Fixed issues

Jan 18, 2017

> **Note**
>
> This PDF contains the entire set of product documentation for XenMobile Server 10.4. For product documentation on the current release, see XenMobile Server.

The following issues are fixed in XenMobile 10.4. Fixed Upgrade Tool issues appear under the heading "XenMobile Upgrade Tool 10.4" at the end of this article.

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

When you try to add a public app store app for Windows Phone, when you enter a URL from the Microsoft store, the upload fails. [CXM-13468]

For some configurations, after upgrading from XenMobile 9 to 10.3.6, devices that were previously enrolled in XenMobile 9 cannot open installed apps or download new apps from the WorxStore. Apps also disappear from Worx Home and users can't access the WorxStore. [CXM-13708]

When you create a WiFi device policy with a defined WiFi password that includes special characters, such as a less than symbol (<), greater than symbol (>) or an ampersand (&), users are prompted to enter their WiFi password. [CXM-13717]

When you try to upload an iOS enterprise app, an "icon not found" error appears when the icon size exceeds 1,000 KB. [CXM-13729]

If clustering is enabled and a device wipe is sent to a disconnected device, the device is wiped when it reconnects, as expected. However, if the device re-enrolls or connects to a different cluster node, XenMobile wipes the device again. [CXM-13793]

The shared devices enroller permission is enabled by default for the Admin RBAC role in XenMobile Service (cloud) deployments. As a result, all devices belonging to users with the Admin role enroll as shared devices. [CXM-15203]

When you configure client certificate authentication and the Require Server Name Indication option is enabled on the CA server, enrollment fails. [CXM-15312]

When searching for Google Play Store apps from the XenMobile console, the search does not return apps based on the Android operating system on the registered device. For examples, apps that require a minimum operating system of 4.4 do not appear in the results. [CXM-15653]

When you create a local user assigned to a local group and when the local user tries to enroll using a Windows 10 device, enrollment fails. [CXM-16895]

When you create a Citrix Launcher policy, users can enroll an Android device, but if you change a policy setting, they cannot exit Citrix with the password you set in the policy. As a workaround, you need to reinsert the password in the policy settings and update the policy. [CXM-17157]

When you disable the Enable ShareFile option in XenMobile, in Secure Mail for Android, users cannot access any attachment type. [CXM-17887]

When you update from XenMobile 10.3.6 with Rolling Patch 1 to XenMobile 10.4, license types of permanent expire with an error message. [CXM-17900]

When you update from XenMobile 10.3.6 to XenMobile 10.4, even though the license of permanent type is still valid, an expired license error message appears. [CXM-17987]

If you manually enter a URL for a Windows public store app and the URL is not from a U.S. store, the XenMobile console displays an error. When you use the U.S. store app URL, the upload is successful. [CXM-18013]

When users receive one-time password invitations for IMEI binding (username and password) and SMTP and SMS notifications, the first profile installs successfully and the second profile installation fails with the error message "Profile Installation Fails. A connection to the server could not be established." On iPhone 6 and iPhone 6 Plus devices, there is an IMEI number and MEID number and the one-time password binds to the MEID number instead of the IMEI number. You can replace the IMEI number with the iPhone's Unique Device Identifier (UDID) or use a regular phone number. [#606162]

Attempts to download a Certificate Signing Request (CSR) from Internet Explorer and Firefox web browsers fail with the error "The Webpage cannot be displayed." Downloading the CSR from the Chrome web browser works. [#609552]

If you log on to the XenMobile console, navigate to **Analyze > Reporting** and then click **Inactive Devices**, a blank page appears instead of downloading the file. [#609649]

The XenMobile NetScaler Connector doesn't obtain the Samsung 5.x devices from a sync with ActiveSync. [#613522]

When you create a WiFi device policy for Android with an authentication type of 802.1x EAP, the Password field is no longer mandatory. [#614932]

This fix addresses a security vulnerability. For more information, see security bulletin http://support.citrix.com/article/CTX207824.
Note: For this security fix to work, a second reboot of the XenMobile server is required for the fix to take effect. [#624347]

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

Windows Phone enrollment sometimes fails to start Worx Home. [#633884]

Disabled HDX apps do not enumerate in the Worx Store. [#634110]

The XenMobile server shows incorrect user data in the log file. [#636754]

After updating from XenMobile 10.3.1 to 10.3.6, the file type and destination folder in the Files policy properties doesn't display correctly in the XenMobile console. [#640334]

VPP token max length text box is 256 characters. [#640692]

Windows Phone users can't enroll a device with a sAMAccount. [#640847]

After removing enrolled users from the ShareFile control subsystem, the enrolled users might appear in the user audit log file

of the XenMobile console. [#641342]

After upgrading from XenMobile Server 10.1 to 10.3.x, clicking https://<enroll.FQDN>/zdm/enrollmdm.html, the iOS platform is not listed as a platform selection. [#641771]

When you enroll a Worx Home for iOS device, the MDM enrollment might be successful but MAM registration fails. [#644892]

Deletion of nested groups is never reflected. [#647557]

If **Manage > Enrollment** has more than 2,000 entries, after you click **Export** the page goes blank and the report isn't generated. [#647855]

XenMobile administrators attempting to access the XenMobile console might be directed to the XenMobile Self-Help portal instead. This can happen when XenMobile administrator groups are created with role-based control access and a group is moved from one Active Directory OU to another. [#647987]

Uploading iOS app fails with error - Uploaded mobile app is invalid. Application icon was not found.[#649574]

XenMobile server might become unresponsive with an Out of Memory error. [#650490]

Device wipe issues because of clustered messaging. [#650555]

When configuring a VPN device policy, you can't specify a port number. [#650972]

After upgrading XenMobile server with clustering enabled, several deadlocks might occur. The server might become unresponsive. [#651122]

The XenMobile console doesn't include Serial Number details while prompting you to confirm device deletion. [#651185]

SSO Account Policy on XenMobile server 10.3.6 does not work as expected. Users keep getting prompted for password. [#651860]

Cannot disable iPad app association on XenMobile 10.3.6 for VPP applications.[#652280]

If you delete a delivery group from a device policy, XenMobile doesn't save the change and the delivery group remains assigned to the policy. [#652321]

SSO account unable to save short FQDN. [#652704]

When a user removes Device Admin rights from their Android device, XenMobile changes the state of both MDX and MAM enrolled devices to "Orange/unmanaged" and the user doesn't have access to any MDX apps. The MAM state should remain as "Green/managed". [#655180]

XenMobile Upgrade Tool 10.4

If the device setting in XenMobile 9.0 for maximum or minimum operating system is set to 10 or above and for excluded devices for MDX and enterprise apps, after upgrading, the rule does not migrate properly. Apps that should appear do not and apps that should not appear do. [#603412]

If Microsoft SQL server is configured as case-sensitive, an upgrade fails if the table "Id_Generator" is specified as "id_generator". [#623300]

After upgrading from XenMobile 9 to XenMobile 10, the Personal Hotspot policy value type is Boolean instead of string.

[#633337]

If an Active Directory group name contains the "@" character, an upgrade fails. [#633718]

If your Device Manager 9.0 server is set up using Local PostgreSQL and you use localhost as a reference for the database server, an upgrade will fail. To work around this, edit ew-config.properties on the Device Manager 9.0 server and replace all localhost references with the IP address of the Device Manager database server, then continue with the Upgrade pre-requisites. [#635023]

In XenMobile 9.0, when you define the **Users organizational unit** (OU) in the LDAP connection parameters, after you upgrade to XenMobile 10, the full root context is not appended to users organizational unit. For example, OU=MDMUsers, OU=SALES should be OU=MDMUsers, OU=SALES, DC=citrite, DC=com. As a result, you need to make the update manually in XenMobile 10. [#635981]

During an upgrade, when uploading the support bundle, the error "MAM set up failed, see the logs for details" appears and the Upgrade Tool retains corrupted MAM data. [#638062]

If an Active Directory group name contains the "." character, a role migrated as a delivery group loses its group association. [#647590]

If the web proxy setting in App Controller includes the "\" character, XenMobile 10.1 server can't start and the message "Starting main app..." appears as the server continues to reboot. [#647919]

After an upgrade from XenMobile 9 to XenMobile 10, paid VPP apps do not install from the XenMobile (Worx) Store unless the app configuration requires installation. [#668102]

In a cross-domain authentication configuration, after an upgrade to XenMobile 10.3.6, devices that were previously enrolled in XenMobile 9 can't open installed apps or download new apps from the Worx (XenMobile) Store or access the Store. [CXM-13708]

After an upgrade from XenMobile 9 to XenMobile 10, installed public store apps appear as unsubscribed in the XenMobile (Worx) Store. [CXM-17936]

If the database connection URL is localhost, you no longer must modify ew-config.properties.

If you have RBAC roles configured with access restricted to LDAP and Active Directory or any child, after upgrading, when you log on to the XenMobile console as an administrator, the same settings are not selected.

Known issues

Nov 03, 2016

The following are known issues in XenMobile 10.4.

When you configure Citrix Launcher, the **Just Once** option does not work. You must click the **Always** option. [CXM-13413]

Occasionally, when users reenroll an Android device, a selective wipe occurs unexpectedly. [CXM-13716]

When you configured public apps in the XenMobile console, after updating to XenMobile 10.4, when you deploy Secure Hub to a Windows 10 tablet, users cannot view the public apps. [CXM-16516]

With Citrix Launcher, in MDM mode, when users open the XenMobile Store, the store opens in a default browser even if you listed a different browser on a white list. [CXM-17097]

Citrix Launcher can't download logo and background images from a server that has a self-signed certificate. [CXM-17159]

When using the XenMobile console with an Internet Explore 11 browser, you cannot add a new LDAP configuration. [CXM-18324]

XenMobile Upgrade Tool 10.4

Data and policy issues

After upgrading, syslog server configuration data is not migrated to the XenMobile server. [#558539]

Some Restriction policy configurations were deprecated in 10.1. Therefore, XenMobile 10.4 fails to deploy the entire Restriction policy successfully to Windows 10 phones after you upgrade from XenMobile 9 to XenMobile 10.4. If you view and save the policy settings in XenMobile 10.4, however, the policy deploys successfully. [#608541]

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

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]

Google Play apps

If you include a public Google Play app for Android devices with a default icon, after migrating, the default icon does not appear in the XenMobile console. You must either edit and save the app or click Check for Updates in order for the image to appear. [#557996]

SQL Server

If you use a PostgreSQL database, MAM devices are unable to re-enroll after an upgrade. To work around this issue, delete the device entries from XenMobile and send enrollment notifications to the users. [#632831]

RBAC

Issues with RBAC settings occur after upgrading:

- If you have configured a super administrator role, all permissions are selected by default. After upgrading, only three

permissions are selected - RBAC, Enrollment, and Release Management.

- If you have created a custom super administrator role, all support permissions should be selected by default. After upgrading, none of the support permission settings is selected. To work around this issue, create the support permission after upgrading. [#569350, #569395, #569423]

Citrix Secure Hub and Citrix Store

Before upgrading from XenMobile 9 to XenMobile 10.4, if your WorxStore has a custom name, issues occur with enrollment, access to Worx Home and access to the Worx Store. As a workaround, change the store to the default setting of **Store** before upgrading. For details on the prerequisite workaround, see Upgrade Tool prerequisites. [#619458]

Users with MAM-only devices are unable to authenticate to Citrix Secure Hub after an upgrade from XenMobile 9.0 to XenMobile 10.4 followed by setting the LDAP option **User search by** to **sAMAccountName**. [#628233]

Android for Work

After an upgrade, SAML login for Android for Work fails because the SAML certificate has a .pem extension, which the XenMobile server won't import. [#631795]

To work around this issue, make sure XenMobile has the correct SAML certificate, as follows:

1. Export from XenMobile 9 App Controller the SAML certificate with a private key (AppController.example.com). That certificate is in PEM format and has a .pem extension.

2. Use the openssl command to generate a PFX file from the PEM file:

openssl pkcs12 -export -out certificate.pfx -in certificate.pem

3. Imported the PFX file into XenMobile 10.3 as a SAML keystore.

4. Export the SAML certificate without the private key from XenMobile 10.4 and then upload it to Android for Work domain.

Architecture

Oct 19, 2016

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, you want to give users in your organization remote access to mobile apps and you need to track the device types with which users connect. In this scenario, you would 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 to access 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 some or all of these capabilities, 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 XenMobile, StoreFront, or the Web Interface so that you can set up communication with it.
- 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, such as XenMobile Apps. 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 supports an integrated solution that provides device management, as well as 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, as well as server redundancy purposes. Also, leveraging the NetScaler SSL Offload capability can further reduce the load on the XenMobile server and increase throughput. For more information about how to setup clustering for XenMobile 10.x by configuring two load balancing virtual IP addresses on NetScaler, see Clustering.

For more information about how to configure XenMobile 10 Enterprise Edition for a disaster recovery deployment including an architectural diagram, see the Disaster Recovery Guide for XenMobile.

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.

Mobile device management (MDM) mode

XenMobile MDM Edition provides mobile device management for iOS, Android, Amazon, and Windows Phone (see Supported Device Platforms in XenMobile). You deploy XenMobile in MDM mode 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.

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

Mobile app management (MAM) mode

MAM supports iOS and Android devices, but not Windows Phone devices (see Supported Device Platforms in XenMobile). You deploy XenMobile in MAM mode (also referred to as MAM-only mode) 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.

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

MDM+MAM mode

Using the MDM and MAM modes together provides mobile app and data management as well as mobile device management for iOS, Android, and Windows Phone (see Supported Device Platforms in XenMobile). You deploy XenMobile in ENT (enterprise) mode 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.

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

XenMobile in the internal network - Another deployment option is to position the 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. With this deployment, because the XenMobile server is not in the DMZ, you do not need to open up ports on the internal firewall to allow access to SQL Server and PKI servers from the DMZ.

System requirements and compatibility in XenMobile 10.4

Mar 29, 2017

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

- XenMobile Compatibility
- Supported Device Platforms
- Port requirements
- Scalability
- Licensing
- FIPS 140-2 compliance
- Language support

For system requirements and compatibility in the most recent version of XenMobile Server, see System requirements and compatability.

To run XenMobile 10.4, you need the following minimum system requirements:

- One of the following:
  - XenServer (supported versions: 6.5.x or 7.0); for details, refer to XenServer
  - VMware (supported versions: ESXi 5.5, or ESXi 6.0); for details, refer to VMware
  - Hyper-V (supported versions: Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2); for details, refer to Hyper-V
- Dual core processor
- Four virtual CPUs
- 8 GB of RAM
- 50 GB disk space

XenMobile version 10.4.x requires the 11.12.1 Citrix License Server or later.

NetScaler Gateway System Requirements

To run NetScaler Gateway with XenMobile 10.4, you need the following minimum system requirements:

- 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 disk space

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

XenMobile 10.4 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 10.4 supports SQL AlwaysOn Availability Groups and SQL Clustering for database high availability.

  Citrix recommends using Microsoft SQL remotely.

  Note: Make sure 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, select your server version from the **Other Versions** list):

  Server Configuration - Service Accounts

  Configure Windows Service Accounts and Permissions

  Server-Level Roles

- PostgreSQL

  PostgreSQL is included with XenMobile. You can use it locally or remotely.

  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 3.6
StoreFront 3.5
StoreFront 3.0
StoreFront 2.6
Web Interface 5.4
XenApp and XenDesktop 7.9
XenApp and XenDesktop 7.8
XenApp and XenDesktop 7.7
XenApp and XenDesktop 7.6
XenApp and XenDesktop 7.5
XenApp 6.5

XenMobile 10.4 Mail Server Requirements

XenMobile 10.4 supports the following mail servers:

- Exchange 2016
- Exchange 2013
- Exchange 2010

Port requirements

Jan 10, 2017

To enable devices and apps to communicate with XenMobile, you need to open specific ports in your firewalls. The following tables list the ports that must be open.

Opening Ports for NetScaler Gateway and XenMobile to Manage Apps

You must open the following ports to allow user connections from Citrix Secure Hub, Citrix Receiver, and the NetScaler Gateway Plug-in through NetScaler Gateway to XenMobile, StoreFront, XenDesktop, the XenMobile NetScaler Connector, and to other internal network resources, such as intranet websites. For more information about NetScaler Gateway, see Configuration Settings for your XenMobile Environment in the NetScaler Gateway documentation. For more information about NetScaler-owned IP address, such as the NetScaler IP (NSIP) virtual server IP (VIP), and subnet IP (SNIP) addresses, see How a NetScaler Communicates with Clients and Servers in the NetScaler documentation.

TCP port	Description	Source	Destination
21 or 22	Used to send support bundles to an FTP or SCP server.	XenMobile	FTP or SCP server
53 (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 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 and	Used for Network Time Protocol (NTP) services.	NetScaler Gateway XenMobile	NTP server

UDP)			
389	Used for insecure LDAP connections.	NetScaler Gateway XenMobile	LDAP authentication server or Microsoft Active Directory
443	Used for connections to StoreFront from Citrix Receiver or Receiver for Web to XenApp and XenDesktop.	Internet	NetScaler Gateway
	Used for connections to XenMobile for web, mobile, and SaaS app delivery.	Internet	NetScaler Gateway
	Used for general device communication to XenMobile server	XenMobile	XenMobile
	Used for connections from mobile devices to XenMobile for enrollment.	Internet	XenMobile
	Used for connections from XenMobile to XenMobile NetScaler Connector.	XenMobile	XenMobile NetScaler Connector
	Used for connections from XenMobile NetScaler Connector to XenMobile.	XenMobile NetScaler Connector	XenMobile
	Used for Callback URL in deployments without certificate authentication.	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 Connector.	NetScaler	XenMobile NetScaler Connector
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.	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.	Access point (browser)	XenMobile
	Used for downloading logs and support bundles for all XenMobile cluster nodes from one node.	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

Opening XenMobile Ports to Manage Devices

You must 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 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 Google Play (play.google.com)
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.	Internet	XenMobile
	Used for enrollment and agent setup for Android and Windows devices, the XenMobile web console, and MDM Remote Support Client.	Internal LAN and WiFi	
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 WiFi 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	Internet, for app tunnels to user devices (Android and Windows only)
8443	Used for enrollment of iOS and Windows Phone devices.	Internet LAN and WiFi	XenMobile

Port Requirement for Auto Discovery Service Connectivity

This port configuration ensures that Android devices connecting from Secure Hub for Android, versions 10.2 and 10.3, 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 work with your proxy server. In this scenario, allow the ADS connection to bypass the proxy server.

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

- **Collect XenMobile Server and NetScaler certificates**. The certificates need to 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.

New certificate pinning improvements require that devices connect to ADS before the device enrolls. This ensures that the latest security information is available to Secure Hub for the environment in which the device is enrolling. Secure Hub will not enroll a device that cannot 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 10.2 for Android, open port 443 for the following FQDN and IP addresses:

FQDN	IP address

	54.225.219.53
	54.243.185.79
	107.22.184.230
	107.20.173.245
discovery.mdm.zenprise.com	184.72.219.144
	184.73.241.73
	54.243.233.48
	204.236.239.233
	107.20.198.193

Scalability and performance

Jun 26, 2017

> **Note**
>
> For the most recent XenMobile scalability and performance guidelines, see Scalability and performance.

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 10.4 enterprise deployments.

Scalability is defined here in terms of the ability of existing devices – that is, 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 60,000 devices. The tests comprised mobile device using known workloads.

All testing was done on XenMobile Enterprise edition.

Testing was done using the NetScaler Gateway 7500 (for deployments of up to 10,000 devices) and NetScaler Gateway 5550 (for deployments of more than 10,000 devices). 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 60,000 devices**	
Login rate	Reconnection rate of existing users	Up to 7,500 devices per hour
Configuration	NetScaler Gateway	MPX 7500, MPX 5550
	XenMobile Enterprise Edition	XenMobile Server 5-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	10,000	30,000	45,000	60,000
Reconnection rate of existing devices per hour	833	3,750	5,625	7,500
XenMobile server – mode	Standalone	Cluster	Cluster	Cluster
XenMobile server – cluster	N/A	3	4	5
XenMobile server – virtual appliance	Memory = 12 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 = 8 GB RAM vCPUs = 4	Memory = 16 GB RAM vCPUs = 4	Memory = 16 GB RAM vCPUs = 4	Memory = 16 GB RAM vCPUs = 4
Microsoft SQL Server external database	Memory = 32 GB RAM vCPUs = 16	Memory = 32 GB RAM vCPUs = 12	Memory = 48 GB RAM vCPUs = 4 with 4 cores each	Memory = 48 GB RAM vCPUs = 4 with 4 cores each

For deployments of 45,000 devices, the SQL Server was tuned to increase the number of worker threads to 2,000. For deployments of 60,000 devices, the SQL Server was tuned to increase the number of worker threads to 3,000. (For information about setting the number of worker threads on the SQL Server, refer to the Microsoft article, Configure the max worker threads Server Configuration Option.)

Scalability profile

These tables summarizes 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 & 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 the XenMobile server nodes are subject to higher than normal load conditions because the reconnecting devices obtain all entitled security policies. 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, refer to "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 10,000 devices simultaneously.

Licensing

Oct 05, 2016

XenMobile and NetScaler Gateway require licenses. For a data sheet that shows which XenMobile features are available in each edition, see this PDF.

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, 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.

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**
>
> XenMobile version 10.4.x requires the 11.12.1 Citrix License Server or later; older license server versions do not work with XenMobile 10.4.x.

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

Citrix recommends that you retain local copies of all license files you receive. When you save a backup 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 will need the original license files.

XenMobile licensing considerations

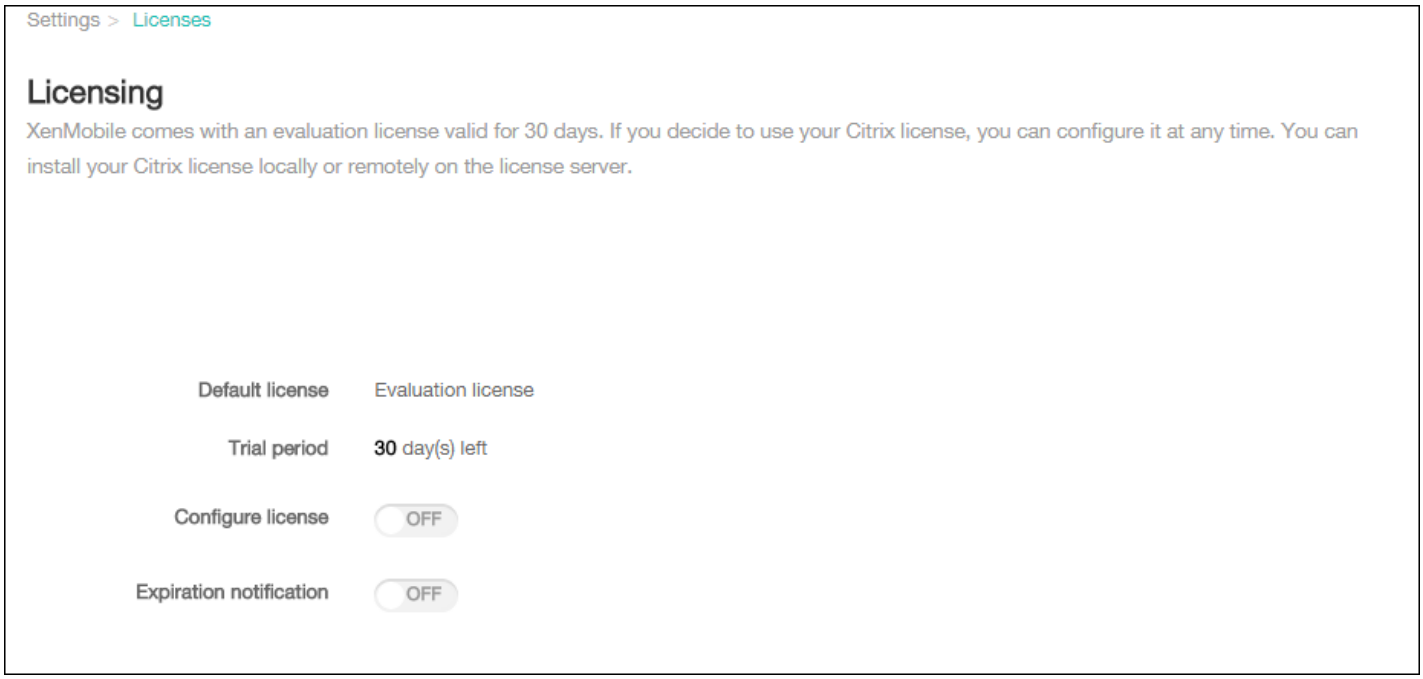
In the absence of a license, XenMobile operates fully featured in trial mode for a grace period of 30 days. This trial mode can be used only one time, with the 30-day period beginning when you install XenMobile. Access to the XenMobile web console is never blocked, regardless of whether a valid XenMobile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



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, such as device, these licenses are shown 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.

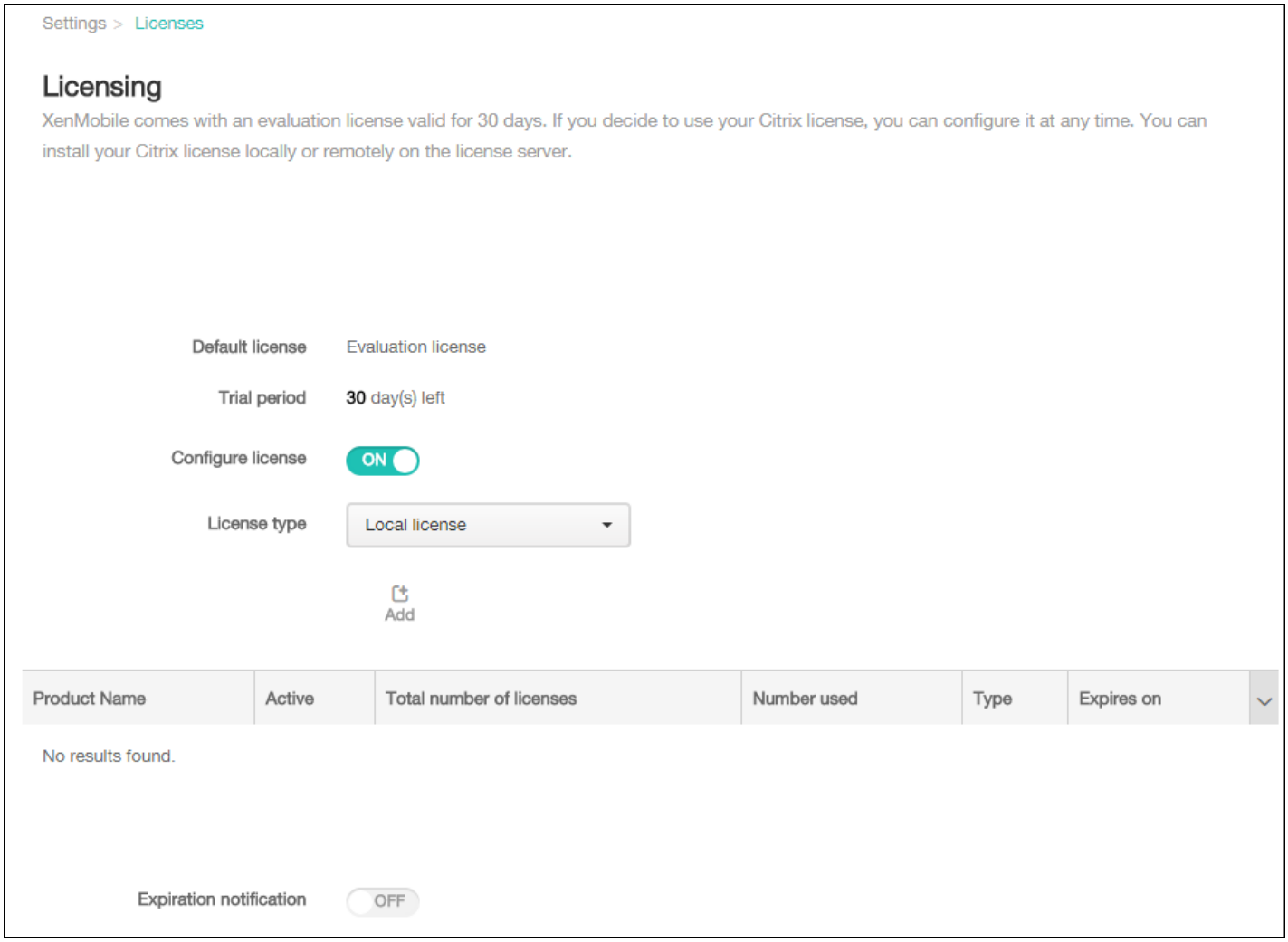
You manage all local licenses through the XenMobile console.

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.

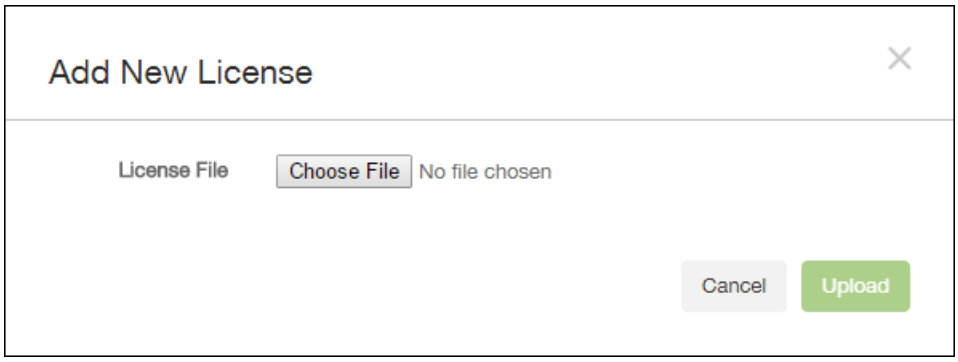
2. On the XenMobile console, click the gear icon in the upper right-hand corner. The **Settings** page appears.

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.

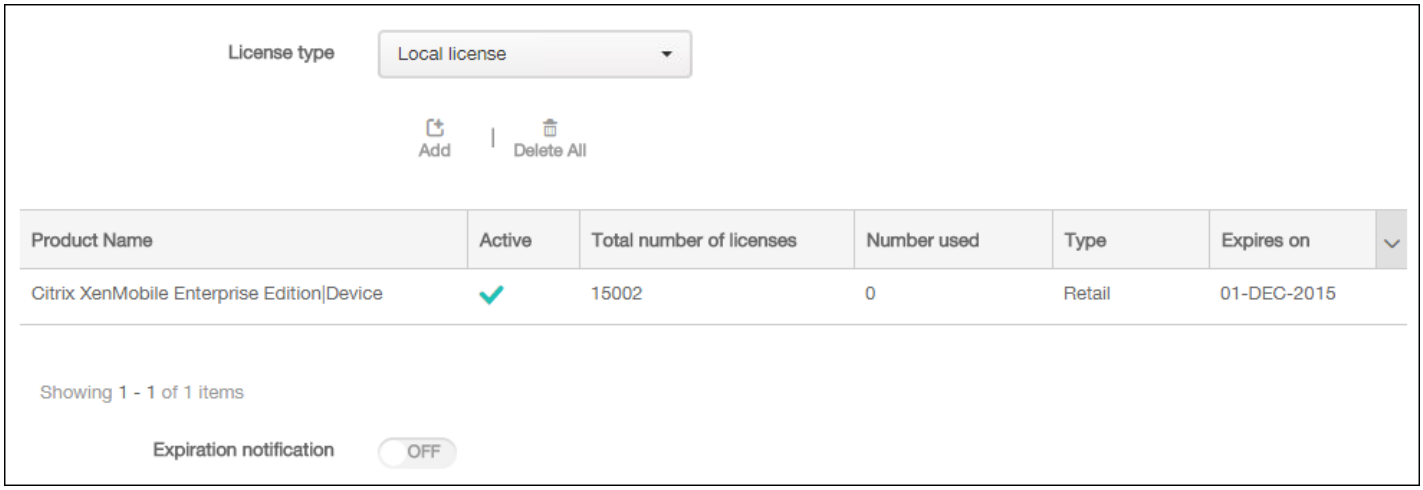


5. Ensure that **License type** is set to **Local license** and then click **Add**. The **Add New License** dialog box appears.



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

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



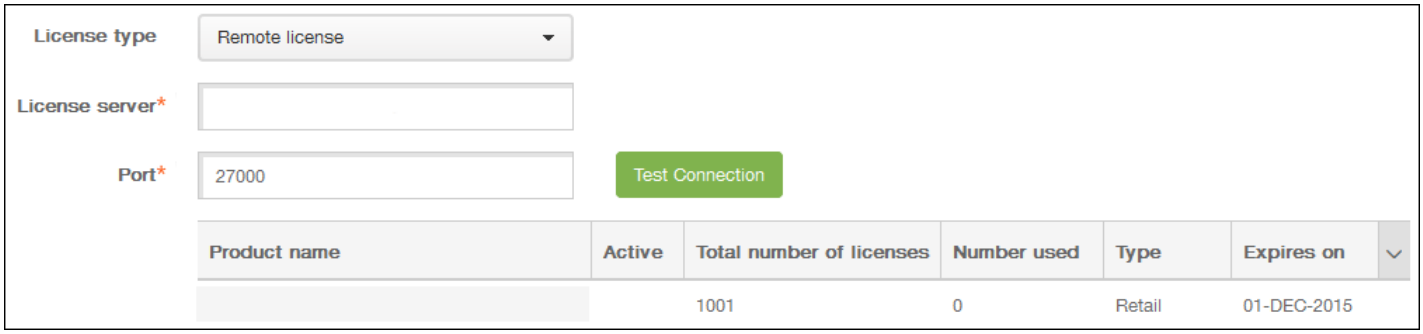
8. When the license appears in the table on the **Licensing** page, activate it. If this is the first license in the table, the license is activated automatically.

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. 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.

3. Set **License type** to **Remote license**. The **Add** button is replaced by the **License server** and **Port** fields and the **Test Connection** button.



4. 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.

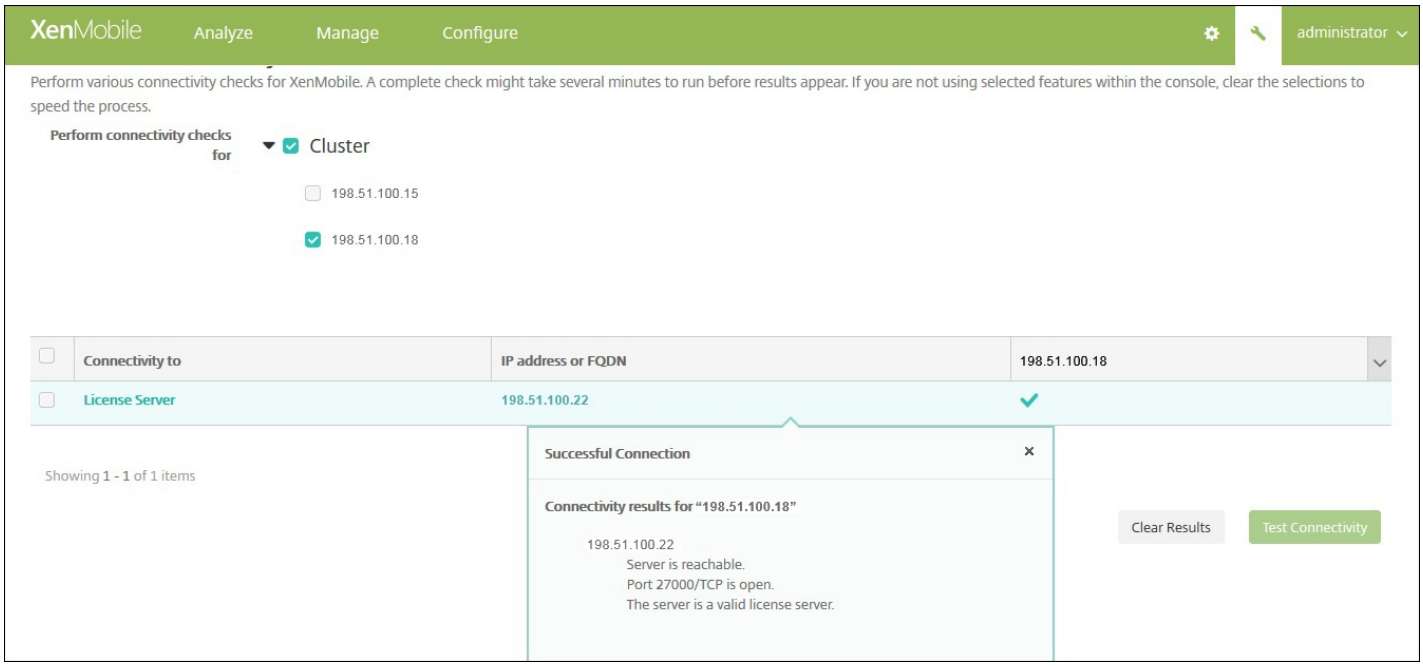
5. Click **Test Connection**. If the connection is successful, XenMobile connects with the Licensing server and the Licensing table is filled with available licenses. If there is only one license, it is activated automatically.

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.

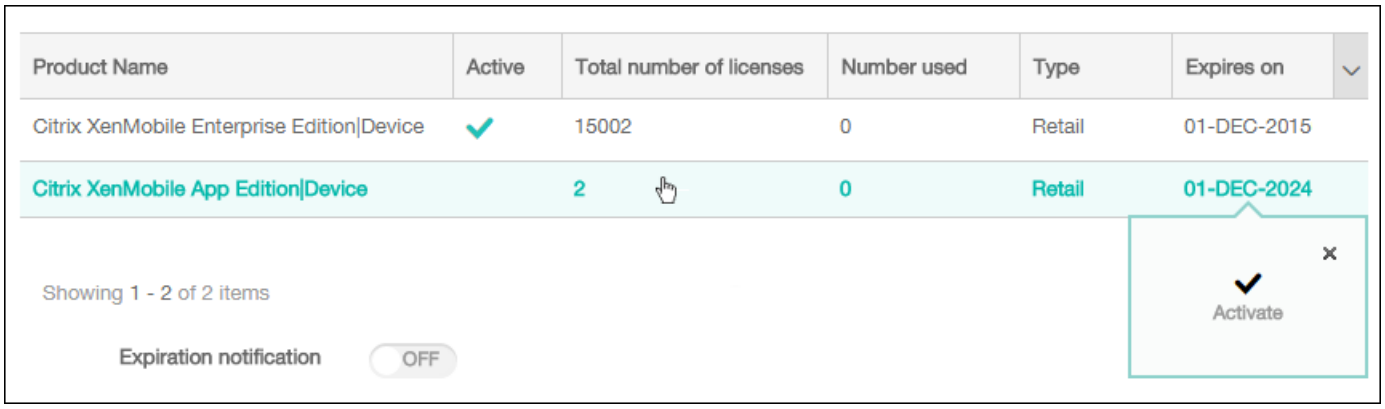
If the connection is unsuccessful, review the displayed error message, make the necessary corrections, and then click **Test Connection**.



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.



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

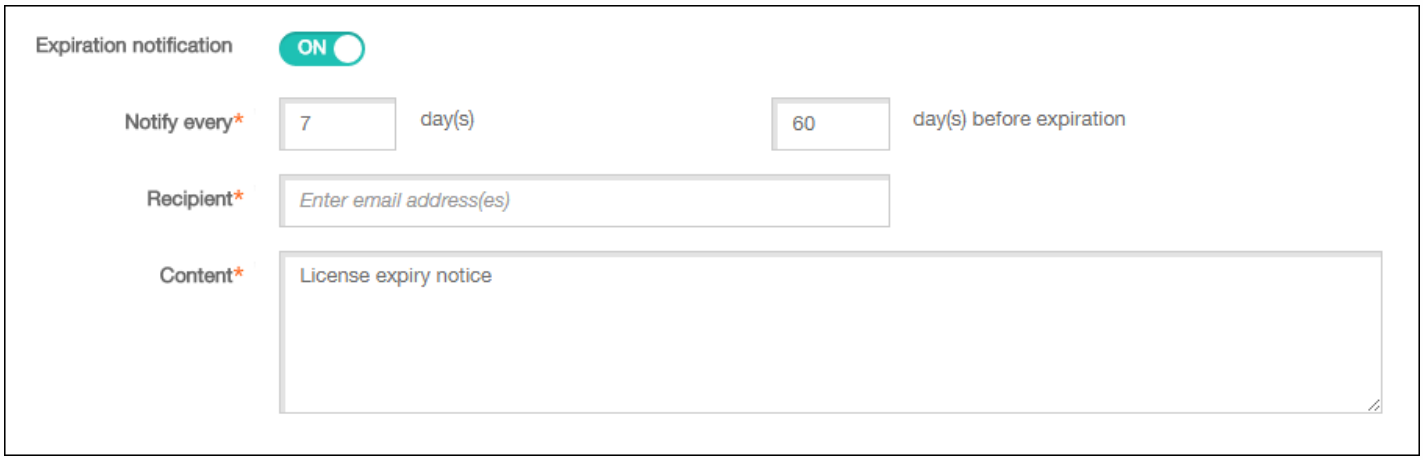
3. Click **Activate**. The selected license is activated.

> **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 automatically 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.



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**. At the number of days before expiration you set, XenMobile begins sending email messages containing the text you entered in **Content** to the recipient you entered in **Recipient**. The notifications are sent with the frequency you set.

FIPS 140-2 compliance

Feb 01, 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 Windows RT, Microsoft Surface, Windows 8 Pro, and Windows Phone 8 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 8.1 and use cryptographic libraries and APIs that are FIPS-compliant on Windows Phone 8. All data-at-rest for MDX apps on Windows Phone 8.1 and all data-in-transit between the Windows Phone 8.1 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

Feb 22, 2017

XenMobile Apps and the XenMobile console are adapted for use in languages other than English. This includes support for non-English characters and keyboard input even when the app is not localized in the users' preferred language. For more information about globalization support for all Citrix products, see http://support.citrix.com/article/CTX119253.

This articles lists the supported languages in XenMobile 10.4.

XenMobile console and the Self Help Portal

- French
- German
- Korean
- Portuguese
- Simplified Chinese

XenMobile Apps

An X indicates that the app is available in that particular language. Secure Forms currently is 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 renamed as well. 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	iOS only
Russian	X	X	X	X	X	X

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 in XenMobile 10.4

Mar 29, 2017

For installation information in the most recent version of XenMobile Server, see Install and configure.

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 end-to-end XenMobile environment, see the XenMobile Deployment Handbook.

For installation steps, see the Installing 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 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 of the IP addresses 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 user 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. If you need to configure multiple virtual servers, note all of the 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 when they	NetScaler Gateway	

	connect with Secure Hub or the NetScaler Gateway Plug-in when split tunneling is set to On.		
	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

You need to open ports to allow communication with the XenMobile components.

	Prerequisite	Component	Notes
	Open ports for XenMobile	XenMobile NetScaler Gateway	

Database

You need to configure a database connection. The XenMobile repository requires a Microsoft SQL Server database running

on one of the following supported versions: Microsoft SQL Server 2014, SQL Server 2012, SQL Server 2008 R2, or SQL Server 2008. Citrix recommends using Microsoft SQL remotely. PostgreSQL is included with XenMobile and should be used locally or remotely only in test environments.

•	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. This is the directory level under which users are located; for example, cn=users,dc=ace,dc=com. NetScaler Gateway and XenMobile use this to query Active Directory.	XenMobile NetScaler Gateway	
	Note the Group Base DN. This is the directory level under which groups are located. NetScaler Gateway and XenMobile use this 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 to connect to Windows-based applications and virtual desktops in XenApp and XenDesktop. Citrix recommends that you use the Quick Configuration wizard in NetScaler to configure these settings as well.

	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	

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.

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 set of prerequisites, as discussed in Configuring FIPs.

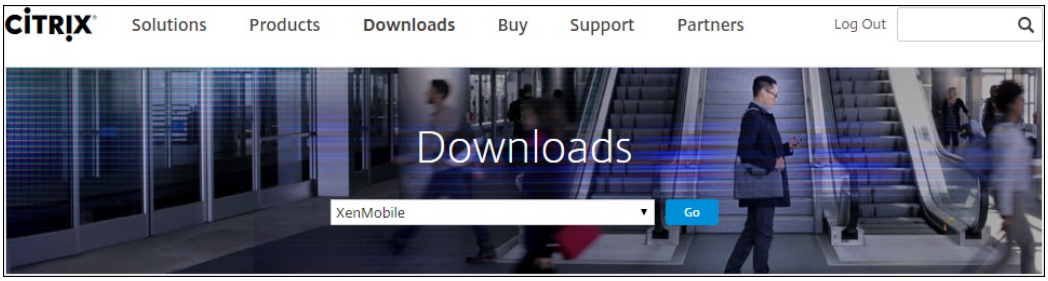
Download XenMobile product software

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 10.
7. Click XenMobile 10.0 Server.
8. On the XenMobile 10.0 Server edition page, click Download next to the appropriate virtual image to use to install XenMobile on XenServer, VMware, or Hyper-V.
9. 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

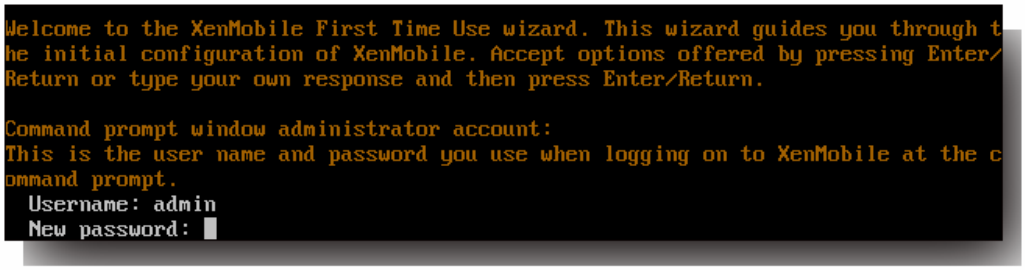
Configuring XenMobile for the first time is a two-part process.

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.
2. Log on to the XenMobile management console and follow the steps in the initial logon screens.

> **Note**
>
> When you use a vSphere web client, it is recommended that you do not 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.

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's 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 8 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, !, #, $, %)

   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)

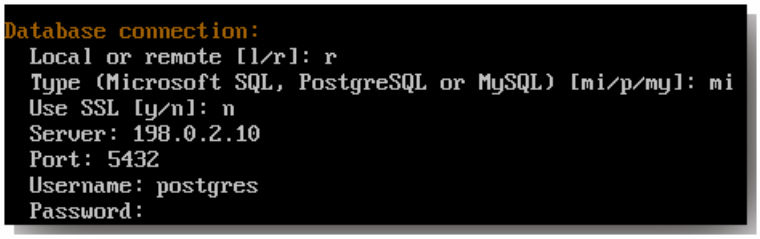
Note: The addresses shown in this and following images are non-working and are provided as examples only.

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 additional servers, you should provide your own passphrase. There is no way to view the passphrase if you selected a random passphrase.

6. Optionally, enable Federal Information Processing Standard (FIPS). For details about FIPS, see FIPS. Also, be sure to complete a set of prerequisites, as discussed in Configuring FIPs.

7. Provide the following information to configure the database connection.



   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.

```
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
.
```

Important: If you enable a XenMobile cluster, after system configuration is complete, be sure to open port 80 to enable real time communication between cluster members. This must be completed 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, re-enter the new password to confirm it.

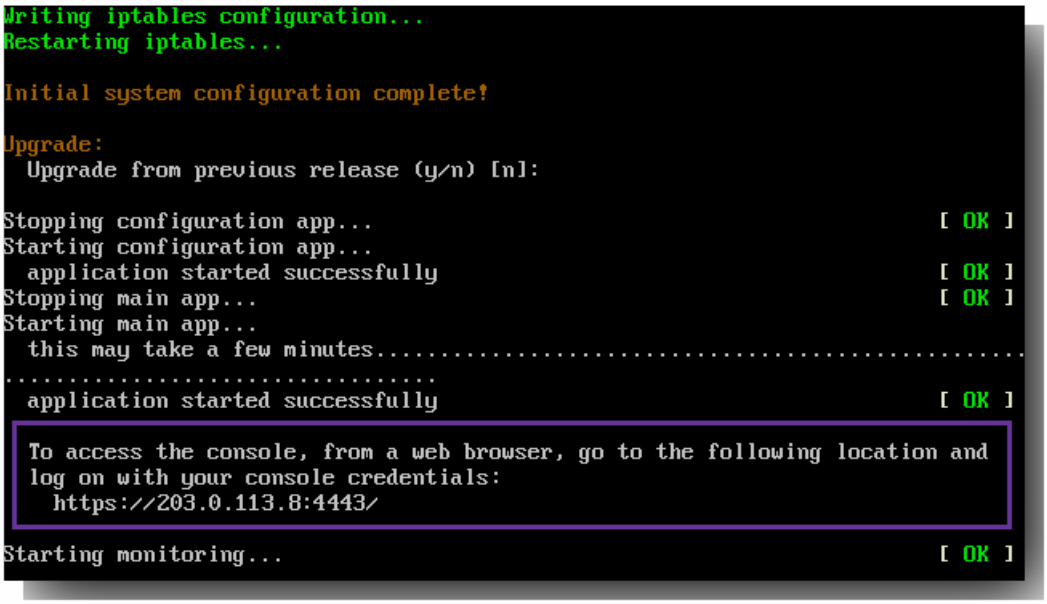
Note: No characters, such as asterisks, are shown when you type the new password. Nothing appears.

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.

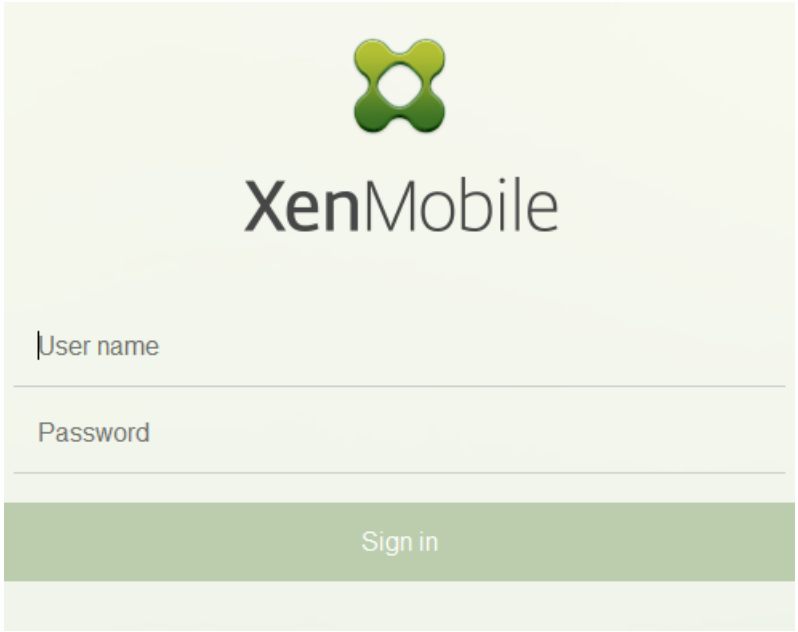


Configure XenMobile in a web browser

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 need to 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 organization's internal network (or intranet) to provide a secure single point of access to the servers, applications, 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

Oct 05, 2016

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 the Importing Certificates section later in this article.

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 Internet Information Services (IIS) 8.5.

> **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.

Configure clustering

Feb 08, 2017

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 fully qualified domain name (FQDN) of the MDM load balancing virtual IP address and the MAM load balancing virtual IP addresses are the same as the enrollment FQDN, which is the FQDN of the XenMobile server.
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.
- One public IP address for MDM load balancer.
- One private IP address, in a range defined by RFC 1918, for MAM load balancer.
- Server certificates.
- One free IP for NetScaler Gateway virtual IP address.

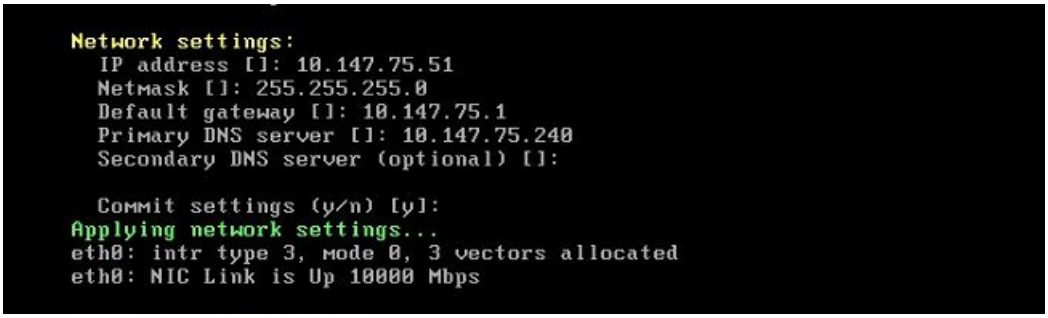
For reference architectural diagrams for XenMobile 10.x in clustered configurations, see Architecture.

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.

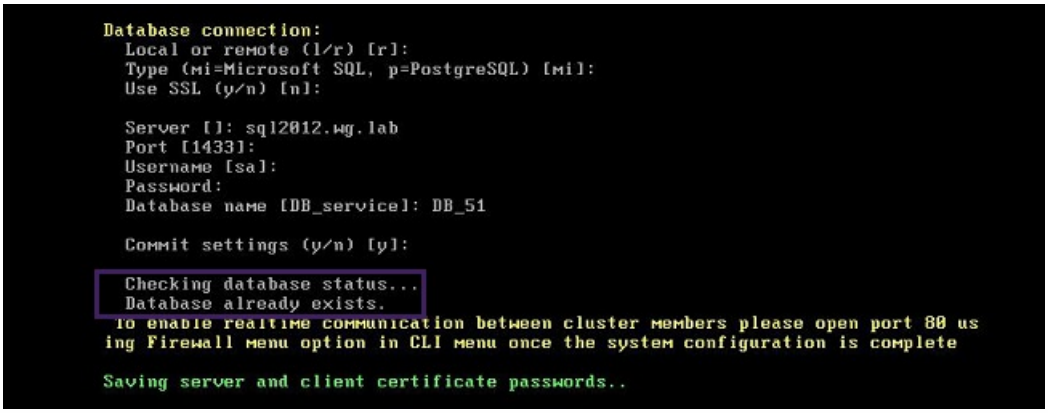
2. Provide the network configuration details as shown in the following figure.



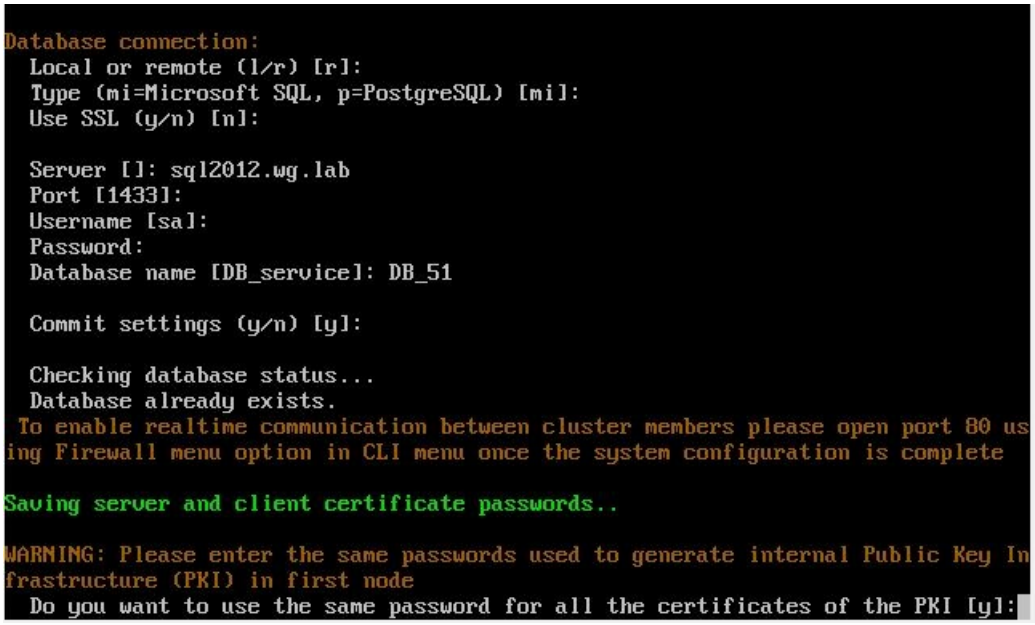
3. If you want to use the default password for data protection, type y; or, type n and enter a new password.

4. If you want to use FIPS, type y; or, type 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.

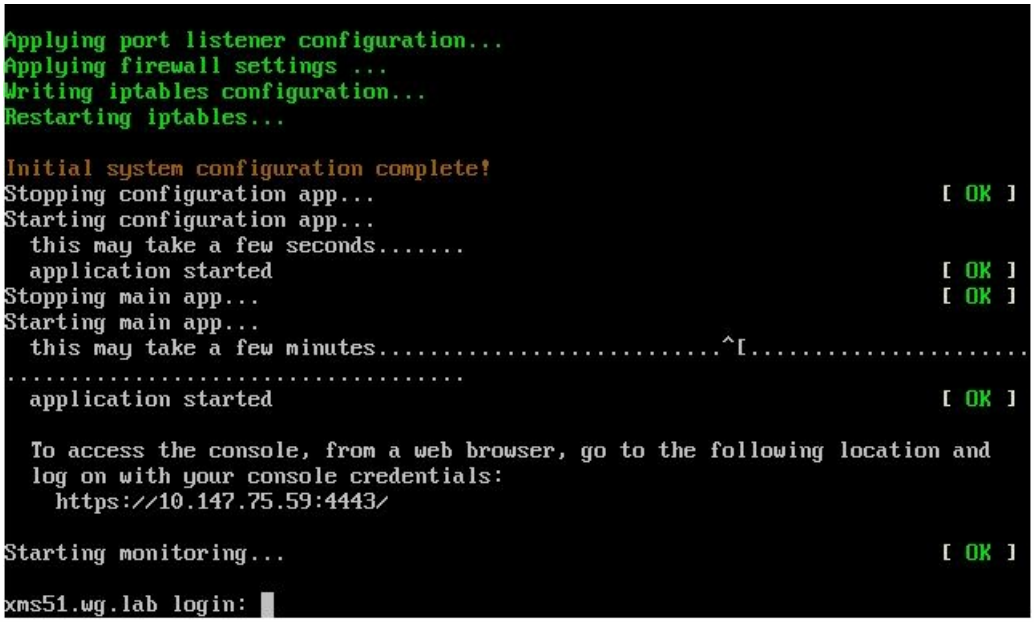


6. Enter the same passwords for the certificates that you provided for the first VM.



After you have entered the password, the initial configuration on second node will complete.

7. When the configuration is complete, the server restarts and the logon dialog box appears.

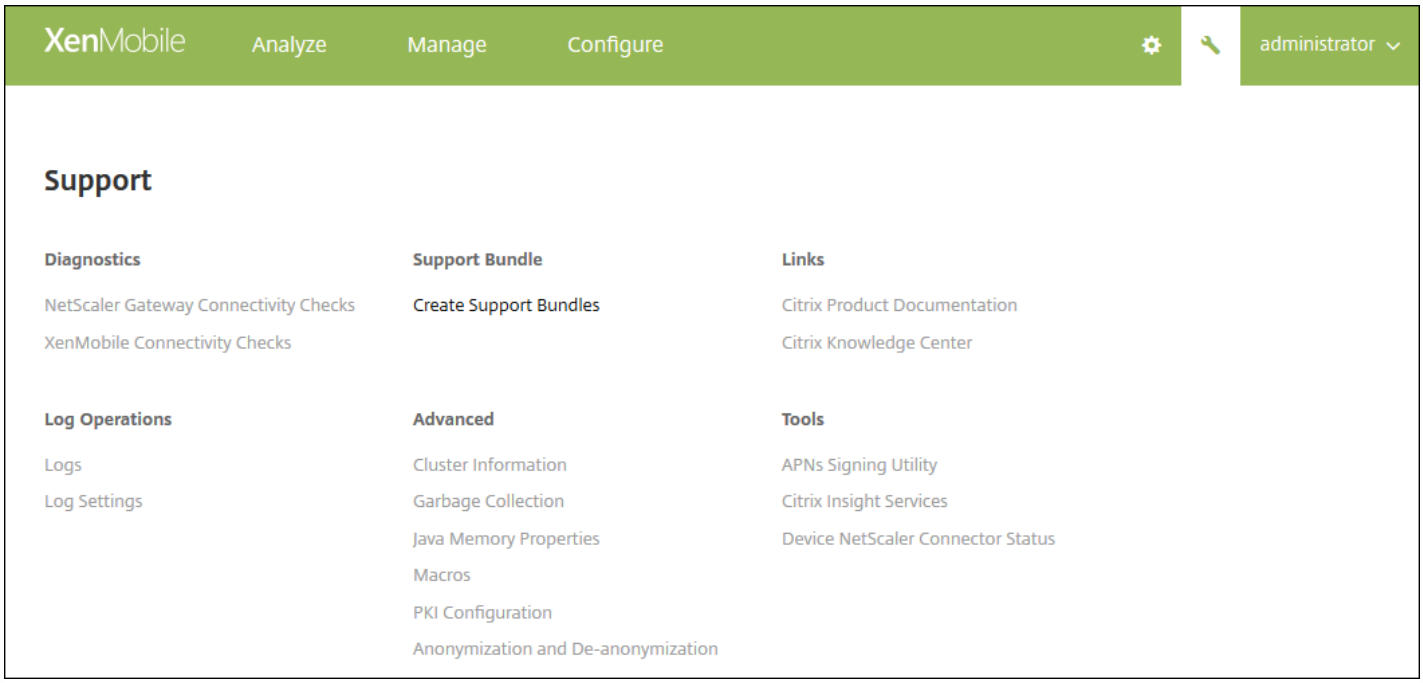


Note: The logon dialog box is identical to the logon dialog box of the first VM. The match is a way for you to confirm that both VMs are using the same database server.

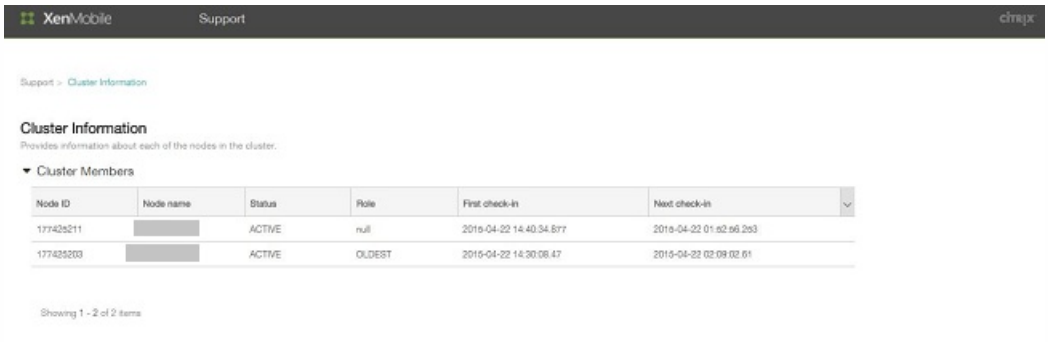
8. Use the fully qualified domain name (FQDN) of XenMobile to open the XenMobile console in a web browser.
9. In the XenMobile console, click the wrench icon in the upper-right corner of the console.

The **Support** page opens.

10. Under **Advanced**, click **Cluster Information**.



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.



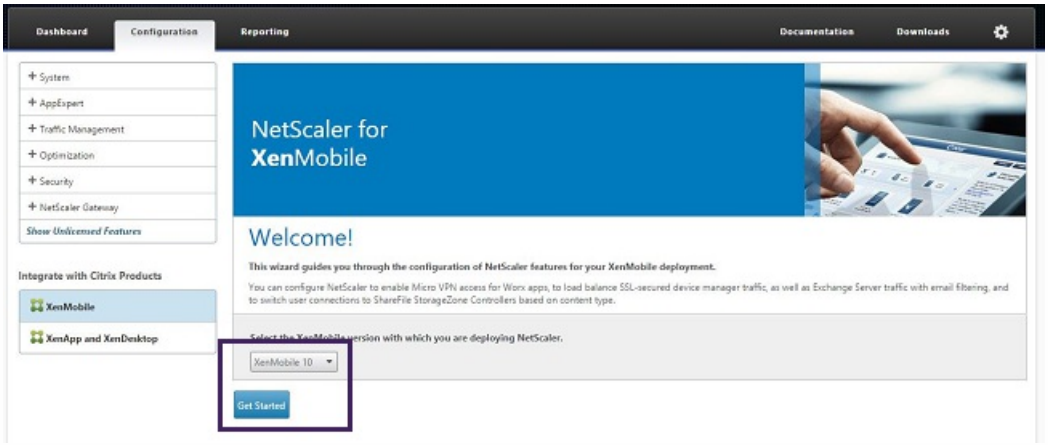
You can add other nodes by following the same steps. The first cluster added to the node has a Role of **OLDEST**. Clusters added after that will show a Role of **NONE** or **null**.

To configure load balancing for the XenMobile cluster in NetScaler

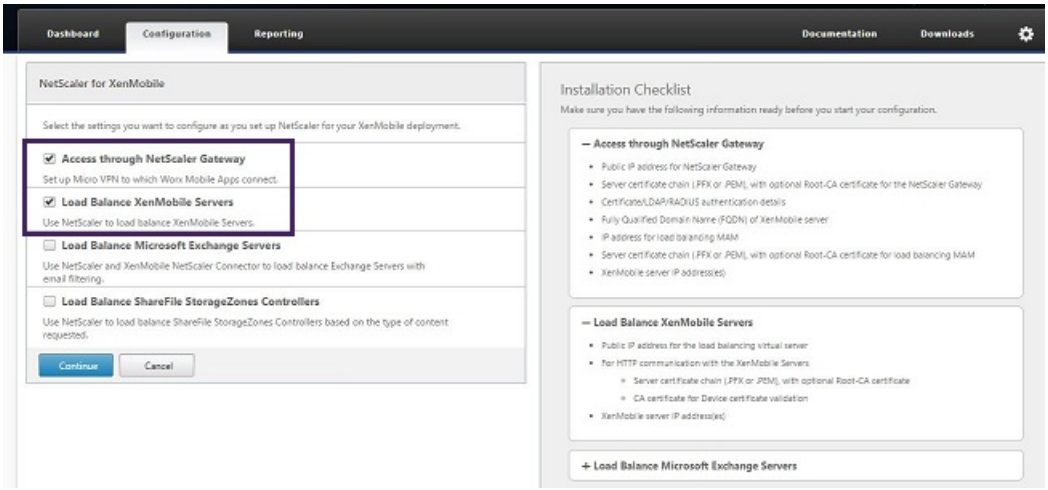
After you add the required nodes as members of the XenMobile cluster, you need to load balance the nodes to be able to access the clusters. Load balancing is done by running XenMobile Wizard available in NetScaler 10.5.x. You can following the steps in this procedure to load balance XenMobile by running the wizard.

1. Log on to NetScaler.

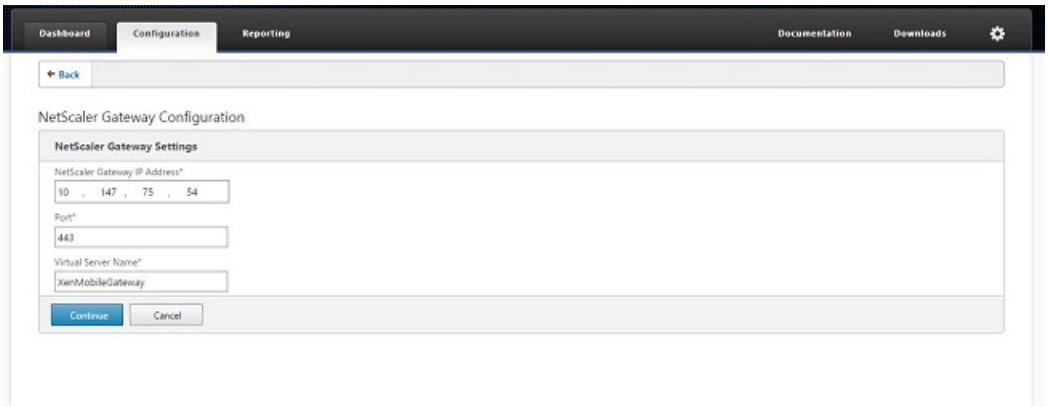
2. On the Configuration tab, click XenMobile and then click Get Started.



3. Select the Access through NetScaler Gateway check box and the Load Balance XenMobile Servers check box and then click Continue.

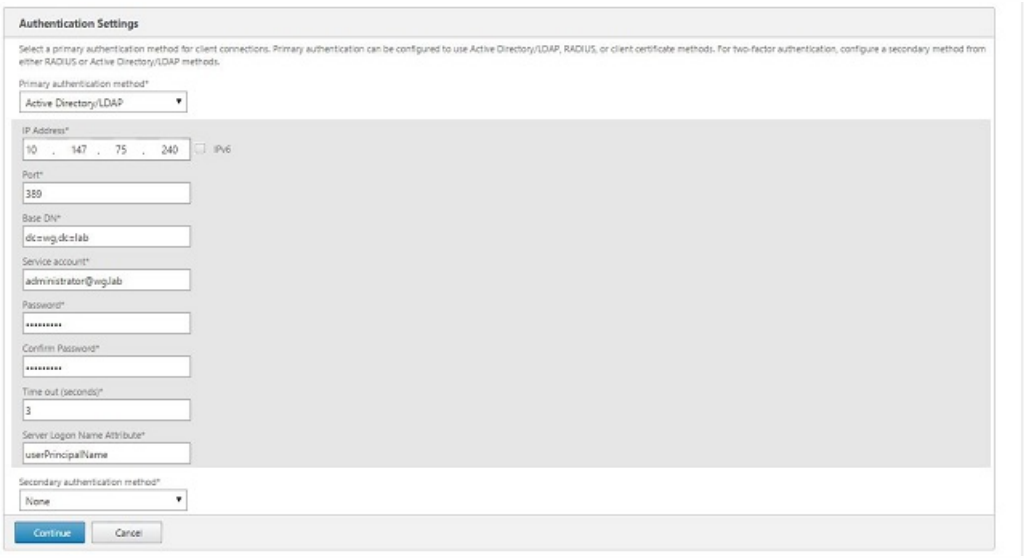


4. Enter the IP address for NetScaler Gateway and then click Continue.



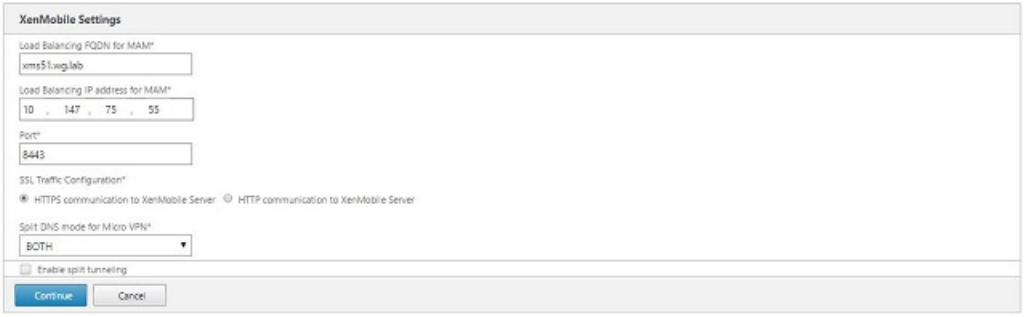
5. Bind the server certificate to the NetScaler Gateway virtual IP address by doing one of the following and then click Continue.
   - In Use existing certificate, choose the server certificate from the list.
   - Click the Install Certificate tab to upload a new server certificate.

6. Enter the Authentication server details and then click Continue.



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.

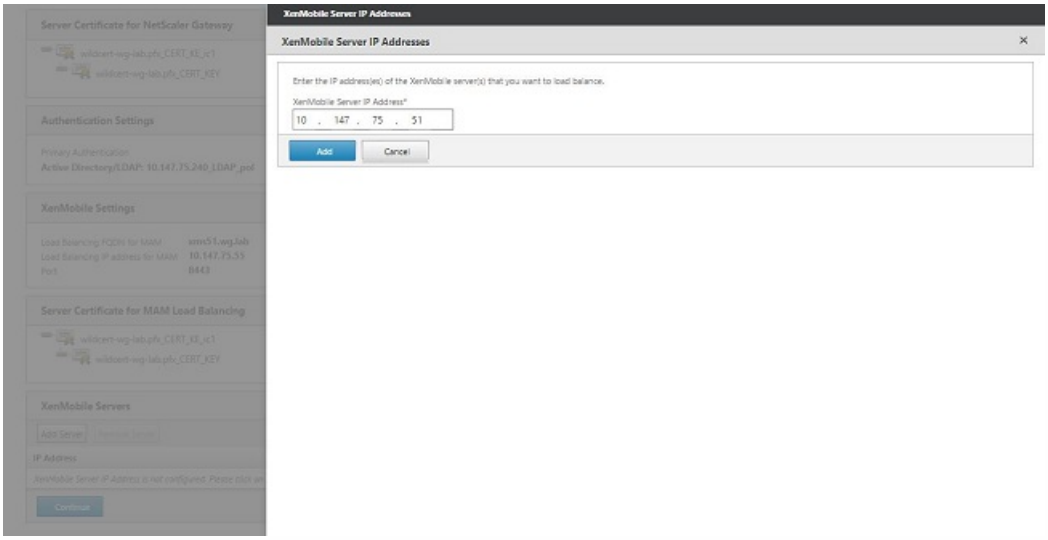


Note: Make sure the FQDN of the MAM load balancing virtual IP address and the FQDN of XenMobile are the same.

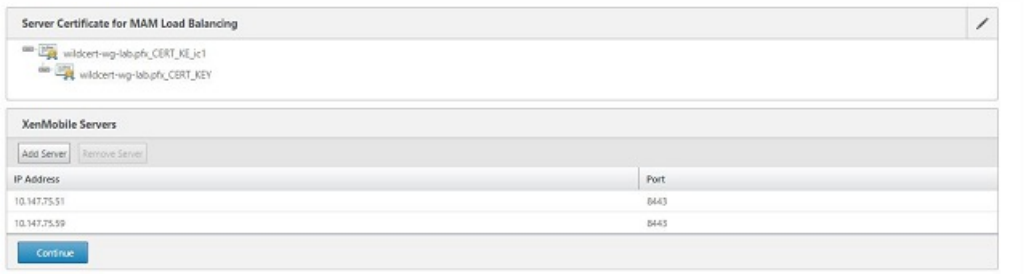
8. If you want to use SSL Bridge mode (HTTPS), select HTTPS communication to XenMobile Server. However, if you want to use SSL offload, select HTTP communication to XenMobile Server, as shown in the preceding figure. For the purposes of this article, the choice is SSL Bridge mode (HTTPS).
9. Bind the server certificate for the MAM load balancing virtual IP address and then click Continue.

10. Under XenMobile Servers, click Add Server to add the XenMobile nodes.

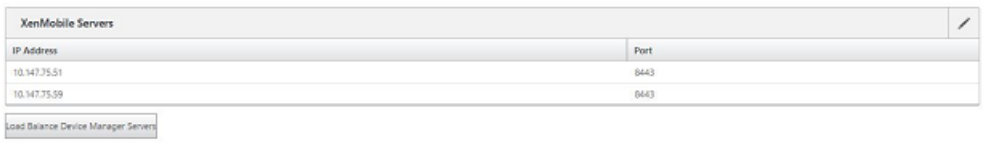
11. Enter the IP address of the XenMobile node and then click Add.



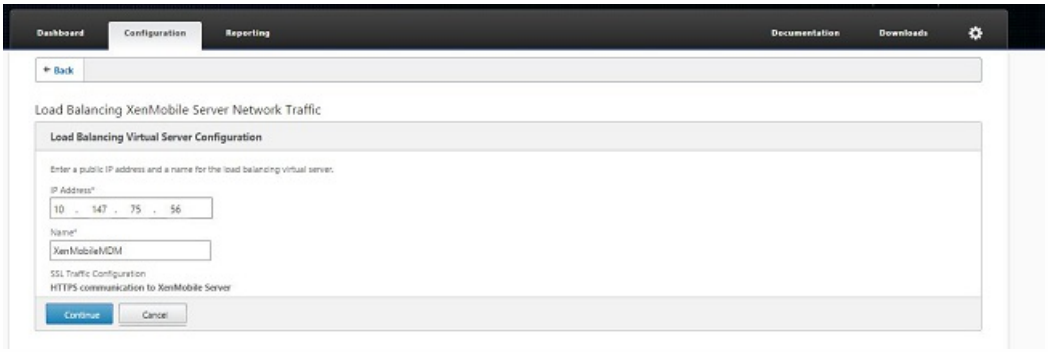
12. Repeat steps 10 and 11 to add additional XenMobile nodes that are part of the XenMobile cluster. You will see all the XenMobile nodes that you have added. Click Continue.



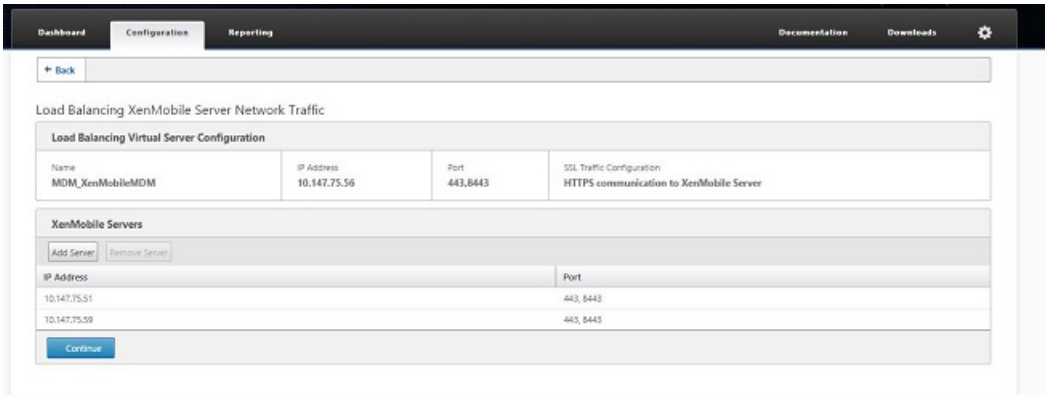
13. Click Load Balance Device Manager Servers to continue with the MDM load balancing configuration.



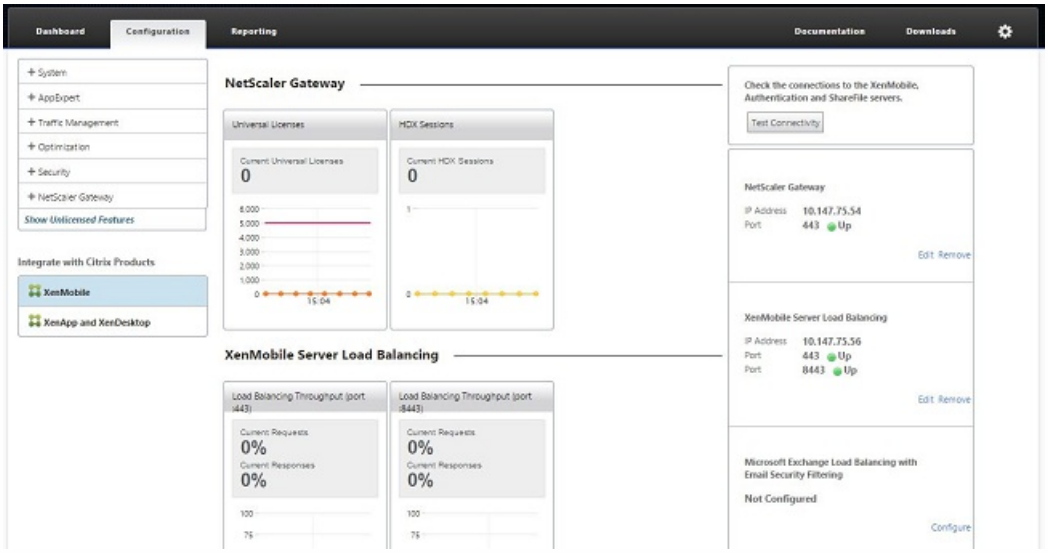
14. Enter the IP address to be used for MDM load balancing IP address and then click Continue.



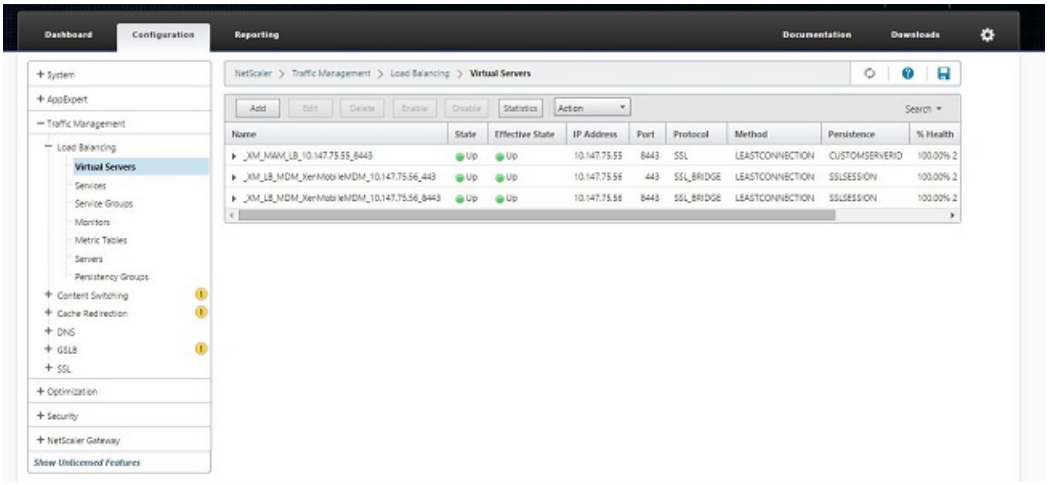
15. Once you see the XenMobile nodes in the list, click Continue and then click Done to finish the process.



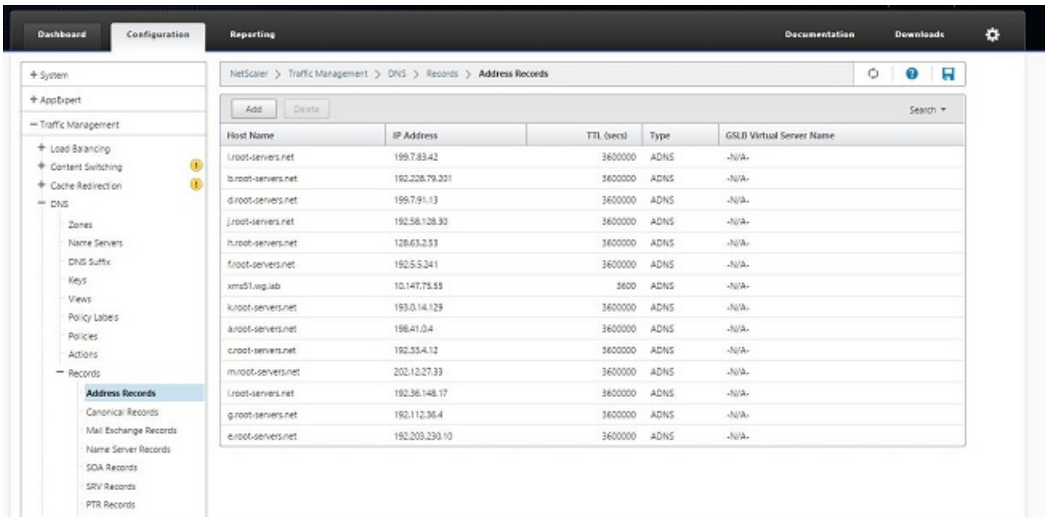
You will see the virtual IP address status on the XenMobile page.



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.



You will also see that the DNS entry in NetScaler points to the MAM load balancing virtual IP address.



Disaster recovery guide

Dec 22, 2016

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.

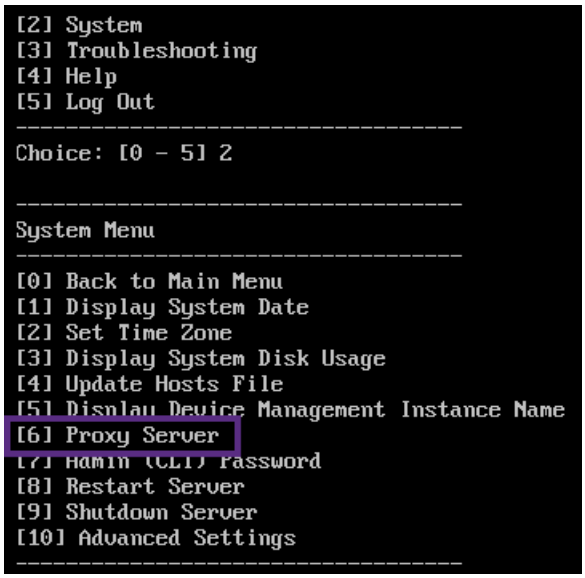
Enable proxy servers

Oct 05, 2016

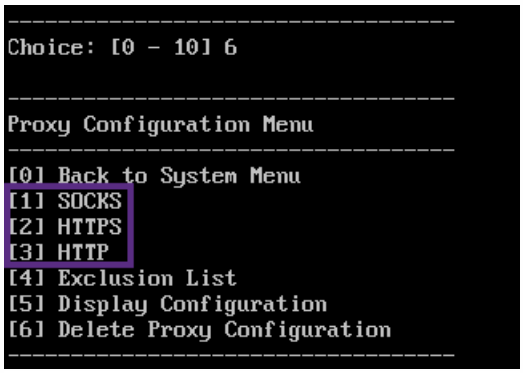
When you want to control outbound internet traffic, you can set up a proxy server in XenMobile to carry that traffic. To do this, you need to set up the proxy server through the command-line interface (CLI). Note that setting up the proxy server requires restarting your system.

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.



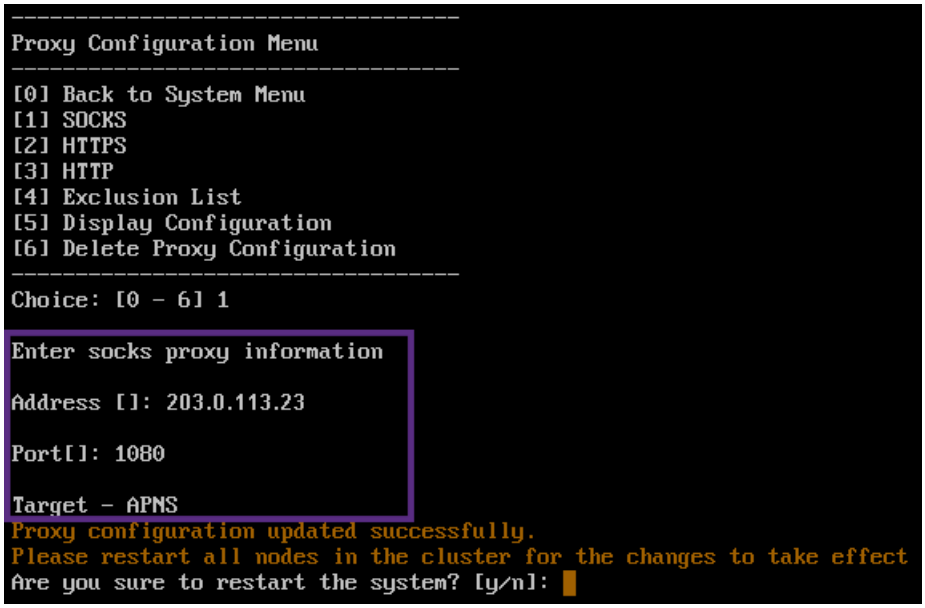
3. In the Proxy Configuration Menu, type **1** to select SOCKS, **2** to select HTTPS, or **3** to select HTTP.



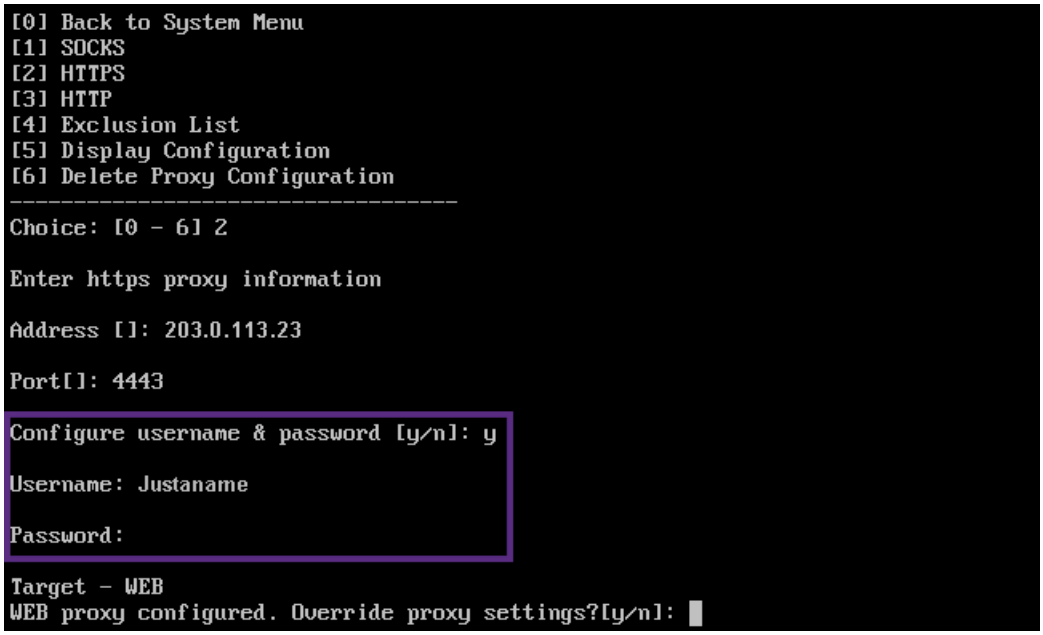
4. Type your proxy server IP address, port number, and target. See the following table for supported target types for each proxy server type.

Proxy type	Supported targets
SOCKS	APNS

HTTP	APNS, Web. PKI
HTTPS	Web, PKI
HTTP with authentication	Web, PKI
HTTPS with authentication	Web, PKI



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.



6. Type **y** to finish setting up your proxy server.

Server properties

Feb 10, 2017

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.

For information about the properties typically configured, refer to 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**.

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 the XenMobile server should retain 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 the XenMobile server should retain the audit log. Defaults to **7**.

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 se to 30 days, XenMobile attempts to renew the certificate if the device connects between December 1 and December 30. Defaults to **2592000** seconds (30 days).

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 a lot of traffic, you can increate this to 60 seconds or more. A certificate server that doesn't respond after 120 seconds needs maintenance. Defaults to **15000** milliseconds (15 seconds).

Deploy Log Cleanup (in Days)

The number of days that the XenMobile server should retain the deployment log. Defaults to **7**.

Disable SSL Server Verification

If **True**, disables SSL server certificate validation when all of the following conditions are met: You have enabled certificate-based authentication on your XenMobile server, the Microsoft CA server is the certificate issuer, and your

certificate has been signed by an internal CA whose root is not trusted by XenMobile server. Defaults to **True**.

Enable Console

If **true**, enables user access to the Self Help Portal Console. Defaults to **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 Notification Trigger

Enables or disables Secure Hub client notifications. The value **true** enables notifications. Defaults to **true**.

Full Pull of ActiveSync 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 baseline of ActiveSync devices. Defaults to **28800** seconds.

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 used the XenMobile server Public API to access the XenMobile console or any third-party app. A timeout of **0** means 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 will need to 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 property value specifies the amount of time to wait before showing a prompt to install the root CA. Citrix recommends that you don't edit this property unless you have network latency or speed issues. In that case, don't set to the value to more than 5000 millisecond (5 seconds). Defaults to **1000** millisecond (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 don't edit this property unless you have network latency or speed issues. In that case, don't set to the value to more than 5000 millisecond (5 seconds). Defaults to **1000** millisecond (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 XeMobile 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.

iOS MDM APNS Private Key Password

This property contains the APNs password, which is required for XenMobile to push notifications to Apple servers.

MAM_MACRO_SUPPORT

Configures XenMobile server for MAM-only deployments so that users with Android or iOS devices who enroll in Secure Hub with email credentials automatically enroll in Secure Mail. This means users do not have to enter additional information or take additional steps to enroll in Secure Mail. Add this custom key and use the default value **True** to enable automatic email enrollment. The client properties ENABLE_CREDENTIAL_STORE and SEND_LDAP_ATTRIBUTES are also required.

On first-time use of Secure Mail, Secure Mail obtains the user's email address, domain, and user ID from Secure Hub. Secure Mail uses the email address for autodiscovery. XenMobile identifies the Exchange server by the domain and user ID, which enables Secure Mail to authenticate the user automatically. XenMobile prompts the user to enter a password if the policy is set to not pass through the password, but the user is not required to enter any additional information.

NetScaler Single Sign-On

If **False**, disables the XenMobile callback feature during single signon from NetScaler to the XenMobile server. XenMobile uses the callback feature to verify the NetScaler Gateway session ID, if the NetScaler Gateway configuration includes a callback URL. 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 referred to as 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 a lot of traffic, you can increate this to 60 seconds or more. A certificate server that doesn't respond after 120 seconds needs maintenance. Defaults to **15000** milliseconds (15 seconds).

REST Web Services

Enables or disables the REST Web Service. Defaults to **true**.

Session Log Cleanup (in Days)

The number of days that the XenMobile server should retain 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 every time a license is activated or deleted and when 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.

Static Timeout in Minutes

If the **WebServices timeout type** server property is **STATIC_TIMEOUT**, this property defines the number of minutes after which XeMobile logs out an administrator who used the XenMobile server Public API to access the XenMobile console or 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**.

Users only from Exchange

If **true**, disables user authentication for ActiveSync Exchange users. Defaults to **false**.

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**.

XAM One-Time Ticket

The number of milliseconds that a one-time authentication token (OTT) is valid for downloading an app. This property works in conjunction with the properties **Unauthenticated App download for Android** and **Unauthenticated App download for Windows**, which specify whether to allow un-authenticated 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 an inactive user remains logged in. Defaults to **30**.

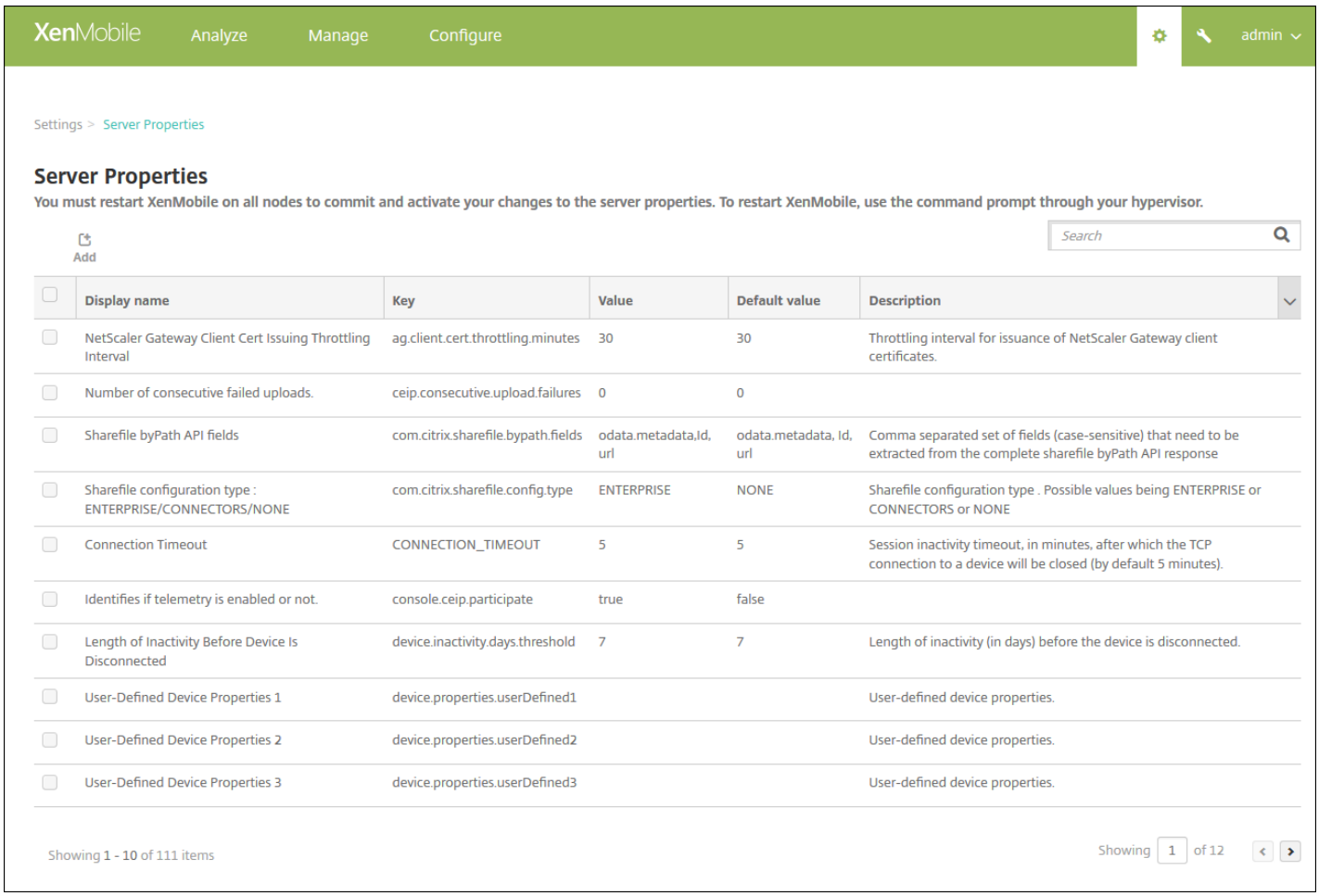
Adding, Editing, or Deleting Server Properties

In XenMobile, you can apply properties to the server. After making changes, you must restart XenMobile on all nodes to commit and activate changes.

> **Note**
>
> To restart XenMobile, use the command prompt through your hypervisor.

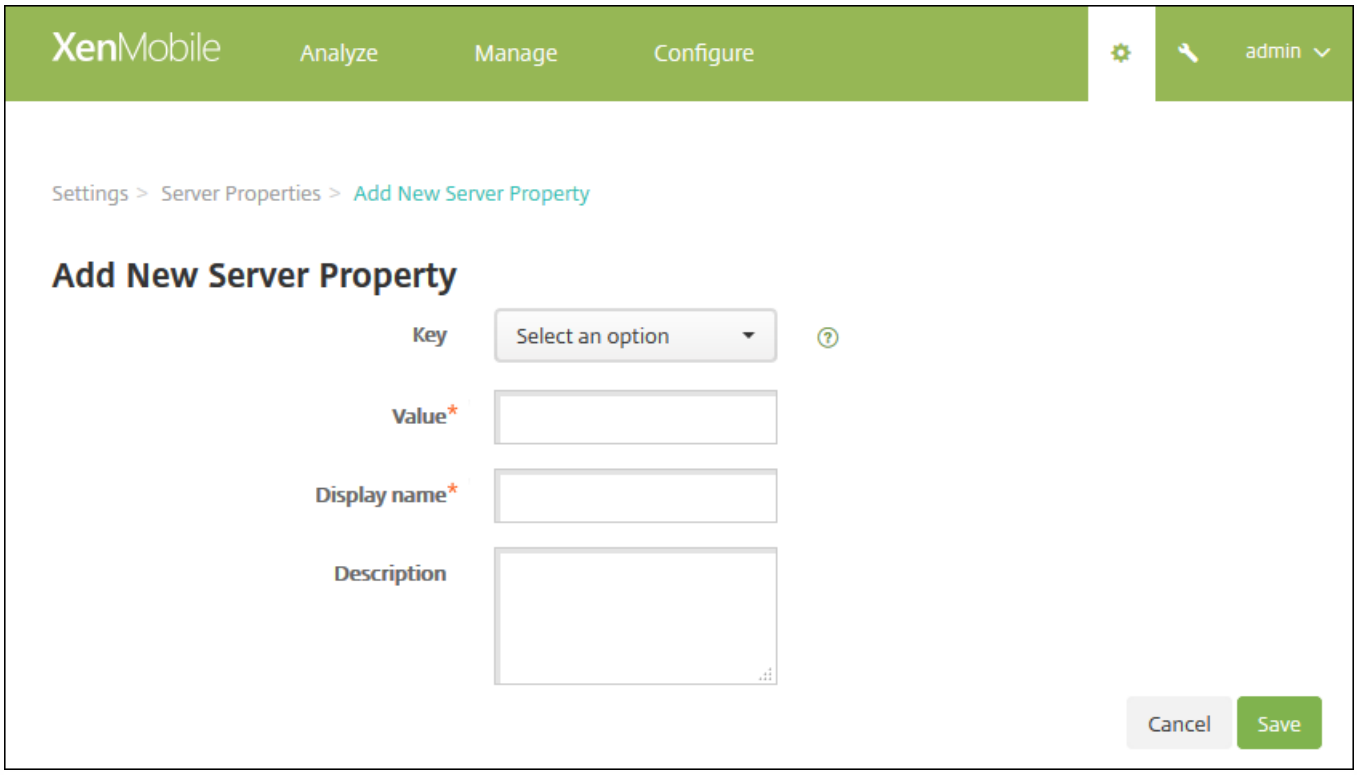
1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.

2. Under **Server**, click **Server Properties**. The **Server Properties** page appears. You can add, edit, or delete server properties from this page.



To add a server property

1. Click **Add**. The **Add New Server Property** page appears.



2. Configure these settings:

- **Key**: In the list, select the appropriate key. Keys are case-sensitive. You must contact Citrix Support before making any changes, 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.

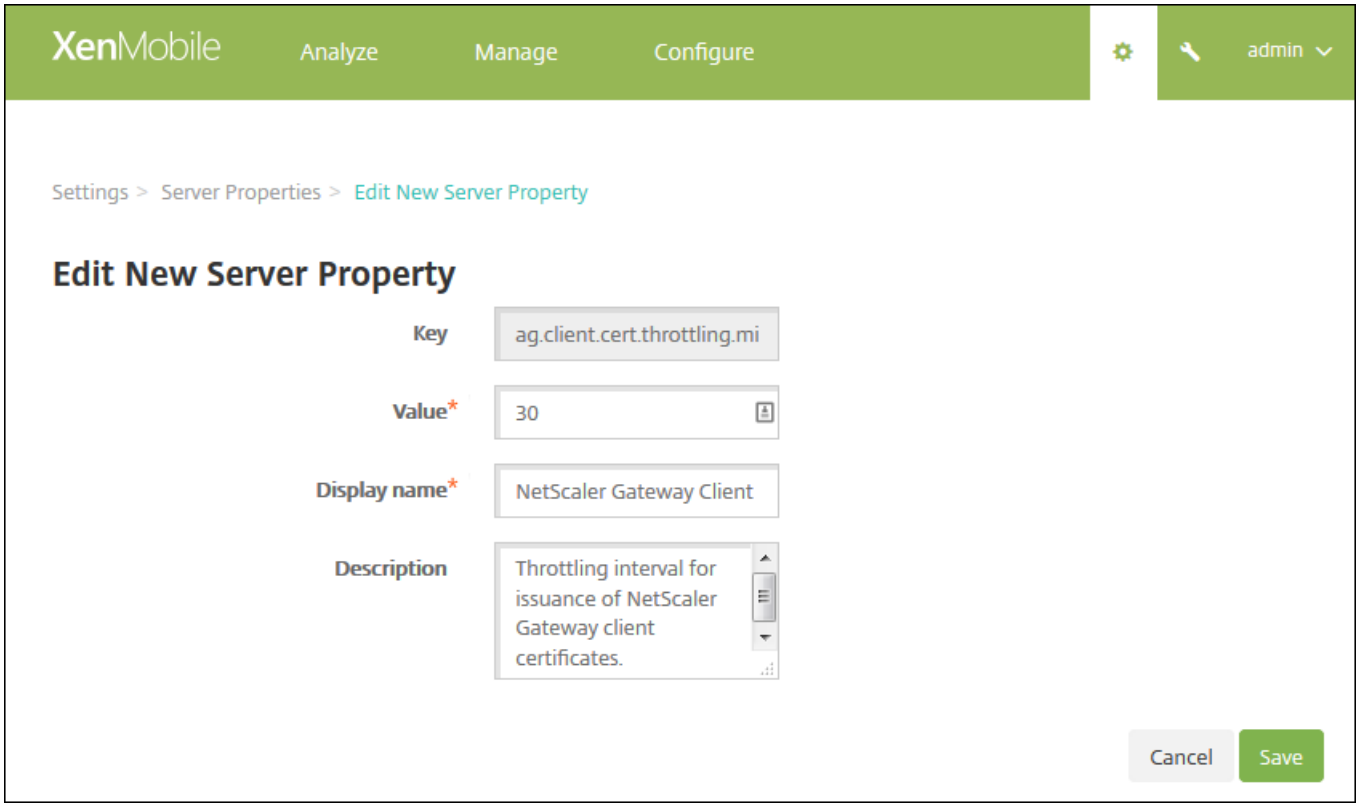
3. Click **Save**.

To edit a server property

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.



3. Change the following information as appropriate:

- **Key**: You cannot change this field.
- **Value**: The property's value.
- **Display Name**: The property's name.
- **Description**: The property's description.

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

To delete a server property

1. In the **Server Properties** table, select the server property you want to delete.

    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.

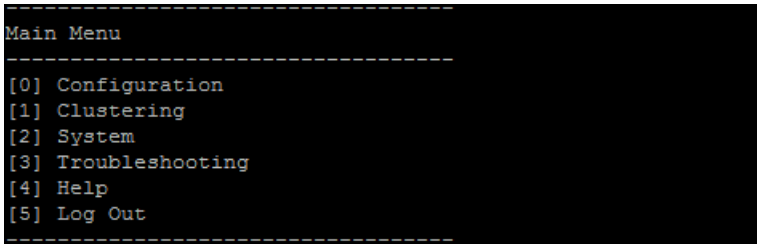
Command-line interface options

Jan 09, 2017

At any time, you can access the command-line interface (CLI) options as follows:

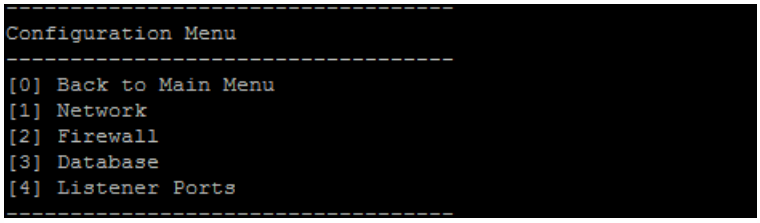
- On the hypervisor on which you installed XenMobile - Citrix XenServer, Microsoft Hyper-V, or VMware ESXi. In your hypervisor, select the imported XenMobile virtual machine, start the command prompt view, and log on to your administrator account for XenMobile. For details, see the documentation for your hypervisor.
- By using SSH, if SSH is enabled in your firewall. Log on to your administrator account for XenMobile.

You can perform a variety of configuration and troubleshooting tasks using the CLI. Following is the top-level menu for the CLI.

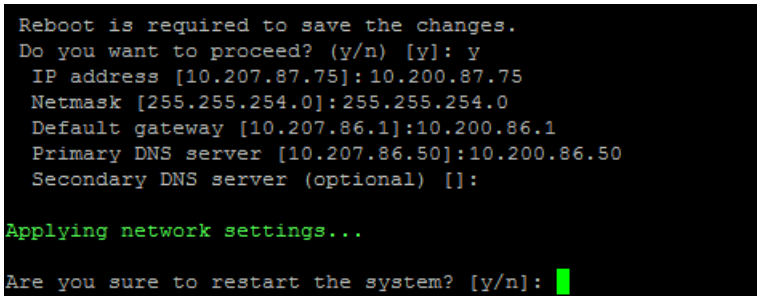


Configuration options

Following are samples of the **Configuration Menu** and the settings displayed for each option.



[1] Network



[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]:
```

Clustering options

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 realtime 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 will open 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:

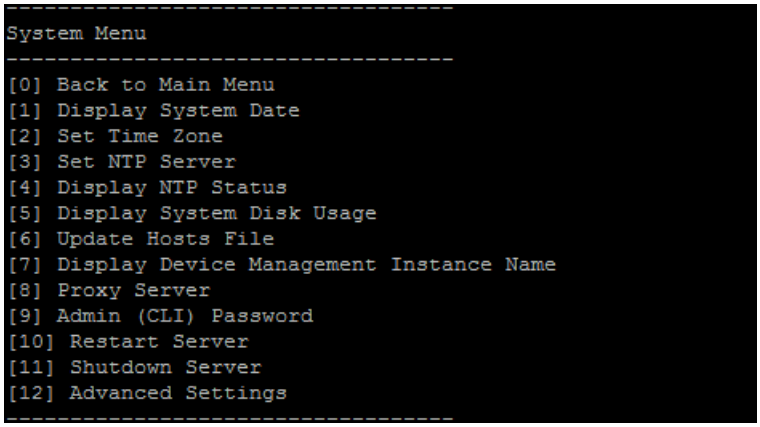
Hazlecast Cluster Members:

[IP addresses listed]

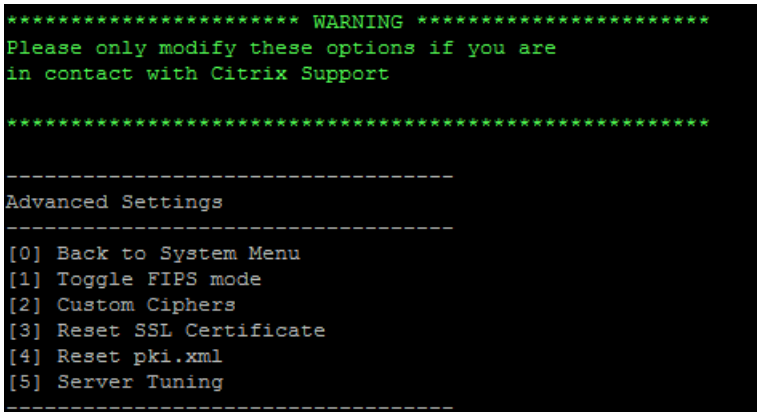
NOTE: If a configured node is not part of the cluster, please reboot that node.

System options

From the **System Menu**, you can display or set various system-level information, restart or shut down the server, or access **Advanced Settings**.



[12] Advanced Settings



Server Tuning options include the server connection timeout, maximum connections (by port), and maximum threads (by port).

Troubleshooting options

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

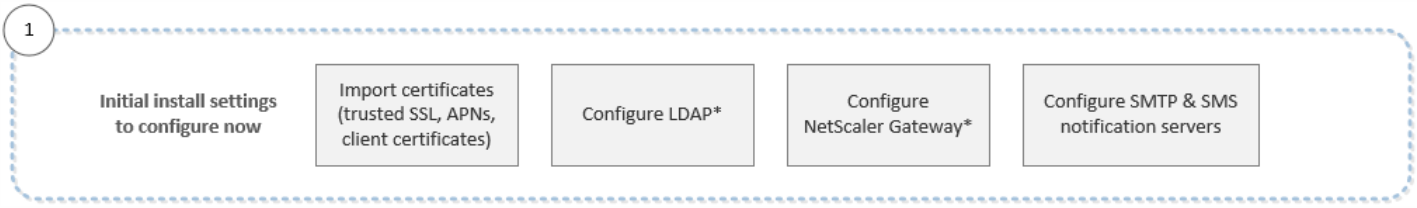
Jan 18, 2017

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 need to install XenMobile, see Installing XenMobile. For details on browser support for the XenMobile console, see Browser Support in the XenMobile Compatibility article.

Initial settings workflow

After you finish configuring XenMobile first in the command-line console and next in the XenMobile console, the dashboard opens. Because you cannot return to the initial configuration screens, if you skipped some of the install configurations at that time, you can configure the following settings in the console. Before you start adding users, apps, and devices, you should considering 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.



For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and their sub-articles:

- 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 Getting Started with Publishing.
- 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 Google Apps.
- Enable APIs and create a service account for Android for Work. For details, see Android for Work 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. You need an Apple APNs certificate if you plan to manage IOS devices with your XenMobile Service (cloud) deployment and if you plan to use push notification for your WorxMail deployment. 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.

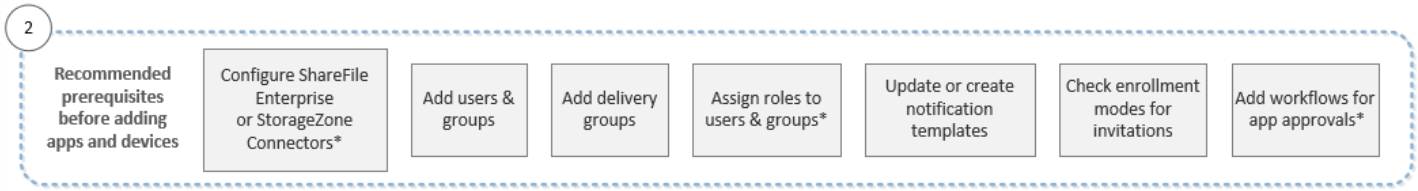
Windows

- 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.
- Make sure 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.

Console prerequisites workflow

This workflow shows recommended prerequisites for you to configure before you add apps and devices.

Note: The items with an asterisk are optional.



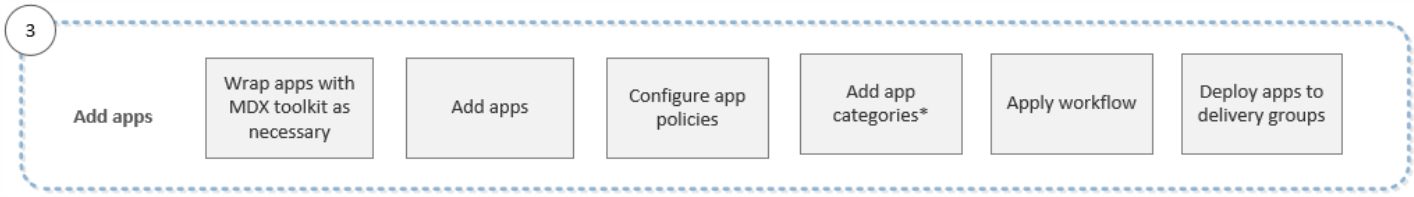
For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and their sub-articles:

- User accounts, roles, and enrollment
- Deploy resources
- Configure roles with RBAC
- Notifications
- Create and manage workflows

Add apps workflow

This workflow shows a recommended order to follow when adding apps to XenMobile.

Note: The items with an asterisk are optional.



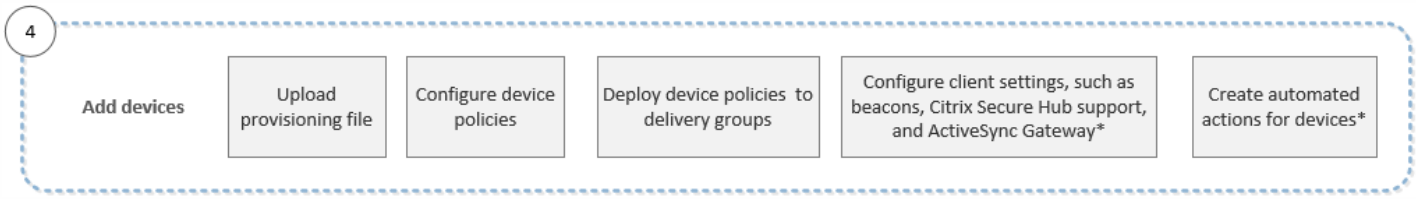
For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and their sub-articles:

- About the MDX Toolkit
- Add apps
- MDX Policies at a Glance
- Create and manage workflows
- Deploy resources

Add devices workflow

This workflow shows a recommended order to follow when adding and registering devices in XenMobile.

Note: The items with an asterisk are optional.

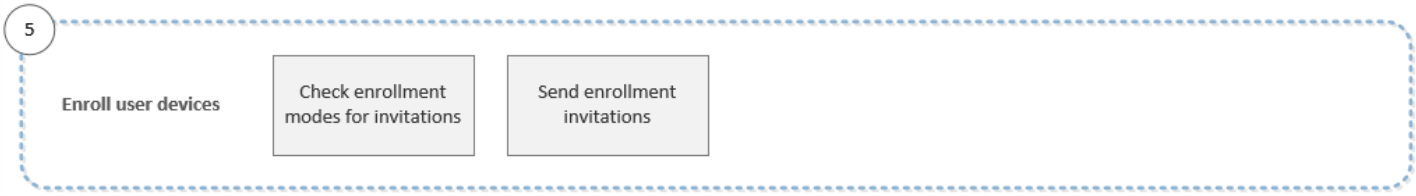


For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and their sub-articles:

- Devices
- Supported Device Platforms
- Deploy resources
- Monitor and support
- Automated actions

Enroll user devices workflow

This workflow shows a recommended order to follow when enrolling user devices in XenMobile.



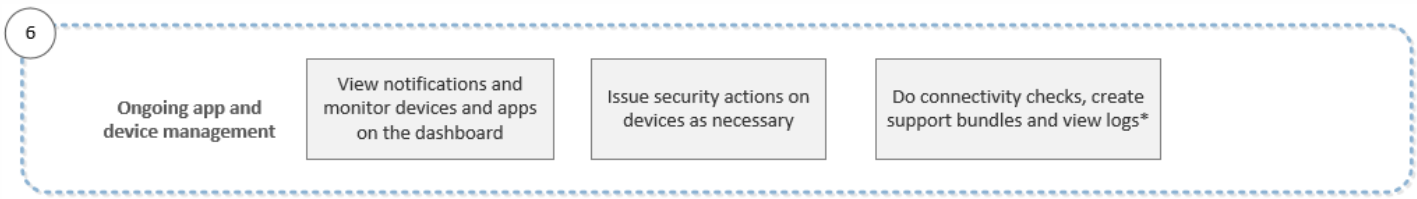
For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles:

- User accounts, roles, and enrollment
- Notifications

Ongoing app and device management workflow

This workflow shows recommended ongoing app and device management activities you can do in the console.

Note: The items with an asterisk are optional.



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 and its sub-articles.

Certificates and Authentication

Feb 27, 2017

Several components play a role in authentication during XenMobile operations:

- **XenMobile server**: The XenMobile server is where you define the security involved in enrollment as well as 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 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, 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: If 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 new 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 that come into play when deciding how to configure authentication, including an overview of single-factor, and two-factor 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 you replace the SSL certificate with a trusted SSL certificate from a well-known certificate authority (CA).

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, user enter their Citrix PIN for Single Sign on 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, you need to 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.
StoreFront	PFX (PKCS#12)	SSL, Root

XenMobile supports SSL listener certificates and client certificates with bit lengths of 4096, 2048, and 1024. Be aware 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.

Uploading certificates in XenMobile

Each certificate you upload is represented by an entry in the Certificates table, summarizing its contents. When you configure PKI integration components that require a certificate, you are prompted to choose from a list of the server certificates that satisfy the context-dependent criteria. For example, you might want to configure XenMobile to integrate with your Microsoft CA. The connection to the Microsoft CA should be authenticated 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 and then 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.

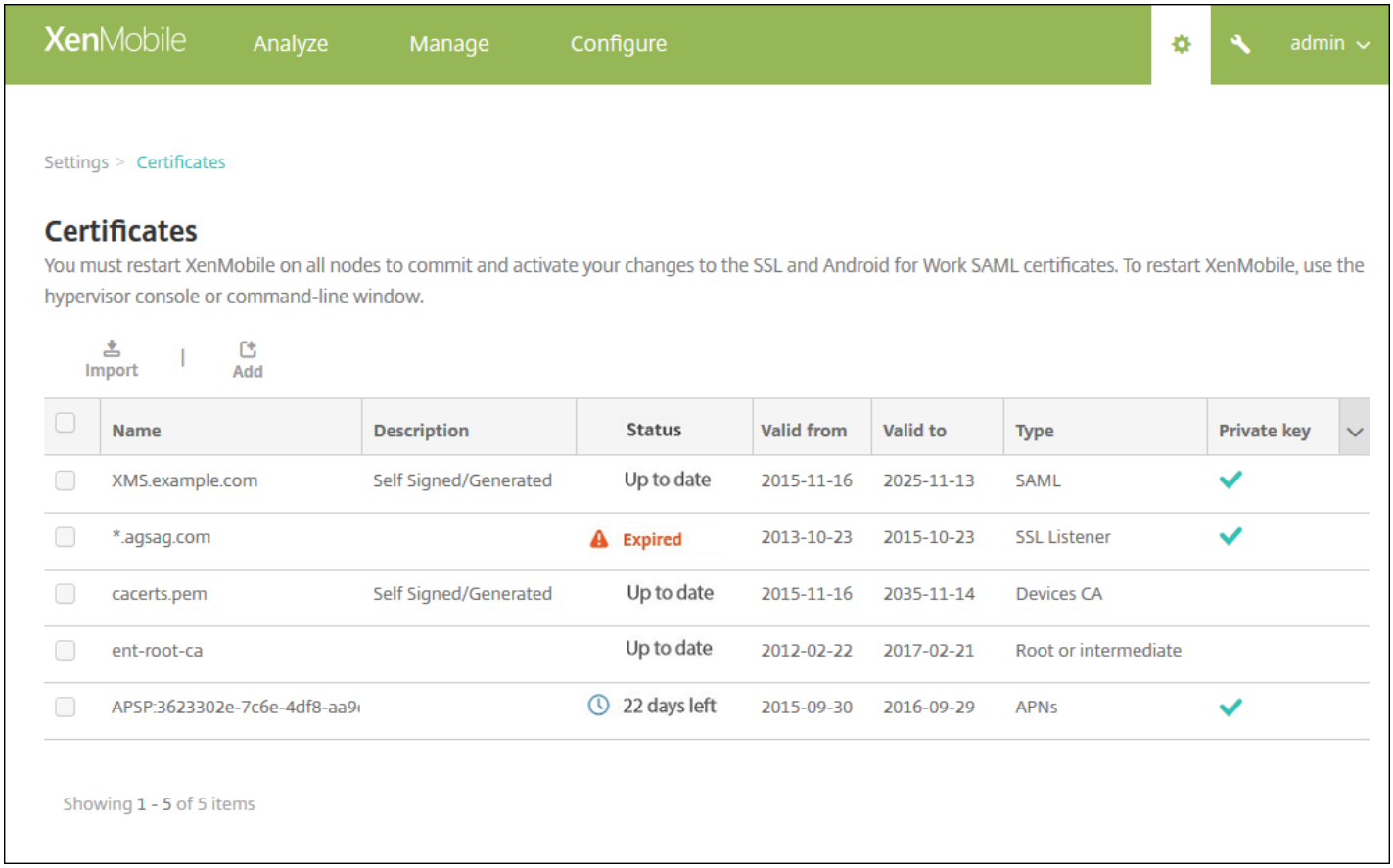
You can upload the CA certificate (without the private key) that the CA uses to sign requests, and you can upload an SSL client certificate (with the private key) for client authentication. When configuring the Microsoft CA entity, you need to specify the CA certificate, which you can then select from 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.

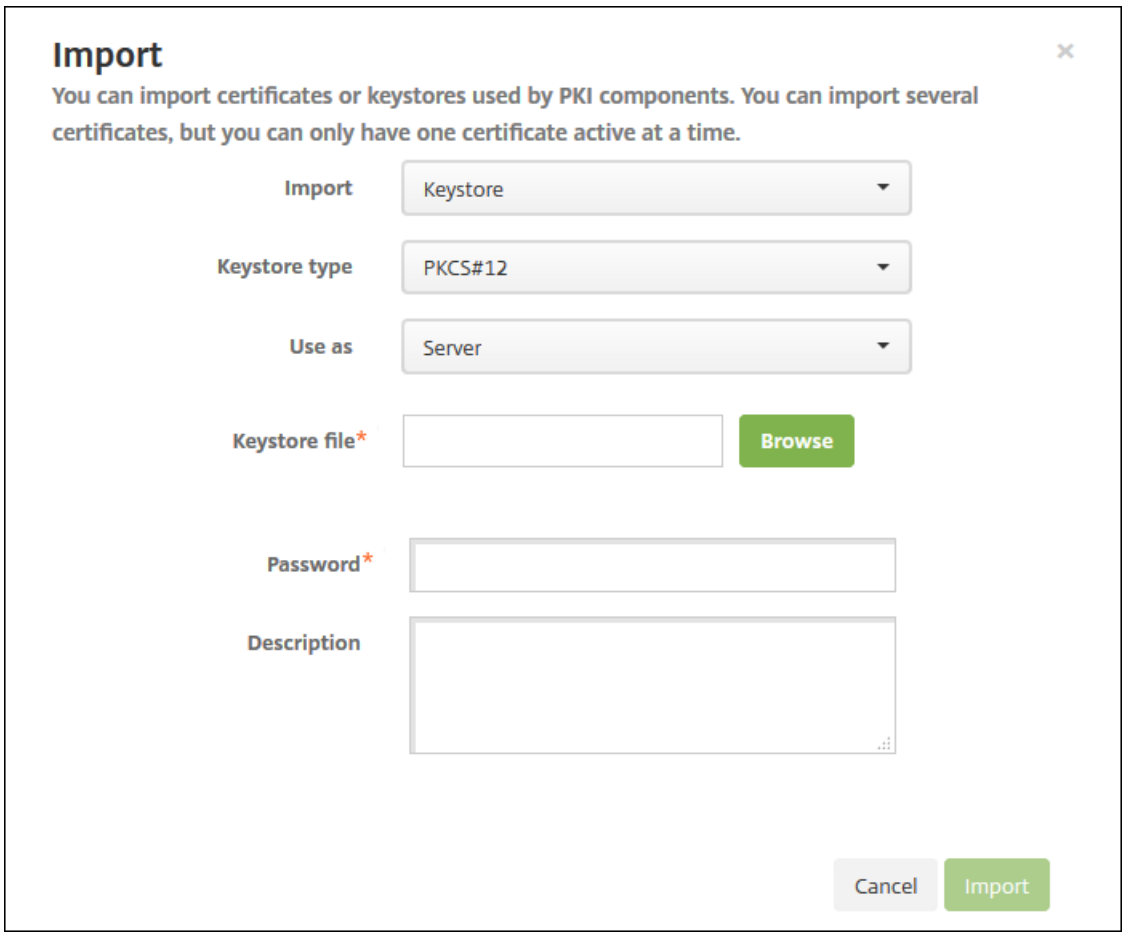
2. Click **Certificates**. The **Certificates** page appears.



3. Click **Import**. The **Import** dialog box appears.

4. Configure these settings:

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



- **Keystore type**: In the list, click **PKCS#12**.
- **Use as**: In the list, click how you will 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 may use server certificates as a 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 single sign-on (SSO) access to servers, websites, and apps.
  - **APNs**. Apple Push Notification service (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 really do form a chain, such as 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 may use server certificates as a 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 in conjunction 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 have the option to either replace the existing entry or to delete the entry.

To most effectively update your certificates, in the XenMobile console, 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 keep track of 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 & Intermediate CA Certificates for the preceding certificates and any other internal resources (StoreFront/Proxy, etc.)
APNS 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

XenMobile Certificate Expiration Policy

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

> **Note**
>
> The Certification Authority (CA) will prompt you to renew your SSL certificate prior to the expiration date.

APNs certificate for Citrix Secure Mail

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

APNs certificate for iOS device management

In order to enroll and manage iOS devices with XenMobile, you need to 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. Make sure to log on as the same user who created the certificate.

You will 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 AppleID CustomersID 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"

MDX Toolkit (iOS distribution certificate)

Any app that runs on a physical iOS device (other than apps in the Apple App Store) must be signed with a provisioning profile and 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. Make sure that all certificates including APNS, SSL Listener, Root and Intermediate certificate are valid.

Android keystore

The keystore is a file that contains certificates used to sign your Android app.When your key's validity period expires, users can no longer seamlessly upgrade to new versions of your app.

Enterprise certificate from Symantec for Windows phones

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, install an app published and signed by the company, or start a company app that was installed on the phone.

NetScaler

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, accessing the Store, connecting to Exchange Server when using Secure Mail, and enumerating and opening HDX apps (depending on which certificate expired).

The Expiry Monitor and Command Center can help you to keep track of your NetScaler certificates and will notify you when the certificate expires. These two 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

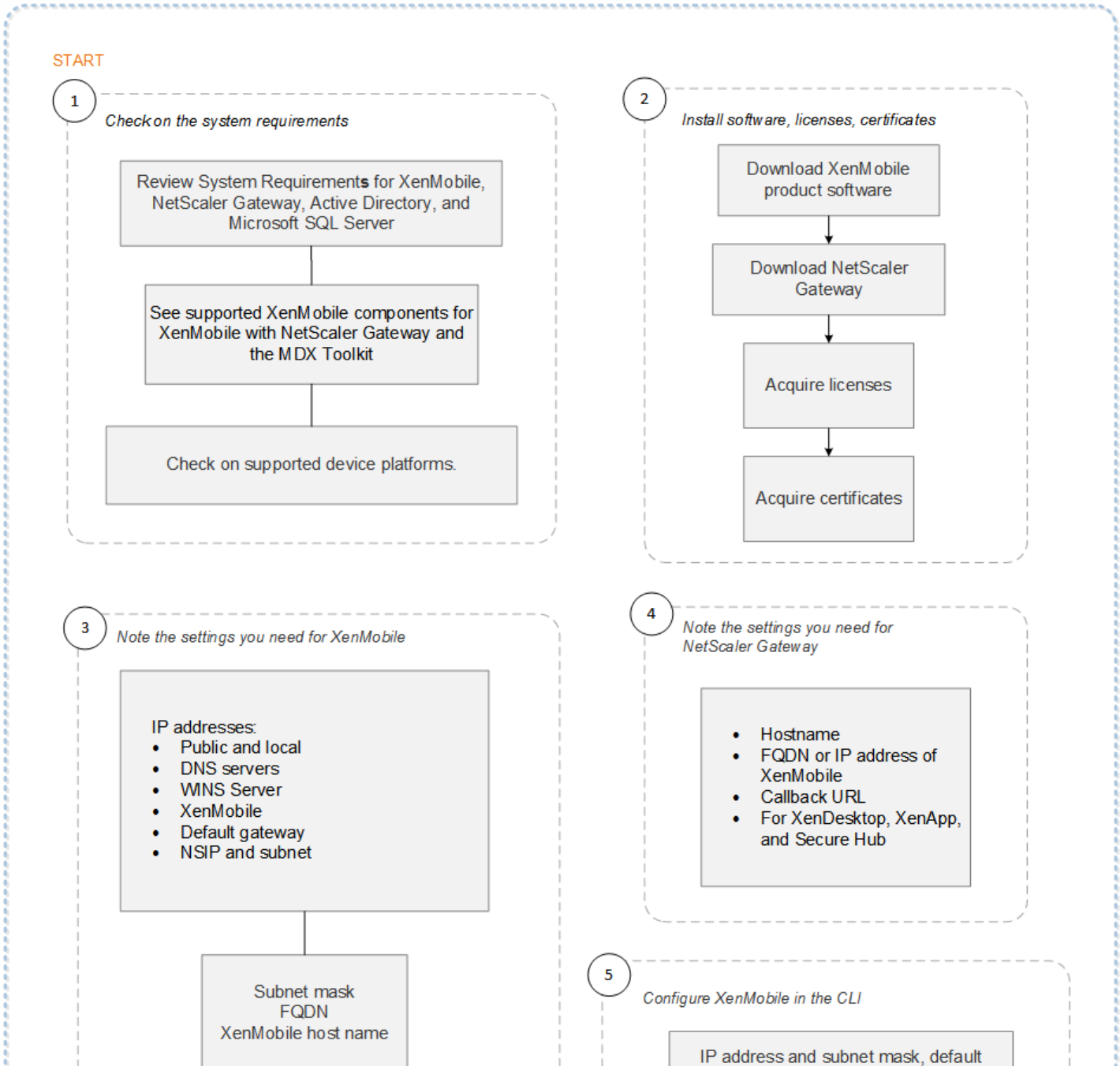
NetScaler Gateway and XenMobile

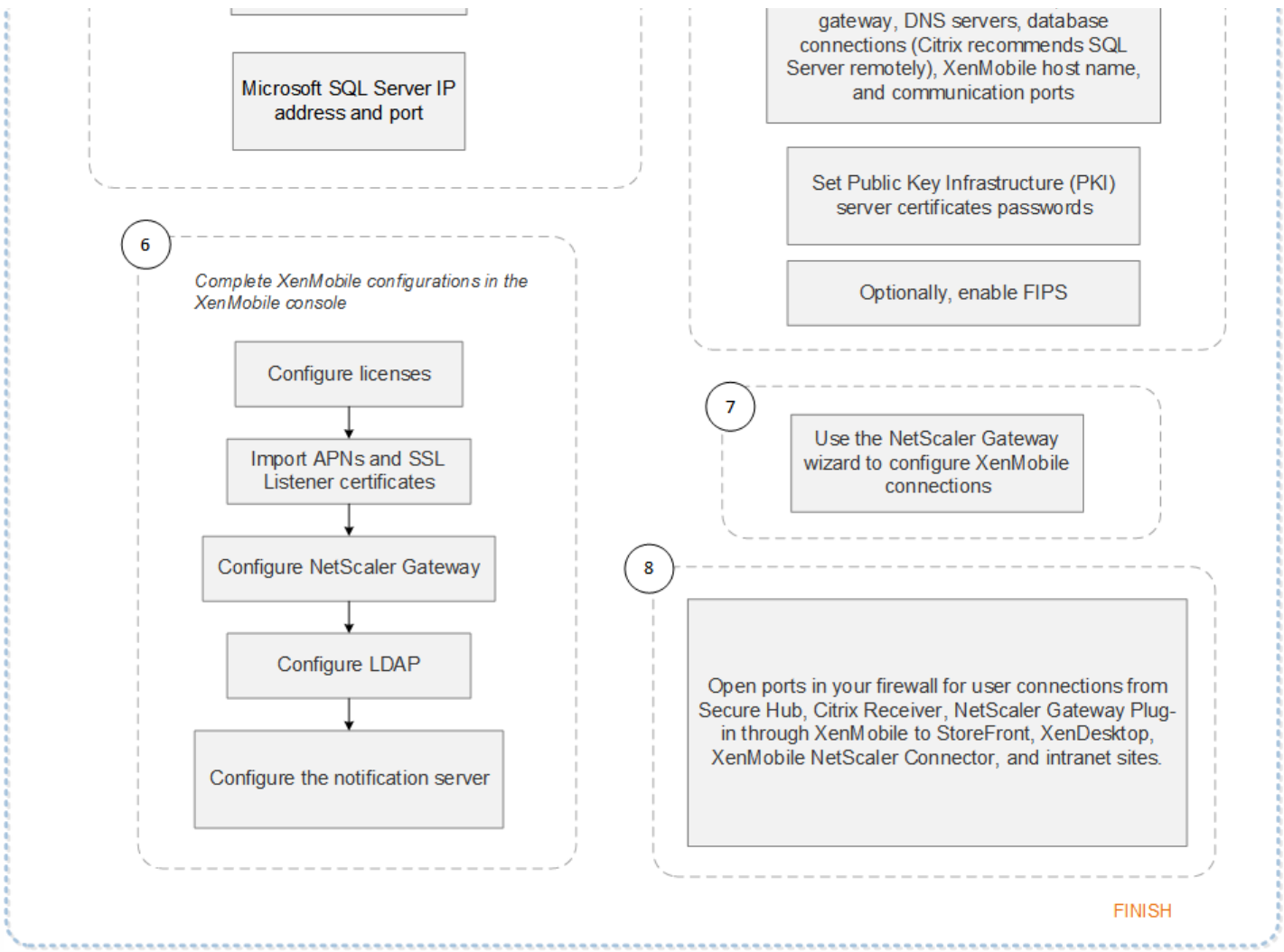
Nov 10, 2016

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 by creating a micro VPN from the apps on the device to NetScaler Gateway. You configure NetScaler Gateway in the XenMobile console, as described in this article.

Flowchart for XenMobile deployment with NetScaler Gateway

You can use this flowchart to guide you through the main steps for deploying XenMobile with NetScaler Gateway. Links to topics on each step follow the figure.





1

- System requirements and compatibility

2

- Install and configure

3

- Preinstallation checklist

4

- Preinstallation checklist

5

- Configure XenMobile in the Command Prompt Window

6

- Configure XenMobile in a web browser

7

- Configuring Settings for Your XenMobile Environment

8

- Ports

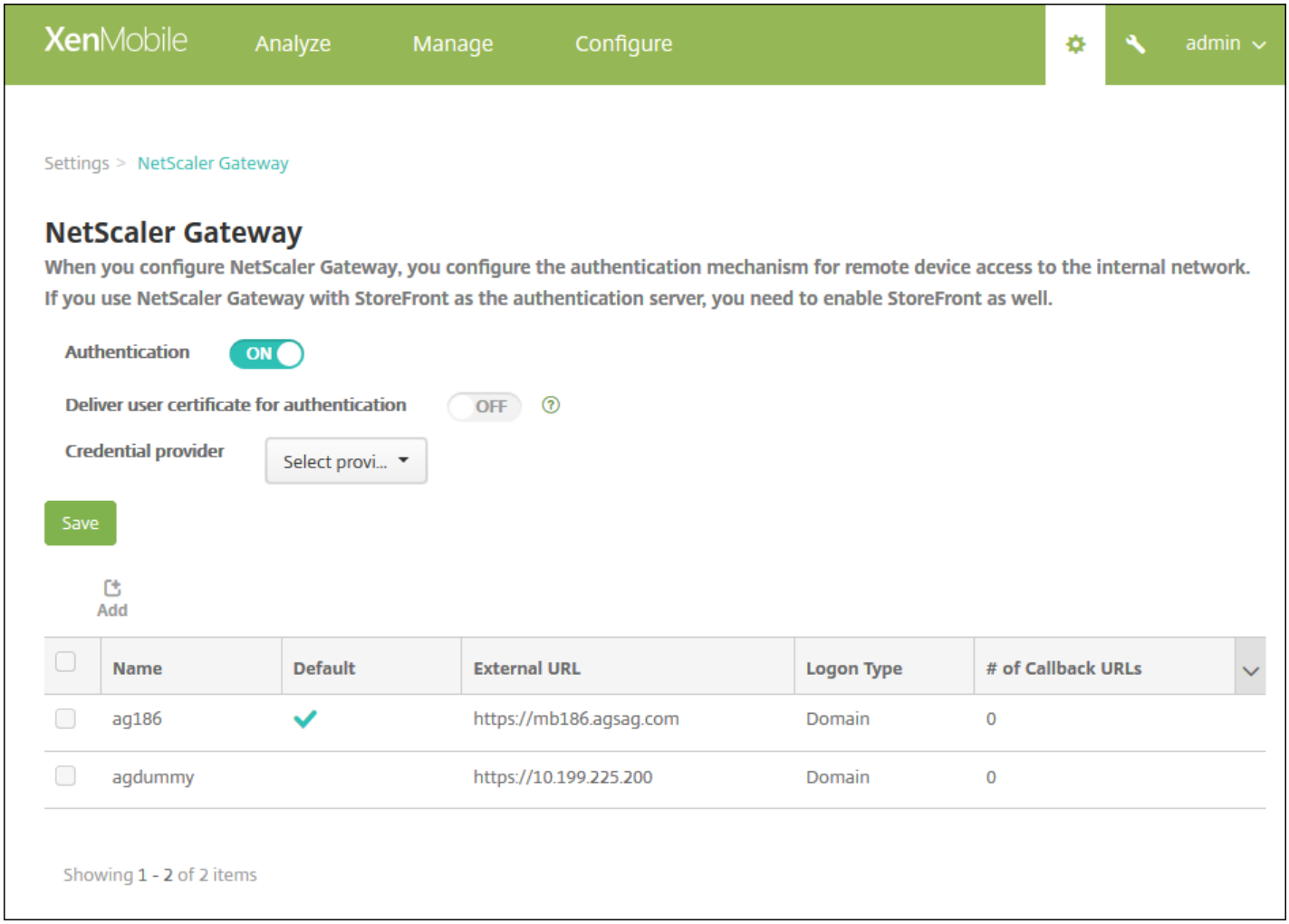
The flowchart is also available in PDF format.

PDF Flowchart for Deploying XenMobile

To configure NetScaler Gateway

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.



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.

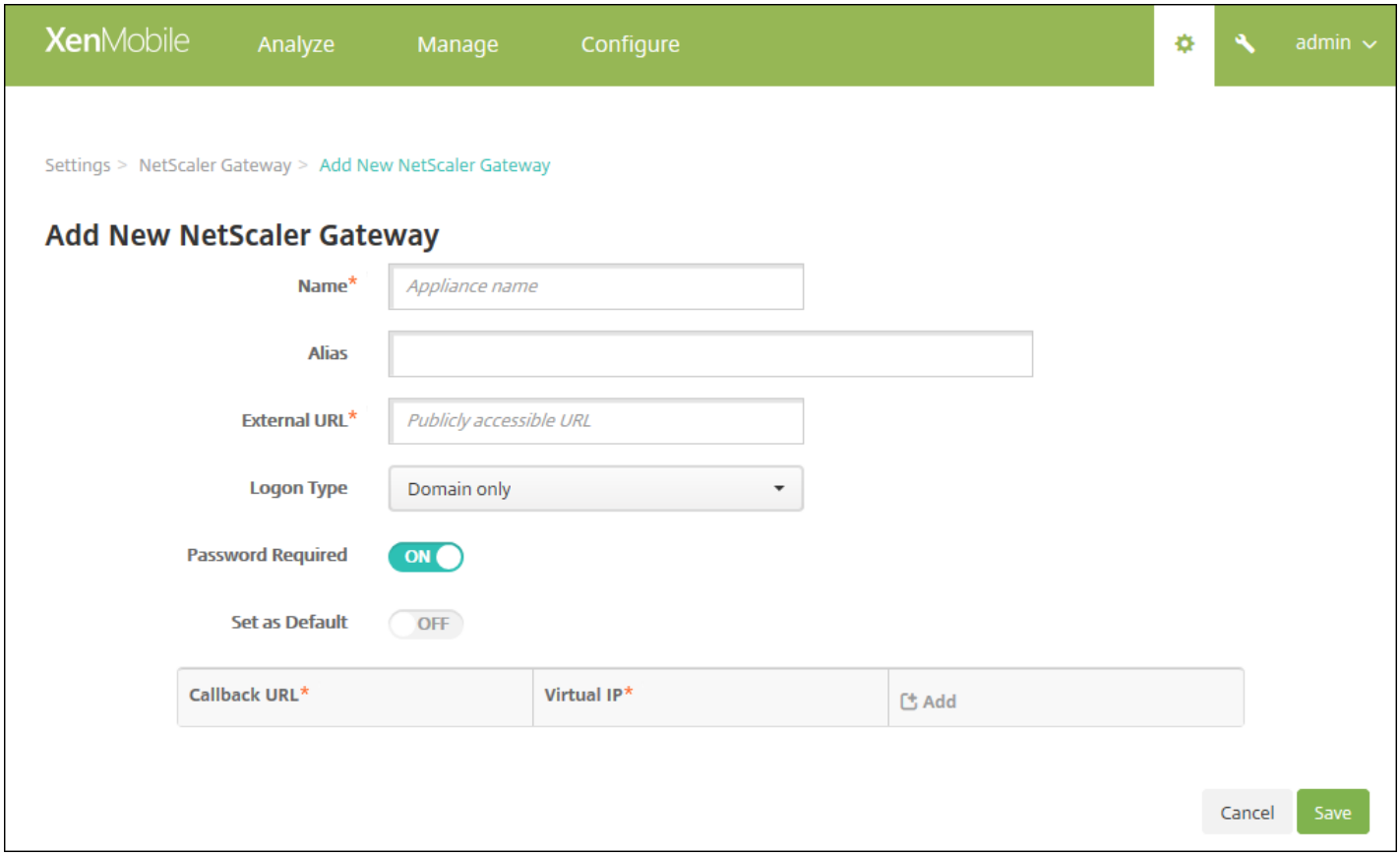
6. Click **Save**.

To add a new NetScaler Gateway instance

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.



4. Configure these settings:

- **Name**: Type a name for the NetScaler Gateway instance.
- **Alias**: optionally include an alias.
- **External URL**: Type the publicly accessible URL for NetScaler Gateway. For example, https://receiver.com.
- **Logon Type**: In the list, click 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 is **Domain only**.

  If you have multiple domains, **Domain only** will not work, you have to use **Certificate and domain**. For some options, for example, for **Domain only**, you cannot change the **Password** field.

  For this logon type, the field is always **ON**. In addition, the default values for the **Password Required** field change based on the **Logon Type** you select.

  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.
- **Password Required**: Select whether you want to require password authentication. The default is **ON**.
- **Set as Default**: Select whether to use this NetScaler Gateway as the default. The default is **OFF**.

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.

After adding the NetScaler Gateway instance, you can add a callback URL and specify a NetScaler Gateway VPN virtual IP address. **Note**: This is optional, but can be configured for additional security, especially when the XenMobile server is in the

DMZ.

1. In the NetScaler Gateway screen, select the NetScaler Gateway in the table, and click **Add**. The **Add New NetScaler Gateway** page appears.

2. In the table listing callback URLs, click **Add**.

3. Specify the Callback URL. This field represents the fully qualified domain name (FQDN) and verifies that the request originated from NetScaler Gateway. The callback URL must resolve to an IP address that is reachable from the XenMobile server, but does not have to be an external NetScaler Gateway URL.

4. Enter the NetScaler Gateway virtual IP address and then click **Save**.

Domain or domain plus security token authentication

Dec 14, 2016

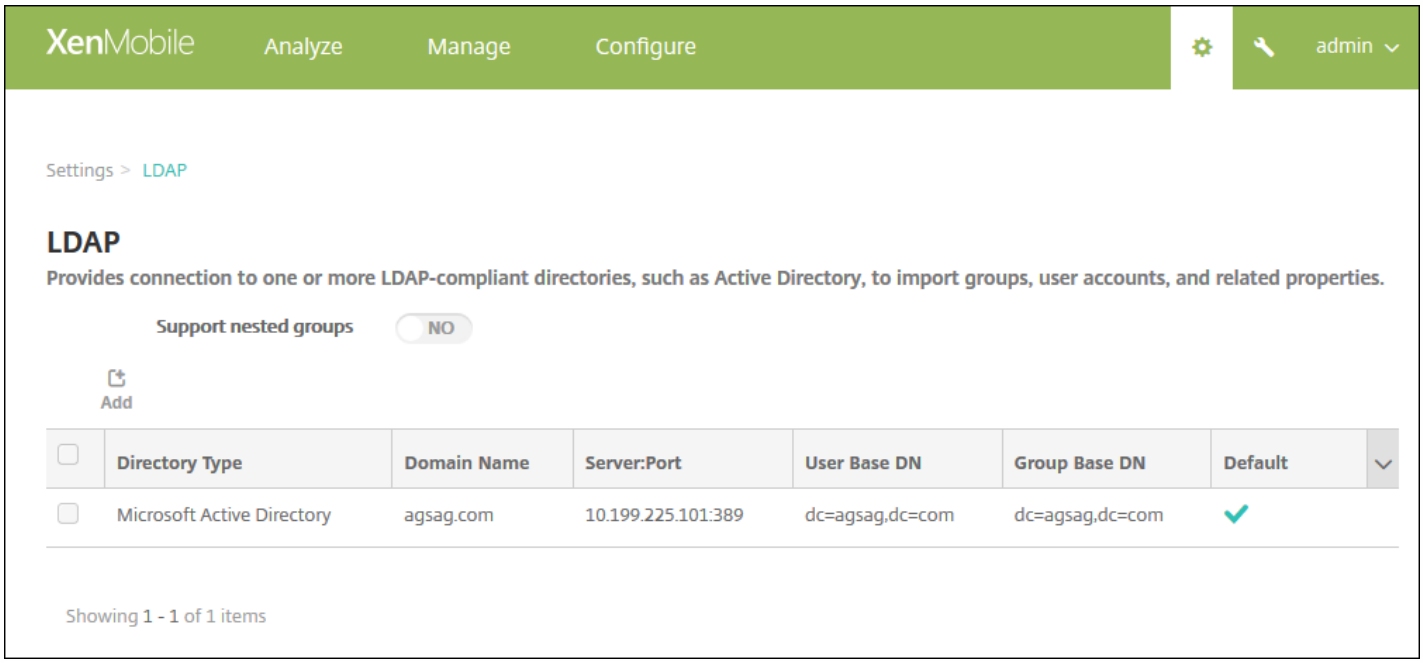
XenMobile supports domain-based authentication against one or more directories, such as Active Directory, that are compliant with the Lightweight Directory Access Protocol (LDAP). You can configure a connection in XenMobile to one or more directories and then use the LDAP configuration to import groups, 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.

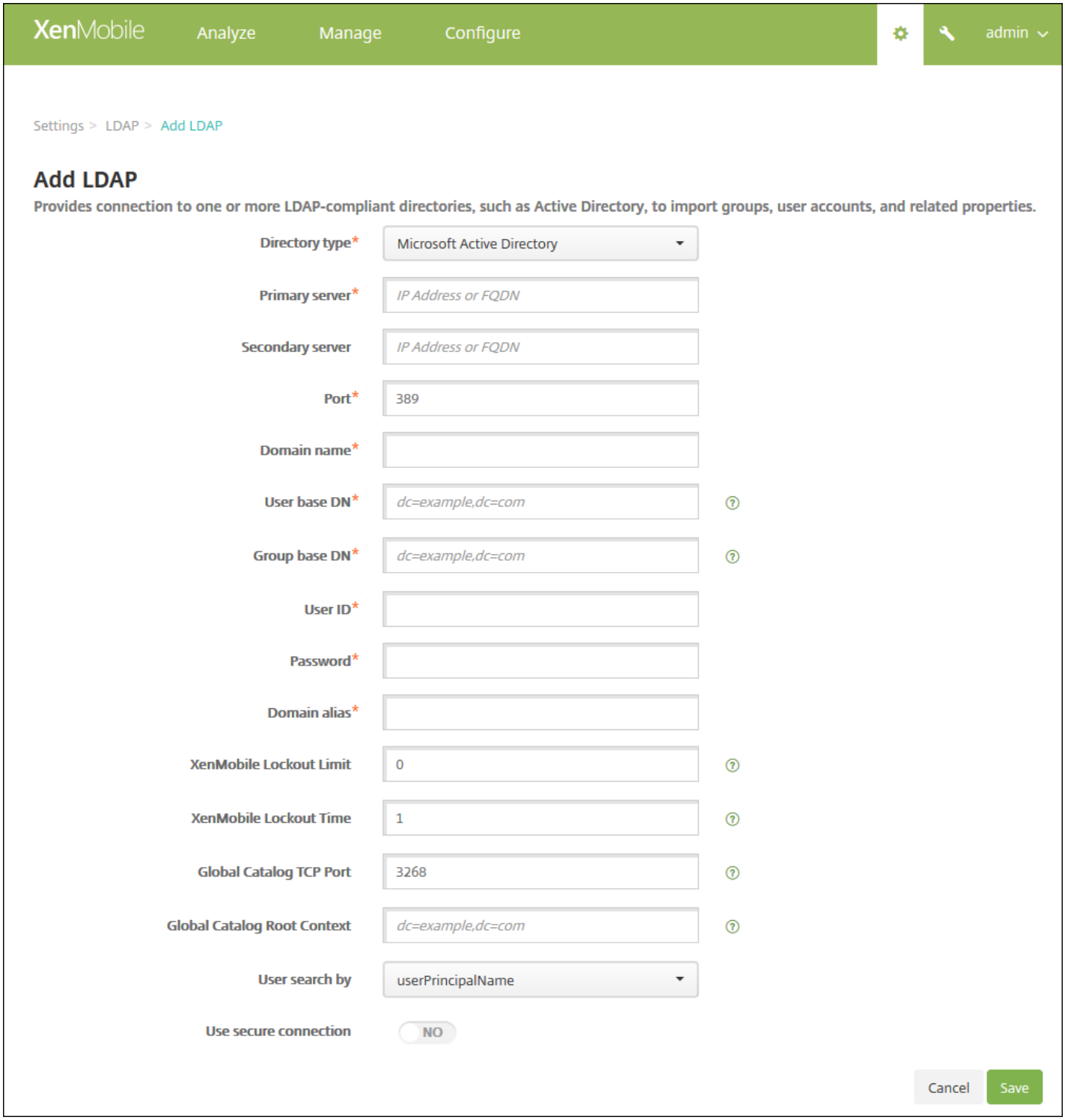
To add LDAP connections in XenMobile

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.



To add an LDAP-compliant directory

1. On the **LDAP** page, click **Add**. The **Add LDAP** page appears.



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**.

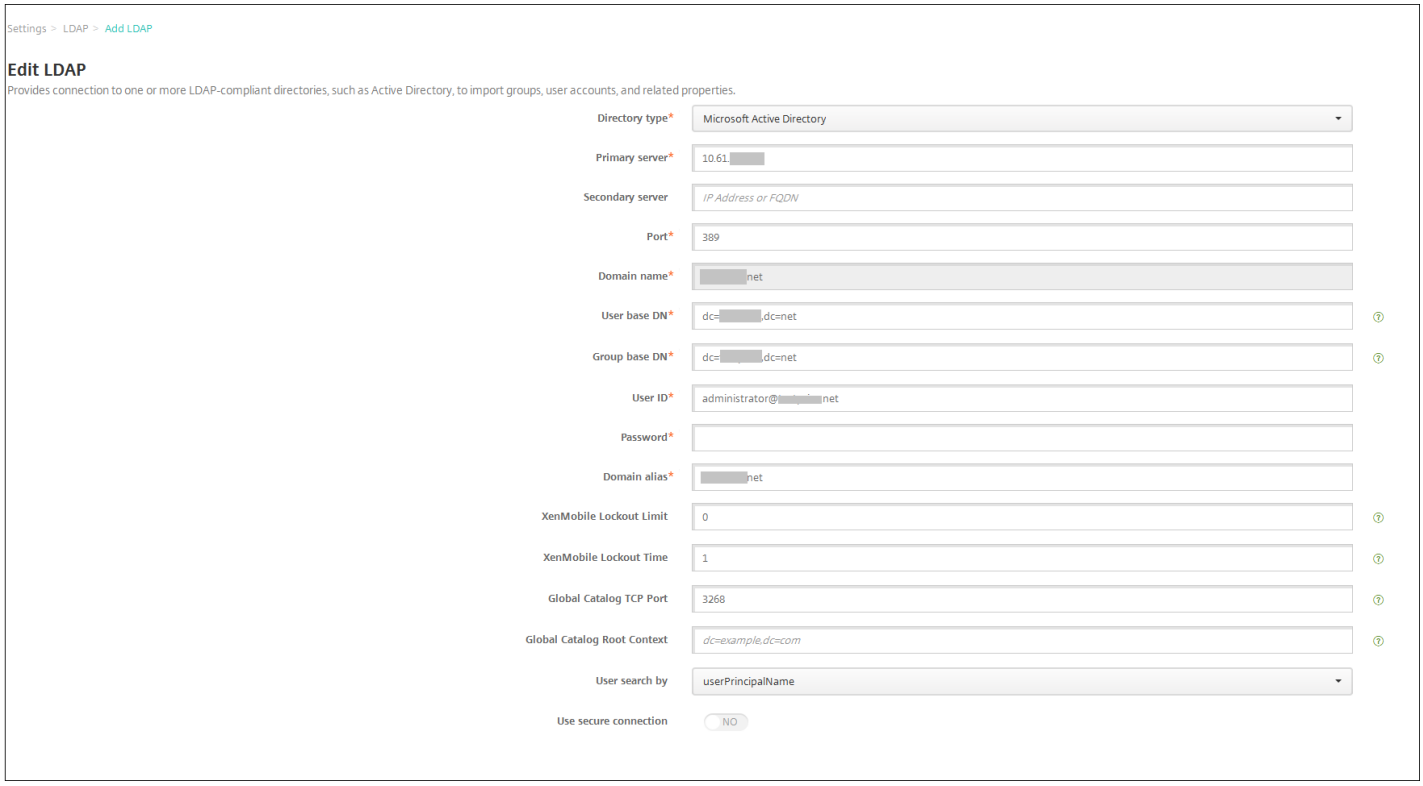
3. Click **Save**.

To edit an LDAP-compliant directory

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.



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 serve**r: 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.

To delete an LDAP-compliant directory

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.

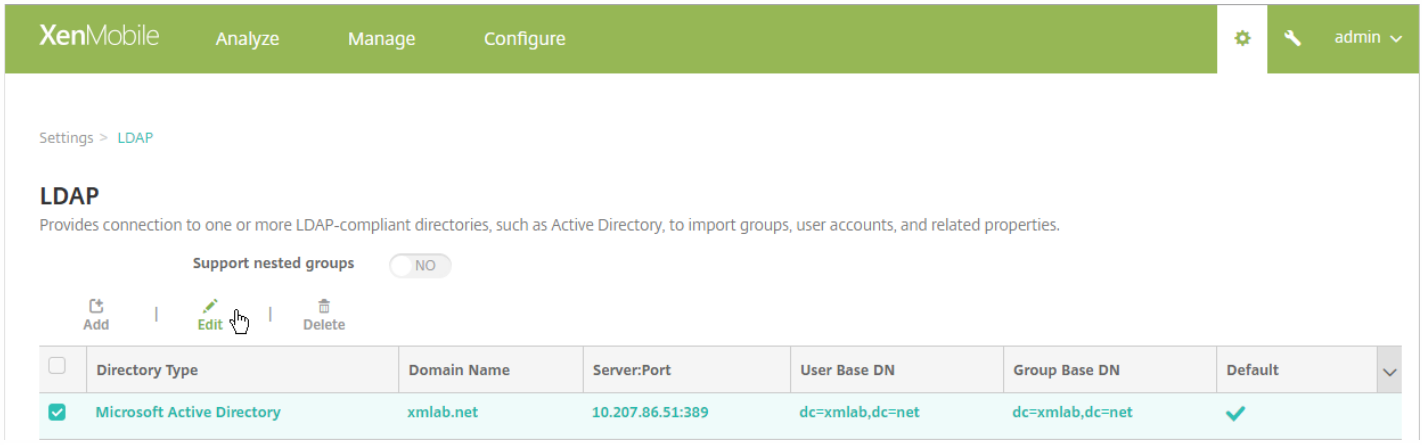
For optimal usability, you can combine this configuration with Citrix PIN and Active Directory password caching so users do not have to repeatedly enter their Active Directory user names and passwords. Users will need to enter user names and passwords for enrollment, password expiration, and account lockout.

Configure LDAP settings

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.

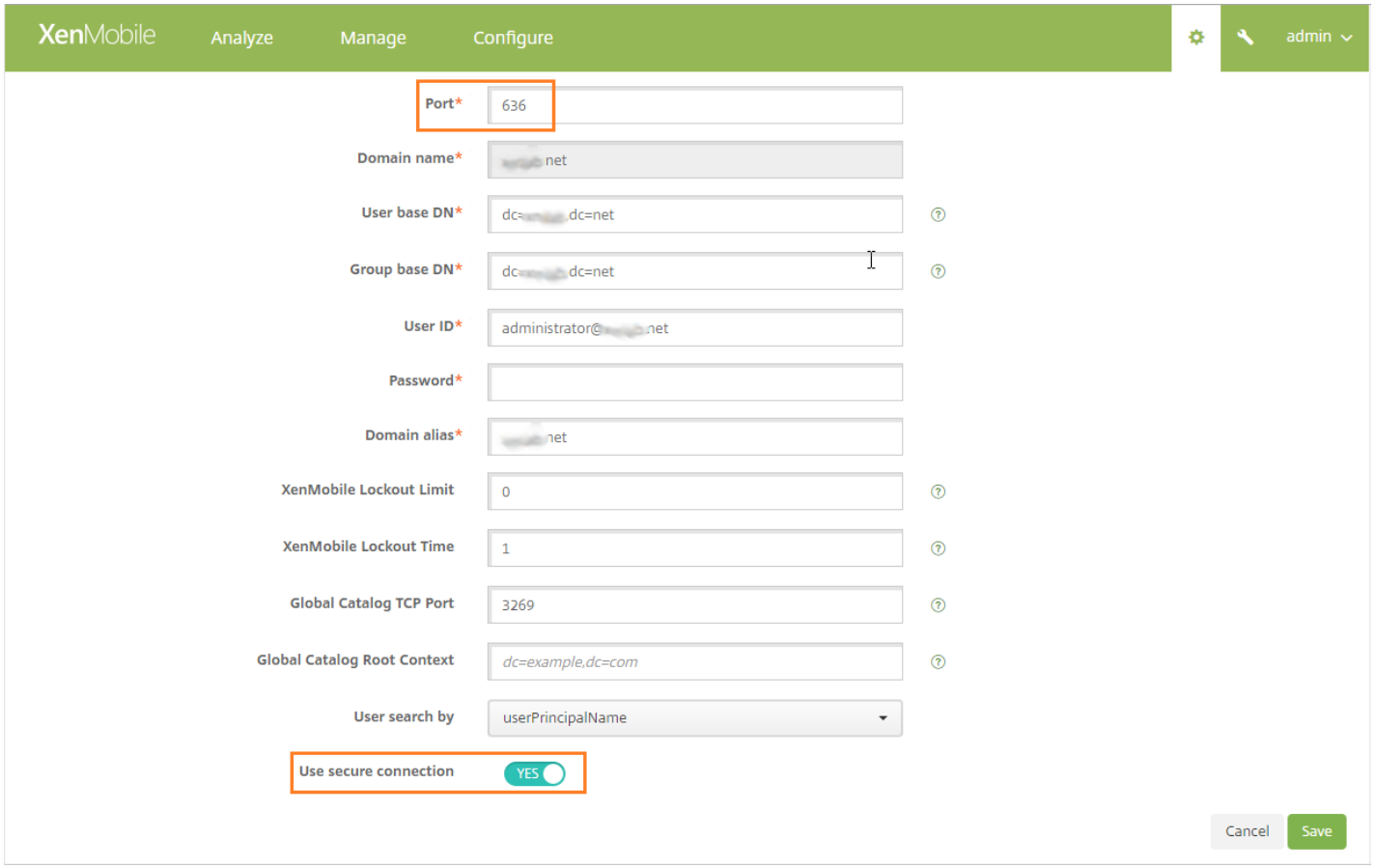
1. In **Settings**, click **LDAP**.

2. Select **Microsoft Active Directory** and then click **Edit**.



3. Verify that the Port is 636, which is for secure LDAP connections, or 3269 for Microsoft secure LDAP connections.

4. Change **Use secure connection** to **Yes**.



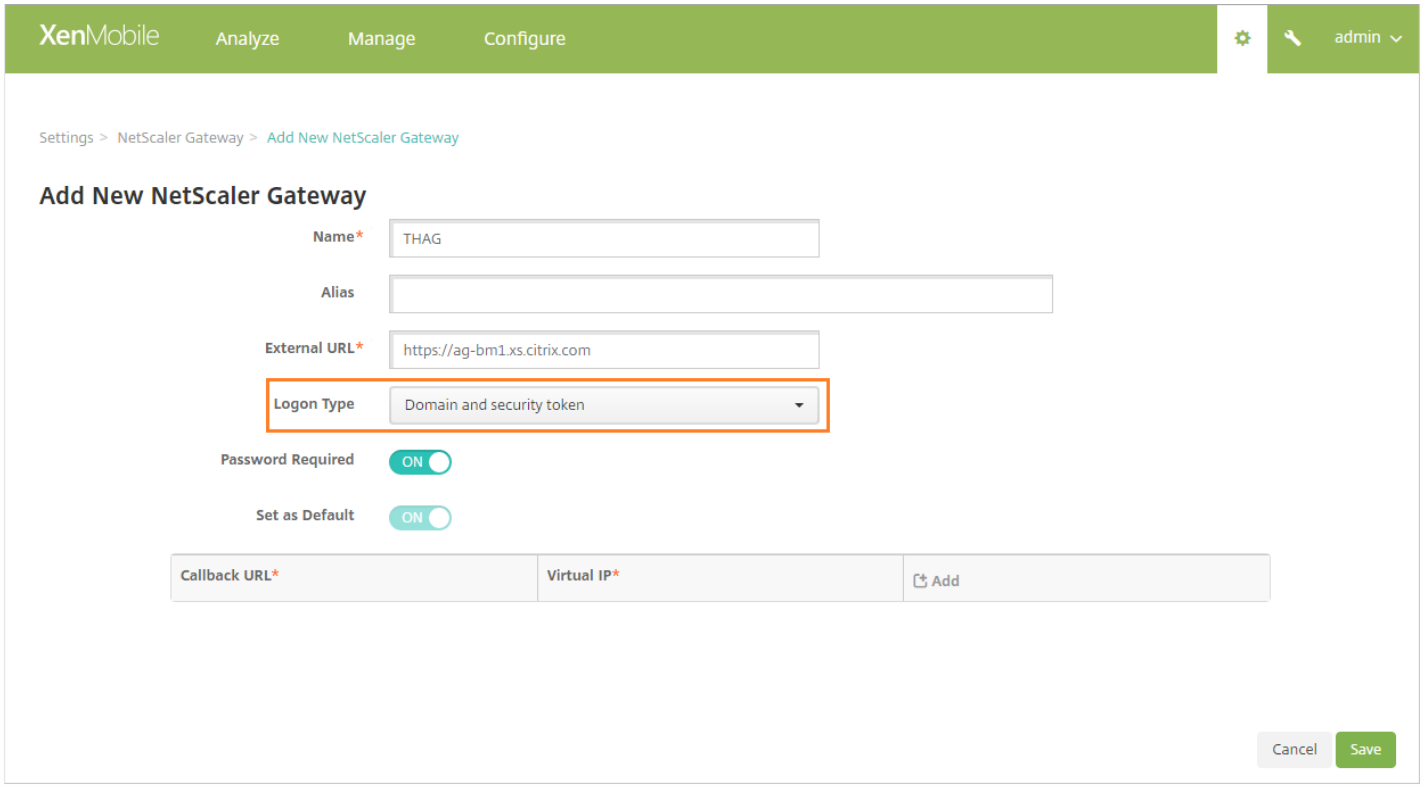
Configure NetScaler Gateway settings

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**.



Enable Worx PIN and user password caching

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

Configure NetScaler Gateway for domain and security token authentication

Configure NetScaler Gateway session profiles and policies for your virtual servers used with XenMobile. For information, see Configuring Domain and Security Token Authentication for XenMobile in the NetScaler Gateway documentation.

Client certificate or certificate plus domain authentication

Feb 16, 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.

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

- 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.

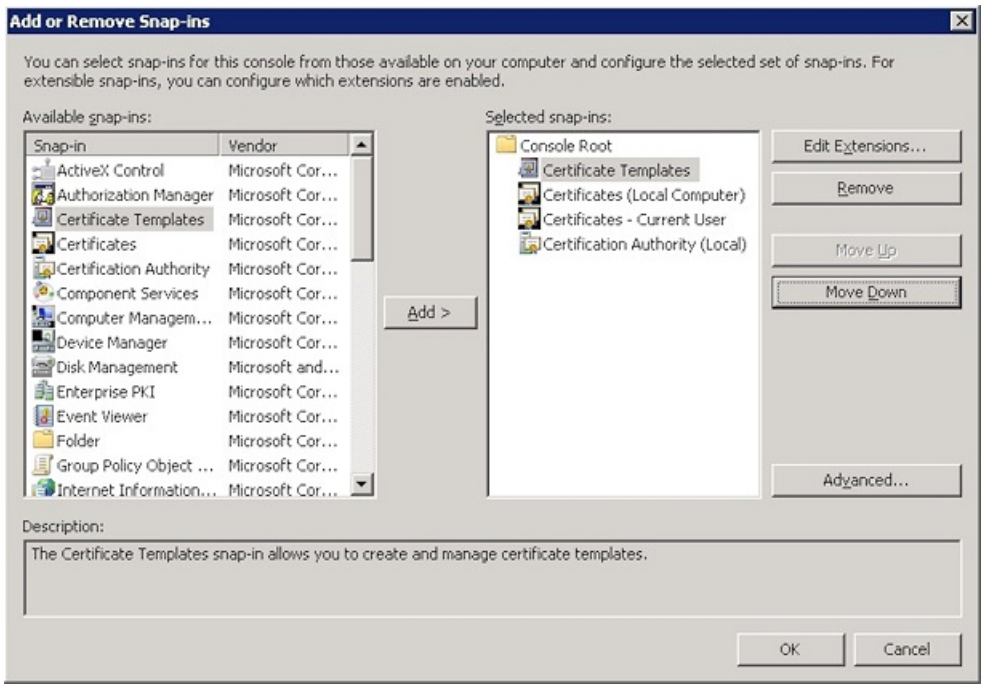
- To configure Certificate-based Authentication for Exchange ActiveSync, see this Microsoft blog.
- If you are using private server certificates to secure the ActiveSync traffic to the Exchange Server, ensure that the mobile devices have all of the Root/Intermediate certificates. Otherwise, certificate-based 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 for iOS, Android, and Windows Phone is wrapped with the latest MDX Toolkit.

Adding a certificate snap-in to the Microsoft Management Console

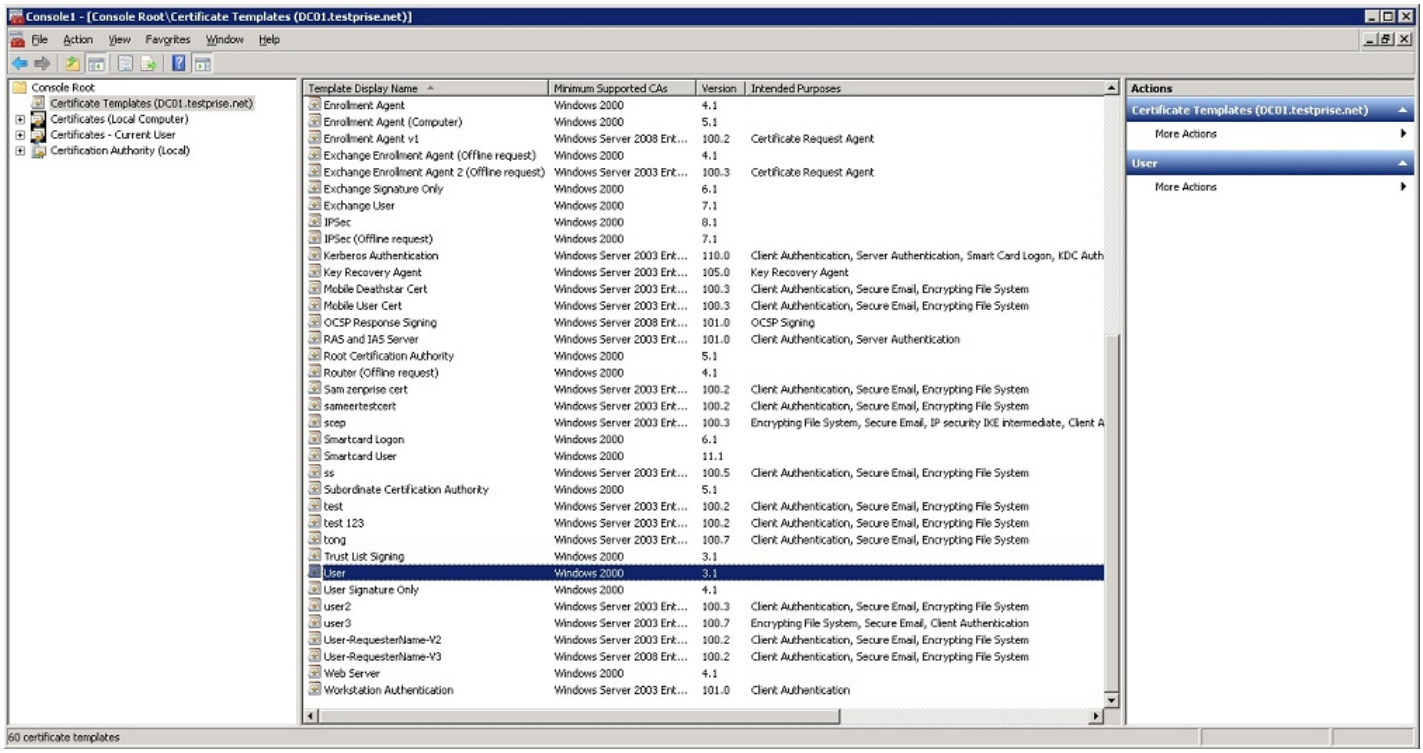
1. Open the console and then click **Add/Remove Snap-Ins**.

2. Add the following snap-ins:

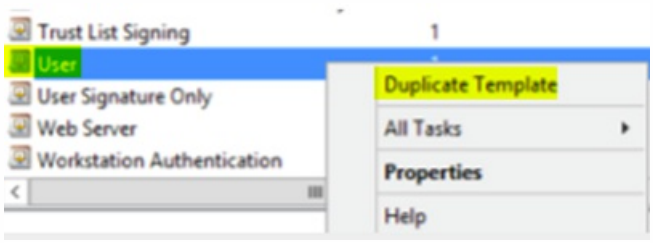
Certificate Templates
Certificates (Local Computer)
Certificates - Current User
Certificate Authority (Local)



3. Expand **Certificate Templates**.



4. Select the **User** template and **Duplicate Template**.

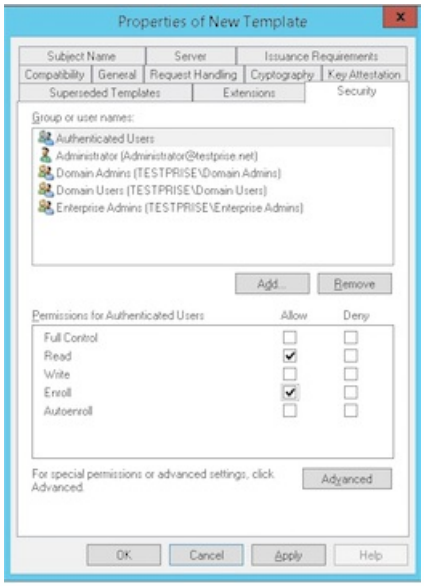


5. Provide the Template display name.

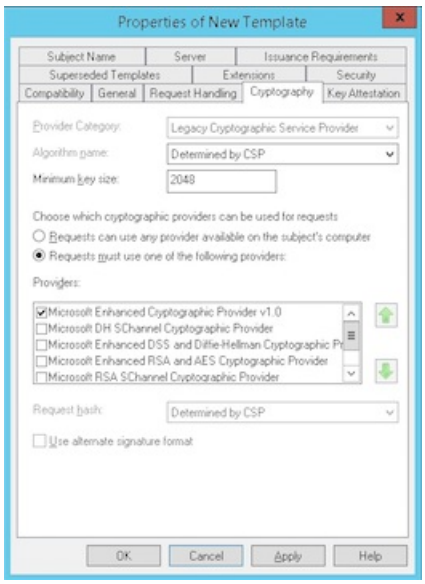
> **Important:** Do not select the **Publish certificate in Active Directory** check box unless required. If this option is selected, all user client certificates will be pushed/created in Active Directory, which might clutter your Active Directory database.

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**.

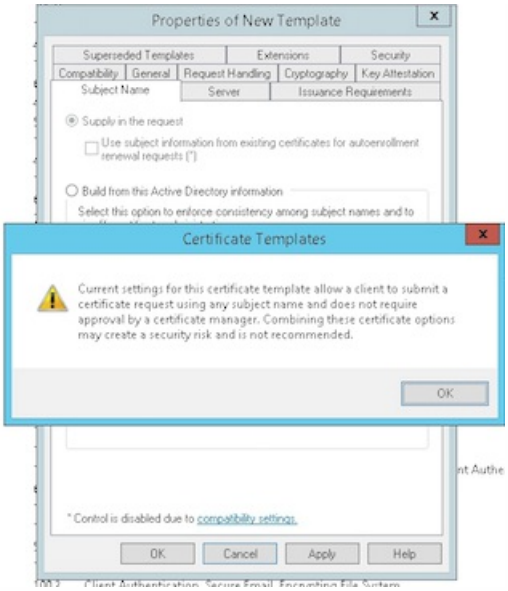
7. Under **Security**, select the **Enroll** option in the **Allow** column for the authenticated users.



8. Under **Cryptography**, make sure you provide the key size, which you will need to enter during XenMobile configuration.



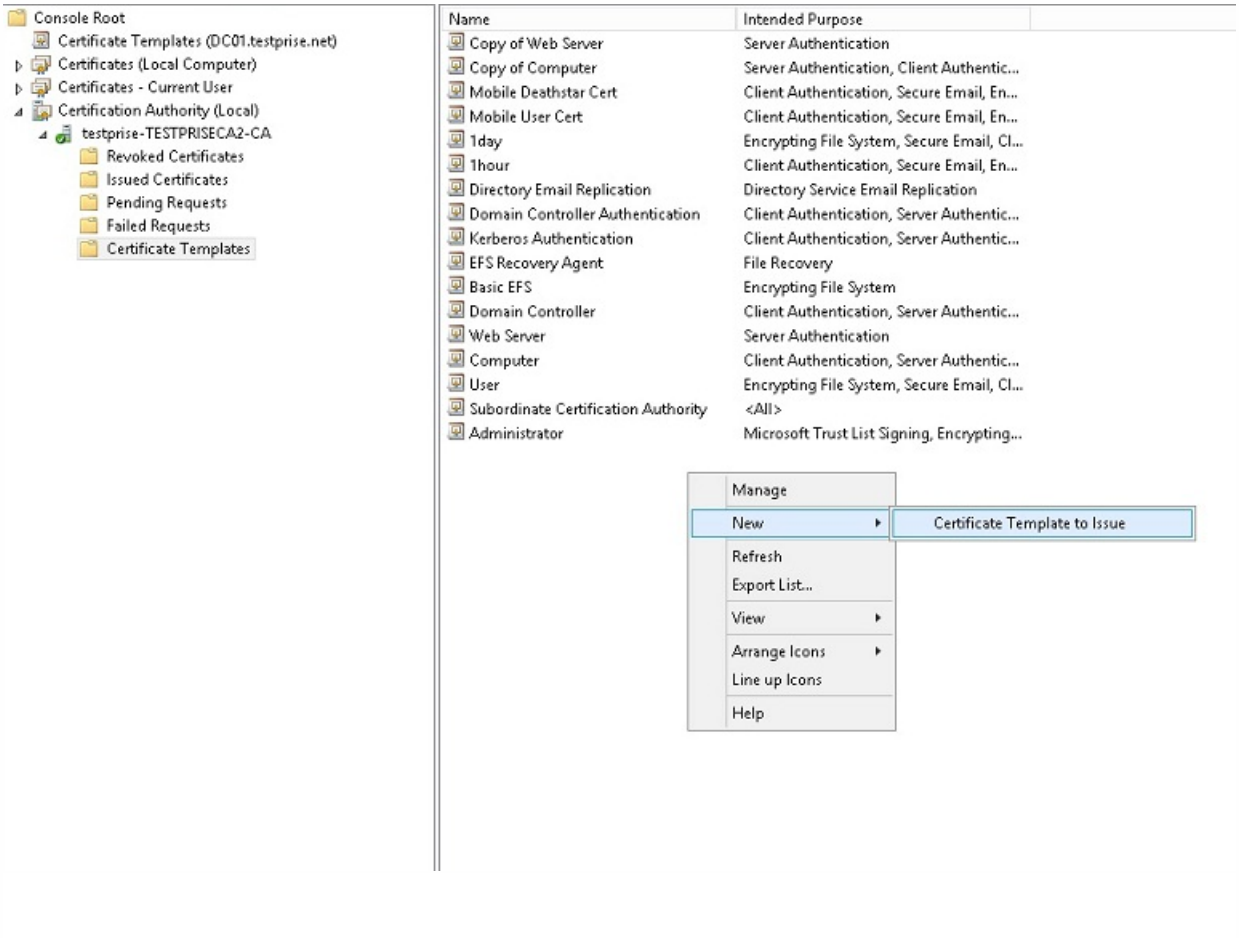
9. Under **Subject Name**, select **Supply in the request**. Apply the changes and then save.



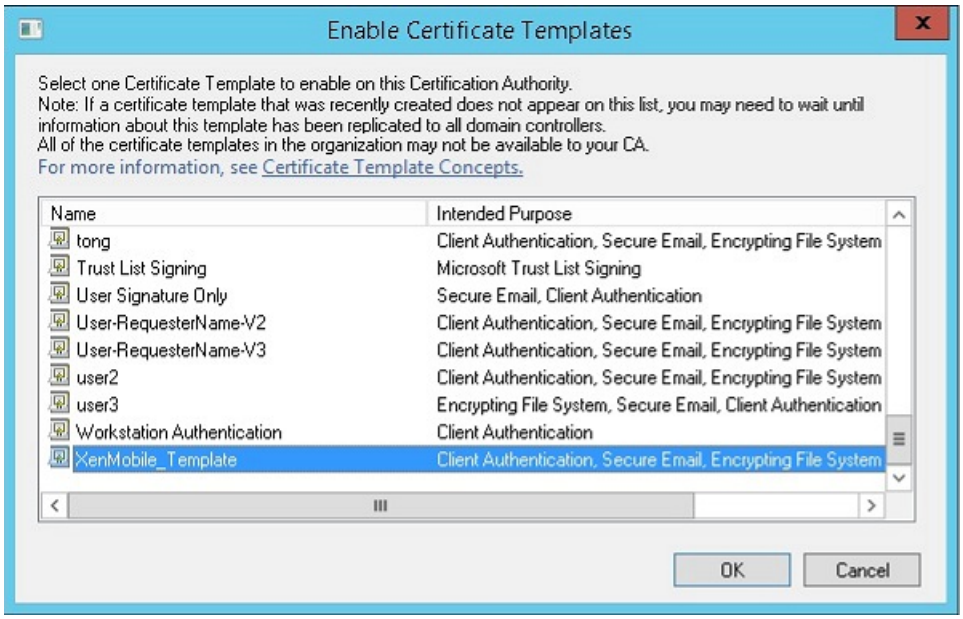
Adding the template to Certificate Authority

1. Go to **Certificate Authority** and select **Certificate Templates**.

2. Right-click in the right pane and then select **New > Certificate Template to Issue**.



3. Select the template you created in the previous step and then click **OK** to add it into the **Certificate Authority**.

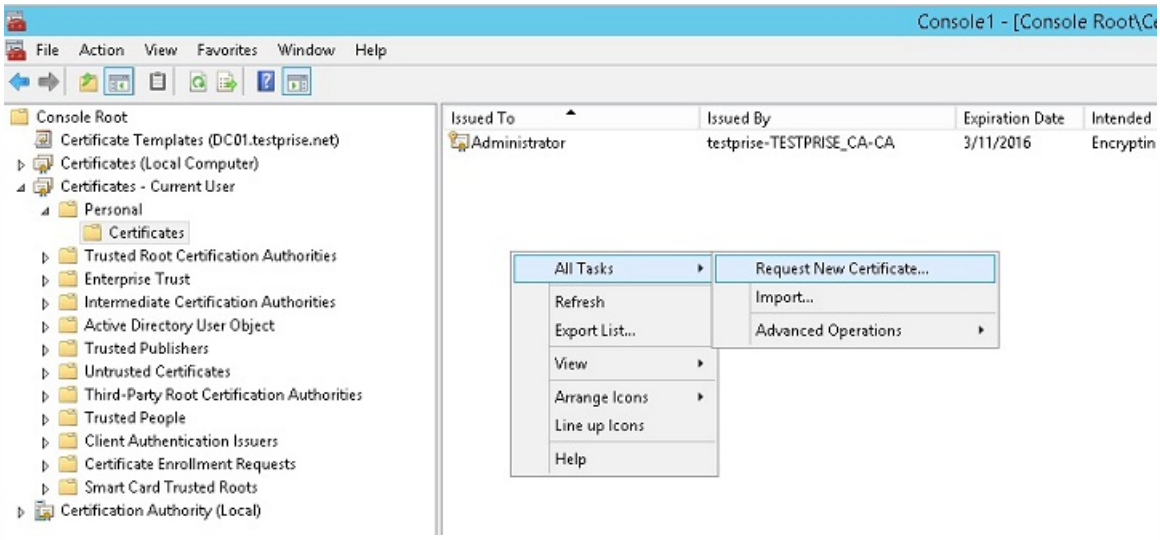


Creating a PFX certificate from the CA server

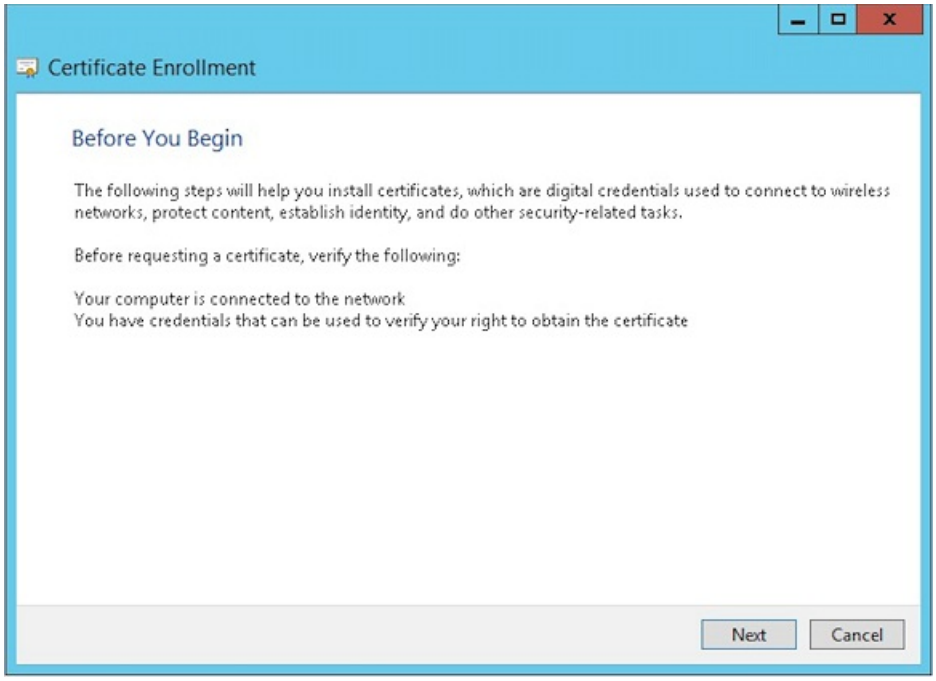
1. Create a user .pfx cert using the service account with which you logged in. This .pfx will be uploaded into XenMobile, which will request a user certificate on behalf of the users who enroll their devices.

2. Under **Current User**, expand **Certificates**.

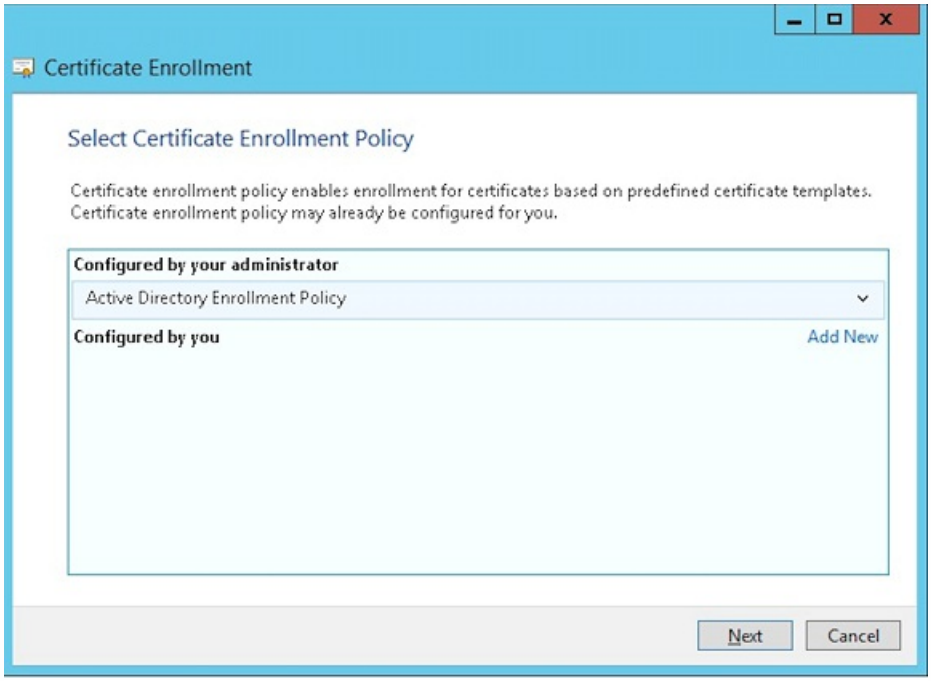
3. Right-click in the right pane and then click **Request New Certificate**.



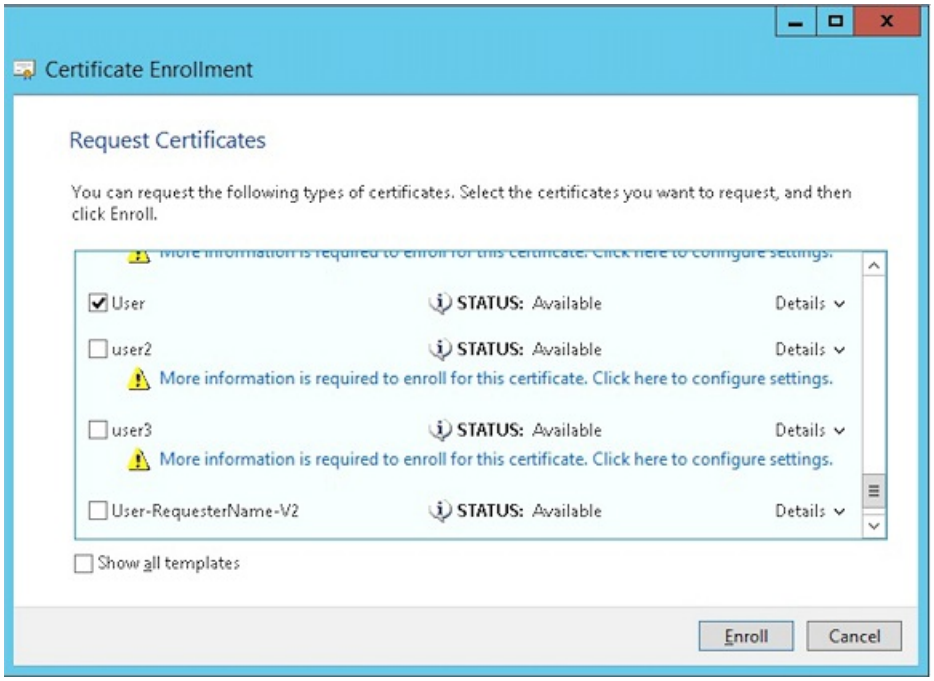
4. The **Certificate Enrollment** screen appears. Click **Next**.



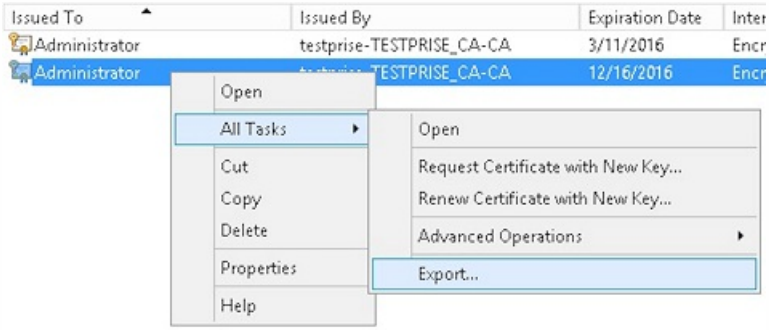
5. Select **Active Directory Enrollment Policy** and then click **Next**.



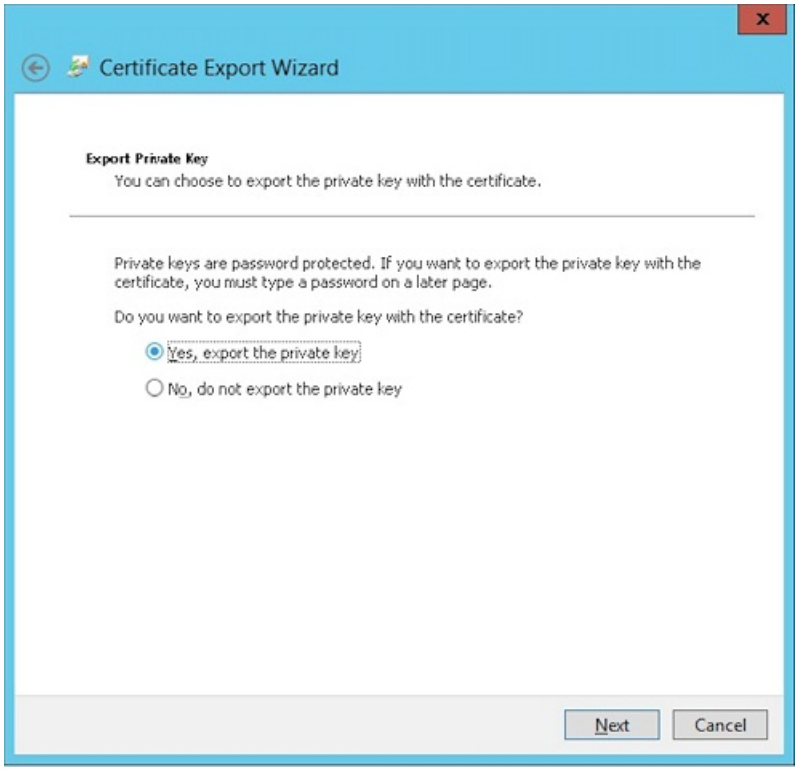
6. Select the **User** template and then click **Enroll**.



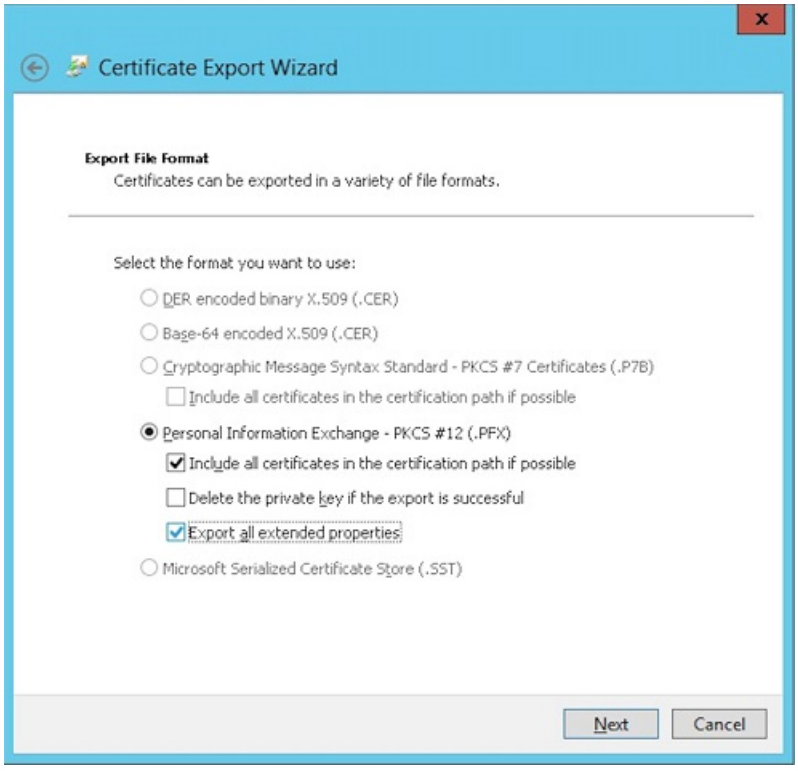
7. Export the .pfx file that you created in the previous step.



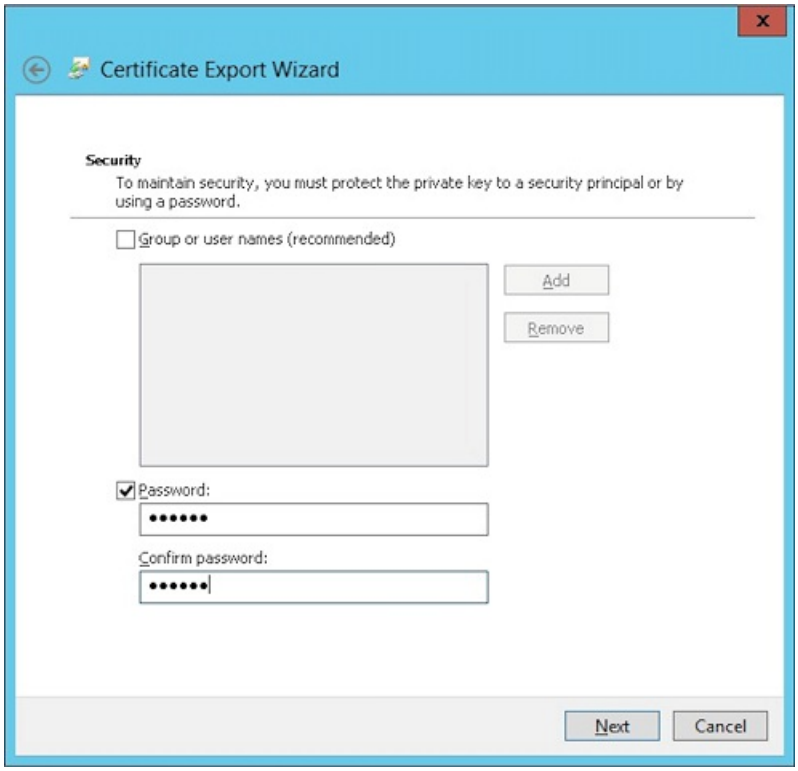
8. Click **Yes, export the private key**.



9. Select **Include all certificates in the certification path if possible** and select the **Export all extended properties** check box.



10. Set a password that you'll use when uploading this certificate into XenMobile.



11. Save the certificate onto your hard drive.

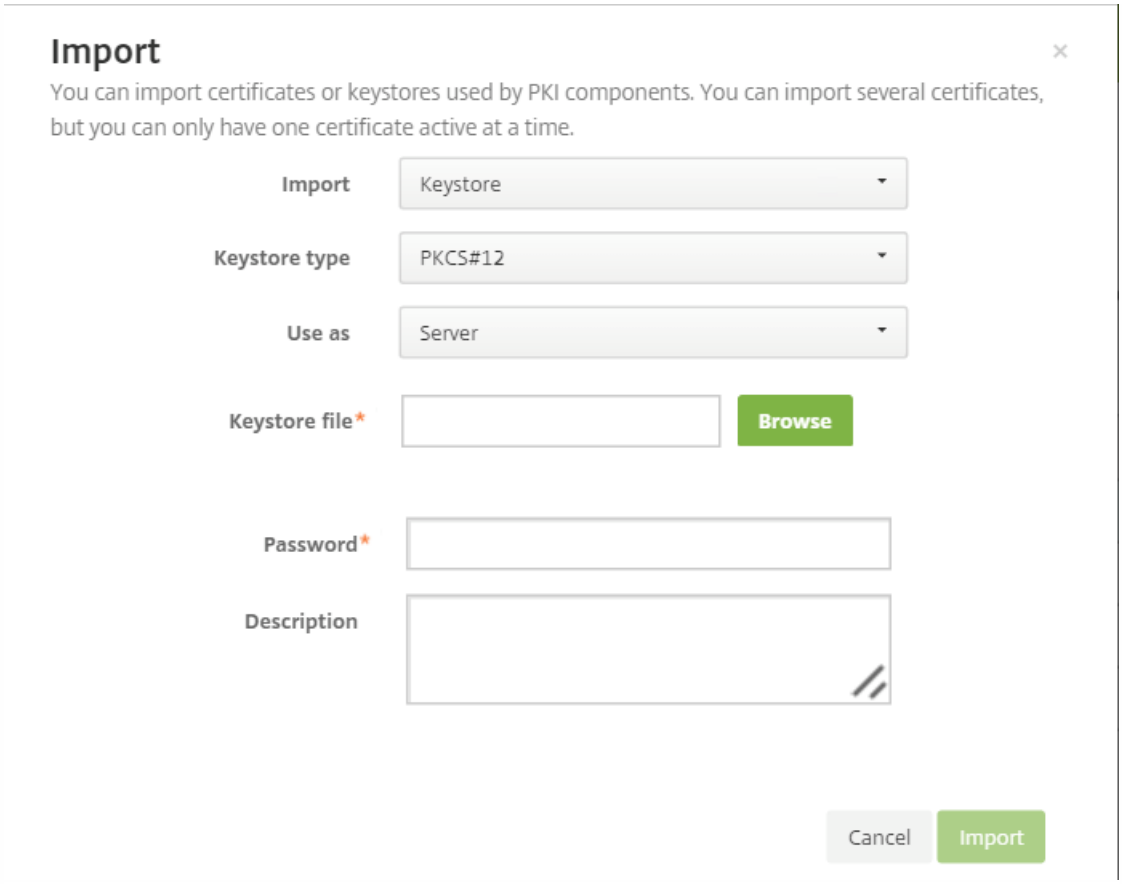
Uploading the certificate to XenMobile

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.



4. Click **Import**.

5. Verify that the certificate installed correctly. It should display as a User certificate.

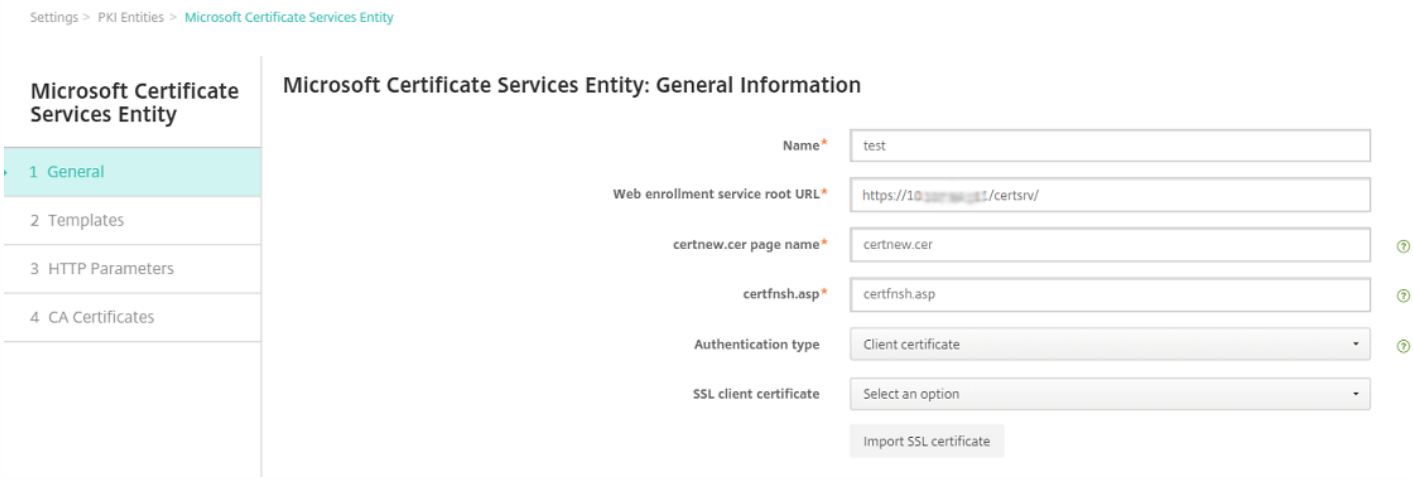
Creating the PKI entity for certificate-based authentication

1. In **Settings**, go to **More > Certificate Management > PKI Entities**.

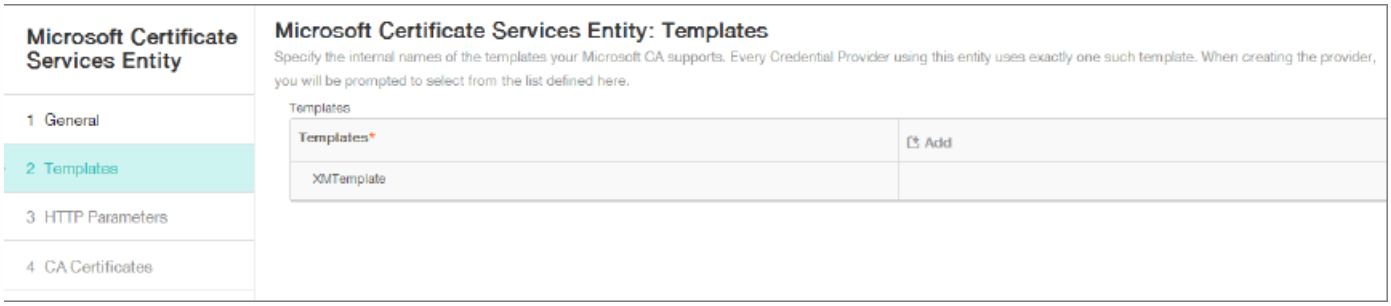
2. Click **Add** and then click **Microsoft Certificate Services Entity**. The **Microsoft Certificate Services Entity: General Information** screen appears.

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.

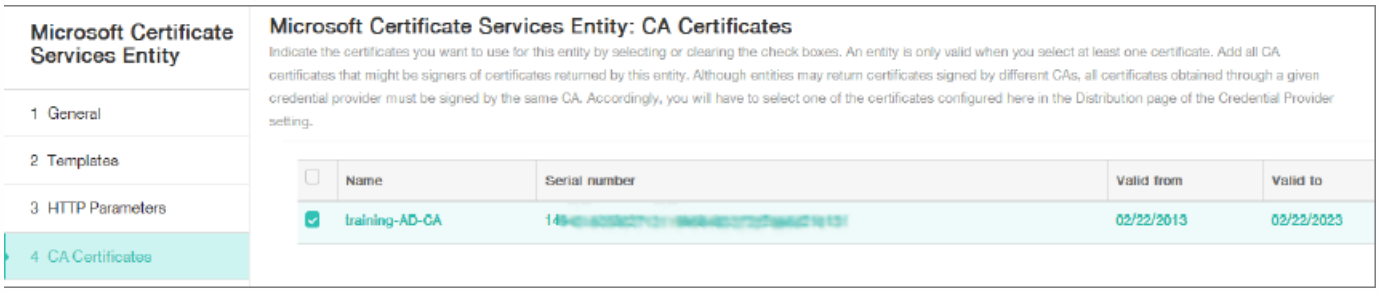


4. Under **Templates**, add the template that you created when configuring the Microsoft certificate. Be sure not to add spaces.



5. Skip HTTP Parameters and then click **CA Certificates**.

6. Select the root CA name that corresponds to your environment. This root CA is part of the chain imported from the XenMobile client certificate.



7. Click **Save**.

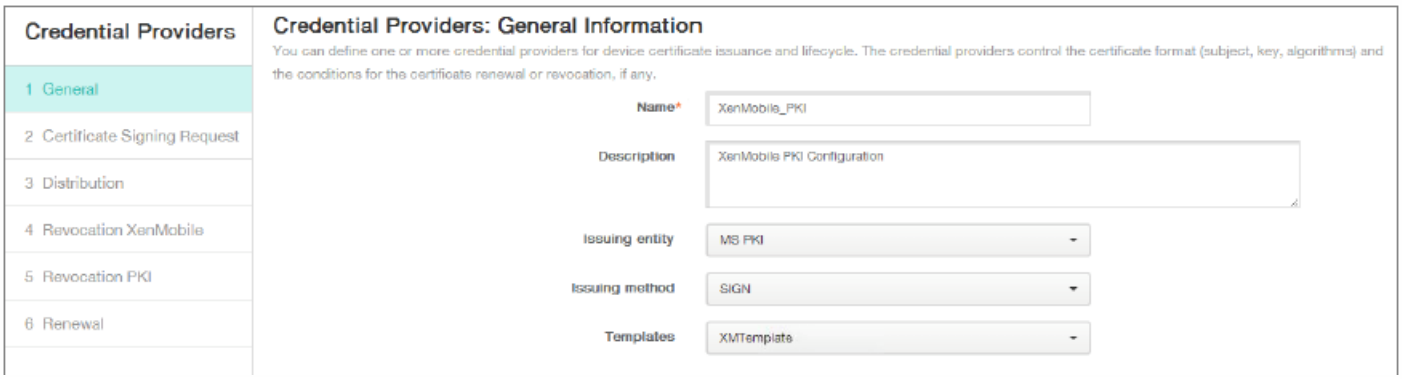
Configuring credentials providers

1. In **Settings**, go to **More > Certificate Management > Credential Providers**.

2. Click **Add**.

3. Under **General**, enter the following parameters:

- **Name**: Type any name.
- **Description**: Type any description.
- **Issuing entity**: Select the PKI entity created earlier.
- **Issuing method**: SIGN
- **Templates**: Select the template added under the PKI entity.



4. Click **Certificate Signing Request** and then enter the following parameters:

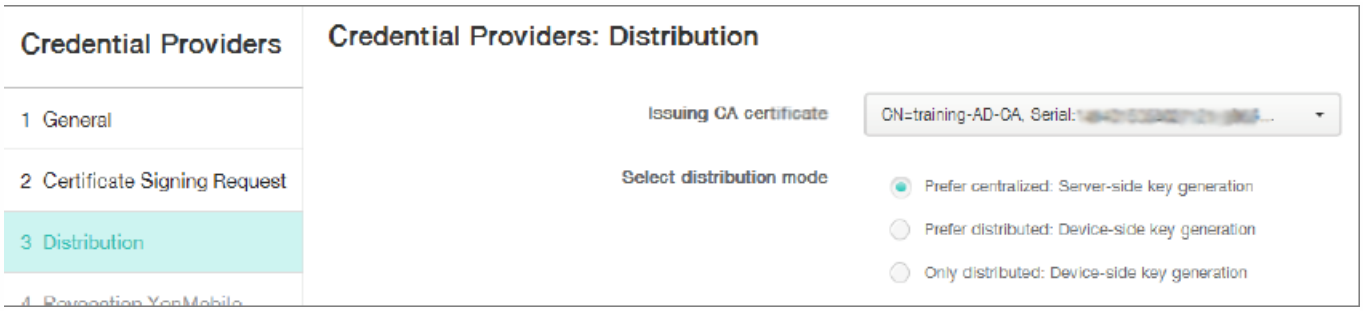
- **Key algorithm**: RSA
- **Key size**: 2048
- **Signature algorithm**: SHA1withRSA
- **Subject name**: cn=$user.username

For **Subject Alternative Names**, click **Add** and then enter the following parameters:

- **Type**: User Principal name
- **Value**: $user.userprincipalname

5. Click **Distribution** and enter the following parameters:

- **Issuing CA certificate**: Select the Issuing CA that signed the XenMobile Client Certificate.
- **Select distribution mode**: Select **Prefer centralized: Server-side key generation**.

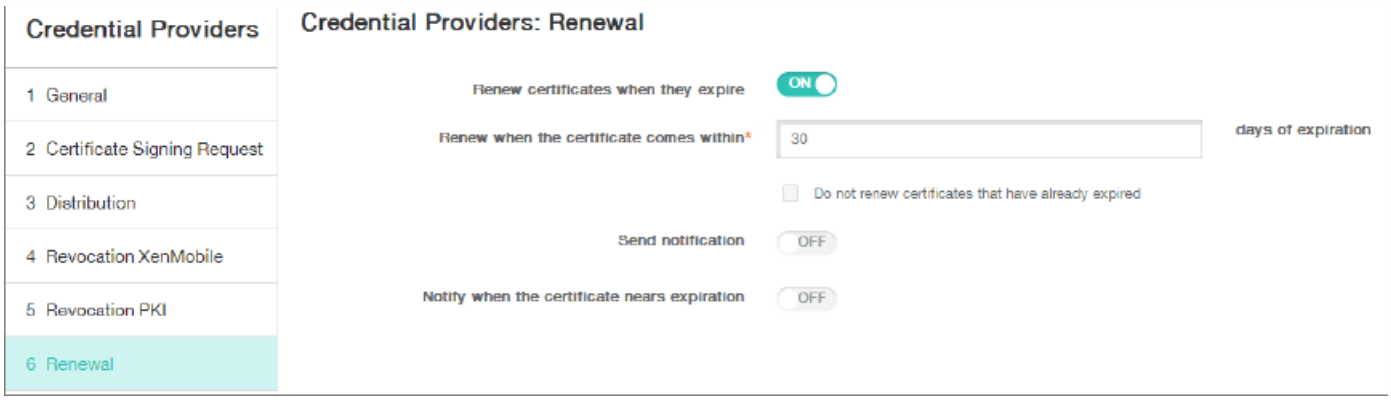


6. For the next two sections -- **Revocation XenMobile** and **Revocation PKI** -- set the parameters as required. For the purpose of this article, both options are skipped.

7. Click **Renewal**.

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

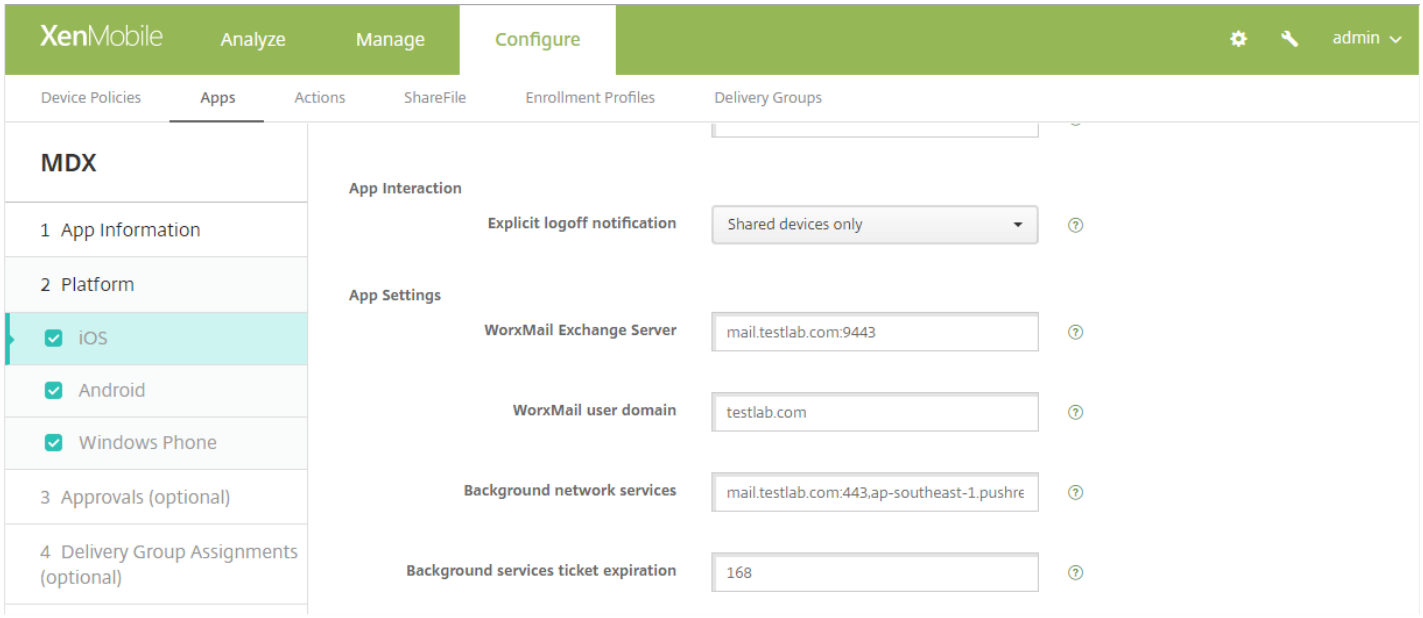
9. Leave all other settings as default or change them as required.



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**.



Configuring NetScaler certificate delivery in XenMobile

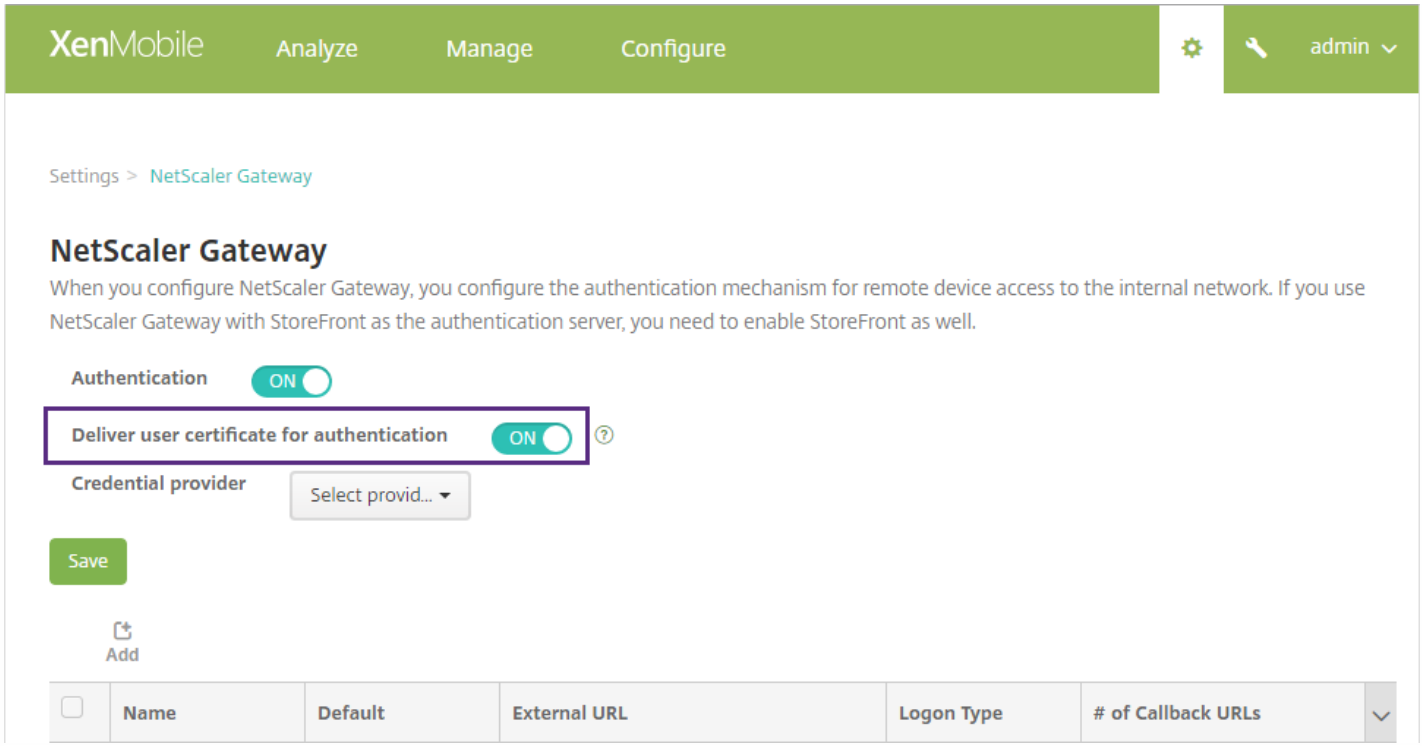
1. Log on to the XenMobile console and click the gear icon in the upper-right corner. The **Settings** screen appears.

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

3. If NetScaler Gateway isn't already added, click **Add** and specify the settings:

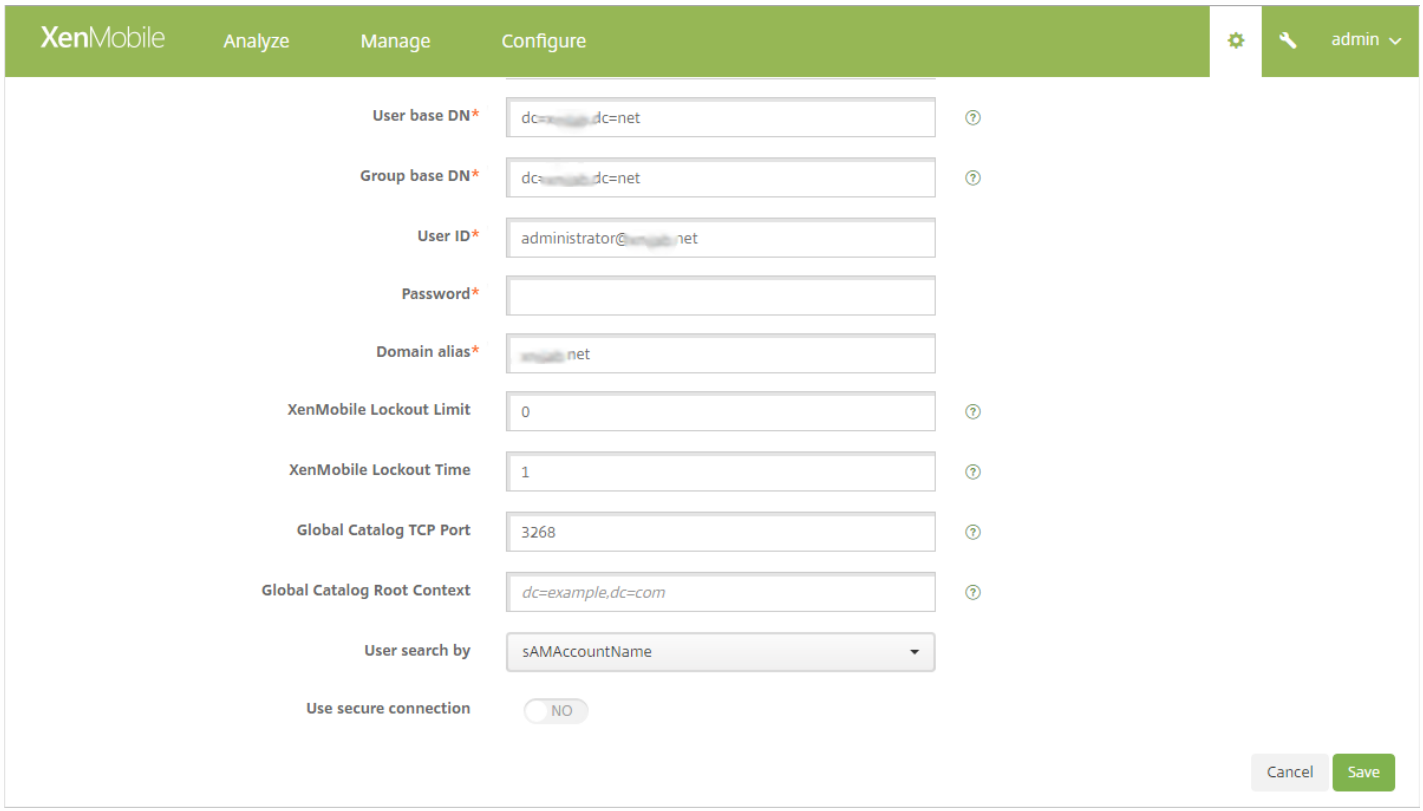
- **External URL**: https://YourNetScalerGatewayURL
- **Logon Type**: Certificate
- **Password Required**: OFF
- **Set as Default**: ON

4. For **Deliver user certificate for authentication**, select **On**.



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**.



Creating an Enterprise Hub policy for Windows Phone 8.1 and 10

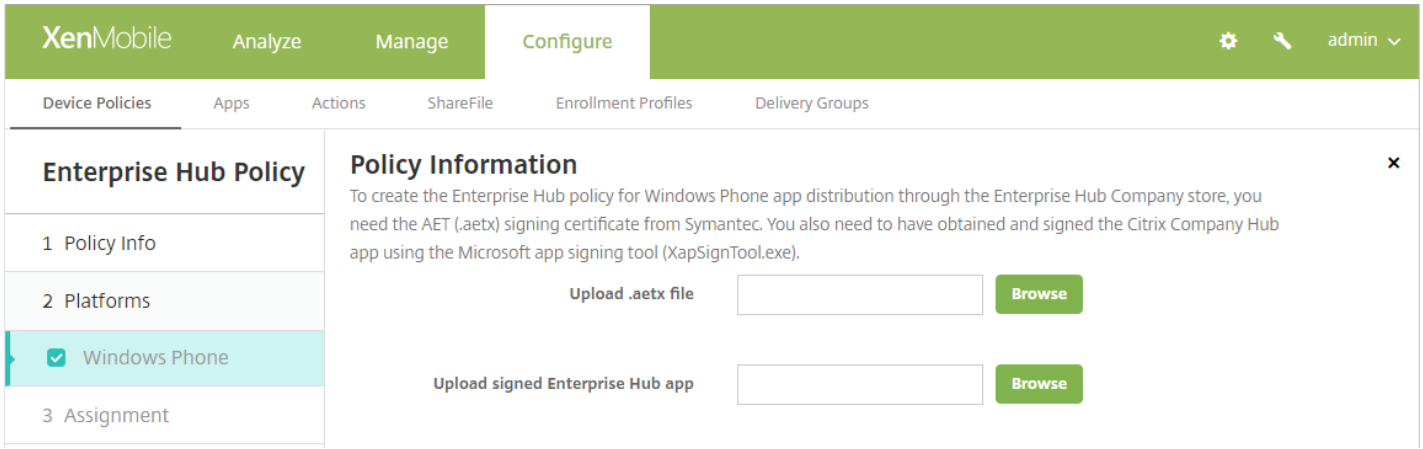
For Windows Phone devices, you must create an Enterprise Hub device policy to deliver the AETX file and the Secure Hub client.

> **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.



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.

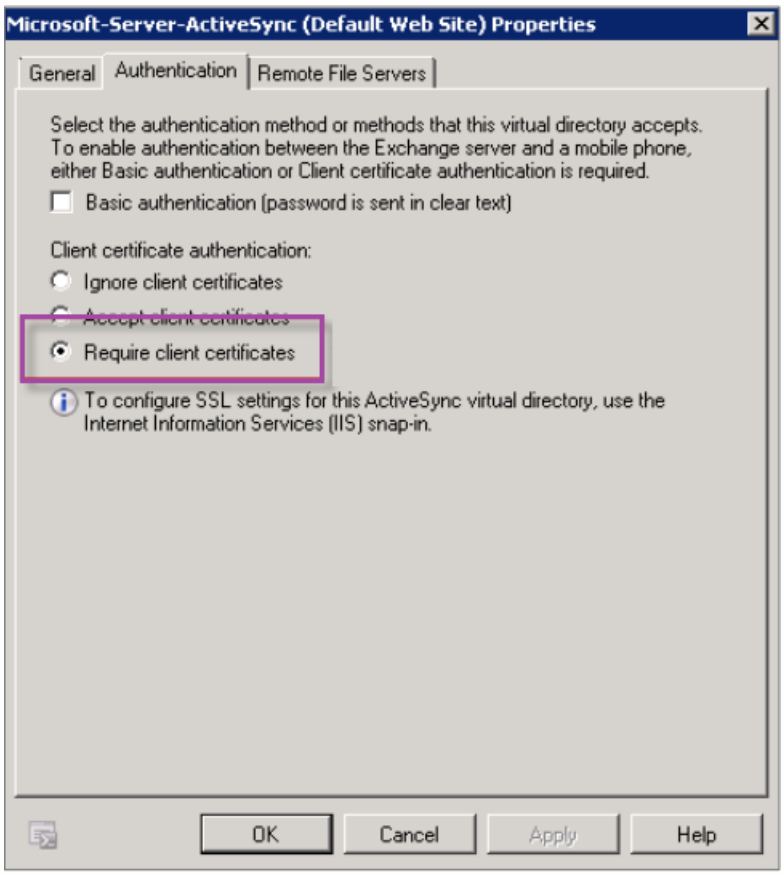
4. When users start Secure Mail for iOS, Android or Windows Phone 8.1, XenMobile will not prompt them for user

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.

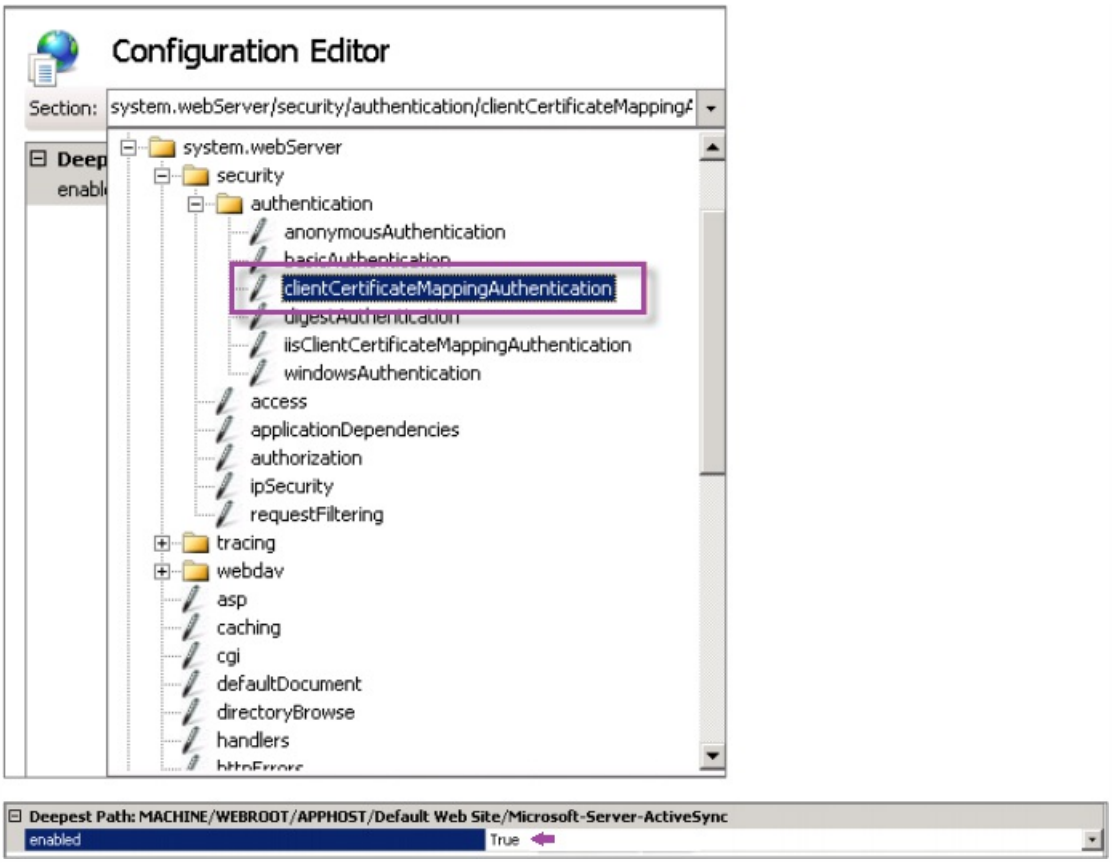
If users can download and install Secure Mail, but during the mailbox configuration Secure Mail fails to finish the configuration:

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**.



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**.



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

Jan 03, 2017

A XenMobile Public Key Infrastructure (PKI) entity configuration represents a component performing actual PKI operations (issuance, revocation, and status information). These components may either be internal to XenMobile, in which case they are called discretionary, or external to XenMobile if they are part of your corporate infrastructure.

XenMobile supports the following types of PKI entities:

- Discretionary Certificate Authorities (CAs)
- Generic PKIs (GPKIs)
- Microsoft Certificate Services

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.

About CA Certificates

When you configure a PKI entity, you must indicate to XenMobile which CA certificate is going to be the signer of certificates issued by (or recovered from) that entity. One and the same PKI entity may return (fetched or newly signed) certificates signed by any number of different CAs. You must provide the certificate of each of these CAs as part of the PKI entity configuration. To do so, you upload the certificates to XenMobile and then reference them in the PKI entity. For discretionary CAs, the certificate is implicitly the signing CA certificate, but for external entities, you must specify the certificate manually.

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 is capable of taking CSRs, transmitting them to the PKI, and returning newly signed certificates.
- fetch: The adapter is capable of retrieving (recovering) existing certificates and key pairs (depending on input parameters) from the PKI.
- revoke: The adapter is able to 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. In other words, there is a GPKI adapter for RSA, another for EnTrust, and so on.

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 are defined by the GPKI adapter for a specific operation and for which you need to provide values to XenMobile. XenMobile determines which operations the adapter supports (which capabilities it has) and which parameters the adapter requires for each of the operations by parsing the WSDL file. If you choose, use SSL client authentication to secure the connection between XenMobile and the GPKI adapter.

To add a generic PKI

1. In the XenMobile console, click **Configure** > **Settings** > **More** > **PKI Entities**.

2. On the **PKI Entities** page, click **Add**.

A list showing the types of PKI entities you can add appears.

3. Click **Generic PKI Entity**.

The Generic PKI Entity: General Information page appears.

4. On the **Generic PKI Entity: General Information** page, do the following:

- **Name**: Type a descriptive name for the PKI entity.
- **WSDL URL**: Type the location of the WSDL describing the adapter.
- **Authentication type**: Click the authentication method you want to use.
- **None**
- **HTTP Basic**: Provide the user name and password needed 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, all certificates obtained through a given certificate provider must be signed by the same CA. Accordingly, 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.

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.

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.

To add a Microsoft Certificate Services entity

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 list showing the types of PKI entities you can add 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, do the following:

- Name: Type a name for your new entity, which you will 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: Click the authentication method you want to use.
- None
- HTTP Basic: Provide the user name and password needed to connect.
- Client certificate: Select the correct SSL client certificate.

5. 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.

6. 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.

7. 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. This will only be useful if you have customized scripts running on the CA.

8. 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 are required to inform XenMobile of the signers of the certificates that the system will obtain through this entity. When your CA certificate is renewed, update it in XenMobile and then the change is applied to the entity transparently.

9. On the **Microsoft Certificate Services Entity: CA Certificates** page, select the certificates you want to use for this entity.

10. 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 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.

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 have the option to activate Online Certificate Status Protocol (OCSP) support for that CA. If, and only if you enable OCSP support, the CA adds an id-pe-authorityInfoAccess extension to the certificates that the CA issues, pointing to the XenMobile internal OCSP Responder at the following location.

`https://server/instance/ocsp`
When configuring the OCSP service, you must specify an OCSP signing certificate for the discretionary entity in question. You can use the CA certificate itself as the signer. If you want to avoid the unnecessary exposure of your CA private key (recommended), create a delegate OCSP signing certificate, signed by the CA certificate and include an id-kp-OCSPSigning extendedKeyUsage extension.

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).

To add discretionary CAs

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 list showing the types of PKI entities you can add 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 additional 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's 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

Nov 01, 2016

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.

Methods of Certificate Issuance

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.

Certificate Delivery

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 even 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, when using the SCEP protocol, XenMobile acts like a delegate (a registrar) to the actual CA and must prove to the client that it has the authority to act as such. That authority is established by providing XenMobile with the aforementioned certificates.

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. Each credential provider can be configured 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
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

Certificate Revocation

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.

Certificate Renewal

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.

To create a credential provider

Configuring a credential provider varies mostly as a factor of which issuing entity and which issuing method you select for the credential provider. You can distinguish between a credential provider using an internal entity, such as discretionary, and a credential provider using an external entity, such as Microsoft CA or GPKI. 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.

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 a template for the credential provider.

4. Click **Next**.

Note: These templates become available when Microsoft Certificate Services Entities are added at **Settings** > **More** > **PKI Entities**.

The **Credential Providers: Certificate Signing Request** page appears.

5. On the **Credential Providers: Certificate Signing Request** page, do the following:

- **Key algorithm**: Click 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**: 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. This is a required field.

  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

Feb 02, 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	Create a CSR on IIS Create a CSR on a Mac	Generate a CSR with a Windows Server 2012 R2 or Windows 2008 R2 Server and Microsoft IIS or on a Mac computer. Citrix recommends this method.
Step 2	To sign the CSR	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.
Step 3	Submit Signed CSR to Apple	Submit the signed CSR to Apple at Apple Push Certificate Portal (Apple ID required) and then download the APNs certificate from Apple.
Step 4	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	Export the APNs certificate as a PCKS #12 (.pfx) certificate (on IIS, Mac, or SSL).
Step 5	Import an APNs certificate into XenMobile	Import the certificate into XenMobile.

Apple MDM Push Certificate Migration Information

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.

To create a CSR by using Microsoft IIS

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**.

To create a CSR on a Mac computer

1. On a Mac computer running Mac OS X, 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.

To create a CSR by using OpenSSL

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.

To sign the CSR

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.

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

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 condition**s 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 create a .pfx APNs certificate by using Microsoft IIS

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**.
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**.

To create a .pfx APNs certificate on a Mac computer

1. On the same Mac computer running Mac OS X 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, choose a folder location for the saved certificate, select the .pfx file format and then 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.

To create a .pfx APNs certificate by using OpenSSL

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

1. At a command prompt or shell, execute the following command.
   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.

To import an APNs certificate into XenMobile

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

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 06, 2017

You can configure XenMobile and ShareFile to use Security Assertion Markup Language (SAML) to provide single sign-on (SSO) access to ShareFile mobile apps that are wrapped with the MDX toolkit, as well as to 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 log on, users can access the ShareFile mobile app through SSO and can attach documents from ShareFile to Secure Mail emails 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.

For a detailed reference architecture diagram, see the XenMobile Deployment Handbook article, Reference Architecture for On-Premises Deployments.

Prerequisites

You must complete the following prerequisites before you can configure SSO with XenMobile and ShareFile apps:

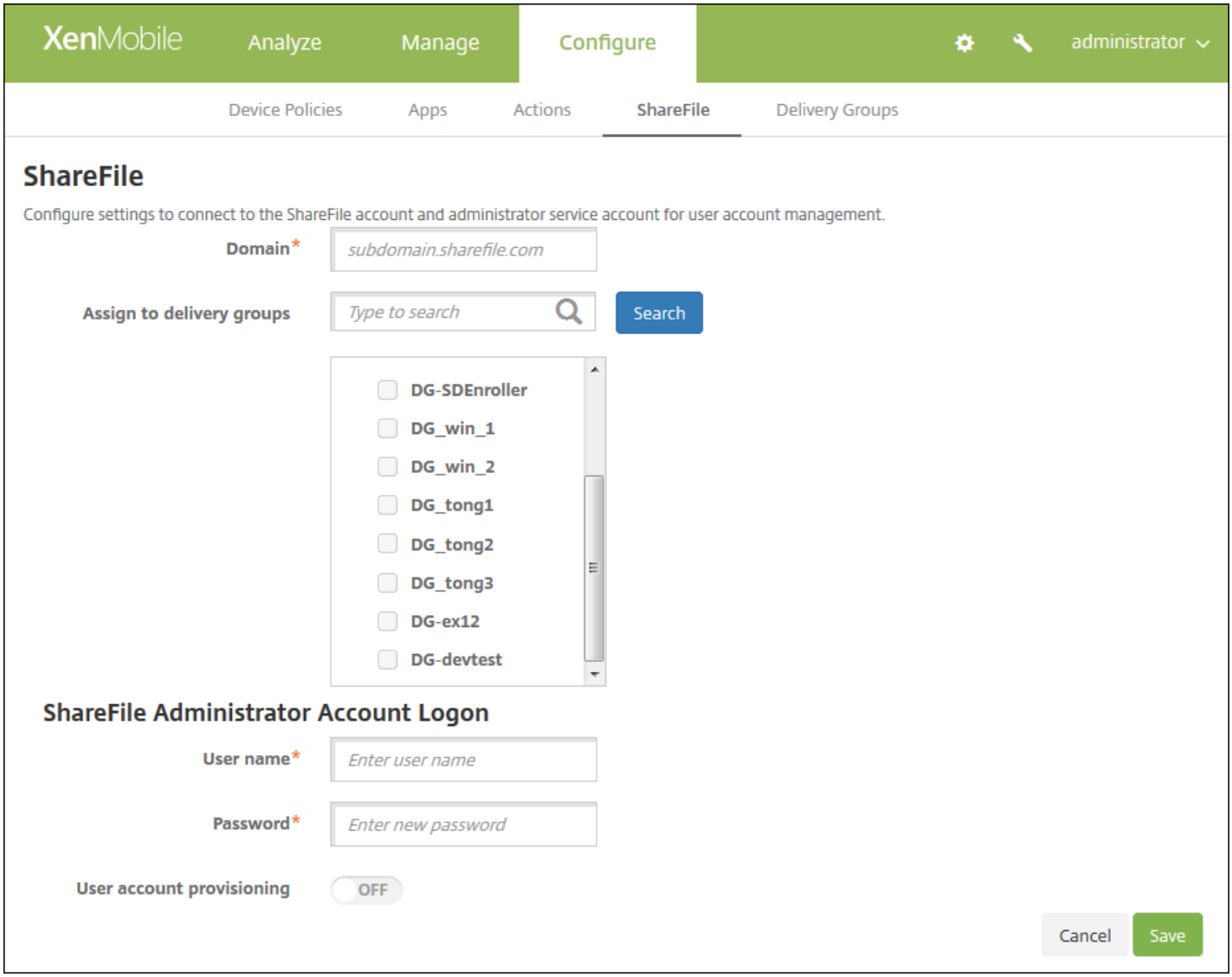
- MDX Toolkit Version 9.0.4 or later (for ShareFile mobile apps)
- ShareFile mobile apps as appropriate:
  - ShareFile for iPhone Version 3.0.x
  - ShareFile for iPad Version 2.2.x
  - ShareFile for Android Version 3.2.x
- Secure Hub 9.0 (for ShareFile mobile apps) - Install the iOS or Android version as appropriate.
- ShareFile administrator account

Make sure that XenMobile and ShareFile are able to connect.

Configure ShareFile Access

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.



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 **Save**.

Set up SAML for Wrapped ShareFile MDX Apps

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.

Configure the NetScaler Gateway for Other ShareFile Clients

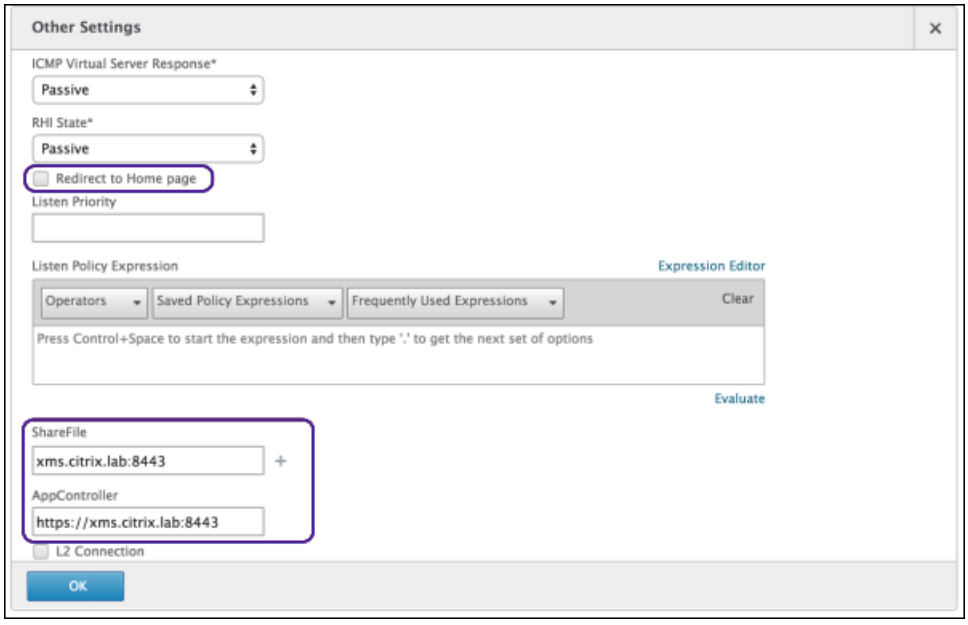
If you want to configure access for non-wrapped ShareFile clients, such as the web site, Outlook plugin, or the sync clients, you must configure NetScaler Gateway to support the use of XenMobile as a SAML identity provider as follows:

- 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**.



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

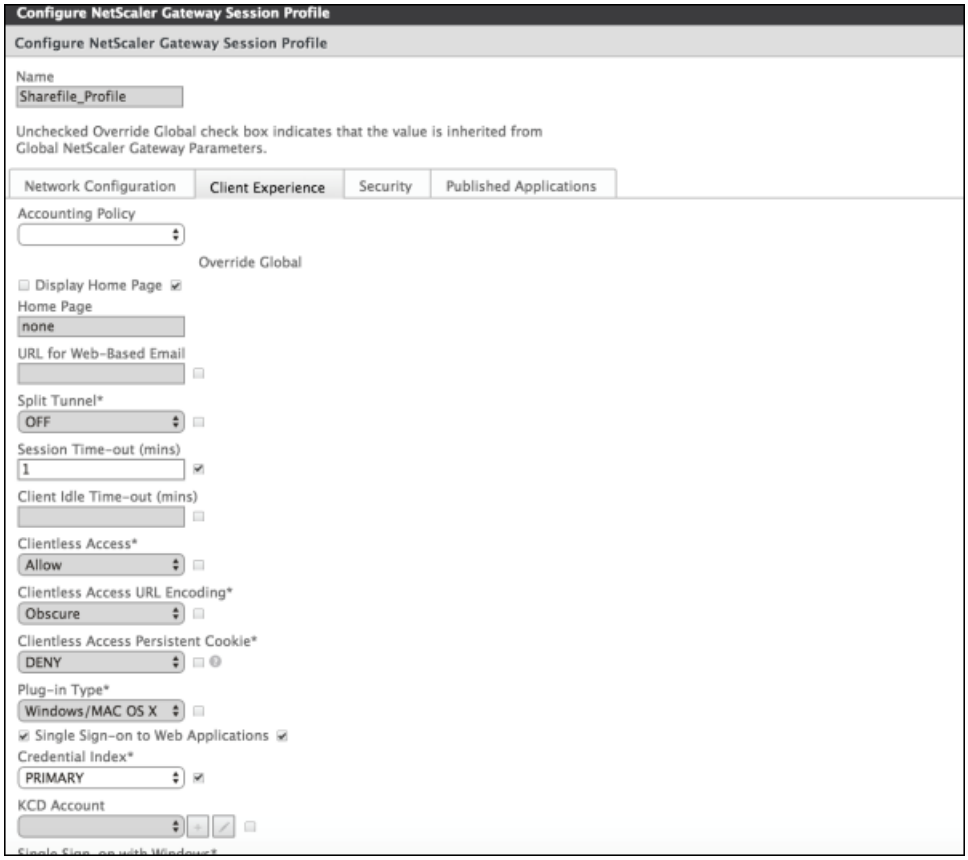
Configure these settings to create a ShareFile session policy and request profile:

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**.

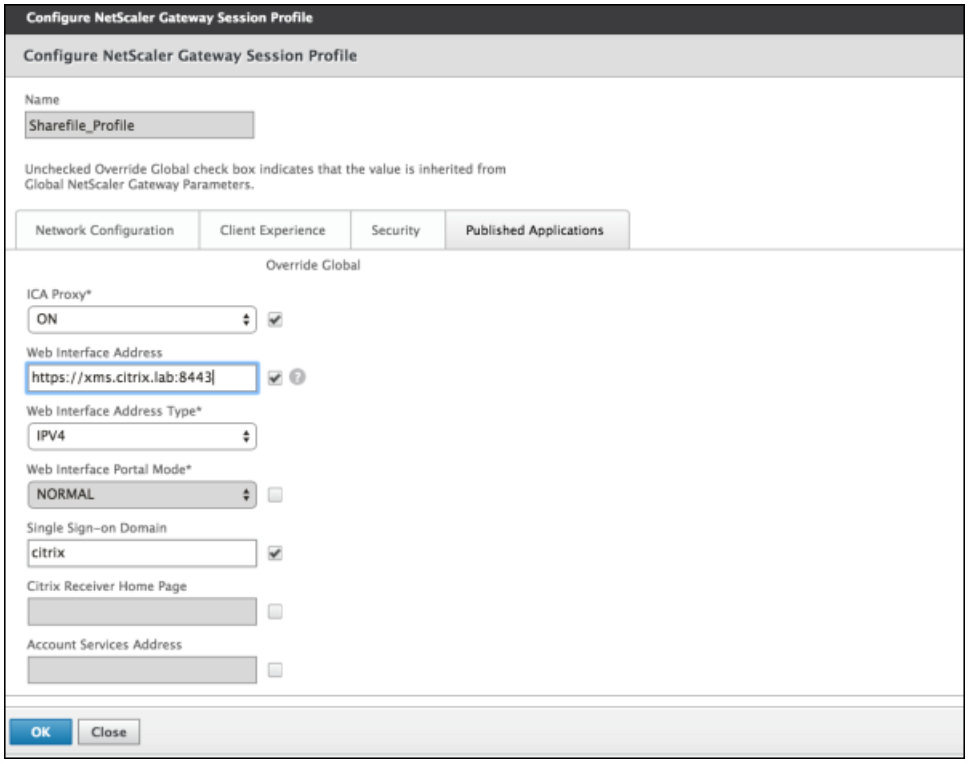
3. In the **Name** field, type **ShareFile_Policy**.

4. Create a new action by clicking the **+** button. The **Create NetScaler Gateway Session Profile** page appears.



Configure 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.



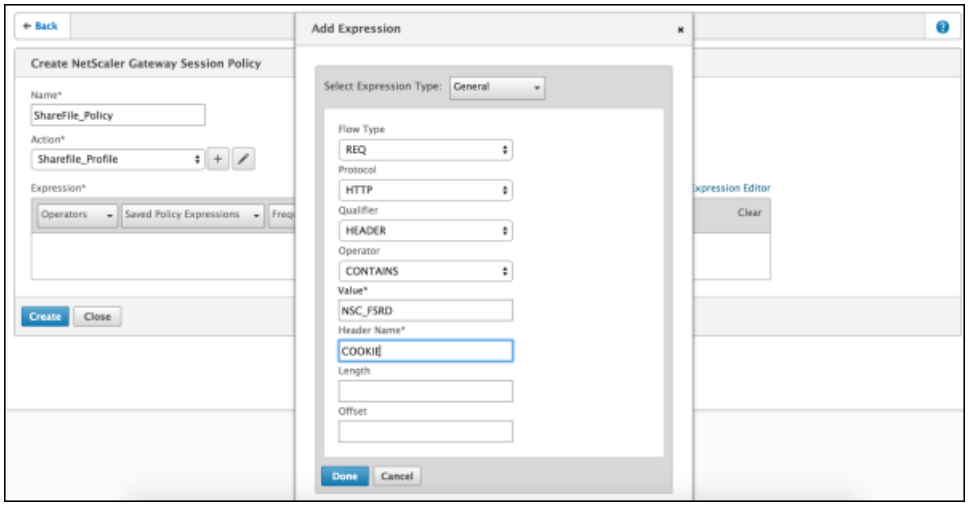
Configure these settings:

- **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**.



Configure these settings:

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

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

Configure policies on the NetScaler Gateway virtual server

Configure these settings on the NetScaler Gateway virtual server.

1. In the NetScaler Gateway configuration utility, in the left-hand navigation pane, click **NetScaler Gateway > Virtual Servers**.

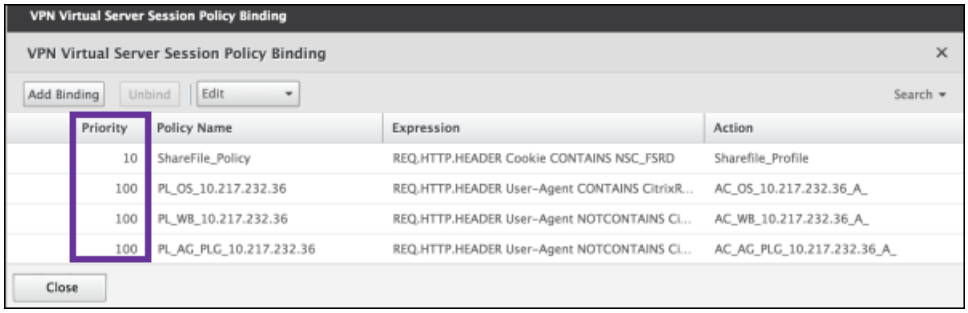
2. In the **Details** pane, click your NetScaler Gateway virtual server.

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.



7. Click **Done** and then save the running NetScaler configuration.

Configure SAML for non-MDX ShareFile apps

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**.

3. Click **Applications > Applications** and note the **Application Name** for the app with the **Display Name** "ShareFile".

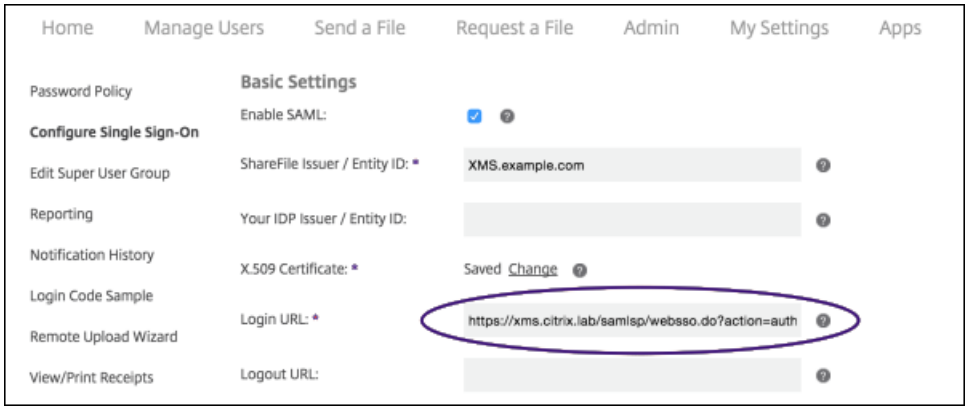
Modify the ShareFile.com SSO settings

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.



- 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).

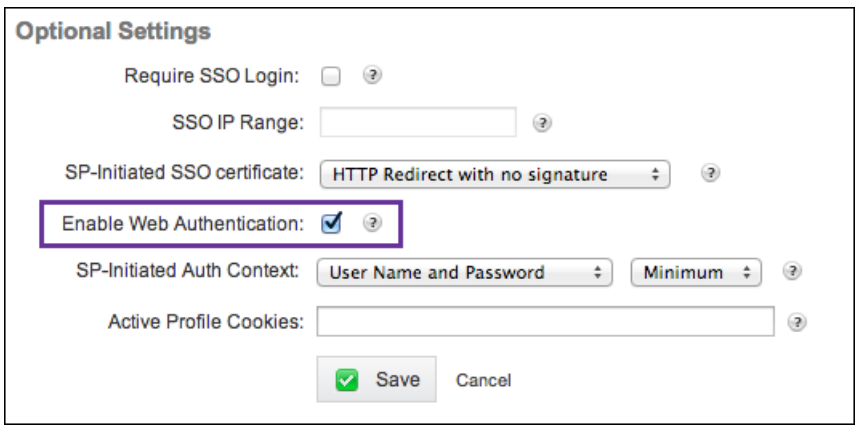
  The URL should now look similar to this:
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**r&app=ShareFile_SAML**&reqtype=1

- 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.



Validate the configuration

Do the following to validate the configuration.

1. Point your browser to https://<subdomain>sharefile.com/saml/login.

You are redirected to the NetScaler Gateway log on 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.

Microsoft Azure Active Directory server settings

Feb 22, 2017

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. This feature is not available on Windows 10 Phones.
- Enroll in MDM as part of Azure AD Join as part of addinga work account on a personal device.

You need a Microsoft Azure Active Directory premium license before you can integrate XenMobile with Microsoft Azure. The license is required to enable MDM integration with Azure AD so that users with Windows 10 devices can enroll using Azure AD. See Microsoft Azure for information about obtaining the premium license. For information about pricing, see Azure Active Directory pricing.

Before Windows device users can enroll with Azure, you must configure the Microsoft Azure server settings in XenMobile, as well as set up a Terms and Conditions device policy for Windows devices. This article describes how to configure the Microsoft Azure settings. For information about configuring a Terms and Conditions device policy for Windows devices, see Terms and conditions device policies.

Before you can set up the Microsoft Azure server settings in XenMobile, you need to log on to the Azure AD portal and do the following:

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-premise directory to Azure Active Directory using directory integration tools. For details, see Directory Integration.

3. Make the MDM a reliable party of Azure AD. To do so, click **Azure Active Directory** > **Applications** and then click **Add**. Select **Add an application** from the gallery. Go to **MOBILE DEVICE MANAGEMENT**, select **On-premise MDM application** and then save the settings.

4. In the application, configure XenMobile server discovery, terms of use endpoints, and APP ID URI as follows:

- MDM Discovery URL: https://<FQDN>:8443/zdm/wpe
- MDM Terms of Use URL: https://<FQDN>:8443/zdm/wpe/tou
- APP ID URI: https://<FQDN>:8443/

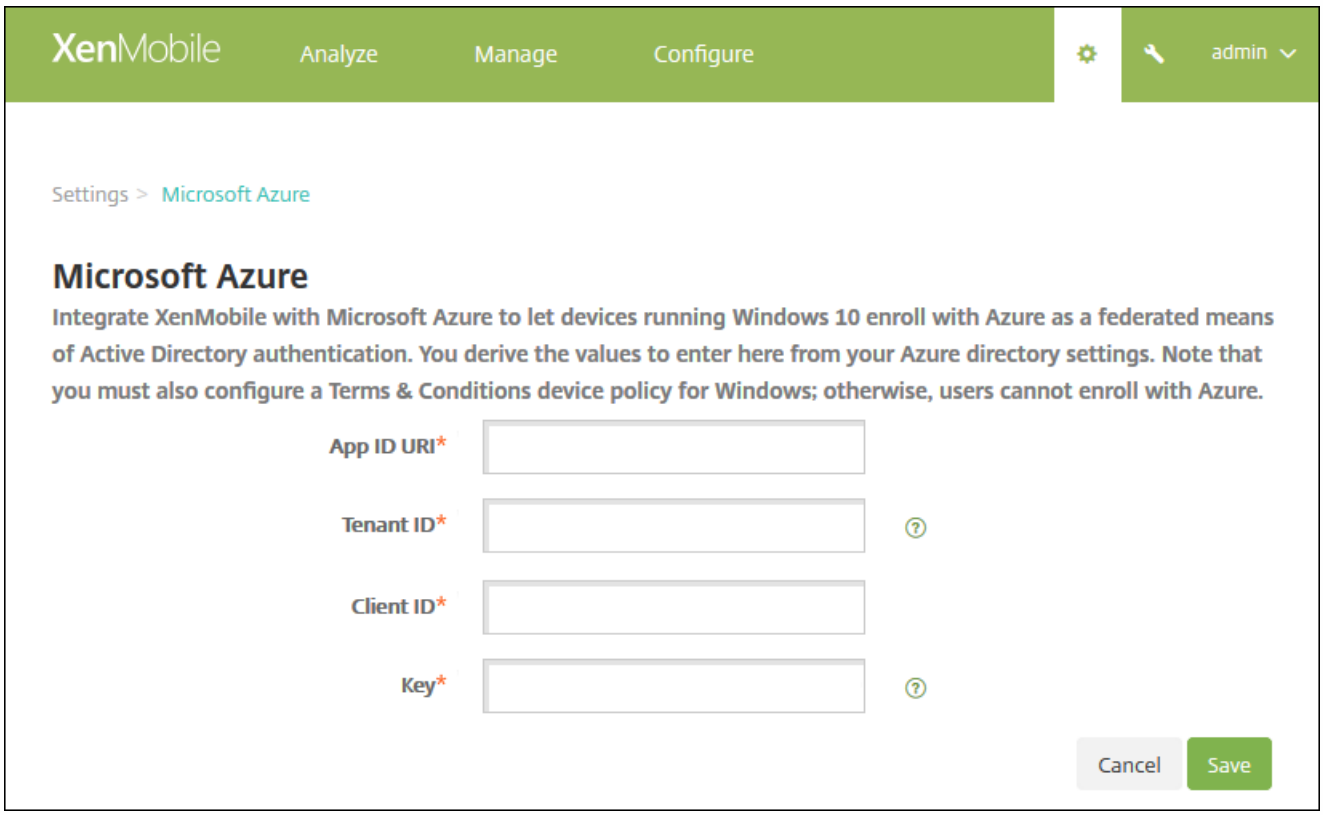
5. Select the on-premise MDM application that you created in step 3 and enable the **Manage devices for these users** option to enable MDM management for all users or any specific user group.

You also need to note the following information from your Microsoft Azure account in order to configure the settings in the XenMobile console:

- App ID URI – the URL for the server running XenMobile.
- Tenant ID – from the Azure application settings page.
- Client ID – the unique identifier for your app.
- Key – from the Azure application settings page.

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

2. Under **Platforms**, click **Microsoft Azure**. The **Microsoft Azure** page appears.



3. Configure these settings:

- **App ID URI**: Type the URL for the server running XenMobile that you entered when you configured your Azure settings.
- **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*.
- **Client ID**: Copy and paste this value from the Azure Configure page. This 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.

4. Click **Save**.

Important

When users join Azure AD on their Windows devices, the XenMobile Store and Weblink device policies you configured in XenMobile are only available for Azure AD users, but not to local users. For local users to be able to use these device policies, they must do the following:

1. Join Azure AD on behalf of an Azure user in **Settings** > **About** > **Join Azure AD**.
2. Sign out of Windows and then sign in with an Azure AD account.

Upgrade in XenMobile 10.4

Mar 29, 2017

When new versions or important updates of XenMobile are available, they are published to Citrix.com. At the same time, a notice is sent to the contact on record for each customer. For Upgrade documentation in the most recent version of XenMobile Server, see Upgrade.

You have these options for upgrading XenMobile:

- **To upgrade from XenMobile 9.0 to XenMobile 10.4.**
  Use the XenMobile Upgrade Tool that is built in to XenMobile 10.4. See the articles in this section for details.
  The Upgrade Tool supports all XenMobile 9 editions: MDM, App, and Enterprise.
  For fixed and known issues, see Fixed issues and Known issues.
  The older Upgrade Tool is no longer available from Citrix.com.
- **To upgrade from XenMobile 10.3.x to XenMobile 10.4.**
  Use the **Release Management** page in the XenMobile console. See the instructions in this article for details.
  You do not use the Upgrade Tool for XenMobile 10.3.x installations.
- **To upgrade from XenMobile 10 or XenMobile 10.1 to XenMobile 10.4.**
  First, use the **Release Management** page in the XenMobile console to upgrade from XenMobile 10 or XenMobile 10.1 to XenMobile 10.3. Then, use the **Release Management** page in the XenMobile console to upgrade from XenMobile 10.3 to XenMobile 10.4. See the instructions in this article for details. You do not use the Upgrade Tool for these installations.

Upgrade path summary

XenMobile Server version	Release number	Upgrade to	Release number	Upgrade path	Release update Location
XenMobile Server 9 that has App Controller Rolling Patch 9 installed	9.0.0_97106	XenMobile Server 10.4	10.4.0.116	XenMobile Server 9 to XenMobile Server 10.4	Download the App Controller rolling patch prerequisite. The Upgrade Tool for XenMobile 10.4 is built into XenMobile Server. For more information, see the Upgrade Tool prerequisites.
XenMobile Server 10 or XenMobile 10.1	10.1.0.63030	XenMobile Server 10.3	10.3.0.824	XenMobile 10 or XenMobile 10.1 upgrade to XenMobile 10.3	Download
XenMobile Server 10.3.x	10.3.x	XenMobile Server 10.4	10.4.0.116	XenMobile 10.3.x upgrade to XenMobile 10.4	Download

10.4.0.?

10.4.0.?

To upgrade from XenMobile 10 or XenMobile 10.1 to XenMobile 10.3, or XenMobile 10.3 to XenMobile 10.4

Prerequisites:

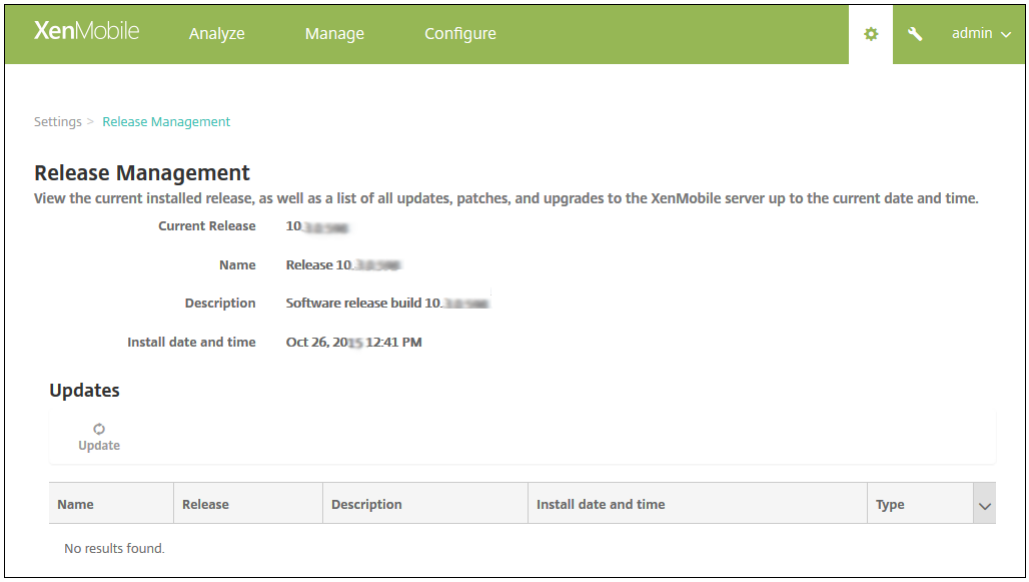
- Before you install a XenMobile update, use the facilities in your virtual machine (VM) to take a snapshot of your system.
- Back up your system configuration database.
- Review the System Requirements for the version to which you are updating. For XenMobile 10.4, see System Requirements.

If you have a clustered deployment, see the instructions at the end of this article.

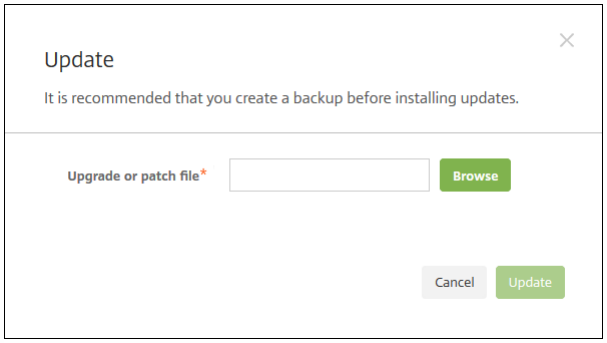
1. Log on to your account on the Citrix website and download the XenMobile Upgrade (.bin) file to an appropriate location

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.



4. Under **Updates**, click **Update**. The **Update** dialog box appears.



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 the update cannot be completed successfully, an error message appears indicating the problem. The system is reverted to its state before the update attempt.

Note: XenMobile might not require a restart after the update installs. In this case, a message indicates that the updated installation is successful. If, however, XenMobile does require a restart, you must use the command line. It's important that you clear your browser cache after the system restarts.

To upgrade clustered XenMobile deployments

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 nodes other than the one you are upgrading first. To shut down a node, use the **System menu** in the command line interface.

3. Upgrade the node that is running.

3. Check that the service is running on the upgraded node.

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 the state before the update attempt.

Upgrade Tool prerequisites

Jan 24, 2017

To upgrade from XenMobile 9.0 to XenMobile 10.4, you use the XenMobile 10.4 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 XenMobile 10.4 deployment. 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 10.4.

XenMobile 10.4 supports NetScaler Gateway versions 11.1.x, 11.0.x, and 10.5.x.

The Upgrade Tool built in to XenMobile 10.4 also supports NetScaler Gateway version 10.1.x. Citrix doesn't support NetScaler Gateway 10.1 for use with XenMobile 10.4. However, you can upgrade a NetScaler Gateway 10.1 deployment using the Upgrade Tool built in to XenMobile 10.4. 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 XenMobile 10.4 instance in the command-line console and start the Upgrade Tool again.

Plan your upgrade

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 11.1 (or 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 10.4 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 XenMobile 10.4 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 XenMobile 10.4 with the same fully qualified domain name (FQDN). Everything in XenMobile 9.0 remains intact until you move the XenMobile 10.4 server into production.

When you log on to the XenMobile 10.4 console after the upgrade, you see all the user and device data that the upgrade moved from XenMobile 9.0.

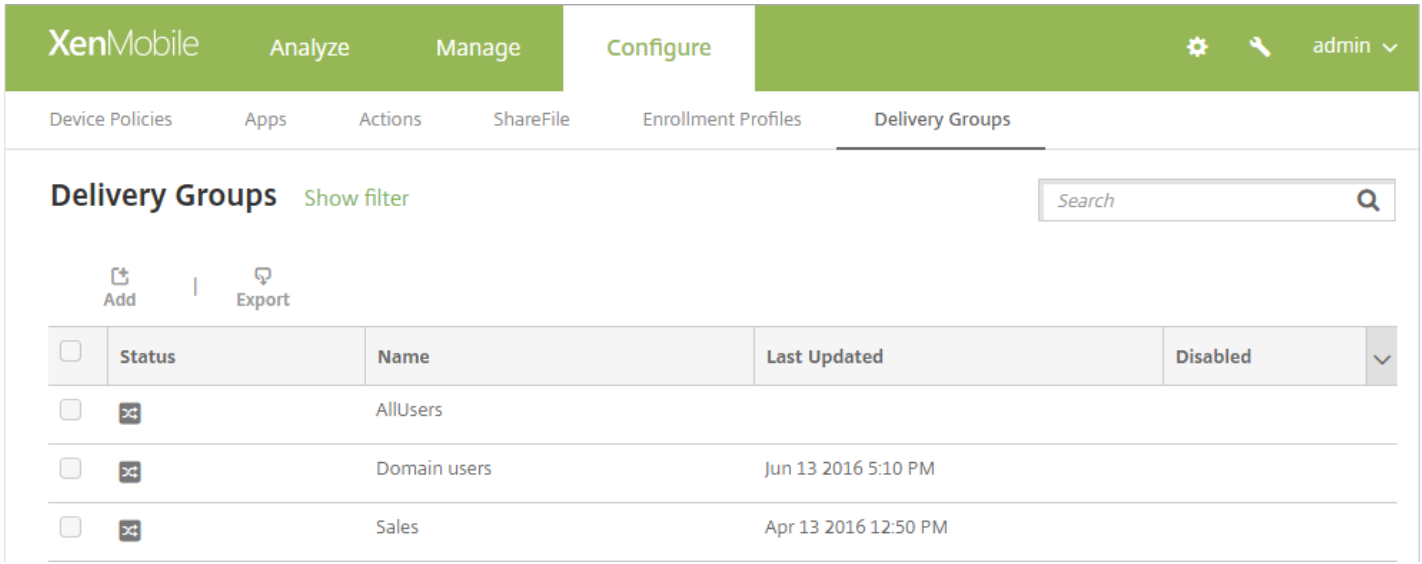
What the Upgrade Tool does not do

The following information isn't upgraded to XenMobile 10.4 when you use the Upgrade Tool:

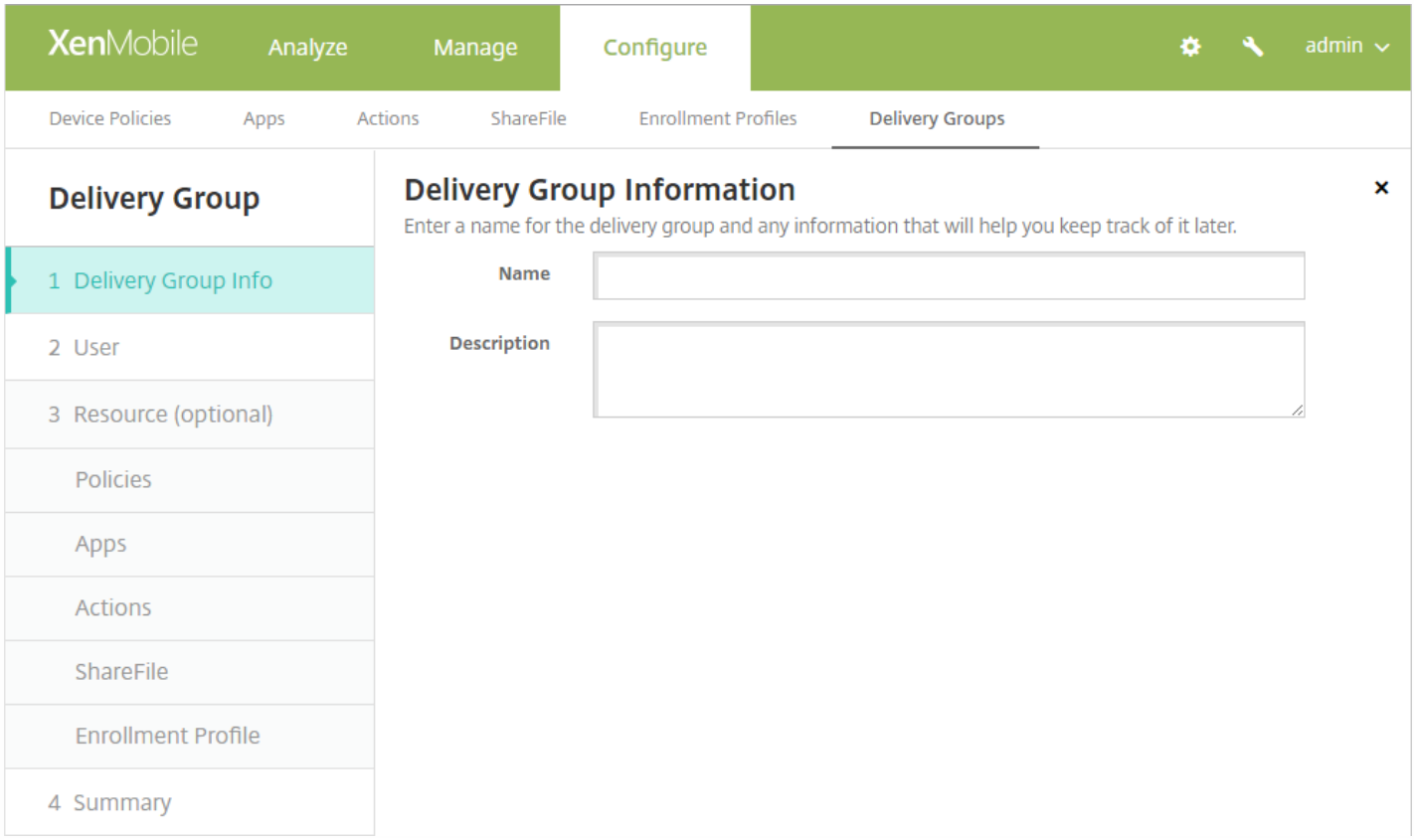
- Licensing information.
- Reports data.
- Server group policies and associated deployments (not supported in XenMobile 10.4).
- Managed Service Provider (MSP) group.
- Policies and packages related to Windows 8.0.
- Deployment packages not in use; for example, when no users or groups are assigned to 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, the branding policy is not upgraded. XenMobile 10.4 supports one branding policy; you have to leave one branding policy in XenMobile 9.0 to successfully upgrade to XenMobile 10.4.
- Any settings in the auth.jsp file in XenMobile 9.0 that are used to restrict access to the console. Console access restrictions in XenMobile 10.4 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 XenMobile 10.4).

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.

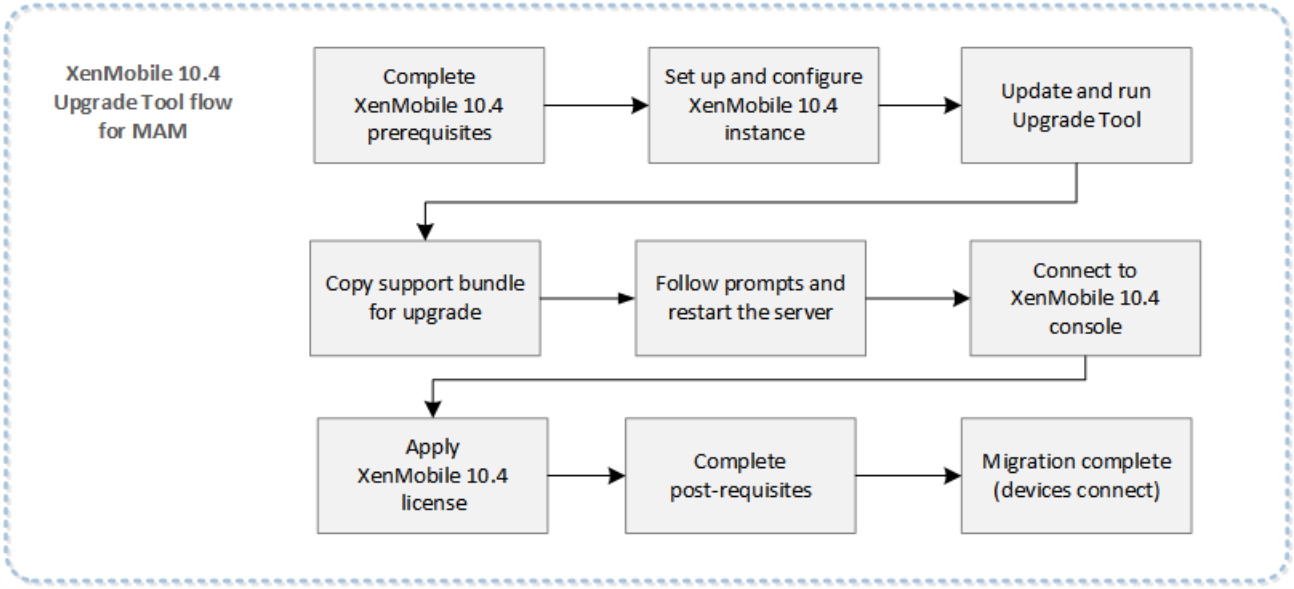


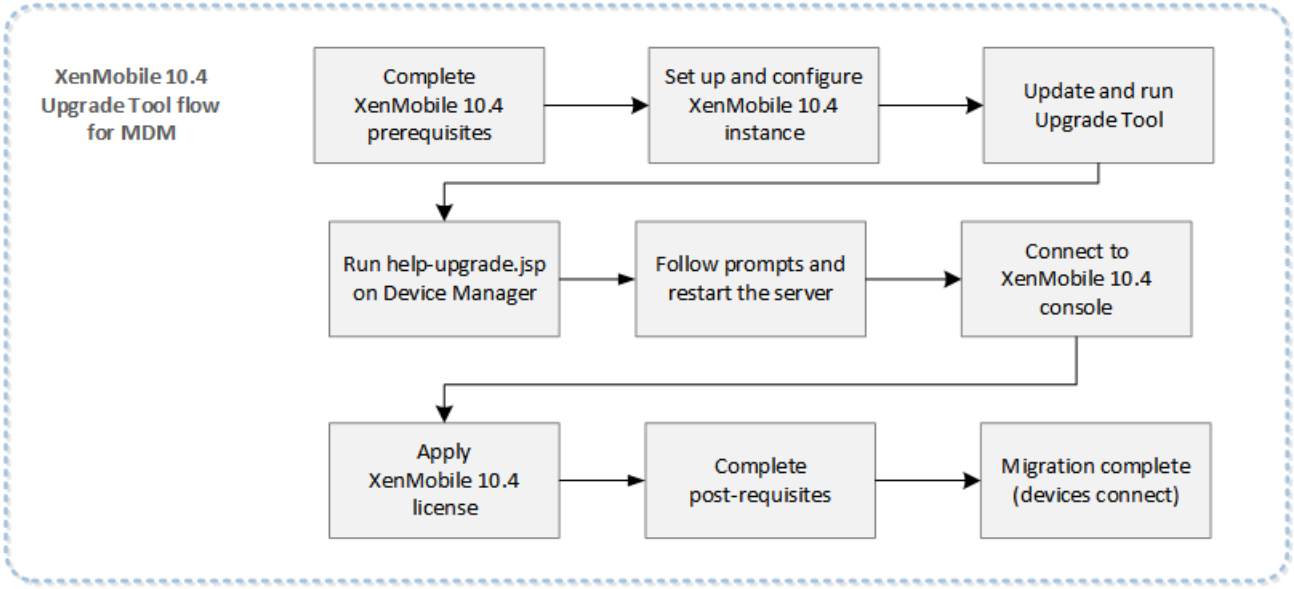
Inside the delivery group, you can view the policies, actions, and apps required for the group of users who require the resources.

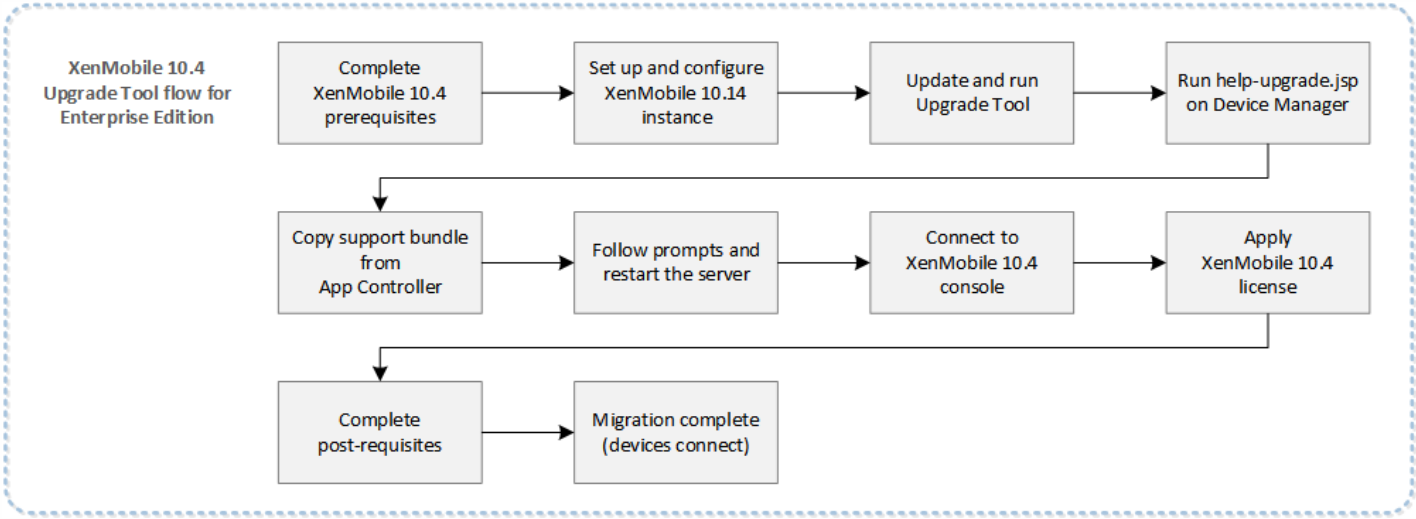


Upgrade workflow for XenMobile 9.0 to XenMobile 10.4

The following figures illustrate the basic steps you take to upgrade from XenMobile 9.0 to XenMobile 10.4.







Prerequisites for Windows phones in Enterprise mode

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 XenMobile 10.4.

1. Upgrade Worx Home on Device Manager to Worx Home 10.2 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, which you deployed from Device Manager.

4. After you complete the prerequisites described in this article, Upgrade to XenMobile 10.4 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.

Required App Controller patch

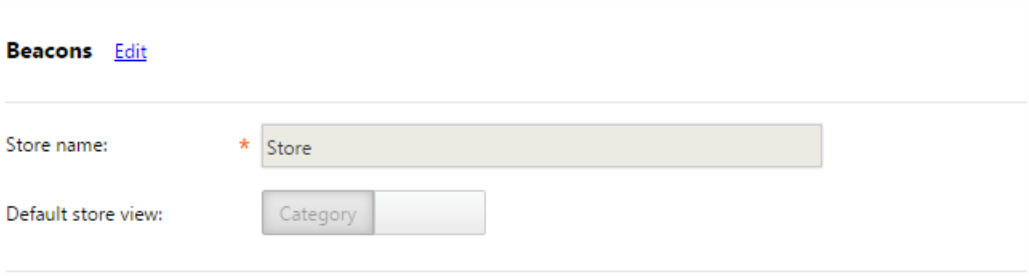
Download XenMobile 9.0 App Controller Rolling Patch 9 from https://support.citrix.com/article/CTX218552.

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.

Custom store names in XenMobile 9

Before you upgrade XenMobile 9 to XenMobile 10.4, 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.



System and port requirements

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 10.4 server IP similar to the ports opened for the XenMobile

9.0 IP server. For XenMobile 10.4 port requirements, see Port requirements.

- **LDAP Server**: Make sure that the new XenMobile 10.4 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.

Database migration

The following table lists the possible database migration options. For system requirements, see XenMobile 10.4 Database Requirements.

From XenMobile 9.0		To XenMobile 10.4
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 XenMobile 10.4 to connect to the database and migrate the required information.

Deployment package names with special characters

Deployment package names in XenMobile 9.0 that contain special characters (!, $, (), #, % , +, *, ~, ?, |, {}, and []) upgrade, however you can't edit the delivery groups in XenMobile 10.4 after the upgrade. In addition, local users and local groups created in XenMobile 9.0 that contain an open square bracket ([) cause problems in XenMobile 10. 4 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 certificate

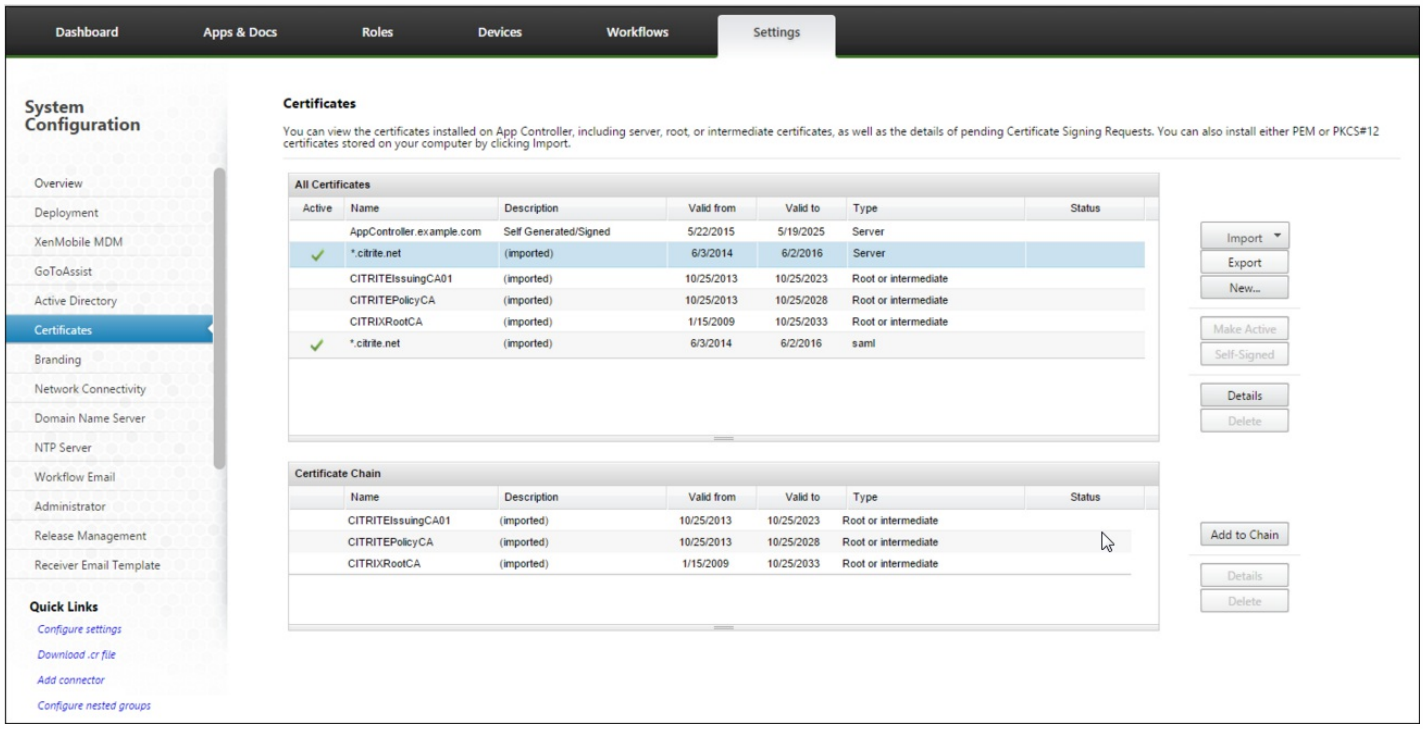
External SSL certificates must meet the conditions outlined in the Citrix Support article How to Configure an External SSL Certificate. Be sure to review your pki.xml before starting the upgrade to ensure that the SSL certificate meets those conditions.

Export XenMobile 9.0 server certificate

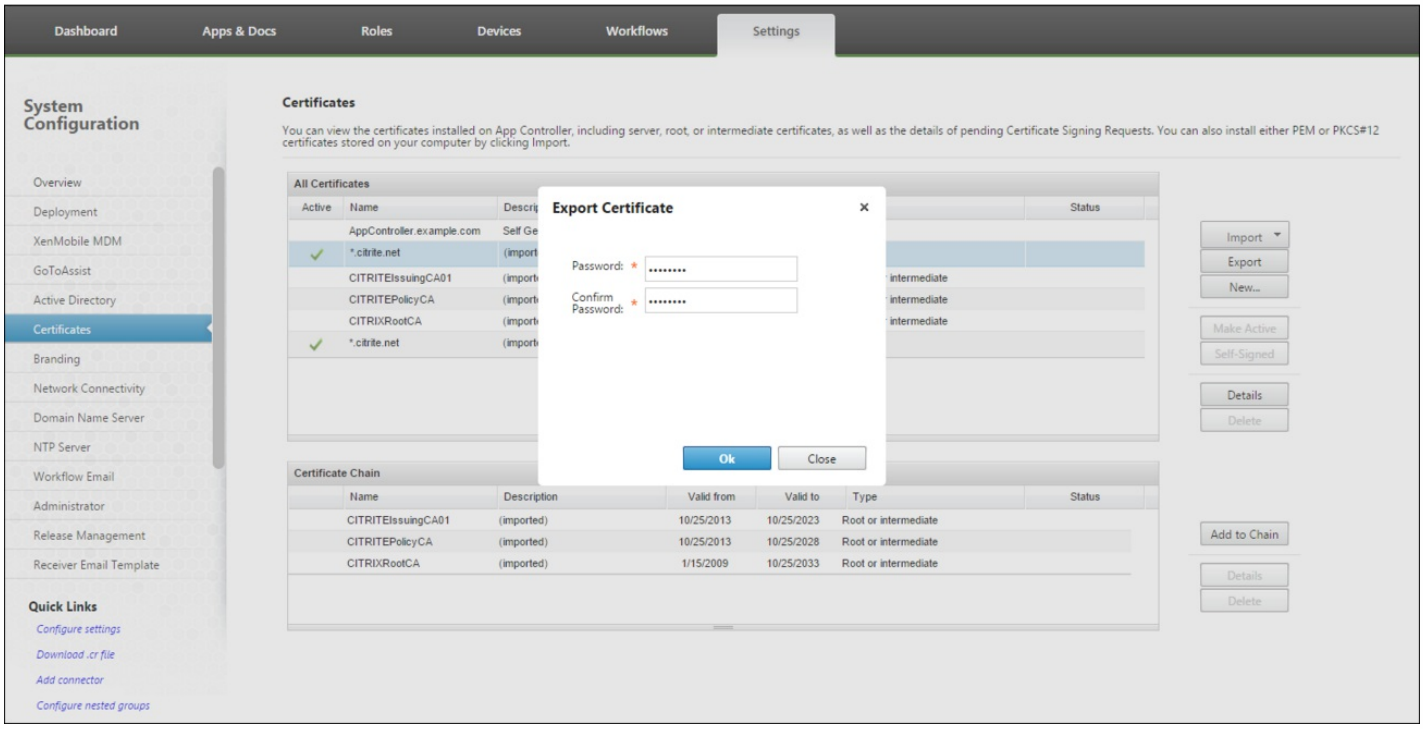
If you are upgrading a XenMobile 9.0 Enterprise Edition deployment, you must export the App Controller server certificate. Later, when you are handling the upgrade post-requisites, you must import the server certificate into NetScaler Gateway. Follow these steps to export the server certificate:

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**.



3. In the **Export Certificate** dialog box, type your certificate password in both fields and then click **OK**.



Server for uploading the encrypted support bundle

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).

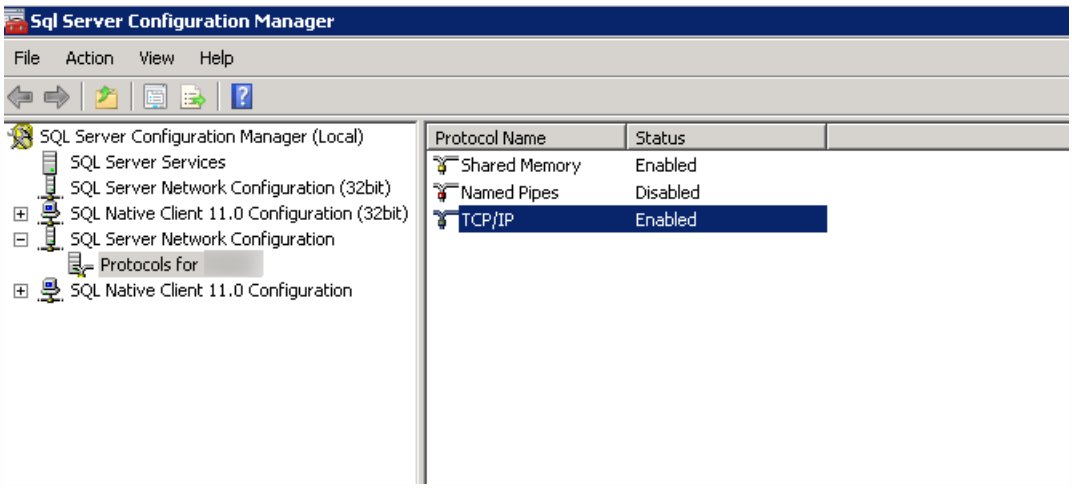
Enable and run the XenMobile Upgrade Tool

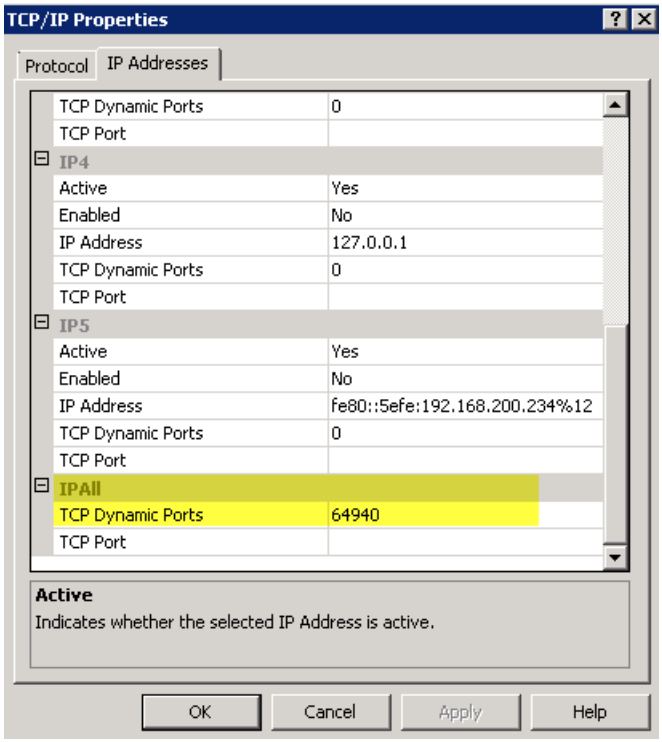
Nov 29, 2016

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.

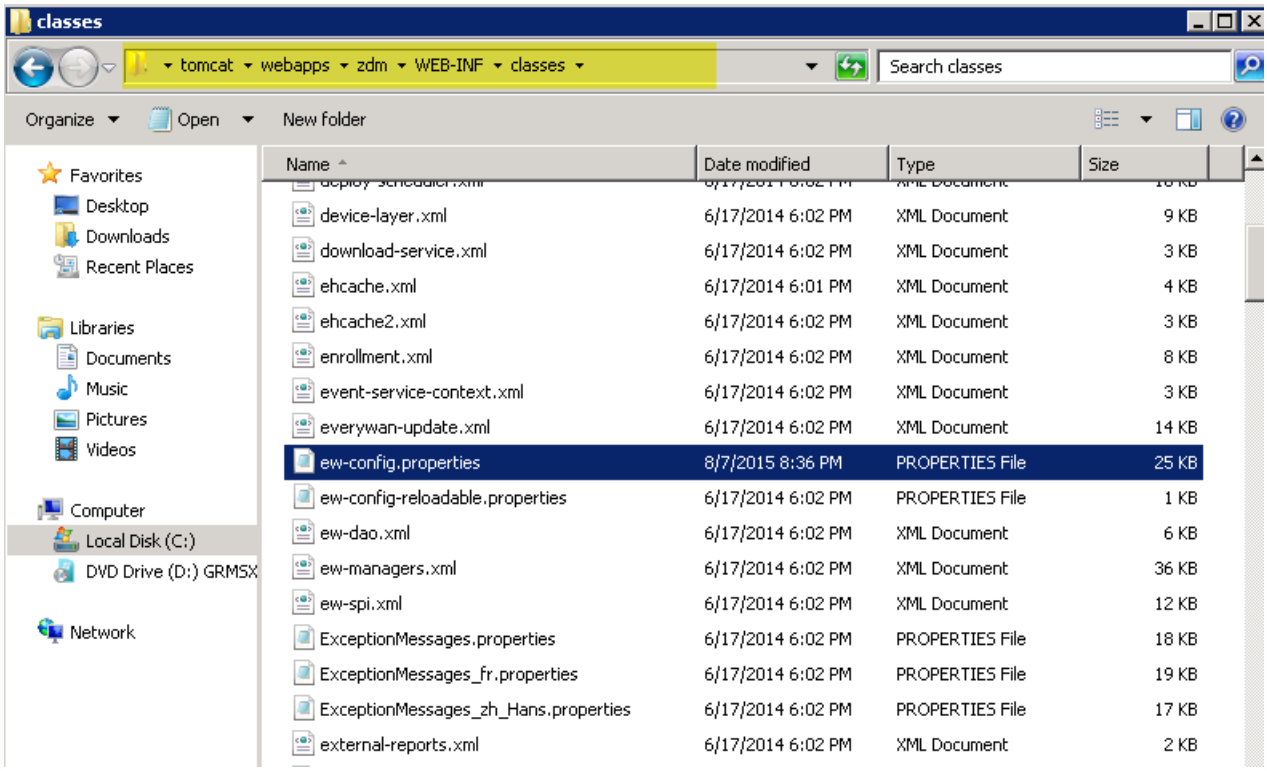
> ## Note
>
> Citrix recommends that the SQL server database instance always runs on a static port, because the XenMobile server needs continuing access to the database. This connection generally traverses through a firewall. As a result, you need to open the appropriate port in the firewall; therefore, you the need to have the database instance running on a static port.





Pre-upgrade steps

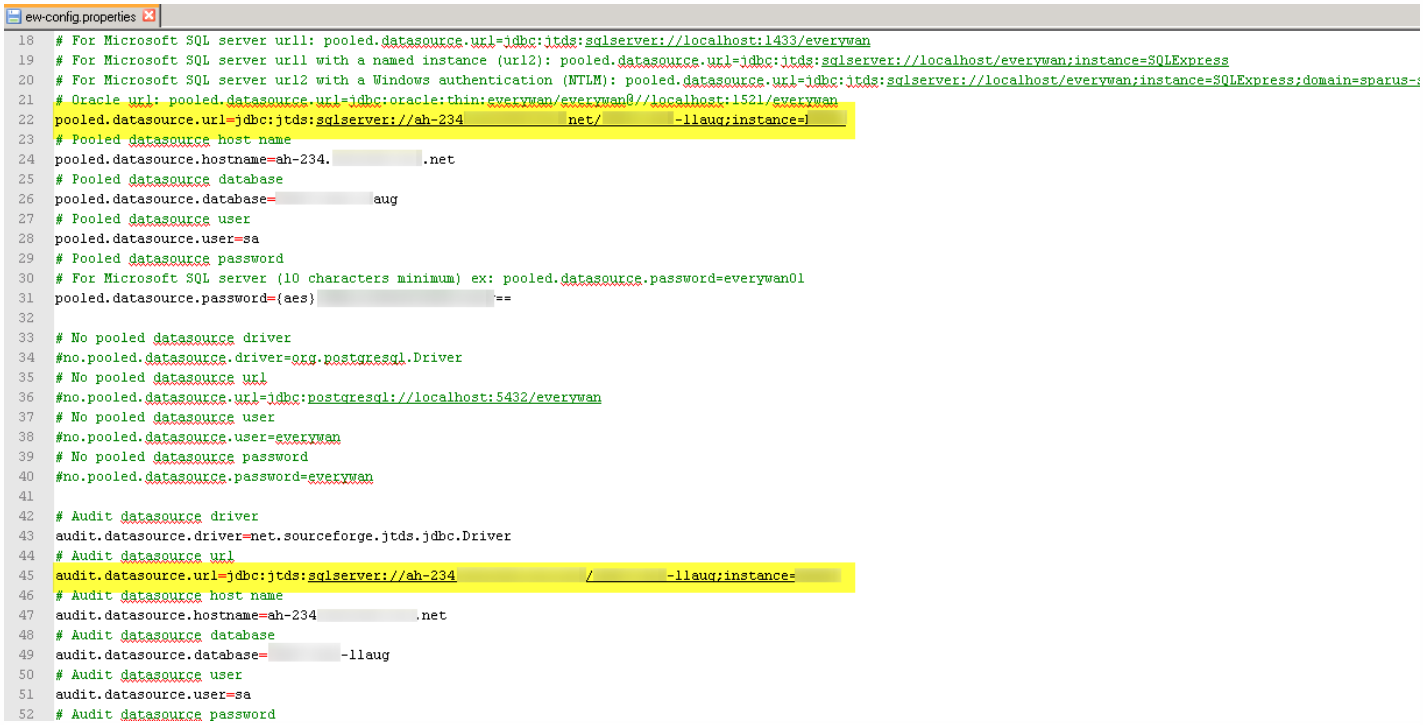
1. Go to the Device Manager installation directory and open the ew-config.properties file. This file is available in tomcat\webapps\zdm\WEB-INF\classes.



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>



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>

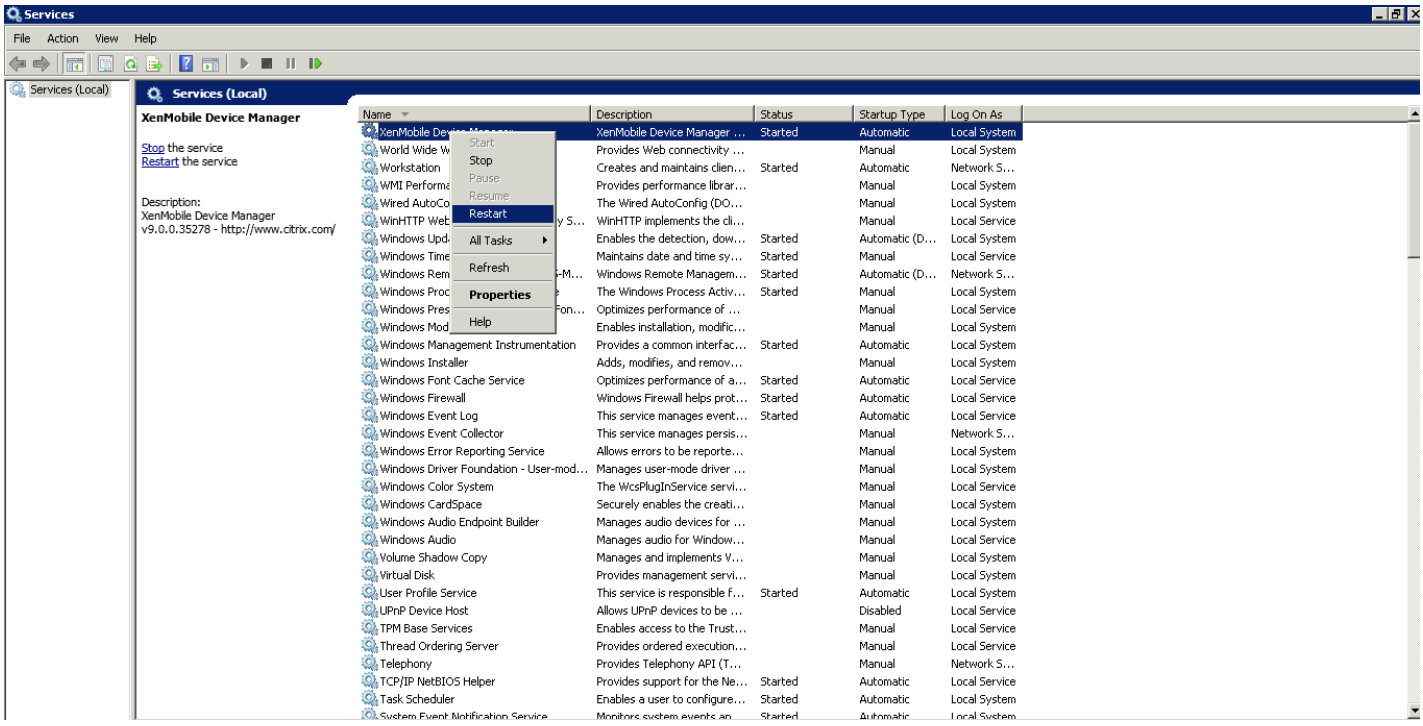
audit.datasource.url=jdbc:jtds:sqlserver:// <SQLserver_FQDN>:64940/<DB_Name>

> ## 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.

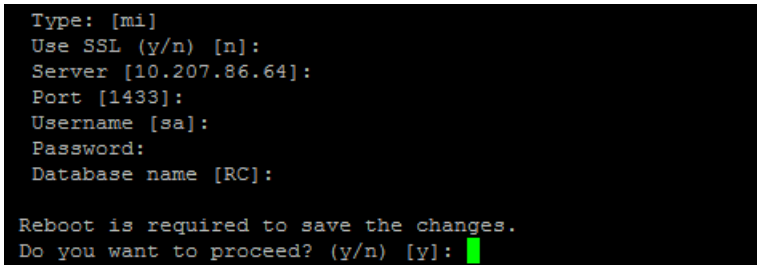
ew-config.properties

```
# 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.                net:                -llaug
# Pooled datasource host name
pooled.datasource.hostname=ah-234.          .net
# Pooled datasource database
pooled.datasource.database=          -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}                    ==

# 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://                -inc.net:                -llaug
# Audit datasource host name
audit.datasource.hostname=ah-234.          .net
# Audit datasource database
audit.datasource.database=          -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.



5. Determine if the new XenMobile 10.x server also needs to 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.



You can now proceed with the upgrade.

To upgrade clustered XenMobile deployments

If your system is configured in cluster mode:

1. Shut down all nodes other than the one you will 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's 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.

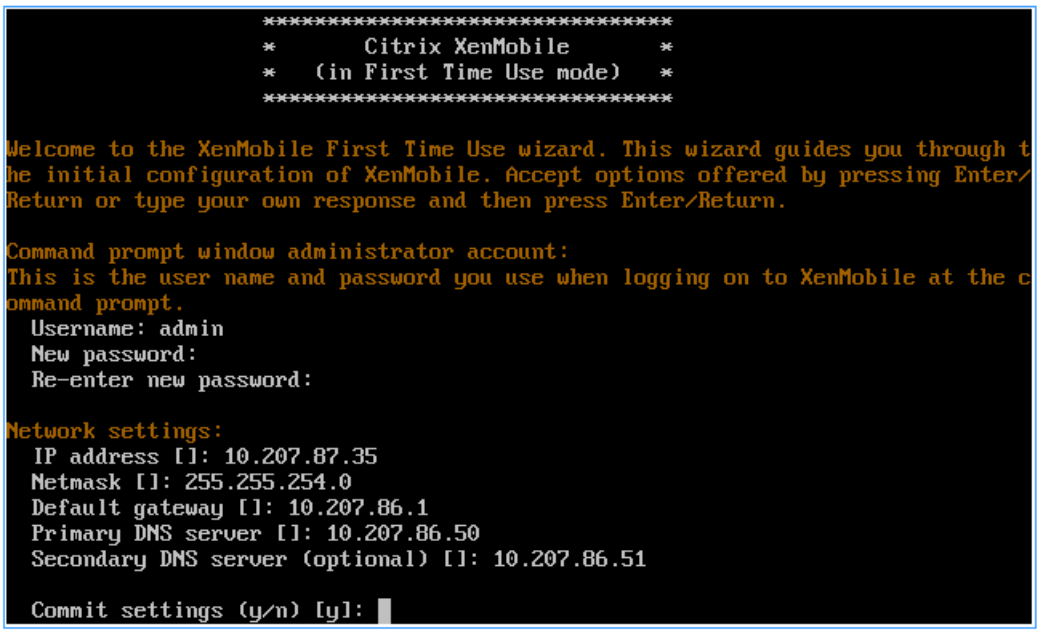
To enable and run the Upgrade Tool

Enable the Upgrade Tool through the command-line interface (CLI) when you first install XenMobile 10.4.

> **Important**
>
> If you want to take a snapshot of your system, do so after the initial XenMobile 10.4 configuration and before accessing 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.

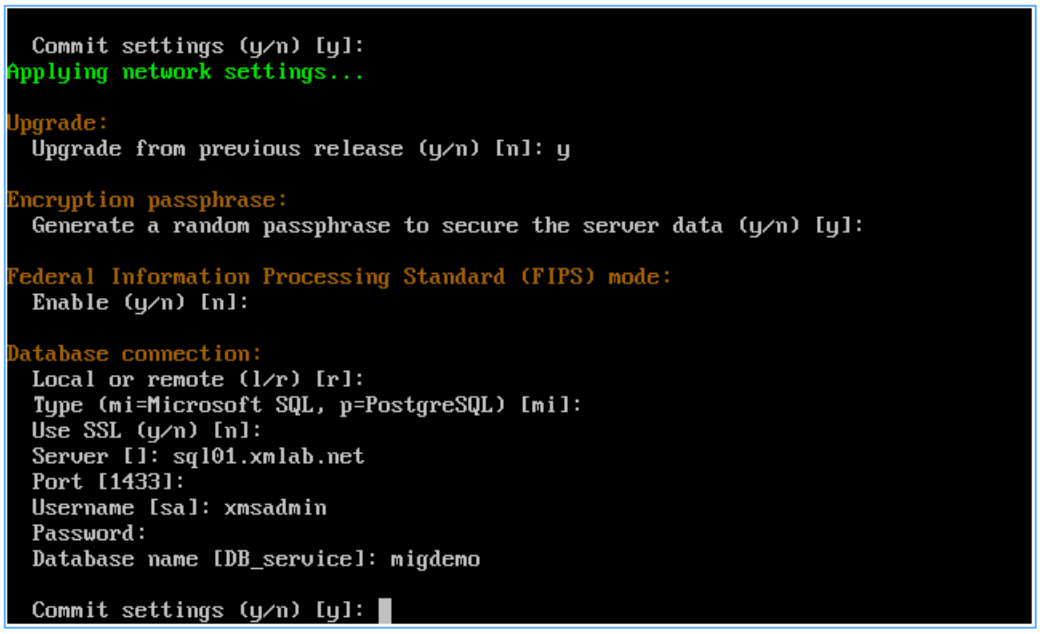


3. Type **y** to upgrade.

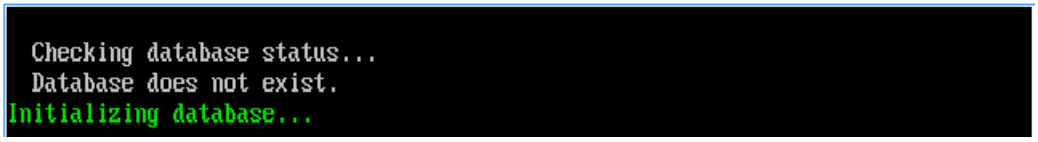
> ## Note
>
> If you do not select y here, you must configure a new XenMobile 10.4 instance in the command-line console and start the Upgrade Tool again.

4. Select to generate a random passphrase and, optionally, enable FIPS. Enter your database connection information.

5. Type **y** to commit the settings.



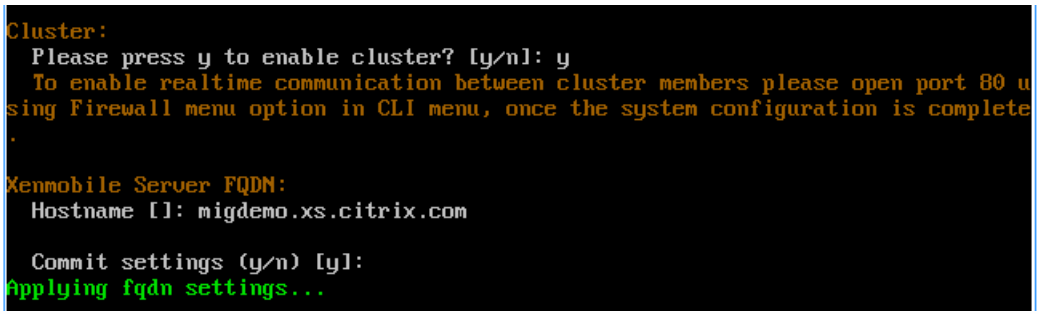
XenMobile initializes the database.



6. Select whether to enable clustered servers. Type the XenMobile fully qualified domain name (FQDN). Note the following:

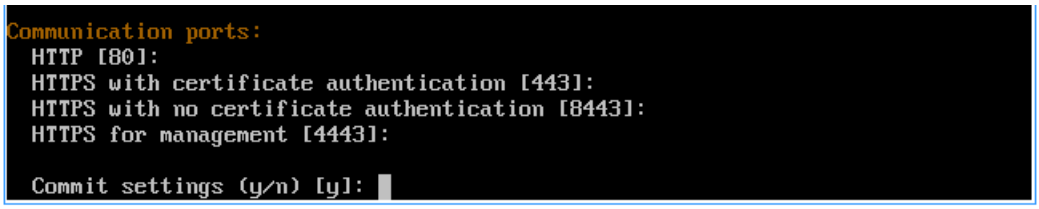
- For XenMobile Enterprise Edition deployments, the FQDN is the same as the XenMobile 9.0 MDM FQDN.
- For MAM deployments, the FQDN is the same as the XenMobile 9.0 App Controller FQDN.
- For MDM deployments, the FQDN is the same as the XenMobile 9.0 Device Manager FQDN.

> **Important**
>
> The FQDN for the 9.0 environment and for the 10.4 environment must match.



7. Type **y** to commit the settings.

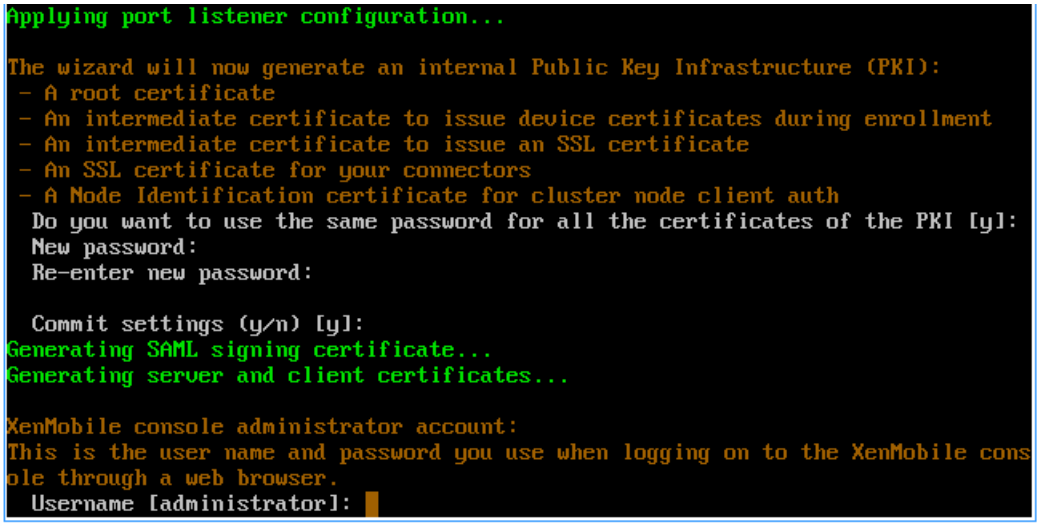
8. Set communication ports.



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.

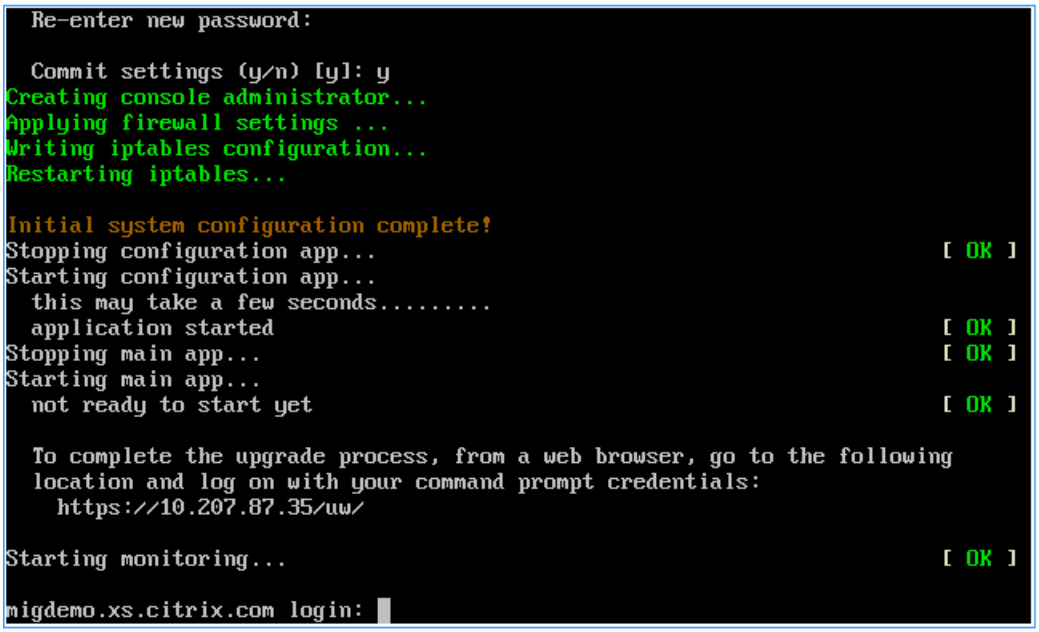
11. Type **y** to commit the settings.



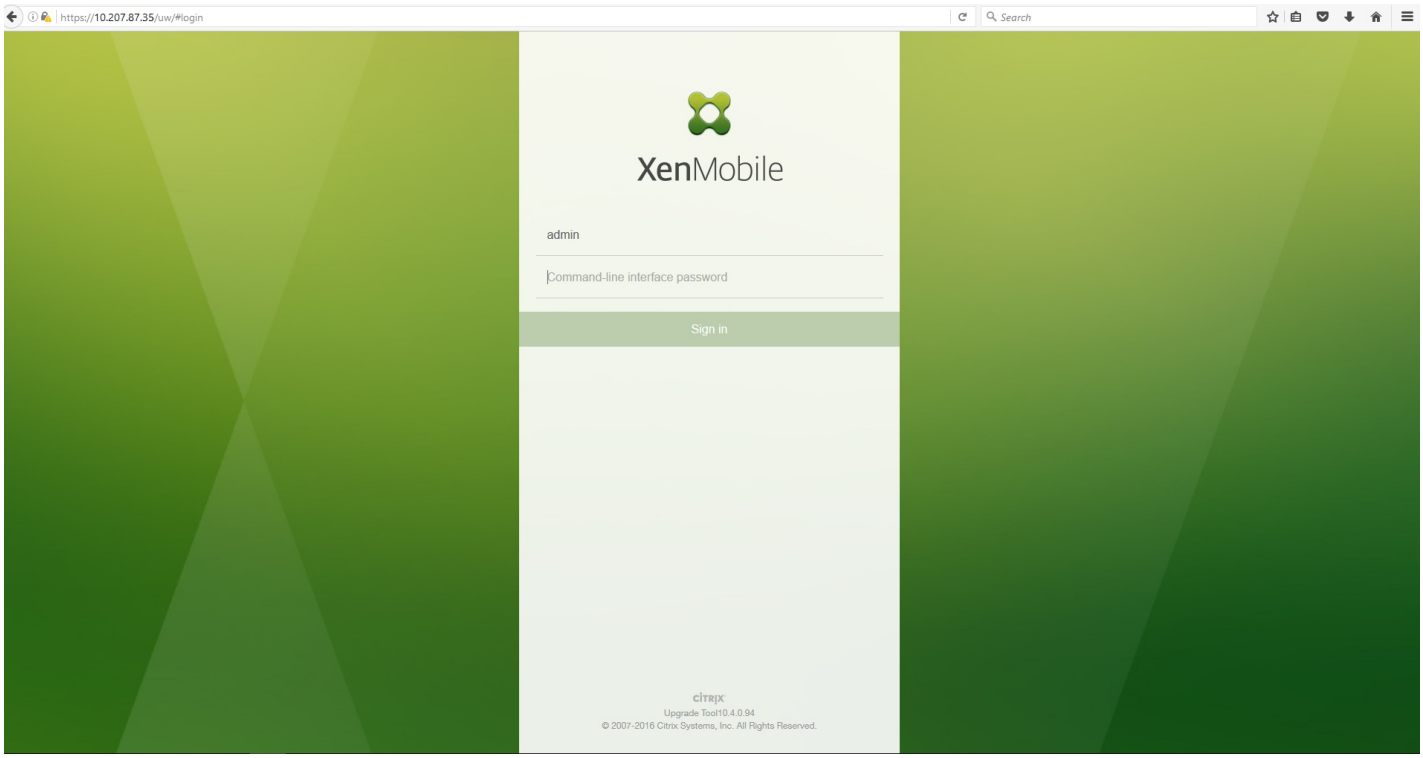
12. Type the user name and password for the XenMobile console administrator.

13. Type **y** to commit the settings.

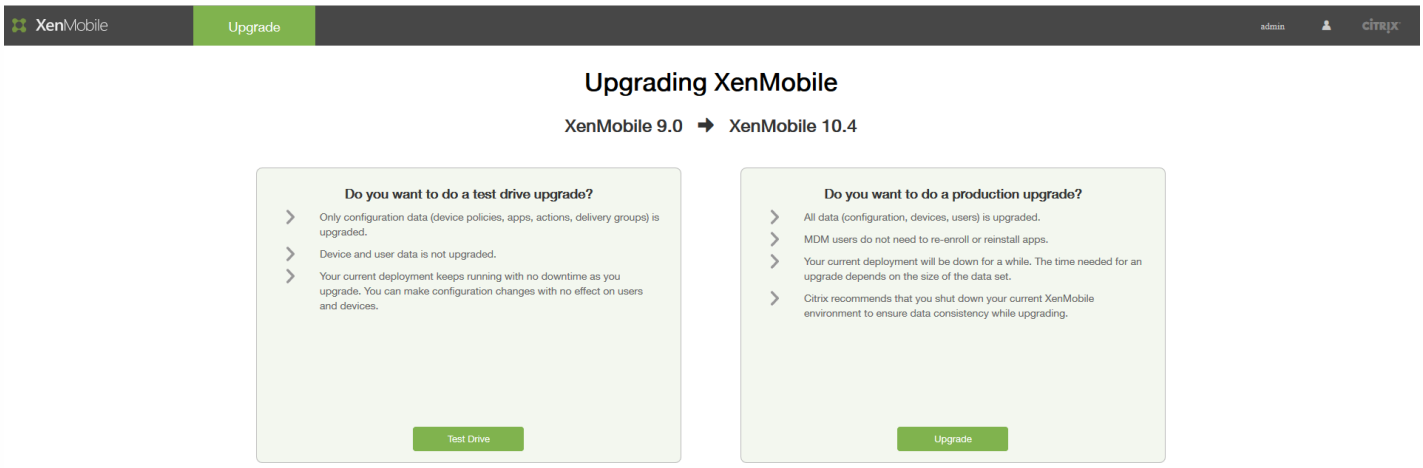
XenMobile 10.4 enables the one-time-only Upgrade Tool.



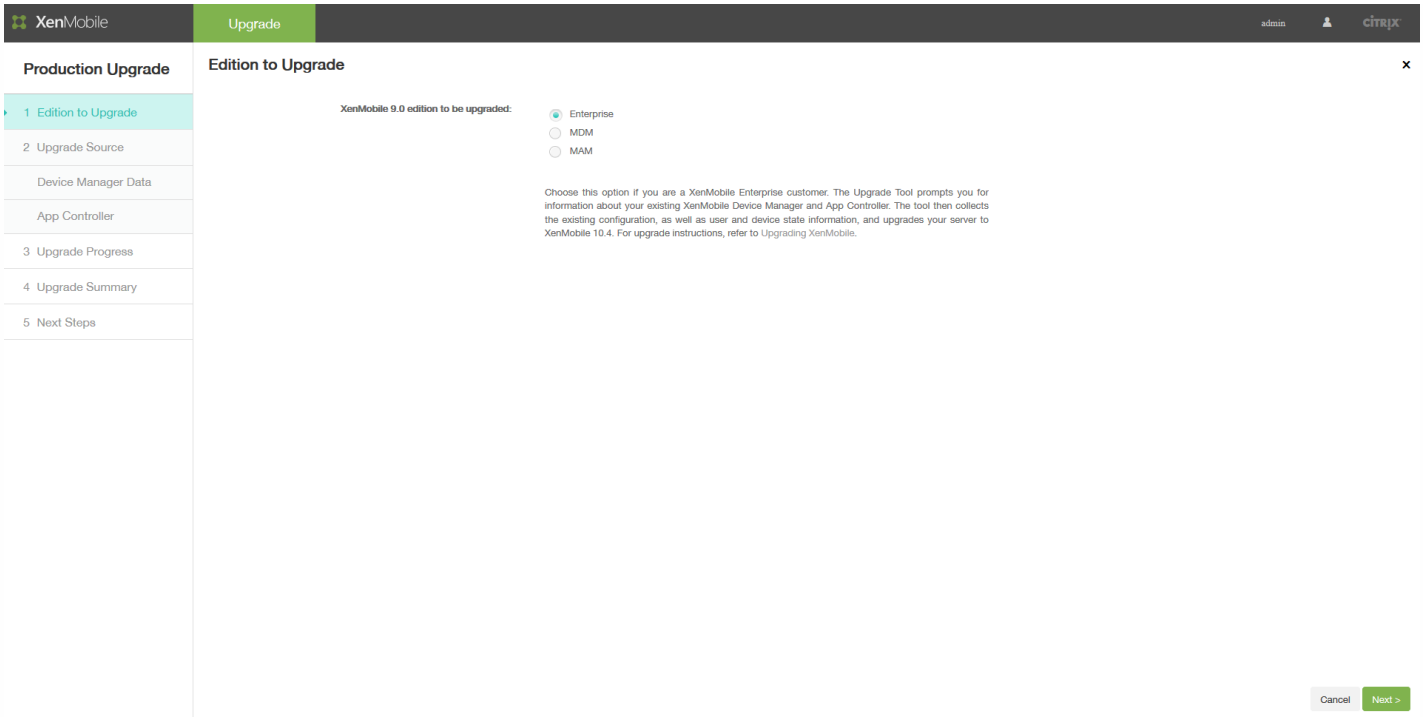
14. Access the Upgrade Tool on a web browser through https://<XenMobile-Server-IPAddress>/uw/ and log in using the credentials you specified using the CLI.



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**.



16. In the **Edition to Upgrade** page, select your edition. The example screen below shows Enterprise edition selected.



17. Click **Next**.

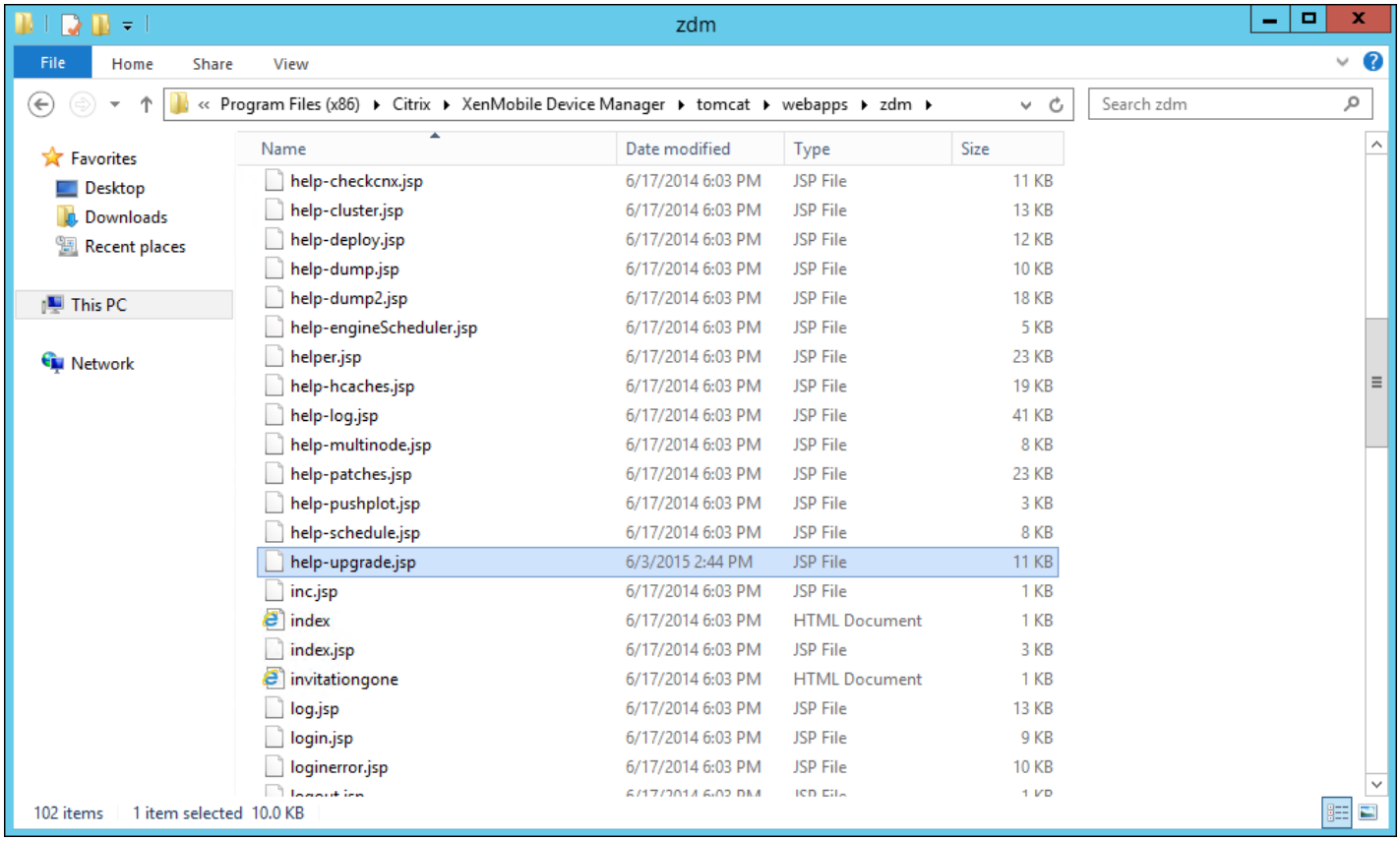
If you are upgrading a Enterprise or MDM edition, the **Device Manager** page appears. Follow steps 18 through 22 to complete this page.

If you are upgrading a MAM edition, skip to step 23 to complete the **App Controller** page.

18. Collect the files needed to migrate your existing XenMobile 9.0 Device Manager data. You will also get access to the database URL and user name that you will 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.

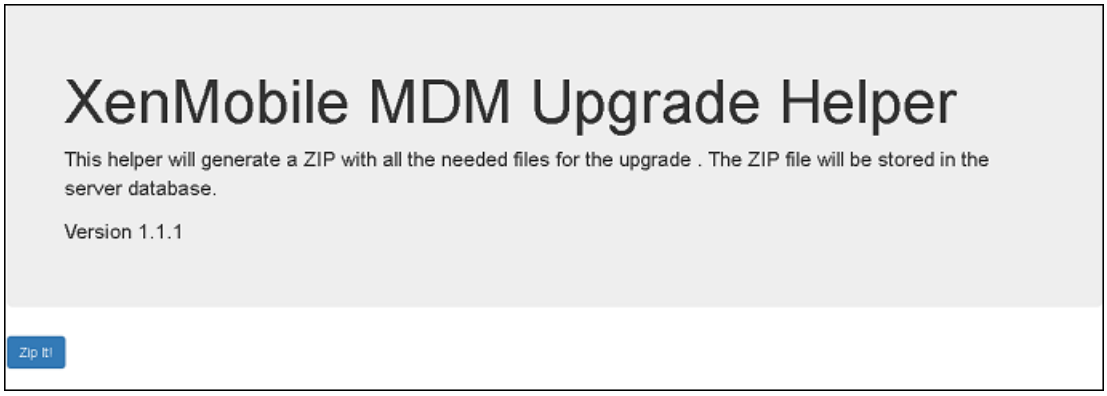
b. Extract the help-upgrade.jsp file to <MDM-Install-Path>\tomcat\webapps\zdm on your existing XenMobile 9.0 Device Manager.



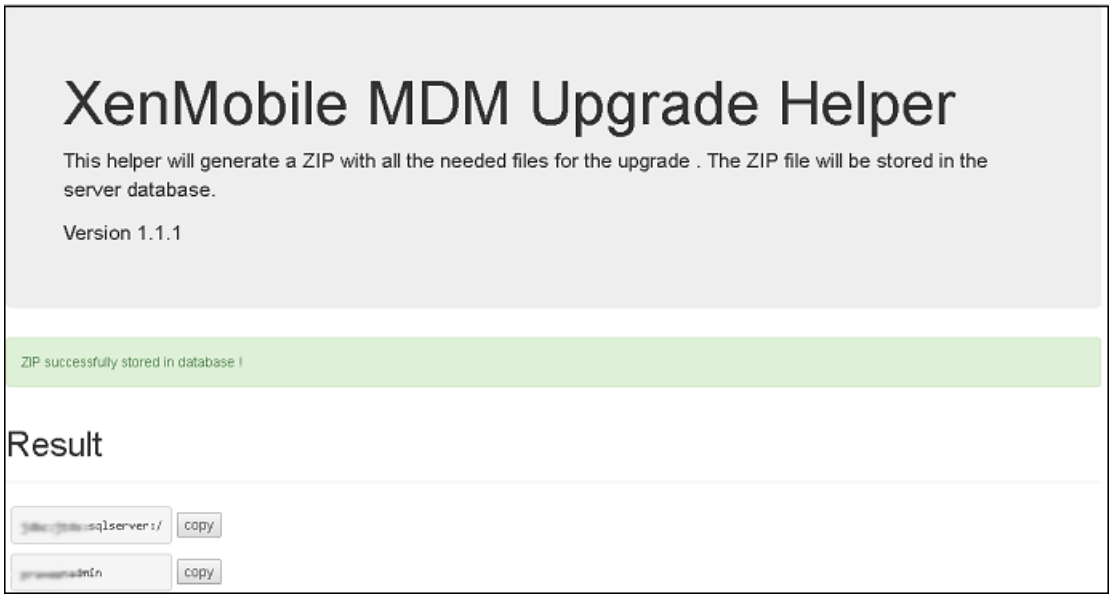
c. In a browser window, log on to the XenMobile 9.0 server.

d. In a separate browser tab, enter this URL: https://localhost/zdm/help-upgrade.jsp. This opens the **XenMobile MDM Upgrade Helper** page, which collects and zips all the files from XenMobile 9.0 that are needed for the upgrade to XenMobile 10.4. The zip file is then 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.



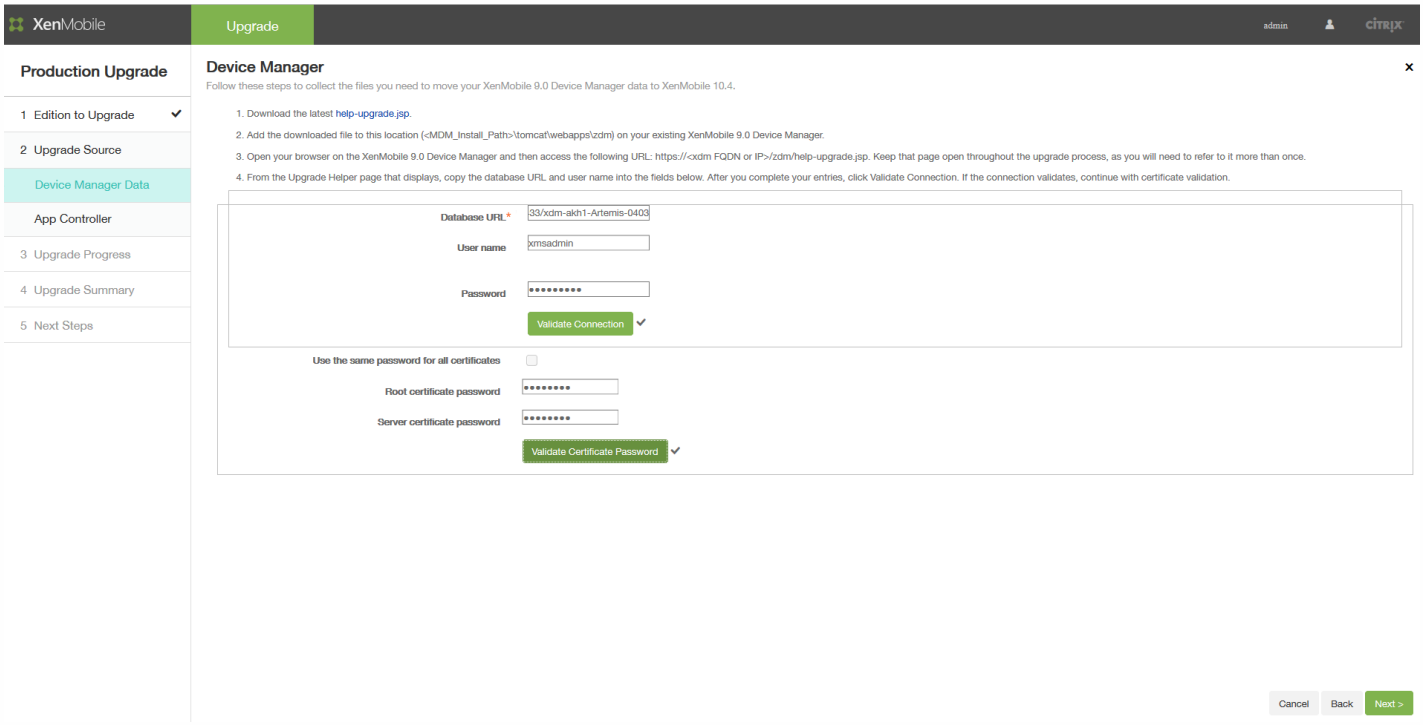
19. Under **Result**, copy the URL and paste it in the **Database URL** field in the Upgrade Tool's **Device Manager** page. Then copy the user name and copy it to the **Device Manager** page.



20. In the Upgrade Tool:

    a. Enter the password and then click **Validate Connection**.

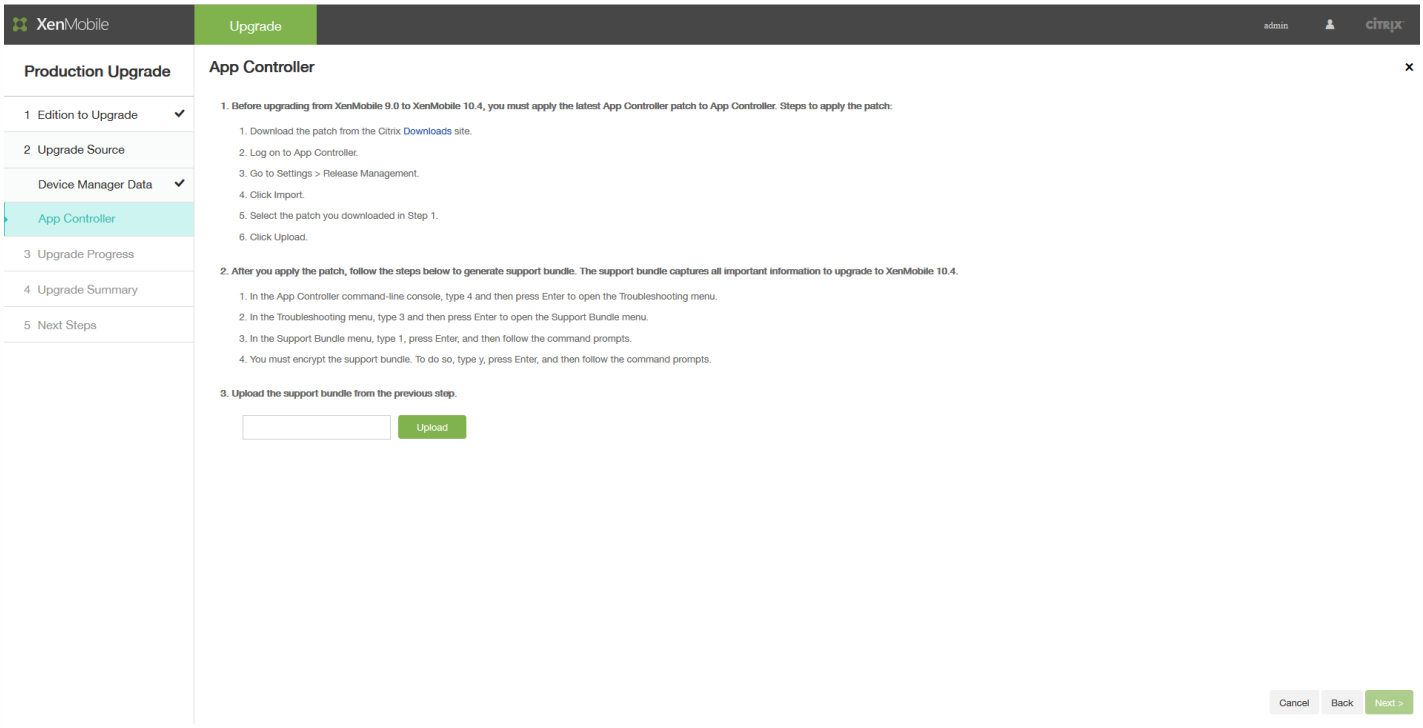
    b. Enter the password for each certificate and then click **Validate Password**.



21. Click **Next**.

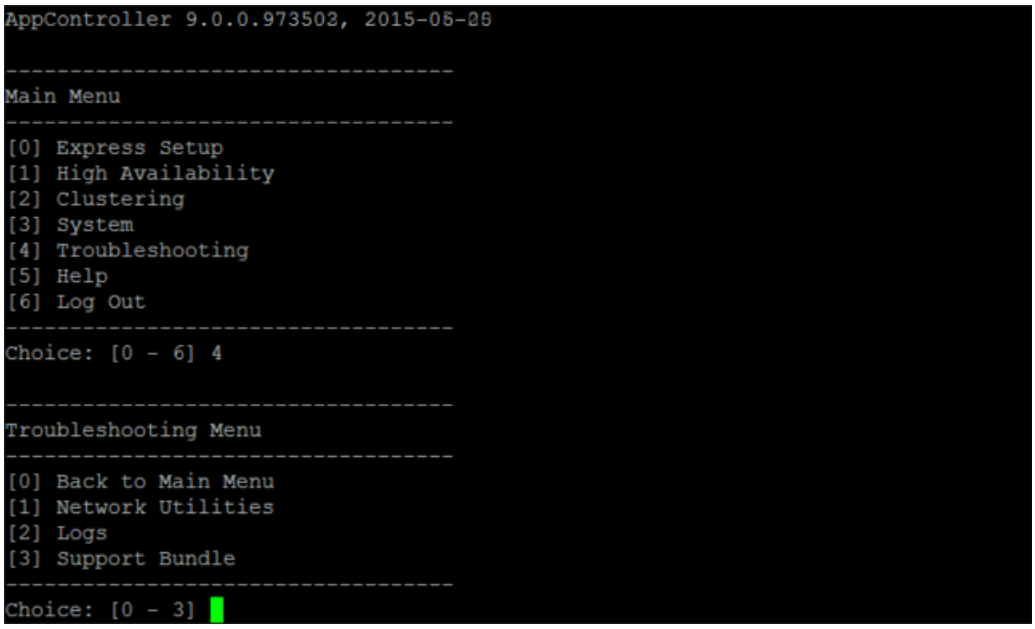
22. If you changed the ew-config.properties file, restart the xdm service on XenMobile 9 MDM and then go to https://localhost/zdm/help-upgrade.jsp to run the zip again. Doing so re-reads the ew-config.properties file and saves it to the XenMobile MDM 9 database to prepare for migration.

23. Next you will 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 the **App Controller** page to upgrade App Controller.

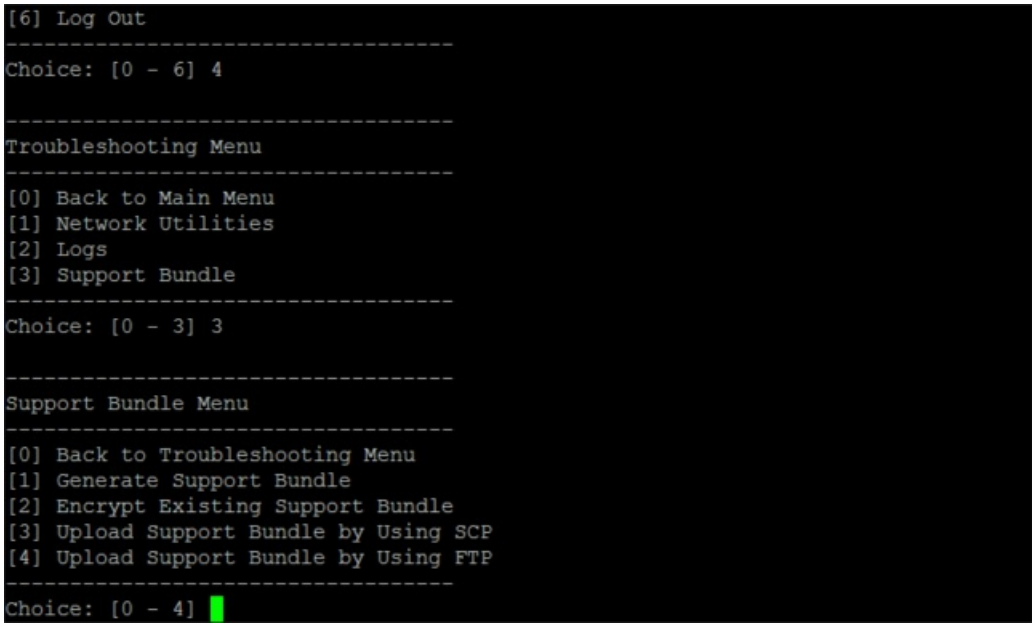


25. Continue to the instructions in section 2 of the **App Controller** page:

a. In the App Controller command-line console, type **4** and then press ENTER to open the Troubleshooting menu.

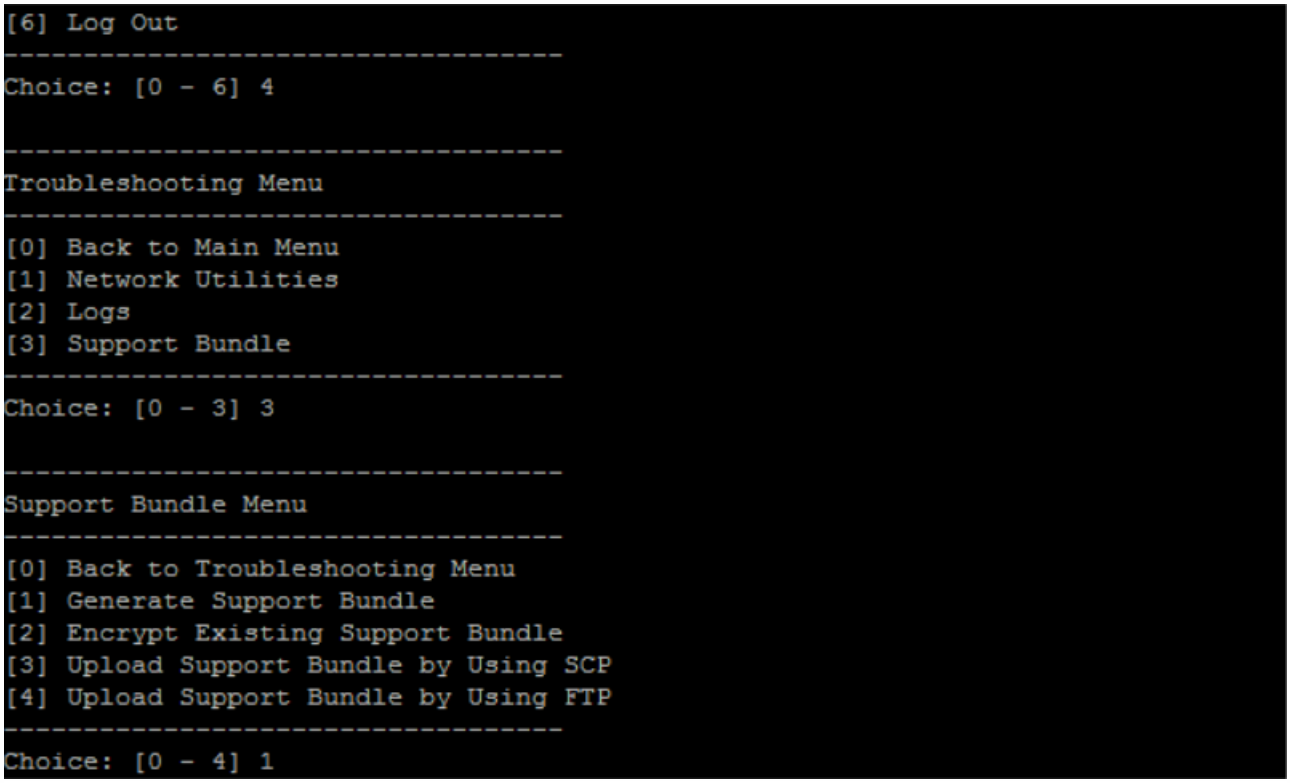


b. In the Troubleshooting menu, type **3** and then press ENTER to open the Support Bundle menu.



c. In the Support Bundle menu, type **1**, press ENTER, and then follow the command prompts.

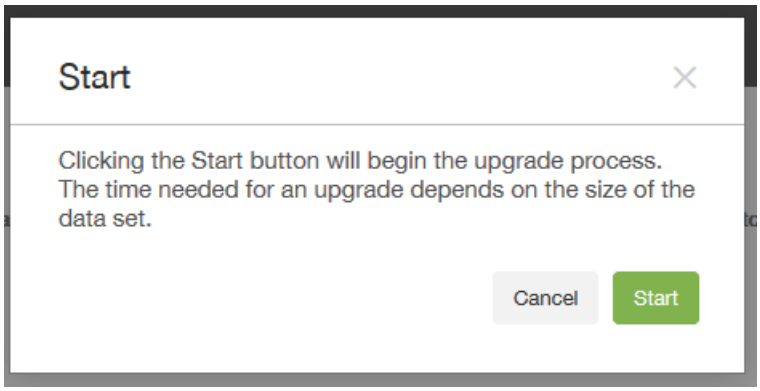
Note: You must encrypt the support bundle.



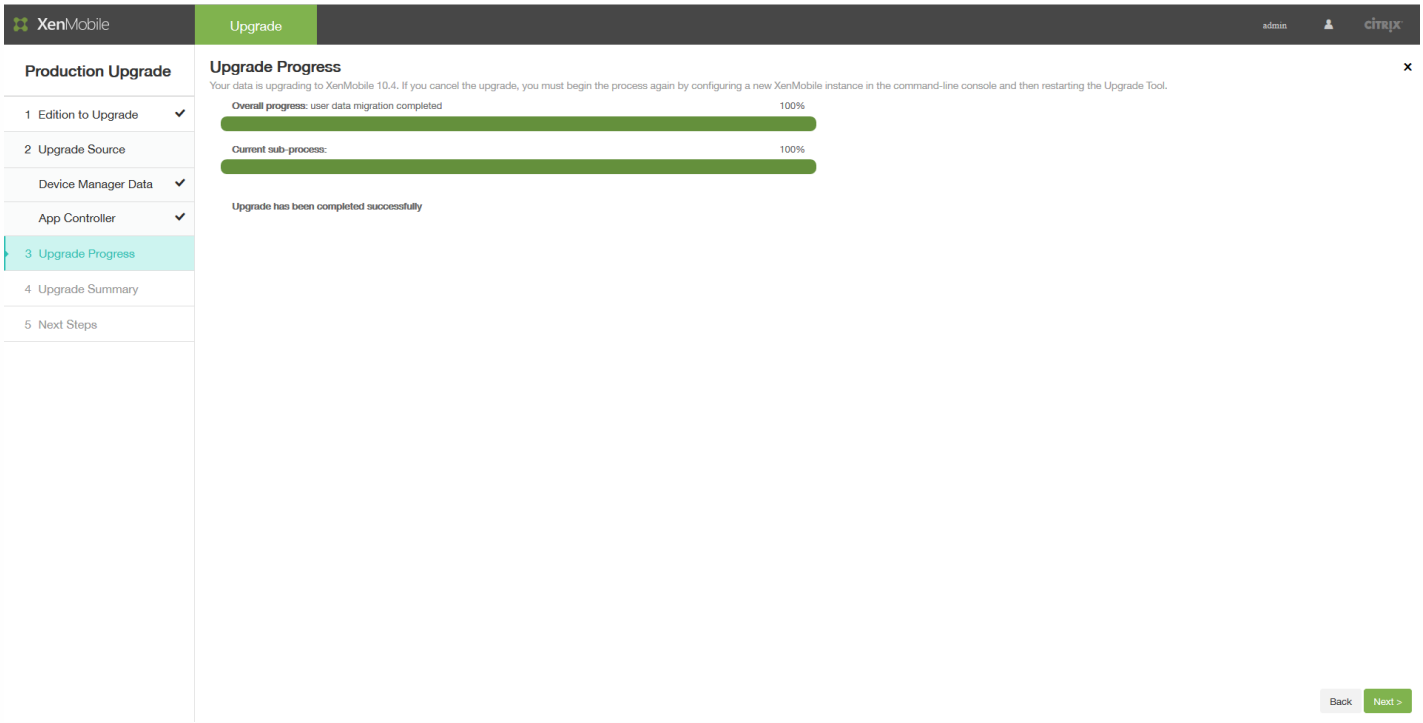
26. In section 3 of the the **App Controller** page, specify the support bundle and then click **Upload**.

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 a large number of users.

27. Click **Next**. The **Start** confirmation dialog box appears.



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.



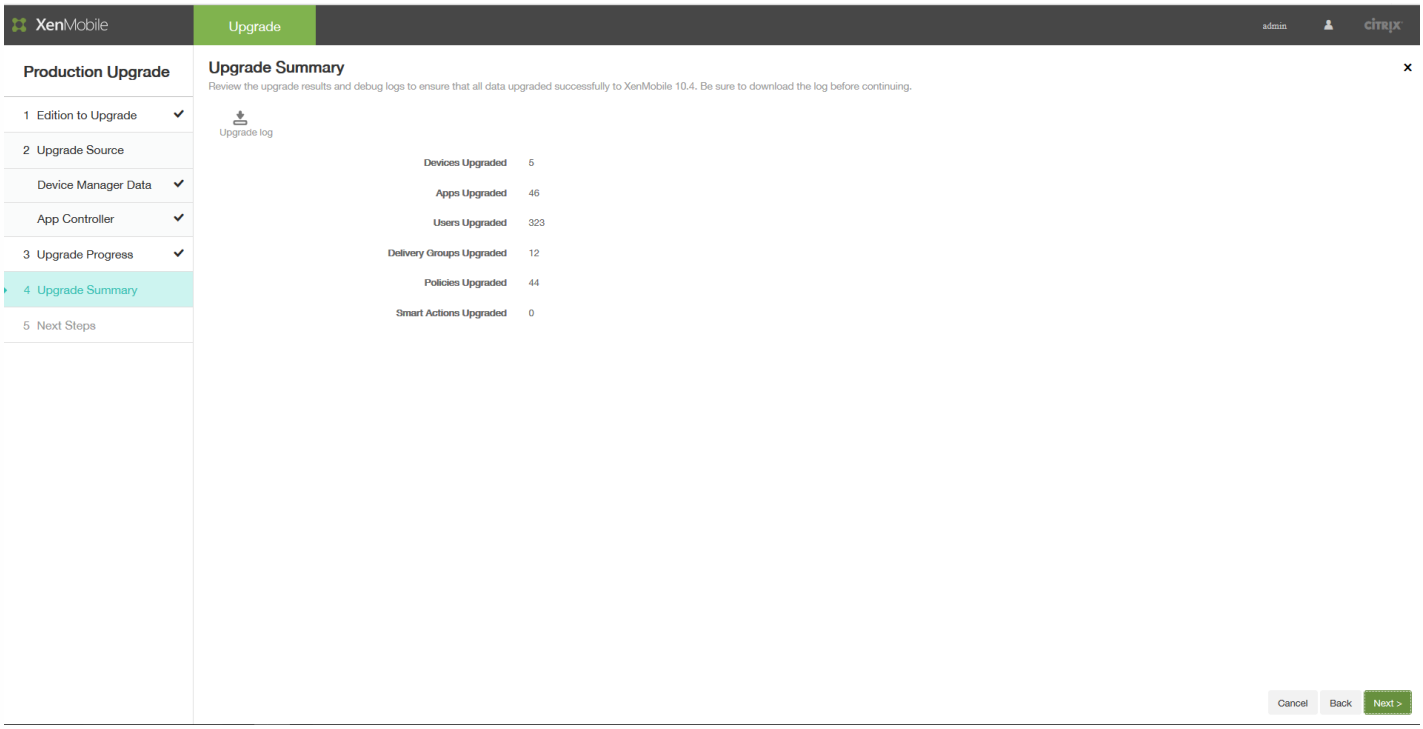
Note

If the upgrade fails, you can view the logs to understand the reason for the error. Then, you need to import a new XenMobile 10.4 instance and restart the upgrade process. You cannot use the browser Back button to return to earlier pages and correct information.

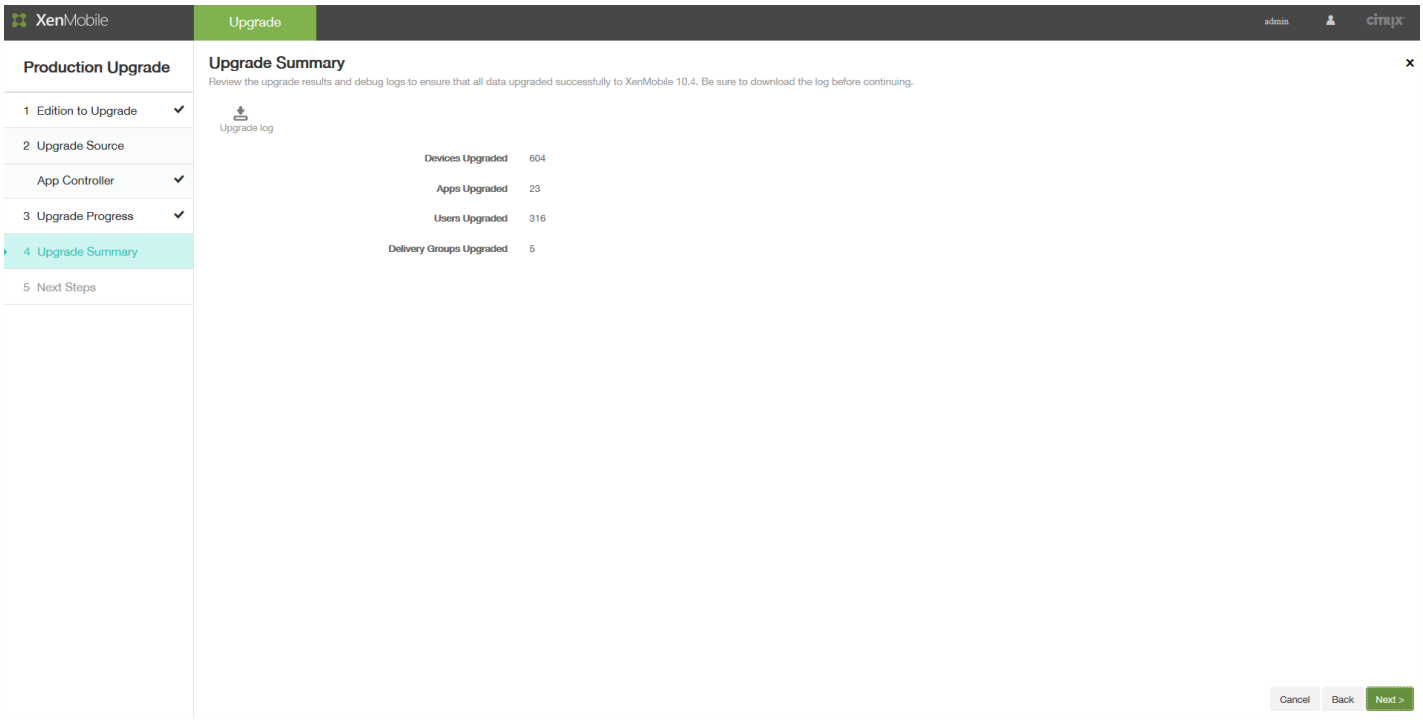
The Upgrade Progress page lets you know when the upgrade has completed successfully.

29. Click **Next**. The **Upgrade Summary** page appears.

If you are upgrading an Enterprise or MAM edition, the **Upgrade Summary** page might look like this:



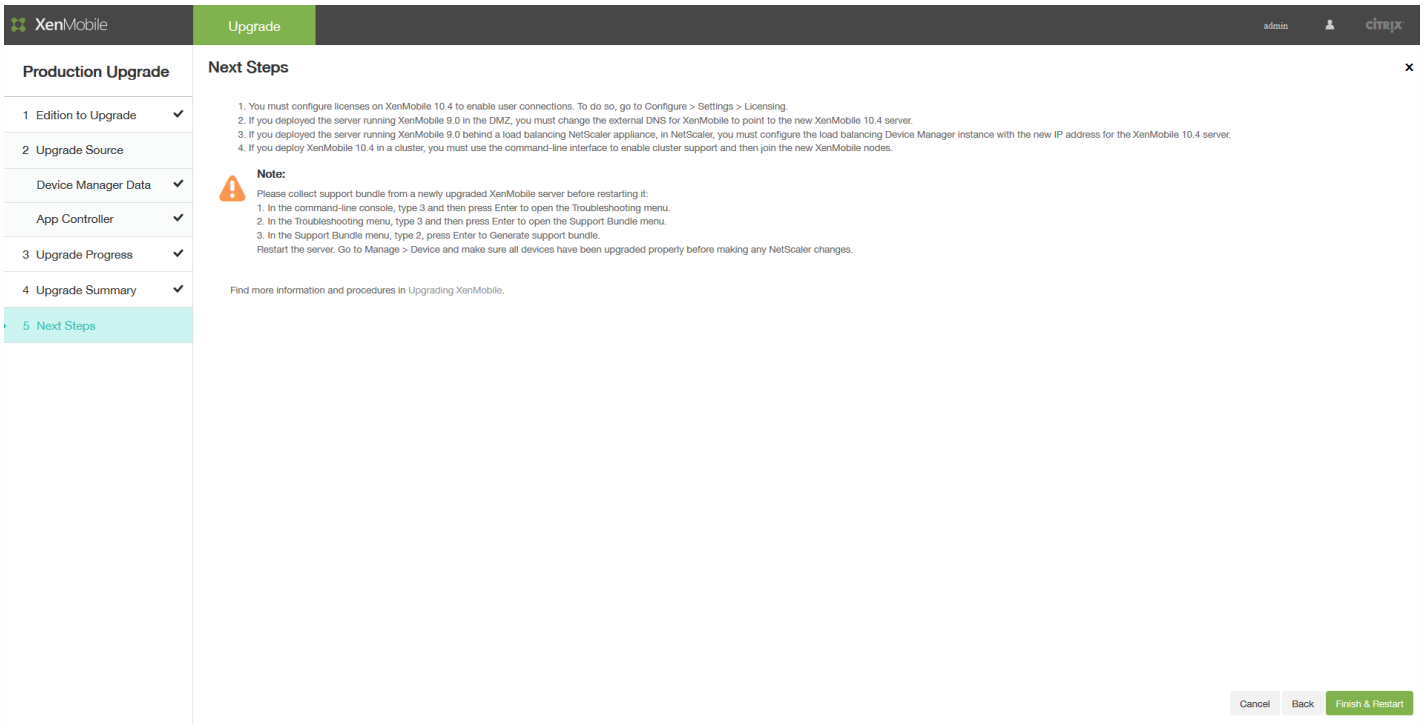
If you are upgrading an MDM edition, the **Upgrade Summary** page might look like this:



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 the policies, settings, user data, and so on that was or was not upgraded to XenMobile 10.4.

31. After you download the upgrade log, click **Next**. The **Next Steps** page appears.



For instructions related to those steps, see Upgrade Tool Post-Requisites.

Upgrade Tool post-requisites

Nov 29, 2016

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 10.4 server.

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 XenMobile 10.4 in a cluster, you must use the XenMobile 10.4 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.

Configure licenses on XenMobile to enable user connections

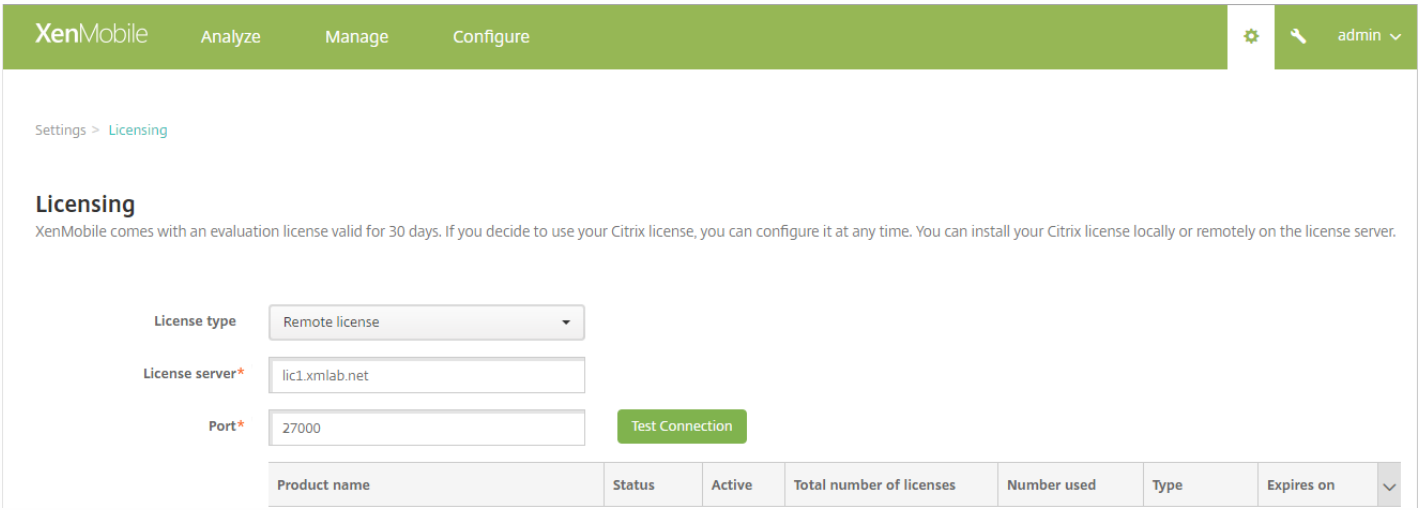
XenMobile 10.4 only supports Citrix V6 licensing. You must set the local or remote license configuration in the XenMobile 10.4 console to enable user connections, as follows.

1. Download the license file. To do so, see Citrix Licensing.

2. Log on to the upgraded XenMobile 10.4 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**.



For more details about adding local and remote licenses, see Licensing.

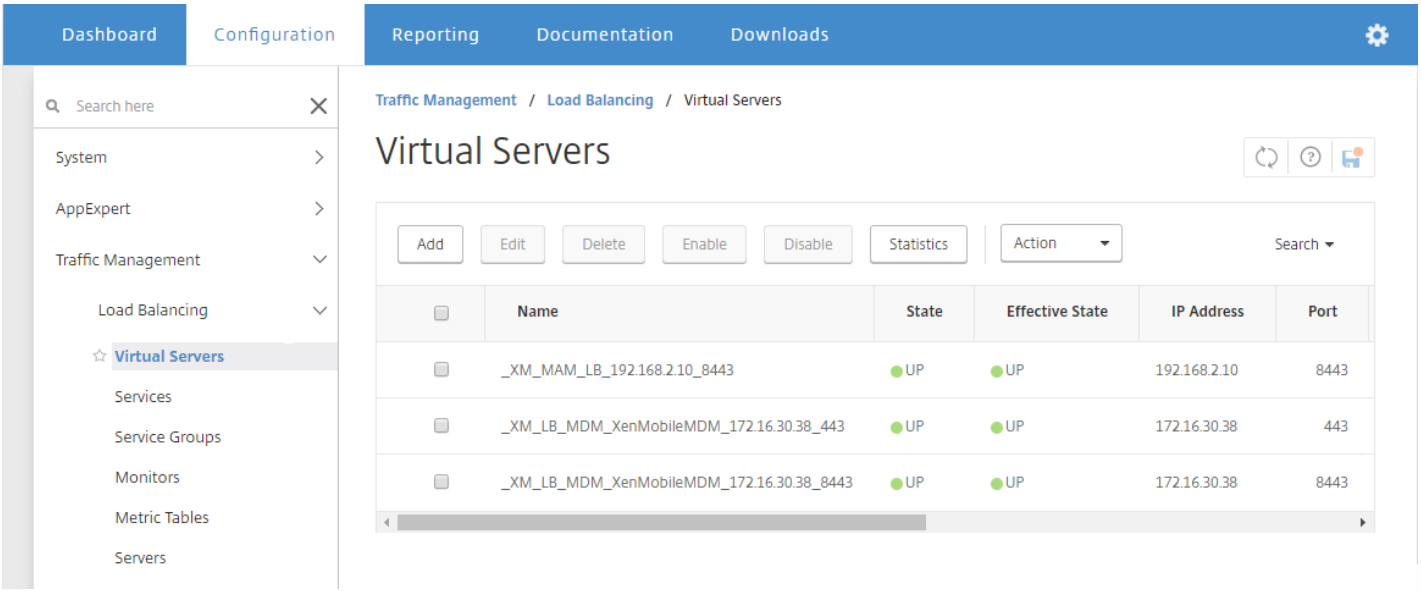
Configure a new load balancing virtual server for the upgrade

> ### 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 XenMobile 10.4, 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.

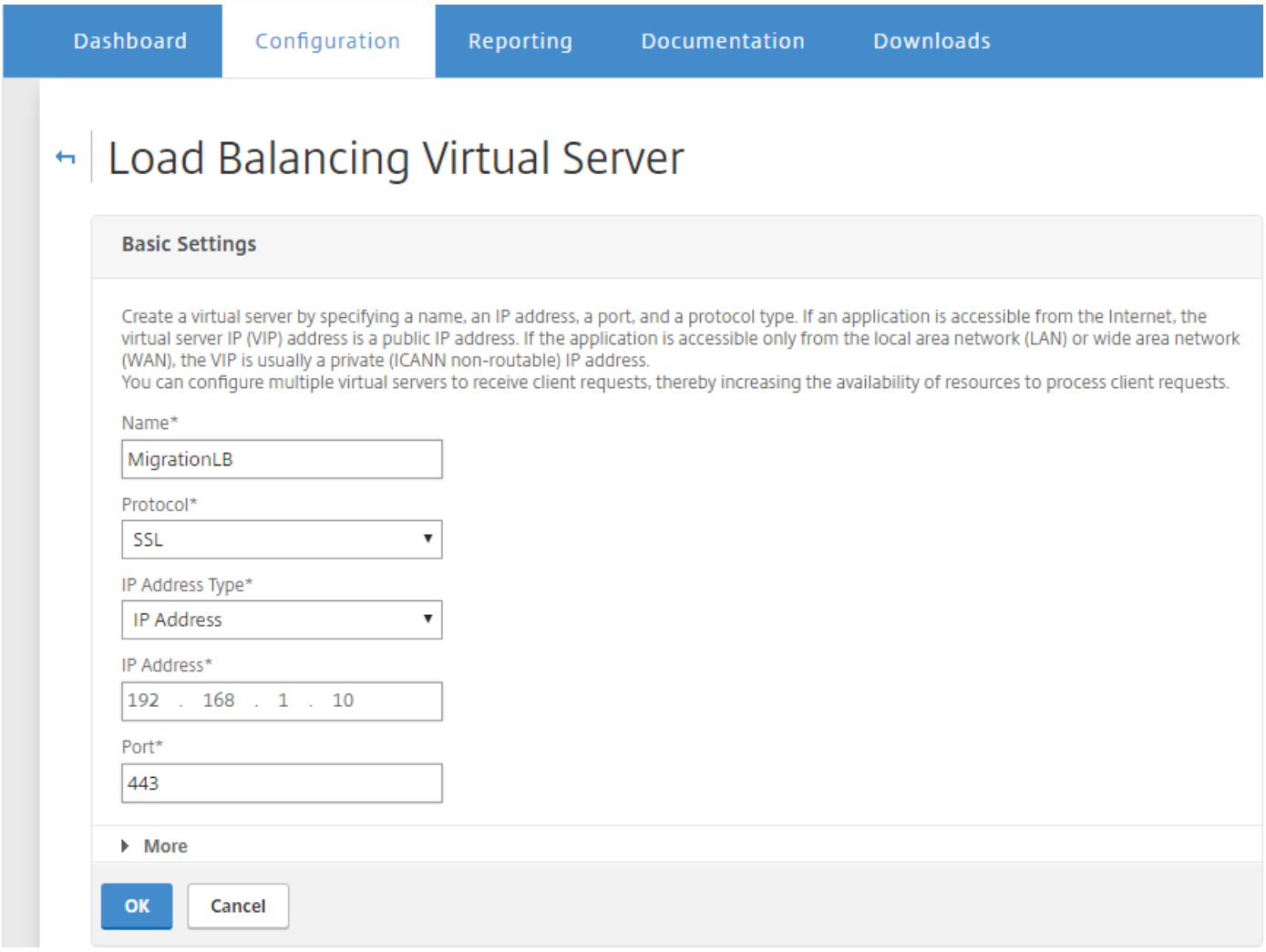
The example screens in this section, for NetScaler Gateway 11.1, are similar to NetScaler Gateway versions 11.0 and 10.5.

1. Click **Traffic Management > Load Balancing > Virtual Servers**.



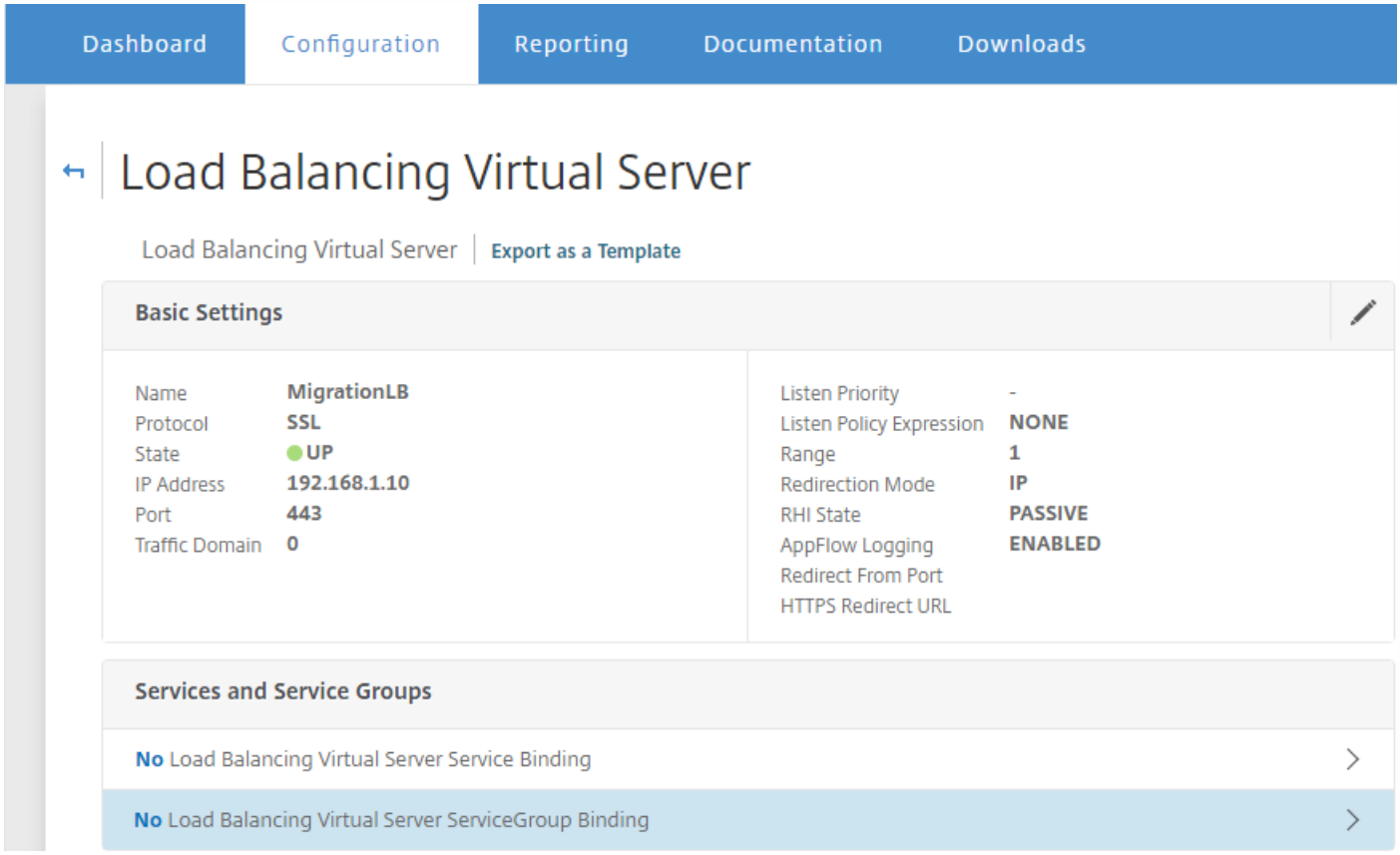
2. Click **Add**.

3. On the **Load Balancing Virtual Server** page, configure the following settings and then click **OK**.

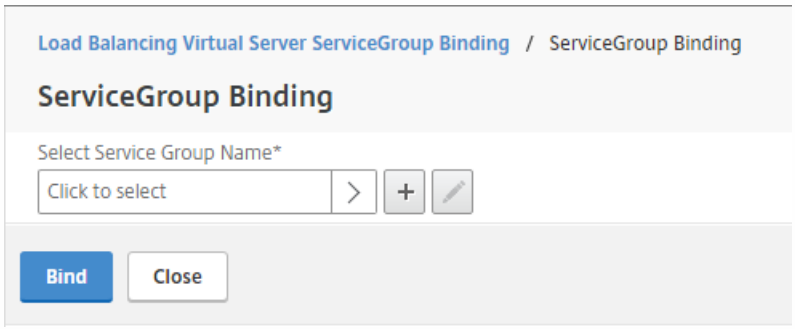


- **Name**: Type a name for the new load balancer.
- **Protocol**: Set to **SSL**. The default is **HTTP**.
- **IP Address**: Enter an IP address for the new load balancer, which follows RFC 1918; for example 192.168.1.10.
- **Port**: Set to **443**.

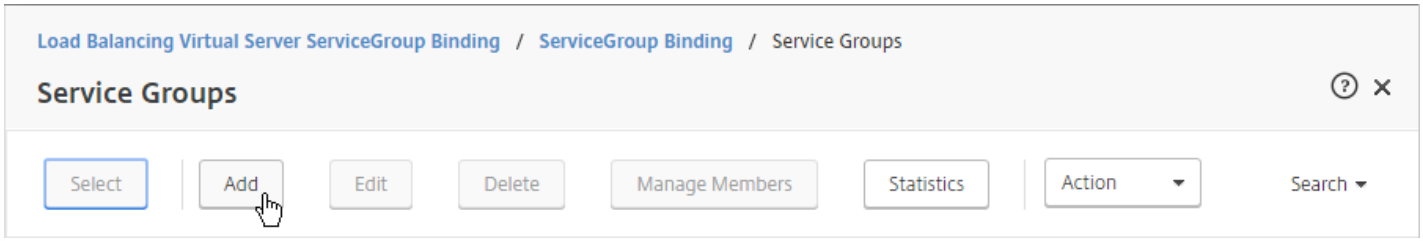
4. Under **Services and Service Groups**, click **No Load Balancing Virtual Server Service Group Binding**.



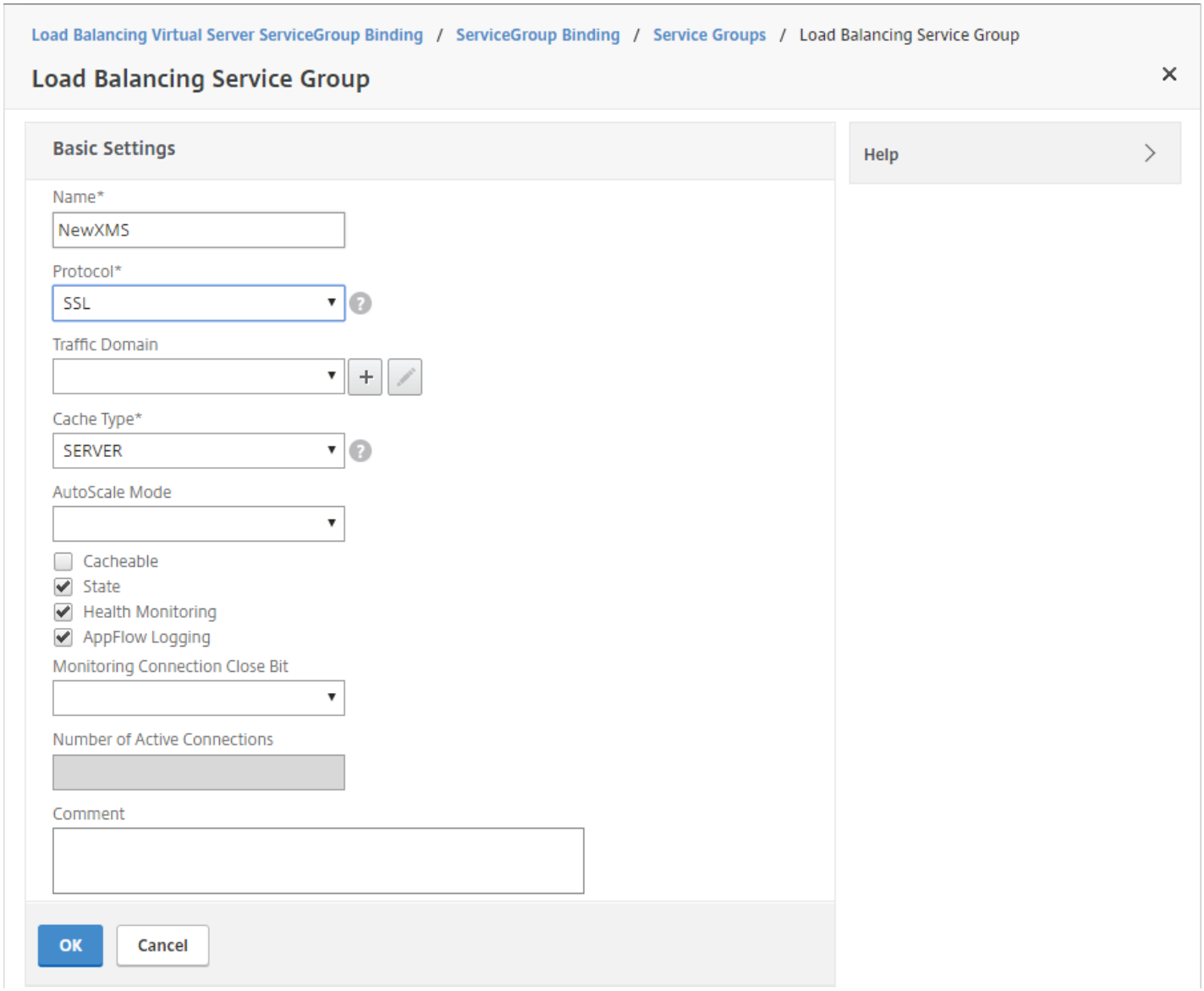
5. Under **Select Service Group Name**, click **Click to Select**.



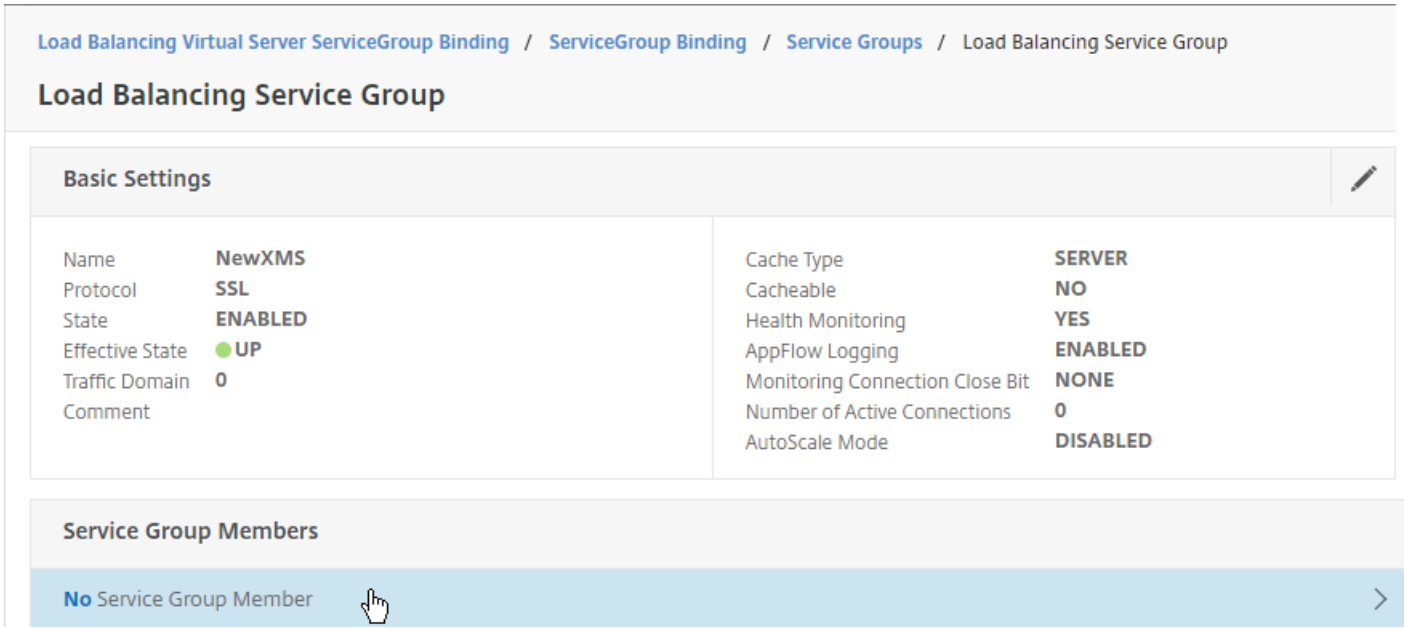
6. Click **Add** to create a new service group.



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**.

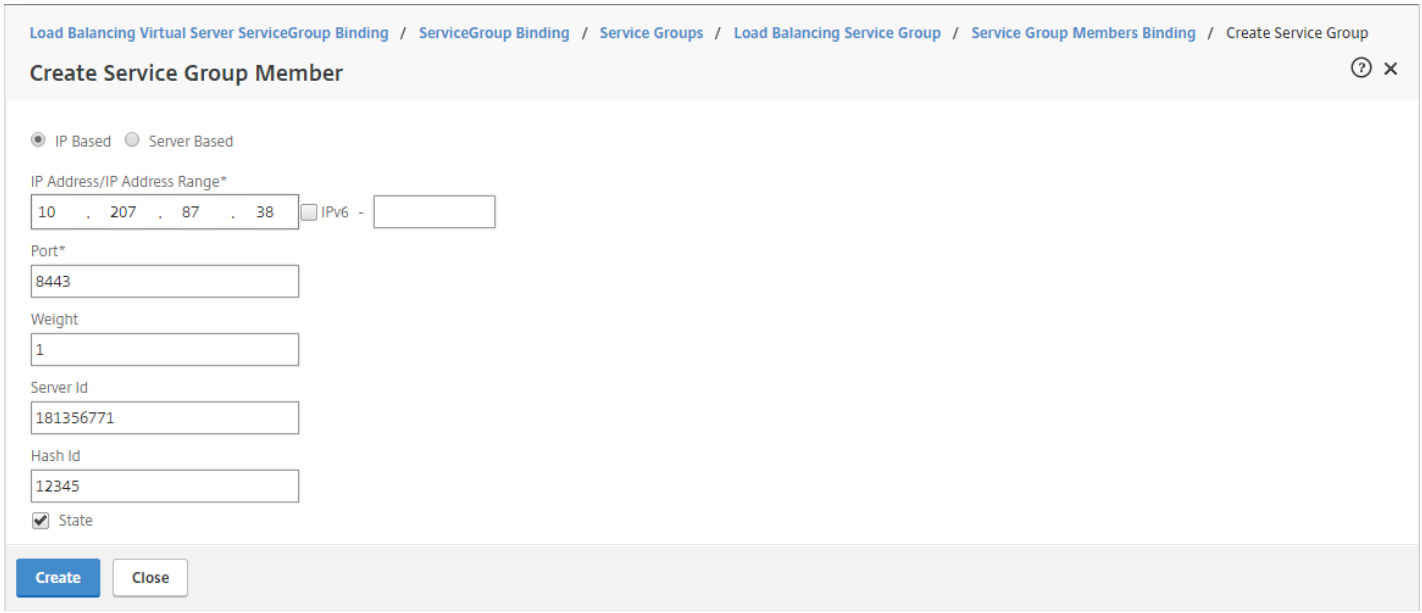


8. Click **No Service Group Member**.

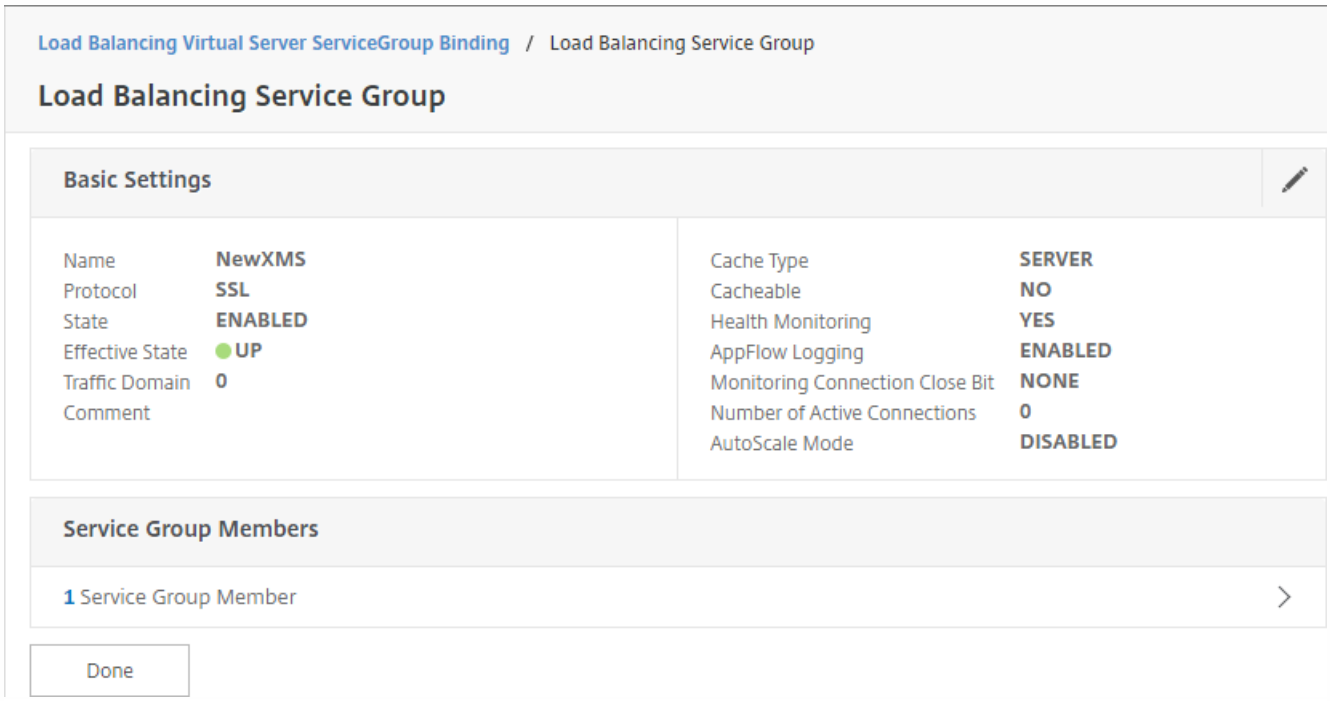


9. On the **Create Service Group Member** page, configure the following settings:

- **IP Address/IP Address Range**: Enter the IP address for XenMobile 10.4 server.
- **Port**: Set to **8443**.
- **Server ID**: If you are migrating from a clustered XenMobile 9.0 environment to a XenMobile 10.4 clustered environment, enter the server node ID for the current XenMobile server. To obtain the server node ID, log on to the XenMobile 10.4 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**.

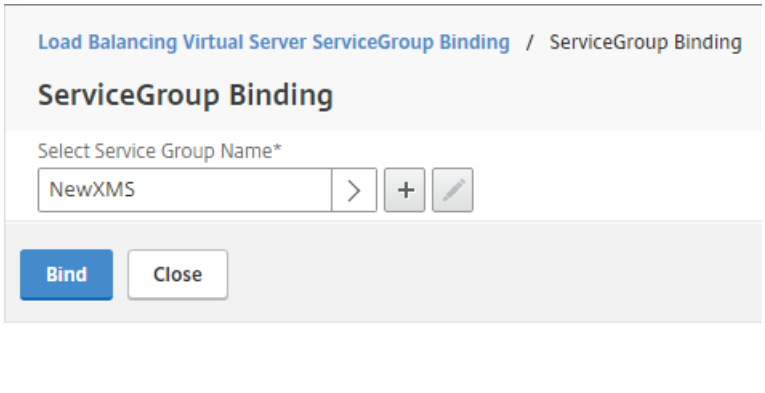


10. Click **Create** and then click **Done**.

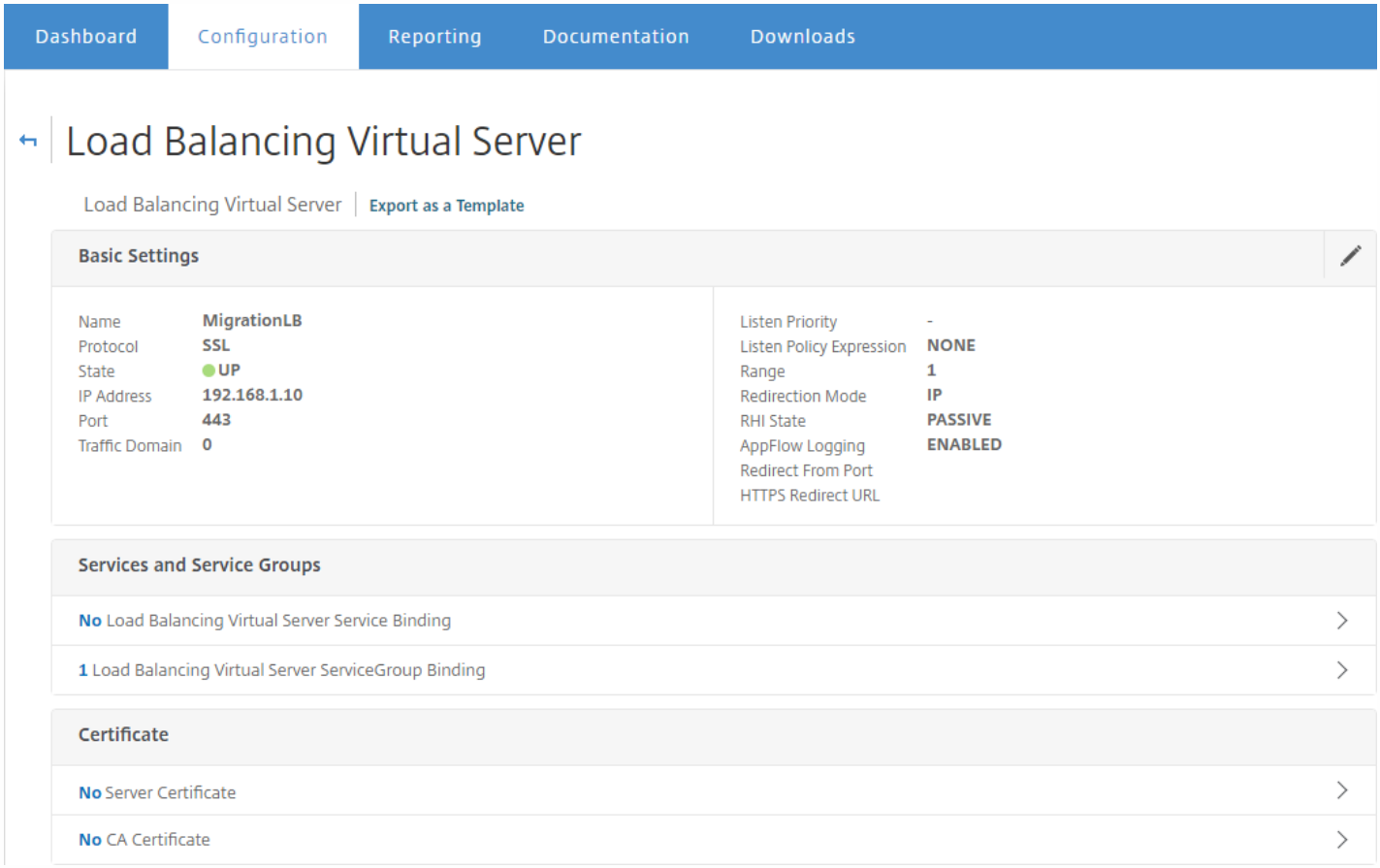


11. Click **Done** and then **OK**.

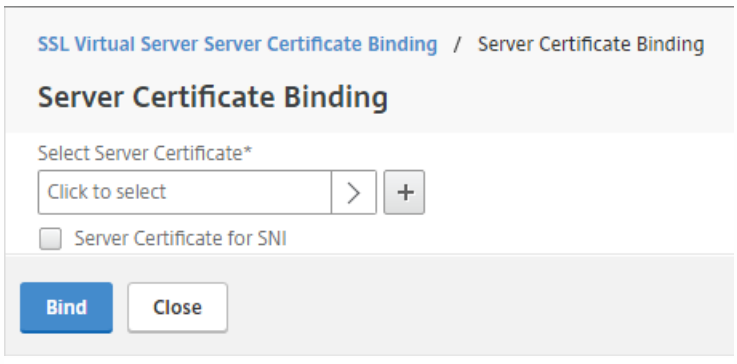
12. Click **Bind** and then on the next screen, click **Done**.



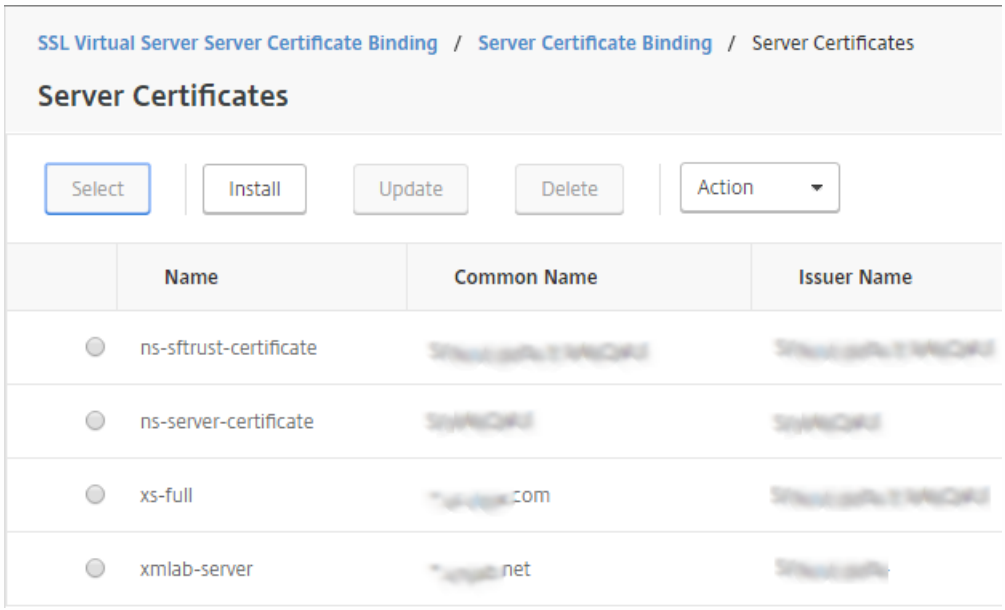
13. Under **Certificates**, click **No Server Certificate**.



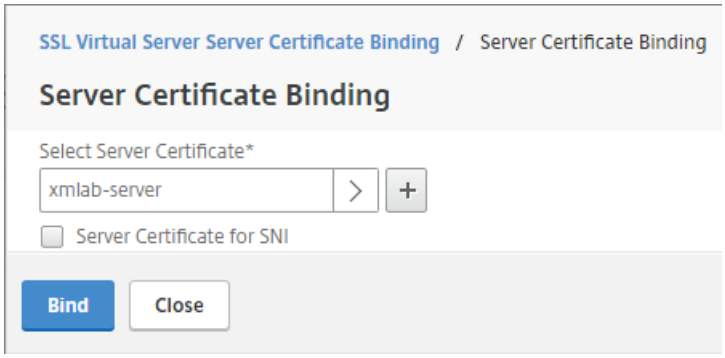
14. Under **Server Certificate Binding**, click **Click to Select**.

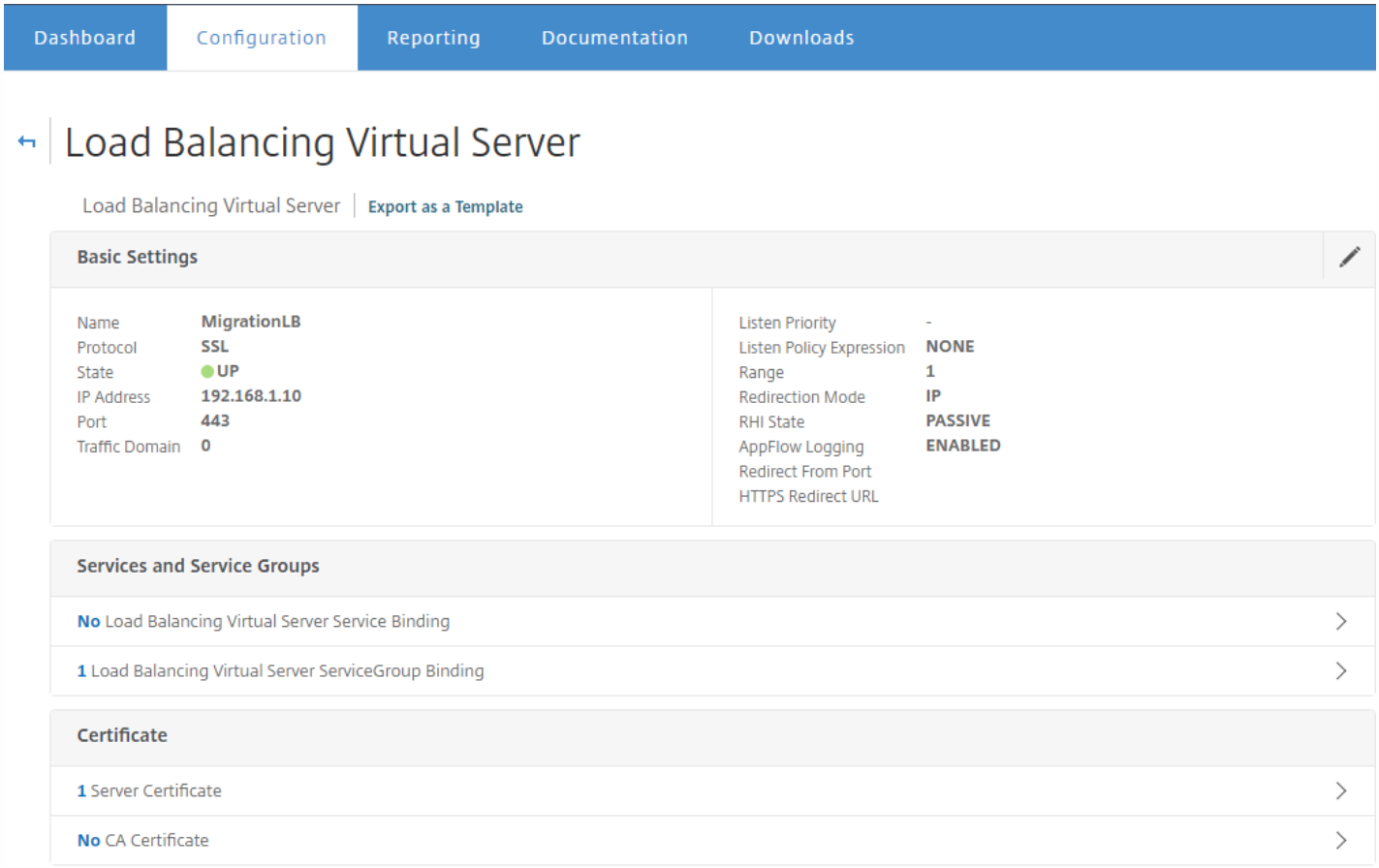


15. Under **Certificates**, click the XenMobile 9.0 server certificate you exported in Upgrade Tool prerequisites and then click **OK**.

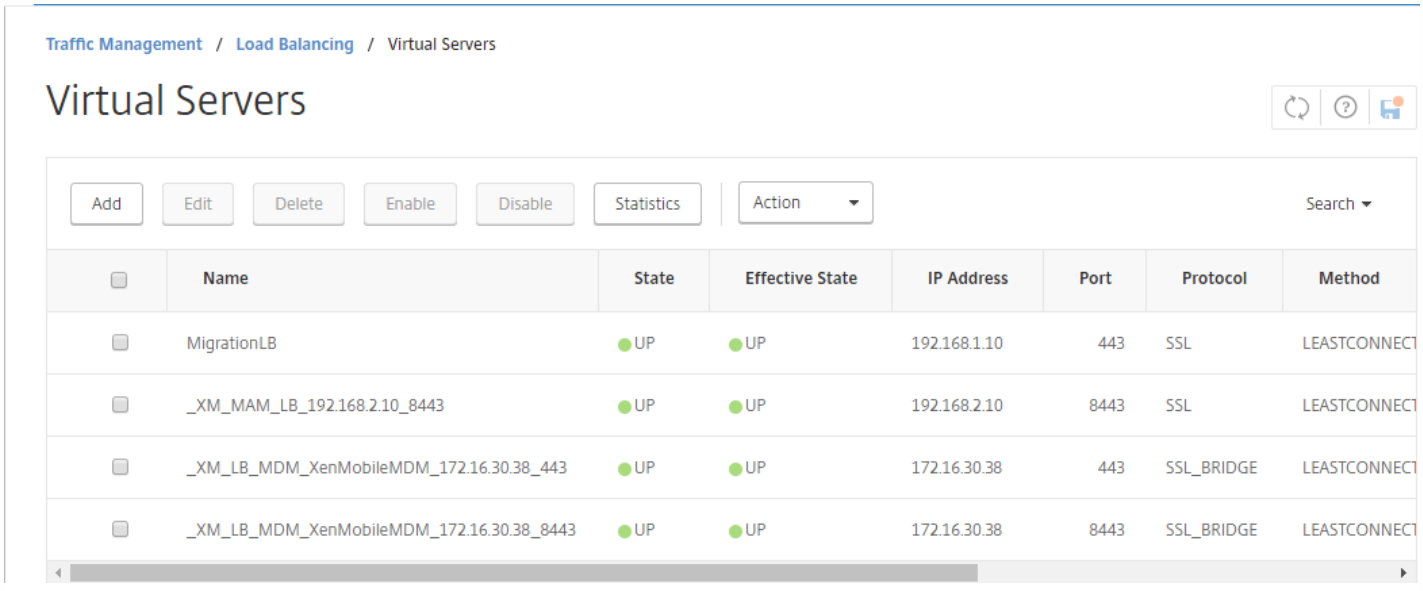


16. Click **Bind** and then on the next screen, click **Done**.





17. Click the refresh button to confirm that the server is up.

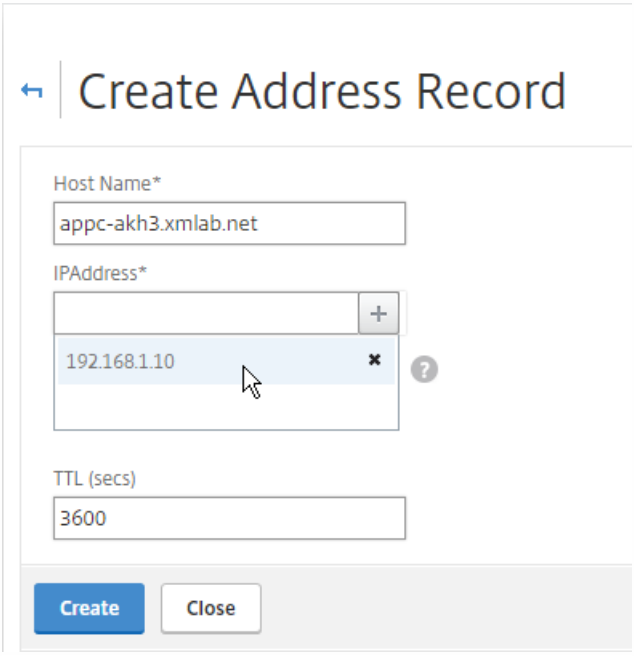


Configure an address record to point the App Controller server FQDN to the new load balancer for the upgrade

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.



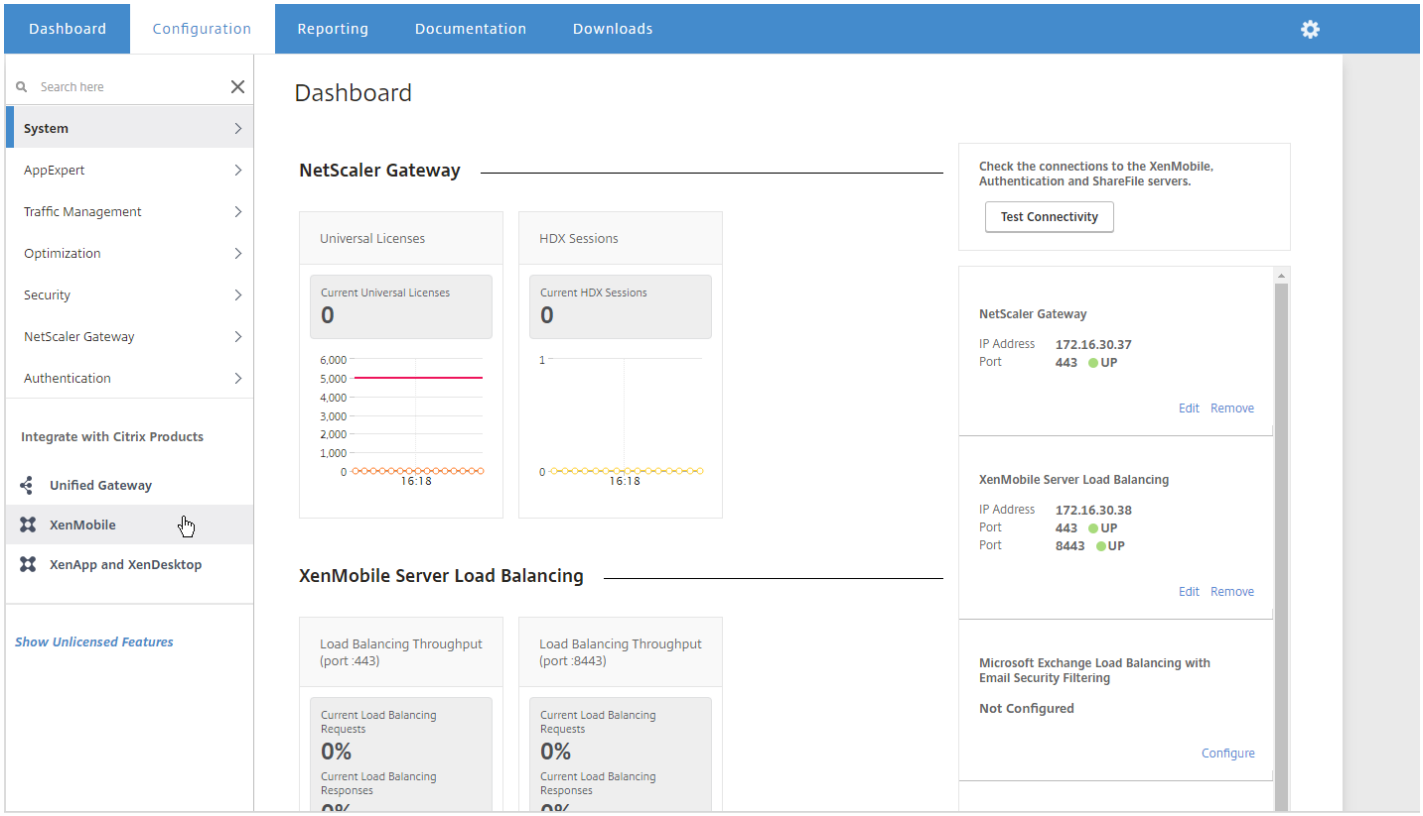
Change the Device Manager load balancing virtual server to point to the new XenMobile server IP address

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 XenMobile 10.4 server.

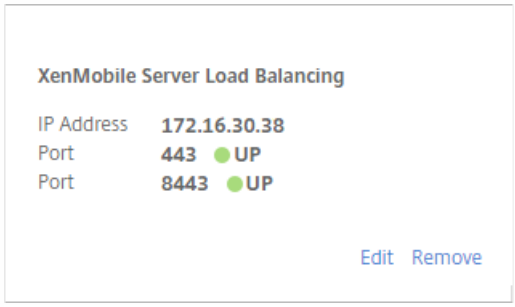
The procedure differs depending on whether you're using NetScaler 11.1 or NetScaler versions 11.0 or 10.5.

For NetScaler 11.1

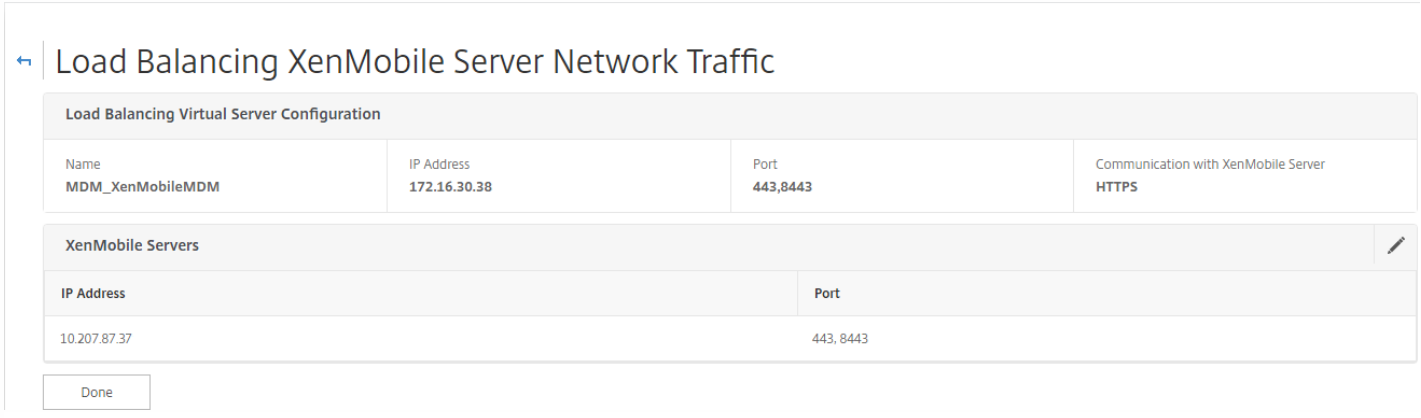
1. Under **Integrate with Citrix Products**, click **XenMobile**.



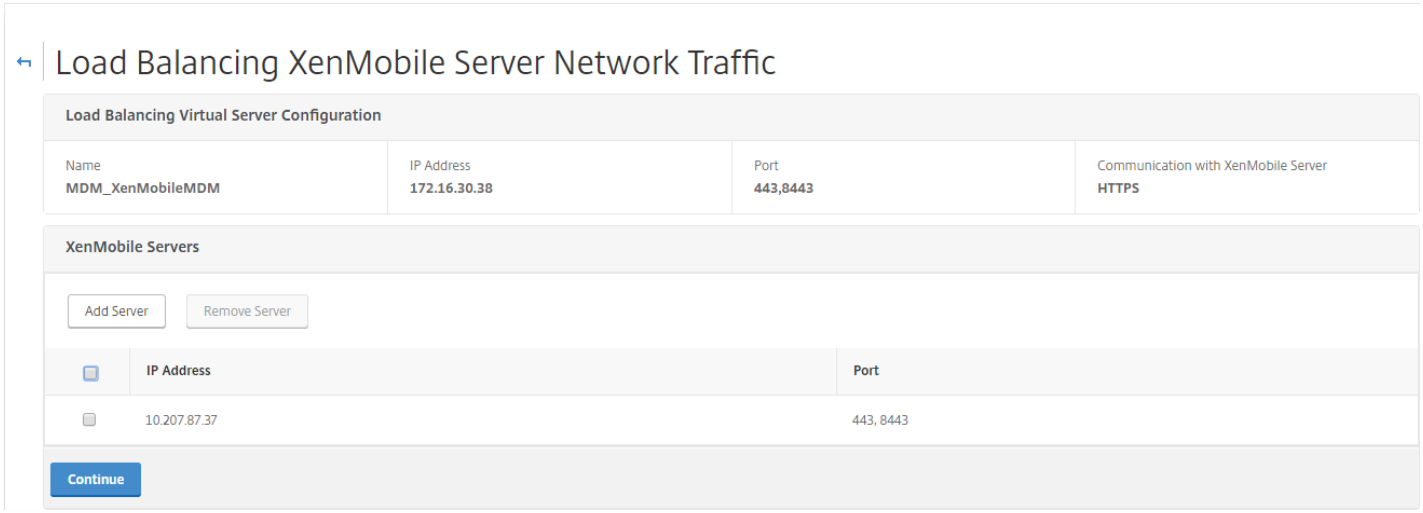
2. On the right side of the screen, under **XenMobile Server Load Balancing**, click **Edit**.



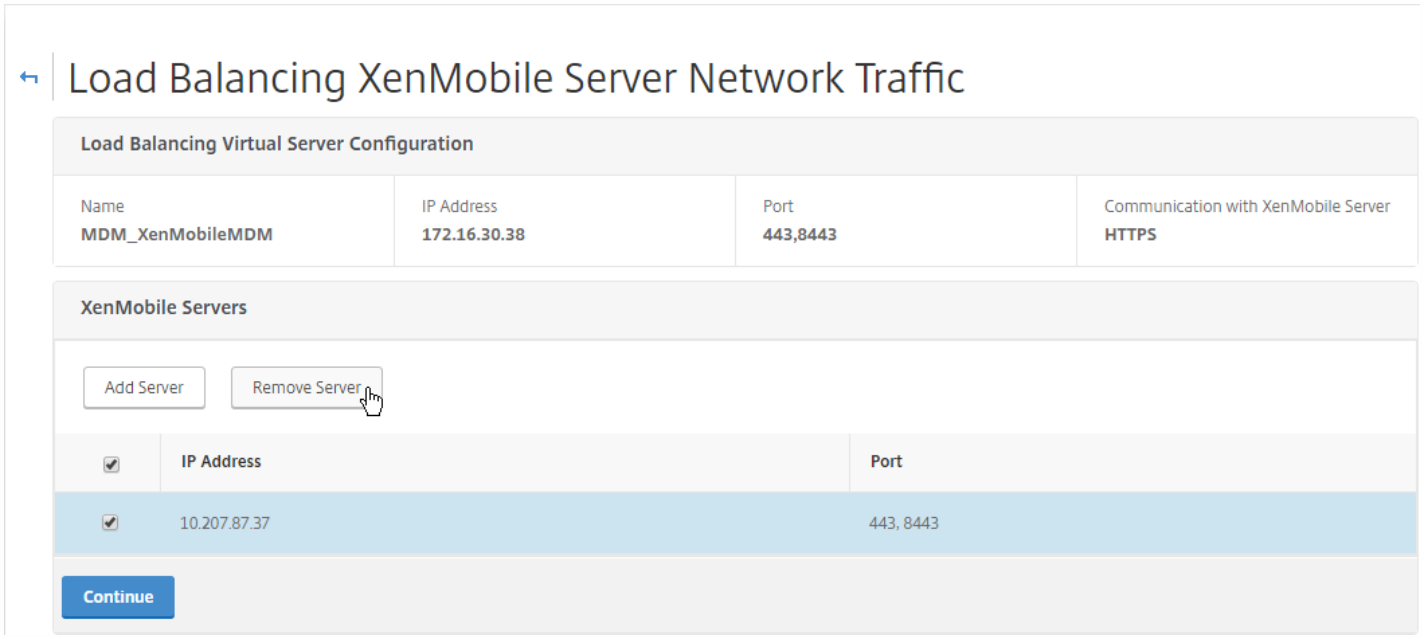
The **Load Balancing XenMobile Server Network Traffic** page appears.



3. Click the pen icon for XenMobile Servers to open those settings.



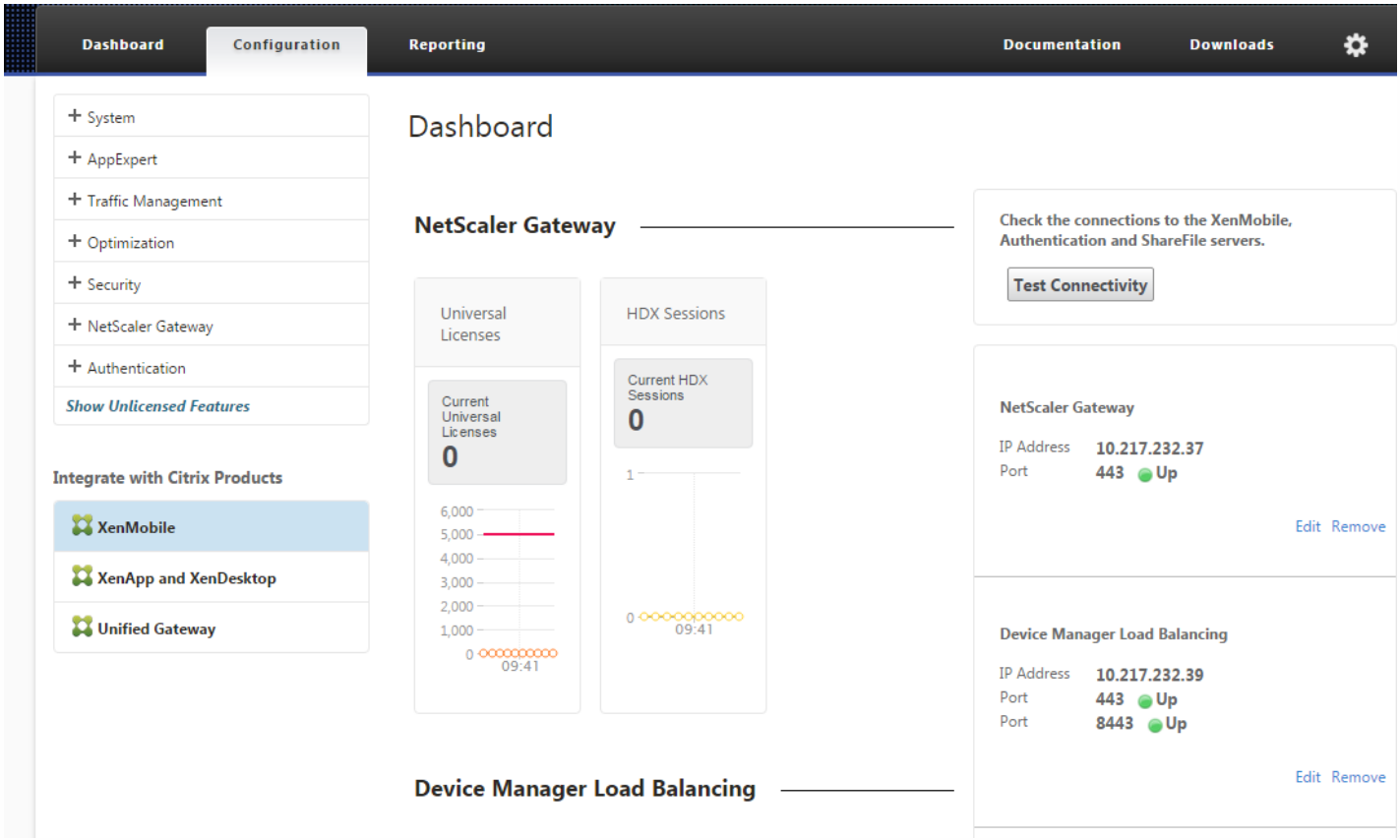
4. Select the 9.0 Device Manager server IP address and then click **Remove Server**.



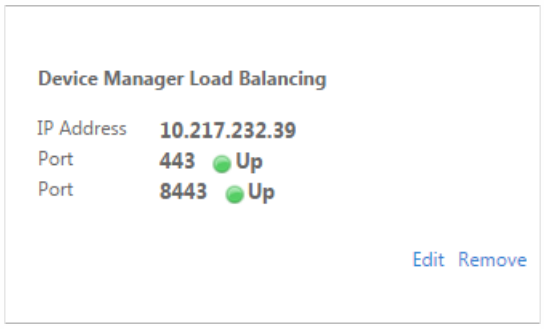
5. Click **Add Server** and then add the new XenMobile 10.4 server IP address.

For NetScaler versions 11.0 or 10.5

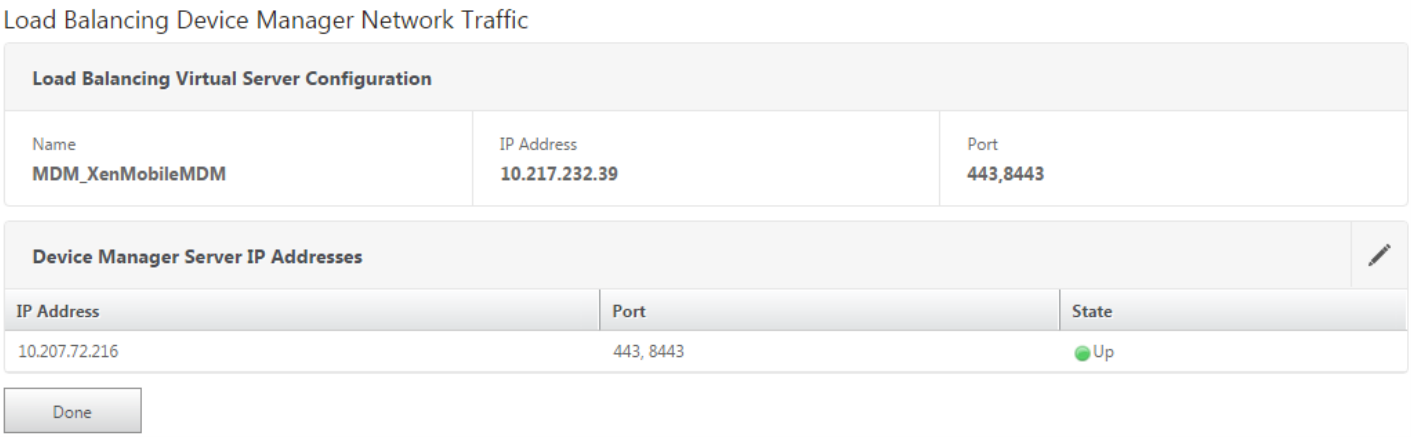
1. Under **Integrate with Citrix Products**, click **XenMobile**.



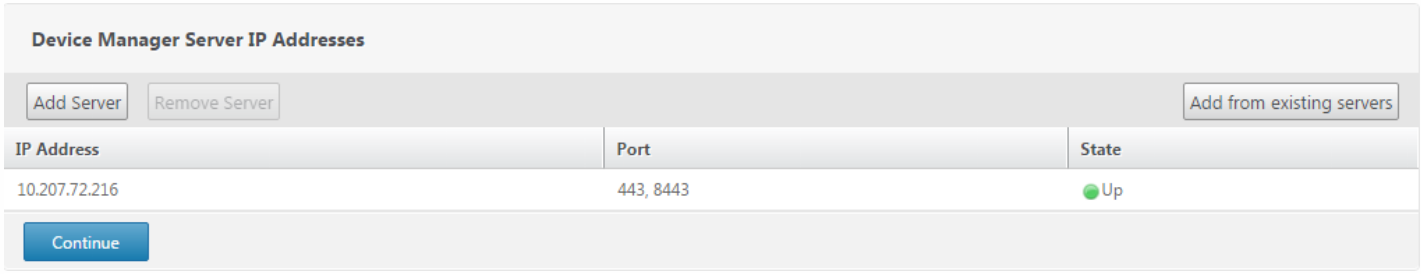
2. On the right side of the screen, under **Device Manager Load Balancing**, click **Edit**.



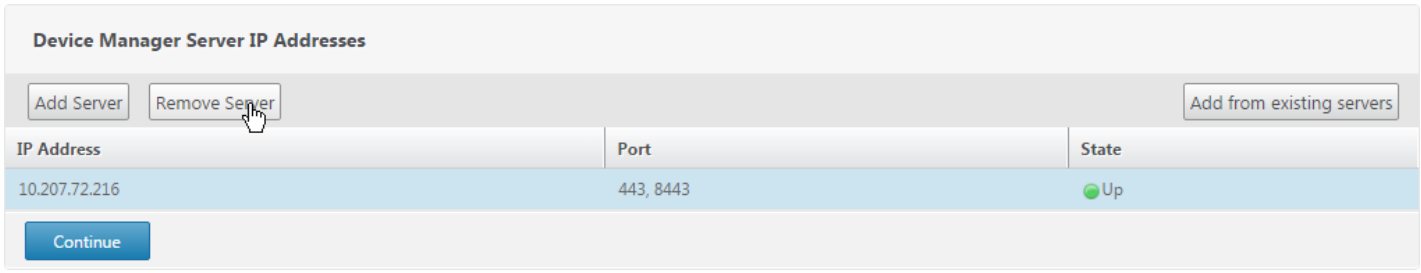
The **Load Balancing Device Manager Network Traffic** page appears.



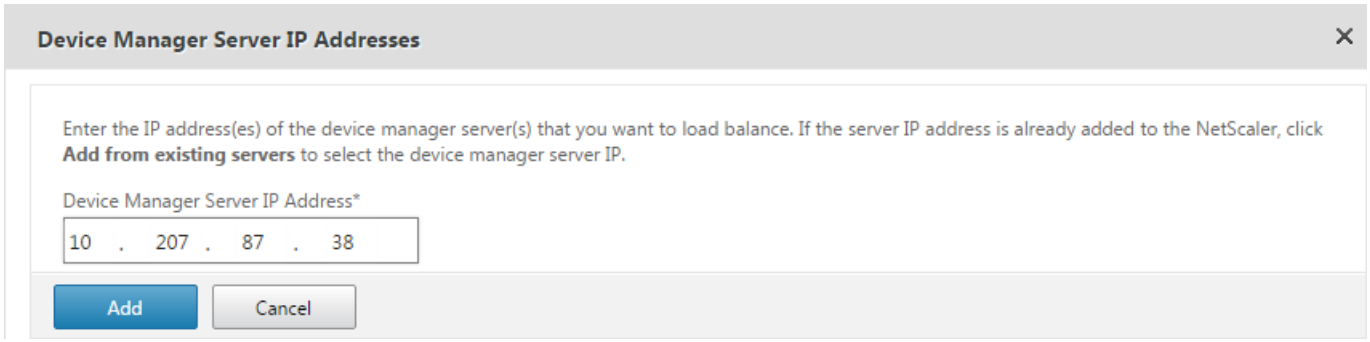
3. Click the pen icon for **Device Manager Server IP Addresses** to open those settings.



4. Select the 9.0 Device Manager server IP address and then click **Remove Server**.



5. Click **Add Server** and then add the new XenMobile 10.4 server IP address.



Change NetScaler Gateway to point to the new XenMobile server FQDN

At this point, NetScaler Gateway points to the App Controller FQDN. You must change NetScaler to point to the new XenMobile 10.4 FQDN. XenMobile 10.4 listens 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 10.4 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	XenMobile 10.4 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

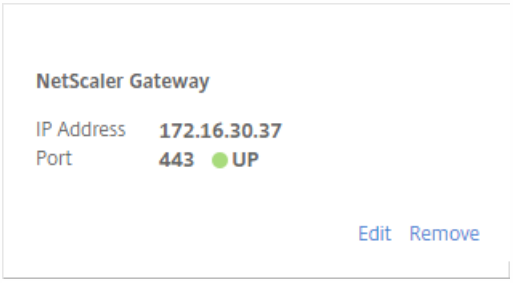
XenMobile App Edition

Change the App Controller FQDN to point to the new XenMobile 10.4 FQDN, which is the XenMobile 9.0 App Controller FQDN followed by port 8443. The following table shows an example.

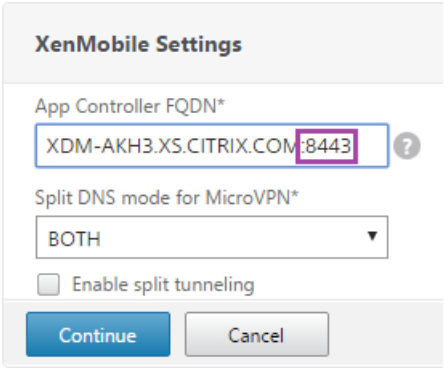
XenMobile 9.0 Component	Component FQDN	XenMobile 10.4 Enterprise Edition FQDN
App Controller	appc.example.net	appc.example.net:8443
NetScaler Gateway	access.example.com	N/A

1. Under **Integrate with Citrix Products**, click **XenMobile**.

2. Under **NetScaler Gateway**, click **Edit**.



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**.



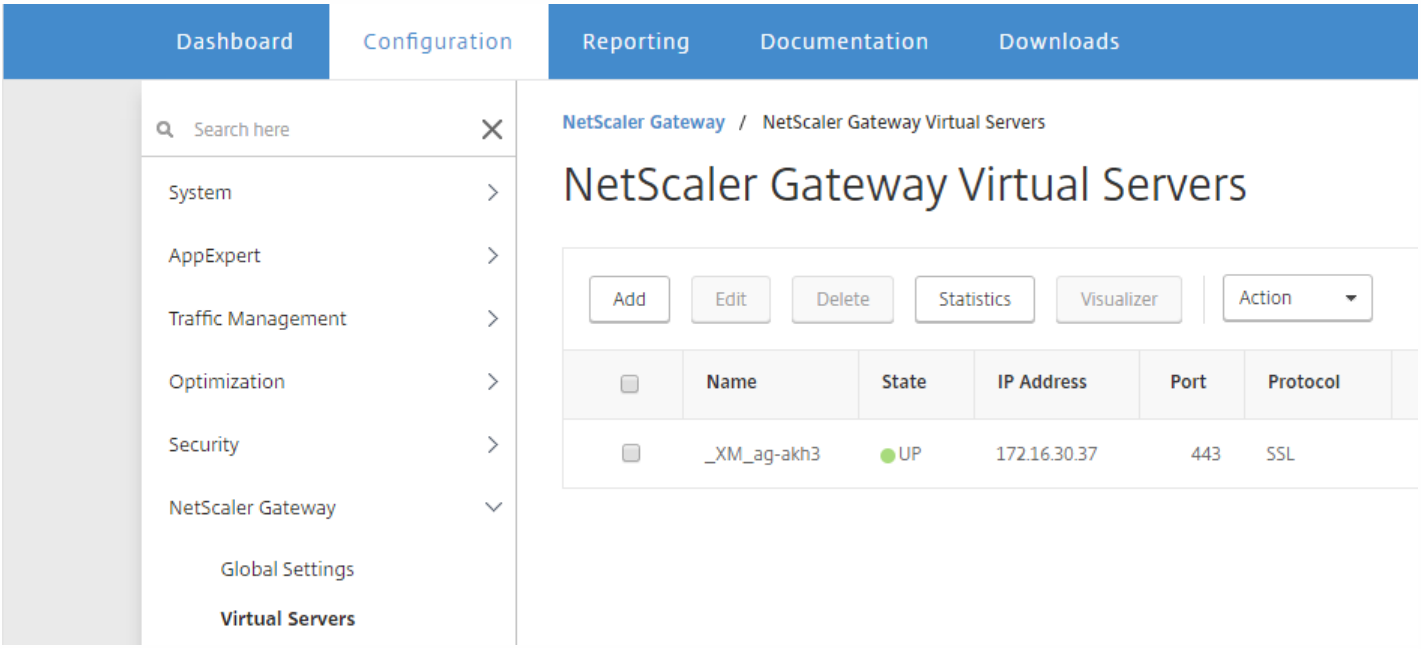
4. Click **Continue** and **Finish**.

Add the IP address or FQDN of the server running Secure Ticket Authority (STA)

Next, you must update your DNS to resolve the FQDN of the server running Secure Ticket Authority to the IP address of XenMobile Server 10.4. 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.

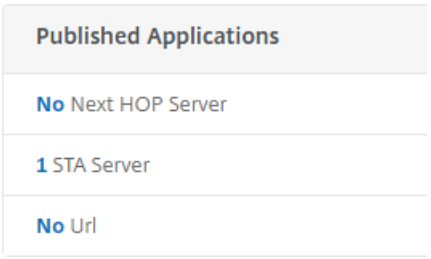
In NetScaler Gateway, you add the IP address or FQDN of the server running the Secure Ticket Authority, as follows:

1. Click **Netscaler Gateway > Virtual Servers**.

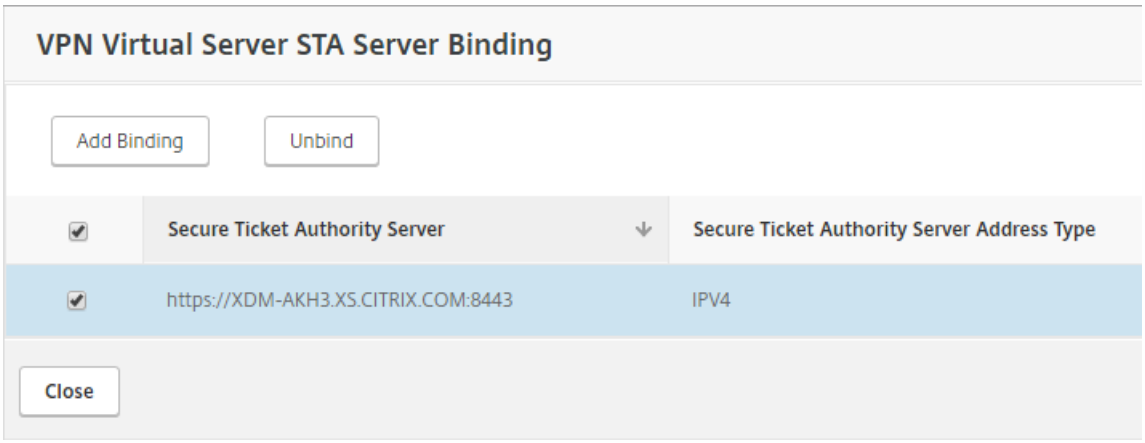


2. Make sure that the NetScaler Gateway virtual server is in the **Up** state. Select the configured Netscaler Gateway Virtual Server and then click **Edit**.

3. Under **Published Applications**, click **STA server**.



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.



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**.

NTP Settings

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.

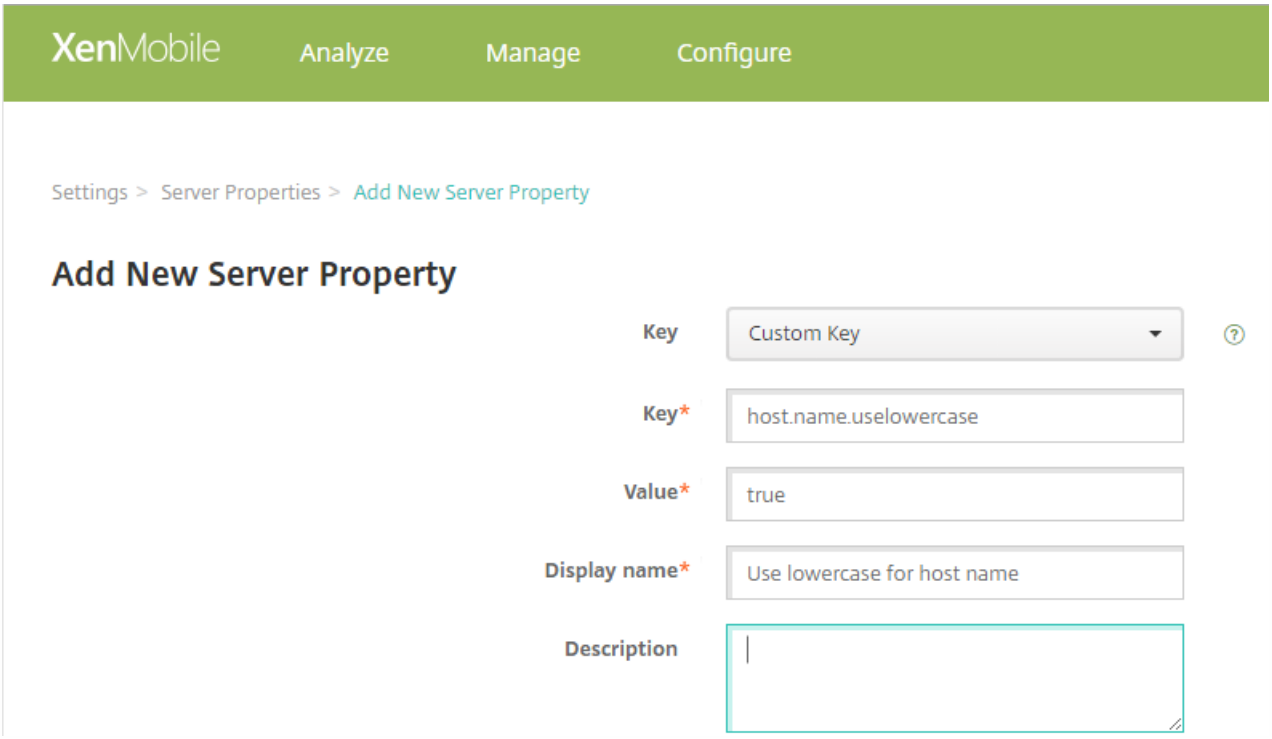
Server property if your XenMobile 9.0 host name has uppercase letters

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 XenMobile 10.4 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.



3. Restart the XenMobile server.

Update information that did not upgrade

Update the following as necessary:

- Managed Service Provider (MSP) group
- Custom Active Directory attributes
- RBAC roles
  For an on-premises ugprade, 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

Custom store name

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 XenMobile Server 10.4:

- 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.

XenMobile device enrollment after upgrade

Users do not need to re-enroll their devices after you do a production upgrade to XenMobile 10.4. The devices should connect automatically to the XenMobile 10.4 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.

Upgrade the MTC tenant server to XenMobile 10.4

Oct 05, 2016

If XenMobile 9.0 MDM or Enterprise Edition has Multi-Tenant Console (MTC) enabled, you can migrate MTC-managed XenMobile 9 instances to standalone XenMobile 10.4 instances. XenMobile 10 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 XenMobile 10.4.

3. If no port mapping is enabled on the MTC tenant, do the following:

    a. Make sure the XenMobile 10.4 server port that allows HTTPS communication with certificates (normally, 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. When 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.p1"

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 XenMobile 10.4 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

Feb 23, 2017

In XenMobile, you configure user accounts and groups and roles for user accounts and groups. You also configure enrollment mode and invitations. You configure these settings in the XenMobile console, on the **Manage** tab and the **Settings** page.

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. Each mode has its own level of security and number of steps users must take to enroll their devices, and to send enrollment invitations. For details, see:
  - To configure enrollment modes and enable the Self Help Portal
  - Enable autodiscovery in XenMobile for user enrollment

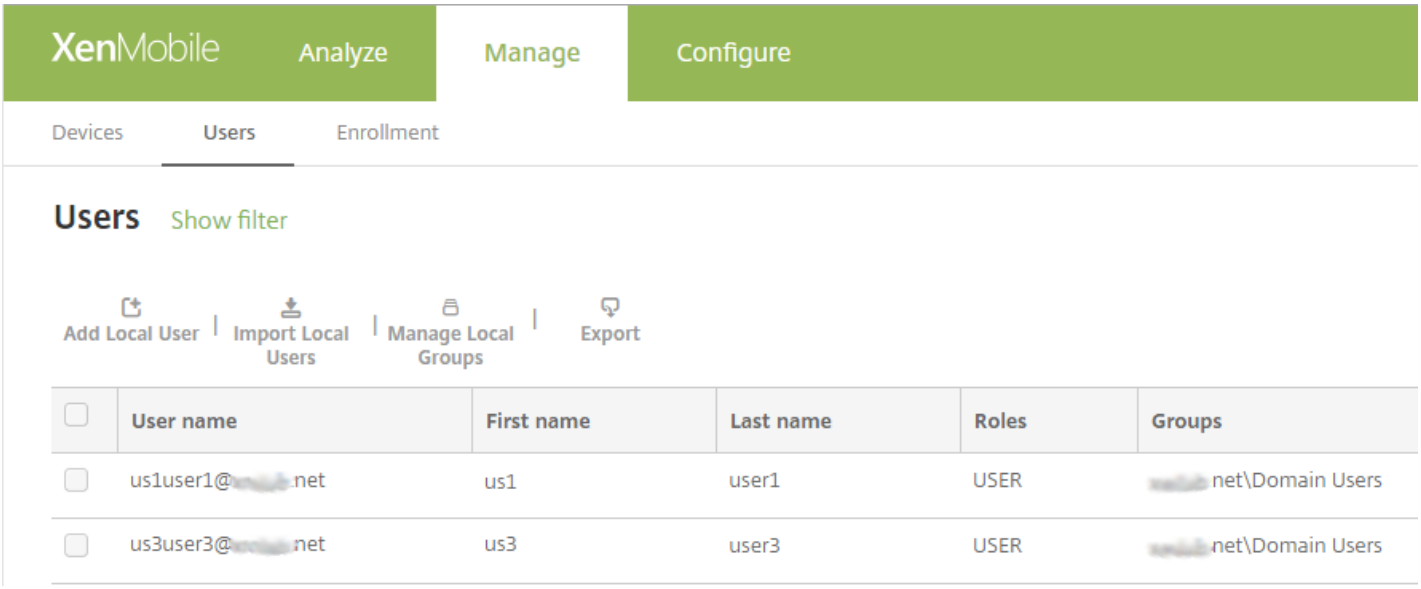
From the **Settings** page, you can do the following:

- 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

To add, edit, or delete local user accounts

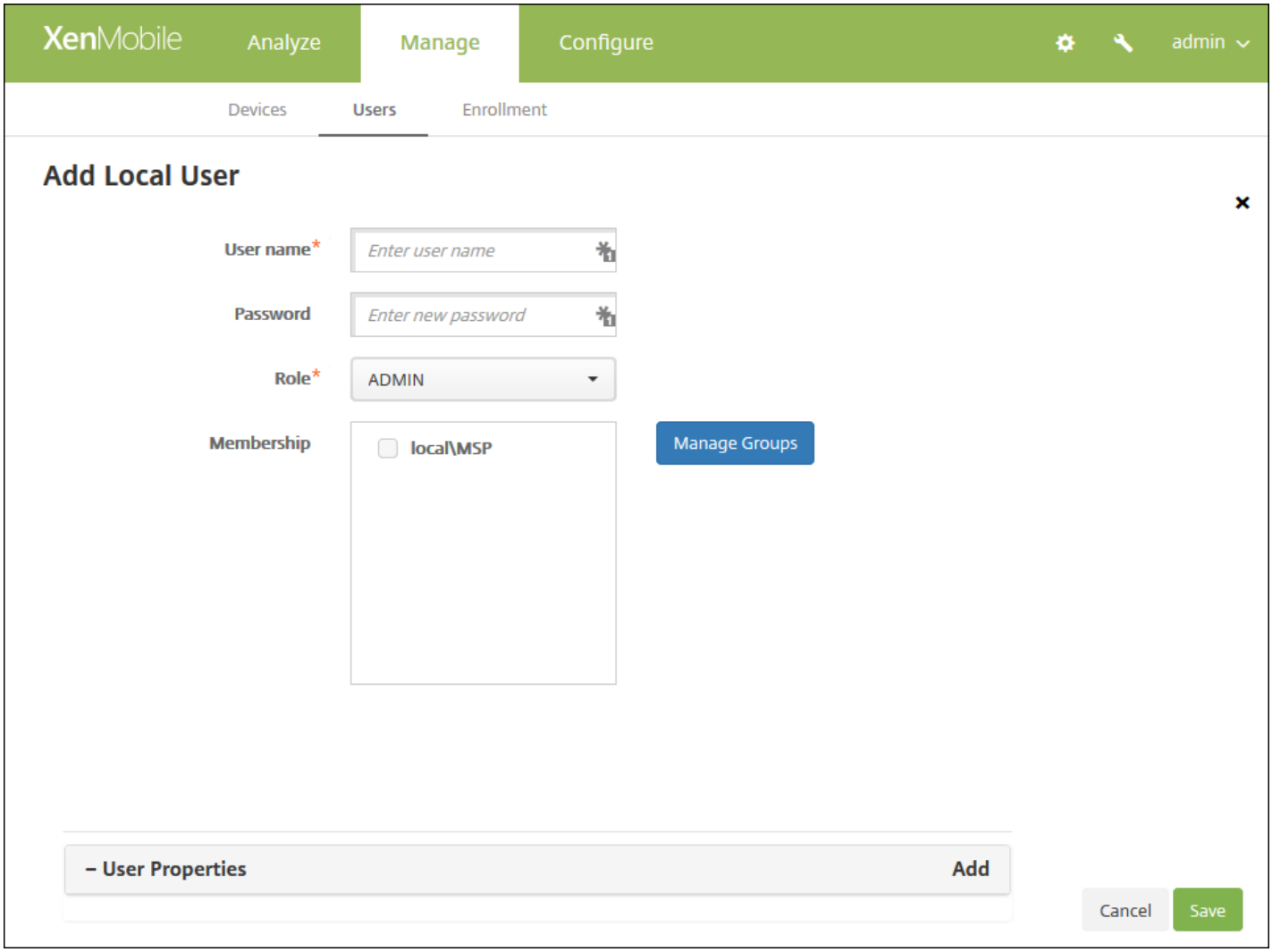
You can add local user accounts to XenMobile manually or you can use a provisioning file to import the accounts. For the steps to import user accounts from a provisioning file, see To import user accounts by using a .csv provisioning file.

1. In the XenMobile console, click **Manage** > **Users**. The **Users** page appears.



To add a local user account

1. On the **Users** page, click **Add Local User**. The **Add Local User** page appears.

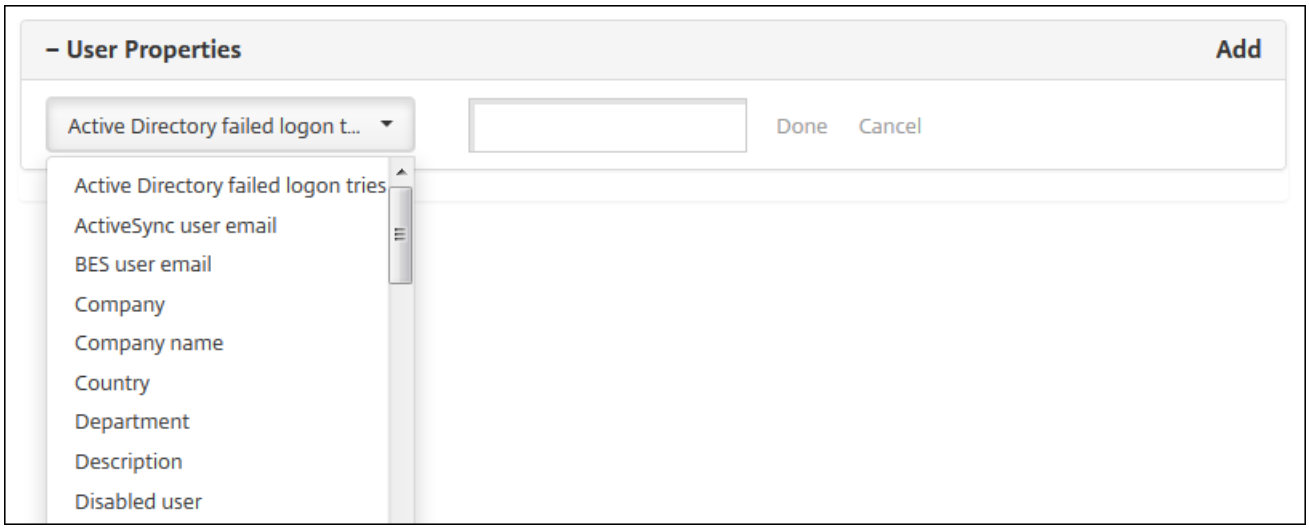


2. Configure these settings:

- **User name**: Type the user name. This field is required. You can include spaces in names, in addition to 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** not to save the user property.

Note: To delete an existing user property, hover over the line containing the property and then click the X on the right-hand side. The property is deleted immediately.

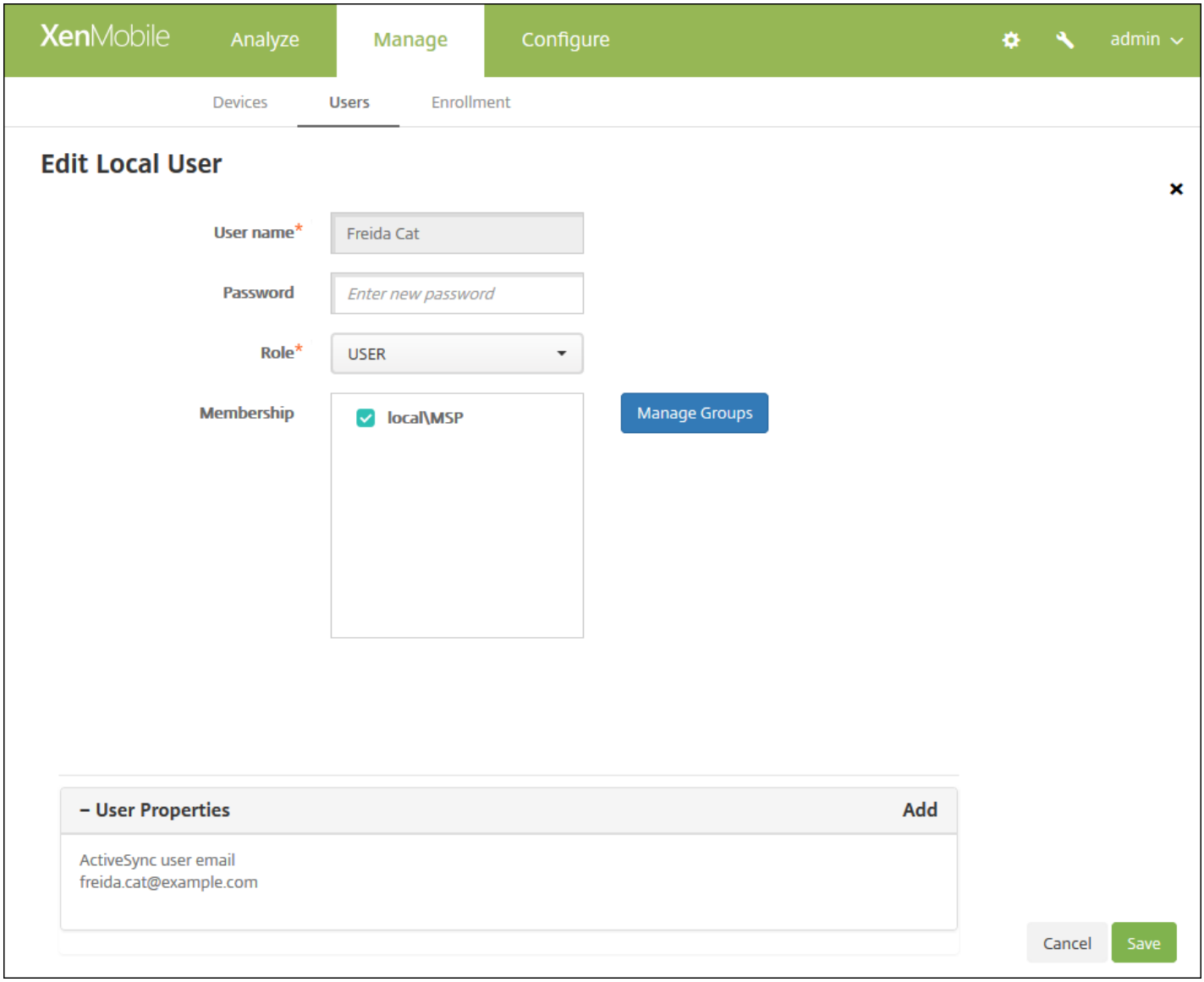
To edit an existing user property, click the property and make changes. Click **Done** to save the changed listing or **Cancel** to leave the listing unchanged.



3. Click **Save**.

To edit a local user account

1. On the **Users** page, in the list of users, click to select a user and then click **Edit**. The **Edit Local User** page appears.



2. Change the following information as appropriate:

- **User name**: You cannot change the user name.
- **Password**: Change or add a user password.
- **Role**: In the list, click the user role.
- **Membership**: In the list, click the group or groups to which to add or edit the user account. To remove the user account from a group, clear the check box next to the group name.
- **User properties**: Do one of the following:
  - For each user property you want to change, click the property and make changes. Click **Done** to save the changed listing or **Cancel** to leave the listing unchanged.
  - For each user property you want to add, click **Add** and do the following:
    - **User Properties**: In the list, click a property and then type the user property attribute in the field next to the property.
    - Click **Done** to save the user property or click **Cancel** not to save the user property.
  - For each existing user property you want to delete, hover over the line containing the property and then click the X on the right-hand 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** not to delete the user account.

Importing user accounts

You can import local user accounts and properties from a .csv file called a provisioning file, which you can create manually. For more information about formatting provisioning files, see Provisioning file formats.

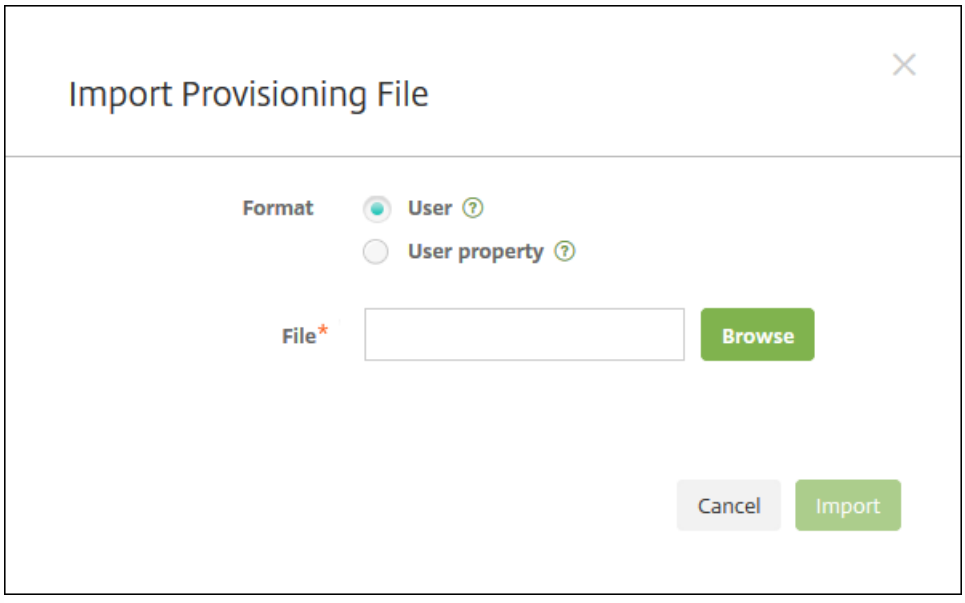
Note:

- For local users, use the domain name along with the user name in the import file. For example, specify username@domain. When the local user that you create or import in this format is for a managed domain in XenMobile, keep the following in mind. The user cannot enroll by using the corresponding LDAP credentials.
- When 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. Therefore, you should reenable the default domain after the import of internal users is complete.
- Local users can be in User Principal Name (UPN) format, but we recommend that you do not use the managed domain. For example, when 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.



3. Select **User** or **Property** for the format of the provisioning file you are importing.

4. Select the provisioning file to use by clicking **Browse** and then navigating to the file location.

5. Click **Import**.

Provisioning file formats

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:

- The fields within the provisioning file are separated by a semi-colon (;). When part of a field contains a semi-colon, it must be escaped by using a backslash character (\). For example, the property propertyV;test;1;2would be typed as propertyV\;test\;1\;2 in the provisioning file.
- Valid values for **Role** are the predefined roles USER, ADMIN, SUPPORT, and DEVICE_PROVISIONING, plus other roles that you have defined.
- The period character (.) is used as a separator to create group hierarchy; therefore, you cannot use a period in group names.
- Property attributes in attribute provisioning files must be lowercase. 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

In 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

To configure enrollment modes and enable the Self Help Portal

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. The Self Help Portal is where users can log on 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** page. For information, see Send an enrollment invitation.

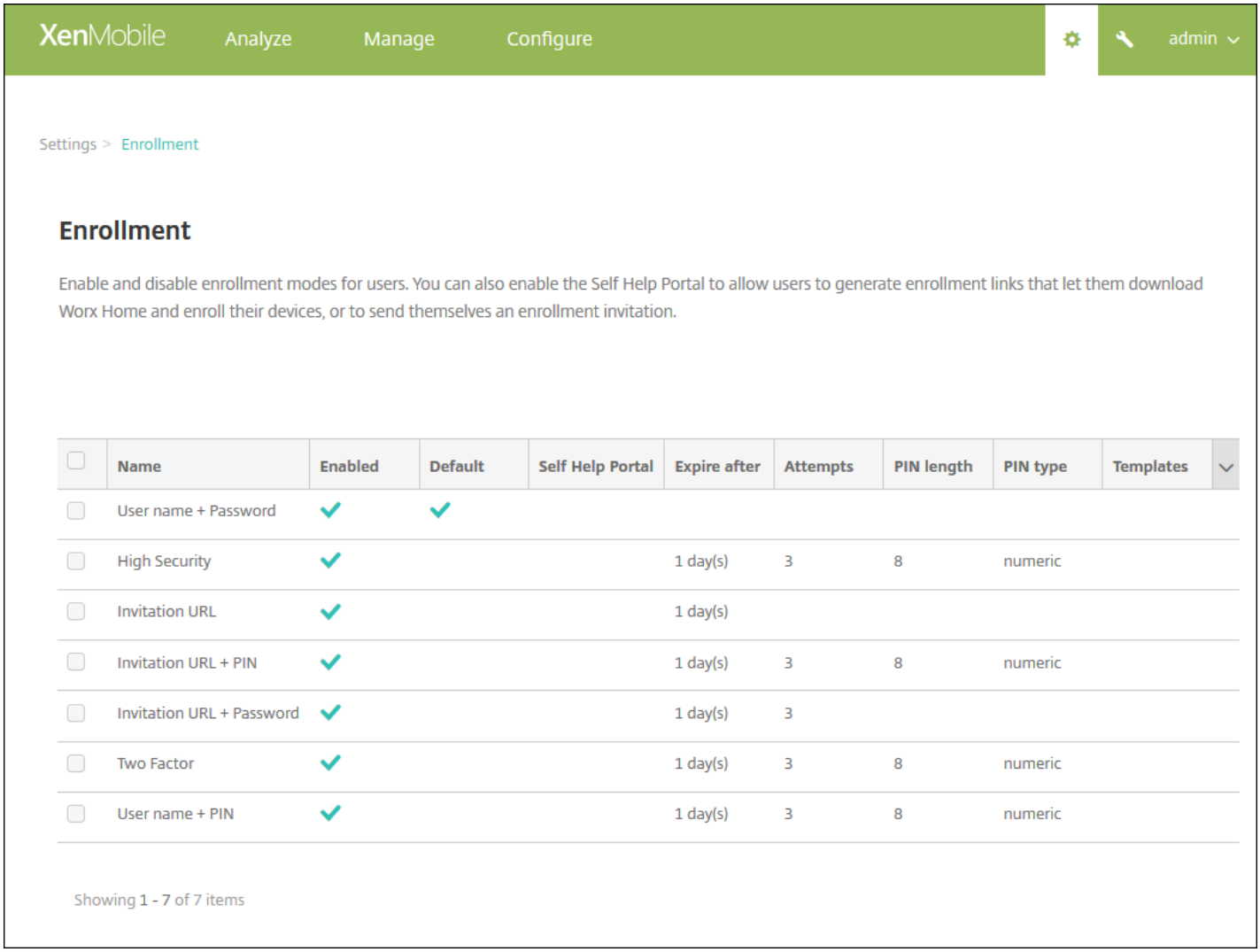
Note: If you plan to use custom notification templates, you must set up the templates before you configure enrollment modes. For more information about notification templates, see Creating or Updating Notification Templates.

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.

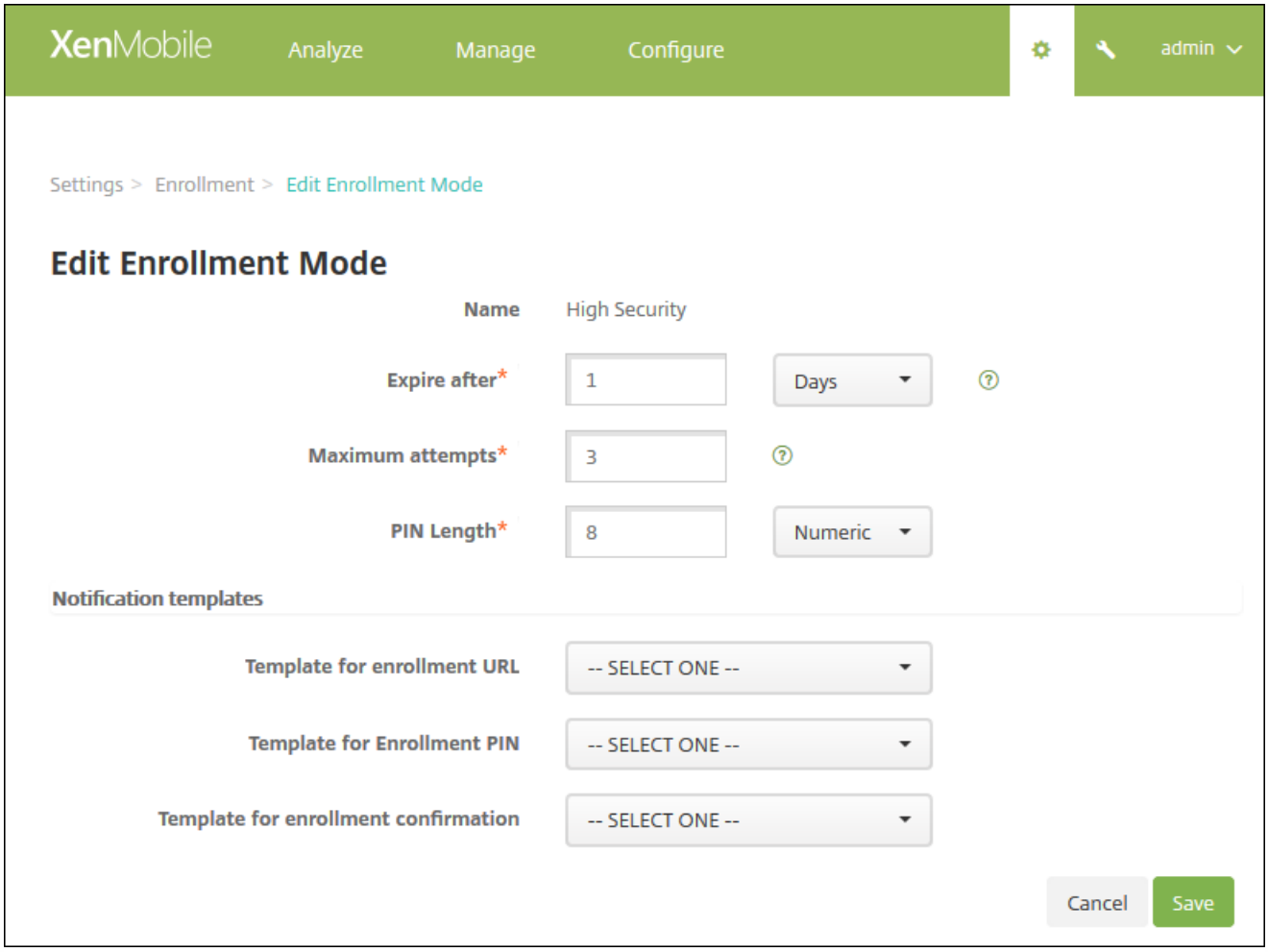
3. Select any enrollment mode in the list to edit and then set the mode as the default, disable the mode, or allow users access through the Self Help Portal.

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.



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.



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 for how many digits/characters the generated PIN contains.
- **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 depending 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: You can only set **Only Username + Password**, **Two Factor**, or **Username + PIN** as the default enrollment mode.

1. Select one of **Username + Password**, **Two Factor**, or **Username + PIN** to set as the default enrollment mode.

Note: The selected mode must be enabled to be set as the default.

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 no the Self Help Portal is no longer available to users.

Adding or removing groups

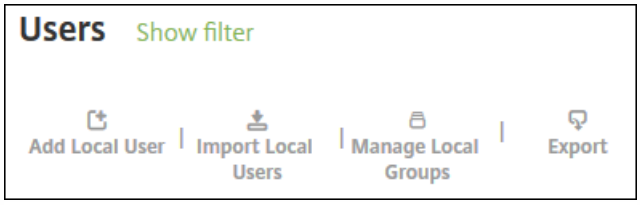
You manage groups in the **Manage Groups** dialog box in the XenMobile console, which you can find on the **Users** page, the **Add Local User** page, or the **Edit Local User** page. There is no group edit command.

If you remove a group, keep in mind that removing the group has no effect on user accounts. Removing a group simply removes the association of the user 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.

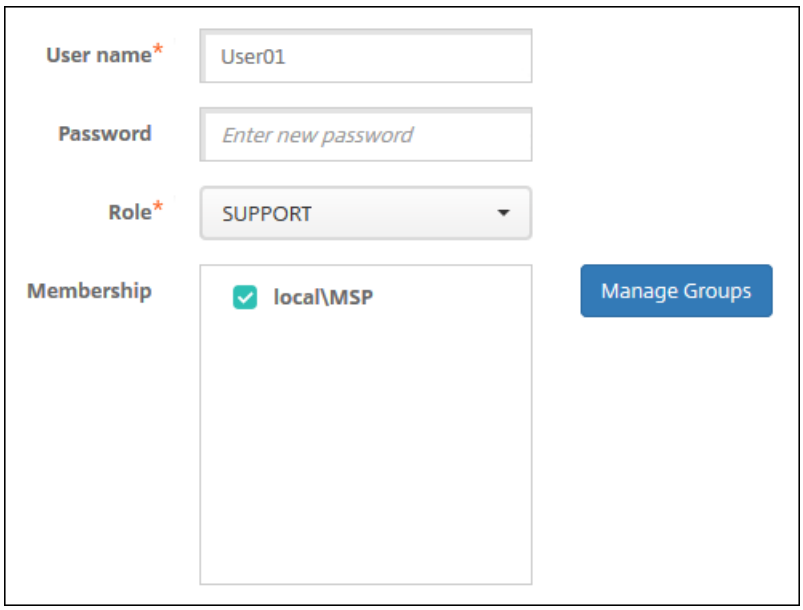
To add a local group

1. Do one of the following:

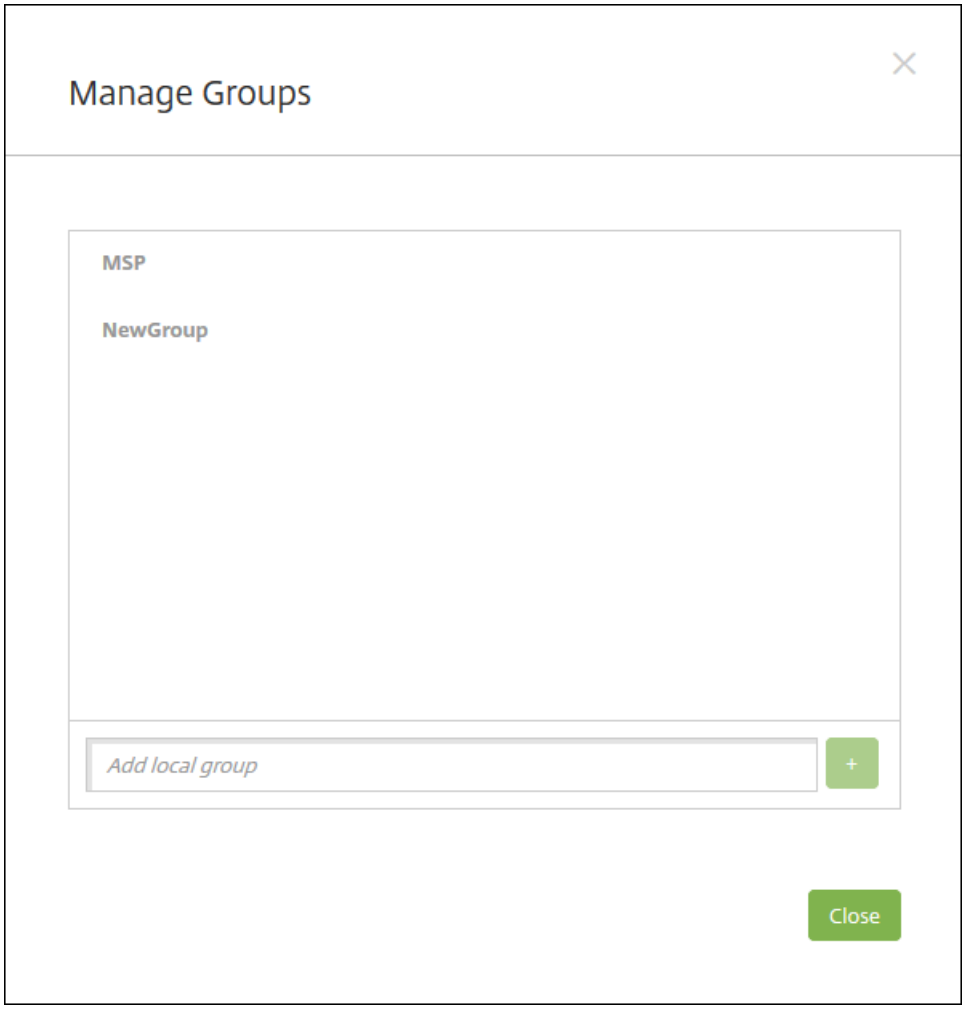
- On the **Users** page, click **Manage Local Groups**.



- On either the **Add Local User** page or the **Edit Local User** page, click **Manage Groups**.



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**.

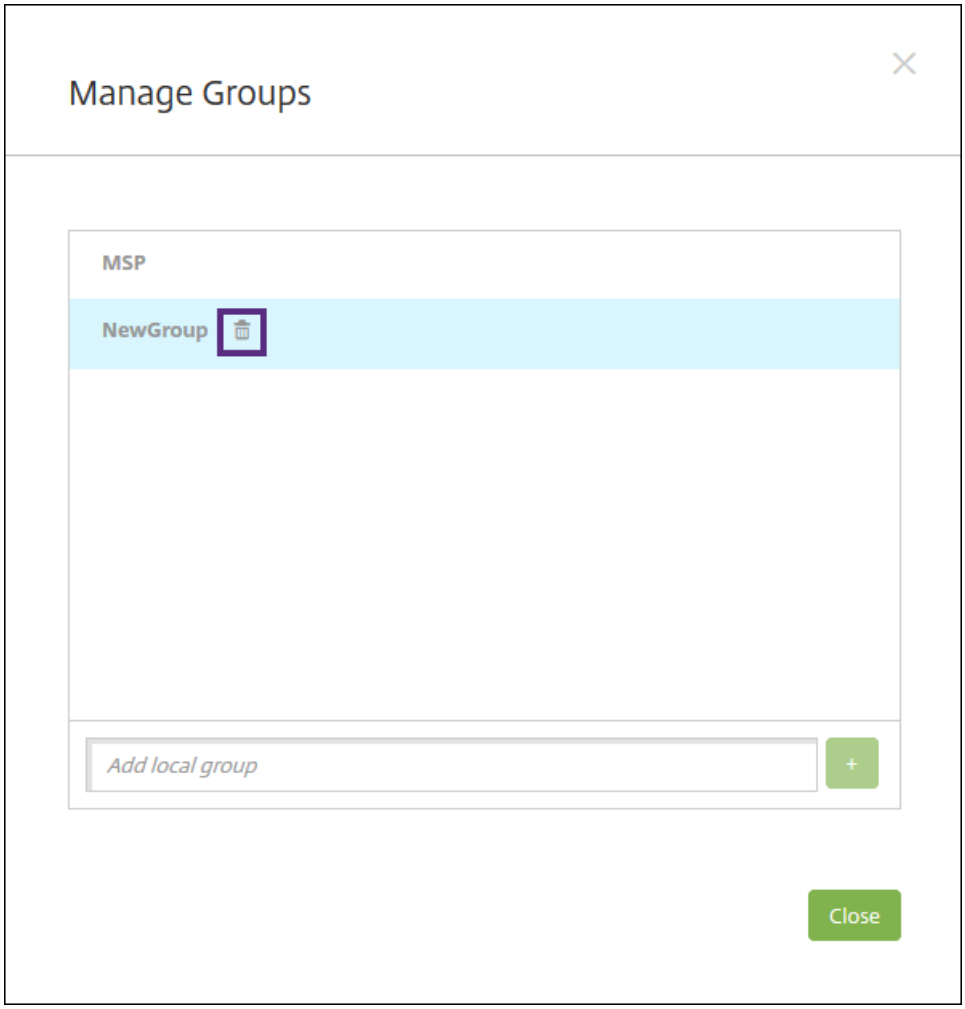
To remove a group

Note: Removing a group has no effect on user accounts. Removing a group simply removes the association of the user 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**.

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. 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 user their name or email address to search for and select the approvers. When XenMobile finds the person, you then add the person 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.

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 the required name of the 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, in the list of existing workflows, select a specific workflow. To do so, 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

Jan 10, 2017

Each predefined role-based access control (RBAC) role has certain access and feature permissions associated with the role. 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.

- Admin Role
- Device Provisioning Role
- Support Role
- User 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.

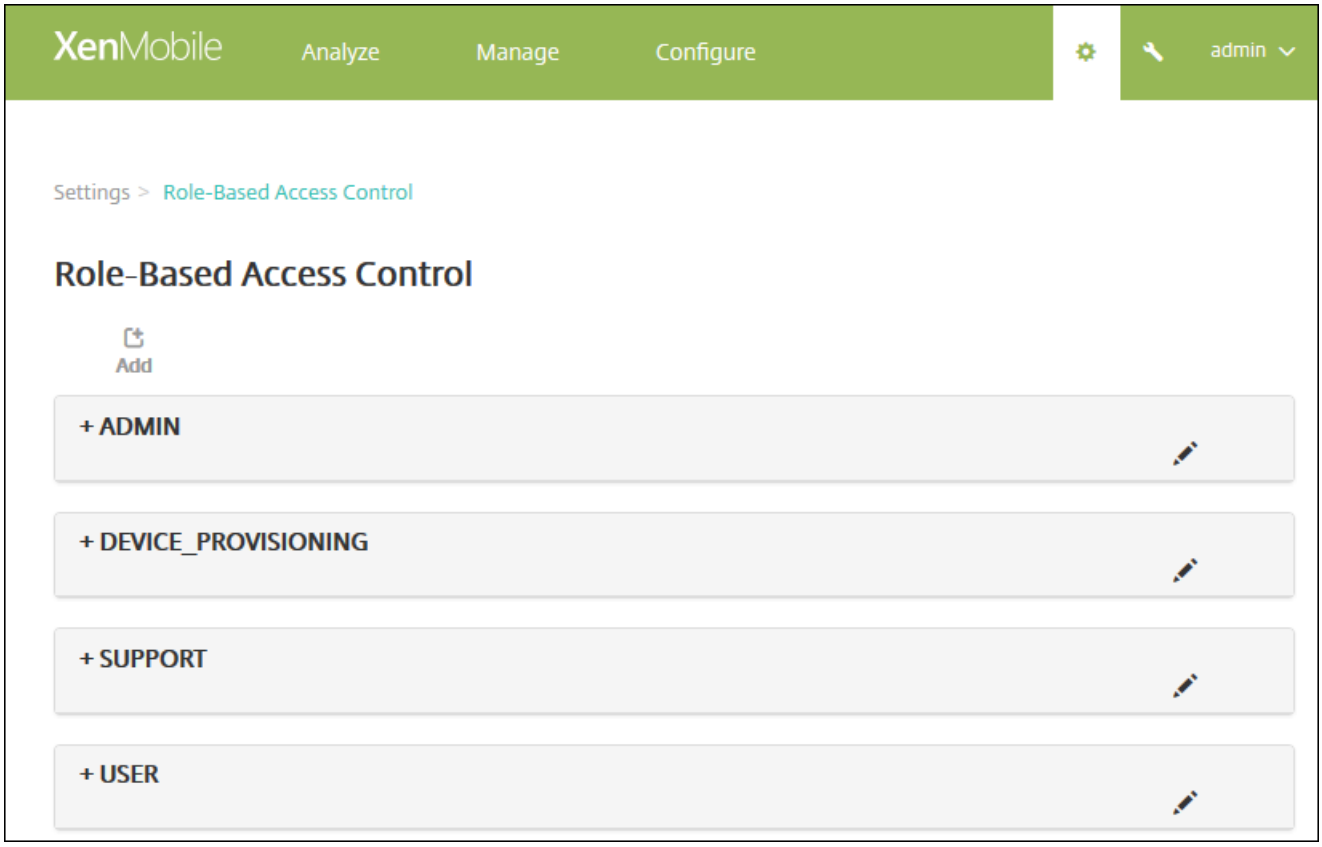
You can use the RBAC feature in XenMobile to do the following:

- 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.

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.

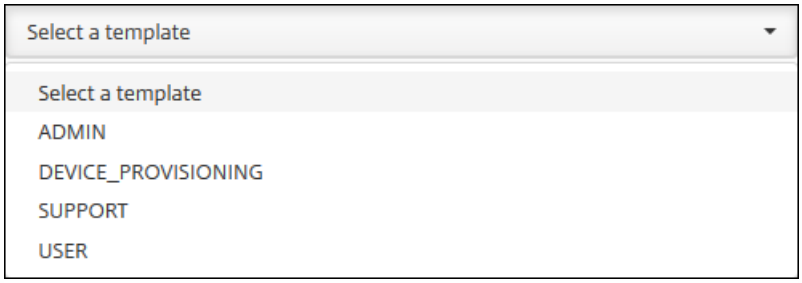
- When you click **Add** or the pen icon, the **Add Role** or the **Edit Role** page appears.

- When you click the trash can icon, a confirmation dialog appears. Click **Delete** to remove the selected role.

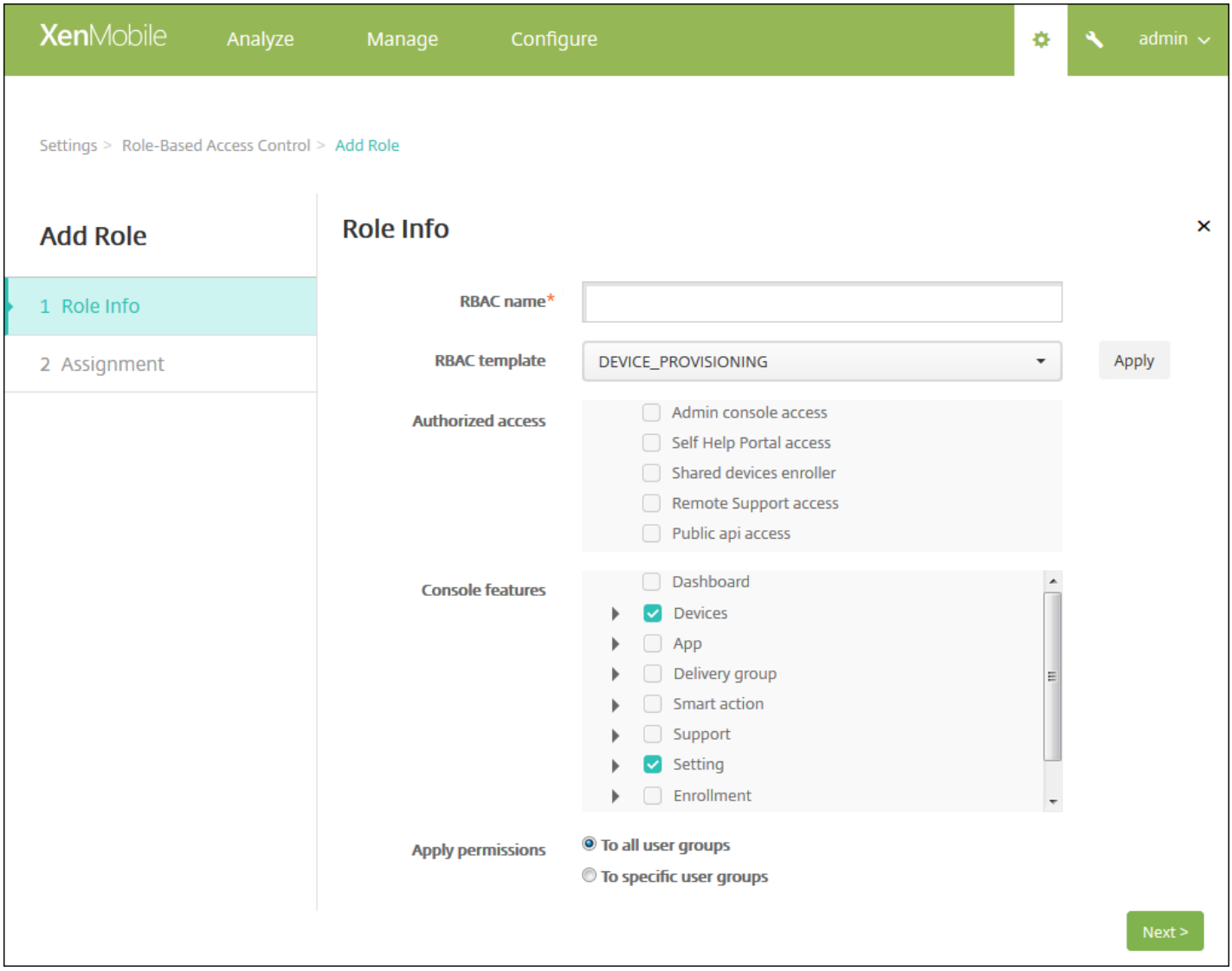
4. Enter the following information to create a new user role or to edit an existing user role:

- **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.

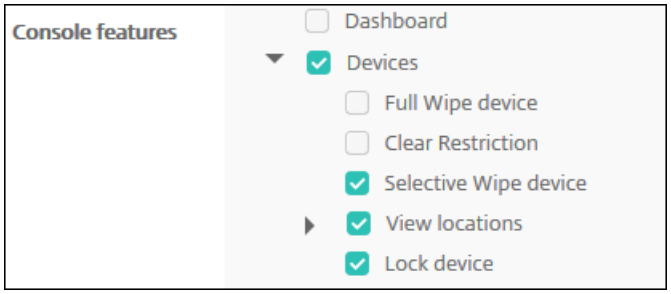


5. Click **Apply** to the right of the **RBAC template** field to populate the **Authorized access** and **Console features** check boxes with the pre-defined access and feature permissions for the selected template.

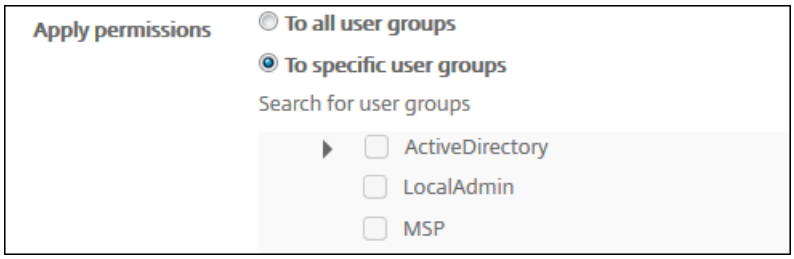


6. Select and clear the check boxes in **Authorized access** and **Console features** to customize the role.

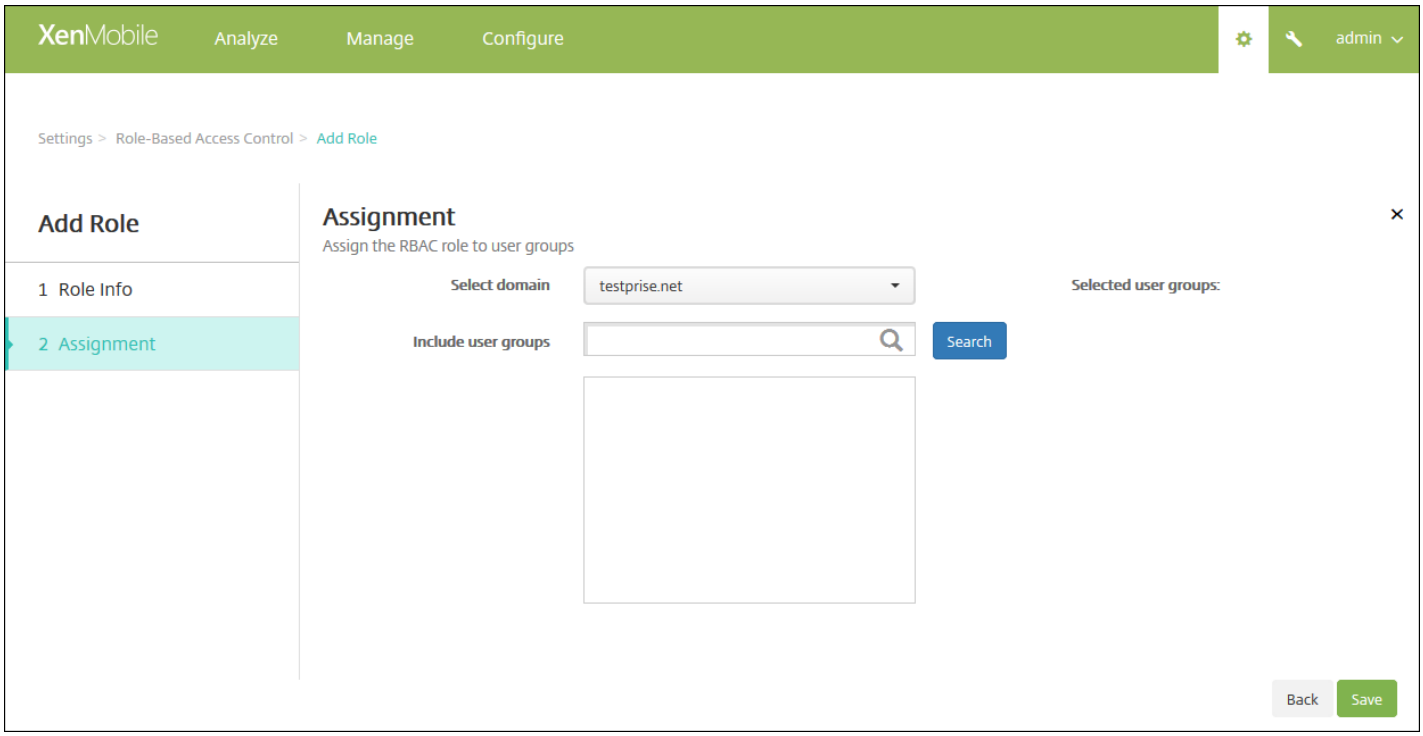
If you click the triangle next to a Console feature, permissions specific to that feature appear that you can select and clear. Clicking the top-level check box prohibits access to that console part; you must select individual options below the top level to enable those options. For example, in the following 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.



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.

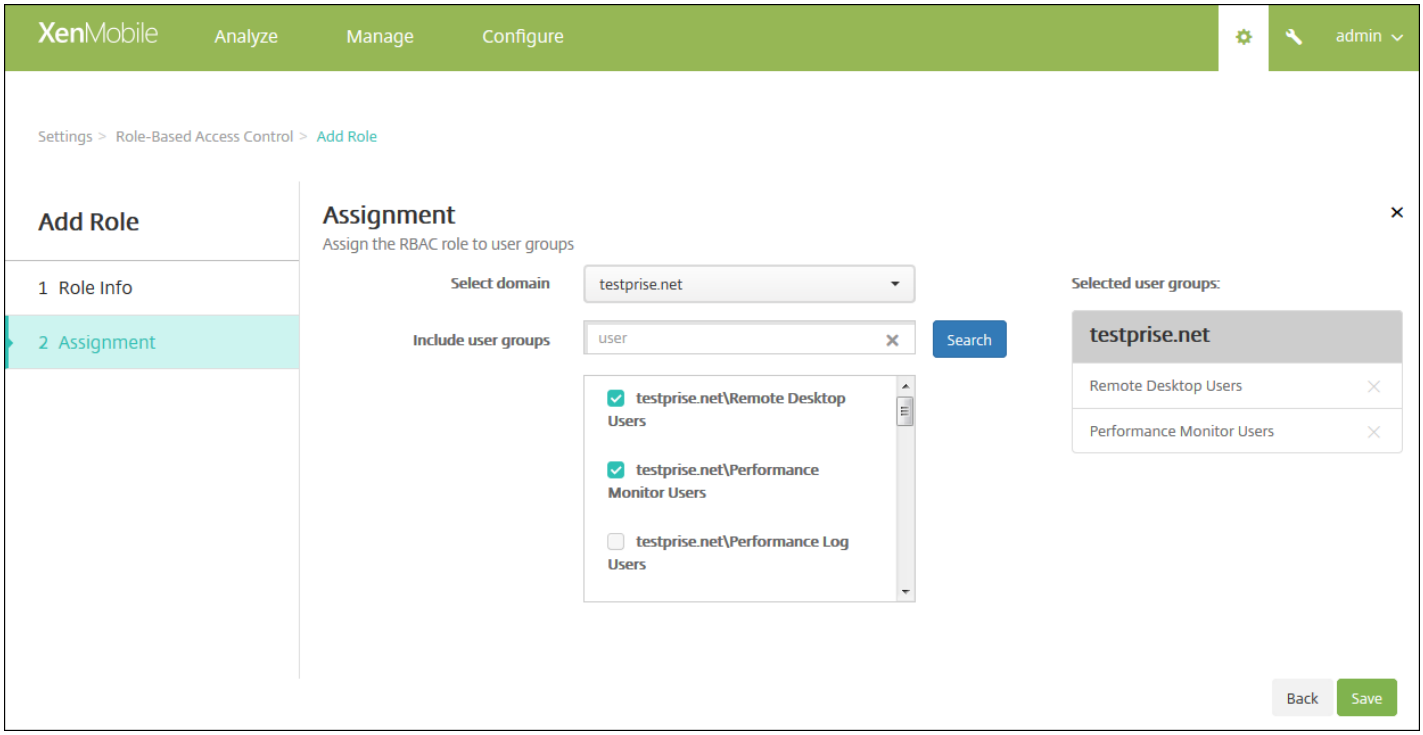


8. Click **Next**. The **Assignment** page appears.



9. Enter the following information to assign the role to user groups.

- **Select domain**: In the list, click a domain.
- **Include user groups**: Click Search to see a list of all available groups, or type a full or partial group name to limit the list to only groups with that name.
- In the list that appears, select the user groups to which you want to assign the role. When you select a user group, the group appears in the **Selected user groups** list.



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

Jan 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, such as when a user's device is about to be blocked from the corporate domain because of a compliance issue, or 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 carrier's SMS gateway. 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.

The procedures in this article explain how to configure an SMTP server and an SMS gateway, and a carrier SMS gateway.

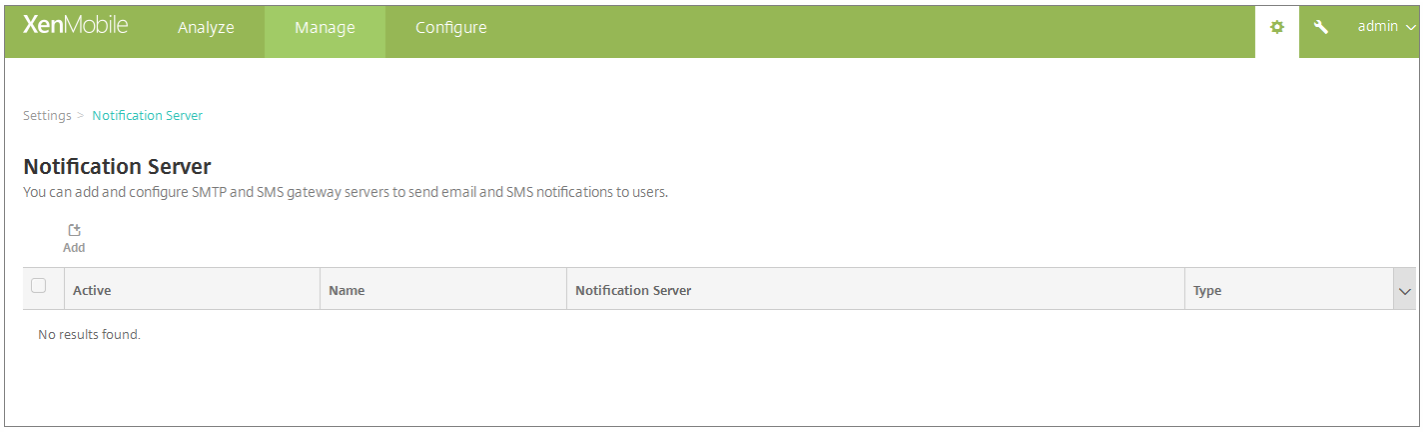
Prerequisites

- 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 which case you will need information from the service provider's web site.
- You must 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 service provider's website.
- Only one SMTP server and only one SMS server is active at a time.
- Port 25 must be opened from XenMobile located in your network's DMZ to point back to the SMTP server on your internal network in order for notifications to be sent successfully.

To 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.

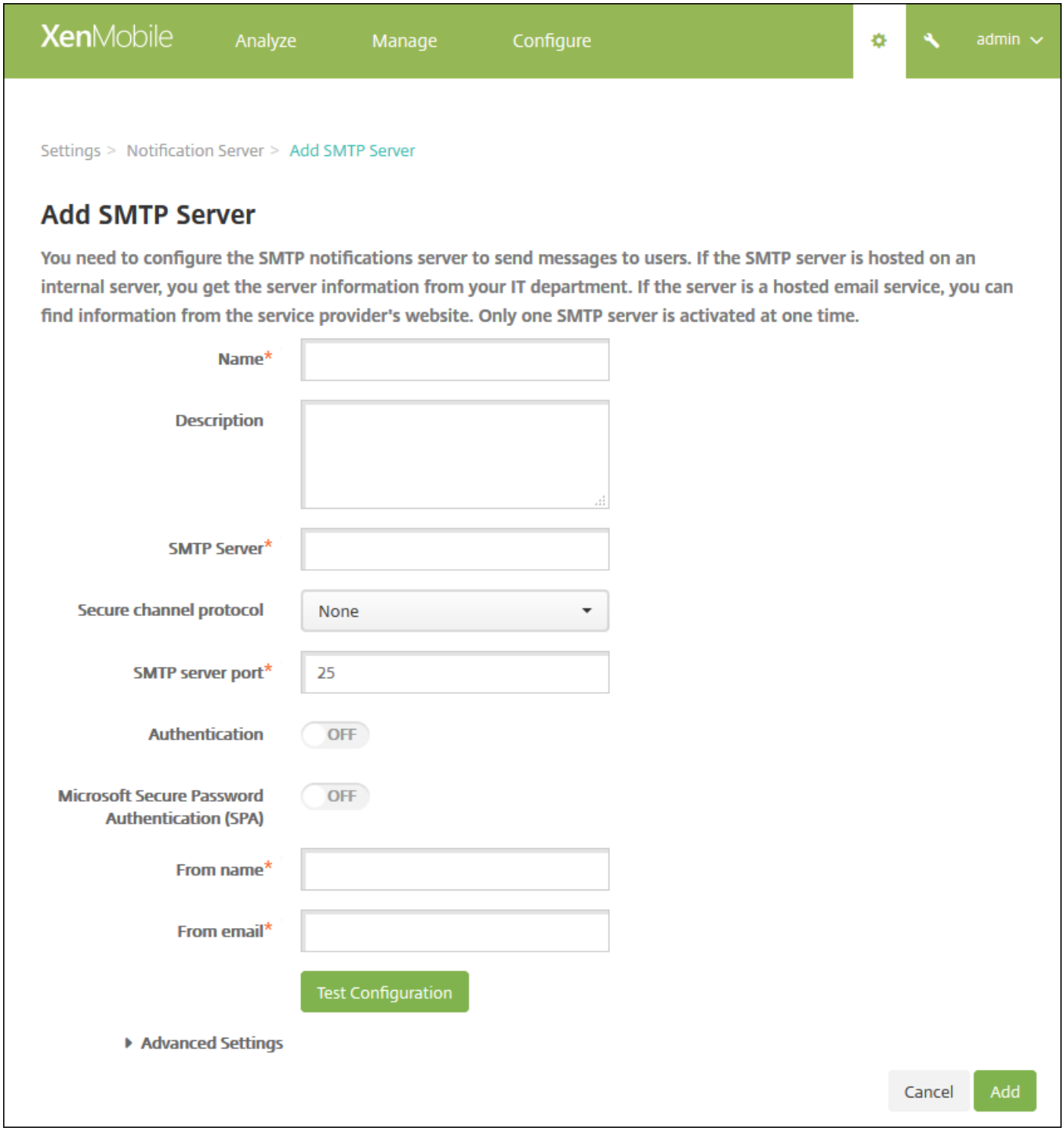
2. Under **Notifications**, click **Notification Server**. The **Notification Server** page appears.



2. Click **Add**. A menu appears with options to configure an SMTP server or an SMS gateway.

- 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.

To add an SMTP server



1. Configure these settings:

- **Name**: Type the name associated with this SMTP server account.
- **Description**: Optionally, enter a description of the server.
- **SMTP Server**: Type the host name for the server. 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.

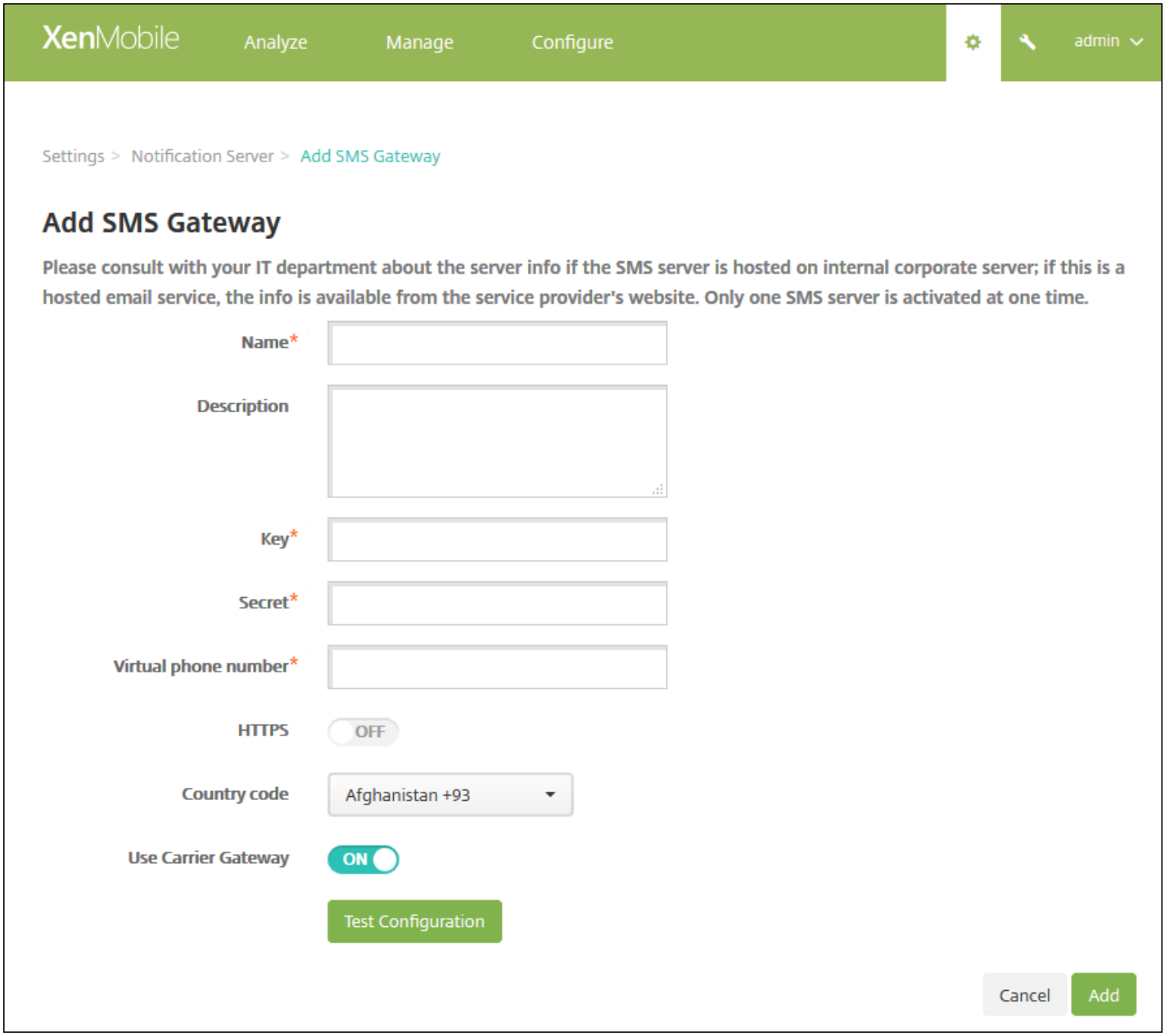
2. Click **Test Configuration** to send a test email notification.

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**.

To add an SMS gateway



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.

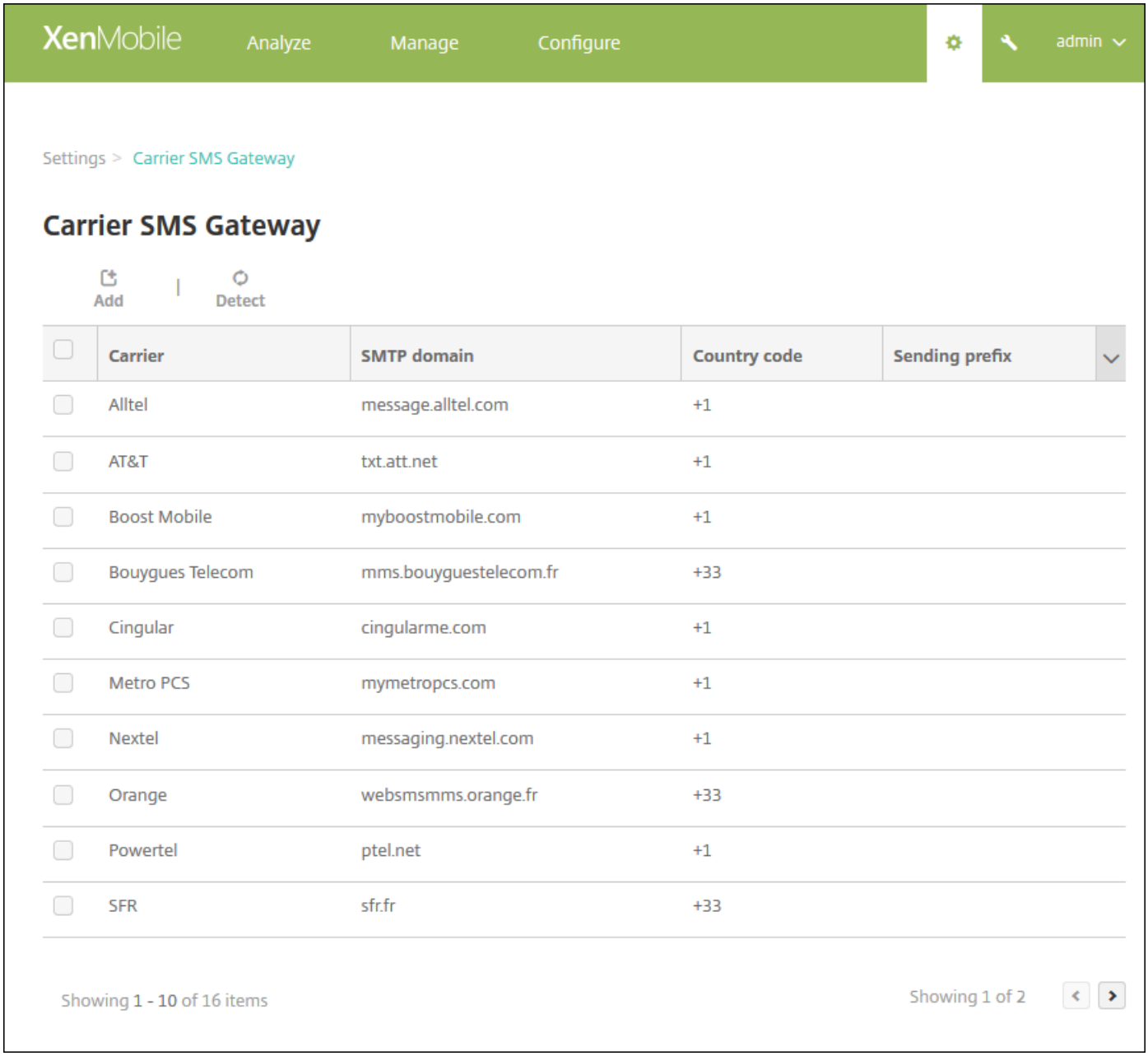
2. Click **Add**.

To 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.

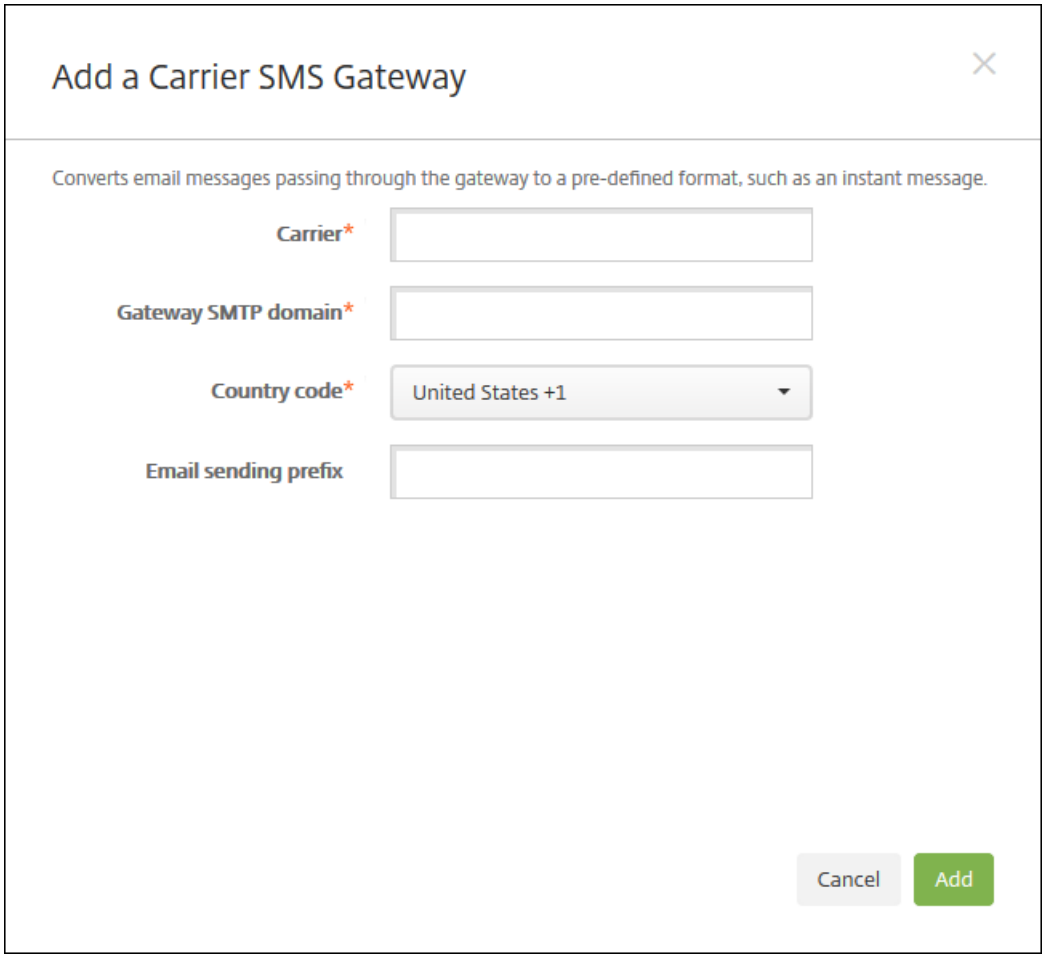
1. In the XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.

2. Under **Notifications**, click **Carrier SMS Gateway**. The **Carrier SMS Gateway** page opens.



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.



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.

Creating and updating 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.

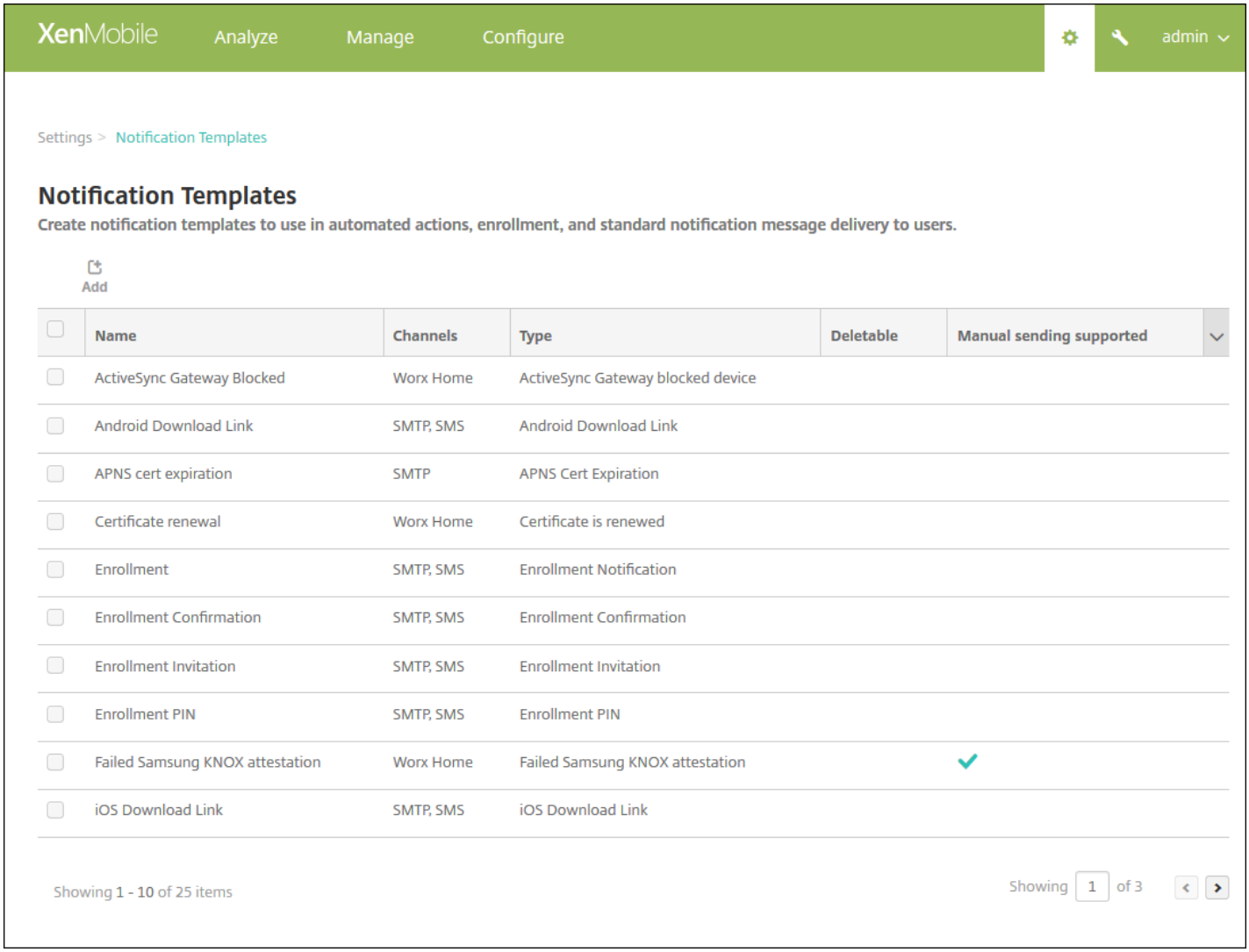
XenMobile includes many predefined notification templates that reflect the distinct types of events that XenMobile automatically responds to for every device in the system.

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.



To 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.
- **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.

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.

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.

To 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**.

To 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 in XenMobile 10.4

Mar 29, 2017

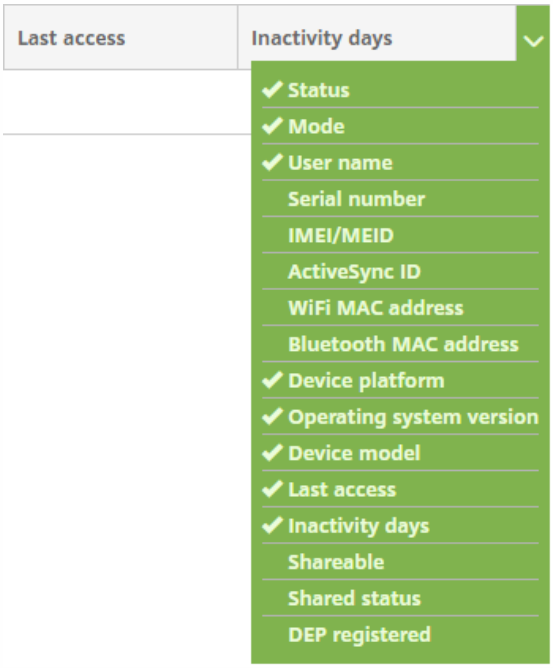
For information on devices in the most recent version of XenMobile Server, see Devices.

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 are the default headings shown.

To customize the **Devices** table, click the down arrow on the last heading and then select the additional headings you want to see in the table or clearing those you want to remove.



You can add devices manually, import devices from a device provisioning file, edit device details, perform security actions, send notifications to devices, and delete devices. You can also export all of the device table data to a .csv file to create a custom report. The server exports all device attributes and, if you apply filters, XenMobile uses the filters when creating the .csv file.

See the following sections for details about managing devices:

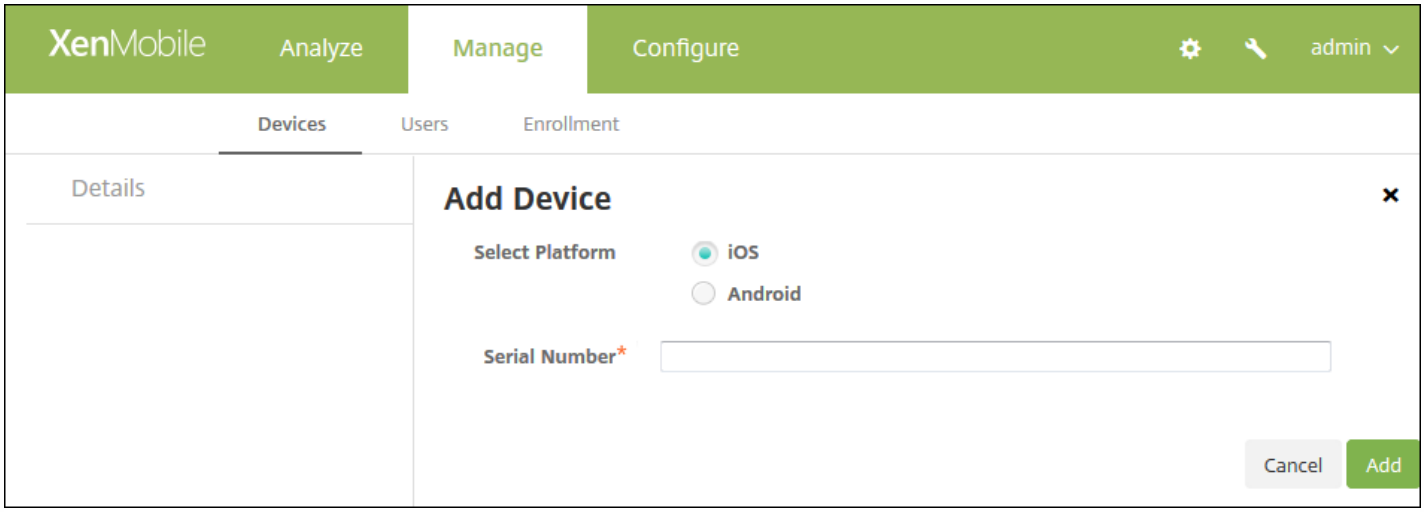
- Add a device manually
- Import devices from a device provisioning file
- Perform security actions

- Send a notification to devices
- Delete 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.

2. Click **Add**. The **Add Device** page appears.



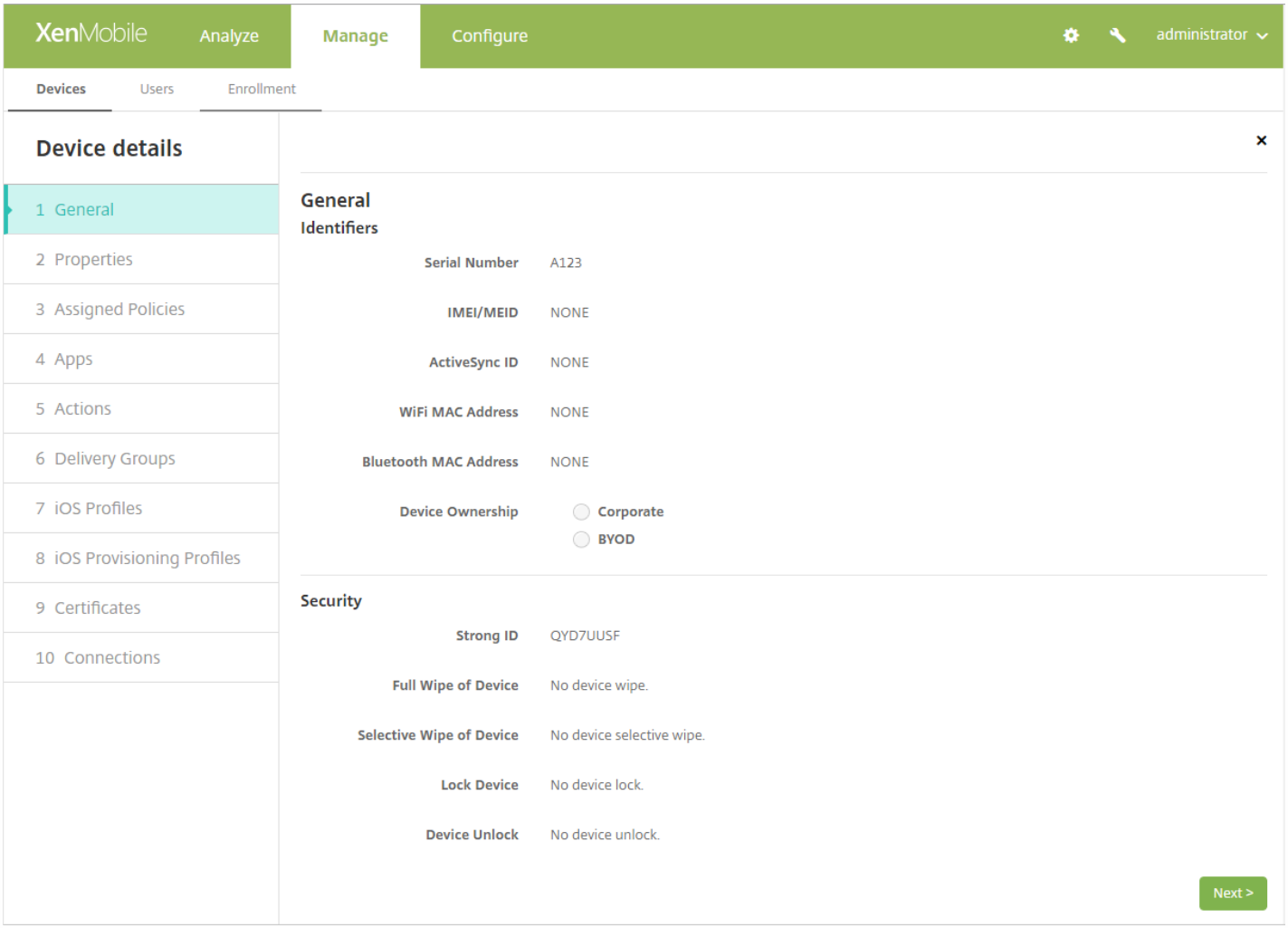
3. Configure these settings:

- **Select platform**: Click either **iOS** or **Android**.
- **Serial Number**: Type the device's serial number.
- **IMEI/MEID**: Optionally, for Android devices only, type the device's IMEI/MEID information.

4. Click **Add**. The **Devices** table appears with the device added to the bottom of the list. In the list, select 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.



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.

6. The **Properties** page lists the device properties that XenMobile will 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,

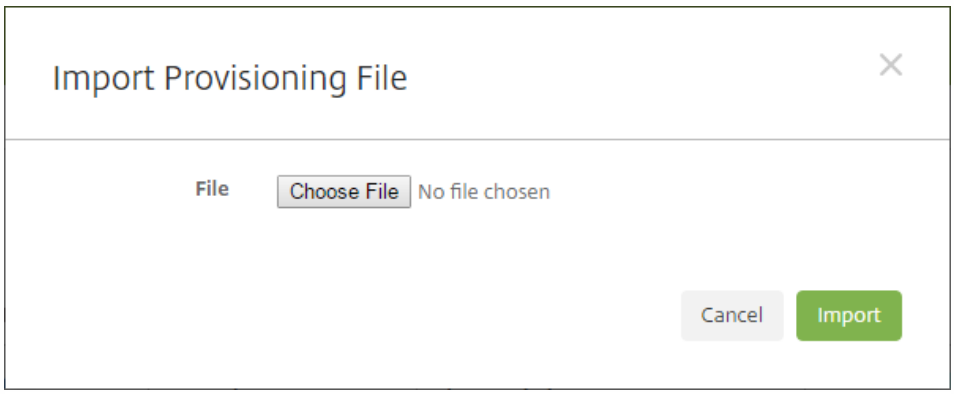
type, and other information.

- **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.

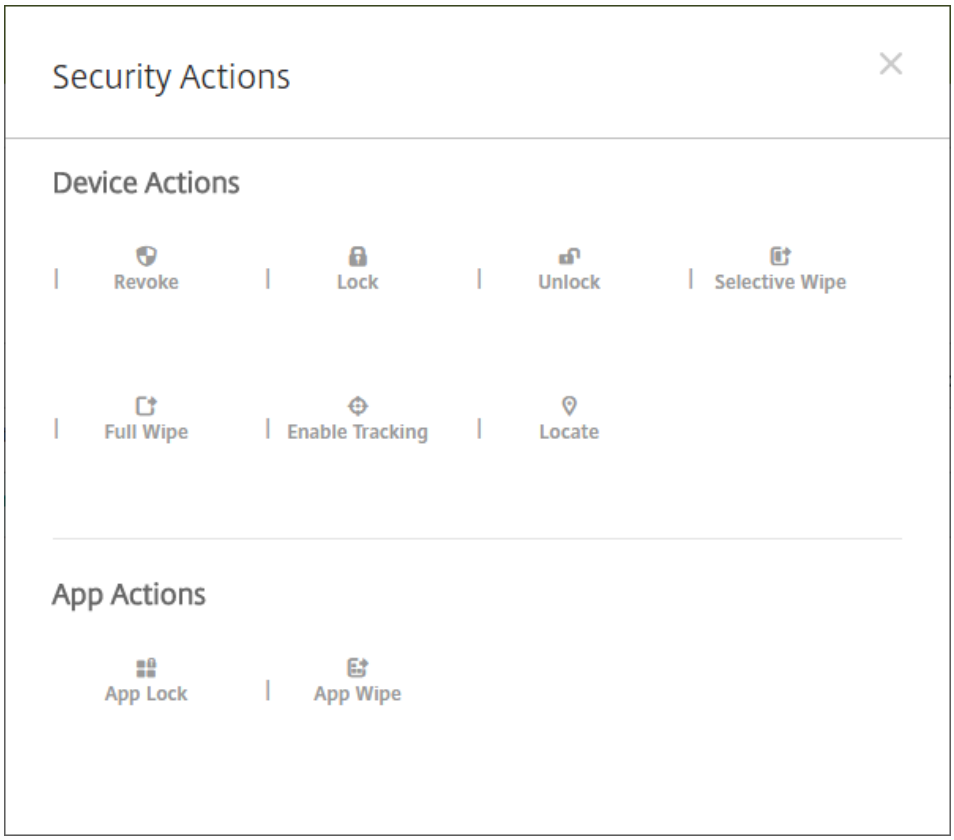
Perform security actions

You can perform device and app security actions from the **Devices** page. Device actions include revoke, lock, unlock, and wipe. App security actions include app lock and app wipe.

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

2. In **Security Actions**, click an action and respond to any prompts.

For more information about actions, see Automated actions.



To perform an app lock, unlock, wipe, or unwipe manually

1. Go to **Manage** > **Devices**, select a managed device and then click **Secure**.

2. In the **Security Actions** dialog box, click an action.

Note: You can also use this dialog box to check the status of a device for a user whom you know is disabled or deleted from Active Directory. The presence of the App Unlock or App Unwipe actions indicate the users' apps are currently locked or wiped.

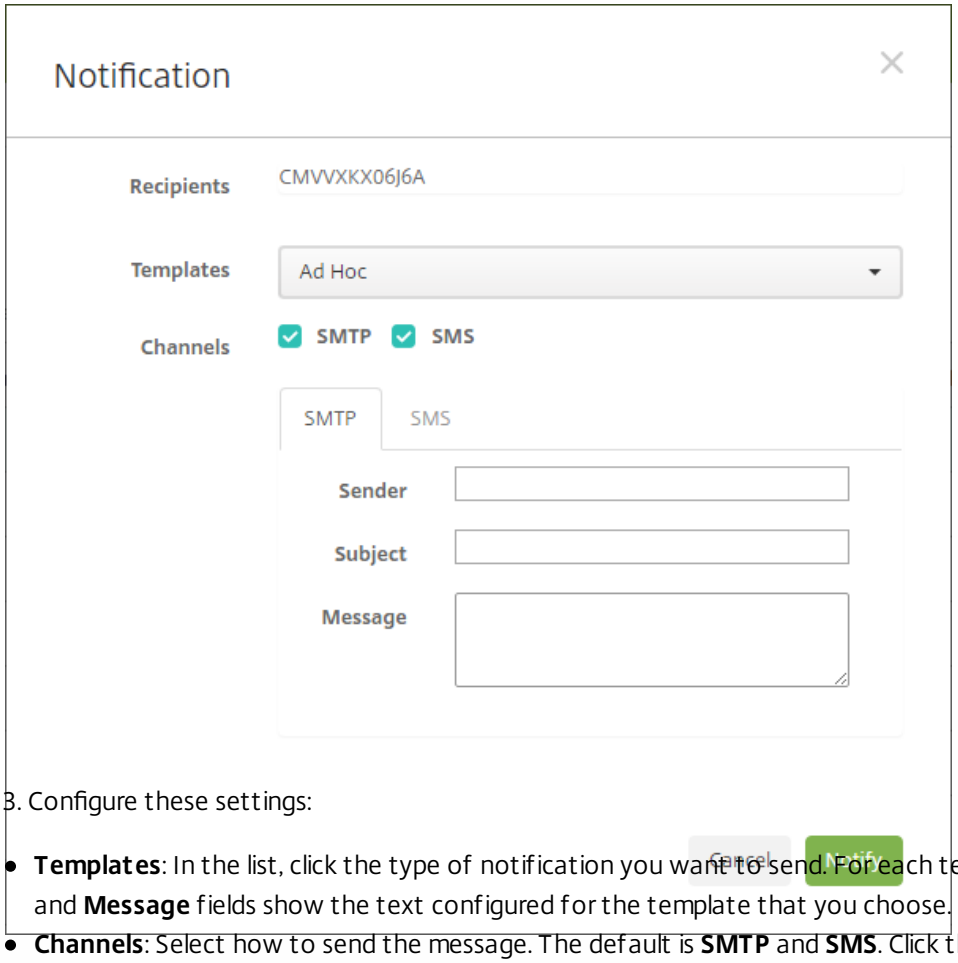
3. Confirm the action.

Send a notification to devices

You can send notifications to devices from the Devices page. For more information about notifications, see Notifications.

1. On the **Manage > Devices** page, 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 of the devices to receive the notification.



3. Configure these settings:

- **Templates**: In the list, click the type of notification you want to send. For each template except for **Ad Hoc**, the **Subject** and **Message** fields show the text configured for the template that you choose.
- **Channels**: Select how to send the message. The default is **SMTP** and **SMS**. Click the tabs to see the message format for each channel.
- **Sender**: Enter an optional sender.
- **Subject**: Enter a subject for an **Ad Hoc** message.
- **Message**: Enter the message for an **Ad Hoc** message.

4. Click **Notify**.

Delete devices

1. In the **Devices** table, select the device or devices you want to delete.

2. Click **Delete**. A confirmation dialog box appears. Click **Delete** again. You cannot undo this operation.

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.

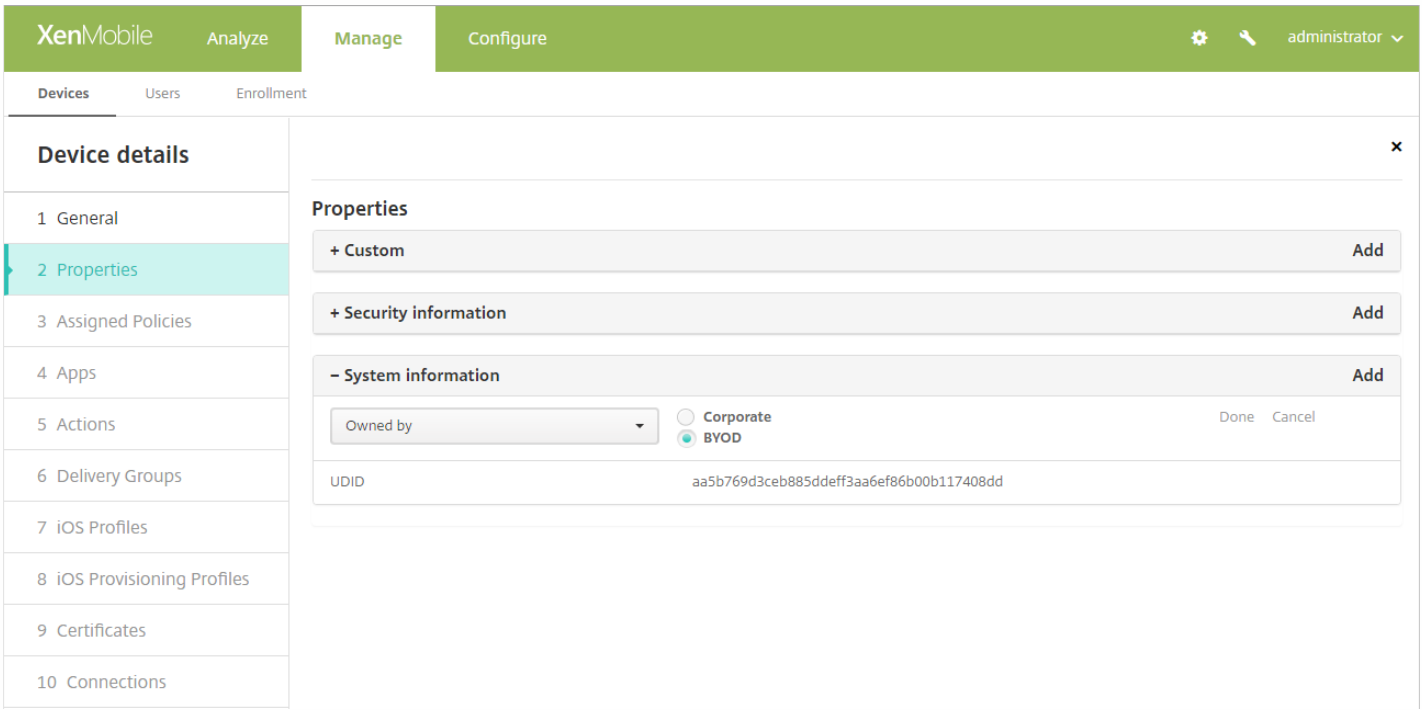
3. When prompted, open or save the .csv file. How you do this depends on the browser you are using. You can also cancel the operation.

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 also tag the device as either corporate- or employee-owned. As shown in the following figure, you can also tag a device manually by adding a property to the device from the Devices tab in the XenMobile console, adding the property named Owned by and choosing either Corporate or BYOD (employee-owned).



Device provisioning file formats

Many mobile operators or device manufacturers provide lists of authorized mobile devices, and 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

```
1050BF3F5173010816100655105903911;5244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903922;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F5173010816100655105903933;35244201625379903;iOS;test;

4050BF3F5173010816100655105903933;;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: 1050BF3F51730108161006551059039 1
- 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	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 Values (meaning): 1 (Yes) 0 (No)	Boolean
Active iTunes account	ACTIVE_ITUNES Values (meaning): 1 (Yes) 0 (No)	Boolean
ActiveSync ID	EXCHANGE_ACTIVESYNC_ID	String
ActiveSync device known by MSP	AS_DEVICE_KNOWN_BY_ZMSP Values (meaning): 1 (True) 0 (False)	Boolean
Administrator disabled	ADMIN_DISABLED Values (meaning): 1 (Yes) 0 (No)	Boolean
Amazon MDM API available	AMAZON_MDM Values (meaning): 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 Values: DeviceAdministrator (Device Owner) AvengerManagedProfile (Work Managed Device) ManagedProfile (Work Profile)	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	BATTERY_CHARGING Values (meaning): 1 (True) 0 (False)	Boolean
Bes device known by MSP	BES_DEVICE_KNOWN_BY_ZMSP Values (meaning): 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 Values (meaning): 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 Policy	WINDOWS_HAS_DEP_POLICY	String

Data roaming allowed	DATA_ROAMING_ENABLED Values (meaning): 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 Values (meaning): 1 (Yes) 0 (No)	Boolean
ELAM Driver Loaded?	WINDOWS_HAS_ELAM_DRIVER_LOADED	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 Values (meaning): 1 (Yes) 0 (No)	Boolean
Firewall Status	FIREWALL_STATUS	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 Values (meaning): 1 (Yes) 0 (No)	Boolean
HTC API version	HTC_MDM_VERSION	String
HTC MDM API available	HTC_MDM Values (meaning): 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 Values (meaning):	Boolean

	1 (True) 0 (False)	
Issued At	WINDOWS_HAS_ISSUED_AT	String
Jailbroken/Rooted	ROOT_ACCESS Values (meaning): 1 (Yes) 0 (No)	Boolean
Kernel Debugging Enabled?	WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED	String
Kiosk mode	IS_KIOSK Values (meaning): 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 Values (meaning): 1 (Yes) 0 (No)	Boolean
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 Values (meaning): 1 (True) 0 (False)	Boolean
NitroDesk TouchDown licensed via MDM	TOUCHDOWN_LICENSED_VIA_MDM Values (meaning): 1 (True) 0 (False)	Boolean
Operating system build	SYSTEM_OS_BUILD	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 Values (meaning): 1 (True) 0 (False)	Boolean
Owned by	CORPORATE_OWNED Values (meaning):	Boolean

	1 (Corporate) 0 (BYOD)	
PCR0	WINDOWS_HAS_PCR0	String
PIN code for geofence	PIN_CODE_FOR_GEO_FENCE	String
Passcode compliant	PASSCODE_IS_COMPLIANT Values (meaning): 1 (Yes) 0 (No)	Boolean
Passcode compliant with configuration	PASSCODE_IS_COMPLIANT_WITH_CFG Values (meaning): 1 (Yes) 0 (No)	Boolean
Passcode present	PASSCODE_PRESENT Values (meaning): 1 (Yes) 0 (No)	Boolean
Perimeter breach	GPS_PERIMETER_BREACH Values (meaning): 1 (Yes) 0 (No)	Boolean
Personal Hotspot activated	PERSONAL_HOTSPOT_ENABLED Values (meaning): 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 IMEI	IDENTITY1_IMEI	String
Primary SIM IMSI	IDENTITY1_IMSI	String
Primary SIM Roaming	IDENTITY1_ROAMING Values (meaning): 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 Values (meaning): 1 (True) 0 (False)	Boolean
Safe Mode Enabled?	WINDOWS_HAS_SAFE_MODE	String
Samsung KNOX API available	SAMSUNG_KNOX Values (meaning): 1 (True) 0 (False)	Boolean
Samsung KNOX API version	SAMSUNG_KNOX_VERSION	String
Samsung KNOX attestation	SAMSUNG_KNOX_ATTESTED Values (meaning): 1 (Passed) 0 (Failed)	Boolean

Samsung KNOX attestation updated date	SAMSUNG_KNOX_ATT_UPDATED_TIME	Date
Samsung SAFE API available	SAMSUNG_MDM Values (meaning): 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 Values (meaning): 1 (True) 0 (False)	Boolean
Secure Boot Enabled?	WINDOWS_HAS_SECURE_BOOT_ENABLED	String

SecureContainer Enabled	WINDOWS_HAS_BIT_LOCKER_STATUS	String
Serial number	SERIAL_NUMBER	String
Sony Enterprise API available	SONY_MDM Values (meaning): 1 (True) 0 (False)	Boolean
Sony Enterprise API version	SONY_MDM_VERSION	String
Supervised	Supervised Values (meaning): 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
UDID	UDID	String
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 Values (meaning): 1 (True) 0 (False)	Boolean
Voice roaming allowed	VOICE_ROAMING_ENABLED Values (meaning): 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

Lock iOS devices

Feb 01, 2017

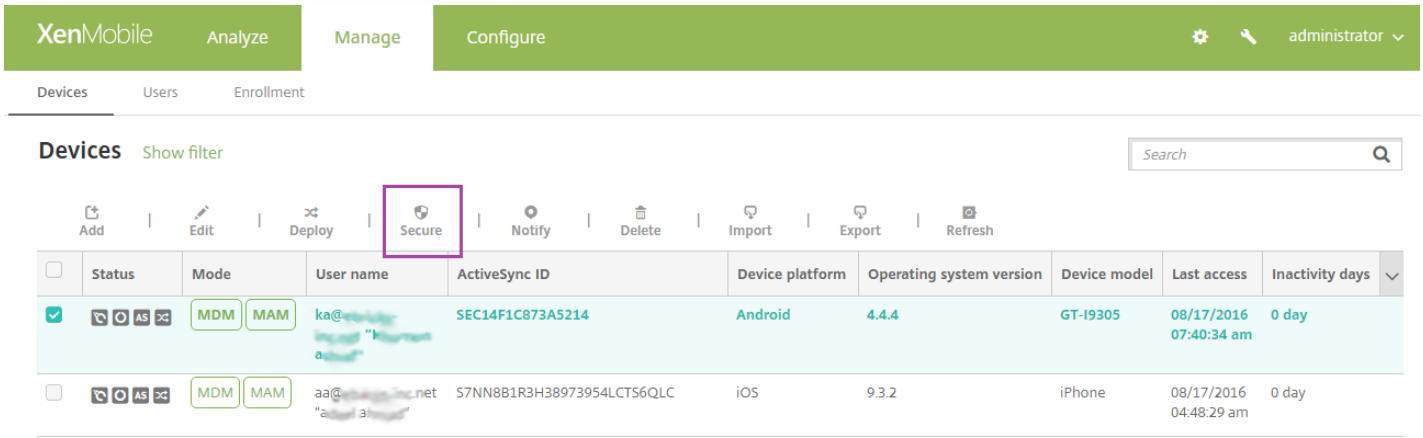
You can lock a lost iOS device with an accompanying display of a message and phone number that displays on the device lock screen. This feature is supported on devices running iOS 7 and above.

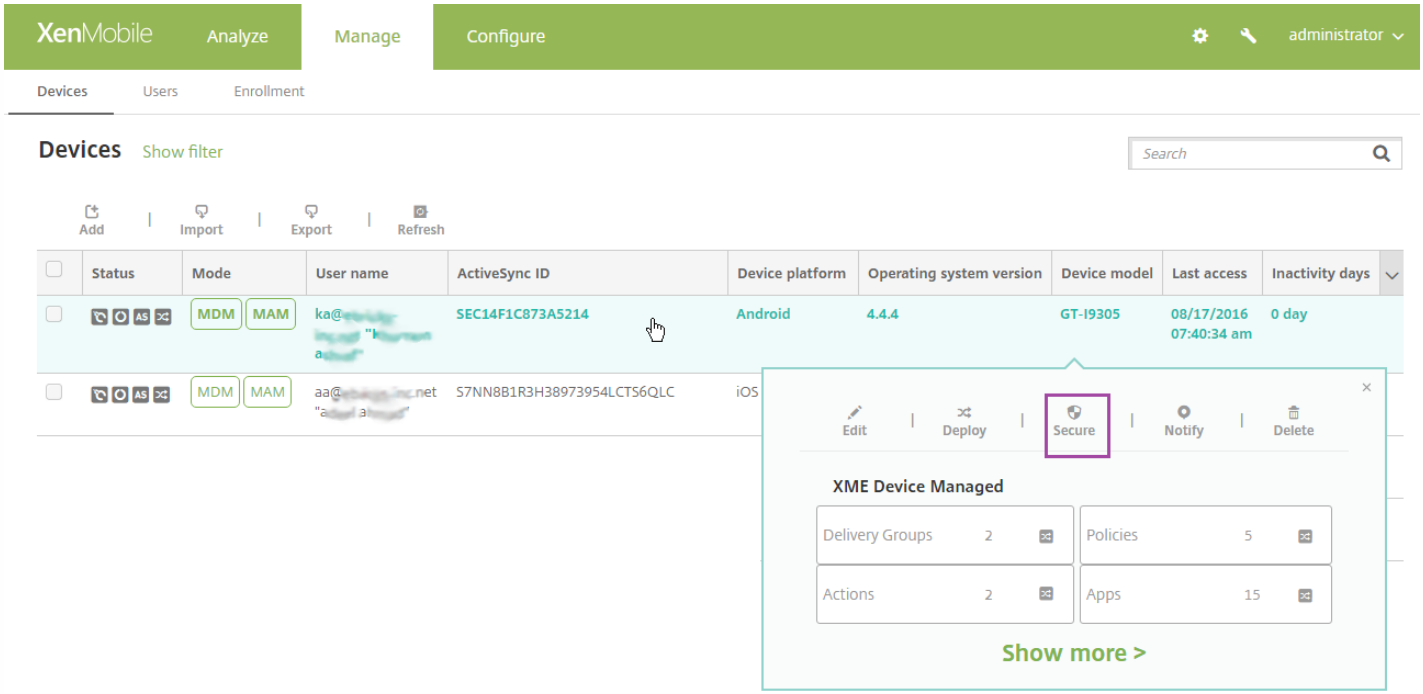
In order for a message and phone number to display on a locked device, the Passcode policy must be set to true in the XenMobile console. Alternatively, users must enable the passcode on the device manually.

1. In the XenMobile console, click **Manage > Devices**. The **Devices** page displays.

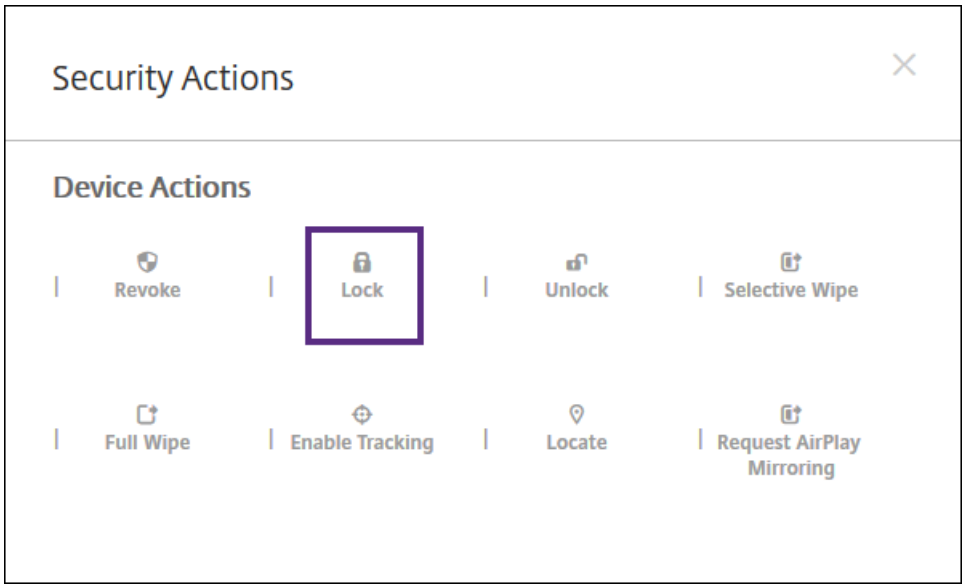
2. Select the iOS device you want to lock.

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.

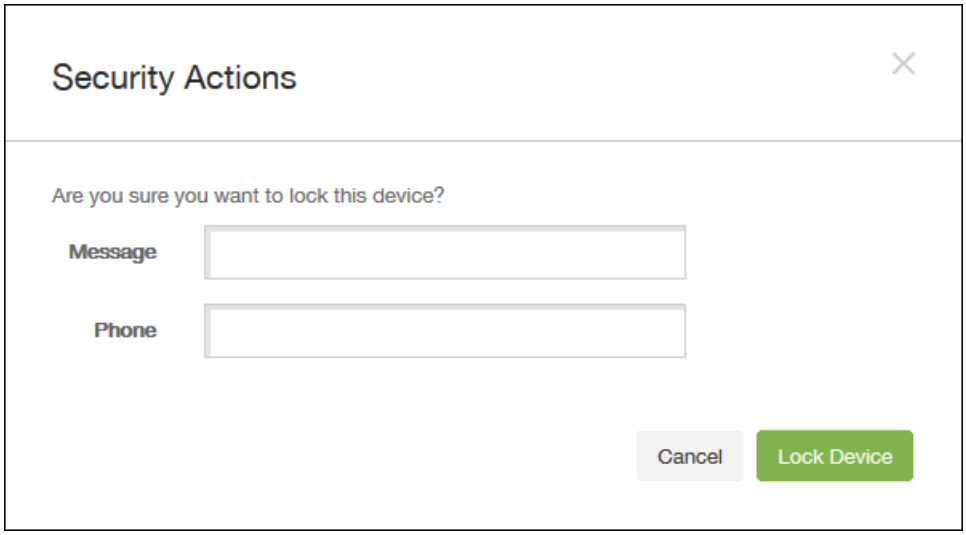




3. In the options menu, click **Secure**. The **Security Actions** dialog box displays.



4. Click **Lock**. The **Security Actions** confirmation dialog box displays.



5. Optionally, type a message and phone number that appears on the lock screen of the device.

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.

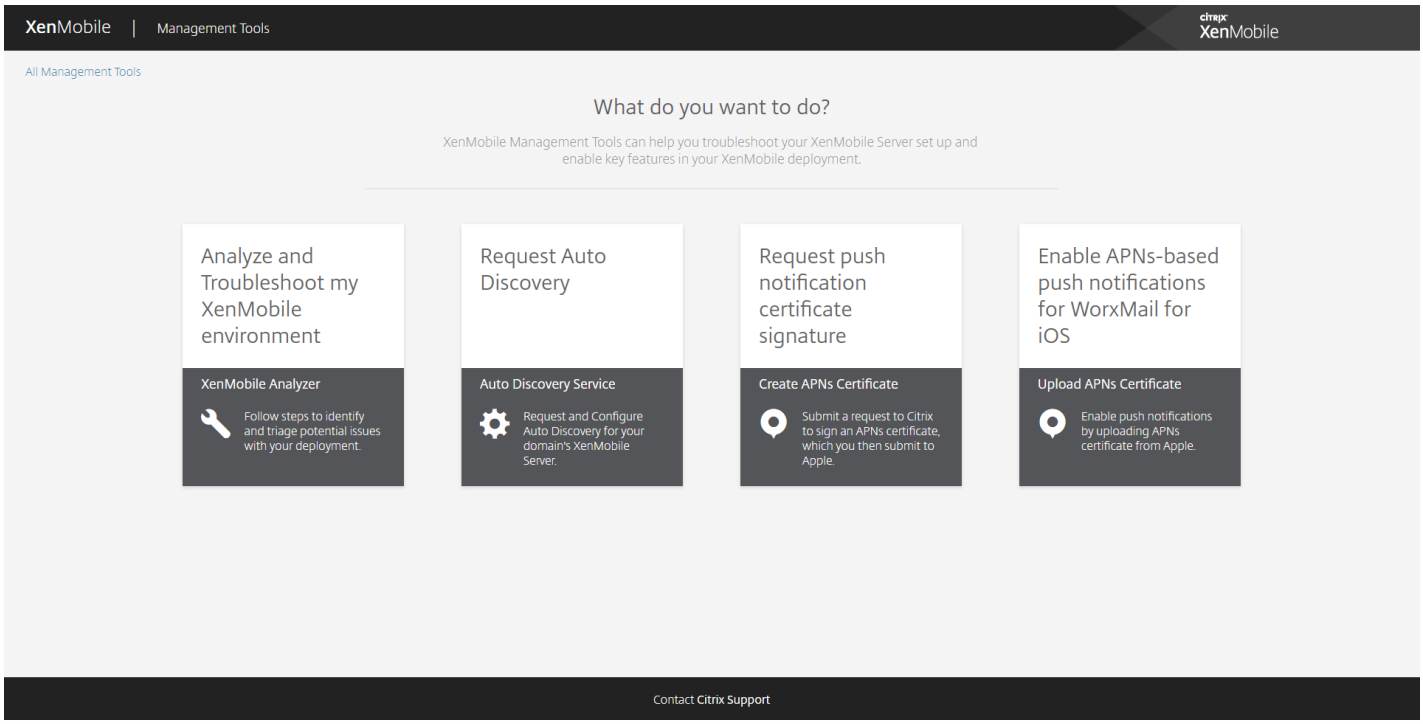
6. Click **Lock Device**.

XenMobile Autodiscovery Service

Feb 25, 2017

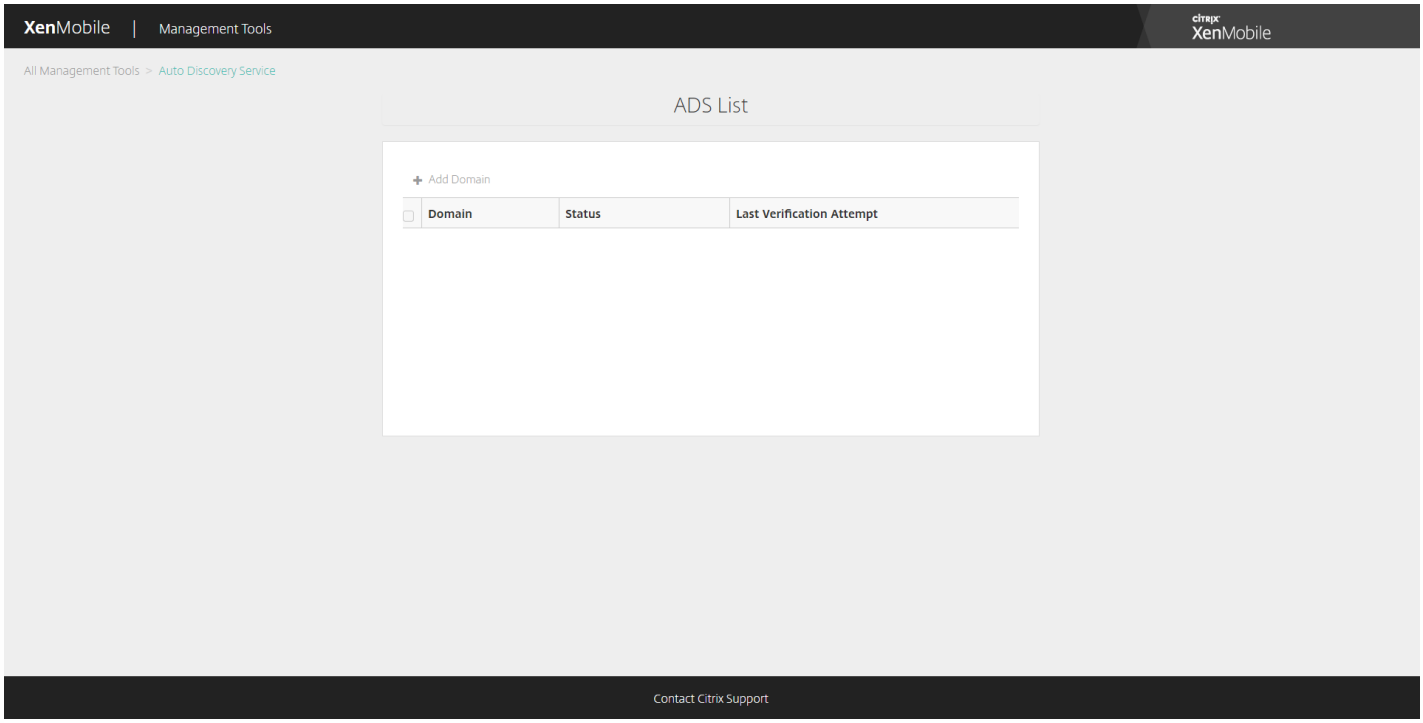
Autodiscovery is an important part of many XenMobile deployments. Autodiscovery simplifies the enrollment process for users. They can use their network user names and Active Directory passwords to enroll their devices, rather than having to also enter details about the XenMobile server. Users enter their 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://xenmobiletools.citrix.com and the click **Request Auto Discovery**.

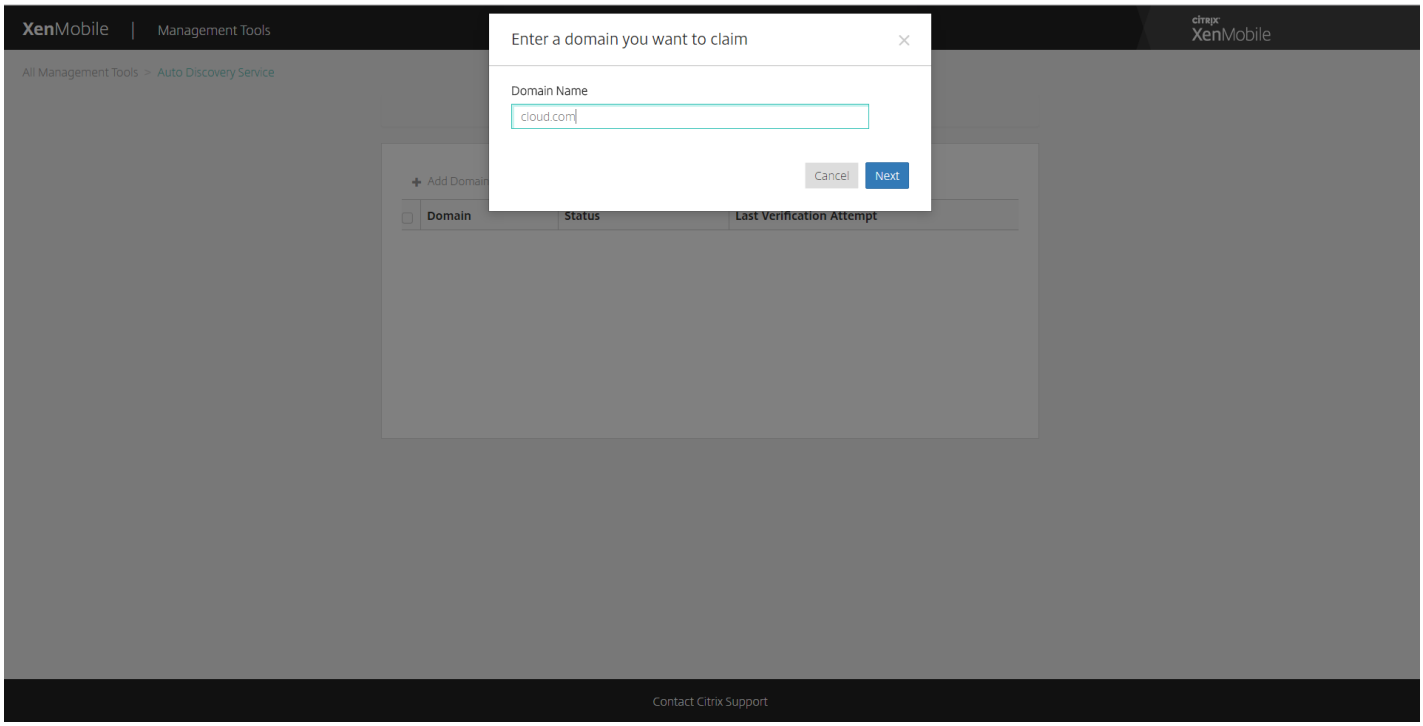


Requesting AutoDiscovery

1. On the AutoDiscovery Service page, you need to first claim a domain. Click **Add Domain**.



2. In the dialog box that opens, enter the domain name of your XenMobile environment and then click **Next**.



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.

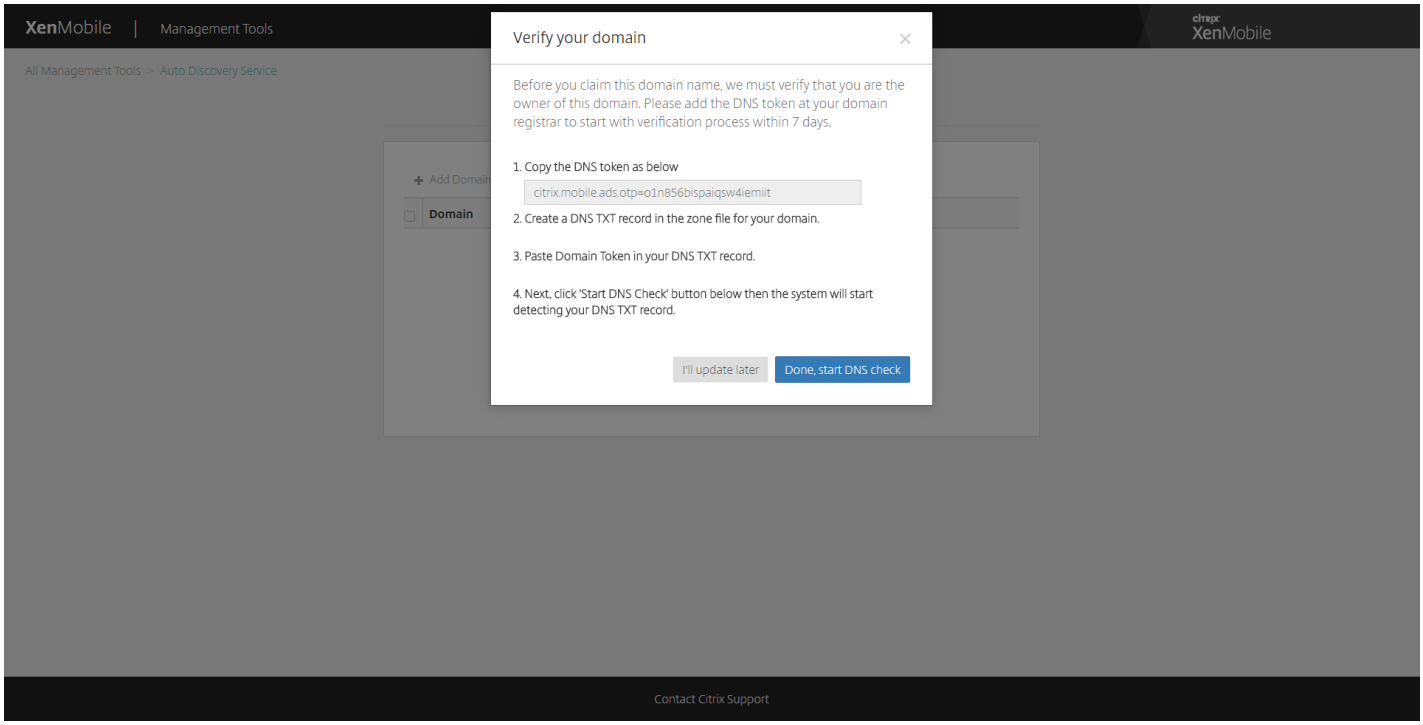
To create a DNS TXT record you need to log into the Domain Hosting Provider portal for the domain you have added in step 2 above. In the Domain Hosting portal you can edit your Domain Name Server Records and add a custom TXT record. An example below of a adding a DNS TXT entry in a hosting portal for 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.

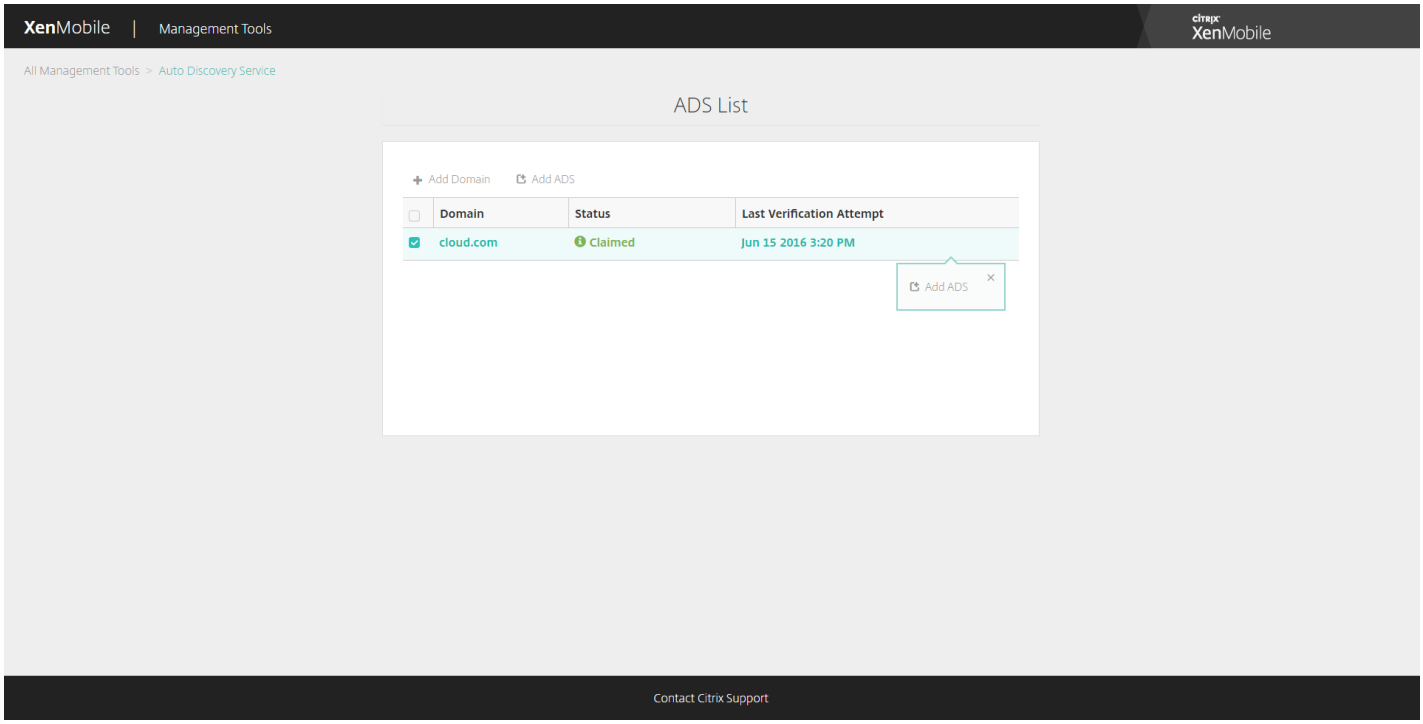
The system detects your DNS TXT record. Alternatively, you can click I'll update later, and the record is saved. The DNS check won't start until you select the Waiting record and click DNS Check.

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.

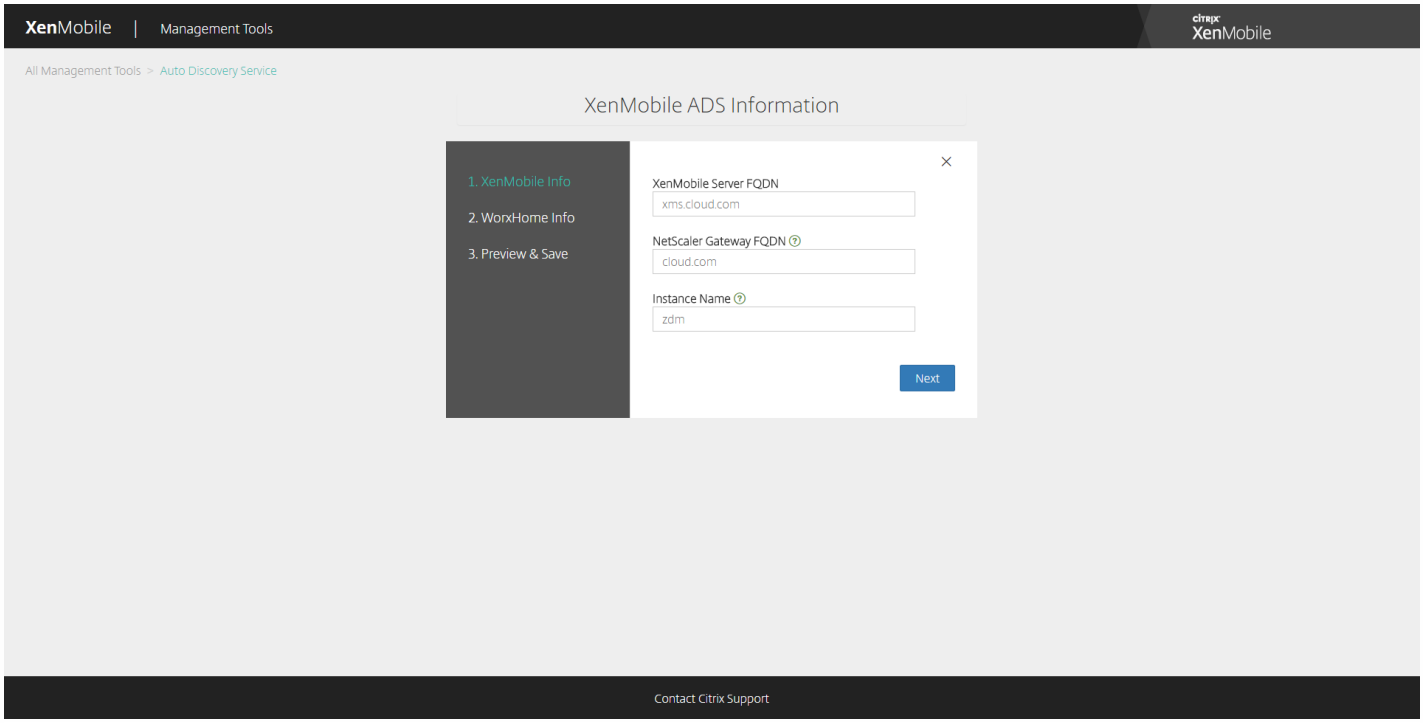


4. After you claim your domain, you can enter AutoDiscovery Service information. Right-click the domain record for which you want to request autodiscovery and then click **Add ADS**.

If your domain already has an AutoDiscovery record, please log a case with Citrix Technical Support to modify details as required.



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".



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**.

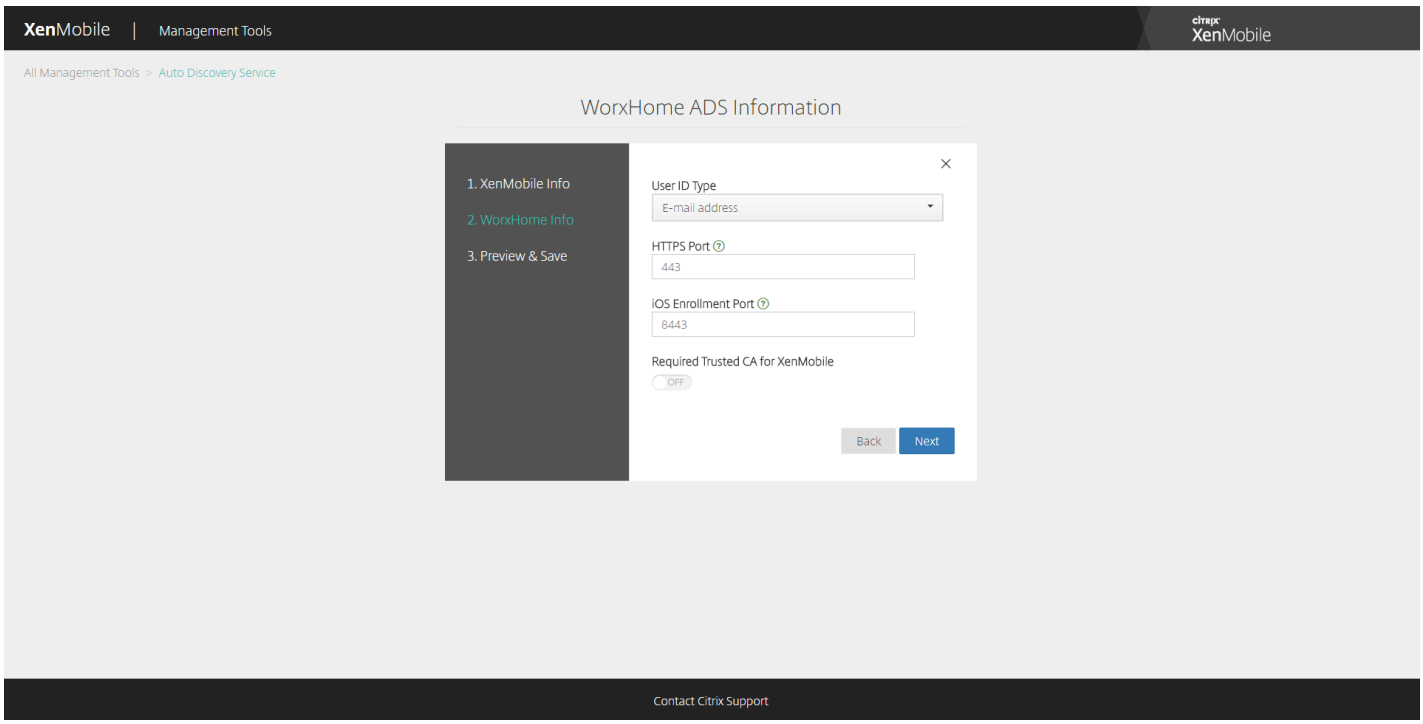
a. **User ID Type**: Select the type of ID with which users sign on as either **E-mail address** or **UPN**.

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.

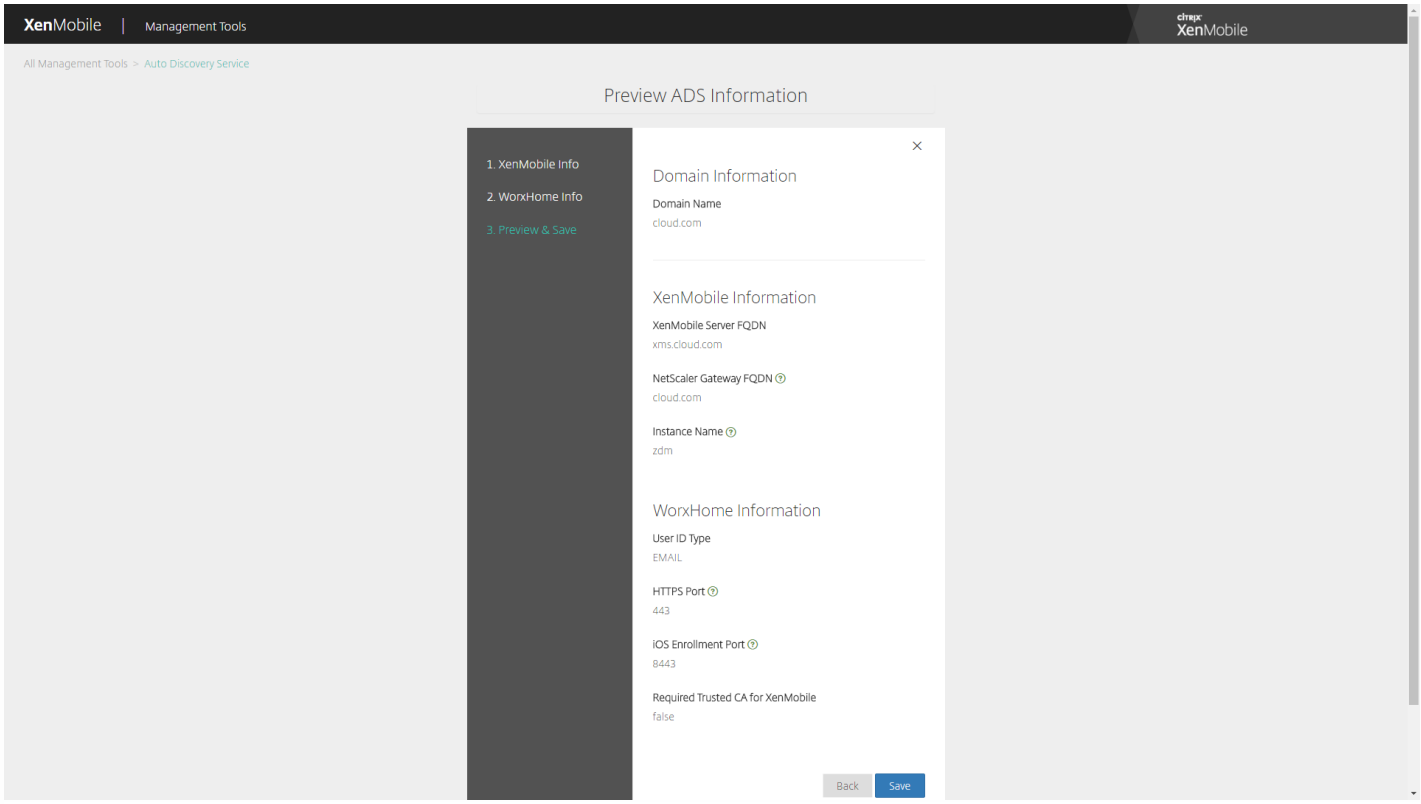
c. **iOS Enrollment Port**: Enter the port used to access Secure Hub for iOS enrollment. Typically, this is port 8443.

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.



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**.



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://xenmobiletools.citrix.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://xenmobiletools.citrix.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).

Enroll devices

Feb 16, 2017

To manage user devices remotely and securely, user devices are enrolled in XenMobile. The XenMobile client software is installed on the user device and a users' 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.

Note: Before you can enroll iOS device users, you must request an APNs certificate. For details, see Certificates.

To update configuration options for users and devices, go to **Manage > Enrollment** page. For details, see Send an enrollment invitation in this article.

Android devices

1. Go to the Google Play store on your Android device, download the Citrix Secure Hub app and then tap the app.
2. When prompted to install the app, click **Next** and then click **Install**.
3. After Secure Hub installs, tap **Open**.
4. Enter your corporate credentials, such as the organization's XenMobile server name, User Principal Name (UPN), or email address and 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, which you can use to sign on to Secure Hub and other XenMobile-enabled apps, such as Secure Mail, Secure Web, ShareFile, and more. You will need to 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 automatically push apps to users' devices after enrollment, messages appear prompting them 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 take action 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.

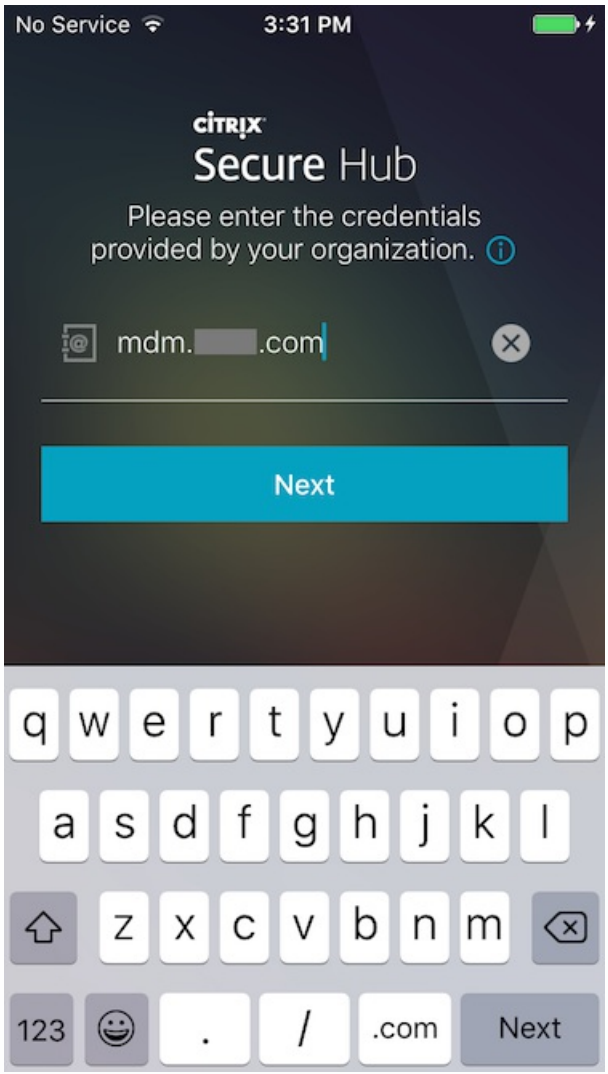
iOS devices

1. Download the Secure Hub app from the Apple iTunes App Store on the device and then install the app on the device.

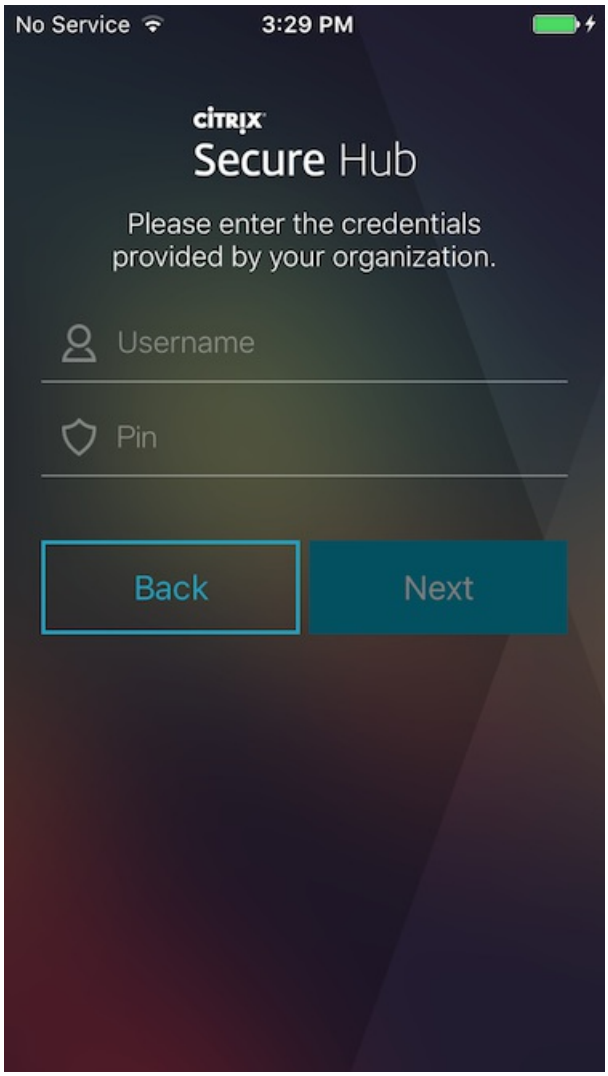
2. On the iOS device Home screen, tap the Secure Hub app.

3. When the Secure Hub app opens, enter the server address that your help desk provided.

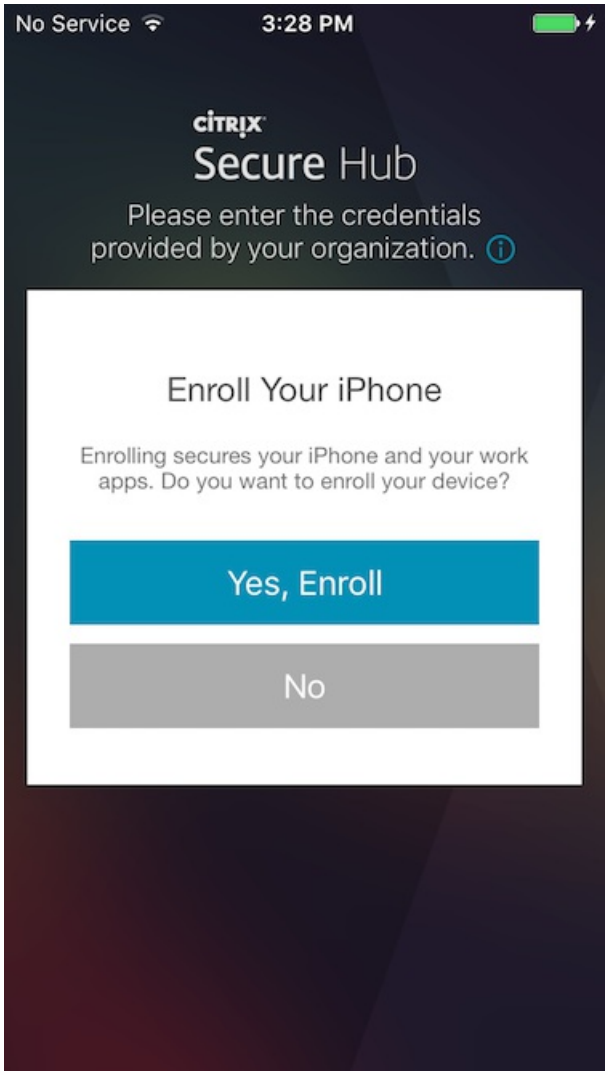
(The screens presented might differ from these examples, depending on how XenMobile is configured.)

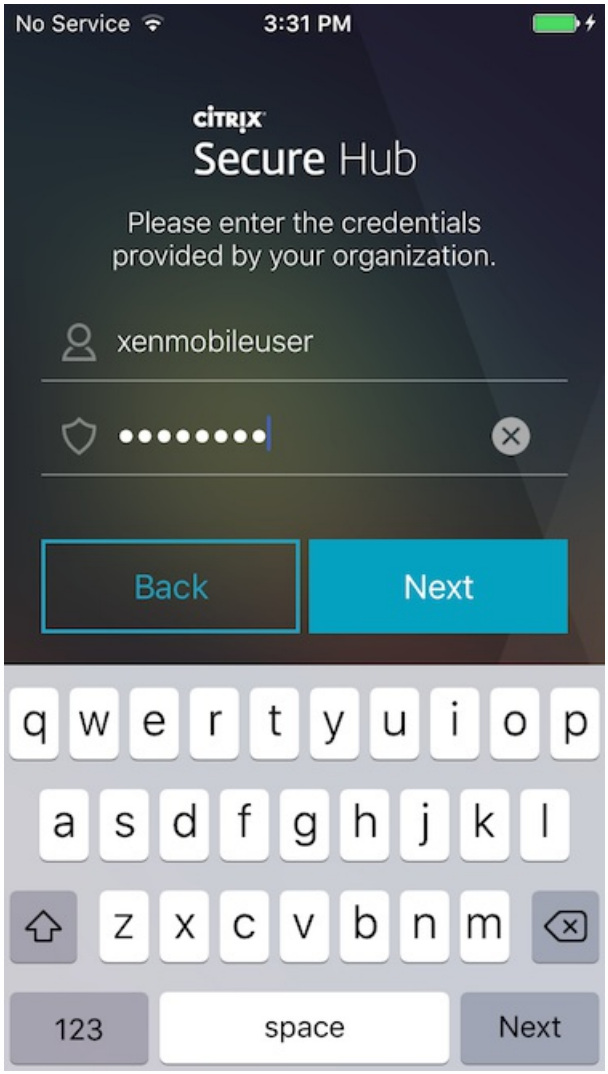


4. When prompted, enter your user name and password or PIN. Click **Next**.



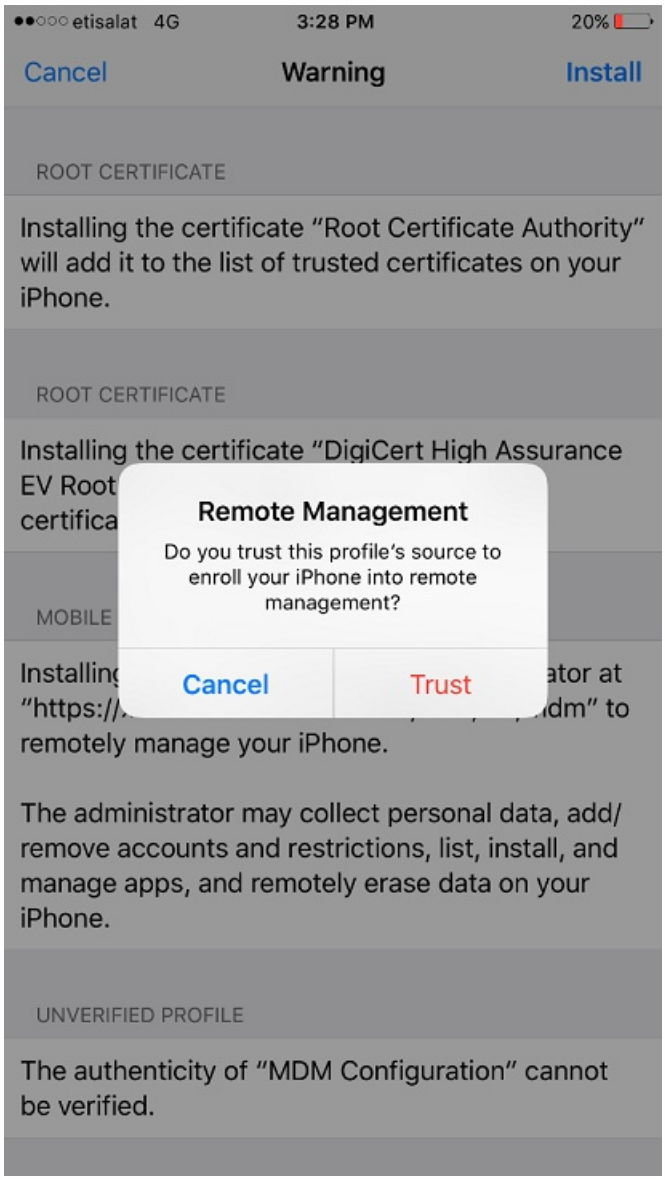
5. When prompted to enroll, click **Yes, Enroll** and then enter your credentials when prompted.



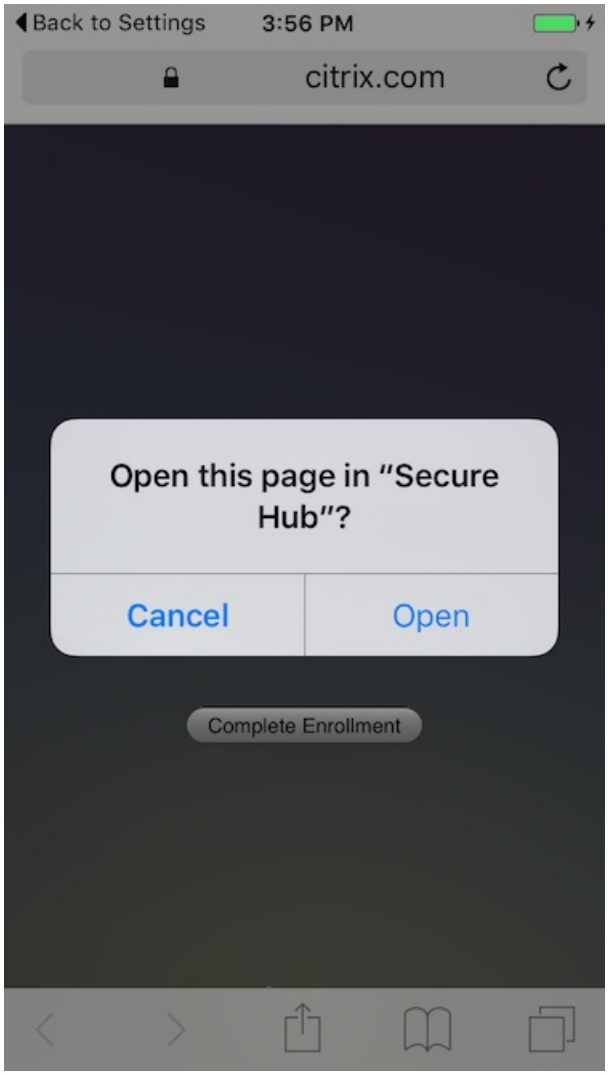


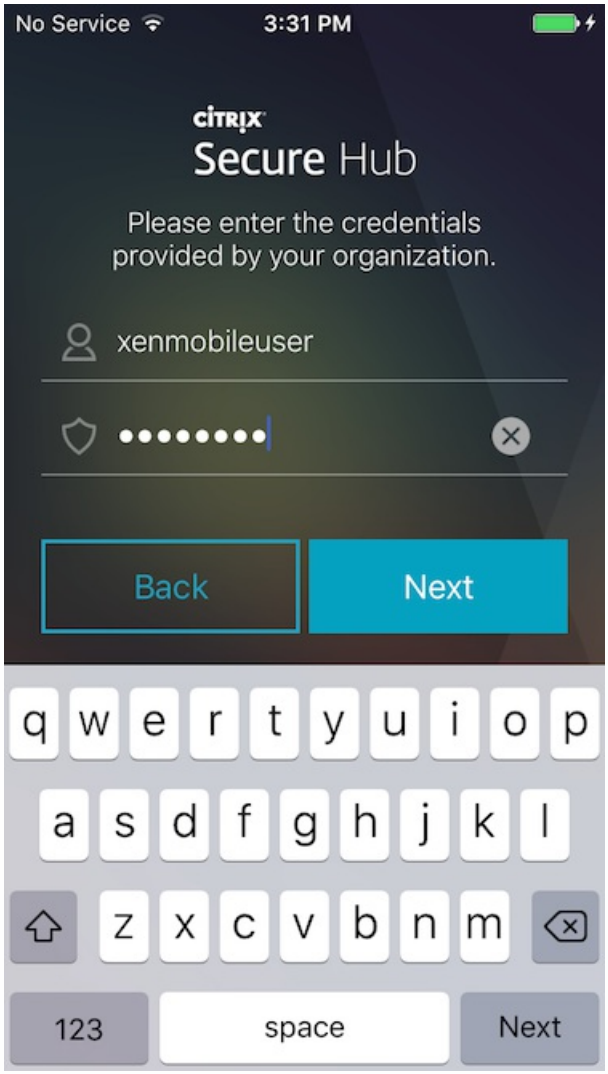
6. Tap **Install** to install the Citrix Profile Services.

7. Tap **Trust**.



8. Tap **Open** and then enter your credentials.





Mac OS X and macOS devices

You can enroll Mac devices that are running OS X or macOS in XenMobile for MDM-only. Mac users enroll over the air, directly from their devices.

To enroll Mac devices, XenMobile administrators do the following:

1. Optionally, set up Mac 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 Mac devices, see XenMobile Device Policies by Platform.

2. Send the enrollment link to the user: https://<serverFQDN>:8443/zdm/macos/otae

- 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.
- zdm is the default instance name used during server installation. If you configured a different instance name, use that instance name instead.

You can also send the link in an email invitation. For details, see Sending enrollment invitations.

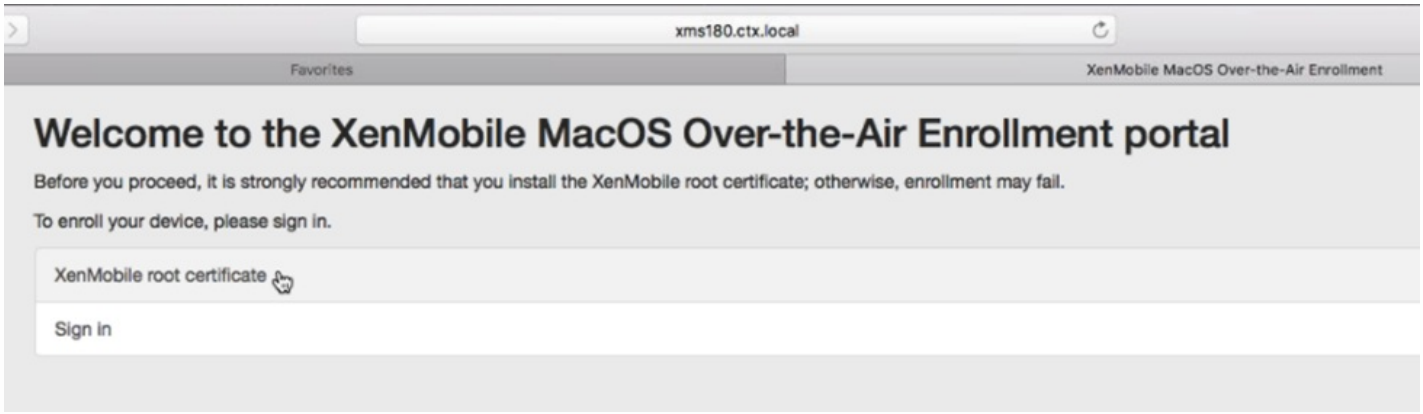
3. Users install certificates as necessary. If you configured a publicly trusted SSL certificate and a publicly trusted digital signed certificate for iOS and macOS, users see the prompt to install certificates. For more information about certificates, see Certificates.

4. On the Mac device to be enrolled, users access the enrollment link using Safari.

Note: If users cannot access the link, they can clear browsing history and cache or use another browser.

5. By default, user see these prompts to install certificates.

a. Users click **XenMobile root certificate**.

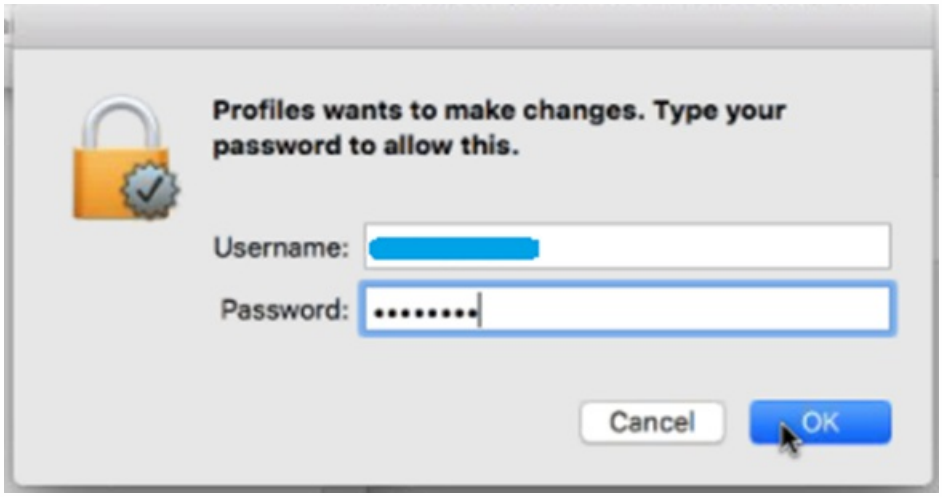


b. Users click **Continue** to install the certificates.

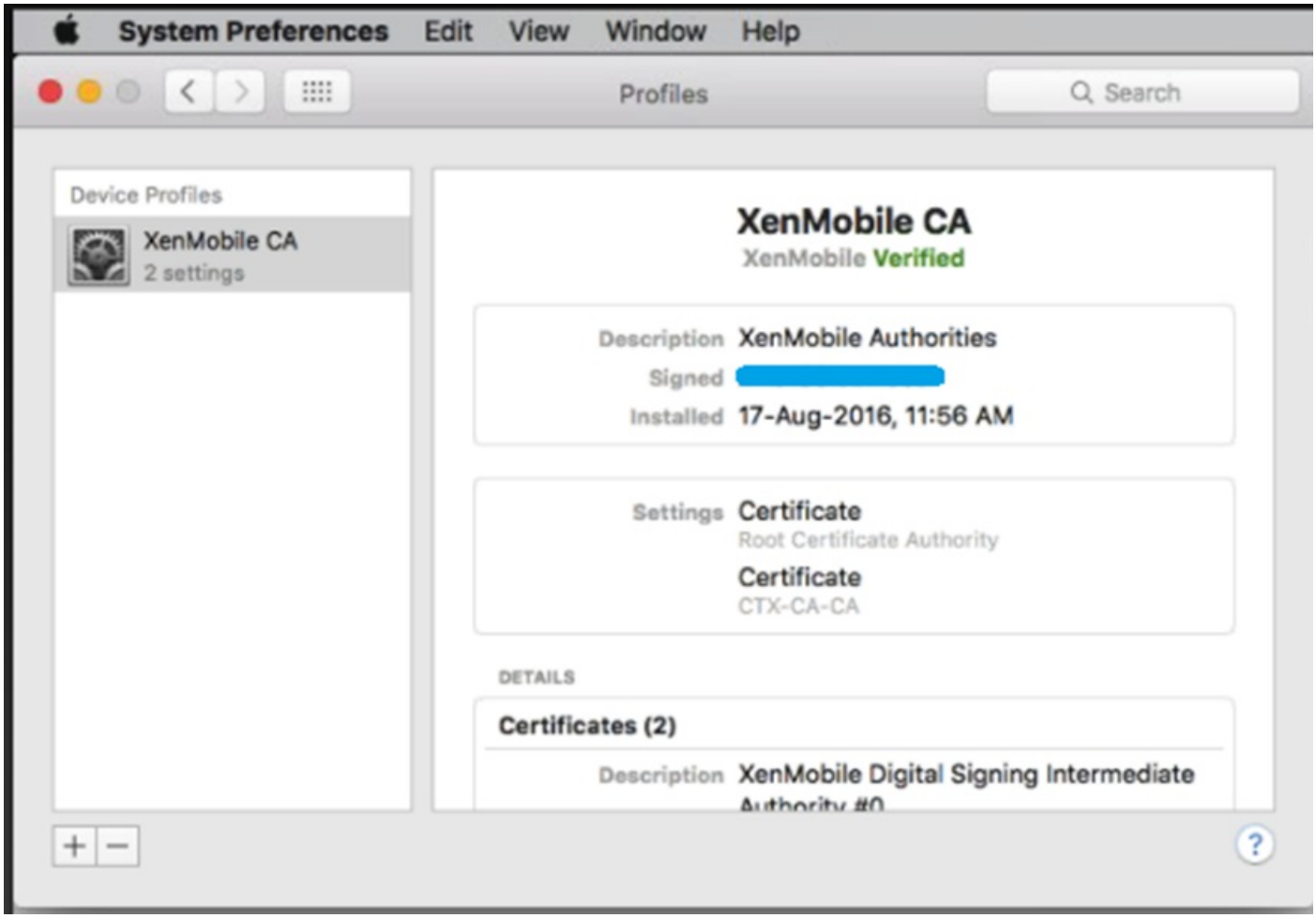
Note: Installing the Root CA certificate of the XenMobile Server enables a trusted communication channel between the device and XenMobile.

c. Users click **Install** to install the XenMobile Profile installation.

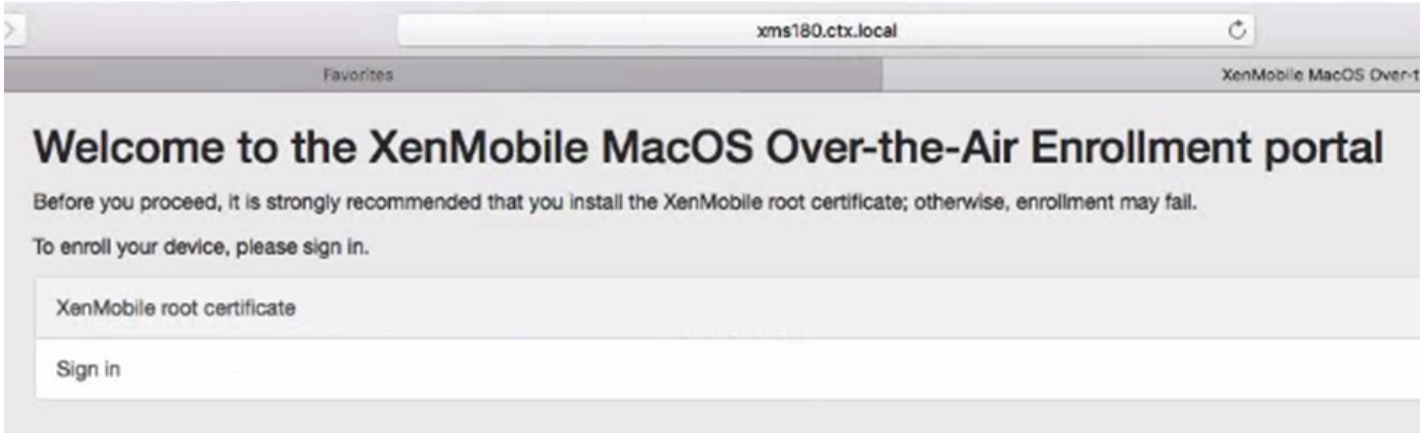
d. Users type the device logon credentials when prompted.



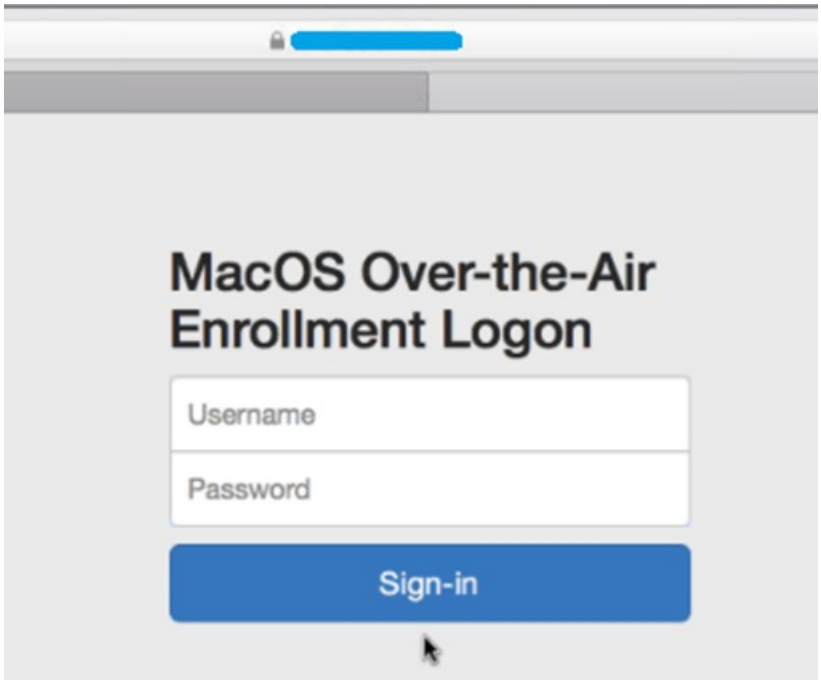
e. This screen appears on successful installation of the XenMobile Certificates under **Profiles**. Users close this screen to proceed with the device enrollment.



6. At the macOS Over-the-Air Enrollment portal, users click **Sign in**.

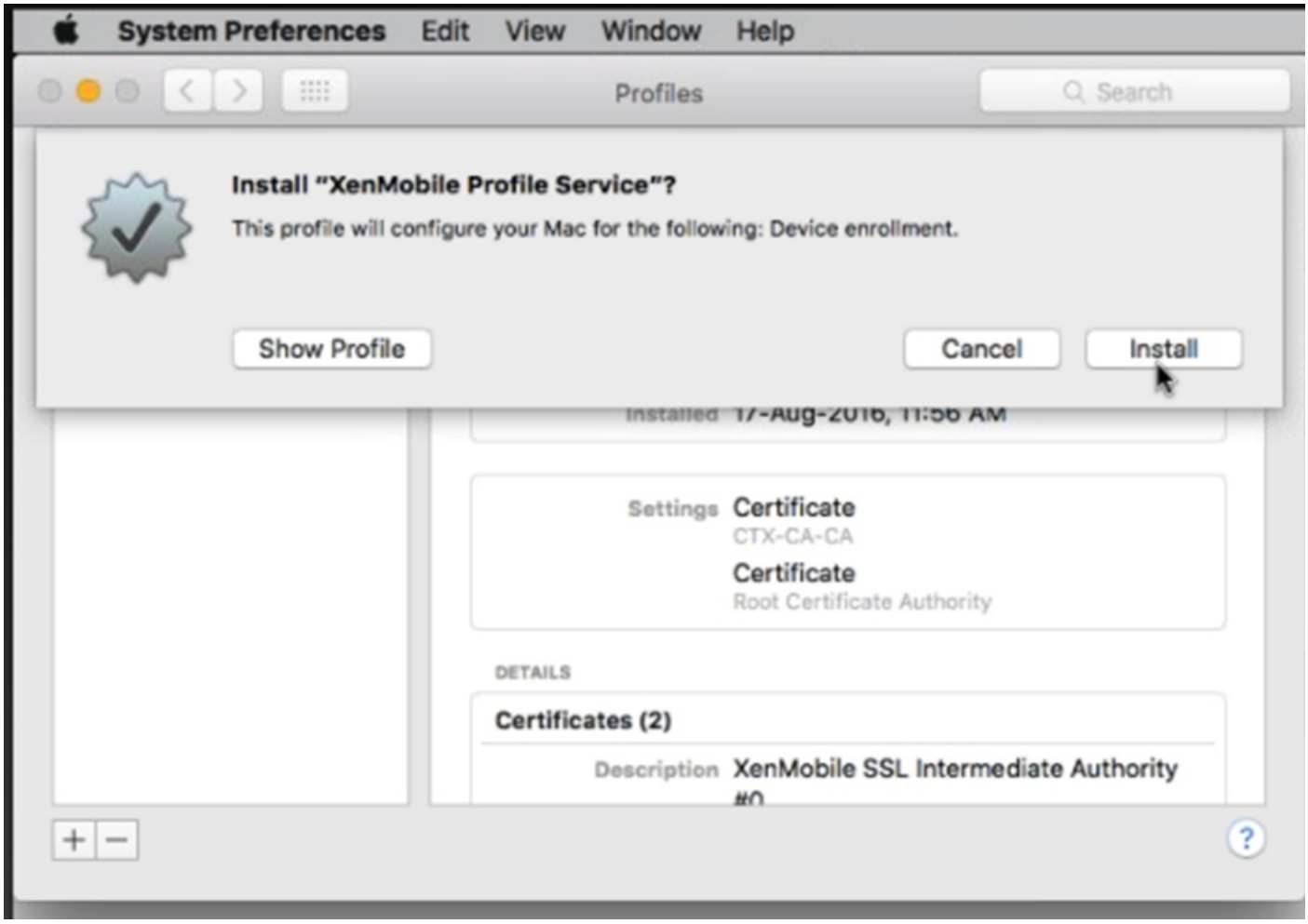


7. Users type the user credentials in UPN or sAMAccountName format, as configured by the XenMobile administrator and then click **Sign-in**.



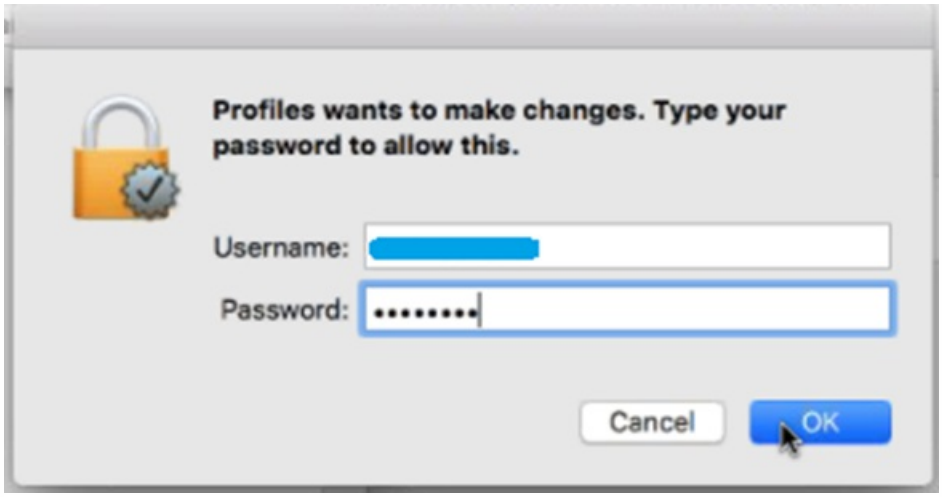
Note: XenMobile validates the user request and verifies the credentials using the Active Directory. The credentials are validated against Active Directory.

8. If the logon is successful, the XenMobile Profile Service window appears. Users click **Install** to install the XenMobile Profile Service. Installing XenMobile Profile Service allows the XenMobile administrator to manage the Mac device remotely.

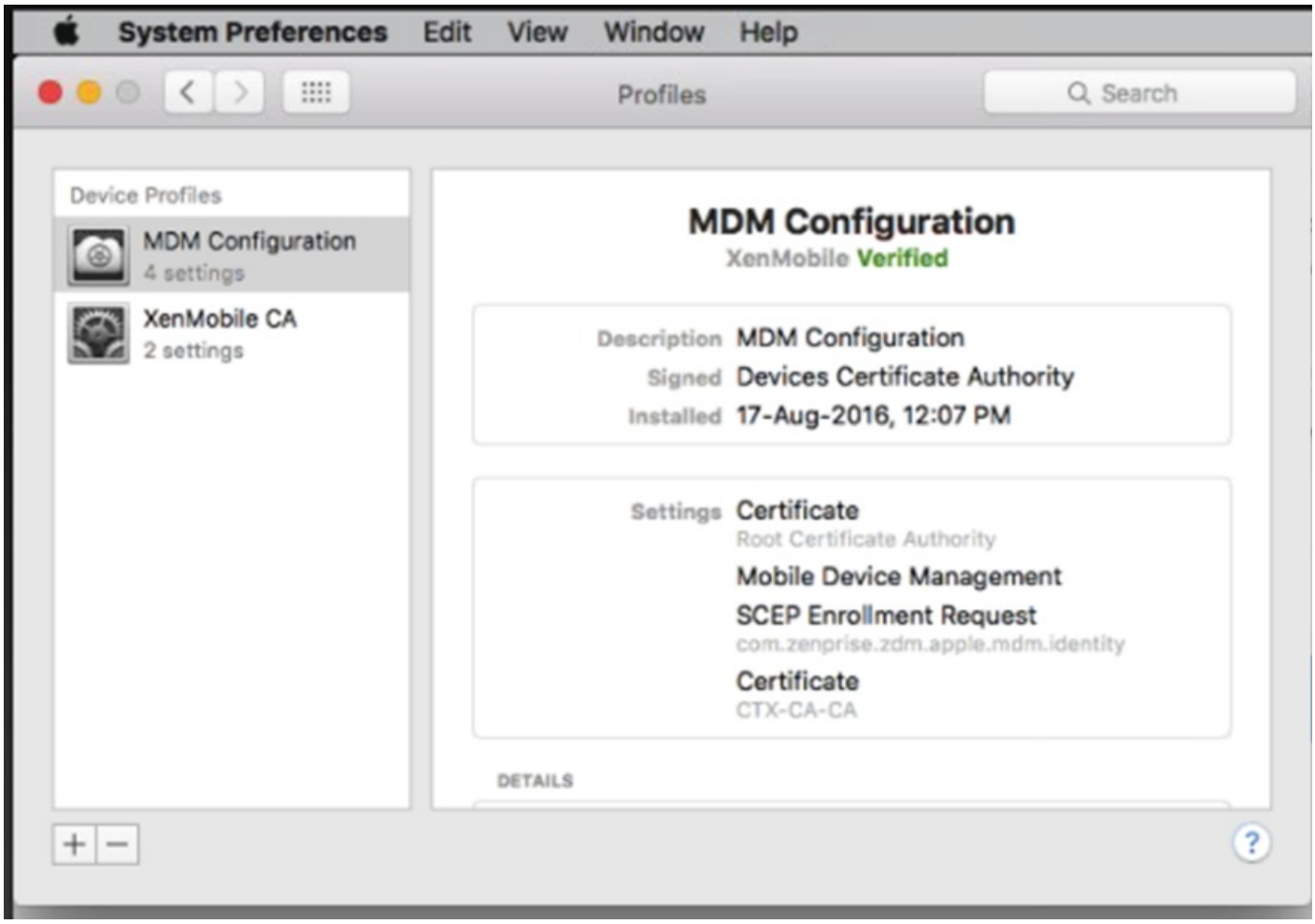


9. To install the MDM profile, users click **Continue** and then click **Install**.

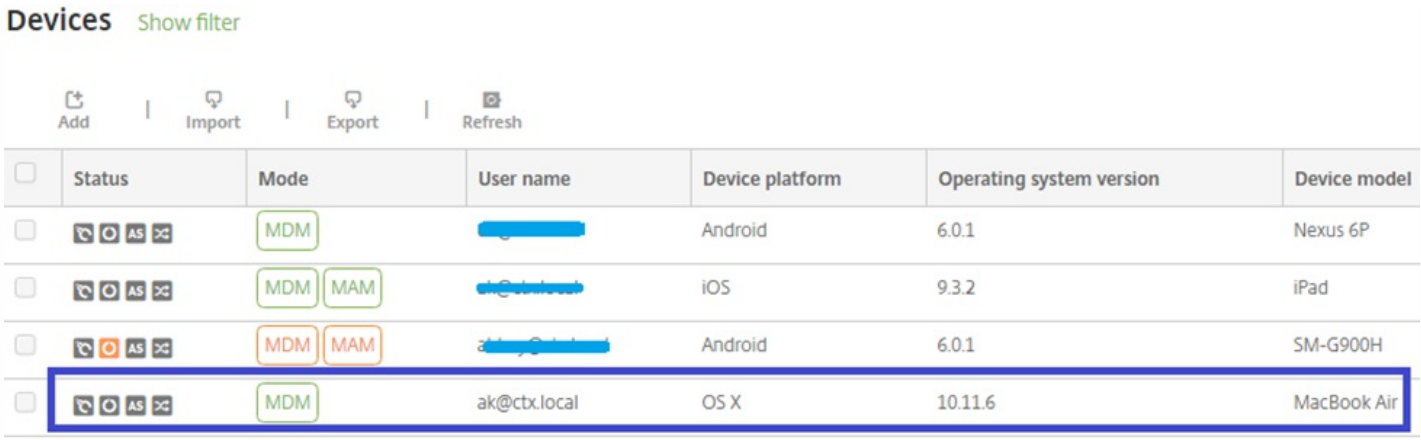
10. When prompted, users type the device logon credentials.



11. When the MDM configuration profile has been installed successfully, the MDM Configuration screen appears.



12. The Mac device now appears in the Device tab of the XenMobile console. You can now start managing Mac devices using XenMobile in the same way you manage mobile devices.



Windows devices

You can enroll devices in XenMobile that are running the following Windows operating systems:

- Windows 8.1 and Windows 10
- Windows Phone 8.1 and 10

Windows and Windows Phone users enroll directly through their devices.

You must configure autodiscovery and the Windows discovery service for user enrollment to enable the management of Windows and Windows Phone devices.

> **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

Users can enroll devices running Windows RT 8.1, both 32-bit and 64-bit versions of Windows 8.1 Pro and Windows 8.1 Enterprise, and Windows 10. To enable management of Windows devices, Citrix recommends you configure autodiscovery and the Windows discovery service. For details, see To enable autodiscovery in XenMobile for user enrollment.

1. On the device, check for and install all available Windows Updates. This step is particularly important when upgrading from Windows 8 to Windows 8.1, because users may not be automatically notified of all available updates.

2. In the charms menu, tap Settings and then:

- For Windows 8.1, tap PC Settings > Network > Workplace.
- For Windows 10, tap Accounts > Access work or school > Connect to work or school.

3. Enter your corporate email address and then tap **Turn on device management** on Windows 8.1 or **Continue** on Windows 10. 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 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**. For Windows 10, in the **Terms of use** dialog box, indicate that you agree to have your device managed and then tap **Accept**.

To enroll Windows devices without self-discovery

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. This step is particularly important when upgrading from Windows 8 to Windows 8.1, because users may not be automatically notified of all available updates.

2. In the charms menu, tap **Settings**, and then:

- For Windows 8.1, tap **PC Settings > Network > Workplace**.
- For Windows 10, tap **Accounts > Access work or school > Connect to work or school**.

3. Enter your corporate email address.

4. On Windows 10, if autodiscovery is not configured, an option appears where you can enter the server details, as described in step 5. On Windows 8.1, if **Automatically detect server address** is set to on, tap to turn the option off.

5. In the **Enter server address** field:

- 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
- For Windows 10, use this address: https://beta.managedm.com:8443/zdm/wpe. If a port other than 8443 is used for unauthenticated SSL connections, use that port number in place of 8443 in this address.

6. Enter your password.
7. 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**. For Windows 10, in the **Terms of use** dialog box, indicate that you agree to have your device managed and then tap **Accept**.

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, make sure 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 a Windows 10 Phone, 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 Phone 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, but should 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.

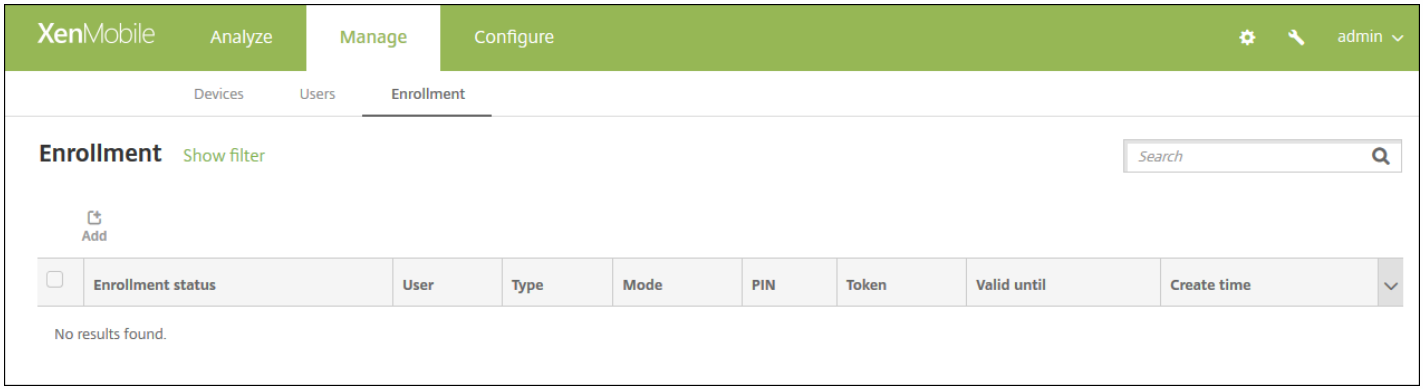
7. On Windows phone 8.1, on the **Account Added** screen, tap **done**.

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.

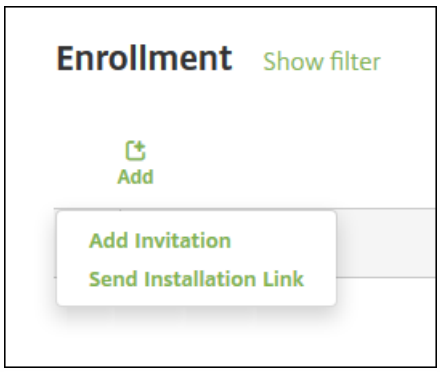
Send an enrollment invitation

In the XenMobile console, you can send an enrollment invitation to users with iOS or Android devices. You can also send an installation link to users with iOS, Android, or Windows devices.

1. In the XenMobile console, click **Manage** > **Enrollment**. The **Enrollment** page appears.



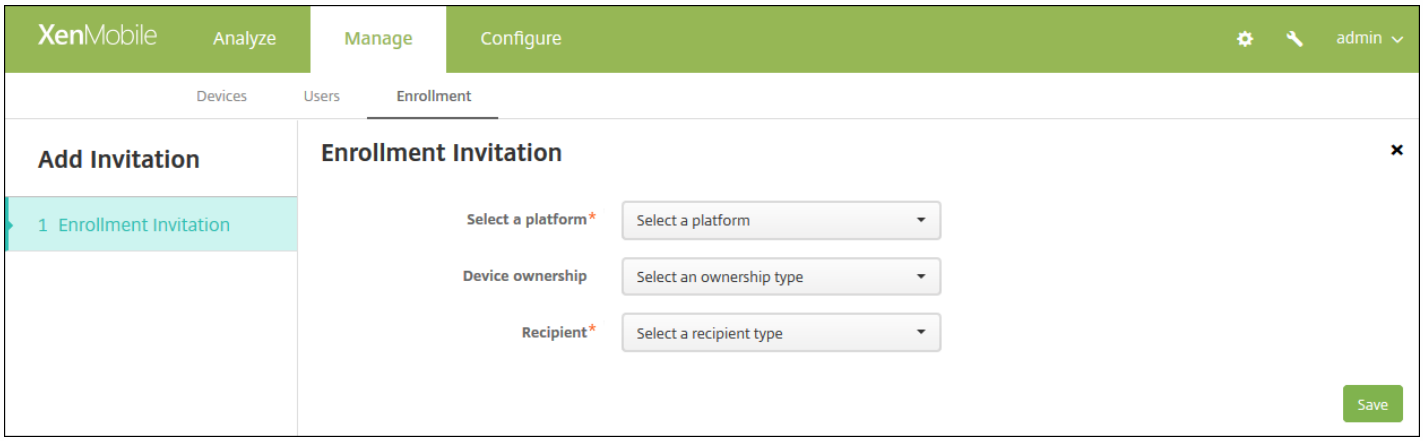
2. Click **Add**. A menu appears listing enrollment options.



- To send an enrollment invitation to a user or group, click **Add Invitation** and then see To send an invitation for the steps to configure this setting.
- To send an enrollment installation link to a list of recipients over SMTP or SMS, click **Send Installation Link** and then see To send an installation link for the steps to configure this setting.

To send an invitation

1. Click **Add Invitation**. The **Enrollment Invitation** screen appears.

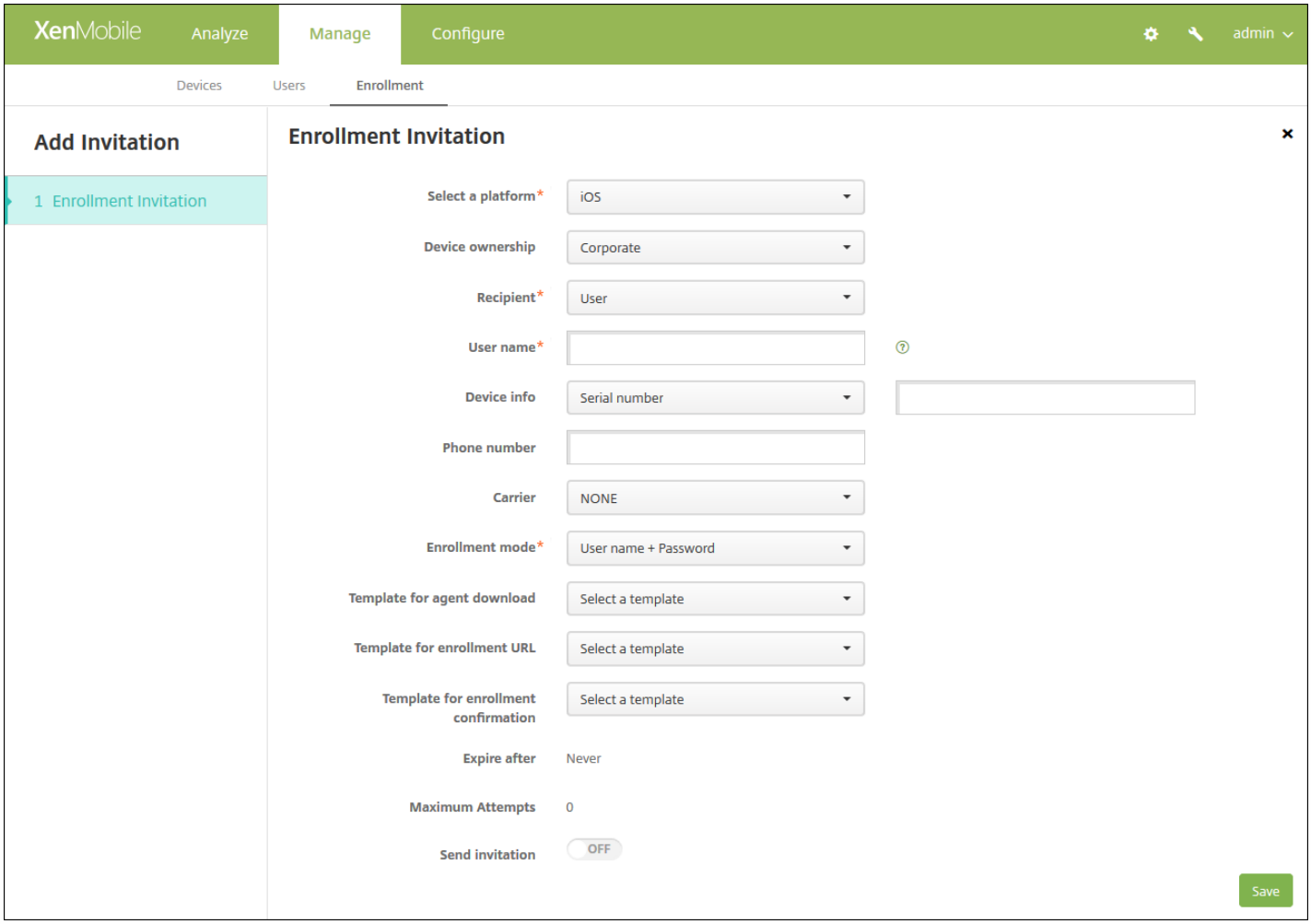


2. Configure these settings:

- **Select a platform**: In the list, click **iOS** or **Android**.
- **Device ownership**: In the list, click **Corporate** or **Employee**.
- **Recipient**: In the list, click **User** or **Group**.

Depending on the recipient you select, you see more settings to configure. For **User** settings, see To send an enrollment invitation to a user; for **Group** settings, see To send an enrollment invitation to a group.

To send an enrollment invitation to a user



1. Configure these **User** settings:

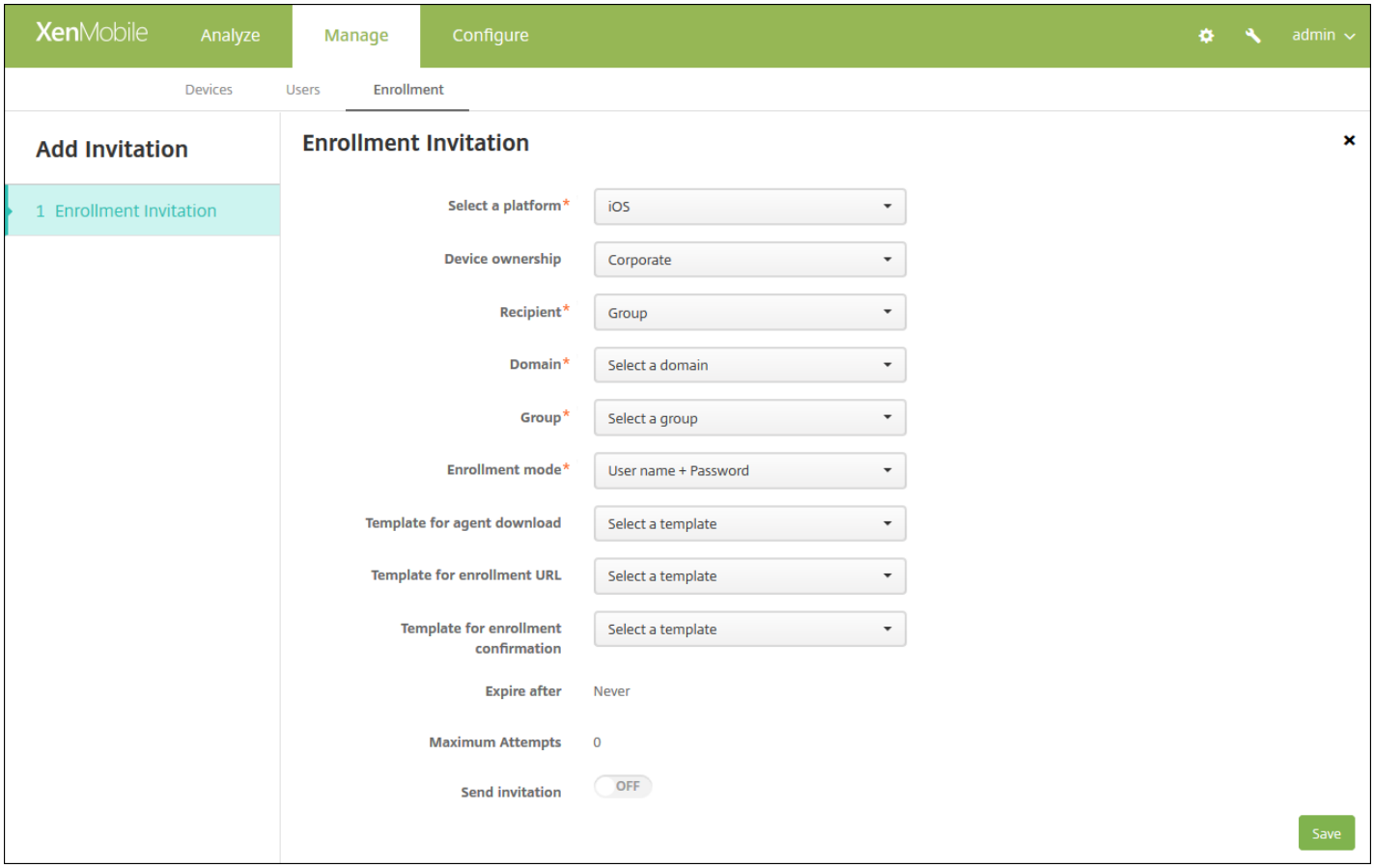
- **User name**: Type a user name. The user must exist in the XenMobile server as a local user or as a user in Active Directory. If the user is local, make sure the user's email property is set so you can send that user notifications. If the user is in Active Directory, make sure LDAP is configured.
- **Device info**: In the list, click **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**: Optionally, type the user's phone number.
- **Carrier**: In the list, click a carrier with which to associate the user's phone number.
- **Enrollment mode**: In the list, click how you want users to enroll. The default is **User name + Password**. Possible options are:
  - High Security
  - Invitation URL
  - Invitation URL + PIN
  - Invitation URL + Password
  - Two Factor
  - User name + PIN

  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**: In the list, click the template to use for enrollment invitation.The choices for this option are based on the platform type. For example, **iOS Download Link** appears as an option if you selected **iOS** as a platform.
- **Template for enrollment URL**: In the list, click **Enrollment Invitation**.
- **Template for enrollment confirmation**: In the list, click **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, or click **OFF** to only add the invitation to the table on the **Enrollment** page.

2. Click **Save and Send** if you enabled **Send invitation**; otherwise, click **Save**. The invitation appears in the table on the **Enrollment** page.

To send an enrollment invitation to a group



1. Configure these settings:

- **Domain**: In the list, click the domain from which to select the group.
- **Group**: In the list, click the group to receive the invitation.
- **Enrollment mode**: In the list, click how you want users in the group to enroll. The default is **User name + Password**. Possible options are:

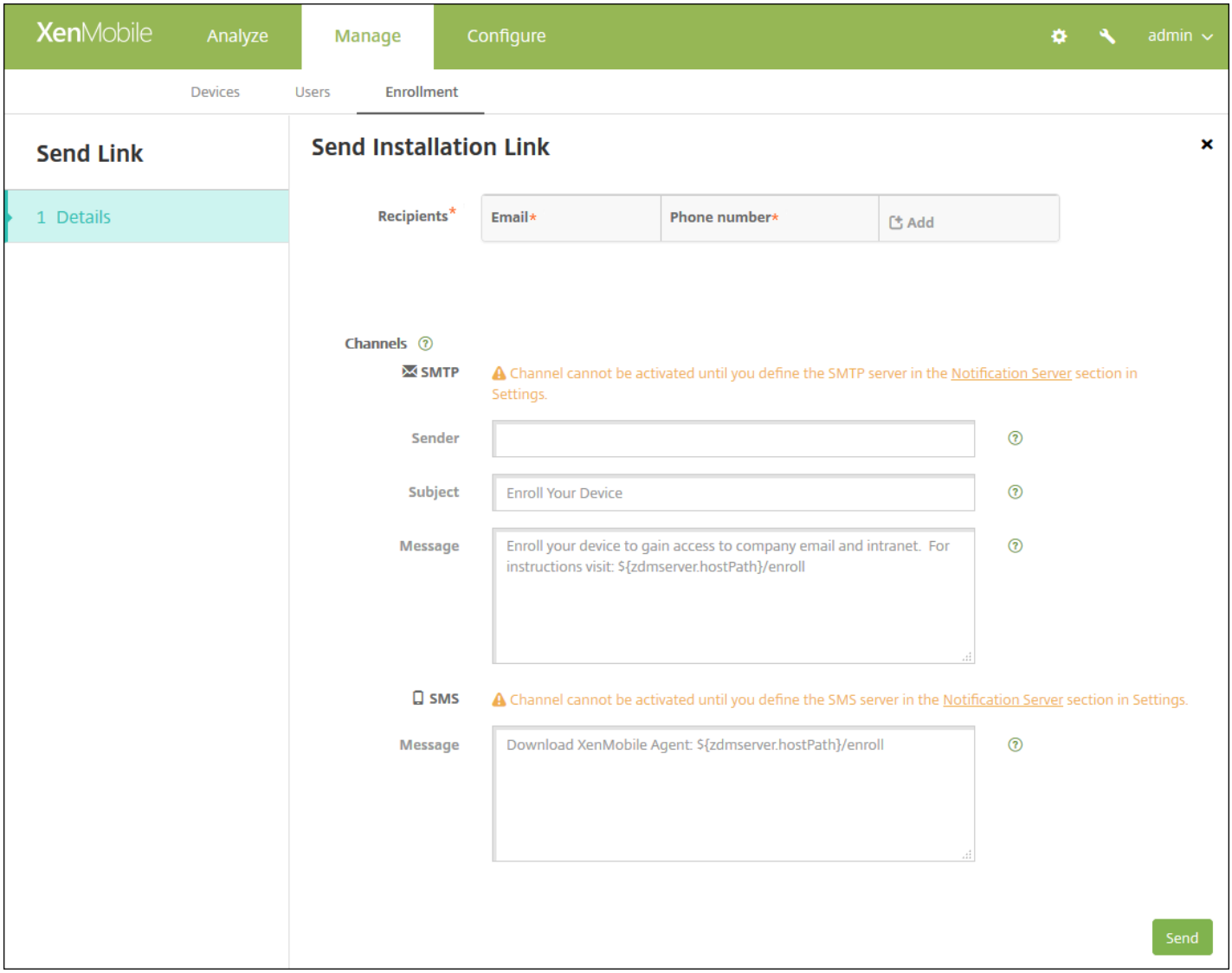
- High Security
- Invitation URL
- Invitation URL + PIN
- Invitation URL + Password
- Two Factor
- User name + PIN

  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**: In the list, click the template to use for enrollment invitation.The choices for this option are based on the platform type. For example, **iOS Download Link** appears as an option if you selected **iOS** as a platform.
- **Template for enrollment URL**: In the list, click **Enrollment Invitation**.
- **Template for enrollment confirmation**: In the list, click **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, or click **OFF** to only add the invitation to the table on the **Enrollment** page.

2. Click **Save and Send** if you enabled **Send invitation**; otherwise, click **Save**. The invitation appears in the table on the **Enrollment** page.

To send an installation link



Before you can send an enrollment installation link, you must configure channels (SMTP or SMS) on the notification server from the **Settings** page. For details, see Notifications.

1. Configure these settings:

- **Recipient**: For each recipient that you want to add, click Add and do the following:
  - **Email**: Type the recipient's email address. This field is required.
  - **Phone number**: Type the recipient's phone number. This field is required.
  - Click **Save**.

    Note: To delete an existing recipient, 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 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. Make any changes to 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 leverages SAMAccountName, after users receive the invitation and click the link, they must edit the user name to complete the authentication. For example, they need to remove domainname in SAMAccountName@domainname.com.

Device enrollment limit

Oct 05, 2016

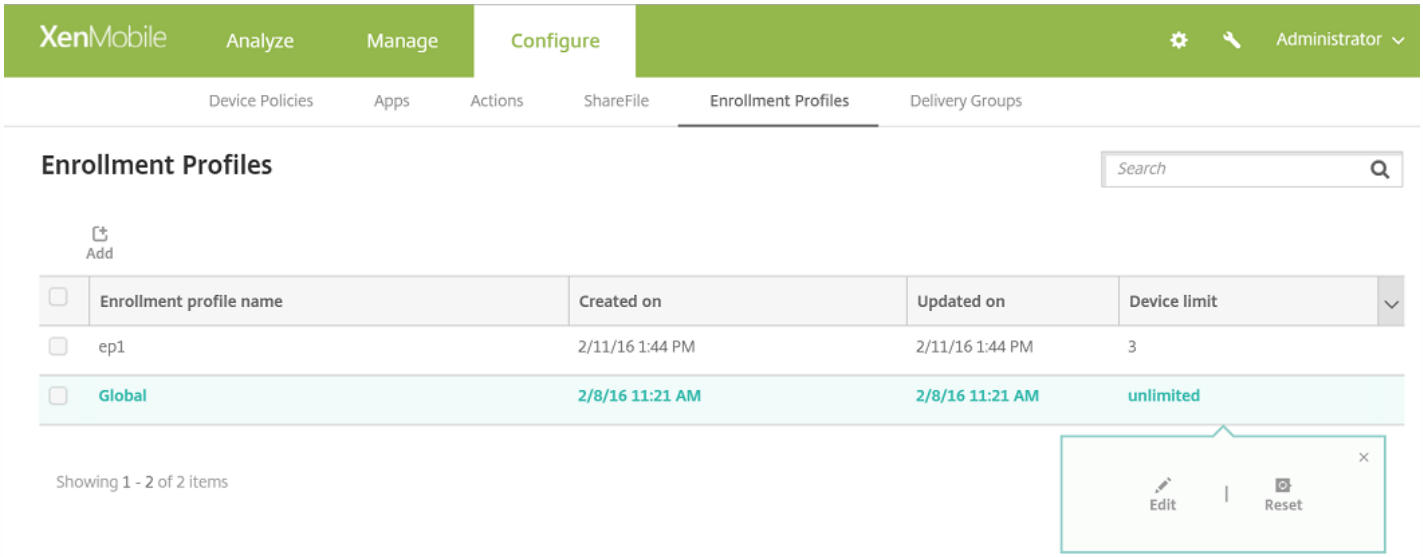
You can limit the number of devices that a user can enroll under **Configure > Enrollment Profiles** in the XenMobile console, in ENT, MDM, and MAM server modes. Limitations can apply globally or per delivery group. You can create multiple enrollment profiles and associate them with different delivery groups.

If you do not set a limit, users can enroll an unlimited number of devices. This feature is supported only on iOS and Android devices.

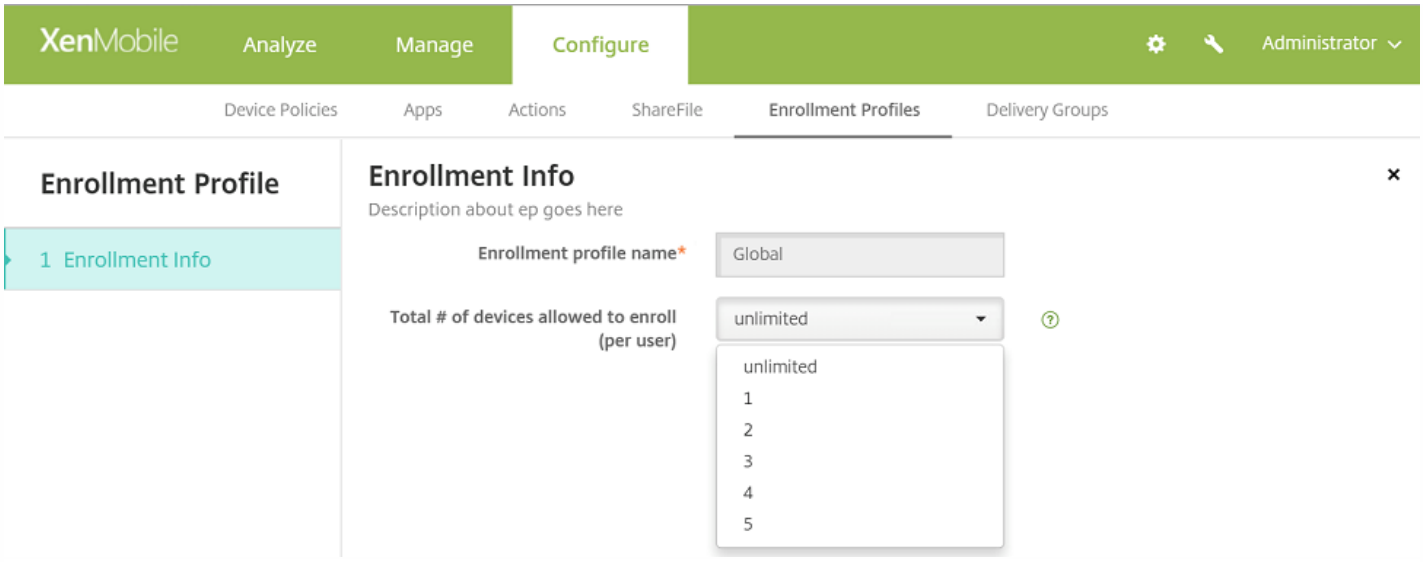
To configure a global device enrollment limit

1. Go to **Configure > Enrollment Profiles**.

2. Click **Global** and select **Edit**.



The **Enrollment Info** screen appears with **Global** automatically filled in as the profile name. From here, you can select the total number of devices users are allowed to enroll. This limitation will apply to all XenMobile enrollees.

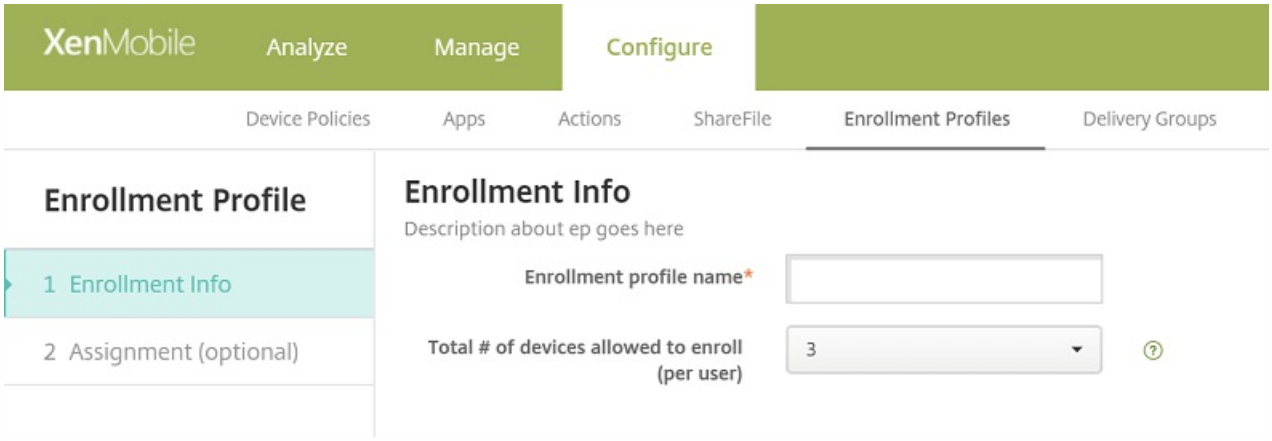


To configure a delivery group device enrollment limit

1. Go to **Configure > Enrollment Profiles > Add**.

   The **Enrollment Info** screen appears.

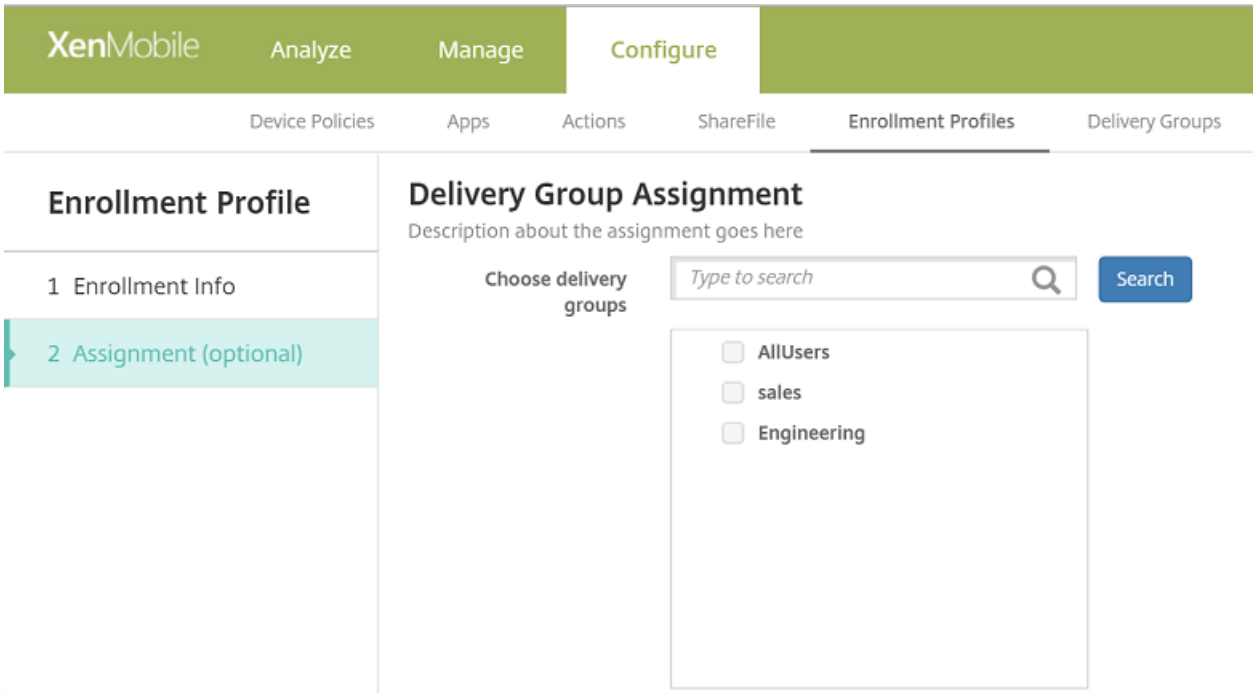
2. Enter a name for the new enrollment profile and then select the number of devices that members with this profile are allowed to enroll.



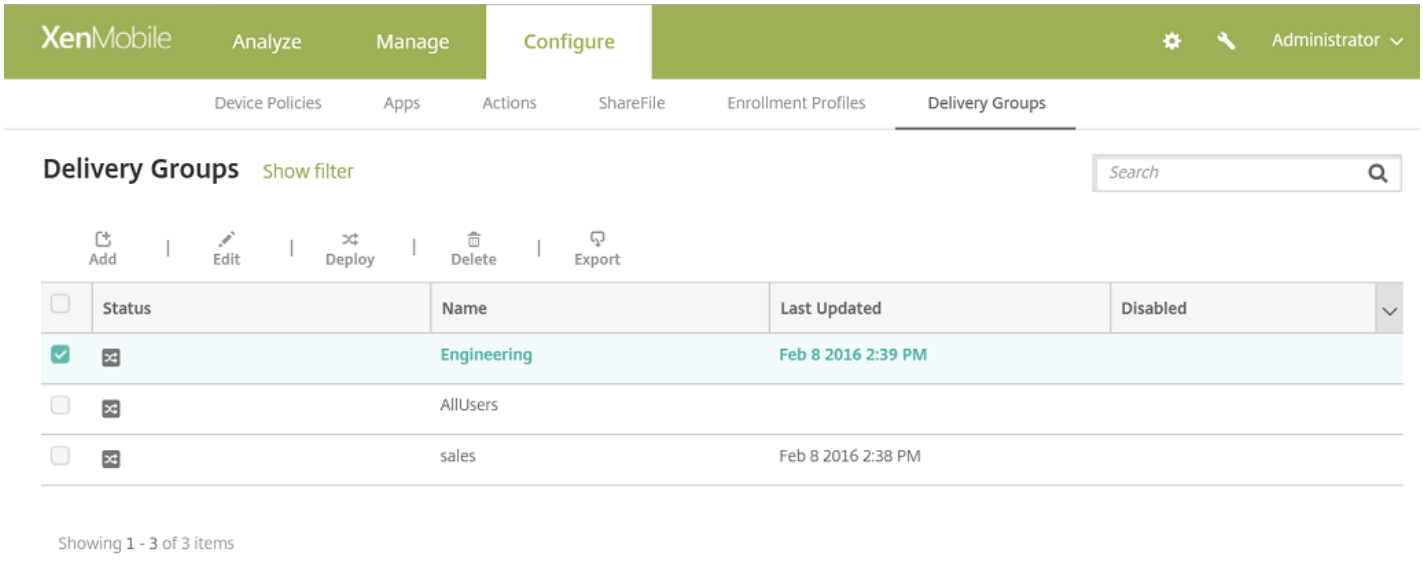
3. Click **Next**.

   The **Delivery Group Assignment** screen appears.

4. Select the delivery groups to which the device enrollment limit will apply and then click **Save**.

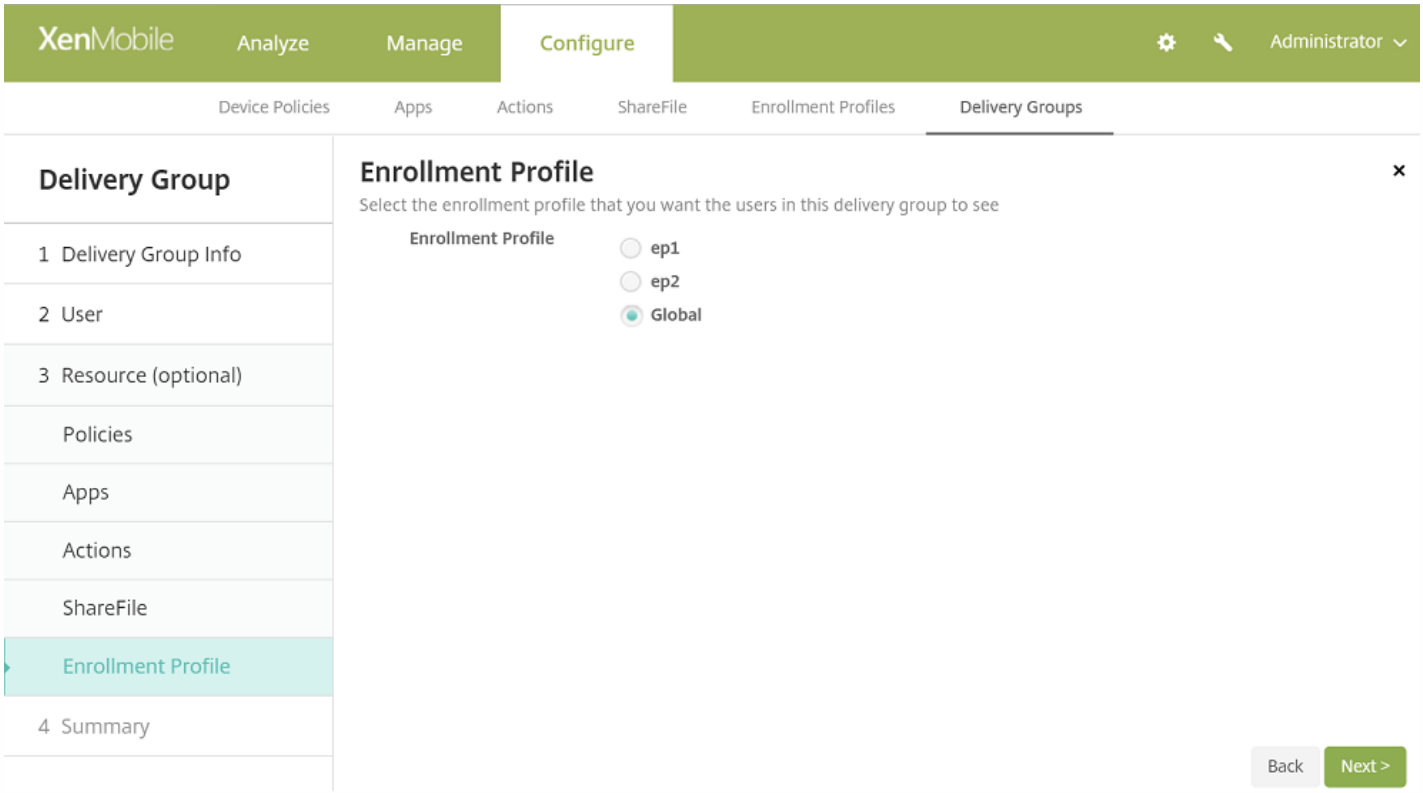


If later you want to change a delivery group's enrollment profile, go to **Configure > Delivery Groups**. Select the group you want and click **Edit**.



The **Enrollment Profile** screen appears.

5. From this screen, select the enrollment profile that you want to apply to this delivery group and then click **Next** to view and save your changes.



User Experience with a Device Enrollment Limit

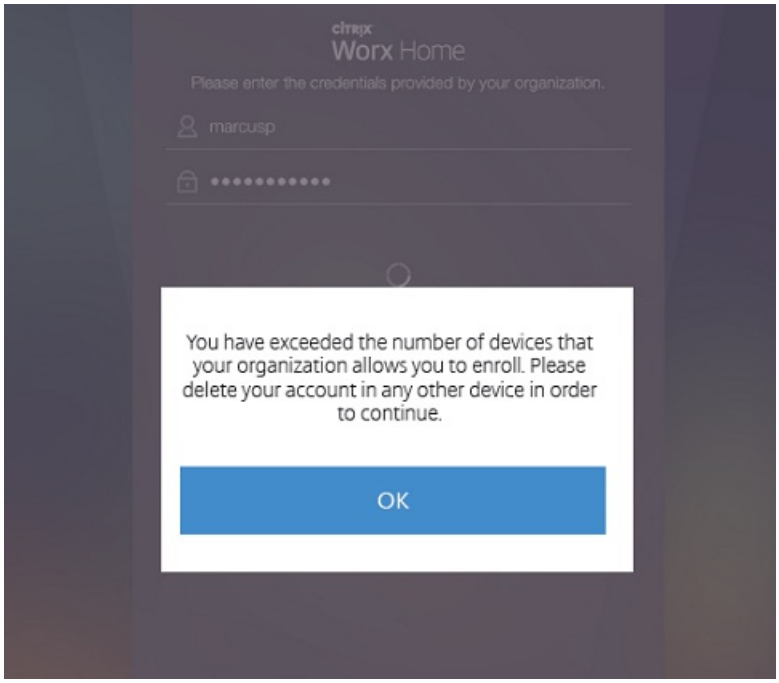
When you set the device enrollment limit and users try to enroll a new device, they follow these steps:

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 appears that tells the user that the device registration is exceeded and that they should contact an administrator.



The Secure Hub enrollment screen appears again.

Shared devices

Jan 03, 2017

XenMobile lets you configure devices that can be shared by multiple users. 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:

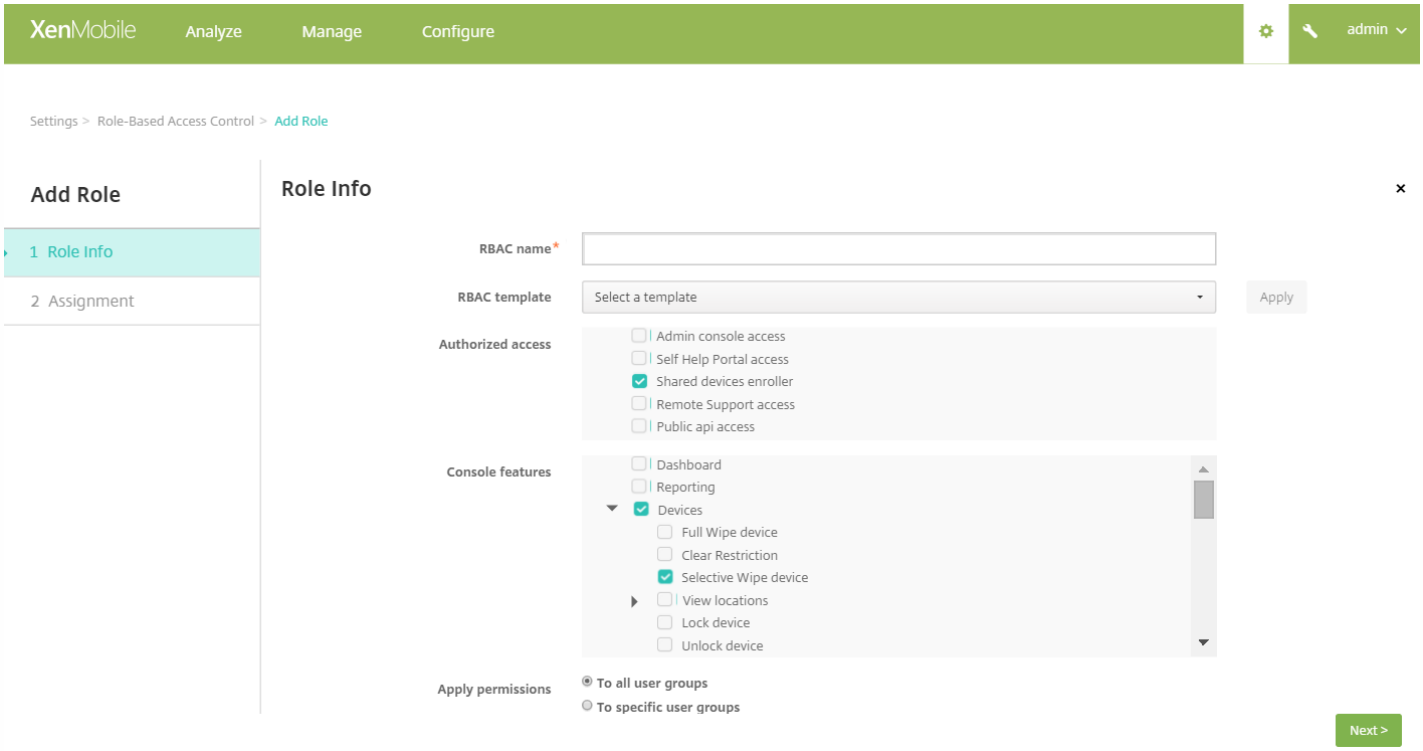
- iOS 9 and 10
- Android M
- Android 5.x
- Android 4.4.x
- Android 4.0.x (MDM-only mode)

Configuring a Shared Device

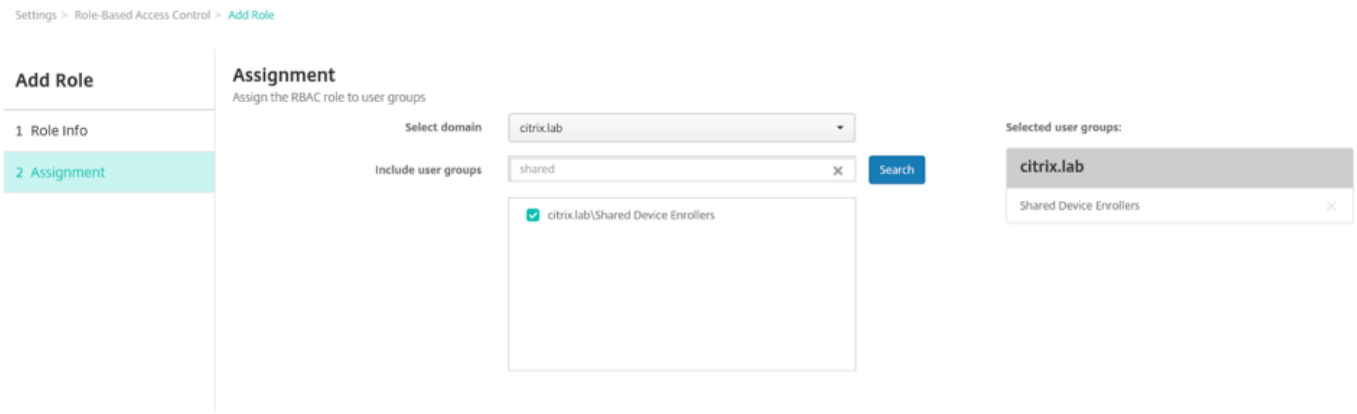
Follow these steps to configure a shared device.

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.

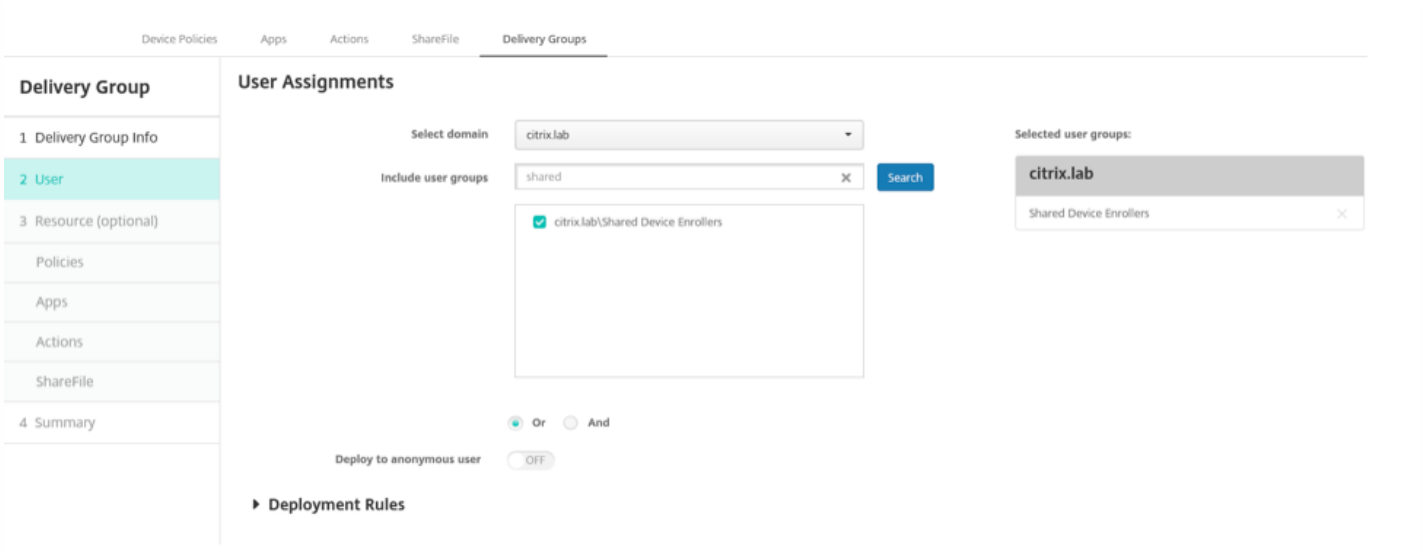
   For **Apply Permissions**, keep the default setting, **To all user groups**, or assign permissions to specific Active Directory user groups with the **To specific user groups**.



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

-
-
-
-
-

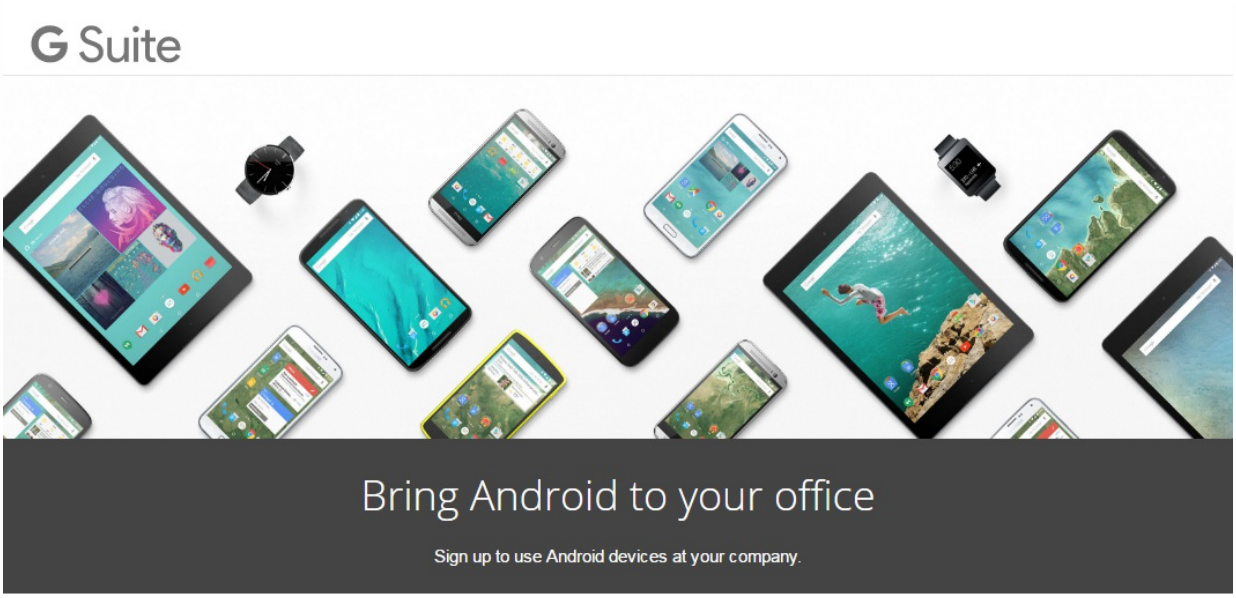
-
-
-
-
-

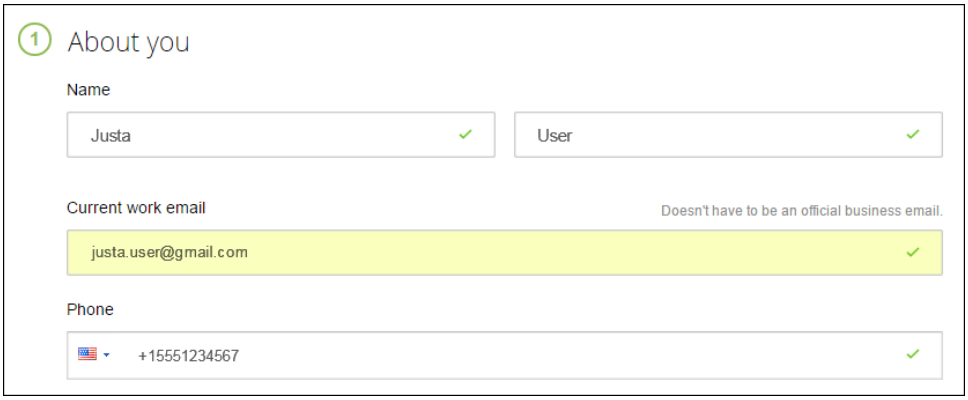
-
-
-
-

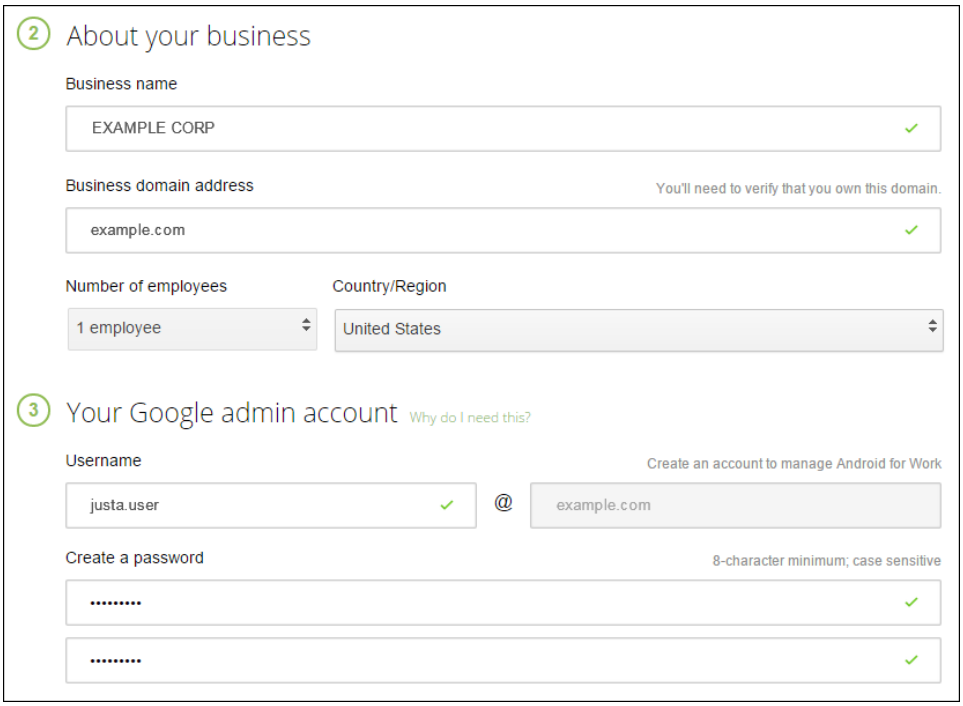
Android at Work Prerequisites

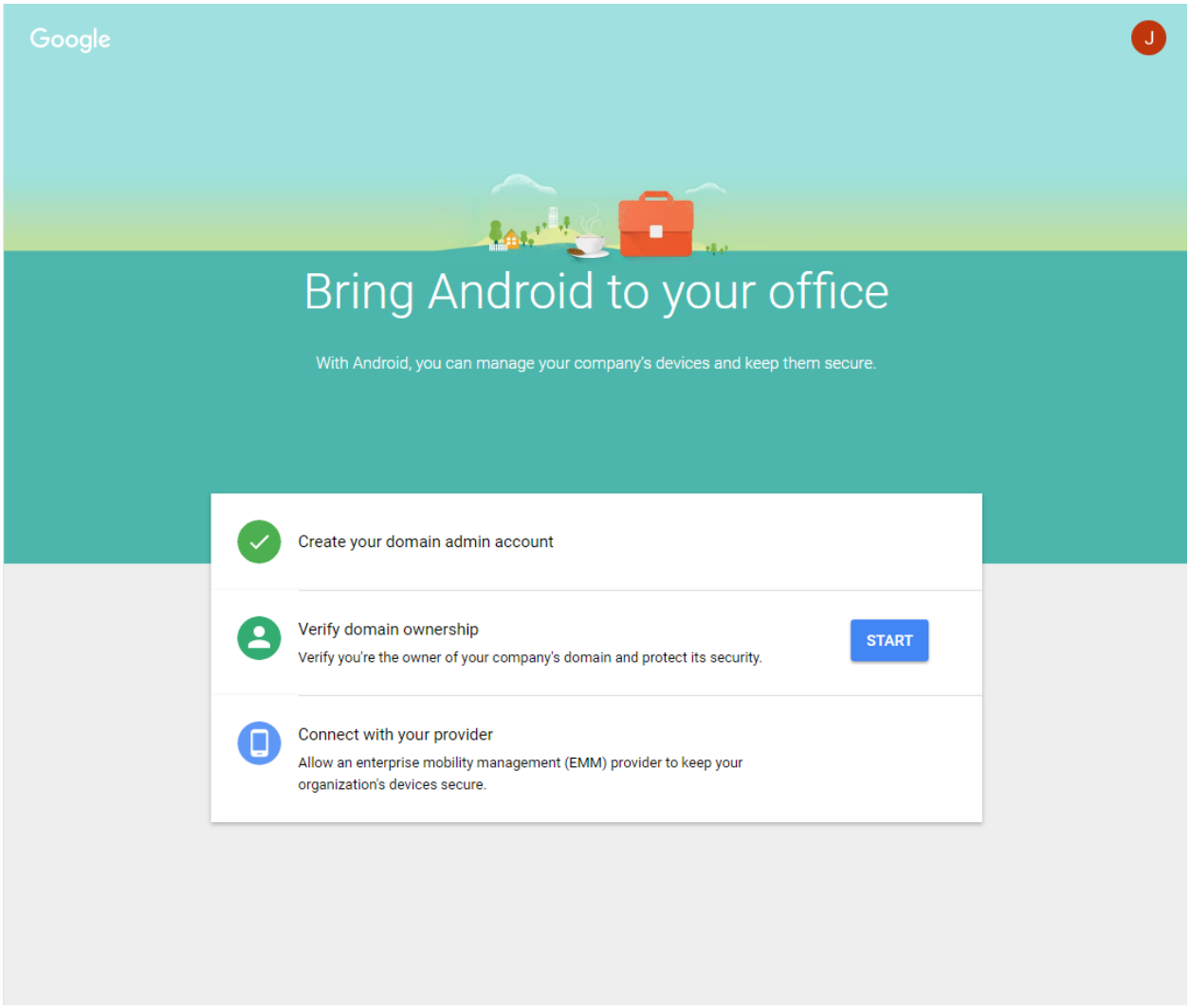
-
-
-
-
-
-

-
-
-

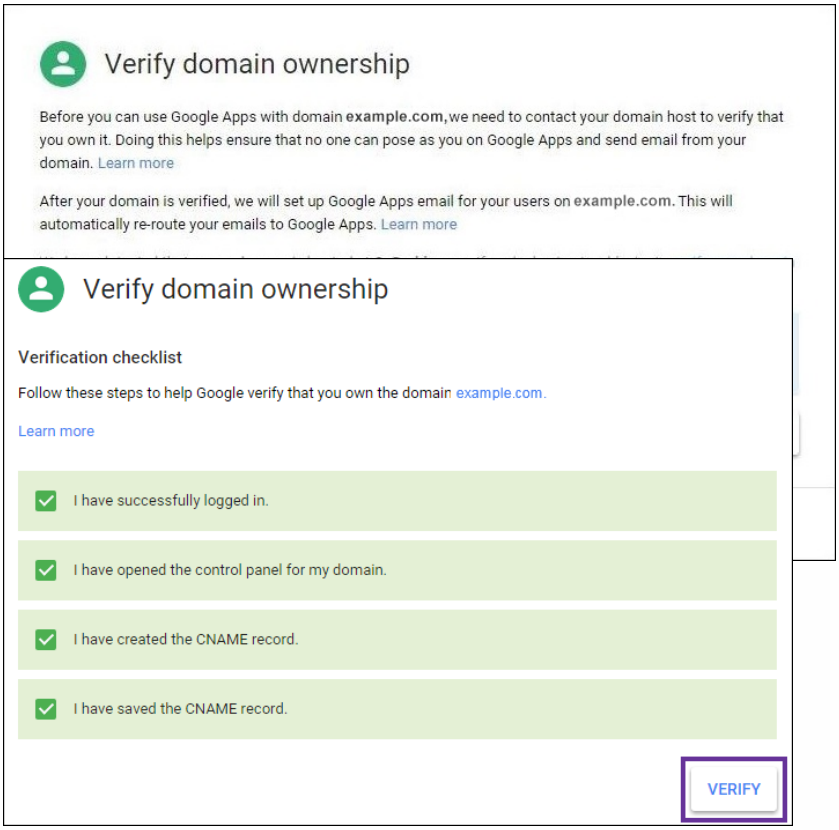


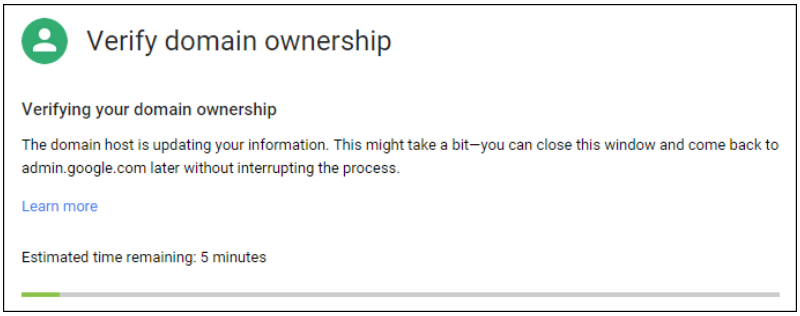


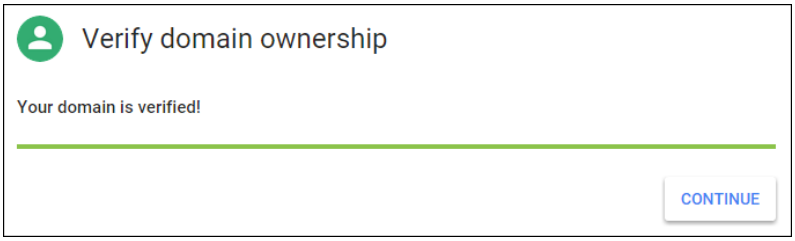


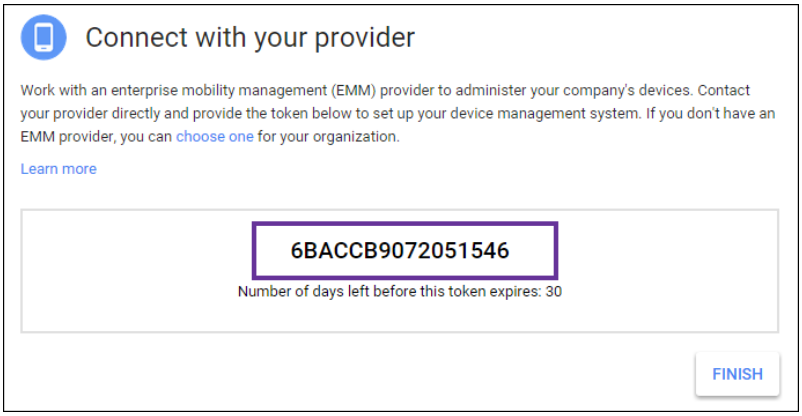


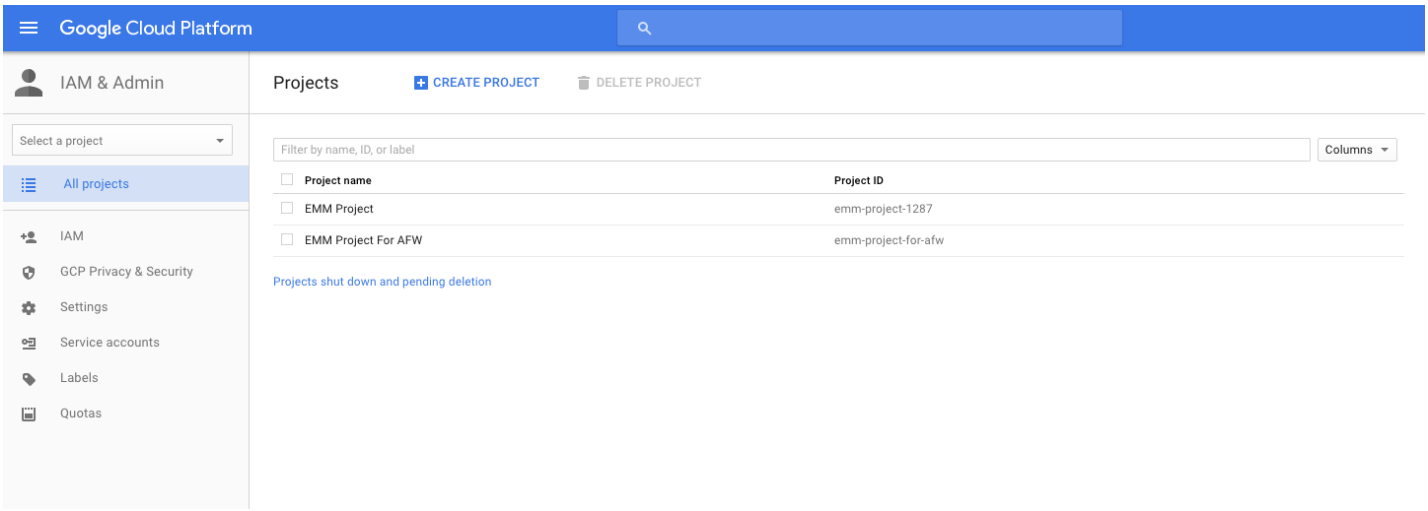
-
-
-

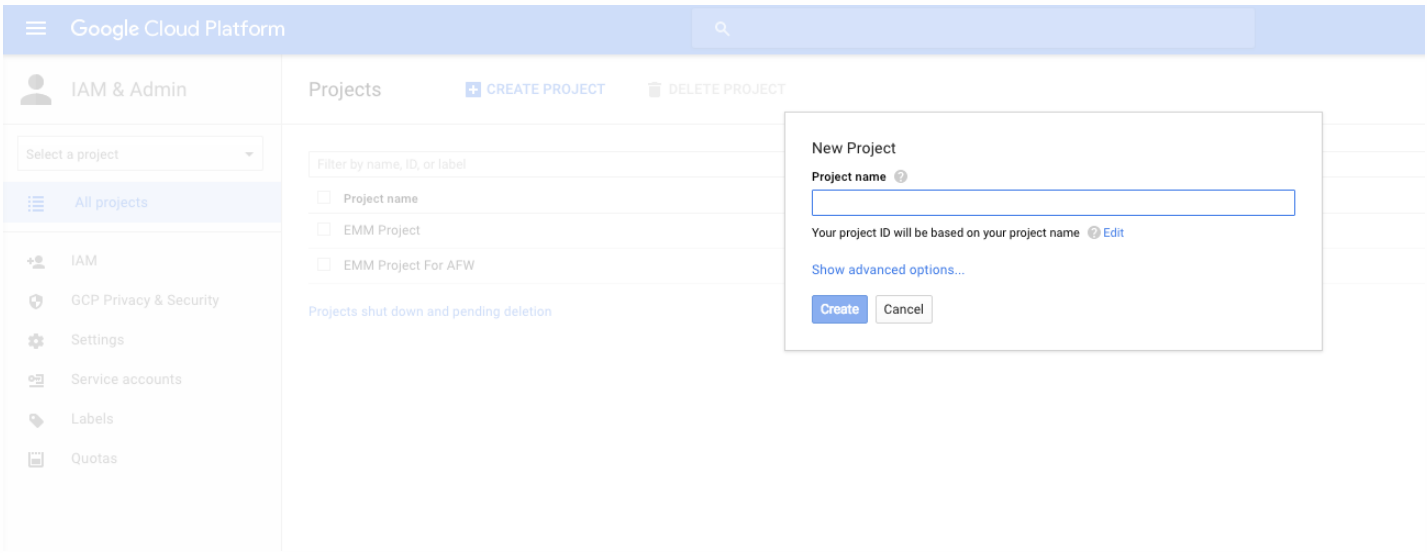


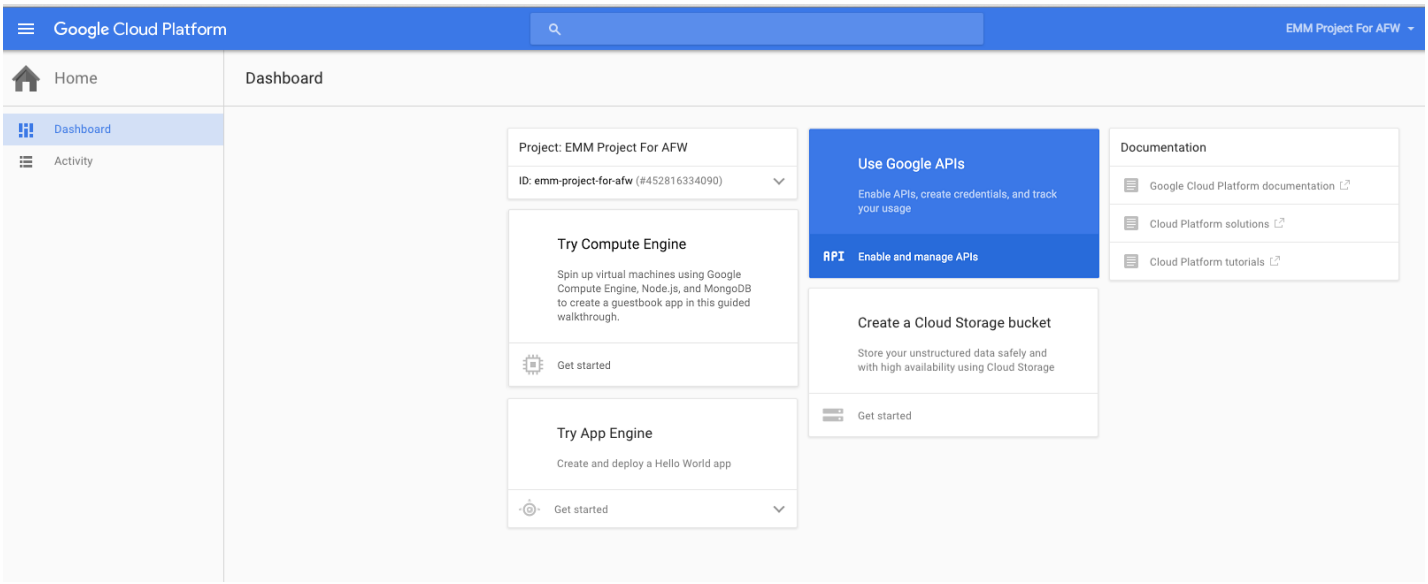


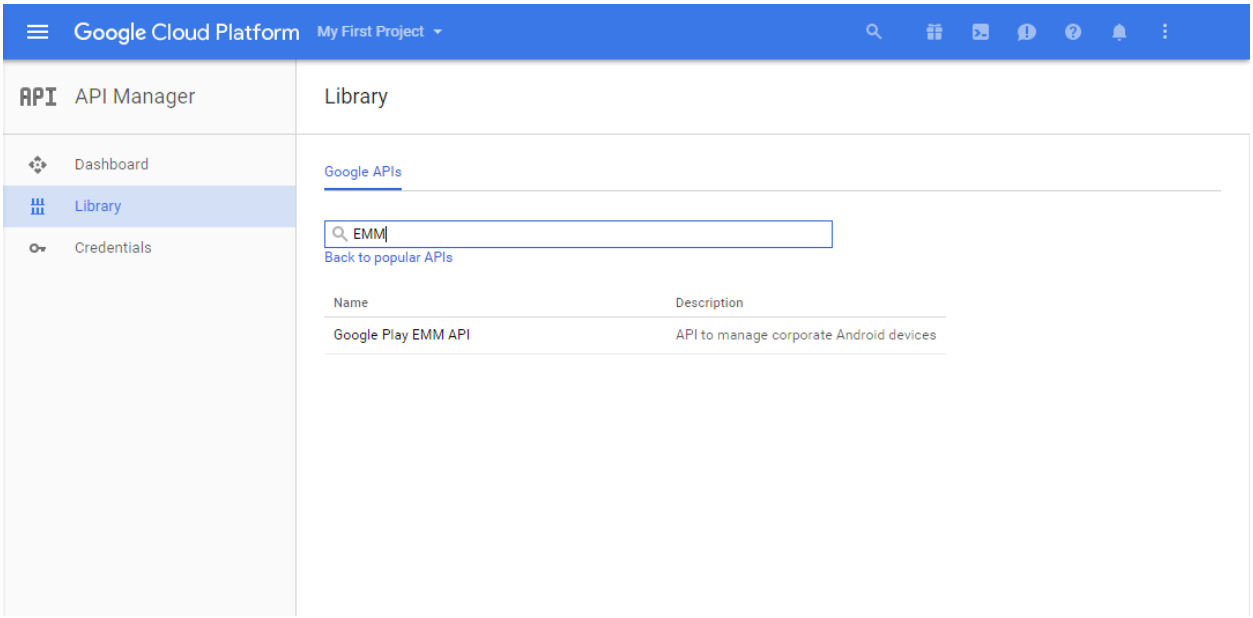


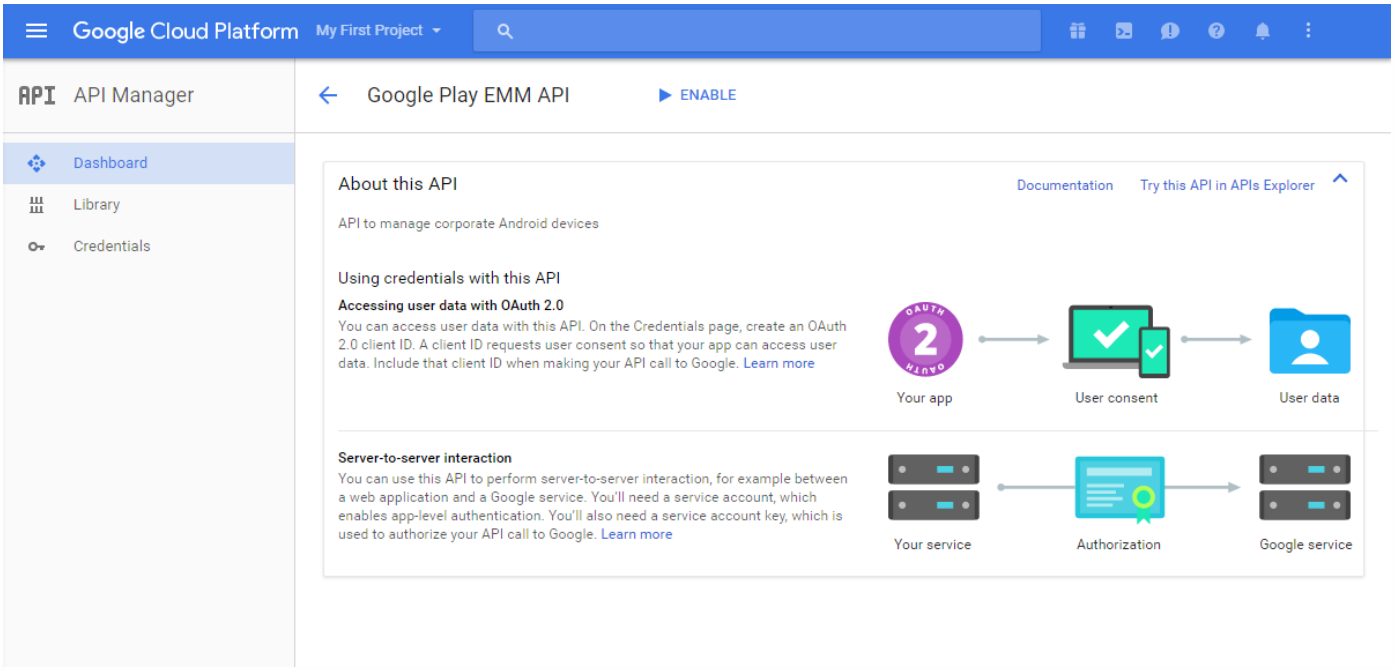


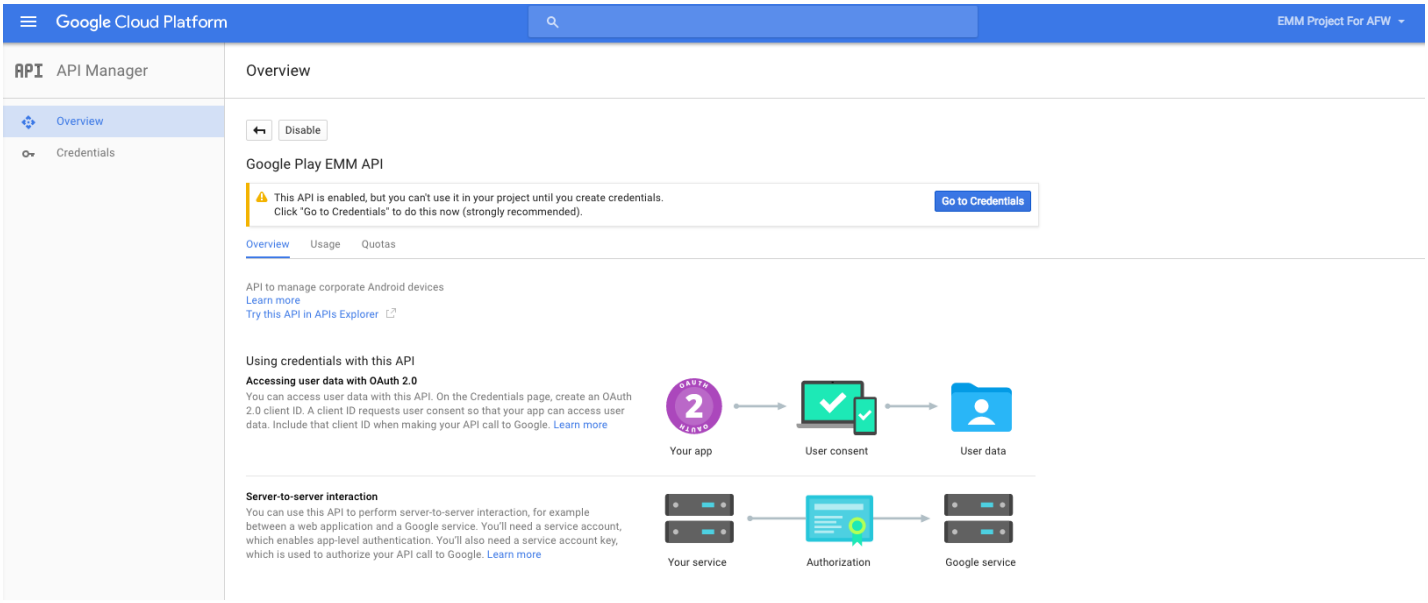


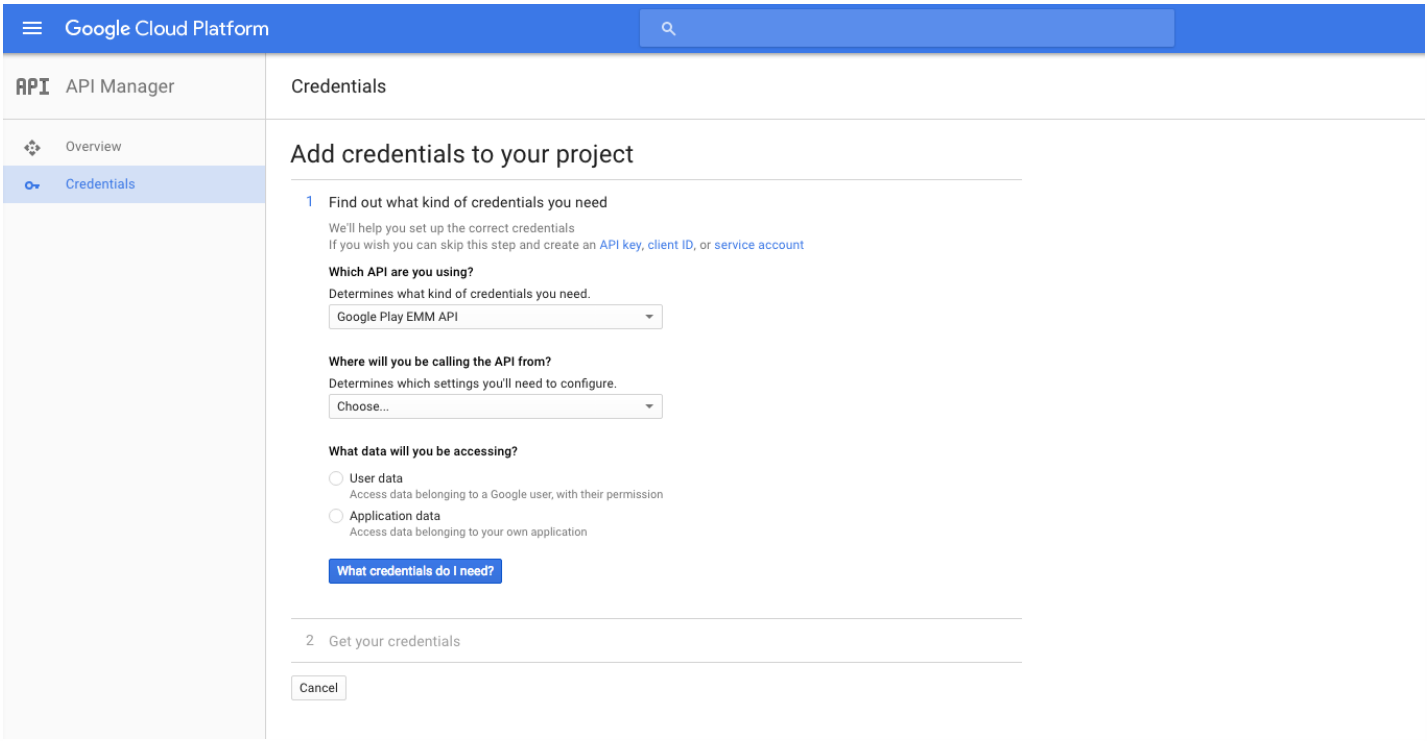


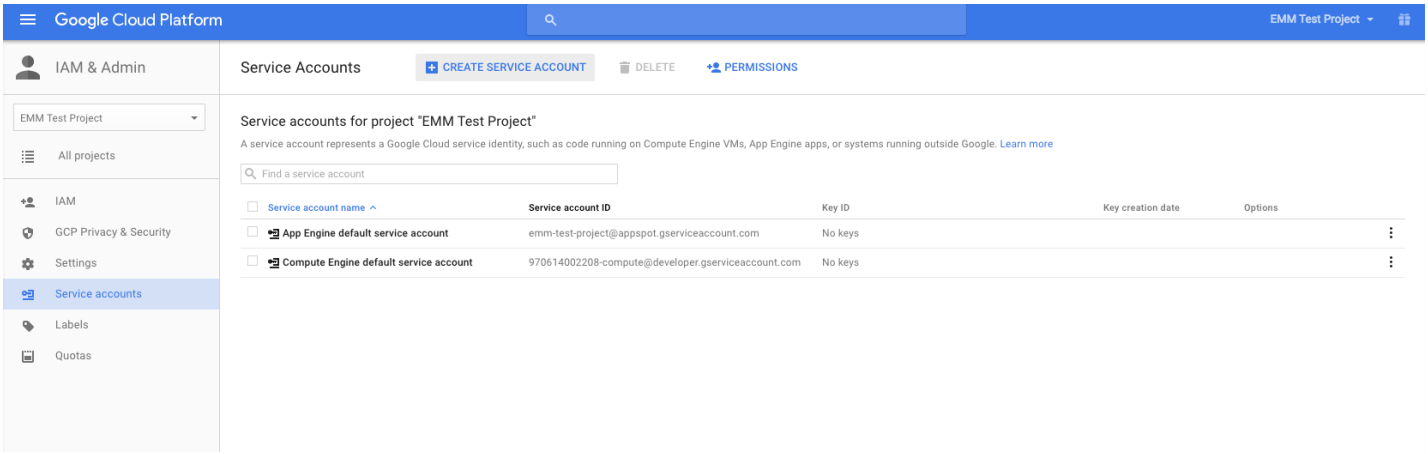


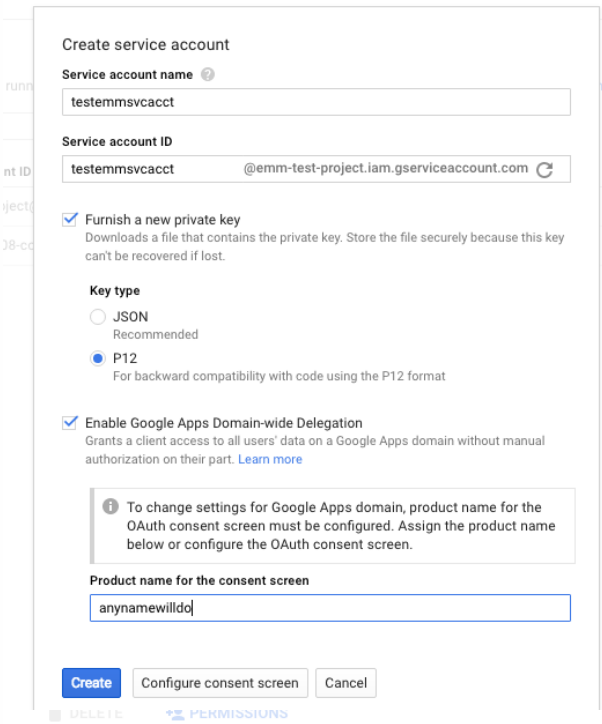


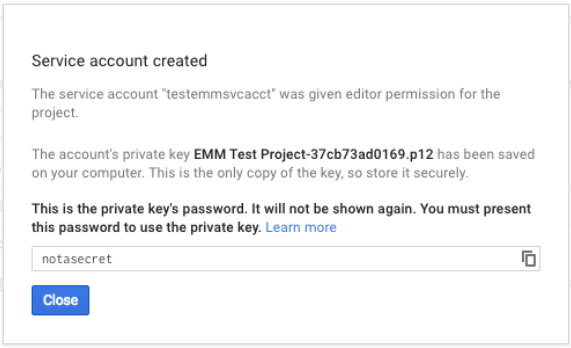


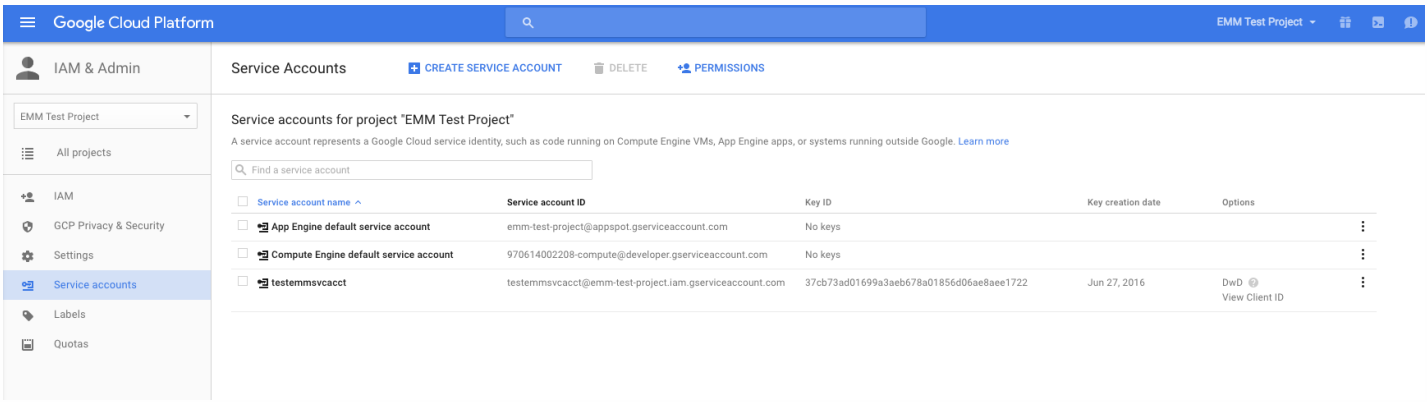


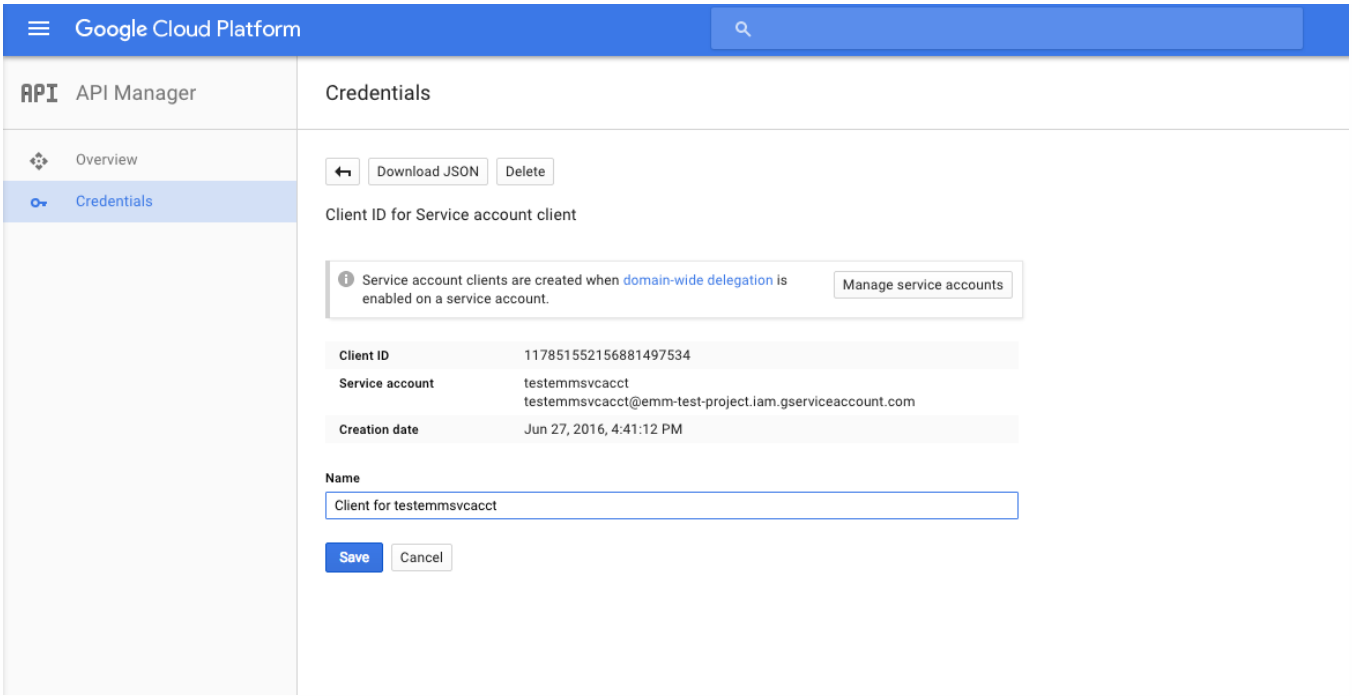


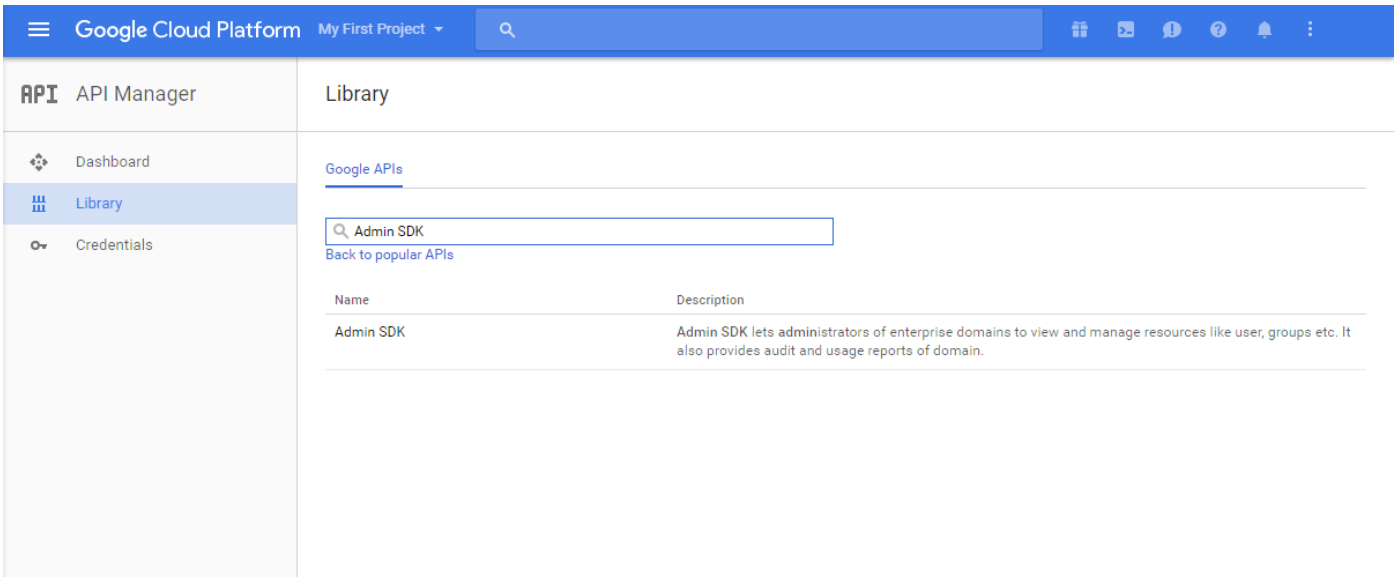


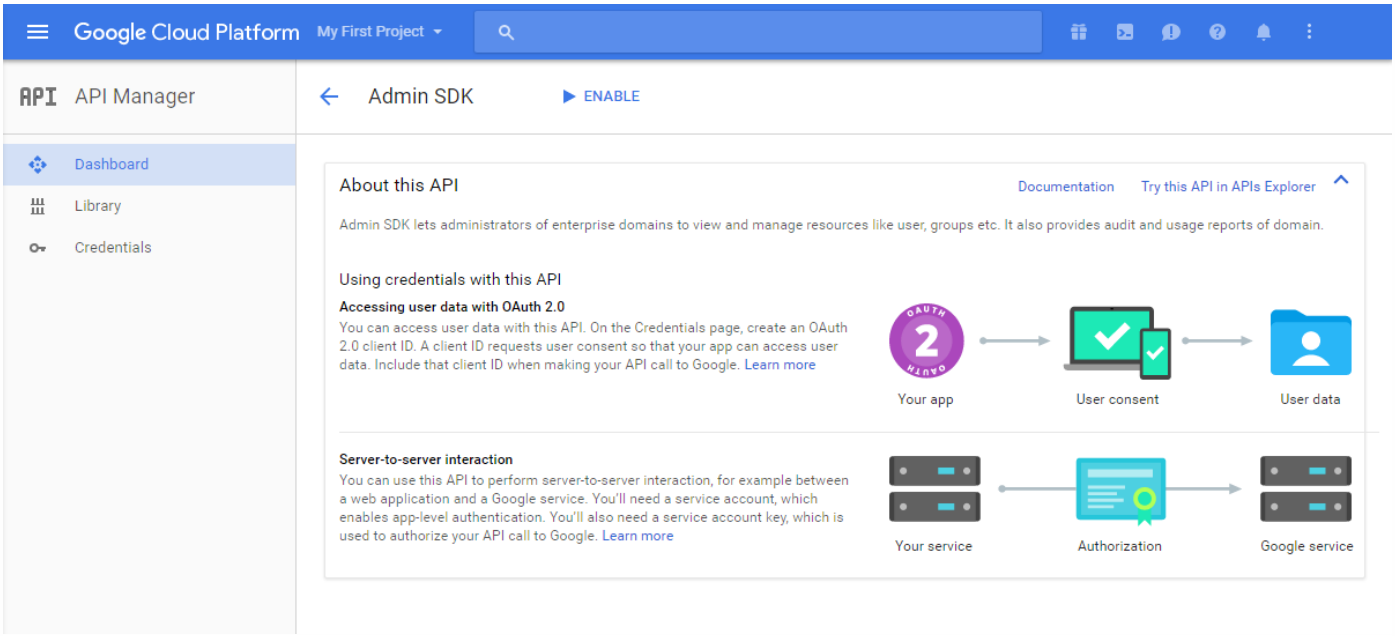


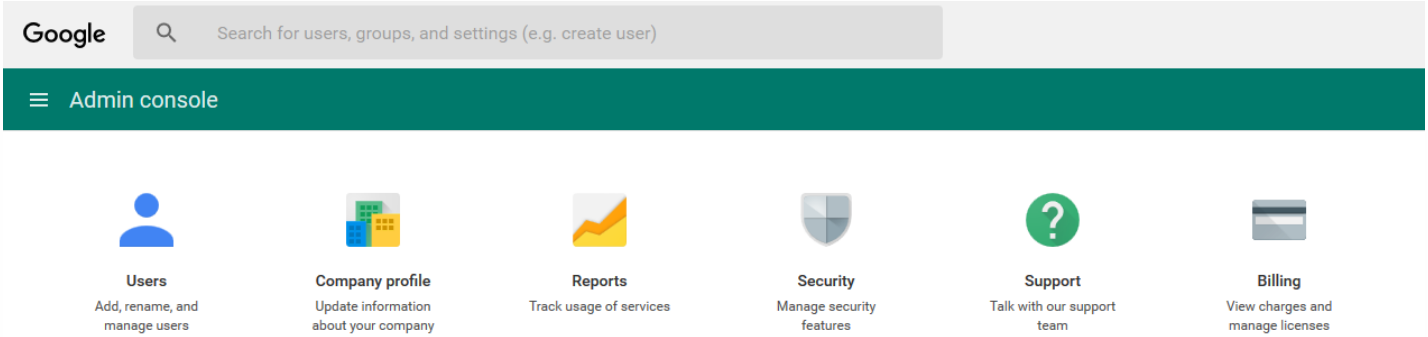


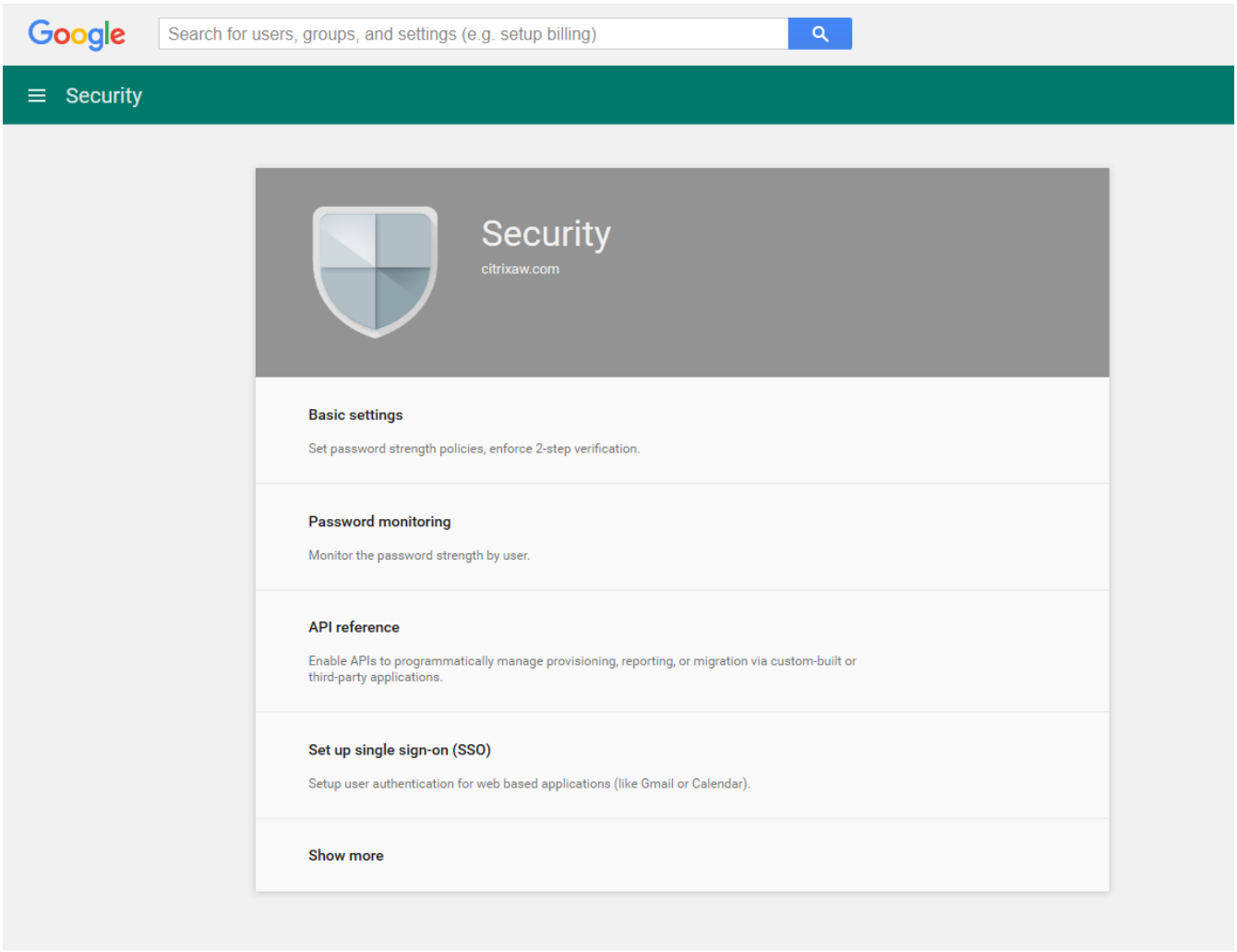


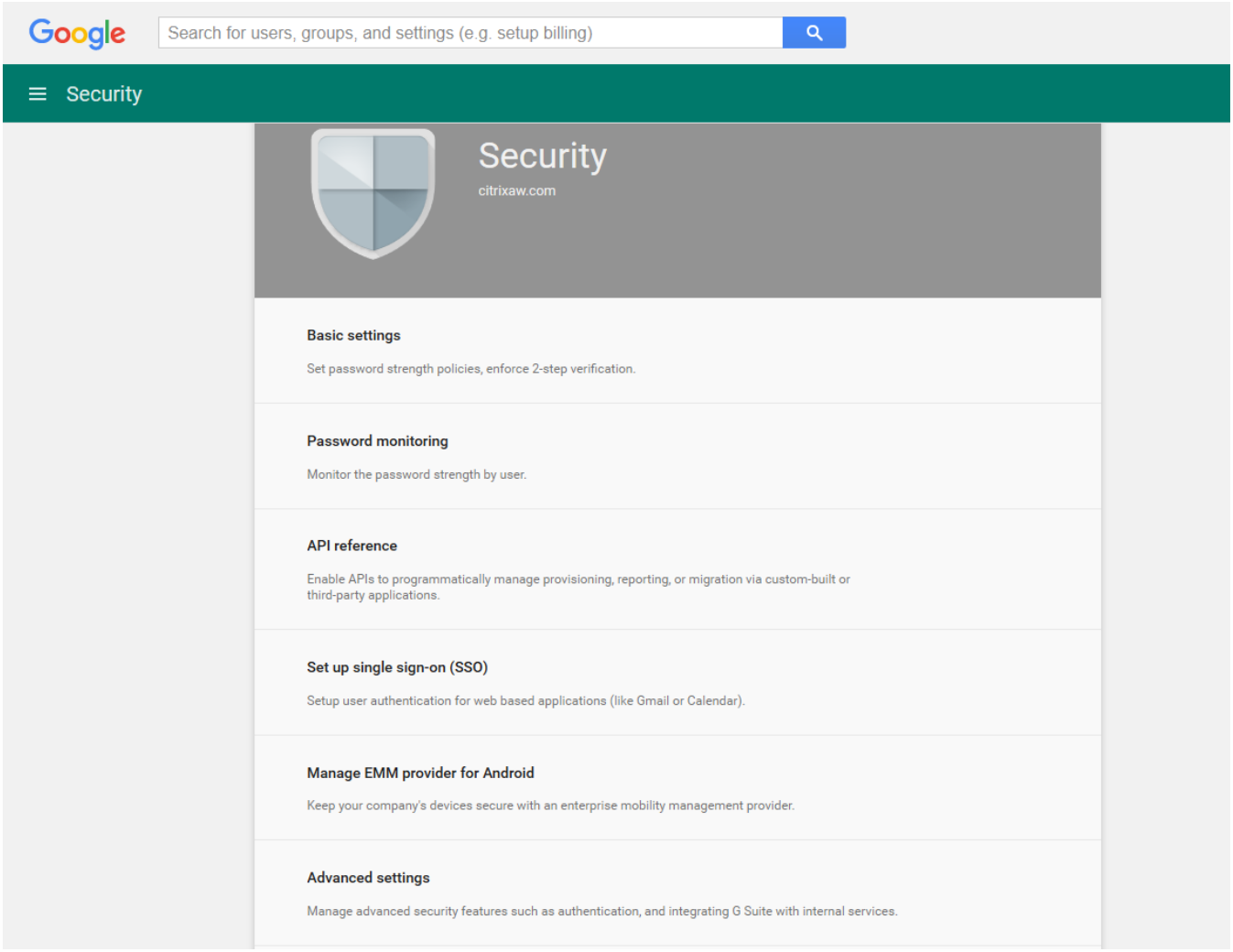


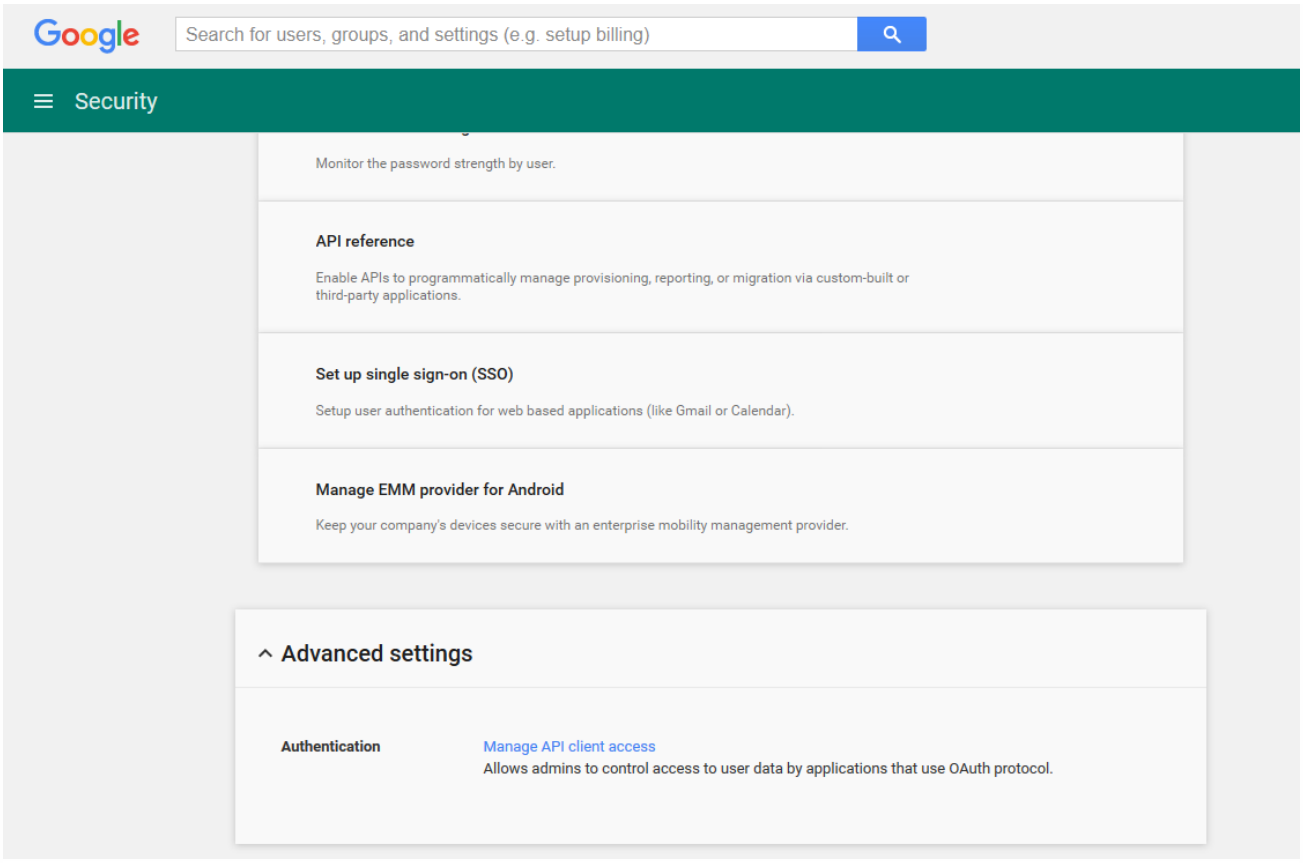


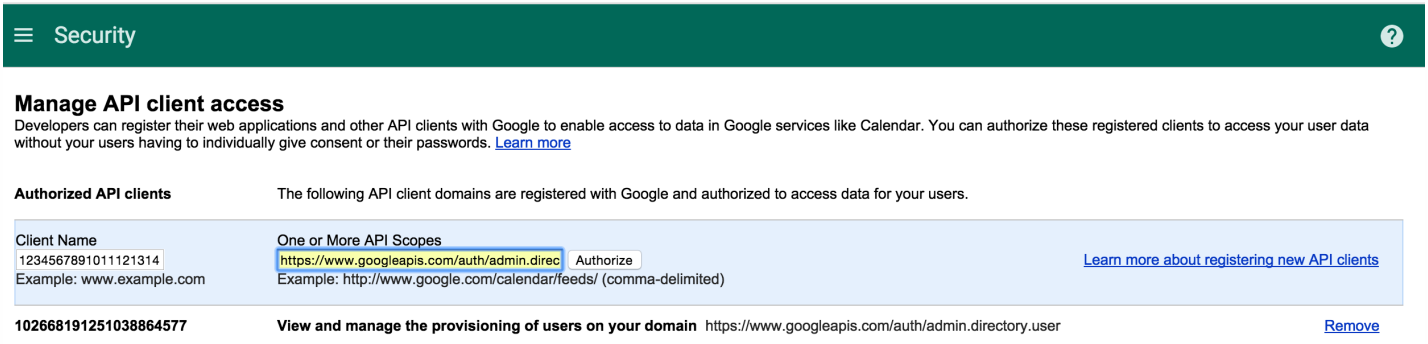




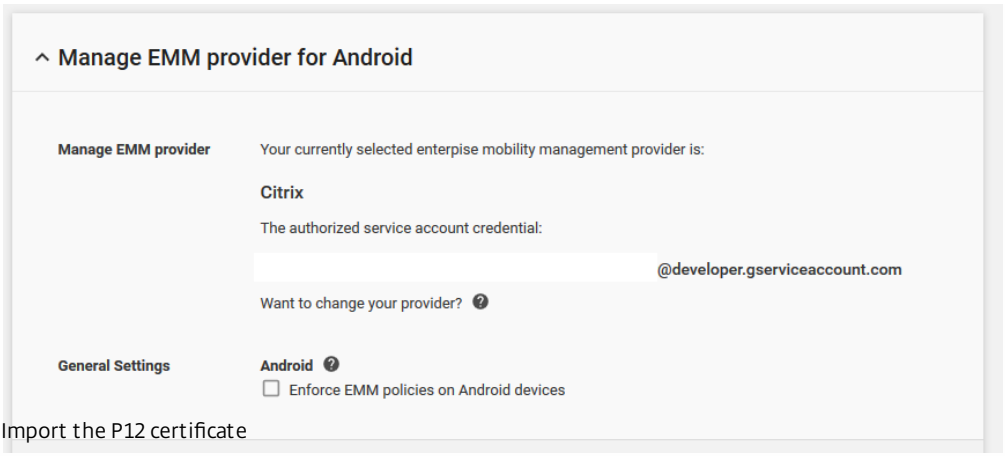




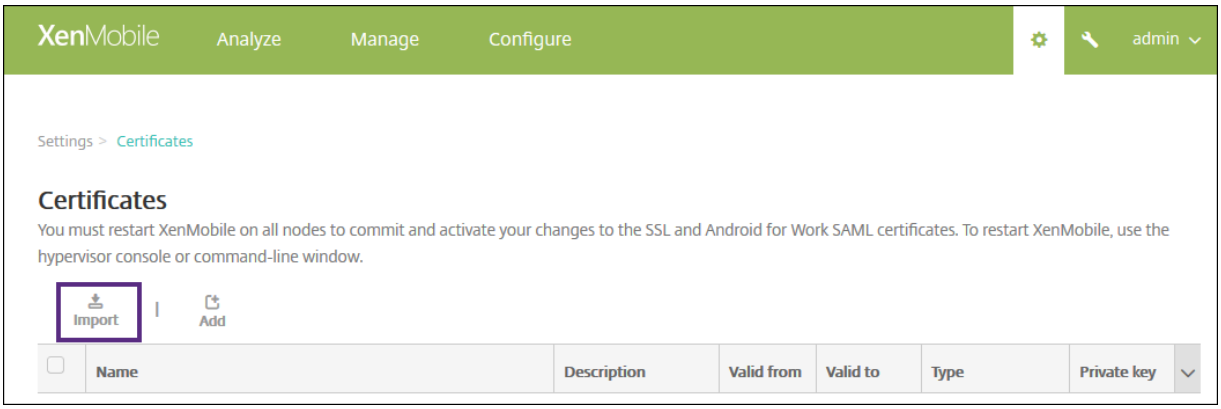


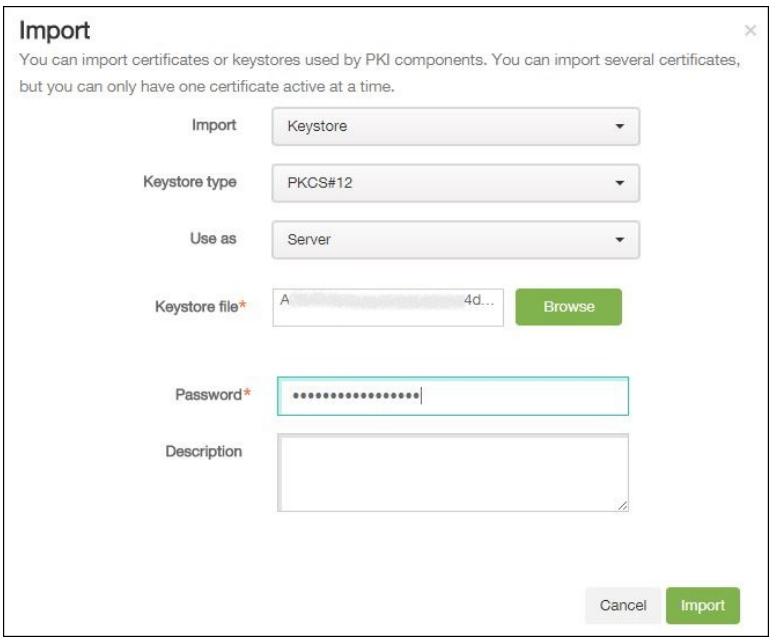


Binding to EMM



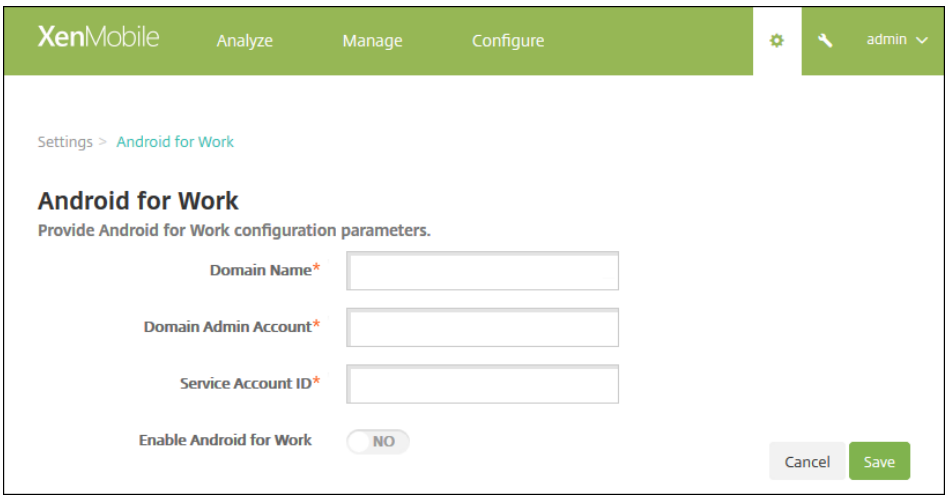
Import the P12 certificate





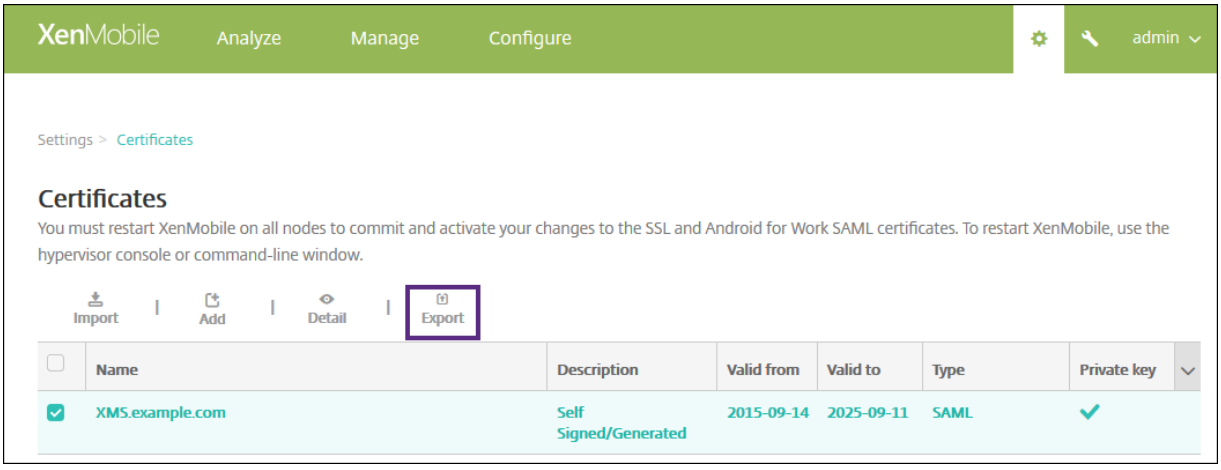
-
-
-
-
-
-

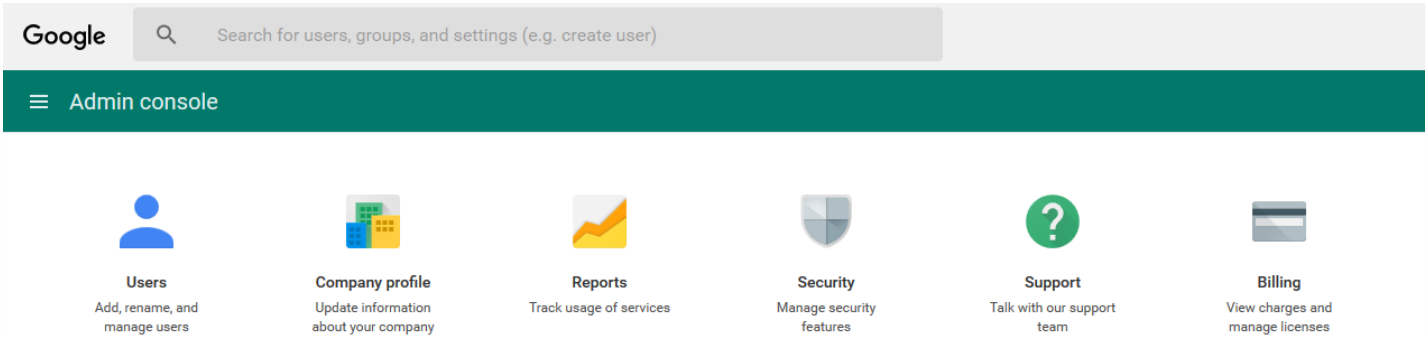
Set up Android at Work server settings

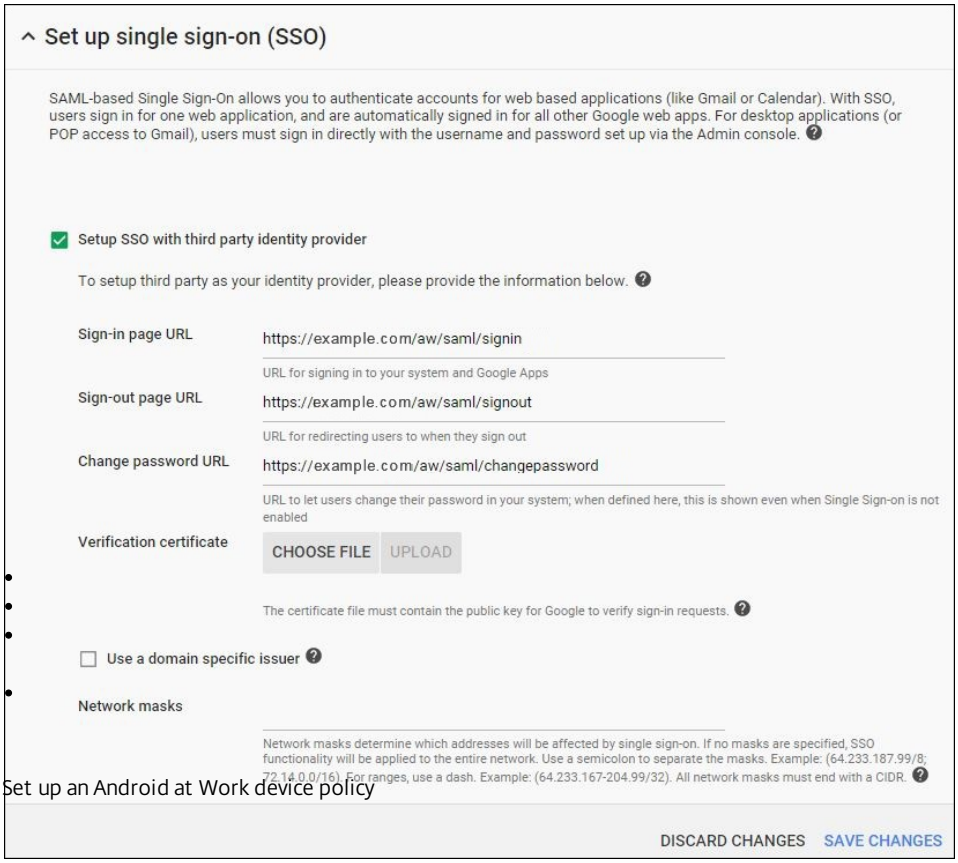


-
-
-
-

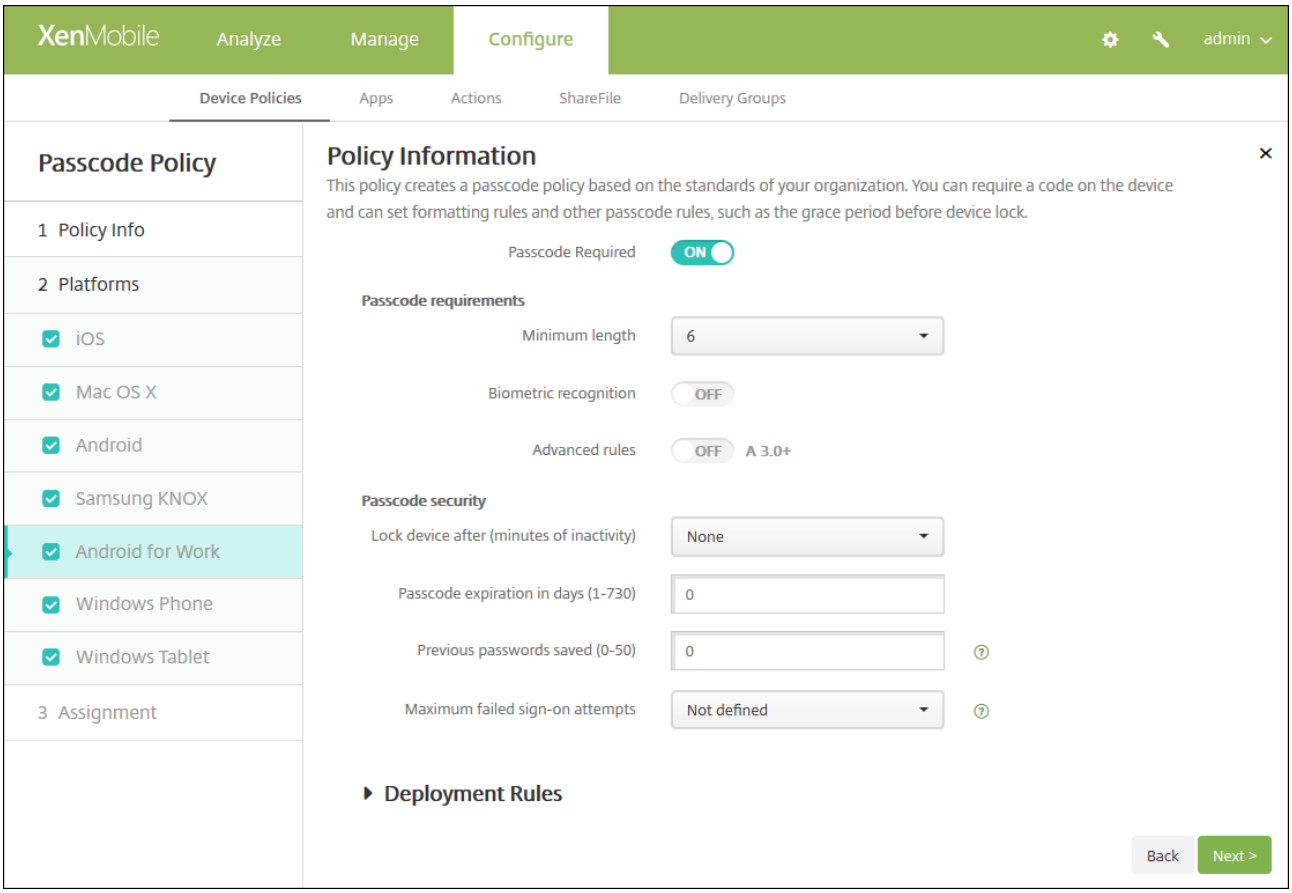
Enable SAML-based single-sign-on

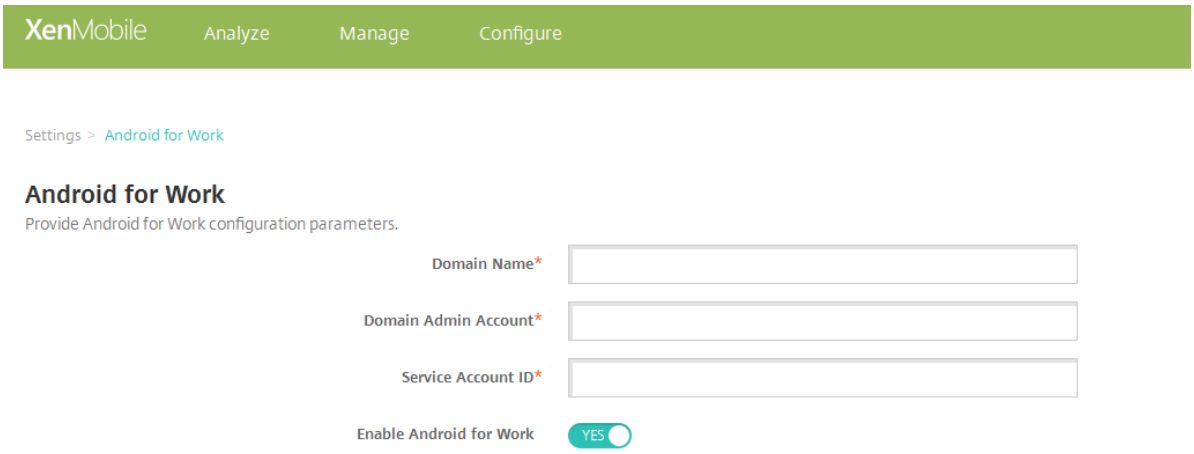






Set up an Android at Work device policy





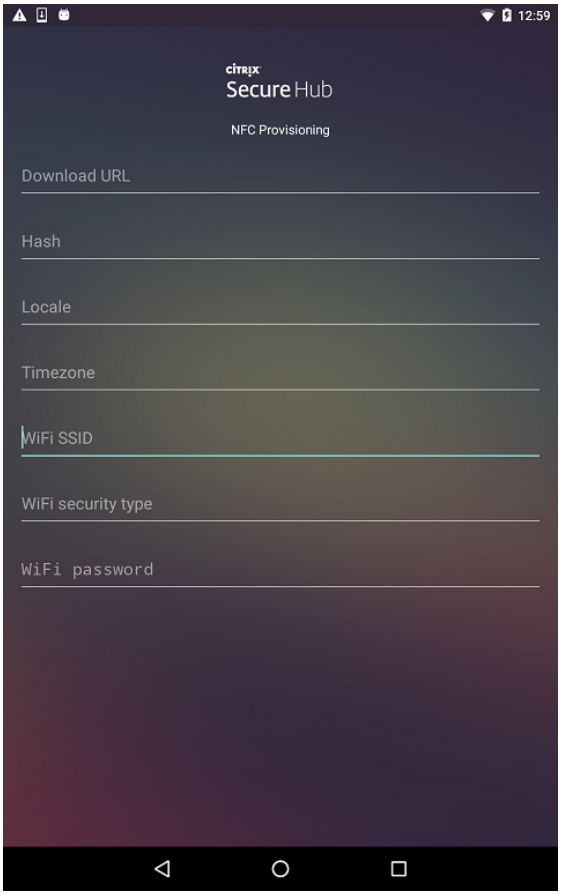
-
-
-
-

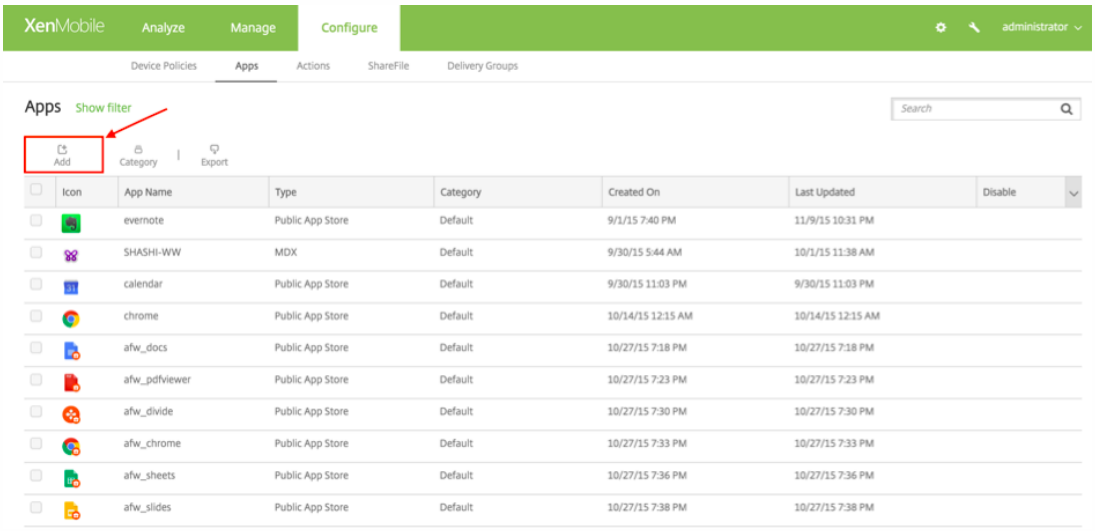
-

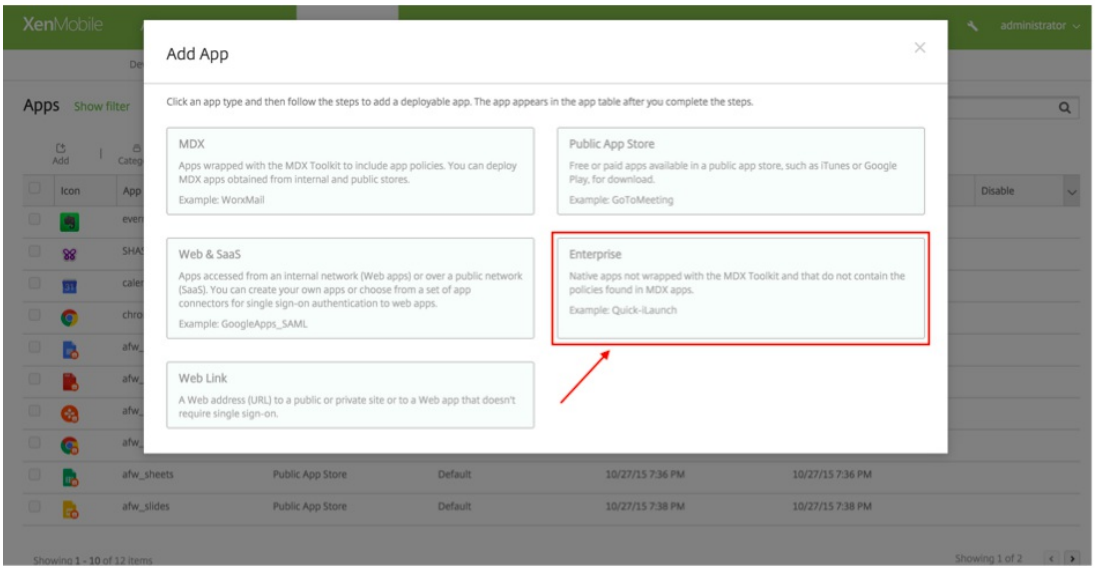
-
-

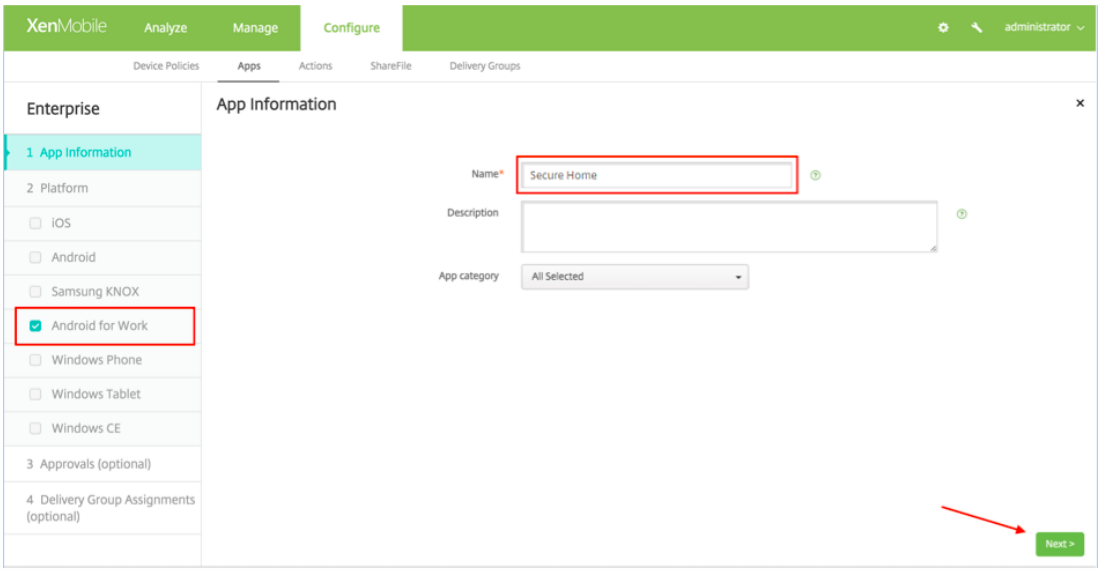
-
-
-
-

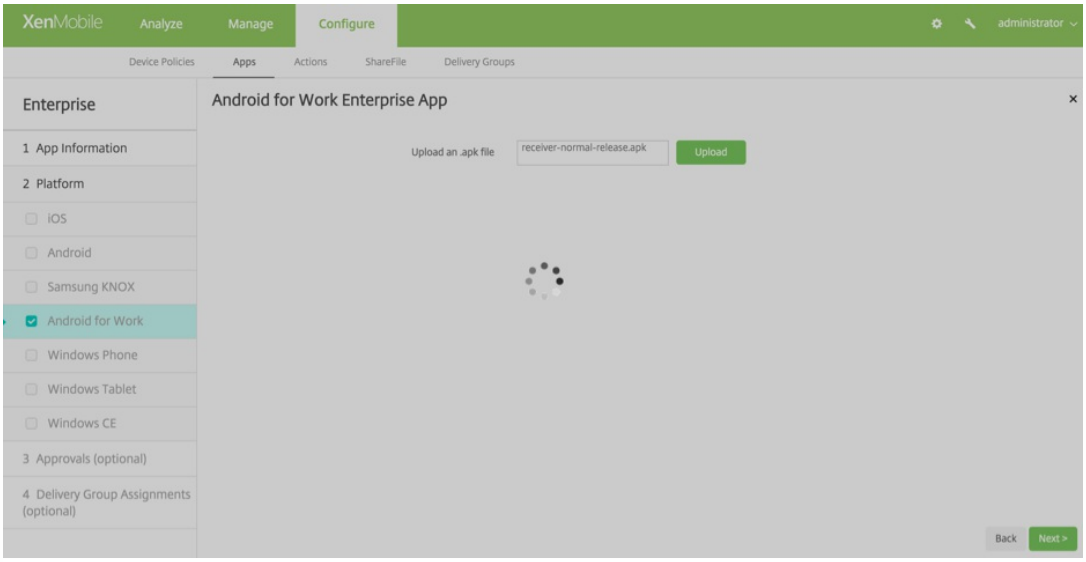
-
-

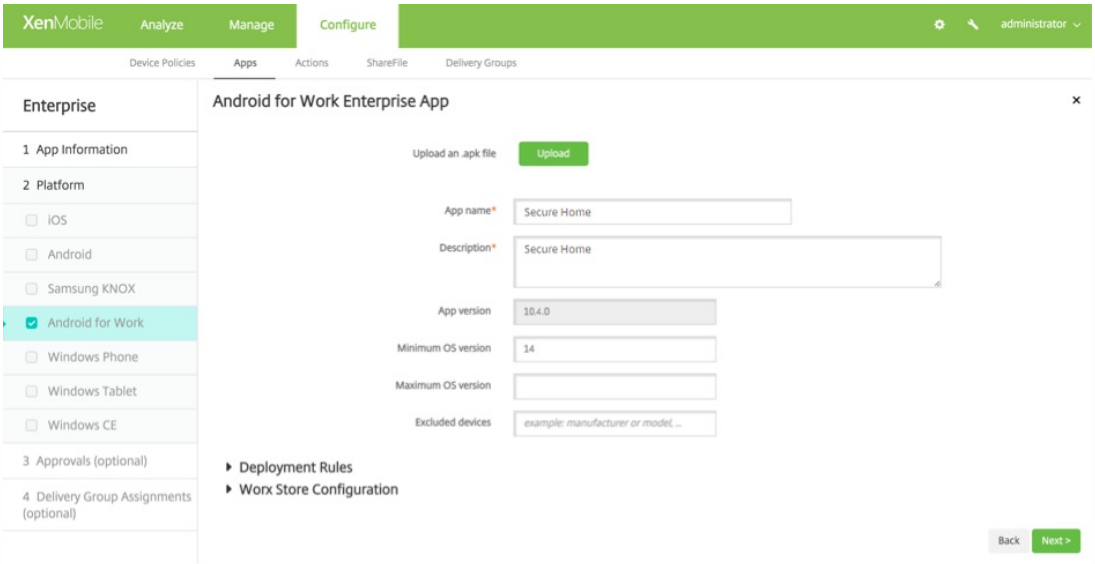


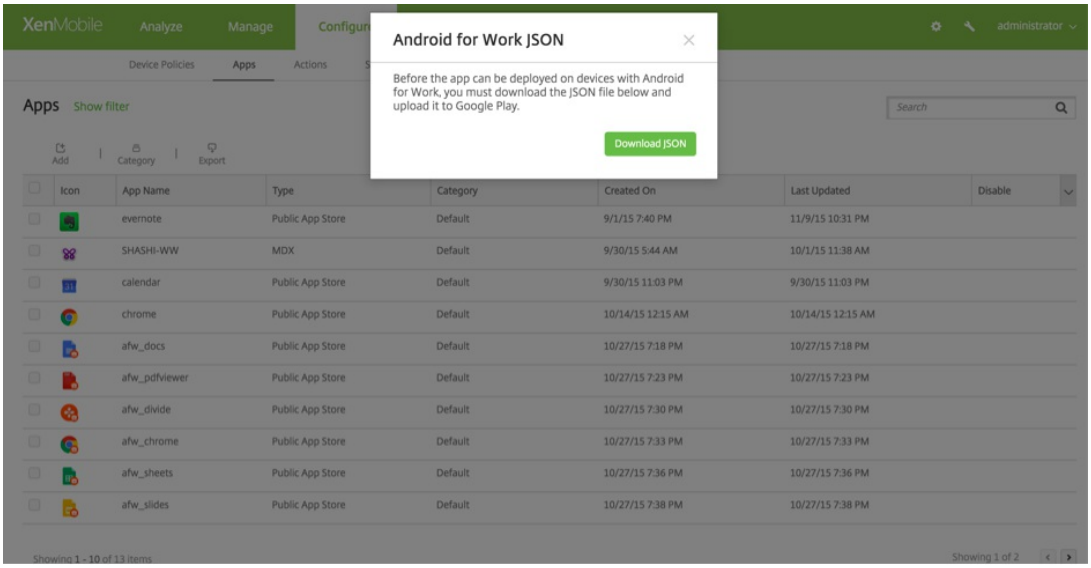


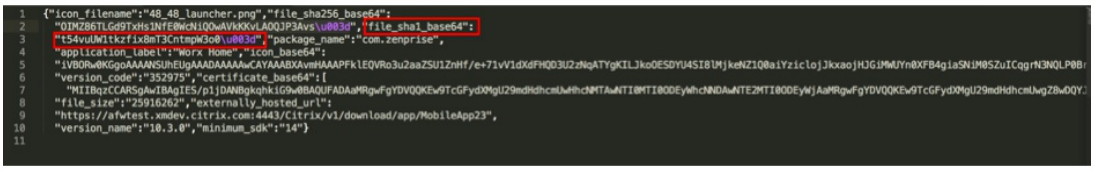




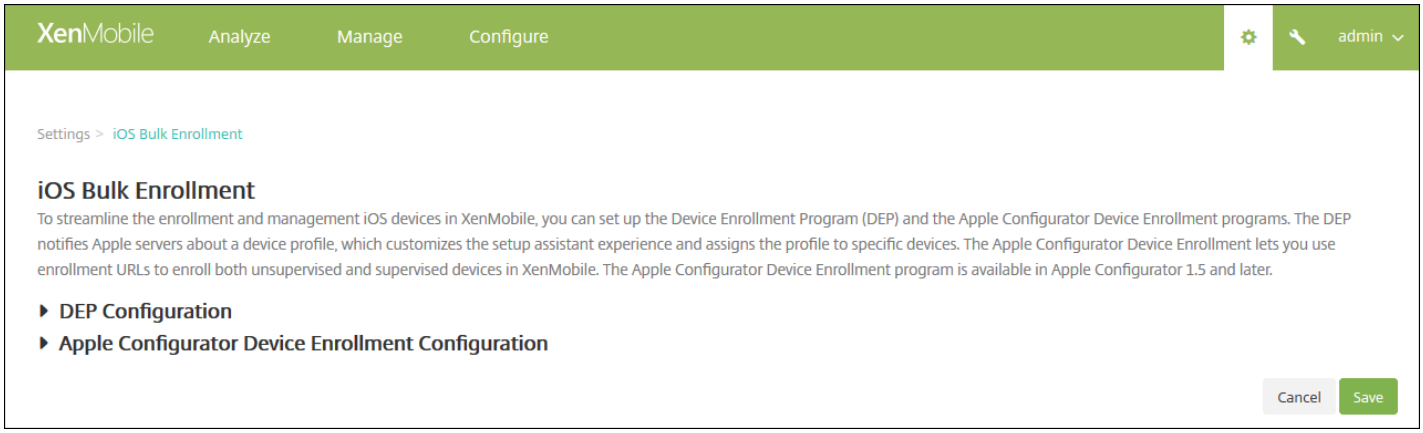




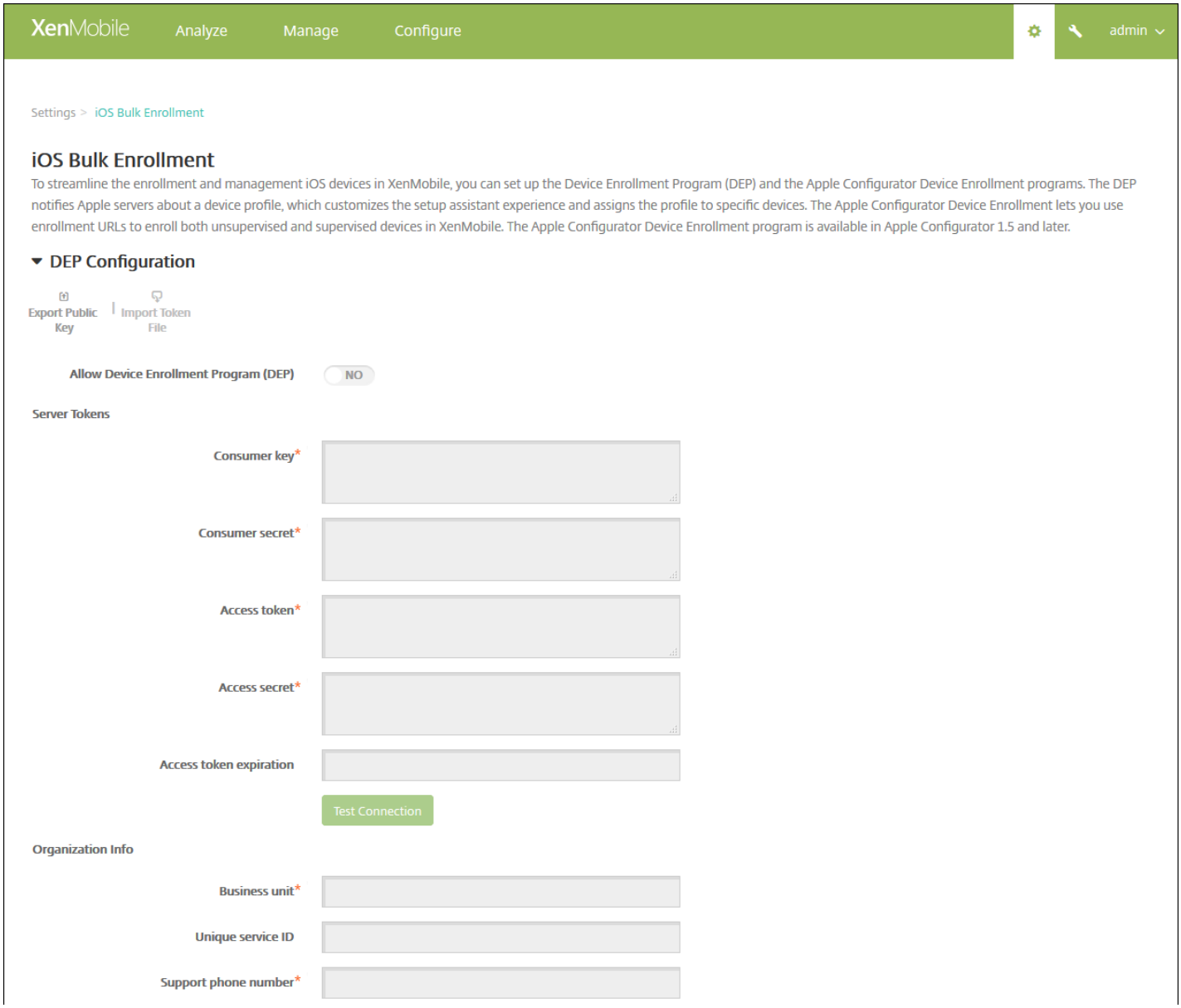


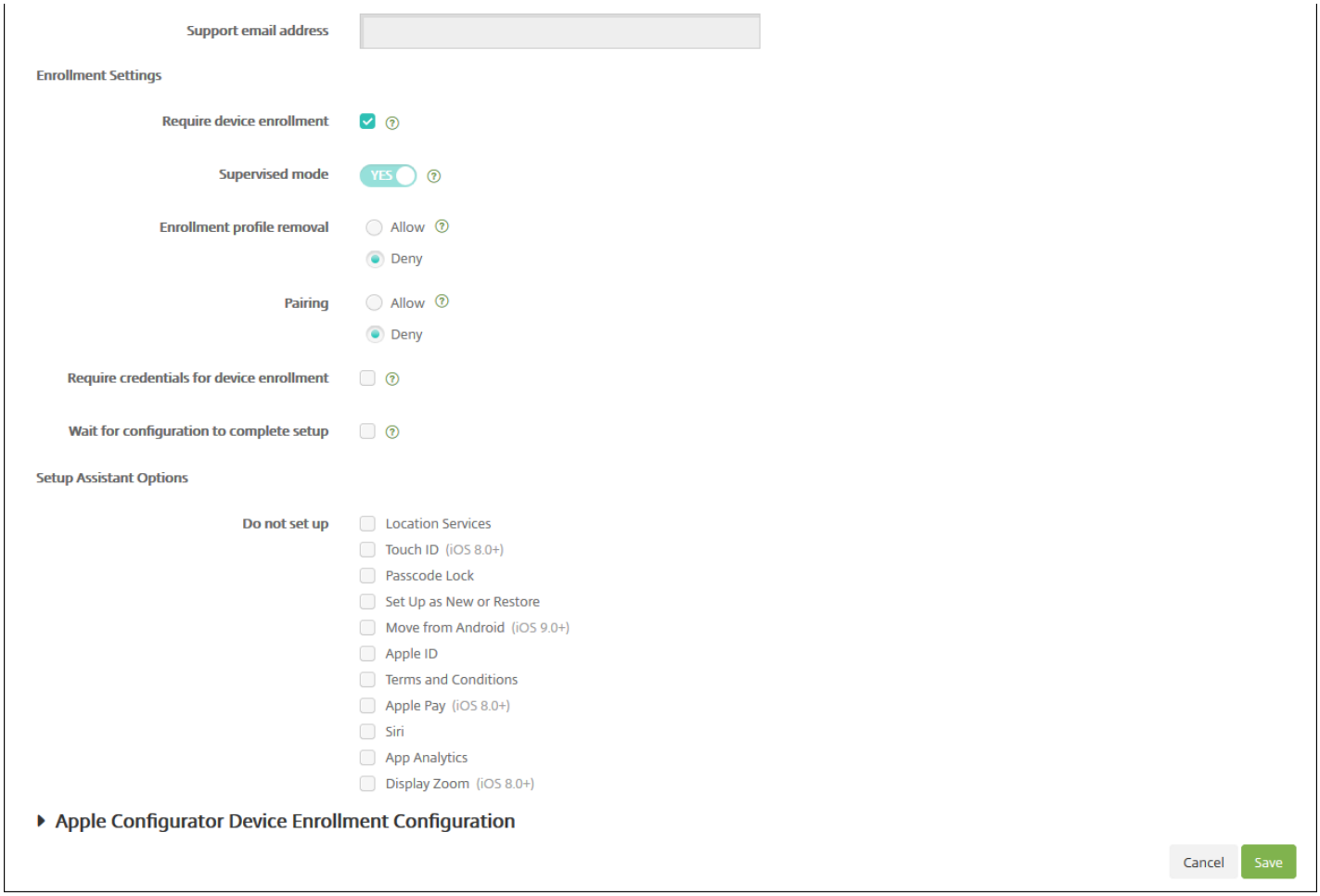


-
-
-



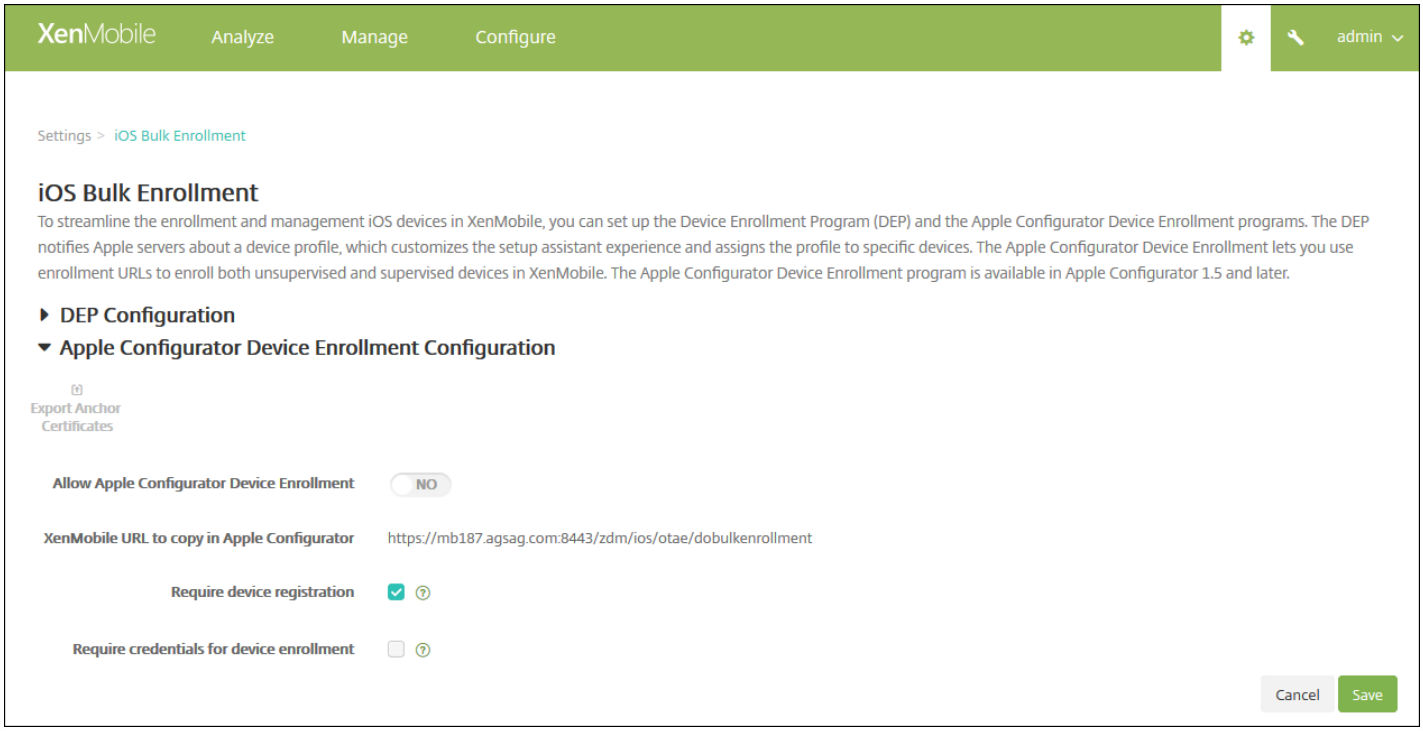
Configuring DEP settings





-
-
  -
    -
    -
    -
    -
    -
    -
-
-
-
-
-
-
-
-
-
-
-

Configuring Apple Configurator settings



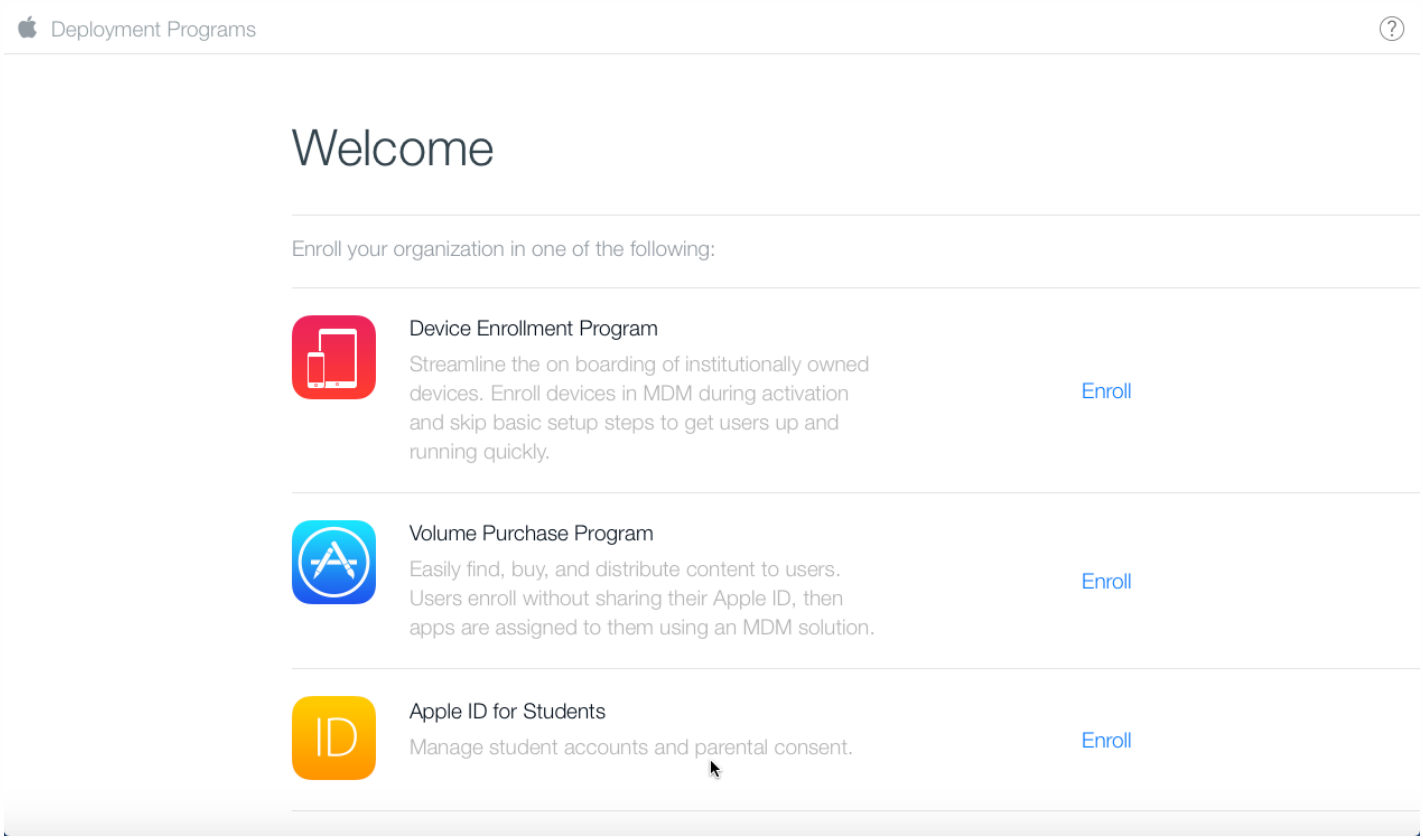
-
-
-

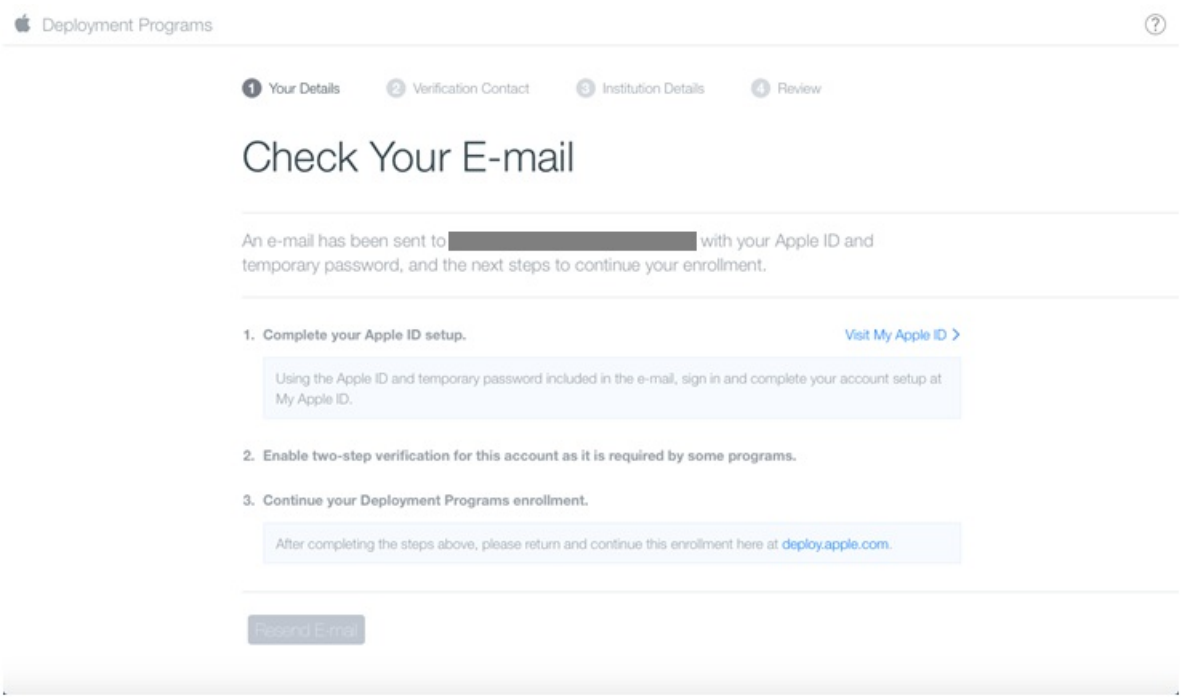
To renew or update certificates when using the Apple DEP

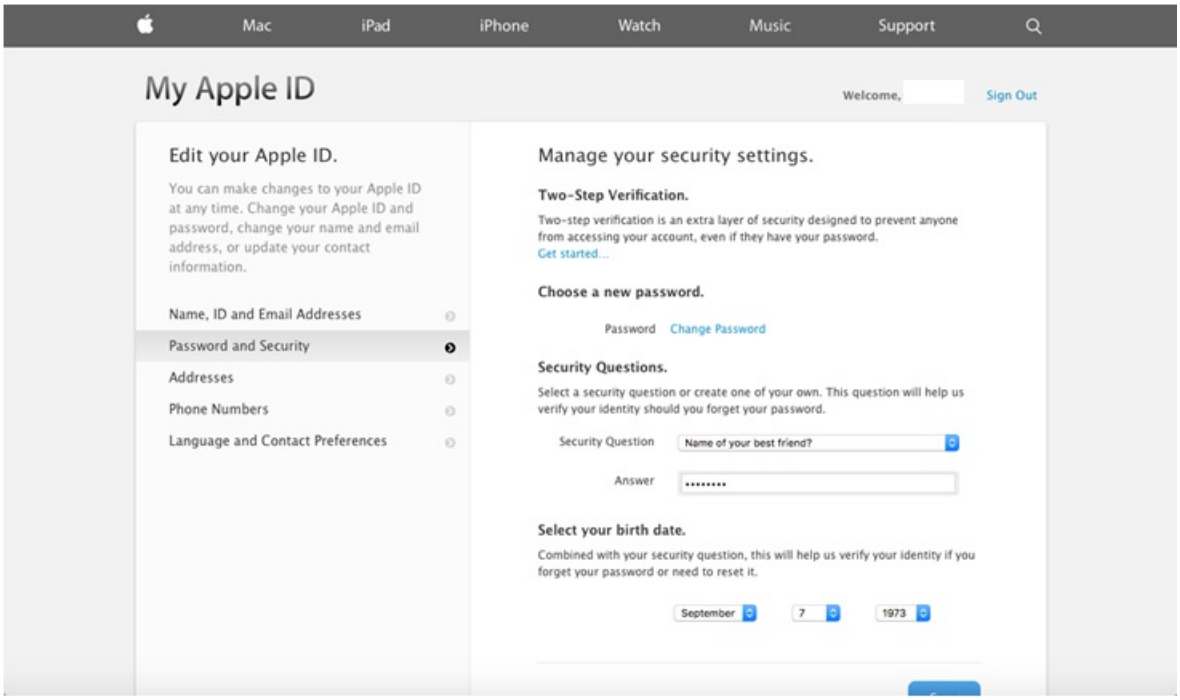
To place an iOS device in Supervised mode by using the Apple Configurator

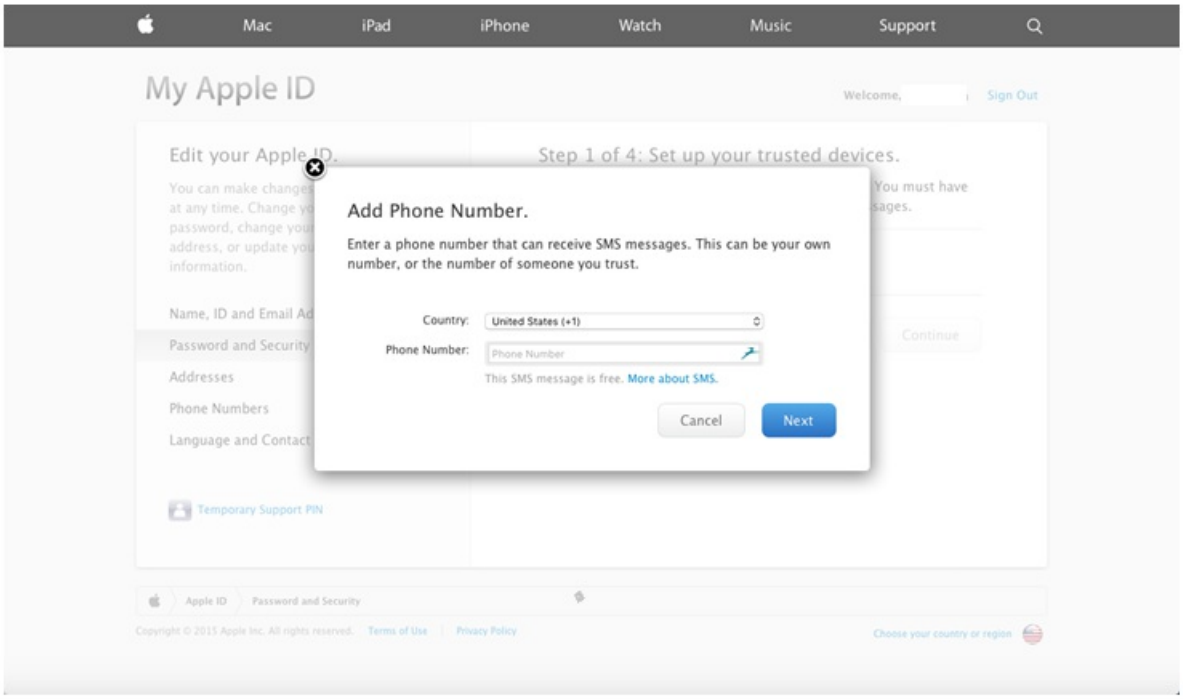
-
-
-
-

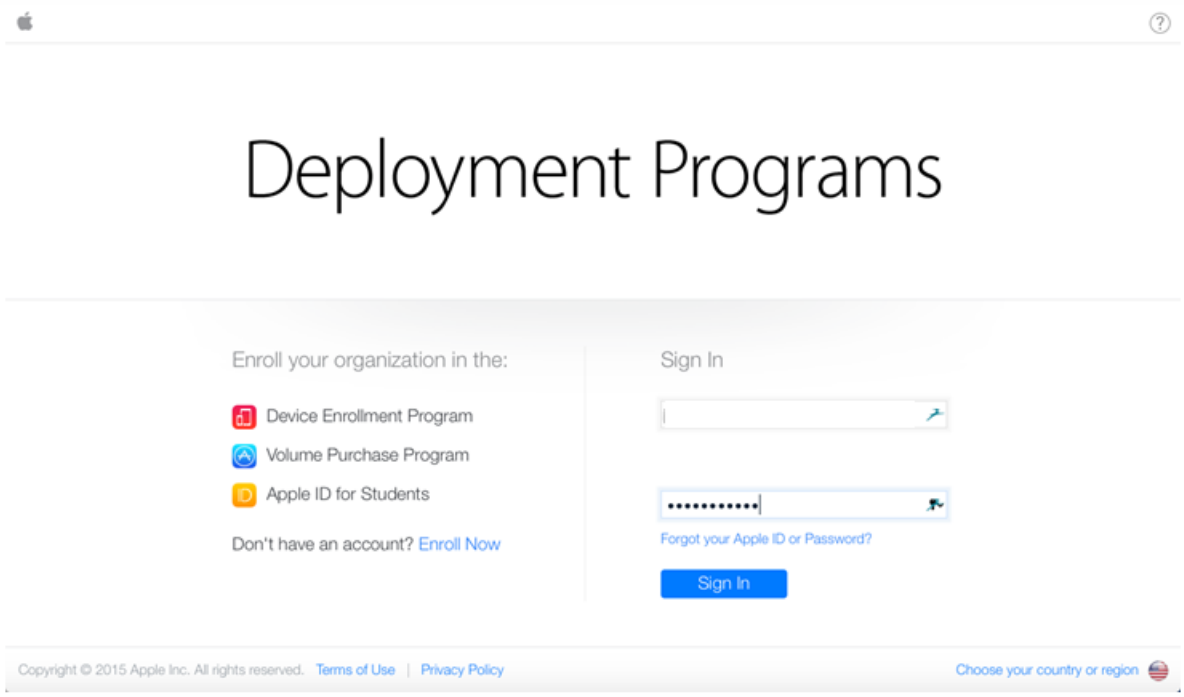
Applying for the Apple DEP account

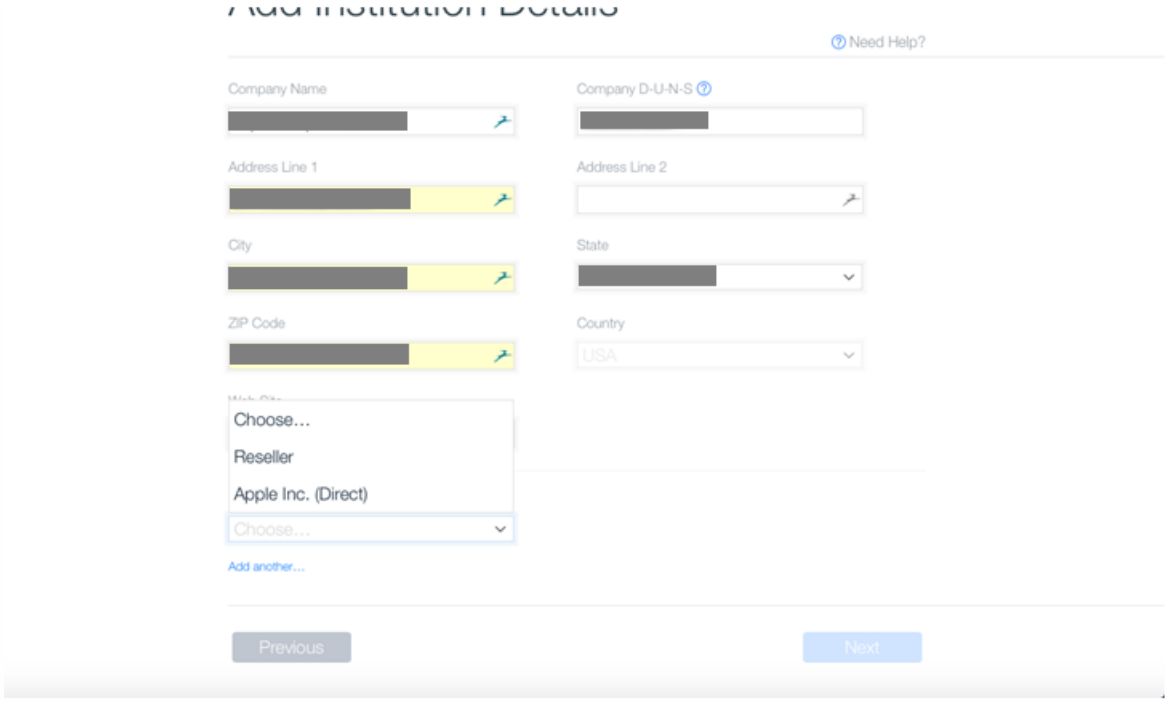


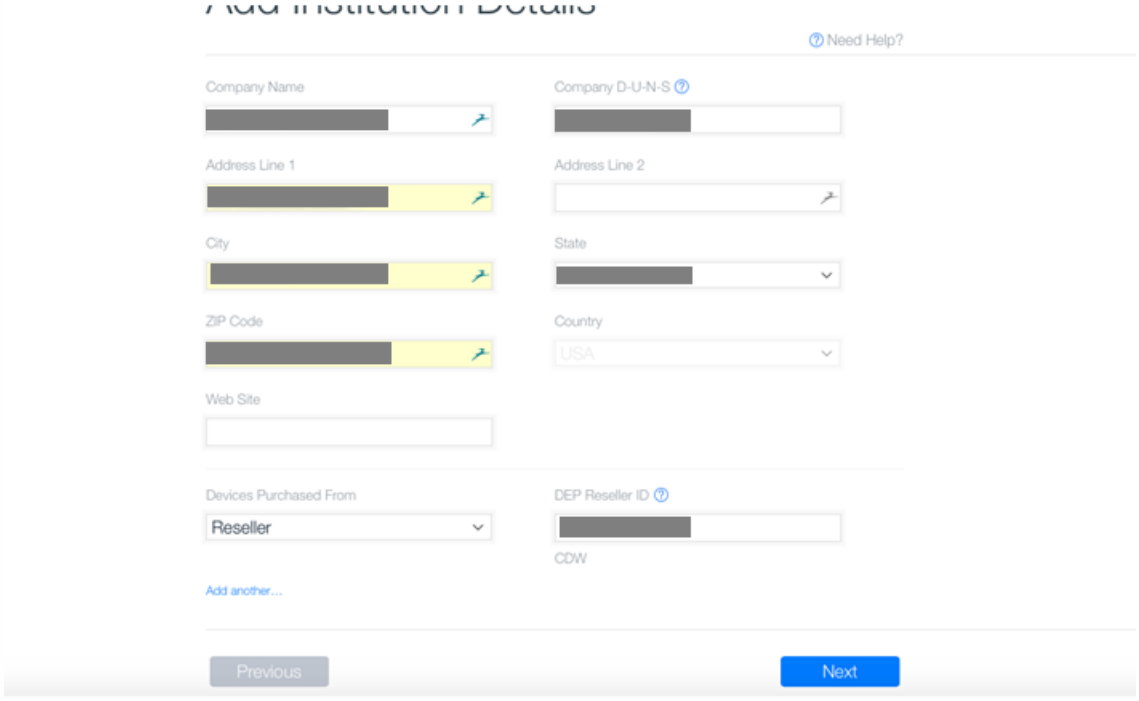


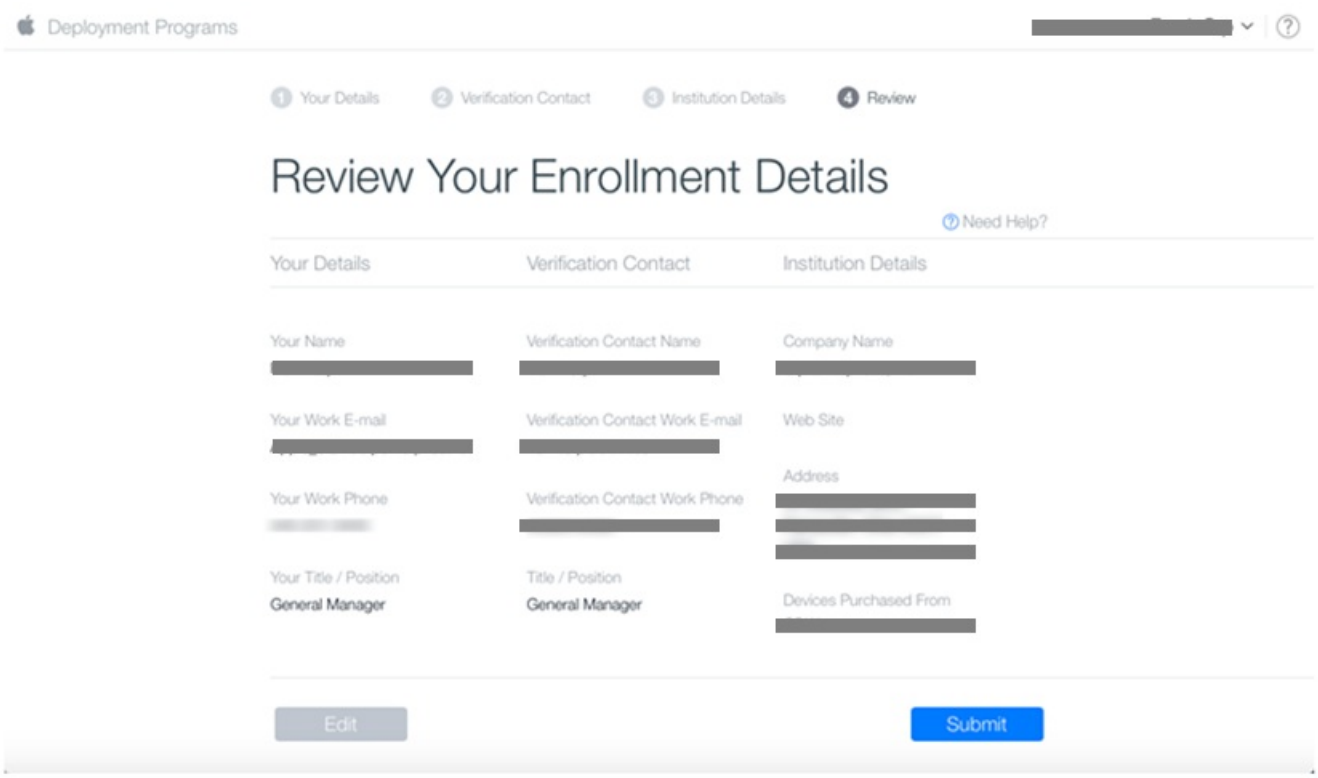


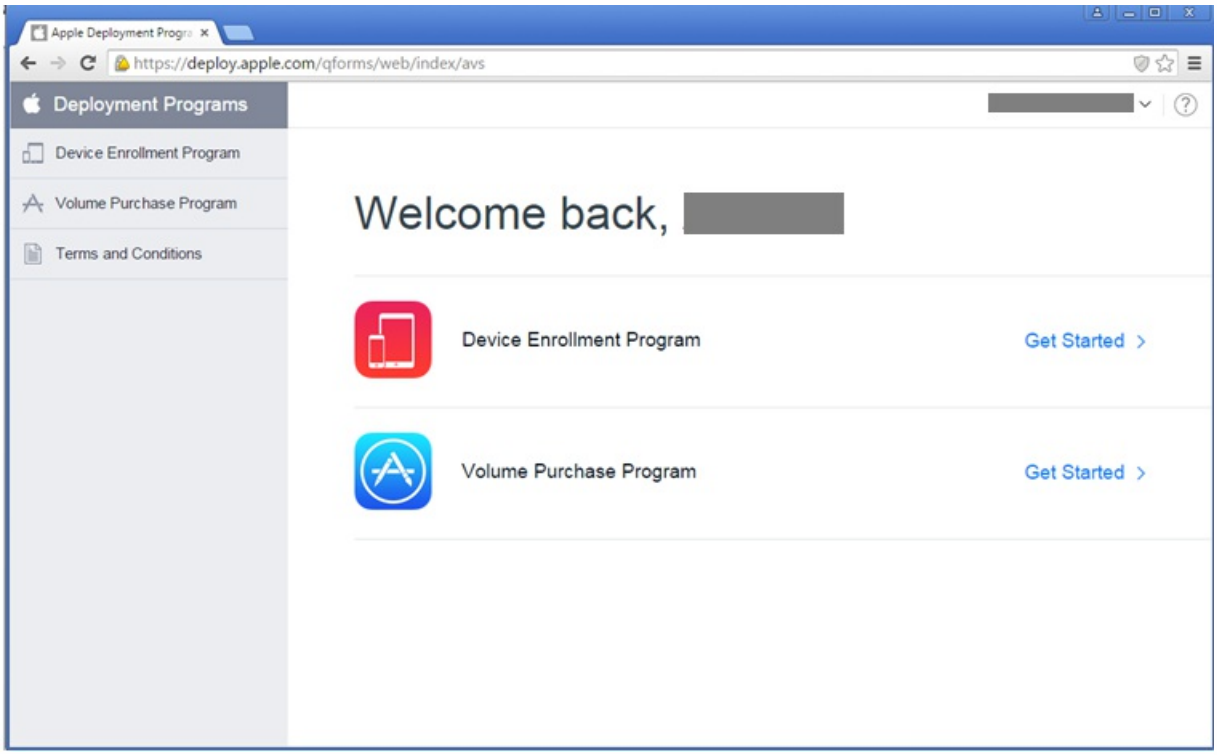




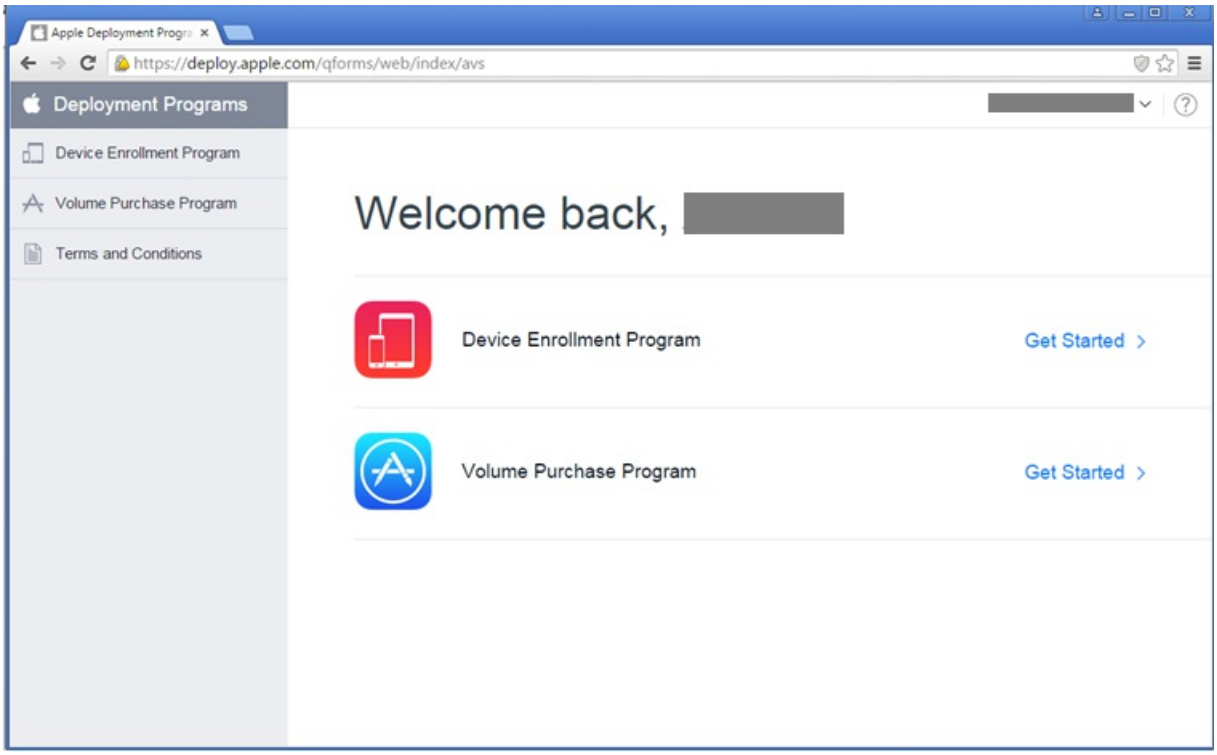


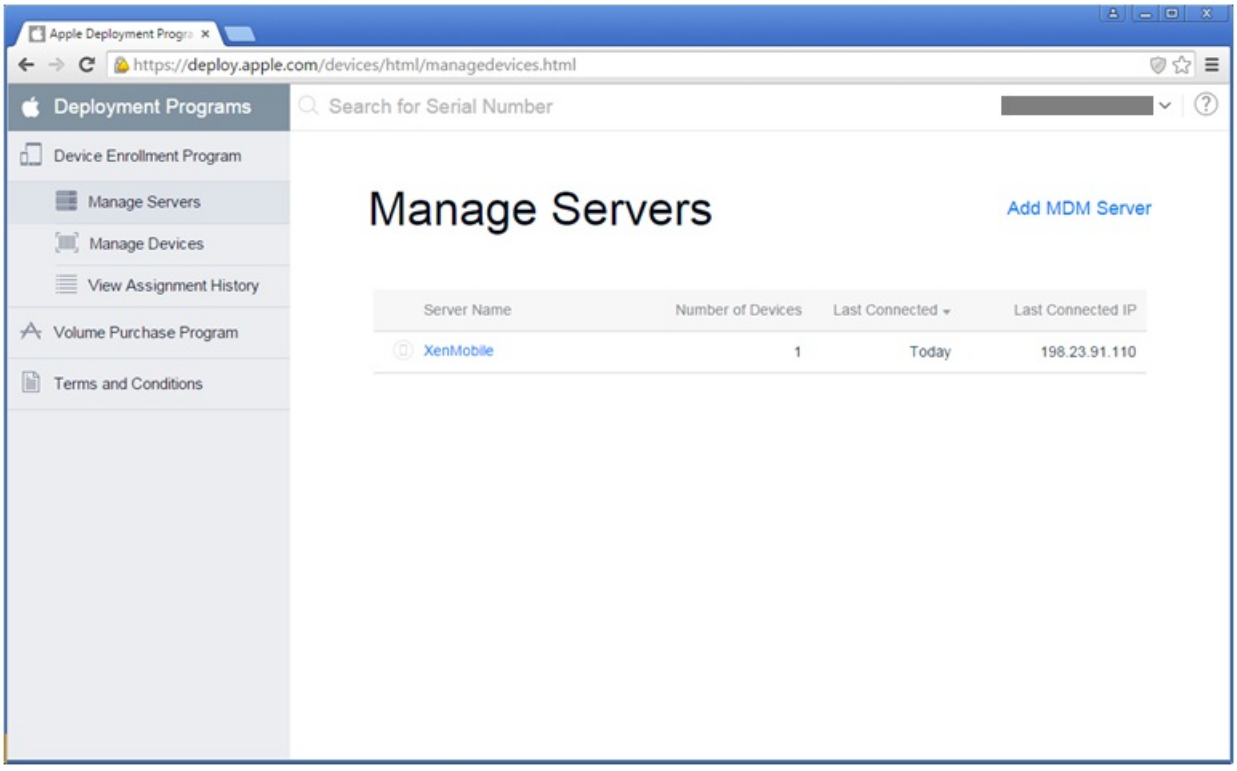


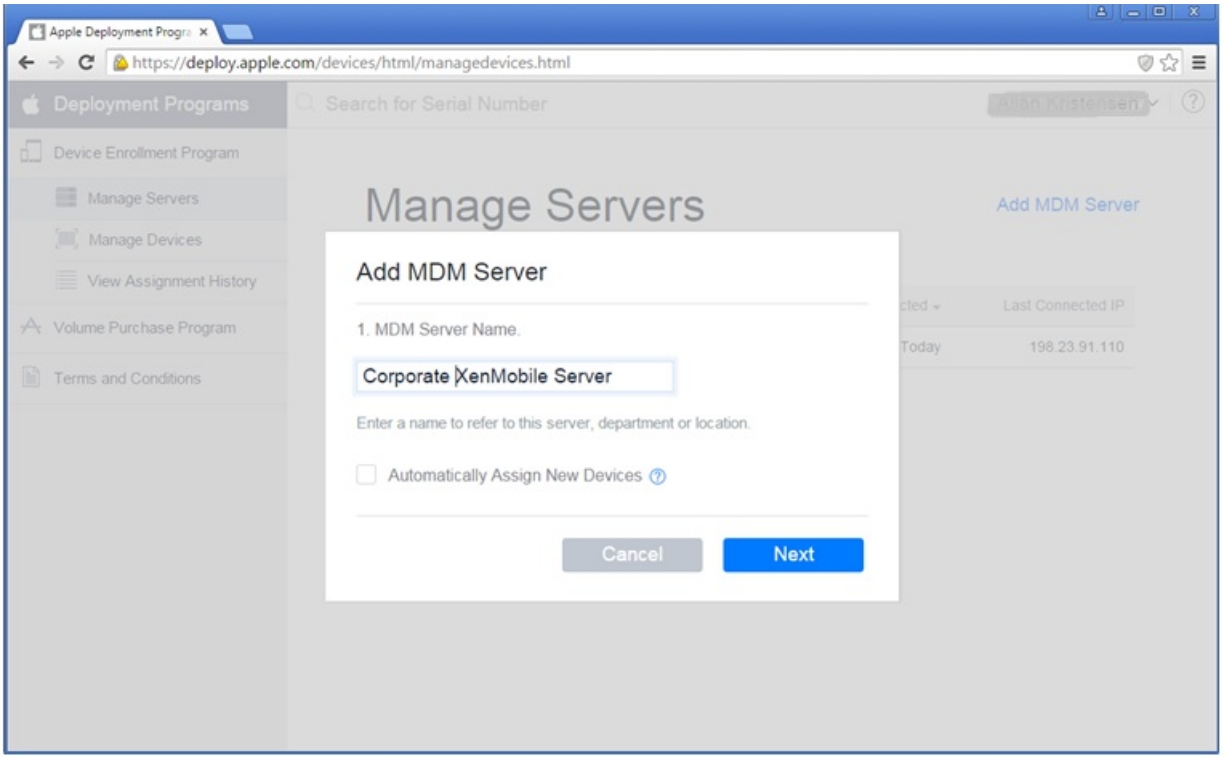


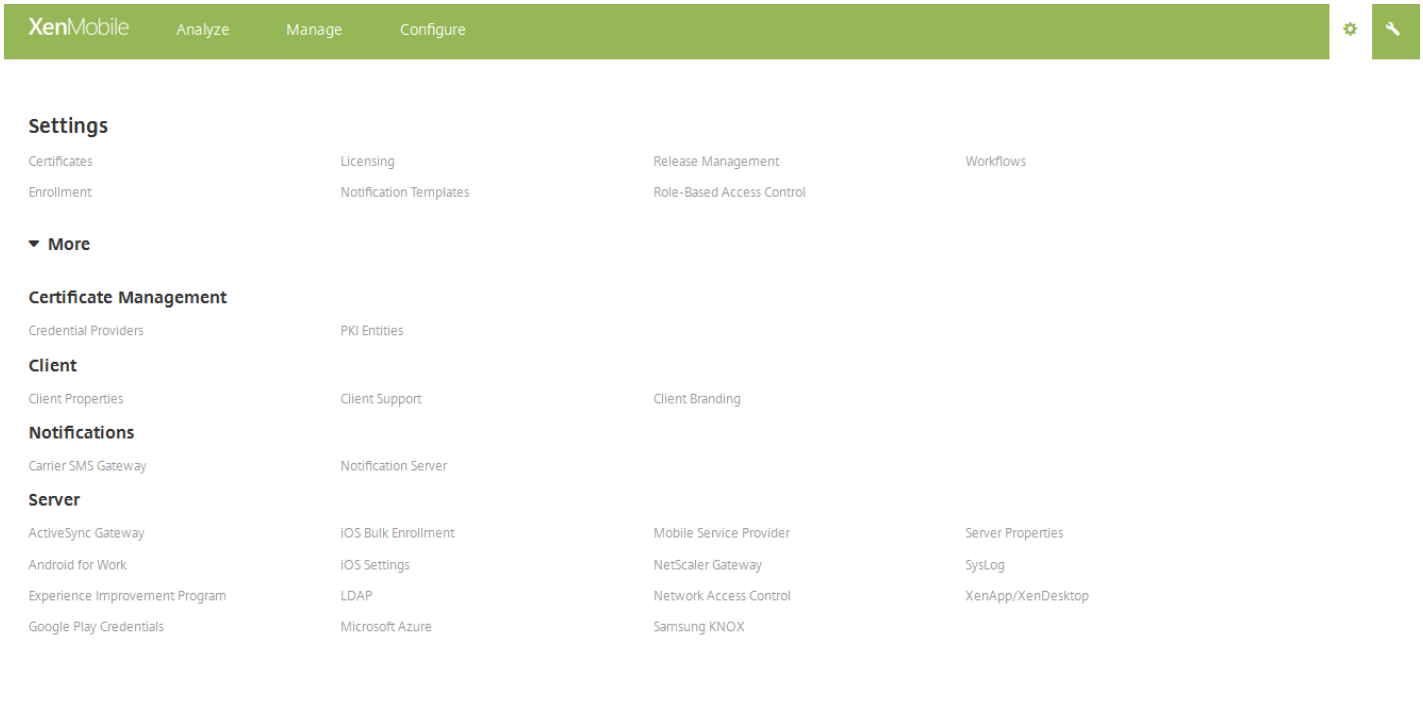


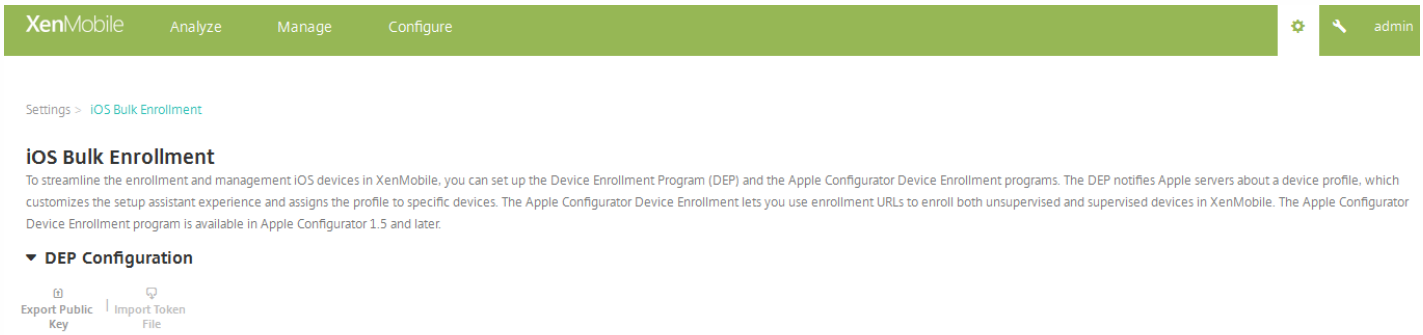
Integrating your Apple DEP account with XenMobile

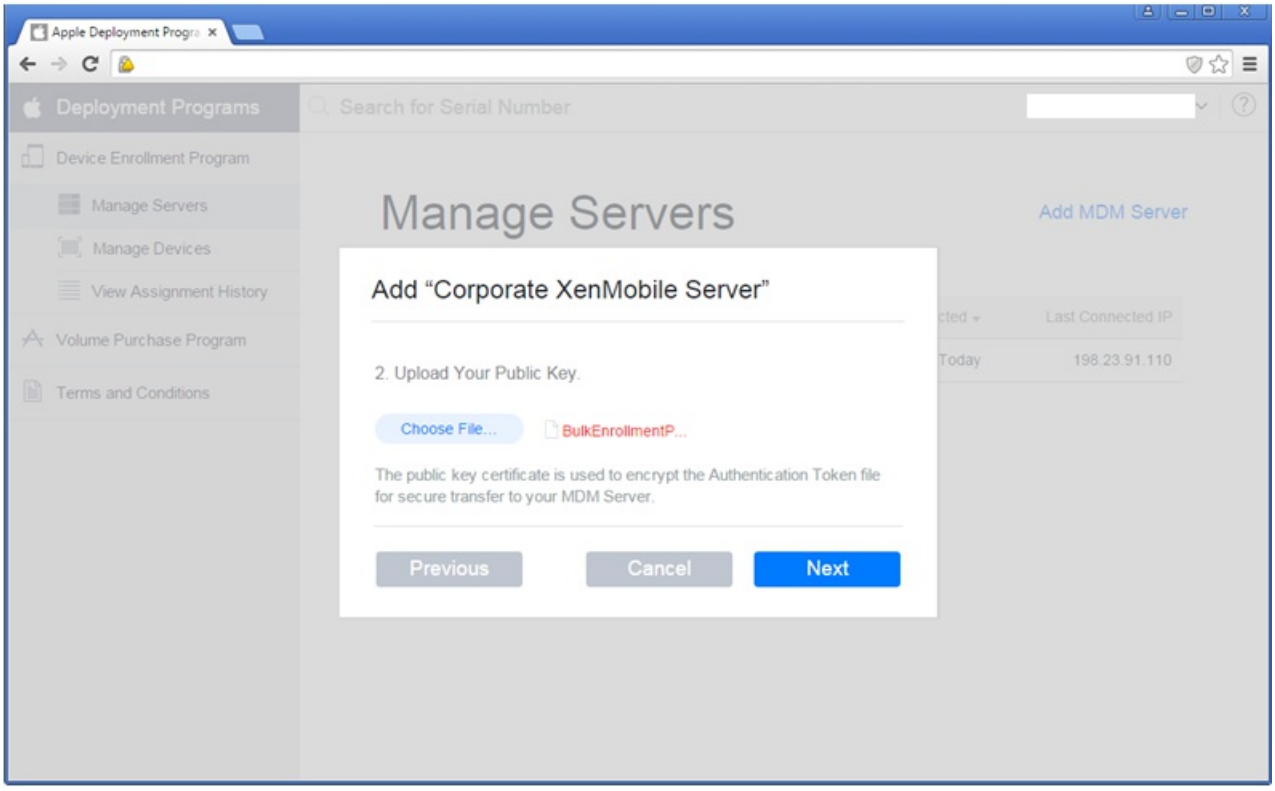


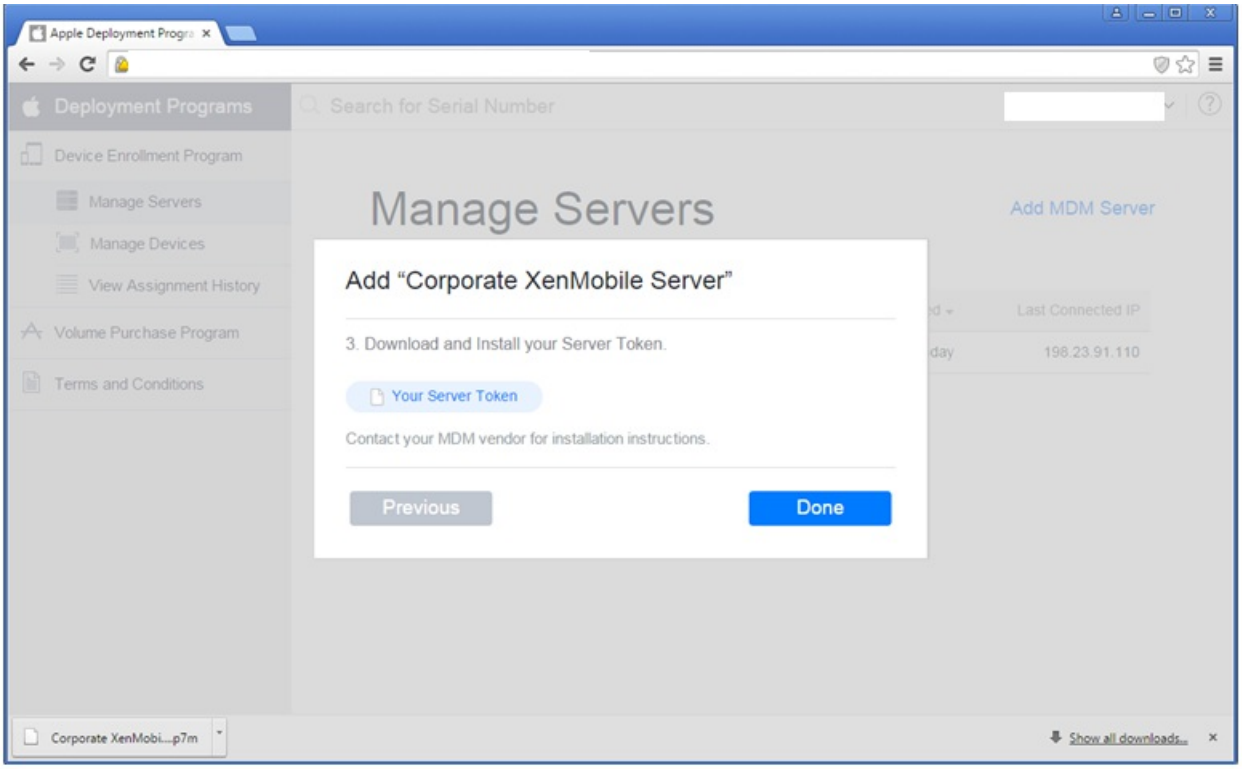


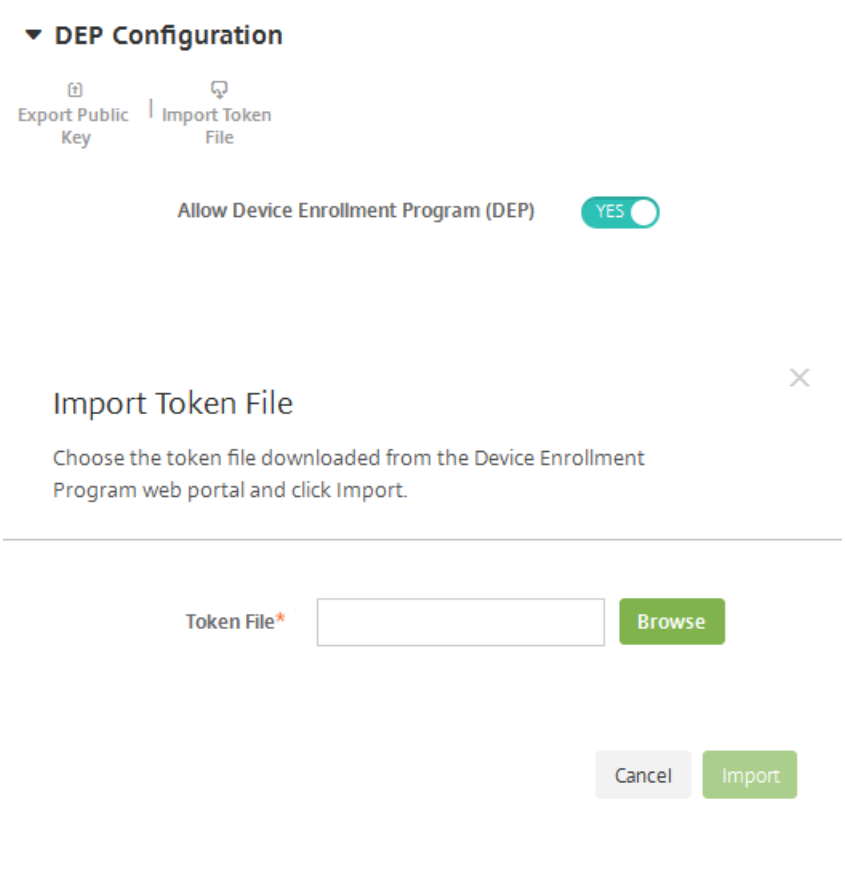


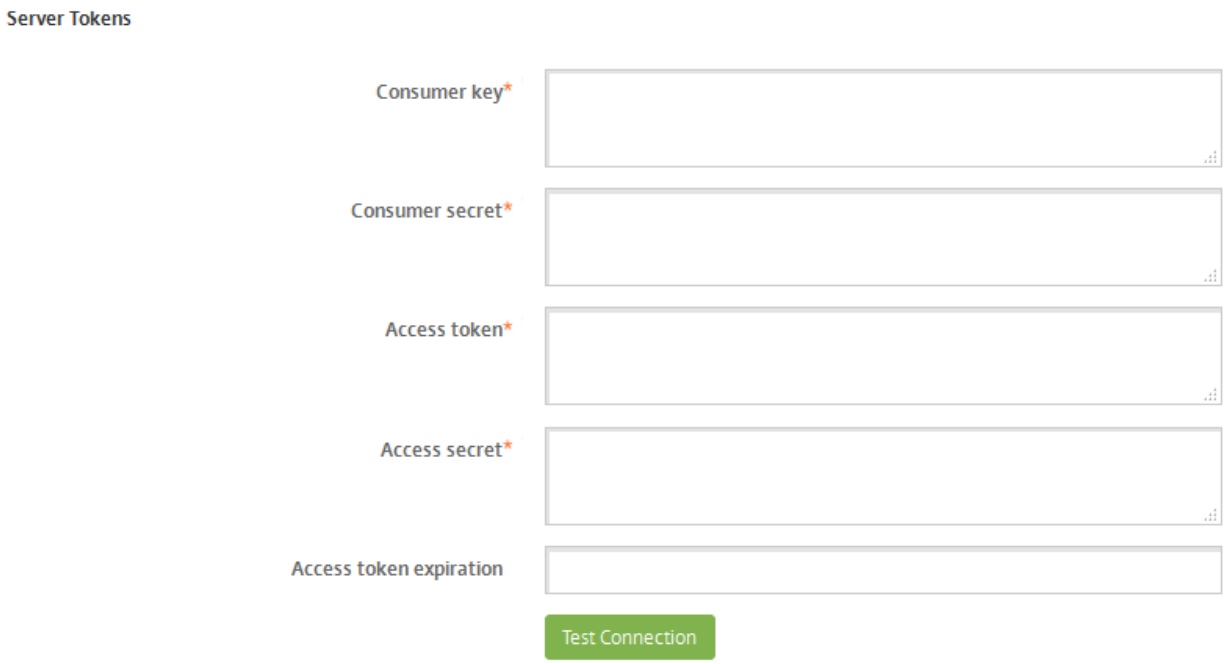


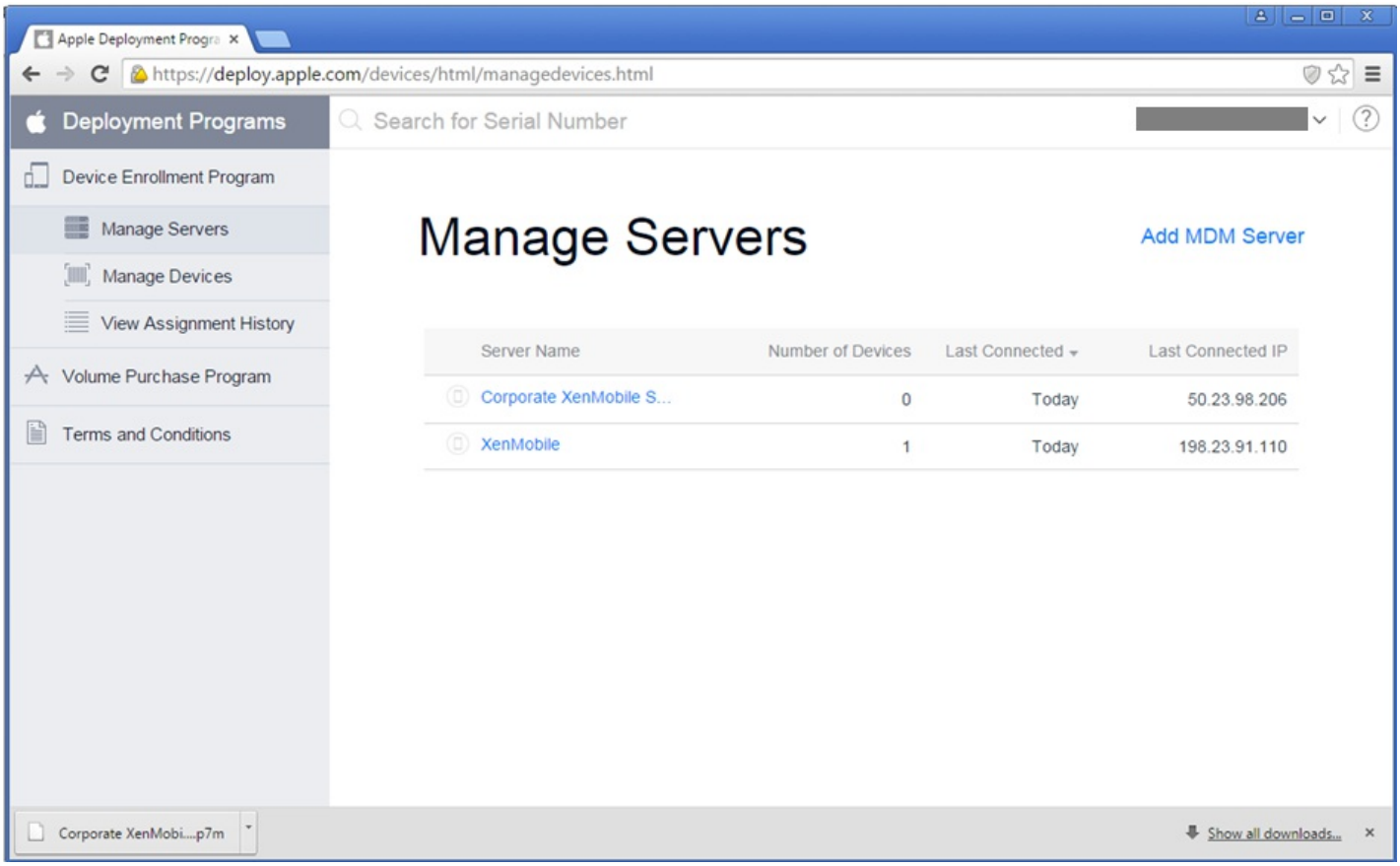






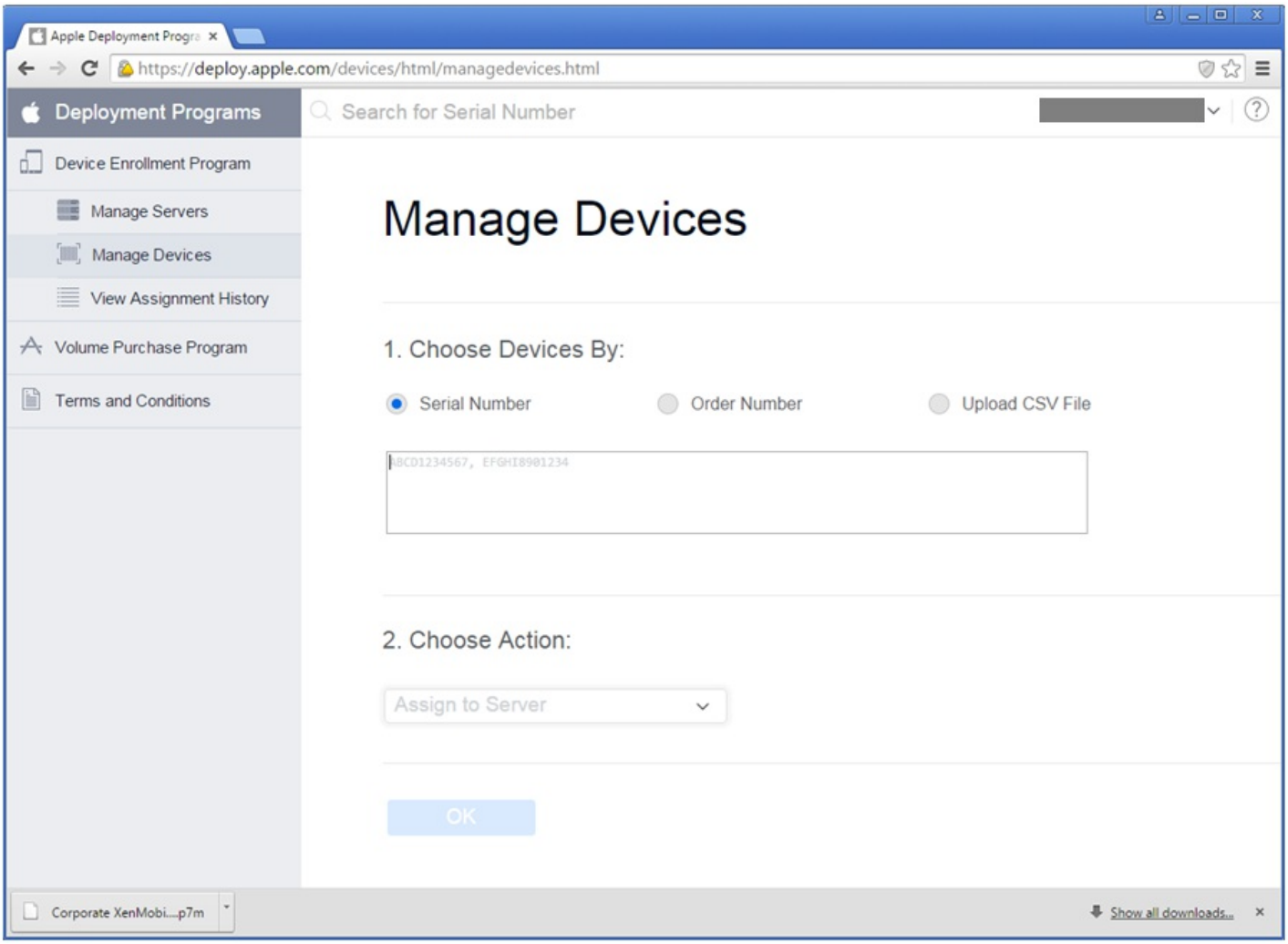


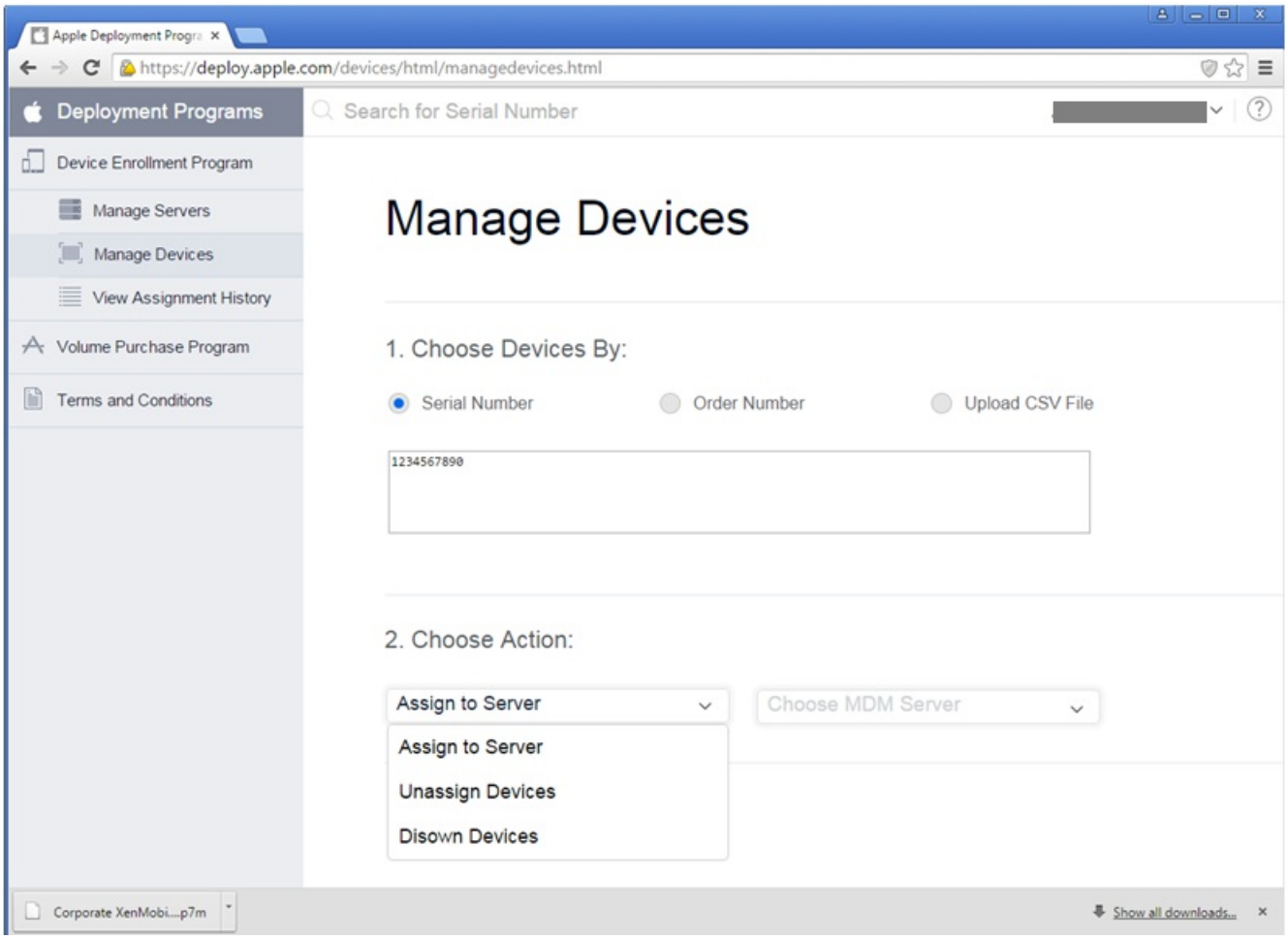


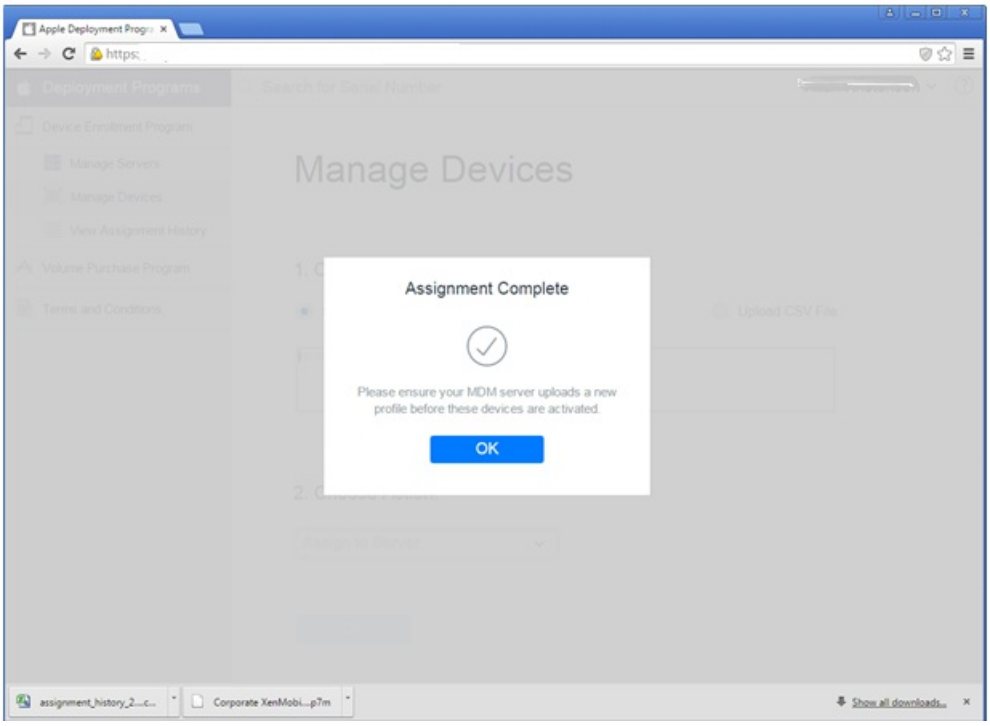


Ordering DEP-enabled devices

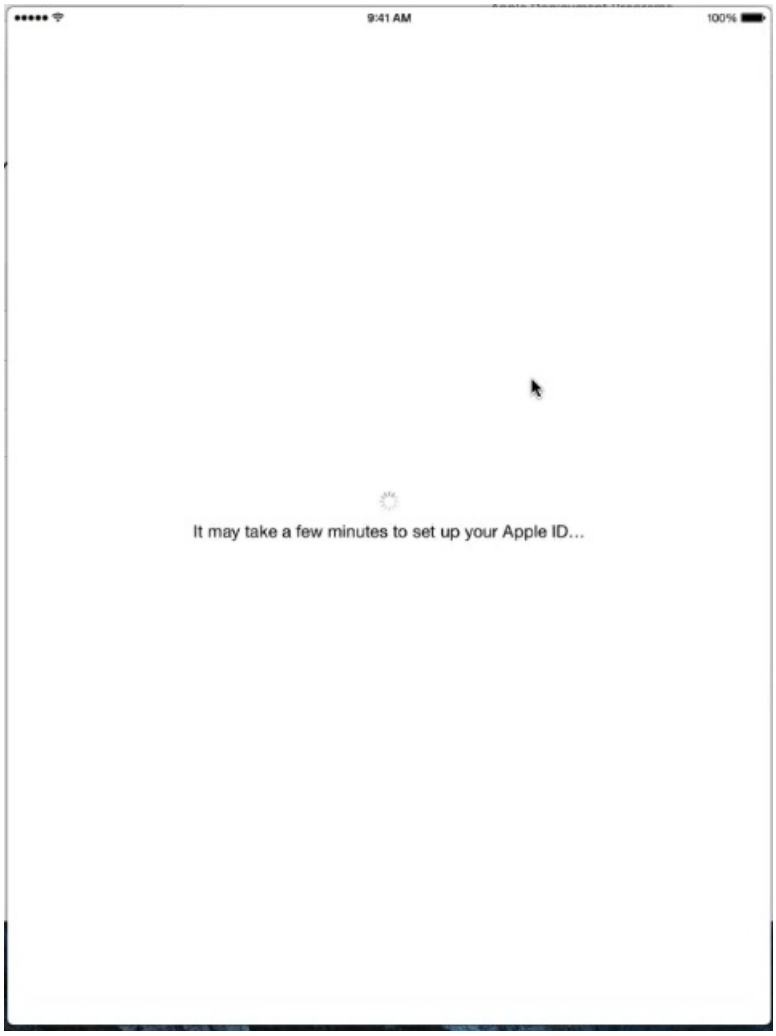
Managing DEP-enabled devices

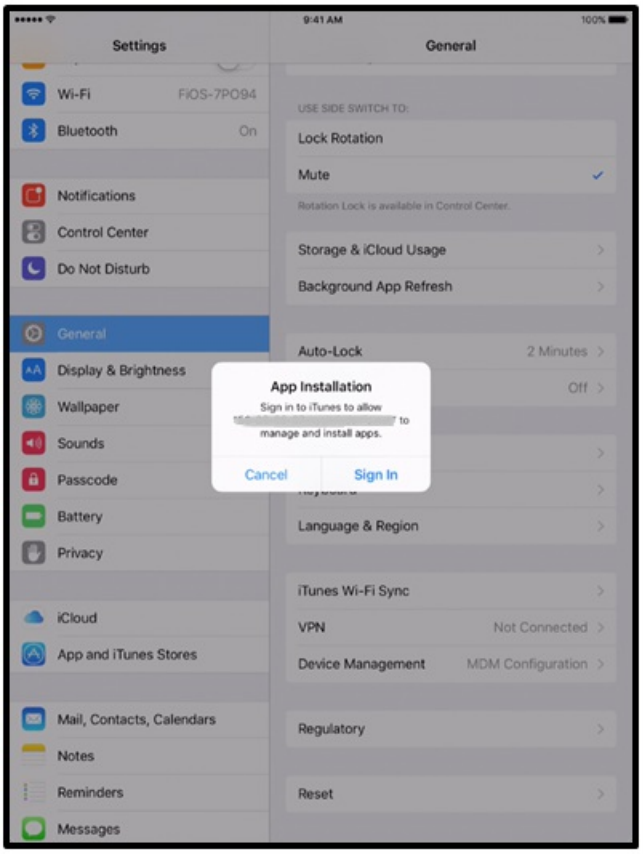


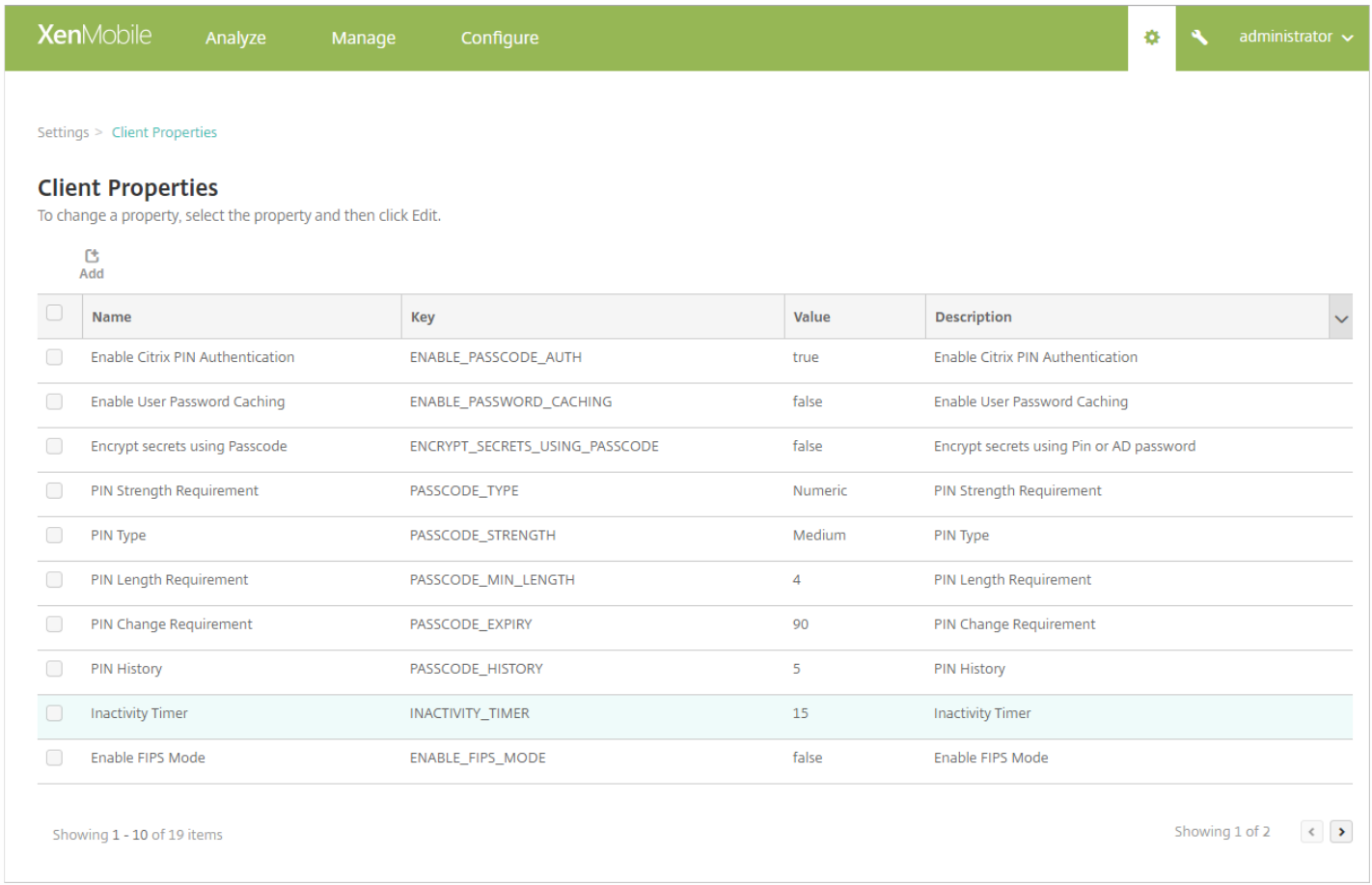




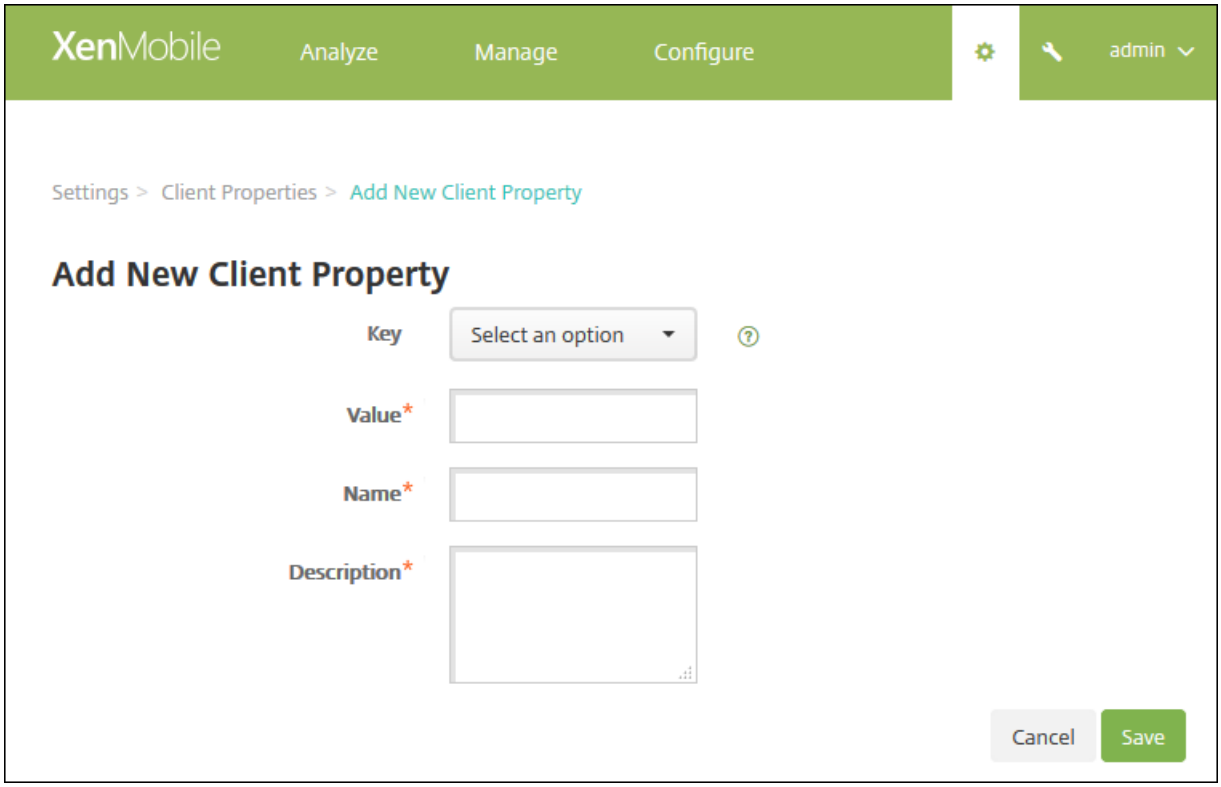
User experience enrolling an Apple DEP-enabled device





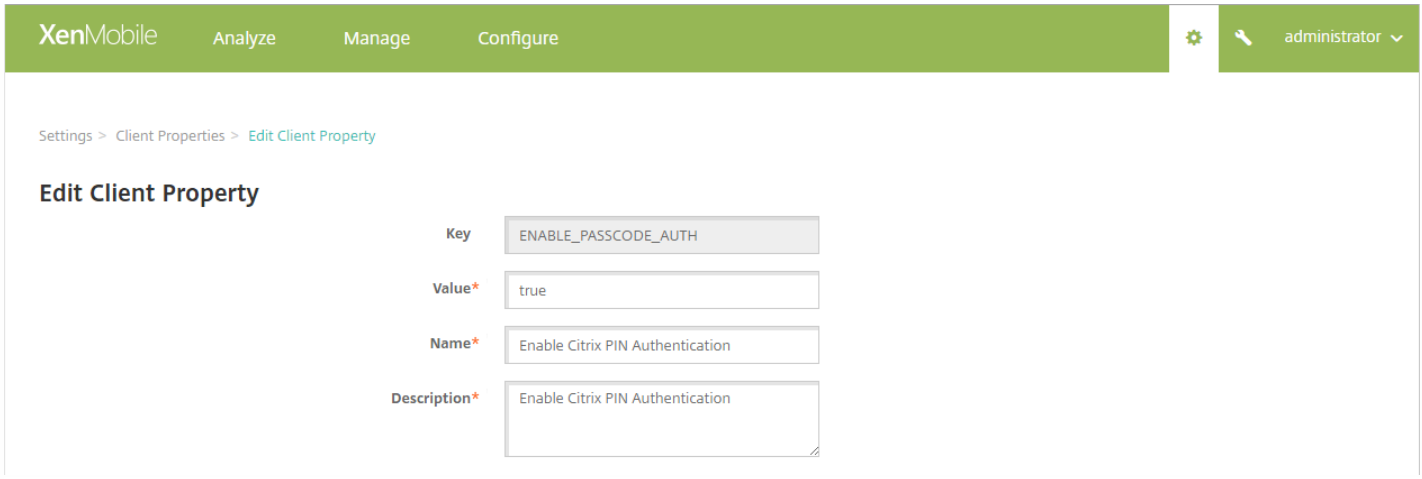


To add a client property



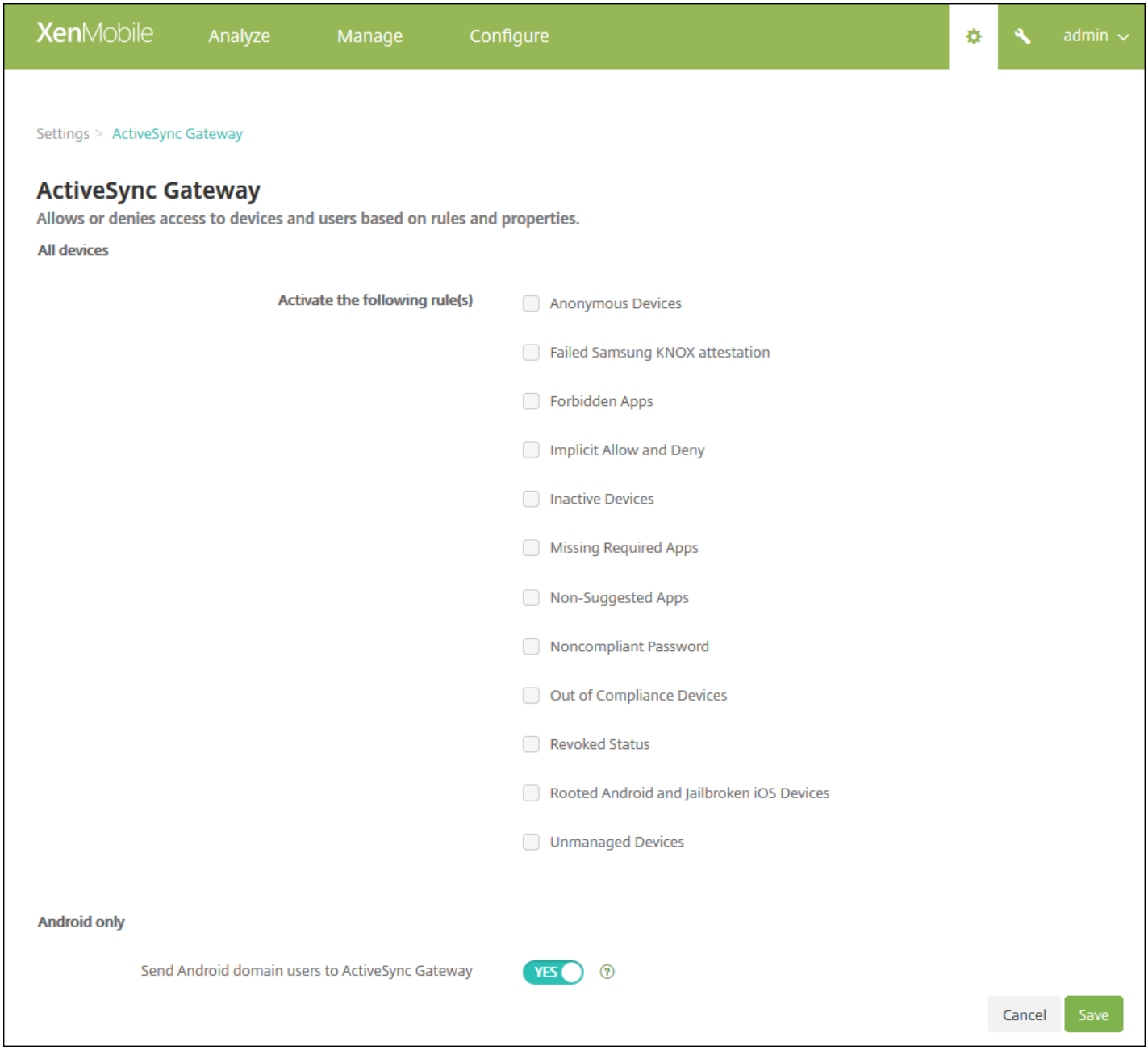
-
-
-
-

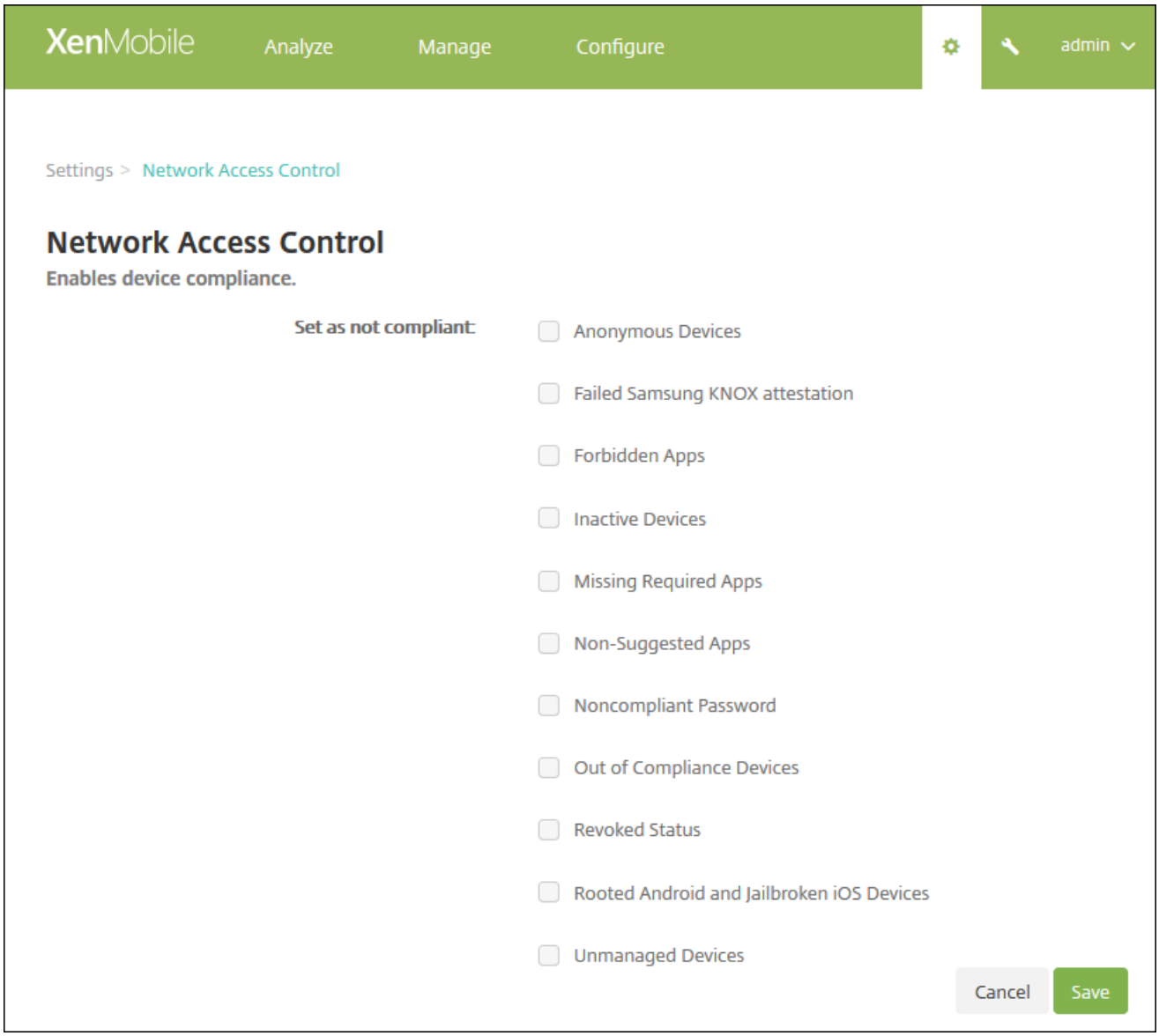
To edit a client property

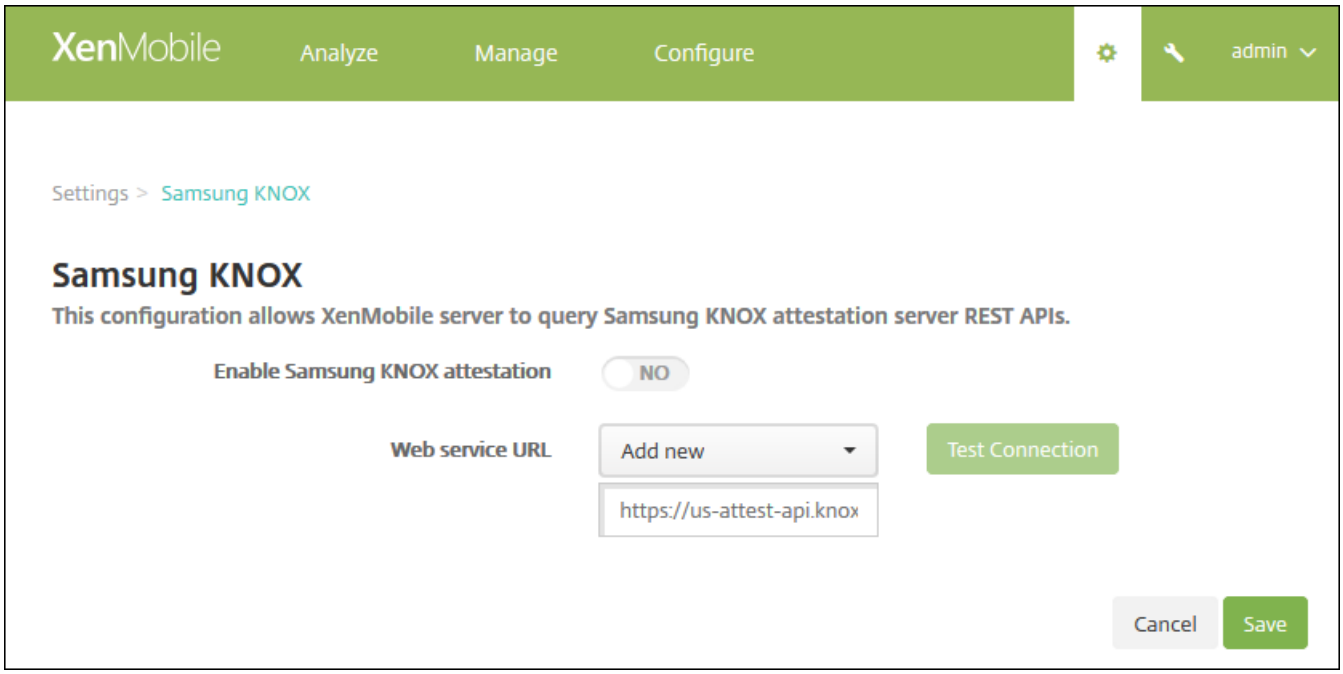


-
-
-
-

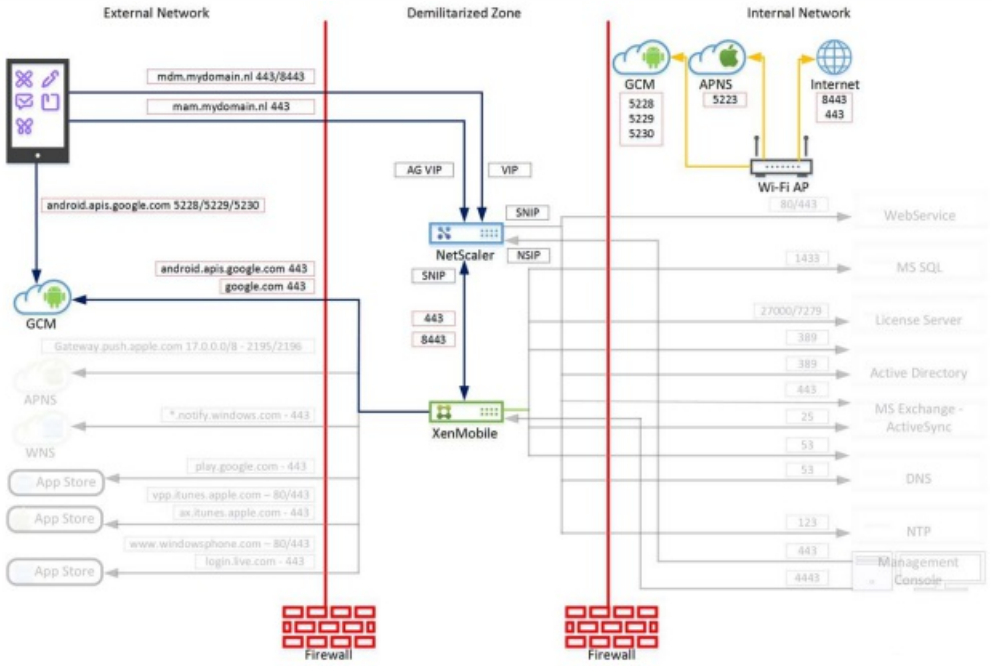
To delete a client property

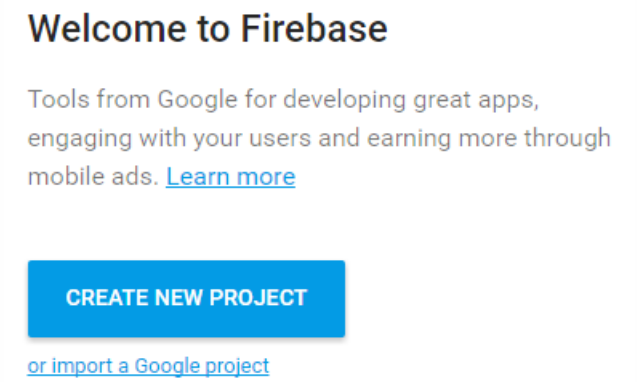


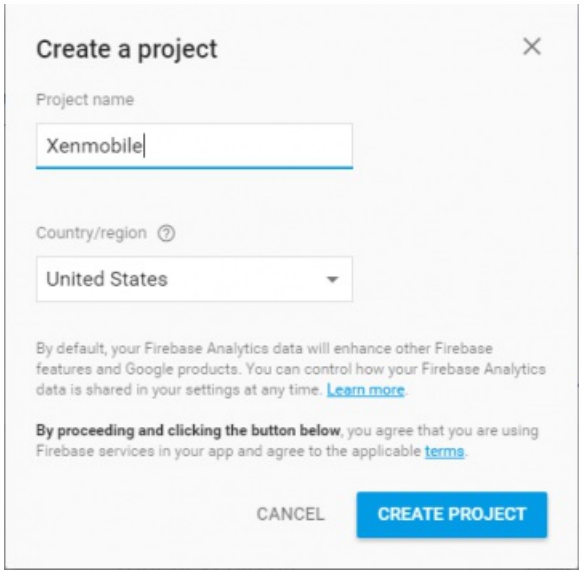


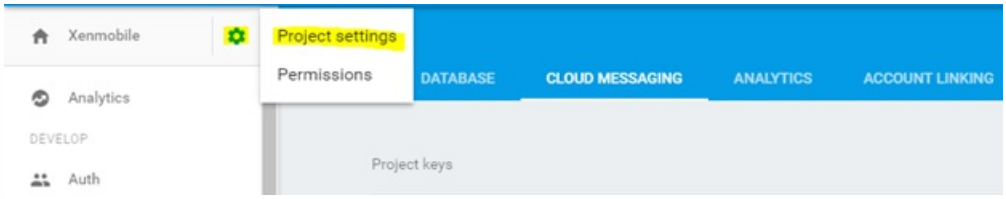


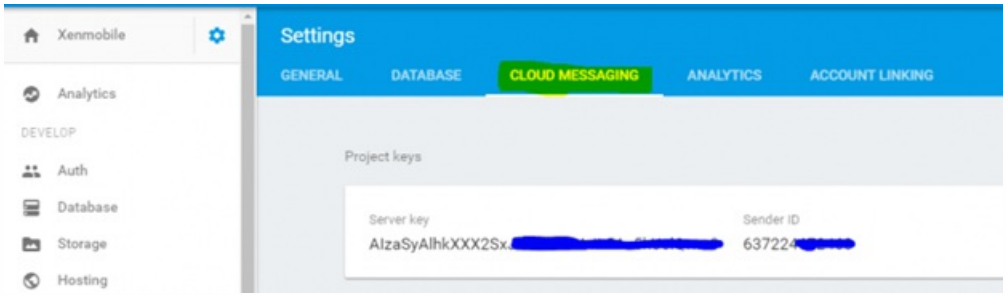
-
-
-
-

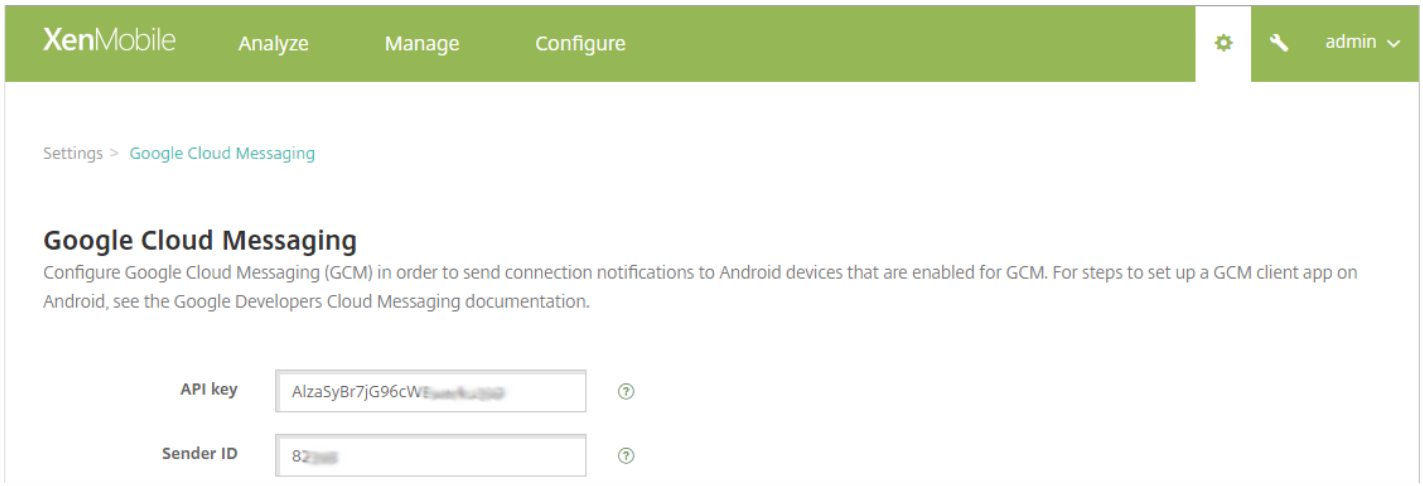


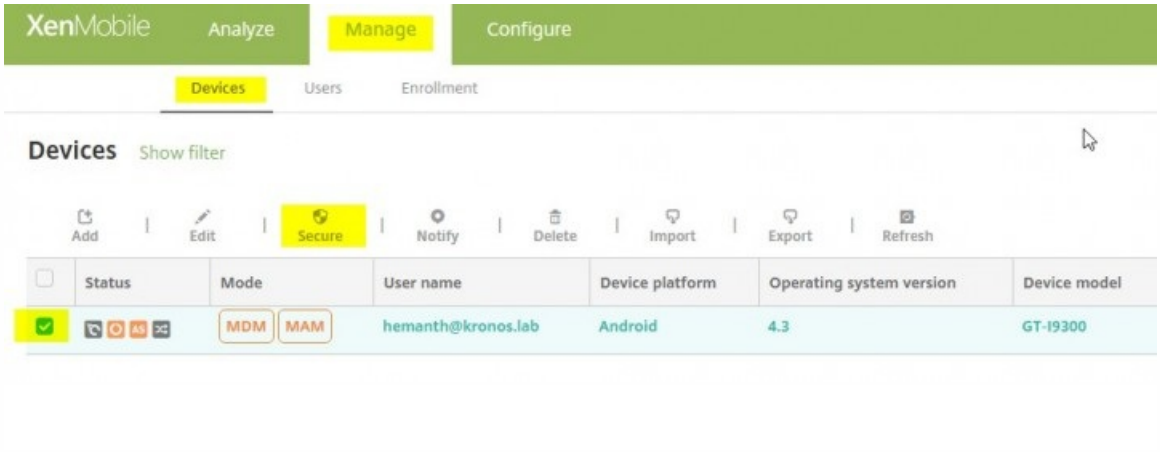


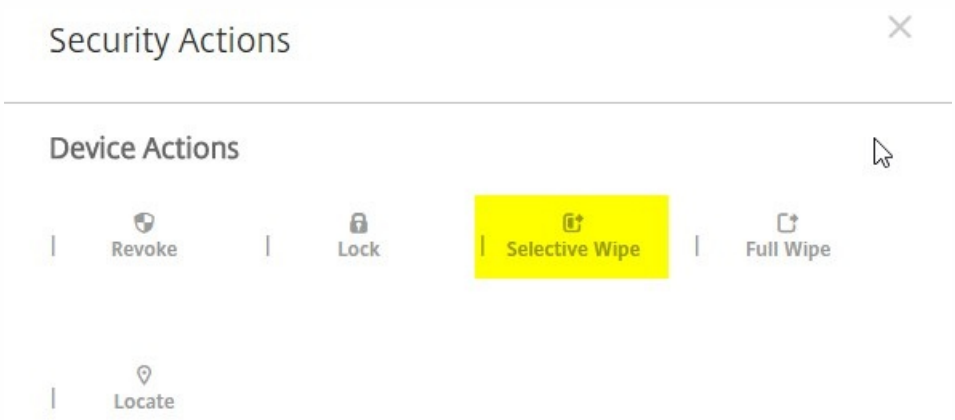


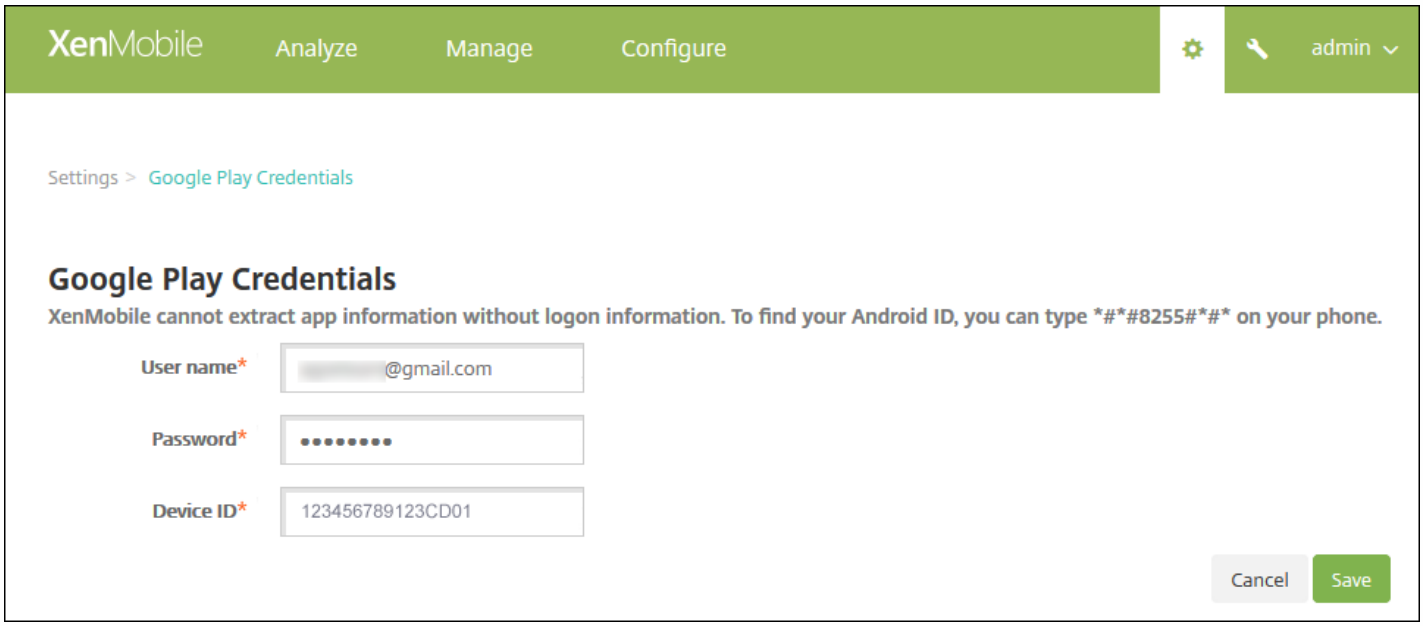












-
-
-

-
-

	• •
	•

	• •

	• • • •

	• •
	• • •

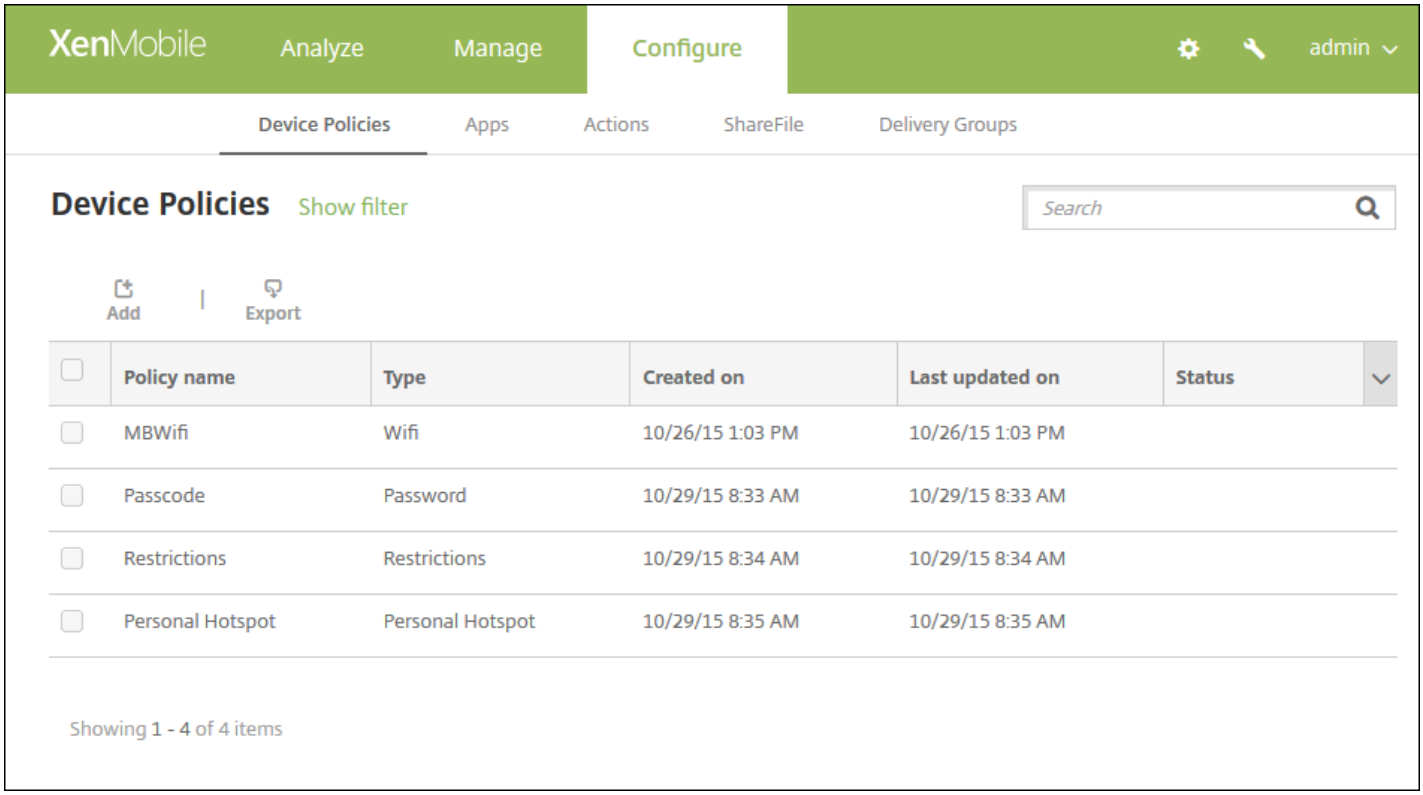
	• •

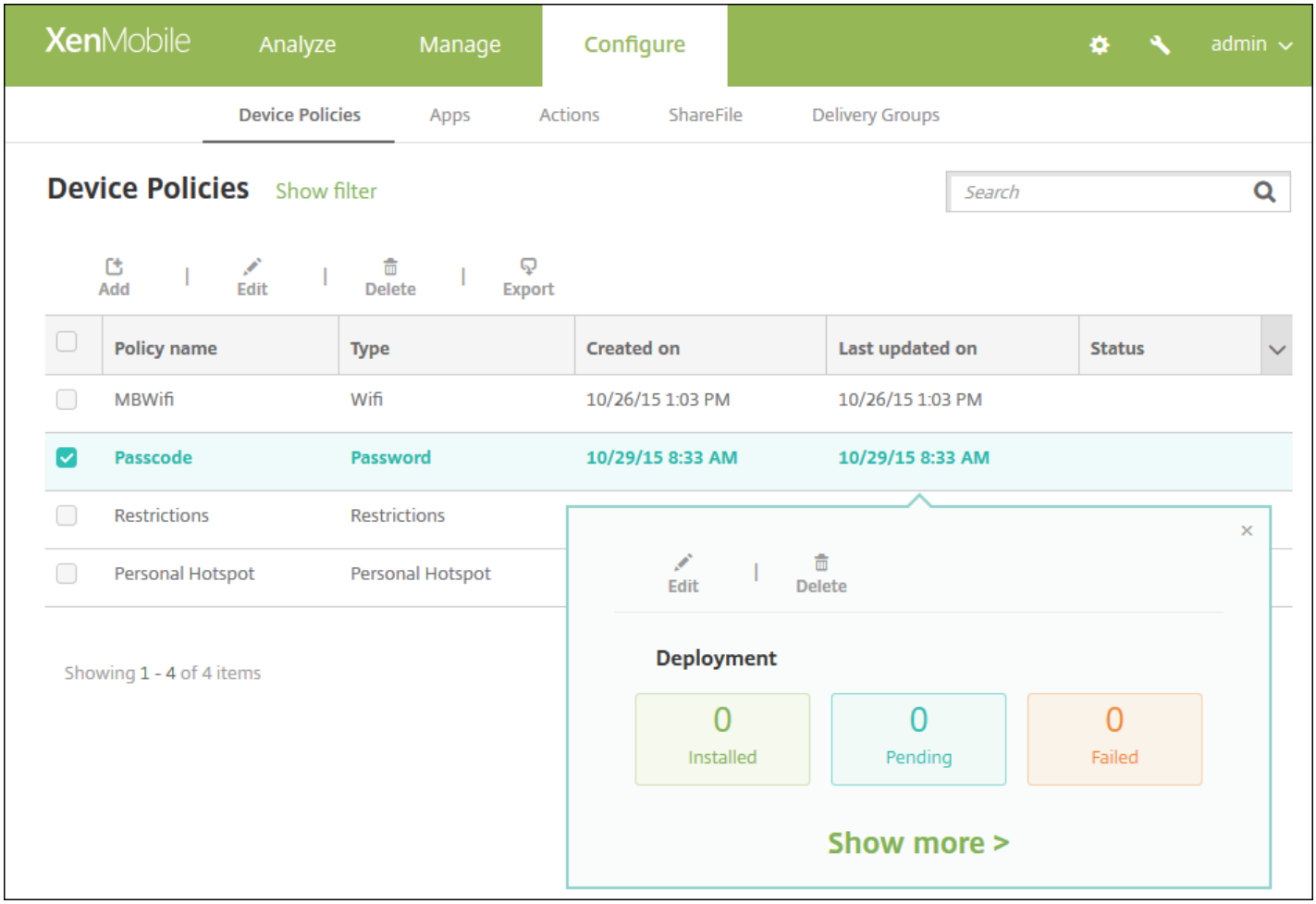
	• •

	• •

	• •

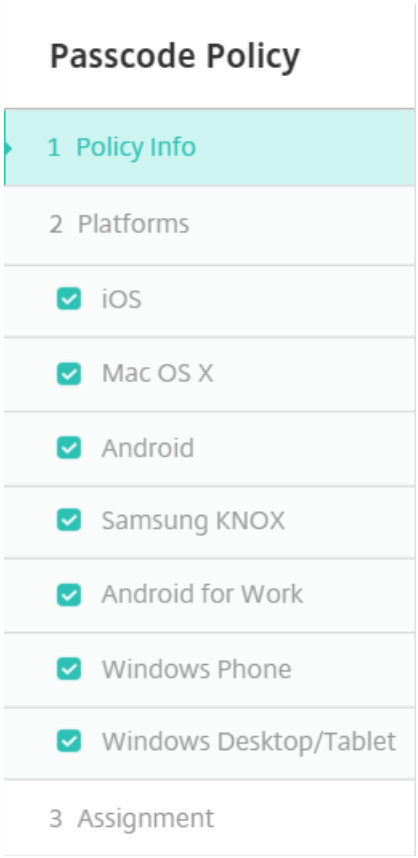
The Device Policies Page in the Console

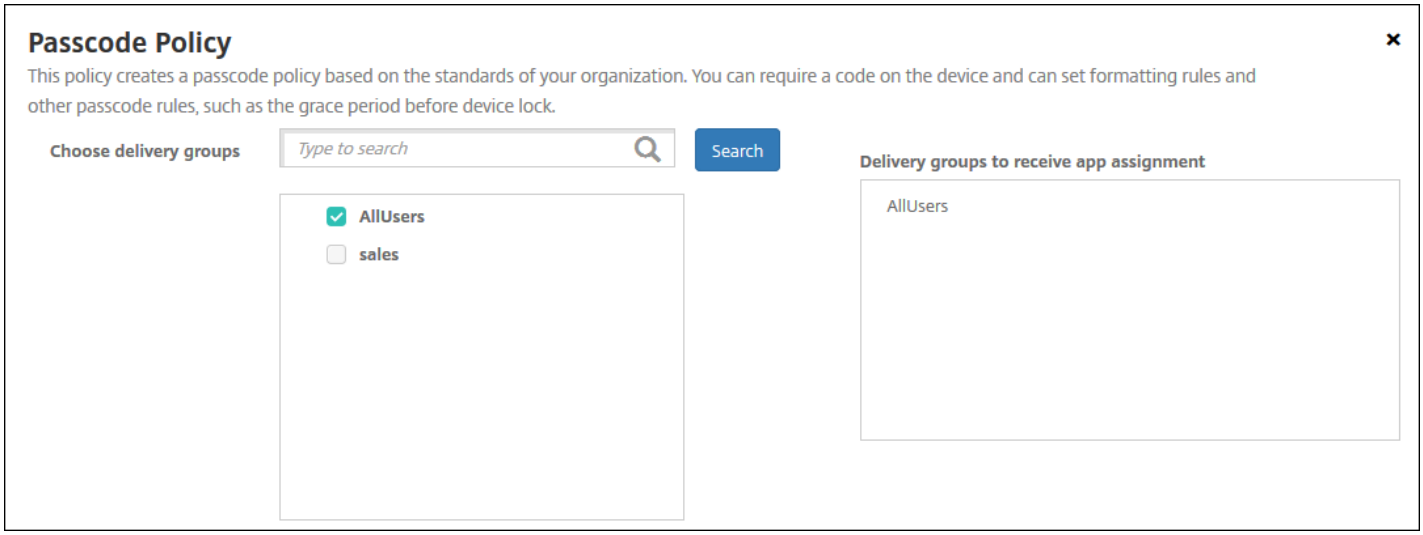




To add a device policy

-
-

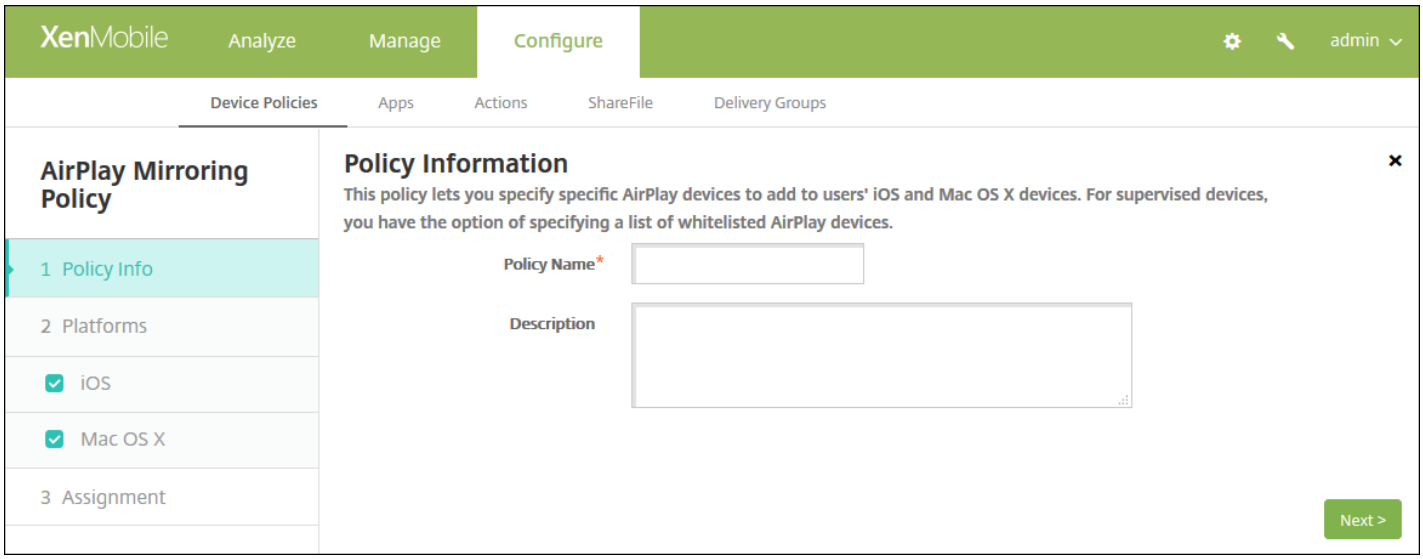




To edit or delete a device policy

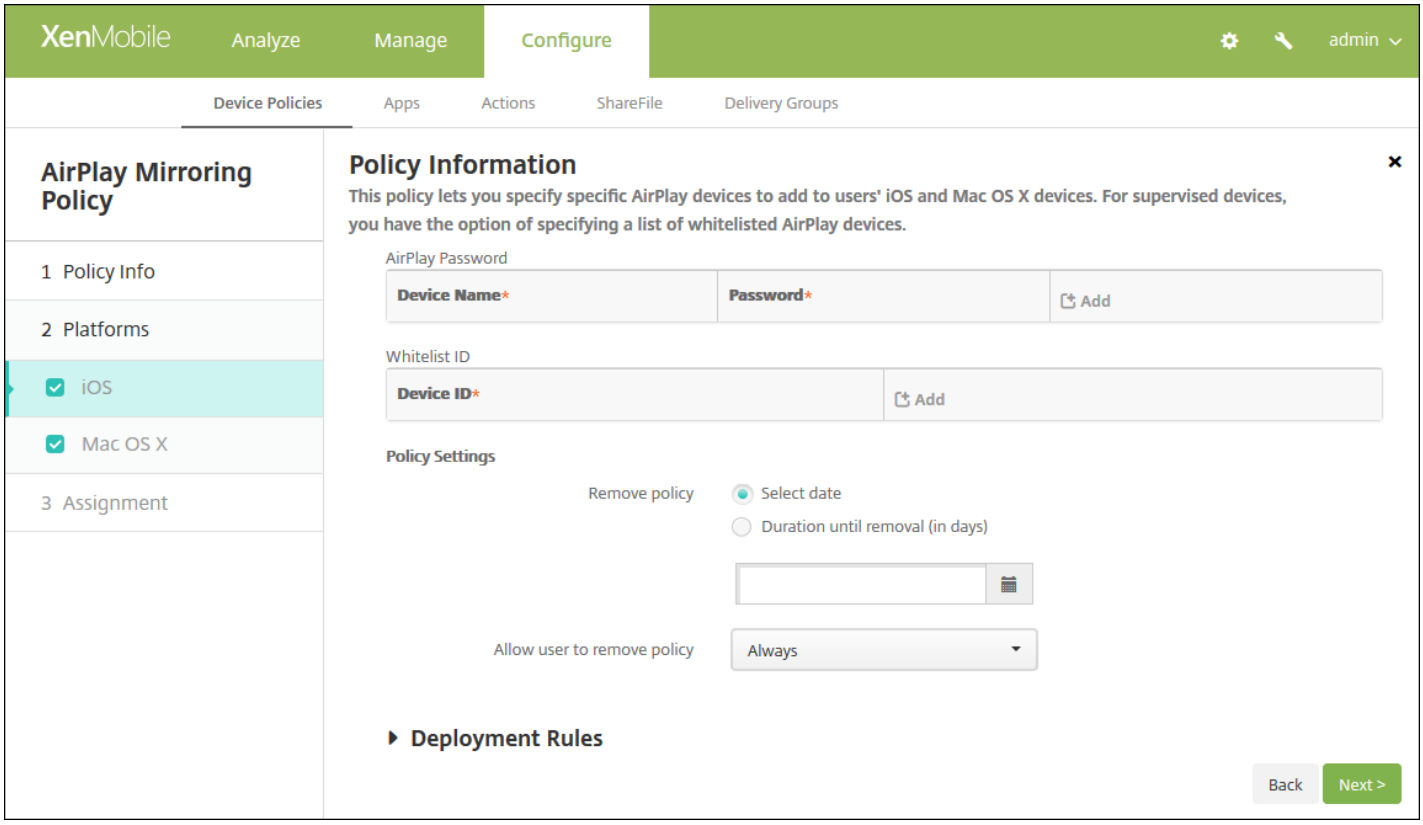
-
-

-
-
-
-
-
-
-
-
-
-
-



-
-

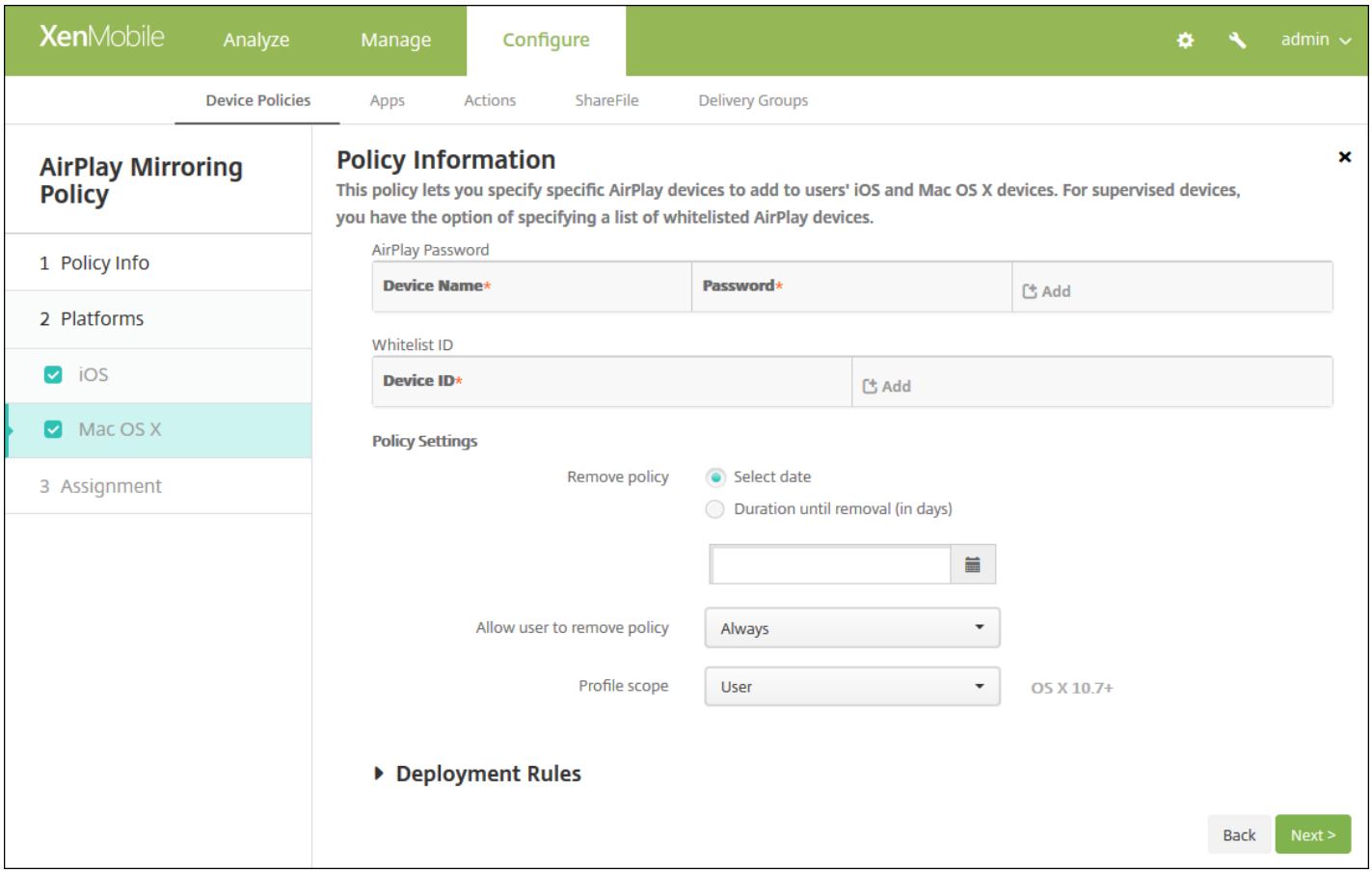
Configure iOS settings



-
  -
  -
  -
-
  -
  -
-
  -
  -

-
-

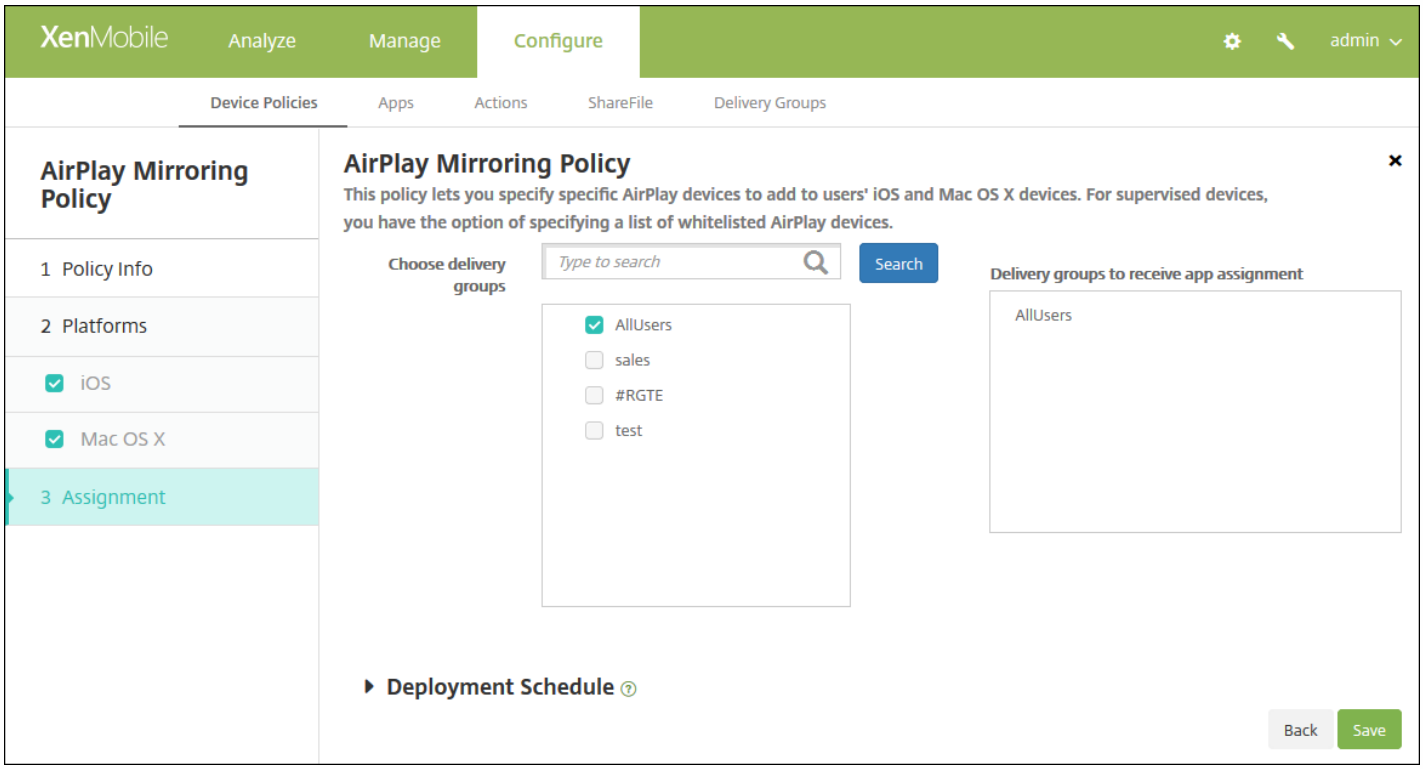
Configure Mac OSX settings



-
  -
  -
  -
-
  -
  -

-
  -
  -
  -
  -
  -

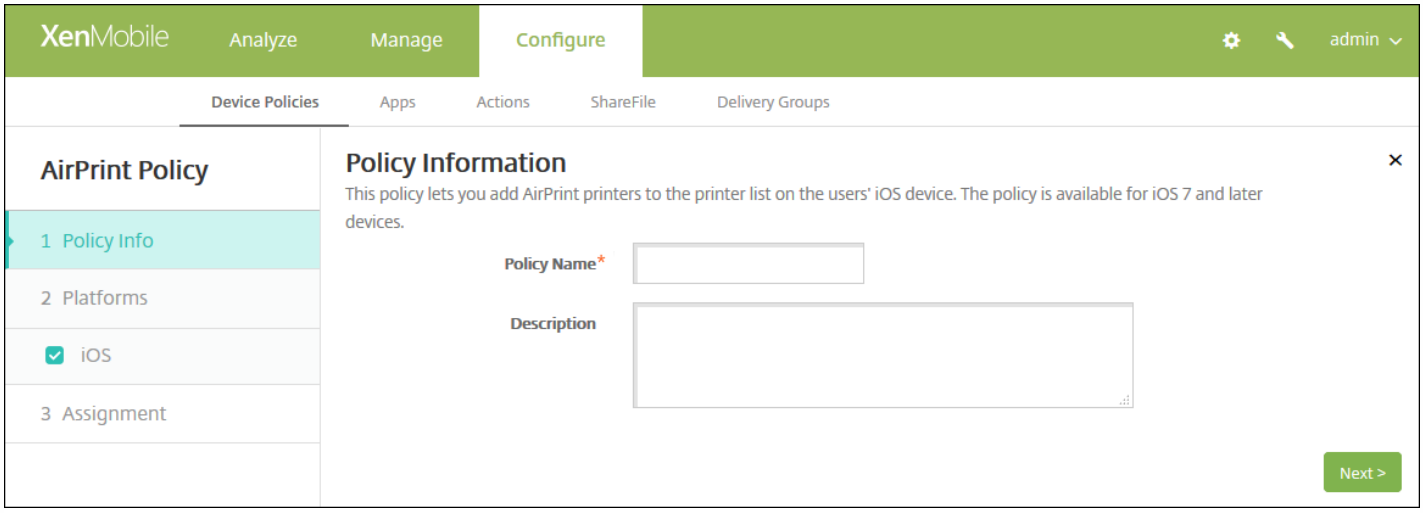
7. Configure deployment rules



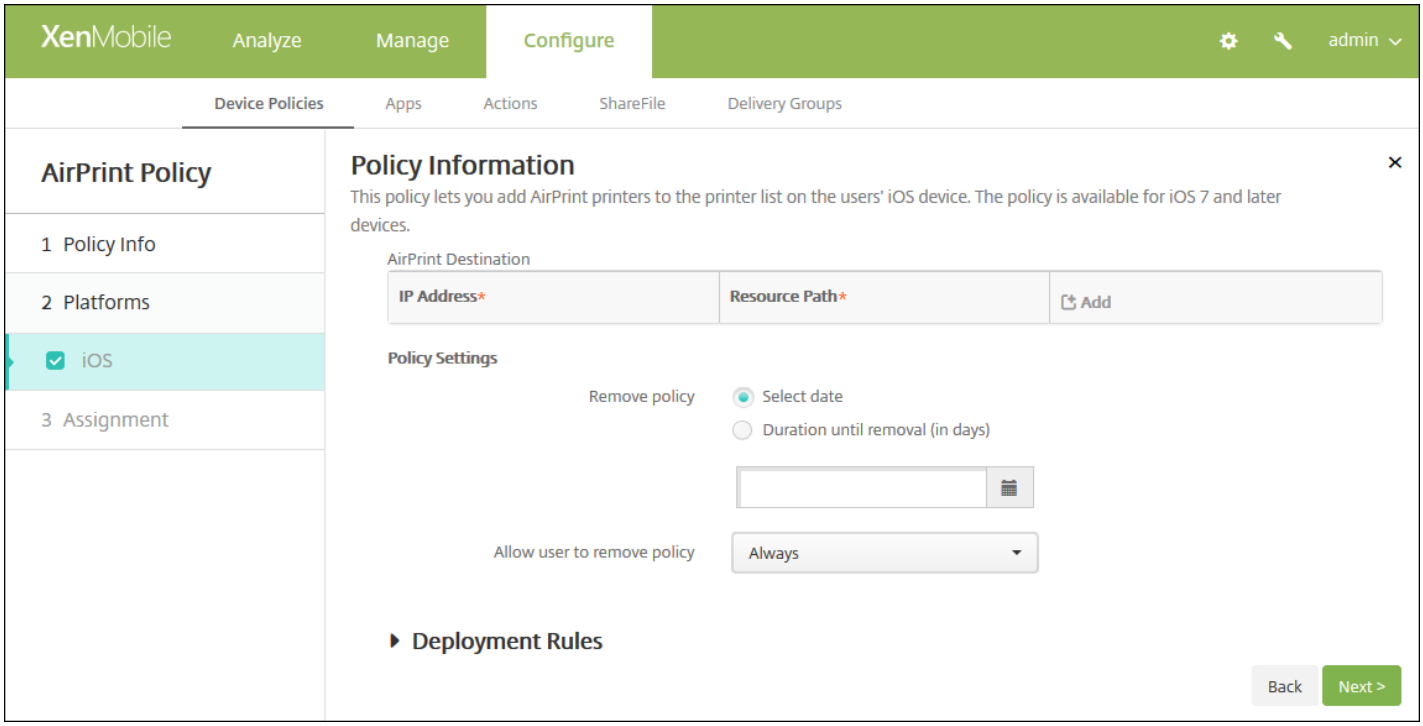
-
-
-
-

-
-

-
-

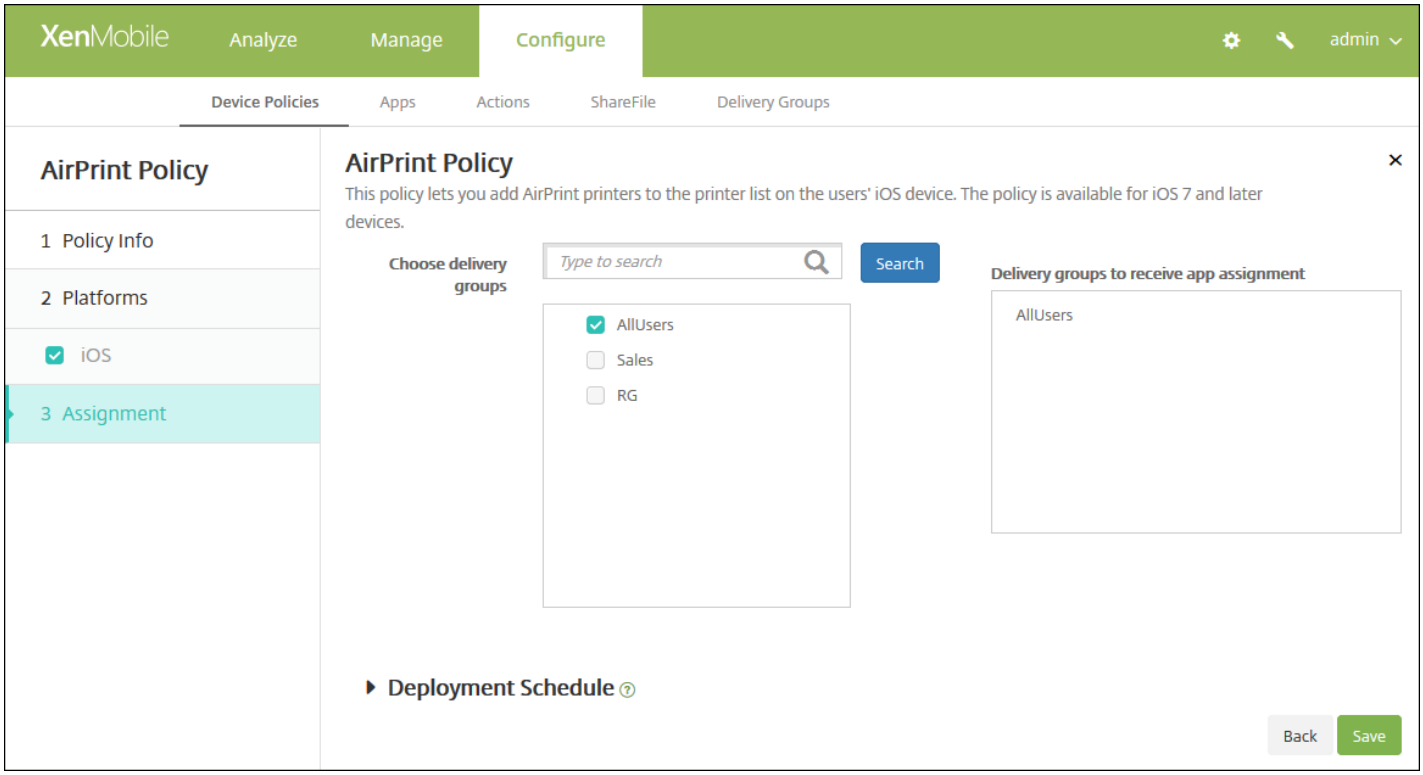


-
-

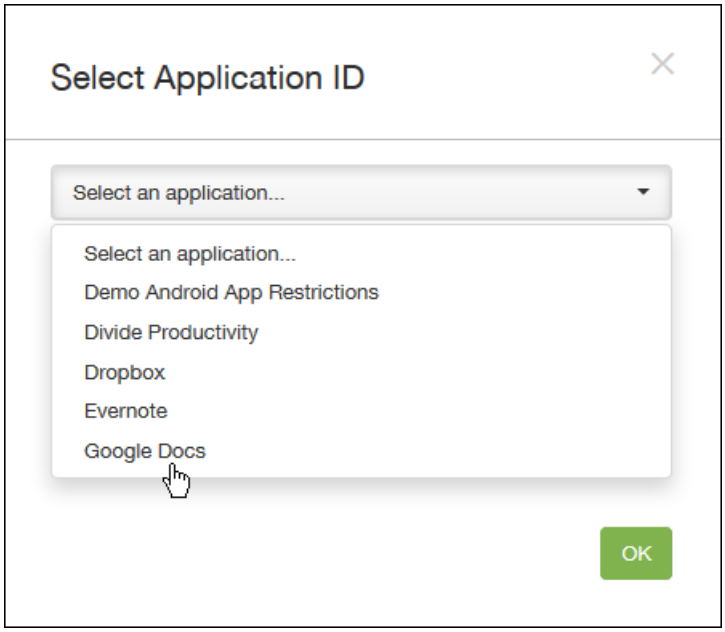


-
  -
  -
  -
-
  -
  -
  -
  -
  -

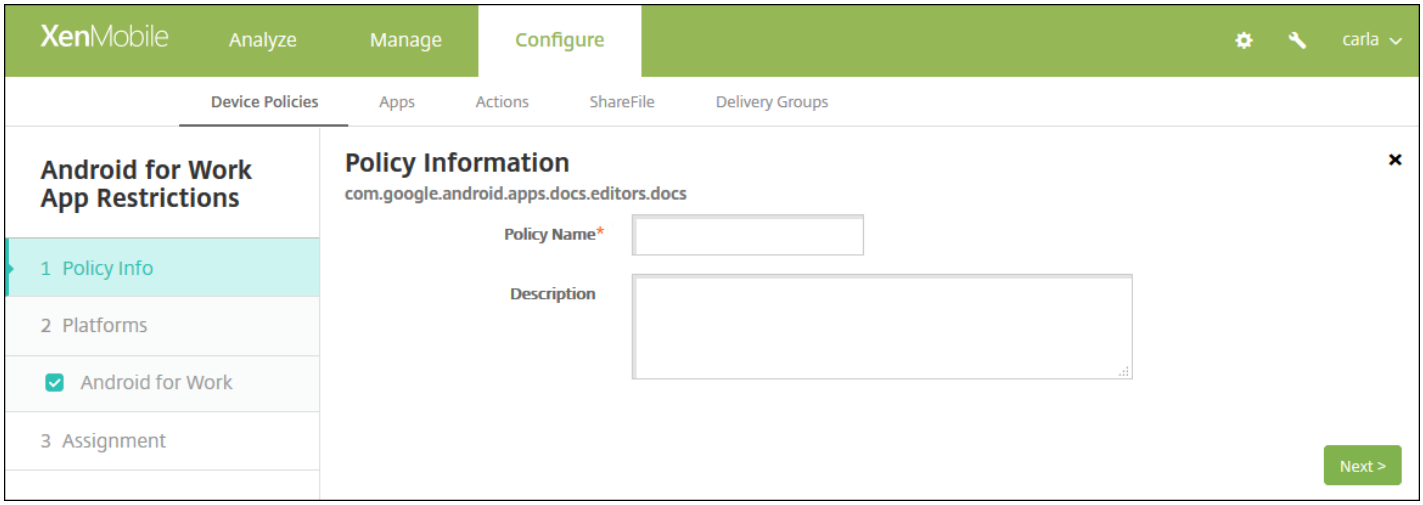
7. Configure the deployment rules



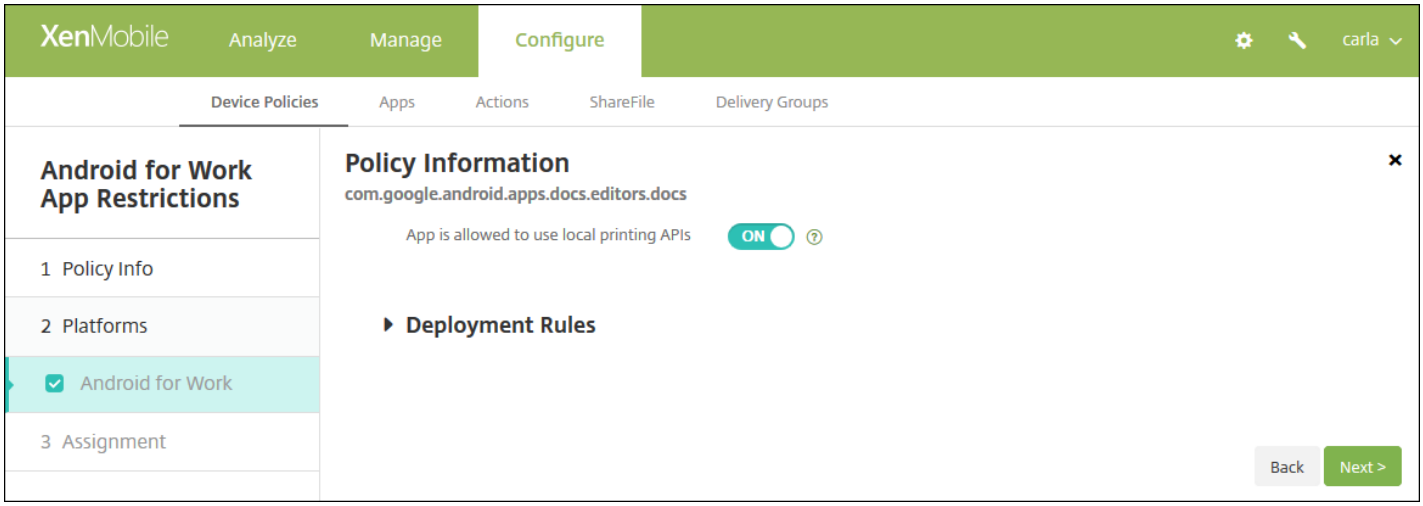
-
-
-



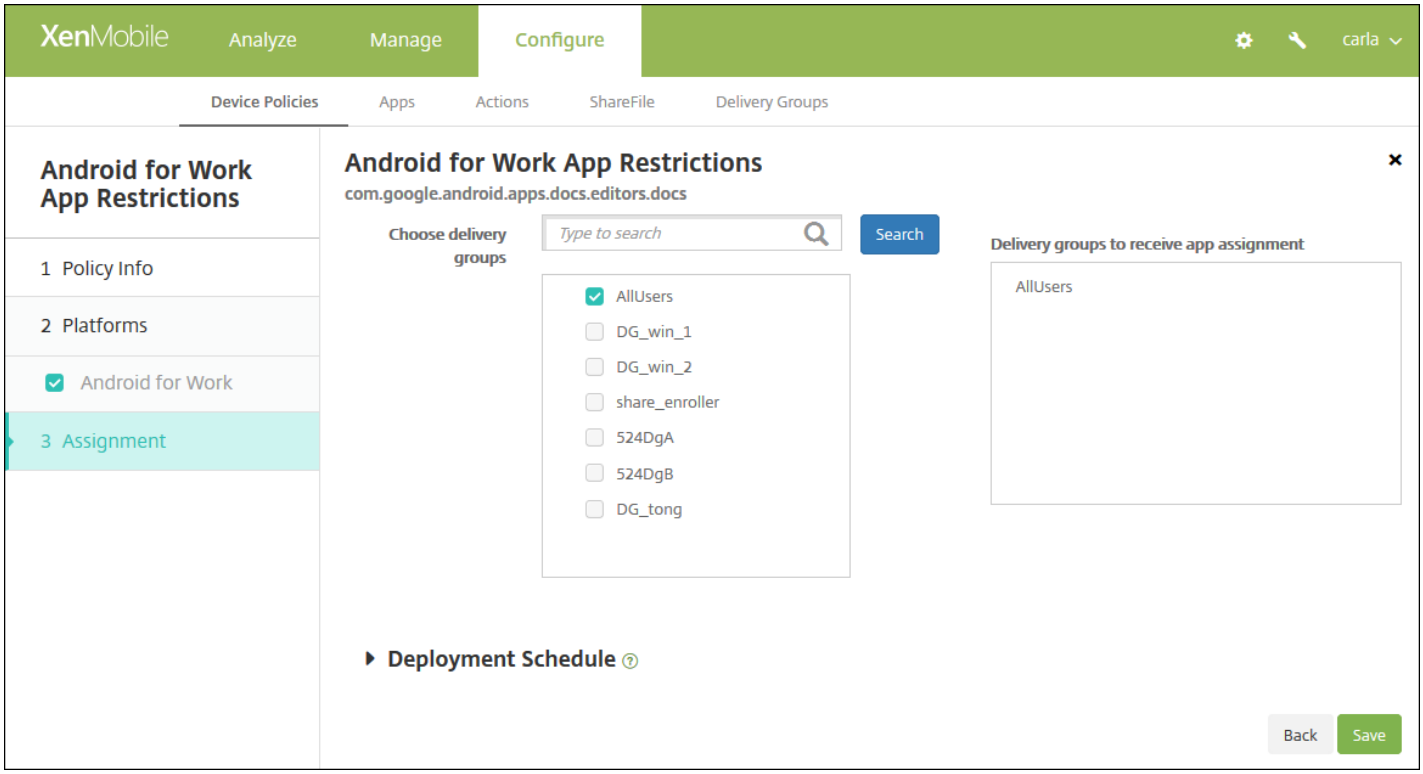
-
-
-



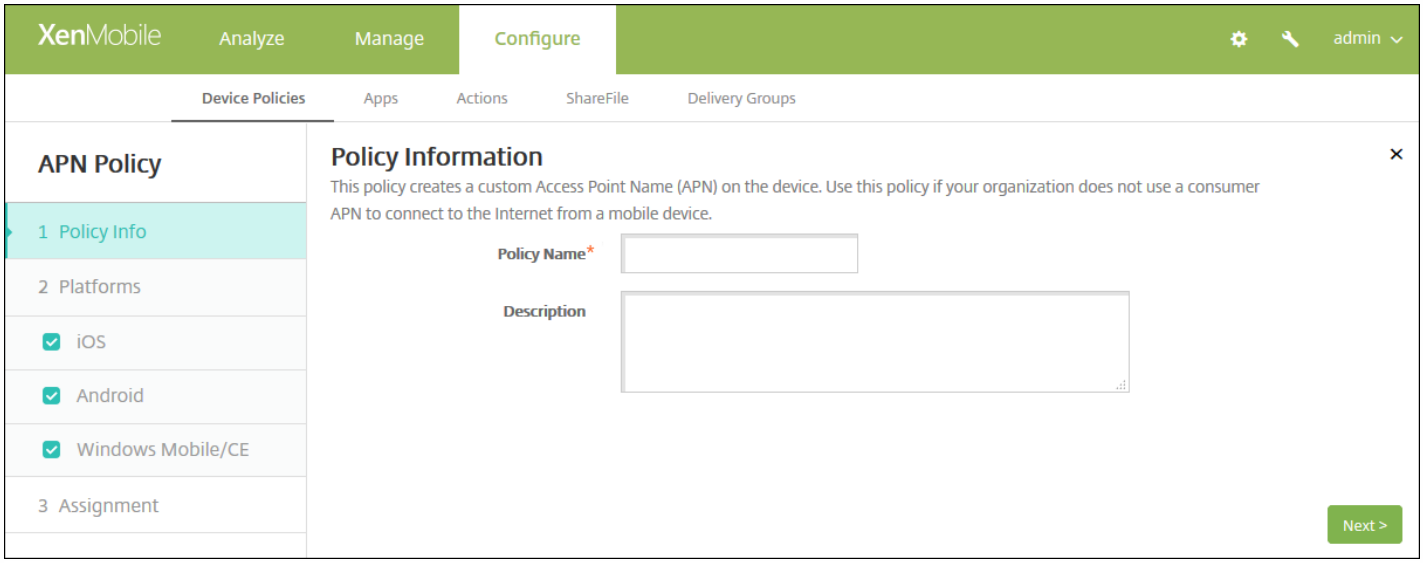
-
-



8. Configure the deployment rules

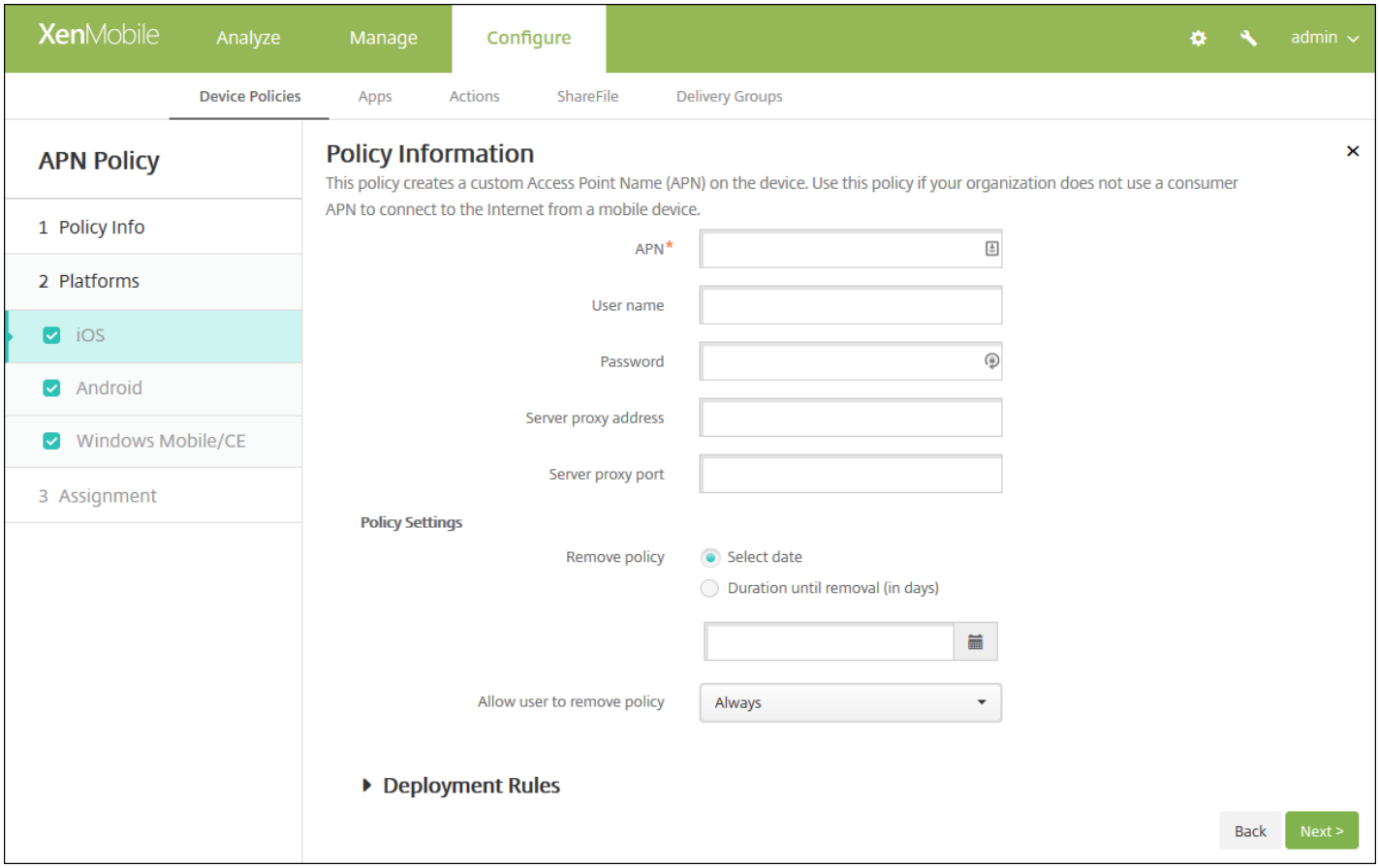


-
-
-
-
-
-
-



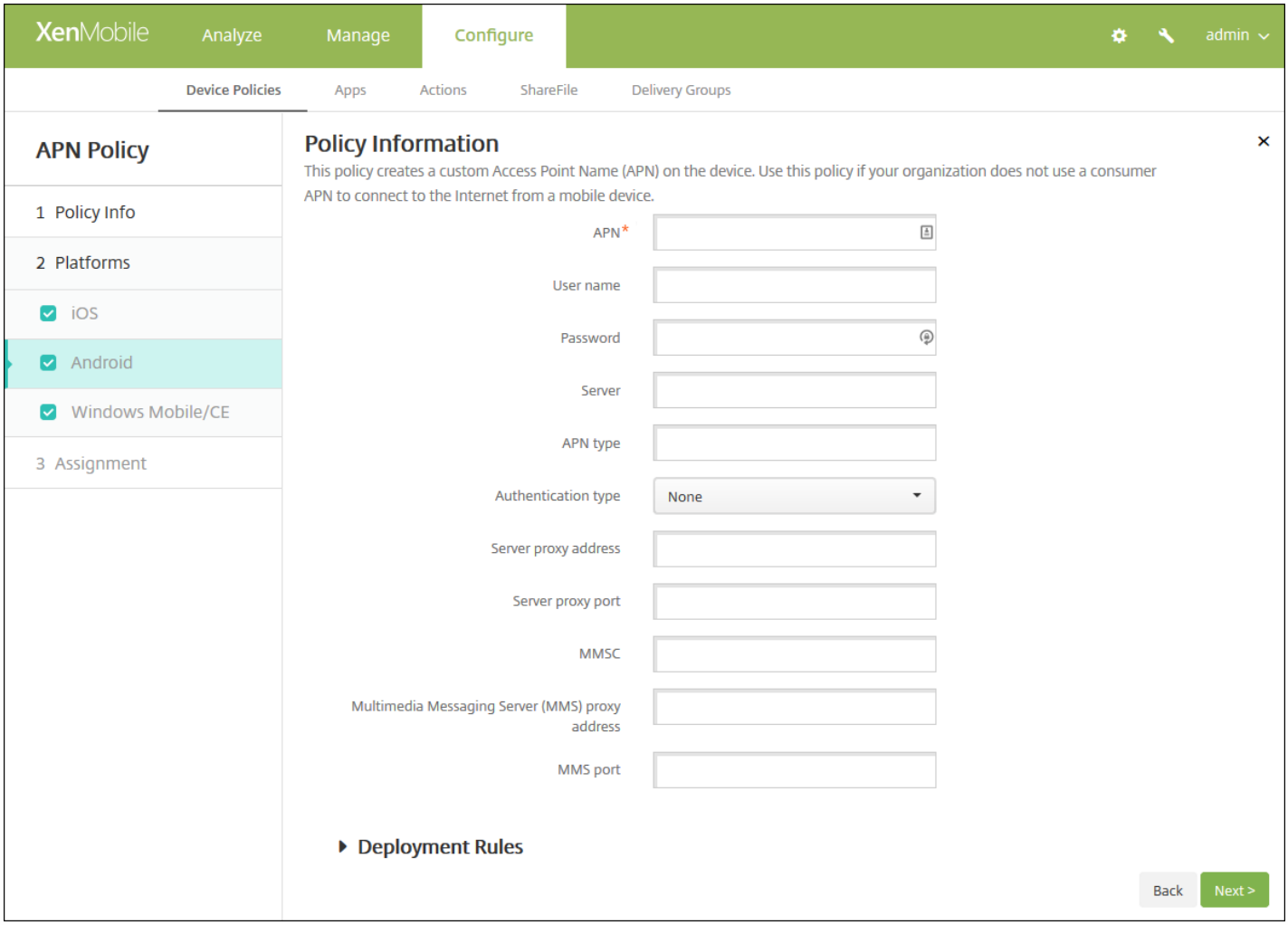
-
-

Configure iOS settings



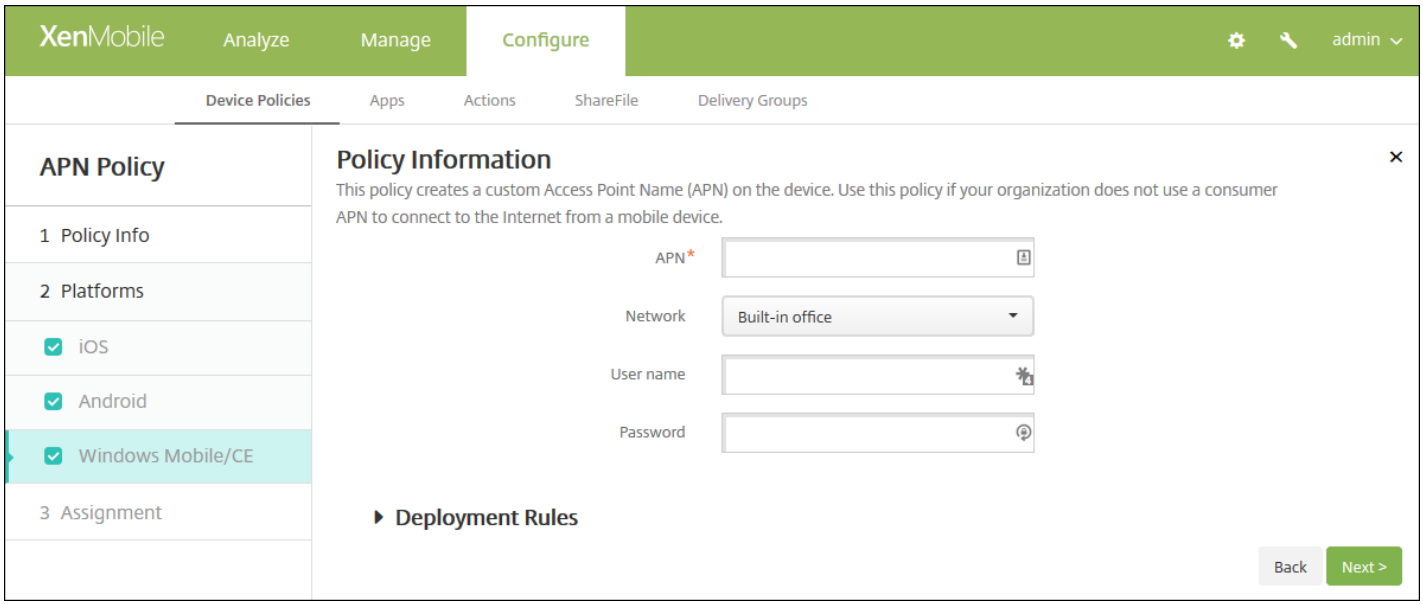
-
-
-
-
-
-
  -
  -
  -

Configure Android settings



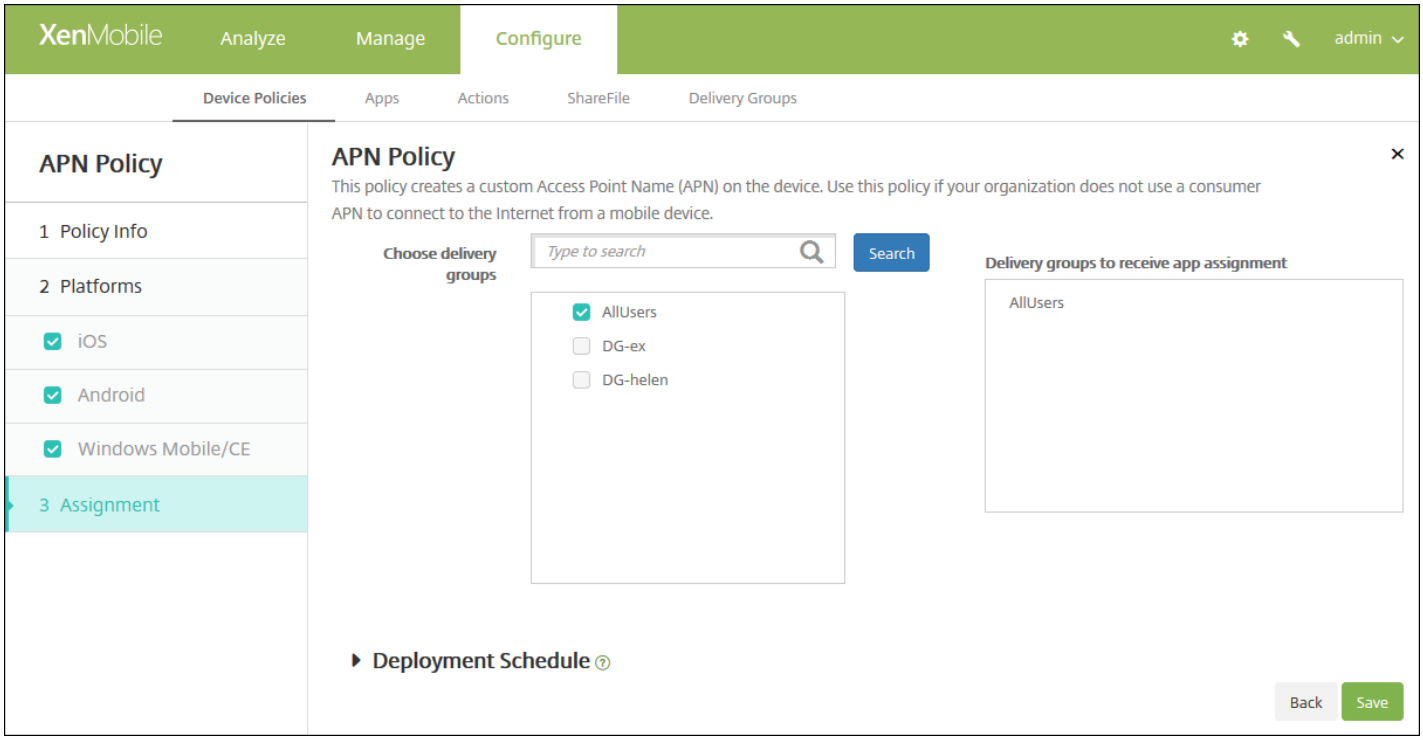
-
-
-
-
-
-

Configure Windows Mobile/CE settings

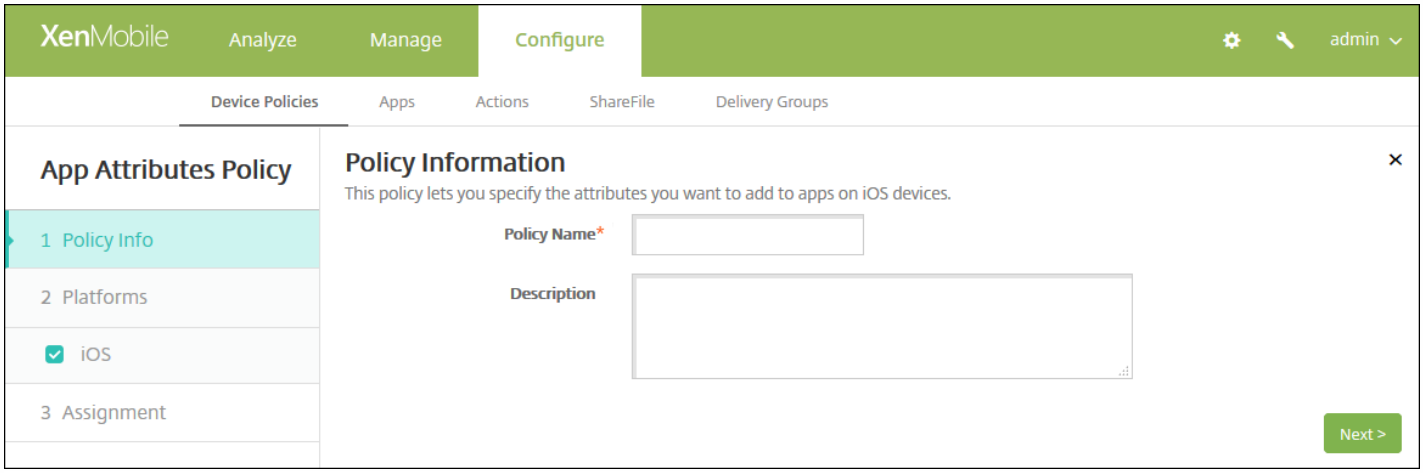


-
-
-
-

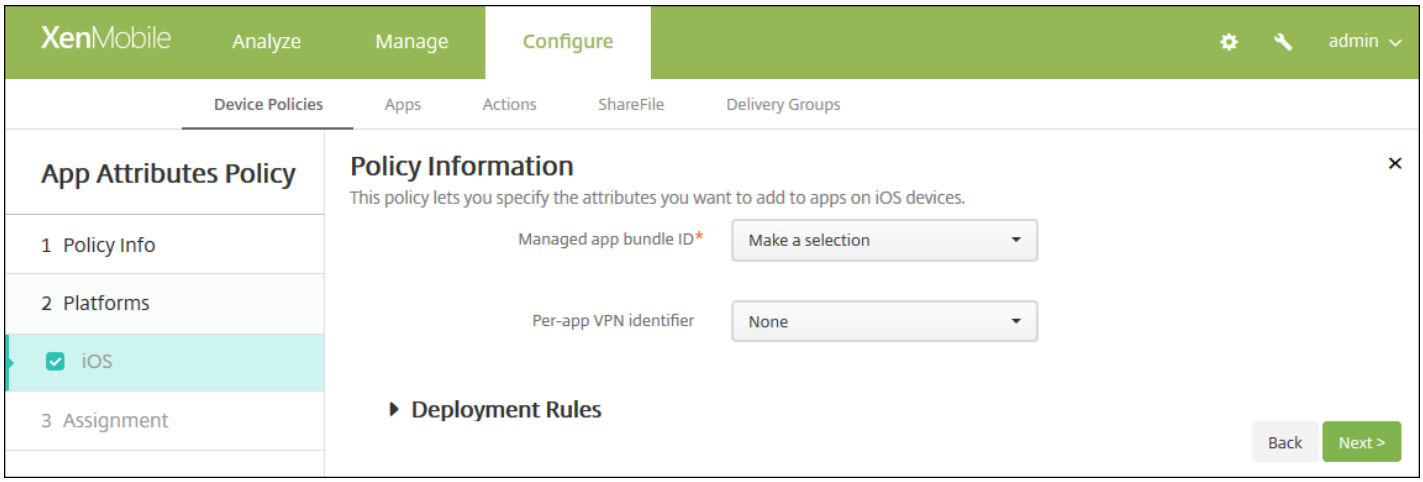
7. Configure the deployment rules



-
-
-
-
-
-
-

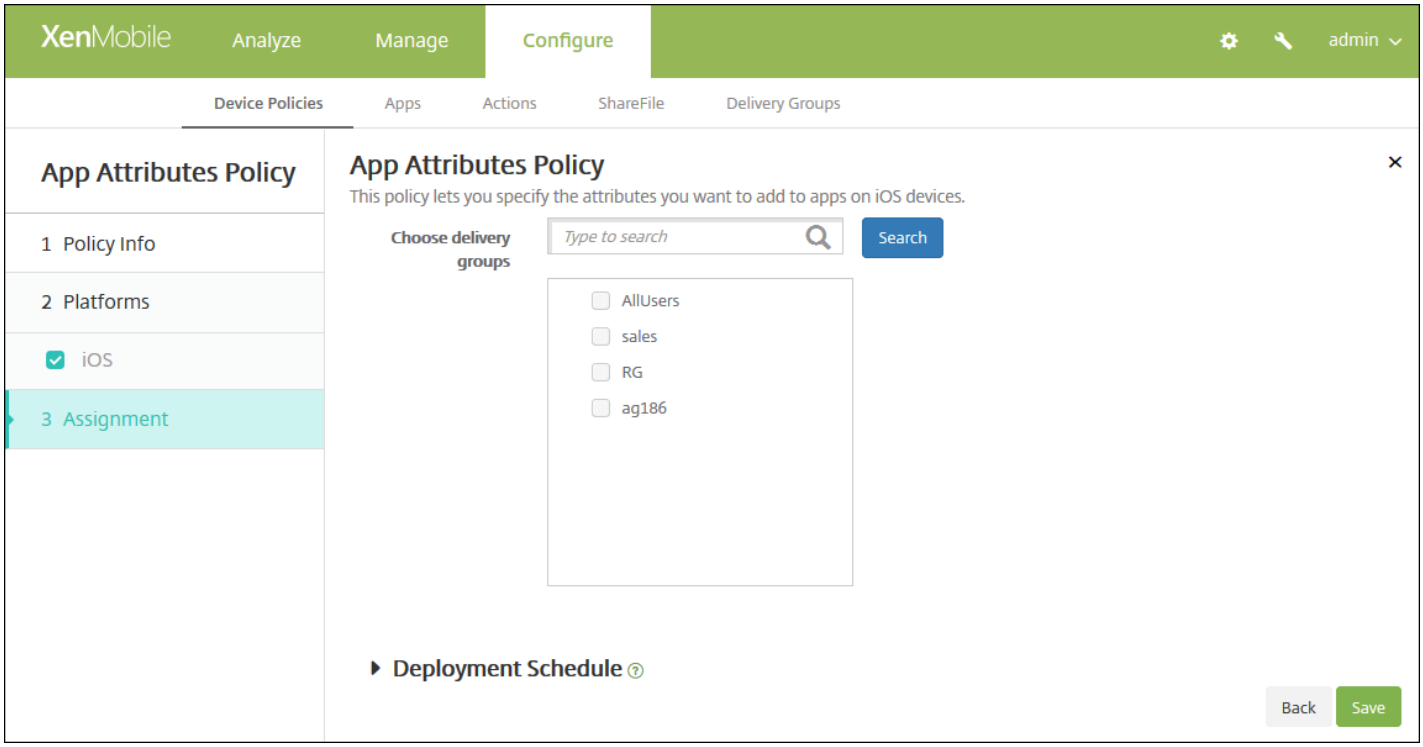


-
-

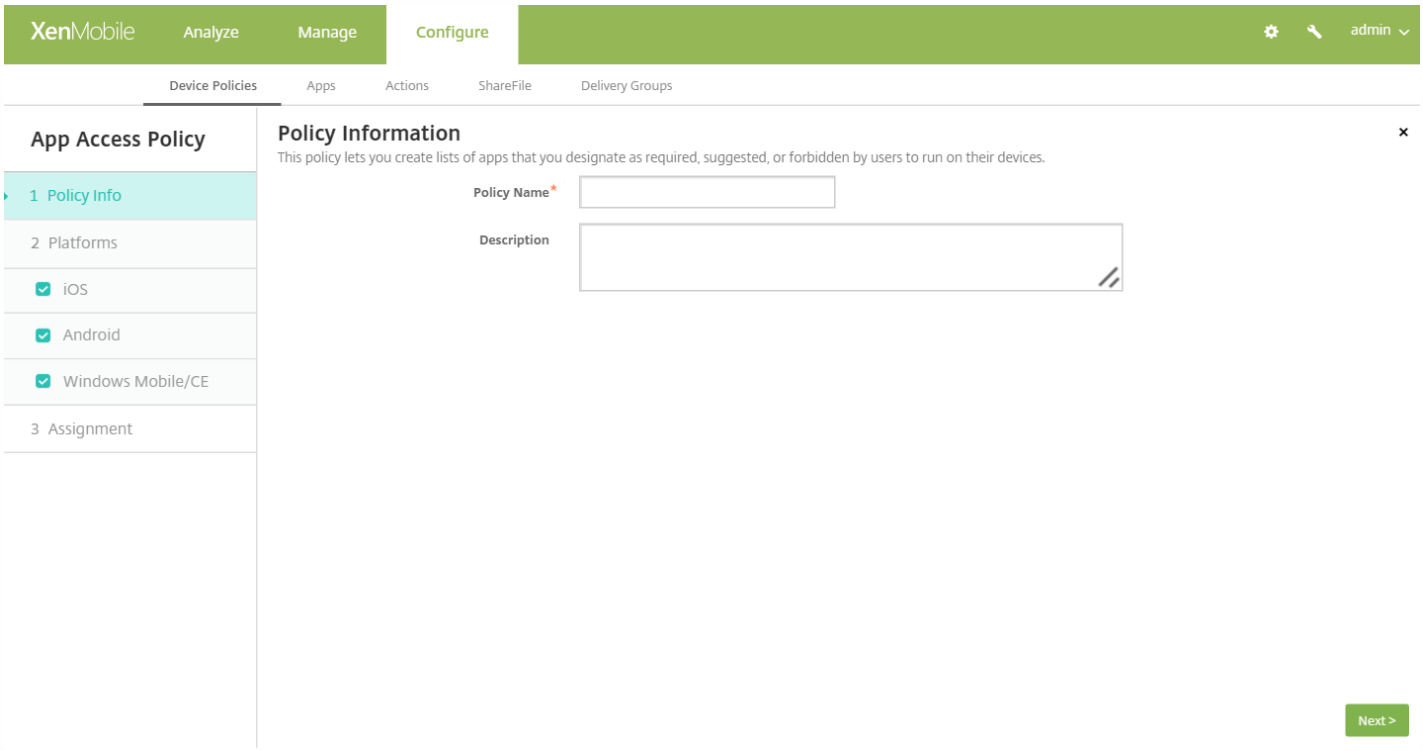


-
  -
-

7. Configure the deployment rules



-
-
-
-
-
-
-

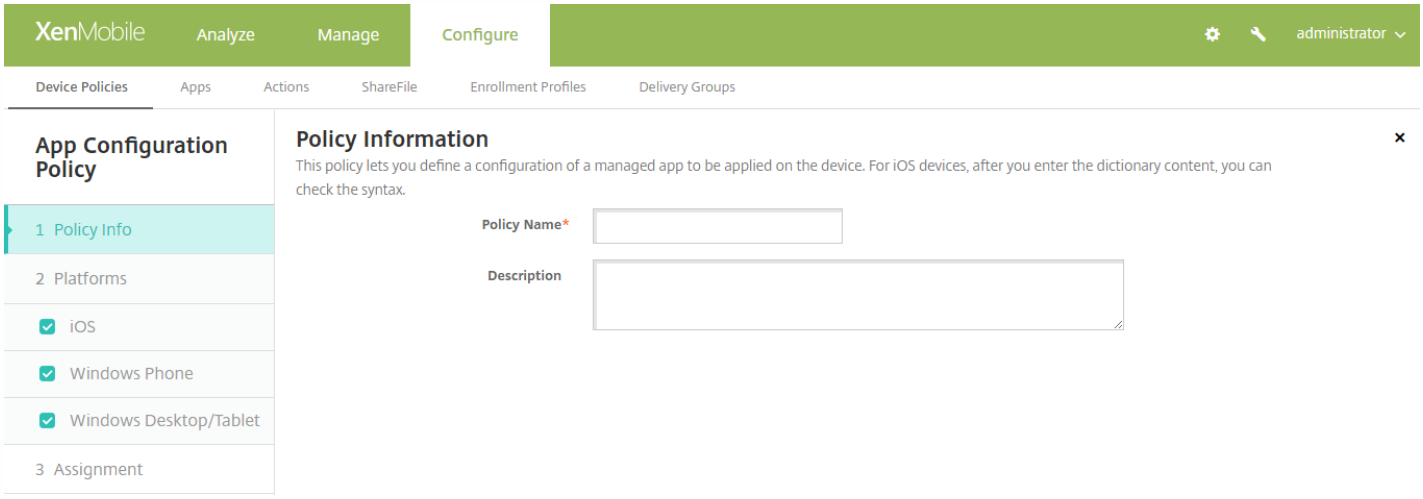


-
-

-
-
  -
  -
  -
  -

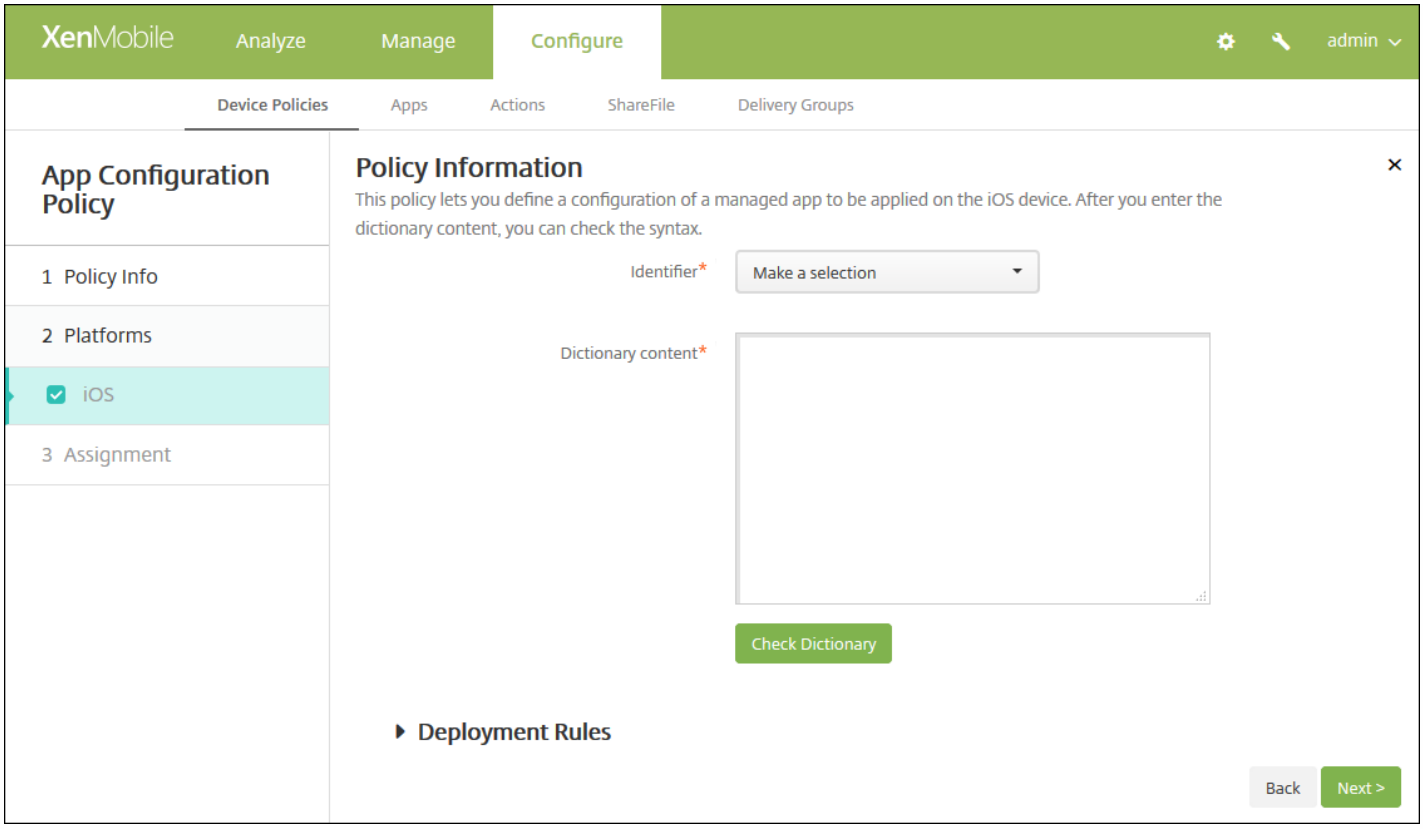
7. Configure the deployment rules

-
-
-
-
-
-
-

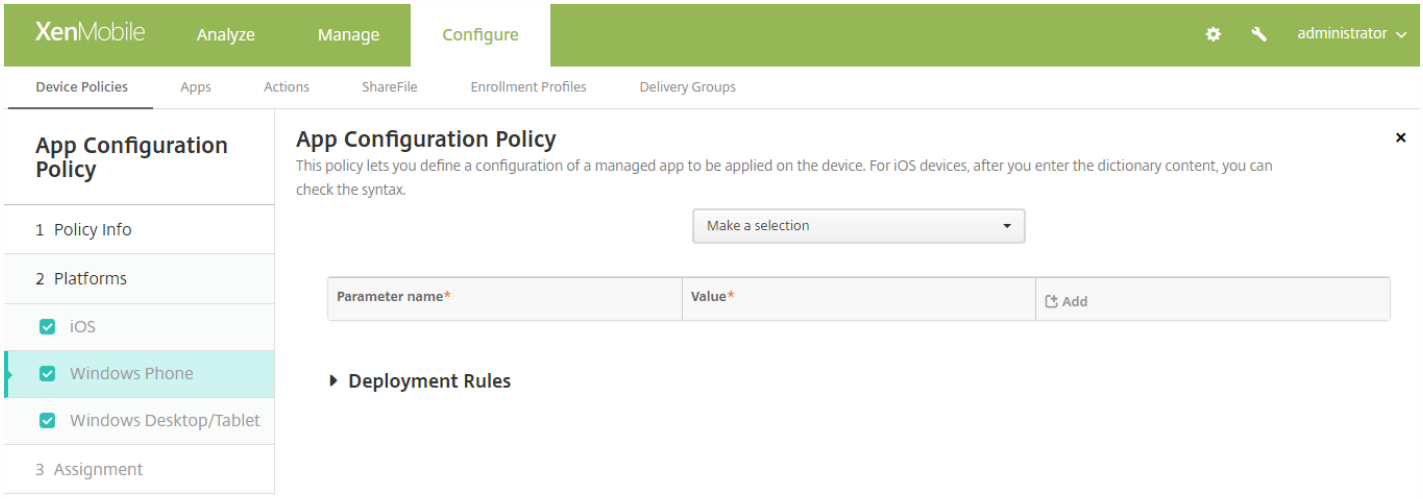


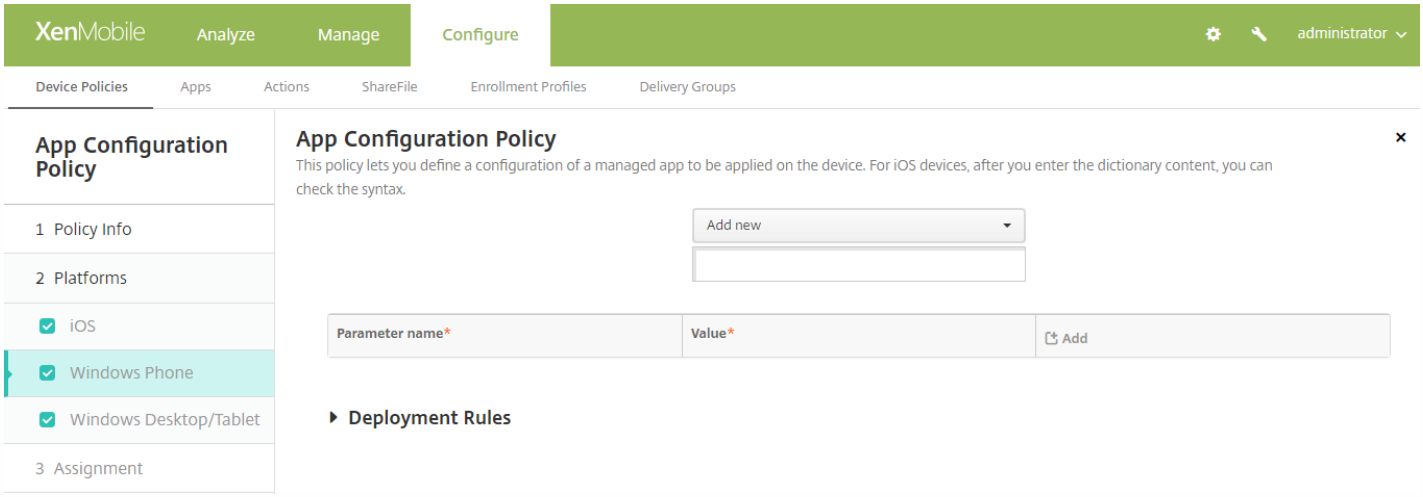
-
-

Configure iOS settings

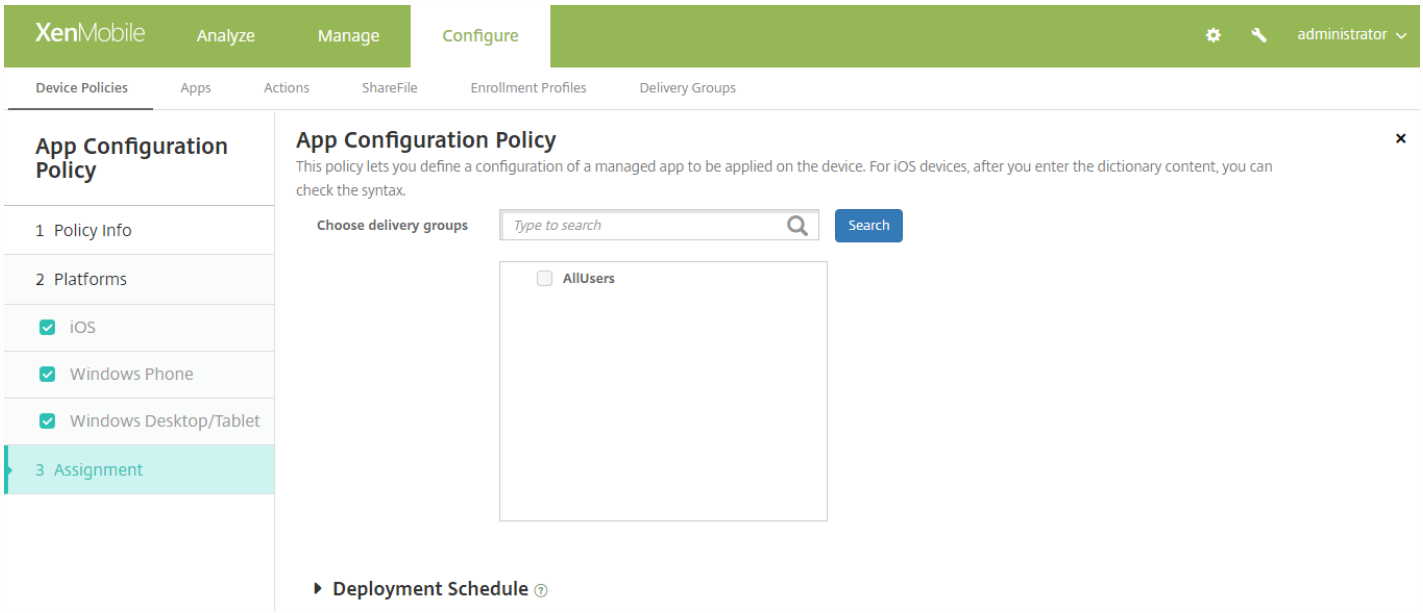


Configure Windows Phone or Desktop/Tablet settings



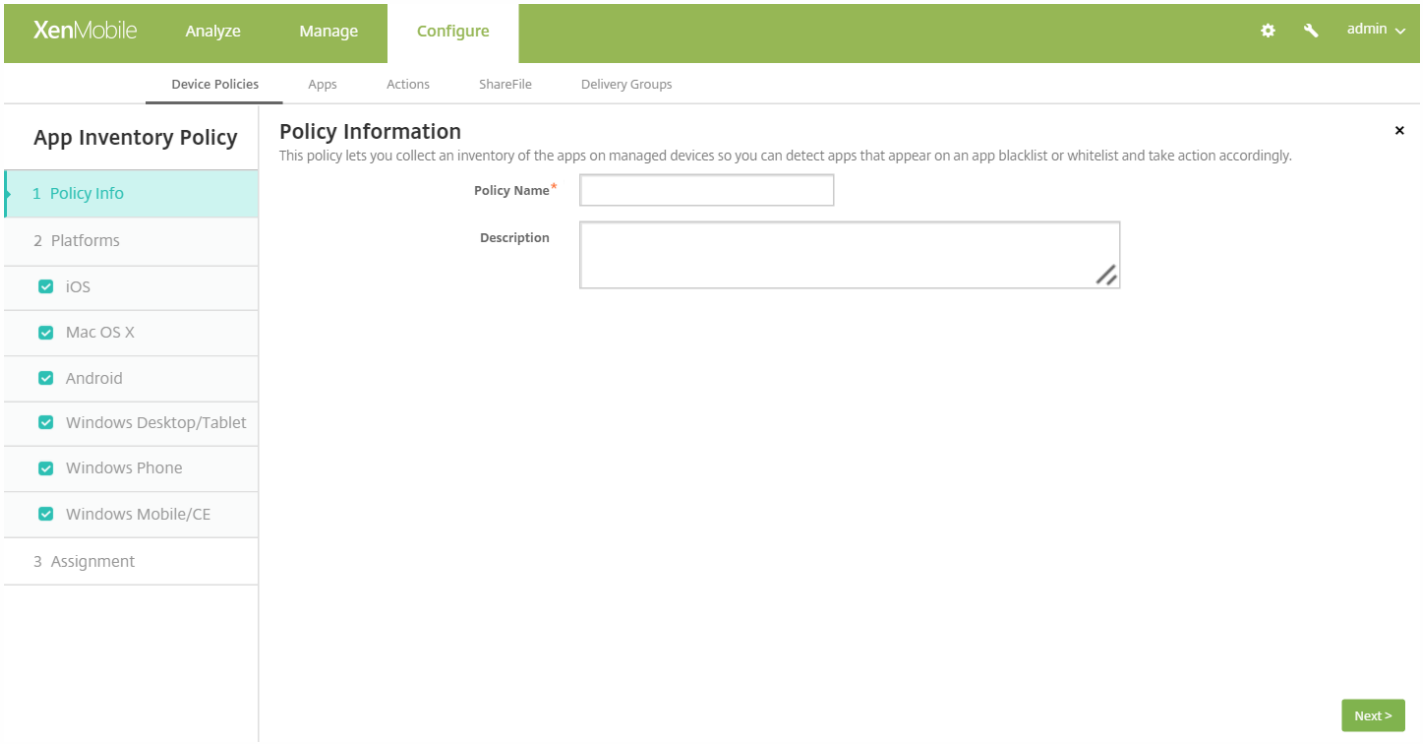


6. Configure the deployment rules

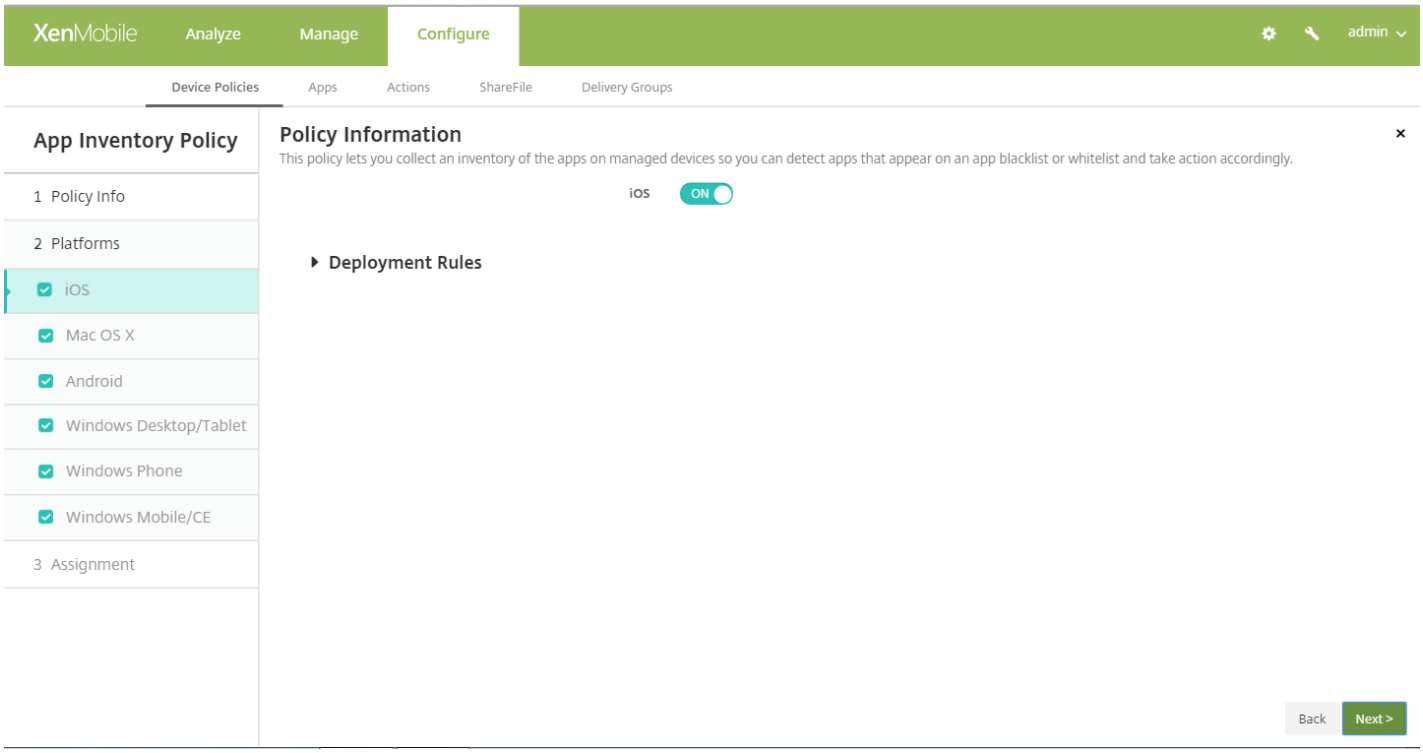


-
-
-
-
-

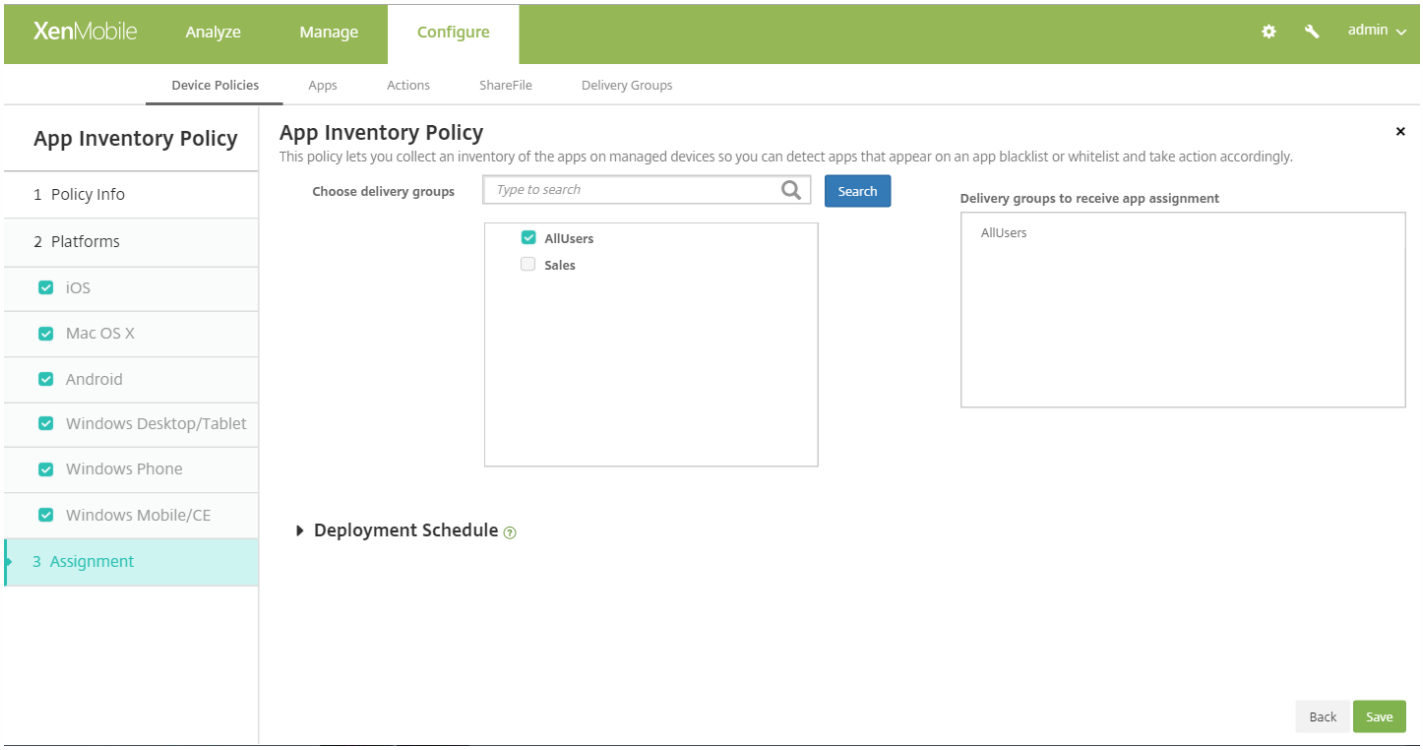
-
-



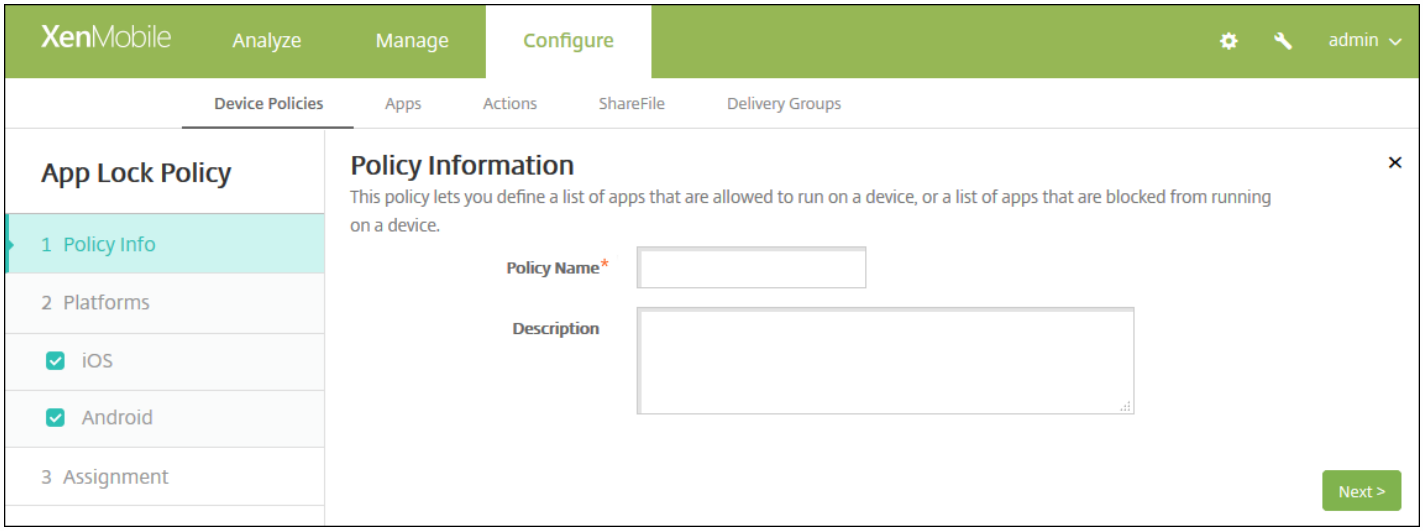
-
-



7. Configure the deployment rules

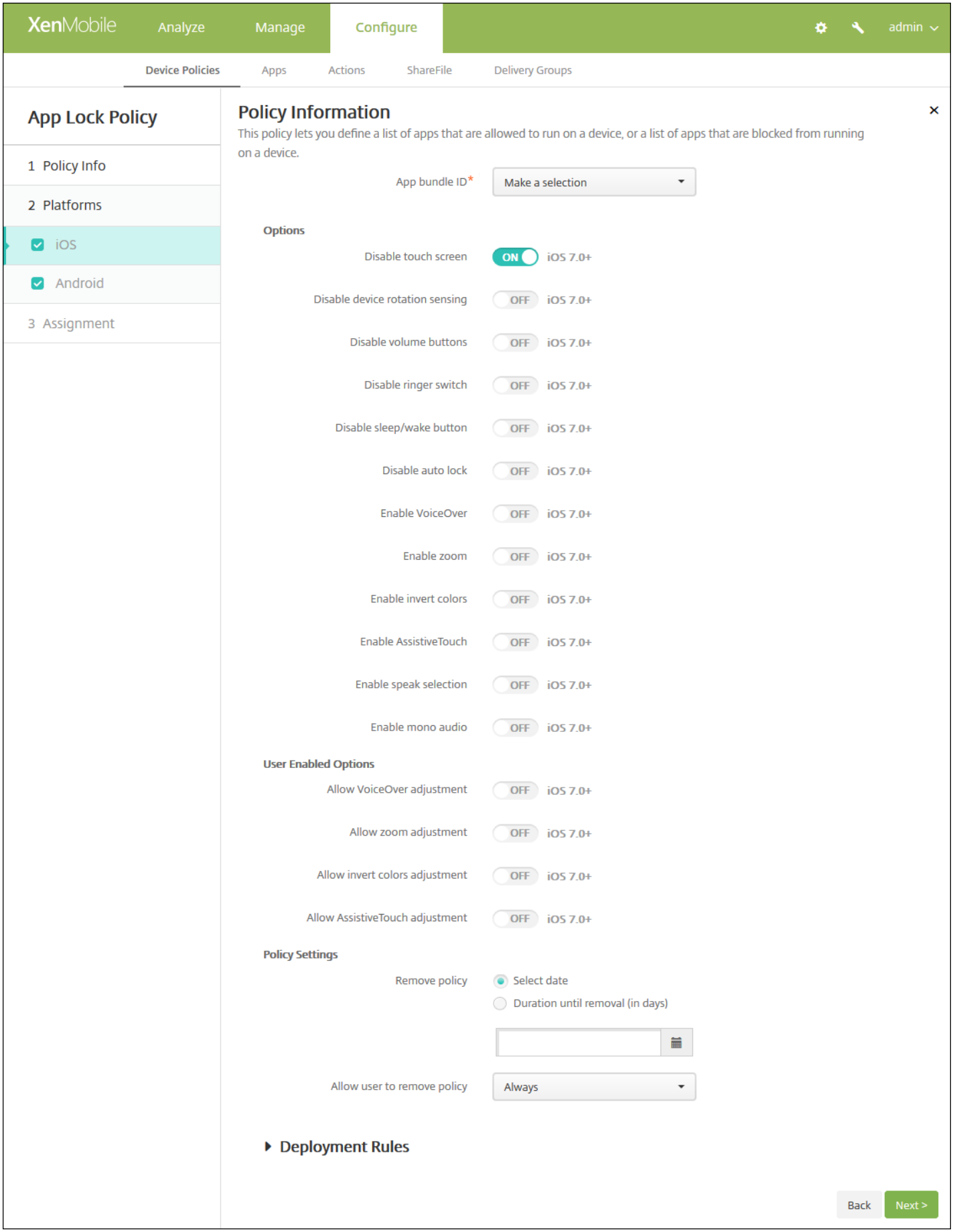


-
-
-
-
-
-
-



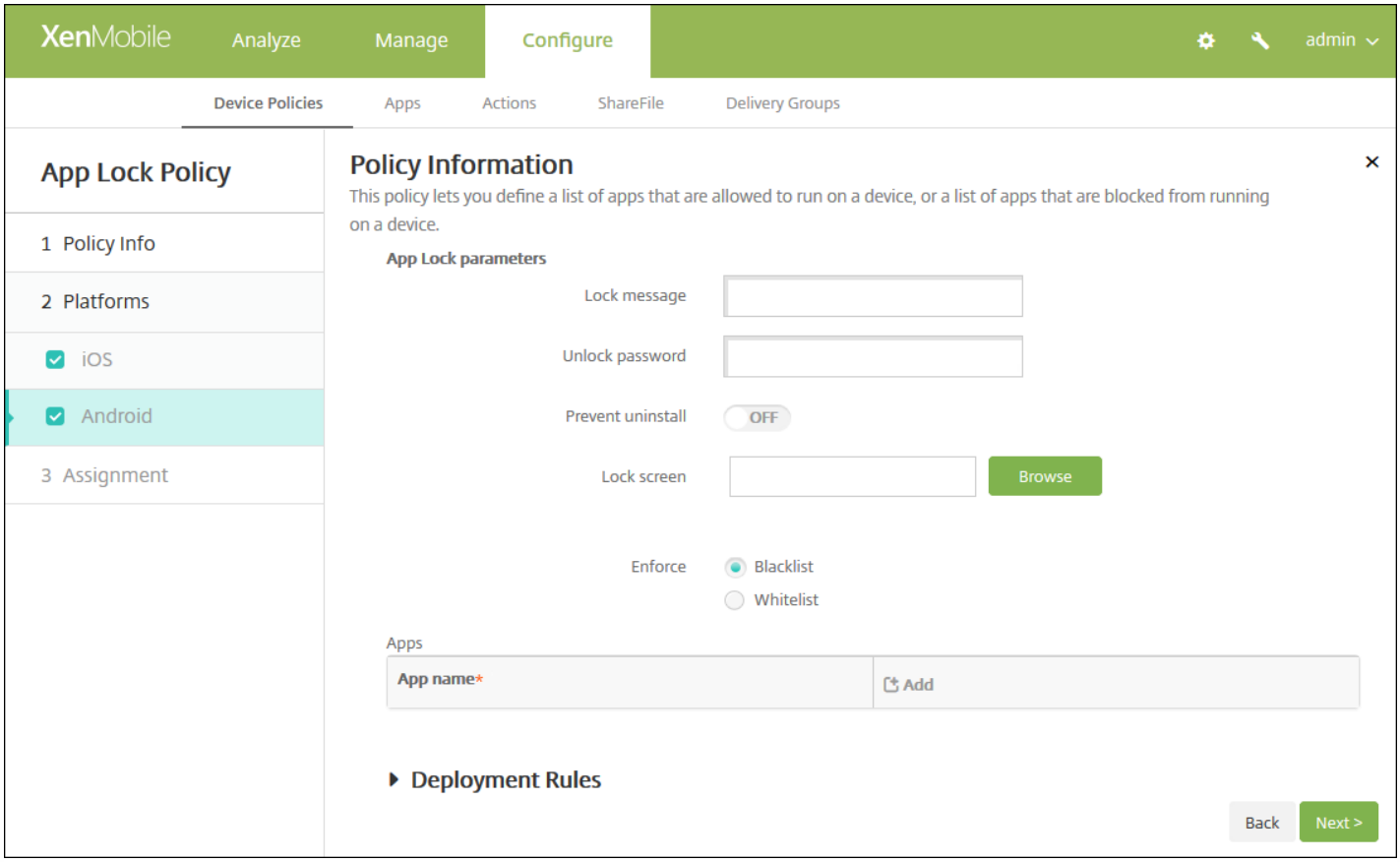
-
-

Configure iOS settings



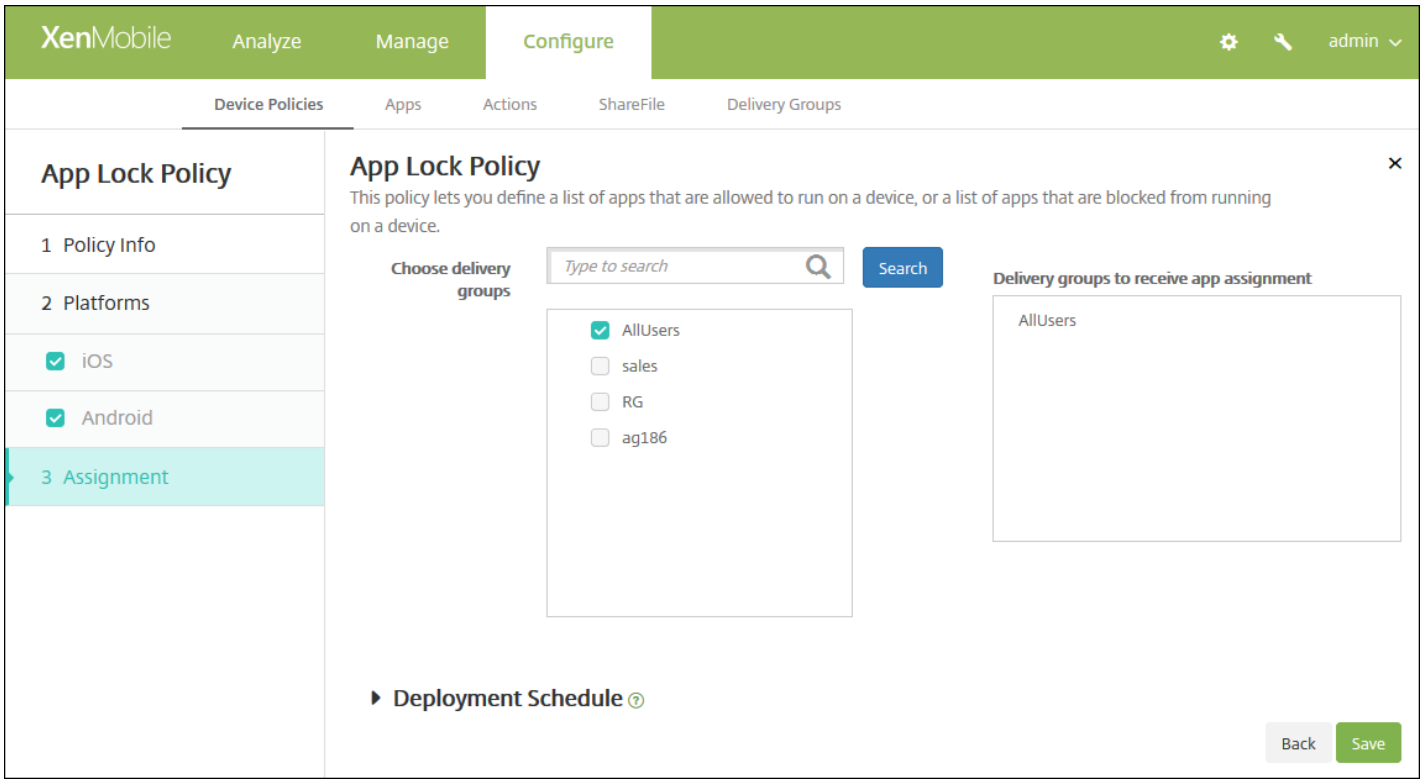
-
-
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
-
  -
  -
  -
  -
-
  -
  -
  -
  -

Configure Android settings



-
  -
  -
  -
  -
  -
-
  -
  -
  -
  -

7. Configure the deployment rules



-
-
-
-
-
-
-

App network usage device policy

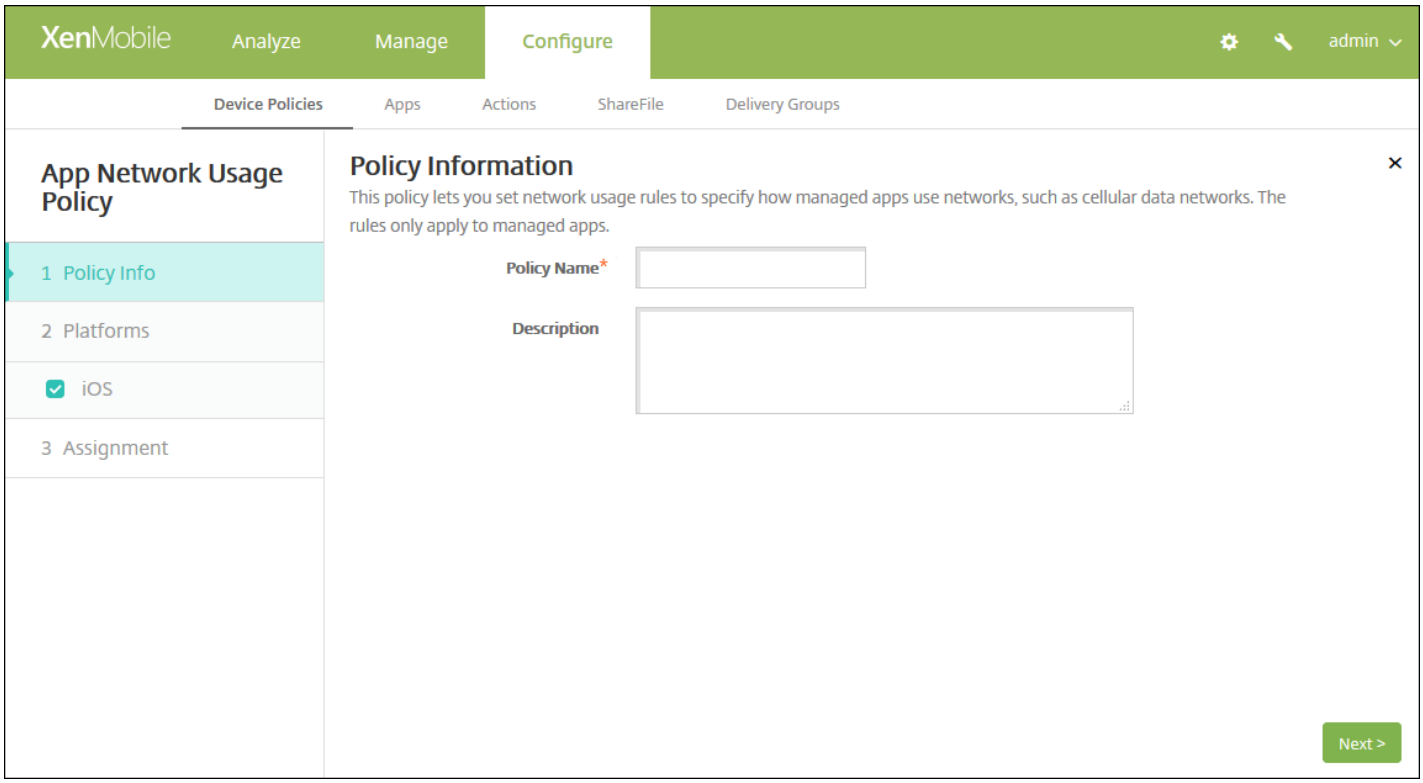
Nov 15, 2016

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.

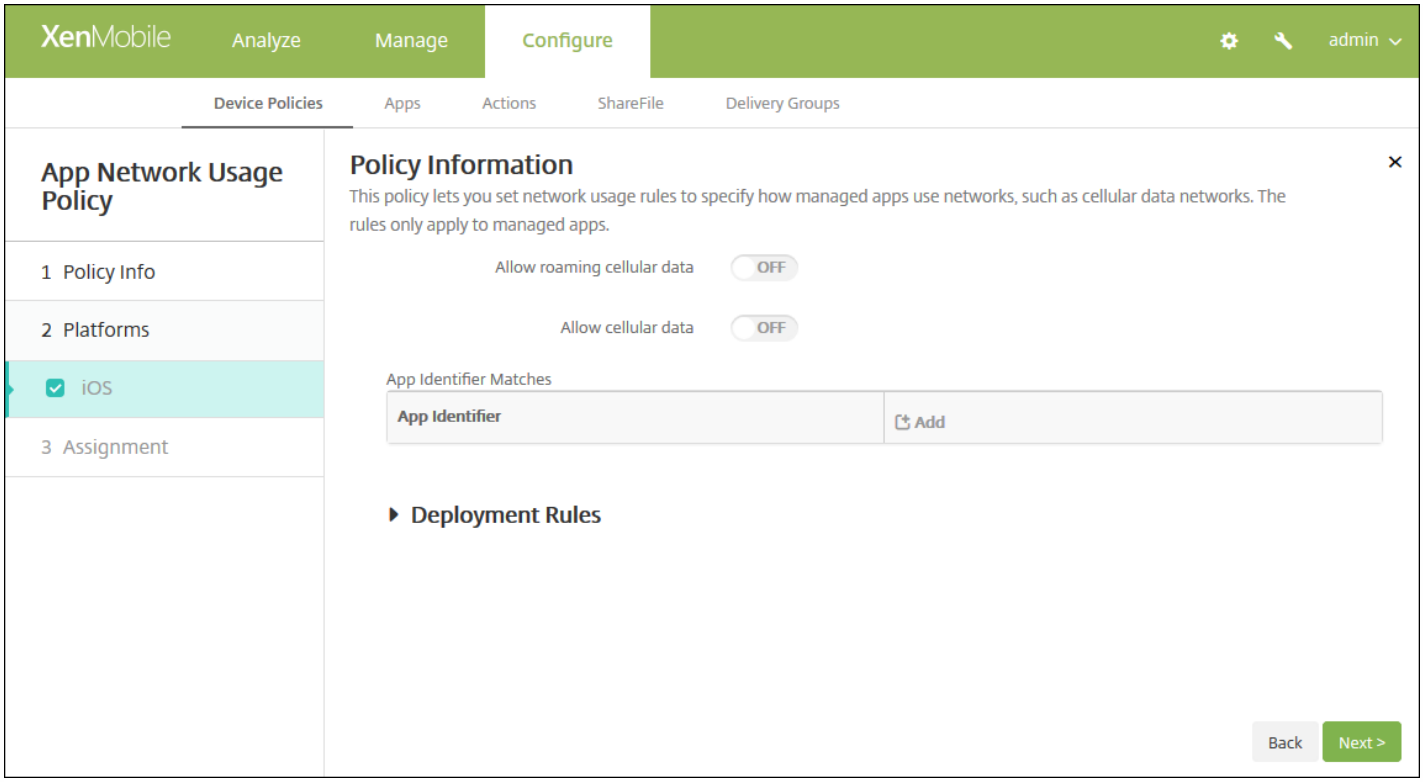
3. Expand **More**, and then under **Apps**, click **App Network Usage**. The **App Network Usage Policy** information page appears.



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.

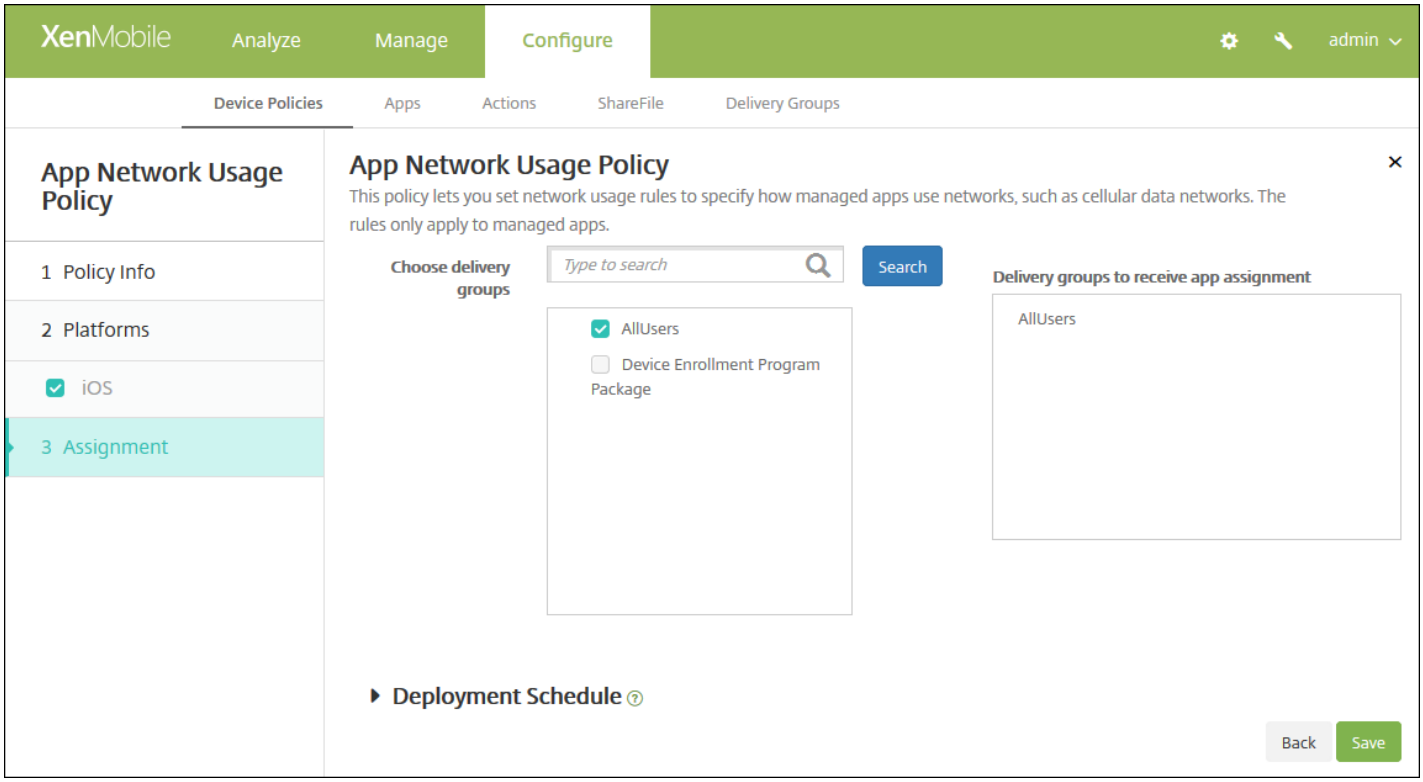
- **Allow roaming cellular data**: Select whether the specified apps can use a cellular data connection while roaming. The default is **OFF**.
- **Allow cellular data**: Select whether the specified apps can use a cellular data connection. The default is **OFF**.
- **App Identifier Matches**: For each 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

8. Click **Next**. The **App Network Usage 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** to save the policy.

App restrictions device policy

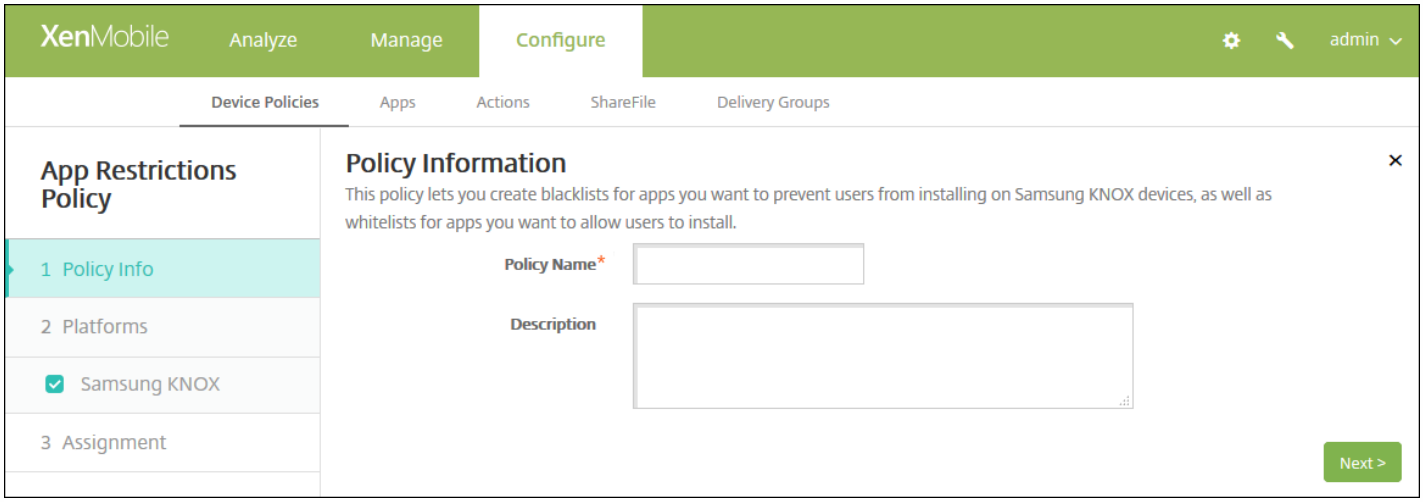
Nov 15, 2016

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.

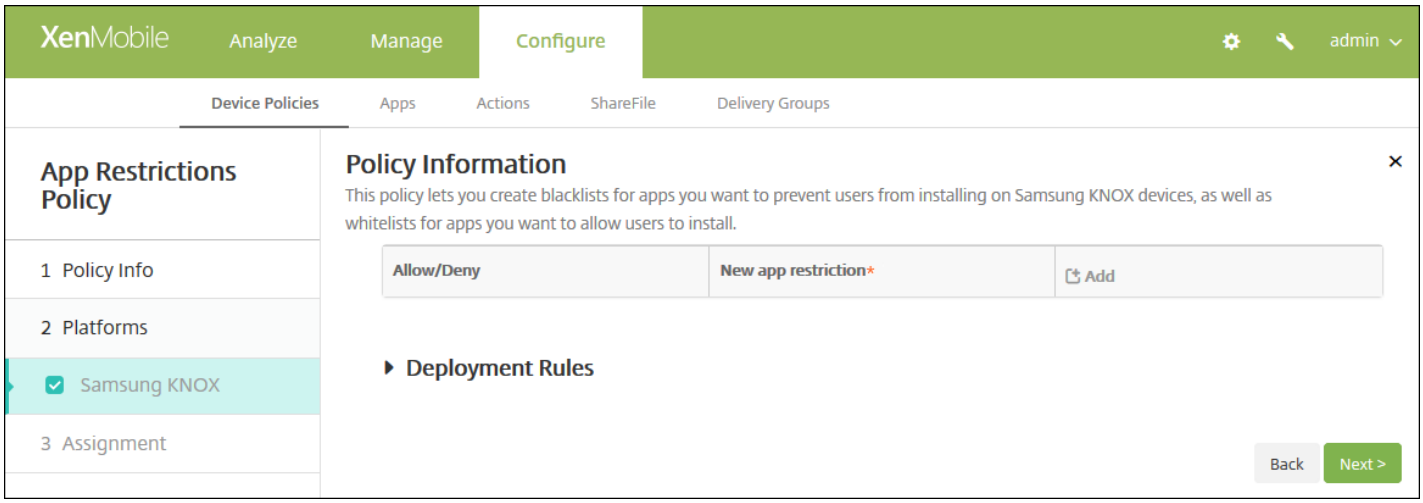
3. Expand **More** and then, under **Security**, click **App Restrictions**. The **App Restrictions Policy** information page appears.



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.



6. For each app you want to add to the Allow/Deny list, click **Add** and then do the following:

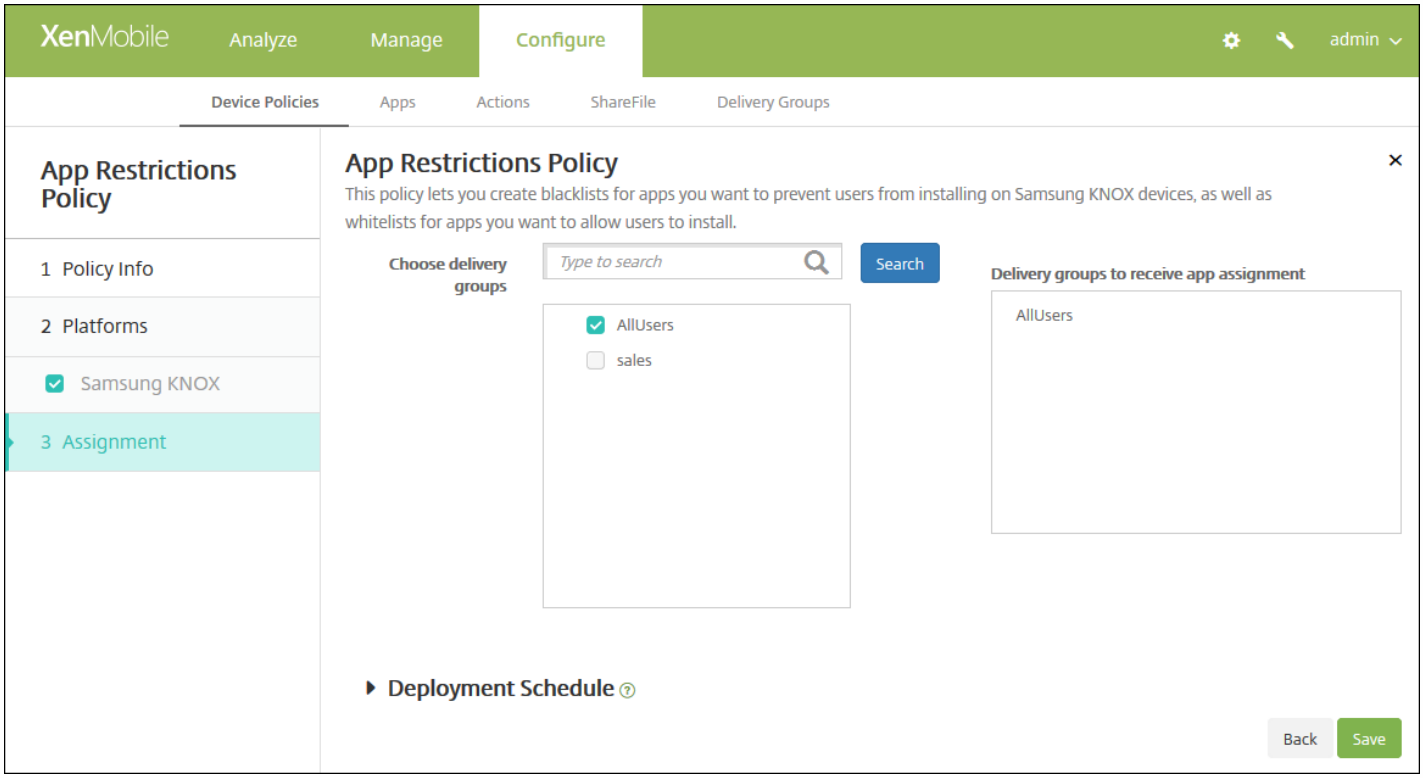
- **Allow/Deny**: Select whether users are allowed to install the app.
- **New app restriction**: Type the app package ID; for example, com.kmdm.af.crackle.
- Click **Save** to save the app to the Allow/Deny list or click **Cancel** to not save the app to the Allow/Deny list.

  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 the deployment rules

8. Click **Next**. The **App Restrictions 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**.

Tunneling device policy

Feb 16, 2017

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.

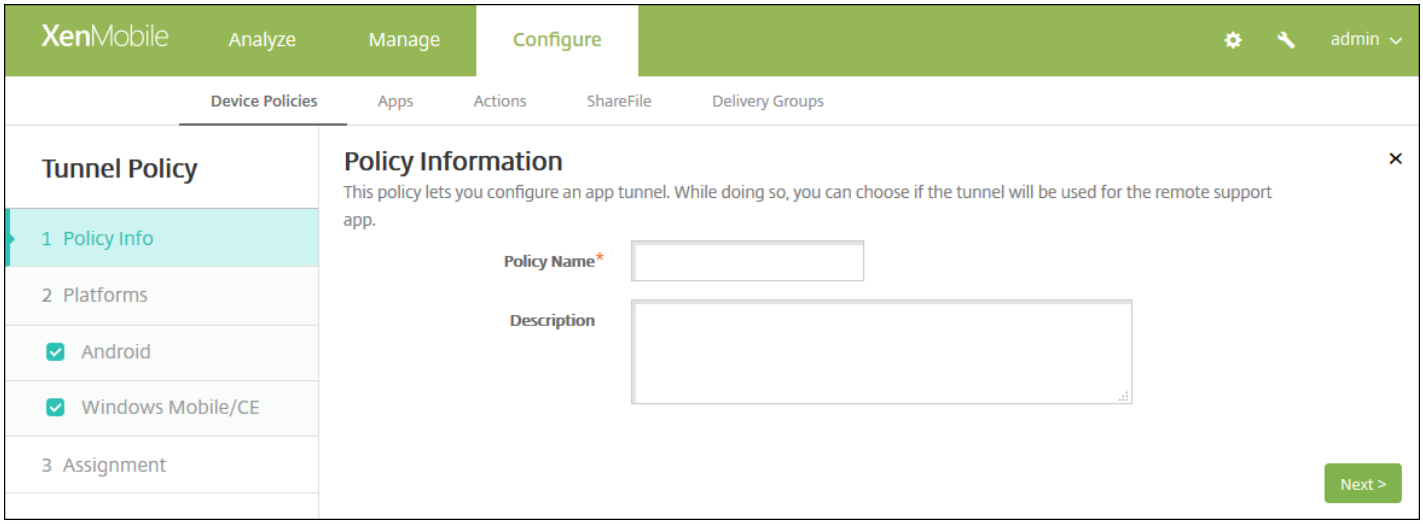
Android settings

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:

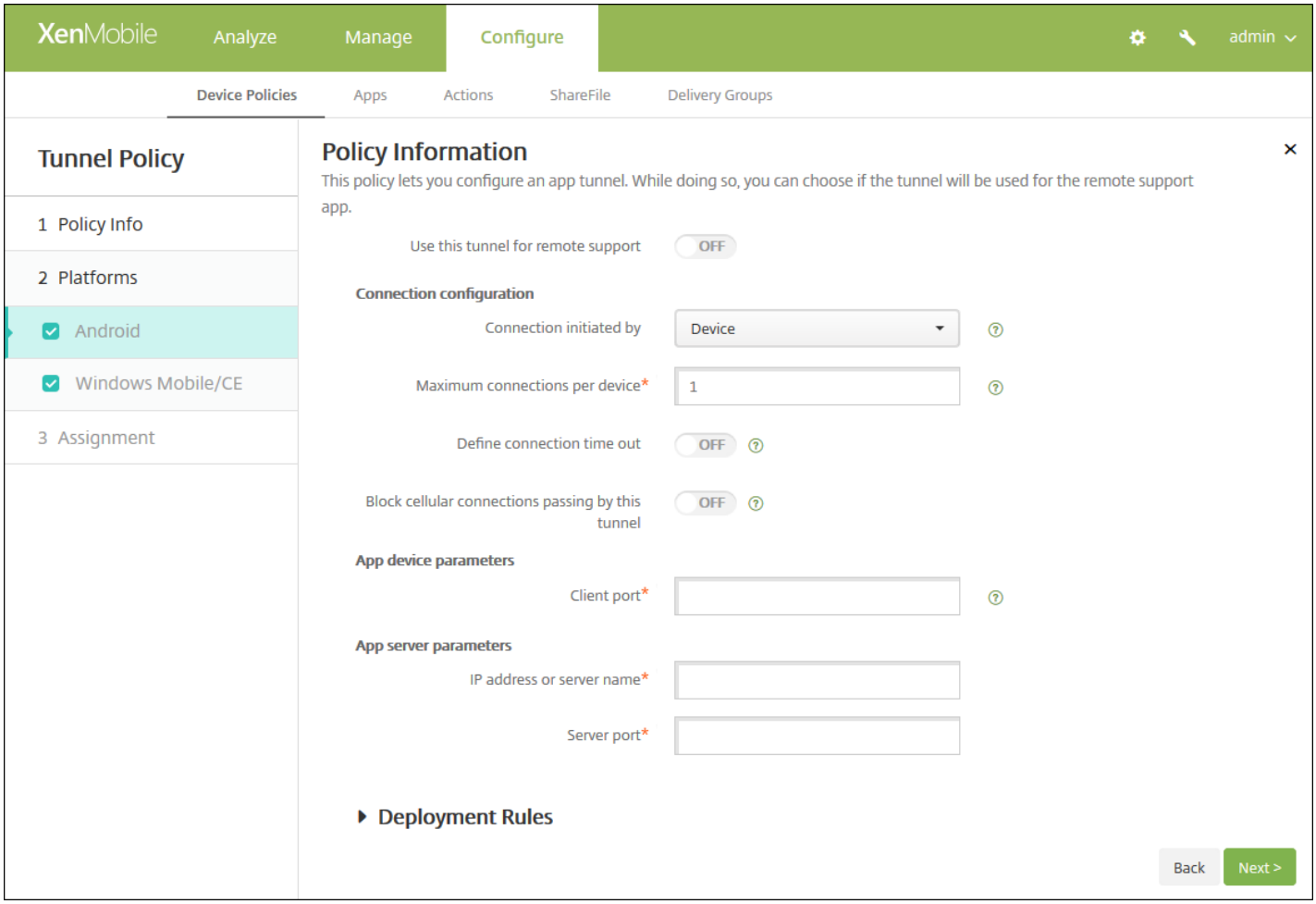
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

Configure Android settings



Configure these settings:

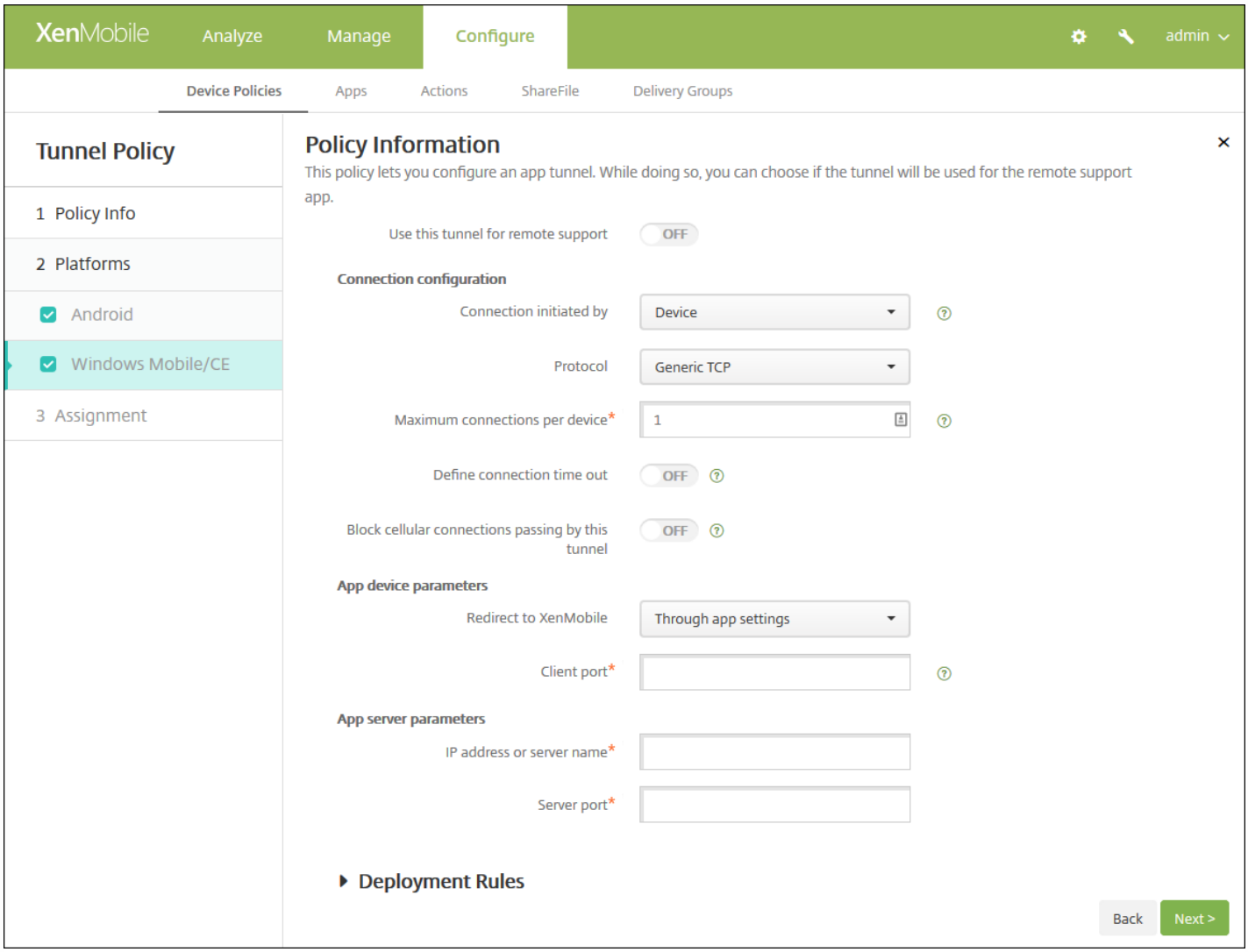
- **Use this tunnel for remote support:** Select whether the tunnel will be used for remote support.

  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.

Configure Windows Mobile/CE settings



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.

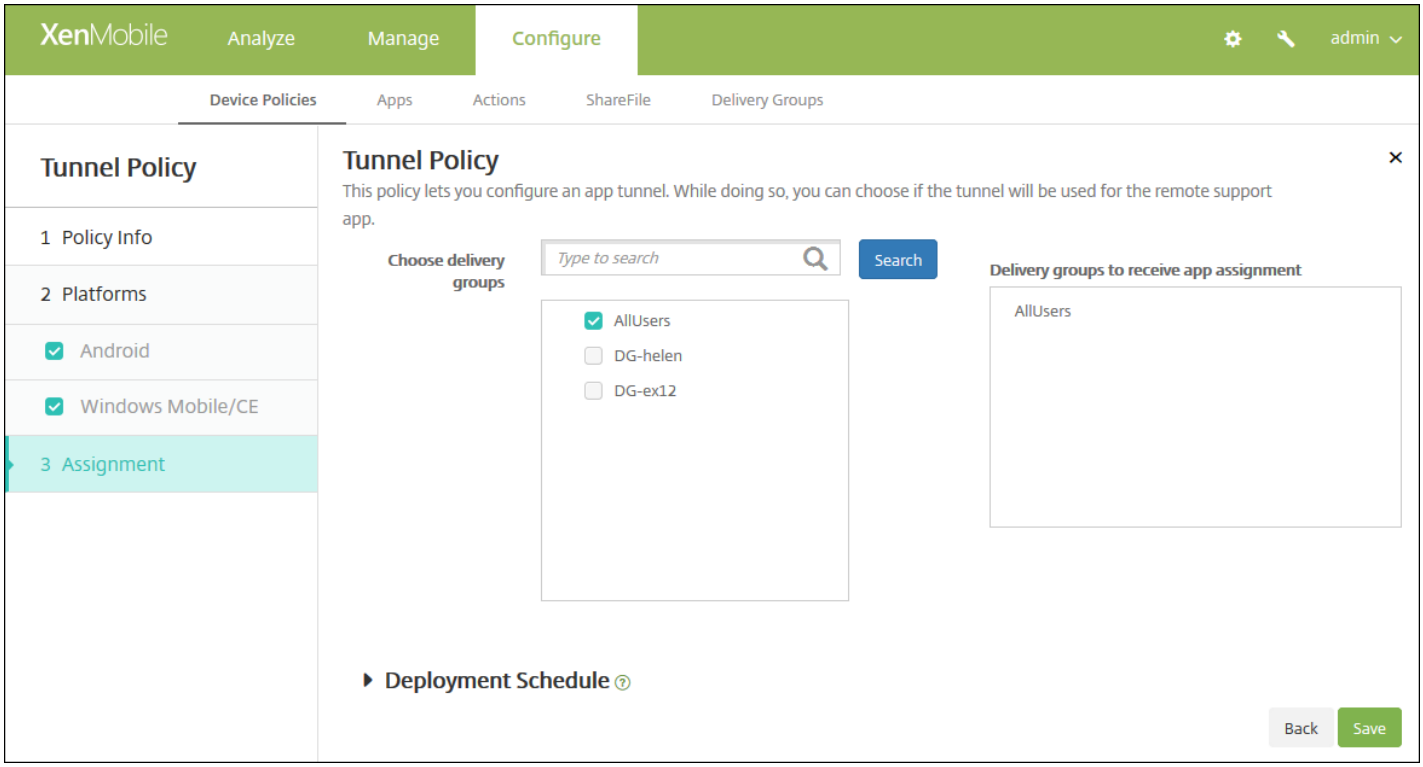
- **Define connection time out**: Select whether to set a length of time an app can be idle before the tunnel is closed.
  - **Connection time out**: If you set **Define connection time out** to **On**, type the length of time in seconds that an app can be idle before the tunnel is closed.
- **Block 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 the deployment rules

8. Click **Next**. The **Tunnel 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**.

App uninstall device policy

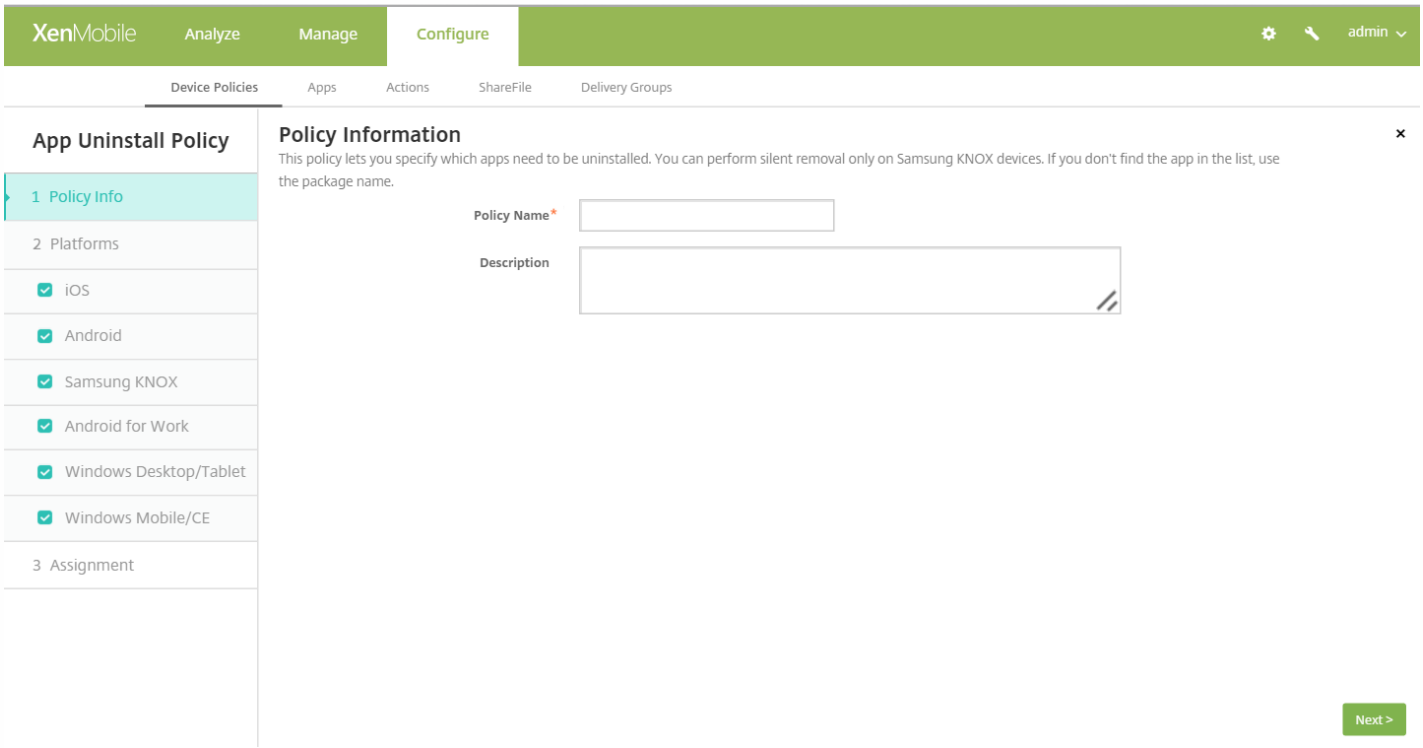
Nov 15, 2016

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:

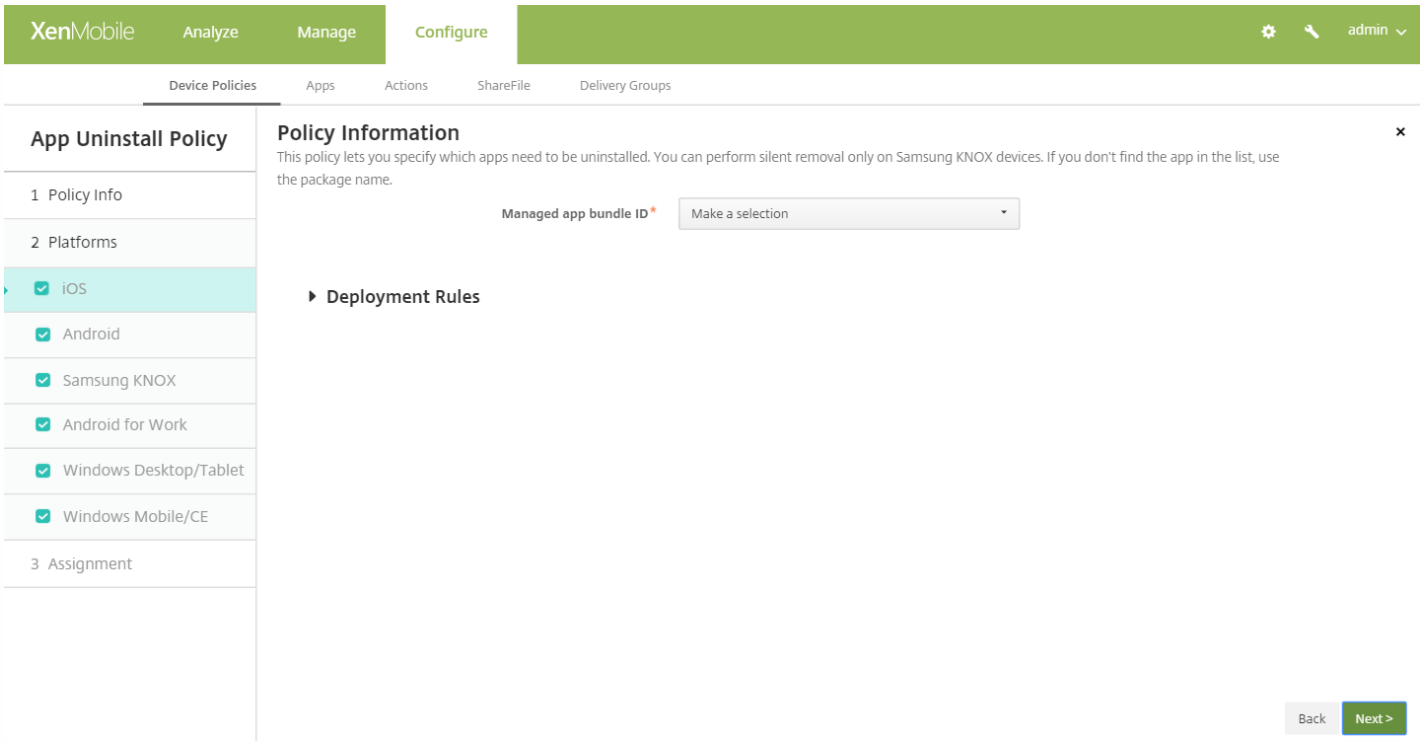
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

When you finish configuring the settings for a platform, refer to Step 7 for how to set that platform's deployment rules.

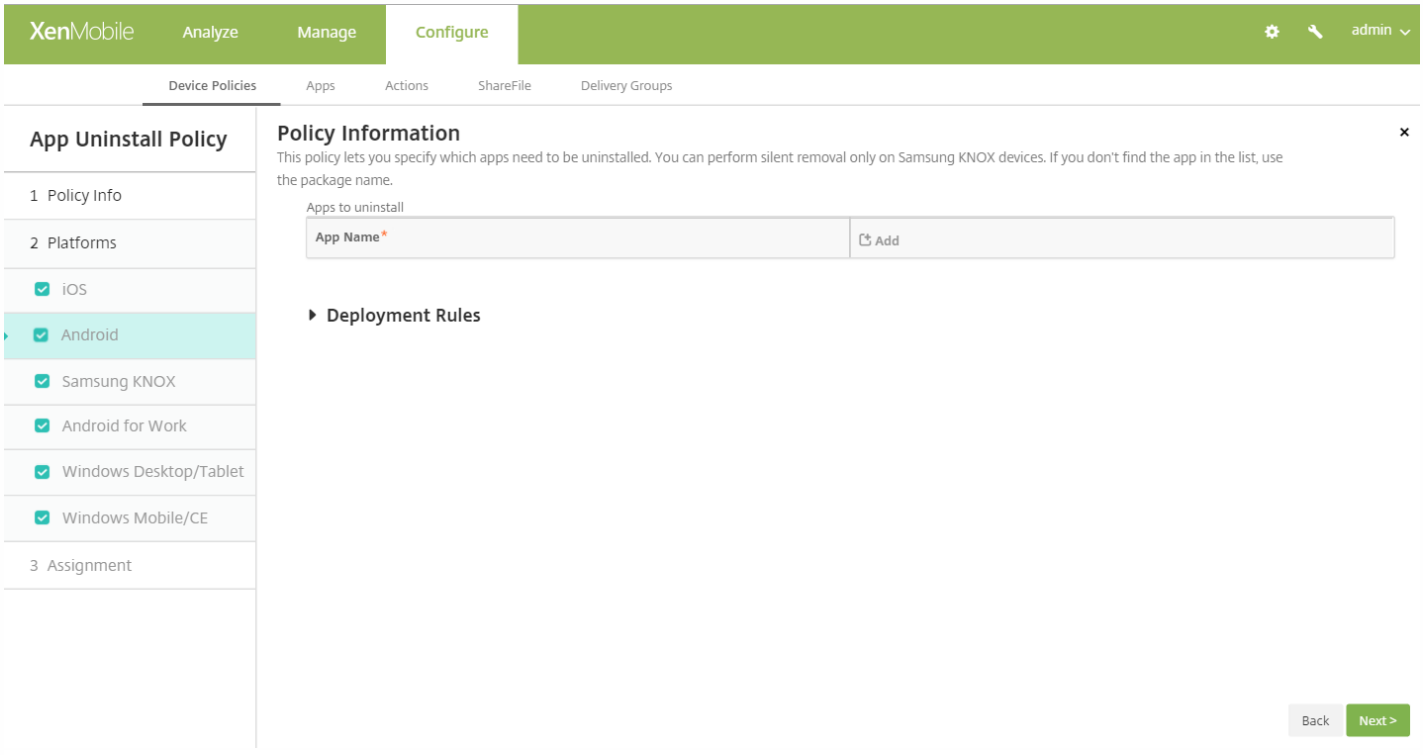
Configure iOS settings



Configure 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 all other platform settings



Configure this setting:

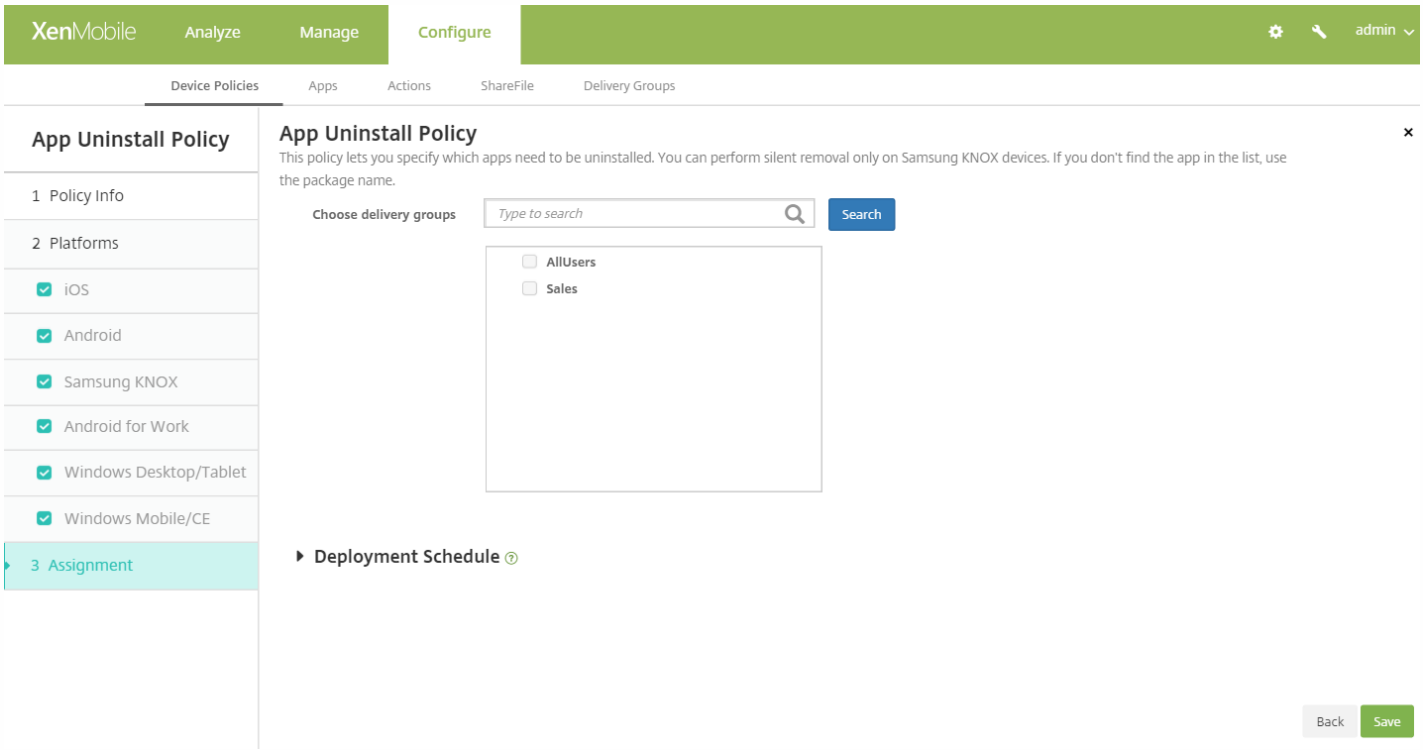
- **Apps to uninstall**: For each app you want to add, click **Add** and then do the following:
  - **App name**: In the list, click an existing app or click **Add new** to enter a new app name. If there are no apps configured for this platform, the list will be empty and you must add new apps.
  - Click **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 the deployment rules

8. Click **Next**. The **App Uninstall 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**.

App uninstall restrictions device policy

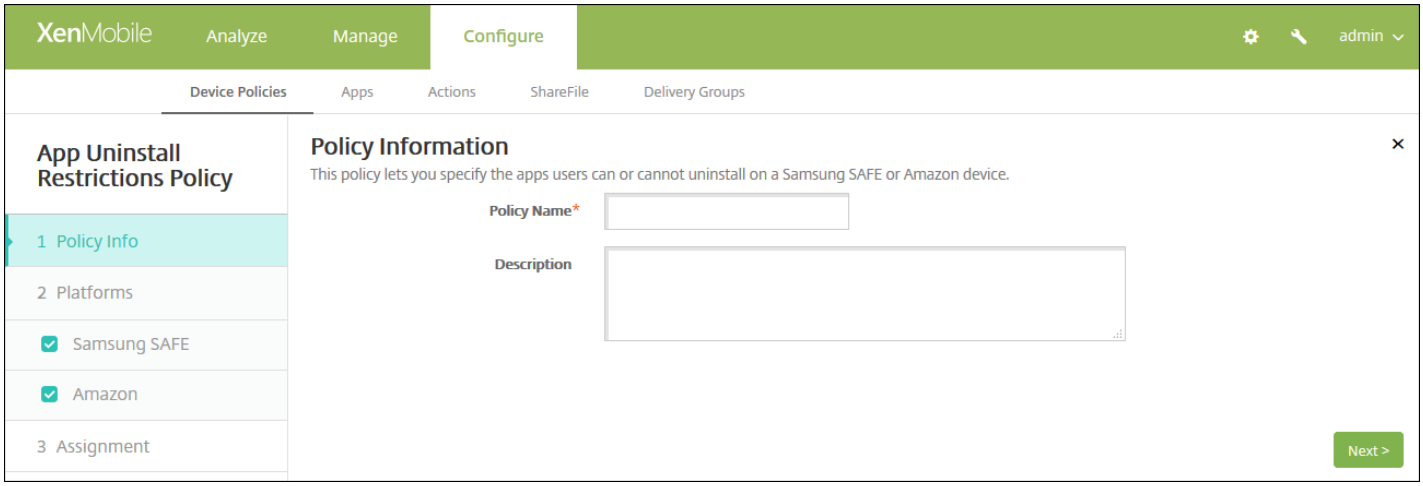
Nov 15, 2016

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.

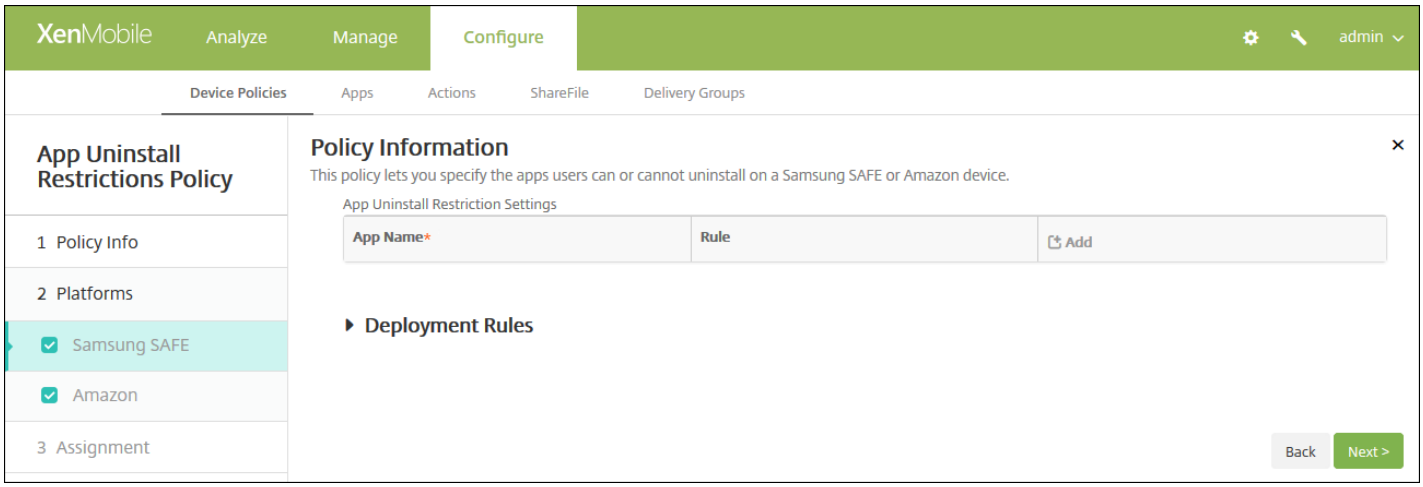
3. Expand **More**, and then under **Apps**, click **App Uninstall Restrictions**. The **App Uninstall Restrictions Policy** information page appears.



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:

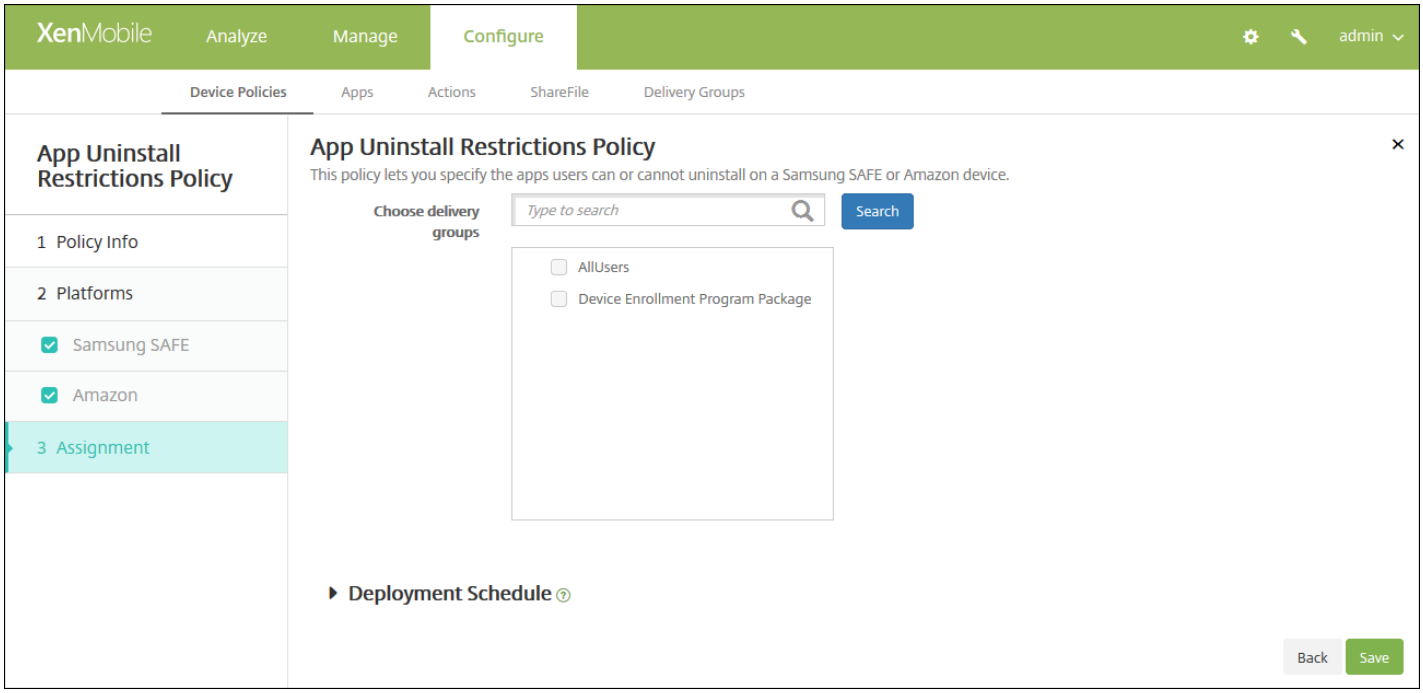
- **App Uninstall Restrictions Settings**: For each app rule you want to adds, click **Add** and then do the following:
  - **App Name**: In the list, click an app or **Add new** to add a new app.
  - **Rule**: Select whether users can uninstall the app. The default is to allow uninstallation.
  - Click **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 the deployment rules

9. Click **Next**. The **App Uninstall Restrictions 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**. 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.

12. Click **Save**.

Browser device policy

Jan 11, 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.

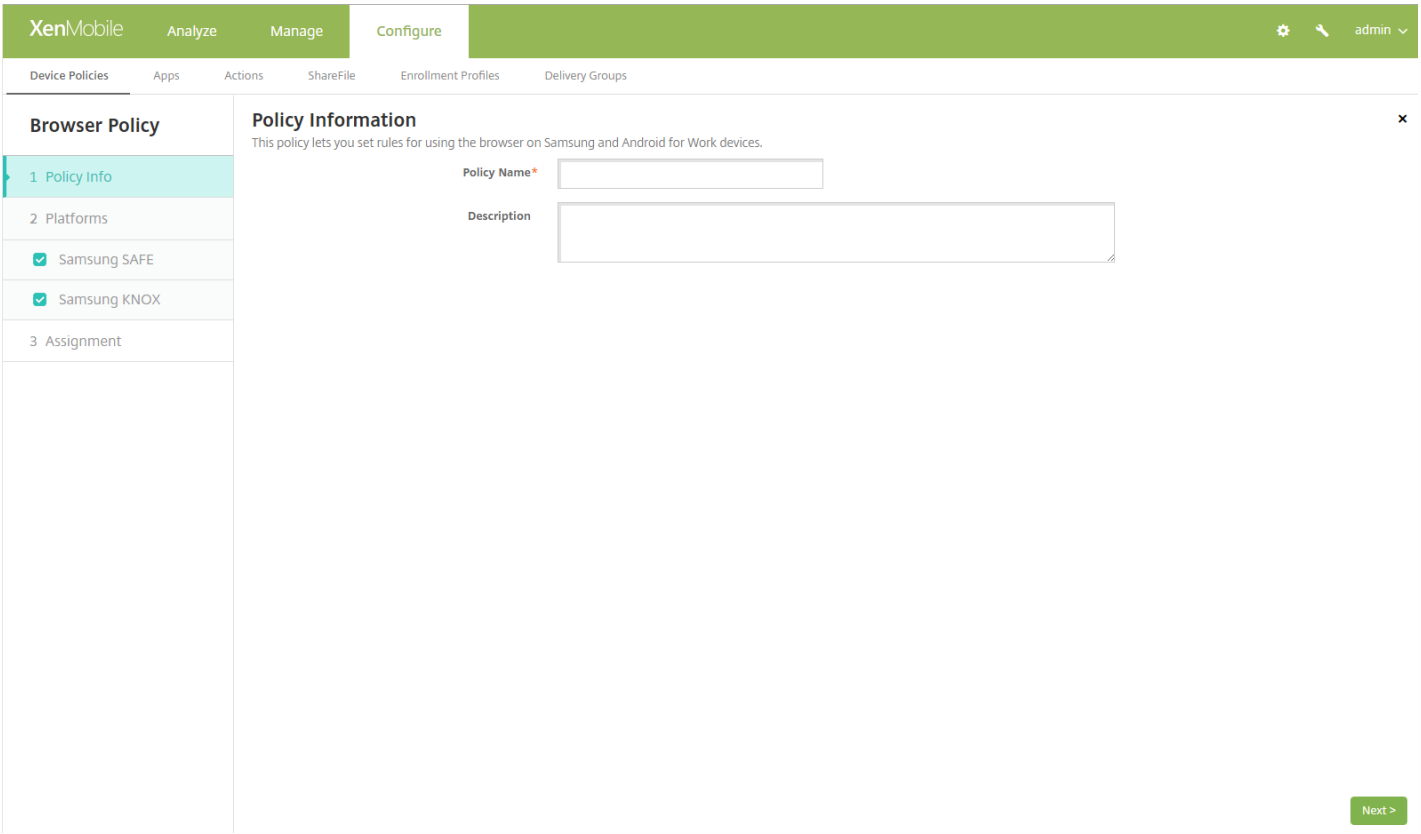
On Samsung devices, you can completely disable the browser, or you can enable or disable pop-ups, JavaScript, cookies, autofill, and whether to force fraud warnings.

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:

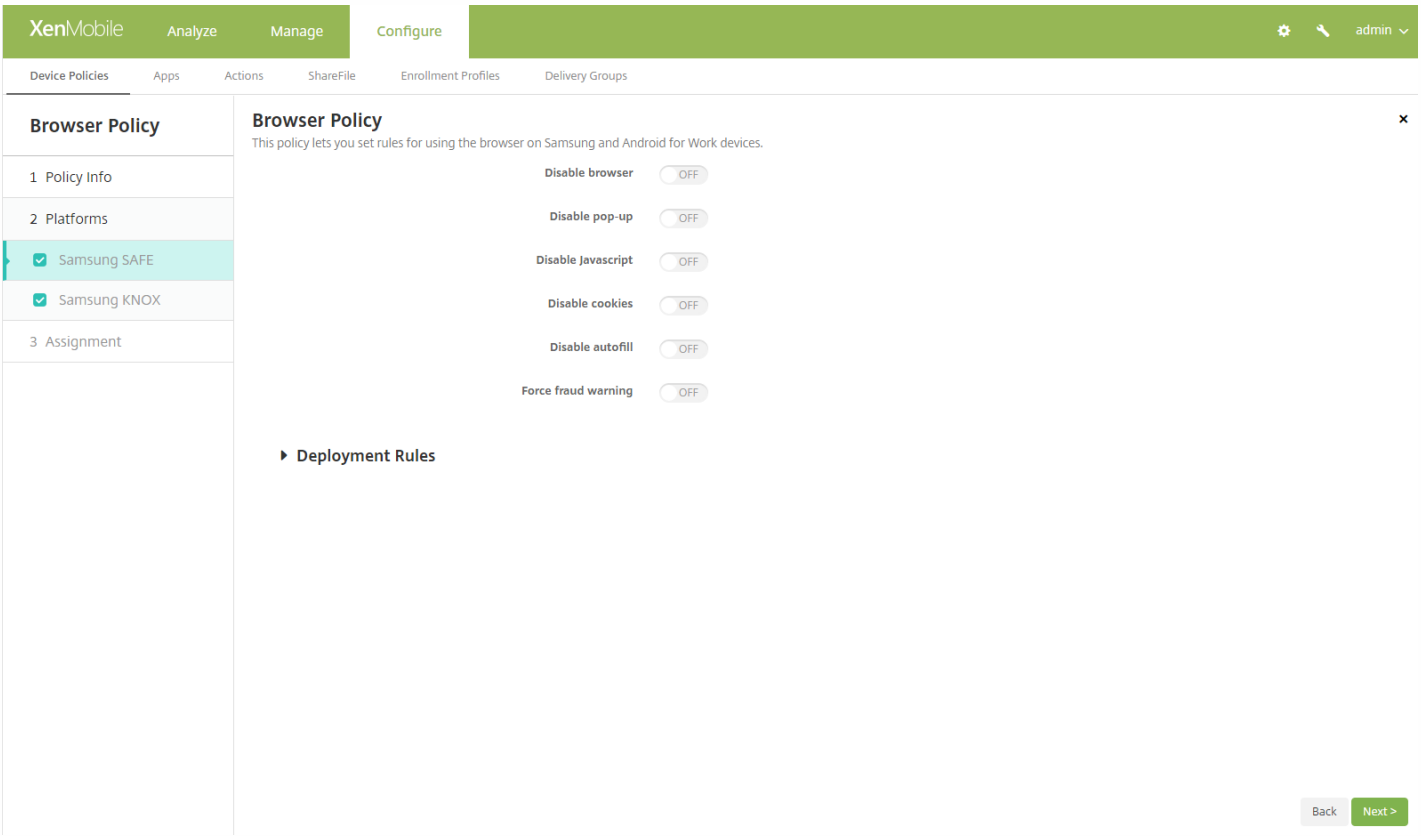
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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 Samsung SAFE and Samsung KNOX settings

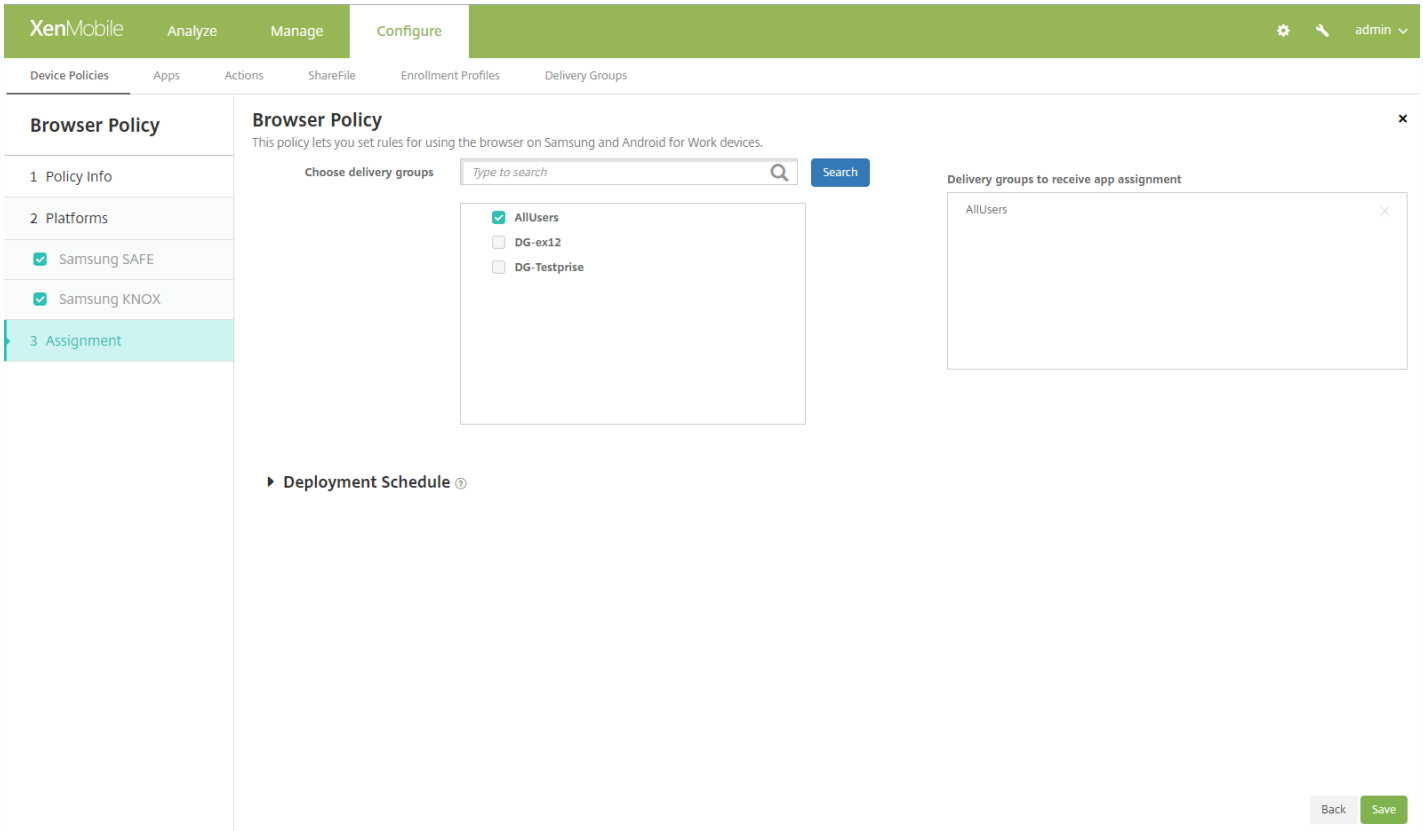


Configure these settings:

- **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.

7. Configure the deployment rules

8. Click **Next**. The **Browser 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** to save the policy.

Calendar (CalDav) device policy

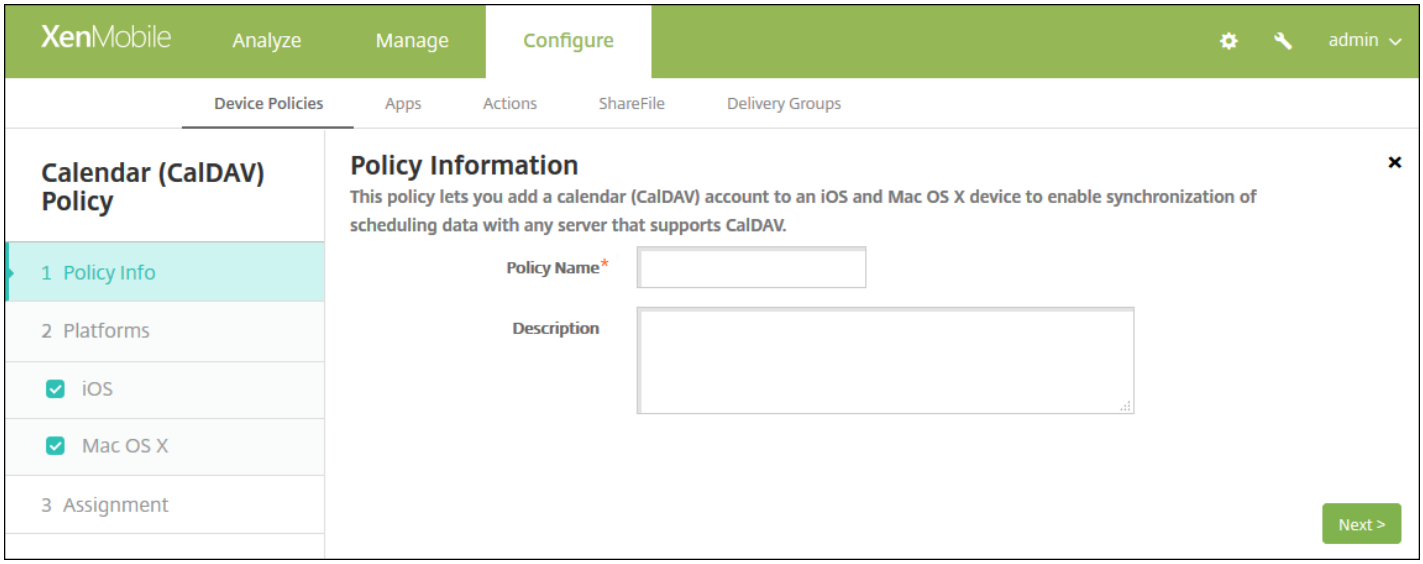
Nov 15, 2016

You can add a device policy in XenMobile to add a calendar (CalDAV) account to users' iOS or Mac OS X 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:

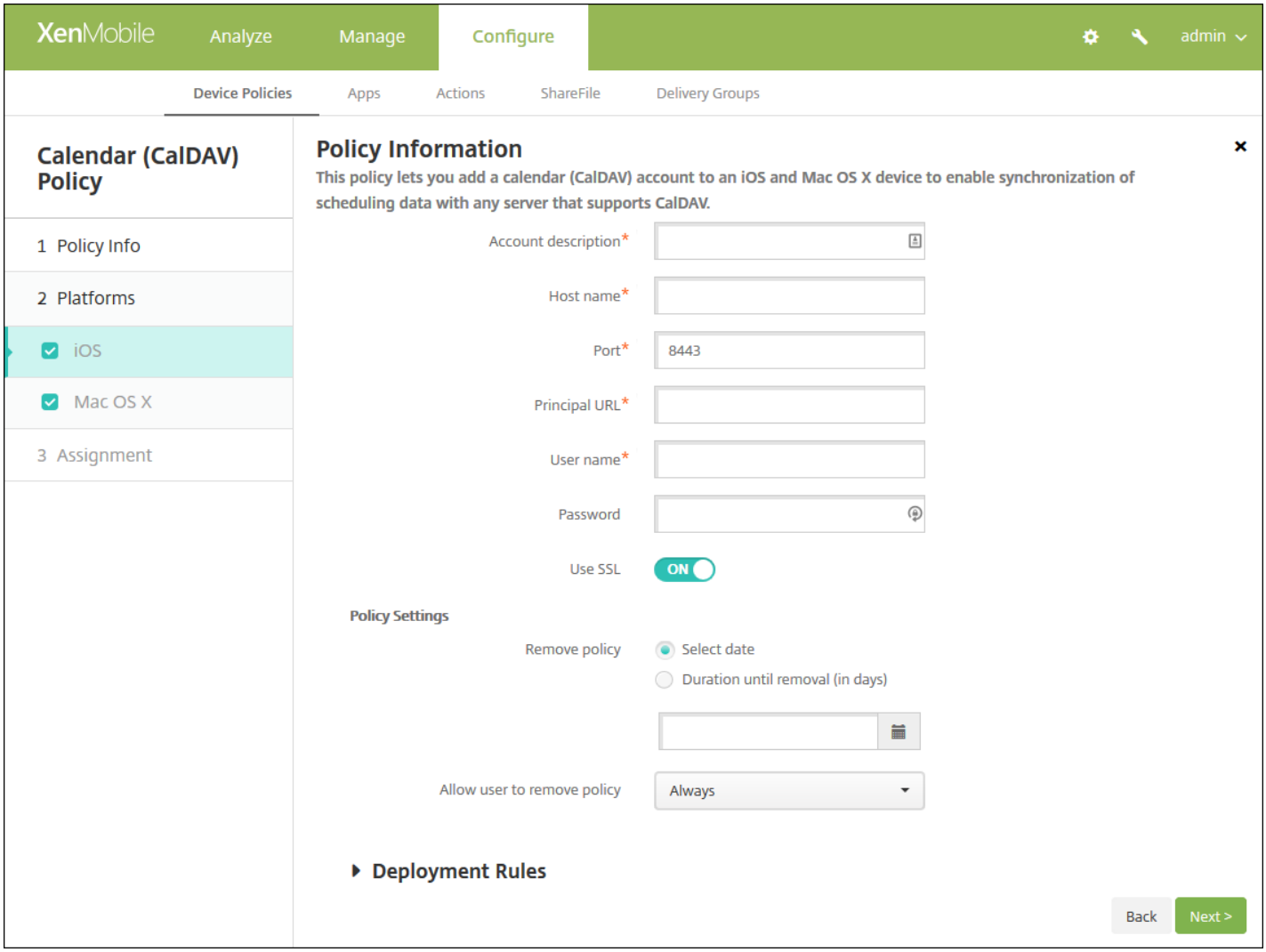
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

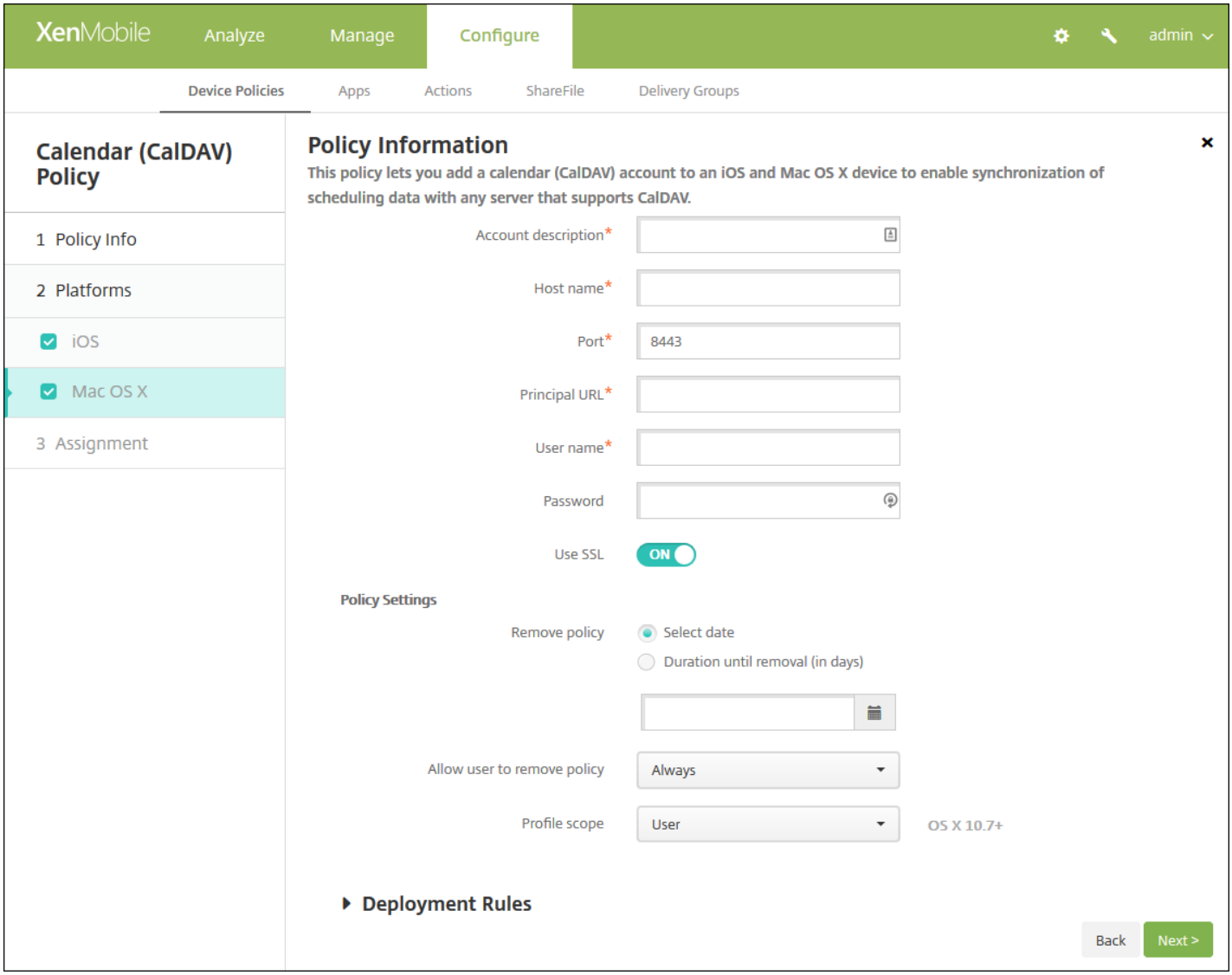
Configure iOS settings



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 days)**.
  - 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 Mac OS X settings

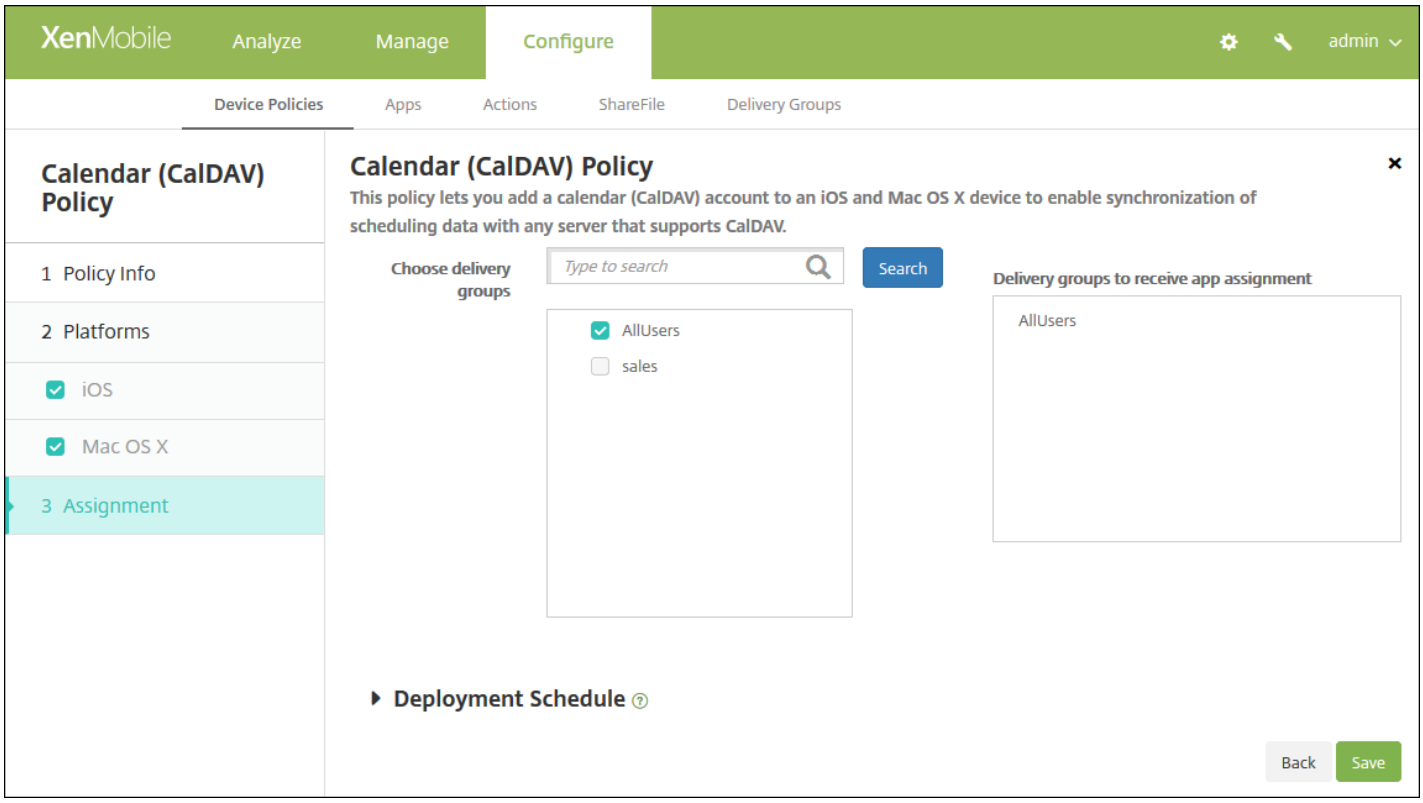


Configure the following settings:

- **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 days)**.
  - 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 OS X 10.7 and later.

7. Configure the deployment rules

8. Click **Next**. The **Calendar (CalDAV) 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**.

Cellular device policy

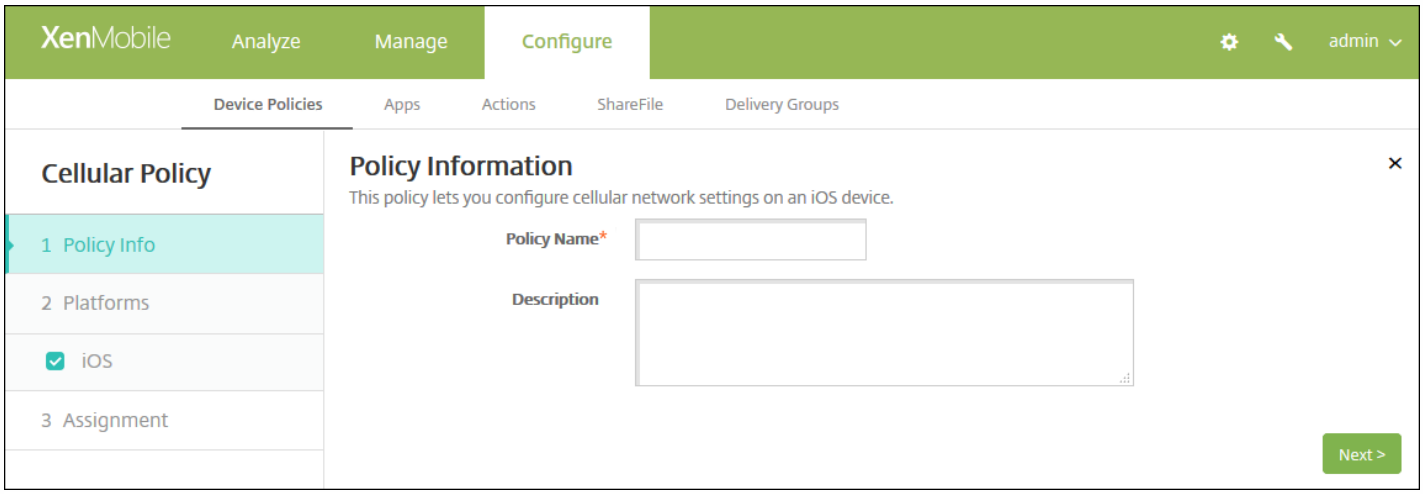
Nov 15, 2016

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.

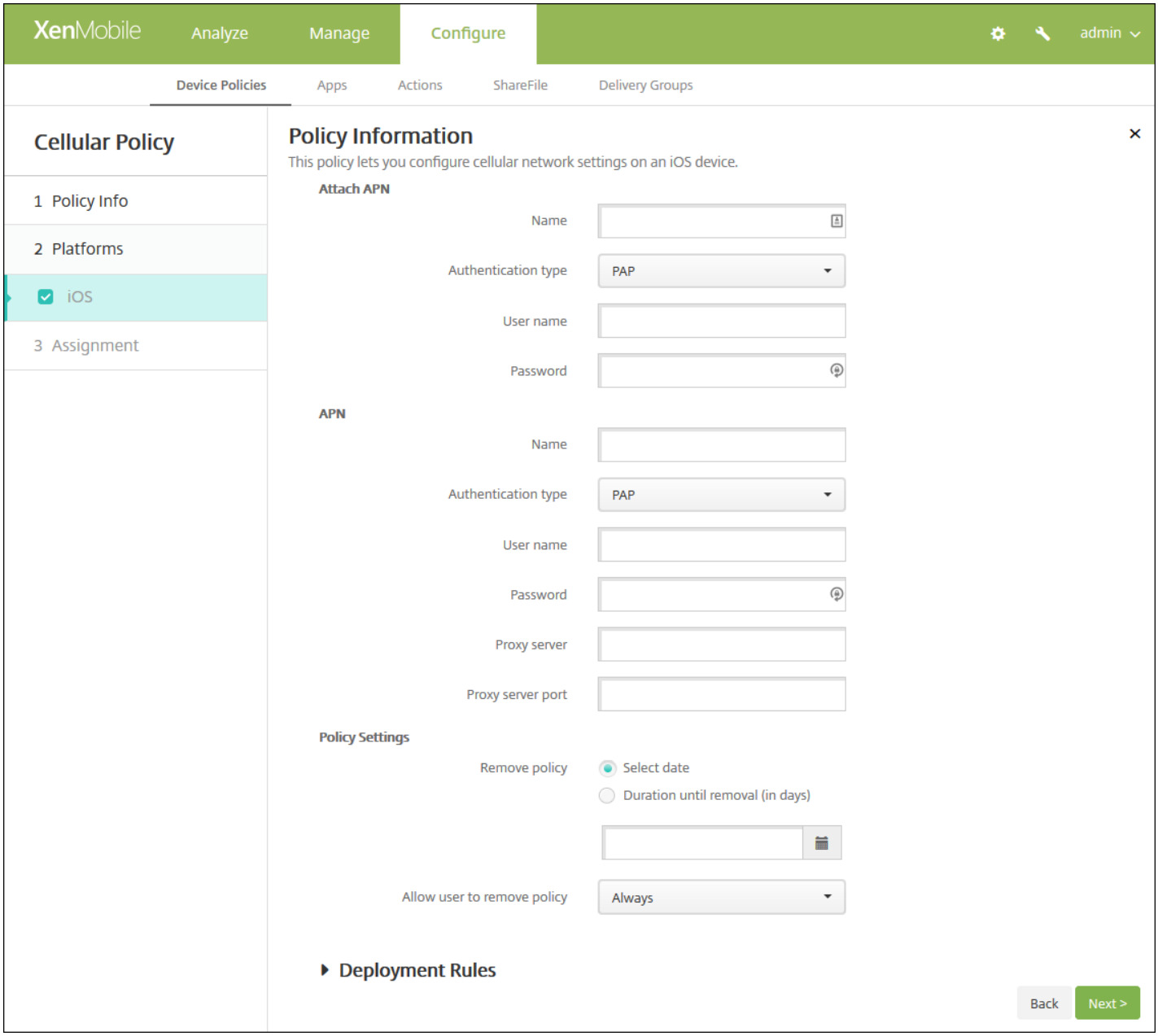
3. Expand **More**, and then, under **Network Access**, click **Cellular**. The **Cellular Network Policy** information page appears.



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.



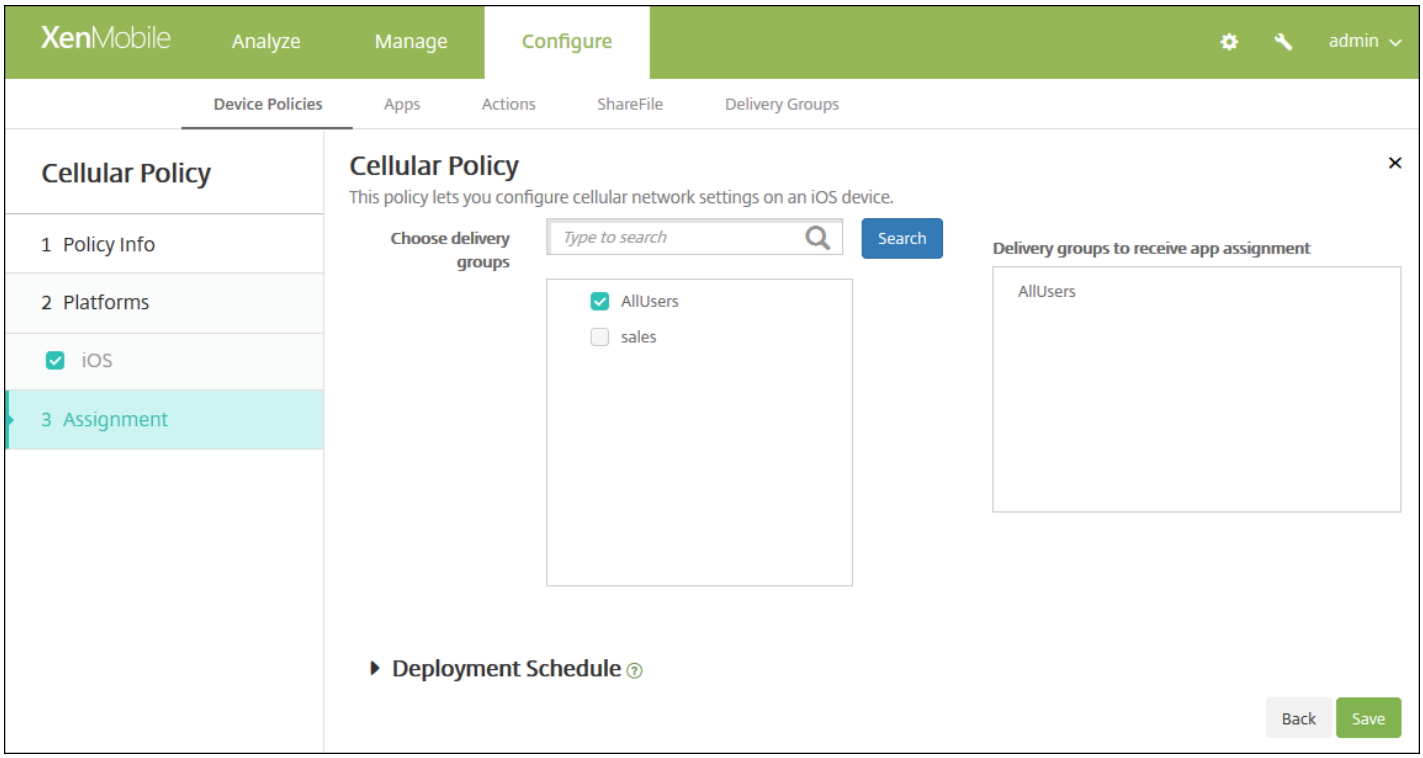
6. Configure these settings:

- **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 days)**.
  - 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 the deployment rules

8. Click **Next**. The **Cellular Network 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**.

Connection manager device policy

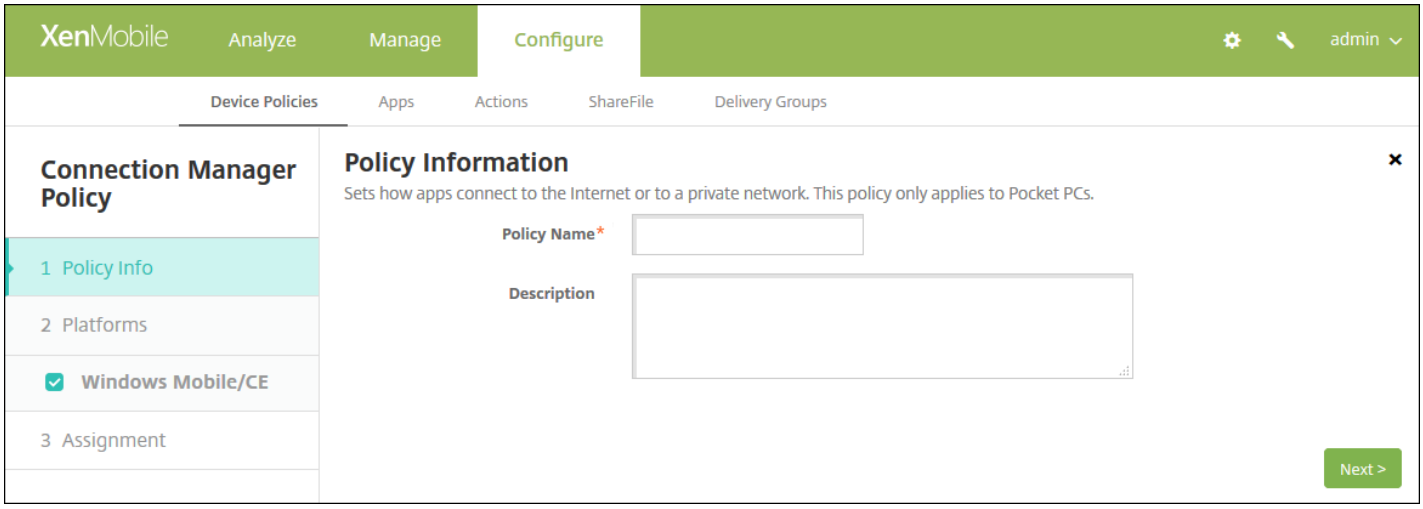
Nov 15, 2016

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.

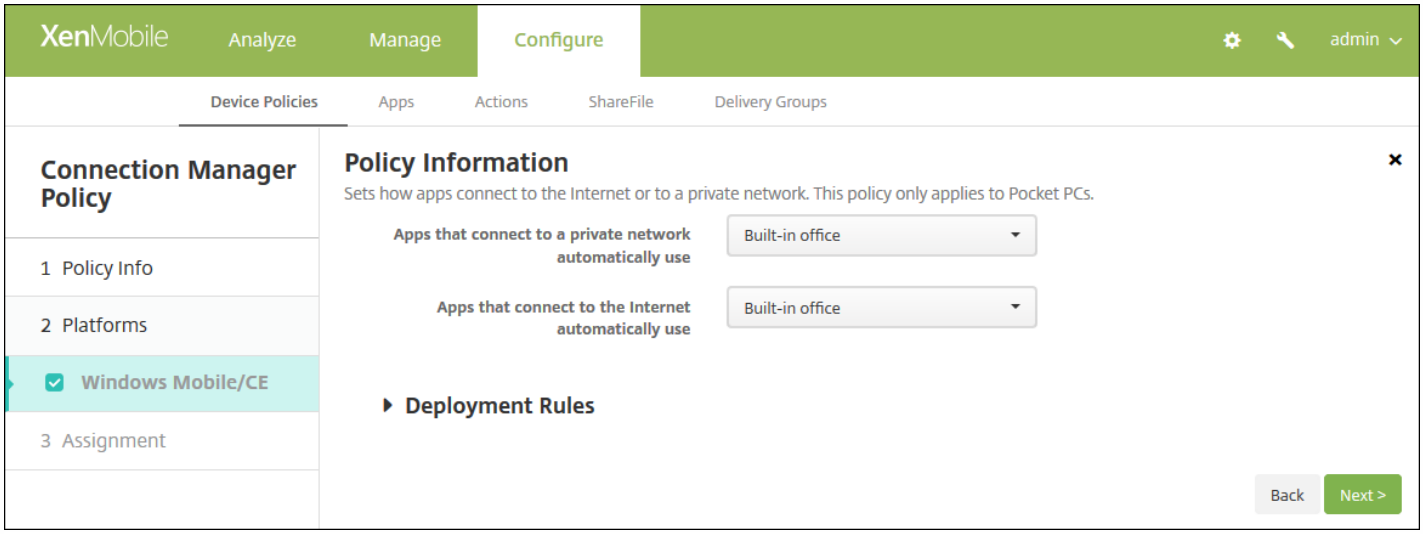
3. Click **More**, and then, under **Network Access**, click **Connection manager**. The **Connection Manager** policy information page appears.



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.



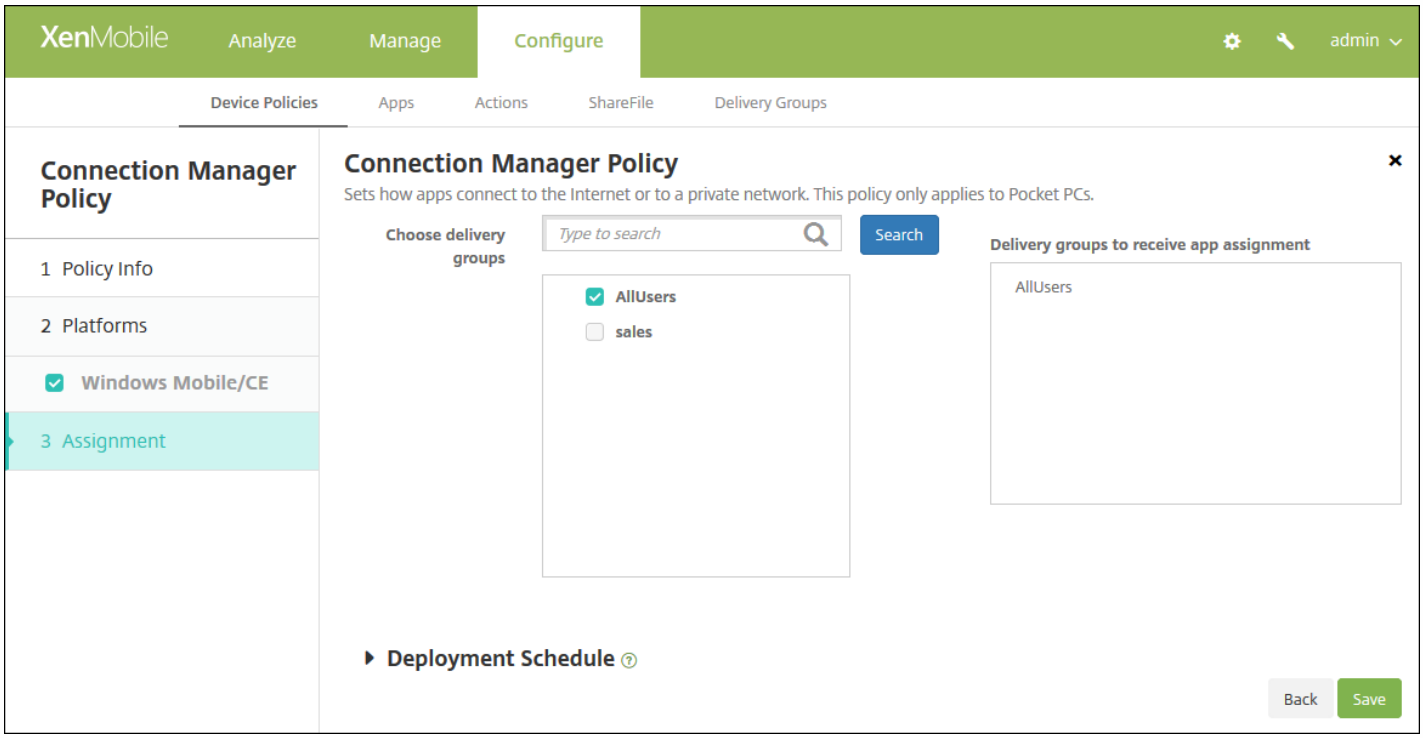
6. Configure these settings.

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 the deployment rules

8. Click **Next**. The **Connection Manager** 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**.

Connection scheduling device policy

Nov 15, 2016

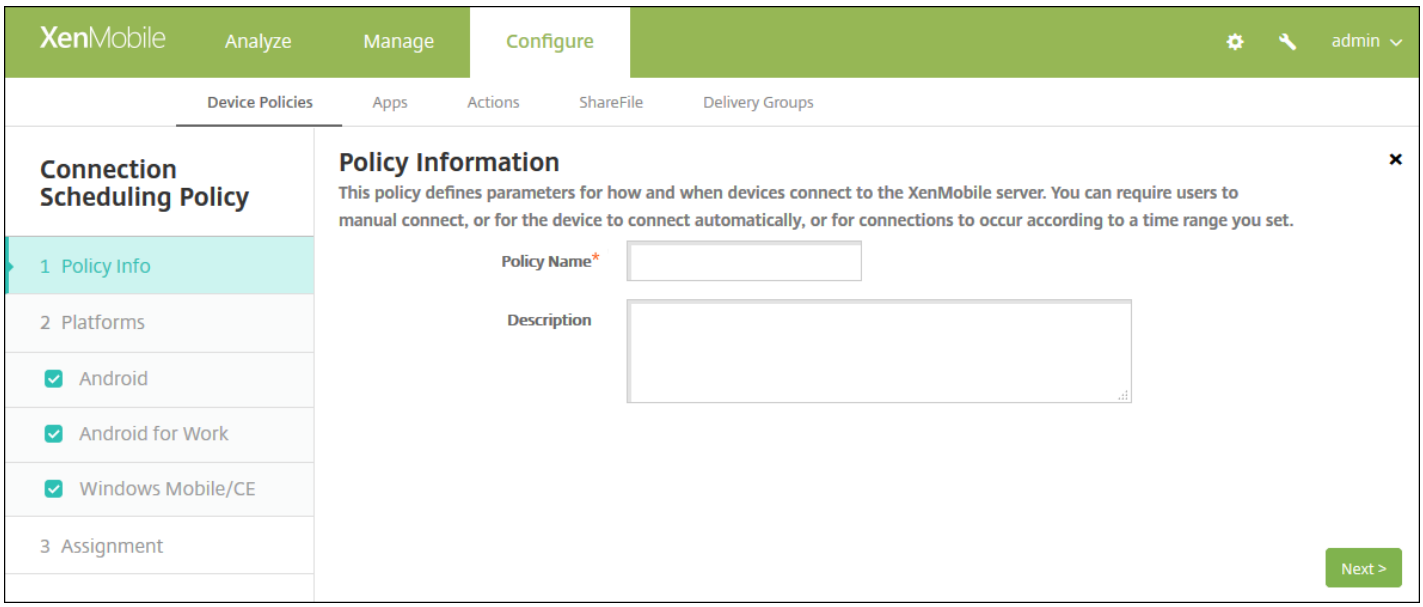
You create connection scheduling policies to control how and when users' devices connect to XenMobile. Note that you can configure this policy for devices enabled for Android for Work as well.

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.

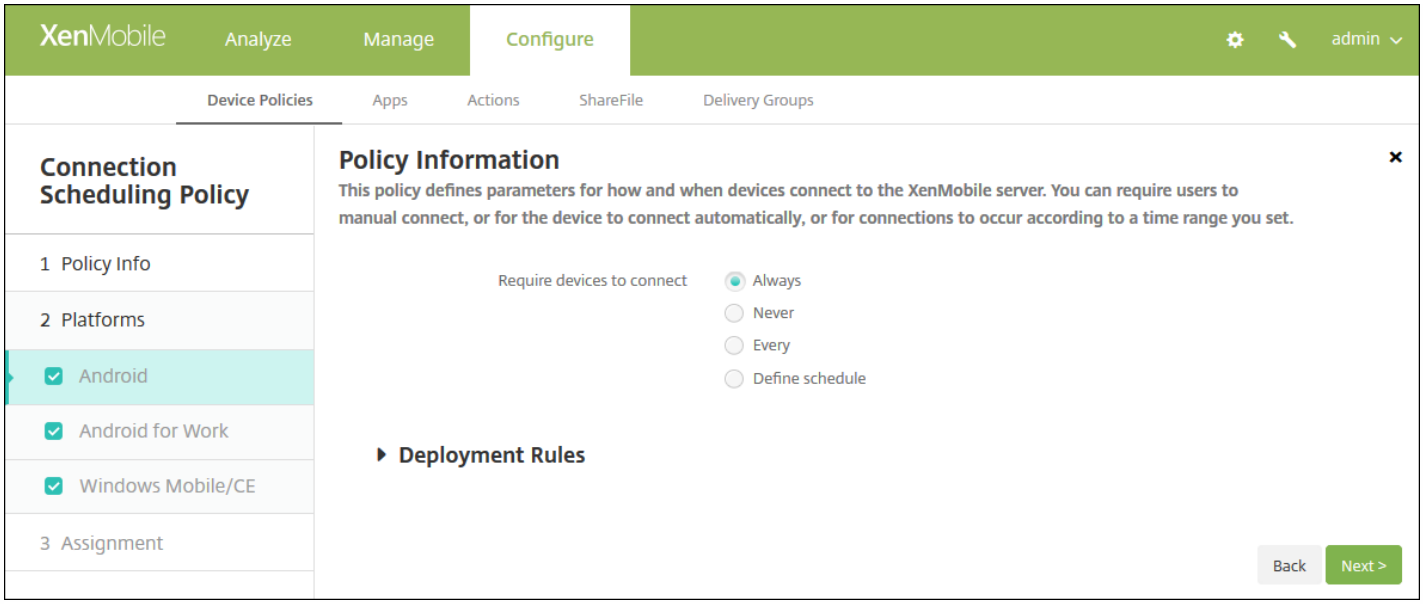
3. Click **Scheduling**. The **Connection Scheduling Policy** information page appears.



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.

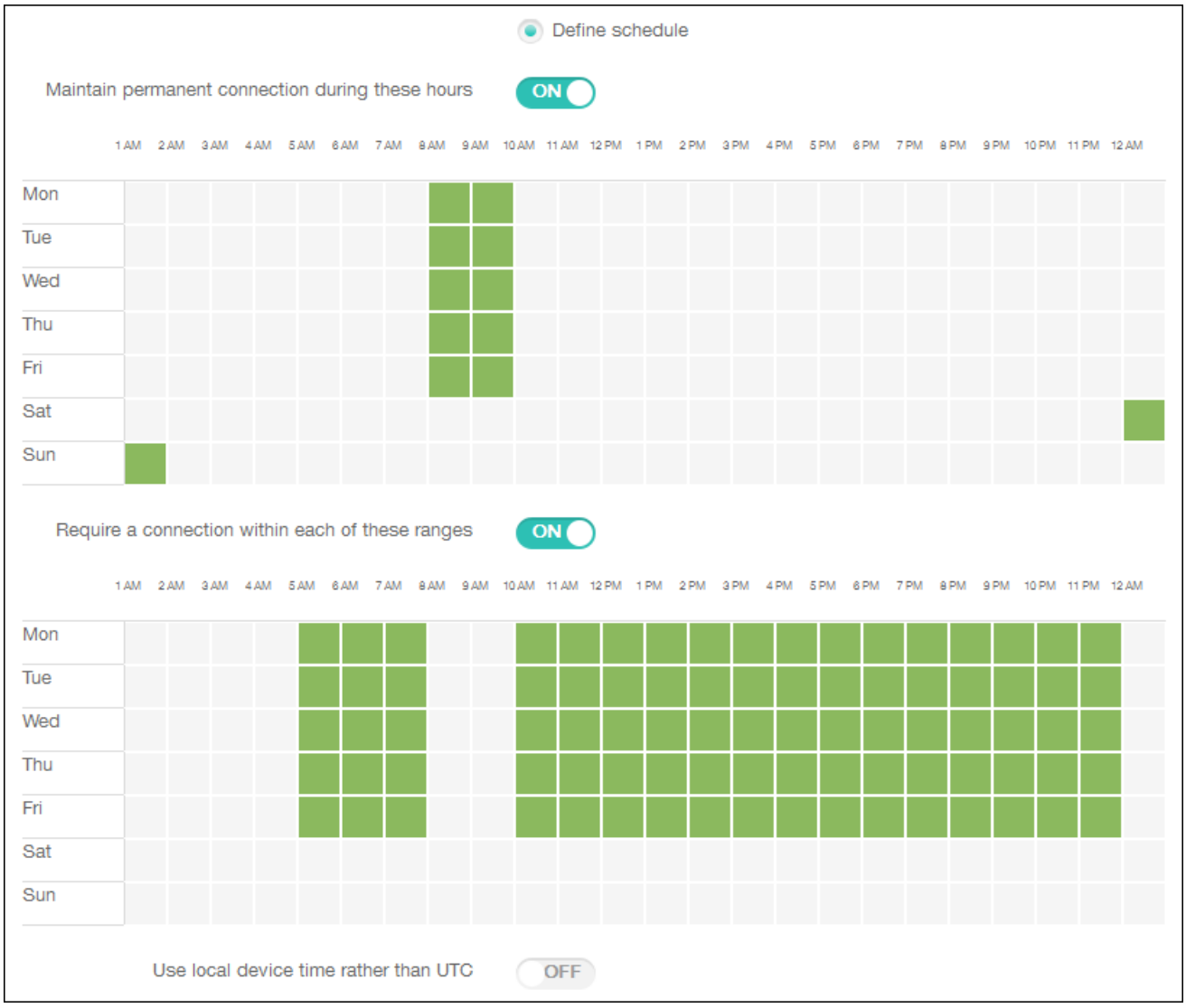
7. Configure the following settings for each of the platforms you selected:

- **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

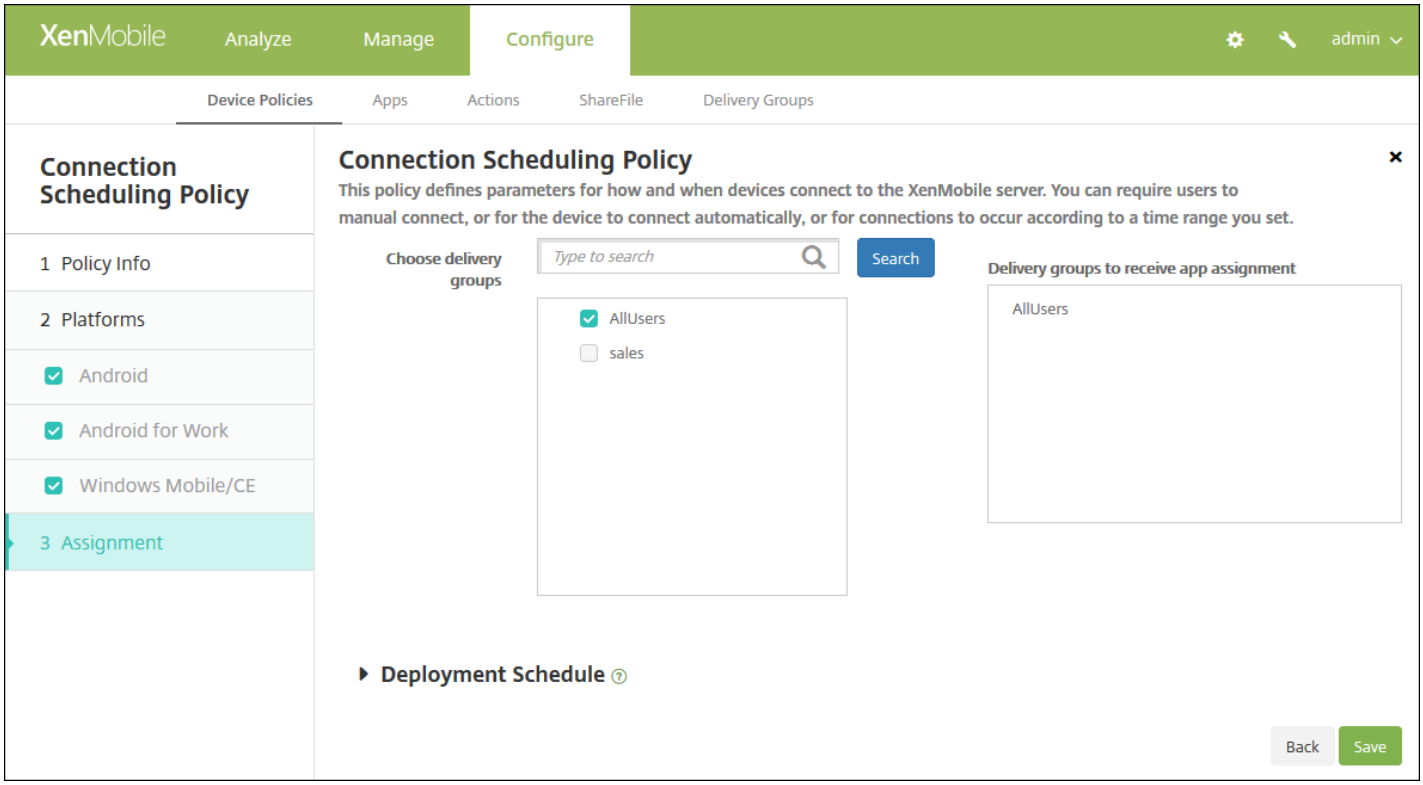
When you enable the following options, a timeline appears where you can define the time frames you want. You can enable either or both options to require a permanent connection during specific hours or to require a connection within certain time frames. Each square in the timeline is 30 minutes, so if 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.



8. Configure the deployment rules

9. Click **Next**. The **Connection Scheduling 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**. 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.

12. Click **Save**.

Contacts (CardDAV) device policy

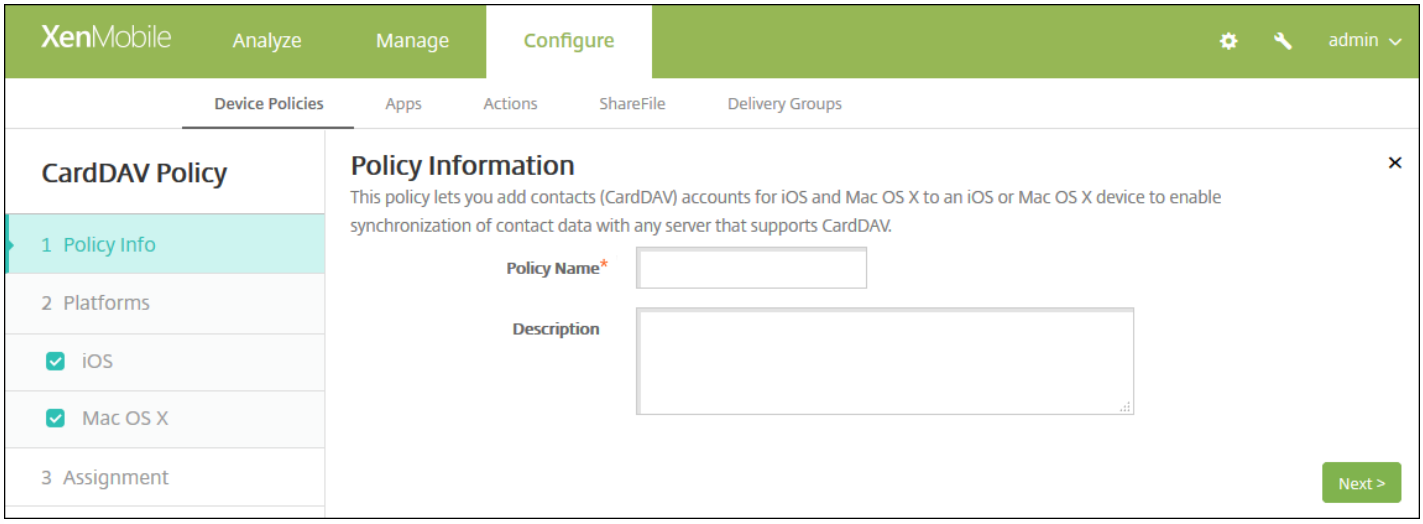
Nov 15, 2016

You can add a device policy in XenMobile to add an iOS contacts (CardDAV) account to users' iOS or Mac OS X 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:

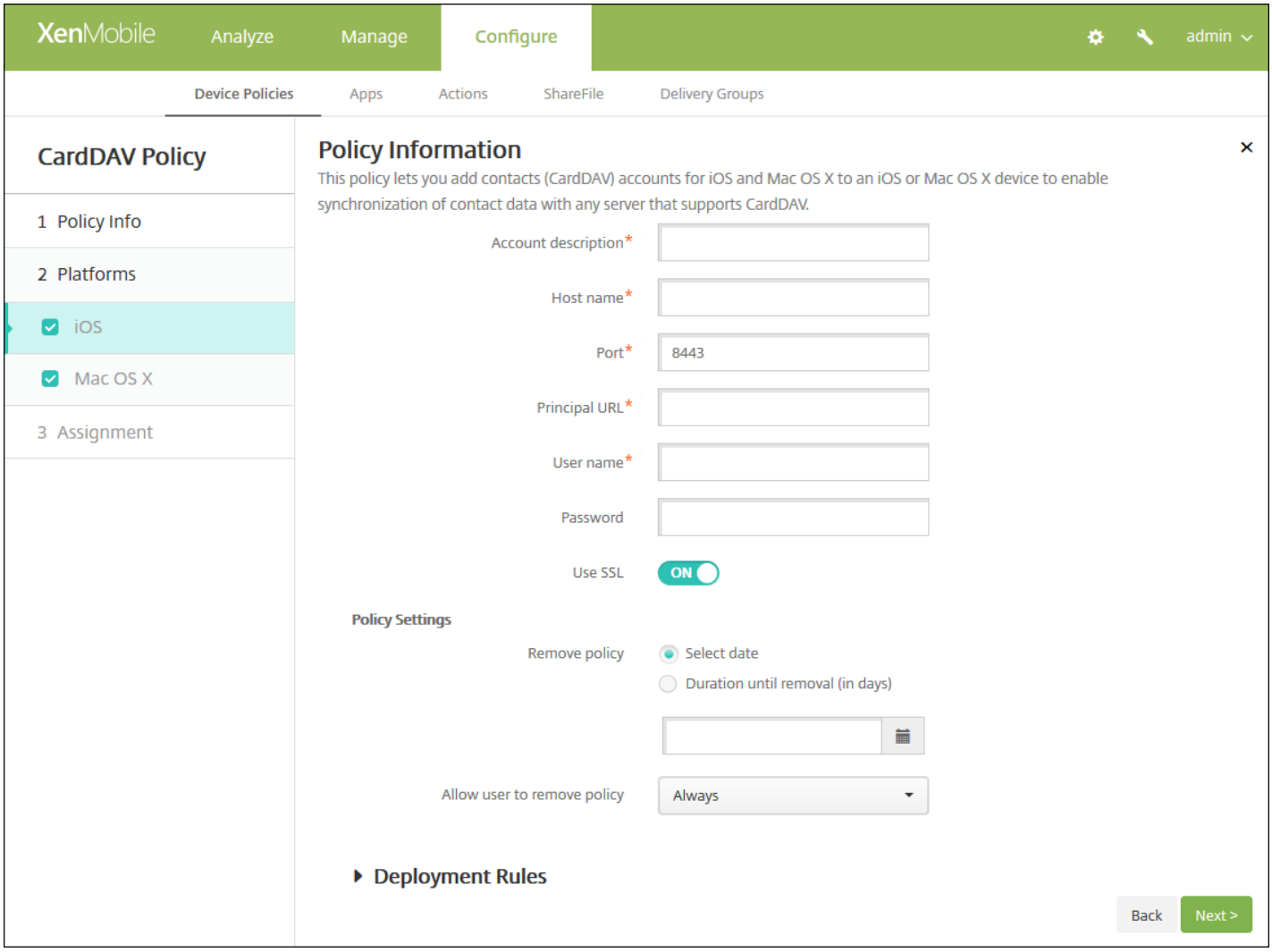
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

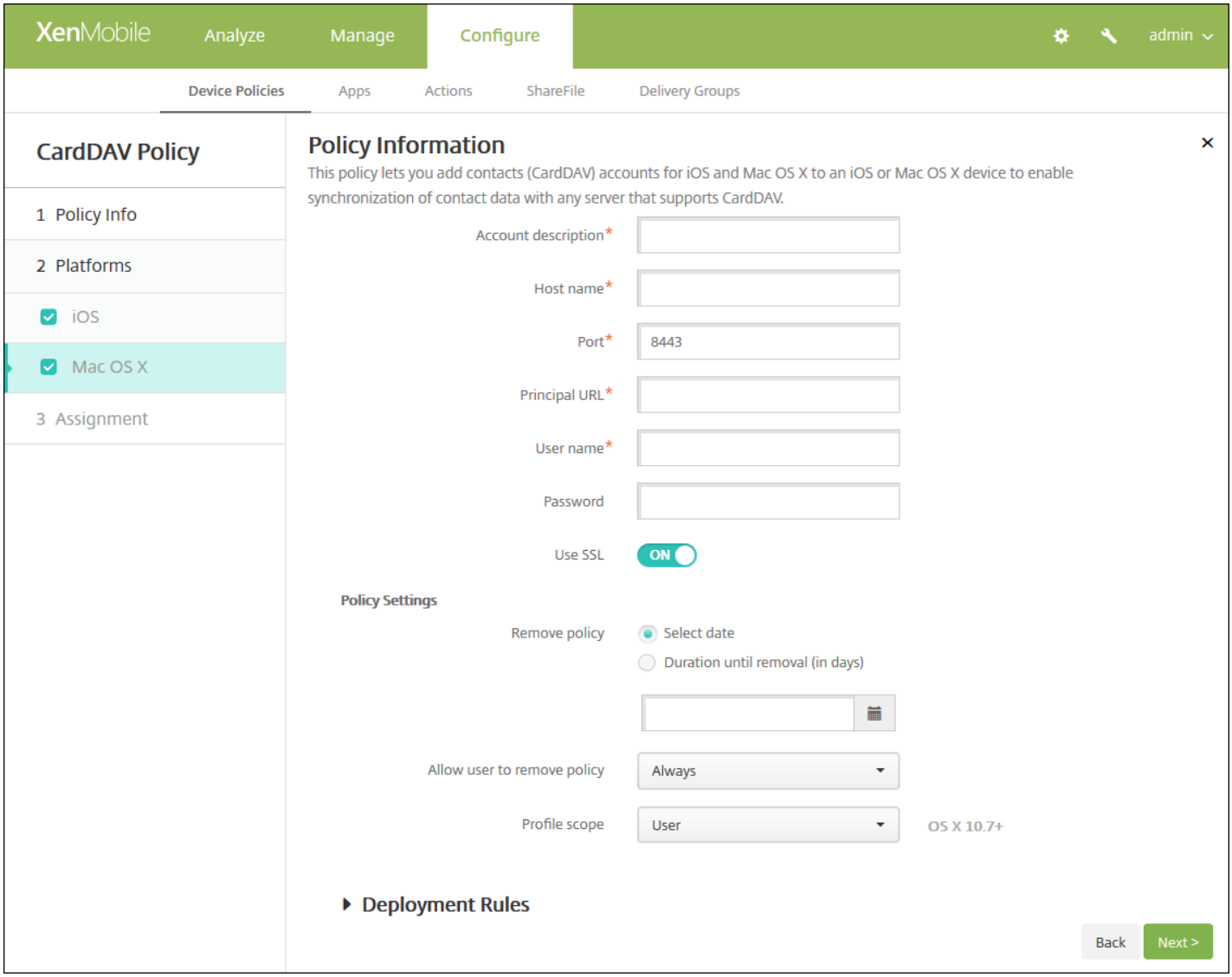
Configure iOS settings



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 days)**.
  - 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 Mac OS X settings

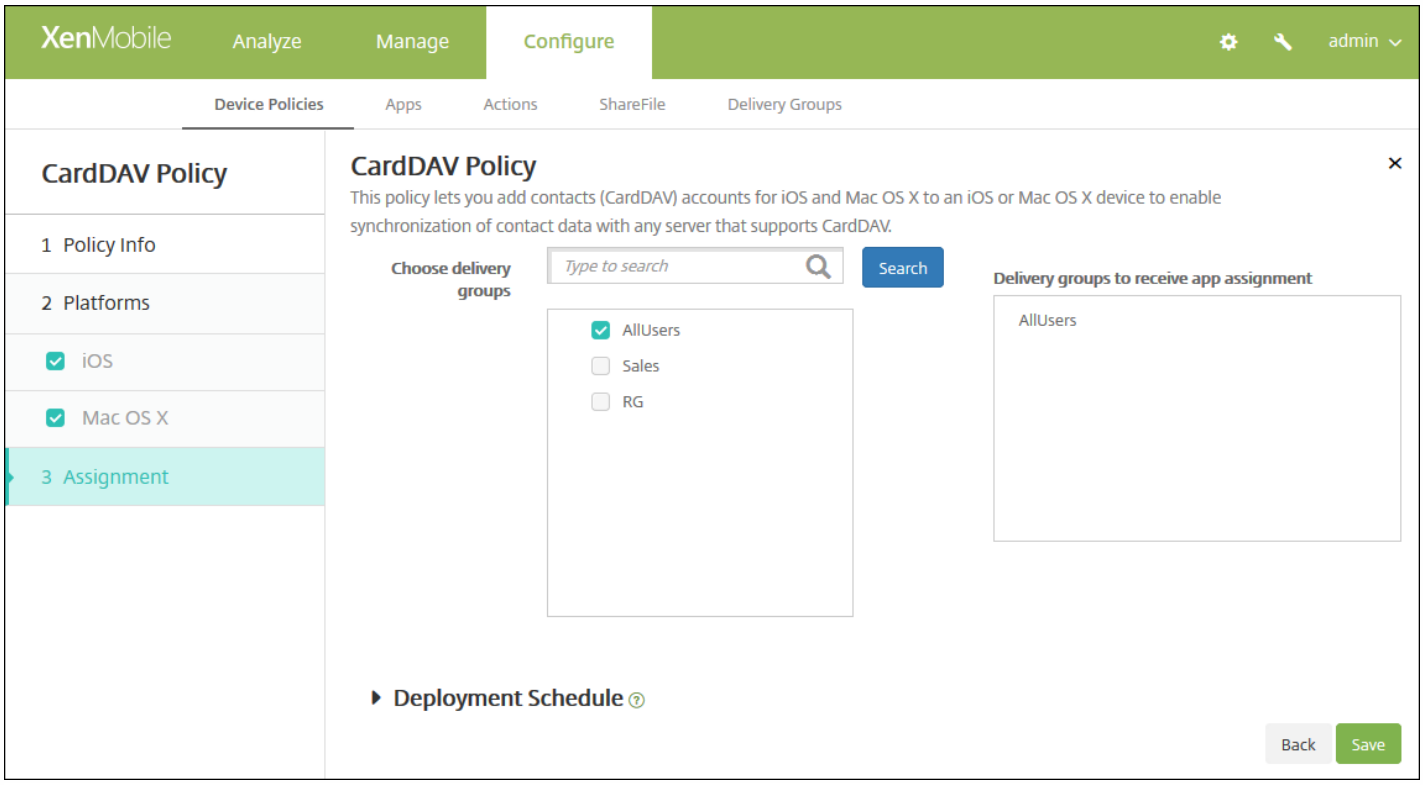


Configure these settings:

- **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 days)**.
  - 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 OS X 10.7 and later.

7. Configure the deployment rules

8. Click **Next**. The **CardDAV 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**.

Copy Apps to Samsung Container device policy

Nov 15, 2016

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.

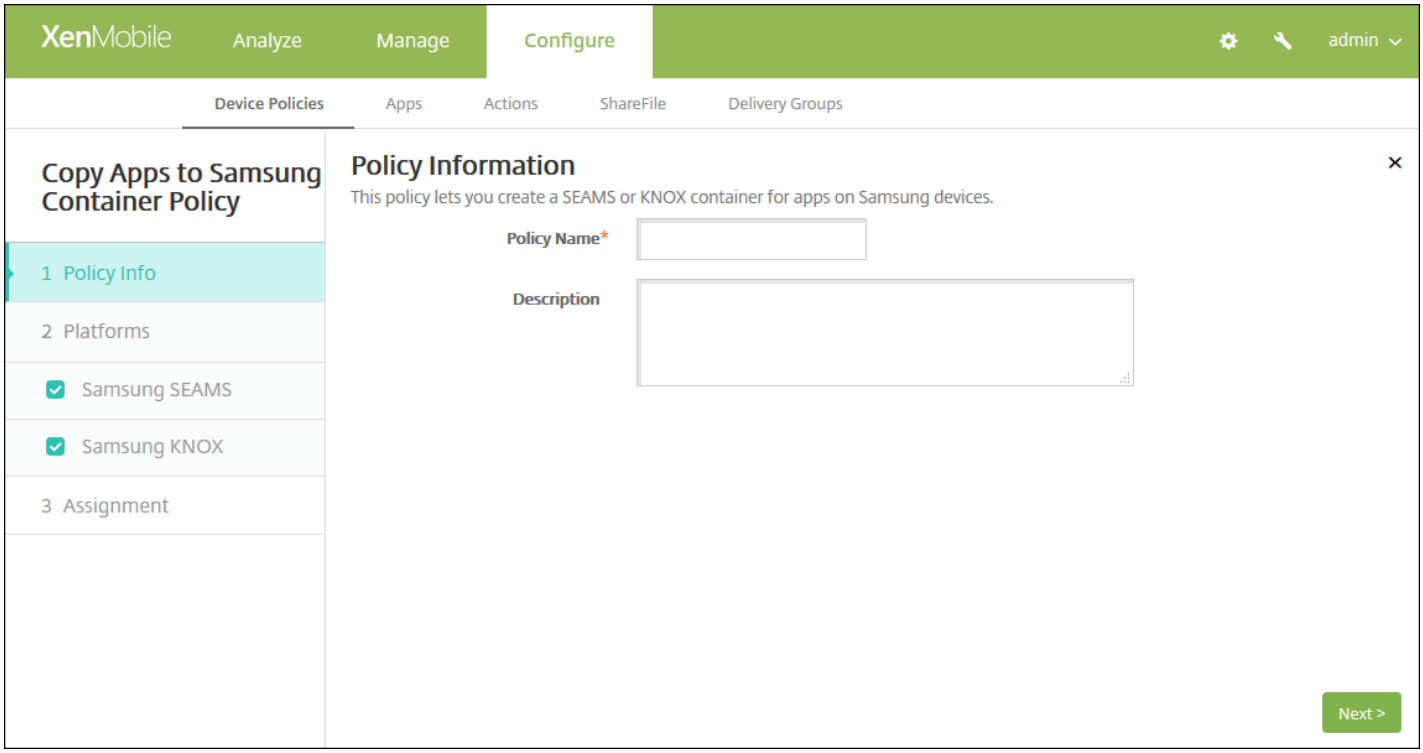
Prerequisites:

- 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.

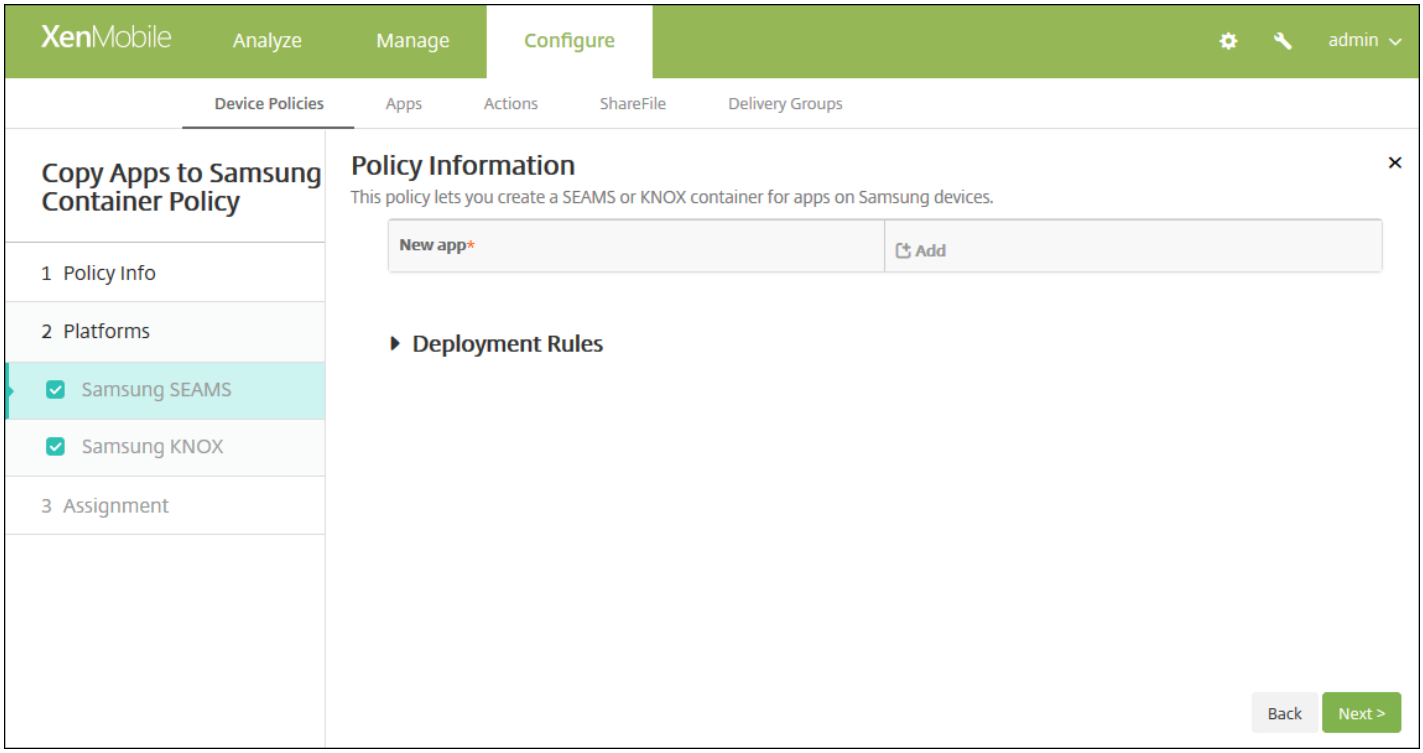
3. Expand **More**, and then under **Security**, click **Copy Apps to Samsung Container**. The **Copy Apps to Samsung Container Policy** information page appears.



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.

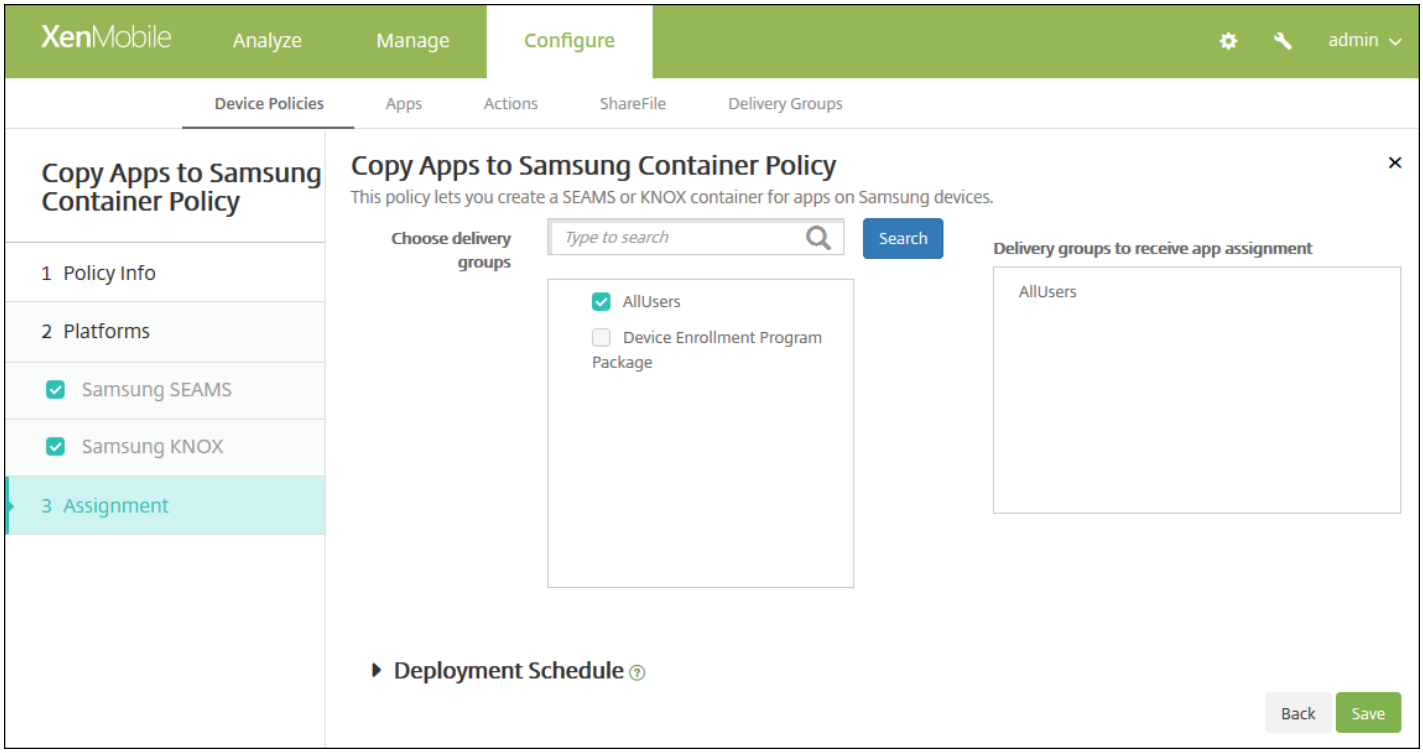
- **New app**: For each app you want to add to the list, click **Add** and then do the following:
  - Type a package ID; for example, com.mobiwolf.lacingart fo the LacingArt app.
  - Click **Save** or **Cancel**.

    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 the deployment rules

9. Click **Next**. The next platform page or **Copy Apps to Samsung Container 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**. 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.

12. Click **Save** to save the policy.

After the policy is successfully deployed, the SEAMS apps appear on the **Device details** page under the heading **Location: Enterprise SEAMS Location**, and the KNOX apps appear under the heading **Location: Enterprise Location**.

Credentials device policy

Jan 12, 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, Mac OS X, 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

Mac OS X settings

Android and Android for Work settings

Windows desktop/tablet settings

Windows Mobile/CE settings

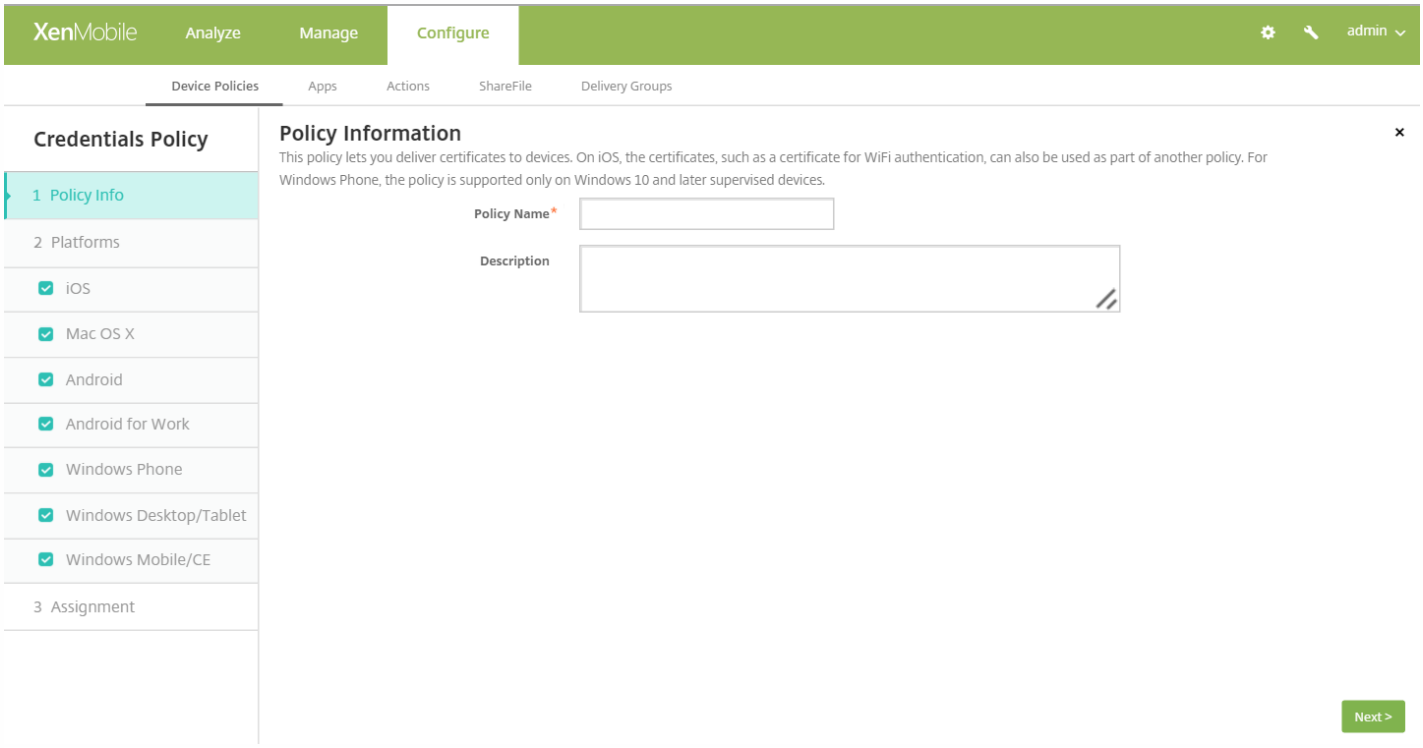
Windows Phone settings

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:

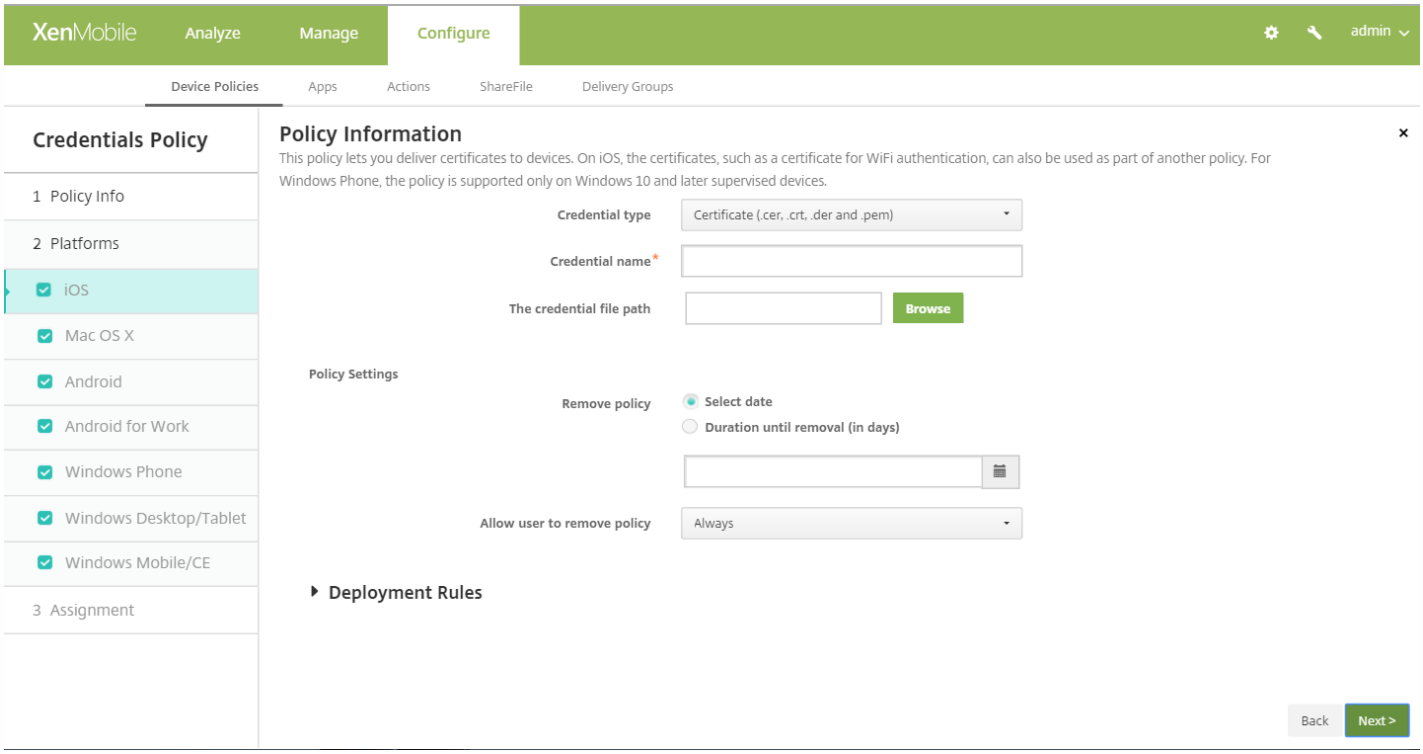
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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



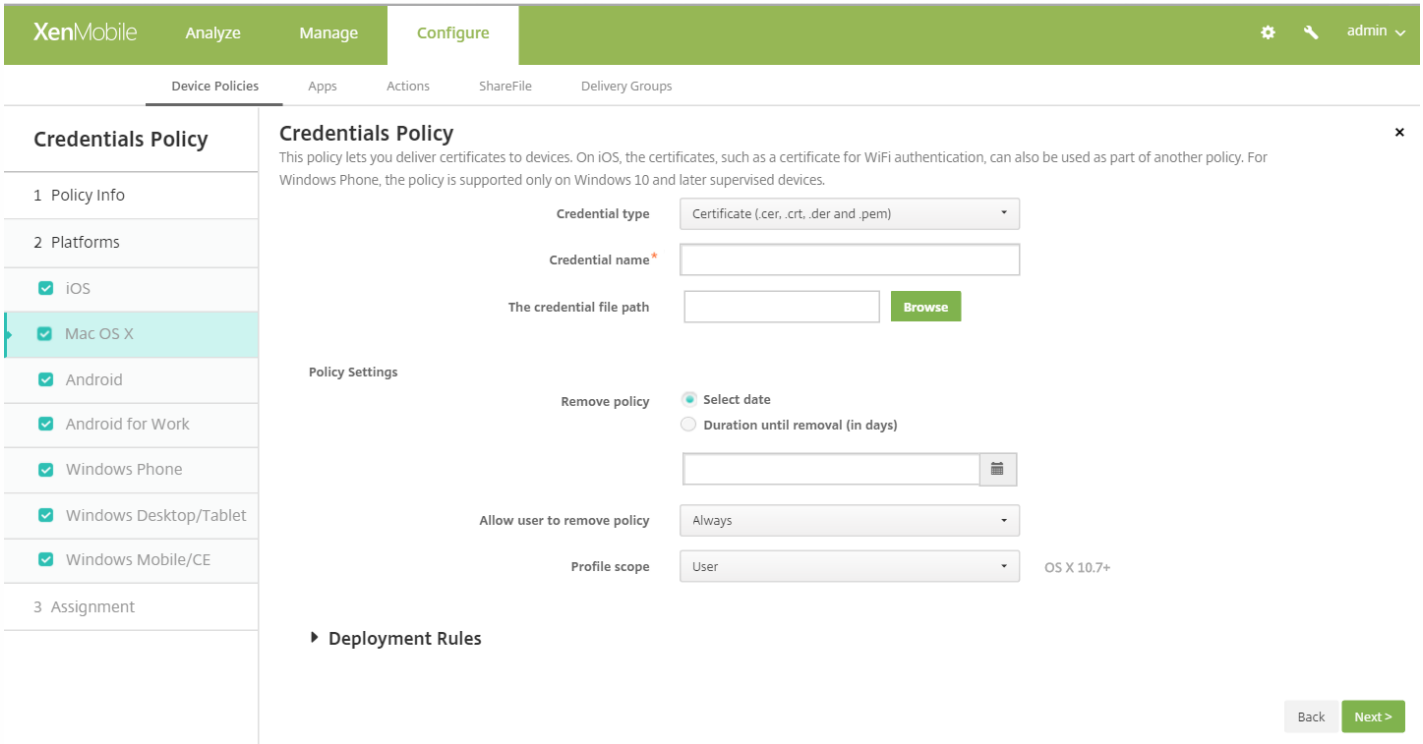
Configure the following settings:

- **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 days)**.
  - 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 Mac OS X settings

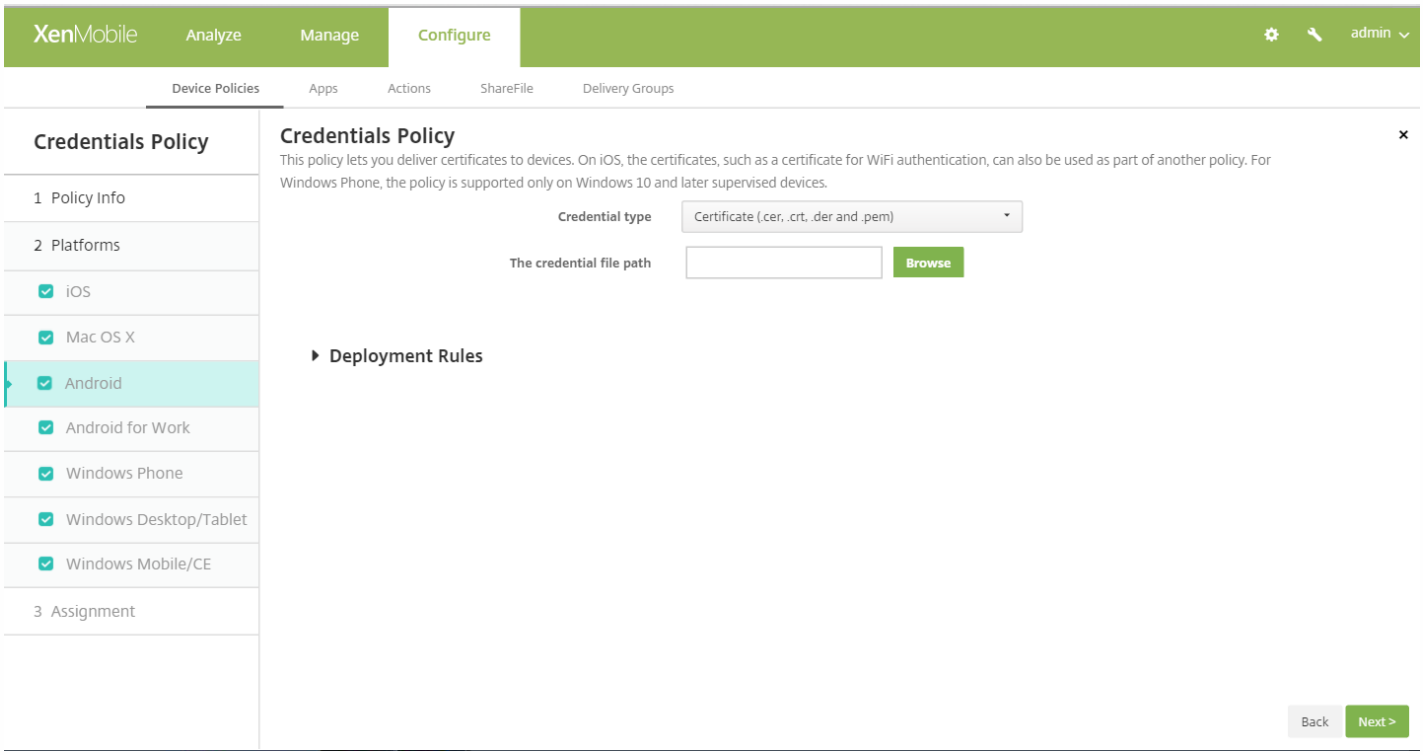


Configure the following settings:

- **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 days)**.
  - 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 OS X 10.7 and later.

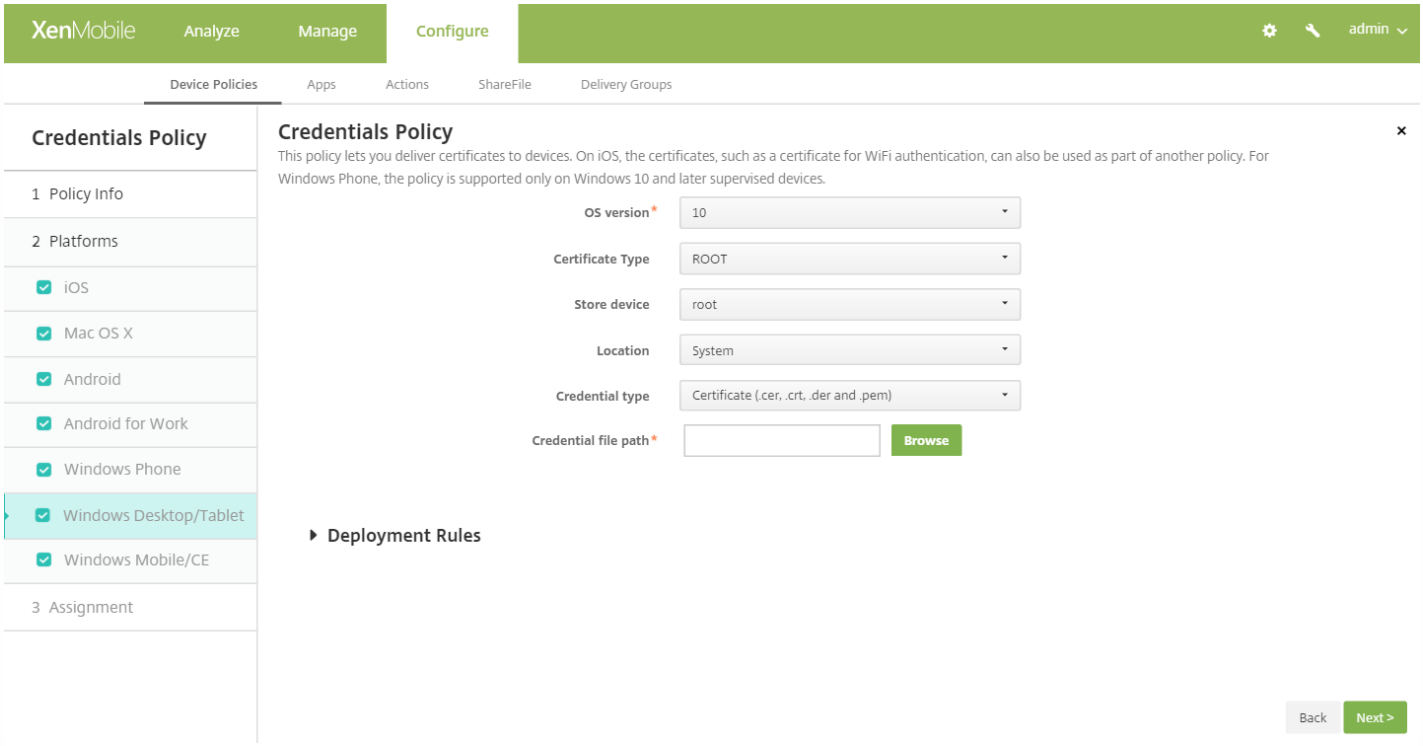
Configure Android and Android for Work settings



Configure the following settings:

- **Credential type**: In the list, click the type of credential to use with this policy and then, enter the following information for the selected credential:
  - **Certificate**
    - **Credential name**: 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



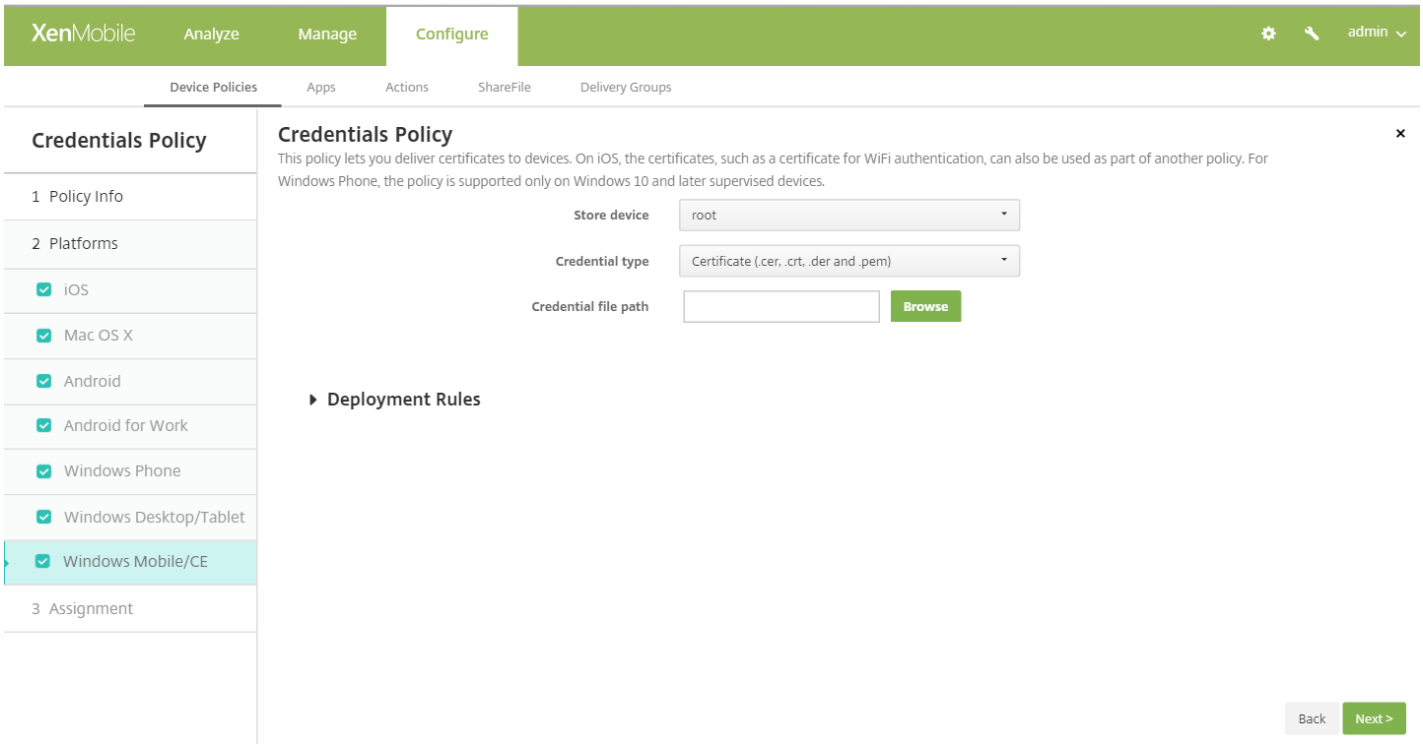
Configure the following settings:

- **OSVersion**: In the list, click either **8.1** for Windows 8.1 or **10** for Windows 10. The default is **10**.

Windows 10 settings

Windows 8.1 settings

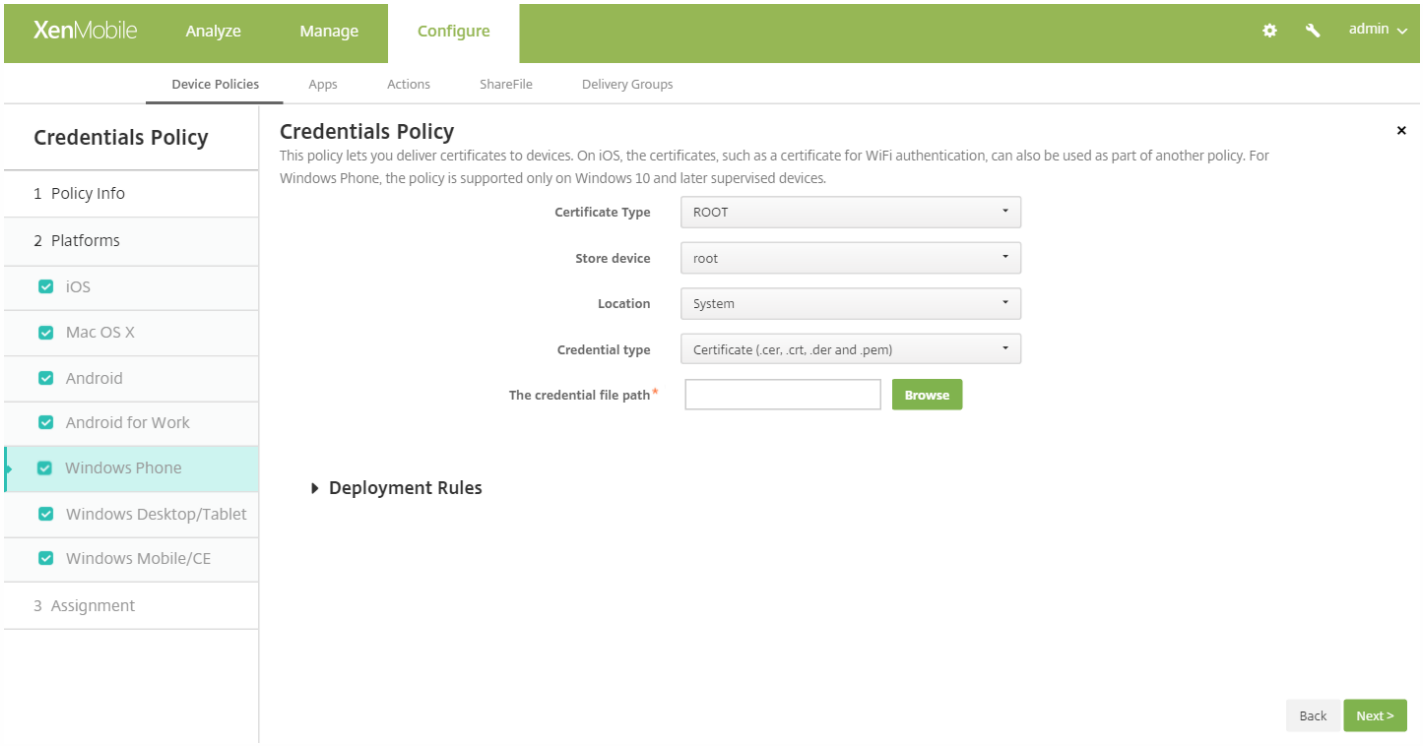
Configure Windows Mobile/CE settings



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

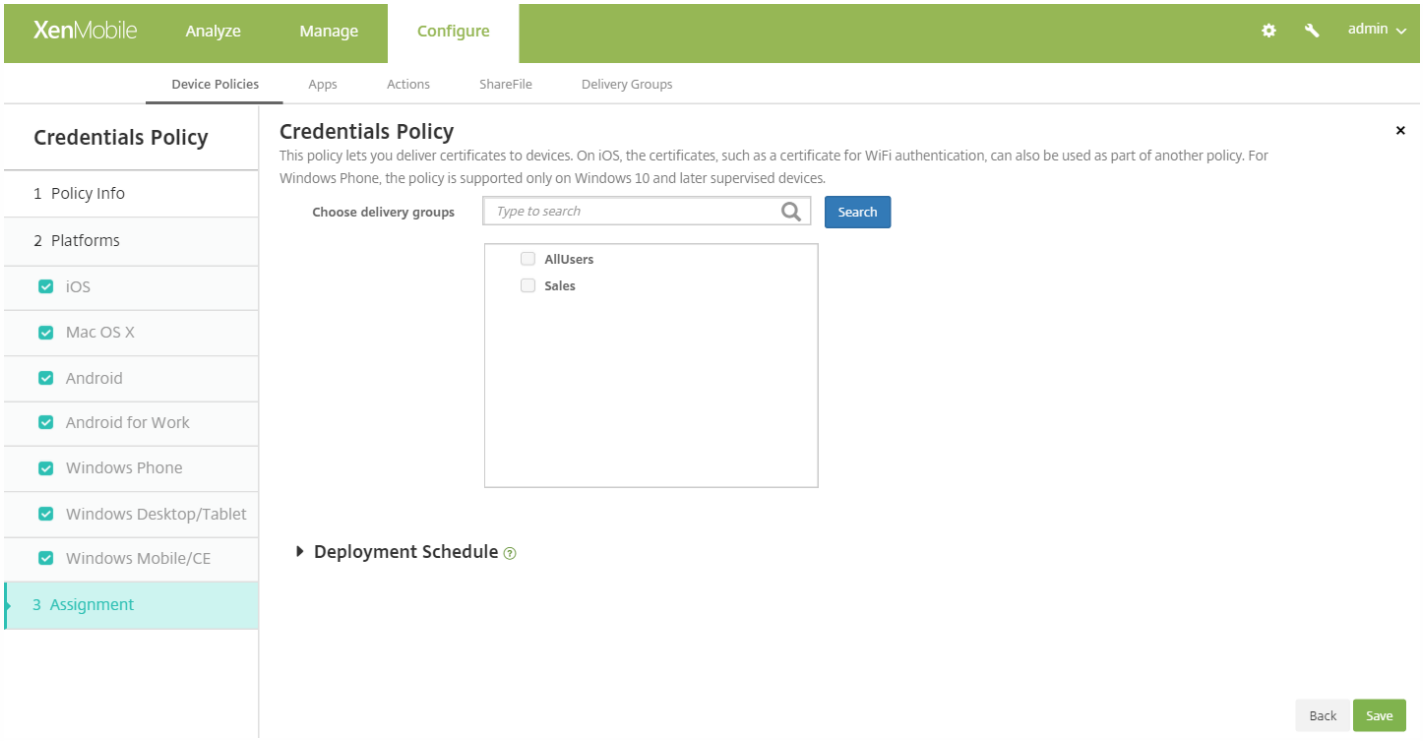


Configure the following settings:

- **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 the deployment rules

8. Click **Next**. The **Credentials 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**.

Custom XML device policy

Nov 15, 2016

You can create custom XML policies in XenMobile when you want to customize the following features on Windows Phone, Windows Desktop/Tablet, and Windows Mobile/CE devices:

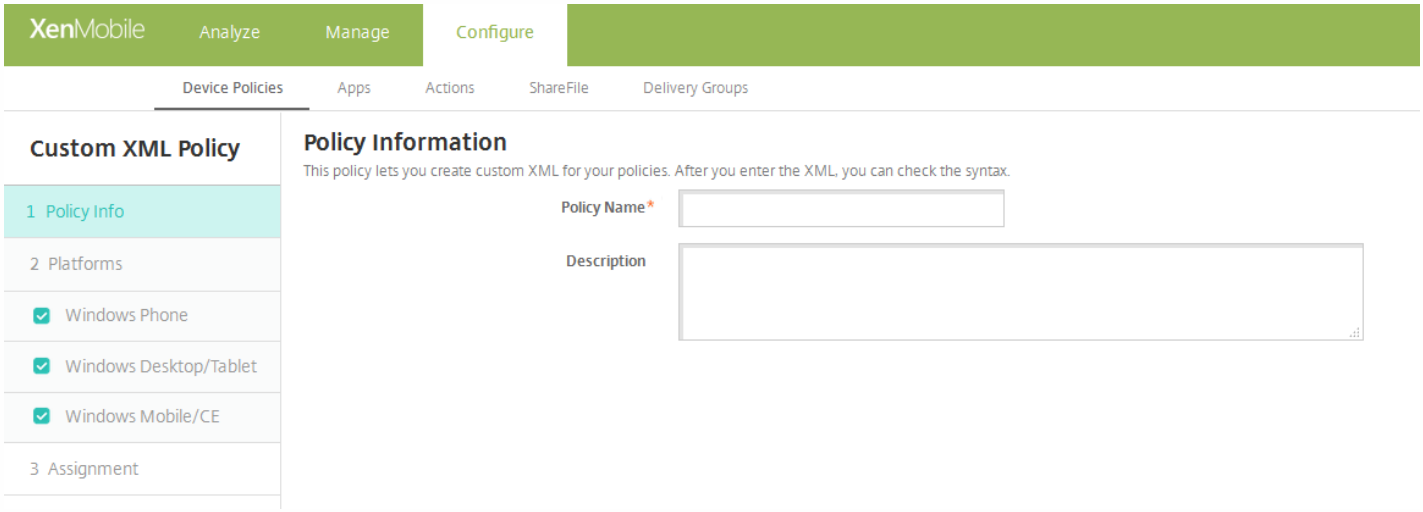
- Provisioning, which includes configuring the device, and enabling or disabling features
- Device configuration, which includes allowing users to change settings and device parameters
- Software upgrades, which includes providing new software or bug fixes to be loaded onto the device, including apps and system software
- Fault management, which includes receiving error and status reports from the device

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.

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

2. Click **Add**. The **Add New Policy** dialog box appears.

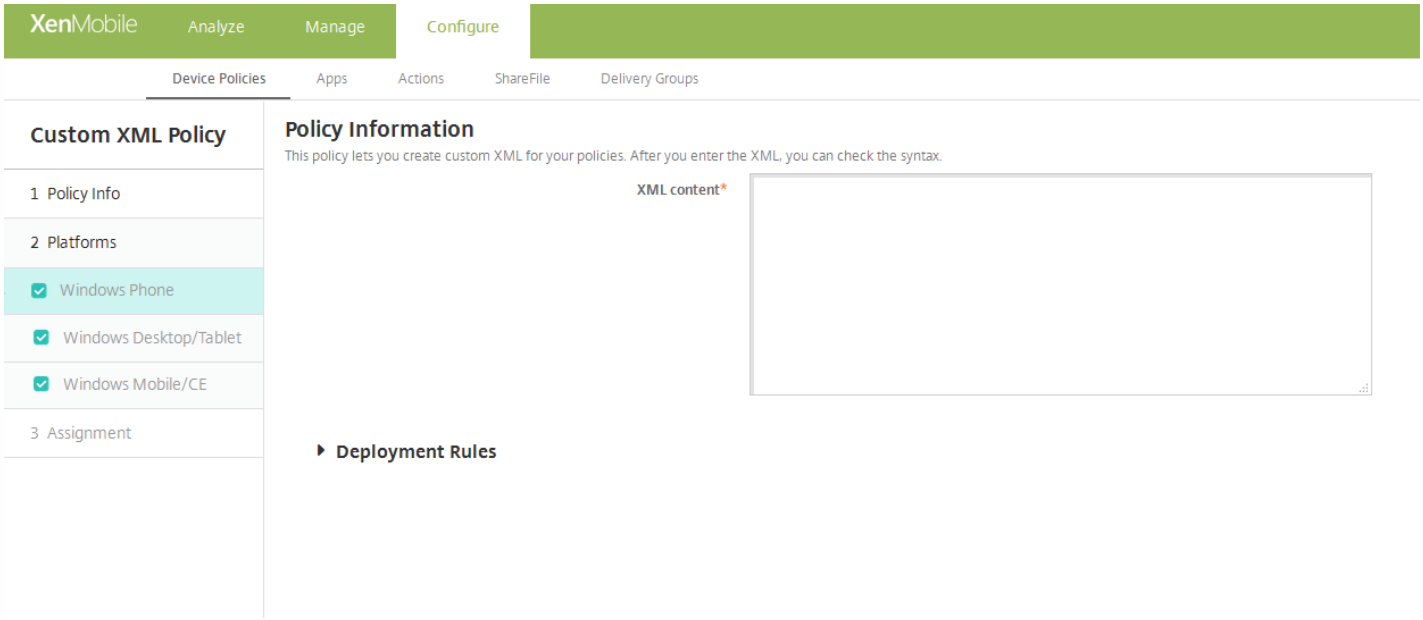
3. Expand **More** and then under **Custom**, click **Custom XML**. The **Custom XML Policy** information page appears.



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 the deployment rules

9. Click **Next**. XenMobile checks the XML content syntax. Any syntax errors appear below the content box. You must fix any errors before you can 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**. 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 deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms.

12. Click **Save**.

Delete files and folders device policy

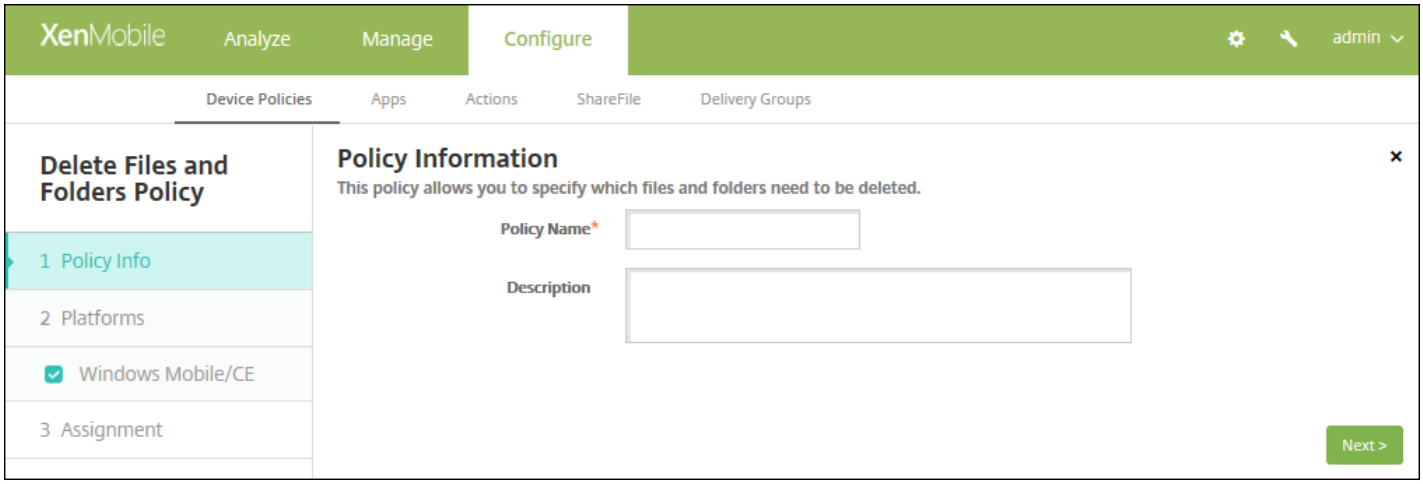
Nov 15, 2016

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.

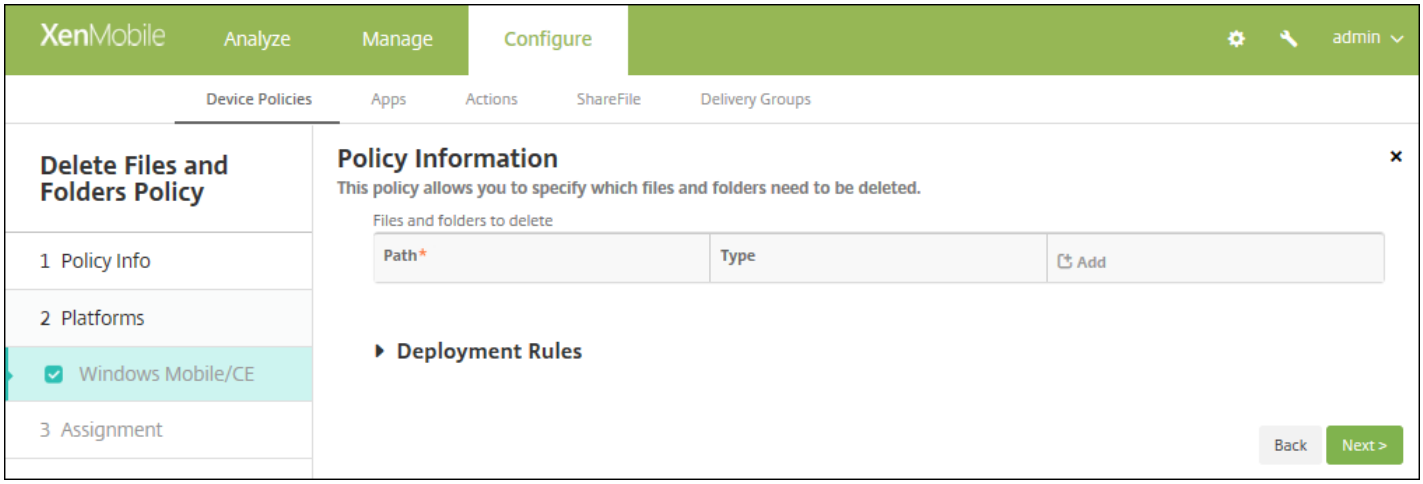
3. Expand **More** and then, under **Apps**, click **Delete Files and Folders**. The **Delete Files and Folders Policy** information page appears.



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:

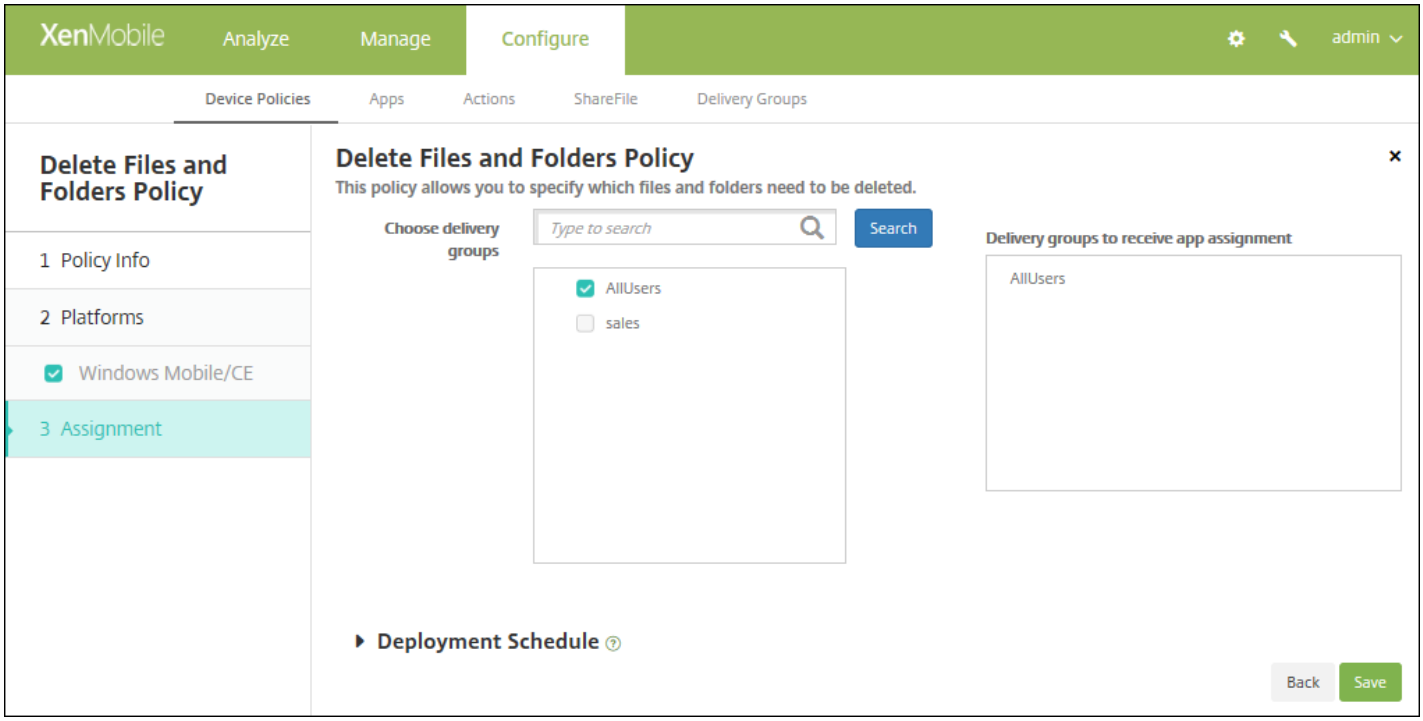
- **Files and folders to delete**: for each file or folder you want to delete, click Add and then do the following:
  - **Path**: Type the path to the file or folder.
  - **Type**: In the list, click File or Folder. The default is File.
  - Click **Save** to save the file or folder, or click **Cancel** 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 the deployment rules

8. Click **Next**. The **Delete Files and Folders 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**.

Delete registry keys and values device policy

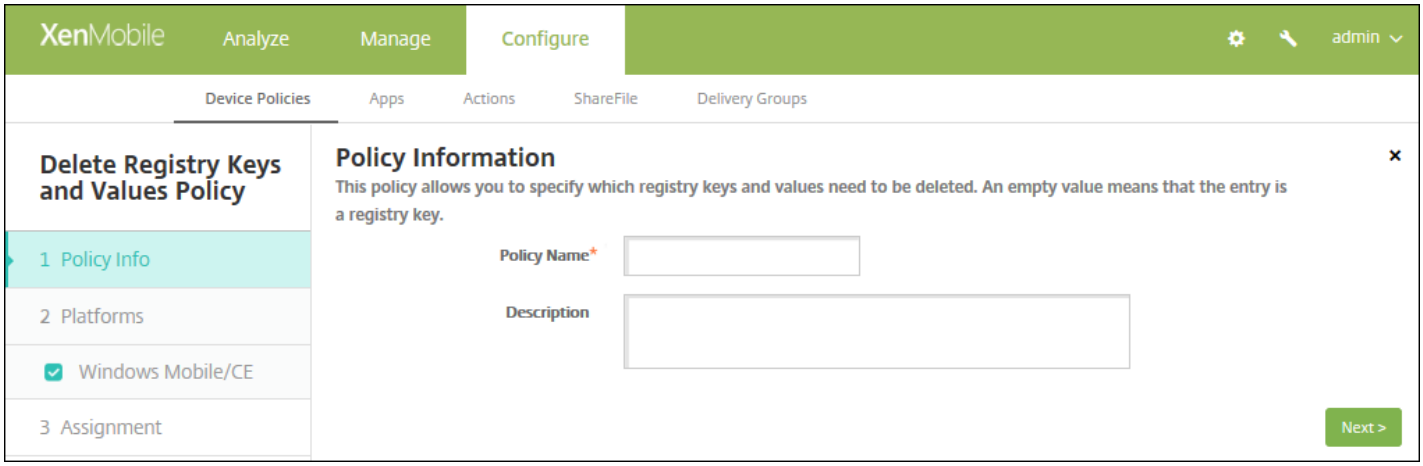
Nov 15, 2016

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.

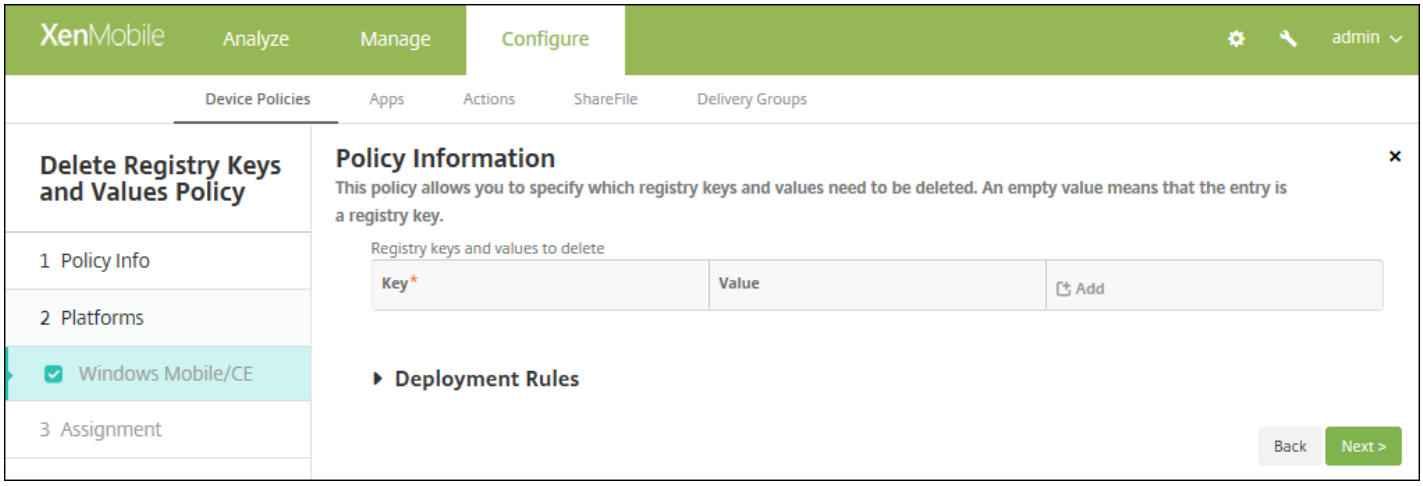
3. Expand **More** and then, under **Apps**, click **Delete Registry Keys and Values**. The **Delete Registry Keys and Values Policy** information page appears.



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:

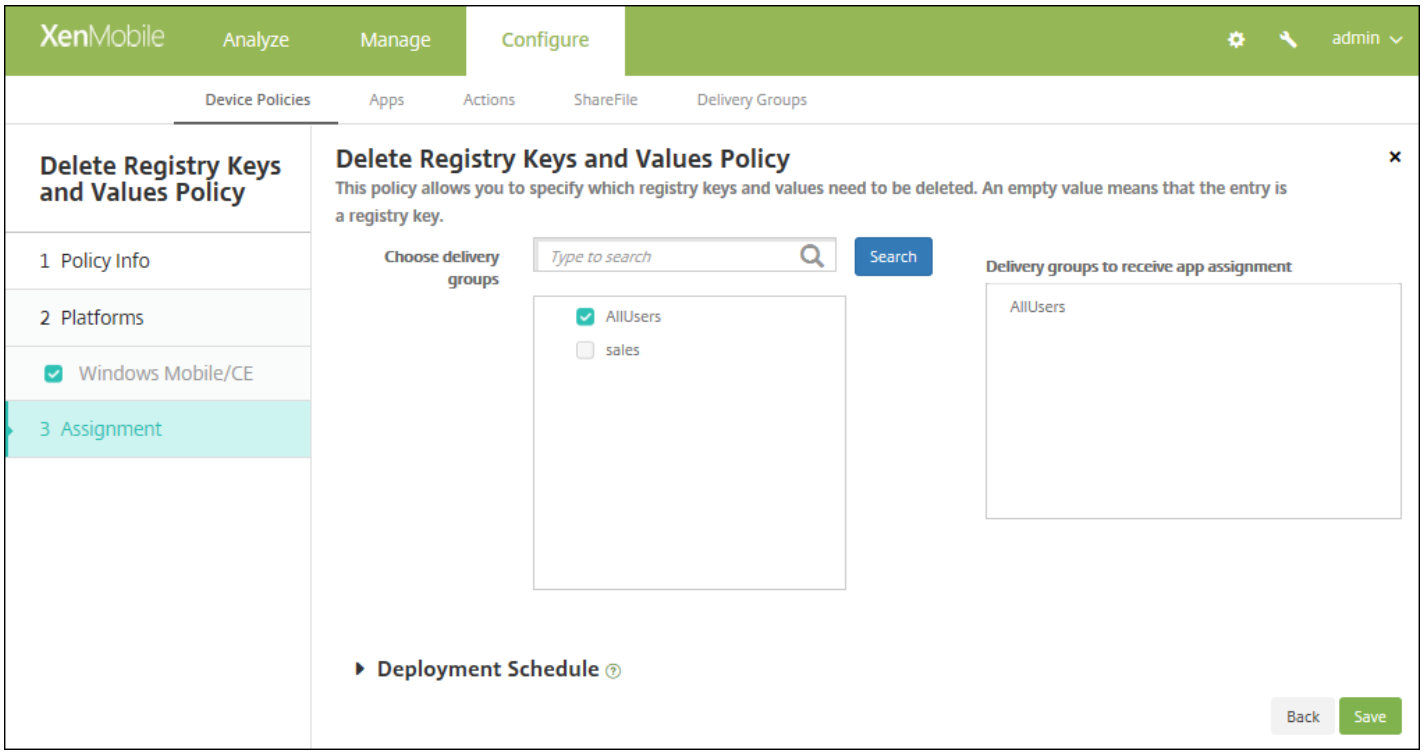
- **Registry keys and values to delete**: for each registry key and value you want to delete, click **Add** and then do the following:
  - **Key**: Type the registry key path. This is a required field.The registry key path should either start with HKEY_CLASSES_ROOT\ or HKEY_CURRENT_USER\ or HKEY_LOCAL_MACHINE\ 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 the deployment rules

8. Click **Next**. The **Delete Registry Keys and Values 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**.

Device Health Attestation device policy

Nov 15, 2016

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:

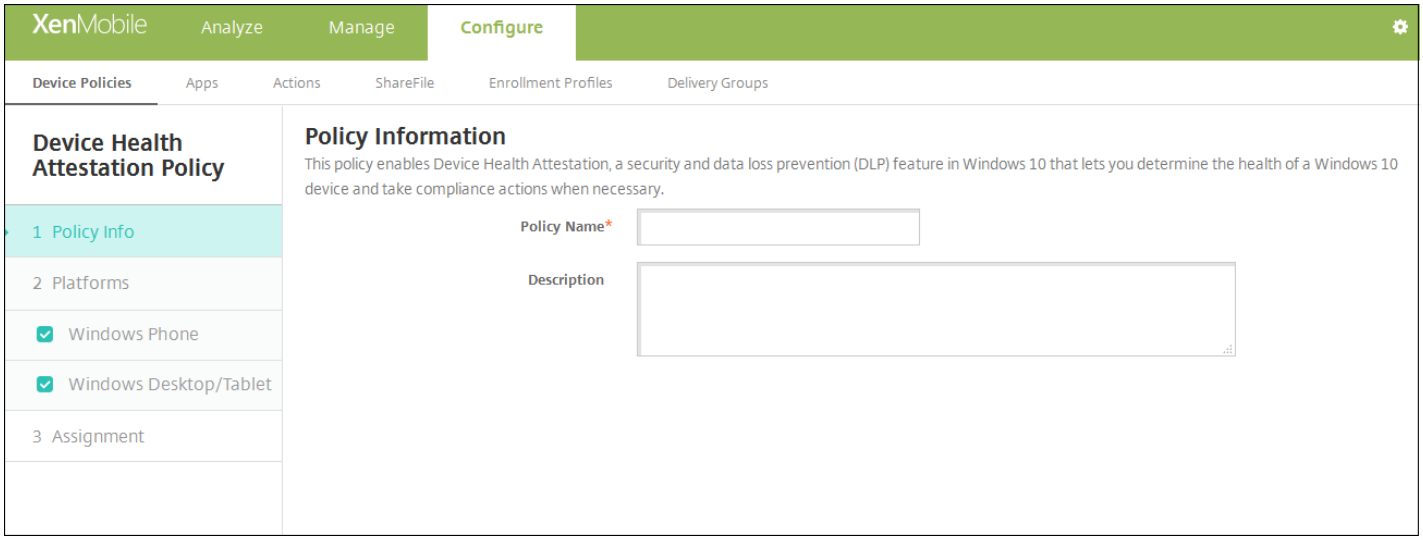
- AIK Present
- Bit Locker Status
- Boot Debugging Enabled
- Boot Manager Rev List Version
- Code Integrity Enabled
- Code Integrity Rev List Version
- DEP Policy
- ELAM Driver Loaded
- Issued At
- Kernel Debugging Enabled
- PCR
- Reset Count
- Restart Count
- Safe Mode Enabled
- SBCP Hash
- Secure Boot Enabled
- Test Signing Enabled
- VSM Enabled
- WinPE Enabled

For more information, refer to the Microsoft HealthAttestation CSP page.

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.



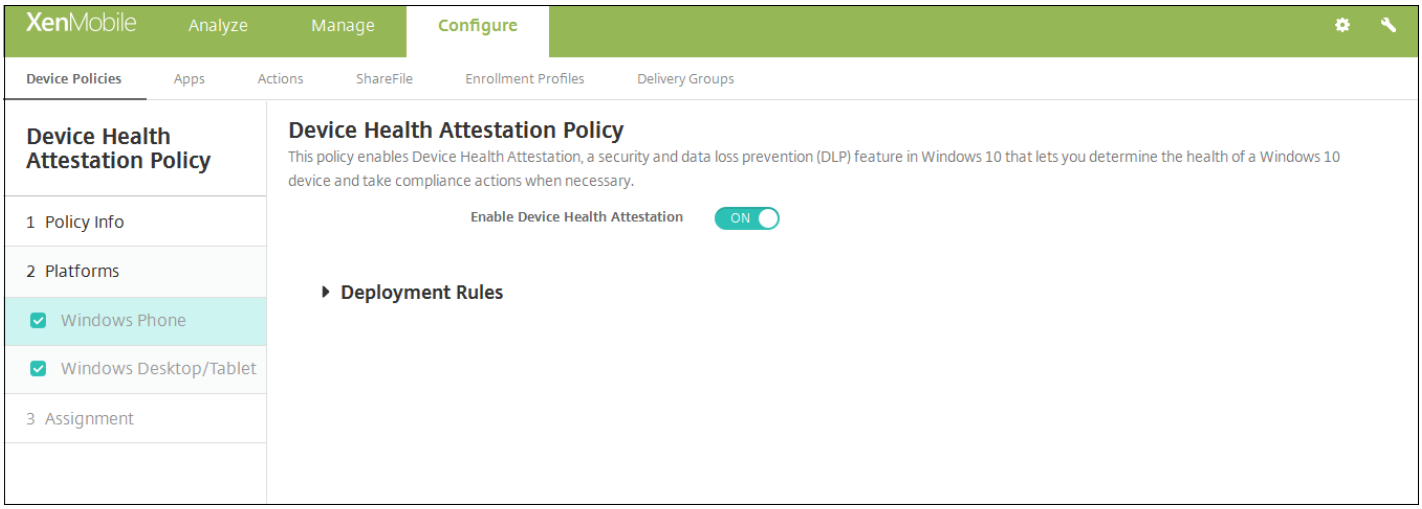
4. In the **Policy Information** pane, enter the following information:

- **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.

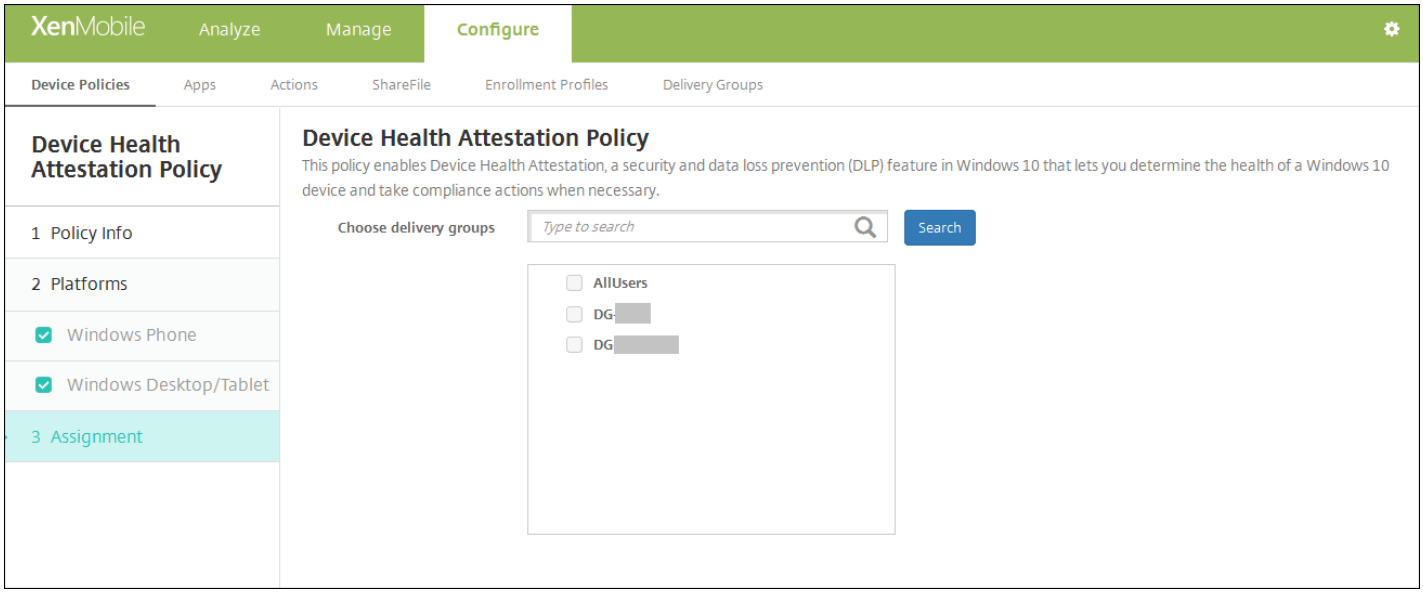


Configure this setting for each platform that you choose:

- **Enable Device Health Attestation**: Select whether to require Device Health Attestation. The default is **OFF**.

7. Configure the deployment rules

8. Click **Next**. The **Device Health Attestation** 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**.

Device name device policy

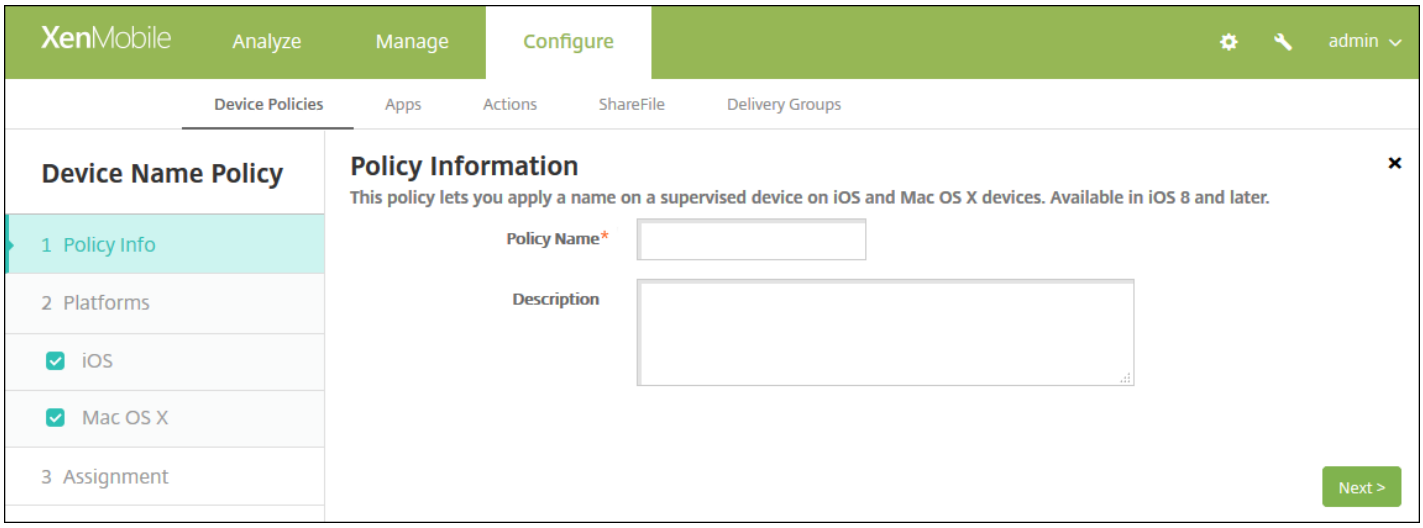
Nov 15, 2016

You can set the names on iOS and Mac OS X 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. See Macros in XenMobile for more information about macros.

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:

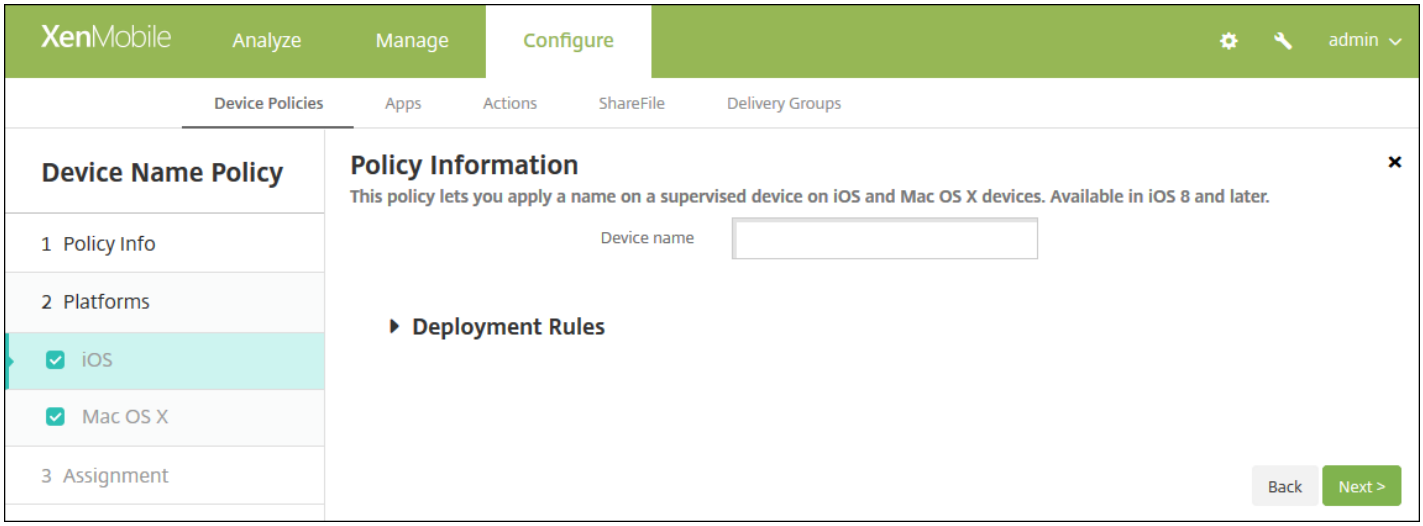
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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 Mac OS X settings

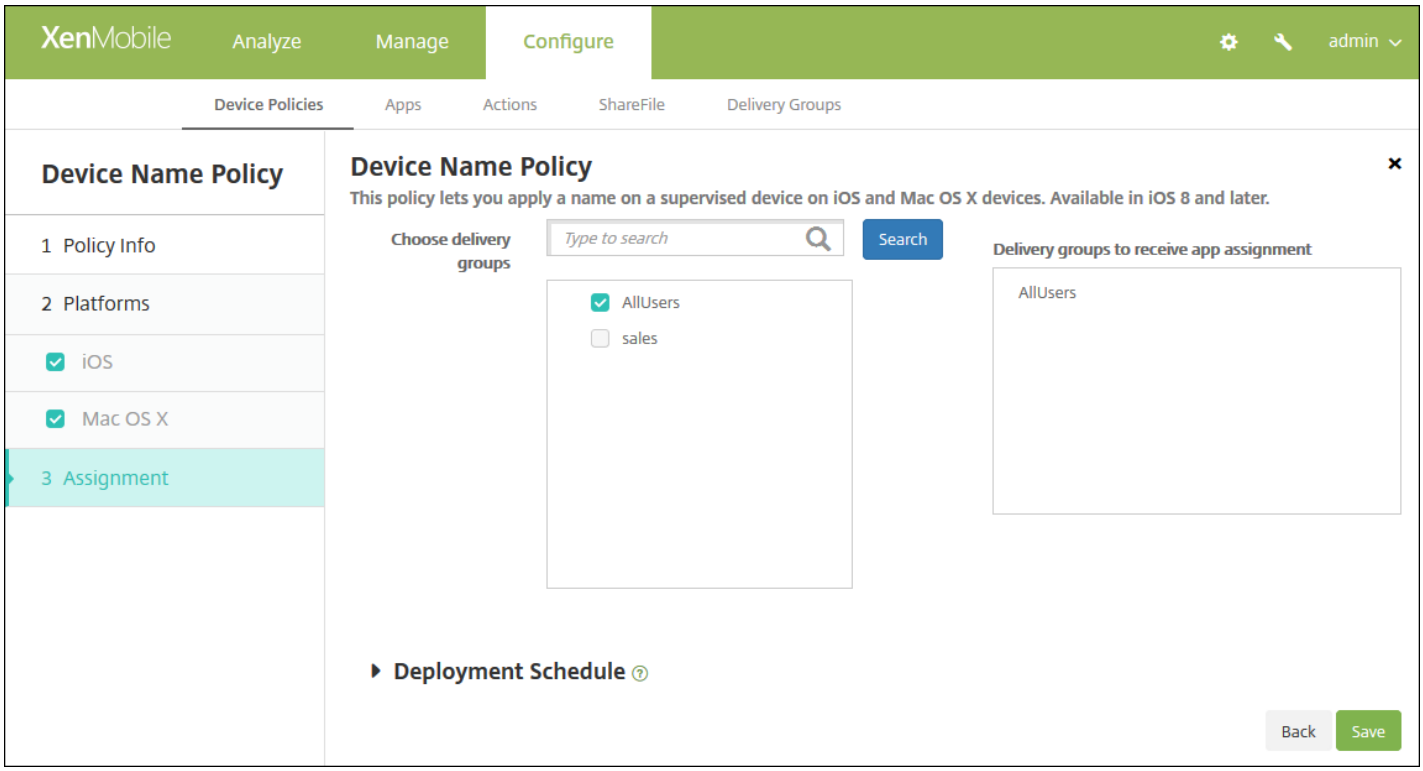


Configure this setting for the platforms you choose:

- **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 the deployment rules

8. Click **Next**. The **Device Name 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** to save the policy.

Enterprise Hub device policy

Nov 15, 2016

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:

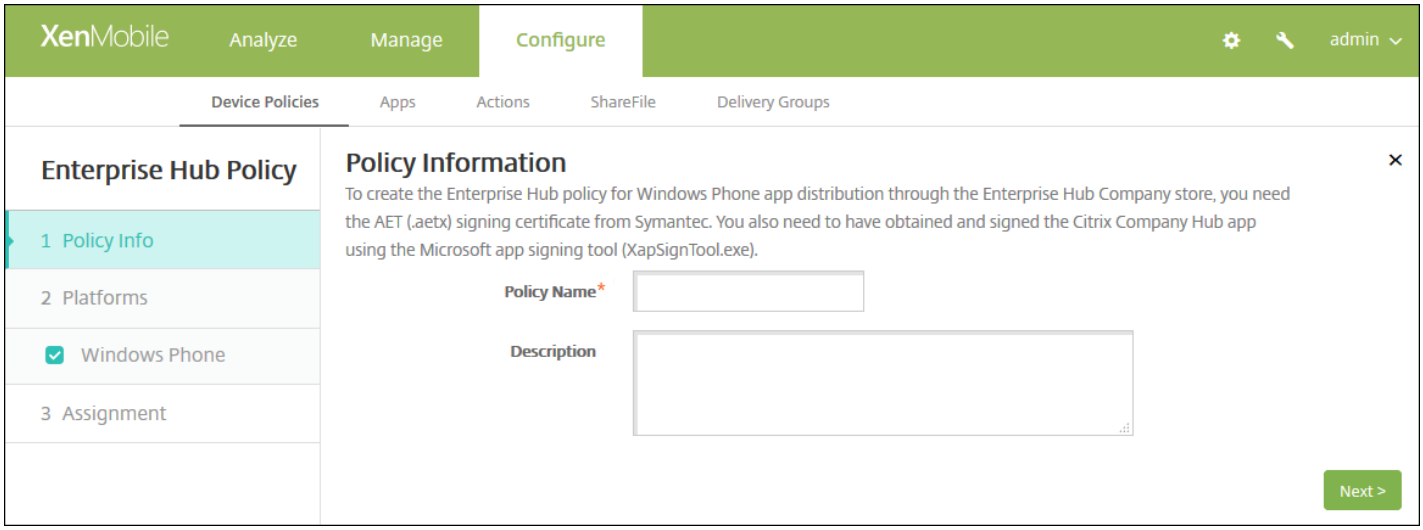
- An AET (.aetx) signing certificate from Symantec
- The Citrix Company Hub app signed by using the Microsoft app signing tool (XapSignTool.exe)

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.

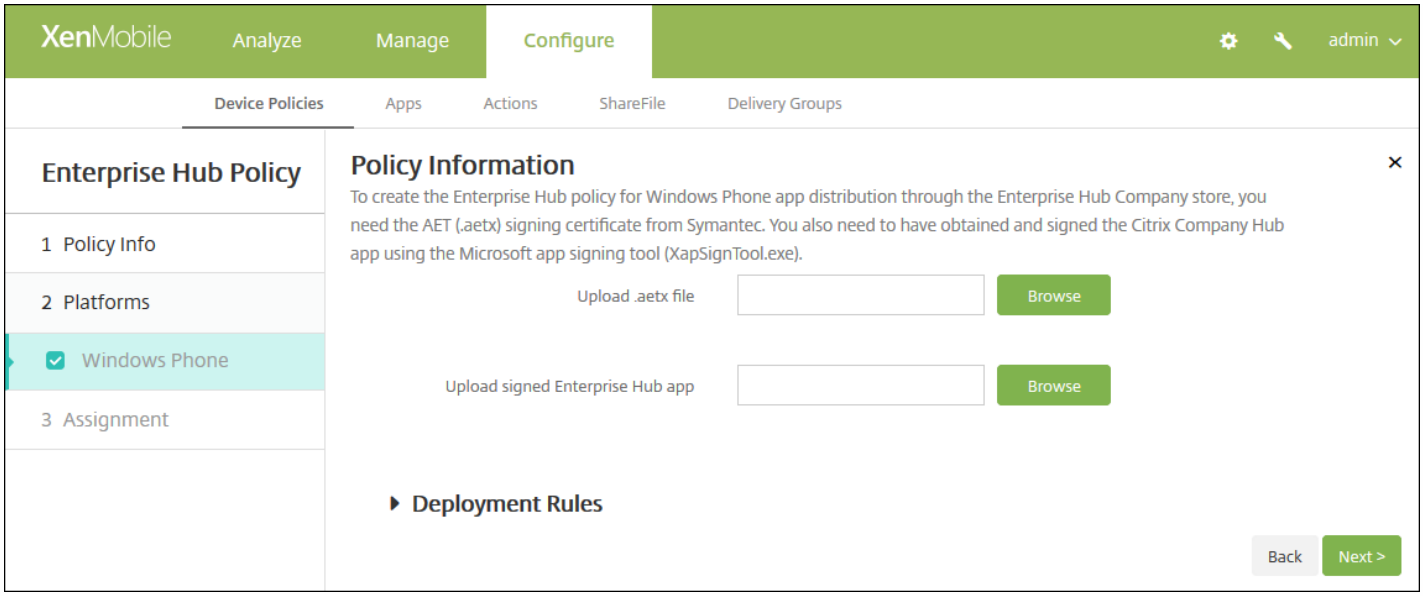
3. Expand **More** and then, under **XenMobile agent**, click **Enterprise Hub**. The **Enterprise Hub Policy** page appears.



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.

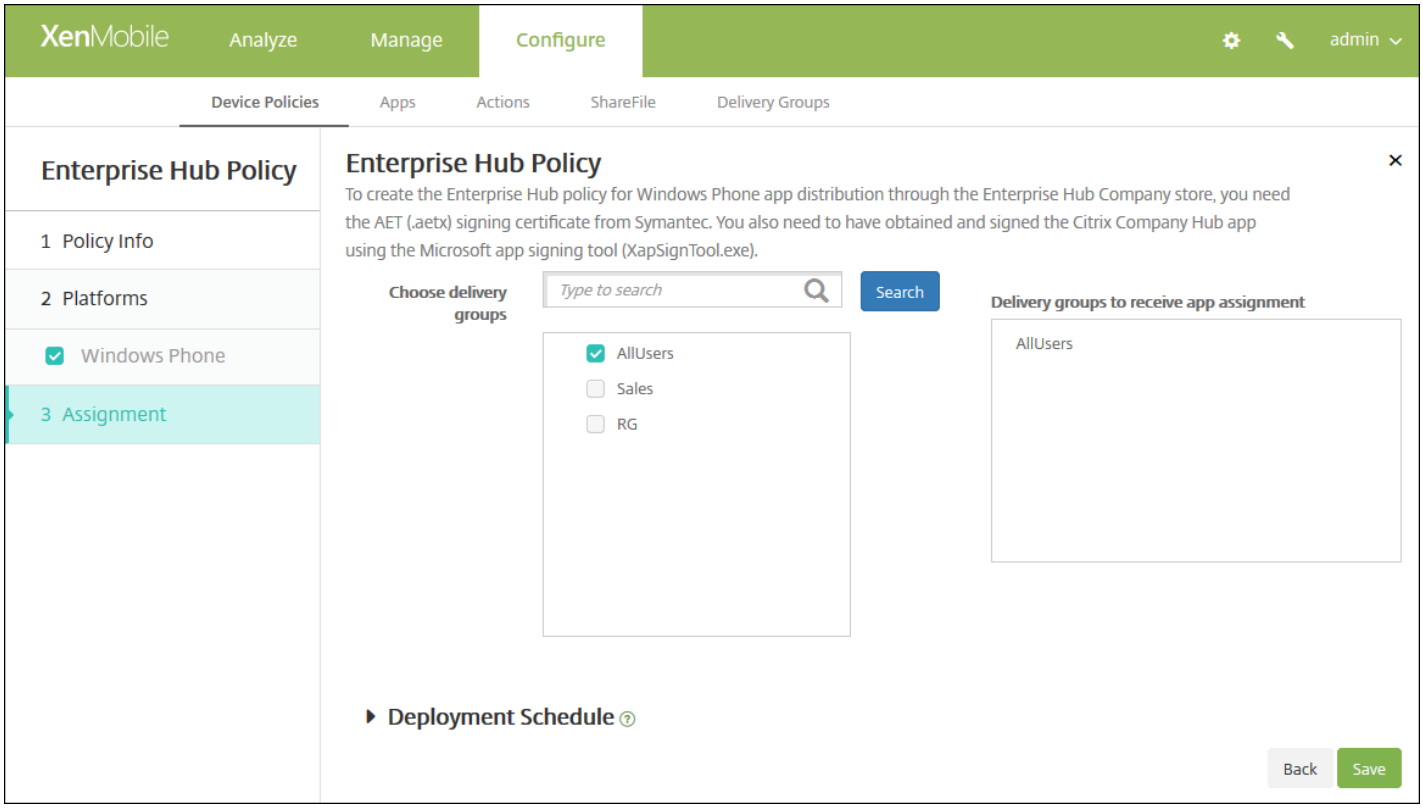


6. Configure these settings:

- **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 the deployment rules

8. Click **Next**. The **Enterprise Hub 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**.

Files device policy

Nov 15, 2016

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.

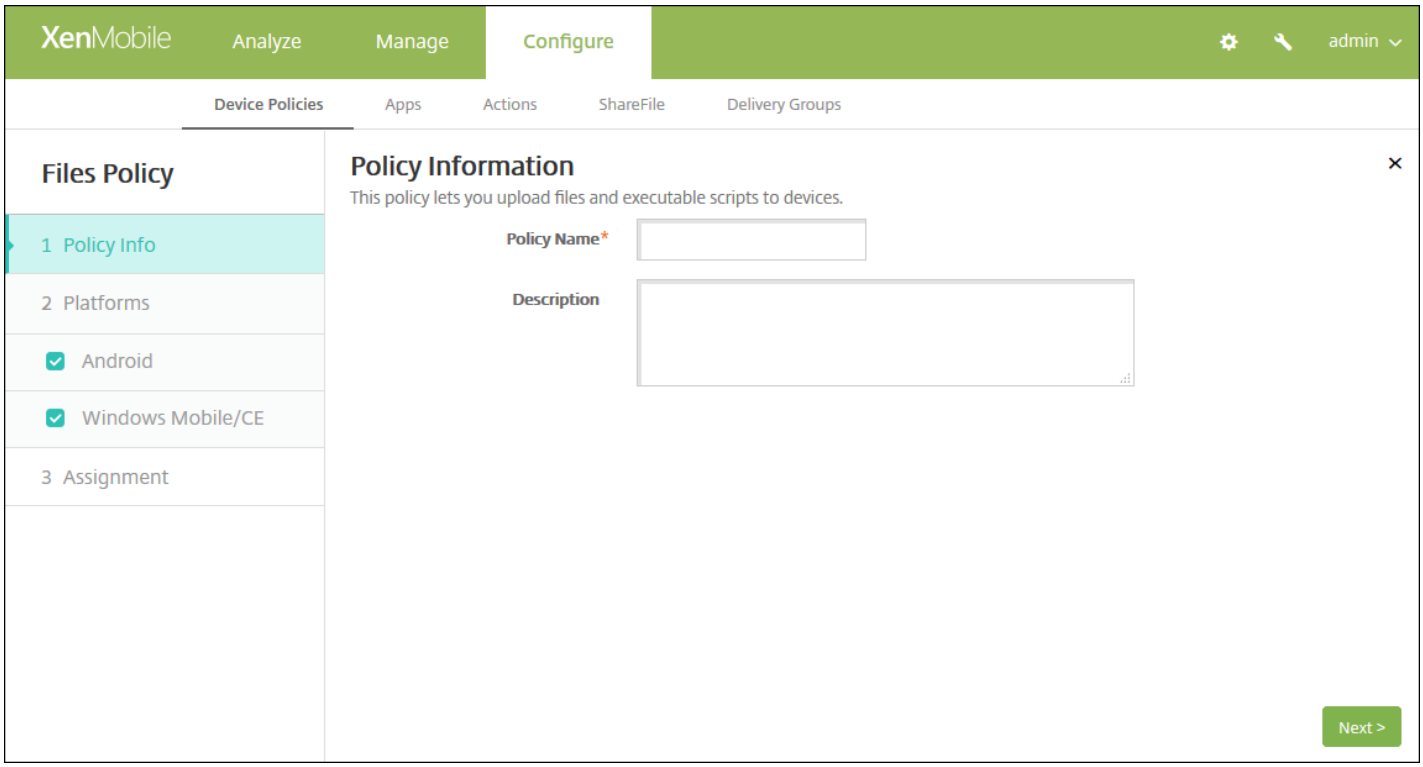
You can add the following file types with this policy:

- 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.

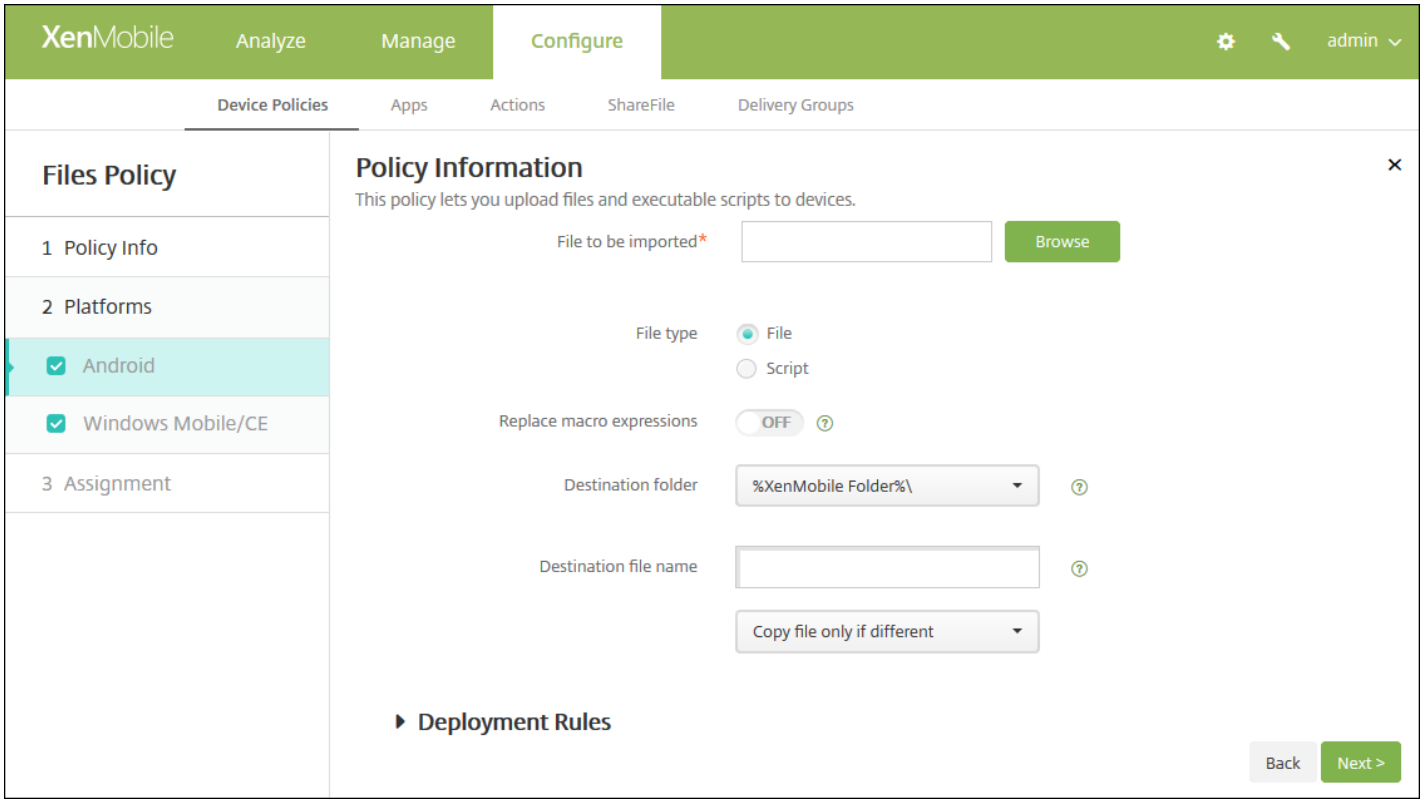
3. Expand **More** and then, under **Apps**, click **Files**. The **Files Policy** information page appears.



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.

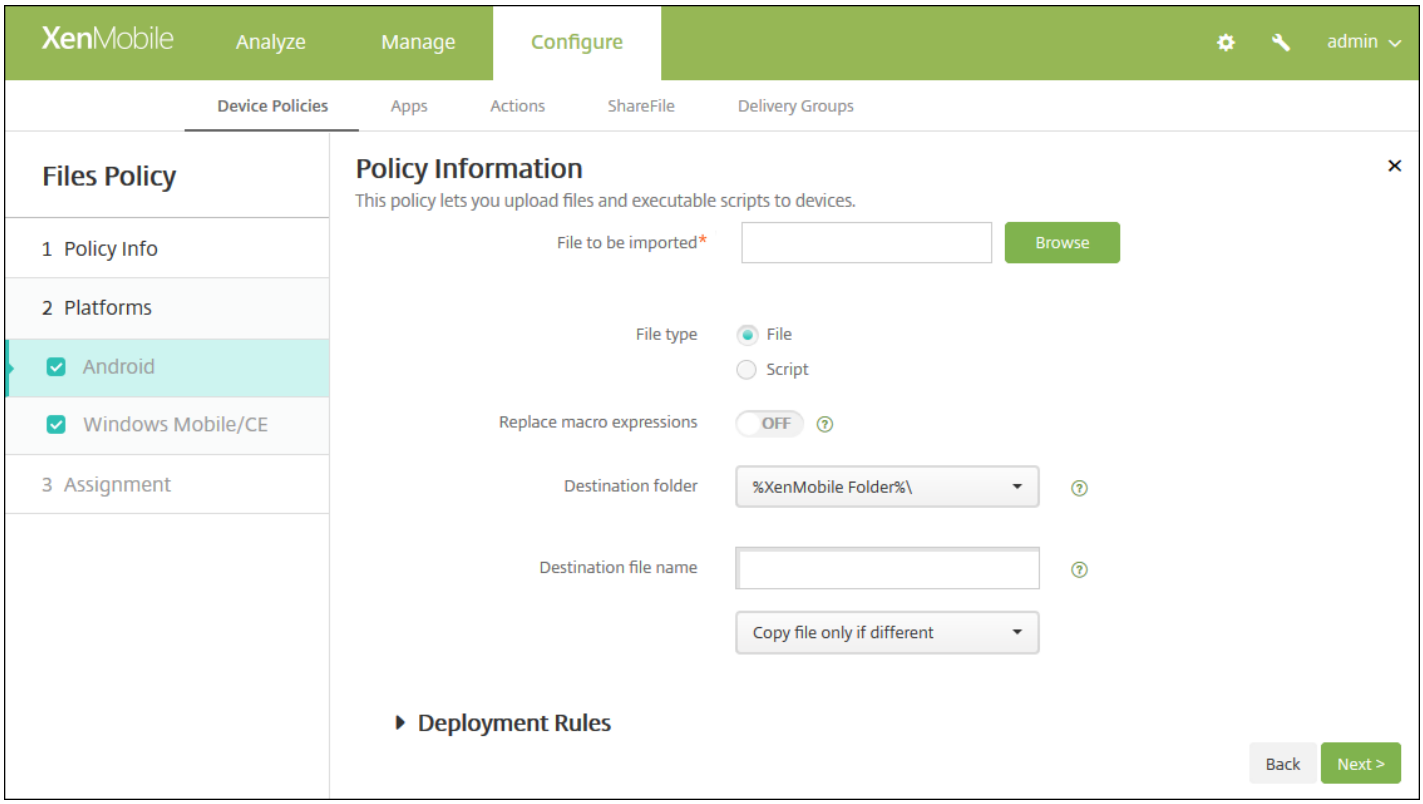
5. Click **Next**. The **Policy Platforms** page appears.



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.

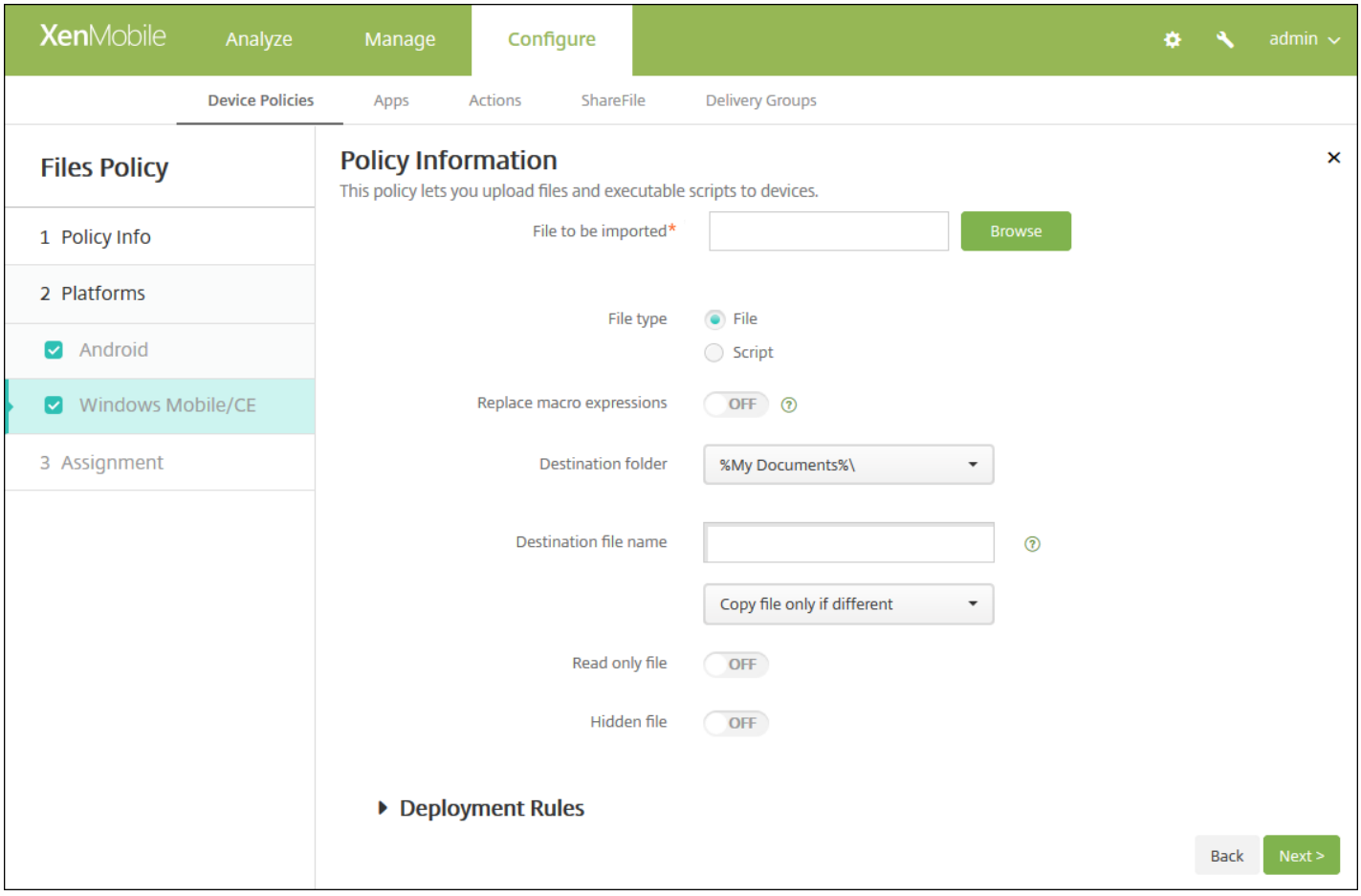
Configure Android settings



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:

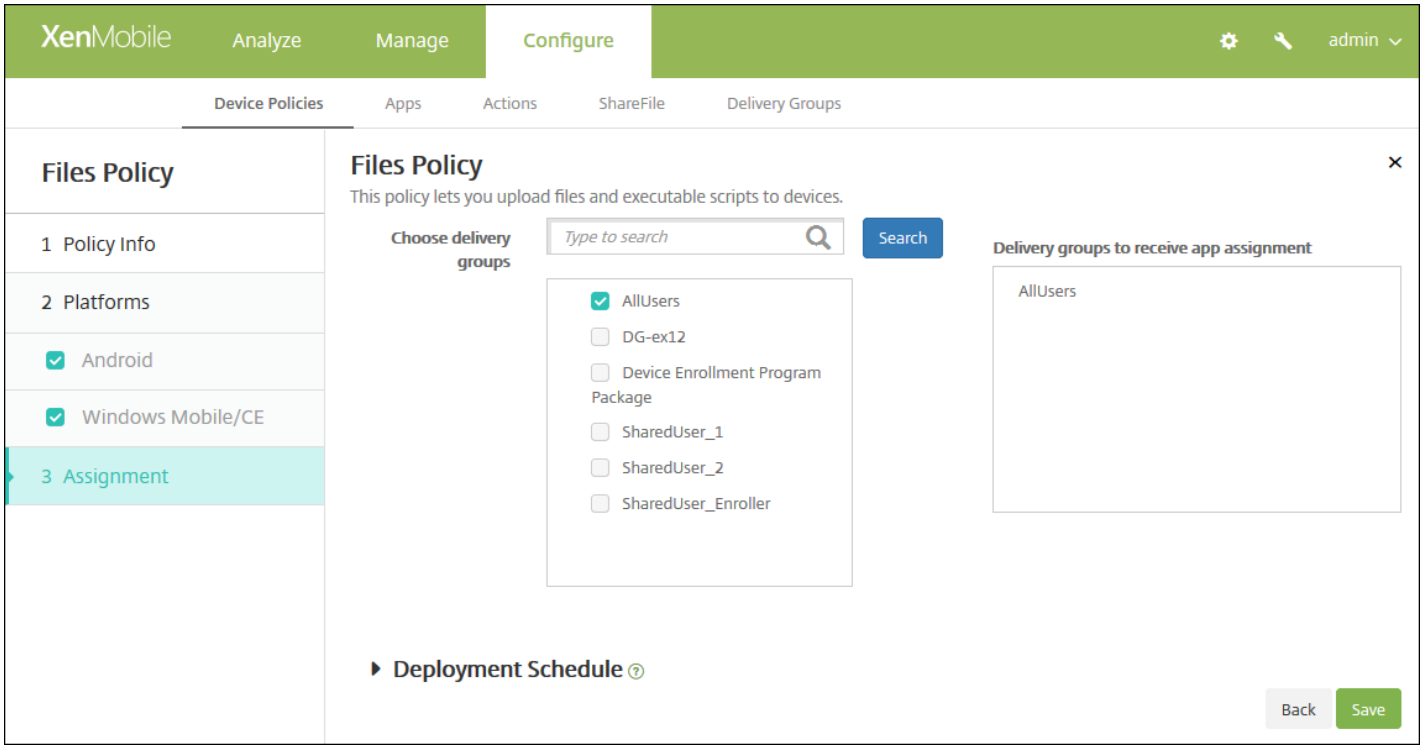
- **File to be imported**: Select the file to import by clicking Browse and navigating to the file's location.
- **File type**: Select either **File** or **Script**. When you select **Script**, **Execute immediately** appears. Select whether the script

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 the deployment rules

8. Click **Next**. The **Files 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** to save the policy.

Font device policy

Nov 15, 2016

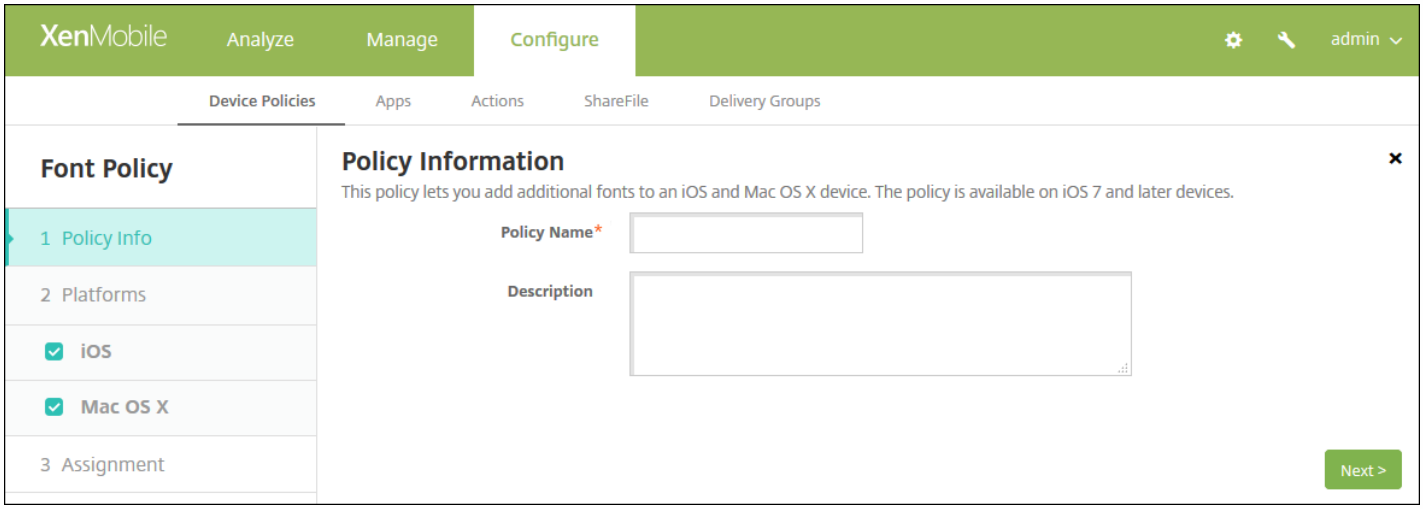
You can add a device policy in XenMobile to add additional fonts to users' iOS and Mac OS X devices. Fonts must be TrueType (.ttf) or OpenType (.oft) fonts. Font collections (.ttc or .otc) are not supported.

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:

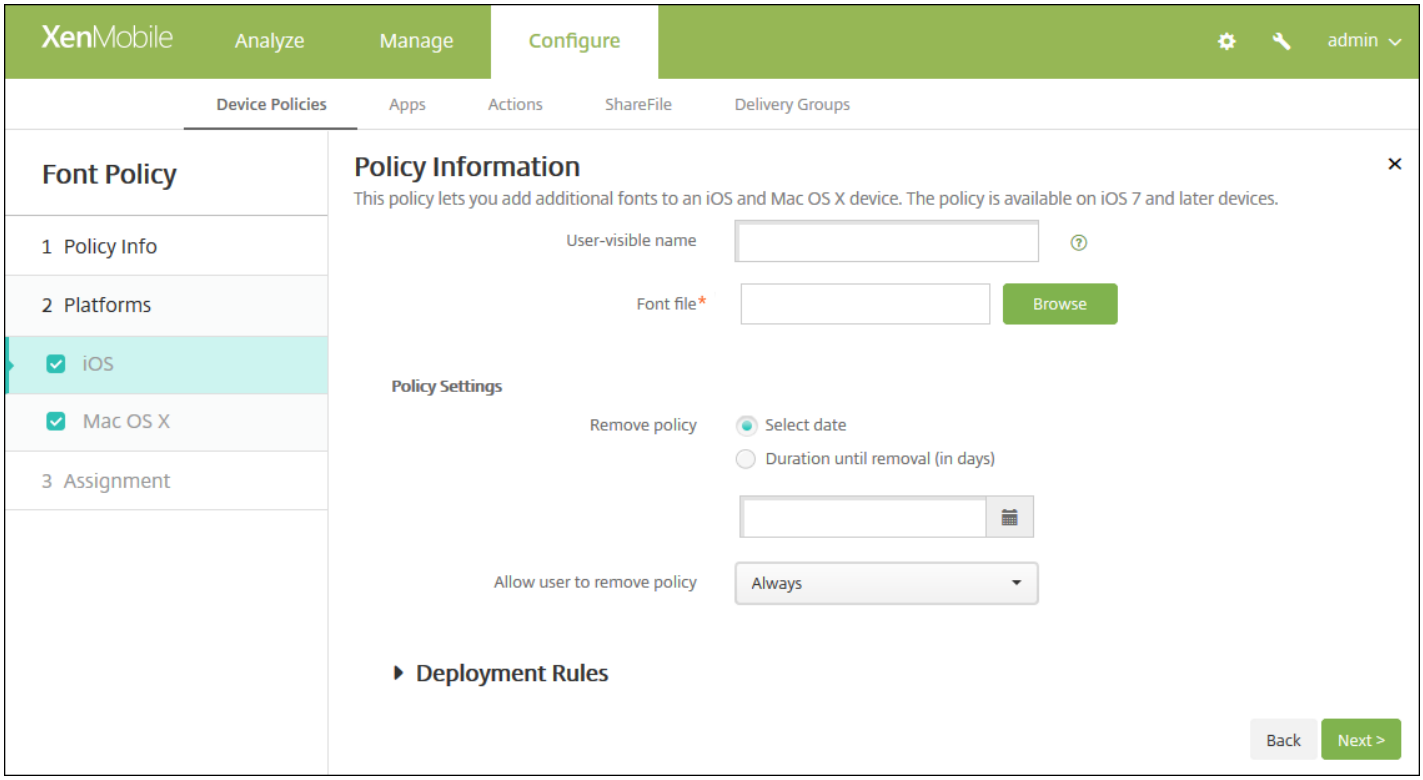
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

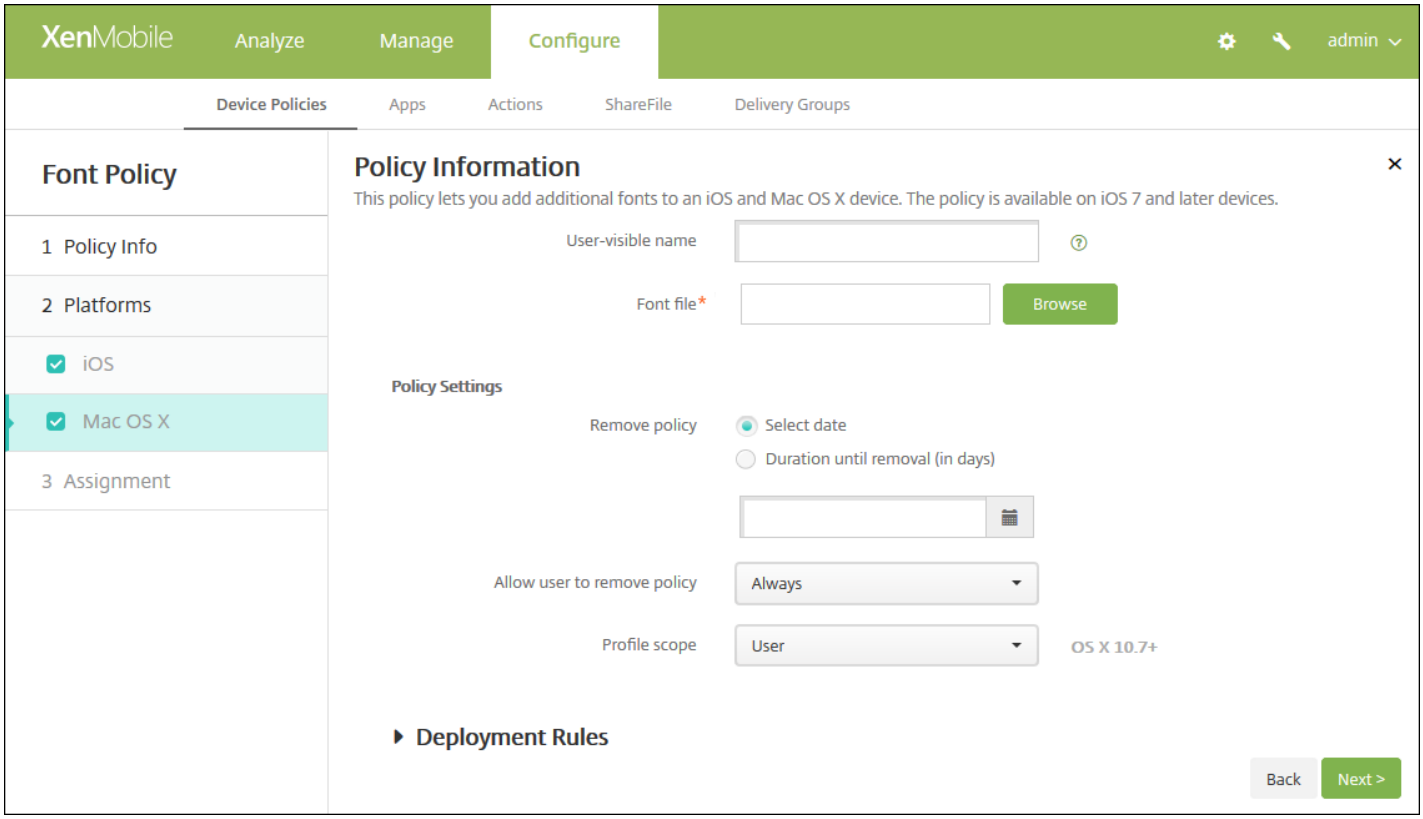
Configure iOS setting



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 days)**.
  - 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 Mac OS X settings

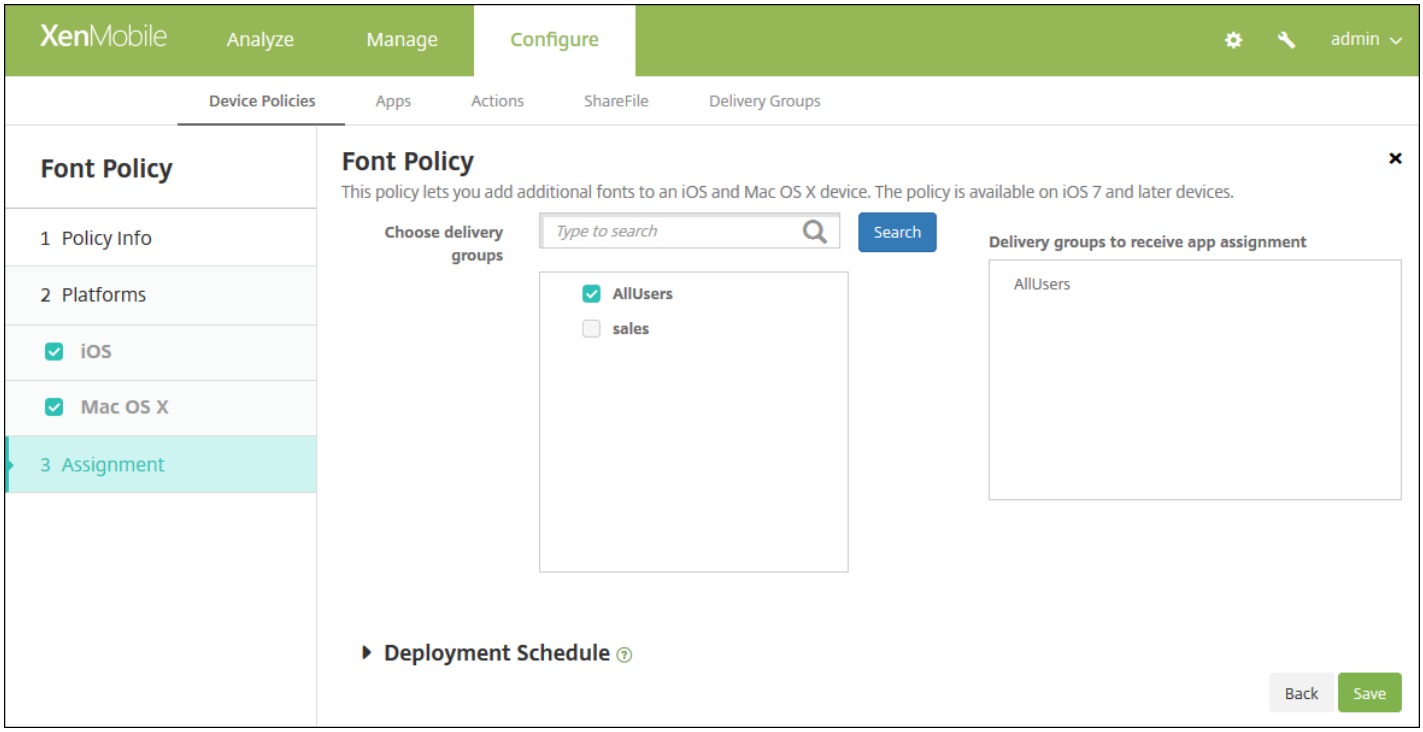


Configure the following settings:

- **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 days)**.
  - 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 OS X 10.7 and later.

7. Configure the deployment rules

8. Click **Next**. The **Font 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**.

Import iOS & Mac OS X Profile device policy

Nov 15, 2016

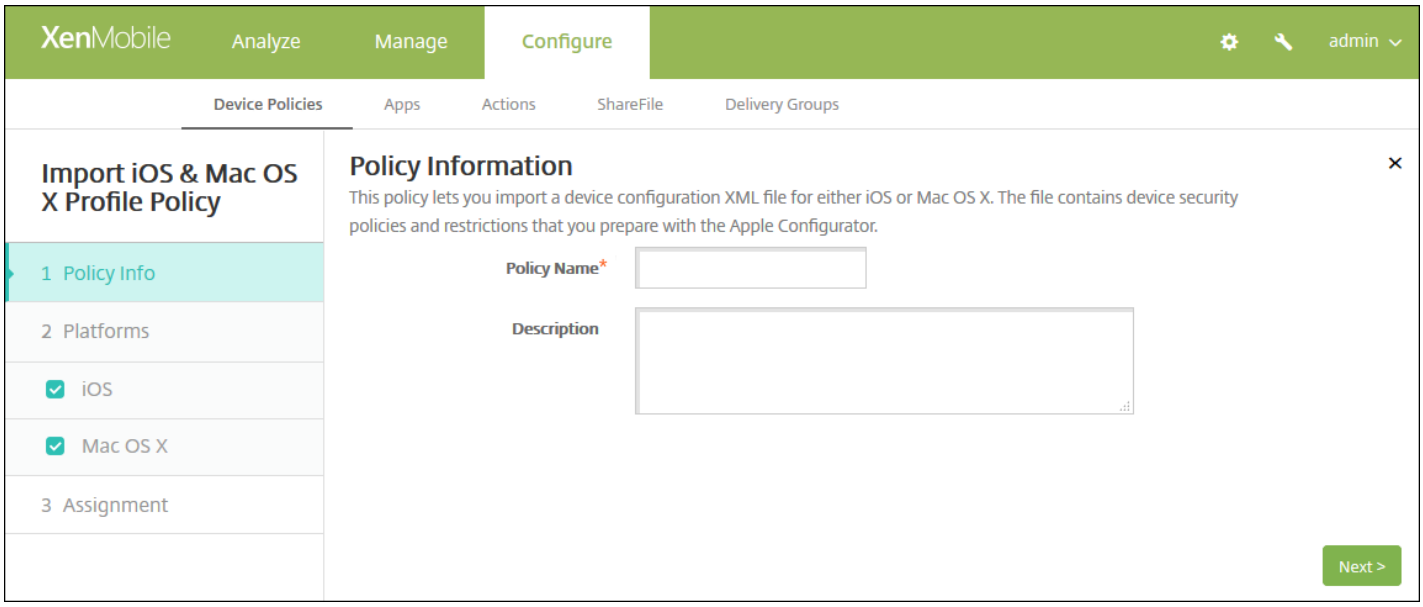
You can import device configuration XML files for iOS and OS X devices into XenMobile. The file contains device security policies and restrictions that you prepare with the Apple Configurator.

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.

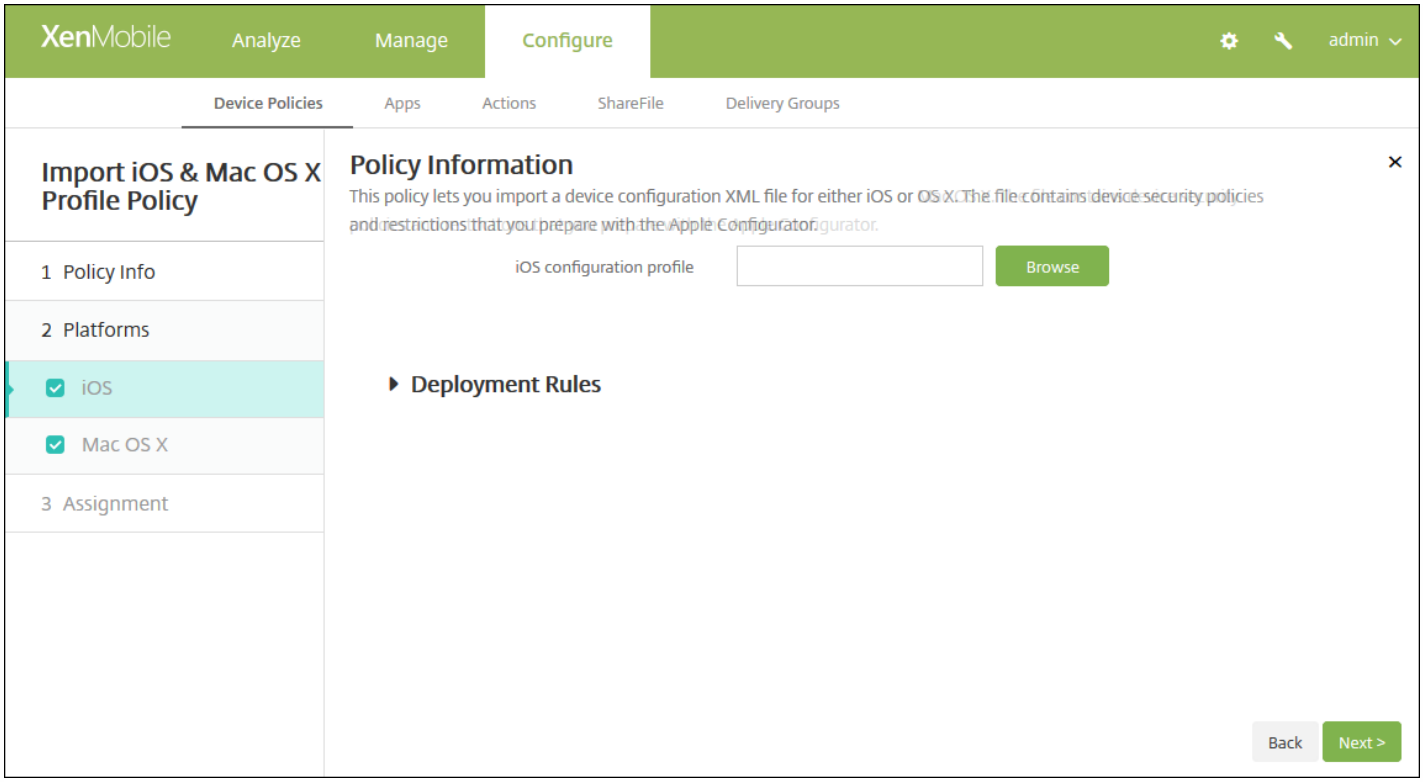
3. Expand **More**, and then under **Custom**, click **Import iOS & Mac OS X Profile**. The **Import iOS & Mac OX X Profile Policy** information page appears.



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.



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

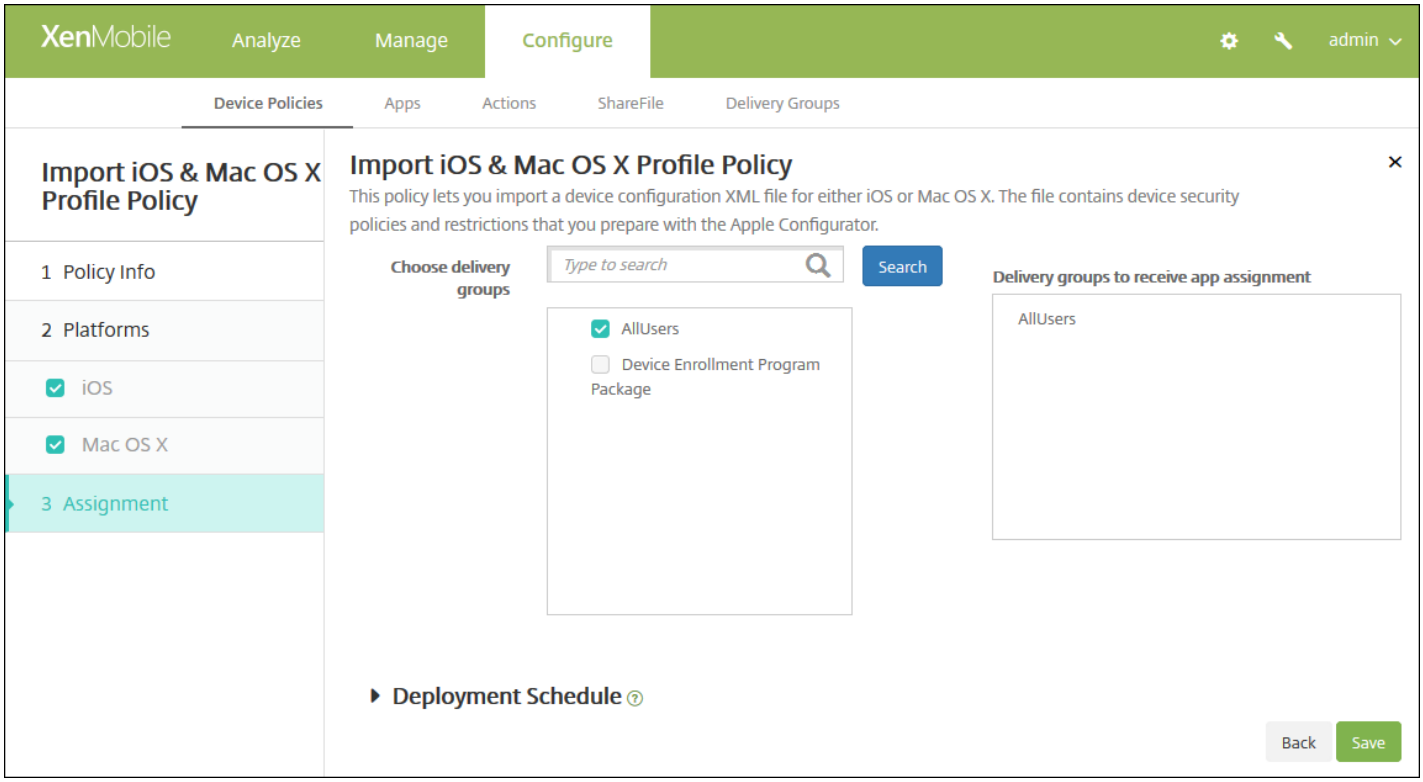
When you finish configuring the settings for a platform, refer to Step 8 for how to set that platform's deployment rules. .

7. Configure this setting for each platform you selected:

- **iOS configuration profile** or **Mac OS X configuration profile**: Select the configuration file to import by clicking **Browse** and navigating to the file's location.

8. Configure the deployment rules

9. Click **Next**. The **Import iOS & Mac OS X Profile 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**. 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.

12. Click **Save** to save the policy.

Place an iOS device in Supervised mode with the Apple Configurator

To use the Apple Configurator, you need an Apple computer running OS X 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

Nov 15, 2016

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.

If you later want to remove the devices from Kiosk mode, create a new Kiosk device policy that has **Kiosk mode** set to **Disable**. Update the delivery group(s) 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

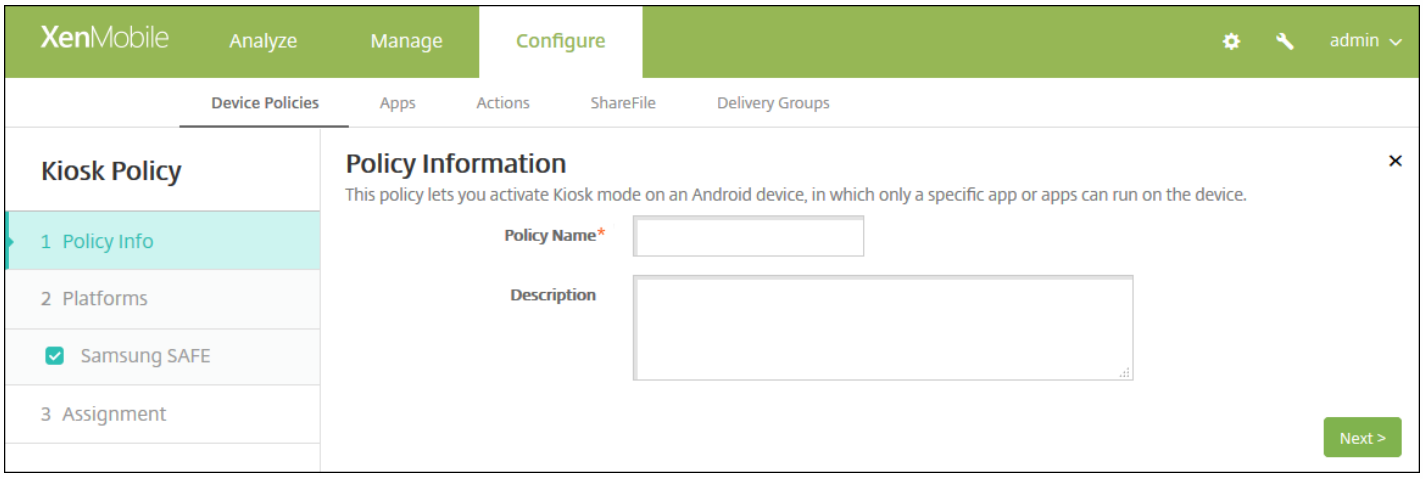
Note:

- All apps that you specify for Kiosk mode must already be installed on the users' 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.

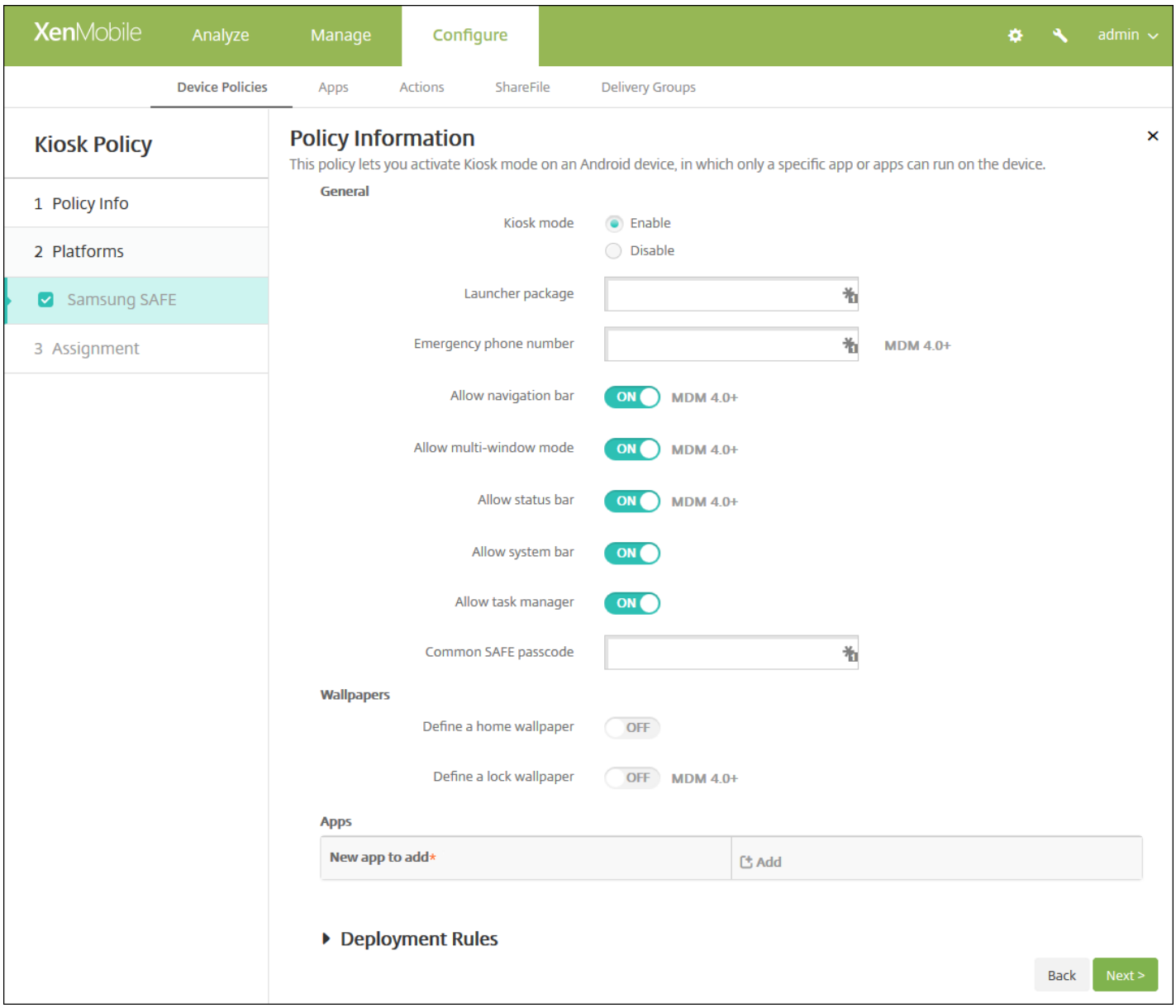
3. Expand **More** and then, under **Security**, click **Kiosk**. The **Kiosk Policy** page appears.



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 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 are using an in-house launcher, enter the full name of the launcher application package.
- **Emergency phone number**: Enter an optional phone number. This number can be used by anyone finding a lost device

to contact your company. Applies only to MDM 4.0 and later.

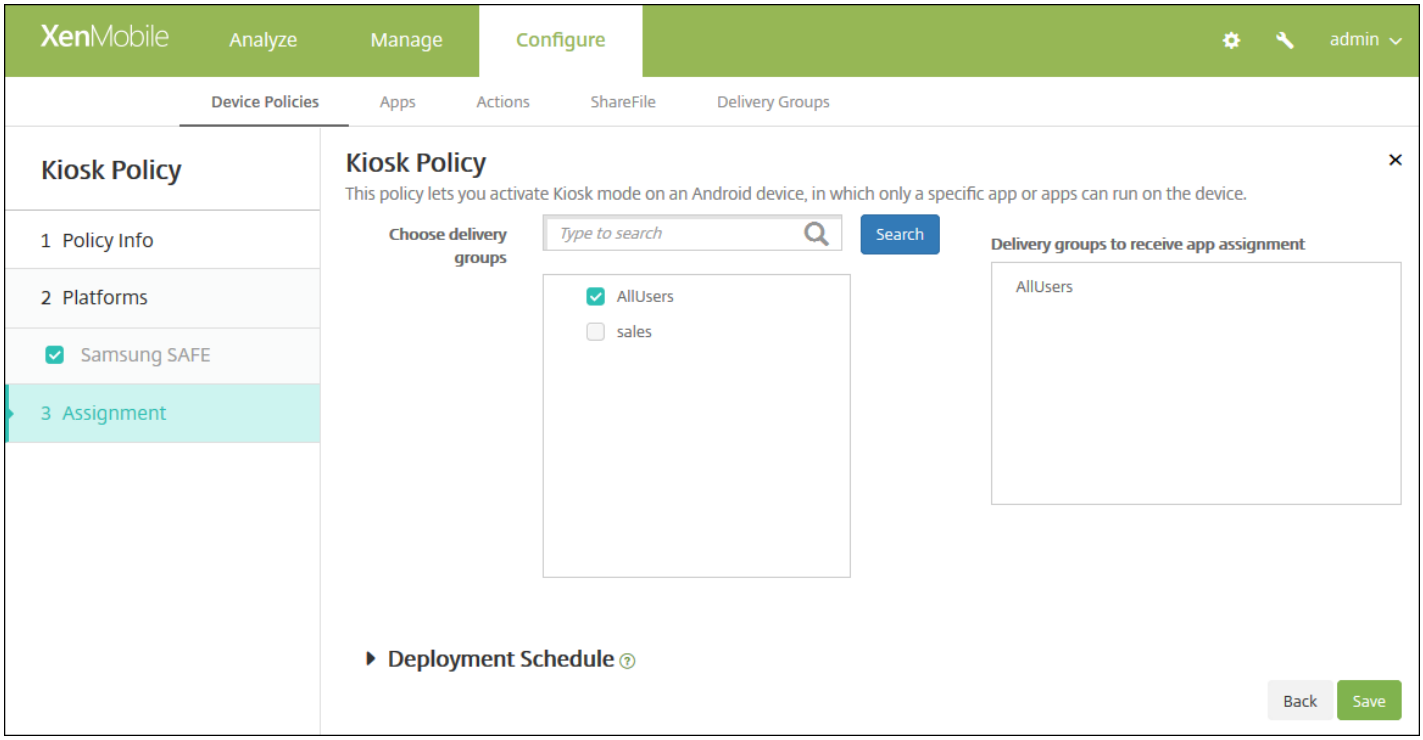
- **Allow navigation bar**: Select whether to let users see and use the navigation bar while in Kiosk mode. Applies only to MDM 4.0 and later. The default is **ON**.
- **Allow multi-window mode**: Select whether to let users use multiple windows while in Kiosk mode. Applies only to MDM 4.0 and later. 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**.
- **Common SAFE passcode**: If you have 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's location.
  - **Define a lock wallpape**r: 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's 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 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 the deployment rules

8. Click **Next**. The **Kiosk 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**.

Launcher configuration device policy for Android

Nov 15, 2016

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.

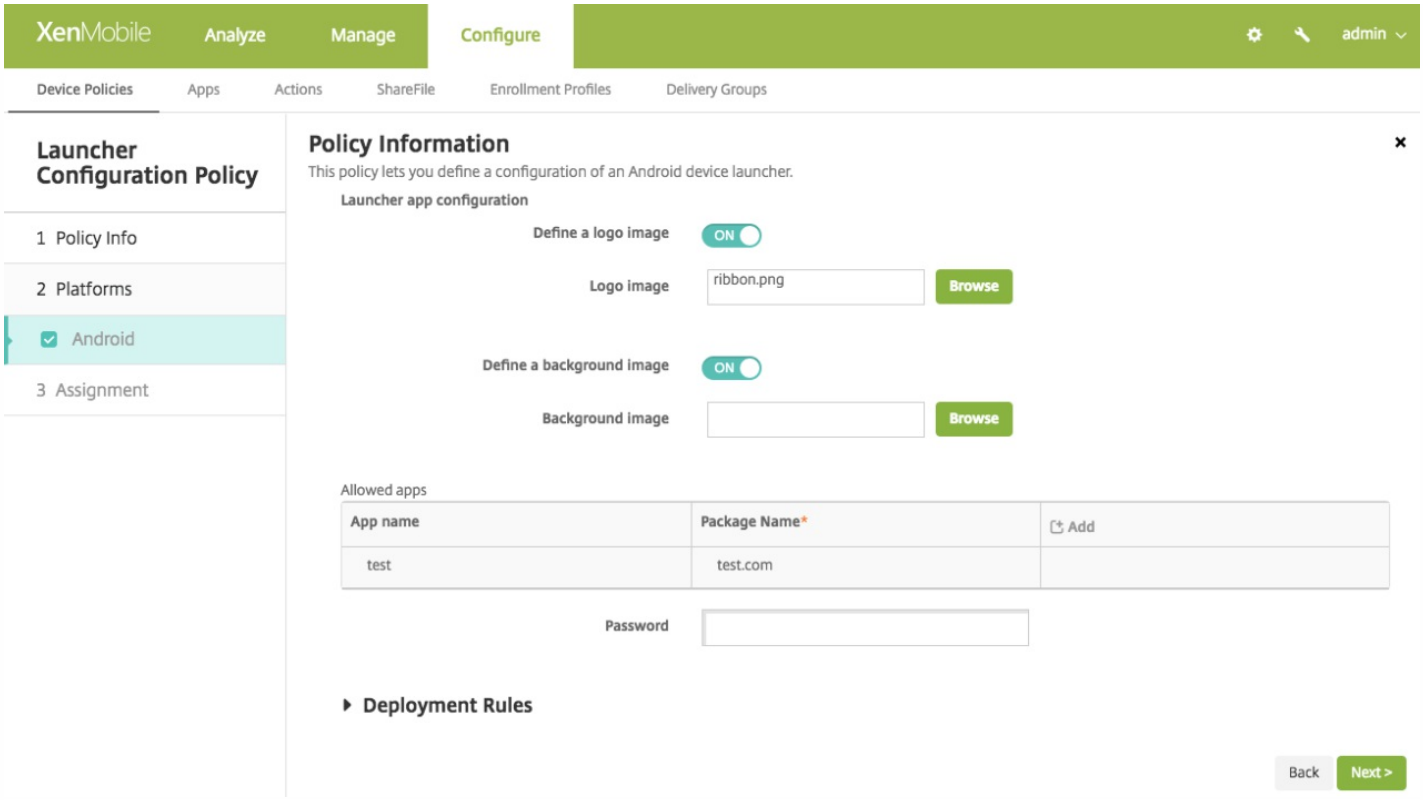
2. Click **Add**. The **Add a New Policy** dialog box appears.

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.



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 the deployment rules

8. Click **Next**. The **Launcher Configuration Policy** assignment page appears.

9. Configure the deployment rules

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**. 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**.

12. Click **Save**.

LDAP device policy

Nov 15, 2016

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.

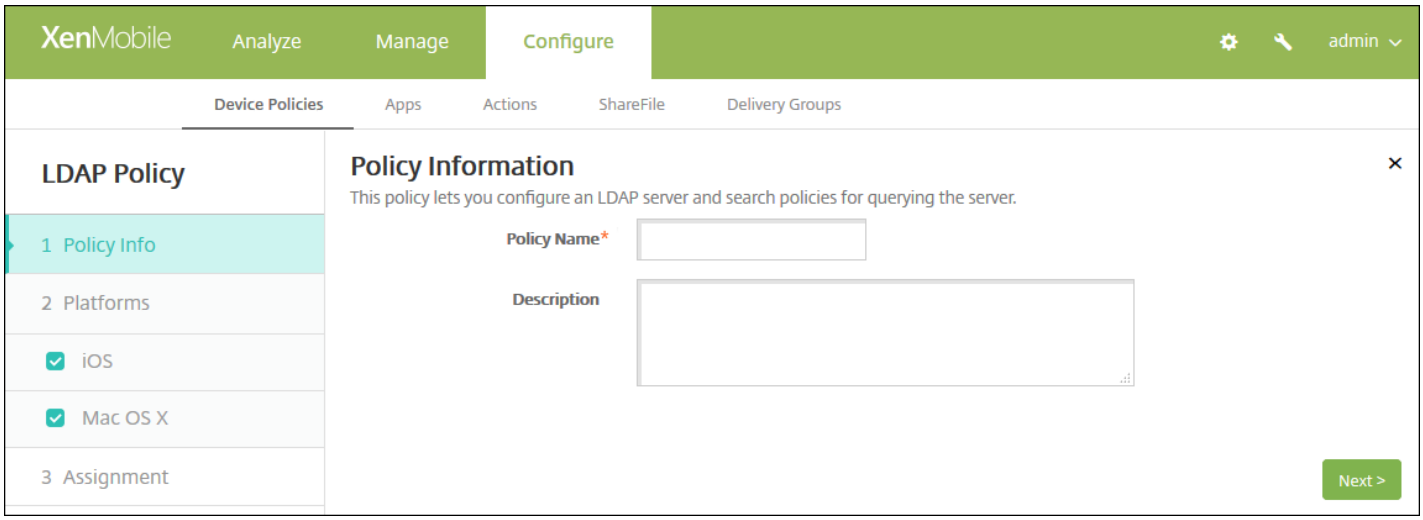
iOS settings

Mac OS X 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. Expand **More** and then, under **End user**, click **LDAP**. The **LDAP Policy** page appears.



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

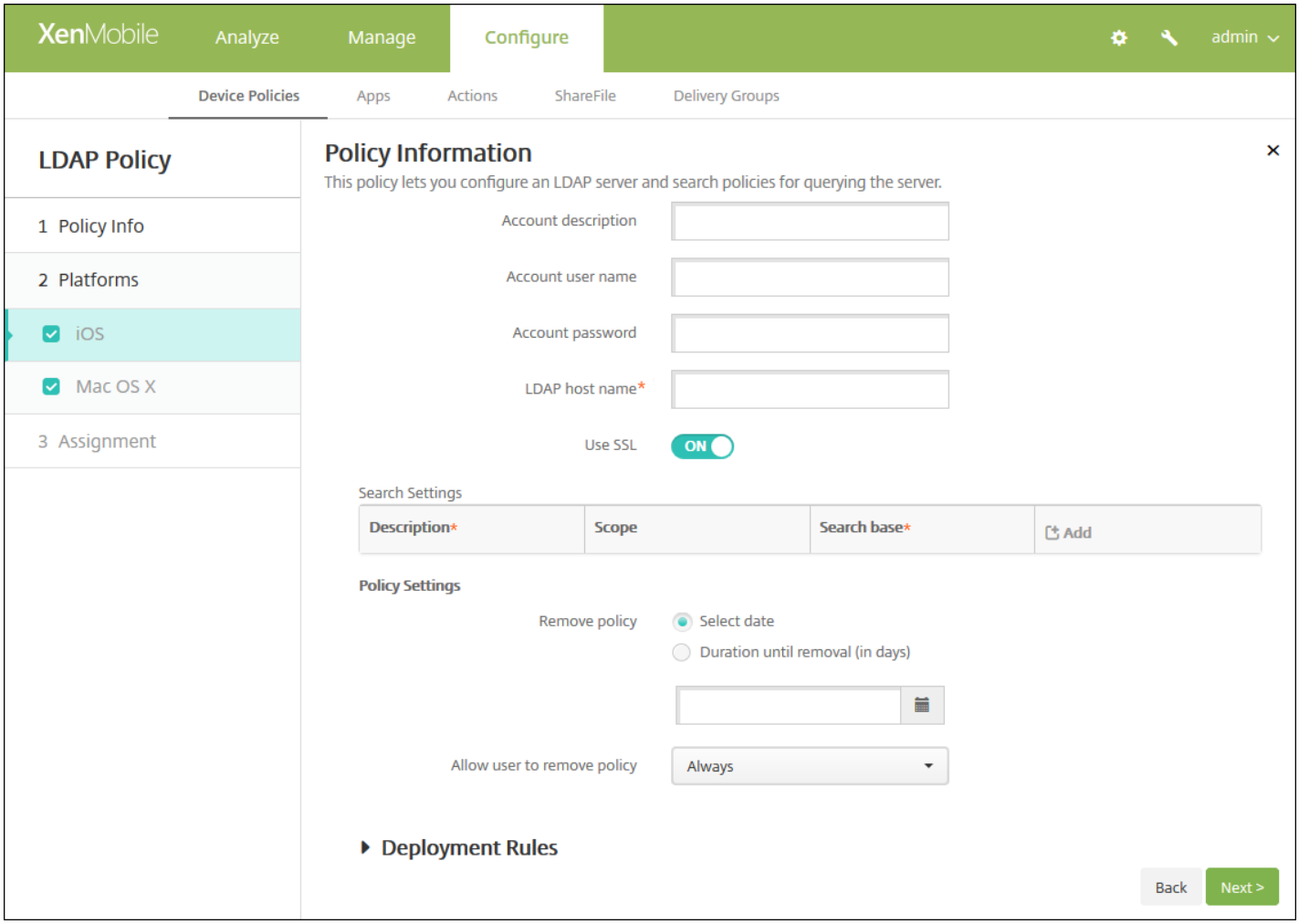
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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 that platform's deployment rules.

Configure iOS settings



Configure the following settings:

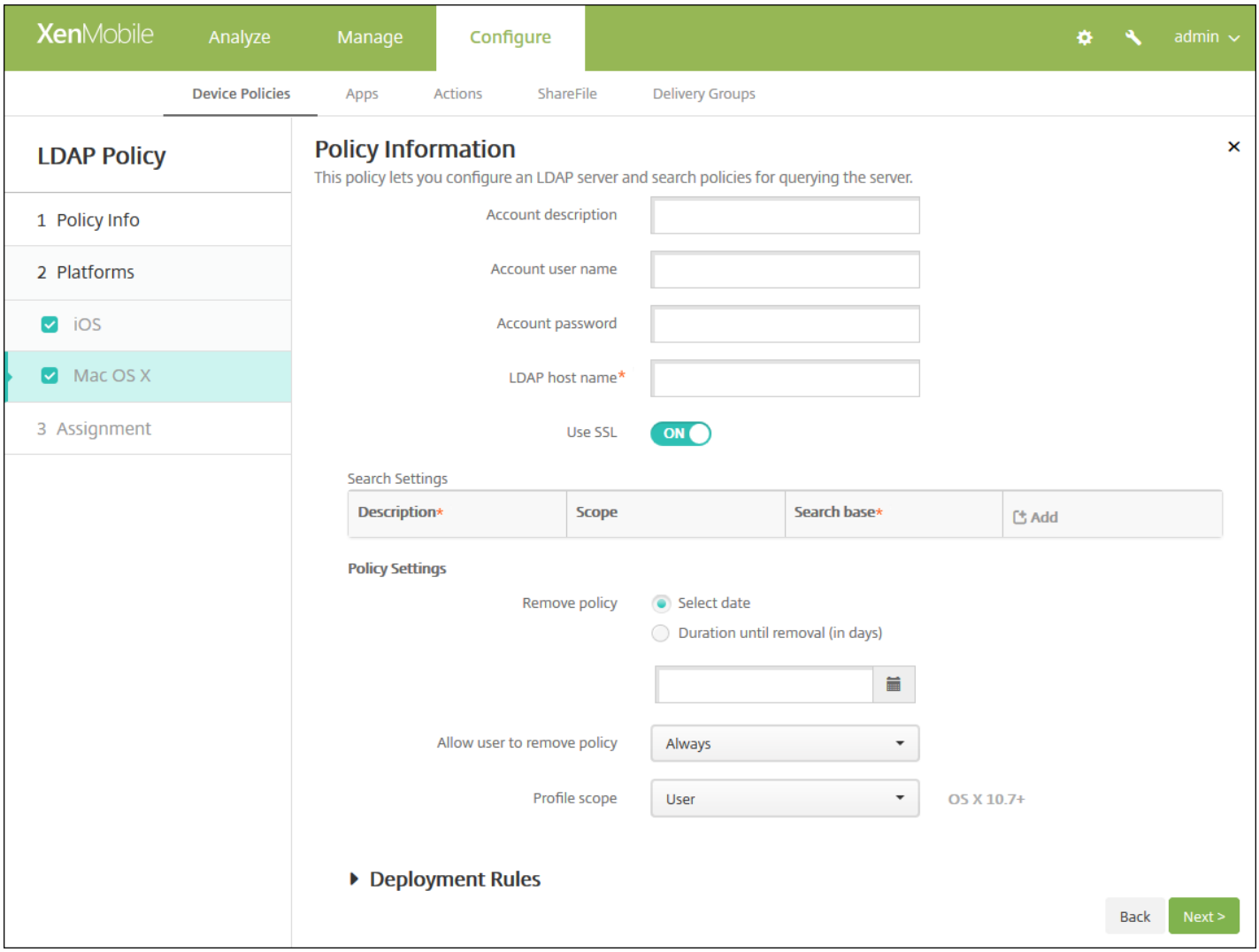
- **Account description**: Enter an optional account description.
- **Account user name**: Enter an optional user name.
- **Account password**: Enter an optional password. Use this only with encrypted profiles.
- **LDAP host name**: Enter the LDAP server host name. This field is required.
- **Use SSL**: 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**: In the list, click **Base**, **One level**, or **Subtree** to define how deeply into the LDAP tree to search. The default is Base.
    - Base searches the node pointed to by Search base.
    - One level searches the Base node and one level below it.
    - Subtree searches the Base node, plus all of 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 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 search setting, 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.

- Under **Policy Settings**, next to **Remove policy**, click either **Select date** or **Duration until removal (in days)**.
- 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 Mac OS X 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 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**: In the list, click **Base**, **One level**, or **Subtree** to define how deeply into the LDAP tree to search. The default is Base.
    - Base searches the node pointed to by Search base.
    - One level searches the Base node and one level below it.
    - Subtree searches the Base node, plus all of 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.

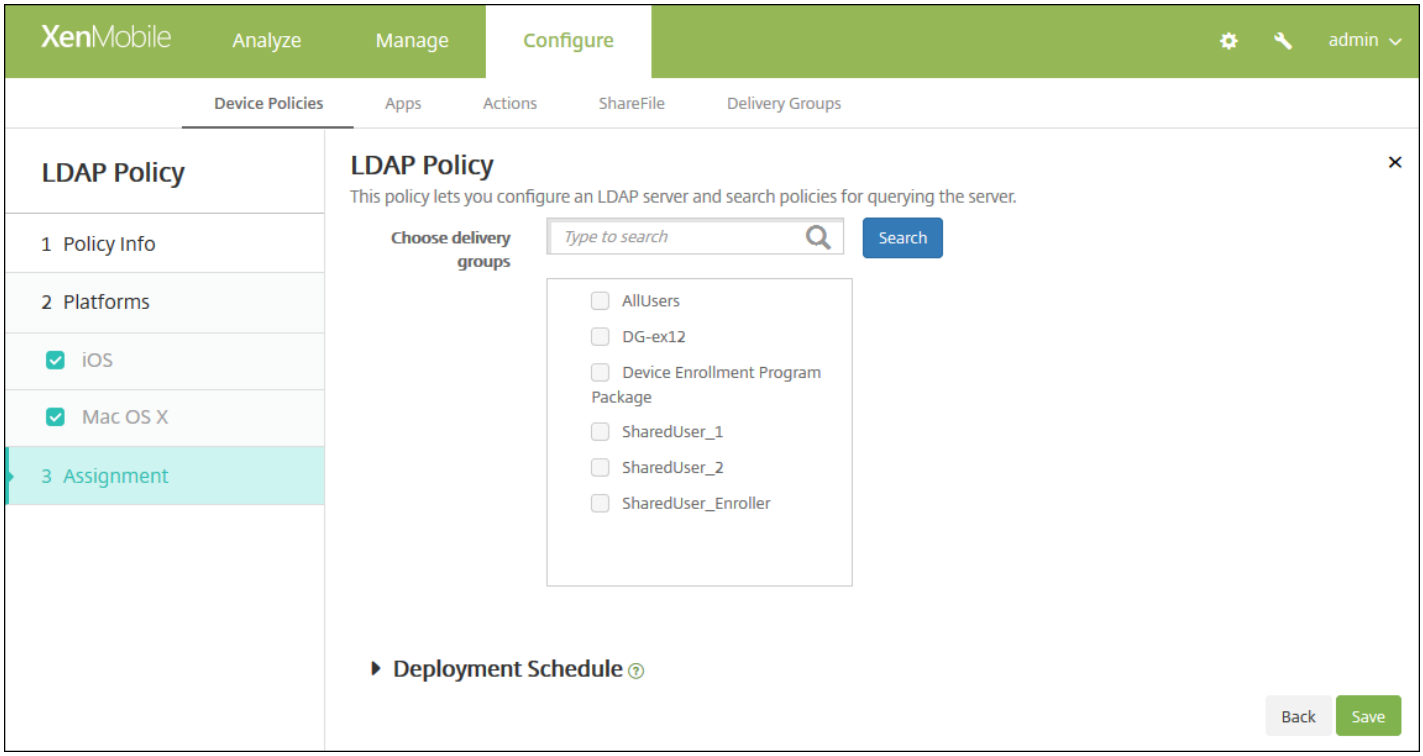
    Note: To delete an existing search setting, hover over the line containing the listing and click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing.

    To edit an existing search setting, 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.

- Under **Policy Settings**, next to **Remove policy**, click either **Select date** or **Duration until removal (in days)**.
- 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 OS X 10.7 and later.

7. Configure the deployment rules

8. Click **Next**. The **LDAP 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** to save the policy.

Location device policy

Nov 15, 2016

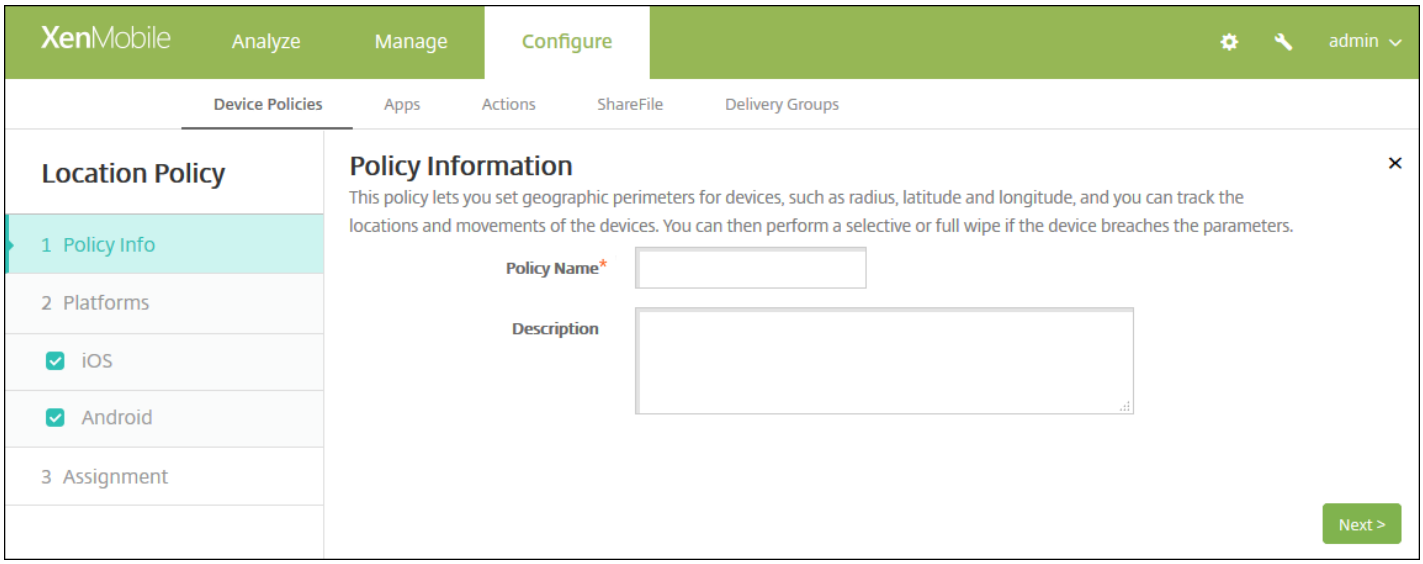
You create location device policies in XenMobile to enforce geographic boundaries, as well as to track the location and movement of users' devices. When users breach the defined boundary, also called a *geofence*, XenMobile can perform a selective or full wipe immediately or after a specific time period to let users return to the allowed location.

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:

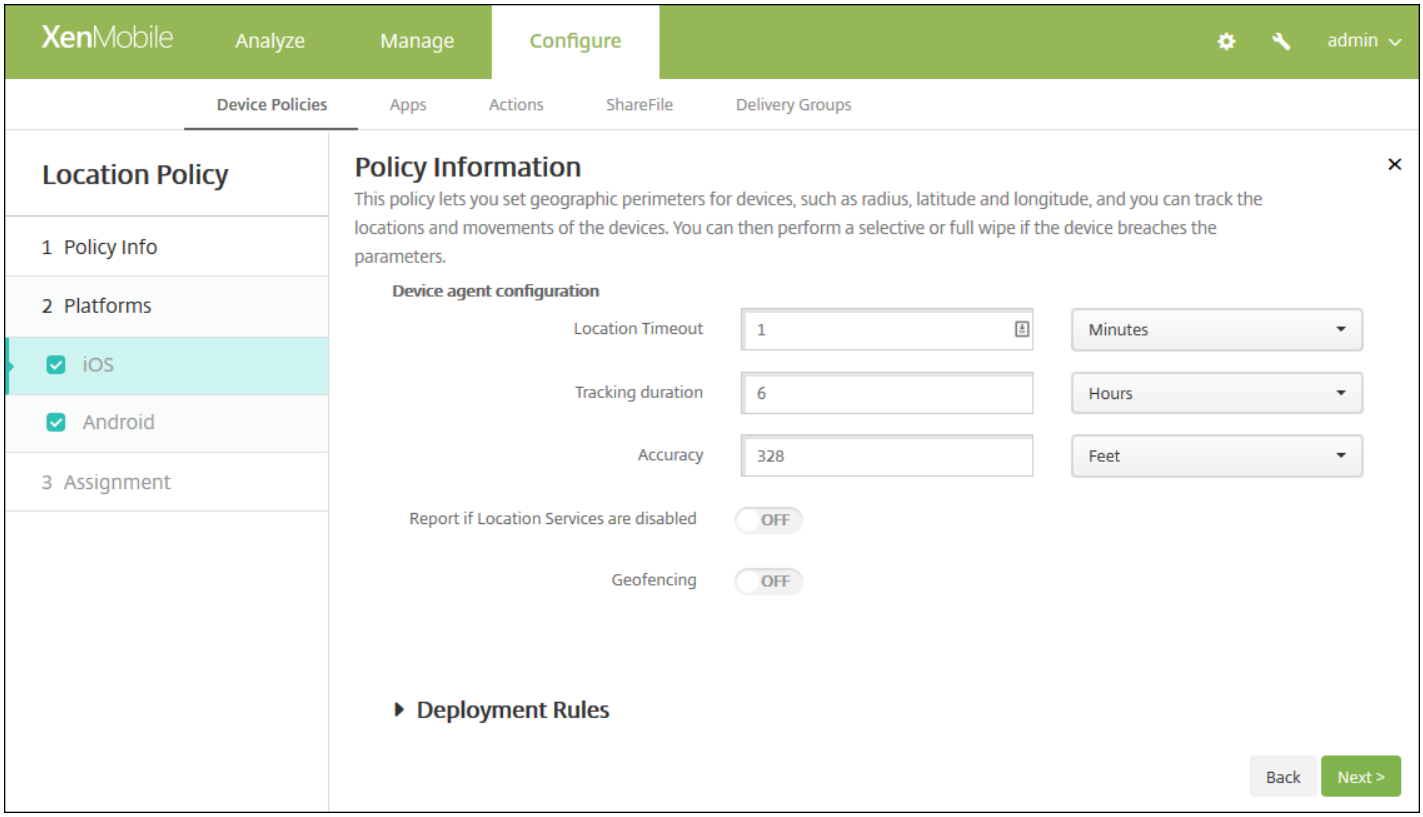
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

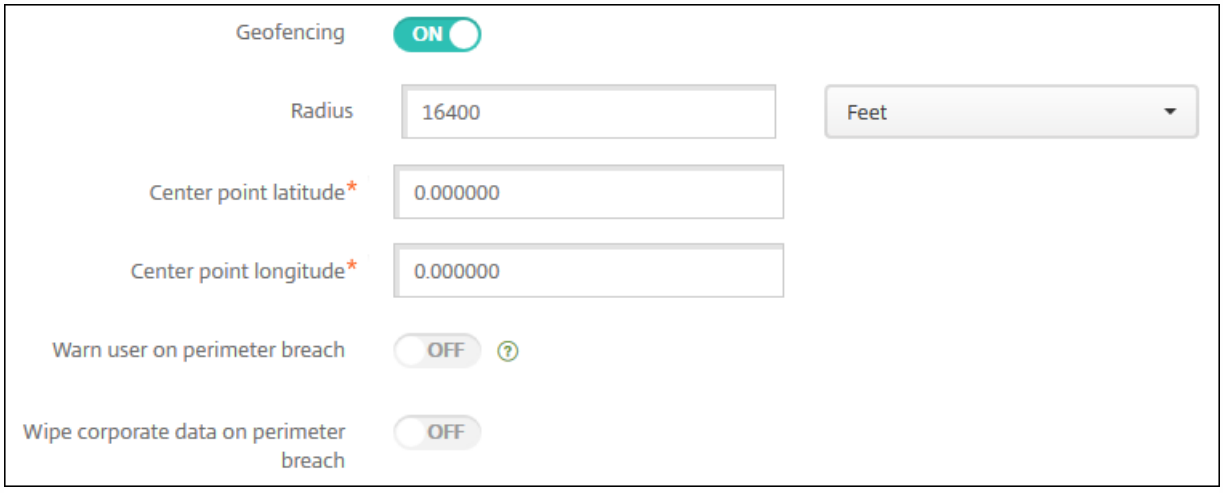
When you finish configuring the settings for a platform, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS settings



Configure these settings:

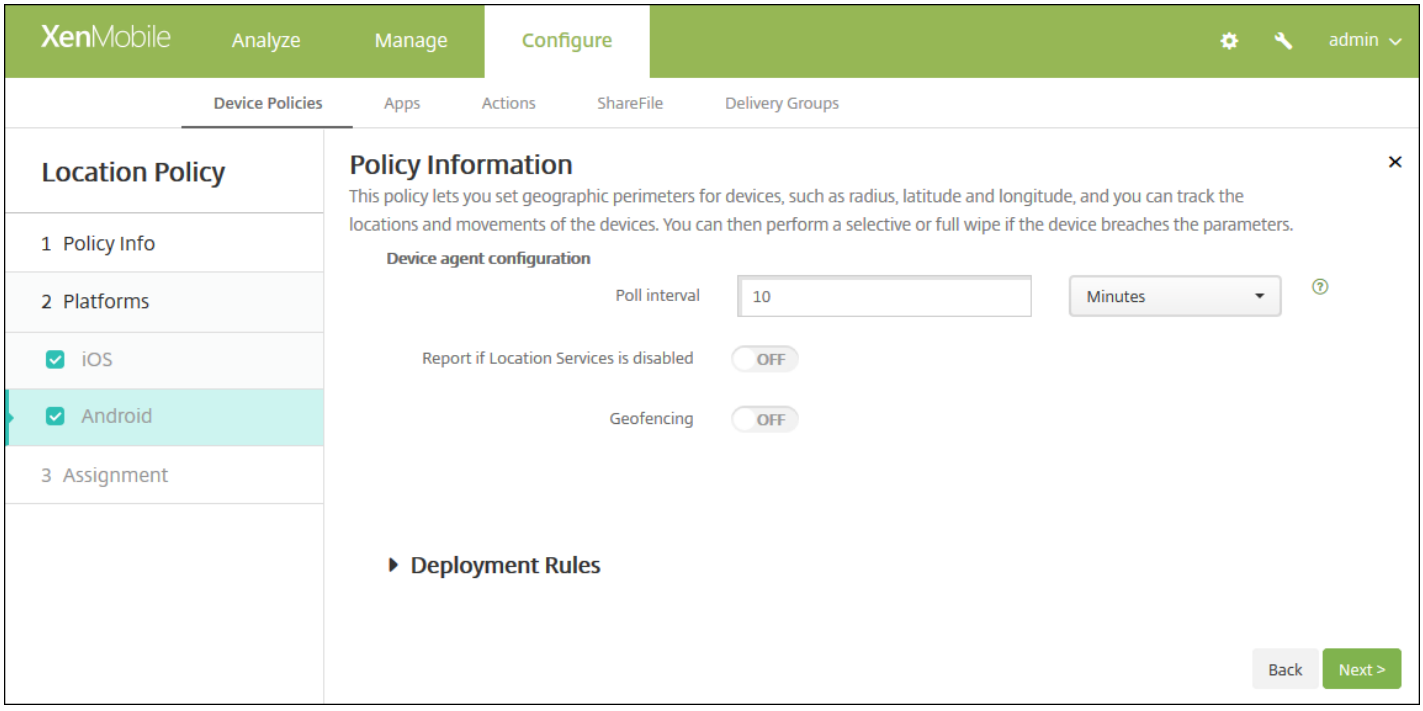
- **Location timeout**: Type a numeral and then, in the list, click **Seconds** or **Minutes** to set how often XenMobile attempts to fix the device's location. Valid values are 60-900 seconds or 1-15 minutes. The default is 1 minute.
- **Tracking duration**: Type a numeral and then, in the list, click **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**



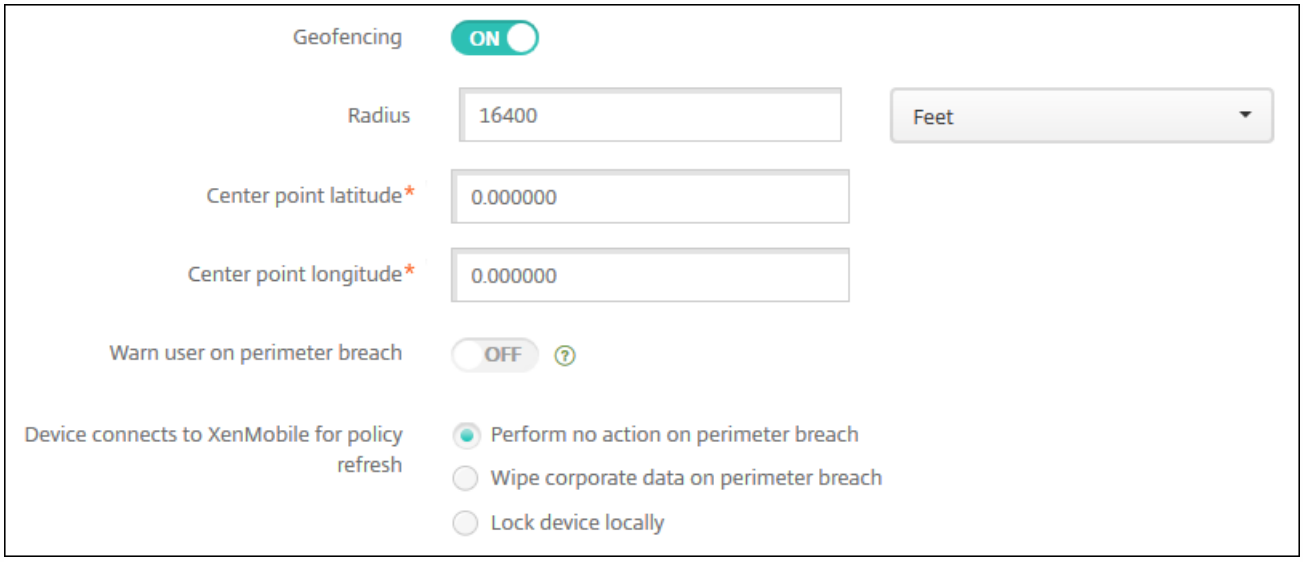
When you enable Geofencing, configure these settings:

- **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



- **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**

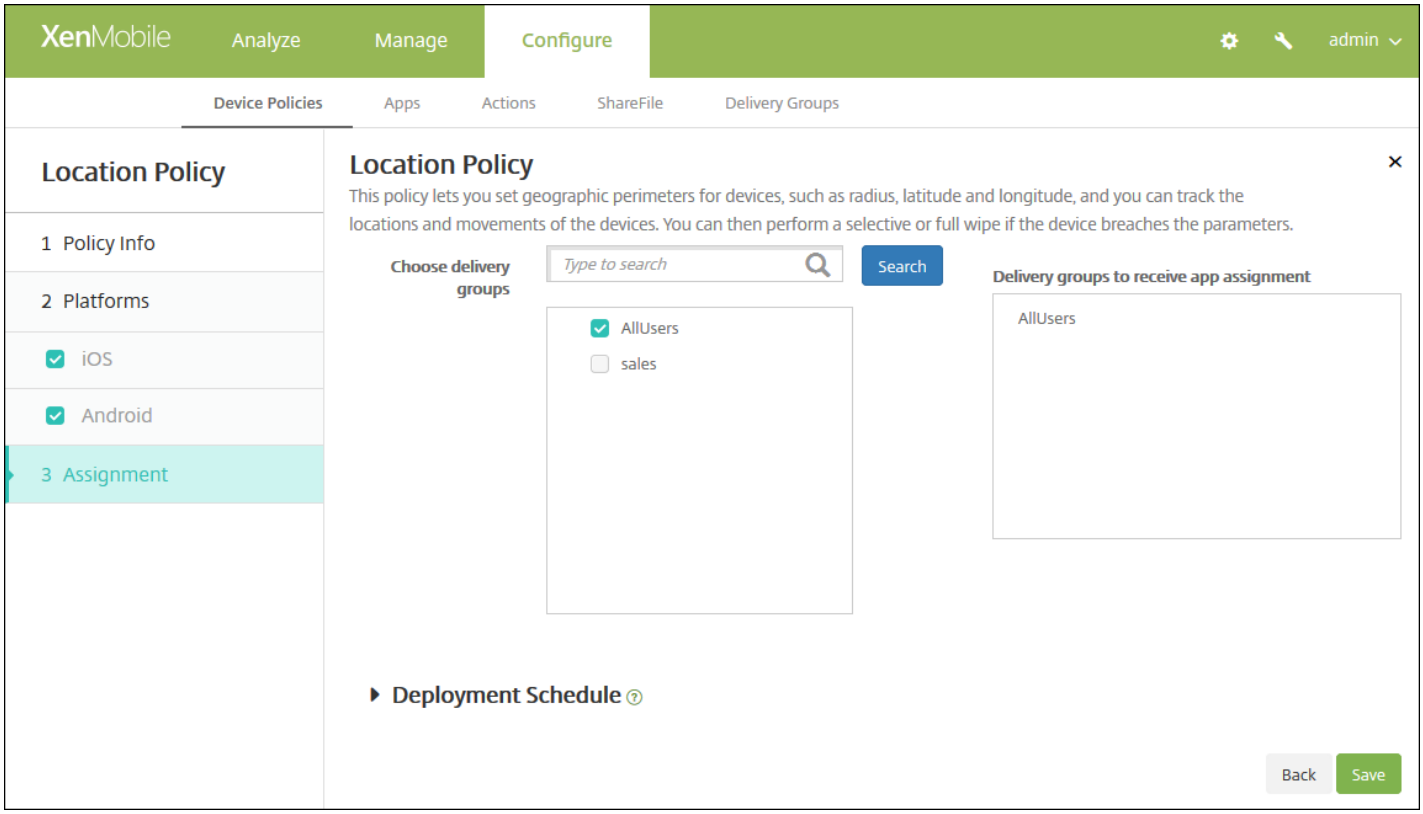


When you enable Geofencing, configure these settings:

- **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 the deployment rules

8. Click **Next**. The **Location 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**.

Mail device policy

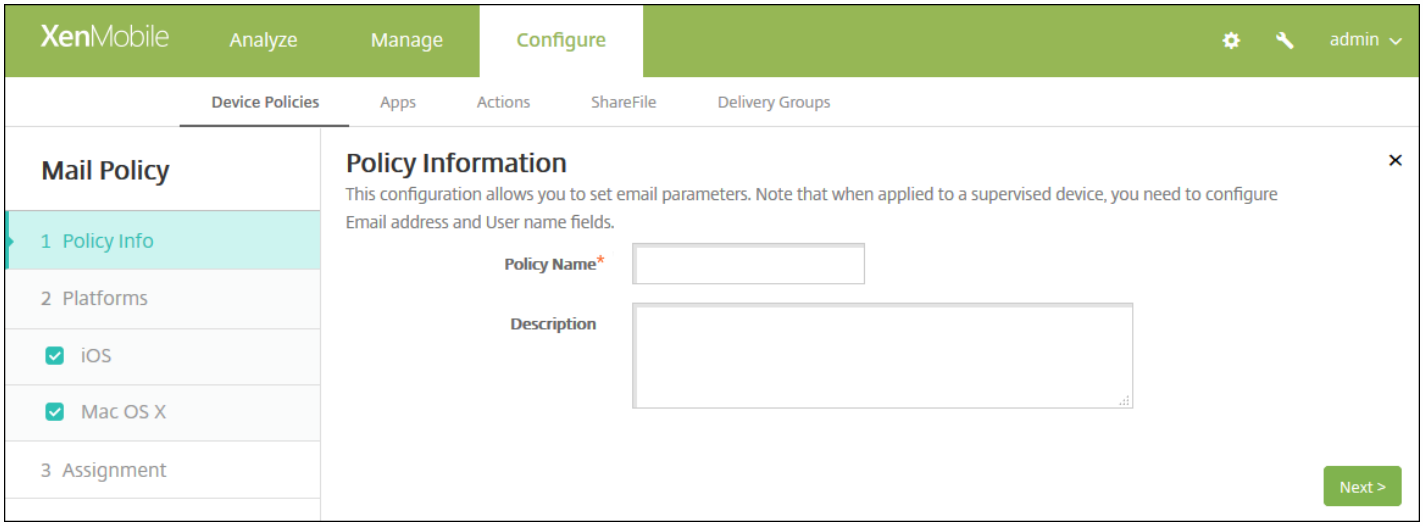
Nov 16, 2016

You can add a mail device policy in XenMobile to configure an email account on users' iOS or Mac OX X devices.

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.

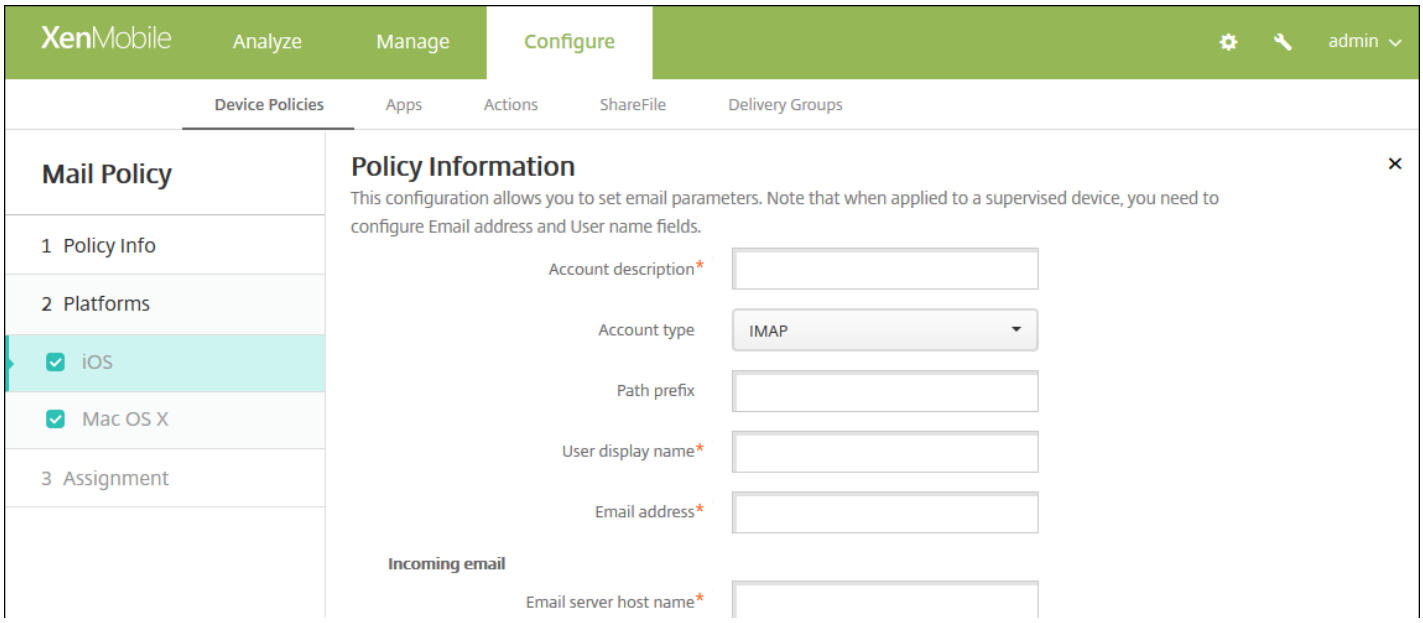
3. Click **More** and then, under **End user**, click **Mail**. The **Mail Policy** page appears.

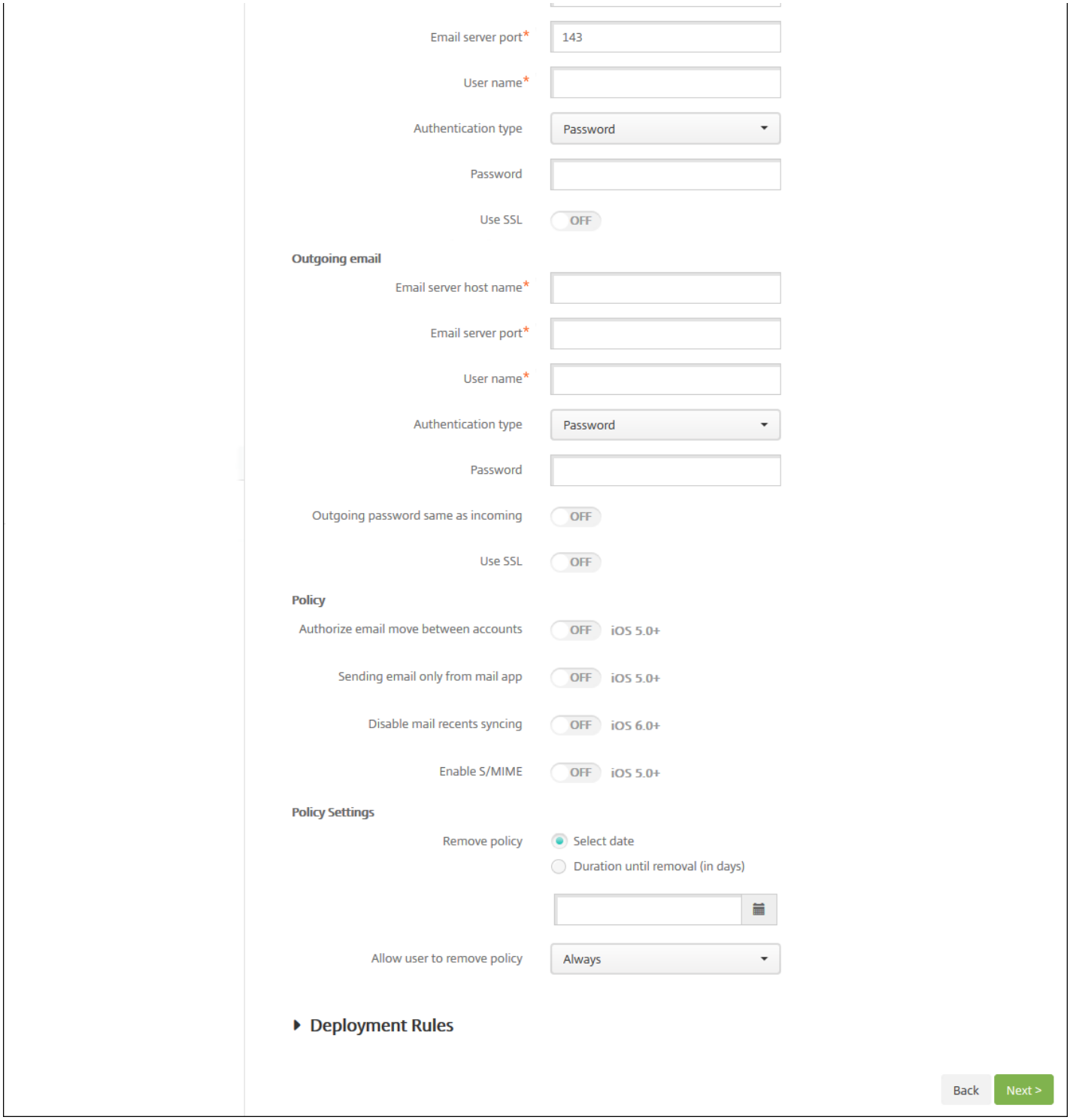


4. In the **Policy Information** pane, enter the following information:

- **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 others.

When you finish configuring the settings for a platform, refer to Step 8 for how to set that platform's deployment rules.

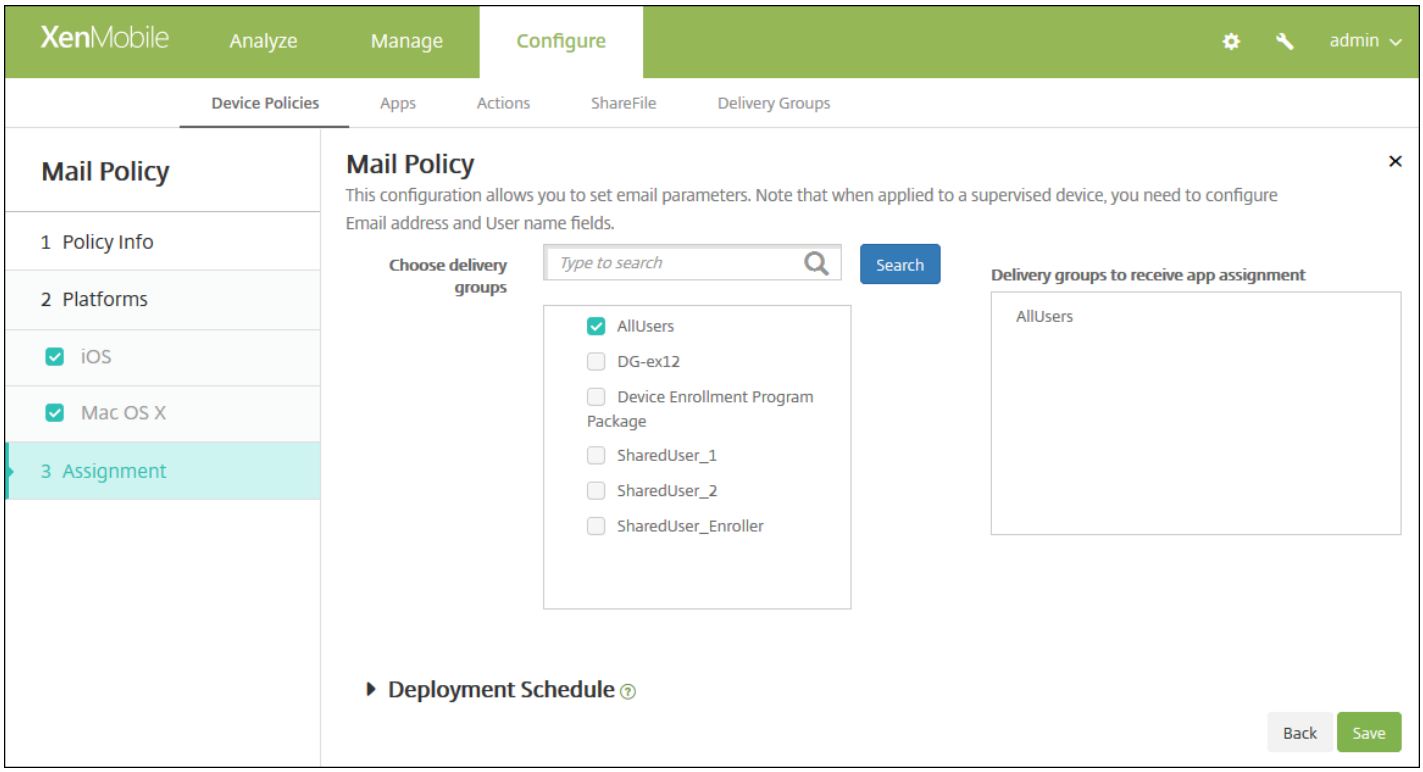
7. Configure the following settings for the platforms you selected.

- **Account description**: Type an account description that appears in the Mail and Settings apps. This field is required.
- **Account type**: In the list, click 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 if it is not **INBOX**. This field is required.
- **User display name**: Type the full user name to be used for messages and so on. 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 user's email address up to the @ character. This field is required.
  - **Authentication type**: In the list, click to select 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 is generally the same as the user's email address up to the @ character. This field is required.
  - **Authentication type**: In the list, click to select 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 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. When set to **ON**, the preceding **Password** field disappears.
  - **Use SSL**: Select whether the outgoing mail server uses Secure Socket Layer authentication. The default is **OFF**.
- **Policy**
  - **Note**: When you are configuring iOS settings, these options apply only to iOS 5.0 and later; there are no restrictions when you are configuring Mac OS X.
  - **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.
  - **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**: In the list, select the signing credential to be used.
  - **Encryption identity credential**: In the list, select the encryption credential to be used.
- **Policy Settings**
  - Next to **Remove policy**, click either **Select date** or **Duration until removal (in days)**.
  - 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**: In the list, click either **User** or **System**. The default is **User**. This option is available only on Mac OS X 10.7 and later.

8. Configure the deployment rules

9. Click **Next**. The **Mail 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 right-hand **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**. 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.

12. Click **Save** to save the policy.

Managed domains device policy

Nov 16, 2016

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. You specify URLs or subdomains to control how users can open documents, attachments, and downloads from the browser. This policy is supported only on iOS 8 and later 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.

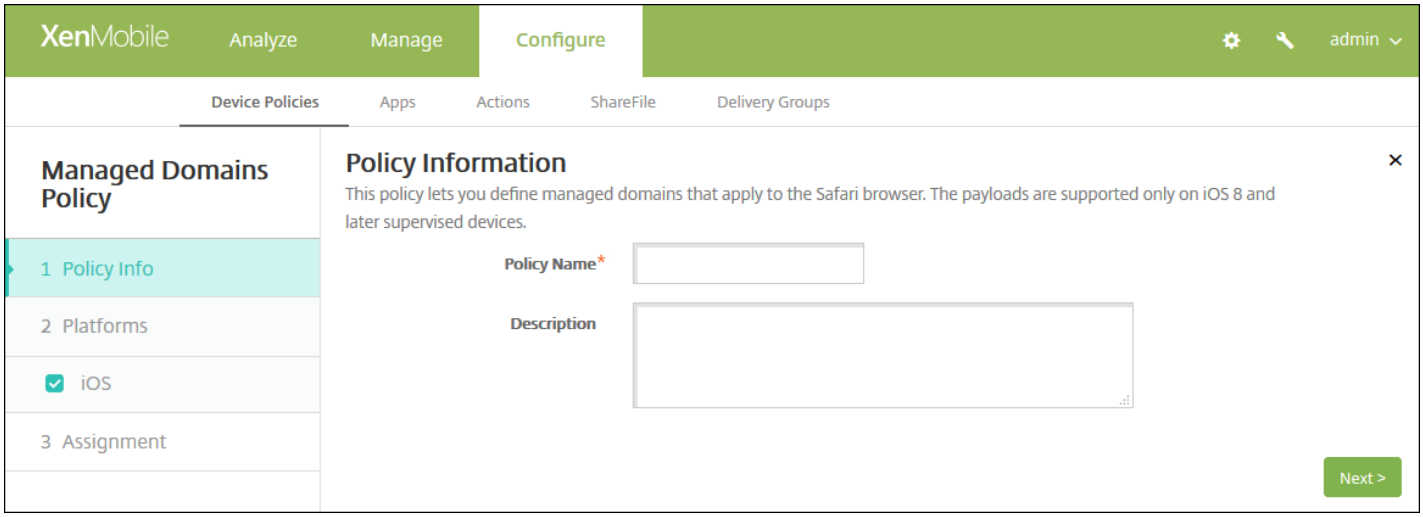
When a user sends email to a recipient whose domain is not on the managed email domains list, the message is flagged on the user's device to warn them that they are sending a message to someone outside your corporate domain.

When a user attempts to open an item (document, attachment, or download) 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.

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

2. Click **Add**. The **Add New Policy** dialog box appears.

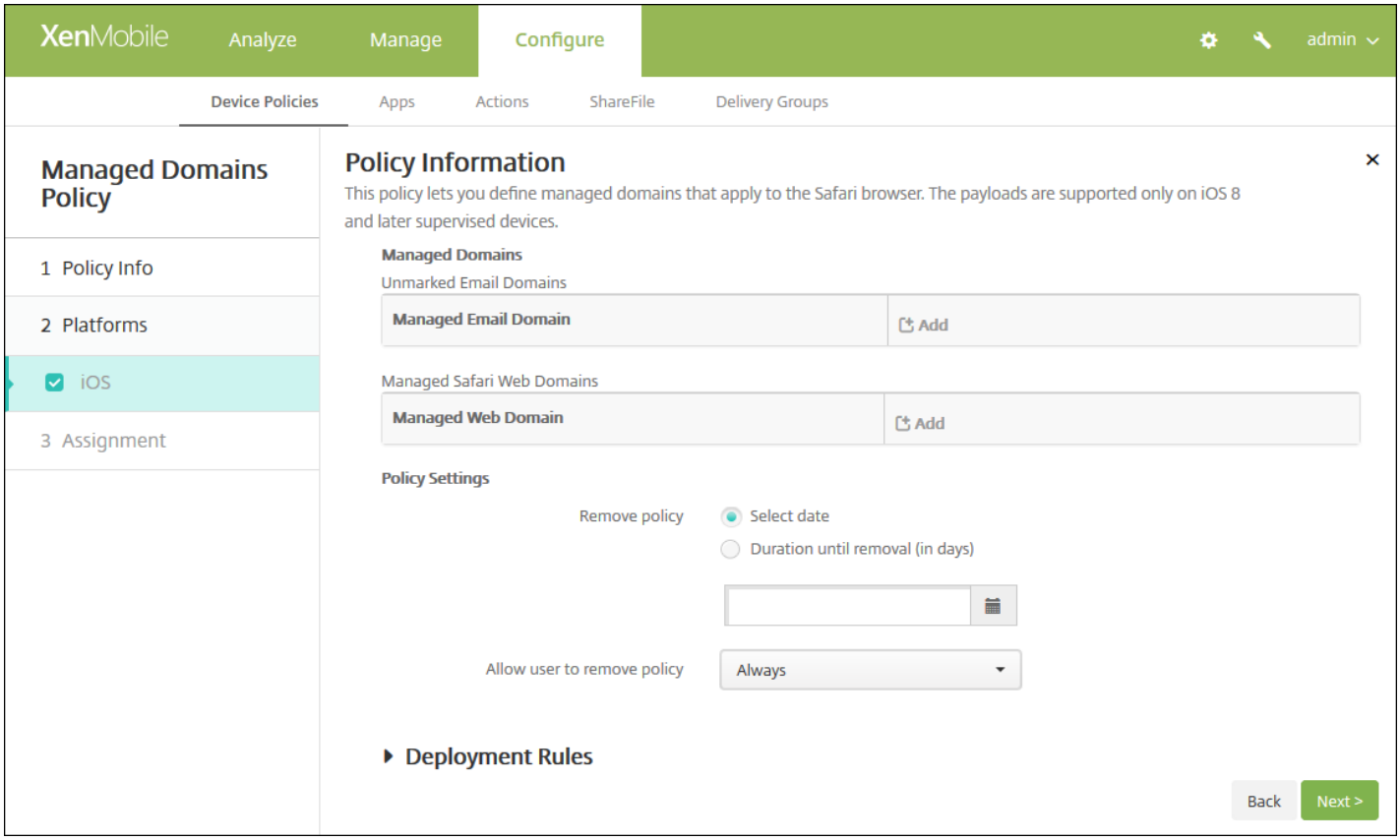
3. Expand **More** and then, under **Security**, click **Managed domains**. The **Managed Domains Policy** information page appears.



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.

      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.

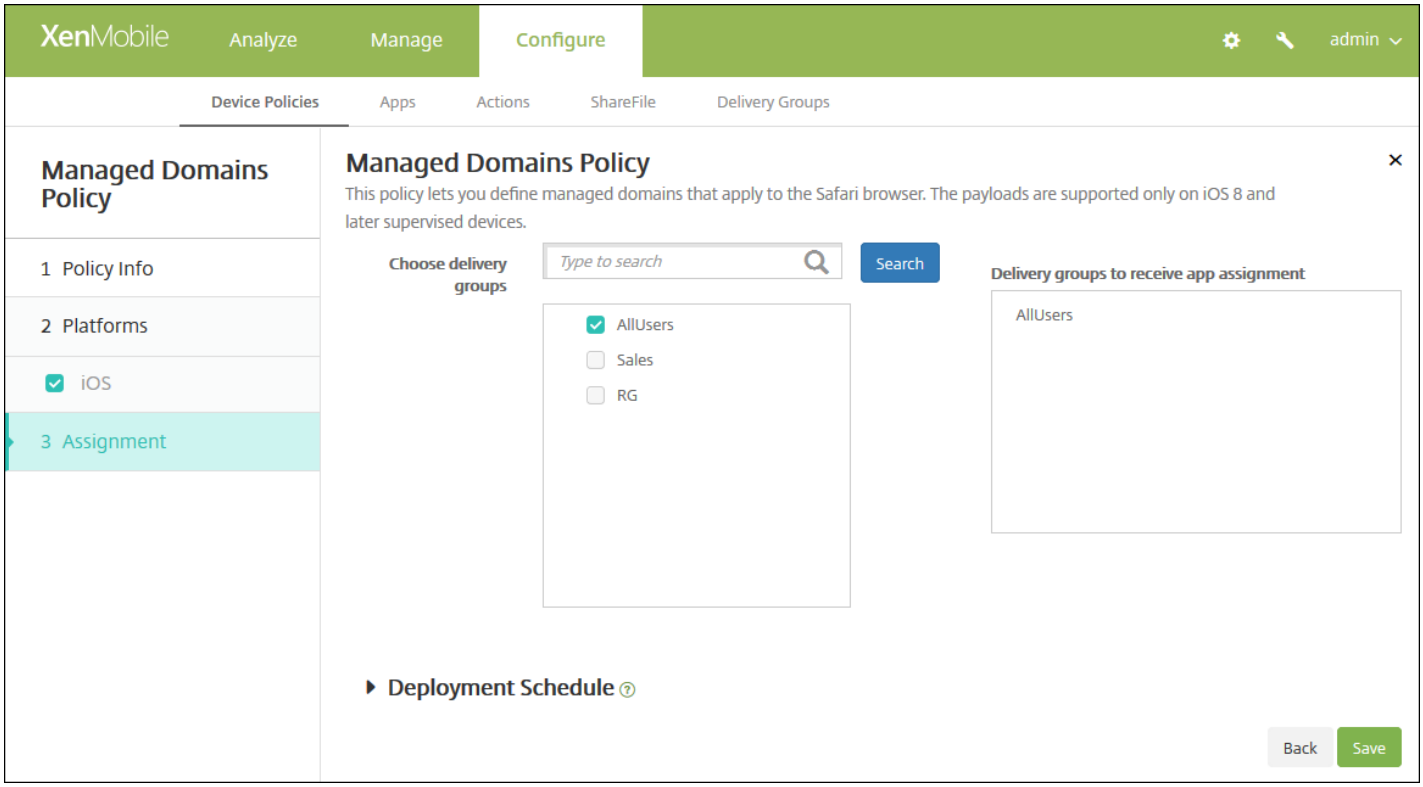
      To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- **Policy Settings**
  - Under **Policy Settings**, next to **Remove policy**, click either **Select date** or **Duration until removal (in days)**.
  - 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 the deployment rules

8. Click **Next**. The **Managed Domains 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**.

MDM options device policy

Nov 16, 2016

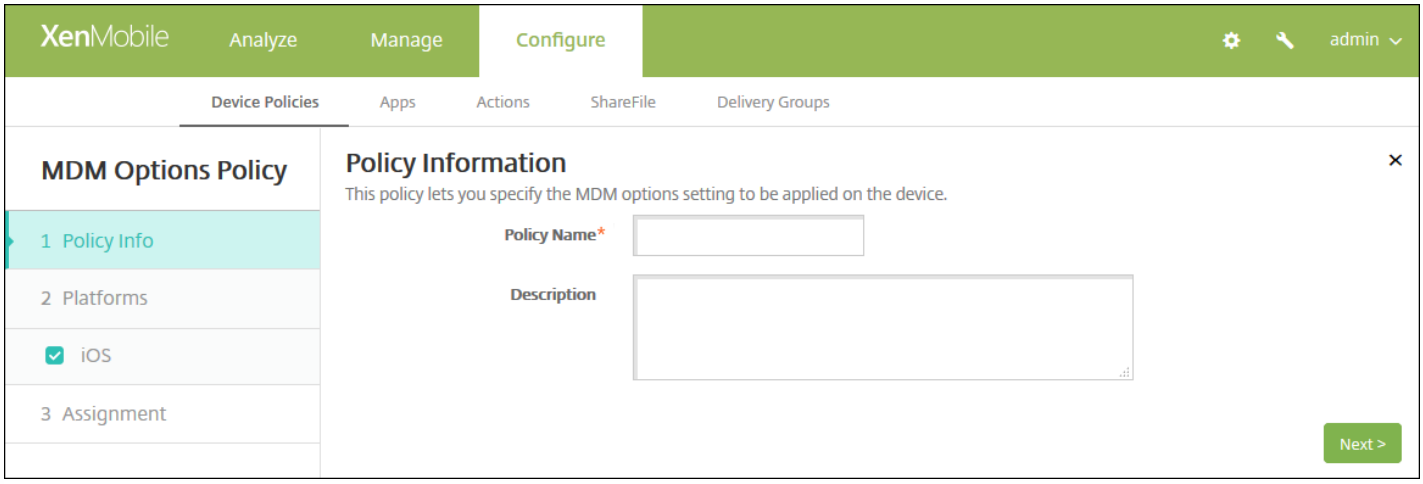
You can create a device policy in XenMobile to manage Find My Phone/iPad Activation Lock on supervised iOS 7.0 and later phone devices. For the steps on setting an iOS device to supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator or iOS Bulk Enrollment.

Activation Lock is a feature of Find My iPhone/iPad that is designed to prevent reactivation of lost or stolen devices by requiring the user's Apple ID and password before anyone can turn off Find My iPhone, erase the device, or reactivate and use the device. In XenMobile, you can bypass the Apple ID and password requirement by enabling Activation Lock in the MDM Options device policy. When a user returns a device with Find My iPhone enabled, you can manage the device from the XenMobile console without their Apple credentials.

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.

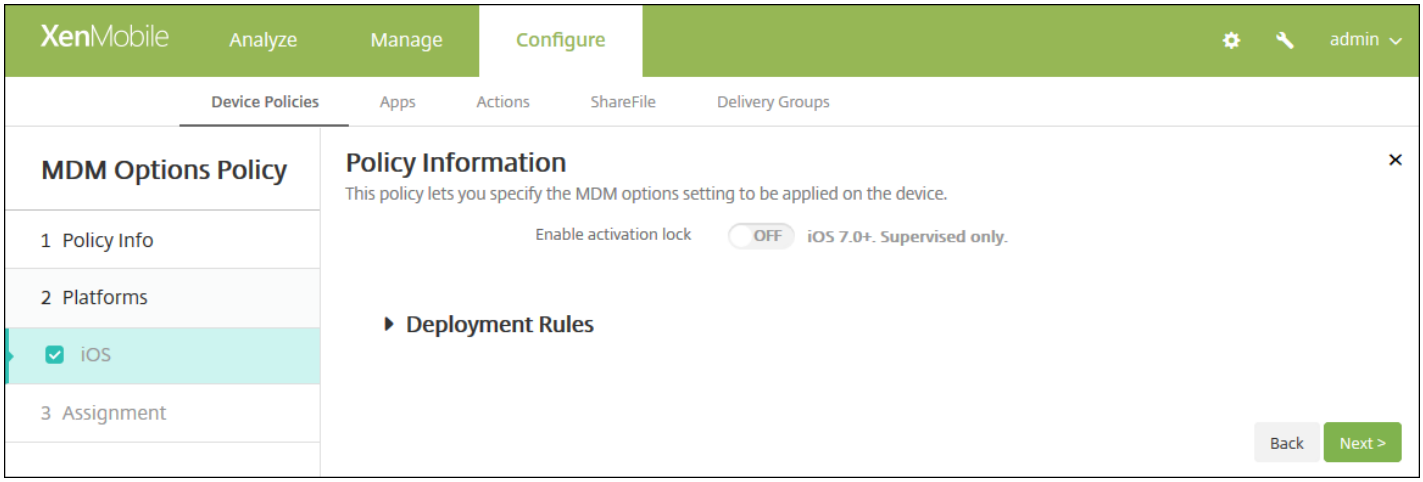
3. Expand **More** and then, under **End user**, click **MDM Options**. The **MDM Options Policy** information page appears.



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.

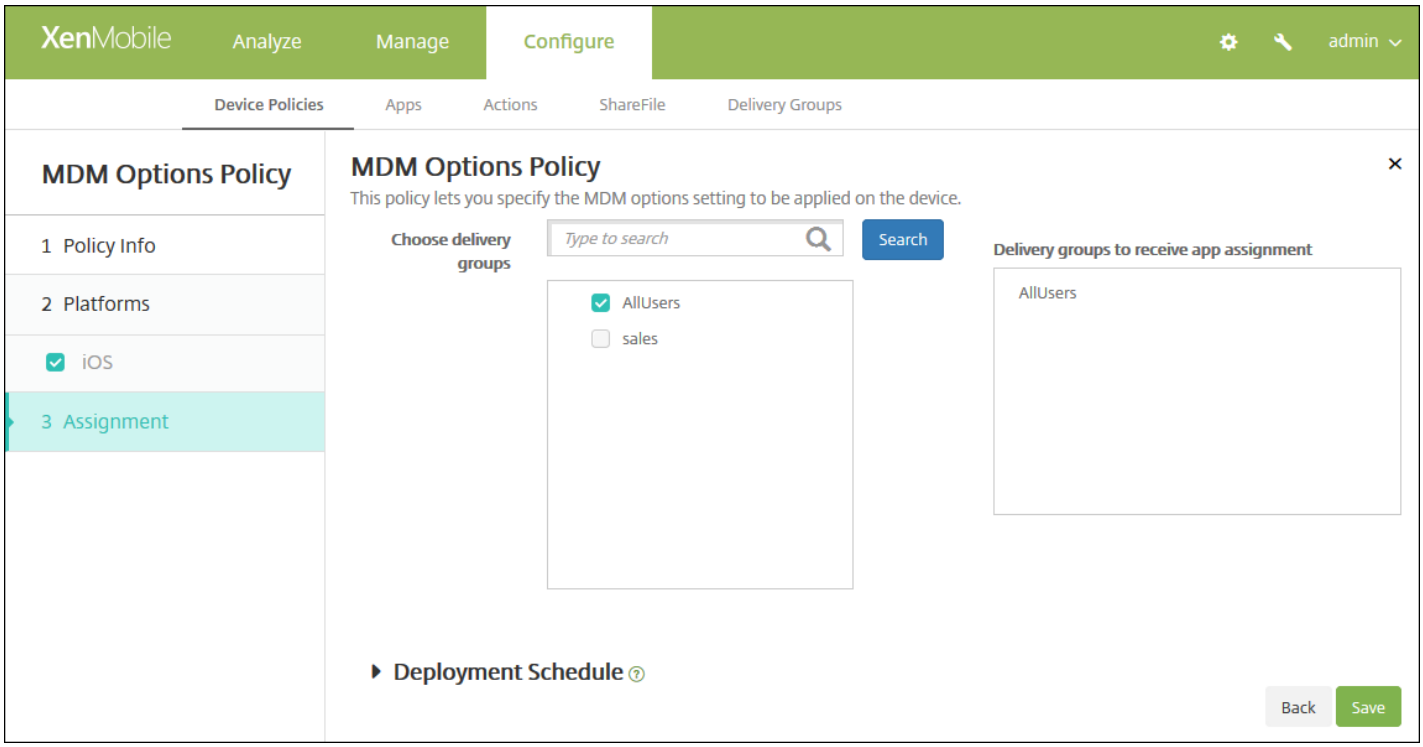


6. Configure this setting:

- **Enable Activation Lock**: Select whether to enable Activation Lock on the devices to which you deploy this policy. The default is **OFF**.

7. Configure the deployment rules

8. Click **Next**. The **MDM Options 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 connectio**n 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**.

Microsoft Exchange ActiveSync device policy

Nov 16, 2016

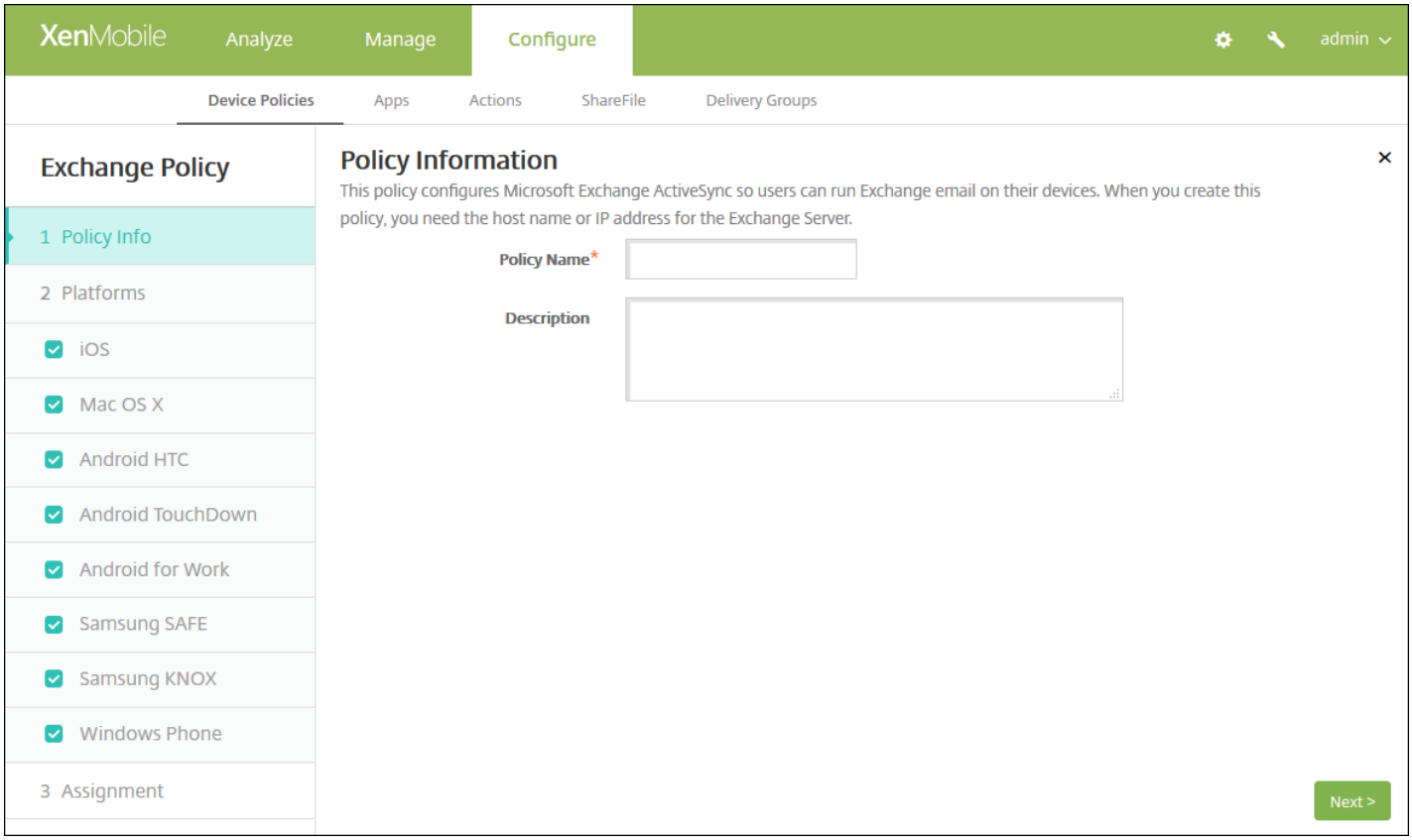
You can use the Exchange ActiveSync device policy to configure an email client on users' devices to let them access their corporate email hosted on Exchange. You can create policies for iOS, Mac OS X, Android HTC, Android TouchDown, Android for Work, Samsung SAFE, Samsung KNOX, and Windows Phone. Each platform requires a different set of values, which are described in detail in the following sections.

Before you can create this policy, you will need to know the host name or IP address of the Exchange Server.

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.



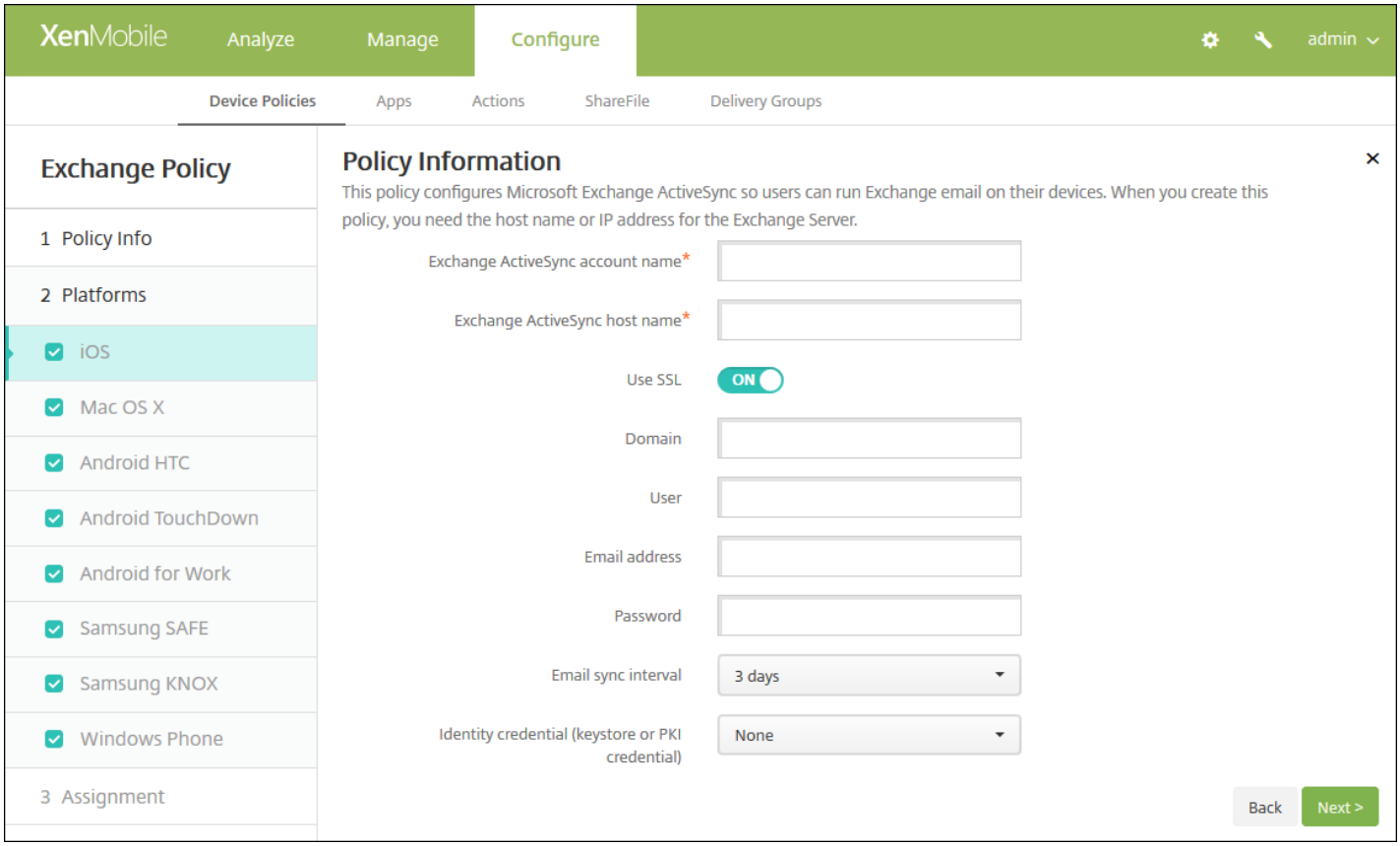
4. In the **Policy Information** pane, type the following information:

- **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 that platform's deployment rules.

Configure iOS settings



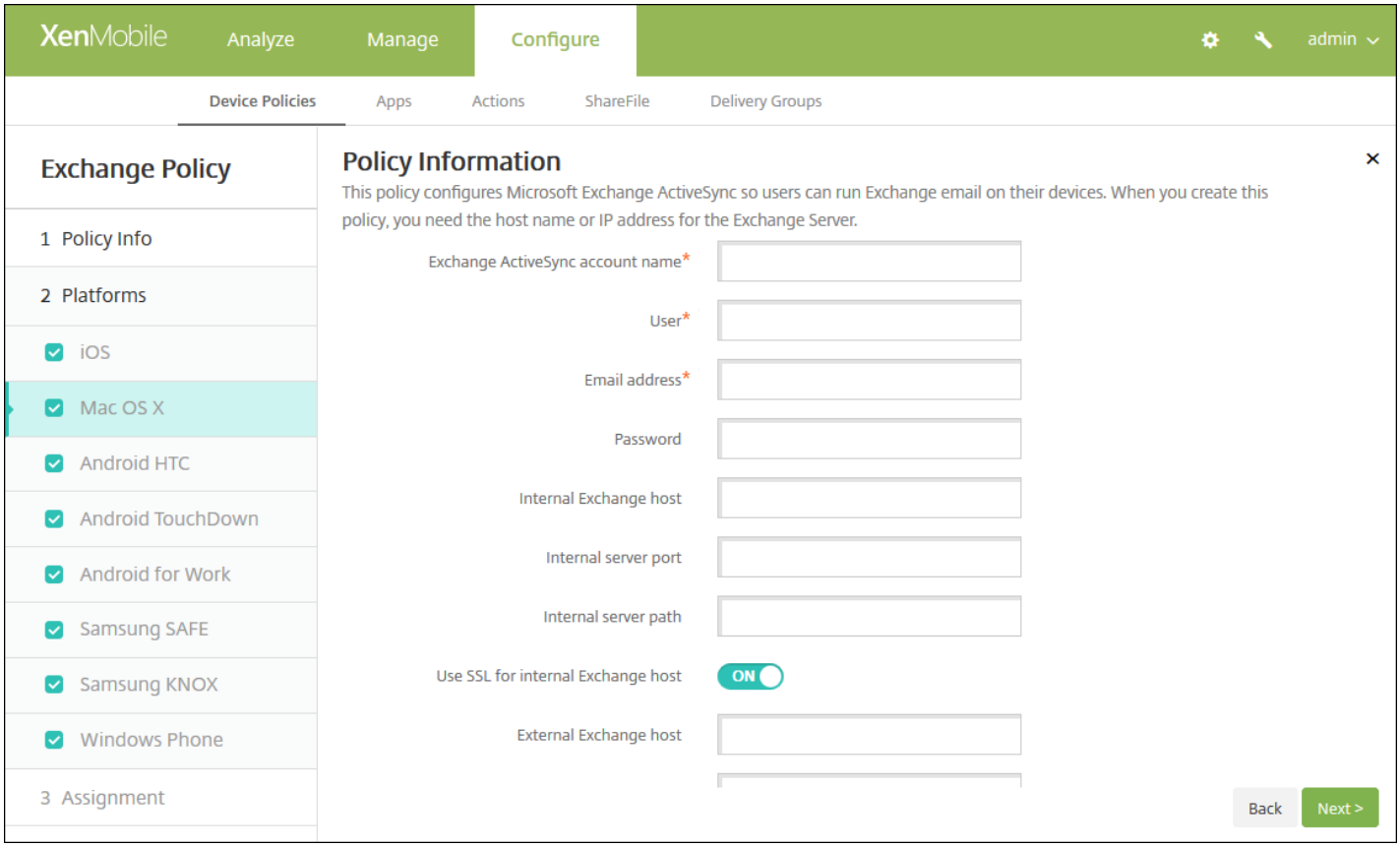
Configure these settings:

- **Exchange ActiveSync account name**: Type the description of the email account that is displayed on users' devices.
- **Exchange ActiveSync host name**: Type the address of the email server.
- **Use SSL**: Select whether to secure connections between users' 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 users' 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 users' names.
- **Email address**: Specify the user's full email address. You can use the system macro ${user.mail} in this field to automatically look up users' 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 Mac OS X settings



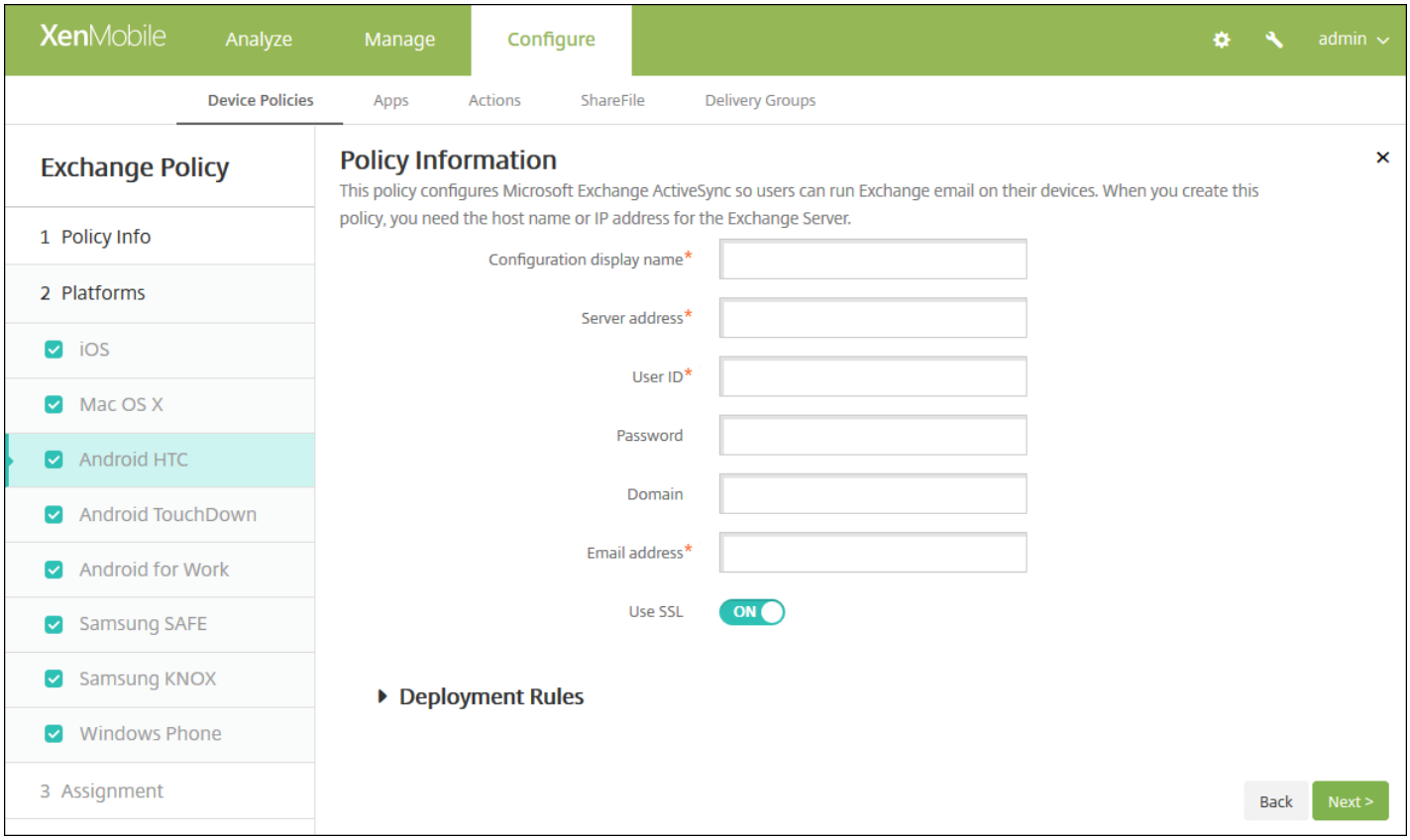
Configure these settings:

- **Exchange ActiveSync account name**: Type the description of the email account that is displayed on users' 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 users' names.
- **Email address**: Specify the user's full email address. You can use the system macro ${user.mail} in this field to automatically look up users' 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 users' 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 users' 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**.

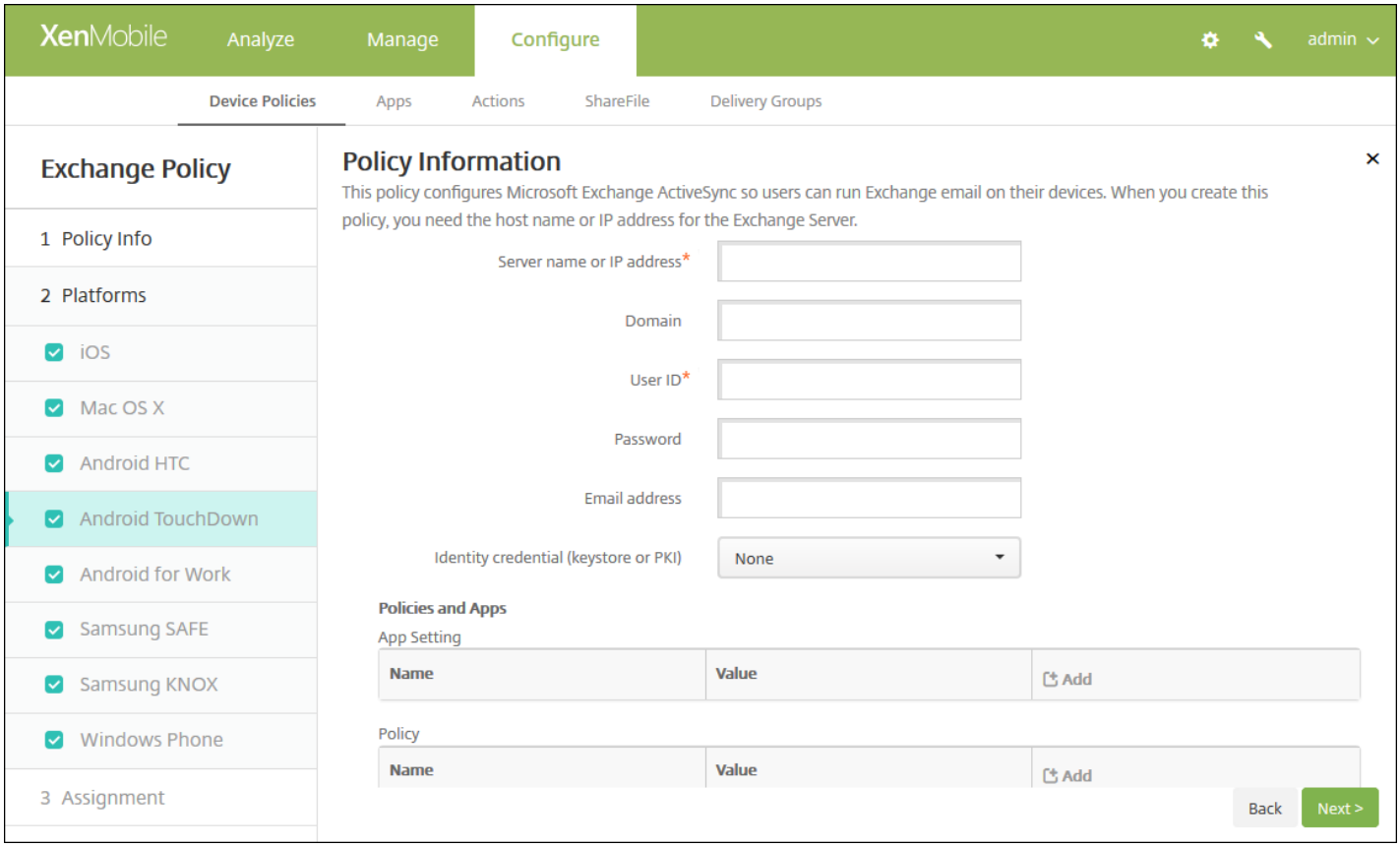
Configure Android HTC settings



Configure these settings:

- **Configuration display name**: Type the name for this policy that appears on users' 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 users' 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 users' domain names.
- **Email address**: Specify the user's full email address. You can use the system macro ${user.mail} in this field to automatically look up users' email accounts.
- **Use SSL**: Select whether to secure connections between users' devices and the Exchange Server. The default is **ON**.

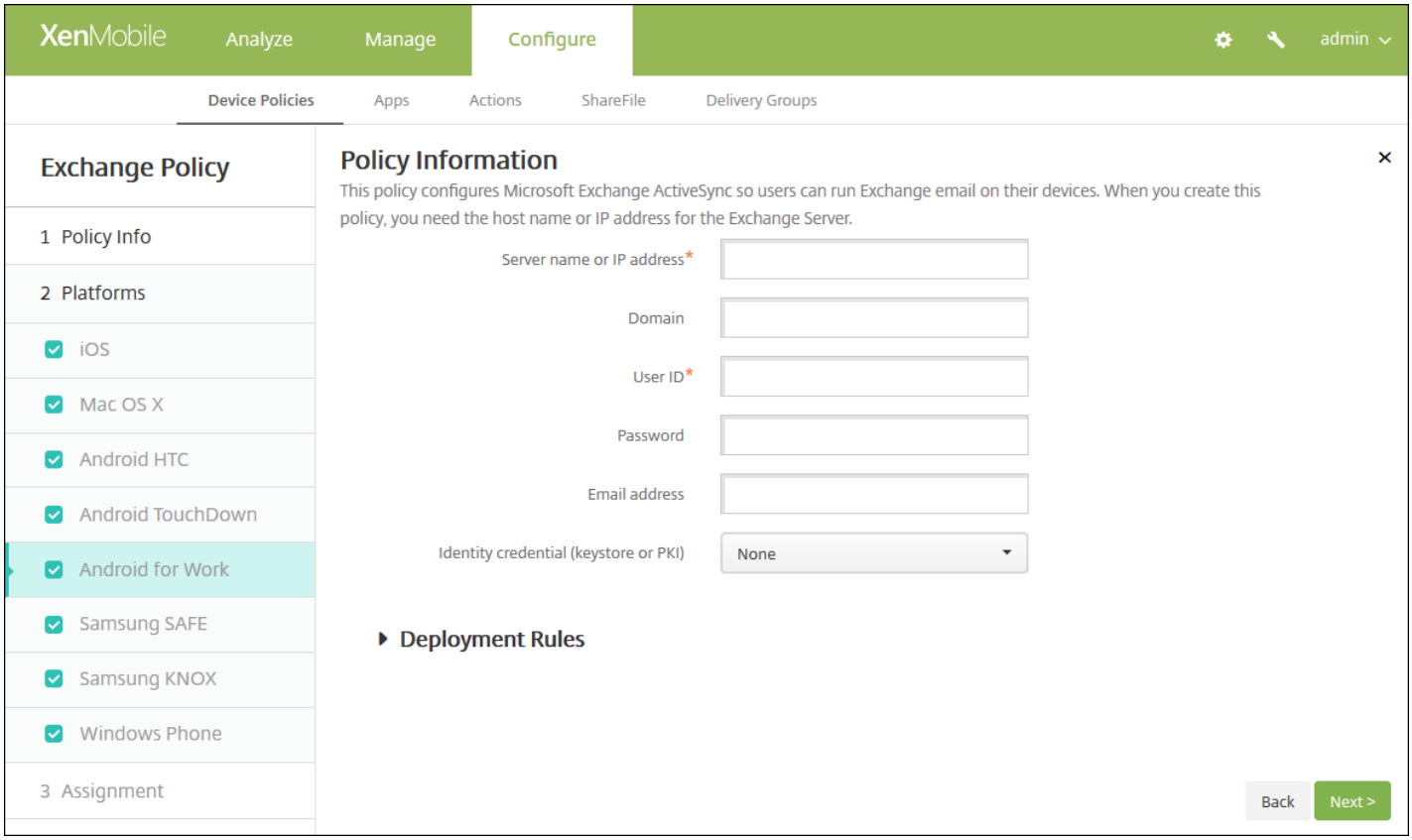
Configure Android TouchDown settings



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 users' 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 users' names.
- **Password**: Type an optional password for the Exchange user account.
- **Email address**: Specify the user's full email address. You can use the system macro ${user.mail} in this field to automatically look up users' 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.

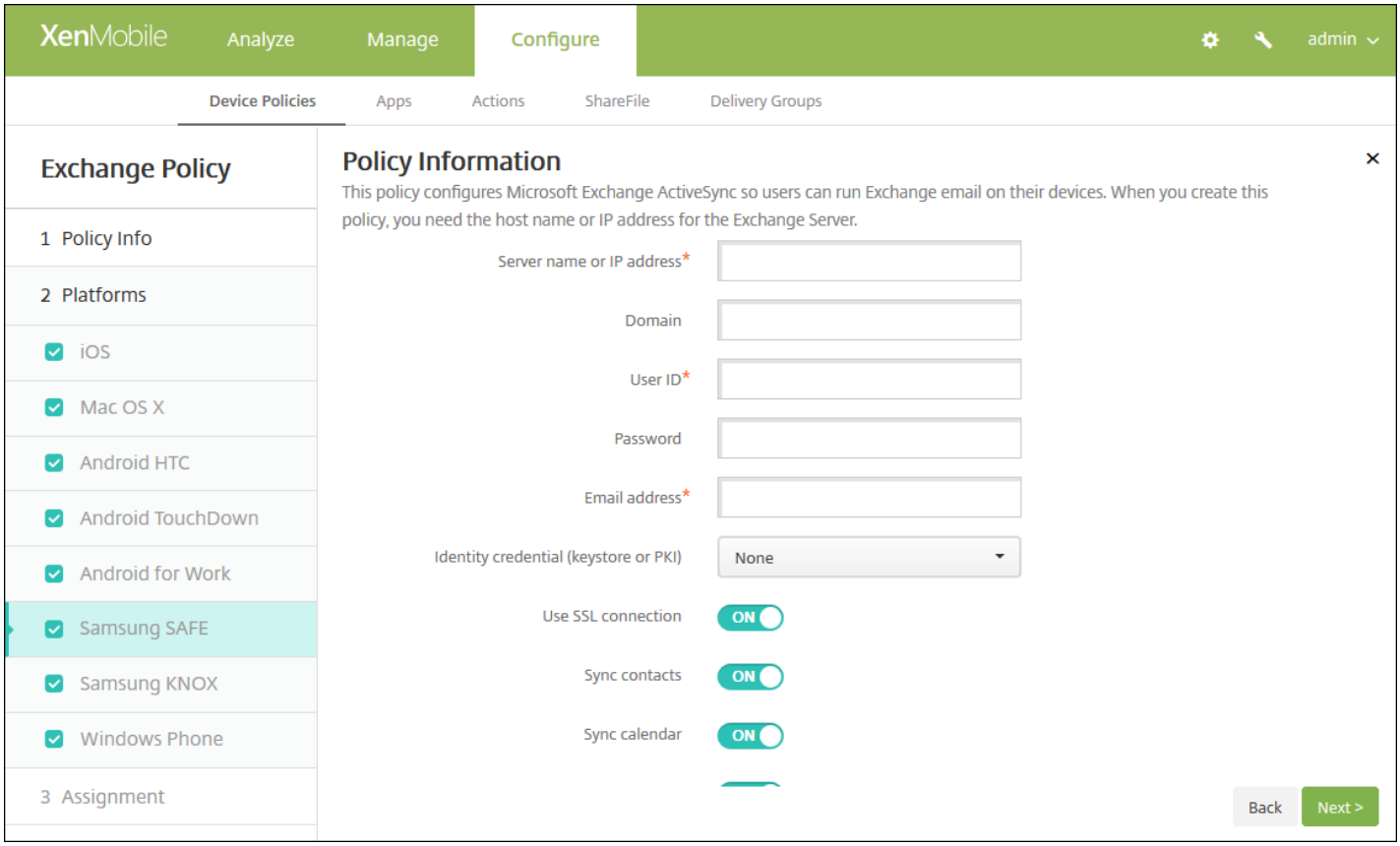
Configure Android for Work



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 users' 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 users' names.
- **Password**: Type an optional password for the Exchange user account.
- **Email address**: Specify the user's full email address. You can use the system macro ${user.mail} in this field to automatically look up users' 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**.

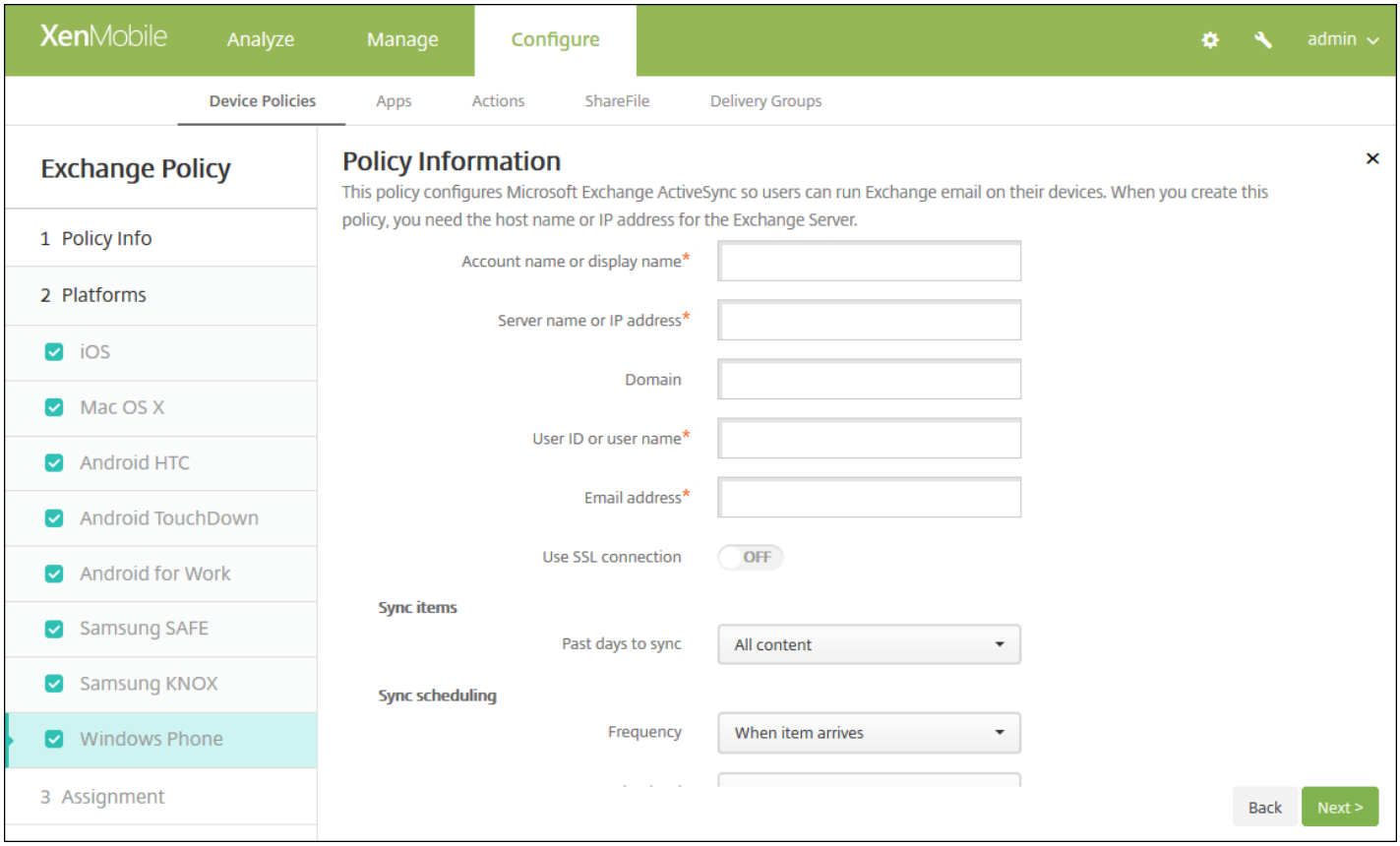
Configure Samsung SAFE and Samsung KNOX settings



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 users' 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 users' names.
- **Password**: Type an optional password for the Exchange user account.
- **Email address**: Specify the user's full email address. You can use the system macro ${user.mail} in this field to automatically look up users' 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 users' devices and the Exchange Server. The default is **ON**.
- **Sync contacts**: Select whether to enable synchronization for users' contacts between their devices and the Exchange Server. The default is **ON**.
- **Sync calendar**: Select whether to enable synchronization for users' calendars between their devices and the Exchange Server. The default is **ON**.
- **Default account**: Select whether to make users' Exchange account the default for sending email from their devices. The default is **ON**.

Configure Windows Phone settings



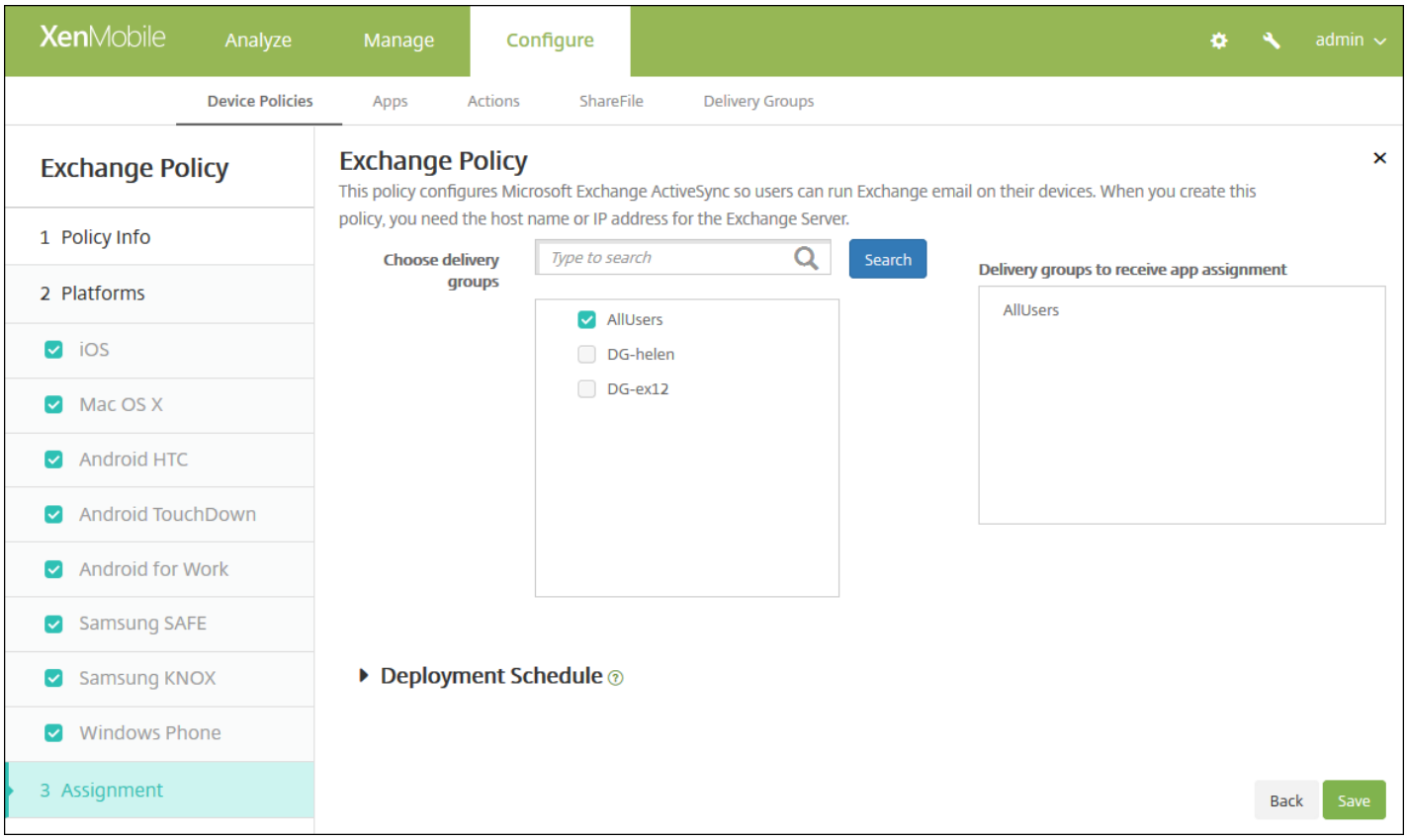
Configure these settings:

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 users' 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 users' names.
- **Email address**: Specify the user's full email address. You can use the system macro ${user.mail} in this field to automatically look up users' email accounts.
- **Use SSL connection**: Select whether to secure connections between users' 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 the deployment rules

8. Click **Next**. the **Exchange 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**.

Organization information device policy

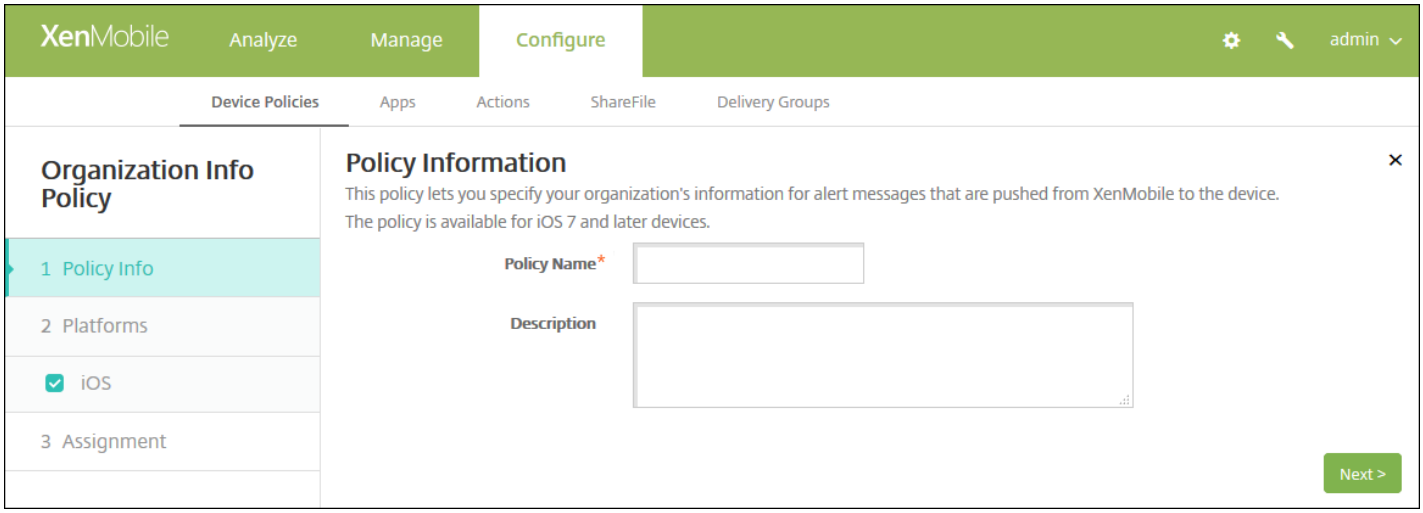
Nov 16, 2016

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.

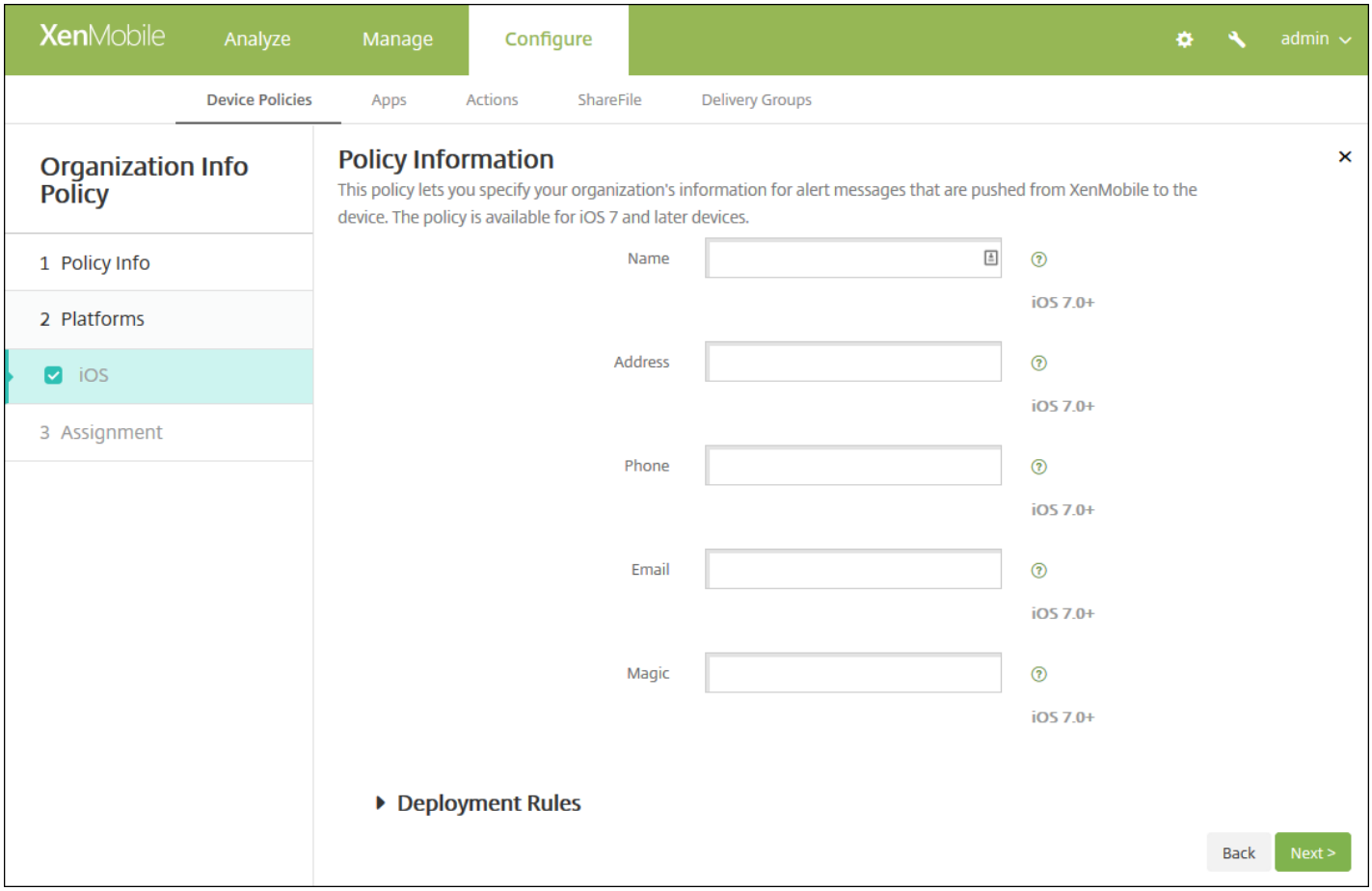
3. Click **More** and then, under **End user**, click **Organization info**. The **Organization Info Policy** page appears.



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.

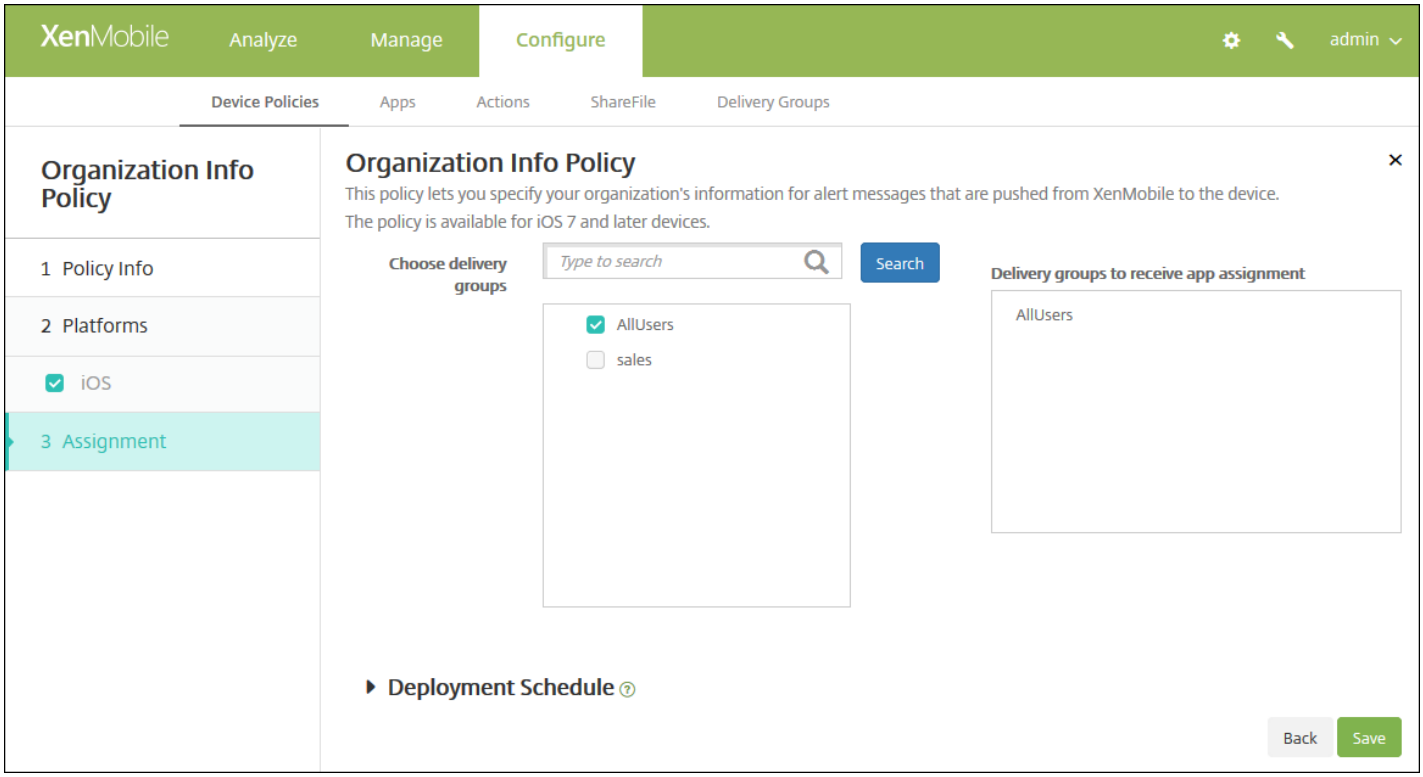


Configure these settings:

- **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 the deployment rules

8. Click **Next**. The **Organization Info 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.

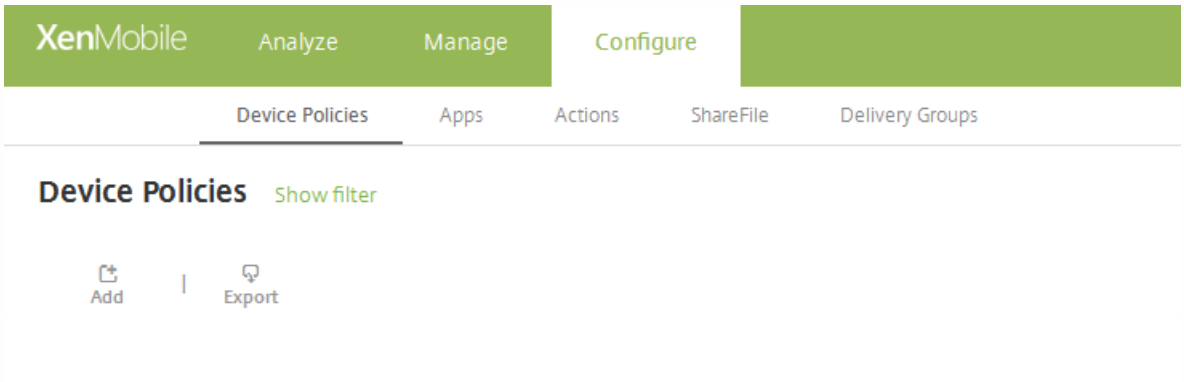
11. Click **Save**.

Passcode device policy

Nov 16, 2016

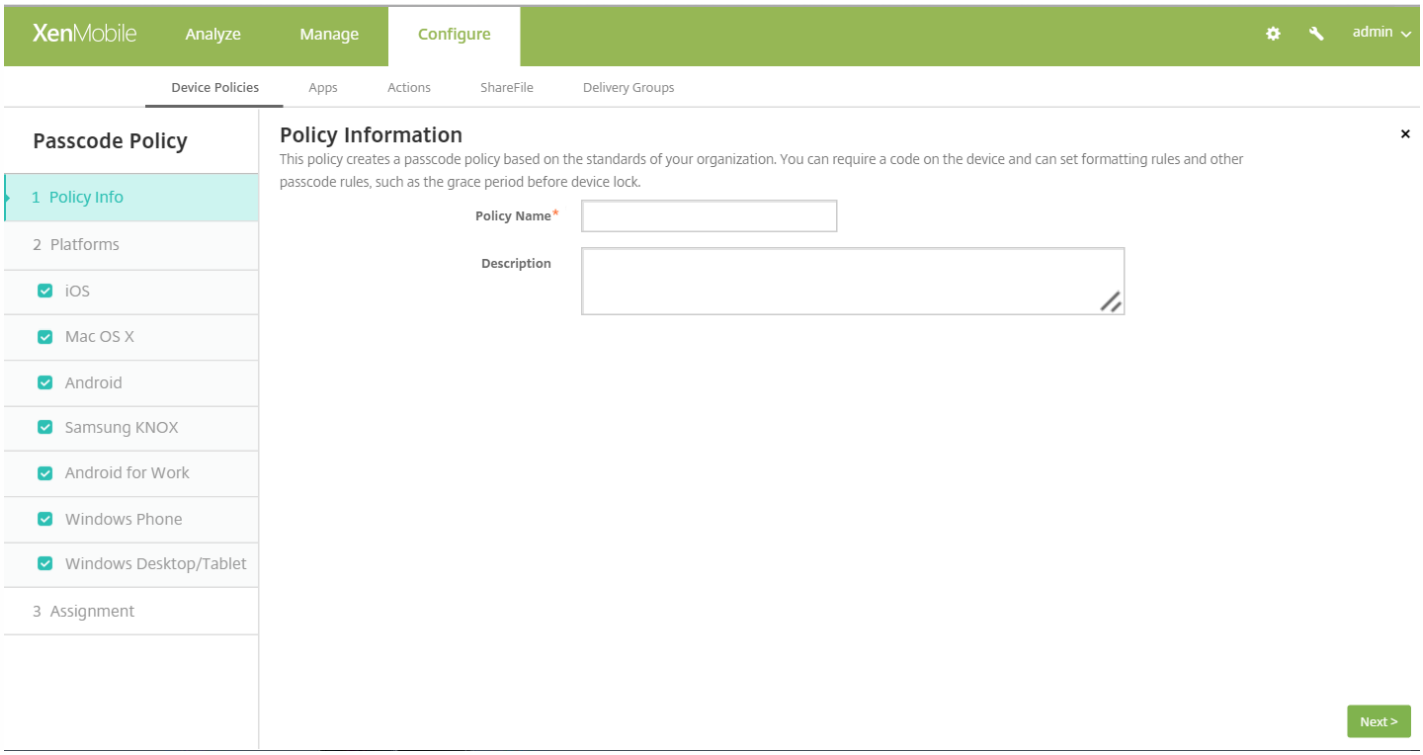
You create a passcode policy in XenMobile based on your organization's standards. You can require passcodes on users' devices and can set various formatting and passcode rules. You can create policies for iOS, Mac OS X, Android, Samsung KNOX, Android for Work, Windows Phone, and Windows desktop/tablet. Each platform requires a different set of values, which are described in this article.

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:

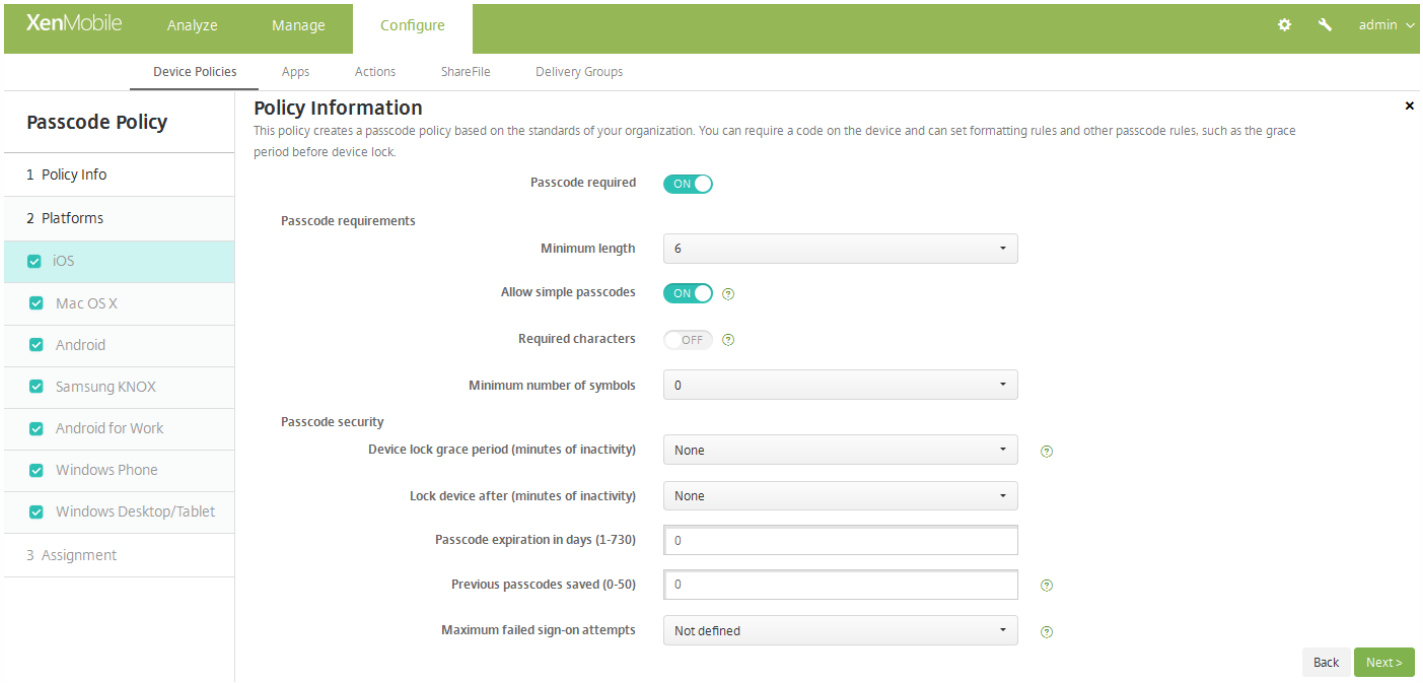
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

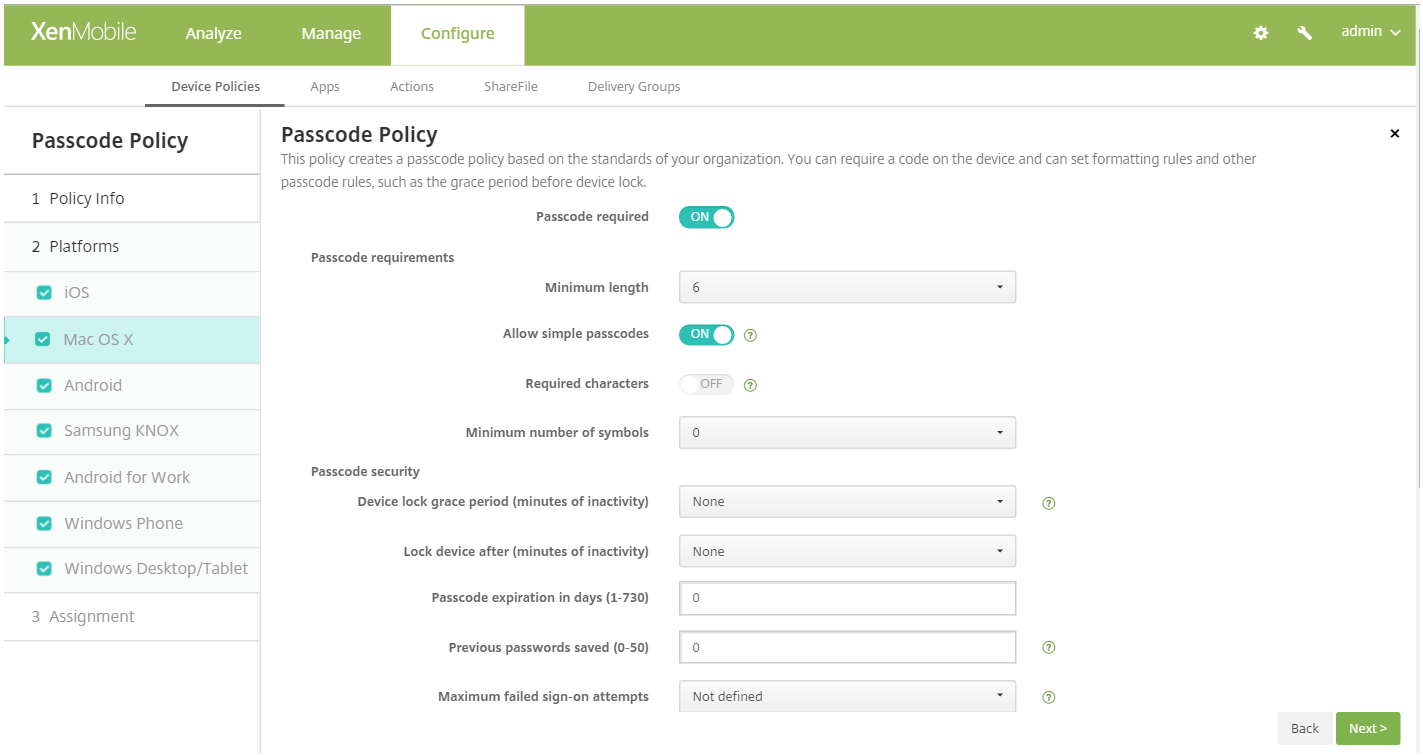
Configure iOS settings



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 days)**.
  - 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 Mac OS X settings



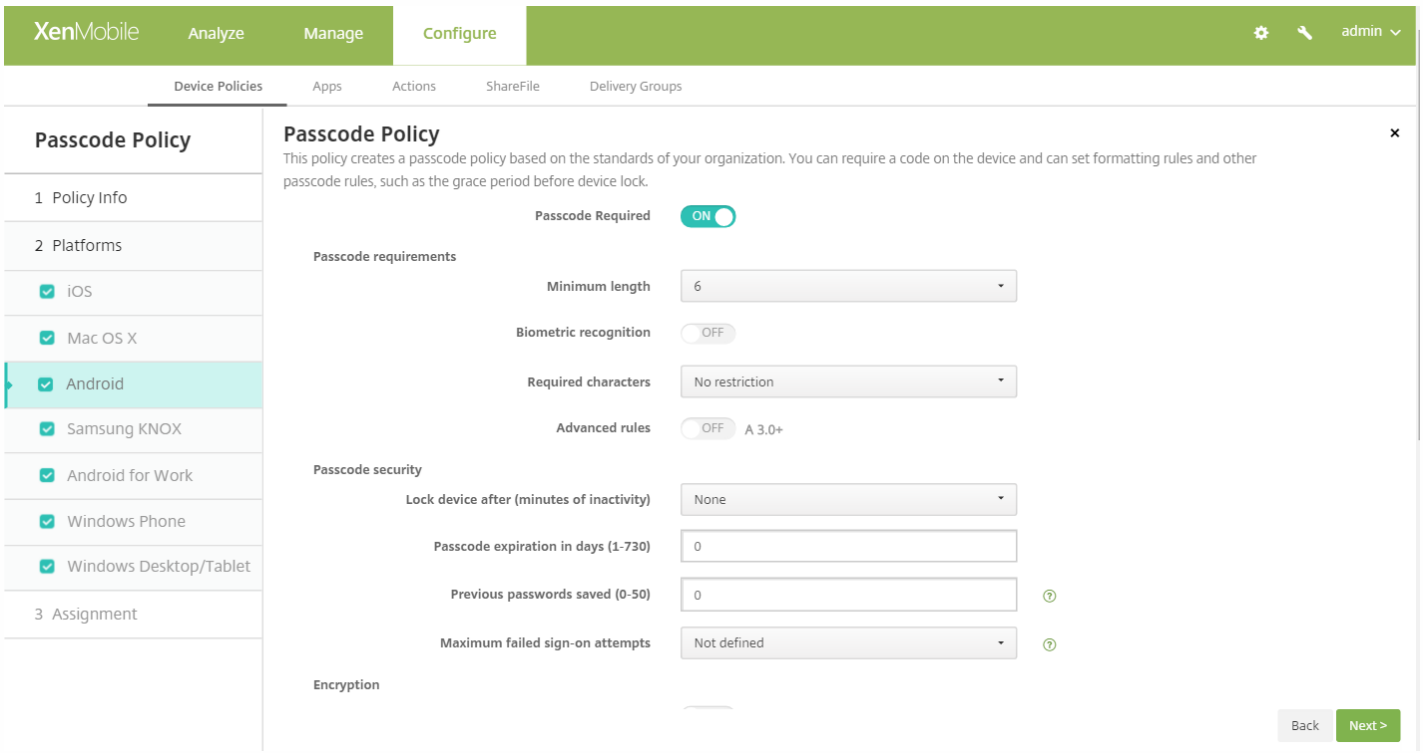
Configure these settings:

- **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 days)**.
  - 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 OS X 10.7 and later.

Configure Android settings



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.

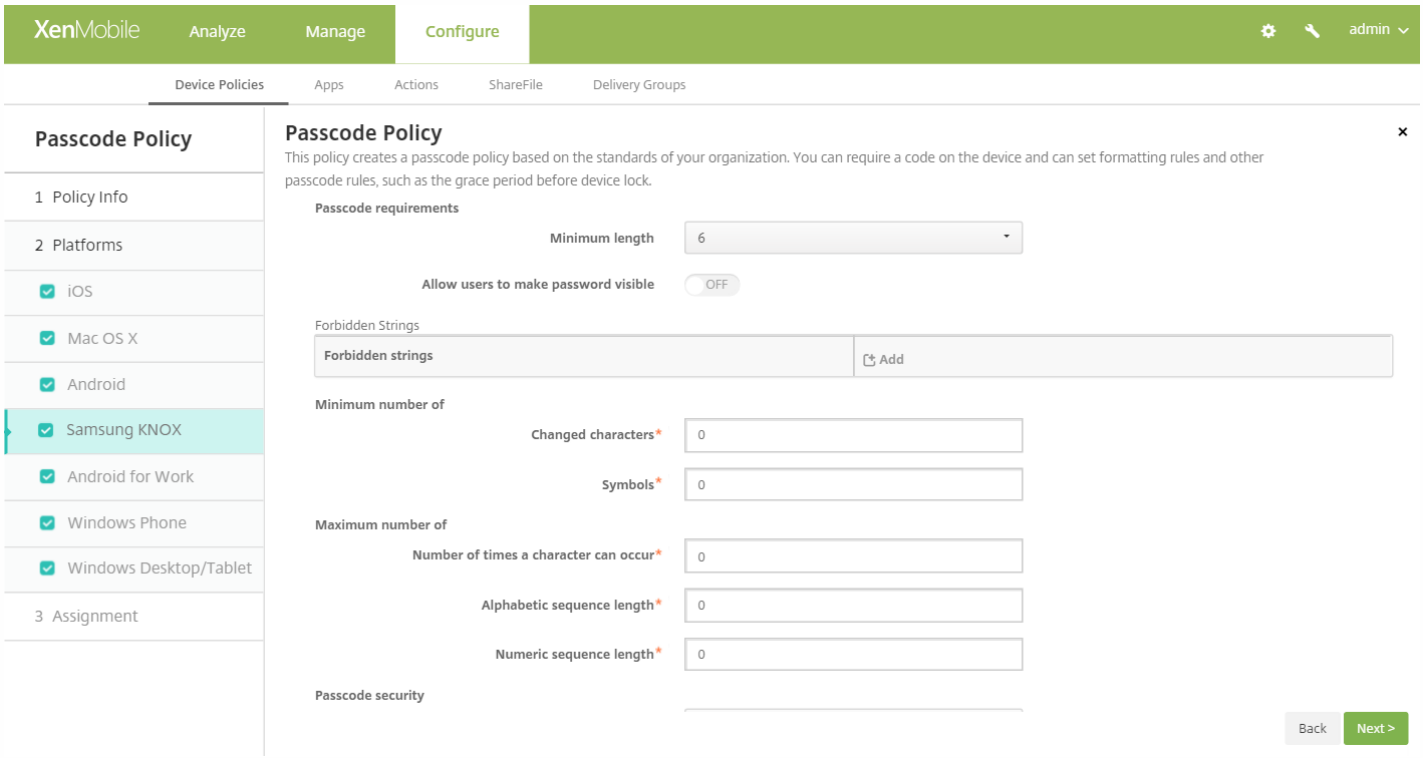
- **Samsung SAFE**
  - **Use same passcode across all users**: Select whether to use the same passcode for all users. The default is **OFF**. This setting applies only to Samsung SAFE devices and is available regardless of the **Passcode required** setting.
  - When you enable **Use same passcode across 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**.
    - **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



Configure these settings:

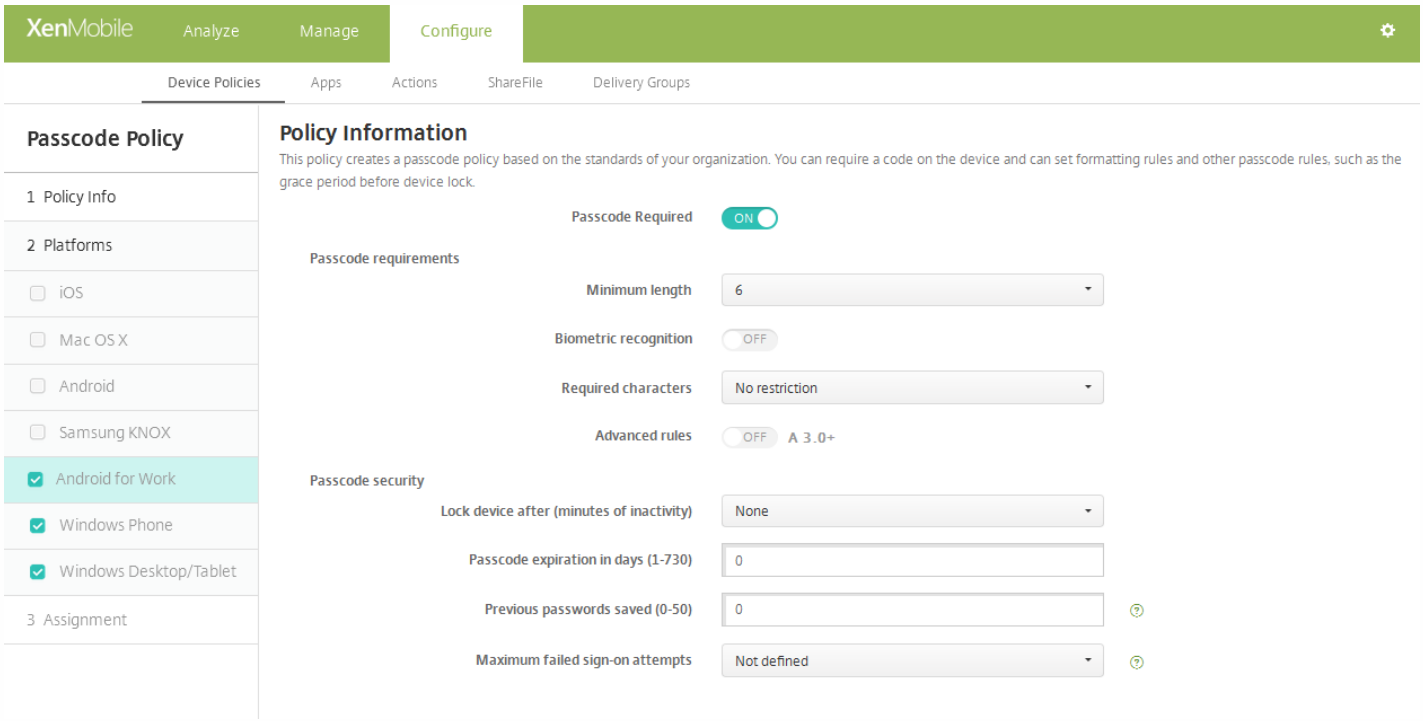
- **Passcode requirements**
  - **Minimum length**: In the list, click the minimum passcode length. The default is **6**.
  - **Allow users to make password visible**: Select whether to let users make the password visible.
  - **Forbidden strings**: You create forbidden strings to prevent users from 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



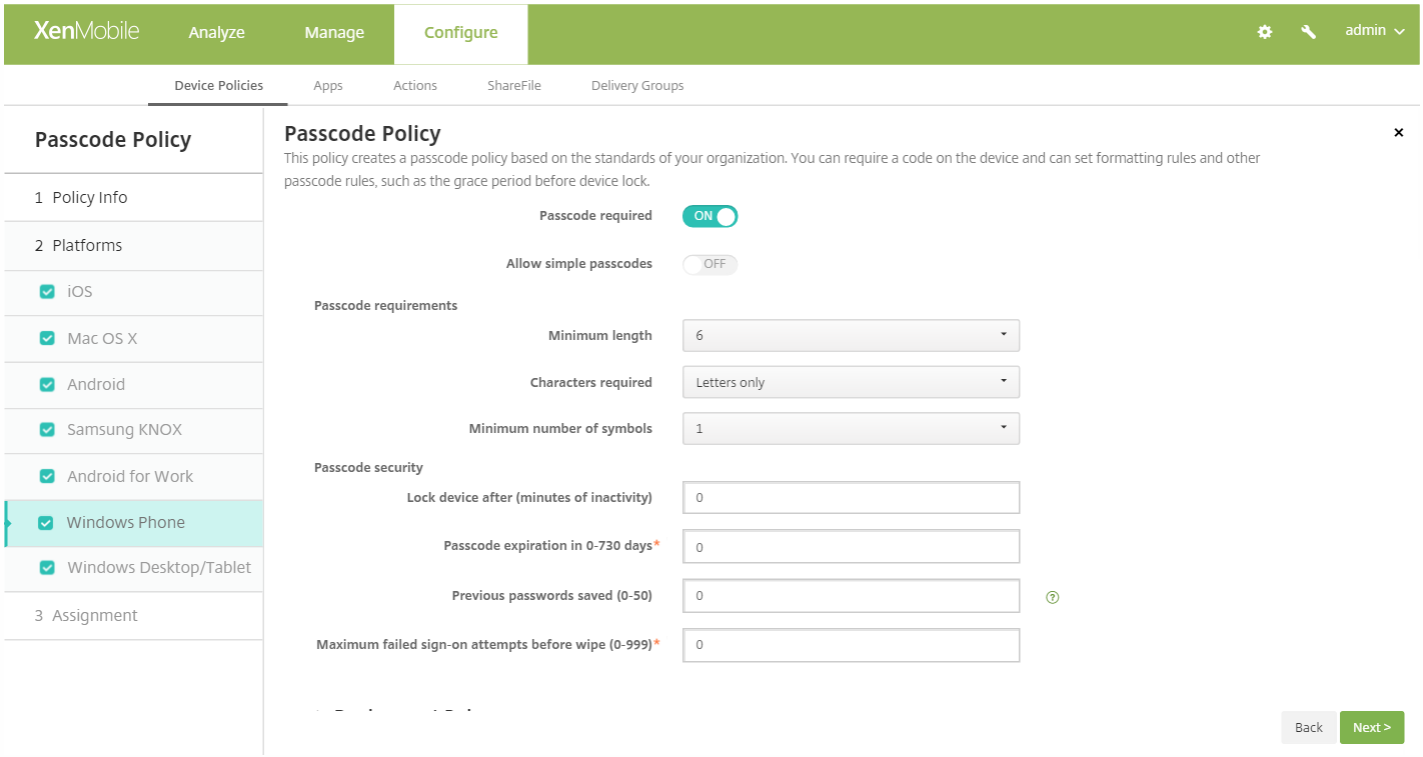
Configure these settings:

- **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**.

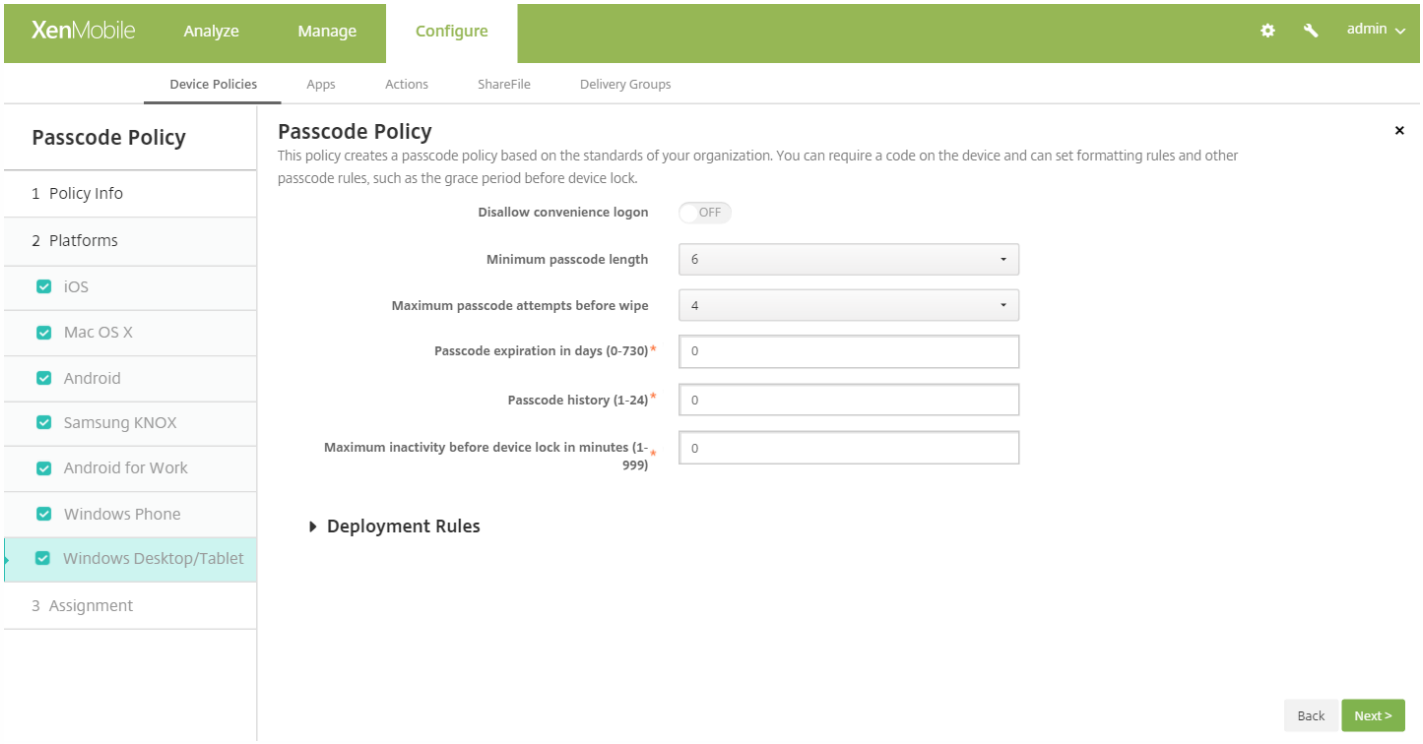
Configure Windows Phone settings



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

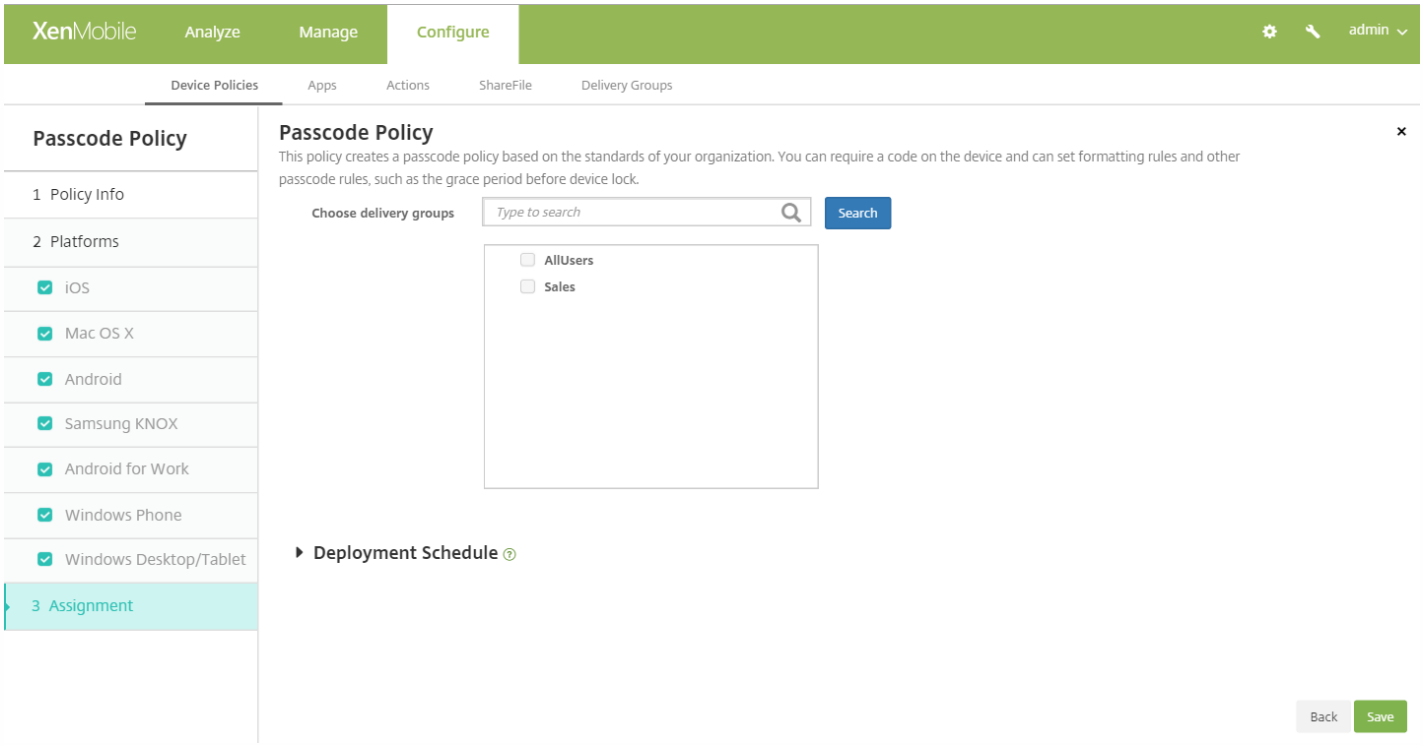


Configure these settings:

- **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 the deployment rules

8. Click **Next**. The **Passcode 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**.

Personal hotspot device policy

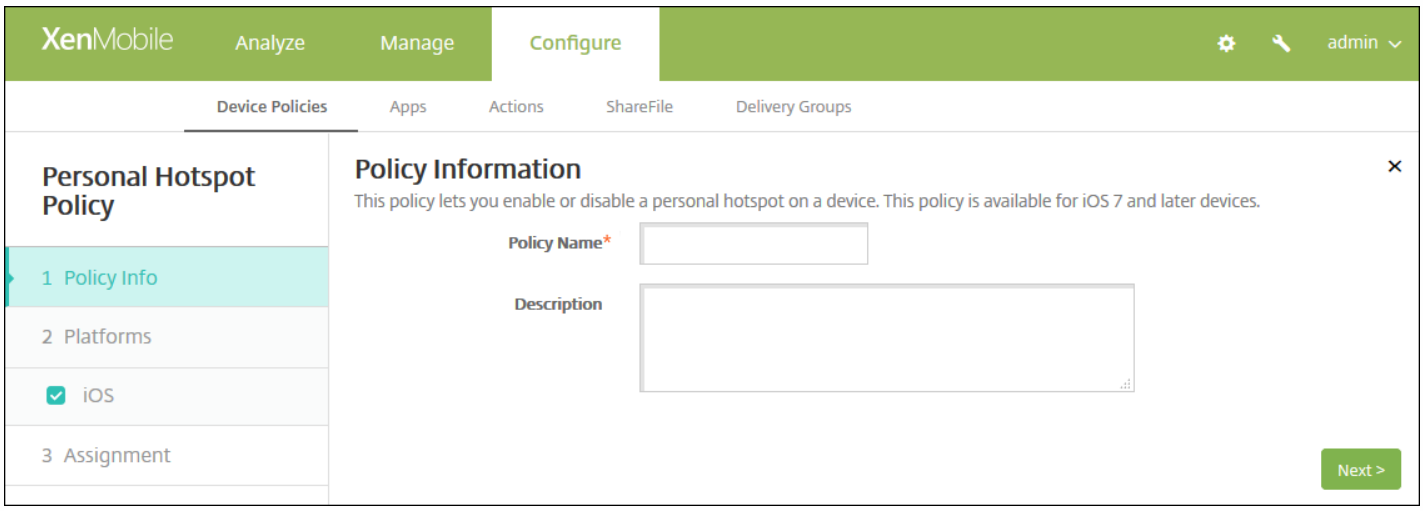
Nov 16, 2016

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.

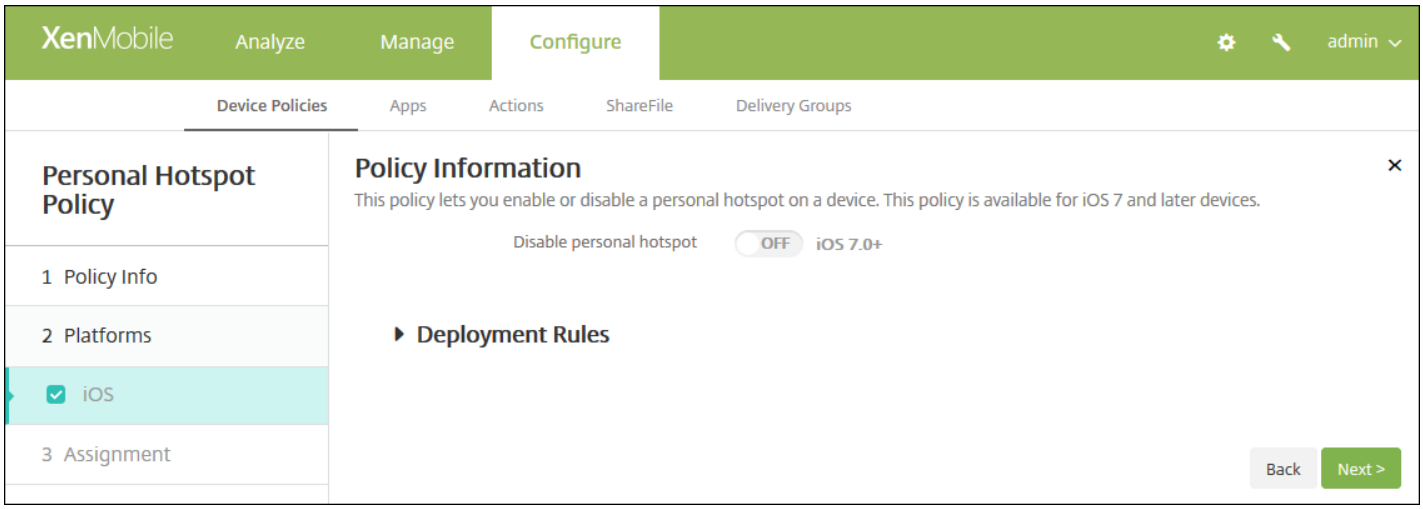
3. Expand **More**, and then under **Network Access**, click **Personal Hotspot**. The **Personal Hotspot Policy** information page appears.



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.

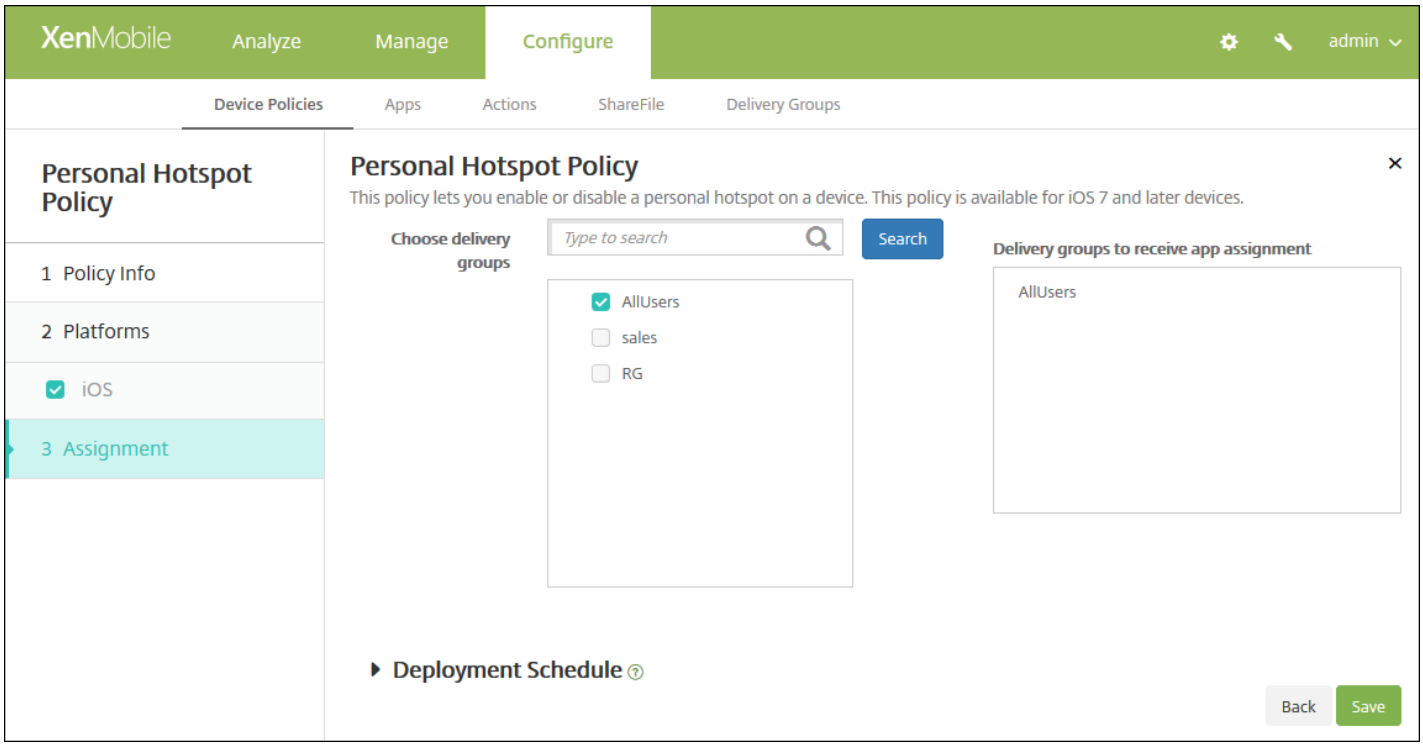


6. Configure this setting:

- **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 the deployment rules

8. Click **Next**. The **Personal Hotspot 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**.

Profile Removal device policy

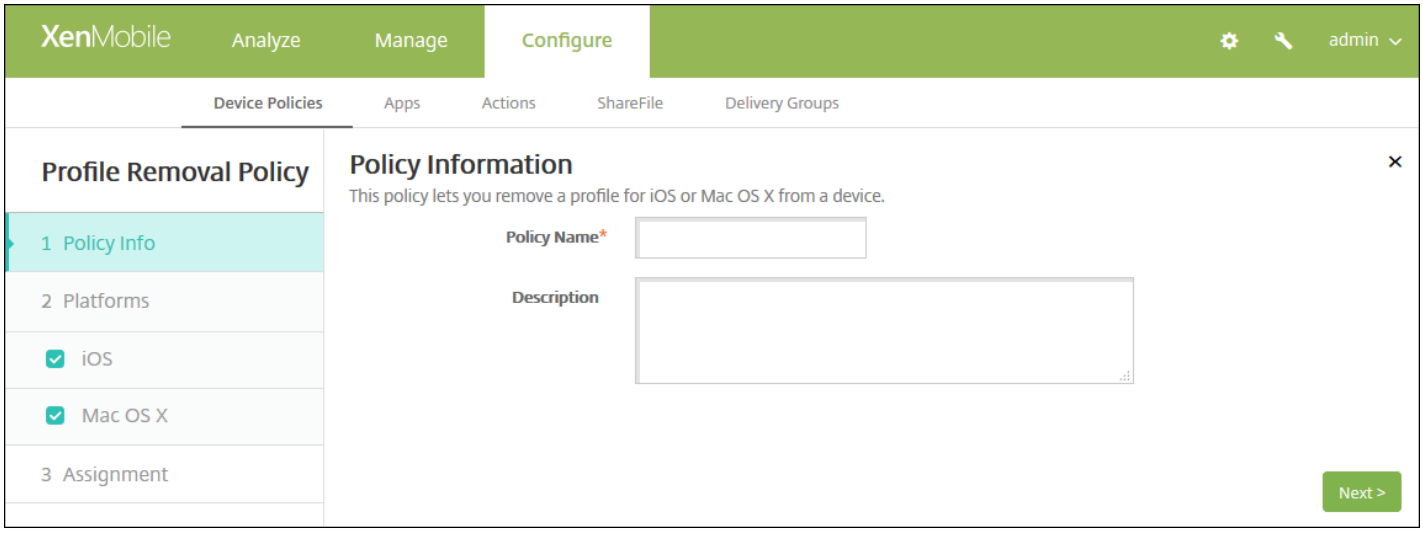
Nov 16, 2016

You can create an app profile removal device policy in XenMobile. The policy, when deployed, removes the app profile from users' iOS or Mac OS X 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:

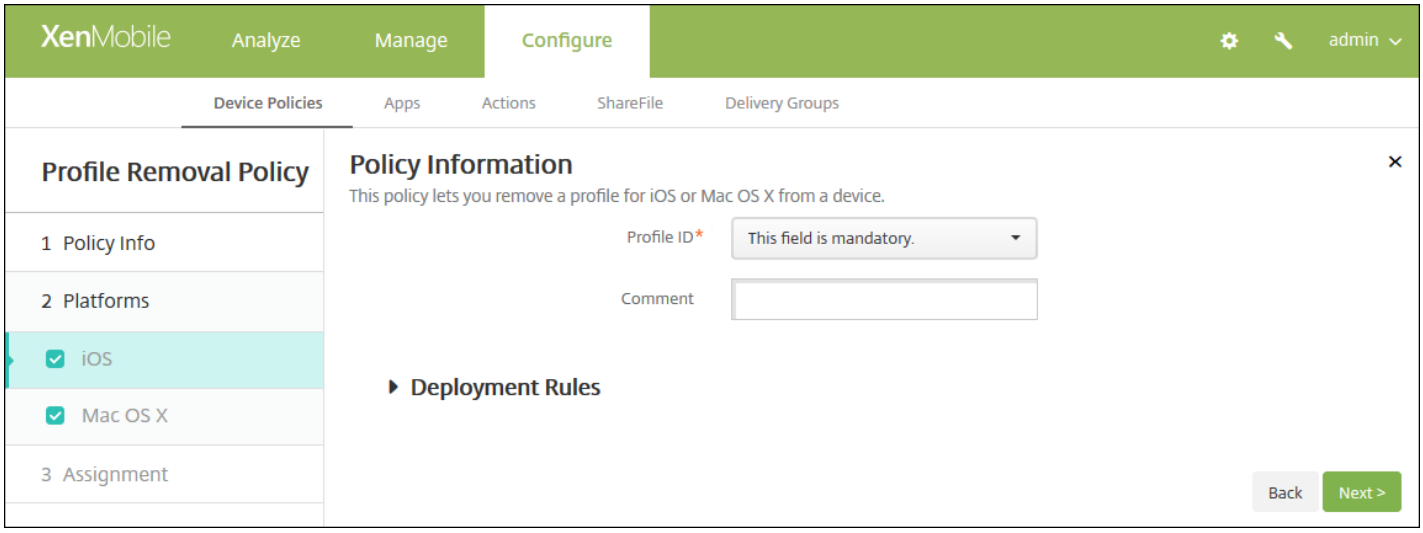
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

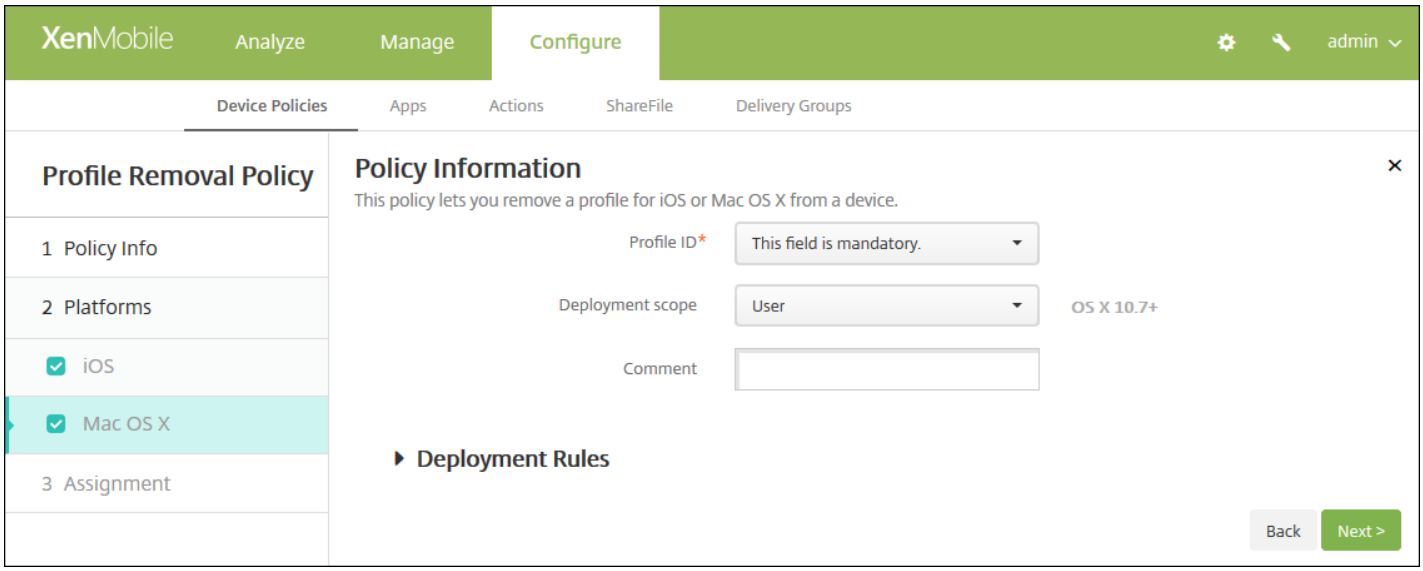
Configure iOS setting



Configure these settings:

- **Profile ID**: In the list, click the app profile ID. This field is required.
- **Comment**: Type an optional comment.

Configure Mac OS X settings

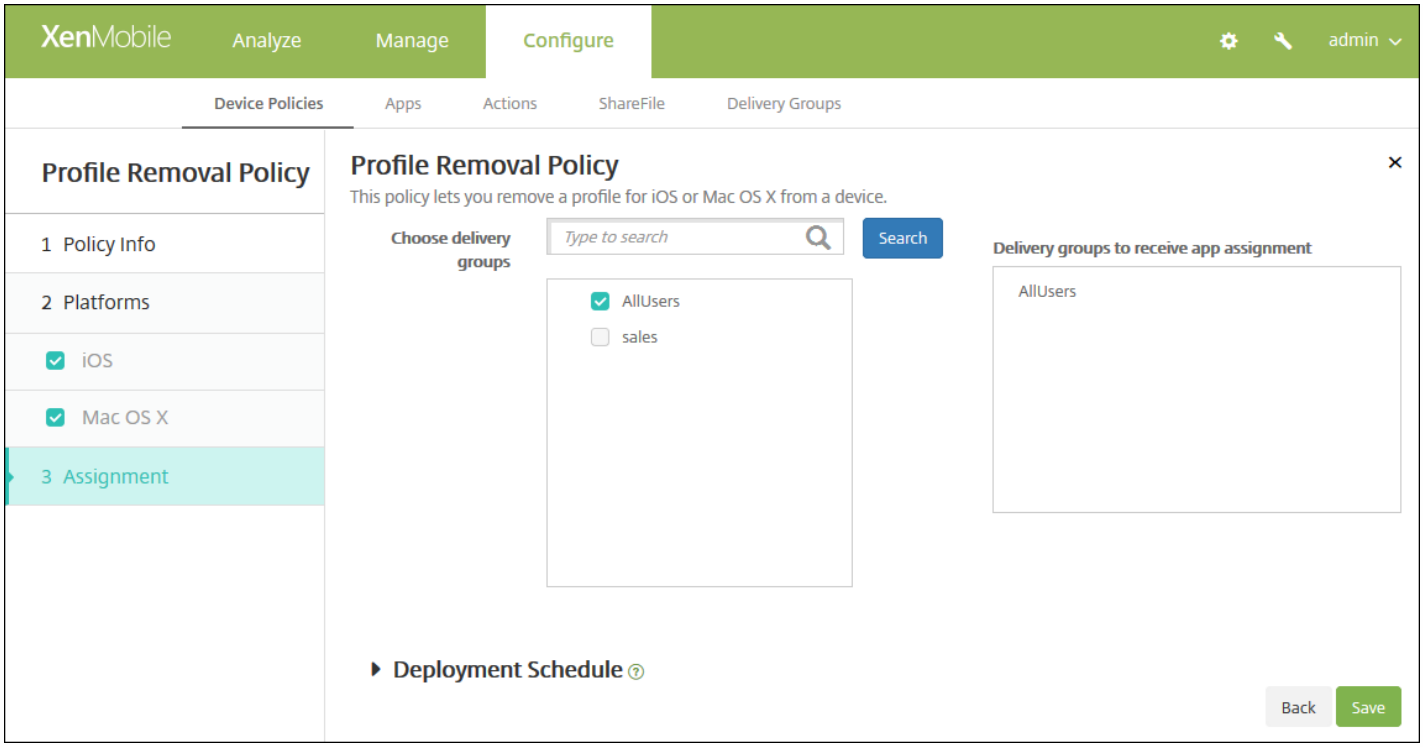


Configure these settings:

- **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 OS X 10.7 and later.
- **Comment**: Type an optional comment.

7. Configure the deployment rules

8. Click **Next**. The **Profile Removal 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**.

Provisioning profile device policy

Nov 16, 2016

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.

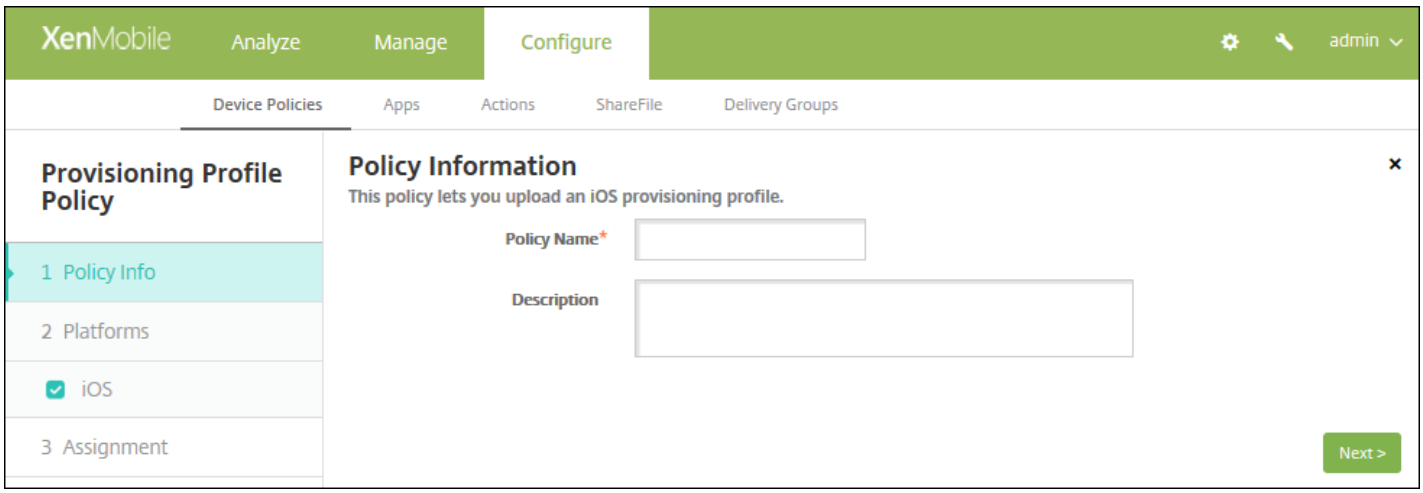
To make this process transparent to users, in XenMobile you can install and remove provisioning profiles with device policies. Missing or expired profiles are removed as necessary and the up-to-date profiles are installed on users' devices, so that tapping an app simply opens it for use.

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.

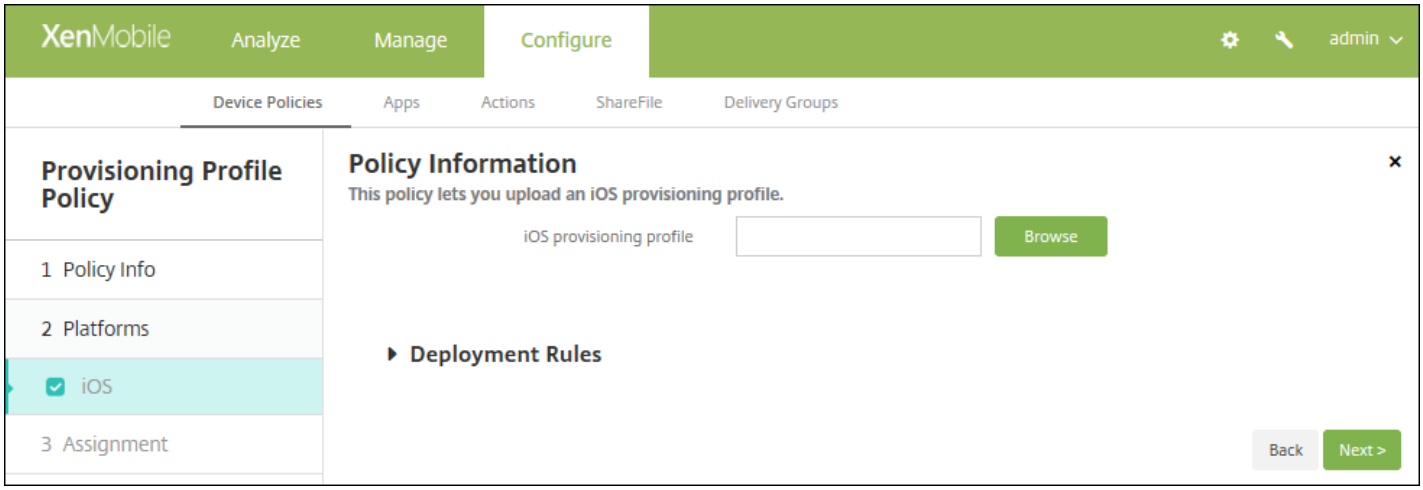
3. Expand **More** and then, under **Apps**, click **Provisioning Profile**. The **Provisioning Profile Policy** information page appears.



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.

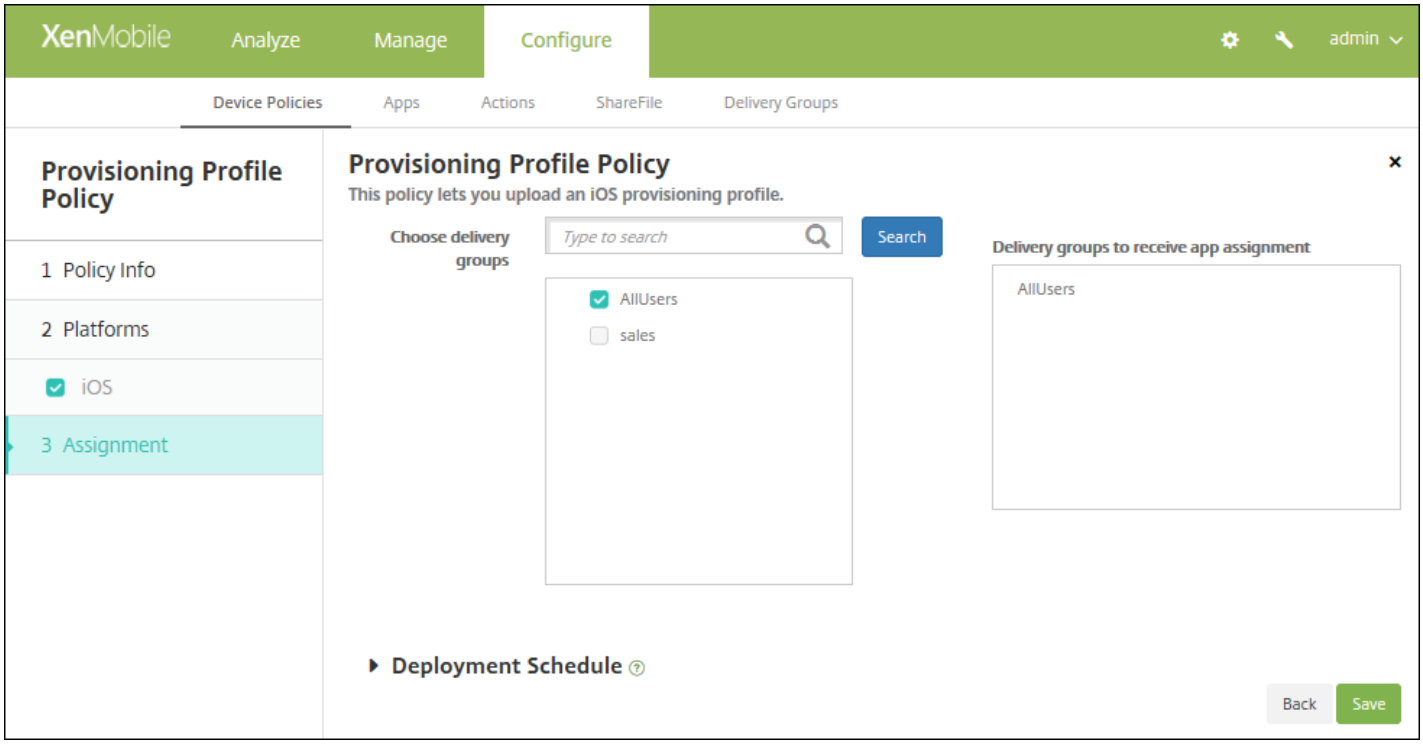


6. Configure this setiing:

- **iOS provisioning profile**: Select the provisioning profile file to import by clicking **Browse** and then navigating to the file's location.

7. Configure the deployment rules

8. Click **Next**. The **Provisioning Profile 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**.

Provisioning profile removal device policy

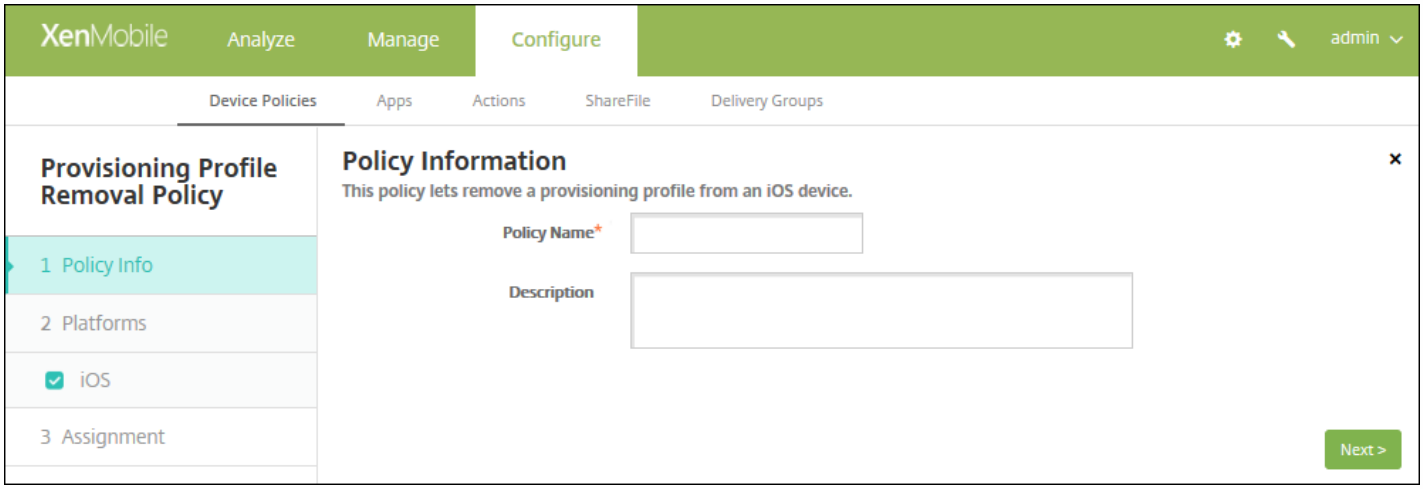
Nov 16, 2016

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.

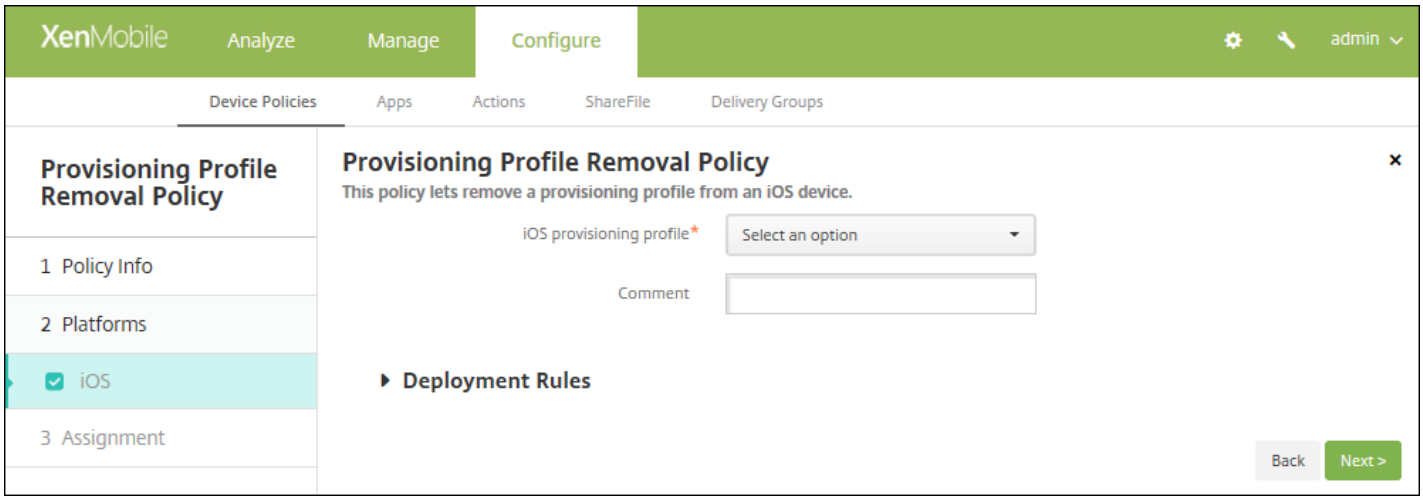
3. Expand **More** and then, under **Removal**, click **Provisioning Profile removal**. The **Provisioning Profile Removal Policy** information page appears.



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.

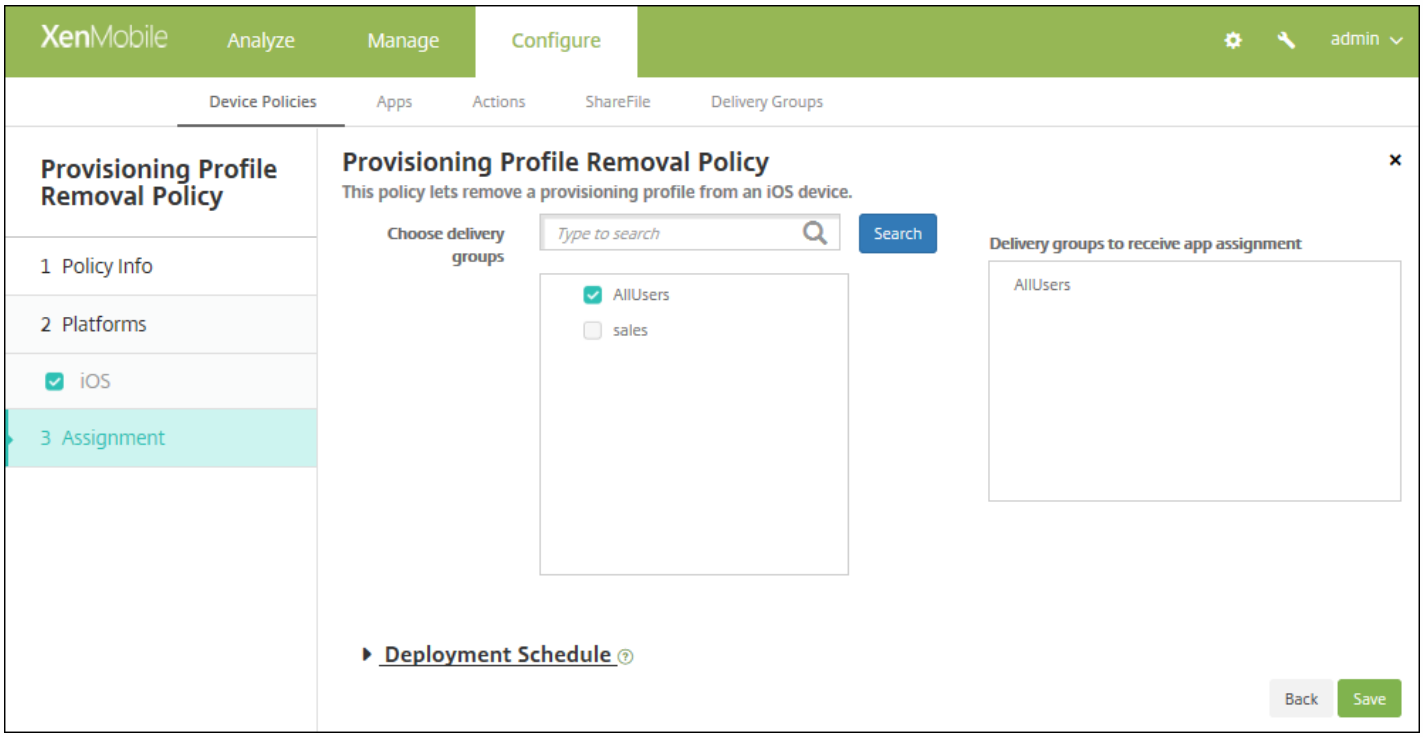


6. Configure these settings:

- **iOS provisioning profile**: In the list, click the provisioning profile you want to remove.
- **Comment**: Optionally, add a comment.

7. Configure the deployment rules

8. Click **Next**. The **Provisioning Profile Removal 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**.

Proxy device policy

Nov 16, 2016

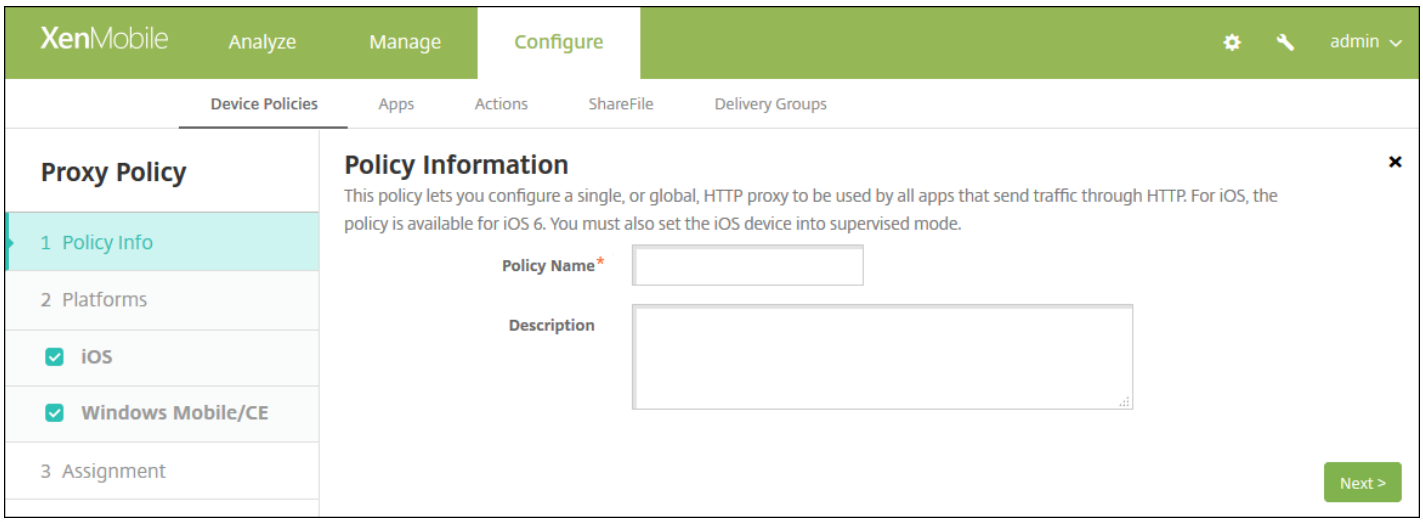
You can add a device policy in XenMobile to specify global HTTP proxy settings for devices running Windows Mobile/CE andiOS 6.0 or later. You can deploy only one global HTTP proxy policy per device.

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:

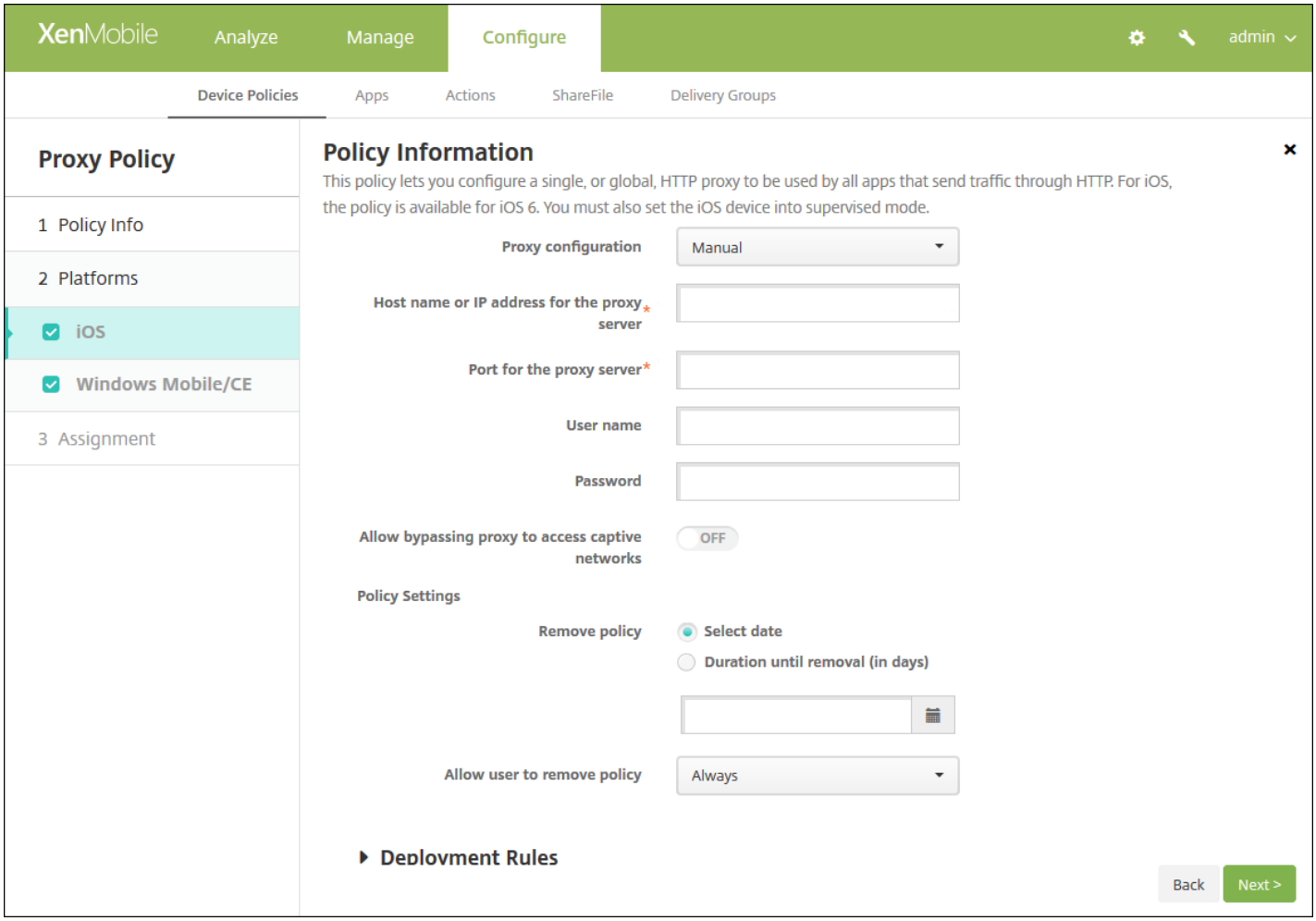
- **Policy Name**: Enter a descriptive name for the policy.
- **Description**: Optionally, enter a description of the policy.

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.

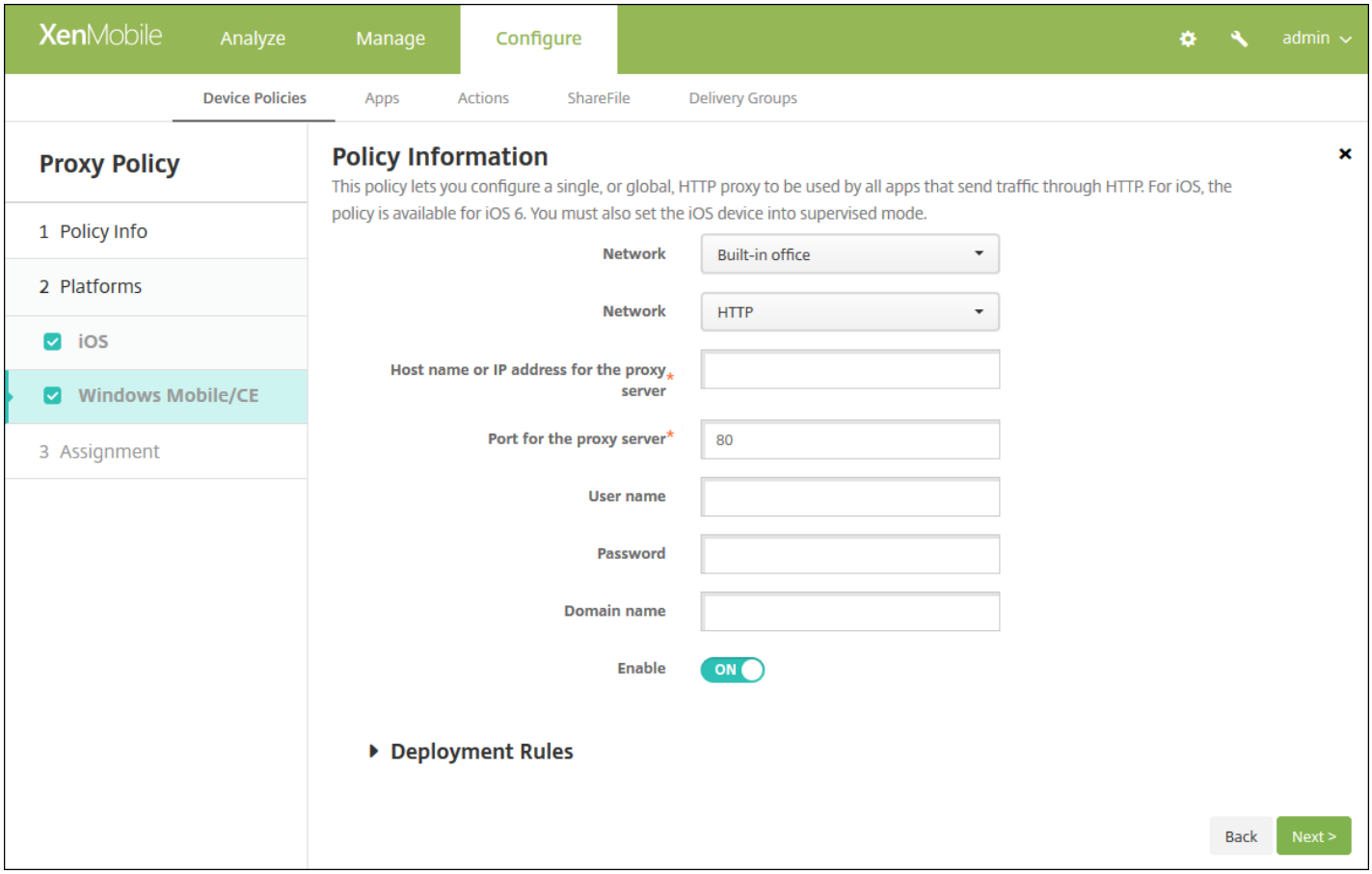
Configure iOS settings



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 days)**.
  - 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

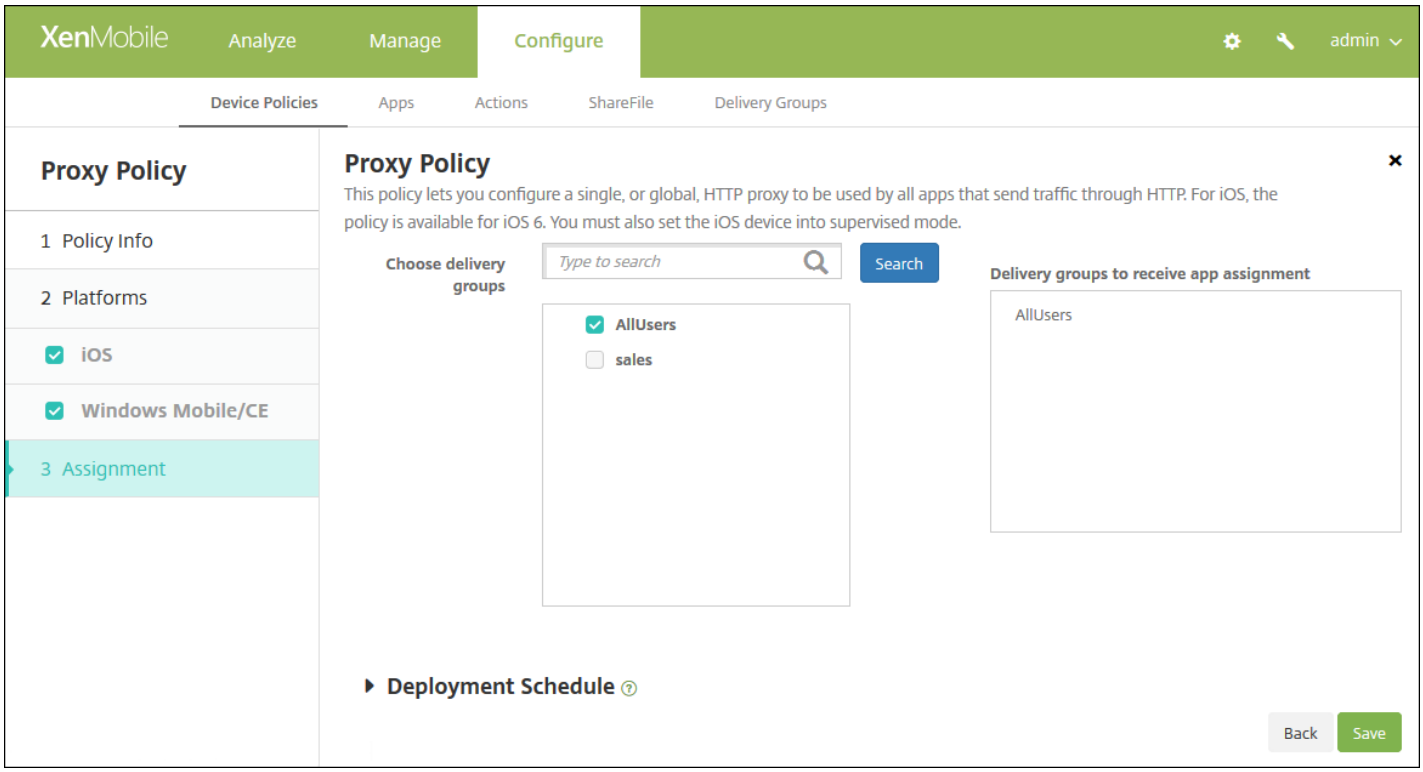


Configure these settings:

- **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

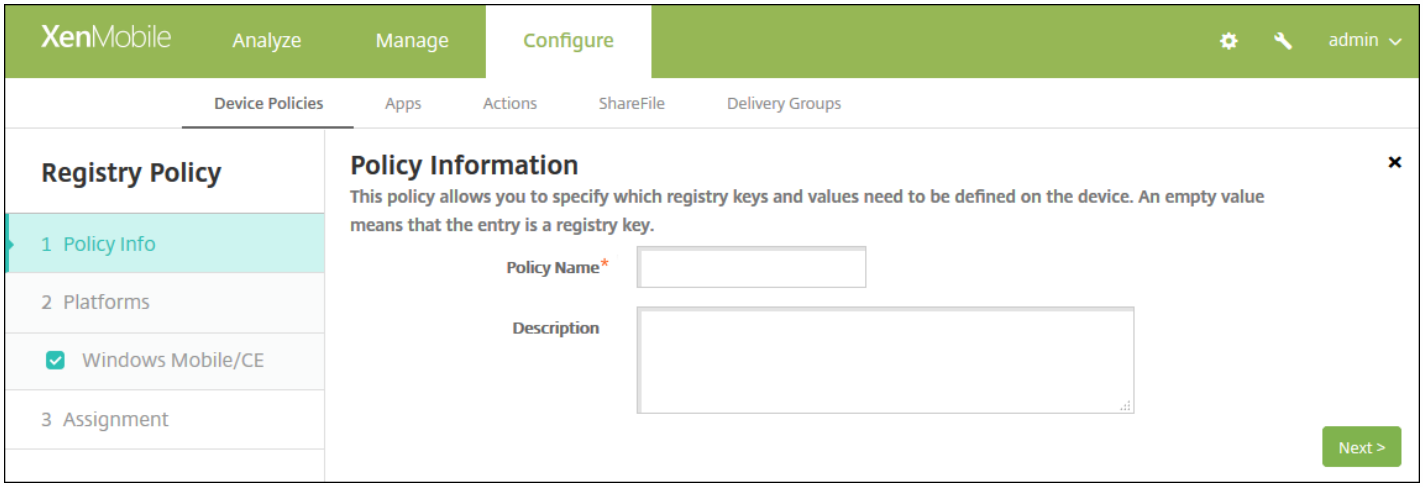
Nov 16, 2016

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.

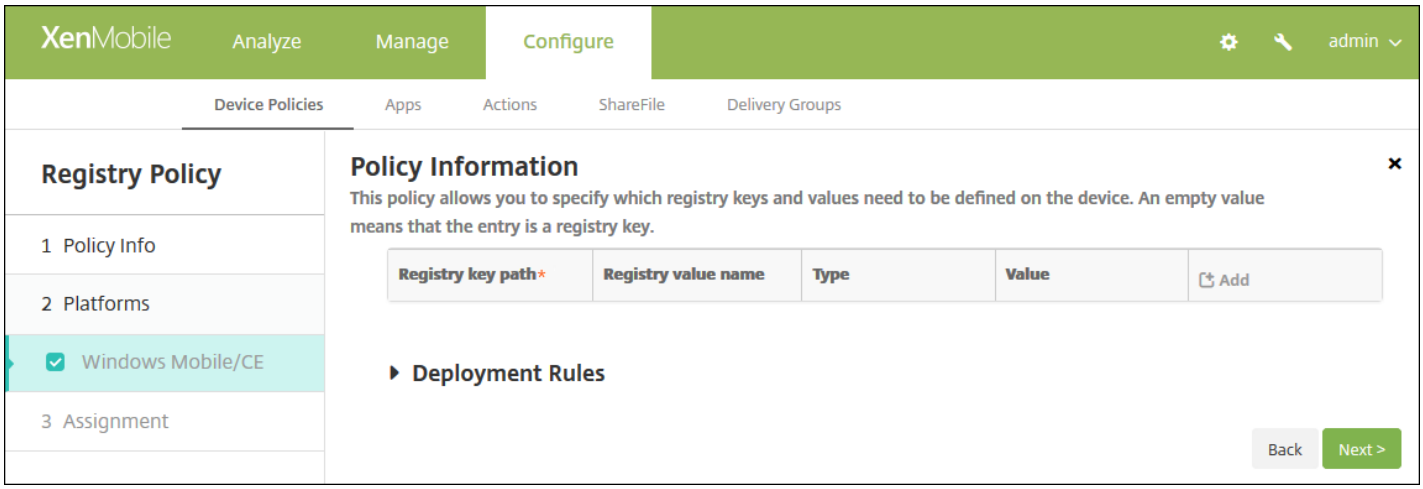
3. Expand **More** and then, under **Custom**, click **Registry**. The **Registry Policy** information page appears.



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:

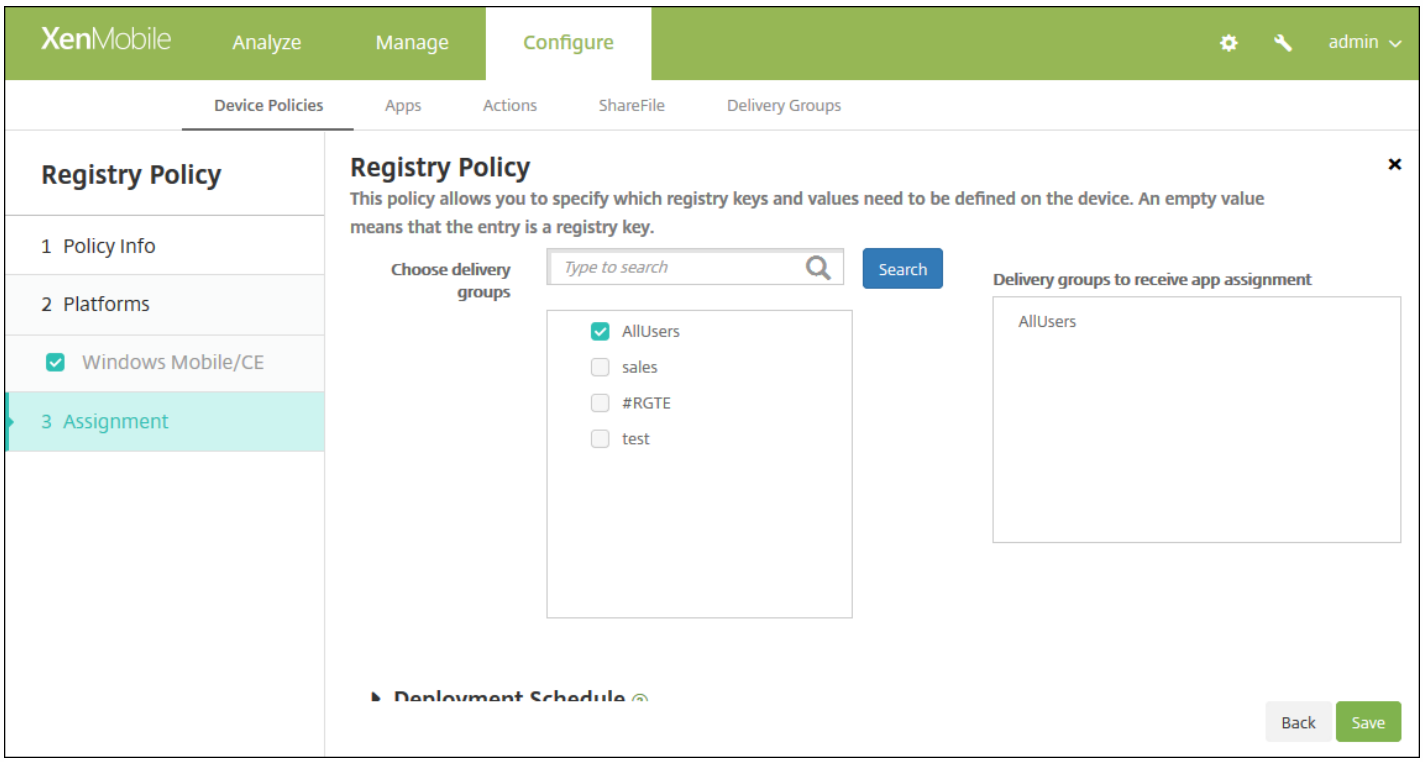
- For each registry key or registry key/value pair you want to add, click **Add** and do the following:
- **Registry key path**: Type the full path for the registry key. For example, type *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows* to specify the route to the Windows key from the HKEY_LOCAL_MACHINE 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 the deployment rules

8. Click **Next**. The **Registry 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**.

Remote support device policy

Nov 16, 2016

You create a remote support policy in XenMobile to give you remote access to users' Samsung KNOX 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.

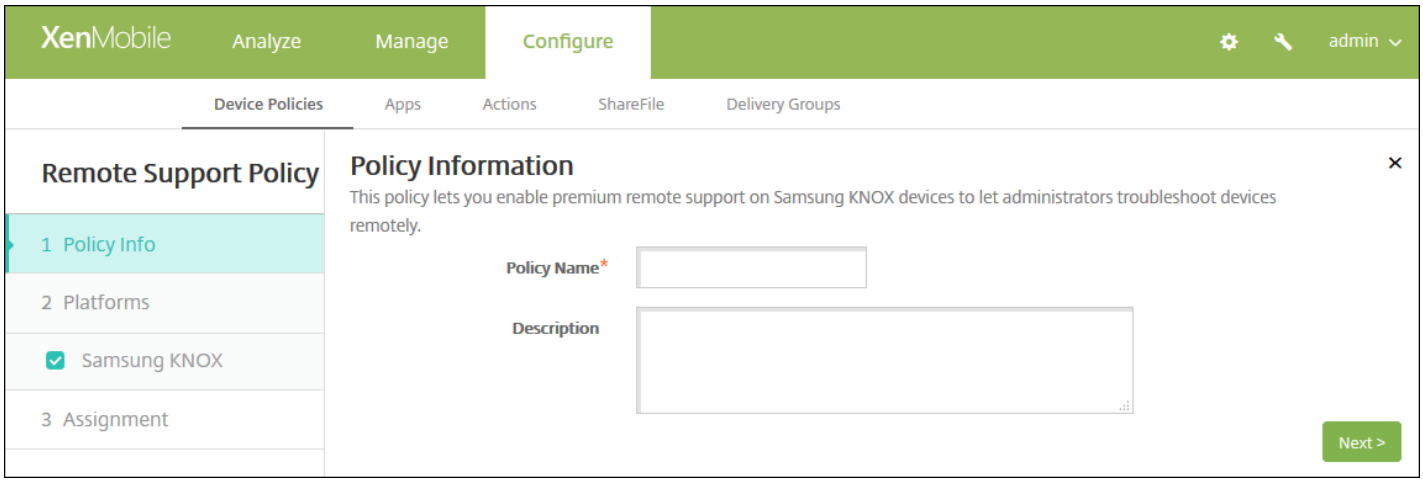
Note: To implement this policy, you must do the following:

- 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 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.

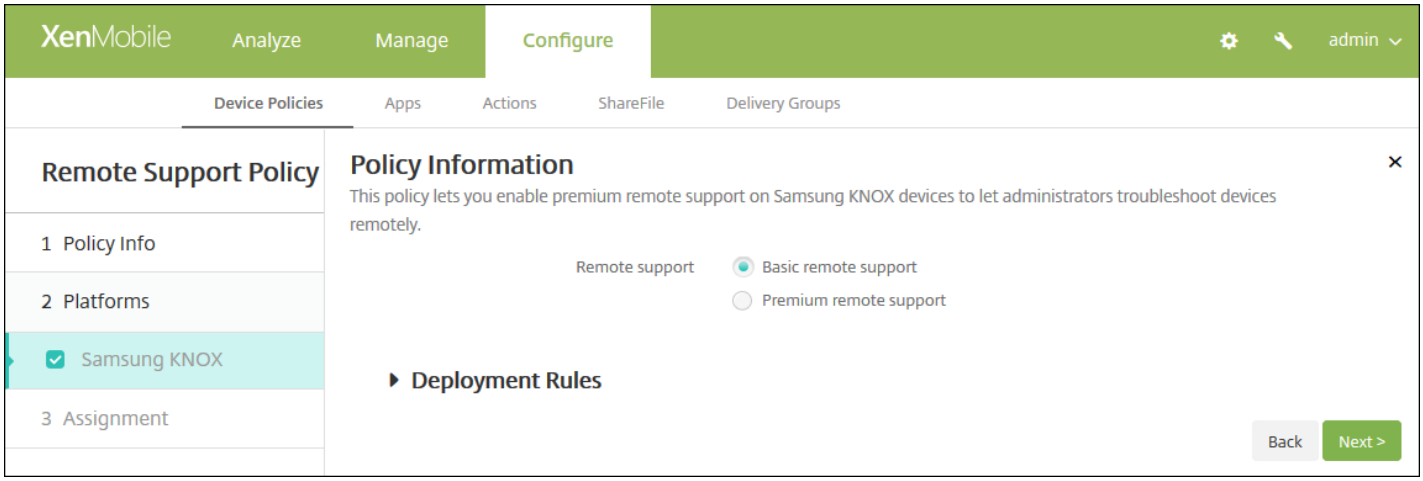
3. Expand **More** and then, under **Network access**, click **Remote Support**. The **Remote Support Policy** page appears.



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.

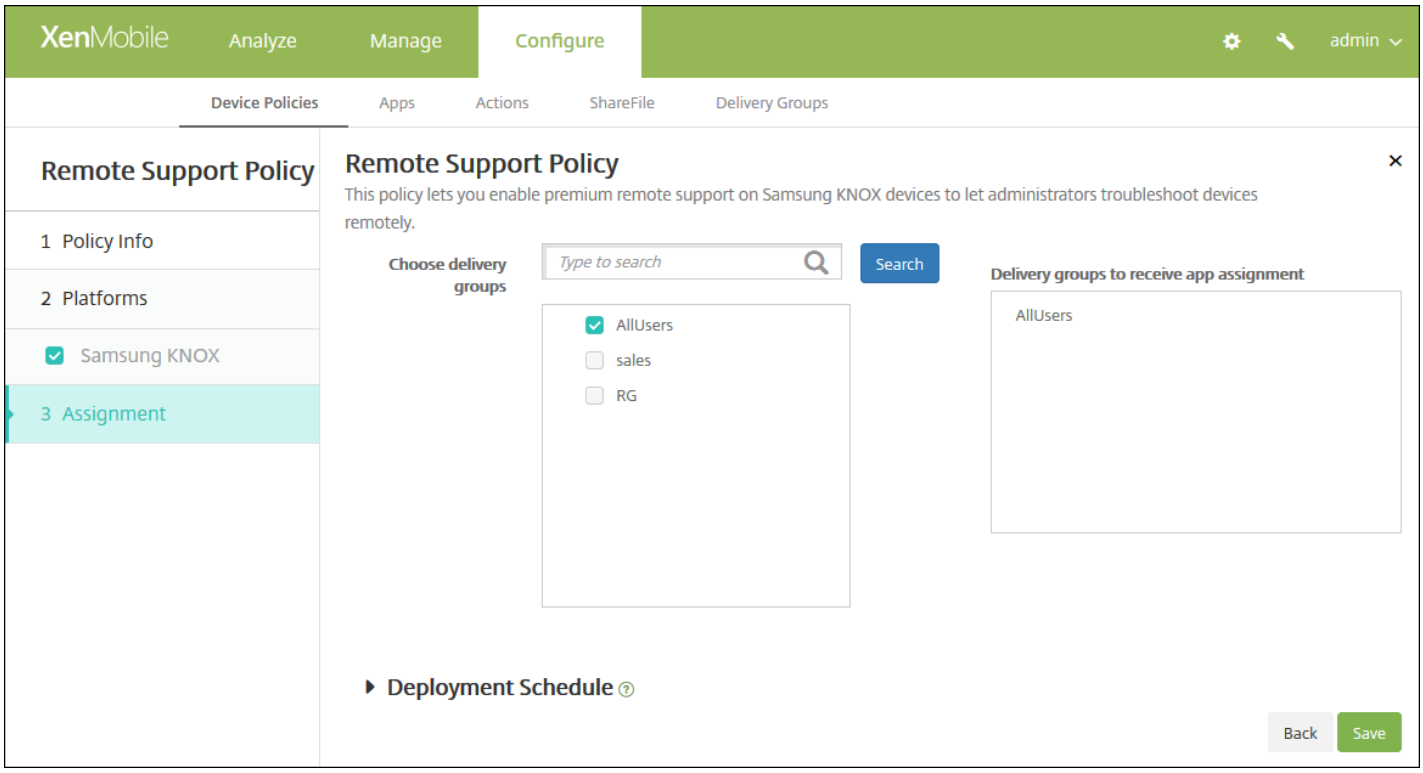


6. Configure this setting:

- **Remote support**: Select **Basic remote support** or **Premium remote support**. The default is **Basic remote support**.

7. Configure the deployment rules

8. Click **Next**. The **Remote Support 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**.

Restrictions device policy

Jan 06, 2017

You can add a device policy in XenMobile to restrict certain features or functionality on users' devices, phones, tablets, and so on. You can configure the device restriction policy for the following platforms: iOS, Mac OS X, Samsung SAFE, Samsung KNOX, Windows tablets, Windows Phone, Amazon, and Windows Mobile/CE. Each platform requires a different set of values, which are described in this article.

This device 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 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

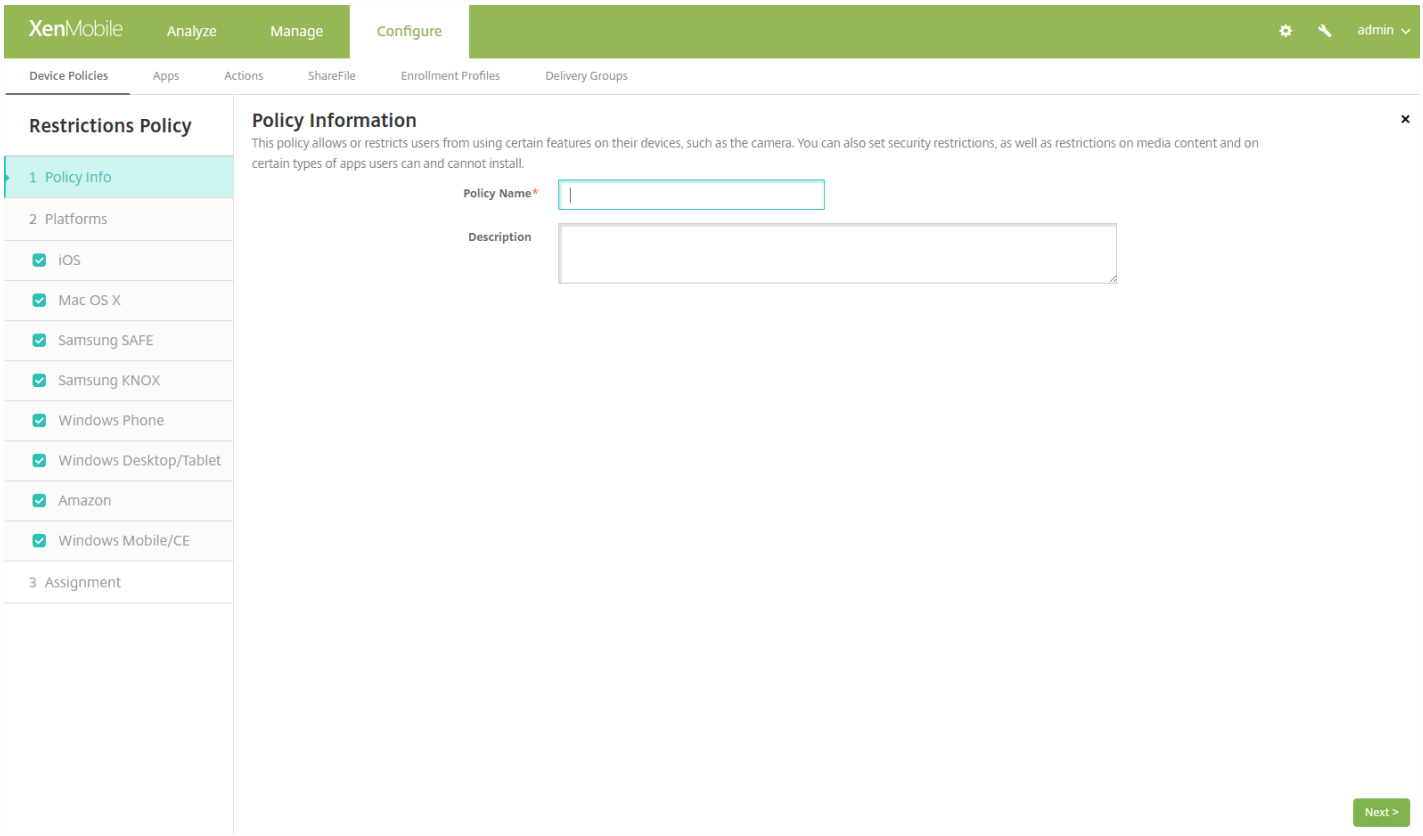
perform the operation or use the feature. For example:

- **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.

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.

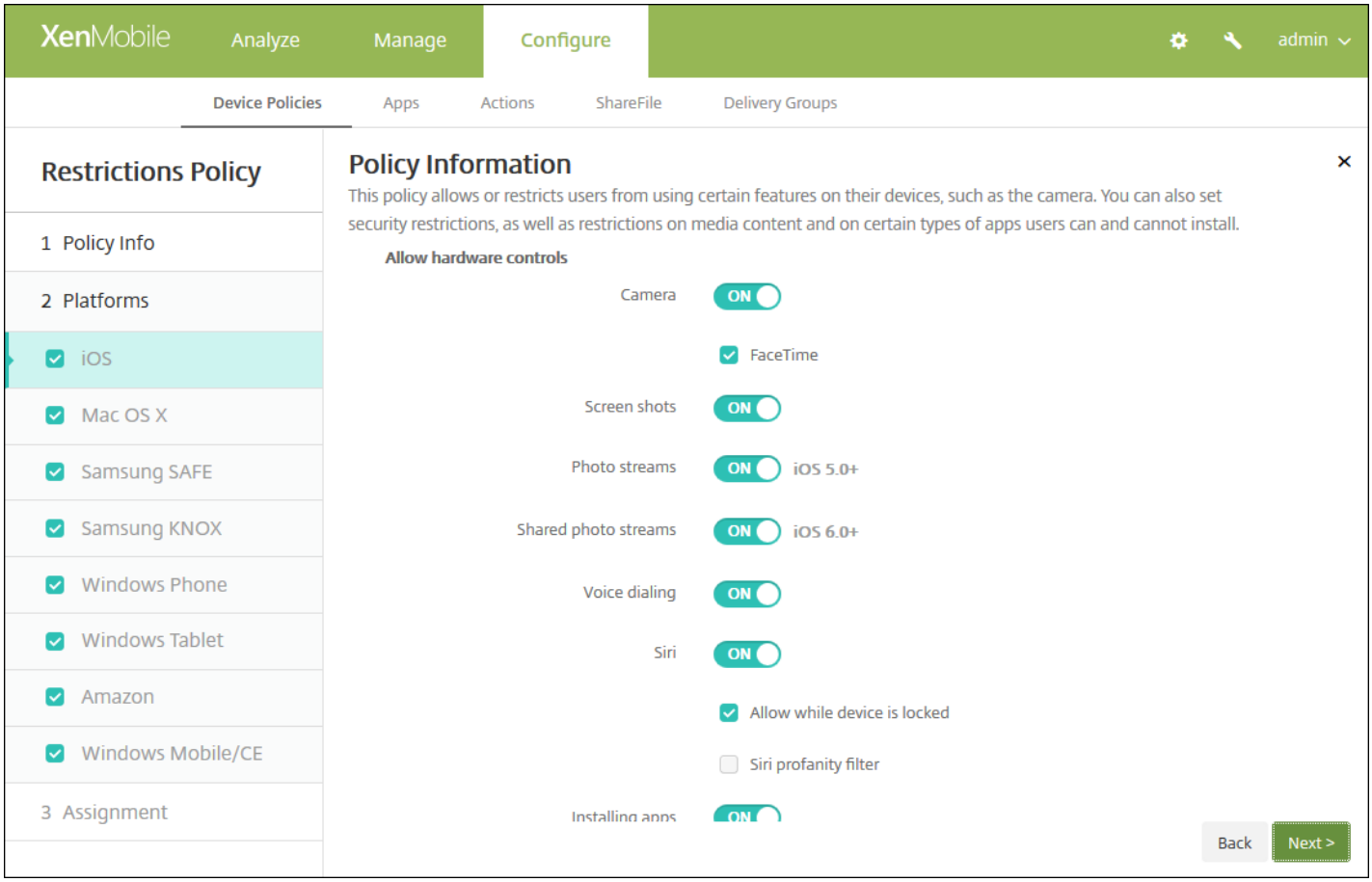
5. Under **Platforms**, select the platform or platforms you want to add. You can then change the policy information for each platform you selected. Click to restrict any of the features in the following sections, which changes the setting to **OFF**. Unless otherwise noted, the default setting is to enable the feature.

If you selected:

iOS, configure these settings
Mac OS X, configure these settings
Samsung SAFE, configure these settings
Samsung KNOX, configure these settings
Windows Phone, configure these settings
Windows Tablet, configure these settings
Amazon, configure these settings
Windows Mobile/CE, configure these settings

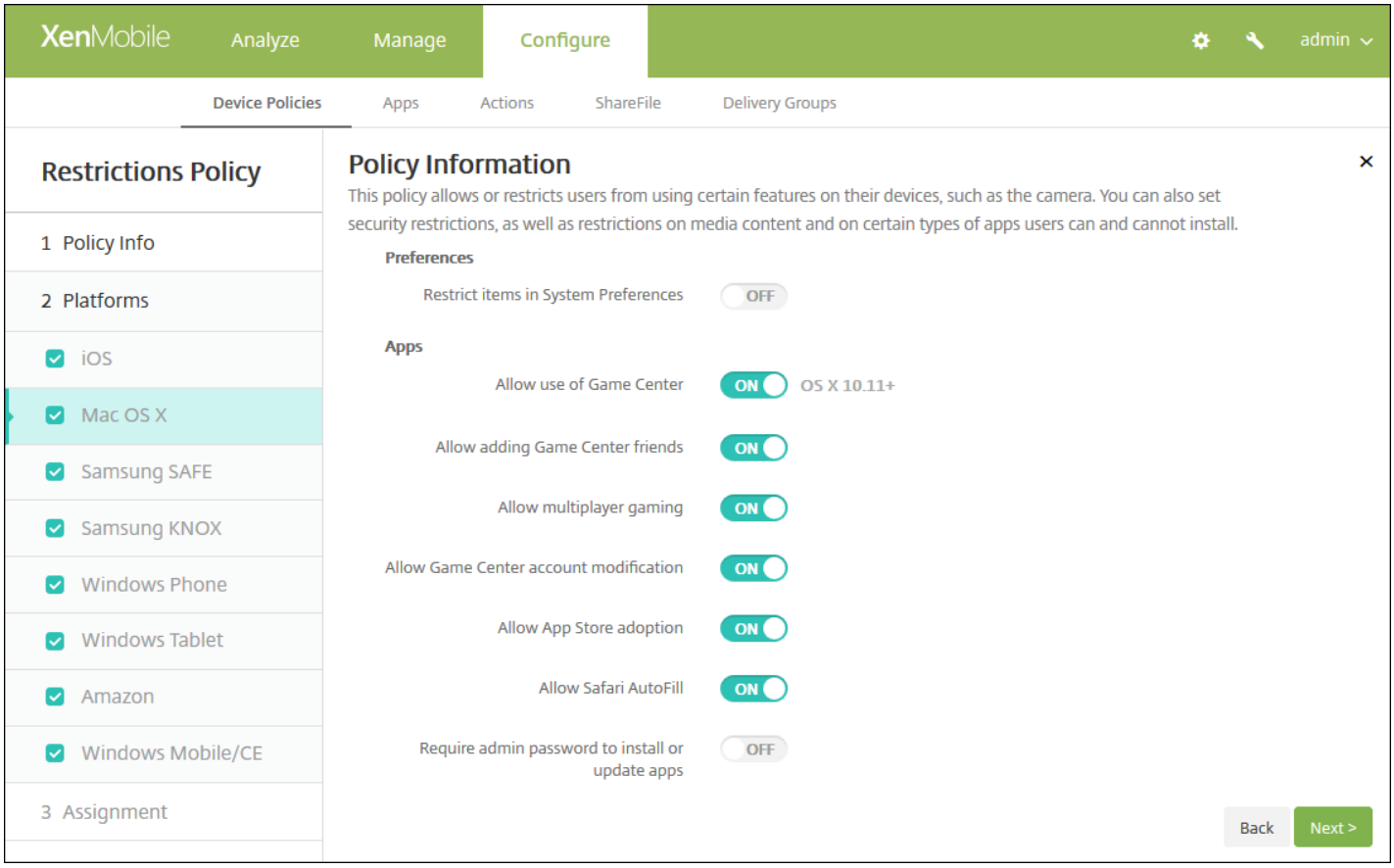
When you finish setting the restrictions for a platform, refer to Step 7 later in this article for how to set that platform's deployment rules.

If you selected iOS, configure these settings



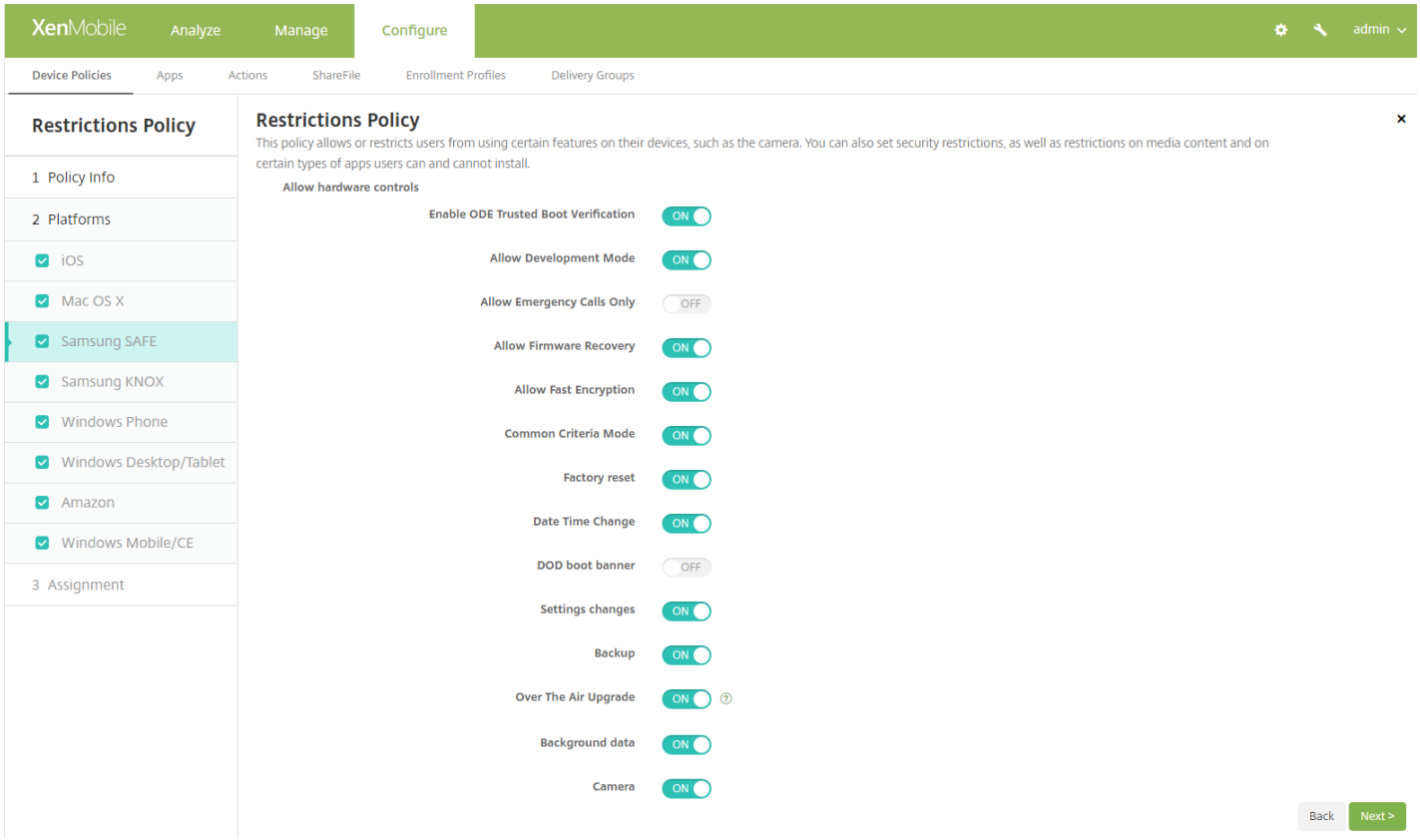
iOS settings

Configure Mac OS X settings



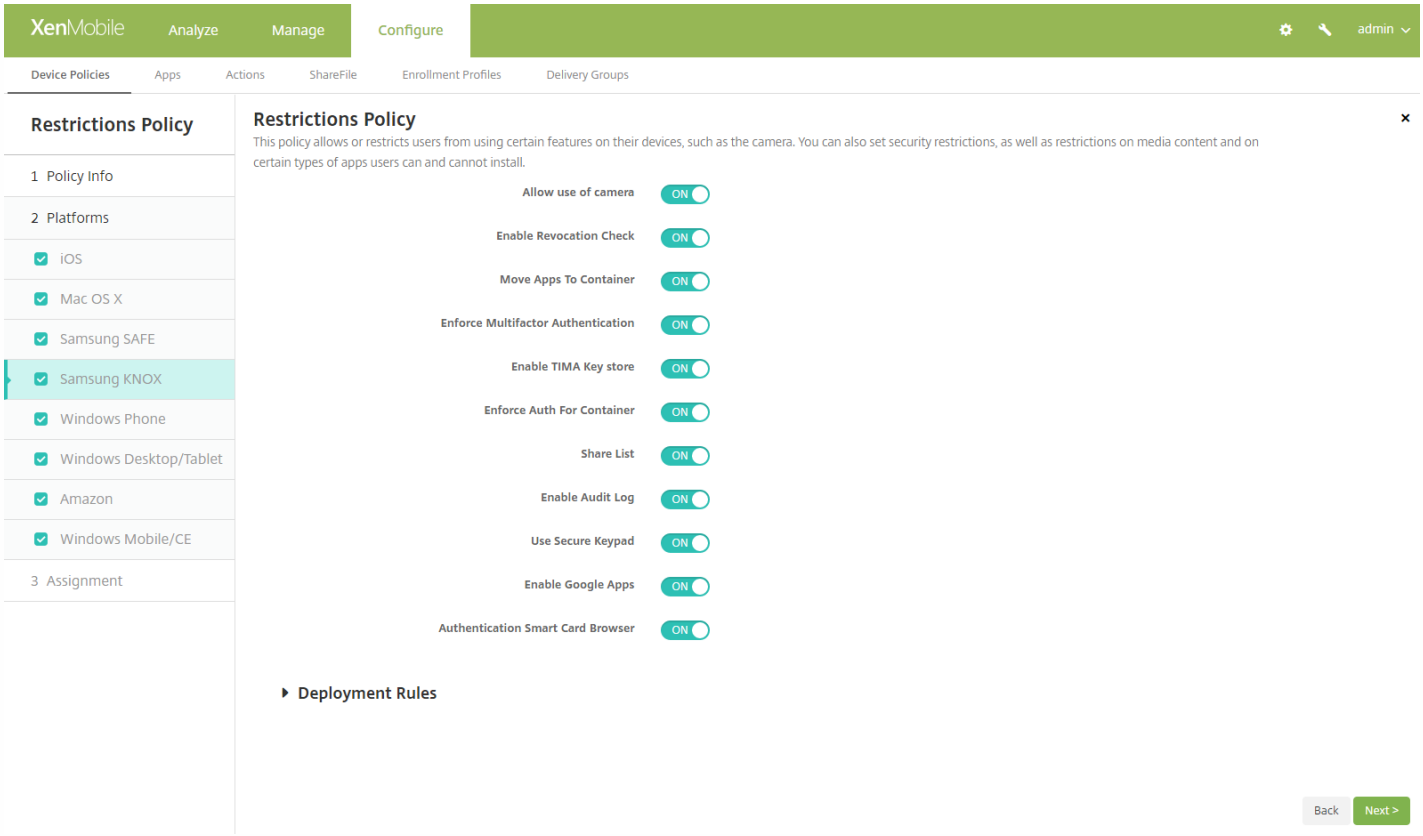
Mac OS X settings

Configure Samsung SAFE settings



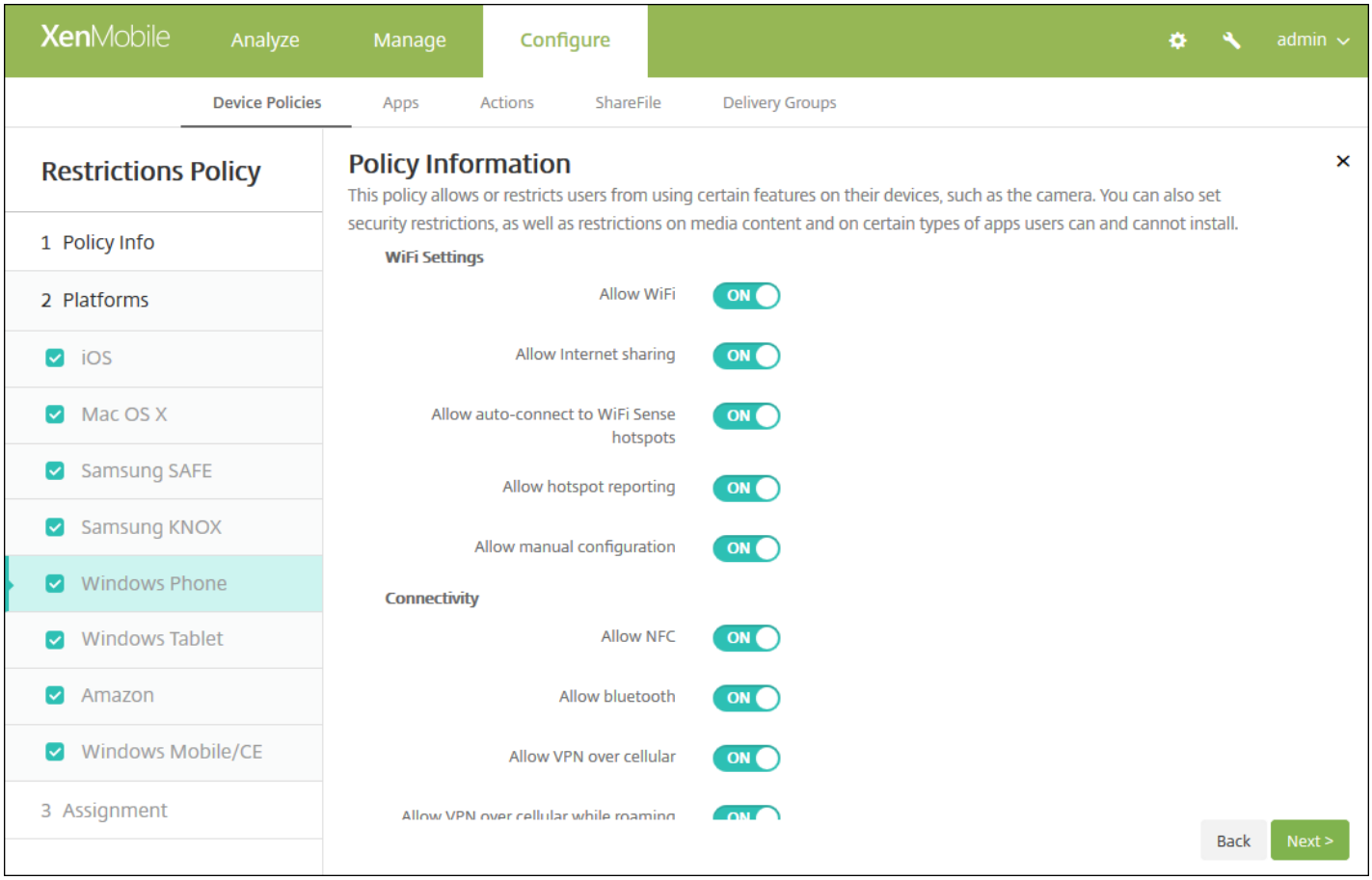
Samsung SAFE settings

Configure Samsung KNOX settings



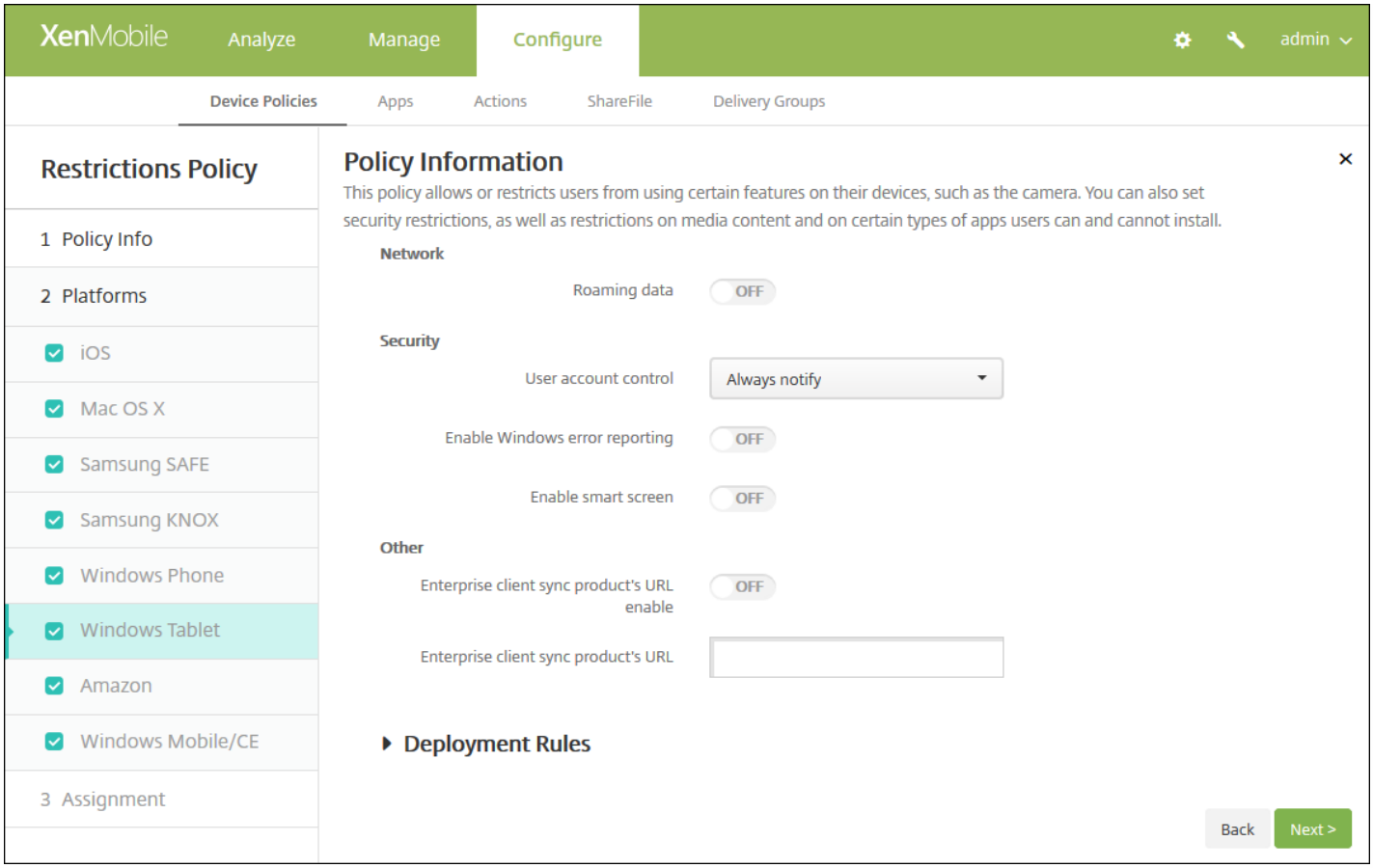
Samsung KNOX settings

Configure Windows Phone settings



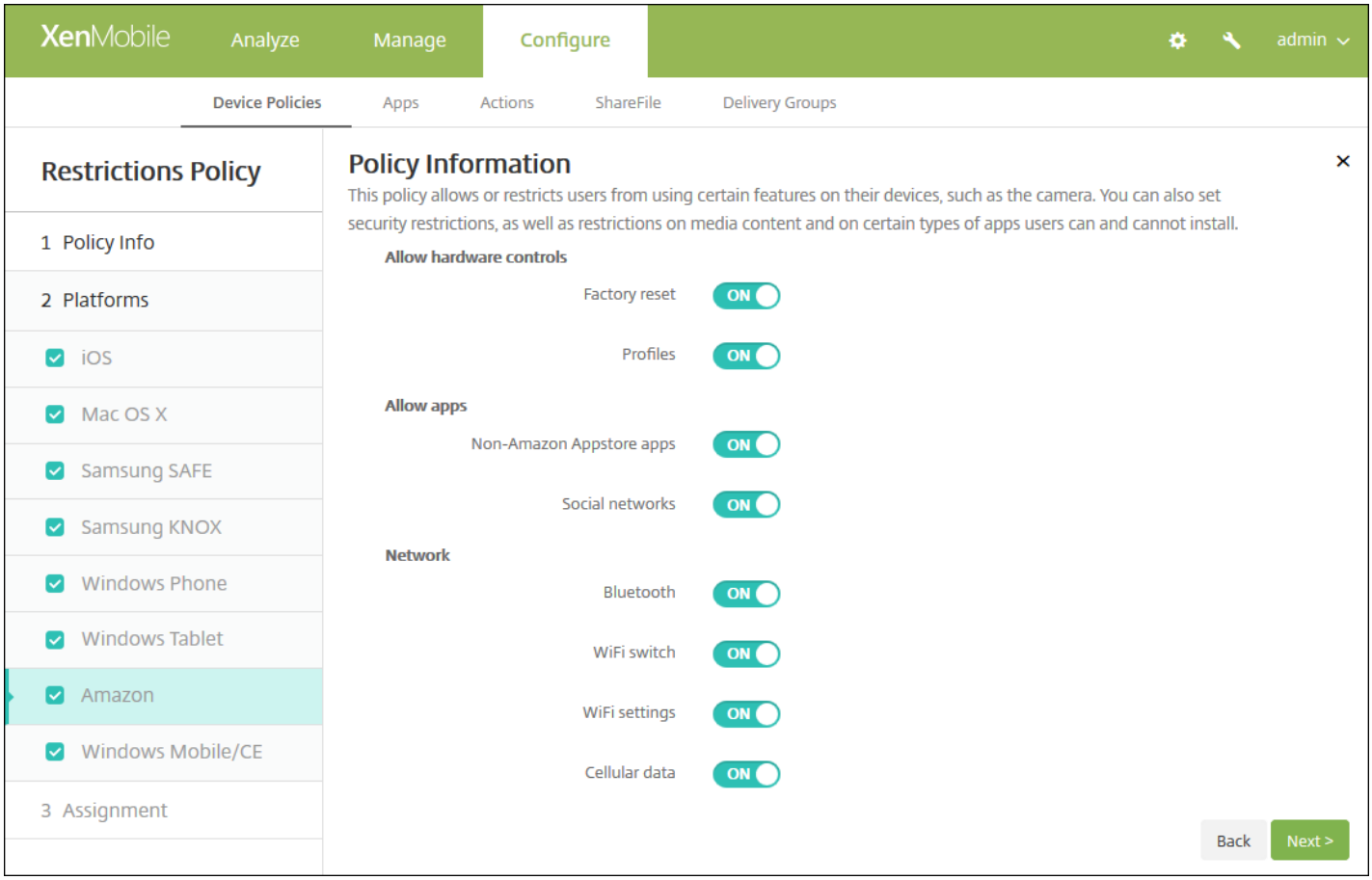
Windows Phone settings

Configure Windows Desktop/Tablet settings



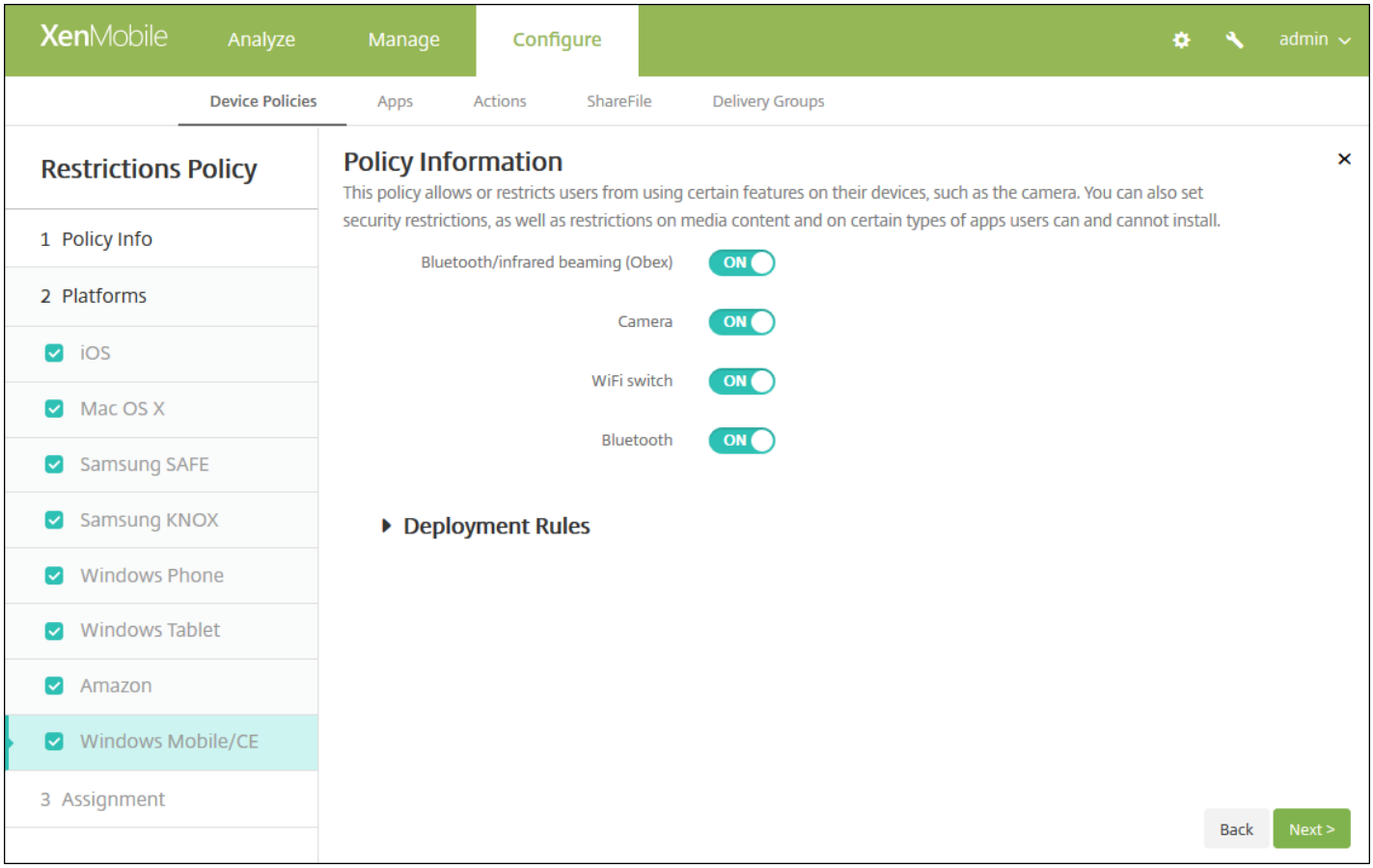
Windows Desktop/Tablet settings

Configure Amazon settings



Amazon settings

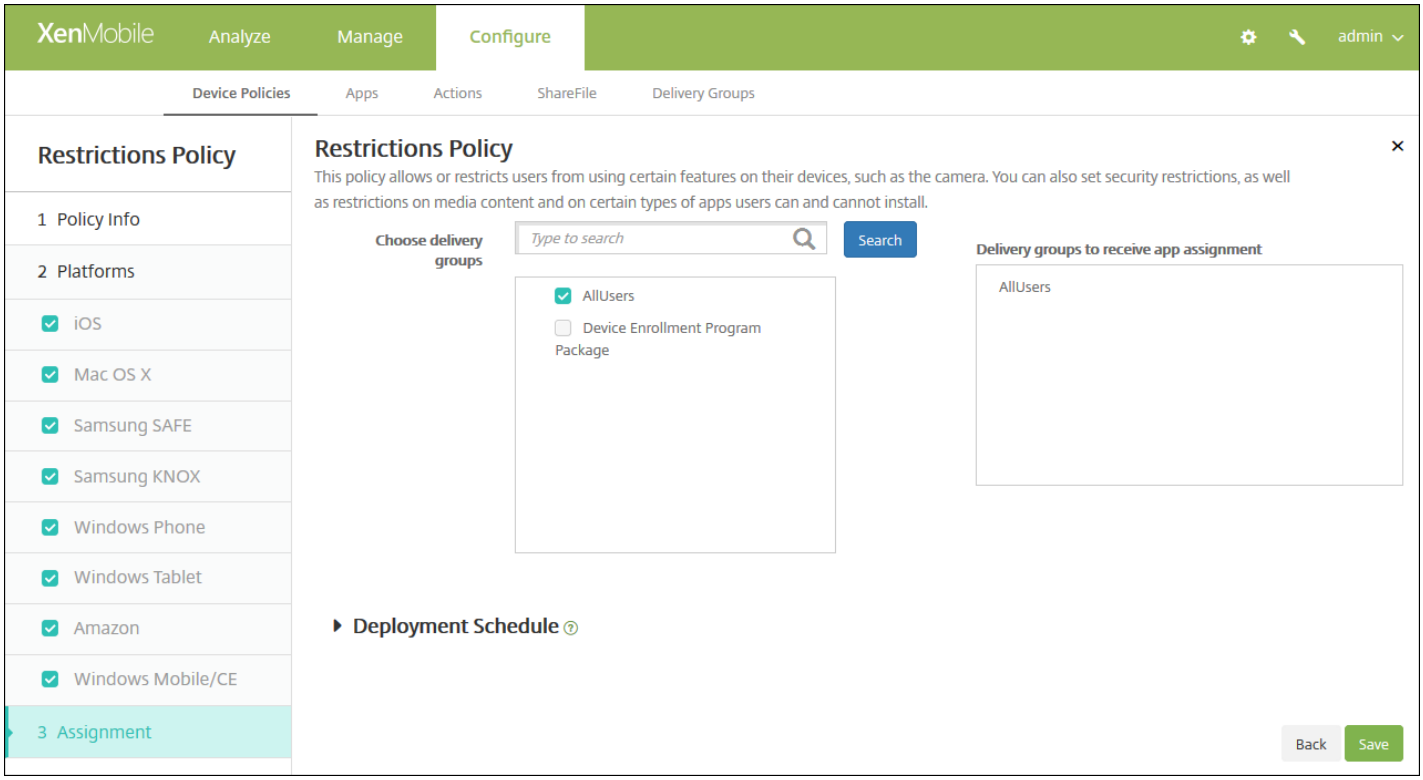
Configure Windows Mobile/CE settings



Windows Mobile/CE settings

7. Configure the deployment rules

8. Click **Next** and the **Restrictions Policy** assignment page appears.



9. 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.

10. Click **Save** to save the policy.

Roaming device policy

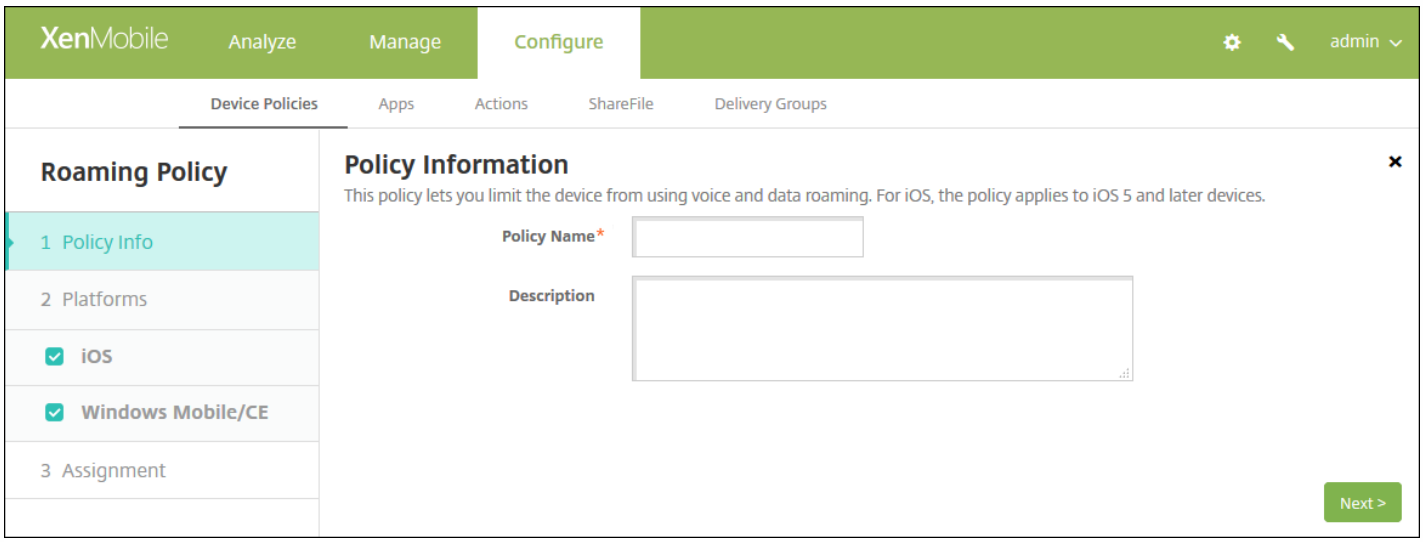
Nov 16, 2016

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:

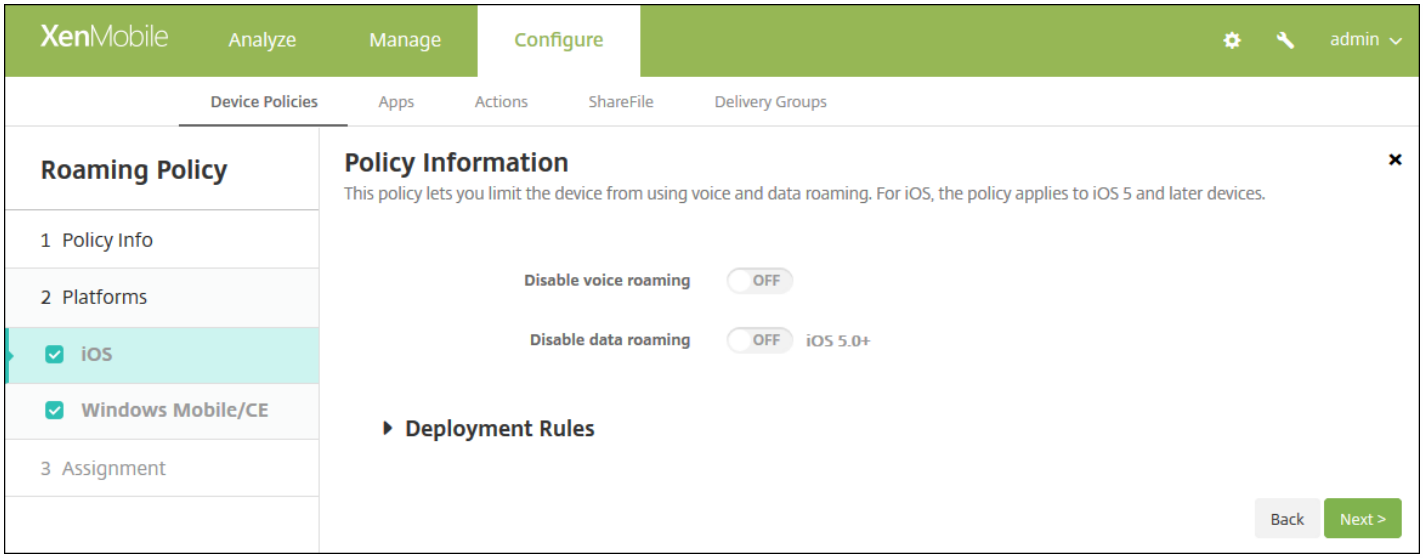
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

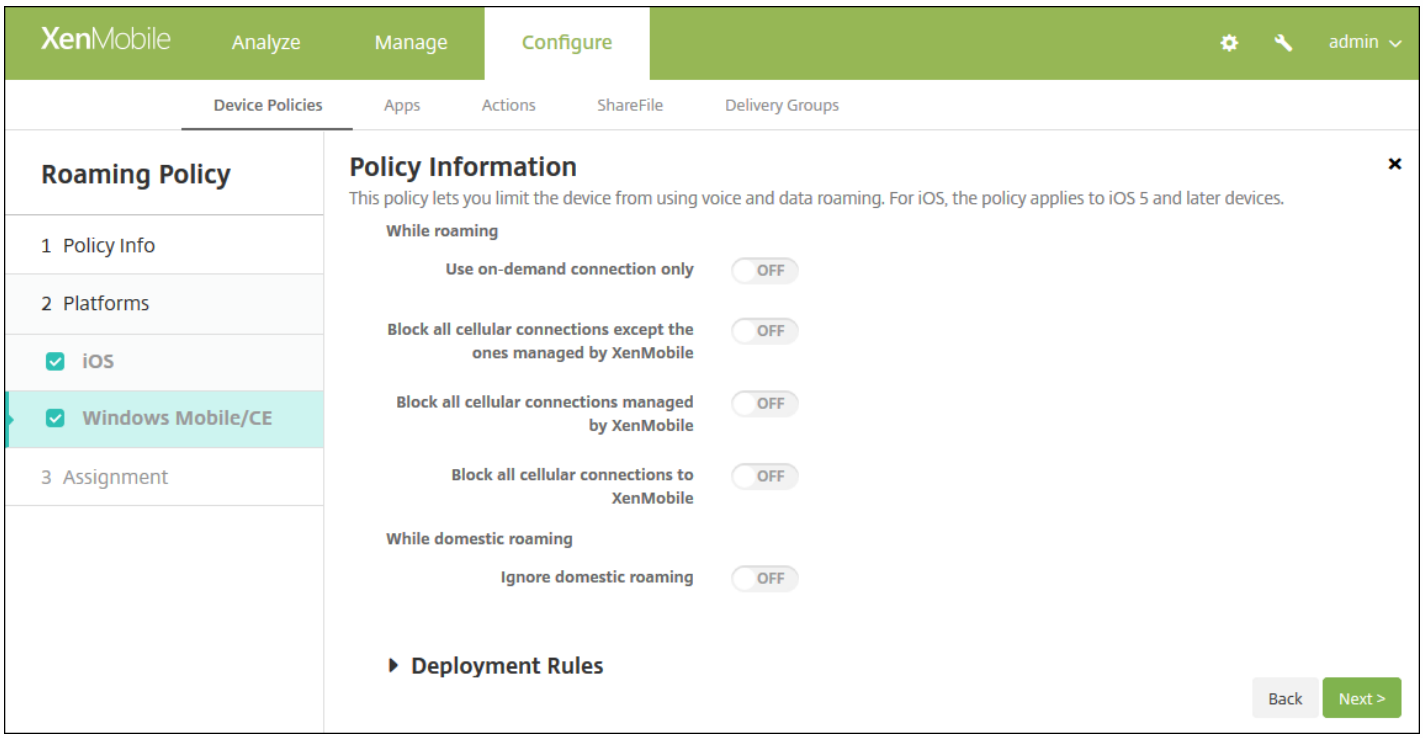
Configure iOS settings



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:

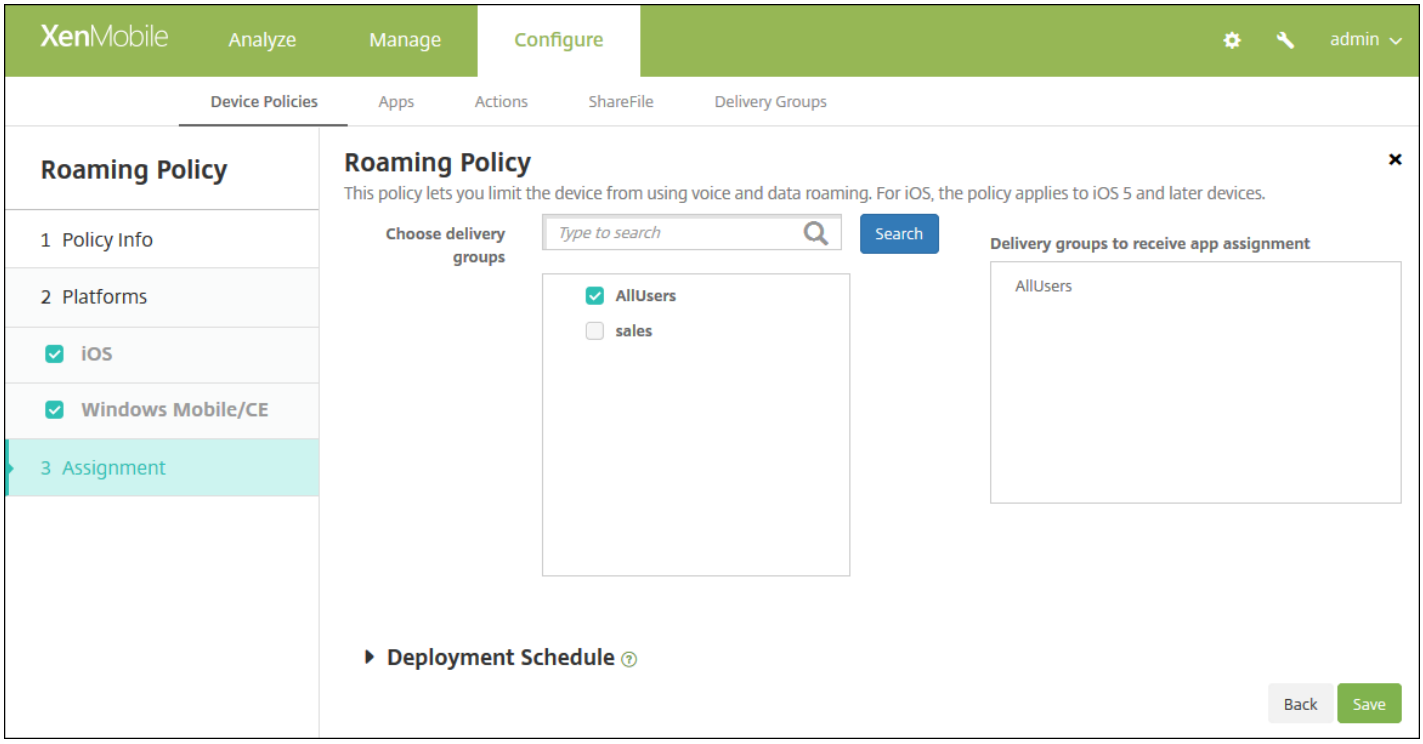
- **While roaming**

- **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 the deployment rules

8. Click **Next**. The **Roaming 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**.

Samsung MDM license key device policy

Jan 05, 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.

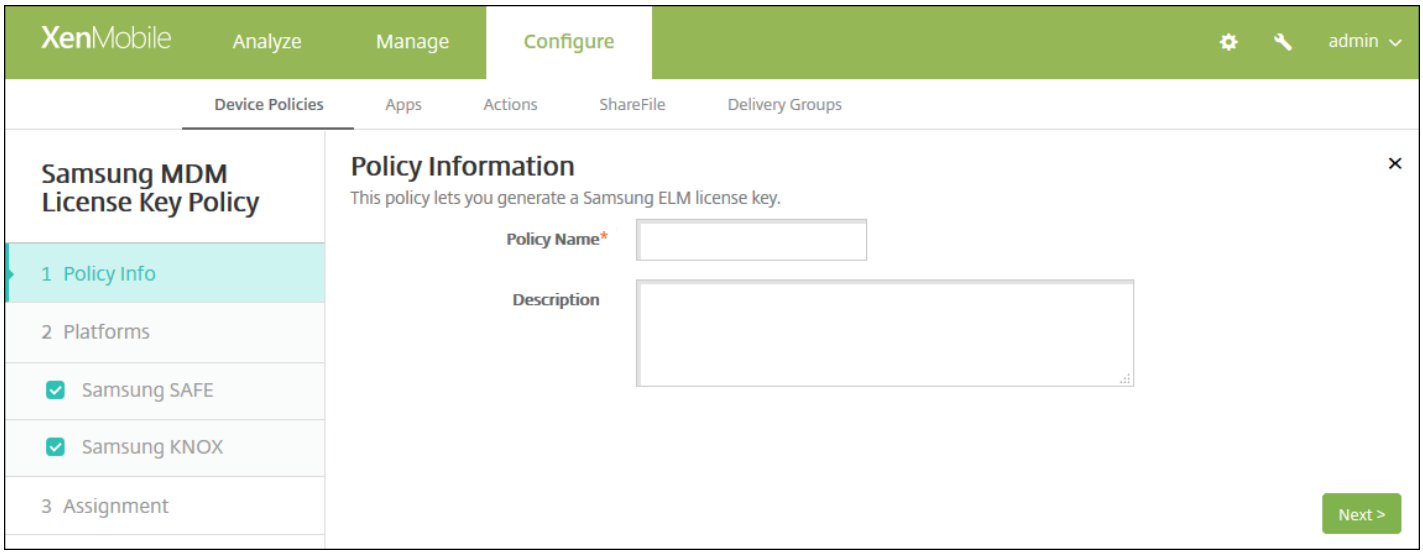
You must enable the SAFE APIs by deploying the built-in Samsung Enterprise License Management (ELM) key to a device before you can deploy SAFE policies and restrictions. To enable the Samsung KNOX API, you also need to purchase a Samsung KNOX Workspace license using the Samsung KNOX License Management 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:

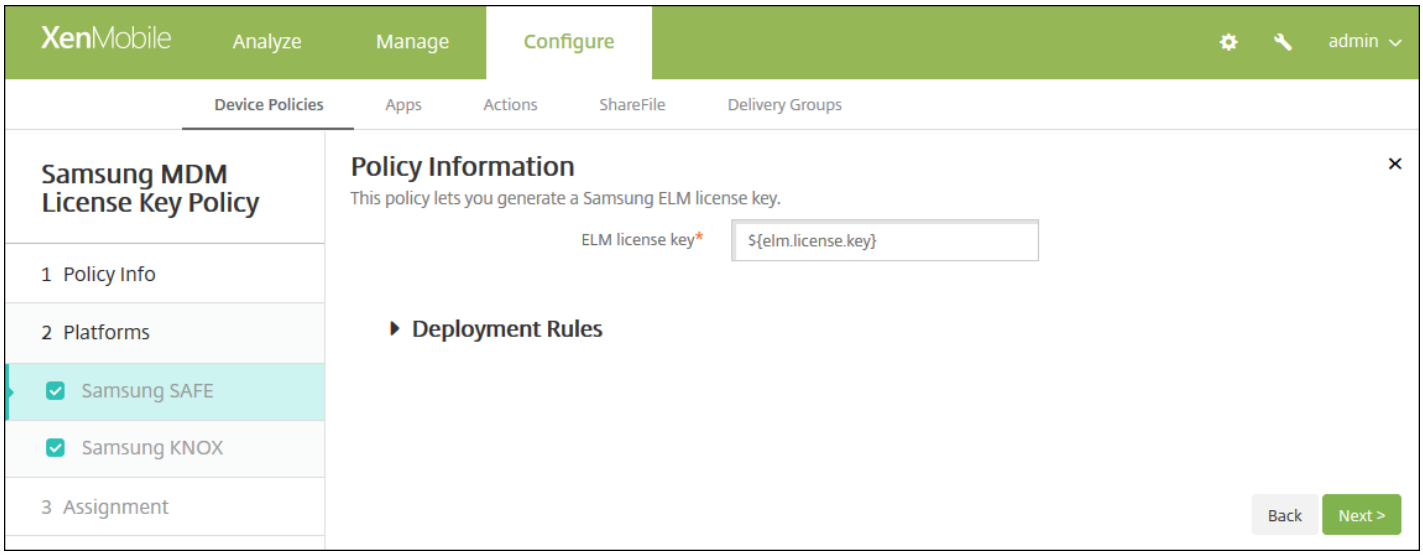
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

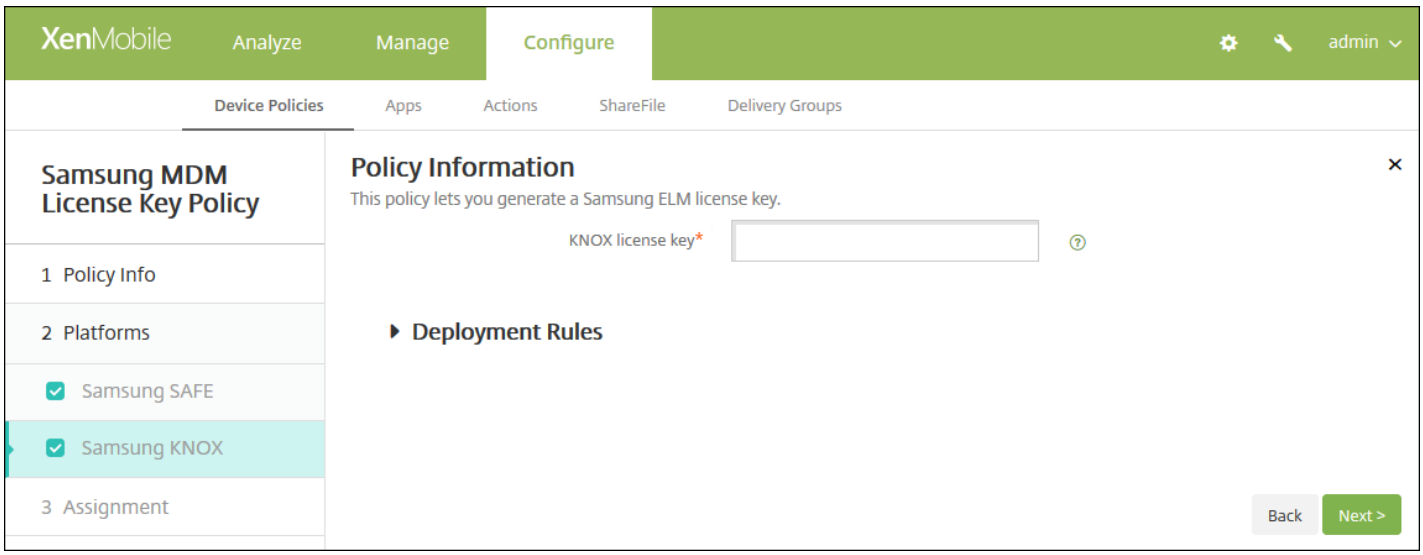
Configure Samsung SAFE settings



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

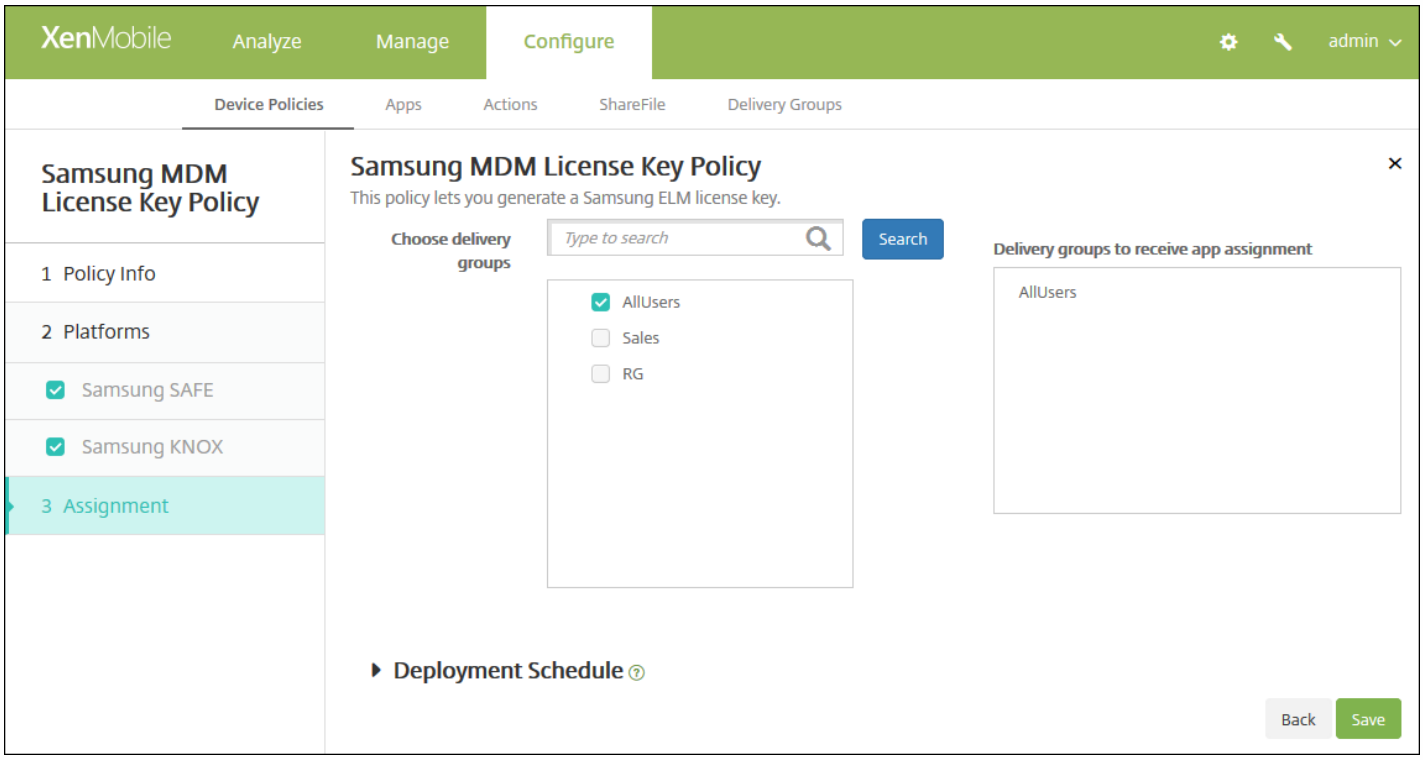


Configure this setting:

- **KNOX License key**: Type the KNOX license key that you obtained from Samsung.

7. Configure the deployment rules

8. Click **Next**. The **Samsung MDM License Key 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**.

Samsung SAFE firewall device policy

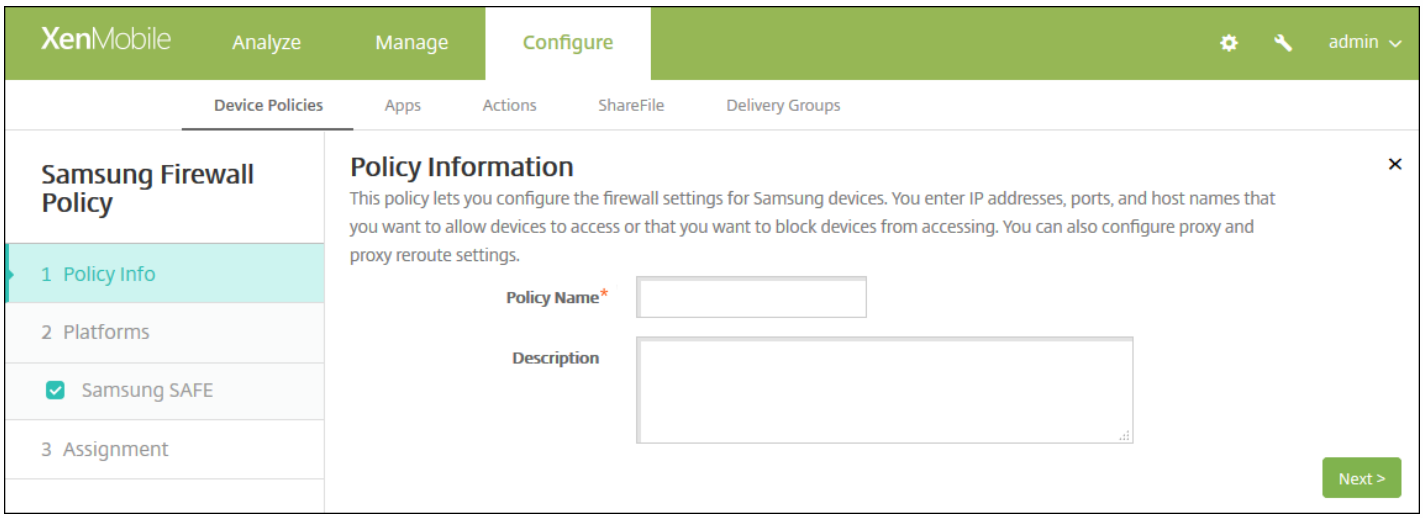
Nov 16, 2016

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.

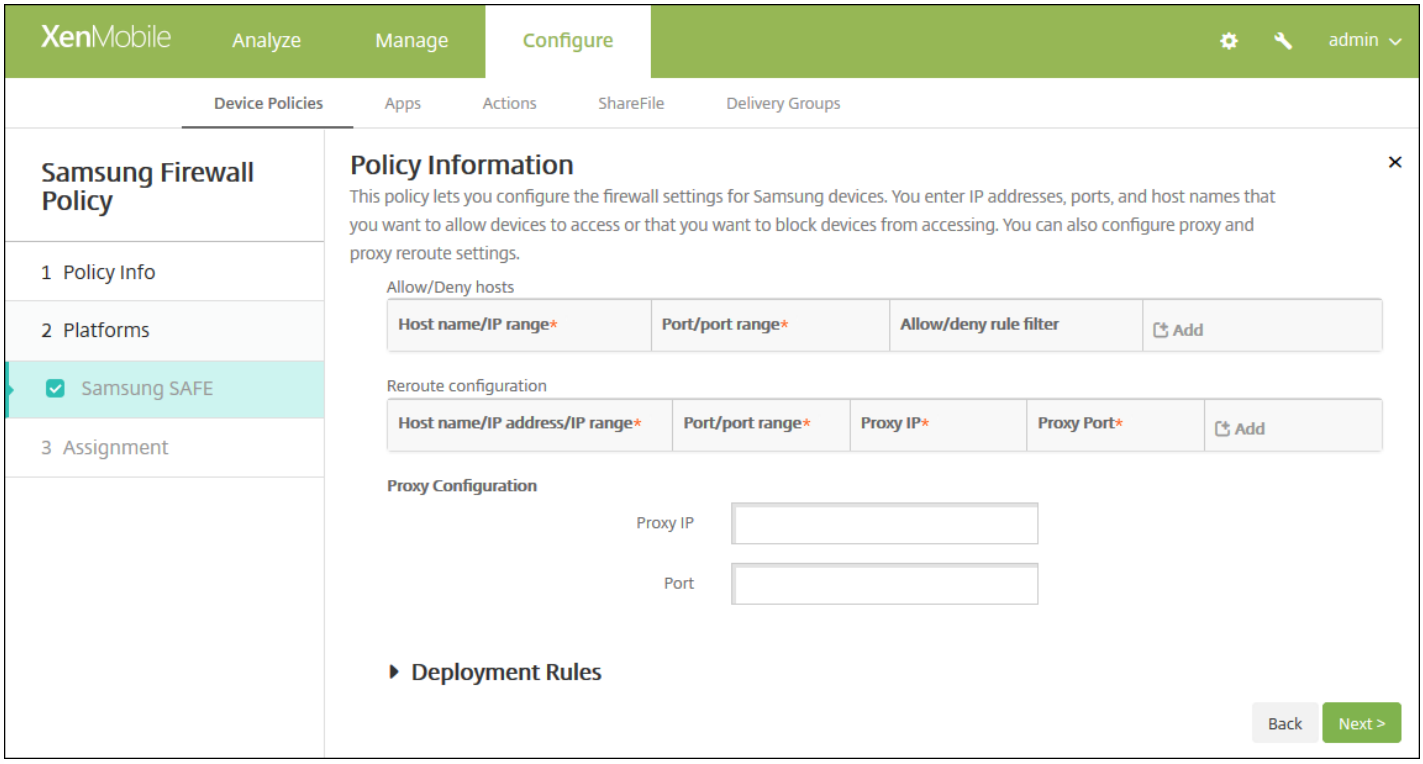
3. Expand **More** and then, under **Network access**, click **Samsung Firewall**. The **Samsung Firewall Policy** page appears.



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:

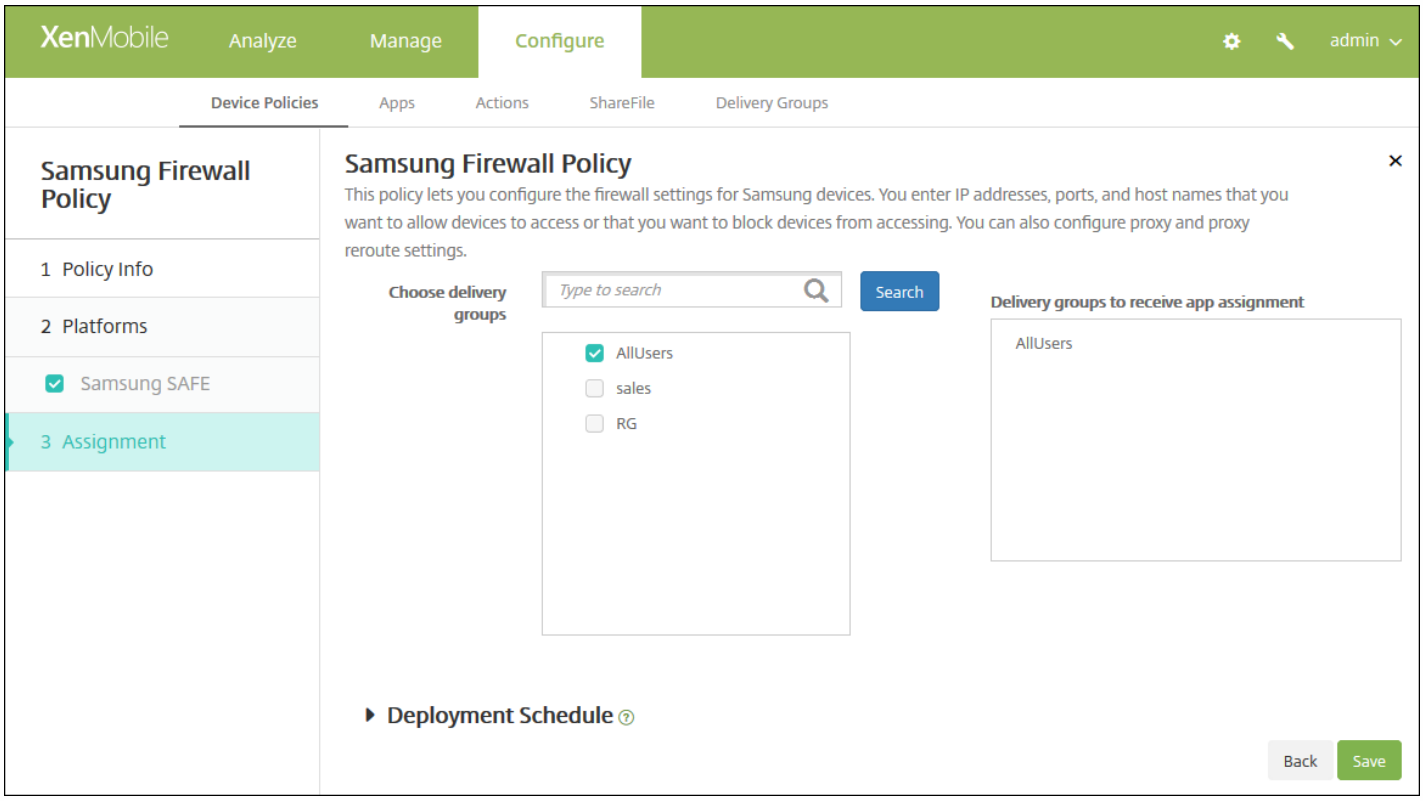
- **Allow/Deny hosts**
  - For each host to which you want to allow or deny access, click **Add** and do the following:
    - **Host name/IP range**: Type the host name or IP address range of the site you want to affect.
    - **Port/port range**: Type the port or port range.
    - **Allow/deny rule 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 the deployment rules

8. Click **Next**. The **Samsung Firewall 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**.

SCEP device policy

Nov 16, 2016

This policy allows you to configure iOS and Mac OS X 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.

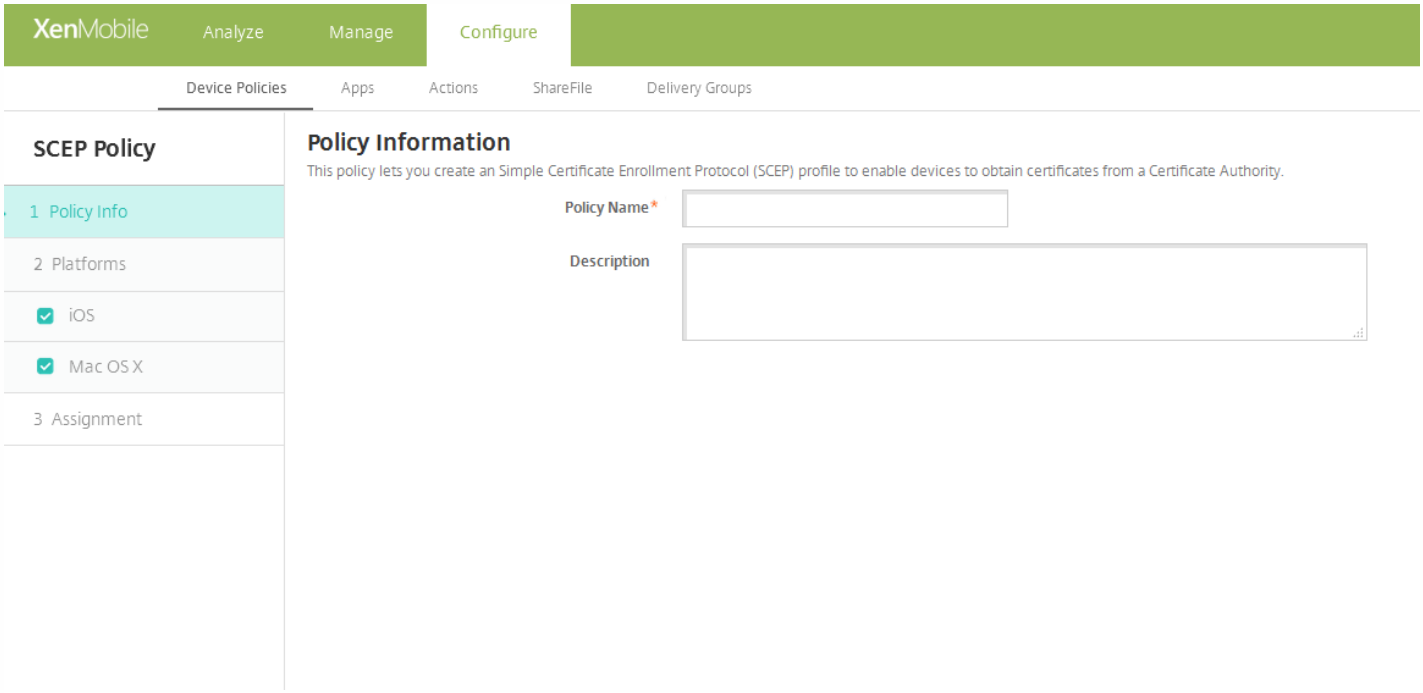
iOS settings

Mac OS X 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:

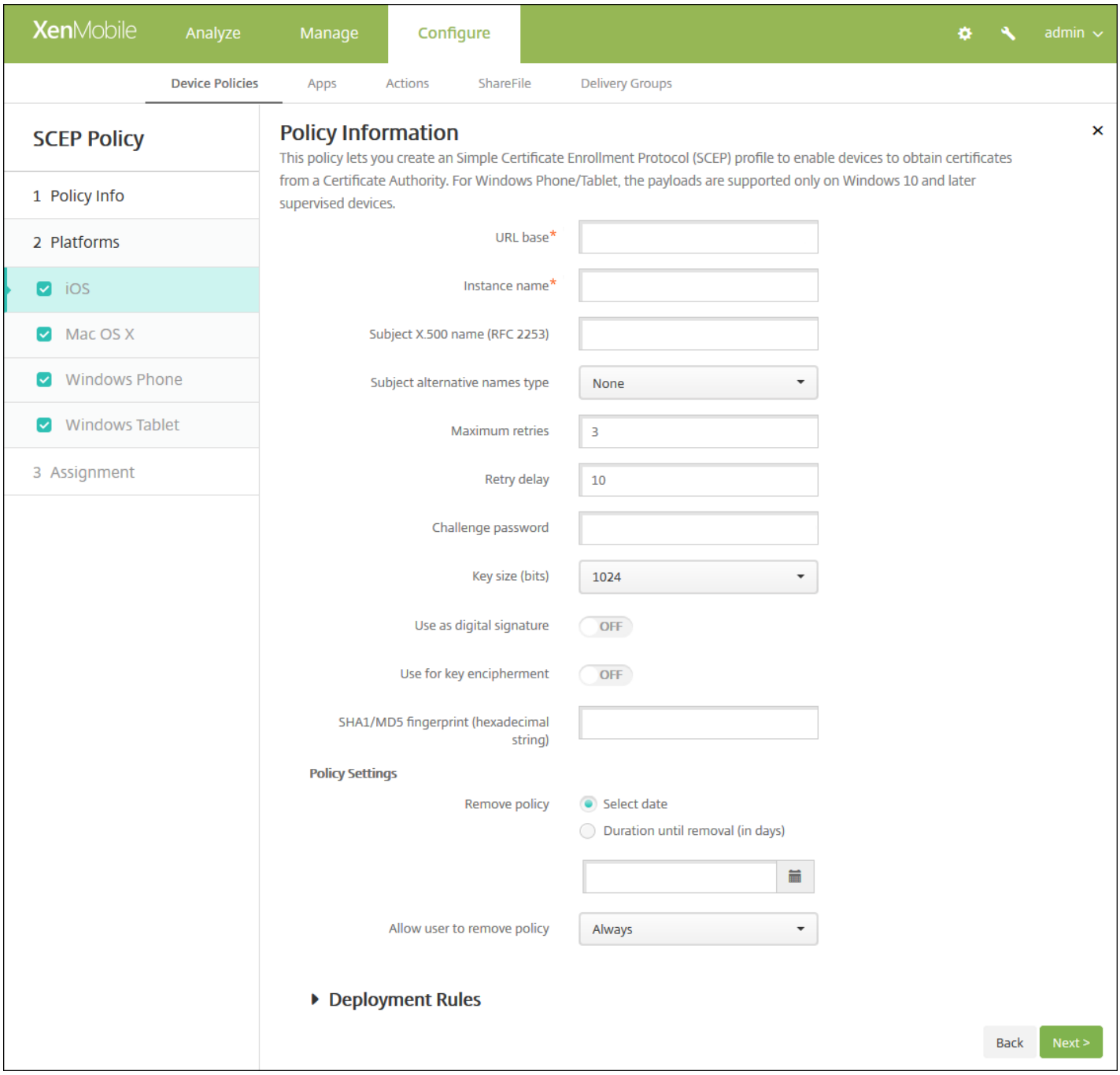
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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



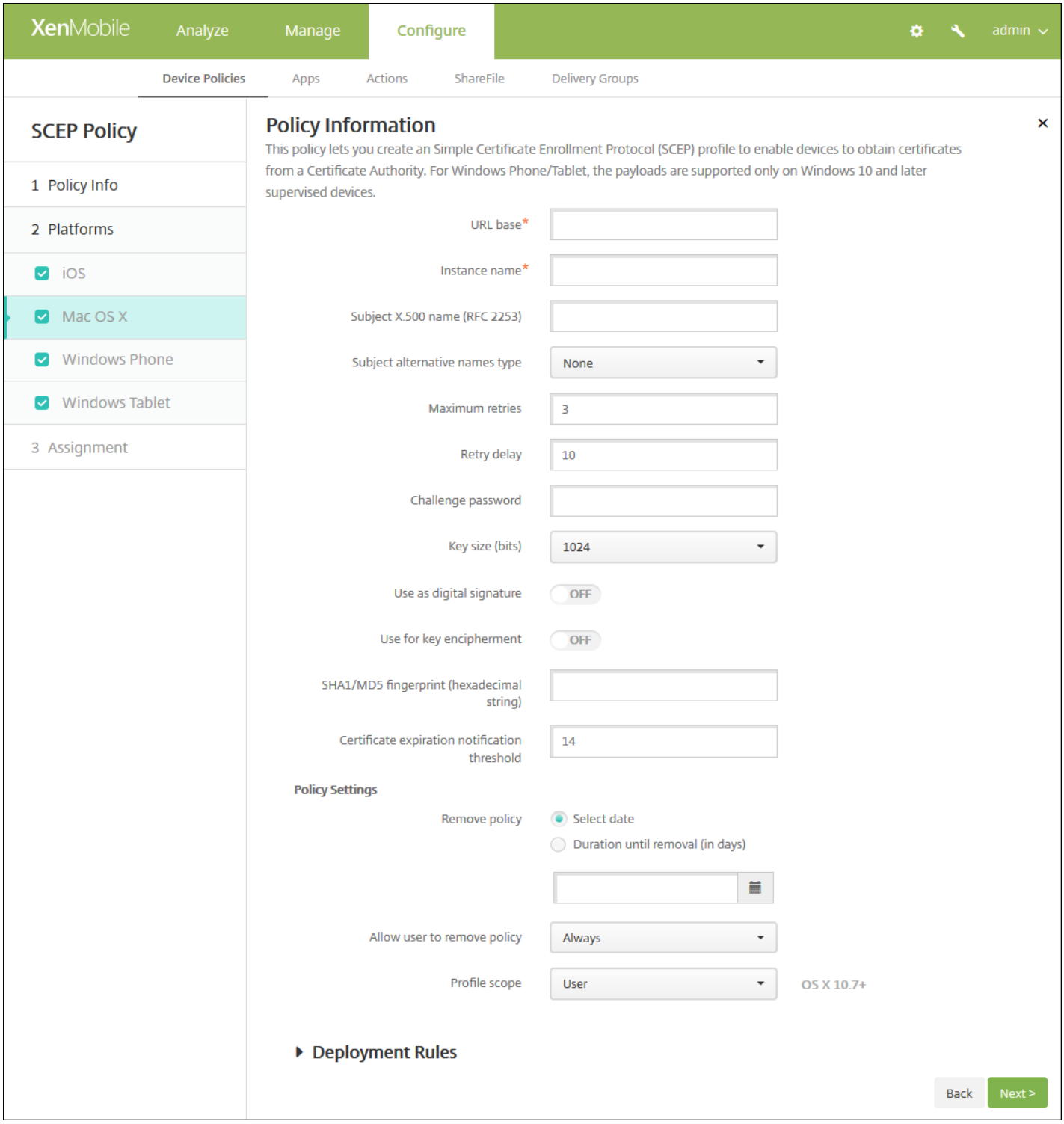
Configure these settings:

- **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 days)**.
  - 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 Mac OS X settings



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 days)**.
  - 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 OS X 10.7 and later.

7. Configure the deployment rules

8. Click **Next**. The **SCEP 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** to save the policy.

Sideloading key device policy

Jan 12, 2017

Sideloading in XenMobile lets you deploy apps that have not been purchased from the Windows Store to Windows 8.1 devices. Most frequently you sideload apps that you develop for corporate use that you do not want to be made public in the Windows Store. To sideload apps, you configure the sideloading key and key activations and then deploy the apps to users' devices.

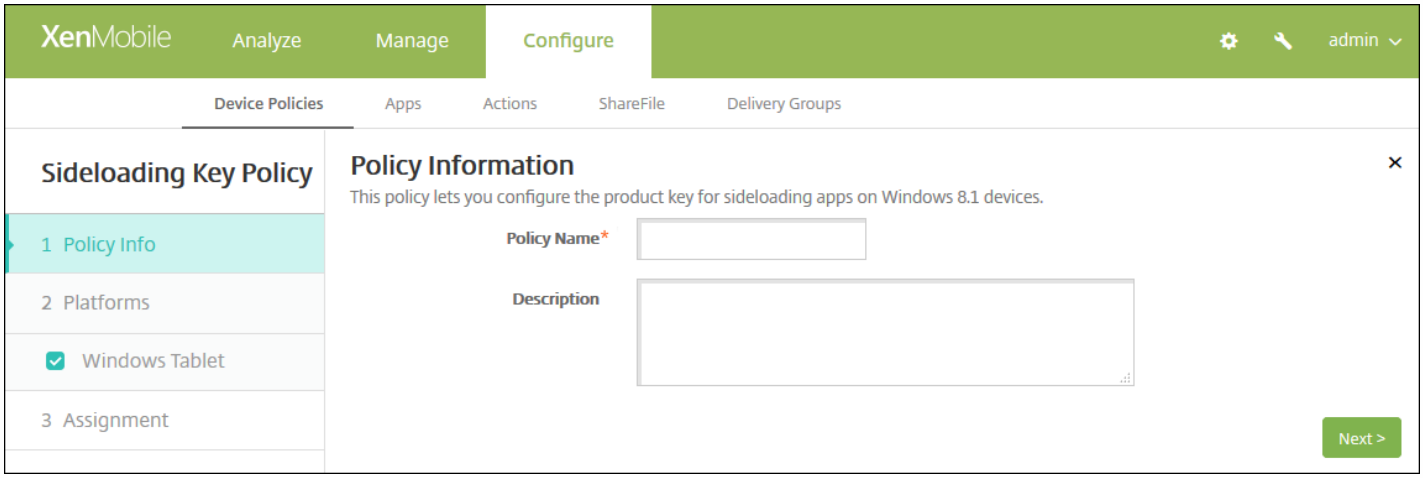
You need the following information before you can create this policy:

- The sideloading product key, which you obtain by signing in to the Microsoft Volume Licensing Service Center
- The key activation, which you create through the command line after obtaining the sideloading product key

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

2. Click **Add**. The **Add New Policy** dialog box appears.

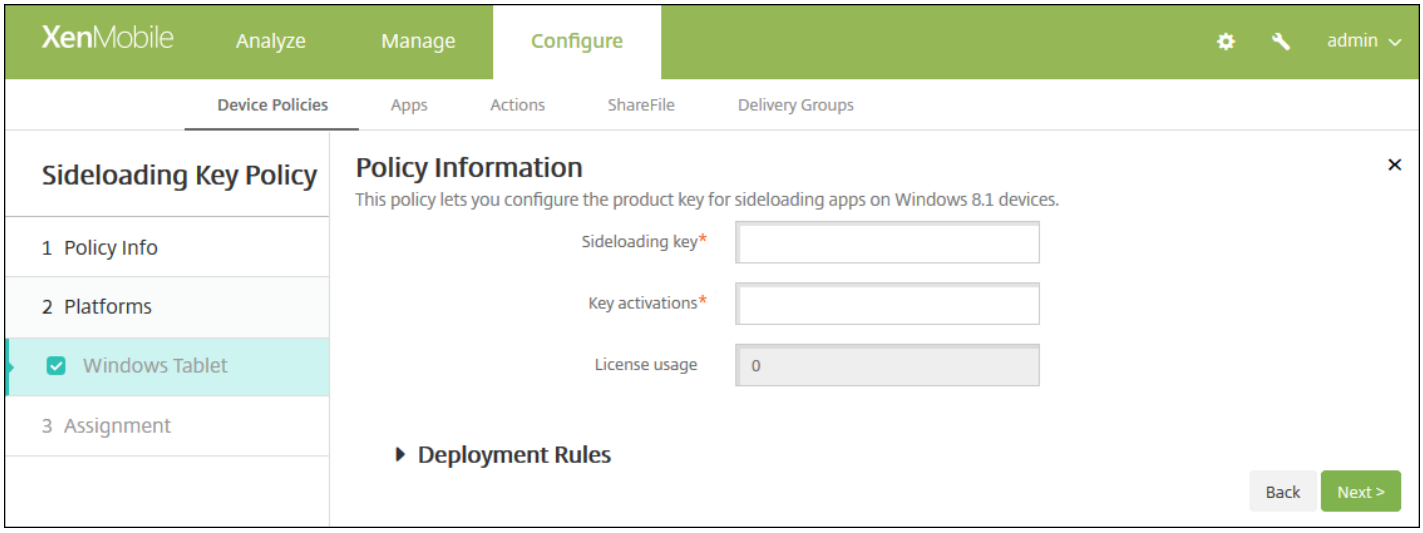
3. Expand **More**, and then under **Apps**, click **Sideloading Key**. The **Sideloading Key Policy** page appears.



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 **Windows Tablet Platform** information page appears.

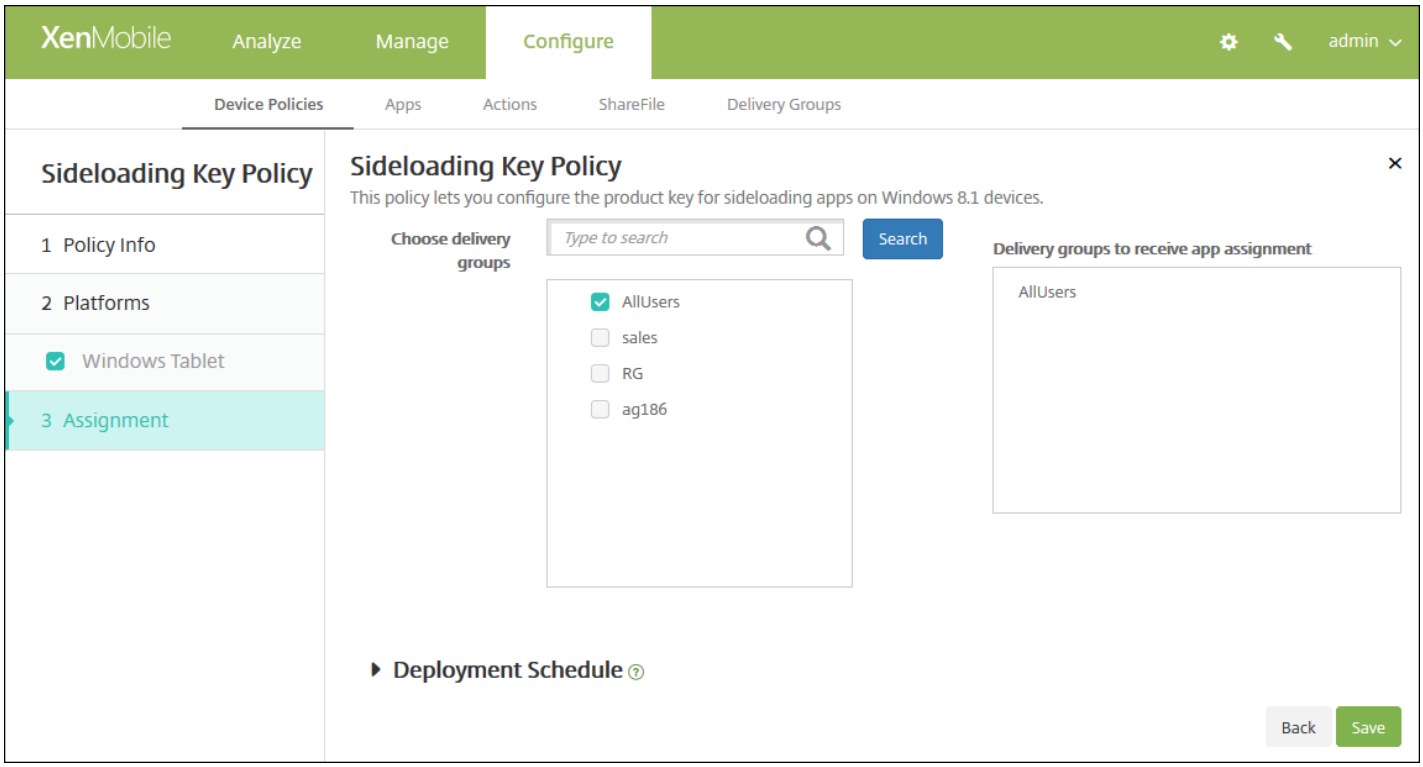


6. Configure these settings:

- **Sideloading key**: Type the sideloading key that you obtained from the Microsoft Volume Licensing Service Center.
- **Key activations**: Type the key activation you created for the sideloading key.
- **License usage**: XenMobile calculates this value based on the number of enrolled tablets. You cannot change this field.

7. Configure the deployment rules

8. Click **Next**. The **Sideloading Key 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**.

Signing certificate device policy

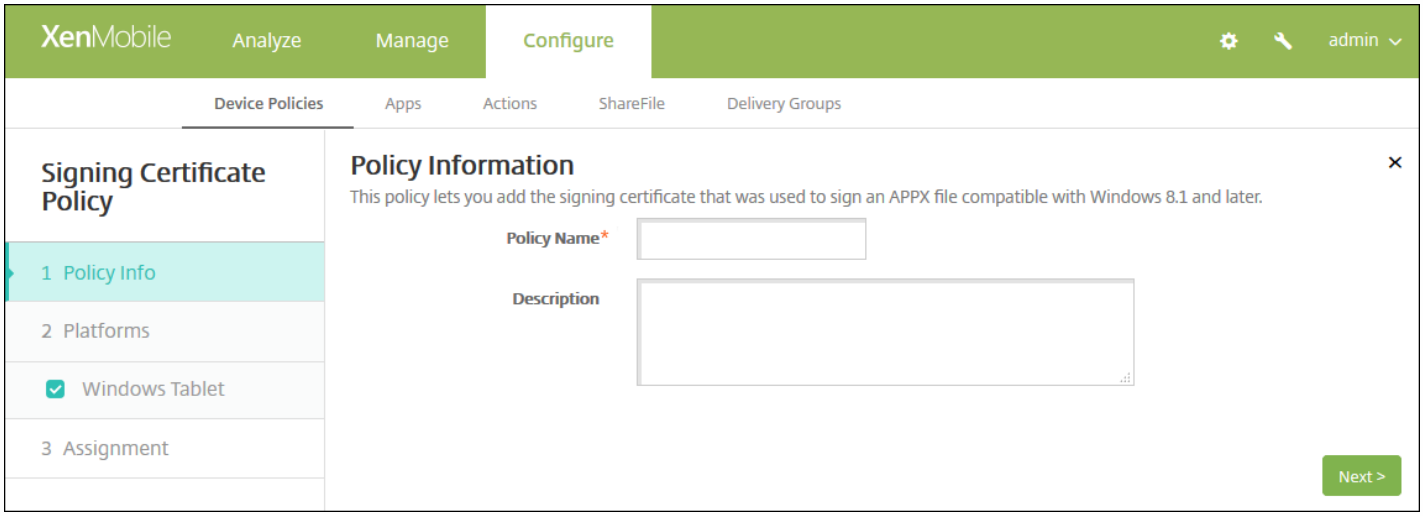
Nov 16, 2016

You can add a device policy in XenMobile to configure signing certificates that are used to sign APPX files. You need the signing certificates if you want to distribute APPX files to users to allow them to install apps on their Windows tablets.

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.

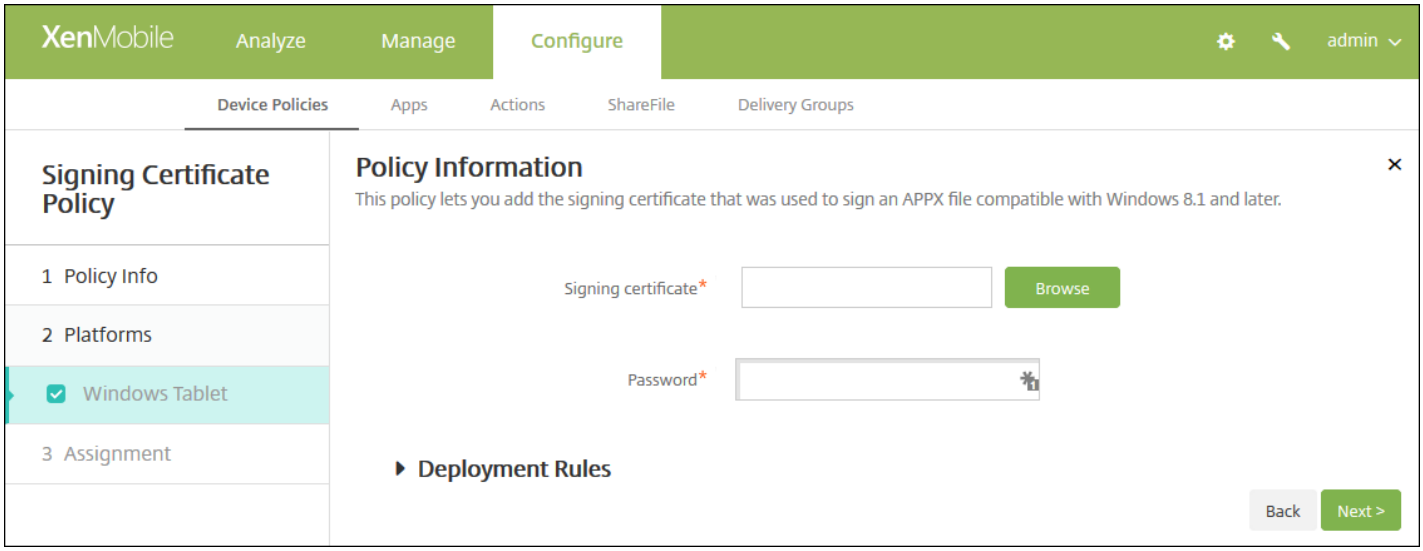
3. Click **More** and then, under **Apps**, click **Signing Certificate**. The **Signing Certificate Policy** page appears.



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 **Windows tablet Platform** page appears.

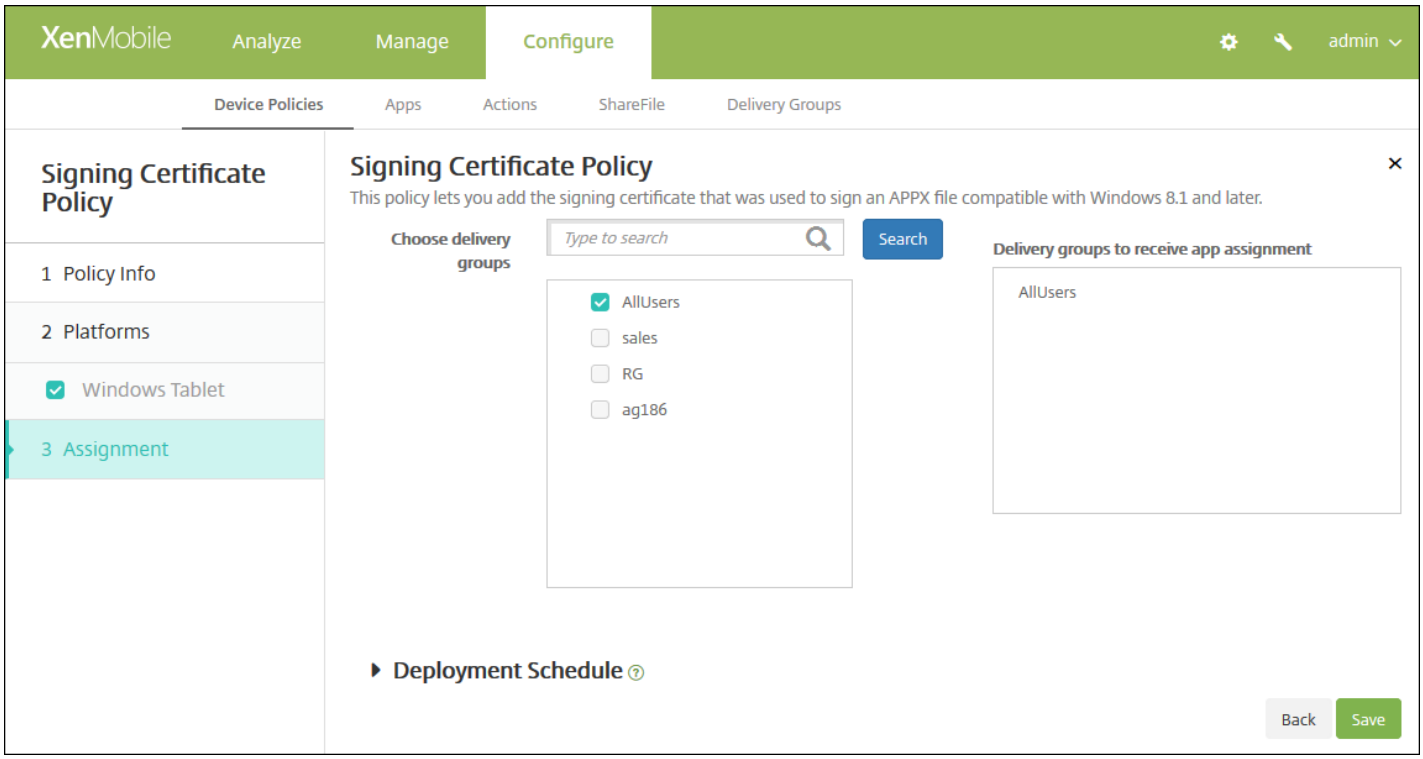


6. Configure these settings:

- **Signing certificate**: Select the certificate that was used to sign the APPX file by clicking **Browse** and navigating to the file's location.
- **Password**: Type the password required to access the signing certificate.

7. Configure the deployment rules

8. Click **Next**. The **Signing 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 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**.

SSO account device policy

Nov 16, 2016

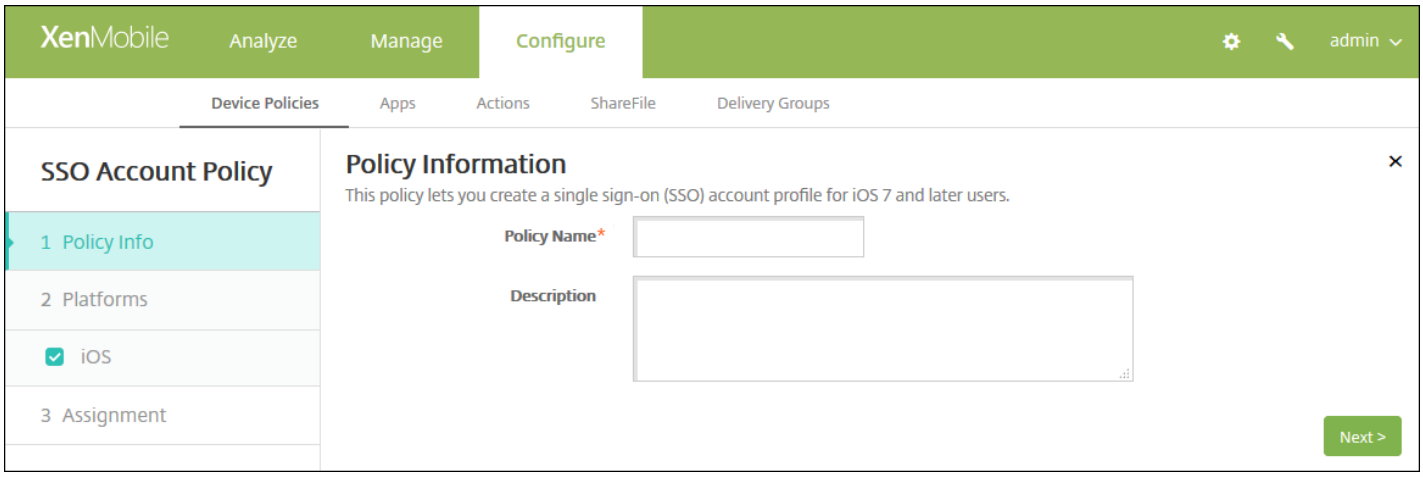
You create single sign-on (SSO) accounts in XenMobile to let users sign on one-time only to access XenMobile and your internal company resources from various apps. Users do not need to store any credentials on the device. The SSO account enterprise user credentials are used across apps, including apps 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.

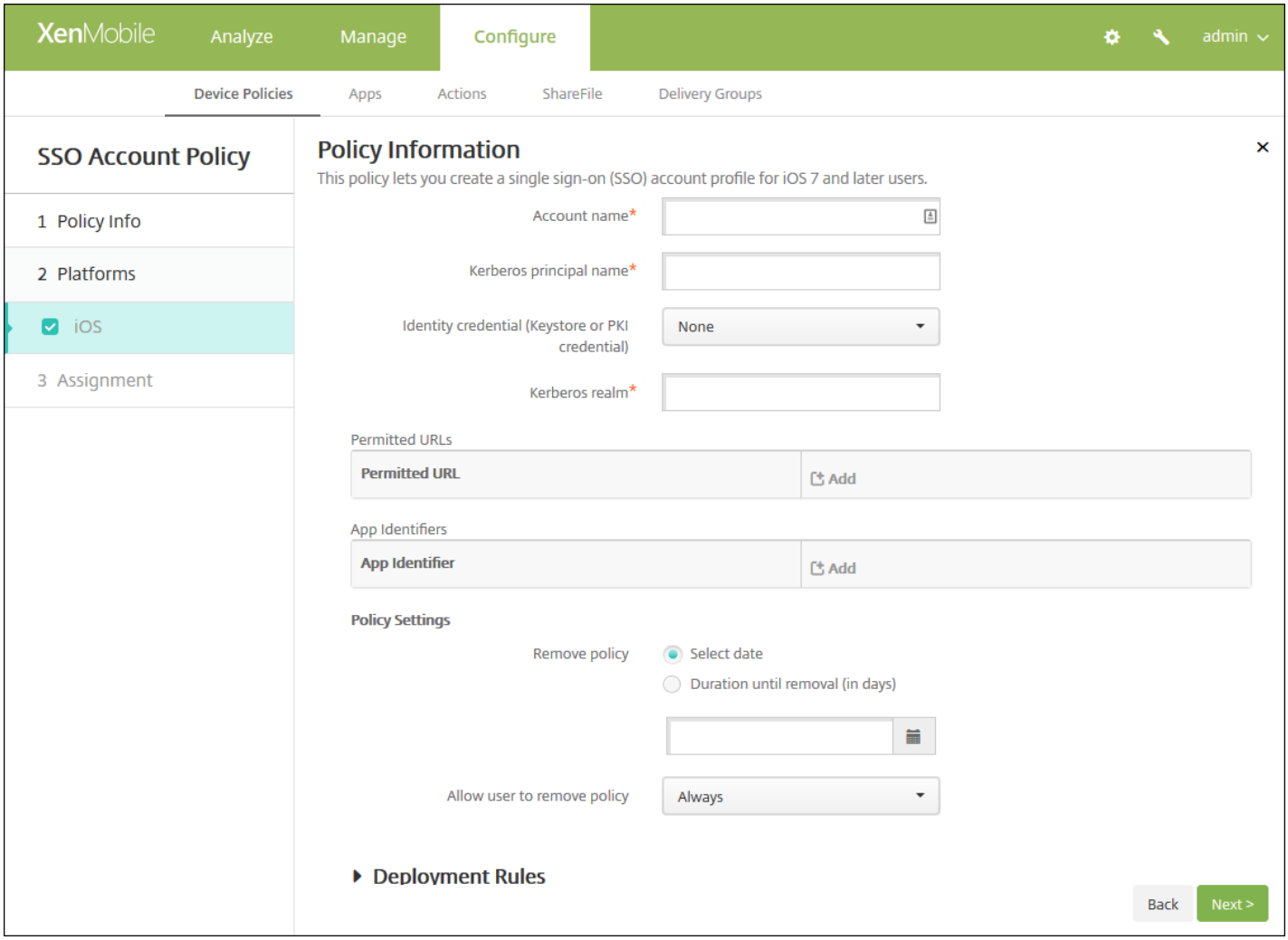
3. Click **More** and then, under **End user**, click **SSO Account**. The **SSO Account Policy** page appears.



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.

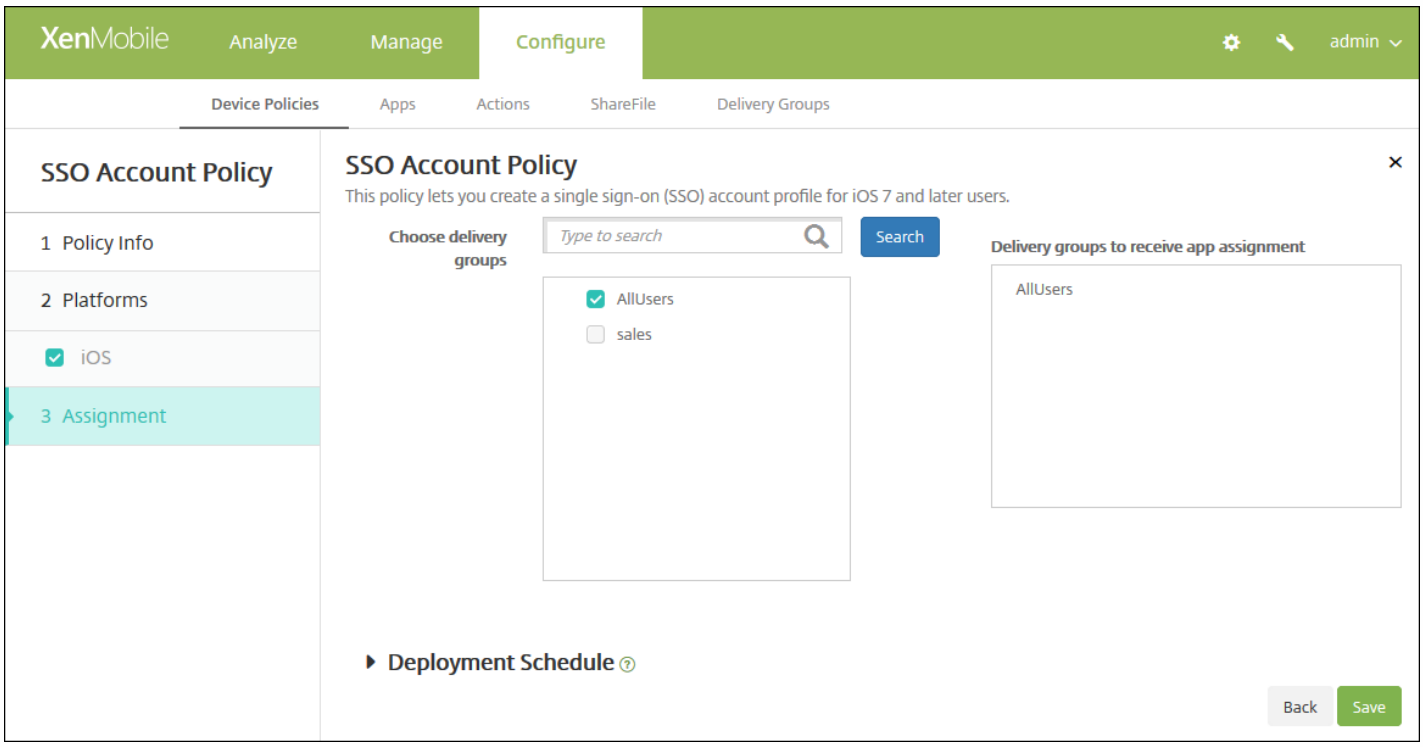
  Note: To delete an existing URL or app identifier, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing.

  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 days)**.
  - 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 the deployment rules

8. Click **Next**. The **SSO Account 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 O**nly 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**.

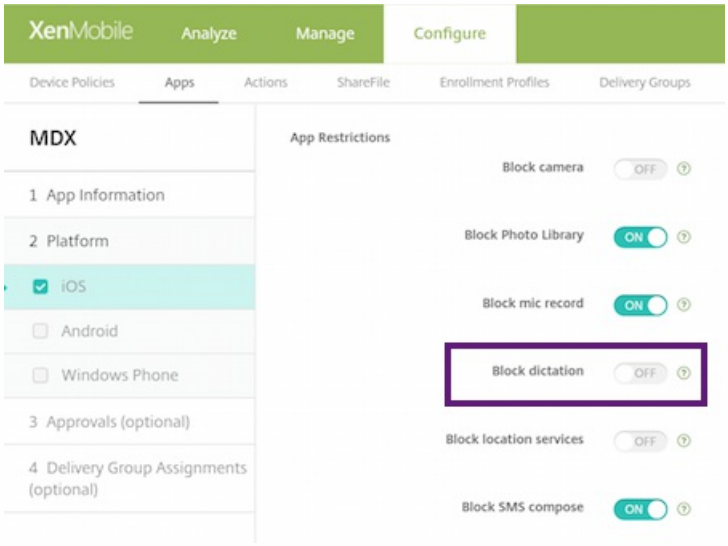
Siri and dictation policies

Nov 16, 2016

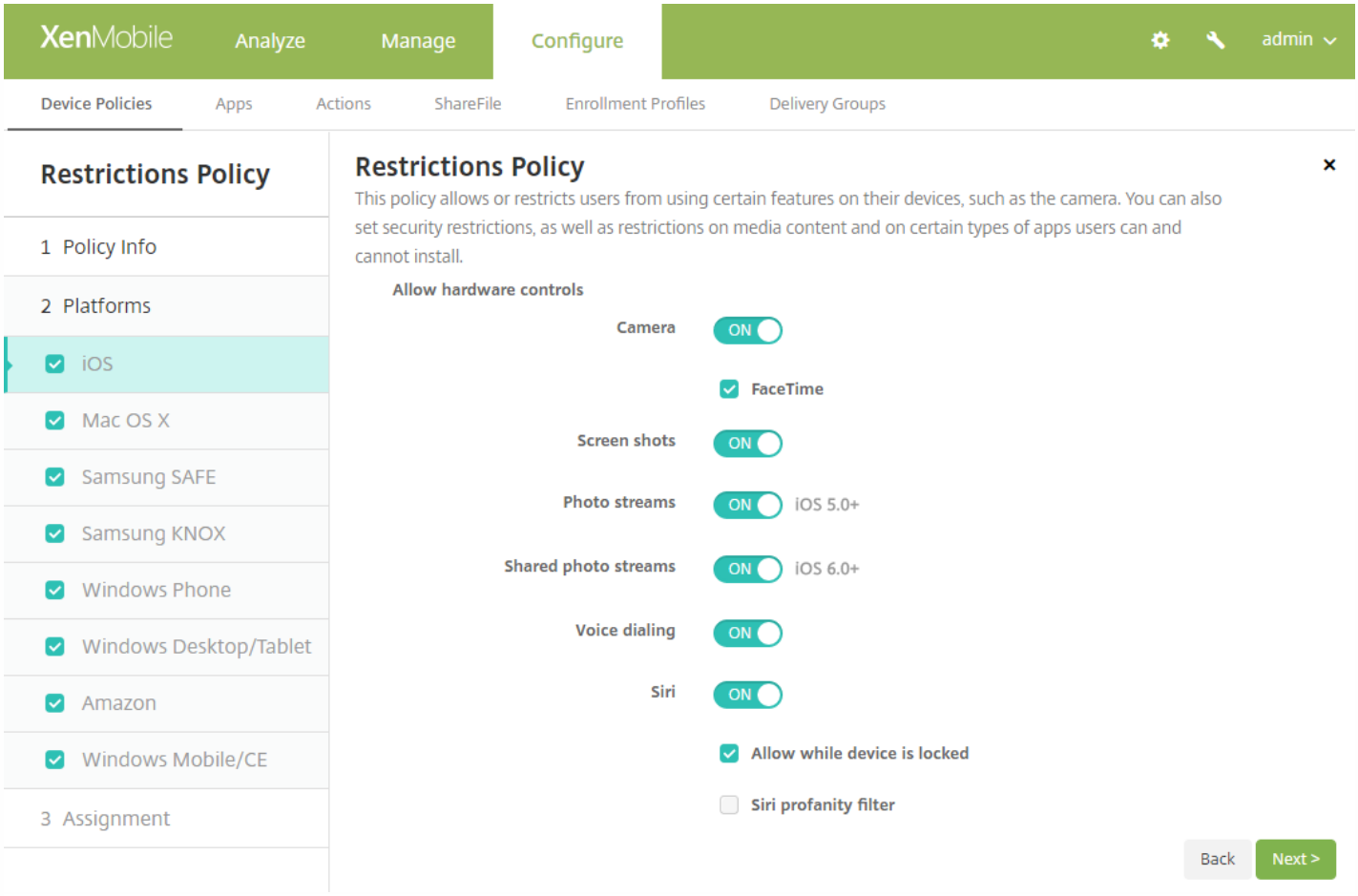
When users ask Siri something or dictate text on managed iOS devices, Apple collects the voice data for purposes of improving Siri. The voice data passes through Apple's cloud-based services, and therefore exists outside the secure XenMobile container. The text that results from dictation, however, remains 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**.



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.



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**.

Storage encryption device policy

Nov 16, 2016

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

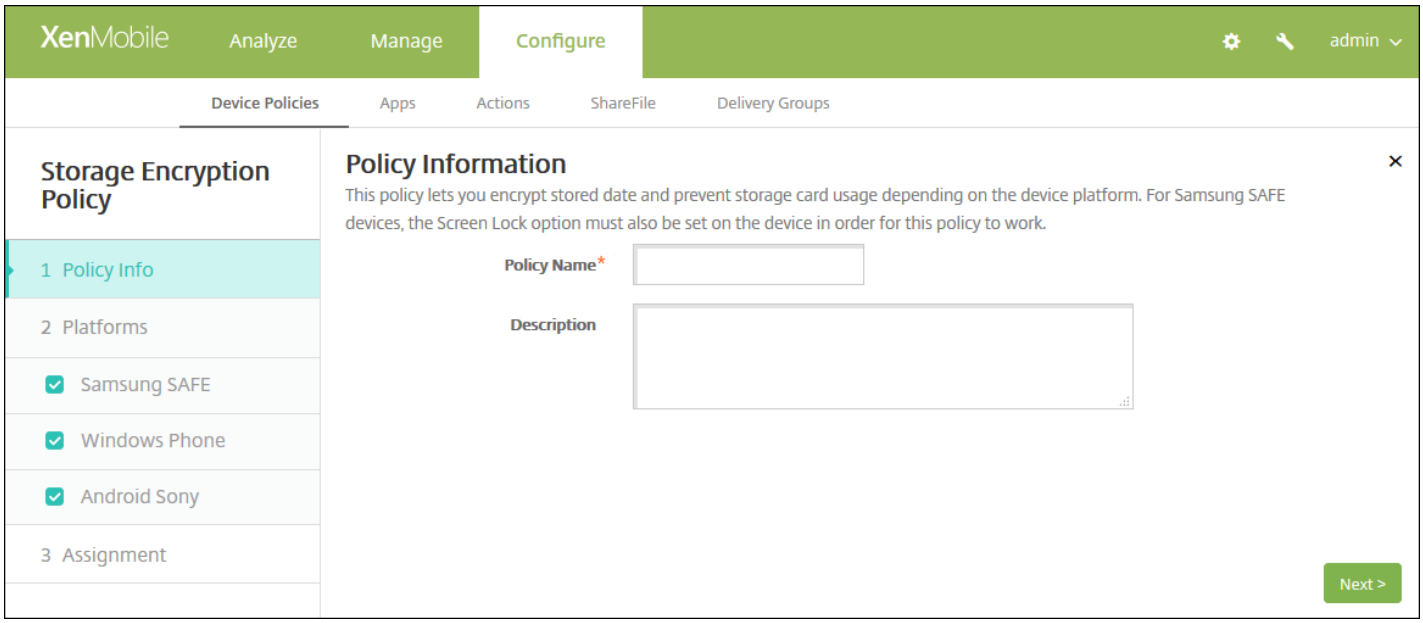
Note: For Samsung SAFE devices, before configuring this policy, make sure the following requirements are met:

- 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:

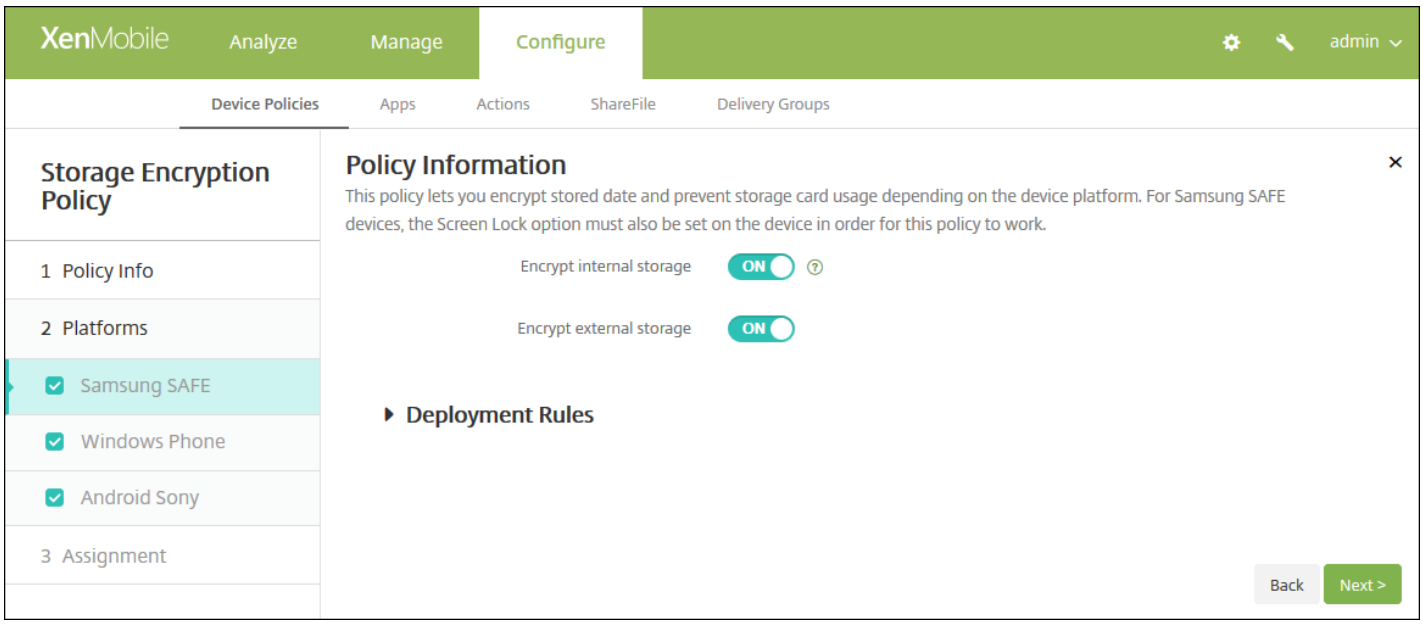
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

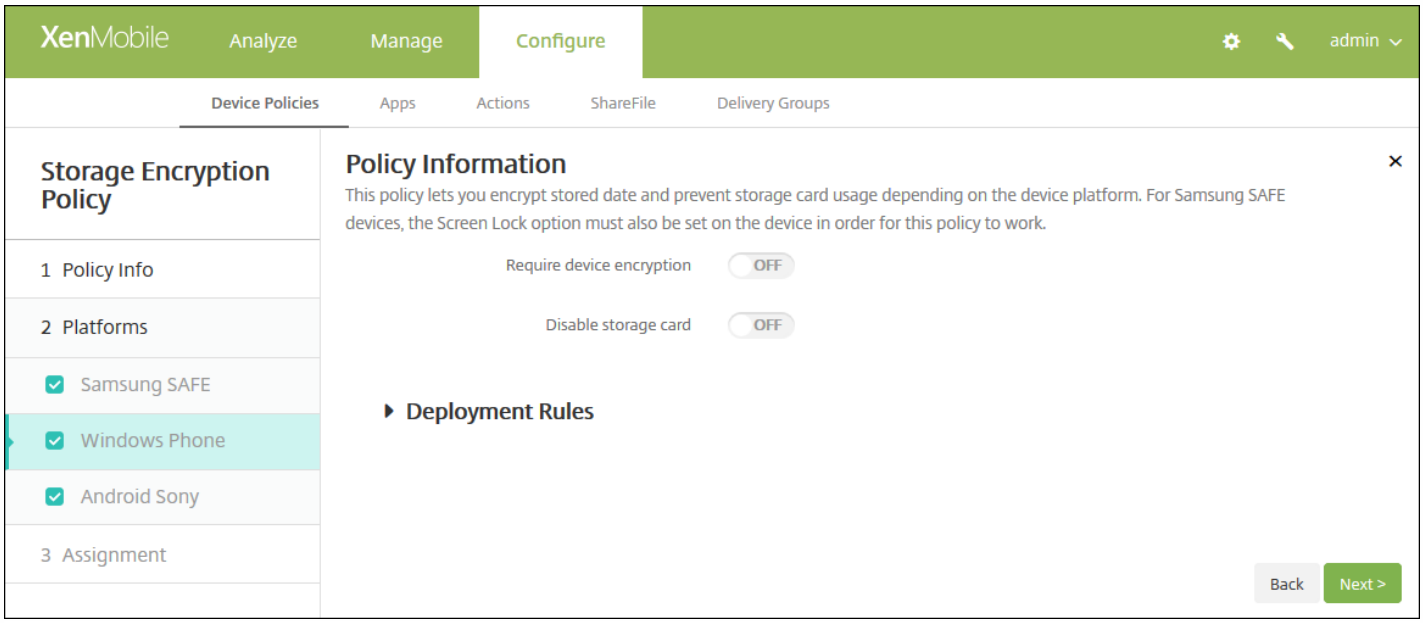
Configure Samsung SAFE settings



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**.

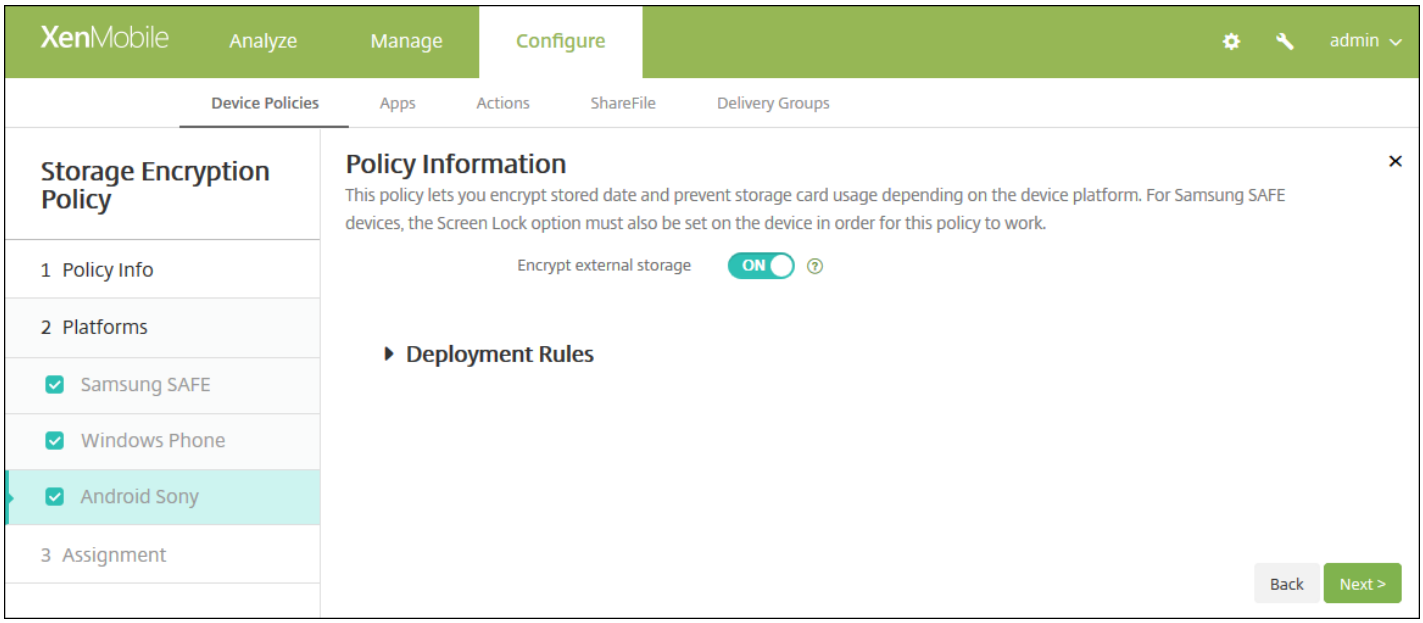
Configure Windows Phone settings



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 Android Sony settings

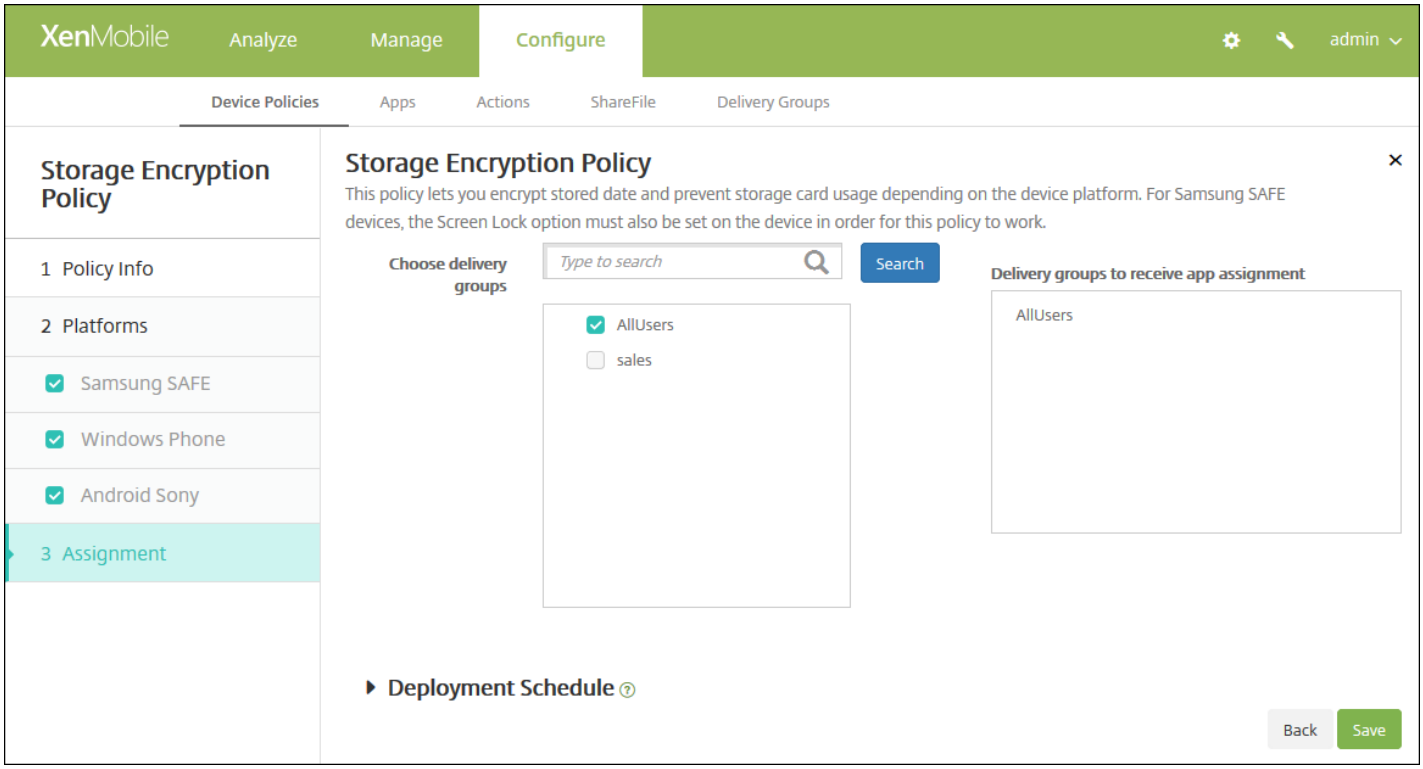


Configure this setting:

- **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 the deployment rules

8. Click **Next**. The **Storage Encryption 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**.

Subscribed calendars device policy

Nov 16, 2016

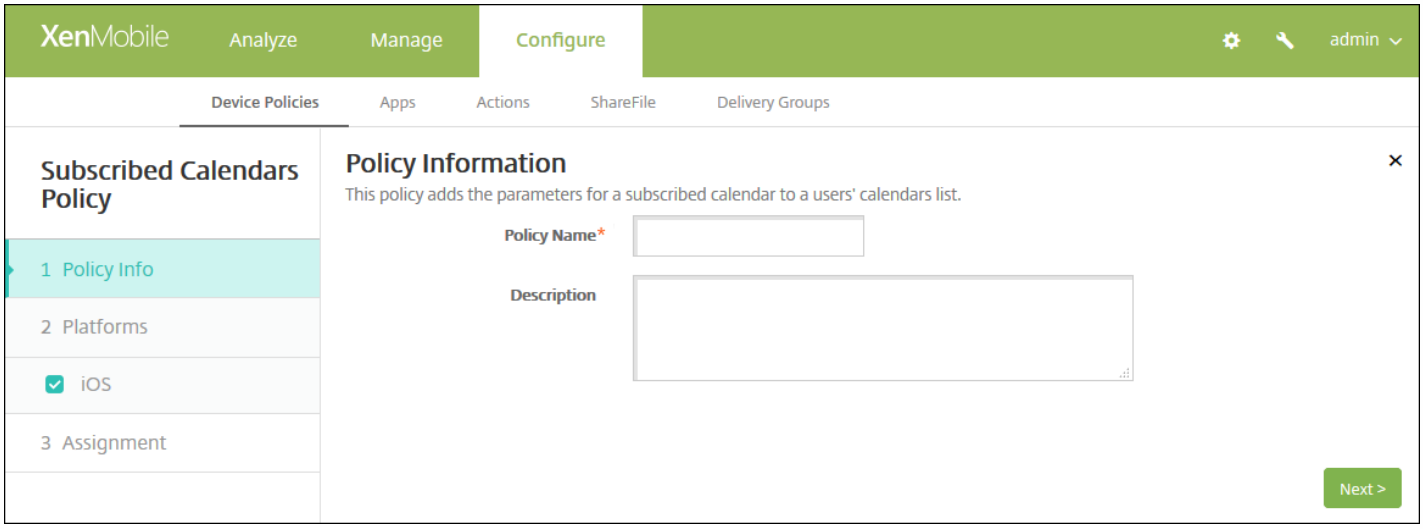
You can add a device policy in XenMobile to add a subscribed calendar to the calendars list on users' iOS devices. The list of public calendars to which you can subscribe is available at www.apple.com/downloads/macosx/calendars.

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.

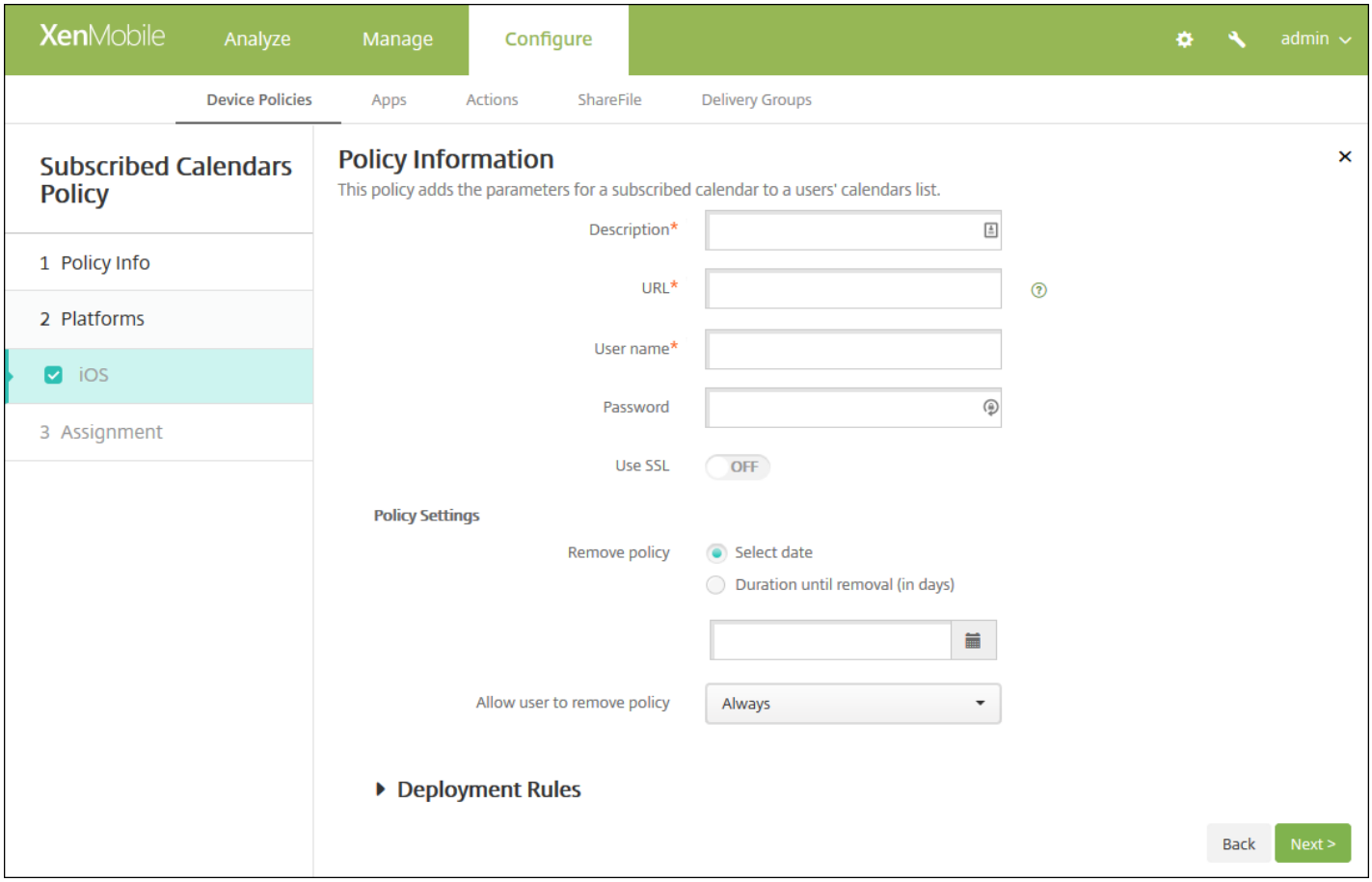
3. Click **More** and then, under **End user**, click **Subscribed Calendars**. The **Subscribed Calendars Policy** page appears.



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.

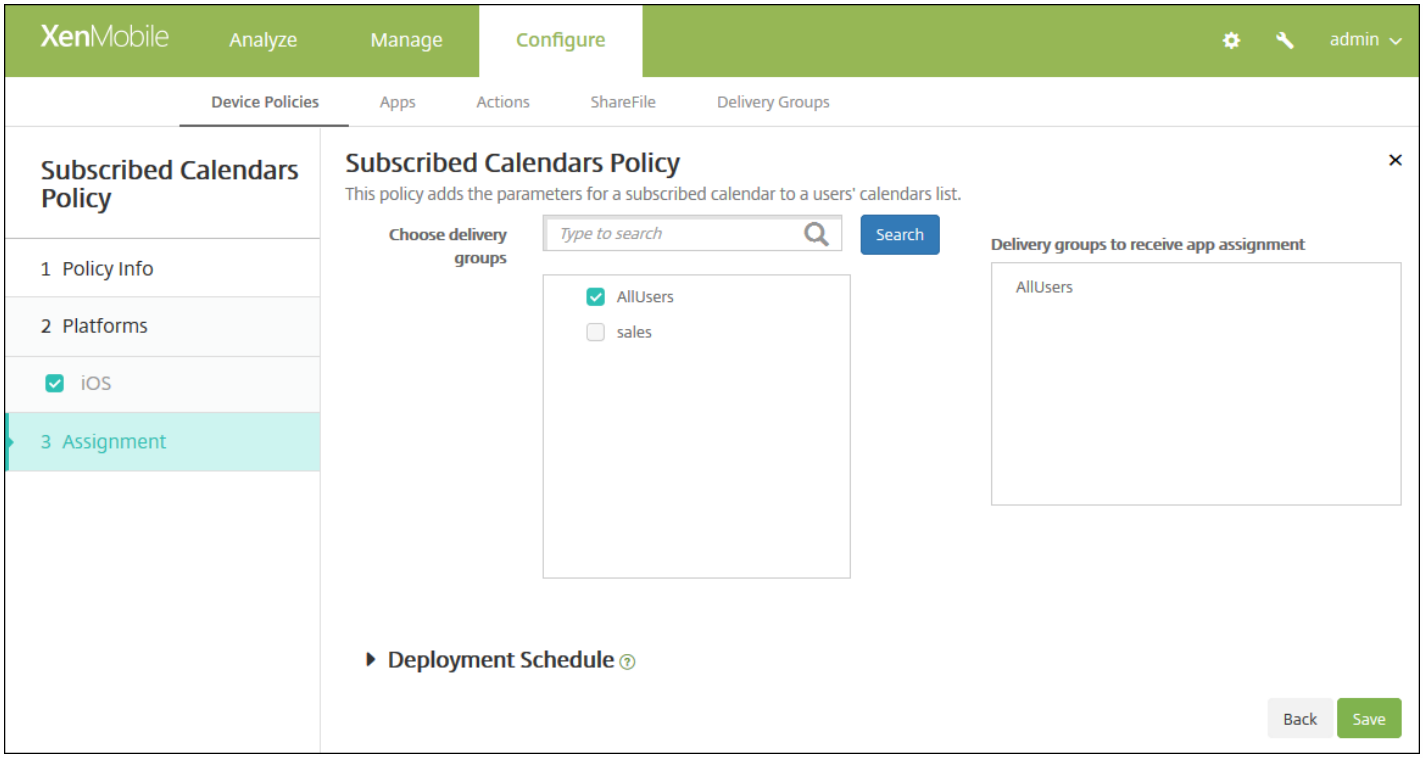


6. Configure these settings:

- **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 days)**.
  - 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 the deployment rules

8. Click **Next**. The **Subscribed Calendars 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**.

Terms and conditions device policy

Nov 16, 2016

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.

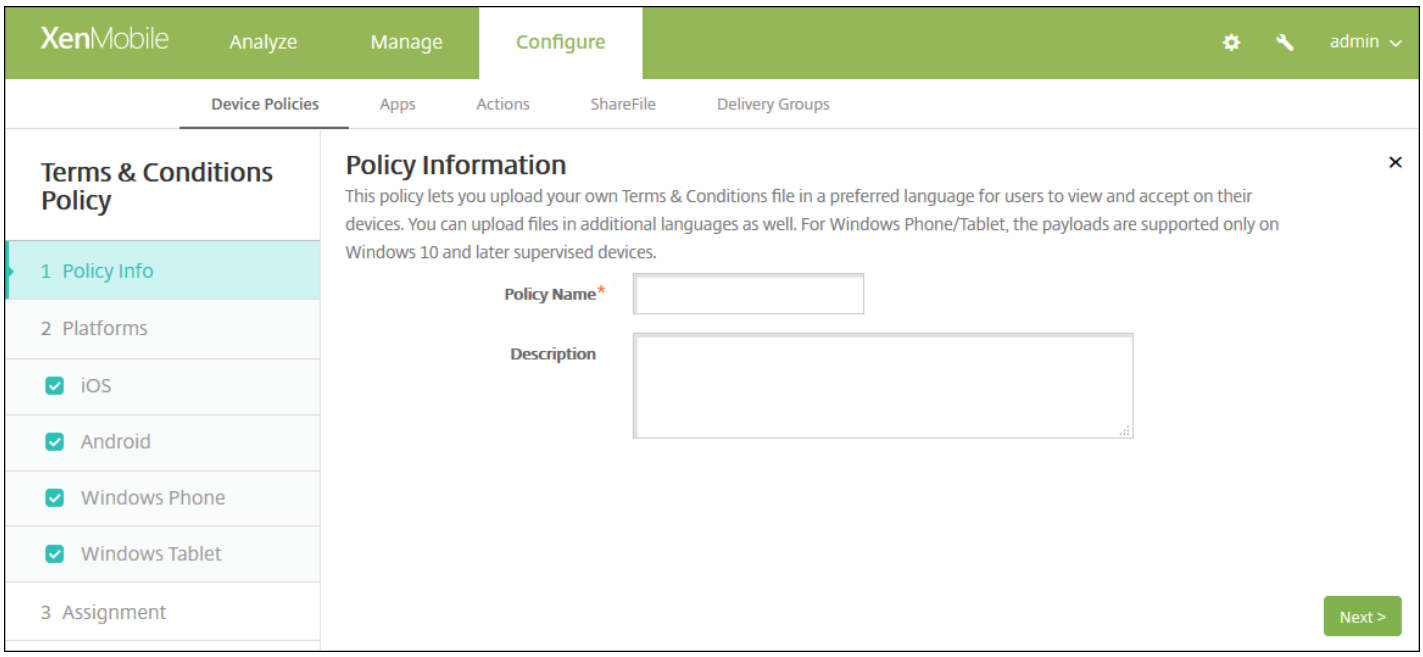
iOS and Android settings

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.

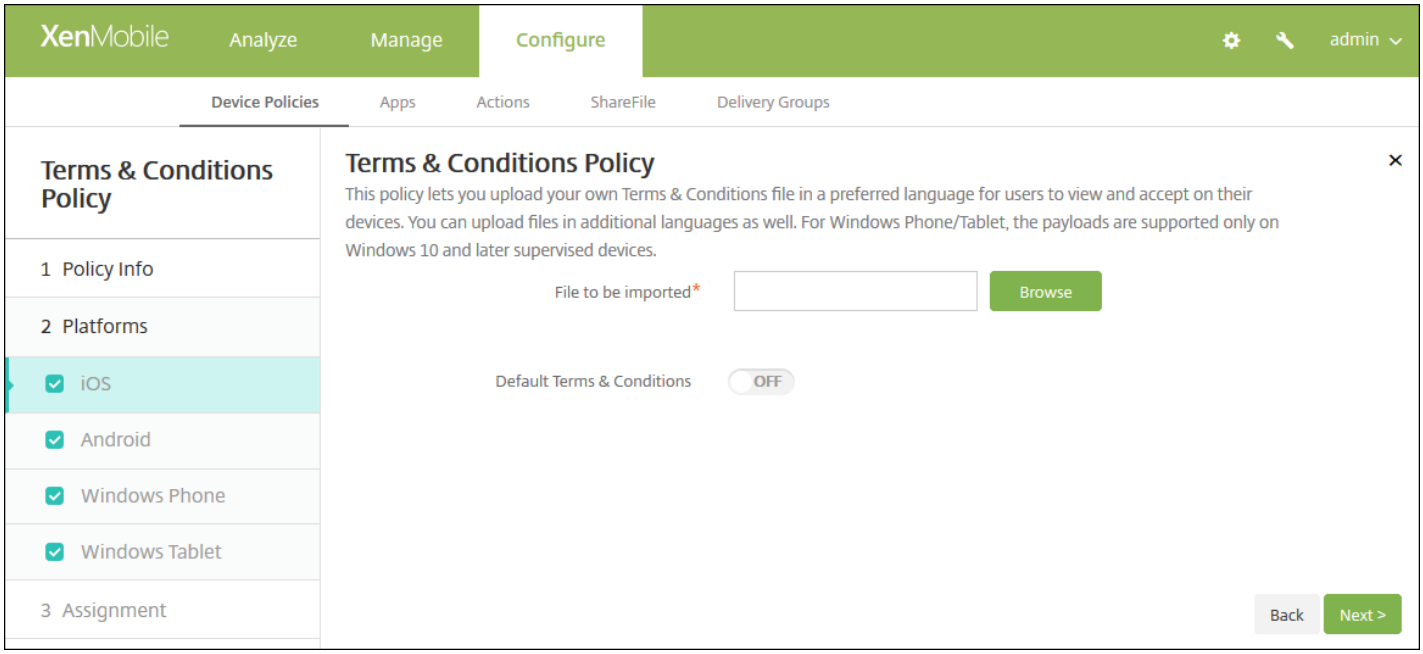
3. Click **Terms & Conditions**. The **Terms & Conditions Policy** page appears.



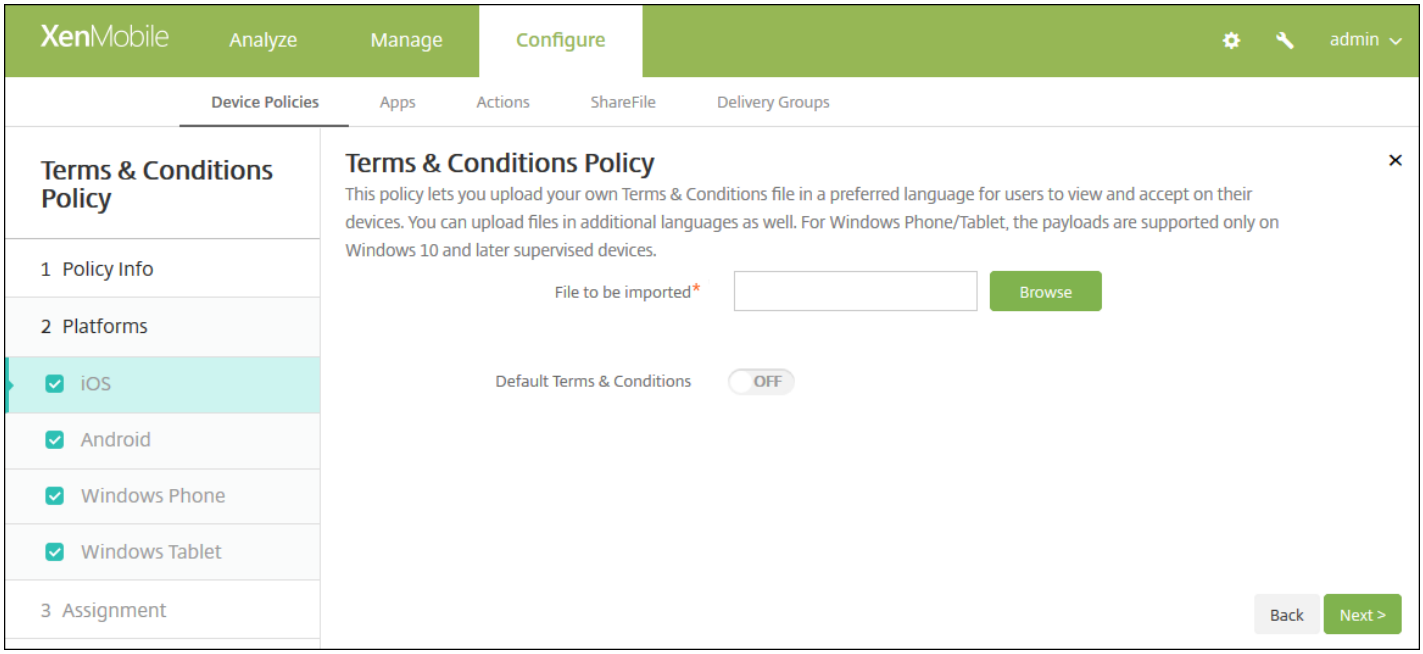
4. In the **Policy Information** pane, enter the following information:

- **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.



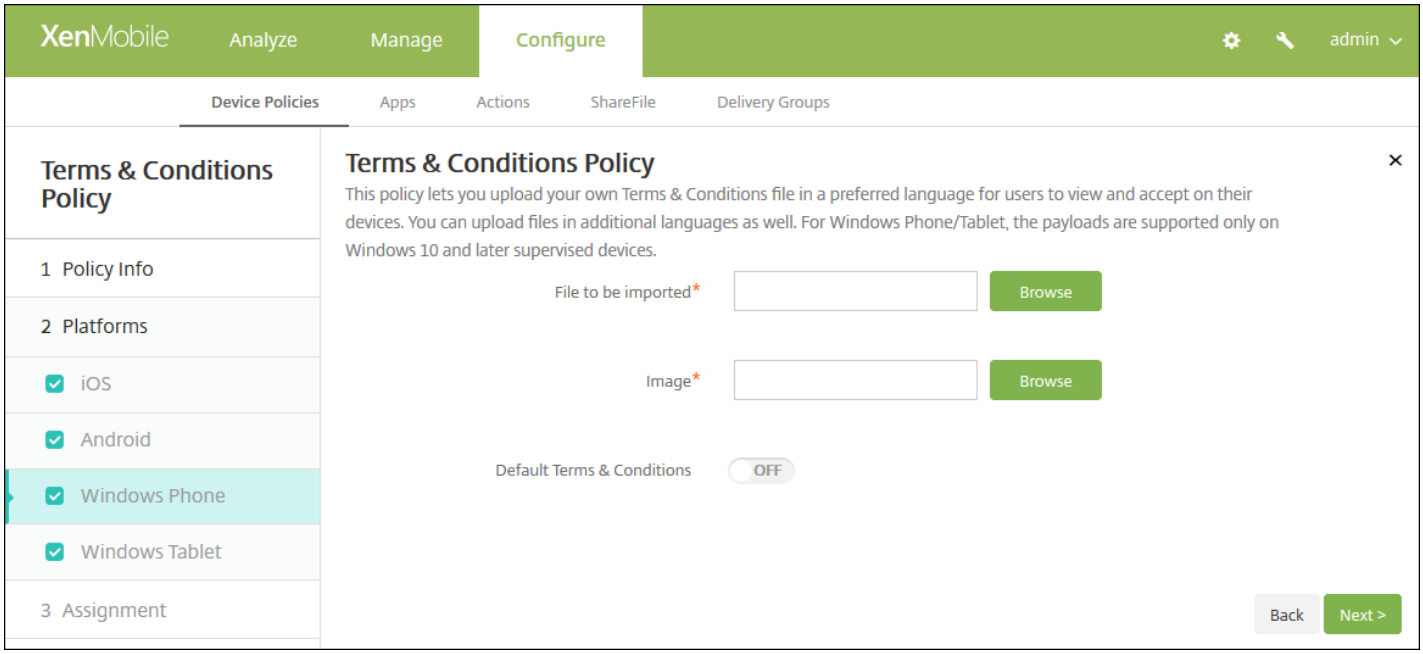
iOS and Android settings



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**.

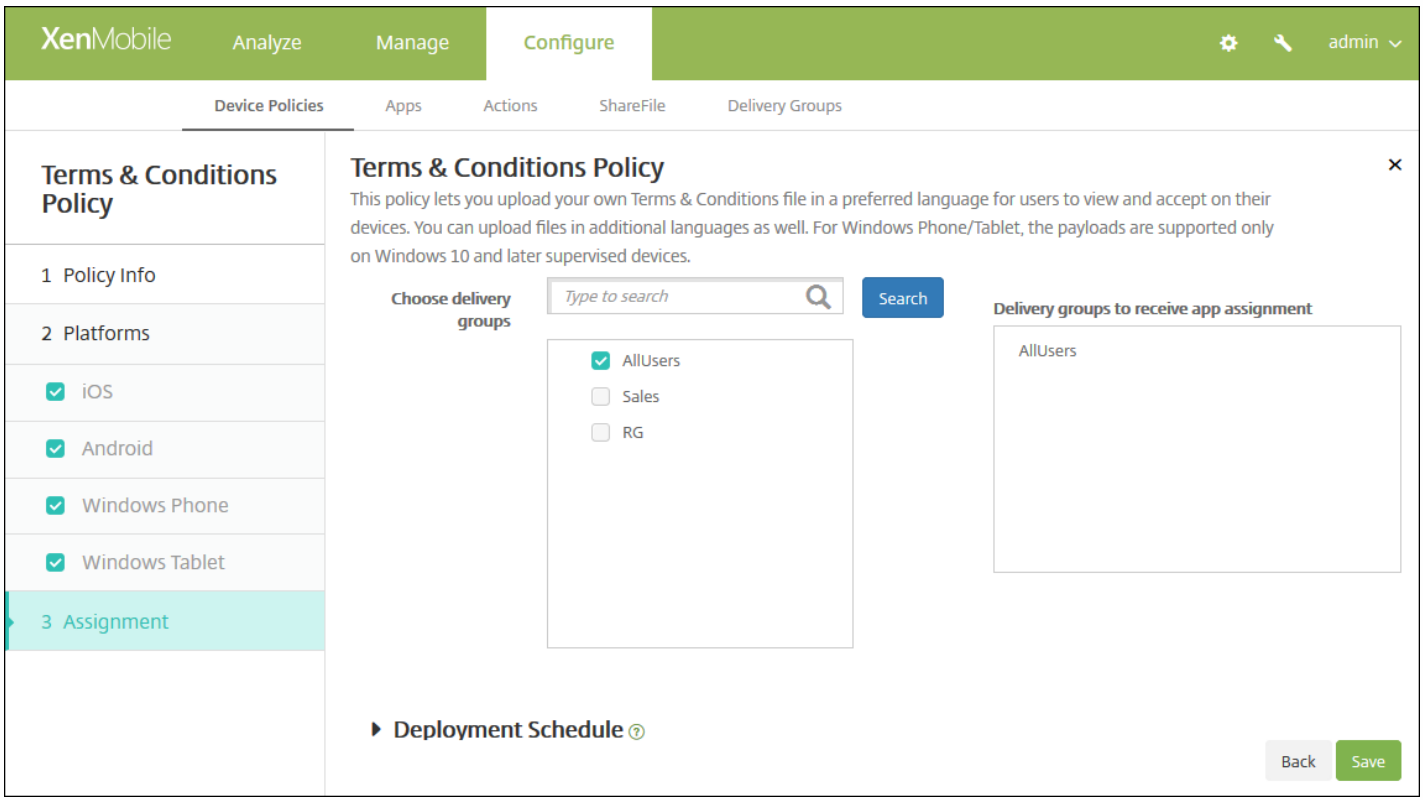
Windows Phone and Windows Tablet settings



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**.

To place an iOS device in Supervised mode by using the Apple Configurator

Nov 16, 2016

With the Apple Configurator, you attach devices to an Apple computer running the Apple Configurator app. You prepare the devices and configure policies through the Apple Configurator. After you provision the devices with the required policies, the first time the devices connect to XenMobile, the policies are applied and you can start managing the devices. For more information about Apple Configurator including the system requirements, see Apple Support.

> **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:
    1. 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.
    2. Optionally, provide a name for the device.
    3. 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.

VPN device policy

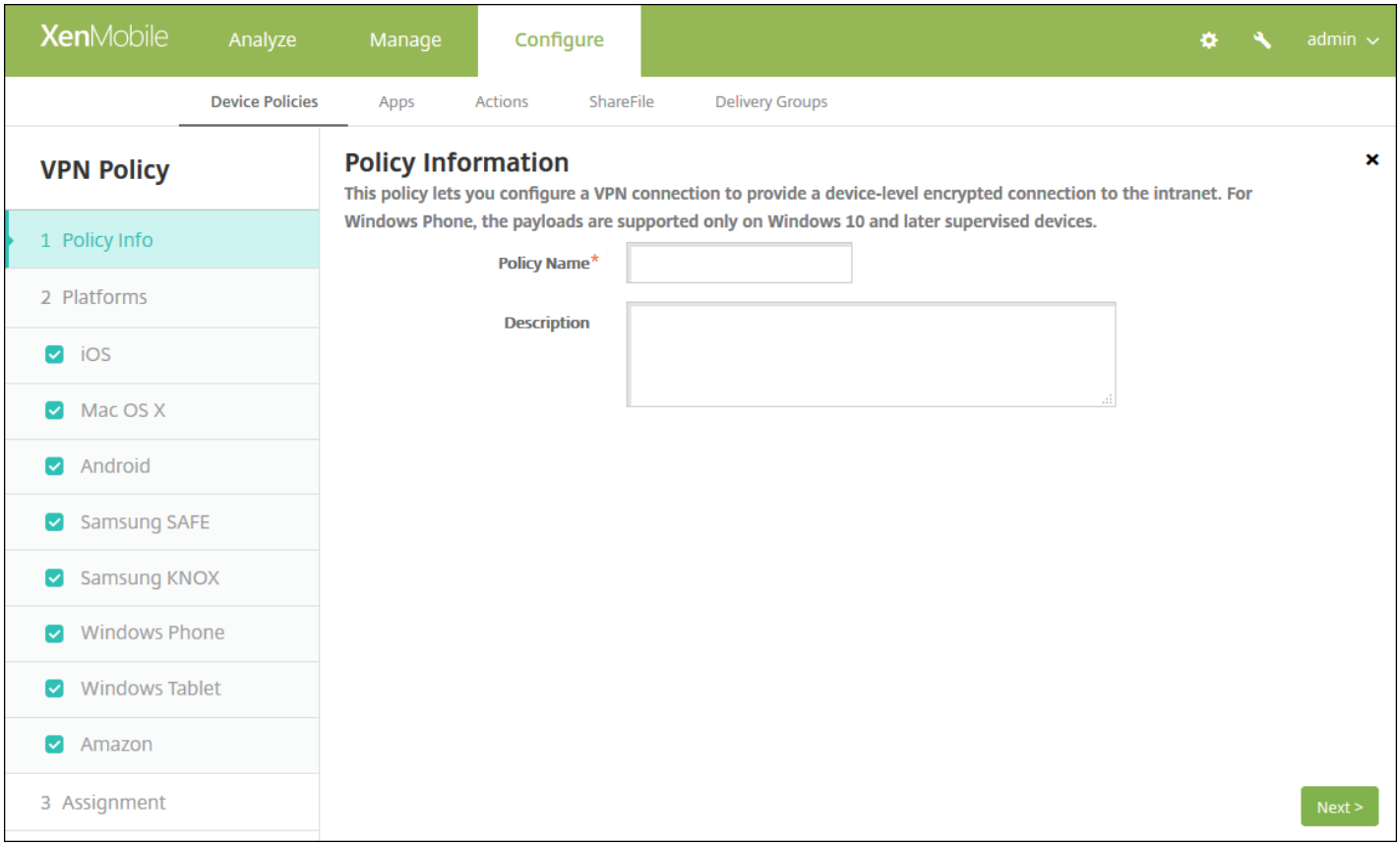
Jan 12, 2017

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: iOS, Android (which includes devices enabled for Android for Work), Samsung SAFE, Samsung KNOX, Windows Tablet, Windows Phone, and Amazon. Each platform requires a different set of values, which are described in detail 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 **VPN**. The **VPN Policy** page appears.



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

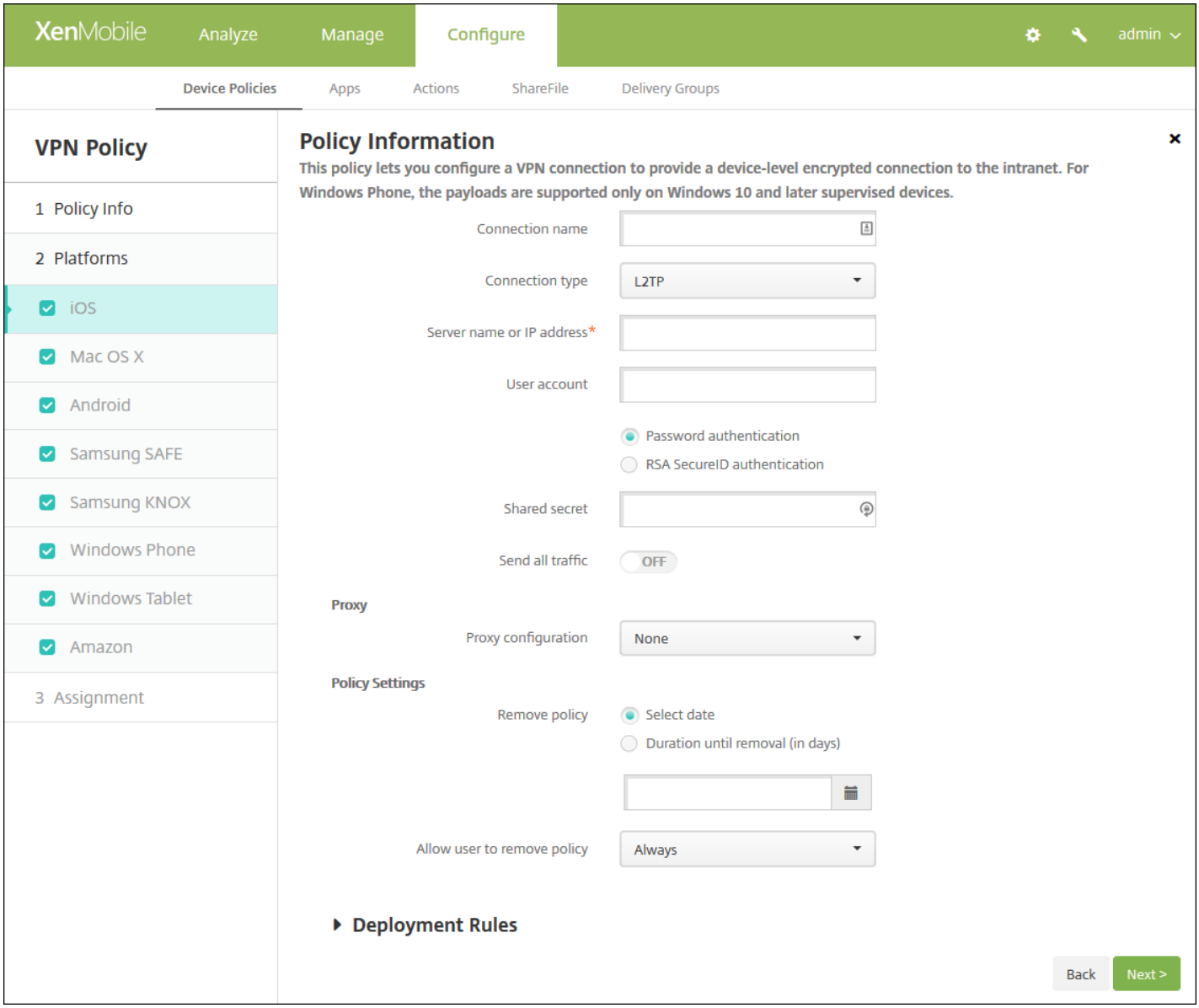
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

Configure iOS settings



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.
  - **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

Configure PPTP Protocol

Configure IPSec Protocol

Configure Cisco AnyConnect Protocol

Configure Juniper SSL Protocol

Configure F5 SSL Protocol

Configure SonicWALL Protocol

Configure Ariba VIA protocol

Configure IKEv2 protocol

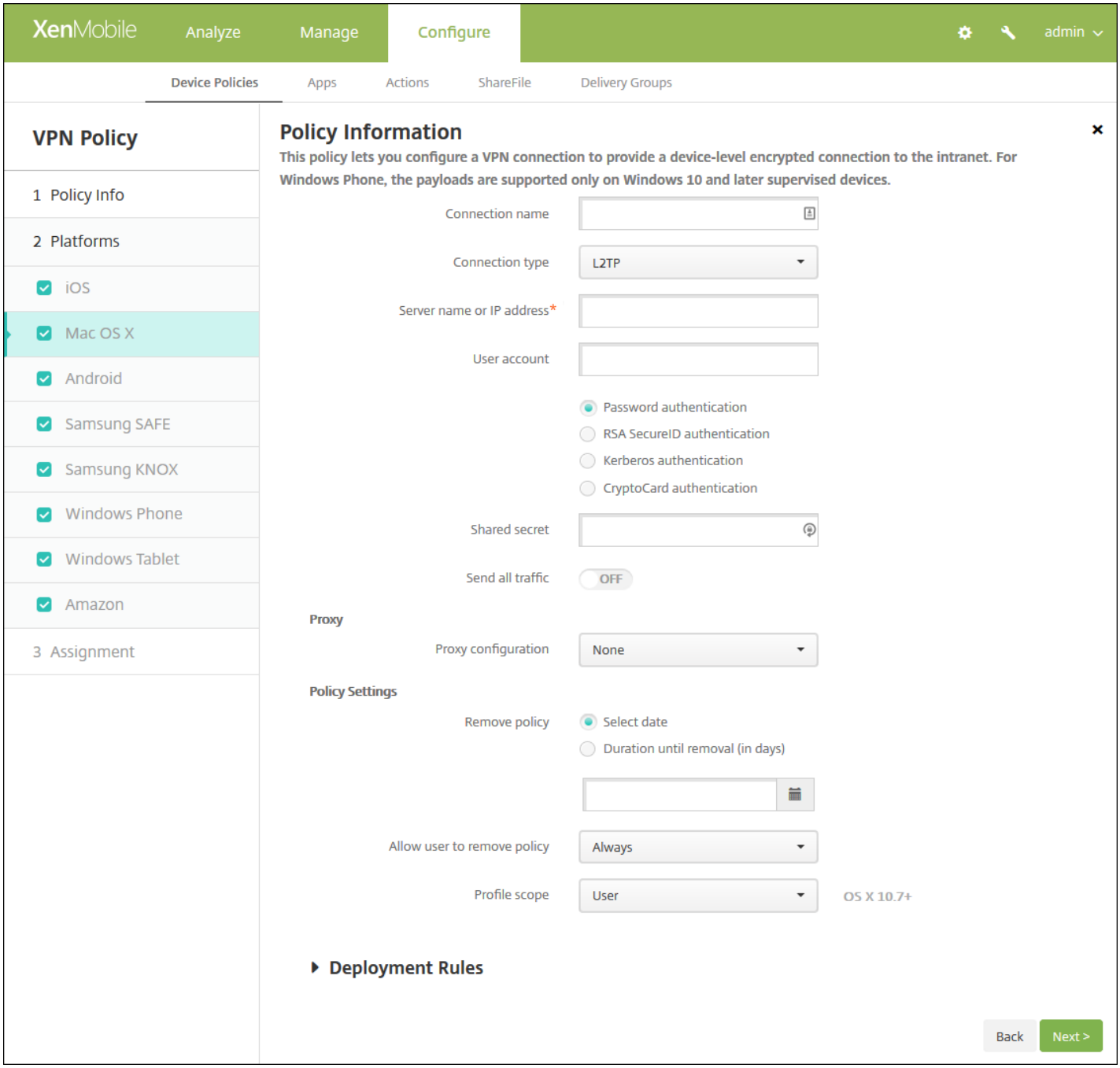
Configure Citrix VPN protocol

Configure Custom SSL protocol

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 days)**.
  - 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 Mac OS X settings



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

Configure PPTP Protocol

Configure IPSec Protocol

Configure Cisco AnyConnect Protocol

Configure Juniper SSL Protocol

Configure F5 SSL Protocol

Configure SonicWALL Protocol

Configure Ariba VIA protocol

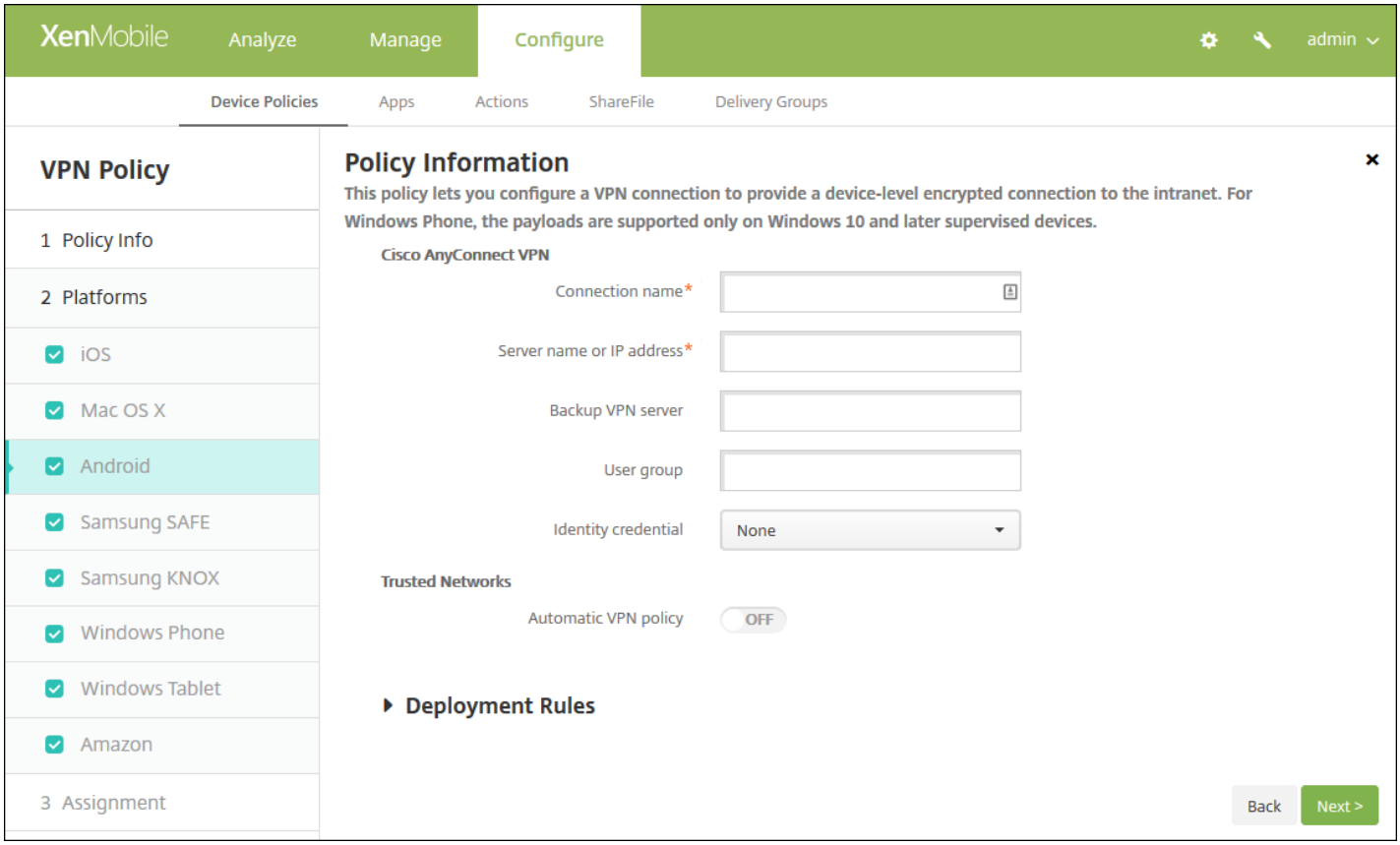
Configure Citrix VPN protocol

Configure Custom SSL protocol

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 days)**.
  - 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 OS X 10.7 and later.

Configure Android settings



Configure these settings:

- **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:

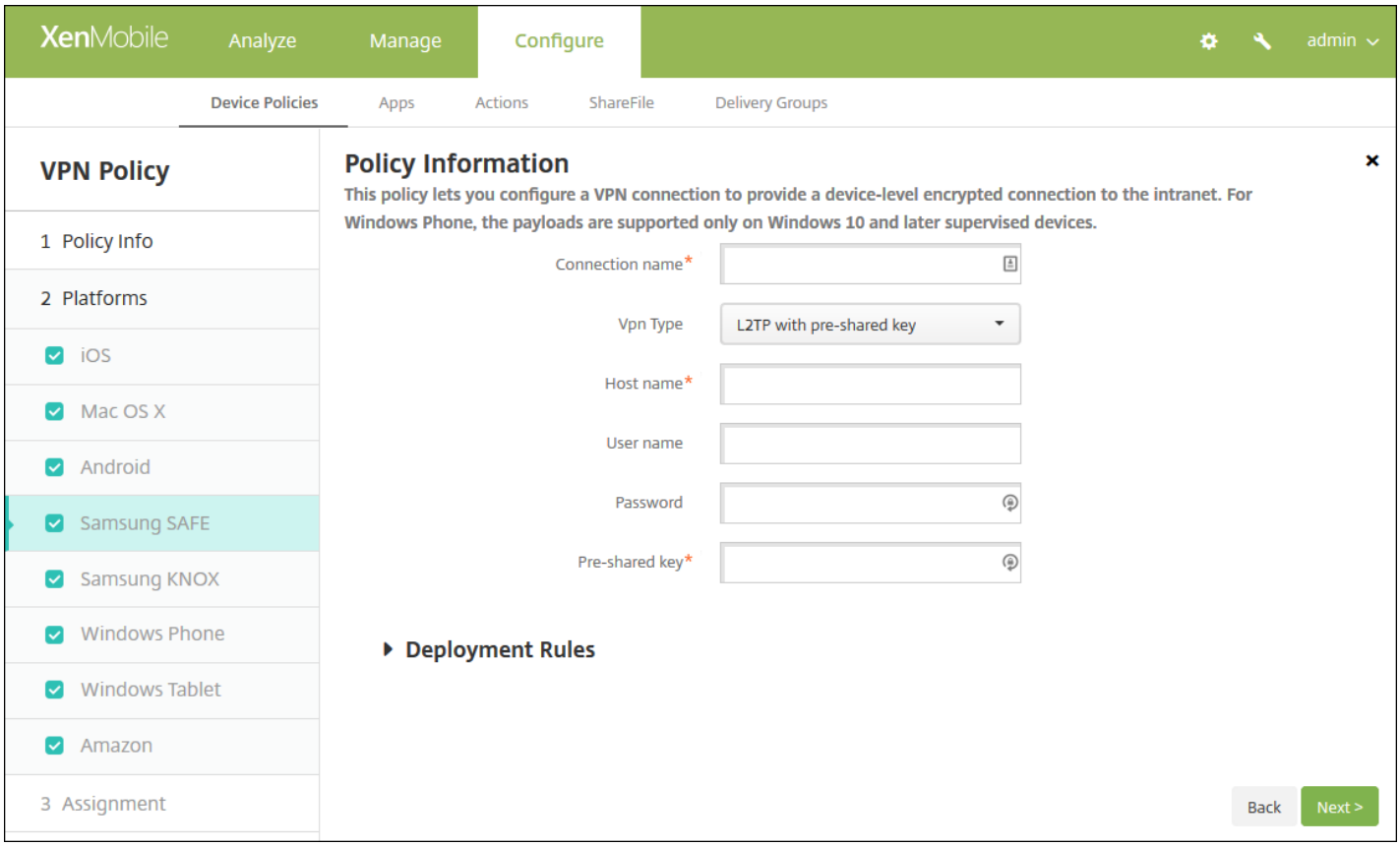
- **Domain**: Type the domain to be added.
- Click **Save** to save the domain or click **Cancel** to not save the domain.

- **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.

Configure Samsung SAFE settings



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

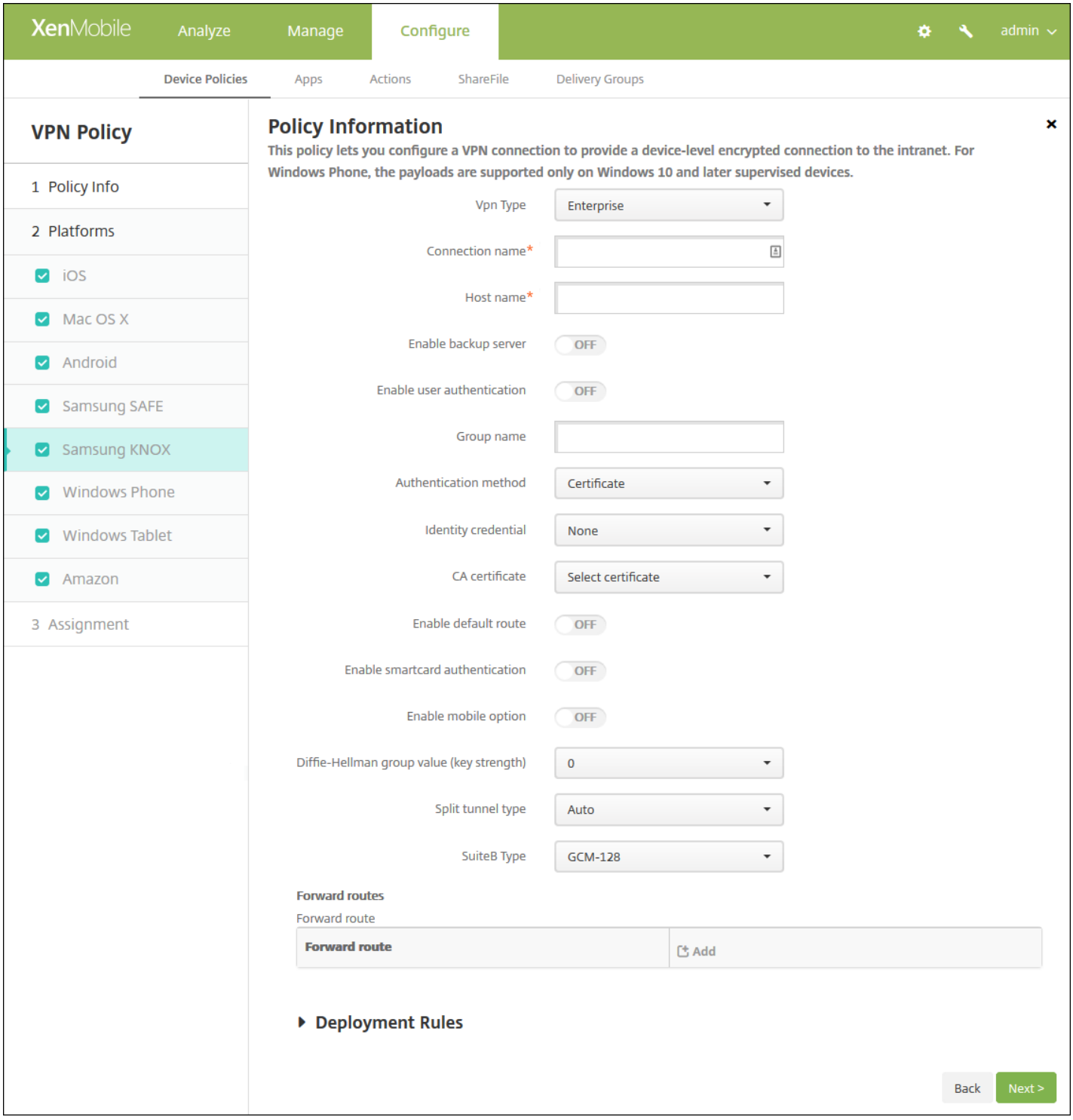
Configure L2TP with certificate protocol

Configure PPTP protocol

Configure Enterprise protocol

Configure Generic protocol

Configure Samsung KNOX settings



Note: When you configure any policy for Samsung KNOX, it applies only inside the Samsung KNOX container.

Configure these settings:

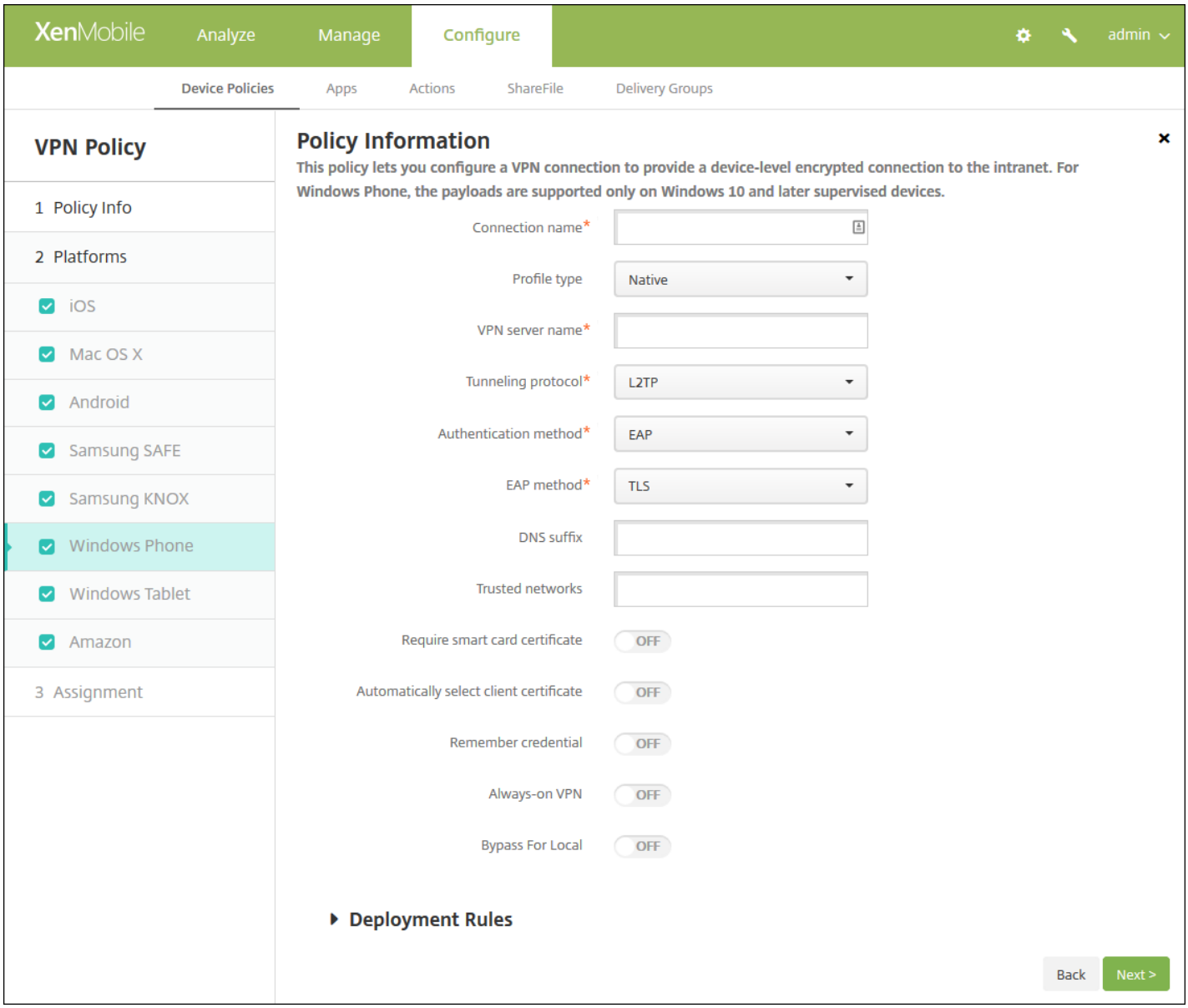
- **Vpn Type**: In the list, click the type of VPN connection to configure, either **Enterprise** (applicable to KNOX versions earlier than 2.0) or **Generic** (applicable to KNOX versions 2.0 or higher). The default is **Enterprise**.

The following sections list the configuration options for each of the preceding connection types.

Configure Enterprise protocol

Configure generic protocol

Configure Windows Phone settings



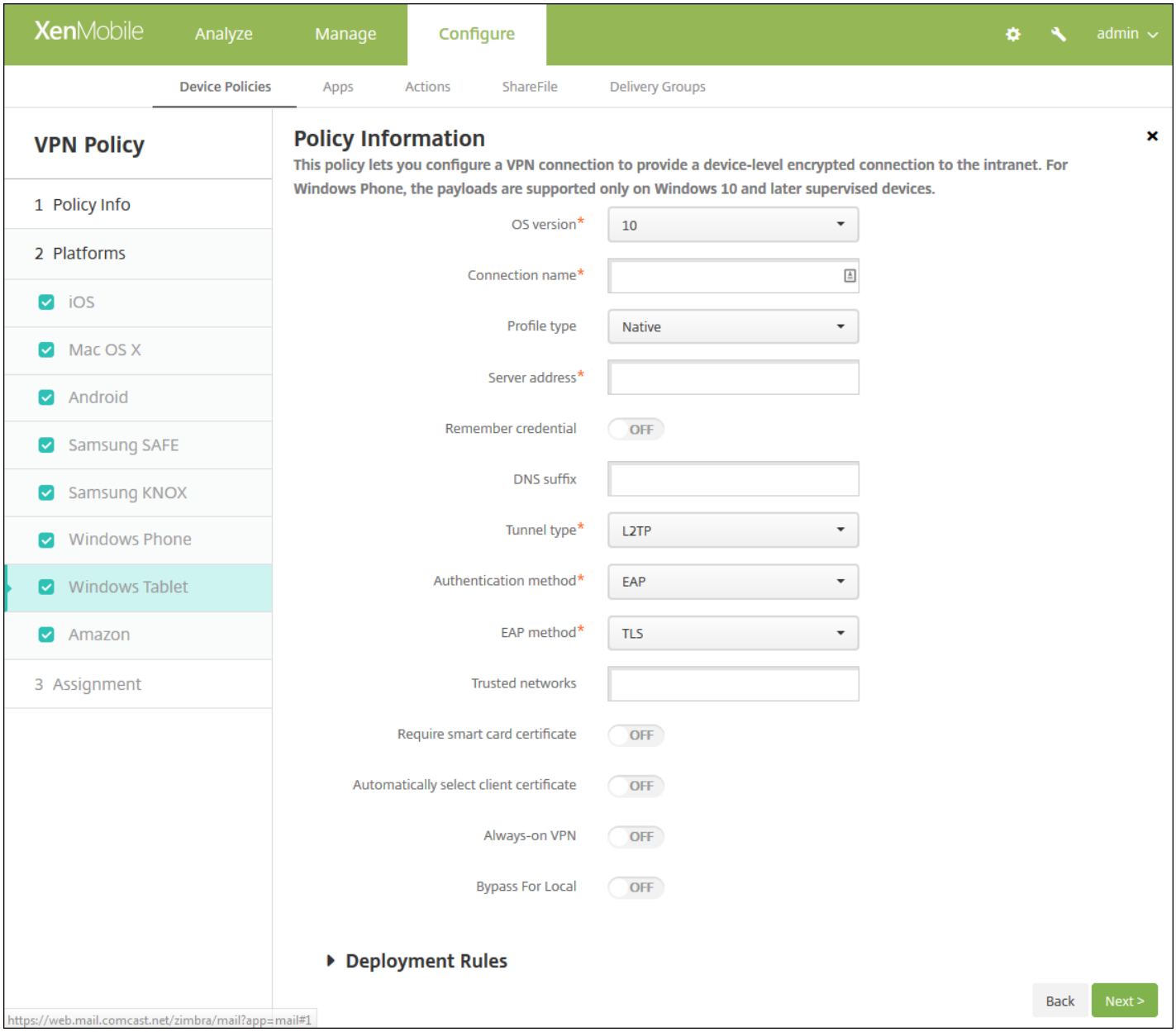
Note: These settings are supported only on Window 10 and later supervised phones.

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.

Configure Windows Tablet settings



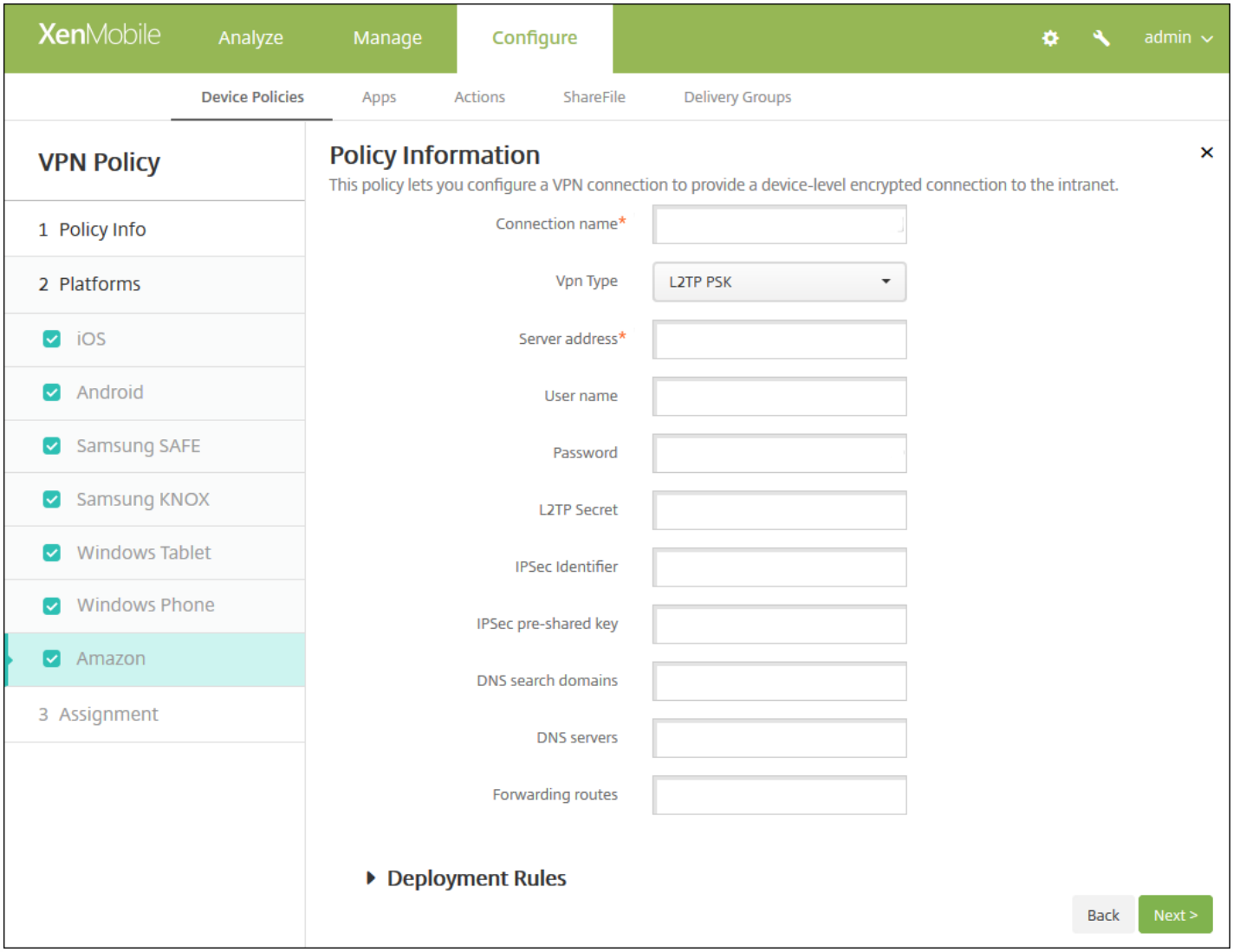
Configure these settings:

- **OS Version**: In the list, click either **8.1** for Windows 8.1 or **10** for Windows 10. The default is **10**.

Configure Windows 10 settings

Configure Windows 8.1 settings

Configure Amazon settings



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

Configure L2TP RSA settings

Configure IPSEC XAUTH PSK settings

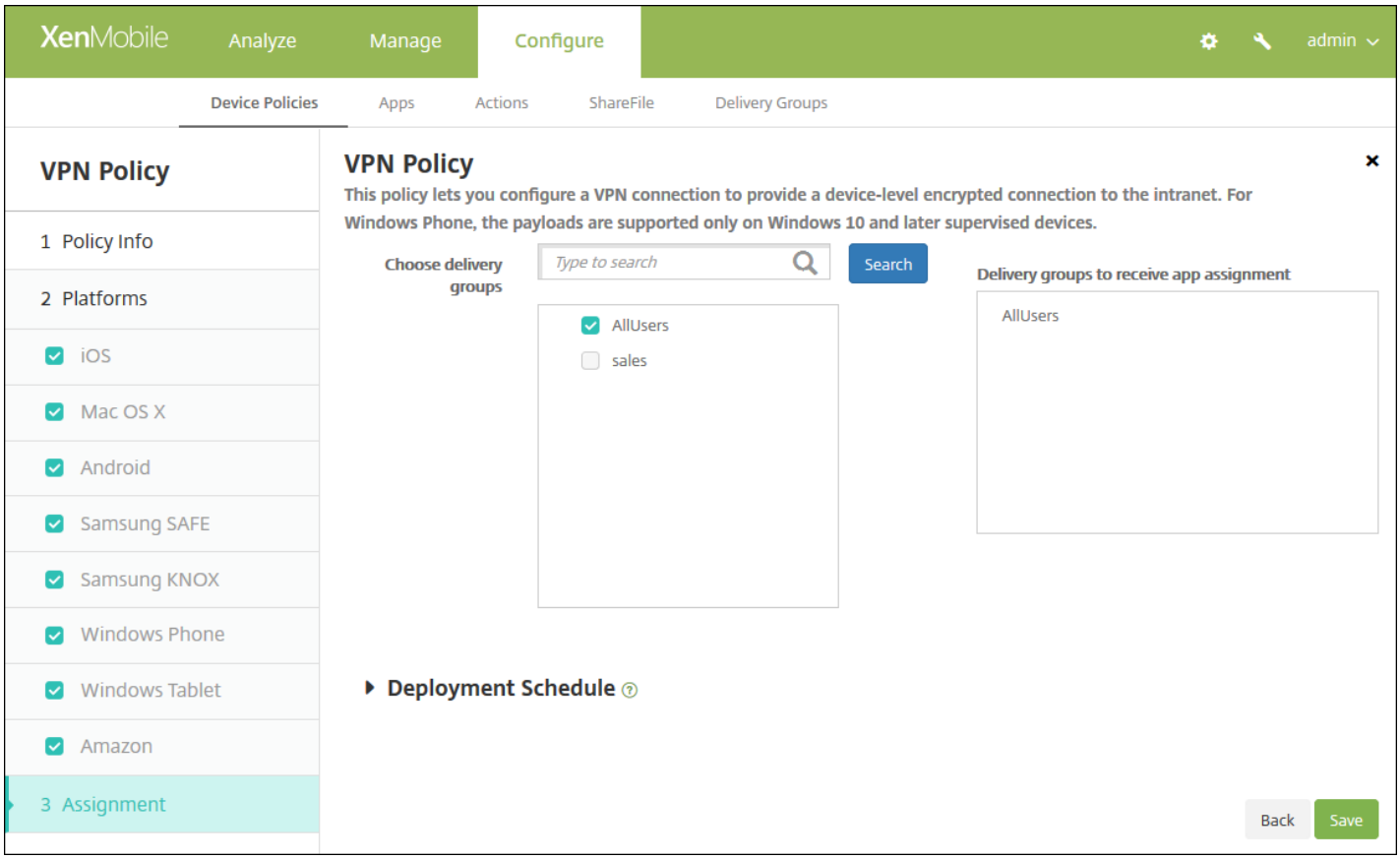
Configure IPSEC AUTH RSA settings

Configure IPSEC HYBRID RSA settings

Configure PPTP settings

7. Configure the deployment rules

8. Click **Next**, the **VPN 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**. 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:

- 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**.

Wallpaper device policy

Nov 16, 2016

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.

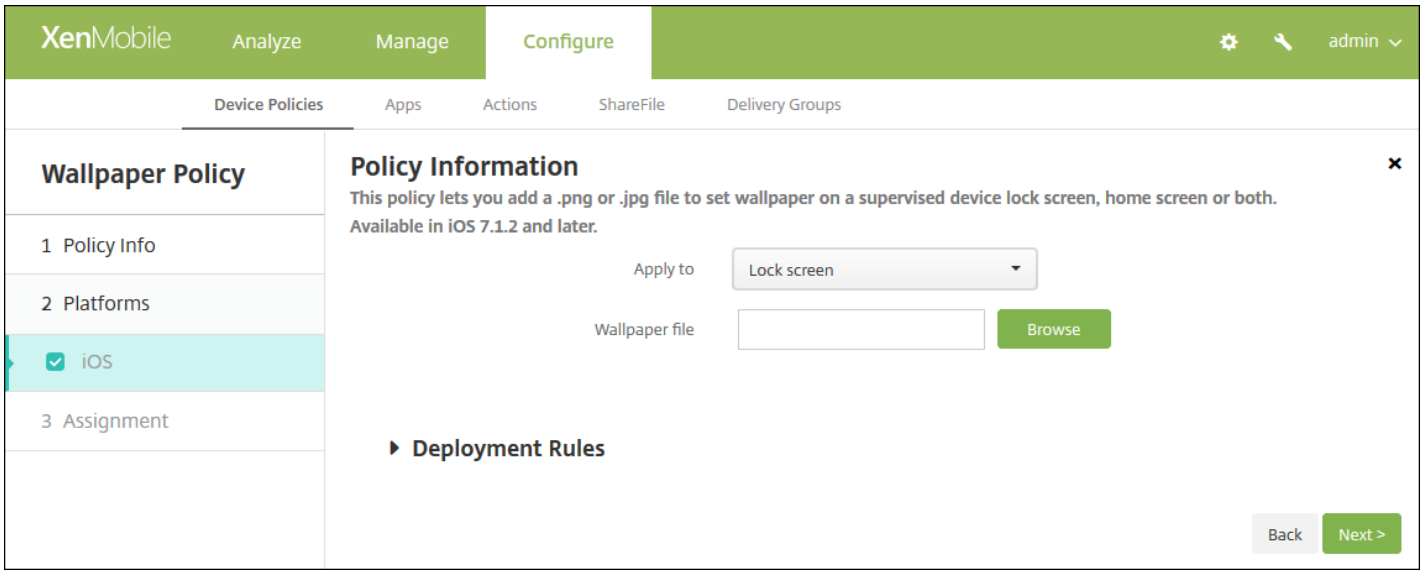
2. Click **Add**. The **Add a New Policy** dialog box appears.

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.

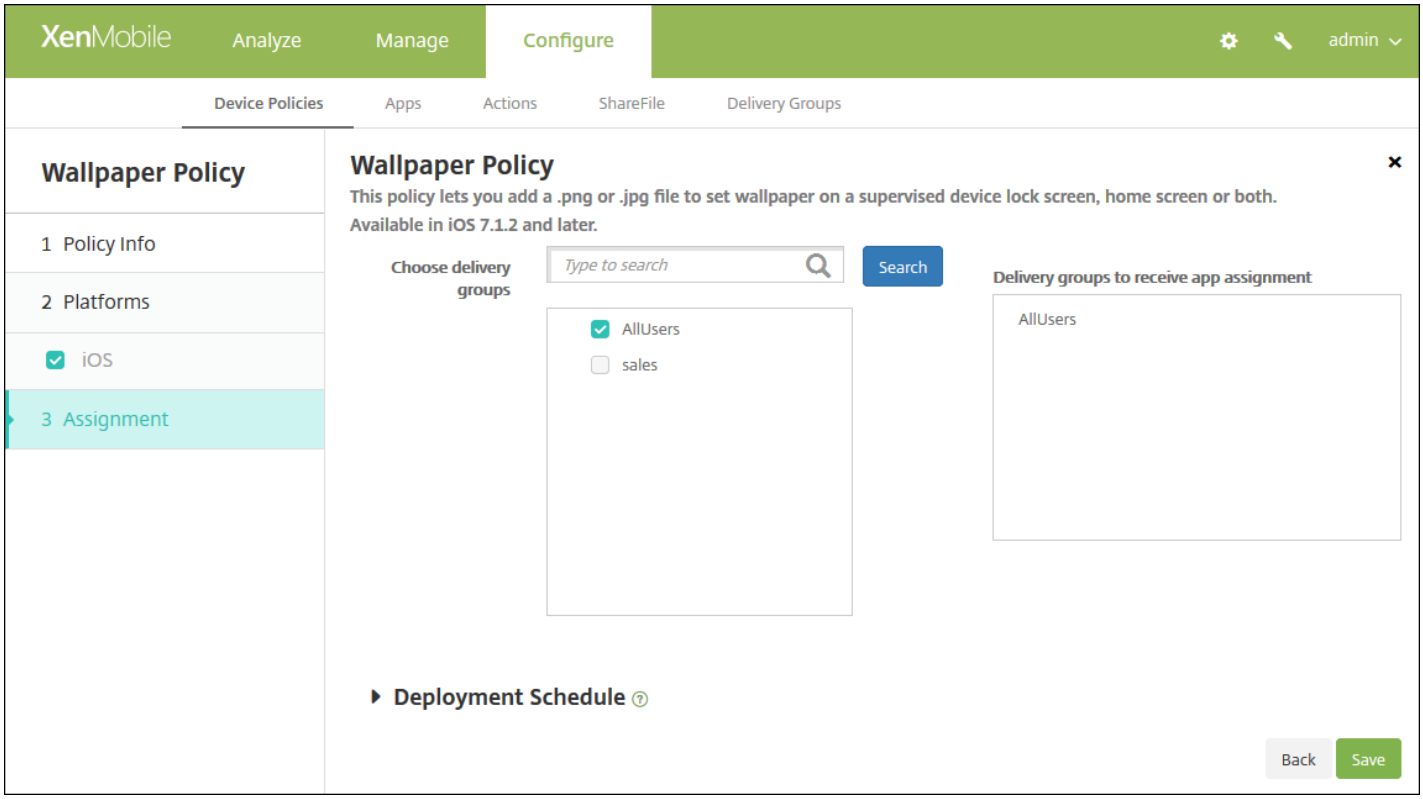


Configure these settings:

- **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 the deployment rules

8. Click **Next**. The **Wallpaper 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**.

Web content filter device policy

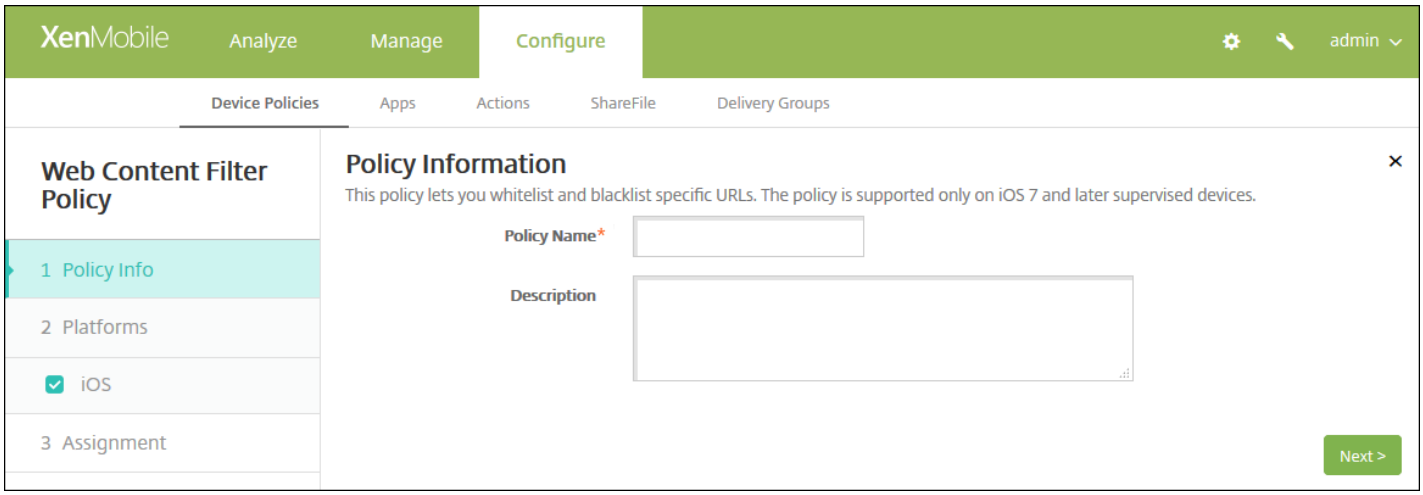
Nov 16, 2016

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.

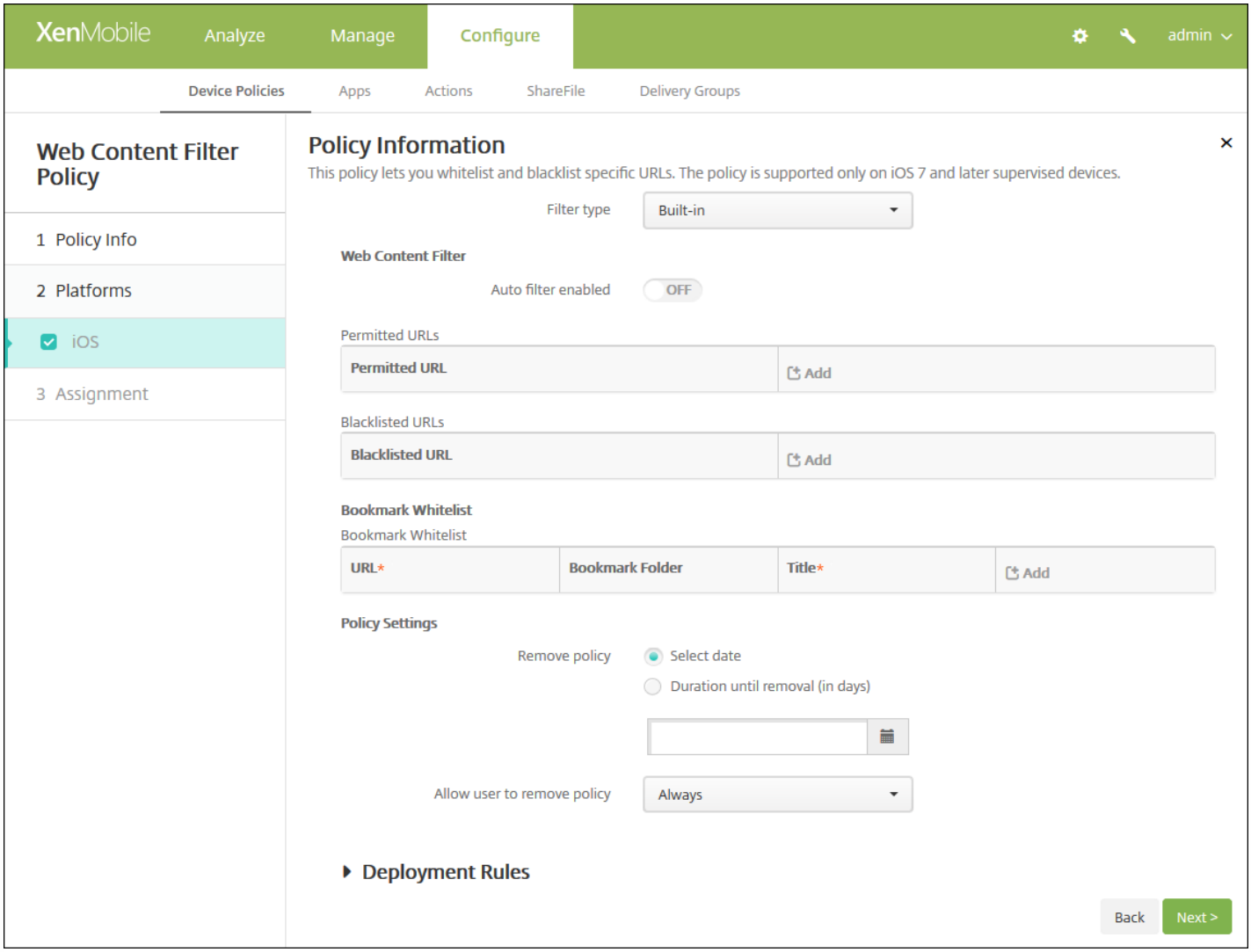
3. Click **More** and then, under **Security**, click **Web Content Filter**. The **Web Content Filter Policy** page appears.



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**.

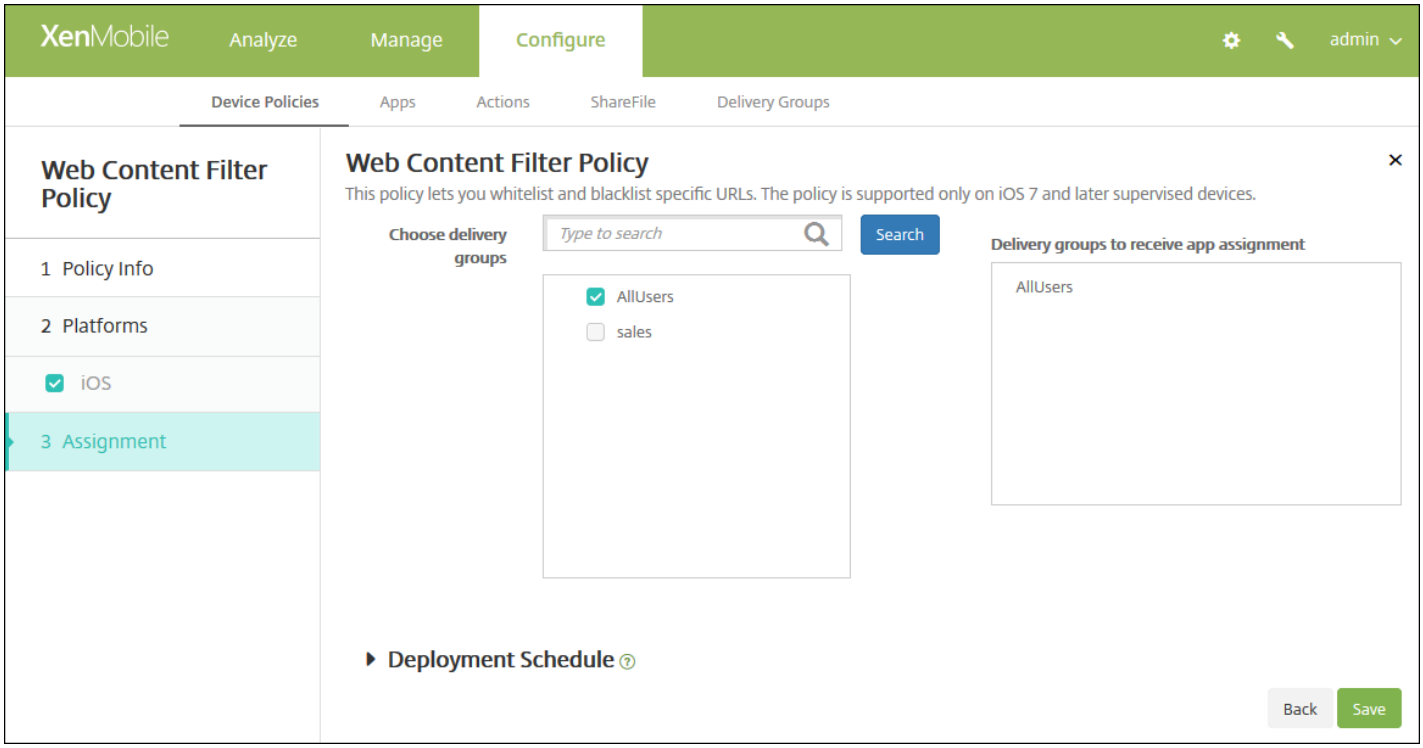
Built-in filter type settings

Plug-in filter type settings

- **Policy Settings**
  - Next to **Remove policy**, click either **Select date** or **Duration until removal (in days)**.
  - 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 the deployment rules

8. Click **Next**. The **Web Content Filter 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**.

Webclip device policy

Nov 16, 2016

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, Mac OS X, and Android devices; Windows tablet only requires a label and a URL.

iOS settings

Mac OS X settings

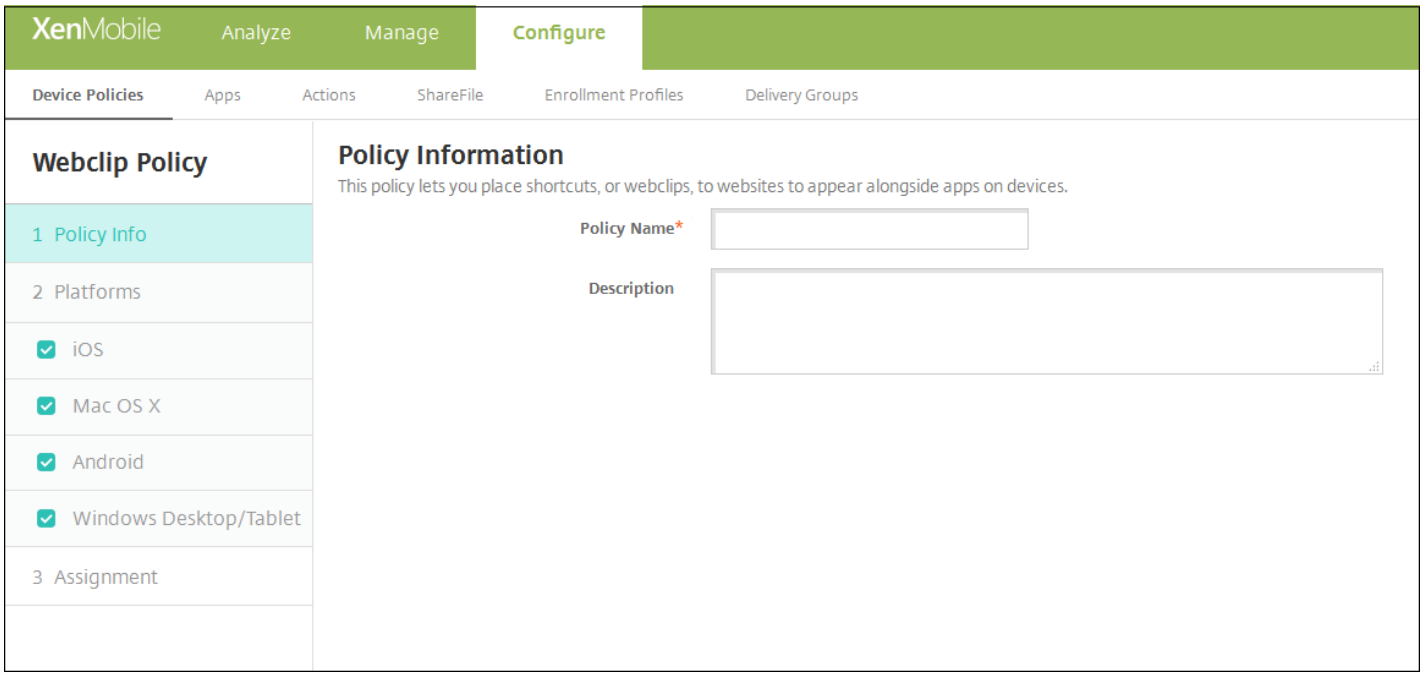
Android settings

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:

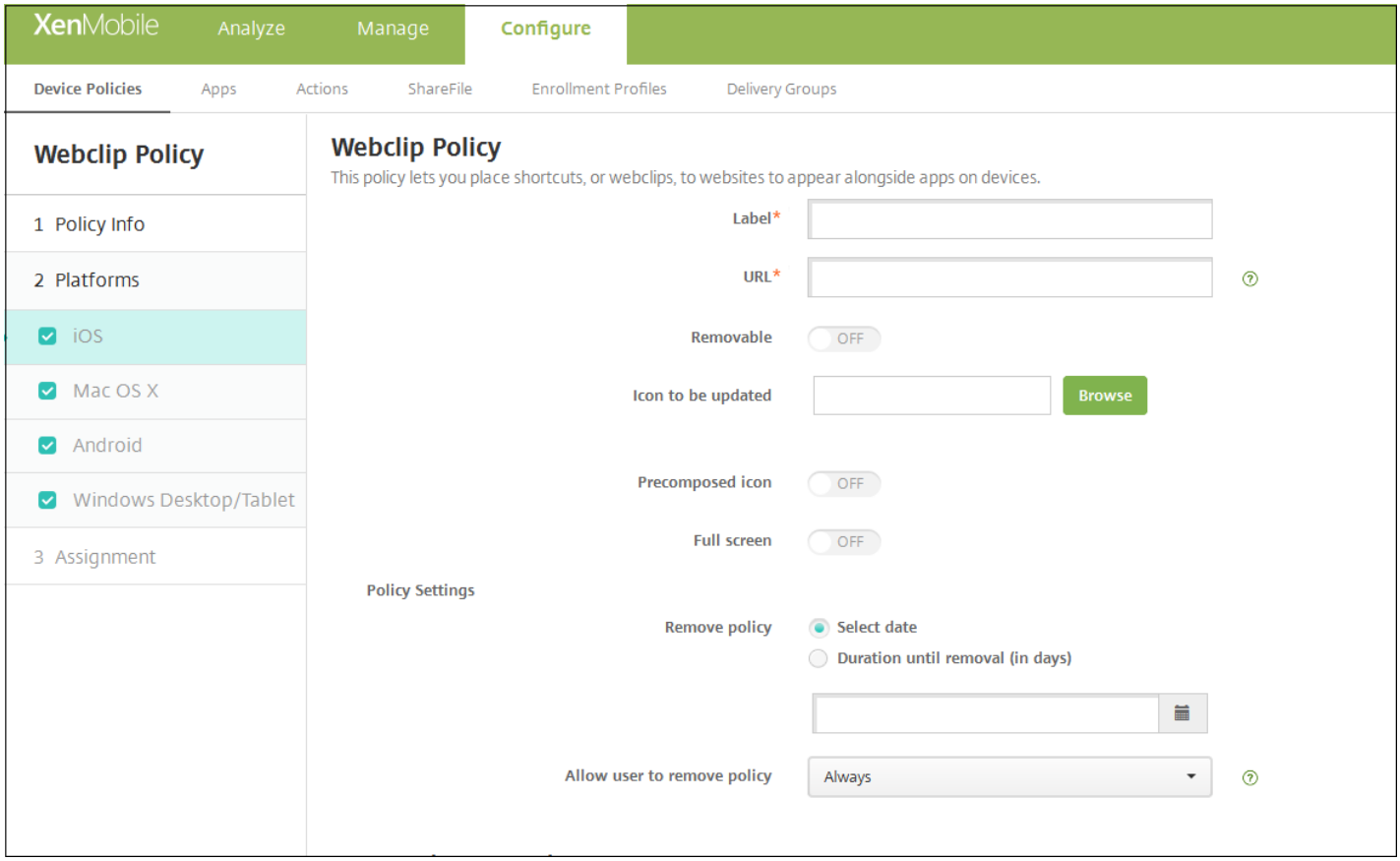
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

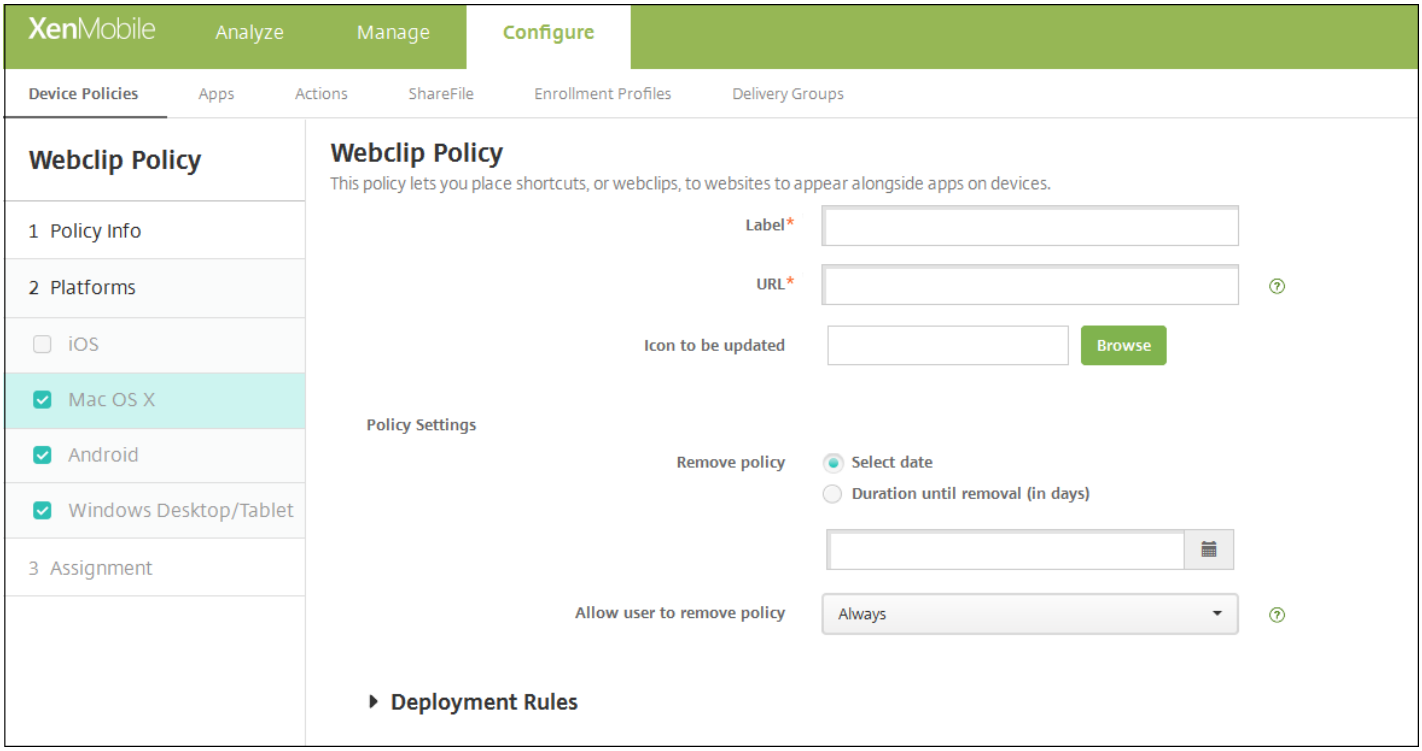
Configure iOS settings



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 days)**.
  - 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.

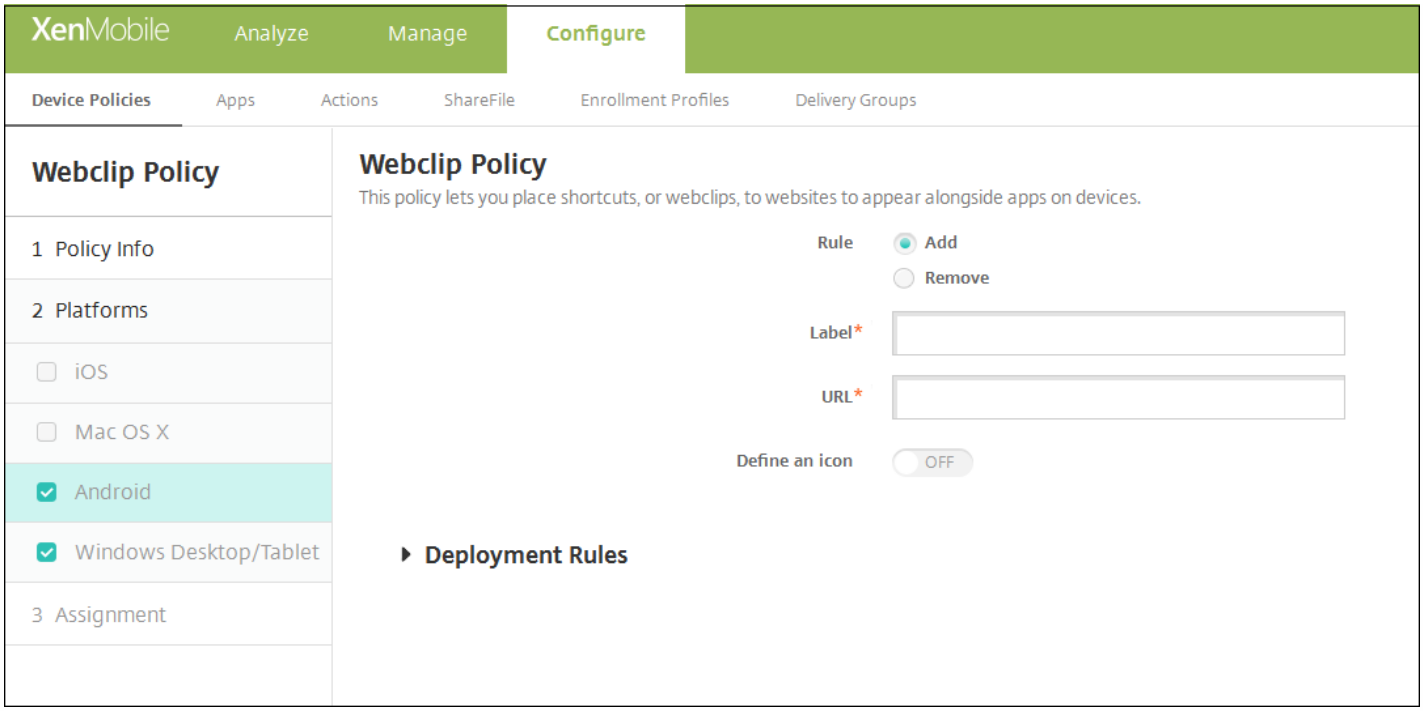
Configure Mac OS X settings



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 days)**.
  - 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 OS X 10.7 and later.

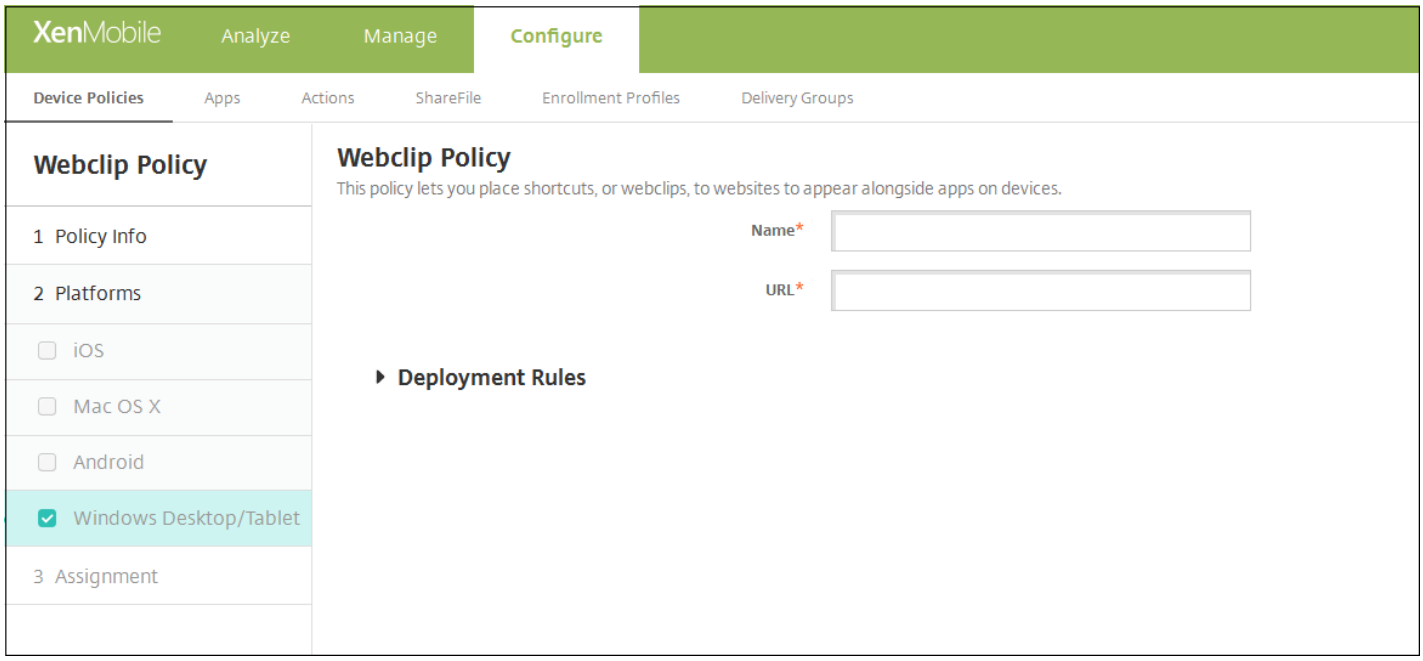
Configure Android settings



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 Windows Desktop/Tablet settings

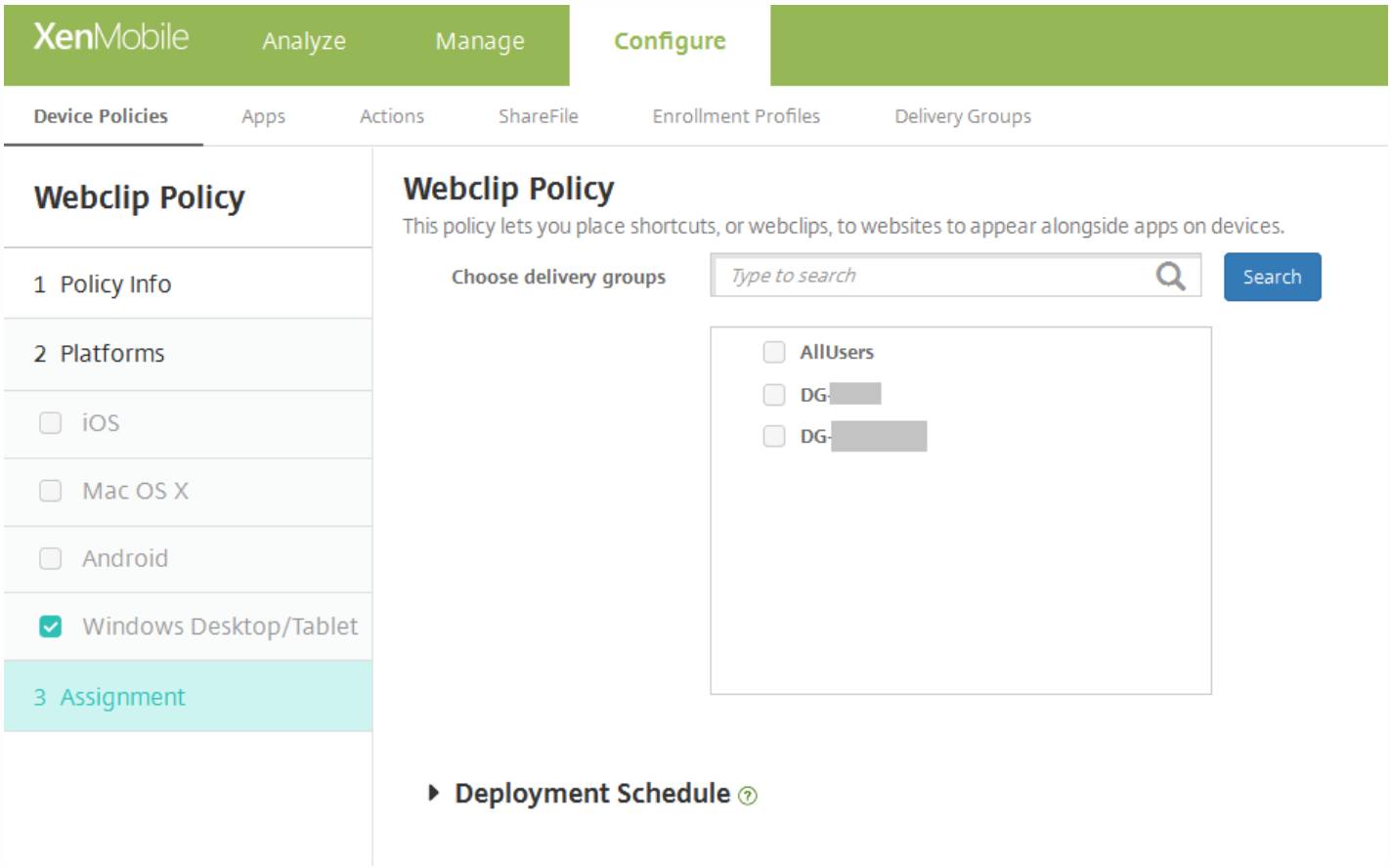


Configure these settings:

- **Name**: Type the label that is to appear with the webclip.
- **URL**: Type the URL associated with the webclip.

7. Configure the deployment rules

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

Jan 12, 2017

You create new or edit existing WiFi device policies in XenMobile by using the **Configure > Device Policies** page of the XenMobile console. WiFi policies let you manage how users connect their devices to WiFi networks by defining network names and types, authentication and security policies, proxy server use, and other WiFi-related details consistently for all users on device platforms you select.

You can configure WiFi settings for users for the following platforms: iOS, Mac OS X, Android (which includes devices enabled for Android for Work), Windows Phone, and Windows Desktop/Tablet. Each platform requires a different set of values, which are described in detail in this article.

Important

Before you create a new policy, be sure you complete these steps:

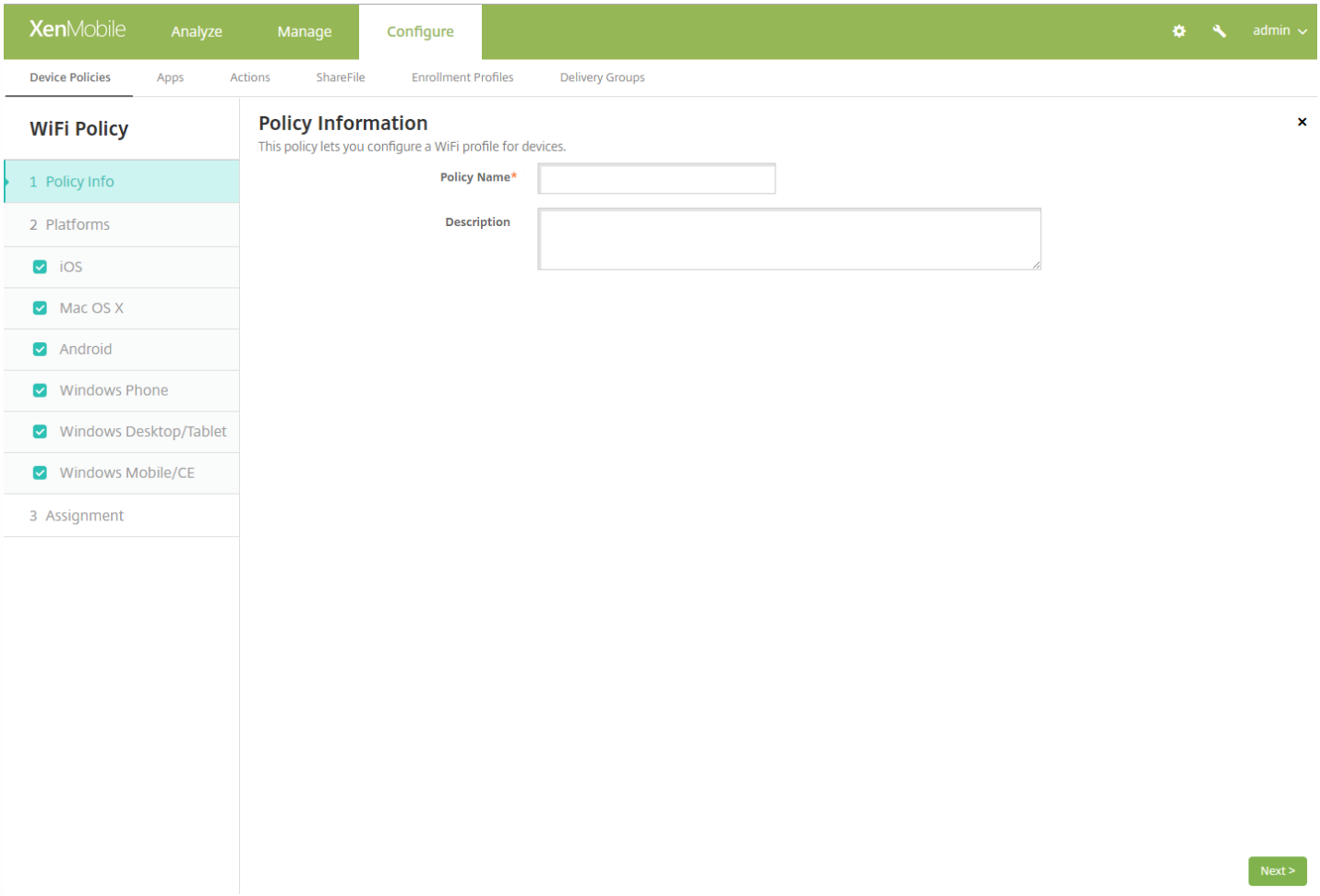
- Create any deployment groups you plan to use.
- Know the network name and type.
- Know any authentication or security types you plan to use.
- Know any proxy server information you may need.
- Install any necessary CA certificates.
- Have any necessary shared keys.
- Create the PKI entity for certificate-based authentication.
- Configure credential providers.

For more information, see Authentication and its sub-articles.

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, enter the following information:

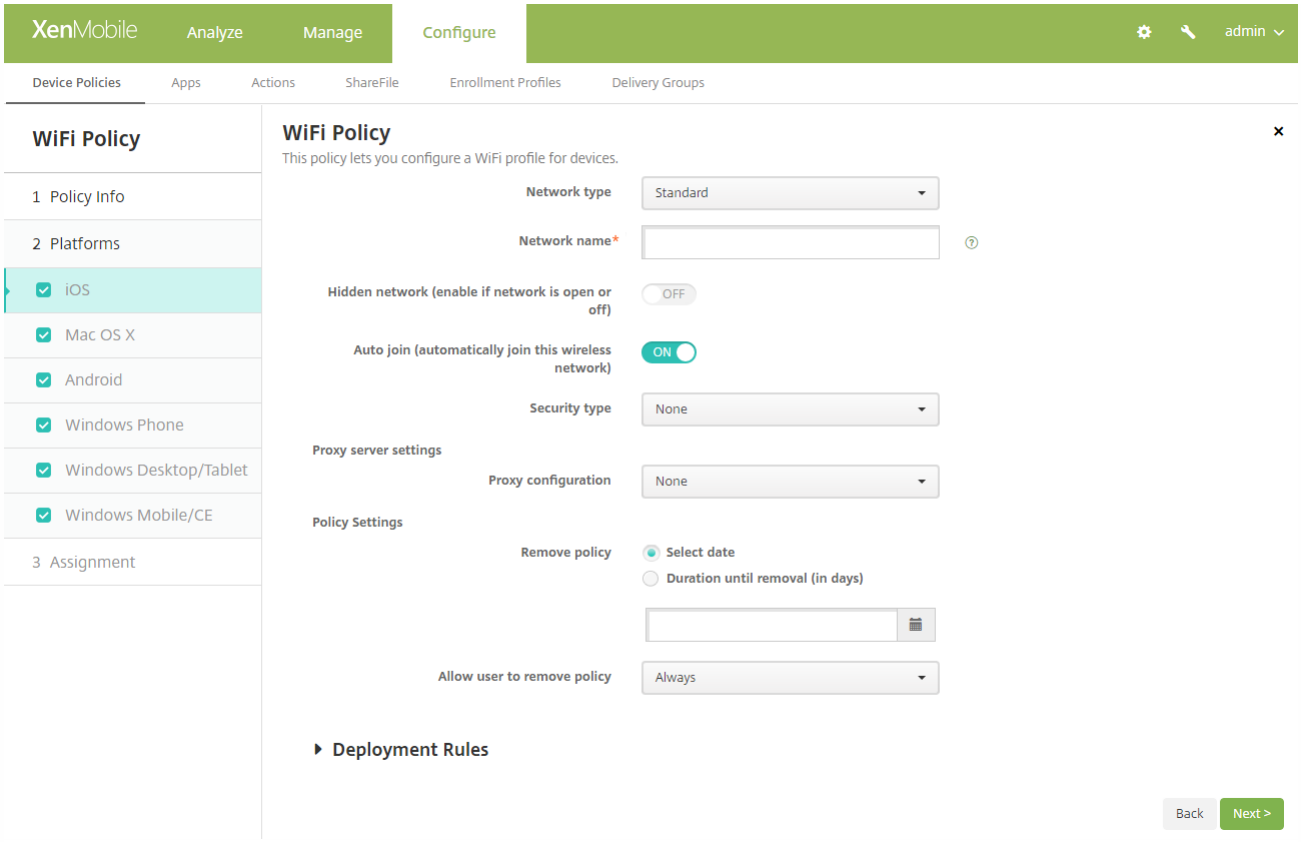
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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:

- **Network type**: In the list, click **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 device's list of available networks. Does not apply to **Hotspot 2.0**.
- **Hidden network (enable if network is open or off)**: Select whether the network is hidden.
- **Auto Join (automatically join this wireless network)**: Select whether the network is joined automatically. The default is **ON**.
- **Security type**: In the list, click 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.

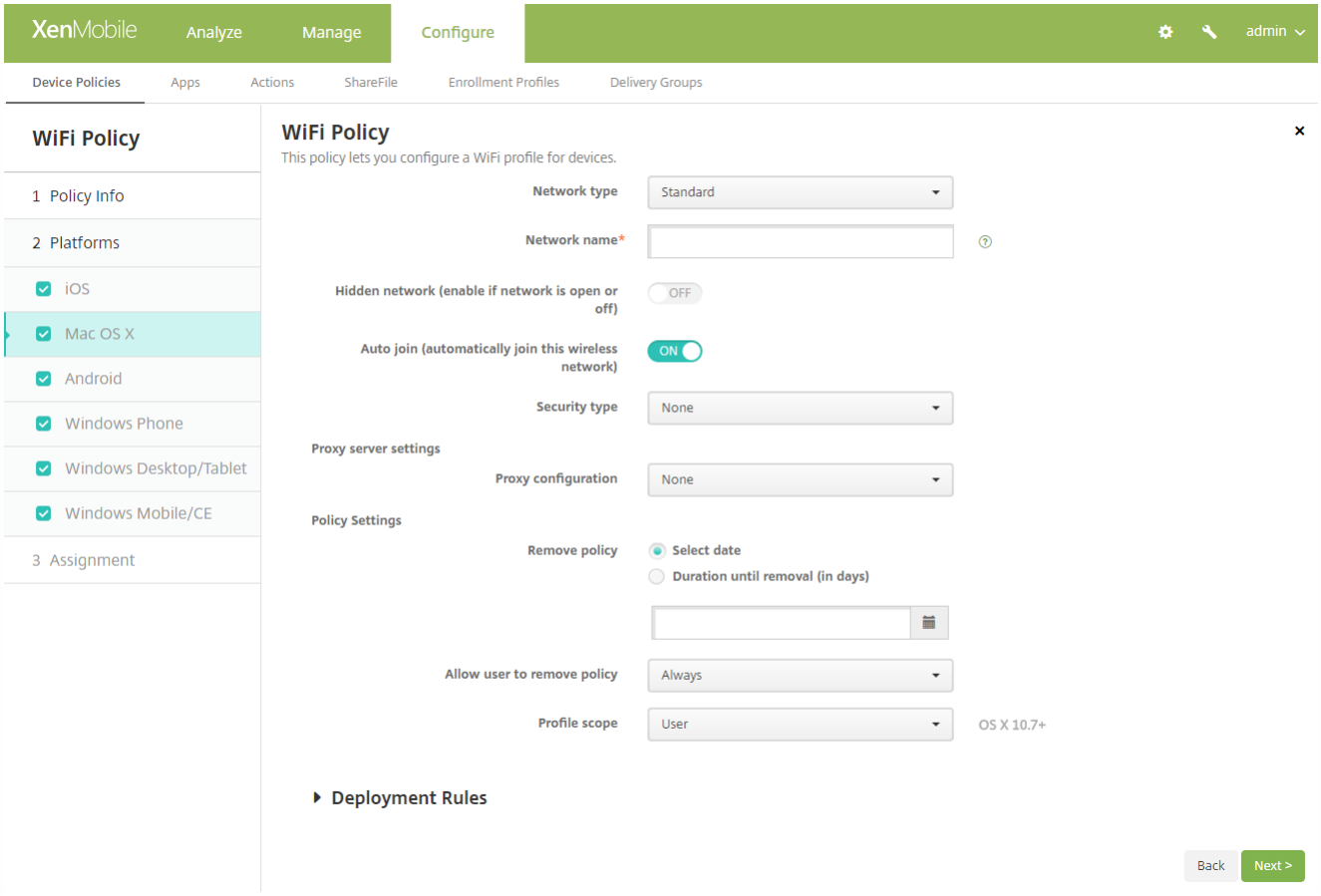
WPA, WPA Personal, Any (Personal)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise)

- **Proxy server settings**
  - **Proxy configuration**: In the list, click 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 click **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 click **Automatic**, configure these settings:
    - **Server 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.

- **Policy Settings**
  - Next to **Remove policy**, click either **Select date** or **Duration until removal (in days)**.
  - 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 Mac OS X settings



Configure these settings:

- **Network type**: In the list, click **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 device's list of available networks. Does not apply to **Hotspot 2.0**.
- **Hidden network (enable if network is open or off)**: Select whether the network is hidden.
- **Auto Join (automatically join this wireless network)**: Select whether the network is joined automatically. The default is **ON**.
- **Security type**: In the list, click 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.

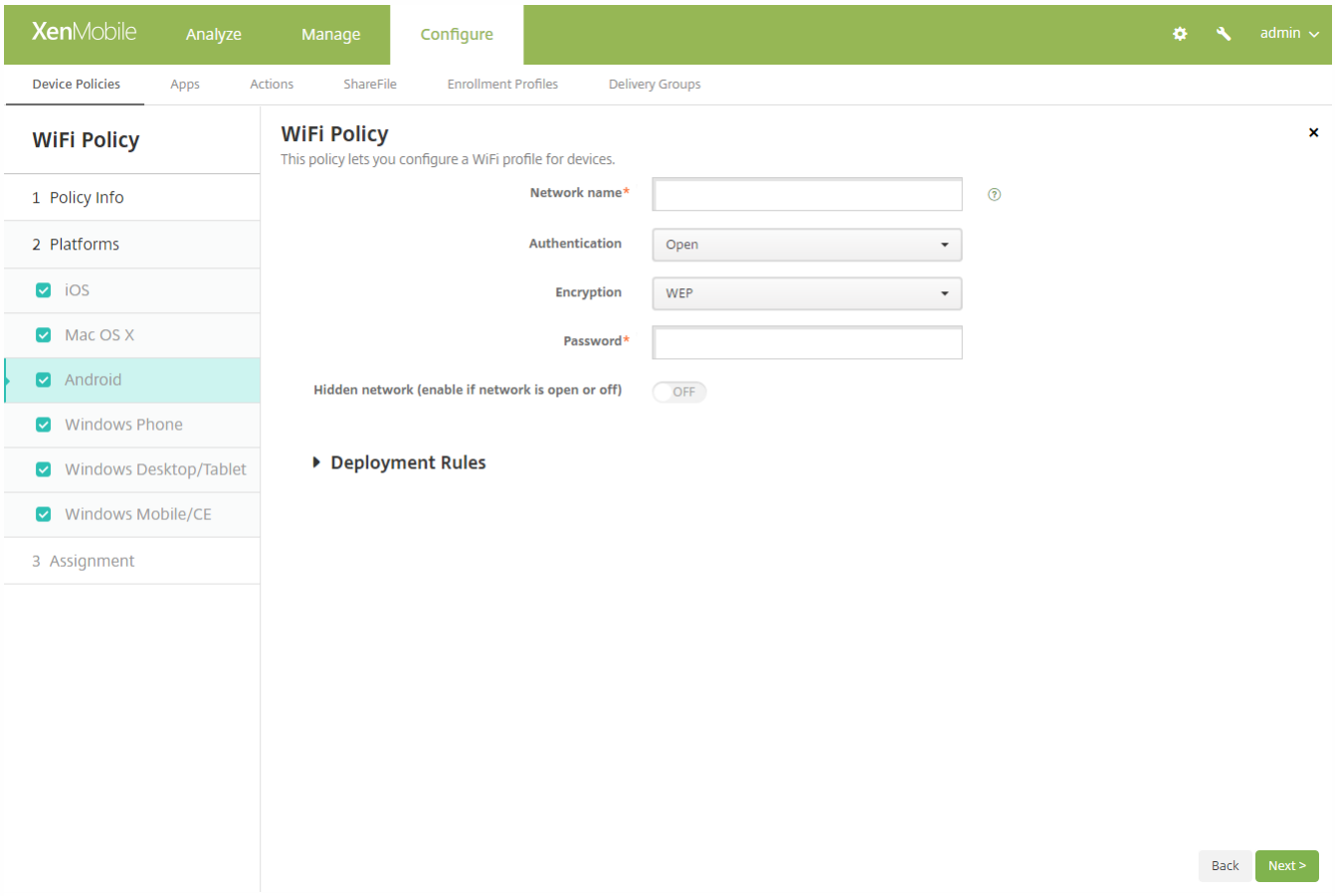
WPA, WPA Personal, WPA 2 Personal, Any (Personal)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise)

- **Use as a Login Window configuration**: Select whether to use the same credentials entered at the login window to authenticate the user.
- **Proxy server settings**
  - **Proxy configuration**: In the list, click 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 click **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 click **Automatic**, configure these settings:
    - **Server 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.
- **Policy Settings**
  - Next to **Remove policy**, click either **Select date** or **Duration until removal (in days)**.
  - 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 for OS X 10.7 and later.

Configure Android settings



Configure these settings:

- **Network name**: Type the SSID that is seen in the list of available networks on the user's device.
- **Authentication**: In the list, click 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.

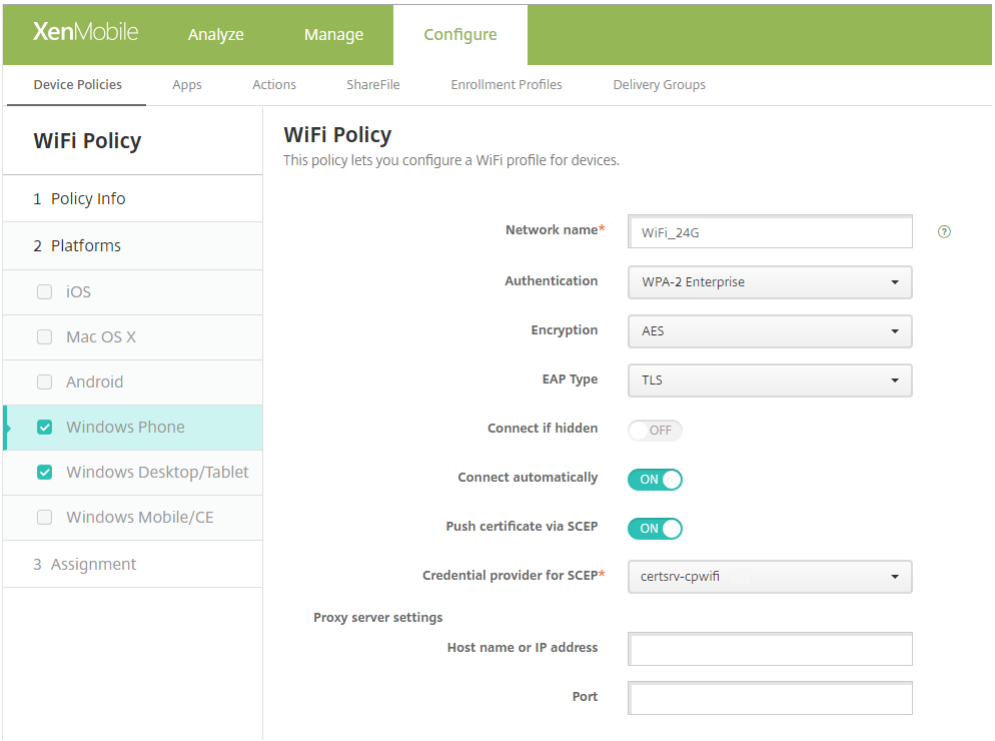
Open, Shared

WPA, WPA-PSK, WPA2, WPA2-PSK

802.1x

- **Hidden network (Enable if network is open or off)**: Select whether the network is hidden.

Configure Windows Phone settings



Configure these settings:

- **Network name**: Type the SSID that is seen in the list of available networks on the user's device.
- **Authentication**: In the list, click 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 so that XenMobile can 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.

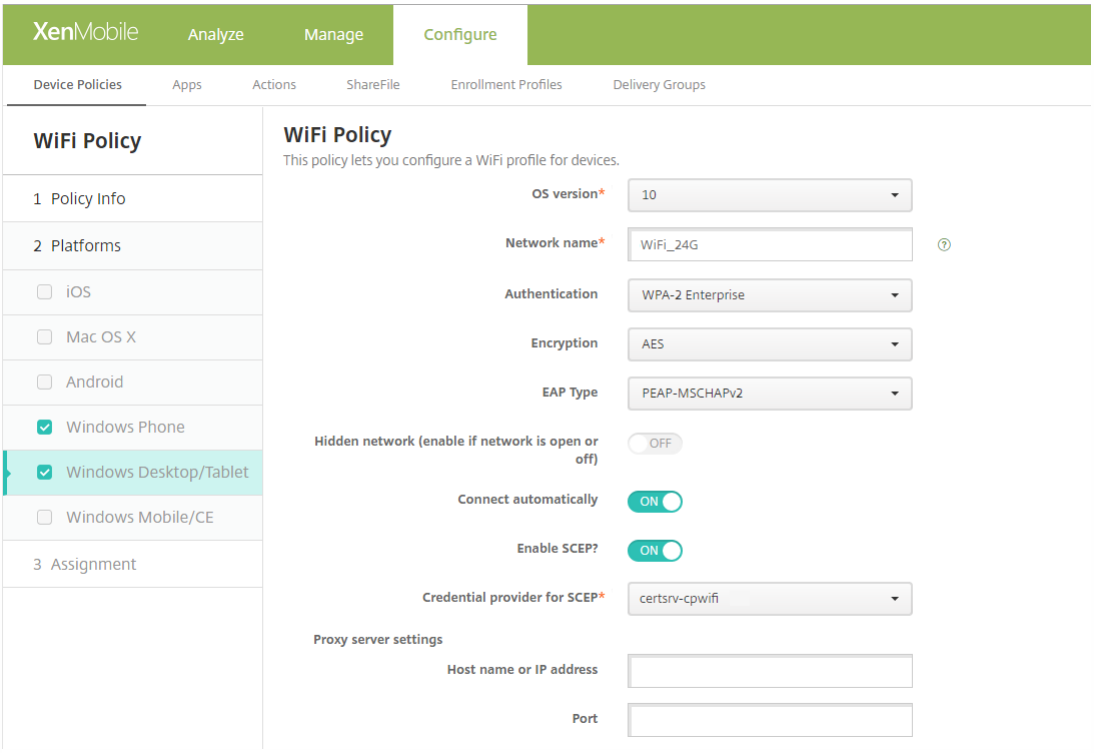
Open

WPA Personal, WPA-2 Personal

WPA-2 Enterprise

- **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.

Configure Windows Desktop/Tablet settings



Configure the following settings:

- **OS version**: In the list, click either **8.1** for Windows 8.1 or **10** for Windows 10. The default is **10**.

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 so that XenMobile can 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

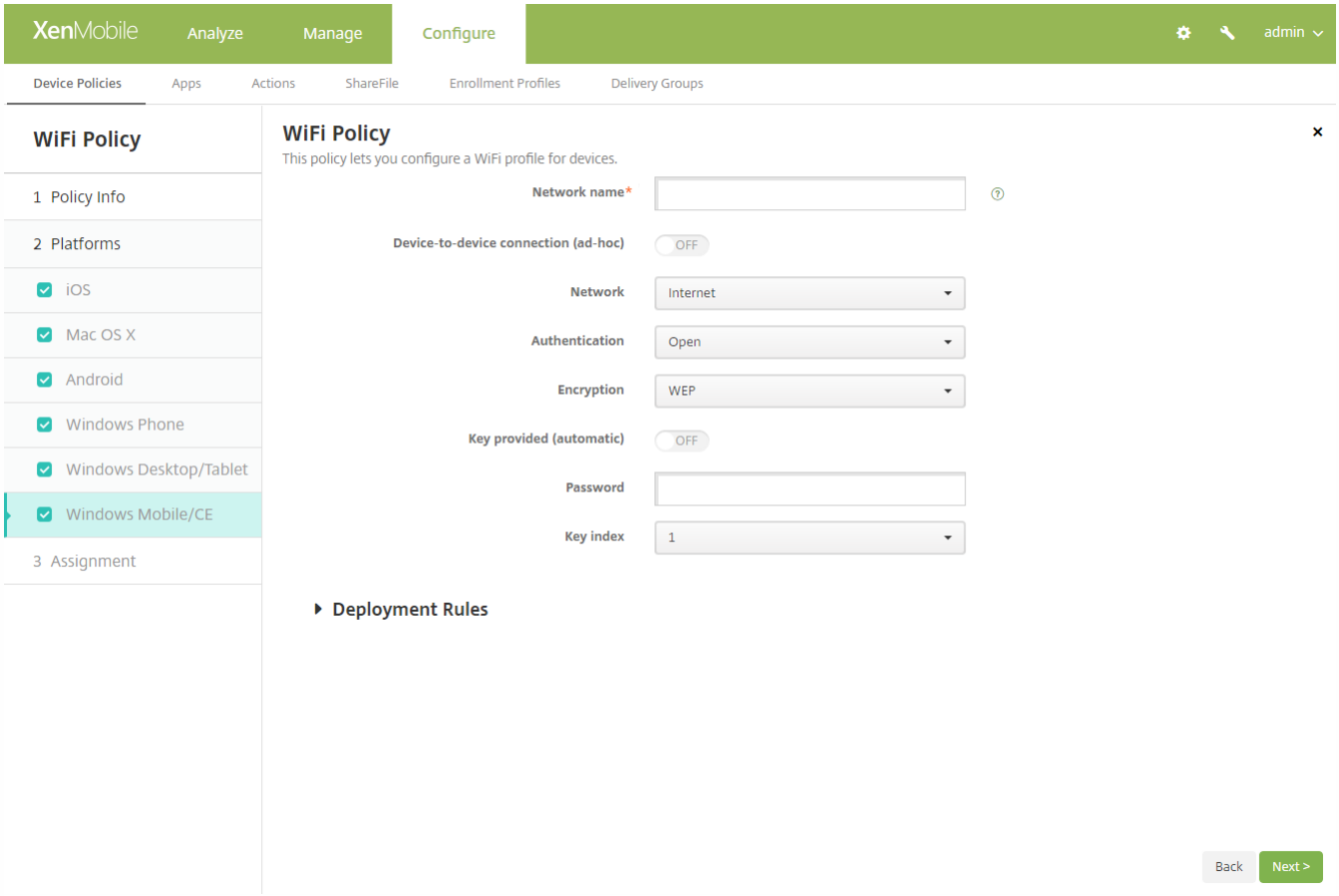
WPA Personal, WPA-2 Personal

WPA-2 Enterprise

Windows 8.1 settings

- **Network name**: Type the SSID that is seen in the list of available networks on the user's device.
- **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
- **Hidden network (Enable if network is open or off)**: Select whether the network is hidden.
- **Connect automatically**: Select whether to connect to the network automatically.

Configure Windows Mobile/CE



Configure these settings:

- **Network name**: Type the SSID that is seen in the list of available networks on the user's device.
- **Device-to-device connection (ad-hoc)**: Allows two devices to connect directly. Default is **Off**.
- **Network**: Select whether the device is connected to an external internet source or an Office intranet.
- **Authentication**: In the list, click 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

WPA Personal, WPA-2 Personal

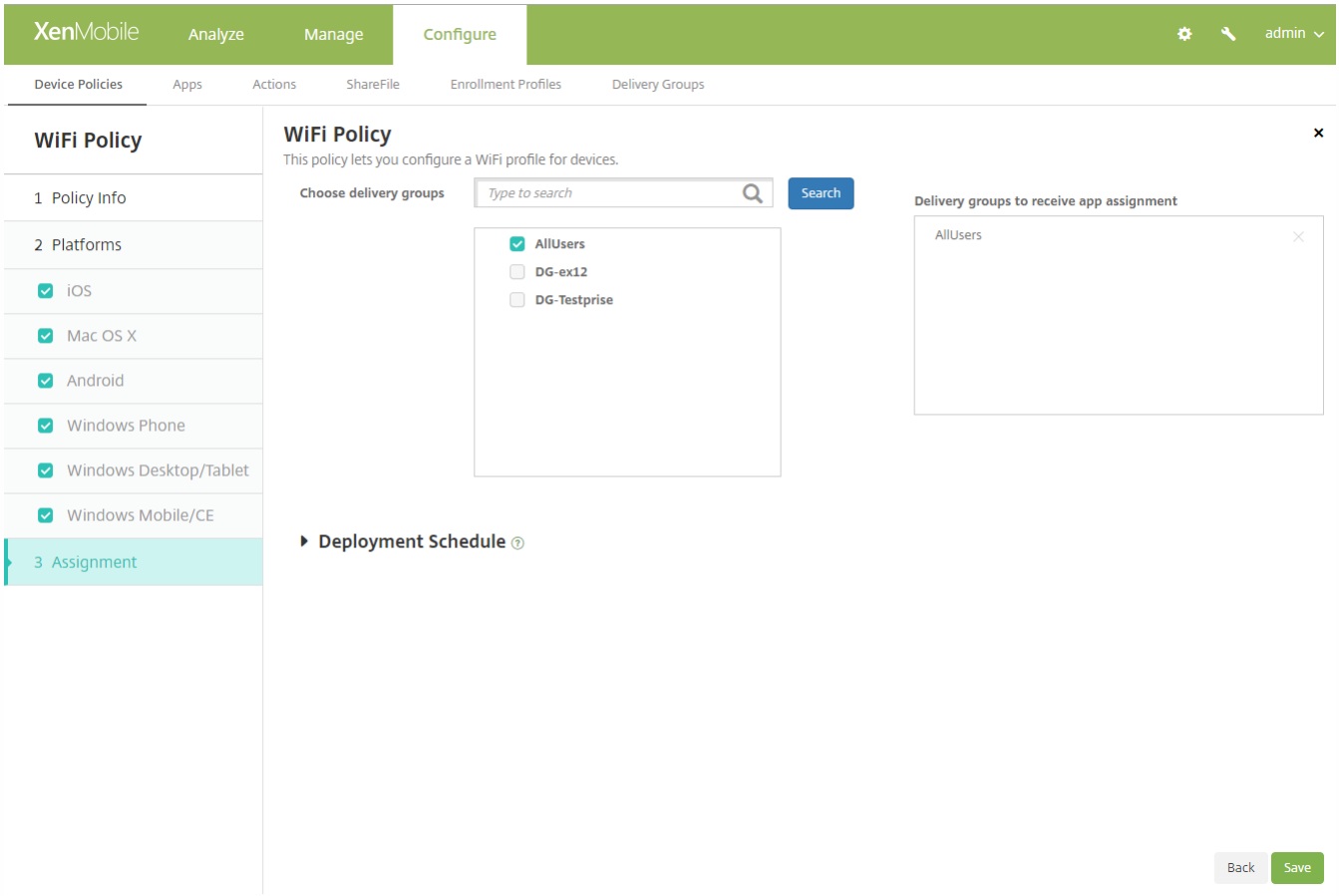
WPA-2 Enterprise

- **Key provided (automatic)**: Select whether the key is automatically provided or not. Default is **Off**.
- **Password**: Enter the password in this field.
- **Key index**: Indicate the key index. Available options are 1, 2, 3, and 4.

7. Configure the deployment rules

8. Click **Next**. The **WiFi Policy Assignment** page appears.

8. Click **Next**. The WiFi Policy **Assignment** page appears.
8. Click **Next**. The WiFi Policy **Assignment** page appears.
8. Click **Next**. The WiFi 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 CE certificate device policy

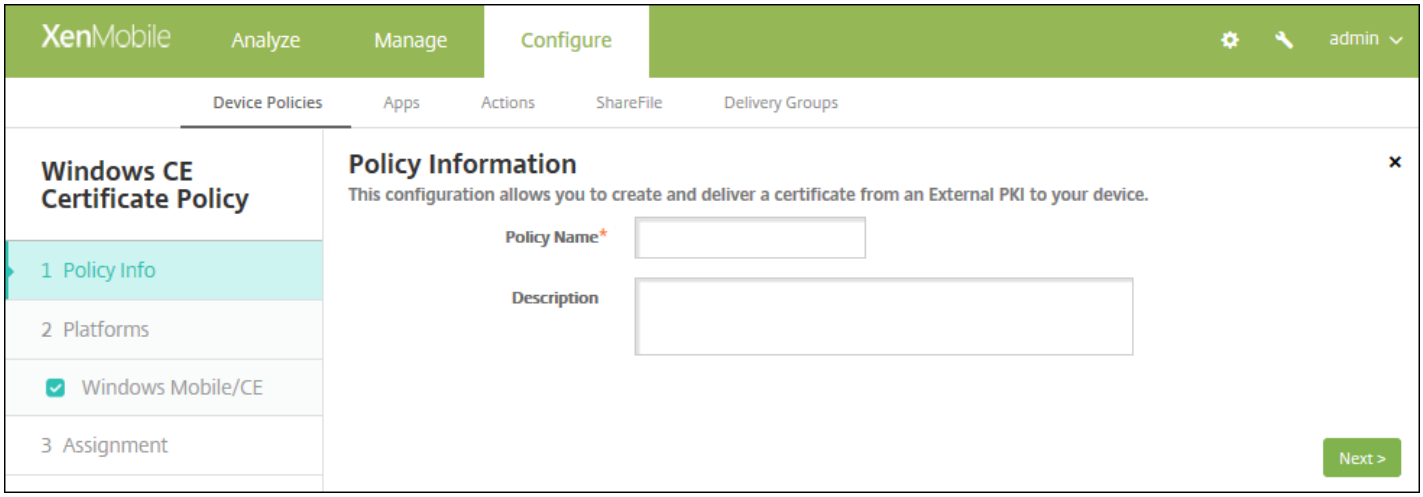
Nov 16, 2016

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.

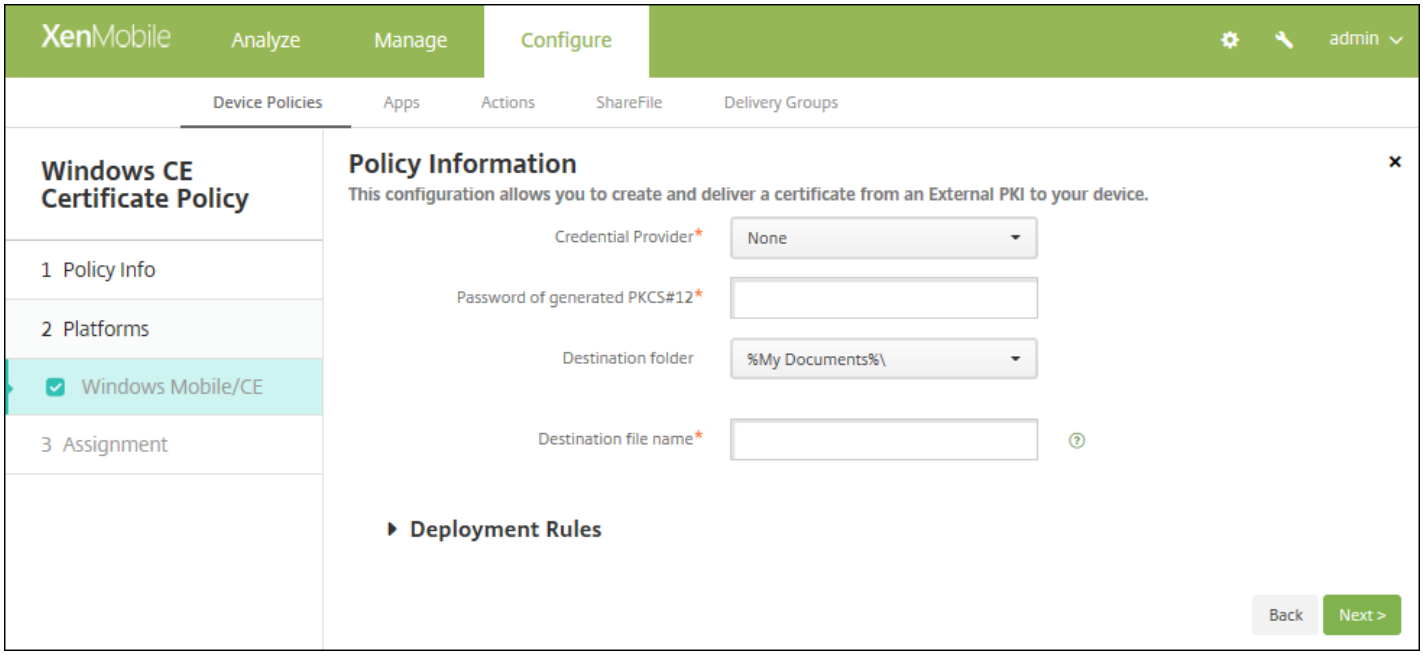
3. Expand **More** and then, under **Security**, click **Windows CE Certificate**. The **Windows CE Certificate Policy** information page appears.



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.

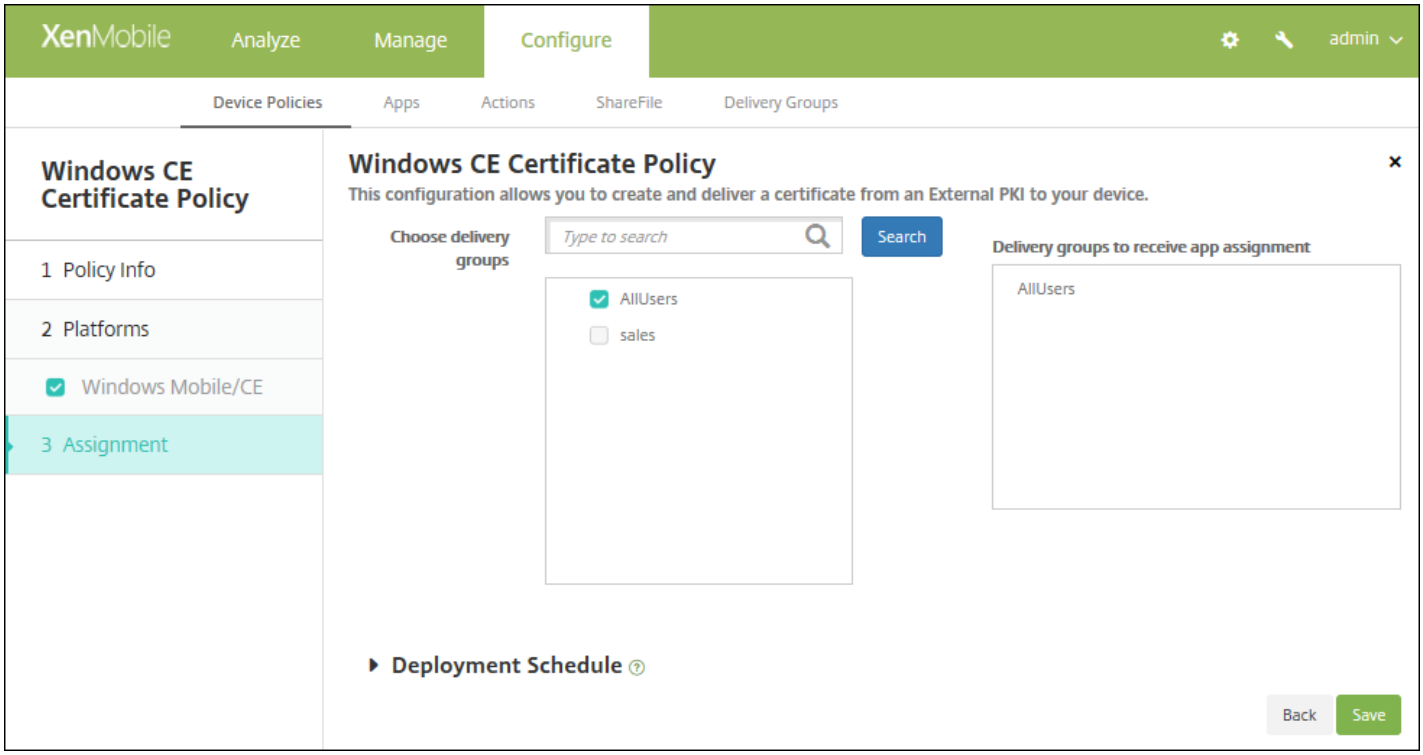


6. Configure these settings:

- **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 the deployment rules

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**.

Store device policy

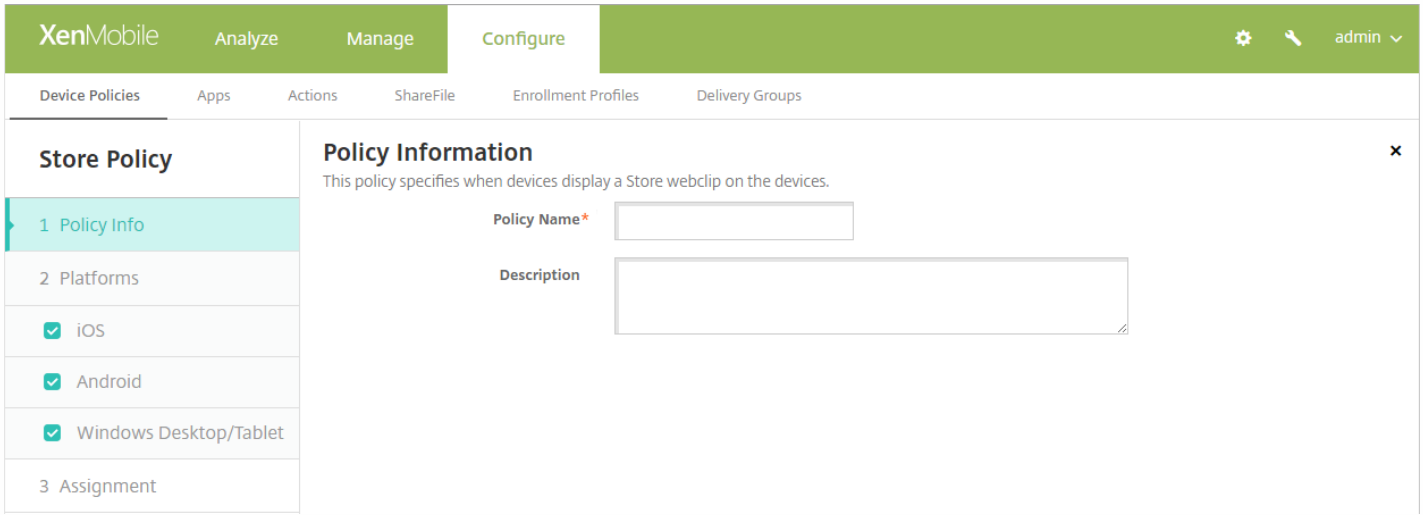
Feb 16, 2017

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.

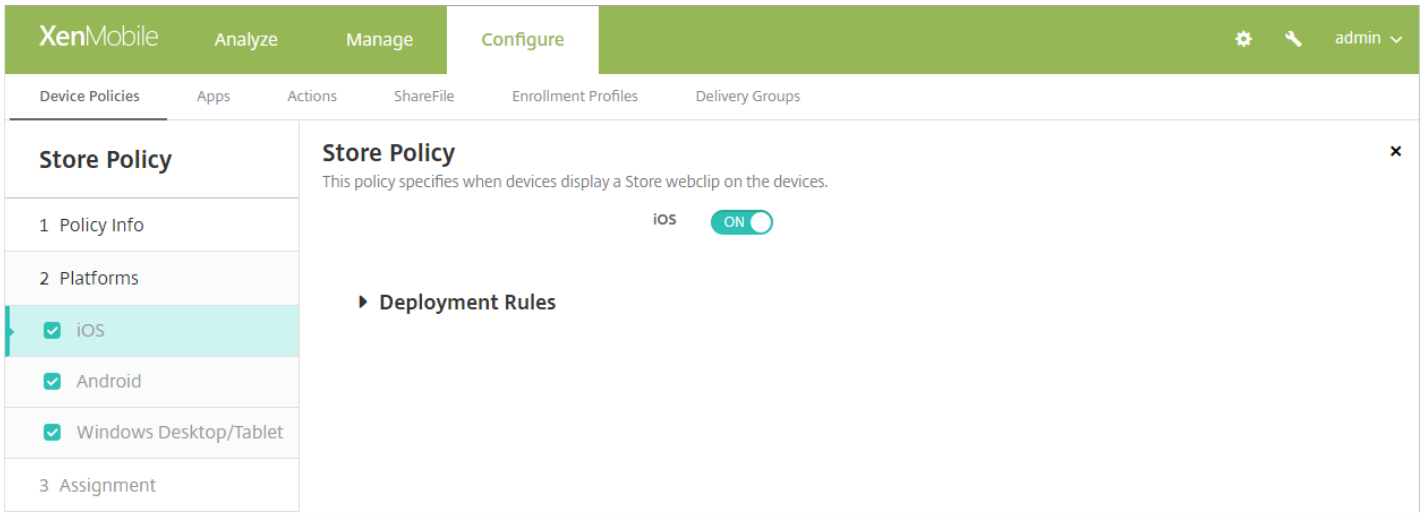
3. Expand **More**, and then under **Apps**, click **Store**. The **Store Policy** page appears.



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.

8. Configure the deployment rules

9. Click **Next**, the **XenMobile Store 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 right-hand **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**. 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.

12. Click **Save**.

XenMobile options device policy

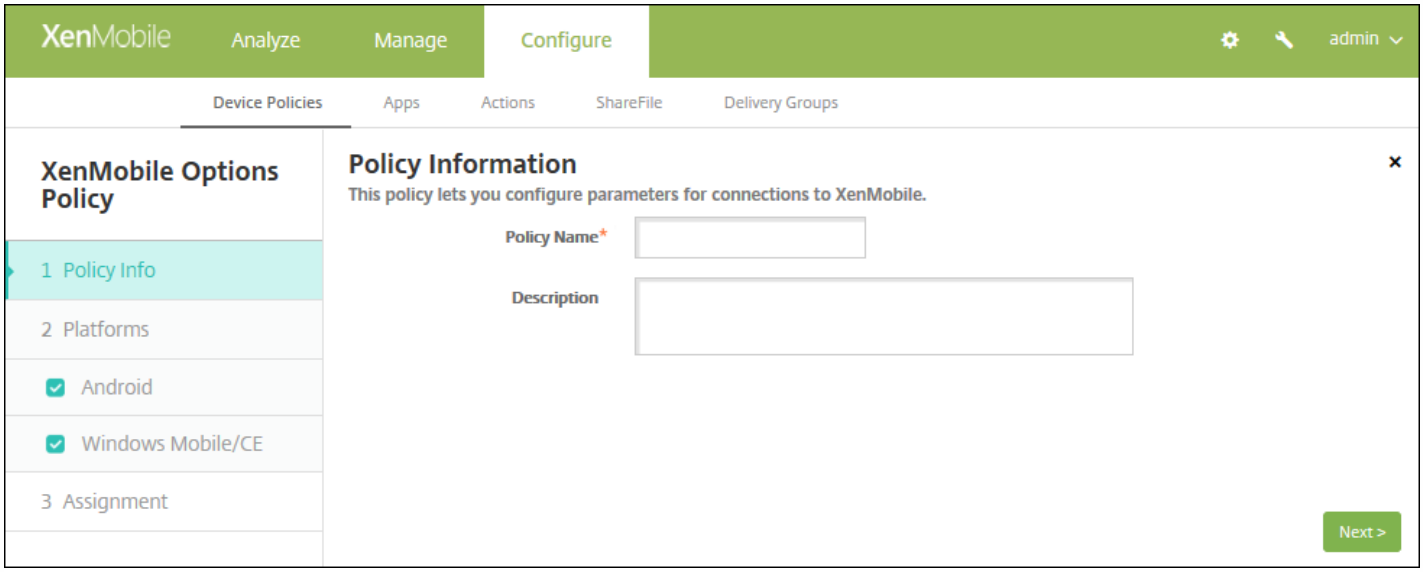
Nov 16, 2016

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:

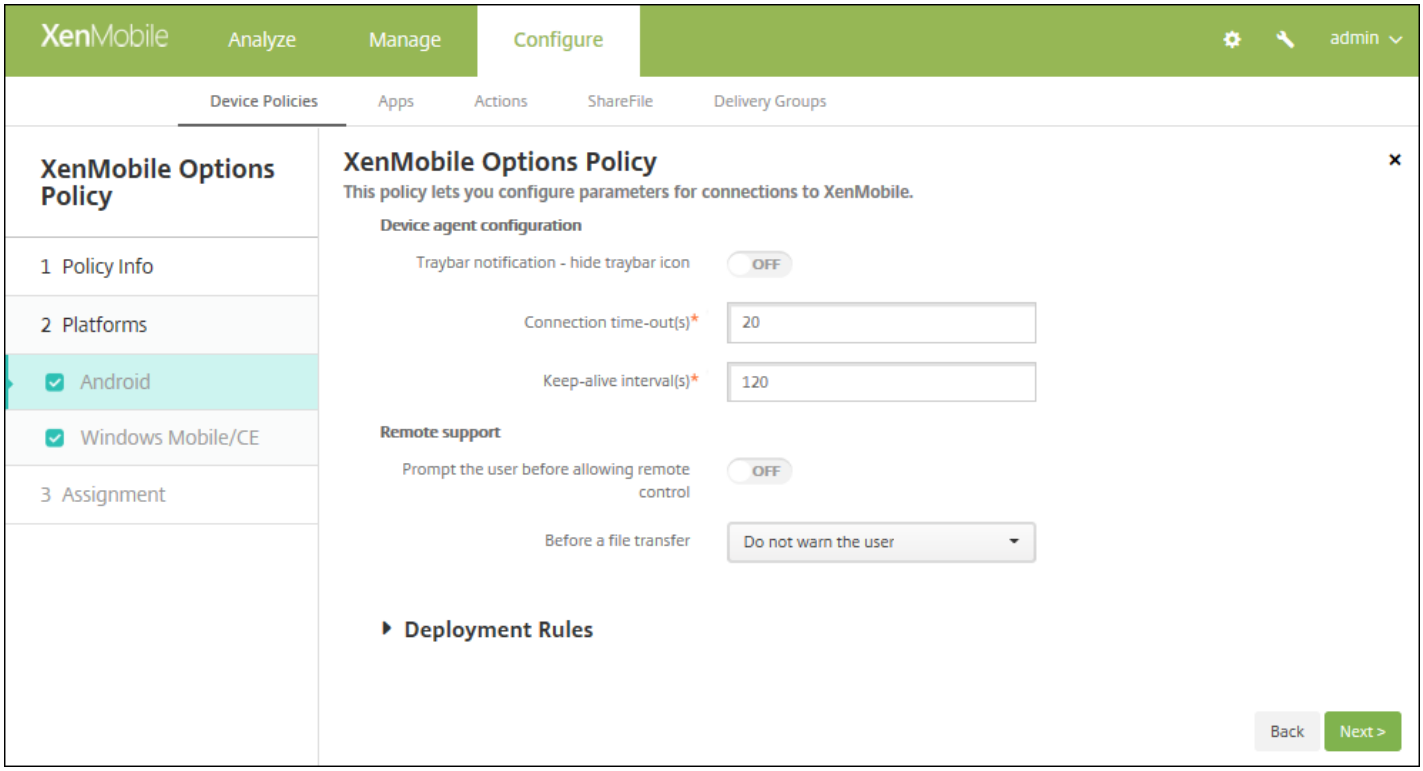
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

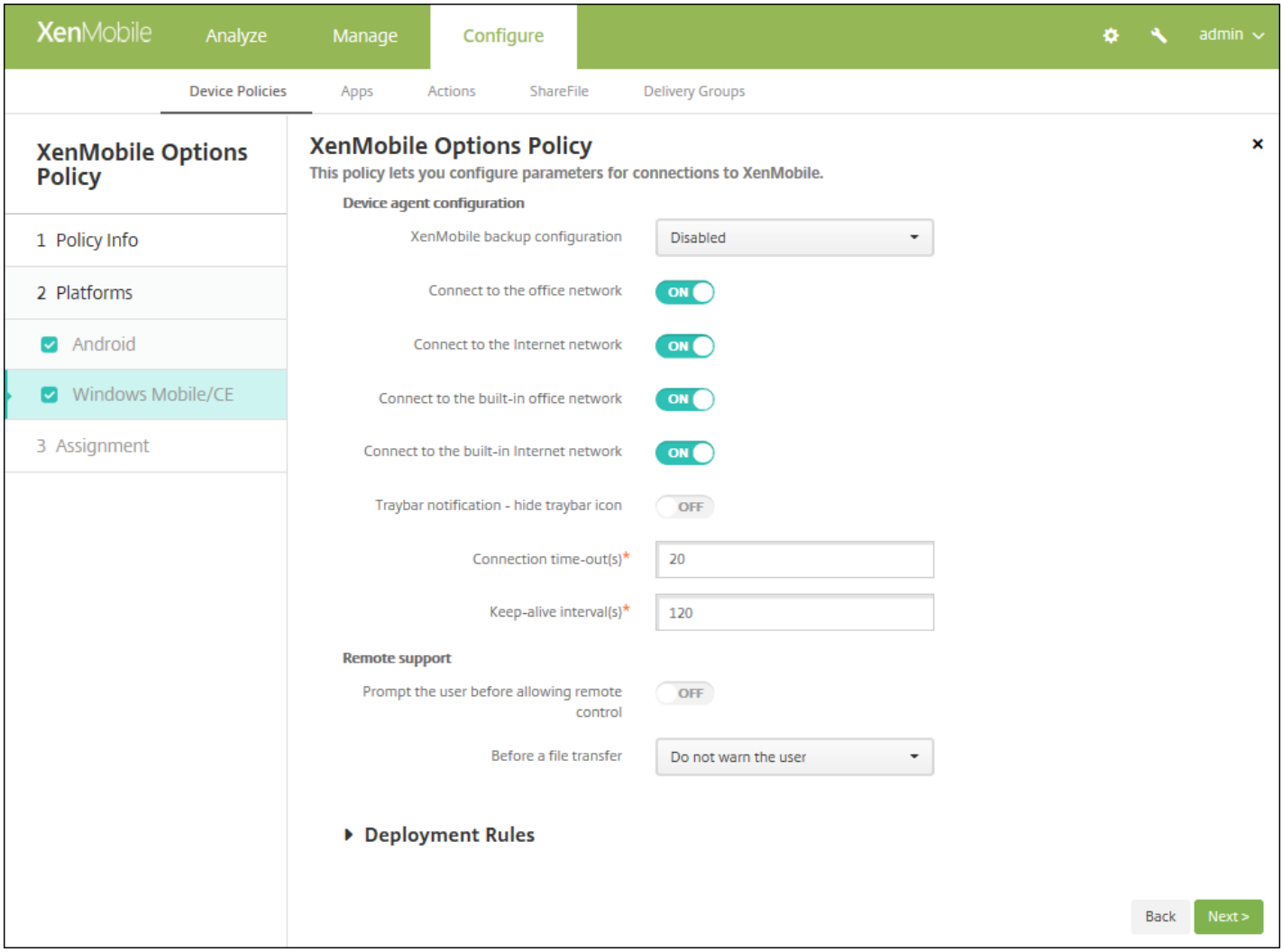
Configure Android settings



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**.

Configure Windows Mobile/CE settings



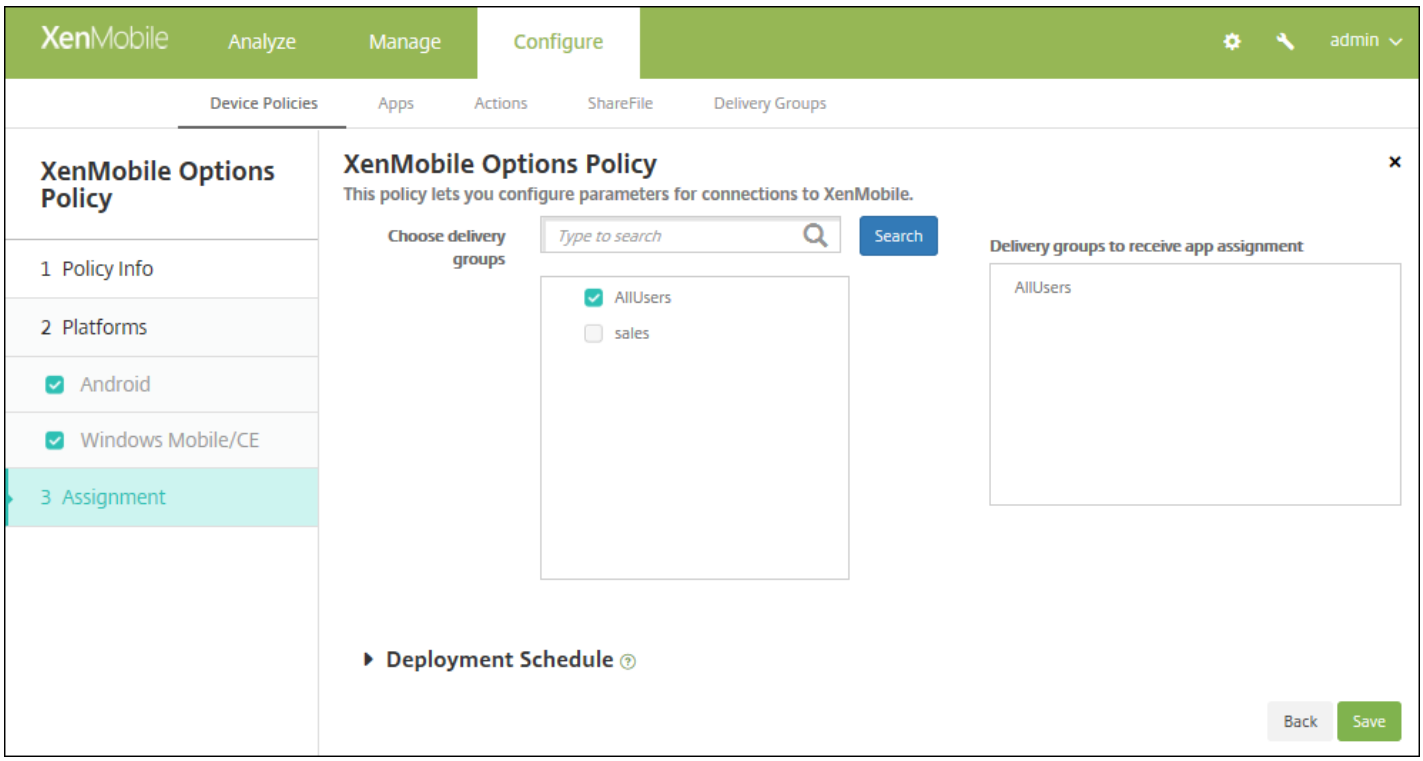
Configure these settings:

- **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 the deployment rules

8. Click **Next**. The **XenMobile Options 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**.

XenMobile uninstall device policy

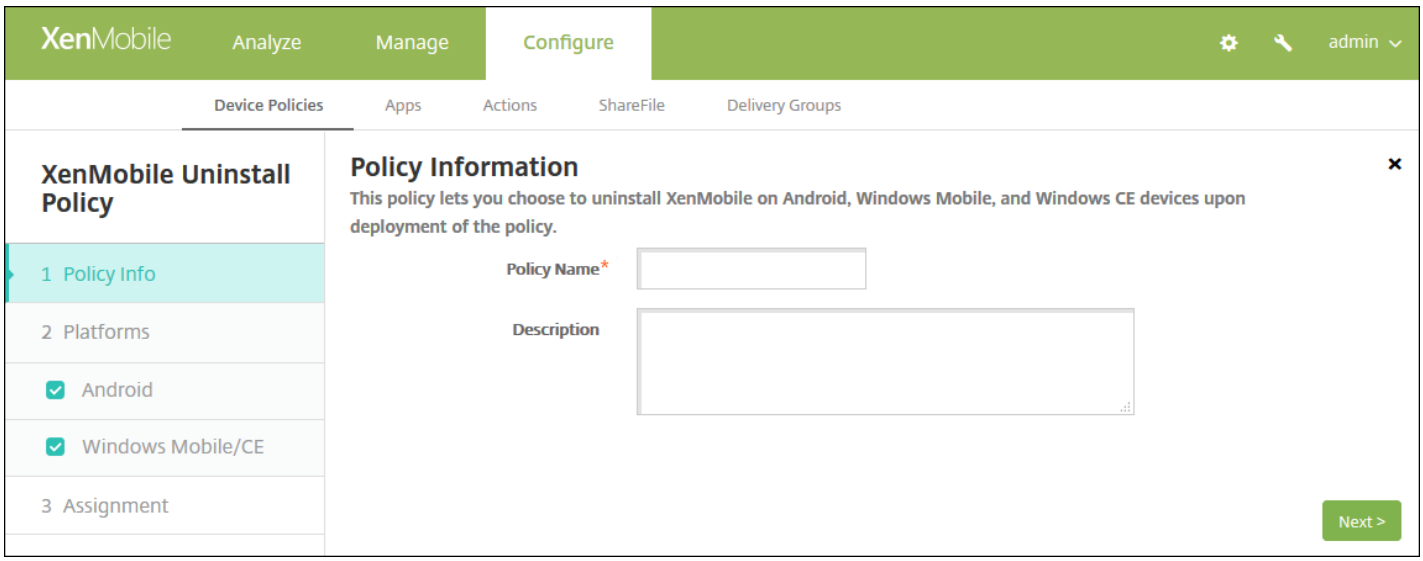
Nov 16, 2016

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:

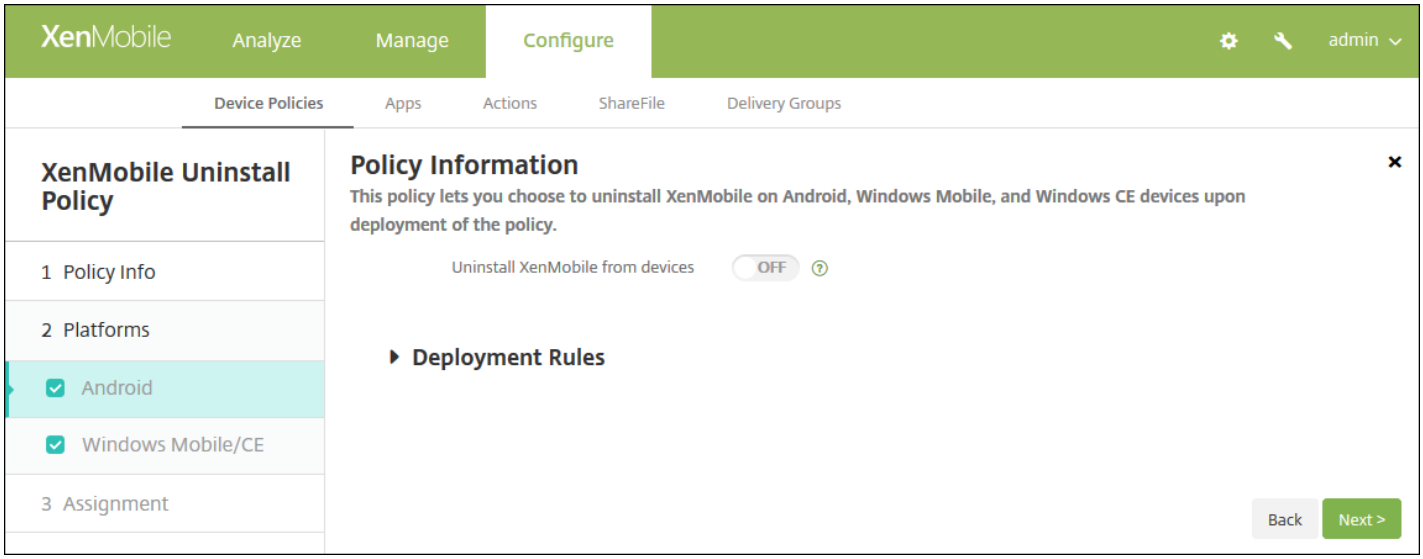
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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 Android and Windows Mobile/CE settings

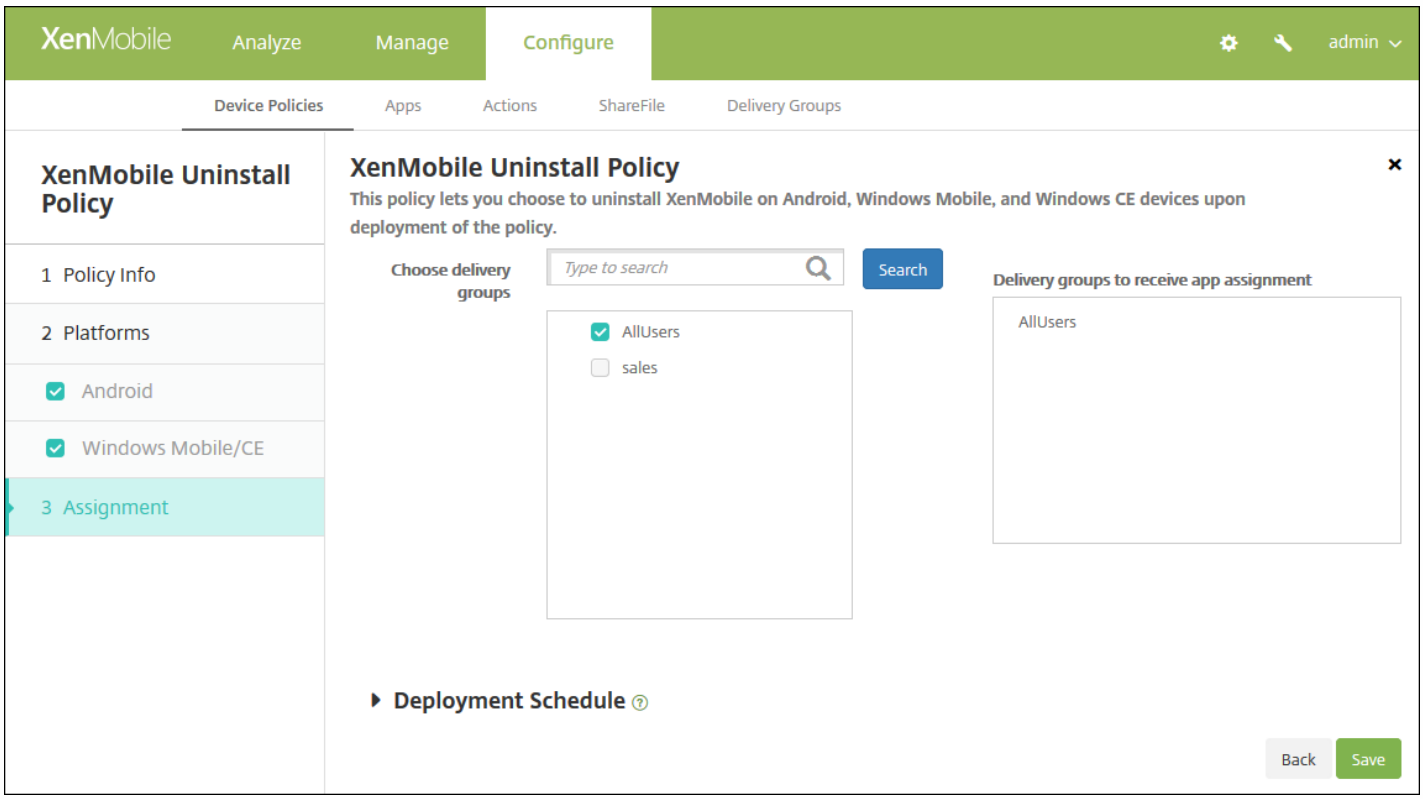


Configure this setting for each platform you choose:

- **Uninstall XenMobile from devices**: Select whether to uninstall XenMobile from every device to which you deploy this policy. The default is **OFF**.

7. Configure the deployment rules

8. Click **Next**. The **XenMobile Uninstall 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**.

Add apps

May 10, 2017

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 are apps wrapped with the MDX Toolkit (and associated policies). 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**. This is a Web address (URL) to a public or private site, or to a web app that does not 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. You must meet these prerequisites in order to implement silent installation:
>
> - For iOS apps, the managed iOS device must be in supervised mode. For details, see Import iOS & Mac OS X Profile device policies.
> - For Android apps, Samsung for Enterprise (SAFE) or KNOX policies must be enabled on the device.
>   To do so, you set the Samsung MDM license key device policy to generate Samsung ELM and KNOX license keys. For details, see Samsung MDM license key device policies.

How Mobile and MDX Apps Work

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, you download the public-store MDX files from Citrix, upload those files to the XenMobile console (**Configure > Apps**), update MDX policies as needed, and then 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, you download the app files from Citrix, wrap them using the MDX toolkit, upload them to the XenMobile console, modify the MDX policies as needed, and deliver the apps to user devices through delivery groups. For details, see Public App Store Delivery of XenMobile Apps in the XenMobile Apps documentation.

Citrix provides the MDX Toolkit that 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.

How Web and SaaS Apps Work

XenMobile comes with a set of application connectors, which are templates that you can configure for single sign-on (SSO) to web and Software as a Service (SaaS) applications, and in some cases 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.

How Enterprise Apps Work

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.

How the Public App Store Works

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.

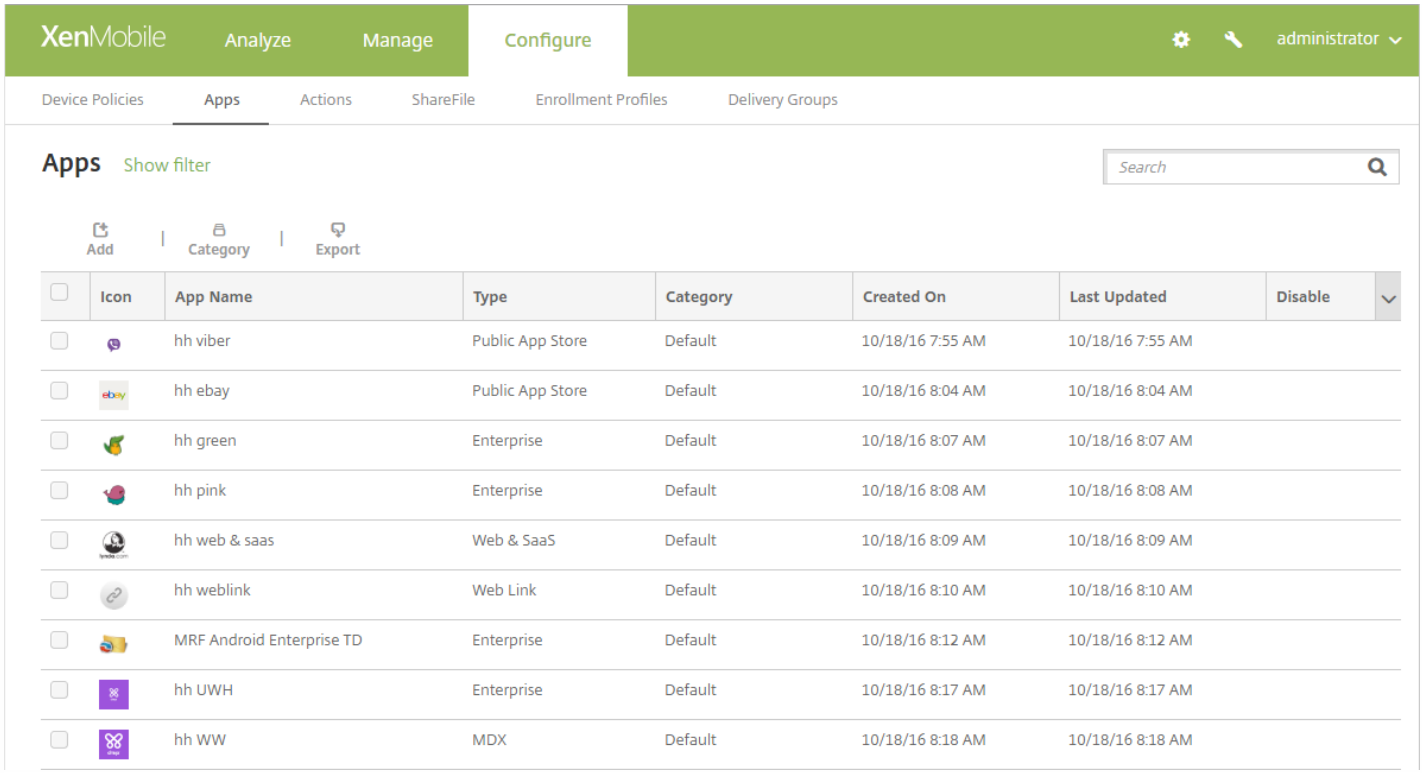
How Web Links Work

A web link is a web address to an Internet or intranet site. A web link can also point to a web application that doesn't require SSO. When you finish configuring a web link, the link appears as an icon in the 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.

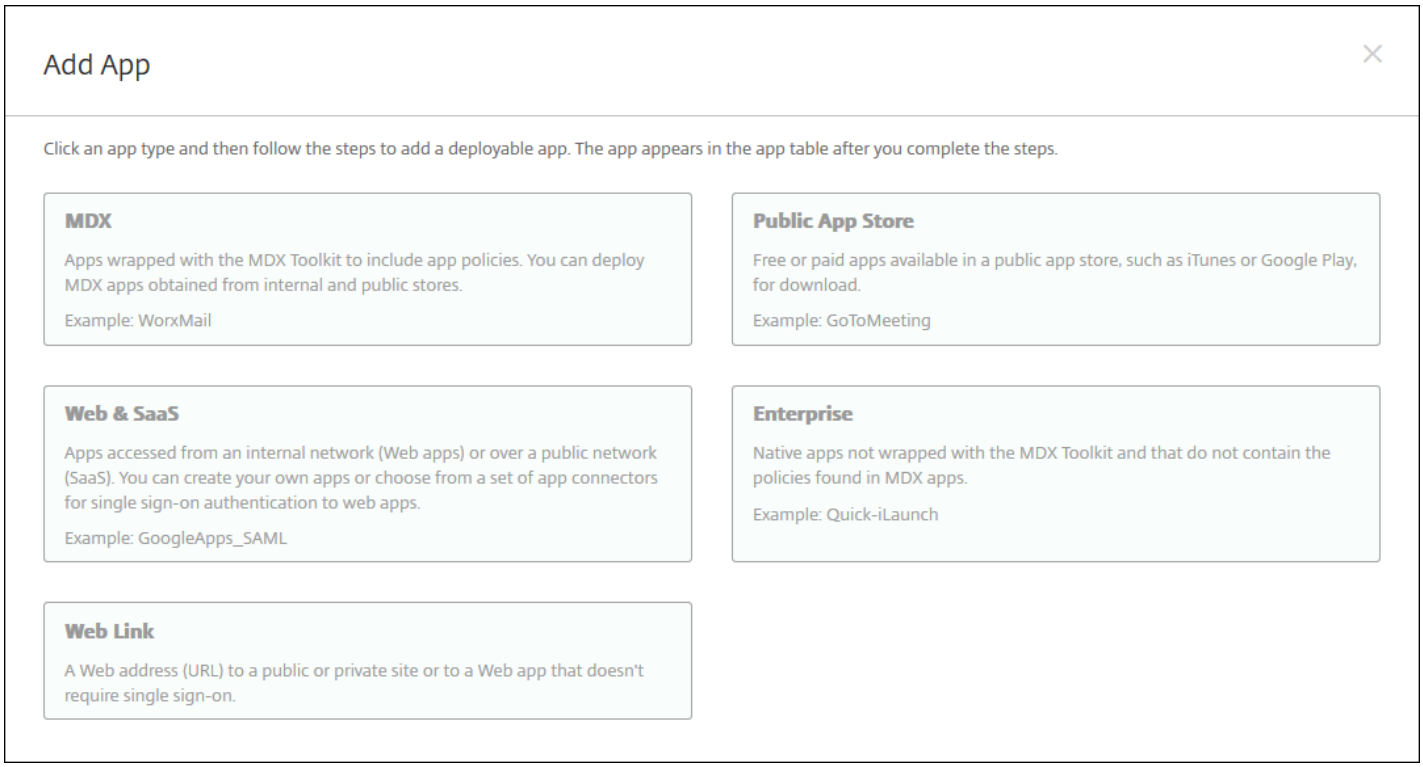
Add an MDX app

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.

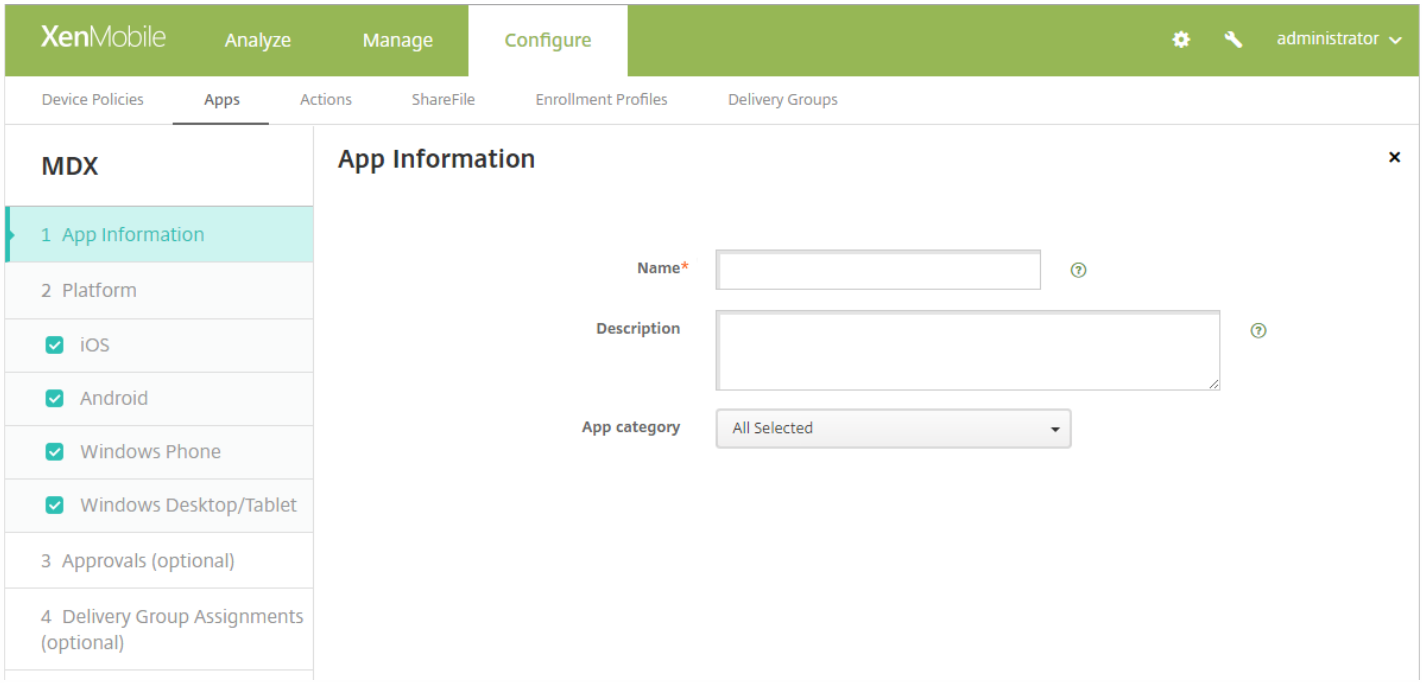
1. In the XenMobile console, click **Configure** > **Apps**. The **Apps** page appears.



2. Click **Add**. The **Add App** dialog box appears.



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. This will appear 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, refer to Step 11 for how to set that platform's deployment rules.

7. Select an .mdx file to upload by clicking **Upload** and navigating to the file's location.

- If you are adding an iOS VPP B2B app, click **Your application is a VPP B2B application?** and in the list, click the B2B VPP account to use.

8. Click **Next**. The app details page appears.

9. Configure these settings:

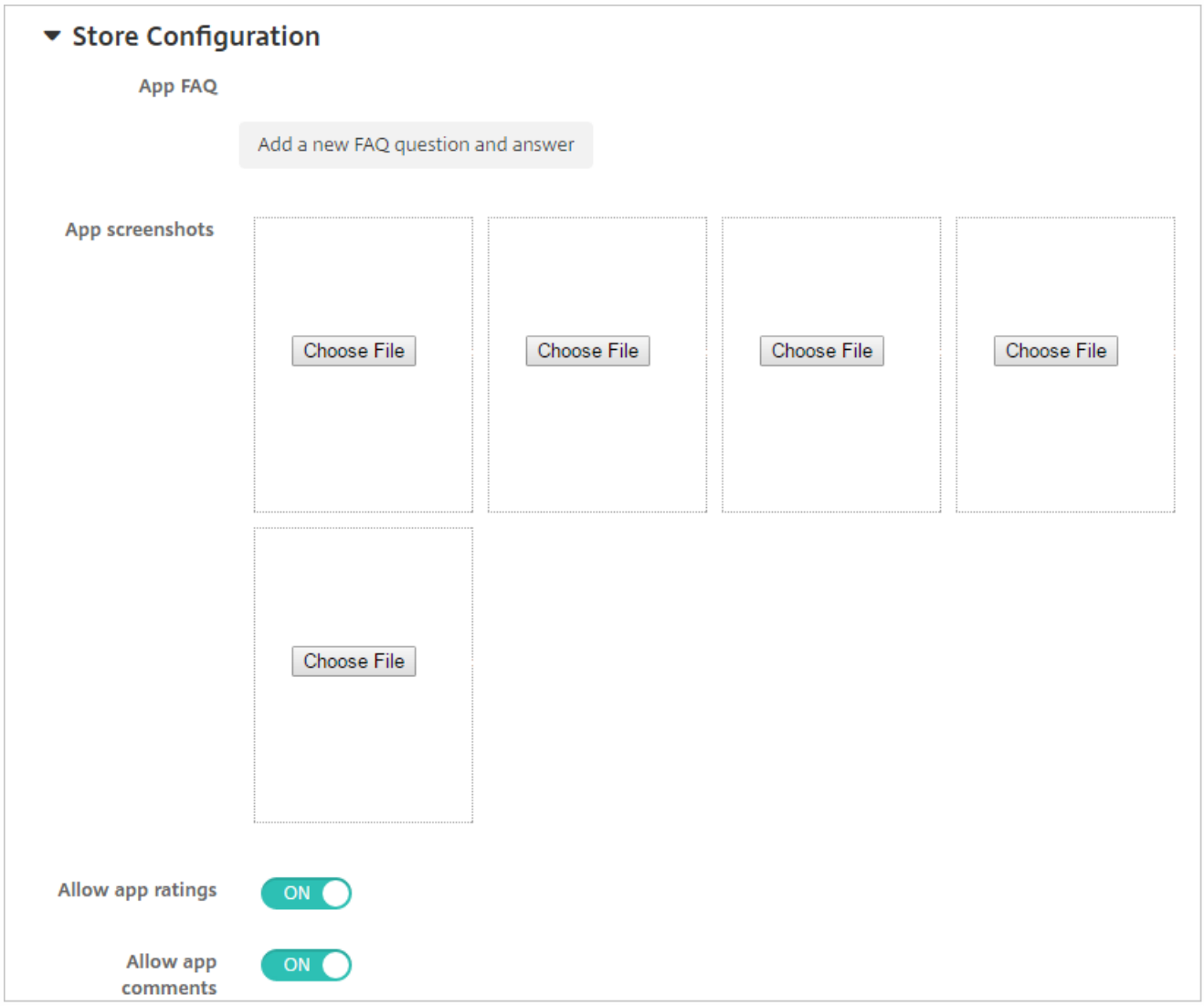
- **File name**: Type the file name associated with the app.
- **App Description**: Type a description for the app.
- **App version**: Optionally, type the app's version number.
- **Minimum OS version**: Optionally, type the oldest operating system version that the device can run to use the app.
- **Maximum 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.

10. Configure the **MDX Policies**. MDX policies vary by platform and include options for such policy areas as Authentication, Device Security, Network Requirements, Miscellaneous Access, Encryption, App Interaction, App Restrictions, App Network Access, App logs, and App Geofence. In the console, each of the policies has a tooltip that describes the policy. For more information about app policies for MDX apps that includes a table showing which policies apply to which platform types, see MDX Policies at a Glance.

11. Configure the deployment rules.

12. Expand **XenMobile Store Configuration**.



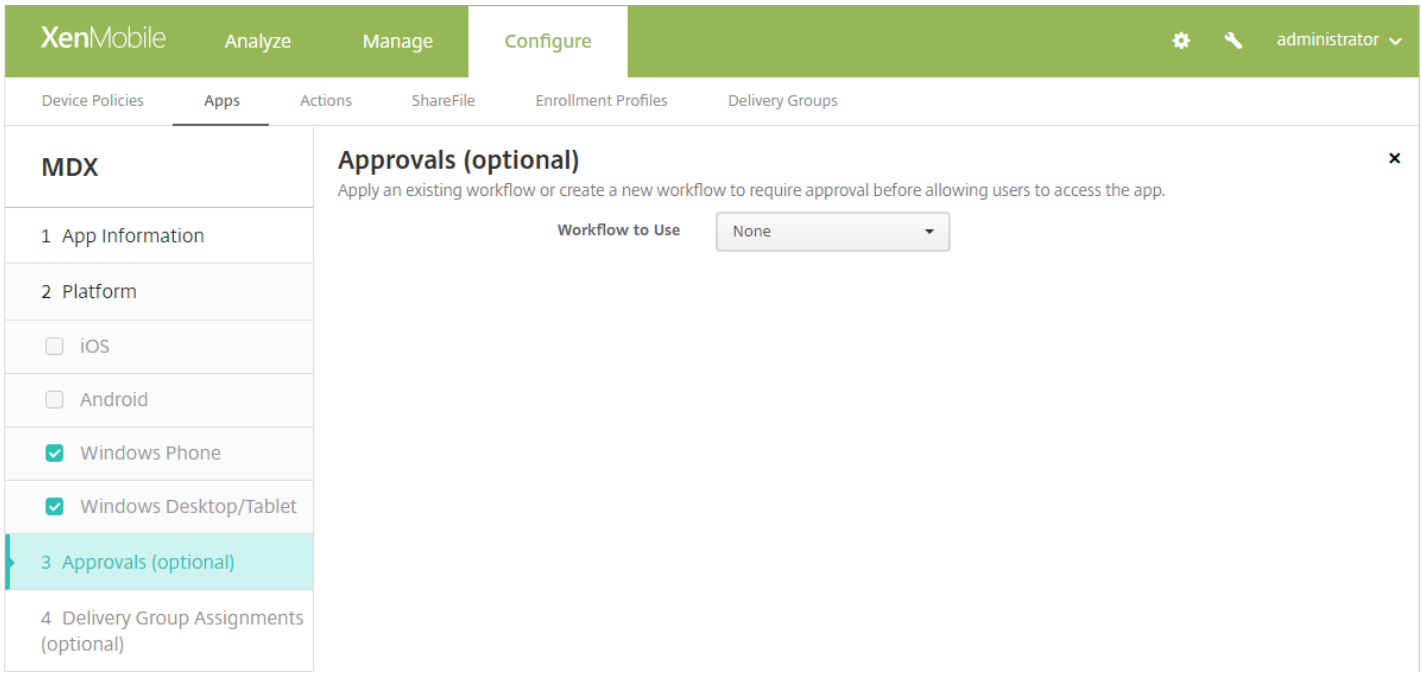
Optionally, you can add an FAQ for the app or screen captures that appear in the XenMobile Store. You can also set whether users can rate or comment on the app.

- 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.



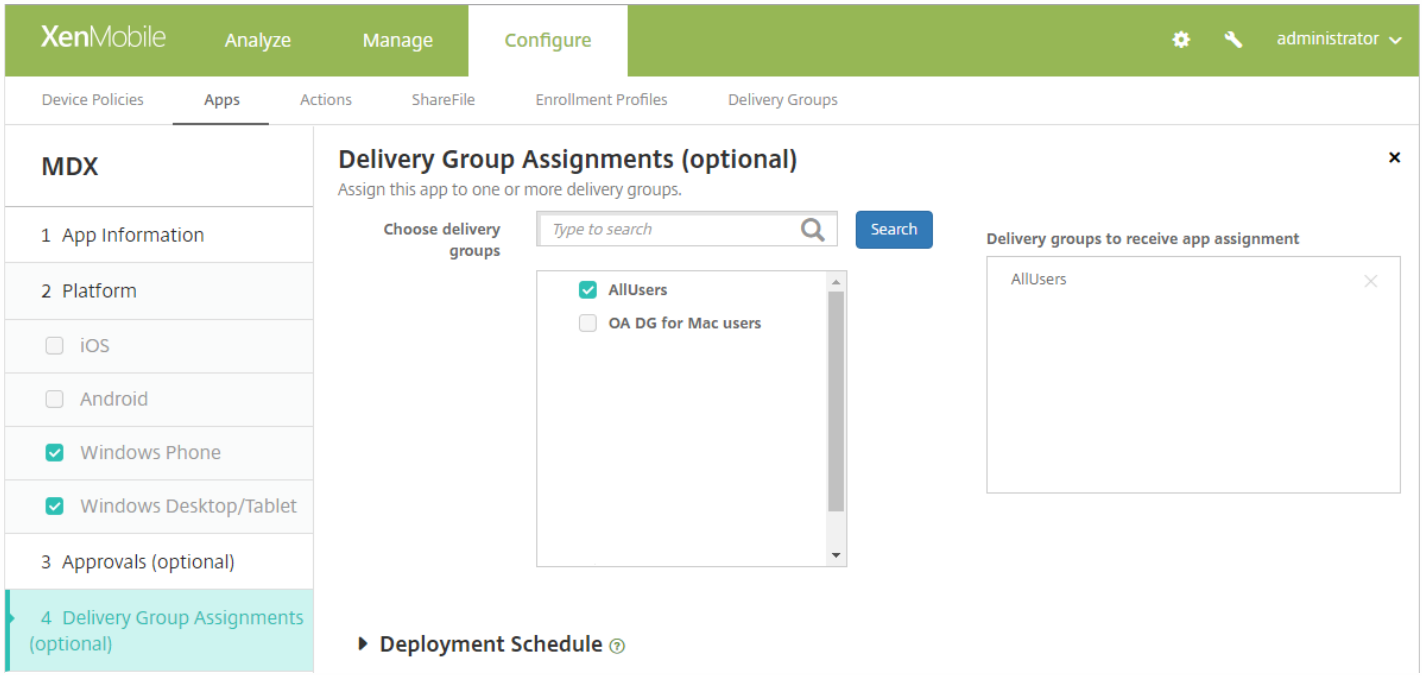
You use workflows when you need approval when creating user accounts. If you don't need to set up approval workflows, you can skip to Step 15.

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:
  - **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 additional required person's name in the search field and then click **Search**. Names originate in Active Directory.
  - When the person's name appears in the field, select the check box next to his or her name. The person's 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 to which you want to assign the app. 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**. 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.

17. Click **Save**.

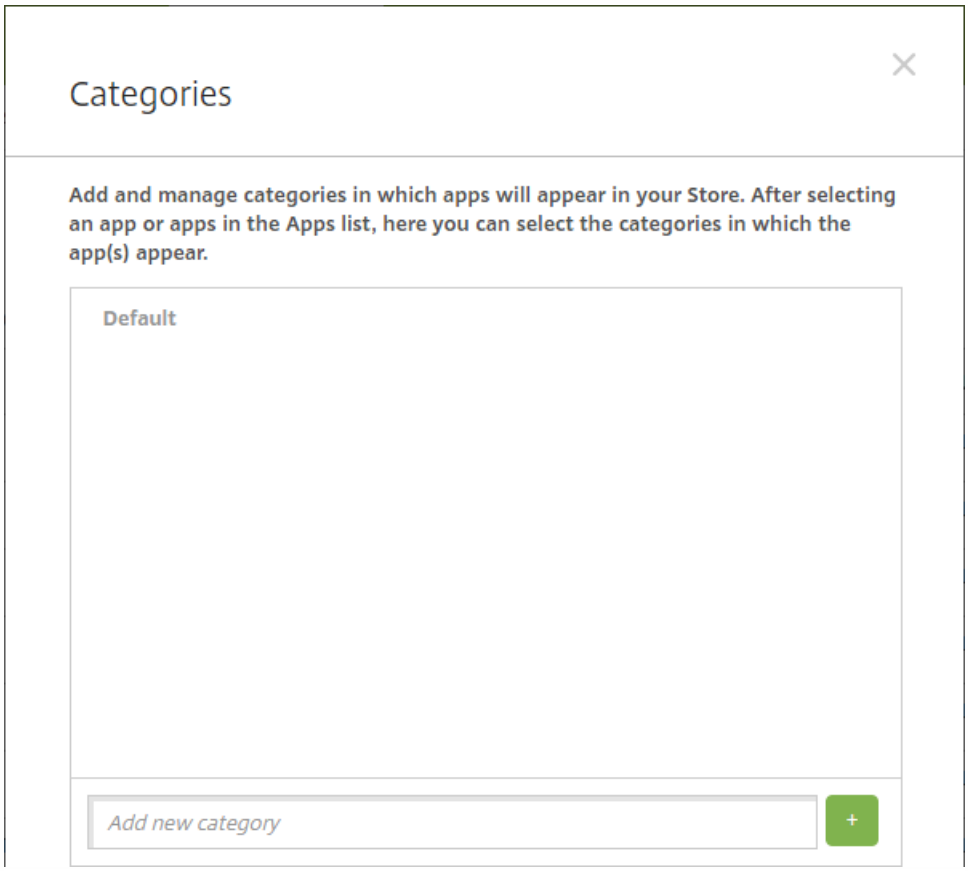
Create app categories

When users log on to Secure Hub, they receive a list of the apps, web links, and stores that you have added and set up in XenMobile. You can use app categories to let users access only the apps, stores, or web links that you want. 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 categories you've configured.

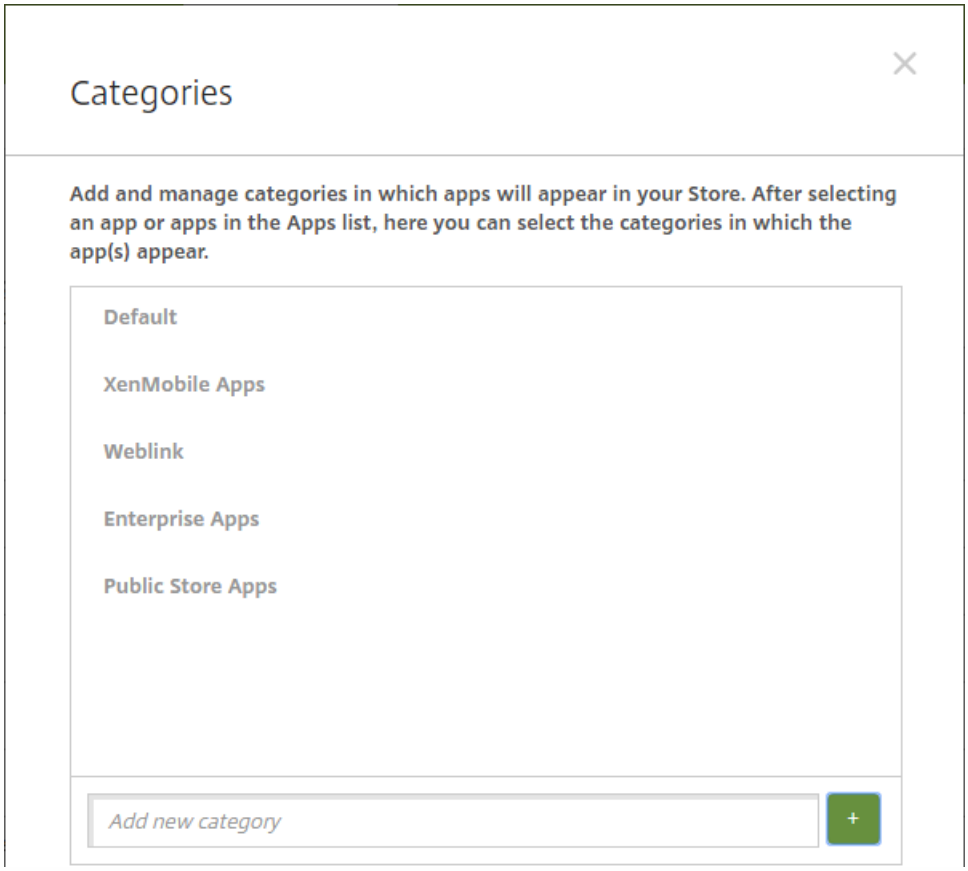
1. In the XenMobile console, click **Configure** > **Apps**. The **Apps** page appears.

2. Click **Category**. The **Categories** dialog box appears.



3. For each category you want to add, do the following:

- Type the name of the category you want to add in the **Add a new category** field at the bottom of the dialog box. For example, you could type Enterprise Apps to create a category for enterprise apps.
- Click the plus sign (+) to add the category. The newly created category is added and appears in the **Categories** dialog box.



4. When you're done adding categories, close the **Categories** dialog box.

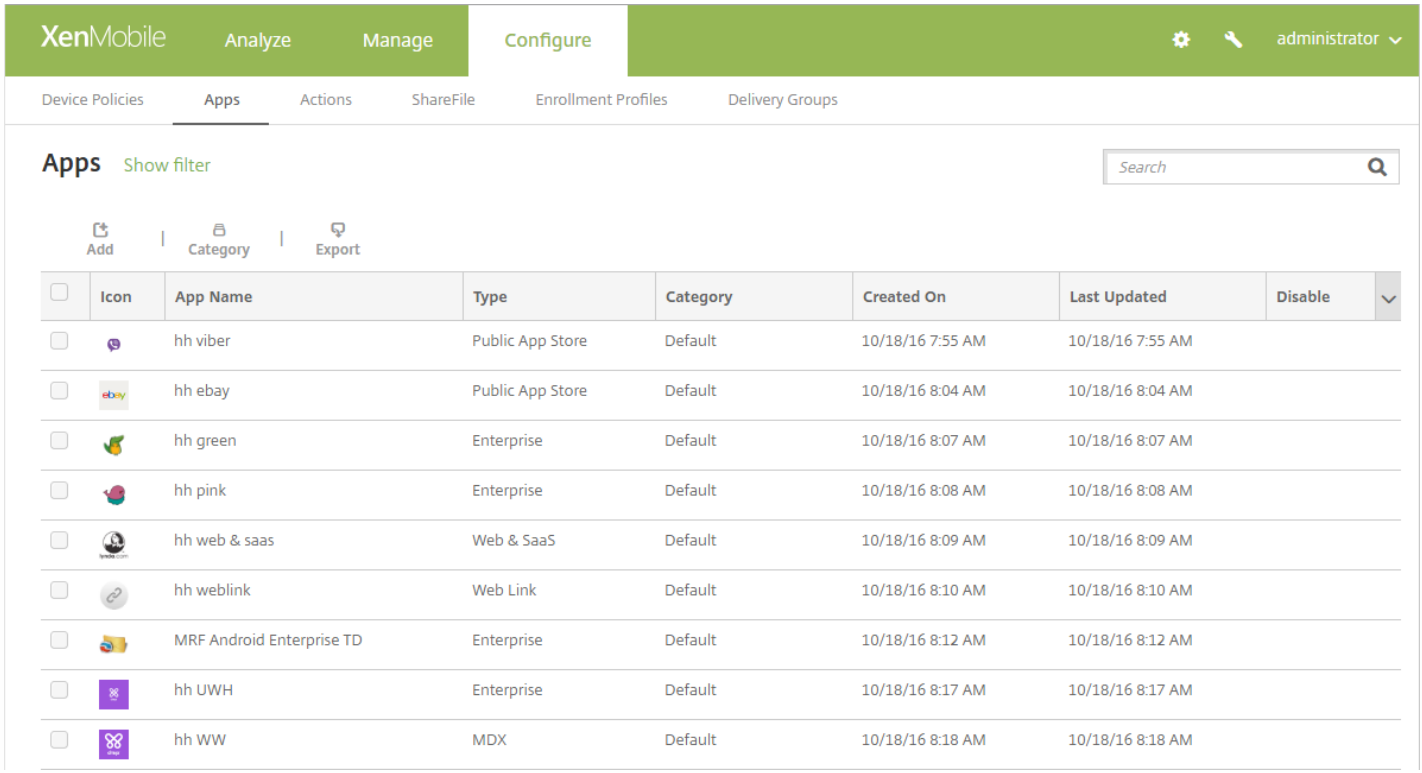
5. On the **Apps** page, you can place an existing app into a new category.

- Select the app you want to categorize.
- Click **Edit**. The **App Information** page appears.
- In the **App category** list, apply the new category by selecting the category check box. Clear the check boxes for any existing categories that you don't want to apply to the app.
- Click the **Delivery Groups Assignments** tab or click **Next** on each of the following pages to step through the remaining app set-up pages.
- Click **Save** on the **Delivery Groups Assignments** page to apply the new category. The new category is applied to the app and appears in the **Apps** table.

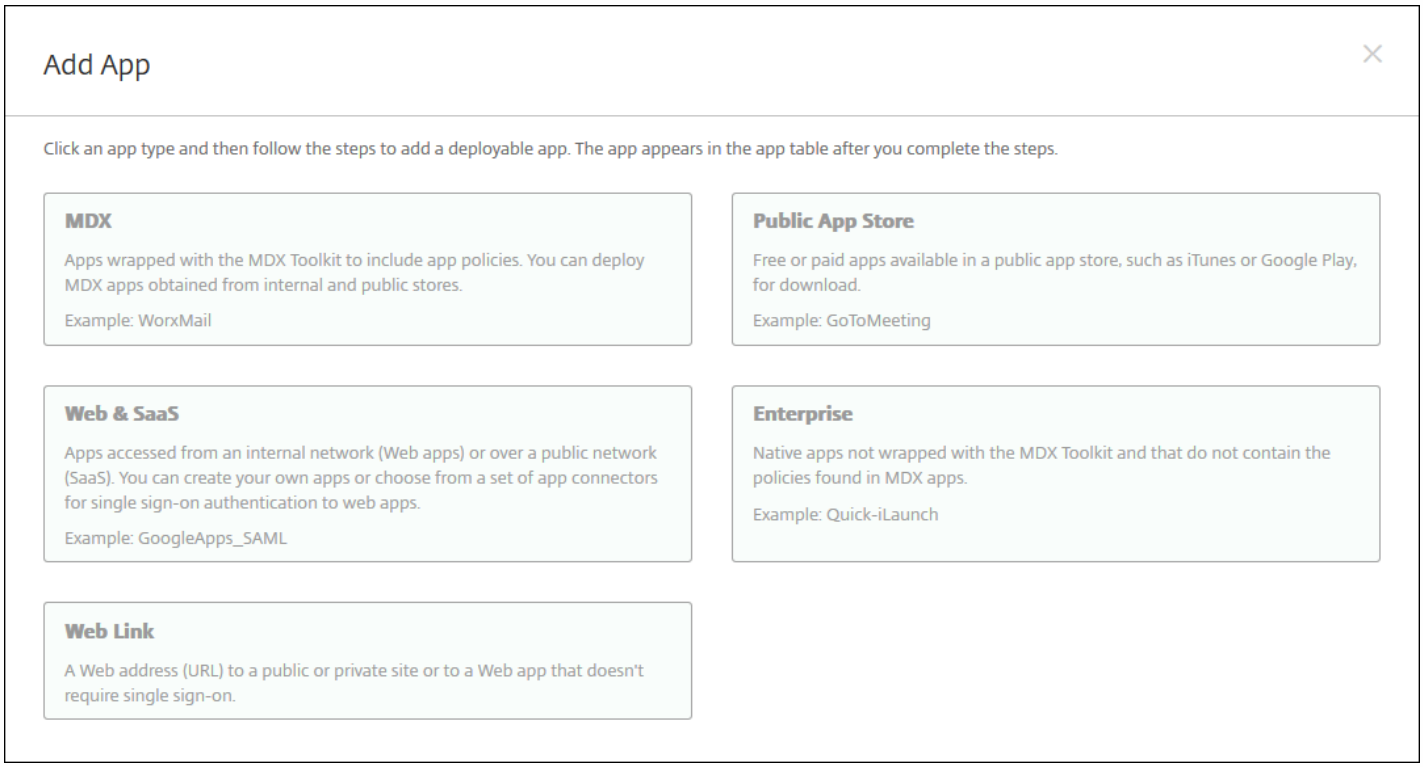
Add a public app store app

You can add free or paid apps to 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 - the total number of licenses available and the number currently in use, as well as 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.



2. Click **Add**. The **Add App** dialog box appears.



3. Click **Public App Store**. The **App Information** page appears.

4. On the **App Information** pane, type the following information:

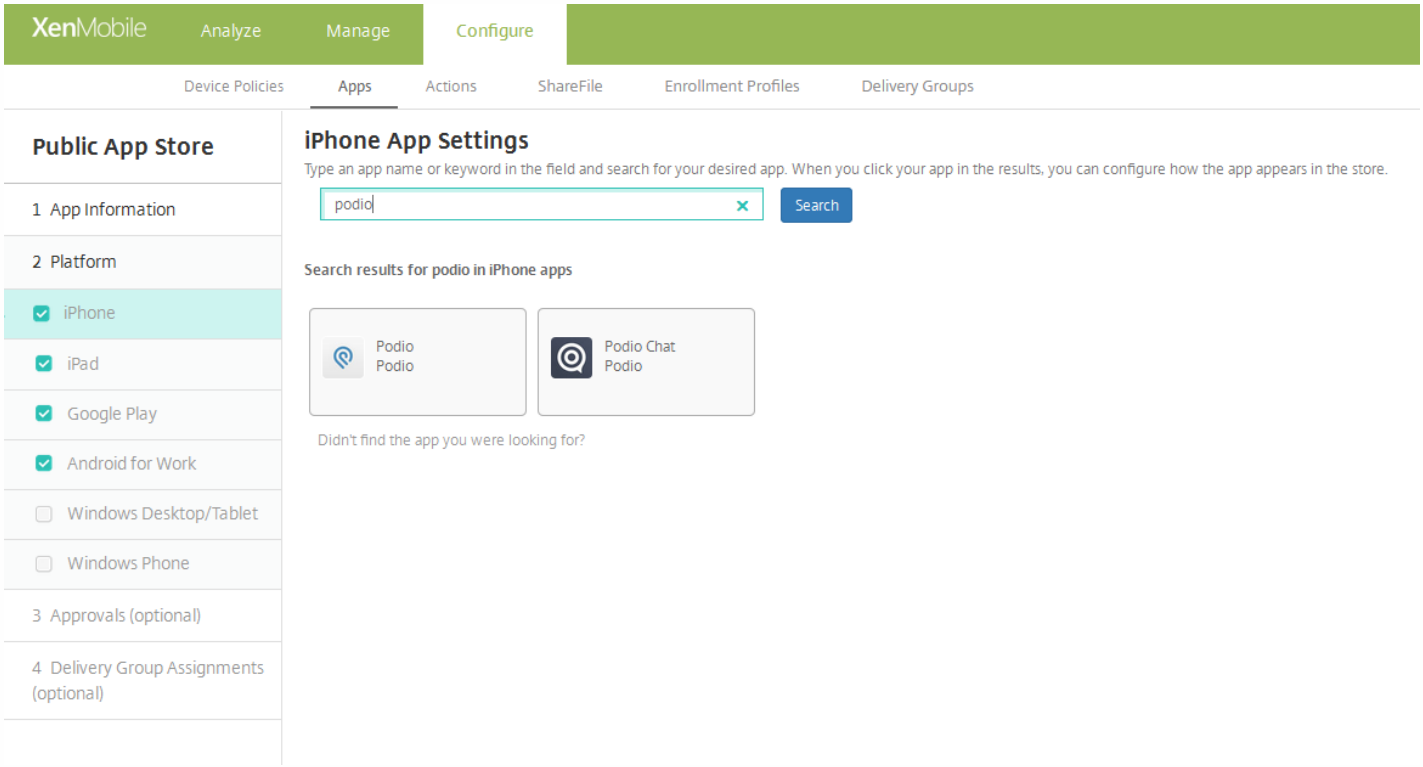
- **Name**: Type a descriptive name for the app. This will appear under **App Name** on the **Apps** table.
- **Description**: Type an optional description of the app.
- **App category**: Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see Create app categories.

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

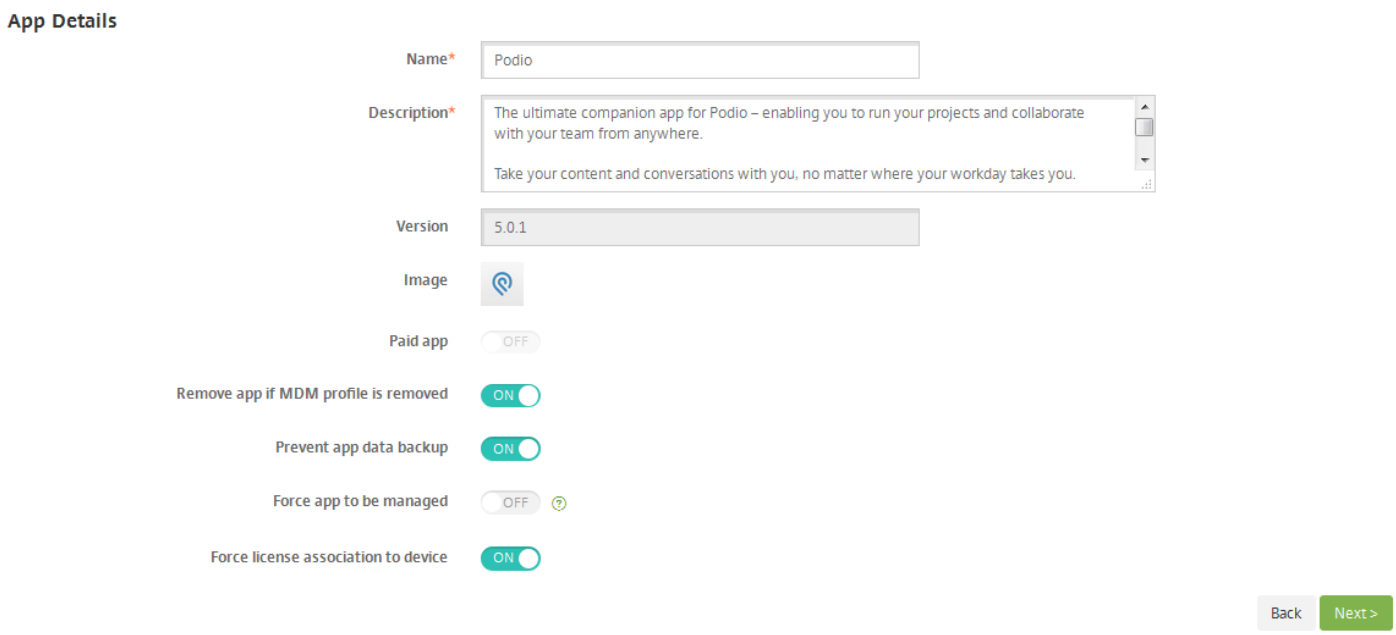
6. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.

When you finish configuring the settings for a platform, refer to Step 10 for how to set that platform's 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".



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).

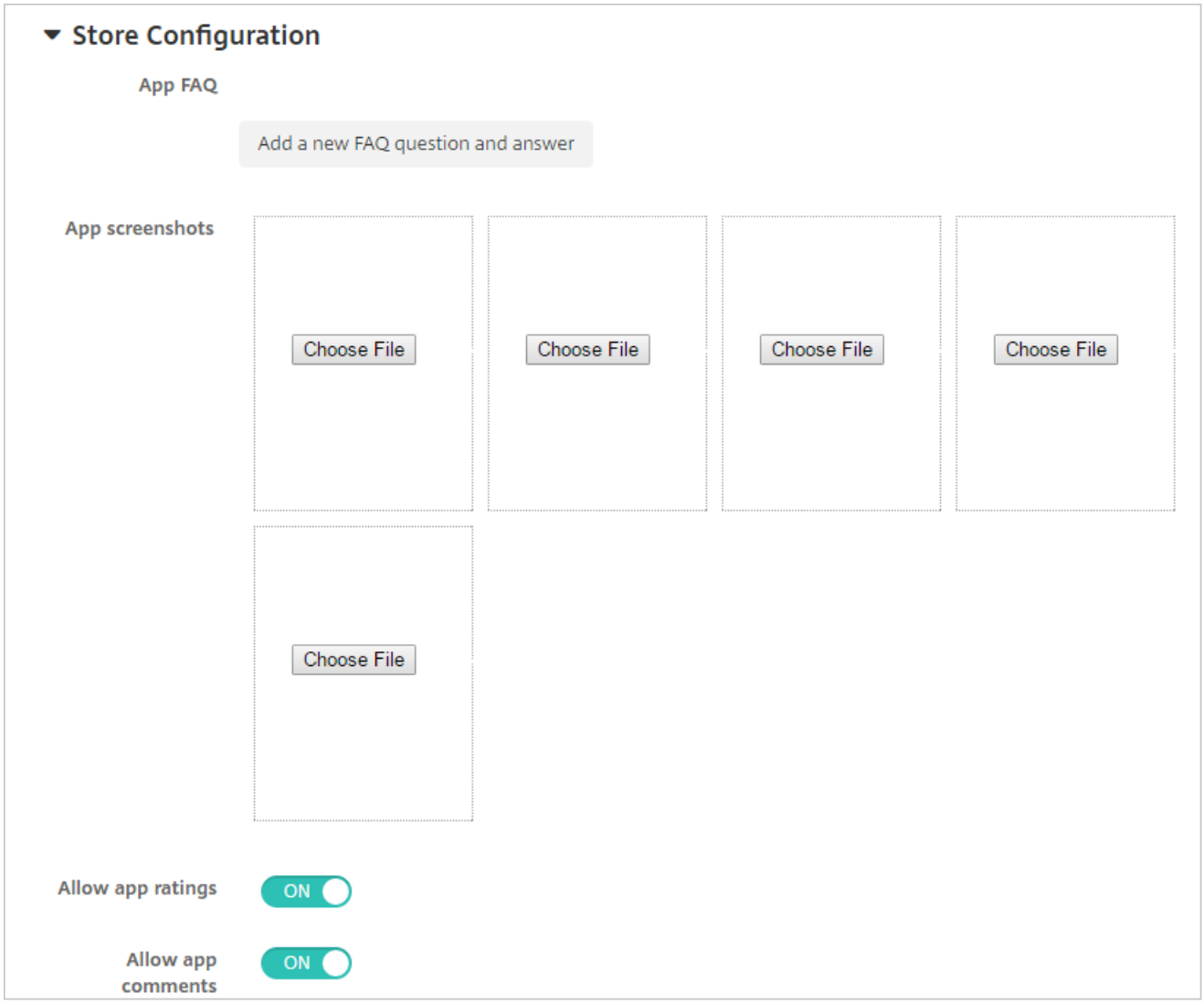


9. Configure these settings:

- 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.

11. Expand **XenMobile Store Configuration**.

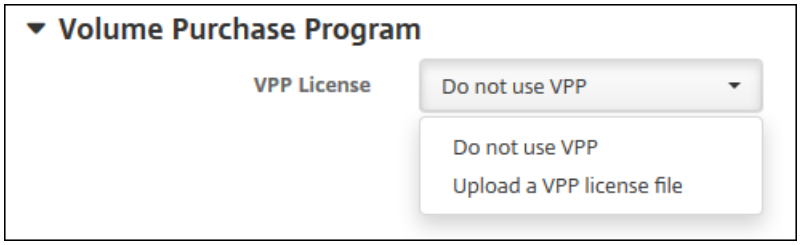


Optionally, you can add an FAQ for the app or screen captures that appear in the XenMobile Store. You can also set whether users can rate or comment on the app.

- 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 in the case of Android for Work, expand **Bulk Purchase**.

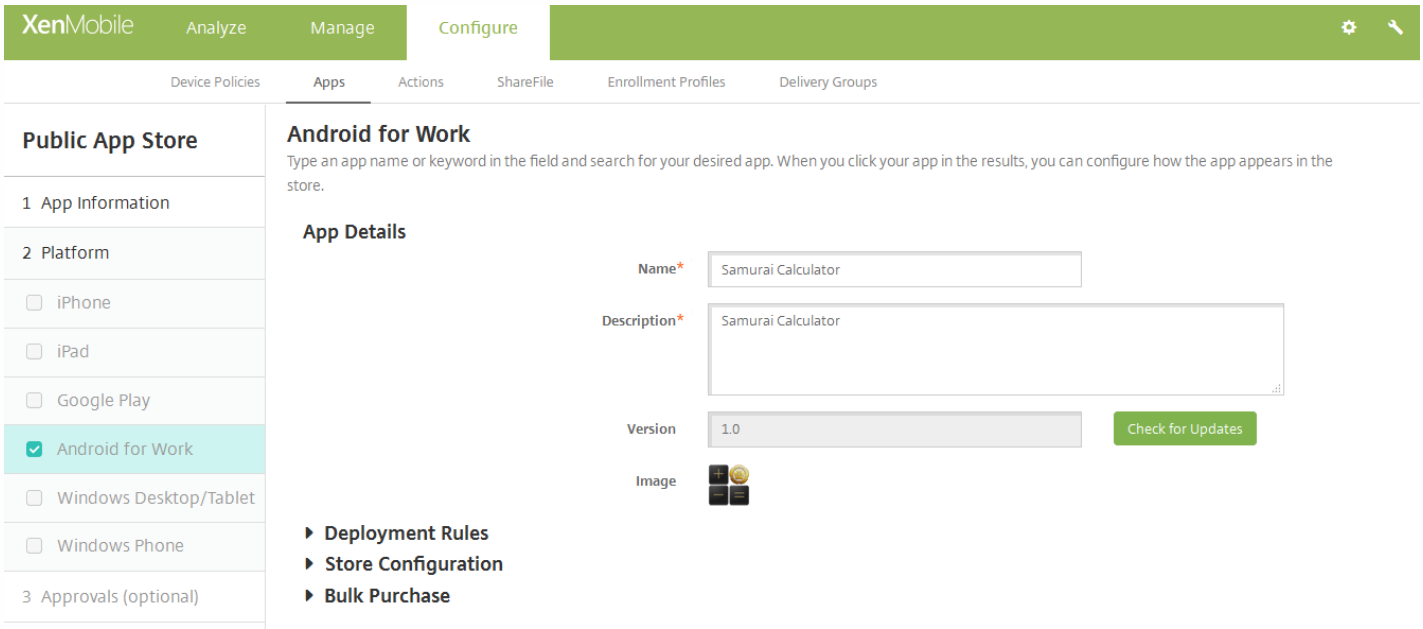
For the Volume Purchase Program, complete the following steps.



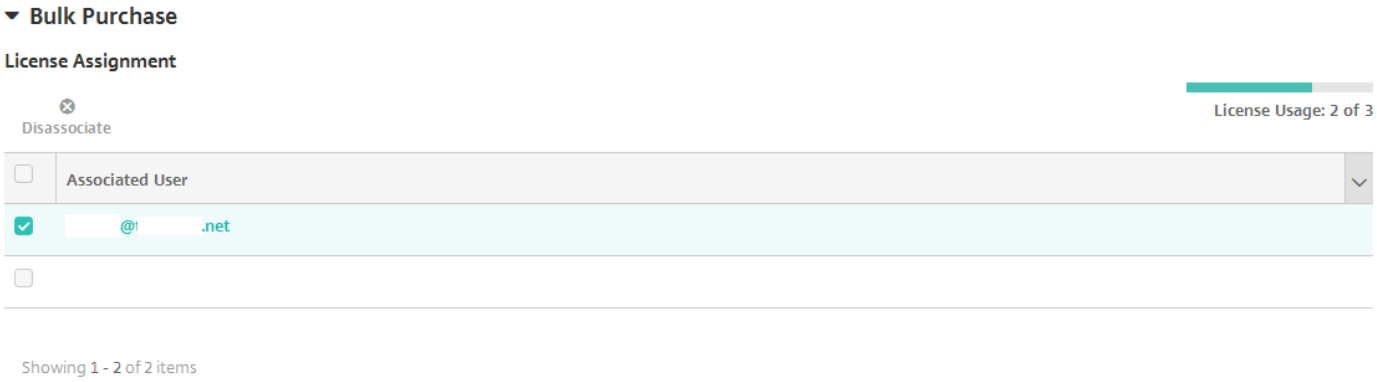
a. In the **VPP license** list, click **Upload a VPP license** file if you want to enable XenMobile to apply a VPP license for the app.

b. In the dialog box that appears, import the license.

For Android for Work Bulk Purchase, expand the **Bulk Purchase** section.



In the License Assignment table, you'll see how many licenses are currently being used for the app out of the total available. 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.



13. 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 additional required person's name in the search field and then click **Search**. Names originate in Active Directory.
  - When the person's name appears in the field, select the check box next to his or her name. The person's 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 to which you want to assign the app. 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**. 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.

17. Click **Save**.

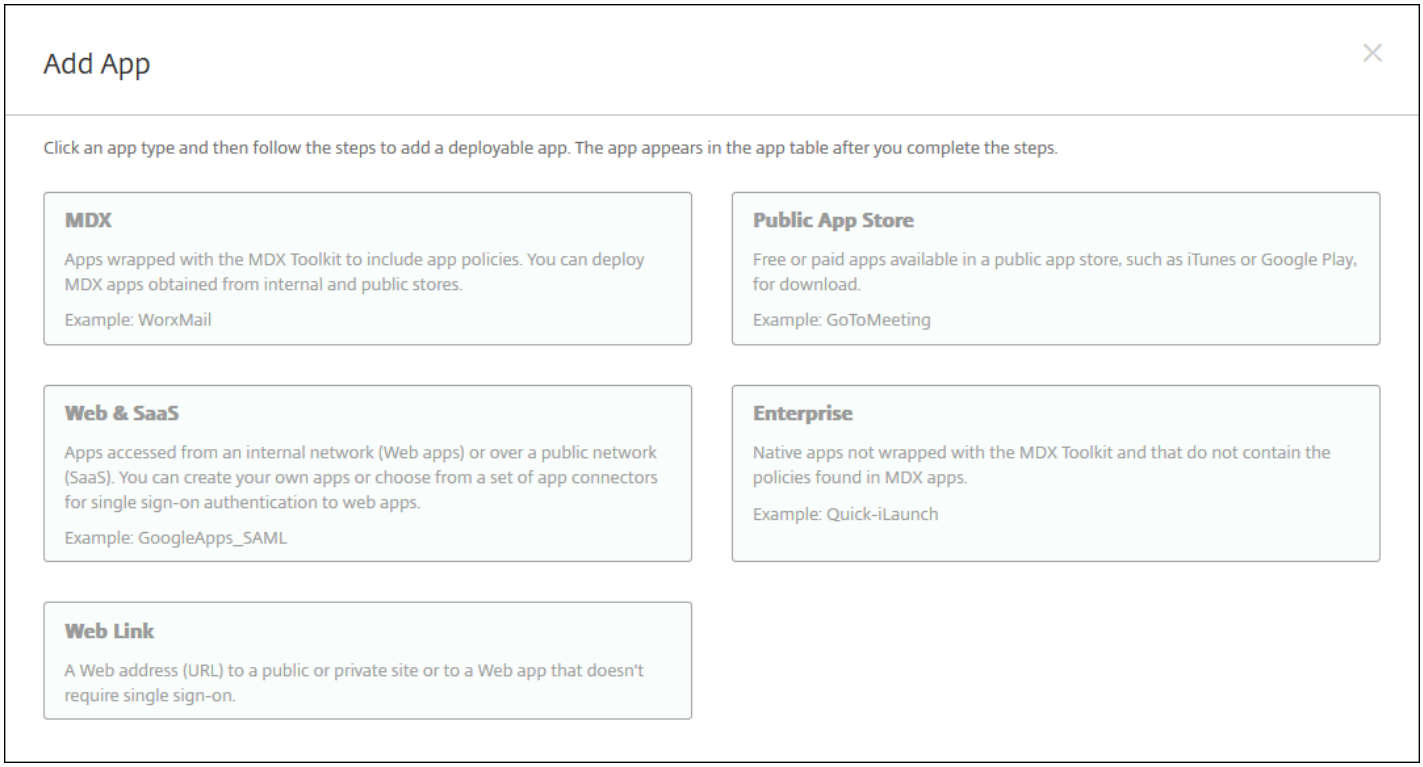
Add a Web or SaaS app

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.

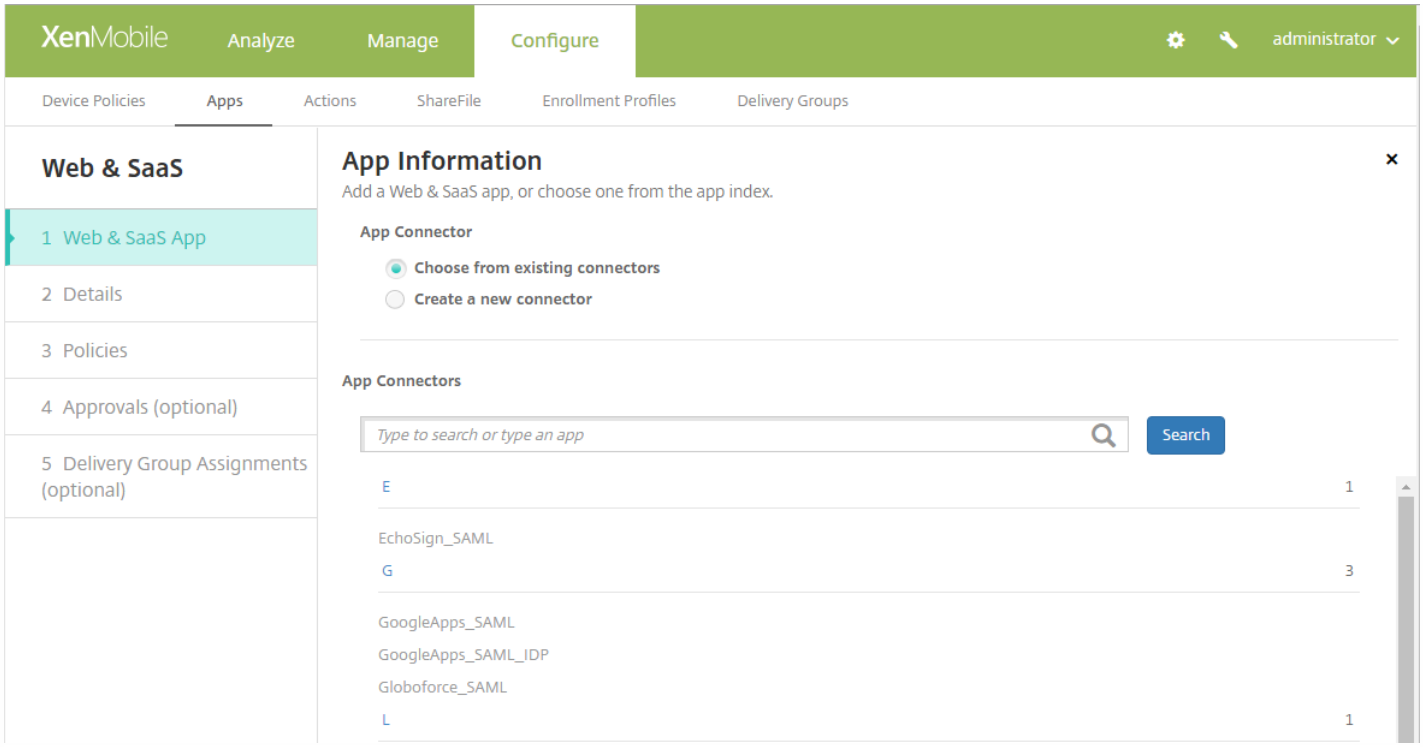
If an app is available for SSO only, when you finish configuring the preceding settings, you save the settings and the app appears on the **Apps** tab in the XenMobile console.

1. In the XenMobile console, click **Configure** > **Apps**. The **Apps** page opens.

2. Click **Add**. The **Add App** dialog box appears.



3. Click **Web & SaaS**. The **App Information** page appears.



4. Configure an existing or new app connector, as follows.

To configure an existing app connector

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.

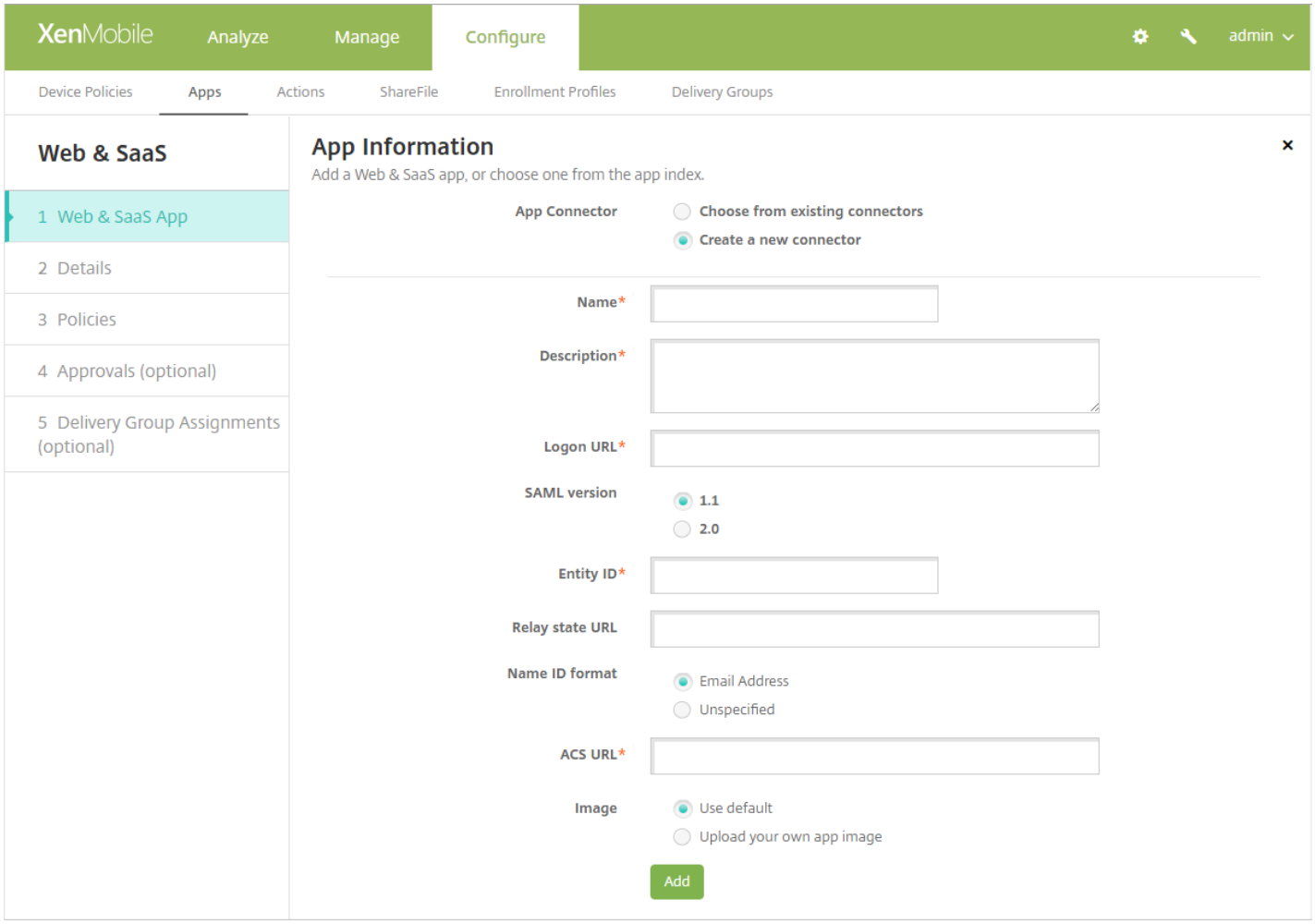
Configure these settings:

- **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

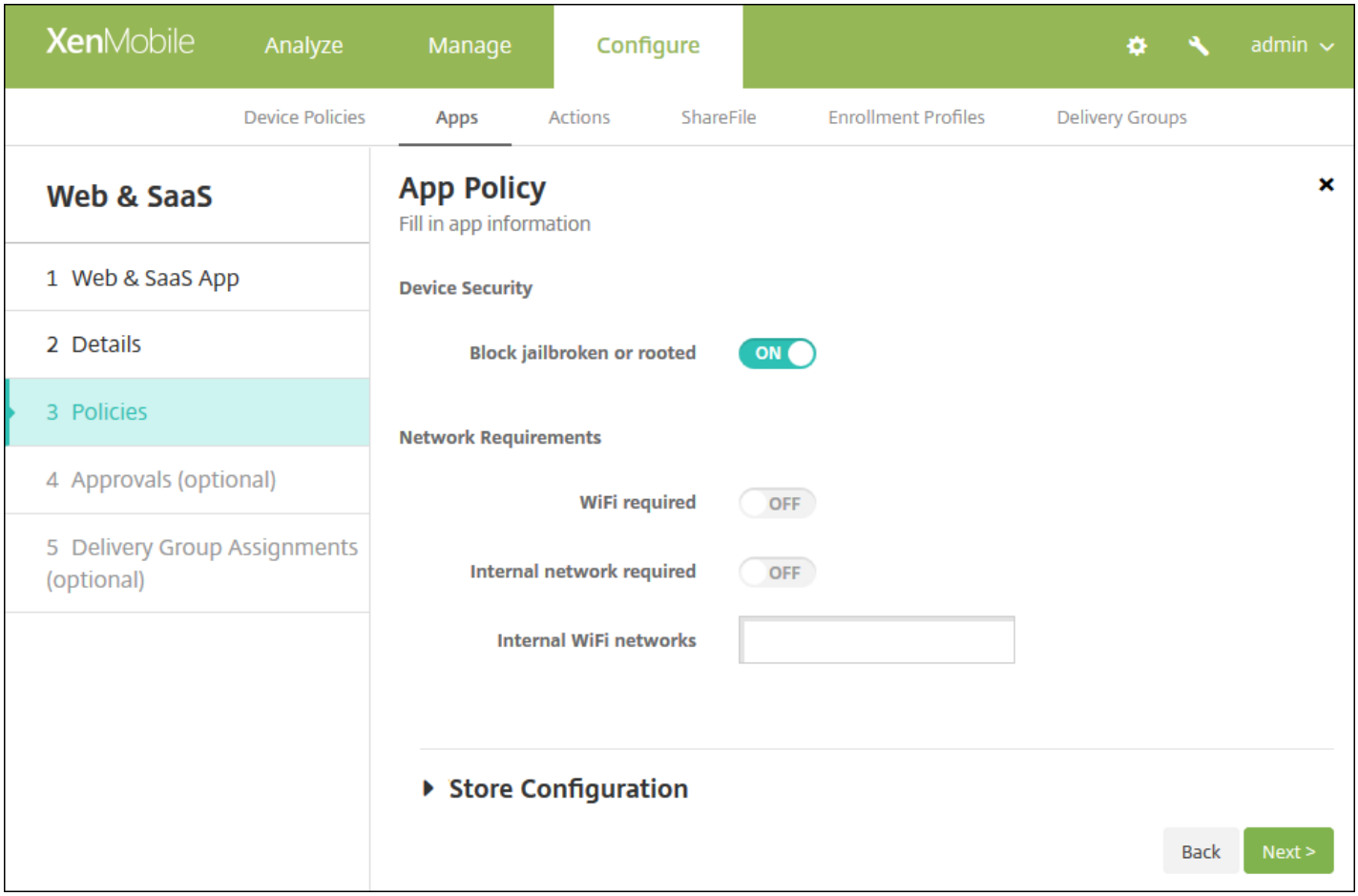
In the **App Information** page, select **Create a new connector**. The app connector fields appear.



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's 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 at a later time.
  - When you're finished, click **Add**. The **Details** page appears.

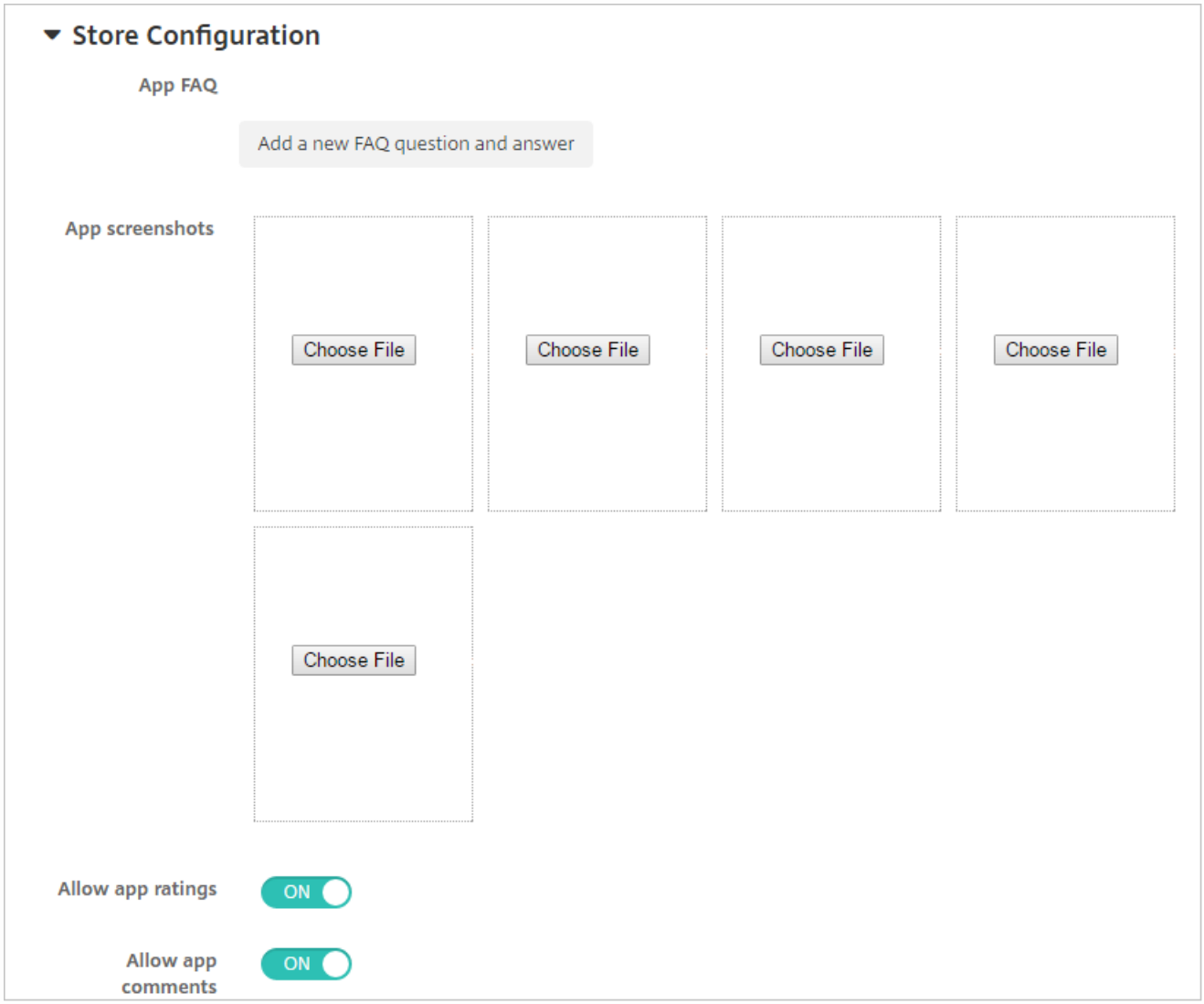
5. Click **Next**. The **App Policy** page appears.



- 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.

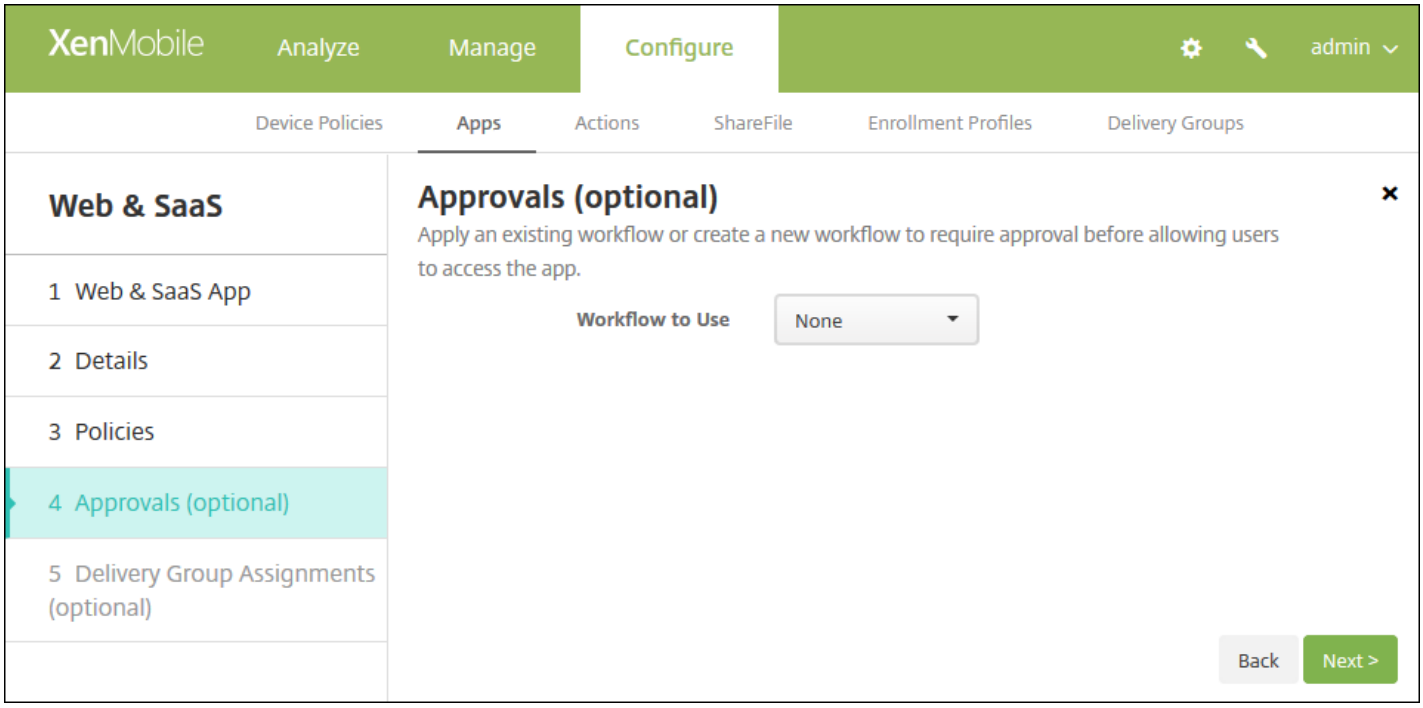
6. Expand **XenMobile Store Configuration**.



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.

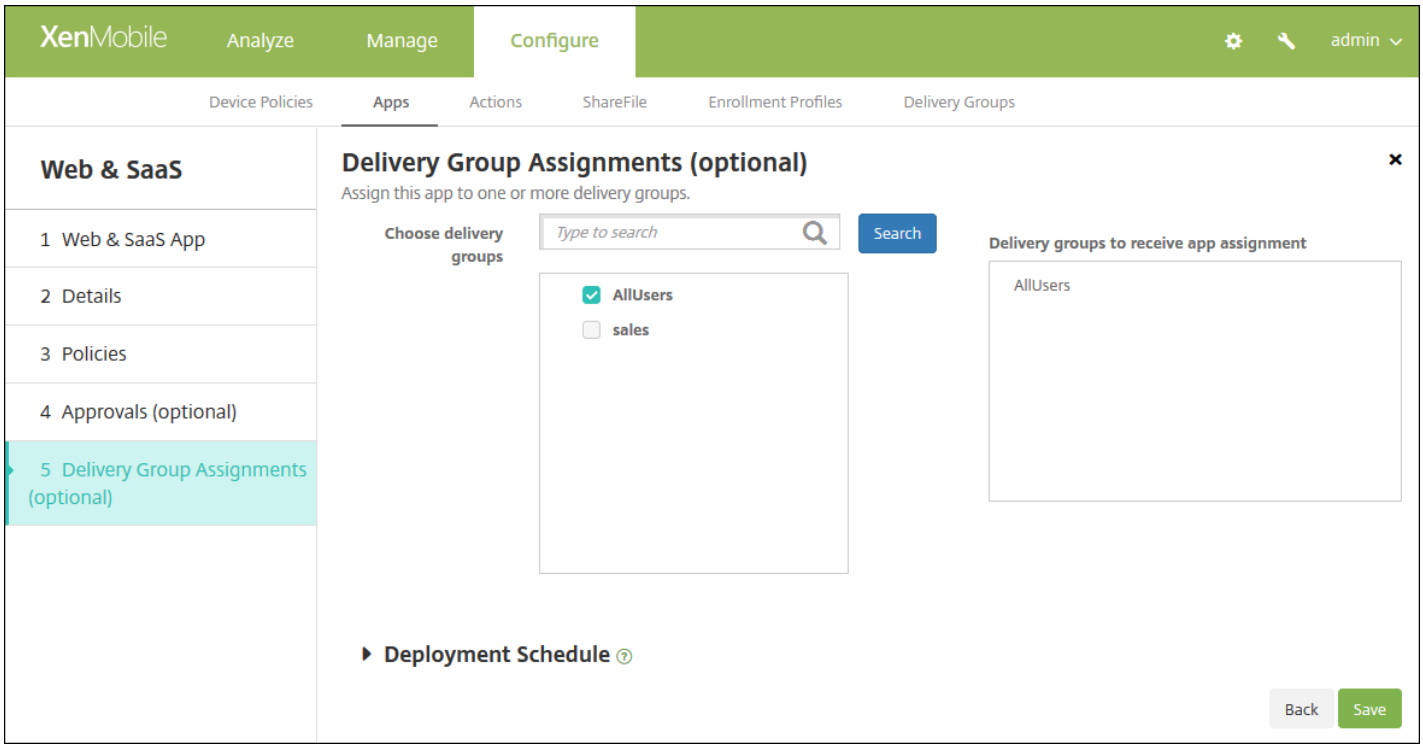


You use workflows when you need approval when creating user accounts. If you don't need to set up approval workflows, you can skip to Step 8.

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 additional required person's name in the search field and then click **Search**. Names originate in Active Directory.
  - When the person's name appears in the field, select the check box next to his or her name. The person's 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 in the list to which you want to assign the app. 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**.

Add an enterprise app

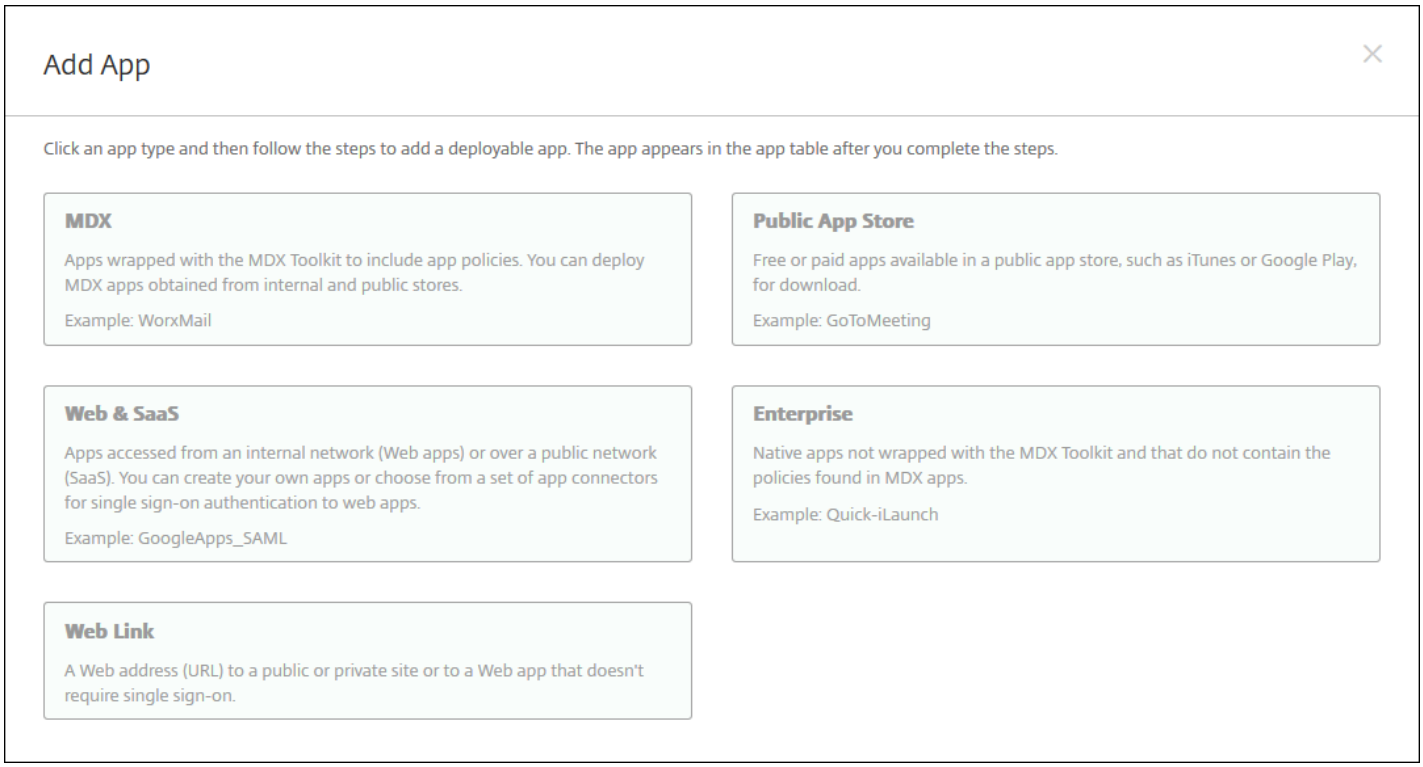
Enterprise apps in XenMobile represent native apps that are not wrapped with the MDX Toolkit and do not contain the

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):

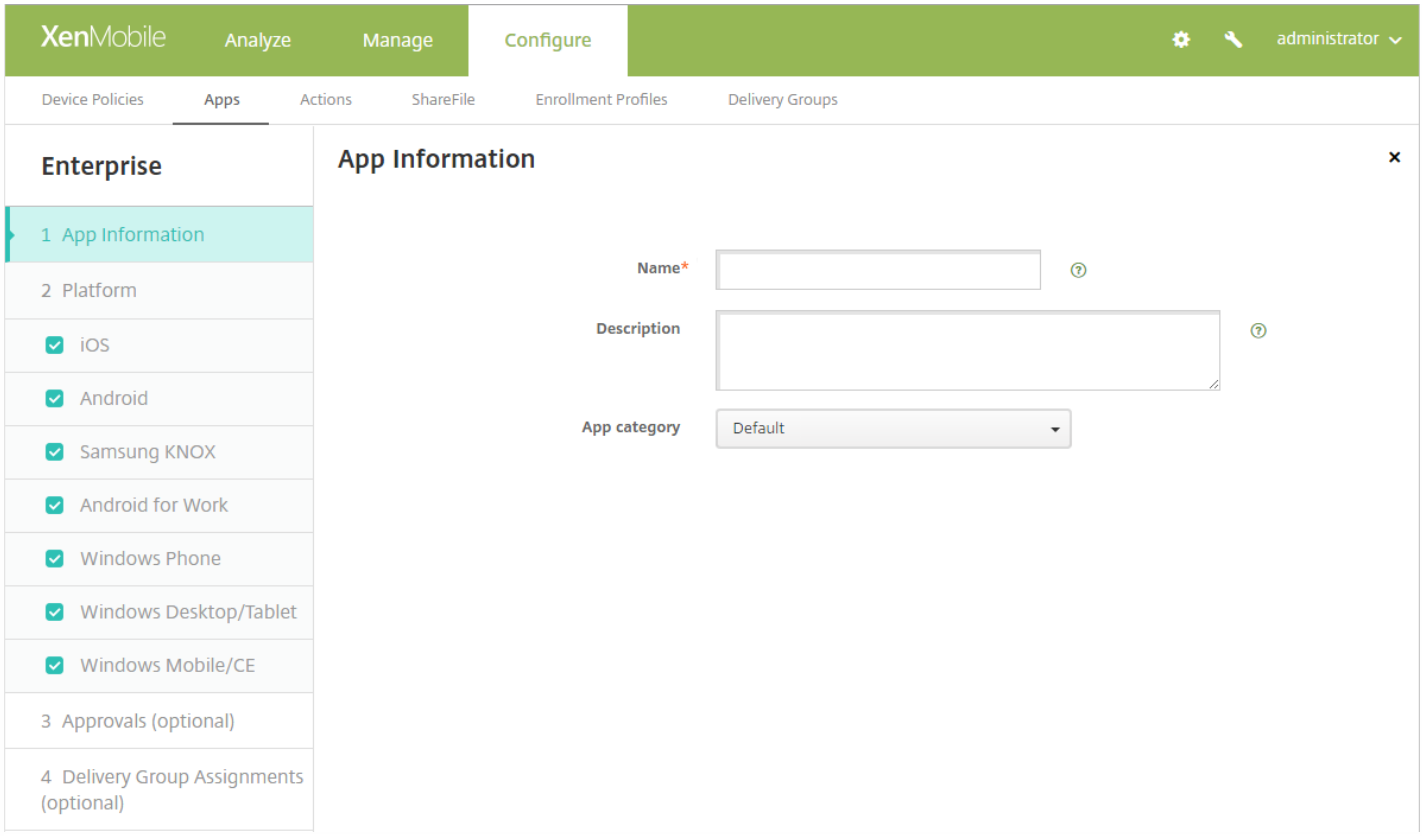
- iOS (.ipa file)
- Android (.apk file)
- Samsung KNOX (.apk file)
- Android for Work (.apk file)
- Windows Phone (.xap or .appx file)
- Windows Tablet (.appx file)
- Windows Mobile/CE (.cab file)

1. In the XenMobile console, click **Configure** > **Apps**. The **Apps** page opens.

2. Click **Add**. The **Add App** dialog box appears.



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 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 Creating App Categories in XenMobile.

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, refer to Step 10 for how to set that platform's deployment rules.

7. For each platform you chose, select the file to upload by clicking **Browse** and navigating to the file's location.

8. Click **Next**. The app information page for the platform appears.

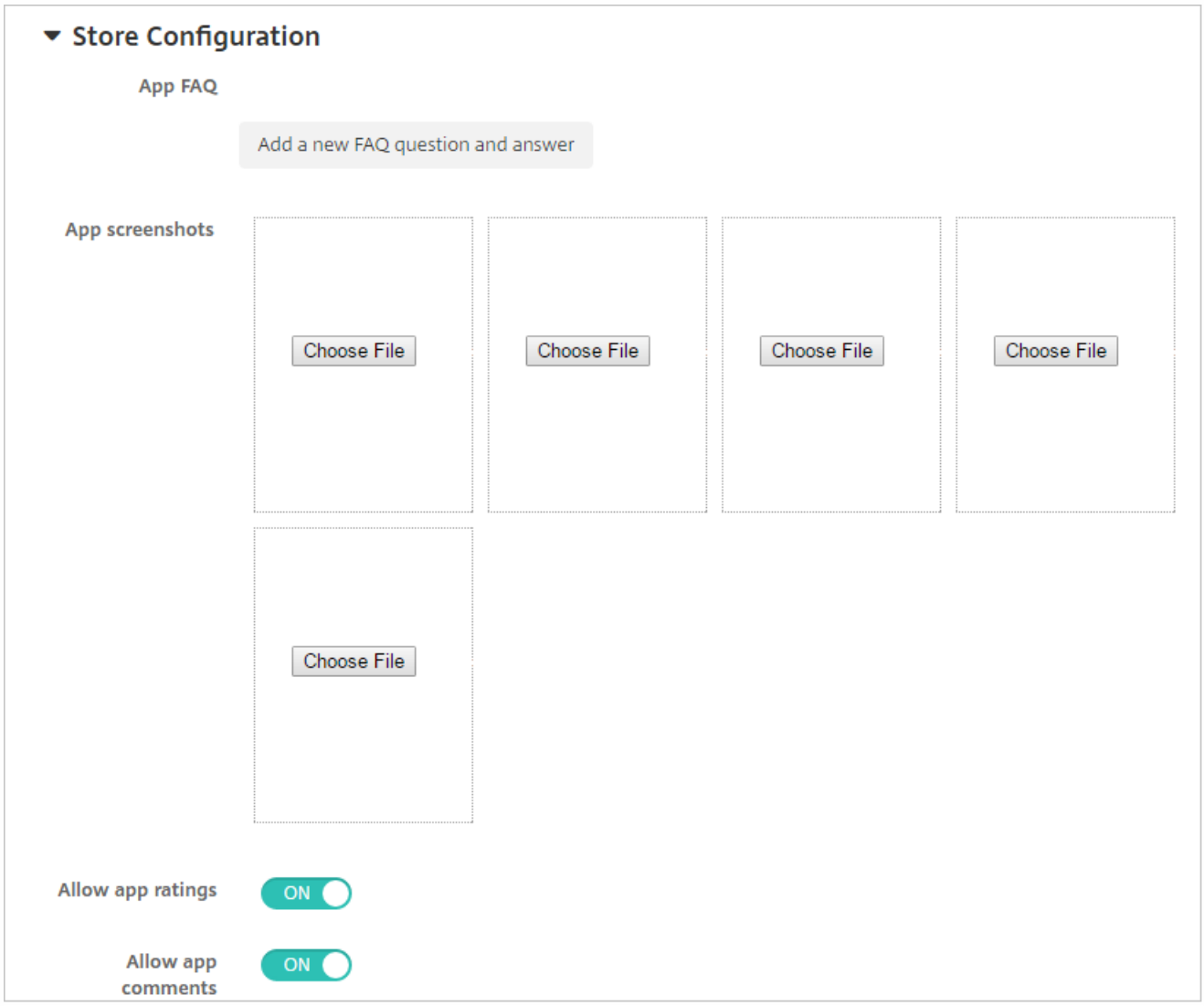
9. Configure the settings for the platform type, such as:

- **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.

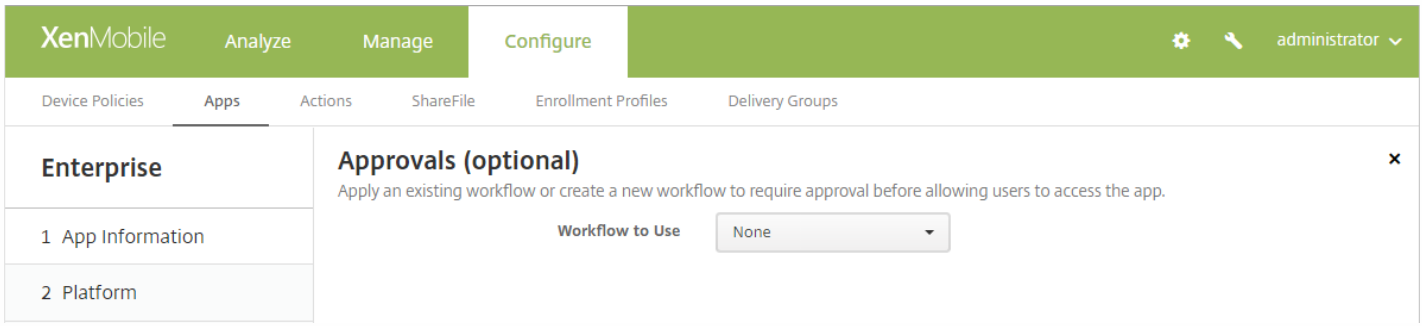
11. Expand **XenMobile Store Configuration**.



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.

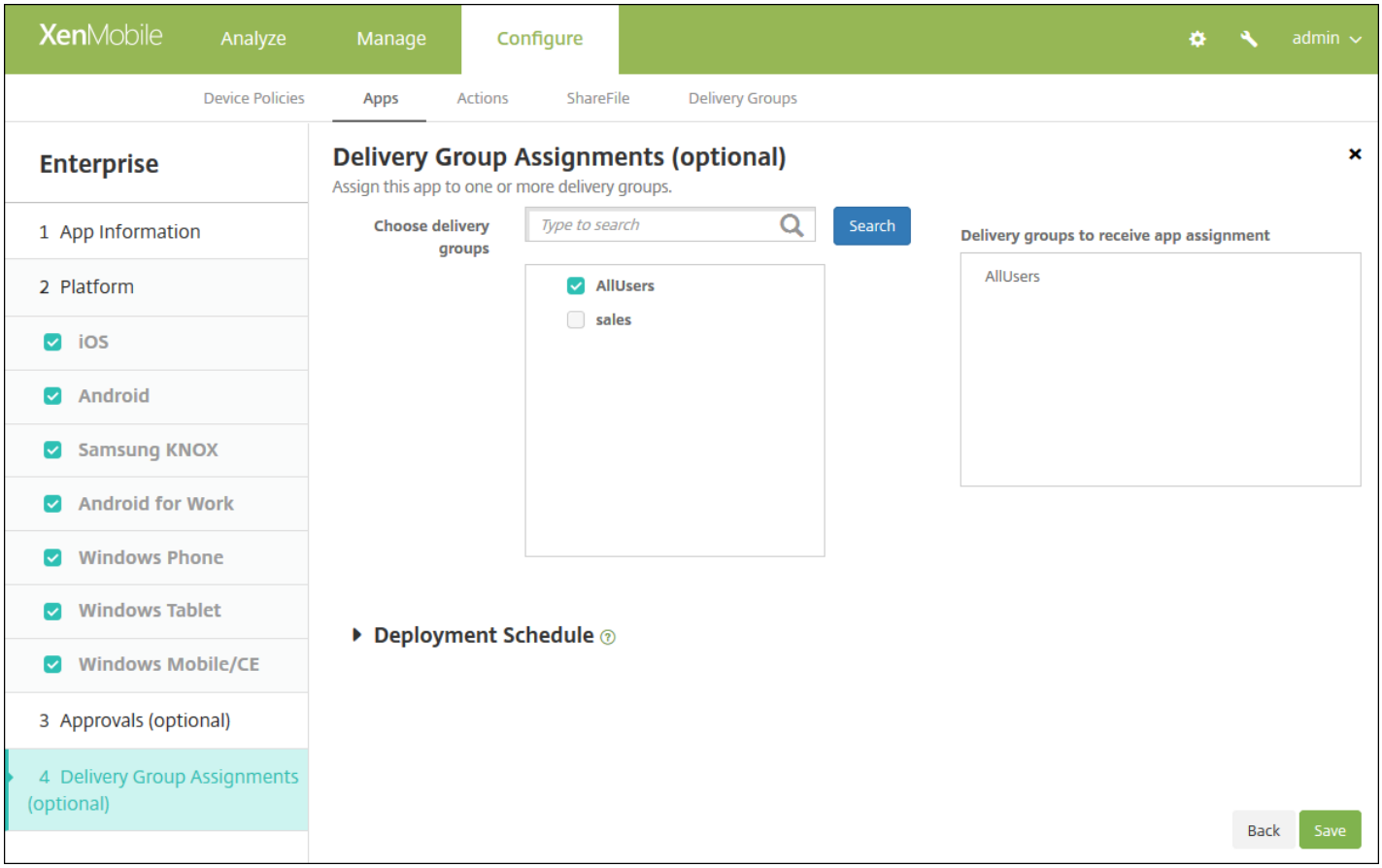


You use workflows when you need approval when creating user accounts. If you don't need to set up approval workflows, you can skip to Step 13.

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 additional required person's name in the search field and then click **Search**. Names originate in Active Directory.
  - When the person's name appears in the field, select the check box next to his or her name. The person's 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 to which you want to assign the app. 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**. 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.

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).

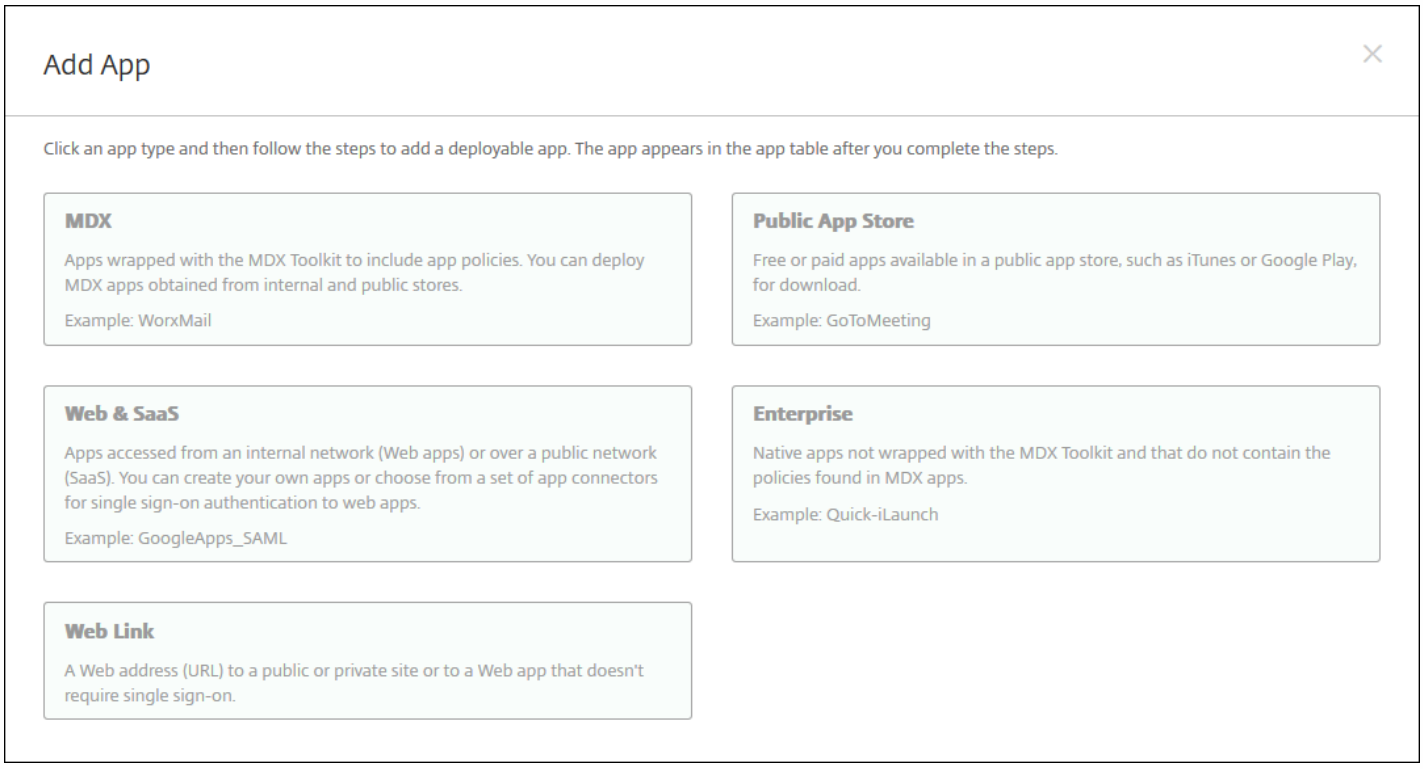
You can configure web links from the **Apps** tab in the XenMobile console. When you finish configuring the web link, the link appears as a link icon in the list in the **Apps** table. When users log on with Secure Hub, the link appears with the list of available apps and desktops.

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.



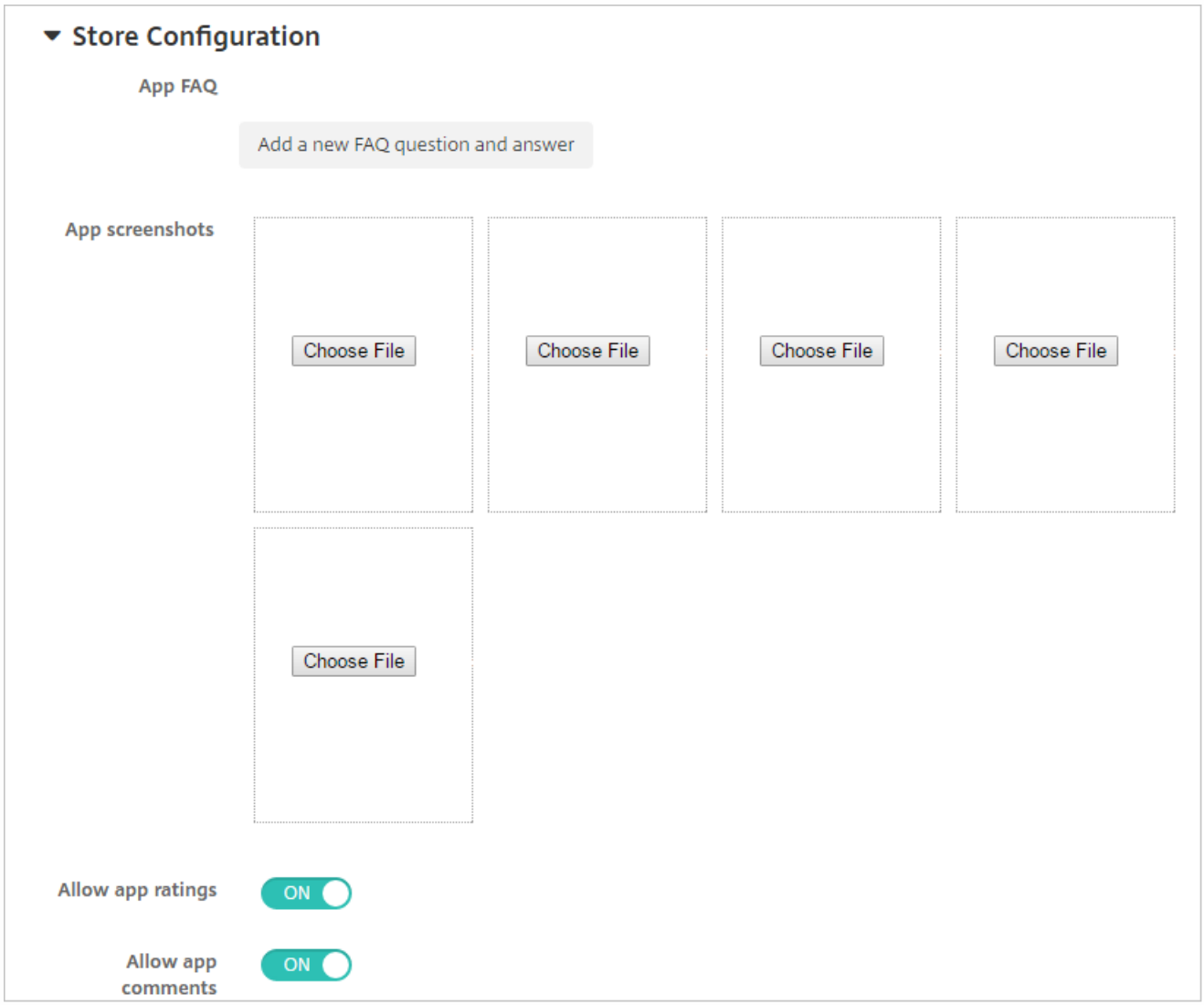
3. Click **Web Link**. The **App Information** page appears.

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's 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 at a later time.

5. 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**.

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 to which you want to assign the app. 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**. 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.

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, you need to 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.

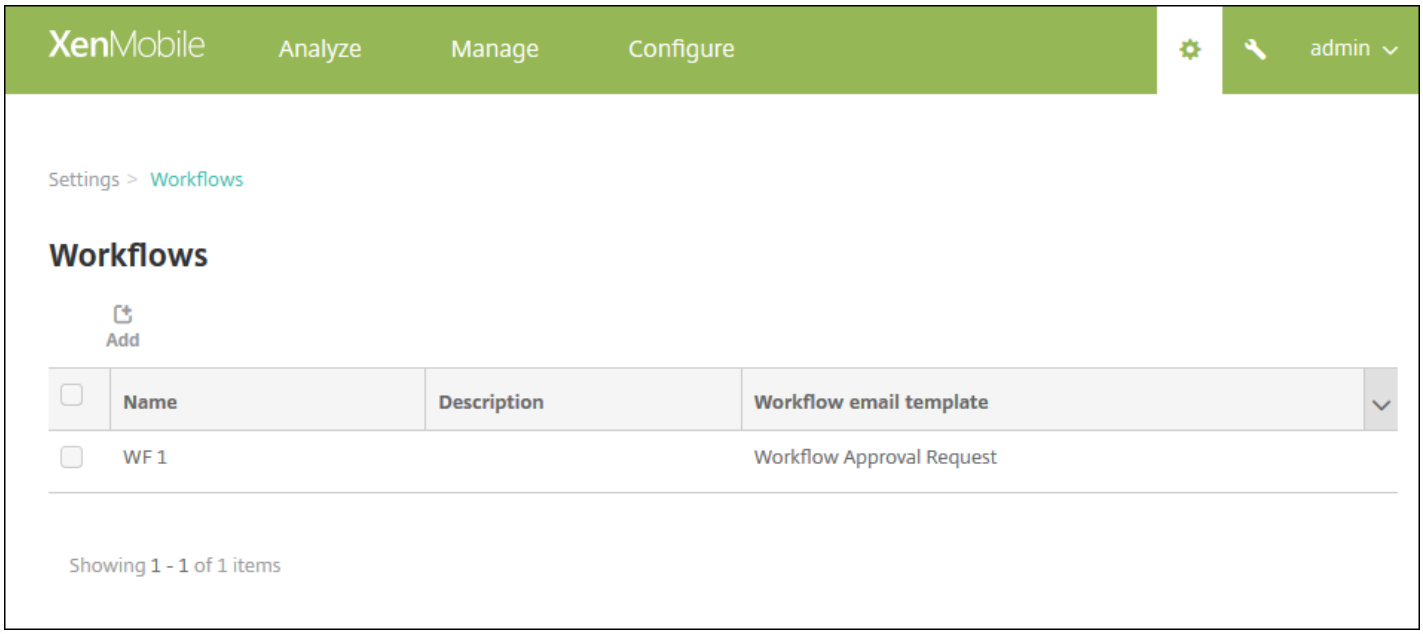
You can configure workflows in two places in XenMobile:

- 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.

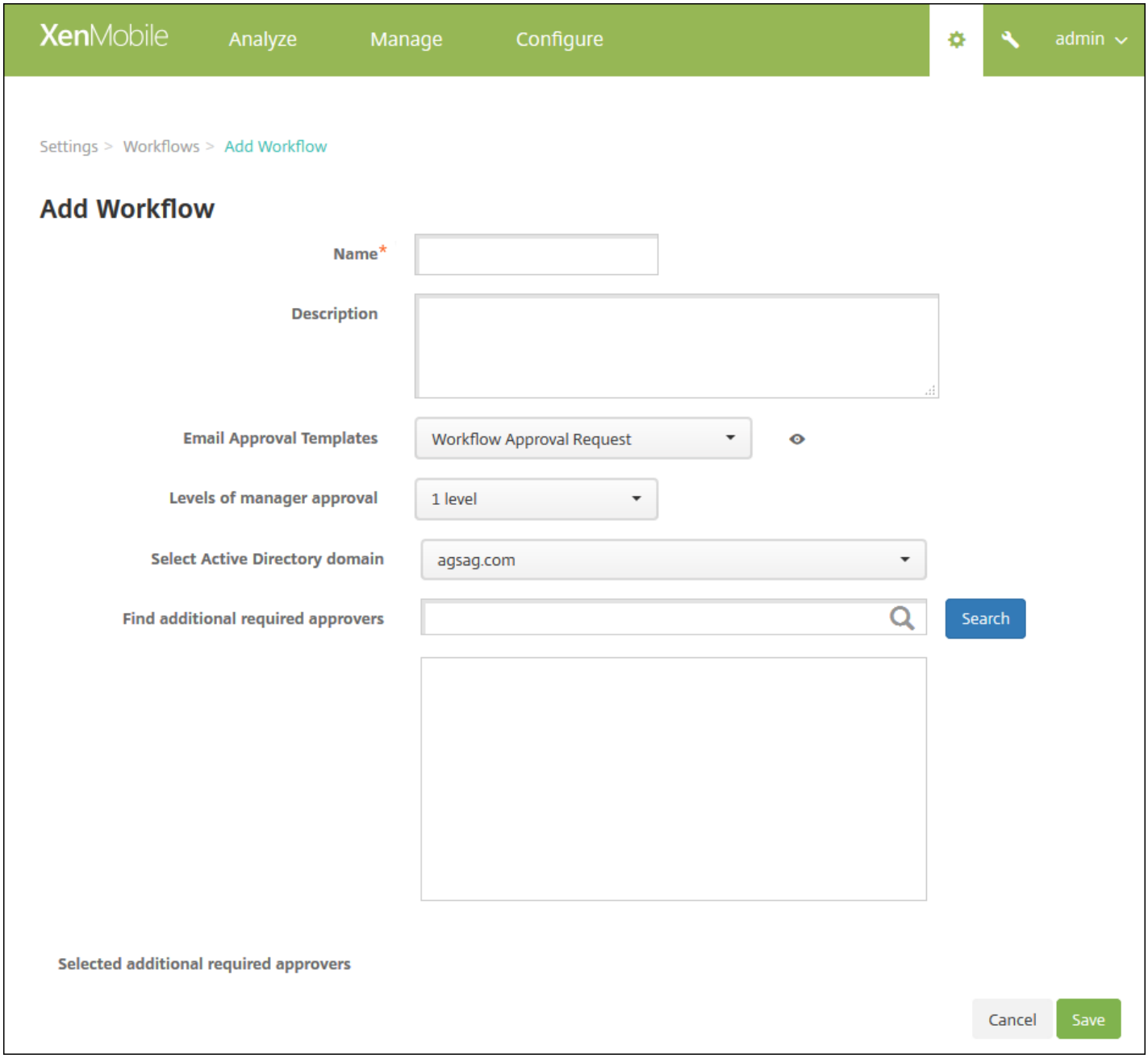
You can assign up to three levels for manager approval of user accounts. If you need other persons to approve the user account, you can search for and select additional persons by using the person's name or email address. When XenMobile finds the person, you then add him or her to the workflow. All individuals 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.

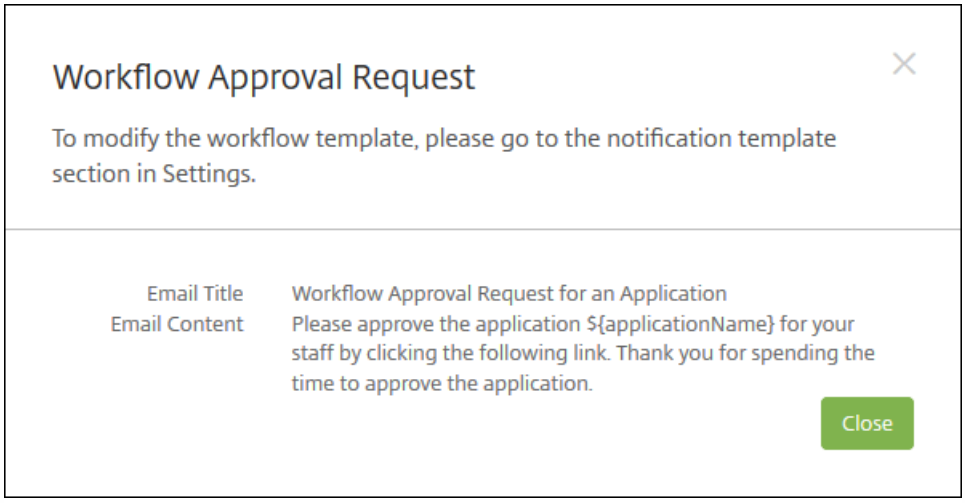


3. Click **Add**. The **Add Workflow** page appears.



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.



- **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 additional required person's name in the search field and then click Search. Names originate in Active Directory.
- When the person's name appears in the field, select the check box next to his or her name. The person's 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 a new workflow.

To view details and delete a workflow

1. On the **Workflows** page, in the list of existing workflows, select a specific workflow by clicking the row in the table or by checking 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

Nov 10, 2016

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

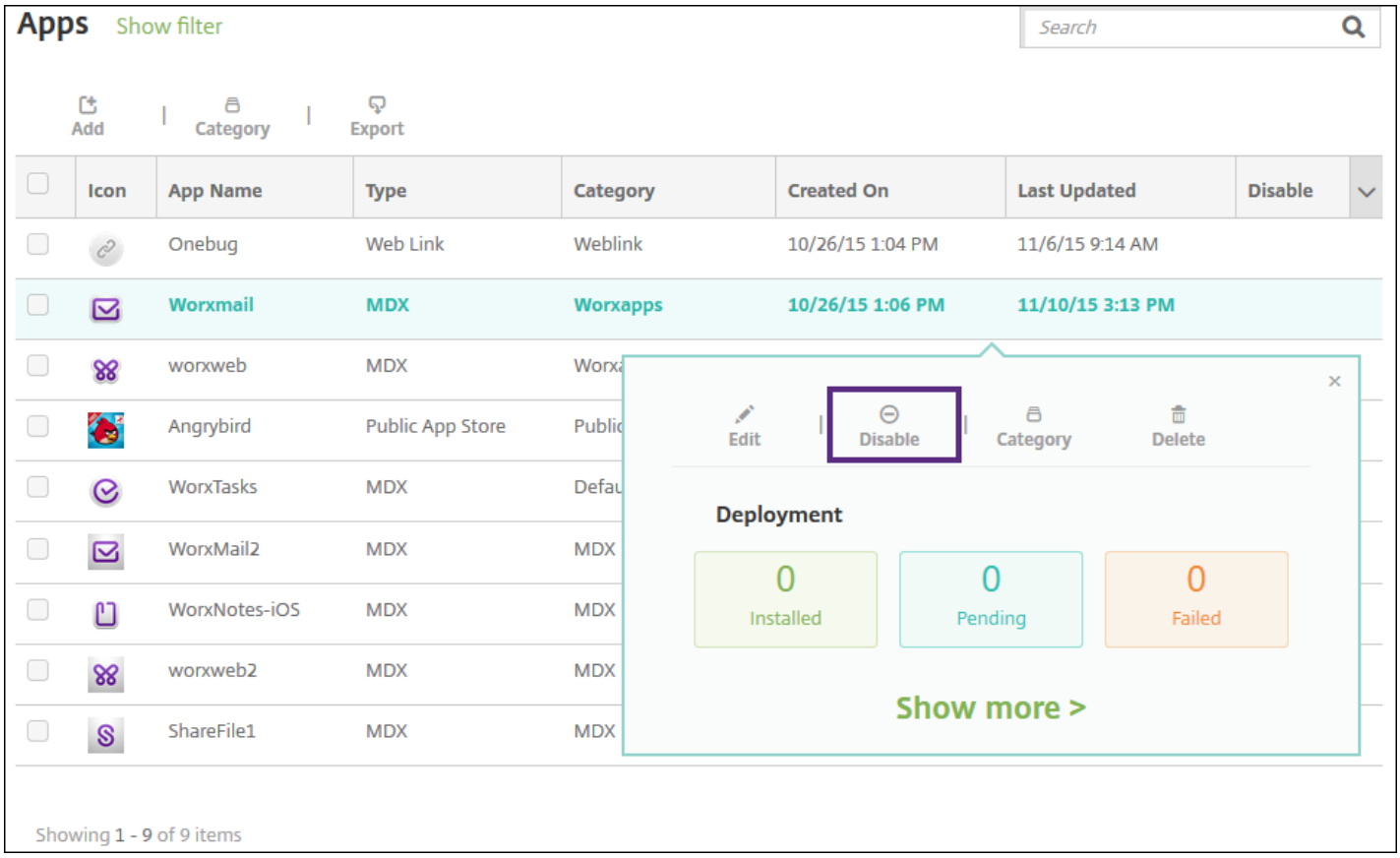
Nov 14, 2016

To upgrade an MDX or Enterprise app in XenMobile, you disable the app in the XenMobile console, and then you 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, click 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.



- Click **Disable** in the confirmation dialog box. *Disabled* appears in the **Disable** column for the app.

Note: Disabling an app puts the app in maintenance mode. While the app is disabled, users cannot reconnect to the app

after they log off. Disabling an app is an optional setting, but we recommend disabling the app to avoid issues with app functionality. Issues may result from policy updates, for example, or if users request a download at the same time you are uploading the app to 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:

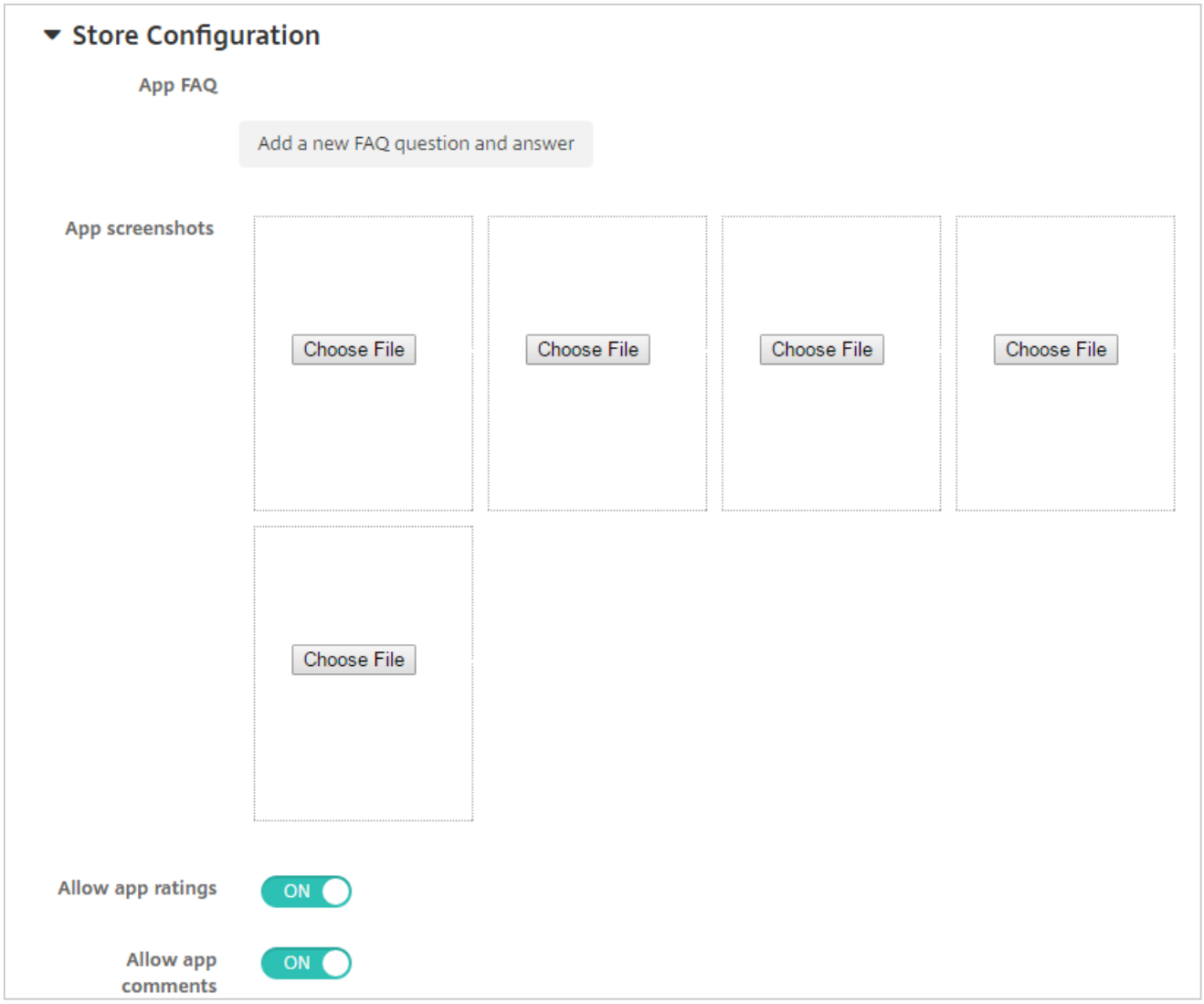
- **Name**: Optionally, change the app name.
- **Description**: Optionally, change the app description.
- **App category**: Optionally, change the app category.

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's location. The app uploads to XenMobile.
- Optionally, change the app details and policy settings for the platform.
- Optionally, configure deployment rules (see Step 7) and XenMobile Store configurations (see Step 8).

7. Configure the deployment rules

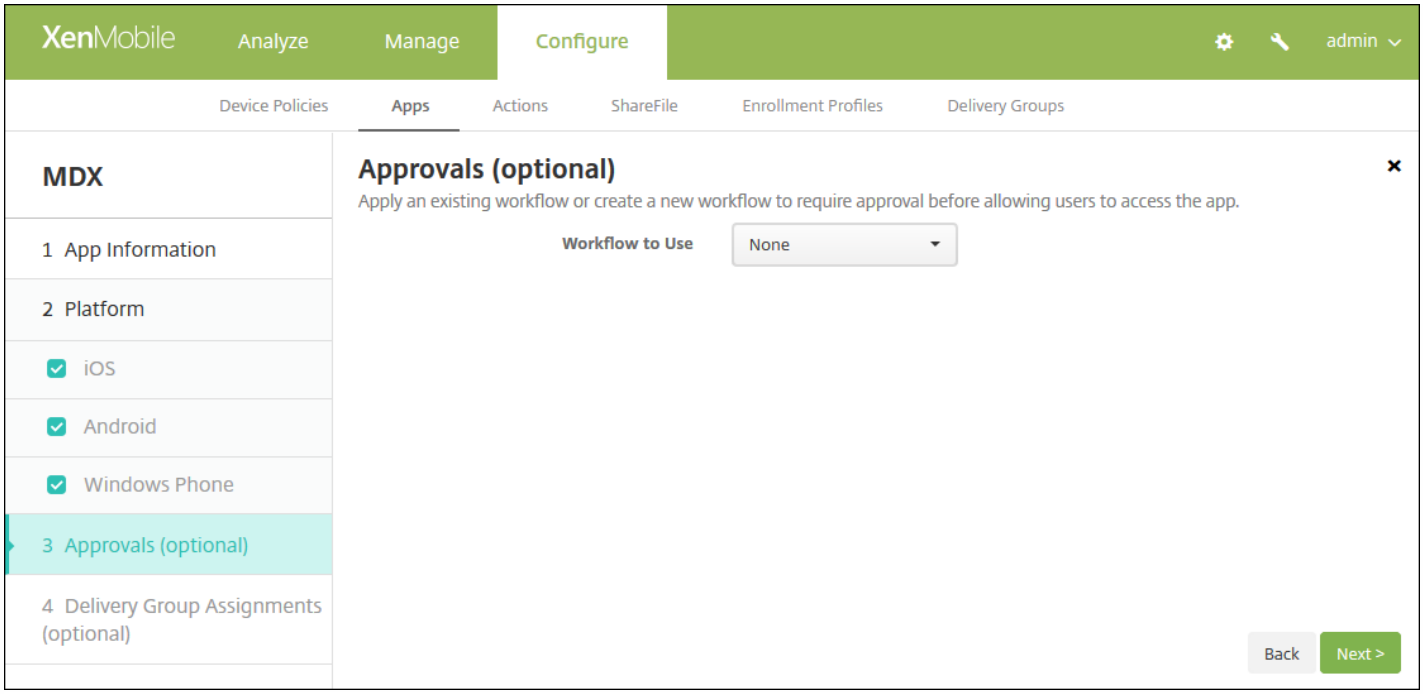
8. Expand **Store Configuration**.



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**.

9. Click **Next**. The **Approvals** page appears.

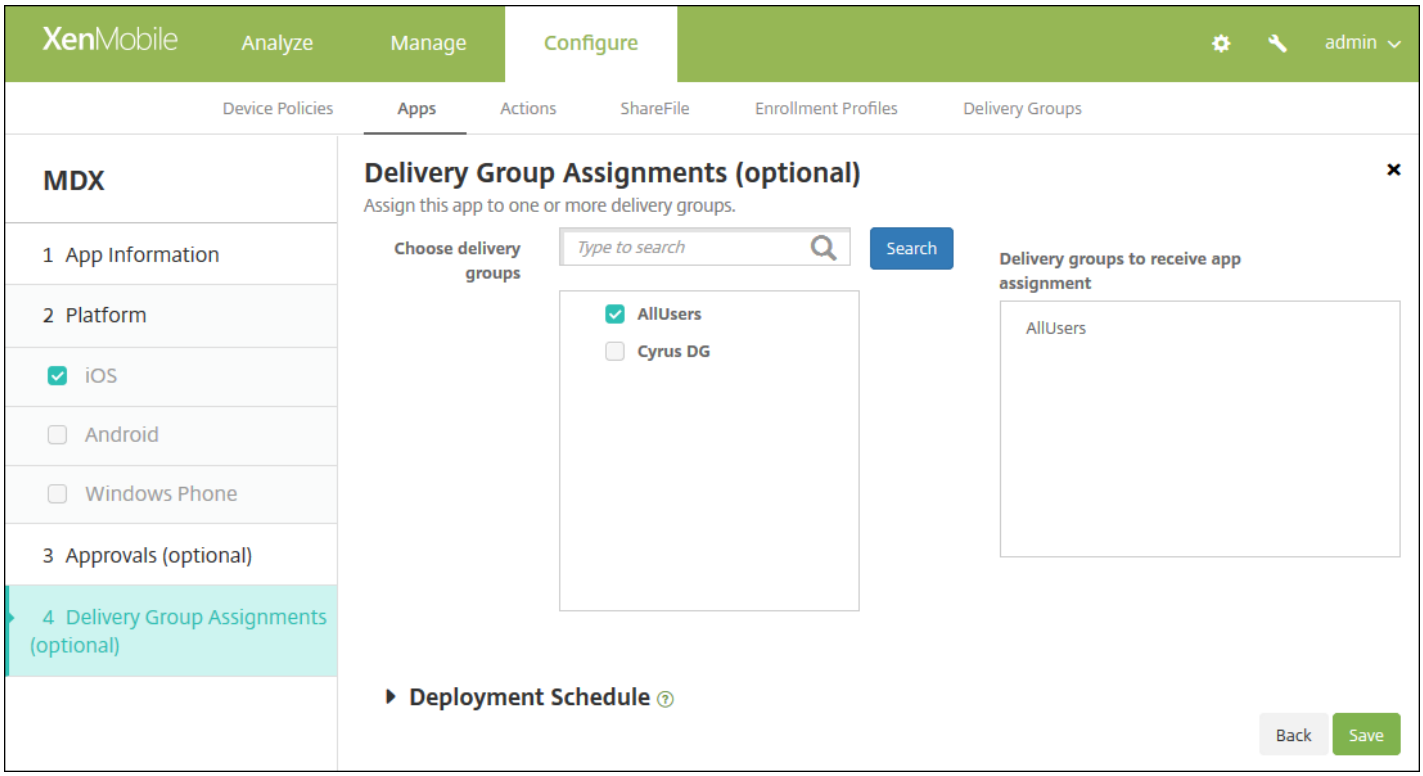


10. You use workflows when you need approval when creating user accounts. If you don't need to set up approval workflows, you can skip to Step 11.

Configure this setting 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 leve**l. 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 additional required person's name in the search field and then click **Search**. Names originate in Active Directory.
  - When the person's name appears in the field, select the check box next to his or her name. The person's 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.

11. Click **Next**. The **Deliver Group Assignmen**t page appears.



12. 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 app. The groups you select appear in the **Delivery groups to receive app assignment** list.

13. 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.

14. Click **Save**. The **Apps** page appears.

15. 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

Oct 05, 2016

For a table listing the MDX app policies for iOS, Android, and Windows Phone 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

Oct 05, 2016

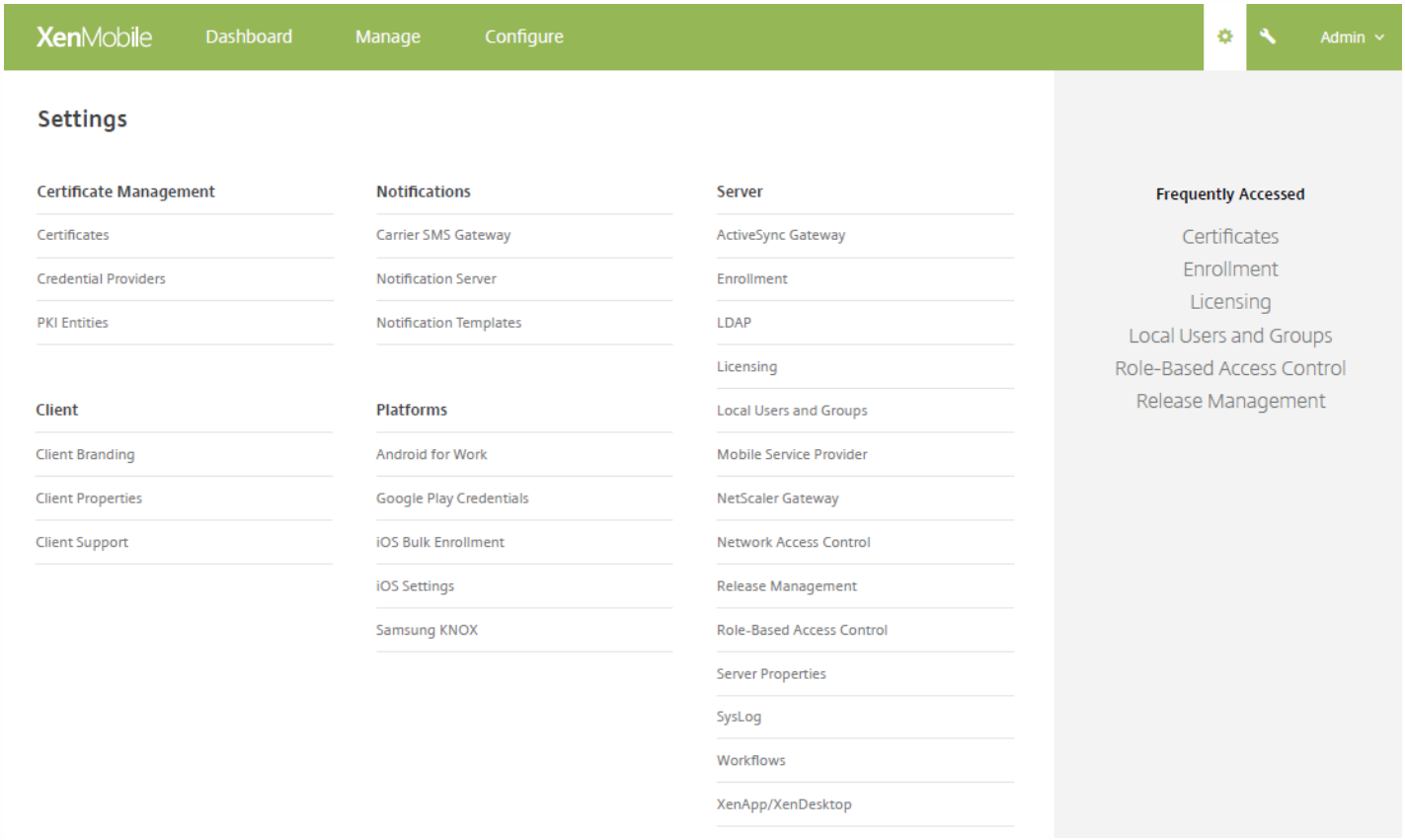
You can set the way apps appear in the store and add a logo to brand Secure Hub and the XenMobile Store on mobile devices for iOS and Android.

Note: Before you begin, make sure you have your custom image ready and accessible.

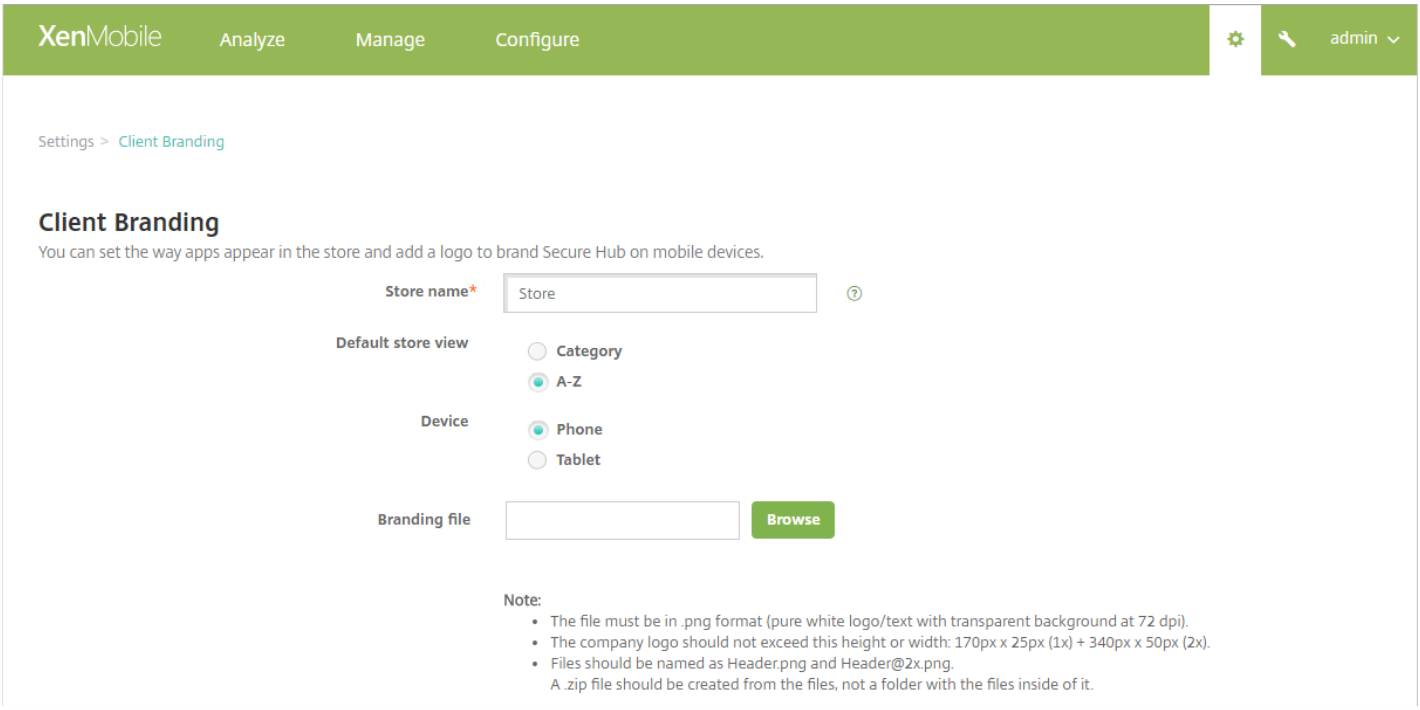
The custom image must meet these requirements:

- 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.



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

Mar 02, 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 device-level restrictions:

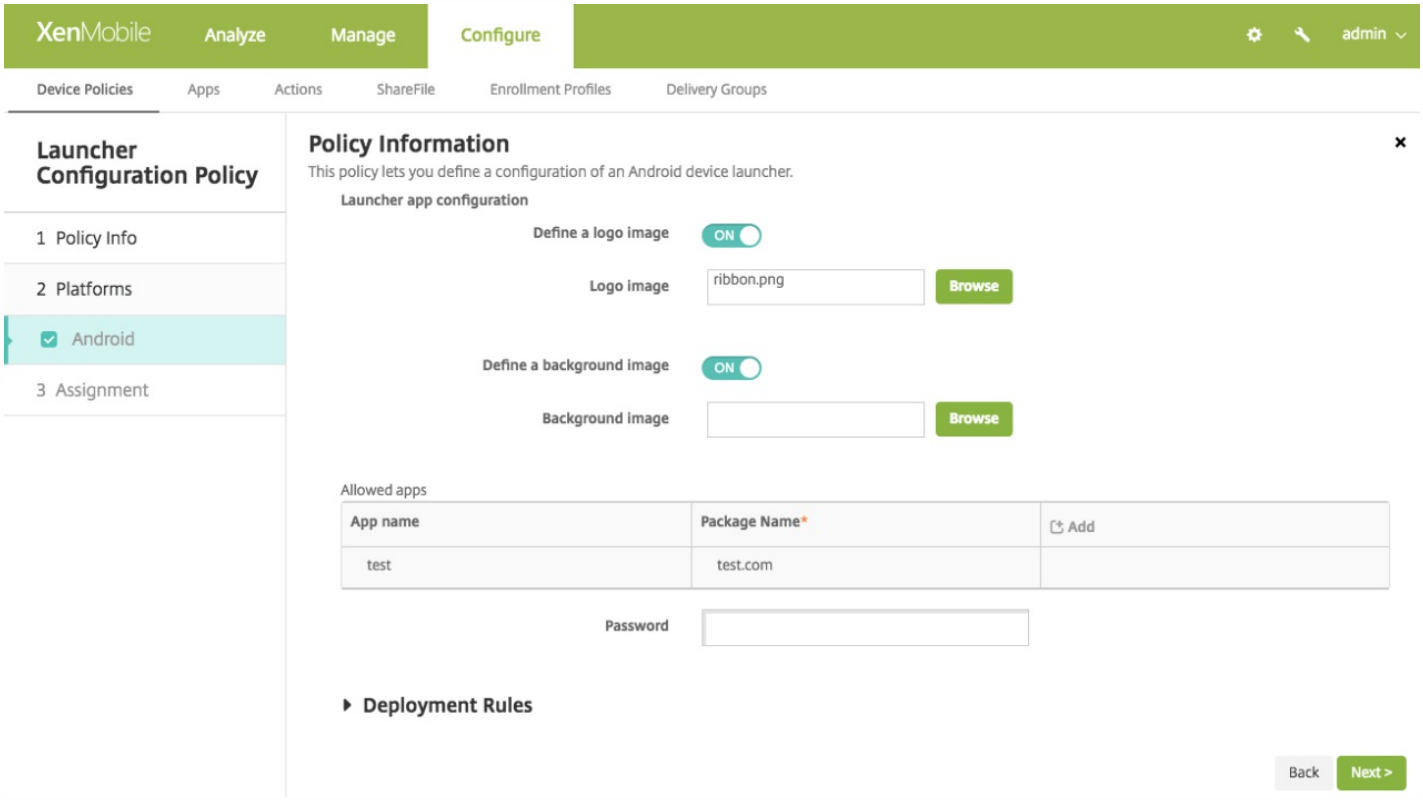
- Manage Android devices so that users can access only the apps that you specify.
- Optionally specify a custom logo image for the Citrix Launcher icon and a custom background image for Citrix Launcher.
- Specify a password that users must enter to exit the launcher.

The device launcher provides built-in access to device settings for WiFi, Bluetooth, device passcode, and other settings. Citrix Launcher isn't intended as an extra layer of security over what the device platform already provides.

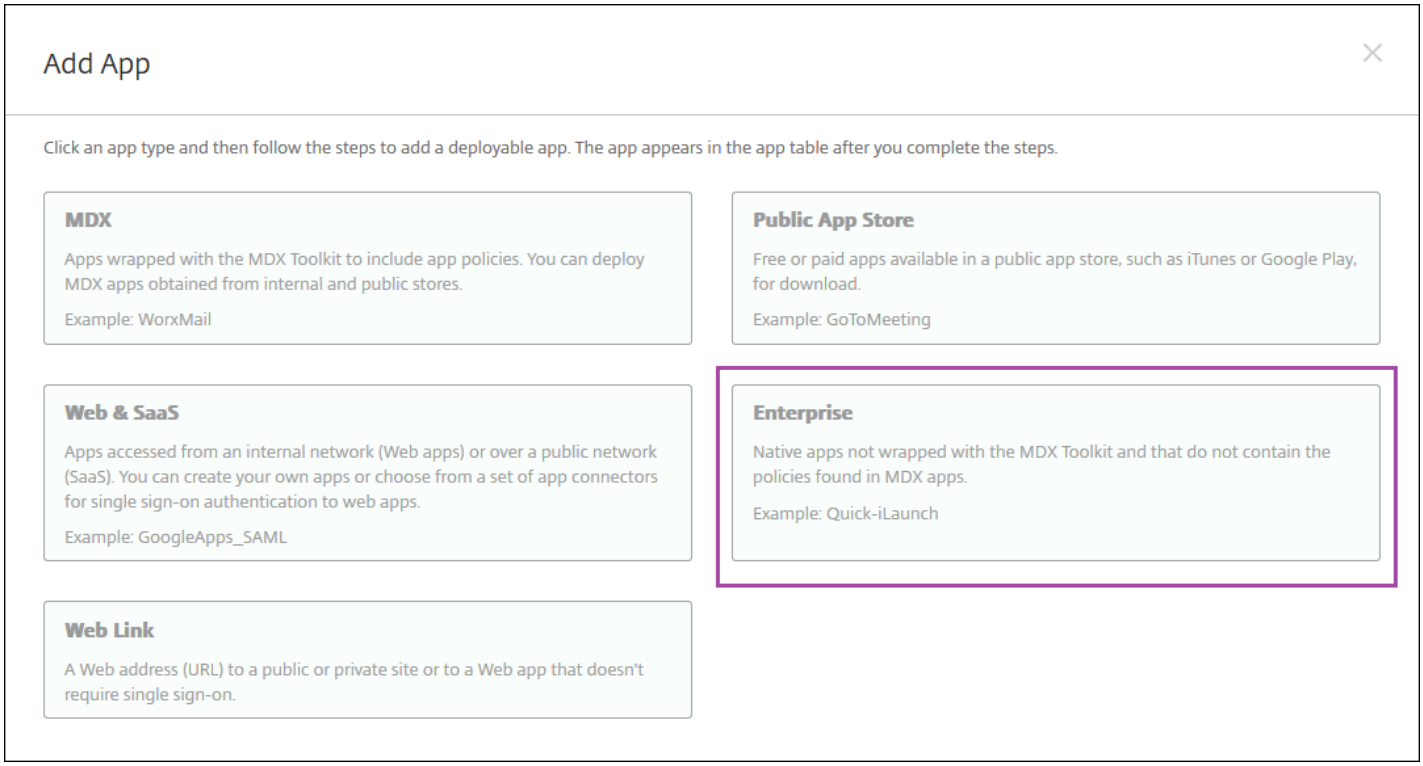
To provide Citrix Launcher to Android devices, follow these general steps.

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 to upload 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.

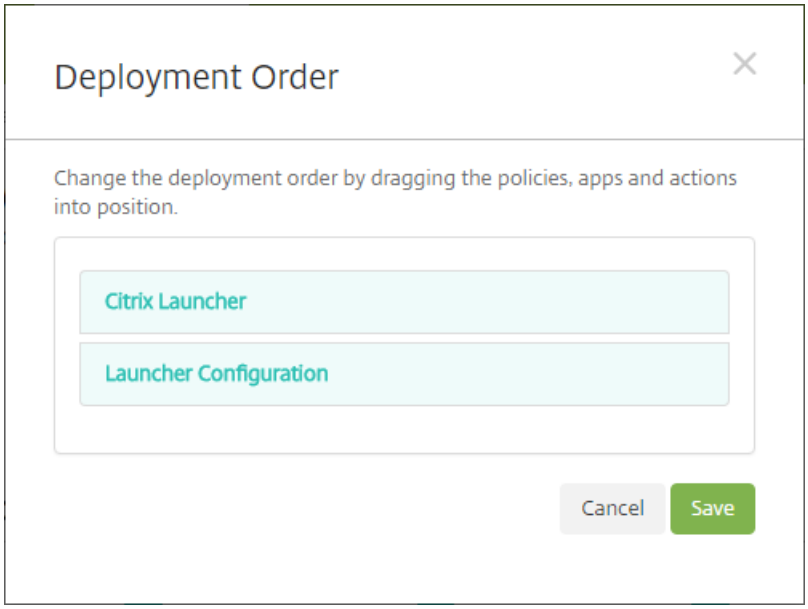


3. Add the Citrix Launcher app to XenMobile as an enterprise app. In **Configure > Apps**, click **Add**. Then, click **Enterprise**. For more information, see Add an enterprise app.



4. Create a Delivery Group for Citrix Launcher with the following configuration in **Configure > Delivery groups**:

- On the **Policies** page, add the **Launcher Configuration Policy**.
- On the **Apps** page, drag **Citrix Launcher** to **Required Apps**.
- On the **Summary** page, click **Deployment Order** and verify that the **Citrix Launcher** app precedes the **Launcher Configuration** policy.



For more information, see Deploy resources.

iOS Volume Purchase Plan

Jan 19, 2017

You can manage iOS app licensing by using the Apple iOS Volume Purchase Program (VPP), a simple, scalable solution to manage your organization's content needs. VPP 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 apps, including XenMobile apps and other MDX apps, directly to your devices or you assign content to your users using redeemable codes. You configure settings specific to the iOS Volume Purchase Plan (VPP) in XenMobile.

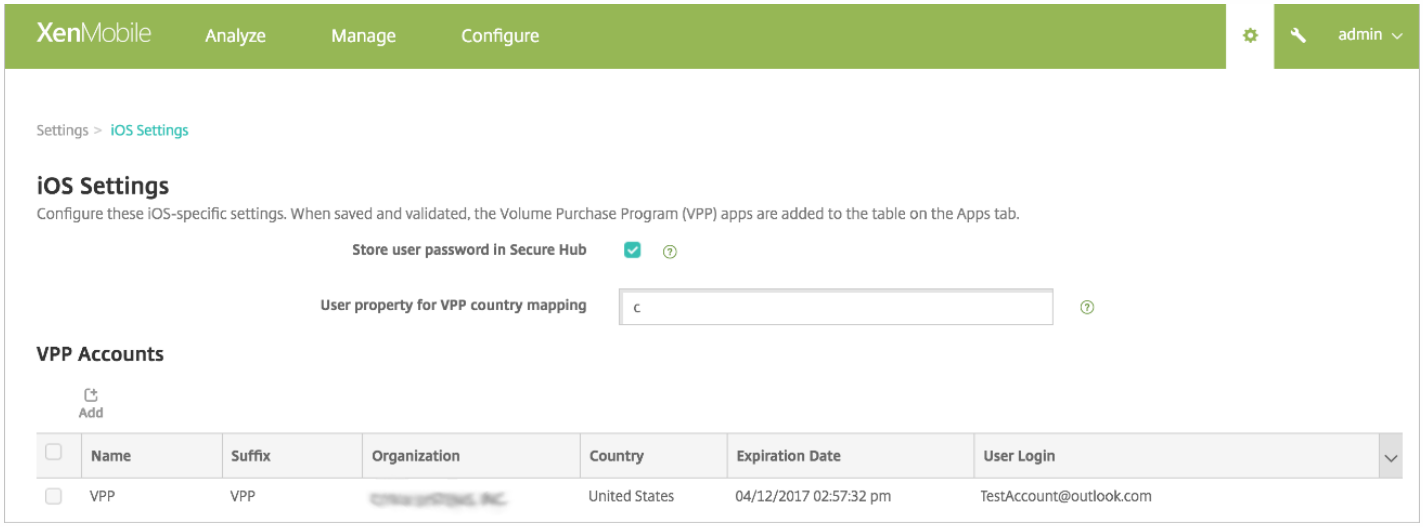
This article focuses on using VPP with managed licenses, which enables you to use XenMobile to distribute apps. If you currently use redemption codes and want to change to managed distribution, see the Apple Support document, Migrate from redemption codes to managed distribution with the Volume Purchase Program.

For information about the iOS Volume Purchase Program, 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 and validate the iOS VPP settings in XenMobile, the purchased apps are added to the table on the **Configure > Apps** page in the XenMobile console.

1. In the XenMobile web 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.



3. Configure these settings:

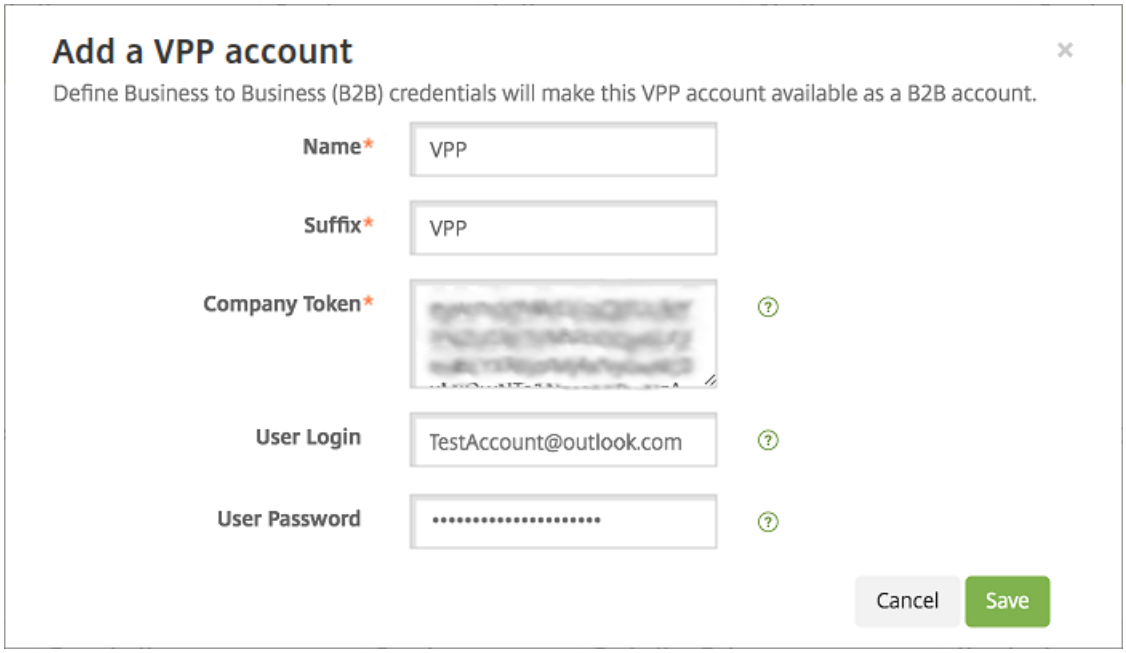
- **Store user password in Secure Hub**: Select whether to store a user name and password in Secure Hub for XenMobile authentication. The default is to store the information using this secure method.
- **User property for VPP country mapping**: Type a code to allow users to download apps from country-specific 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.



Configure these settings for each account you add:

Note: If you are using Apple Configurator 1, upload a license file as follows: Go to **Configure > Apps**, go to a platform page, and 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 as well as other information like the country code and expiry. Save the file in a secure location.
- **User Login**: Type an optional authorized VPP account admin name used to import custom B2B apps.
- **User Password**: Type the VPP account admin password.

5. Click **Save** to close the dialog box.

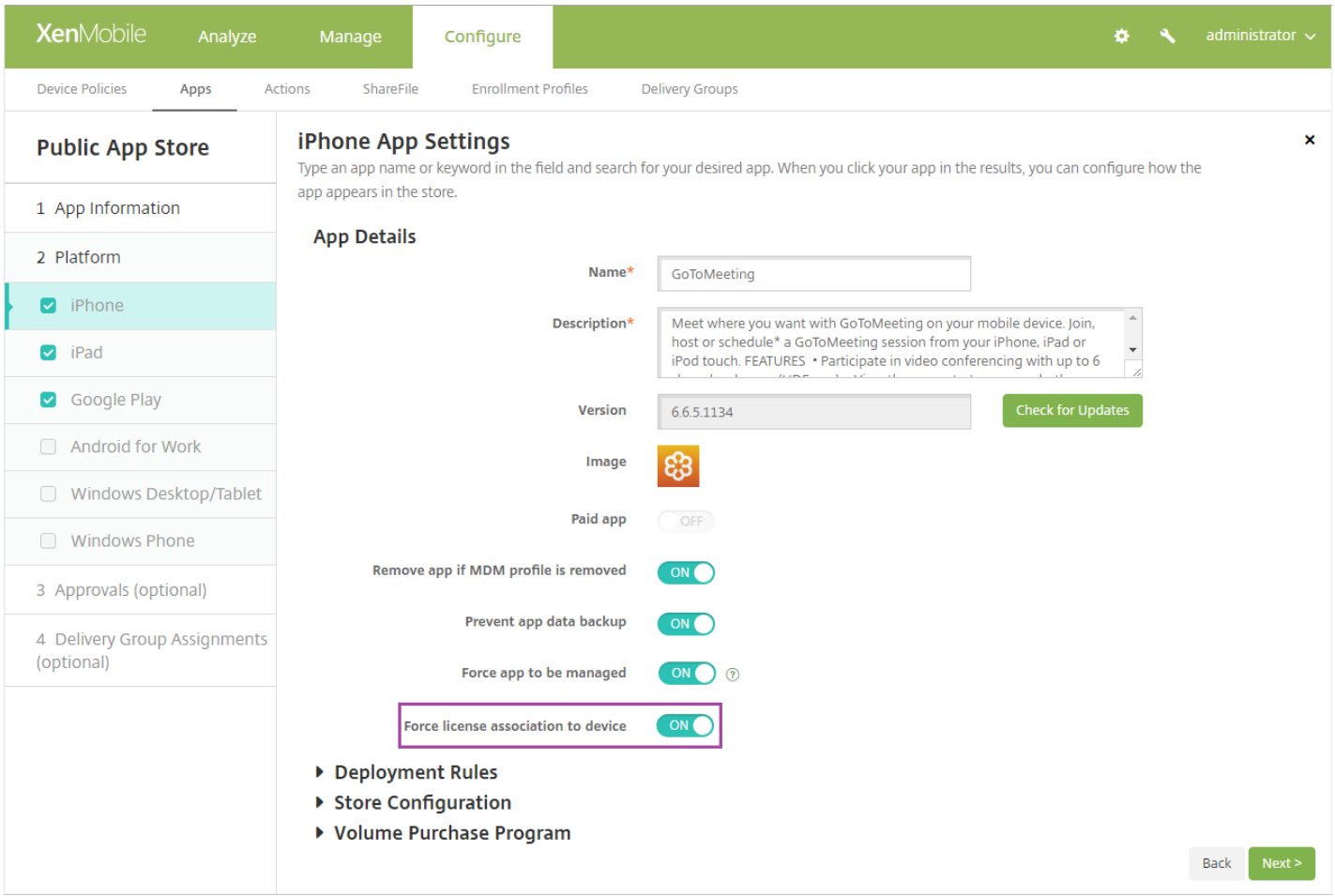
6. Click **Save** to save the iOS settings.

A message appears to let you know that XenMobile will add the apps to the list on the **Configure > Apps** page. On the **Configure > Apps** page, notice that the name of the apps pulled in from your VPP account include the suffix you provided in the above configuration.

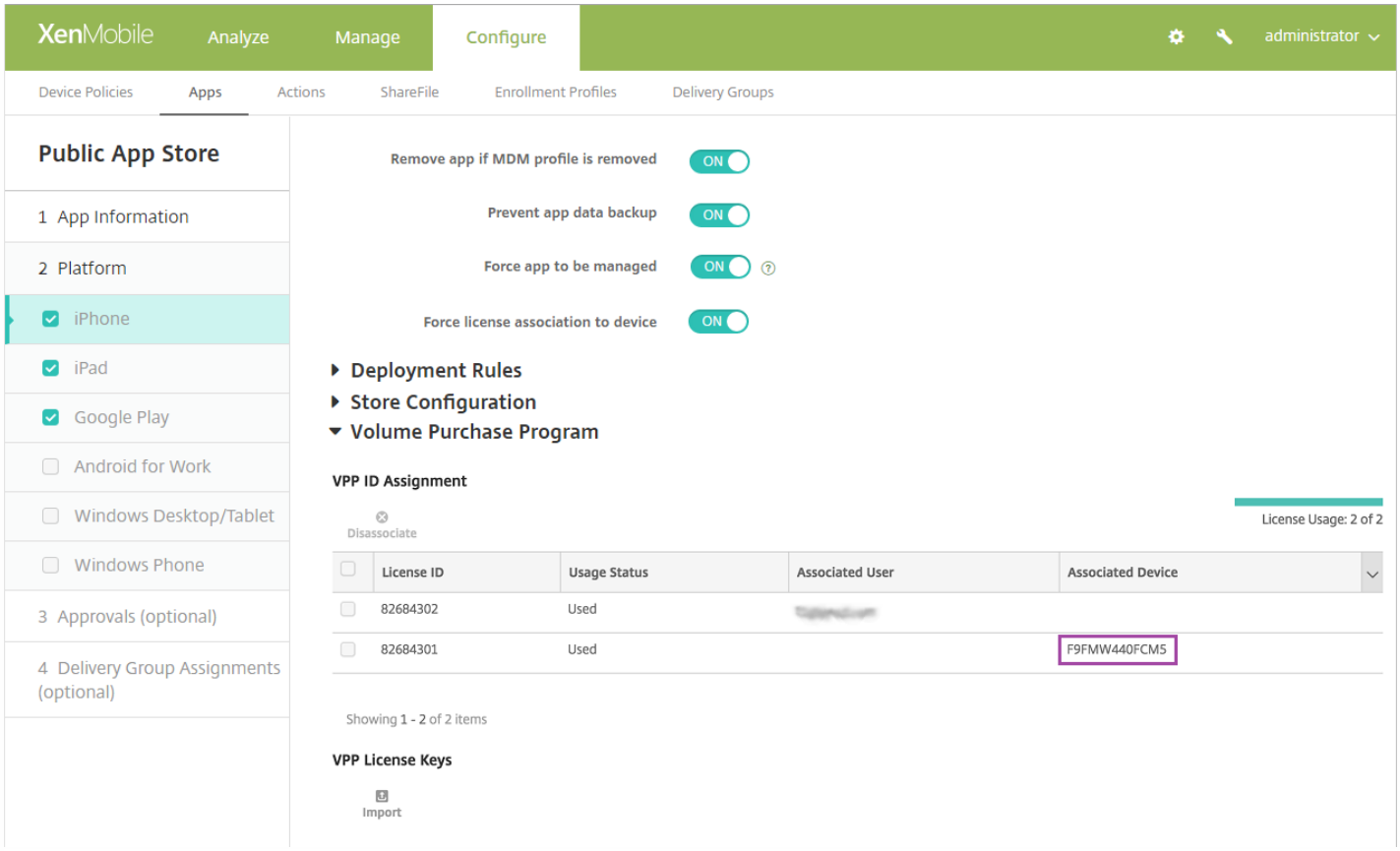
You can now configure the VPP app settings and then tune your delivery group and device policy settings for VPP apps. After you complete those configurations, users can enroll their devices. The following notes provide considerations for

those processes.

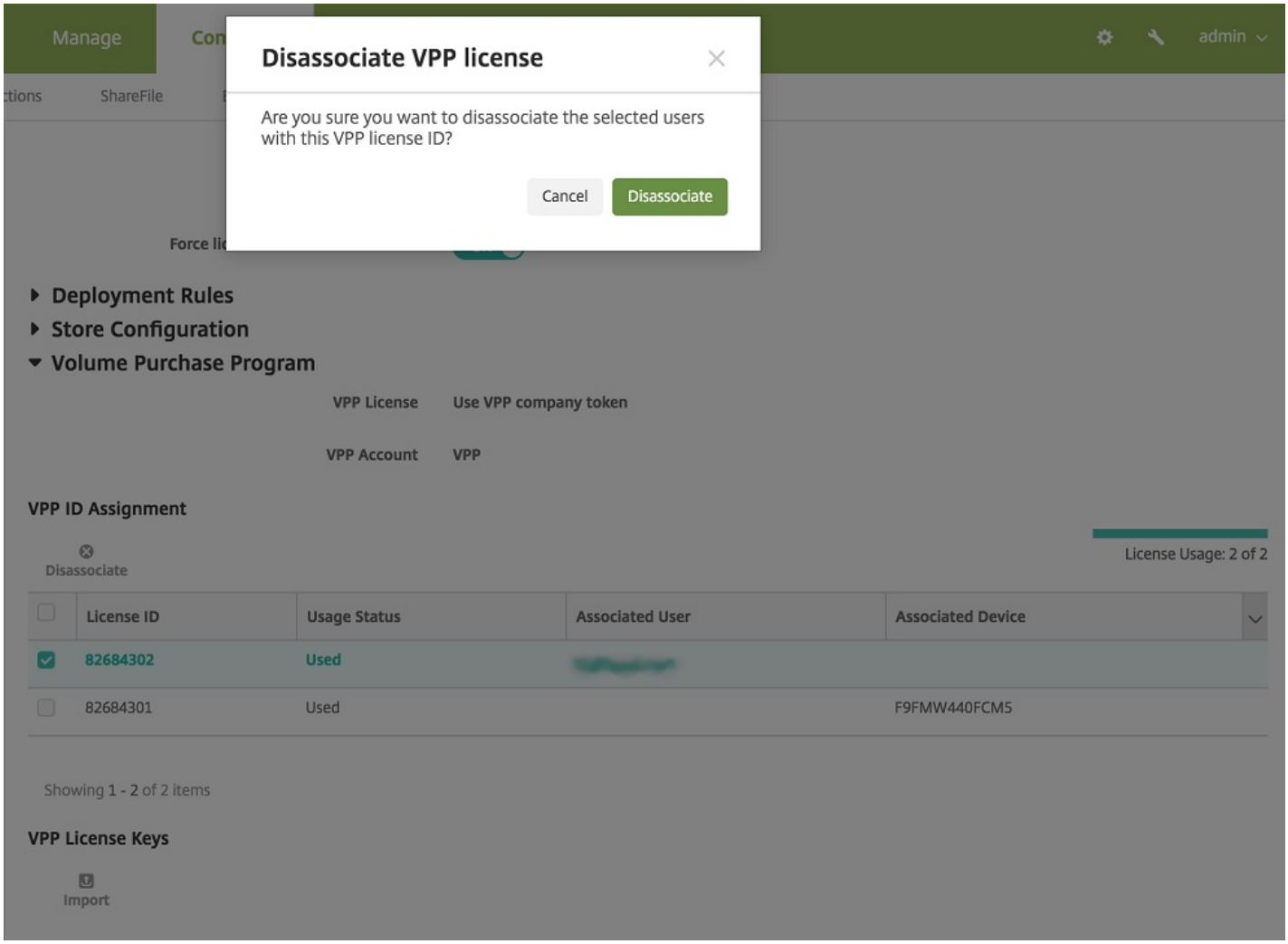
- When configuring VPP app settings (**Configure > Apps**), enable **Force license association to device**. An advantage of using Apple VPP and DEP with supervised devices is the ability to use XenMobile to assign the app at the device (rather than user) level. As a result, you don't have to use an Apple ID device, users won't receive an invitation to join the VPP program, and users can download the apps without signing into their iTunes account.



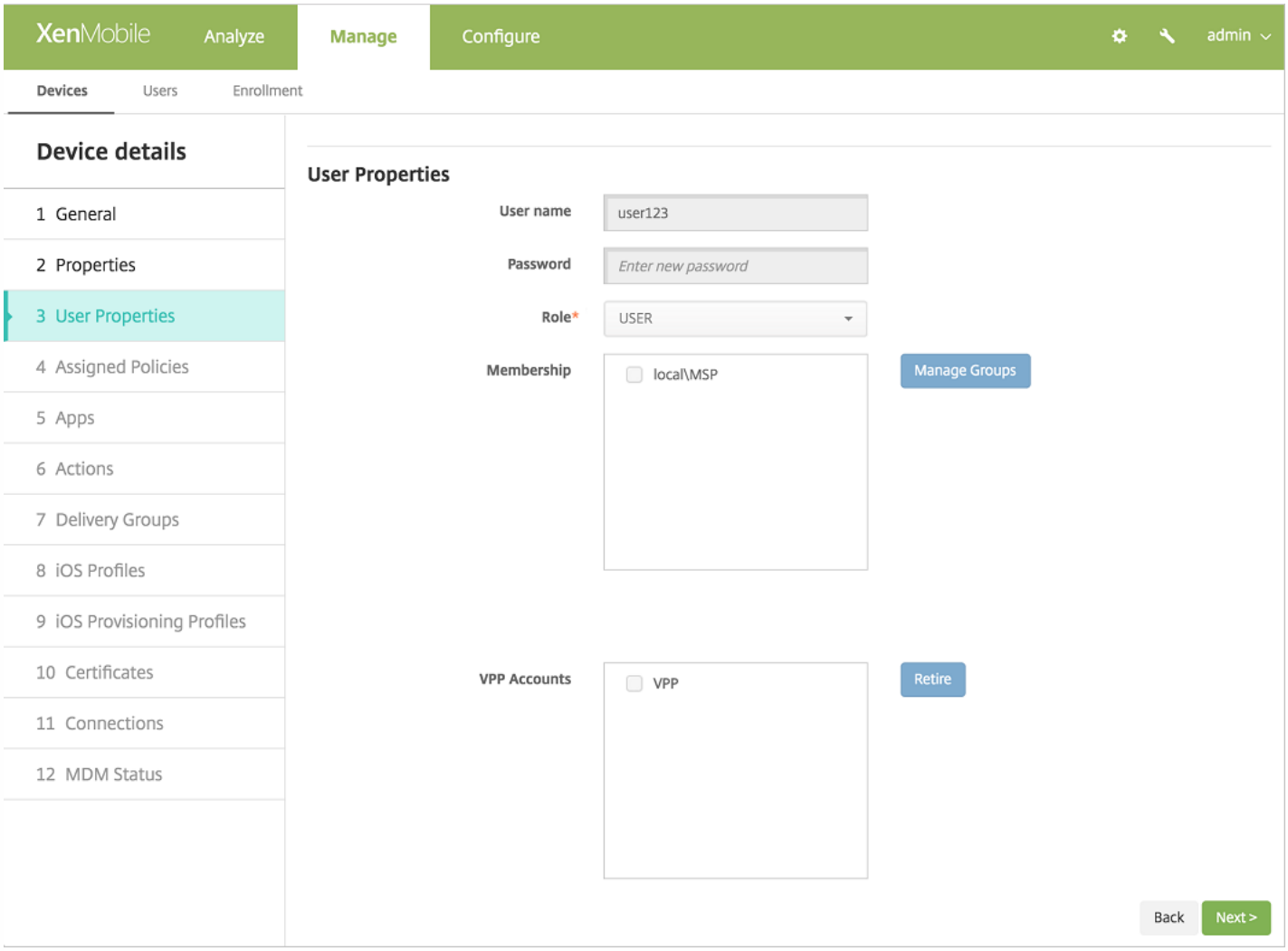
To view the VPP info for that app, expand **Volume Purchase Program**. Notice in the **VPP ID Assignment** table, the license is associated with a device. The device serial number appears in the **Associated Device** column. If the user removes the token and then imports it again, the word **Hidden** appears instead of the serial number, due to Apple privacy restrictions.



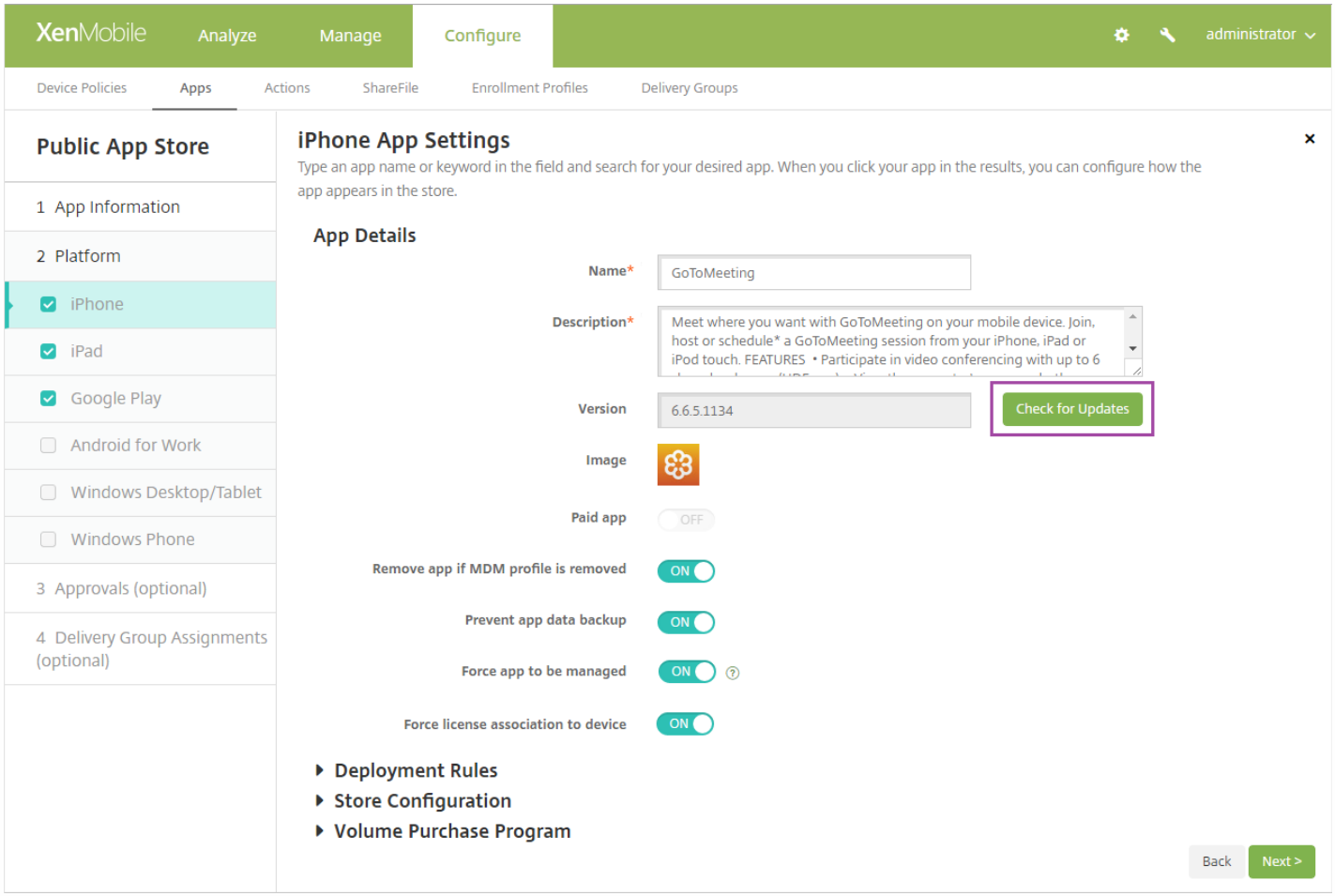
To disassociate a license, click the row for the license and click **Disassociate**.



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**.



- 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** and, on the **Apps** page, move the app to the **Required Apps** list.
- When an update for a public app store app is available, and that app is pushed through VPP, the app doesn't automatically update on devices until you check for updates and apply them. For example, to push an update for Secure Hub (if assigned to device, not user), in **Configure > Apps**, on a platform page, click **Check for Updates** and apply the update.



XenApp and XenDesktop through Citrix Secure Hub

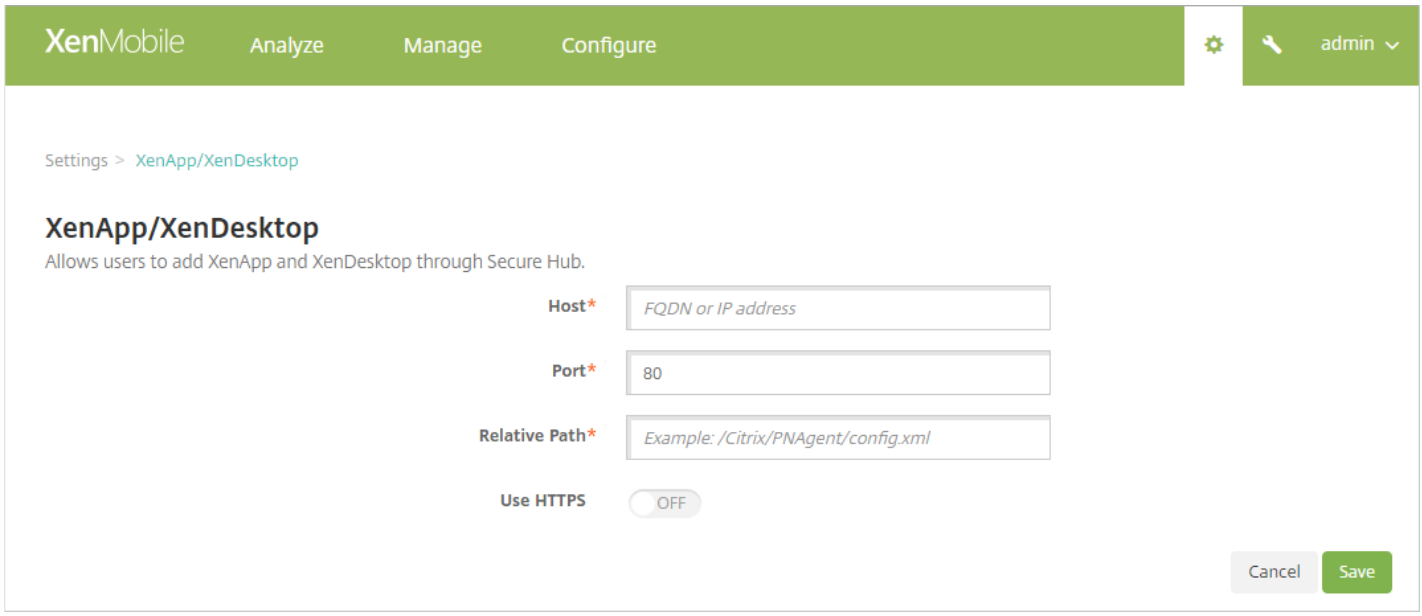
Nov 14, 2016

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.



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 **Save**.

Deploy resources

Dec 16, 2016

Device configuration and management typically involves creating resources (policies and apps) 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; how to change the deployment order of resources and actions in delivery groups; and how 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, and actions. Inclusion in a delivery group is usually based on users' characteristics, such as company, country, department, office address, title, and so on. 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 iOS, Windows Phone, and Windows tablet devices who belong to the delivery group to reconnect to XenMobile, so that you can reevaluate the devices and deploy apps, policies, and actions; users with other platform devices receive the resources immediately if they are already connected or, based on their scheduling policy, the next time 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, 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 and apps) 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, 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 actions, apps, and device policies 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 those and other criteria that you can associate with specific objects or resources to filter them or control their deployment.

Object/Resource	Filter/Control Criteria
Device policy	Device platform Deployment rule (based on device properties) Deployment schedule
App	Device platform Deployment rule (based on device properties) Deployment schedule
Action	Deployment rule (based on device properties) Deployment schedule
Delivery group	User/Groups Deployment rule (based on device properties)

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 of 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 of the delivery groups for a specific user, based upon the filters of user/groups and the deployment rules.
2. Create an ordered list of all resources (policies, actions and apps) within the selected delivery groups that apply 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 those without one. The rationale for this 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 those from delivery group B.

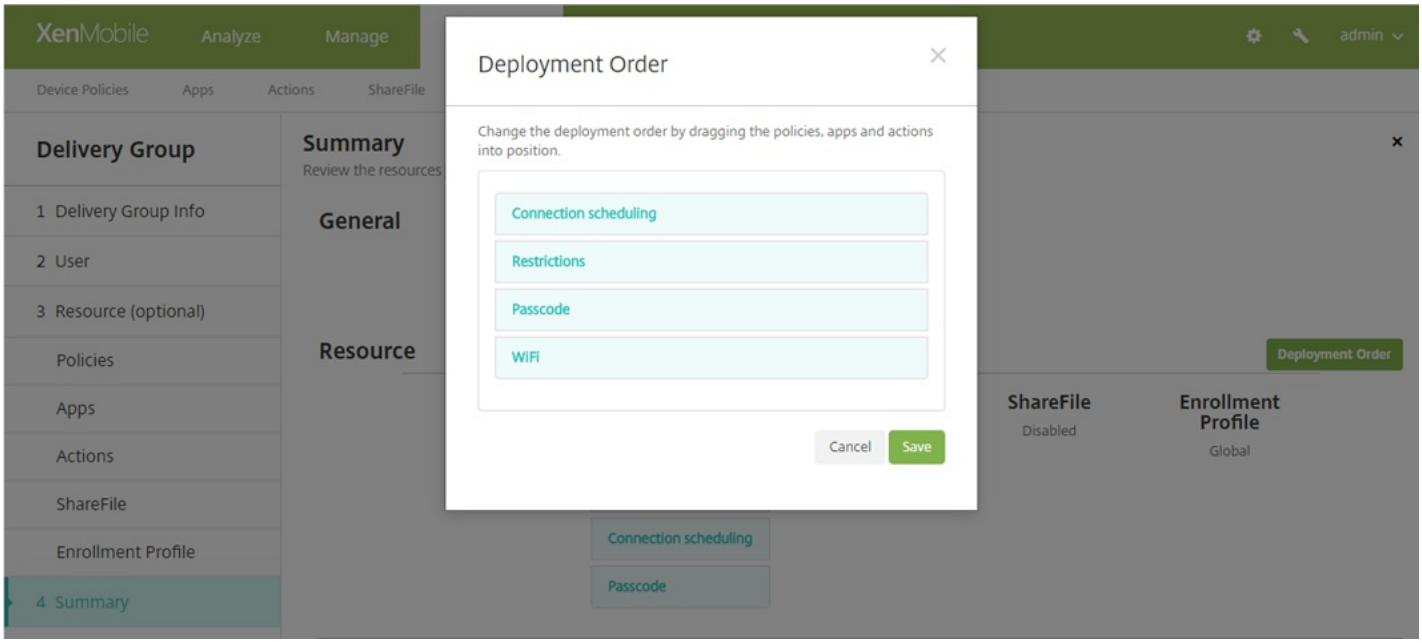
    c. While sorting, if a user-defined deployment order is specified for resources of a delivery group, maintain that order. Otherwise, sort the resources within that delivery group by resource name.

    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 prior to 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.

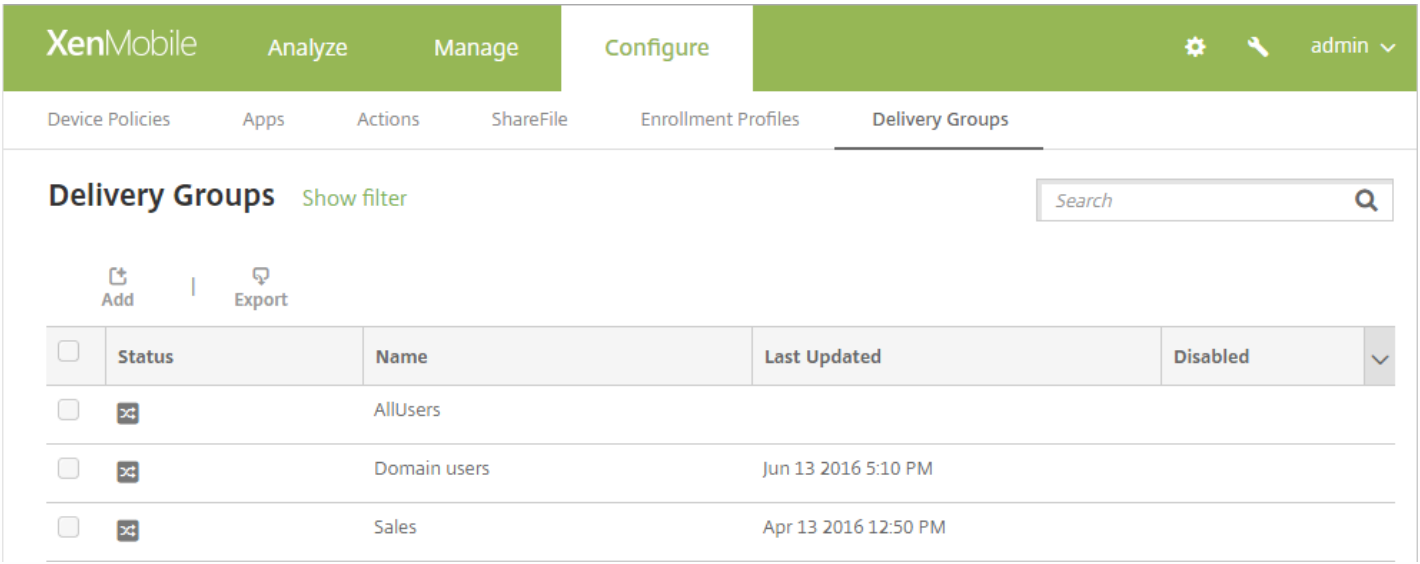


If the calculation algorithm ordered deployment groups only by name, XenMobile would perform the deployment in this order, starting with the delivery group Account Managers 1: **WiFi**, **Passcode**, **Connection scheduling**, and **Restrictions**. XenMobile would ignore **Passcode** and **WiFi**, both duplicates, from the Account Managers 2 delivery group.

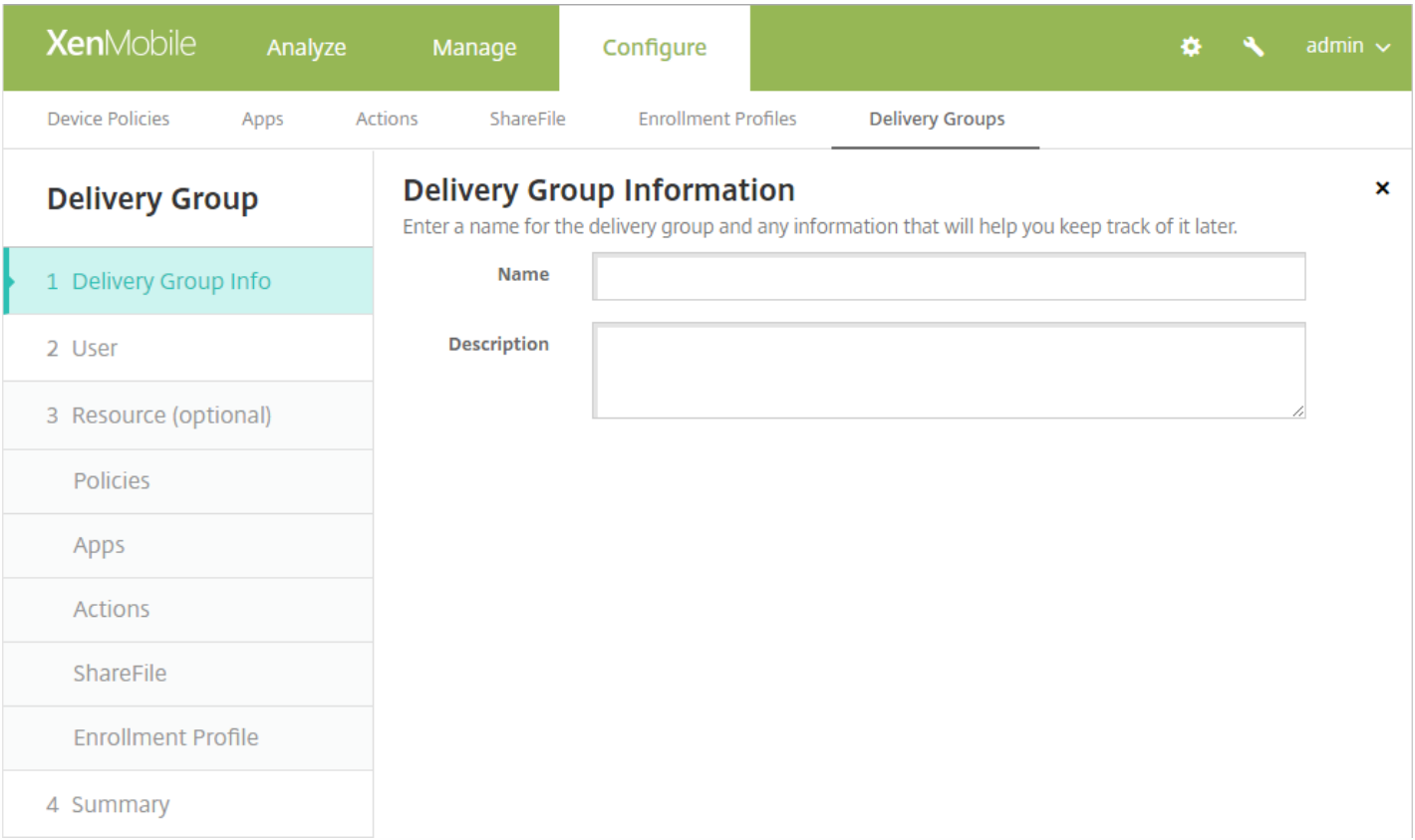
However, because the Account Managers 2 group has an admin-specified deployment order, the calculation algorithm places resources from the Account Managers 2 delivery group higher in the list over those from the Account Managers 1 delivery group. As a result, XenMobile deploys the policies in this order: **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.

To add a delivery group

1. In the XenMobile console, click **Configure > Delivery Groups**. The **Delivery Groups** page appears.



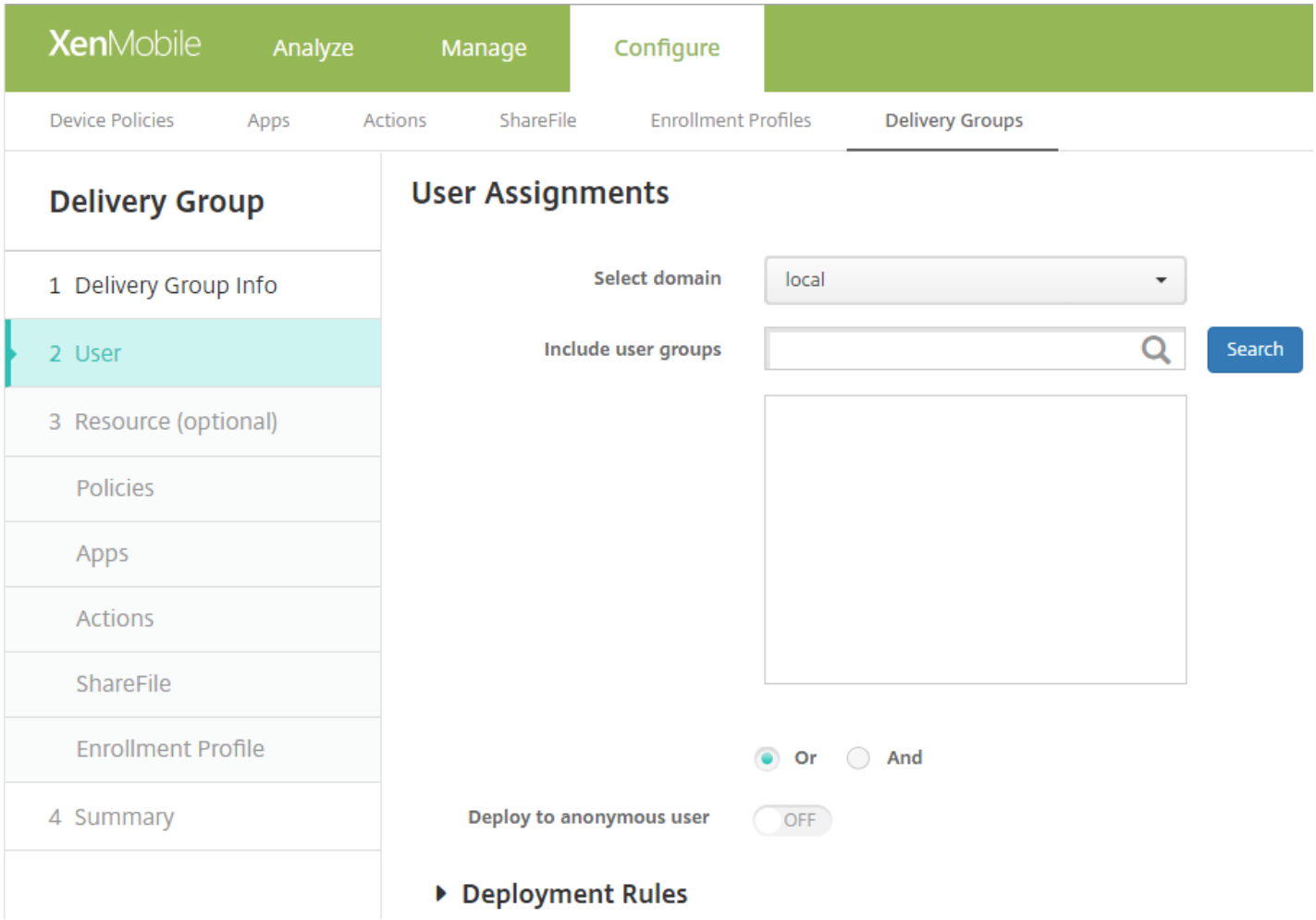
2. From the **Delivery Groups** page, click **Add**. The **Delivery Group Information** page appears.



3. In the **Delivery Group Information** page, enter the following information:

- **Name**: Type a descriptive name for the delivery group.
- **Description**: Type an optional description of the delivery group.

4. Click **Next**. The **User Assignments** page appears.



5. 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.

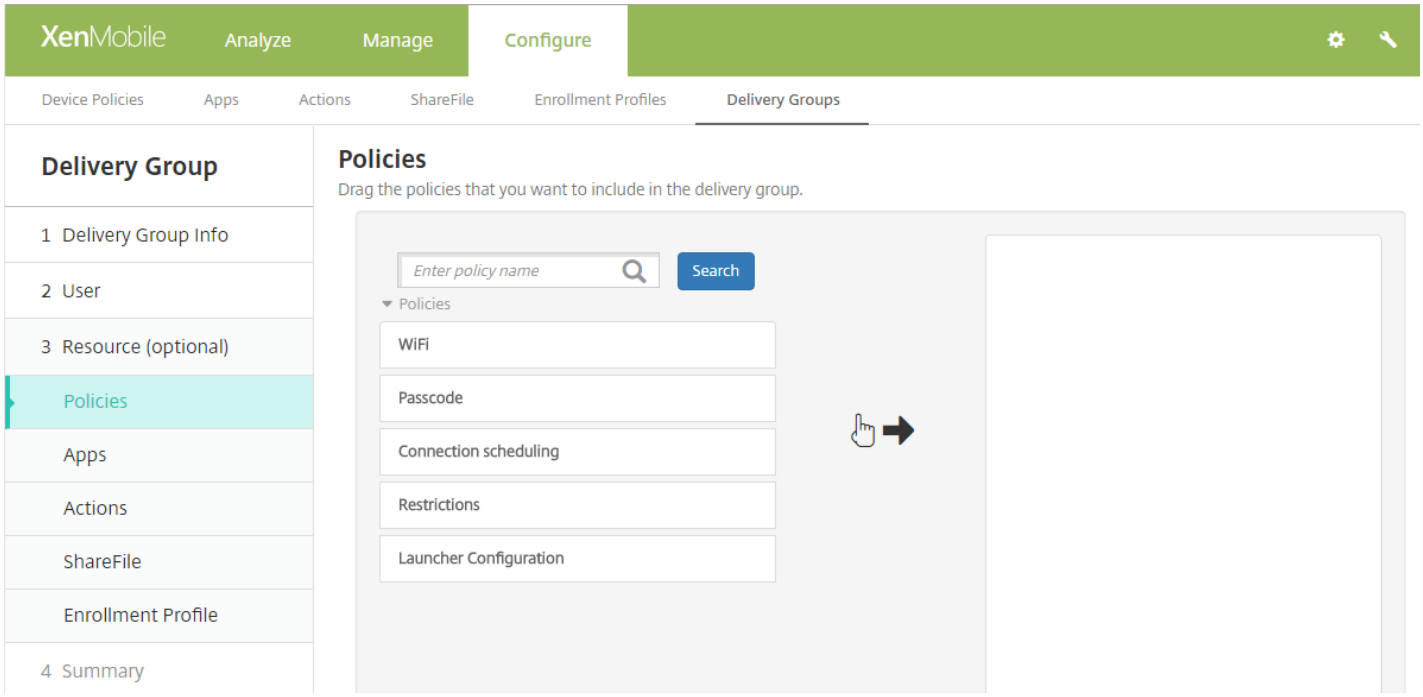
  Note: Unauthenticated users are users whom you were not able to authenticate, but you allowed their devices to connect to XenMobile anyway.

6. Configure the deployment rules

To add optional resources to delivery groups

You can add optional resources to delivery groups to apply specific policies, provide required and optional apps, add automatic actions, and 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



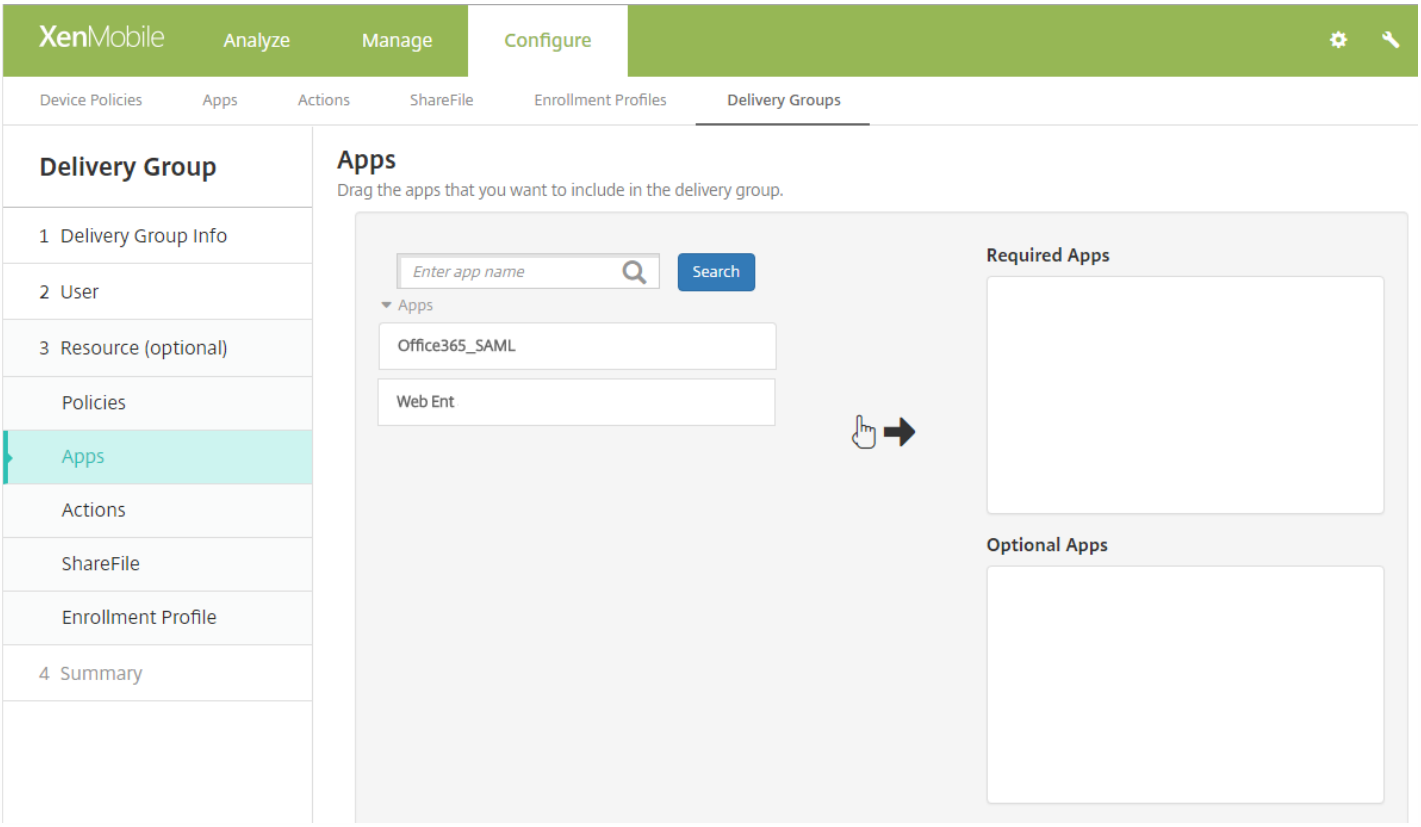
1. For each policy you want to add, do the following:

- 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 right-hand box.

Note: To remove a policy, click the **X** next to the policy name in the right-hand box.

2. Click **Next**. The **Apps** page appears.

Add apps



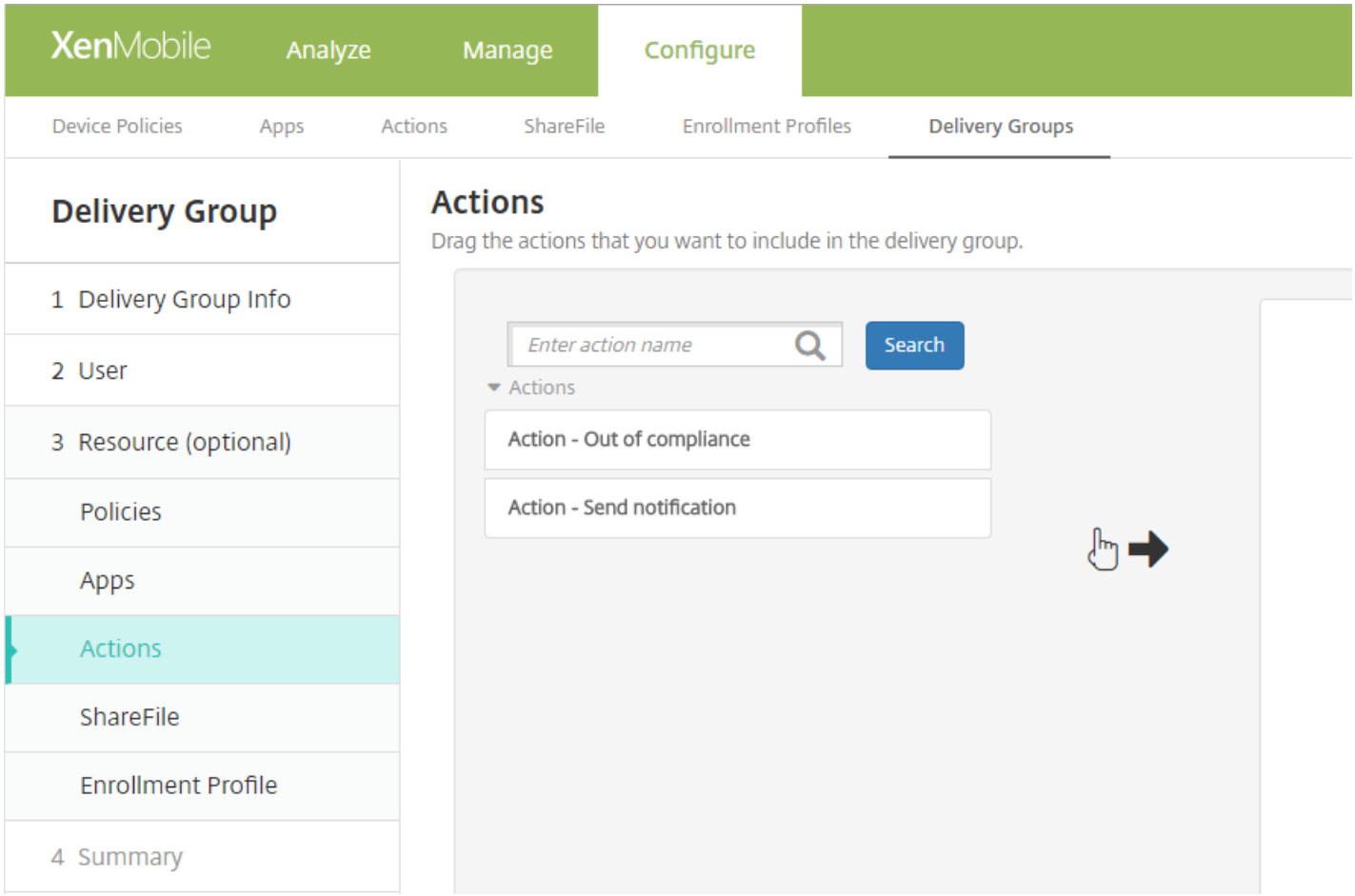
1. For each app you want to add, do the following:

- 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.

Note: To remove an app, click the **X** next to the app name in the right-hand box.

2. Click **Next**. The **Actions** page appears.

Add actions



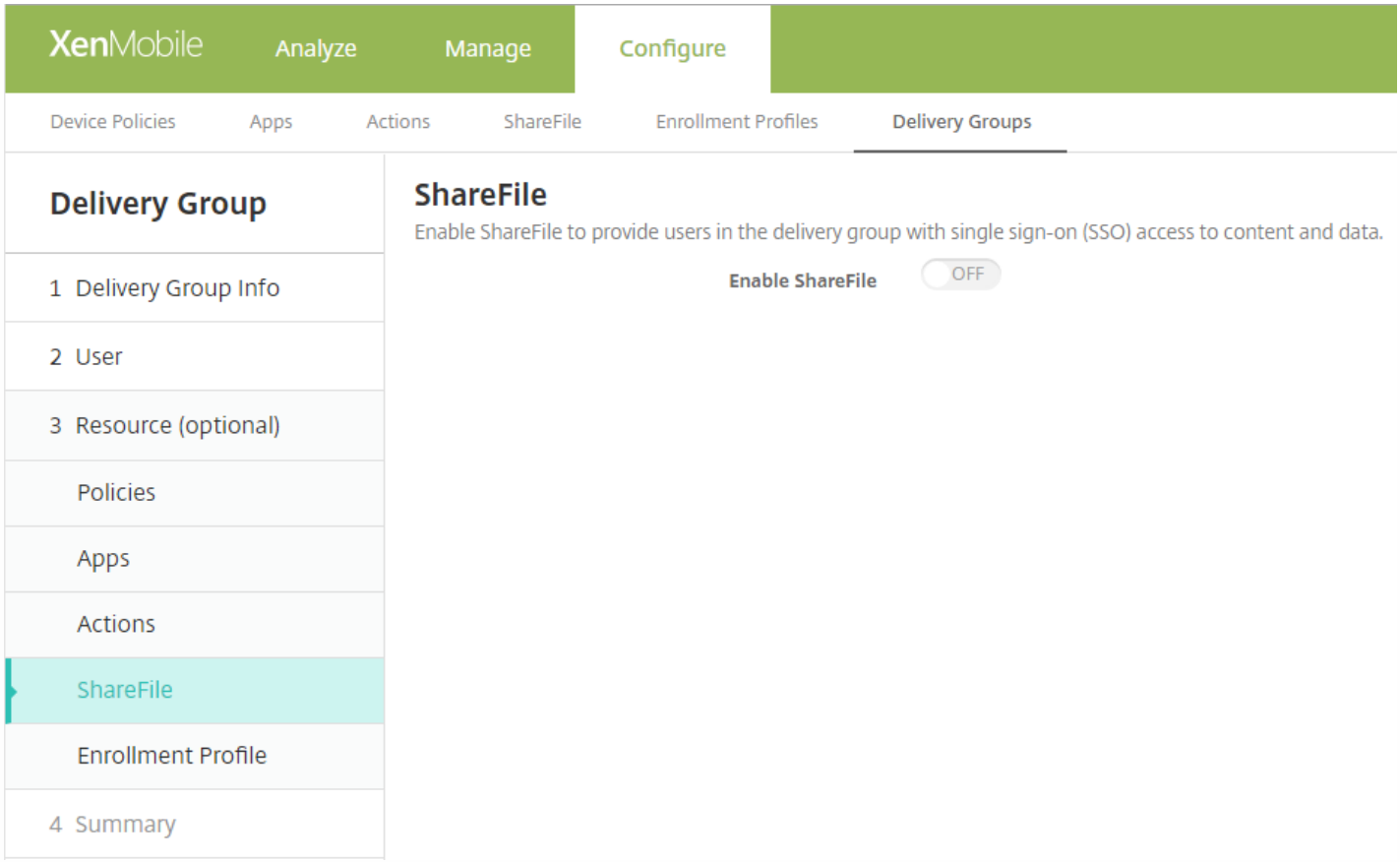
1. For each action you want to add, do the following:

- 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 right-hand box.

Note: To remove an action, click the **X** next to the action name in the right-hand box.

2. Click **Next**. The **ShareFile** page appears.

Enable ShareFile

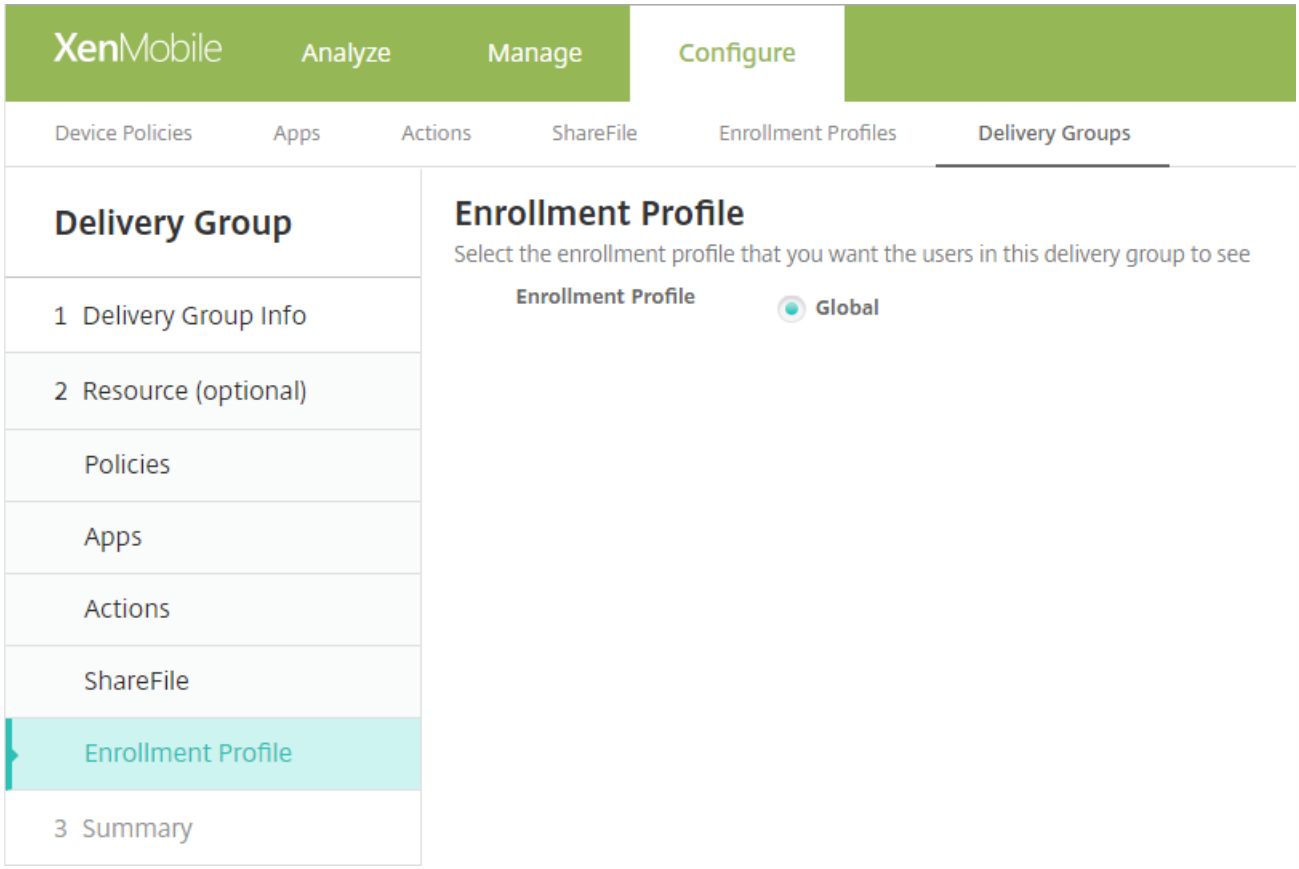


1. Configure this setting:

- **Enable ShareFile**: Click **ON**, to enable ShareFile single sign-on access to content and data.

2. Click **Next**. The **Summary** page appears.

Enrollment Profile

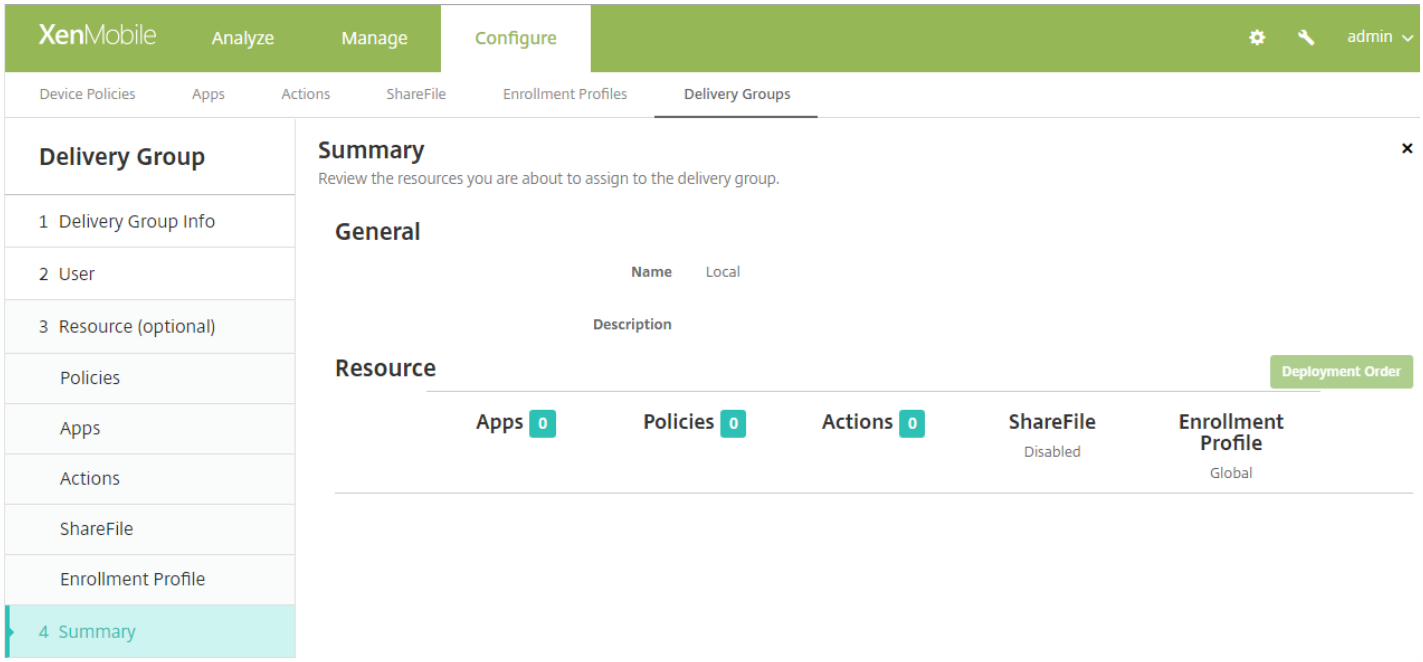


1. Configure this setting:

- **Enrollment Profile**: Select an Enrollment Profile. To create an enrollment profile, see Device enrollment limit.

2. Click **Next**. The **Summary** page appears.

Review configured options and change deployment order



On the **Summary** page, you can review the options you have configured for the delivery group and change the deployment order of resources. The Summary page shows your resources by category; it doesn't reflect the deployment order.

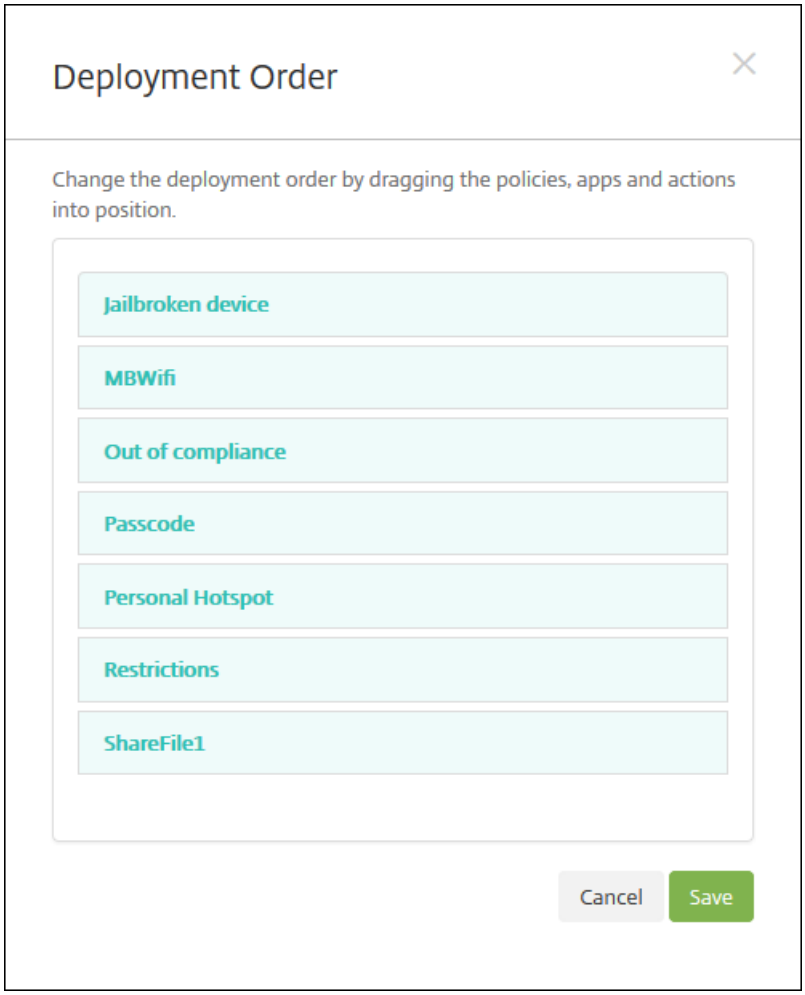
1. Click **Back** to return to previous pages to make any necessary adjustments to the configuration.

2. Click **Deployment Order** to view the deployment order or to reorder the deployment order.

3. Click **Save** to save the delivery group.

To change the deployment order

1. Click the **Deployment Order** button. The **Deployment Order** dialog box appears.



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.

To edit a delivery group

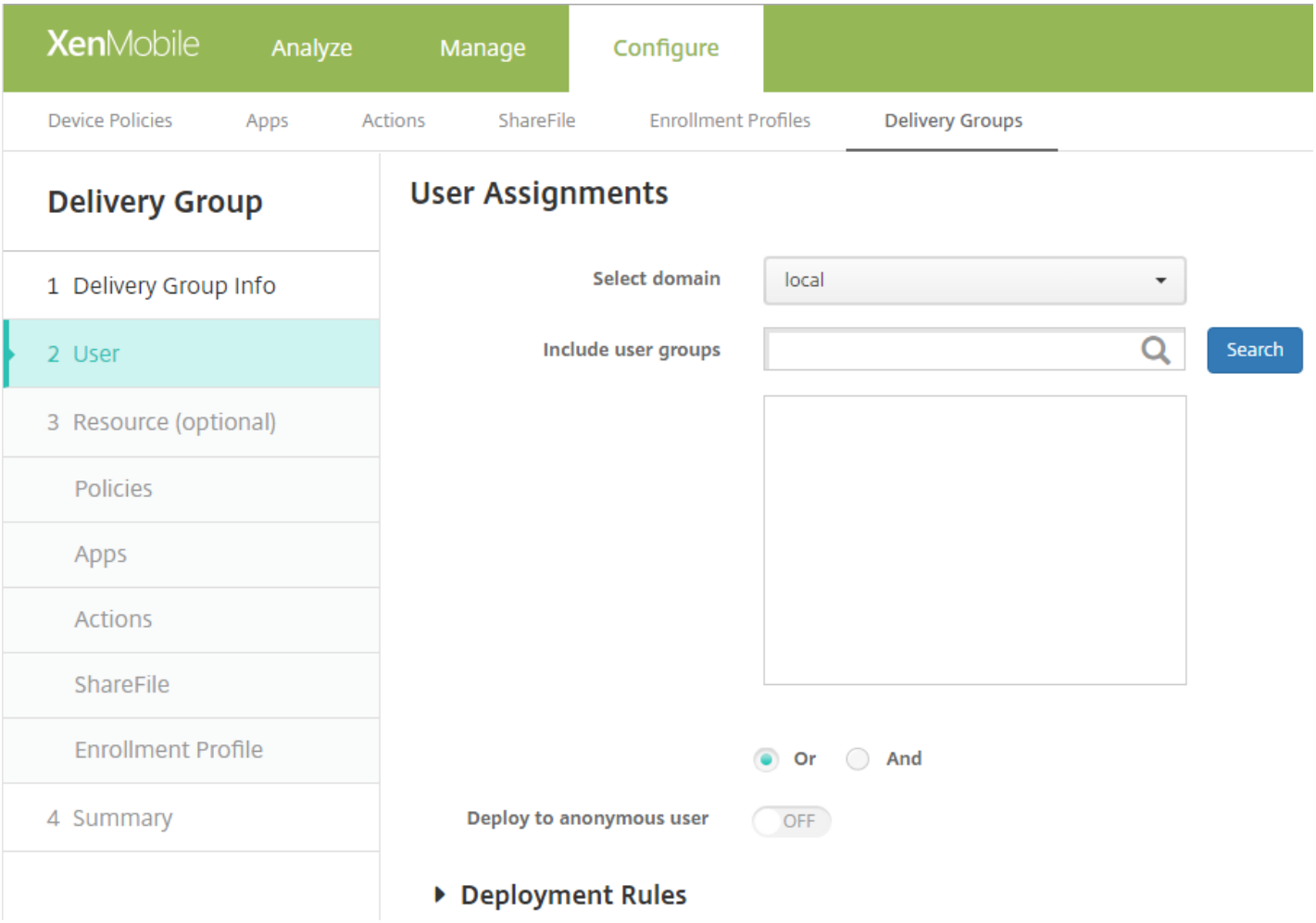
1. On the **Delivery Groups** page, choose the delivery group you want to edit by selecting the check box next to its name or by clicking in the line containing its name and then click **Edit**. The **Delivery Group Information** edit page appears.

> **Note**
>
> Depending on how you selected the delivery group, the **Edit** command appears above or to the right of the delivery group.

2. Add or change the **Description**.

Note: You cannot change the name of an existing delivery group.

3. Click **Next**. The **User Assignments** page appears.



4. In the **Select User Groups** page, enter or change the following information:

- **Select domain**: In 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.

    Note: To remove user groups, click **Search**, and then in the list of user groups, clear the check box next to the group or

groups you want to remove. You can type a full or partial group name in the search box and then click **Search** to limit the number of user groups displayed in the list.

- **Or/And**: Select whether users may be in any group (Or) or whether they must be in all groups (And) for deployment.
- **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 whose devices you allowed to connect to XenMobile.

5. Expand **Deployment Rules** and then configure the settings as you did in Step 5 earlier in this procedure.

6. Click **Next**. The **Delivery Group Resources** page appears. Add or delete policies, apps, or actions here. To skip this step, under **Delivery Group**, click **Summary** to see a summary of the delivery group configuration.

7. When you are done modifying a resource, click **Next**, or under **Delivery Group**, click **Summary**.

8. On the **Summary** page, you can review the options you have configured for the delivery group and change the deployment order of resources.

9. Click **Back** to return to previous pages to make any necessary adjustments to the configuration.

10. Click **Deployment Order** to reorder the resource deployment order; for more information on changing deployment order, see To change deployment order.

11. Click **Save** to save the delivery group.

To enable and disable the AllUsers delivery group

> **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 currently disabled. **Disabled** disappears from under the **Disabled** heading in the delivery group table.

To deploy to delivery groups

Deploying to a delivery group means sending a push notification to all users with iOS, Windows Phone, and Windows tablet devices who belong to the delivery group to reconnect to XenMobile. That way, you can reevaluate the devices and deploy apps, policies, and actions. Users with other platform devices receive the resources immediately if they are already connected; or, based on their scheduling policy, the next time they connect.

Note: For updated apps to appear in the Updated Available list in the XenMobile Store on users' Android devices, you must

first deploy an App Inventory policy to the users' 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.

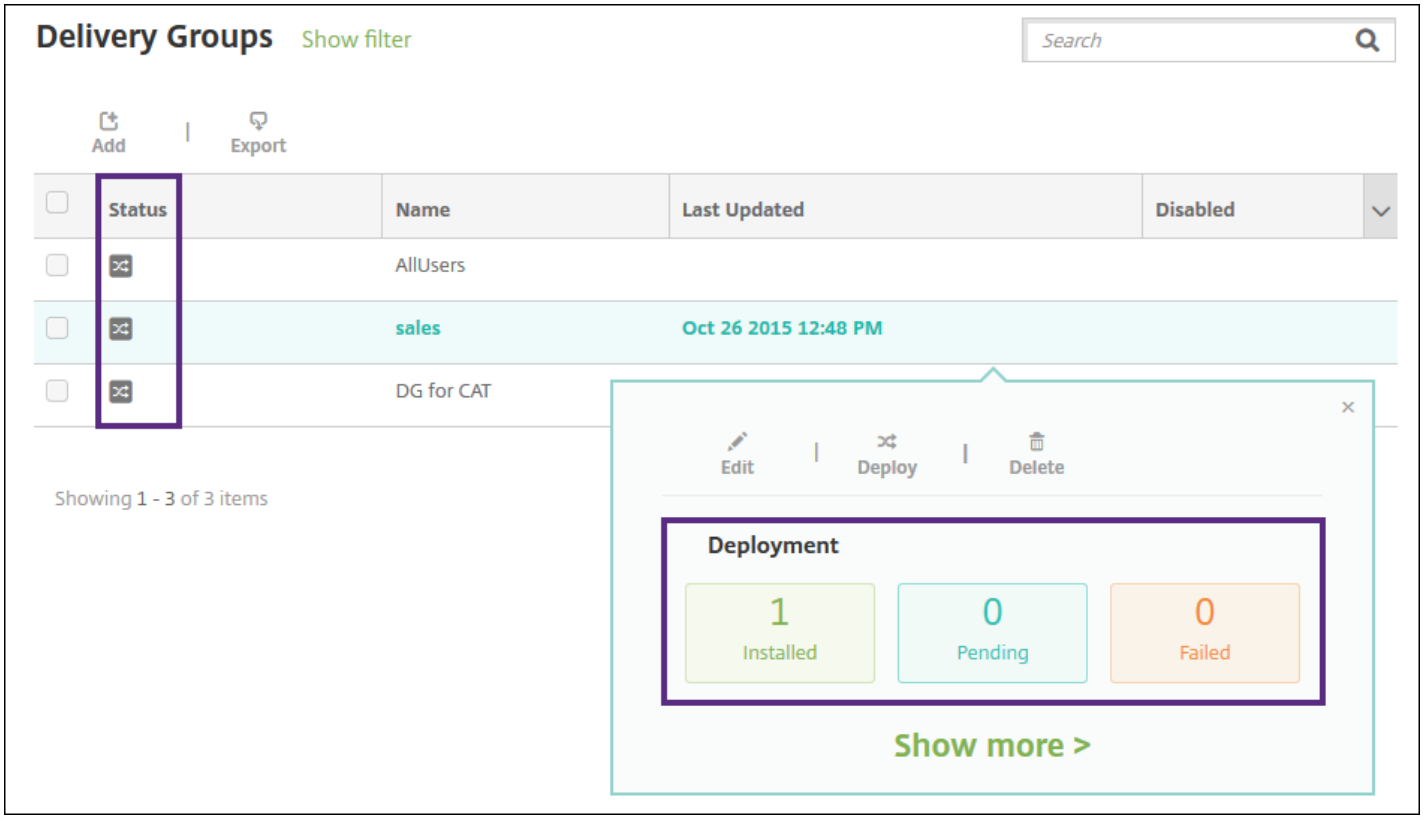
2. Click **Deploy**.

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.



To delete delivery groups

> **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.

To export the Delivery Groups table

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. How you do this depends on the browser you are using. You can also cancel the operation.

Macros

Oct 05, 2016

XenMobile provides powerful macros as a way to populate user or device property data within the text field of a profile, policy, notification, or enrollment template (for some Actions), among other uses. With macros, you can configure a single policy and deploy it to a large user base and have user-specific values appear for each targeted user. For example, you can prepopulate the mailbox value for a user in an Exchange profile across thousands of users.

This feature is currently only available in the context of configurations and templates for iOS and Android devices.

Defining user macros

The following user macros are always available:

- loginname (username plus domainname)
- username (loginname minus the domain, if any)
- domainname (domain name, or the default domain)

The following administrator-defined properties may be available:

- c
- cn
- company
- companyname
- department
- description
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename
- postalcode
- postofficebox

- telephonenumber
- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname (overrides property described previously)

Additionally, if the user is authenticated by using an authentication server, such as LDAP, all the properties associated with the user in that store are available.

Macro syntax

A macro can take the following form:

- ${type.PROPERTYNAME}
- ${type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]}

As a general rule, all syntax following the dollar sign ($) must be enclosed 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.")}.

For example, ${user.username} populates the user name value in the text field of a policy. This is useful for configuring Exchange ActiveSync profiles and other profiles used by multiple users.

For custom macros (properties that you define), the prefix is ${custom}. You can omit the prefix.

Note: Property names are case-sensitive.

Automated actions

Feb 01, 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.

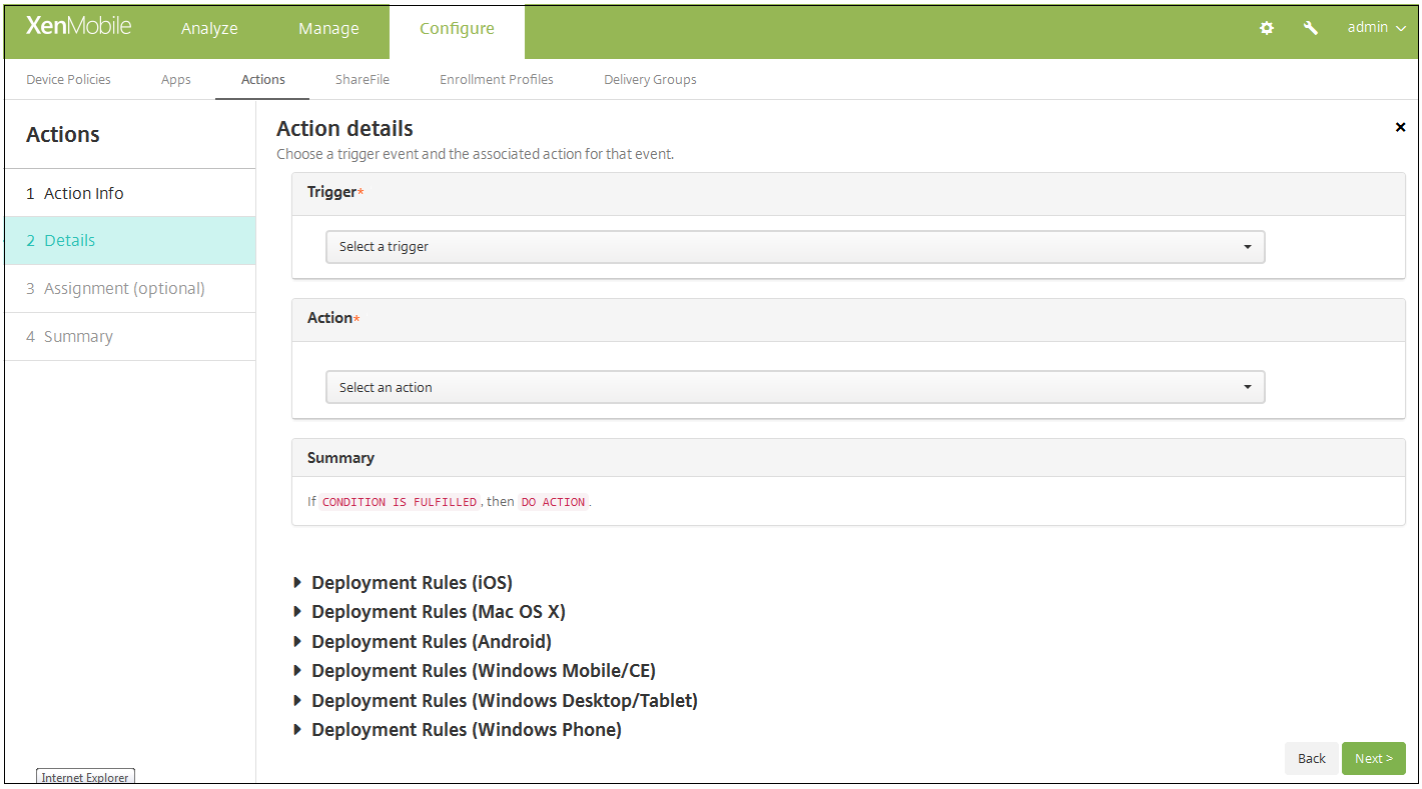
4. On the **Action Information** page, enter or modify the following information:

- **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.



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.
  - **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. With the exception of **Send notification**, you choose a time frame in which users can resolve the issue that caused the trigger. If the issue is not resolved within that time frame, the selected action is taken. The available actions are as follows:

- **Selectively wipe the device**: Erase all corporate data and apps from a device, leaving personal data and apps in place.
- **Completely wipe the device**: Erase all data and apps from a device, including memory cards, if the device has one.
- **Revoke the 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,

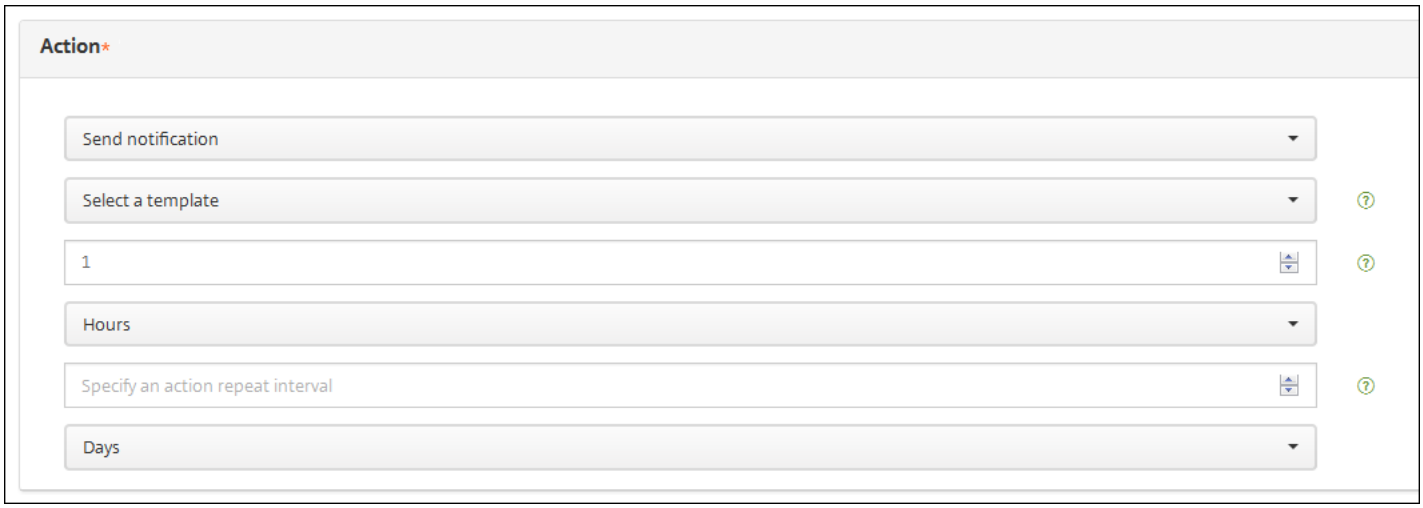
users will still be able to log in, but they will be unable to access apps. For more information, see "App lock and App wipe actions for MAM-only mode," later in this article.

- **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. For more information, see "App lock and App wipe actions for MAM-only mode," later in this article.
- **Mark the device as out of compliance**: Set the device as out of compliance.
- **Send notification**: Send a message to the user.

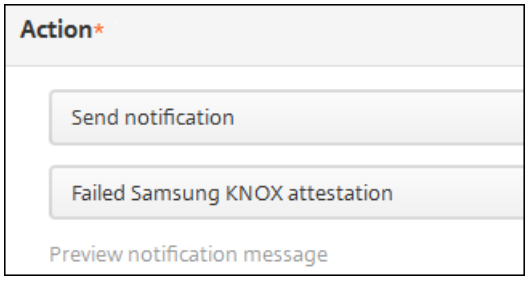
If you pick **Send notification**, the remainder of this procedure explains how to send a notification action.

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.



Note: After you select the template, you can preview the notification by clicking **Preview notification message**.



10. In the following fields, set the delay in days, hours, or minutes before taking action and the interval at which the action repeats until the user addresses the triggering issue.

11. In **Summary**, verify that you created the automated action as you intended.

12. After you configure the action details, you can configure deployment rules for each platform individually. To do so, complete step 13 for each platform you choose.

13. Configure deployment rules

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.

App lock and App wipe actions for MAM-only mode

You can wipe or lock apps on a device in response to all four categories of triggers listed in the 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:

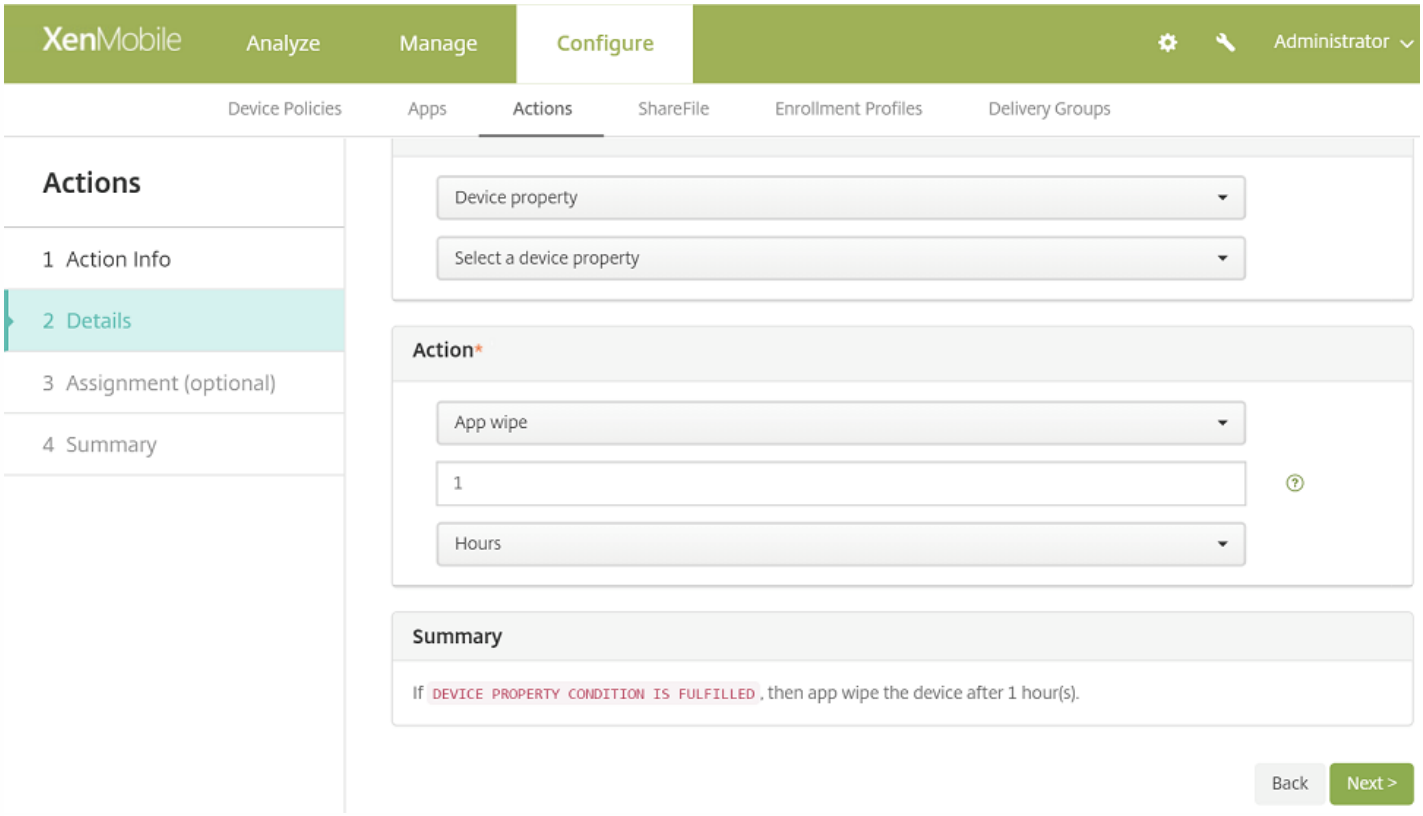
When the trigger type is **Event** and the value is not **Active Directory disabled user**, the **App wipe** and **App lock** actions will not appear.

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.



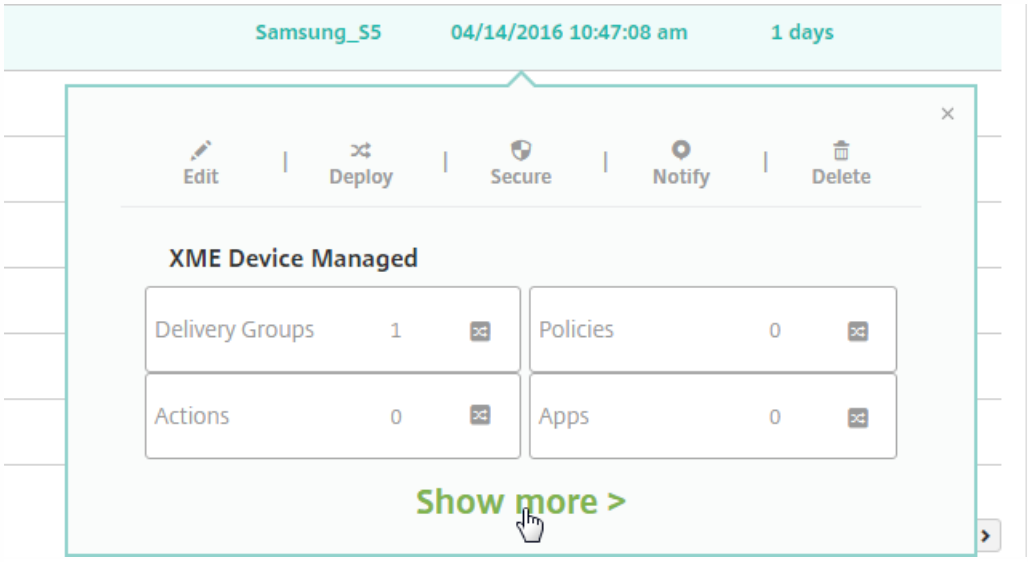
6. Configure deployment rules and then click **Next**.

7. Configure delivery group assignments and a deployment schedule and then click **Next**.

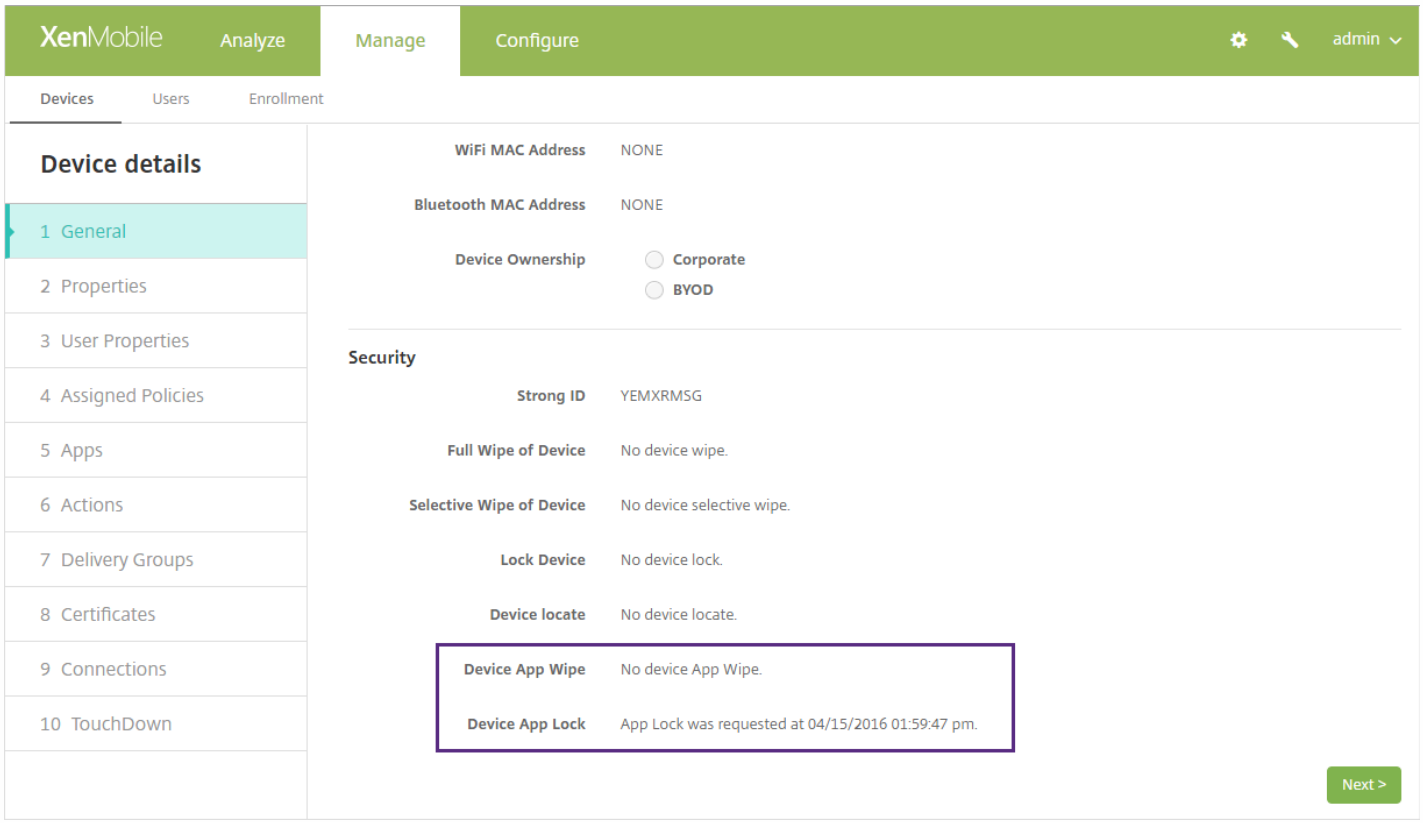
8. Click **Save**.

To check app lock or app wipe status

1. Go to **Manage > Devices**, click a device and then click **Show more**.



2. Scroll to **Device App Wipe** and **Device App Lock**.



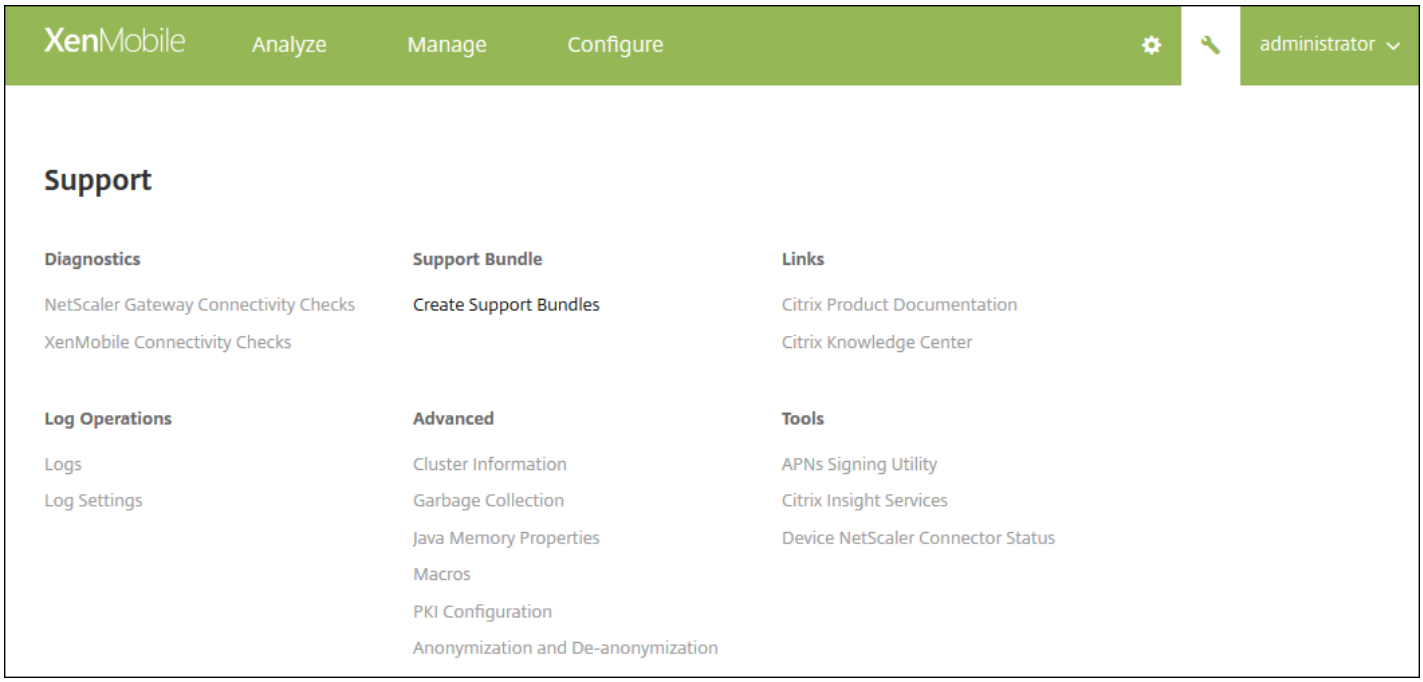
Monitor and support

Feb 23, 2017

Use the XenMobile Support page to access a number of support-related information and tools. You can also carry out actions from the command-line interface. For details, see Command-line interface options.

In the XenMobile console, click the wrench icon in the upper-right corner of the console.

The Support page appears.



Use the XenMobile **Support** page to:

- Access diagnostics.
- Create support bundles.
- Access links to Citrix Product Documentation and the Knowledge Center.
- Access log operations.
- Select from a set of advanced information and configuration options.
- Access a set of tools and utilities.

Reports

Feb 09, 2017

XenMobile provides the following pre-defined reports that let you analyze your app and device deployments:

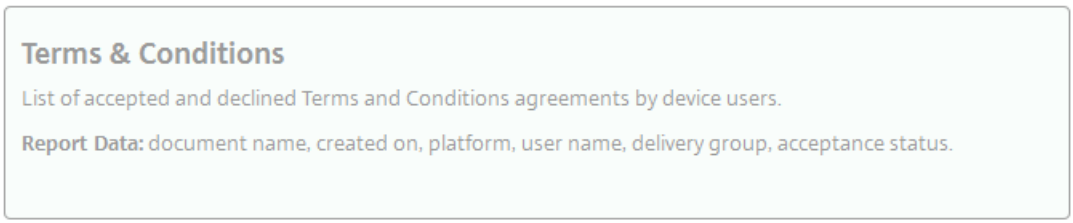
- **Apps by Devices & User** – Lists managed apps that users have on their devices. This report does not include the personal apps installed on a device.
- **Terms & Conditions** – Lists users who have accepted and declined Terms and Conditions agreements.
- **Top 25 Apps** – Lists up to 25 apps that most users have on their devices.
- **Jailbroken/Rooted Devices** – Lists jailbroken iOS devices and rooted Android devices.
- **Top 10 Apps** – Failed Deployment - Lists up to 10 apps that have failed to deploy.
- **Inactive Devices** – Lists devices that have been inactive for a specified period of time.
- **Apps by Type & Category** – Lists apps by version, type, and category.
- **Device Enrollment** – Lists all enrolled devices.
- **Apps by Platform** – Lists apps and app versions by device platform and version.
- **Blacklisted Apps by Device & User** - Lists blacklisted apps that users have on their devices.
- **Devices & Apps** – Lists devices that are running managed apps.

The reports are in .csv format, which you can open with programs like Microsoft Excel.

Follow these steps to create a report:

1. In the XenMobile console, click **Analyze**, and then click **Reporting**. The **Reporting** page appears.

Each report type includes a description of the information the report gathers, as well as the specific report data, as shown in the following example:



2. Click the report you want to create. Depending on the browser you are using, the file is automatically downloaded or you are asked to save the file.

3. Repeat step 2 for each report you want to create.

The following figure shows part of a Top 25 Apps report as it appears in Microsoft Excel:

	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORIES	AVAILABLE_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	GoToMeeting	6.6.4.1127	Default	10/17/2016 14:21		7	7	0	0	Public App Store
3	Secure Web - Inception	10.4.0-11	Default	10/17/2016 14:37	citrix.com	7	6	0	1	MDX
4	Secure Mail	10.4.1-221	Default	10/17/2016 16:06	citrix.com	6	5	0	1	MDX
5	Twitter	6.64	appstore	10/17/2016 17:04		3	3	0	0	Public App Store
6	Salesforce1	11.0.3	Default	12/14/2016 17:52		2	2	0	0	Public App Store

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 with your XenMobile deployment. If you do decide to pursue this method of reporting, ensure that SQL queries are run using a read-only account.

Mobile Service Provider

Oct 17, 2016

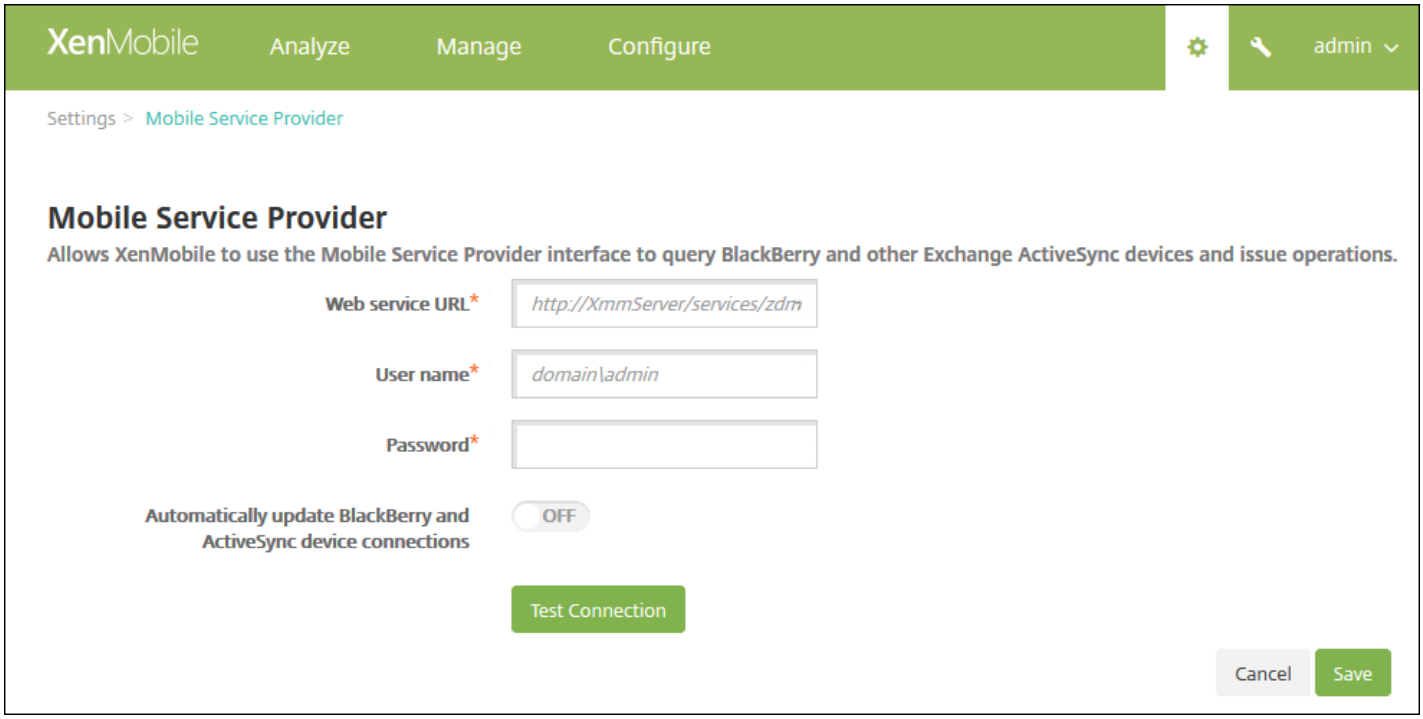
You can enable XenMobile to use the Mobile Service Provider interface to query BlackBerry and Exchange ActiveSync devices and issue operations.

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.



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

Jan 18, 2017

You can configure XenMobile 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:

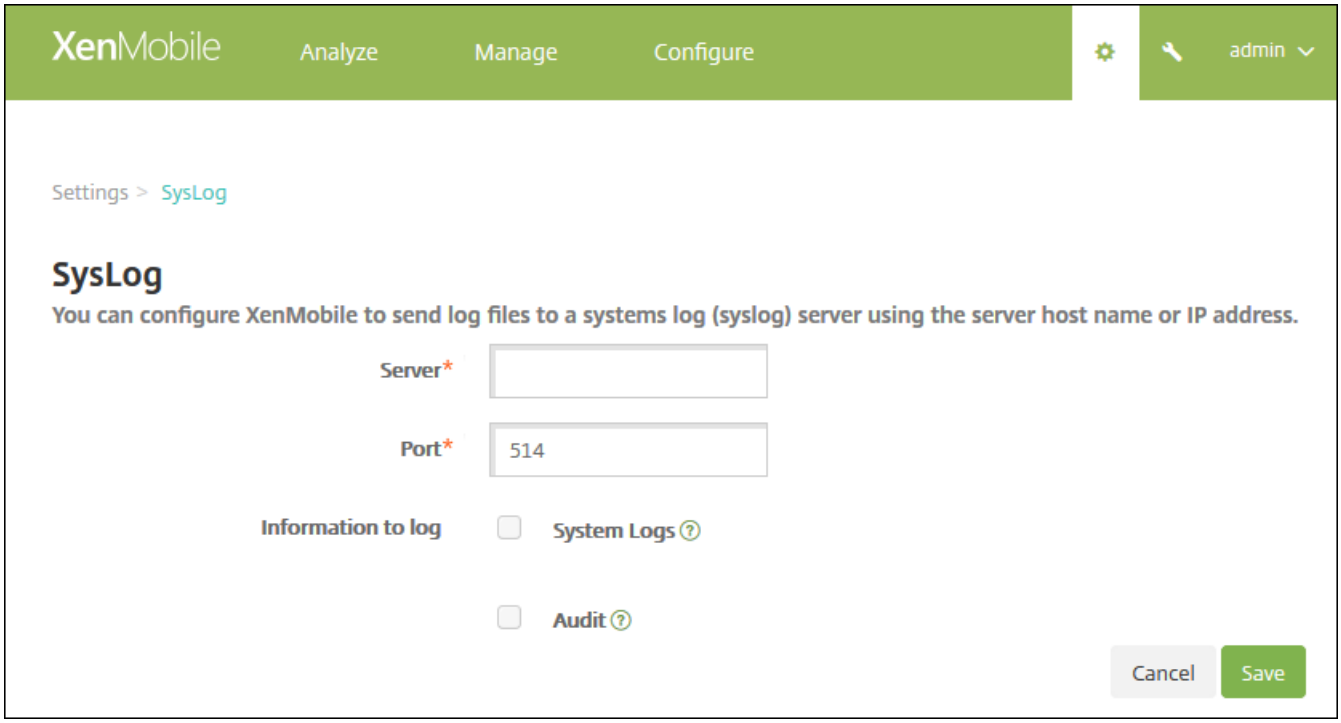
- The IP address of the appliance that generated the log message
- A time stamp
- The message type
- The log level associated with an event (Critical, Error, Notice, Warning, Informational, Debug, Alert, or Emergency)
- The message information

You can use this information to analyze the source of the alert and take corrective action if required.

> ## 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** in order 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.



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**.

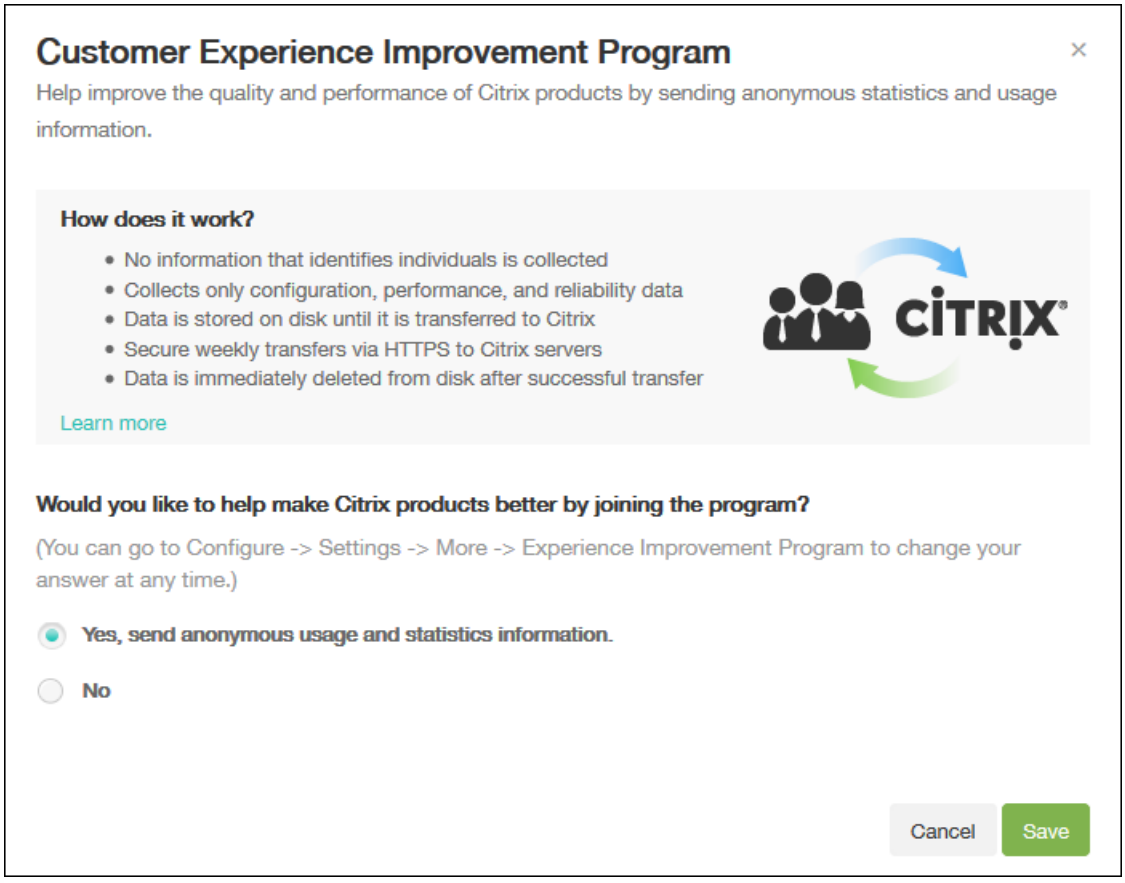
Customer Experience Improvement Program

Nov 08, 2016

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).

Choosing to participate in the CEIP

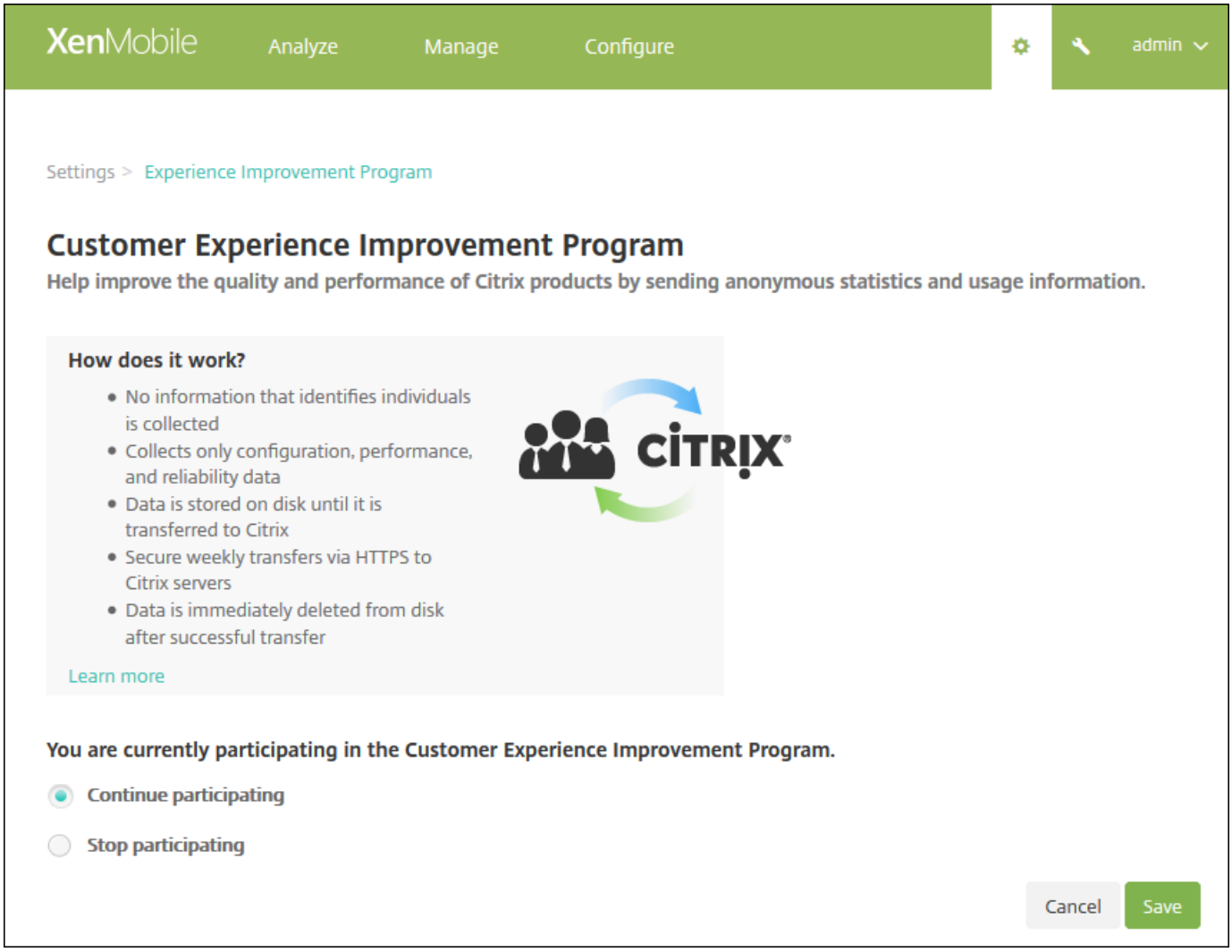
The first time you install XenMobile or when you do an update, you see the following dialog box that prompts you to participate.



Changing your CEIP participation setting

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.



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**.

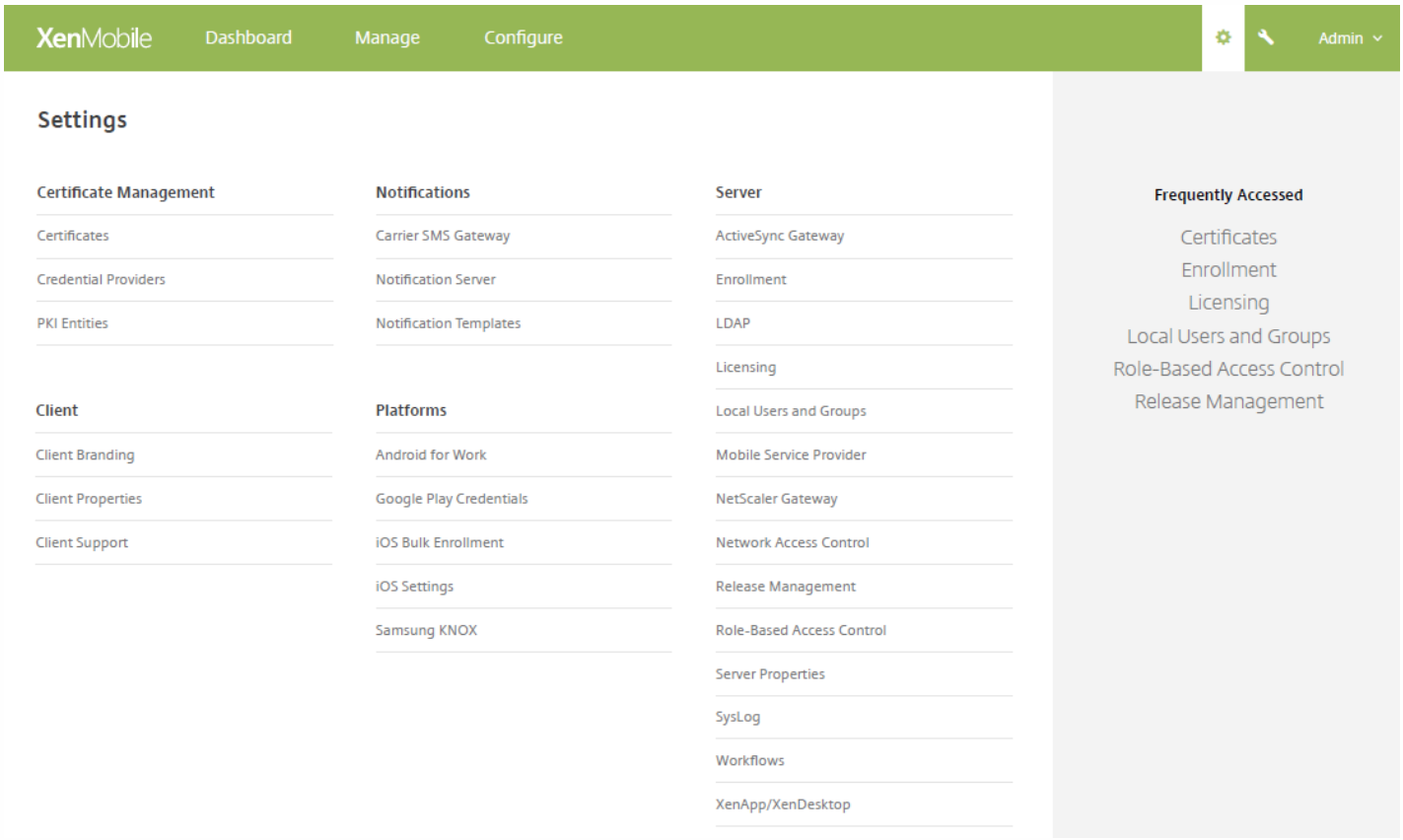
Support options and Remote Support

Feb 06, 2017

You can give users different ways to contact support staff by providing email addresses and phone numbers. When users request assistance from their devices, they see the options that you have set.

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 to configure a phone number and email address and to indicate how the device sends logs to the help desk.

- **Support phone (IT help desk)**: Type the phone number for your IT help desk.
- **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 if there is 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**.

Remote Support

Remote support enables your help desk representatives to take remote control of managed Windows and Android mobile devices.

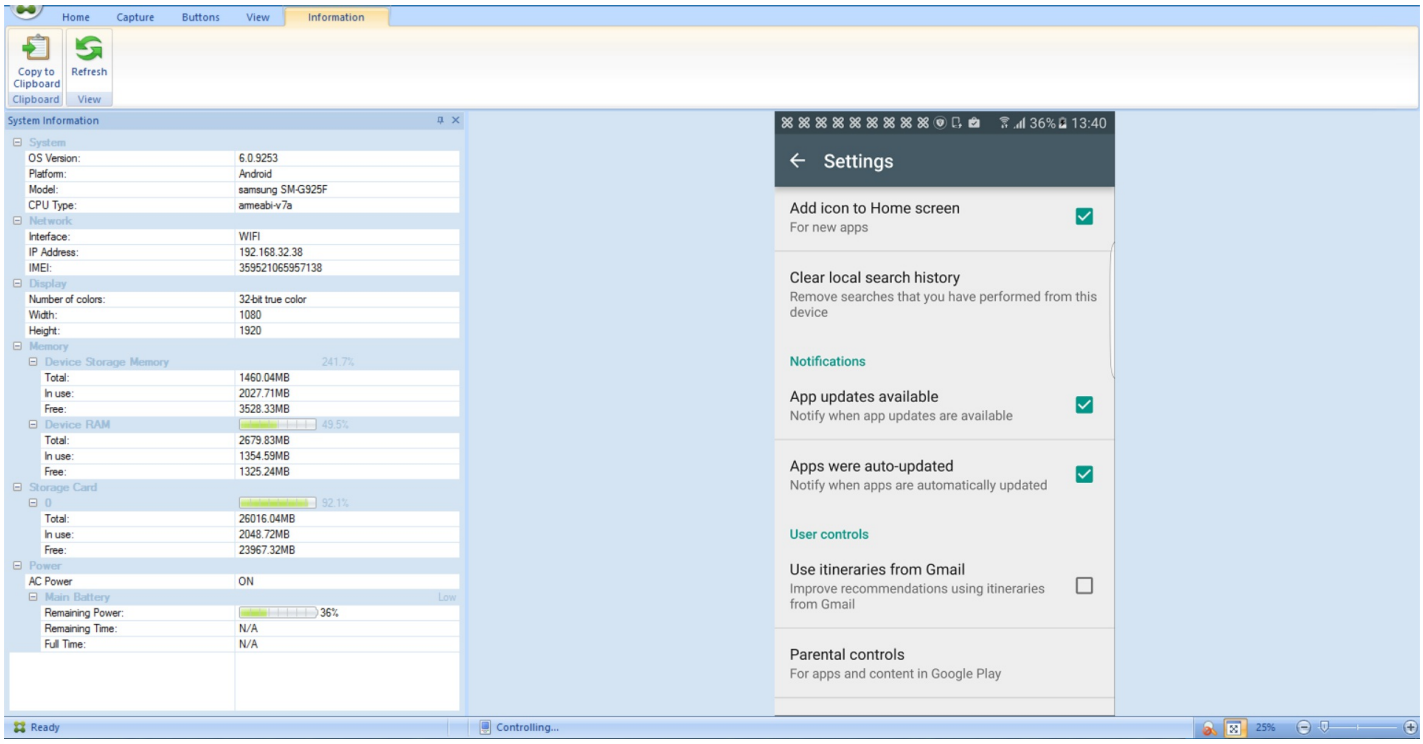
Remote Support is available on all Windows mobile devices and on Android Samsung SAFE devices and non-Samsung devices.

Screen cast is supported on Samsung KNOX devices only.

Remote control of iOS devices is not supported.

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.



By using Remote Support, you can do the following:

- Remotely sign on to a user's mobile device and control the user's 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) and 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

where *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:

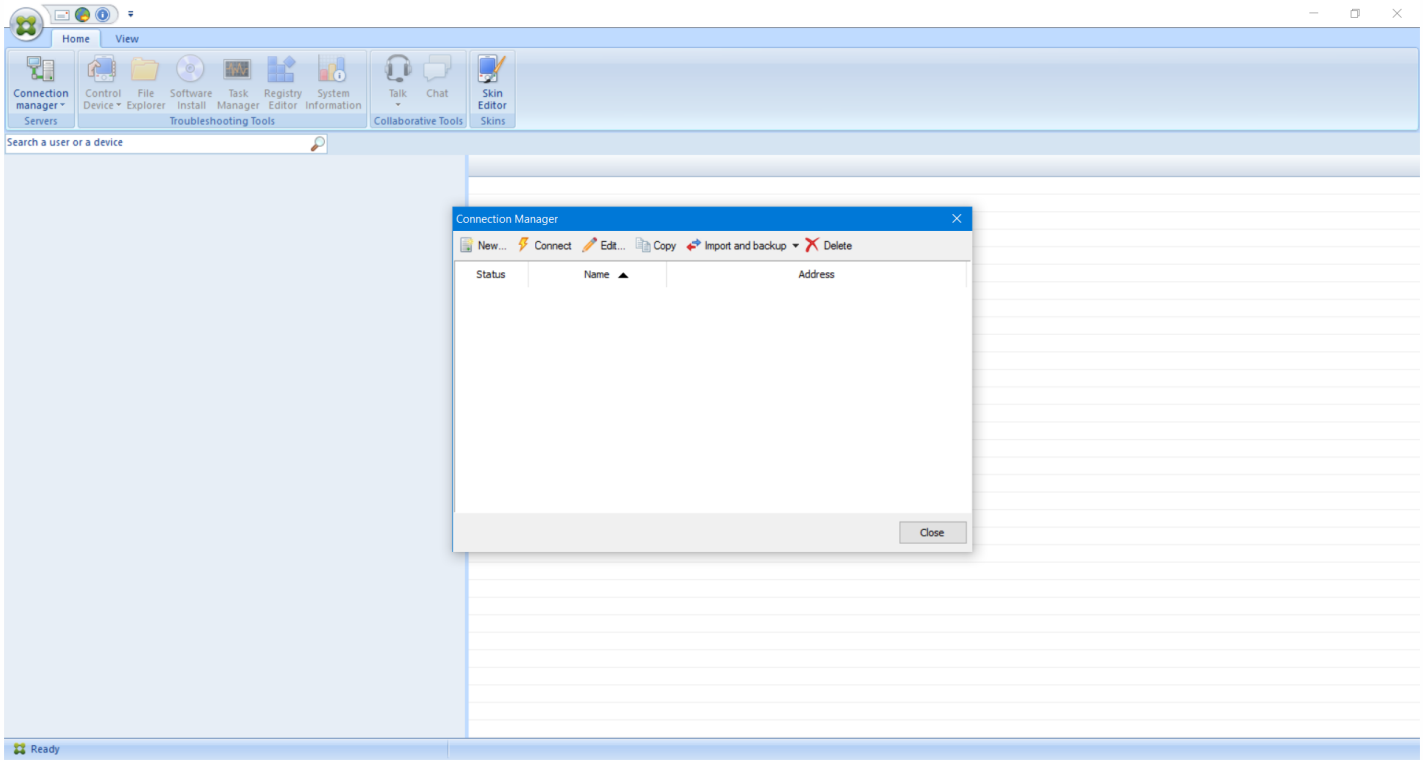
- /S: to install the Remote Support software silently with the default parameters.
- /D=dir: to specify a custom installation directory.

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.

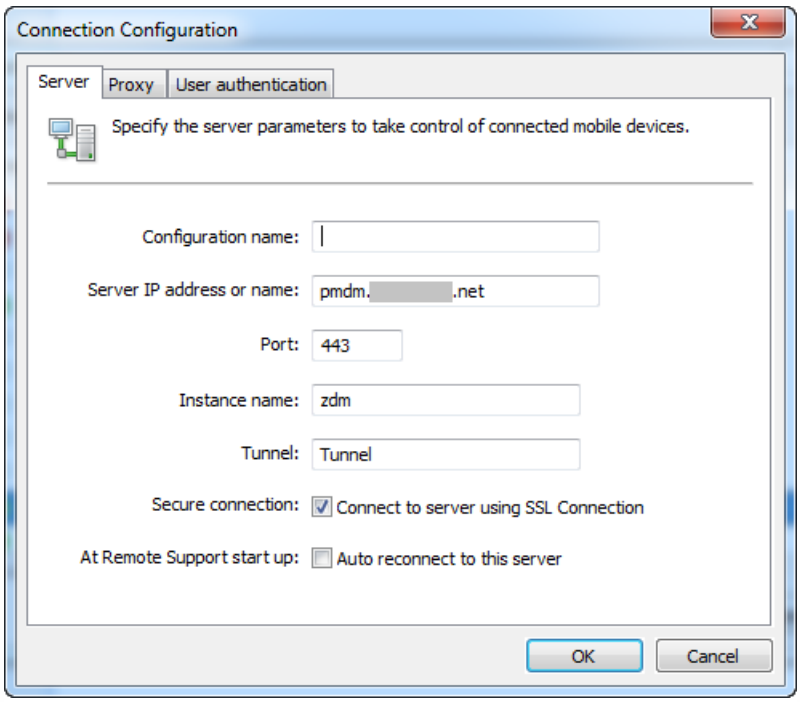
c. In **Port**, type a TCP port number, as defined in the XenMobile server configuration.

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.



4. On the **Proxy** tab, select **Use a http proxy server** and then type the following information:

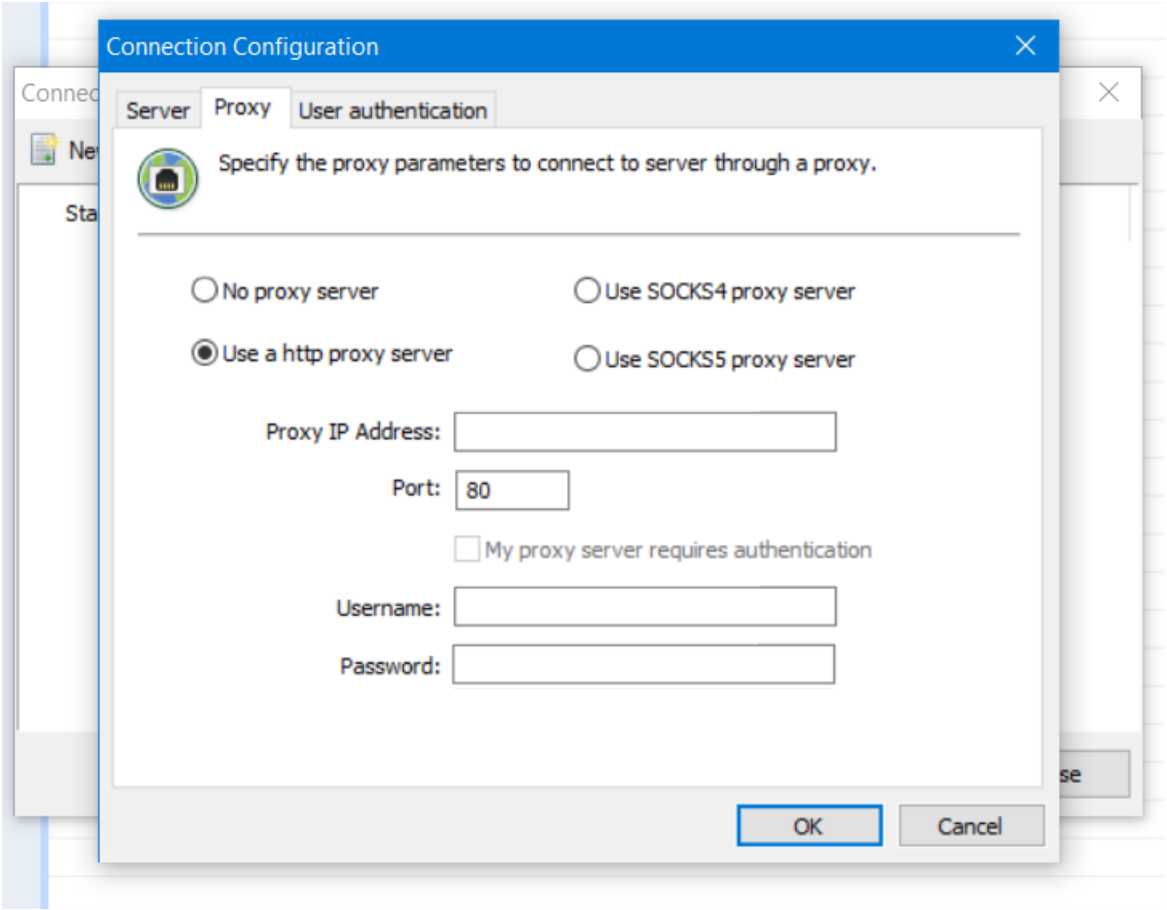
a. In **Proxy IP Address**, type the IP address of the proxy server.

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.



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, 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 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.

  With Premium support, you need to configure the Samsung MDM License Key device policy in the XenMobile console. When you configure this policy, only select the **Samsung KNOX** platform. You don't need to configure the Samsung SAFE platform for this scenario, because the ELM key is automatically deployed on Samsung devices when they enroll in XenMobile. 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.

Client branding

Nov 08, 2016

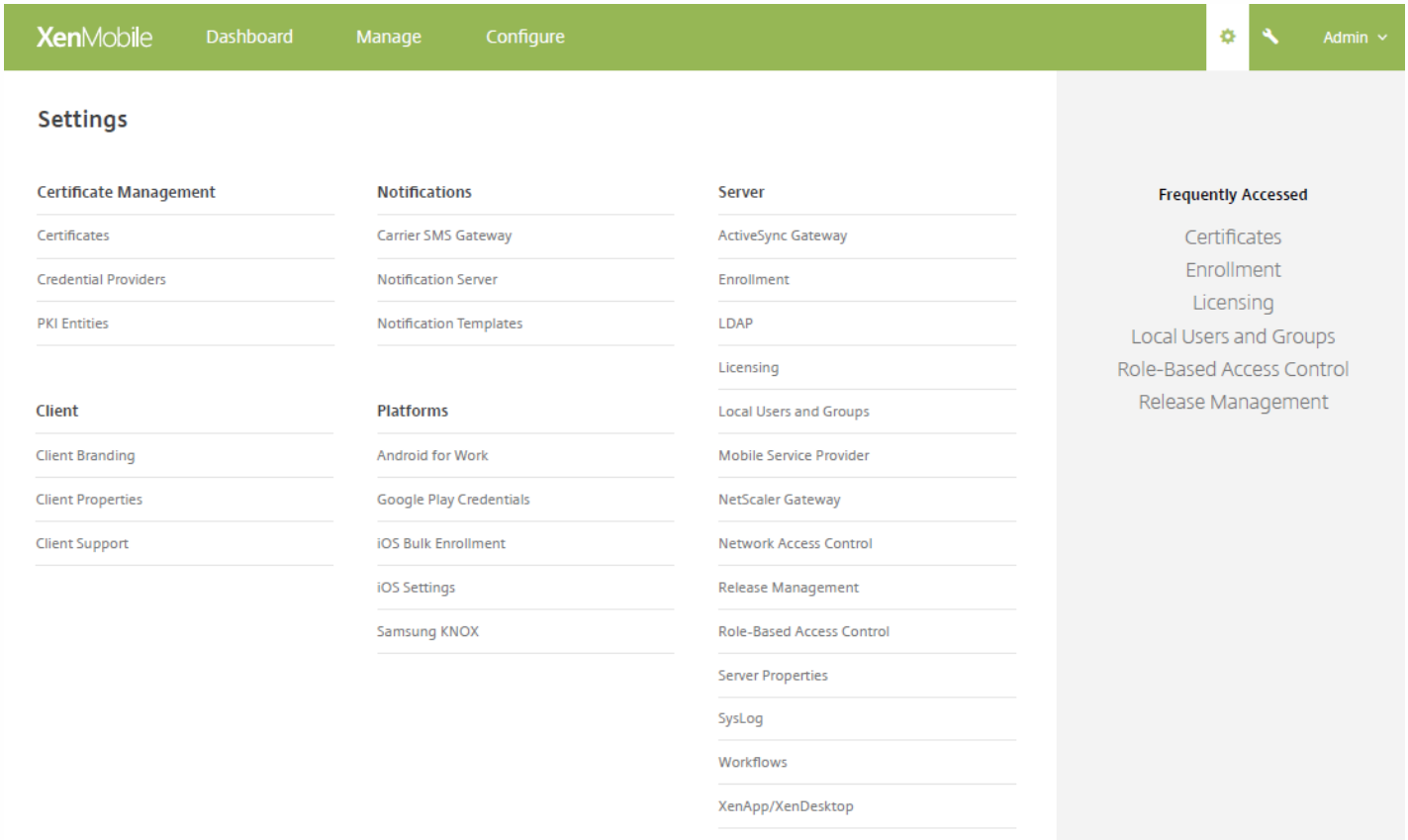
You can set the way apps appear in the store and add a logo to brand Secure Hub and the XenMobile Store on mobile devices for iOS and Android.

Note: Before you begin, make sure you have your custom image ready and accessible.

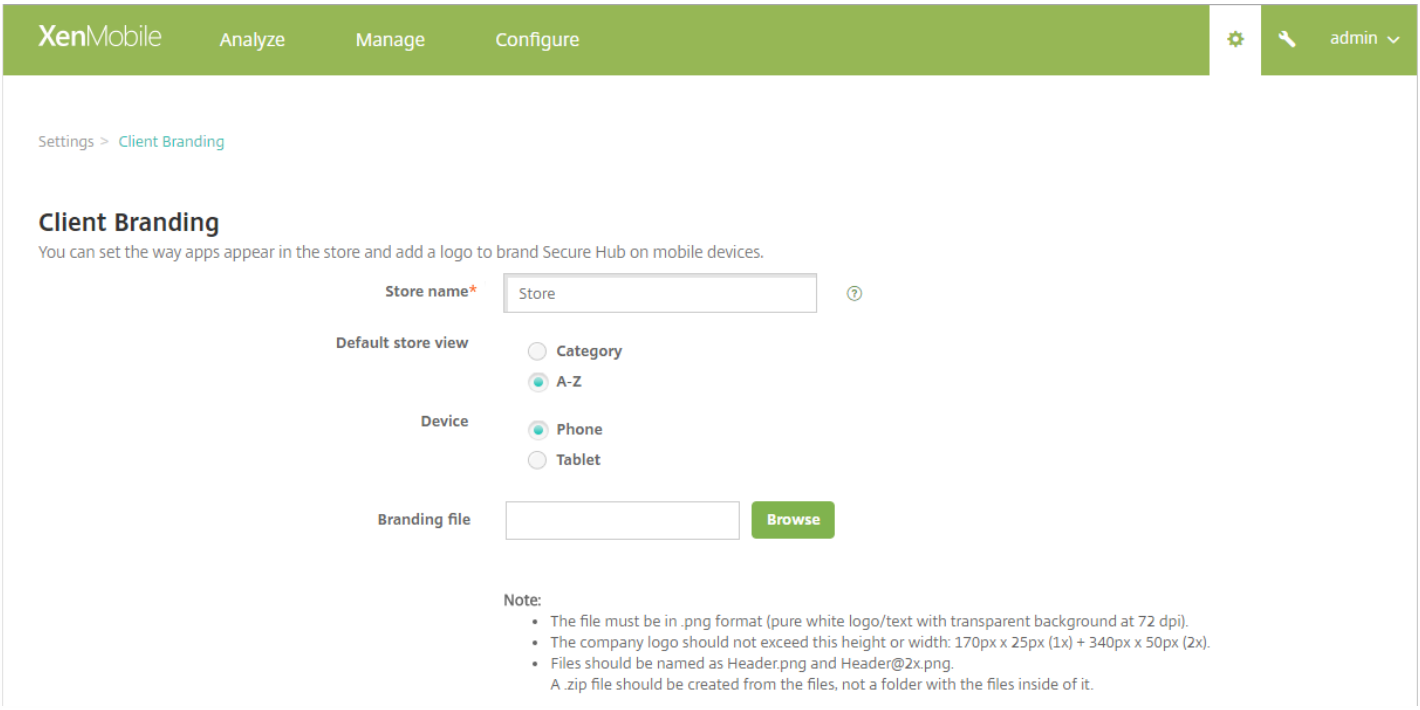
The custom image must meet these requirements:

- 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.



3. 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**: To select an image or .zip file of images to use for branding, click **Browse** and navigate to the file location.

4. Click **Save**.

To deploy this package to users' devices, you need to create a deployment package and deploy it.

Connectivity checks

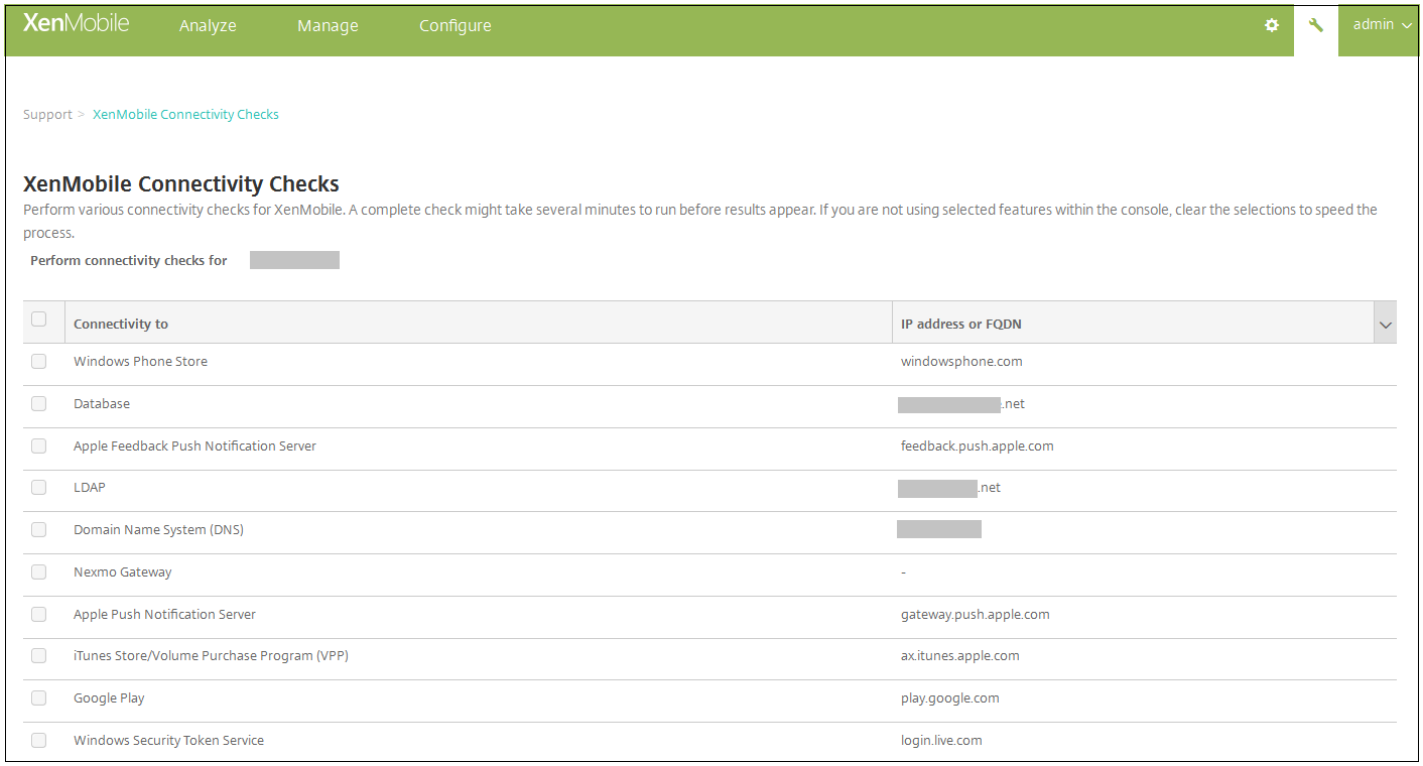
Feb 13, 2017

From the XenMobile **Support** page, you can check the XenMobile connection to NetScaler Gateway and to other servers and locations.

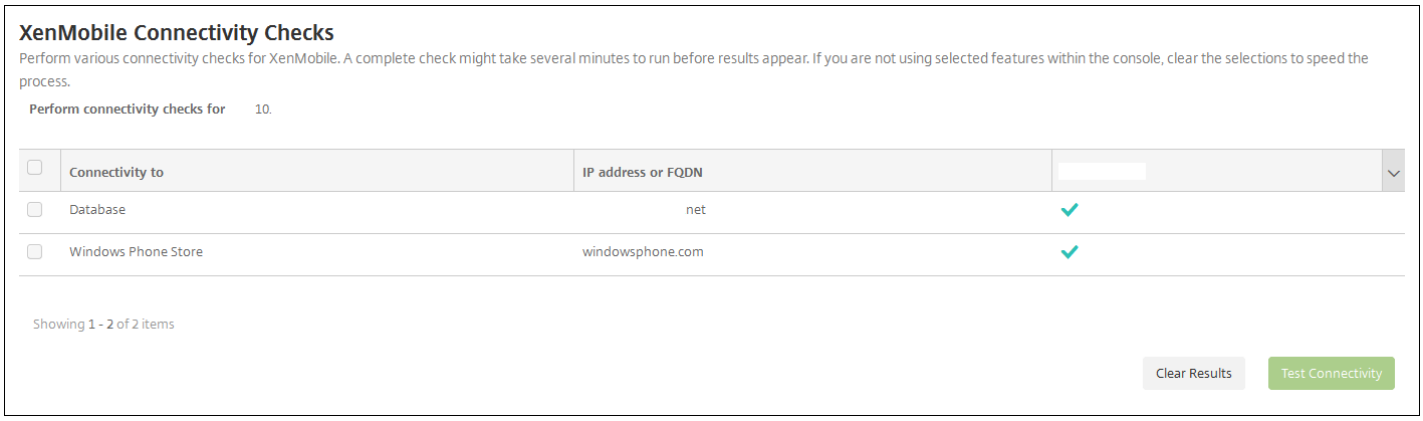
Conducting XenMobile Connectivity Checks

1. In the XenMobile console, click the wrench icon in the upper-right corner of the console. The **Support** page appears.

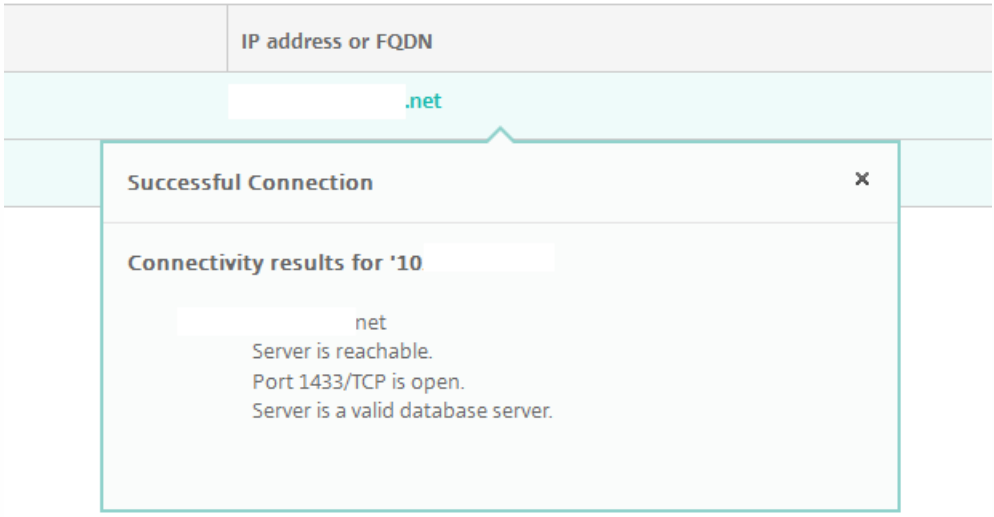
2. Under **Diagnostics**, click **XenMobile Connectivity Checks**. The **XenMobile Connectivity Checks** page appears. If your XenMobile environment contains clustered nodes, all nodes are shown.



2. Select the servers you want to include in the connectivity test and then click **Test Connectivity**. The test results page appears.

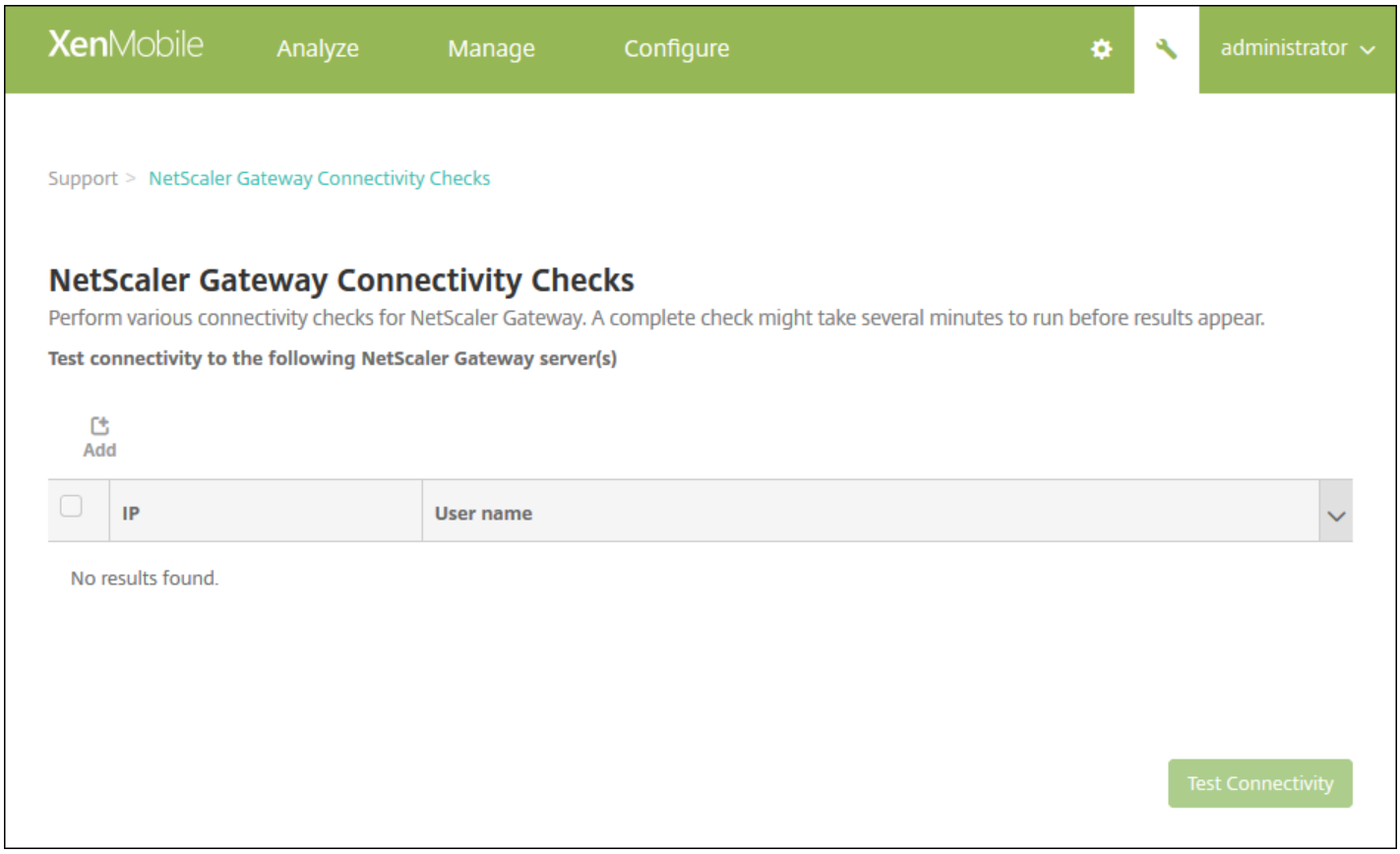


3. Select a server in the test results table to see detailed results for that server.

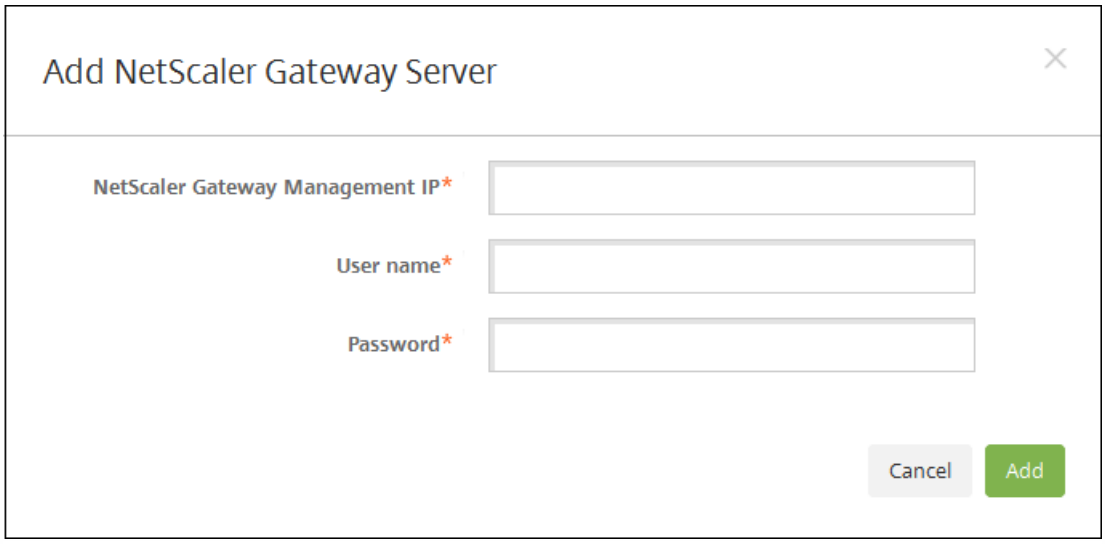


Conducting NetScaler Gateway Connectivity Checks

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.



2. Click **Add**. The **Add NetScaler Gateway Server** dialog box appears.



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 was already 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 was already 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.

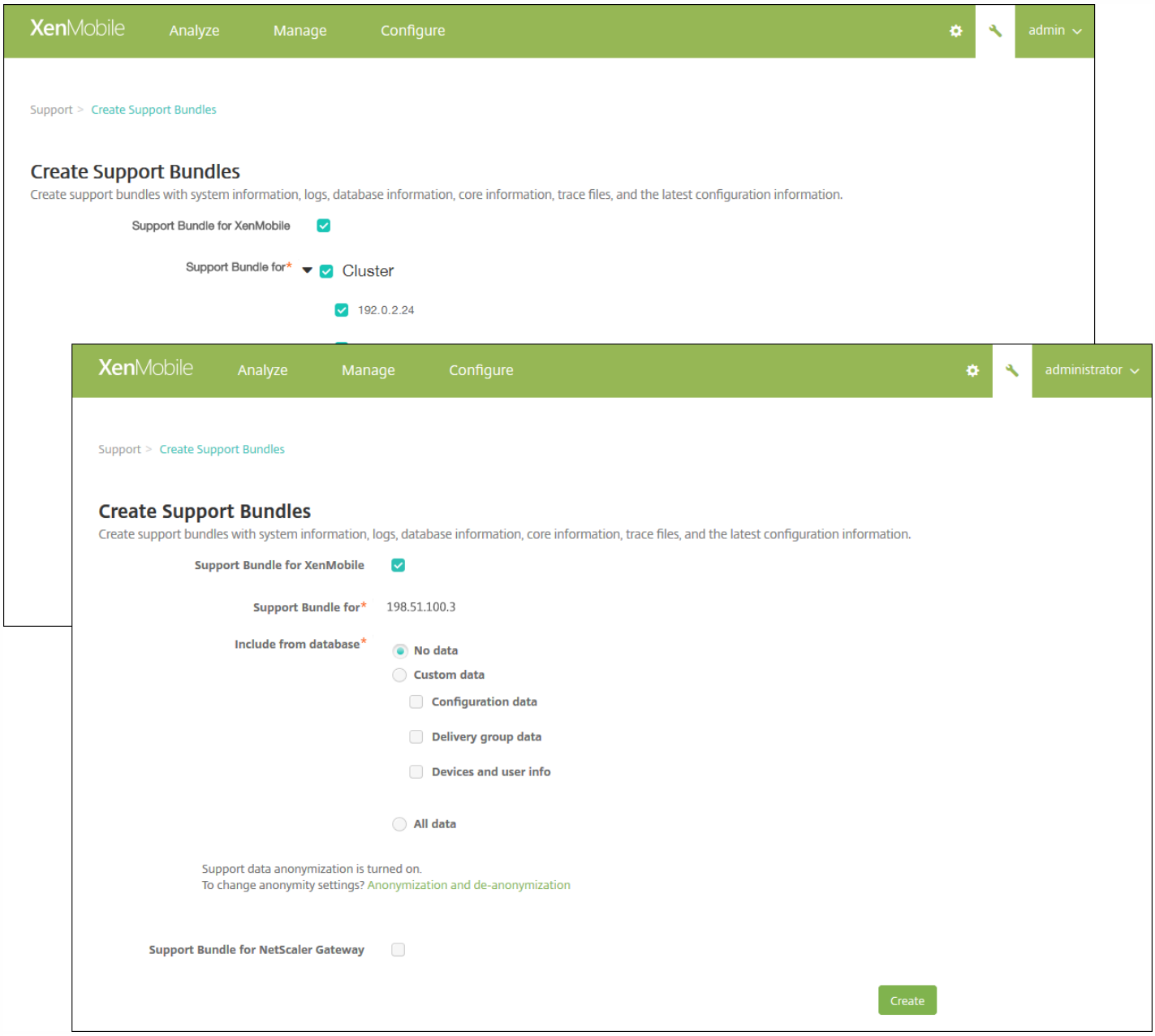
Support bundles

Nov 09, 2016

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.



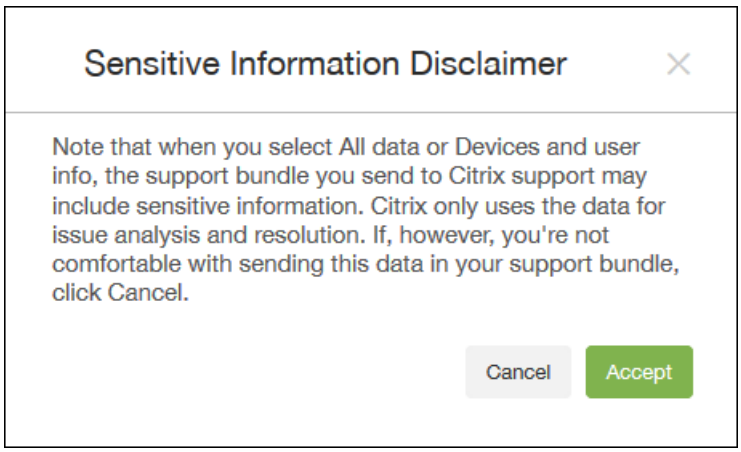
3. Make sure that the **Support Bundle for XenMobile** check box is selected.

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.

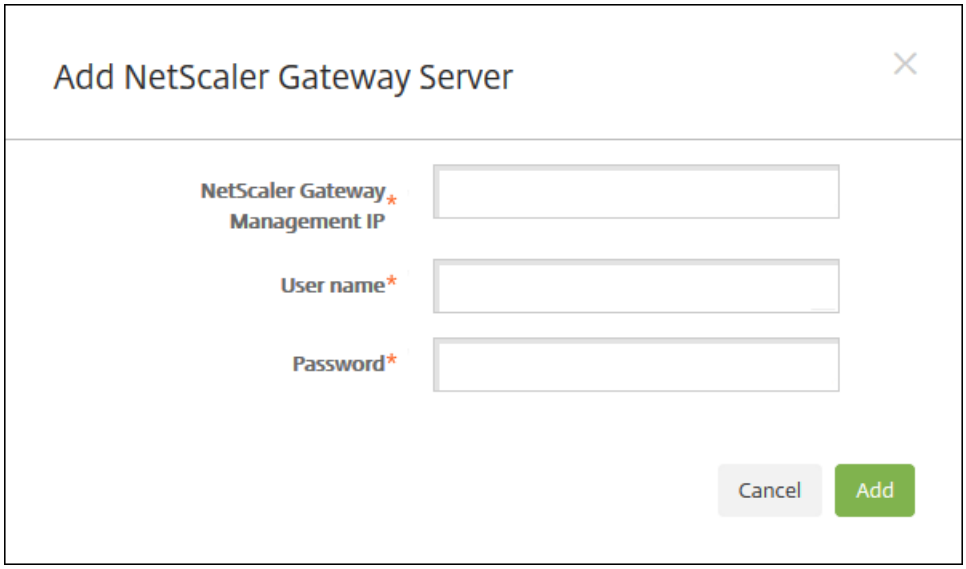


6. The **Support data anonymization is turned on** option indicates that the default setting is to anonymize the data, which means that sensitive user, server, and network data is made anonymous in support bundles.

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.



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.

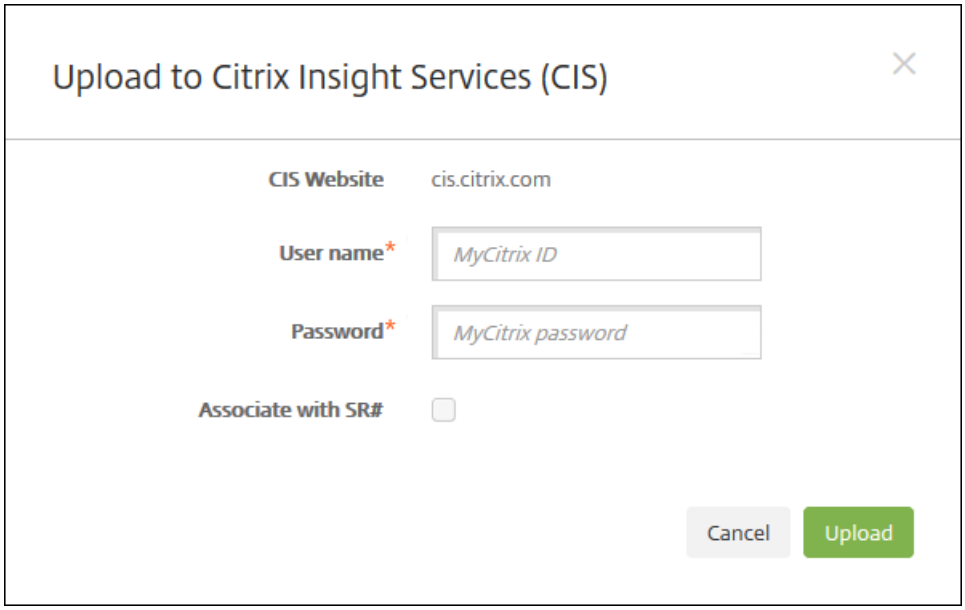
8. Repeat Step 7 to add more NetScaler Gateway support bundles.

9. Click **Create**. The support bundle is created and two new buttons, **Upload to CIS** and **Download to Client**, appear.

Uploading Support Bundles to Citrix Insight Services

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.



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.

6. Read the agreement and then click **Agree and upload**. The support bundle is uploaded.

Downloading support bundles to your computer

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.

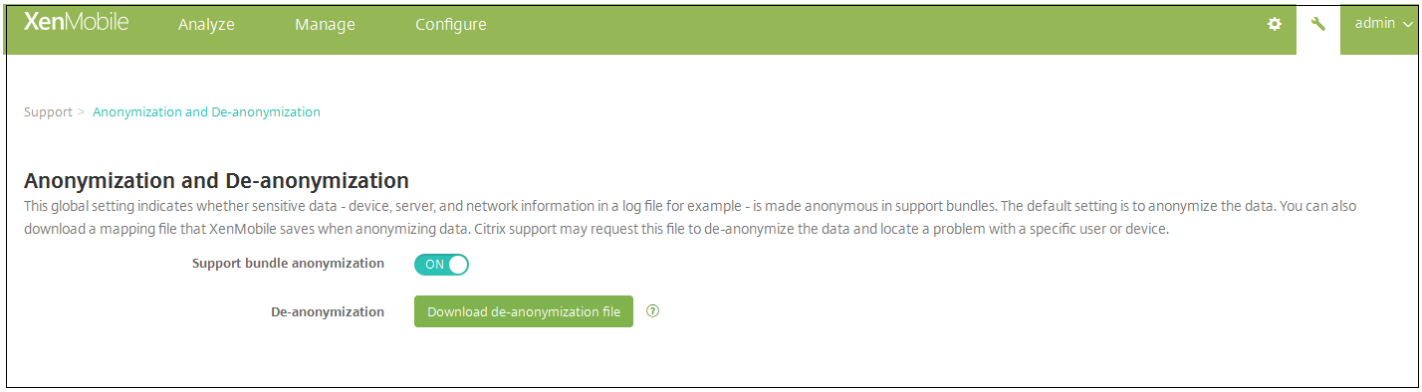
Anonymize data in support bundles

Nov 09, 2016

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.



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.

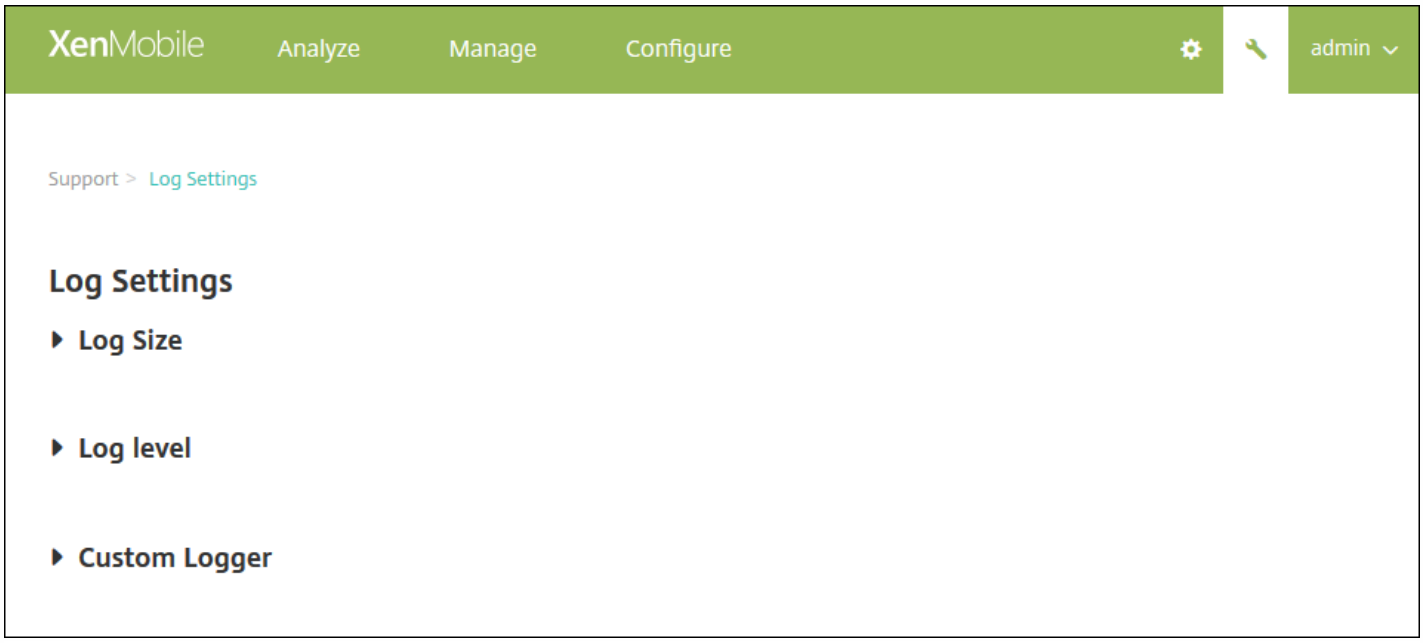
Logs

Oct 05, 2016

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.

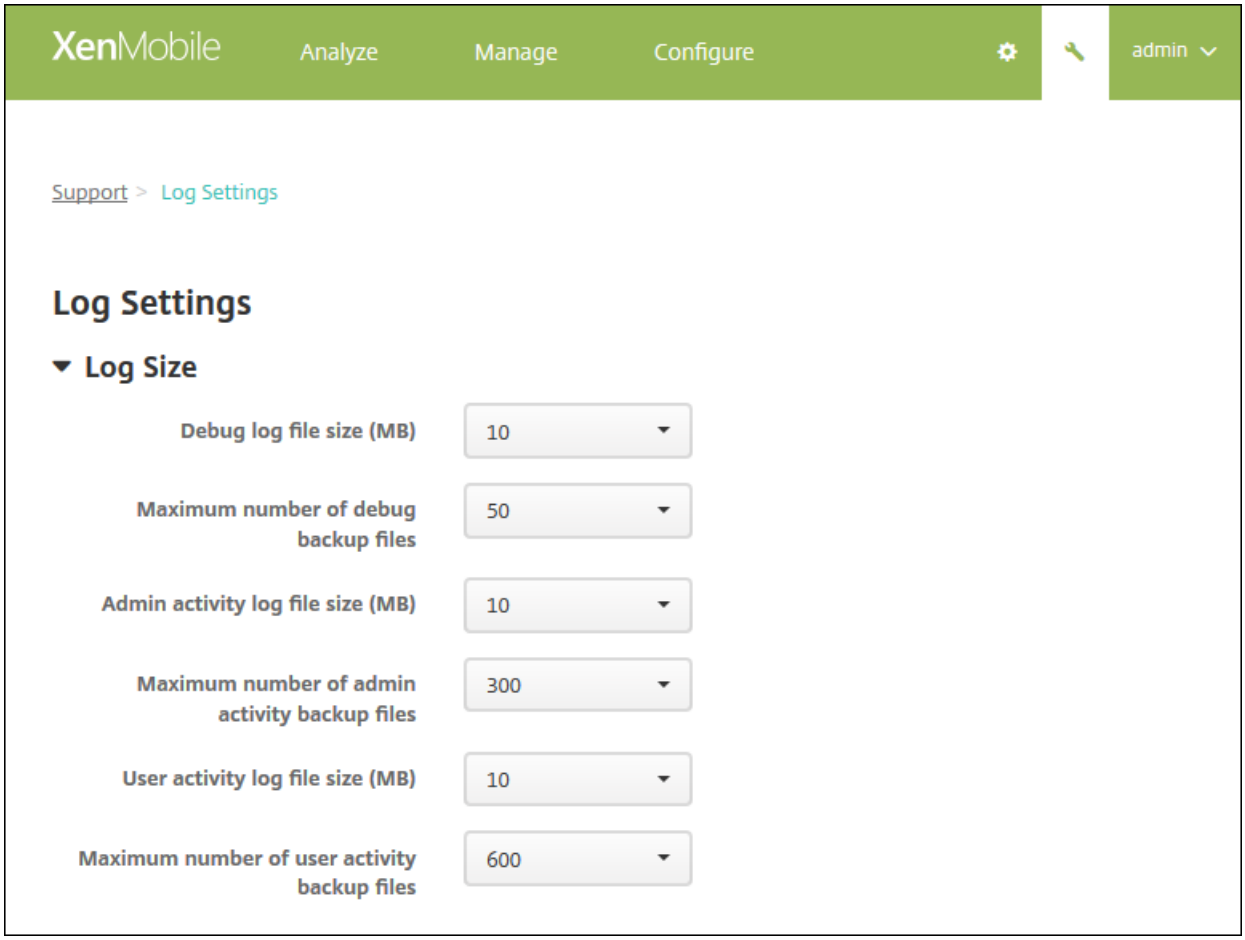


On the **Log Settings** page you can access the following options:

- **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.

To configure the Log Size options

1. On the **Log Settings** page, expand **Log Size**.



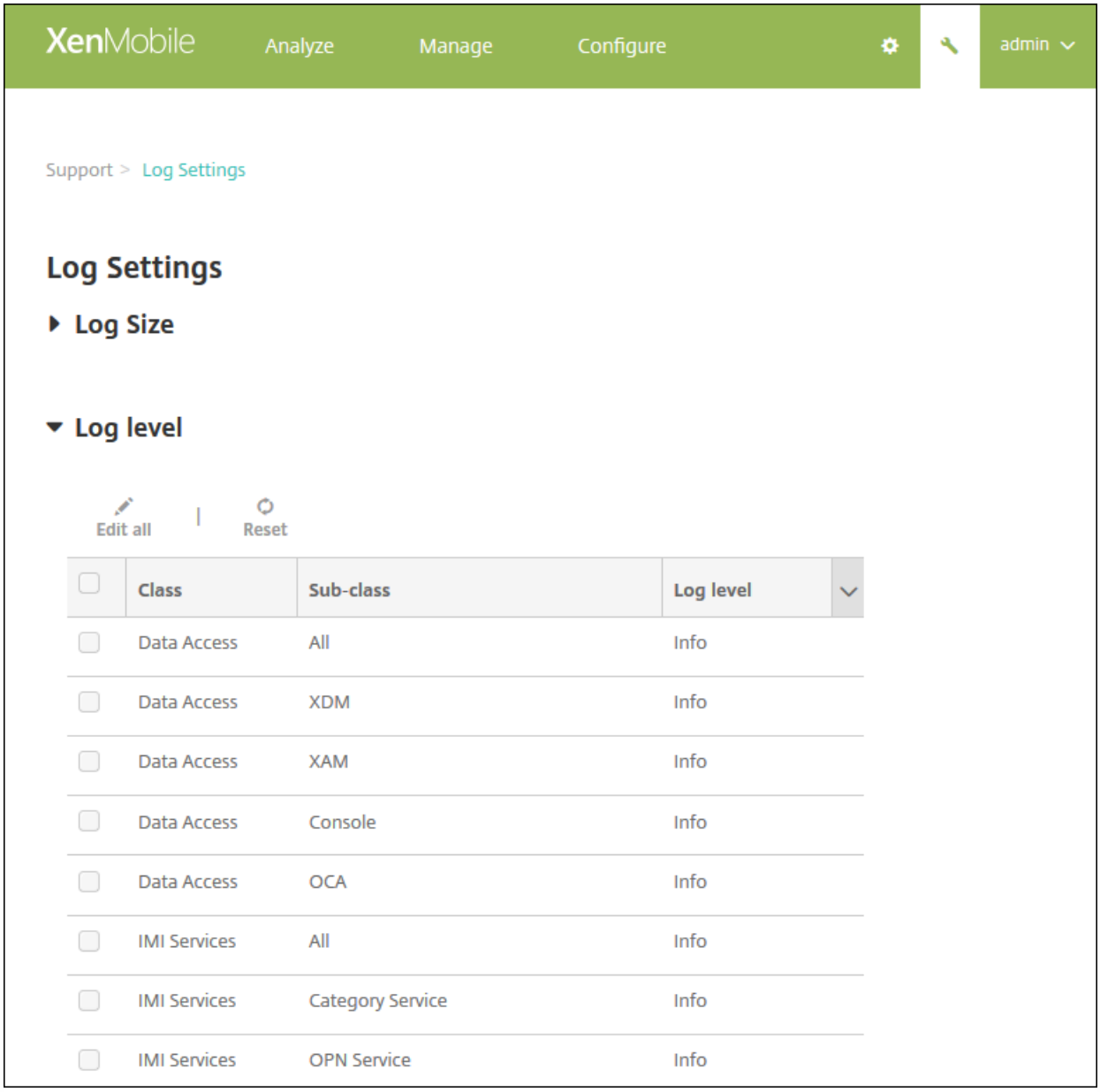
2. Configure these settings:

- **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.

To configure Log Level options

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.

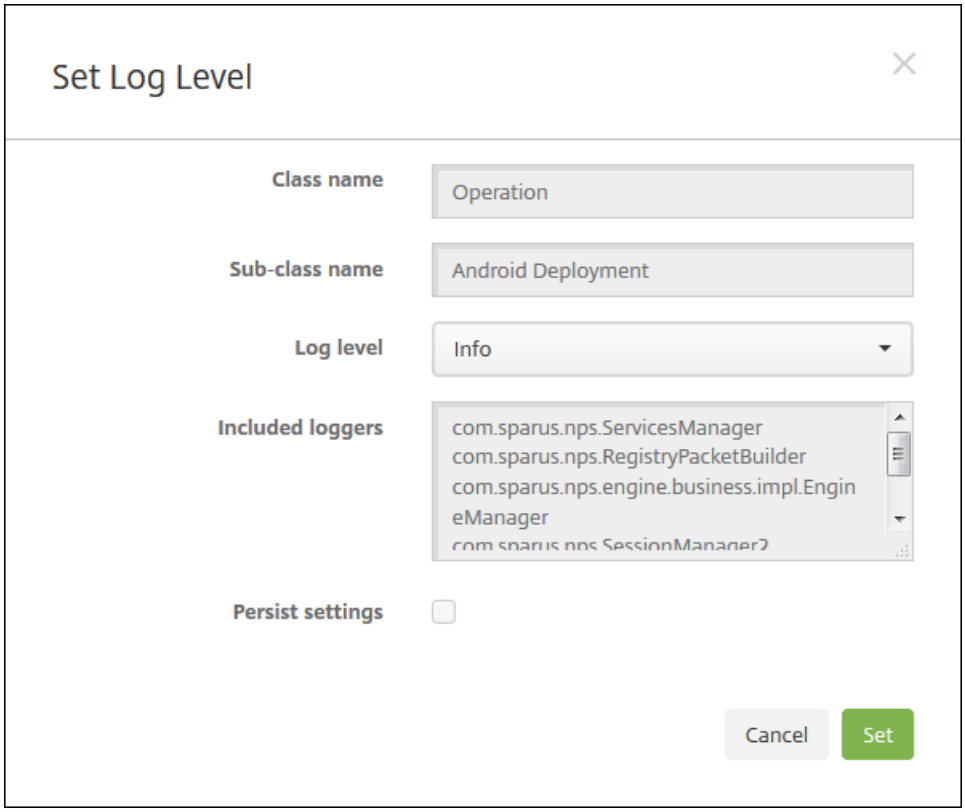
1. On the **Log Settings** page, expand **Log level**. The table of all log classes appears.



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.

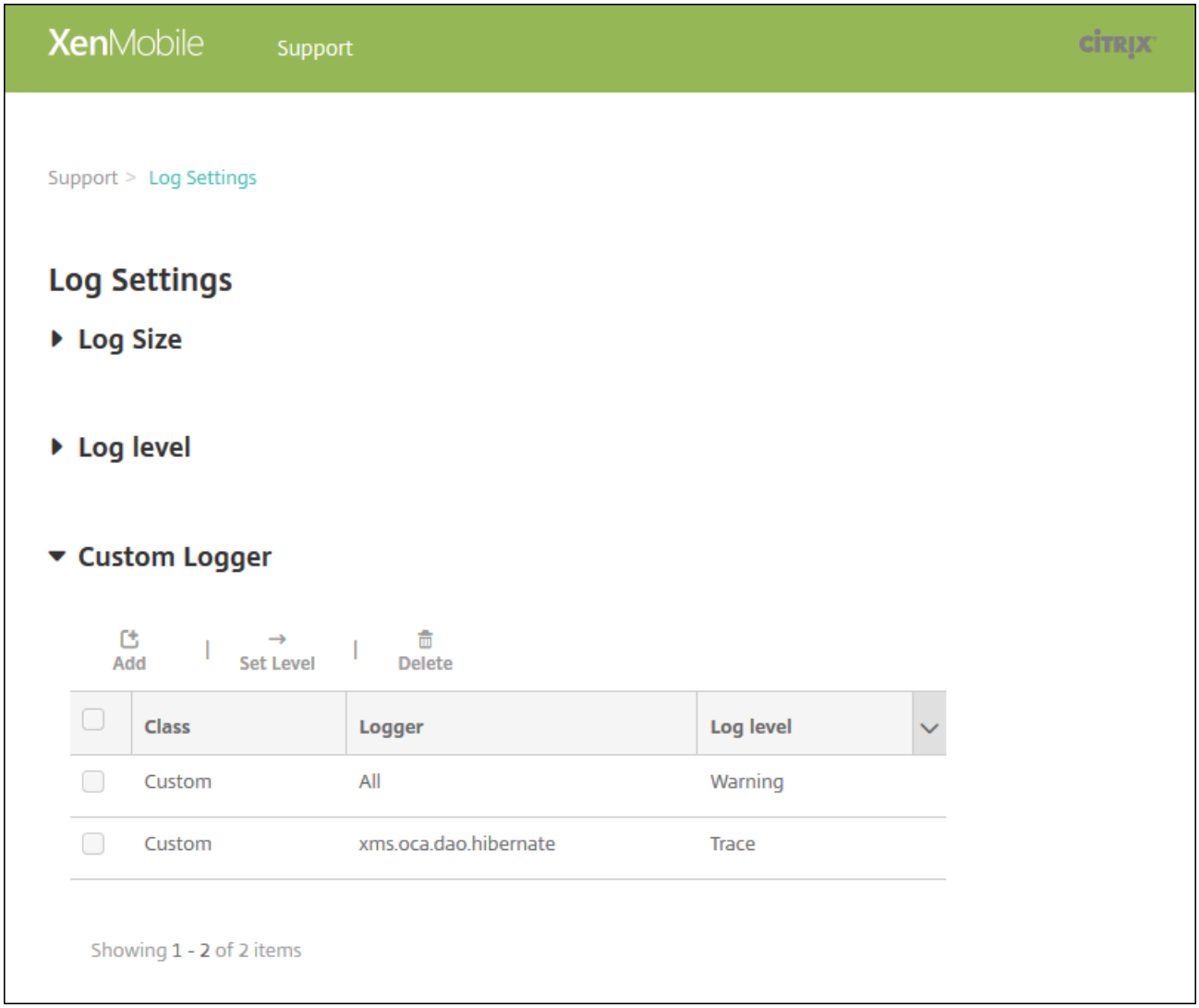


- **Class Name**: This field displays All when you are changing the log level for all classes or it displays the individual class name; it is not editable.
- **Sub-class name**: This field displays All when you are changing the log level for all classes or it displays the individual class sub-class name; 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.

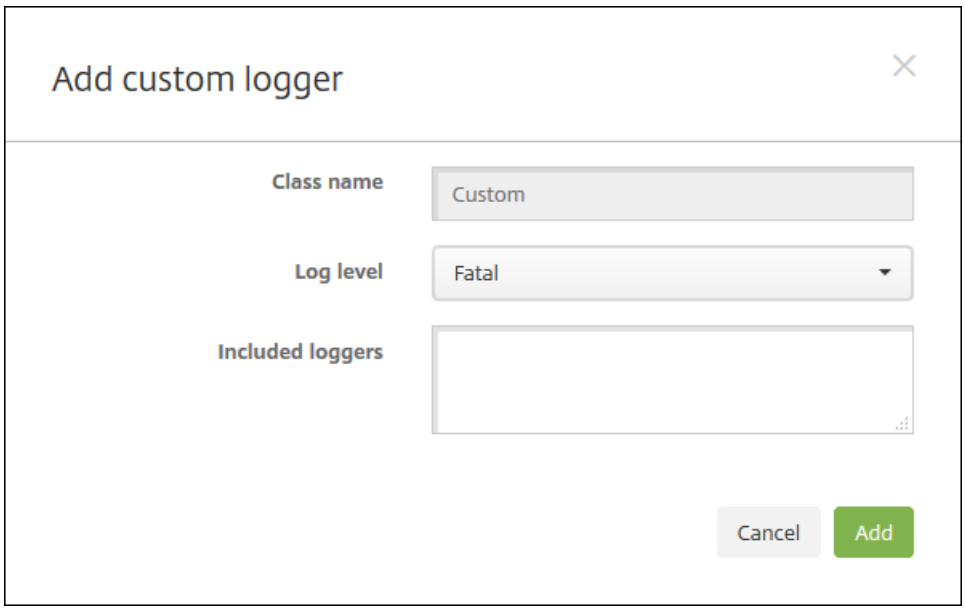
3. Click **Set** to commit your changes.

To add a Custom Logger

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.



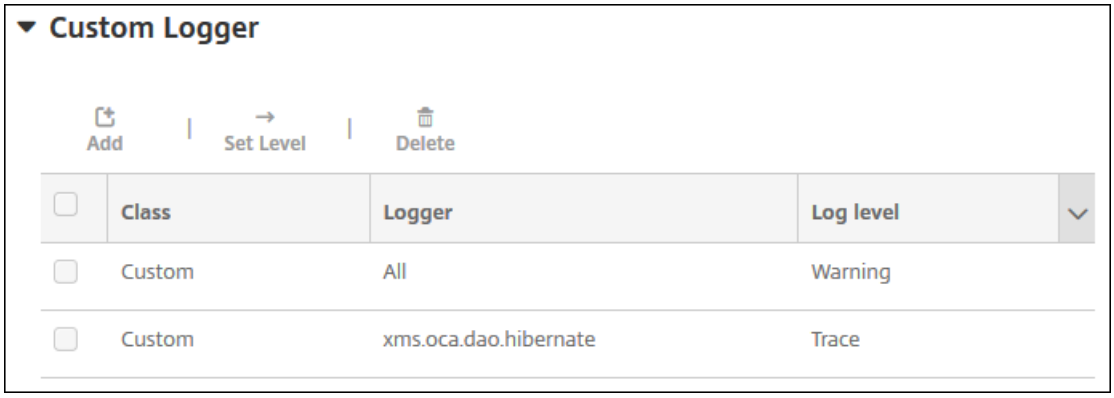
2. Click **Add**. The **Add custom logger** dialog box appears.



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.



To delete a Custom Logger

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 with XenMobile 10.4

Mar 29, 2017

For the documentation on the most recent version of the XenMobile Analyzer, see XenMobile Analyzer Tool.

XenMobile Analyzer is a cloud-based tool that you can use to diagnose and troubleshoot XenMobile-related issues with installation and other features. The tool checks for device or user enrollment and authentication issues within your XenMobile environment.

To enable the checks, you need to configure the tool to point to your XenMobile server and you need to provide information, such as server deployment type, mobile platform, authentication type, and user credentials for testing. 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.

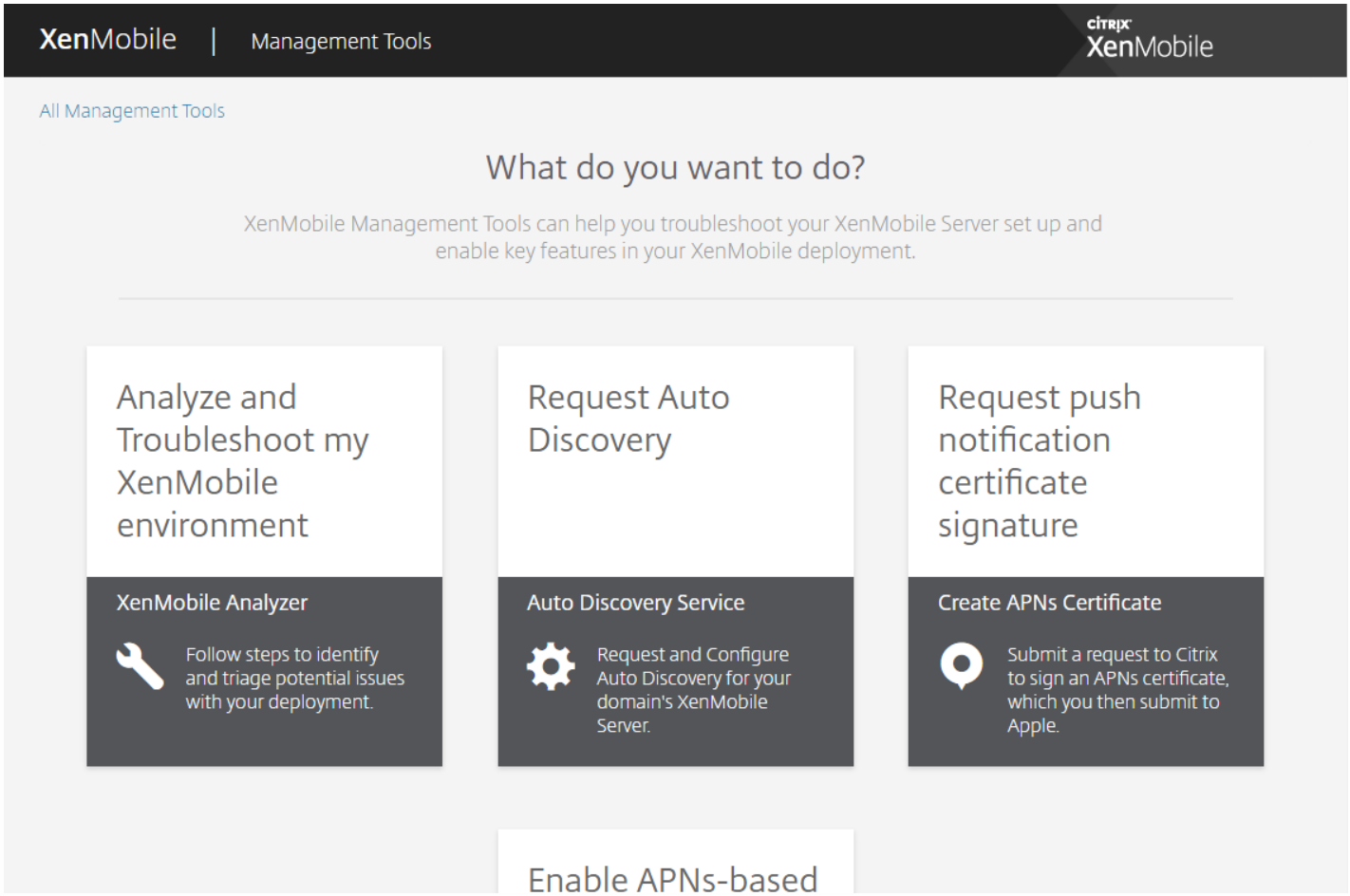
XenMobile Analyzer Key Features

- Offers a secure, cloud-based micro-service to troubleshoot all XenMobile-related issues.
- Provides accurate recommendations when there are XenMobile configuration issues.
- Reduces support calls and accelerates the troubleshooting of XenMobile environments.
- Offers zero-day support for XenMobile server releases.
- Enables iOS custom enrollment: custom port support for XenMobile (on ports other than 8443).
- Displays a certificate acceptance dialog box for untrusted or incomplete server certificates.
- Automatically detects two-factor authentication scenarios.
- Secure Web tests for reachability to intranet sites.
- Secure Mail Auto Discovery service checks.
- ShareFile single sign-on (SSO) checks.
- Enables custom port support for NetScaler.
- Supports non-EN browsers.

Prerequisites

Product	Supported Version
XenMobile Server	10.3.0 and above
NetScaler Gateway	10.5 and above
Client Enrollment Simulation	iOS and Android

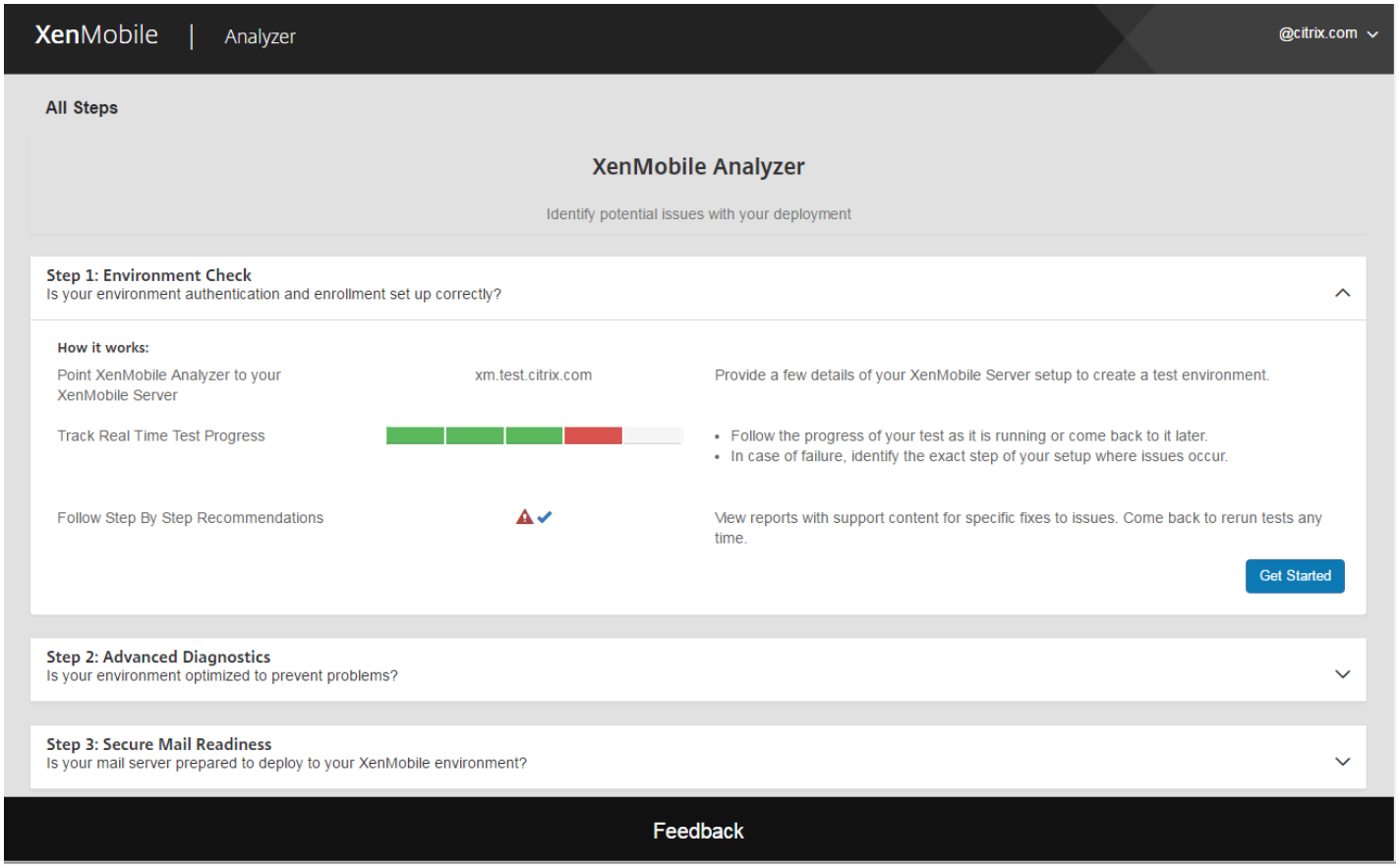
You use your MyCitrix credentials to access the tool from https://xenmobiletools.citrix.com. On the XenMobile Management Tools page that opens, to start the XenMobile Analyzer, click **Analyze and Troubleshoot my XenMobile Environment**.



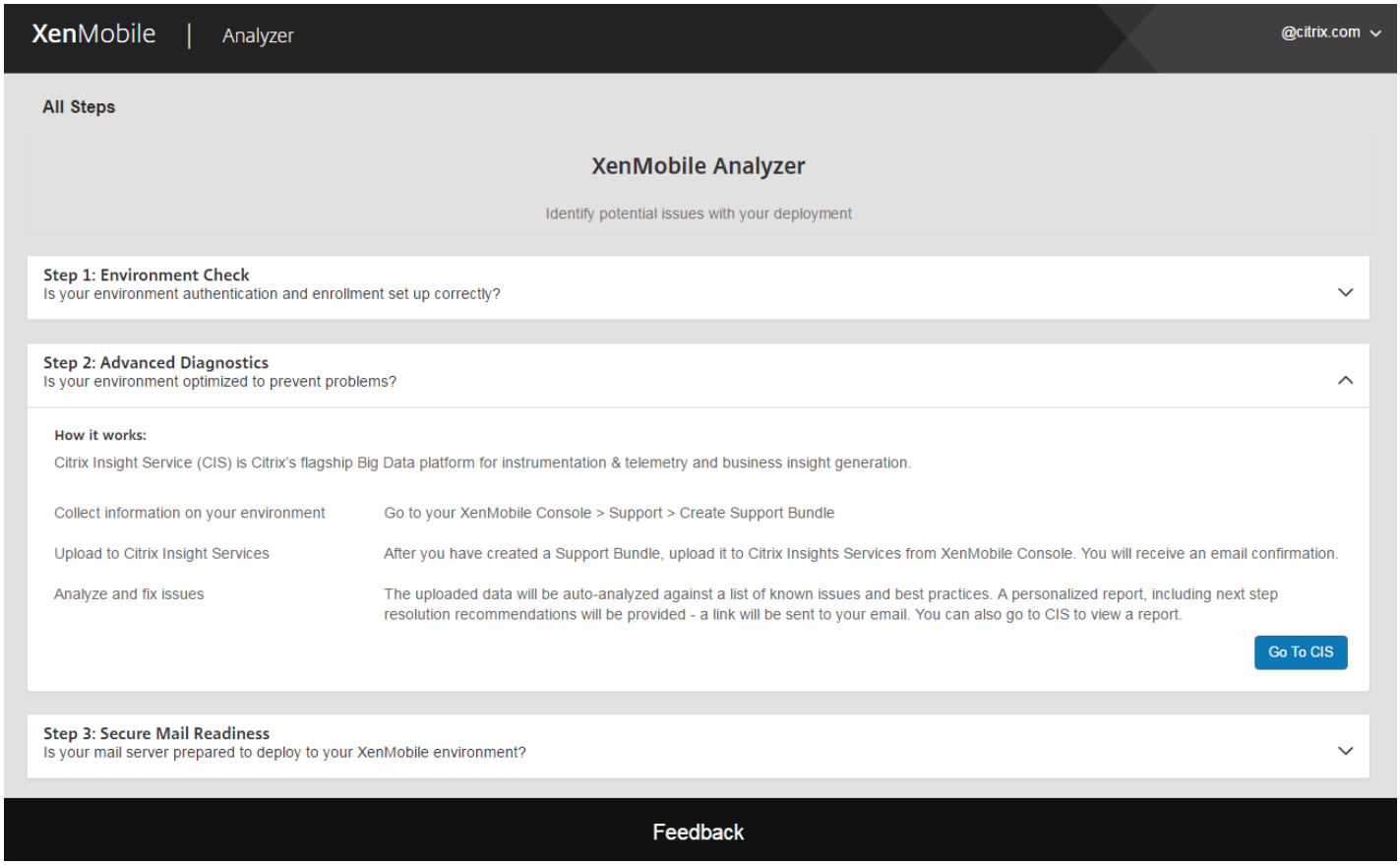
XenMobile Analyzer contains five main steps designed to lead you through the triage process and to reduce the number of support tickets, which can lower costs for everyone.

The steps are as follows:

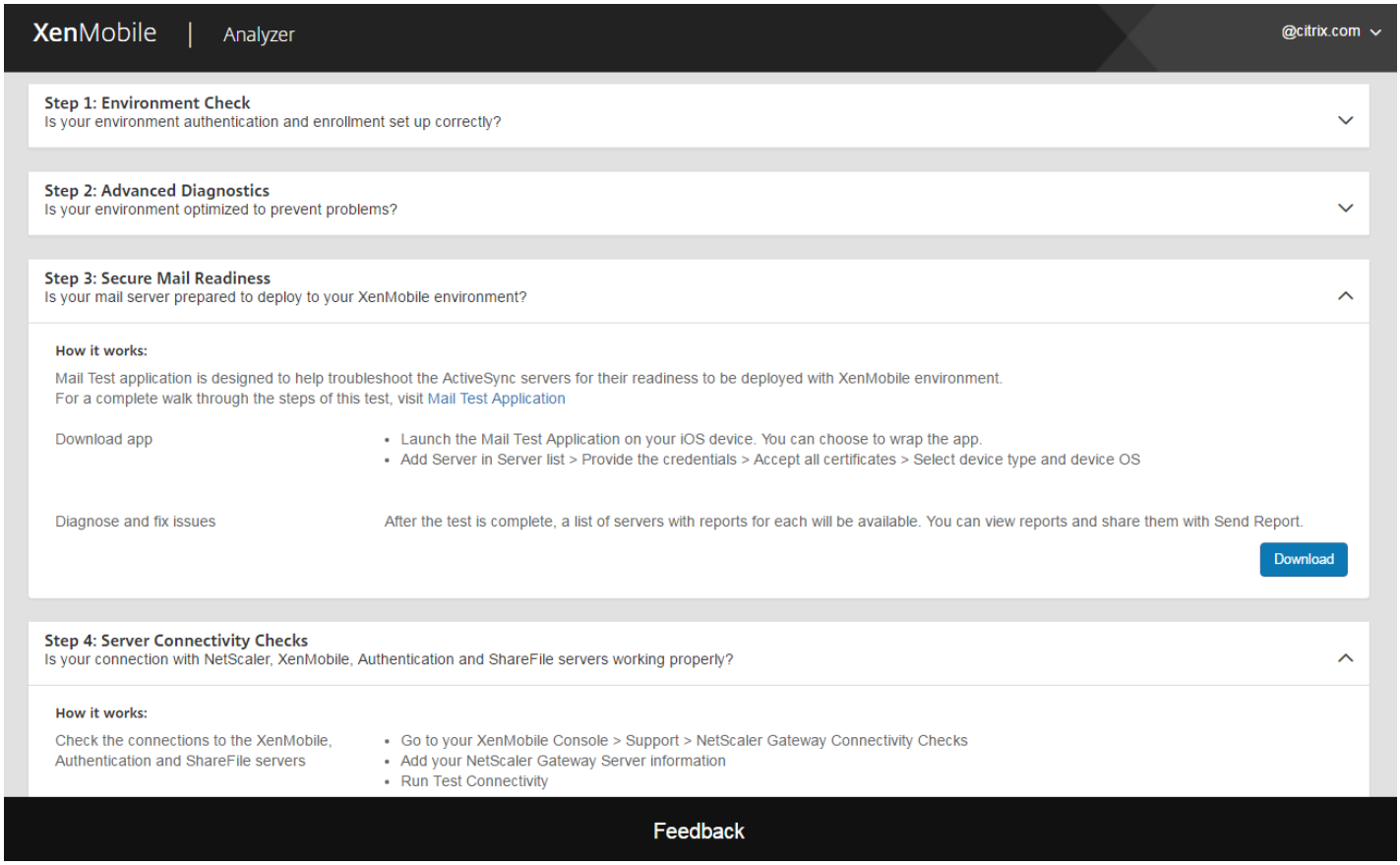
1. **Environment Check** - This step guides you in setting up tests to check your setup for issues. The step also provides recommendations and solutions on device, user enrollment, and authentication issues.



2. **Advanced Diagnostics** - This step provides information on using Citrix Insight Services to find further issues that the environment check may have missed.

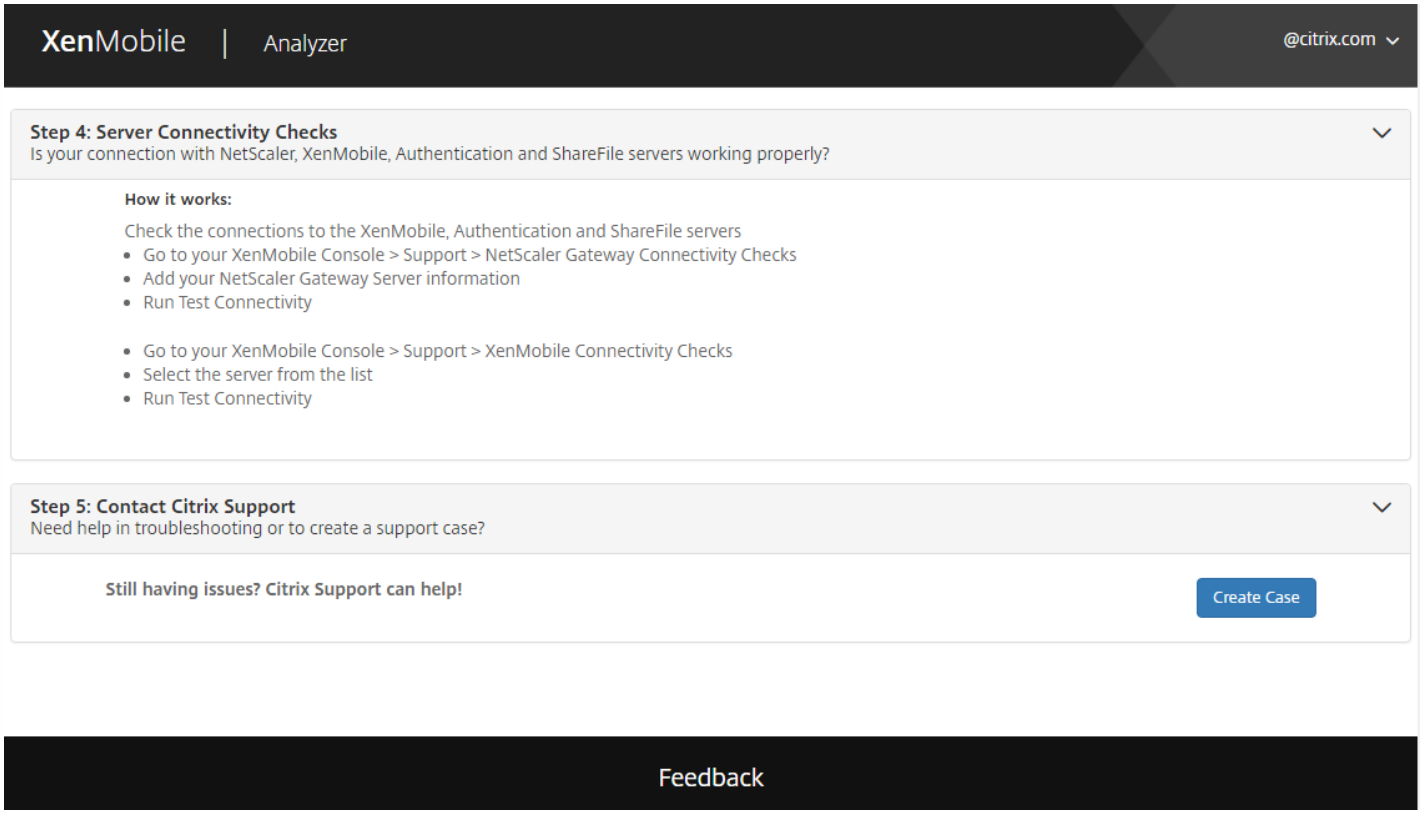


3. **Secure Mail Readiness** - This step directs you to download the XenMobile Exchange ActiveSync Test application, which helps to troubleshoot the ActiveSync servers for their readiness to be deployed with a XenMobile environment.



4. **Server Connectivity Checks** - This step instructs you to test the connectivity of your servers.

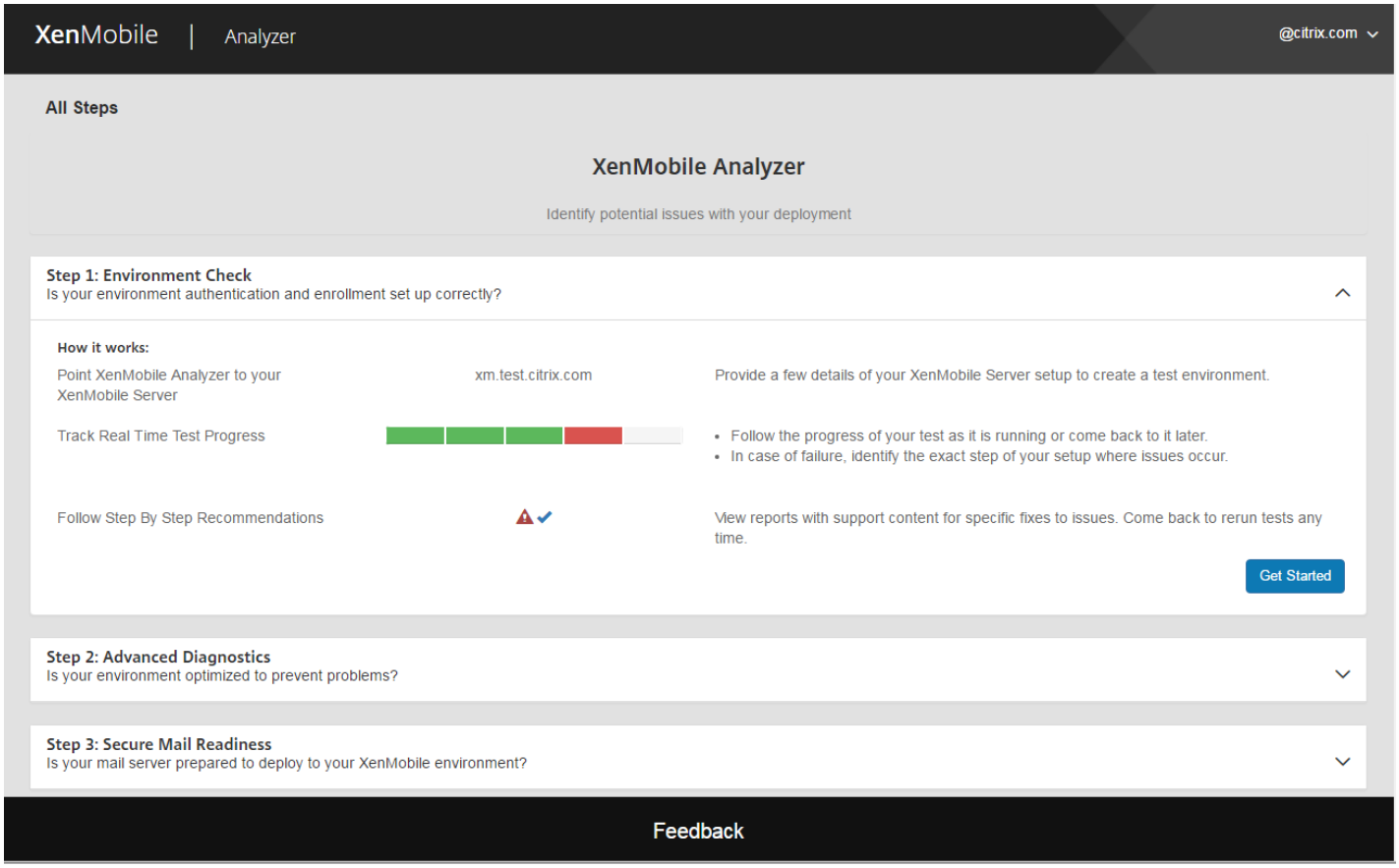
5. **Contact Citrix Support** - This step links you to the site where you can create a Citrix Support case if you are still having issues.



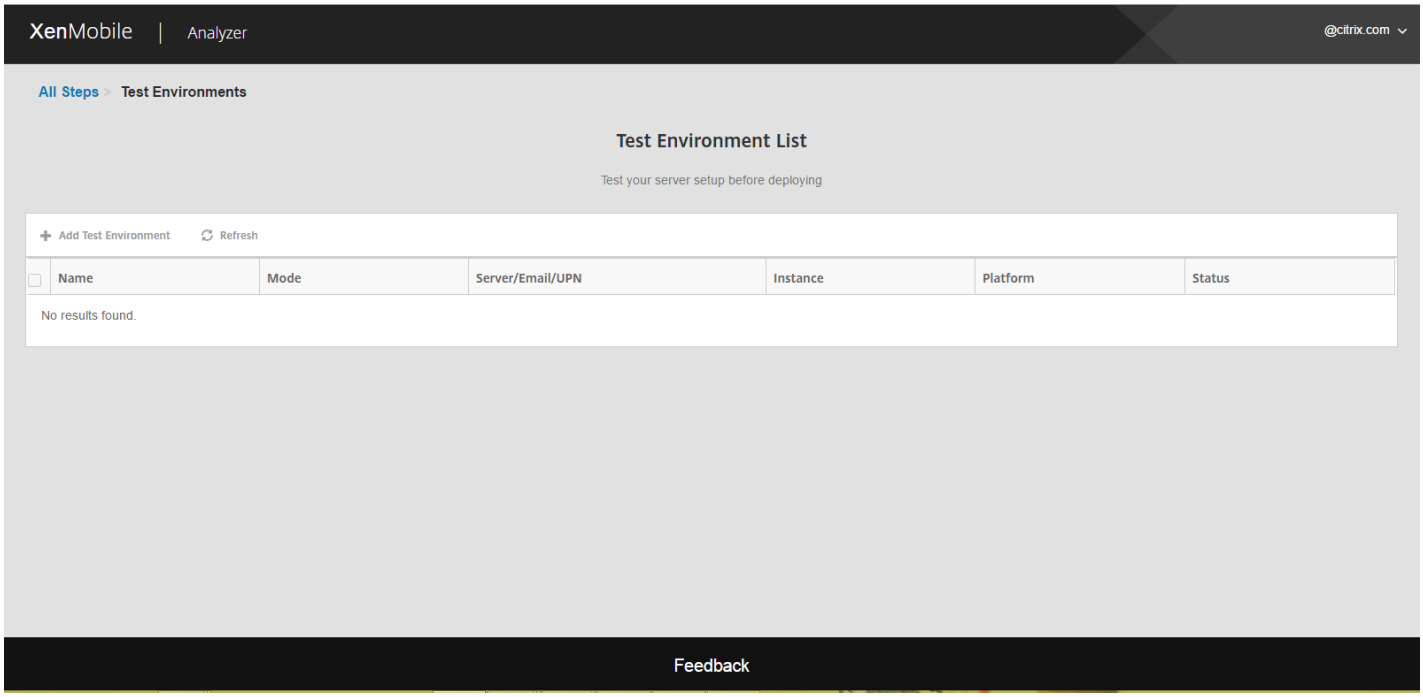
The following sections describe each step in more detail.

Performing an Environment Check

1. Log on to the XenMobile Analyzer and then click **Step 1: Environment Checks**.
2. Click **Get Started**.

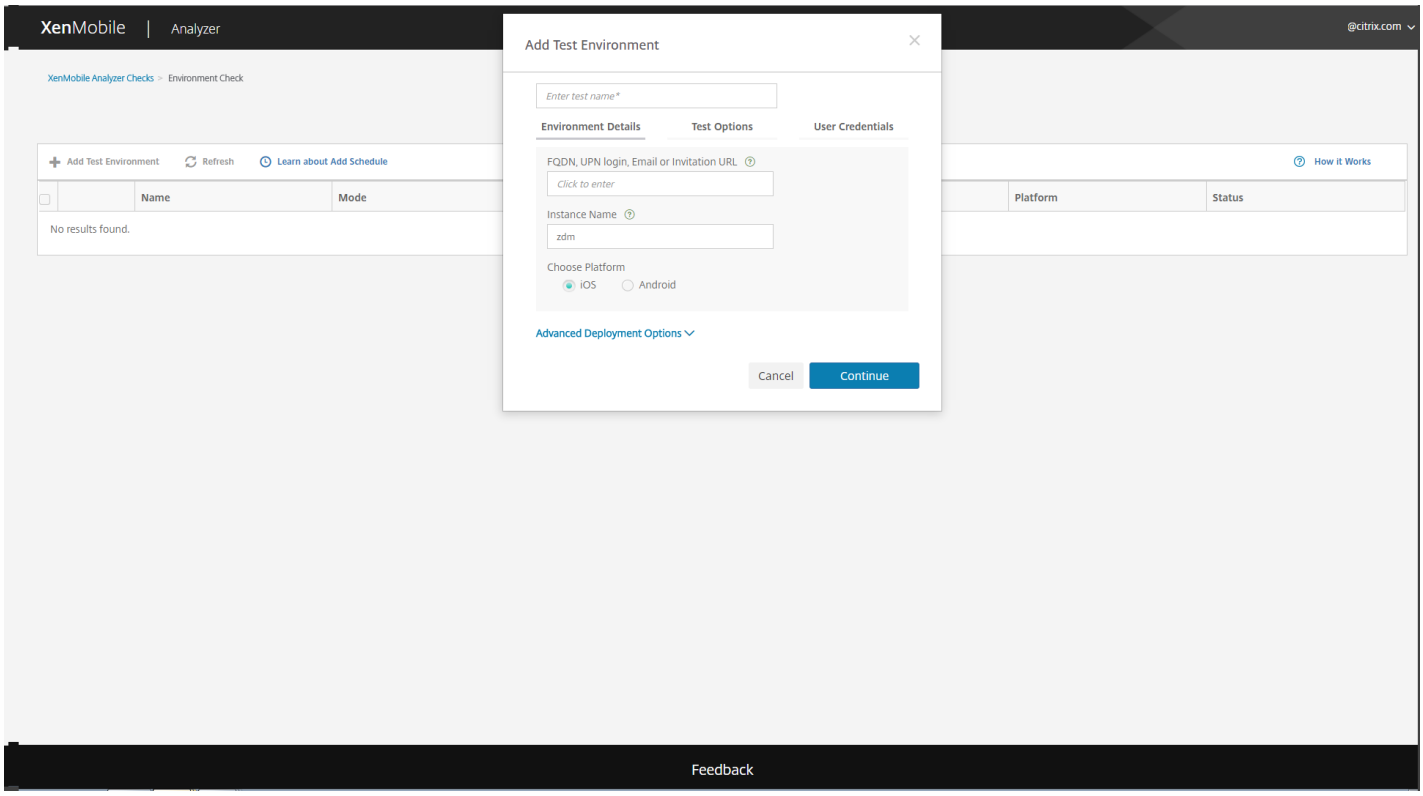


3. Click **Add Test Environment**.



4. In the new **Add Test Environment** dialog box, do the following:

In the above screenshot, please note that Worx Home is now called Secure Hub.



a. Provide a unique name for the test that will help identify the test in the future.

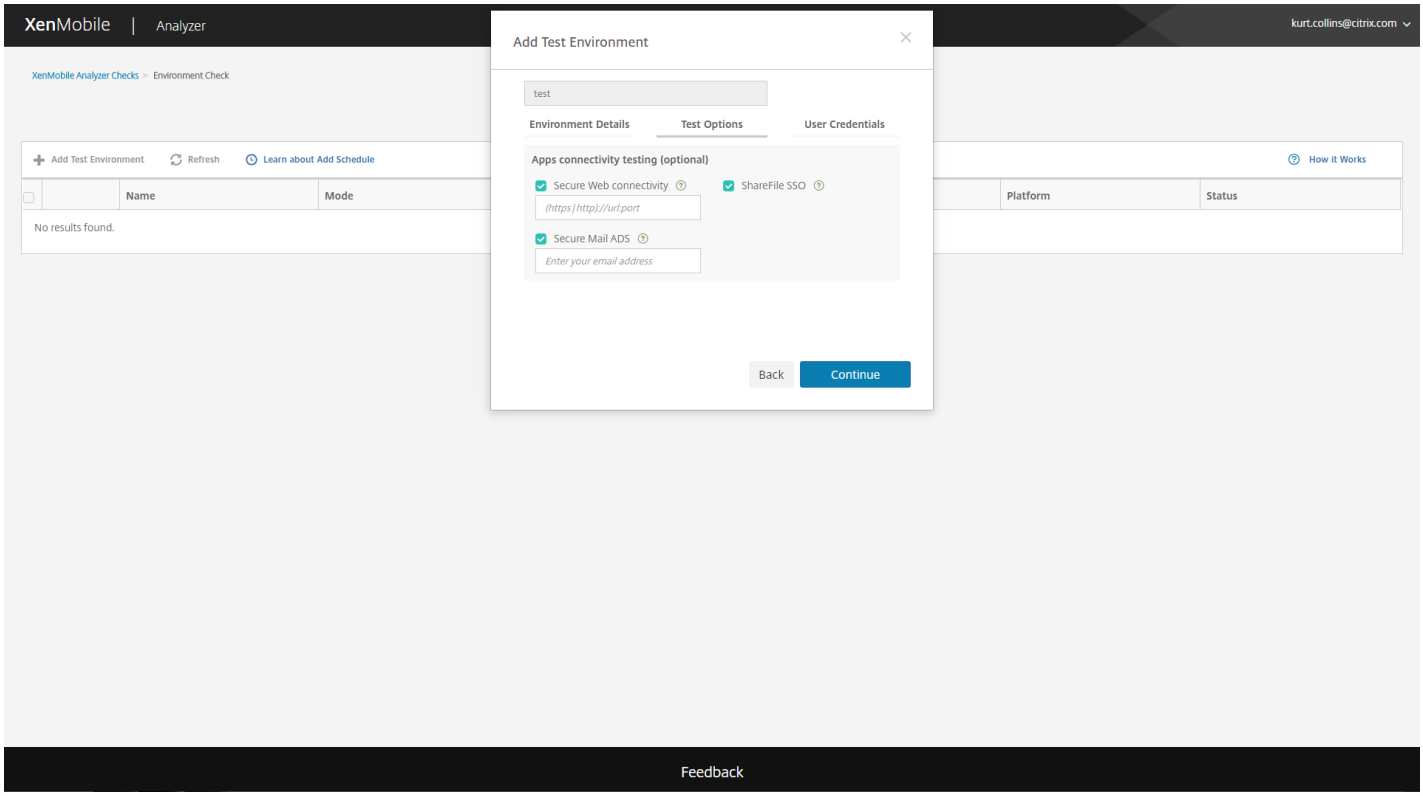
b. In the **FQDN, UPN login, Email or URL Invitation** field, enter the information that will be used to access the server.

c. In **XMS Instance**, if you use a custom instance, you can provide that value.

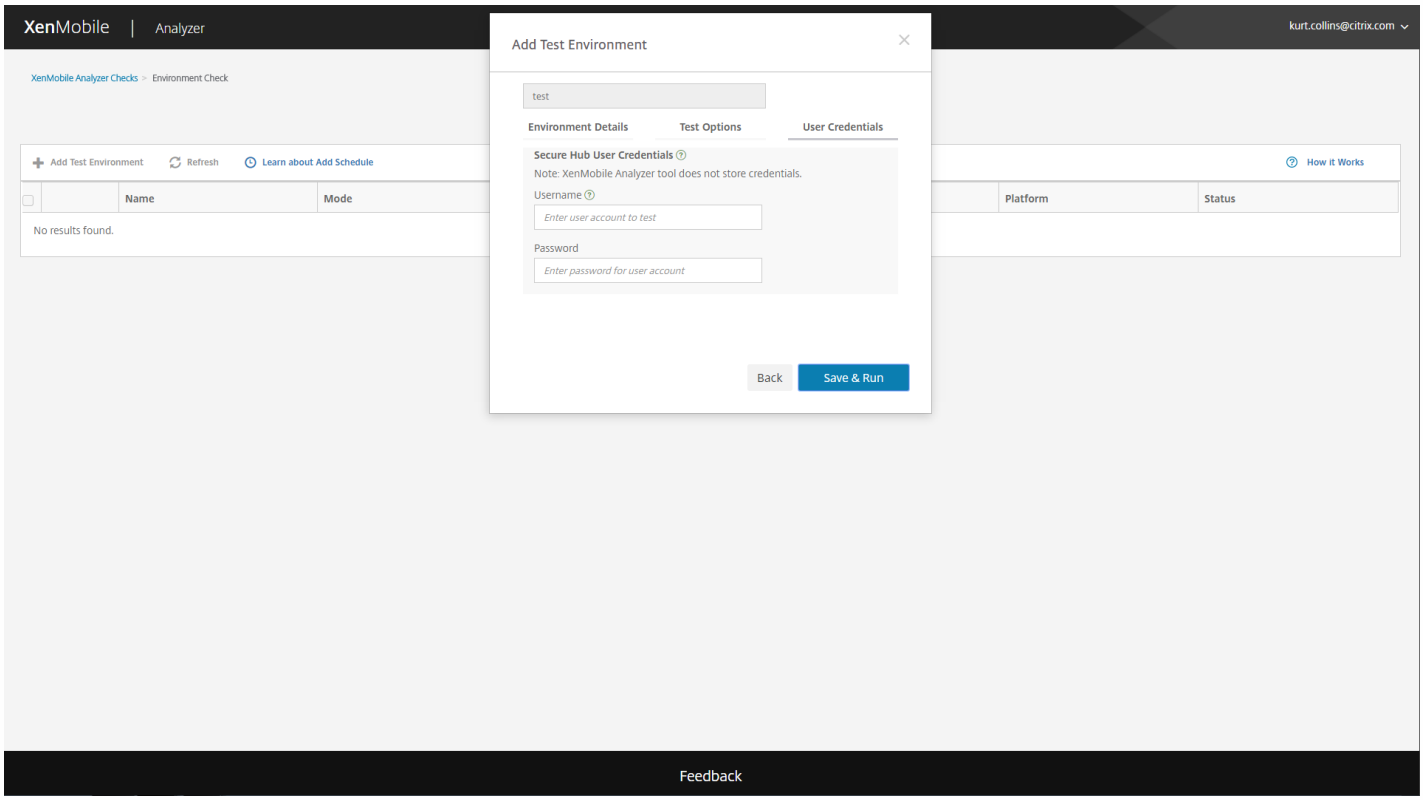
d. In **Choose Platform**, select either **iOS** or **Android** as the platform for testing.

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 Managment (MDM)**.

In the above screenshot, please note that Worx Home is now called Secure Hub.



5. Click **Continue**.



In the above screenshot, please note that WorxWeb is now called Secure Web, and WorxMail is now Secure Mail.

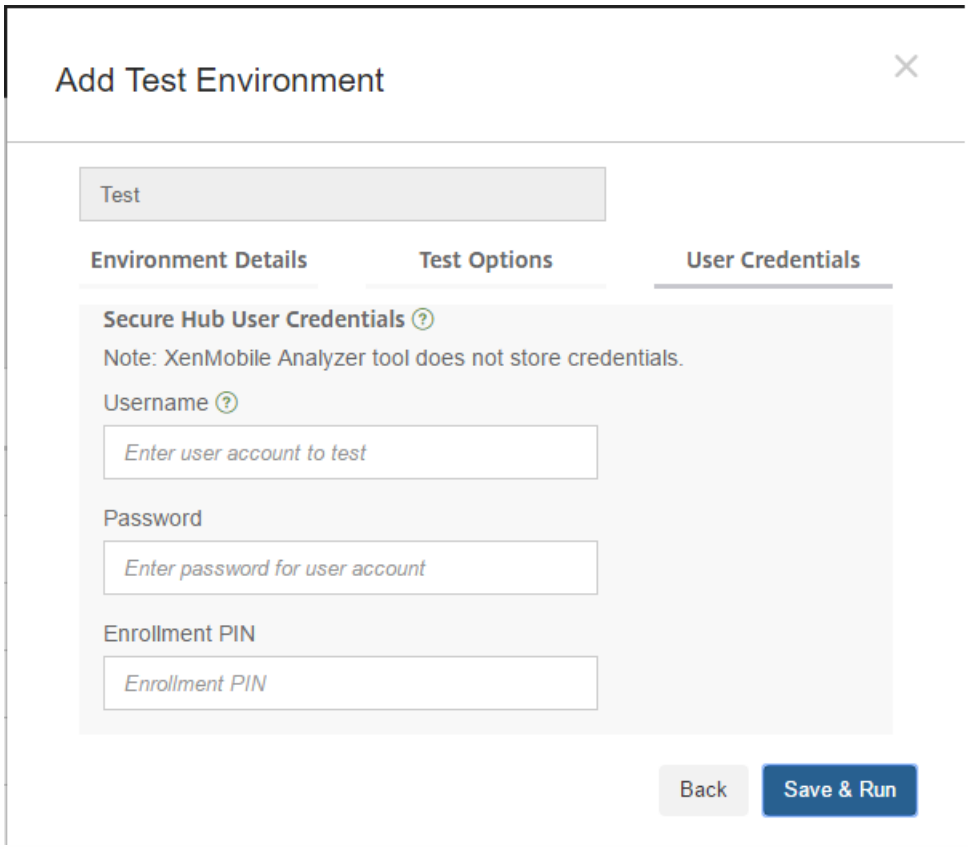
6. You can choose application level tests to run. You can choose one or more of the following tests.

    a. **Secure Web micro VPN Connectivity with intranet sites**. Provide an intranet URL. The tool will test for the reachability of the URL. This will detect if there are any connectivity issues that could potentially occur in the Secure Web app while trying to reach intranet URLs.

    b. **Secure Mail ADS**. Provide a user email ID. This will be used to test the autodiscovery of the Microsoft Exchange Server in your XenMobile environment. It will detect if there are any issues related to Secure Mail Auto Discovery.

    c. **ShareFile SSO**. If selected, XenMobile Analyzer will test if the ShareFile DNS resolution happens successfully and if ShareFile single sign-on (SSO) works with the provided user credentials.

7. Click **Continue**.

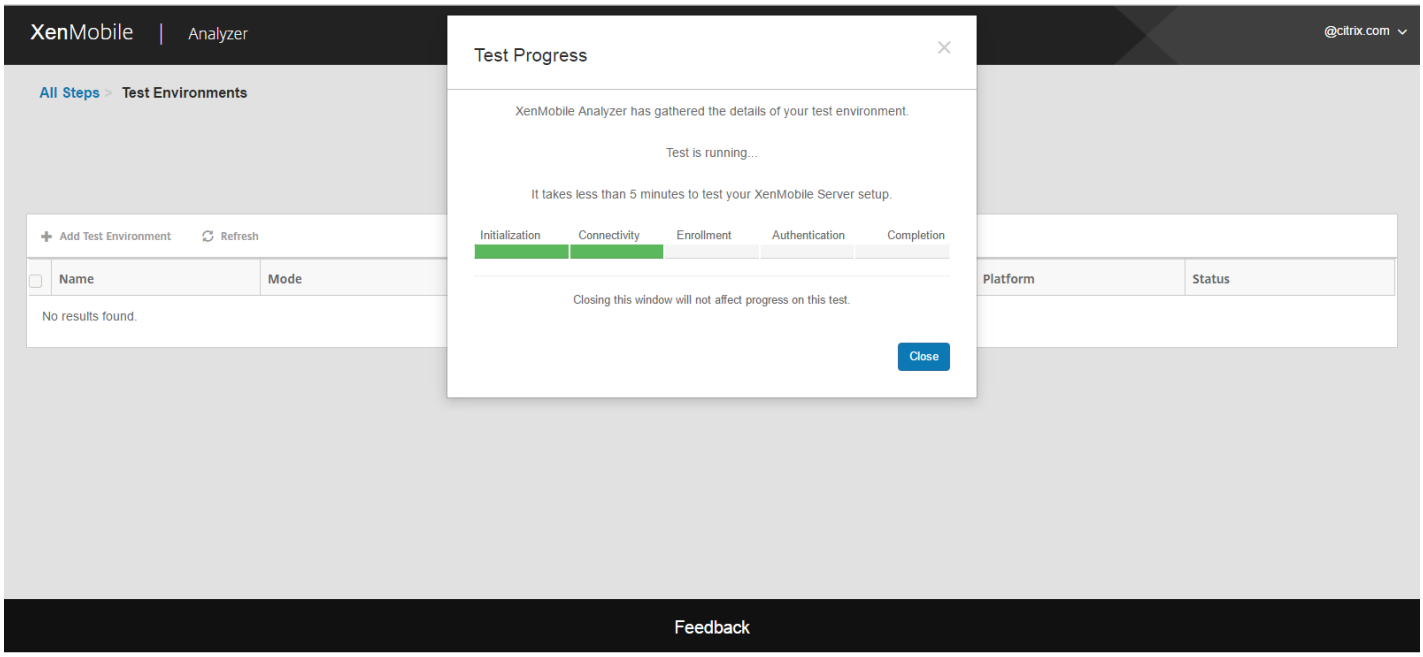


8. Depending on your server setup, you may see different fields available to enter User Credentials. The possible fields are **Username** alone, **Username** and **Password**, or **Username**, **Password**, and **Enrollment PIN.**

9. After entering this information, click **Save & Run** to start the tests.

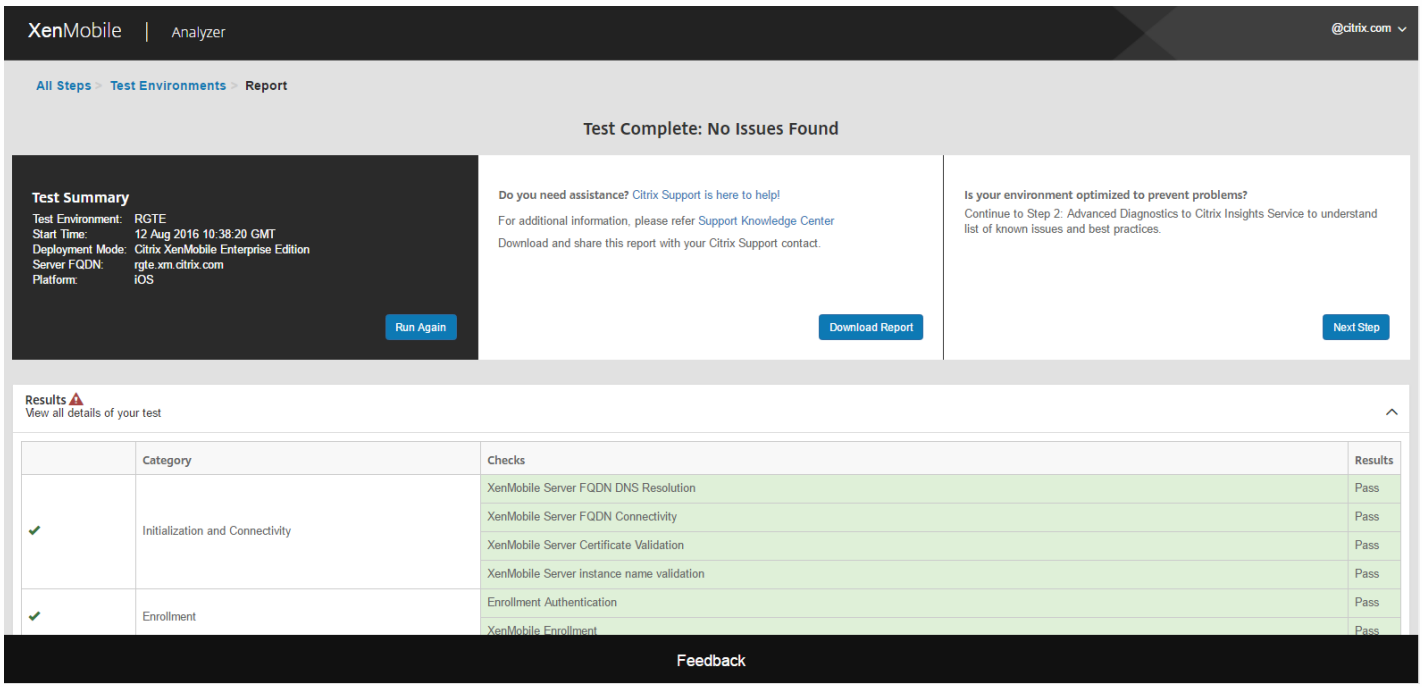
A progress notification appears. You can leave the progress dialog box open or close the dialog box and the tests will continue to run.

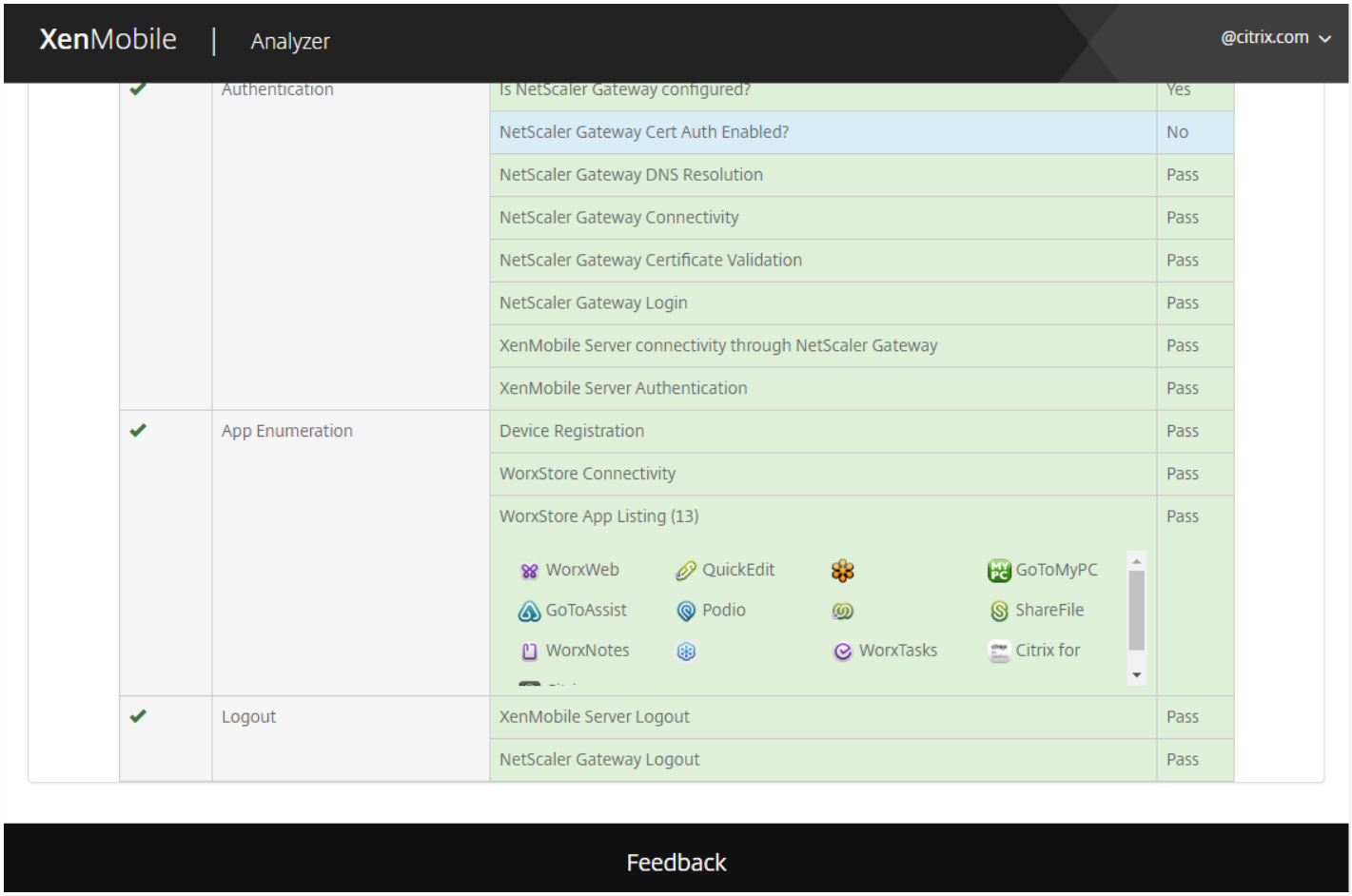
Tests that have passed appear in green. Tests that fail appear as red.



8. At any point after closing the progress dialog box, you can return to the **Test Environments List** page and then click the **View Report** icon to see test results.

The **Results** page displays Test Details, Recommendations, and Results.





In the above screenshot, please note that WorxWeb is now called Secure Web, WorxNotes is Secure Notes, WorxTasks is Secure Tasks, and WorxStore is XenMobile Store.

If any recommendations have Citrix Knowledge Base articles associated with them, the articles are listed on this page.

9. Click the **Results** tab to display the individual Category and Tests that the tool performed, with their results.

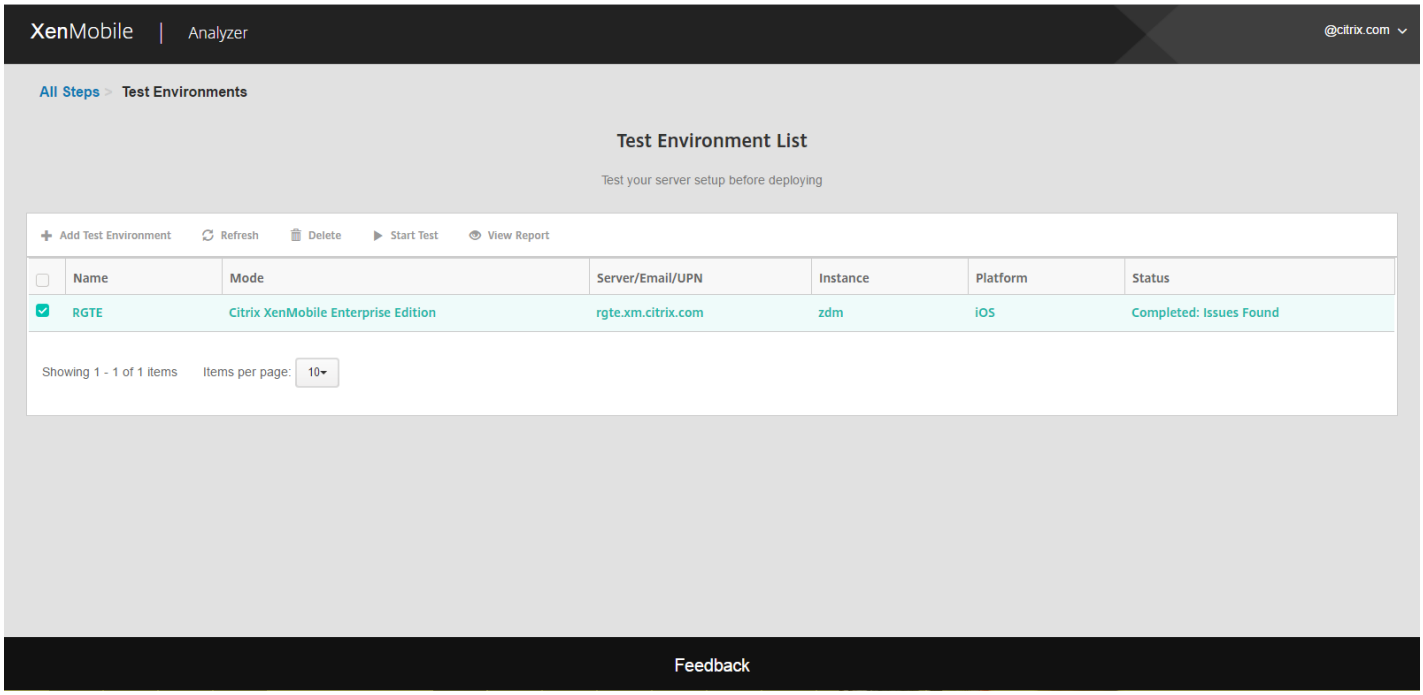
    a. To download the report, click **Download Report**.

    b. To return to the list of test environments, click **Test Environments**.

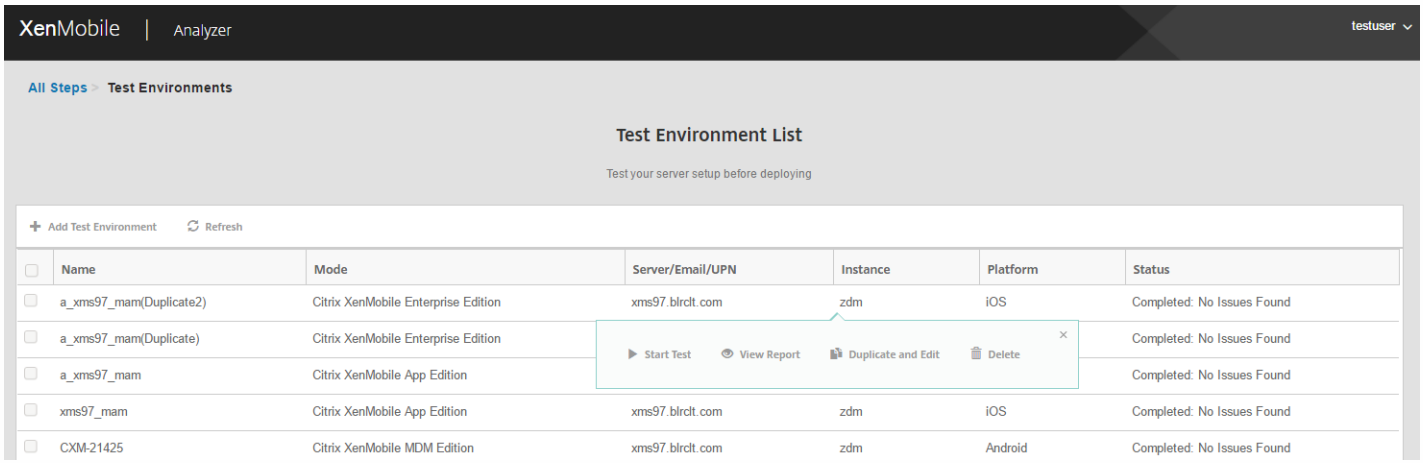
    c. To rerun the same test, click **Run Again**.

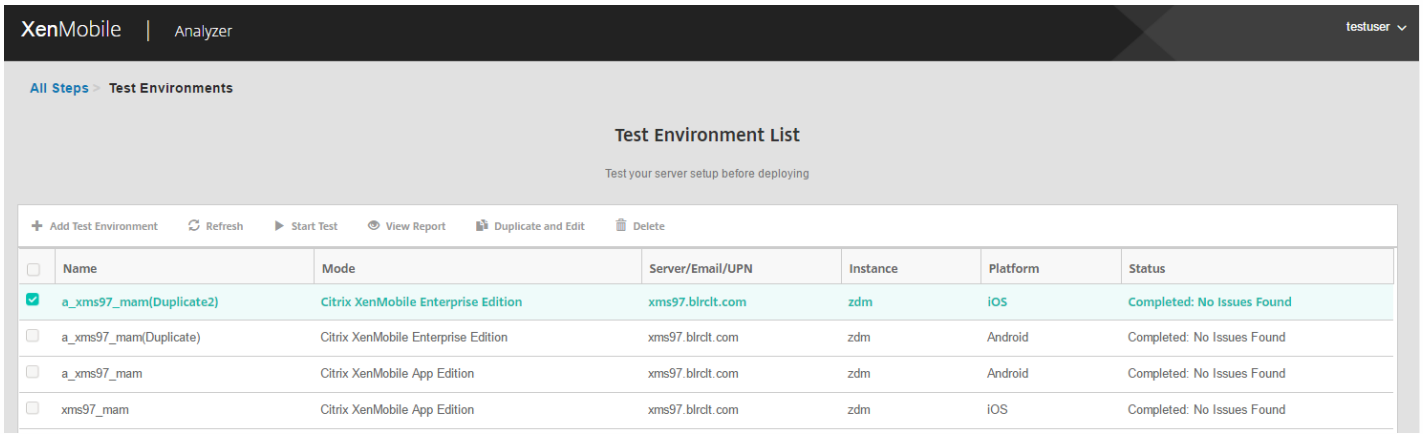
    d. If you want to re-run another test, go back to **Test Environments**, select the test, and click **Start Test**.

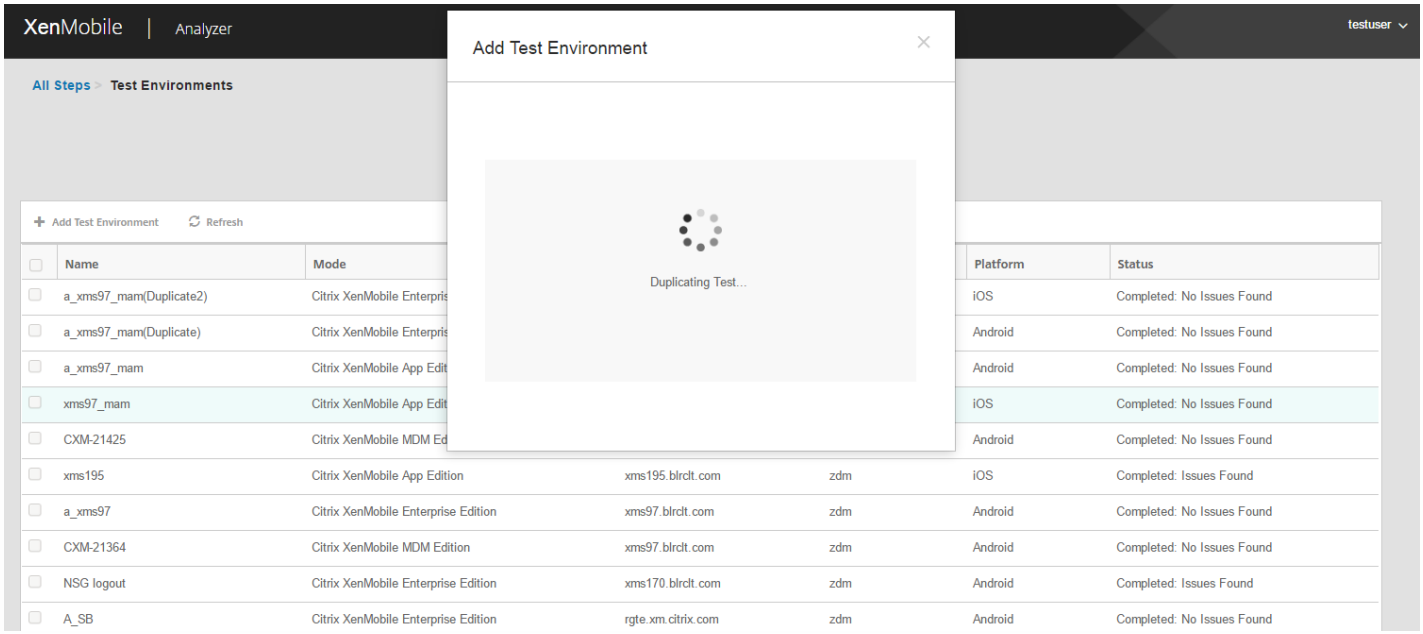
    e. To go to the next step of XenMobile Analyzer, click **Next Step**.

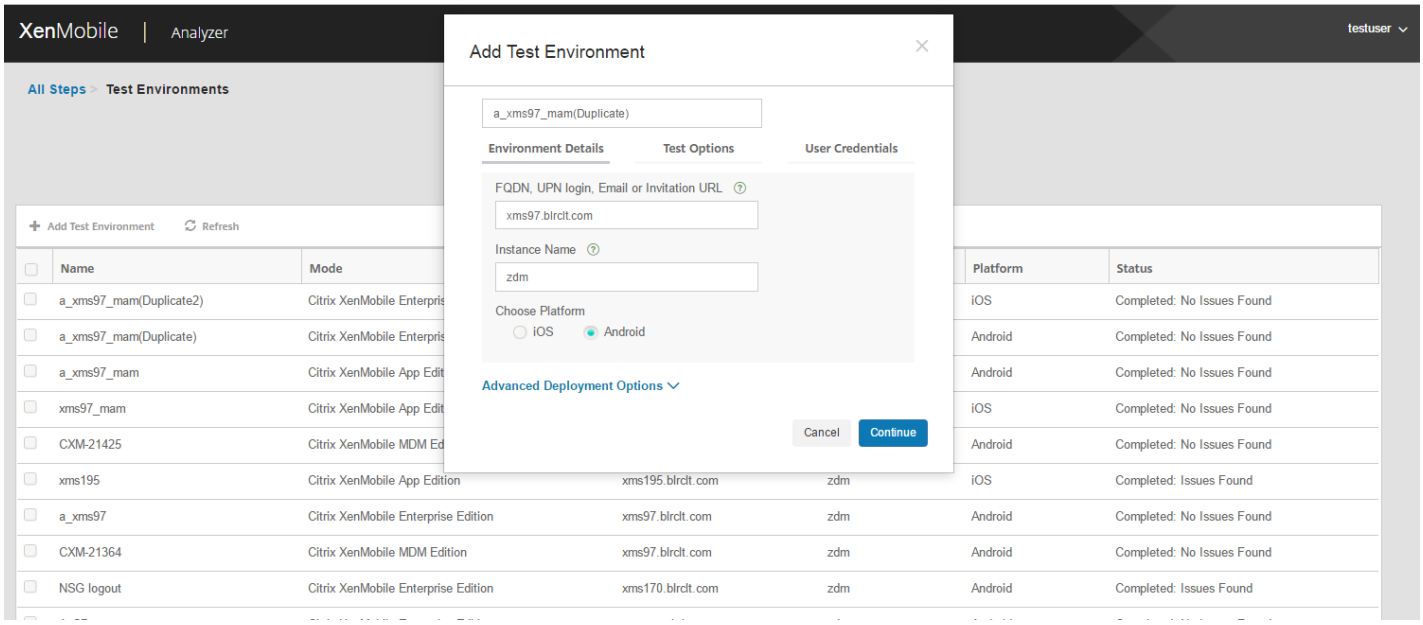


10. From the Test Environments page, you can copy and edit tests. To do so, select a test, and then click **Duplicate and Edit**. A copy of the selected test will be created and the Add Test Environment dialog will open, allowing you to modify the new test.









Performing XenMobile Analyzer Steps 2 Through 5

You interact with the Environment Check step of the XenMobile Analyzer directly to perform tests, whereas Steps 2 through 5 are informative. Each of these steps provides information concerning other support tools you can use to ensure that your XenMobile environment is set up correctly.

- **Step 2 - Advanced Diagnostics**: This step 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.

- **Step 3** - **Secure Mail Readiness:** This step 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.
- **Step 4** - **Server Connectivity Checks:** This step provides you with instructions for checking your connections to XenMobile, Authentication, and ShareFile servers.
- **Step 5** - **Contact Citrix Support**: If all else fails, you can create a support ticket with Citrix Support.

Known Issues

The following issues are known concerning XenMobile Analyzer:

- The number of apps listed might vary based on the client if the Platform Restriction Policy is set on XenMobile Server.
- When performing the Secure Web Intranet Connectivity checks, entering 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.
- For PIN based authentication modes, if you select the Secure Mail ADS test, you are prompted for a password to perform the test. The password is not for enrollment or authentication.

Fixed Issues

The following issues with XenMobile Analyzer have been fixed:

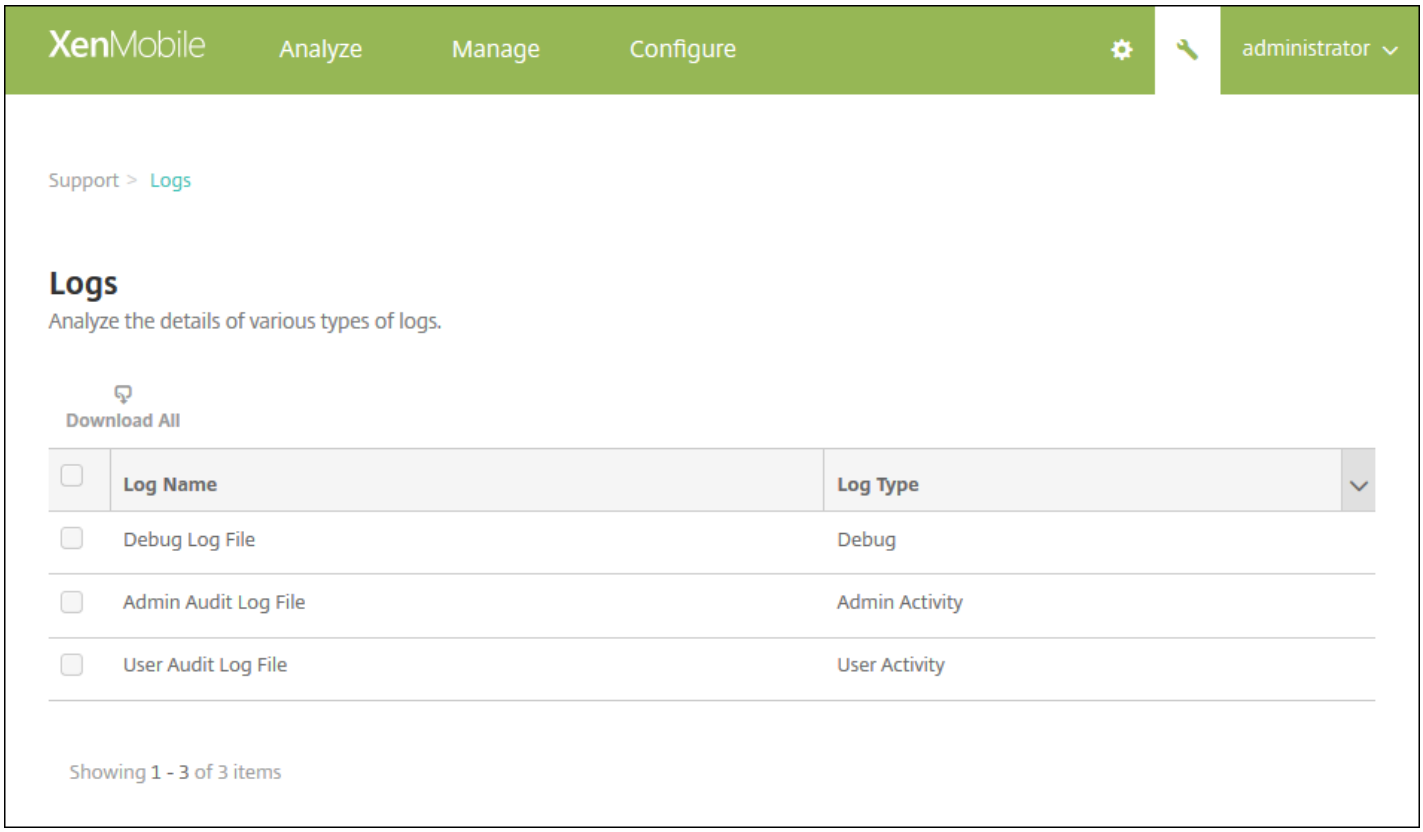
- When performing a check using enrollment invitation, the test passes but the enrollment invitation is not redeemed.

View and analyze log files in XenMobile

Dec 21, 2016

1. In the XenMobile console, click the wrench icon in the upper-right corner of the console. The **Support** page opens.

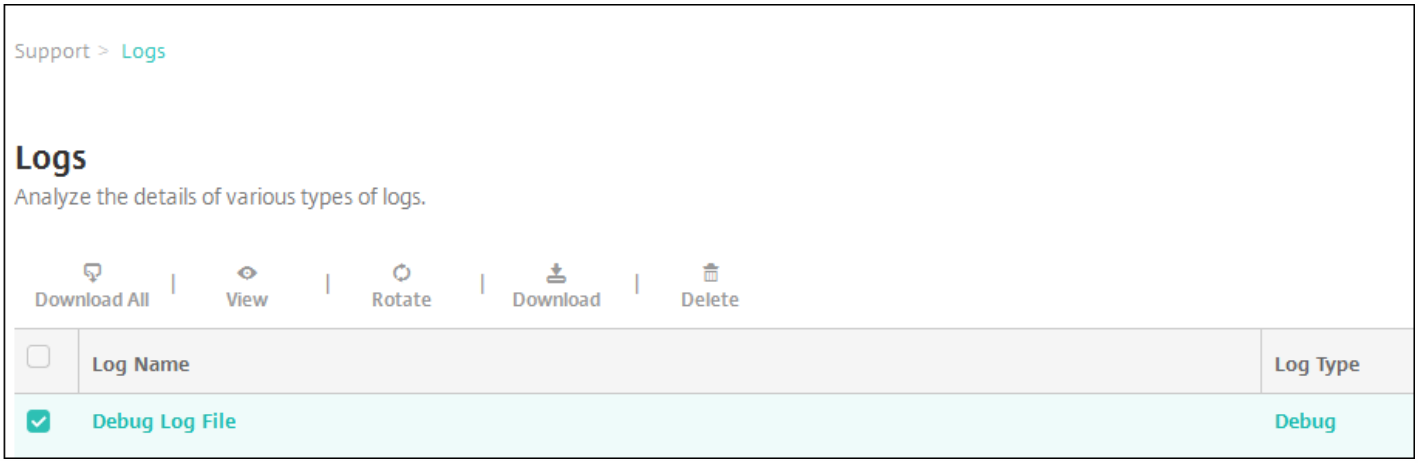
2. Under **Log Operations**, click **Logs**. The **Logs** page appears. Individual logs appear in a table.



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.

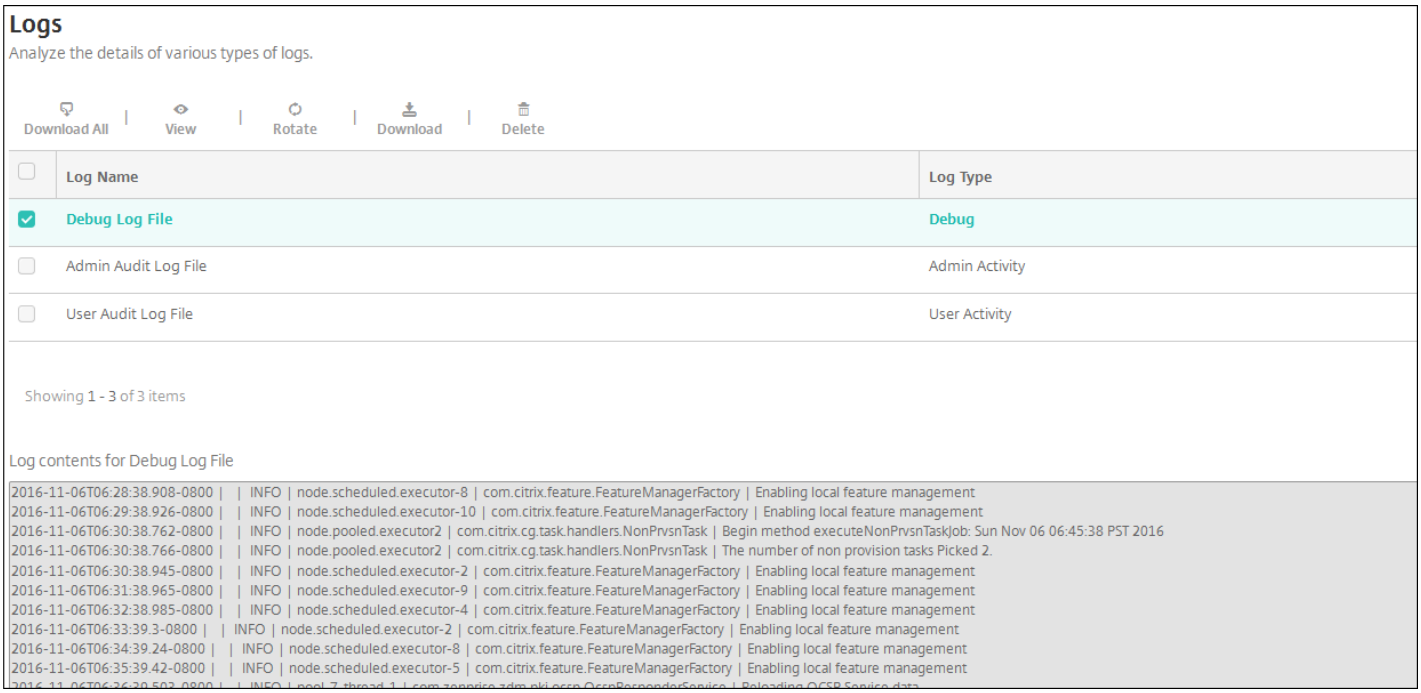


Note:

- 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.



REST APIs

Oct 19, 2016

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 REST API Reference PDF. This article doesn't include the full set of APIs.

Permissions needed to access the REST API

You need one of the following permissions to access the REST API:

- Public API access permission set as part of role-based access configuration (for more 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.

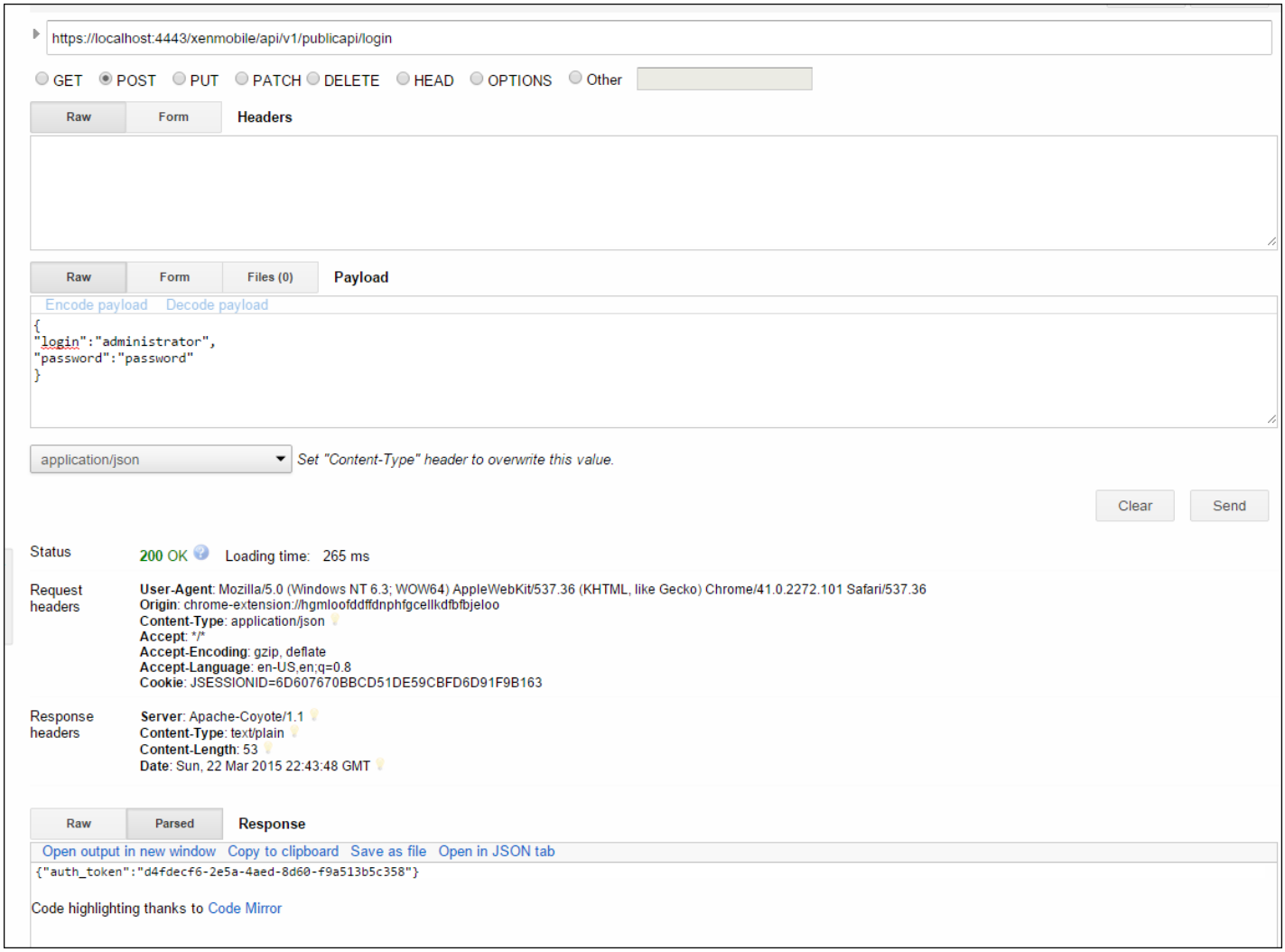
Login

URL: https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login

Request: { "login":"administrator", "password":"password" }

Method type: POST

Content type: application/json



SOAP APIs

Nov 08, 2016

Citrix no longer supports the SOAP web services APIs. Please use the REST APIs instead. For more information, see REST APIs.

XenMobile Mail Manager 10.x

Oct 21, 2016

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.
- Provides the ability for XenMobile to access EAS device partnership information provided by Exchange.
- Provides the ability for XenMobile to perform an EAS Wipe on a mobile device.
- Provides 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.

What's New in XenMobile Mail Manager 10.1

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.

Fixed Issues

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]

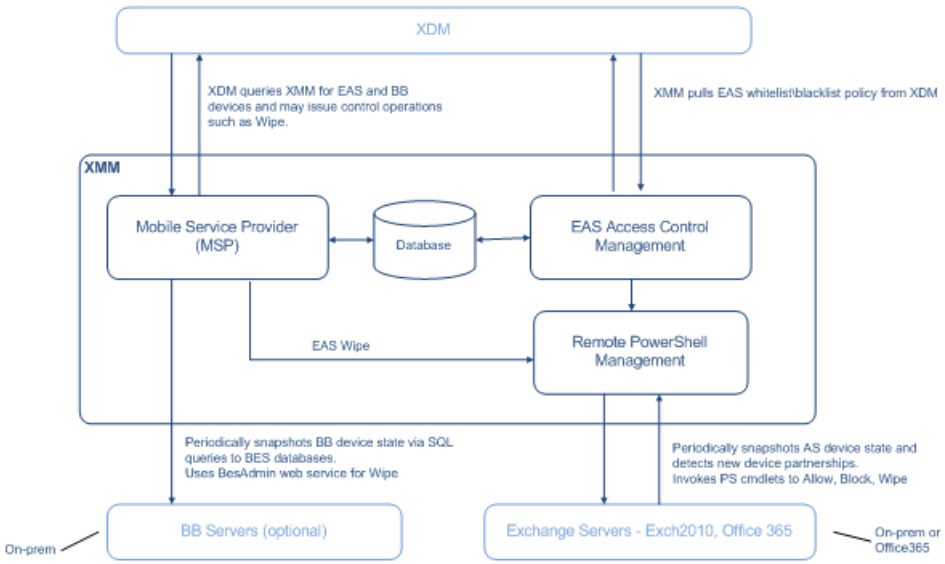
In support scenarios where pipelining is disabled (the Disable Pipelining option is selected in the Configuration window of the XenMobile Mail Manager console), data for deep snapshots is no longer collected regardless of whether the environment was configured for deep or shallow snapshots. Now data 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]

Architecture

Oct 05, 2016

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.



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 Provider. 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.

System requirements and prerequisites

Jan 06, 2017

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

XenMobile Mail Manager Prerequisites

- Windows Management Framework must be installed.
  - PowerShell V5, V4, and V3
- The PowerShell execution policy must be set to RemoteSigned via Set-ExecutionPolicy RemoteSigned.
- TCP port 80 must be open between the computer running 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.

Requirements for Office 365 Exchange

- **Permissions**. The credentials specified in the Exchange Configuration UI must be able to connect to Office 365 and be given full access to execute the following Exchange-specific PowerShell cmdlets:
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **Privileges**. The supplied credentials must have been granted the right to connect to the Office 365 server via the remote Shell. By default, Office 365 online administrator has the requisite privileges.
- **Throttling policies**. Exchange has many throttling policies. One of the policies controls how many concurrent PowerShell connections are allowed per user. The default number of simultaneous connections allowed for a user is three on Office 365. When the connection limit is reached, 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.

Install and configure

Oct 05, 2016

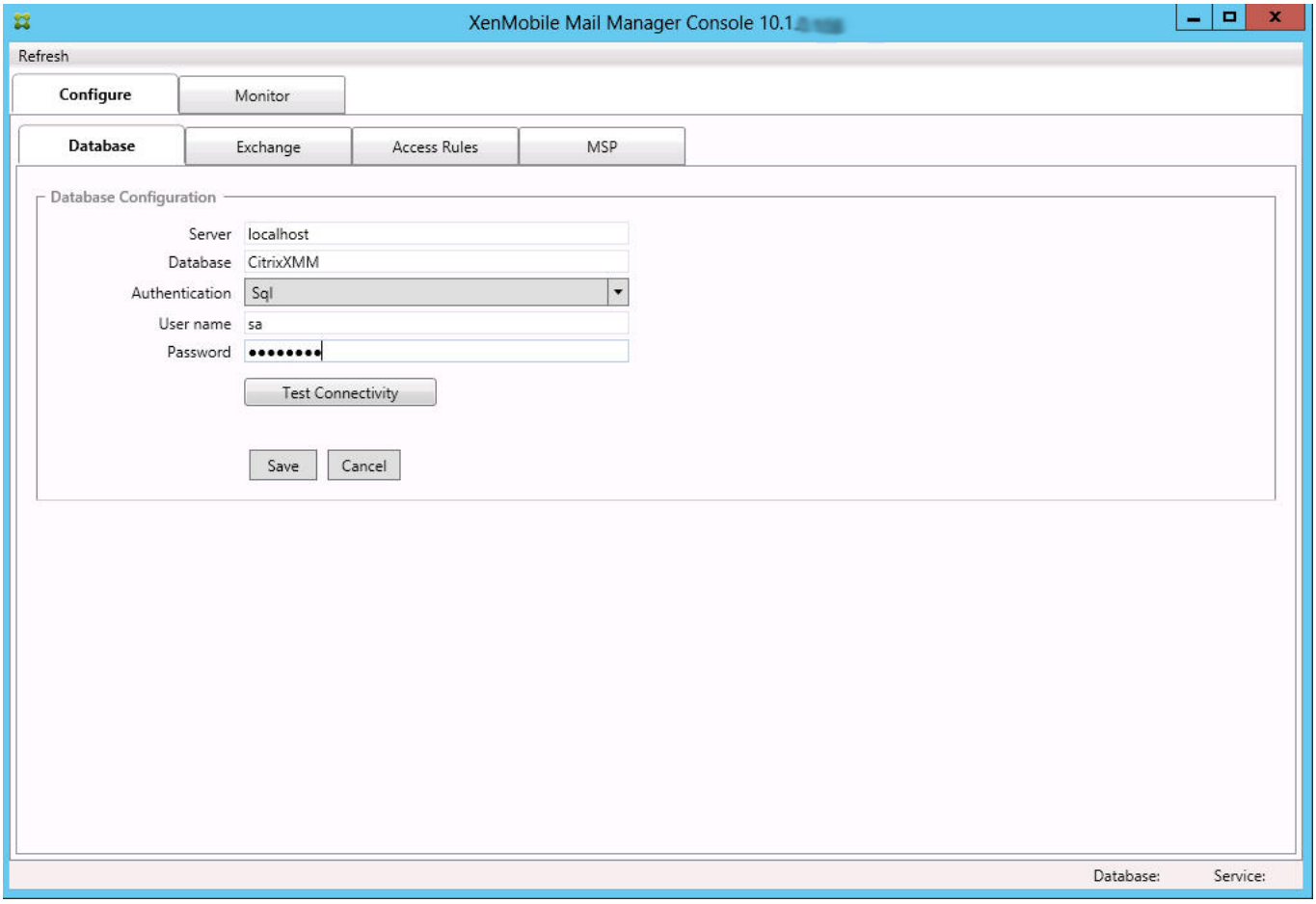
1. Click the XmmSetup.msi file and then follow the prompts in the installer to install XenMobile Mail Manager.

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**.

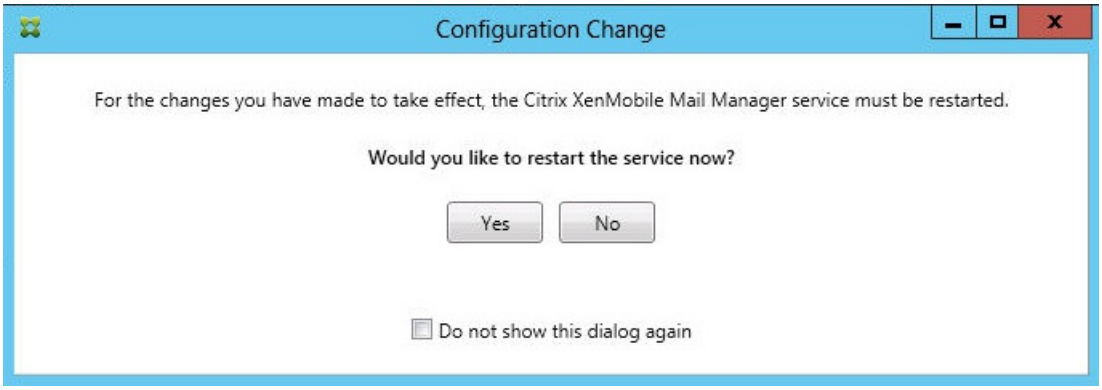
3. Configure the following database properties:
    1. Select the **Configure** > **Database** tab.
    2. Enter the name of the SQL Server (defaults to localhost).
    3. Keep the database as the default CitrixXmm.
    4. Select one of the following authentication modes used for SQL:
        - **Sql**. 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.

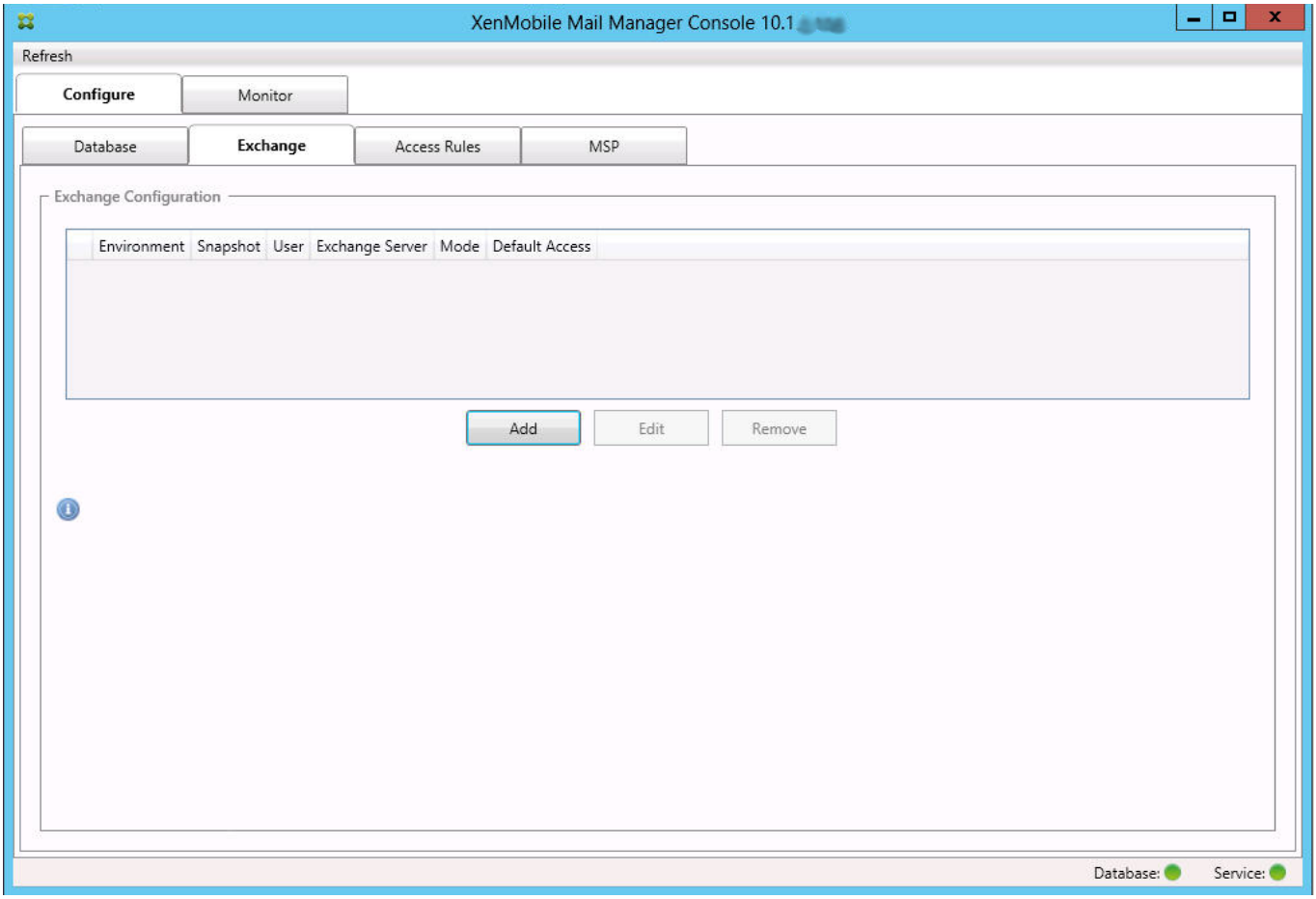
5. Click **Test Connectivity** to check that a connection can be made to the SQL Server and then click **Save**.



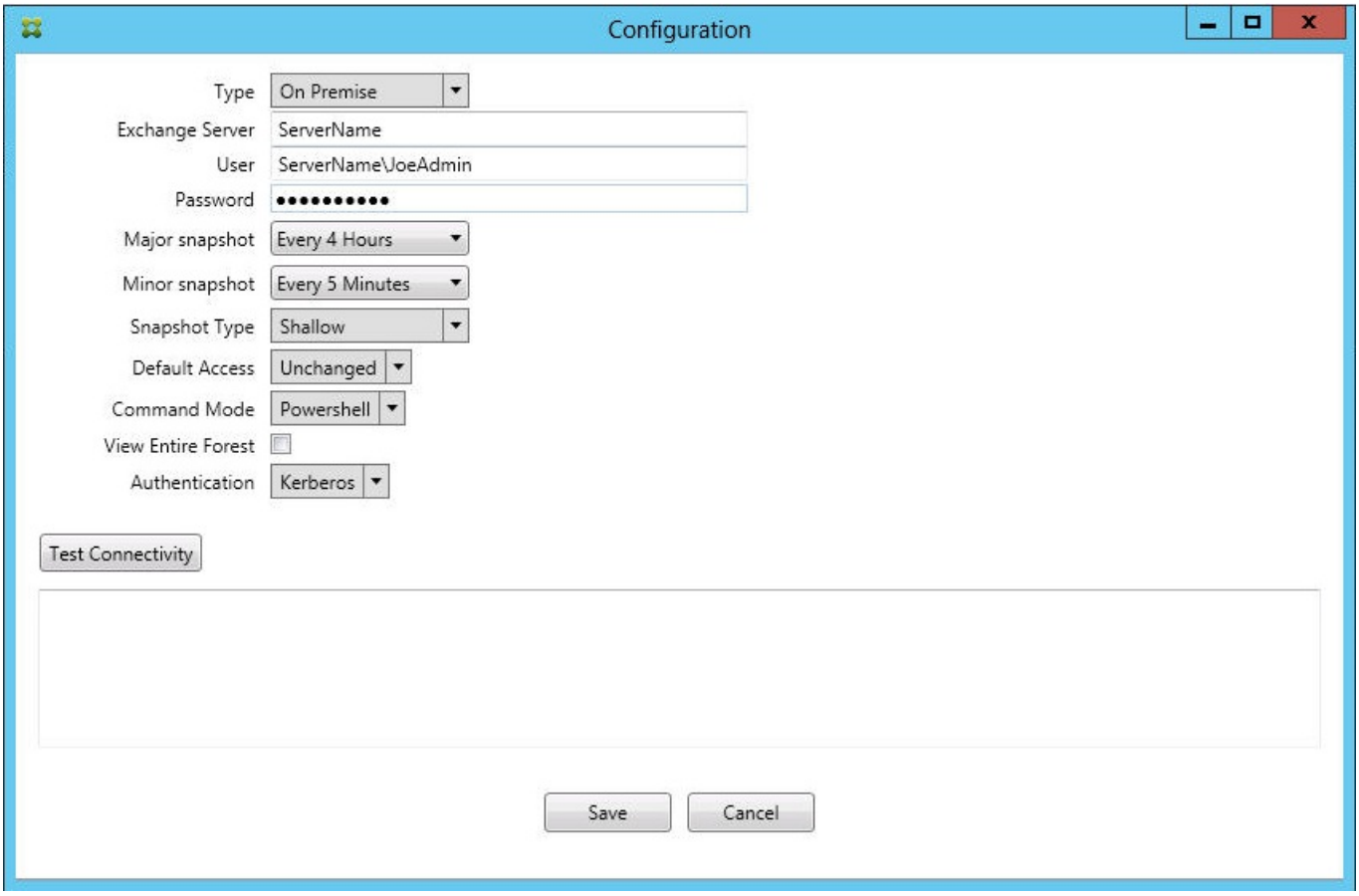
4. A message prompts you to restart the service. Click **Yes**.



5. Configure one or more Exchange Servers:
   1. 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.
   2. Select the **Configure > Exchange tab**.



3. Click **Add**.
4. Select the type of Exchange Server environment: **On Premise** or **Office 365**.

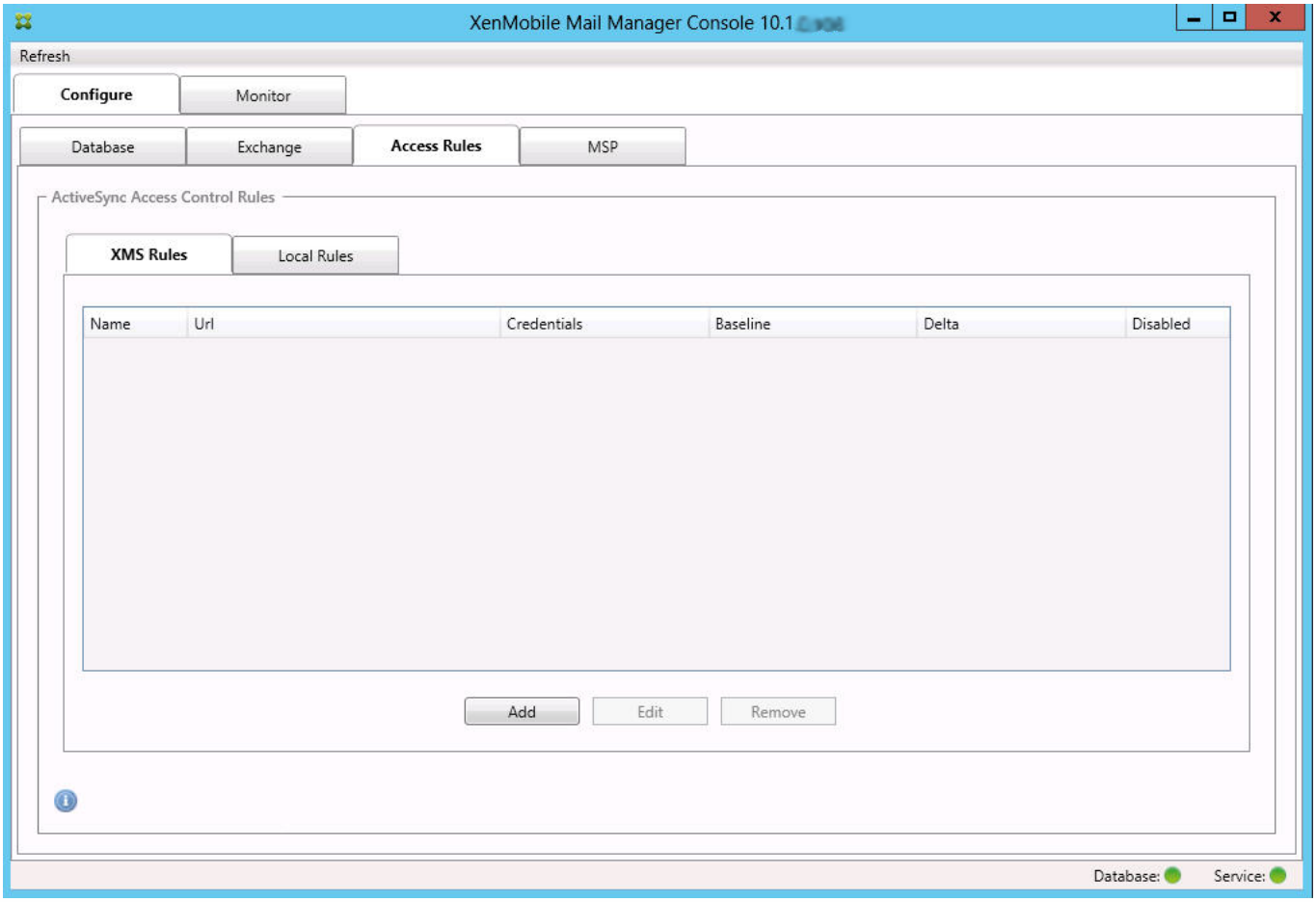


5. If you select **On Premise**, enter the name of the Exchange Server that will be used for Remote PowerShell commands.
6. Enter the user name of a Windows identity that has appropriate rights on the Exchange Server as specified within the Requirements section.
7. Enter the **Password** for the user.
8. Select the schedule for running Major snapshots. A major snapshot detects every Exchange ActiveSync partnership.
9. Select the schedule for running Minor snapshots. A minor snapshot detects newly created Exchange ActiveSync partnerships.
10. 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.
11. 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.
12. 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.
13. Select **View Entire Forest** to configure XenMobile Mail Manager to view the entire Active Directory forest in the Exchange environment.
14. 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

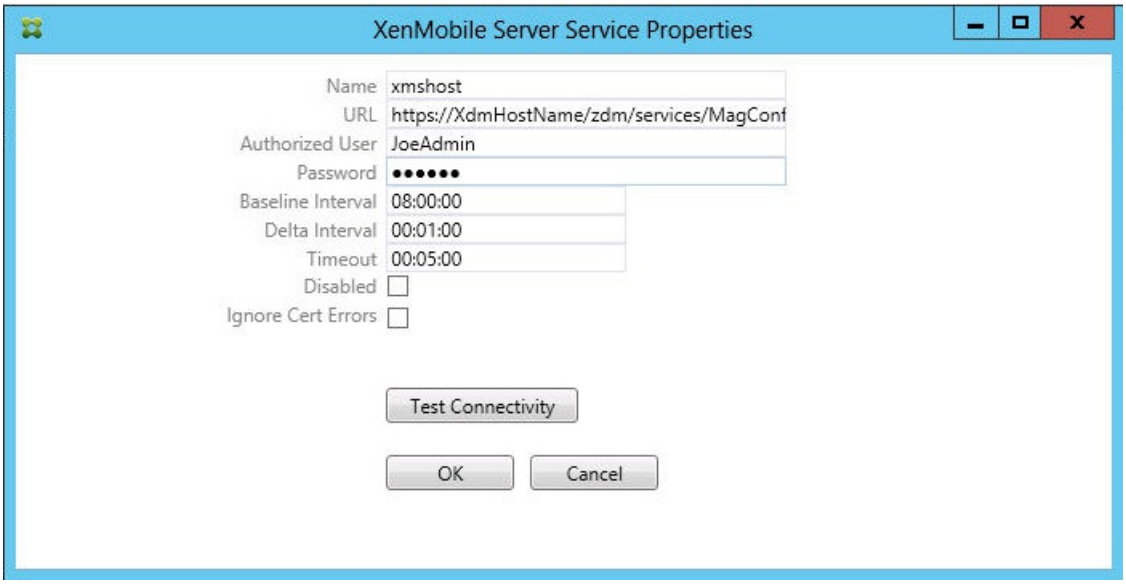
not a member of the domain in which the Exchange server resides.

15. Click **Test Connectivity** to check that a connection can be made to the Exchange Server and then click **Save**.
16. A message prompts you to restart the service. Click **Yes**.

6. Configure the access rules:
    1. Select the **Configure** > **Access Rules** tab.
    2. Click the **XDM Rules** tab.

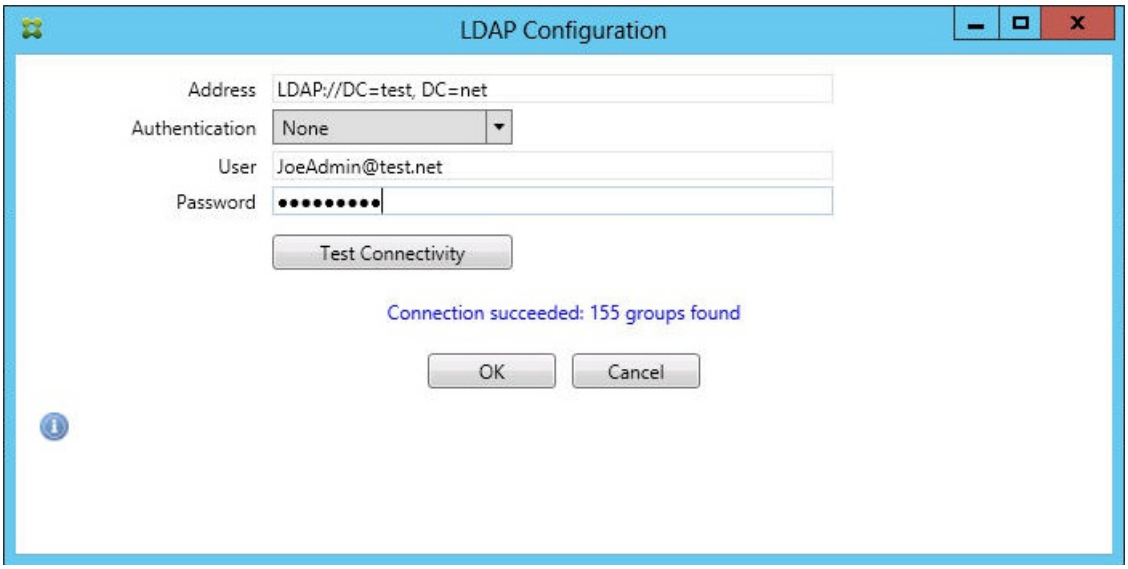


3. Click **Add**.



4. Enter a name for the XenMobile server rules, such as XdmHost.
5. Modify the URL string to refer to the XenMobile server; for example, if the server name is XdmHost, enter http://XdmHostName/zdm/services/MagConfigService.
6. Enter an authorized user on the server.
7. Enter the password of the user.
8. Keep the default values for the **Baseline Interval**, **Delta Interval**, and **Timeout values**.
9. Click **Test Connectivity** to check the connection to the server.
   Note: If the Disabled check box is checked, the XenMobile Mail Service will not collect policy from the XenMobile server.
10. Click **OK**.

7. Click the **Local Rules** tab.
   1. If you want to construct local rules that operate on Active Directory Groups, click **Configure LDAP** and then configure the LDAP connection properties.

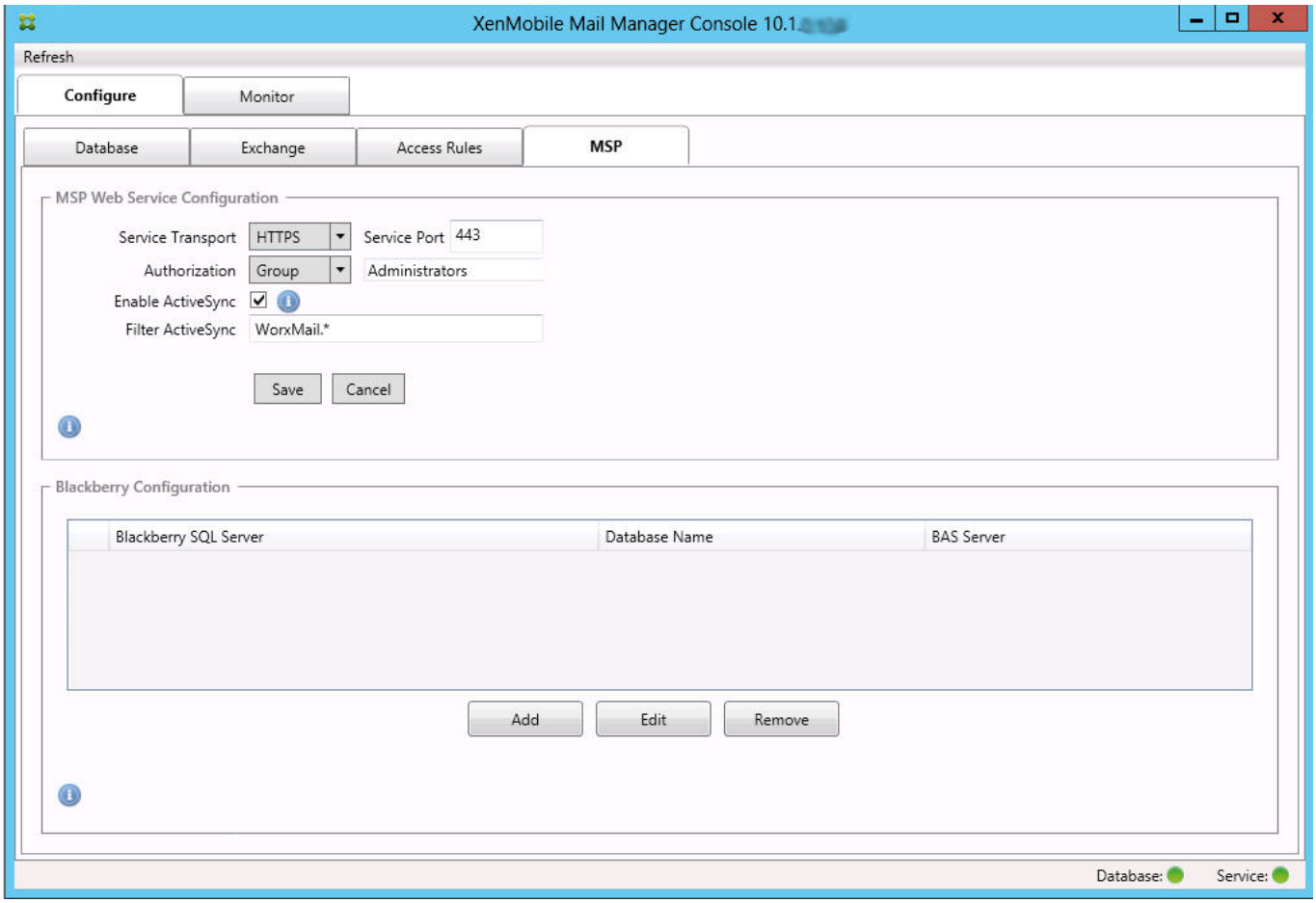


   2. You can add local rules based on **ActiveSync Device ID**, **Device Type**, **AD Grou**p, **User**, or device **UserAgent**. In the list, select the appropriate type. For details, see XenMobile Mail Manager Access Control Rules.
   3. Enter text or text fragments in the text box. Optionally, click 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.
   4. 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.
   5. To perform an analysis of the rules within the rules list to find any potential overrides, conflicts, or supplemental constructs, click **Analyze**.
   6. Click **Save**.

8. Configure the Mobile Service Provider.

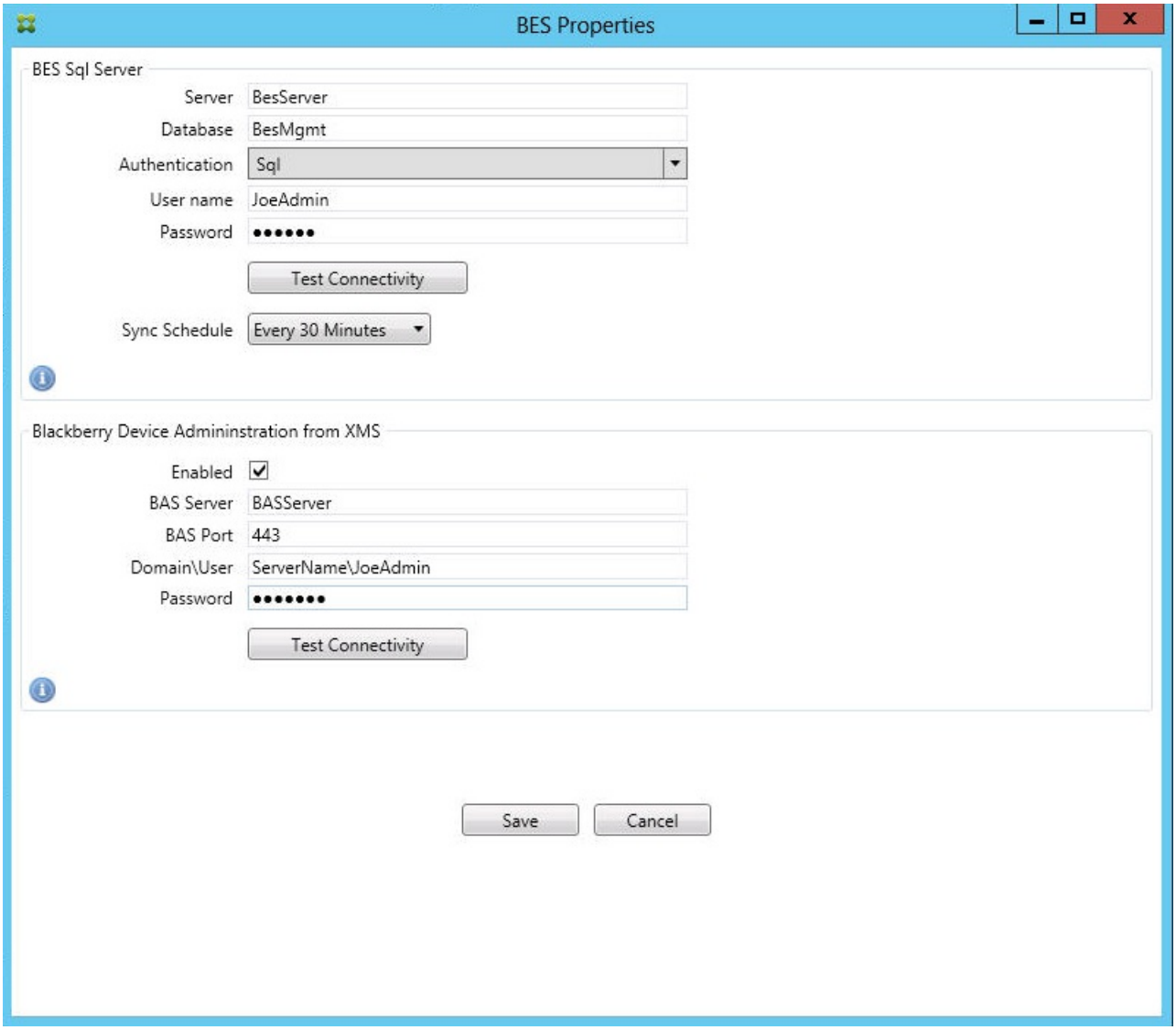
Note: The Mobile Service Provider is optional and is necessary only if XenMobile is also configured to use the Mobile Service Provider interface to query unmanaged devices.

1. Select the **Configur**e > **MSP** tab.



2. Set the Service Transport type as **HTTP** or **HTTPS** for the Mobile Service Provider service.
3. 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.
4. 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.
5. 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.
6. 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.
7. Click **Save**.

9. Optionally, configure one or more BlackBerry Enterprise Server (BES):
   1. Click **Add**.
   2. Enter the server name of the BES SQL Server.



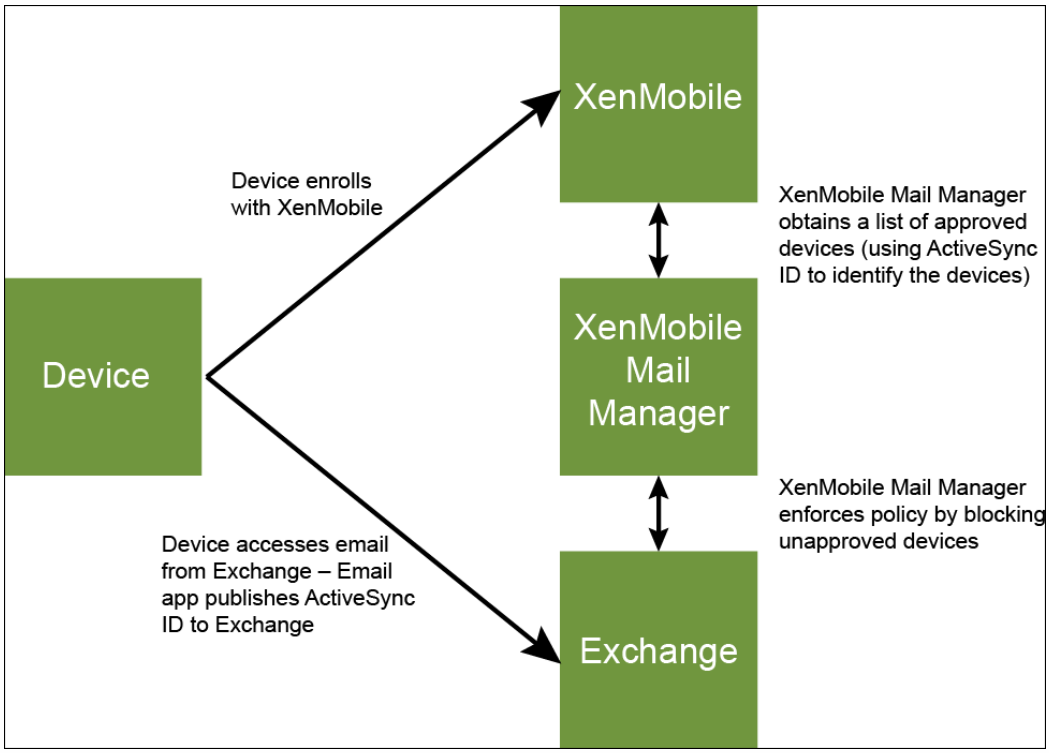
3. Enter the database name of the BES management database.
4. Select the Authentication mode. If you select Windows Integrated authentication, the user account of the XenMobile Mail Manager service is the account that is used to connect to the BES SQL Server.
   Note: If you also choose Windows Integrated for the XenMobile Mail Manager database connection, the Windows account specified here must also be given access to the XenMobile Mail Manager database.
5. If you select **SQL authentication**, enter the user name and password.
6. Set the **Sync Schedule**. This is the schedule used to connect to the BES SQL Server and checks for any device updates.
7. 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.
8. If you want to support remote Wipe and/or ResetPassword of BlackBerry devices from XenMobile, check the **Enabled** check box.
   1. Enter the BES fully qualified domain name (FQDN).
   2. Enter the BES port used for the admin web service.
   3. Enter the fully qualified user and password required by the BES service.
   4. Click **Test Connectivity** to test the connection to the BES.
   5. Click **Save**.

Enforce email policies with ActiveSync IDs

Oct 05, 2016

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:



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.

Access control rules

Jan 23, 2017

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:

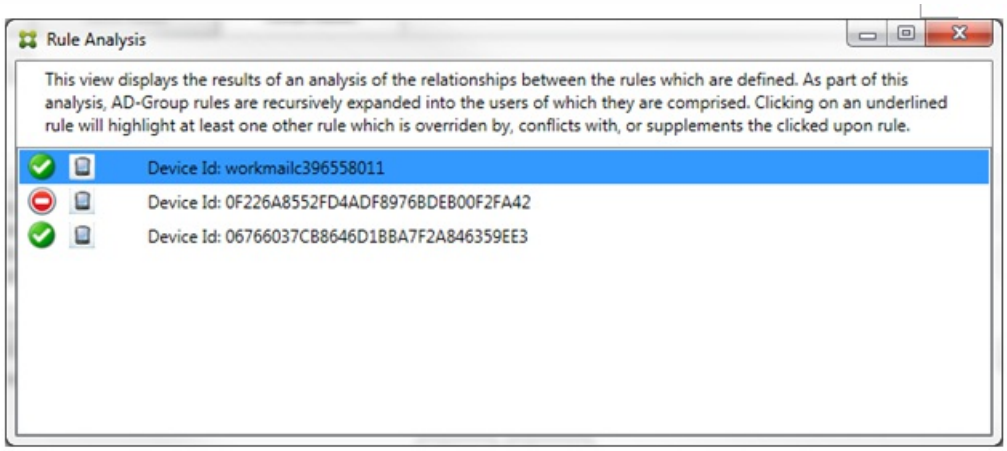
- **Overriding rule**. An override occurs when more than a single rule could apply to the same device. Because rules are evaluated by priority in the list, the later rule instance(s) which might apply might never be evaluated.
- **Conflicting rule**. A conflict occurs when more than a single rule could 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

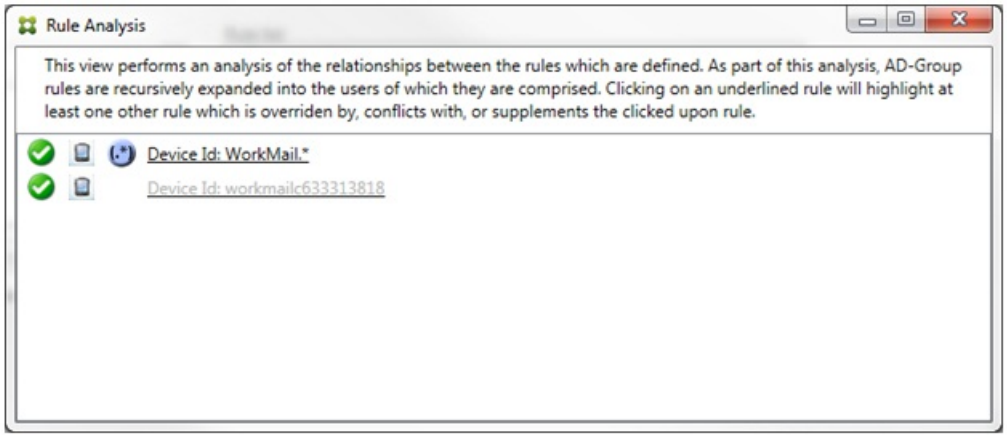
When there are no conflicts, overrides, or supplements, the Rule Analysis dialog box has no underlined entries. Clicking on

any of the items has no impact; for example, normal selected item visuals will occur.

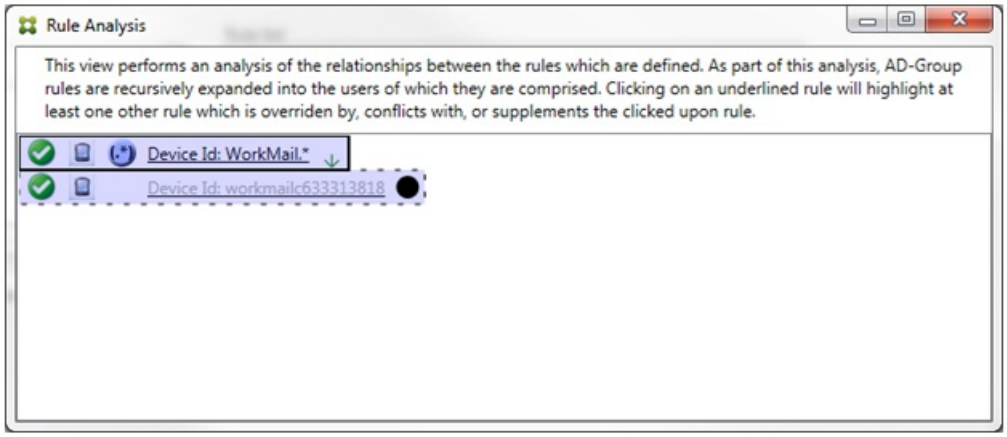
The Rule Analysis window has a check box which, when selected, displays only those rules which are conflicts, overrides, redundancies, or supplements.



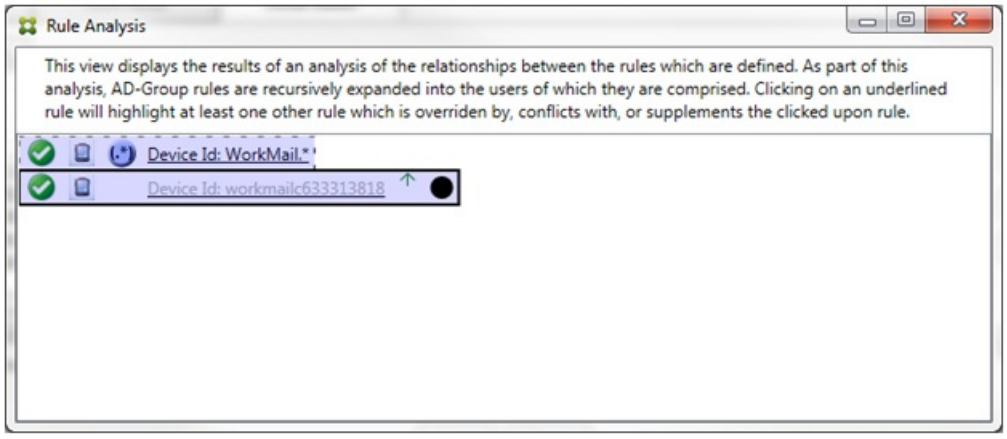
When an override occurs, at least two rules will be underlined: the primary rule and the ancillary rule or rules. At least one ancillary rule will appear in a lighter font to indicate that the rule has been overridden by a higher priority rule. You can click on the overridden rule to find out which rule 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:



When you click the highest-priority rule, the dialog box appears as follows:

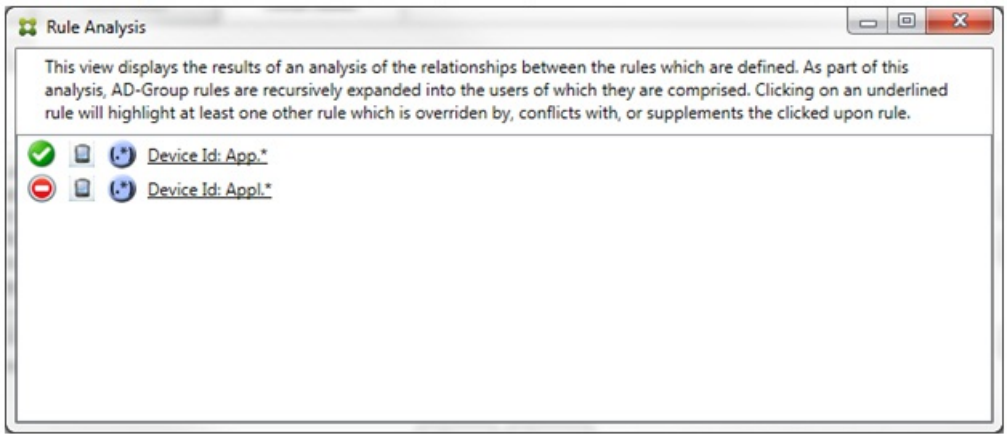


In this example, the regular expression rule WorkMail.* is the primary rule (indicated by the solid border) and the normal rule workmailc633313818 is an ancillary rule (indicated by the dashed border). The black dot next to the ancillary rule is a visual cue that further indicates that the rule is inactive (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:

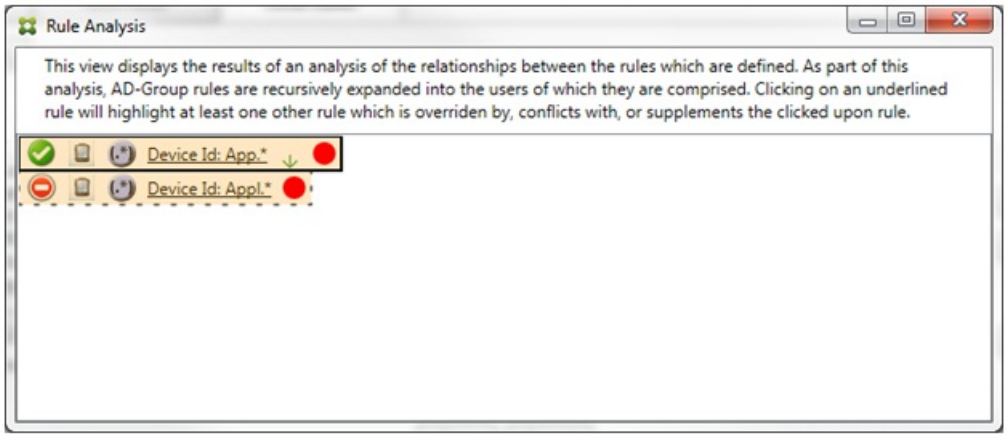


In the preceding example, the regular expression rule WorkMail.* is the ancillary rule (indicated by the dashed border) and the normal rule workmailc633313818 is a primary rule (indicated by the solid border). For this simple example, there's not much difference. For a more complicated example, see the 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:

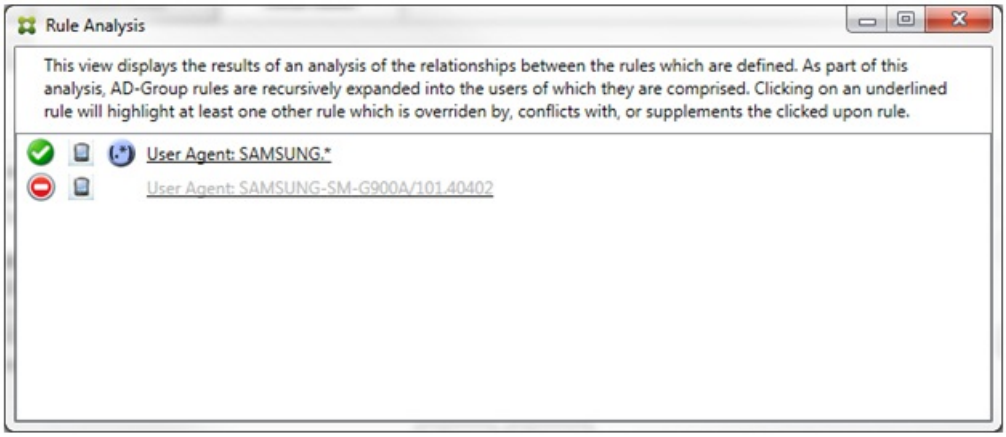


By inspecting the two regular expression rules, it's evident that the first rule allows all devices with a device ID that contains "App" and that the second rule denies all devices with a device ID that contains Appl. In addition, even though the second rule denies all devices with a device ID that contains 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:



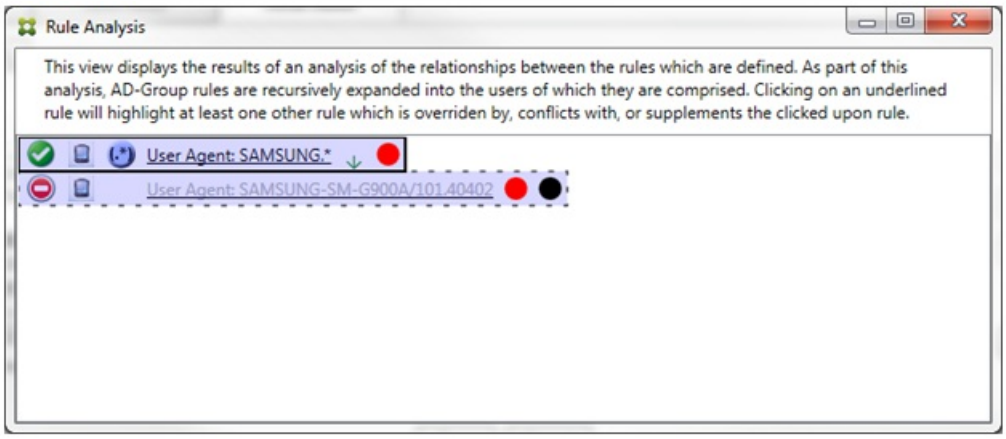
In the preceding scenario, both the primary rule (regular expression rule App.*) and the ancillary rule (regular expression rule Appl.*) are both highlighted in yellow. This is simply a visual warning to alert you to the fact that you have applied more than a single regular expression rule to a single 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.



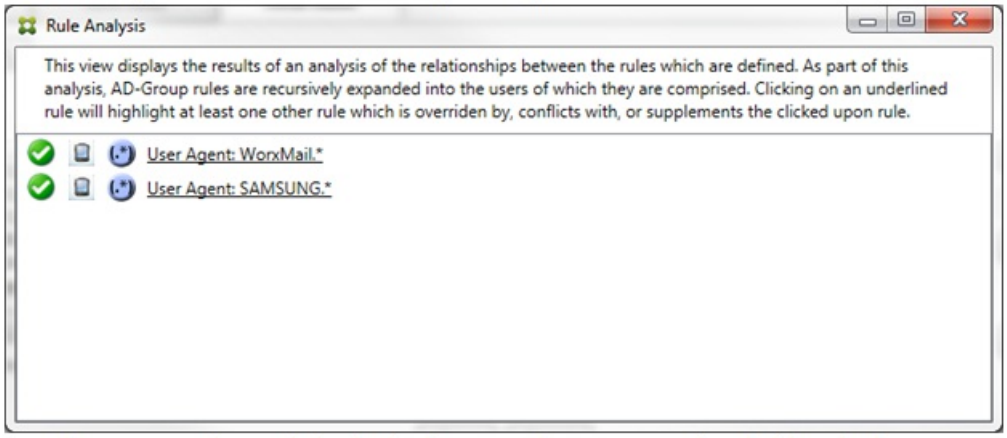
It is easy to see in the preceding example that the first rule (regular expression rule SAMSUNG.*) not only overrides the next rule (normal rule SAMSUNG-SM-G900A/101.40402), but that the two rules differ in their access (primary specifies Allow, ancillary specifies Block). The second rule (normal rule 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:

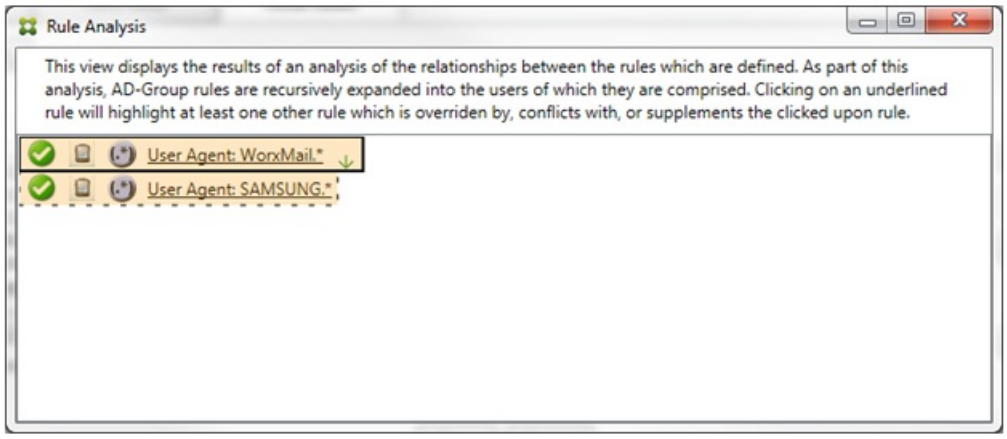


The primary rule (regular expression rule SAMSUNG.*) is followed by a red dot to indicate that its access state conflicts with one or more ancillary rules. The ancillary rule (normal rule SAMSUNG-SM-G900A/101.40402) is followed by a red dot to indicate that its access state conflicts with the primary 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:



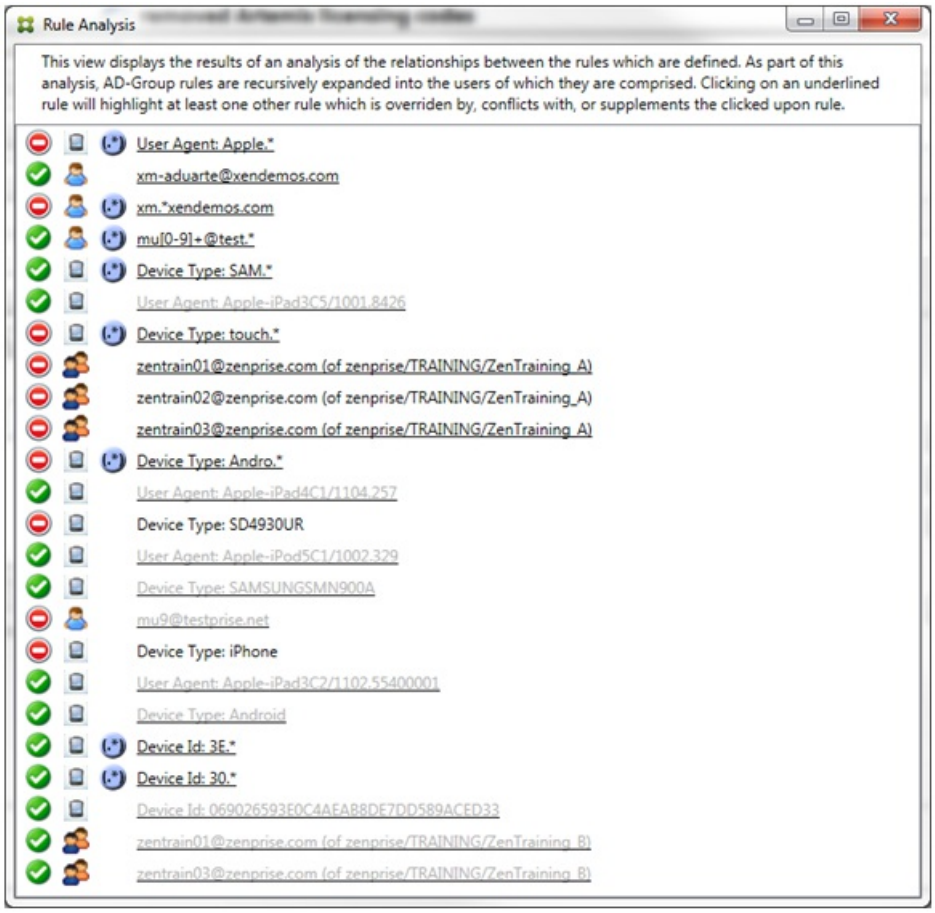
Visual inspection easily reveals that both rules are regular expression rules which have both been applied to the ActiveSync device ID field in XenMobile Mail Manager. After clicking on the first rule, the dialog box looks as follows:



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

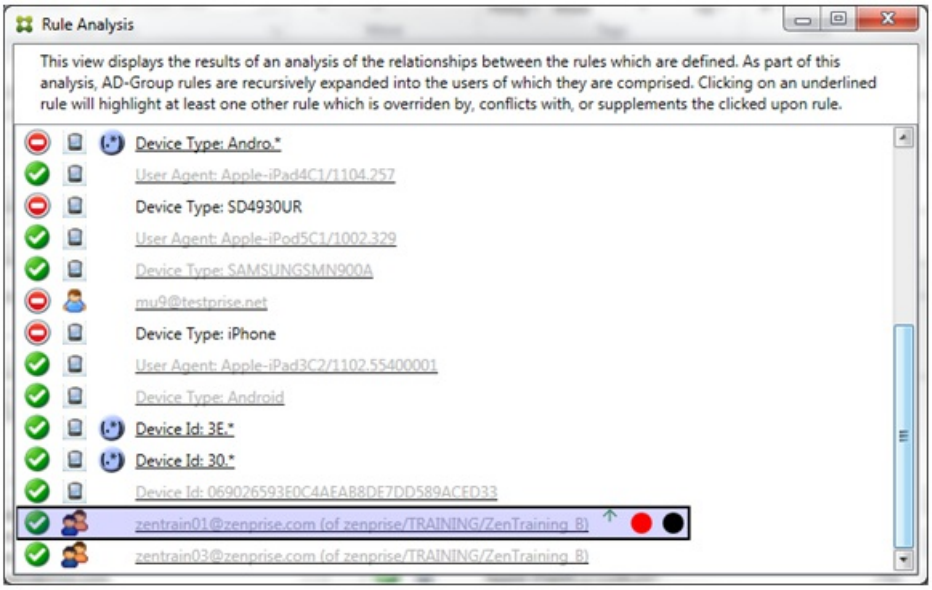
Many potential overrides, conflicts, or supplements can occur, making it impossible to give an example of all possible scenarios. The following example discusses what not to do, while also serving to illustrate the full power of the rule analysis visual construct. Most of the items are underlined in 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.



How to Analyze an Override

To see which rule or rules have overridden a particular rule, you click the rule.

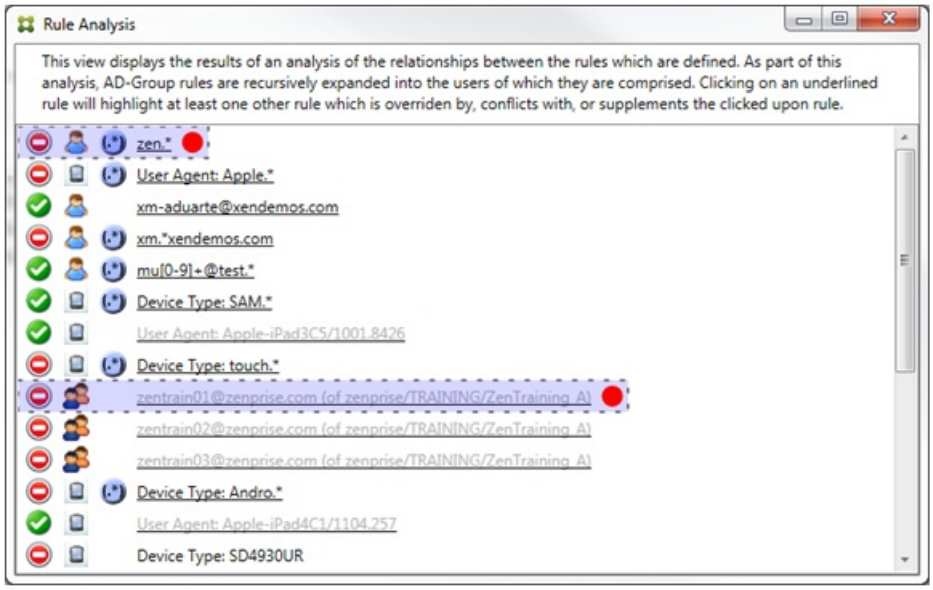
Example 1: This example examines why zentrain01@zenprise.com has been overridden.



The primary rule (AD-Group rule zenprise/TRAINING/ZenTraining B, of which zentrain01@zenprise.com is a member) has the following characteristics:

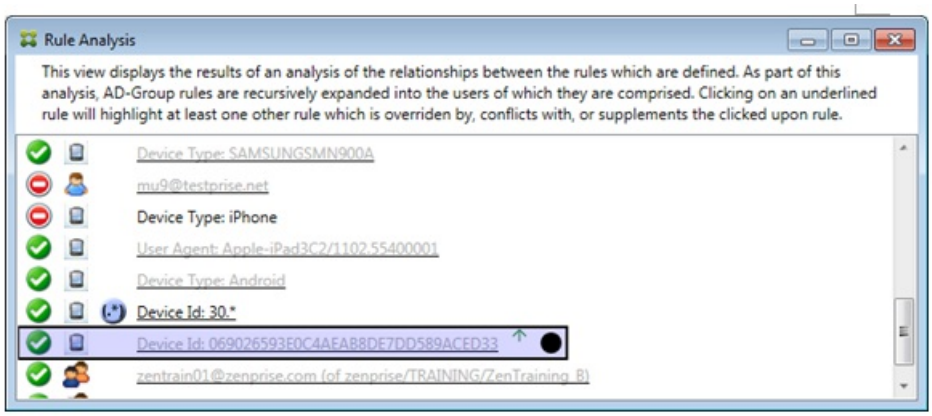
- Is highlighted in blue and has a solid border.
- Has an upwards pointing green arrow (to indicate that the ancillary rule or rules are all to be found above it).
- Is followed by both a red circle and black circle to indicate respectively that one or more ancillary rule conflicts with its access and that the primary rule has been overridden and is hence inactive.

When you scroll up, you see the following:



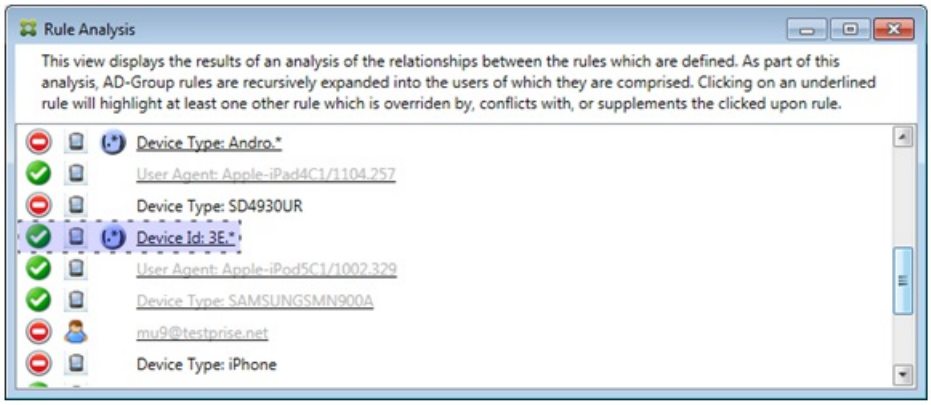
In this case, there are two ancillary rules that override the primary rule: the regular expression rule zen.* and the normal rule zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining A). In the case of the latter ancillary rule, what has occurred is that the Active Directory Group rule ZenTraining A contains the user zentrain01@zenprise.com, and the Active Directory Group rule ZenTraining B also contains the user zentrain01@zenprise.com. Because the ancillary rule has a higher precedence than the primary rule, however, the primary rule has been overridden. The primary rule's access is Allow, and because both of the ancillary rule's access is Block, all are followed with a red circle to further indicate an access conflict.

Example 2: This example shows why the device with an ActiveSync device ID of 069026593E0C4AEAB8DE7DD589ACED33 has been overridden:



The primary rule (normal device ID rule 069026593E0C4AEAB8DE7DD589ACED33) has the following characteristics:

- Is highlighted in blue and has a solid border.
- Has an upwards pointing green arrow (to indicate that the ancillary rule is to be found above it).
- Is followed by a black circle to indicate an ancillary rule has overridden the primary rule and is hence inactive.



In this case, a single ancillary rule overrides the primary rule: the regular expression ActiveSync device ID rule 3E.* Because the regular expression 3E.* would match 069026593E0C4AEAB8DE7DD589ACED33, the primary rule will never be evaluated.

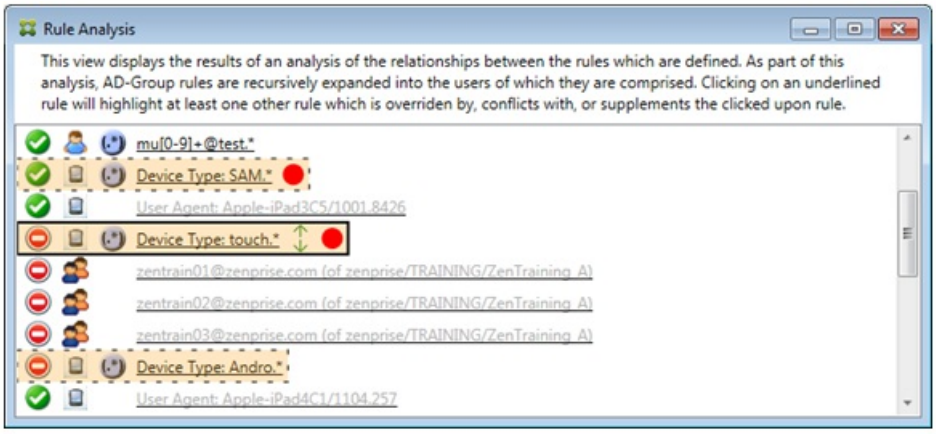
How to Analyze a Supplement and Conflict

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.



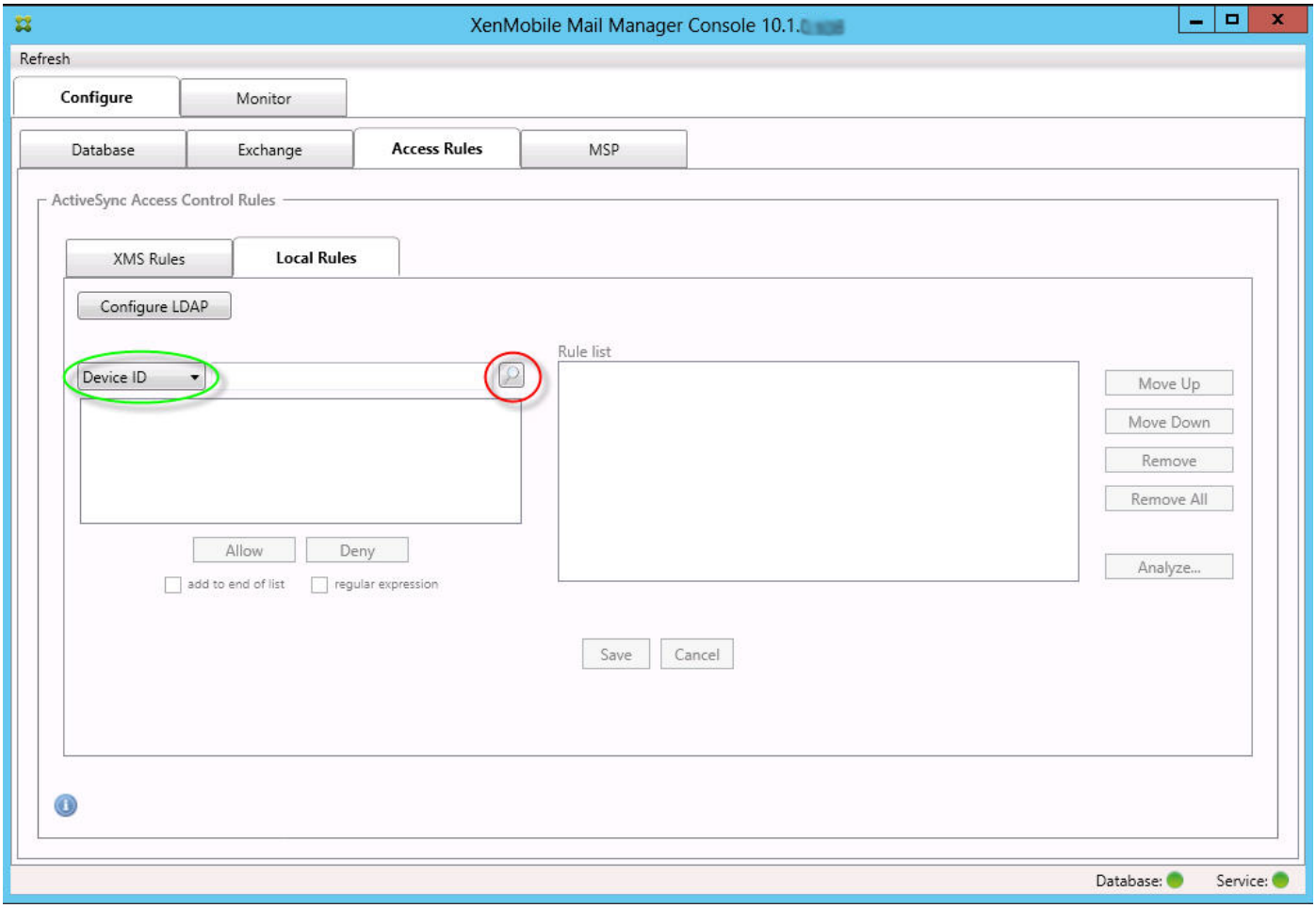
How to Further Analyze the Rules

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.

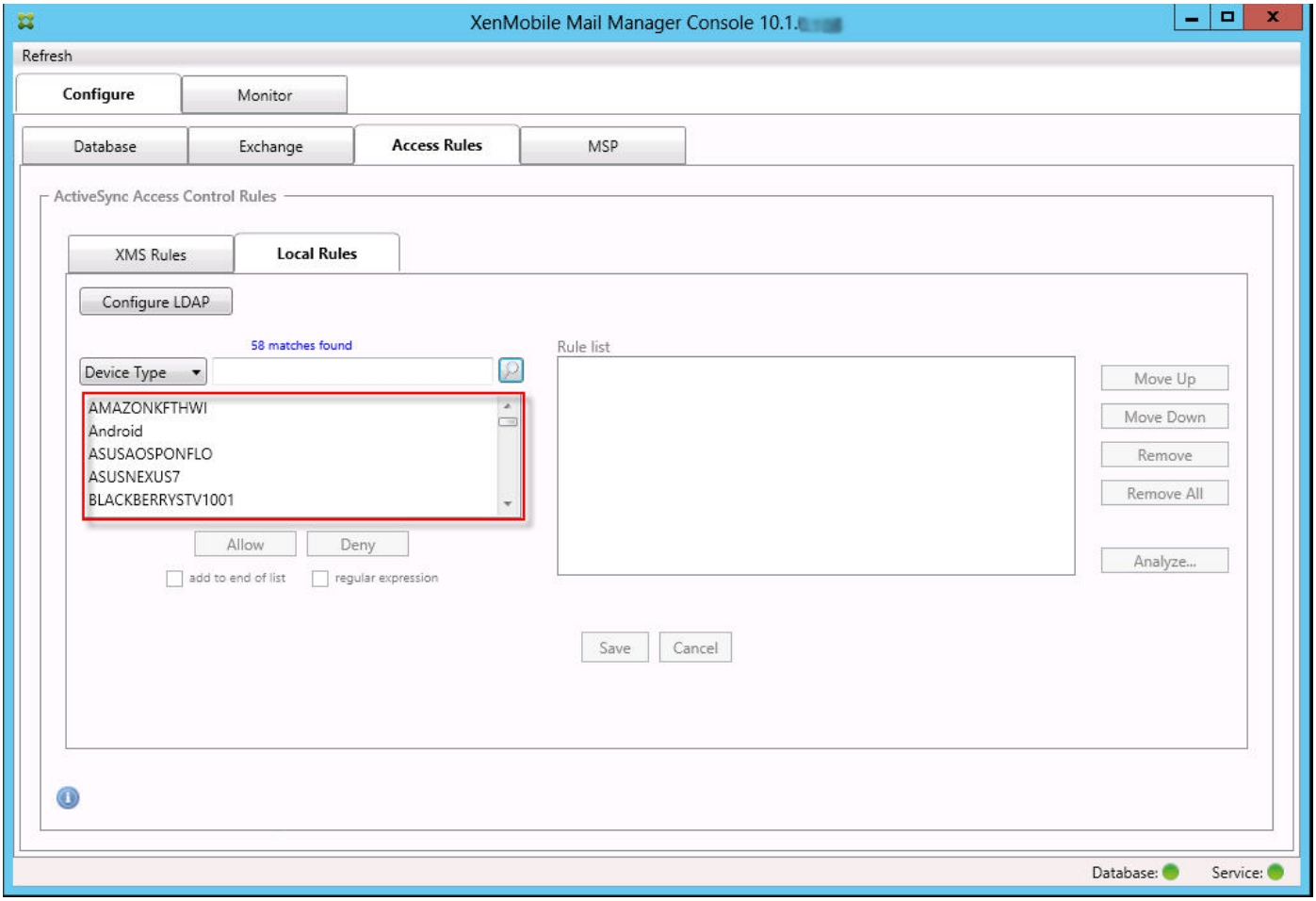
The example shows an overridden rule that is included in the rule relationship. This rule is the normal ActiveSync device type rule Android, which is overridden (indicated by the lightened font and the black circle next to it) and also conflicts in its access with the primary rule regular expression ActiveSync device type rule Andro.*; that rule was formerly an ancillary rule prior to being clicked. In the preceding example, the normal ActiveSync device type rule Android, was not displayed as an ancillary rule because, from the perspective of the then primary rule (the regular expression ActiveSync device type rule touch.*), it was not related to it.

To configure a normal expression local rule

1. Click the Access Rules tab.

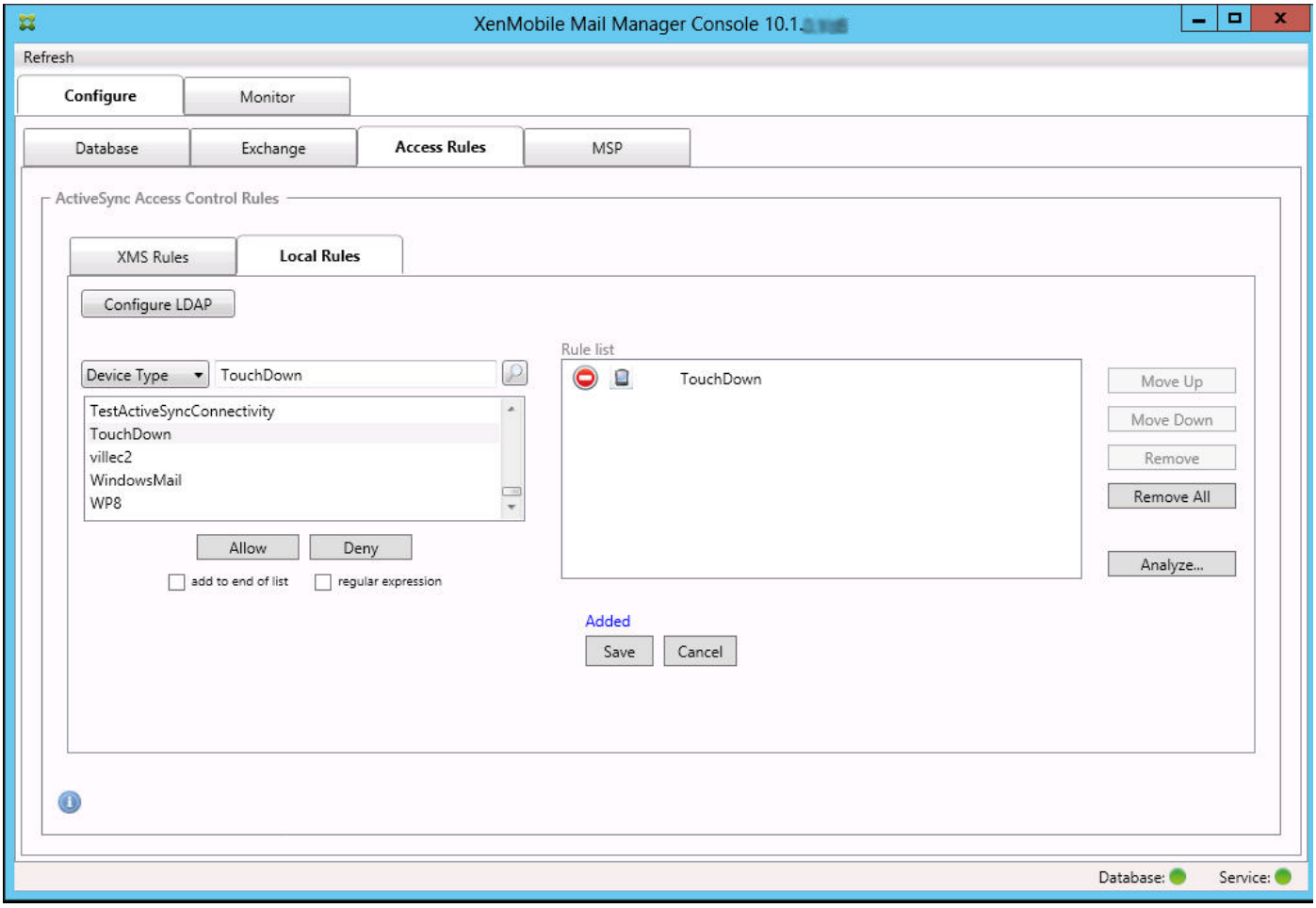


2. In the Device ID list, select the field for which you want to create a Local Rule.
3. Click on the magnifying glass icon to display all of the unique matches for the chosen field. In this example, the field Device Type has been chosen and the choices are shown below in the list box.



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.

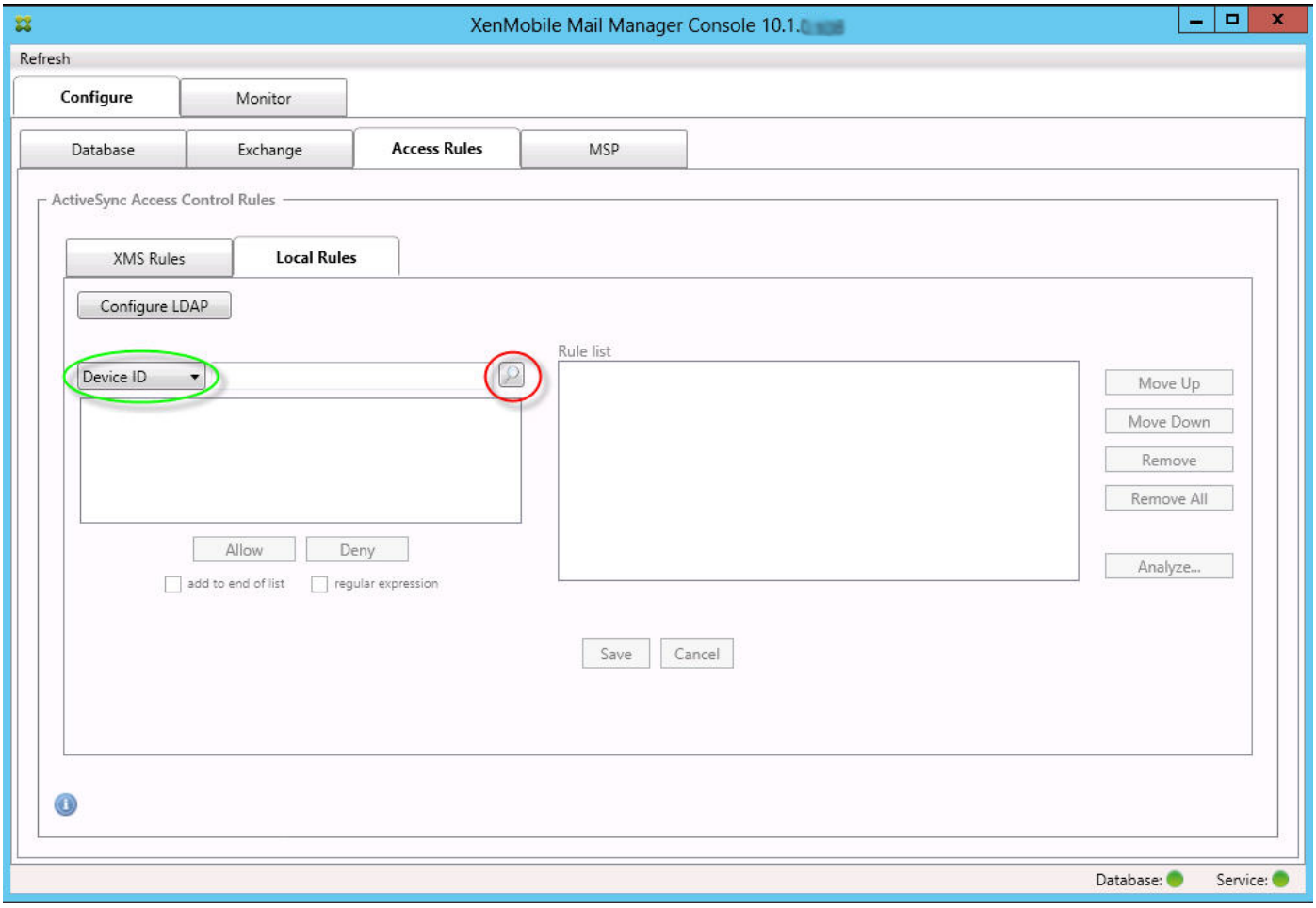


To add a regular expression

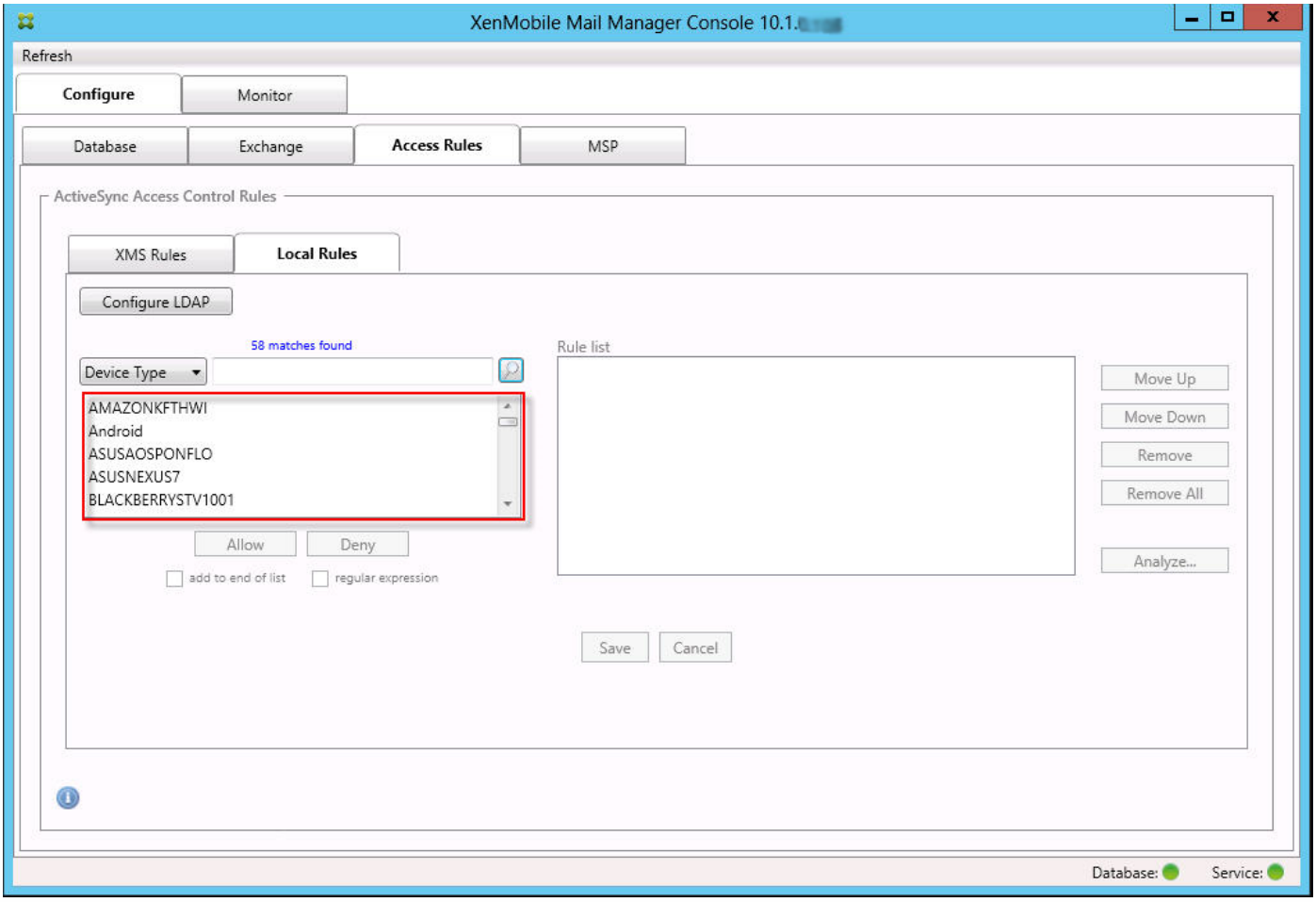
Regular expression local rules can be distinguished by the icon which appears next to them -  . To add a regular expression rule, you can either build a regular expression rule from an existing value from the results list for a given field (as long as a major snapshot has completed), or you can simply type in the regular expression that you want.

To build a regular expression from an existing field value

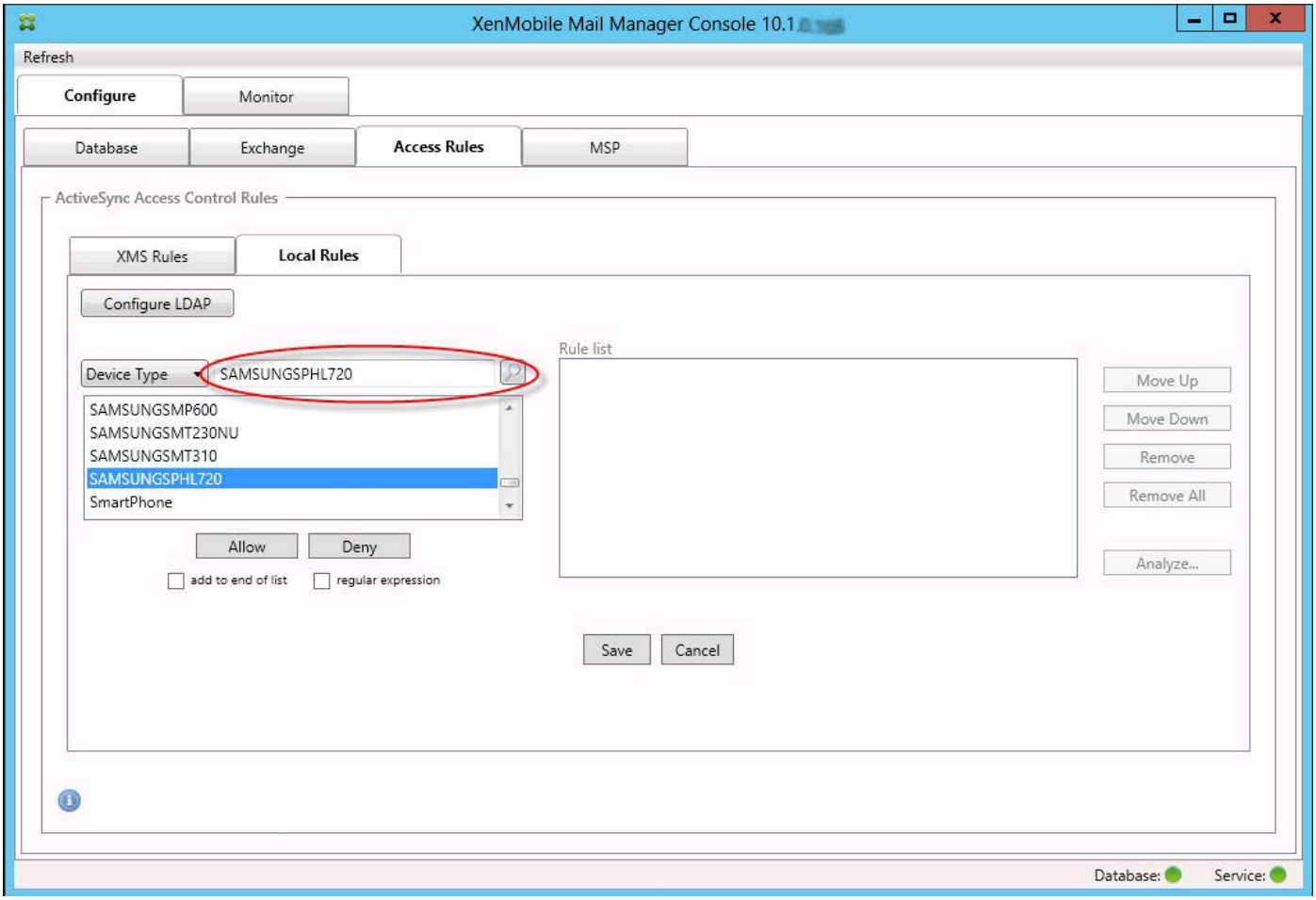
1. Click the Access Rules tab.



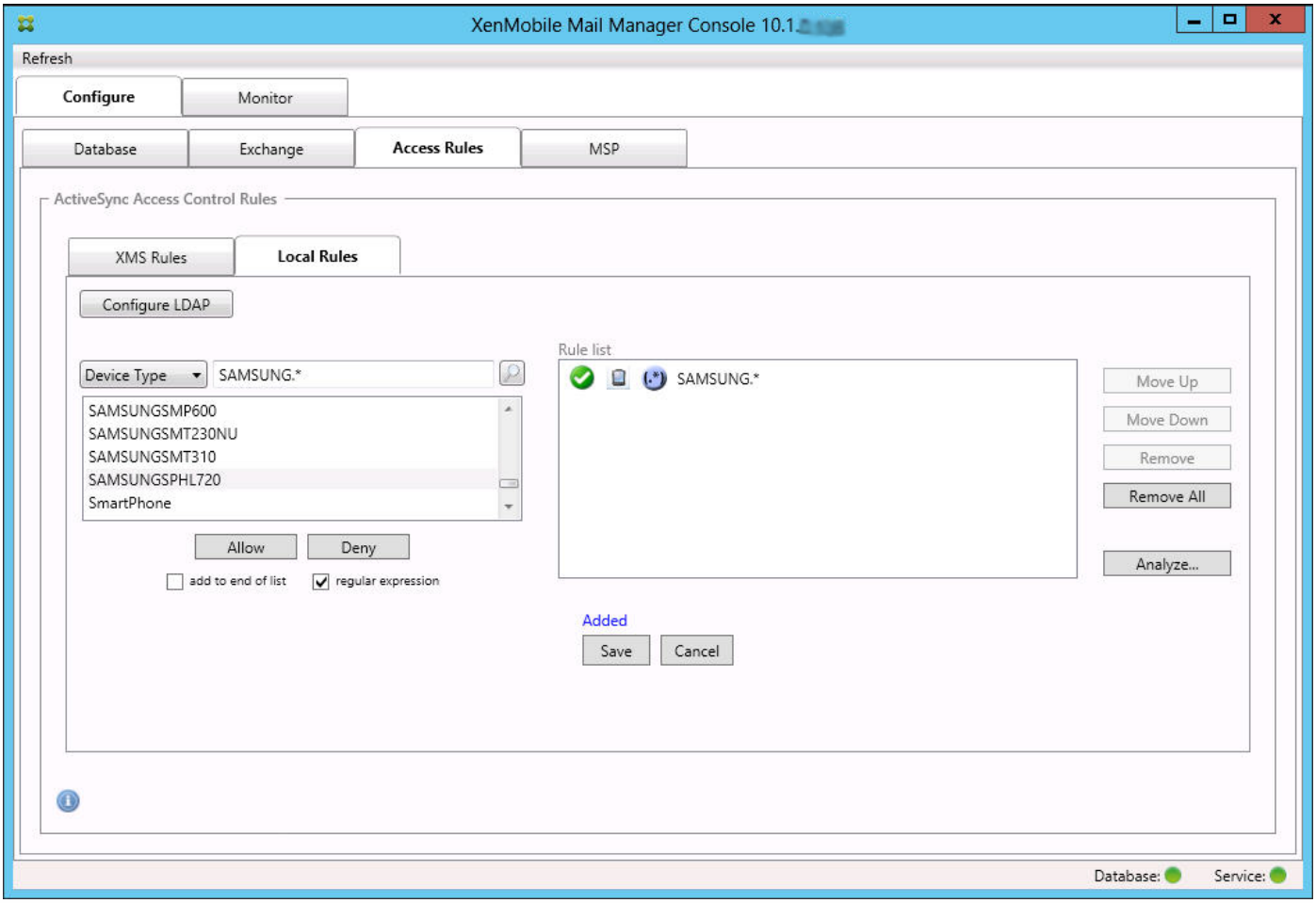
2. In the Device ID list, select the field for which you want to create a regular expression Local Rule.
3. Click on the magnifying glass icon to display all of the unique matches for the chosen field. In this example, the field Device Type has been chosen and the choices are shown below in the list box.



4. Click one of the items in the results list. In this example, SAMSUNGSPHL720 has been selected and appears in the text box adjacent to Device Type.

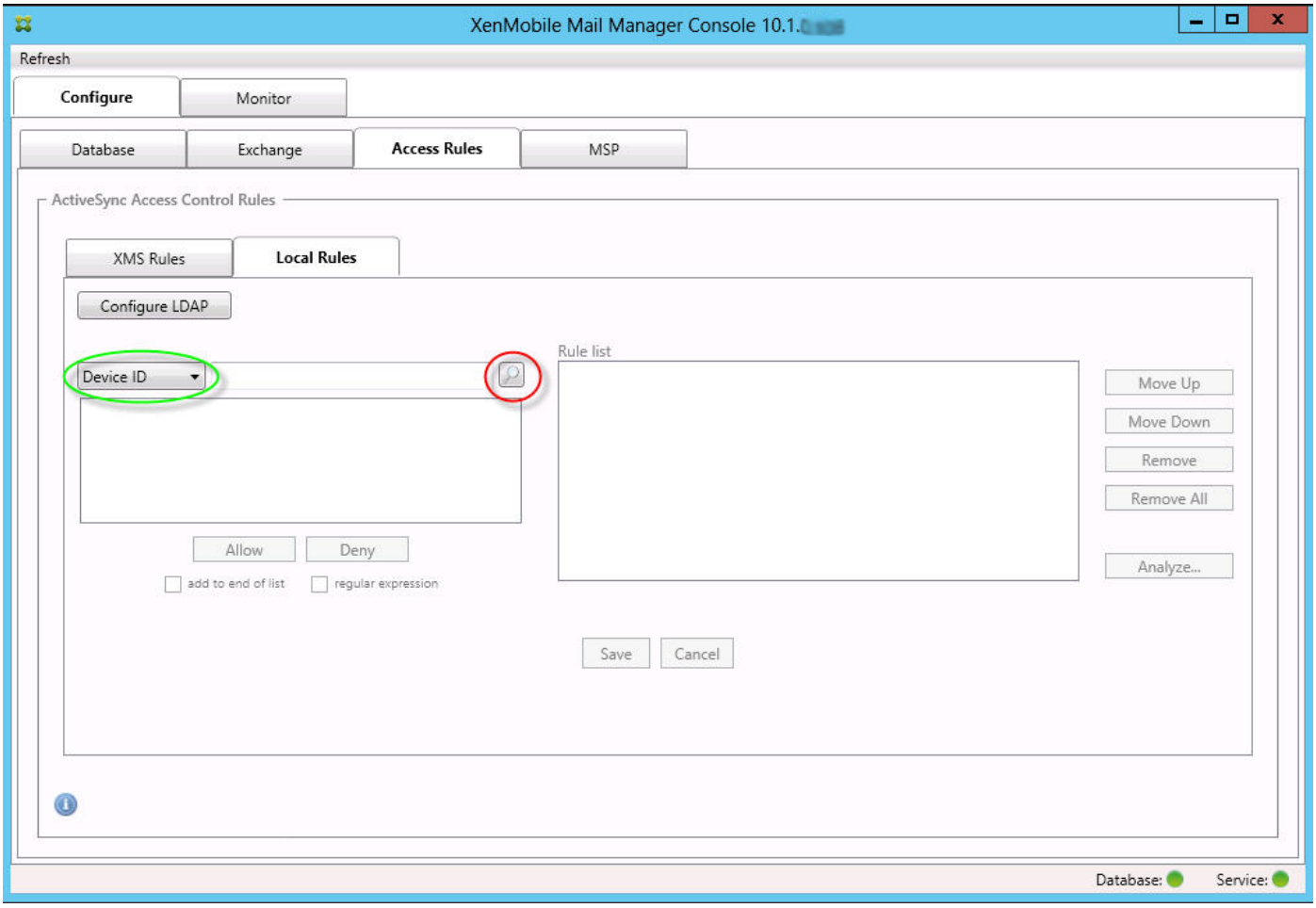


5. To allow all device types that have "Samsung" in their device type value, add a regular expression rule by following these steps:
   1. Click within the selected item text box.
   2. Change the text from SAMSUNGSPHL720 to SAMSUNG.*
   3. Make sure that the regular expression check box is selected.
   4. Click Allow.

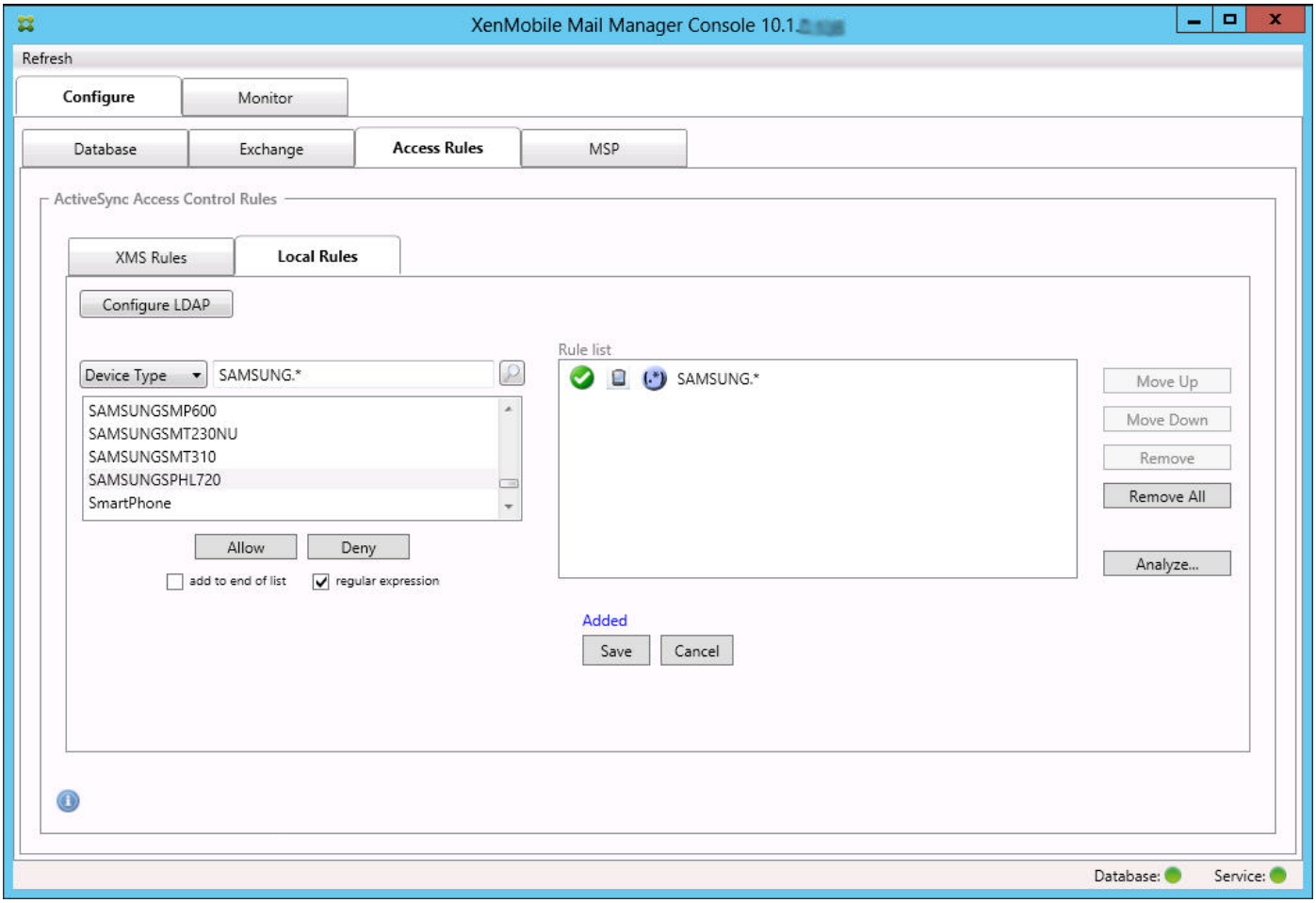


To build an access rule

1. Click the Local Rules tab.
2. To enter the regular expression, you need to make use of both the Device ID list and the selected item text box.



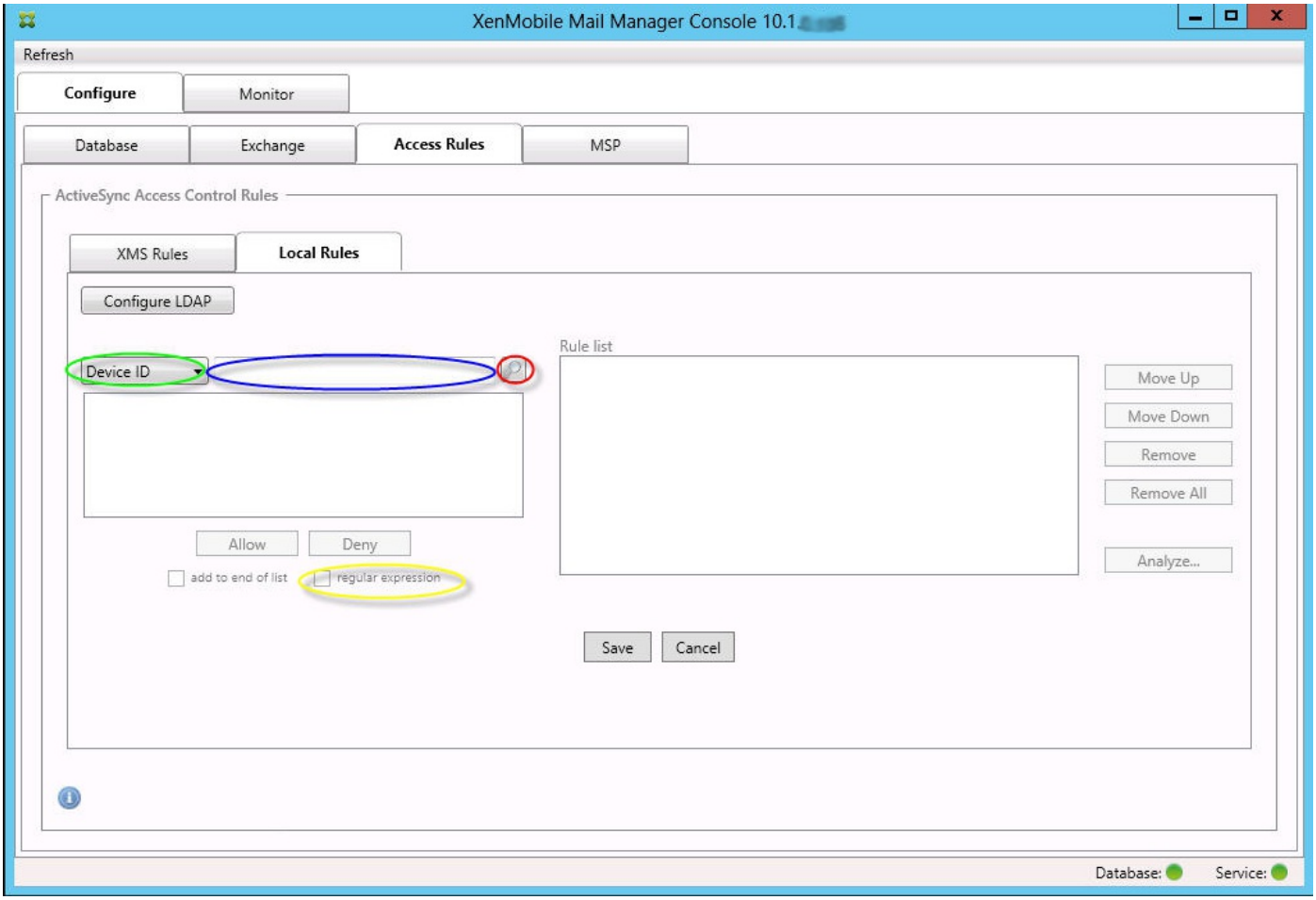
3. Select the field you want to match against. This example uses Device Type.
4. Type in the regular expression. This example uses samsung.*
5. Ensure that the regular expression check box is selected and then click Allow or Deny. In this example, the choice is Allow so that the final result is as follows:



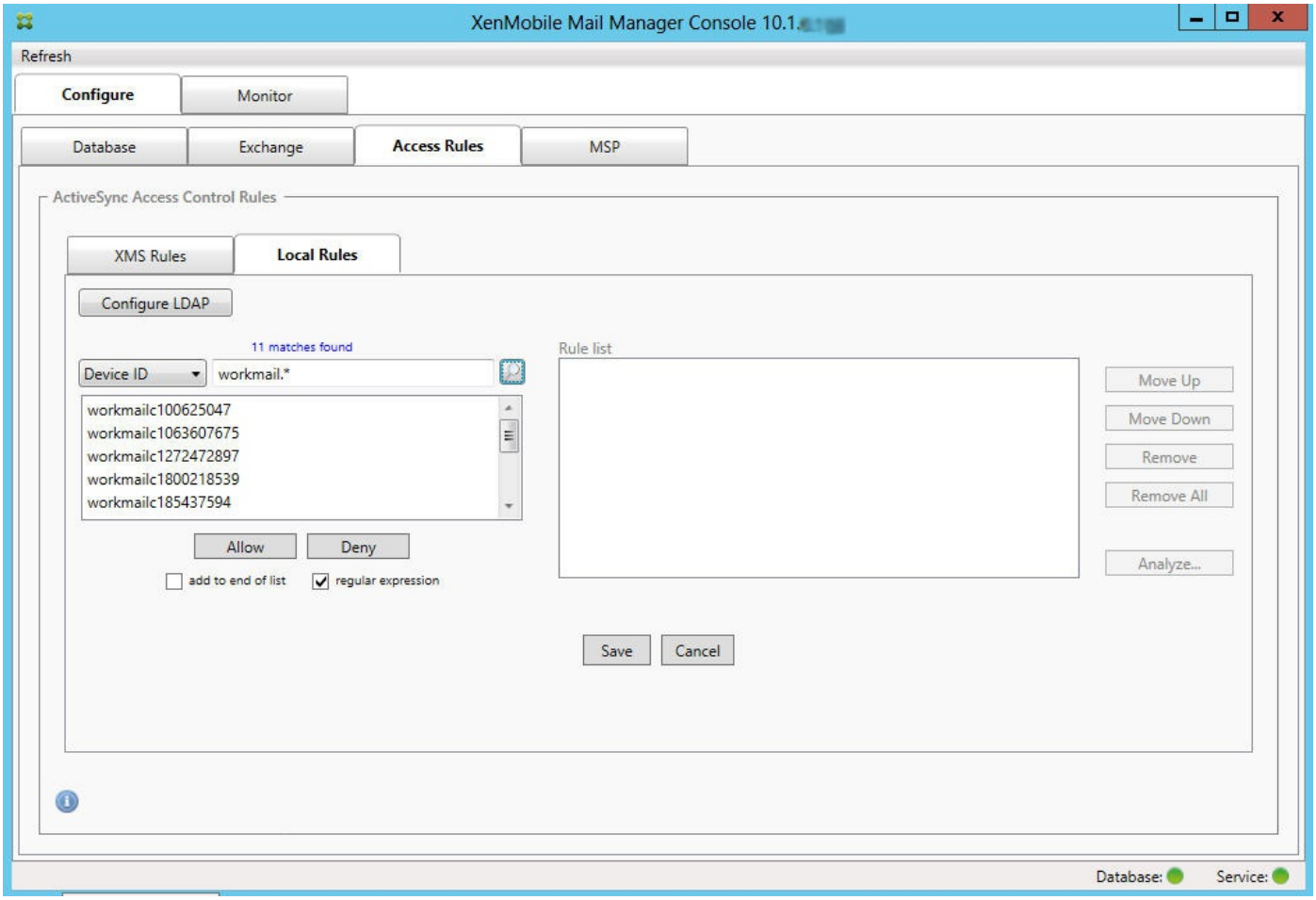
To find devices

By selecting the regular expression check box, you can run searches for specific devices that match the given expression. This feature is only available if a major snapshot has successfully completed. You can use this feature even if there is no plan to use regular expression rules. For example, assume that you want to find all devices that have the text "workmail" in their ActiveSync device ID. To do so, follow this procedure.

1. Click the Access Rules tab.
2. Ensure that the device match field selector is set to Device ID (the default).



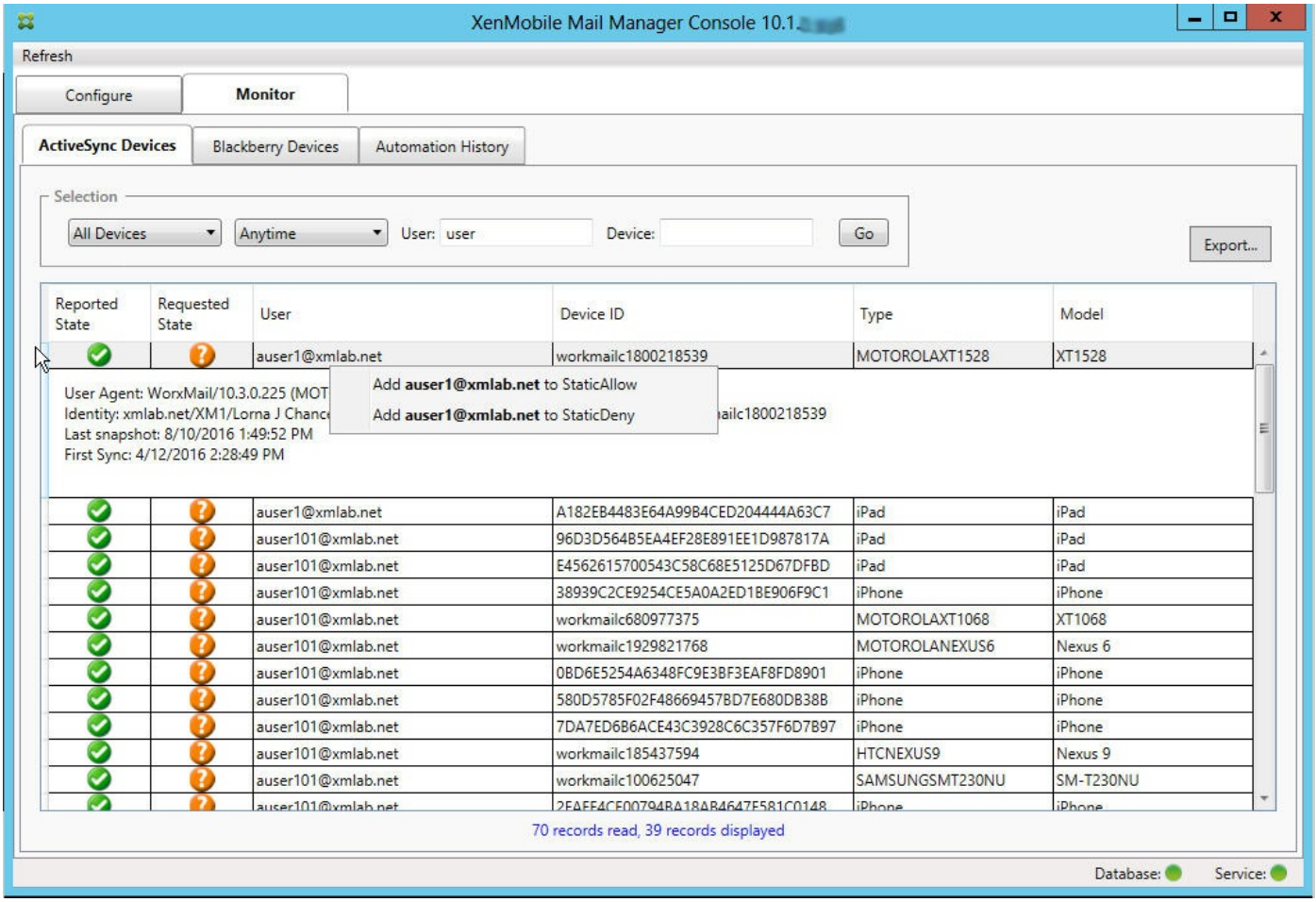
3. Click within the selected item text box (as shown in blue in the preceding figure) and then type workmail.*.
4. Make sure the regular expression check box is selected and then click the magnifying glass icon to display matches as shown in the following figure.



To add an individual user, device, or device type to a static rule

You can add static rules based on user, device ID, or device type on the ActiveSync Devices tab.

1. Click the ActiveSync Devices tab.
2. In the list, right-click a user, device, or device type and select whether to allow or deny your selection.
   The following image shows the Allow/Deny option when user1 is selected.



Device monitoring

Oct 05, 2016

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.

Troubleshooting and diagnostics

Jan 06, 2017

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.

Common Errors

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.

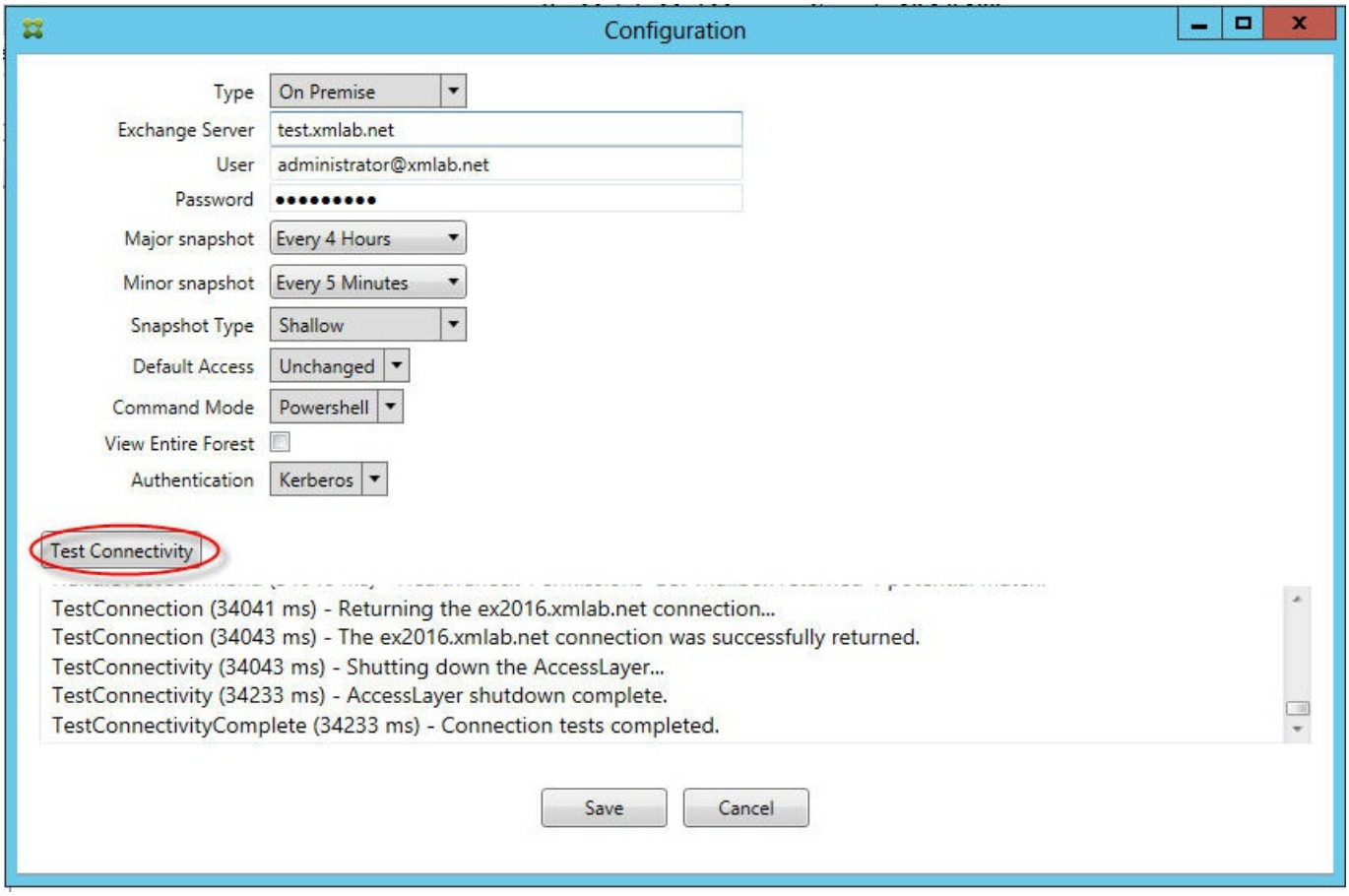
  If Windows Integrated authentication is configured, the user account of the XenMobile Mail Manager service must be an allowed SQL logon. The account of the XenMobile Mail Manager service defaults to Local System, but may be changed to any account that has local administrator privileges. If SQL authentication 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.



Troubleshooting Tools

A set of PowerShell utilities for troubleshooting is available in the Support\PowerShell folder.

A troubleshooting tool performs in-depth analysis of user mailboxes and devices, detecting error conditions and potential areas of failure, and in-depth RBAC analysis of users. It can save raw output of all cdmlets to a text file.

XenMobile NetScaler Connector

Nov 17, 2016

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 the following articles:

- XenMobile NetScaler Connector
- ActiveSync Gateway in XenMobile

For a detailed reference architecture diagram, see the XenMobile Deployment Handbook article, Reference Architecture for On-Premises Deployments.