal 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 the XenMobile server, 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 XenMobile 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 in appropriate 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.

XenMobile Store policy

Why use this policy: The XenMobile 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 productivity apps, native mobile apps such as .ipa or .apk files, iTunes and Google play apps, web links, and XenApp and XenDesktop apps published using Citrix StoreFront.

User example: After a user enrolls their device into XenMobile, they access the XenMobile Store through the Citrix Secure Hub app. 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 XenMobile Store.

User Enrollment Options

Sep 06, 2017

Note: This section applies to XenMobile Service and XenMobile on-premises deployments.

You can have users enroll their devices in XenMobile in a number of ways. Before considering the specifics, you must decide if the devices in your environment will enroll in Enterprise mode (MDM+MAM), MDM mode, or MAM mode (also referred to 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 the Apple Device Enrollment Program (DEP) and Google Android for Work. Through each of these programs, you can purchase devices that are pre-configured and ready for employees to use. For more information, see Apple Device Enrollment Program (DEP) and Google Android for Work.

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 XenMobile Settings page, and you can select a default from Username + Password, Two Factor, and Username + PIN. For information on each enrollment mode, see To configure enrollment modes in the XenMobile documentation.

If you choose certificate-based, consider excluding Username + Password traditional authentication from the allowed options, because this mode may 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; once 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 XenMobile 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 for iOS.

In the XenMobile console, you can also choose the option for Enrollment Profiles, through which 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 additional infrastructure. For more information on this option, see Notifications in the XenMobile documentation.

In addition, if you plan to send invitations by email, ensure that users have a way of accessing email outside of Secure Hub. You may use one-time password (OTP) enrollment modes as an alternative to Active Directory passwords for MDM enrollment. Note that OTP is available on iOS and Android devices only and is not currently available on Windows devices.

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 To configure enrollment modes and the Self Help Portal in the XenMobile documentation.

With manual enrollment, users connect to XenMobile 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 XenMobile Autodiscovery Service in the XenMobile documentation.

You can facilitate manual enrollment in a number of 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 and/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.

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 XenMobile 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, this shouldn't be an issue. You may want to consider this method, however, in a BYOD workplace where 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 invite, see Sending an enrollment invitation in the XenMobile documentation.

You'll need to send an invite for each user or group whom you want enrolled in your environment, which 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.

When you have decided whether you want to use open enrollment or selective invitation and have set up those environments, you'll need to make users aware of 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 XenMobile console for open enrollment as well. For details, see Sending an enrollment invitation in the XenMobile documentation.

In either case, keep in mind that for email, you need an SMTP server. For text messages, you need an SMS server. These may 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 XenMobile, sending them an invitation email would be problematic.

You may also send communication by another means outside of XenMobile for an open enrollment environment, as long as you include all the relevant information, such as where users can get the Secure Hub app and what method they should use to enroll. If you have autodiscovery turned off, you need to tell them the XenMobile server address as well. To learn more about autodiscovery, see XenMobile Autodiscovery Service in the XenMobile documentation.

Tuning XenMobile Operations

Sep 06, 2017

The performance and stability of XenMobile operations involves many settings across XenMobile and depends on your NetScaler and SQL Server database configuration. This article focuses on the settings that are most often configure, related to the tuning and optimization of XenMobile. Citrix recommends that you evaluate each of the settings in this article before deploying XenMobile.

> ## Important
>
> These guidelines assume that the XenMobile server CPU and RAM is adequate for the number of devices. For more information about scalability, see Scalability and performance in the XenMobile documentation.

The following server properties globally apply to operations, users, and devices across an entire XenMobile instance. Be aware that a change to some server properties requires a restart of each XenMobile server node. XenMobile notifies you when a restart is required.

These tuning guidelines apply to both clustered and non-clustered environments.

Settings	Up to 5,000 devices	5,000 to 10,000 devices	More than 10,000 devices
hibernate.c3p0.max_size This XenMobile server property, Custom Key, determines the maximum number of connections that XenMobile can open to the SQL Server database. XenMobile uses the value you specify for this custom key as an upper limit; the connections open only if you need them. Base your settings on the capacity of your database server. Default is **1000**. To change this setting, you must add a server property to XenMobile server with the following configuration: Key: **Custom Key** Key: **hibernate.c3p0.max_size** Value: **500** Display name:	200	500	1000 **Note:** In high load situations, such as a very large deployment, consider setting this key to **1000** to better handle the extra load when a large number of devices connect simultaneously.

hibernate.c3p0.max_size=*nnn* Description: **DB connections to SQL** Note the following equation in a clustered configuration. Your c3p0 connection multiplied by the number of nodes equals your actual maximum number of connections that XenMobile can open to the SQL Server database. In clustered and non-clustered configuration, setting the value too high with an undersized SQL Server can cause resource issues on the SQL side during peak load. Setting the value too low means you might not be able to take advantage of the SQL resources available.			
hibernate.c3p0.timeout This XenMobile server property, Custom Key, determines the idle time-out. Default is **300**. Key: **Custom Key** Key: **hibernate.c3p0.timeout** Value: **30** Display name: **hibernate.c3p0.timeout=30** Description: **Database idle timeout**	If you use database cluster failover, Citrix recommends that you add this Custom Key and set it to reduce the idle time-out to about **30** seconds.		
Push Services Heartbeat Interval This setting determines how frequently an iOS device checks if an APNs notification is not delivered in the interim. Increasing the APNs heartbeat frequency can optimize database communications. Too large a value can add unnecessary load. This setting applies only to iOS.	23 hours	23 hours	7 days

Default is **6** hours. If you have a large number of iOS devices in your environment, the heartbeat interval can lead to higher load than necessary. Security actions, such as selective wipe, lock, full wipe, and so on do not rely on this heartbeat, as an APNs notification is sent to the device when these actions are executed. This value governs how quickly a policy updates after Active Directory Group membership changes. As such, it is often suitable to increase this value to something between 12 and 23 hours to reduce load.	
iOS MDM APNS Connection Pool Size An APNs connection pool that is too small can negatively affect APNs activity performance when you have more than 100 devices. Performance issues include slower deployment of apps and policies to devices and slower device registration. Default is blank, meaning 1.	Recommended setting is **10** or up to the maximum number of APNs servers for your geographic location.

Server Property	Default Setting	Why Change This Setting?
Background Deployment	360 minutes	The frequency for background policy deployments, in minutes. Applies only to always-on connections for Android devices. Increasing the frequency of policy deployments reduces server load. Recommended setting is **1440** (24 hours).
Background Hardware Inventory	360 minutes	The frequency for background hardware inventory, in minutes. Applies only to always-on connections for Android devices. Increasing the frequency of hardware inventory reduces server load. Recommended setting is **1440** (24 hours).

Interval for check deleted Active Directory user	0 minutes	The default value **0** prevents XenMobile from checking for deleted Active Directory users. Increase this value to match your Active Directory sync setting. The standard sync time for Active Directory is **15** minutes.
MaxNumberOfWorker	3	The number of threads used when importing a large number of VPP licenses. Defaults to **3**. If you need further optimization, you can increase the number of threads. However, be aware that with a larger number of threads, such as 6, a VPP import results in very high CPU usage.
Custom keys: **auth.ldap.connect.timeout=60000** **auth.ldap.read.timeout=60000**	6000	To compensate for slow LDAP responses, Citrix recommends that you add server properties for the following Custom Keys. Key: **Custom Key** Key: **auth.ldap.connect.timeout** Value: **60000** Display name: **auth.ldap.connect.timeout=60000** Description: **LDAP connection timeout** Key: **Custom Key** Key: **auth.ldap.read.timeout** Value: **60000** Display name: **auth.ldap.read.timeout=60000** Description: **LDAP read timeout**

You can schedule deployments for Android devices using the Google Firebase Cloud Messaging (FCM, previously named Google Cloud Messaging) or XenMobile settings.

If using FCM to schedule deployments

Enabling FCM for your XenMobile environment allows for near real-time notifications to Android devices, similar to APNs for iOS devices. With FCM configured, when XenMobile needs to connect to a device for a policy update, selective wipe, and so on, the XenMobile server sends a notification message to the FCM server to forward the request to the client device. After the device receives the notification from FCM, the device connects back to XenMobile for further instructions. Keep in mind that this method relies on third-party servers (Google) and therefore is subject to service interruptions outside the control of your IT department or Citrix Support.

For information on how to register with the FCM service, refer to XenMobile and Firebase Cloud Messaging (FCM) Configuration.

If using FCM for Android, be aware of the following XenMobile server properties. The properties still use the prior acronym for Google Cloud Messaging, GCM.

- **GCM API Key**: The key created in the Google Developers Console.
- **GCM Sender ID**: The Project Number in the Google Developers Console.

- **GCM Registration ID TTL**: The delay, in days, before renewing the device FCM registration ID. Defaults to **10**.
- **GCM Heartbeat Interval**: Defaults to **6** hours.

If using XenMobile settings to schedule deployments

To schedule deployments to Android devices, use these XenMobile settings:

- Set the **Connection Scheduling Policy** (a XenMobile device policy) to **Always**, which keeps the connection alive permanently. This enables you to deploy policies to delivery groups immediately. The open connection also enables the background services defined in the server properties **Background Deployment** and **Background Hardware Inventory** to occur per those property settings.
- Select the **Deployment Schedule** option **Deploy for always-on connection** in each policy deployed to the device.

> Note
>
> For Android devices, setting the **Deployment condition** to **Only when previous deployment has failed** helps with device usage, because some devices overwrite the policy and some devices reset the policy. If a device resets the policy, XenMobile might prompt users for credentials every time a policy that requires authentication is re-deployed. Enabling this feature also helps with server load and prevents the success reported from bouncing between failed and success when XenMobile pushes the policy every time the device connects.

App Provisioning and Deprovisioning

Sep 06, 2017

Application provisioning revolves around mobile app lifecycle management, which mainly consists of wrapping, configuring, delivering, and managing mobile apps within a XenMobile environment. In some instances, developing or modifying application code may also be part of the provisioning process. XenMobile 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 secure browse or full VPN

Example:

Factor	Secure Mail	Secure Mail	In-House	Epic Rover
Version	10.1	10.1	X.x	X.x
Instance	VIP	Physicians	Clinical	Clinical
Platform	iOS	iOS	iOS	iOS
Target Users	VIP Users	Physicians	Clinical Users	Clinical Users
Ownership	IT	IT	IT	IT

Type	MDX	MDX	Native	Public
Upgrade Cycle	Quarterly	Quarterly	Yearly	N/A
Licensing	N/A	N/A	N/A	VPP
MDX Policies	Yes	Yes	Yes	No
Network Access	VPN	VPN	VPN	Public

- **App versioning**: Maintaining and tracking app versions is a critical part of the provisioning process. Versioning is 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 XenMobile, you can use MDX policies with managed apps to secure the corporate data through app wrapping. For more information about the MDX Toolkit for app wrapping, see MDX Toolkit in the XenMobile documentation. 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 XenMobile 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**: XenMobile allows you to deliver apps as MDM apps or as MAM apps. The MDM apps appear in the XenMobile 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 in which you have an on-premises XenMobile deployment with app management requirements along with MDM. 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 device 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.
3. Testing: Identify test users, issues, and bugs.
4. Deployment: Deploy the app to production users.
5. Maintenance: Update app version. Deploy the app in a test environment before updating the app in a production environment.

Application Lifecycle Example Using Secure Mail

1. Requirements for specifications: As a security requirement, you require a mail app that is containerized and supports MDX security policies.
2. Development: Validate that the app meets business needs. You must be able to apply MDX policy controls to the app.
3. Testing: Assign Secure Mail to a test users group and deploy the corresponding MDX file from the XenMobile Server. The test users validate that they can successfully send and receive email, and have calendar and contact access. The test users also report issues and identify bugs. Based on the test users' feedback you optimize Secure Mail configuration for production use.
4. Deployment: When the testing phase is complete, you assign Secure Mail to production users and deploy the corresponding MDX file from XenMobile Server.
5. Maintenance: A new update to Secure Mail is available. You download the new MDX file from Citrix downloads and replace the existing MDX file on the XenMobile Server. Instruct the users to perform the update. Note: Citrix recommends that you complete and test this process in a test environment before uploading the app to a XenMobile production environment and deploying the app to users.

For more information, see Wrapping iOS Mobile Apps and Wrapping Android Mobile Apps in the XenMobile documentation.

Dashboard-Based Operations

Sep 06, 2017

You can view information at a glance by accessing your XenMobile 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 XenMobile 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.
  - **Android TouchDown License Status**: Displays the number of devices that have a TouchDown license.
  - **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.
  - **VPP Apps License Usage**: Displays license usage statistics for Apple Volume Purchase Program apps.

Use Cases

Some examples for the many ways you can use dashboard widgets to monitor your environment are as follows.

- You have deployed XenMobile Apps and are receiving support tickets regarding XenMobile Apps failing to install on devices. Use the **Out of Compliance Devices** and **Installed Apps** widgets to see the devices that do not have XenMobile 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.

After your environment is setup and users enroll, you can run reports to learn about your deployment. XenMobile 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 in the XenMobile documentation.

Important: Although it is possible to use SQL Server to create custom reports, Citrix does not recommend this method. Using the SQL Server database in this manner may have unforeseen consequences in your XenMobile deployment. If you do decide to pursue this method of reporting, ensure that SQL queries are run using a read-only account.

Role-Based Access Control and XenMobile Support

Nov 29, 2017

XenMobile uses role-based access control (RBAC) to restrict user and group access to XenMobile system functions, such as the XenMobile console, Self Help Portal, Remote Support, and public API. This article describes the roles built in to XenMobile and includes considerations for deciding on a support model for XenMobile 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 from the XenMobile documentation. For a definition of each feature, see Configure roles with RBAC in the XenMobile documentation.

Roles	Default Access Granted	Considerations
Admin	Full system access except to the Self-Help Portal and Remote Support. By default, administrators can perform some support tasks, such as check connectivity and create support bundles.	Do some or all of your administrators need access to the Self-Help Portal or Remote Support? 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	Access to the XenMobile console to perform basic administration on Windows CE devices: add, change, and remove devices; use the Settings page.	The Device Provisioning role applies only to Windows CE devices.
Support	Access to Remote Support.	For on-premises XenMobile Server deployments: Remote support enables your help desk representatives to take remote control of managed Windows CE and Android mobile devices. Screen cast is supported on Samsung KNOX devices only. Remote support isn't available to XenMobile Service customers and isn't supported for clustered on-premises XenMobile Server deployments.

User	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 XenMobile 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.	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 XenMobile 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 XenMobile 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 XenMobile 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 XenMobile-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 XenMobile Self Help Portal?

Although some organizations prefer not to grant users access to XenMobile, 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.

Systems Monitoring

Sep 06, 2017

To ensure optimal uptime for app access and connectivity, you should monitor the following core components in the XenMobile environment:

XenMobile server

XenMobile server generates and stores logs on local storage that you can also export to a systems log (syslogs) server. You can configure log settings to specify size constraints, log level, or you can create custom loggers to filter specific events. You can look at XenMobile server logs from the XenMobile console at any time. You can also export information in the logs via the syslog server to your production Splunk logging servers.

The following list describes the different types of log files available in XenMobile:

Debug log file: Contains debug level information about core web services of XenMobile, including error messages and server-related actions.

Message format:

<date> <timestamp> <loglevel> <class name (including the package)> - <id> <log message>

- where <id> is a unique identifier like sessionID.
- where <log message> is the message supplied by the application.

Admin audit log file - Contains audit information about activity on the XenMobile console.

Note: The same format is used for both admin audit and user audit logs.

Message format:

With the exception of required Date and Timestamp values, all other attributes are optional. Optional fields are represented with " " in the message.

<date> <timestamp> "<username/id>" "<sessionid>" "<deviceid>" "<clientip>" "<action>" "<status>"

"<application name>" "<app user id>" "<user agent>" "<details>"

The following table lists the available admin audit log events:

Admin Audit Log Messages	
Event	**Status**
Login	success/failure
Logout	success/failure

Event	Status
Update admin	success/failure
Get application	success/failure
Add application	success/failure
Update application	success/failure
Delete application	success/failure
Bind application	success/failure
Unbind application	success/failure
Disable application	success/failure
Enable application	success/failure
Get category	success/failure
Add category	success/failure
Update category	success/failure
Delete category	success/failure
Add certificate	success/failure
Delete certificate	success/failure
Active certificate	success/failure
Self-sign certificate	success/failure
CSR certificate	success/failure

Event	Status
Export certificate	success/failure
Delete certificate chain	success/failure
Add certificate chain	success/failure
Get connector	success/failure
Add connector	success/failure
Delete connector	success/failure
Update connector	success/failure
Get device	success/failure
Lock device	success/failure
Unlock device	success/failure
Wipe device	success/failure
Unwipe device	success/failure
Delete device	success/failure
Get role	success/failure
Add role	success/failure
Update role	success/failure
Delete role	success/failure
Bind role	success/failure
Unbind role	success/failure

Event	Status
Update config settings	success/failure
Update workflow email	success/failure
Add workflow	success/failure
Delete workflow	success/failure
Add Active Directory	success/failure
Update Active Directory	success/failure
Add masteruserlist	success/failure
Update masteruserlist	success/failure
Update DNS	success/failure
Update Network	success/failure
Update log server	success/failure
Transfer log from log server	success/failure
Update syslog	success/failure
Update receiver updates	success/failure
Update time server	success/failure
Update trust	success/failure
Add service record	success/failure
Update service record	success/failure
Update receiver email	success/failure

Event	Status
Upload patch	success/failure
Import snapshot	success/failure
Fetch app store app details	success/failure
Update MDM	success/failure
Delete MDM	success/failure
Add HDX	success/failure
Update HDX	success/failure
Delete HDX	success/failure
Add Branding	success/failure
Delete Branding	success/failure
Update SSL offload	success/failure
Add account property	success/failure
Delete account property	success/failure
Update account property	success/failure
Add beacon	success/failure

User audit log file: Contains information related to the user activity from enrolled devices.

Note: The same format is used for both user audit and admin audit logs.

Message format:

With the exception of required Date and Timestamp values, all other attributes are optional. Optional fields are represented with " " in the message. For example,

```
<date> <timestamp> " <username/id>" "<sessionid>" "<deviceid>" "<clientip>" "<action>" "<status>"  " <application name>" "<app user id>" "<user agent>" "<details>"
```

The following table lists the available user audit log events:

User Audit Log Messages

Event	Status
Login	success/failure
Session time-out	success/failure
Subscribe	success/failure
Unsubscribe	success/failure
Pre-launch	success/failure
AGEE SSO	success/failure
SAML Token for ShareFile	success/failure
Device registration	success/failure
Device check	lock/wipe
Device update	success/failure
Token refresh	success/failure
Secret saved	success/failure
Secret retrieved	success/failure
User initiated change password	success/failure
Mobile client download	success/failure

Event	Status
Logout	success/failure
Discovery Service	success/failure
Endpoint Service	success/failure

MDM Functions	
REGHIVE	success/failure
Cab inventory	success/failure
Cab	success/failure
Cab auto install	success/failure
Cab shell install	success/failure
Cab create folder	success/failure
Cab file get	success/failure
File create folder	success/failure
File get	success/failure
File sent	success/failure
Script create folder	success/failure
Script get	success/failure
Script sent	success/failure
Script shell execution	success/failure

MDM Functions	
APK inventory	success/failure
APK	success/failure
APK shell install	success/failure
APK auto install	success/failure
APK create folder	success/failure
APK file get	success/failure
APK App	success/failure
EXT App	success/failure
List get	success/failure
List sent	success/failure
Locate device	success/failure
CFG	success/failure
Unlock	success/failure
SharePoint wipe	success/failure
SharePoint Configuration	success/failure
Remove profile	success/failure
Remove application	success/failure
Remove unmanaged application	success/failure

MDM Functions	
IPA App	success/failure
EXT App	success/failure
Apply redemption code	success/failure
Apply settings	success/failure
Enable tracking device	success/failure
App management policy	success/failure
SD card wipe	success/failure
Encrypted email attachment	success/failure
Branding	success/failure
Secure browser	success/failure
Container browser	success/failure
Container unlock	success/failure
Container password reset	success/failure
AG client auth creds	success/failure

NetScaler also monitors the XenMobile web service state, which is configured with intelligent monitoring probes to simulate HTTP requests to each XenMobile server cluster node. The probes determine whether the service is online and then respond based on the response received. In the event that a node does not respond as expected, NetScaler marks the server as down. In addition, NetScaler takes the node out of the load-balancing pool and logs the event for use in generating alerts through the NetScaler monitoring solution.

You can also use standard hypervisor monitoring tools to monitor the XenMobile virtual machines and to provide relevant alerts regarding CPU, memory, and storage utilization metrics.

SQL Server and database

SQL Server and database performance directly affects XenMobile services. The XenMobile instance requires access to the database at all times and goes offline (for example, stops responding) in the event of an outage to the SQL infrastructure. The XenMobile console may continue to function for a while following any disk space issues with SQL Server. To ensure maximum database uptime and adequate performance for the XenMobile workload, you should proactively monitor the state of your SQL Servers following Microsoft recommendations. Additionally, you should adjust resource allocation for CPU, memory, and storage to guarantee service level agreements as your XenMobile environment continues to grow.

NetScaler

NetScaler provides the ability to log metrics to internal storage or to send logs to an external logging server. You can configure the syslog server to export NetScaler logs to your production Splunk logging servers. The following logging levels are available in NetScaler:

- Emergency
- Alert
- Critical
- Error
- Warning
- Information

The log files are also stored in NetScaler storage in the /var/log/ns.log directory and named newnslog. NetScaler rolls over and compresses the files by using the GZIP algorithm. Log file names are newnslog.xx.gz, where xx represents a running number.

NetScaler also supports SNMP traps and alerts as a monitoring option. The following table lists the SNMP traps recommended for the environment.

NetScaler SNMP traps

Configuration	Setting
cpuUtilization 1.3.6.1.4.1.5951.1.1.0.3	This trap indicates that the CPU utilization has exceeded the high threshold.
averageCpuUtilization 1.3.6.1.4.1.5951.1.1.0.51	This trap indicates that the average CPU usage in the multi-processor NetScaler system has exceeded the high threshold.
memoryUtilization 1.3.6.1.4.1.5951.1.1.0.13	This trap is sent when the memory utilization of the system exceeds the threshold value.
netScalerLoginFailure 1.3.6.1.4.1.5951.1.1.0.55	This trap is sent when a logon attempt to NetScaler fails.
diskUsageHigh 1.3.6.1.4.1.5951.1.1.0.64	This trap indicates that disk usage has gone high.
haSyncFailure 1.3.6.1.4.1.5951.1.1.0.69	This trap indicates that configuration synchronization has failed on the secondary instance.

Configuration	Setting
1.3.6.1.4.1.5951.1.1.0.70	This trap indicates that high availability heartbeats are not received from the secondary instance.
haBadSecState 1.3.6.1.4.1.5951.1.1.0.71	This trap indicates that the secondary instance is in DOWN/UNKNOWN/STAY SECONDARY state.
haPropFailure 1.3.6.1.4.1.5951.1.1.0.85	This trap indicates that configuration propagation has failed on the secondary instance.
ipConflict 1.3.6.1.4.1.5951.1.1.0.86	This trap indicates that an IP address conflict is present with another device in the network.

Disaster Recovery

Sep 06, 2017

You can architect and configure XenMobile deployments that include multiple sites for disaster recovery using an active-passive failover strategy.

The recommended disaster recovery strategy discuss in this article consists of:

- A single XenMobile active site in the datacenter of one geographical location serving all the enterprises users globally, known as the primary site.
- A second XenMobile site in the datacenter of a second geographical location, known as the disaster recovery site. This disaster recovery site provides active-passive site failover in if a site-wide datacenter failure occurs in the primary site. The primary site includes XenMobile, SQL database, NetScaler infrastructure in order to facilitate failover and provide users with access to XenMobile via the event of connectivity failure to the primary site.

The XenMobile servers at the disaster recovery site remains offline during normal operations and is brought online during only disaster recovery scenarios, where complete site failover from the primary site to the disaster recovery site is required. The SQL Servers at the disaster recovery site must be active and ready to service connections before you start the XenMobile servers at the disaster recovery site.

This disaster recovery strategy relies on manual failover of the NetScaler access tier by means of DNS changes for routing MDM and MAM connections to the disaster recovery site in the event of an outage.

> ### Note
>
> To use this architecture, you must have a process in place for asynchronous backups of the databases and some way of ensuring high availability for the SQL infrastructure.

Disaster Recovery Failover Process

1. If you are testing your disaster recovery failover process, shut down XenMobile servers in the primary site to simulate site failure.
2. Change public DNS records for the XenMobile servers to point to the disaster recovery site's external IP addresses.
3. Change internal DNS record for the SQL Server to point to the disaster recovery site's SQL Server IP address.
4. Bring XenMobile SQL databases online at the disaster recovery site. Ensure that the SQL Server and database is active and ready to service connections from the XenMobile servers local to the site.
5. Turn on the XenMobile servers on the disaster recovery site.

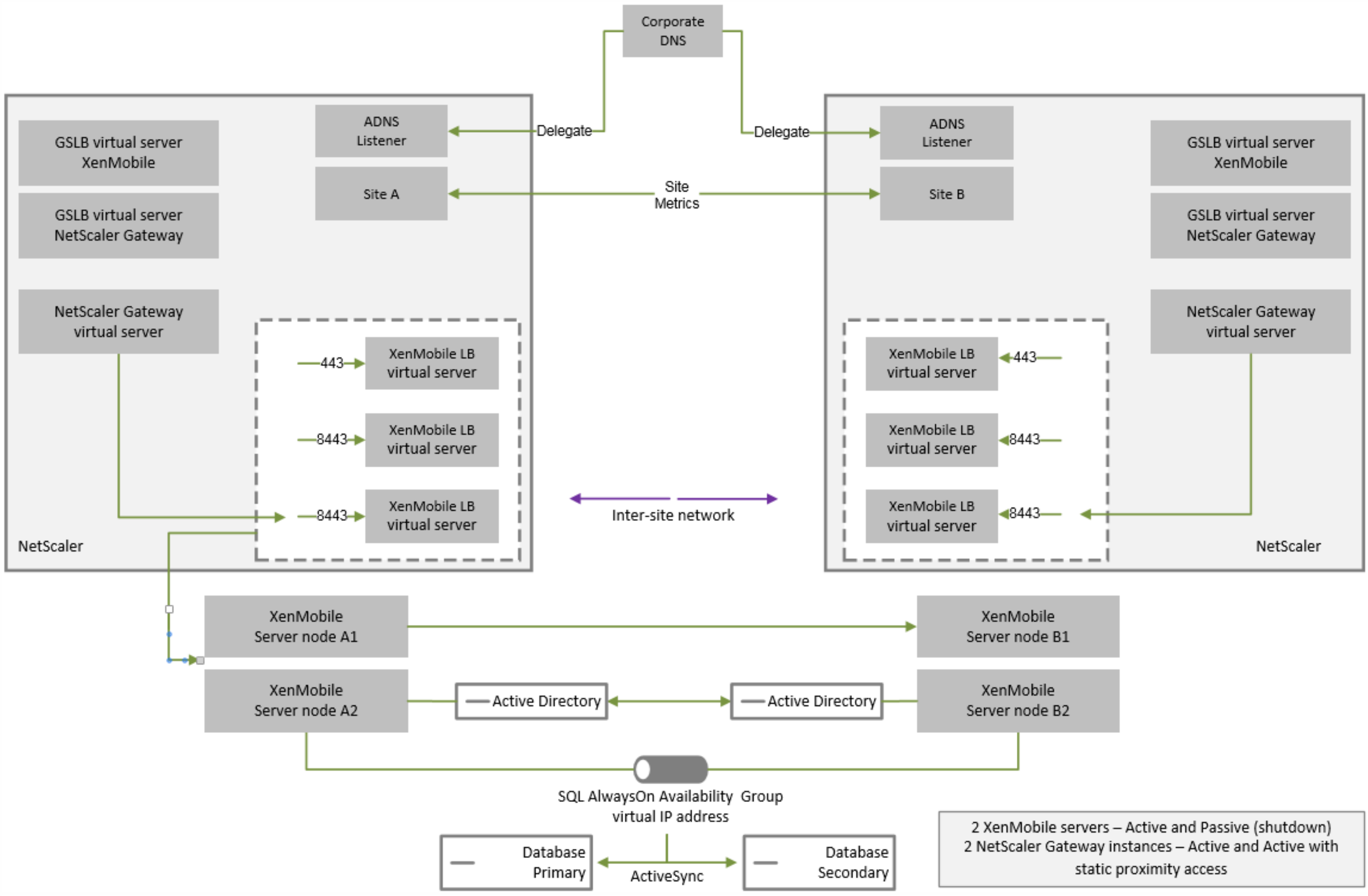
XenMobile Server Update Process

Follow these steps any time you update XenMobile with patches and releases, in order to keep the code of the primary and disaster recovery servers uniform.

1. Ensure that XenMobile servers in primary site have been patched or upgraded.
2. Ensure that DNS record for the SQL Server is resolving to the active SQL Server database in the primary site.
3. Bring the disaster recovery site's XenMobile servers online. The servers connect to the primary site's database across the WAN during the upgrade process only.
4. Apply required patches and updates to all disaster recovery site's XenMobile servers.
5. Restart the XenMobile servers and confirm that the patch or upgrade is successful.

Disaster Recovery Reference Architecture Diagram

The following diagram shows the high-level architecture for a disaster recovery deployment of XenMobile.



Corporate DNS
Delegate
Delegate
ADNS Listener
ADNS Listener
Site A
Site B
Site Metrics
GSLB virtual server XenMobile
GSLB virtual server NetScaler Gateway
NetScaler Gateway virtual server
GSLB virtual server XenMobile
GSLB virtual server NetScaler Gateway
NetScaler Gateway virtual server
443
8443
8443
XenMobile LB virtual server
XenMobile LB virtual server
XenMobile LB virtual server
XenMobile LB virtual server
XenMobile LB virtual server
XenMobile LB virtual server
443
8443
8443
Inter-site network
NetScaler
NetScaler
XenMobile Server node A1
XenMobile Server node A2
XenMobile Server node B1
XenMobile Server node B2
Active Directory
Active Directory
SQL AlwaysOn Availability Group virtual IP address
Database Primary
ActiveSync
Database Secondary
2 XenMobile servers – Active and Passive (shutdown)
2 NetScaler Gateway instances – Active and Active with static proximity access

GSLB for Disaster Recovery

A key element of this architecture is the use of Global Server Load Balancing (GSLB) to direct traffic to the correct data center.

By default, the NetScaler for XenMobile wizard configures NetScaler Gateway in a way that does not enable the use of GSLB for disaster recovery. Therefore, you must take additional steps.

GSLB is at its core a form of DNS. Participating NetScaler appliances act as authoritative DNS servers and resolve DNS records to the correct IP address (typically the VIP that is supposed to receive traffic). The NetScaler appliance checks the system health before responding to a DNS query directing traffic to that system.

When a record is resolved, GSLB's role in resolving the traffic is complete. The client communicates directly with the target virtual IP (VIP) address. DNS client behavior plays an important part on controlling how and when a record expires. This is largely outside the boundaries of the NetScaler system. As such, GSLB is subject to the same limitations as DNS name resolution. Clients cache responses; thus, load balancing in this way isn't as real-time as is traditional load balancing.

The GSLB configuration on NetScaler, including sites, services, and monitors, exist in order to provide the correct DNS name resolution.

The actual configuration for publishing servers (in this scenario, the configuration that the NetScaler for XenMobile wizard creates) is not affected by the GSLB. GSLB is a separate service on the NetScaler.

The NetScaler for XenMobile wizard configures NetScaler Gateway for XenMobile. This wizard generates three load balancing virtual servers and a NetScaler Gateway virtual server.

Two of the load balancing virtual servers handle MDM traffic, on port 443 and 8443. NetScaler Gateway receives MAM traffic and forwards it to the third server, the MAM load balancing virtual server, on port 8443. All traffic to the MAM load balancing virtual server is passed through NetScaler Gateway.

The MAM load balancing virtual server requires the same SSL certificate as the XenMobile servers and uses the same FQDN as used to enroll devices. The MAM load balancing server also uses the same port (8443) as one of the MDM load balancing servers. To enable traffic to be resolved, the NetScaler for XenMobile wizard creates a local DNS record on NetScaler Gateway. The DNS record matches the FQDN used to enroll devices.

This configuration is effective when the XenMobile server URL is not a GSLB domain URL. If a GSLB domain URL is used as the XenMobile server URL, as is required for disaster recovery, the local DNS record prevents NetScaler Gateway from resolving traffic to the MDM load balancing servers.

To address the challenges presented by the default configuration created by the NetScaler for XenMobile wizard, you can create a CNAME record for the XenMobile server FQDN in the parent domain (company.com) and point a record in the delegated subzone (gslb.company.com) for which NetScaler is authoritative. Doing so allows for the creation of the static DNS A record for the MAM load balancing VIP address required to resolve traffic.

1. On the external DNS, create a CNAME for the XenMobile server FQDN that points to the GSLB domain FQDN on NetScaler GSLB. You need two GSLB domains: one for MDM traffic and another for MAM (NetScaler Gateway) traffic.

Example: CNAME = xms.company.com   IN CNAME xms.gslb.comany.com

2. On the NetScaler Gateway instance of each site, create a GSLB virtual server with a FQDN that is what the CNAME record is pointing to.

Example: bind gslb vserver xms-gslb -domainName xms.gslb.company.com

When using the NetScaler for XenMobile wizard to deploy NetScaler Gateway, use the XenMobile server URL when configuring the MAM load balancing server. This creates a static DNS A record for the XenMobile server URL.

3. Test with clients enrolling on Secure Hub using the XenMobile server URL (xms.company.com).

This example uses the following FQDNs:

- xms.company.com is the URL that is used by the MDM traffic and is used by devices enrolling, which is configured in this example by using the NetScaler for XenMobile wizard.
- xms.gslb.company.com is the GSLB domain FQDN for the XenMobile server.

Citrix Support Process

Sep 06, 2017

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 XenMobile, XenDesktop, XenServer, XenApp, and NetScaler. 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 XenMobile 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 XenMobile

John Bartel III , | Oct 02, 2017

You can send enrollment invitations to groups in XenMobile. 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 Creating or Updating Notification Templates.

For more information on basic configurations on user accounts, roles, and enrollment modes and invitations, see User accounts, roles, and enrollment.

1. Within the XenMobile 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 Creating or Updating Notification Templates.

For these notification templates, use your configured SMTP server setup within XenMobile. Set your SMTP information first before proceeding.

> ## Note
>
> You will note **Expire after** and **Maximum Attempts** options. These 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.

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.

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, XenMobile 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 an on-premises Device Health Attestation server

Sanket Mishra , | Oct 23, 2017

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 a XenMobile Server policy to enable the on-premises DHA service. For information on creating this policy, 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 be 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.

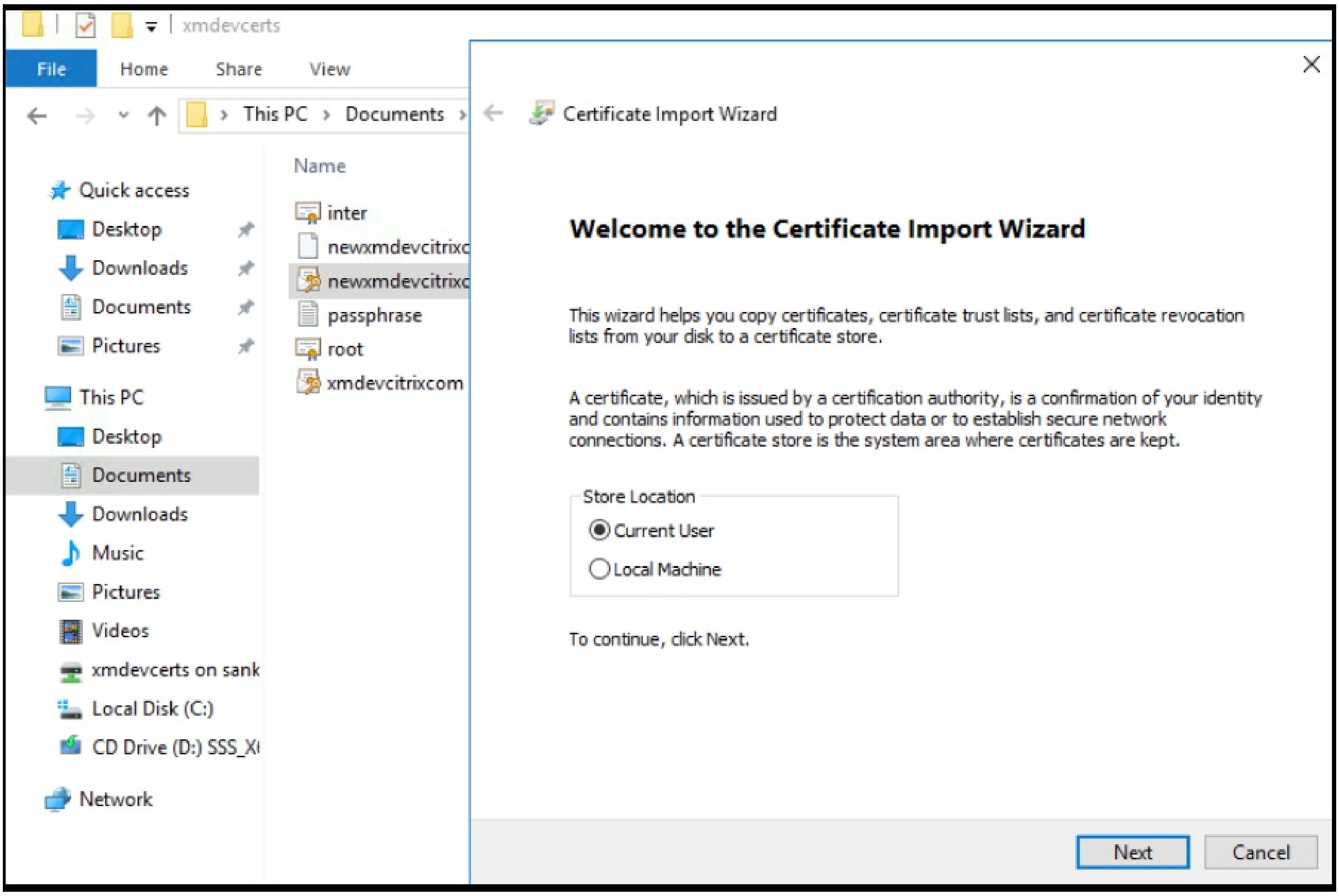
Add the DHA server role to the Windows server

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 role**s 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 feature**s page, click **Next**.
10. On the **Web Server Role (IIS)** page, click **Next**.

11. On the **Select role services** page, click **Next**.
12. On the **Device Health Attestation Service** page, click **Next**.
13. On the **Confirm installation selections** page, click **Install**.
14. When the installation is done, click **Close**.

Add the SSL certificate to the certificate store of the server

1. Go to the SSL certificate file and select it.
2. Select **Current user** as the store location and click **Next**.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

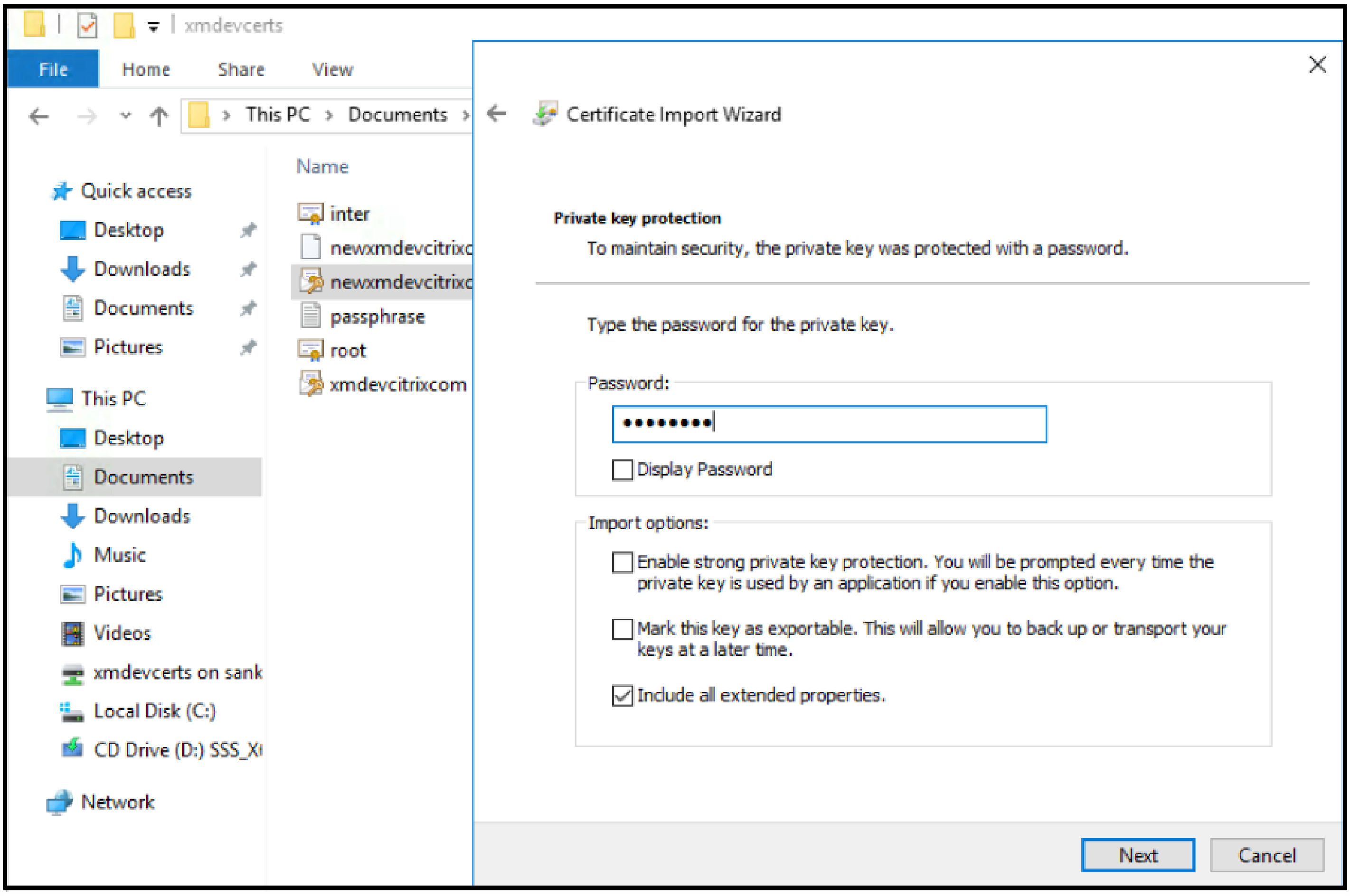
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
● Current User
○ Local Machine

To continue, click Next.

3. Type the password for the private key.

4. Ensure the import option **Include all extended properties** is selected. Click **Next**.



Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••••

□ Display Password

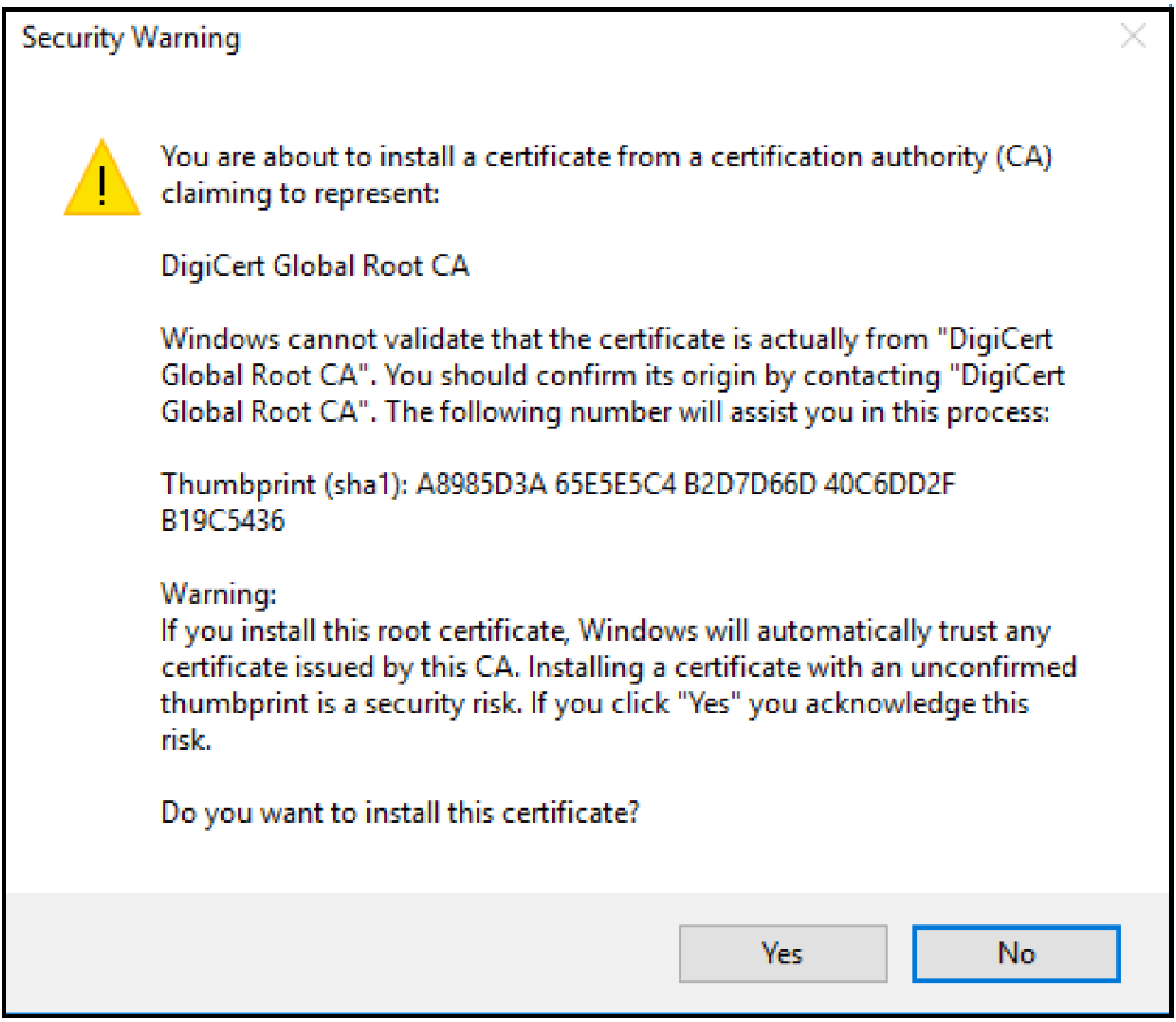
Import options:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

5. When this window appears, click **Yes**.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

DigiCert Global Root CA

Windows cannot validate that the certificate is actually from "DigiCert Global Root CA". You should confirm its origin by contacting "DigiCert Global Root CA". The following number will assist you in this process:

Thumbprint (sha1): A8985D3A 65E5E5C4 B2D7D66D 40C6DD2F B19C5436

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

6. Confirm that the certificate is installed, as described in this Microsoft article:

   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**.

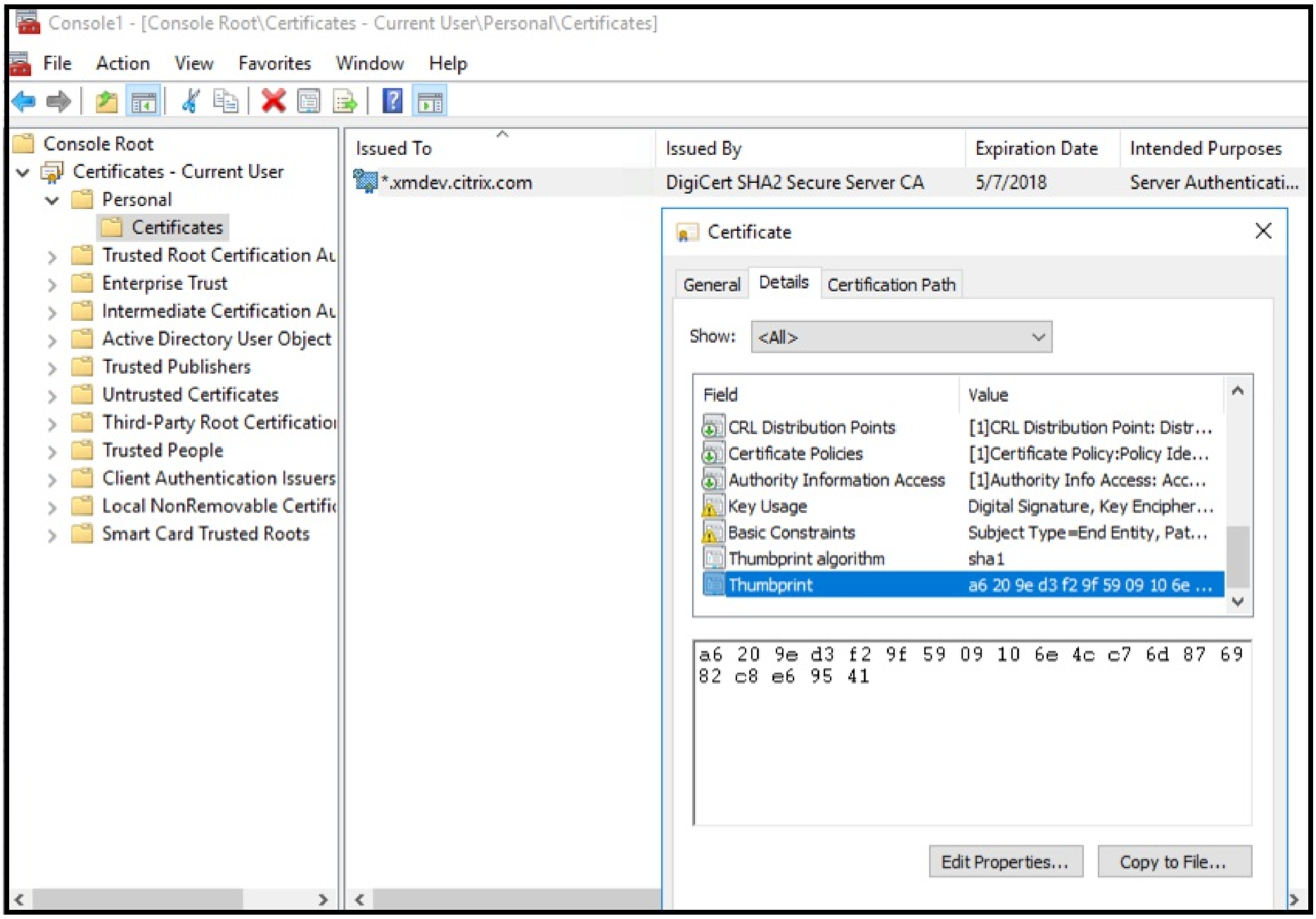
   d. Click **Add**.

   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**.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatio
Trusted People
Client Authentication Issuers
Local NonRemovable Certific
Smart Card Trusted Roots
Certificate
General
Details
Certification Path
Edit Properties...
Copy to File...

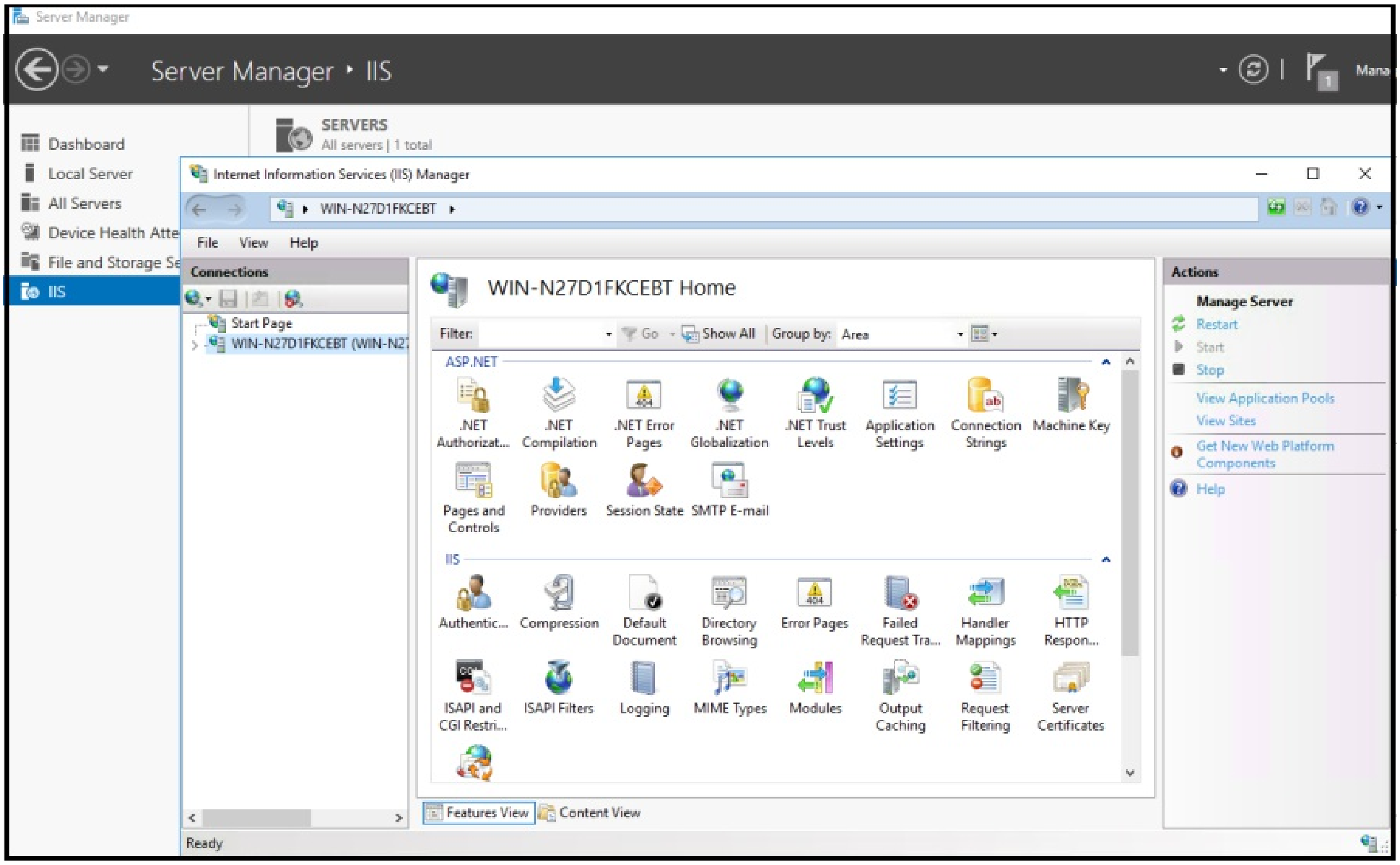
Issued To	Issued By	Expiration Date	Intended Purposes
*.xmdev.citrix.com	DigiCert SHA2 Secure Server CA	5/7/2018	Server Authenticati...

Show: <All>

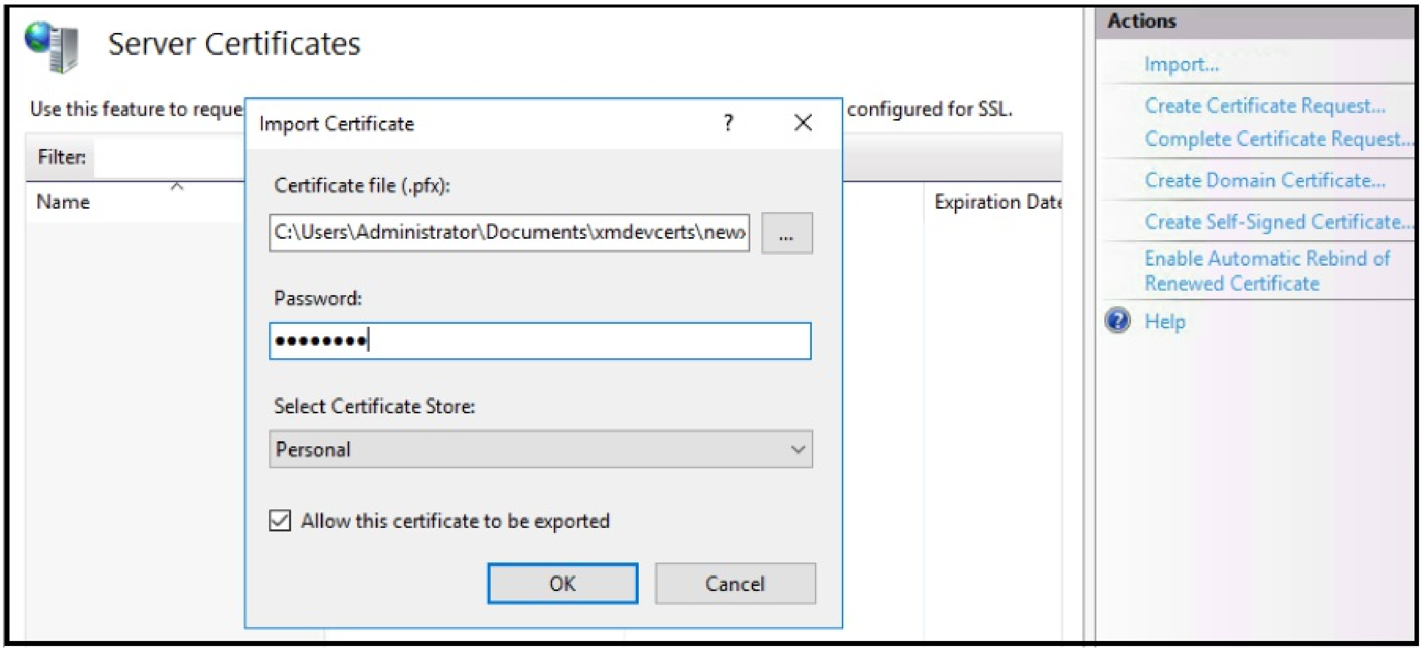
Field	Value
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature, Key Encipher...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint algorithm	sha1
Thumbprint	a6 20 9e d3 f2 9f 59 09 10 6e ...

```
a6 20 9e d3 f2 9f 59 09 10 6e 4c c7 6d 87 69
82 c8 e6 95 41
```

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.


Server Certificates
Use this feature to reque
configured for SSL.
Filter:
Name
Expiration Date
Import Certificate
?
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
...
OK
Cancel

Certificate file (.pfx): C:\Users\Administrator\Documents\xmdevcerts\new

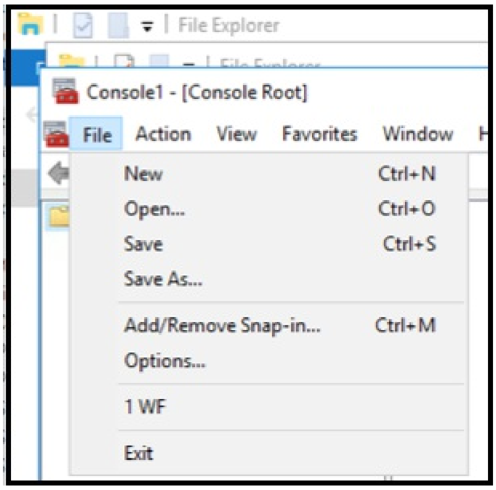
Password: ●●●●●●●●●

Select Certificate Store: Personal

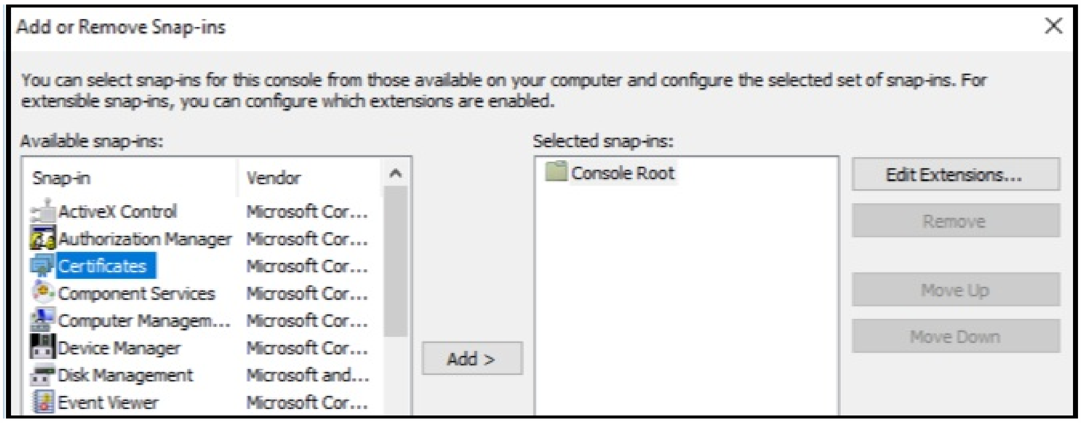
☑ Allow this certificate to be exported

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.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

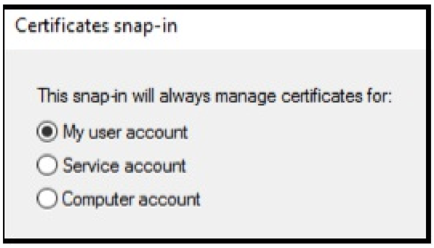
Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...

Selected snap-ins:

Console Root

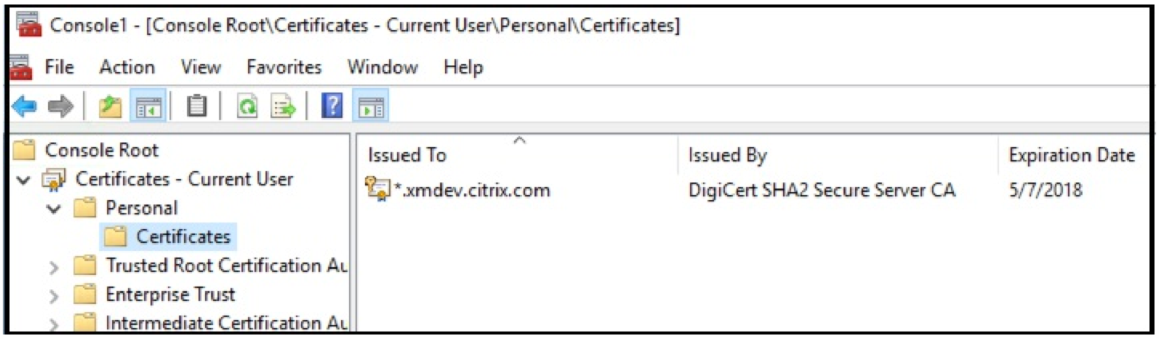
4. Select **My user account**.



This snap-in will always manage certificates for:

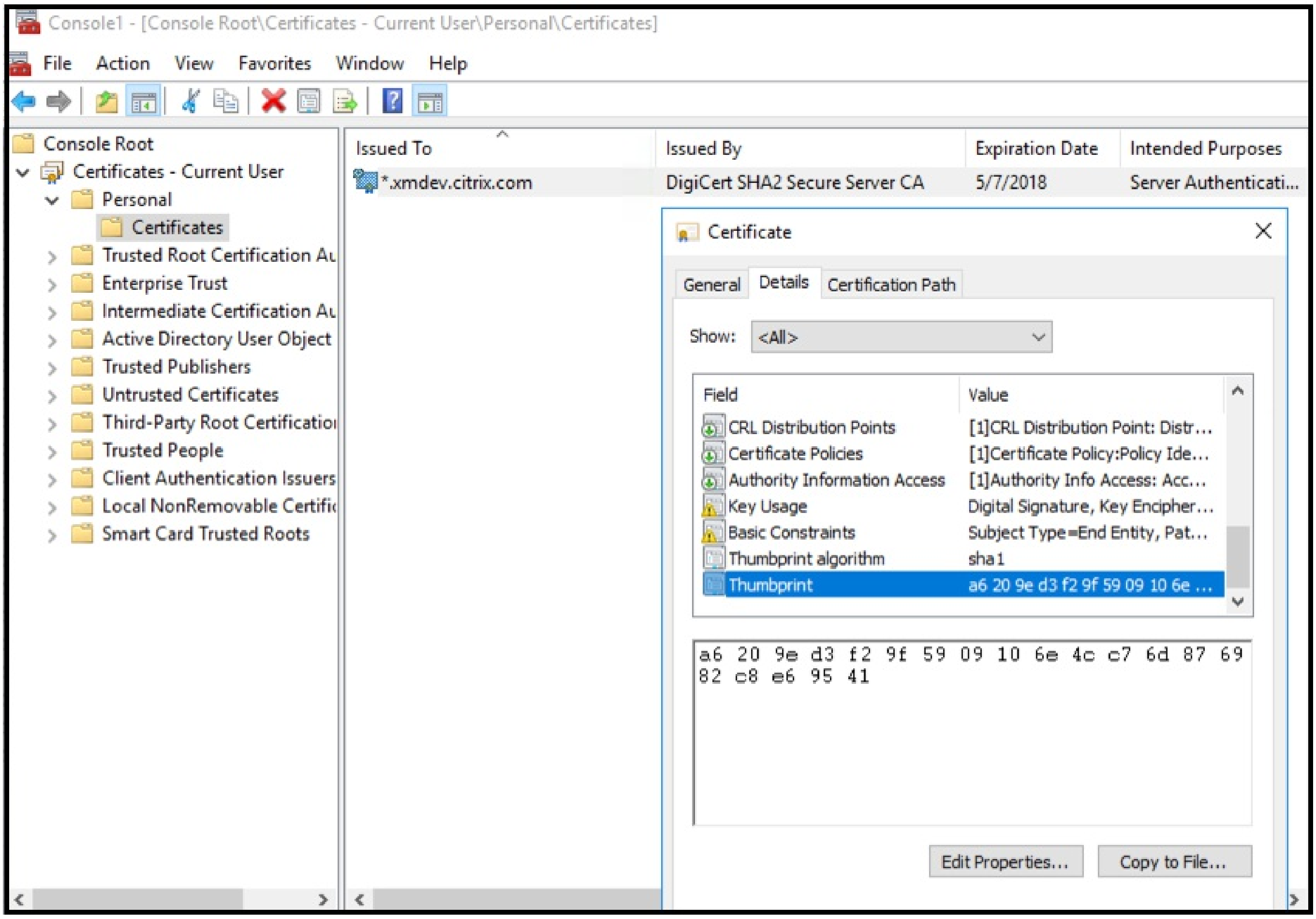
● My user account
○ Service account
○ Computer account

5. Select the certificate and click **OK**.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au

Issued To	Issued By	Expiration Date
*.xmdev.citrix.com	DigiCert SHA2 Secure Server CA	5/7/2018

6. Double-click on the certificate and select the **Details** tab. Scroll down to see the certificate thumbprint.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatio
Trusted People
Client Authentication Issuers
Local NonRemovable Certific
Smart Card Trusted Roots
Certificate
General
Details
Certification Path
Edit Properties...
Copy to File...

Issued To	Issued By	Expiration Date	Intended Purposes
*.xmdev.citrix.com	DigiCert SHA2 Secure Server CA	5/7/2018	Server Authenticati...

Show: <All>

Field	Value
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature, Key Encipher...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint algorithm	sha1
Thumbprint	a6 20 9e d3 f2 9f 59 09 10 6e ...

```
a6 20 9e d3 f2 9f 59 09 10 6e 4c c7 6d 87 69
82 c8 e6 95 41
```

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 certificates on the Windows server to install the signing and encryption:

$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.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:

```
mkdir .\TrustedTpm

expand -F:* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
```

Configure the DHA service

Run this command on the Windows server to configure the DHA service:

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint <ReplaceWithThumbprint>

-SigningCertificateThumbprint <ReplaceWithThumbprint>

-SslCertificateStoreName My -SslCertificateThumbprint <ReplaceWithThumbprint>

-SupportedAuthenticationSchema "AikCertificate"
```

Run these commands on the Windows server to set up the certificate chain policy for the DHA service:

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

Respond to these prompts, as follows:

```
Confirm

 Are you sure you want to perform this action?

 Performing the operation "Install-DeviceHealthAttestation" on target "WIN-N27D1FKCEBT".

 [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A

 Adding SSL binding to website 'Default Web Site'.

 Add SSL binding?
```

```
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

Add application pool?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Adding web application 'DeviceHealthAttestation' to website 'Default Web Site'.

Add web application?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Adding firewall rule 'Device Health Attestation Service' to allow inbound connections on port(s) '443'.

Add firewall rule?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Setting initial configuration for Device Health Attestation Service.

Set initial configuration?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Registering User Access Logging.

Register User Access Logging?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

Check the configuration

To check whether the DHASActiveSigningCertificate is active, run this command on the server:

```
Get-DHASActiveSigningCertificate
```

If the certificate is active, the certificate type (Signing) and thumbprint is displayed.

To check whether the DHASActiveSigningCertificate is active, run this command on the server:

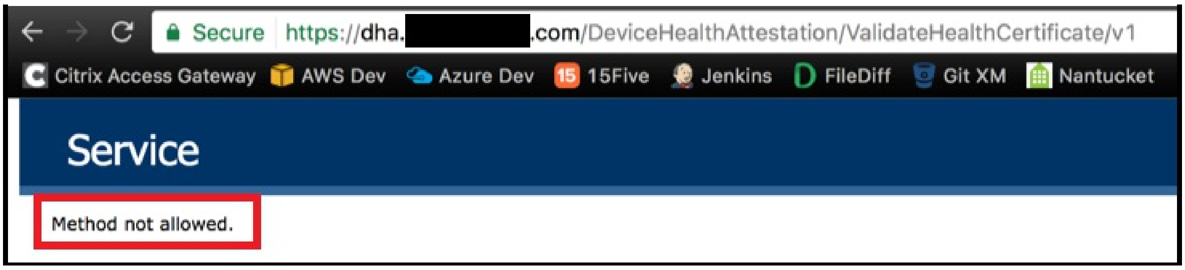
```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint" -Force

Get-DHASActiveEncryptionCertificate
```

If the certificate is active, the thumbprint is displayed.

To perform a final check, go to this URL:

```
https://dha.myserver.com/DeviceHeathAttestation/ValidateHealthCertificate/v1
```

If the DHA service is running, “Method not allowed” is displayed.



https://dha.[redacted].com/DeviceHealthAttestation/ValidateHealthCertificate/v1

Service

Method not allowed.

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

Vijay Kumar Kunchakuri , | Dec 05, 2017

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 XenMobile 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.

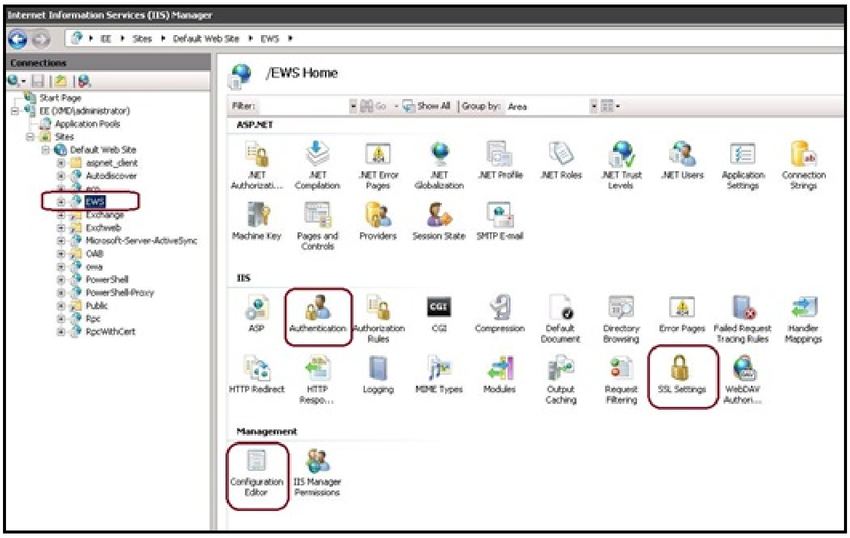
To get started with the configuration, do the following:

1. Log on to the server or servers where the EWS virtual directory is installed.

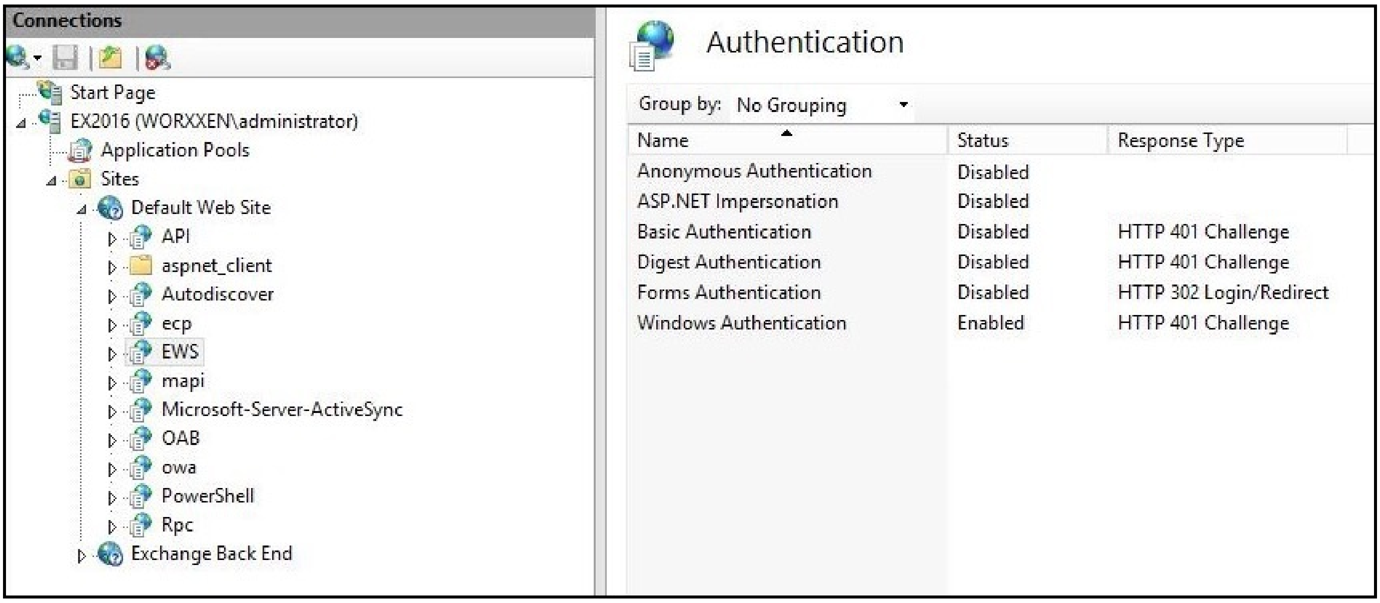
2. Open the IIS Manager Console.

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.



- Start Page
- EX2016 (WORXXEN\administrator)
  - Application Pools
  - Sites
    - Default Web Site
      - API
      - aspnet_client
      - Autodiscover
      - ecp
      - EWS
      - mapi
      - Microsoft-Server-ActiveSync
      - OAB
      - owa
      - PowerShell
      - Rpc
    - Exchange Back End

Authentication

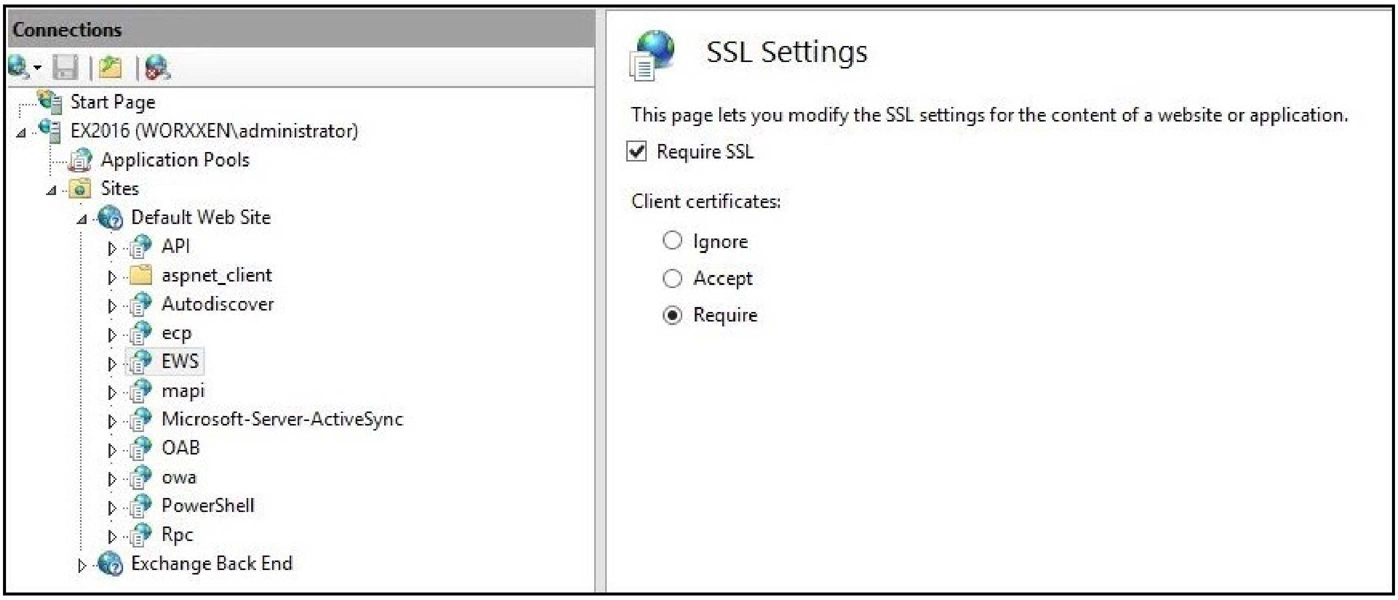
Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

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 username/password as credentials to authenticate and connect to the Exchange Server.



- Start Page
- EX2016 (WORXXEN\administrator)
  - Application Pools
  - Sites
    - Default Web Site
      - API
      - aspnet_client
      - Autodiscover
      - ecp
      - EWS
      - mapi
      - Microsoft-Server-ActiveSync
      - OAB
      - owa
      - PowerShell
      - Rpc
    - Exchange Back End

SSL Settings

This page lets you modify the SSL settings for the content of a website or application.

☑ Require SSL

Client certificates:

○ Ignore

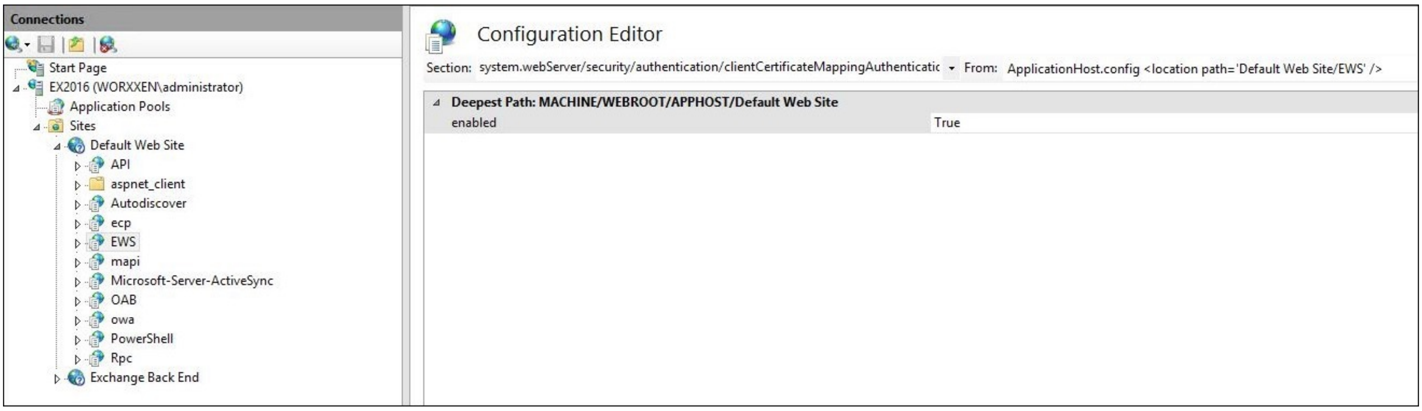
○ Accept

● Require

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**.



Section: system.webServer/security/authentication/clientCertificateMappingAuthenticatic From: ApplicationHost.config <location path='Default Web Site/EWS' />

Deepest Path: MACHINE/WEBROOT/APPHOST/Default Web Site

enabled	True

8. Click **Configuration Editor** and in the **Section** drop-down list, navigate to the following section:

system.webServer/serverRuntime

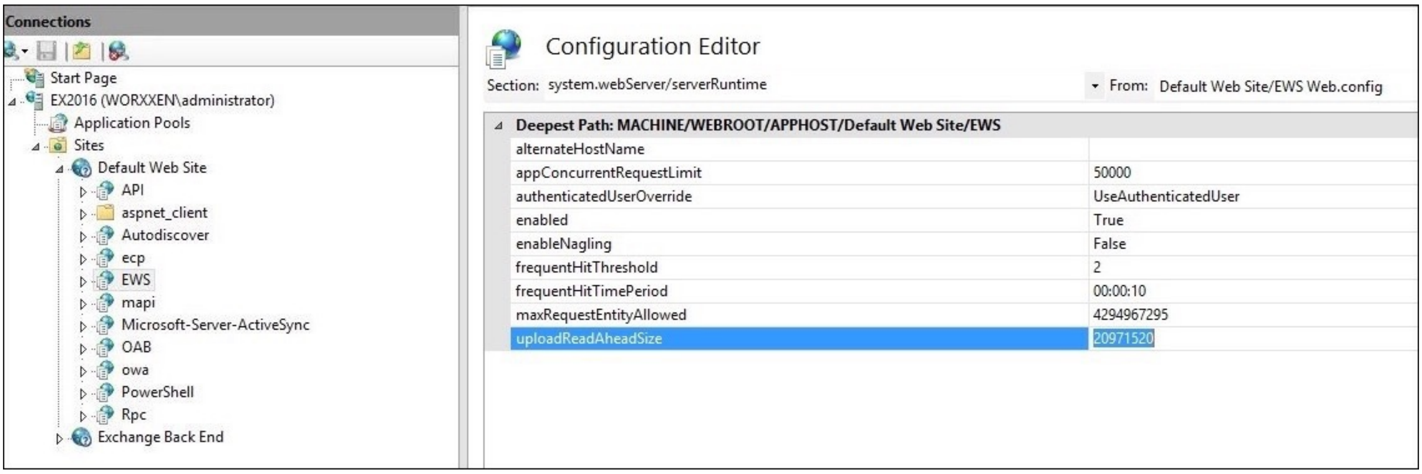
9. Set the **uploadReadAheadSize** value to **10485760** (10 MB) or **20971520** (20 MB) or to a value as required by your organization.

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.

Note: Do not set this value to **0**.

For more information, see the following third-party resources:

- Microsoft IIS server runtime
- Butsch Client Management Blog



Section: system.webServer/serverRuntime From: Default Web Site/EWS Web.config

Deepest Path: MACHINE/WEBROOT/APPHOST/Default Web Site/EWS

alternateHostName	
appConcurrentRequestLimit	50000
authenticatedUserOverride	UseAuthenticatedUser
enabled	True
enableNagling	False
frequentHitThreshold	2
frequentHitTimePeriod	00:00:10
maxRequestEntityAllowed	4294967295
uploadReadAheadSize	20971520

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