About XenMobile Server 10.3.6

Oct 31, 2016

> **Note**
>
> Citrix supports the current version of XenMobile Server and the prior two versions. We keep the product documentation for versions earlier than those versions as PDFs in the Archive List of Legacy Documents.
>
> For product documentation on the current release, see XenMobile Server.

You can directly upgrade to XenMobile 10.3.6 Service Pack only from XenMobile 10.3.5.

> **Note**
>
> Before you upgrade to XenMobile 10.3.6, the Subscription Advantage (SA) date on your Citrix license must be later than June 1, 2016. You can view your SA date next to the license in the License Server. To renew the SA date on your license, download the latest license file from the Citrix Portal and upload the file to the Licensing Server. For more information, see http://support.citrix.com/article/CTX209580.

To perform the upgrade, you use xms_10.3.6.310.bin. In the XenMobile console, click the gear icon in the upper-right corner of the console and then click **Release Management**. Click **Upgrade** and then upload the xms_10.3.6.310.bin file. For more information about upgrades in the console, see Upgrading XenMobile.

To complete a new installation of XenMobile 10.3.6, see Installing XenMobile.

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.

What's New in XenMobile 10.3.6

The XenMobile 10.3.6 release focuses on quality and scalability. For information about the many bug fixes, see Known and Fixed Issues in XenMobile 10.3.6. XenMobile 10.3.6 also includes the following new features.

Scalability improvements

The significant quality improvements on the XenMobile 10.3.6 server also provide better scale and performance in areas such as XenMobile server to database communications, XenApp integration, deployment notifications to devices, and LDAP lookups.

- HDX enumeration has improved about 40% over XenMobile 10.3.5.
- When you use the **Server Tuning** command in the XenMobile CLI main menu (option **5** under **Advanced Settings**), the defaults applied for the following settings now differ as follows:

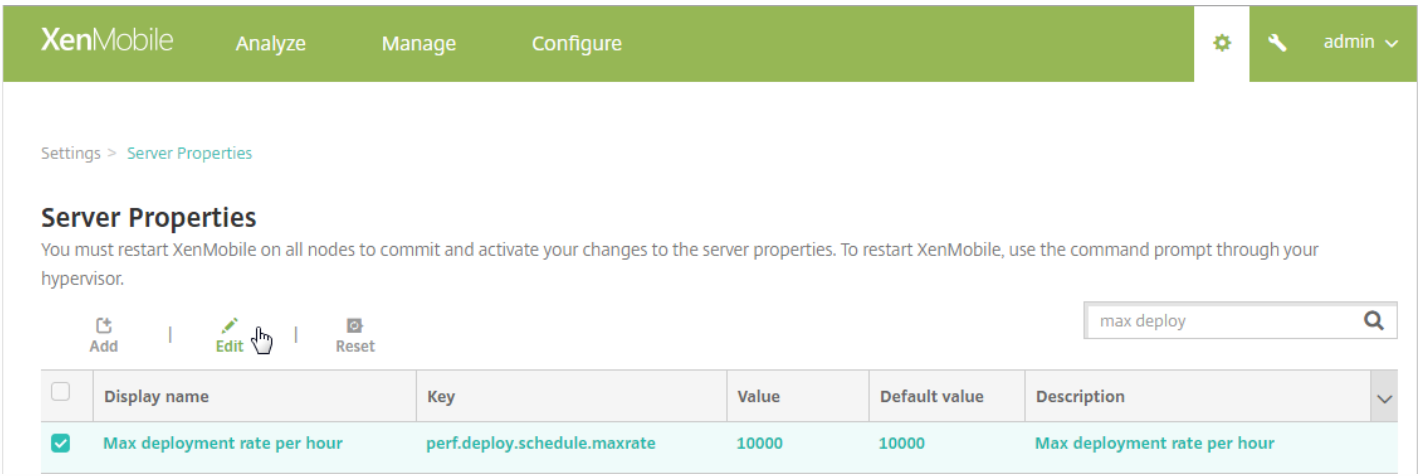
  Maximum connections on port 443: The default changed from **10000** to **12000**.

Maximum connections on port 8443: The default changed from **10000** to **12000**.

Maximum threads on port 443: The default changed from **750** to **2000**.

Maximum threads on port 8443: The default changed from **750** to **2000**.

- XenMobile now sends notifications in a phased deployment to avoid spikes in reconnection requests from iOS and Windows Phone devices, as well as Android devices configured for Google Cloud Messaging. The deployment rate defaults to 10,000 devices per hour. To change the deployment rate, edit the **Max deployment rate** server property (perf.deploy.schedule.maxrate).



- XenMobile deployments now target only the devices that are part of the target delivery groups. Previously, all devices were deployed regardless of role.

Worx app updates

> ### Note
>
> Starting with version 10.4, Worx Mobile Apps are renamed XenMobile Apps. Most of the individual apps are renamed as well. For details, see About XenMobile Apps.

Worx Home

- **Send logs with WorxMail**. When users send logs while reporting an issue, WorxMail now opens by default. This allows users to send large files successfully. In earlier versions of Worx Home, large files sometimes failed to send.

WorxMail

- **Support for Exchange Server 2016**. You can now integrate WorxMail with Exchange Server 2016. Active Sync 14 is supported, but WorxMail should also be compatible with Active Sync 16.
- **Attach files from ShareFile (Android)**. Users can tap **Attach from ShareFile** to attach files to emails or calendar events.
- **Attach files from ShareFile Restricted StorageZones and connectors (iOS)**. When users tap **Attach from ShareFile** in an email or calendar event, they can attach files not only from ShareFile, but also from Restricted StorageZones and

connectors, such as from SharePoint and network shares.

- **Share contact data with .vcard files**. Users can import contact information from attachments sent as .vcard files.
- **New network access default**. The default for the **Network access** policy in the MDX Toolkit is now **Tunneled to the internal network**. This change should reduce configuration errors.

WorxWeb

- **Block pop-ups by default**. If you want pop-ups for Safari to be blocked by default, use the XenMobile console to set the **Restrictions** device policy option **Block pop-ups** to **On**. If you had **Block pop-ups** set to **Off** before upgrading to version 10.3.6, the setting remains off. Otherwise, the setting is **On** and pop-ups in Safari are blocked.
- **Open links in ShareFile**. ShareFile 4.0 allows users to choose whether to open links in a browser or directly in ShareFile.

WorxChat Tech Preview

- **Support for Android.** WorxChat is now available on Android.
- **Support for Lync 2013 and Skype for Business 2015**. You can now integrate WorxChat with Lync 2013 and Skype for Business 2015 in the same pool.

Secure Forms

- **Support for ShareFile Restricted Zones**. You can now configure Secure Forms with ShareFile Restricted Zones. Follow the setup instructions at Integrating Secure Forms with ShareFile.
- **iBeacon capability**. Using iBeacon technology, you can configure and track beacons that allow users to autofill forms on the mobile app. Beacon information is included when users submit forms. For information on setting up beacons, please see Beacons.
- **Creator name**. Secure Forms Composer now displays the name of the person who created a form. This feature helps with tracking when there are multiple users accessing the composer.
- **Number ranges**. In the **Number** field on the composer, you can specify a range of numbers that users are allowed to enter when filling out forms.
- **New file name format.** Forms and attachments submitted on the mobile app are now saved with the submitter's name and a time stamp, making the file names easier to read and organize.

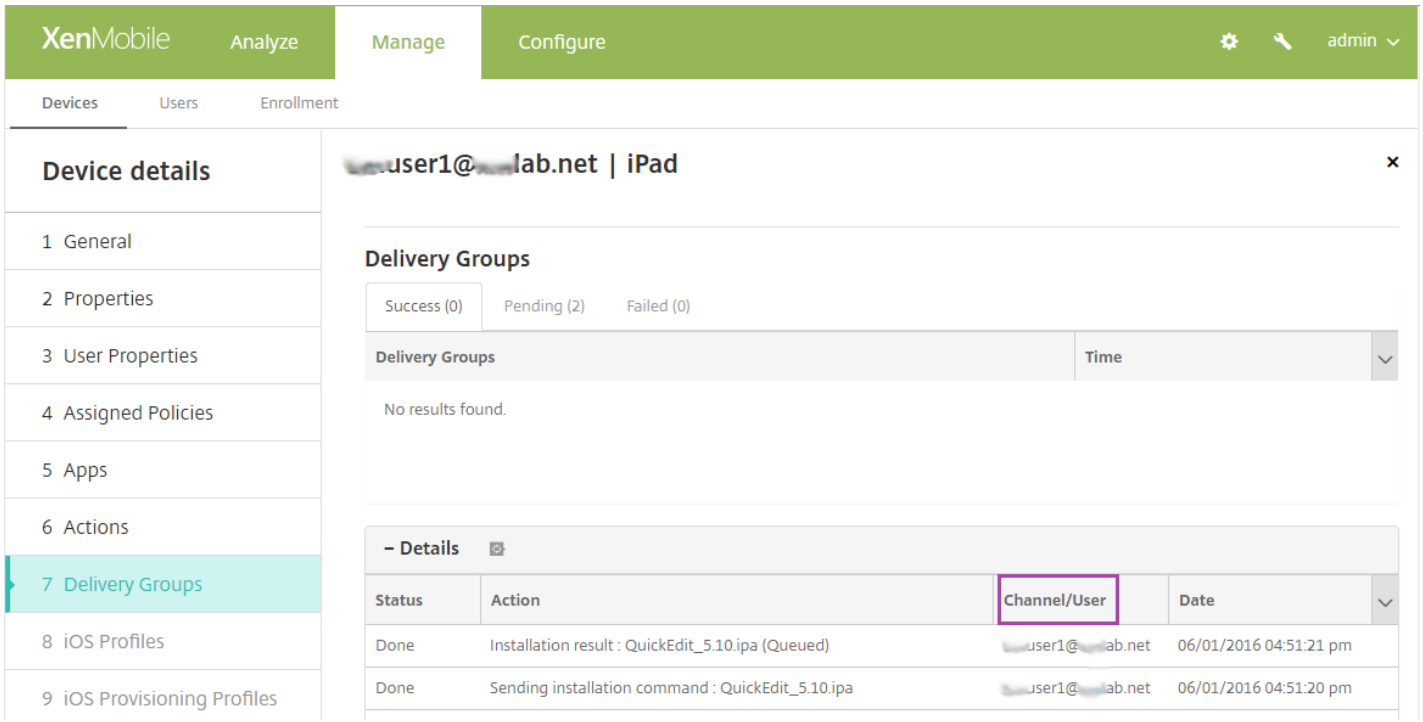
For more information, see What's New in Worx Mobile Apps.

Other updates

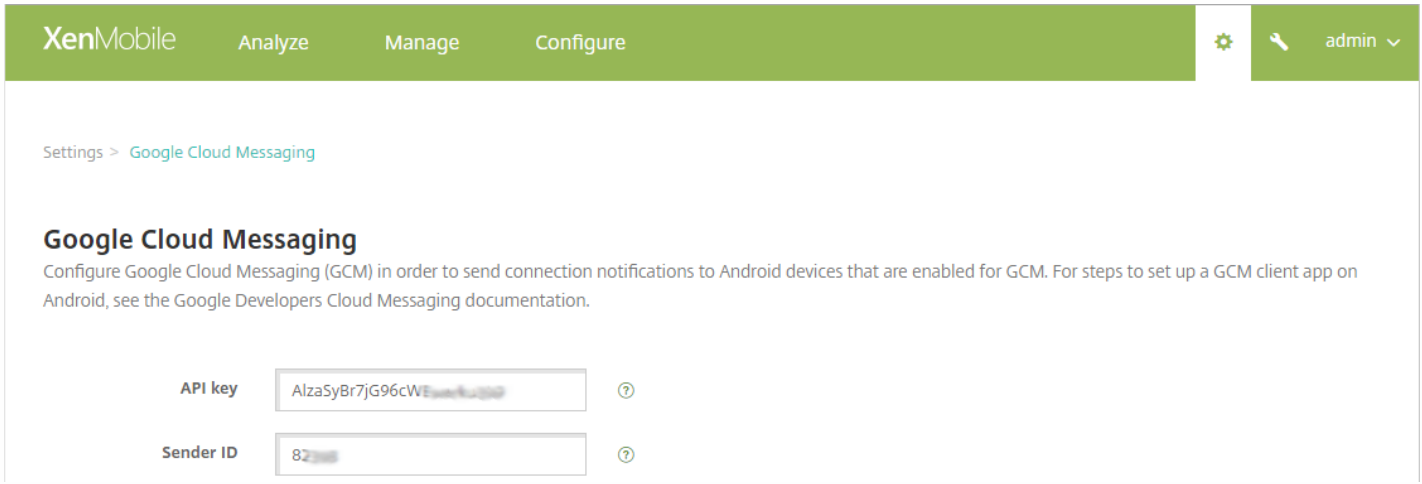
- **Support for additional Citrix component versions.**
  - NetScaler Gateway 10.5.x, 11.0.x, and 11.1.x (XenMobile on-premises)
  - NetScaler Gateway 10.5.57.7 (XenMobile Cloud)
  - XenApp and XenDesktop 7.9 and 7.8
  - StoreFront 3.6
  - License Server 11.13.1.2
- **Whitelisted WiFi networks.** The Whitelisted WiFi networks policy allows you to specify allowed networks. Apps work only when connected to one of the networks on the list. This feature is available in MDM+MAM mode only.
- **ShareFile support for shared devices.** ShareFile mobile app version 4.4 now supports shared devices in MDM+MAM mode, allowing multiple users to share a device without re-enrolling. For more information, please see Shared Devices in XenMobile.
- **Icon handling (iOS).** App developers can now put icon files in the app bundle root folder, as an alternative to the usual practice of putting them in info.plist. For the toolkit to be able to locate the icon files, their names must be in one the following formats:

- icon.png
- icon-60x2.pn
- icon-72.png
- icon-76.png

- **Improved mail sync (iOS).** Updates to mail sync and ShareFile integration have made mail sync more reliable.
- **Additional device information.** The **Device details** page in the XenMobile console now includes a **Channel/User** column that shows the target of a deployment action on the device. The target may show a user who enrolled the device, a checked-in user on a shared device, or system-level settings or deployment actions not tied to a specific user. You can use this information to better track the deployment process, especially when you have many users handling one device or many containers on a specific platform like Mac OS X.

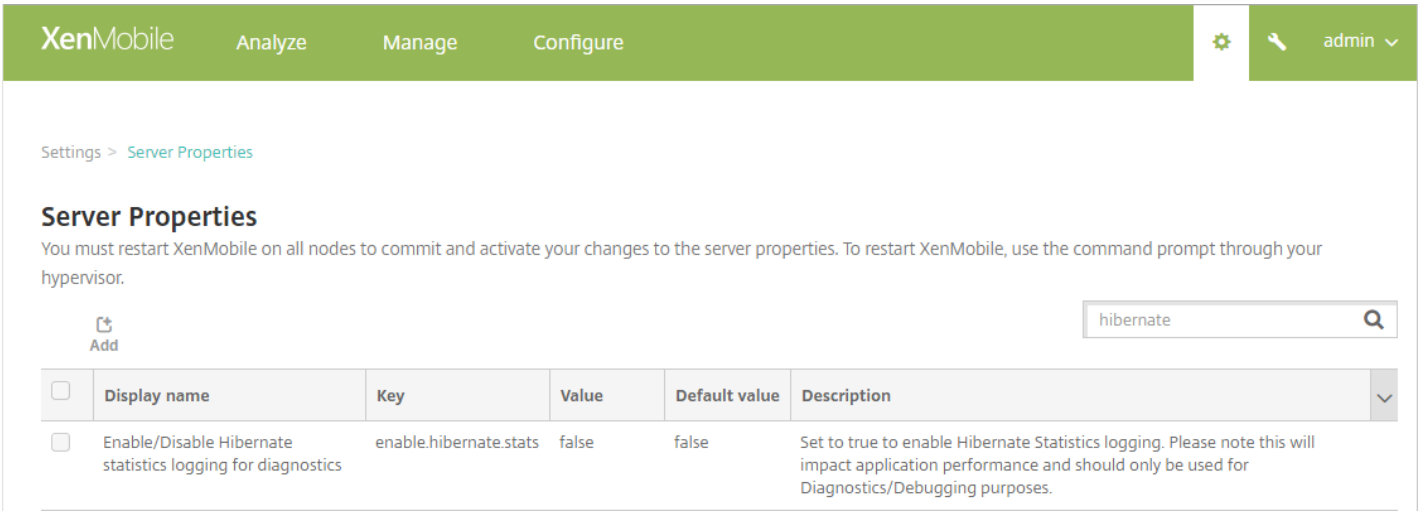


- **New XenMobile console page.** The XenMobile console includes a new page, **Settings > Google Cloud Messaging**, where you can specify your GCM **API key** and **Sender ID**. Previously those items appeared only in **Server Properties**.



- **Hibernate statistics logging for diagnostics.** To assist with troubleshooting application performance issues, XenMobile can now provide a statistics logging report for Hibernate, a component used for XenMobile connections to Microsoft SQL Server.

  To enable Hibernate statistics logging, change the **Enable/Disable Hibernate statistics logging for diagnostics** server property (enable.hibernate.stats) to **true**. 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.



- **Updates in the Android app store.** The Android app store will show an updated app version only if the version installed on the Android device is older than the version in the app store. With this change, iOS and Android app updates work the same way.
- **XenMobile Analyzer Tool.** When you have an issue with your XenMobile environment, contacting Citrix Support can cost your organization time and money. With XenMobile Analyzer, you can triage common issues on your own before contacting support. The XenMobile Analyzer Tool supports numerous use-cases and deployment options, including MDM, MDM+MAM, and MAM-only; 5 different authentication scenarios; and both iOS and Android mobile environments.

  XenMobile Analyzer can do the following:
  - Check your environment for issues and recommend solutions. XenMobile Analyzer environmental checks can identify device issues, user enrollment issues, and authentication issues.
  - Walk you through the steps to receive advanced diagnostics.
  - Direct you to tools to check your WorxMail Readiness and Sever Connectivity Checks.
  - If all else fails, the tool provides a direct link to Citrix Support.

  For more information, see XenMobile Analyzer Tool.

- **XenMobile AutoDiscovery Service.** Up until now, activating autodiscovery required creating a support ticket. With the AutoDiscovery Service portal, you can set up autodiscovery on your own. The service walks you through the steps for claiming your domain then creating autodiscovery records. For more information, see XenMobile AutoDiscovery Service.

Known and Fixed Issues in XenMobile 10.3.6

Nov 02, 2016

The following issues are known or fixed in XenMobile 10.3.6:

Known Issues

When users attempt to enroll their personal device with a Microsoft work account, the enrollment fails. [#597037]

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

After updating XenMobile to 10.3.6, in a clustered configuration, iOS device enrollment may fail. As a workaround, see this Knowledge Article. [#650061]

Fixed Issues

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. [#585032]

This fix ensures that when a user sets the log file size and maximum number of backup log files, these values are configured correctly in XenMobile and the files roll over properly. However, the XenMobile console might not reflect the updated values as noted in Known Issue #551199. [#597772]

In editions of XenMobile that include unified MDM and MAM, iOS devices occasionally fail to be completely enrolled. The device might be MDM enrolled but not MAM enrolled, or MAM enrolled but not MDM enrolled. [#610847]

When updating from XenMobile 10.1 to version 10.3, if the WorxStore has a custom name, you must change the store name to the default setting of **Store** and deploy the setting to devices before updating. If not, the custom store name causes issues with XenMobile 10.3 enrollment, access to Worx Home and the WorxStore, and app deployment on iOS devices. [#614049]

When you configure an Exchange ActiveSync device policy for Windows and you set the **Only when previous deployment has failed** option in the deployment rules, the following issue occurs: After Windows Phone users change the Exchange Server mail sync time, the users' change is overridden the next time that XenMobile pushes an Exchange ActiveSync policy to the Windows device. [#616725]

When you search for a device or user within the XenMobile console when the database contains a large amount of data, the CPU utilization on SQL Server spikes and the search may take longer than 1 minute. [#618371]

When users on iOS devices enroll in Worx Home, occasionally Worx Home stops responding for up to two minutes before prompting users to create a Worx PIN. After this issue occurs, when users open the WorxStore, Worx Home stops responding again. [#619945]

On Mac OS X computers and iPads, XenMobile 10.3 always carries out deletion (or removal) actions first, regardless of the

order you set in the XenMobile console. [#620459]

Attempts to send SMS notification from the XenMobile server to devices running Windows 10 might fail. [#621229]

When you add a child Active Directory group to a parent group that contains more than 1,500 members, actions that you carry out in the XenMobile console, such as delivery group assignments, are not applied to users in the added child group. [#622523]

After enrolling iOS devices, users are not prompted to install Required applications, until they open the WorkStore or they try to add an app manually. [#622789]

Users are unable to authenticate to Worx Home after an upgrade from XenMobile 9.0 to XenMobile 10.1 followed by setting the LDAP option User search by to sAMAccountName and then upgrading to XenMobile 10.3.x. [#624340]

Policy deployments and RBAC role assignment might fail if explicit UPN doesn't match implicit UPN for the user. [#624612]

On clustered server deployments, issues involving the Hazelcast distributed map and connectivity to the SQL server might cause the XenMobile server to become unresponsive intermittently, preventing logins and causing enrollments to fail. [#624931]

When an Android device connects to XenMobile server the first time or reconnects, Android apps are slow to download or fail to download. [#625199]

The app list might fail to display for WorxHome 10.3 users if a public app containing ASCII character 16 (the data line escape character) in its name or description is added to the XenMobile console. [#627059]

Clustered servers might become unresponsive intermittently if a Hazelcast distributed map has been implemented. [#627114]

After upgrading two server instances to XenMobile 10.3, after running for a while, the first server becomes unresponsive. [#628270]

After successfully enrolling, iOS devices sometimes cannot log into WorxStore and this message appears: "Unable to fetch the required assets to continue. Please try again." This issue occurs because XenMobile server isn't finding the device by its MAM device ID. [#629900]

Devices deleted from the XenMobile console continue to allow access to MAM resources. [#630137]

Occasionally, a selective wipe occurs for iOS users. [#630466]

In XenMobile 10.3.x, the category view of Worx Home might fail to display HDX apps. The "Other" folder that contained HDX apps, by default, in category view for previous versions of XenMobile might not appear. [#631439]

When users enroll a device, MDM enrollment is successful but occasionally MAM registration fails with an error, your apps are locked. [#632073]

Android apps compiled with Android SDK version 22 or later or Obfuscated with Dexguard will not upload to XenMobile. [#632146]

Intermittently, after users enroll in Worx Home, they are prompted to uninstall and reinstall Worx Home. [#633095]

When you perform a selective wipe, a full wipe, or you delete an account or device in the XenMobile console, occasionally the associated VPP licenses are not freed for the apps that were configured on the device. [#633366]

Some VPP licenses have negative IDs, such as -123441212, in which case you cannot distribute the public apps. [#631443]

When users enroll a device, occasionally Worx Home crashes with a 403 error message stating that the app store is locked. Alternately, users may enroll successfully, but when downloading an app, the same error occurs or an error stating "unable to fetch details." [#633515]

If a Google Play credential is configured with an invalid Device ID, when you add a public app store app for Google Play and click to search the Google Play store for the app name, search fails or renders incorrect search results. [#633845]

When users try to configure a WiFi device policy with a shared key in the XenMobile console for Windows-based devices, after they change the authentication type to WPA Personal or WPA-2 Personal, the shared key option does not appear as expected. [#633897]

If you have a NetScaler configured as a forward proxy, XenMobile 10.3 connectivity checks return incorrect results. [#633902]

After upgrading to XenMobile 10.3.5, devices are no longer enrolled in MAM mode. In addition, policy and app deployments fail for devices that are enrolled in MDM+MAM mode. [#634034]

After you enable iOS bulk enrollment and update the root Certificate Authority (CA) of the XenMobile SSL certificate, device enrollment or re-enrollment may fail. The issue may occur when you change from a self-signed certificate to a public certificate, purchase a certificate from a new provider, or move to an internal corporate CA. The issue does not affect existing enrolled devices. [#635699]

In editions of XenMobile that include unified MDM and MAM, MAM authentication might fail for Authorized DEP devices when the "user" search field in LDAP settings is set to samAccountName. As a result, Worx Home registration might not complete and the device might be enrolled in MDM only. [#637599]

XenMobile Scalability and Performance

Jan 06, 2017

Understanding the scale of your XenMobile infrastructure plays a significant role in how you decide to deploy and configure XenMobile. This article offers answers to common questions on determining the requirements for small to large scale enterprise deployments.

> **Note**
>
> Starting with version 10.4, Worx Mobile Apps are renamed XenMobile Apps. Worx Store and most individual apps are renamed as well. For details, see About XenMobile Apps.

Performance and Scalability Guidelines

The data in this article are intended as guidelines for determining performance and scalability of a XenMobile 10.3.6 infrastructure. The two key factors for determining how to configure your server and database are scalability (maximum users/devices) and logon rate.

- Scalability is defined as the maximum number of concurrent users executing a defined workload. For more information on the flows used to load the XenMobile infrastructure, see Workloads.
- Logon Rate is defined as the on-boarding of new users and the authentication of existing users.
  - On-boarding rate is the maximum number of devices that can be enrolled on the environment for the first time. Called First Time Use or FTU in this article, this data point is important when orchestrating a rollout strategy.
  - Existing user rate is the maximum number of users who authenticate to the environment, who have already enrolled and connected with their device. These tests included creating sessions for already enrolled users and the execution of WorxMail and WorxWeb apps.

The following table displays scalability guidelines based on the test results for the corresponding XenMobile environment.

Scalability	Up to 45,000 devices	
Logon Rates	On-boarding (FTU)	Up to 833 devices per hour
	Existing users	Up to 2,812 devices per hour
Configuration	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	XenMobile Server 6-node cluster
	Database	Microsoft SQL Server external database

> **Important**
>
> The automation requirement for this report is 1,000 to 60,000 devices. Any requirement that exceeds 60,000 devices is out of scope of this report.

Test Profile Configuration

This section describes the Active Directory configuration, number of XenMobile policies, number and type of applications, simulated user actions, and simulated administrator actions of the test profile that was used for each hardware configuration and workload used to derive the test results in this article.

> **Note**
>
> This test profile is designed to use more resources than profiles used to test scalability for previous versions of XenMobile. Therefore, these test results are not directly comparable to scalability results from previous versions.

Active Directory (AD) configuration:

- 100,000 unique AD users
- 200,000 unique AD groups
- 5 levels of nesting for AD groups
- 200 users per AD group

Delivery groups:

- 20 delivery groups
- 50 apps assigned to delivery groups
- 10 AD groups per delivery groups

XenMobile device policies:

- 300 device policies
- 20 device policies per user

Applications:

- 200 native applications from a public store
- 50 native enterprise distribution applications
- 100 web and Software as a Service (SaaS) applications

- 50 applications per user

XenMobile user actions:
- 50 total configured actions
- Worx Store launches:
  - First-time users (FTU): 4
  - Returning users (RU): 1
- Application launches:
  - MDX: 1
  - Web/SaaS: 1
- 150 STA validations per user

XenMobile administrator operations:
- Enumerate devices (to simulate help desk call scenerios): 32 operations per 8 hours, one every 15 to 20 minutes.
- Generate reports: 2 times per 8 hours.

System Configuration and Test Results

This section describes hardware configuration used and the results of running the on-boarding (FTU) workload and the Existing User workload scalability tests.

The following table defines the hardware and configuration recommendations for XenMobile when scaling from 1,000 to 60,000 devices. These guidelines are based on the test results and their associated workloads. The recommendations account for the acceptable margin of error as defined in Exit Criteria.

Analysis of the test results led to these conclusions:

- Logon rate is an important factor in determining the scalability of a system. In addition to the initial logon, logon rates are dependent upon the authentication time-out values configured in your environment. For instance, if you set the authentication time-out value too low, users must perform more frequent logon requests. Therefore, you need to clearly understand how time-out settings affect your environment.
- The number of connections per user session on NetScaler is an important consideration.
- To achieve maximum scalability, CPU and RAM resources were increased on XenMobile.
- The 6-node cluster configuration was the largest configuration validated. Scaling beyond 6 nodes requires an additional XenMobile implementation.

The following table shows the recommended on-boarding and existing user logon rates based on the XenMobile configuration, NetScaler Gateway appliance, cluster settings, and database. Use the data in this table to construct an optimal enrollment schedule for new deployments and returning user/device rates for existing deployments. The Configuration section relates enrollment and logon performance data to the appropriate hardware recommendations.

Expected number of devices	1,000	10,000	30,000	45,000
Actuak number of devices	1,000	9,998	29,977	44,991
Logon Rate				
On-boarding (FTU)	250	625	833	833
Existing users (Worx only)	1,000	1,666	3,750	883
Configuration				
Reference environment	VPX-XenMobile Standalone	MPX-XenMobile Standalone	MPX-XenMobile Cluster (3)	MPX-XenMobile Cluster (6)
NetScaler Gateway	VPX with 2 GB RAM 2 virtual CPUs	MPX-10500	MPX-11500	MPX-11500
XenMobile - mode	Standalone*	Standalone*	Cluster	Cluster
XenMobile - cluster	N/A	N/A	3	6
XenMobile - virtual appliance	8 GB RAM and 4 virtual CPUs	8 GB RAM and 4 virtual CPUs	16 GB RAM and 6 virtual CPUs	16 GB RAM and 8 virtual CPUs
Active Directory (AD)	8 GB RAM and 4 virtual CPUs	8 GB RAM and 4 virtual CPUs	16 GB RAM and 4 virtual CPUs	16 GB RM and 4 virtual CPUs
Database	External	External – Microsoft SQL Server Memory = 16 GB vCPUs = 12	External – Microsoft SQL Server Memory = 32 GB vCPUs = 12	External – Microsoft SQL Server Memory = 48 GB vCPUs = 16

MPX-XenMobile Cluster (3)

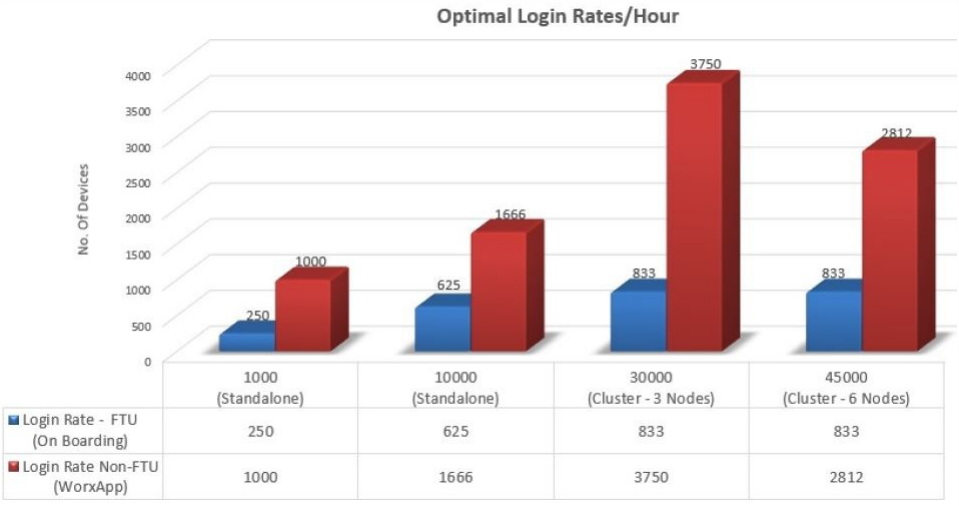
Cluster
Cluster
Cluster
Cluster
8 GB RAM and 4 virtual CPUs
8 GB RAM and 4 virtual CPUs

* Standalone deployments are not recommended for applications that must be highly available to users. Citrix recommends High Availability, clustered deployments for most customers.

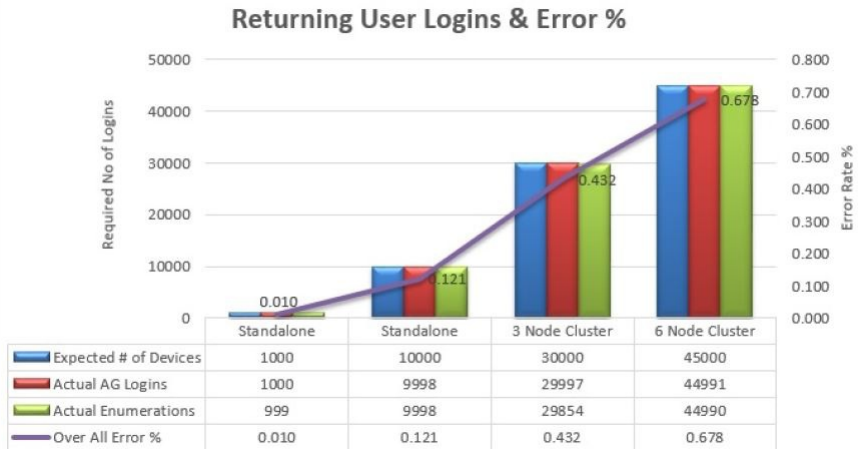
Note: You will experience the following if you exceed the recommended rates or hardware recommendations when sizing your system.

The following information provides additional data points that were recorded and that affect the results in the preceding table.

- Enrollment or logon latency (round-trip time)
  - Total average latency: 0.5 to 1.5 seconds
  - Average latency for a NetScaler Gateway logon: >120 to 440 ms
  - Average latency for a Worx Store request: 2 to 3 seconds
- Physical performance degradation, such as CPU and memory exhaustion, was observed on the infrastructure components when scalability limits were reached.
  - Invalid responses on the NetScaler Gateway and XenMobile appliances.
  - Slow XenMobile console response time during high loads.



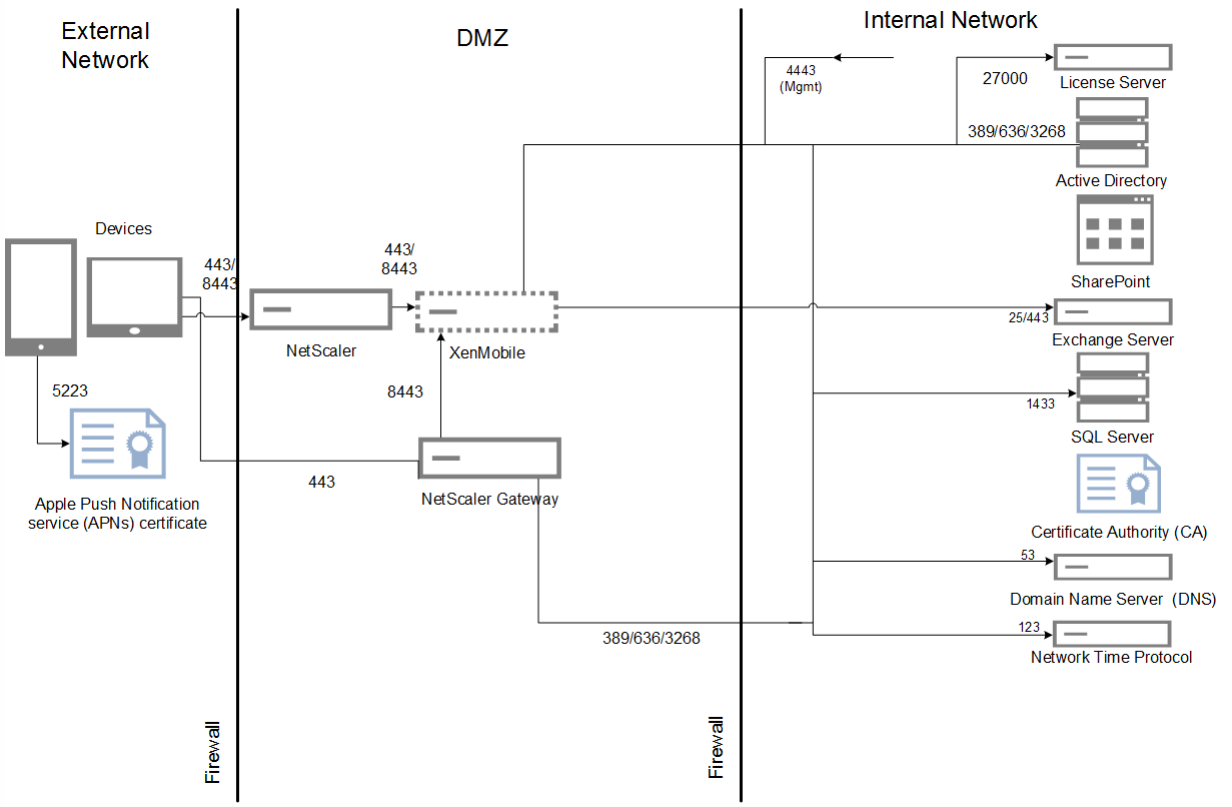
	1000 (Standalone)	10000 (Standalone)	30000 (Cluster - 3 Nodes)	45000 (Cluster - 6 Nodes)
Login Rate - FTU (On Boarding)	250	625	833	833
Login Rate Non-FTU (WorxApp)	1000	1666	3750	2812



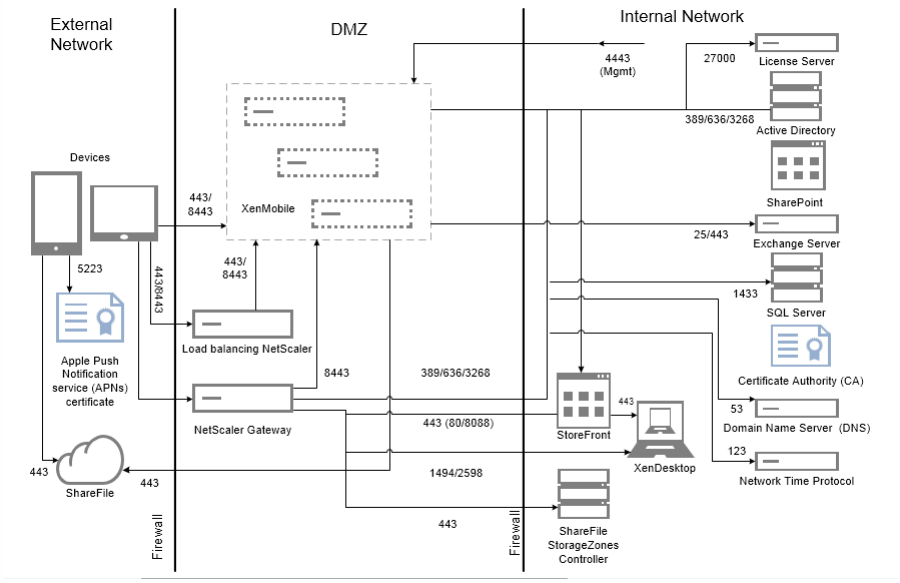
	Standalone	Standalone	3 Node Cluster	6 Node Cluster
Expected # of Devices	1000	10000	30000	45000
Actual AG Logins	1000	9998	29997	44991
Actual Enumerations	999	9998	29854	44990
Over All Error %	0.010	0.121	0.432	0.678

The error percentage in the preceding figure includes the overall error experienced considering requests corresponding to every operation and is not limited to logons. The error percentage is within the acceptable limit of 1% for each test run as defined in Exit Criteria.

The following figure shows the reference architecture for a small scale deployment. It is a standalone architecture that supports up to 10,000 devices.



The following figure shows the reference architecture for an enterprise deployment. It is a clustered architecture with SSL offload for MAM over HTTP that supports 10,000 or more devices.



Test Methodology

The tests were run against XenMobile Enterprise to establish benchmarks. In an effort to target both small and large scale deployments, 1,000 to 60,000 devices were used in the measurements.

Workloads were created to simulate real-world use cases. These workloads were run for each test to study the effect on enrollment and logon rates. The objective of the tests was to obtain an optimal logon rate that was within the acceptable margin of error as outlined in Exit Criteria. Logon rates are a critical factor in determining the hardware configuration recommendations for the infrastructure components.

The On-boarding (FTU) workload logon requests included auto discovery, authentication, and device registration operations. Application subscription, installation, and launch operations were uniformly distributed throughout the test period. This provided the best real-world simulation of user actions. At the conclusion of the test, the session was logged out. The Existing User workload logon requests included only authentication requests.

Workloads

User workloads are defined as follows:

User sessions/devices	Includes NetScaler Gateway logons, enumerations, device registration, and so on for each session.
Worx Store launches	Users launch Worx Store multiple times and each time they subscribe to or install more than one app regardless of whether it is a mobile app (web/SaaS/MDX) or a Windows app (HDX).
Web/SaaS app SSO per device	Accounts for the launch sequence of web/SaaS apps up to the point where XenMobile completes the SSO and returns the actual app URL. Traffic was not sent to actual apps.
MDX app downloads per device	Counts of the number of MDX app downloads (this can happen across Worx Store launches). For iOS, this also includes the automation of app installation from Apple ITMS, which leverages the new token/tms service APIs on NetScaler Gateway.

Notes and Assumptions

The following scenarios are not covered as part of the scalability tests. These scenarios would be considered for future enhancements in scale tests:

- Package deployment is not tested.
- Windows platform is not tested.

Policy push is tested for iOS and Android devices.
Each XenMobile supports a maximum of 10,000 connections simultaneously.

Tests were run in ideal conditions on LAN to ignore network latency issues. In a real world scenario, the scalability also depends on the user bandwidth available, especially for app downloads.

Reconnect Tests

Reconnect tests were done separately from First Time Use and Returning User Scenario tests.

Reconnect tests were run for up to 15,000 devices.

The reconnect rate supported for Android is 17 devices per second. The reconnect rate for iOS is 8 devices per second. In order to acheive this, maxThread count was ser to 1000 in the /opt/sas/tomcat/conf/server.xml file.

TO BE ADDED: INFORMATION ON RECOMMENDED DEVICE RECONNECTION POLICIES

On-Boarding (FTU) Workload

The On-boarding (FTU) workload is defined as the first time a user accesses the XenMobile environment. Operations included in this workload were:

- Auto discovery
- Enrollment
- Authentication
- Device registration
- Application delivery (web, SaaS, and mobile MDX apps)
  - App subscription (including images and icon downloads)
  - Installation of the subscribed MDX apps
- App launch (web, SaaS, and mobile MDX apps) including device status checks
- Policy push (for iOS)
- Minimal WorxMail and WorxWeb connections (VPN tunnels) — two connections
- Installation of required apps through XenMobile

The workload parameters are defined by the following table:

Devices	Device registrations	Enumerations	Apps enumerated per device	WorxStore launches per device	Web/SaaS SSO per device	MDX app downloads per device	Required app downloads triggered through XenMobile server	Policies pushed per device (iOS)
1000	1000	1000	50	4	40	10	2	20
10000	10000	10000	50	4	40	10	2	20
30000	30000	30000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

Existing Users with Worx Only Connections Workload

The following table shows the existing users (with Worx only connections) workload. This workload simulated a user using WorxMail and WorxWeb apps. This simulation was used to measure the NetScaler Gateway scalability within the XenMobile configuration. This is achievable because by only using these two Worx apps, the network is under minimal load. For the WorxWeb app, the user is accessing internal web sites which do not trigger the XenMobile server SSO. Operations in this mode included:

- Authentication (NetScaler Gateway and XenMobile)
- WorxMail and WorxWeb connections (VPN tunnels) — four connections

The following table shows the workload parameters for existing users.

Devices	Enumerations	Apps enumerated per device	VPN tunnels per device[1]
1000	1000	50	3
10000	10000	50	3
30000	30000	50	3
60000	60000	50	3

1. The number of VPN tunnels corresponds to WorxMail and WorxWeb connections.

The connection profiles for WorxMail andWorxWeb are outlined in the following table:

Device connection	Connection type	Data sent per session[1]	Data received per session[1]
WorxMail Connection #1	Type 1[2]	4.1 MB	4.1 MB
WorxMail Connection #2	Type 1	6.3 MB	12.5 MB
WorxWeb Connection #1	Type 2[3]	5.2 MB	15.7 MB
WorxWeb Connection #2	Type 2	4.1 MB	3.4 MB
Total bytes transferred per session[1]		~19.7 MB	~ 40.7 MB

1. Per session: 8 hours.

2. Type 1: Asymmetric send and receive with long lived connections (that is, WorxMail with a dedicated Microsoft Exchange mailbox connection).

3. Type 2: Asymmetric send and receive with connections that close and reopen after delays (that is, WorxWeb connections).

These recommendation are based on the WorxMail and WorxWeb profiles used to automate a
"medium" workload. Modifications to the connection details affect analysis results. For example, if the number of connections per user is increased, the number of NetScaler Gateway sessions supported may be reduced.

WorxMail and WorxWeb Profiles

The profiles used for each app are intended to automate a "very heavy" workload.The following tables show the WorxMail and WorxWeb profile details.

WorxMail Profile for a Medium Workload

Messages sent per day	20
Messages received per day	80
Messages read per day	80
Messages deleted per day	20
Average message size (KB)	200

WorxWeb Profile for Medium Workload

Number of web apps launched	10
Number of web pages opened manually	10
Average number of request–response pairs per web app	100
Average size of request (bytes)	300
Average size of response (bytes)	1000

Configuration and Parameters

The following configurations were used when running the scalability tests:

- NetScaler Gateway and load balancing (LB) virtual servers coexisted on the same NetScaler Gateway appliance.
- NetScaler session timeout configured as 60 minutes.
- A 2048-bit key was used on NetScaler Gateway for SSL transactions.

Exit Criteria

Logon rates are the foundation of this analysis. They provide the guidelines for the infrastructure components and their respective configurations. It is important to note that the logon rates take into account a margin of error that consists of the following:

- Invalid responses
  - A response with status code 401/404 instead of 200 is considered invalid.
- Request time-outs
  - A response is expected within 120 seconds.
- Connection errors
  - A connection reset occurs.
  - An abrupt connection termination occurs.

The logon rate is acceptable if the overall error rate is less than 1 percent of the total requests that are sent from a given device. The error rate includes errors corresponding to each individual workload operation, as well as the physical performance of the infrastructure component, such as CPU and memory exhaustion.

Software and Hardware Details

The following table lists the XenMobile infrastructure software used for these tests.

Component	Version
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824

External database	Microsoft SQL Server 2014

The scalability tests were run on a XenServer platform as outlined in the following table.

Vendor	Genuine Intel
Model	Intel Xeon CPU — E5645 @ 2.40 GHz (CPUs = 24)

This includes the infrastructure core services (for example, Active Directory, Windows Domain Name Service (DNS), Certificate Authority, Microsoft Exchange, and so on), as well as the XenMobile components (XenMobile virtual appliance and the NetScaler Gateway VPX virtual appliance, where applicable).

About XenMobile Server 10.3.5

Jan 05, 2017

> **Note**
>
> Citrix supports the current version of XenMobile Server and the prior two versions. We keep the product documentation for versions earlier than those versions as PDFs in the Archive List of Legacy Documents.
>
> For product documentation on the current release, see XenMobile Server.

You can directly upgrade to XenMobile 10.3.5 in the XenMobile console, from the following releases:

- XenMobile 10.3 Rolling Patch 1
- XenMobile 10.3
- XenMobile 10.1 Rolling Patch 4
- XenMobile 10.1

To perform the upgrade, you use xms_10.3.5.354.bin. In the XenMobile console, click the gear icon in the upper-right corner of the console and then click **Release Management**. Click **Upgrade** and then upload the xms_10.3.5.354.bin file. For more information about upgrades in the console, see Upgrading XenMobile.

To complete a new installation of XenMobile 10.3.5, see Installing XenMobile.

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.

> **Note**
>
> Starting with version 10.4, Worx Mobile Apps are renamed XenMobile Apps. Most of the individual XenMobile Apps are renamed as well. For details, see About XenMobile Apps.

What's New in XenMobile 10.3.5

XenMobile 10.3.5 provides bug fixes and the following new features.

XenMobile Server 10.3.5 cloud updates

Your Cloud Services team can update your XenMobile Server cloud deployment from version 10.3 to 10.3.5 with zero downtime.

Dynamic permissions for Android M

You can allow Android M users to enable or block four types of permissions. When users enroll in Worx Home, they will see a series four messages asking them to allow or deny Worx Home the following permissions:

- Access to device information for Worx Home to function properly.
- The ability to make and manage phone calls.
- Access to photos, media, and files on the device.
- Access to the device's location.

Touch ID authentication in iOS

With this release, you can allow iOS users to re-authenticate to Worx Home now as well as the Worx apps using Touch ID. For iOS 8 and iOS 9 devices, when single sign-on is enabled for Worx Home and Touch ID is enabled, this combination replaces the use of a PIN. Users will still have to enter a PIN whenever online authentication through NetScaler Gateway is required. This is required in the following instances:

- The user's session has expired.
- The user reboots the device.
- Worx Home is not currently running and the user launches it or an MDX app.

Enrollment profiles

You can now create enrollment profiles for Android and iOS devices in the new **Configure > Enrollment Profiles** page in the XenMobile console. An enrollment profile applies to all server modes. You can create multiple enrollment profiles and associate them with different delivery groups.

Note: The **Enrollment Profiles** page does not apply to Windows devices. For information about enrolling Windows devices, see Windows Devices.

Changes in device limits per user

You previously set the device limit per user through the Server Property **Number of Devices Per User**. That server property is now deprecated. You now configure the device limit in the new **Configure > Enrollment Profiles** page. Previously, you could limit the number of devices only for MDM. Now, you can also limit the number of devices for MAM.

By default, the number of devices a user can enroll is unlimited. For more information, see Device Enrollment Limit.

Language support

XenMobile 10.3.5 provides support in the WorxStore for Hebrew and traditional Chinese.

New MAM-only mode

XenMobile 10.3.5 introduces a new MAM-only Server Mode. To distinguish the prior and new MAM modes, Citrix documentation refers to the new mode as "MAM-only" and refers to the prior MAM mode as "legacy MAM mode." While the legacy MAM functionality is the same as before, Citrix won't enhance it in future releases.

MAM-only mode is in effect when the Server Mode property of XenMobile is **MAM**. Devices register in MAM mode.

Legacy MAM functionality is in effect when the Server Mode property of XenMobile is **ENT** and users choose to opt out of device management. Devices register in MDM+MAM mode. In MAM+MDM mode, users who opt out of MDM management continue to receive the legacy MAM functionality whether or not you upgrade to XenMobile 10.3.5.

Note: Previously, setting the Server Mode property to **MAM** had the same effect as setting it to **ENT**: Devices registered in MDM+MAM mode; users who opted out of MDM management received the legacy MAM functionality.

Advantages of MAM-only mode includes additional encryption (not just device passcode), mobile VPN, and better end-user

privacy -- which make MAM-only mode suitable for BYO devices.

If your XenMobile server mode is currently MAM, you can upgrade to the new MAM-only mode to benefit from the following features that were previously available only for MDM. These features are not available for Windows Phone.

- **Certificate-based authentication**
  MAM-only mode supports certificate-based authentication. Users will experience continued access to their apps even when their AD password expires. If you choose to switch to certificate-based authentication for MAM devices, you must configure your NetScaler Gateway. By default, in the XenMobile **Settings > NetScaler Gateway**, **Deliver user certificate for authentication** is set to **Off**, meaning that user name and password authentication is used. You must change that setting to **On** to enable certificate authentication.
- **Self Help Portal**, to enable end users to perform their own app lock and app wipe. Those actions apply to all apps on the device. You can configure the App Lock and App Wipe actions in **Configure > Actions**.
- **All enrollment modes**, including High Security, Invitation URL, and Two Factor, configured through **Manage > Enrollment**.
- **Device registration limit** for Android and iOS devices. The Server Property **Number of Devices Per User** has moved to the new **Configure > Enrollment Profiles** page and now also applies to the new MAM-only mode.
- **MAM-only APIs.** For MAM-only devices, you can call REST services by using any REST client and the XenMobile REST API to call services that are exposed through the XenMobile console.
- The MAM-only APIs available in this release enable you to:
  - Send an invitation URL and one-time PIN
  - Issue app lock and wipe on devices

> ### Important
>
> To use the new MAM-only mode, you must configure XenMobile as described in this article and your users must re-enroll their devices. Be sure to provide users with the XenMobile Server FQDN they'll need for enrollment.
>
> In the new MAM-only mode, just like the ENT mode, devices enroll using the XenMobile Server FQDN. (In the legacy MAM mode, devices enroll using the NetScaler Gateway FQDN.)

How this upgrade affects enrolled devices

The following table summarizes how the new features in XenMobile 10.3.5 affects enrolled devices.

For devices currently enrolled as:	XenMobile 10.3.5 provides	Administrator tasks	User tasks
MDM • Server Mode = MDM MDM+MAM	• Bug fixes • New features	Install XenMobile 10.3.5	None

• Server Mode = ENT • Users opted for device management	• Bug fixes • New features	Install XenMobile 10.3.5	None
MAM • Server Mode = ENT • Users opted out of device management	• Bug fixes • New features Note: In this use case, devices enroll in the legacy MAM mode. If you want to provide those users with the new MAM functionality, set up a new XenMobile server for them.	Install XenMobile 10.3.5	None
MAM • Server Mode = MAM	• Bug fixes • New features • Optional upgrade to new MAM-only mode	To continue using the legacy MAM functionality: Install XenMobile 10.3.5 To upgrade to MAM-only mode: 1. Install XenMobile 10.3.5. 2. See MAM-only Mode Configuration Overview, next, for additional, required configuration.	None Re-enroll devices

MAM-Only Mode Configuration Overview

MAM-only mode refers to the MAM Server Mode when used with Enterprise or Advanced licenses. MAM-only mode differs from *MAM+MDM mode*, which is in use if your XenMobile Server has a Server Mode of ENT. In MAM+MDM mode, users who opt out of MDM management are provided the legacy MAM functionality whether or not you upgrade to XenMobile 10.3.5.

> **Important**
>
> The legacy MAM functionality works the same as for prior releases and will not be enhanced in future releases.

The following table summarizes the Server Mode setting to use for a particular license type and desired device mode:

Your licenses are for this edition	You want devices to register in this mode	Set the Server Mode property to

ENT / ADV / MDM	MDM mode	MDM
ENT / ADV	MAM mode (also referred to as MAM-only mode)	MAM
ENT / ADV	MDM+MAM mode	ENT Users who opt out of device management will operate under the legacy MAM mode.

You must configure MAM-only mode *only* if:

- Your XenMobile server currently has a **Server Mode** of **MAM** and you want to change to the new MAM-only mode to benefit from the additional features.
- You want to set up a XenMobile Server to provide MAM-only functionality to all users who connect to that server.

The general configuration steps for MAM-only mode are as follows:

1. Install or upgrade to XenMobile 10.3.5.
2. On the **Manage > Devices** page, check the **Server Mode**. If the **Server Mode** is **MDM** or **ENT**, do not perform the steps in this procedure, because doing so will result in a configuration that does not support device management.
3. Open ports 8443 and 443 on your XenMobile server and firewall to the Internet so devices can connect to XenMobile server. Enrollment must occur on your XenMobile server.
4. If you are upgrading a server that already has the **Server Mode** set to **MAM**, skip to the next step. If you are performing a new installation of XenMobile 10.3.5, the XenMobile server has a **Server Mode** of **ENT** by default. To enable MAM-only mode, you must set the Server Property **Server Mode** to **MAM**. For information, see Configuring the Server Mode for MAM-only.
5. If you want to use certificate-based authentication, configure XenMobile and your NetScaler Gateway to support certificate-based authentication. By default, in the XenMobile **Settings > NetScaler Gateway**, **Deliver user certificate for authentication** is **Off**, meaning that user name and password authentication is used. You must change that setting to **On**. For configuration details, see Certificate Authentication for MAM-Only Mode.
6. When choosing or setting up a notification template for use with MAM-only mode, be aware that SMTP is the only supported method for sending enrollment invitations.
7. If your users are being upgraded to the new MAM-only mode, provide them the XenMobile server FQDN and let them know that they must re-enroll.
   In the new MAM-only mode, just like the ENT mode, devices enroll using the XenMobile Server FQDN. (In the legacy MAM mode, devices enroll using the NetScaler Gateway FQDN.)

The following table summarizes the differences between the legacy MAM functionality (XenMobile 10.3 and XenMobile 10.3.5) and the new MAM-only mode (XenMobile 10.3.5).

Enrollment Scenarios and Other Features	**XenMobile 10.3 Legacy MAM (server mode is ENT)**	**XenMobile 10.3.5 Legacy MAM (server mode is ENT)**	**XenMobile 10.3.5 MAM-only mode (server mode is MAM)**

Certificate authentication	Not supported.	Not supported.	Supported. To use certificate authentication, NetScaler Gateway is required.
Deployment requirement	XenMobile Server does not need to be directly accessible from devices.	XenMobile Server does not need to be directly accessible from devices.	XenMobile Server must be accessible from devices.
Enrollment option	Use the NetScaler Gateway FQDN or opt not to enroll.	Use the NetScaler Gateway FQDN or opt not to enroll.	Use XenMobile Server FQDN.
Enrollment methods	User name + Password	User name + Password	User name + Password, High Security, Invitation URL, Invitation URL+PIN, Invitation URL + Password, Two Factor, User name + PIN
App lock and wipe	Supported.	Supported.	Supported.
Self Help Portal options for app lock and wipe	Not supported.	Not supported.	Supported.
App wipe behavior	Apps remain on the device but are not usable. Account is deleted on the client only.	Apps remain on the device but are not usable. Account is deleted on the client only.	Apps remain on the device but are not usable. Account is deleted on the client only.
Automated actions for MAM-only users.	Not supported.	Event, device property, user property actions are supported. Installed app-based automated actions are not supported.	Event, device property, user property actions are supported. Installed app-based automated actions are not supported.
Built-in action when an AD user is deleted	Not supported.	App wipe is supported.	App wipe is supported.

Enrollment limit	Supported for MDM only; configured through a server property.	Supported; configured through an enrollment profile.	Supported; configured through an enrollment profile.
Software inventory	Supported; XenMobile lists apps installed on a device	Supported; XenMobile lists apps installed on a device	Not supported.

Reference architecture for MAM-only mode

In a MAM-only deployment of XenMobile, you can deploy a cluster of XenMobile servers in either the DMZ, or within the internal network. In each scenario, authentication occurs through NetScaler Gateway.

Note that, unlike in a XenMobile Enterprise deployment, XenMobile NetScaler Connector (XNC) and XenMobile Mail Manager (XMM) are not required.

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

Notes for MAM-only use

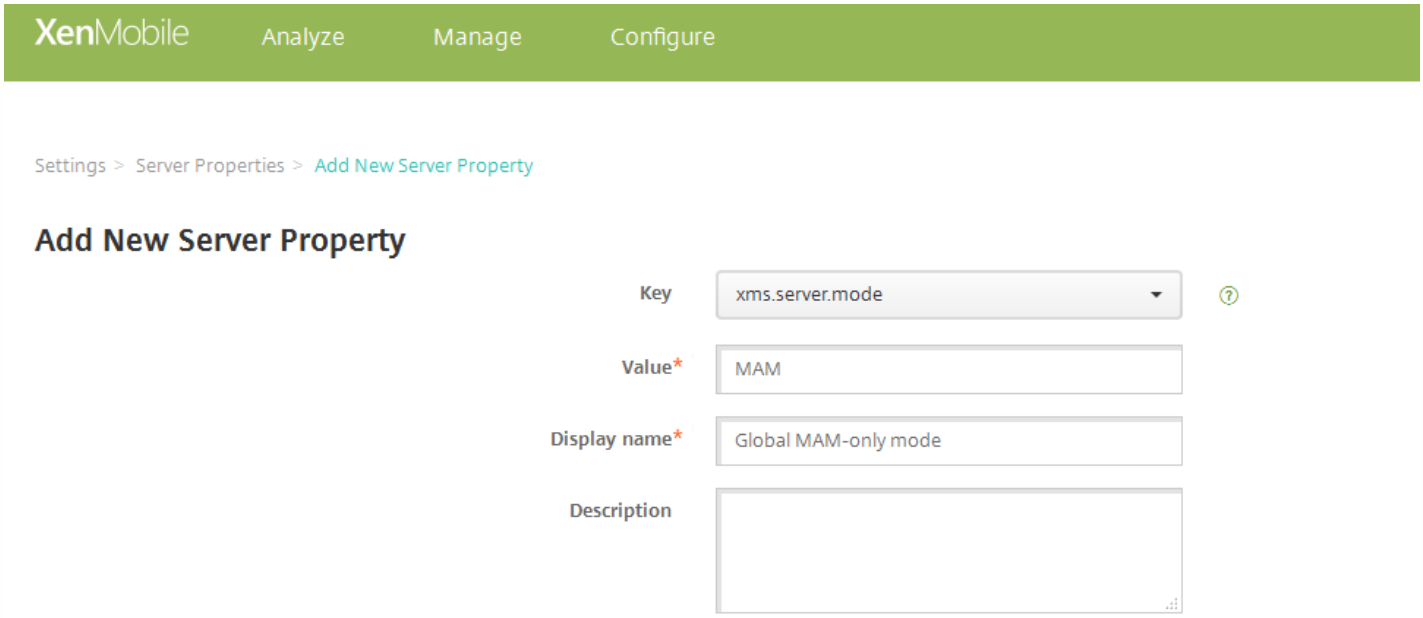
- Required apps don't install automatically. Users must manually add them from WorxStore.
- iOS users must trust the iOS developer certificate. Android users must enable the setting to install from third-party app stores.
- Users receive app update notifications only in WorxStore.
- When a user removes Worx Home or unenrolls from Worx Home, the installed apps remain on the device until the user removes them.
- MAM-only mode does not support APNs or Google Cloud Messaging.
- The XenMobile console does not include the jailbroken/rooted status of devices enrolled in MAM-only mode, however the **Block jailbroken or rooted devices** policy works for those devices.

Configuring the Server Mode for MAM-only

After a new installation, the server is in ENT mode by default. To enable MAM-only mode for XenMobile 10.3.5, configure the server as follows:

1. In the XenMobile console, click the cog icon in the upper-right corner to open the **Settings** page.
2. On the **Settings** page, click **Server Properties**.
3. Click **Add**.
4. In **Key**, click **xms.server.mode**.
5. In **Value**, enter **MAM**.
6. In **Display name**, enter a description to appear in the **Server Properties** table.

Optionally, enter a description and then click **Save**.



Important

After you set the xms.server.mode property to MAM-only, the XenMobile console still shows areas that apply to MDM mode, such as device properties. The settings will not work, however.

Certificate Authentication for MAM-Only Mode

Jan 04, 2017

Certificate authentication is available for XenMobile MAM-only mode. Certificate authentication isn't available for XenMobile ENT mode when users enroll in the legacy MAM mode. For more information about MAM-only mode, see New MAM-only mode.

To use certificate authentication in MAM-only mode, you must configure the Microsoft server, the XenMobile server, and then the NetScaler Gateway server. The following general steps are detailed 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:

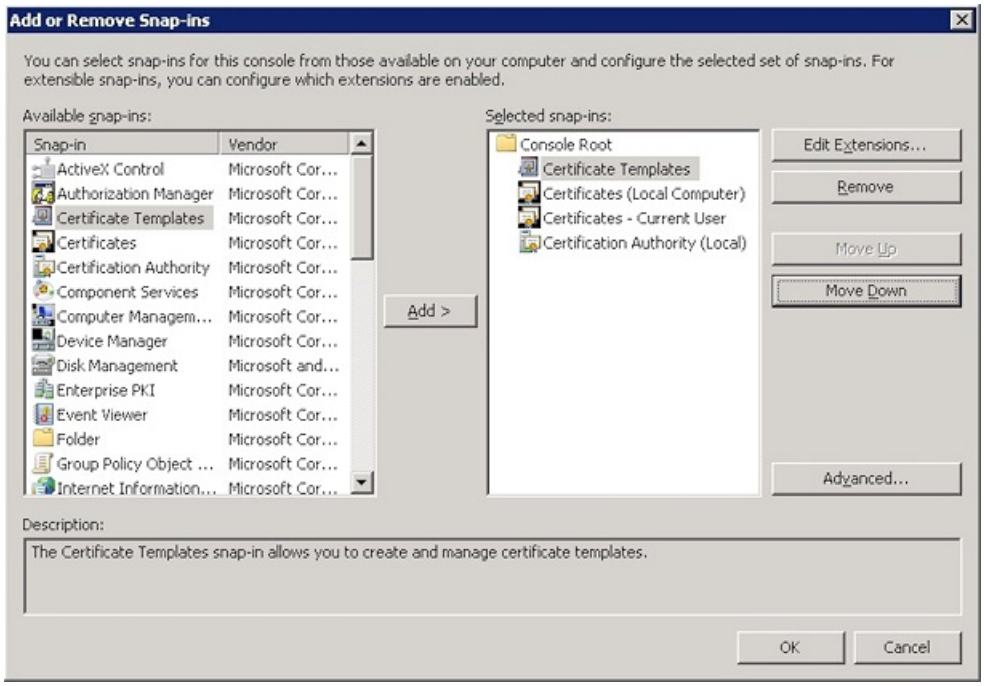
1. Configure NetScaler Gateway for XenMobile MAM-only mode certificate authentication

To add a certificate snap-in to the Microsoft Management Console

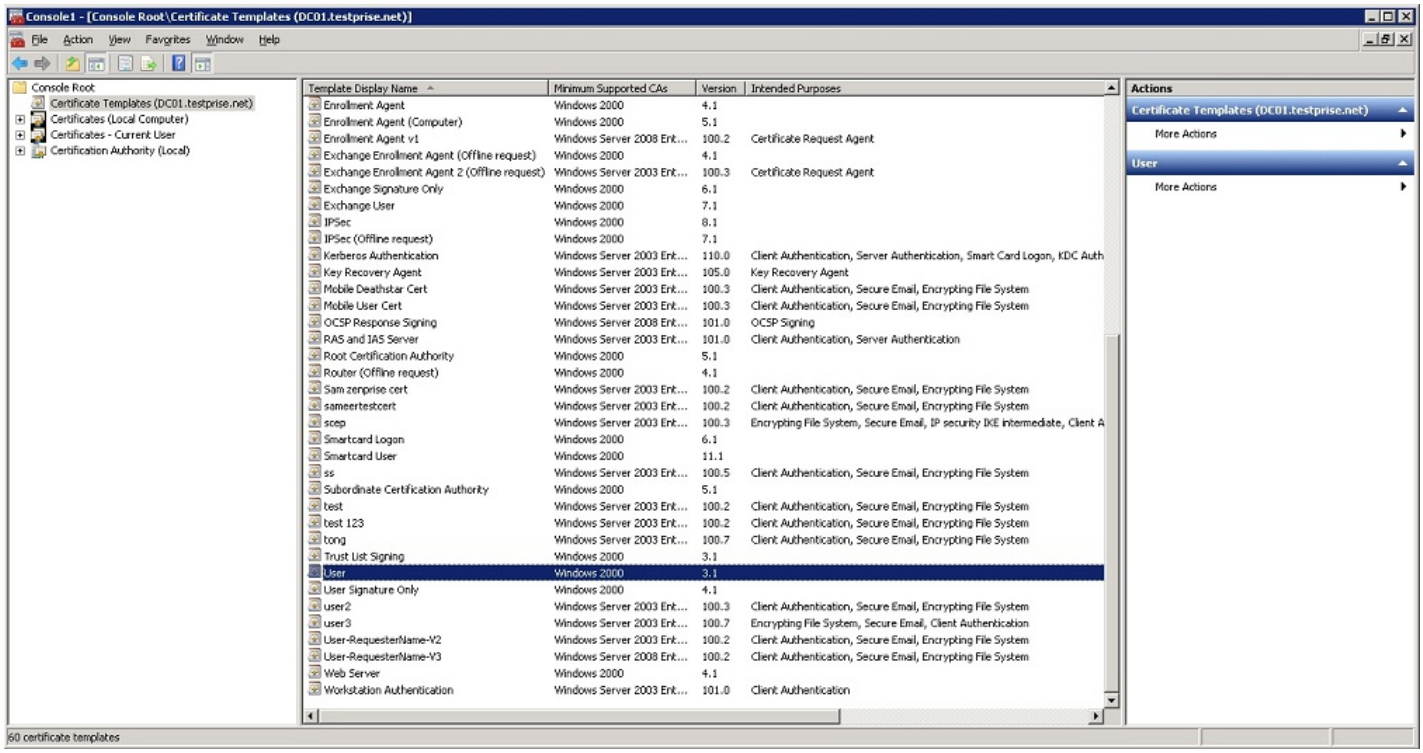
1. Open the console and then click **Add/Remove Snap-Ins**.

2. Add the following snap-ins:

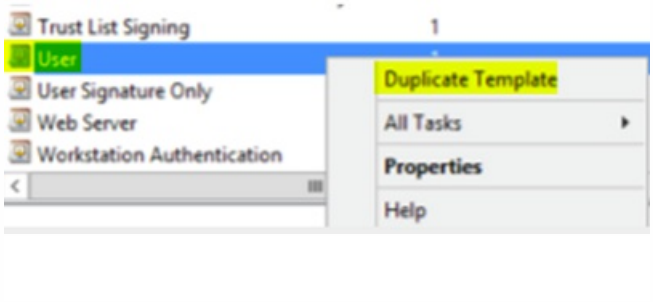
    Certificate Templates
    Certificates (Local Computer)
    Certificates - Current User
    Certificate Authority (Local)



3. Expand **Certificate Templates**.



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

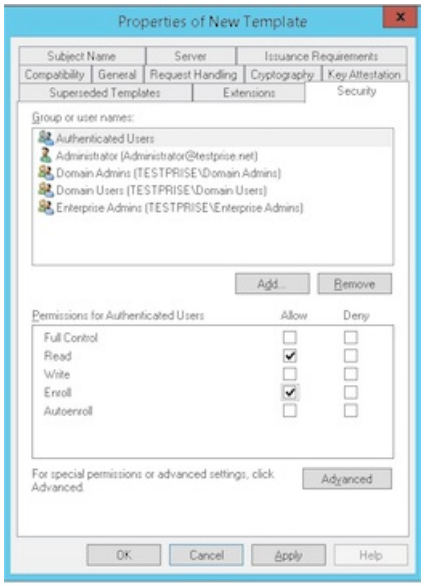


5. Provide the Template display name.

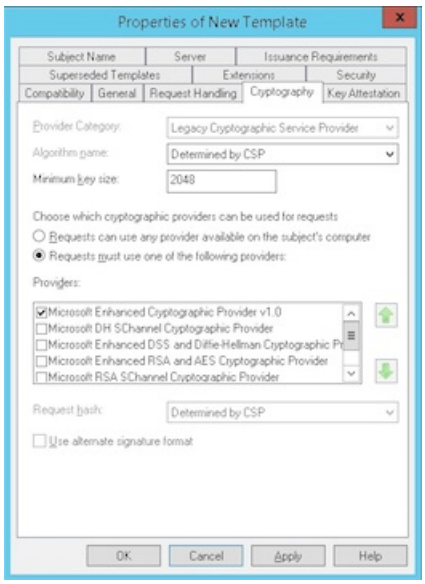
> **Important:** Do not select the **Publish certificate in Active Directory** check box unless required. If this option is selected, all user client certificates will be pushed/created in Active Directory, which might clutter your Active Directory database.

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.

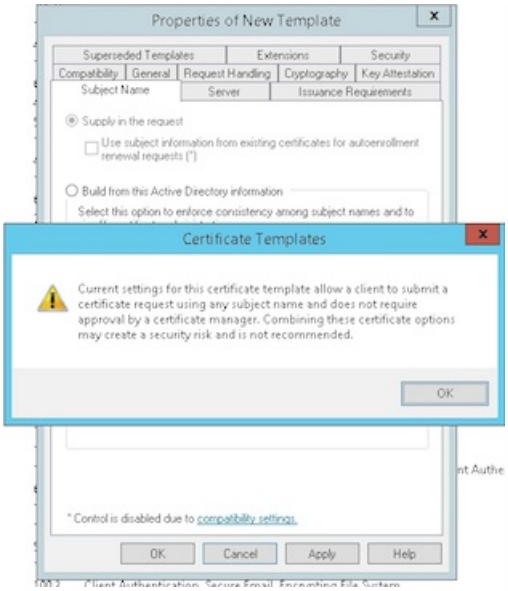
7. Under **Security**, select the **Enroll** option in the **Allow** column for the authenticated users.



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



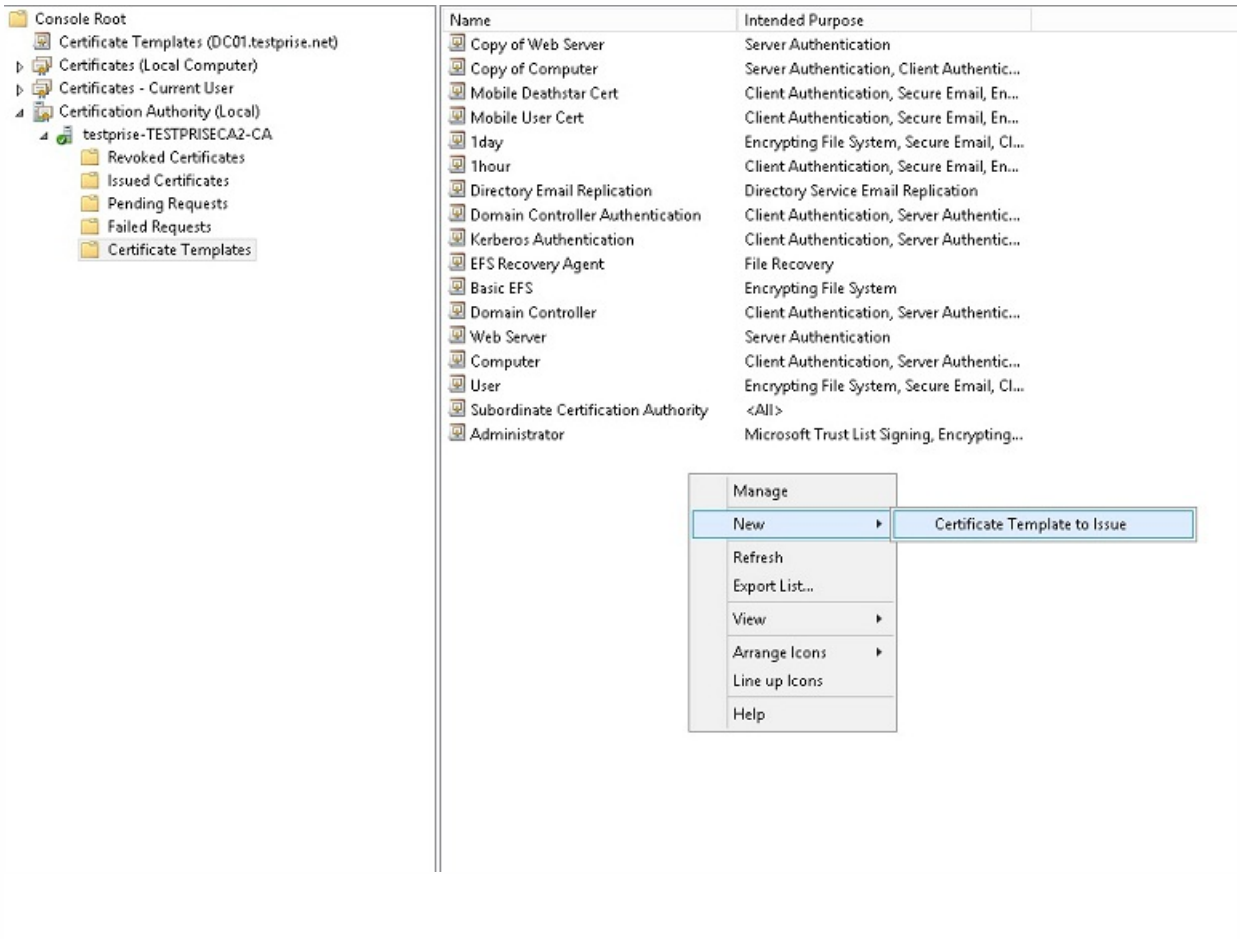
9. Under **Subject Name**, select **Supply in the request**. Apply the changes and then save.



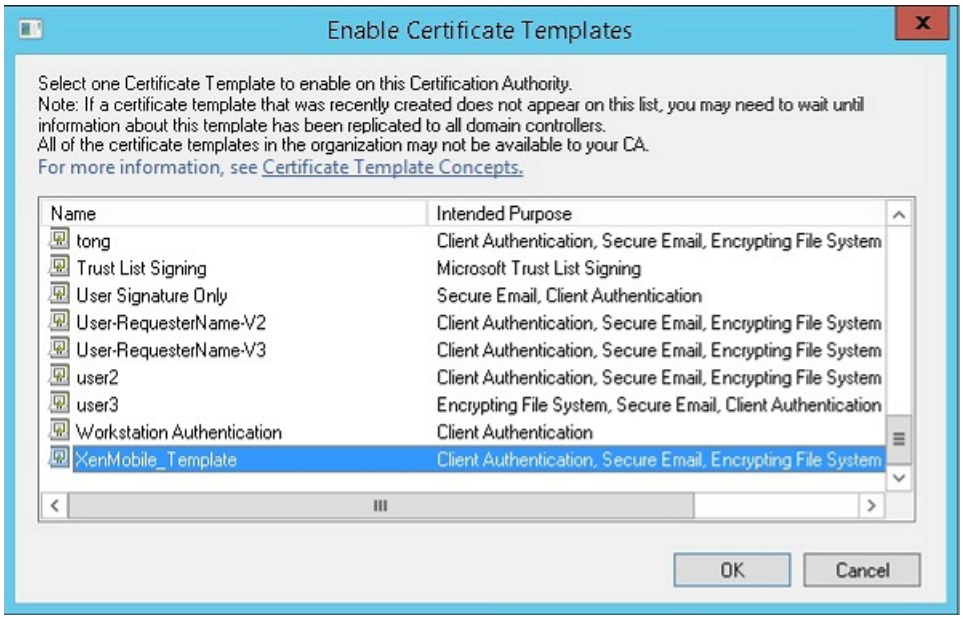
To add the template to Certificate Authority

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.

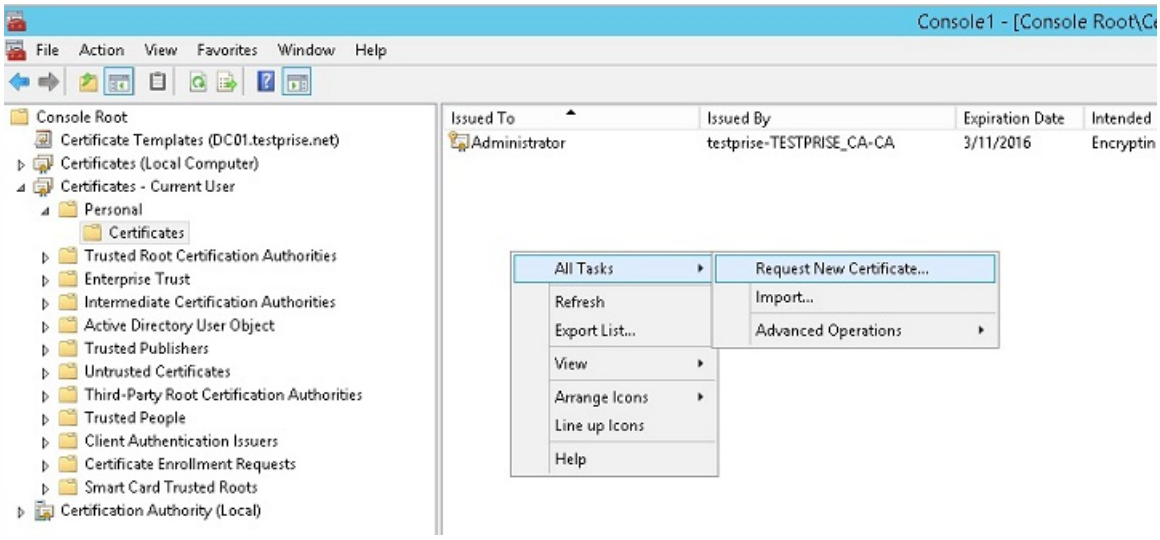


To create a PFX certificate from the CA server

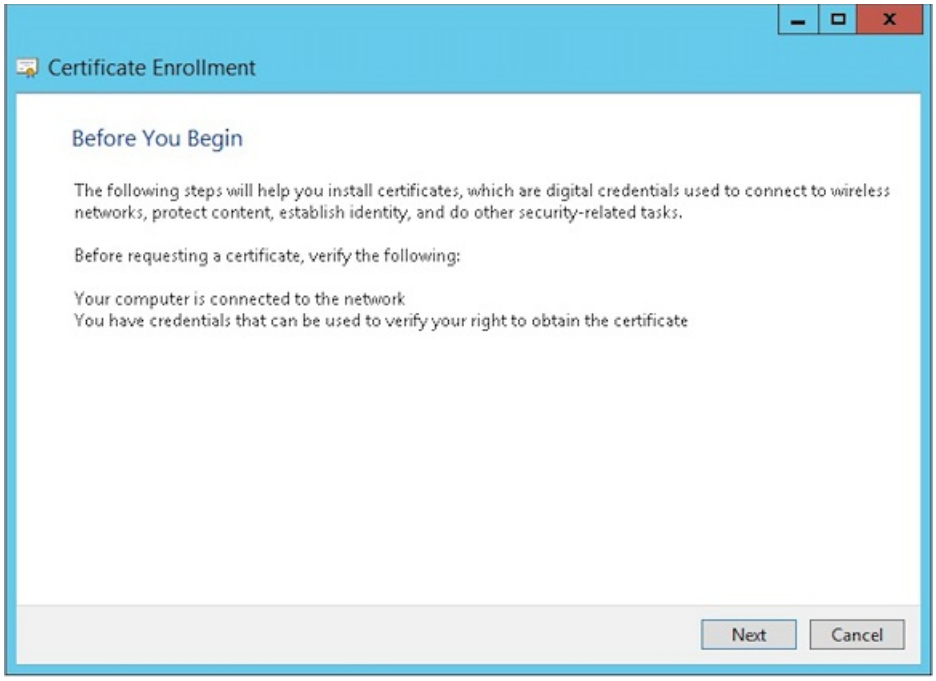
1. Create a user .pfx cert using the service account with which you logged in. This .pfx will be uploaded into XenMobile, which will request a user certificate on behalf of the users who enroll their devices.

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

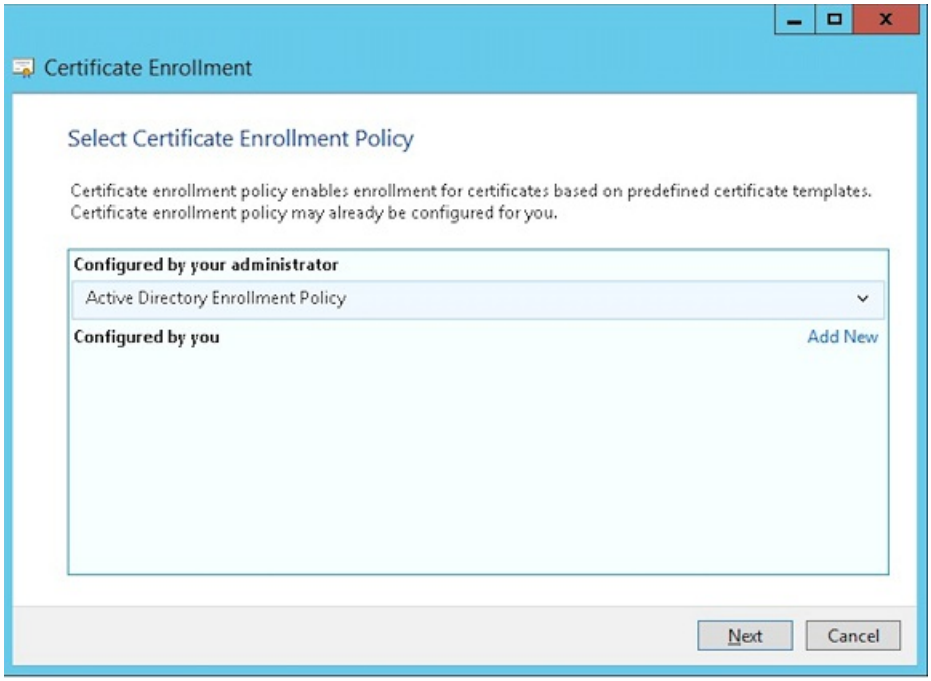
3. Right-click in the right pane and then click **Request New Certificate**.



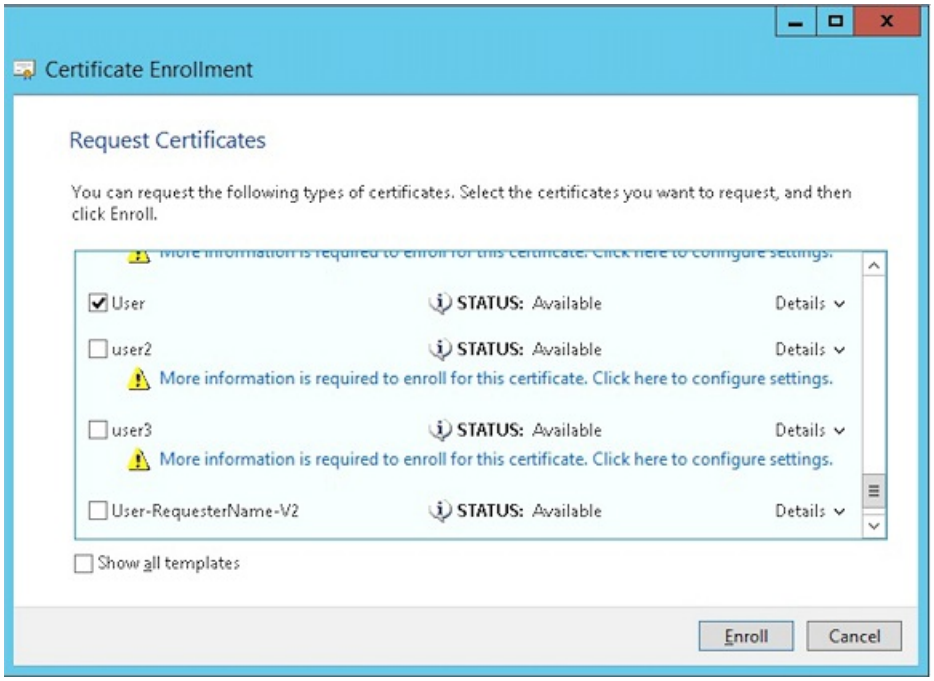
4. The **Certificate Enrollment** screen appears. Click **Next**.



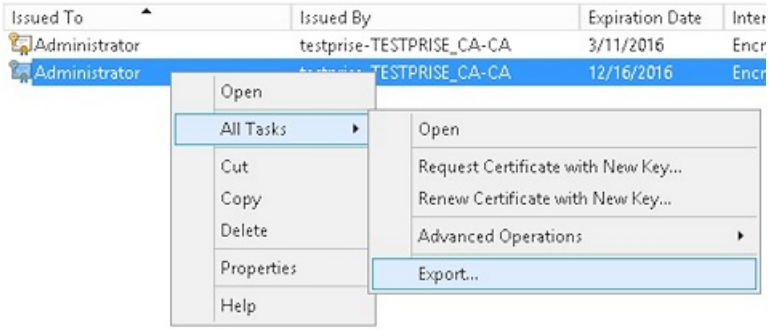
5. Select **Active Directory Enrollment Policy** and then click **Next**.



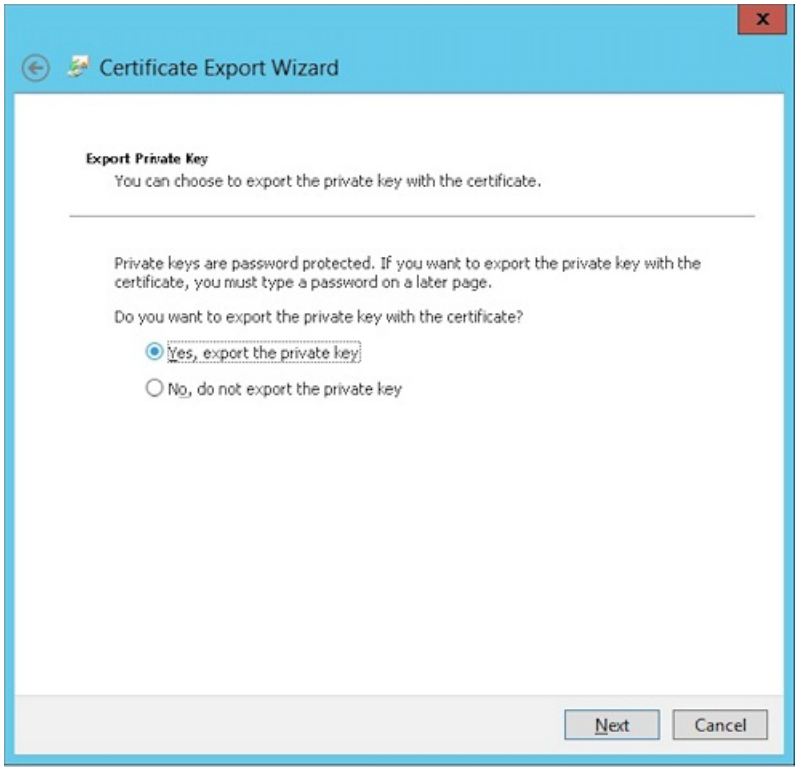
6. Select the **User** template and then click **Enroll**.



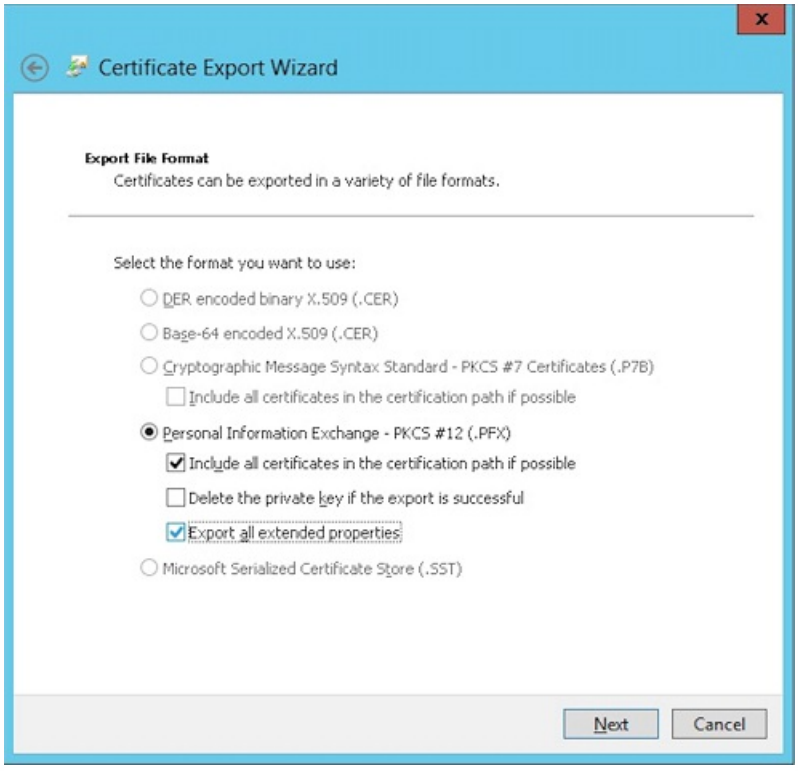
7. Export the .pfx file that you created in the previous step.



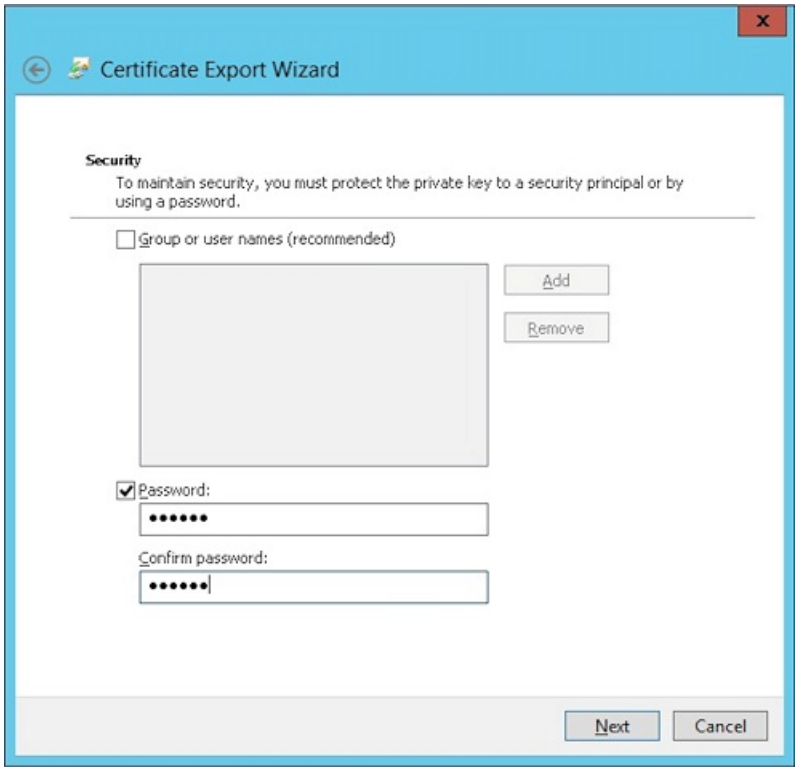
8. Click **Yes, export the private key**.



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.

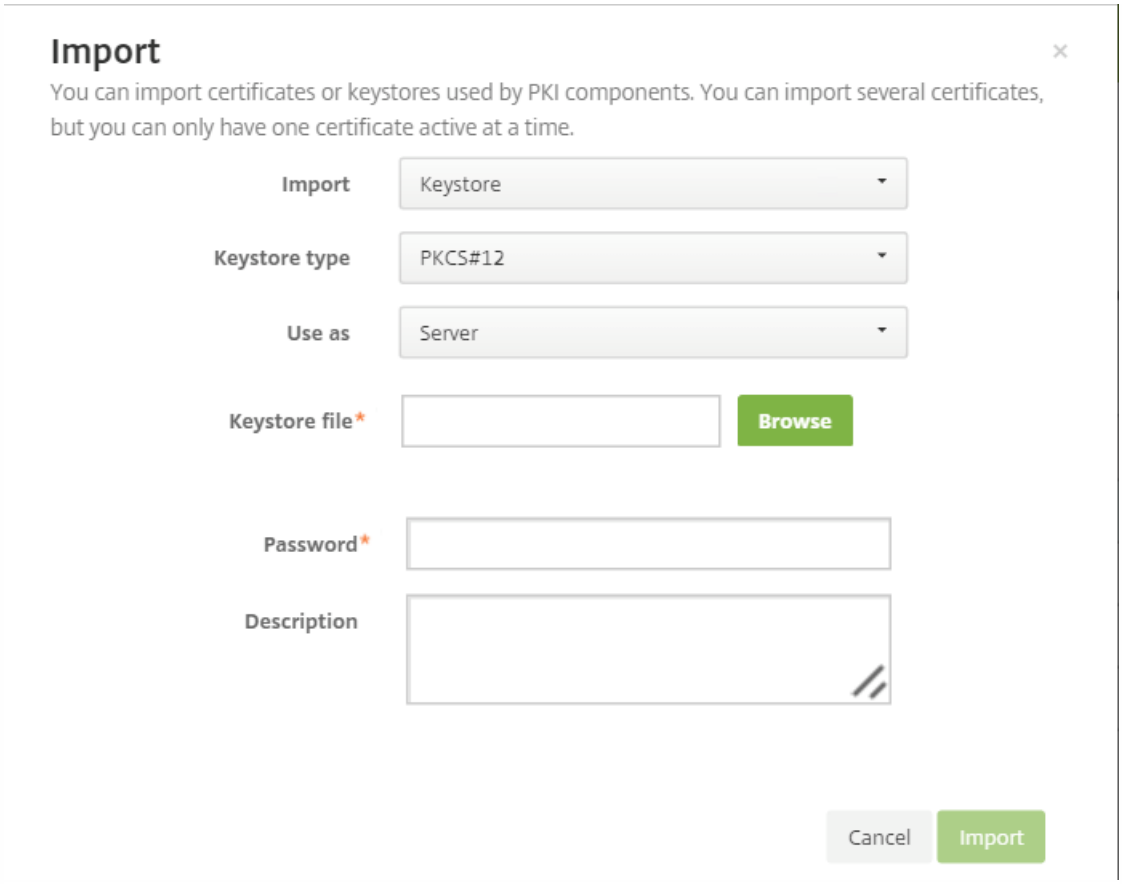
To upload the certificate to XenMobile

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.



5. Click **Import**.

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

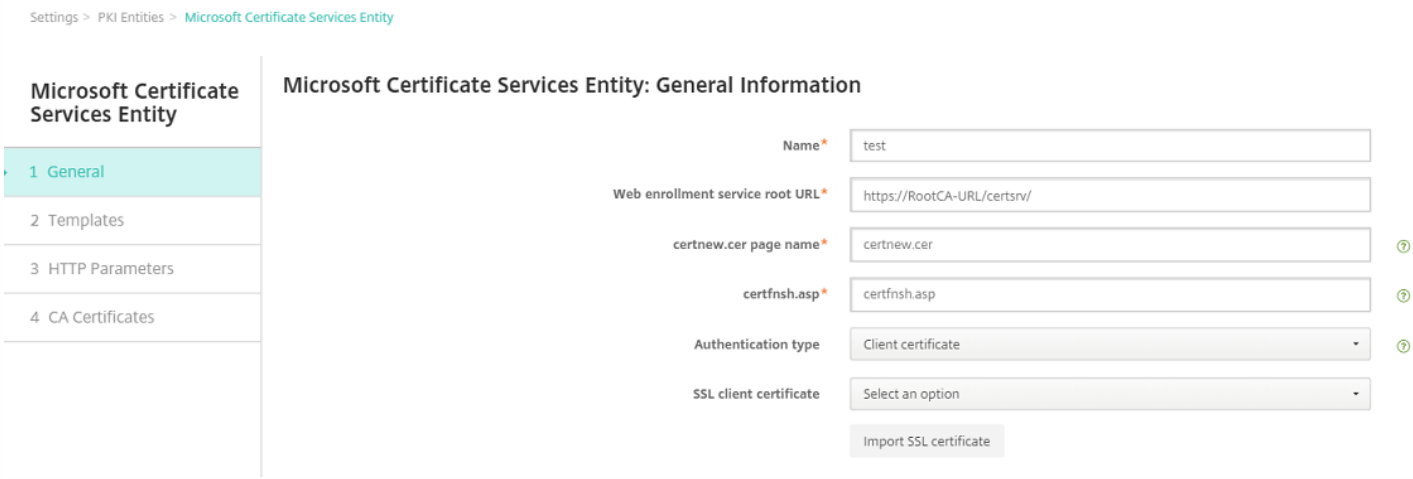
To create the PKI entity for certificate-based authentication

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

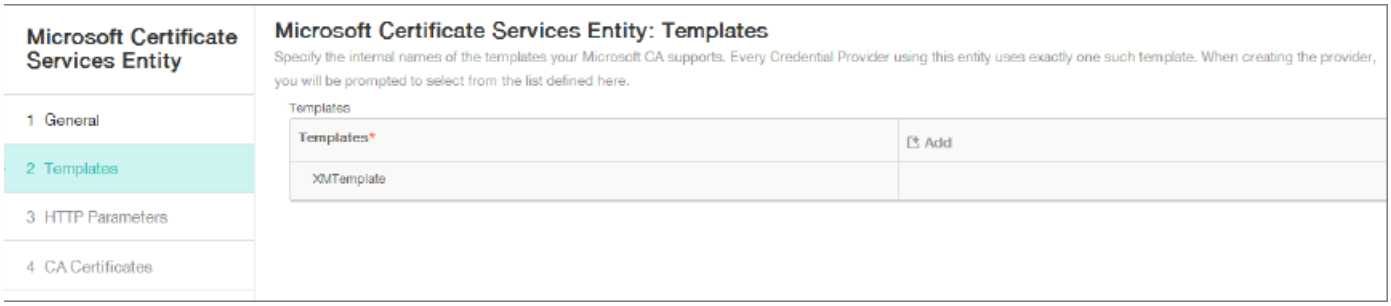
2. Click **Add** and then click **Microsoft Certificate Services Entity**. The Microsoft Certificate Services Entity: General Information screen appears.

3. Enter the following parameters:

- **Name**: Type any name
- **Web enrollment service root URL**: https://RootCA-URL/certsrv/
  Note: 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 RootCA that signed the XenMobile client certificate.

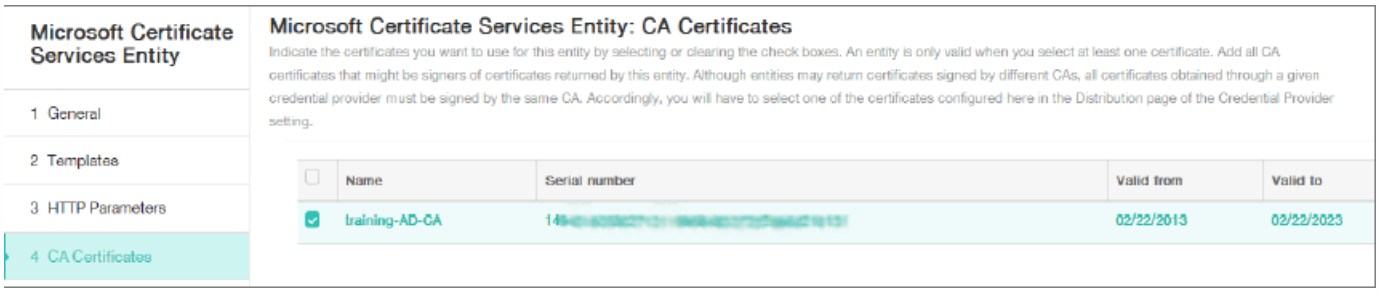


4. Under **Templates**, add the template that you created when configuring the Microsoft certificate. Be sure not to add spaces.



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

6. Select the User Certificate to be used to issue the XenMobile client certificate. This is part of the chain imported from the XenMobile client certificate.



7. Click **Save**.

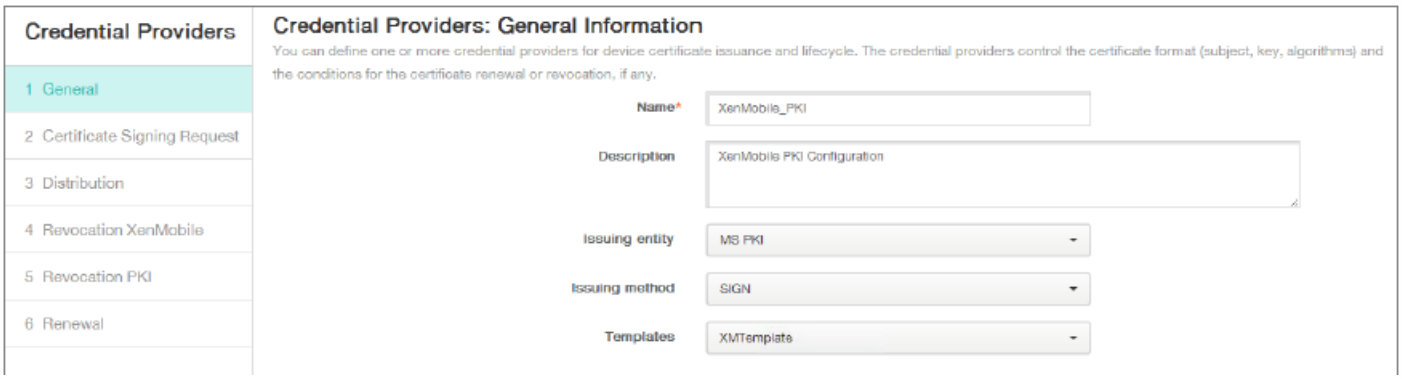
To configure credentials providers

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.



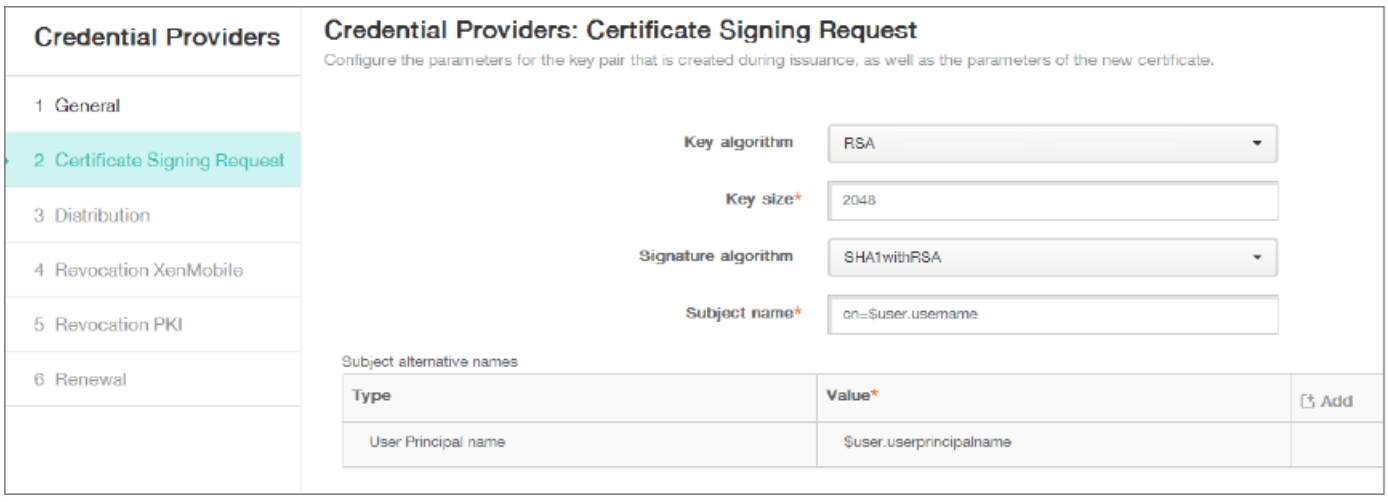
4. Next, click **Certificate Signing Request** and then enter the following parameters:

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

  The subject name references the sAMAccountName. This enables NetScaler to use the User Name field for authentication.

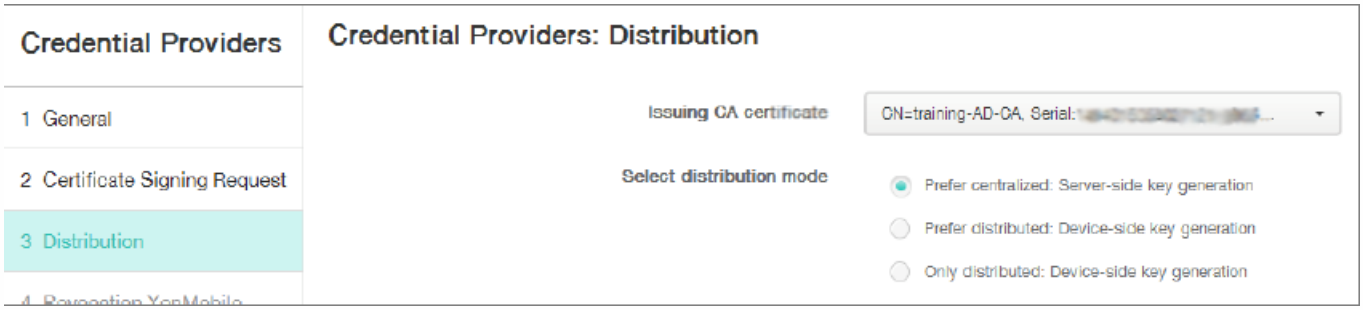
5. For **Subject Alternative Names**, click **Add** and then enter the following parameters:

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



6. 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**.

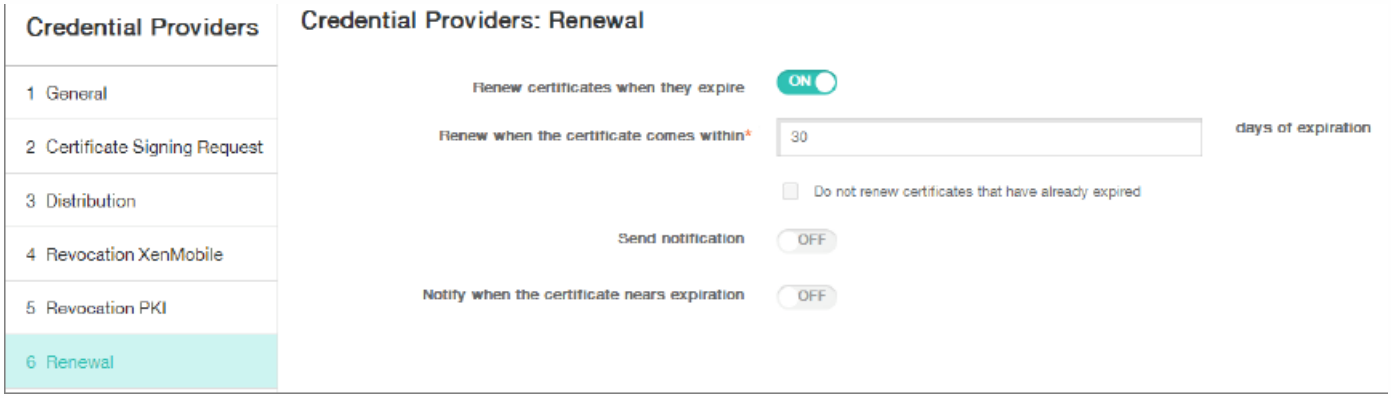


7. For the next two sections -- **Revocation XenMobile** and **Revocation PKI** -- set the parameters as required. For the purpose of this article, both options are skipped.

8. Click **Renewal**.

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

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



11. Click **Save**.

To configure 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:

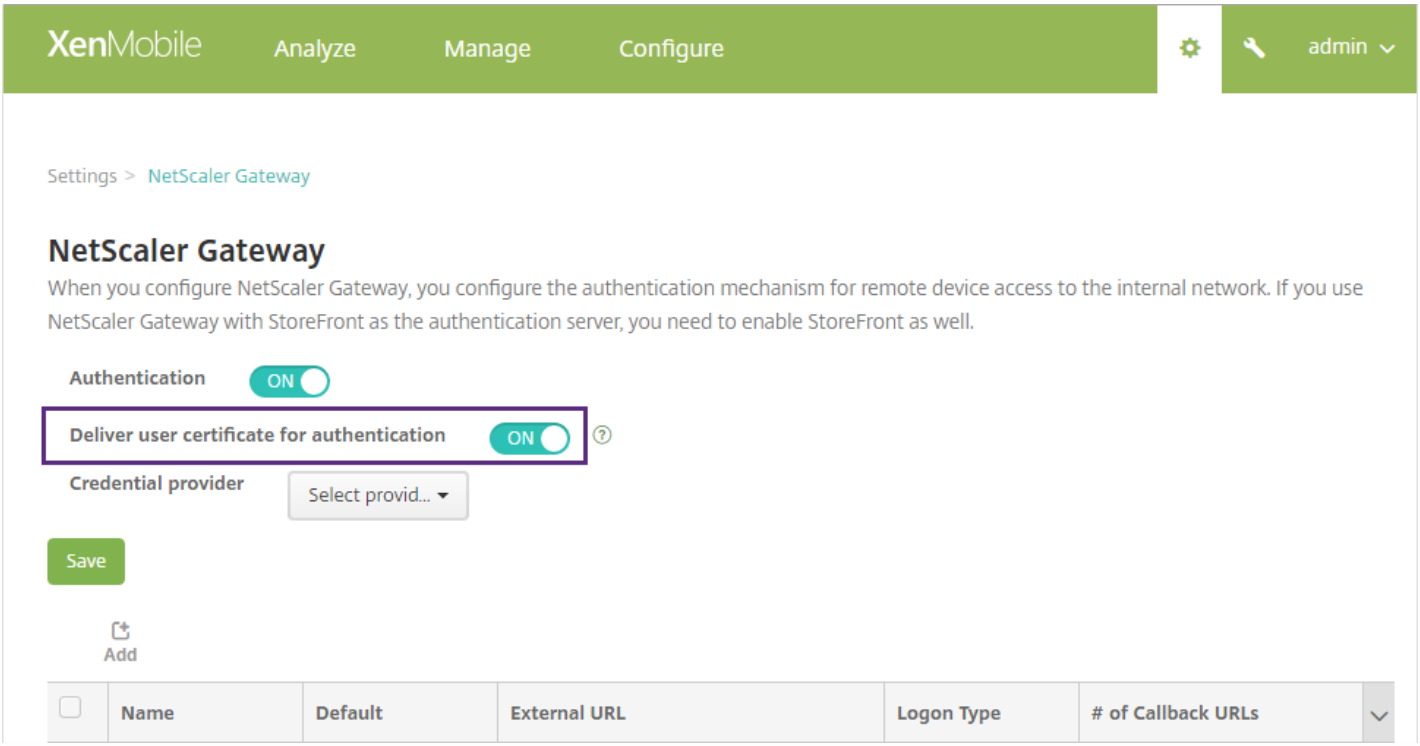
    External URL: https://YourNetScalerGatewayURL

    Logon Type: Certificate

Password Required: OFF

Set as Default: ON

4. For **Deliver user certificate for authentication**, select **On** and then click **Save**.



5. For **Credential Provider**, select a provider and then click **Save**.

To configure NetScaler Gateway for certificate authentication

Follow these steps on your NetScaler appliance to configure certificate authentication in XenMobile in MAM-only mode.

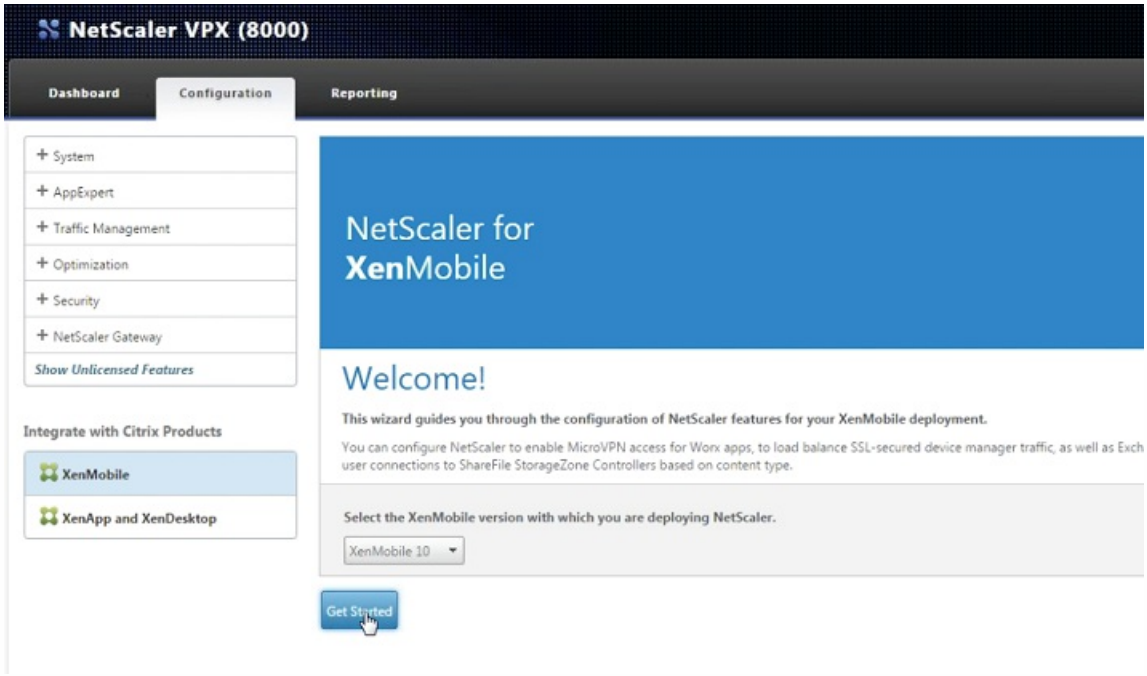
1. Log on to NetScaler.

2. Under **Configuration**, go to **Integrate with Citrix Products** and then select **XenMobile**.

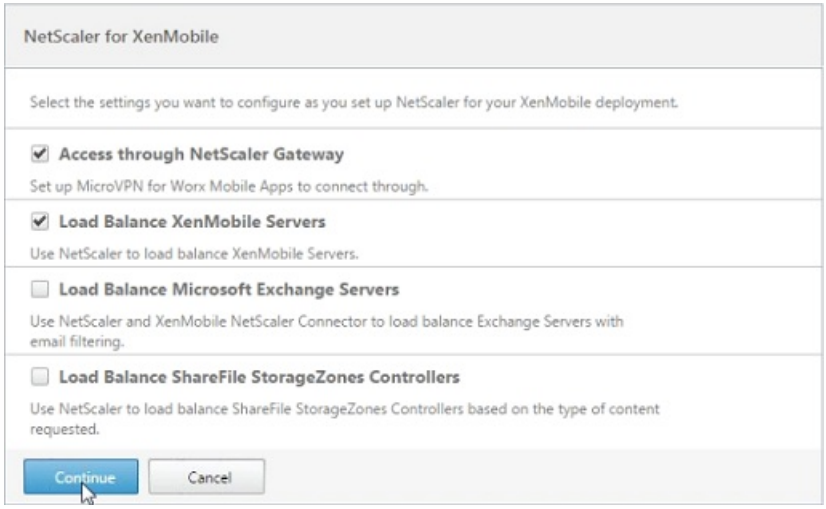
   This opens a wizard to configure NetScaler features for your XenMobile deployment.

3. Choose **XenMobile 10**.

4. Click **Get Started**.



5. On the next screen, select **Access through NetScaler Gateway** and **Load Balance XenMobile Servers** and then click **Continue**.



6. On the next screen, enter the external-facing NetScaler Gateway IP address and then click **Continue**.

   The Server Certificate for NetScaler Gateway screen appears.

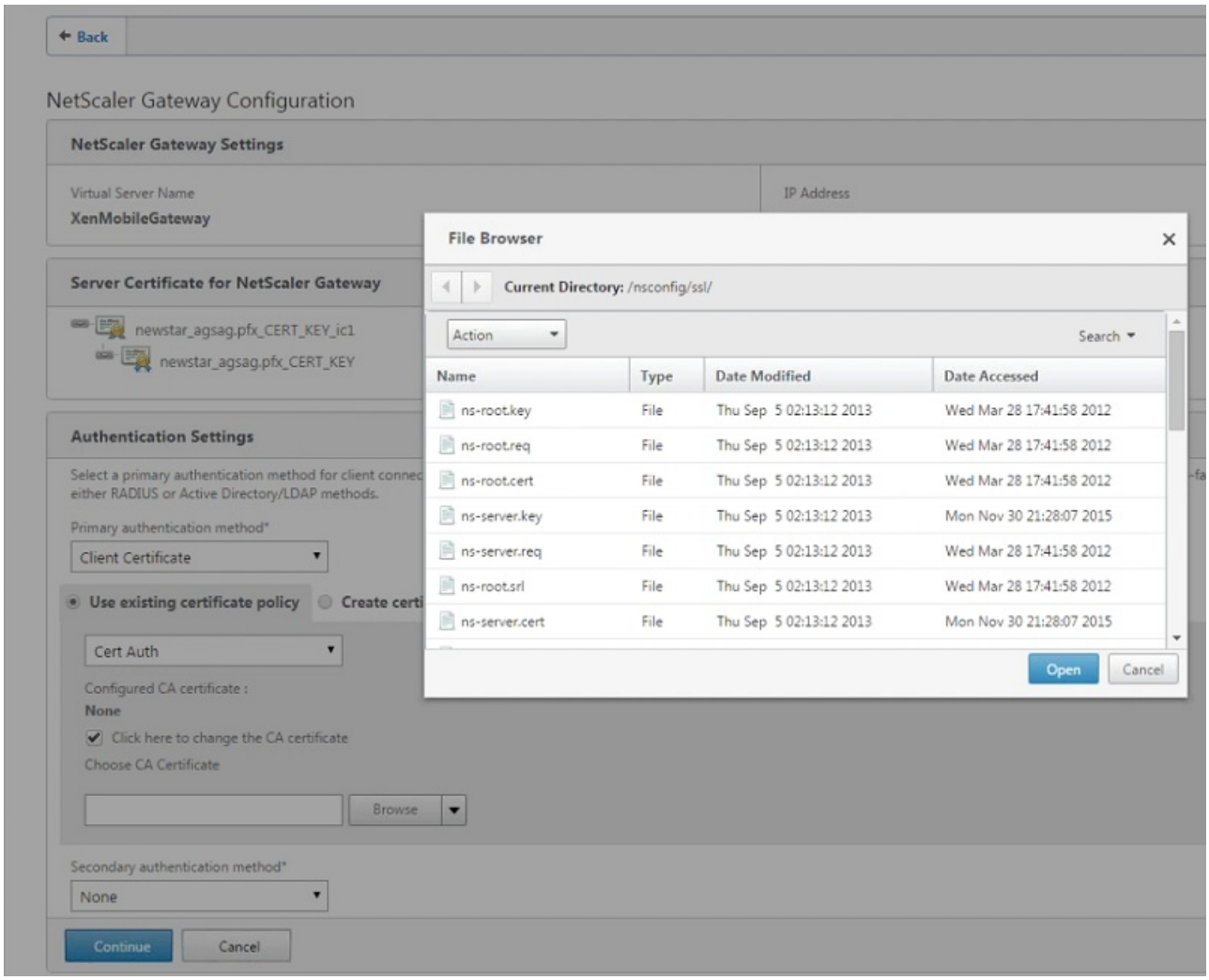
7. You will either use an existing certificate or install one. Click **Continue**.

   The **Authentication Settings** screen appears.

8. In the **Primary authentication method** field, select **Client Certificate**.

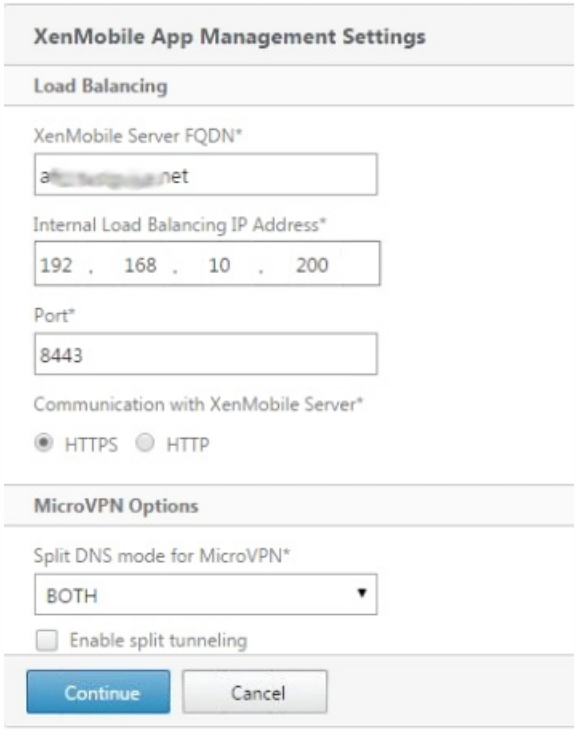
   This will automatically select **Use existing certificate policy** and **Cert Auth** in the next two fields.

9. Select **Click here to change the CA certificate** and then in the **Browse** list, navigate to the CA certificate you want.



10. Leave **Second authentication method** as **None** and then click **Continue**.
11. On the **Load Balancing** screen, enter the XenMobile server FQDN and a MAM-only internal load balancing IP address.
12. Because this is an SSL offload deployment, select **HTTP** in **Communication with XenMobile Server**.

    The **Split DNS mode for MicroVPN** field will appear as **BOTH**.
13. Click **Continue**.



14. On the **XenMobile Server Certificate** screen, choose an existing server certificate or install a new certificate. If you're running multiple XenMobile servers, you will add a certificate for each one. Click **Continue**.

15. On the **Device certificate** screen, if not already installed, you will have to export this certificate from the XenMobile console. To do so:

    a. From the console, click the gear icon in the upper-right corner to open the **Settings** screen.

    b. Click **Certificate** and then choose the CA certificate from the list.

    c. Click **Export**.

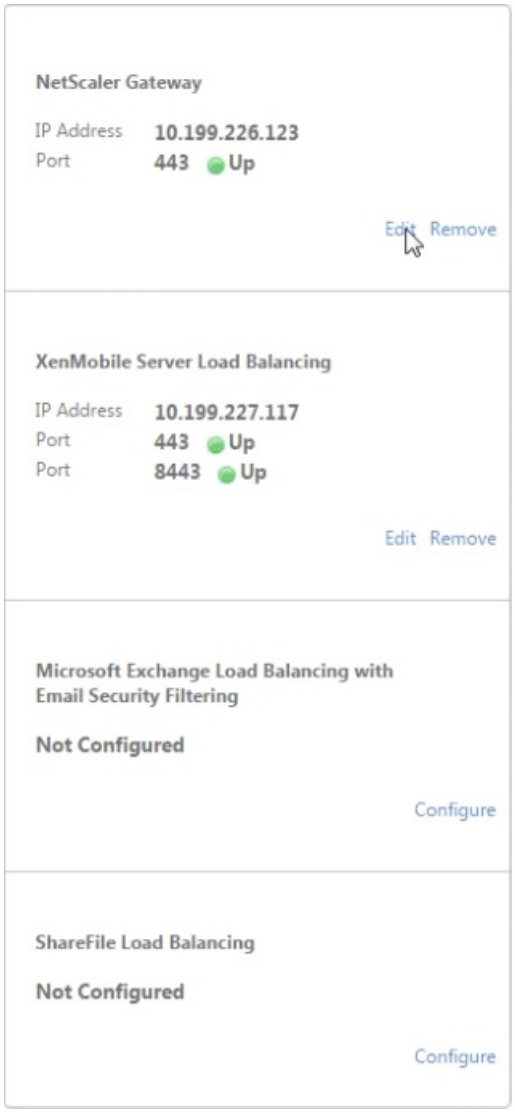
    d. Return to the NetScaler wizard and select the certificate you exported (downloaded) to install it.

    e. Click **Continue**.

The XenMobile server IP addresses that you've configured will appear.

16. Click **Continue**.

    On the NetScaler dashboard, confirm that NetScaler Gateway and XenMobile load balancing are configured:



Device Enrollment Limit

Jan 06, 2017

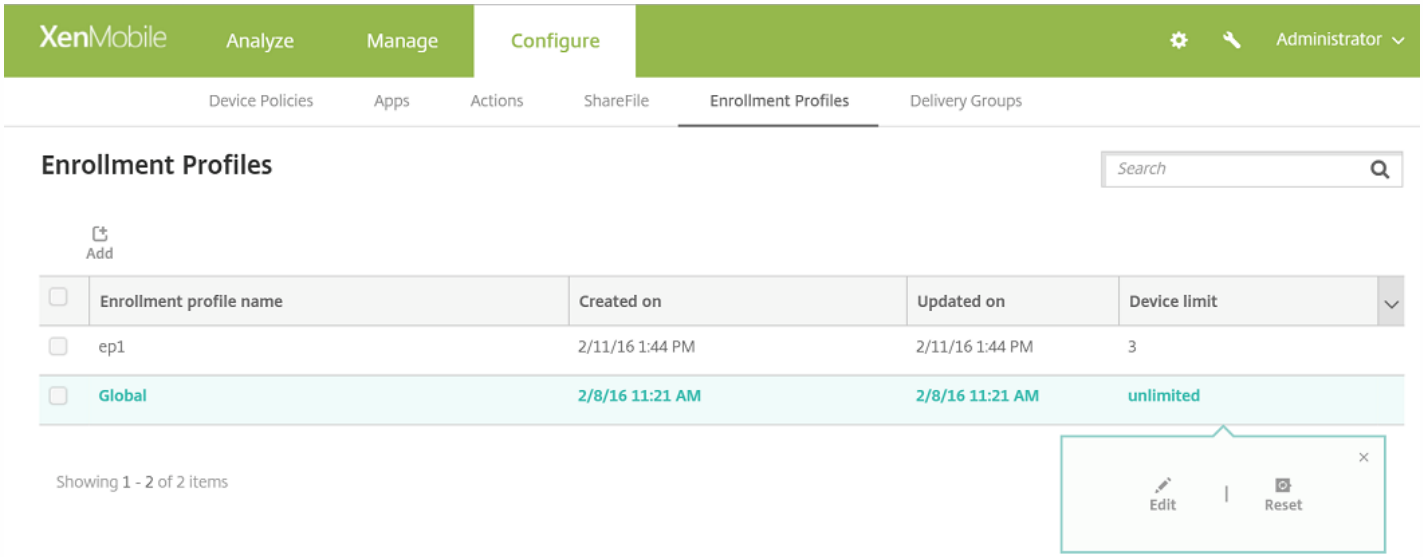
You can limit the number of devices that a user can enroll under **Configure > Enrollment Profiles** in the XenMobile console, in ENT, MDM, and MAM server modes. Limitations can apply globally or per delivery group. You can create multiple enrollment profiles and associate them with different delivery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

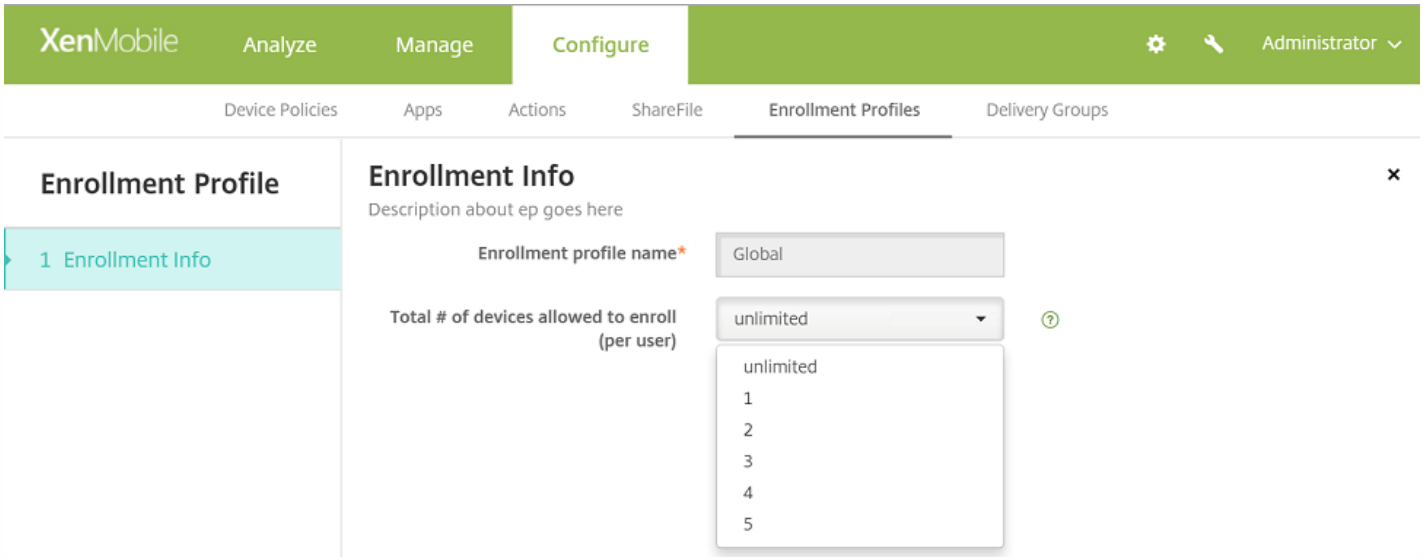
To configure a global device enrollment limit

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.

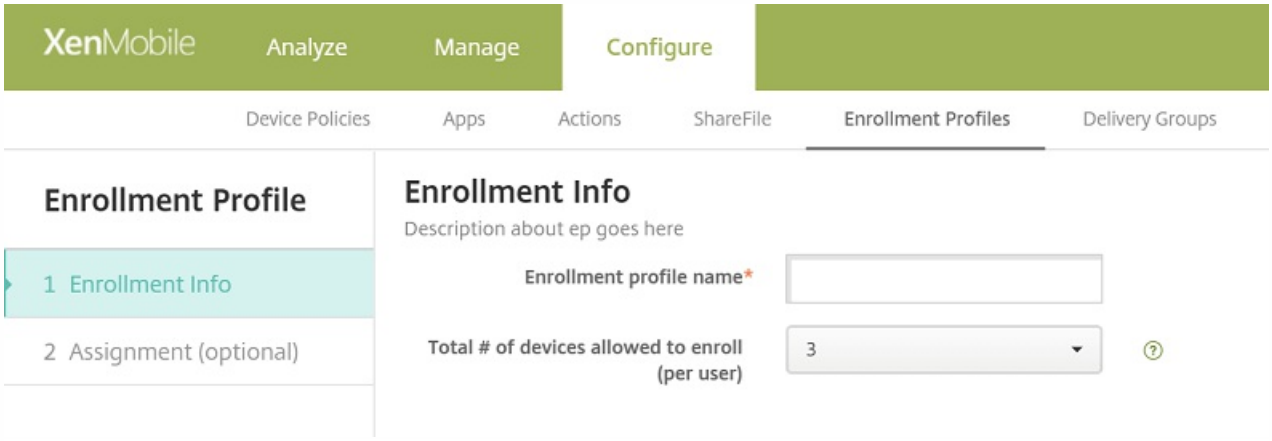


To configure a delivery group device enrollment limit

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

   The **Enrollment Info** screen appears.

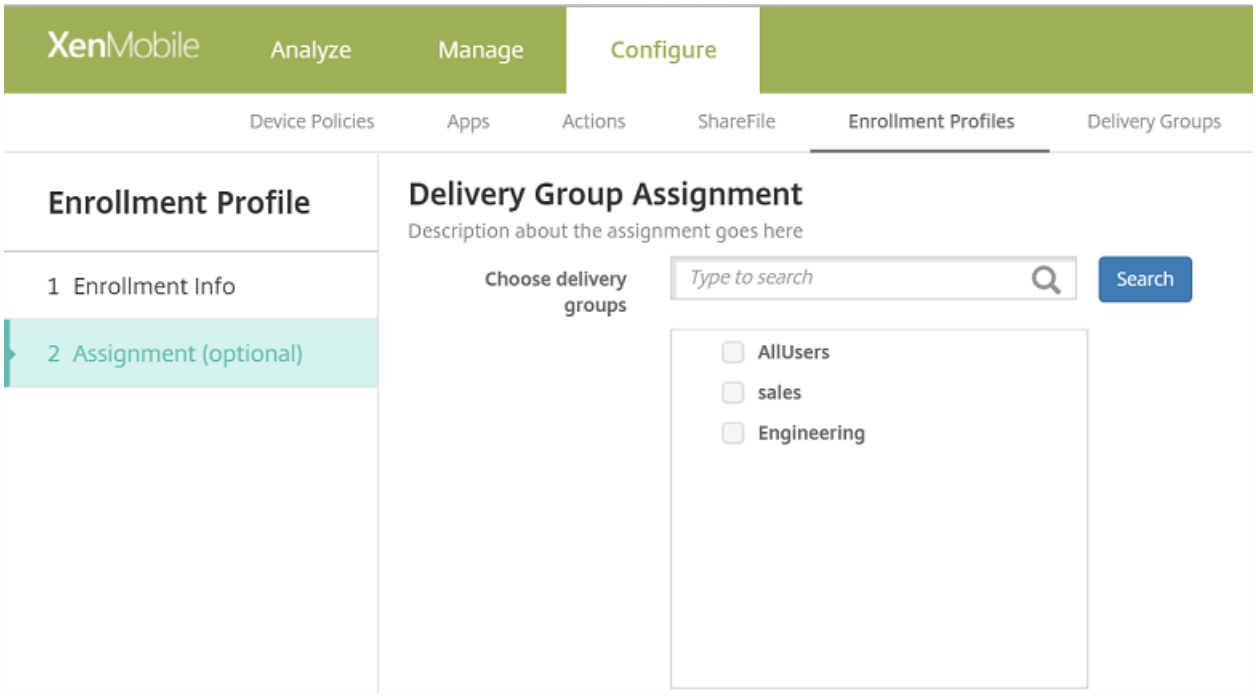
2. Enter a name for the new enrollment profile and then select the number of devices that members with this profile are allowed to enroll.



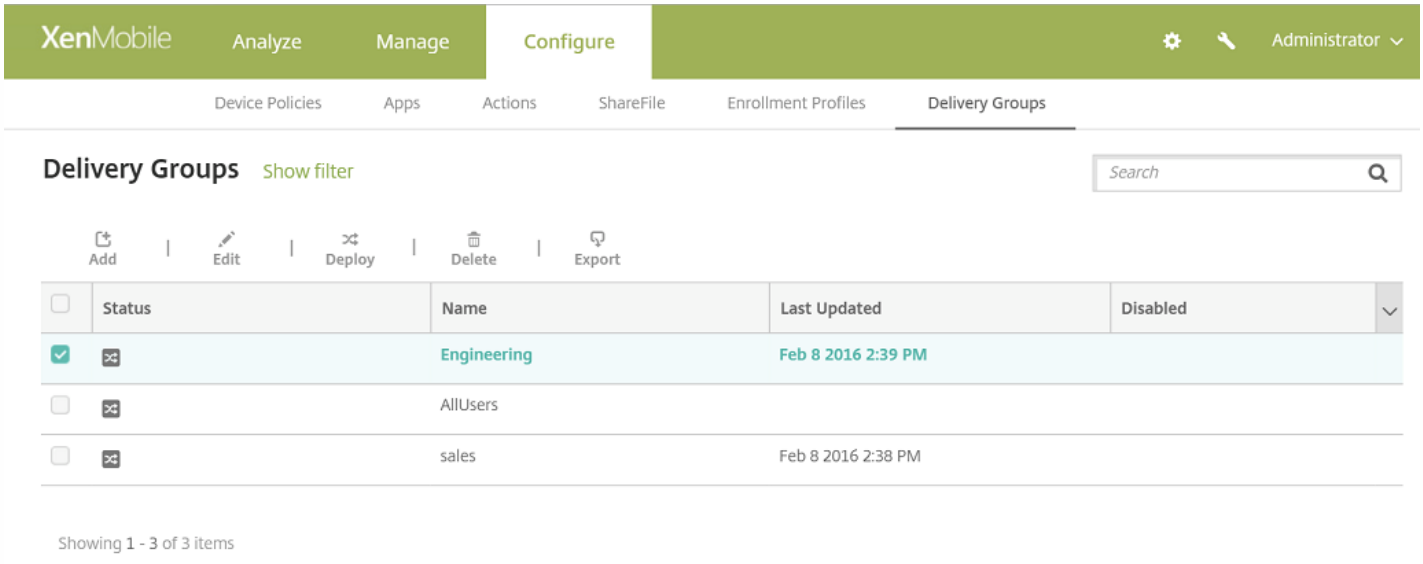
3. Click **Next**.

   The **Delivery Group Assignment** screen appears.

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

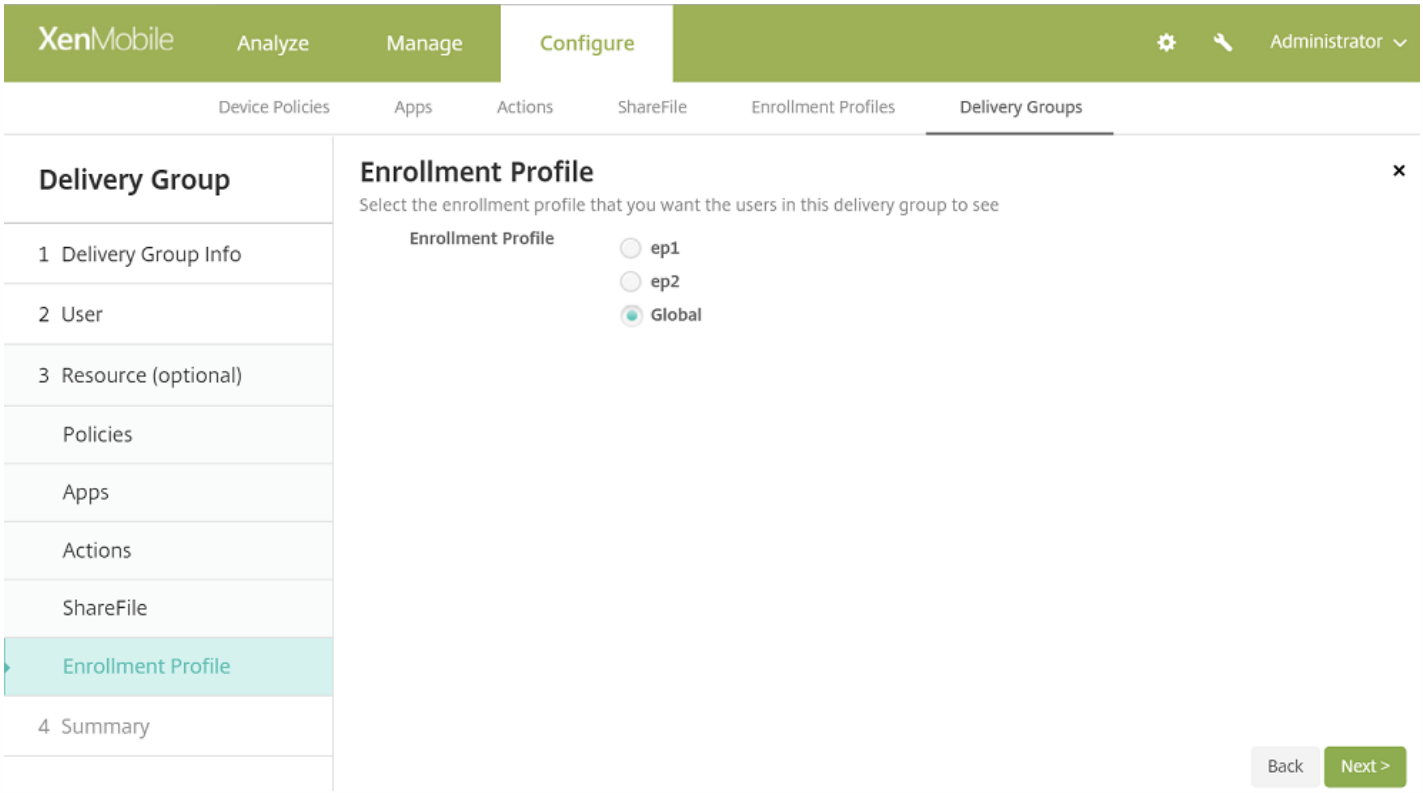


If later you want to change a delivery group's enrollment profile, go to **Configure > Delivery Groups**. Select the group you want and click **Edit**.



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

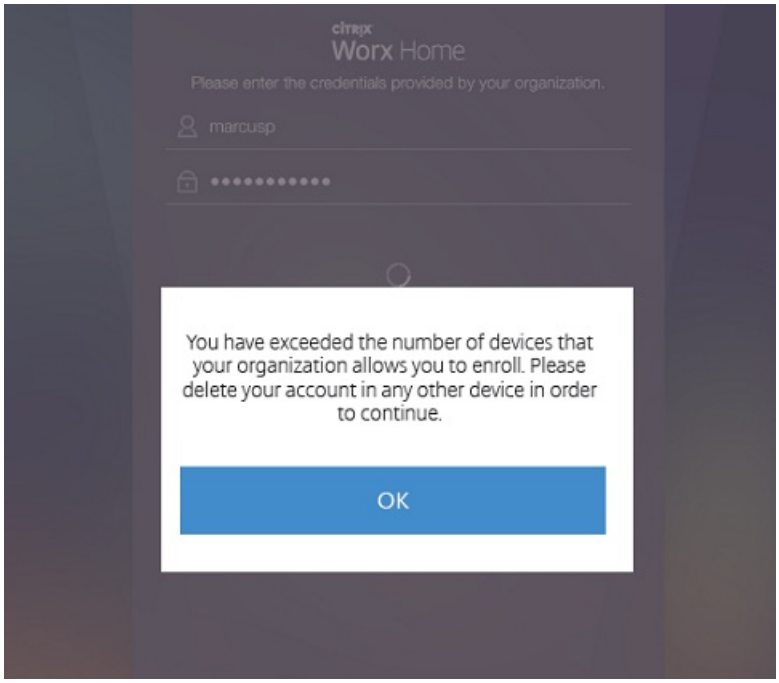
When you set the device enrollment limit and users try to enroll a new device, they follow these steps:

1. Sign on to Worx Home. **Note**: Starting with version 10.4, Worx Home is renamed 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 Worx Home enrollment screen appears again.

App Lock and App Wipe Actions for MAM-Only Mode

Jul 22, 2016

By creating actions, you establish automatic responses on a user's device to certain triggers, such as installation of an unallowed app or a user's deletion from Active Directory. You can also send notifications to users to correct an issue before more serious action becomes necessary.

Starting in XenMobile 10.3.5, 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. Previously, only the event category has this capability.

To configure automatic app wipe or app lock:

1. In the XenMobile console, click **Configure > Actions**.

2. On the **Actions** page, click **Add**.

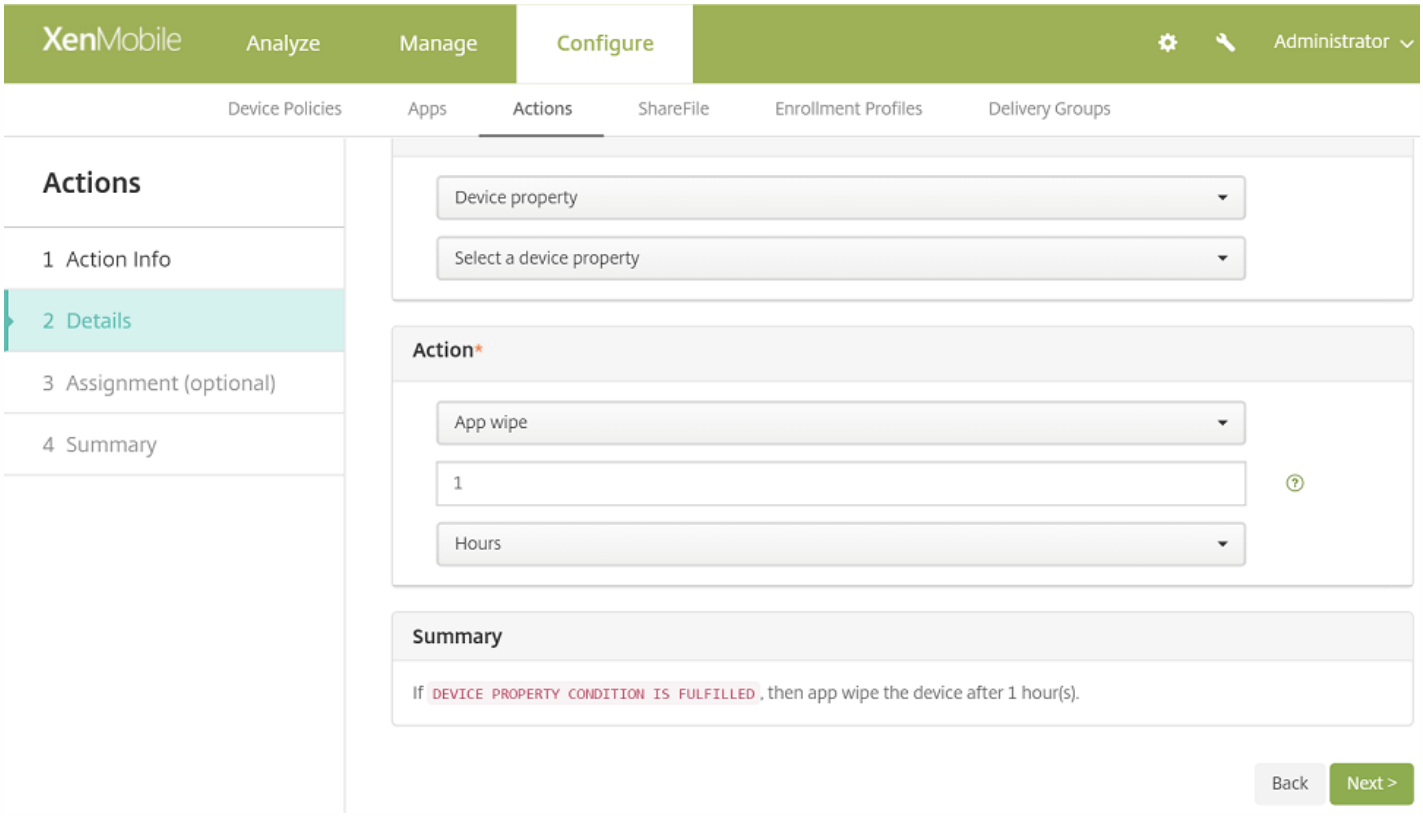
3. On the **Action Information** page, enter a name for the action and an optional description.

4. On the **Action Details** page, select the trigger you want.

5. In **Action**, select either **App wipe** or **App lock**.

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 RBAC Roles and Permissions.

> **Note**
>
> There may also be an additional delay of approximately an hour before the 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**.

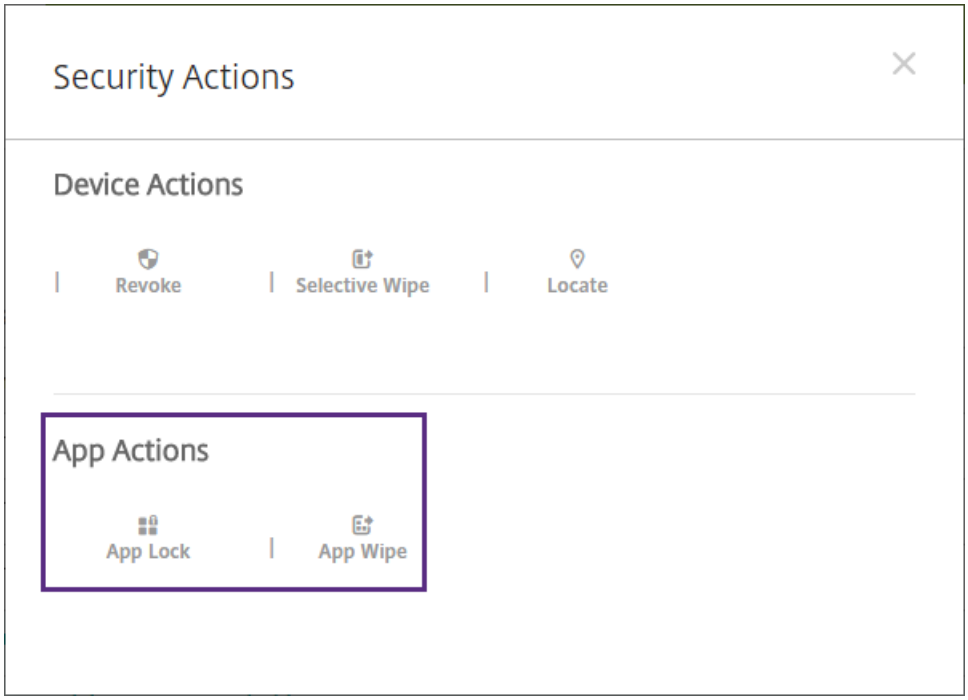
8. Click **Save**.

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

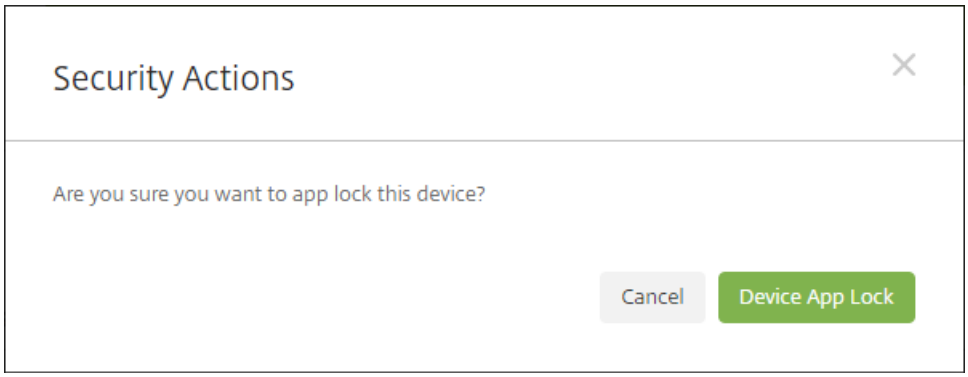
1. Go to **Manage > Devices**, select the device, and click **Secure**.

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's apps are currently locked or wiped.

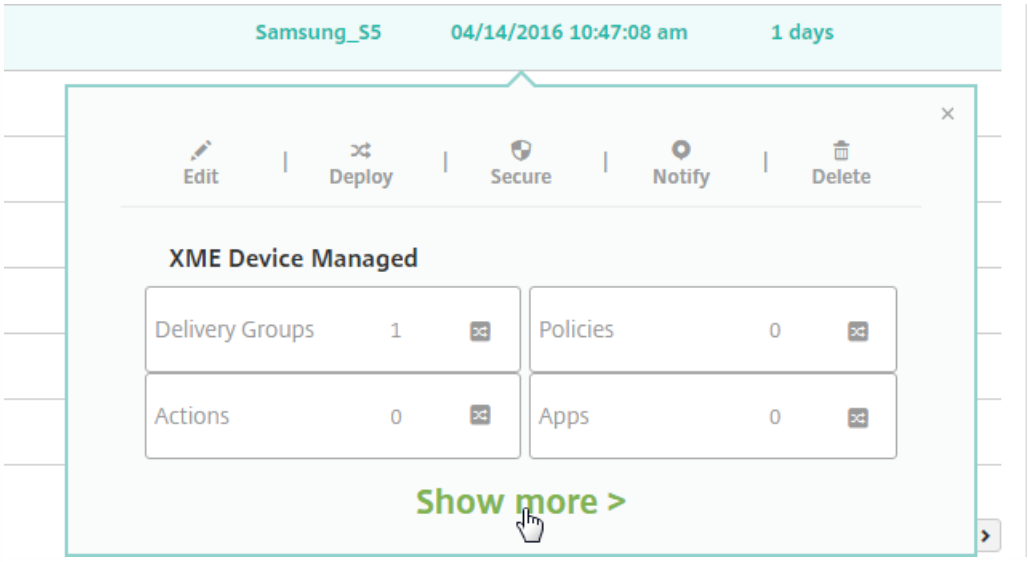


3. Confirm the action.

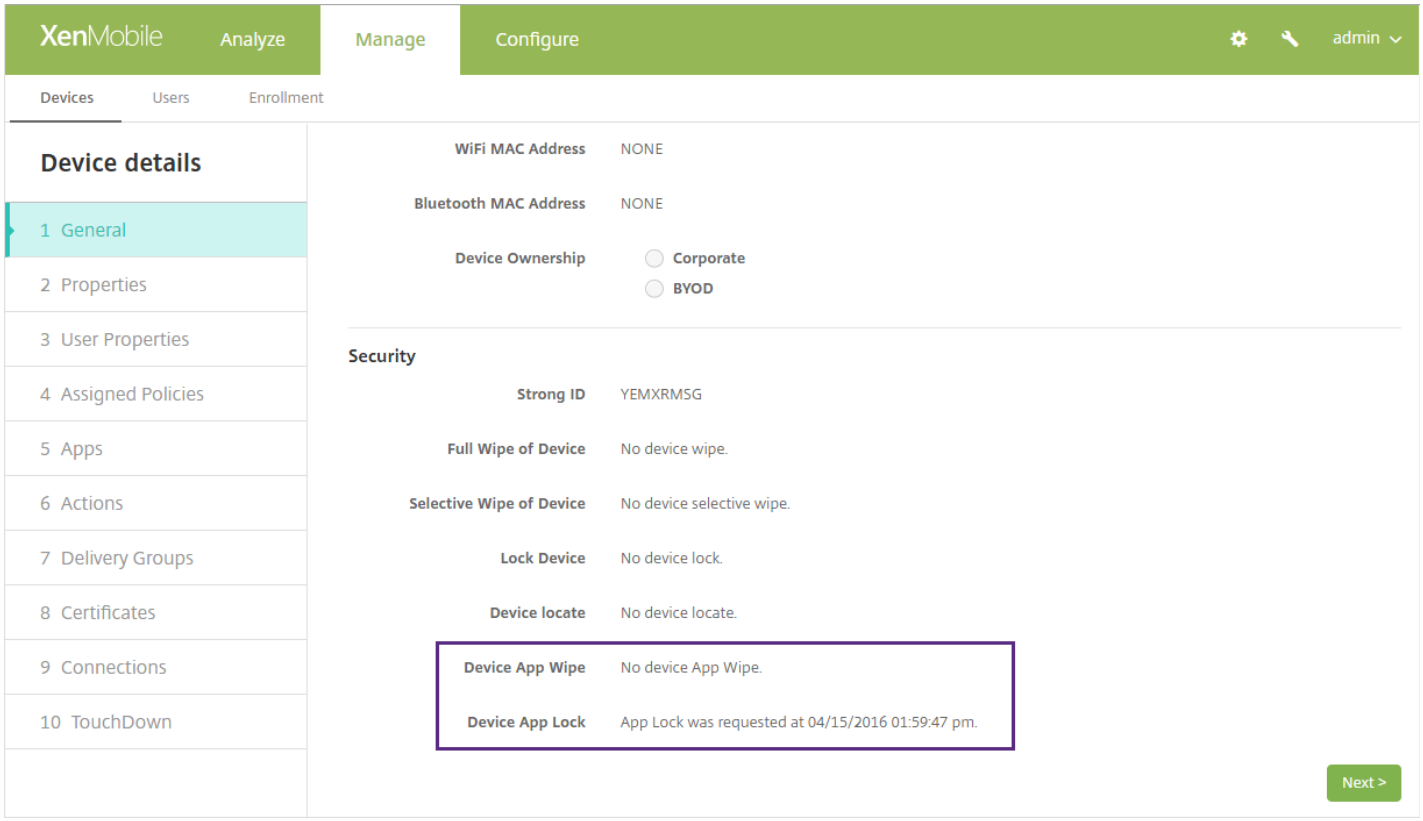


To check app lock or app wipe status:

1. Go to **Manage > Devices**, click a device, and then click **Show more**.



2. Scroll to **Device App Wipe** and **Device App Lock**.



REST Services APIs for MAM-Only Mode

May 04, 2016

For MAM-only devices, you can use any REST client and the XenMobile REST API to call REST services that are exposed through the XenMobile console. The API does not require you to sign on to the XenMobile console to call any service described in this section.

You can invoke REST API services by using the REST client.

The new REST APIs enable you to:

- **Send an Invitation URL and One-Time PIN**

  You can use a XenMobile REST API to allow users to request BYOD access through a self-service portal. When approved, the system calls XenMobile server and issues a request to do the following:

  - Generate and send an enrollment invitation URL to the user.

  - Generate and sent the user a one-time PIN.

  Note: This feature is supported for iOS and Android devices, but not Windows devices.

- **Issue App Lock and App Wipe on devices**

  You can use a XenMobile API to find devices that belong to a user by searching all devices to, for example, be able to wipe all apps on the device or lock apps.

The remainder of this article lists the Device APIs and One-Time PIN Enrollment APIs that are available as of XenMobile 10.3.5. For full documentation on the current set of available APIs, download the XenMobile REST API Reference PDF.

Device APIs

- Get Devices by Filters
- Get Device information by ID
- Get Device applications by device ID
- Get Device actions by device ID
- Get Device delivery groups by device ID
- Get Device managed software inventory by device ID
- Get Device policies by device ID
- Get Device software inventory by device ID
- Get Device GPS Coordinates by device ID
- Send notification to a list of devices/users
- Authorize a list of devices
- Activation lock bypass on a list of devices
- App lock on a list of devices
- App wipe on a list of devices
- Container lock on a list of devices
- Cancel container lock on a list of devices

- Container unlock on a list of devices
- Cancel container unlock on a list of devices
- Reset container password on a list of devices
- Cancel reset container password a list of devices
- Disown a list of devices
- Locate a list of devices
- Cancel locating a list of devices
- GPS tracking a list of devices
- Cancel GPS tracking a list of devices
- Lock a list of devices
- Cancel locking a list of devices
- Unlock a list of devices
- Cancel unlocking a list of devices
- Deploy a list of devices
- Request an Airplay mirroring on a list of devices
- Cancel request for Airplay mirroring a list of devices
- Stop Airplay mirroring on a list of devices
- Cancel stop Airplay mirroring on a list of devices
- Clear the restrictions on a list of devices
- Cancel clear the restrictions on a list of devices
- Revoke a list of devices
- Make ring a list of devices
- Cancel ring on list of devices
- Wipe a list of devices
- Cancel wipe on list of devices
- Selective wipe a list of devices
- Cancel selective wipe on list of devices
- SD card wipe on a list of devices
- Cancel SD card wipe on list of devices
- Get all device known properties
- Get all device used properties
- Retrieve all device properties by device ID
- Update all device properties in bulk by device ID.
- Add or Update a device property by device ID
- Delete a device property by device ID
- Retrieve iOS MDM Status of device by device ID
- Generate pin code

One-Time PIN Enrollment APIs

- Get Enrollment Modes
- Get Enrollment Information
- Trigger Enrollment Notification
- Create Enrollment Invitation
- Get Enrollment Records by Filter

Known and Fixed Issues in XenMobile 10.3.5

Nov 02, 2016

The following issues are known or fixed in XenMobile 10.3.5:

Known Issues

- Limitation: The features for the new MAM-only mode, such as certificate-based authentication, App Lock and App Wipe actions, and MAM-only APIs, are not available for Windows Phone.
- When users re-enroll in Worx Home multiple times and then try to install an app from the WorxStore, an error appears stating that the app has been removed. As a workaround, you can delete the device in the XenMobile console in **Manage > Devices** and then request that users re-enroll. [#611172]
- 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. [#618390]
- When device enrollment reaches the limit you set in the XenMobile console, the appropriate error message doesn't appear on the device, but users cannot enroll. [#623475]
- When users enroll in XenMobile through an Azure Active Directory account, even after you wipe or revoke the device, they can enroll again without authorization. This is third-party issue. [#628865]
- After you delete an iOS device from the XenMobile console, occasionally, when users re-enroll the device in XenMobile enterprise mode (MAM and MDM), MAM mode enrollment fails. [#629021]
- When you disable the option to renew certificates in the XenMobile server, users can renew an expired certificate in Worx Home. [#630894]
- Some VPP licenses have negative IDs, such as -123441212, in which case you cannot distribute the public apps. [#631443]
- If a Google Play credential is configured with an invalid Device ID, when you add a public app store app for Google Play and click to search the Google Play store for the app name, search fails or renders incorrect search results. [#633845]
- 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]
- In the XenMobile console, **Settings > Role Based Access Control** has the following issues related to default settings.
  - In the XenMobile console for Cloud deployments, the **Shared devices enroller** permission is set by default for the Admin role. That permission should not be set by default. [#638069]
  - The console feature permission **Disown device** is now deprecated and should not appear. [#638303]
  - In the XenMobile console for on-premises deployments, the following features are not selected by default for the Admin role. Be sure to select these settings as needed for the default Admin role or any roles you created from the Admin template. [#638314]

    Lock container
    Unlock container
    Reset container password
    Bypass activation lock
    Rings the device

  - In the XenMobile console for on-premises and Cloud deployments, the following features are not selected by default for the Admin role. Be sure to select these settings as needed for the default Admin role or any roles you created from the Admin template. [#638322]

Request AirPlay mirroring
Stop AirPlay mirroring

Fixed Issues

- ShareFile SSO authentication fails due to time sync issues that occur between XenMobile and Hyper-V. [#588249]
- When you enable nesting in your XenMobile LDAP settings, and you configure delivery groups and RBAC settings with corresponding domain groups, if you later delete the domain in your LDAP settings, the nested groups information remains in the database. [#590363]
- When you delete a user from Active Directory, they can still open the WorxStore and subscribe to apps. [#592825]
- After you check for updates for public app store apps in the XenMobile console, Worx Home updates the public app store apps with the latest version, but the app still appears in the pending updates list on the device. [#593034]
- When users receive calendar invites from Exchange account in WorxMail, the invitation does not arrive instantly as expected. [#594542]
- When the iOS device is registered in Device Enrollment Program (DEP), Worx Home might not download to the iOS device. [#595822]
- Time drift issues with the XenMobile server might occur, such as SAML single sign-on (SSO) failure for ShareFile, if you do not configure an NTP client.

  Note: Do the following configuration in order to enable the fix:

  1. Log on to XenMobile Command-Line Interface on the hypervisor on which you installed XenMobile -- Citrix XenServer or VMware ESXi.

  2.Go to **[2] System**.

  3.Go to **[3] Set NTP Server** and provide NTP server details.

  4.Restart the server.

  Important: If your system is configured in cluster mode, perform above configuration on each node. [#597757]

- When users try to remove an app or weblink from within Worx Home, the following error appears: Worx Home could not connect. [#599934]
- PIN-based enrollment might fail if multiple PINs are in a pending state for users. [#600264]
- When you import VPP licenses to XenMobile, if some licenses were refunded by Apple, the licenses are considered valid in XenMobile in error. As a result, users cannot install apps on iOS devices through the WorxStore. [#601845]
- After you create an action, if you rename the action with the same name as one of your device policies or apps, you cannot delete the action at a later time. [#602958]
- When using Samsung Galaxy Note 5 to access the Worx Store, the WorxStore appears in tablet view with a partial screen, rather than in phone view as expected. [#604295]
- When you create an enrollment invitation with a one-time PIN requirement for recipients from the top-level of an Active Directory group, nested groups receive the invitation, but enrollment fails for nested group at the third level. This issue occurs even if you direct an invitation to the third-level group. [#603434]
- When you have an Advanced license type and you select the **Enrollment required** check box in the XenMobile console, users can register in MAM-only mode and access the WorxStore. [#604113]
- The properties **$user.dnsroot** and **$user.netbiosename** are used in macros to deploy policies using user properties. The **dnsroot** and **netbiosename** user properties were deprecated in XenMobile 10.1. This fix enables these properties again in XenMobile 10.3. [#604240]

- An invalid profile error occurs when you try to configure the iOS Device Enrollment Program in the XenMobile console. This is a third-party issue. [#607143]
- The XenMobile server stops responding when saving or opening a file in Internet Explorer. You can restart the server to continue working. [#608724]
- After upgrading to XenMobile 10.3, Android for Work does not exist in the browser policy, even though blocked web addresses and bookmarks are present. [#609002]
- In the Client branding settings of the XenMobile console, the store name only supports alphanumeric (ASCII) characters; if you change the default to a non-ASCII character, users cannot sign on to Worx Home. [#609535]
- When you have LDAP configured with different base DNs for users and groups, after updating to XenMobile 10.3, you cannot add new groups to delivery groups. [#610014]
- If you remove a policy from a Delivery Group, click the **Summary** button and then save the policy, the resource remains in the Delivery Group. Clicking **Next** instead of **Summary** removes the policy from the Delivery Group. [#610109]
- When you configure a WiFi device policy, even though the deployment schedule is set to **Only when previous deployment has failed,** the WiFi policy is pushed to devices every time the device connects. [#610325]
- This fix addresses Java zero-day vulnerability of object deserialization in Apache Commons Collections. [#610427]
- When you set a RBAC role to allow users to sign on to the XenMobile console using a sAMAccountName format for their user name, they are redirected to the Self Help Portal. [#610915]
- After installing XenMobile 10.1 for the first time or upgrading from XenMobile 9 MAM and MDM mode to XenMobile 10.1, in the XenMobile console under **Manage** > **Device**, after refreshing the delivery groups and policies, the information is different; the count of delivery groups and policies is incorrect. [#611630]
- When configuring a VPN device policy for Mac OS X, the **VPN** option appears in the list of **Connection Types**. You cannot, however, configure this option for Mac OS X devices. [#612846]
- When you have more than 10 LDAP domains configured in XenMobile versions earlier than XenMobile 10.1, in XenMobile 10 and after upgrading to XenMobile 10.1, only 10 domains appear in the XenMobile console. [#613502]
- You cannot add or update an MDX app if you do not set an RBAC role for users that includes permissions for public apps. [#614496]
- If you change the default instance name during initial configuration of XenMobile, when you upgrade to version 10.3, the change is not retained. As a result, enrolled devices cannot connect. [#614604]
- When you configure LDAP with a lockout limit, after upgrading to XenMobile 10.3, when a new user in the same domain enrolls a device in Worx Home with invalid credentials, such as a mistyped password, Worx Home stops responding and SQL Server fails. [#615179]
- After updating from XenMobile 10.1 to XenMobile 10.3, you cannot send an enrollment invitation to users using the **Add invitation** option. [#616584]
- This fix enables support for an LDAP multi-domain root in a single forest. This support was available in XenMobile 9, but not available in XenMobile 10.x. [#616633, #618899, #620541]
- When you configure an iOS restriction device policy in the XenMobile console and you change the default value for the **Allow user to remove policy** option, the value is not saved. [#616751]
- When a server has a custom instance name, after updating from XenMobile 10.1 to XenMobile 10.3, users cannot enroll devices. [#616954]
- When users enroll a DEP device in XenMobile Enterprise mode, if they reset their own device to factory settings (full wipe) and then reenroll the device, Worx Home is not deployed to the device automatically as expected. [#616986]
- Occasionally, the XenMobile server goes into recovery mode after about 20 to 30 minutes due to a known Java Runtime Environment (JRE) issue. After restarting the server, the issue occurs again. [#616992]
- On iOS and Android devices, users cannot open WorxStore from Worx Home if you remove the **Store name** in **Settings > Client Branding**. [#617003]
- When you upload an .ipa file to the XenMobile console, the error "no icon found" appears. [#617195]

- When you deploy a VPN device policy with the Enable per-app VPN and the On-demand match app enabled options set to **ON**, and an App Attributes policy for a managed app with the VPN policy applied to it, when users open the managed app, the following issue occurs: The VPN connection is not initiated automatically as expected. Users must enable the **Connect On Demand** setting manually on their device. [#617803]
- In the XenMobile console, in **Manage** > **Users**, a delay occurs in the appearance of existing users. As a consequence, you cannot perform local user operations. [#618094]
- XenMobile 10.x provides support for LDAP multi-domain in a single Active Directory forest. [#618375]
- When you sent an enrollment invitation and enter HTML code, users receive the email in plain text with no HTML link. [#618504]
- When users upload a .appx file as an enterprise app for Windows 10 devices, the app does not deploy to the device. [#628611]
- Users cannot enroll Windows 10 devices to XenMobile in MDM mode if they include any special characters in the user ID or password field. [#618870]
- On iPads, XenMobile 10.3 always carries out deletion (or removal) actions first, regardless of the order you set in the XenMobile console. [#620459]
- When you update an existing iOS enterprise app in the XenMobile console and the .ipa has a different bundle ID, when you deploy the updated app to devices, issues with app deployment occur on devices. [#621009]
- When adding Google Play credentials in XenMobile server, the error "Invalid device ID" appears and you cannot log on. [#623182]
- If you delete an app in XenMobile that you imported using VPP, the app is not imported automatically again until you delete and add the token again. [#623403]
- If you delete or wipe a device, any VPP license associated with this device is not released automatically. As a result, you must dissociate the license manually to be able to use it on another device. [#623716]

About XenMobile Server 10.3

Jan 06, 2017

You can upgrade XenMobile 10.1 to XenMobile 10.3 in the XenMobile console. To perform the upgrade, you use xms_10.3.0.824.bin. In the XenMobile console, click the gear icon in the upper-right corner of the console and then click **Release Management**. Click **Upgrade** and then upload the xms_10.3.0.824.bin file. For more information about upgrades in the console, see Upgrading XenMobile.

To complete a new installation of XenMobile 10.3, see Installing XenMobile.

> **Note**
>
> The Remote Support client is not available in XenMobile Cloud versions 10.x for Windows CE and Samsung Android devices.

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.

What's new in XenMobile 10.3

The following features are new in XenMobile 10.3.

New console appearance

XenMobile 10.3 has a new look. The console is updated with new colors, fonts, tabs, and improved functionality.

- The Dashboard tab in previous versions of the console has been moved under the new Analyze tab, which also includes the new Reporting tab. For details, see Reports.
- The Manage tab now includes the new Users tab where you manage local users and groups.
- The Configure tab now includes the new ShareFile tab where you configure settings to connect to the ShareFile account.
- You access Settings, formerly under the Configure tab, by clicking the gear icon on the upper-right of the console.
- The Support tab now opens in the same tab as the console instead of in a new tab.

New platform support

XenMobile 10.3 now offers support for the following platforms:

- Mac OS X
- Android HTC
- Android Sony
- Samsung SEAMS
- Windows Mobile/CE
- Windows 10 Phone: Device management in XenMobile MDM and Enterprise modes.
- Windows 10 Desktop/Tablet: Device management in XenMobile MDM and Enterprise modes.

For steps on enrolling Mac OS X devices, see Mac OS X devices.

For steps on enrolling Windows 10 devices, see Windows devices.

> **Note**
>
> Support for Symbian devices is deprecated in XenMobile 10.3.

Device policies

The following new MDM policies are available in XenMobile 10.3:

- **App lock**. Lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device. Available for iOS and Android. Although the device policy works on most Android L and M devices, app lock does not function on Android N or later devices due to the deprecation of the required API by Google.
- **App network usage.** Lets you set network usage rules to specify how managed apps use networks, such as cellular data networks. The rules only apply to managed apps. Available for iOS.
- **Connection manager**. Configures how apps will connect to the Internet or to a private network. These settings only work on Pocket PCs (touch screen devices). Available for Windows Mobile/CE.
- **Copy apps to Samsung container**. Lets you create a SEAMS or KNOX container for apps on Samsung devices. Available for Samsung SEAMS or Samsung KNOX.
- **Delete files and folders**. Allows you to specify which files and folders need to be deleted. Available for Windows Mobile/CE.
- **Device health attestation**. Enables Device Health Attestation, a security and data loss prevention (DLP) feature in Windows 10 that lets you determine the health of a Windows 10 device and take compliance actions when necessary. The payloads are supported only on Windows 10 and later supervised devices. Available for Windows Phone and Windows Tablet.
- **Device name.** Allows you to 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.
- **Delete registry keys and values**. Allows you to specify which registry keys and values need to be deleted. An empty value means that the entry is a registry key. Available for Windows Mobile/CE.
- **Enterprise Data Protection.** Allows you to specify apps that require Enterprise Data Protection (EDP) at the enforcement level you require. This policy applies to Windows phones and Windows tablets.
- **Import iOS & Mac OS X profile**. The option to configure this policy for Mac OS X is new in XenMobile 10.3. The policy lets you import a device configuration XML file for either iOS or Mac OS X. The file contains device security policies and restrictions that you prepare with the Apple Configurator.
- **Registry**. The Windows Mobile/CE registry stores data about apps, drivers, user preferences, and configuration settings. You can define the registry keys and values that let you administer Windows Mobile/CE devices.
- **Wallpaper.** Lets you 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.
- **Windows CE certificate**. Allows you to create and deliver a certificate from an External PKI to your device.

For a matrix of all new and existing device policies per platform, see XenMobile Device Policies per Platform.

Summary of new features and enhancements for each platform type

iOS

- **New device policies**. App Network Usage, Device Name, and Wallpaper
- **Assigning an app from managed to unmanaged**. iOS 9.0 option for assigning an app from managed to unmanaged.

When you add and configure settings for a public app store app for iOS in the XenMobile console, you can configure a **Force app to be managed** option. This option is set to **OFF** by default. If you select **ON**, when the app is installed as unmanaged, users are prompted to allow the app to be managed on unsupervised devices. For details, see Adding a public app store app to XenMobile.

- **New Restrictions and Apple Configurator 1.7.2 policy options**. For details, see Restrictions device policies.
- **Support for RequestMirroring and StopMirroring commands**. For details, see the XenMobile REST API reference.
- **DEP device setup assistant enhancements**. For details, see Bulk enrollment of iOS devices.
- **VPN OnDemandRules key**. For details, see VPN device policies.

Android

- **Samsung KNOX Container configurations**. For details, See Copy Apps to Samsung Container device policy.
- **Samsung SAFE APIs**. For details, see XenMobile REST API Reference.
- **ELM key for Samsung Android devices**.
- **App lock device policy**. For details, see App lock device policy.

Windows CE

- **Credential provider configurations**. For details, see Credentials device policy
- **Windows CE Certificate configurations**. For details, see Windows CE certificate device policy.
- **Registry storage device policy**. For details, see Registry device policy.
- **Ability to connect on SMS reception/connect on call**.
- **Other new device policies**: Connection manager, Delete Files and Folders, Delete Registry Keys and Values.

Windows Phone 10 and Windows Tablet 10

- New device policy: Enterprise Data Protection and Device Health Attestation
- New device policy options for Windows Phone and Windows Tablet:

  App inventory
  Credentials
  Custom XML
  Passcode
  Restrictions
  Terms & Conditions
  VPN
  WiFI

- New device policy options for Windows Tablet:

  App Uninstall
  Sideloading Kay
  Signing Certificate
  Webclip
  WorxStore (renamed XenMobile Store as of version 10.4)

- New device policy options for Windows Phone:

  Enterprise Hub
  Storage Encryption

Mac OS X

- Enrollment via OTAE. For details, see Mac OS X.
- Device management information in the XenMobile console showing device properties, certificates, reports, and supported profiles.
- Security actions on Mac OS X devices - selective wipe, lock, revoke, wipe.
- New device policy options:

  Device Name
  Import iOS and Mac OS X Profile
  AirPlay Mirroring
  App Inventory
  Calendar (CalDav)
  Contacts (CardDAV)
  Credentials
  Exchange
  Font
  LDAP
  Mail
  Passcode
  Profile Removal
  Restrictions
  SCEP
  VPN
  Webclip
  WiFI

New features and enhancements to support Android for Work

- **Support for devices earlier then Android**.
- **Provisioning Device Owner mode for Android for Work**

  In addition to managing Android for Work apps or Android devices in BYOD mode, you can also manage corporate-owned devices through the provisioning of Device Owner mode. To do so, you use an Near Field Communication (NFC) bump between devices. One device runs the Worx Provisioning Tool app and bumps either a new out-of-the-box device or a device that is factory reset. Device Owner mode is the corporate-owned device mode for most devices running Android 5.x.x.

- **Android for Work Bulk Purchasing**

  You can manage Bulk Purchase licensing in the XenMobile console for apps enabled for Android for Work. 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. When you add a paid public app store app for an Android for Work to XenMobile, you can review the Bulk Purchase licensing status - the total number of licenses available. After you deploy the app to users, you can later review the number of licenses currently in use, as well as the email address of each user consuming the licenses. 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.

Shared devices

XenMobile lets you configure devices that can be shared by multiple users. For details, see Shared devices in XenMobile.

Language support

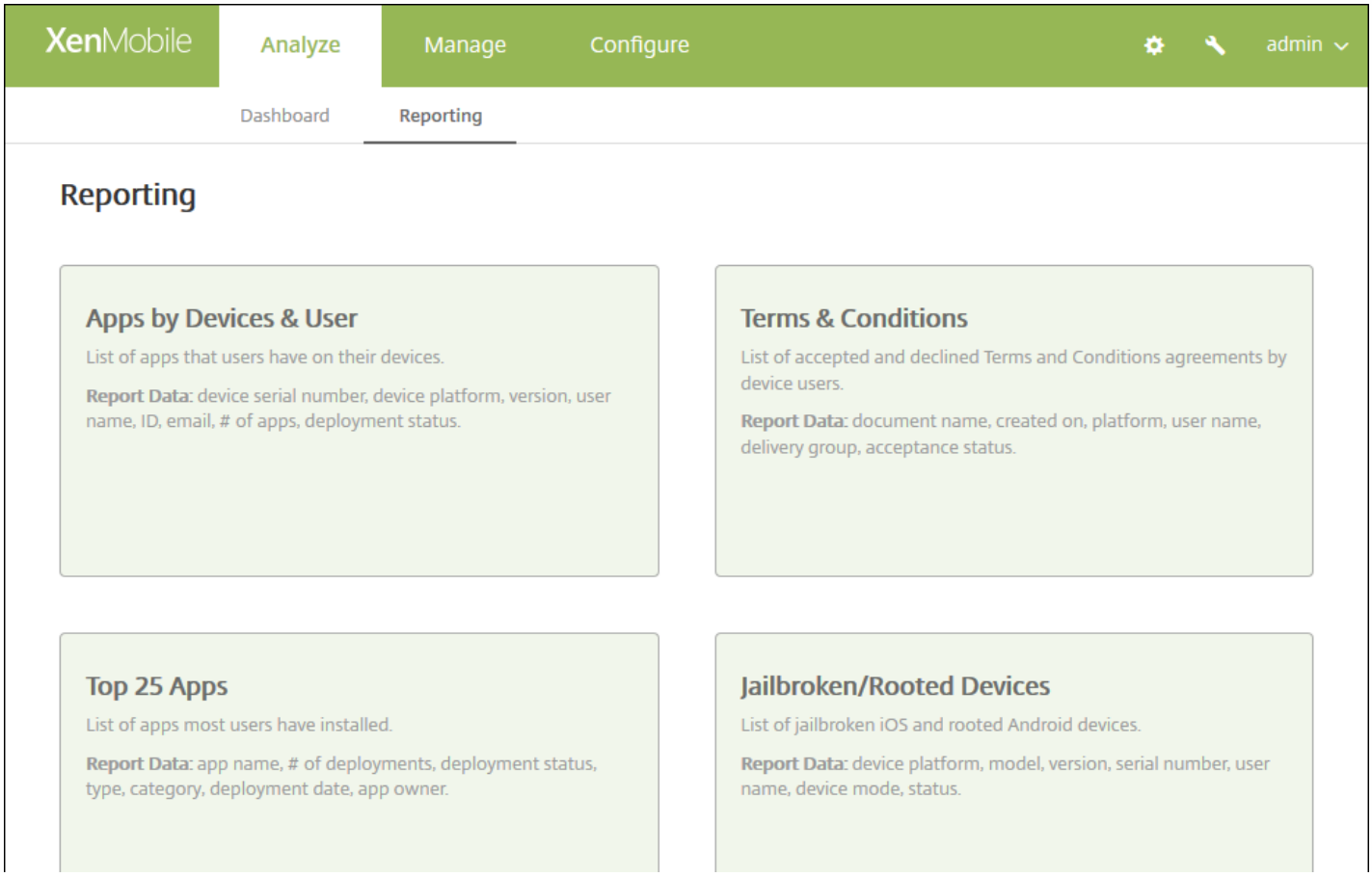
The XenMobile console in XenMobile 10.3 is available in Korean, German, and Portuguese. The MDX policies are now localized when viewed in the XenMobile console. For details, see XenMobile language support.

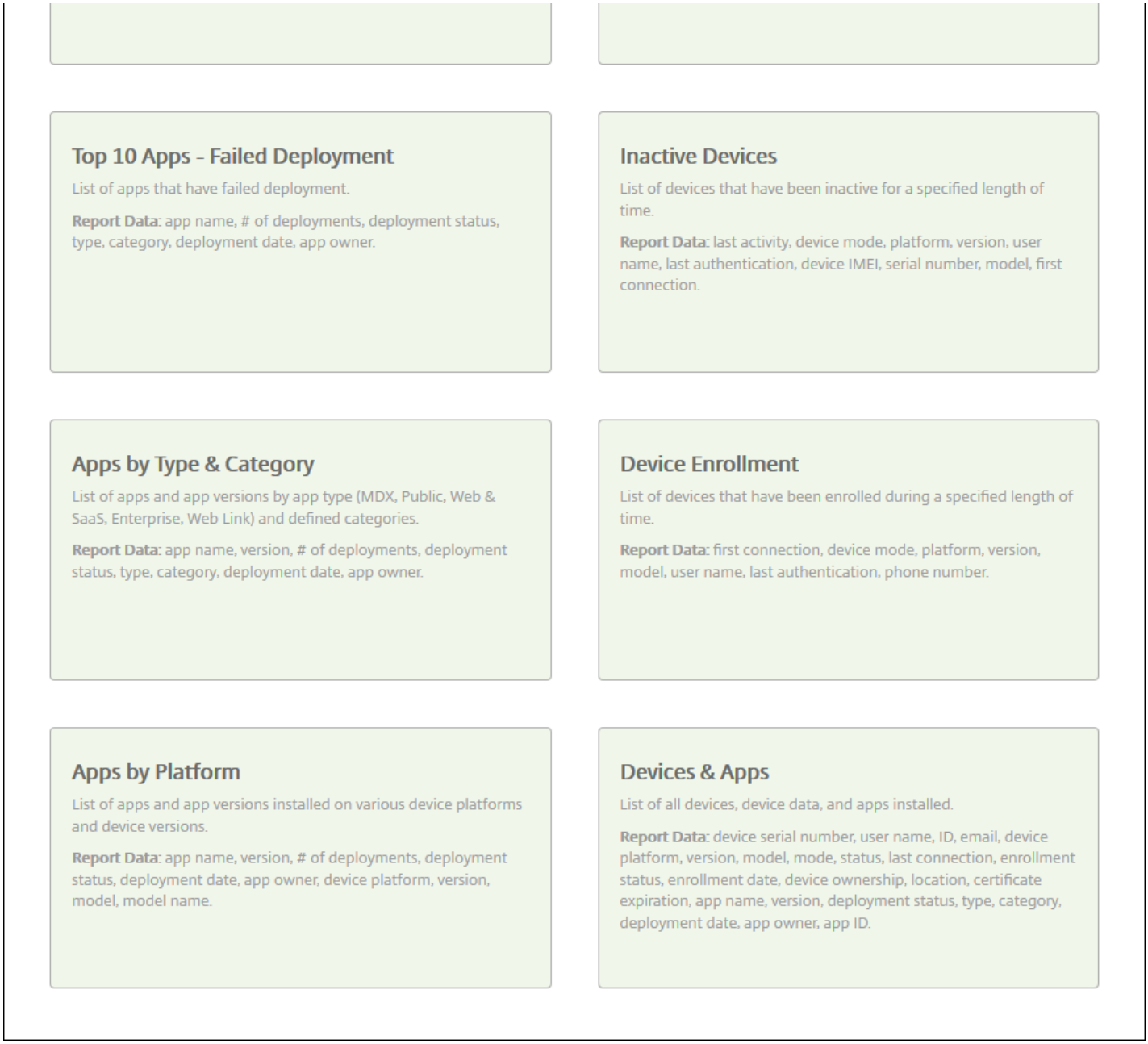
Reports

From the **Reporting** tab, you can generate 10 predefined reports from within the XenMobile console:

- **Apps by Devices & User**: Lists apps that users have on their devices.
- **Terms & Conditions**: Lists users who have accepted and declined the Terms and Conditions agreements.
- **Top 25 Apps:** Lists up to 25 apps that most users have on their devices.
- **Jailbroken/Rooted Devices**: Lists rooted iOS devices and jailbroken Android devices.
- **Top 10 Apps – Failed Deployment**: Lists 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 devices that have enrolled during a specified time period.
- **Apps by Platform**: Lists apps and app versions by device platform and version.
- **Devices & Apps**: Lists all devices, device data, and apps installed.

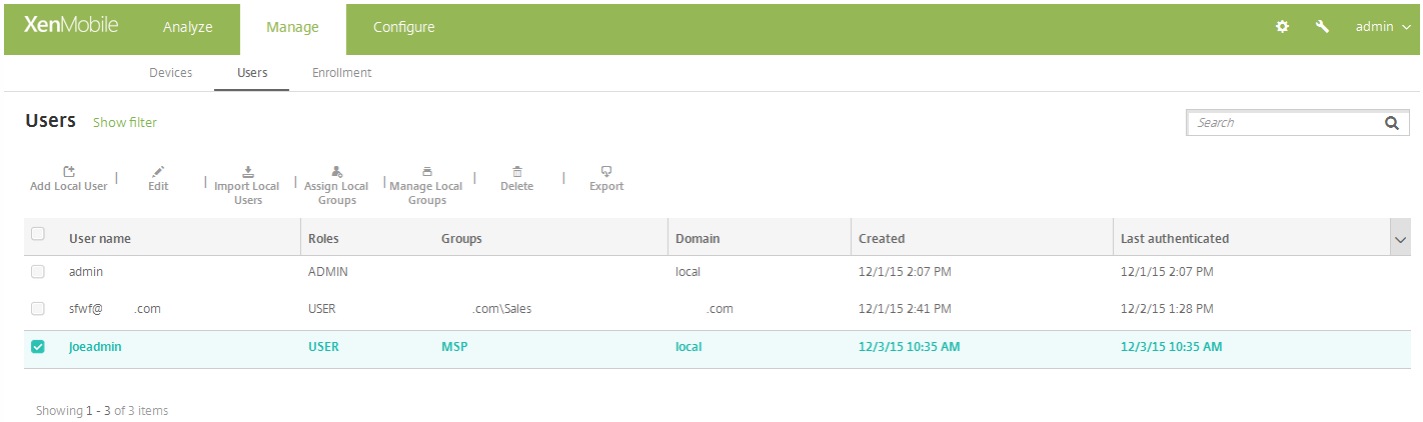
To run reports, click the **Analyze** tab in the XenMobile console and then click **Reporting**. The reports are in .csv format, which you can open with programs like Microsoft Excel. For details, see Reports in XenMobile.





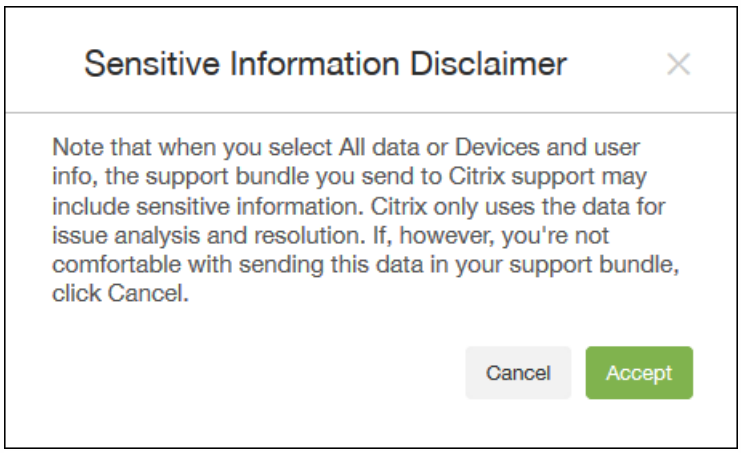
Adding LDAP members - local users - to groups

Many organizations do not configure Active Directory groups, but may need a local group for a particular purpose - a pilot, for example. In XenMobile 10.3, you can make LDAP - local users members of a local group. Then, you can define a delivery group that contains the local group. This set of users can access apps and policies assigned to the delivery group without having to reenroll their devices. For details, see To add, edit, or delete local users in XenMobile.



Support bundle legal agreement

The first time you upload a support bundle to Citrix Insight Services (CIS), you are prompted to accept a legal agreement. For details, see Creating Support Bundles in XenMobile.



Anonymizing data in support bundles

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. For details, see Anonymizing data in support bundles.

Connectivity checks

From the XenMobile Support page, you can check the XenMobile connection to NetScaler Gateway and other servers and locations. For details, see Conducting connectivity checks.

Microsoft Azure

You can join Windows 10 devices to Microsoft Azure AD to allow the devices to enroll with Azure as a federated means of Active Directory authentication. For details, see Microsoft Azure settings.

XenMobile Server 10.3 Fixed Issues

Apr 04, 2016

The following issues are fixed in XenMobile 10.3. For fixed issues in XenMobile 10.3.5, see Known and Fixed Issues in XenMobile 10.3.5.

An email sending prefix can be added twice to an email address when sending email from an SMTP through a carrier SMS gateway. [#492629]

HTTP GET requests from Cisco Identity Service Engine to XenMobile might fail with a 404 error. [#555554]

When a file upload policy is set to push a file to Android devices, pushing files to the device might fail. Instead, the "Terms and Conditions" statement might appear on the device. [#564144]

In certain cases, when MDM identity certificates are distributed via SCEP and are issued using the built-in PKI, upon renewal of these identities, XenMobile does not properly revoke the previous certificate. As a result, in some instances, affected devices lose MDM functionality. [#569999]

After configuring a proxy server, connectivity checks creates network traffic that does not go through the proxy server and the connection fails. [#571467]

If users are members of a child domain, connecting to SAML apps fail. [#571851]

If an iOS MDX app is in the list for Excluded devices, the app does not appear in Worx Store when the device is in mobile app management-only mode (MAM mode). [#571900]

After upgrading to XenMobile 10, searching for a device can take up to 30 seconds and the CPU usage also rises to 100%. [#577010]

When browsing intranet sites with WorxWeb in a multi-node clusters environment, users might fail to access URLs and see the message "Error Invalid OTT." [#577273]

If you configure XenMobile with a proxy server, attempts to add Google Play credentials or create an Android public store app might fail. [#578727]

A blank page appears when attempting to open the XenMobile console in a published version of Internet Explorer 11. [#578729]

This release now supports WPA2 Personal and WPA2 Enterprise for iOS 8. [#579616]

If you add or upload an app in the XenMobile console, an error might occur when you upload the app to XenMobile using the same app file name as an existing app. [#580359]

Attempts to download Worx apps from the Worx Store fail on an Android device. [#582044]

When entering a macro with the user name and phone number, the transform does not correctly translate the phone number. [#589130]

The Bypass Activation Lock command might not work on some iOS devices. [#589991]

If the "memberOf" property value exceeds 255 characters, the error message "No groups found" appears.

If users attempt to open a Windows app through Worx Home, enumeration succeeds, but the app does not open. Users receive the error message "Could not add account." [#590046]

If you create a Simple Certificate Enrollment Protocol (SCEP) policy that requires a challenge password, you cannot save the policy. With this release, the challenge password field is optional. [#590798]

If you configure XenMobile to use a proxy server, Android for Work cannot make a connection to external websites. [#591707]

Attempts to upload an IPA app to App Controller fails with the error message "Invalid package type for selected app." The message appears when there is an error in the PNG image. [#592748]

When users attempt to enroll, they receive the error message "User <userName> does not exist." The error occurs after deleting the users' enrollment and then enrolling again. When this happens, it recreates users in Active Directory. [#593028]

If you create a calendar invitation from a Microsoft Outlook or Microsoft Exchange account, it can take a long time to appear in WorxMail. [#594542]

If you configure a workflow and use a different port number than 443 (the default), users cannot open the workflow link. [#599441]

Users cannot update an Android app on their device from XenMobile Server. [#601251]

Users cannot log on to Worx apps when enrolling through Azure Active Directory. [#608505]

As of December 2015, Nexmo SMS supports HTTPS connections only. In XenMobile, the default setting is **ON**. There is no effect if you change the value to **OFF**. After upgrading, the value still appears as **OFF**, but connections are secure. [#609306]

Worx Store requires a Volume Purchase Program (VPP) user even though the license applies to the device only. [#610338]

XenMobile Server 10.3 Known Issues

Dec 20, 2016

The following are known issues in XenMobile 10.3. For known issues in XenMobile 10.3.5, see Known and Fixed Issues in XenMobile 10.3.5.

- The following bugs relate to an integration between XenMobile and NetScaler for the following versions of NetScaler when the TLS 1.2 security protocol is configured on NetScaler:
  - NetScaler 11.x versions earlier than 11.0.64
  - 10.5.59
  - 10.5.58

  Note that the issue does not arise when your XenMobile MAM deployment includes a NetScaler load balancer between the XenMobile server and NetScaler Gateway.

  Communication between NetScaler Gateway and XenMobile in MAM mode fails due to issues with a backend TLS 1.2 session. As a result, users cannot download apps from the WorxStore, nor files from ShareFile, when connecting to the internal network. [#591600, #595713, #596566, #604409]
- App push fails after uninstalling a corporate app. [#591450]
- After removing the license from an app, the app stays on the user device. This is a third-party issue. [#596656]
- When users attempt to enroll their personal device with a Microsoft work account, the enrollment fails. [#597037]
- The Terms and Conditions policy does not appear with an installed or pending status in the XenMobile console even if the policy is deployed successfully on the device. [#598407]
- Restriction policies take effect on Windows 10 devices. However, users do not receive a message that a blocked feature is disabled. [#599064, #606651]
- If you add a category with public and enterprise apps and then enroll a device in XenMobile, when users sync apps in Worx Home, the category does not appear. [#599495]
- If you do not add the Selective Wipe device permission when creating a Shared Devices RBAC, when users attempt to delete their account in Worx Home on an iOS device (in XenMobile Enterprise mode), users must manually remove the Device Manager profile from the device. [#600705]
- After deploying the App Inventory and Enterprise Hub policies for an app and then creating a public app with a different name and description, when users open the app from Worx Home, the app name and description are the same. [#600369]
- If you configure Microsoft SQL Server in SSL mode during first time use, and the CA certificate is not one that corresponds to the SQL Server certificate, the connection fails. If you attempt to retry the connection with the appropriate CA certificate that corresponds with SQL server certificate, the connection still fails. To allow the certificate to work, restart XenMobile server to clear the truststore cache. [#602609]
- The user names on shared user devices must be in English. Shared Devices do not support non-ASCII user names. [#605544]

- 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]
- After upgrading to XenMobile 10.3, the licensing information appears as the trial period set to to 30 days and the license server configured flag set to true. After upgrading the XenMobile server, upload the same license to the server, which removes the trial license period. [#607939]
- On Windows 8.1 tablets, users can successfully remove apps from the device. Enterprise apps continue to appear in the XenMobile console in device properties. [#608184]
- The options App Wipe and Selective Wipe function the same in XenMobile Enterprise mode. [#608715]
- The XenMobile server stops responding when saving or opening a file in Internet Explorer. You can restart the server to continue working. [#608724]
- After upgrading to XenMobile 10.3, Android for Work does not exist in the browser policy, even though blocked web addresses and bookmarks are present. [#609002]
- On tablets running Windows 8.1 and Windows 10, after deleting accounts manually from the device, some policies remain. [#609201]
- On tablets Windows 10, if users change the Autoupdate setting on the device, the change does not appear in the Security Information section in Device Properties in the XenMobile console. [#609254]
- The Worx Store name supports English (ASCII) characters only. [#609535]
- 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]
- When configuring a workspace in Citrix Workspace Cloud, delivery groups do not update with Active Directory users or groups that belong to child and grandchild domains. [#609673]
- Enrolling a Windows 10 device fails if there are multiple Terms and Conditions policies deployed and none of the policies is the default Term and Conditions. [#609694]
- If you remove a policy from a Delivery Group, click the **Summary** button and then save the policy, the resource remains in the Delivery Group. Clicking **Next** instead of **Summary** removes the policy from the Delivery Group. [#610109]
- To retain the original file extension on a Windows CE device, do not specify the Destination file name in the policy. [#610601]
- When configuring a VPN device policy for Mac OS X, the **VPN** option appears in the list of **Connection Types**. You cannot, however, configure this option for Mac OS X devices. [#612846]
- When updating from XenMobile 10.1 to version 10.3, if the WorxStore has a custom name, you must change the store name to the default setting of **Store** and deploy the setting to devices before updating. If not, the custom store name

causes issues with XenMobile 10.3 enrollment, access to Worx Home and the WorxStore, and app deployment on iOS devices. [#614049]

- You cannot enable Android for Work in the XenMobile console. When you configure Android for Work account settings and enter the service account ID you obtain from Google, which contains only numbers, an error appears when you save the settings. If you enter the service account ID using the earlier Google format that contained numbers and characters, the same error occurs because this format does not correspond to the service account ID in XenMobile server. This is a third-party issue.

  As a workaround, to enable Android for Work, add a server property for the Google client ID.

  1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
  2. Click **Add**. The **Add New Server Property** page appears.
  3. In the **Key** list, click **Custom Key**.
  4. In **Key**, enter **google.aw.enterprise.client.id**
  5. In **Value**, enter the numerical part of the client ID, such as 3838383838388383.
  6. Enter a **Display name**, such as "Google domain client ID."
  7. Click **Save**.

  [#615118]

- On Mac OS X computers and iPads, XenMobile 10.3 always carries out deletion (or removal) actions first, regardless of the order you set in the XenMobile console. [#620459]

- After you enable iOS bulk enrollment and update the root Certificate Authority (CA) of the XenMobile SSL certificate, device enrollment or re-enrollment may fail. The issue may occur when you change from a self-signed certificate to a public certificate, purchase a certificate from a new provider, or move to an internal corporate CA. The issue does not affect existing enrolled devices. As a work around, do the following:

  1. In the XenMobile console, click **Settings** > **iOS Bulk Enrollment**.
  2. Under **DEP Configuration**, next to **Allow Device Enrollment Program (DEP)**, click **NO** and then click **Save**. Wait for few seconds. This step removes the previous DEP profile from DEP devices on the Apple DEP portal.
  3. Click **Manage** > **Devices**. Check that no DEP registered device appears in the column **DEP registered**.
  4. Click **Settings** > **iOS Bulk Enrollment** again.
  5. Under **DEP Configuration**, next to **Allow Device Enrollment Program (DEP)**, click **YES** and then click **Save**. Wait for a few seconds. This step will force the adding of a new profile to all DEP devices.
  6. Click **Test Connection** to ensure that the connection between the XenMobile server and the Apple DEP servers is still functioning.
  7. Click **Manage** > **Devices** again. Check that all of the DEP devices are newly registered in the column **DEP registered**.

For more information about Apple DEP, see Bulk enrollment of iOS devices.
[#635699]

Architecture Overview

Jan 06, 2017

The XenMobile components in the XenMobile reference architecture you choose to deploy are based on the device or app management requirements of your organization. The components of XenMobile are modular and build on each other. For example, 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 Worx Home. **Note**: Starting with version 10.4, Worx Home is renamed 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 an app that was created within your organization or a mobile app made outside the company, such as the Citrix Worx apps (which are renamed XenMobile Apps with version 10.4). 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 Configuring Clustering for XenMobile 10.

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 XenMobile 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.

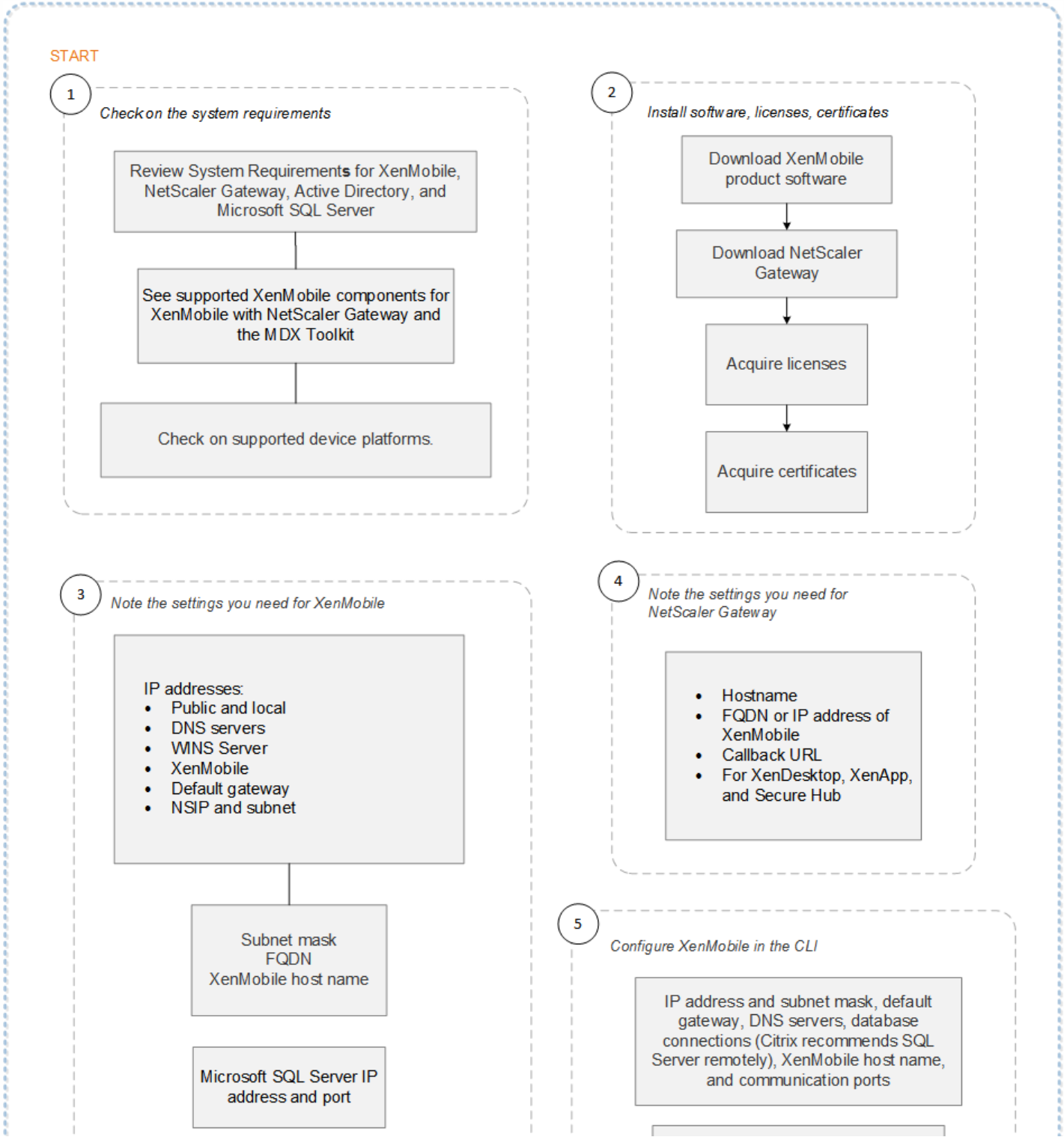
In the recommended deployment model, the XenMobile server is positioned in the DMZ with NetScaler Gateway in front, which provides additional protection for XenMobile.

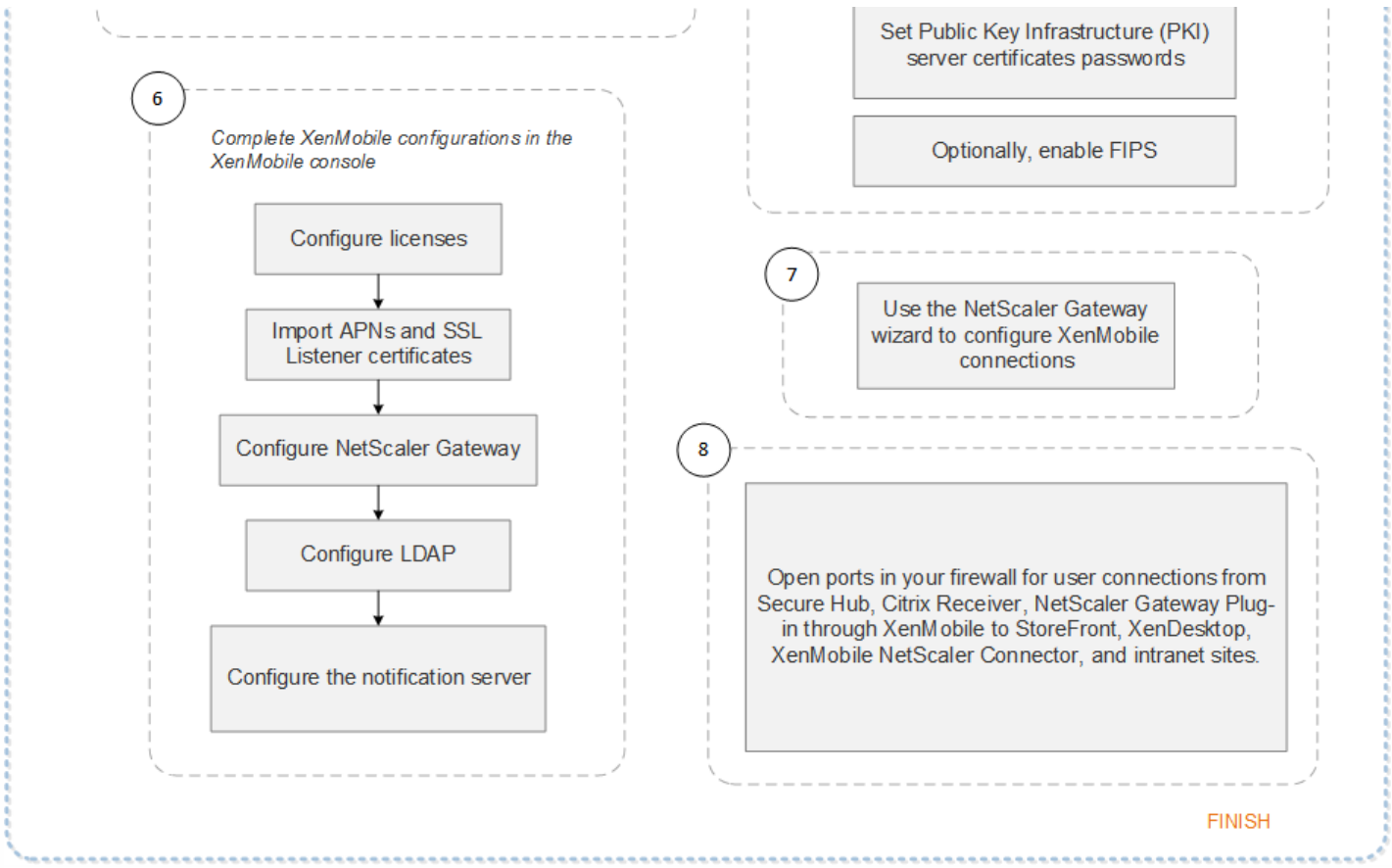
XenMobile in the internal network - Another deployment option is to position the XenMobile server in the internal network, rather than in the DMZ. This deployment is used if your security policy requires that only network appliances can be placed in the DMZ. With this deployment, because the XenMobile 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.

Flowchart for Deploying XenMobile with NetScaler Gateway

May 05, 2016

You can use this flowchart to guide you through the main steps for deploying XenMobile 10.3 with NetScaler Gateway. Links to topics on each step follow the figure.





1

- System Requirements for XenMobile 10.3
- XenMobile Compatibility
- Supported Device Platforms in XenMobile 10.3

2

- Installing XenMobile
- Certificates in XenMobile
- Licensing for XenMobile

3

- XenMobile Pre-Installation Checklist

4

- XenMobile Pre-Installation Checklist

5

- Configuring XenMobile in the Command Prompt Window

6

- Configuring XenMobile in a Web Browser

7

- Configuring Settings for Your XenMobile Environment

8

- XenMobile Port Requirements

The flowchart is also available in PDF format.

PDF Flowchart for Deploying XenMobile

XenMobile 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 offers answers to common questions on determining the requirements for small to large scale enterprise deployments.

Performance and Scalability Guidelines

The data in this article are intended as guidelines for determining performance and scalability of a XenMobile 10.3 infrastructure. The two key factors for determining how to configure your server and database are scalability (maximum users/devices) and logon rate.

- Scalability is defined as the maximum number of concurrent users executing a defined workload. For more information on the flows used to load the XenMobile infrastructure, see Workloads.
- Logon Rate is defined as the on-boarding of new users and the authentication of existing users.
  - On-boarding rate is the maximum number of devices that can be enrolled on the environment for the first time. Called First Time Use or FTU in this article, this data point is important when orchestrating a rollout strategy.
  - Existing user rate is the maximum number of users who authenticate to the environment, who have already enrolled and connected with their device. These tests included creating sessions for already enrolled users and the execution of Secure Mail and Secure Web apps.

The following table displays scalability guidelines based on the test results for the corresponding XenMobile environment.

Scalability	Up to 100,000 devices	
Logon Rates	On-boarding (FTU)	Up to 2,777 devices per hour
	Existing users	Up to 16,667 devices per hour
Configuration	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	XenMobile Server 10-node cluster
	Database	Microsoft SQL Server external database

Important

The automation requirement for this report is 1,000 to 100,000 devices. Any requirement that exceeds 100,000 devices is out of scope of this report.

System Configuration and Test Results

This section describes hardware configuration used and the results of running the on-boarding (FTU) workload and the Existing User workload scalability tests.

The following table defines the hardware and configuration recommendations for XenMobile when scaling from 1,000 to 100,000 devices. These guidelines are based on the test results and their associated workloads. The recommendations account for the acceptable margin of error as defined in Exit Criteria.

Analysis of the test results led to these conclusions:

- Logon rate is an important factor in determining the scalability of a system. In addition to the initial logon, logon rates are dependent upon the authentication time-out values configured in your environment. For instance, if you set the authentication time-out value too low, users must perform more frequent logon requests. Therefore, you need to clearly understand how time-out settings affect your environment.
- The number of connections per user session on NetScaler is an important consideration.
- An external database (SQL Server) with 128 GB of RAM, 300 GB of disk space, and 24 virtual CPUs was used for the tests and is recommended for production environments.
- To achieve maximum scalability, CPU and RAM resources were increased on XenMobile.
- The 10-node cluster configuration was the largest configuration validated. Scaling beyond 10 nodes requires an additional XenMobile implementation.

The following table shows the recommended on-boarding and existing user logon rates based on the XenMobile configuration, NetScaler Gateway appliance, cluster settings, and database. Use the data in this table to construct an optimal enrollment schedule for new deployments and returning user/device rates for existing deployments. The Configuration section relates enrollment and logon performance data to the appropriate hardware recommendations.

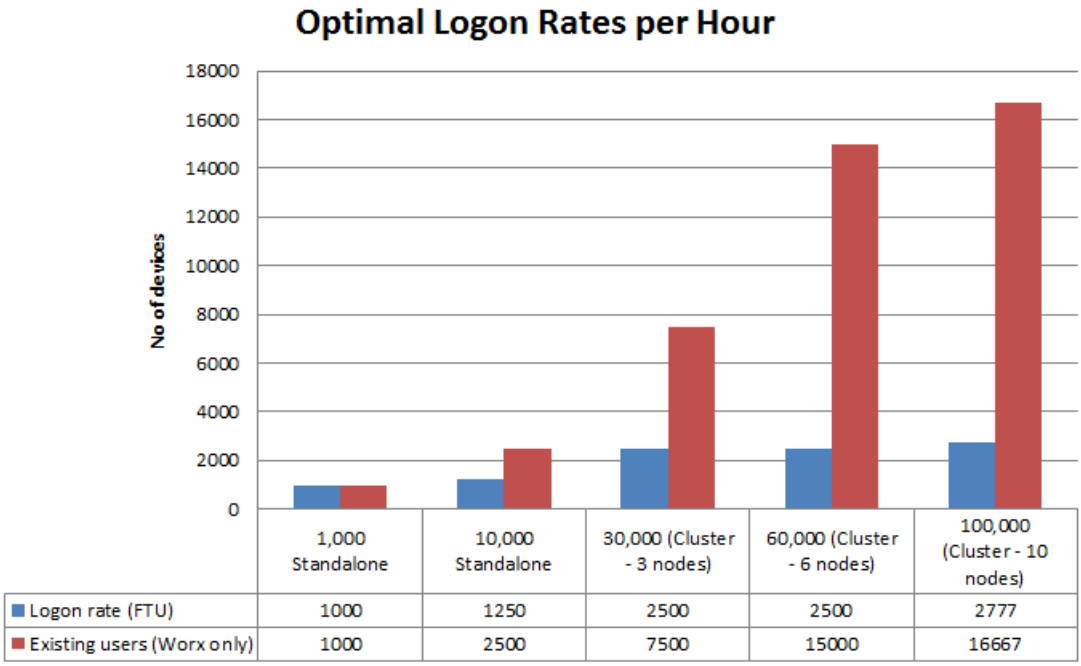
Expected number of devices	1,000	10,000	30,000	60,000	100,000
Actual number of devices	1,000	9,997	29,976	59,831	99,645
Logon Rate					
On-boarding (FTU)	125	1,250	2,500	2,500	2,777
Existing users (XenMobile Apps only)	1,000	2,500	7,500	15,000	16,667

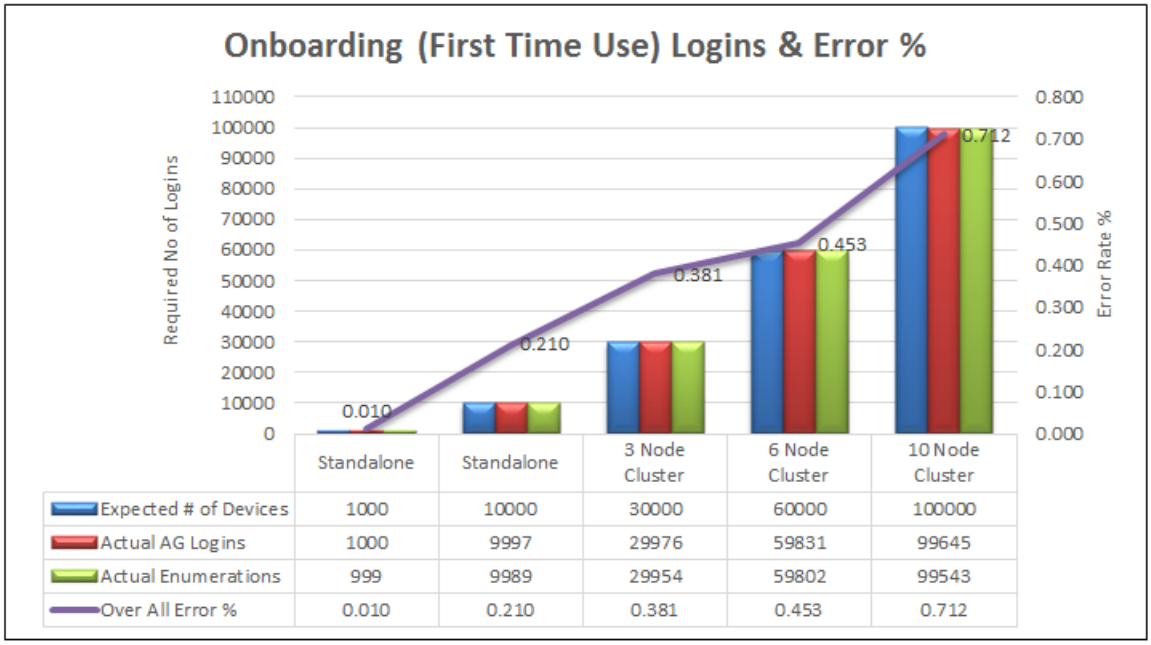
Configuration					
Reference environment	VPX-XenMobile Standalone	MPX-XenMobile Standalone	MPX-XenMobile Cluster (3)	MPX-XenMobile Cluster (6)	MPX-XenMobile Cluster (10)
NetScaler Gateway	VPX with 2 GB RAM 2 virtual CPUs	MPX-10500		MPX-20500	
XenMobile - mode	Standalone	Standalone	Cluster		
XenMobile - cluster	N/A	N/A	3	6	10
XenMobile - virtual appliance	8 GB RAM and 4 virtual CPUs	8 GB RAM and 4 virtual CPUs	8 GB RAM and 4 virtual CPUs	16 GB RAM and 4 virtual CPUs	16 GB RAM and 4 virtual CPUs
Database	External	External – Microsoft SQL Server Memory = 16 GB vCPUs = 12	External – Microsoft SQL Server Memory = 16 GB vCPUs = 12	External – Microsoft SQL Server Memory = 32 GB vCPUs = 12	External – Microsoft SQL Server Memory = 32 GB vCPUs = 16

Note: You will experience the following if you exceed the recommended rates or hardware recommendations when sizing your system.

The following information provides additional data points that were recorded and that affect the results in the preceding table.

- Enrollment or logon latency (round-trip time)
  - Total average latency: 0.5 to 1.5 seconds
  - Average latency for a NetScaler Gateway logon: >120 to 440 ms
  - Average latency for a XenMobile Store request: 2 to 3 seconds
- Physical performance degradation, such as CPU and memory exhaustion, was observed on the infrastructure components when scalability limits were reached.
  - Invalid responses on the NetScaler Gateway and XenMobile appliances.
  - Slow XenMobile console response time during high loads.





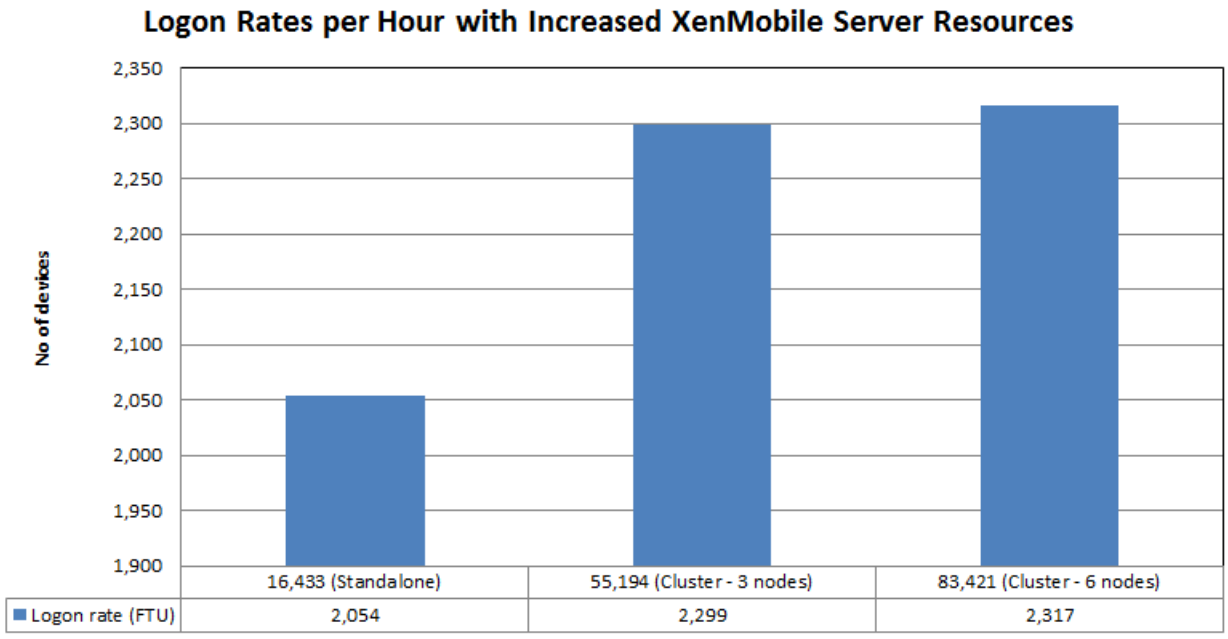
The error percentage in the preceding figure includes the overall error experienced considering requests corresponding to every operation and is not limited to logons. The error percentage is within the acceptable limit of 1% for each test run as defined in Exit Criteria.

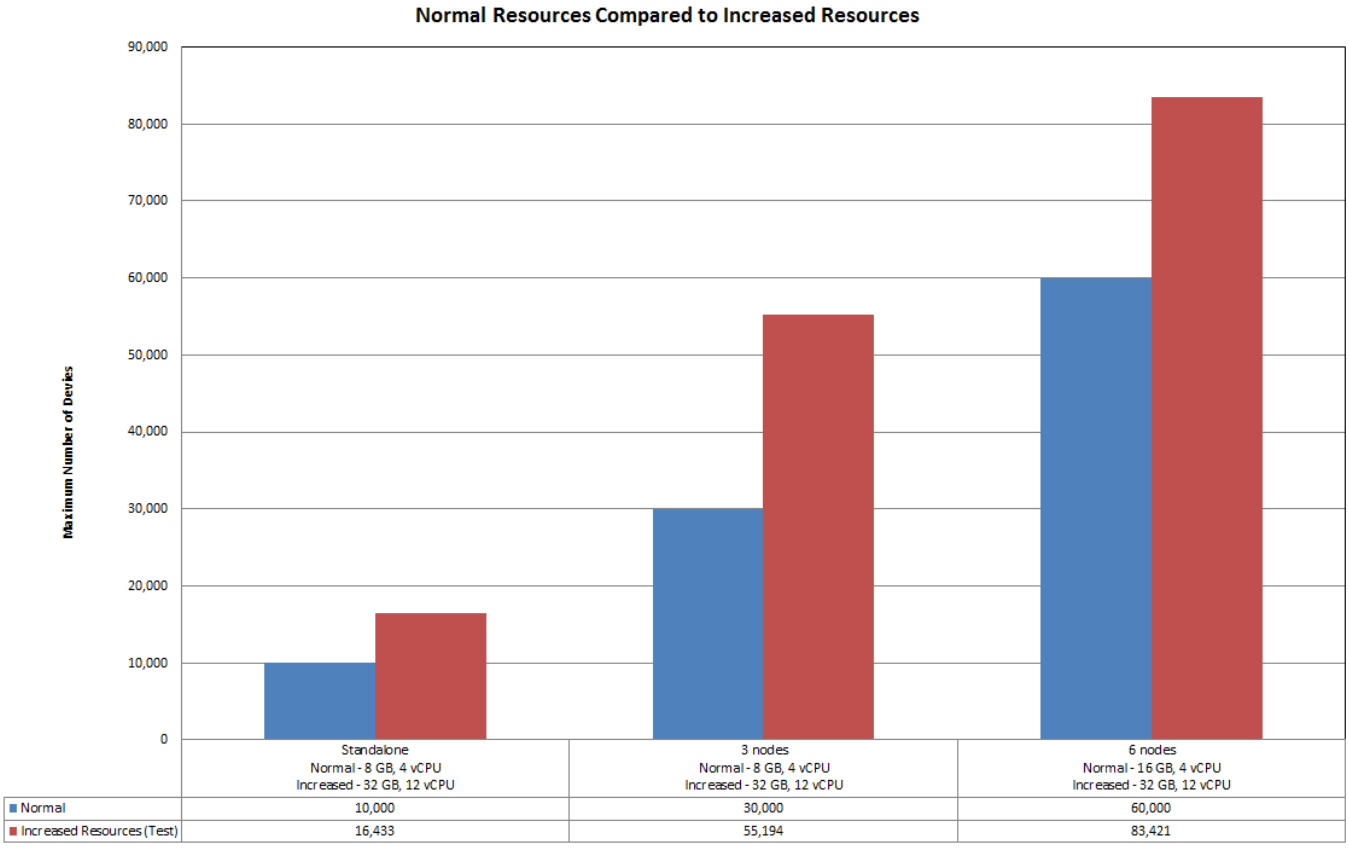
Scale Testing with Increased Resources for XenMobile Enterprise Edition

This test result provides insight into the deployment strategy for XenMobile Enterprise Edition with a lesser number of nodes to support more devices. The test has been run with increased resources for hardware components (CPU and memory) of each XenMobile server node, so as to measure its scale-up capabilities. This

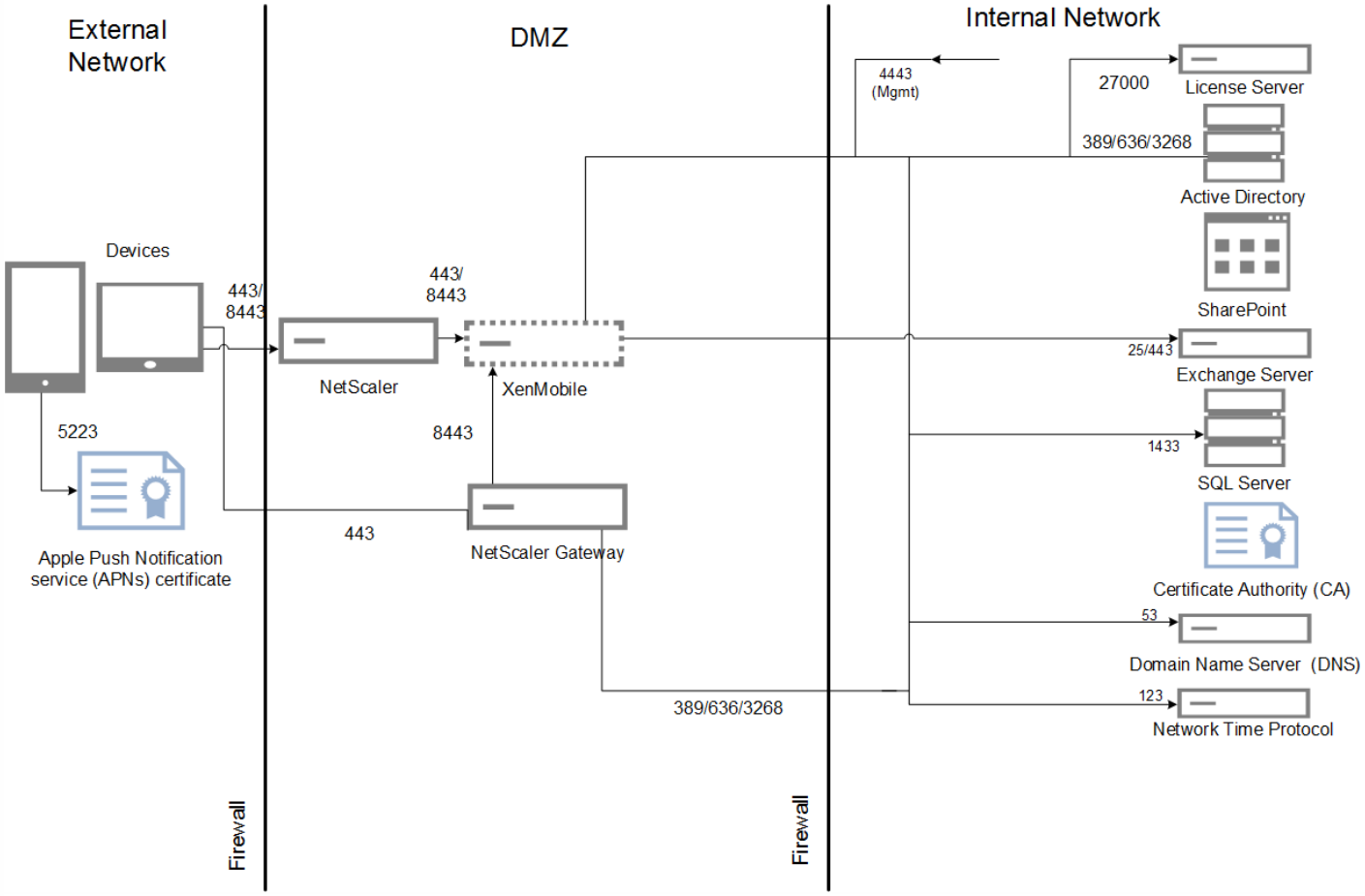
resulted in an increase in the maximum number of sessions/devices supported by the XenMobile server nodes when compared to test run with normal resources and the same number of nodes.

Scalability			
Maximum number of actual devices	16,433	55,194	83,421
Logon Rate			
Onboarding First Time Use - addition of new users	2,054	2,299	2,317
Configuration			
Reference environment	VPX-XenMobile Standalone	MPX-XenMobile Cluster 3	MPX-XenMobile Cluster 6
NetScaler Gateway	MPX-10500	MPX-10500	MPX-20500
XenMobile - mode	Standalone	Cluster	Cluster
XenMobile - cluster	N/A	3	6
XenMobile - virtual appliance	Memory - 32 GB vCPUs - 12	Memory – 32 GB vCPUs - 12	Memory - 32 GB vCPUs - 12
Device Manager database	External – S SQL Server Memory – 16 GB vCPUs - 12	External - SQL Server Memory – 32 GB vCPUs - 12	External -SQL Server Memory - 32GB vCPUs - 16
Active Directory	Memory – 8 GB vCPUs = 4	Memory - 16 GB vCPUs - 4	Memory – 16 GB vCPUs - 4

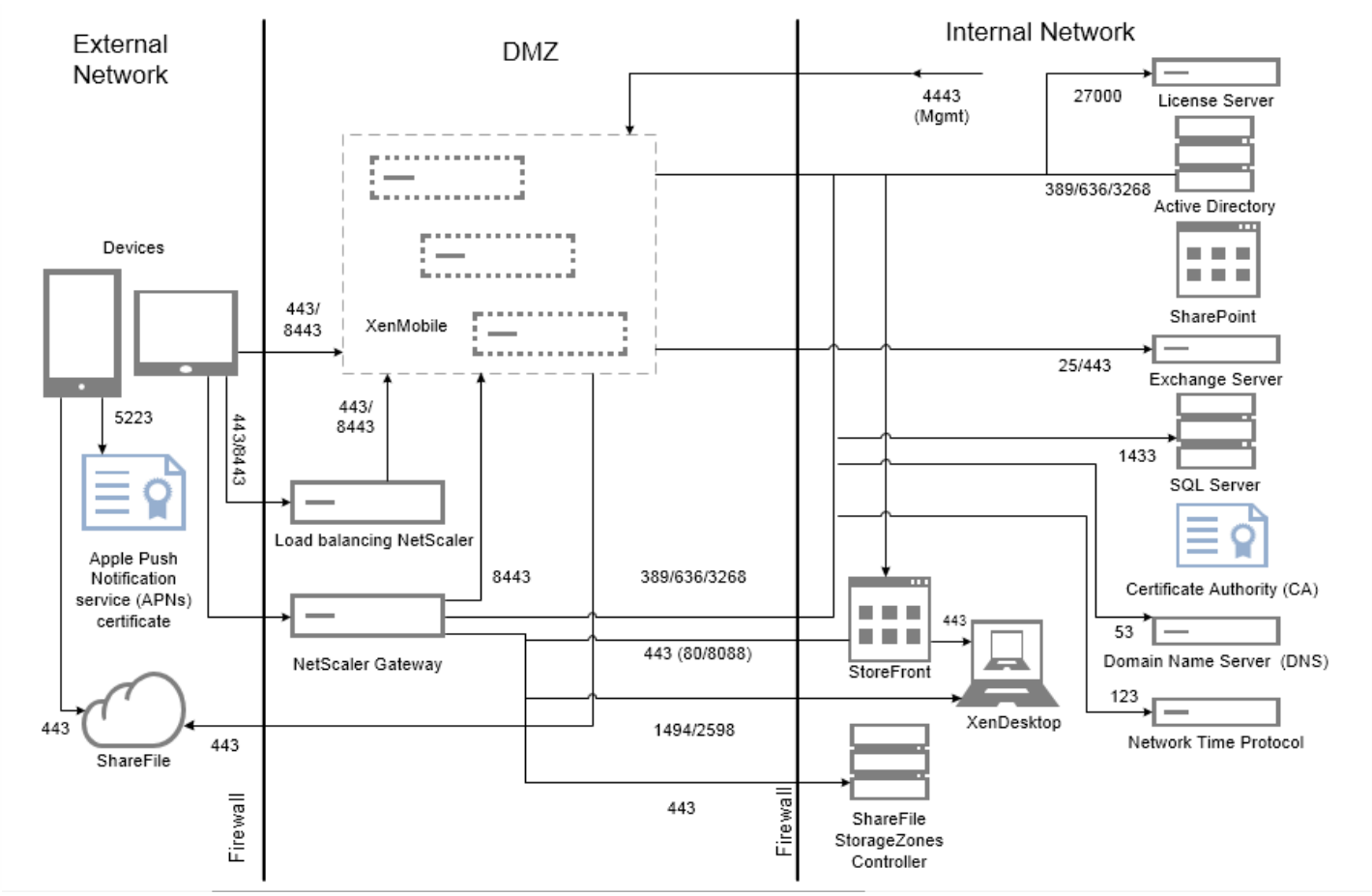




The following figure shows the reference architecture for a small scale deployment. It is a standalone architecture that supports up to 10,000 devices.



The following figure shows the reference architecture for an enterprise deployment. It is a clustered architecture with SSL offload for MAM over HTTP that supports 10,000 or more devices.



Test Methodology

The tests were run against XenMobile Enterprise to establish benchmarks. In an effort to target both small and large scale deployments, 1,000 to 100,000 devices were used in the measurements.

Workloads were created to simulate real-world use cases. These workloads were run for each test to study the effect on enrollment and logon rates. The objective of the tests was to obtain an optimal logon rate that was within the acceptable margin of error as outlined in Exit Criteria. Logon rates are a critical factor in determining the hardware configuration recommendations for the infrastructure components.

The On-boarding (FTU) workload logon requests included auto discovery, authentication, and device registration operations. Application subscription, installation, and launch operations were uniformly distributed throughout the test period. This provided the best real-world simulation of user actions. At the conclusion of the test, the session was logged out. The Existing User workload logon requests included only authentication requests.

Workloads

User workloads are defined as follows:

User	Includes NetScaler Gateway logons, enumerations, device registration, and so on for each session.

sessions/devices	
XenMobile Store launches	Users launch XenMobile Store multiple times and each time they subscribe to or install more than one app regardless of whether it is a mobile app (web/SaaS/MDX) or a Windows app (HDX).
Web/SaaS app SSO per device	Accounts for the launch sequence of web/SaaS apps up to the point where XenMobile completes the SSO and returns the actual app URL. Traffic was not sent to actual apps.
MDX app downloads per device	Counts of the number of MDX app downloads (this can happen across XenMobile Store launches). For iOS, this also includes the automation of app installation from Apple ITMS, which leverages the new token/tms service APIs on NetScaler Gateway.

Notes and Assumptions

In order to scale XenMobile beyond 30,000 devices, you should tune the following server parameters:

Config File - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/push_services.xml

- <property name="heartbeatFrequency" value="24" />

Config File - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/ew-config.properties

- ios.mdm.apns.connectionPoolSize=15
- hibernate.c3p0.max_size=1000

You should make these changes on all XenMobile nodes and then restart the server.

The following scenarios are not covered as part of the scalability tests. These scenarios would be considered for future enhancements in scale tests:

- Android Connected Devices not tested.
- Package deployment is not tested.
- Windows platform is not tested.

Each XenMobile supports a maximum of 10,000 connections simultaneously.

Tests were run in ideal conditions on LAN to ignore network latency issues. In a real world scenario, the scalability also depends on the user bandwidth available, especially for app downloads.

On-Boarding (FTU) Workload

The On-boarding (FTU) workload is defined as the first time a user accesses the XenMobile environment. Operations included in this workload were:

- Auto discovery
- Enrollment
- Authentication

- Device registration
- Application delivery (web, SaaS, and mobile MDX apps)
  - App subscription (including images and icon downloads)
  - Installation of the subscribed MDX apps
- App launch (web, SaaS, and mobile MDX apps) including device status checks
- Policy push (for iOS)
- Minimal Secure Mail and Secure Web connections (VPN tunnels) — two connections
- Installation of required apps through XenMobile

The workload parameters are defined by the following table:

Devices	Device registrations	Enumerations	Apps enumerated per device	Store launches per device	Web/SaaS SSO per device	MDX app downloads per device	Required app downloads triggered through XenMobile server	Policies pushed per device (iOS)
1,000	1,000	1,000	14	4	4	2	2	2
10,000	10,000	10,000	14	4	4	2	2	2
30,000	30,000	30,000	14	4	4	2	2	2
60,000	60,000	60,000	14	4	4	2	2	2
100,000	100,000	100,000	14	4	4	2	2	2

Existing Users with XenMobile-Only Connections Workload

The following table shows the existing users (with XenMobile only connections) workload. This workload simulated use of Secure Mail and Secure Web to measure NetScaler Gateway scalability within the XenMobile configuration. This is achievable because by only using these two apps, the network is under minimal load. On Secure Web, the user is accessing internal web sites that don't trigger the XenMobile server SSO. Operations in this mode included:

- Authentication (NetScaler Gateway and XenMobile)
- Secure Mail and Secure Web connections (VPN tunnels) — four connections

The following table shows the workload parameters for existing users.

Devices	Enumerations	**Apps enumerated per device**	**VPN tunnels per device**[1]
1,000	1,000	14	4
10,000	10,000	14	4
30,000	30,000	14	4
60,000	60,000	14	4
100,000	100,000	14	4

1. The number of VPN tunnels corresponds to Secure Mail and Secure Web connections.

The connection profiles for Secure Mail andSecure Web are outlined in the following table:

Device connection	**Connection type**	**Data sent per session**[1]	**Data received per session**[1]
Secure Mail Connection #1	Type 1[2]	4.1 MB	4.1 MB
Secure Mail Connection #2	Type 1	6.3 MB	12.5 MB
Secure Web Connection #1	Type 2[3]	5.2 MB	15.7 MB
Secure Web Connection #2	Type 2	4.1 MB	3.4 MB
Total bytes transferred per session[1]		~19.7 MB	~ 40.7 MB

1. Per session: 8 hours.

2. Type 1: Asymmetric send and receive with long lived connections (that is, Secure Mail with a dedicated Microsoft Exchange mailbox connection).

3. Type 2: Asymmetric send and receive with connections that close and reopen after delays (that is, Secure Web connections).

These recommendation are based on the Secure Mail and Secure Web profiles used to automate a "medium" workload. Modifications to the connection details affect analysis results. For example, if the number of connections per user is increased, the number of NetScaler Gateway sessions supported may be reduced.

Secure Mail and Secure Web Profiles

The profiles used for each app are intended to automate a "very heavy" workload.The following tables show the Secure Mail and Secure Web profile details.

Secure Mail Profile for a Medium Workload

Messages sent per day	20
Messages received per day	80
Messages read per day	80
Messages deleted per day	20
Average message size (KB)	200

Secure Web Profile for Medium Workload

Number of web apps launched	10
Number of web pages opened manually	10
Average number of request–response pairs per web app	100
Average size of request (bytes)	300
Average size of response (bytes)	1000

Configuration and Parameters

The following configurations were used when running the scalability tests:

- NetScaler Gateway and load balancing (LB) virtual servers coexisted on the same NetScaler Gateway appliance.
- A 2048-bit key was used on NetScaler Gateway for SSL transactions.

Exit Criteria

Logon rates are the foundation of this analysis. They provide the guidelines for the infrastructure components and their respective configurations. It is important to note that the logon rates take into account a margin of error that consists of the following:

- Invalid responses
  - A response with status code 401/404 instead of 200 is considered invalid.
- Request time-outs
  - A response is expected within 120 seconds.
- Connection errors
  - A connection reset occurs.
  - An abrupt connection termination occurs.

The logon rate is acceptable if the overall error rate is less than 1 percent of the total requests that are sent from a given device. The error rate includes errors corresponding to each individual workload operation, as well as the physical performance of the infrastructure component, such as CPU and memory exhaustion.

Software and Hardware Details

The following table lists the XenMobile infrastructure software used for these tests.

Component	Version
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
External database	Microsoft SQL Server 2014

The scalability tests were run on a XenServer platform as outlined in the following table.

Vendor	Genuine Intel
Model	Intel Xeon CPU — E5645 @ 2.40 GHz (CPUs = 24)

This includes the infrastructure core services (for example, Active Directory, Windows Domain Name Service (DNS), Certificate Authority, Microsoft Exchange, and so on), as well as the XenMobile components (XenMobile virtual appliance and the NetScaler Gateway VPX virtual appliance, where applicable).

System Requirements

Dec 05, 2016

To run XenMobile 10.3, you need the following minimum system requirements:

- One of the following:
  - XenServer (supported versions: 6.5.x or 6.2.x); for details, refer to XenServer
  - VMware (supported versions: ESXi 5.1, ESXi 5.5, or ESXi 6.0); for details, refer to VMware. Note that ESXi 6.0 is only supported on XenMobile 10.3.x
  - 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

The recommended configuration for 10,000 and more devices is the following:

- Quad core processor with 8 GB of RAM for each node.

XenMobile version 10.3.x requires the 11.12.1 Citrix License Server or later.

NetScaler Gateway System Requirements

To run NetScaler Gateway with XenMobile 10.3, you need the following minimum system requirements:

- One of the following:
  - XenServer (supported versions: 6.2.x, 6.1.x, or 6.0.x)
  - 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 10.3 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 10.3 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 9.3.11 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 10.3 Mail Server Requirements

XenMobile 10.3 supports the following mail servers:

- Exchange 2016
- Exchange 2013
- Exchange 2010

XenMobile Compatibility

Feb 11, 2016

For a summary of XenMobile components that you can integrate, see XenMobile Compatibility.

Supported Device Platforms

Feb 10, 2016

You can find the complete list of devices that XenMobile 10.x supports for enterprise mobility management in Supported Device Platforms in XenMobile.

Port Requirements

Jan 06, 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.

> **Note**
>
> Starting with version 10.4, Worx Home is renamed Secure Hub.

Opening Ports for NetScaler Gateway and XenMobile to Manage Apps

You must open the following ports to allow user connections from Worx Home, 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	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	XML and Secure Ticket Authority (STA) port used for enumeration, ticketing, and authentication.	StoreFront and Web Interface XML network traffic	XenDesktop or XenApp
443			

	Citrix recommends using port 443.	NetScaler Gateway STA	
123	Used for Network Time Protocol (NTP) services.	NetScaler Gateway	NTP server
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, Worx Home for Android, or Worx Home 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 Worx Home 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 Worx Home for the environment in which the device is enrolling. Worx Home 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 Worx Home 10.2 for Android, open port 443 for the following FQDN and IP addresses:

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

FIPS 140-2 Compliance

Apr 07, 2015

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: 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.

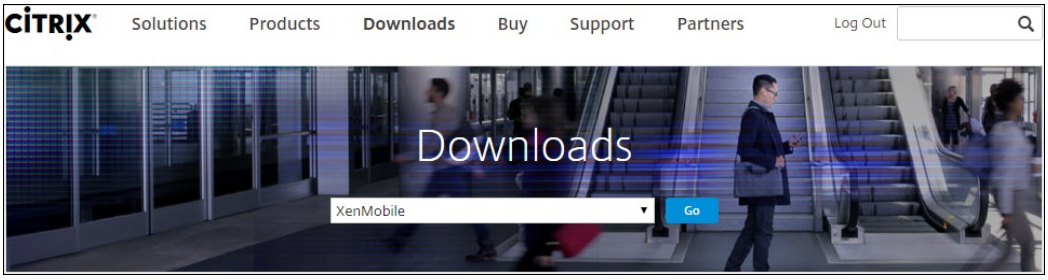
MDX apps are supported on Windows Phone 8.1 and use cryptographic libraries and APIs that are FIPS-compliant on Windows Phone 8. All data-at-rest for MDX apps on Windows Phone 8.1 and all data-in-transit between the Windows Phone 8.1 device and NetScaler Gateway are encrypted using these libraries and 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.

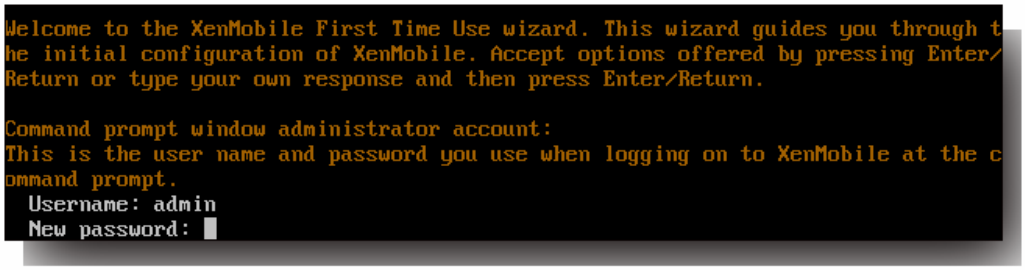
For the full XenMobile FIPS 140-2 compliance statement, including the specific modules used in each case, contact your Citrix representative.

	• •		

•			



-
  -
  -
  -
  -



```
Network settings:
  IP address: 192.0.2.0
  Netmask: 225.225.225.128
  Default gateway: 203.0.113.3
  Primary DNS server: 192.0.2.4
  Secondary DNS server [optional]: 192.0.2.5

  Commit settings [y/n]: y
```

```
Encryption passphrase:
  Generate a random passphrase to secure the server data? [y/n]: y
```

```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

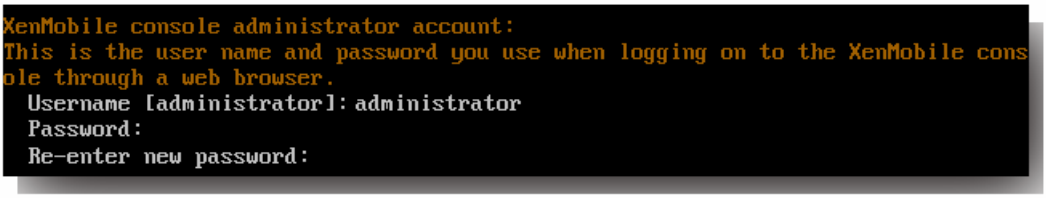
```
Database connection:
  Local or remote [l/r]: r
  Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi
  Use SSL [y/n]: n
  Server: 198.0.2.10
  Port: 5432
  Username: postgres
  Password:
```

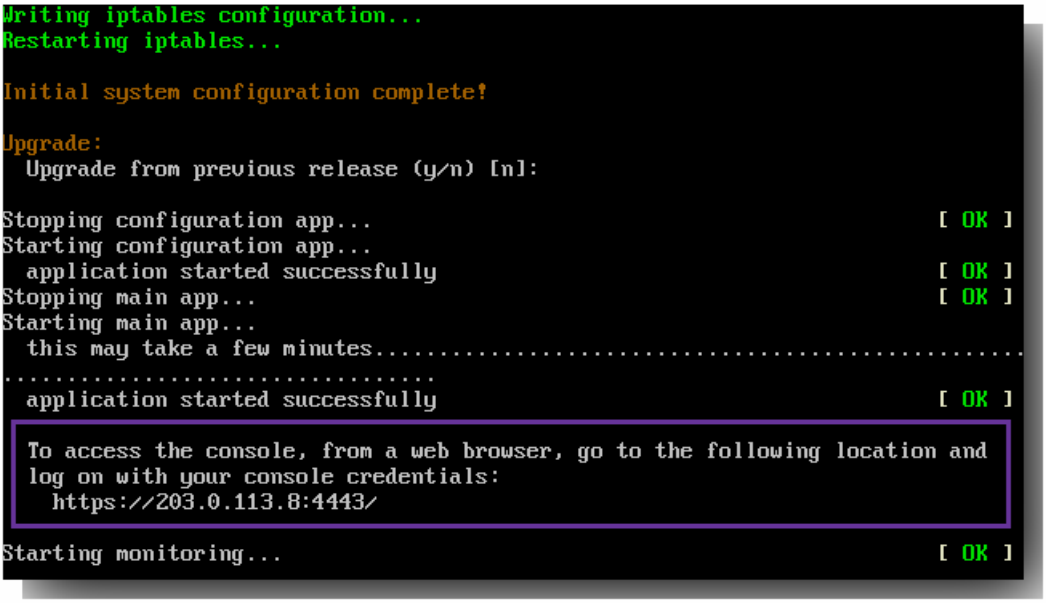
-
-

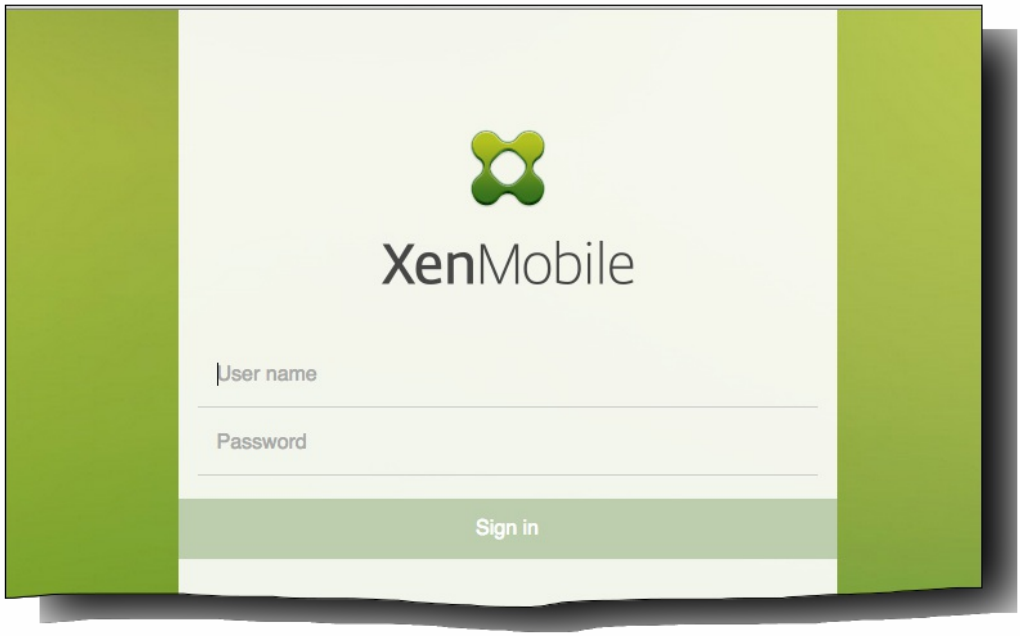
```
XenMobile hostname:
  Hostname: justan.example.com
```

```
  HTTP [80]: 80
  HTTPS with certificate authentication [443]: 443
  HTTPS with no certificate authentication [8443]: 8443
  HTTPS for management [4443]: 4443
```

```
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:
```







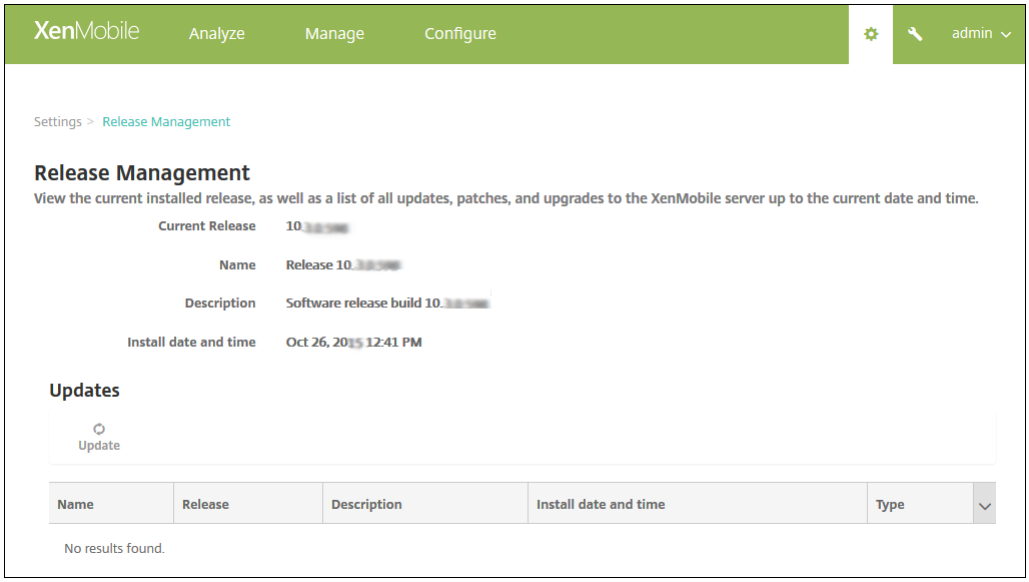
-
-

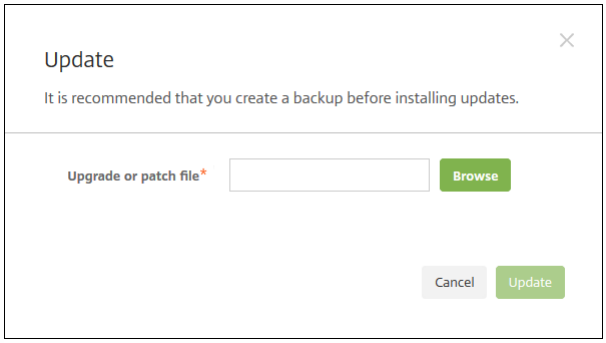
-
-
-

-
-
-

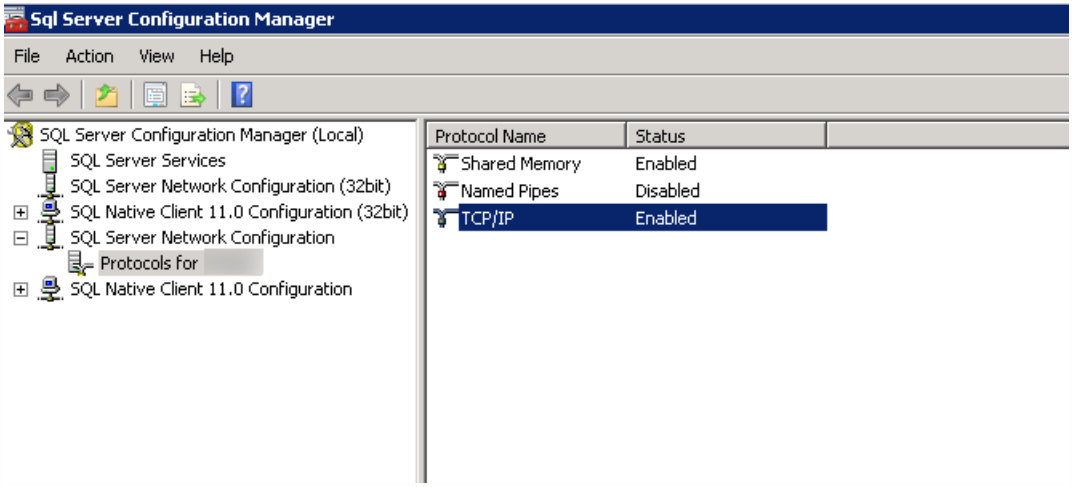
-
-
-

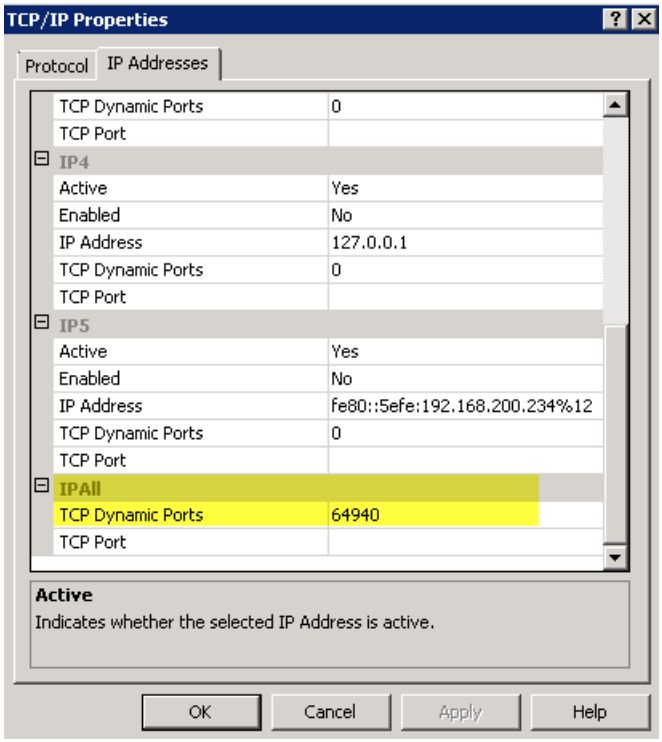
-
-
-

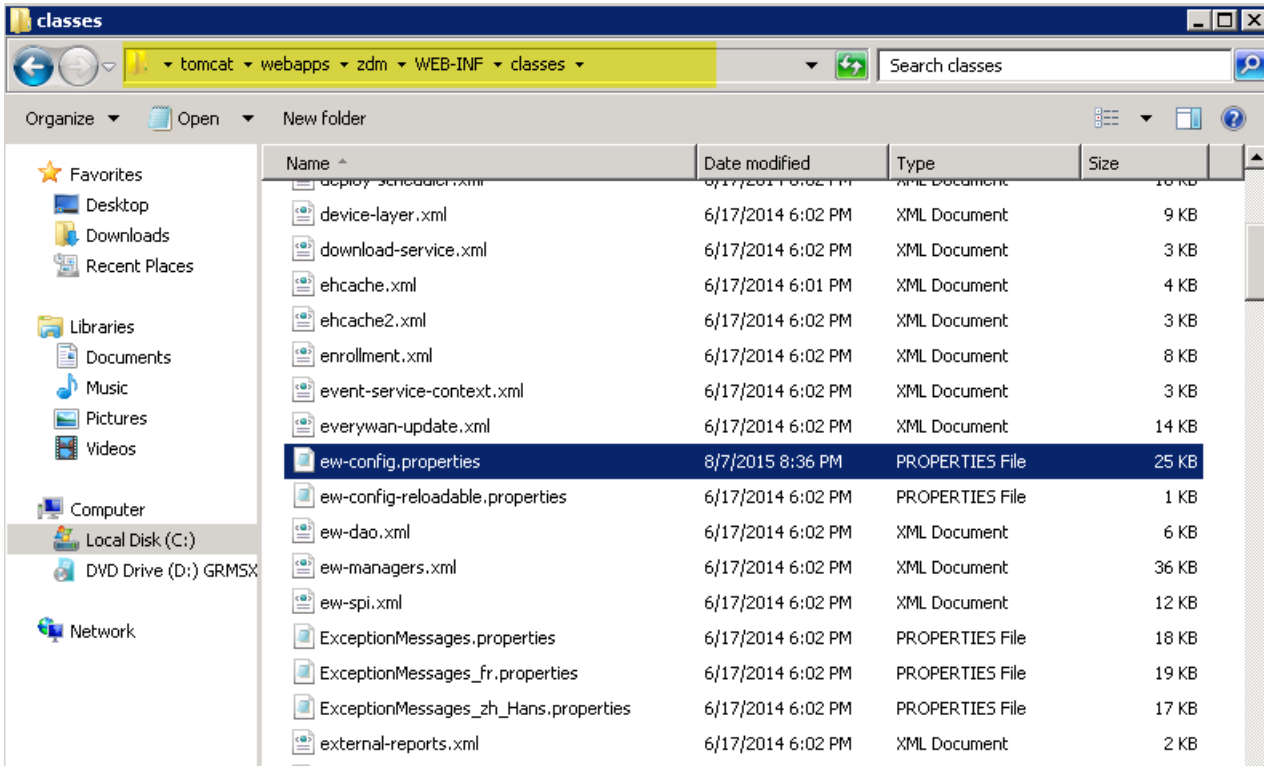




-
-
-





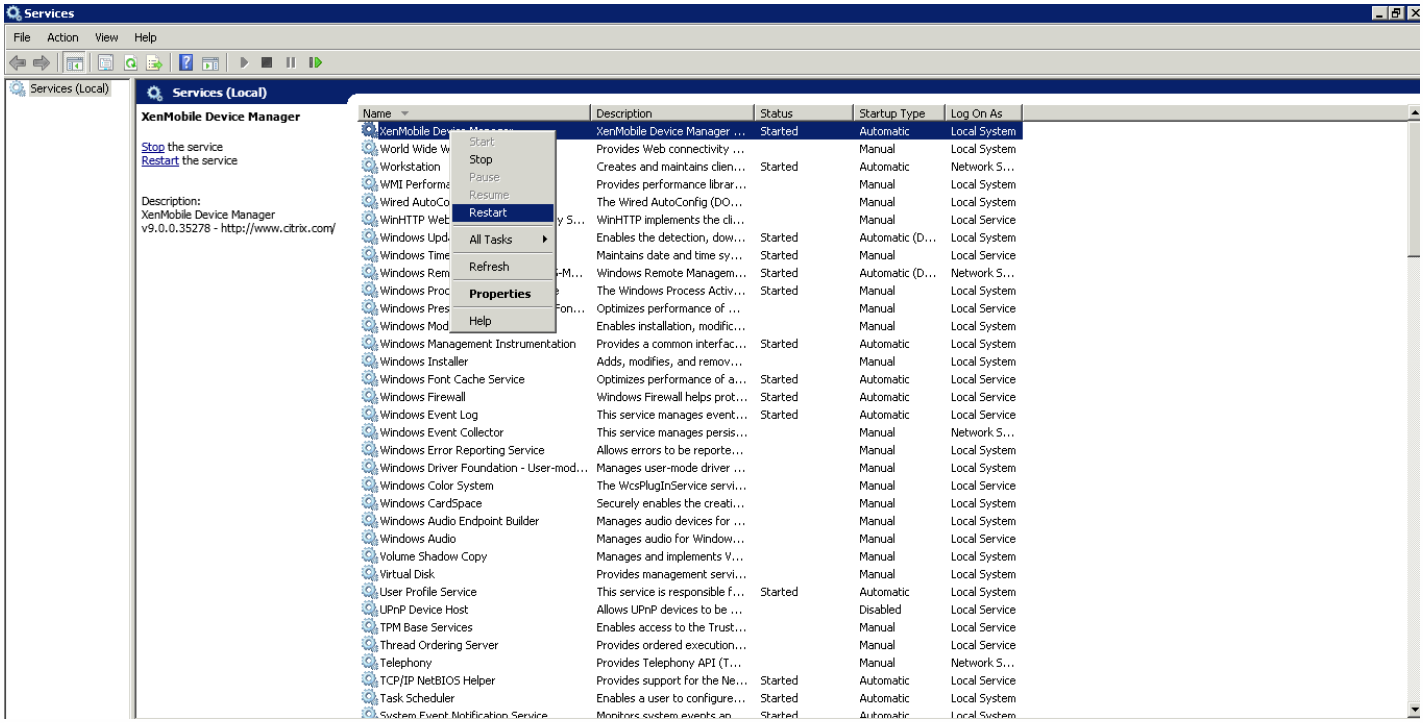


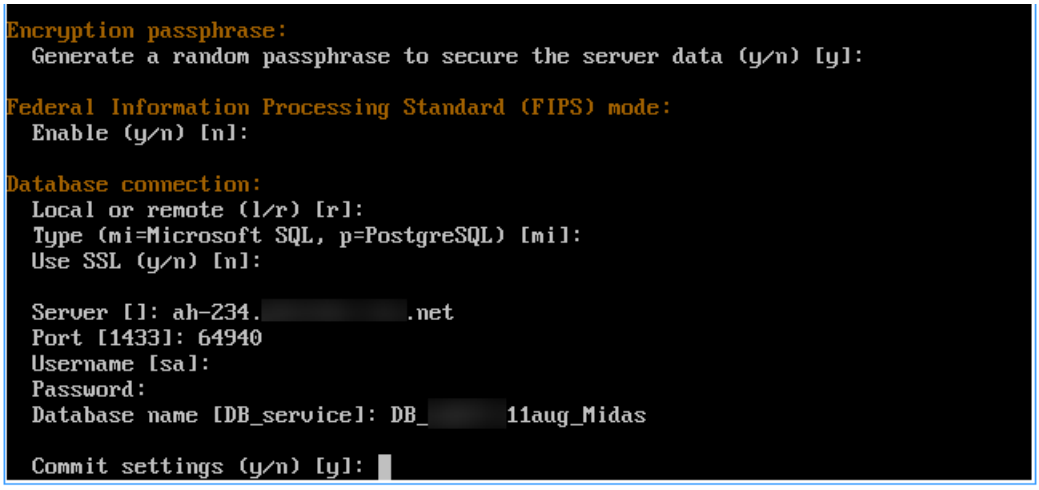
ew-config.properties

```
# 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-
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234                net/          -llaug;instance=
# Pooled datasource host name
pooled.datasource.hostname=ah-234.          .net
# Pooled datasource database
pooled.datasource.database=                aug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}                          ==

# No pooled datasource driver
#no.pooled.datasource.driver=org.postgresql.Driver
# No pooled datasource url
#no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
# No pooled datasource user
#no.pooled.datasource.user=everywan
# No pooled datasource password
#no.pooled.datasource.password=everywan

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://ah-234                /          -llaug;instance=
# 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
```

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
```





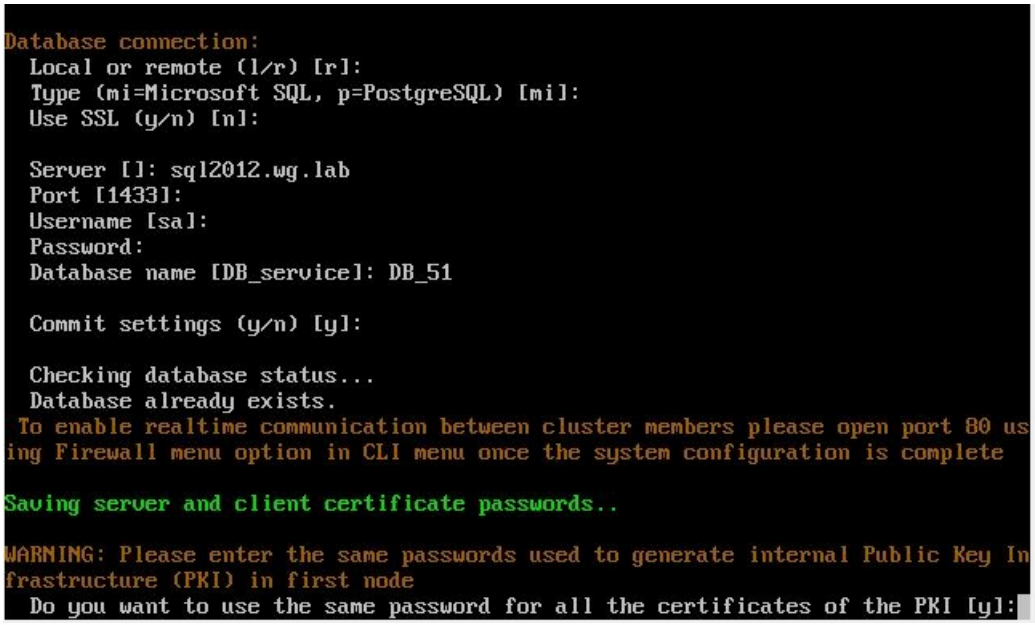
-
-
-
-
-
-

```
Network settings:
  IP address []: 10.147.75.51
  Netmask []: 255.255.255.0
  Default gateway []: 10.147.75.1
  Primary DNS server []: 10.147.75.240
  Secondary DNS server (optional) []:

  Commit settings (y/n) [y]:
Applying network settings...
eth0: intr type 3, mode 0, 3 vectors allocated
eth0: NIC Link is Up 10000 Mbps
```

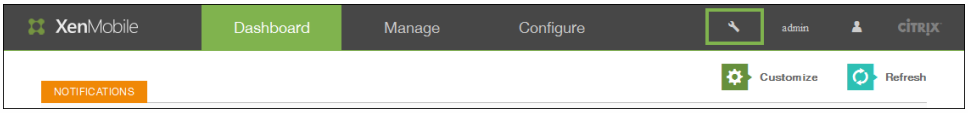
```
Encryption passphrase:
  Generate a random passphrase to secure the server data (y/n) [y]:
```

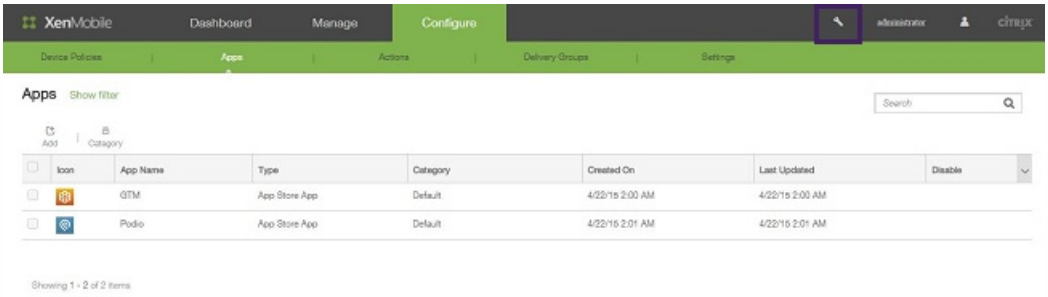
```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

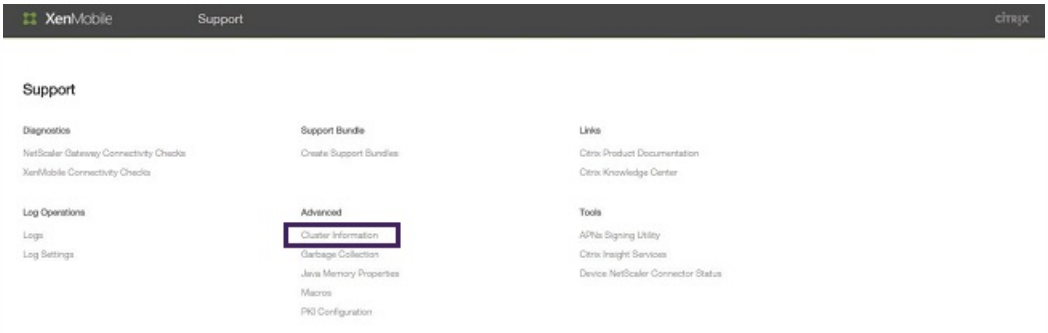
```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

  Server []: sql2012.wg.lab
  Port [1433]:
  Username [sa]:
  Password:
  Database name [DB_service]: DB_51

  Commit settings (y/n) [y]:

  Checking database status...
  Database already exists.
 To enable realtime communication between cluster members please open port 80 us
ing Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..
```

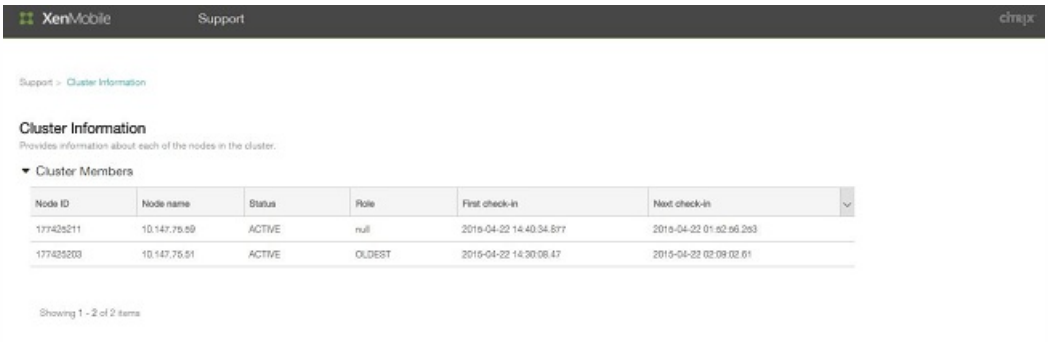


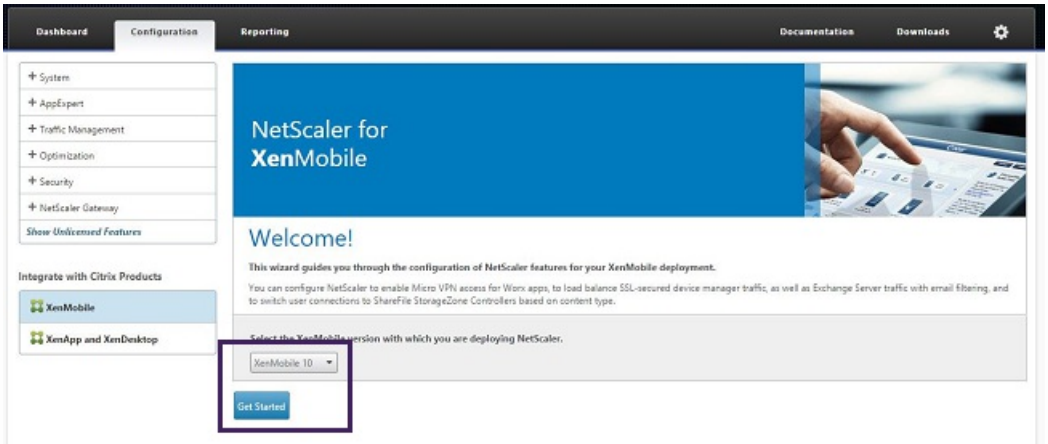
```
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app...                                    [ OK ]
Starting configuration app...
  this may take a few seconds.......
  application started                                            [ OK ]
Stopping main app...                                             [ OK ]
Starting main app...
  this may take a few minutes.....................^[.....................
.....................................
  application started                                            [ OK ]

  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://10.147.75.59:4443/

Starting monitoring...                                           [ OK ]

xms51.wg.lab login:
```

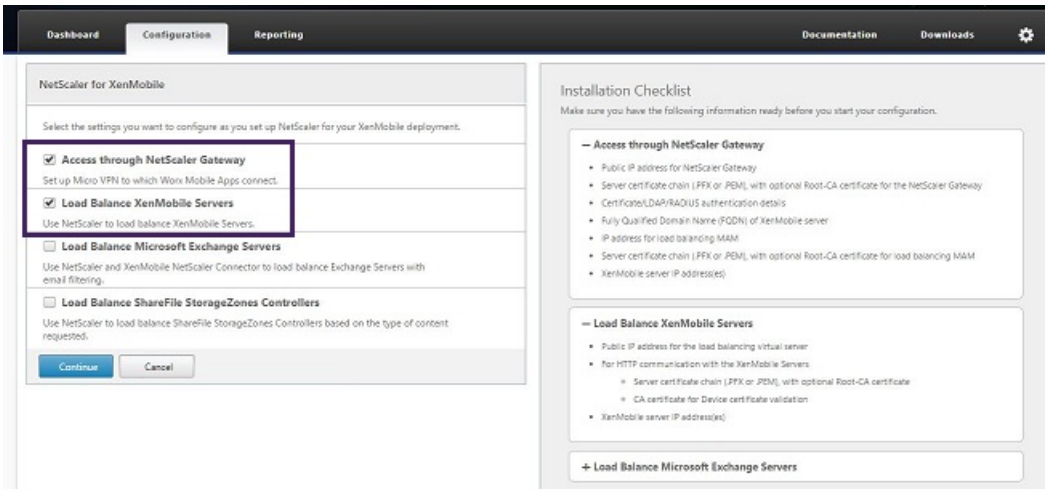


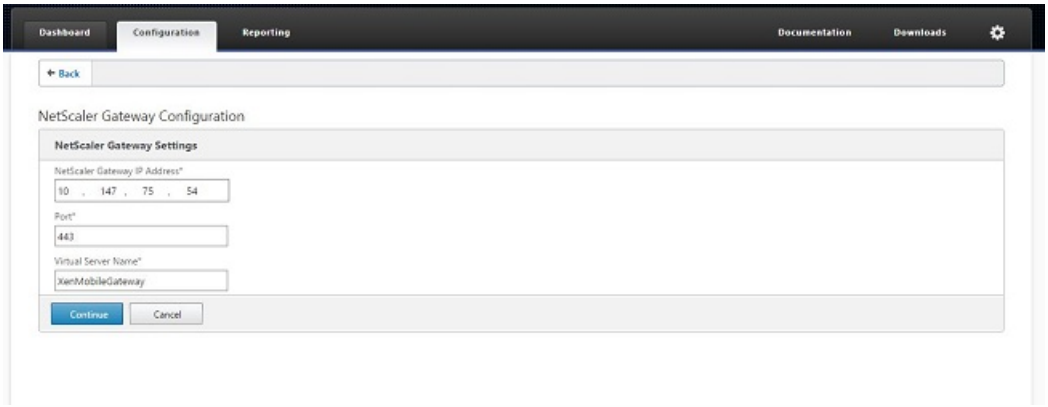




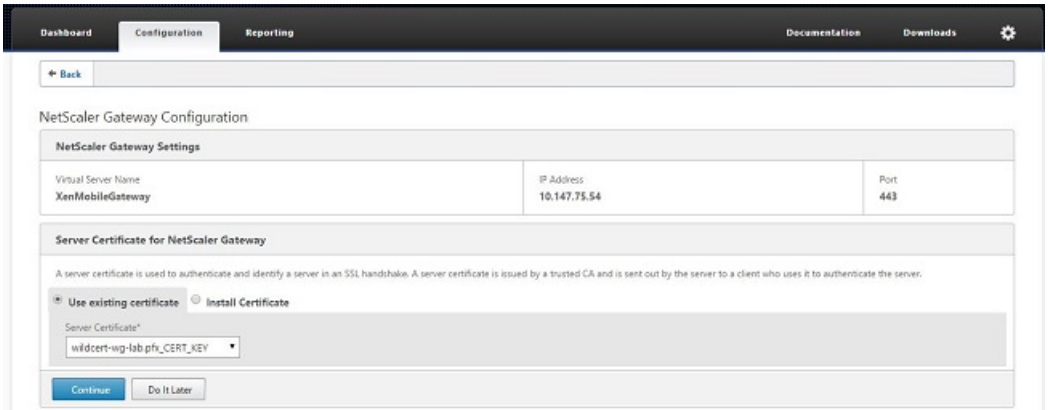


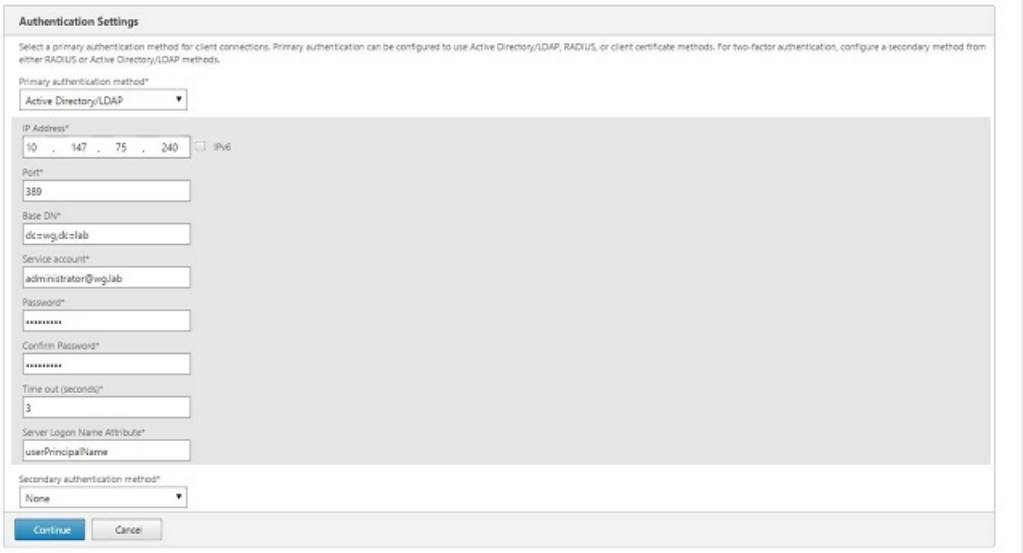


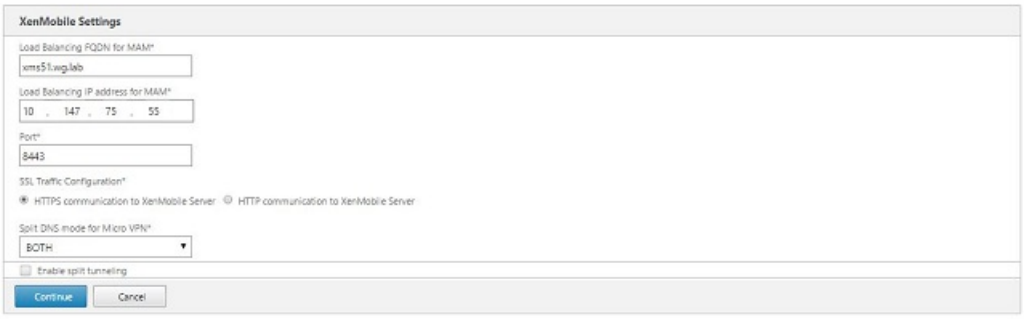


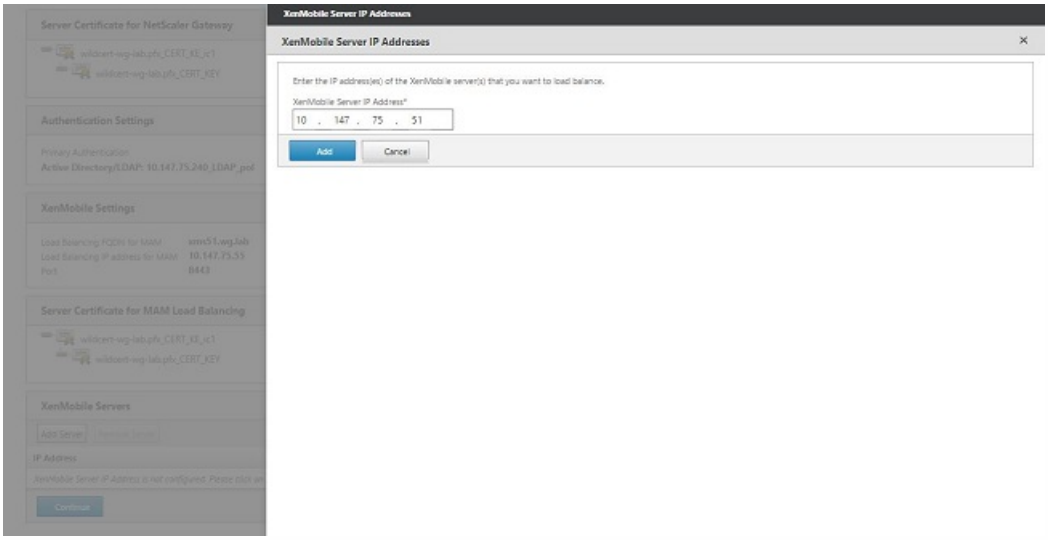


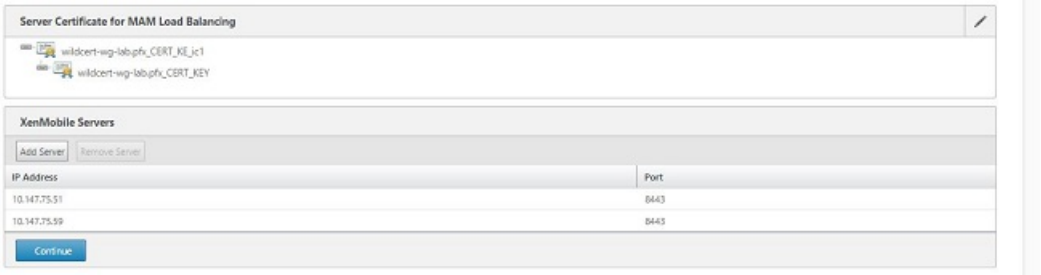
-
-

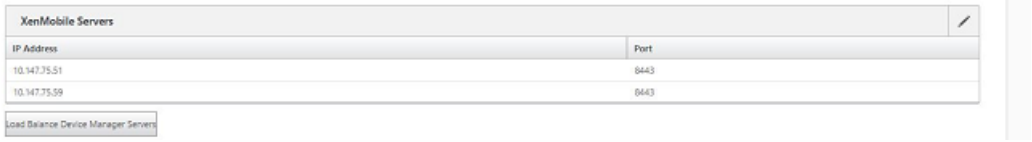


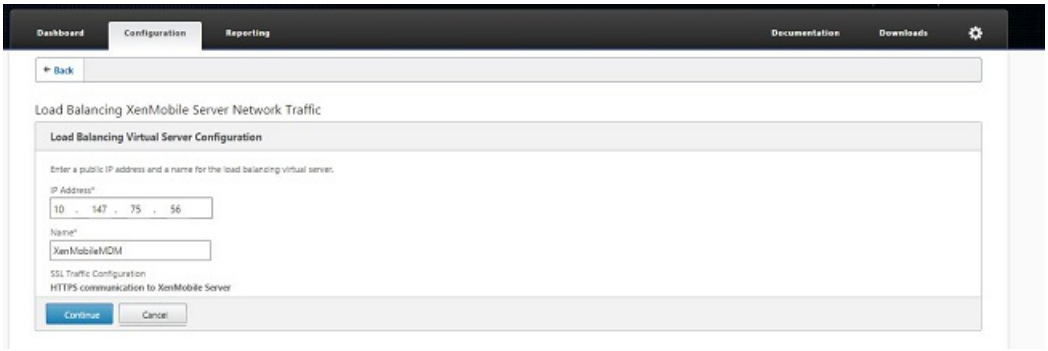


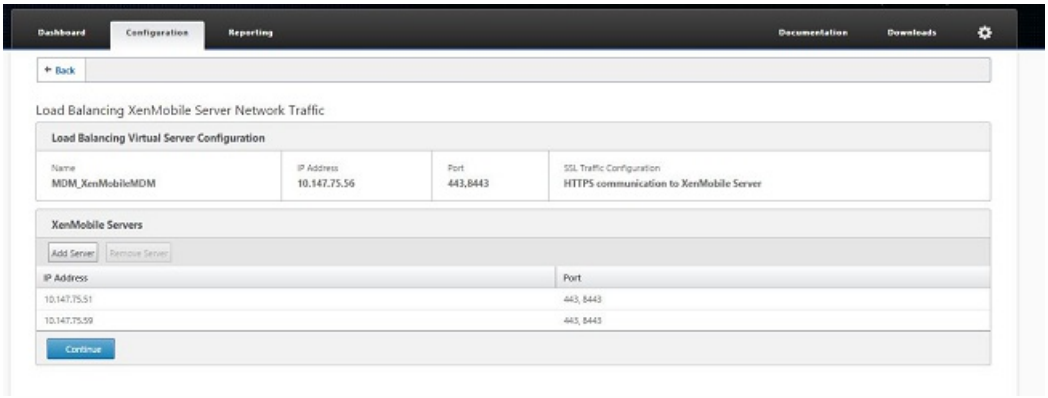


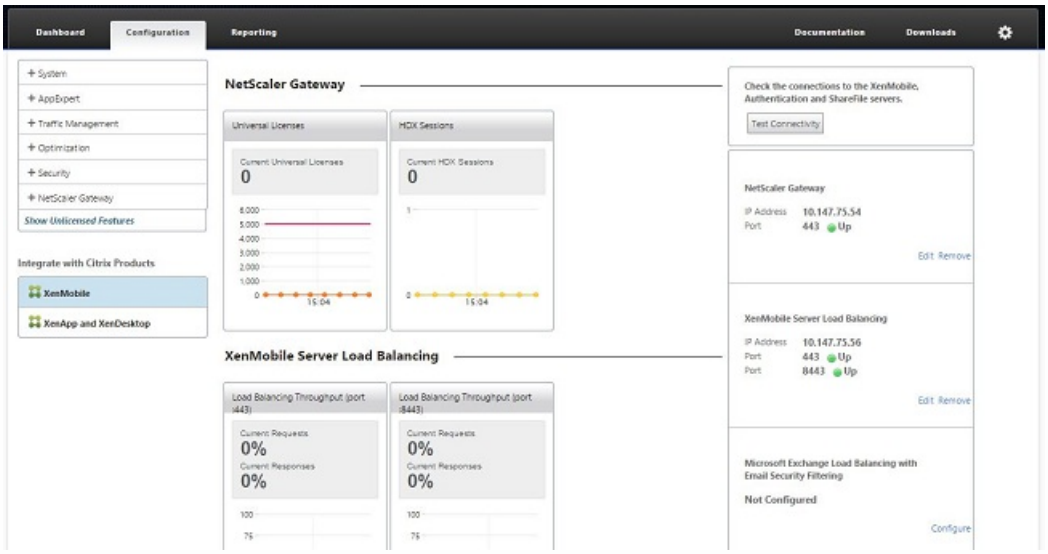


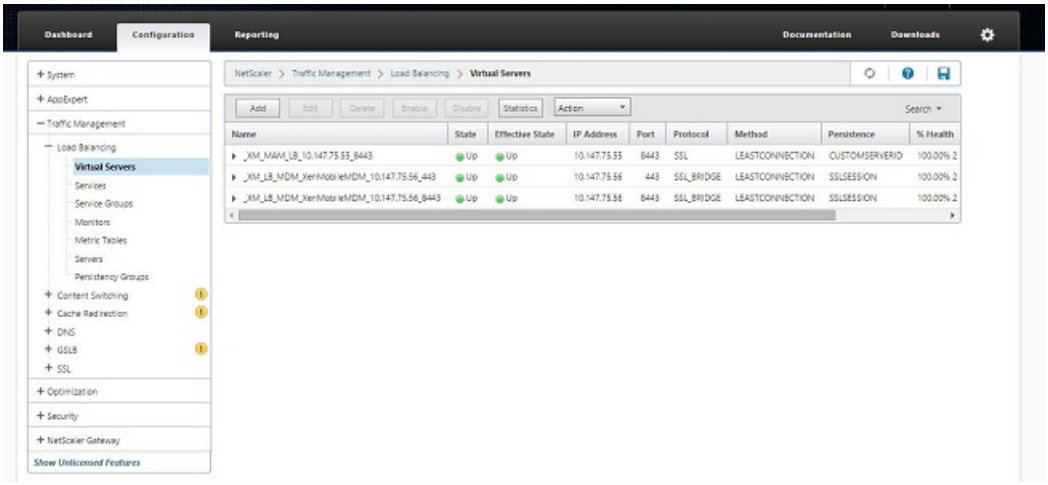


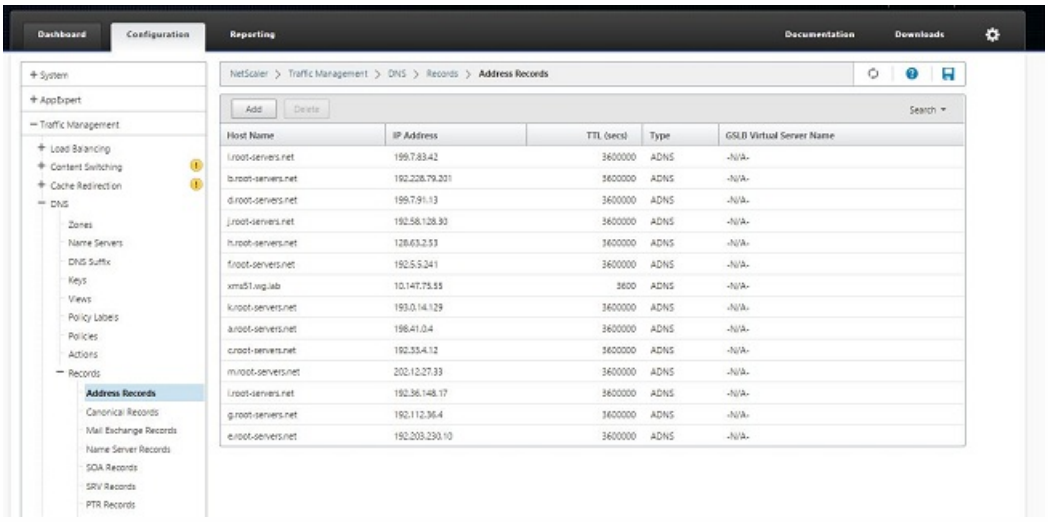


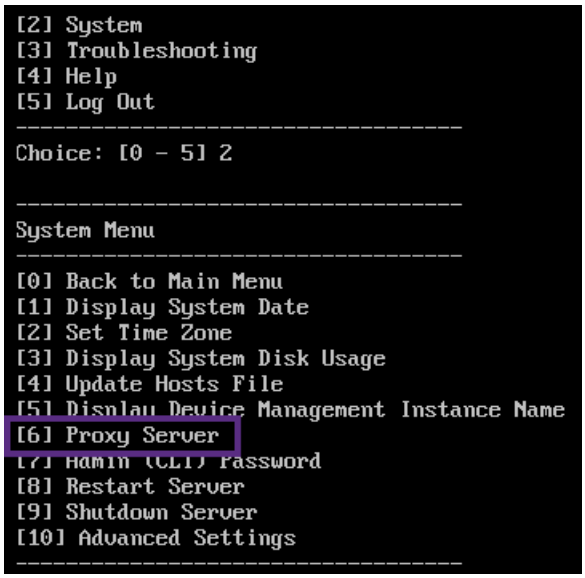


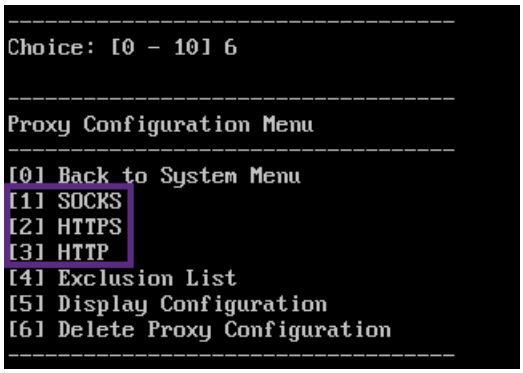


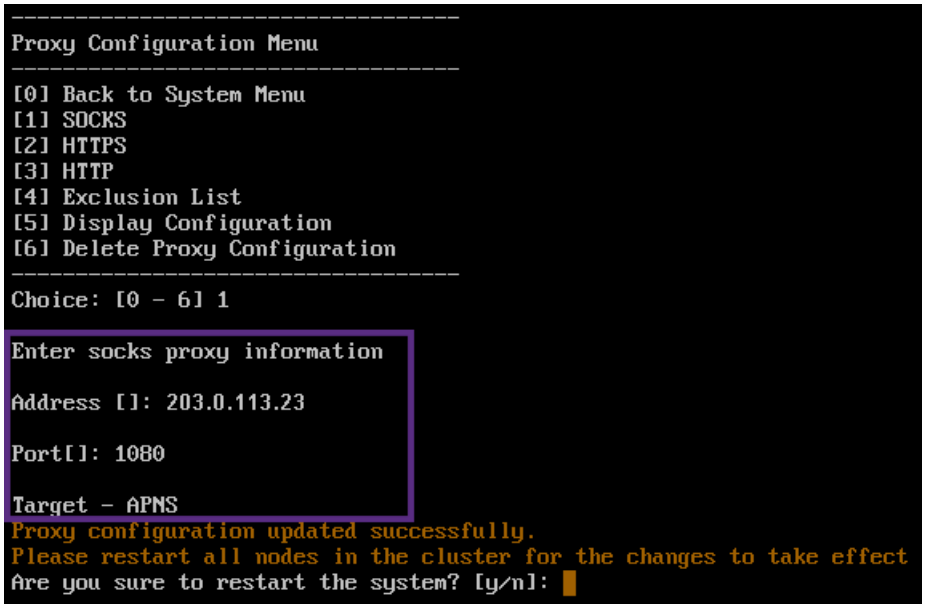


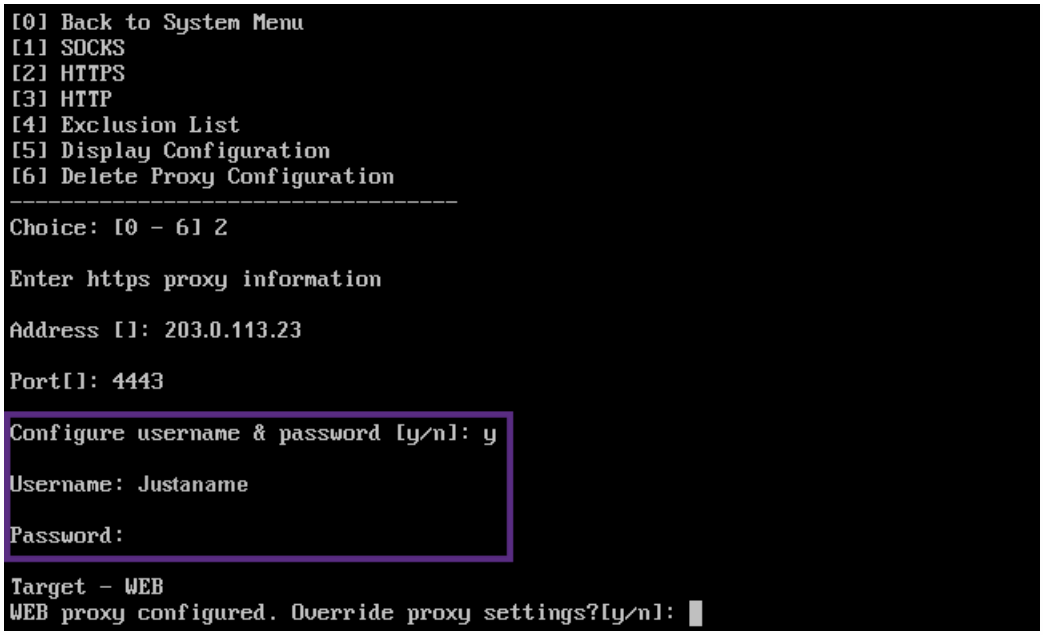


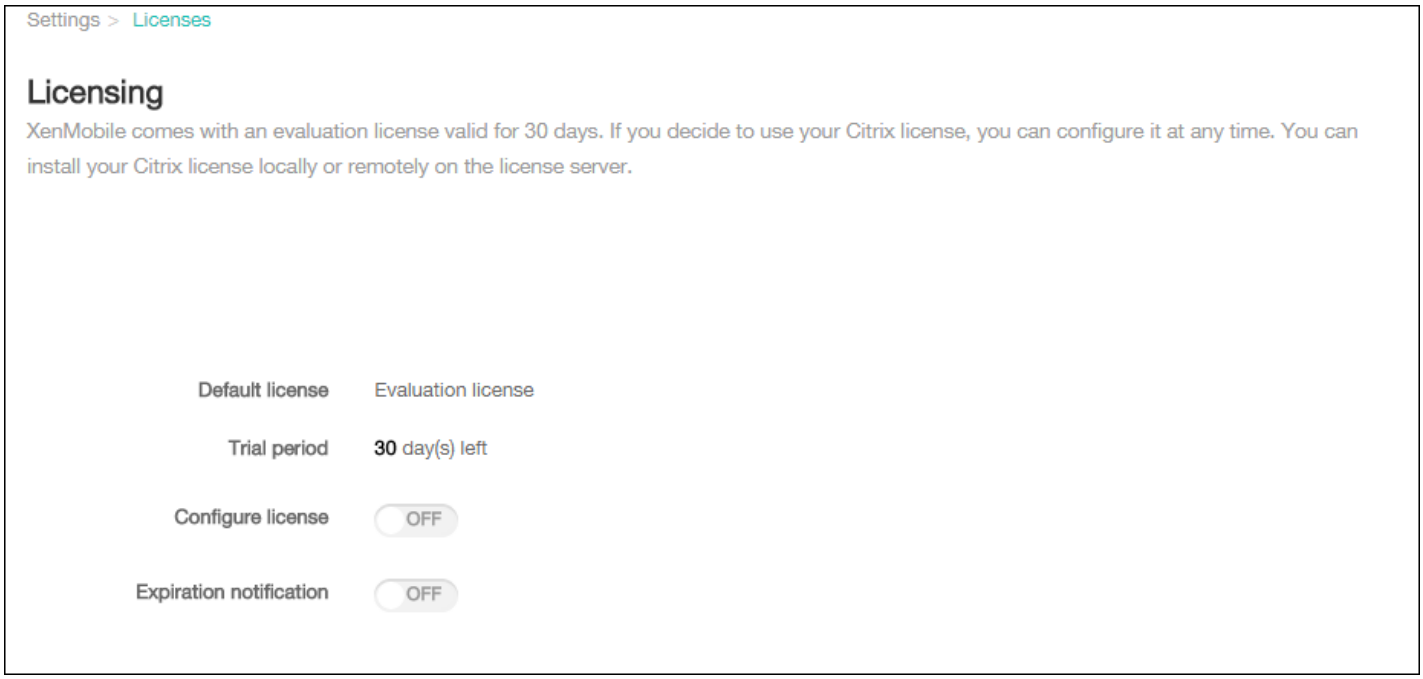


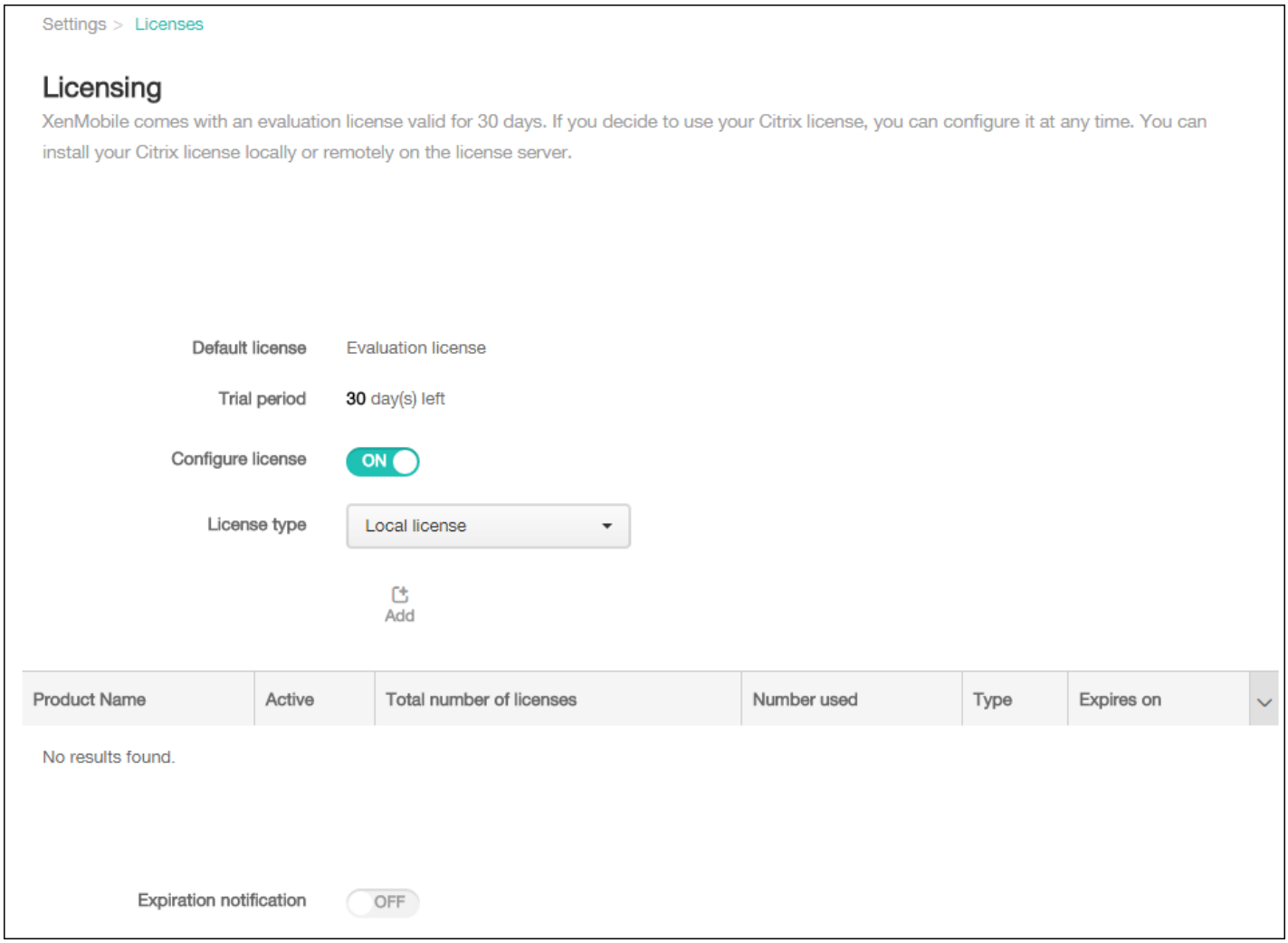


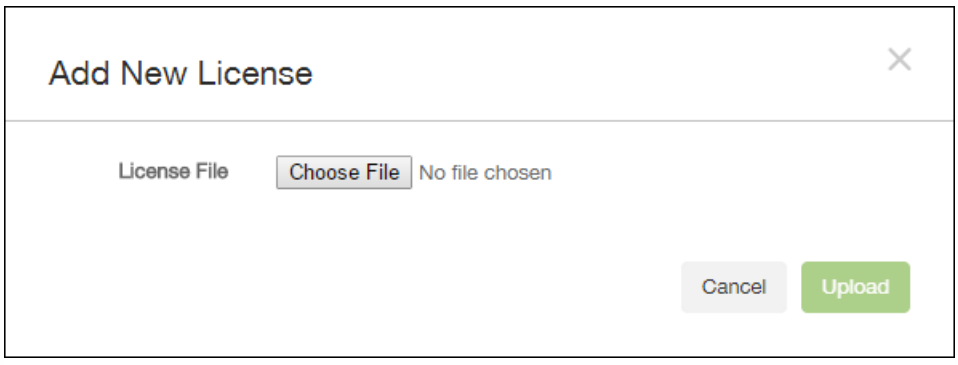


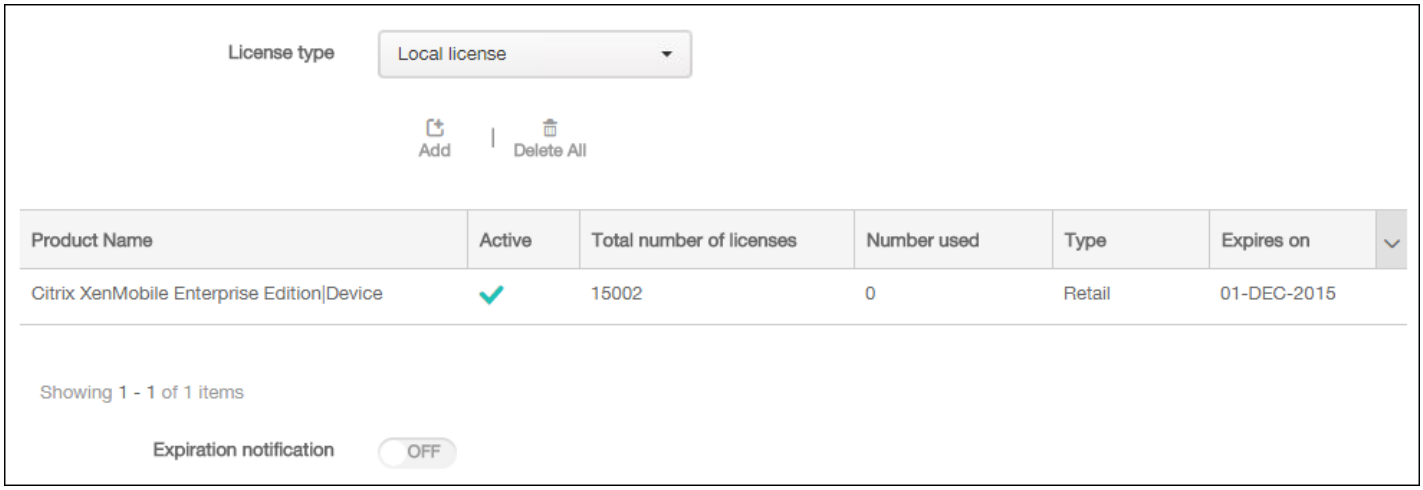


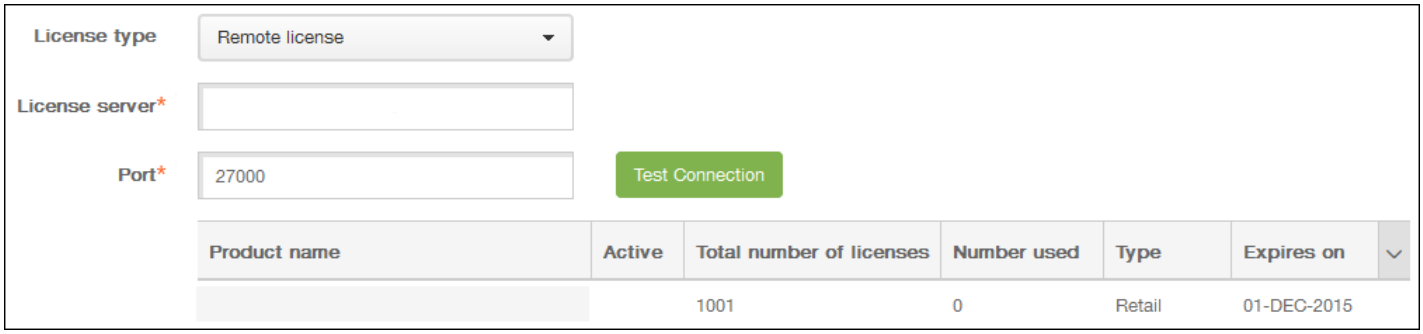






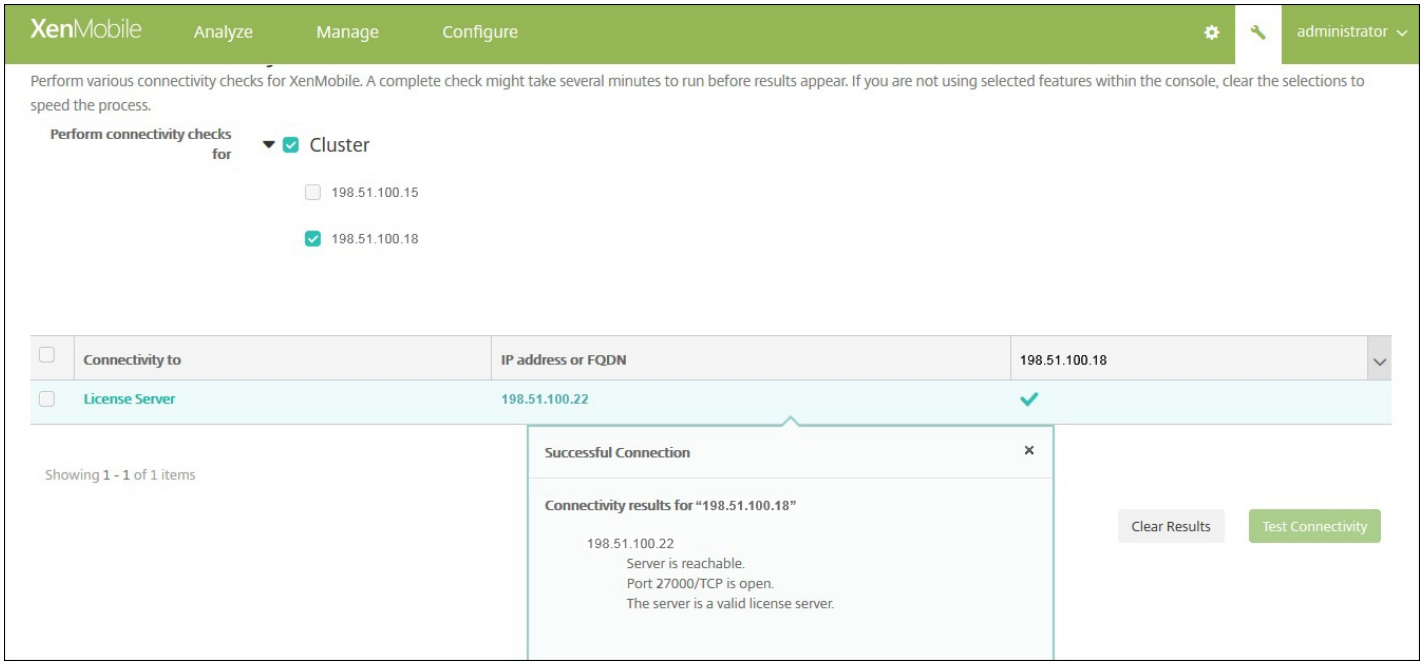


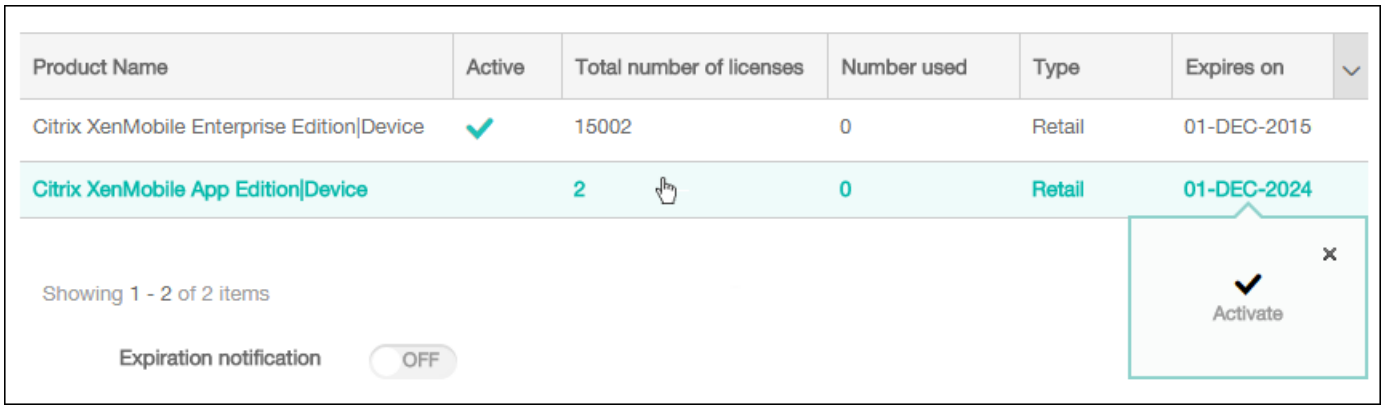


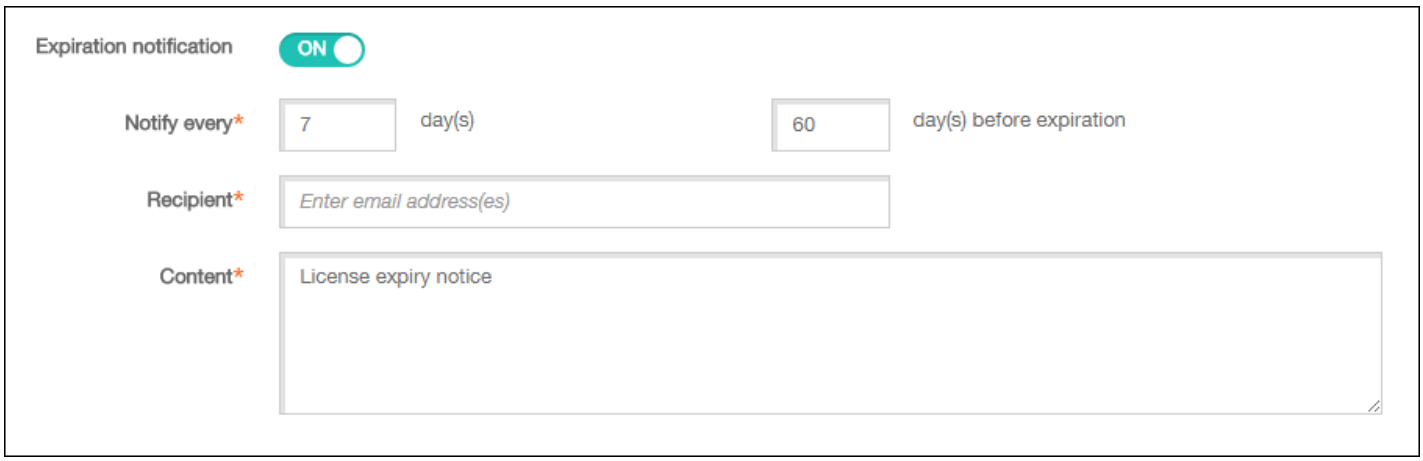


-
-

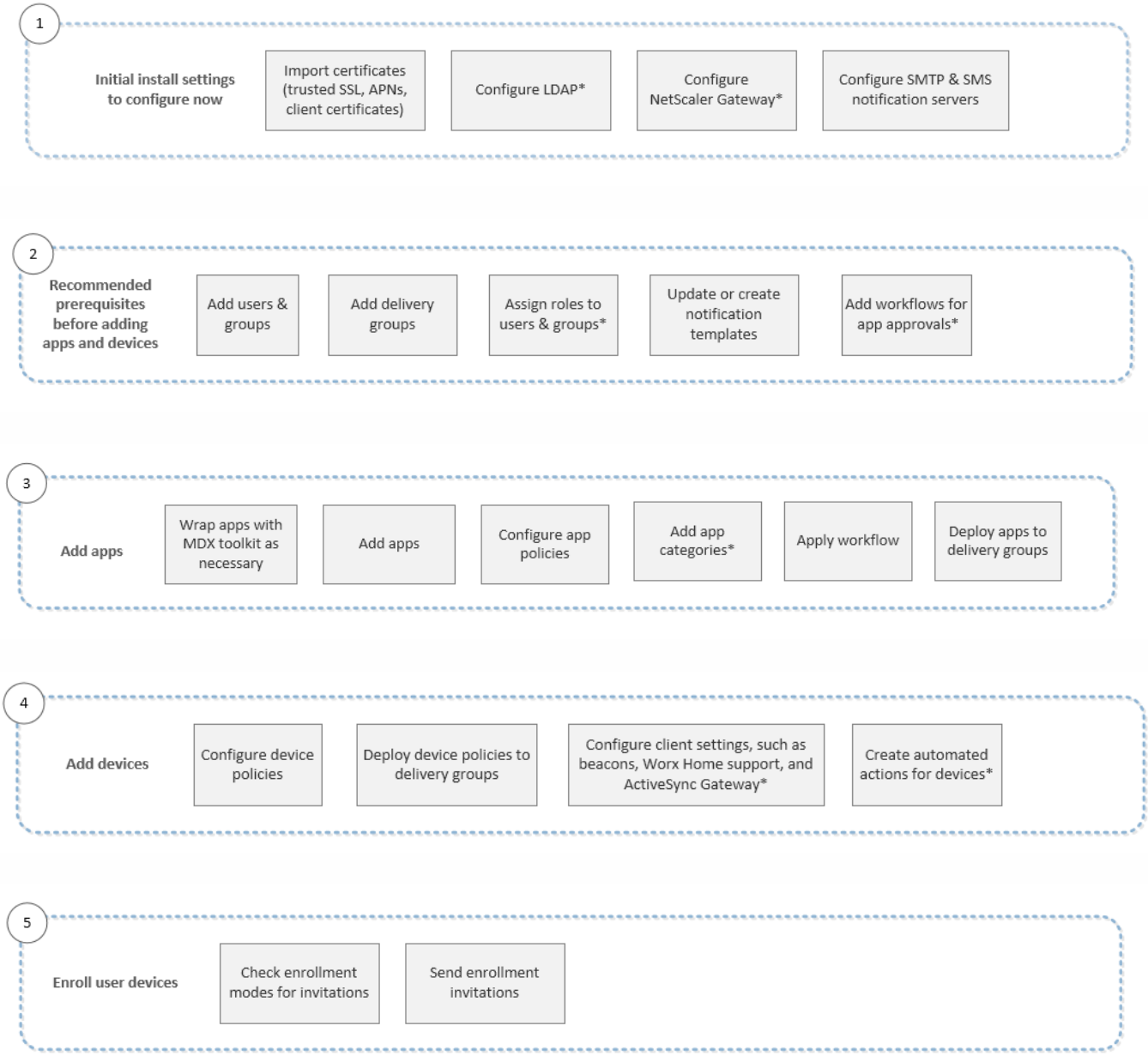
-
-
-

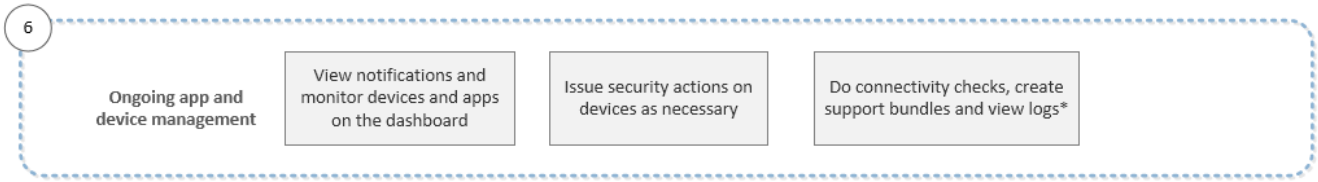


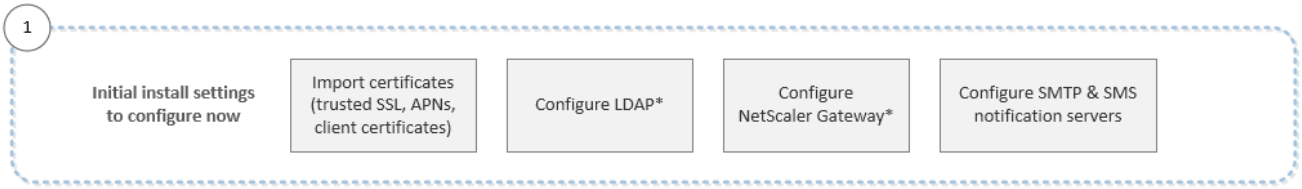




-
  -
  -
-
-

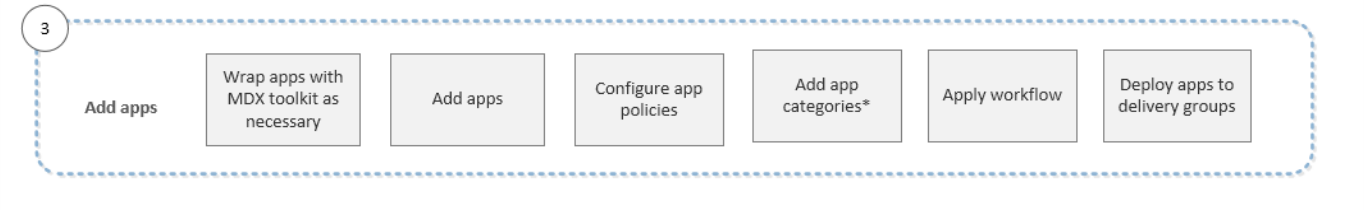




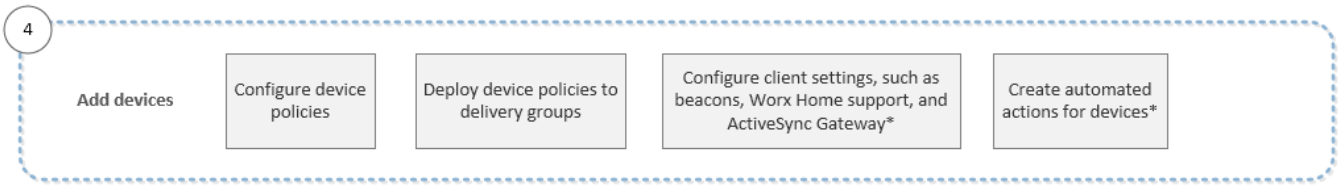


-
-
-
-

-
-
-
-
-
-

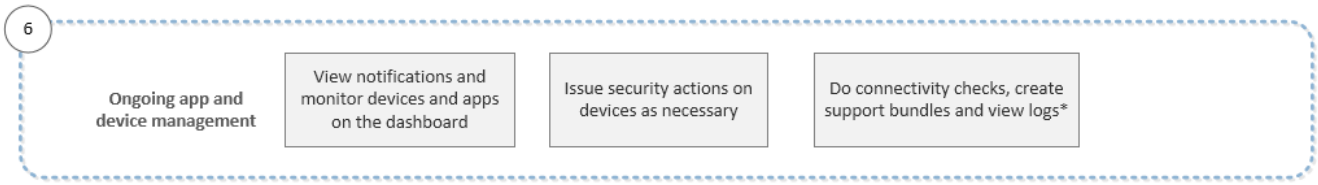


-
-
-
-
-
-



-
-
-
-
-

-
-

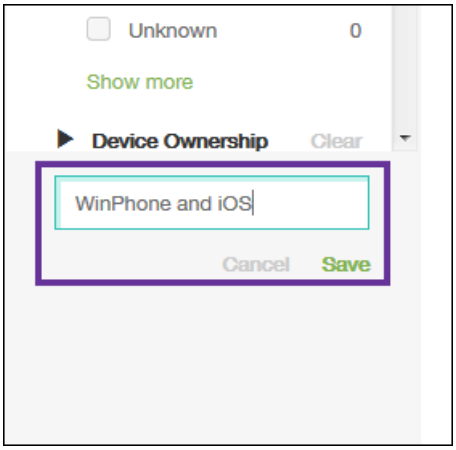


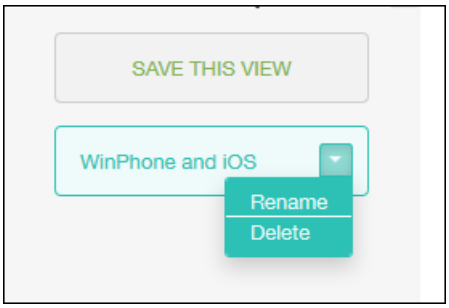
-
-

-

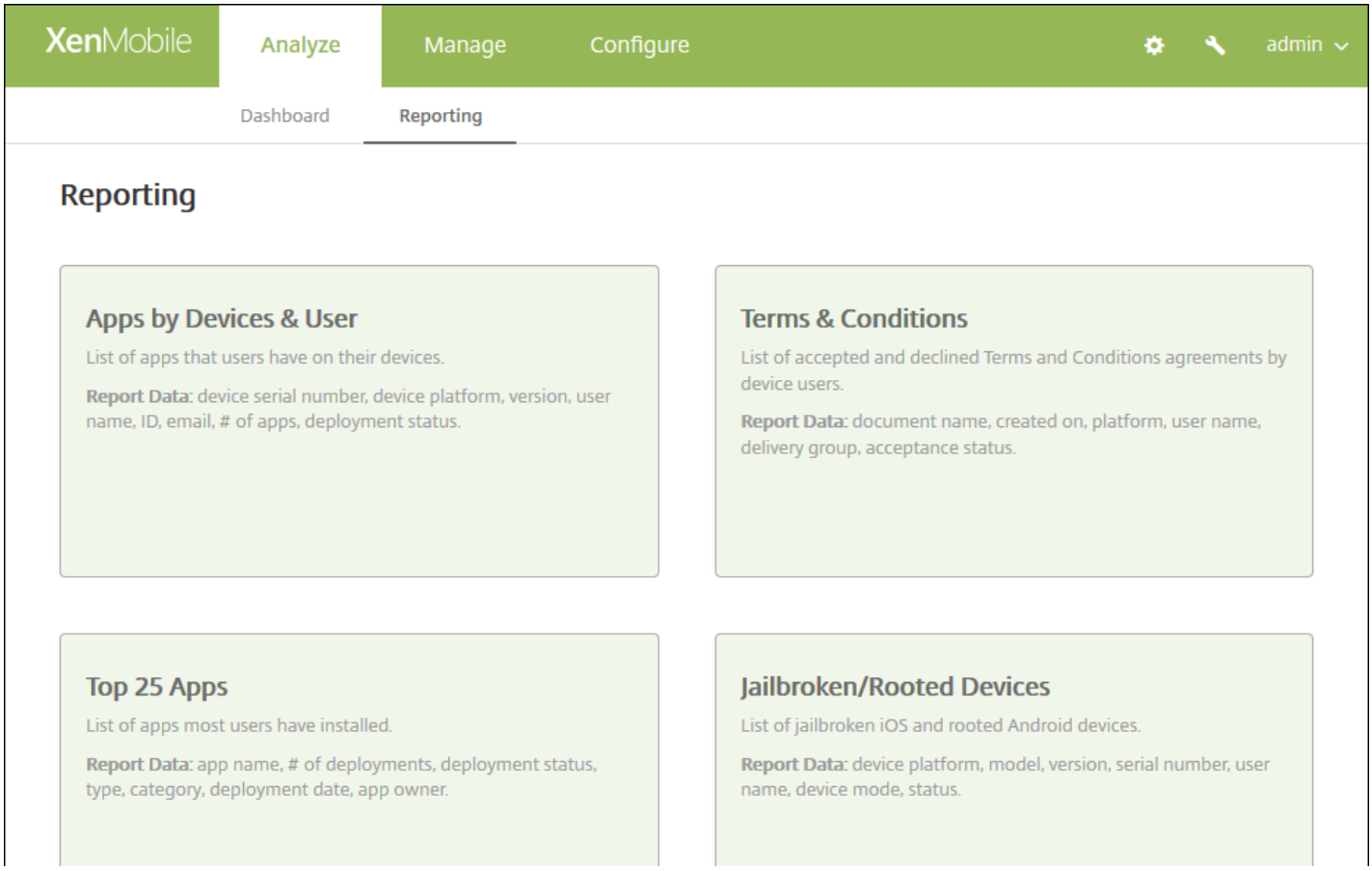
-

-
-
-





-
-
-
-
-
-
-
-
-



Top 10 Apps - Failed Deployment

List of apps that have failed deployment.

Report Data: app name, # of deployments, deployment status, type, category, deployment date, app owner.

Inactive Devices

List of devices that have been inactive for a specified length of time.

Report Data: last activity, device mode, platform, version, user name, last authentication, device IMEI, serial number, model, first connection.

Apps by Type & Category

List of apps and app versions by app type (MDX, Public, Web & SaaS, Enterprise, Web Link) and defined categories.

Report Data: app name, version, # of deployments, deployment status, type, category, deployment date, app owner.

Device Enrollment

List of devices that have been enrolled during a specified length of time.

Report Data: first connection, device mode, platform, version, model, user name, last authentication, phone number.

Apps by Platform

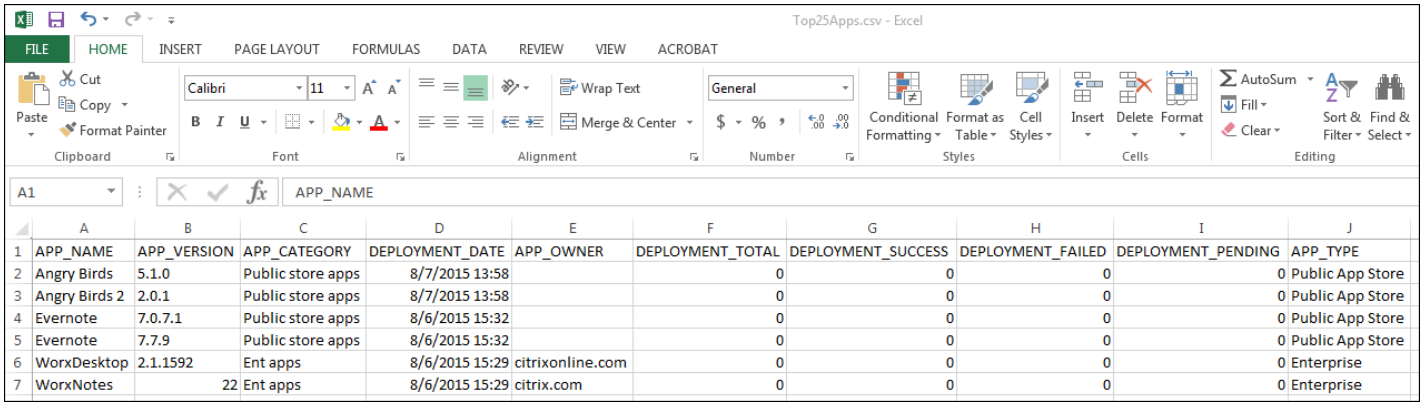
List of apps and app versions installed on various device platforms and device versions.

Report Data: app name, version, # of deployments, deployment status, deployment date, app owner, device platform, version, model, model name.

Devices & Apps

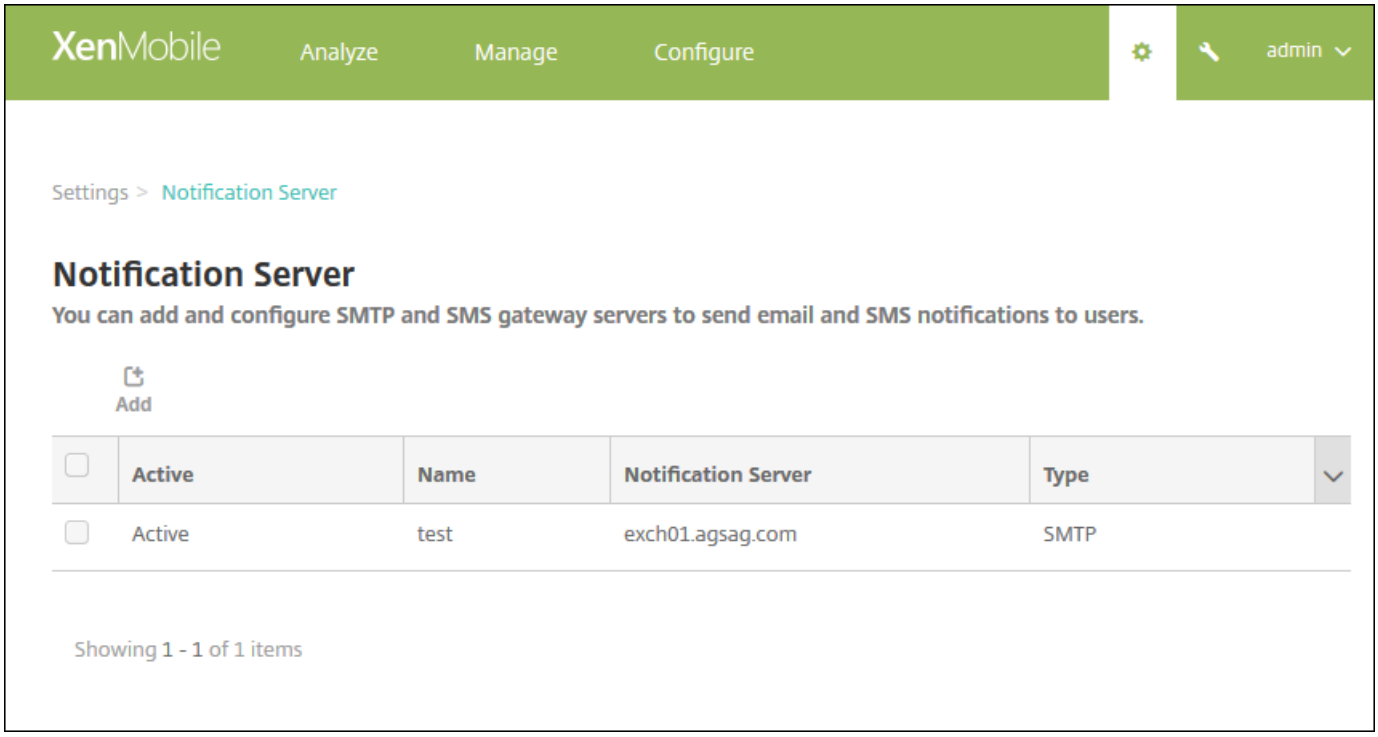
List of all devices, device data, and apps installed.

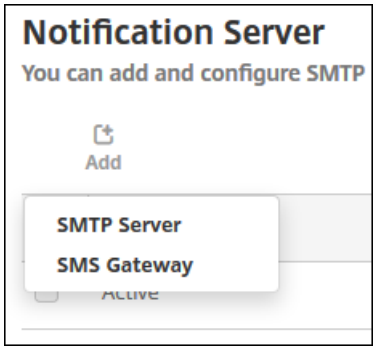
Report Data: device serial number, user name, ID, email, device platform, version, model, mode, status, last connection, enrollment status, enrollment date, device ownership, location, certificate expiration, app name, version, deployment status, type, category, deployment date, app owner, app ID.



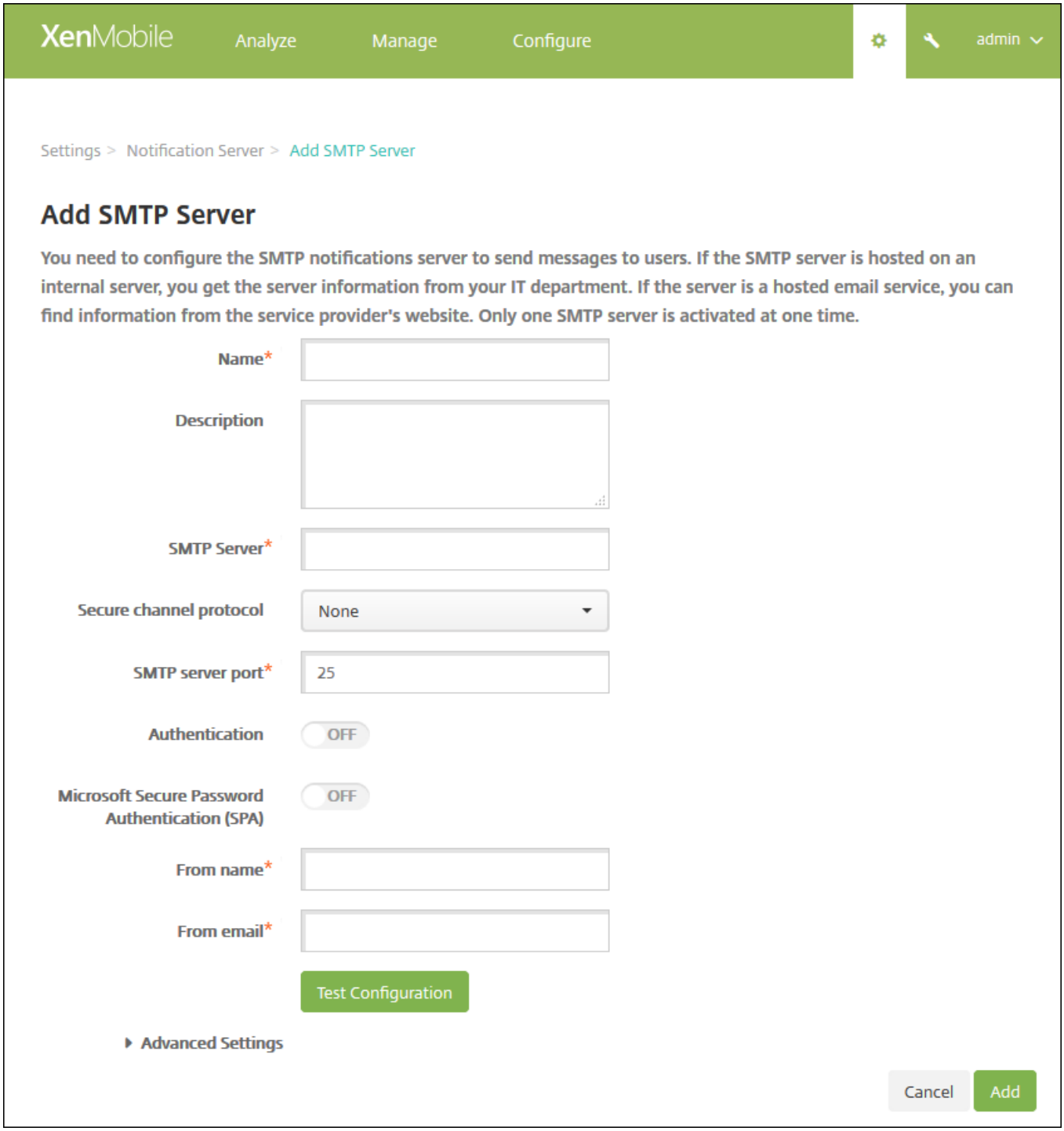
	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORY	DEPLOYMENT_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	Angry Birds	5.1.0	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
3	Angry Birds 2	2.0.1	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
4	Evernote	7.0.7.1	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
5	Evernote	7.7.9	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
6	WorxDesktop	2.1.1592	Ent apps	8/6/2015 15:29	citrixonline.com	0	0	0	0	Enterprise
7	WorxNotes	22	Ent apps	8/6/2015 15:29	citrix.com	0	0	0	0	Enterprise

-
-
-
-
-
-
-
-
-

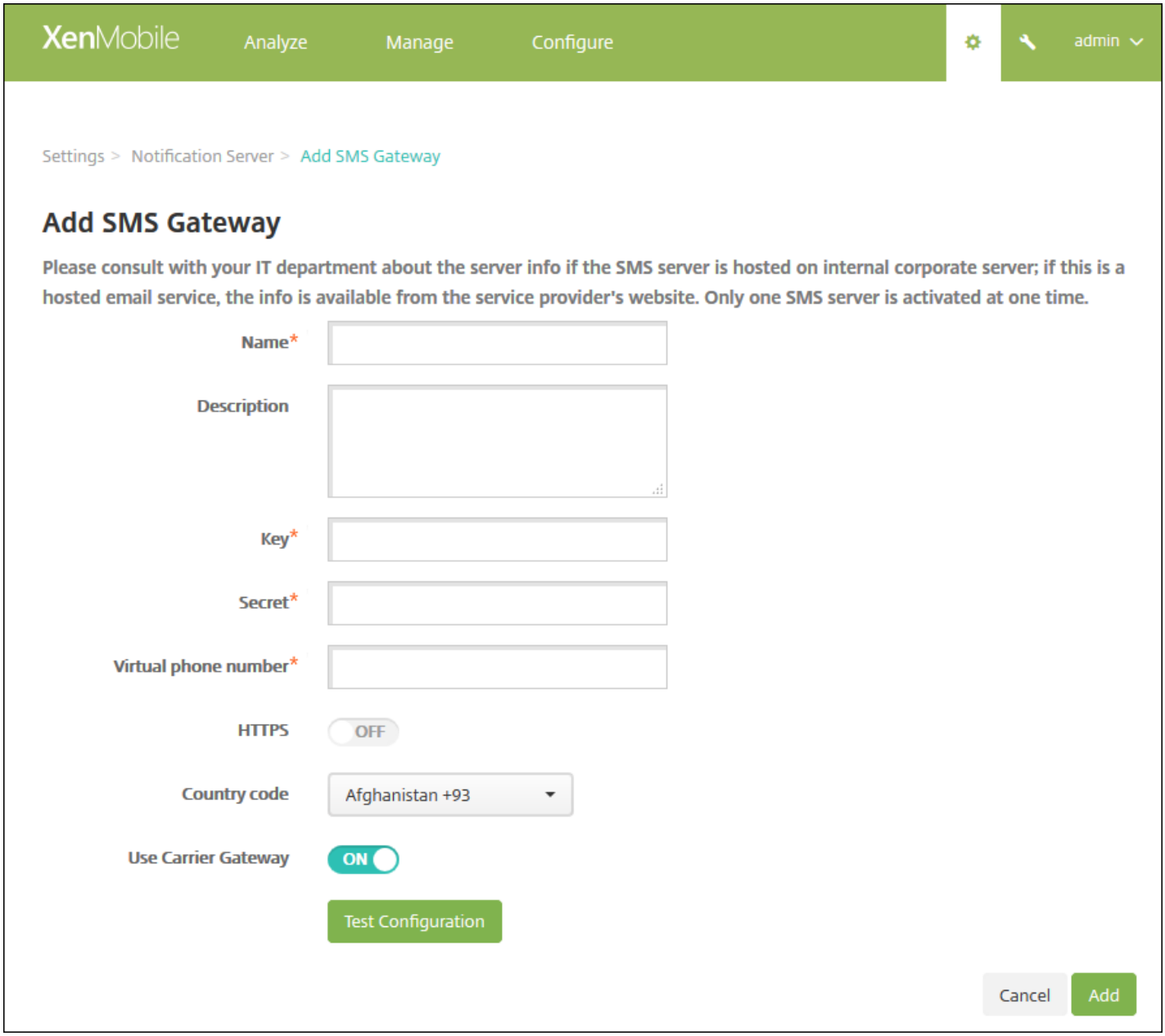




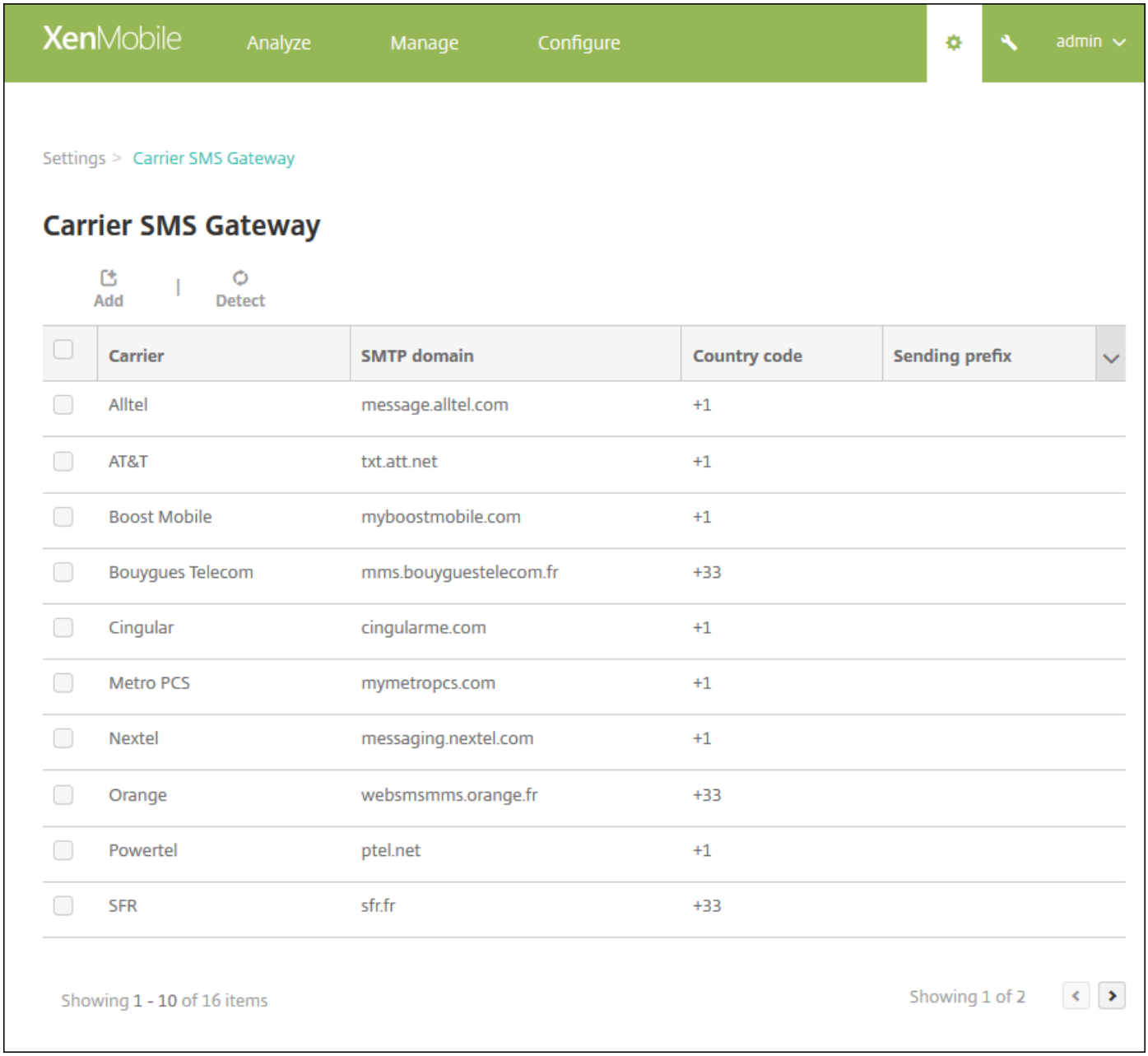
-
-



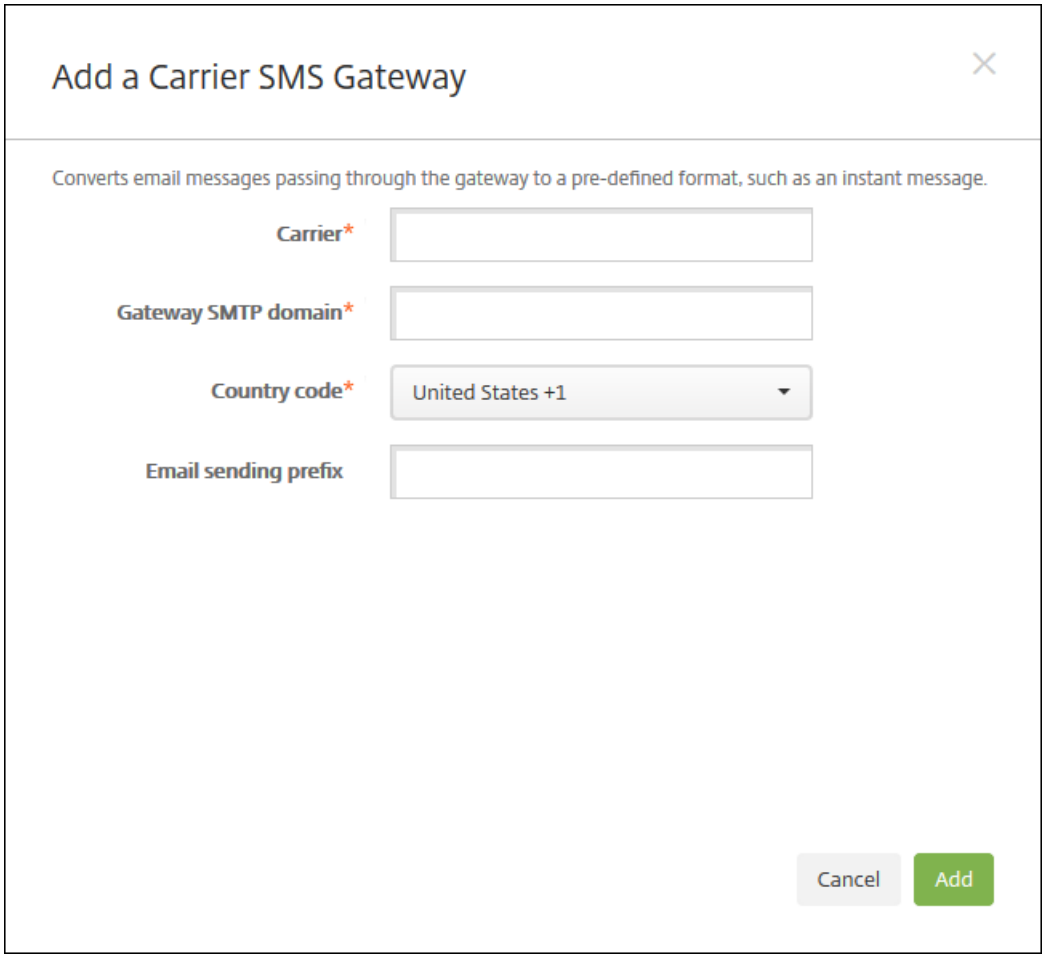
-
-
-
-
-



-
-
-



-
-



-
-
-
-

NetScaler Gateway and XenMobile

Jan 04, 2017

When you configure NetScaler Gateway using XenMobile, you establish the authentication mechanism for remote device access to the internal network. This functionality enables apps on a mobile device to access corporate servers located in the intranet by creating a micro VPN from the apps on the device to NetScaler Gateway. You configure NetScaler Gateway in the XenMobile console.

For NetScaler Gateway versions supported for XenMobile, see XenMobile Compatibilty. For information about setting up NetScaler Gateway for XenMobile on NetScaler, see Configuring Settings for Your XenMobile Environment.

> **Note**
>
> Starting with version 10.4, Worx Mobile Apps are renamed XenMobile Apps. Most of the individual apps are renamed as well. For details, see About XenMobile Apps.

Authentication

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 Worx 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.
- **Worx Home**: Worx Home works with XenMobile server in enrollment operations. Worx Home is the entity on a device that talks to NetScaler: If a session expires, Worx Home 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 Worx Home article.

  Worx Home also facilitates the MDX security container: Worx Home pushes policies, creates a new session with NetScaler when an app times out, and defines the MDX timeout and authentication experience. Worx Home 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 authentication, including single-factor and two-factor authentication methods, the policies, settings, and client properties involved in authentication, and examples of three XenMobile configurations that range from lowest to highest security, see Authentication.

For configuration details, see the following articles:

Configuring Domain and Security Token Authentication

Configuring Client Certificate Authentication

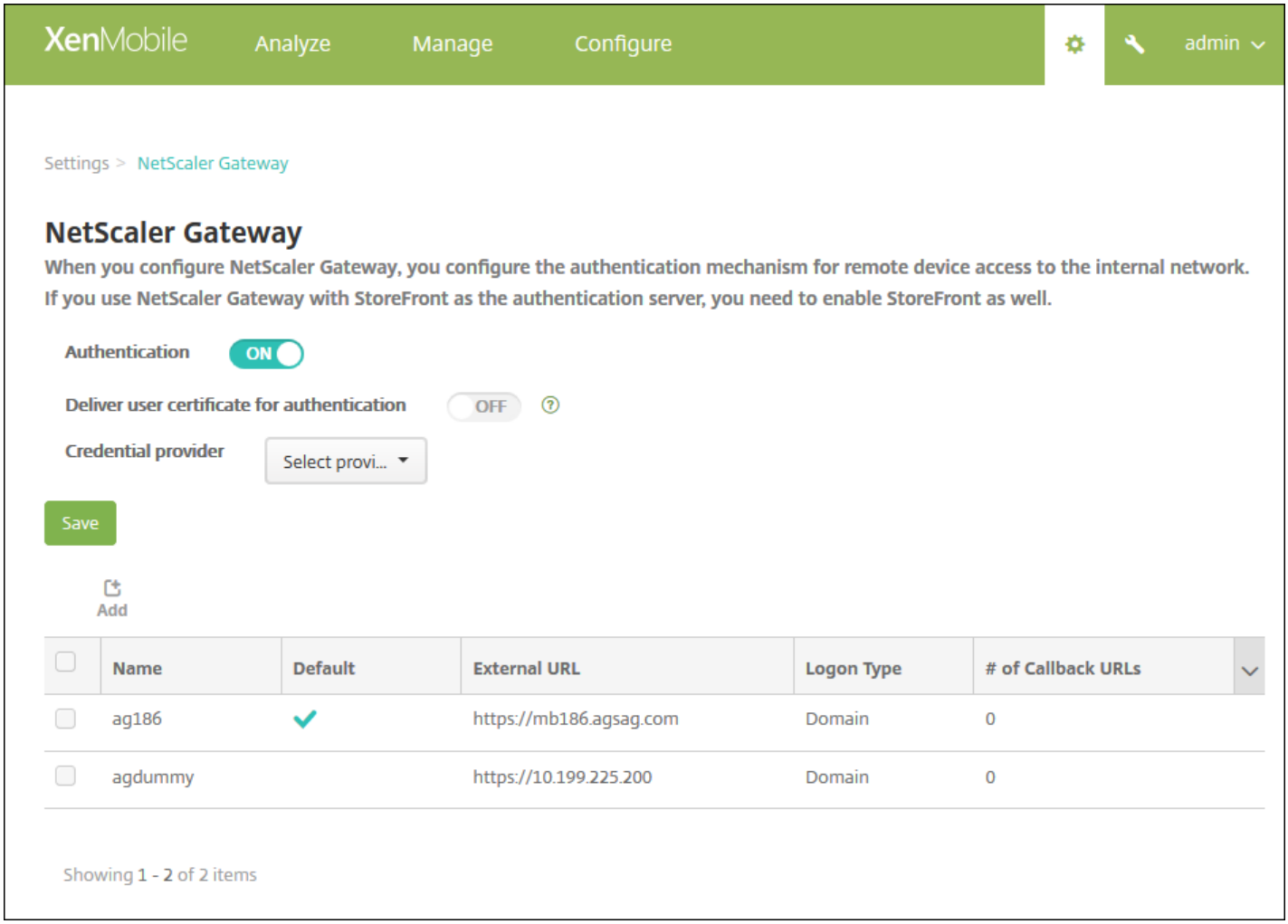
Configuring XenMobile for Certificate and Security Token Authentication

Configuring XenMobile and the ShareFile App for Single Sign-On Using SAML

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 Worx Home 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.

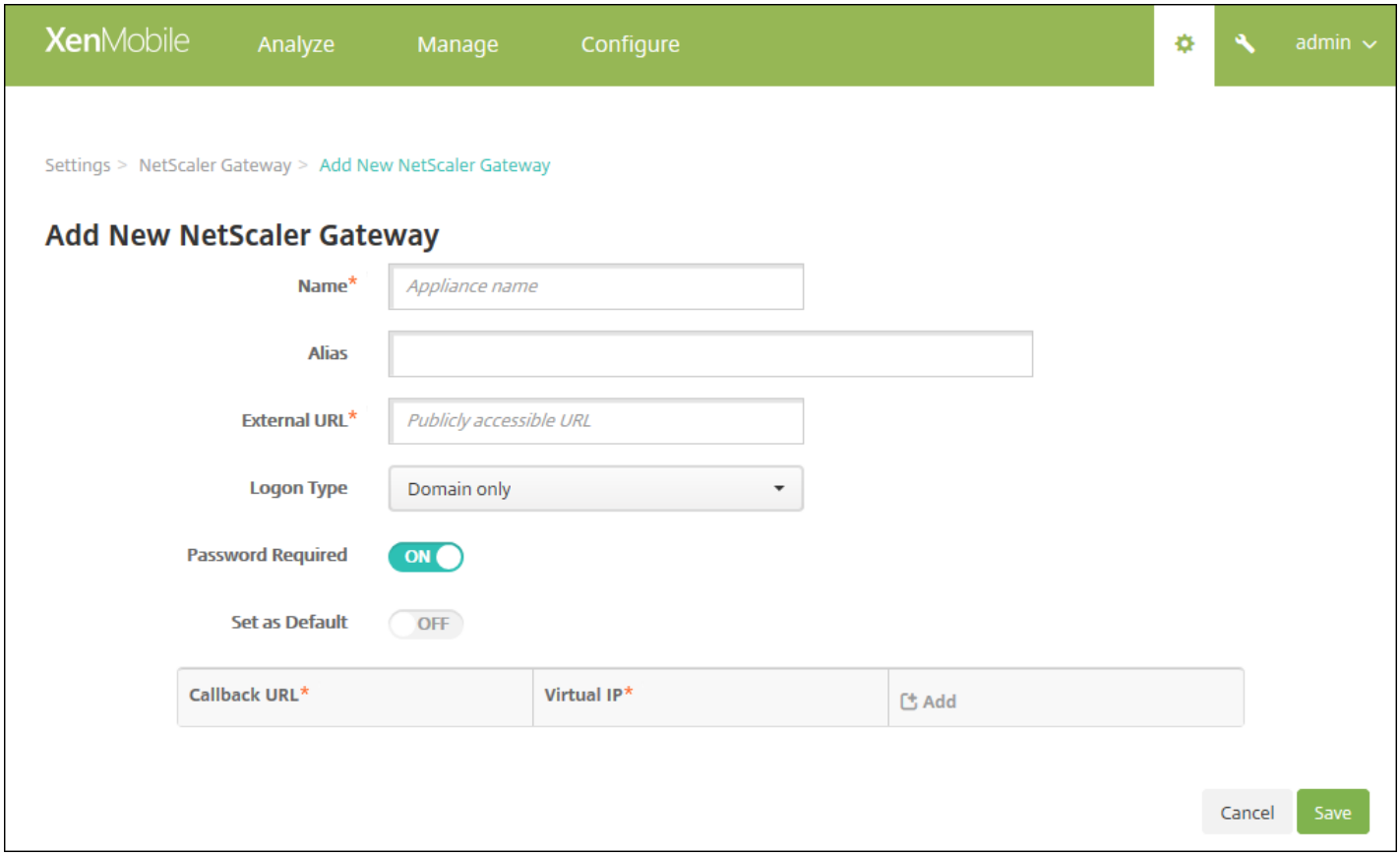
3. Click **Save**.

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: Typer 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 Worx Home. 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 a 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**.

LDAP Configuration

Dec 14, 2016

You can configure a connection in XenMobile to one or more directories, such as Active Directory, that are compliant with the Lightweight Directory Access Protocol (LDAP). You 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.

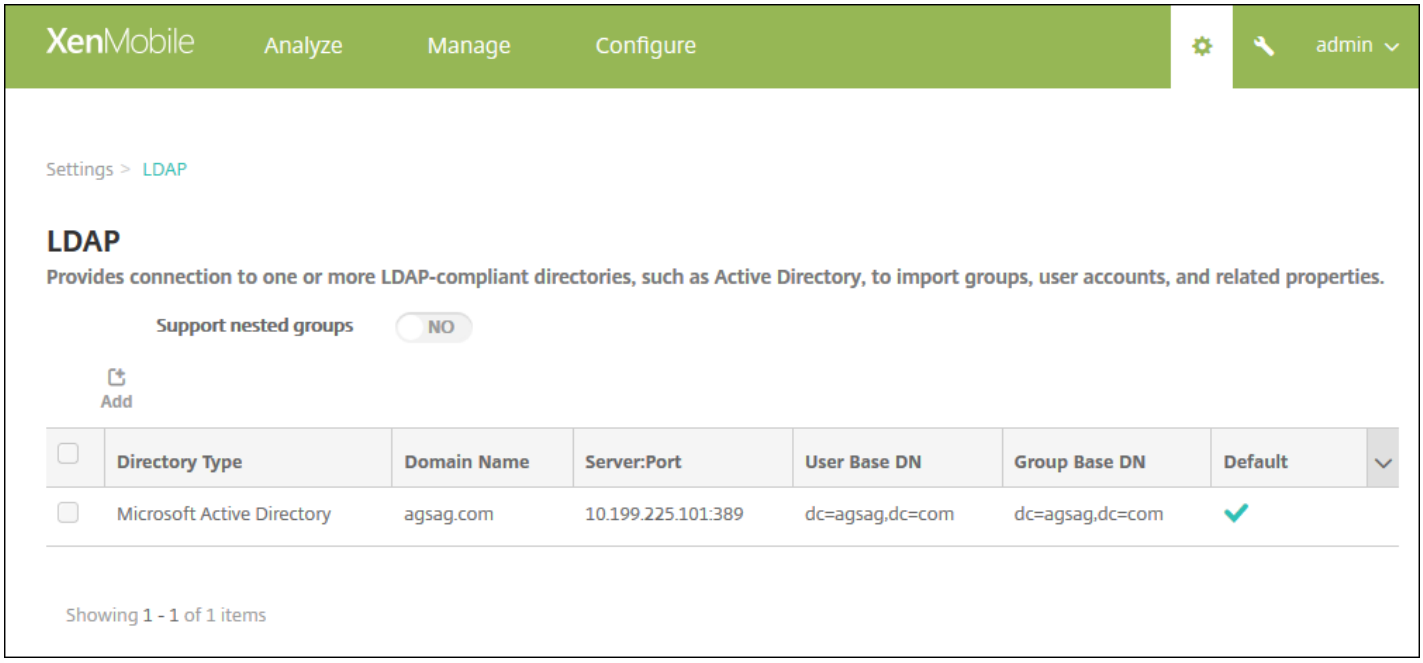
How LDAP works

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

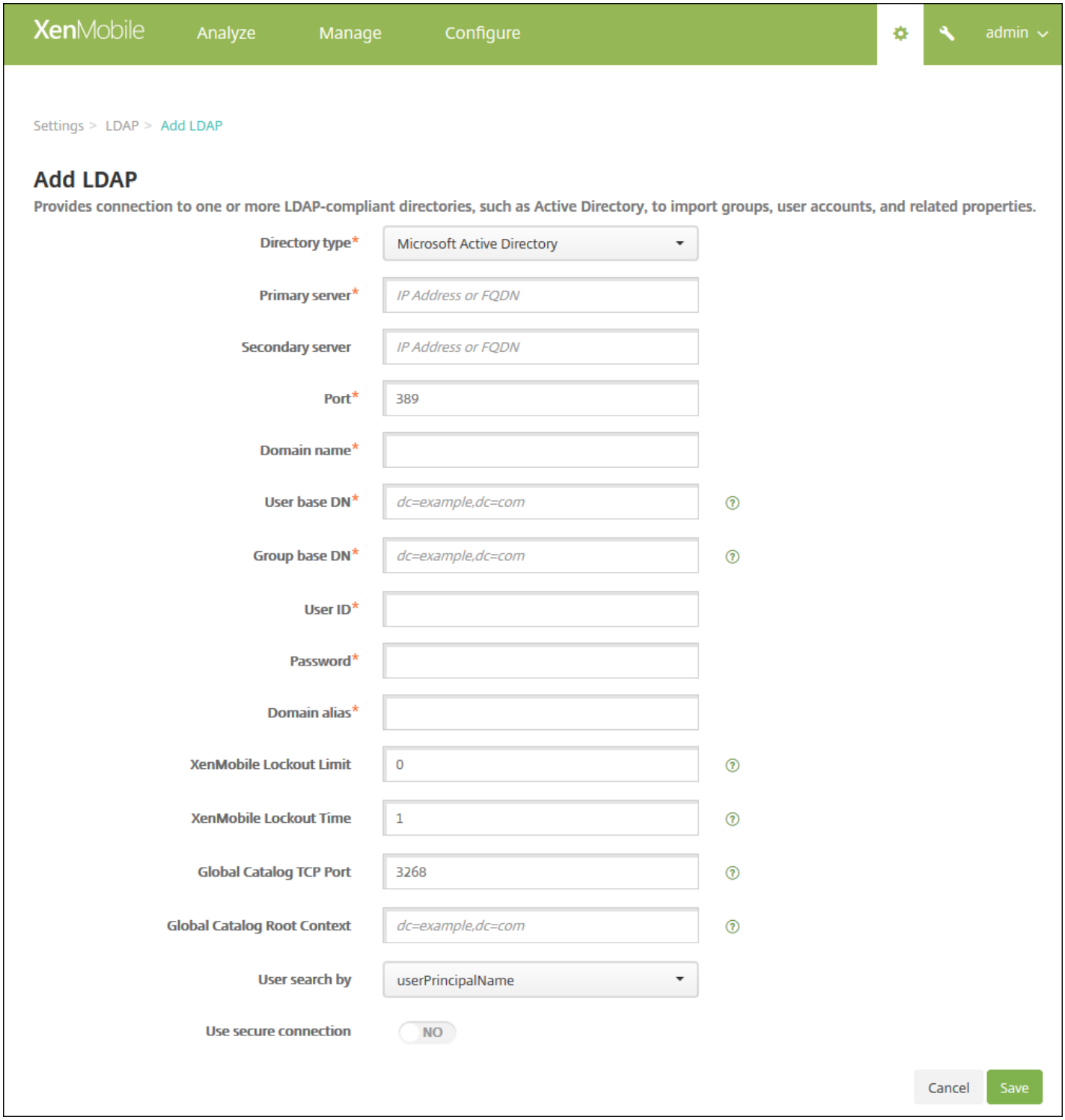
1. In the XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.

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

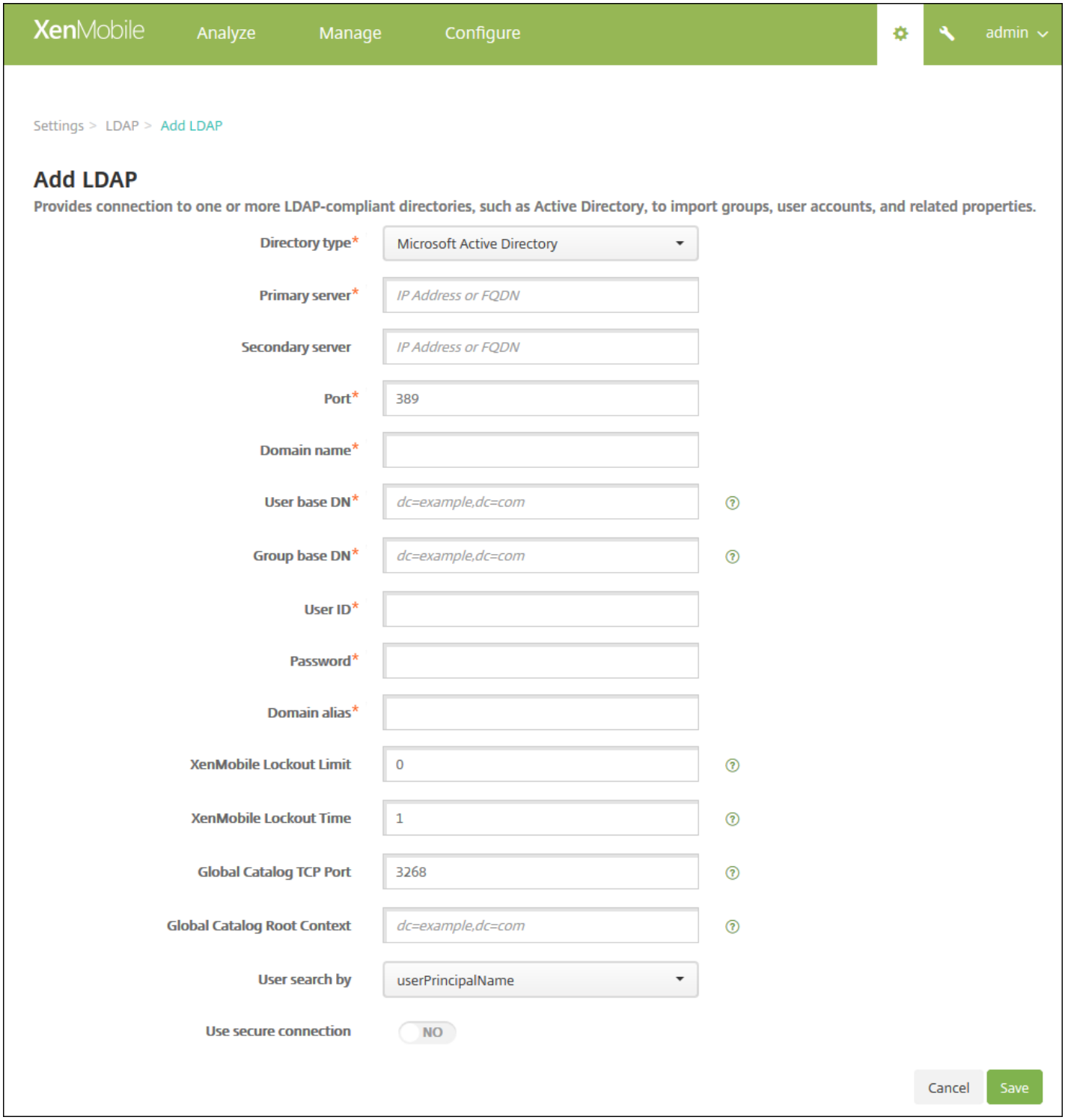
3. Click **Save**.

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 **Add 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.

Configuring Domain and Security Token Authentication

Jan 05, 2017

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 Worx 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.

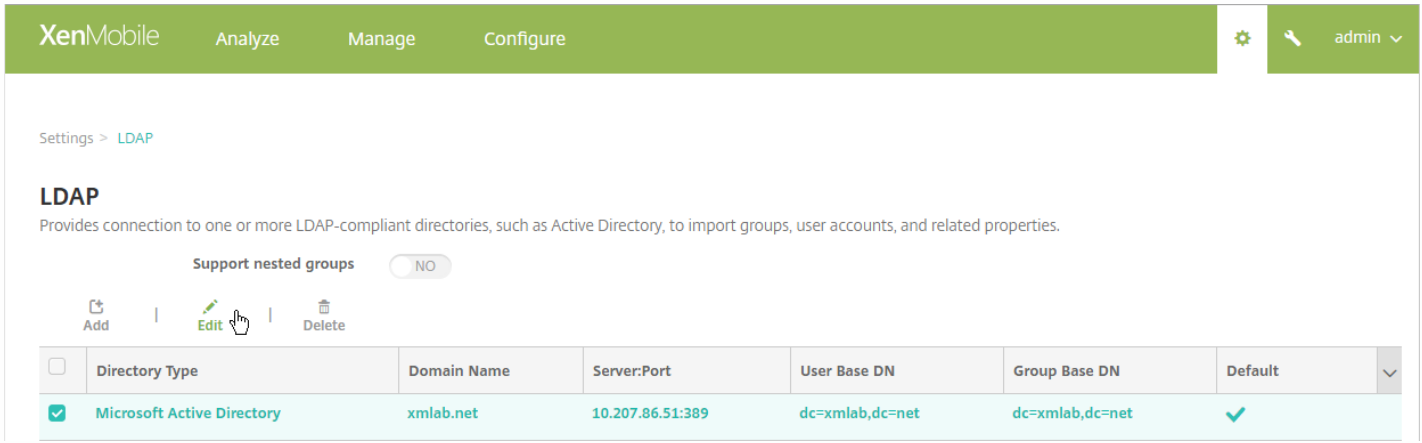
> **Note**
>
> Starting with version 10.4, Worx PIN is renamed Citrix PIN. For more details, see About XenMobile Apps.

Configuring 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.

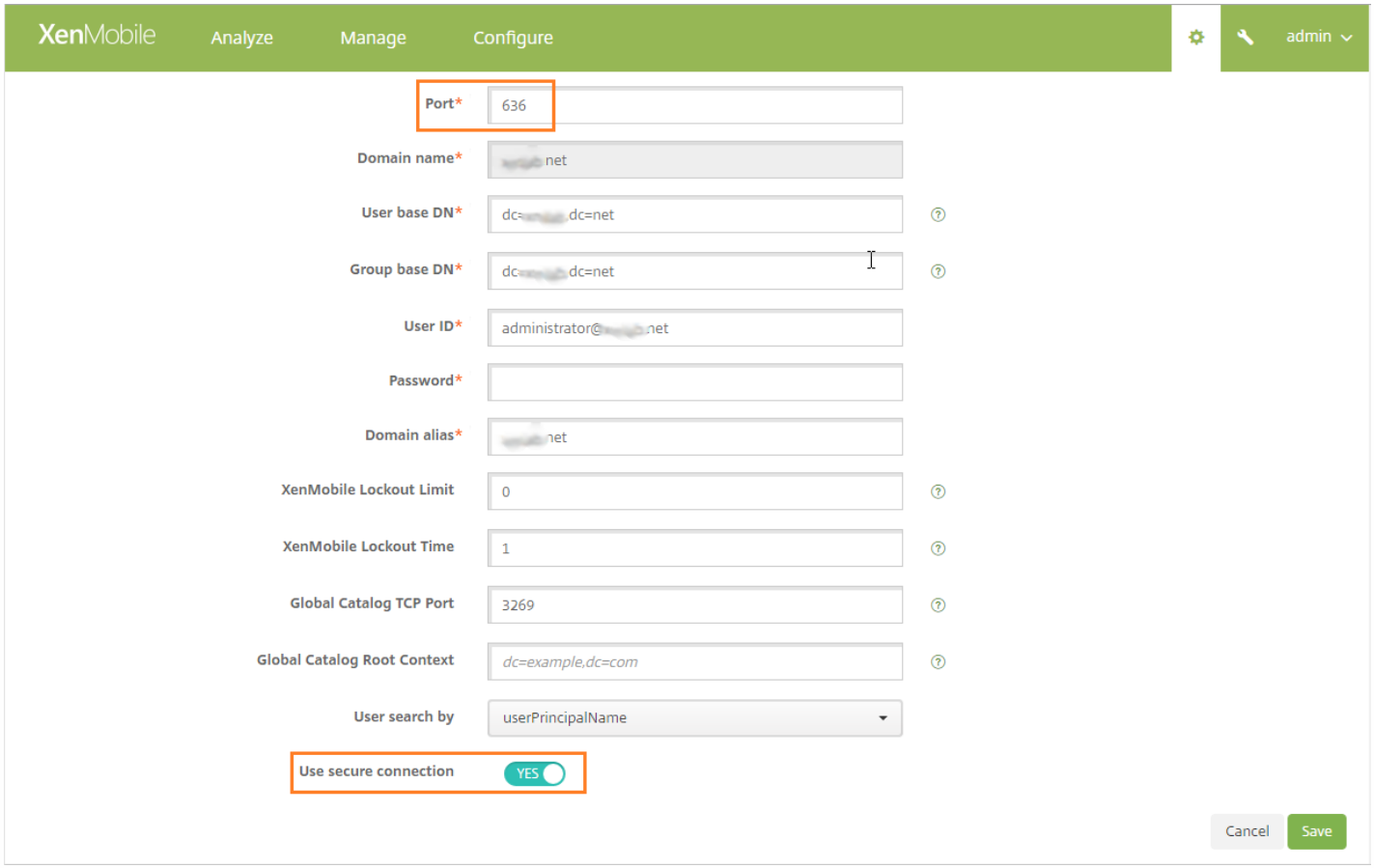
1. In **Settings**, click **LDAP**.

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.**



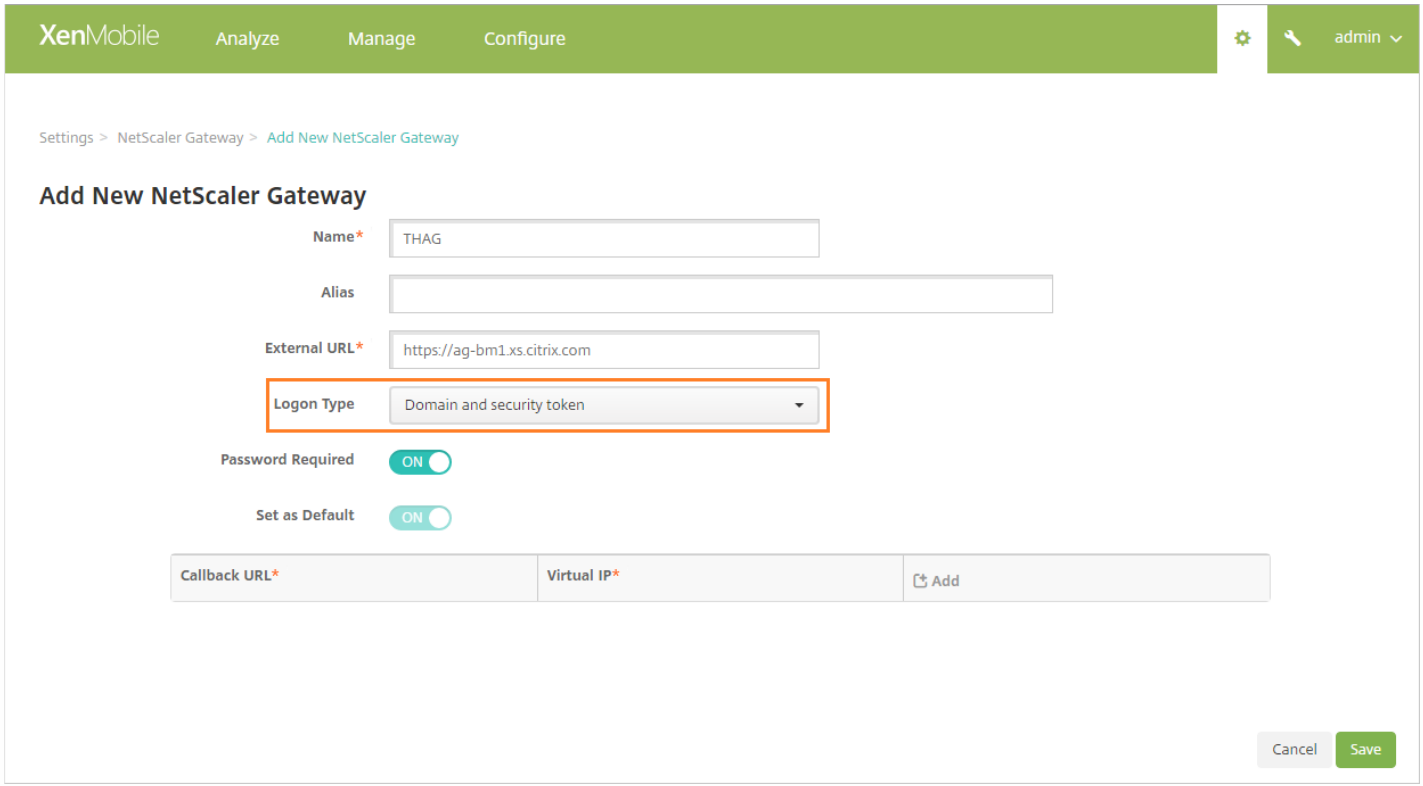
Configuring NetScaler Gateway Settings

The following steps assume that you already have added a NetScaler Gateway instance to XenMobile. To add a NetScaler Gateway instance, see NetScaler Gateway and XenMobile.

1. In **Settings**, click **NetScaler Gateway**.

2. Select the NetScaler Gateway and then click **Edit**.

3. From **Logon Type**, select **Domain and security token**.



Enabling Worx PIN and Active Directory Password Caching

To enable Worx PIN and Active Directory 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 property reference.

Configuring 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.

Certificates

Feb 27, 2017

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

Use certificates to create secure connections and authenticate users in XenMobile.

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 Worx Pin for Single Sign on access to Worx-enabled Apps. Worx PIN also simplifies the user authentication experience. Worx 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 Requesting an APNs Certificate.

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.

Client Certificates for Authentication

In the XenMobile environment, a combination of client certificate plus LDAP authentication is the best solution for security and user experience, with the best SSO possibilities coupled with security provided by two-factor authentication at NetScaler. Using both client certificate and LDAP provides security with both something users know (their Active Directory passwords) and something they have (client certificates on their devices). WorxMail (and some other Worx apps) can automatically configure and provide a seamless first-time user experience with client certificate authentication, with a properly configured Exchange client access server environment. For optimal usability, you can combine this option with Worx PIN and Active Directory password caching.

Client certificate authentication is based on the attributes of the client certificate that is presented to the virtual server. You must bind a root certificate to the virtual server on NetScaler Gateway. When users log on to NetScaler Gateway, the user name information is extracted from the specified field of the certificate. Typically, this field is Subject:CN. If the user name is extracted successfully, the user is then authenticated. If the user does not provide a valid certificate during the Secure Sockets Layer (SSL) handshake or if the user name extraction fails, authentication fails.

Notes:

- Client certificate authentication can also be used with another authentication type, such RADIUS.
- You can authenticate users based on the client certificate by setting the default authentication type to use the client certificate. You can also create a certificate action that defines what is to be done during the authentication based on a client SSL certificate.
- WorxMail (and some other Worx apps) can automatically configure and provide a seamless first-time user experience with client certificate authentication, with a properly configured Exchange client access server environment. For optimal usability, you can combine this option with Worx PIN and Active Directory password caching.
- Device authentication with Netscaler Gateway is not supported for certificates obtained through a discretionary CA.
- XenMobile doesn't support client certificate authentication for shared devices.

XenMobile PKI

The XenMobile Public Key Infrastructure (PKI) integration feature allows you to manage the distribution and life cycle of security certificates used on your devices.

XenMobile creates an internal PKI for device authentication during the installation process.

External PKIs can also be used to issue certificates to devices to be used in configuration policies or for client authentication to NetScaler Gateway.

The main feature of the PKI system is the PKI entity. A PKI entity models a back-end component for PKI operations. That component is part of your corporate infrastructure, such as a Microsoft, RSA, Entrust, Symantex, or OpenTrust PKI. The PKI entity handles the back-end certificate issuance and revocation. The PKI entity is the authoritative source for the certificate's status. The XenMobile configuration will normally contain exactly one PKI entity per back-end PKI component.

The second feature of the PKI system is the credential provider. A credential provider is a particular configuration of certificate issuance and life cycle. The credential provider controls things like the certificate format (subject, key, algorithms) and the conditions for its renewal or revocation, if any. The credential providers delegate operations to the PKI entities. In other words, although credential providers control when and with what data PKI operations are undertaken, PKI entities control how those operations are performed. The XenMobile configuration normally contains many credential providers per PKI entity.

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 and Intermediate CA certificates for the preceding certificates and any other internal resources (StoreFront/Proxy, and so on)
APNs certificate for iOS device management
Internal APNs certificate for XenMobile server Worx Home notifications
PKI user certificate for connectivity to PKI

MDX Toolkit
Apple Developer Certificate
Apple Provisioning Profile (per application)
Apple APNs certificate (for use with WorxMail)
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 and 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 WorxMail

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 WorxMail 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 Requesting an APNs Certificate.

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.

Be aware that an existing iOS Developer for Enterprise certificate and provisioning profile might not be compatible with iOS 9. For details, see Wrapping Worx Apps for iOS 9.

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 Worx Store, connecting to Exchange Server when using WorxMail, 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

Uploading Certificates in XenMobile

Oct 26, 2016

Certificates are used functionally by the XenMobile server. You upload the certificates to XenMobile through the **Certificates** area of the XenMobile console. These certificates include Certificate Authority (CA) certificates, Registration Authority (RA) certificates, and certificates for client authentication with other components of your infrastructure. In addition, you may use the Certificates area as a storage location for certificates you want to deploy to devices. This use especially applies to CAs that are used to establish trust on the device.

Each certificate that 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 Configuring Client Certificate 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.

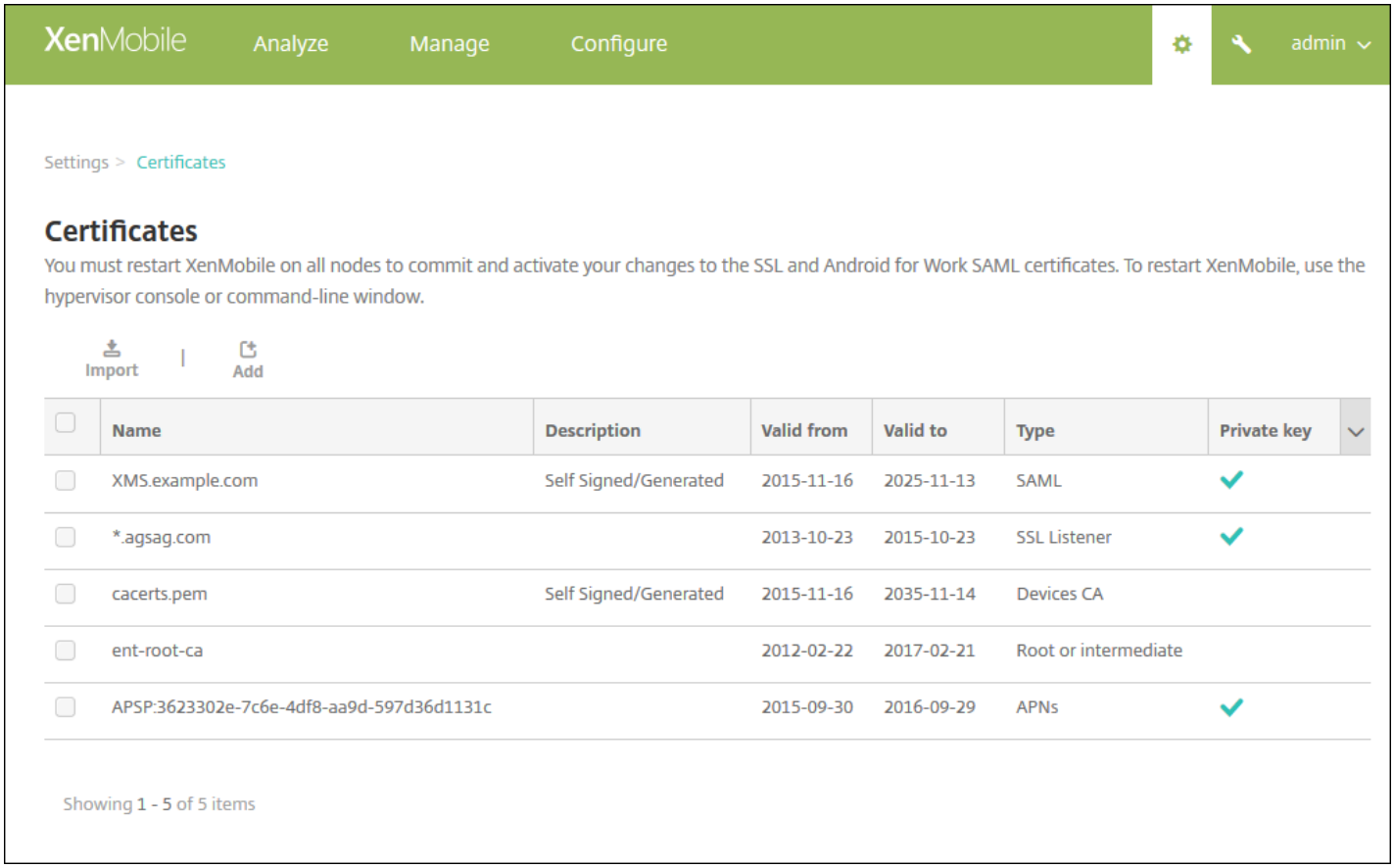
You can upload the CA certificate (without the private key) that the CA uses to sign requests, and you can upload an SSL client certificate (with the private key) for client authentication. When configuring the Microsoft CA entity, you need to specify the CA certificate, which you can then select from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

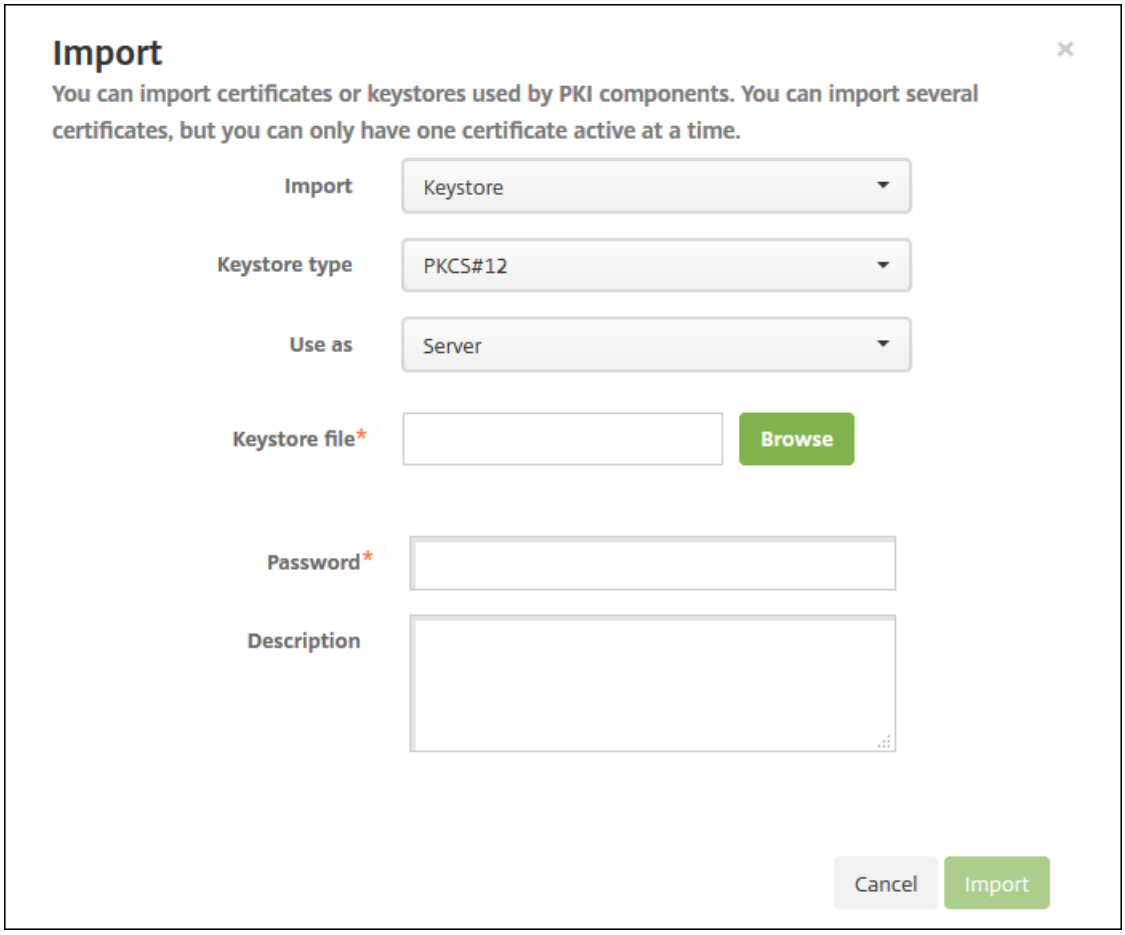
2. Click **Certificates**. The **Certificates** page appears.



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 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 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 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 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.

Configuring Client Certificate Authentication

Jan 05, 2017

To use client certificate authentication for XenMobile ENT and MAM modes, you must configure the Microsoft server, the XenMobile server, and then NetScaler Gateway. The following general steps are detailed 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:

1. Configure NetScaler Gateway for XenMobile MAM mode certificate authentication.

> ### Note
>
> Starting with version 10.4, Worx Mobile Apps are renamed XenMobile Apps. Most of the individual XenMobile Apps are renamed as well. For details, see About XenMobile Apps.

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 WorxMail. 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**.

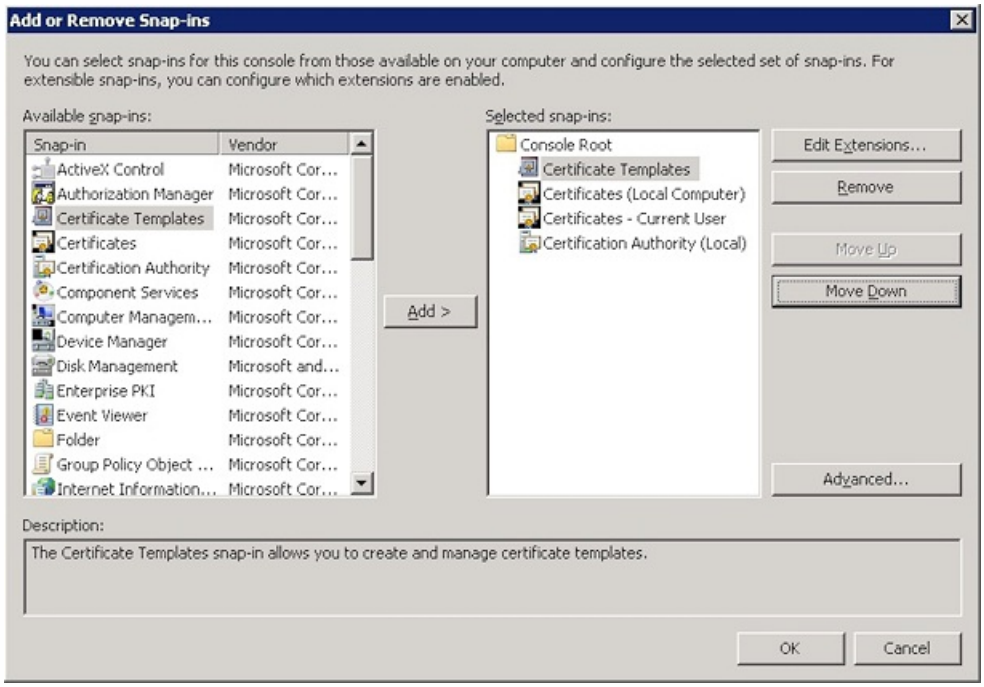
- Make sure that WorxMail for iOS, Android, and Windows Phone is wrapped with the latest MDX Toolkit.

Adding a certificate snap-in to the Microsoft Management Console

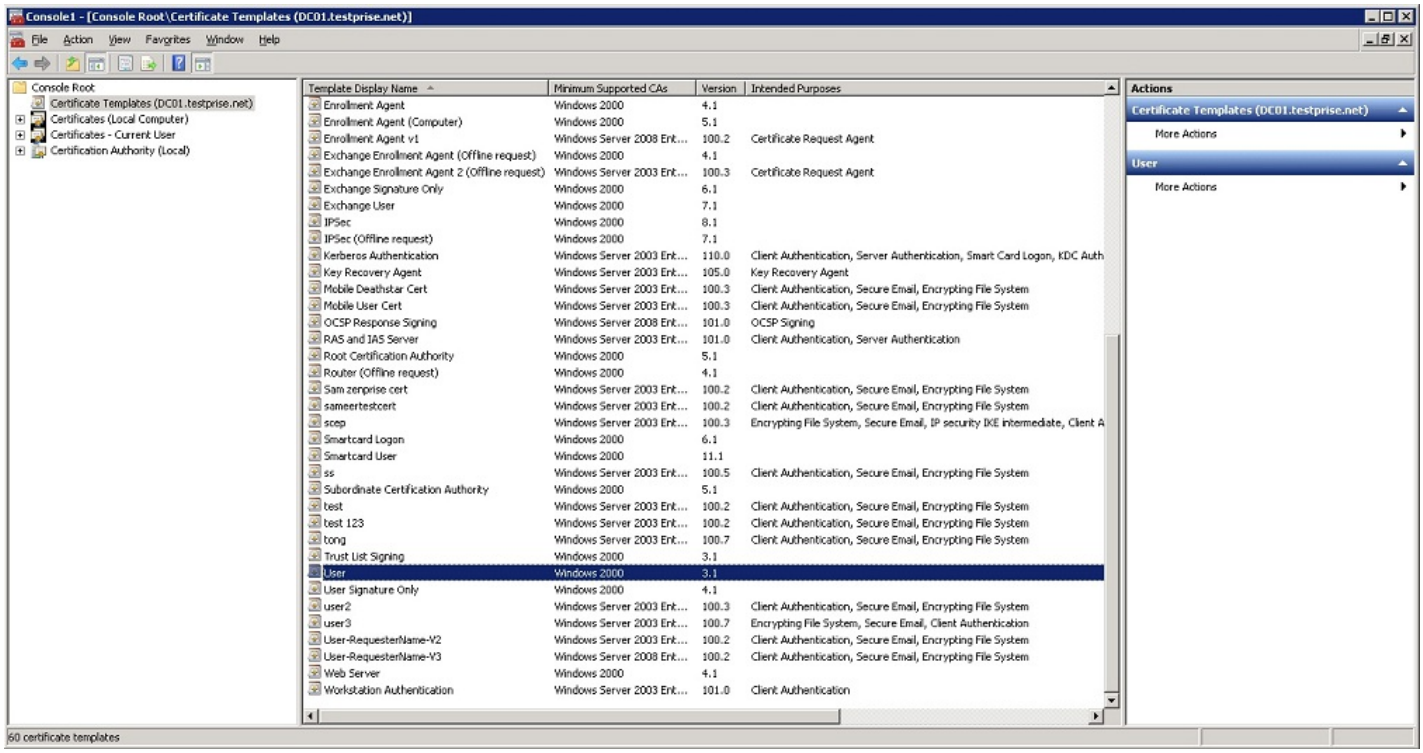
1. Open the console and then click **Add/Remove Snap-Ins**.

2. Add the following snap-ins:

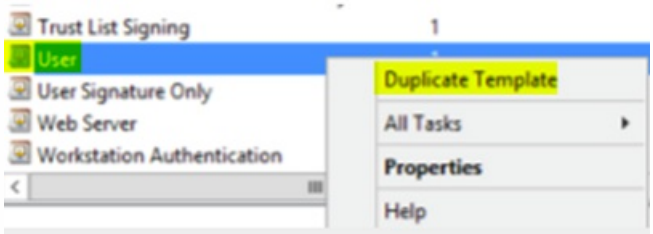
    Certificate Templates
    Certificates (Local Computer)
    Certificates - Current User
    Certificate Authority (Local)



3. Expand **Certificate Templates**.



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

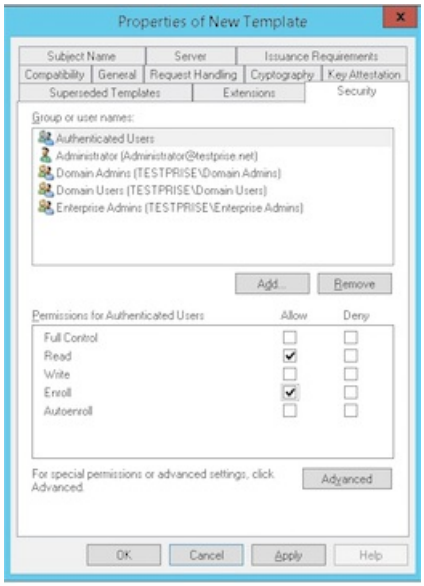


5. Provide the Template display name.

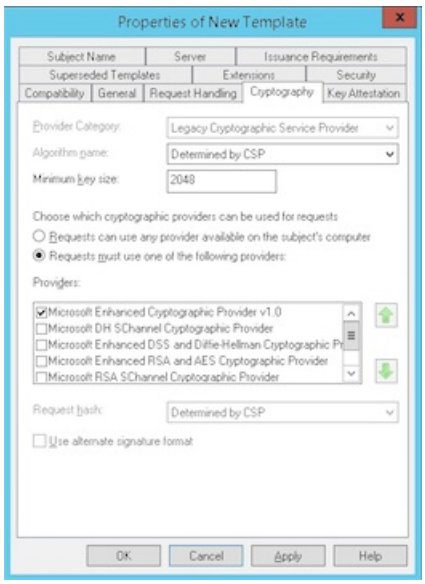
> **Important:** Do not select the **Publish certificate in Active Directory** check box unless required. If this option is selected, all user client certificates will be pushed/created in Active Directory, which might clutter your Active Directory database.

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**.

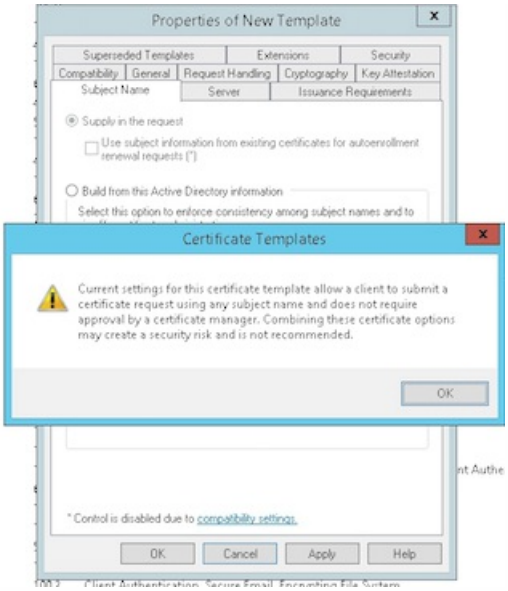
7. Under **Security**, select the **Enroll** option in the **Allow** column for the authenticated users.



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



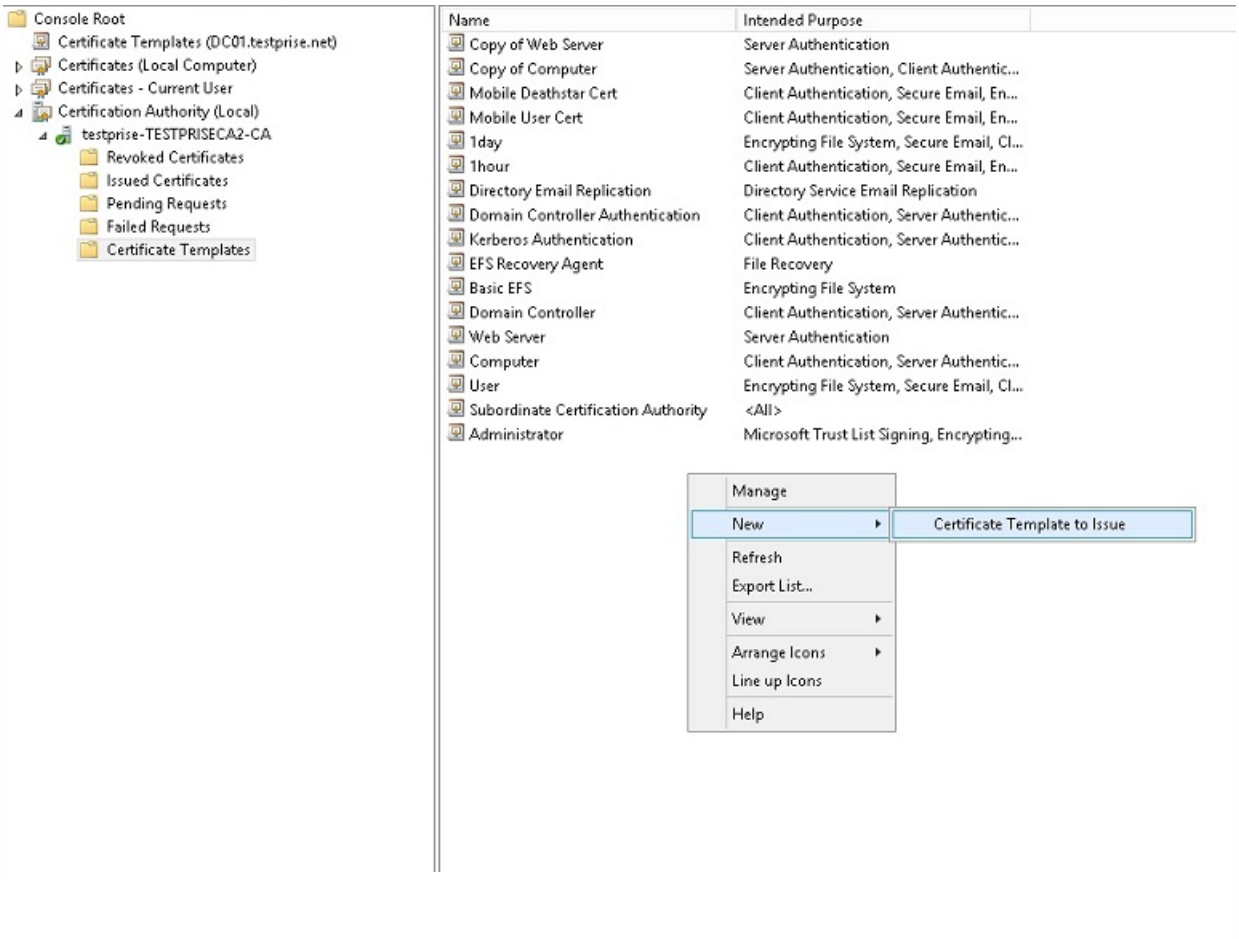
9. Under **Subject Name**, select **Supply in the request**. Apply the changes and then save.



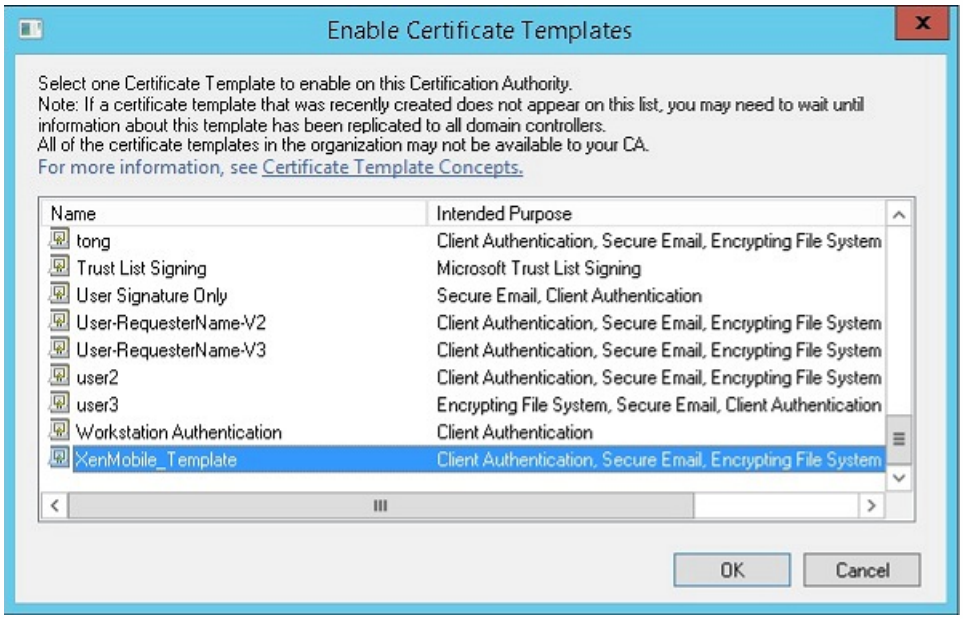
Adding the template to Certificate Authority

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**.

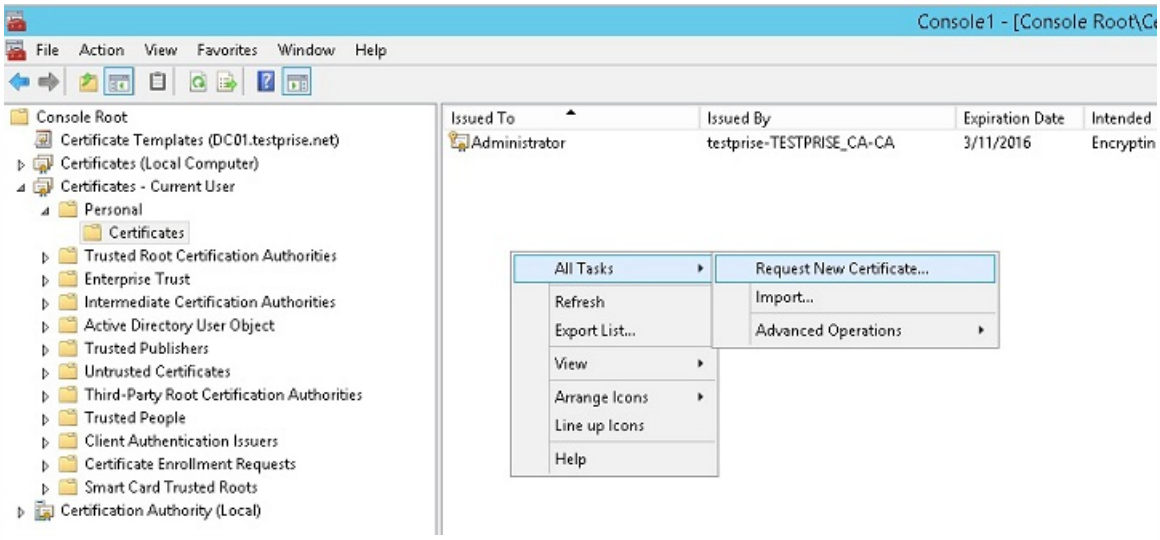


Creating a PFX certificate from the CA server

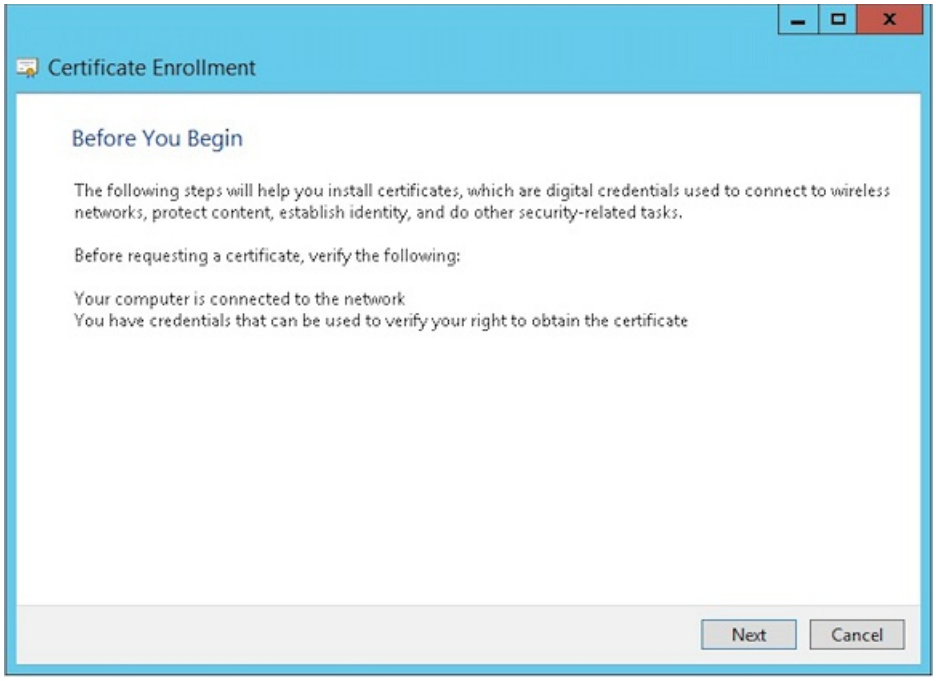
1. Create a user .pfx cert using the service account with which you logged in. This .pfx will be uploaded into XenMobile, which will request a user certificate on behalf of the users who enroll their devices.

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

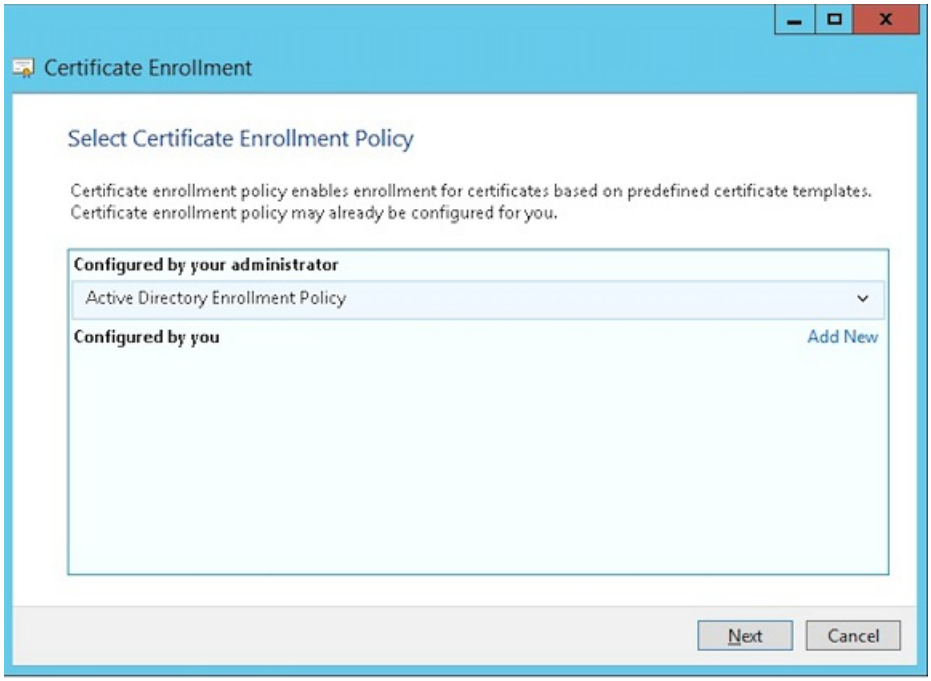
3. Right-click in the right pane and then click **Request New Certificate**.



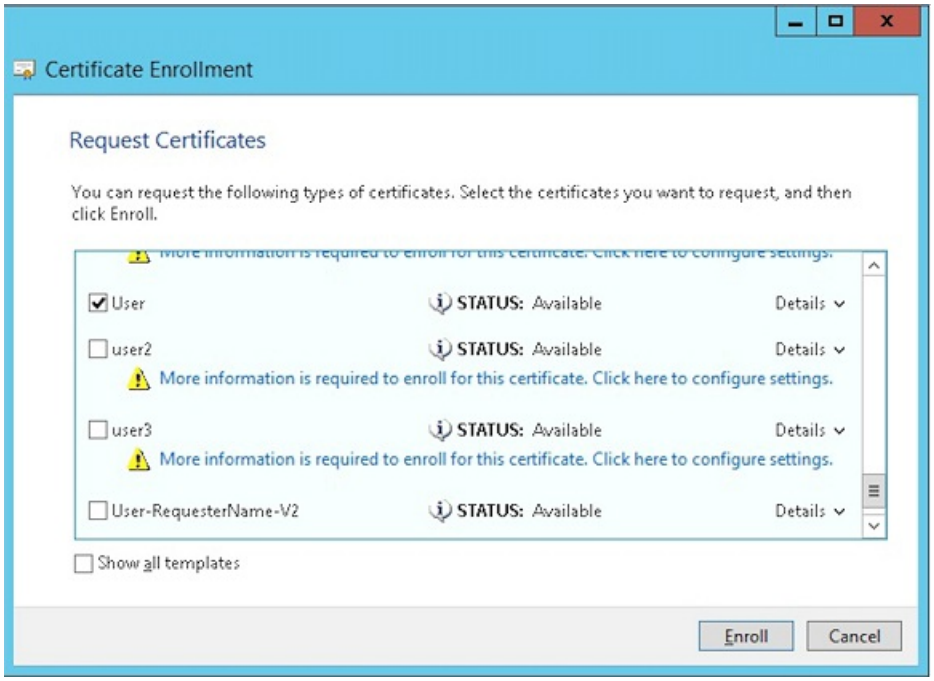
4. The **Certificate Enrollment** screen appears. Click **Next**.



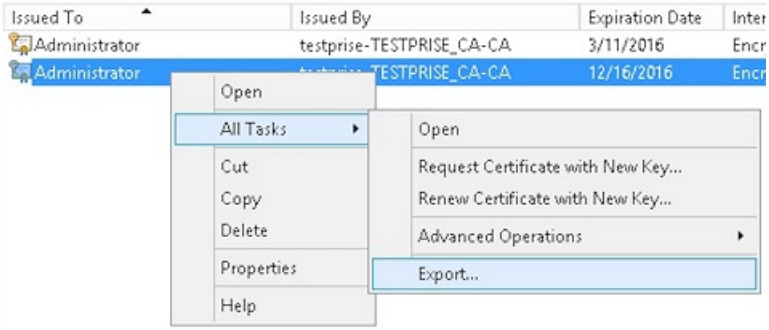
5. Select **Active Directory Enrollment Policy** and then click **Next**.



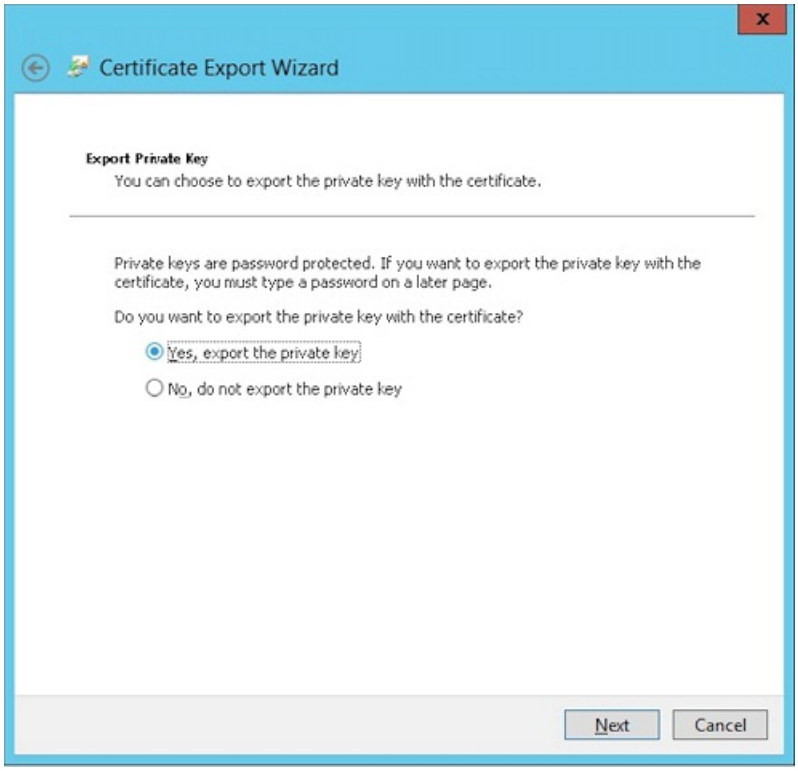
6. Select the **User** template and then click **Enroll**.



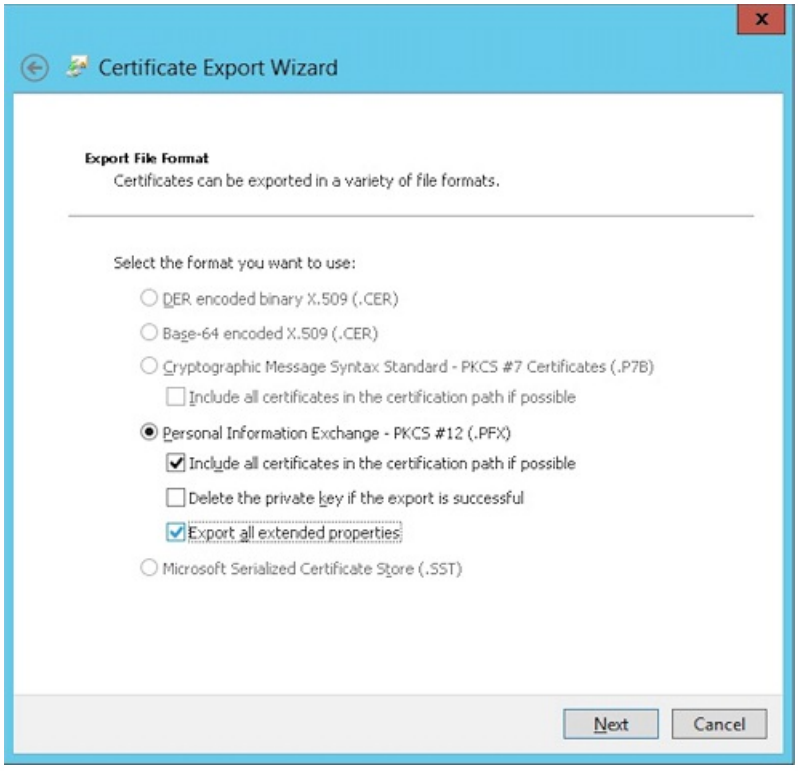
7. Export the .pfx file that you created in the previous step.



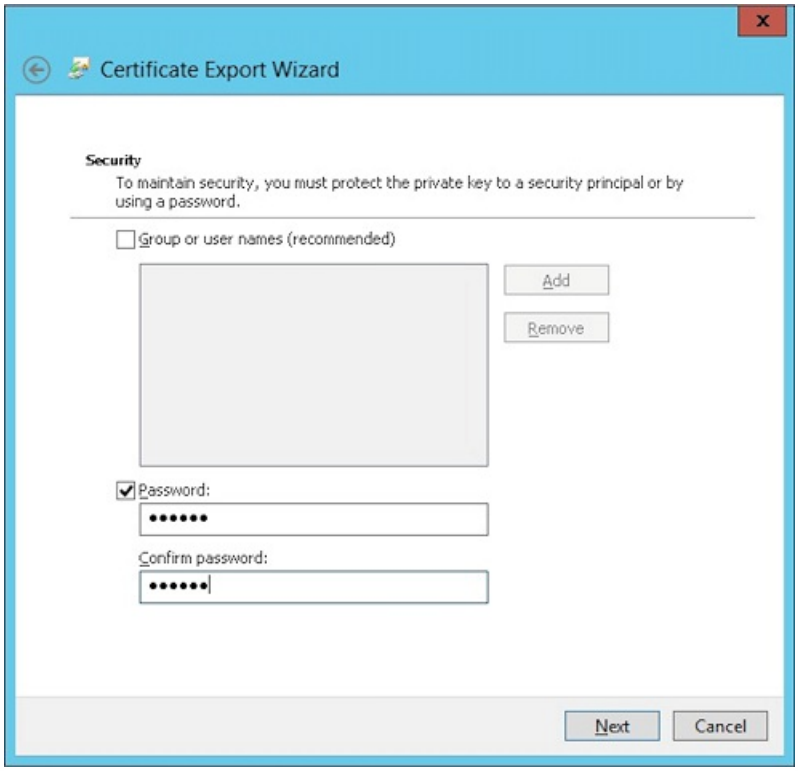
8. Click **Yes, export the private key**.



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.

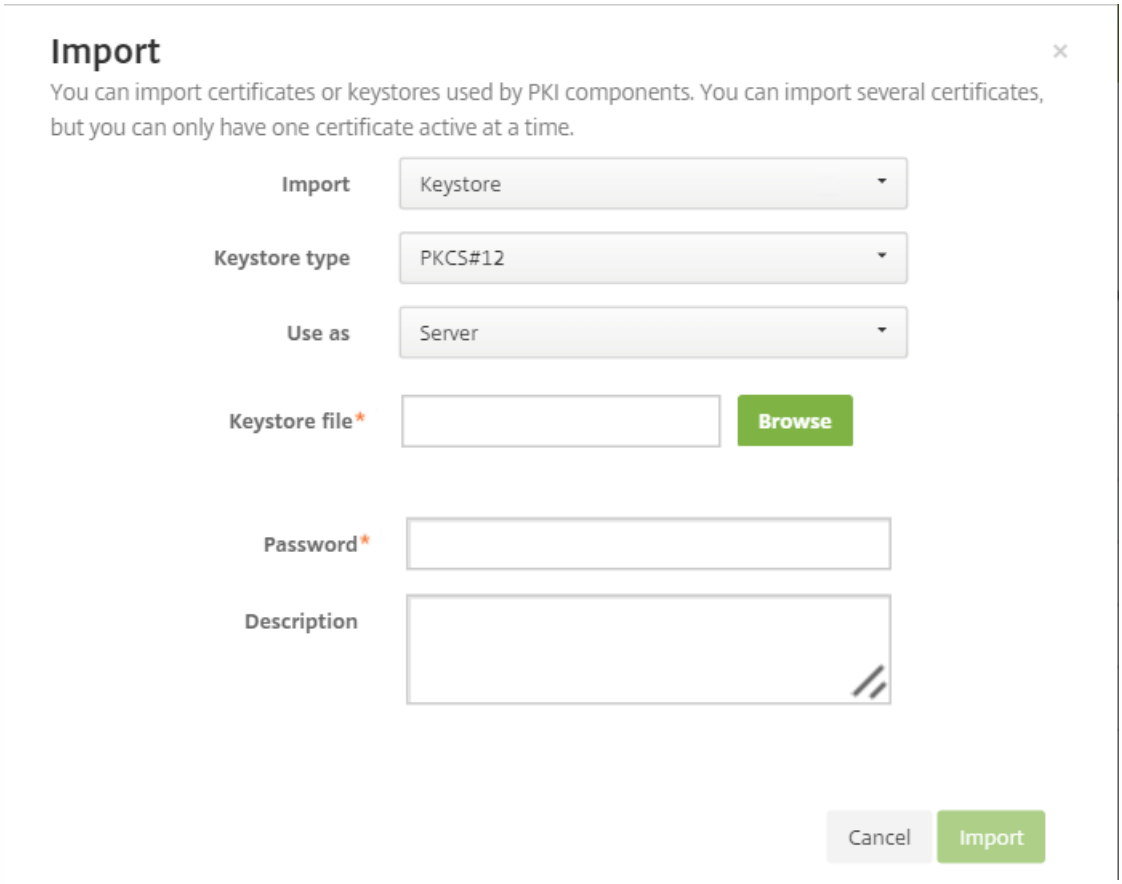
Uploading the certificate to XenMobile

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.

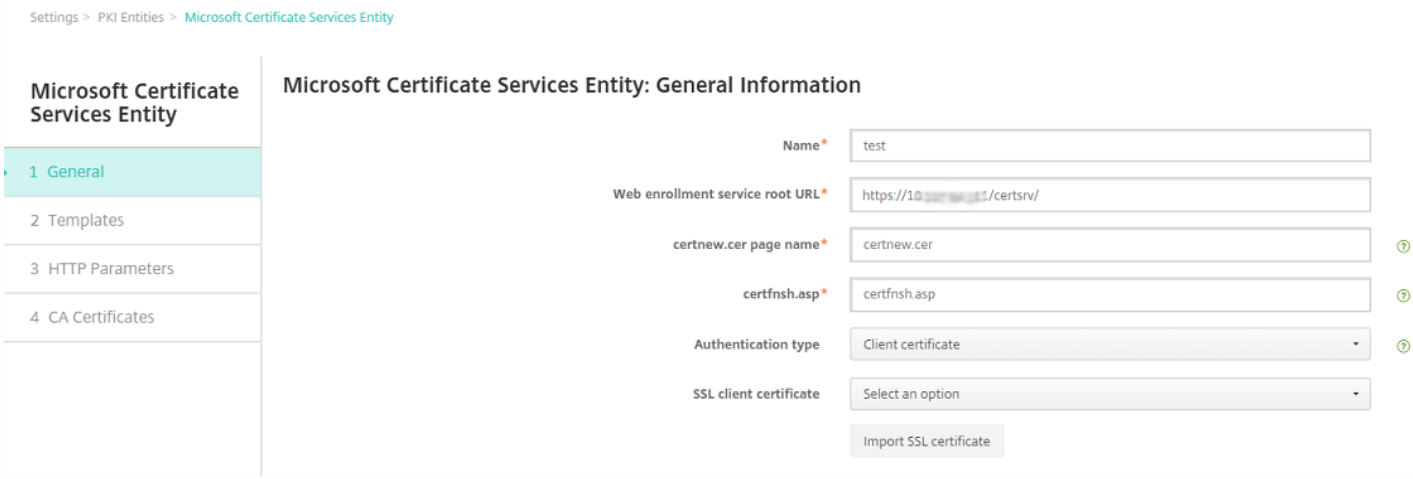
Creating the PKI entity for certificate-based authentication

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

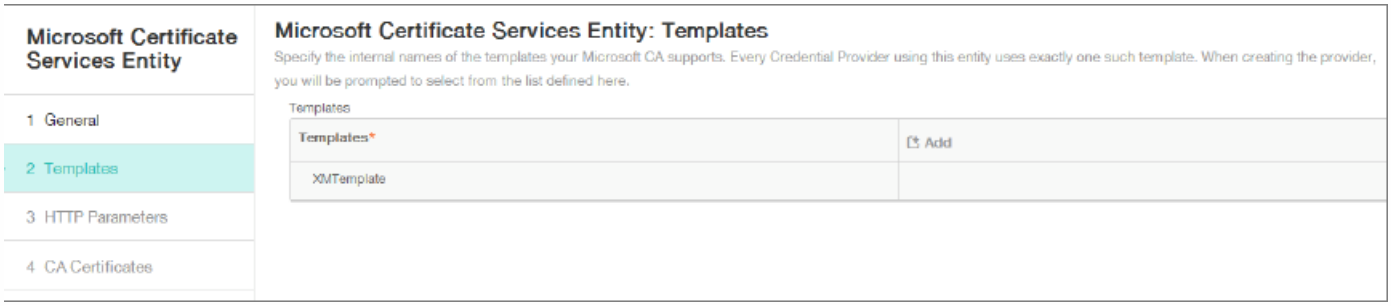
2. Click **Add** and then click **Microsoft Certificate Services Entity**. The **Microsoft Certificate Services Entity: General Information** screen appears.

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.

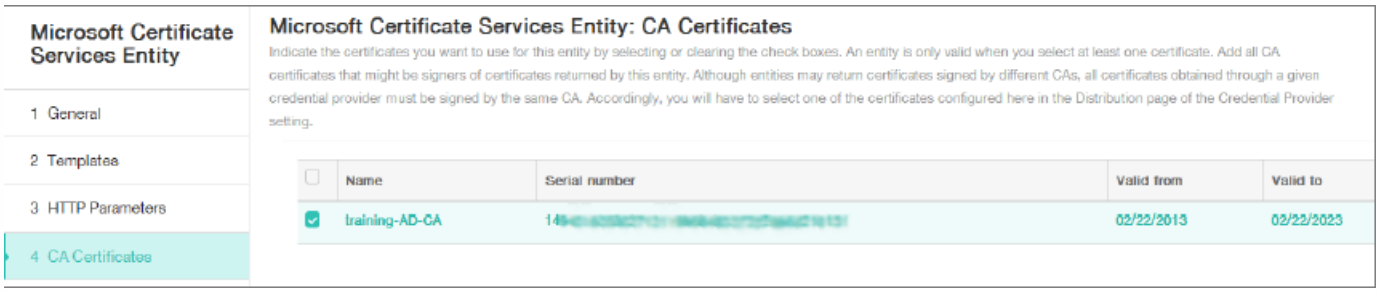


4. Under **Templates**, add the template that you created when configuring the Microsoft certificate. Be sure not to add spaces.



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**.

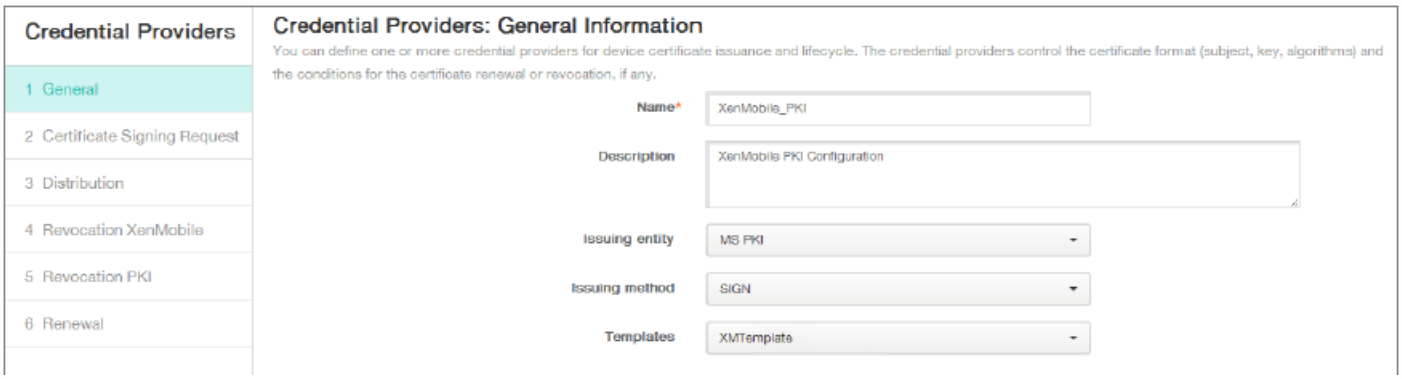
Configuring credentials providers

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:

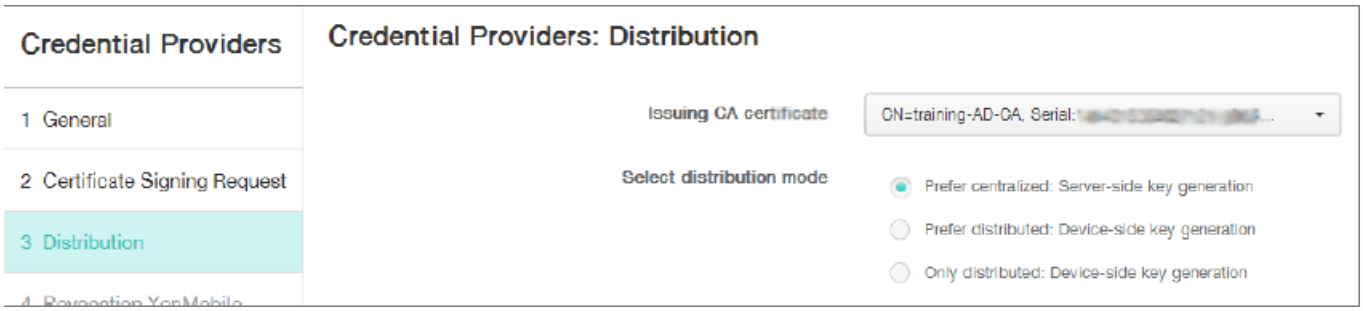
- **Key algorithm**: RSA
- **Key size**: 2048
- **Signature algorithm**: SHA1withRSA
- **Subject name**: cn=$user.username

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**.

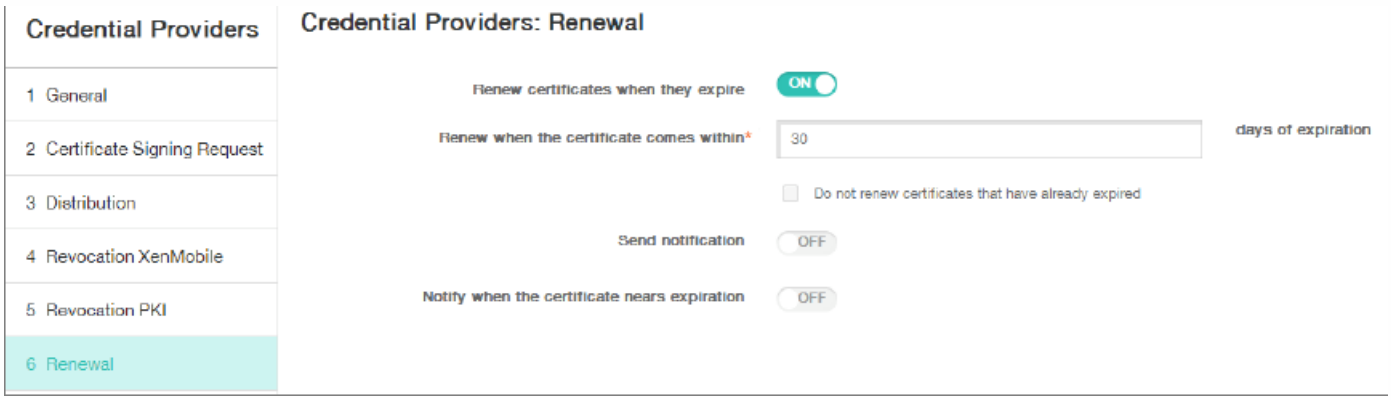


6. For the next two sections -- **Revocation XenMobile** and **Revocation PKI** -- set the parameters as required. For the purpose of this article, both options are skipped.

7. Click **Renewal**.

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

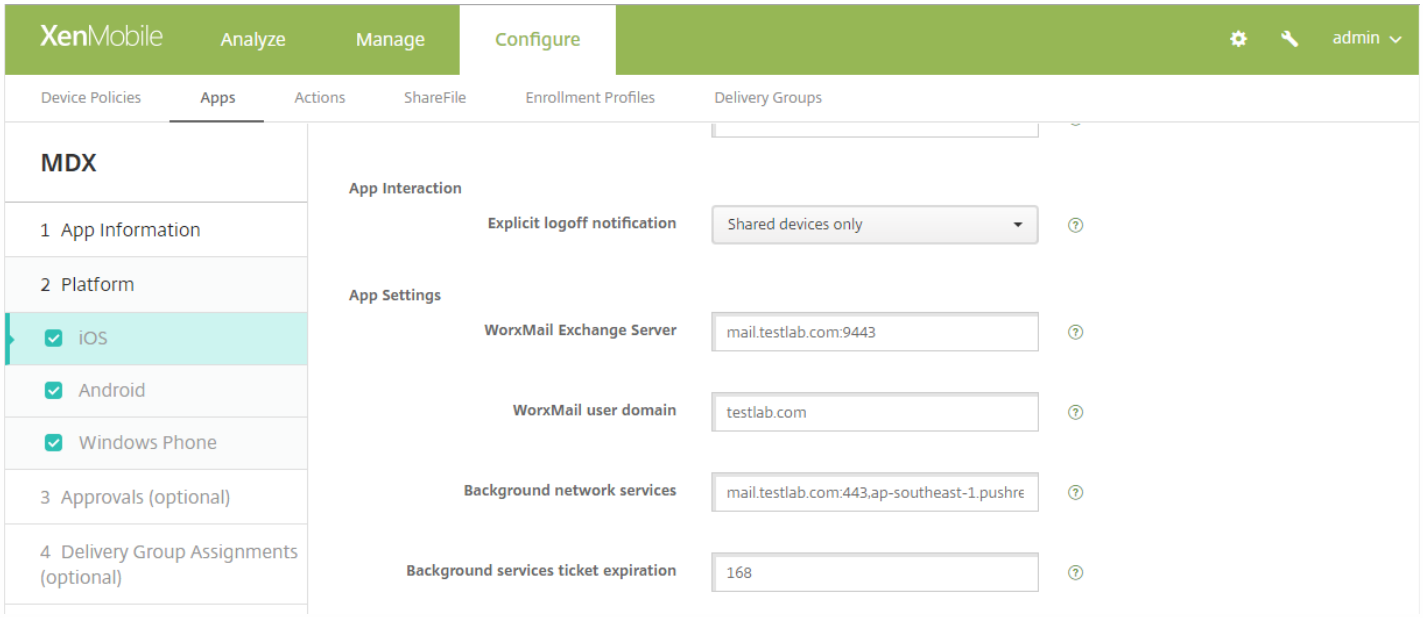
9. Leave all other settings as default or change them as required.



10. Click **Save**.

Configuring WorxMail to use certificate-based authentication

When you add WorxMail to XenMobile, be sure to configure the Exchange settings under **App Settings**.



Configuring NetScaler certificate delivery in XenMobile

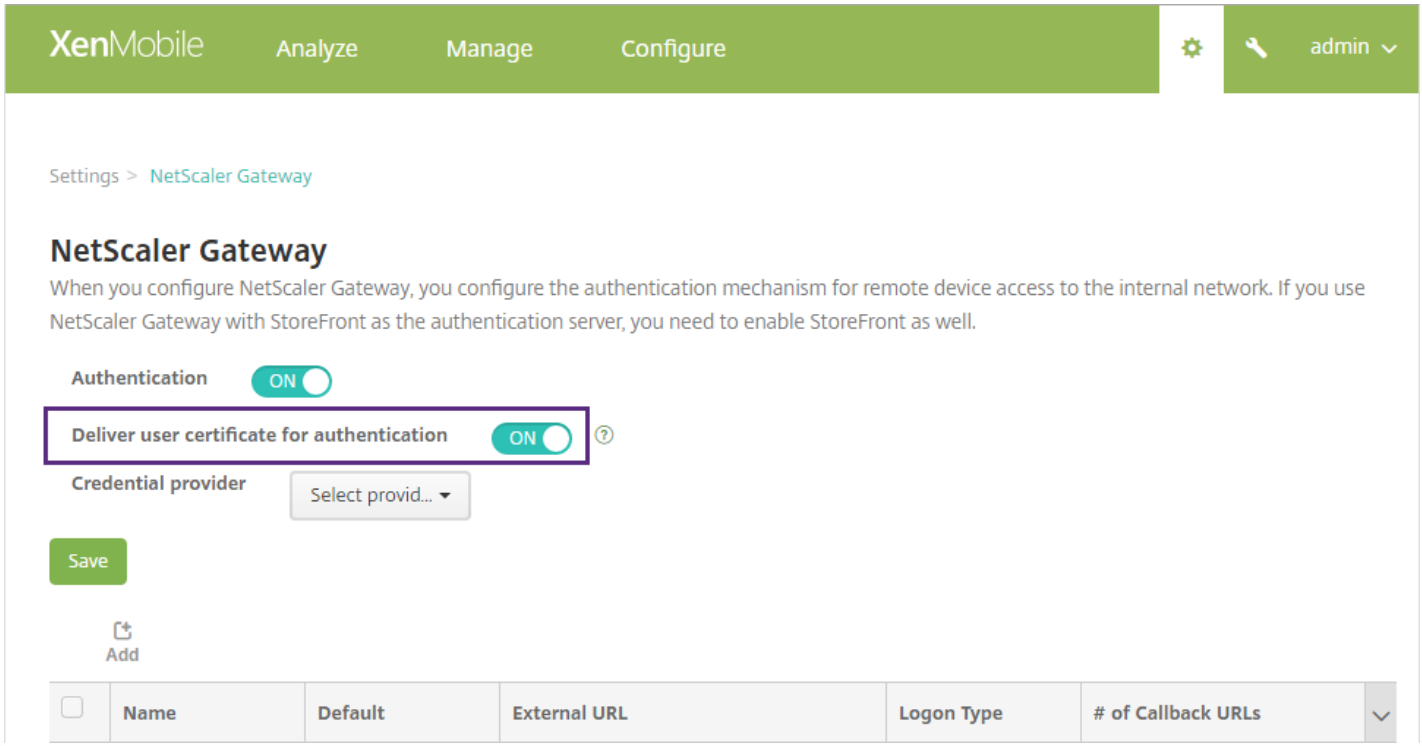
1. Log on to the XenMobile console and click the gear icon in the upper-right corner. The **Settings** screen appears.

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

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

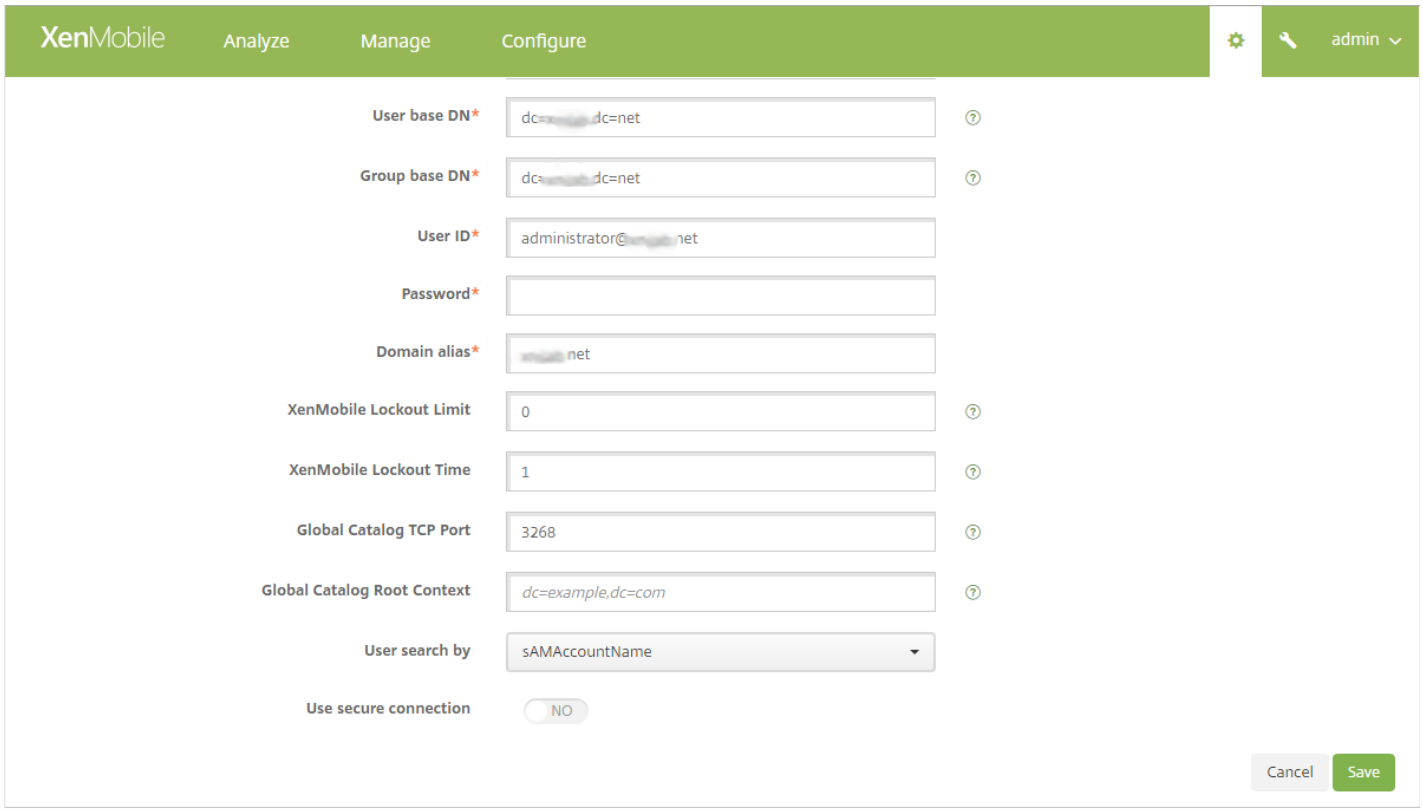
- **External URL**: https://YourNetScalerGatewayURL
- **Logon Type**: Certificate
- **Password Required**: OFF
- **Set as Default**: ON

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

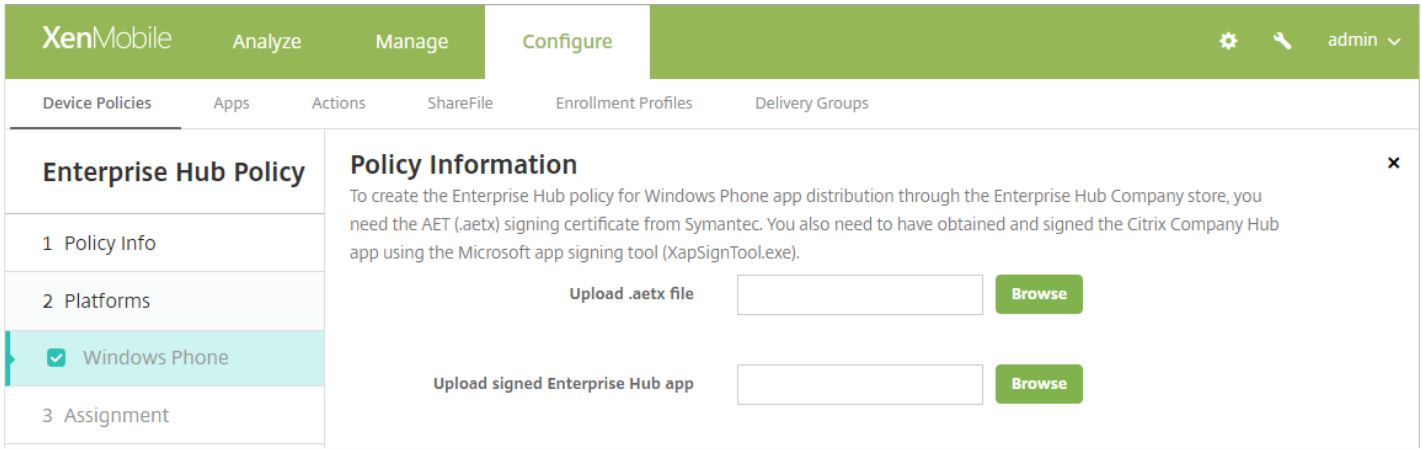
For Windows Phone 8.1 devices, you must create an Enterprise Hub device policy to deliver the AETX file and the Worx Home client.

> **Note**
>
> Ensure that both the AETX and Worx Home 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 Worx Home app for the Enterprise Hub.



4. Assign the policy to delivery groups and save it.

Using the NetScaler for XenMobile wizard to configure NetScaler Gateway for certificate authentication

> **Note**
>
> You can run the NetScaler for XenMobile wizard one time only. If you've already used the wizard, follow the instructions in "To manually configure NetScaler Gateway for certificate authentication", next.

Follow these steps on your NetScaler appliance to configure certificate authentication in XenMobile.

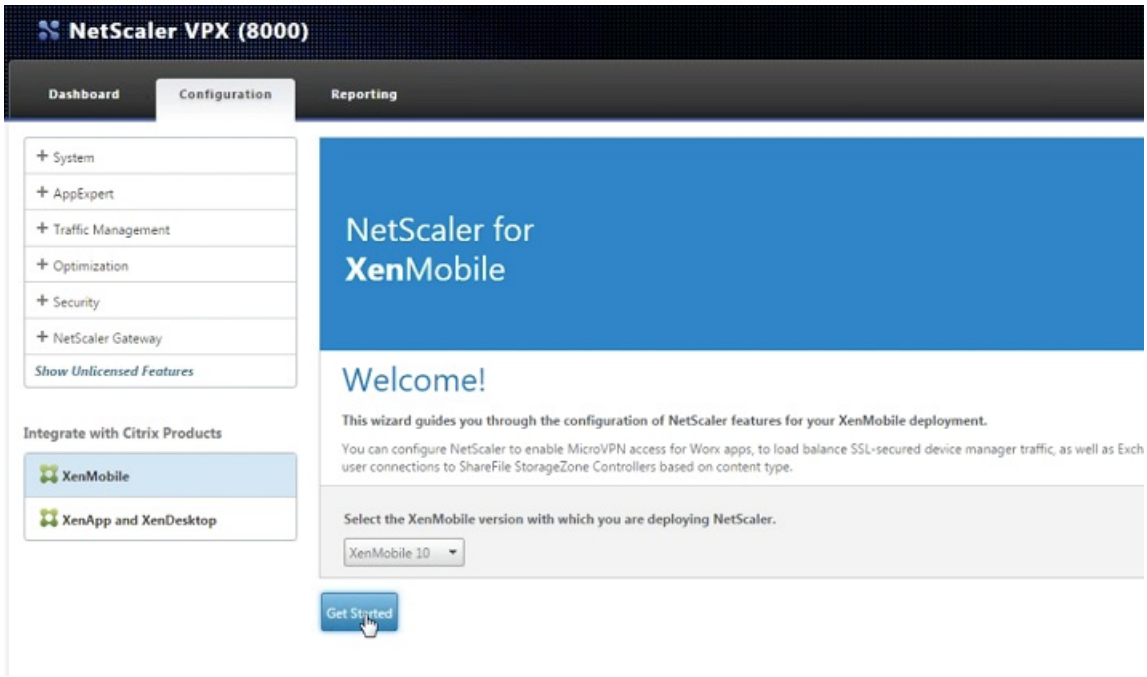
1. Log on to NetScaler.

2. Under **Configuration**, go to **Integrate with Citrix Products** and then select **XenMobile**.

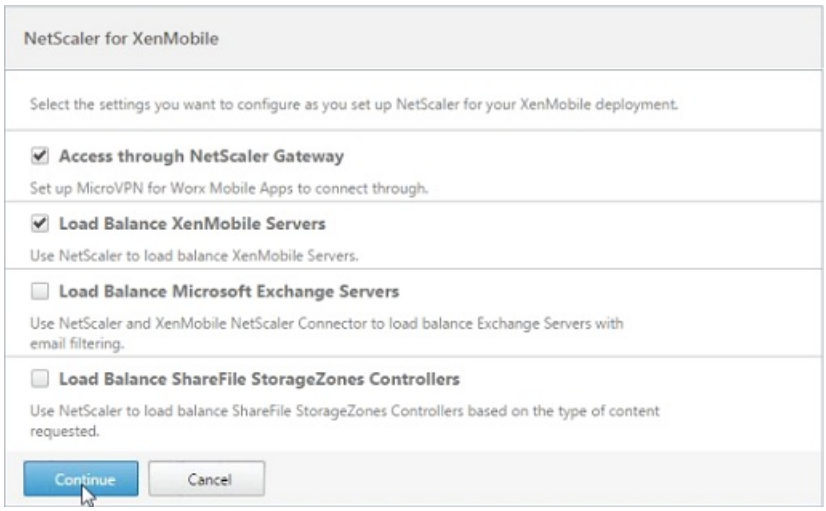
This opens a wizard to configure NetScaler features for your XenMobile deployment.

3. Choose **XenMobile 10**.

4. Click **Get Started**.



5. On the next screen, select **Access through NetScaler Gateway** (for ENT and MAM modes) and **Load Balance XenMobile Servers** and then click **Continue**.



6. On the next screen, enter the external-facing NetScaler Gateway IP address and then click **Continue**.

The Server Certificate for NetScaler Gateway screen appears.

7. You will either use an existing certificate or install one. Click **Continue**.

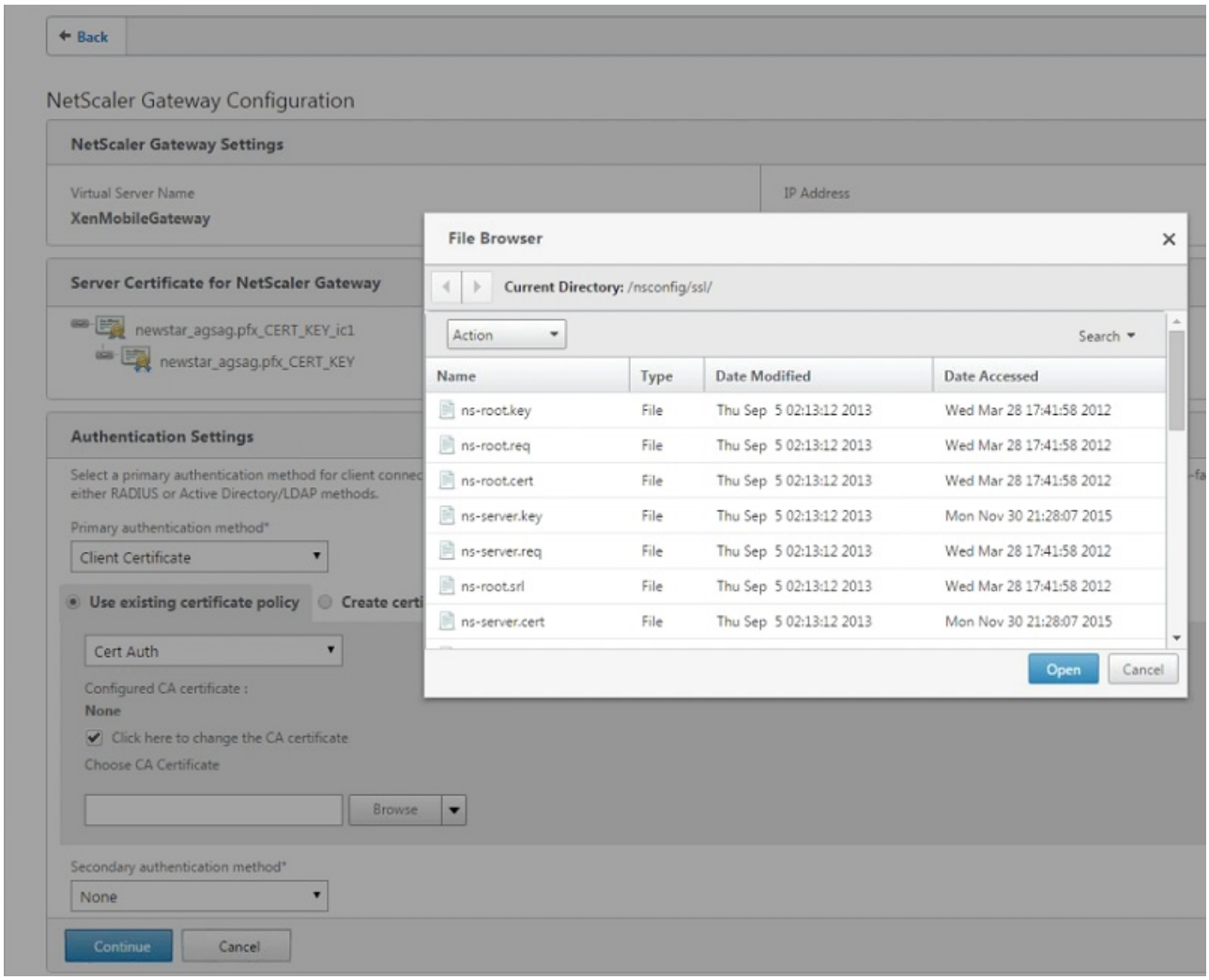
The **Authentication Settings** screen appears.

8. In the **Primary authentication method** field, select **Client Certificate**.

This will automatically select **Use existing certificate policy** and **Cert Auth** in the next two fields. The following steps assume that you already have a certificate policy.

If you need to create a certificate policy, click **Create certificate policy** and complete the settings. On the **XenMobile Server Certificate** screen, choose an existing server certificate or install a new certificate. If you're running multiple XenMobile servers, you will add a certificate for each one. For **Server Logon Name Attribute** specify **userPrincipalName** or **samAccountName.**

9. Select **Click here to change the CA certificate** and then in the **Browse** list, navigate to the CA certificate you want.



10. Leave **Second authentication method** as **None** and then click **Continue**.

11. On the **Device certificate** screen, if the certificate is not already installed, you must export this certificate from the XenMobile console. To do so:

a. From the console, click the gear icon in the upper-right corner to open the **Settings** screen.

b. Click **Certificate** and then choose the CA certificate from the list.

c. Click **Export**.

d. Return to the NetScaler wizard and select the certificate you exported (downloaded) to install it.

e. Click **Continue**.

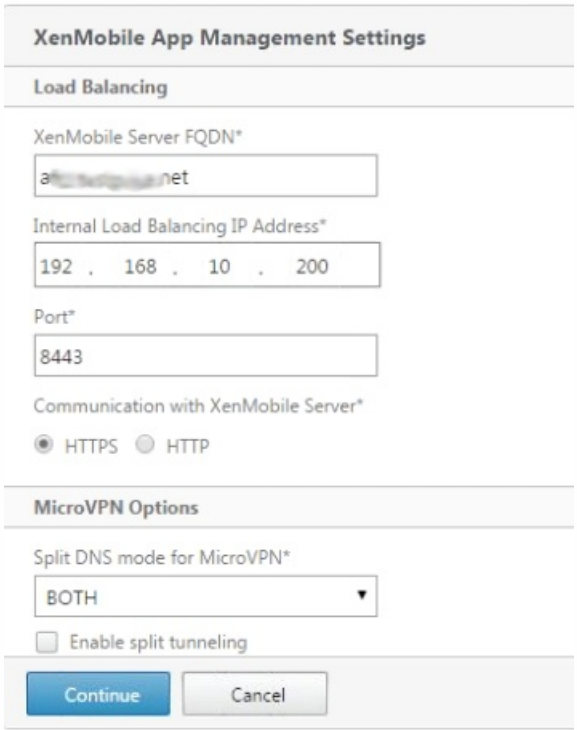
The XenMobile server IP addresses that you've configured will appear.

12. On the **Load Balancing** screen, enter the XenMobile server FQDN and a MAM-only internal load balancing IP address.

13. Because this is an SSL offload deployment, select **HTTP** in **Communication with XenMobile Server**.

The **Split DNS mode for MicroVPN** field will appear as **BOTH**.

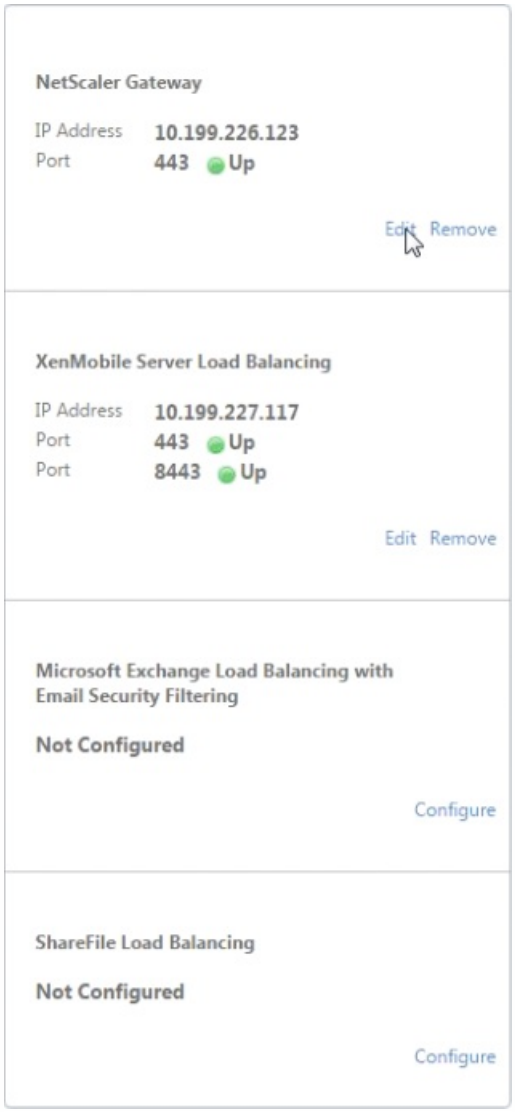
14. Click **Continue**.



The XenMobile server IP addresses that you've configured will appear.

15. Click **Continue**.

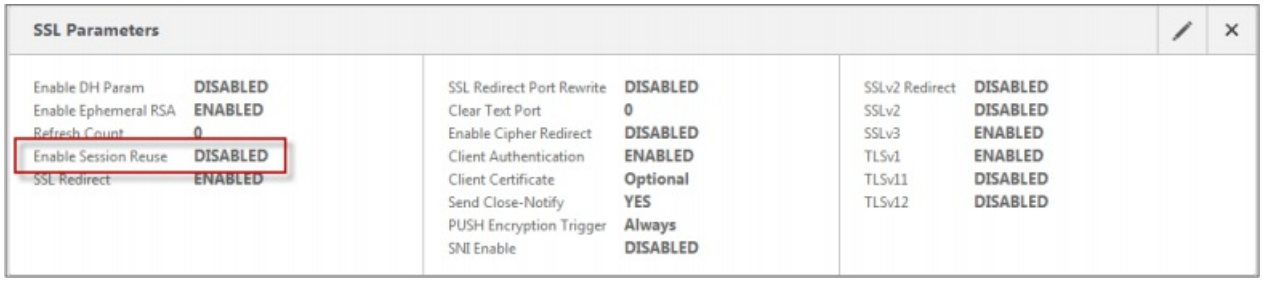
On the NetScaler dashboard, confirm that NetScaler Gateway and XenMobile load balancing are configured as follows.



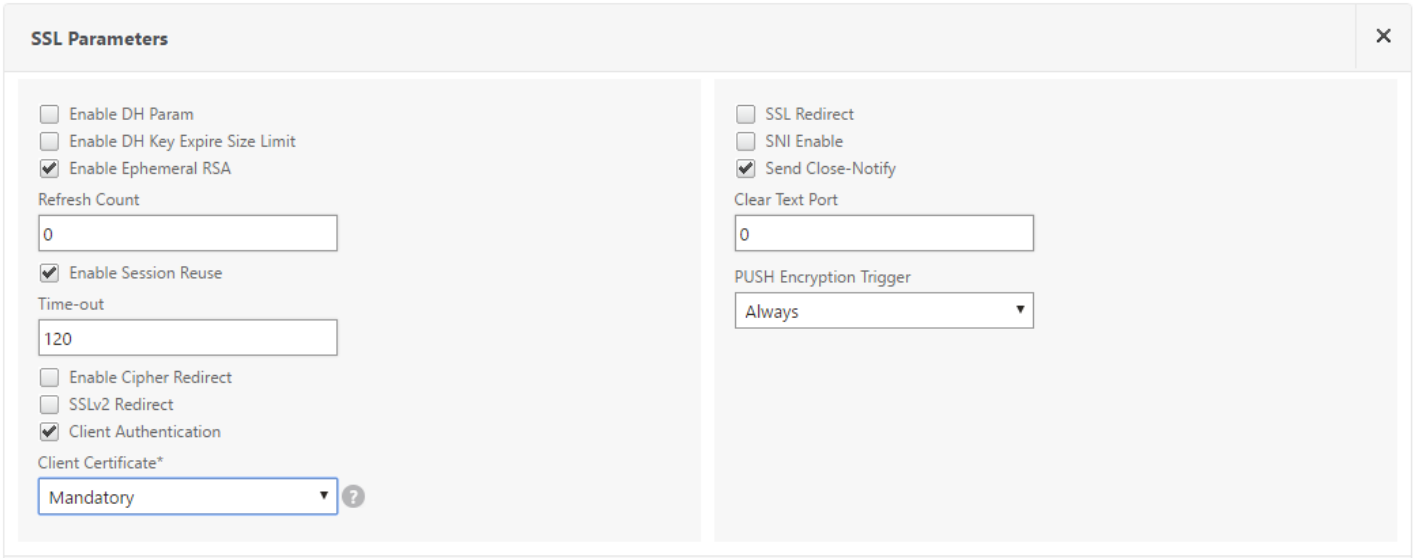
16. If you will use sAMAccount attributes in the user certificates as an alternative to User Principal Name (UPN), configure the certificate profile as described in the next section.

Manually configuring NetScaler Gateway for certificate authentication

1. Under **Traffic Management > Load Balancing > Virtual Servers**, go to each virtual server (both 443 and 8443), update the **SSL Parameters**, and set **Enable Session Reuse** to **DISABLED**.



2. On the NetScaler Gateway virtual server, on **Enable Client Authentication -> Client Certificate**, select **Client Authentication** and for **Client Certificate**, select **Mandatory**.



3. Create a new authentication Certificate policy so XenMobile can extract the **User Principal Name** or the **sAMAccount** from the client certificate provided by Worx Home to NetScaler Gateway.

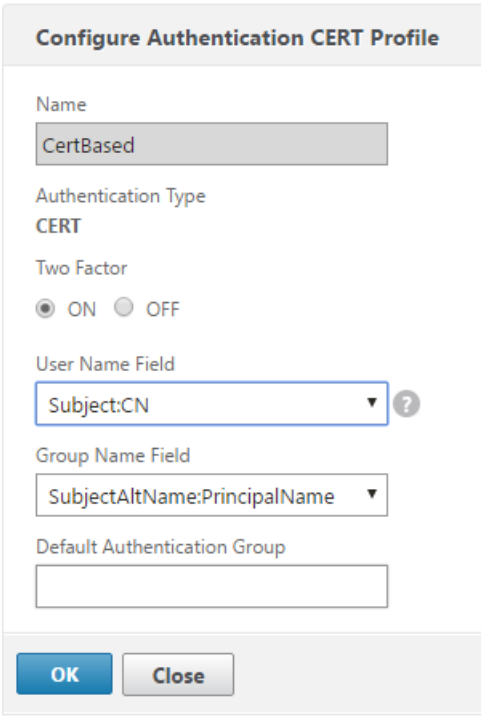
4. Set the following parameters for the certificate profile:

Authentication Type: **CERT**

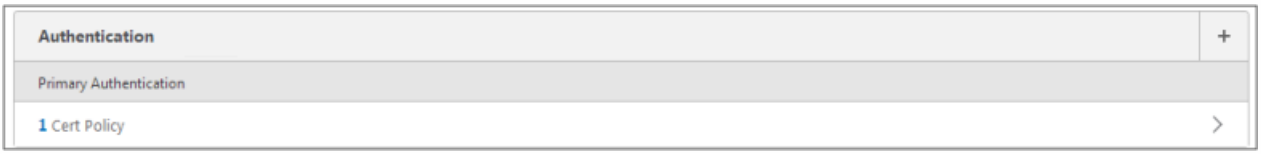
Two Factor: **ON** or **OFF**

User Name Field: **Subject:CN**

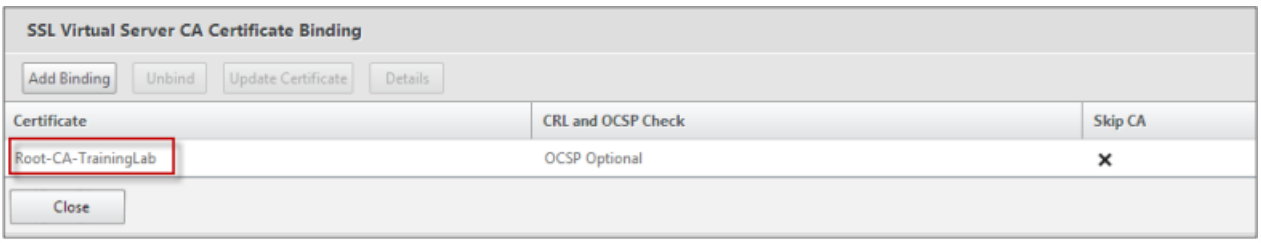
Group Name Field: **SubjectAltName:PrincipalName**

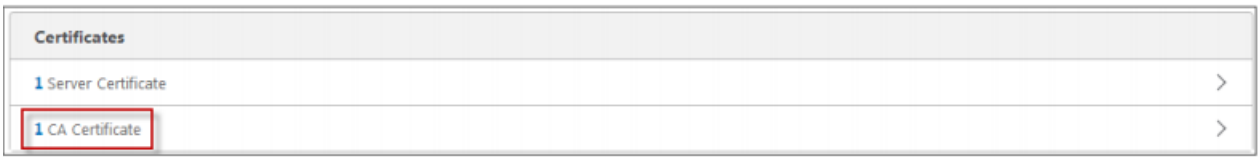


5. Bind only the certificate authentication policy as the **Primary Authentication** in the NetScaler Gateway virtual server.



6. Bind the Root CA certificate to validate the trust of the client certificate presented to NetScaler Gateway.





Troubleshooting your client certificate configuration

After a successful configuration, the user workflow is as follows:

1. Users enroll their mobile device.

2. XenMobile prompts users to create a Worx PIN.

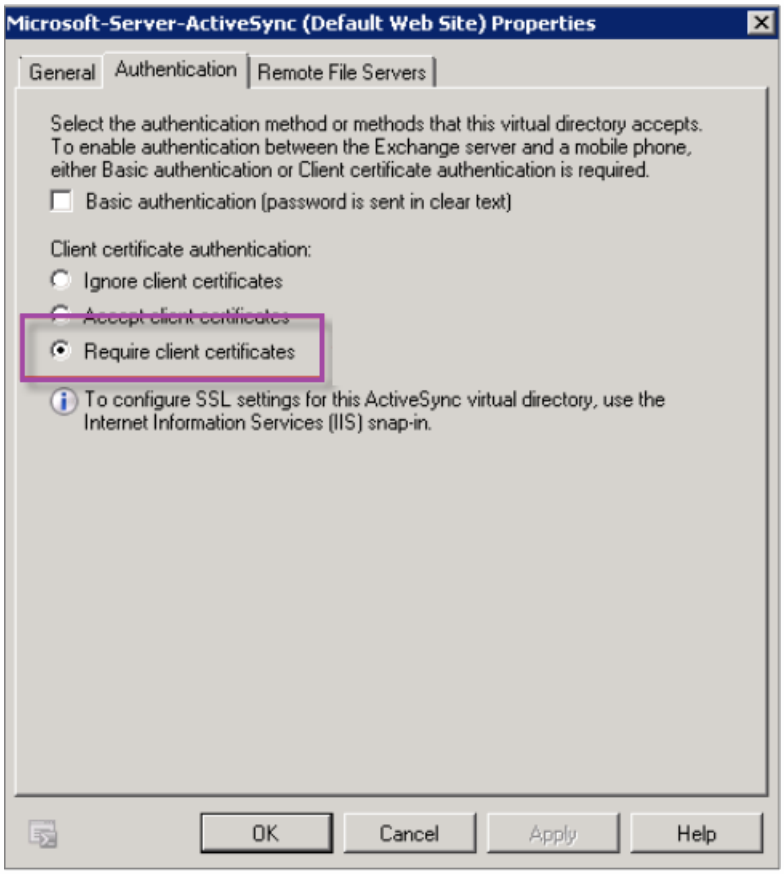
3. Users are then redirected to the Worx Store.

4. When users start WorxMail for iOS, Android or Windows Phone 8.1, XenMobile will not prompt them for user credentials in order to configure their mailbox. Instead, WorxMail requests the client certificate from Worx Home and submits it to Microsoft Exchange Server for authentication. If XenMobile prompts for credentials when users start WorxMail, check your configuration.

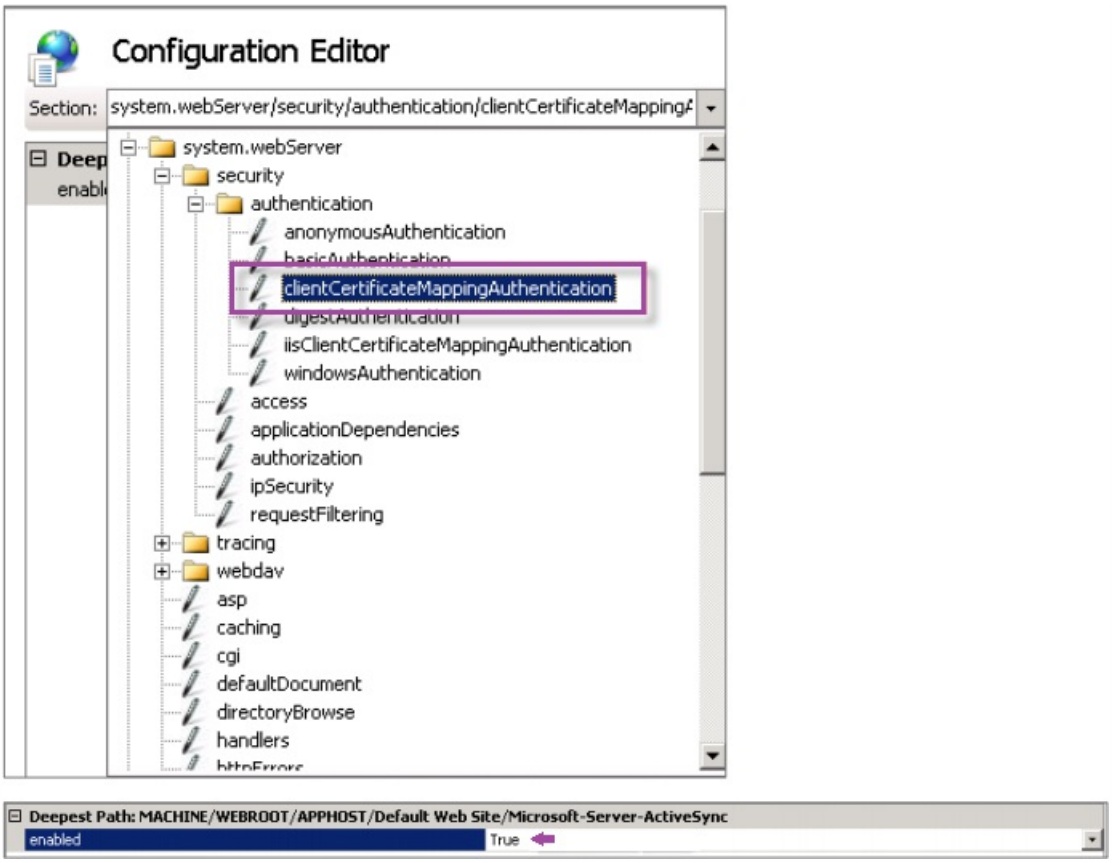
If users can download and install WorxMail, but during the mailbox configuration WorxMail fails to finish the configuration:

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 WorxMail 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 WorxMail and sign Worx Home apps.
- Verify that the same Publisher ID is being used to sign and wrap Worx Home, WorxMail, and the Application Enrollment Token.

PKI Entities

Aug 12, 2016

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

Jul 08, 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 enrollment	No	No
Windows Phone configuration	No	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.

Requesting an APNs Certificate

Apr 07, 2016

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.

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**.

User Accounts, Roles, and Enrollment Settings

Jan 05, 2017

In XenMobile, you configure users and groups, roles for users and groups, as well as enrollment mode and invitations in the XenMobile console Settings page. To open the **Settings** page, click the gear icon in the upper-right corner of the console.

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

- Click **Local Users and Groups** 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 users in XenMobile
  - To import user accounts by using a .csv provisioning file and Provisioning file formats
  - To add or remove groups in XenMobile
- Click **Enrollment** to configure up to seven modes, each with 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
- 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 and RBAC roles and permissions
- 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: Worx Home, SMTP, or SMS. For details, see:
  - Creating and updating Notification Templates

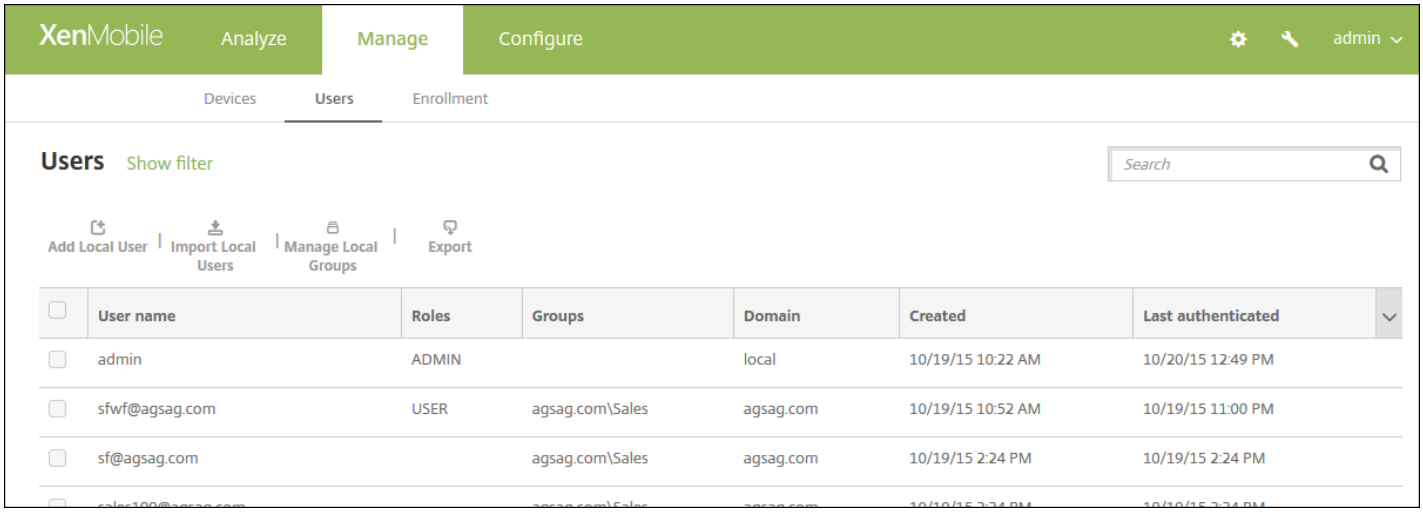
  Note: As of version 10.4, Worx Home is renamed Secure Hub.

To add, edit, or delete local users in XenMobile

May 15, 2015

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

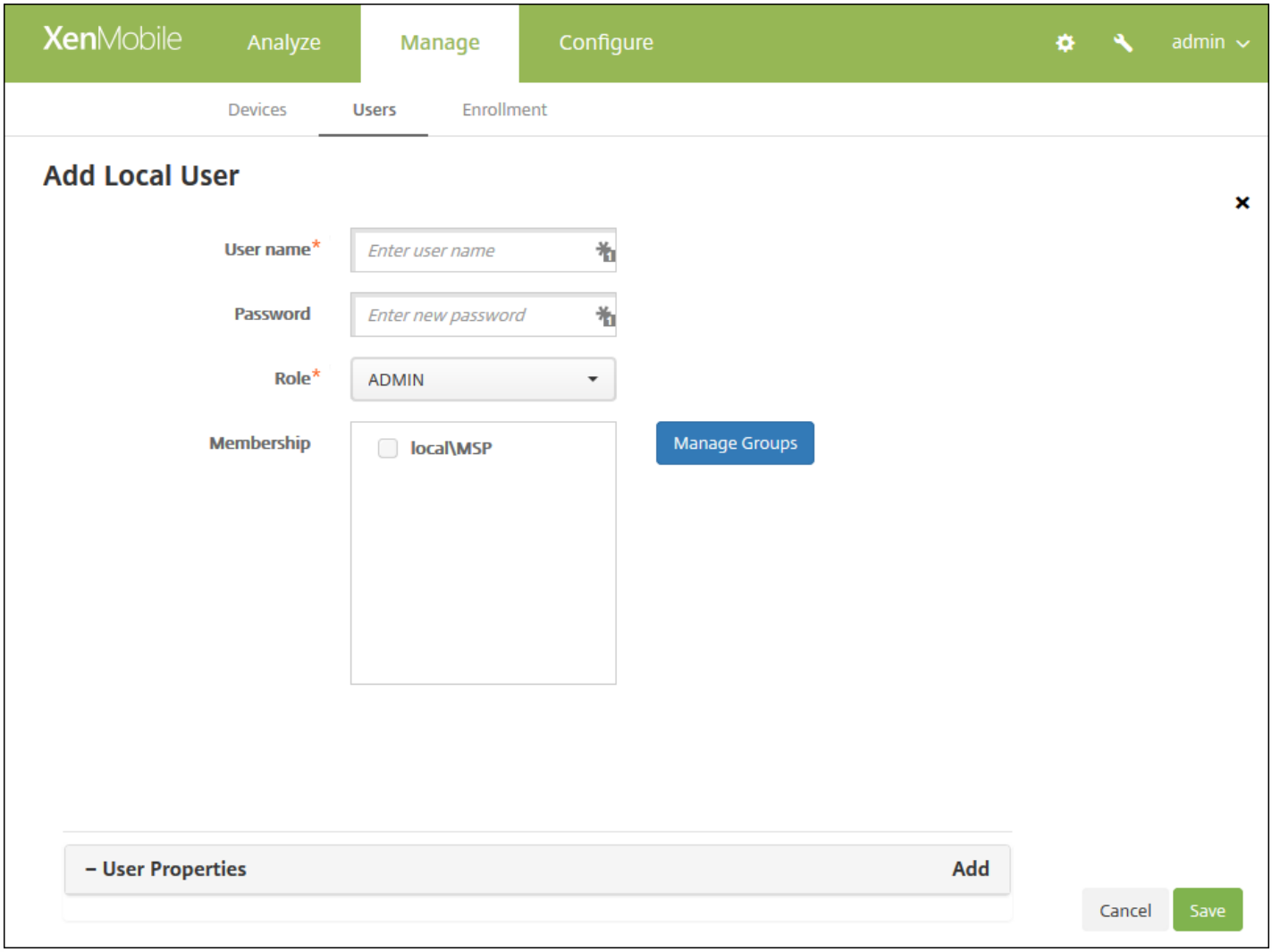
1. In the XenMobile console, click **Manage > Users**. The **Users** page appears.



To add a local user

This procedure adds one user to XenMobile at a time. To add multiple users, see To import user accounts by using a .csv provisioning file.

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

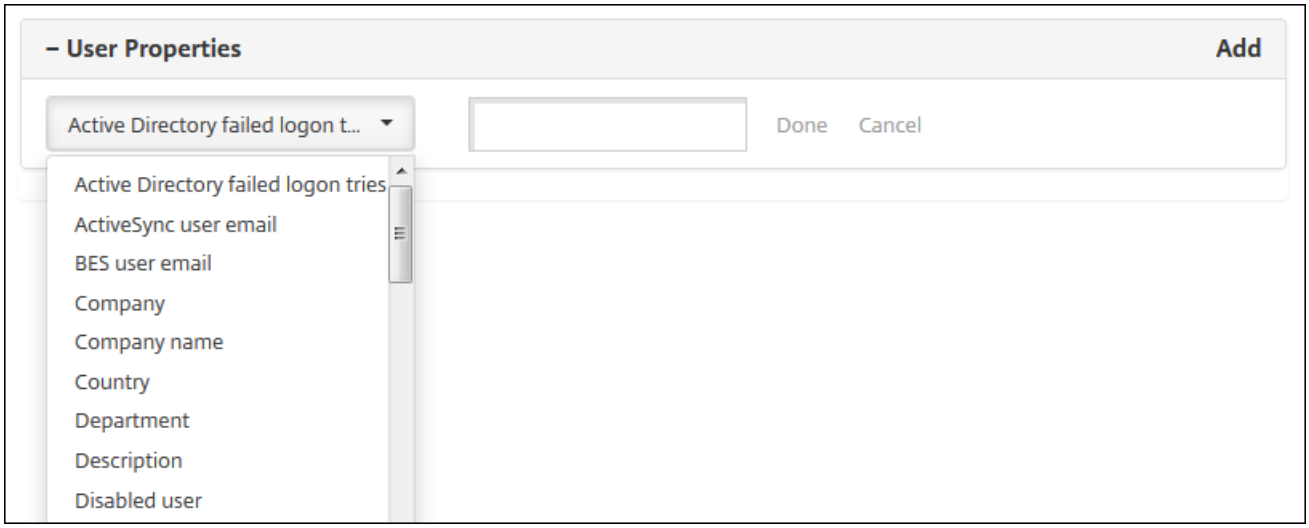


2. Configure these settings:

- **User name**: Type the user's name. This is a required field. You can include spaces in names, as well as upper and lowercase letters.
- **Password**: Type an optional user password.
- **Role**: In the list, click the user's role. For more information about roles, see Configuring Roles with RBAC and RBAC roles and permissions. Possible options are:
  - ADMIN
  - DEVICE_PROVISIONING,
  - SUPPORT
  - USER
- **Membership**: In the list, click the group or groups to which to add the user.
- **User Properties**: Add optional user properties. For each user property you want to add, click **Add** and do the following:
  - **User Properties**: In the list, click a property and then type the user property attribute in the field next to the property.
  - Click **Done** to save the user property or click **Cancel** to not 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.

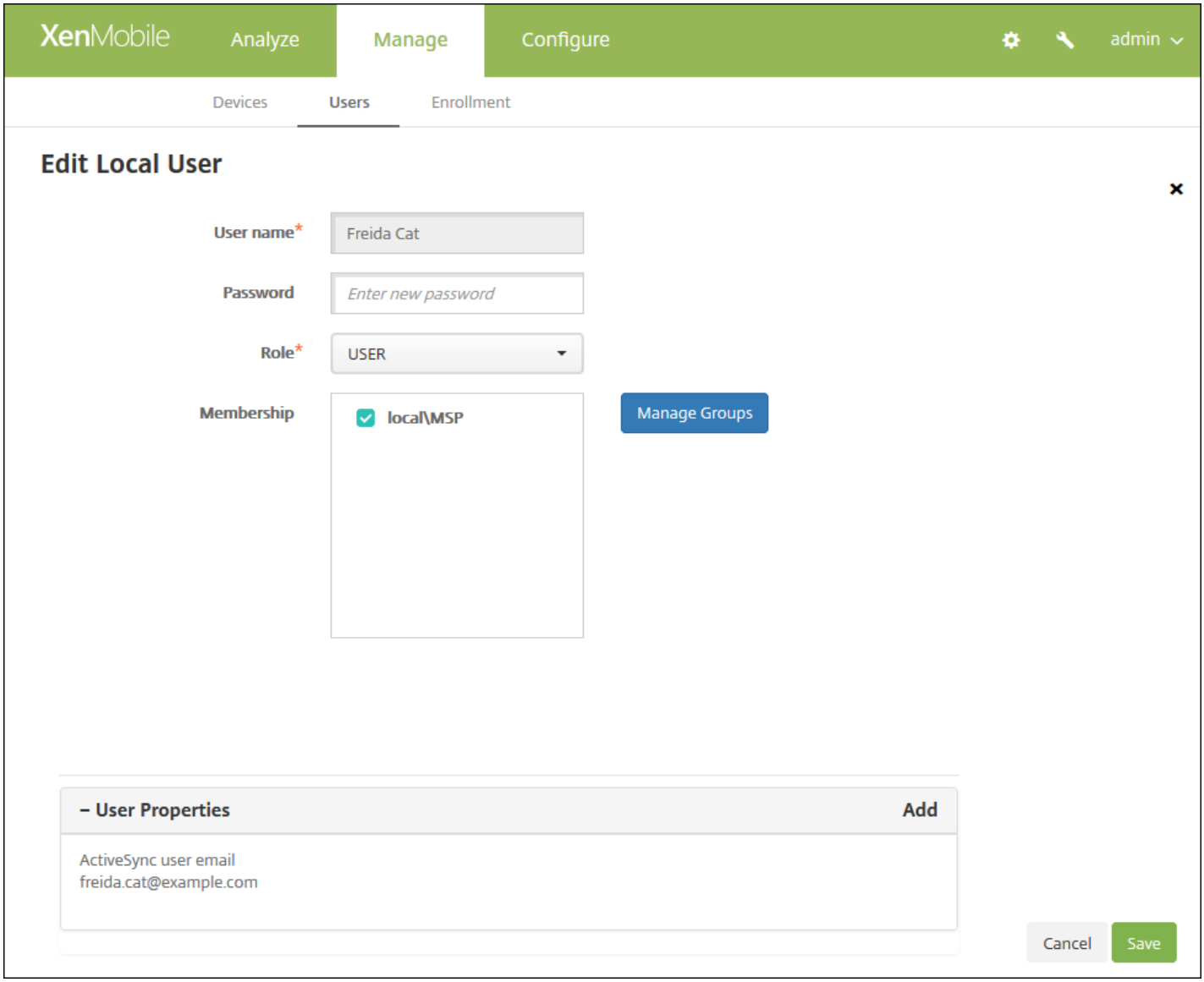
To edit an existing user property, click the property and make changes. Click **Done** to save the changed listing or **Cancel** to leave the listing unchanged.



3. Click **Save**.

To edit a local user

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. See Filters and Tables in the XenMobile console for more information about selecting items in tables.



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's role.
- **Membership**: In the list, click the group or groups to which to add the user. To remove the user 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** to not 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

1. On the **Users** page, in the list of users, click to select a user.

    Note: You can select more than one user to delete by selecting the check box next to each user.

2. Click **Delete**. A confirmation dialog box appears.

3. Click **Delete** to delete the user or click **Cancel** to not delete the user.

Importing User Accounts

Sep 16, 2016

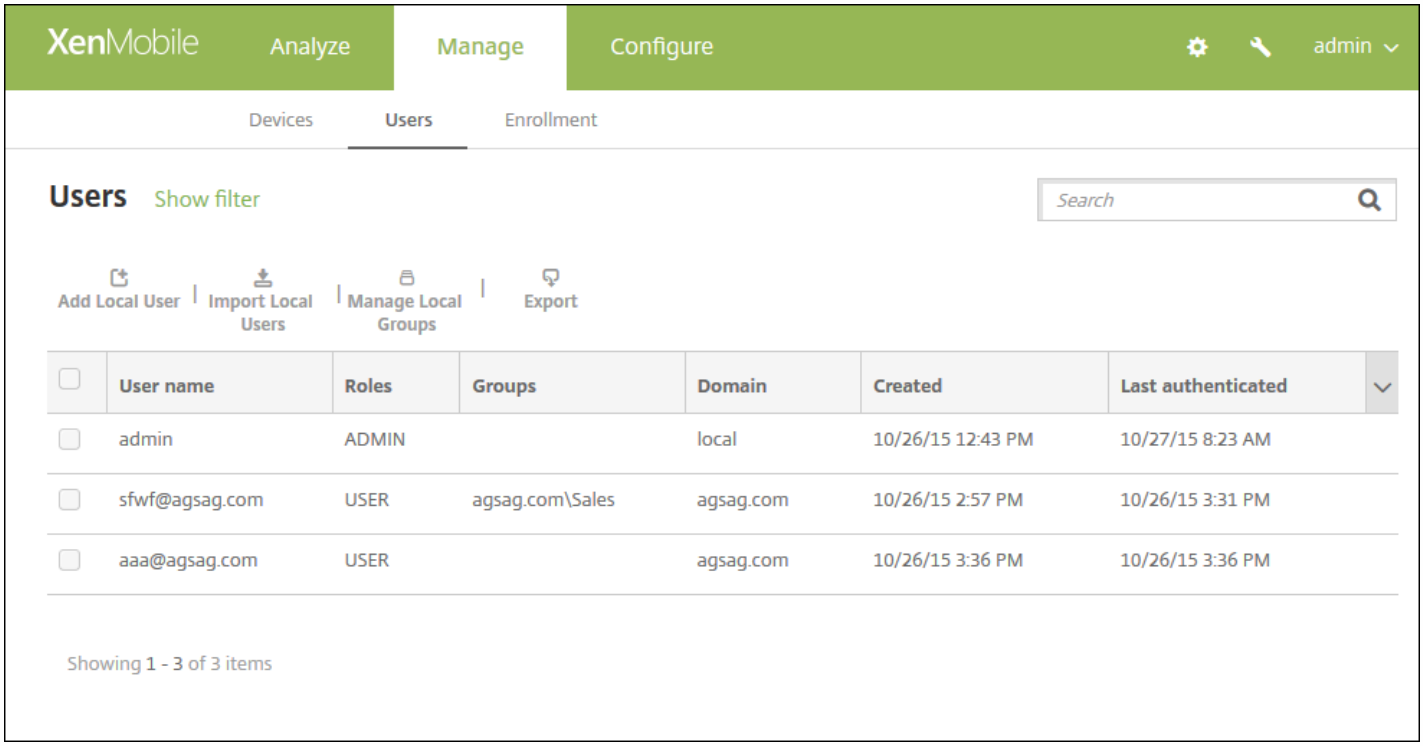
You can import user accounts and properties from a .csv file called a provisioning file, which you can create manually. See Provisioning file formats for information about formatting provisioning files.

Note:

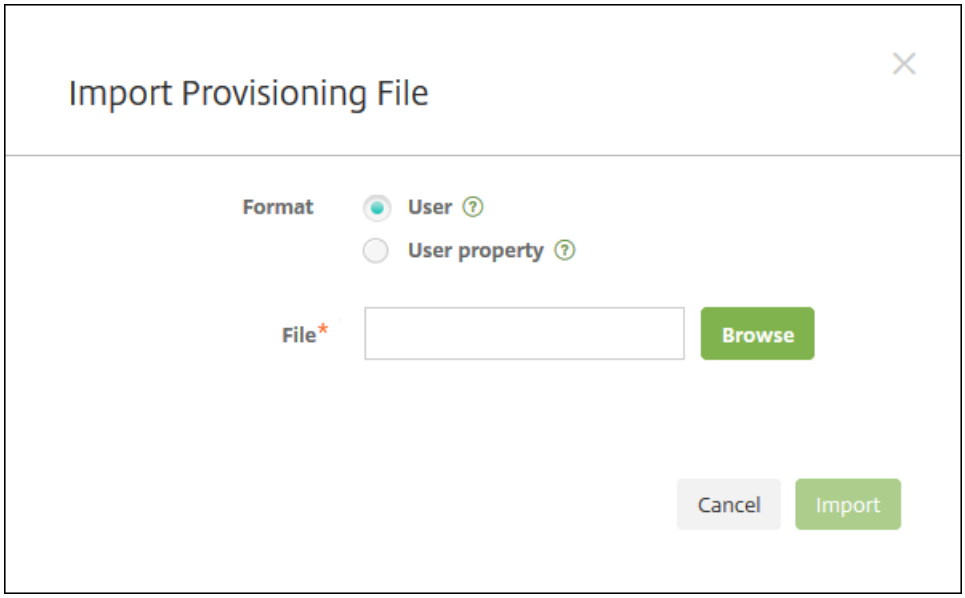
- If you are importing users from an LDAP directory, use the domain name along with the user name in the import file. For example, specify username@domain.com. This syntax prevents additional lookups that will slow the import speed.
- If importing users to the XenMobile internal user directory, disable the default domain to speed up the import process. You can reenable the default domain after the import of internal users is completed.
- Local users can be in User Principal Name (UPN) format, but Citrix recommends that you do not use the managed domain; for example, if example.com is managed, do not create a local user with this UPN format: user@example.com.

After you prepare a provisioning file, follow these steps to import the file to XenMobile.

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



2. Click **Import Local Users**. The **Import Provisioning File** dialog box appears.



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

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

5. Click **Import**.

Provisioning file formats

Aug 09, 2016

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;passowrd;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 (;). If part of a field contains a semi-colon, it must be escaped with a backslash character (\). For example, theproperty 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 any additional 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

As another example, AUser0;1.password;USER;ActiveDirectory.test.net, means:

- User: AUser0
- Password: 1.password
- Role: USER
- Group: ActiveDirectory.test.net

Example of user attribute provisioning content

This entry, user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value, means:

- User: user01
- Property 1
  - name: propertyN
  - value: propertyV;test;1;2
- Property 2:
  - name: prop 2
  - value: prop2 value

Adding or Removing Groups

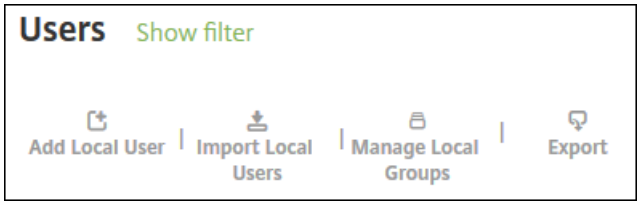
Mar 06, 2015

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 users' association with that group. Users also lose access to apps or profiles provided by the Delivery Groups that are associated with that group; any other group associations, however, remain intact. If users are not associated with any other local groups, they are associated at the top level.

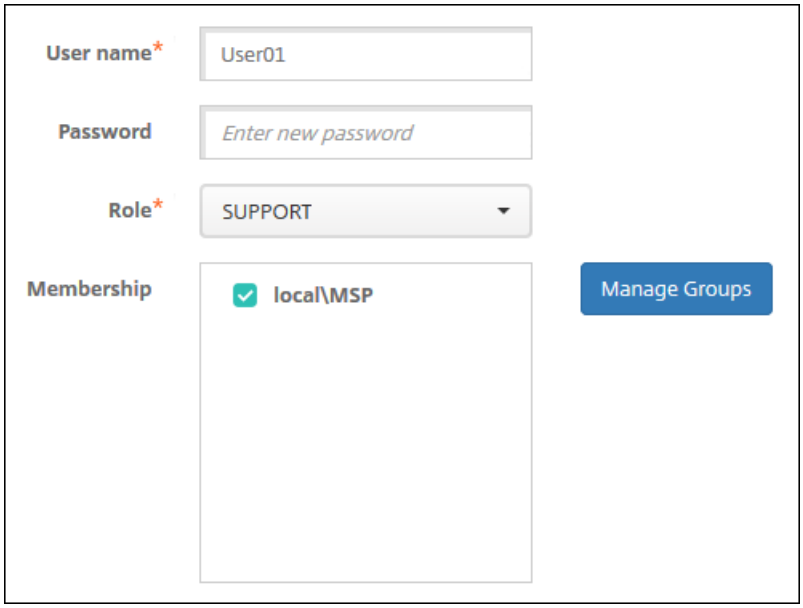
To add a local group

1. Do one of the following:

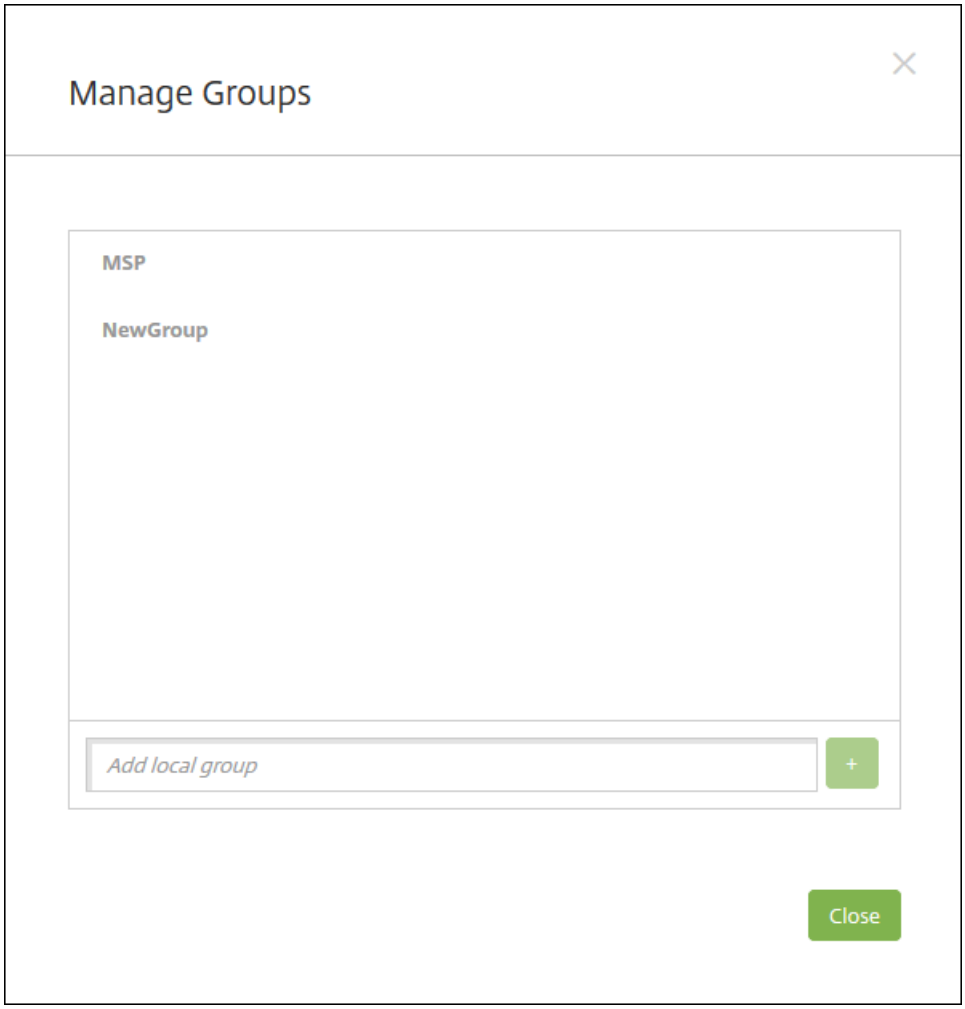
- On the **Users** page, click **Manage Local Groups**.



- 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**.

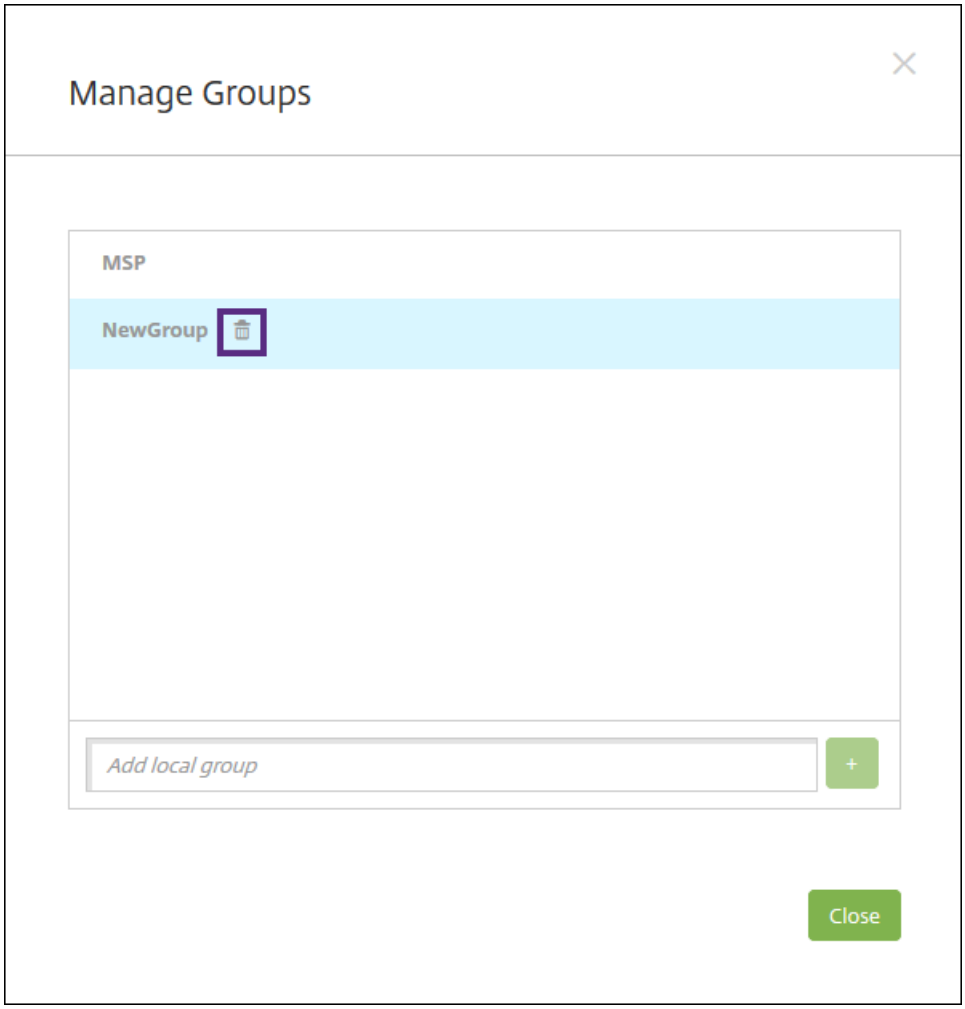
To remove a group

Note: Removing a group has no effect on user accounts. Removing a group simply removes the users' association with that group. Users also lose access to apps or profiles provided by the Delivery Groups that are associated with that group; any other group associations, however, remain intact. If users are not associated with any other local groups, they are associated at the top level.

1. Do one of the following:

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

The **Manage Groups** dialog box appears.



2. On the **Manage Groups** dialog box, click the group you want to delete.

3. Click the trash can icon to the right of the group name. A confirmation dialog box appears.

4. Click **Delete** to confirm the operation and remove the group.

   Important: You cannot undo this operation.

5. On the **Manage Groups** dialog box, click **Close**.

Configuring Roles with RBAC

Sep 16, 2016

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.

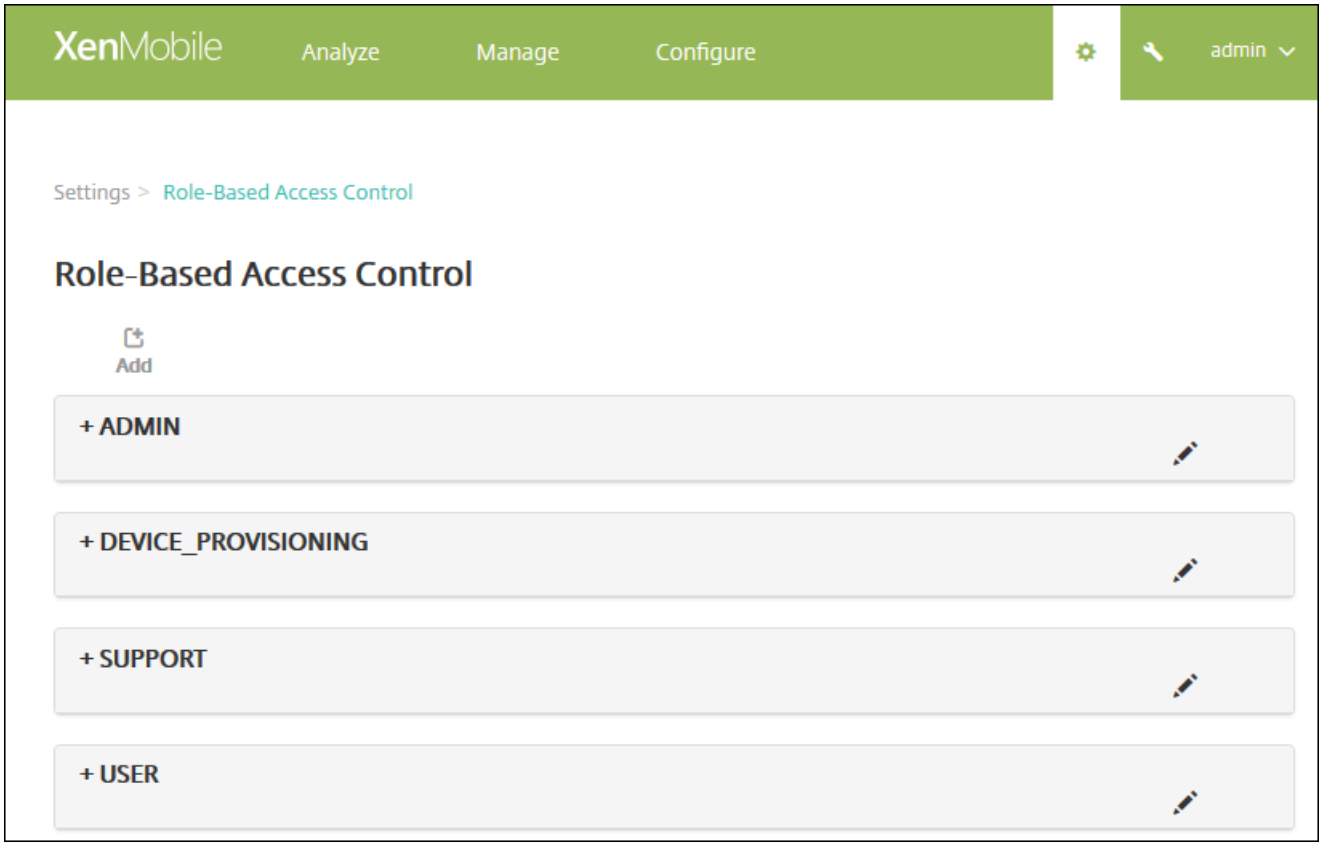
Note: Local users may have only one role assigned to them.

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.

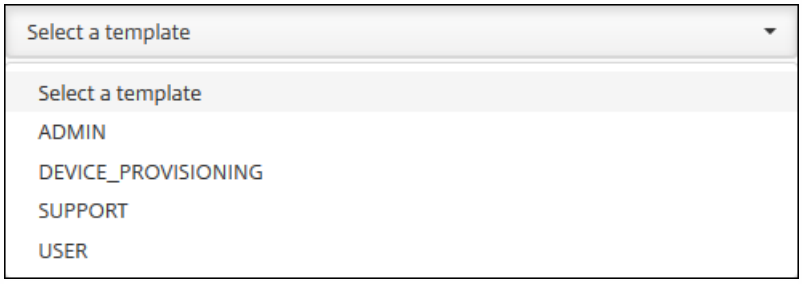
3. Click **Add** to add a new user role, click the pen icon to the right of an existing role to edit the role, or click the trash can icon to the right of a role you previously defined to delete the role. You cannot delete the default user roles.

- 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.

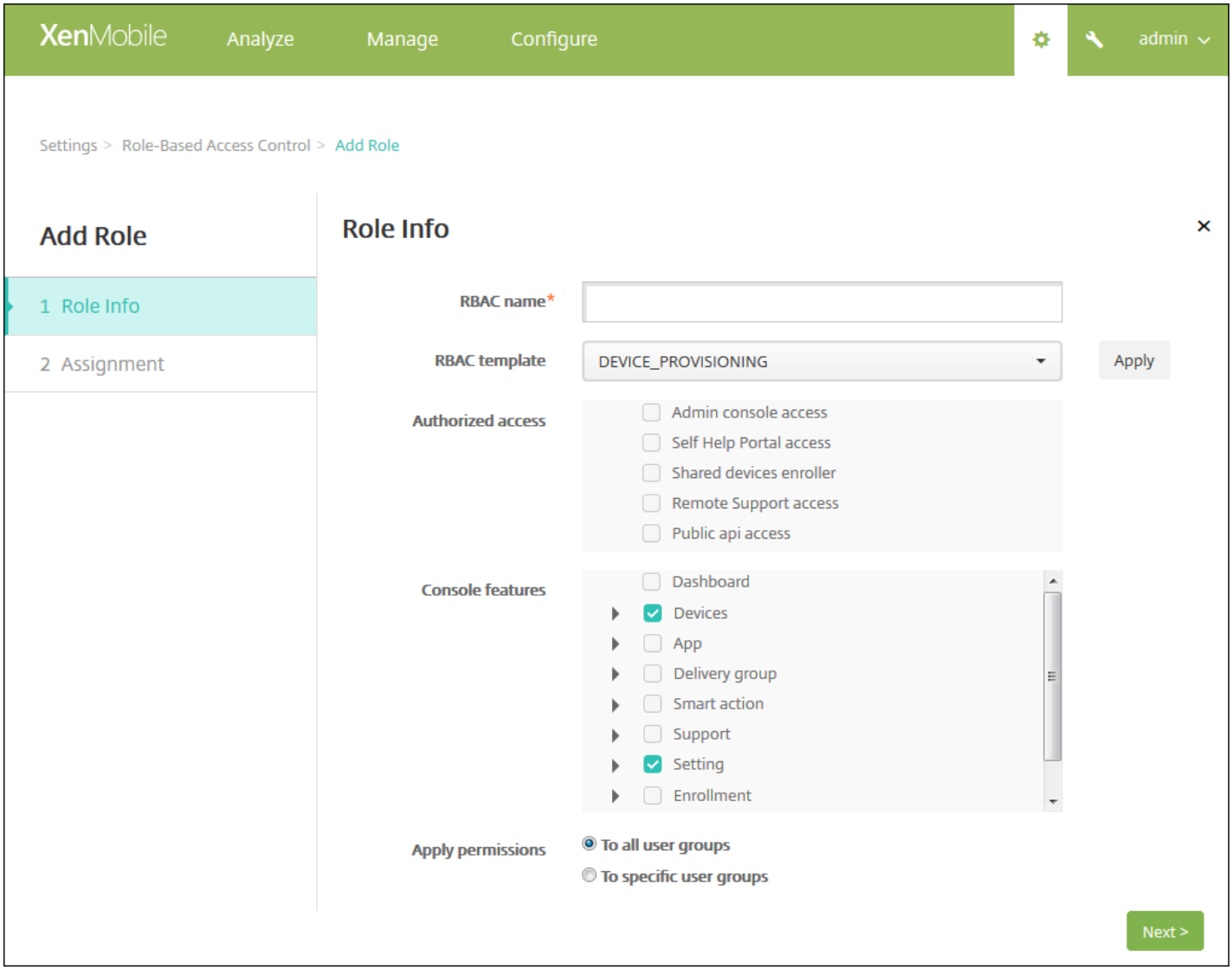
4. Enter the following information to create a new user role or to edit an existing user role:

- **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.

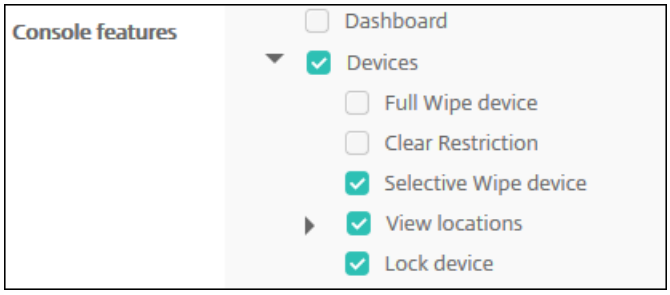


5. Click **Apply** to the right of the **RBAC template** field to populate the **Authorized access** and **Console features** check boxes with the pre-defined access and feature permissions for the selected template.

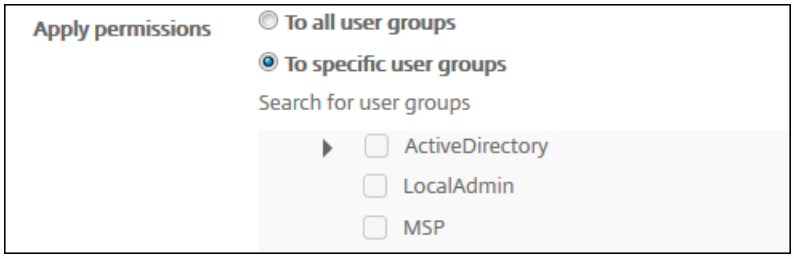


6. Select and clear the check boxes in **Authorized access** and **Console features** to customize the role.

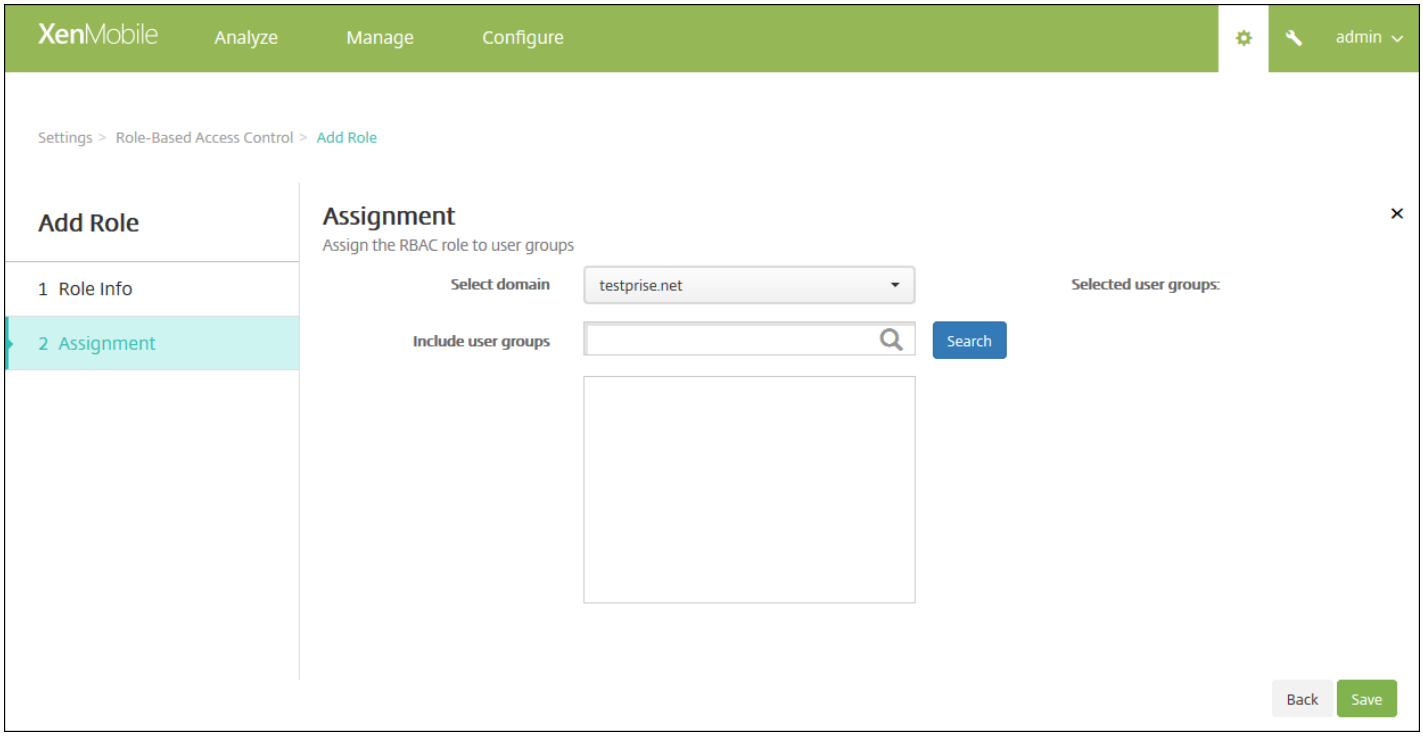
If you click the triangle next to a Console feature, permissions specific to that feature appear that you can select and clear. Clicking the top-level check box prohibits access to that console part; you must select individual options below the top level to enable those options. For example, in the following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

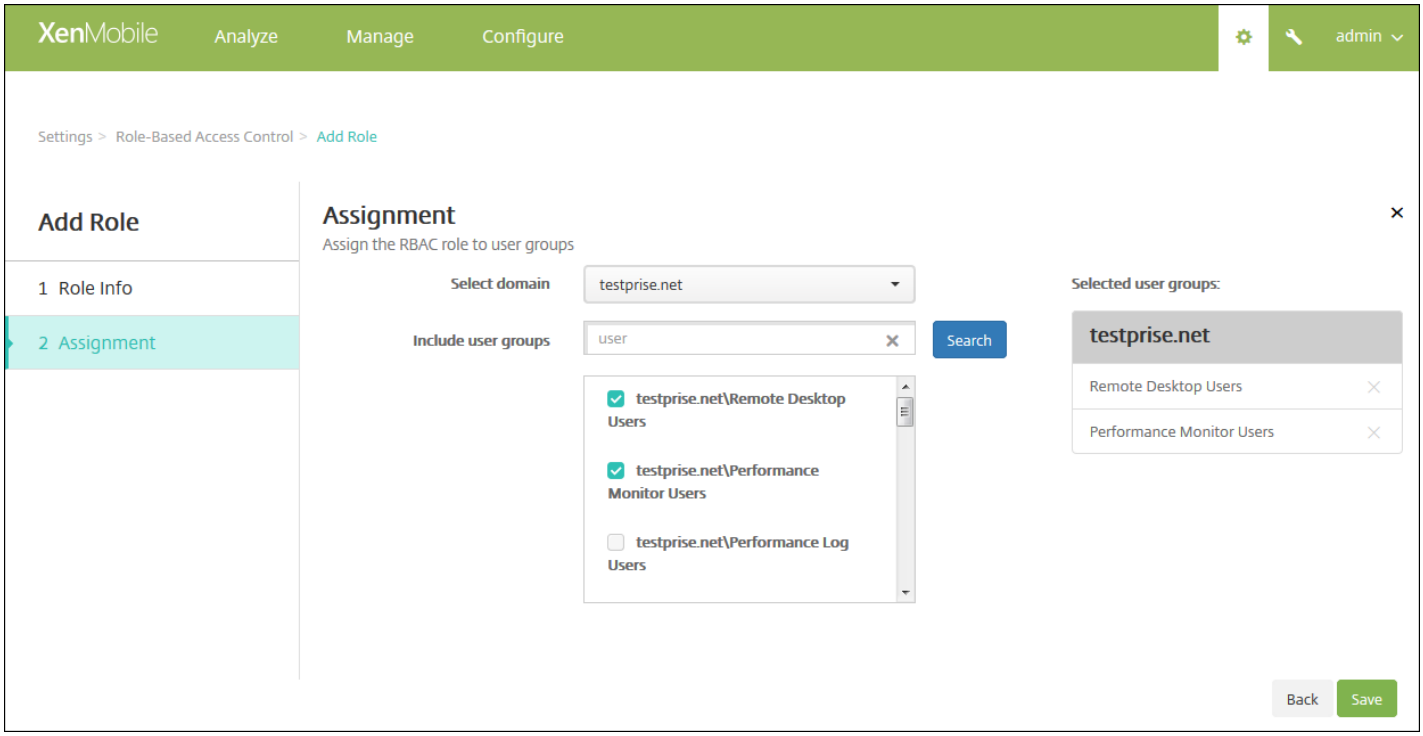


8. Click **Next**. The **Assignment** page appears.



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**.

RBAC Roles and Permissions

Jan 04, 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.

For more information on how to configure RBAC roles, see Configuring Roles with RBAC.

> **Note**
>
> Starting with version 10.4, Worx Mobile Apps are renamed XenMobile Apps. Most of the individual apps are renamed as well. For details, see About XenMobile Apps.

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

To configure enrollment modes and enable the Self Help Portal

Jan 04, 2016

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, 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 in the XenMobile console from the **Manage > Enrollment** page (see Enrolling Users and Devices in XenMobile).

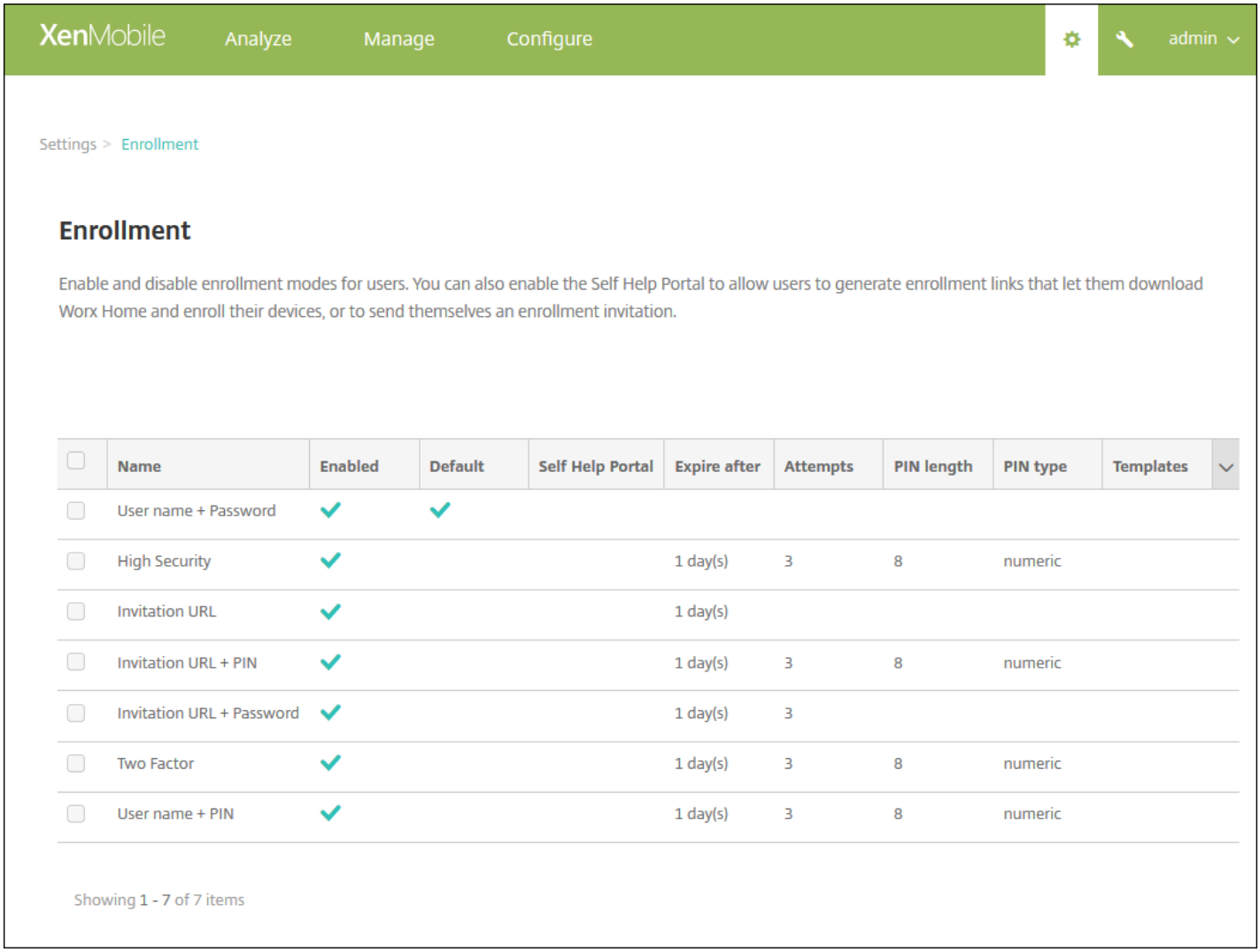
Note: If you plan to use custom notification templates, you must set up the templates before you configure enrollment modes. For more information about notification templates, see Creating or Updating Notification Templates.

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.

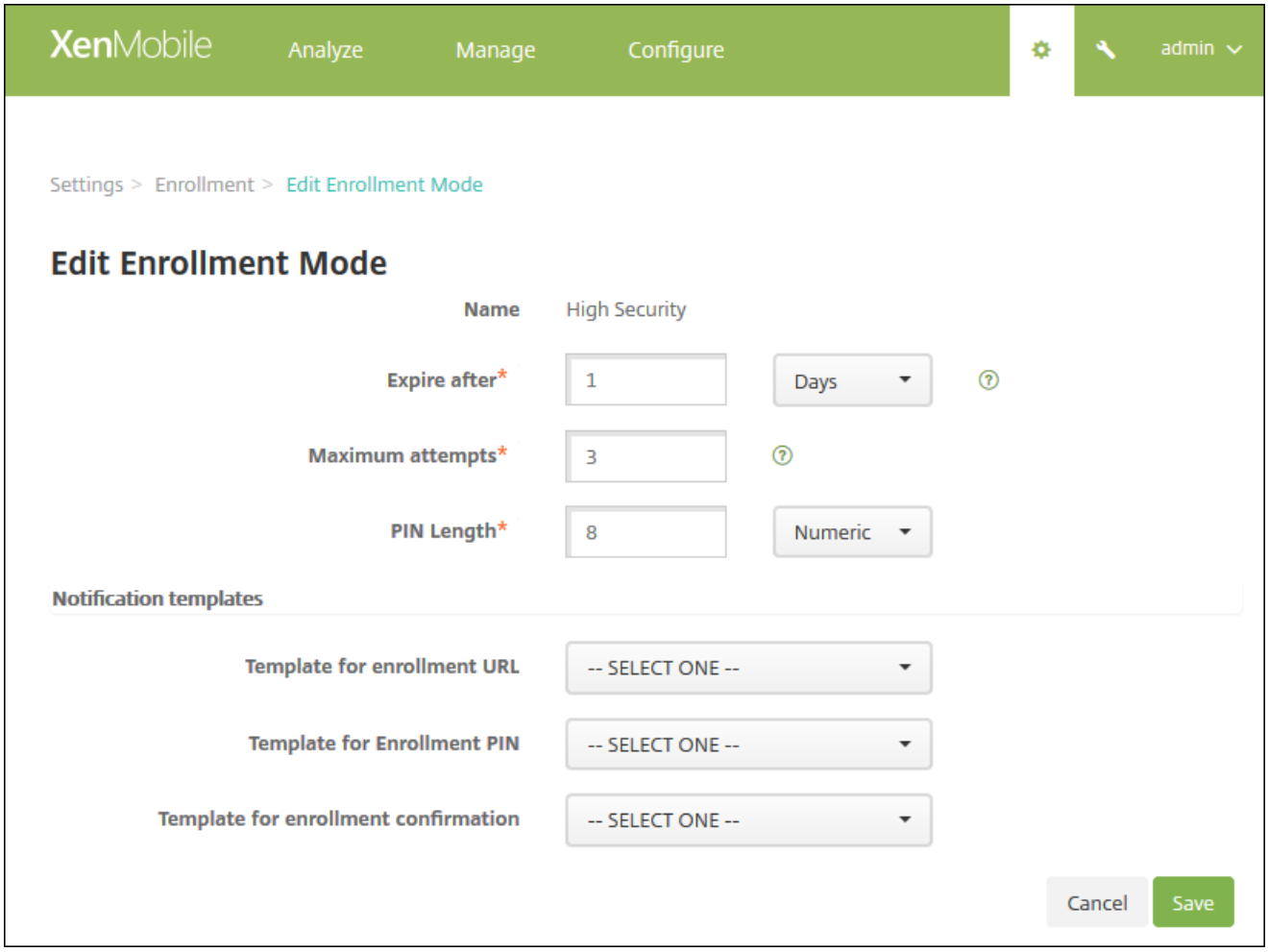
3. Select any enrollment mode in the list to edit and then set the mode as the default, delete the mode, or allow users access through the Self Help Portal.

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 will contain.
- **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 the 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: Only **Username + Password**, **Two Factor**, or **Username + PIN** can be set 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.

Enable autodiscovery in XenMobile for user enrollment

Jun 30, 2016

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. For more about the Autodiscovery Service portal, see the topic on XenMobile Autodiscovery Service.

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).

Creating and Updating Notification Templates

Jan 06, 2017

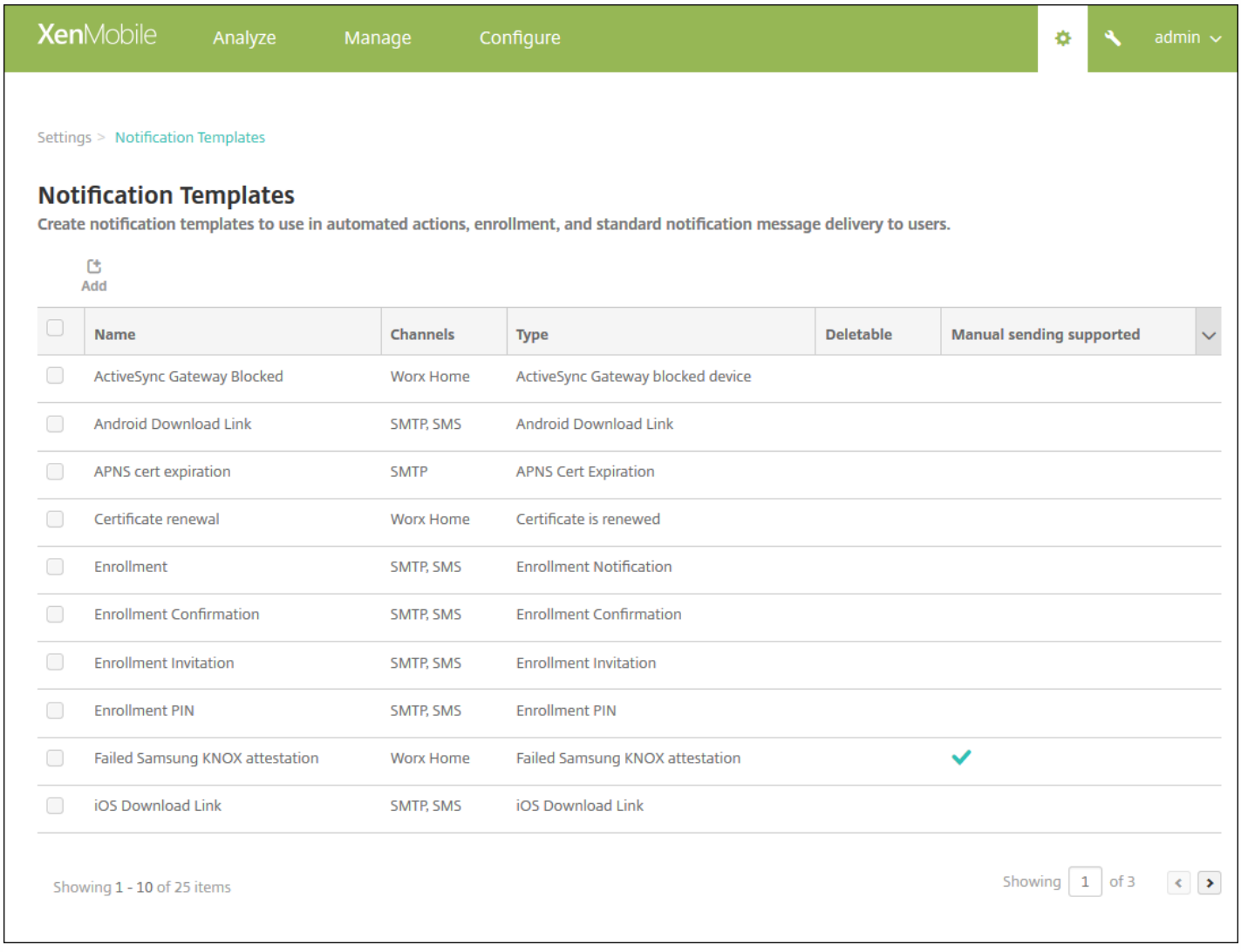
You can create or update notification templates in XenMobile to be used in automated actions, enrollment, and standard notification messages sent to users. You configure the notification templates to send messages over three different channels: Worx Home, SMTP, or SMS. **Note**: Starting with version 10.4, Worx Home is renamed Secure Hub.

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. For details, see Notifications in XenMobile.

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. The **Add Notification Template** page appears.

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 **Worx Home**, 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.

Worx Home:

- **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 Worx Home.
- **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 admin), 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 Adding Devices and Viewing Device Details in XenMobile.
- **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 Worx Home. 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.

Managing Delivery Groups

Jan 06, 2017

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.

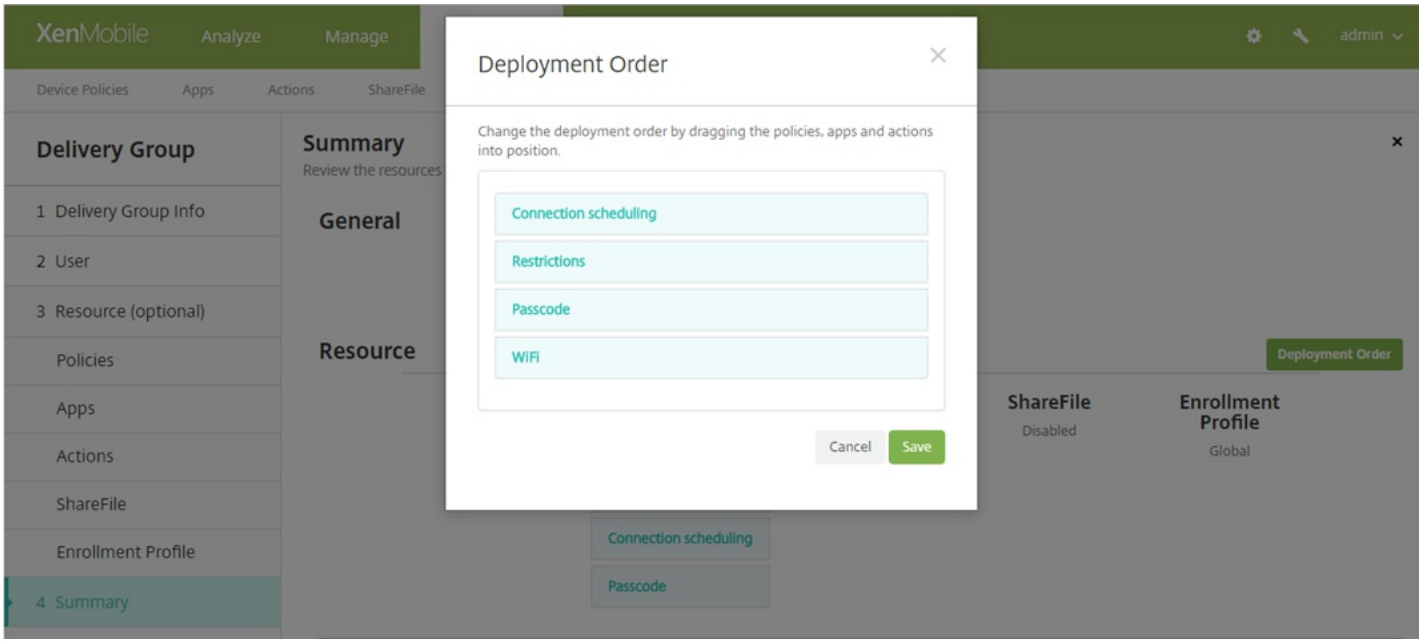
    c. While sorting, if a user-defined deployment order is specified for resources of a delivery group, maintain that order. Otherwise, sort the resources within that delivery group by resource name.

    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.

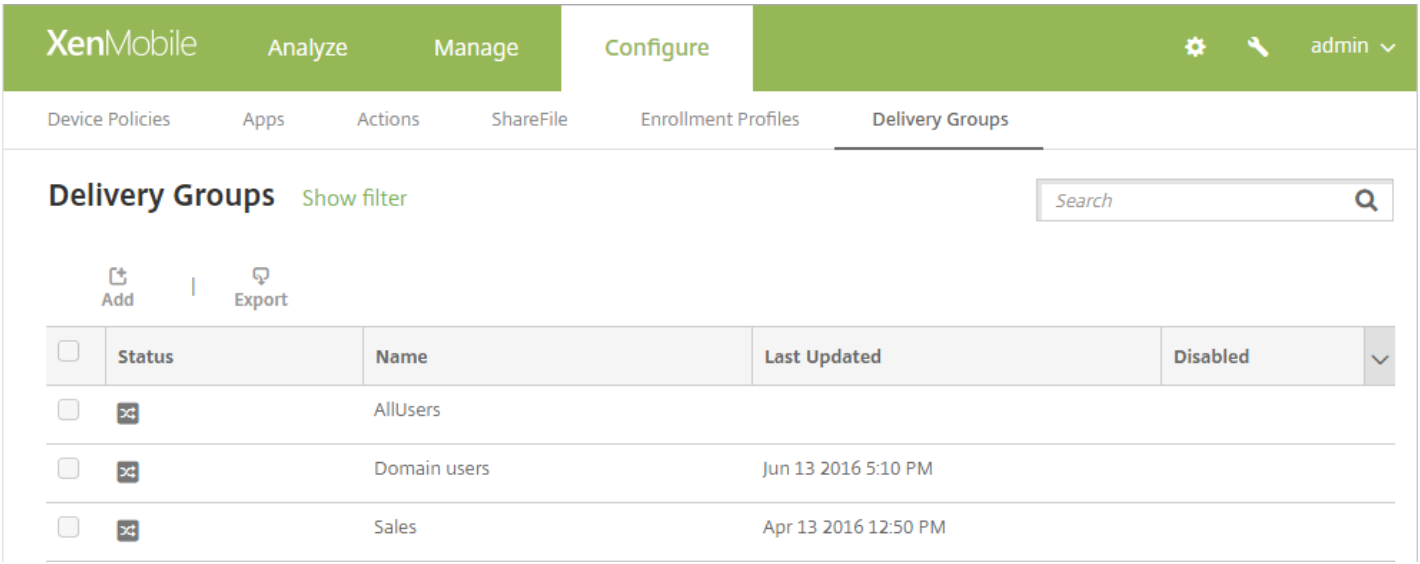


If the calculation algorithm ordered deployment groups only by name, XenMobile would perform the deployment in this order, starting with the delivery group Account Managers 1: **WiFi**, **Passcode**, **Connection scheduling**, and **Restrictions**. XenMobile would ignore **Passcode** and **WiFi**, both duplicates, from the Account Managers 2 delivery group.

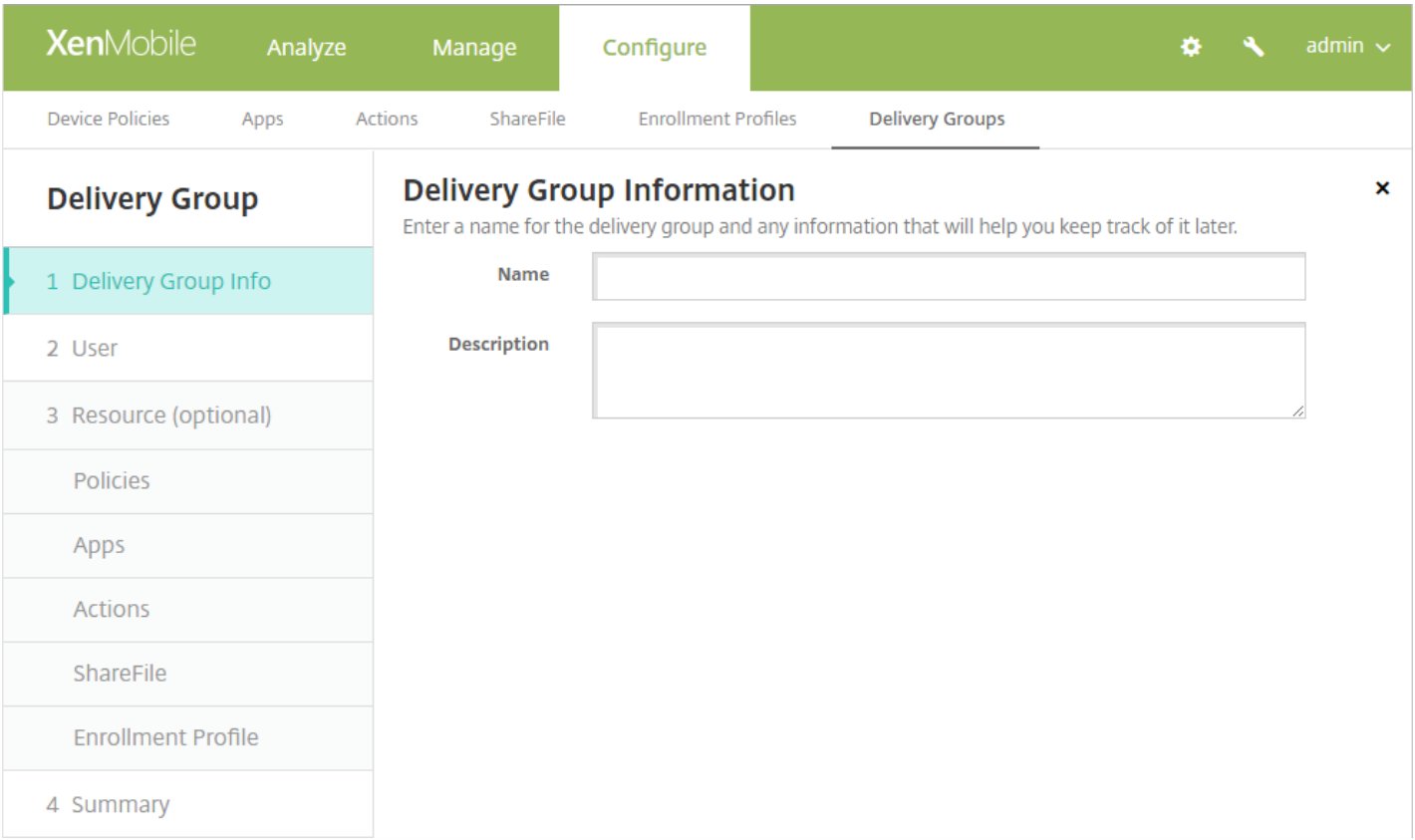
However, because the Account Managers 2 group has an admin-specified deployment order, the calculation algorithm places resources from the Account Managers 2 delivery group higher in the list over those from the Account Managers 1 delivery group. As a result, XenMobile deploys the policies in this order: **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.



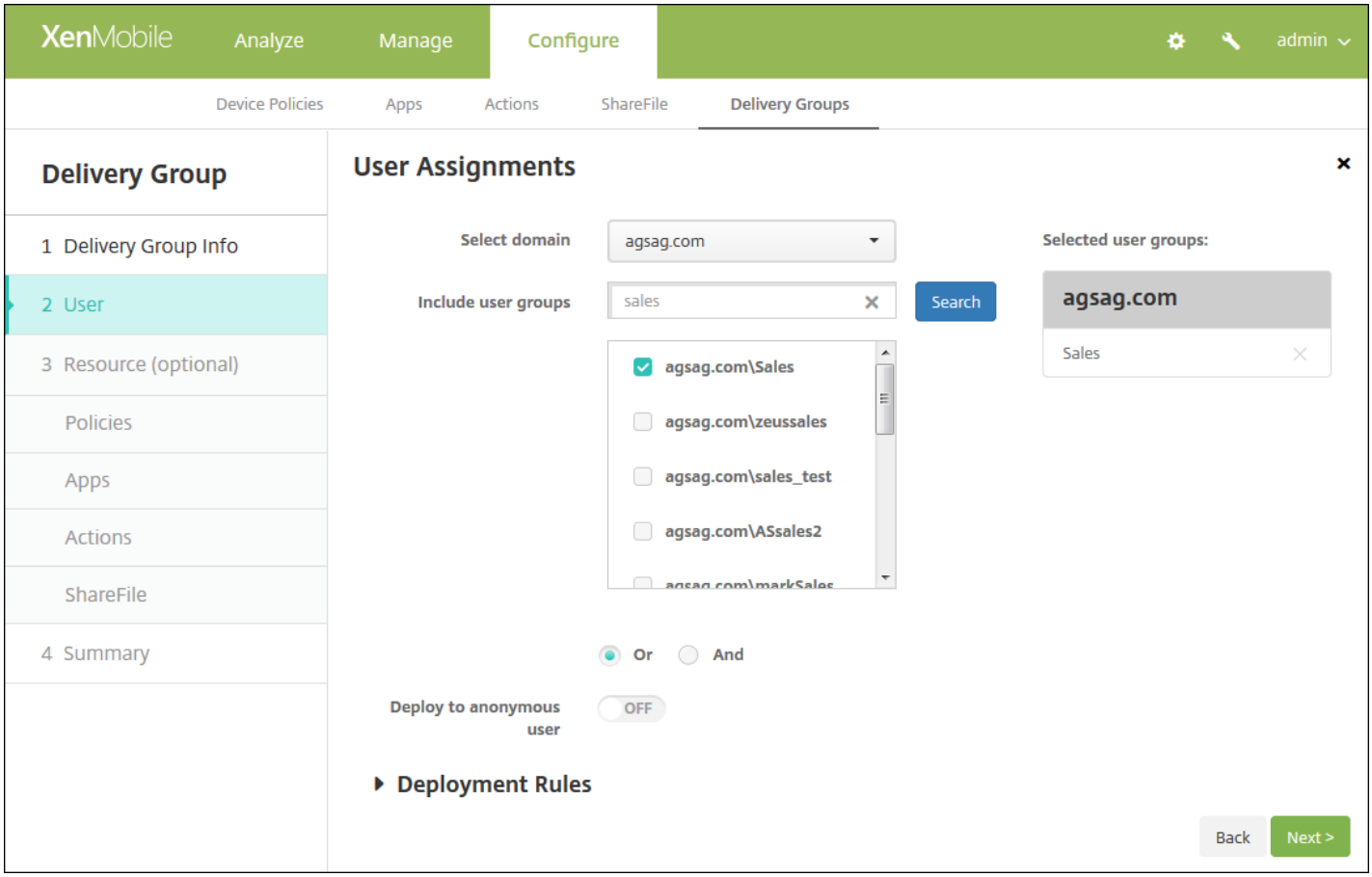
2. From the **Delivery Groups** page, click **Add**. The **Delivery Group Information** page appears.



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.

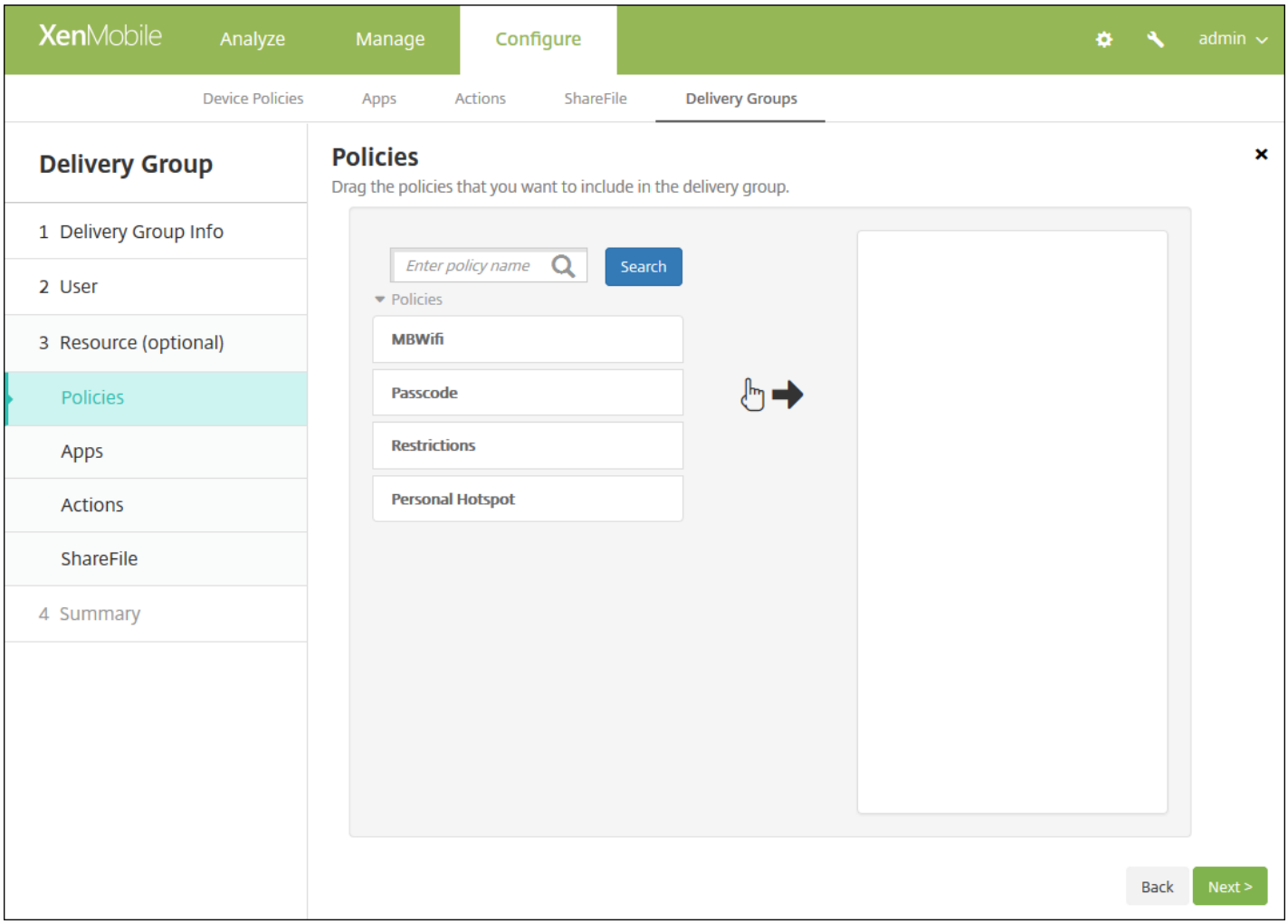
  Note: Unauthenticated users are users whom you were not able to authenticate, but you allowed their devices to connect to XenMobile anyway.

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 the resource you want to add or click **Summary** to skip adding any resource.

Add policies



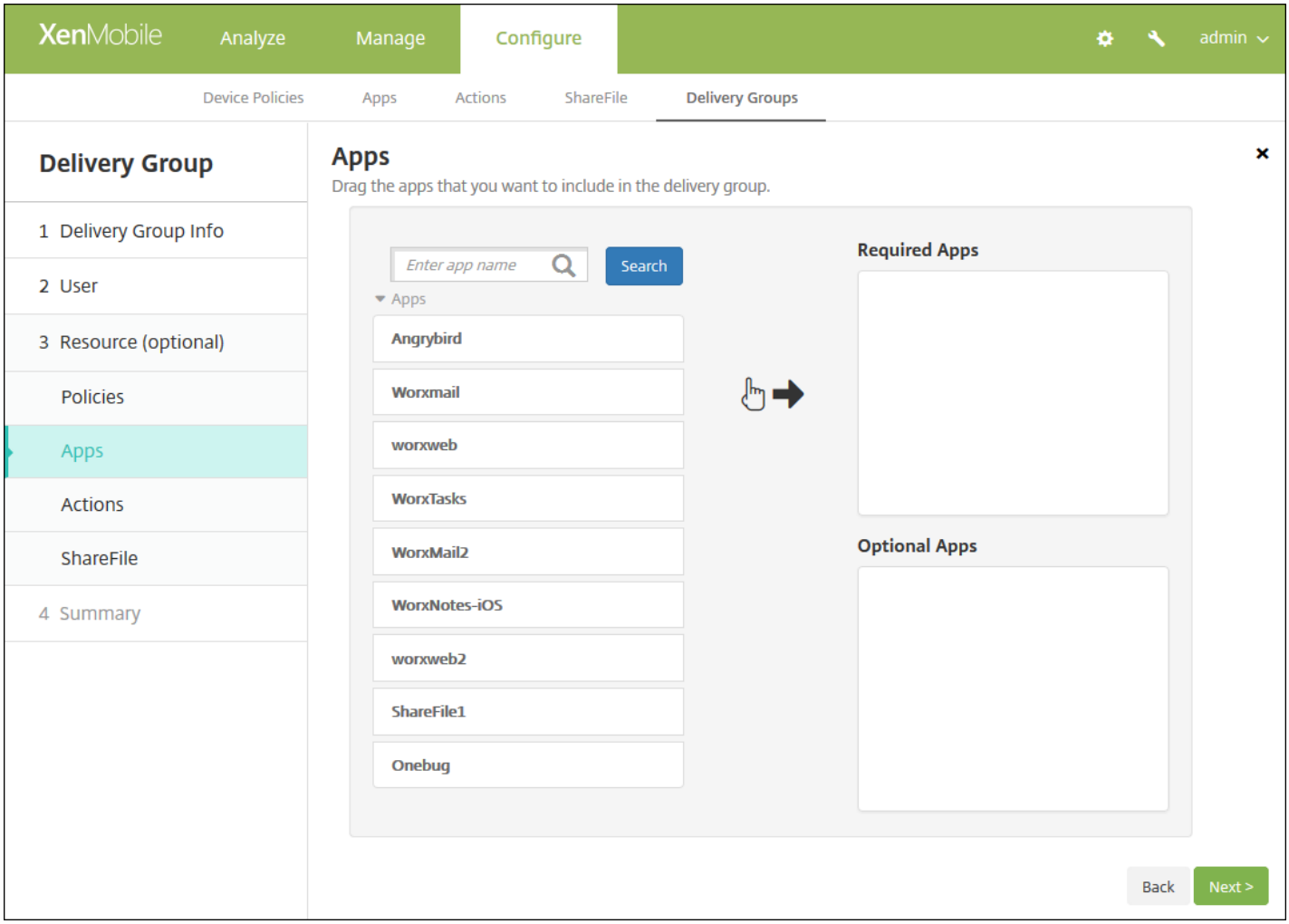
1. For each policy you want to add, do the following:

- 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



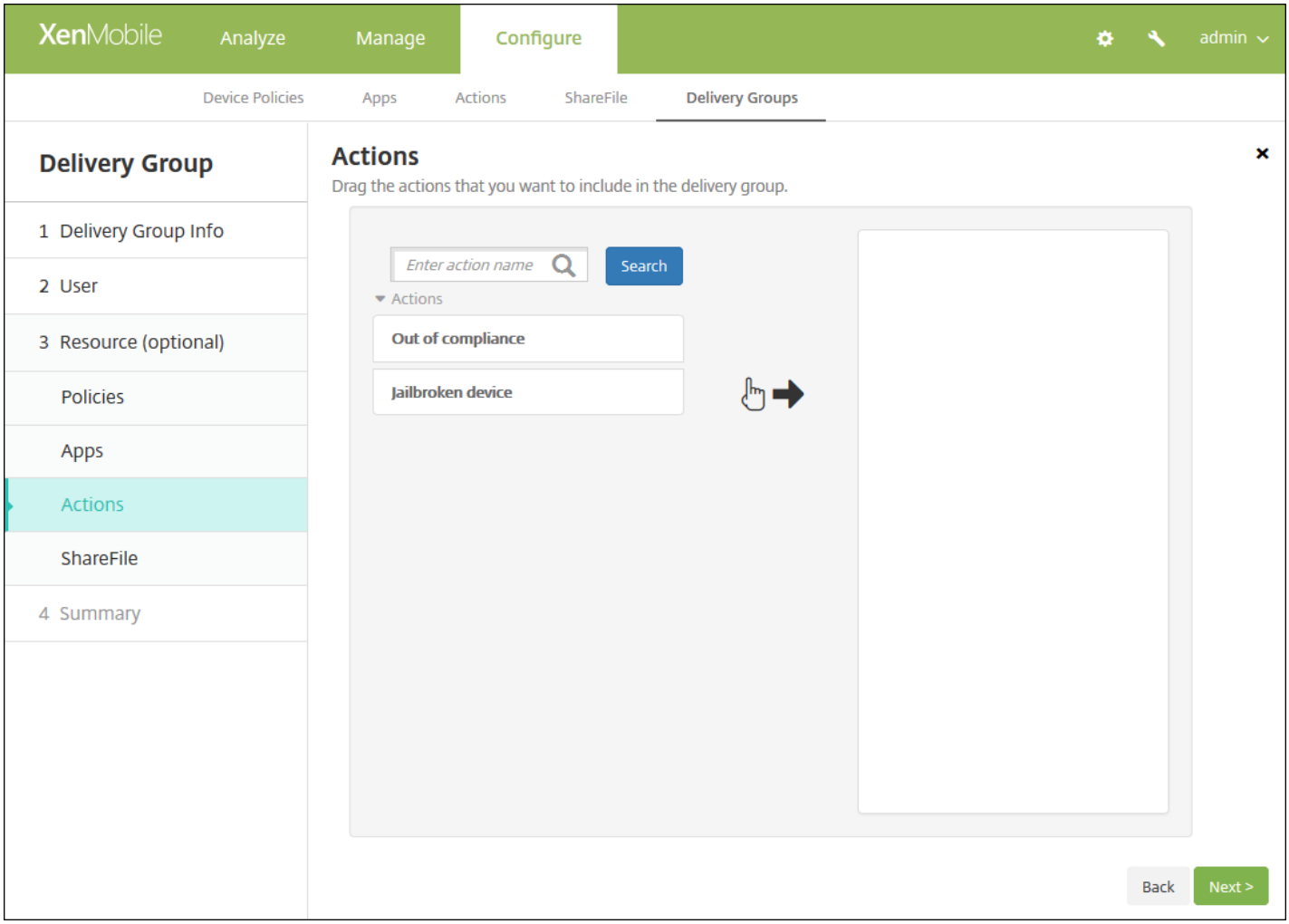
1. For each app you want to add, do the following:

- 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



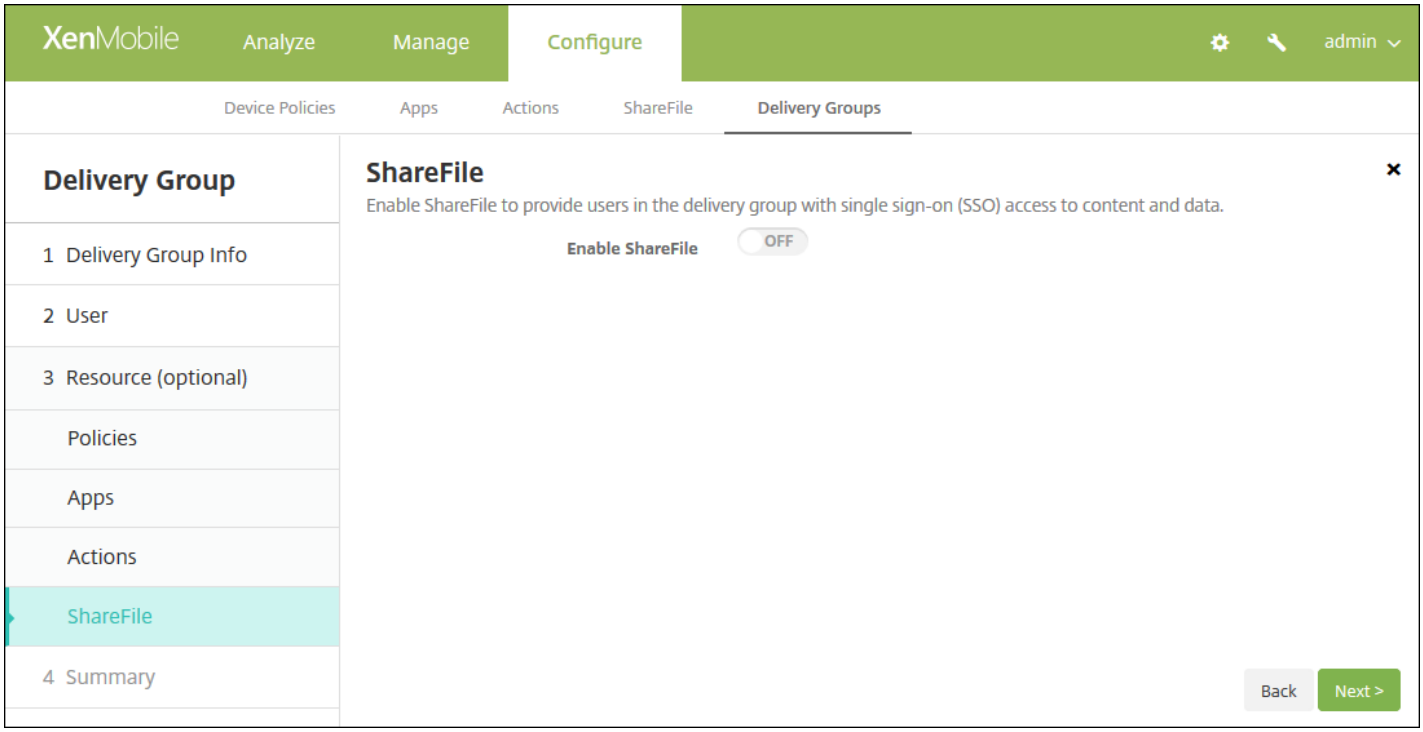
1. For each action you want to add, do the following:

- 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

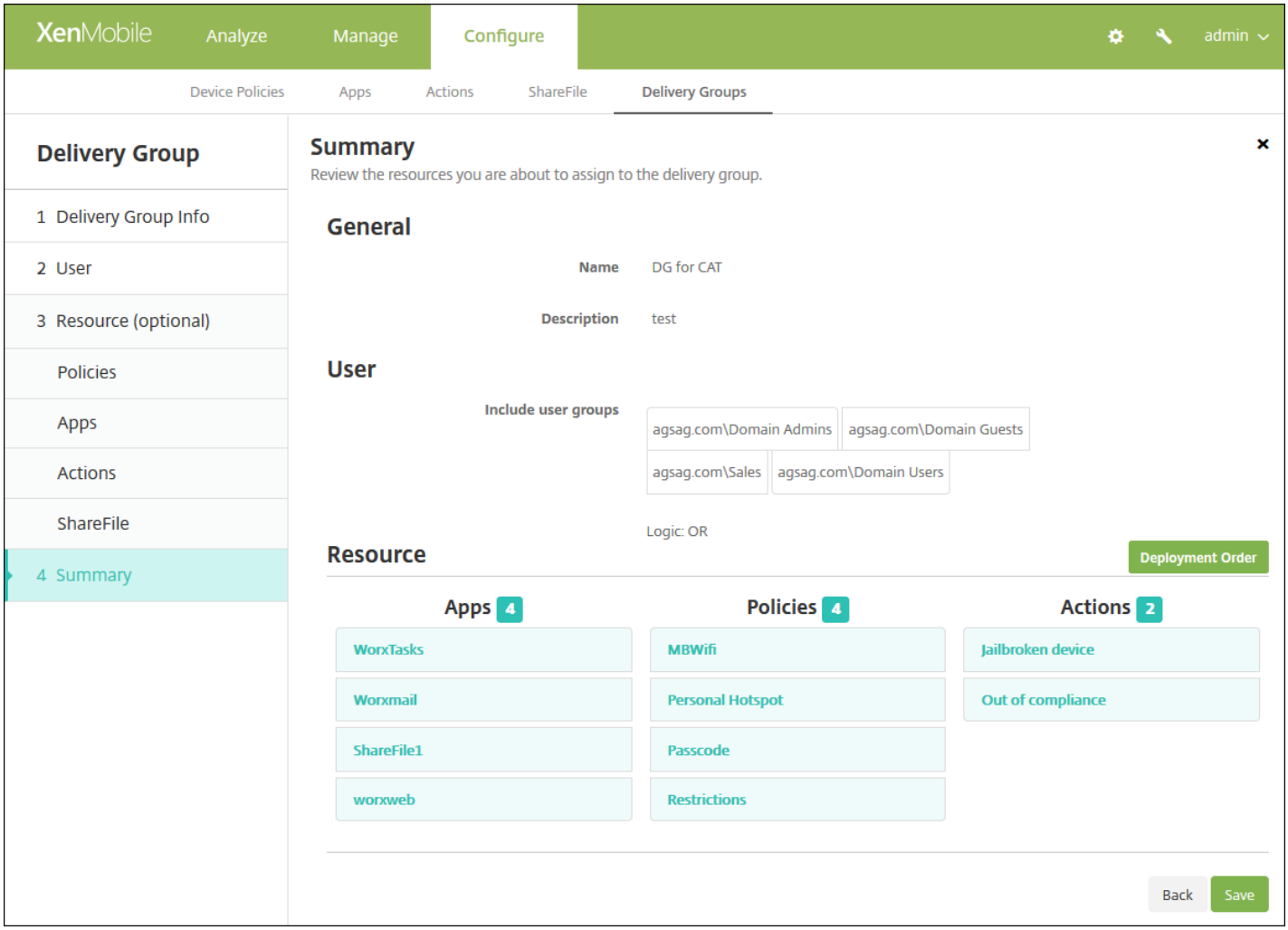


1. Configure this setting:

- **Enable ShareFile**: Click **ON**, to enable ShareFile single sign-on access to content and data.

2. Click **Next**. The **Summary** page appears.

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.

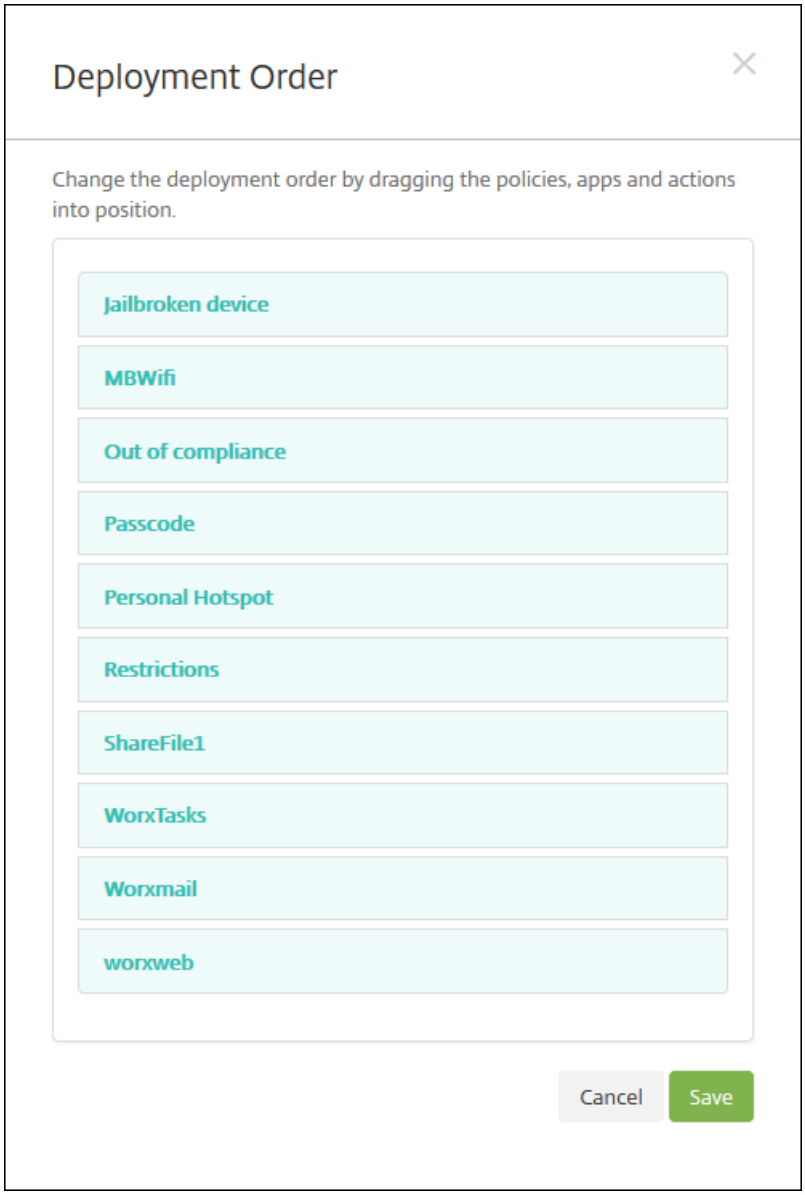
1. Click **Back** to return to previous pages to make any necessary adjustments to the configuration.

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

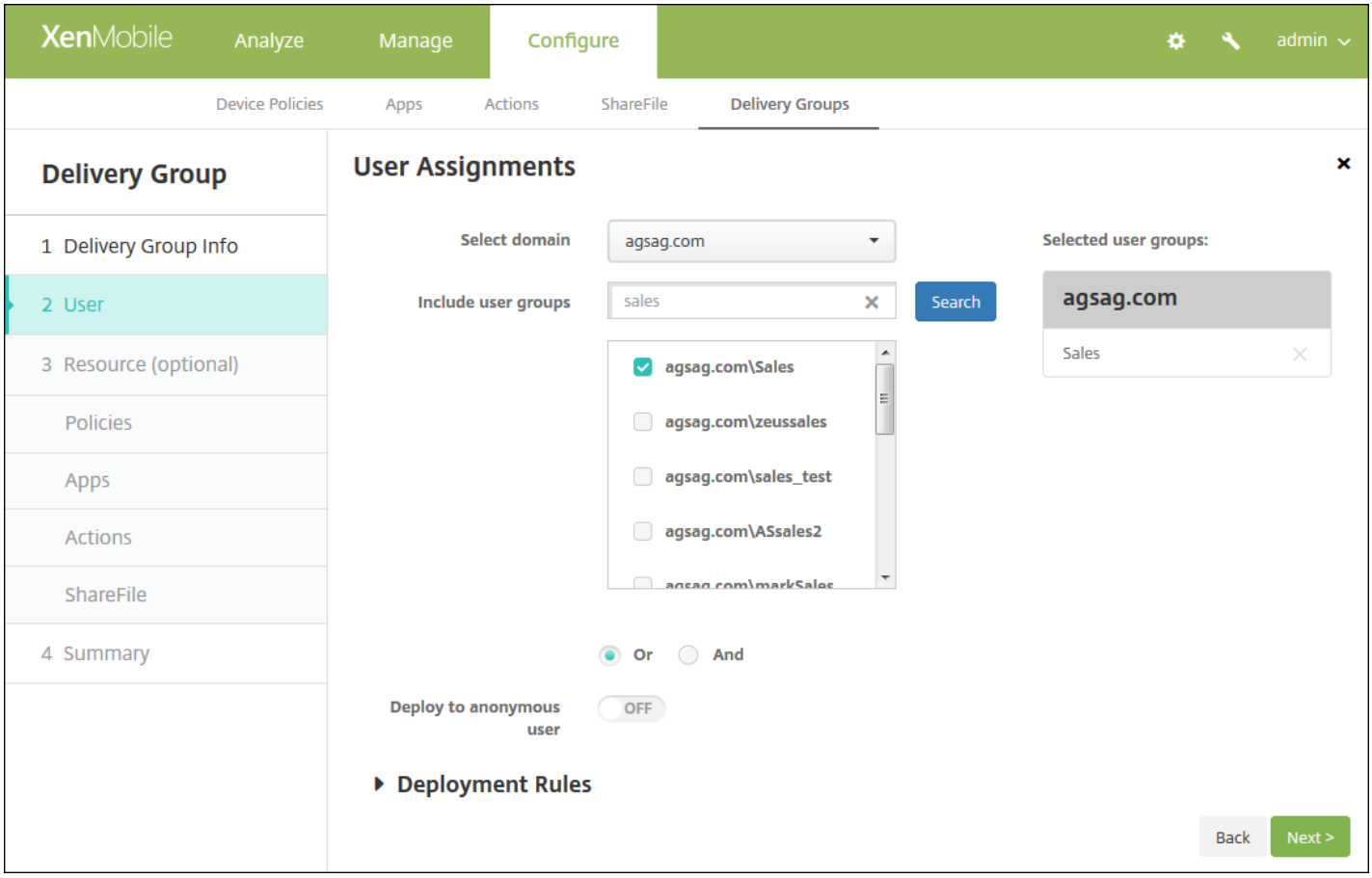
1. On the **Delivery Groups** page, choose the delivery group you want to edit by selecting the check box next to its name or by clicking in the line containing its name and then click **Edit**. The **Delivery Group Information** edit page appears.

> **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 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 Worx Store on users' Android devices, you must first deploy an App Inventory policy to the users' devices. Also please note that as of version 10.4, Worx Store is renamed XenMobile Store.

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**.

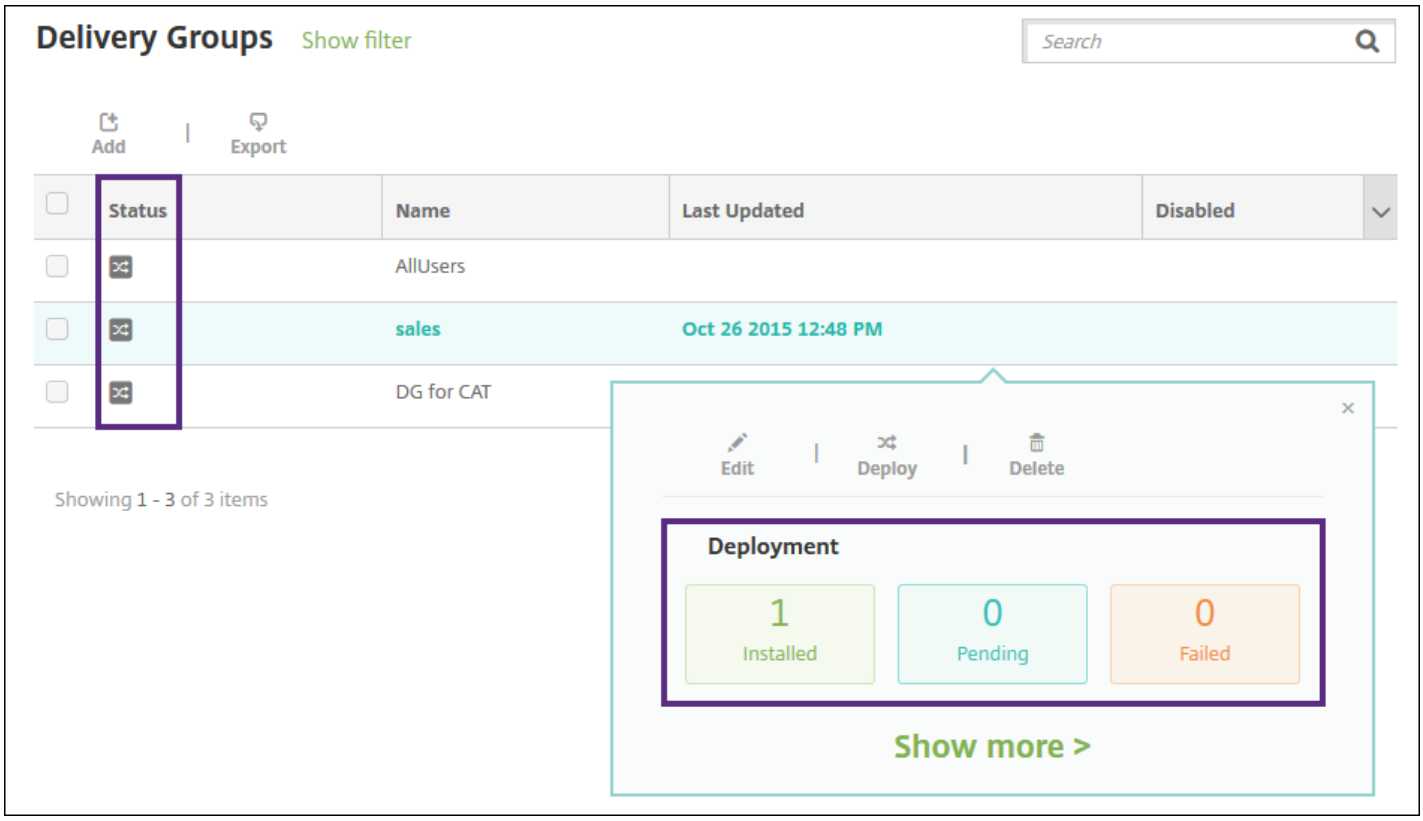
Note: Depending on how you select a single delivery group, the **Deploy** command appears above or to the right of the

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**.

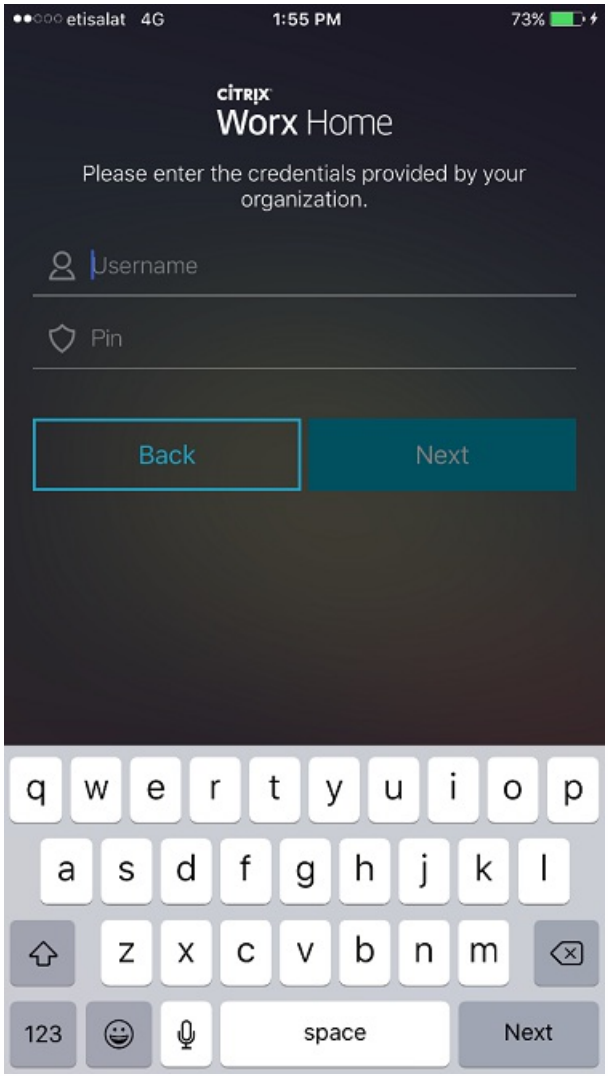
> **Important**
>
> You cannot undo this action.

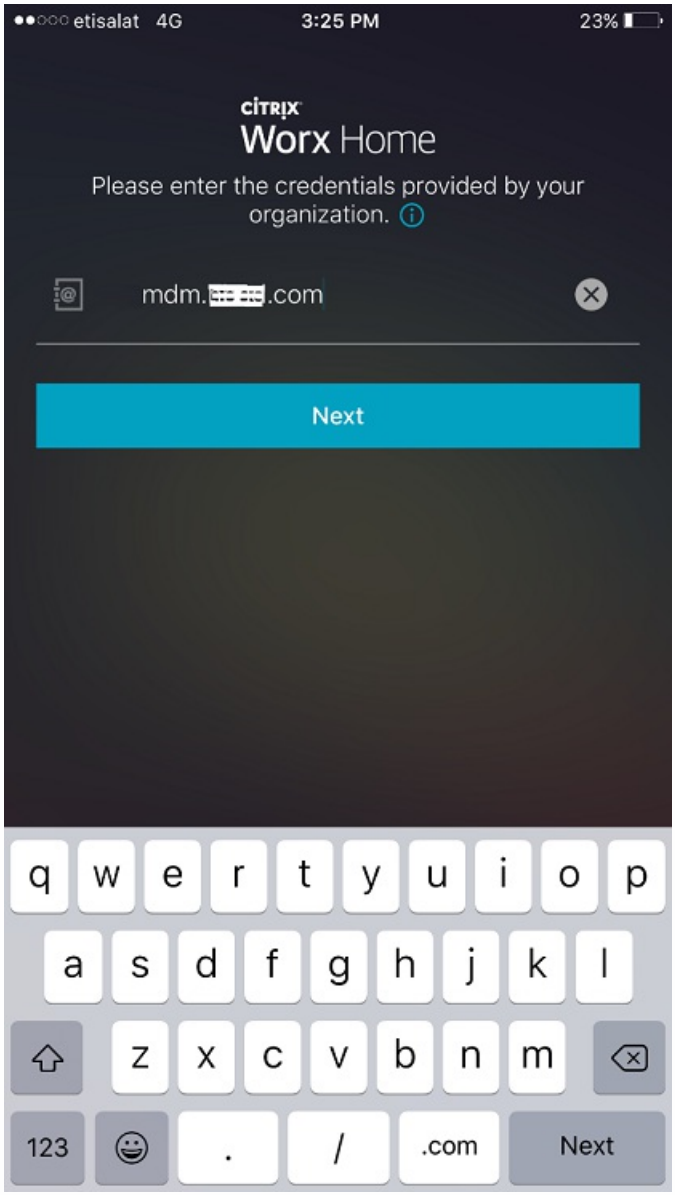
To export the Delivery Groups table

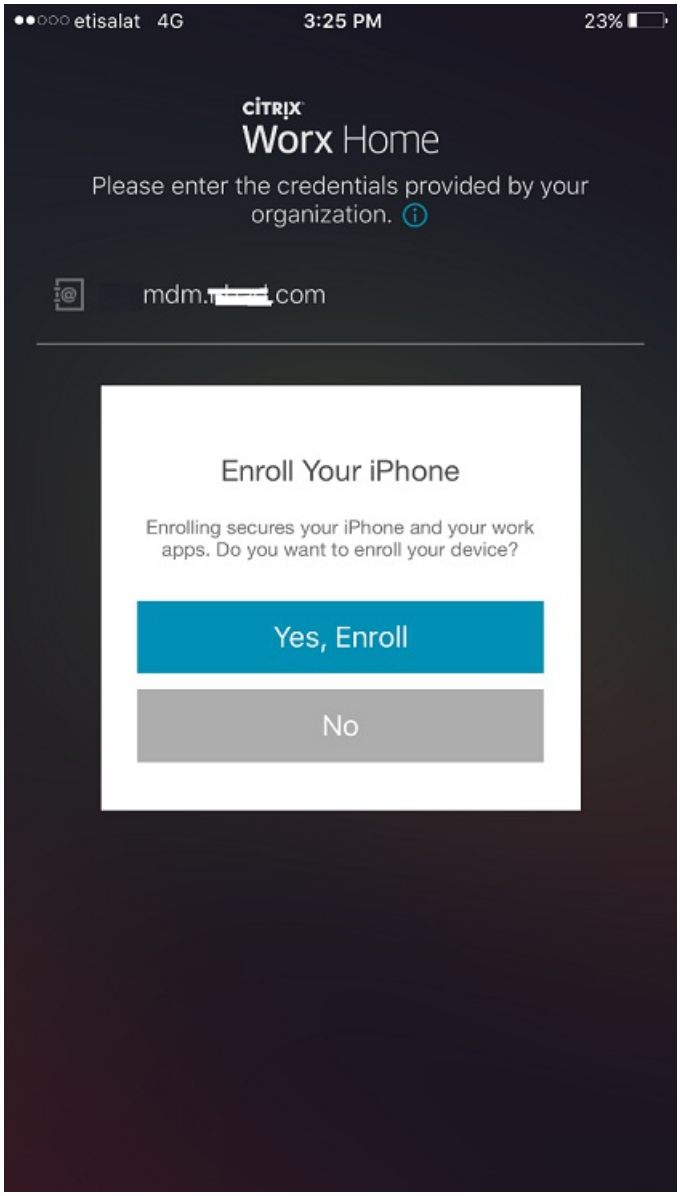
1. Click the **Export** button above the **Delivery Groups** table. XenMobile extracts the information in the **Delivery Groups** table and converts it to a .csv file.

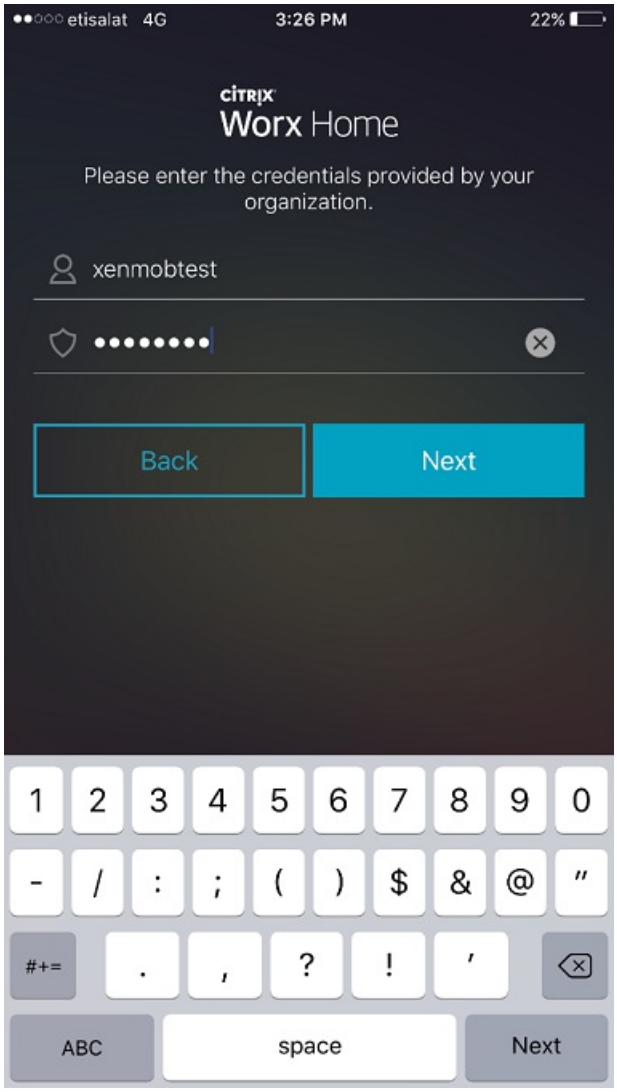
2. Open or save the .csv file. How you do this depends on the browser you are using. You can also cancel the operation.

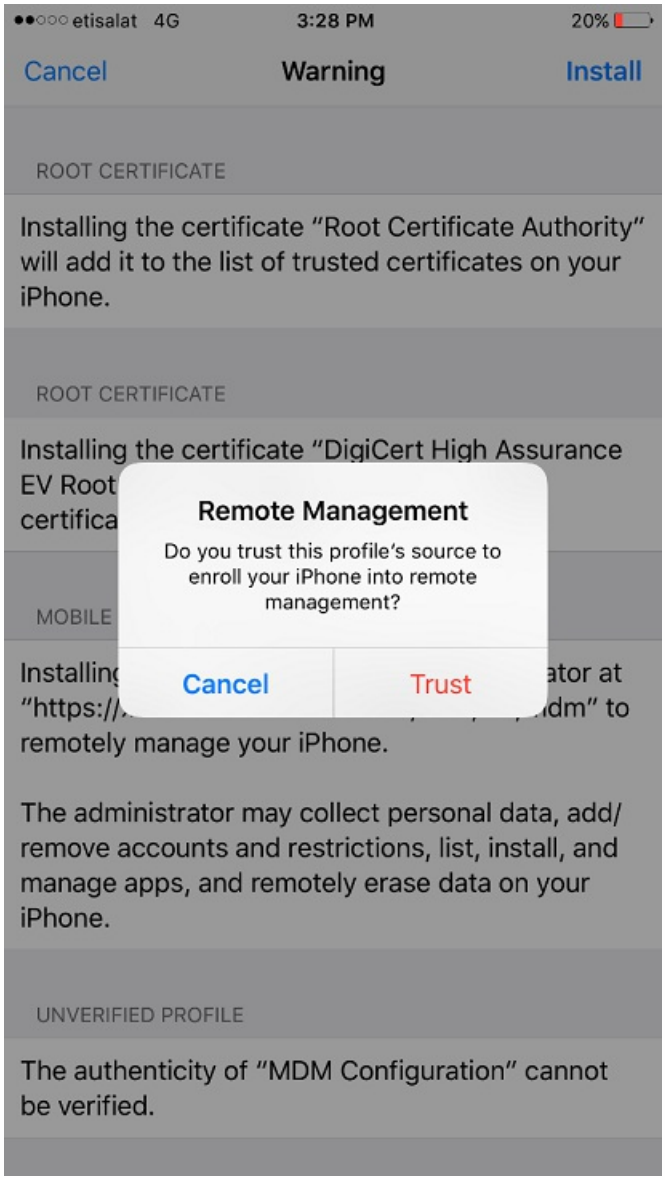
To un-enroll and re-enroll an Android device

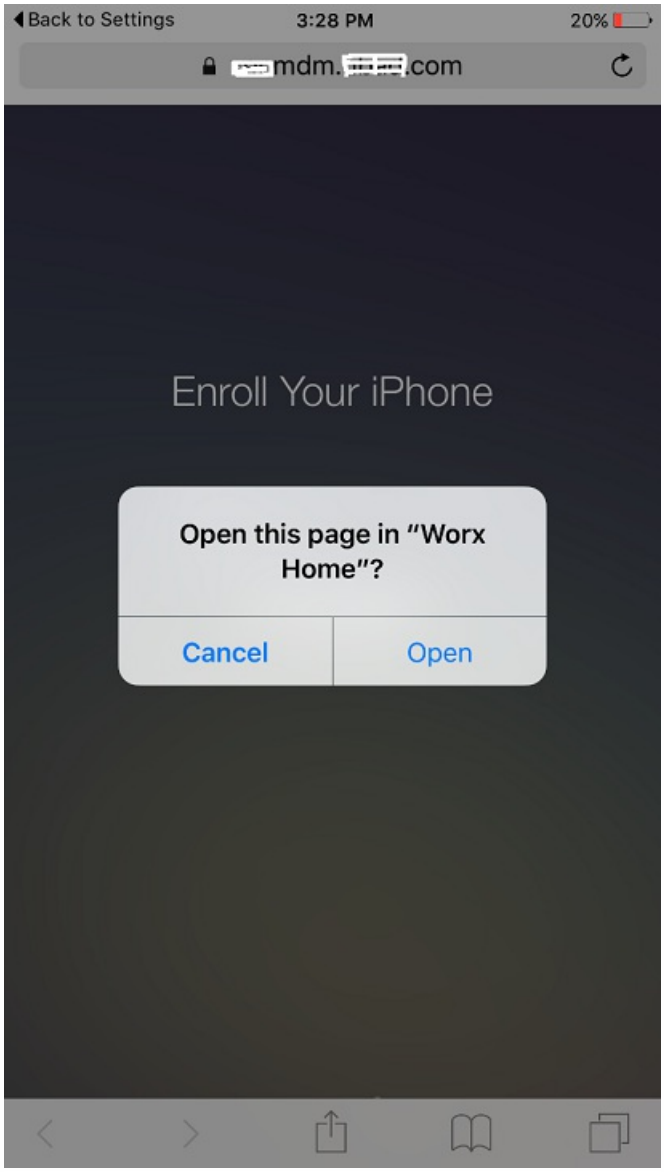


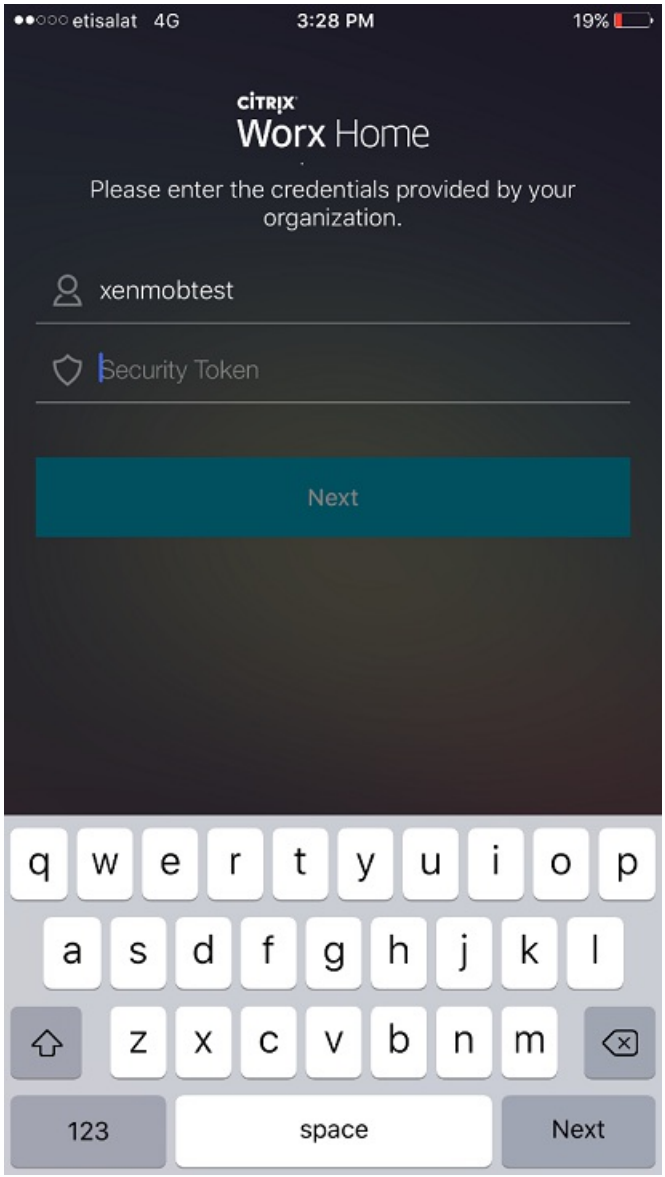




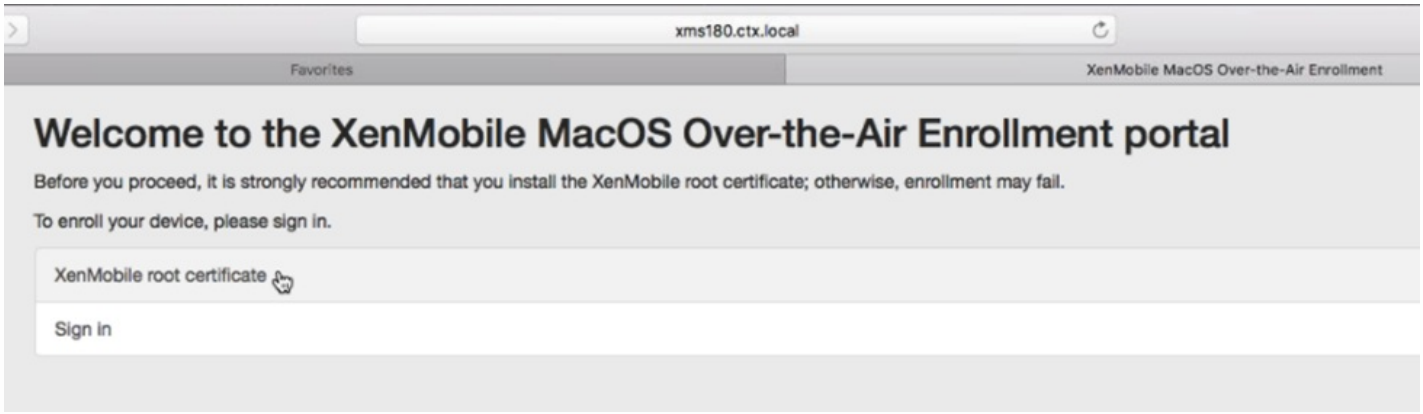


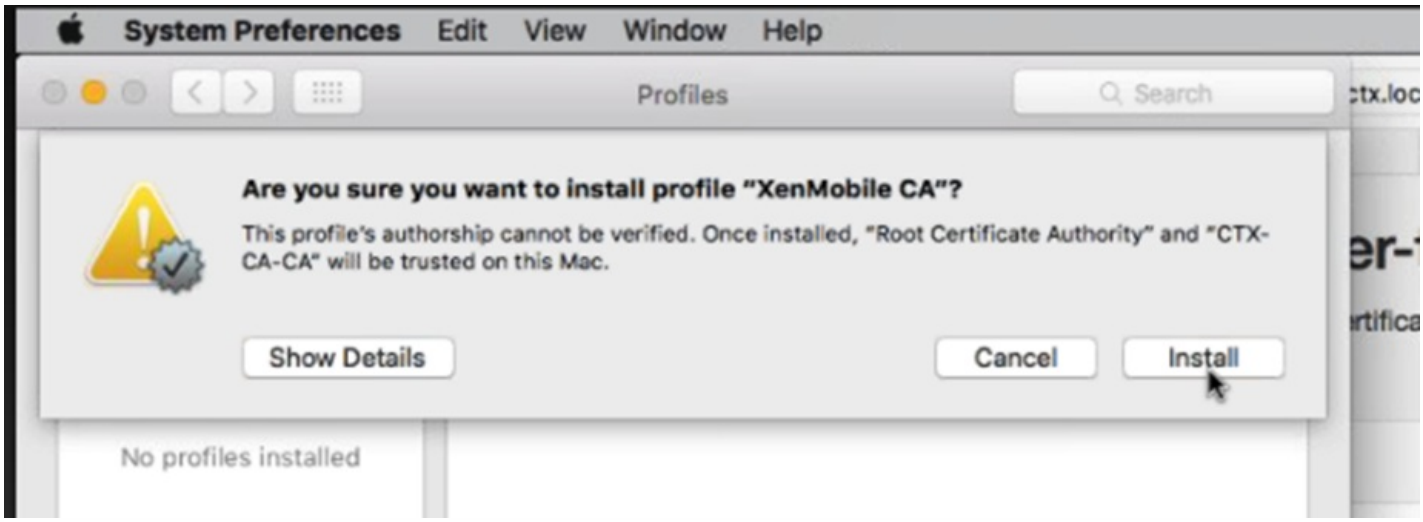


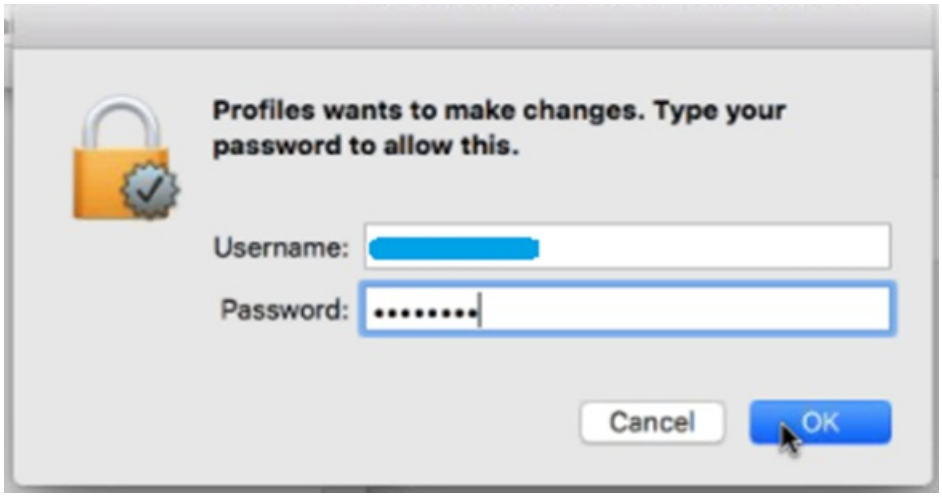


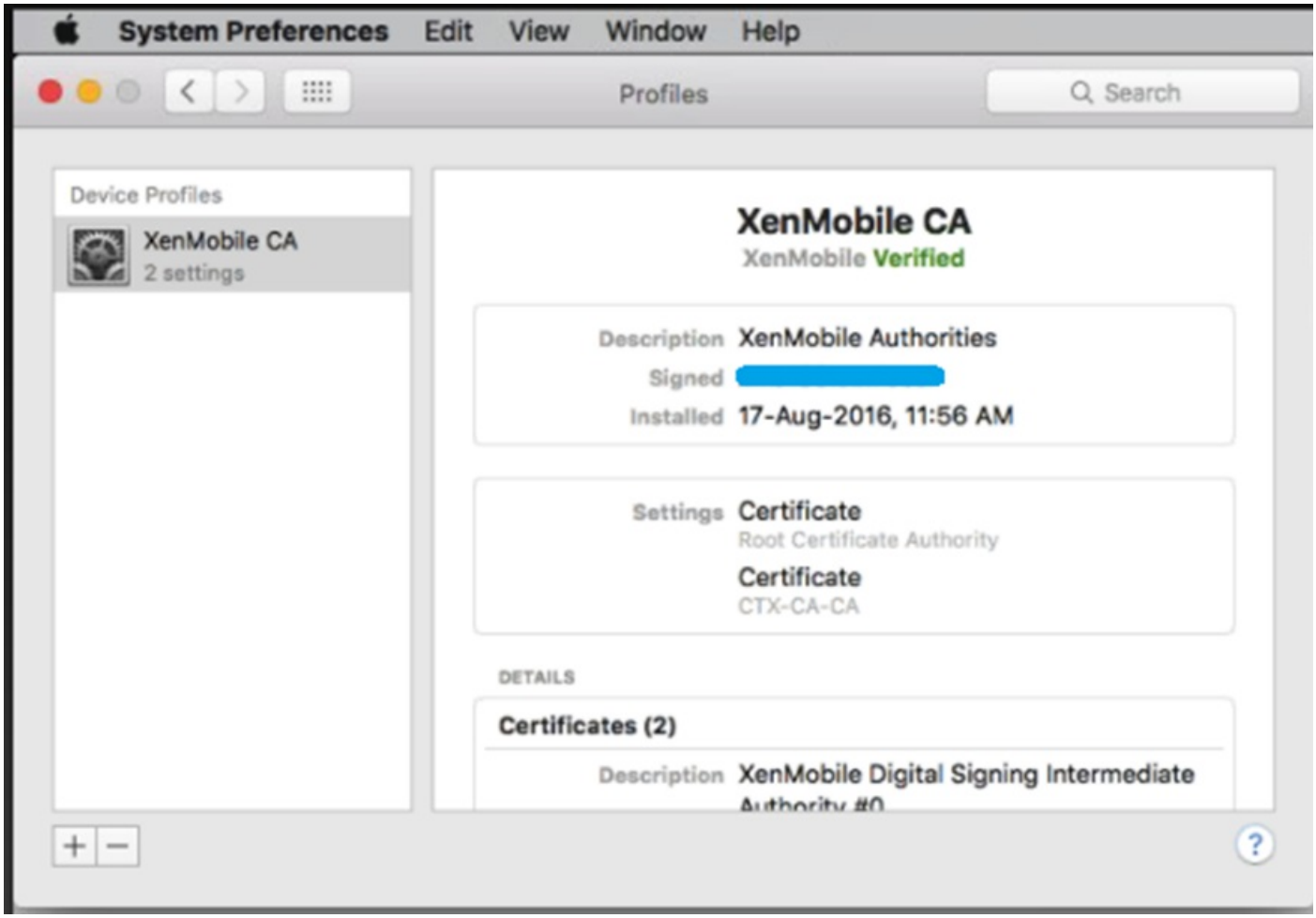


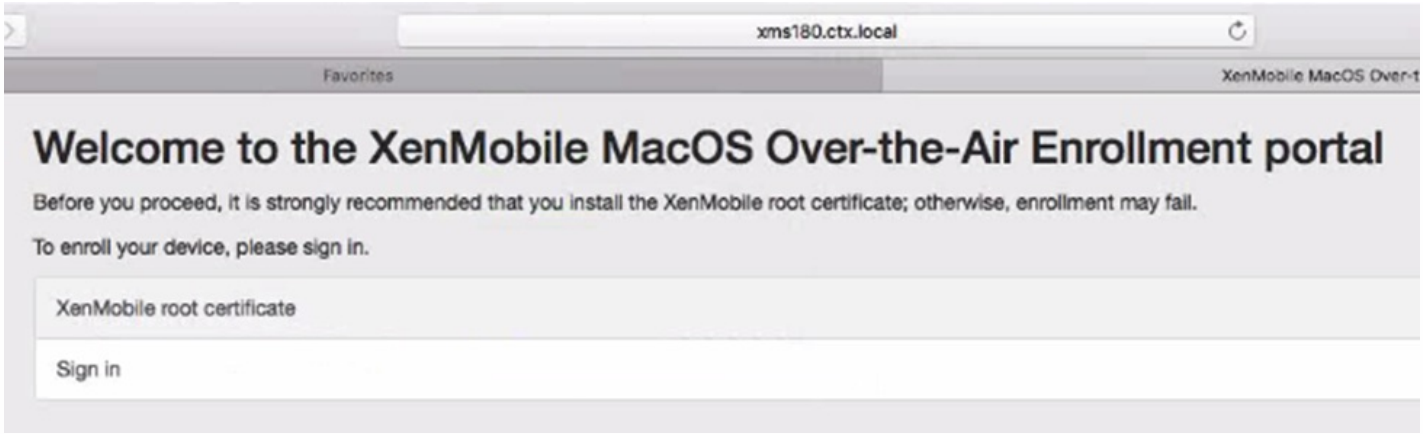
-
-
-

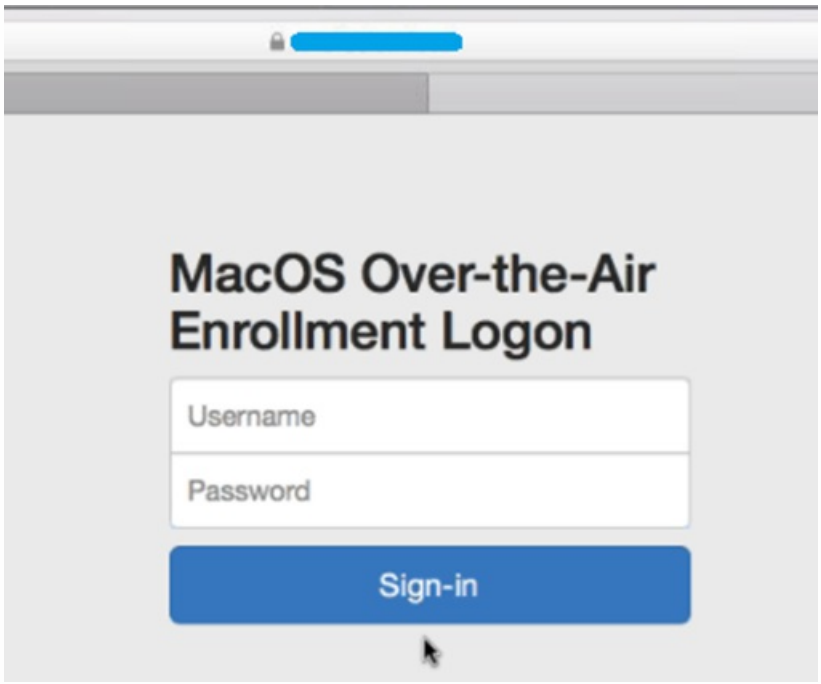


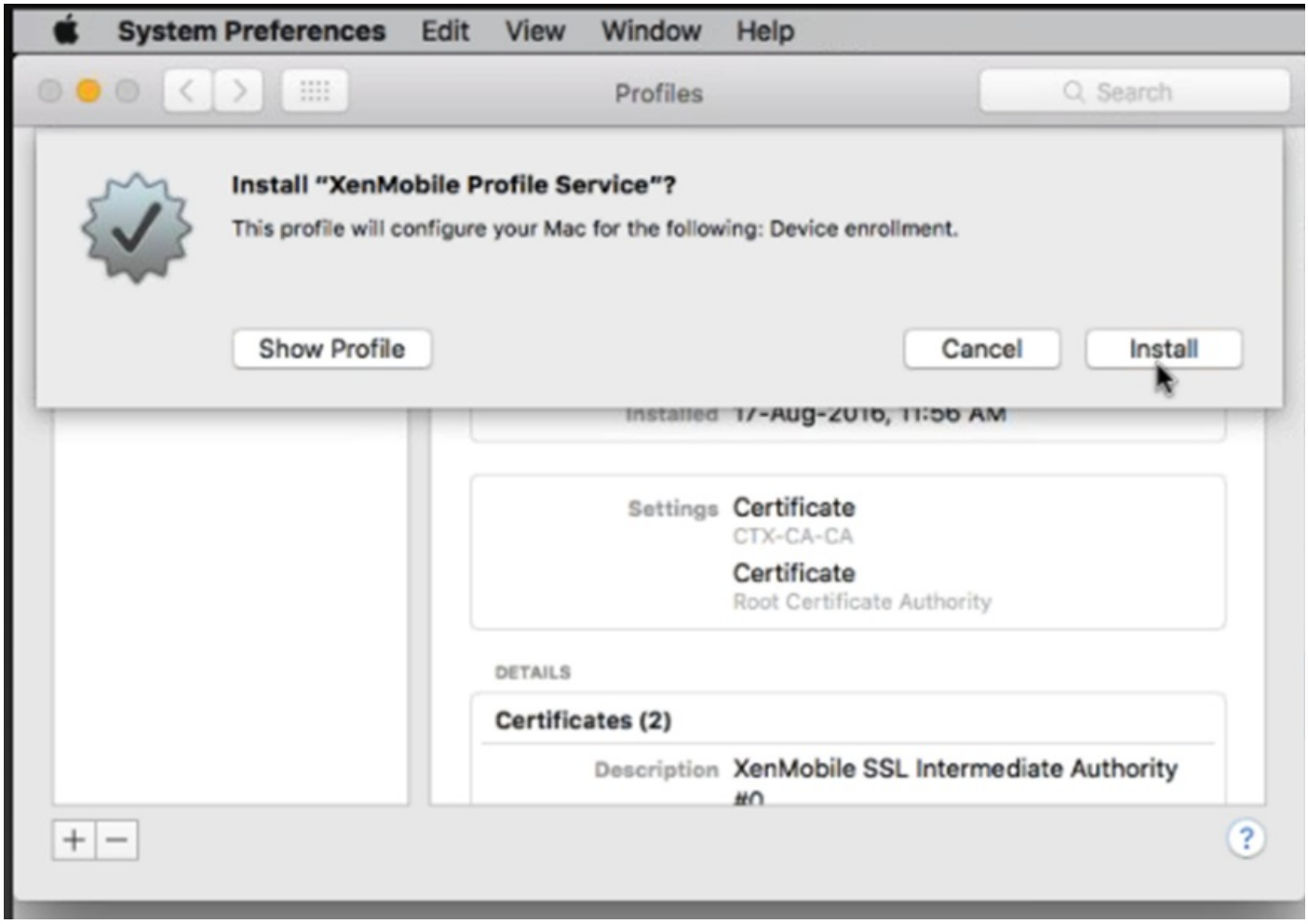


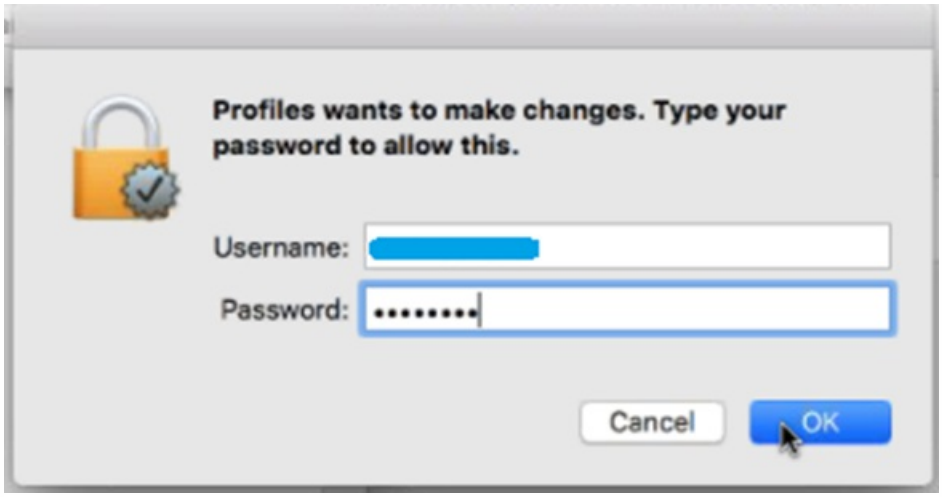


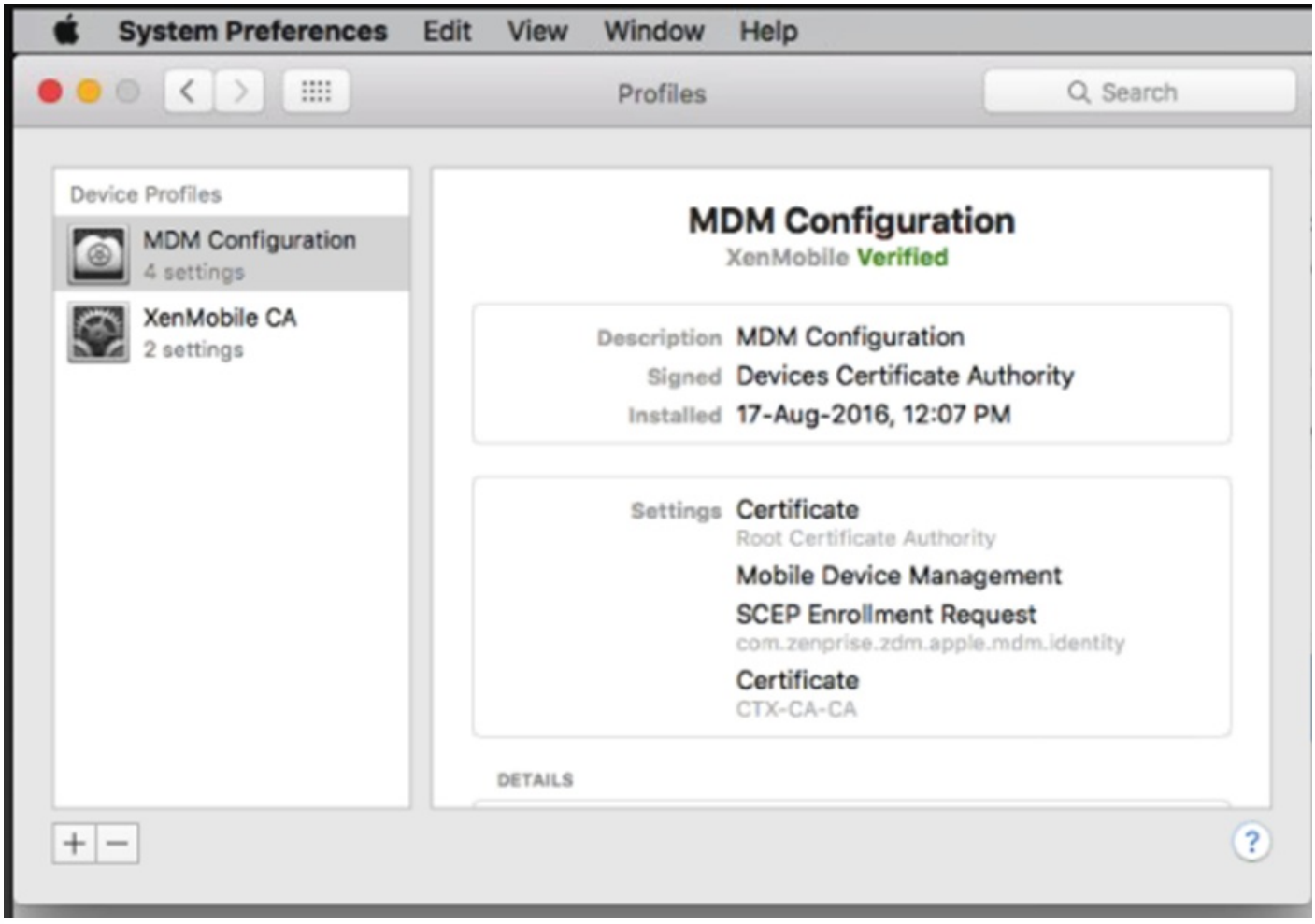


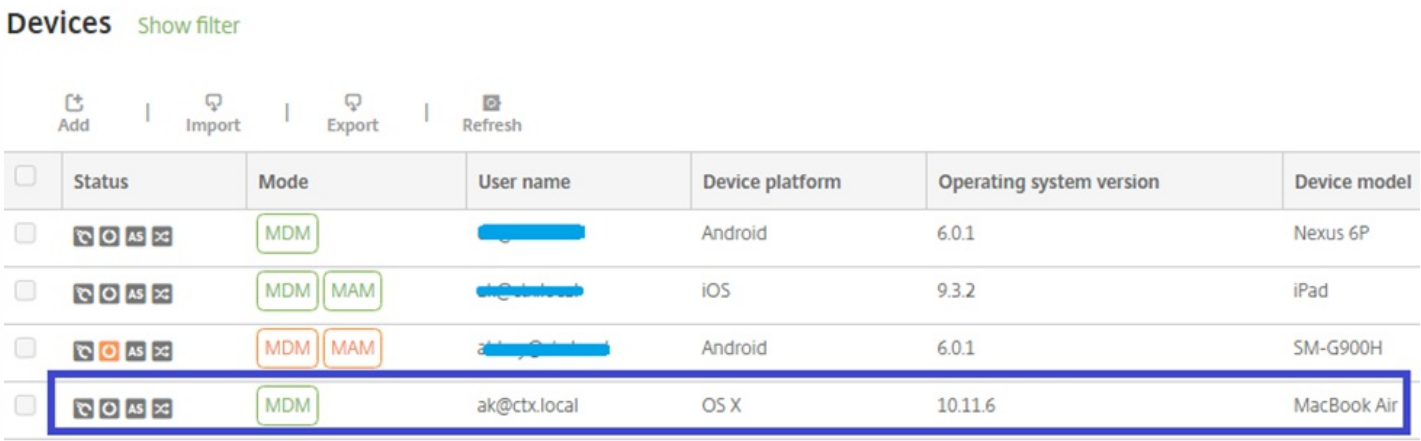












-
-

To enroll Windows devices with autodiscovery

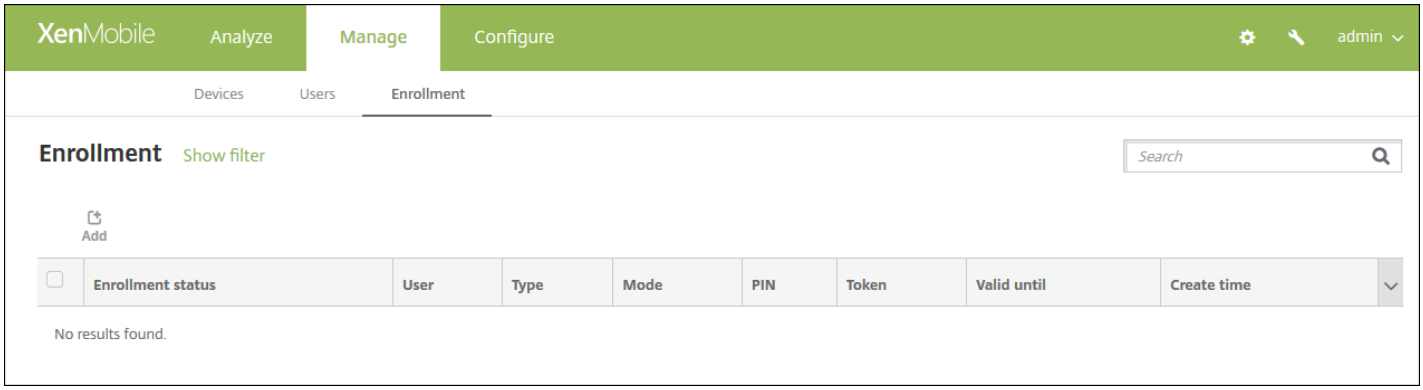
-
-

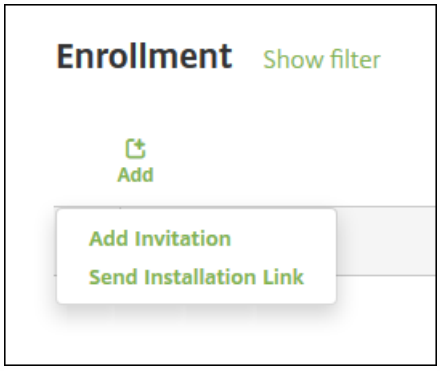
To enroll Windows devices without autodiscovery

-
-
-
-

To enroll Windows Phone devices in XenMobile

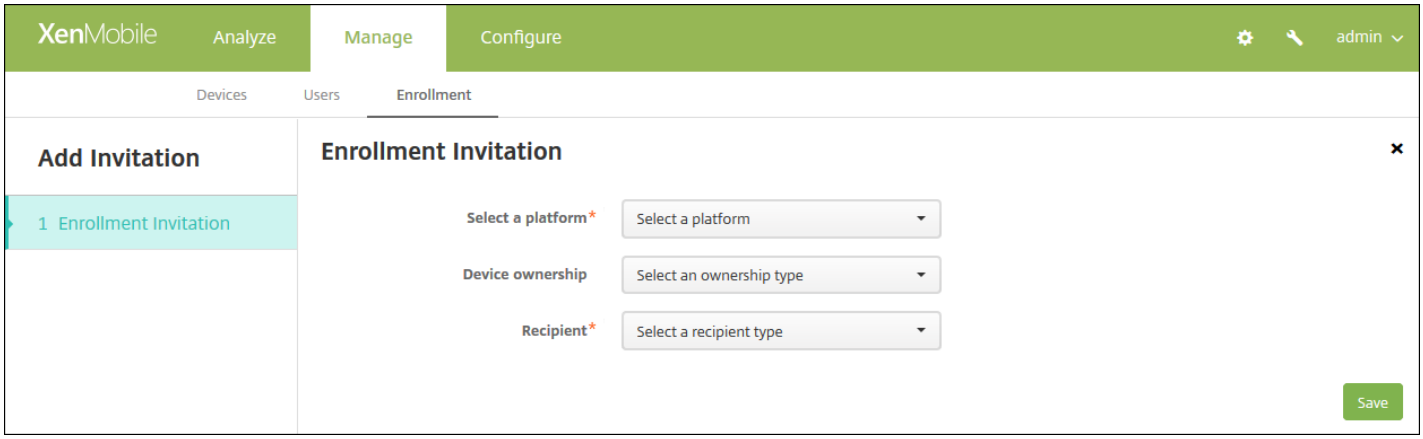
-
-



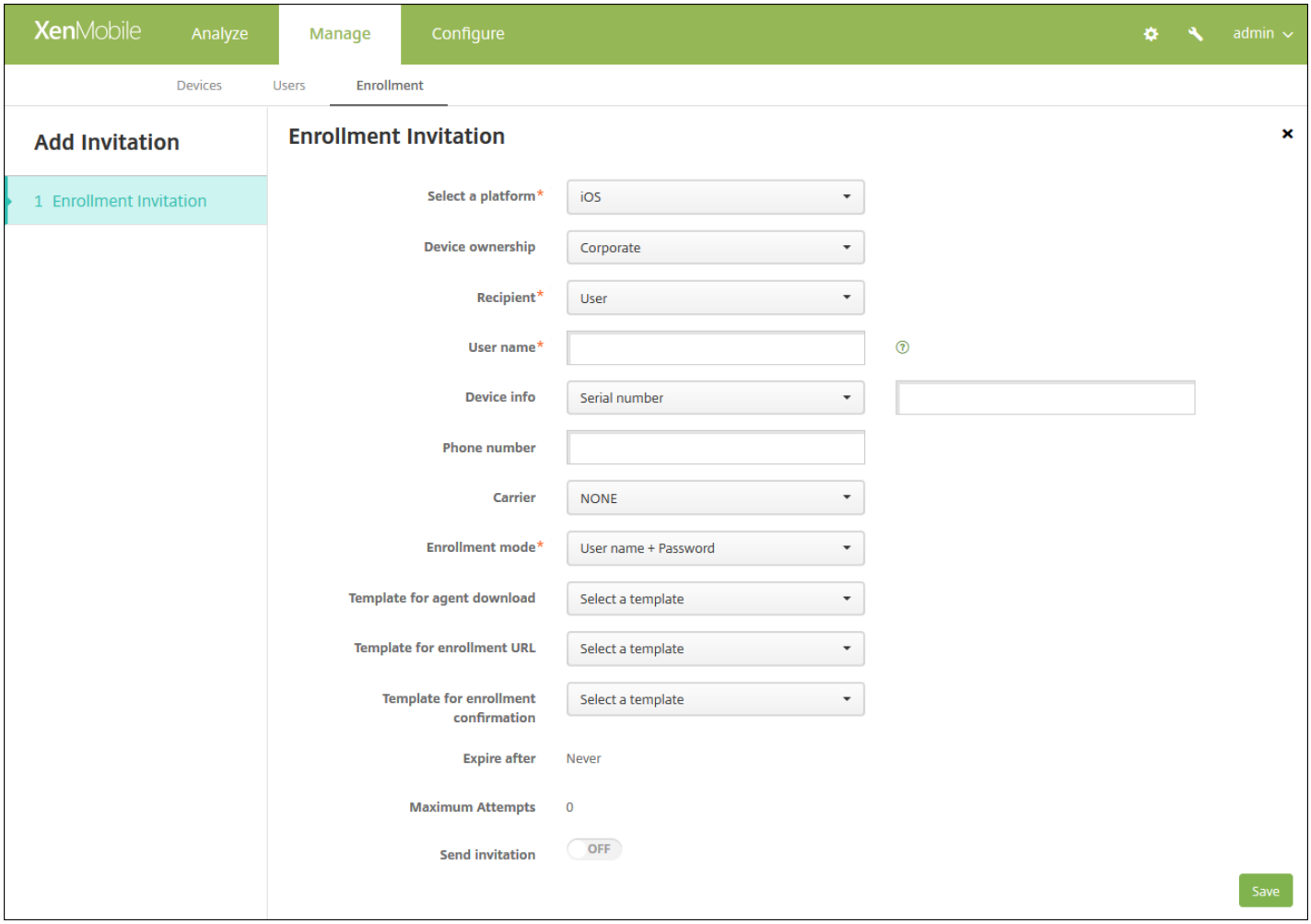


-
-

To send an invitation

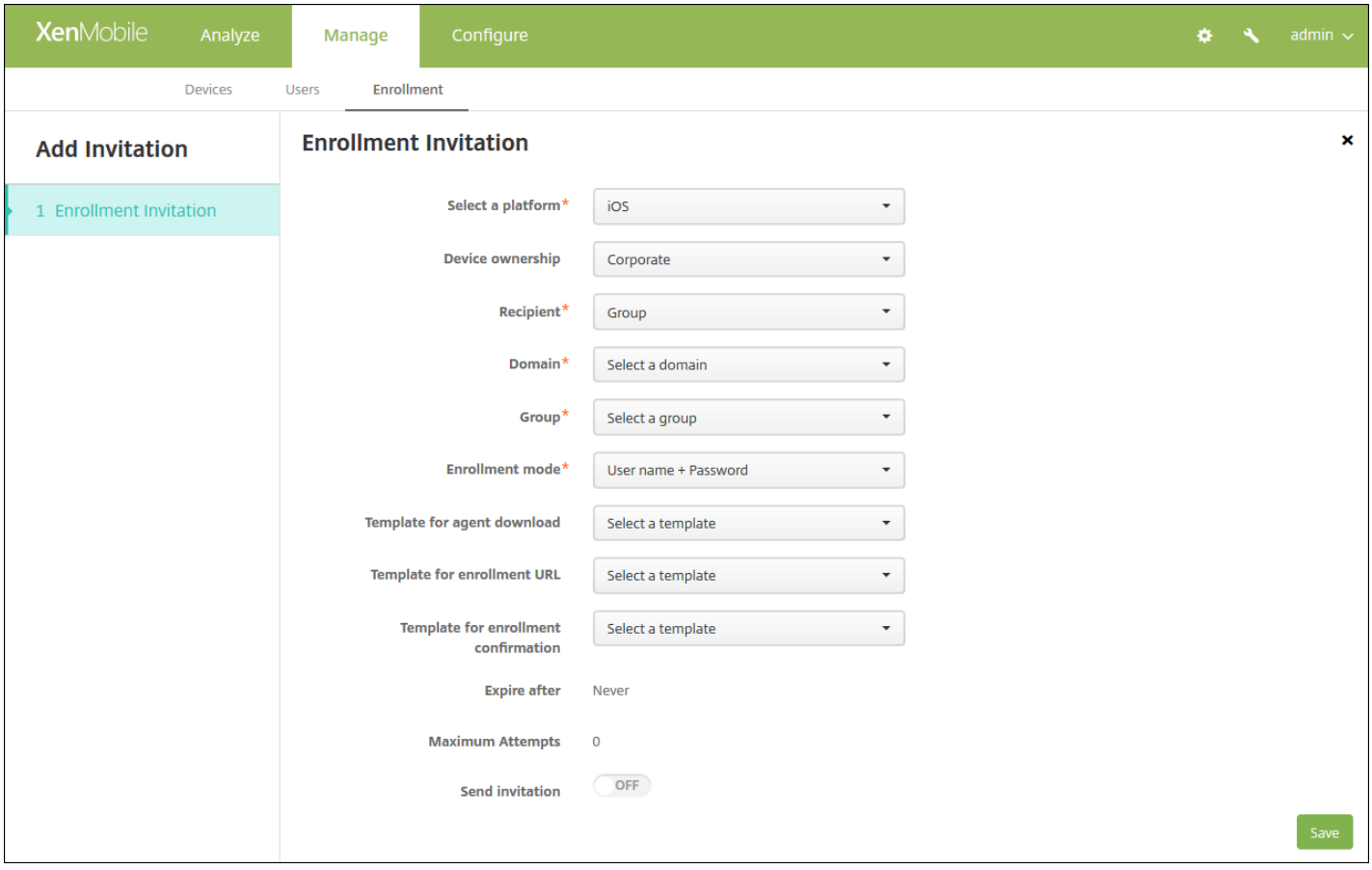


-
-
-



-
-
-
-
-
  -
  -
  -
  -
  -
  -

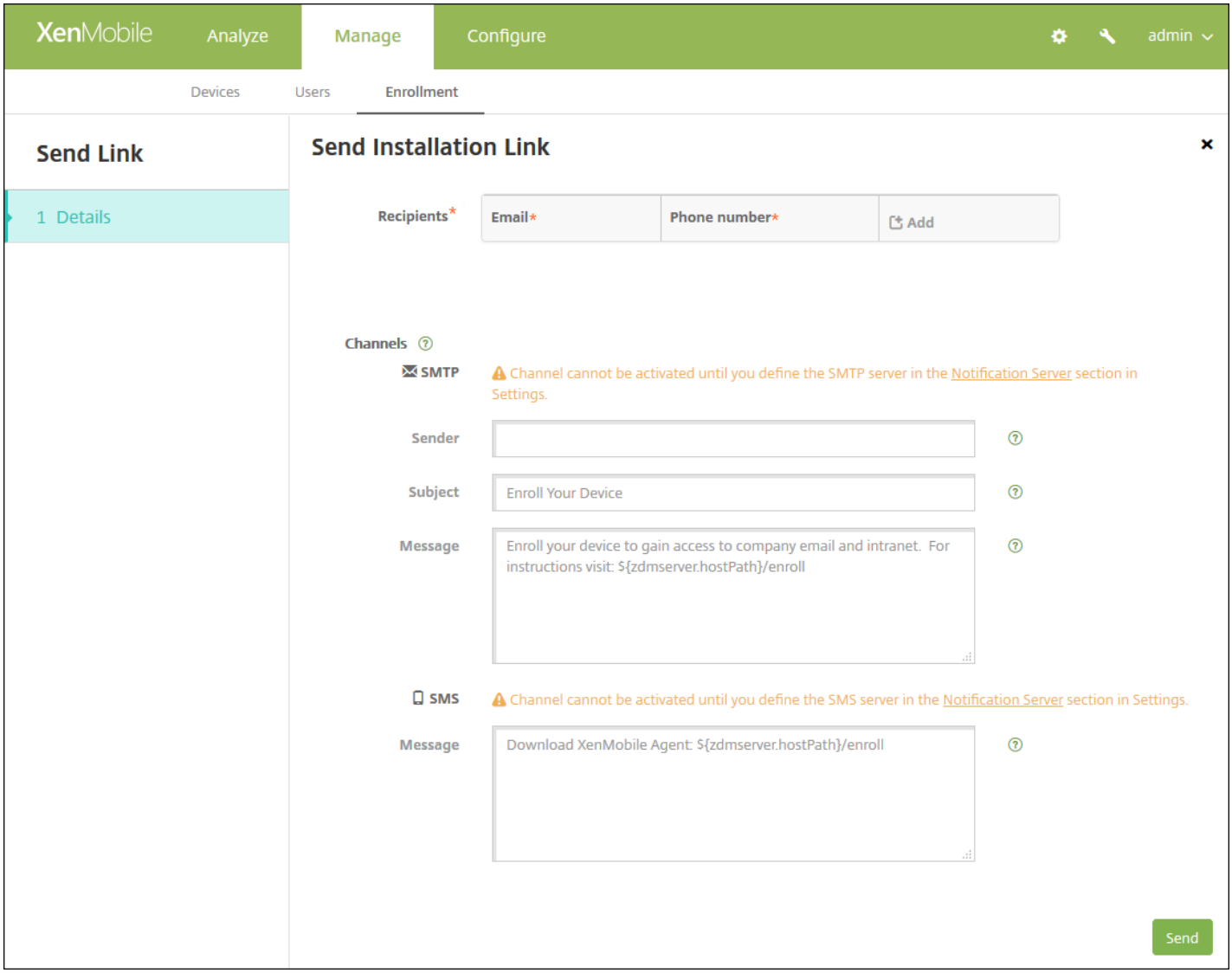
-
-
-
-
-
-



-
-

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

To send an installation link



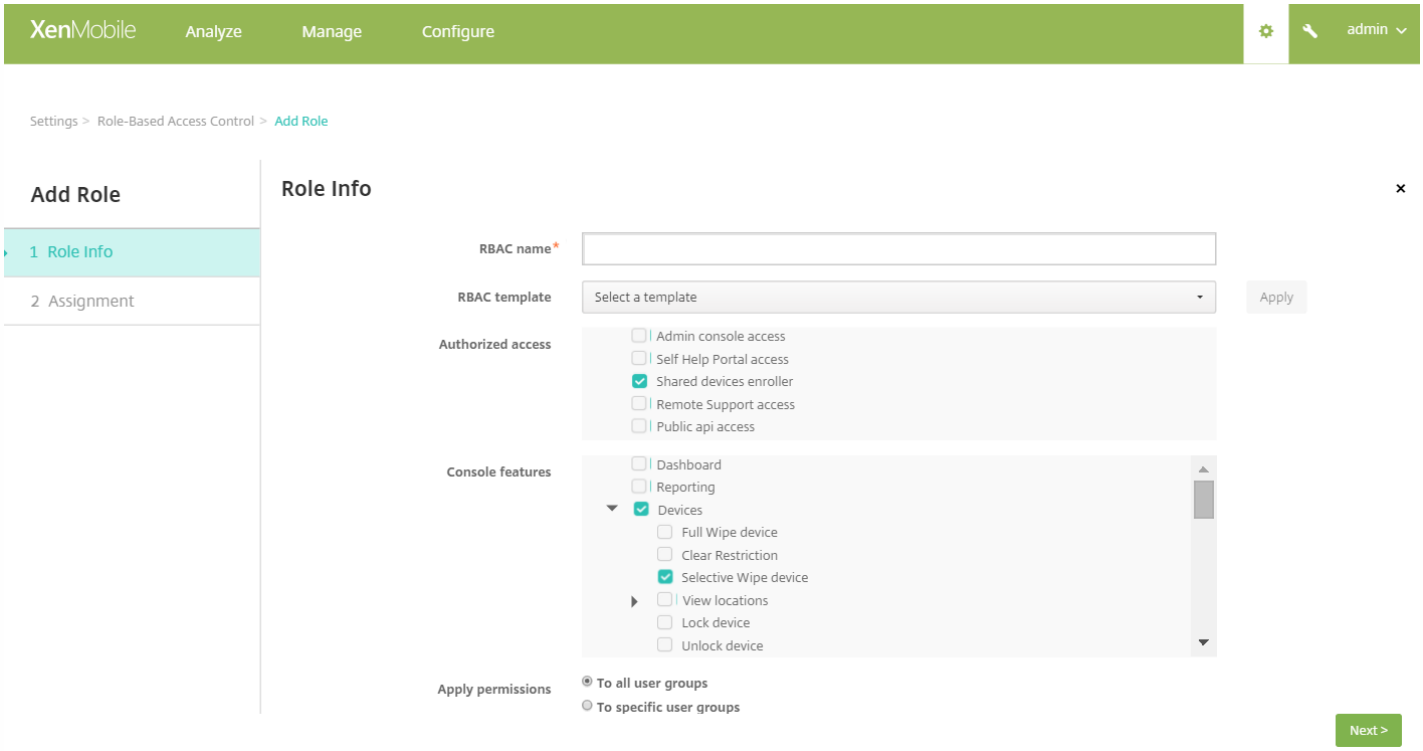
-
  -
  -
  -

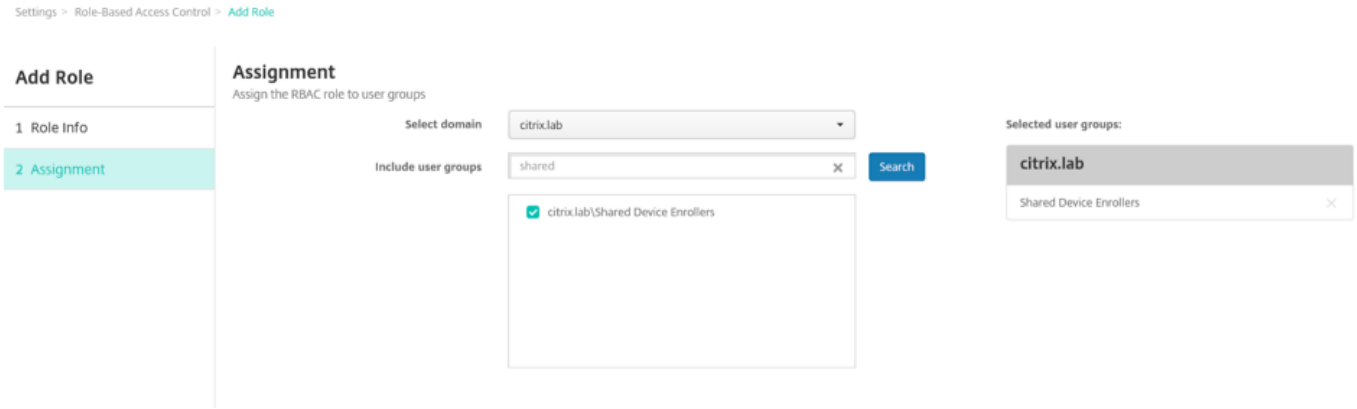
-
  -
    -
    -
    -
  -
    -

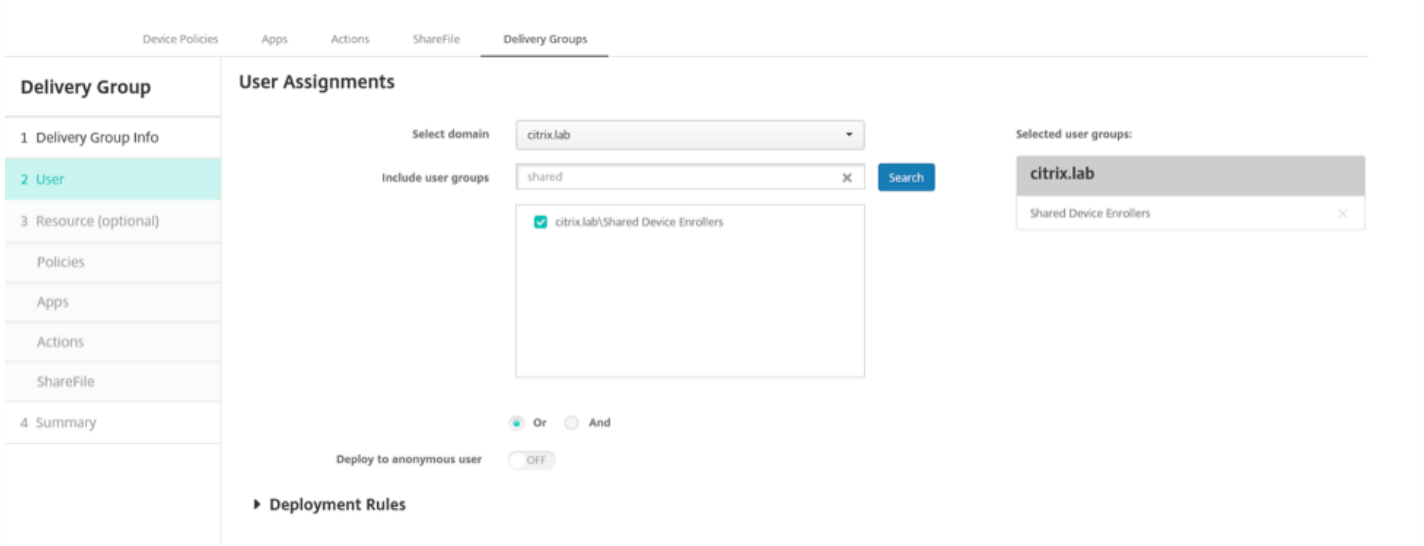
-
-
-

Pre-requisites for MDM+MAM Mode

-
-
-
-
-
-







MDM mode

MDM+MAM mode

-

-
-

-
-
-

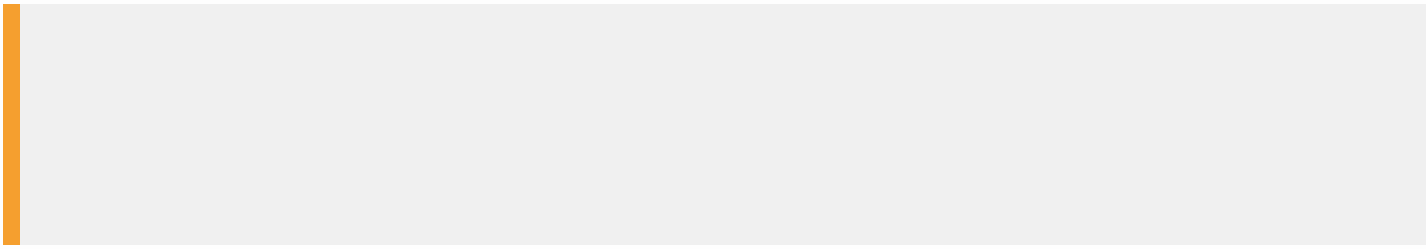
-
-

-
-
-
-
-

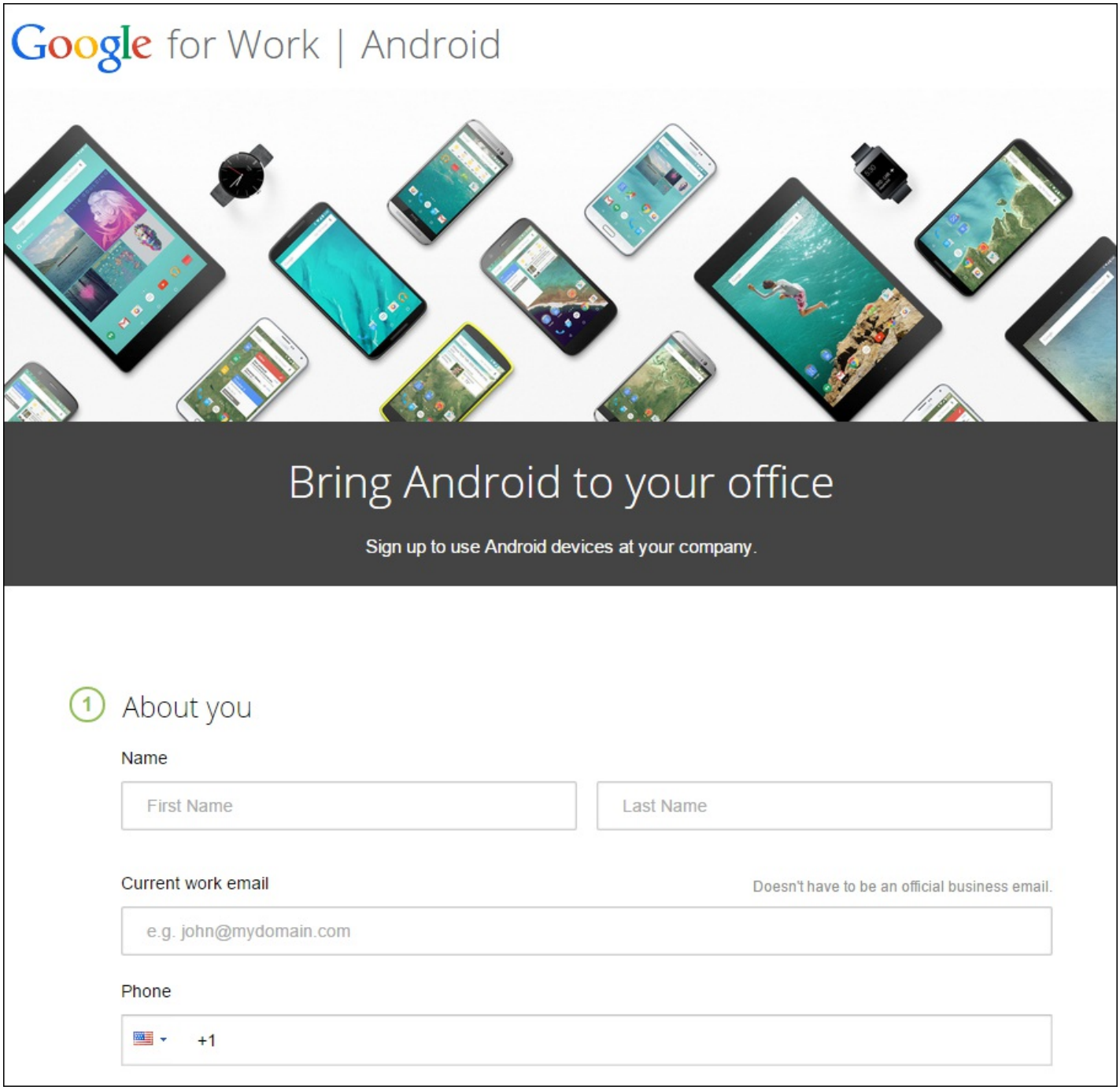
-
-
-
-

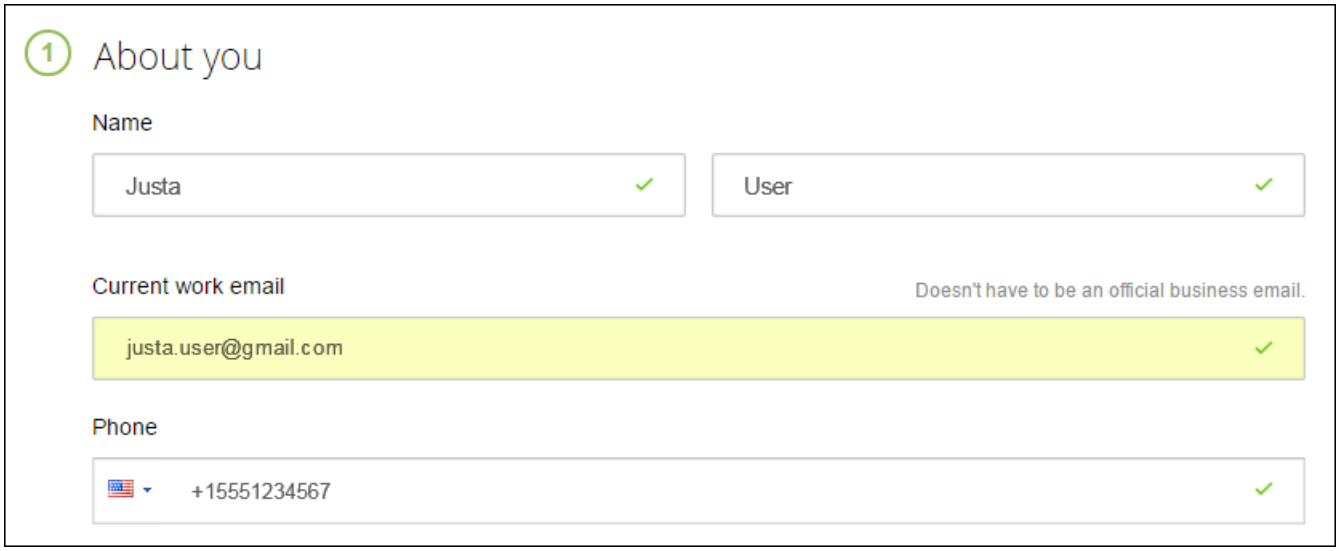
Android for Work Prerequisites

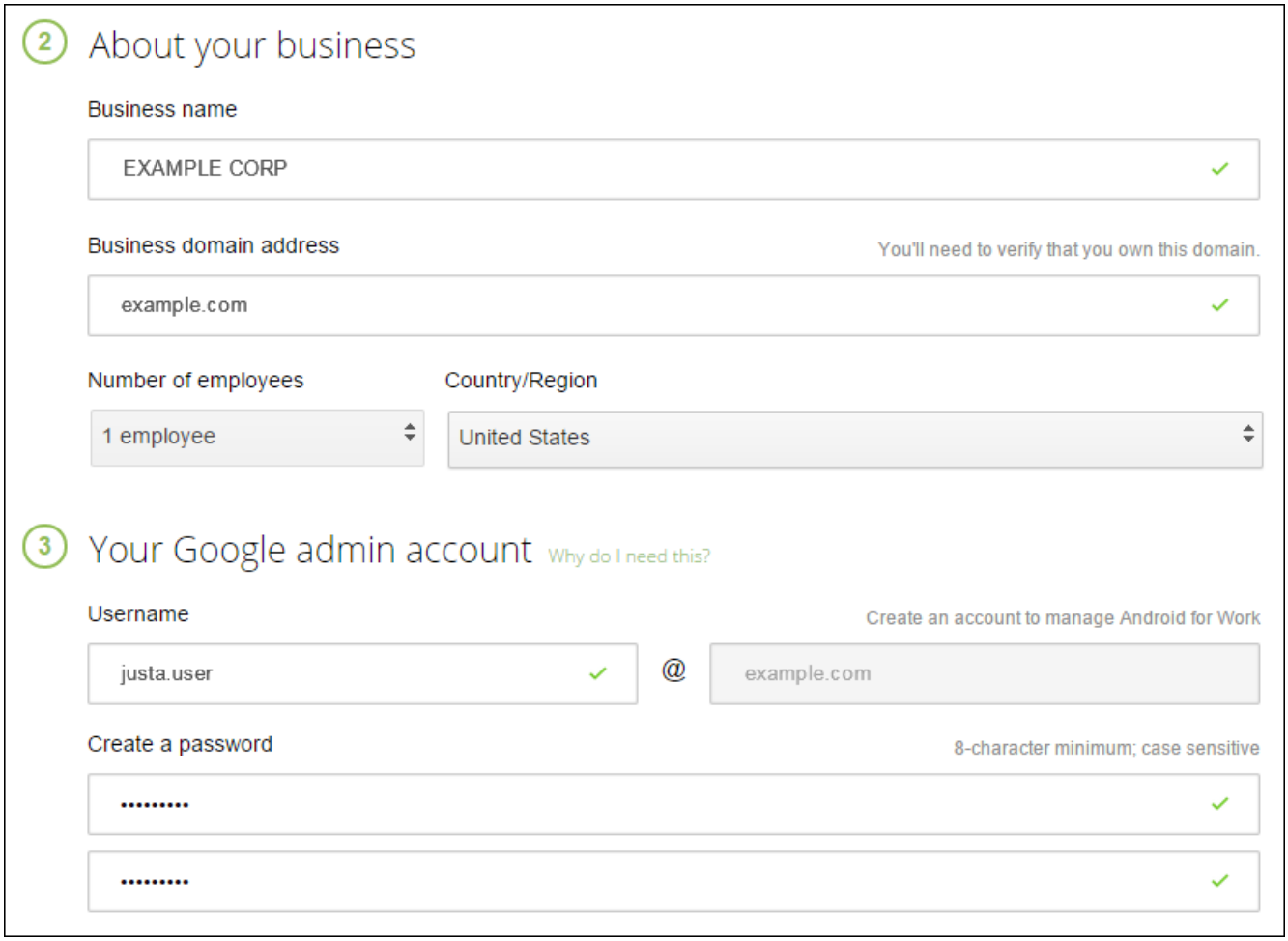
-
-
-
-
-
-

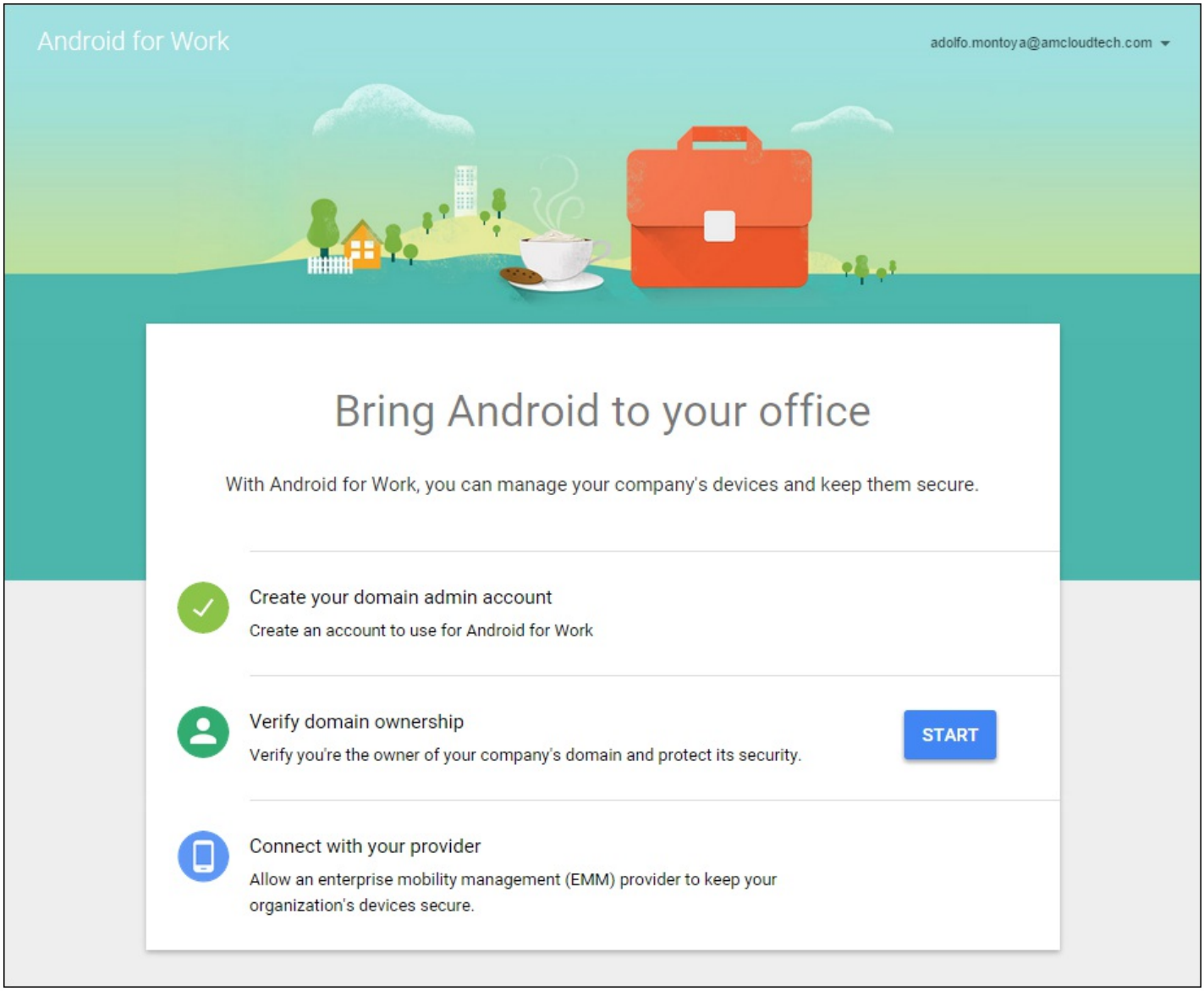


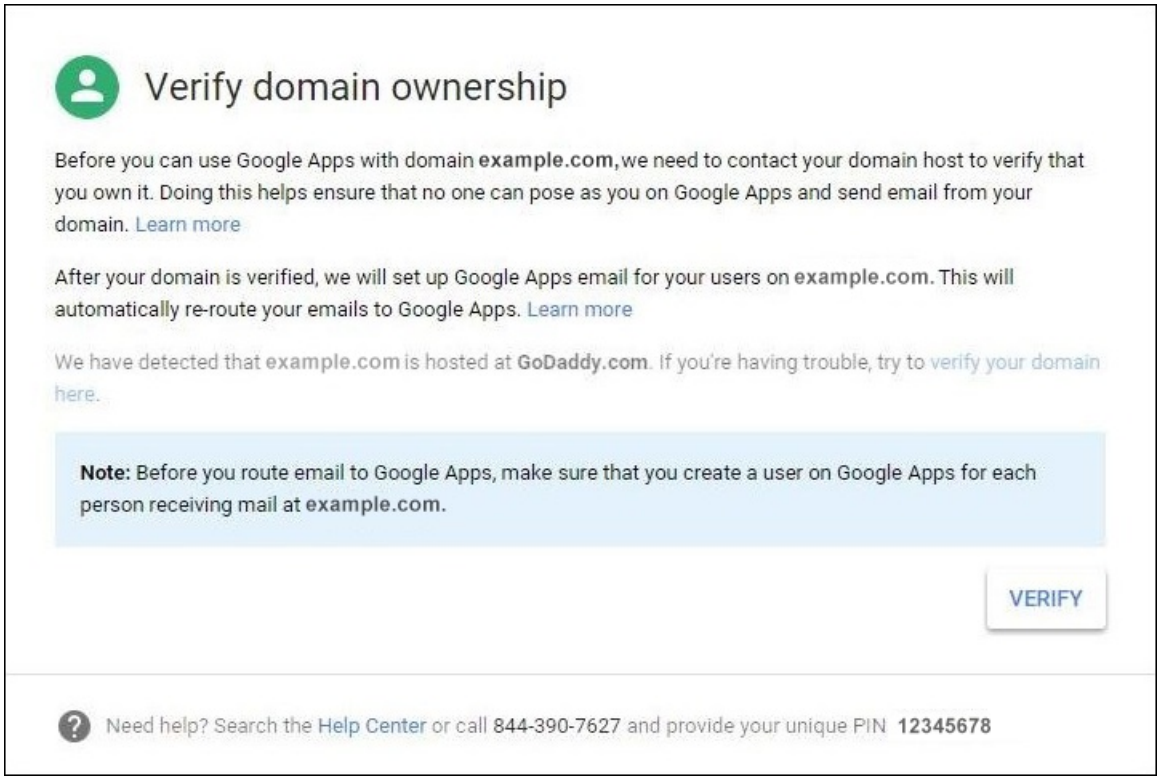
-
-
-

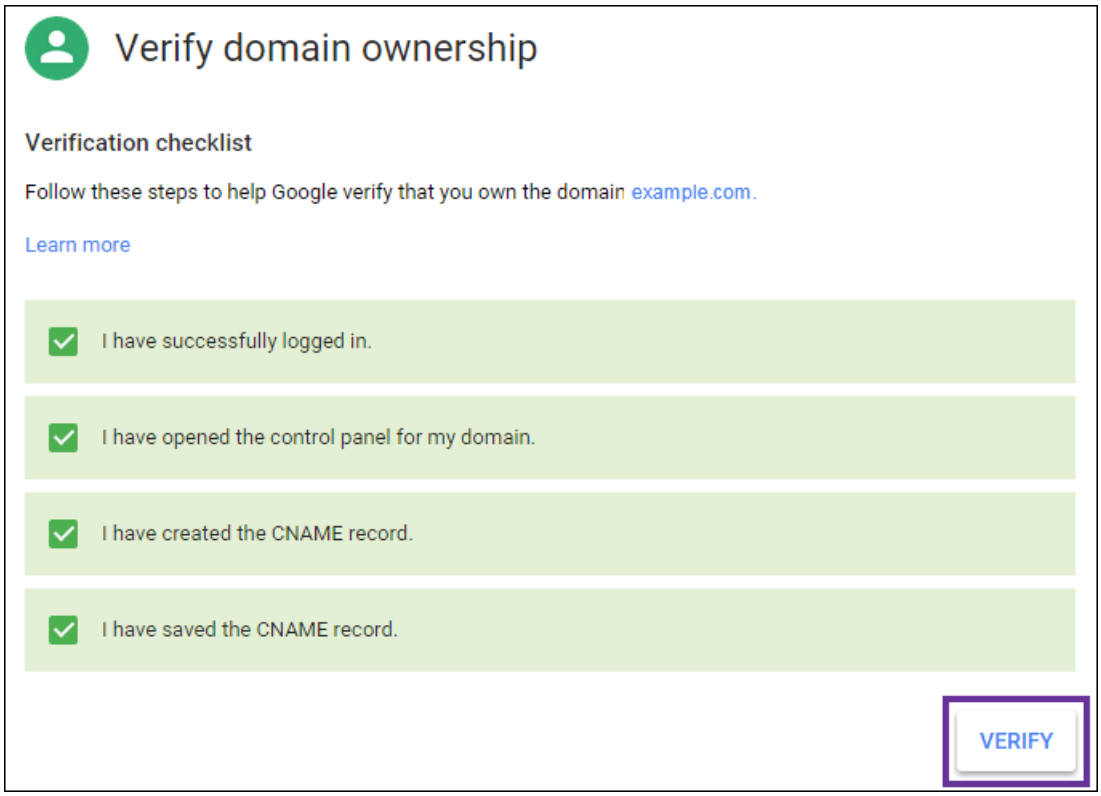


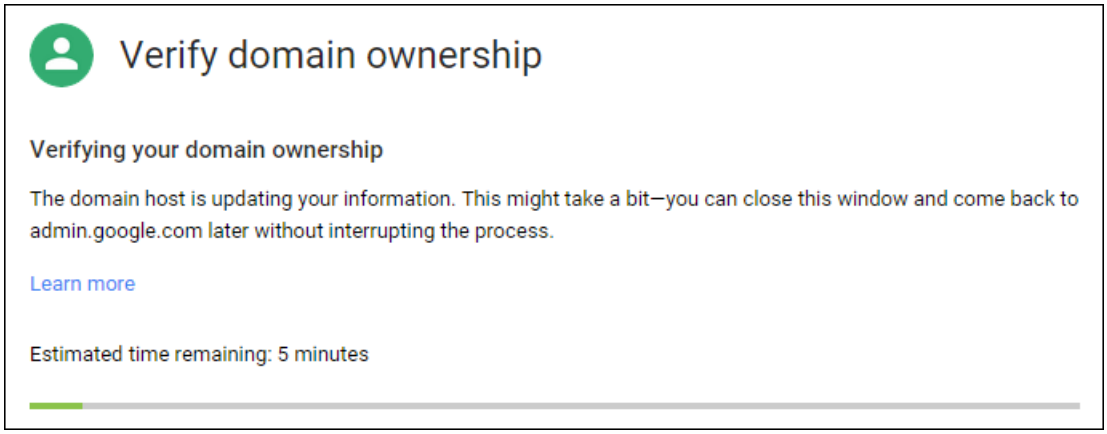


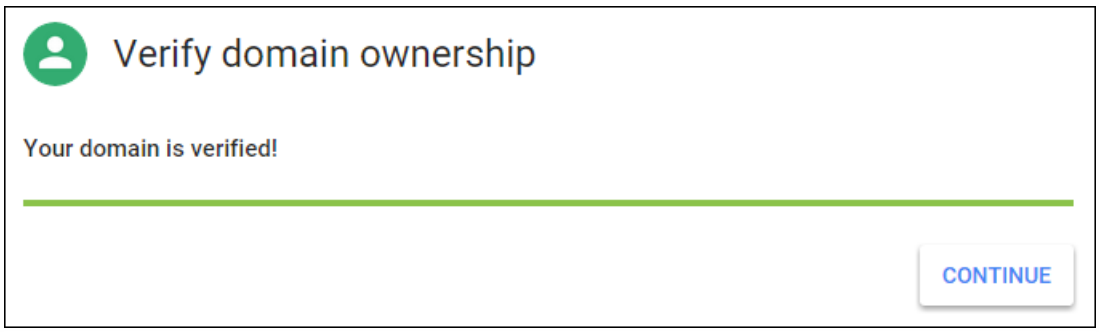


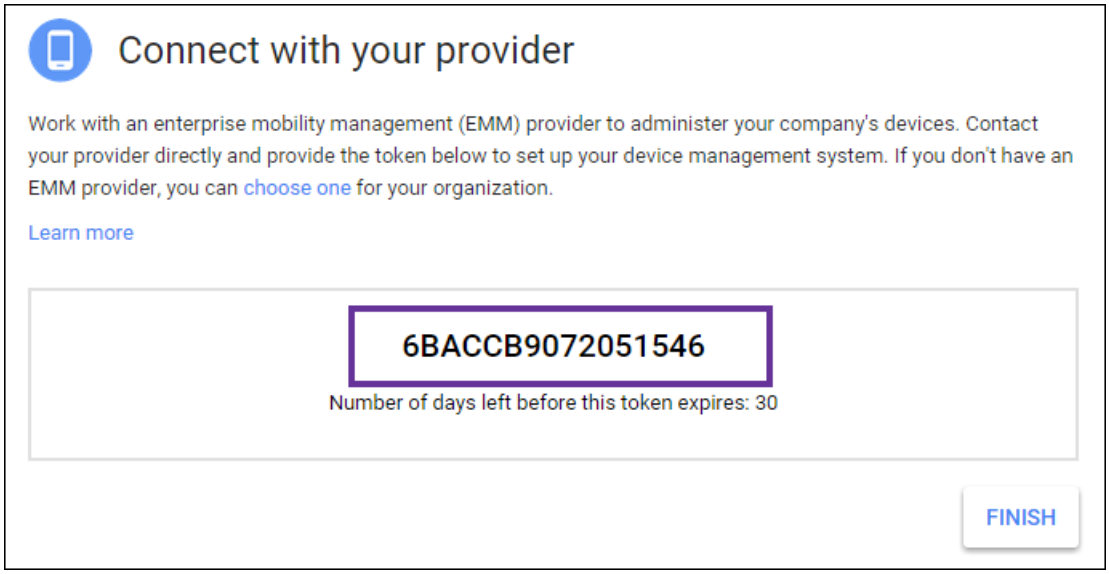


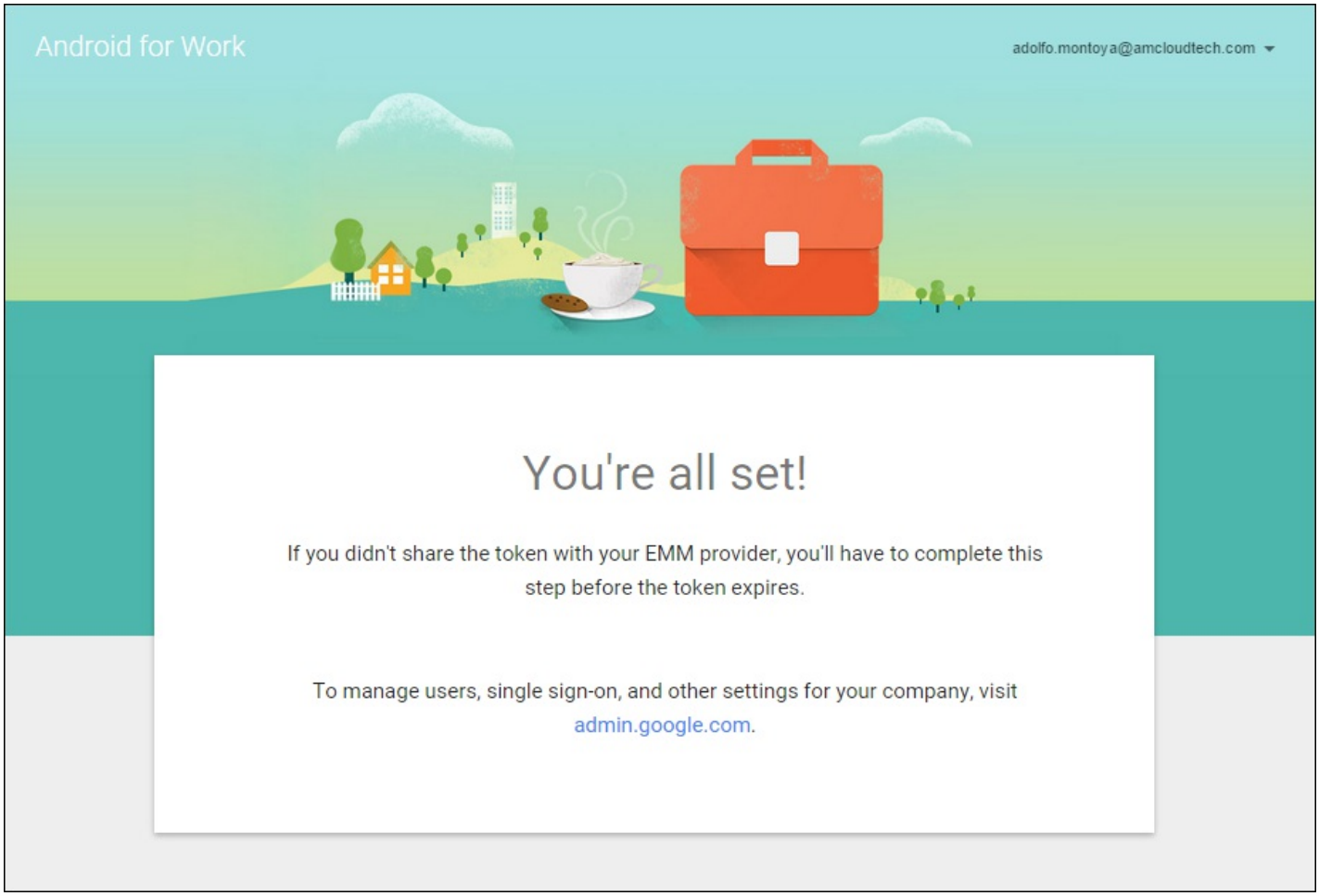


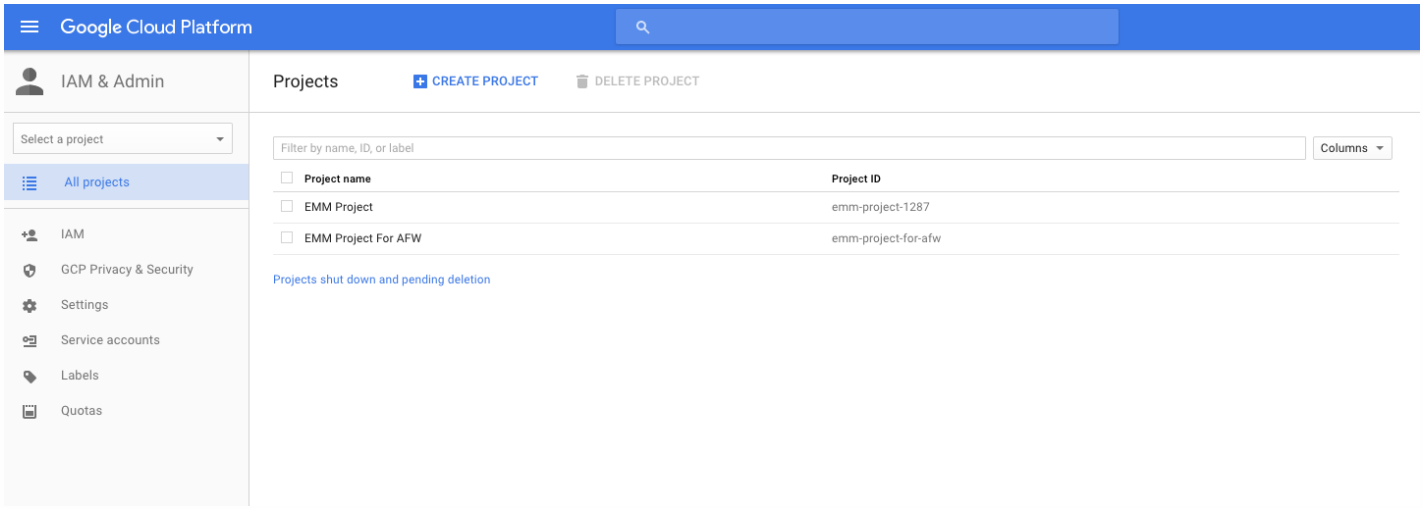


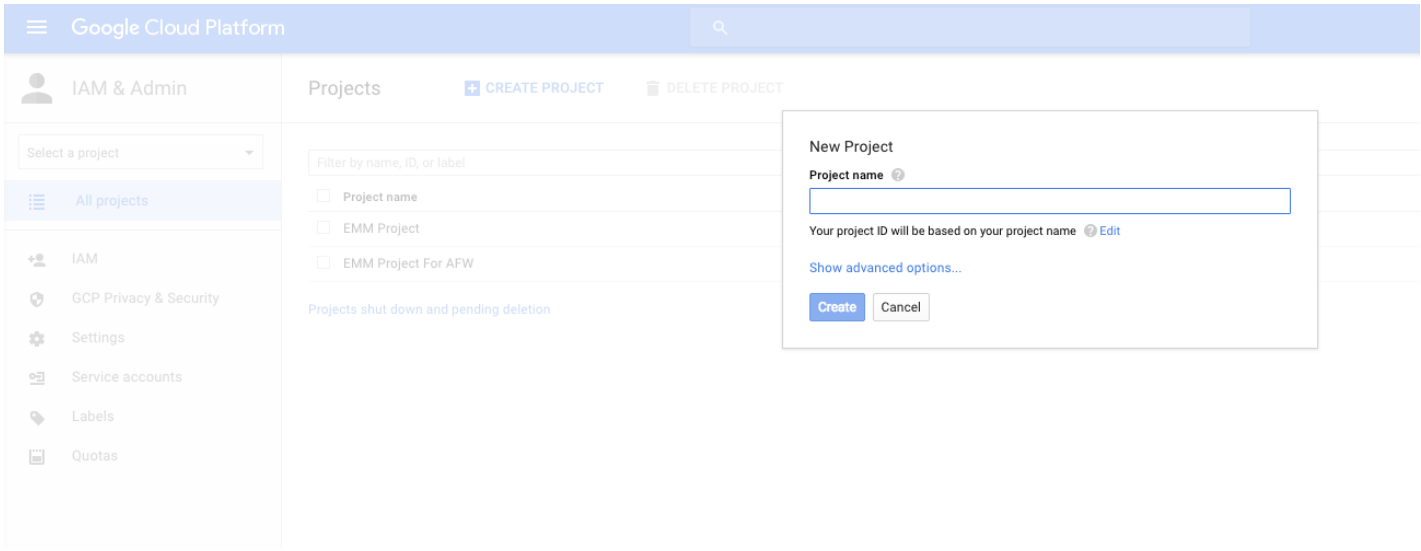


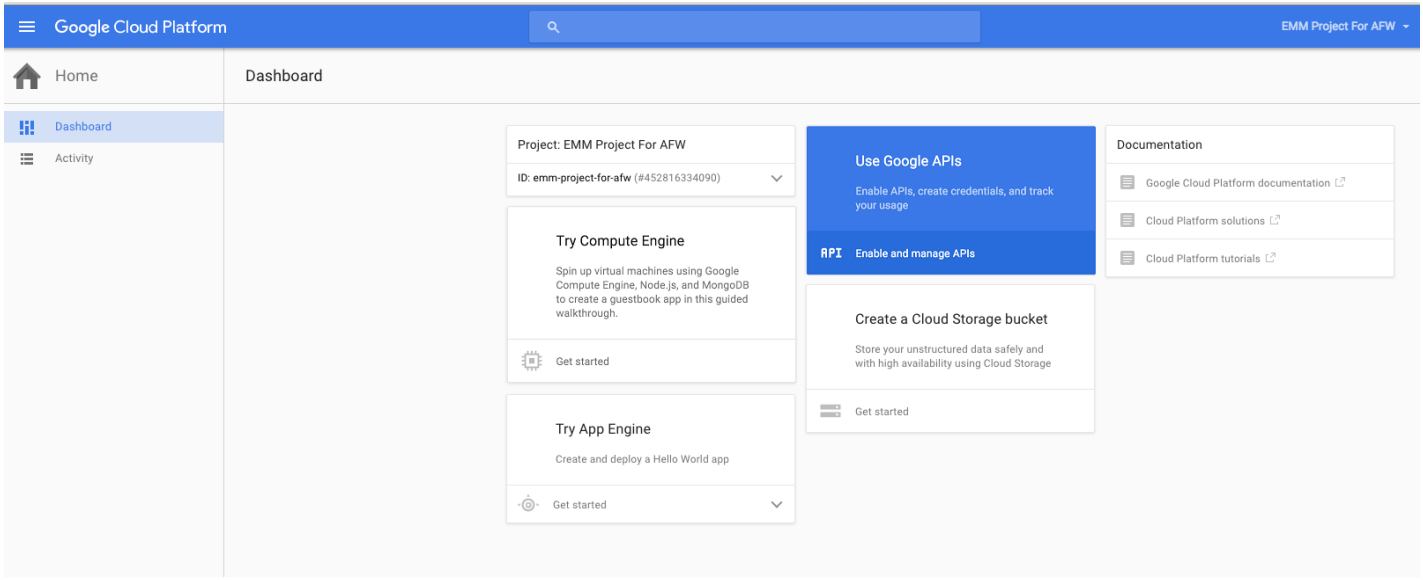


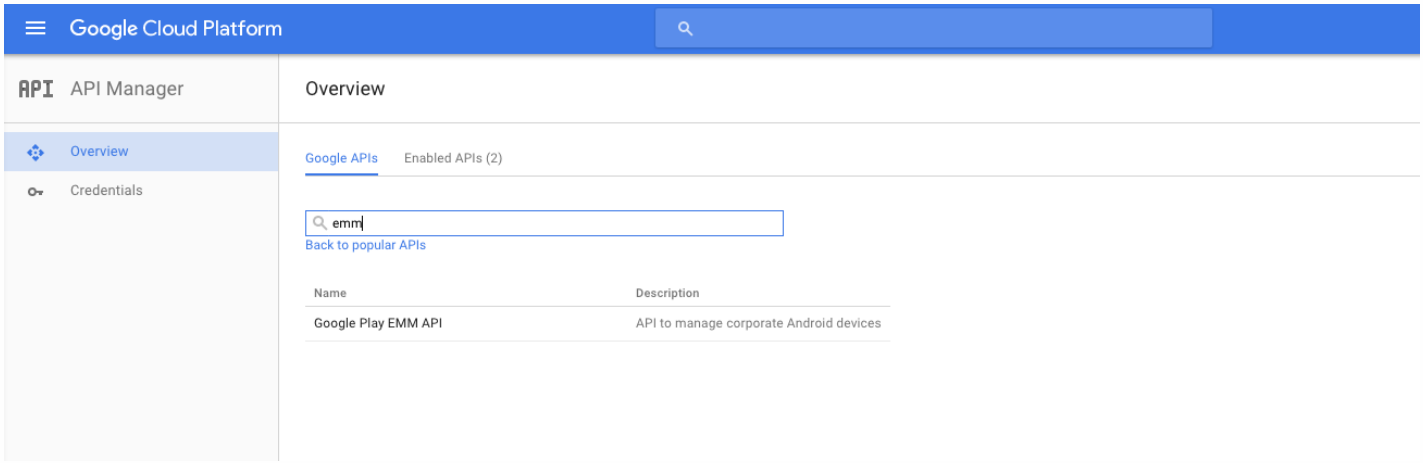


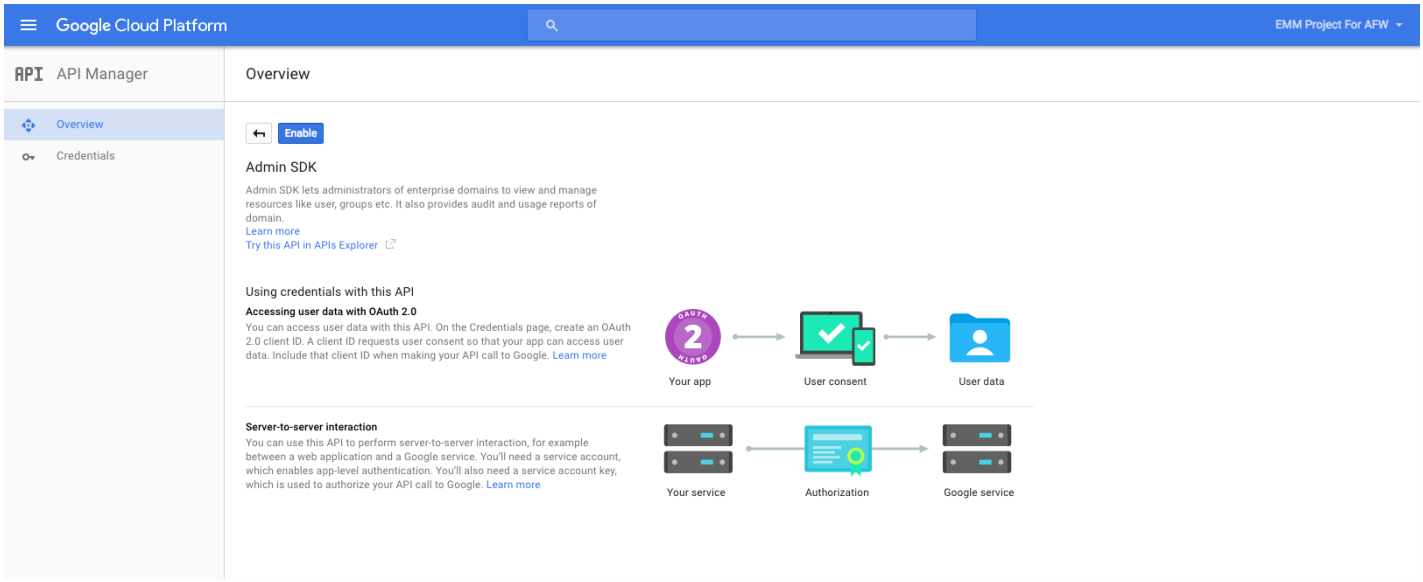


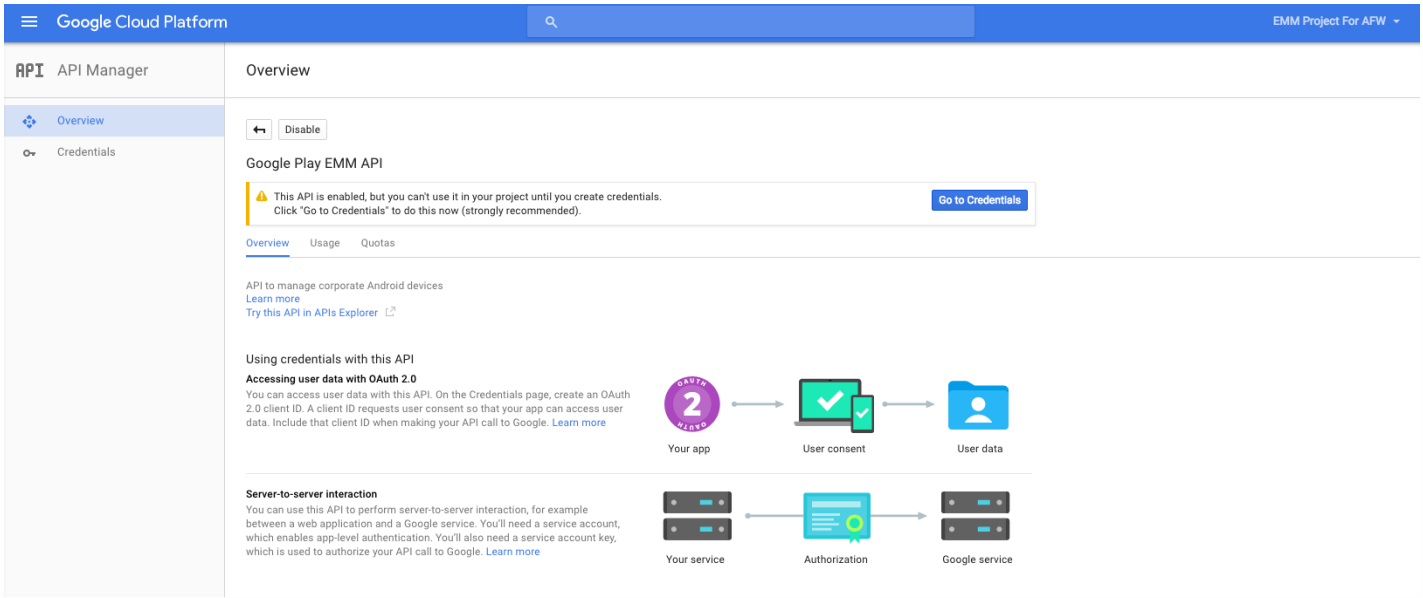


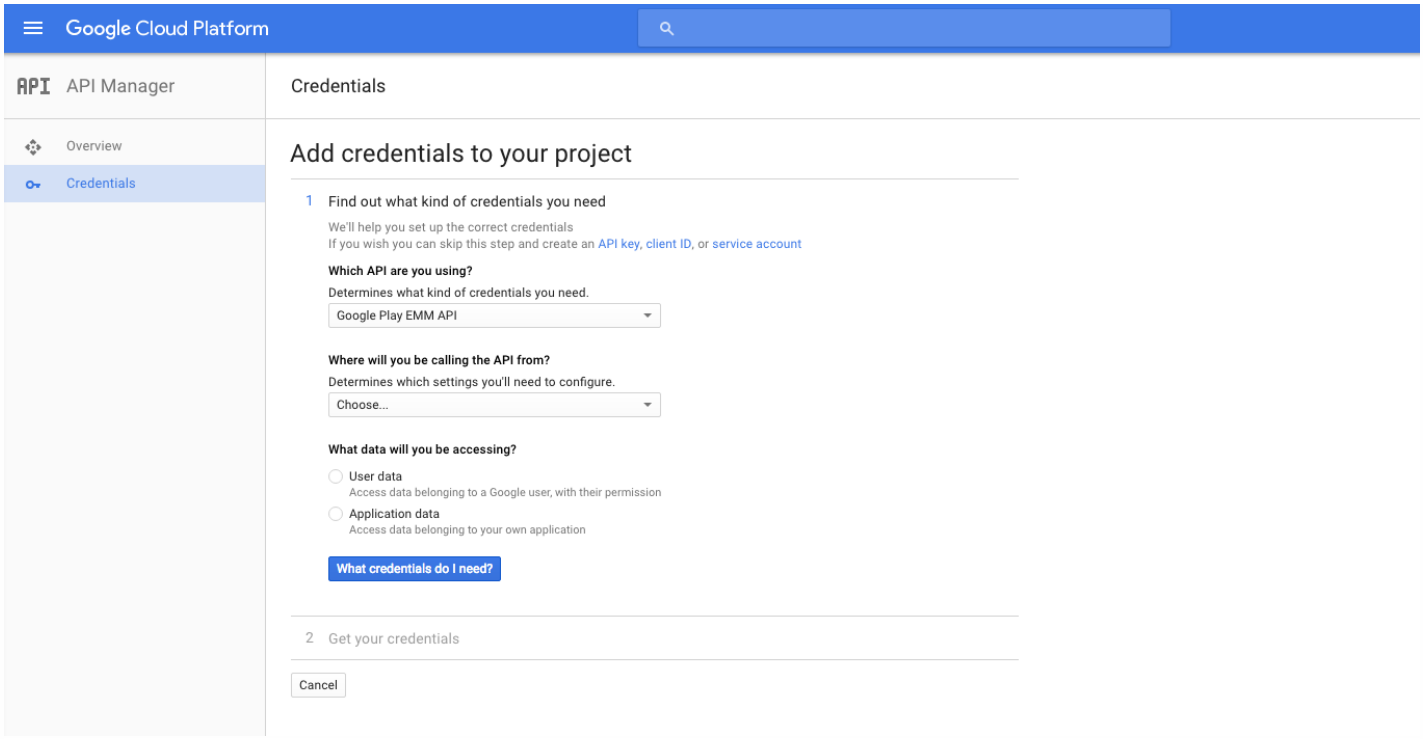


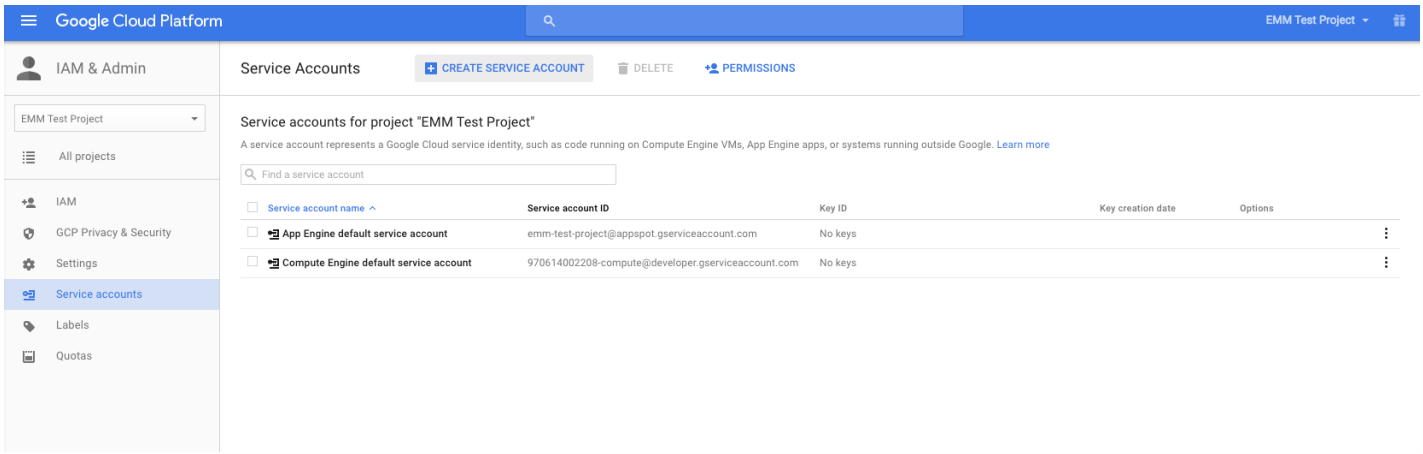


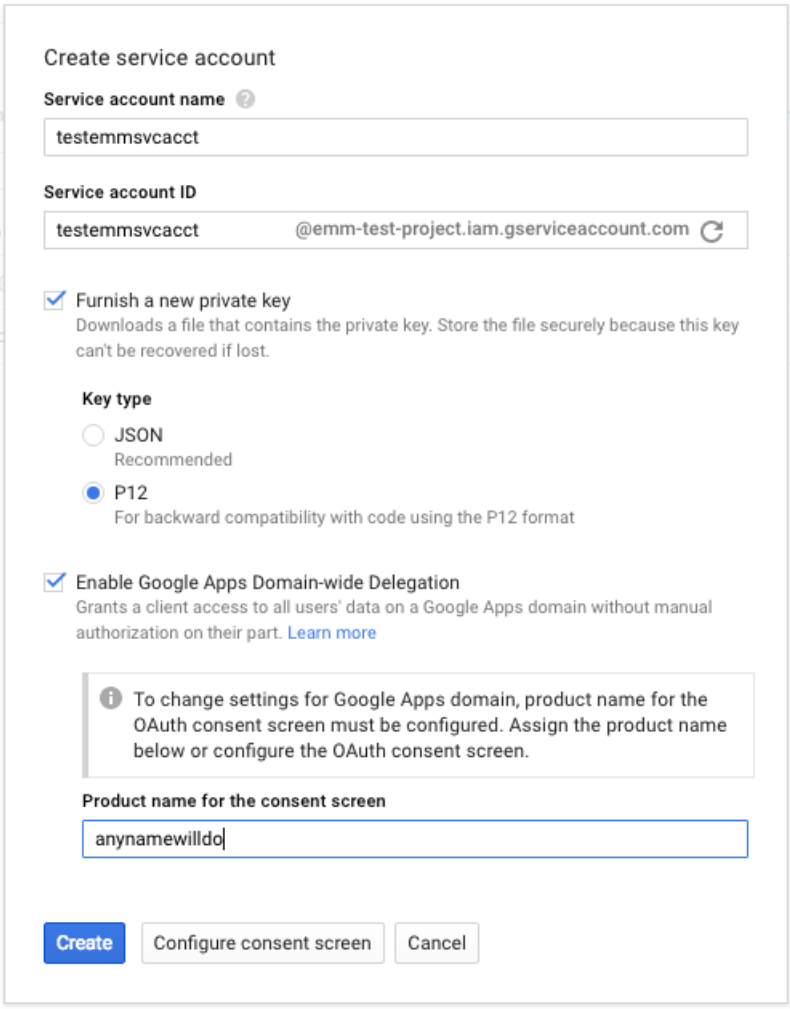


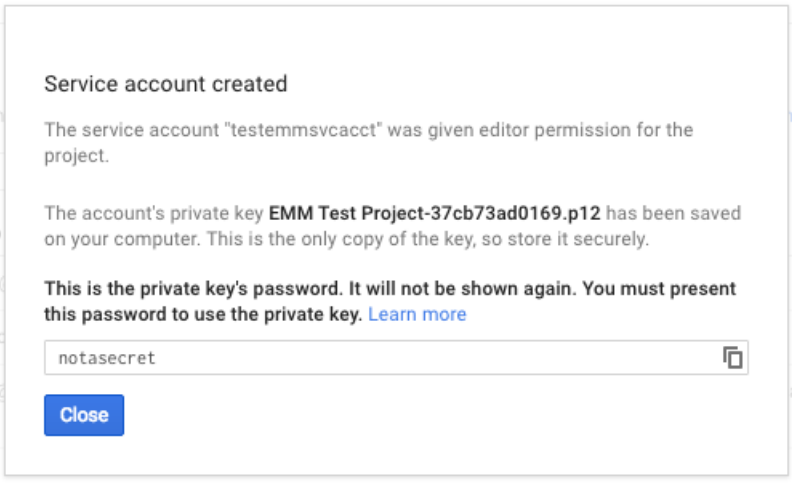


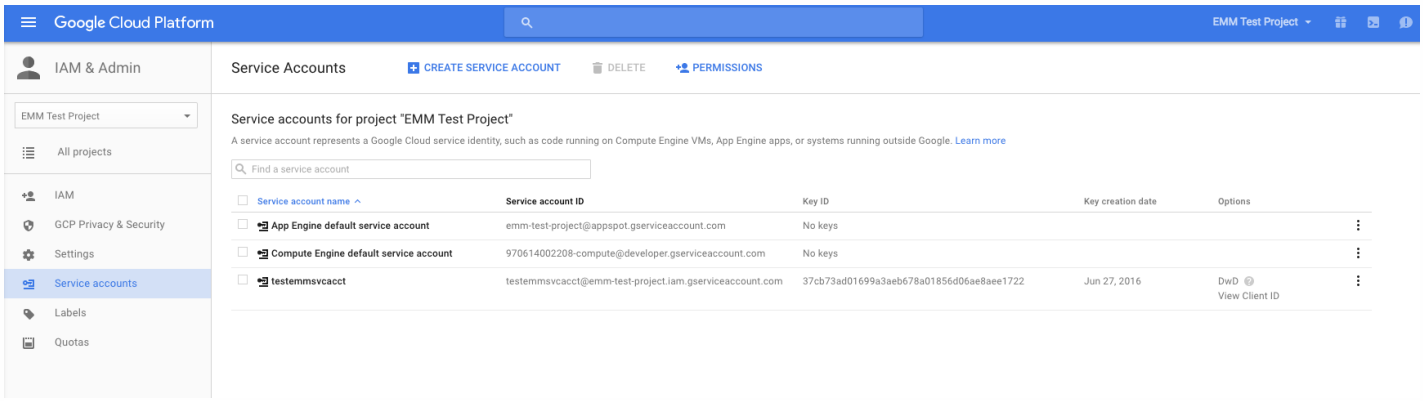


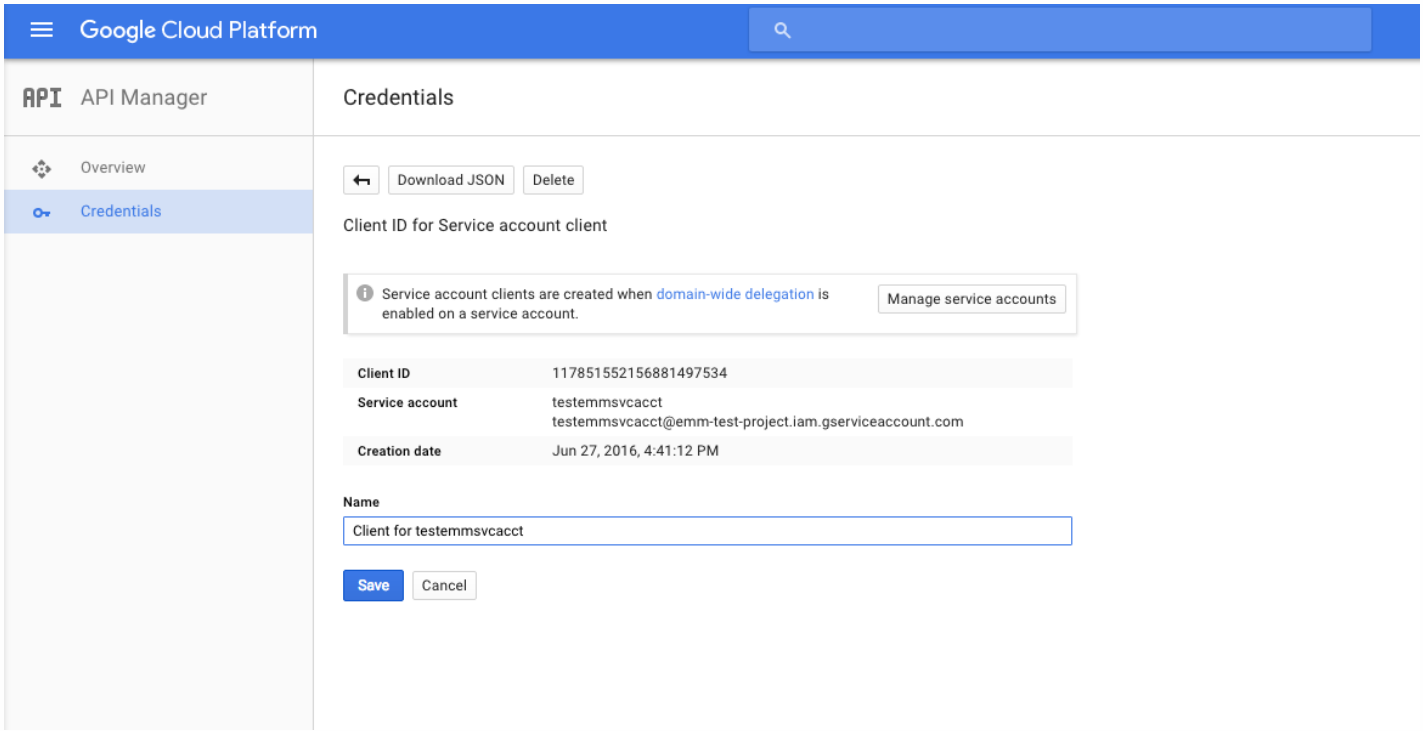


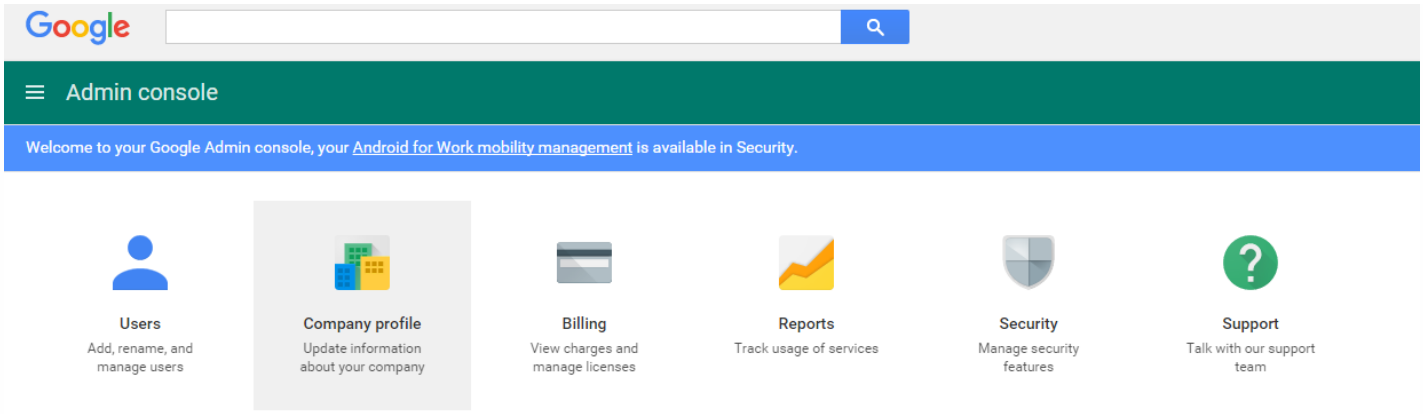


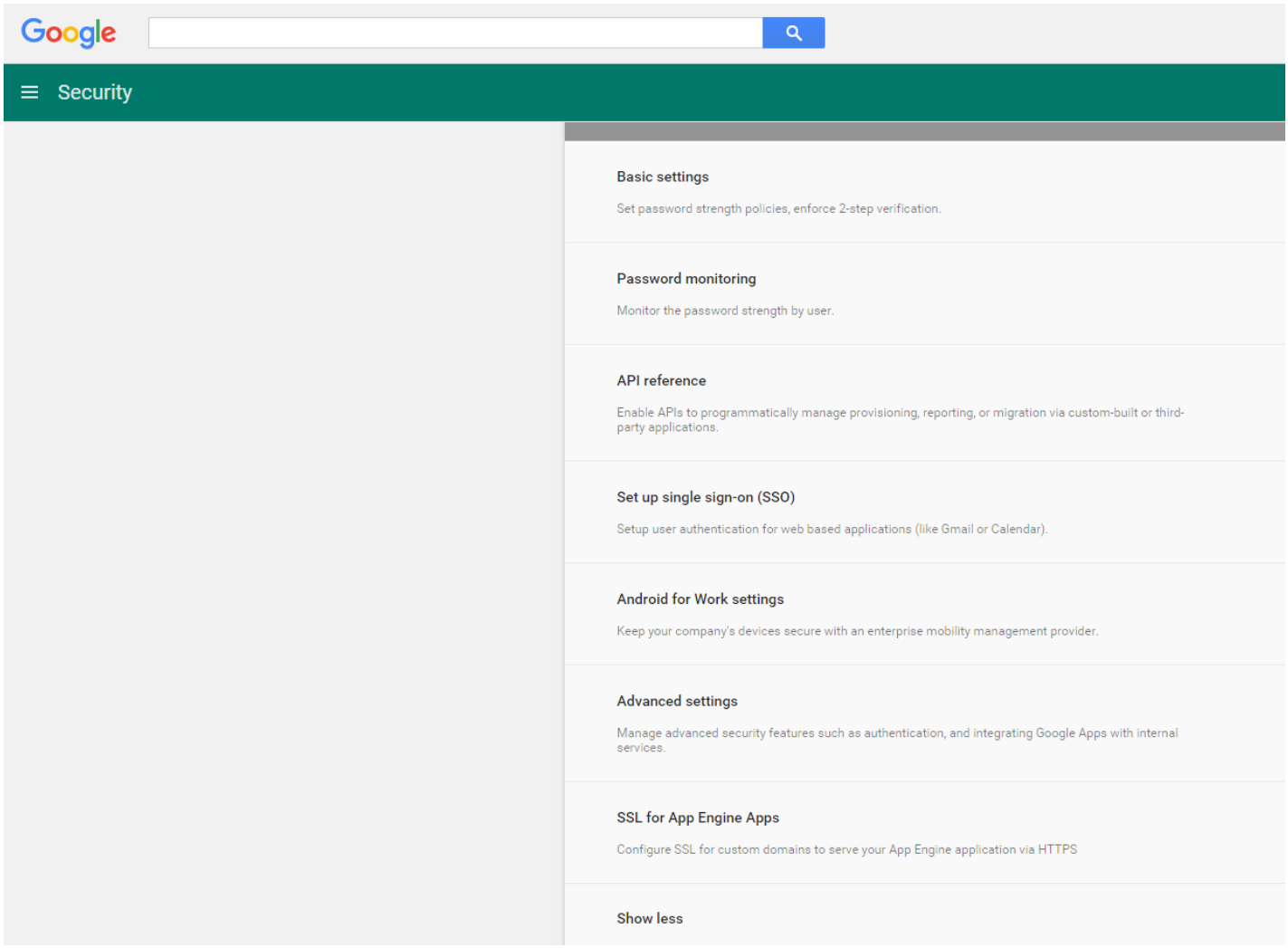


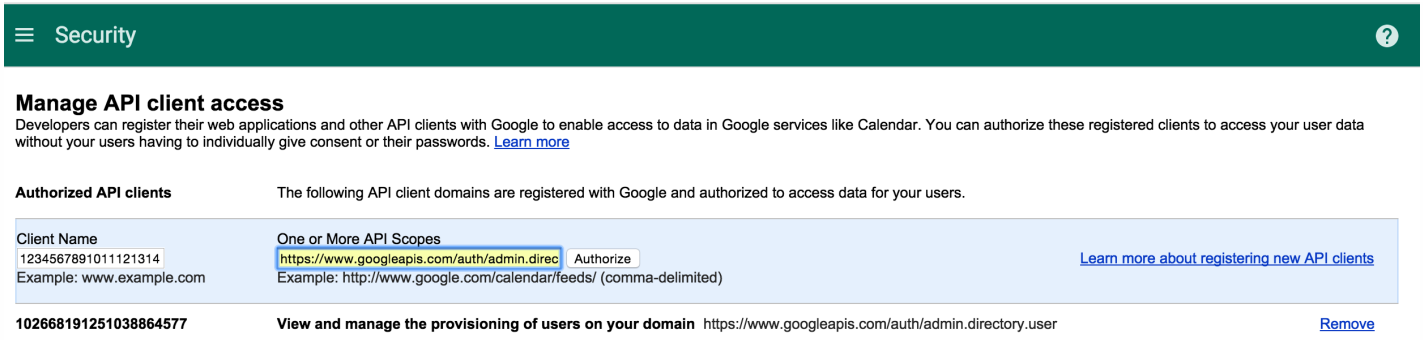




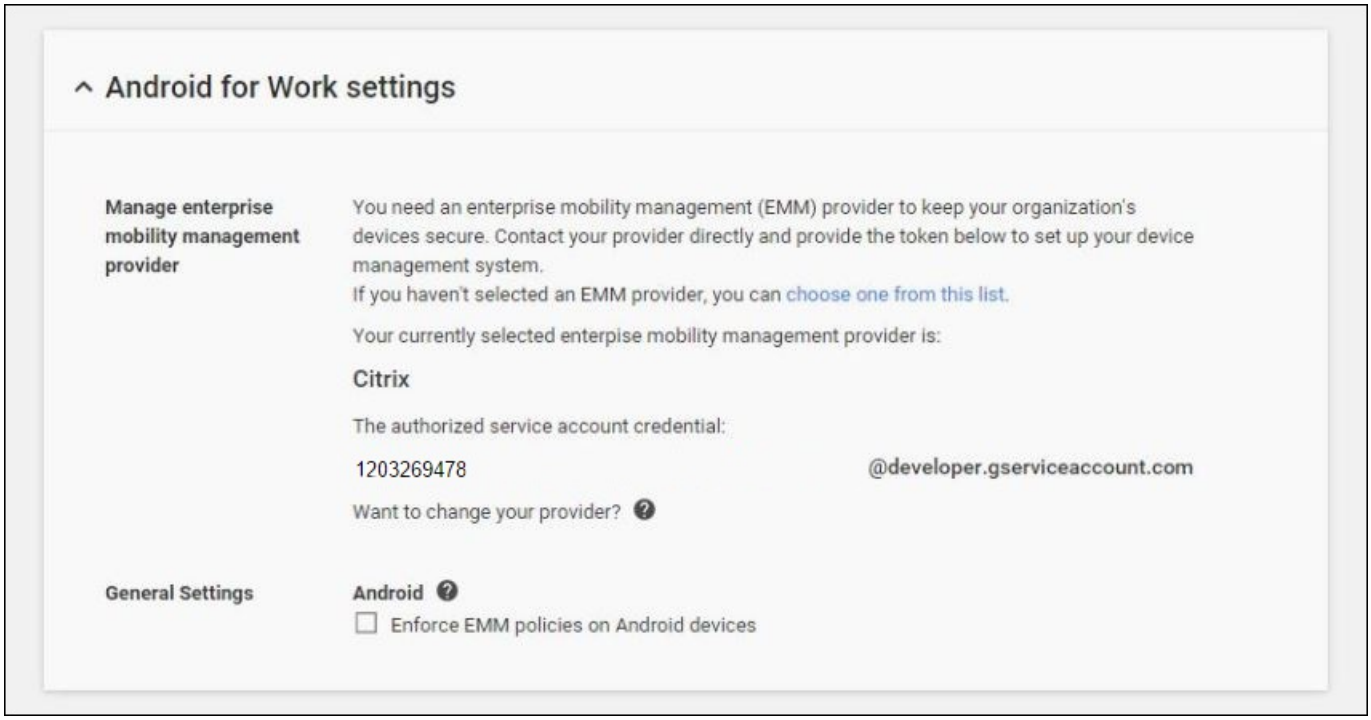




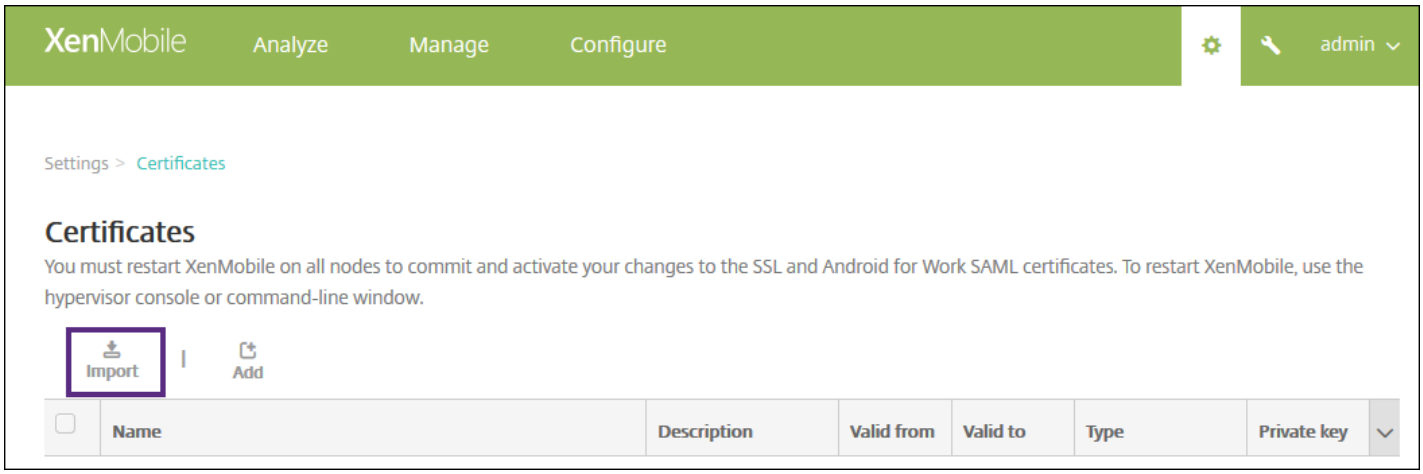


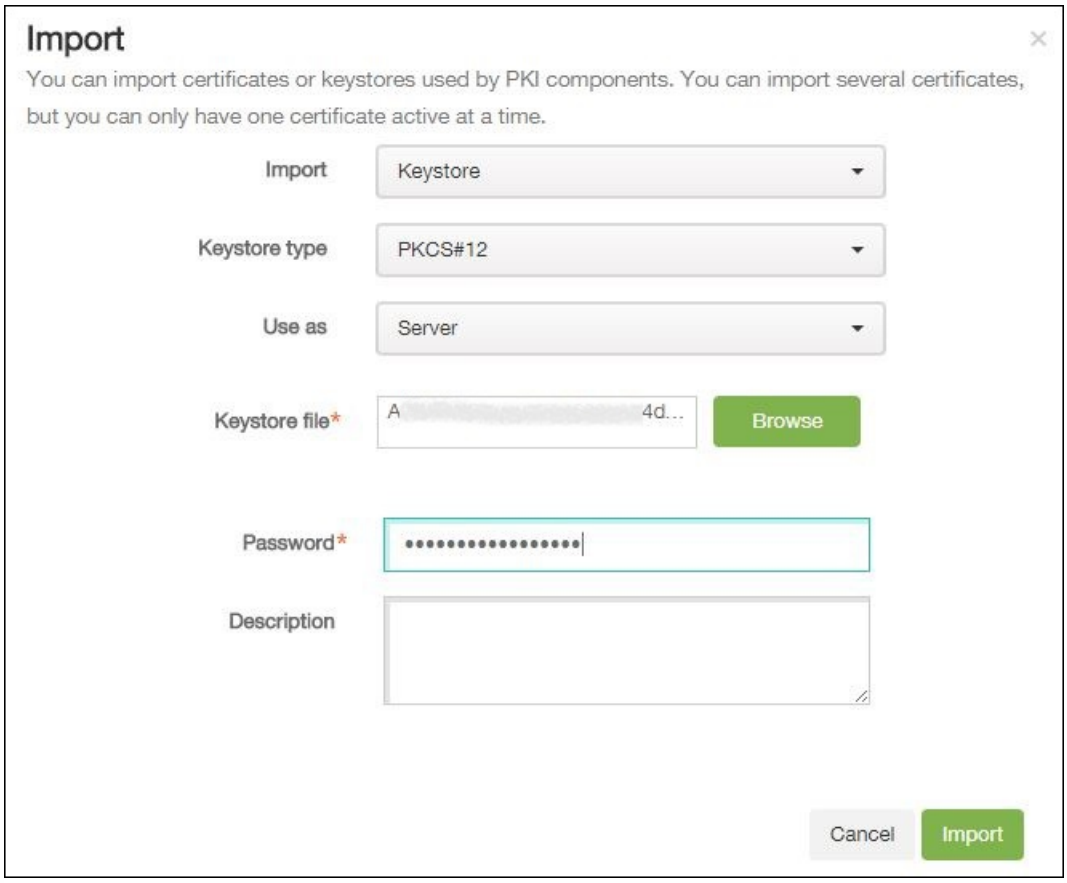


Binding to EMM



Import P12 certificate

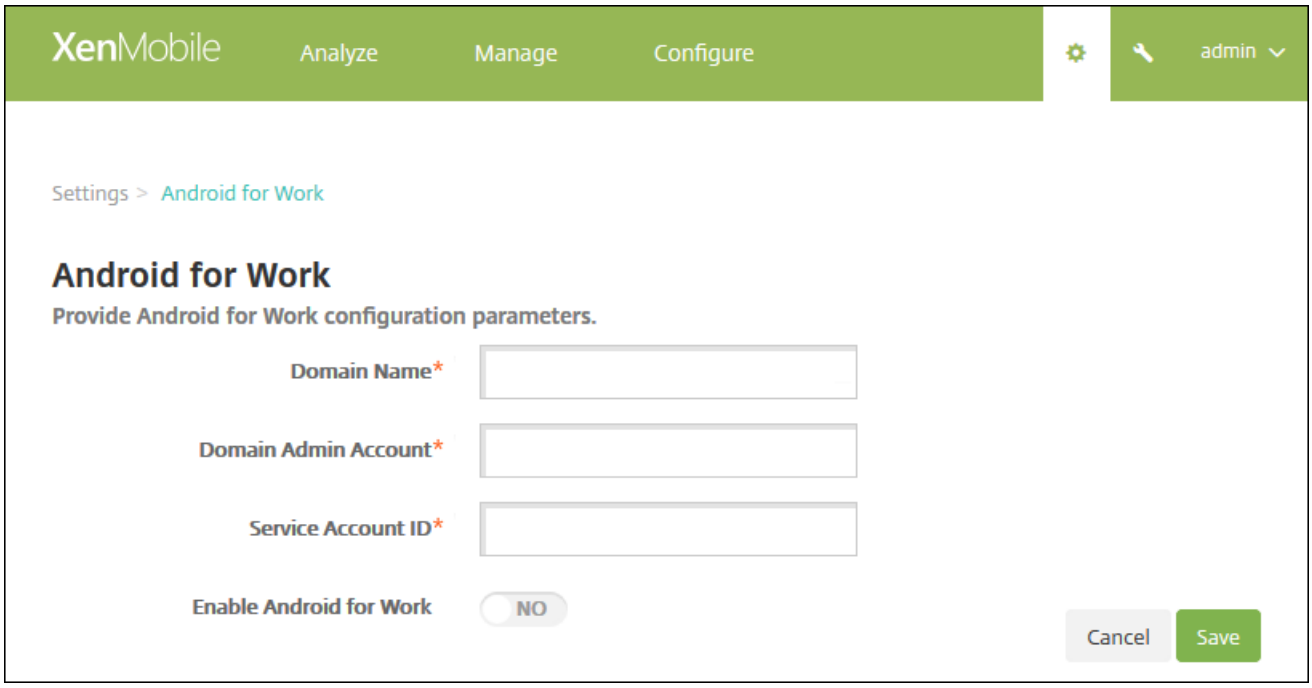




-
-

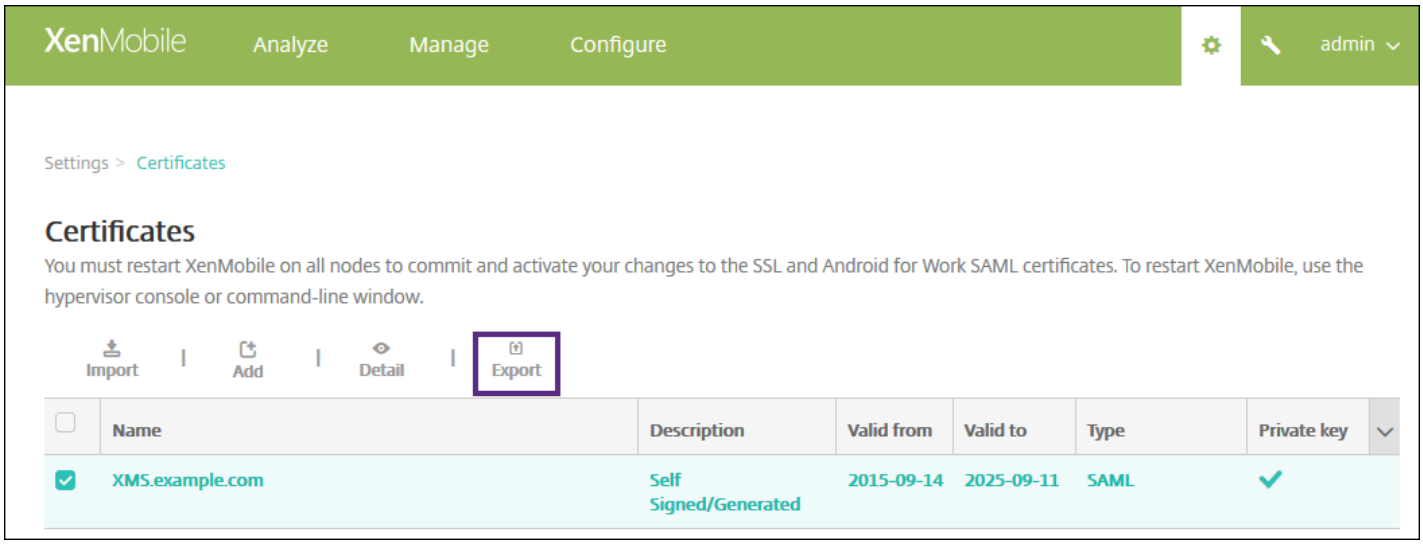
-
-
-
-

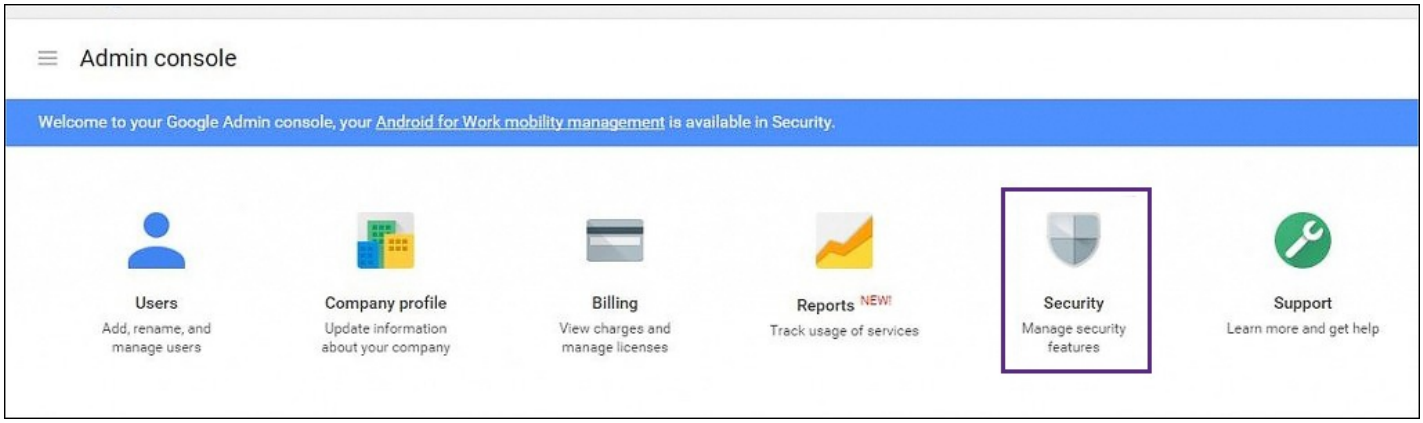
Set up Android for Work server settings

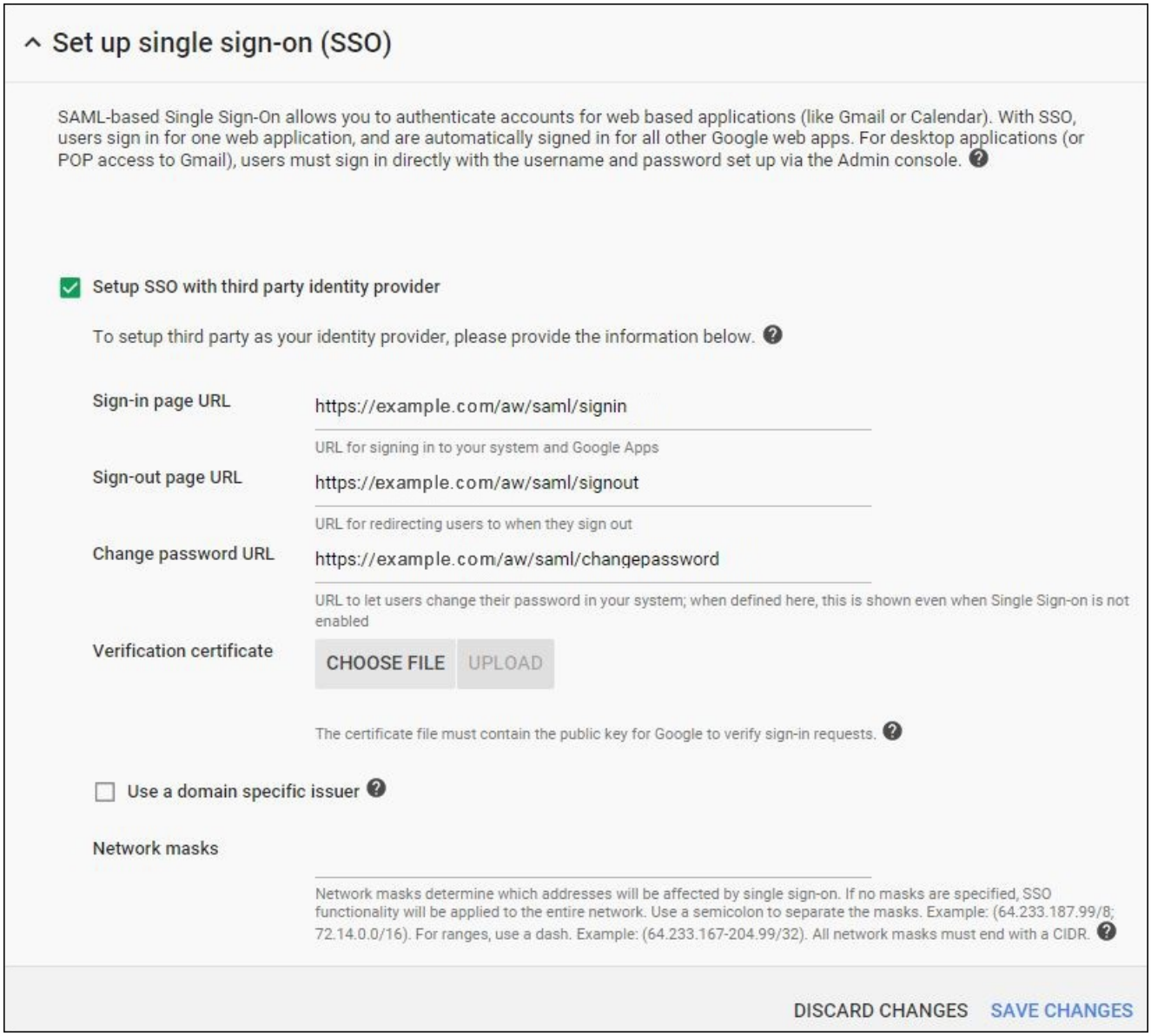


-
-
-
-

Enable SAML-based single-sign-on

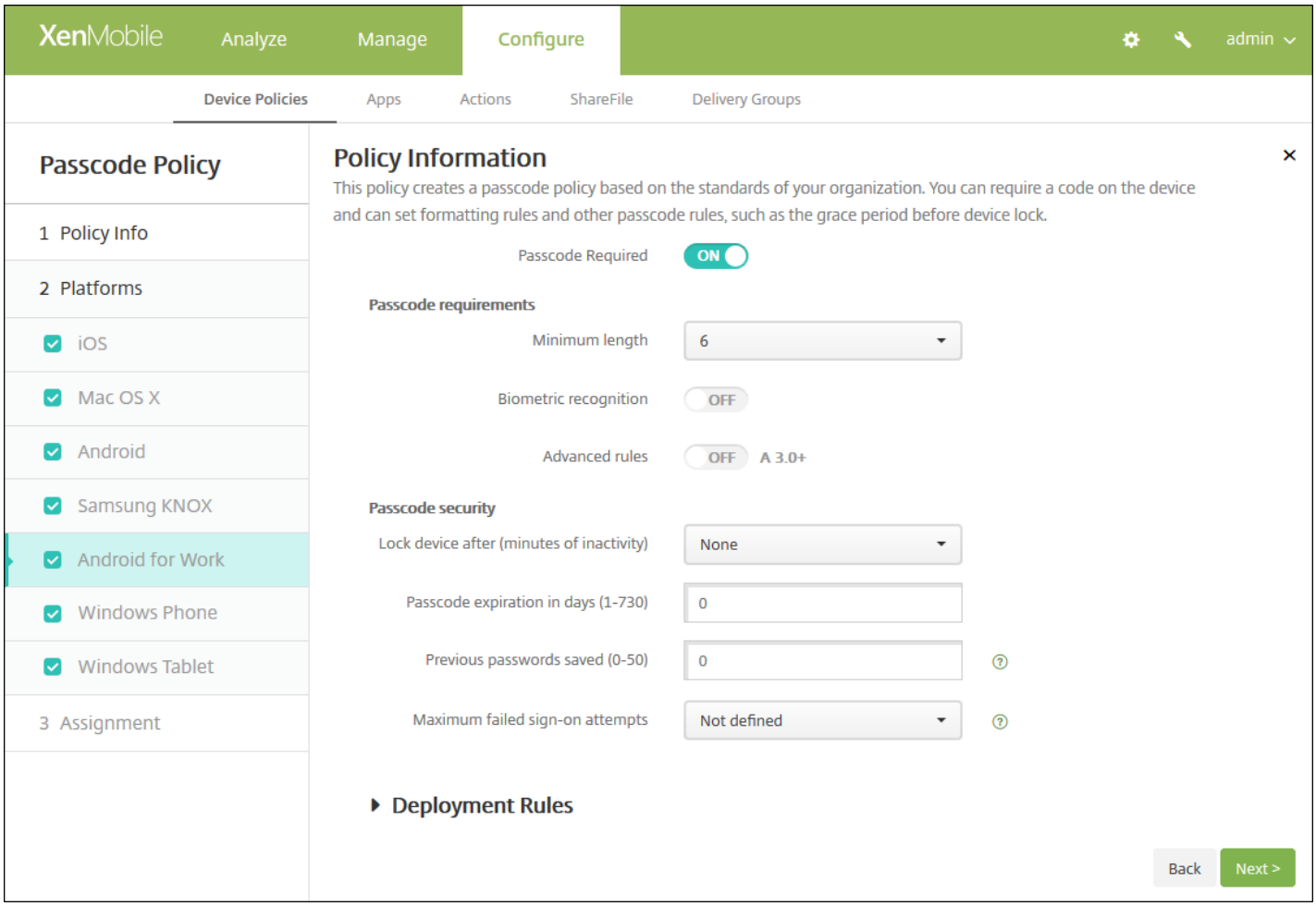


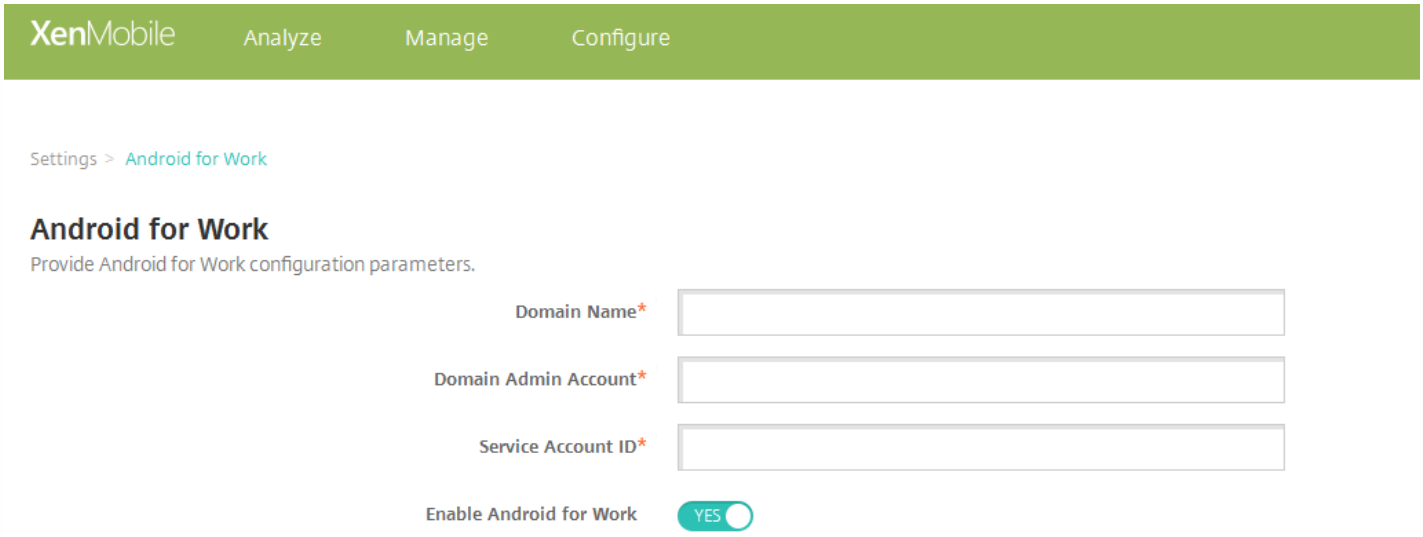




-
-
-
-

Set up an Android for Work device policy





Prerequisites

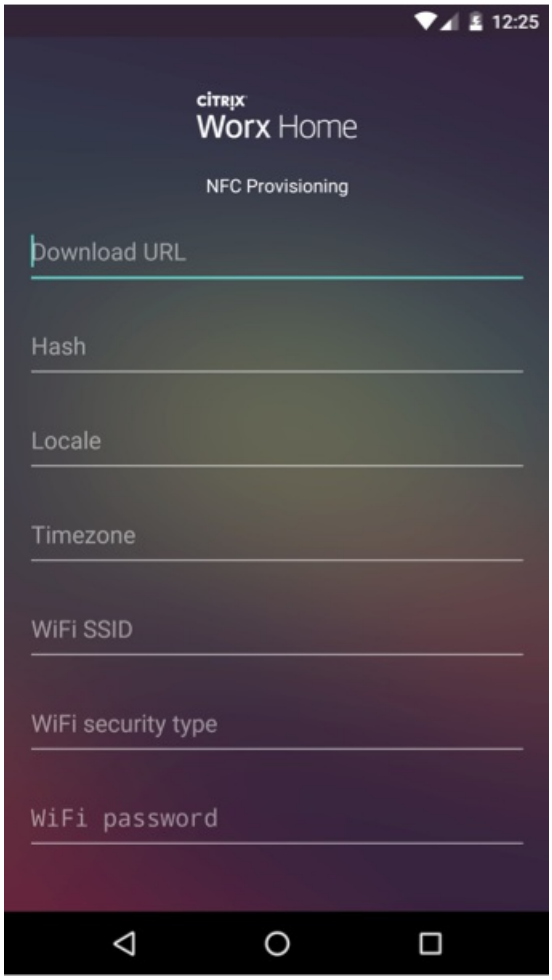
-
-
-

NFC Bump in Device Owner mode

-
-
-
-

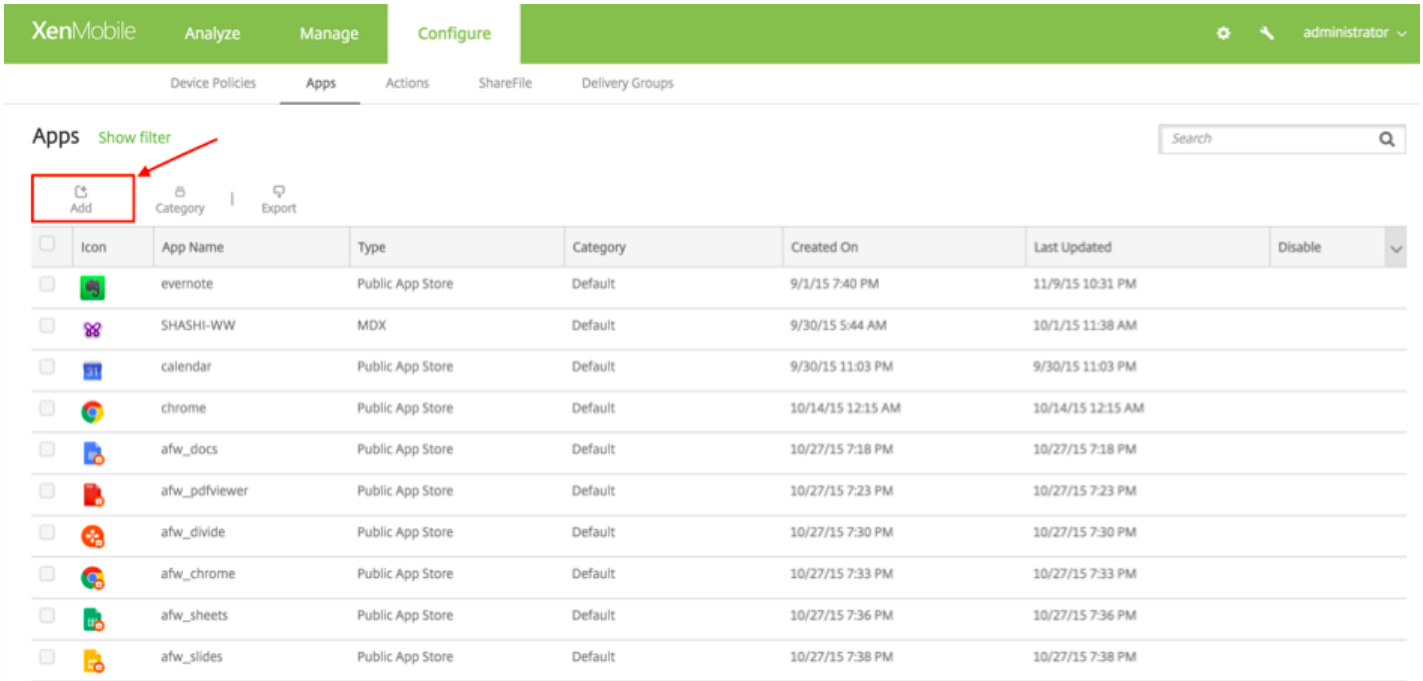
-
-

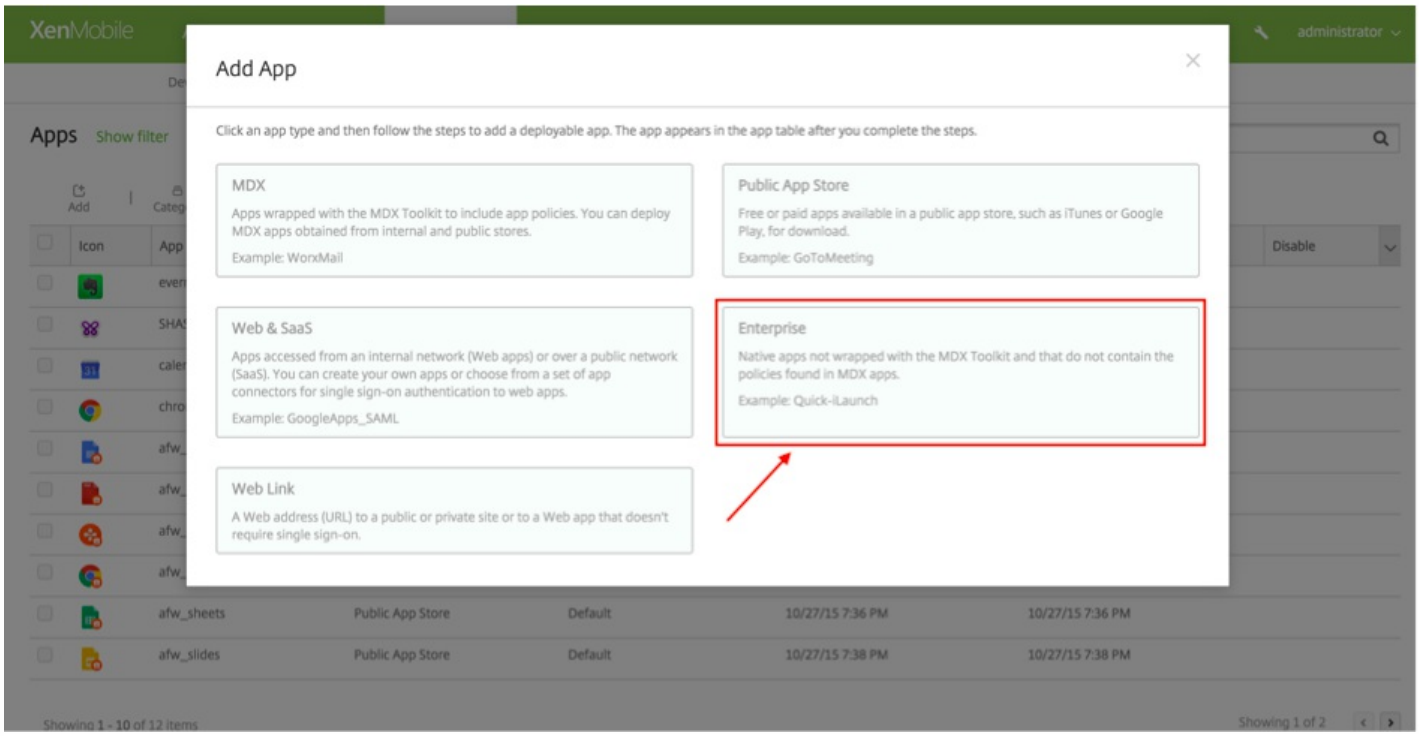
Configuring the Worx Provisioning Tool

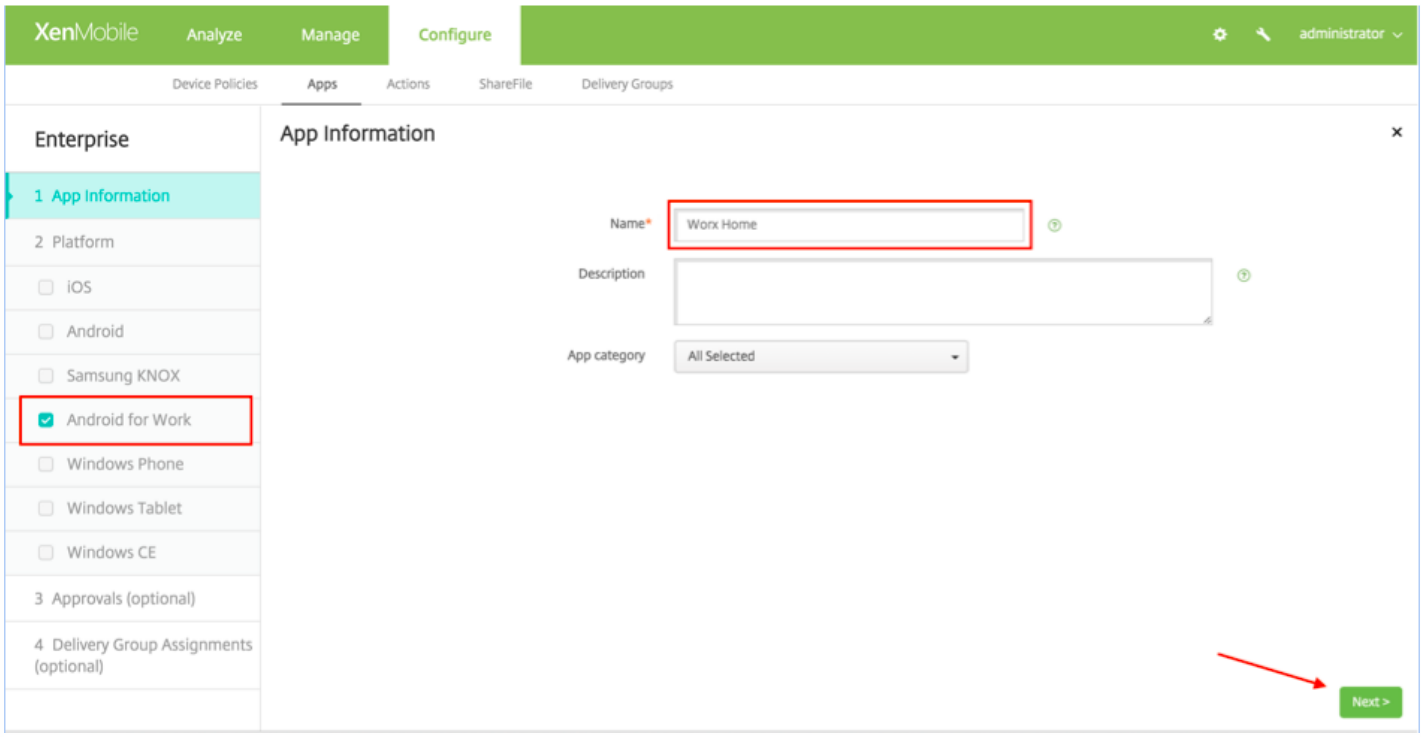


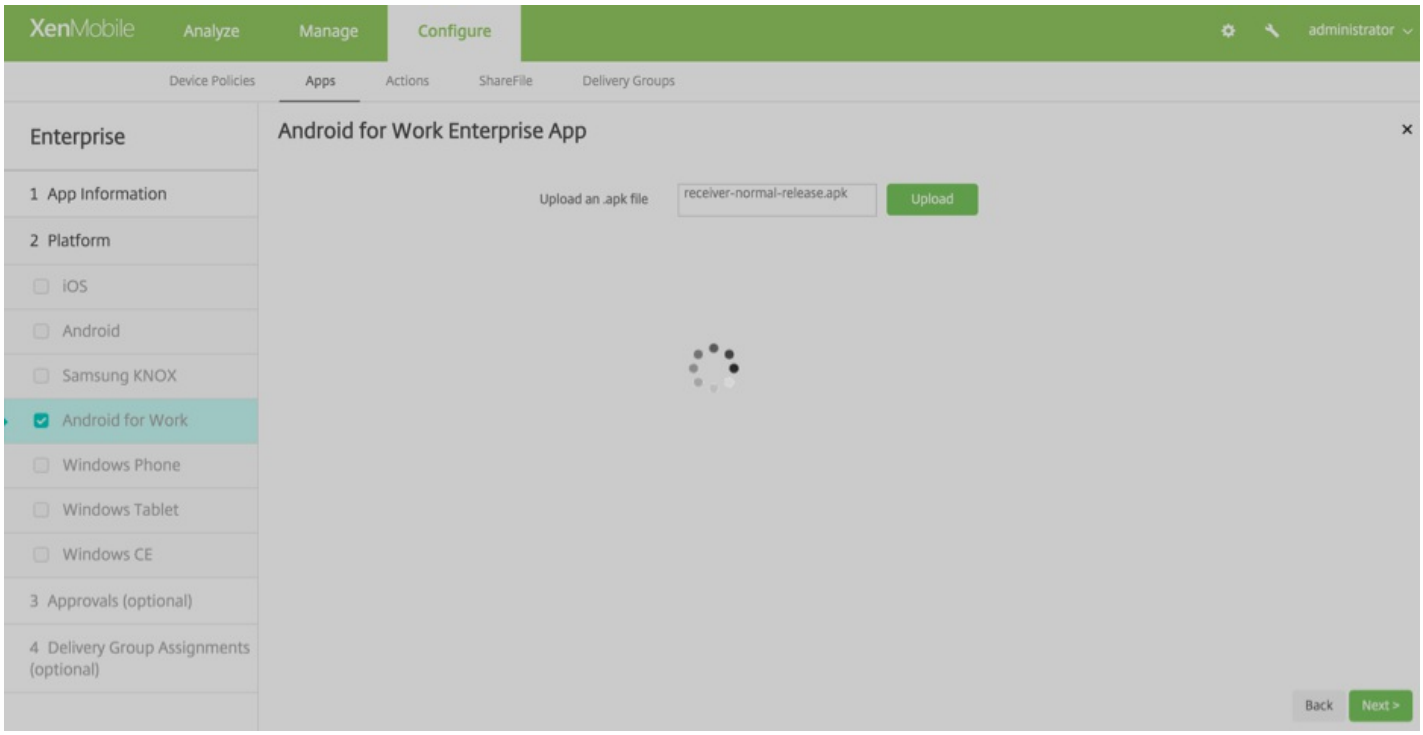
Configuring with text file

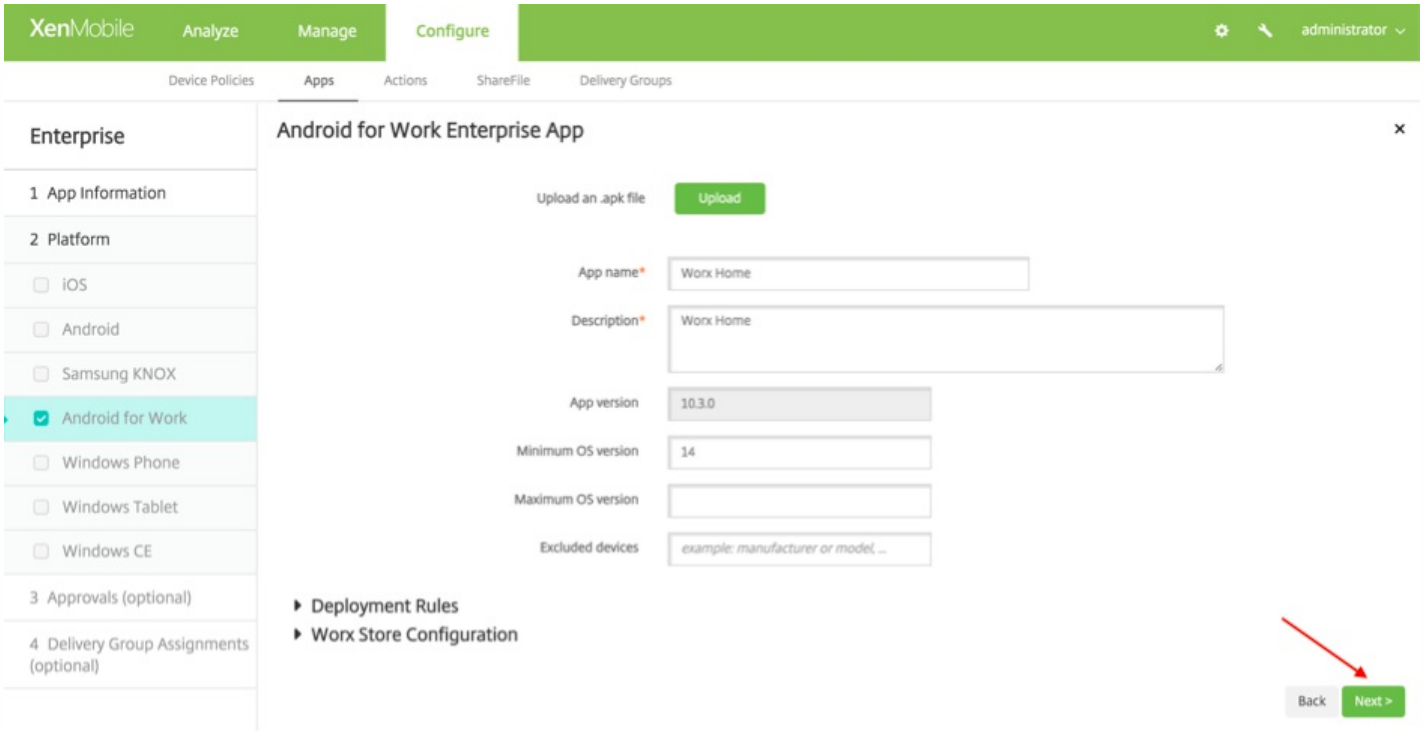
Getting the Worx Home checksum

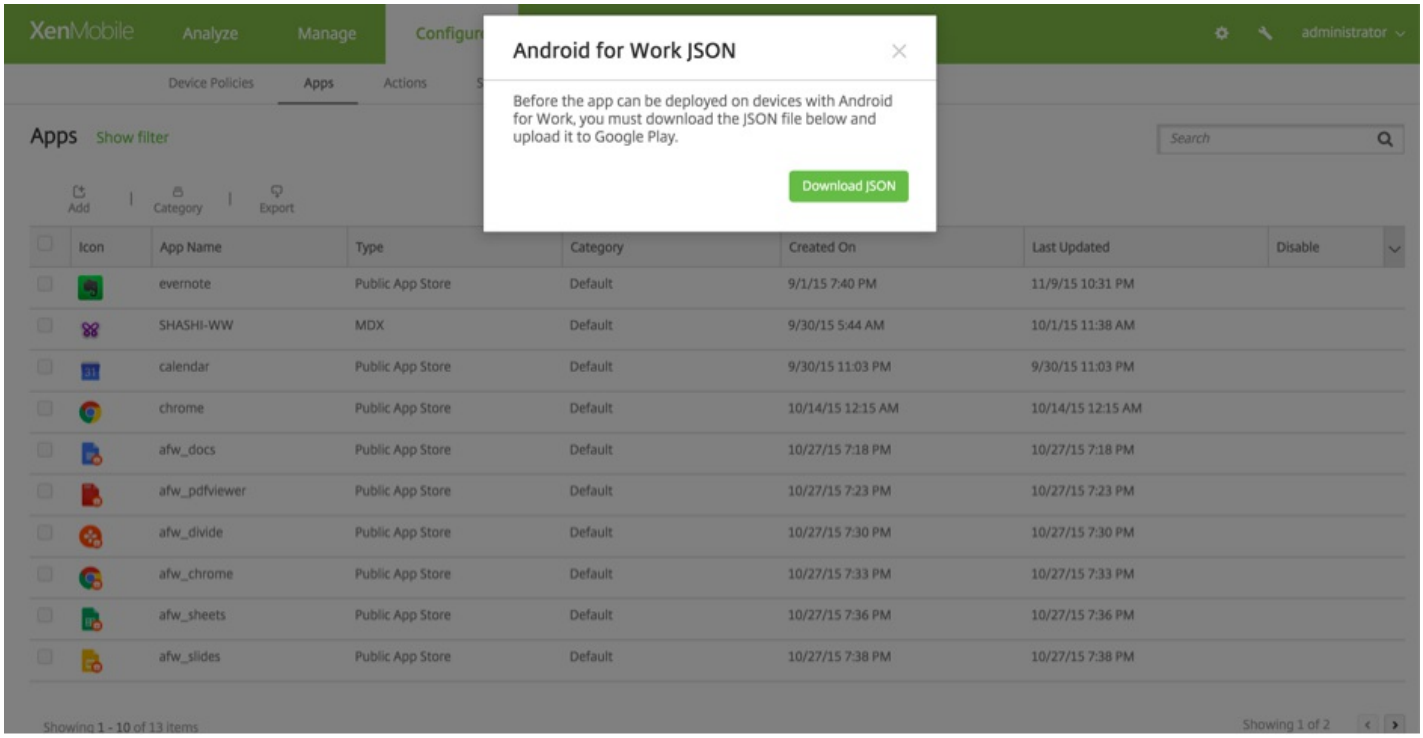










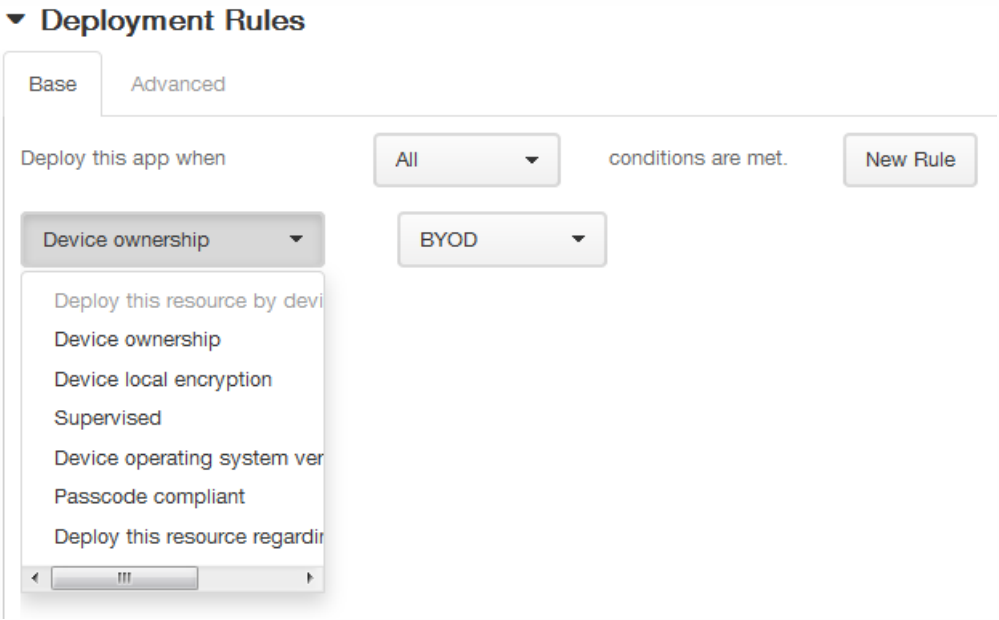


-
-
-

Libraries used

-
-
-
-

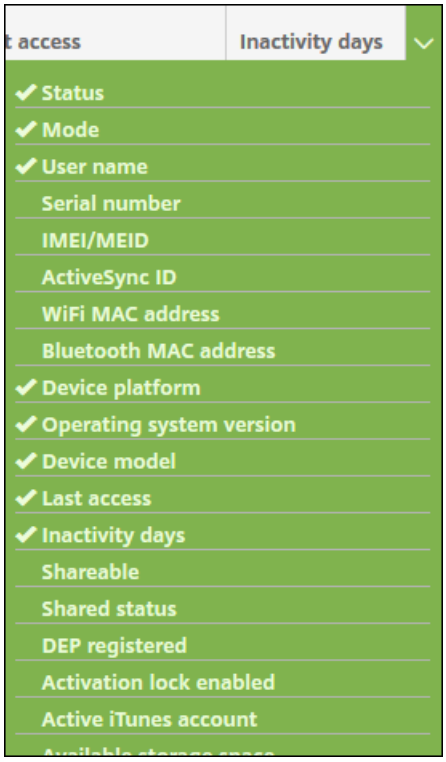
-
-



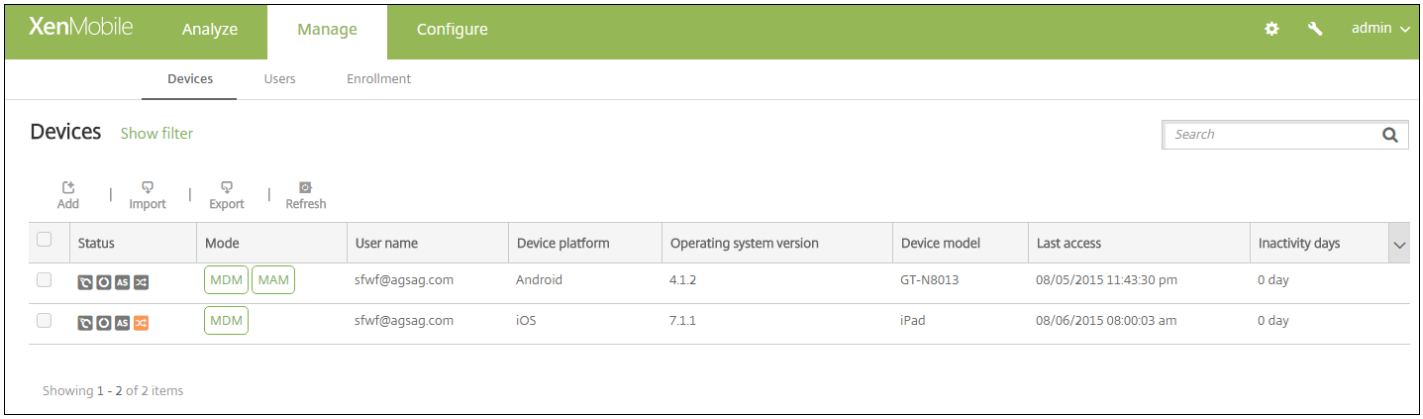
Base Deployment Rules

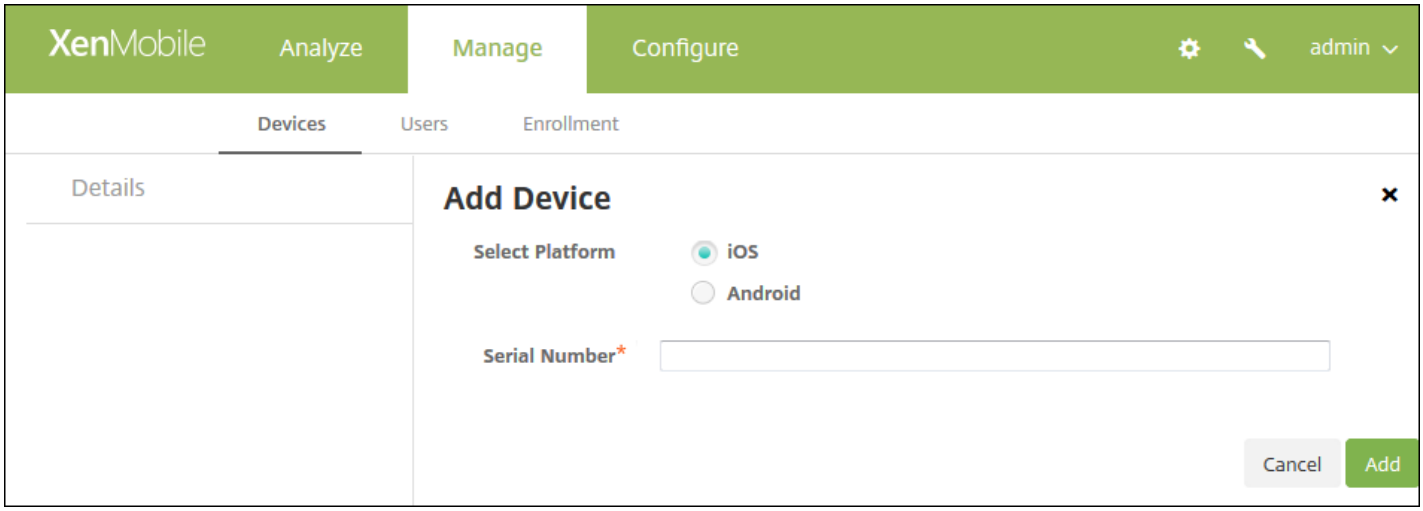
Advanced Deployment Rules

-
-
-
-
-
-

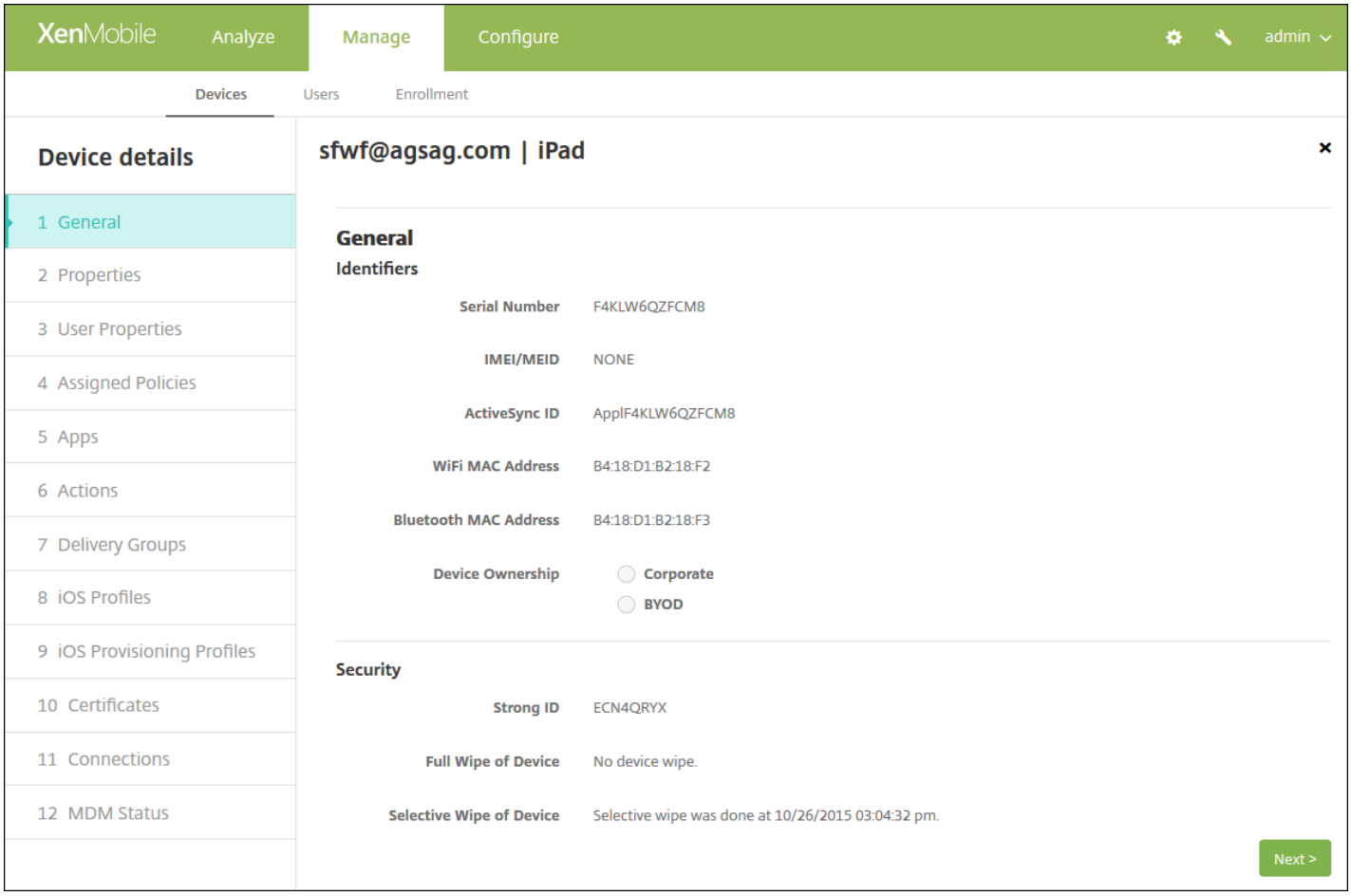


To add a device manually



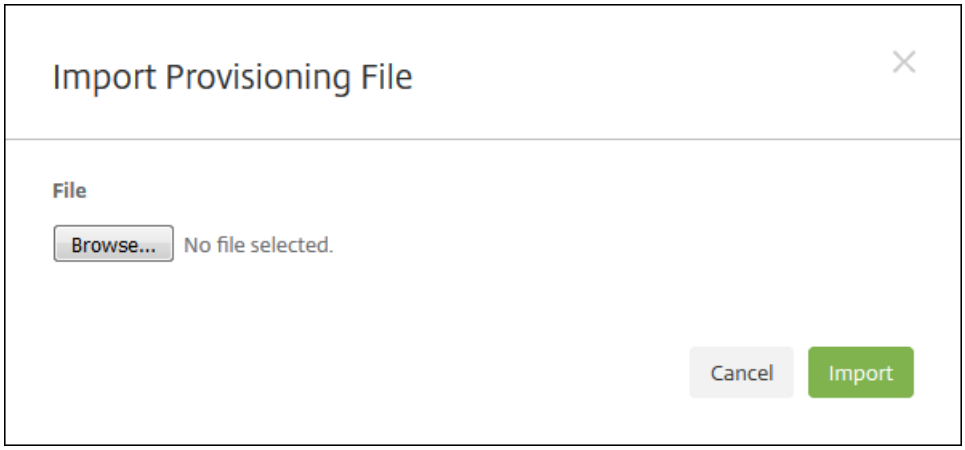


-
-
-

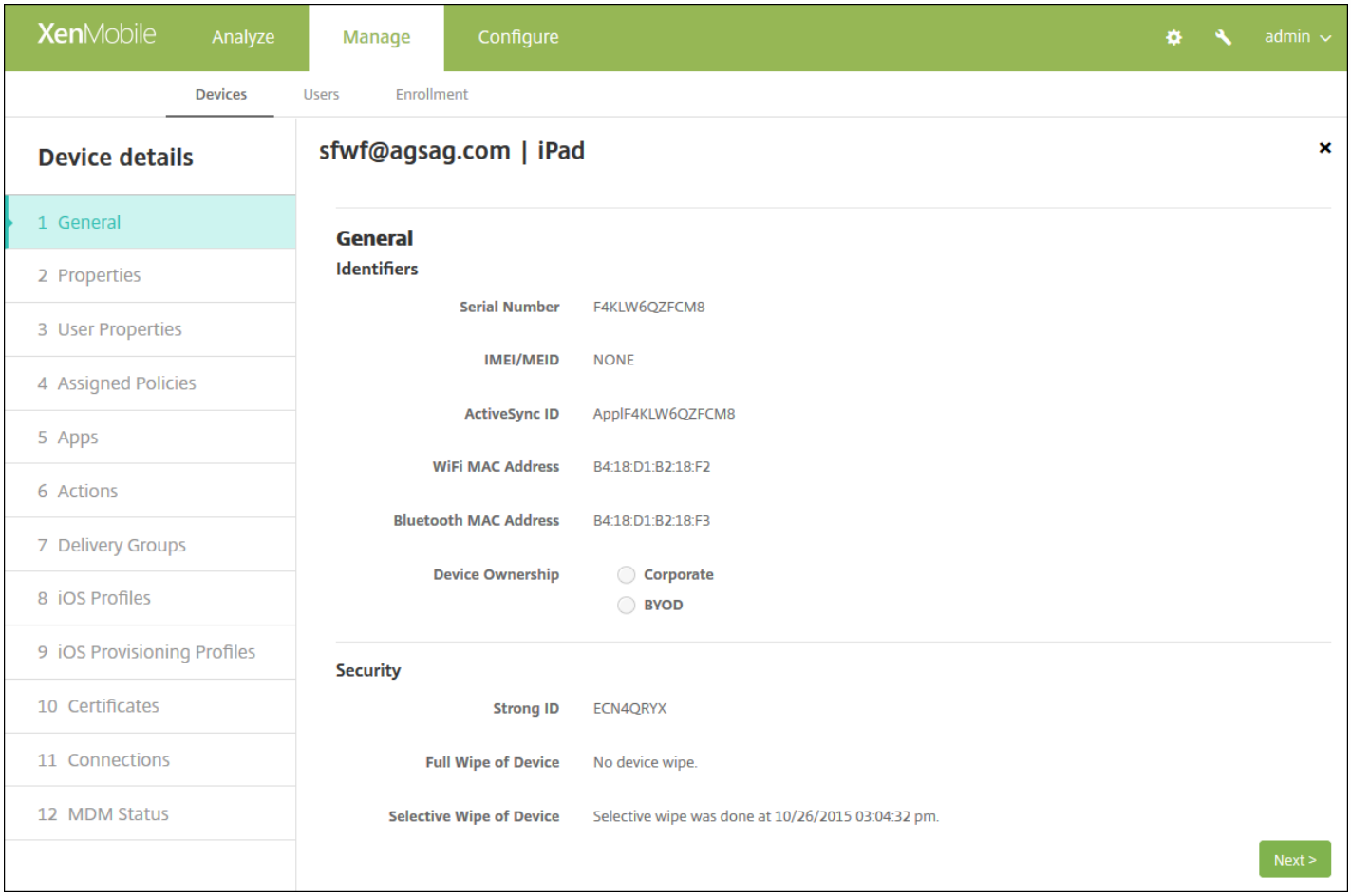


-
-
-
-
-
-
-
-
-
-
-
-
-

To import devices from a provisioning file

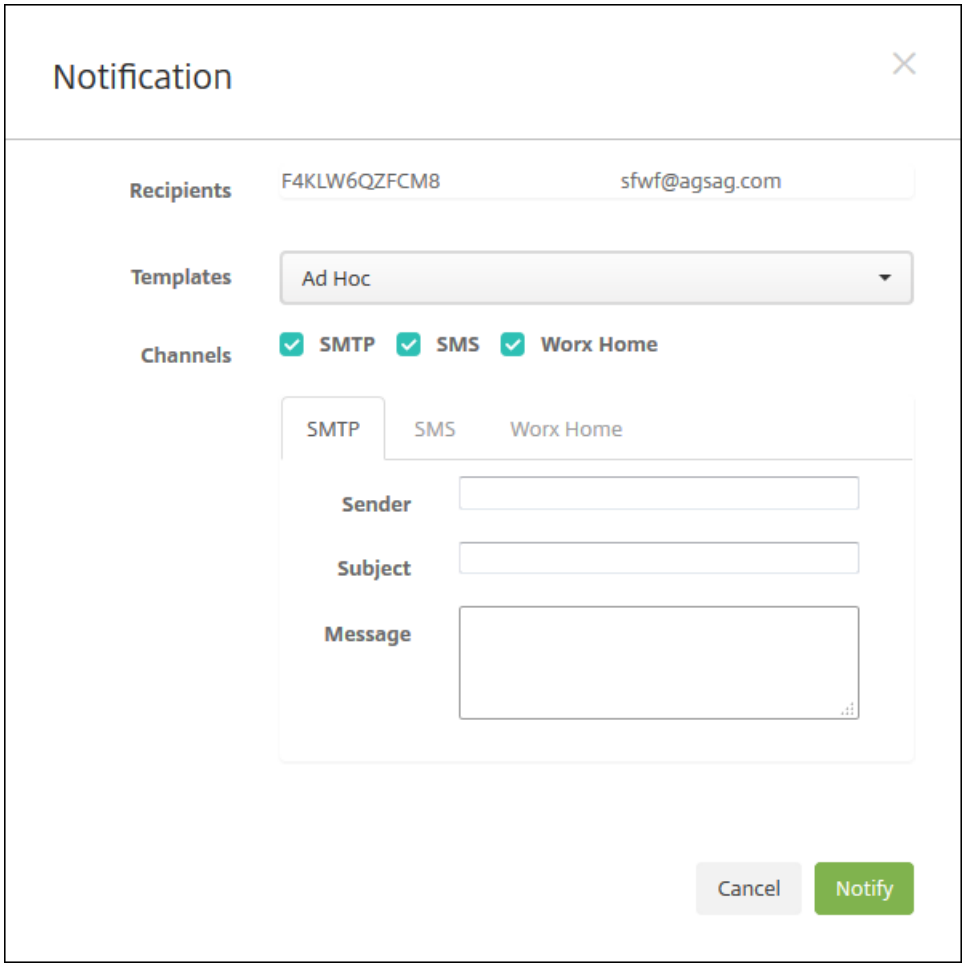


To edit devices



-
-
-
-
    -
-
-

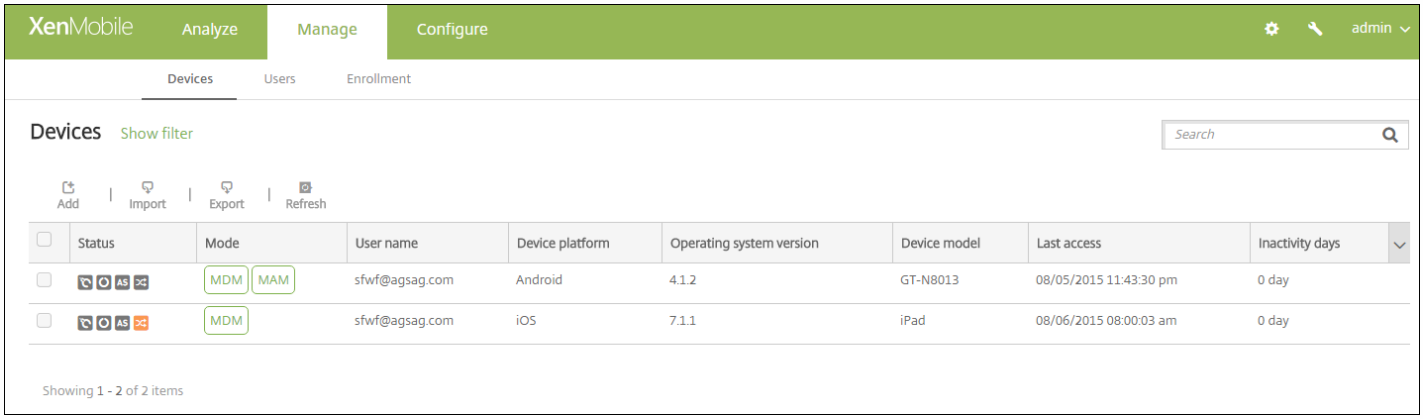
To send a notification to devices

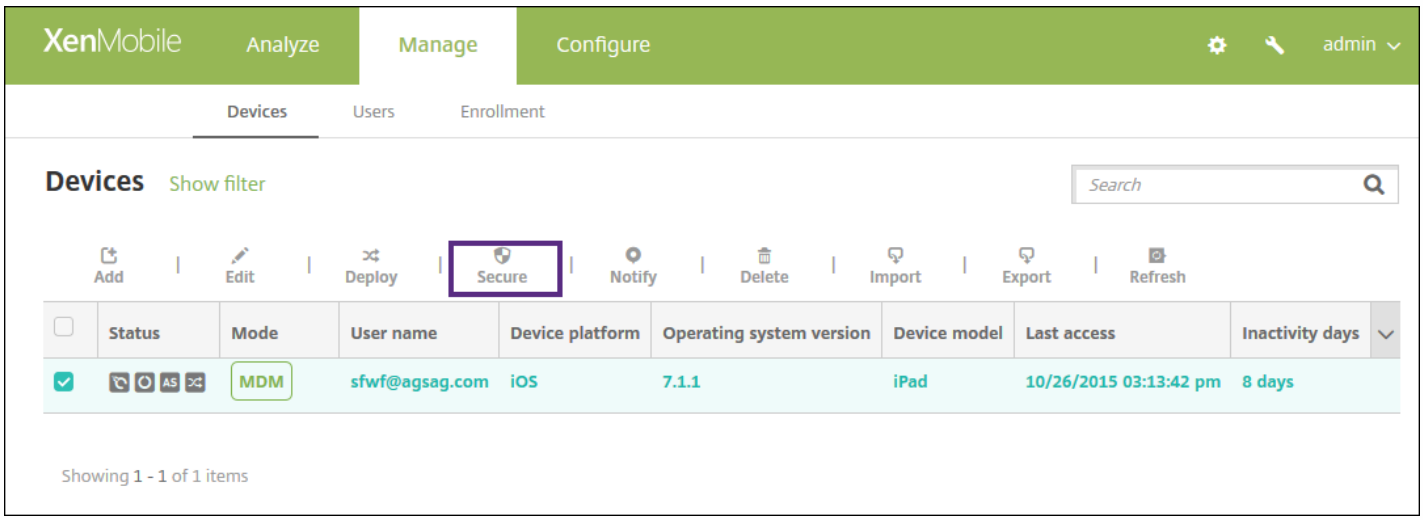


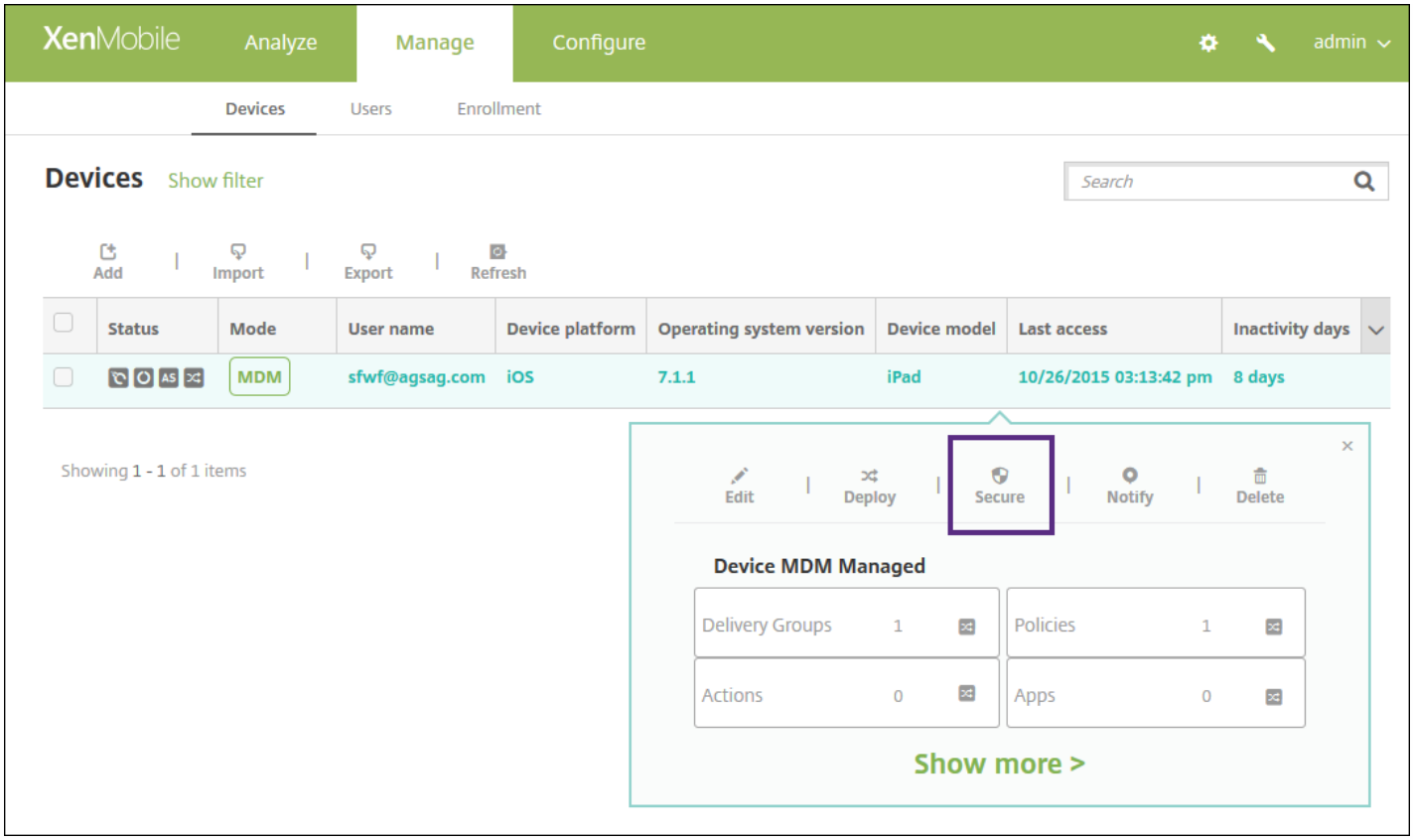
-
-
-
-
-

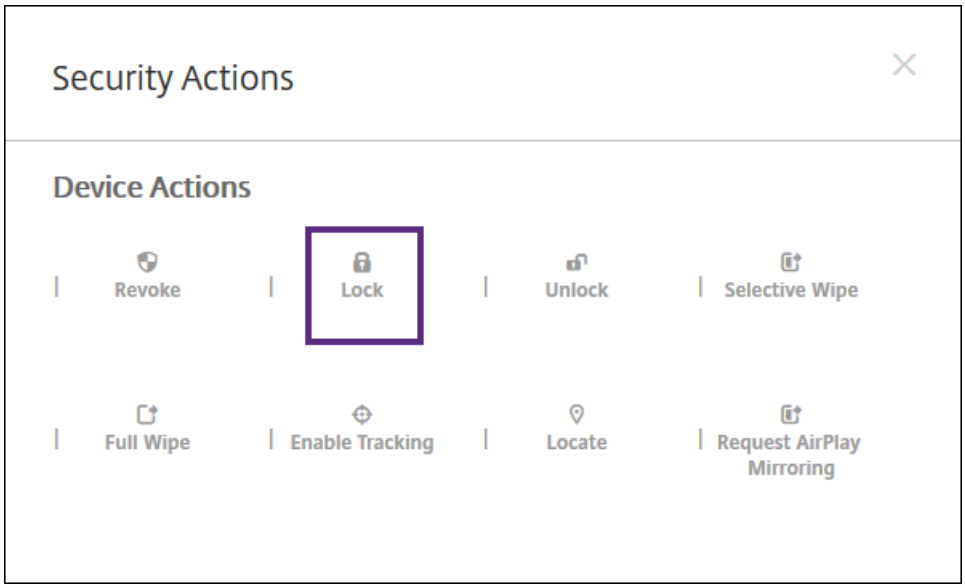
To delete devices

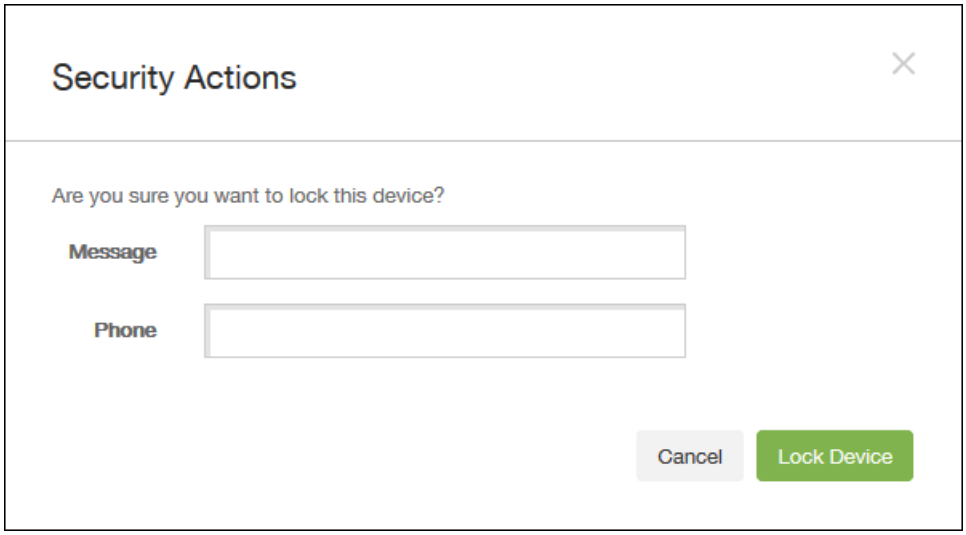
To export the Devices table



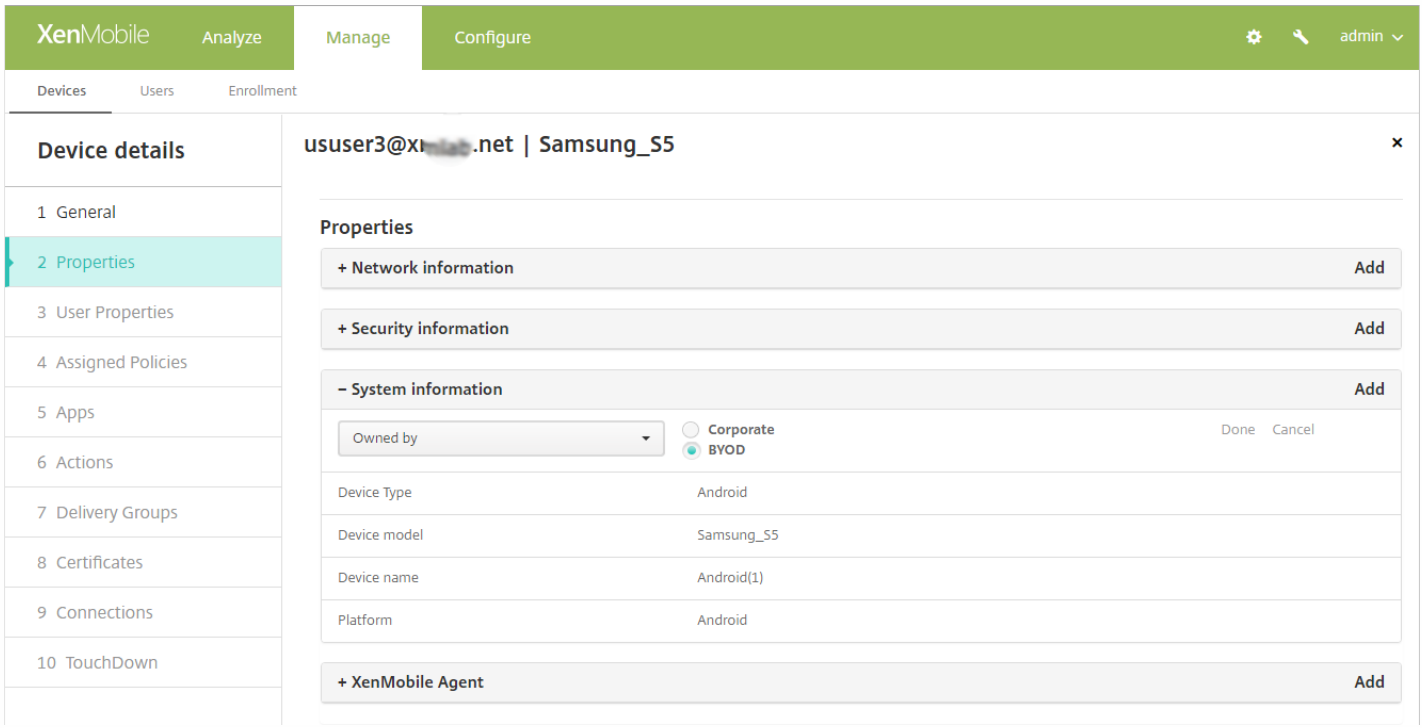








-
-
-



-
-

-
-
-
-

Example of a device provisioning file

-
-
-
-
-

-
-

	• •

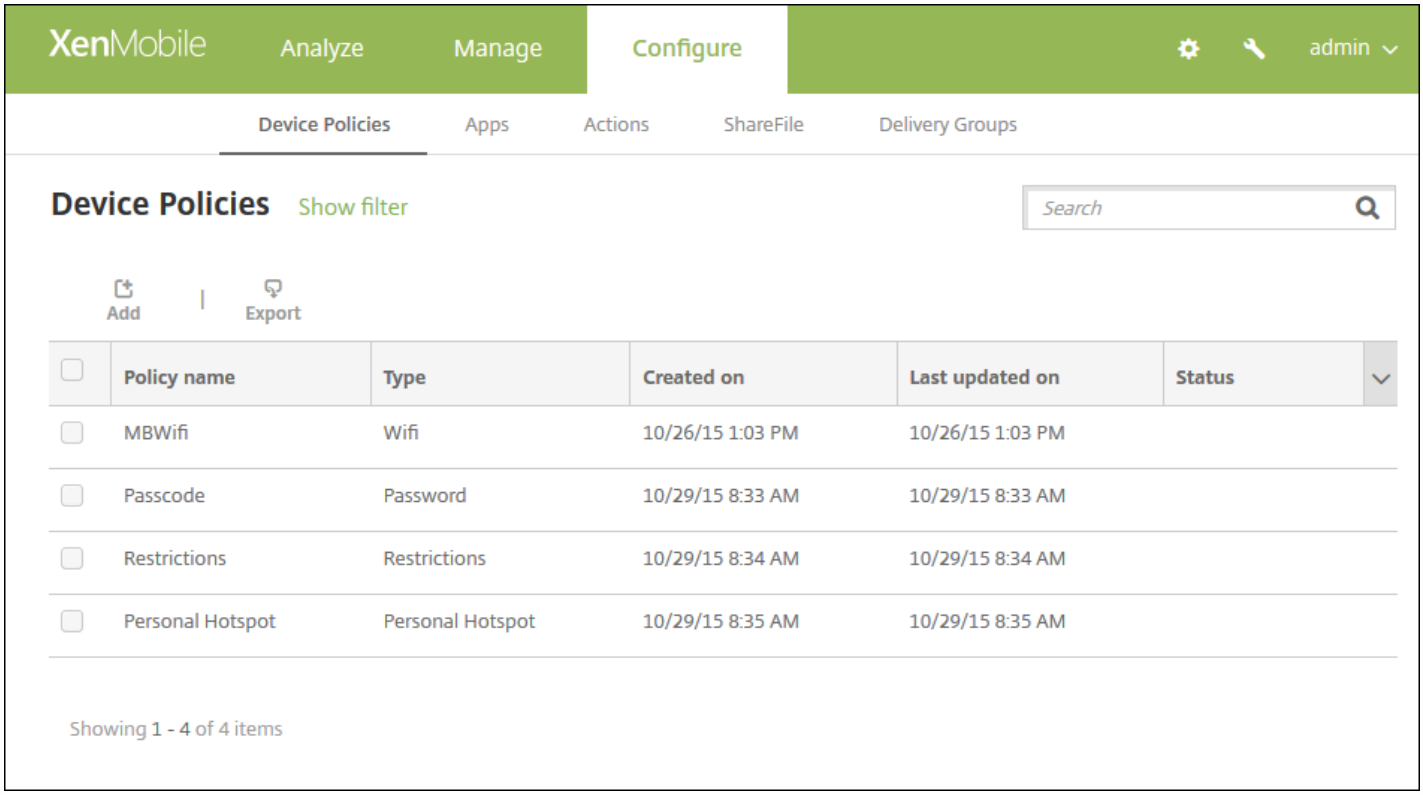
	• • • • • • • • • • • • • • • •
	• •

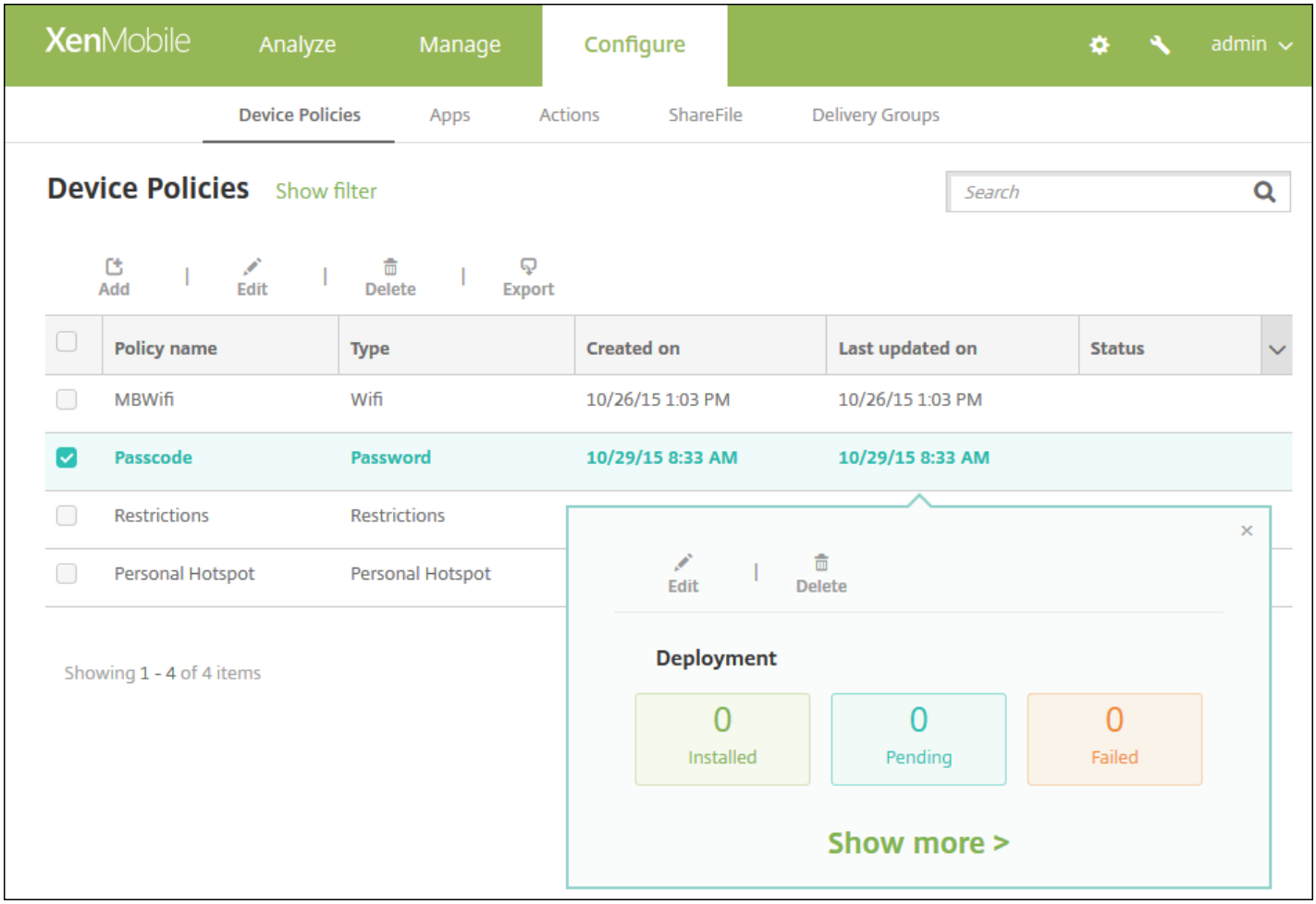
	• • •
	• •

	• •
	• •

	• •

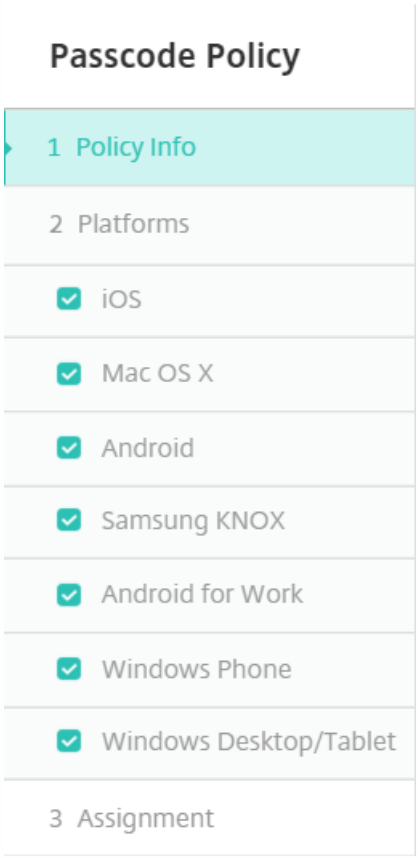
The Device Policies Page in the Console

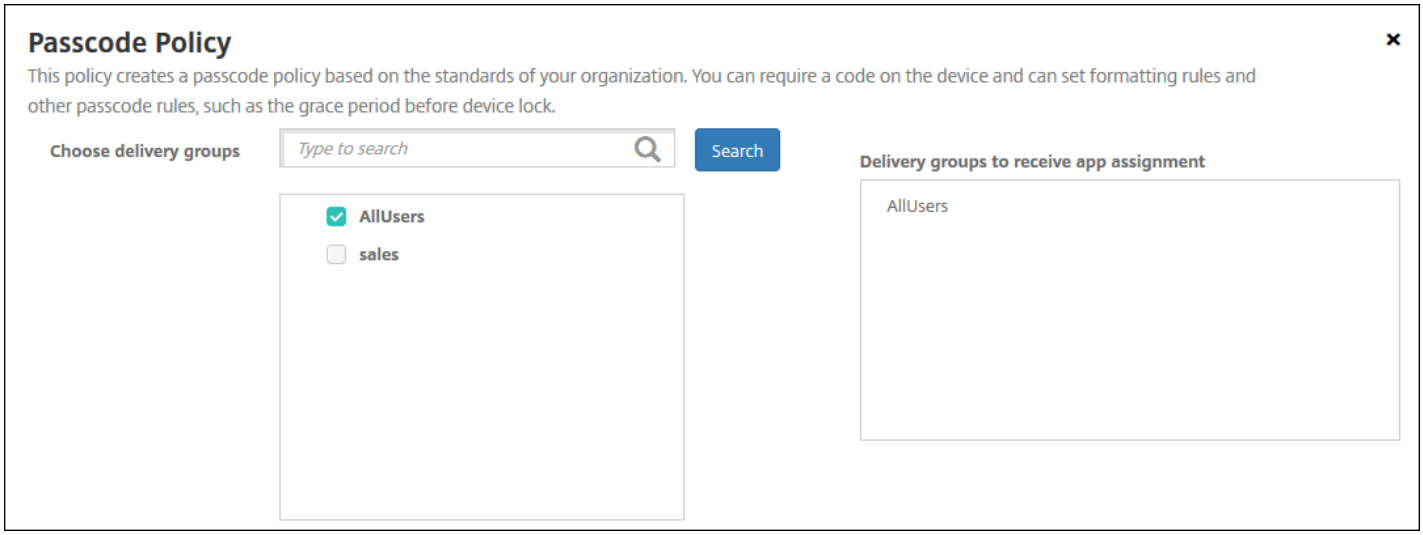




To add a device policy

-
-

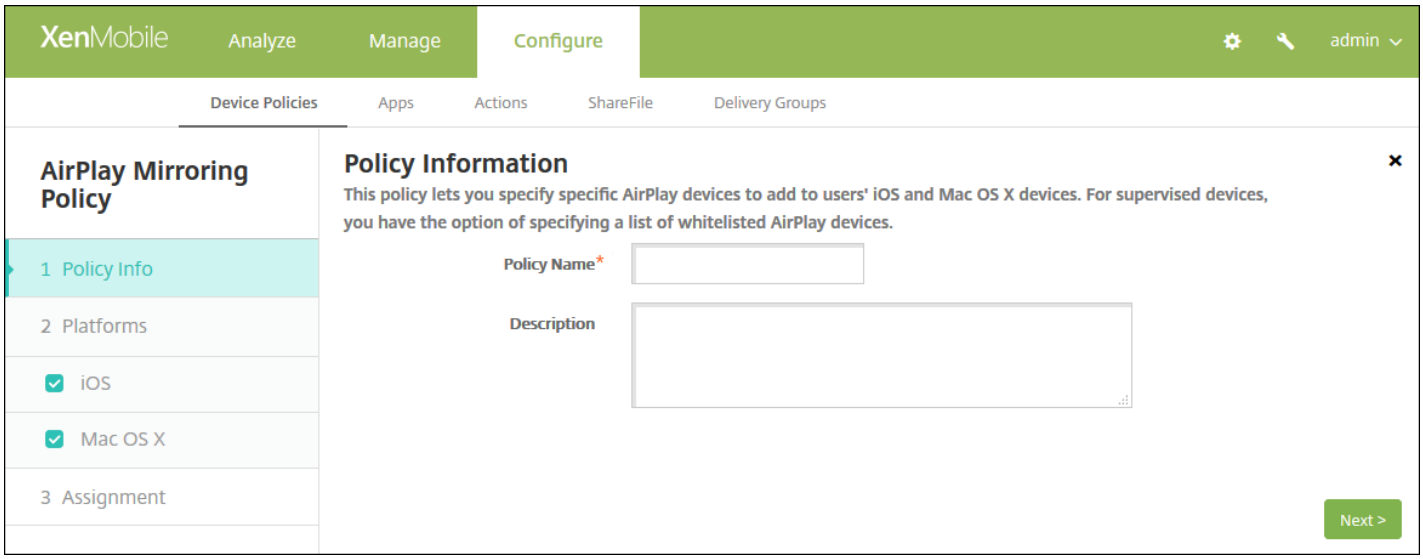




To edit or delete a device policy

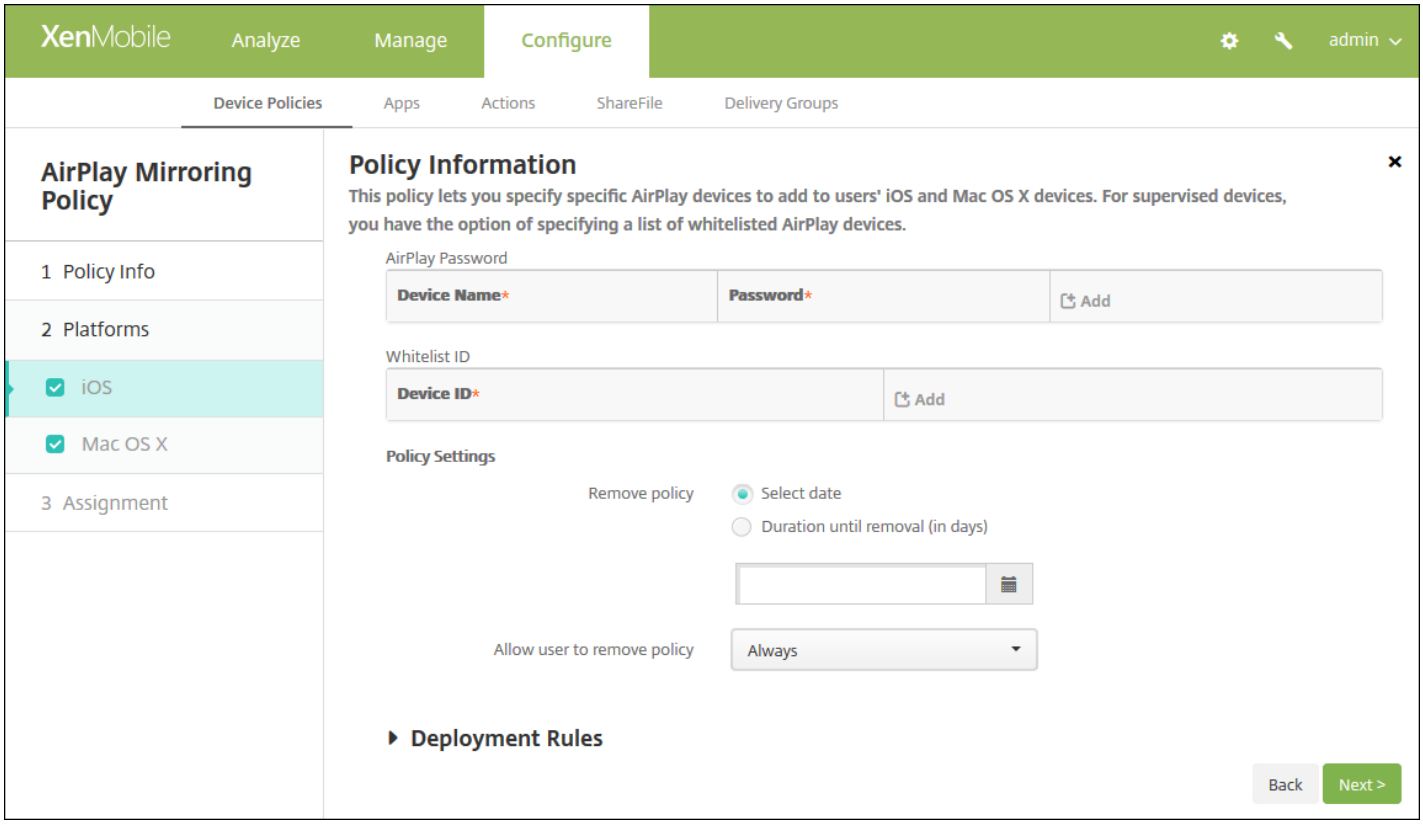
-
-

-
-
-
-
-
-
-
-
-
-
-



-
-

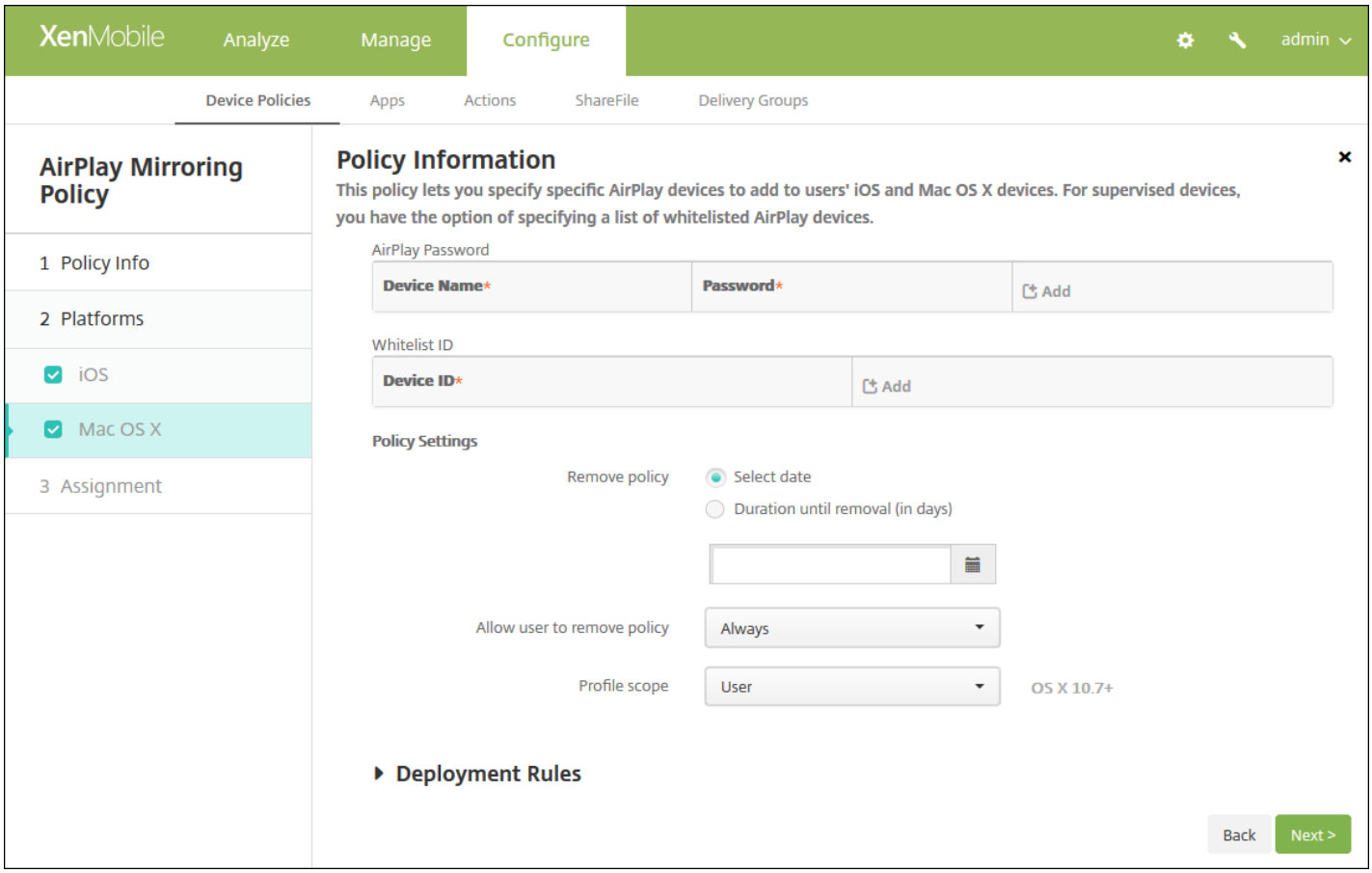
Configure iOS settings



-
  -
  -
  -
-
  -
  -
-
  -
  -

-
-

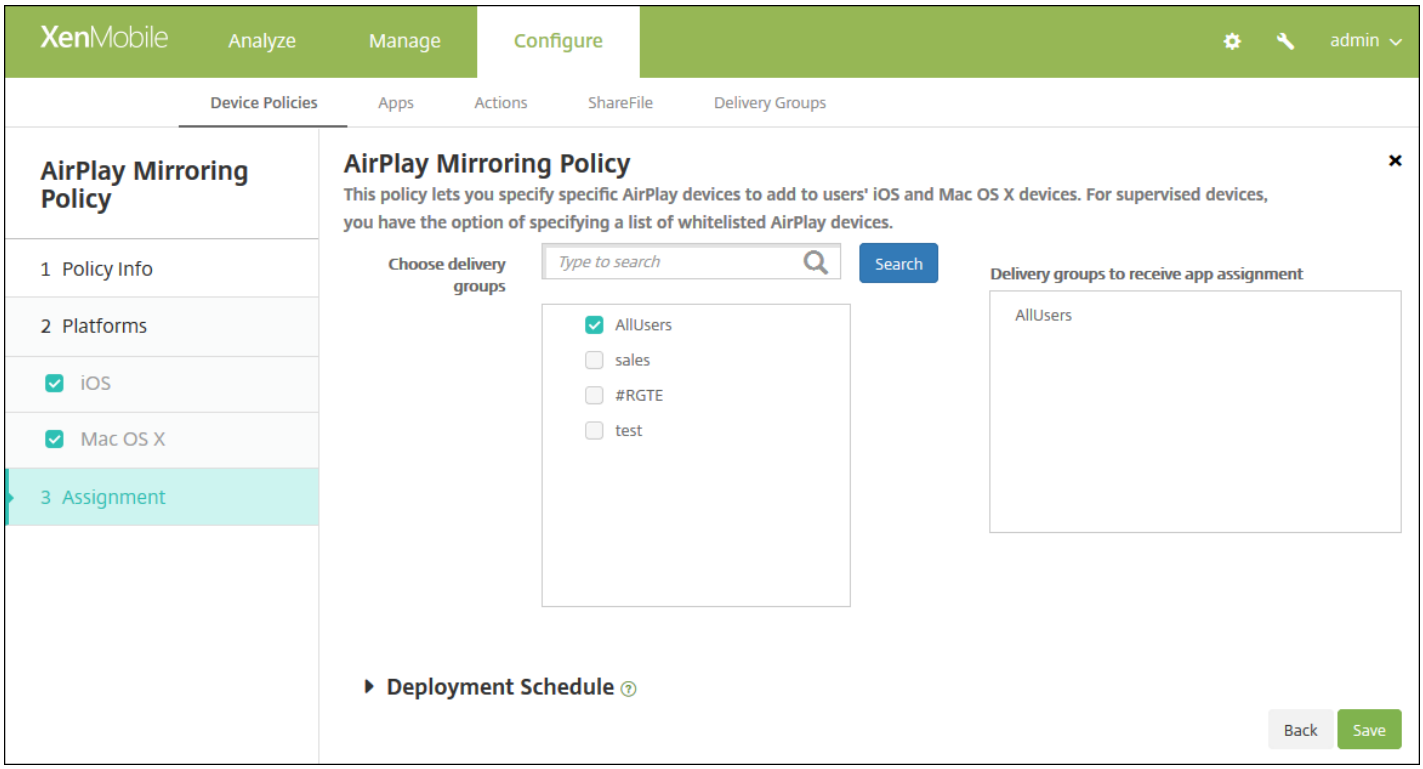
Configure Mac OSX settings



-
  -
  -
  -
-
  -
  -

-
  -
  -
  -
  -
  -

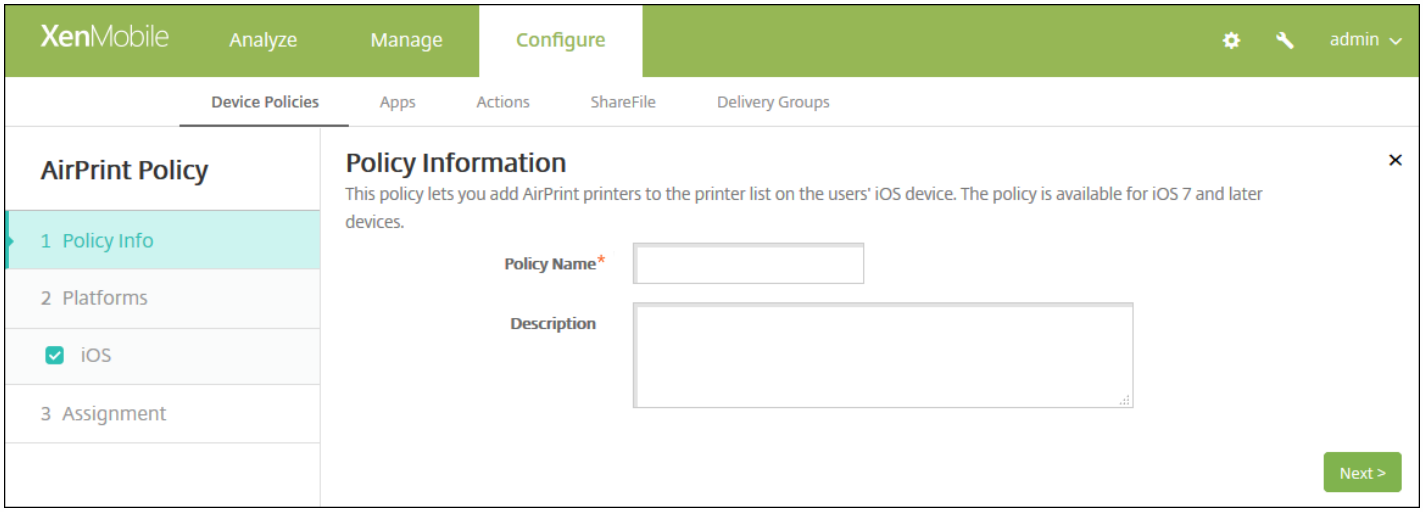
7. Configure deployment rules



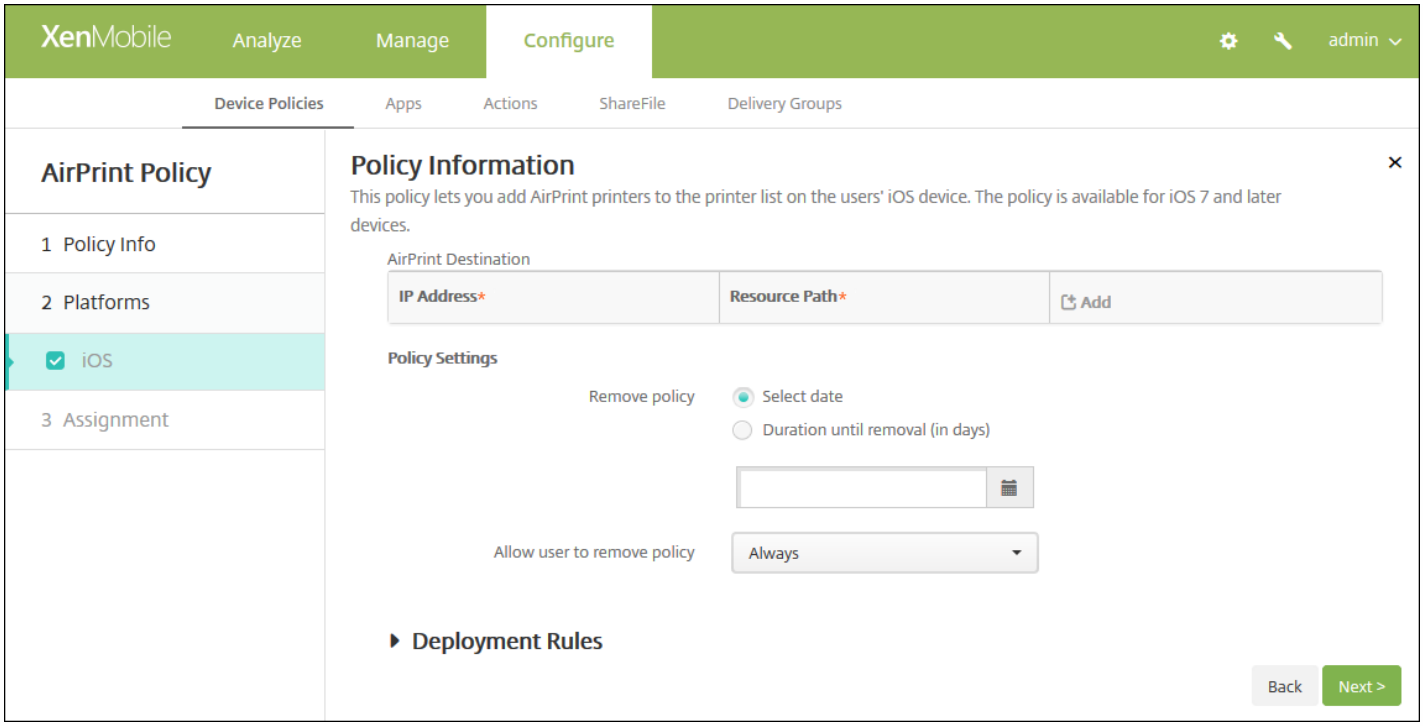
-
-
-
-

-
-

-
-

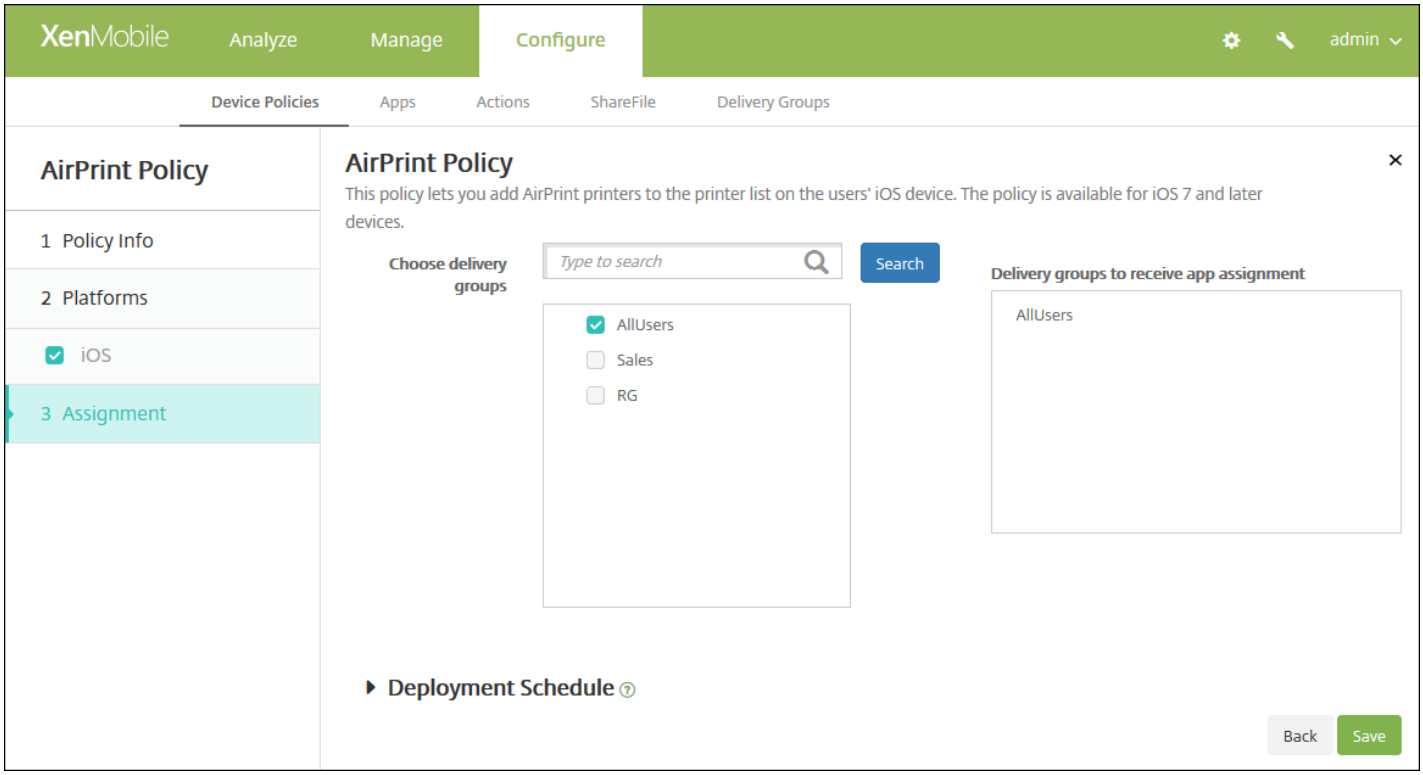


-
-

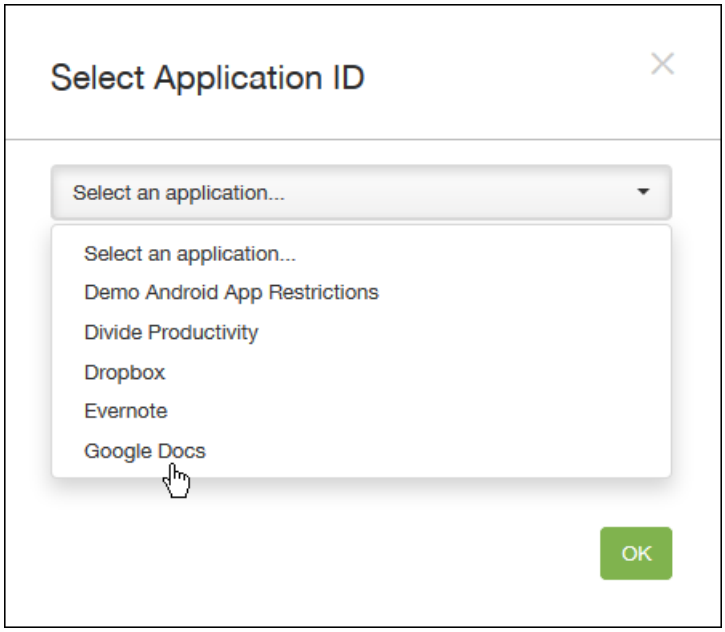


-
  -
  -
  -
-
  -
  -
  -
  -
  -

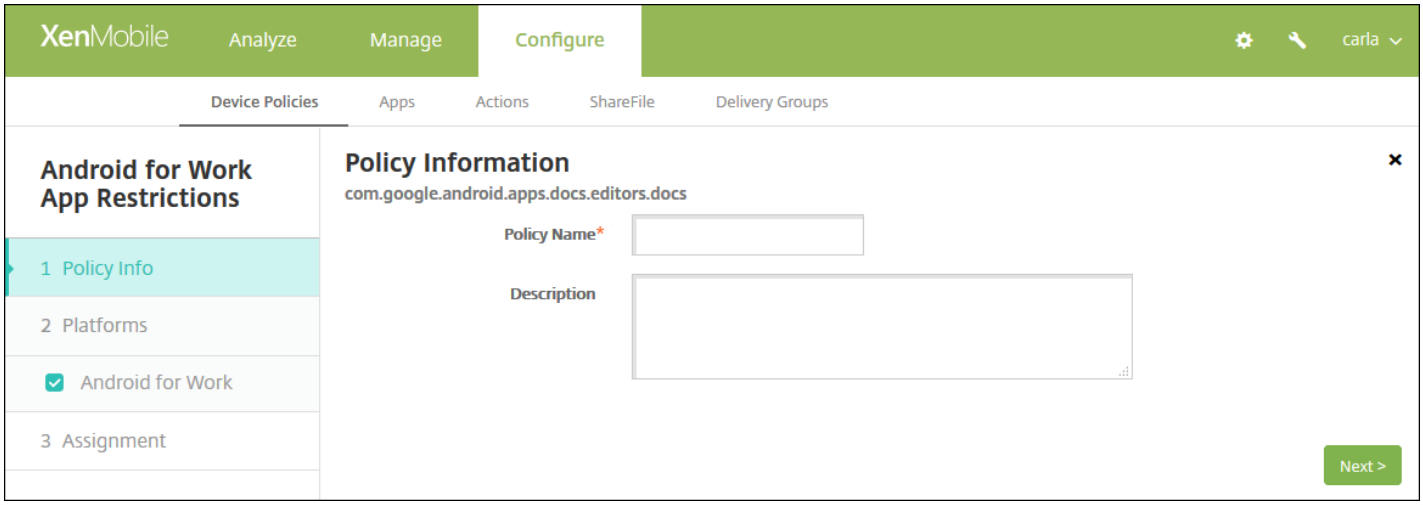
7. Configure the deployment rules



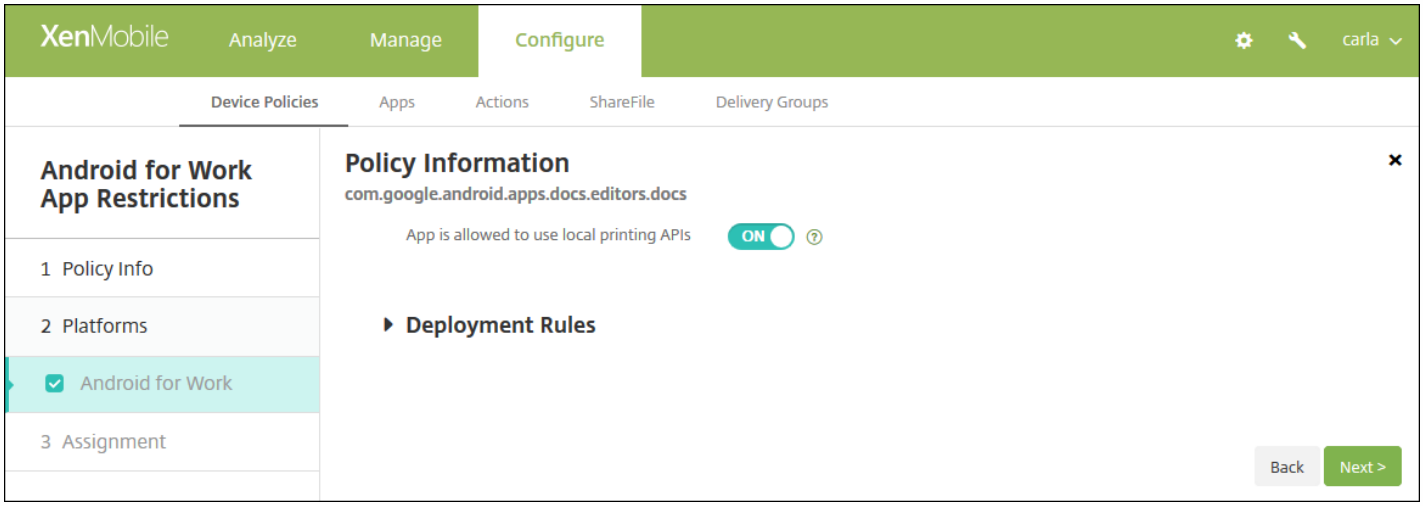
-
-
-
-



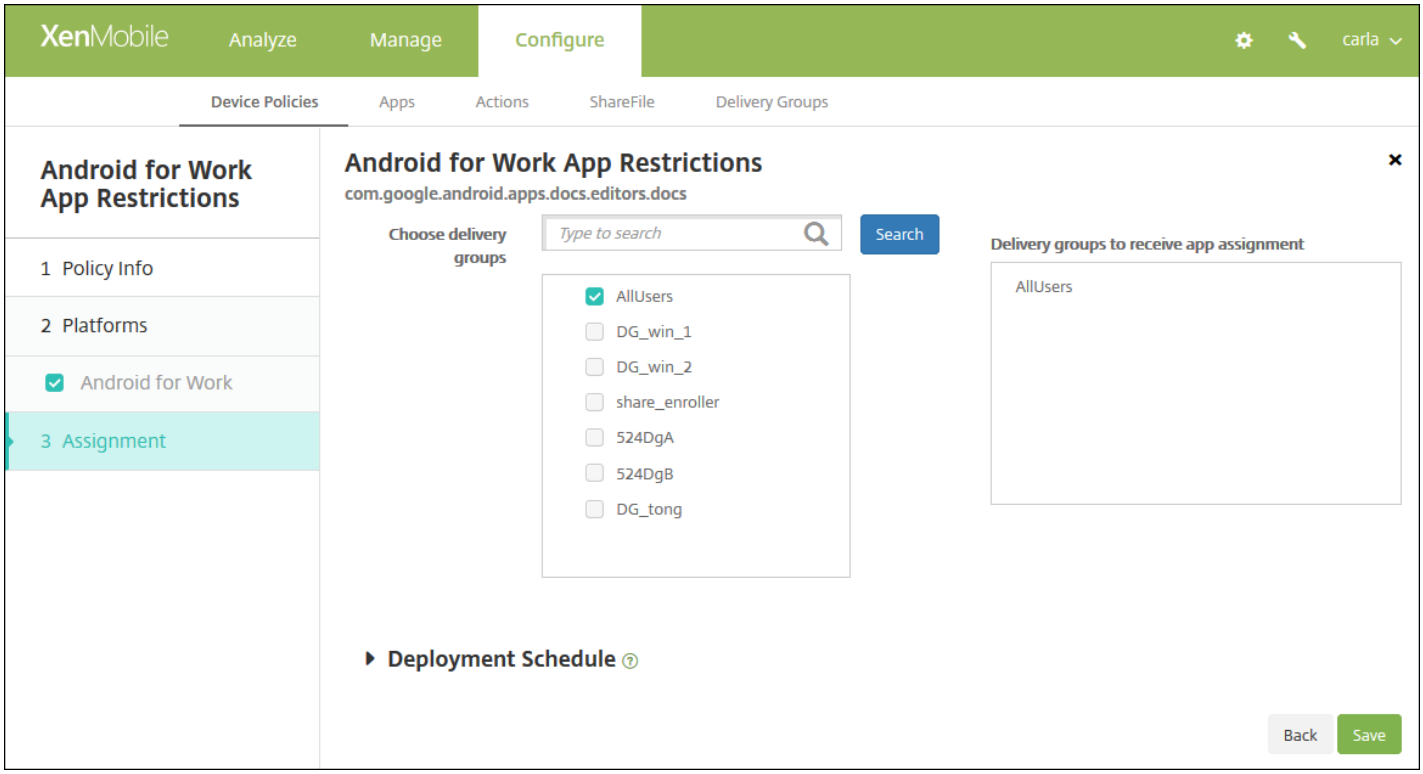
-
-
-



-
-



8. Configure the deployment rules



-
-
-
-
-
-
-

APN device policies

Jun 15, 2015

You can add a custom Access Point Name (APN) device policy for iOS, Android, and Windows Mobile/CE devices. You use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device. An APN policy determines the settings used to connect your devices to a specific phone carrier's General Packet Radio Service (GPRS). This setting is already defined in most newer phones.

iOS settings

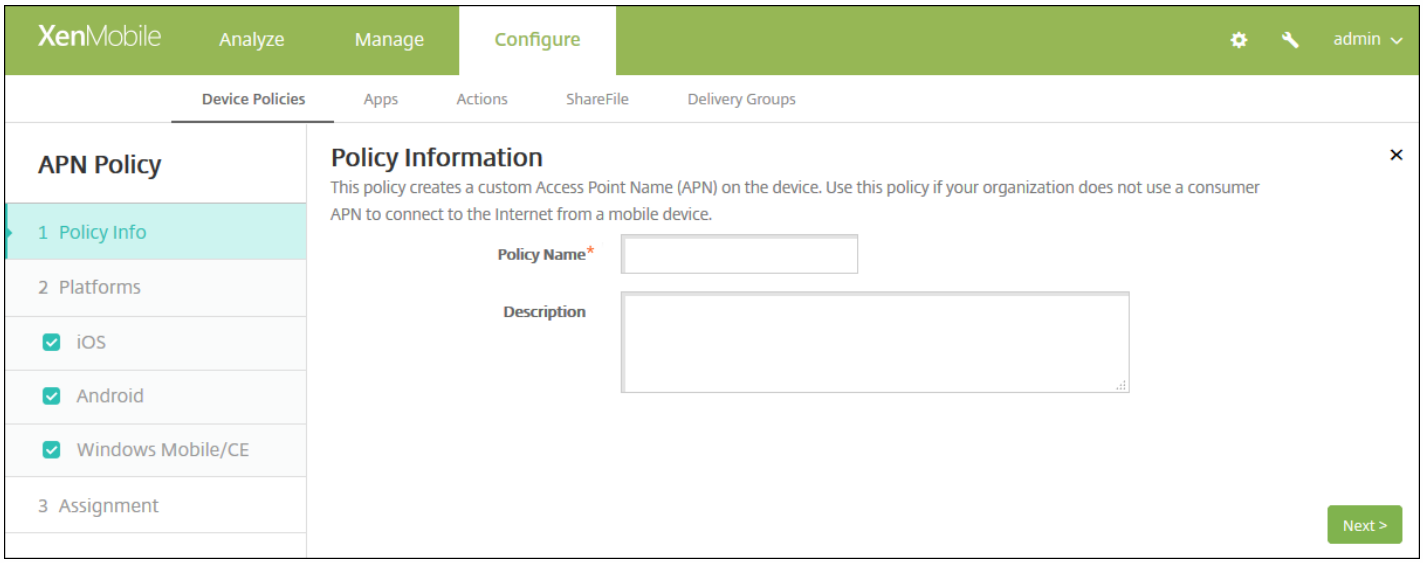
Android settings

Windows Mobile/CE settings

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

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

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



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

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

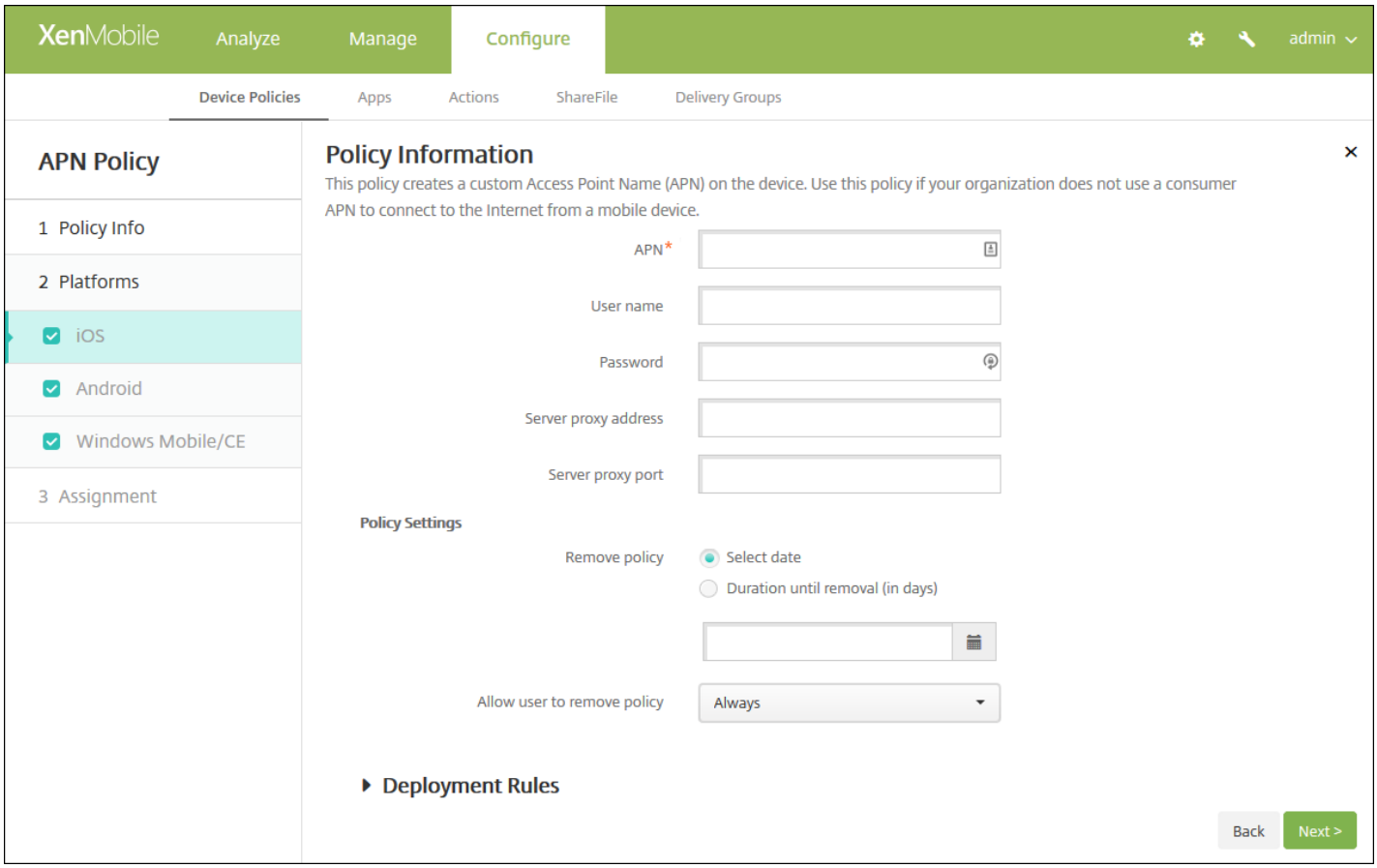
5. Click **Next**. The **Policy Platforms** page appears.

Note: When the **Policy Platforms** page appears, all platforms are selected and you see the iOS platform first.

6. Under **Platforms**, select the platforms you want to add.

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

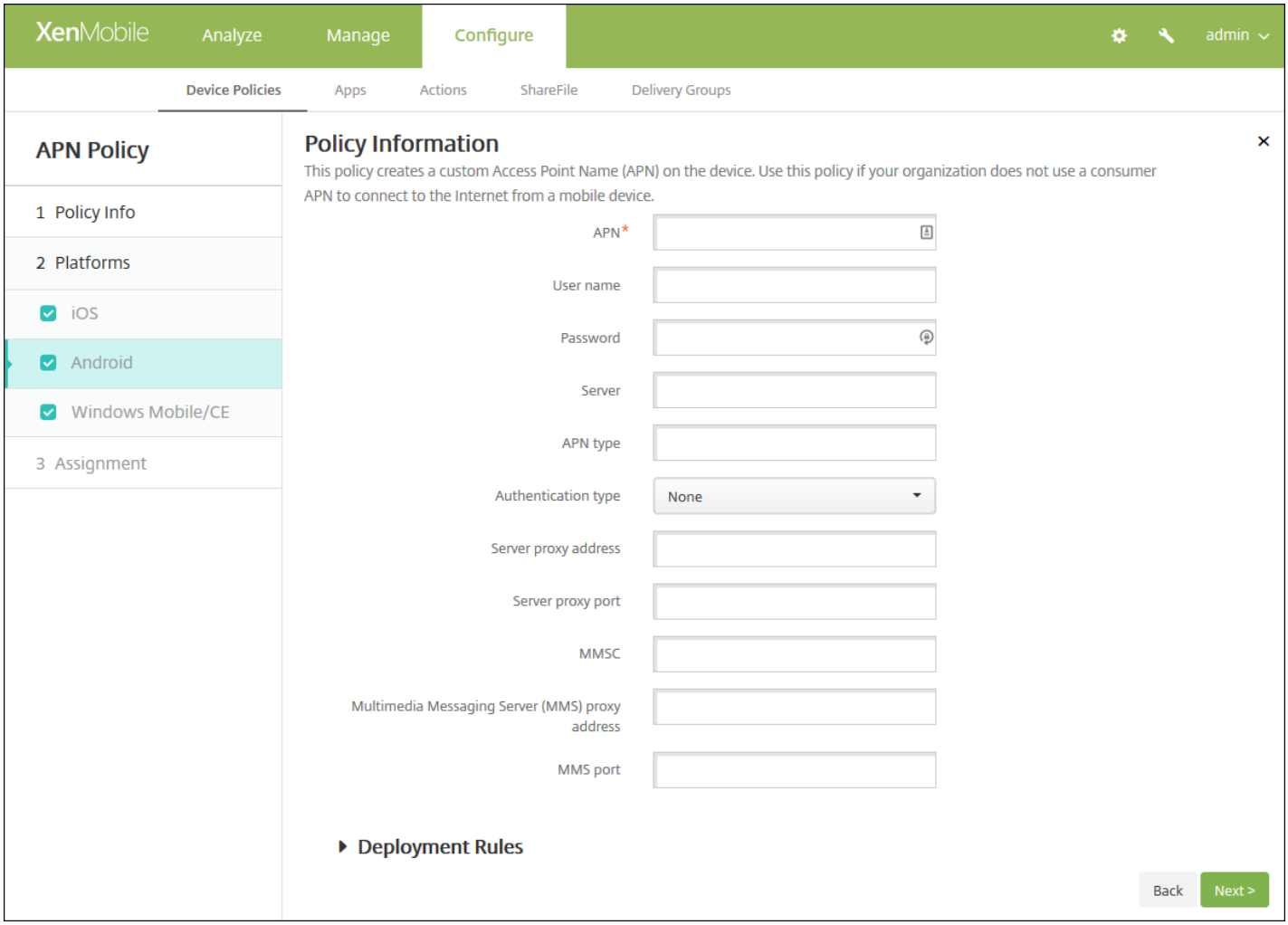
Configure iOS settings



Configure these settings:

- **APN**: Type the name of the access point. This must match an accepted iOS APN or the policy will fail.
- **User name**: This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
- **Password**: The password for the user for this APN. For obfuscation purposes, the password is encoded. If it is missing from the payload, the device prompts for the password during profile installation.
- **Server proxy address**: The IP address or URL of the APN proxy.
- **Server proxy port**: The port number for the APN proxy. This is required if you entered a server proxy address.
- Under **Policy Settings**, next to **Remove policy**, click either **Select date** or **Duration until removal (in 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 Android settings

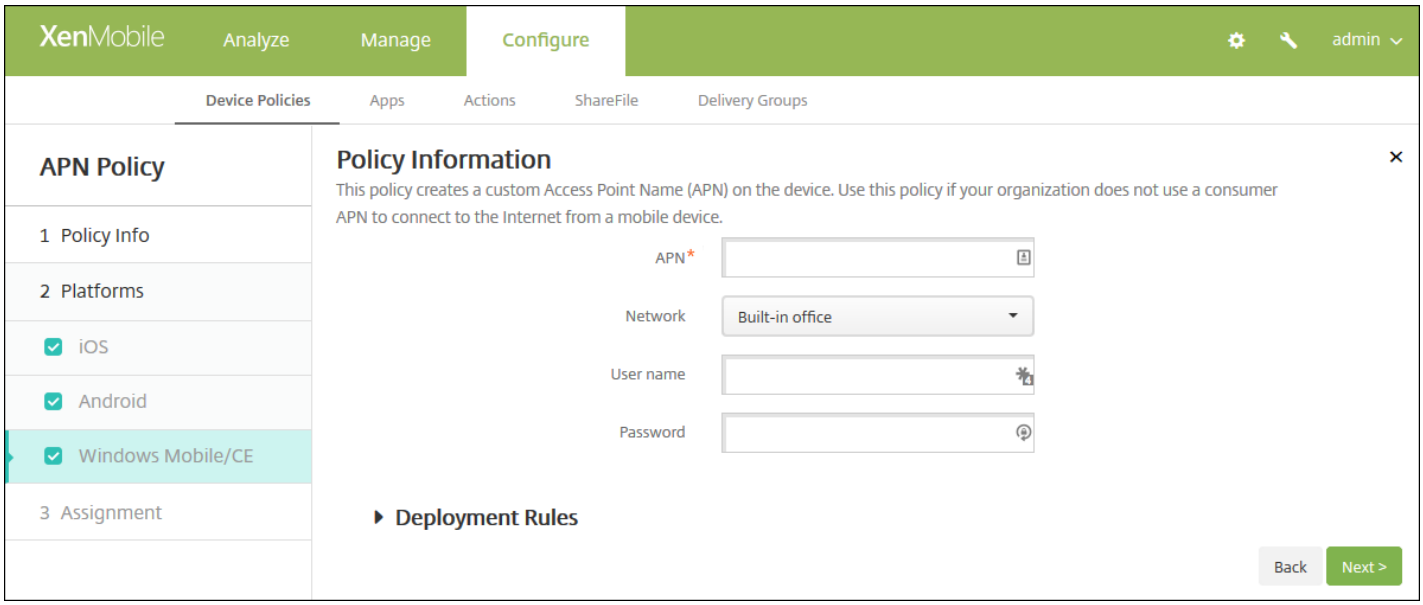


Configure these settings:

- **APN**: Type the name of the access point. This must match an accepted Android APN or the policy will fail.
- **User name**: This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
- **Password**: The password for the user for this APN. For obfuscation purposes, the password is encoded. If it is missing from the payload, the device prompts for the password during profile installation.
- **Server**: This setting, which predates smart phones, is usually empty. It references a Wireless Application Protocol (WAP) gateway server for phones that could not access or render standardweb sites.
- **APN type**: This setting must match the carrier's intended use for the access point. It is a comma separated string of APN service specifiers and must match the wireless carrier's published definitions. Examples include:
  - *. All traffic goes through this access point.
  - mms. Multimedia traffic goes through this access point.
  - default. All traffic, including multimedia, goes through this access point.
  - supl. Secure User Plane Location is associated with assisted GPS.
  - dun. Dial Up Networking is outdated and should rarely be used.
  - hipri. High priority networking.
  - fota. Firmware over the air is used for receiving firmware updates.
- **Authentication type**: In the list, click the type of authentication to be used. Defaults to None.
- **Server proxy address**: The IP address or URL of the carrier's APN HTTP proxy.

- **Server proxy port**: The port number for the APN proxy. This is required if you entered a server proxy address.
- **MMSC**: The MMS Gateway Server address provided by the carrier.
- **Multimedia Messaging Server (MMS) proxy address**: This is the multimedia messaging service server for MMS traffic. MMS succeeded SMS for sending larger messages with multimedia content, such as pictures or videos. These servers require specific protocols (such as MM1, ... MM11).
- **MMS port**: The port used for the MMS proxy.

Configure Windows Mobile/CE settings

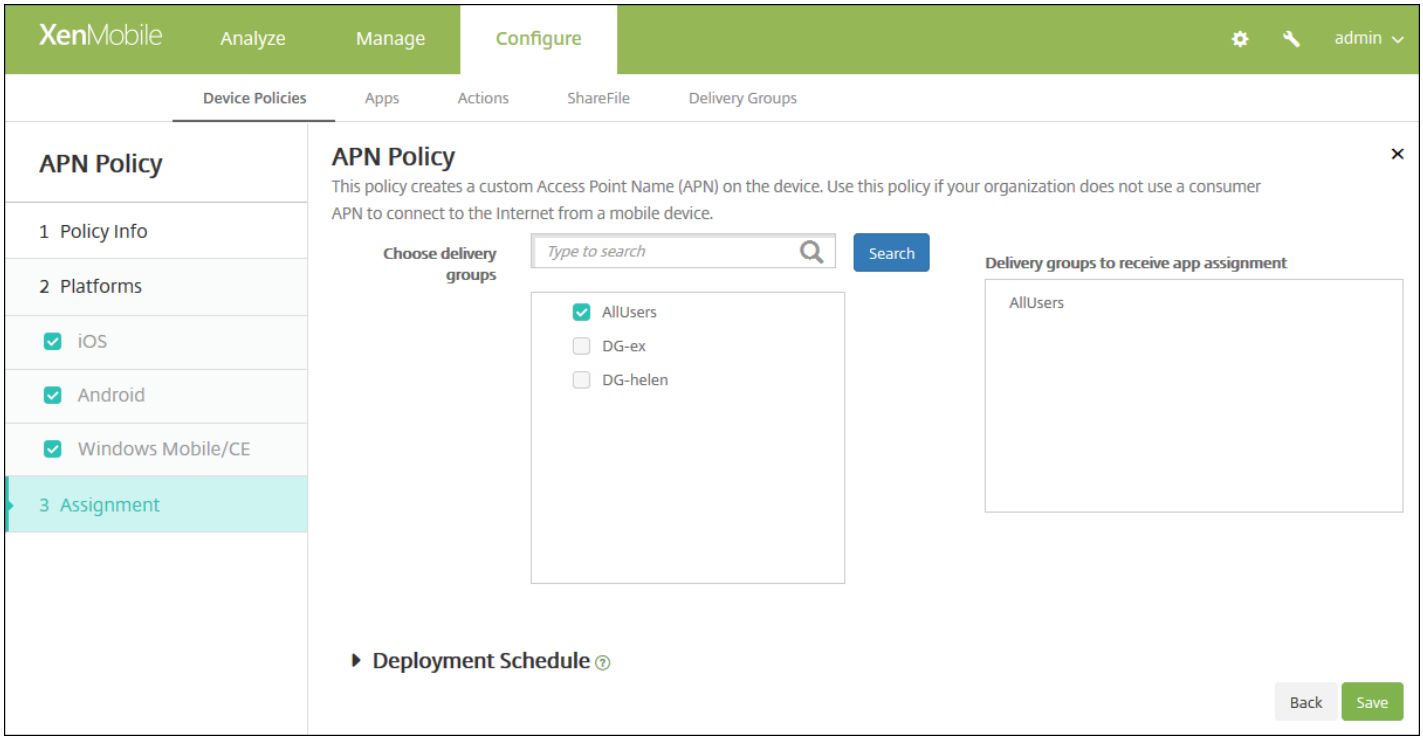


Configure the following settings:

- **APN**: Type the name of the access point. This must match an accepted Android APN or the policy will fail.
- **Network**: In the list, click the type of network to use. The default is **Built-in office**.
- **User name**: This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
- **Password**: The password for the user for this APN. For obfuscation purposes, the password is encoded. If it is missing from the payload, the device prompts for the password during profile installation.

7. Configure the deployment rules

8. Click **Next**. The **APN 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**.

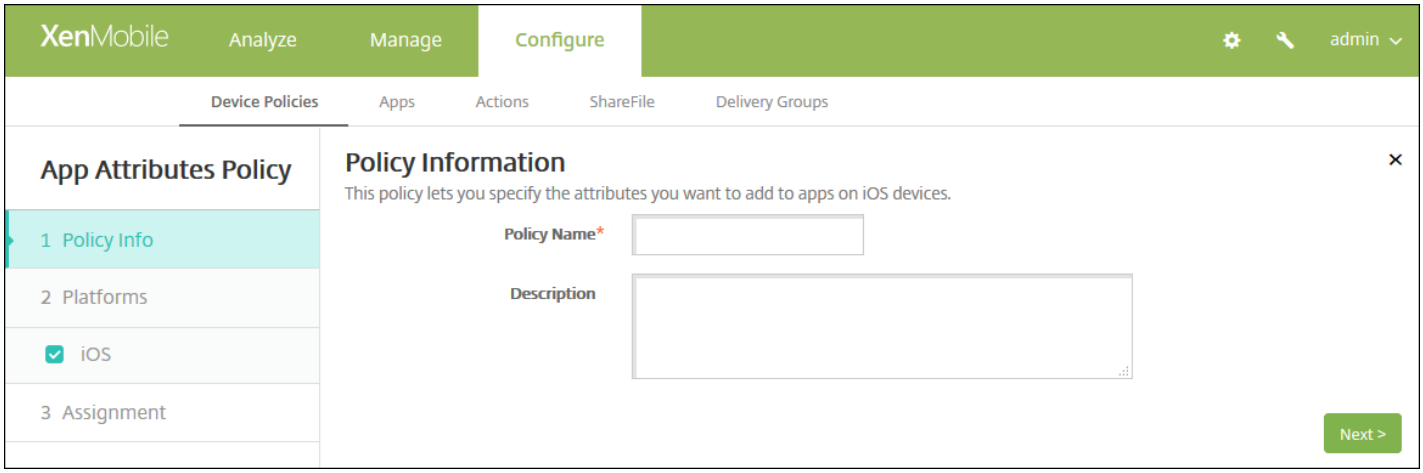
Note:

- 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 attributes device policy

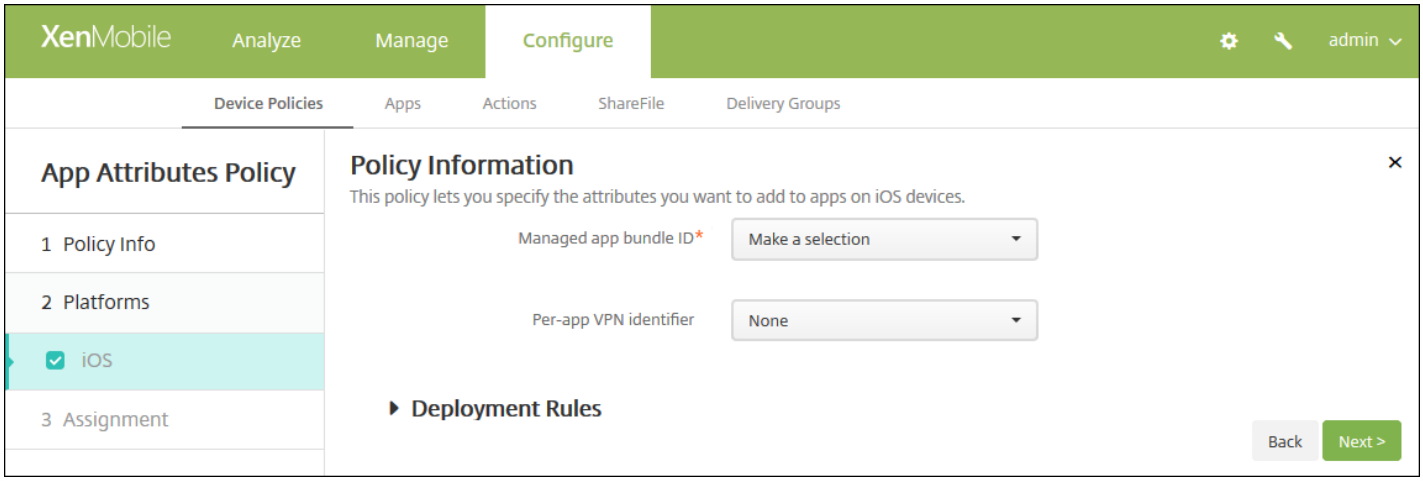
Sep 24, 2015



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

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

5. Click **Next**. The **App Attributes** platform information page appears.

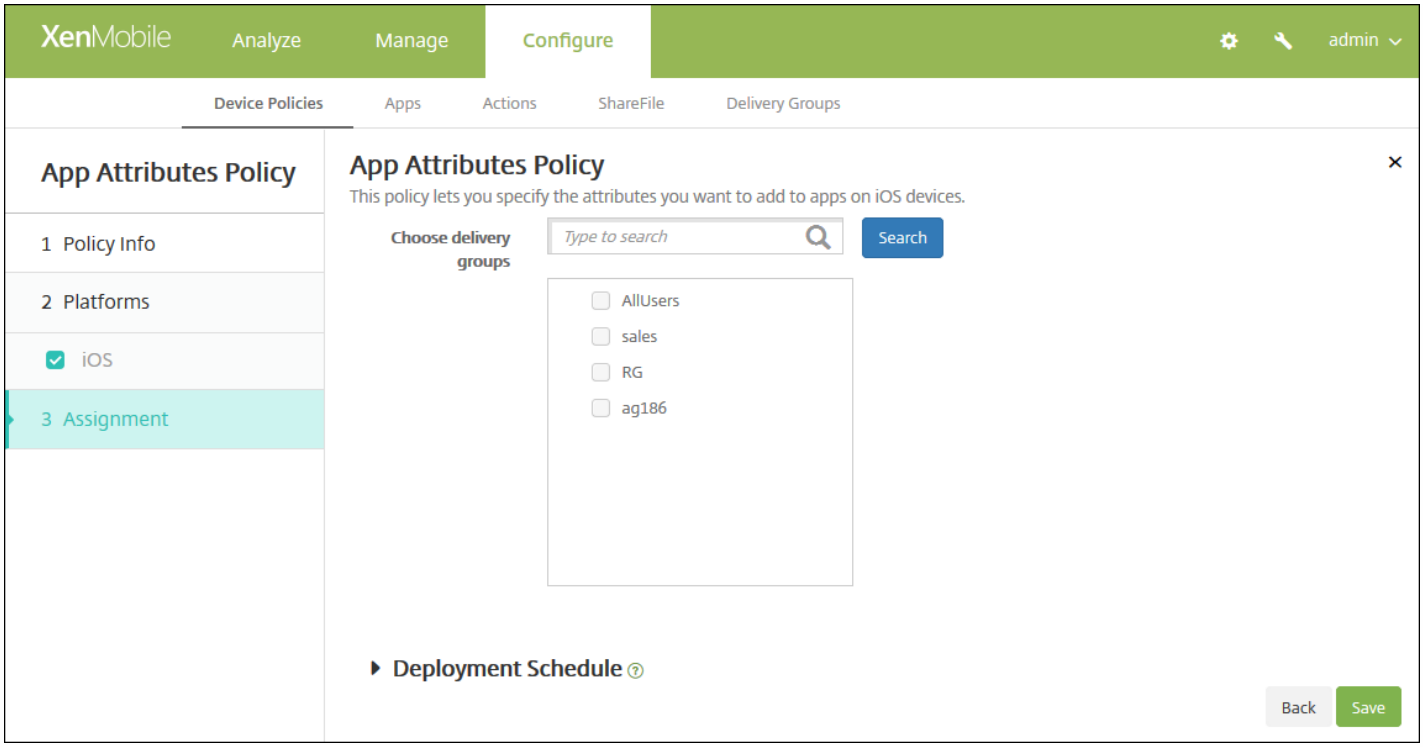


6. Configure these settings:

- **Managed app bundle ID**: In the list click an app bundle ID or click **Add new**.
  - If you click **Add new**, type the app bundle ID in the field that appears.
- **Per-app VPN identifier**: In the list, click per-app VPN identifier.

7. Configure the deployment rules

8. Click **Next**. The App Attributes 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**.

App access device policies

Apr 24, 2015

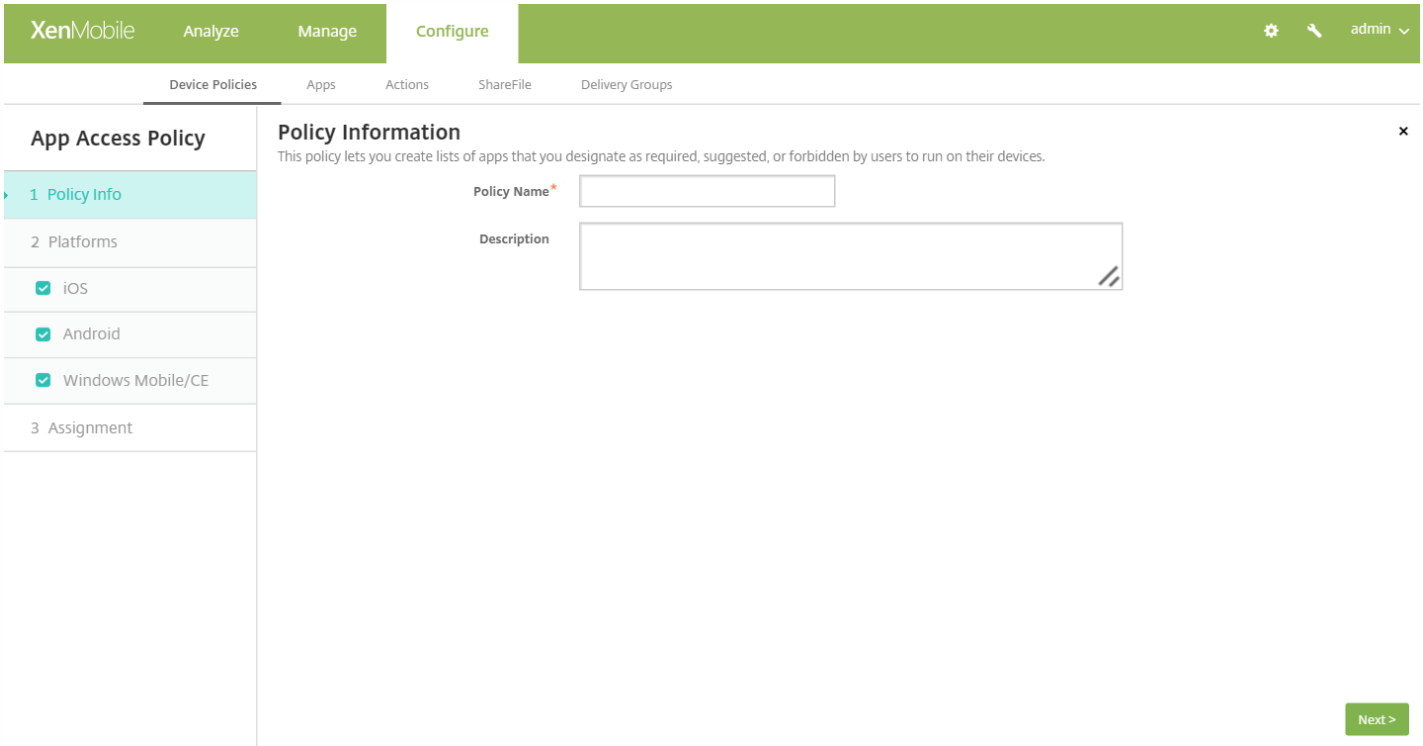
The app access device policy in XenMobile allows you to define a list of apps that are either required to be installed on the device, can be installed on the device, or must not be installed on the device. You can then create an automated action to react to the device compliance with that list of apps. You can create app access policies for iOS, Android, and Windows Mobile/CE devices.

You can only configure one type of access policy at a time. You can add a policy for either a list of required apps, suggested apps, or forbidden apps, but not a mix within the same app access policy. If you create a policy for each type of list, it is recommended that you name each policy carefully, so you know which policy in XenMobile applies to which list of apps.

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

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

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



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

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

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

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

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

6. Configure the following settings for each platform you select.

- **Access policy**: Click Required, Suggested, or Forbidden. The default is Required.
- To add one or more apps to the list, click **Add** and then do the following:
  - **App name**: Enter an app name.
  - **App Identifier**: Enter an optional app identifier.
  - Click **Save** or **Cancel**.
  - Repeat these steps for each app you want to add.

    Note: To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing app, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

7. Configure the deployment rules

8. Click Next. The next platform page or the **App Access 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 configuration device policy

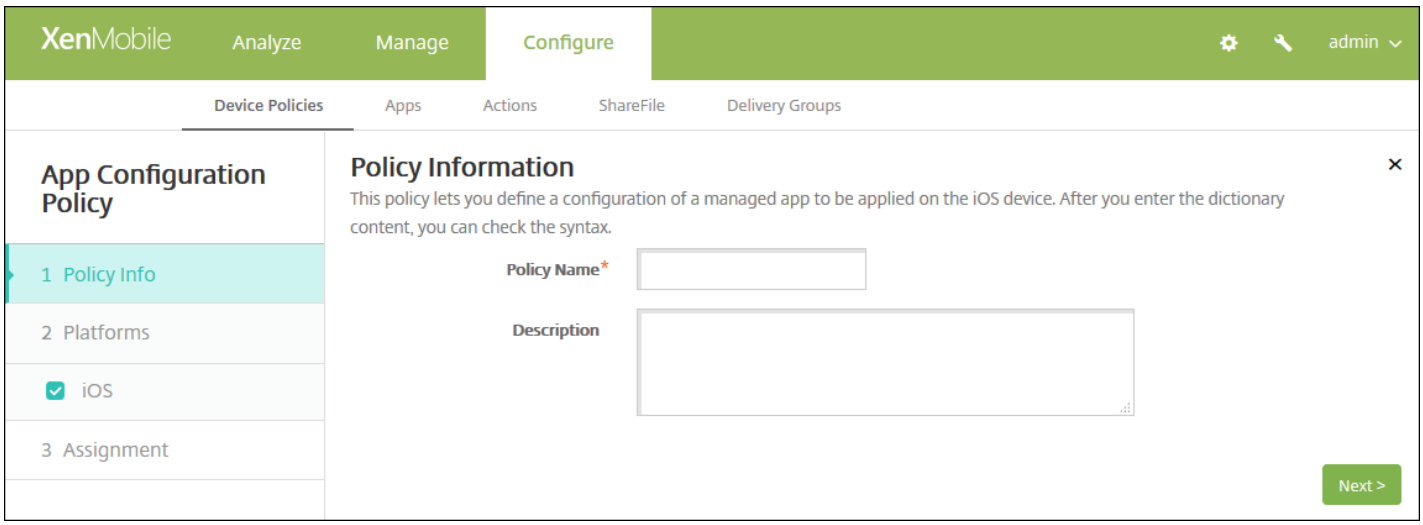
Sep 25, 2015

You can remotely configure an App Store app that supports managed configuration by deploying an XML configuration file (called a property list, or plist) to users' iOS devices to configure various settings and behaviors in the app. The actual settings and behaviors that you can configure depend on the app and are beyond the scope of this article.

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

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

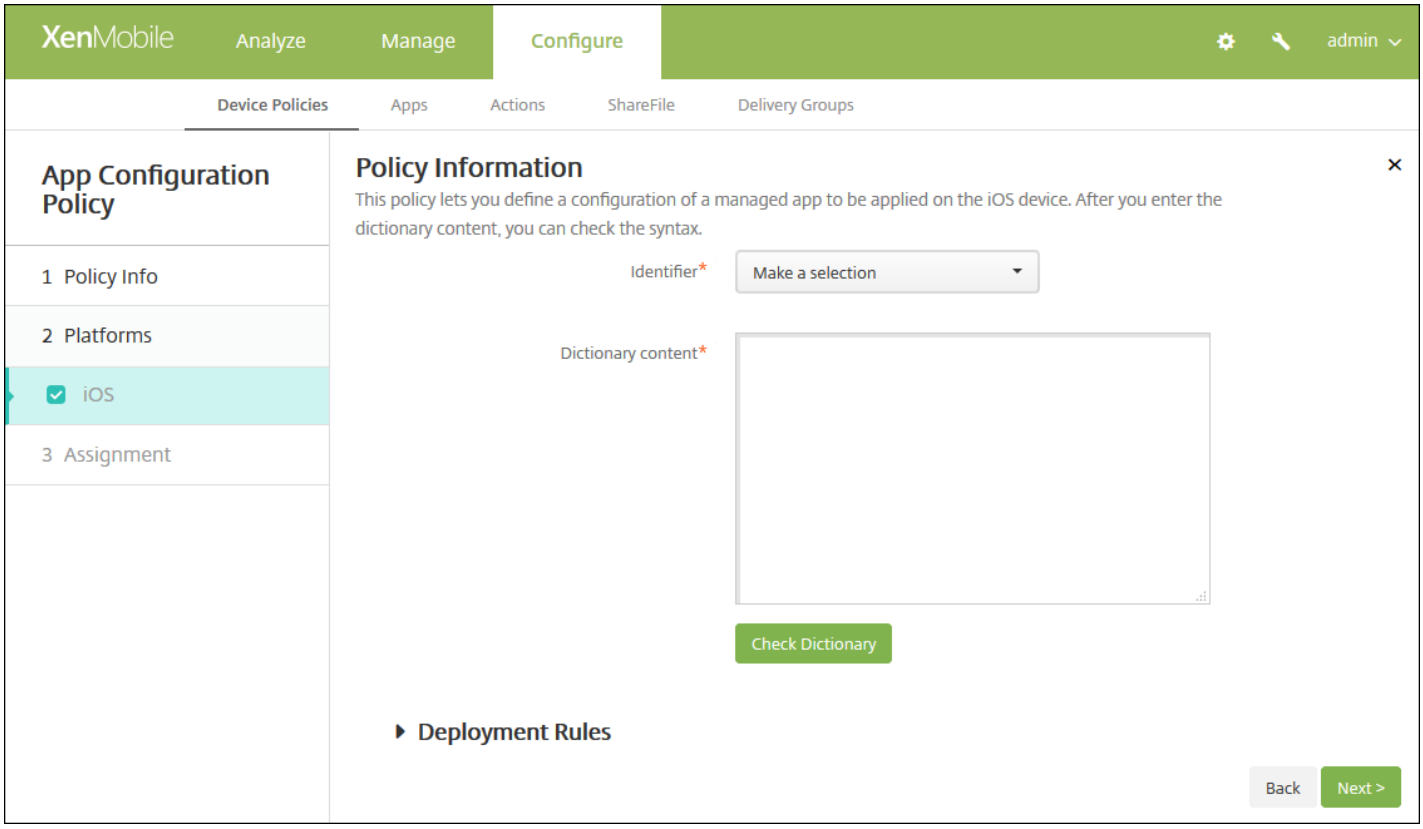
3. Expand **More**, and then under **Apps**, click **App Configuration**. The **App Configuration Policy** information page appears.



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

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

5. Click **Next**. The **iOS Platform** information page appears.

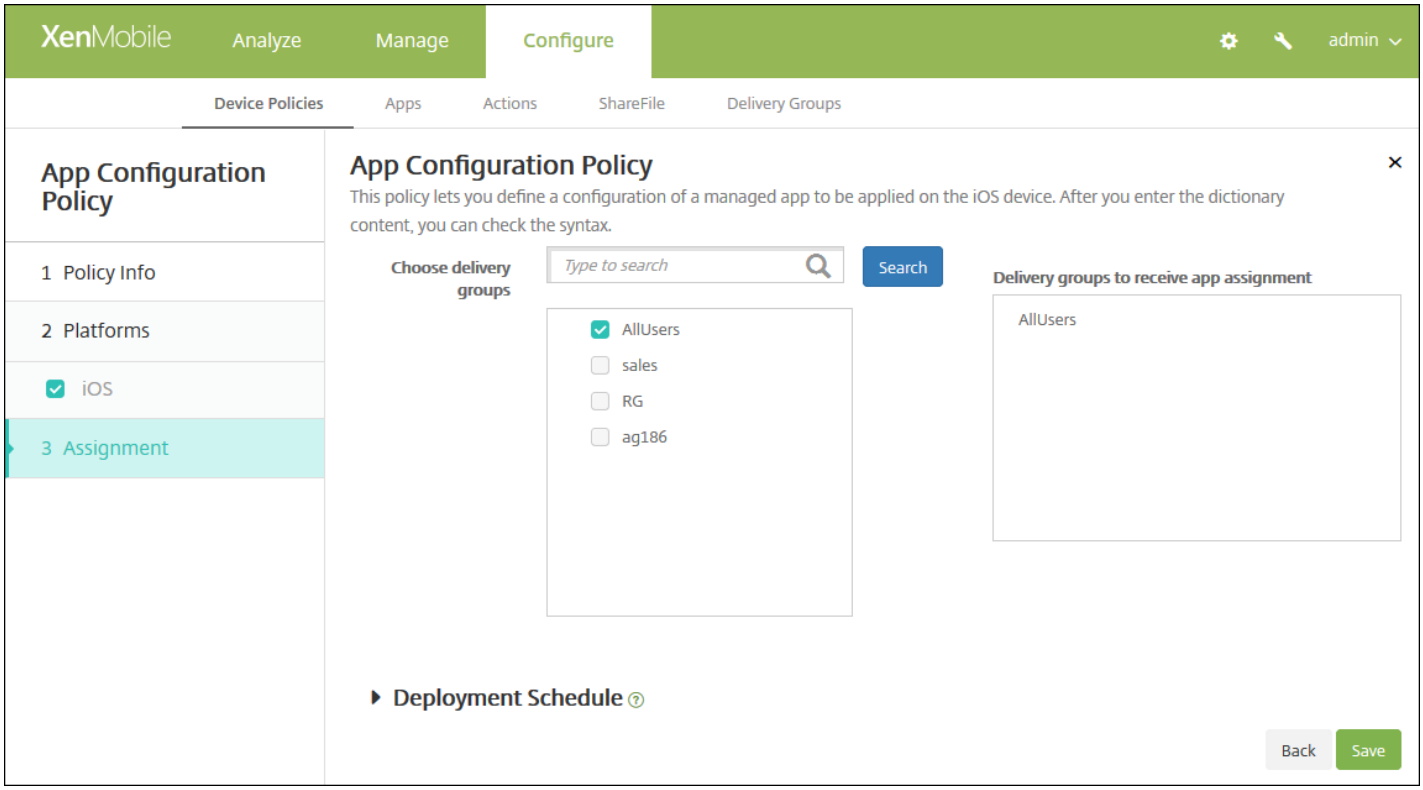


6. Configure these settings:

- **Identifier**: In the list, click the app you want to configure or click **Add new** to add a new app to the list.
  - If you click **Add new**, type the app identifier in the field that appears.
- **Dictionary content**: Type, or copy and paste, the XML property list (plist) configuration information.
- Click **Check Dictionary**. XenMobile verifies the XML. If there are no errors, you see **Valid XML** below the content box. If any syntax errors appear below the content box, you must correct them before you can continue.

7. Configure the deployment rules

8. Click **Next**. The **App Configuration 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**.

App inventory device policies

Jan 06, 2017

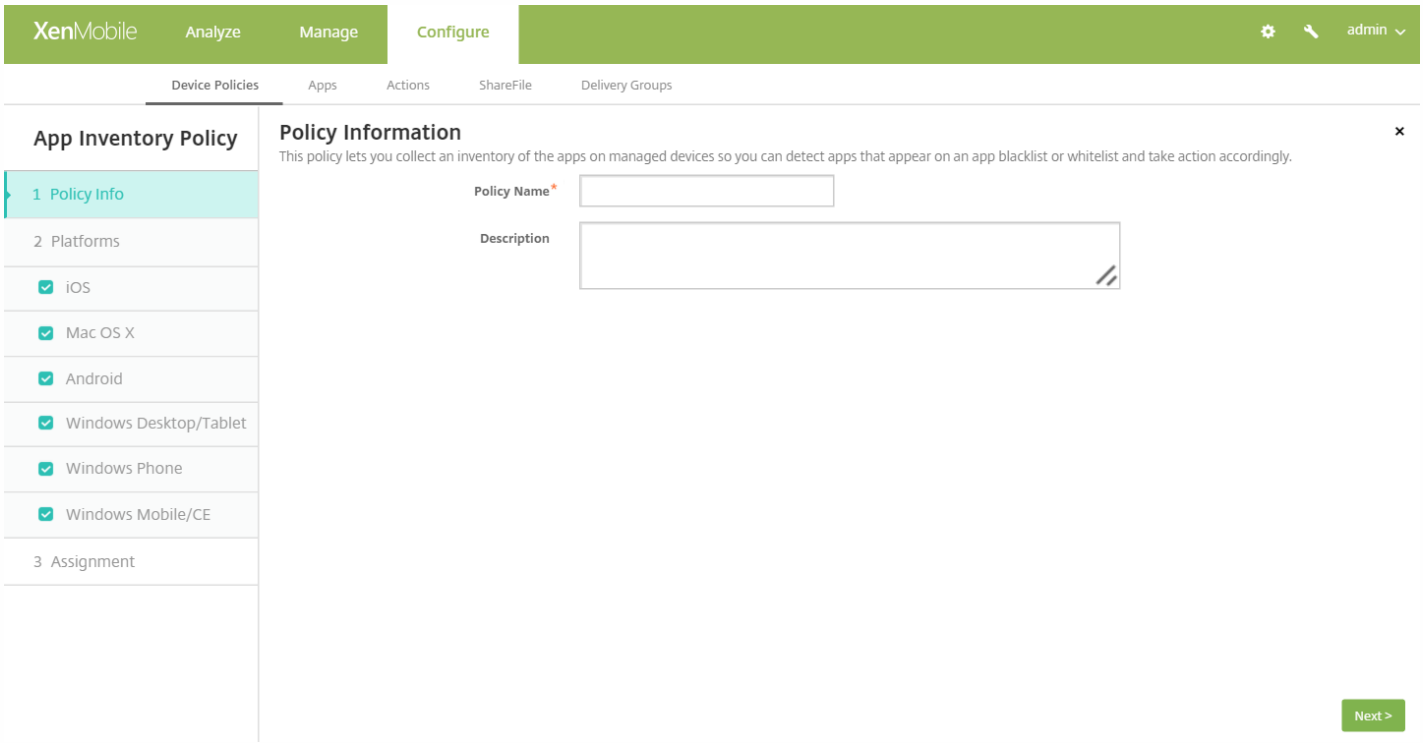
An app inventory policy in XenMobile lets you collect an inventory of the apps on managed devices, and then the inventory is compared to any app access policies deployed to those devices. In this way, you can detect apps that appear on an app blacklist (forbidden in an app access policy) or whitelist (required in an app access policy) and take action accordingly. You can create app access policies for iOS, Mac OS X, Android (including for devices enabled for Android for Work), Windows desktop/tablet, Windows phone, or Windows Mobile/CE devices.

> ## Important
>
> For updated apps to appear in the Updates Available list in the Worx Store on users' Android devices, you must first deploy this policy to the users' devices. Also please note that beginning with version 10.4, the Worx Store is renamed XenMobile Store.

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

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

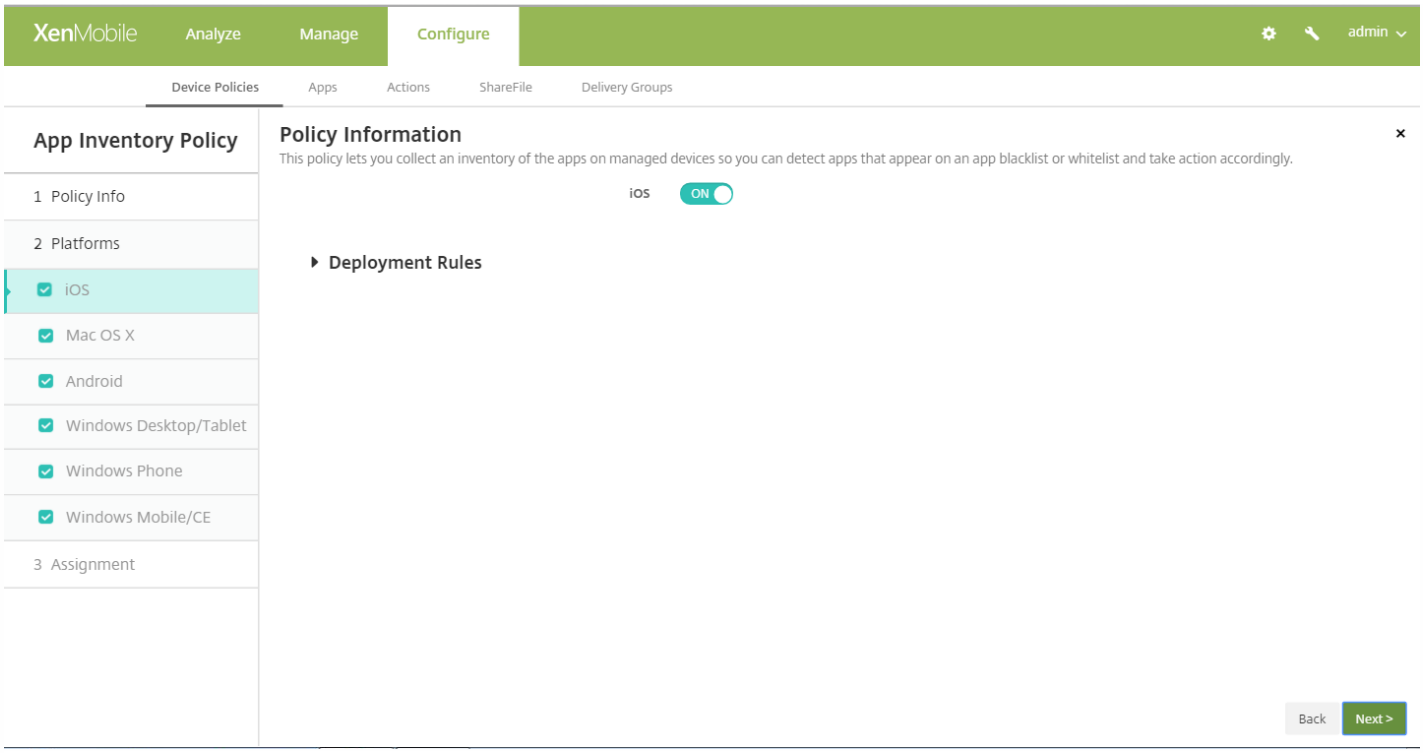
3. Expand **More**, and under **Apps**, click **App Inventory**. The **App Inventory Policy** page appears.



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

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

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



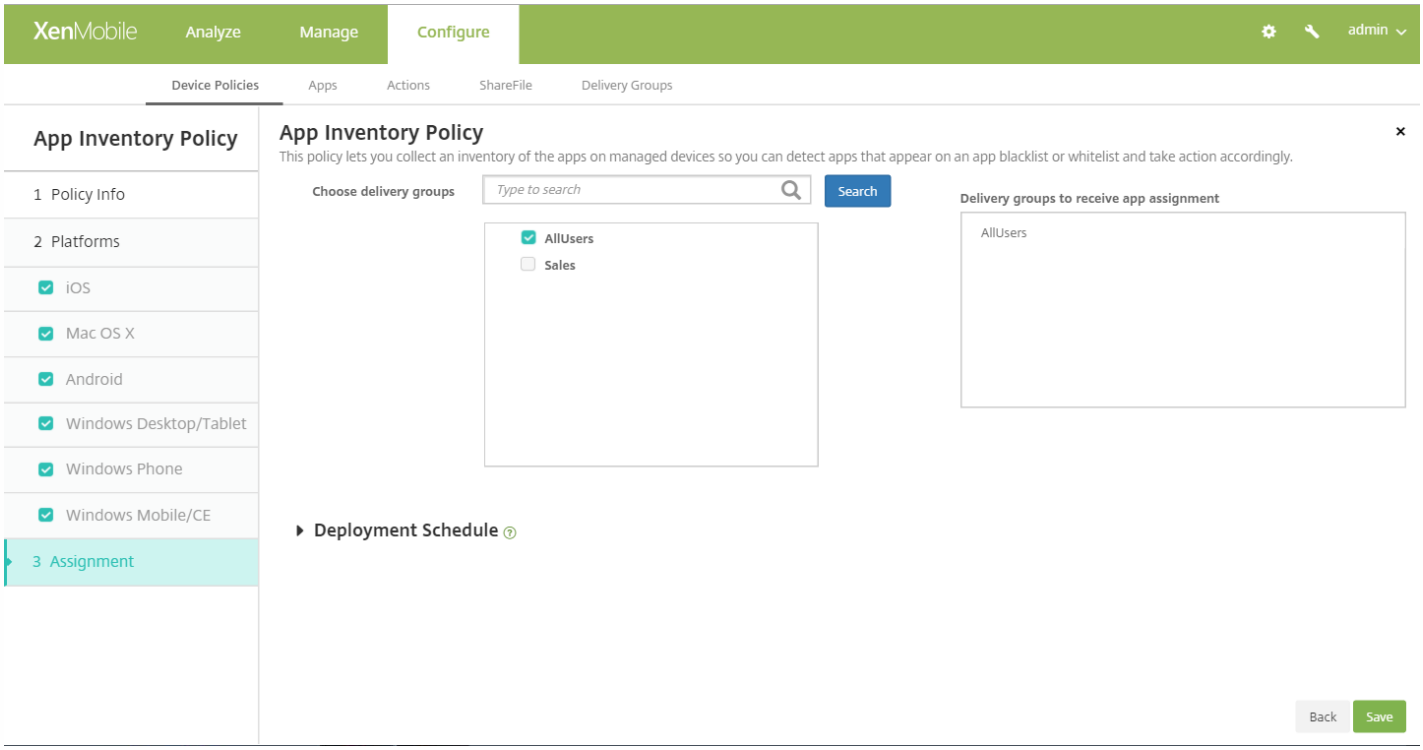
Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.

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

6. For each platform you select, leave the default setting or change the setting to **OFF**. The default is **ON**.

7. Configure the deployment rules

8. Click **Next**. The **App Inventory 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 lock device policy

Aug 09, 2016

You can create a policy in XenMobile to define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device. You can configure this policy for both iOS and Android devices, but the exact way the policy works differs for each platform. For example, you cannot block multiple apps on an iOS device.

Likewise, for iOS devices, you can select only one iOS app per policy. This means that users are only able to use their device to run a single app. They cannot do any other activities on the device except for the options you specifically allow when the app lock policy is enforced.

In addition, iOS devices must be supervised to push App Lock policies.

Although the device policy works on most Android L and M devices, app lock does not function on Android N or later devices due to the deprecation of the required API by Google.

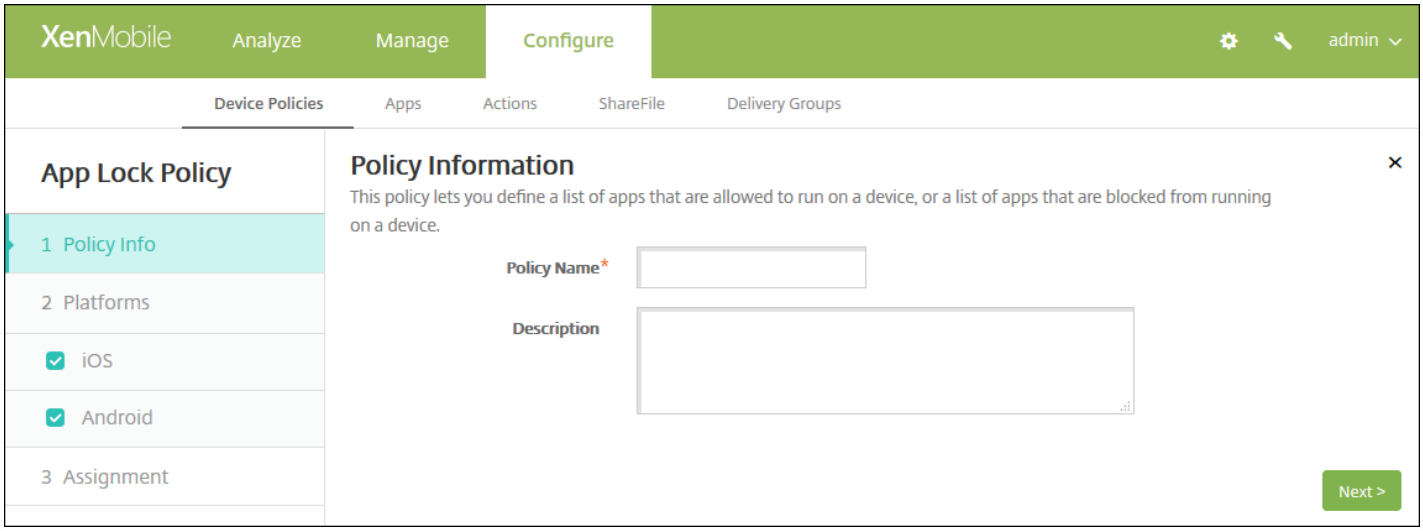
iOS settings

Android settings

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

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

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



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

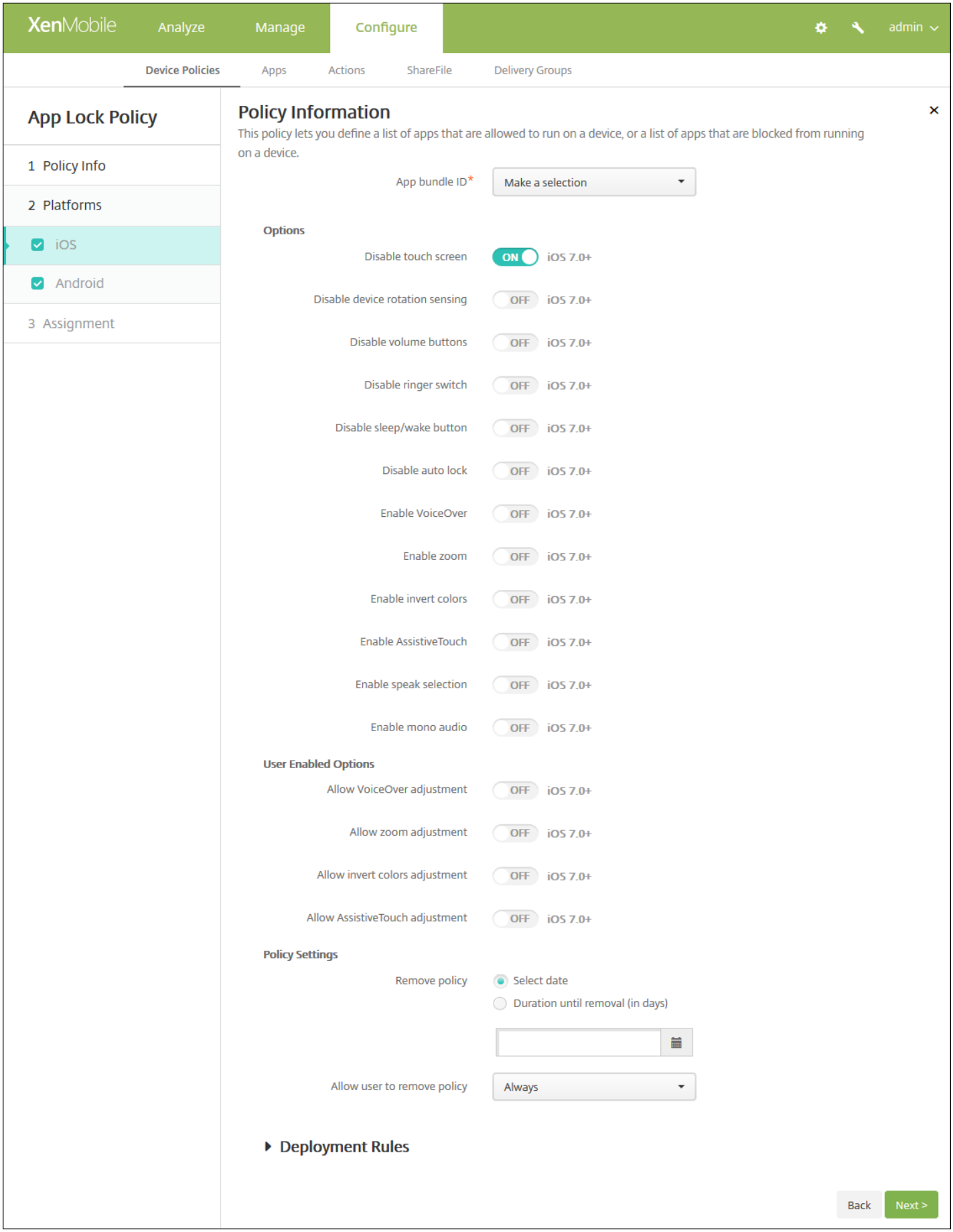
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: If desired, type a description of the policy.

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

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

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

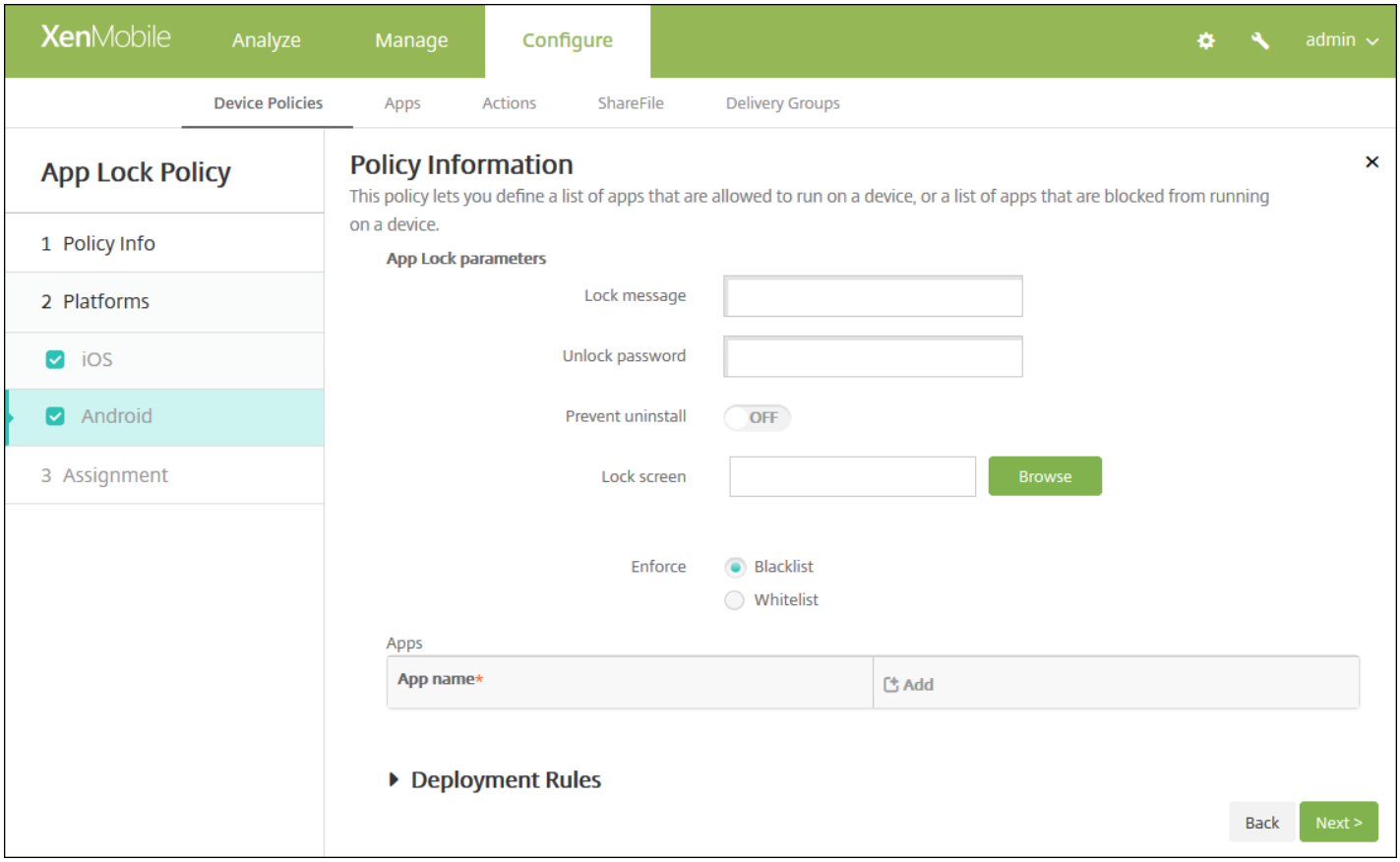
Configure iOS settings



Configure these settings:

- **App bundle ID**: In the list, click the app to which this policy applies or click **Add new** to add a new app to the list. If you select **Add new**, type the app name in the field that appears.
- **Options**: Each of the following options applies only to iOS 7.0 or later. For each option, the default is **OFF** except for Disable touch screen, which defaults to **ON**.
  - Disable touch screen
  - Disable device rotation sensing
  - Disable volume buttons
  - Disable ringer switch - **Note**: When this option is disabled, the ringer behavior depends on what position the switch was in when it was first disabled.
  - Disable sleep/wake button
  - Disable auto lock
  - Disable VoiceOver
  - Enable zoom
  - Enable invert colors
  - Enable AssistiveTouch
  - Enable speak selection
  - Enable mono audio
- **User Enabled Options**: Each of the following options applies only to iOS 7.0 or later. For each option, the default is **OFF**.
  - Allow VoiceOver adjustment
  - Allow zoom adjustment
  - Allow invert colors adjustment
  - Allow AssitiveTouch adjustment
- **Policy Settings**
  - o Next to **Remove policy**, click either **Select date** or **Duration until removal (in days)**.
  - o If you click **Select date**, click the calendar to select the specific date for removal.
  - o In the **Allow user to remove policy** list, click **Always**, **Password required**, or **Never**.
  - o If you click **Password required**, next to **Removal password**, type the necessary password.

Configure Android settings



Configure these settings:

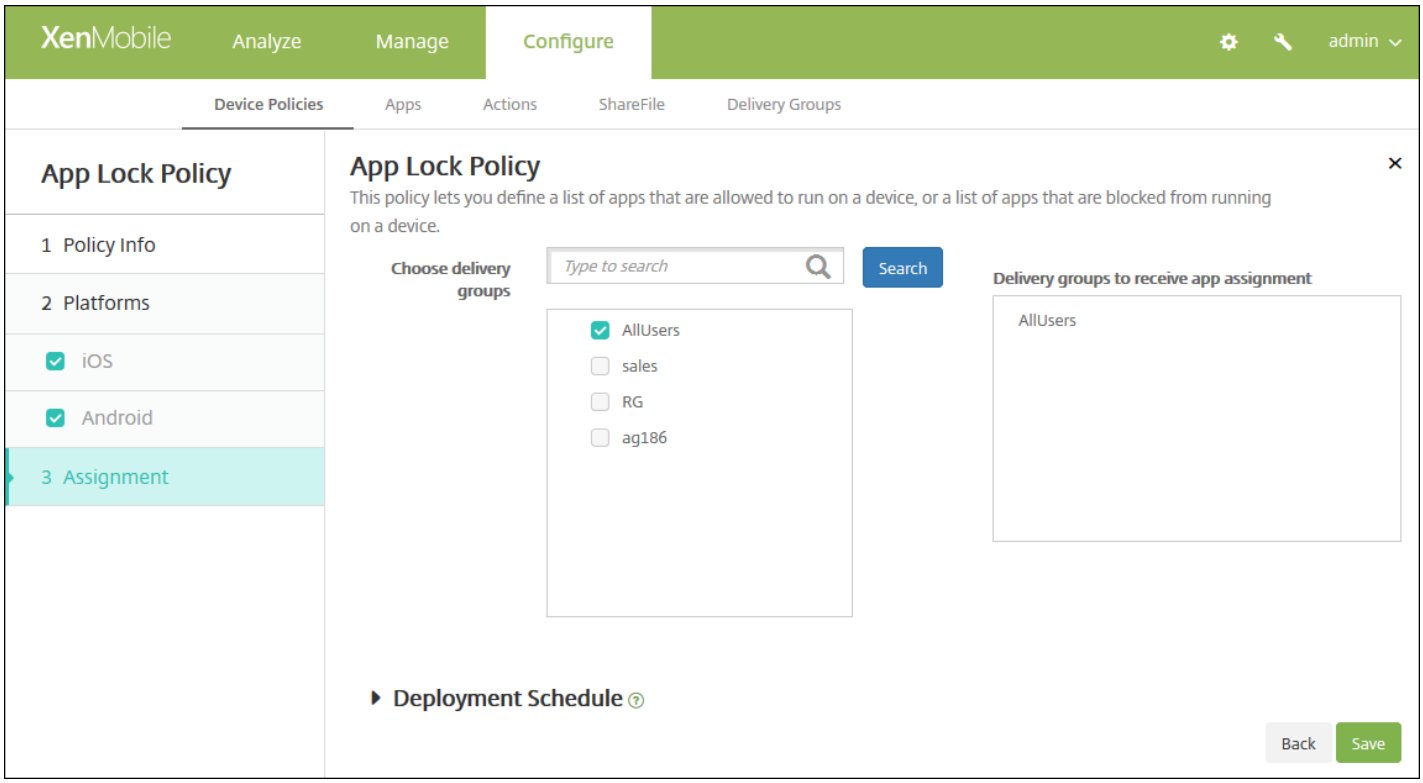
- **App Lock parameters**
  - **Lock message**: Type a message that users see when they attempt to open a locked app.
  - **Unlock password**: Type the password to unlock the app.
  - **Prevent uninstall**: Select whether users are allowed to uninstall apps. The default is **OFF**.
  - **Lock screen**: Select the image that appears on the device's lock screen by clicking Browse and navigating to the file's location.
  - **Enforce**: Click either **Blacklist** to create a list of apps that are not allowed to run on devices or click **Whitelist** to create a list of apps that are allowed to run on devices.
- **Apps**: Click **Add** and then do the following:
  - **App name**: In the list, click the name of the app to add to the whitelist or blacklist, or click **Add new** to add a new app to the list of available apps.
  - If you select **Add new**, type the app name in the field that appears.
  - Click **Save** or **Cancel**.
  - Repeat these steps each app you want to add to the whitelist or blacklist.

    Note: To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click **Delete** to delete the listing or **Cancel** to keep the listing.

    To edit an existing app, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

7. Configure the deployment rules

8. Click **Next**, the **App Lock 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**.

App network usage device policy

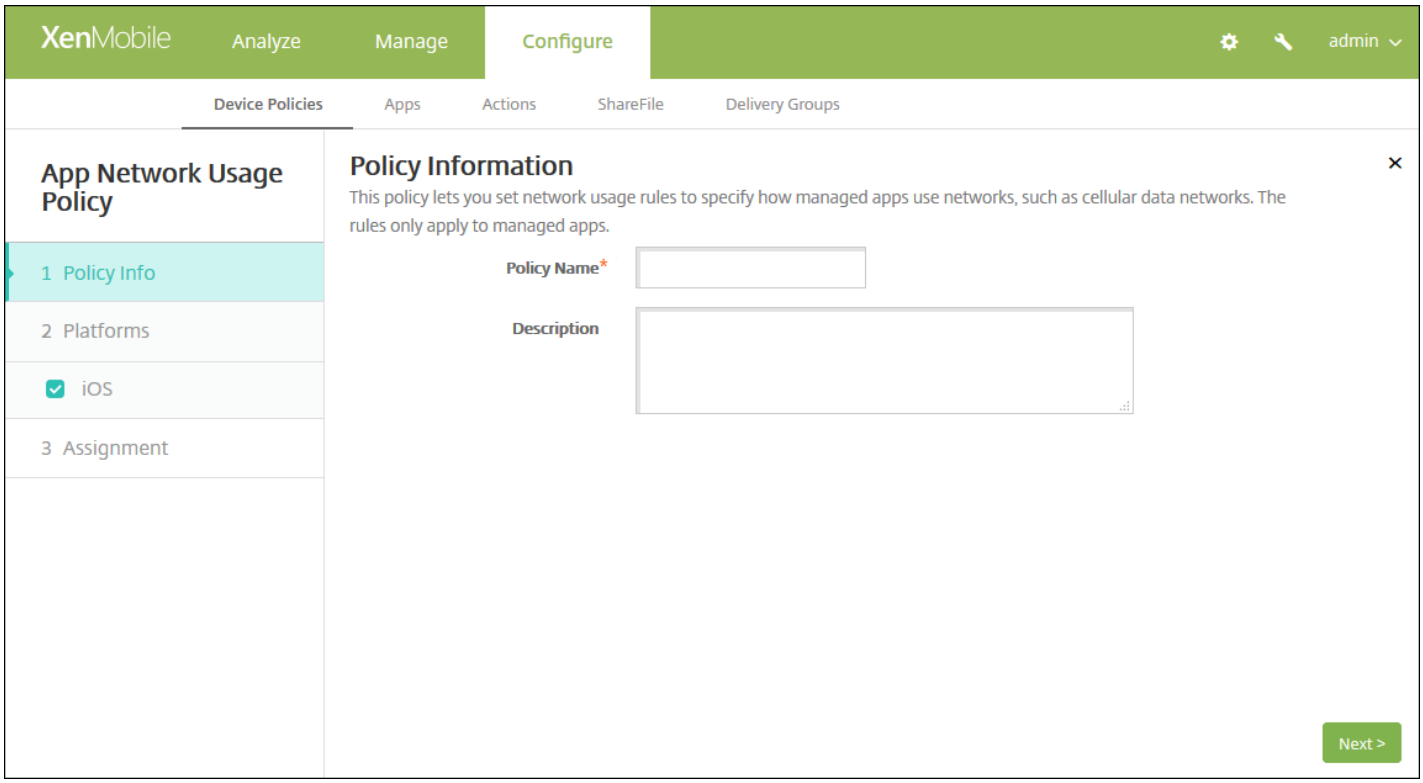
Sep 15, 2015

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.

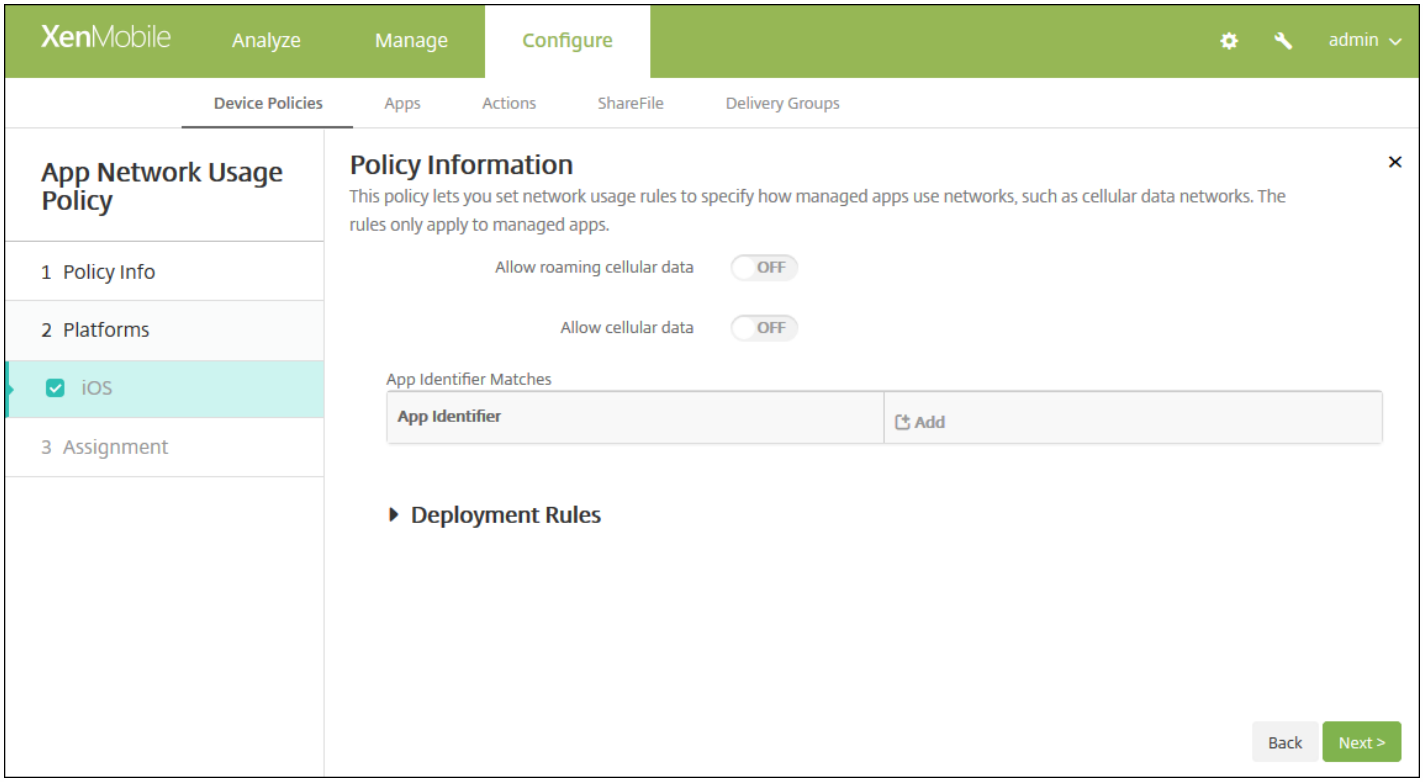
3. Expand **More**, and then under **Apps**, click **App Network Usage**. The **App Network Usage Policy** information page appears.



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.

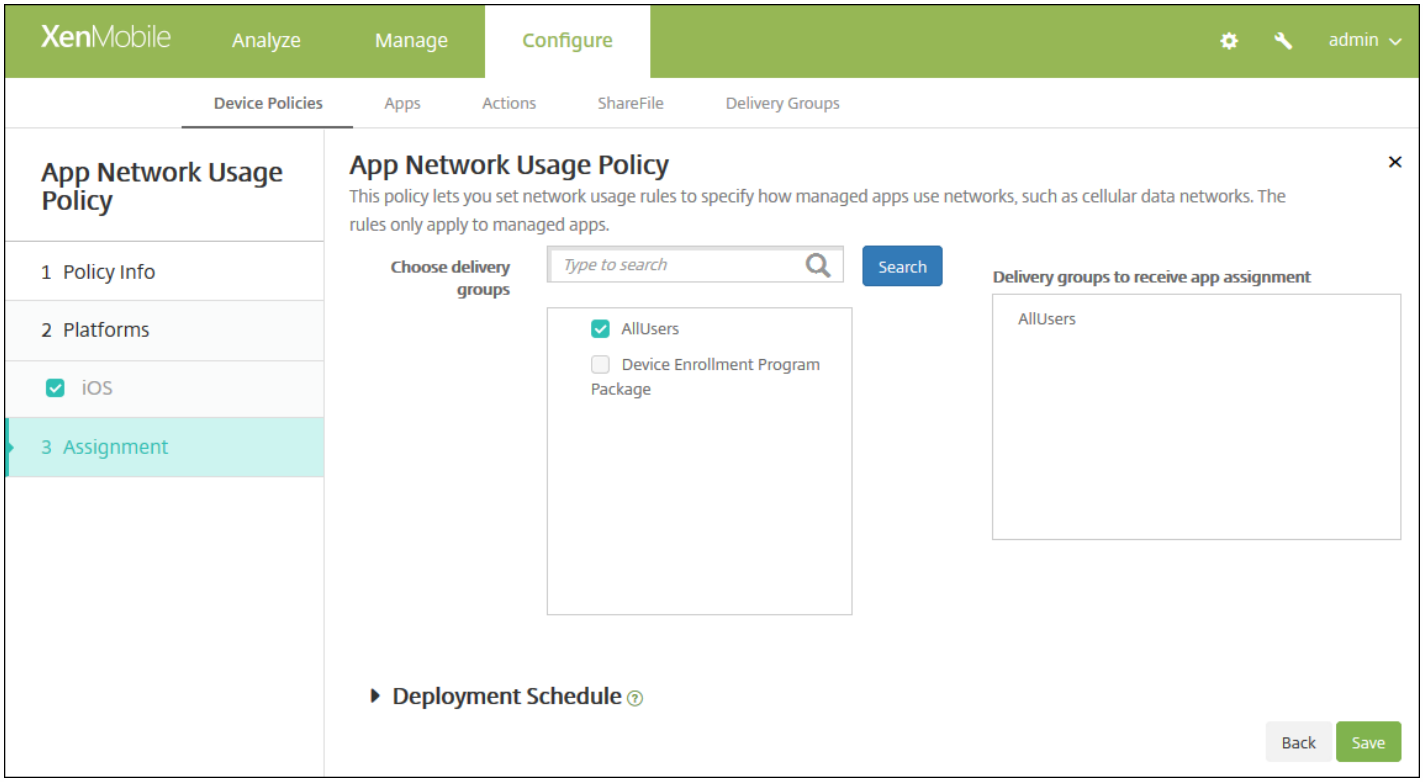
- **Allow roaming cellular data**: Select whether the specified apps can use a cellular data connection while roaming. The default is **OFF**.
- **Allow cellular data**: Select whether the specified apps can use a cellular data connection. The default is **OFF**.
- **App Identifier Matches**: For each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

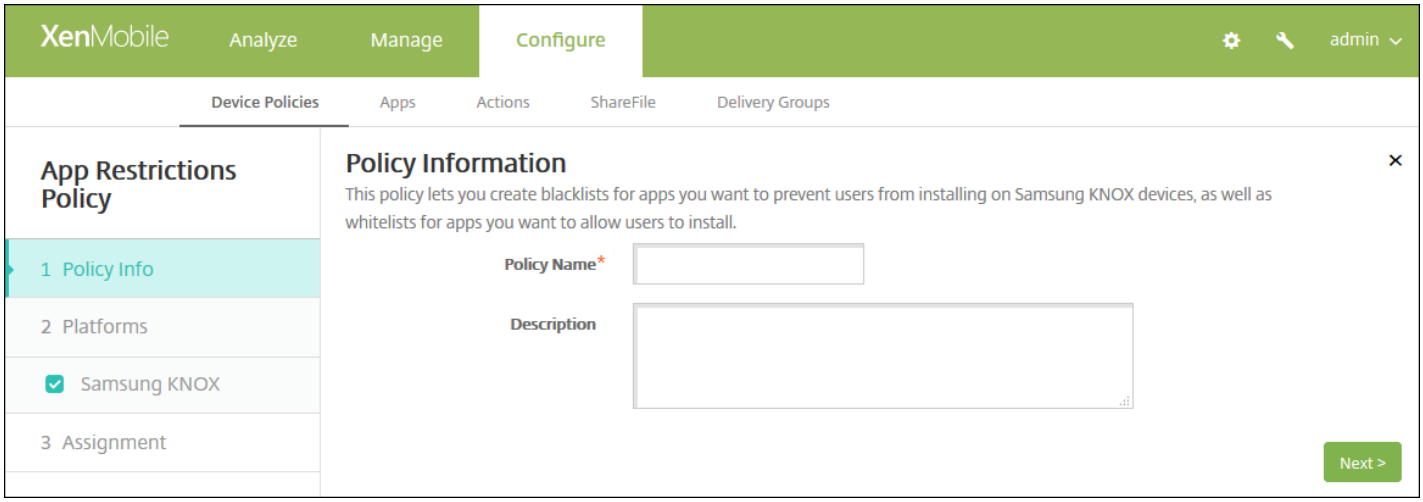
Oct 01, 2015

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.

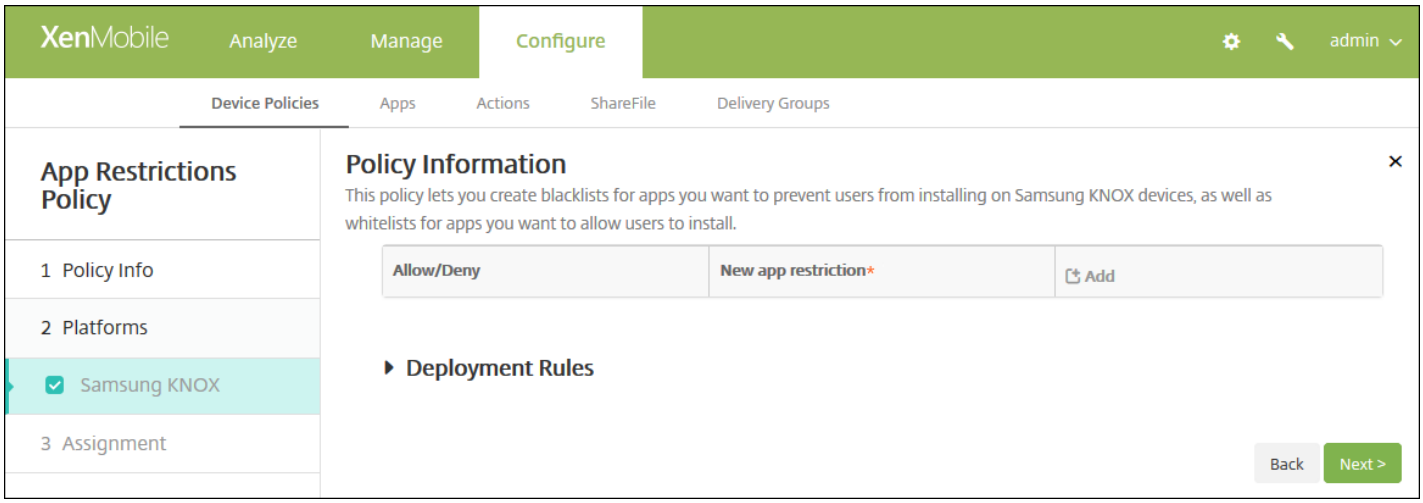
3. Expand **More** and then, under **Security**, click **App Restrictions**. The **App Restrictions Policy** information page appears.



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:

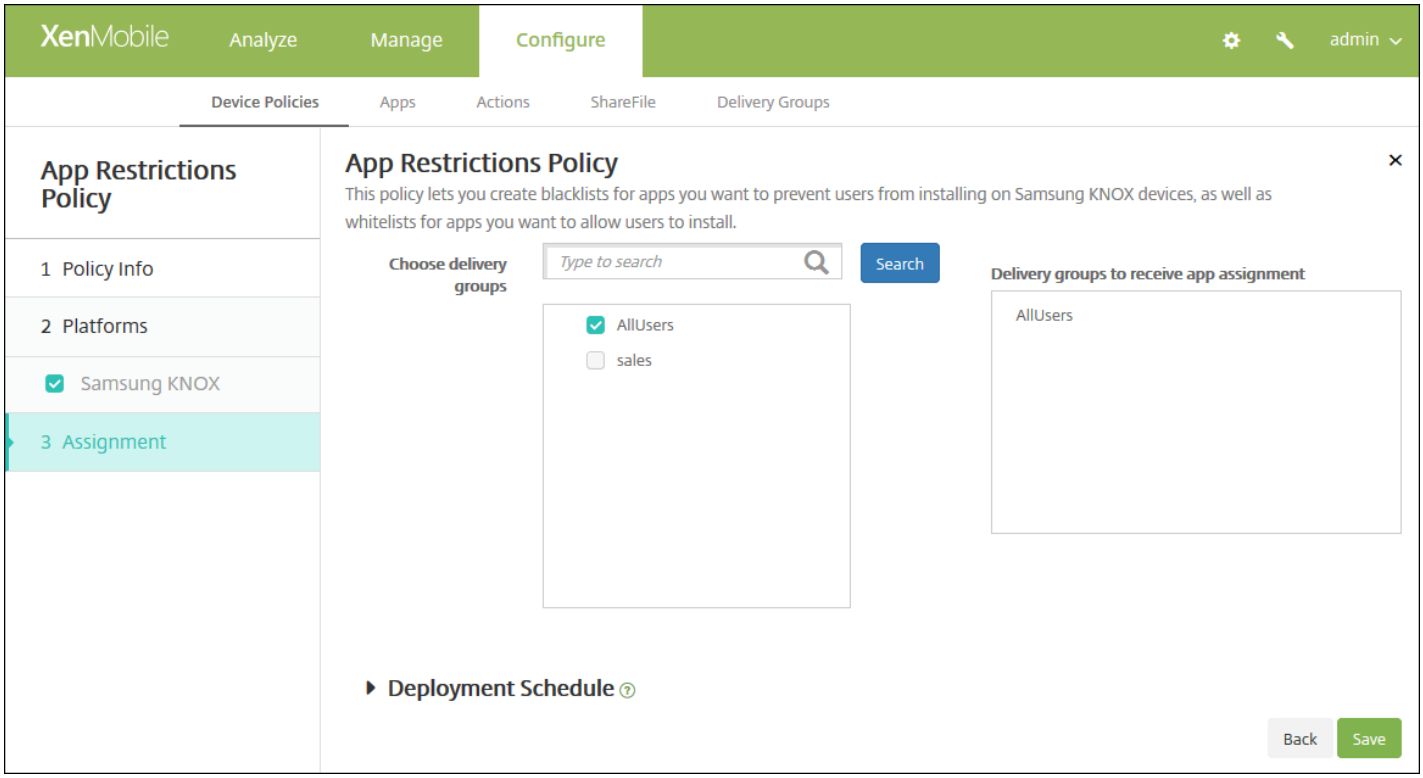
- **Allow/Deny**: Select whether users are allowed to install the app.
- **New app restriction**: Type the app package ID; for example, com.kmdm.af.crackle.
- Click **Save** to save the app to the Allow/Deny list or click **Cancel** to not save the app to the Allow/Deny list.

  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**.

App tunneling device policies

Mar 31, 2015

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.

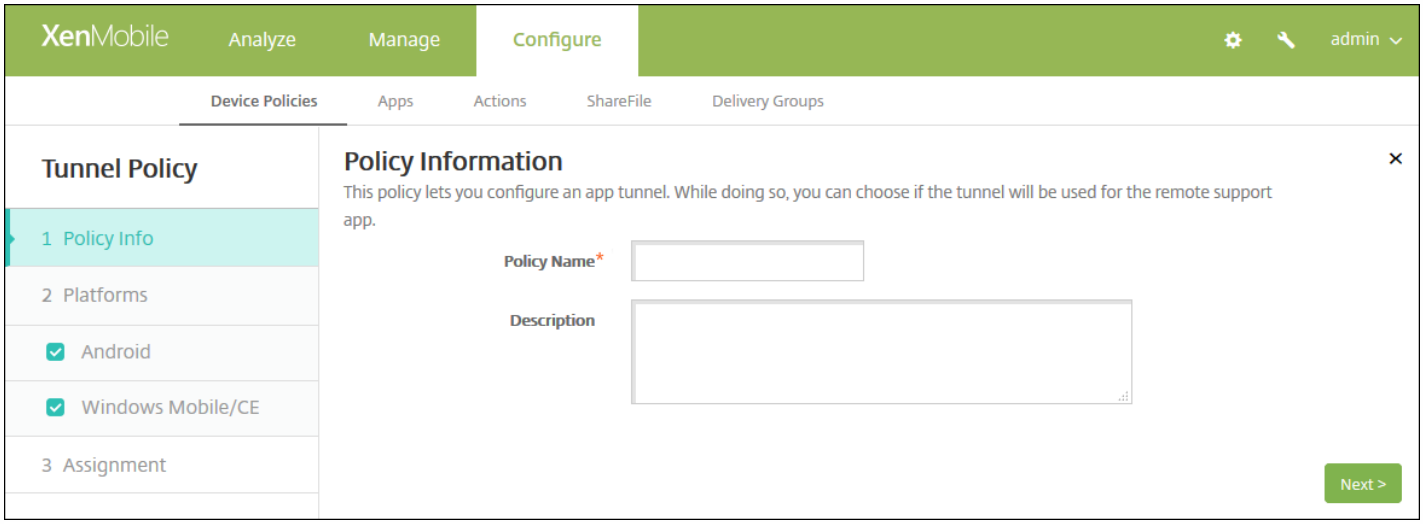
Android settings

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:

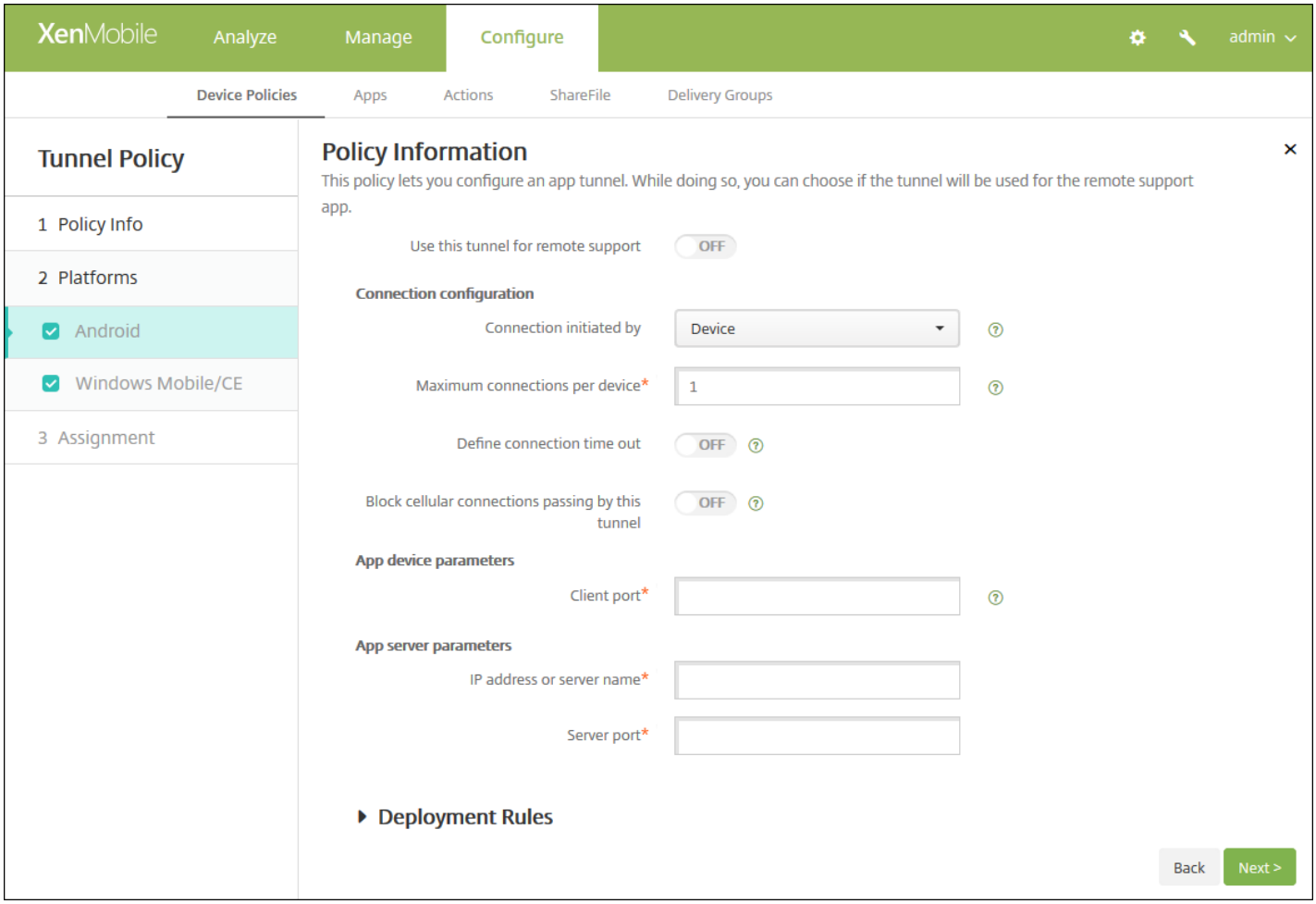
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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:

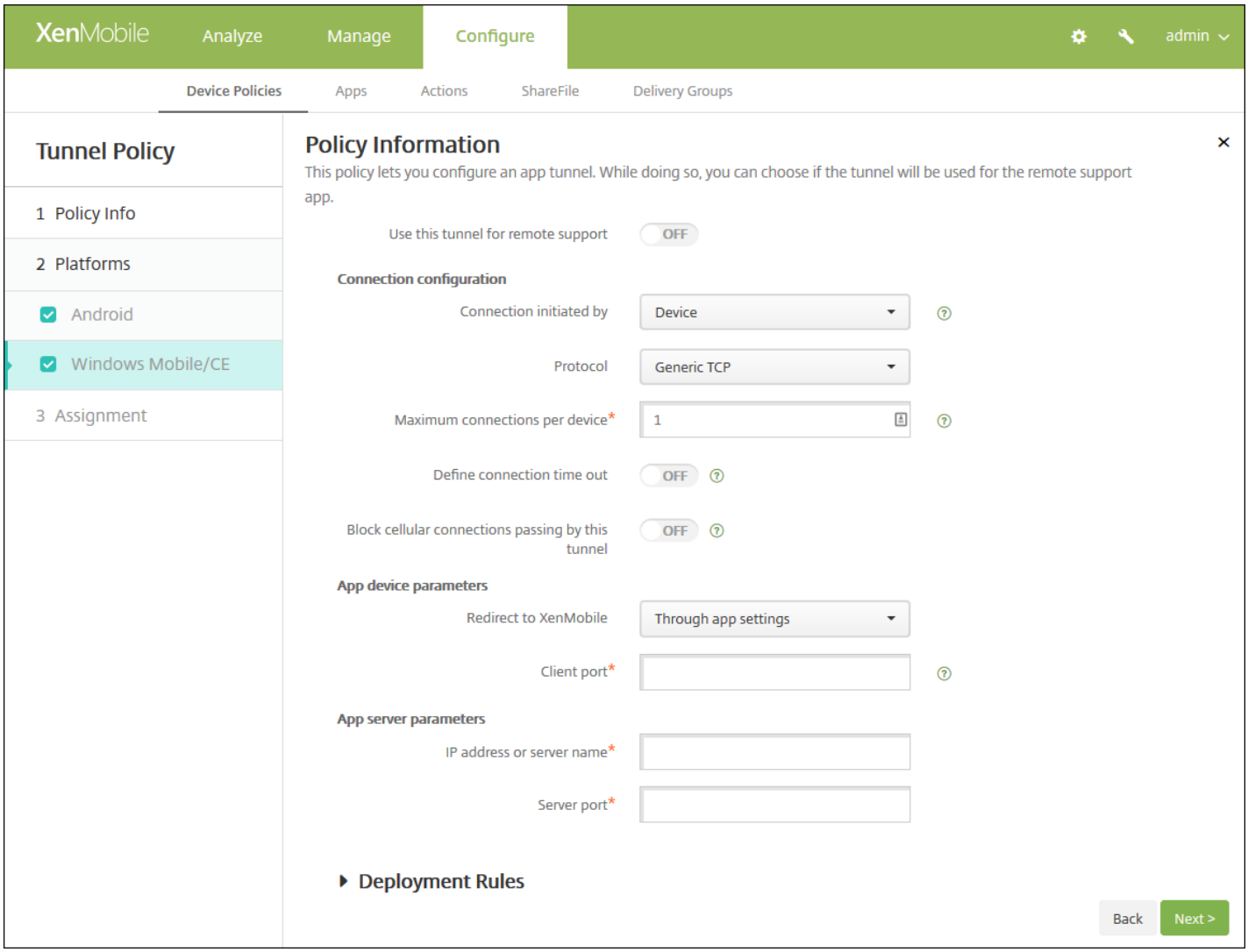
- **Use this tunnel for remote support:** Select whether the tunnel will be used for remote support.

  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

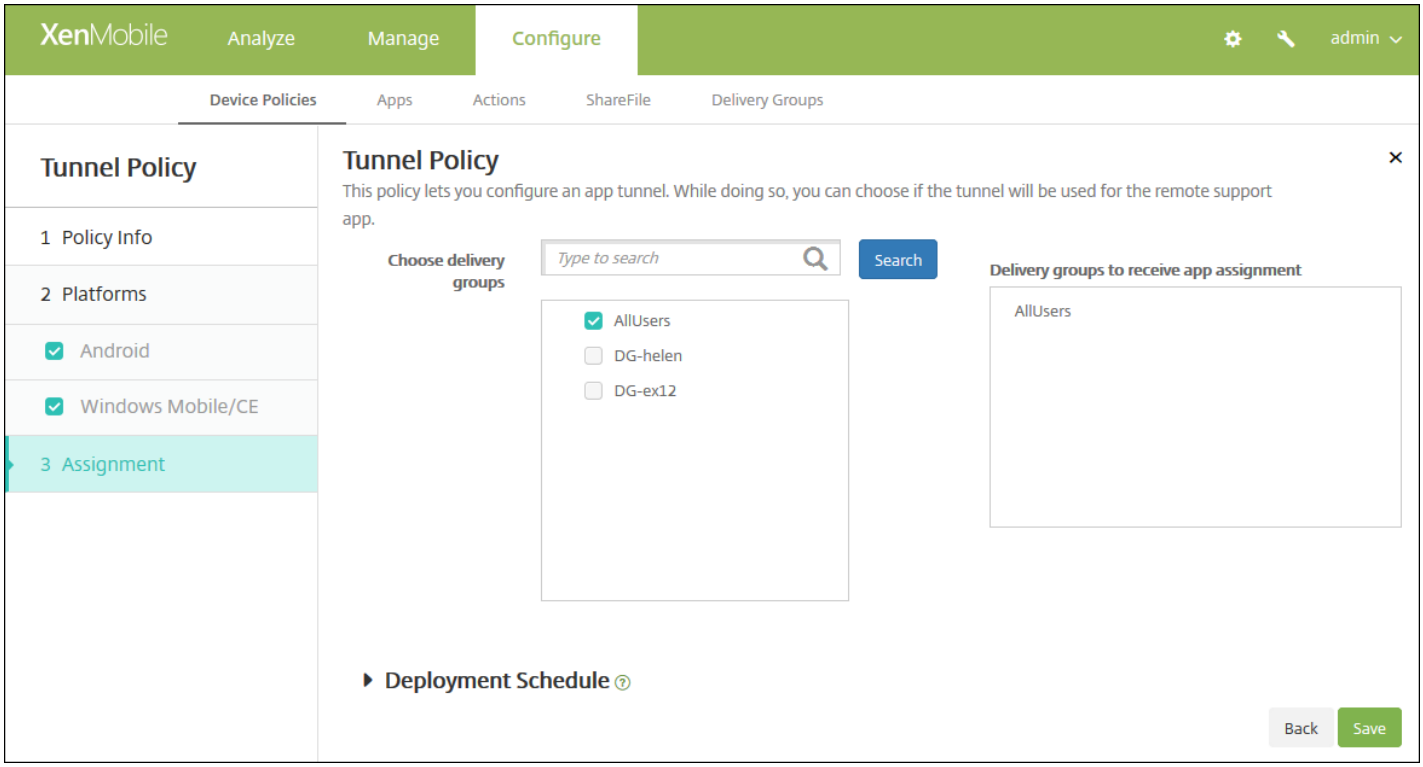
establish. This field applies only to device-initiated connections.

- **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 policies

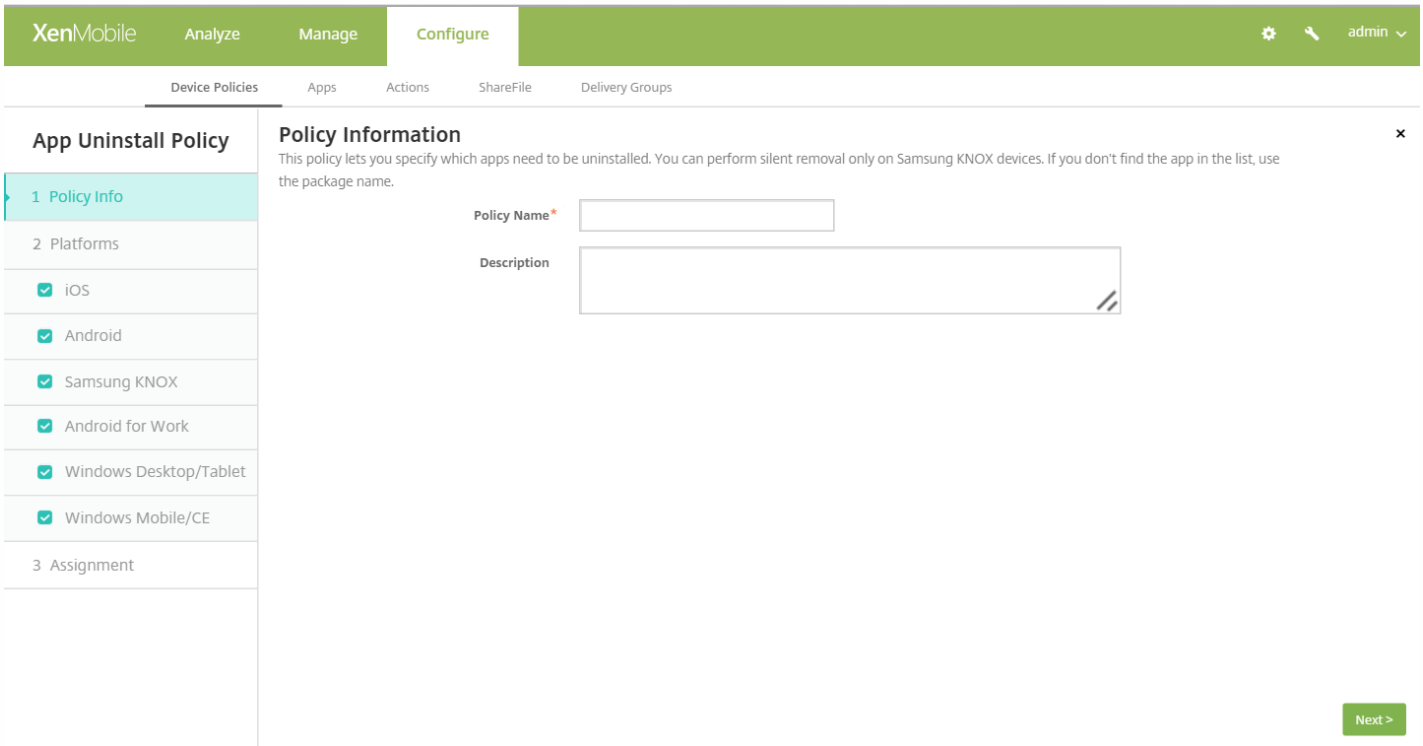
Jun 23, 2015

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:

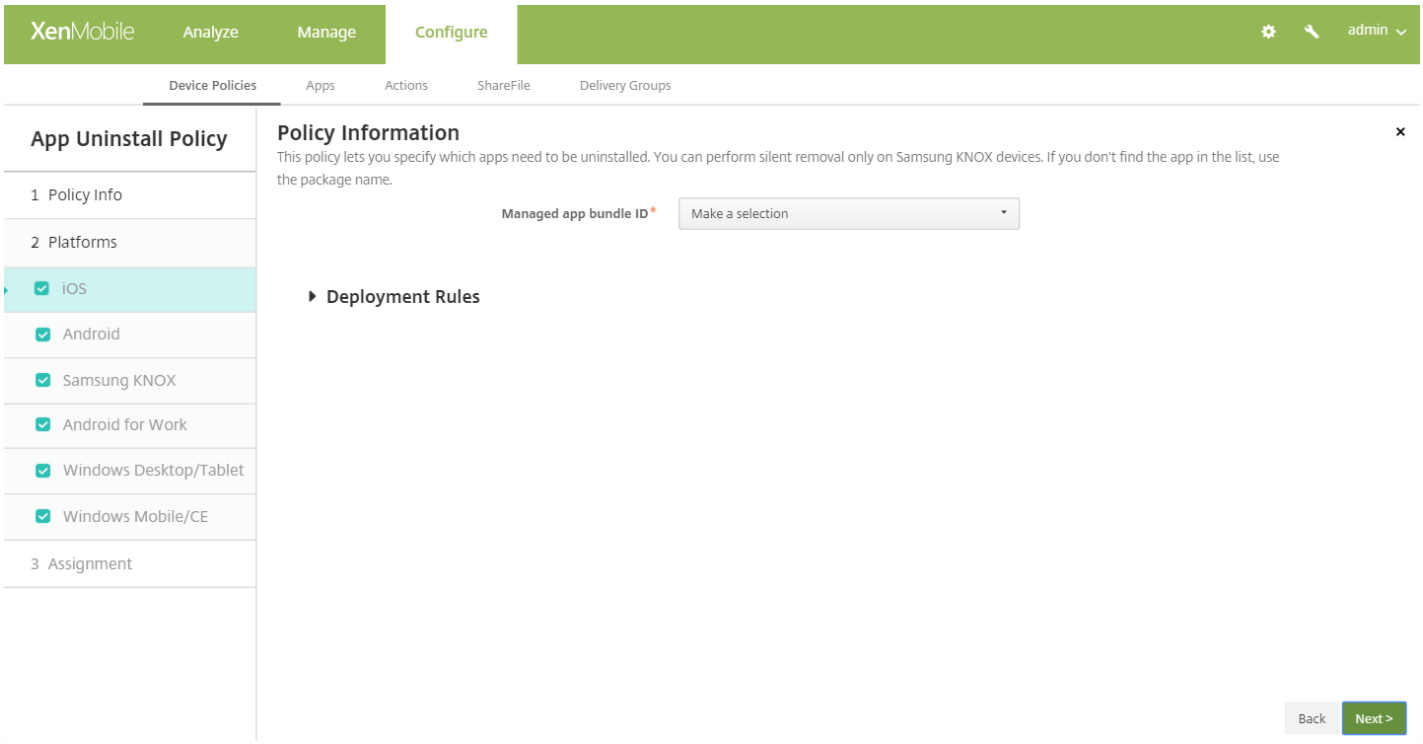
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

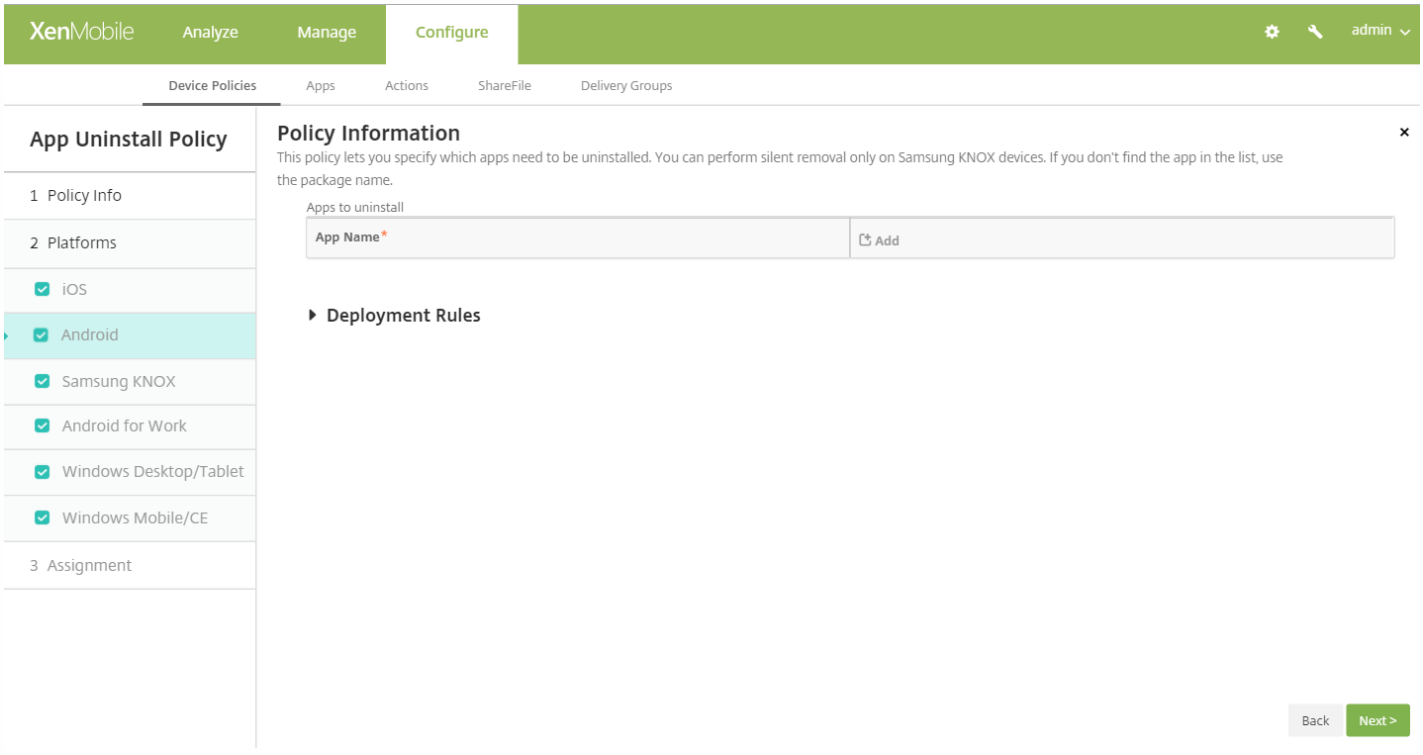
Configure iOS settings



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:

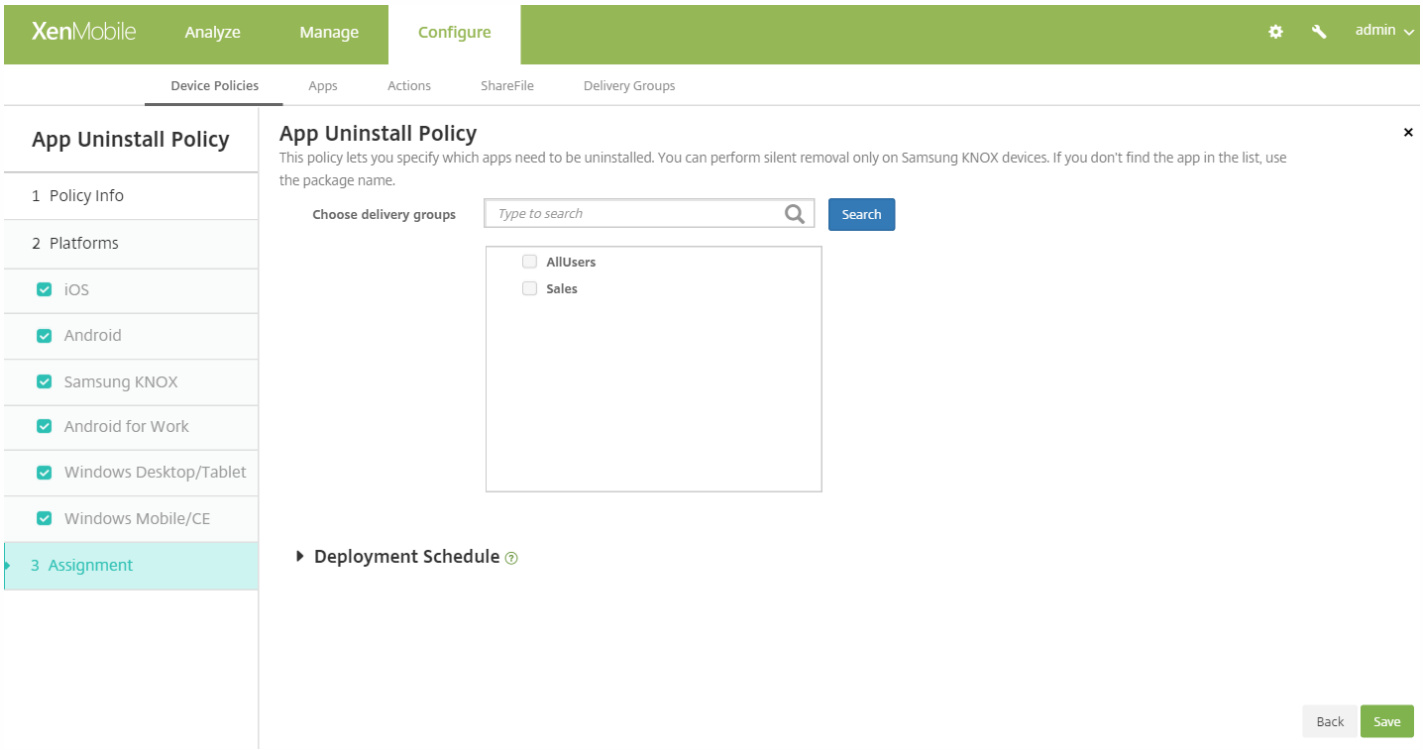
- **Apps to uninstall**: For each app you want to add, click **Add** and then do the following:
  - **App name**: In the list, click an existing app or click **Add new** to enter a new app name. If there are no apps configured for this platform, the list will be empty and you must add new apps.
  - Click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

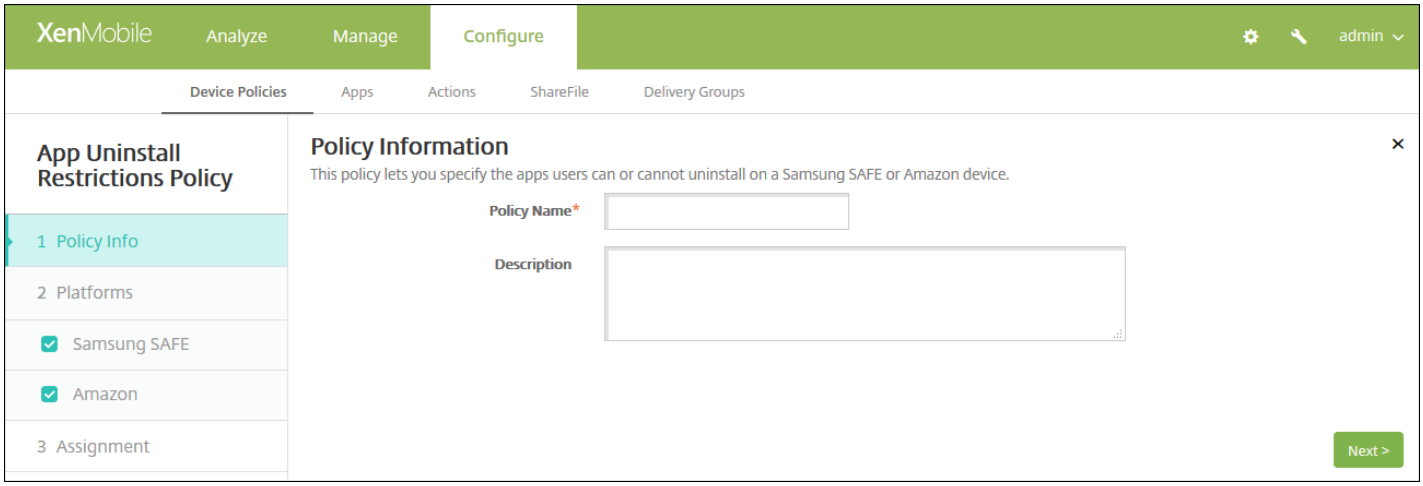
Sep 17, 2015

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.

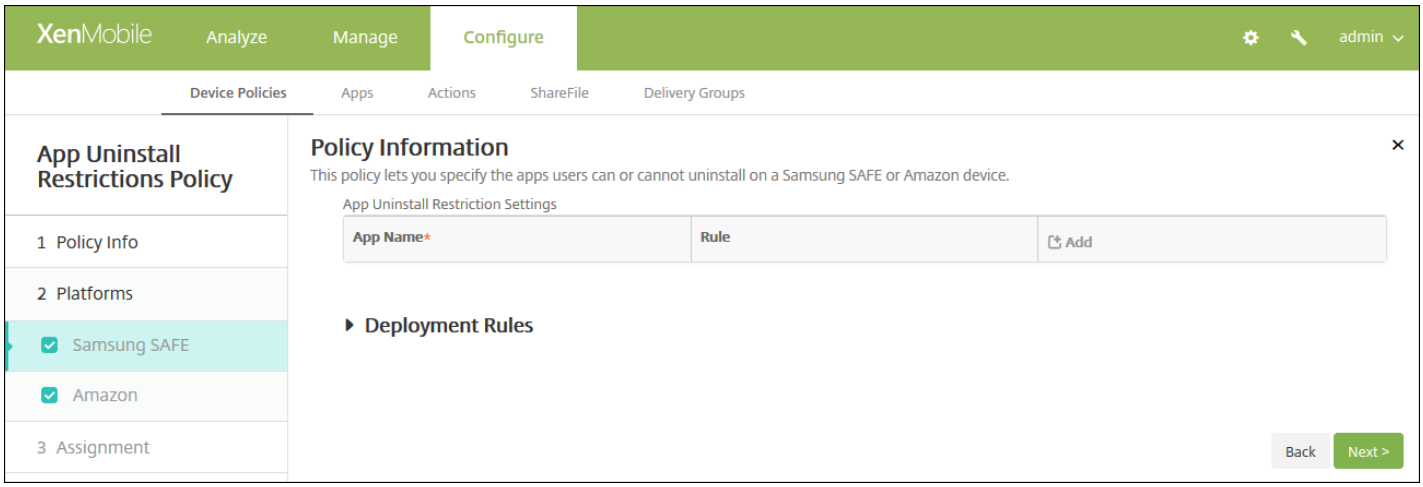
3. Expand **More**, and then under **Apps**, click **App Uninstall Restrictions**. The **App Uninstall Restrictions Policy** information page appears.



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:

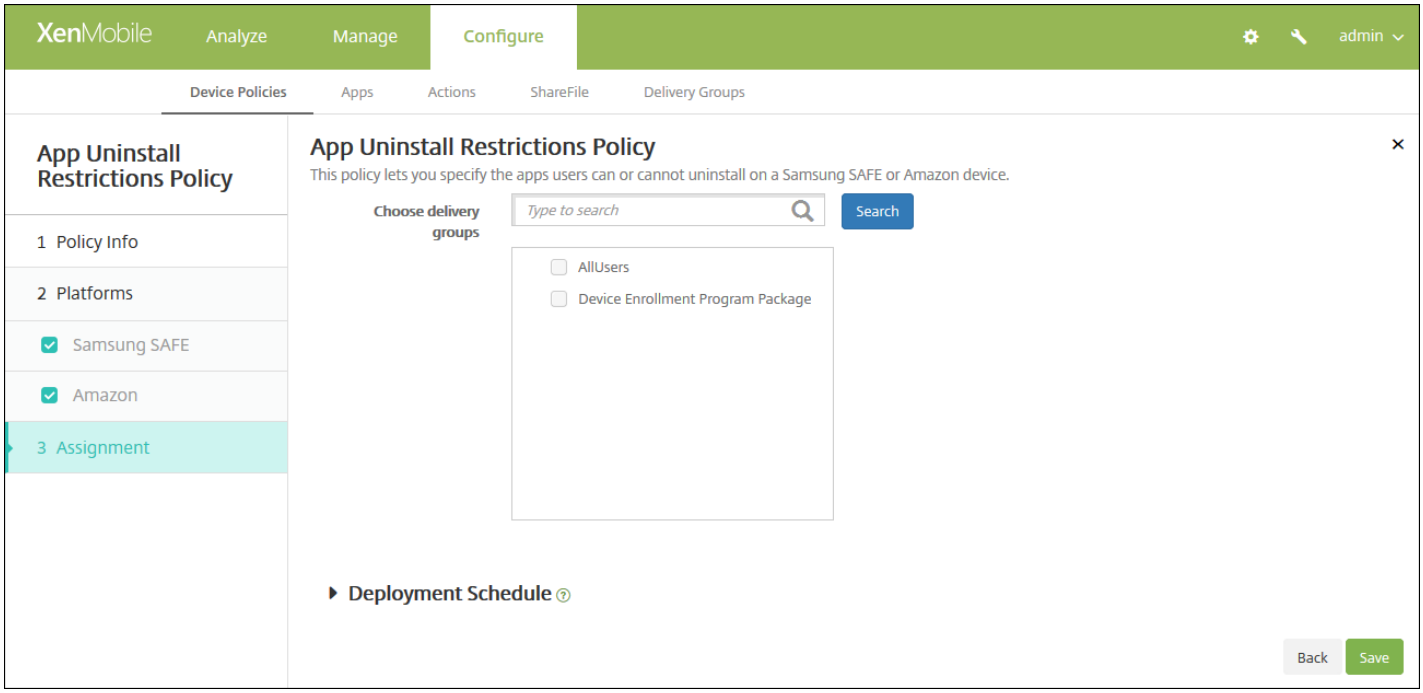
- **App Uninstall Restrictions Settings**: For each app rule you want to adds, click **Add** and then do the following:
  - **App Name**: In the list, click an app or **Add new** to add a new app.
  - **Rule**: Select whether users can uninstall the app. The default is to allow uninstallation.
  - Click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

11. Click **Save**.

Browser device policies

Jun 23, 2015

You can create browser device polices for Samsung SAFE, Samsung KNOX, and Android for Word devices to define whether users' devices can use the browser or to limit which browser functions users' 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. On Android for Works devices, you can blacklist or whitelist specific URLs, as well as add specific secure browser bookmarks.

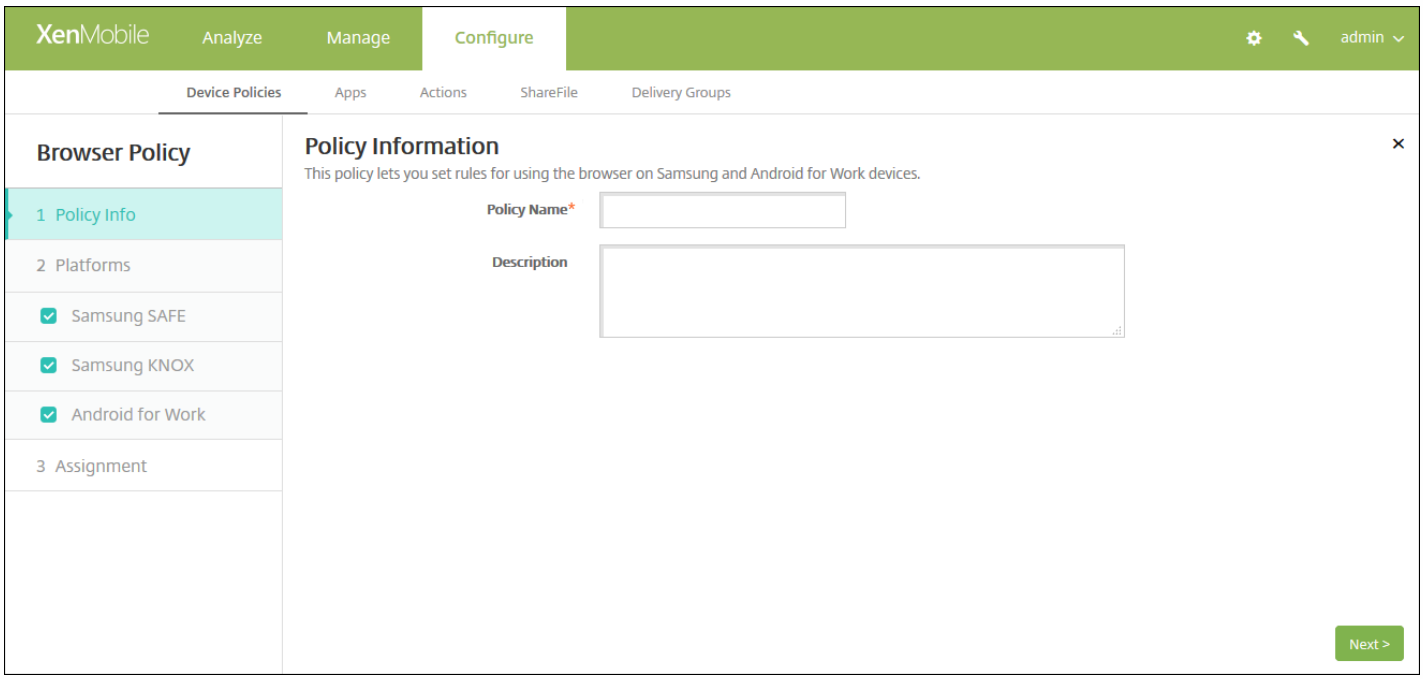
Samsung SAFE and Samsung KNOX settings

Android for Work 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:

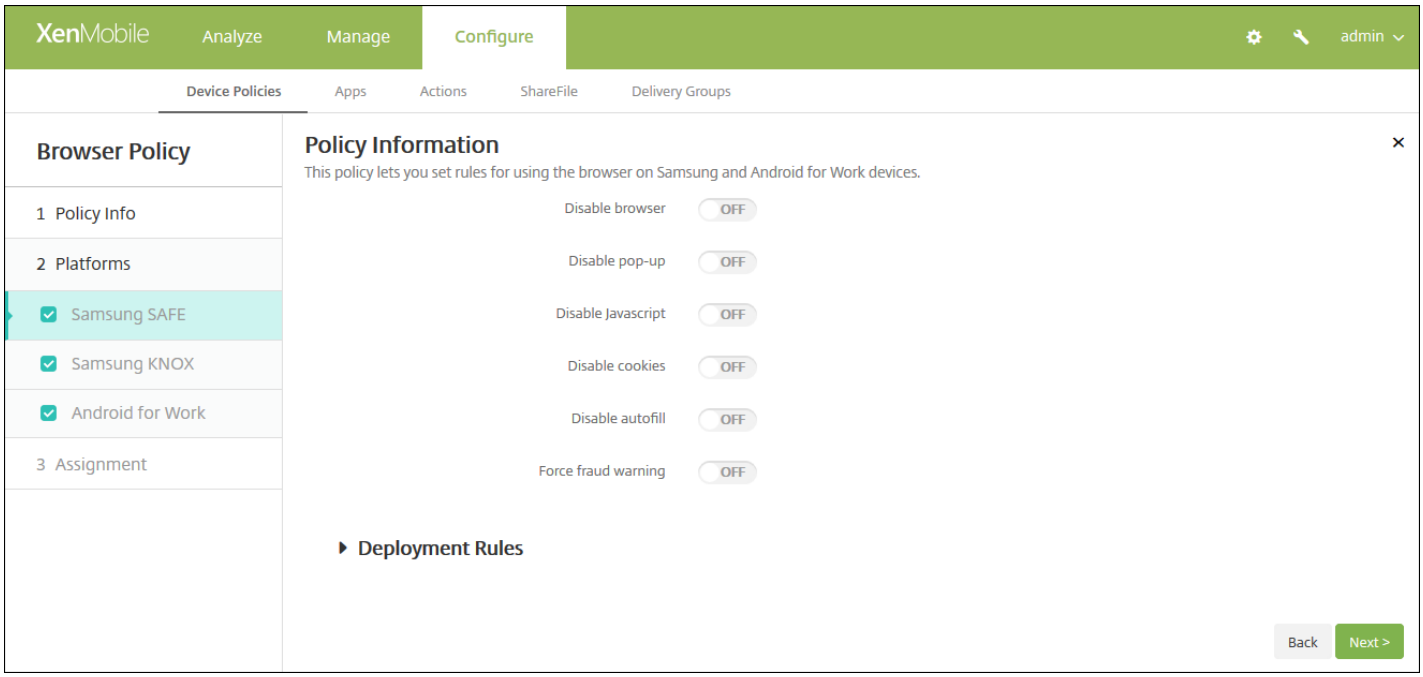
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

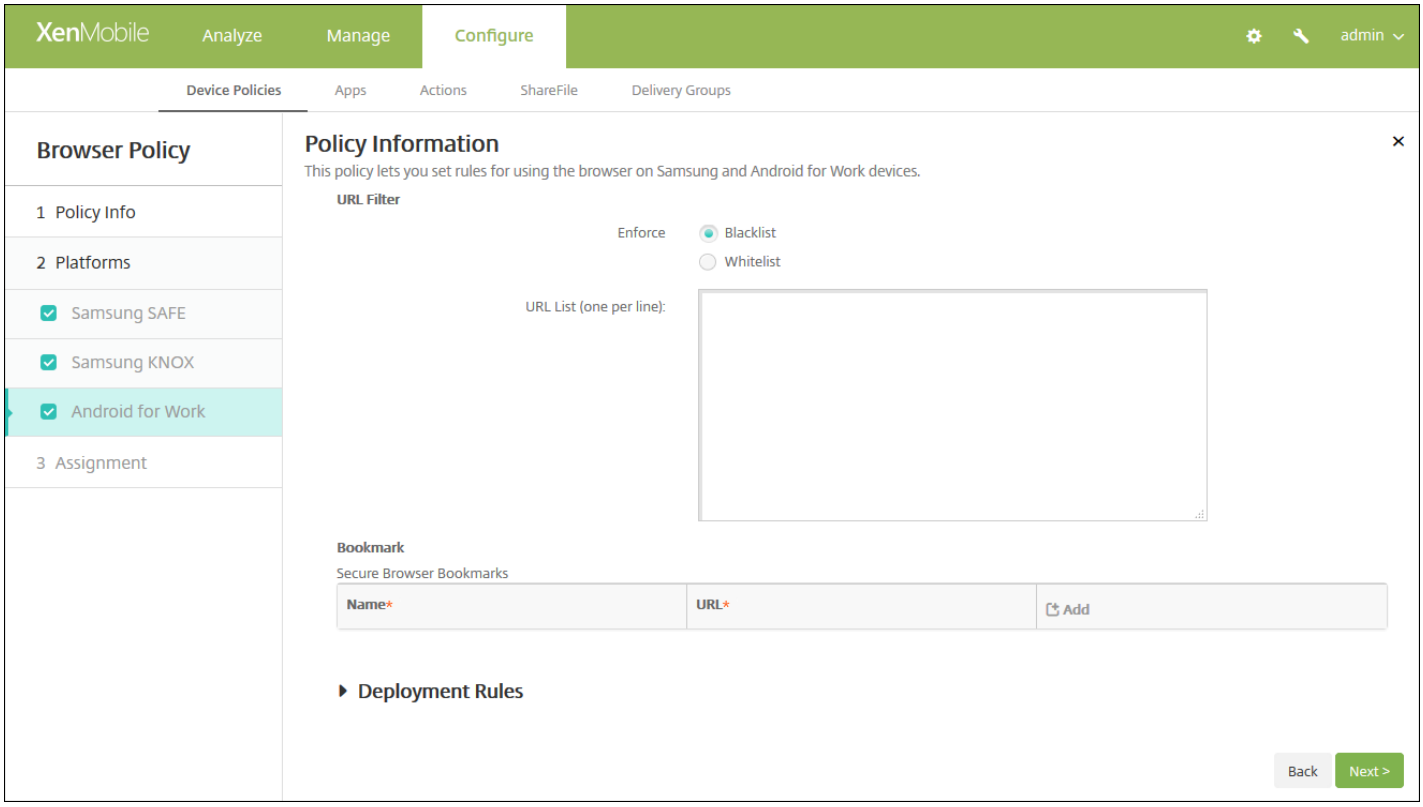
Configure Samsung SAFE and Samsung KNOX settings



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.

Configure Amazon for Work settings

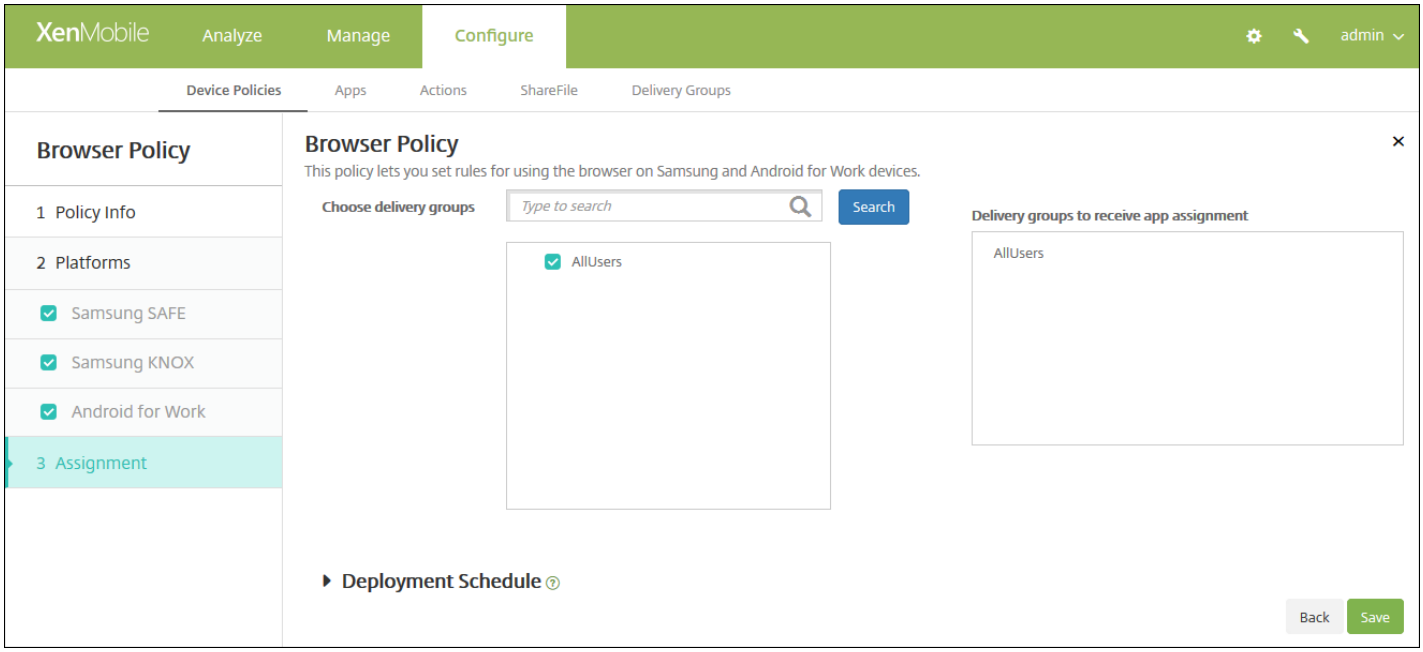


Configure these settings:

- Under **URL Filter**, configure these settings:
  - **Enforce**: Select either **Blacklist** or **Whitelist**. If you select **Blacklist**, users can access all URLs *except* those that you specify. If you select **Whitelist**, users can access *only* the URLs you specify.
  - **URL List**: Type the URLs (one per line) for the type of list you chose in **Enforce**.
- Under **Bookmark**, click **Add**, and type the **Name** and **URL** for the bookmarks that will appear in users' secure browsers.

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 policies

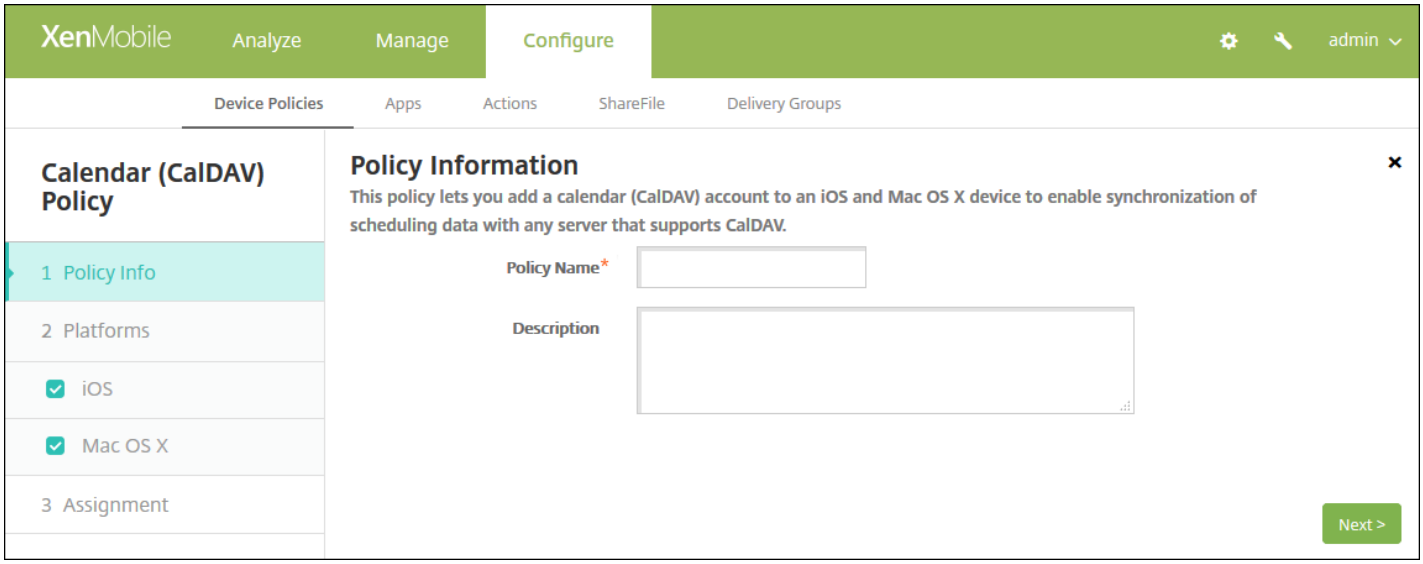
Feb 13, 2015

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:

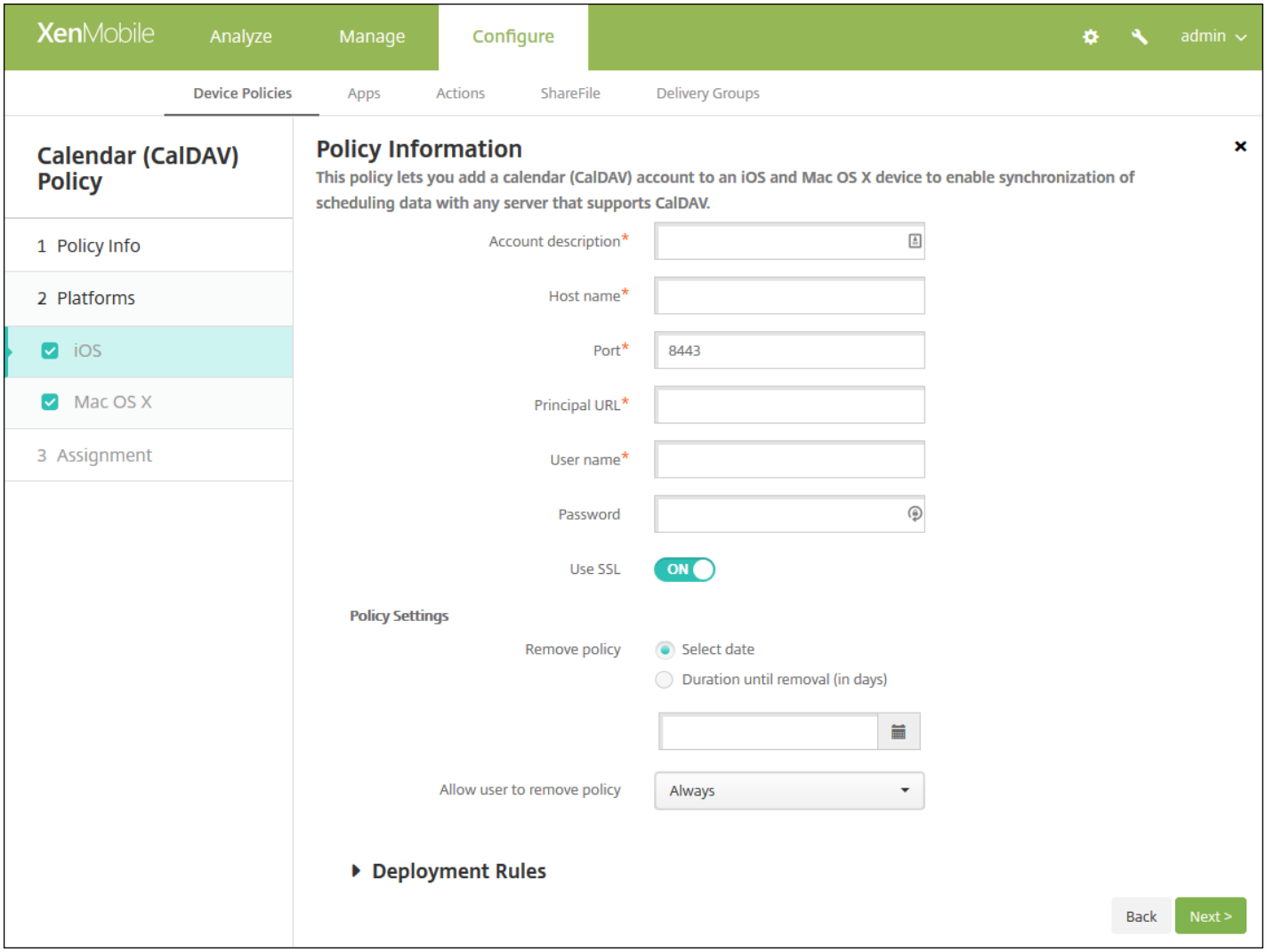
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

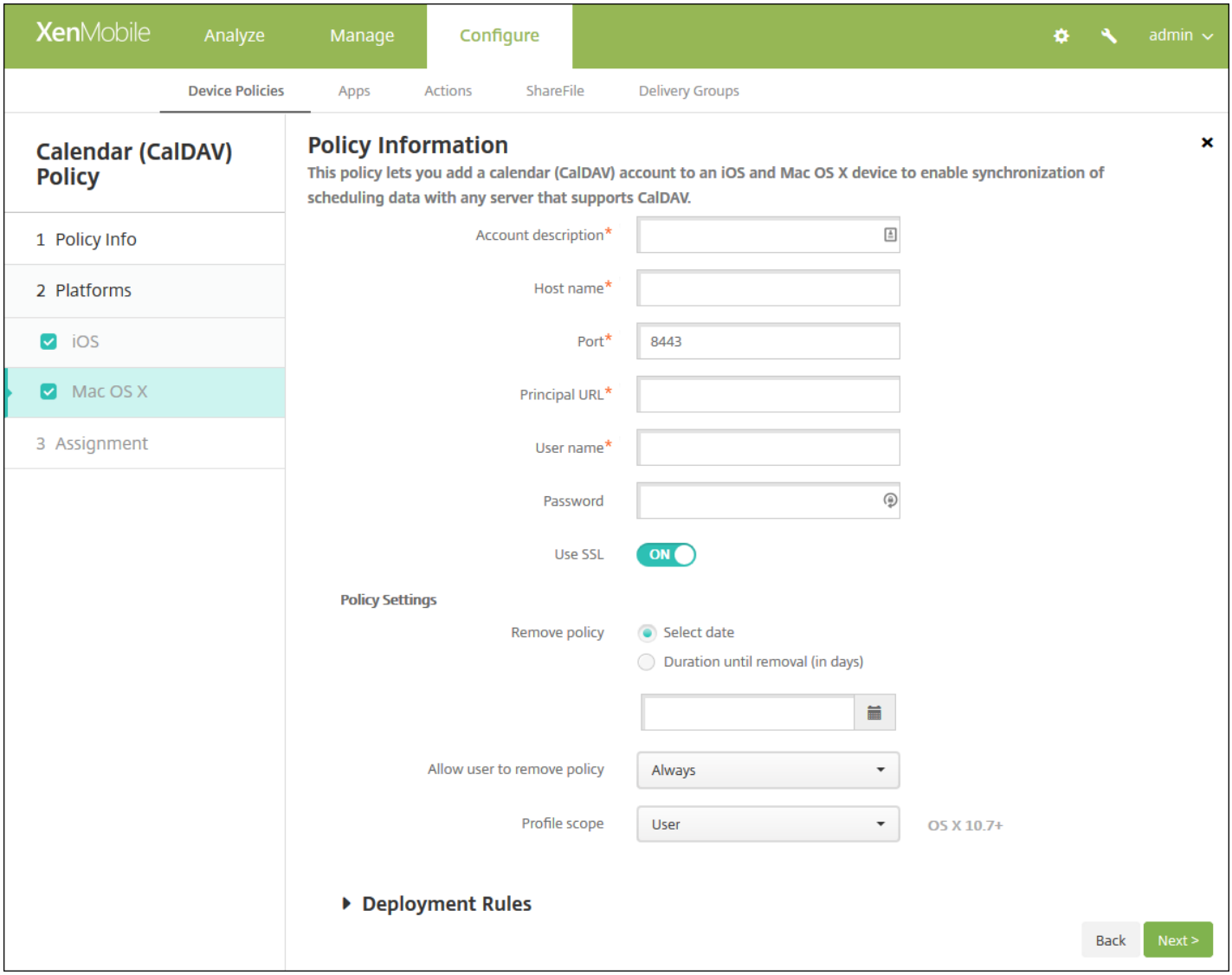
Configure iOS settings



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

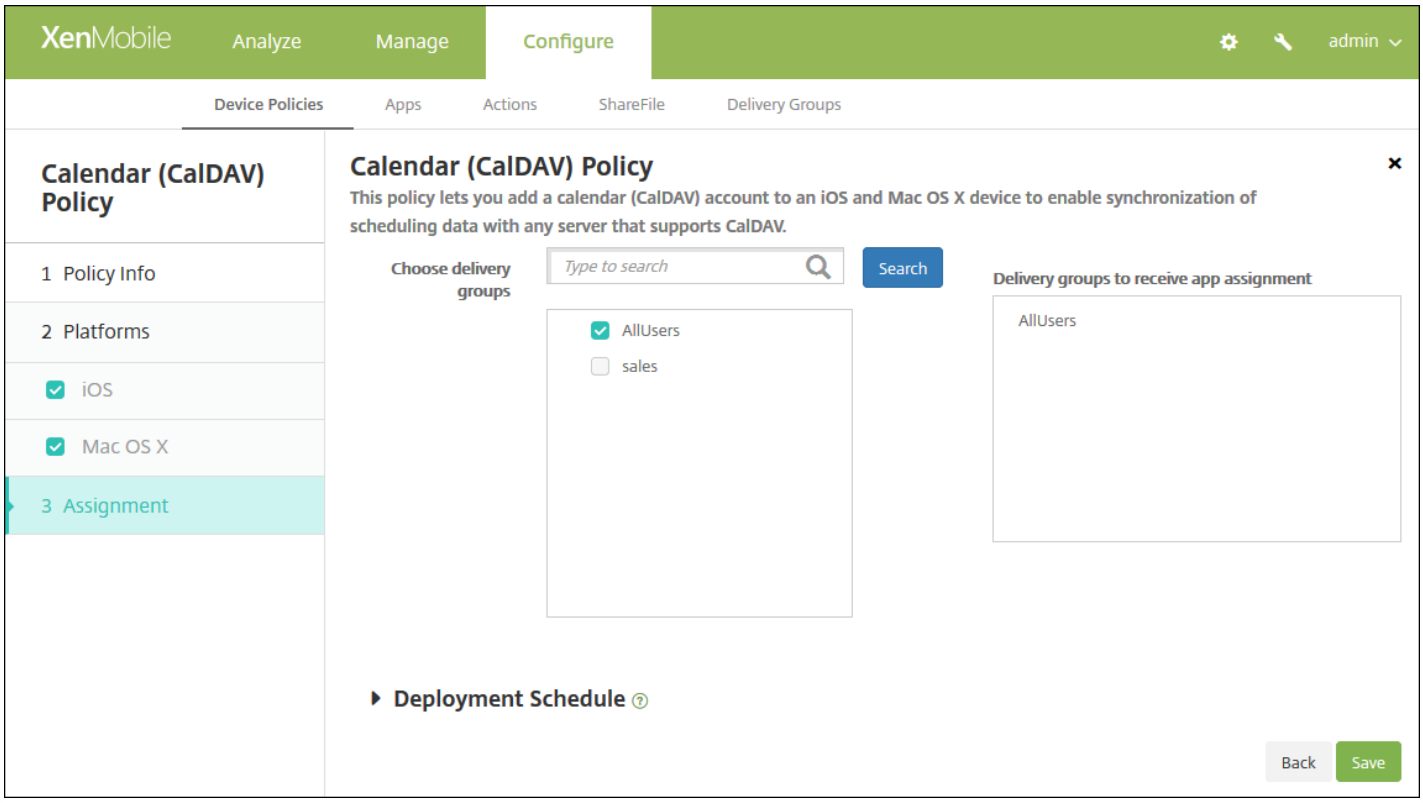


Configure the following settings:

- **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

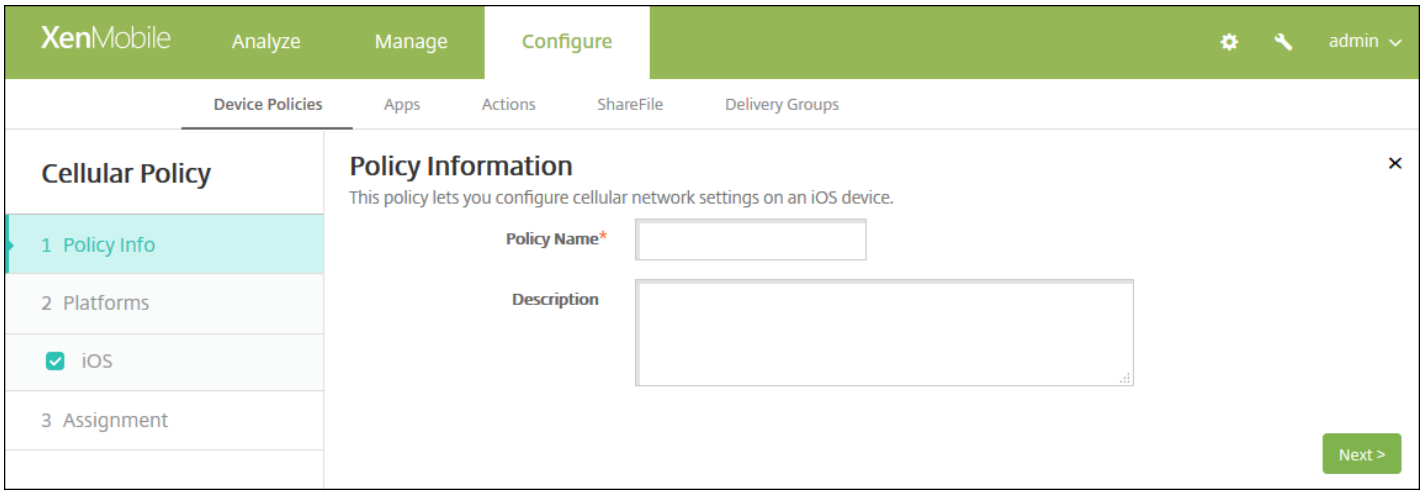
Feb 27, 2015

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.

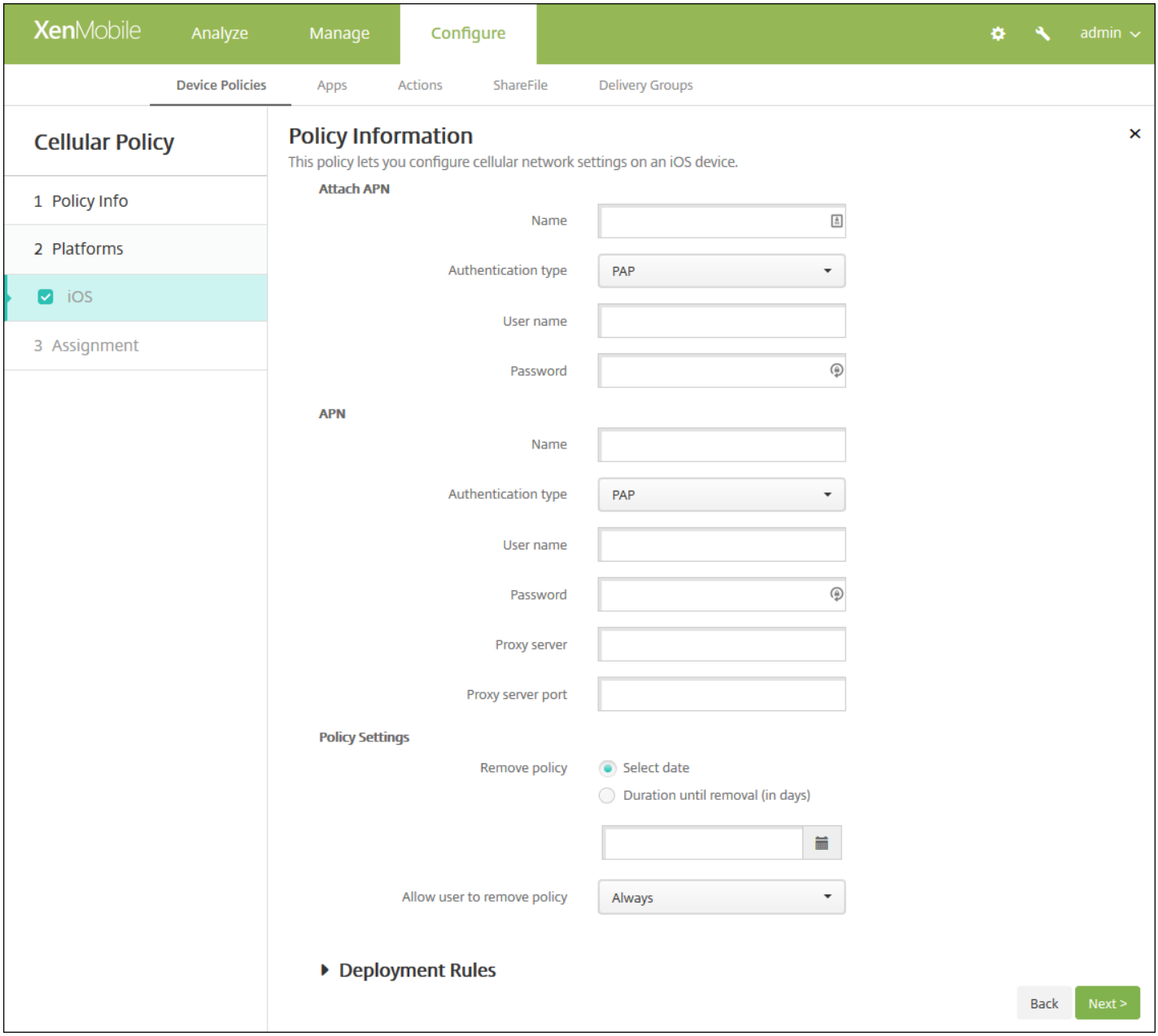
3. Expand **More**, and then, under **Network Access**, click **Cellular**. The **Cellular Network Policy** information page appears.



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.



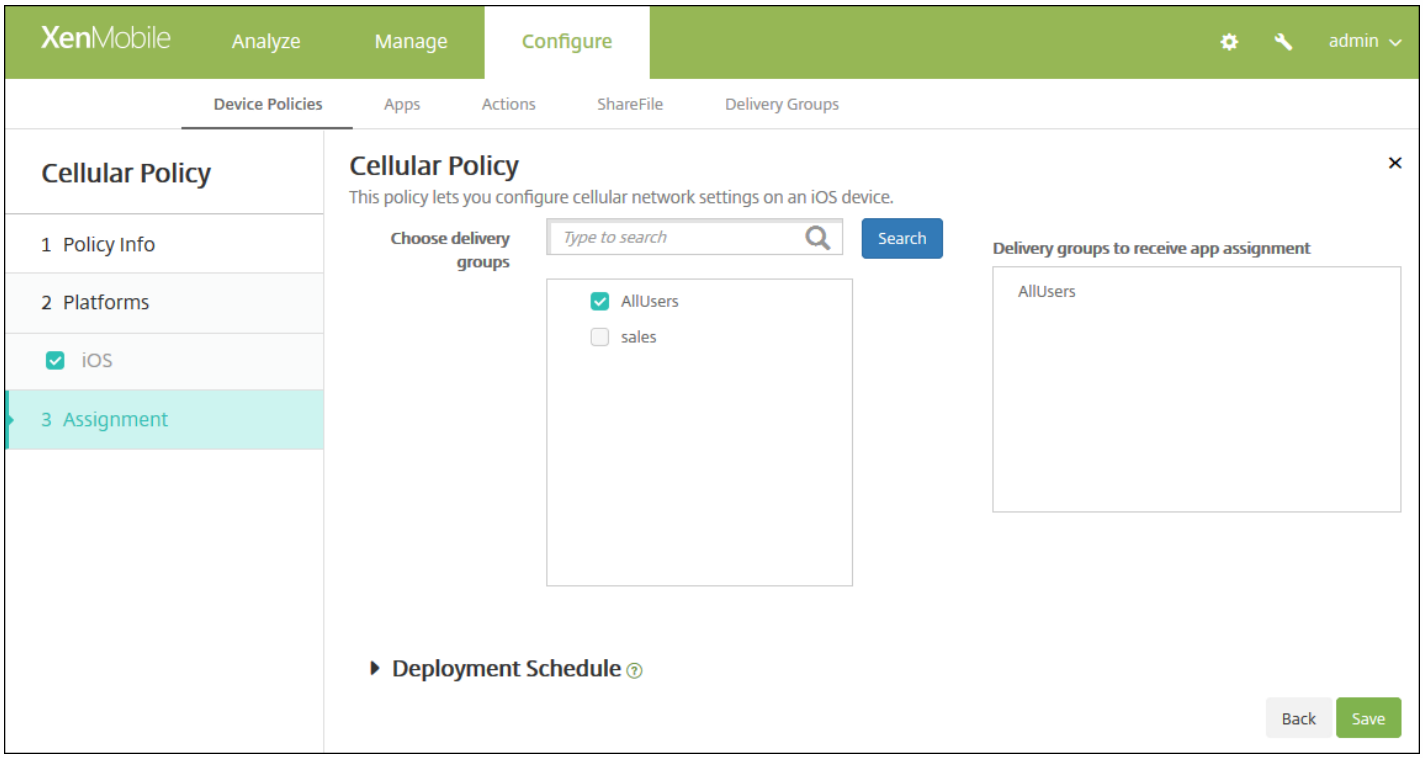
6. Configure these settings:

- **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

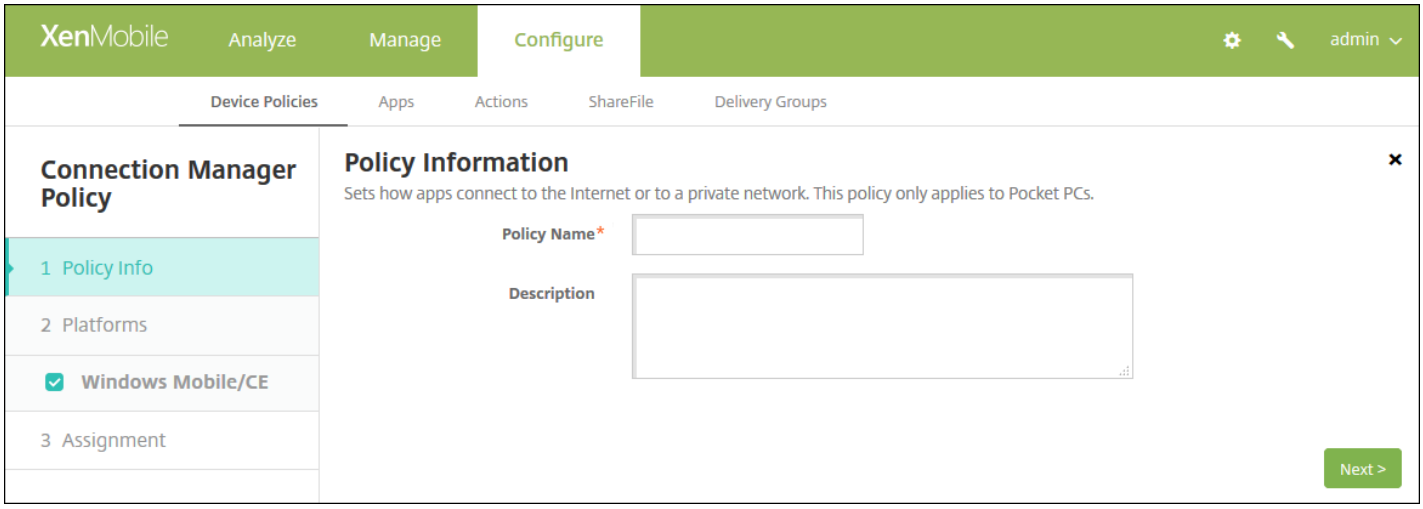
Sep 08, 2015

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.

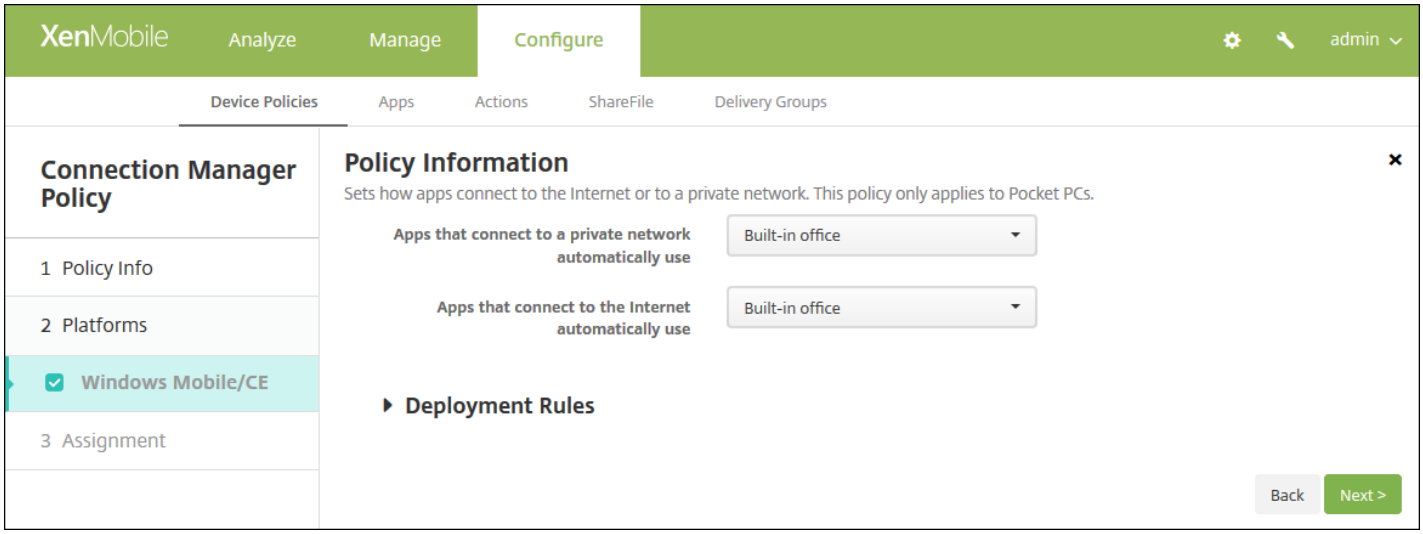
3. Click **More**, and then, under **Network Access**, click **Connection manager**. The **Connection Manager** policy information page appears.



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.



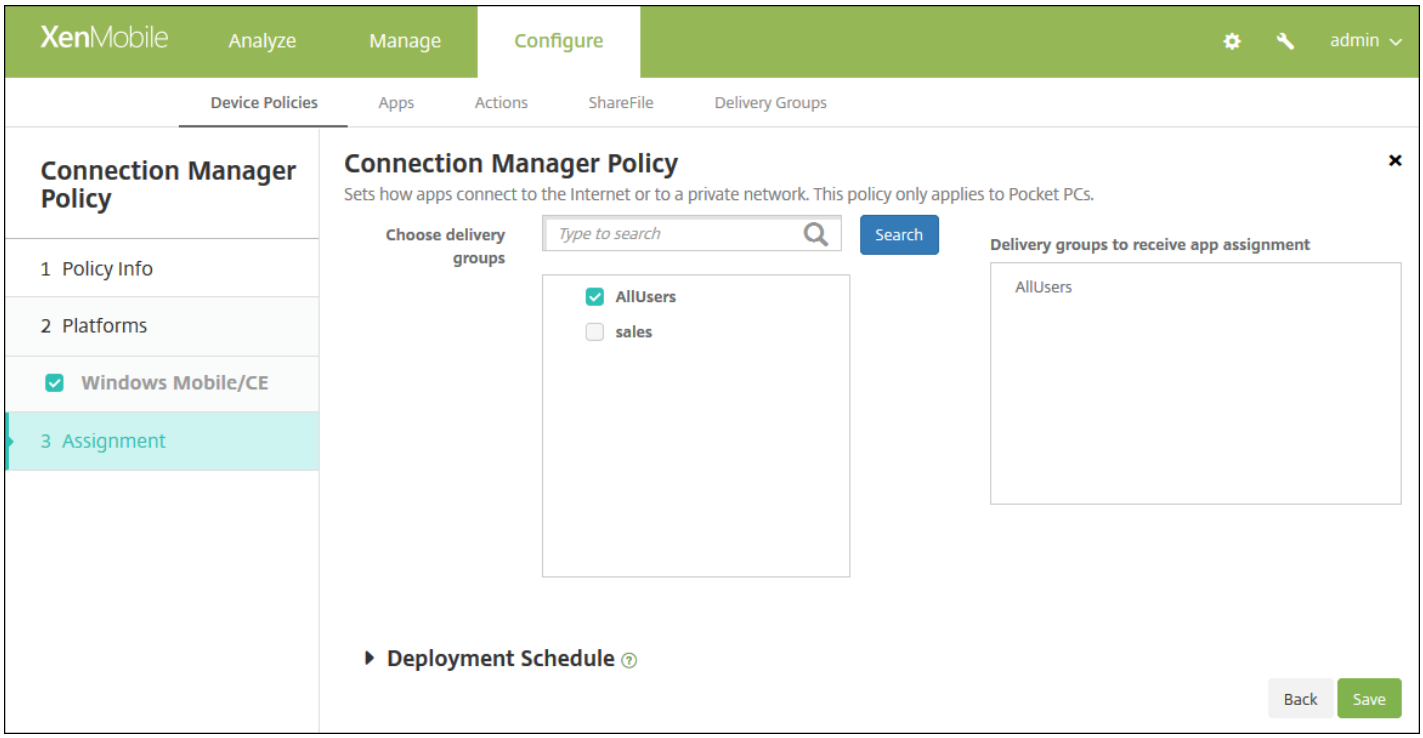
6. Configure these settings.

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 policies

May 31, 2016

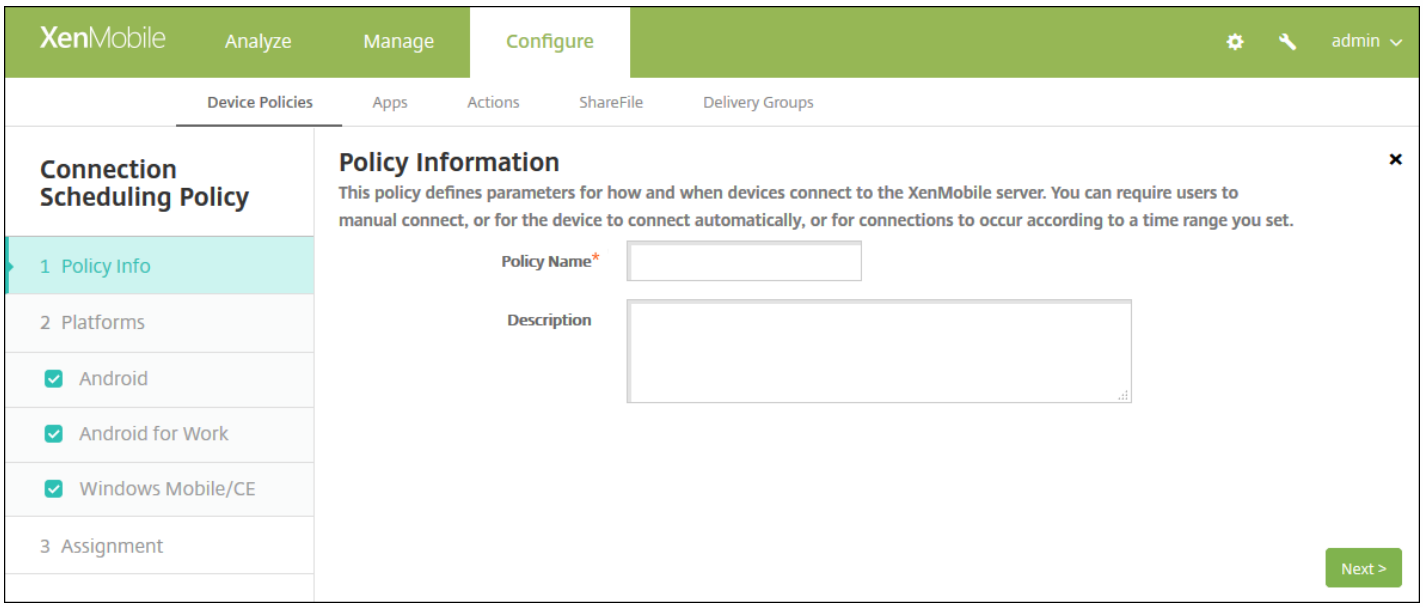
You create connection scheduling policies to control how and when users' devices connect to XenMobile. Note that you can configure this policy for devices enabled for Android for Work as well.

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.

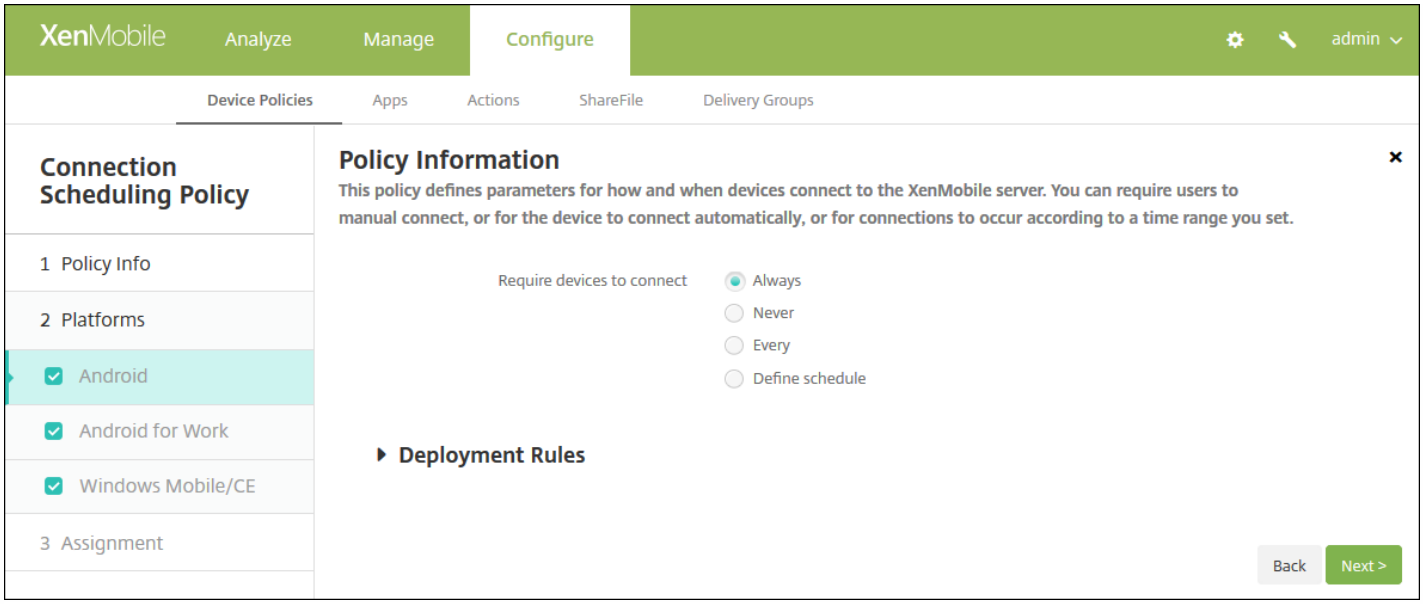
3. Click **Scheduling**. The **Connection Scheduling Policy** information page appears.



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.

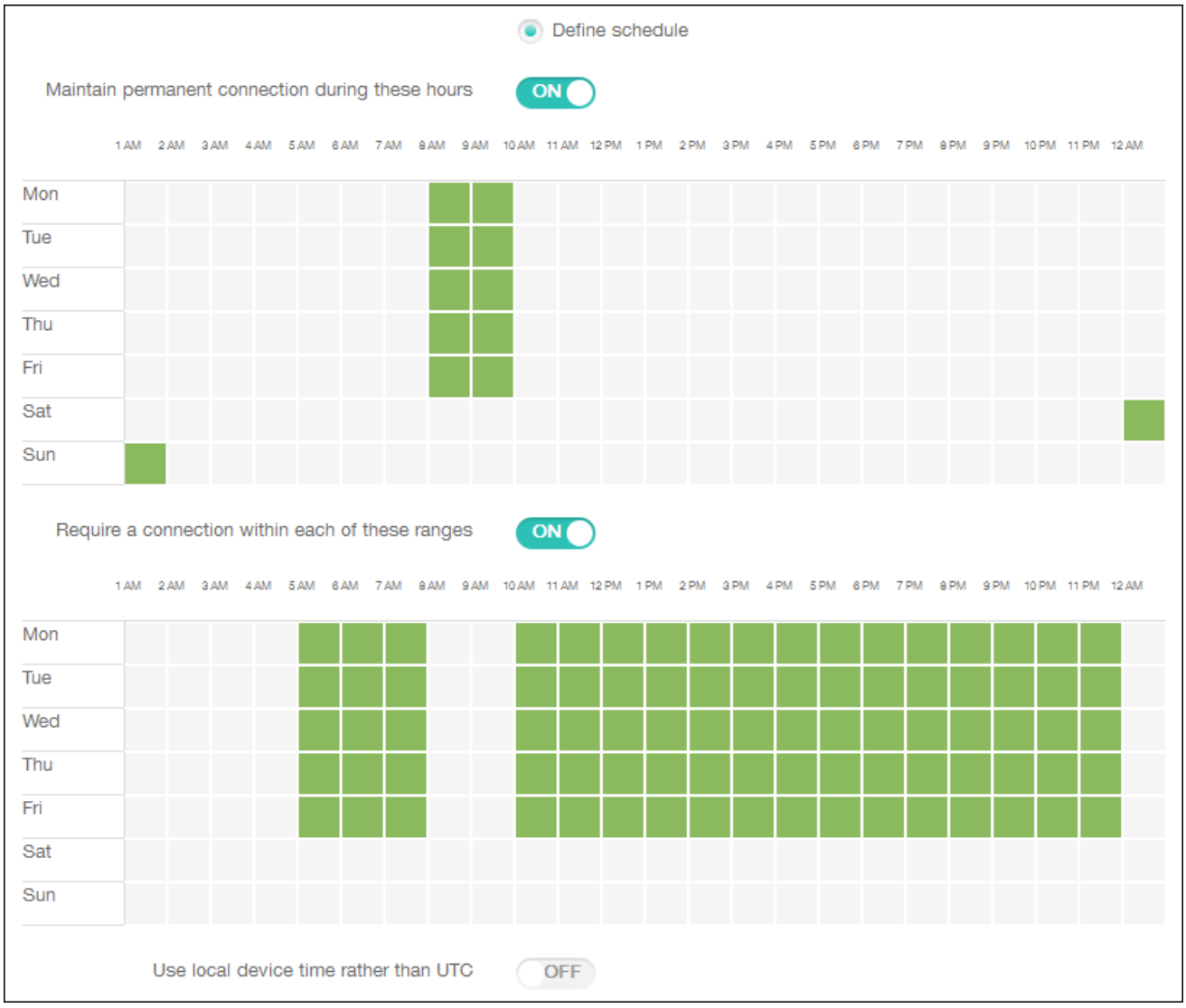
7. Configure the following settings for each of the platforms you selected:

- **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

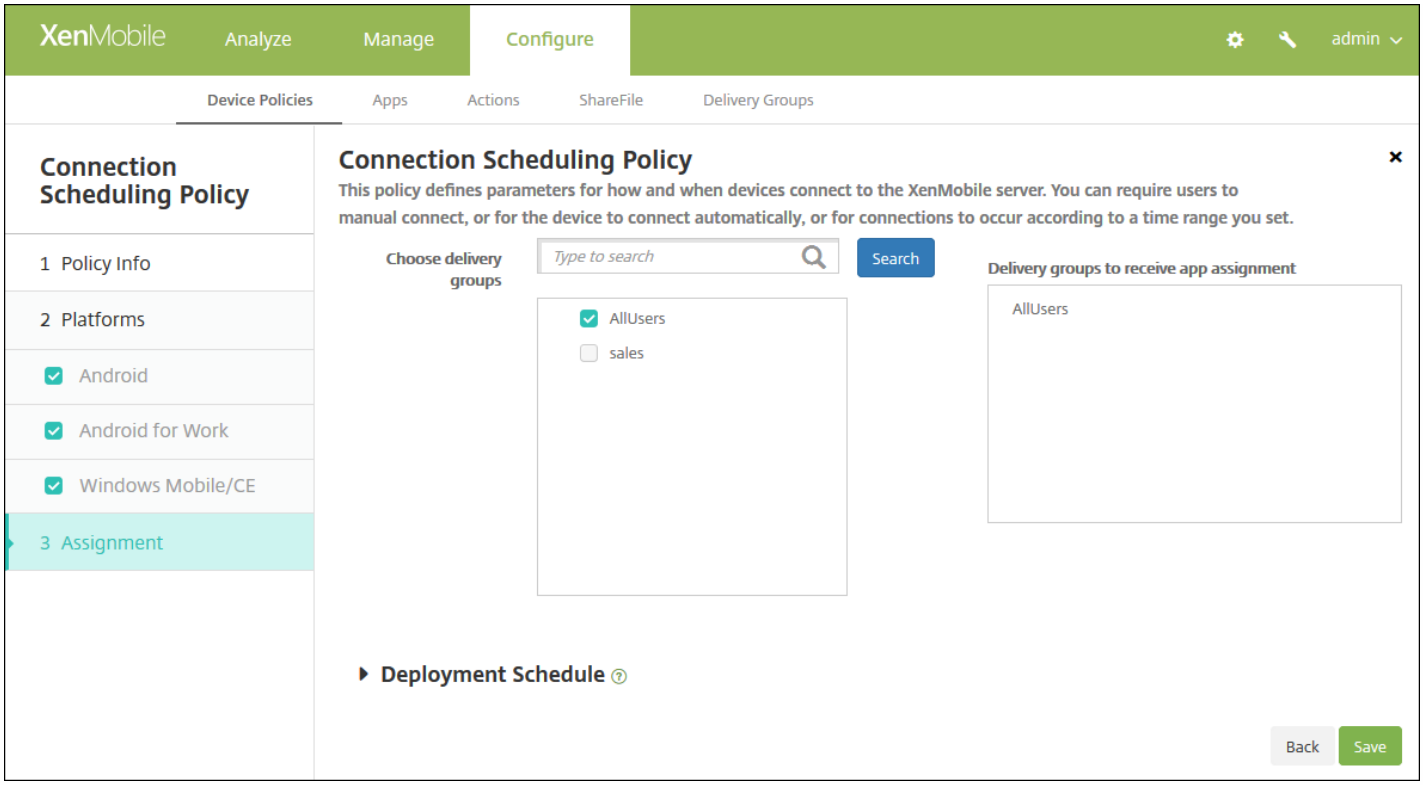
When you enable the following options, a timeline appears where you can define the time frames you want. You can enable either or both options to require a permanent connection during specific hours or to require a connection within certain time frames. Each square in the timeline is 30 minutes, so if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

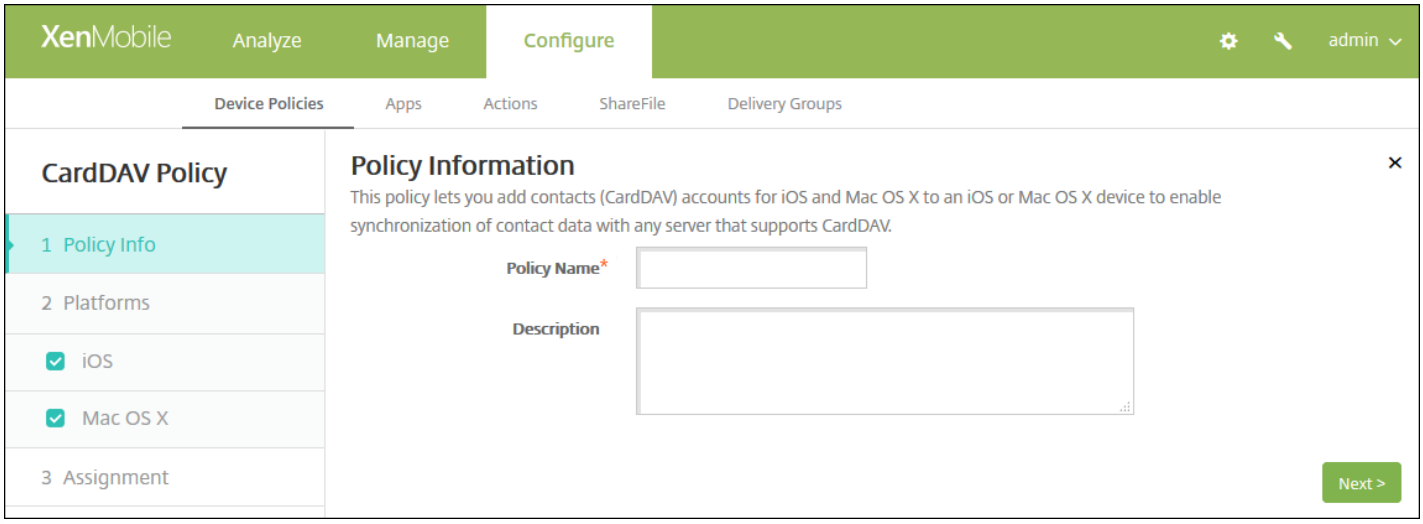
Feb 13, 2015

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:

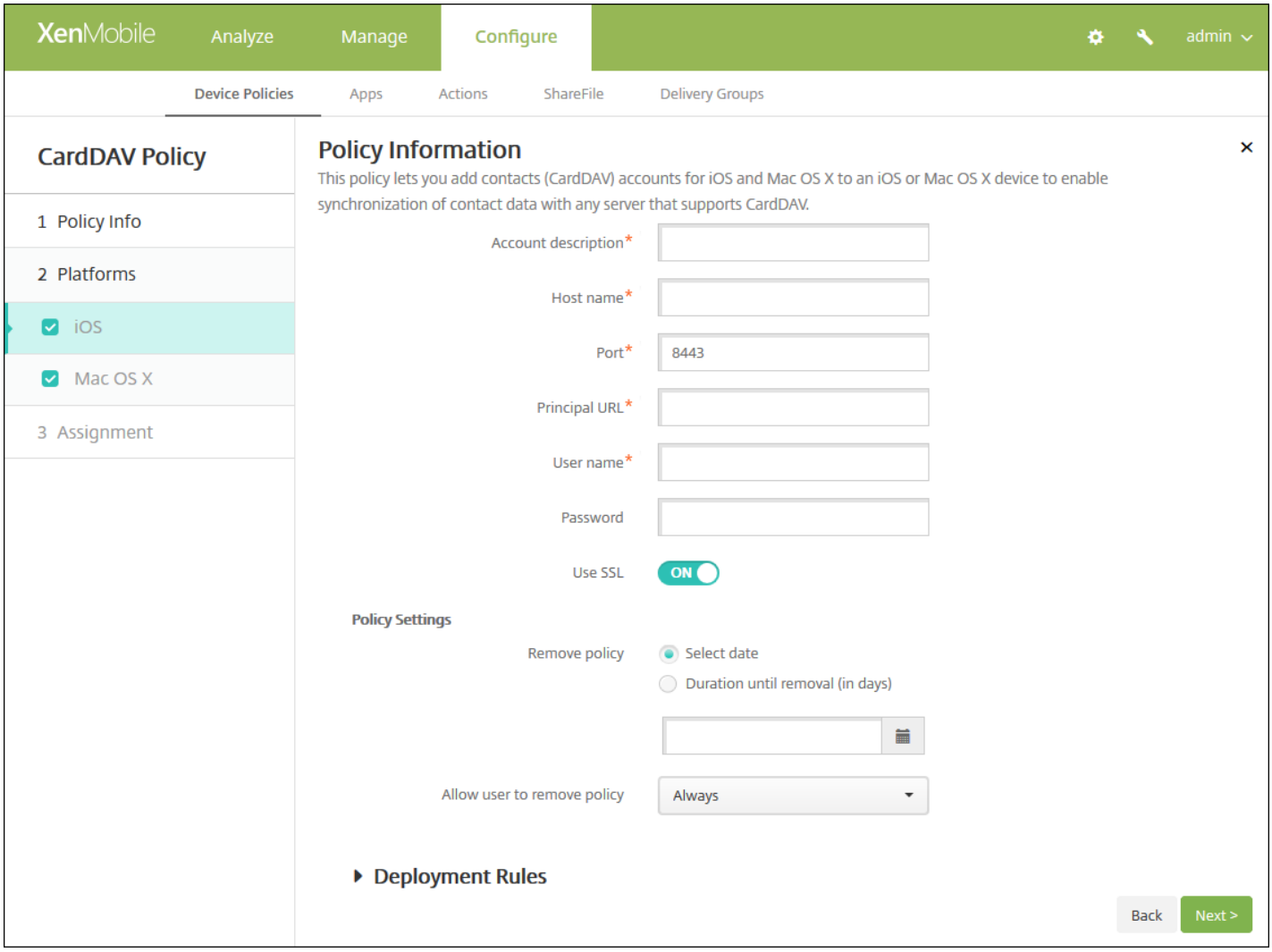
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

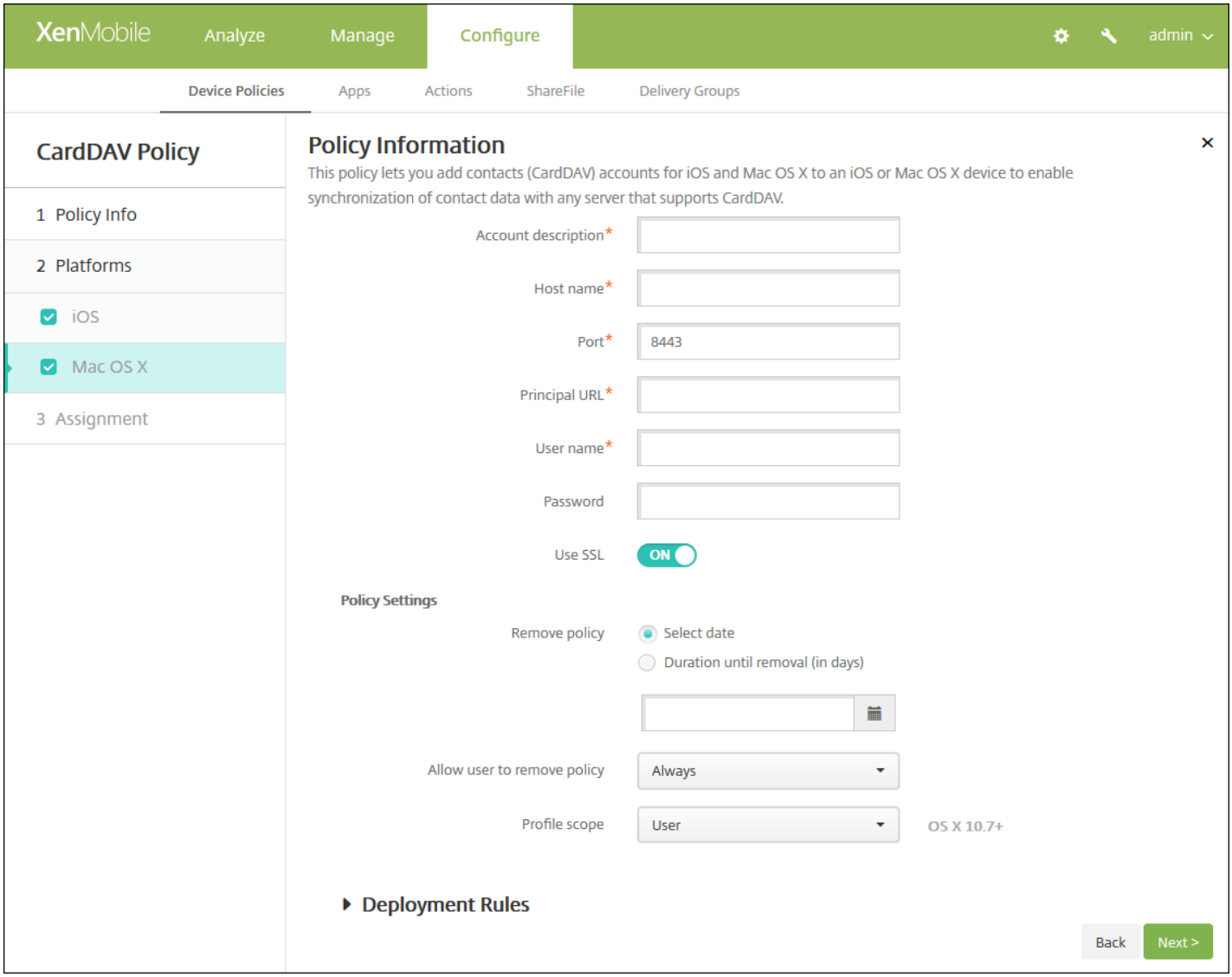
Configure iOS settings



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

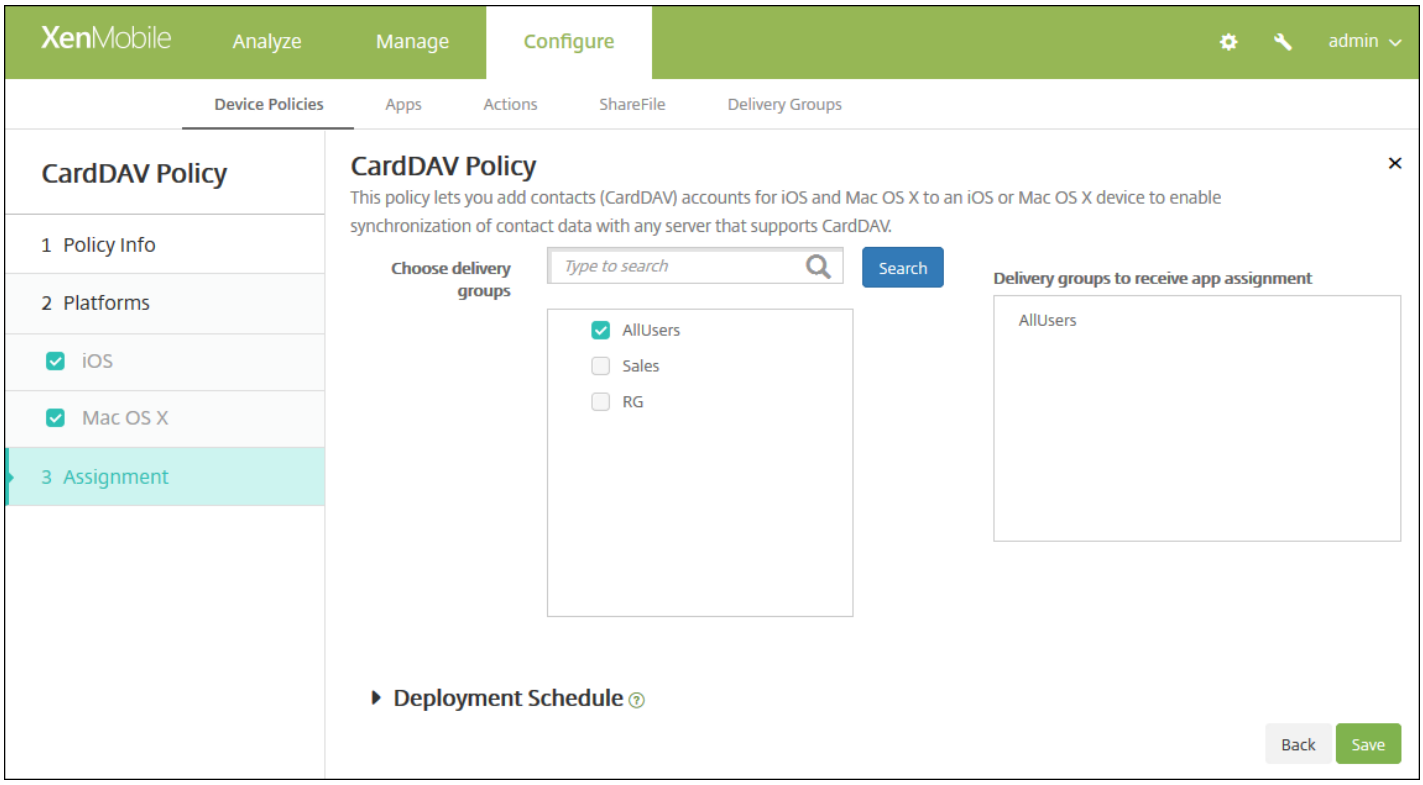


Configure these settings:

- **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 policies

Sep 15, 2015

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.

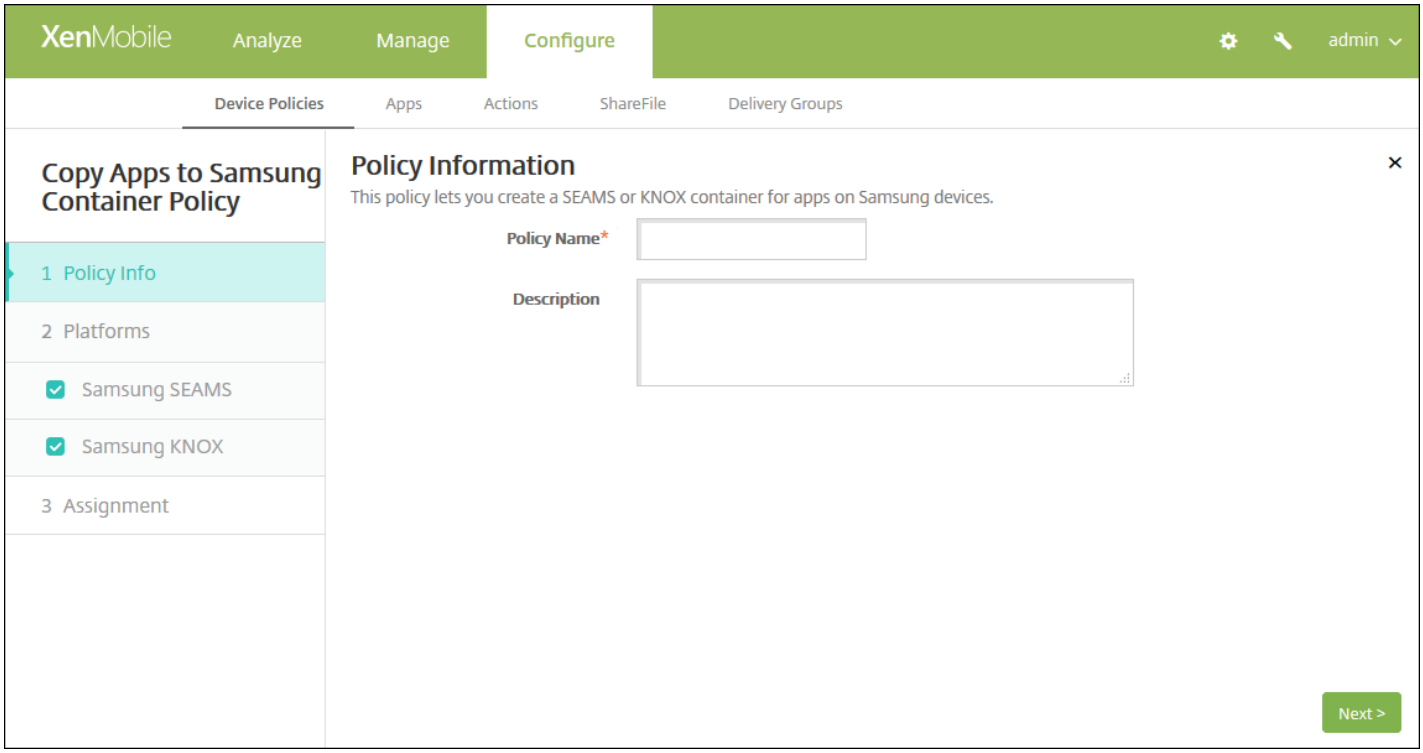
Prerequisites:

- 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.

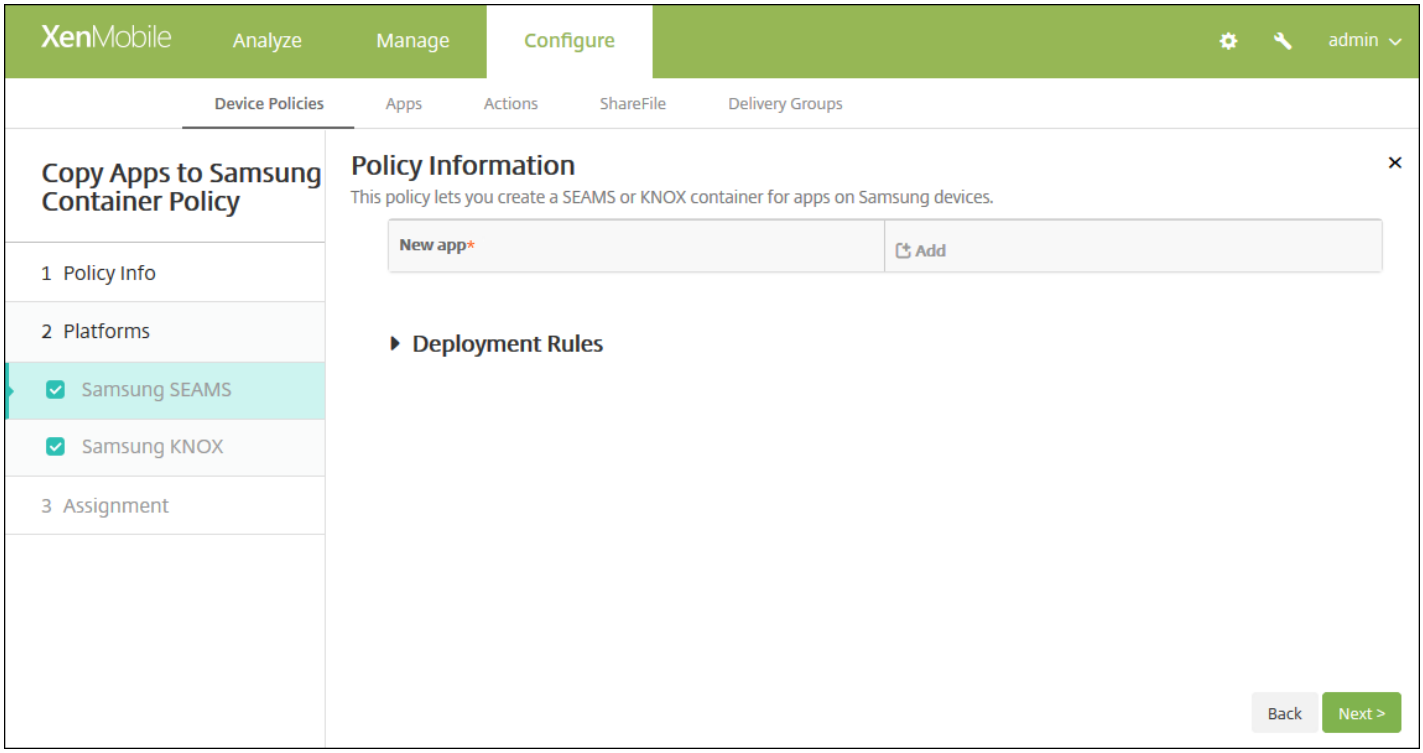
3. Expand **More**, and then under **Security**, click **Copy Apps to Samsung Container**. The **Copy Apps to Samsung Container Policy** information page appears.



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.

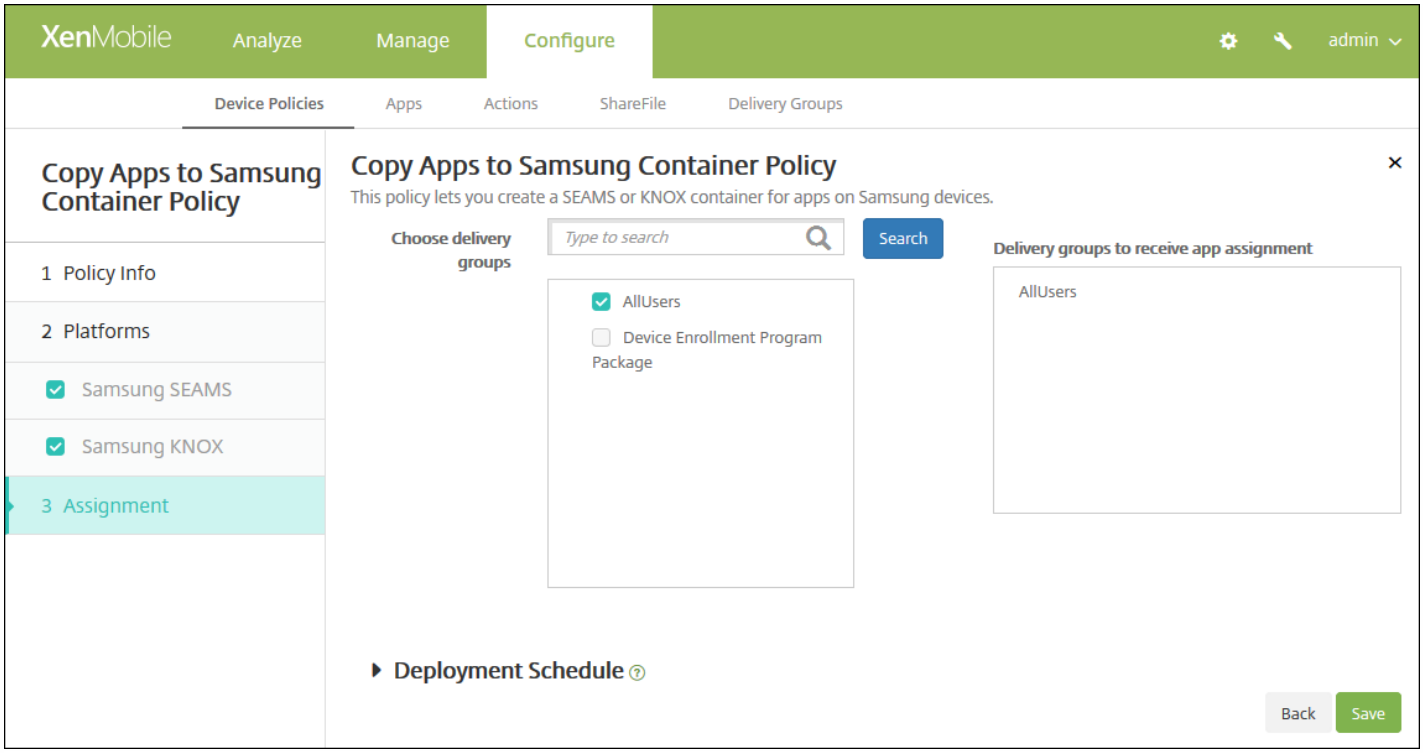
- **New app**: For each app you want to add to the list, click **Add** and then do the following:
  - Type a package ID; for example, com.mobiwolf.lacingart fo the LacingArt app.
  - Click **Save** or **Cancel**.

    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

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

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 policies

Jun 23, 2015

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

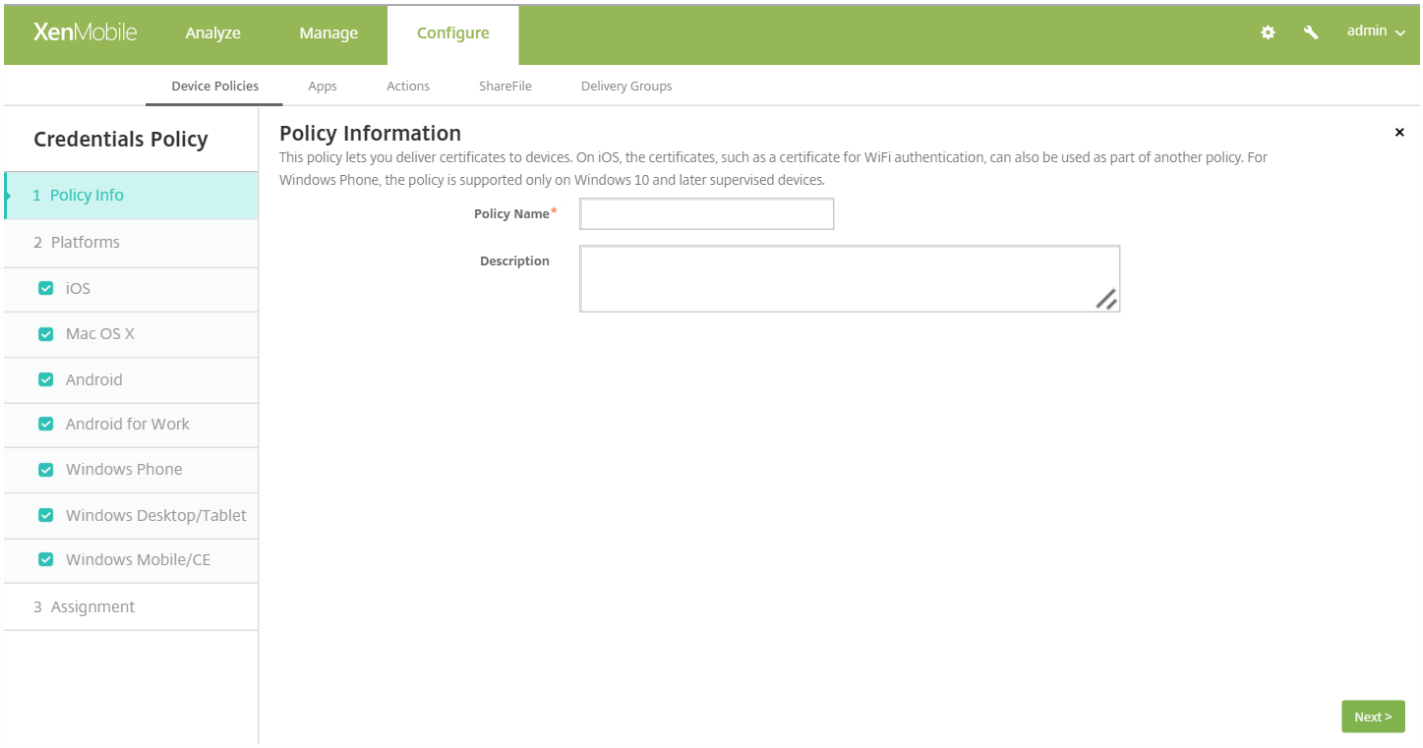
Windows Phone settings

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:

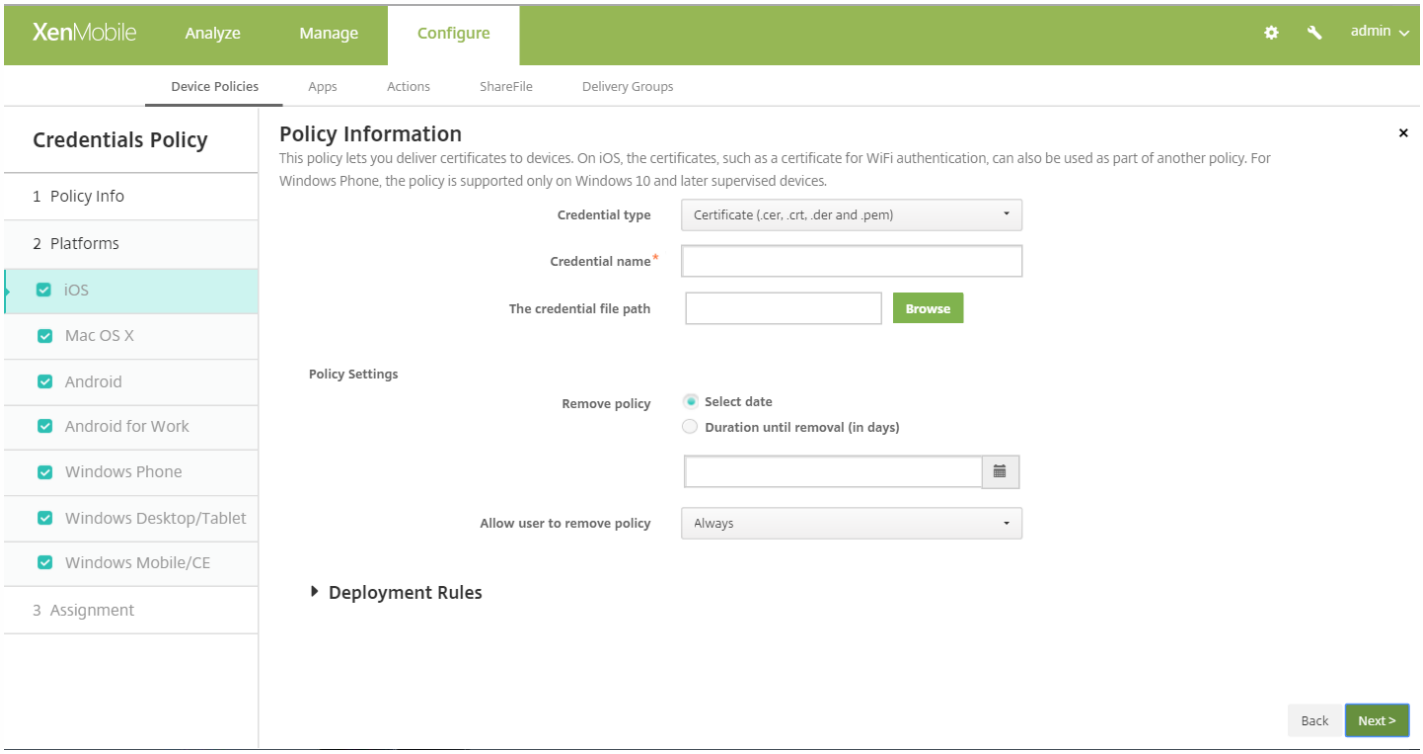
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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



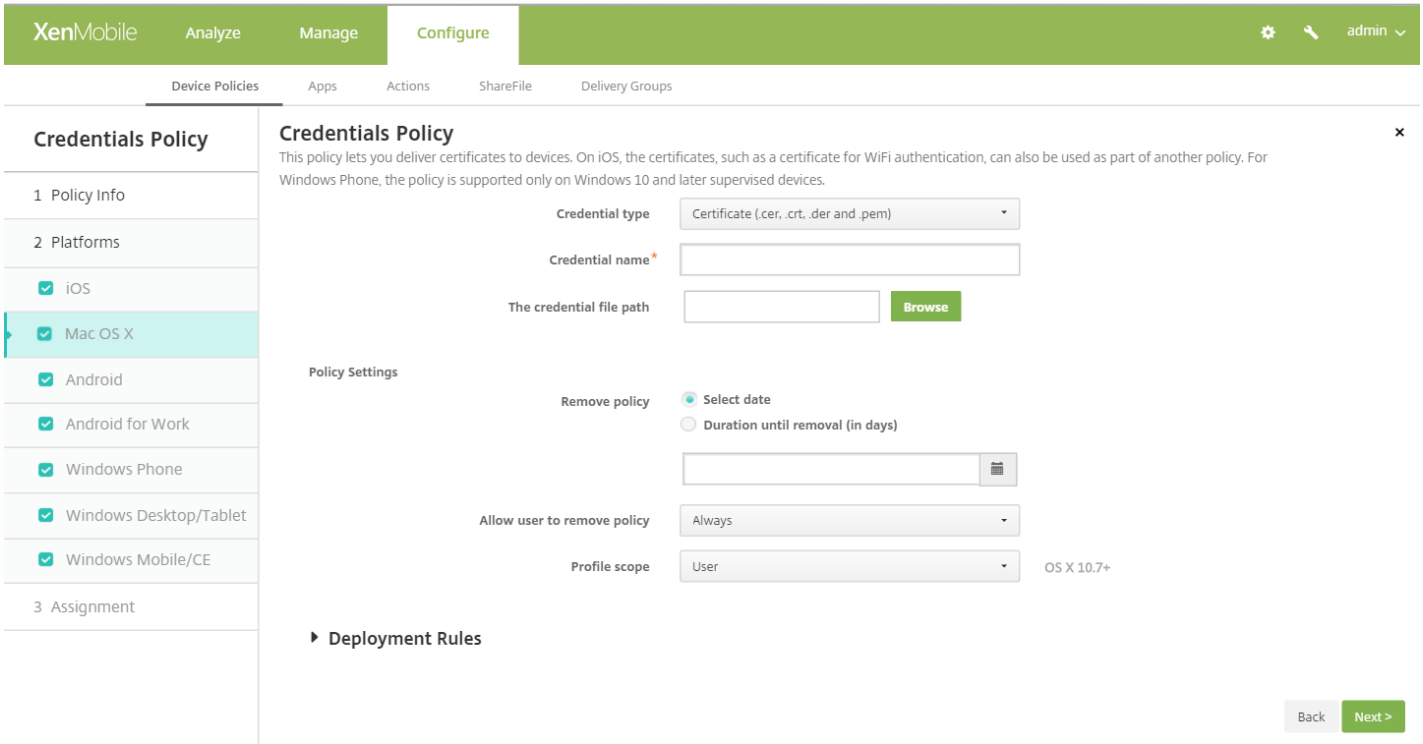
Configure the following settings:

- **Credential type**: In the list, click the type of credential to use with this policy and 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.

Configure Mac OS X settings

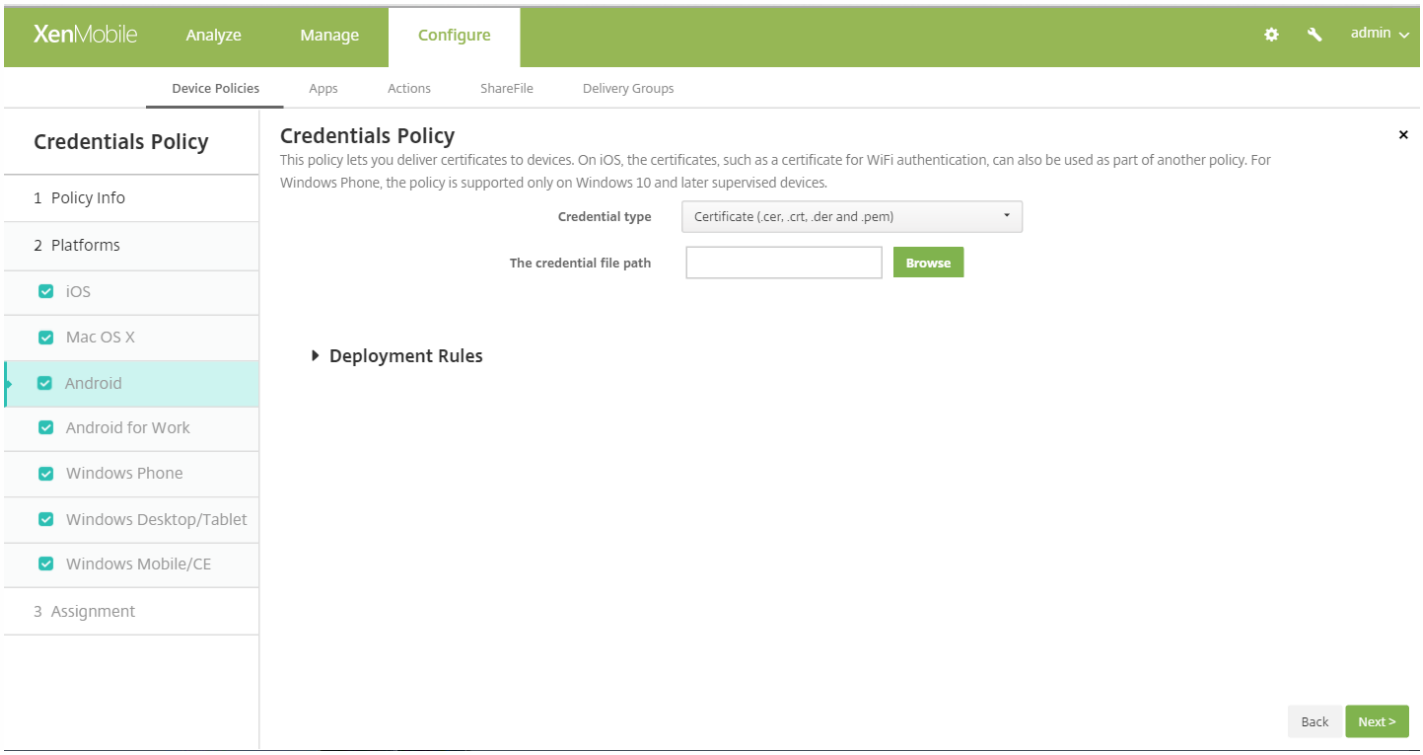


Configure the following settings:

- **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.

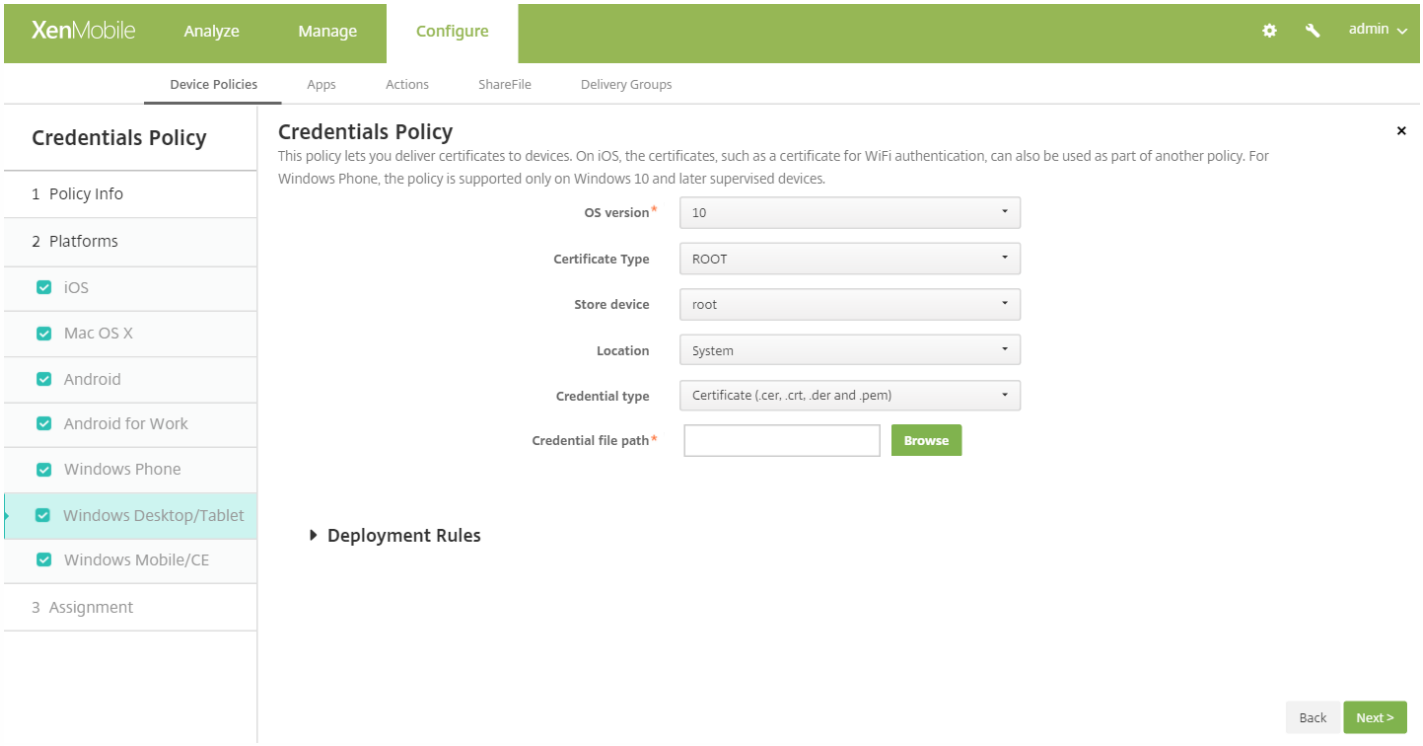
Configure Android and Android for Work settings



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



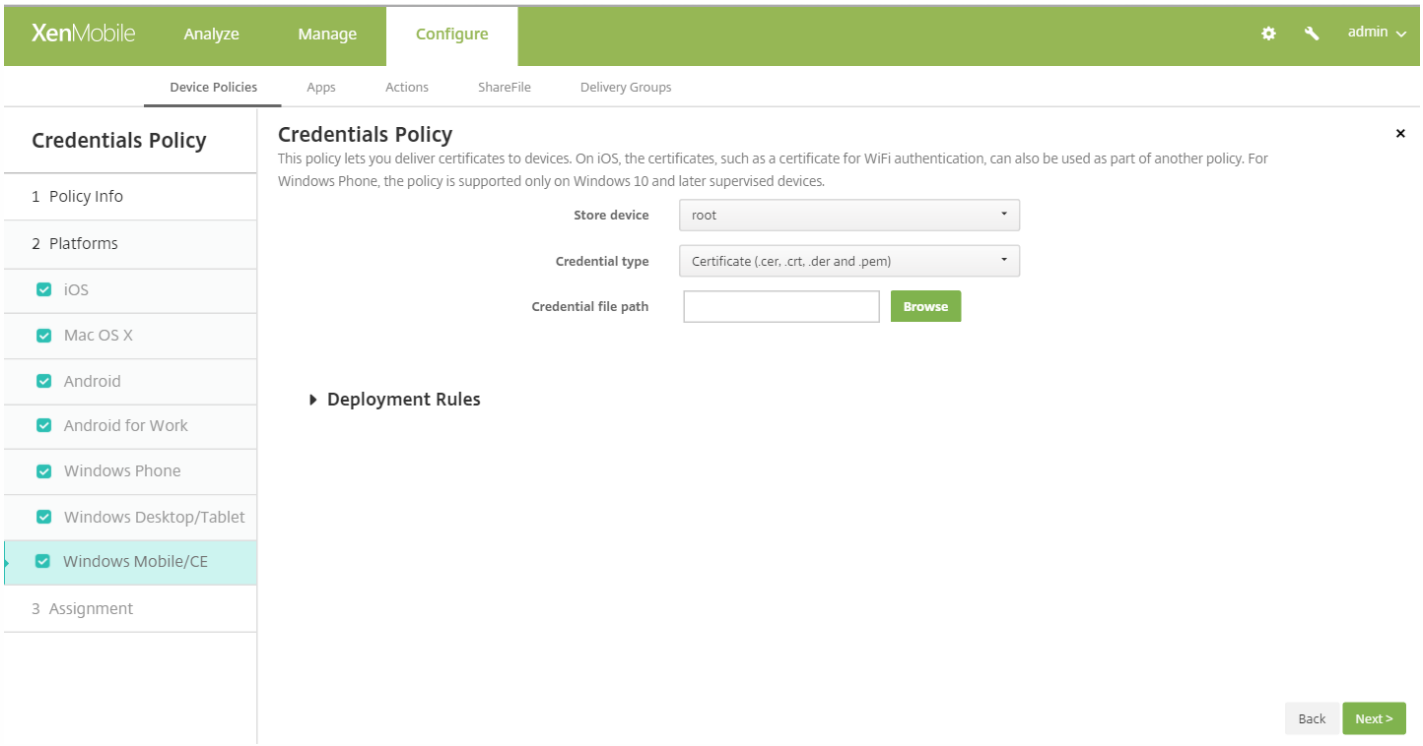
Configure the following settings:

- **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

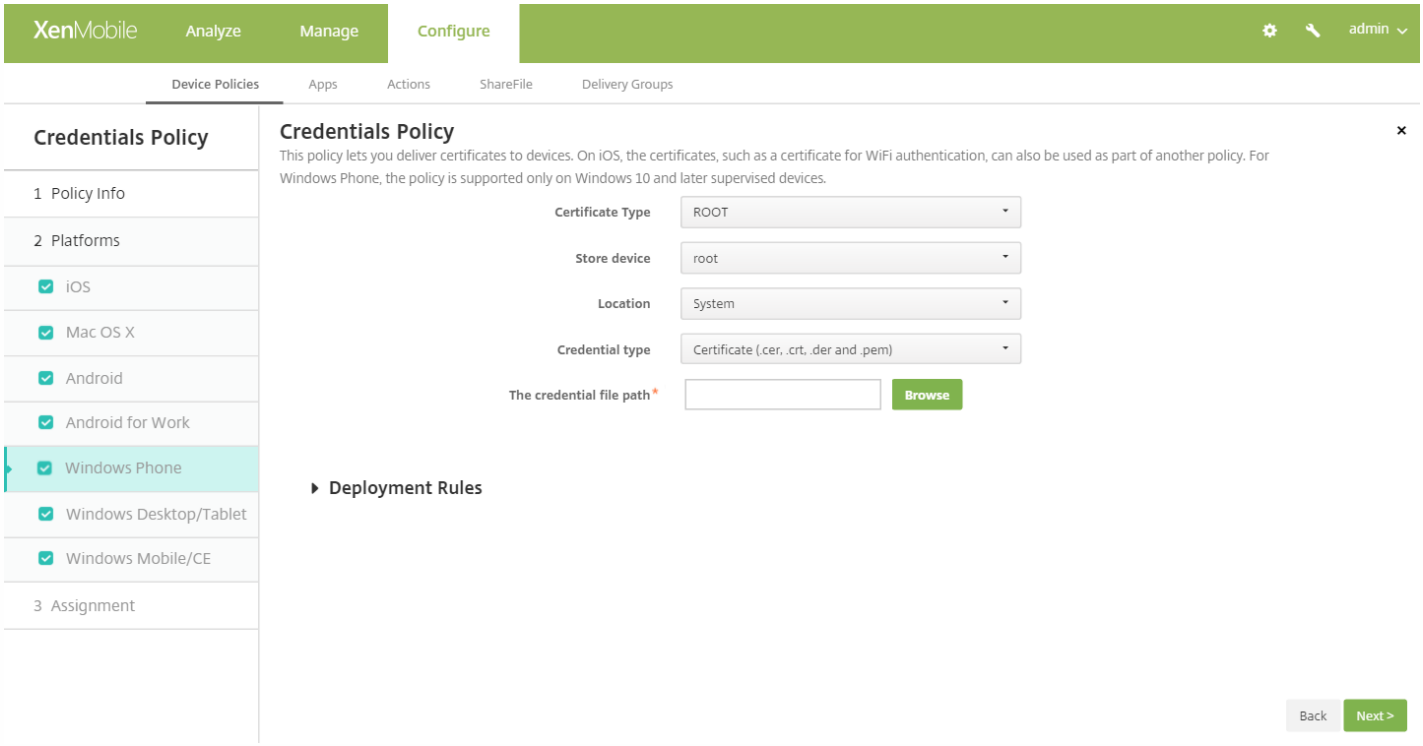
Configure Windows Mobile/CE settings



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

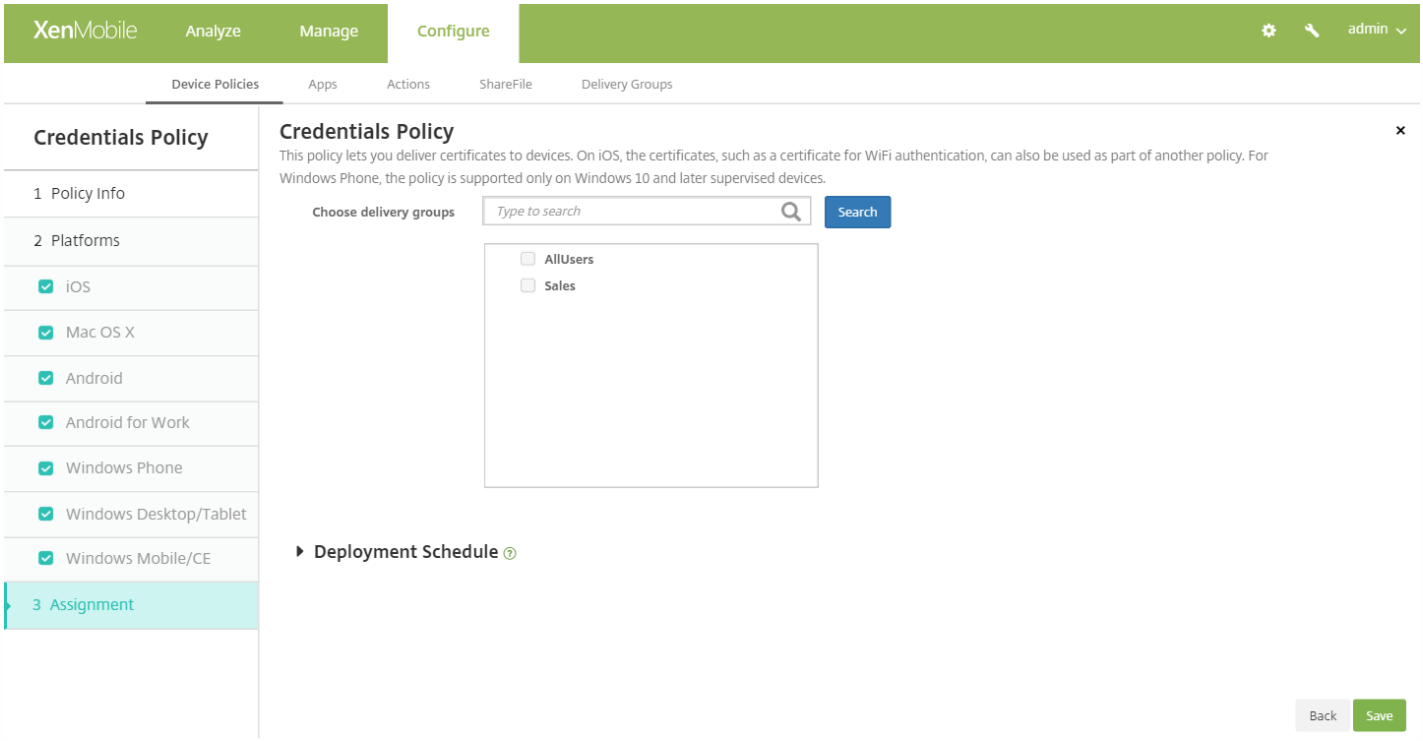


Configure the following settings:

- **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 policies

Mar 17, 2015

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:

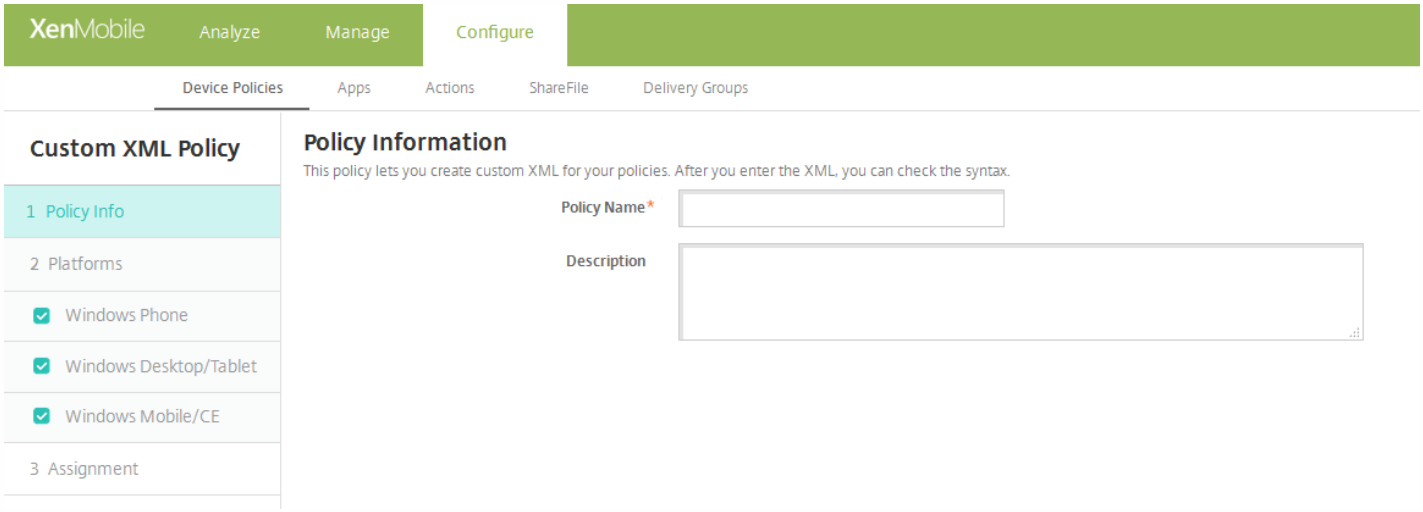
- Provisioning, which includes configuring the device, and enabling or disabling features
- Device configuration, which includes allowing users to change settings and device parameters
- Software upgrades, which includes providing new software or bug fixes to be loaded onto the device, including apps 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.

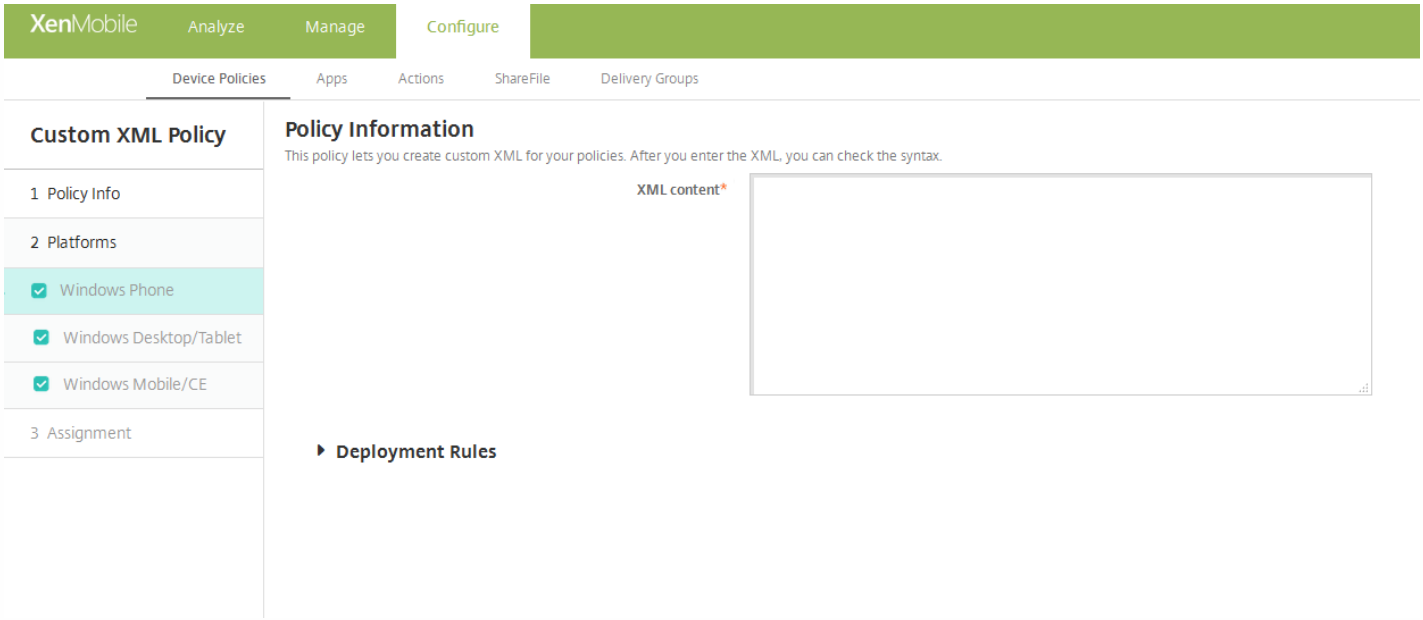
3. Expand **More** and then under **Custom**, click **Custom XML**. The **Custom XML Policy** information page appears.



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

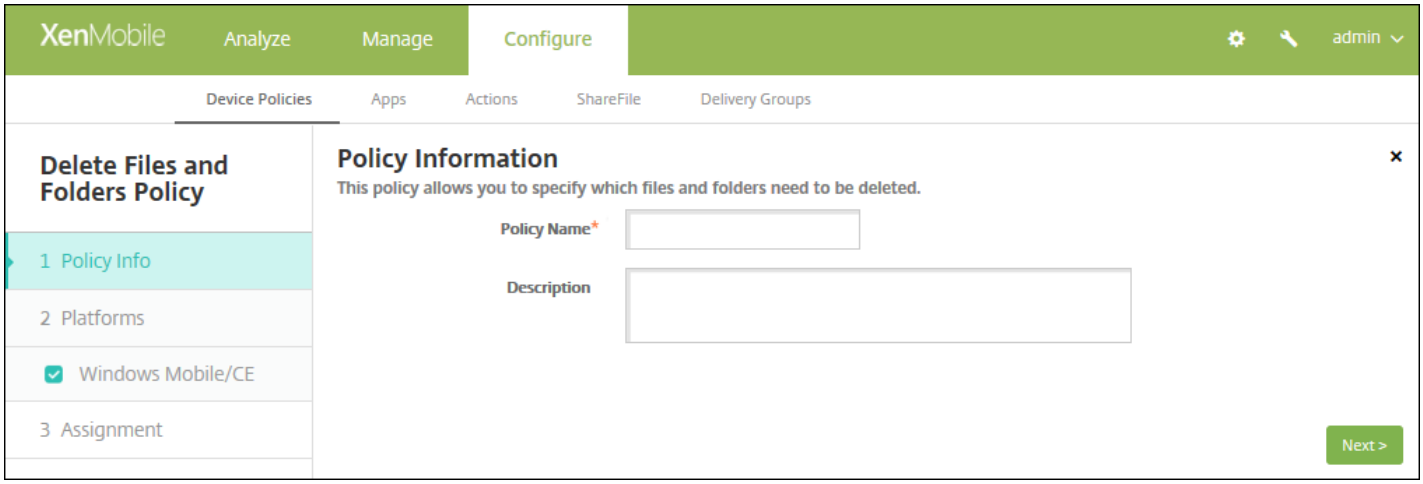
Oct 07, 2015

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.

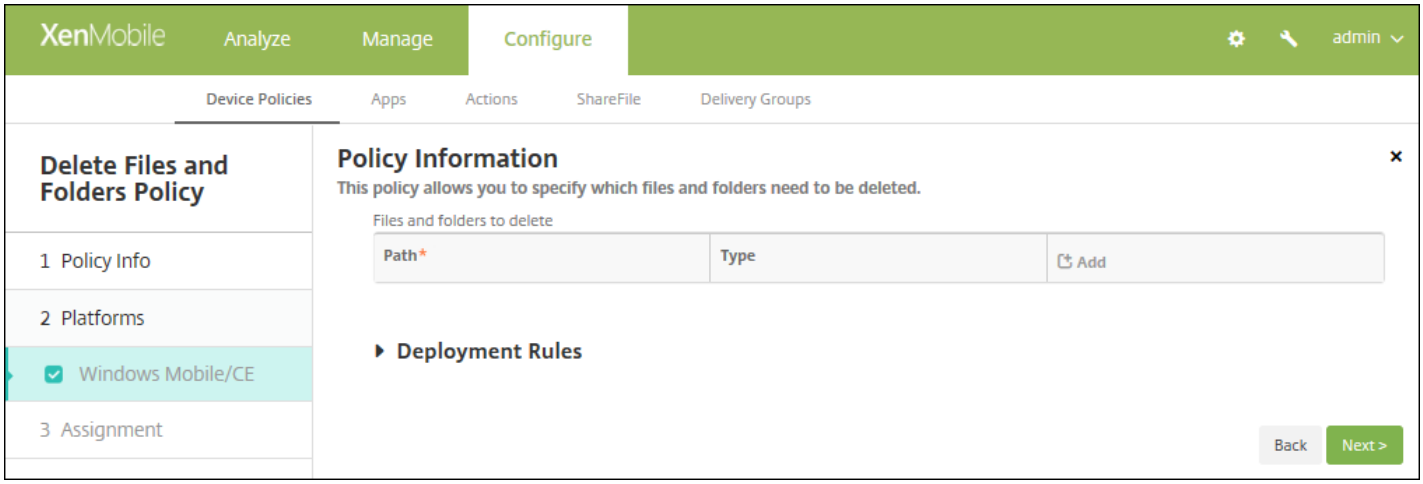
3. Expand **More** and then, under **Apps**, click **Delete Files and Folders**. The **Delete Files and Folders Policy** information page appears.



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:

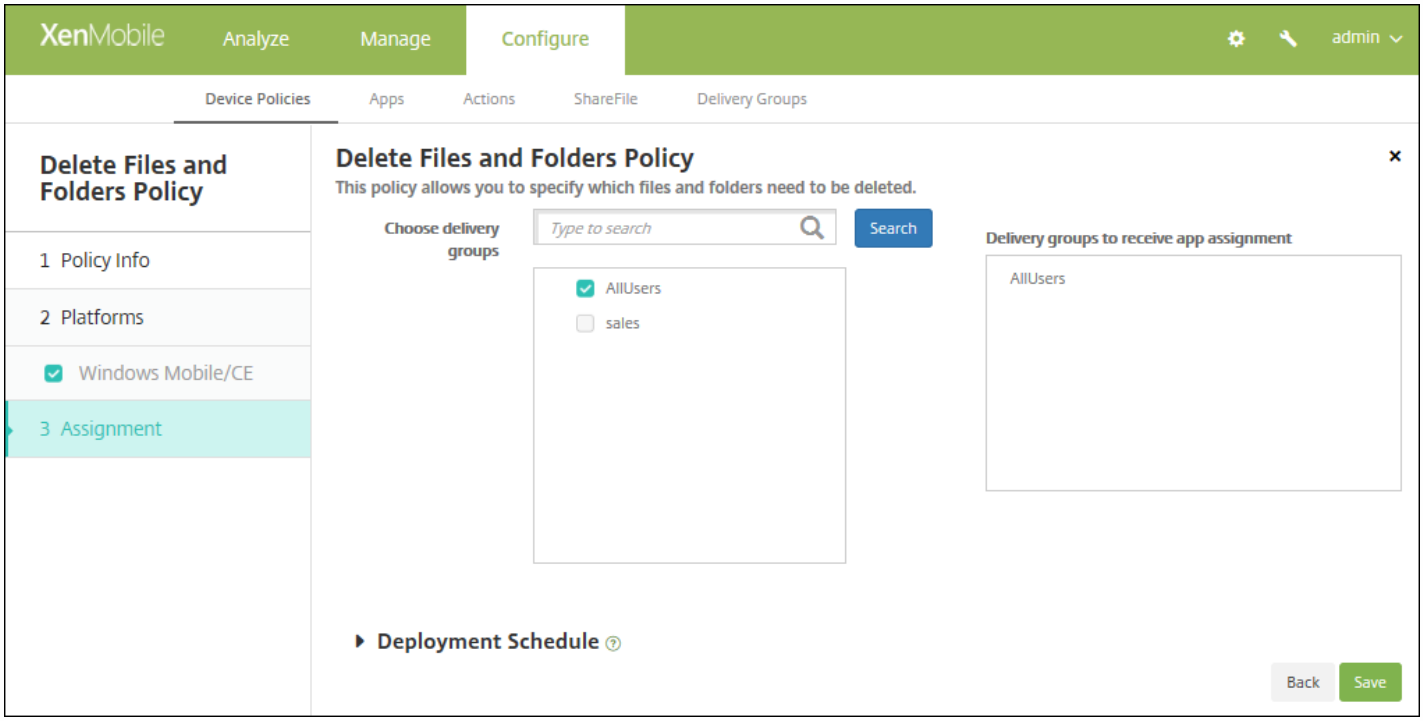
- **Files and folders to delete**: for each file or folder you want to delete, click Add and then do the following:
  - **Path**: Type the path to the file or folder.
  - **Type**: In the list, click File or Folder. The default is File.
  - Click **Save** to save the file or folder, or click **Cancel**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

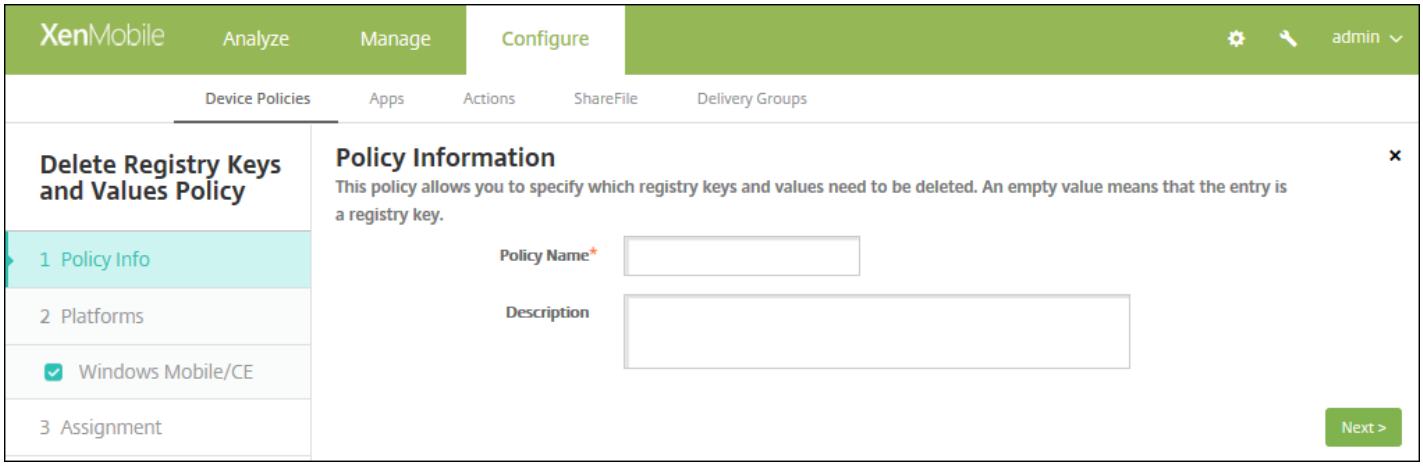
Oct 07, 2015

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.

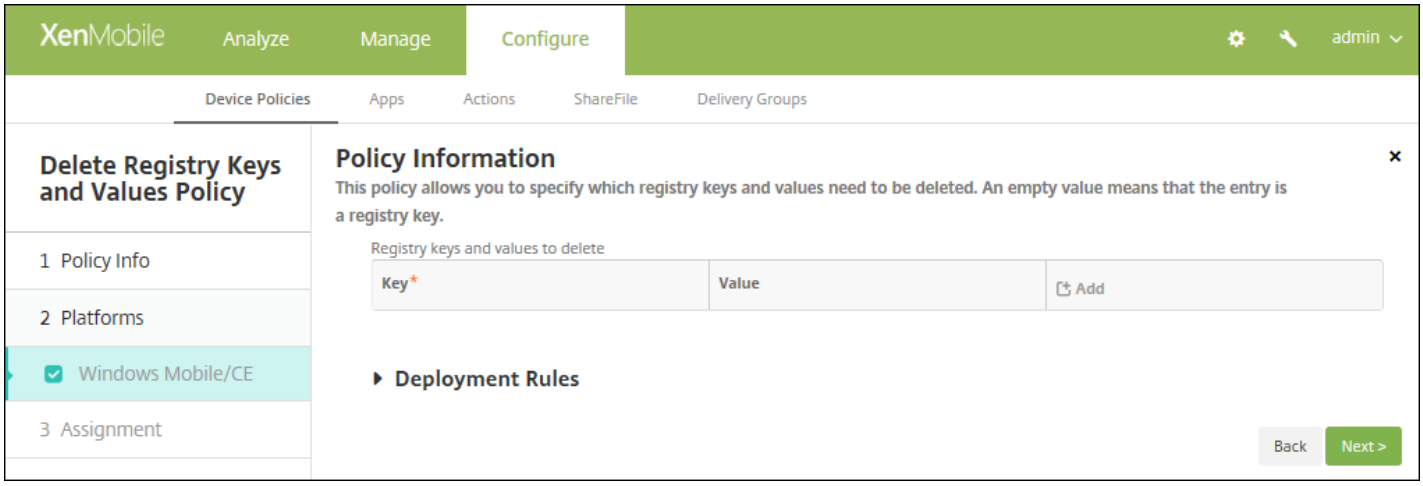
3. Expand **More** and then, under **Apps**, click **Delete Registry Keys and Values**. The **Delete Registry Keys and Values Policy** information page appears.



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:

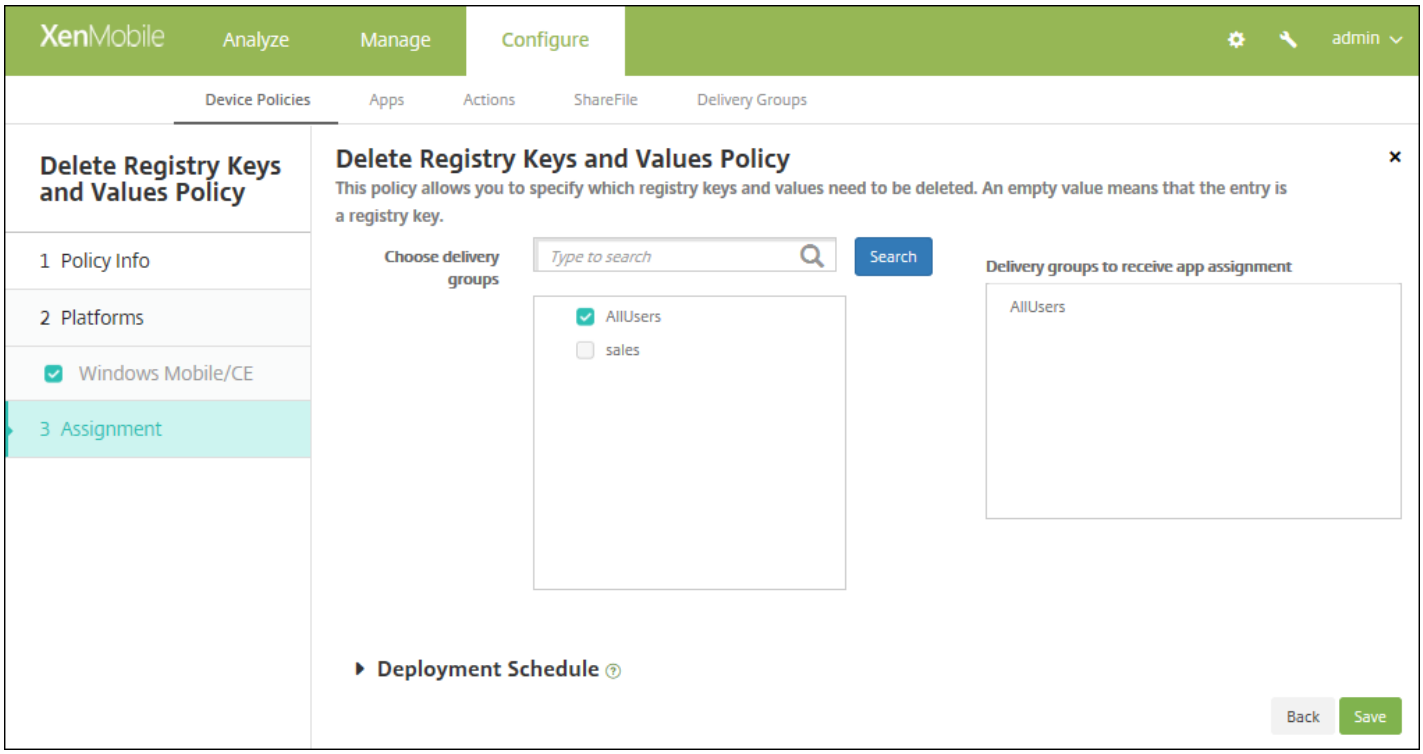
- **Registry keys and values to delete**: for each registry key and value you want to delete, click **Add** and then do the following:
  - **Key**: Type the registry key path. This is a required field.The registry key path should either start with HKEY_CLASSES_ROOT\ or HKEY_CURRENT_USER\ or HKEY_LOCAL_MACHINE\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

Sep 08, 2015

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:

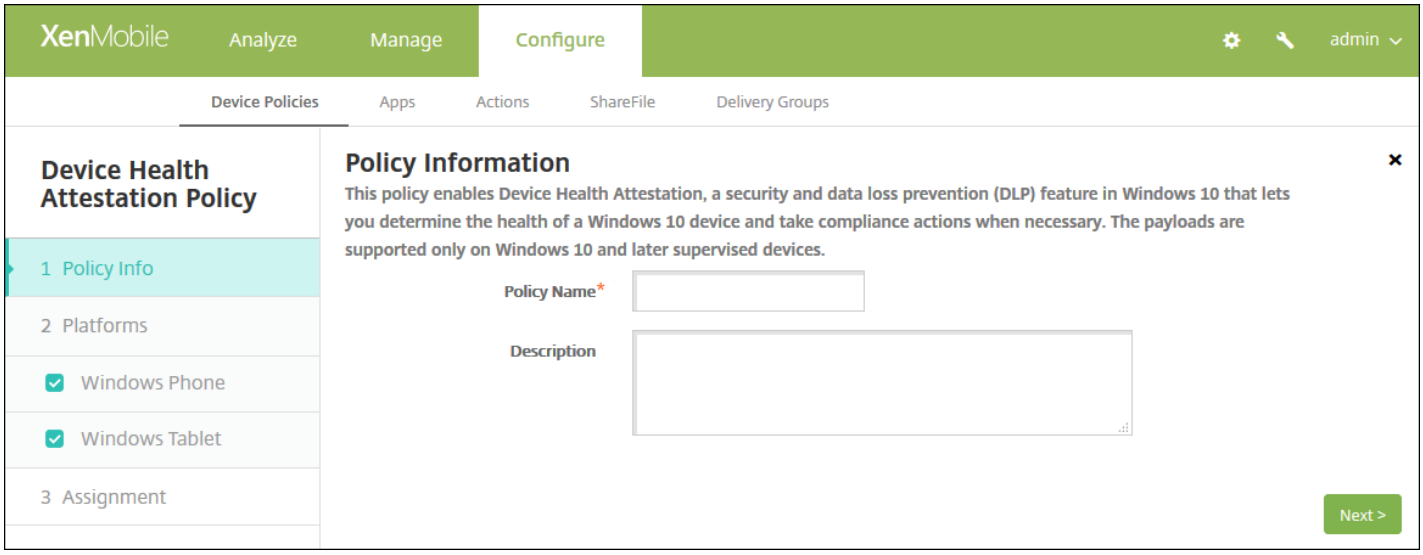
- AIK Present
- Bit Locker Status
- Boot Debugging Enabled
- Boot Manager Rev List Version
- Code Integrity Enabled
- Code Integrity Rev List Version
- DEP Policy
- ELAM Driver Loaded
- Issued At
- Kernel Debugging Enabled
- PCR
- Reset Count
- Restart Count
- Safe Mode Enabled
- SBCP Hash
- Secure Boot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

For more information, refer to Microsoft's 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:

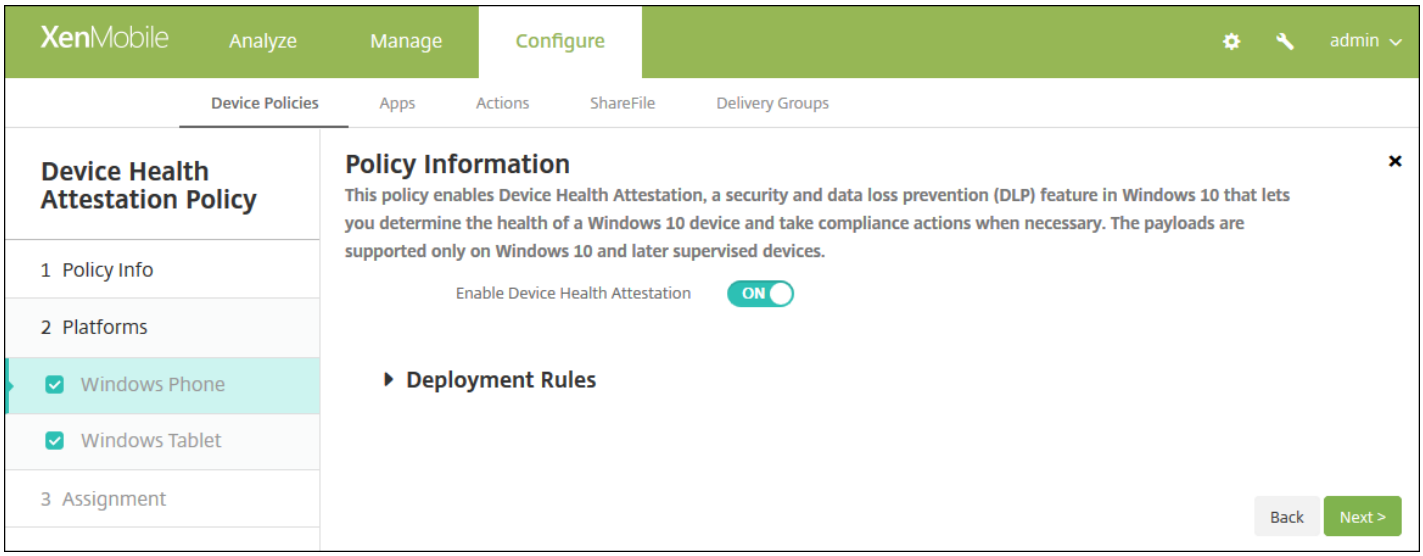
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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 Windows Phone and Windows Tablet settings

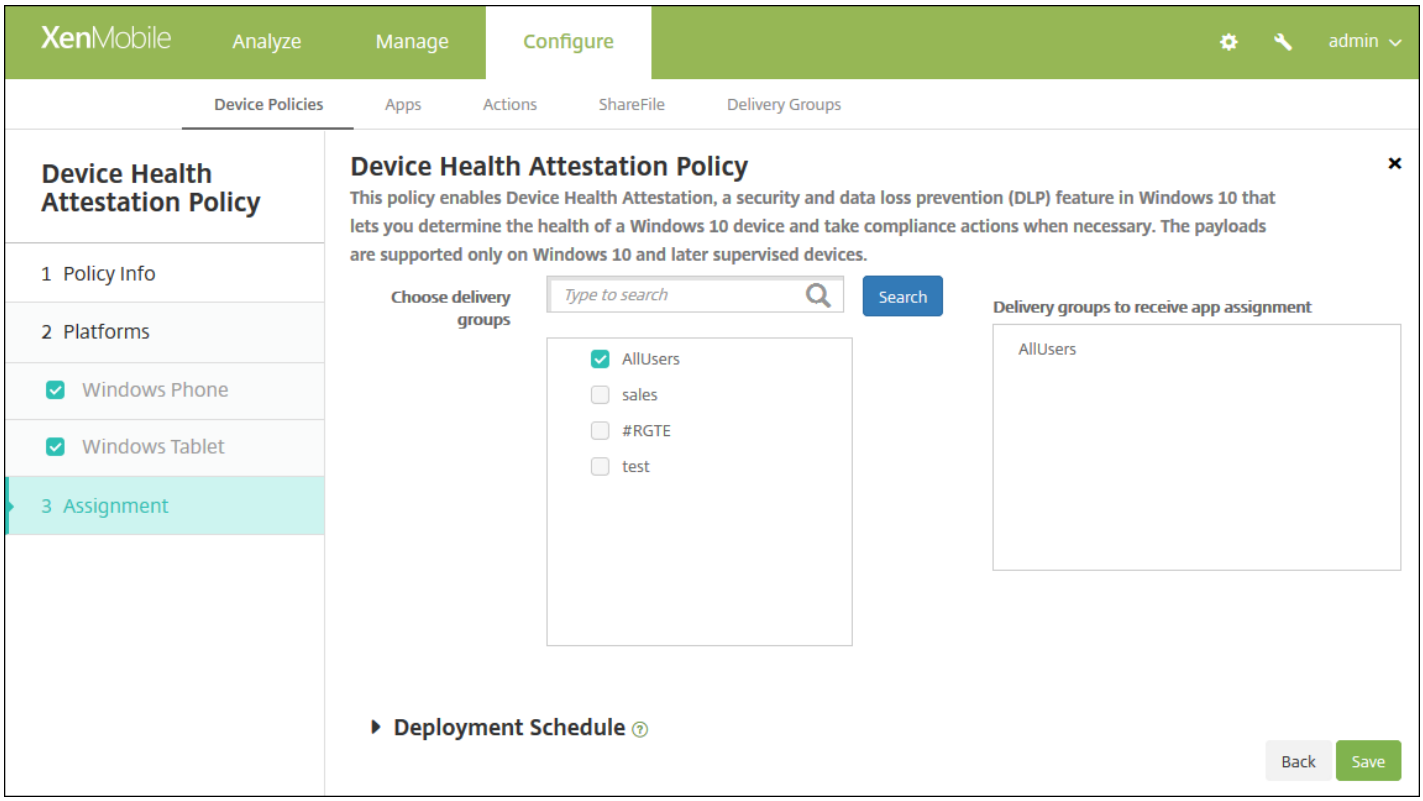


Configure this setting for each platform that you choose:

- **Enable Device Health Attestation Policy**: 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 policies

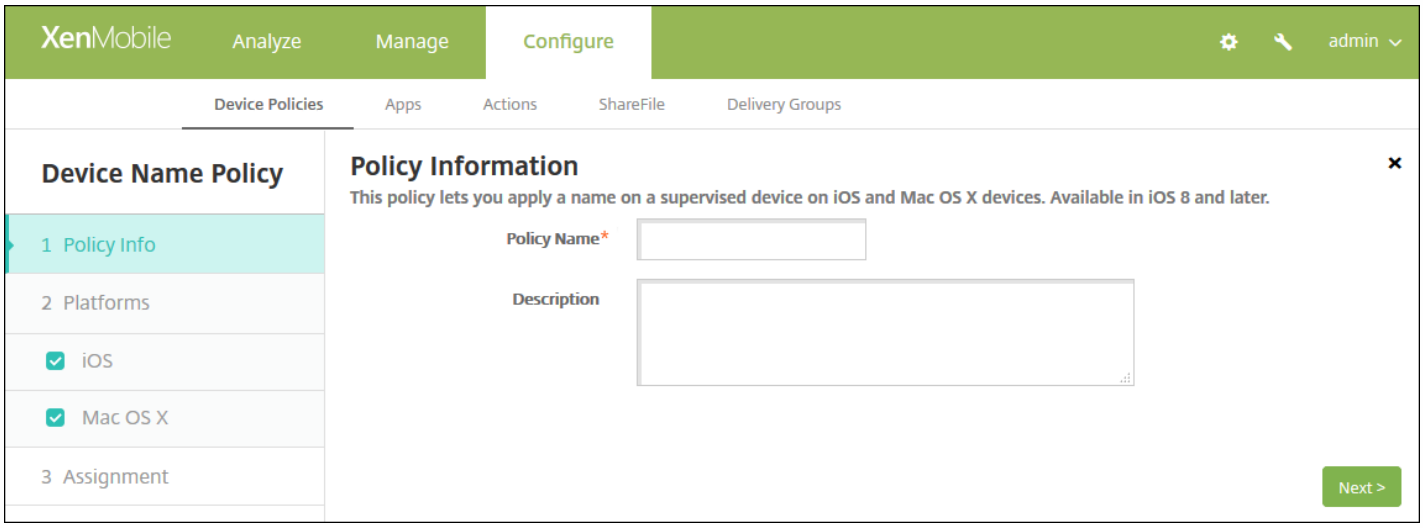
Sep 23, 2015

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:

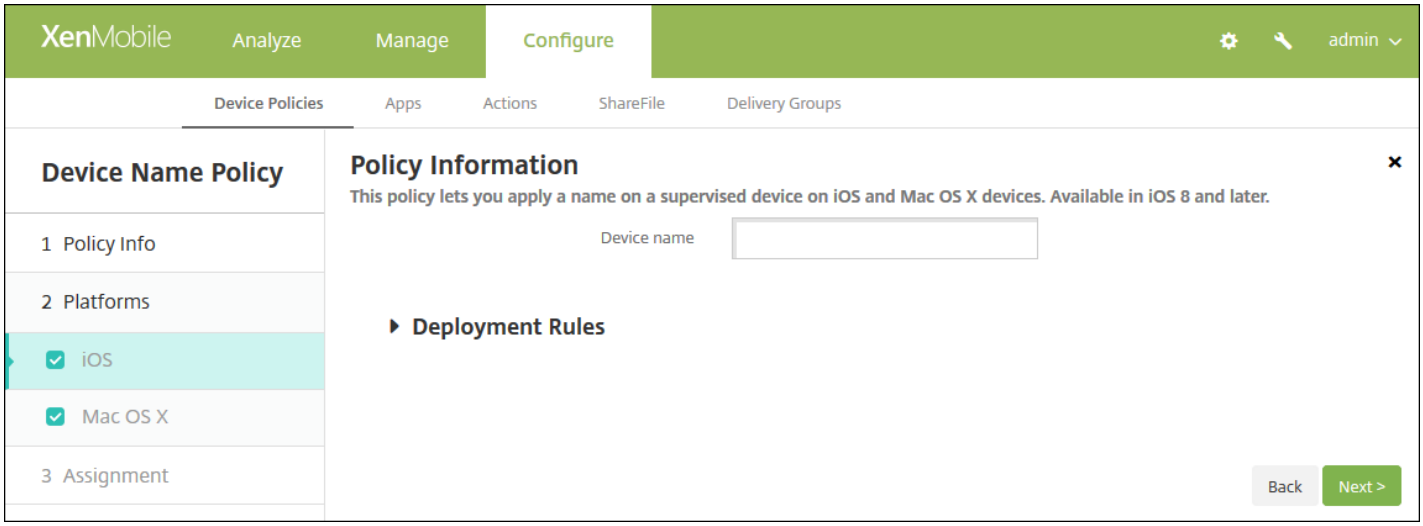
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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

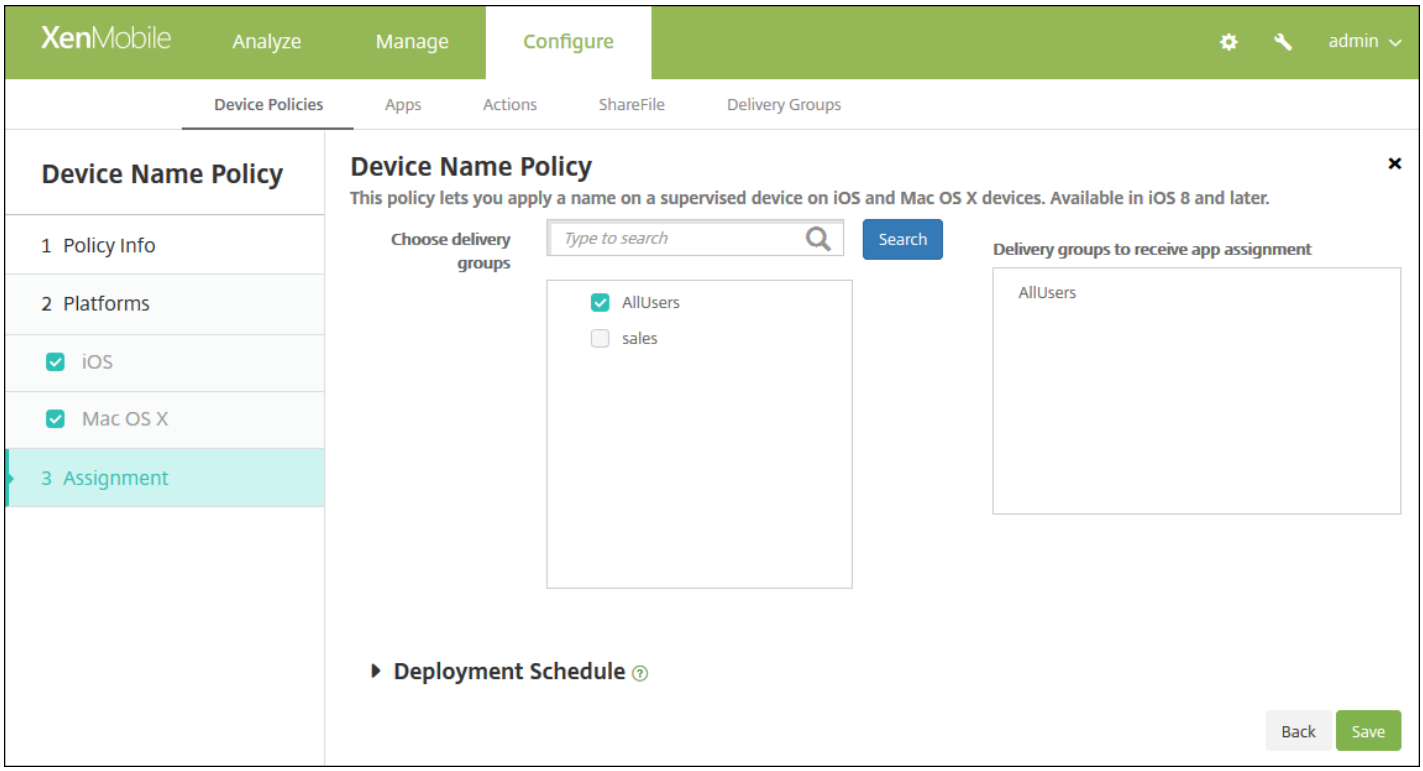


Configure this setting for the platforms you choose:

- **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

Jan 05, 2017

An Enterprise Hub device policy for Windows Phone lets you distribute apps through the Enterprise Hub Company store.

Before you can create the policy, you need the following:

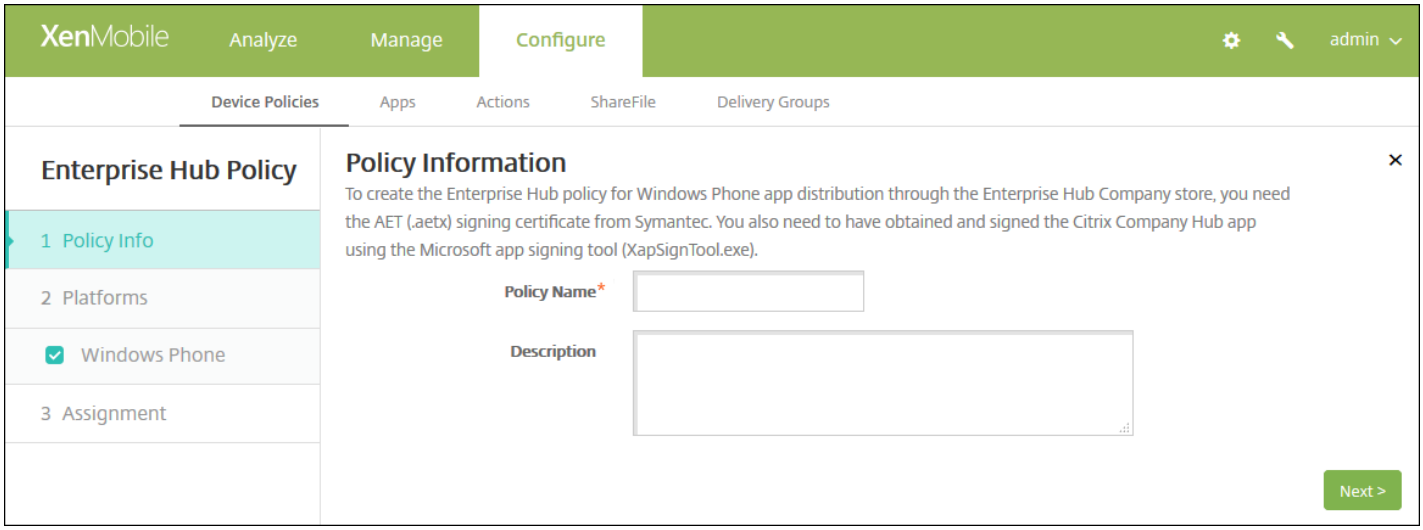
- An AET (.aetx) signing certificate from Symantec
- The Citrix Company Hub app signed by using the Microsoft app signing tool (XapSignTool.exe)

Note: XenMobile supports only one Enterprise Hub policy for one mode of Windows Phone Worx Home. For example, to upload Windows Phone Worx Home 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. Also please note that starting with version 10.4, Worx Home is renamed Secure Hub.

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.

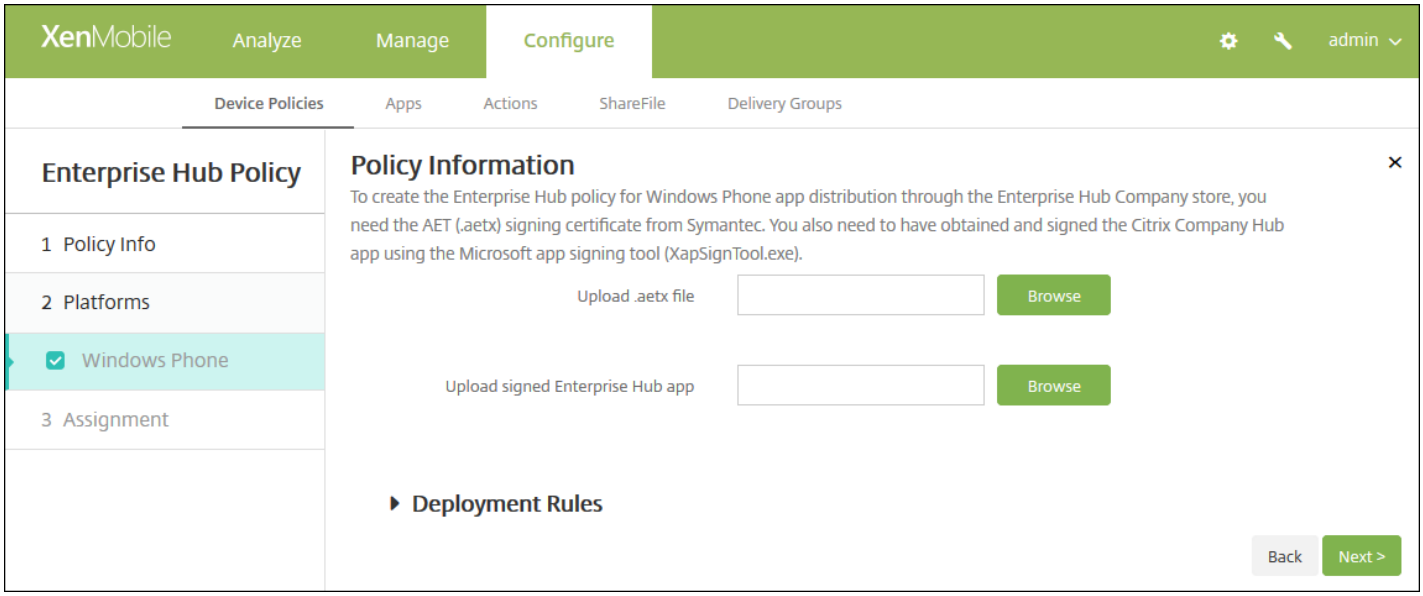
3. Expand **More** and then, under **XenMobile agent**, click **Enterprise Hub**. The **Enterprise Hub Policy** page appears.



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.

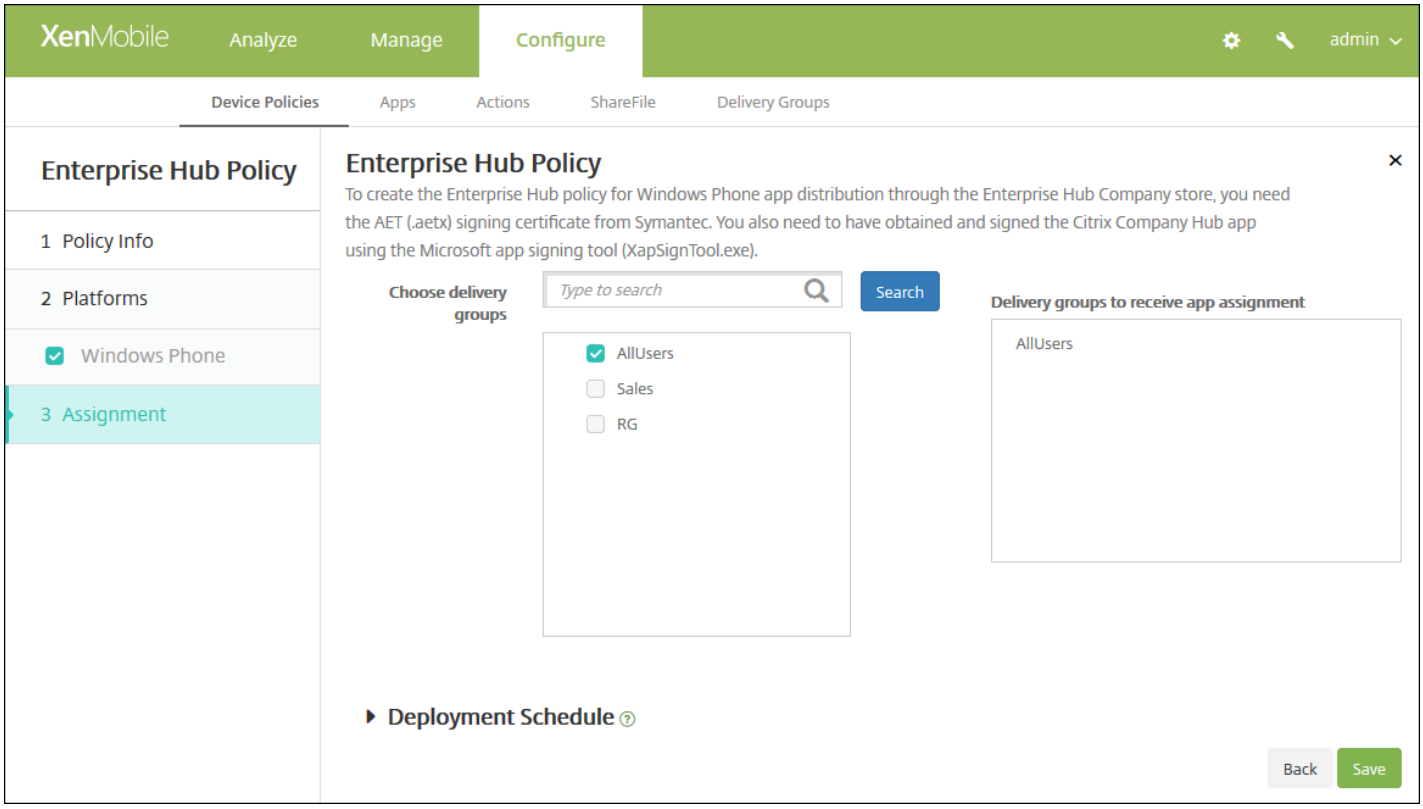


6. Configure these settings:

- **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 policies

Jun 20, 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.

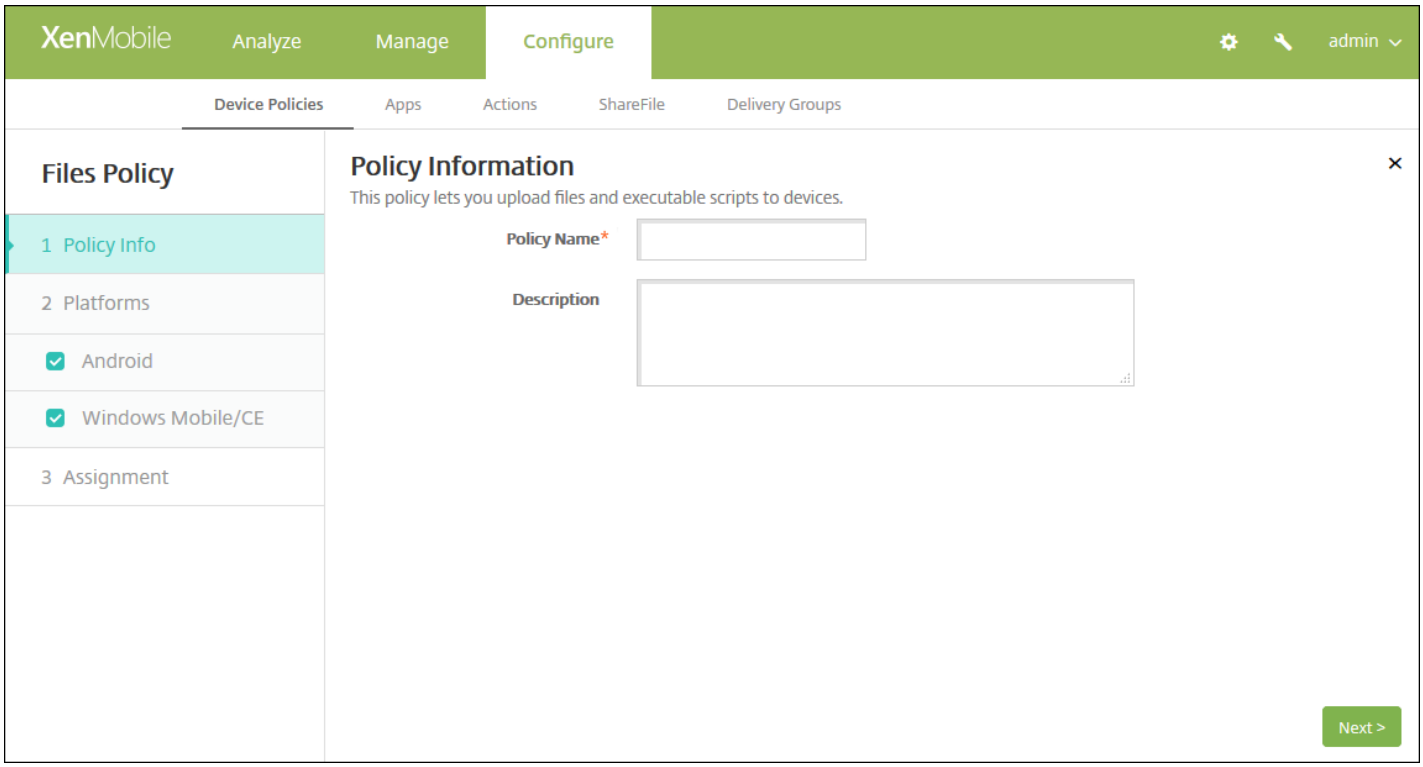
You can add the following file types with this policy:

- 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.

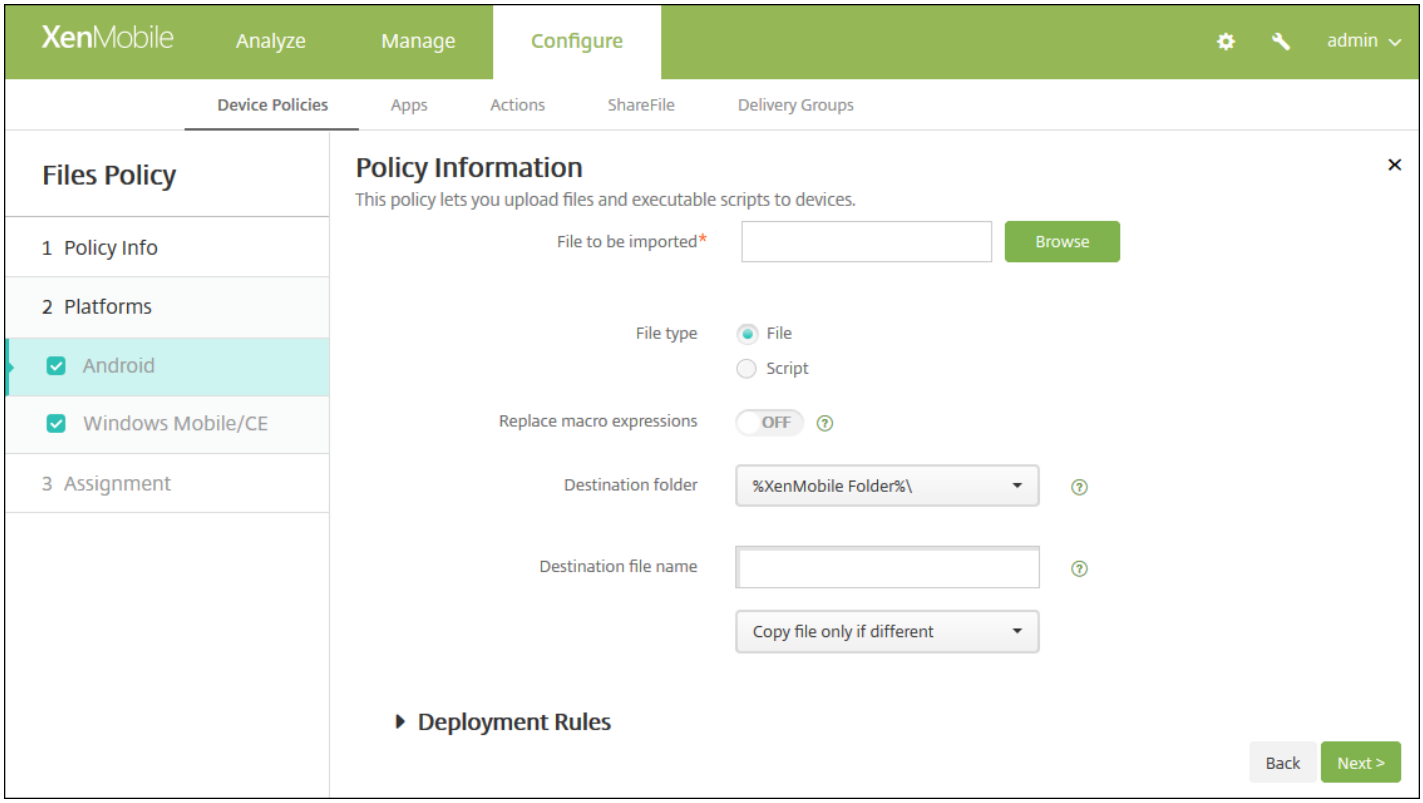
3. Expand **More** and then, under **Apps**, click **Files**. The **Files Policy** information page appears.



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.

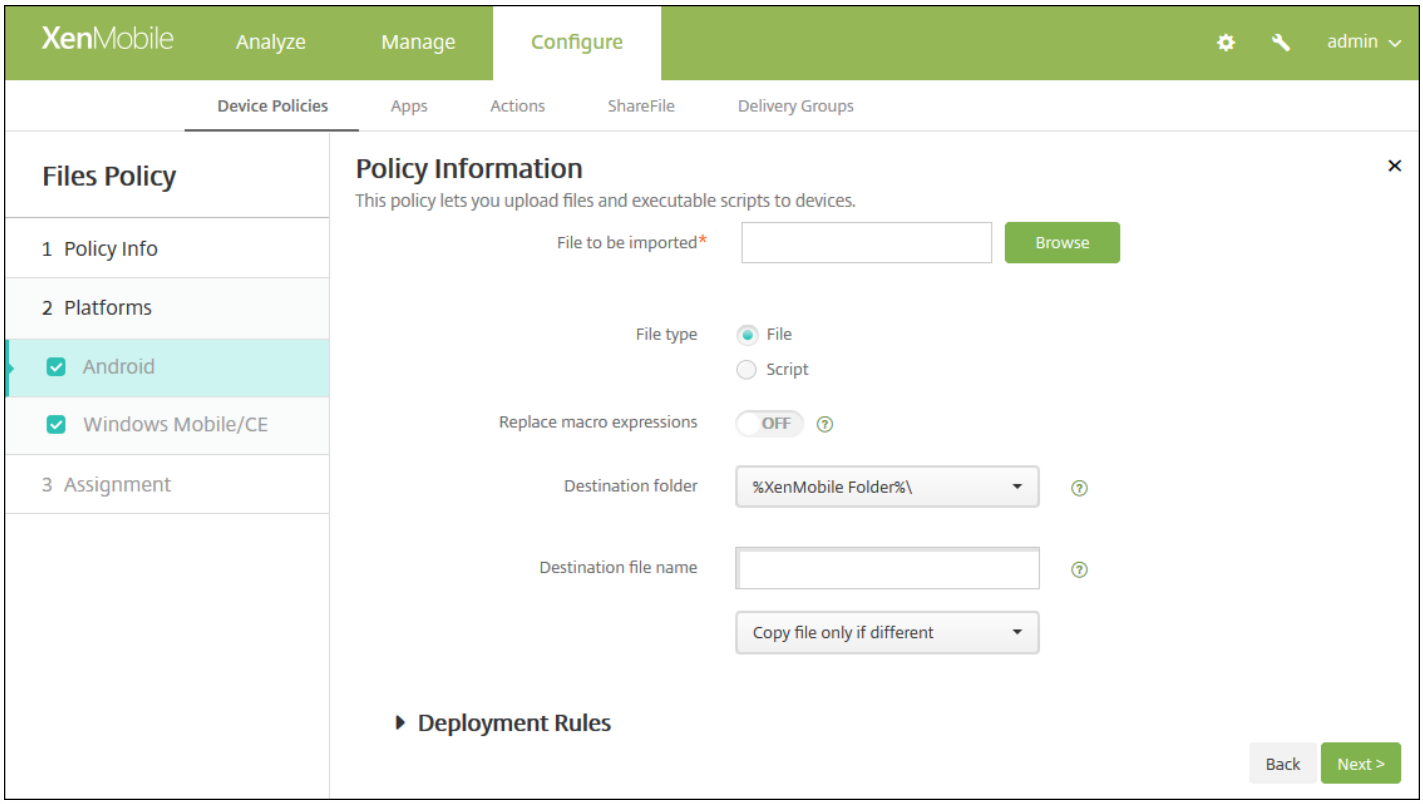
5. Click **Next**. The **Policy Platforms** page appears.



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.

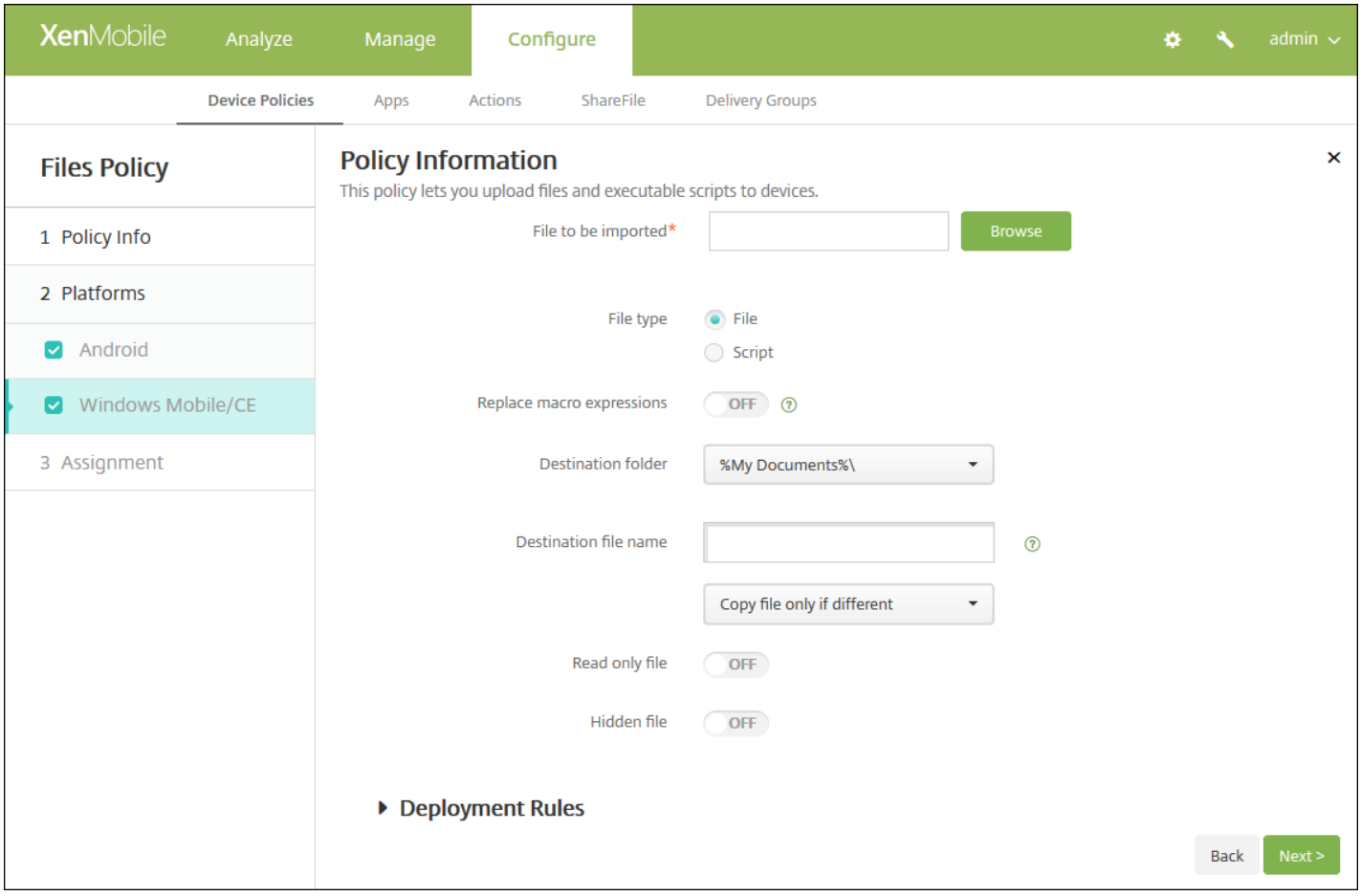
Configure Android settings



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:

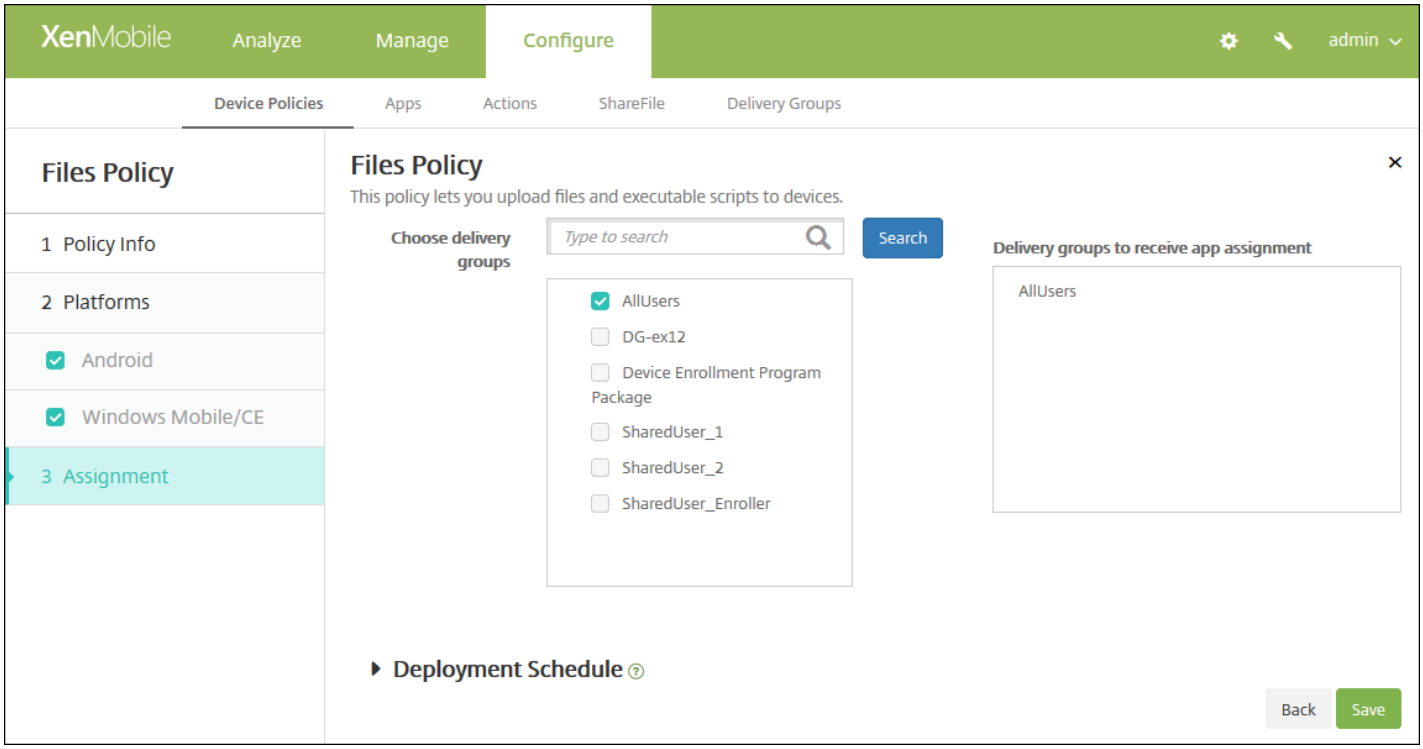
- **File to be imported**: Select the file to import by clicking Browse and navigating to the file's location.
- **File type**: Select either **File** or **Script**. When you select **Script**, **Execute immediately** appears. Select whether the script

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 policies

Mar 02, 2015

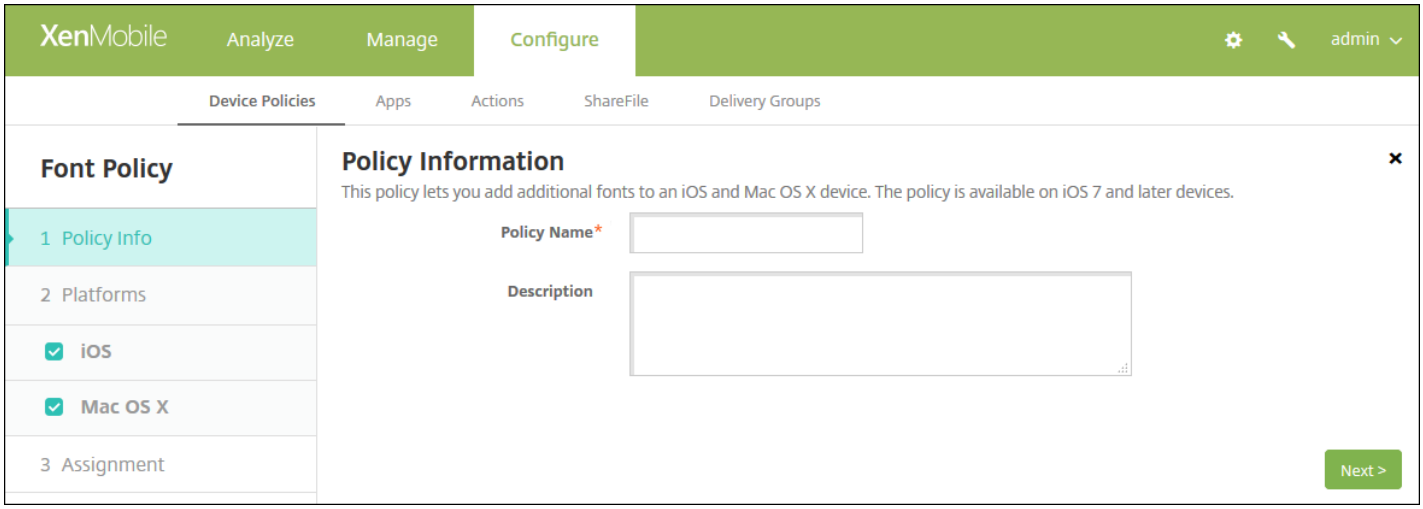
You can add a device policy in XenMobile to add additional fonts to users' iOS and Mac OS X devices. Fonts must be TrueType (.ttf) or OpenType (.oft) fonts. Font collections (.ttc or .otc) are not supported.

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:

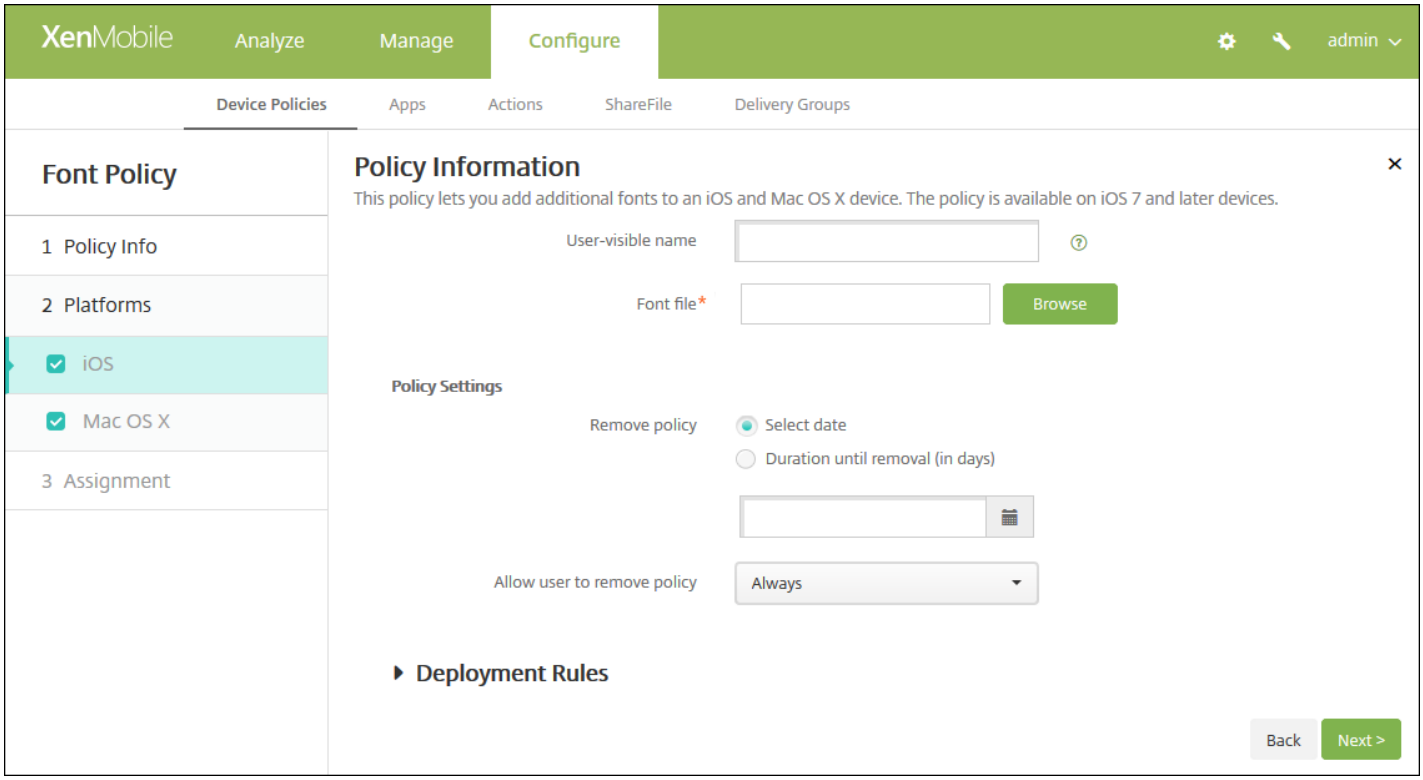
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

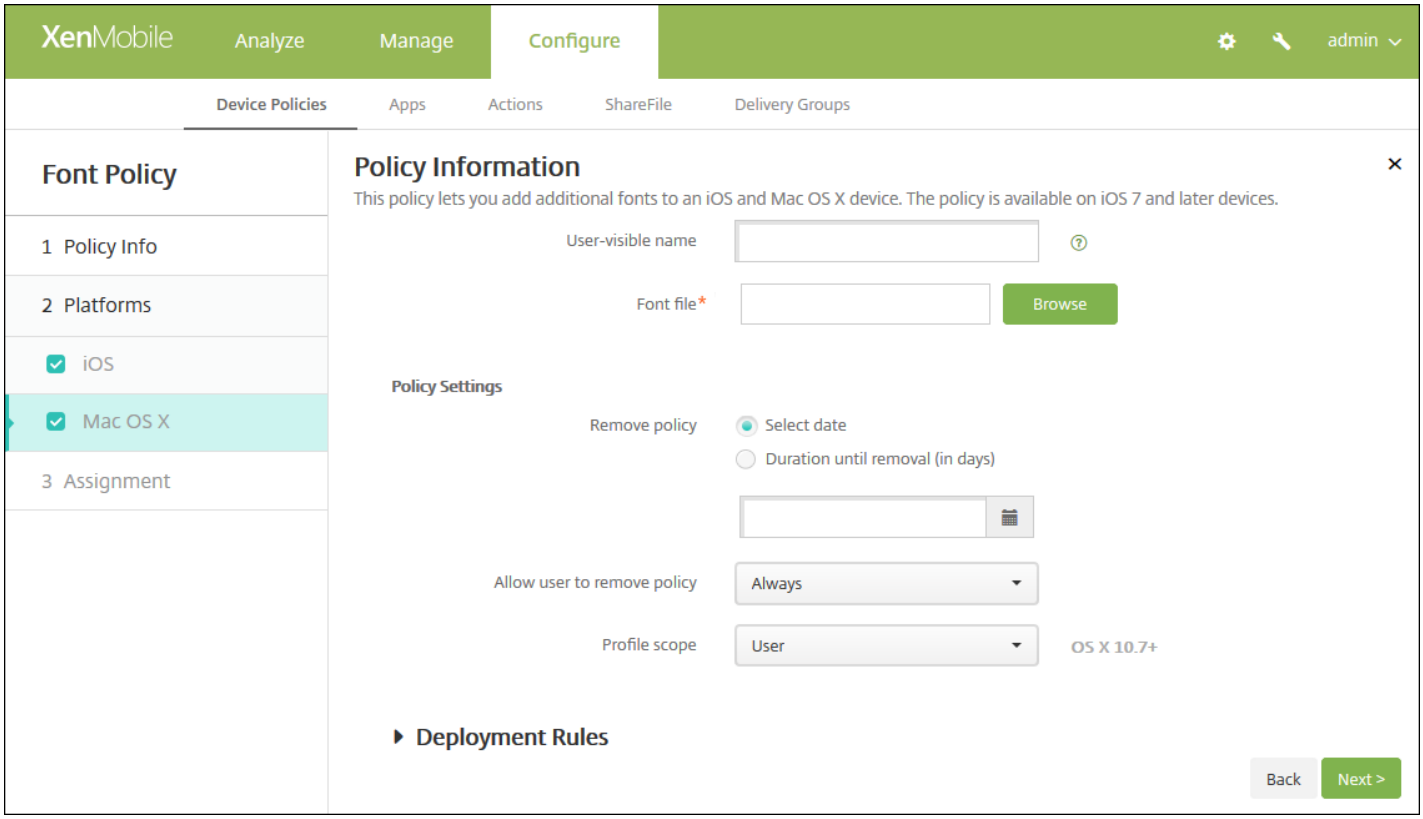
Configure iOS setting



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

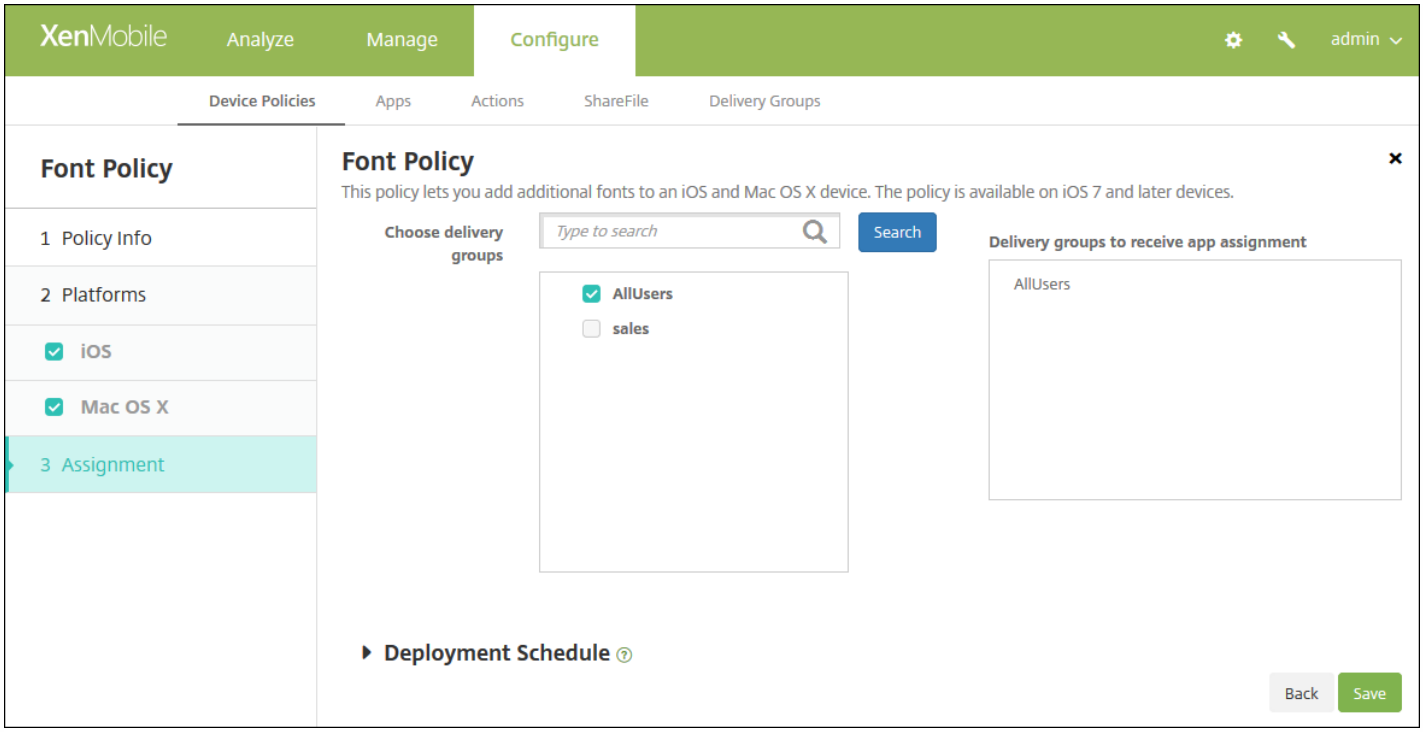


Configure the following settings:

- **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 policies

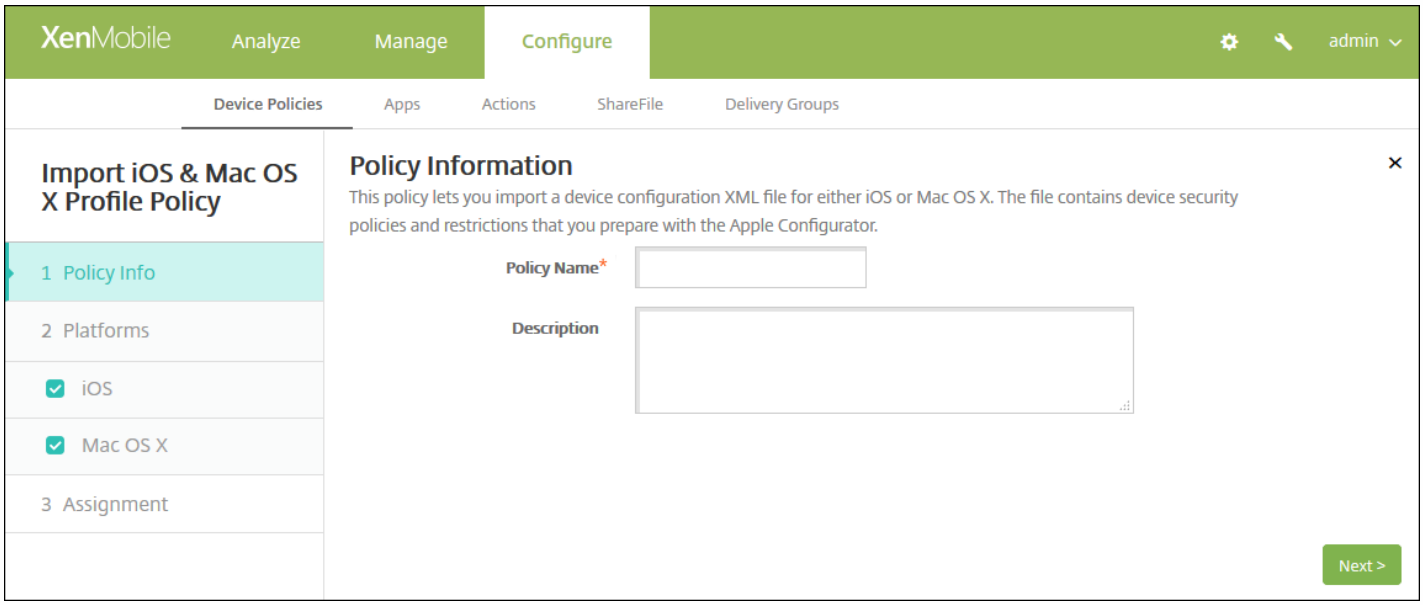
Sep 15, 2015

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. For more information about using the Apple Configurator to create a configuration file, see Apple's Configurator Help page.

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

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

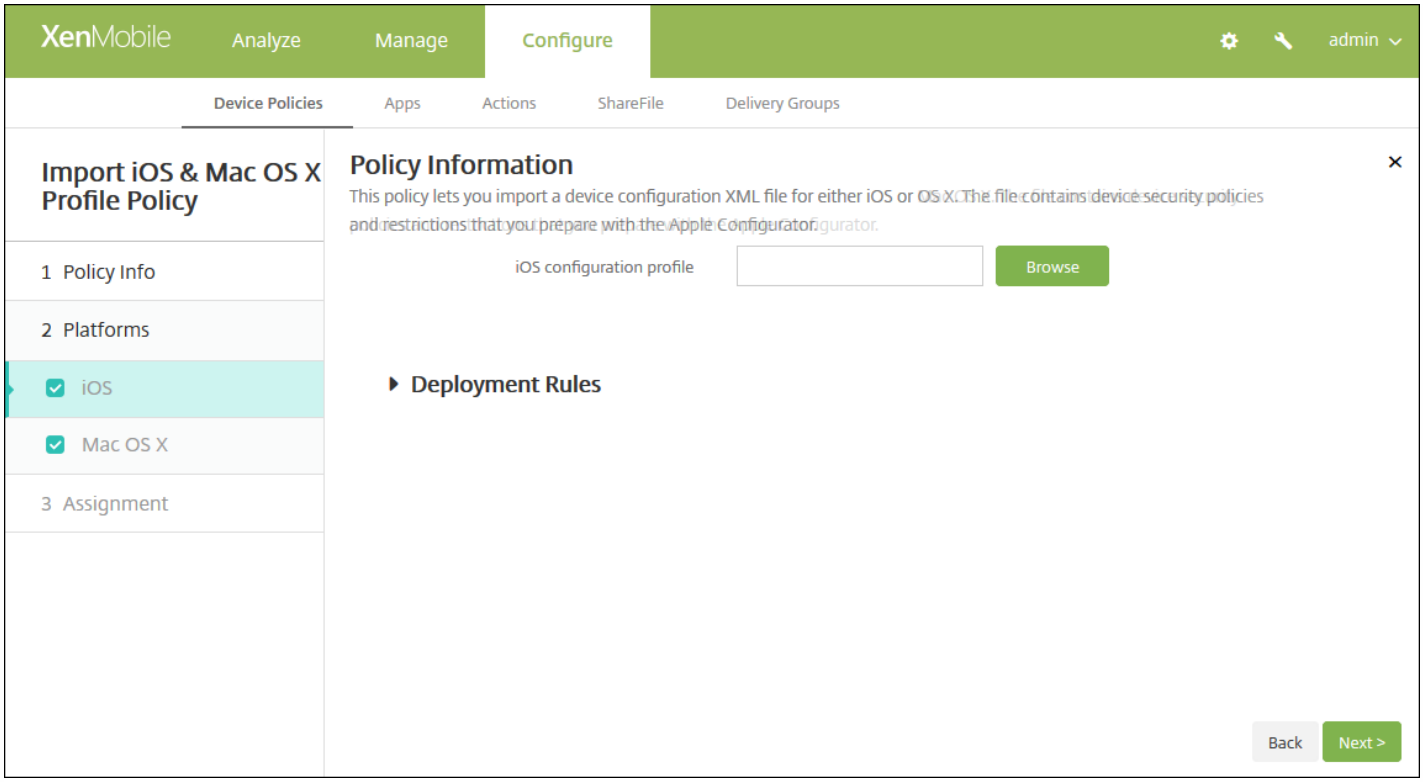
3. Expand **More**, and then under **Custom**, click **Import iOS & Mac OS X Profile**. The **Import iOS & Mac OX X Profile Policy** information page appears.



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.

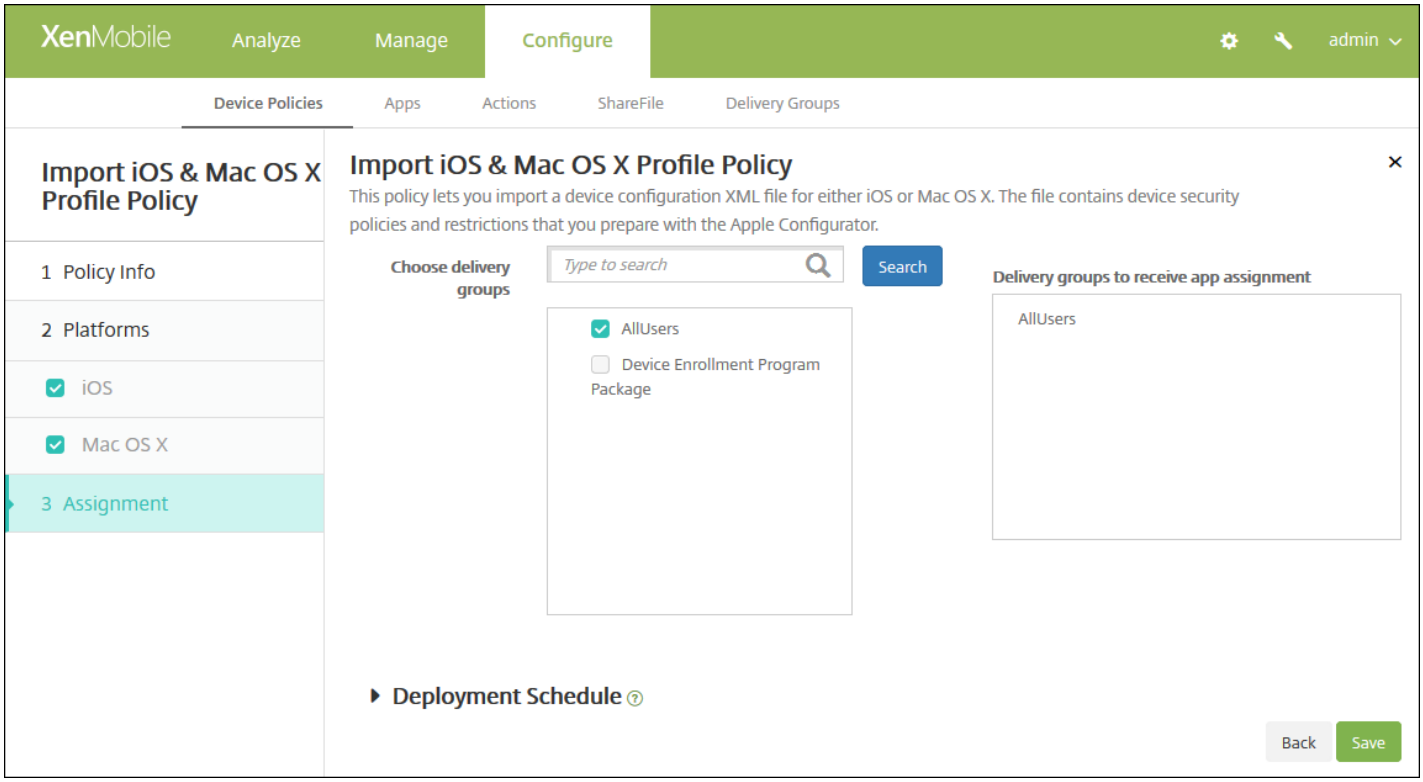
When you finish configuring the settings for a platform, refer to Step 8 for how to set that platform's deployment rules. .

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

8. Click **Next**. The **Import iOS & Mac OS X 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** to save the policy.

Kiosk device policy for Samsung SAFE

Jul 08, 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

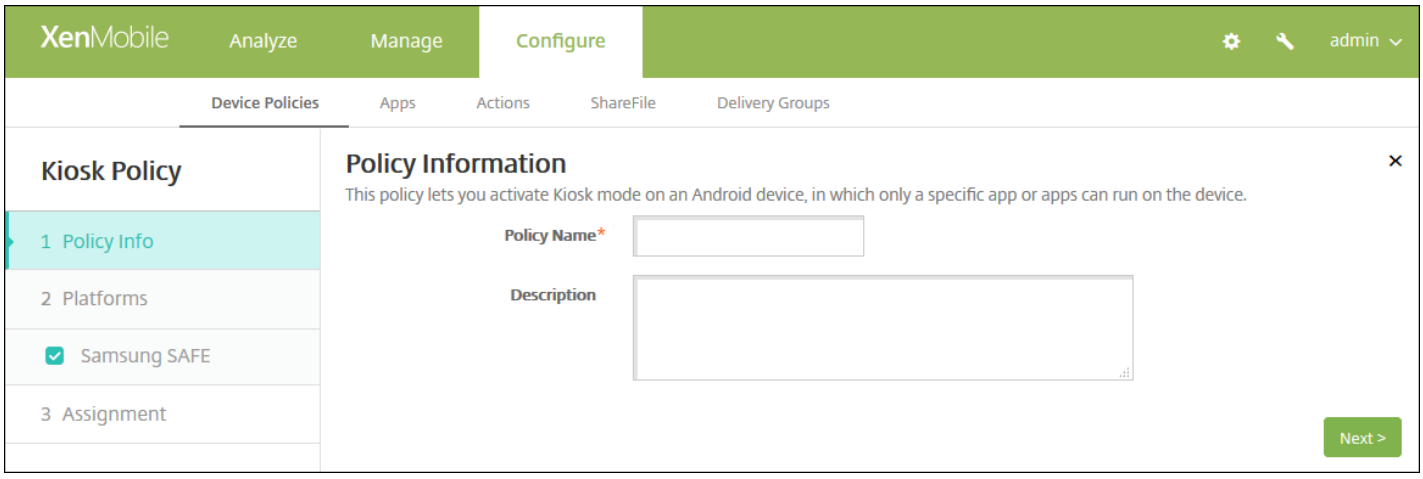
Note:

- 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.

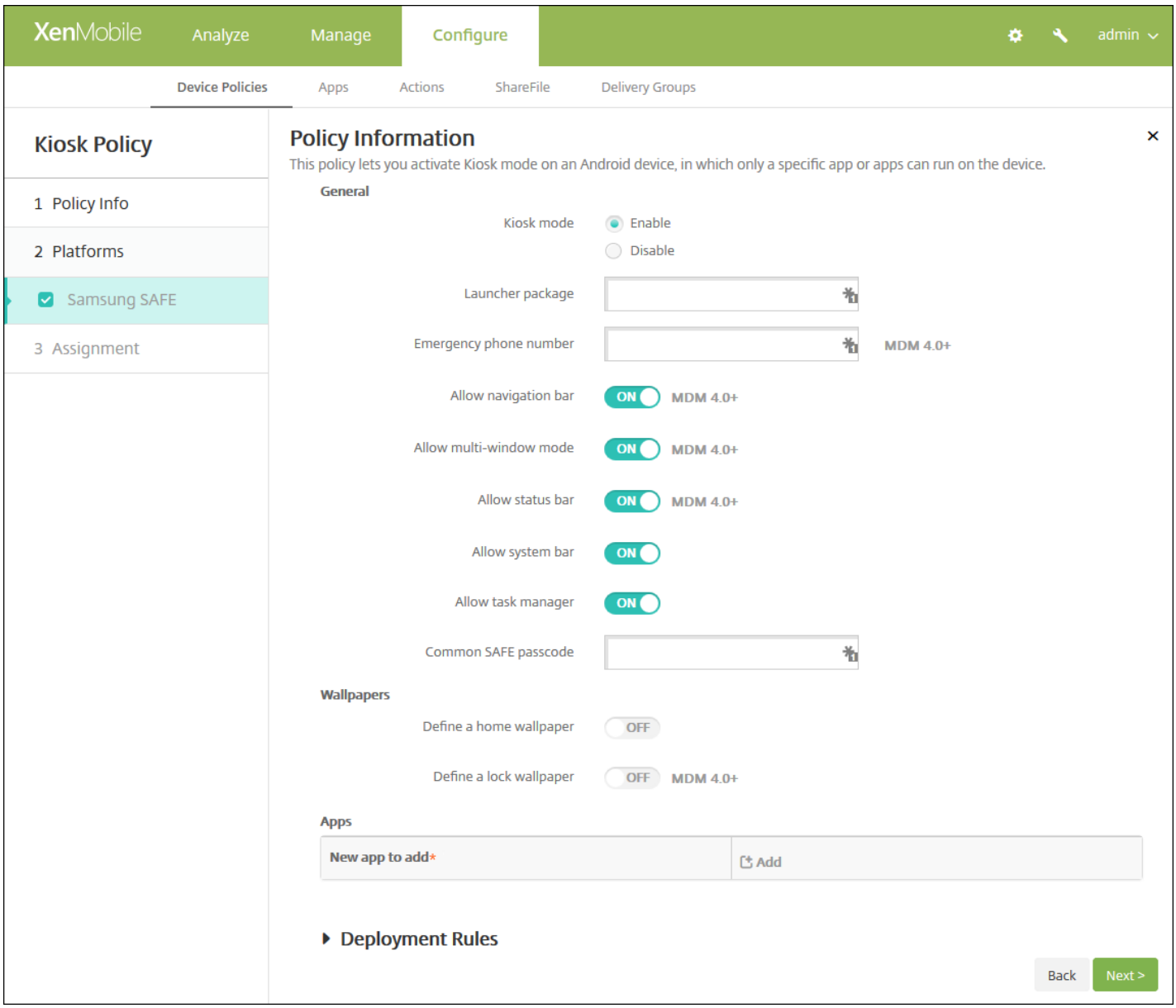
3. Expand **More** and then, under **Security**, click **Kiosk**. The **Kiosk Policy** page appears.



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.

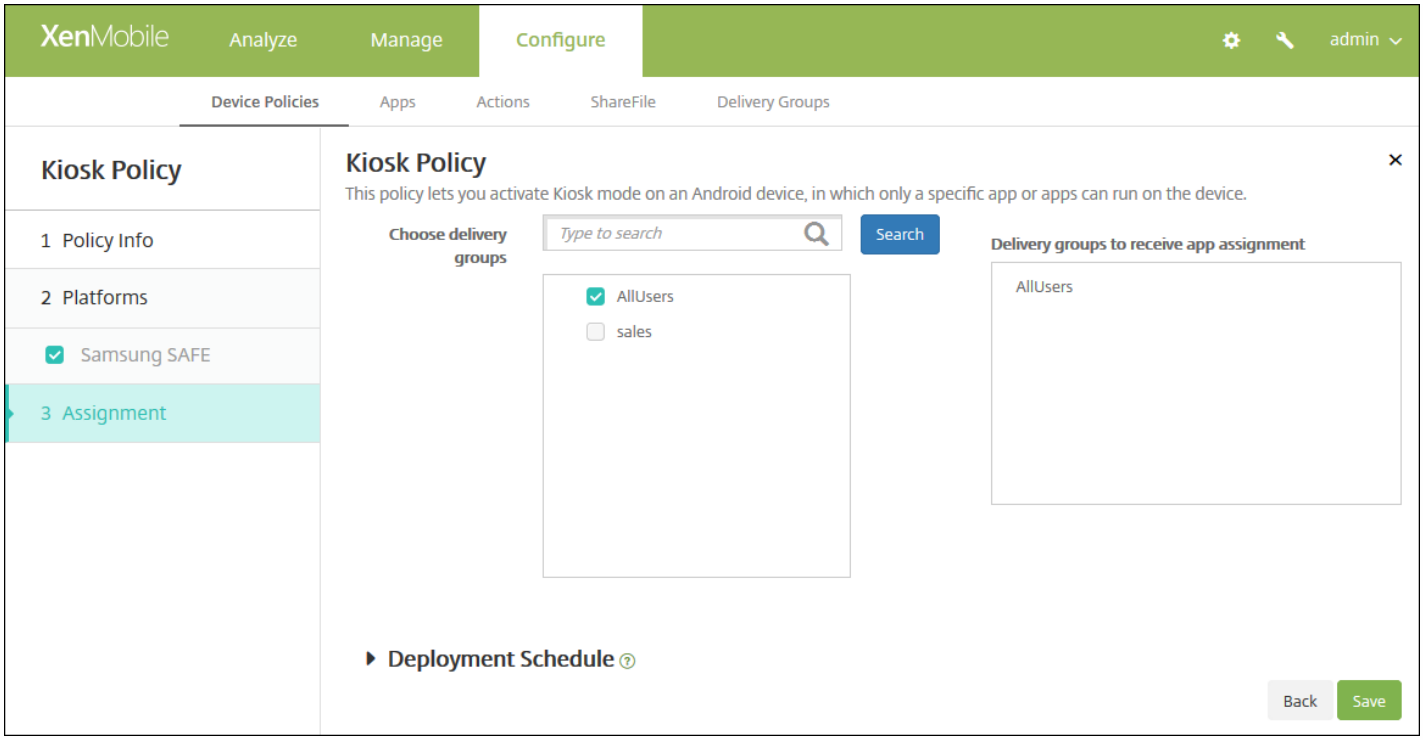
- **Allow navigation bar**: Select whether to let users see and use the navigation bar while in Kiosk mode. Applies only to MDM 4.0 and later. The default is **ON**.
- **Allow multi-window mode**: Select whether to let users use multiple windows while in Kiosk mode. Applies only to MDM 4.0 and later. 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**.

LDAP device policies

Mar 03, 2015

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.

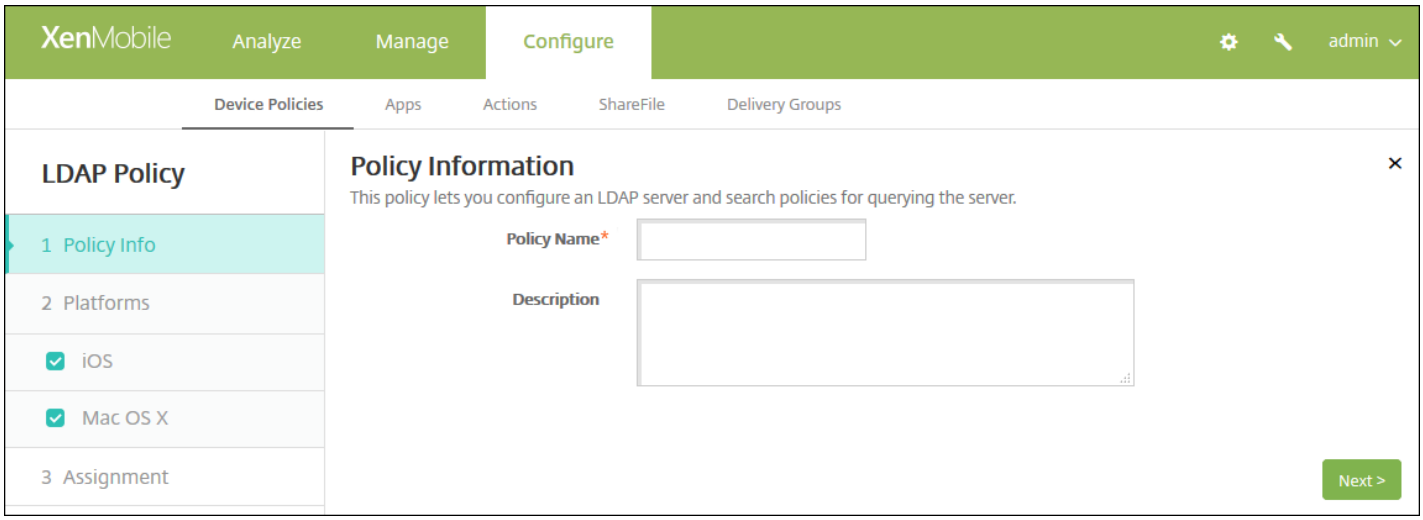
iOS settings

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:

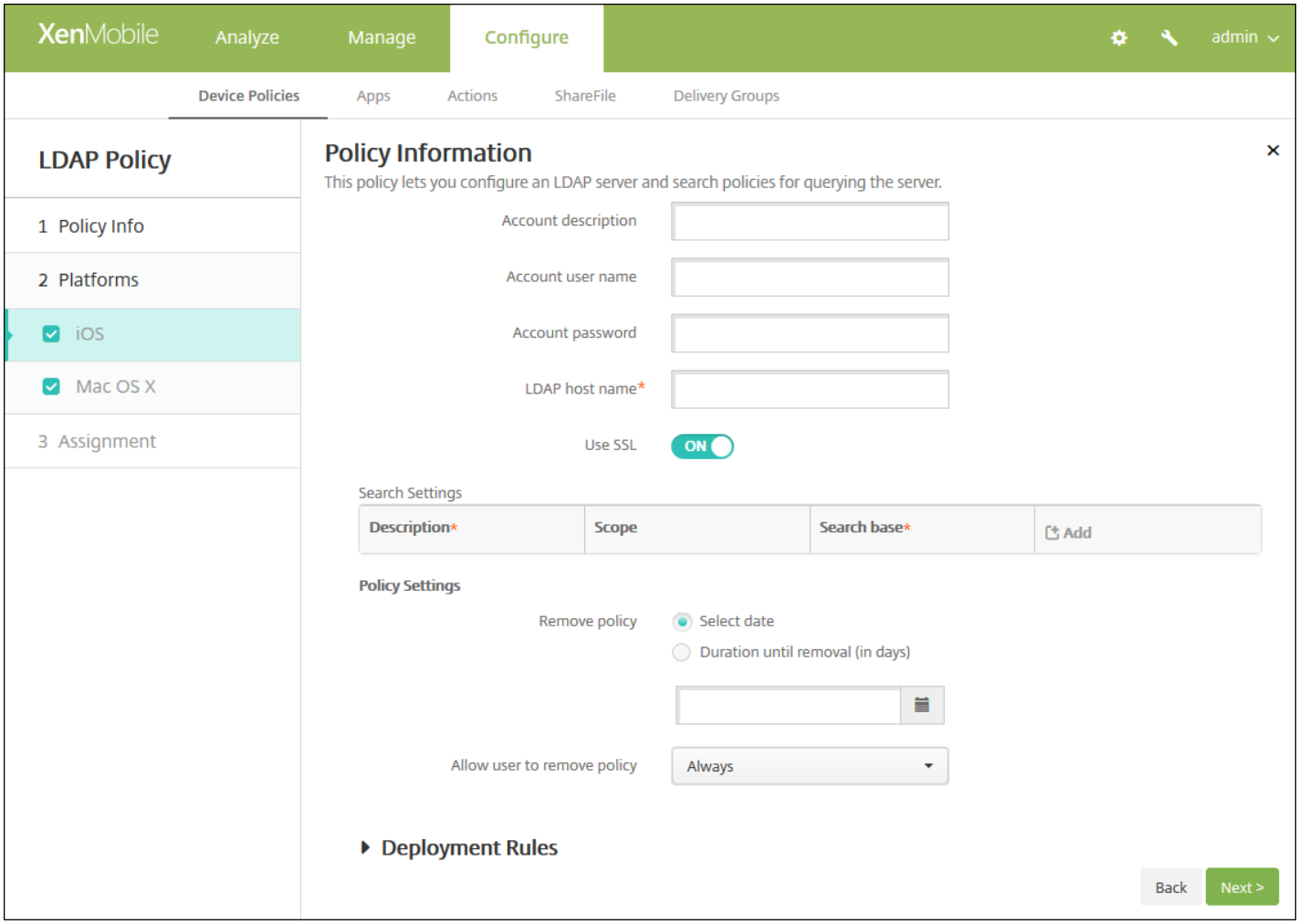
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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:

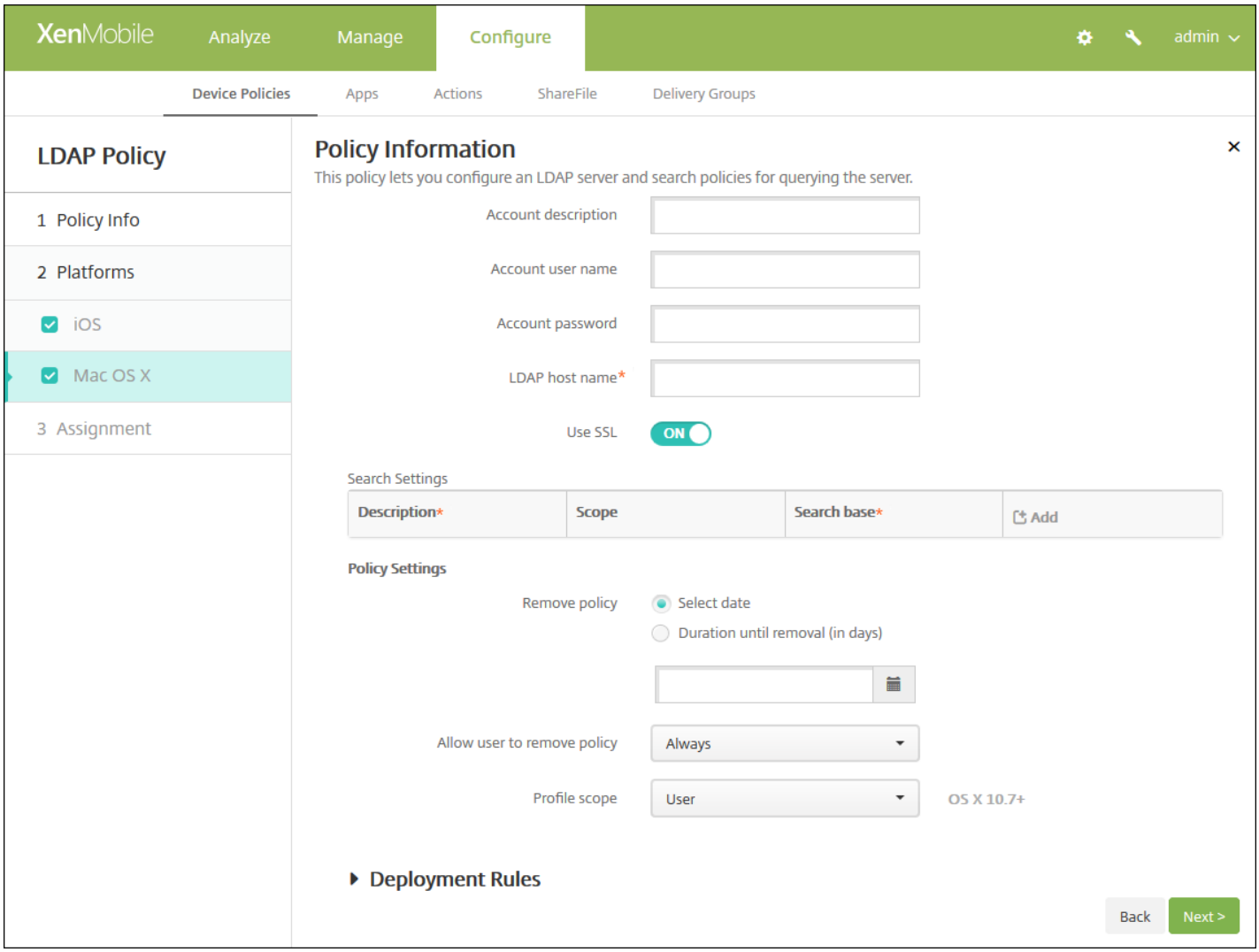
- **Account description**: Enter an optional account description.
- **Account user name**: Enter an optional user name.
- **Account password**: Enter an optional password. Use this only with encrypted profiles.
- **LDAP host name**: Enter the LDAP server host name. This field is required.
- **Use SSL**: 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.

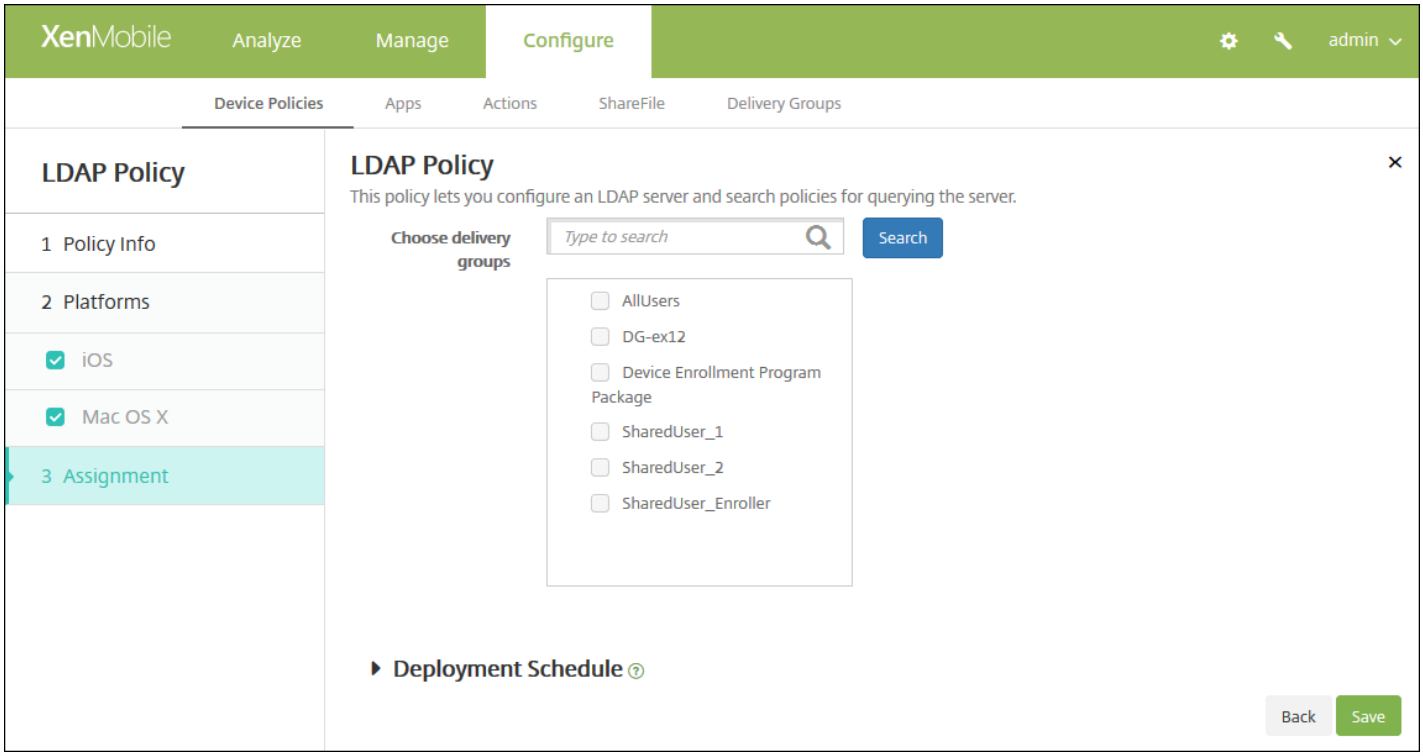
    Note: To delete an existing search setting, hover over the line containing the listing and click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing.

    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 policies

Apr 08, 2015

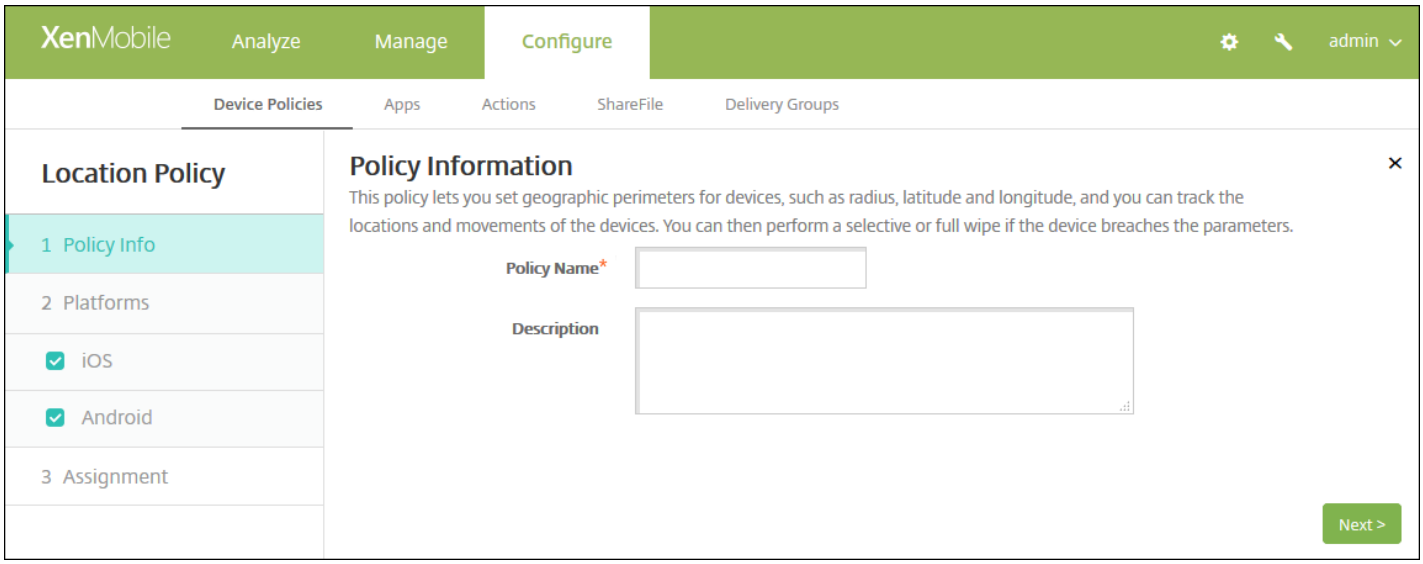
You create location device policies in XenMobile to enforce geographic boundaries, as well as to track the location and movement of users' devices. When users breach the defined boundary, also called a *geofence*, XenMobile can perform a selective or full wipe immediately or after a specific time period 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:

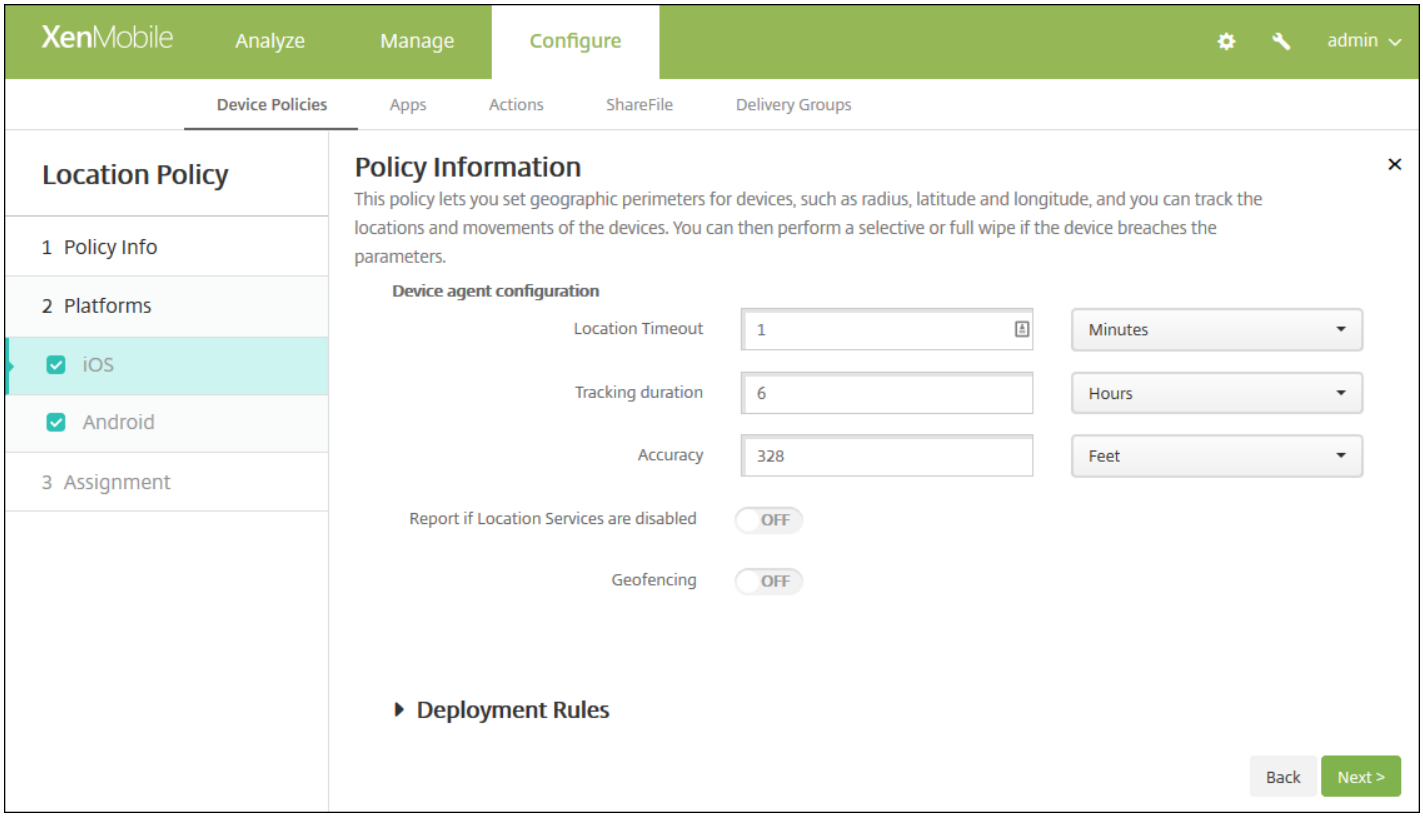
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

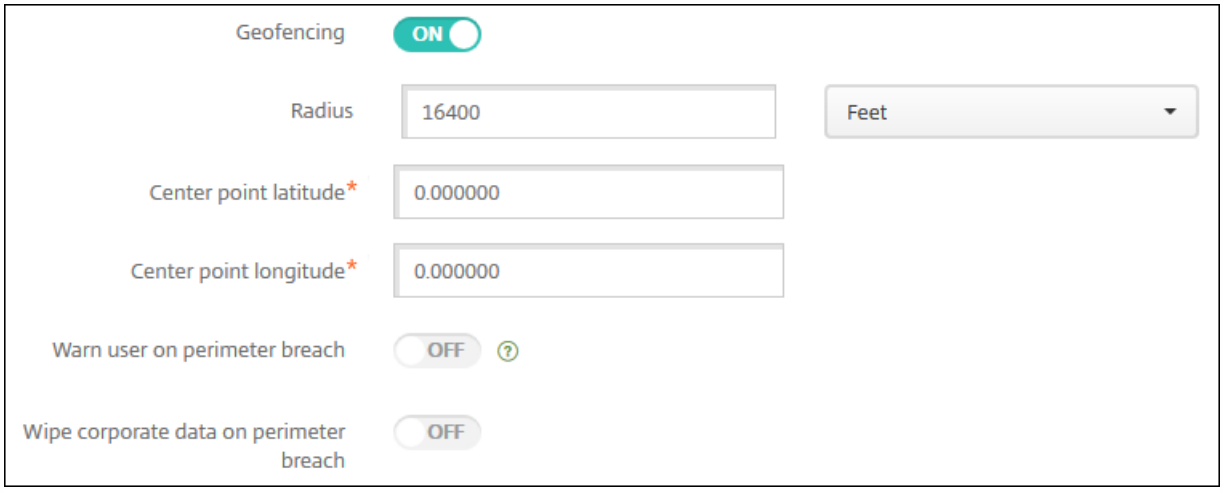
When you finish configuring the settings for a platform, refer to Step 7 for how to set that platform's deployment rules.

Configure iOS settings



Configure these settings:

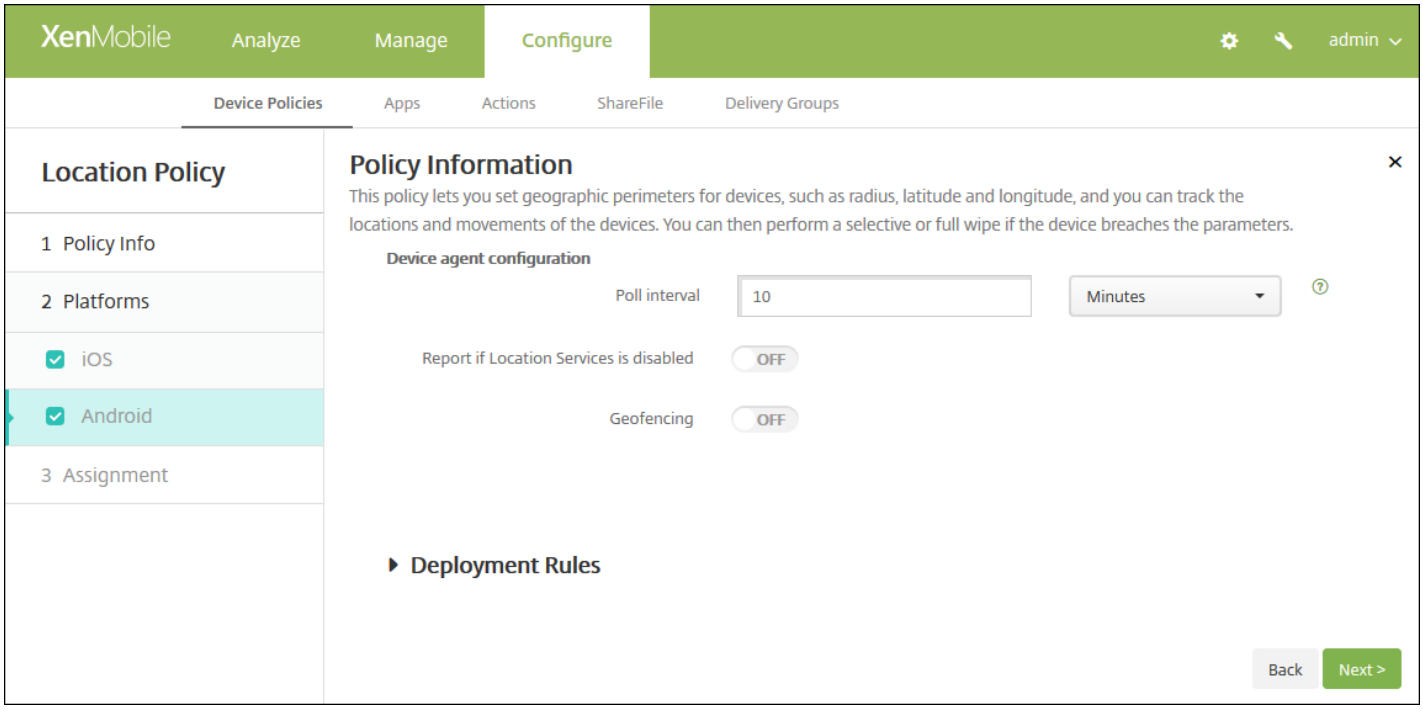
- **Location timeout**: Type a numeral and then, in the list, click **Seconds** or **Minutes** to set how often XenMobile attempts to fix the device's location. Valid values are 60–900 seconds or 1–15 minutes. The default is 1 minute.
- **Tracking duration**: Type a numeral and then, in the list, click **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**



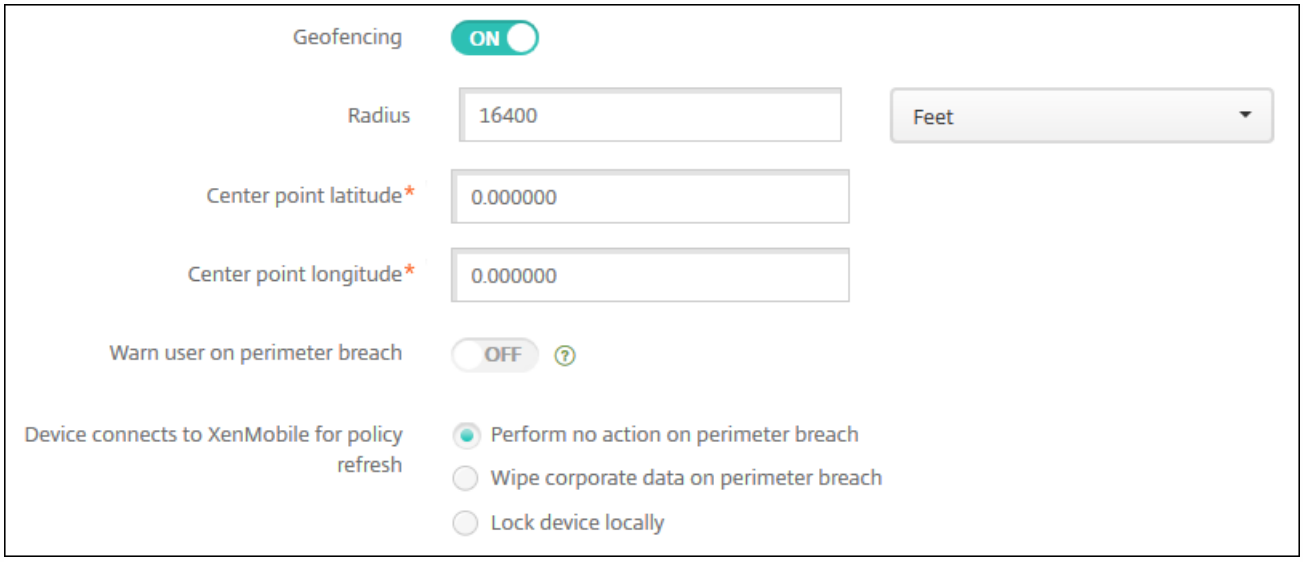
When you enable Geofencing, configure these settings:

- **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**

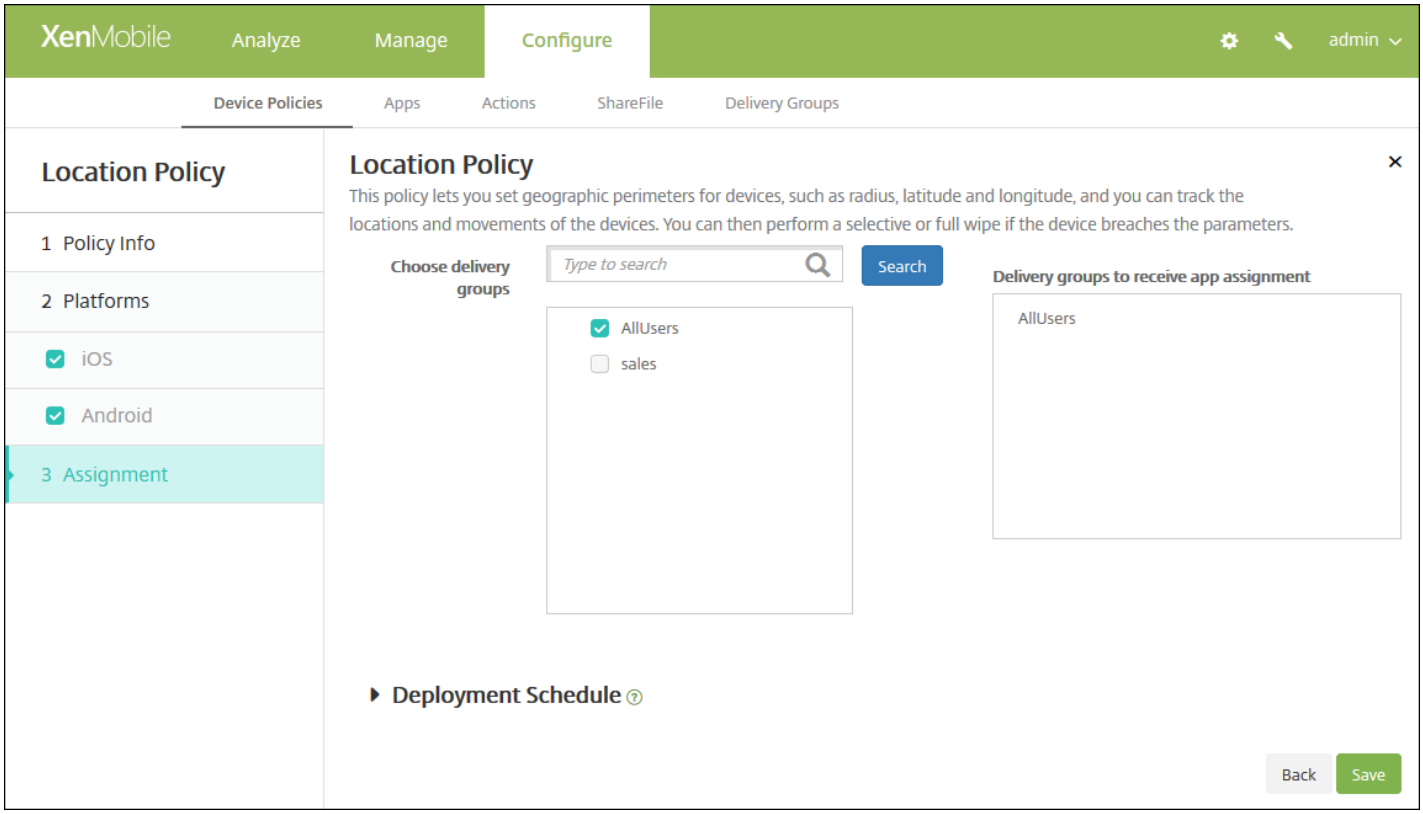


When you enable Geofencing, configure these settings:

- **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 policies

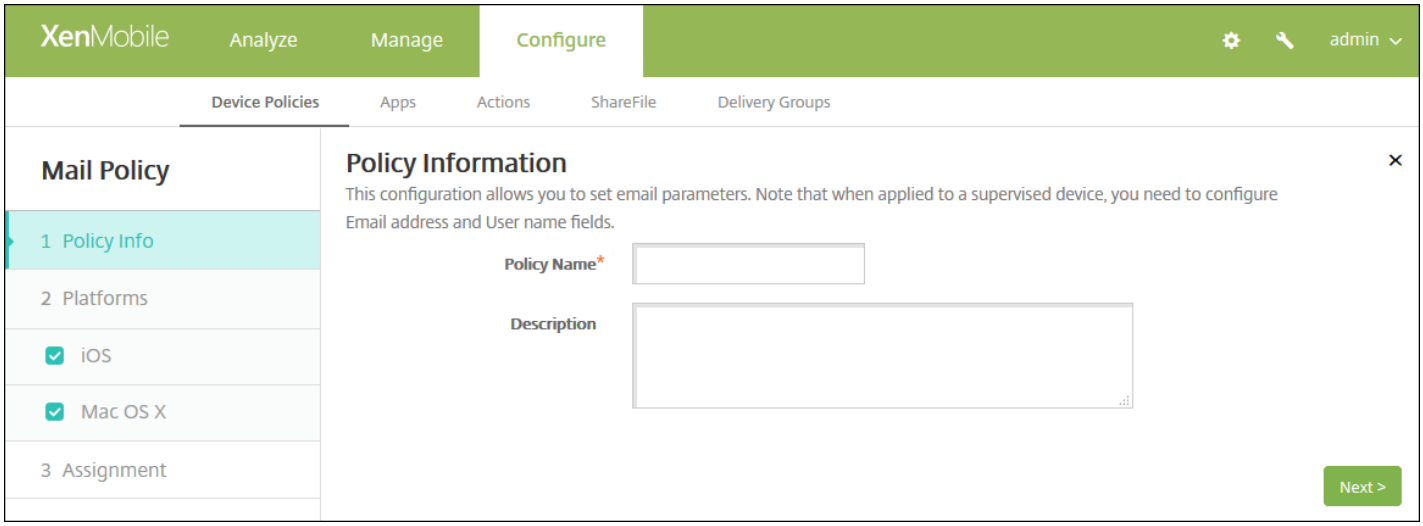
Feb 13, 2015

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.

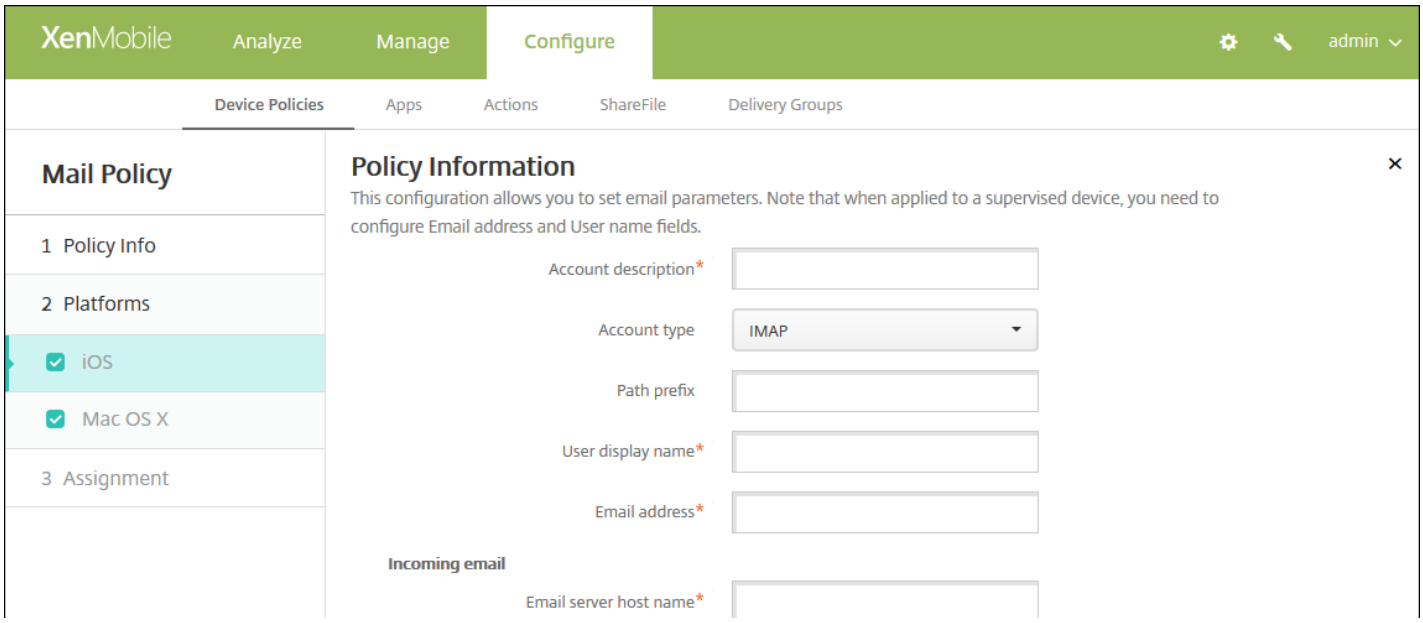
3. Click **More** and then, under **End user**, click **Mail**. The **Mail Policy** page appears.

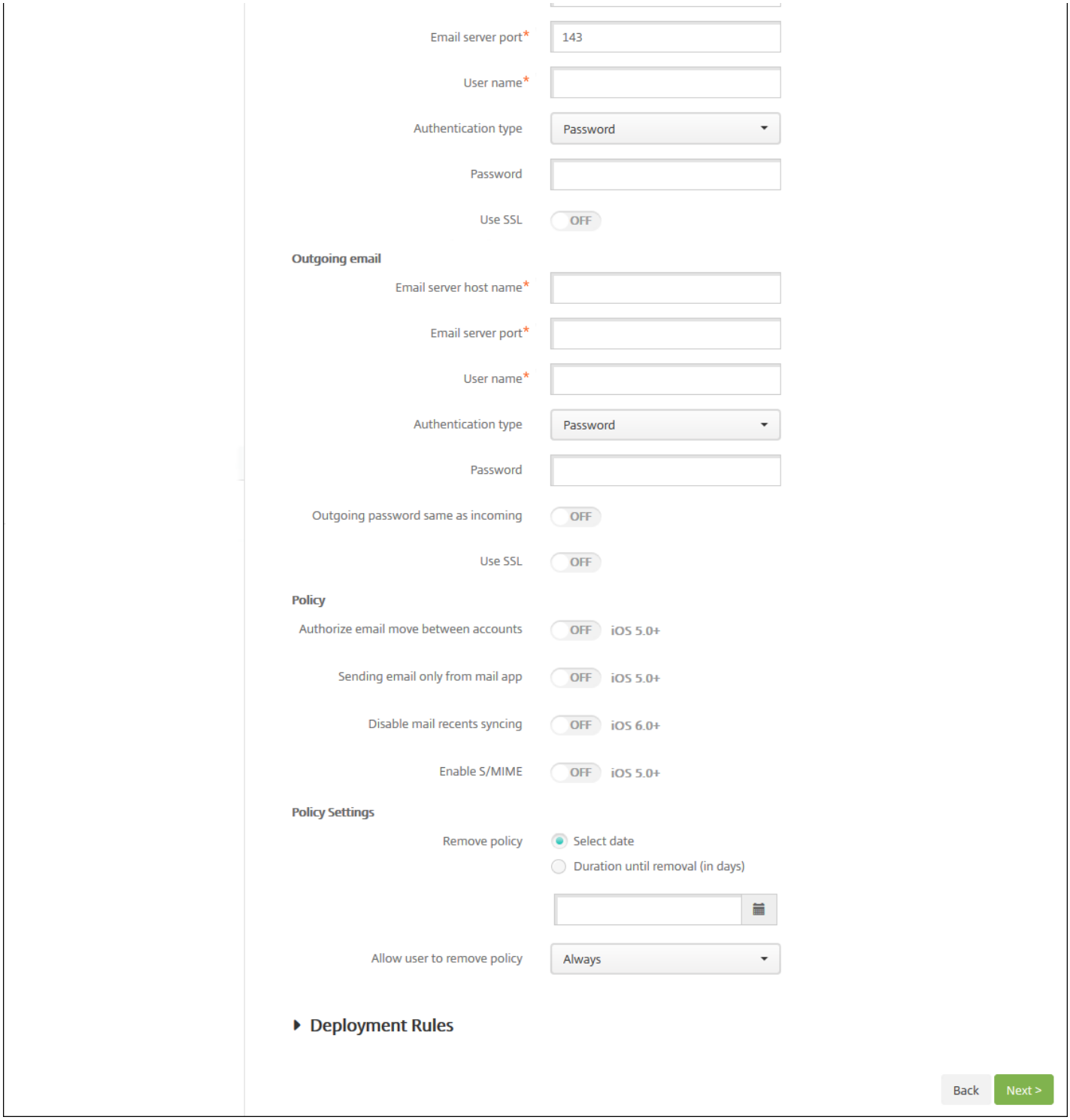


4. In the **Policy Information** pane, enter the following information:

- **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.

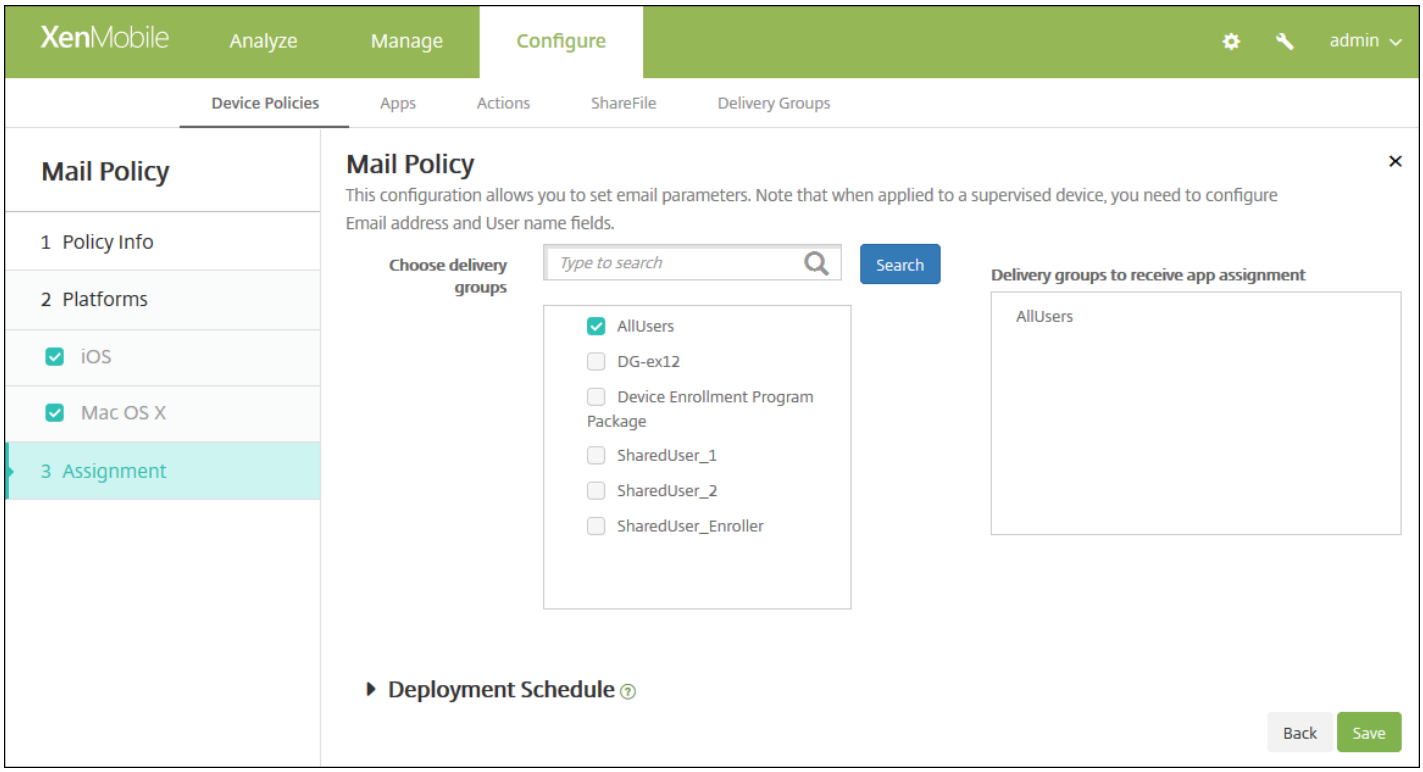
7. Configure the following settings for the platforms you selected.

- **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

Oct 02, 2015

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.

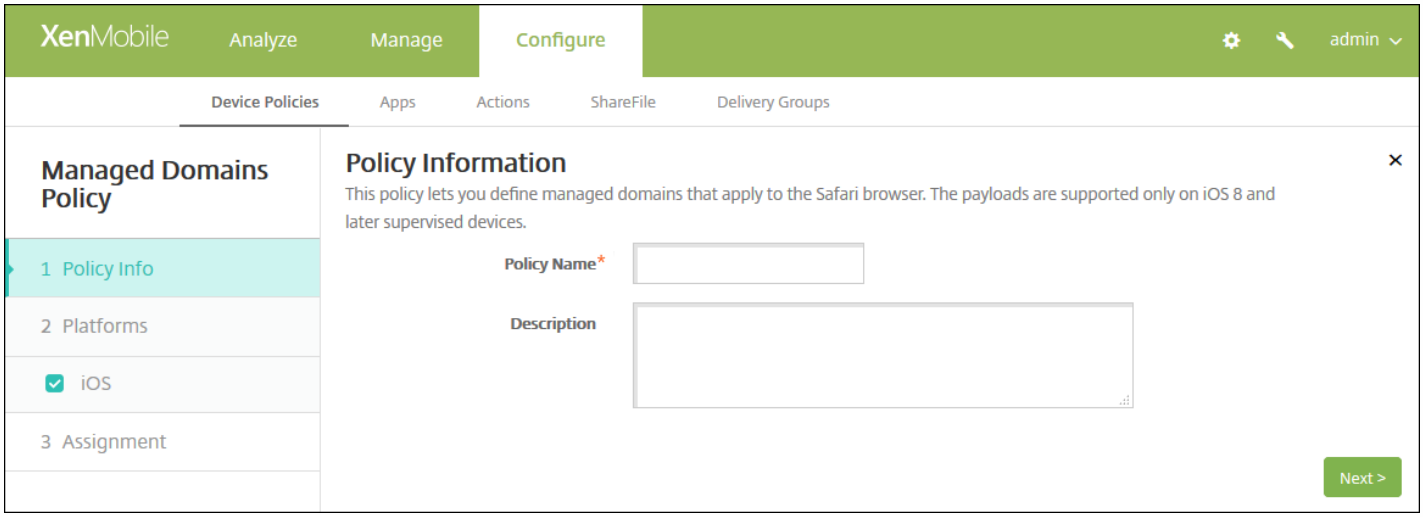
When a user sends email to a recipient whose domain is not on the managed email domains list, the message is flagged on the user's device to warn them that they are sending a message to someone outside your corporate domain.

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.

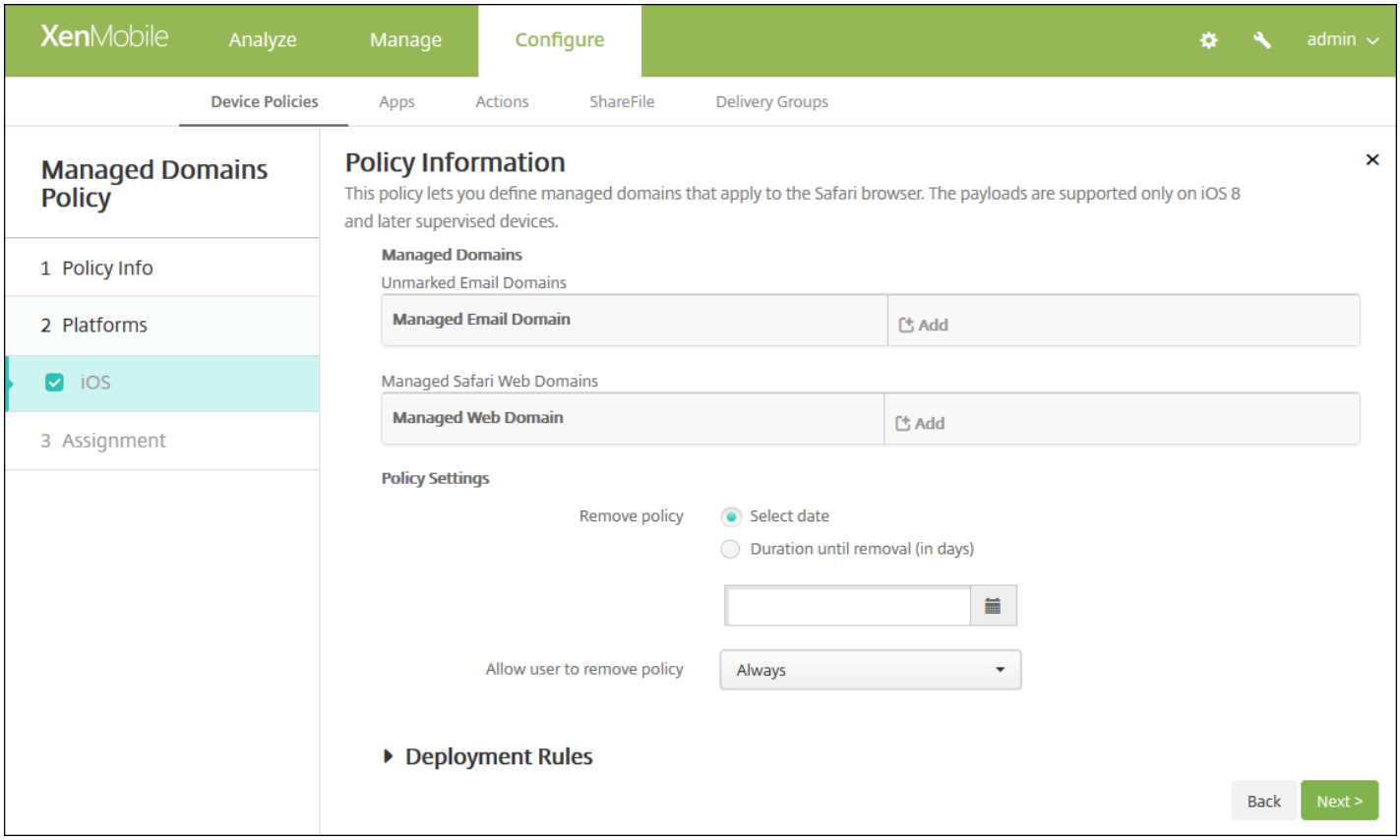
3. Expand **More** and then, under **Security**, click **Managed domains**. The **Managed Domains Policy** information page appears.



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.

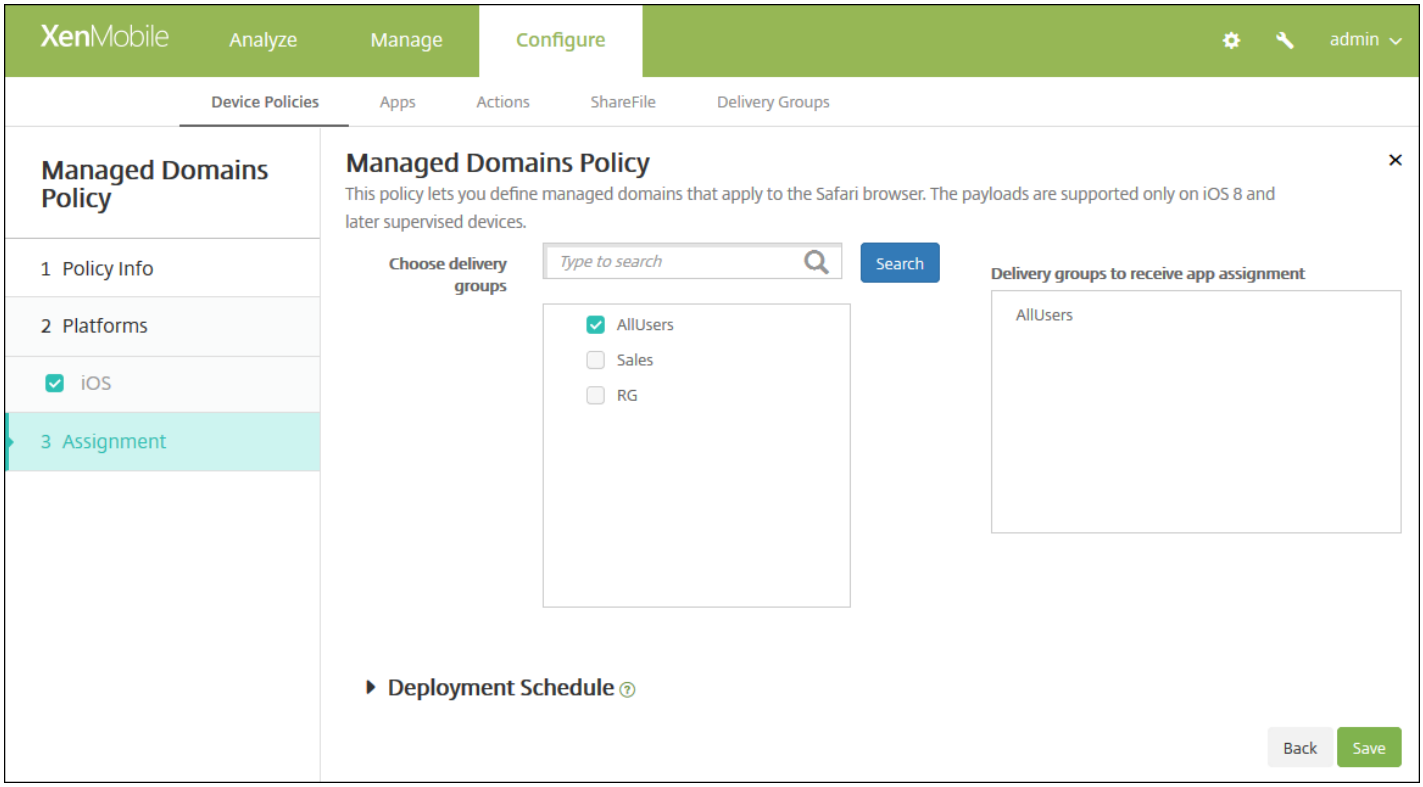
      To edit an existing domain, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- **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

Oct 05, 2015

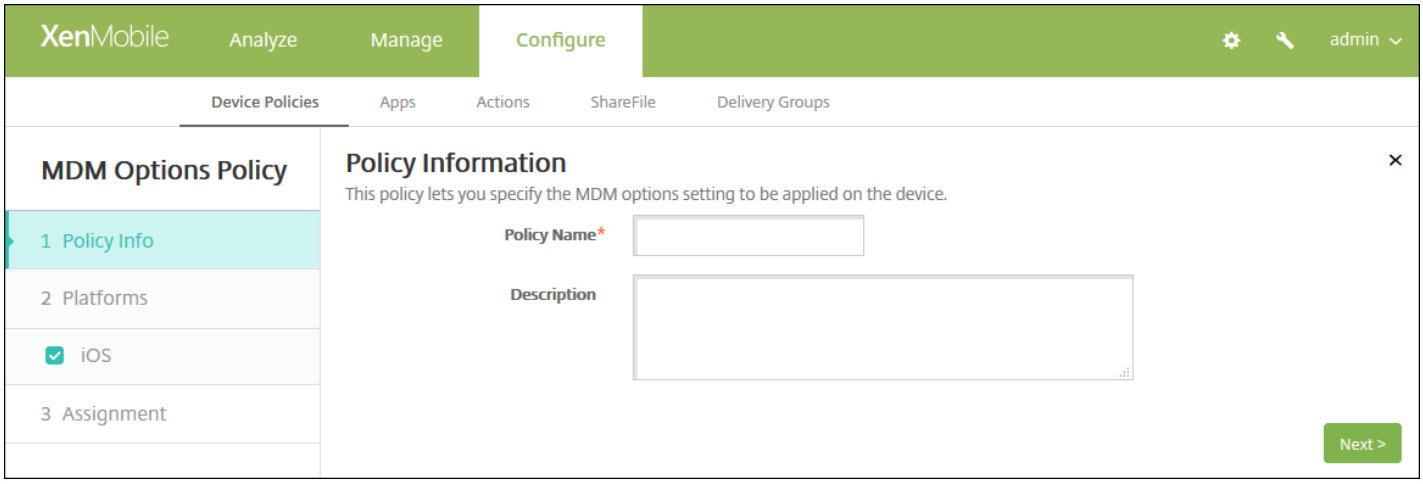
You can create a device policy in XenMobile to manage Find My Phone/iPad Activation Lock on supervised iOS 7.0 and later phone devices. For the steps on setting an iOS device to supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator or iOS Bulk Enrollment.

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.

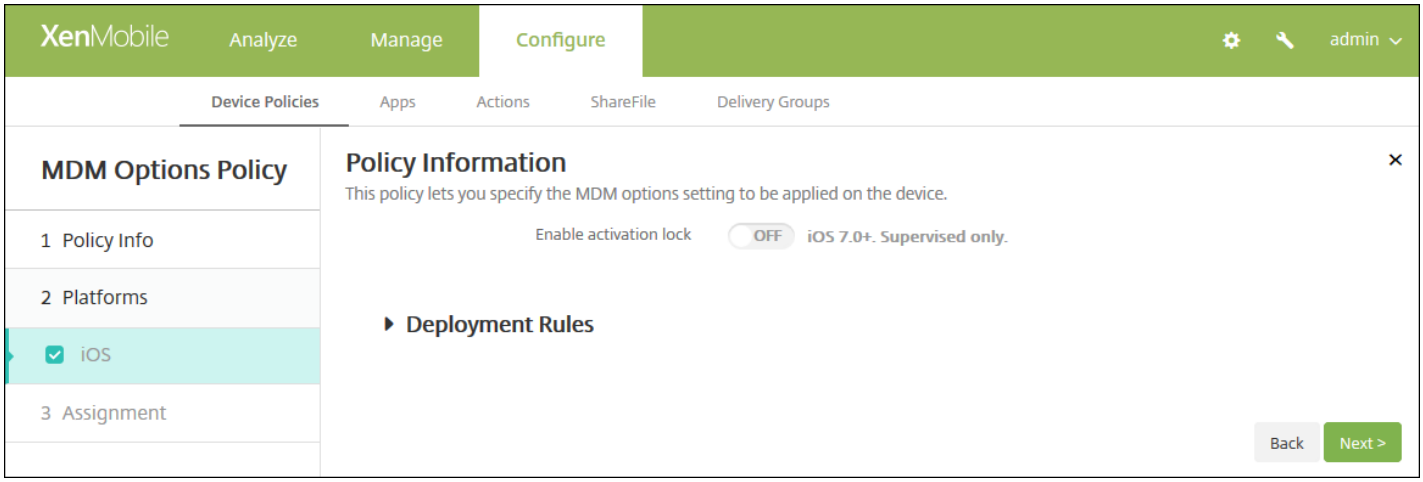
3. Expand **More** and then, under **End user**, click **MDM Options**. The **MDM Options Policy** information page appears.



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.

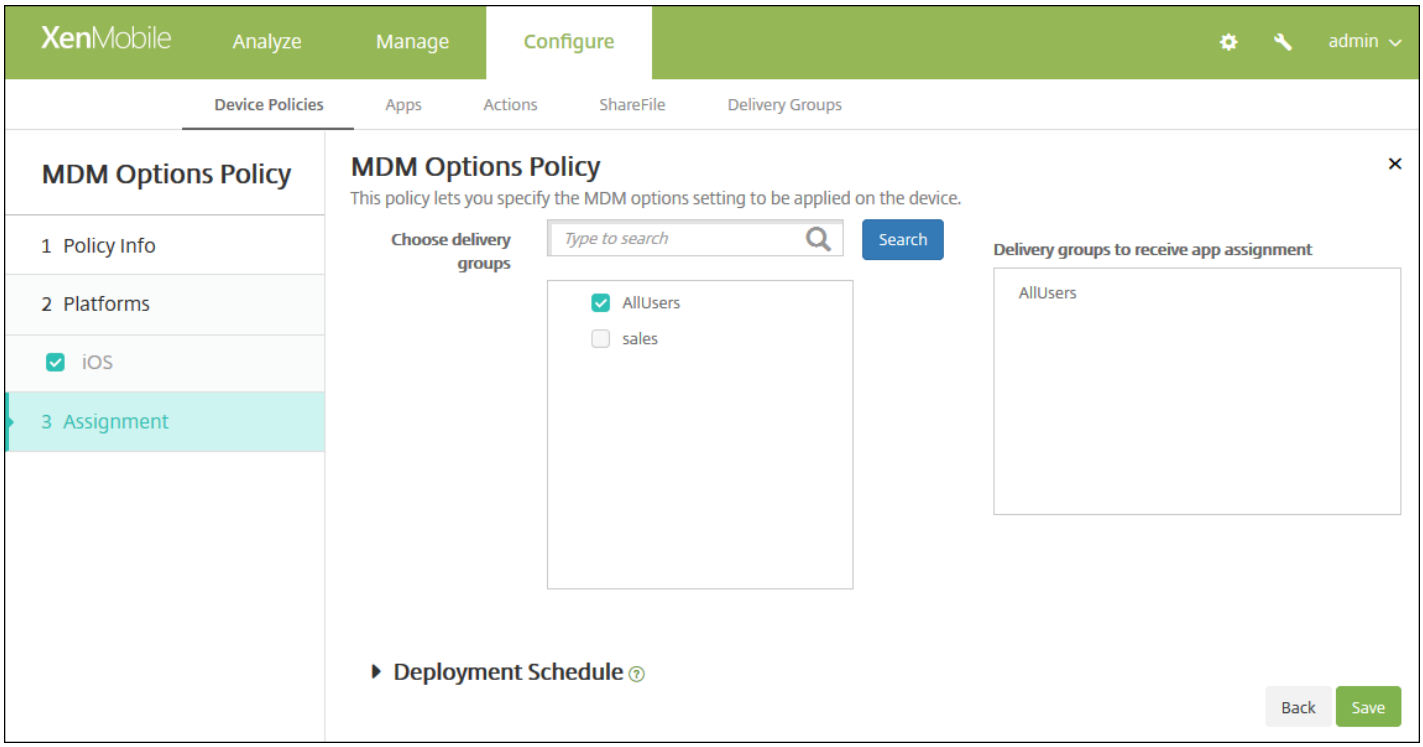


6. Configure this setting:

- **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 policies

Jun 23, 2015

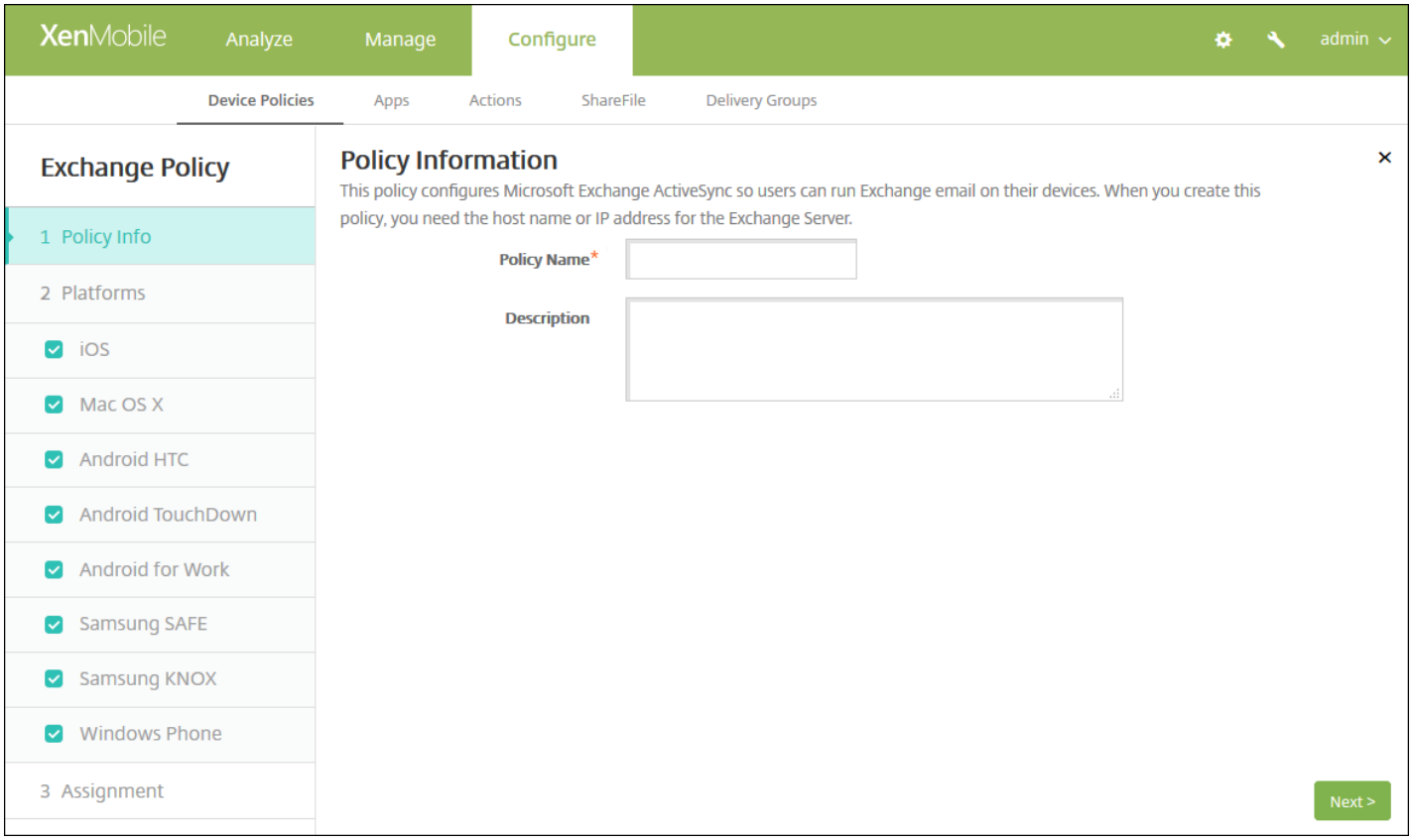
You can use the Exchange ActiveSync device policy to configure an email client on users' devices to let them access their corporate email hosted on Exchange. You can create policies for iOS, Mac OS X, Android HTC, Android TouchDown, Android for Work, Samsung SAFE, Samsung KNOX, and Windows Phone. Each 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.



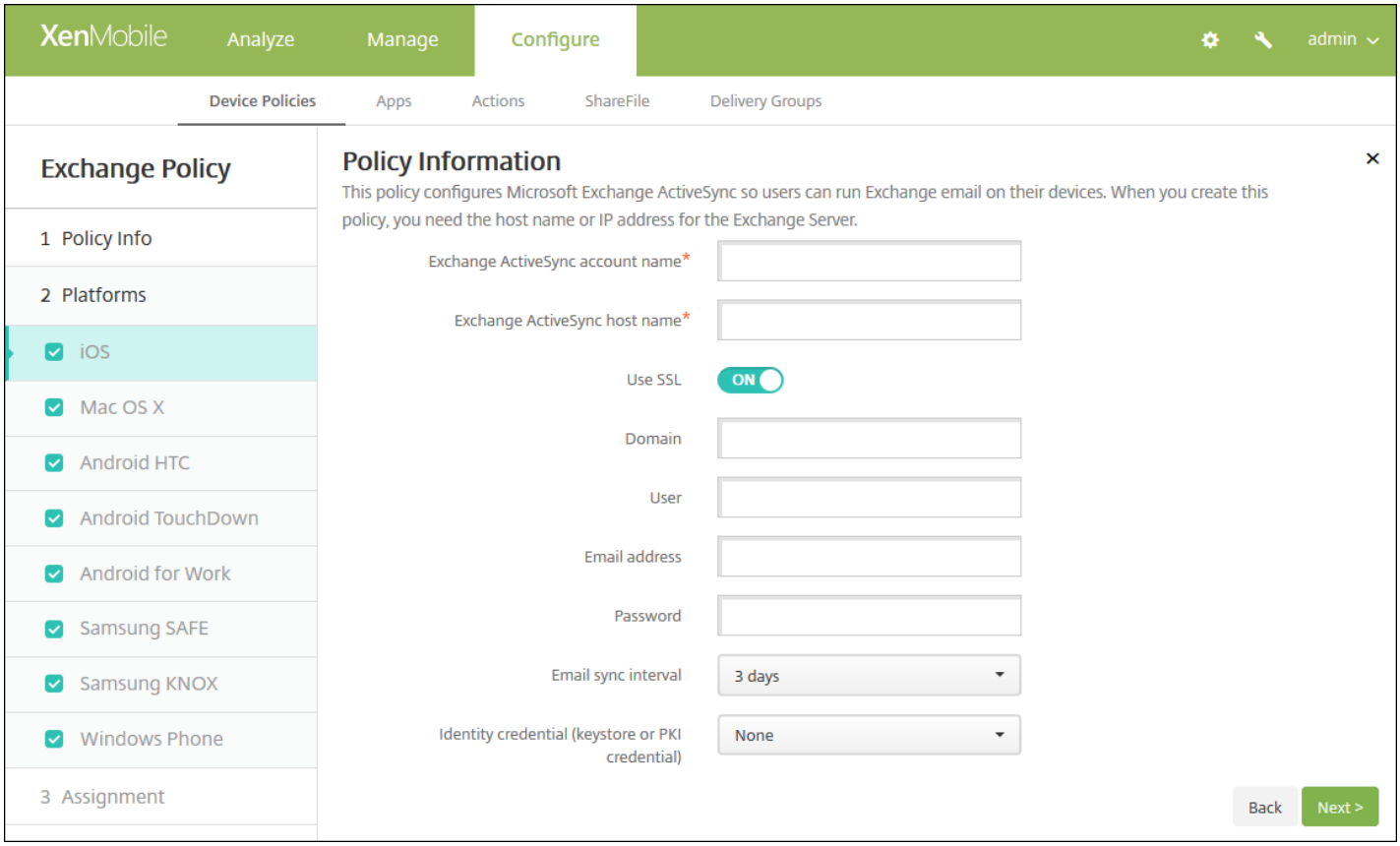
4. In the **Policy Information** pane, type the following information:

- **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



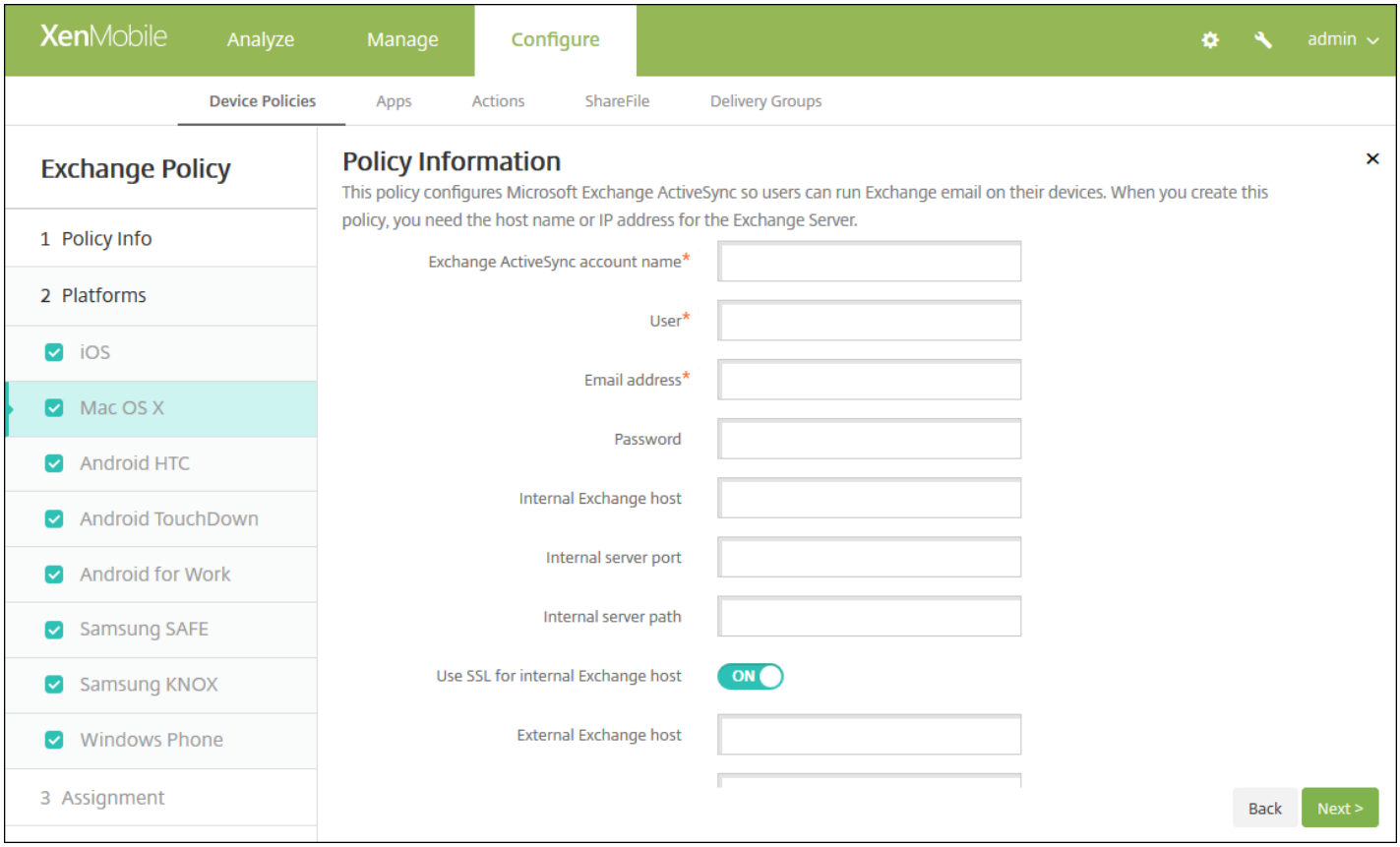
Configure these settings:

- **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



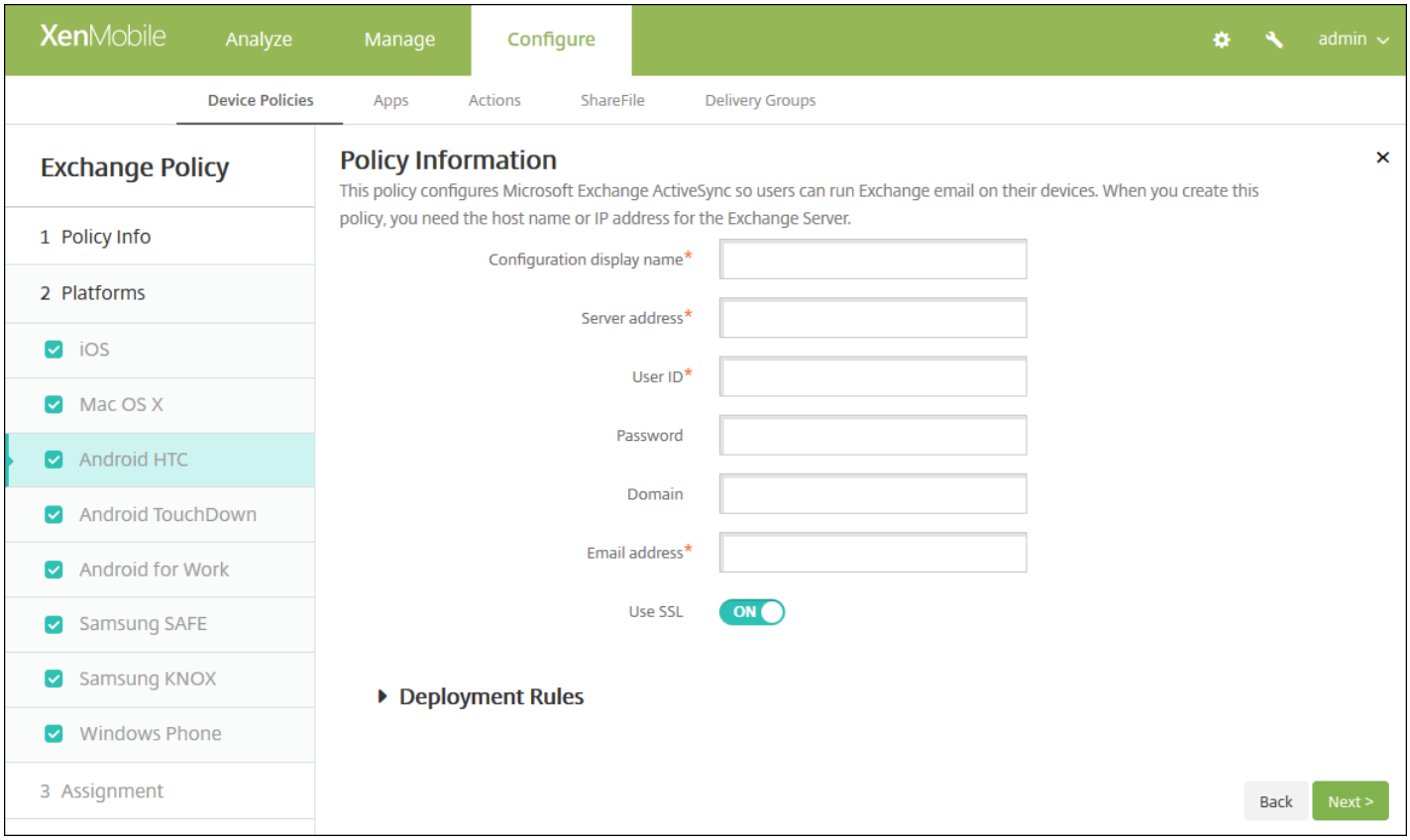
Configure these settings:

- **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**.

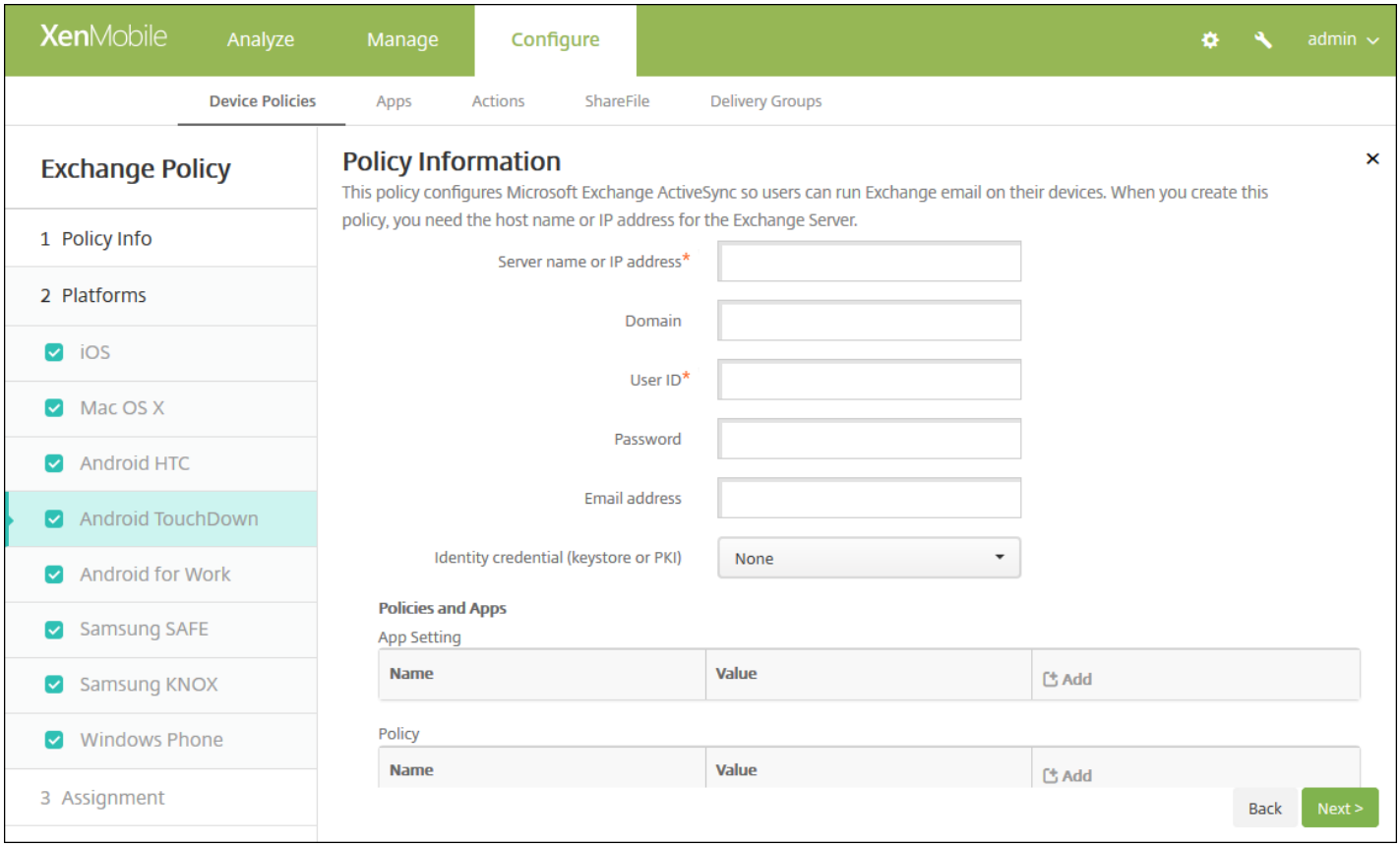
Configure Android HTC settings



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**.

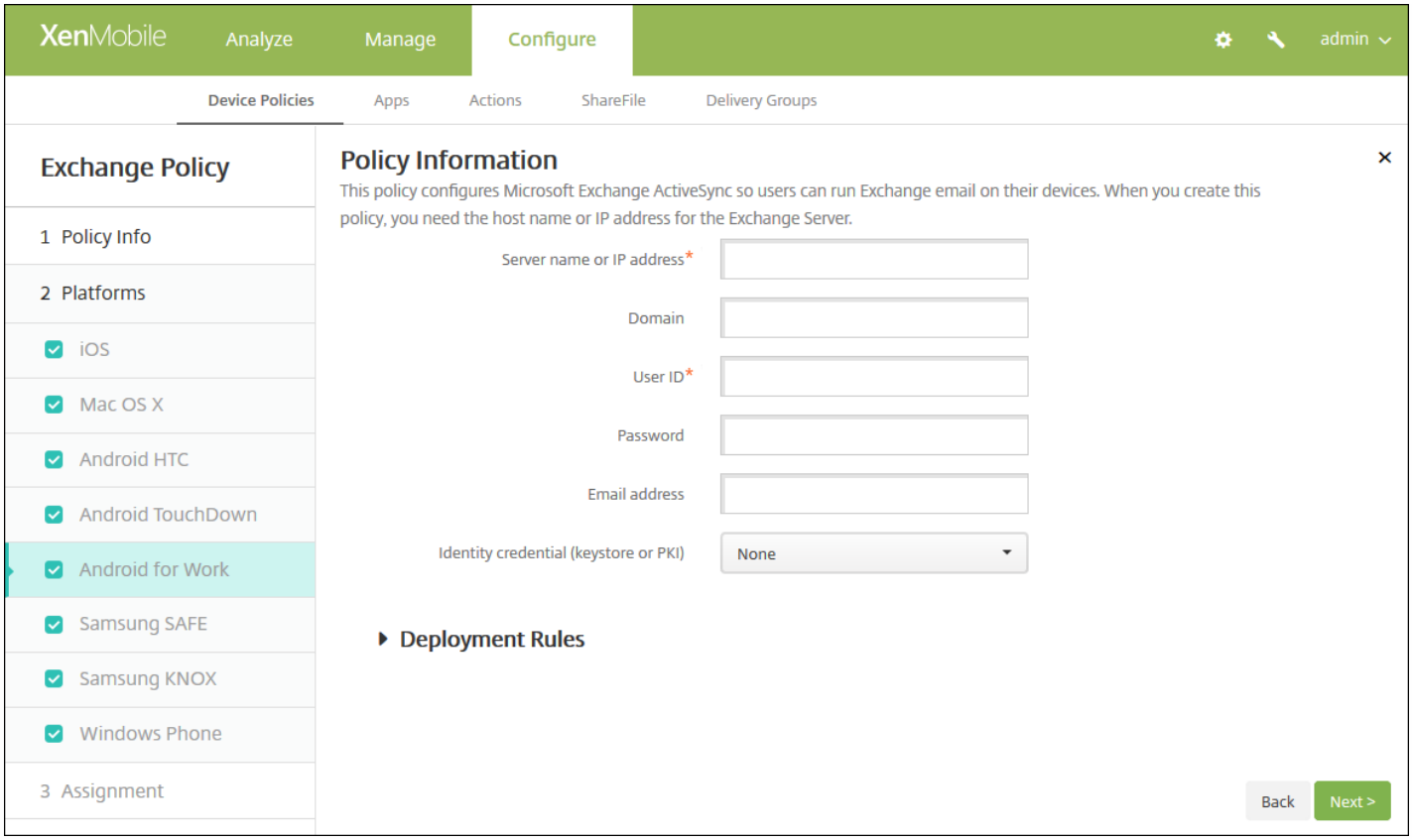
Configure Android TouchDown settings



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.

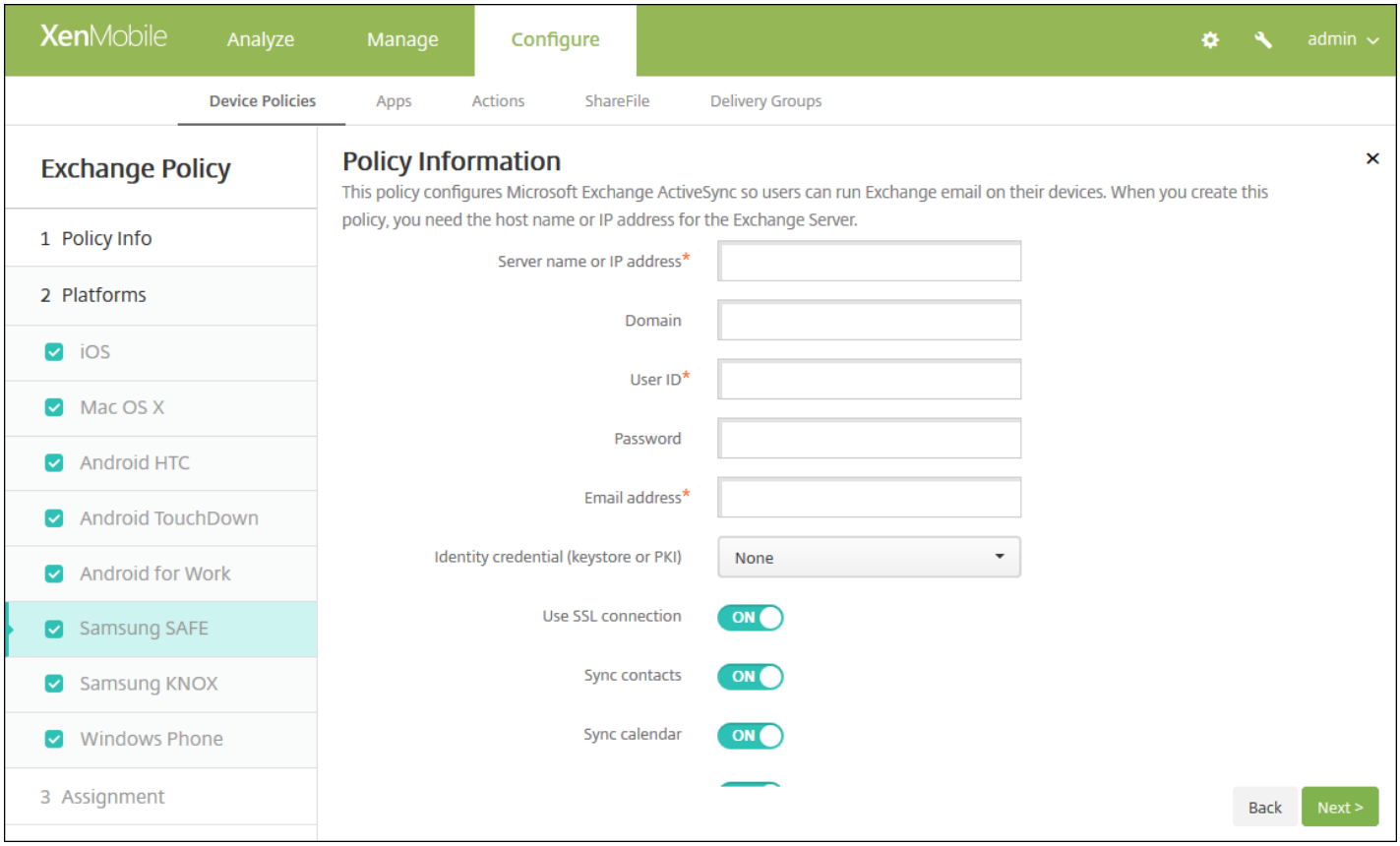
Configure Android for Work



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**.

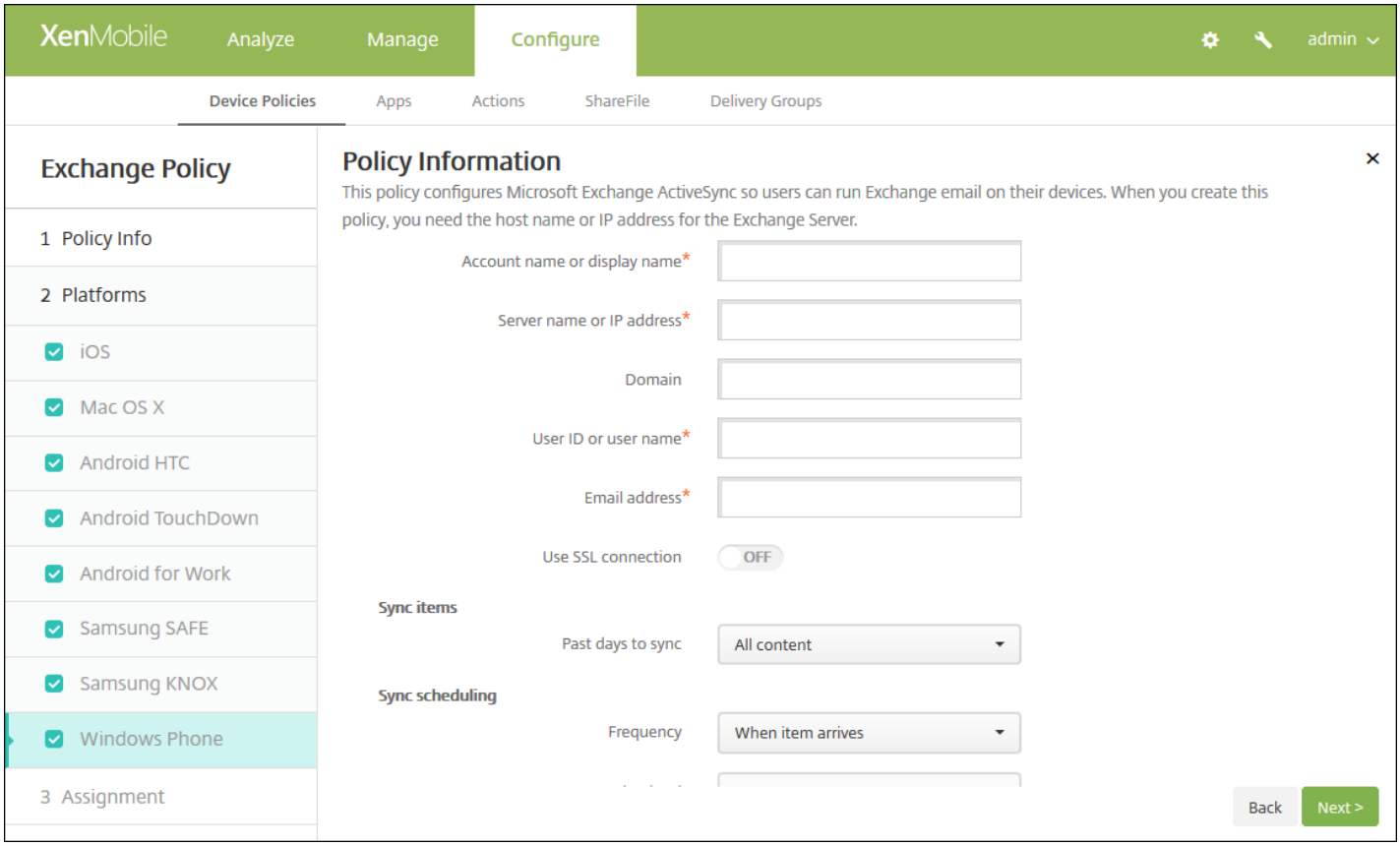
Configure Samsung SAFE and Samsung KNOX settings



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



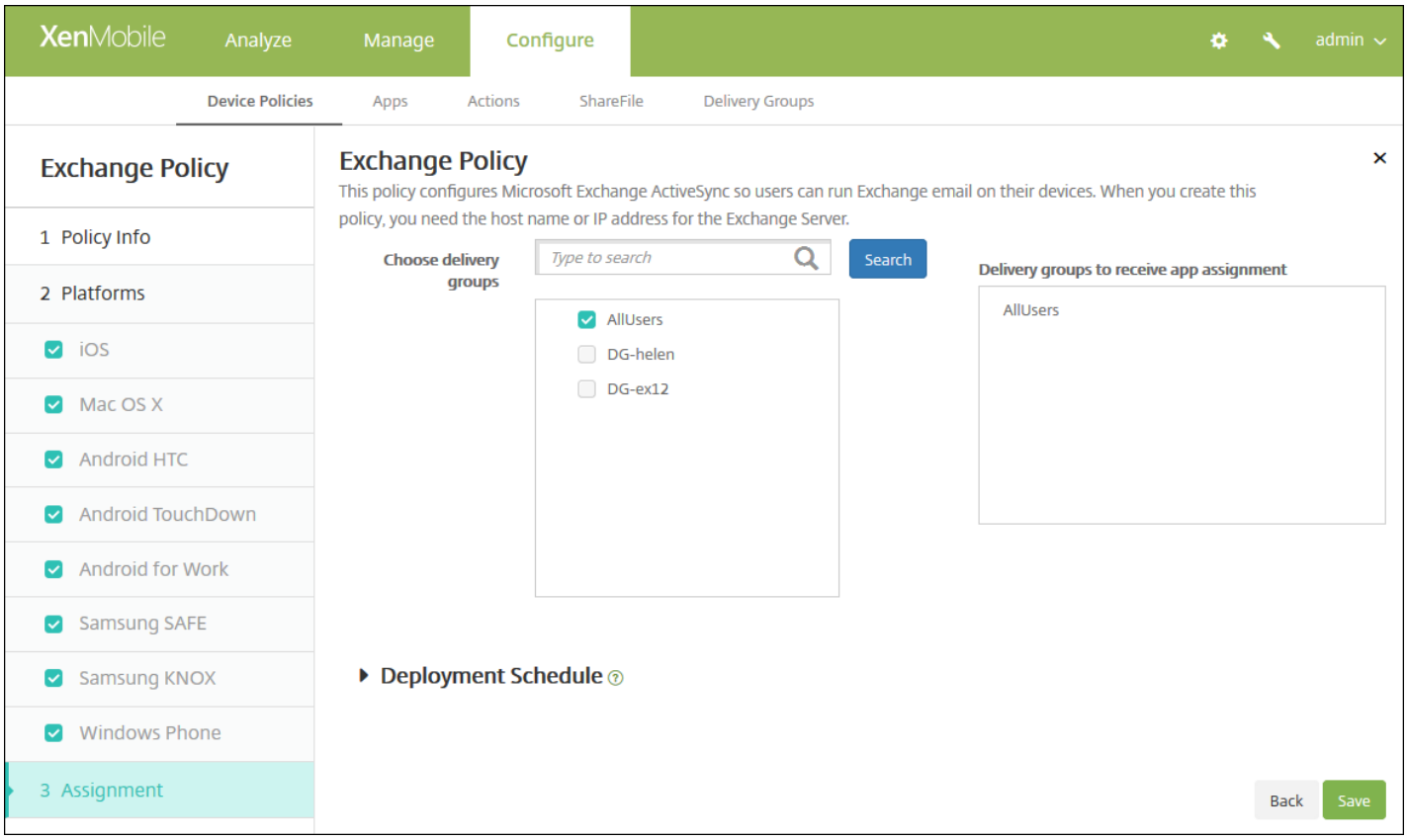
Configure these settings:

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

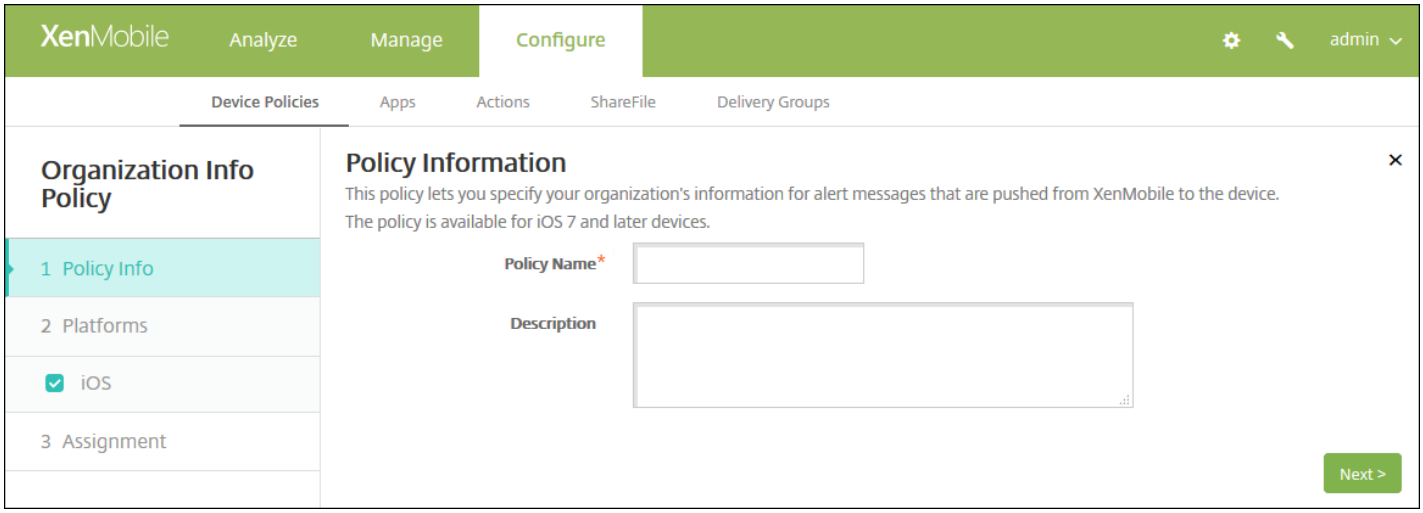
Feb 13, 2015

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.

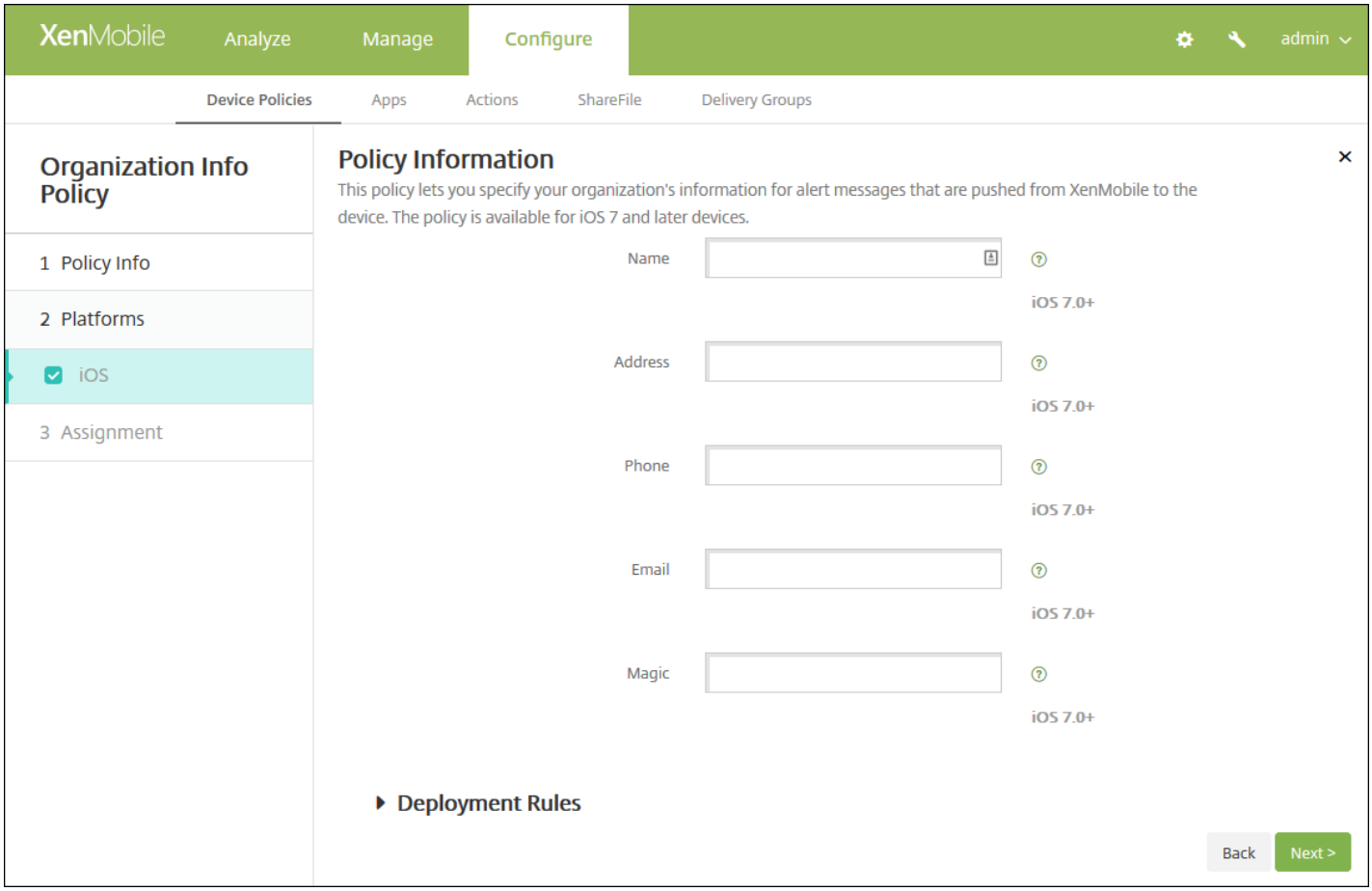
3. Click **More** and then, under **End user**, click **Organization info**. The **Organization Info Policy** page appears.



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.

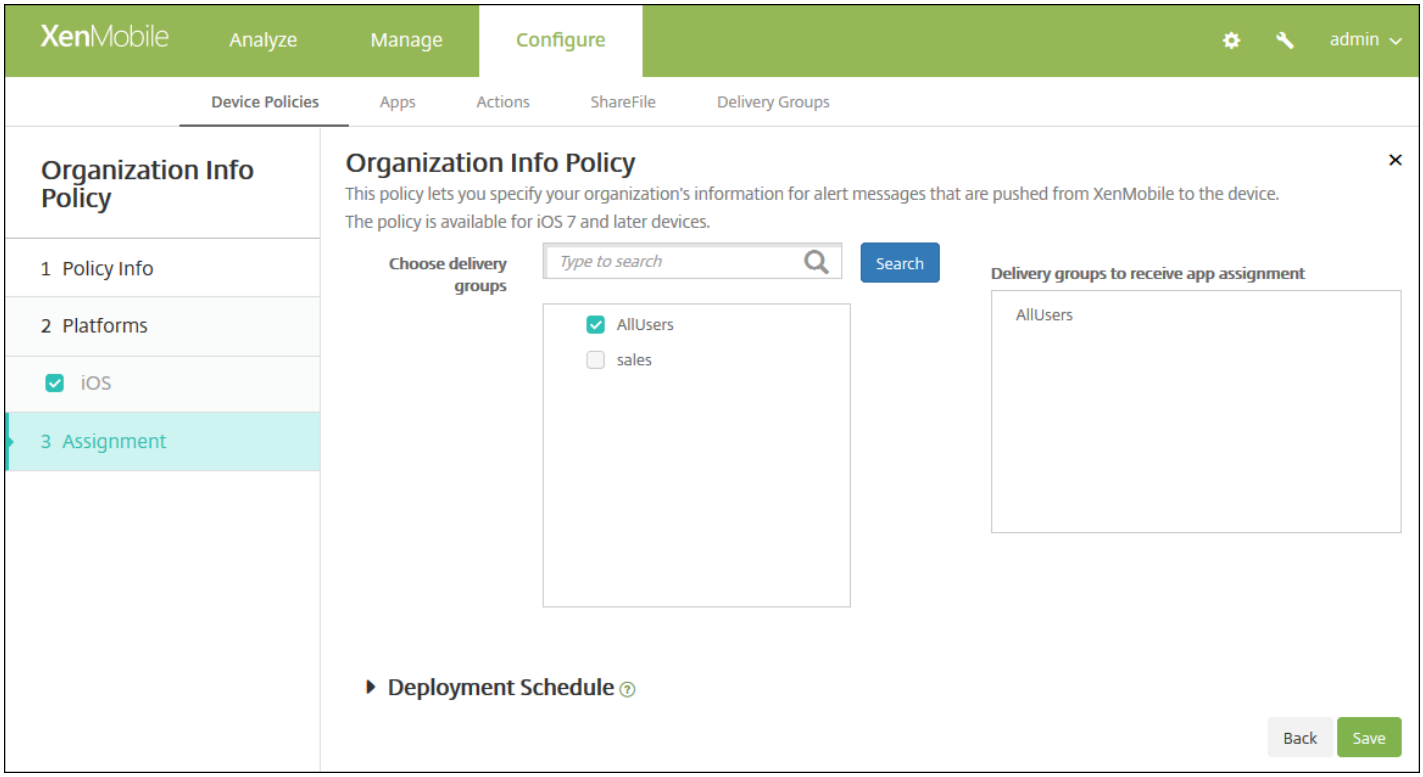


Configure these settings:

- **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.

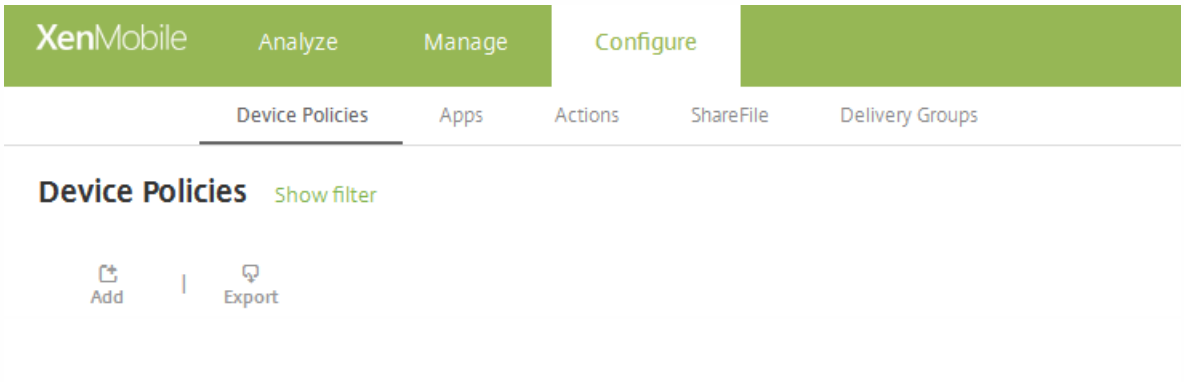
11. Click **Save**.

Passcode device policies

Mar 31, 2016

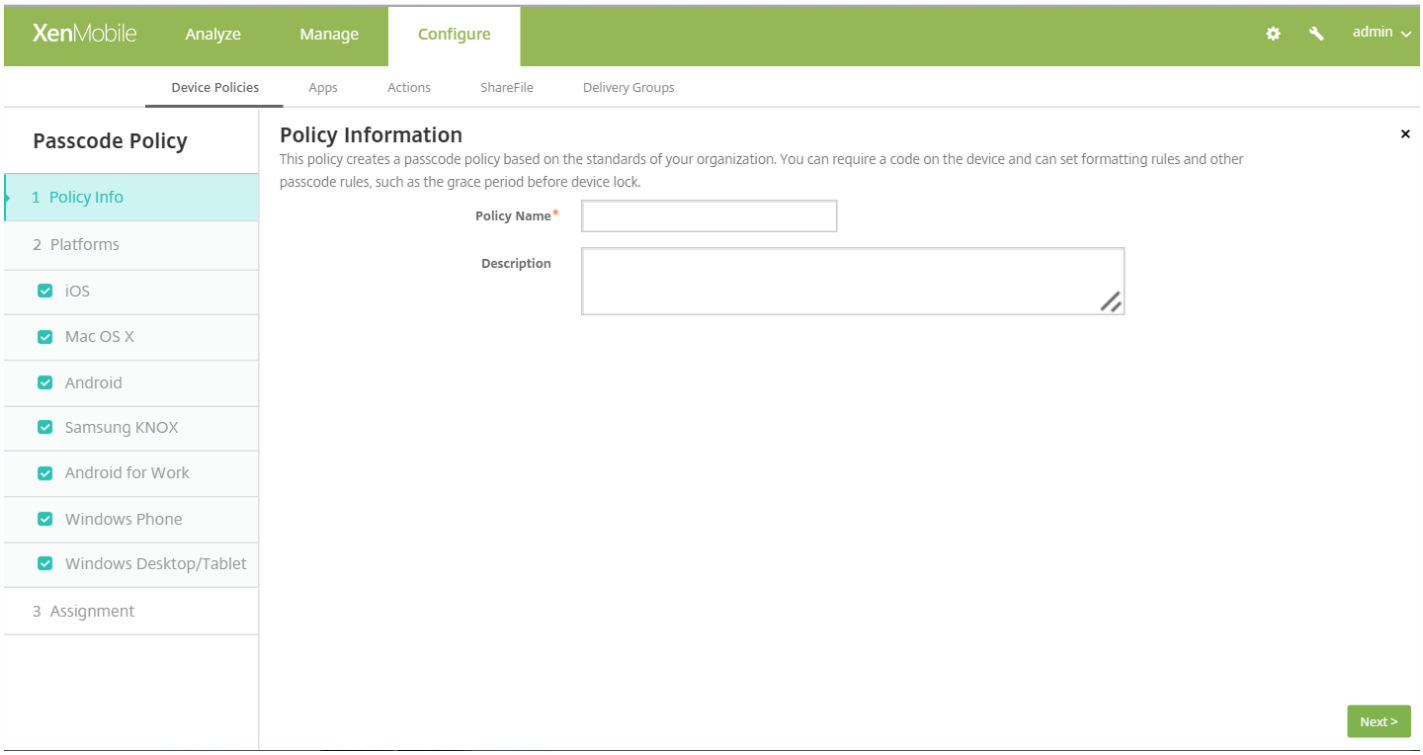
You create a passcode policy in XenMobile based on your organization's standards. You can require passcodes on users' devices and can set various formatting and passcode rules. You can create policies for iOS, Mac OS X, Android, Samsung KNOX, Android for Work, Windows Phone, and Windows desktop/tablet. 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:

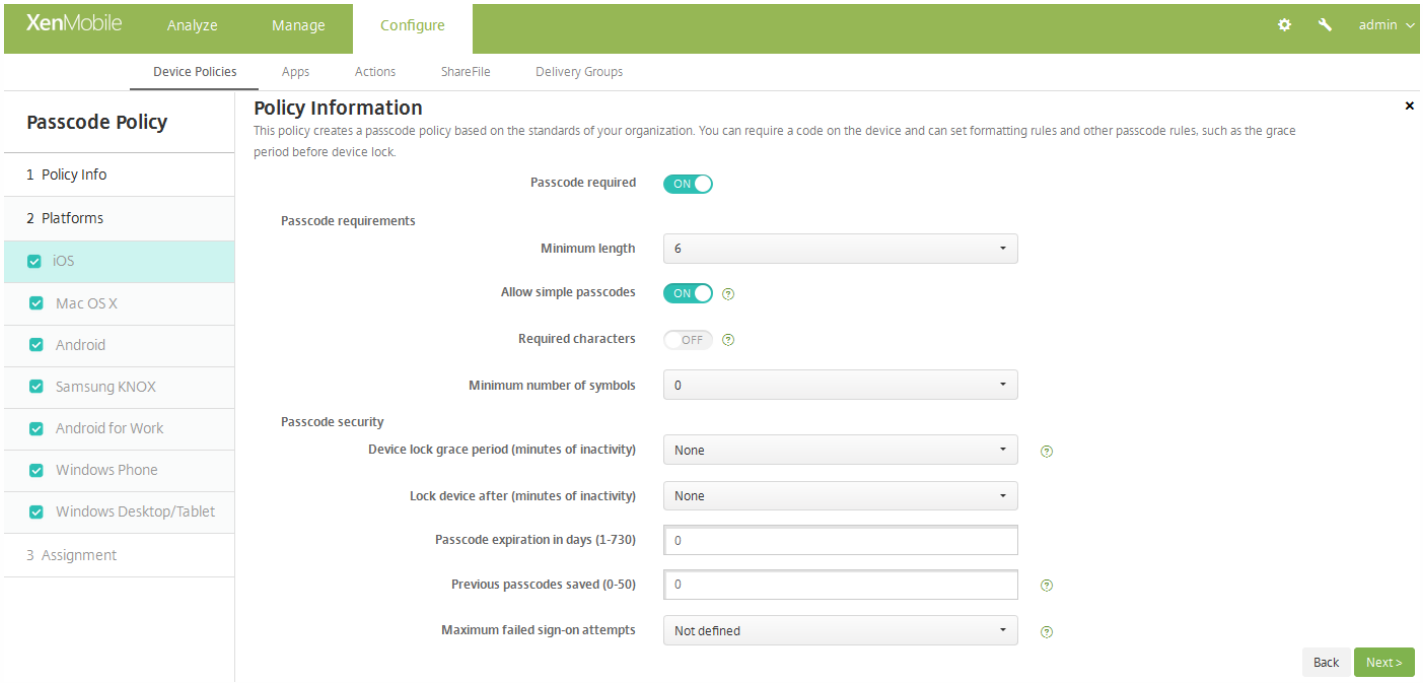
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

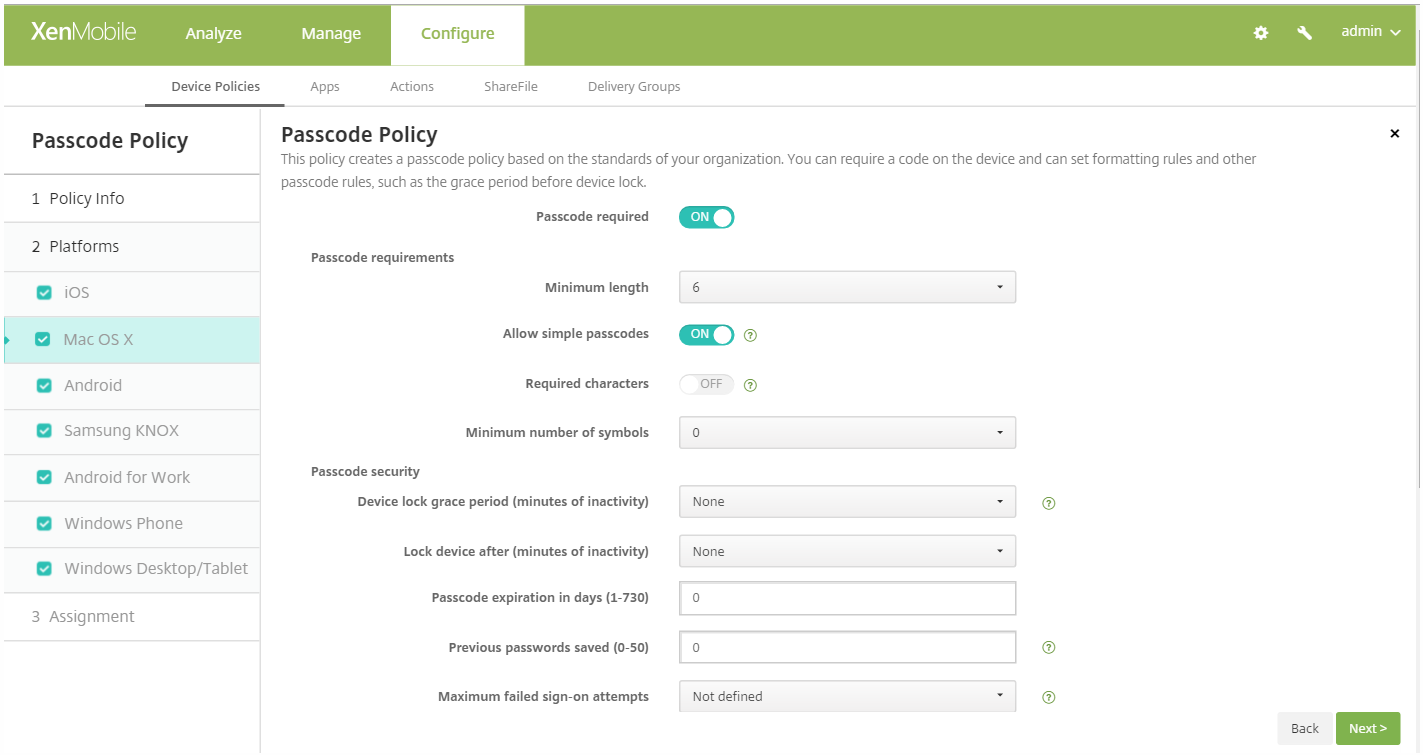
Configure iOS settings



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



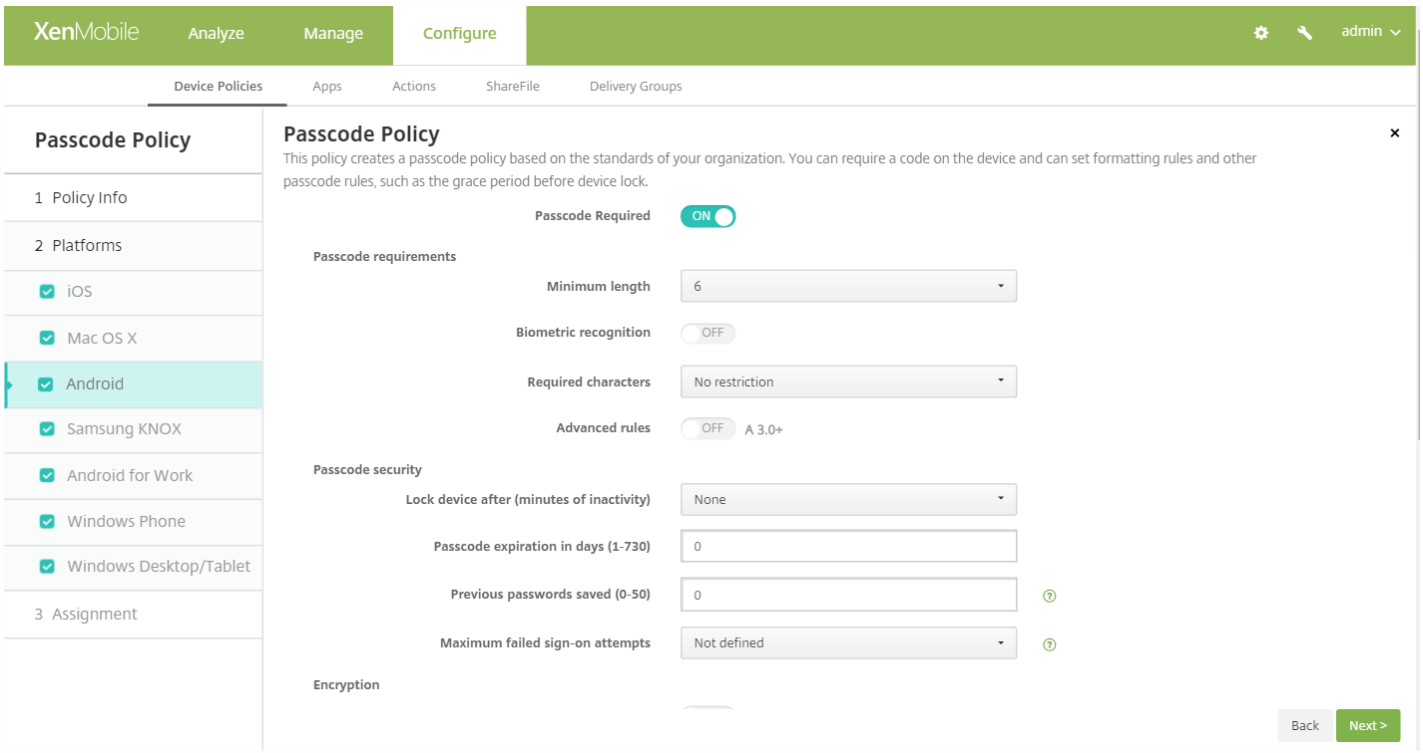
Configure these settings:

- **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.

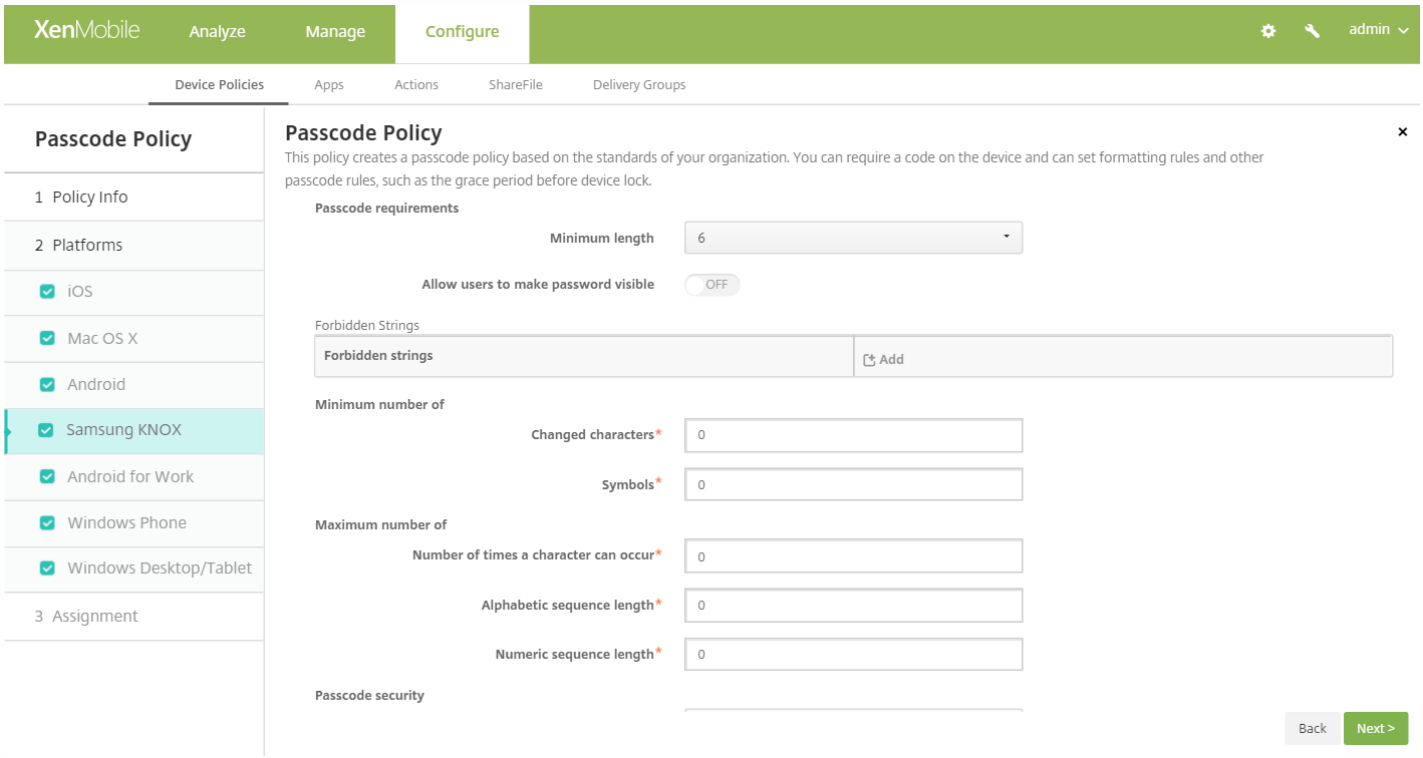
- **Samsung SAFE**
  - **Use same passcode across all users**: Select whether to use the same passcode for all users. The default is **OFF**. This setting applies only to Samsung SAFE devices and is available regardless of the **Passcode required** setting.
  - When you enable **Use same passcode across 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:

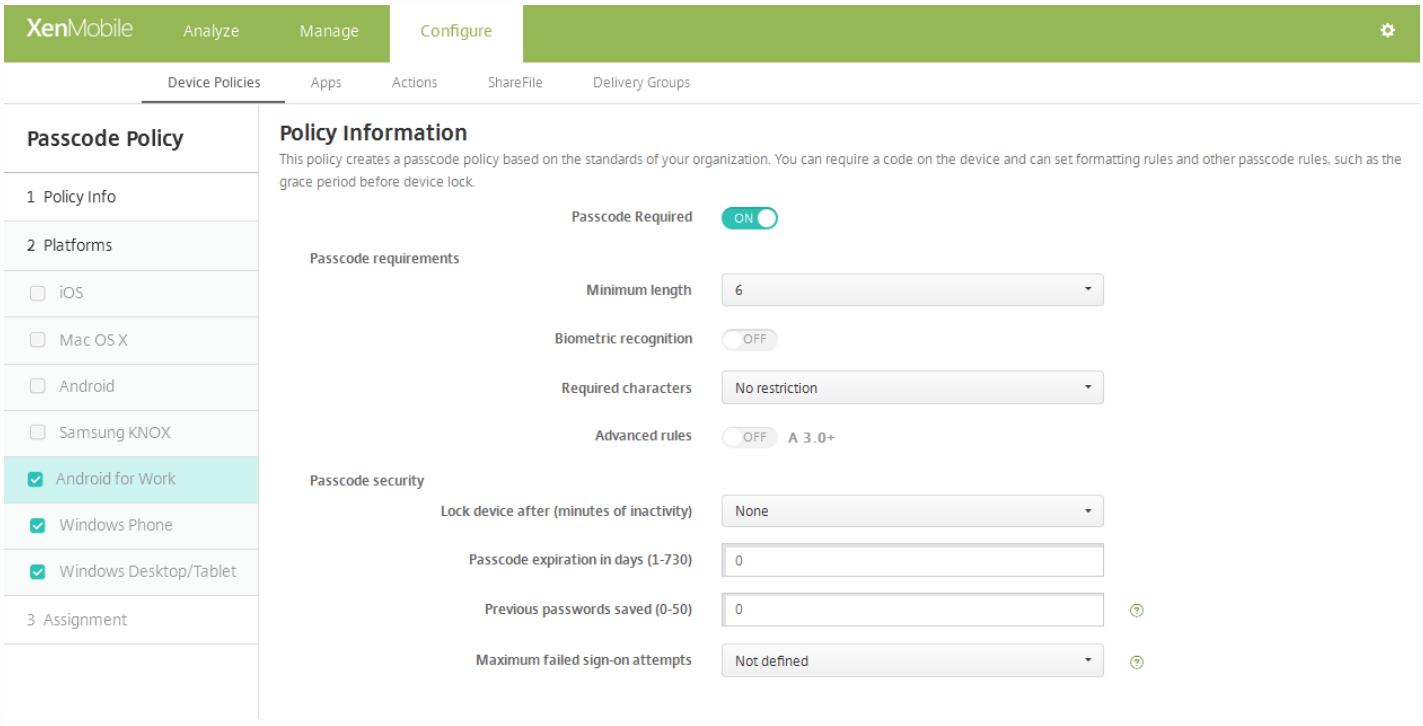
- **Passcode requirements**
  - **Minimum length**: In the list, click the minimum passcode length. The default is **6**.
  - **Allow users to make password visible**: Select whether to let users make the password visible.
  - **Forbidden strings**: You create forbidden strings to prevent users from 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



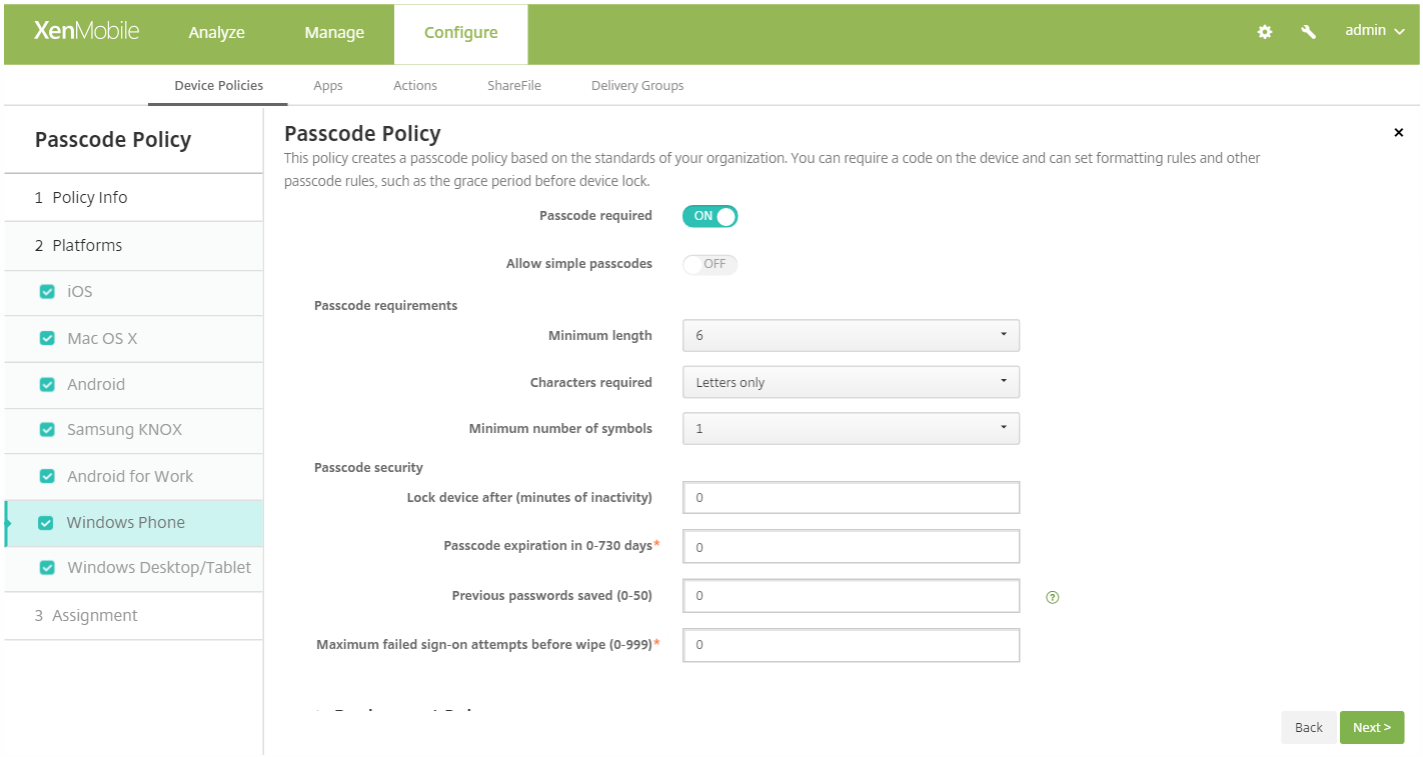
Configure these settings:

- **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**.

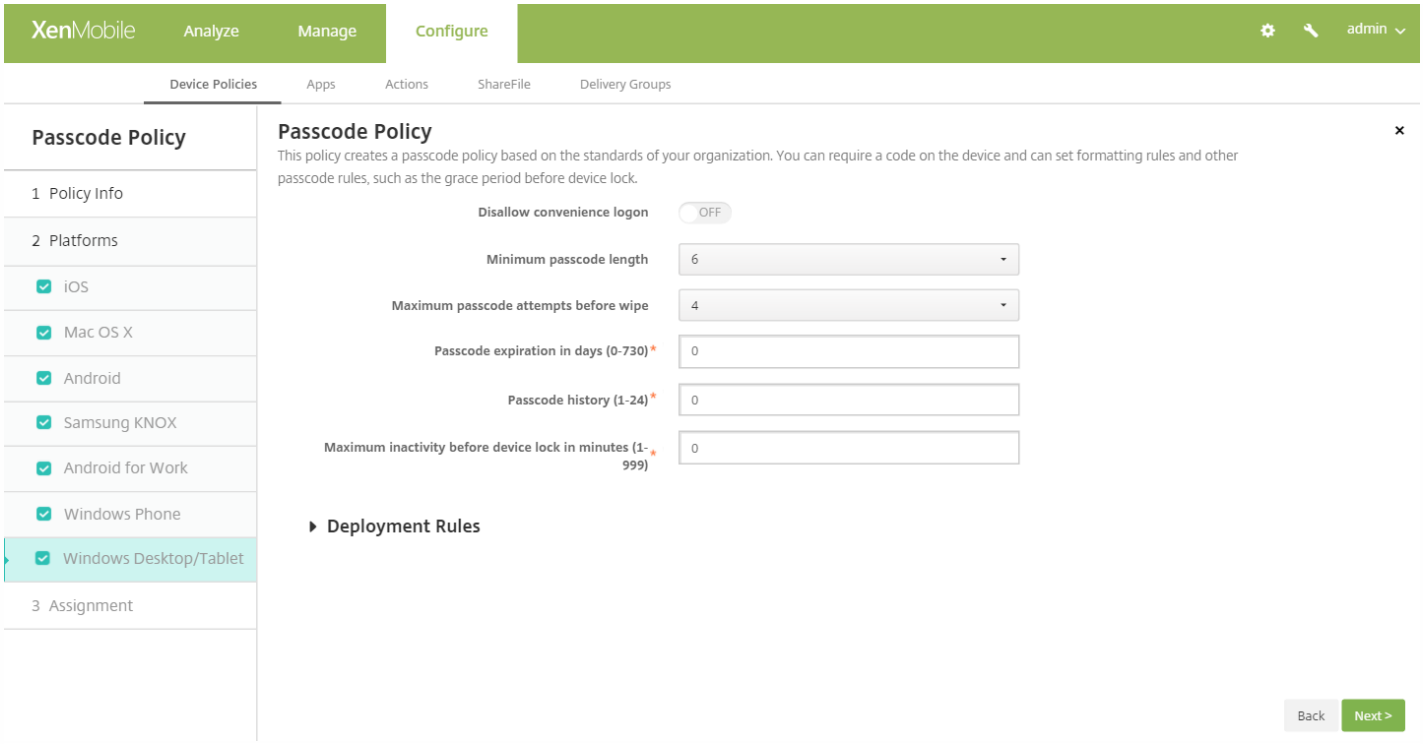
Configure Windows Phone settings



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

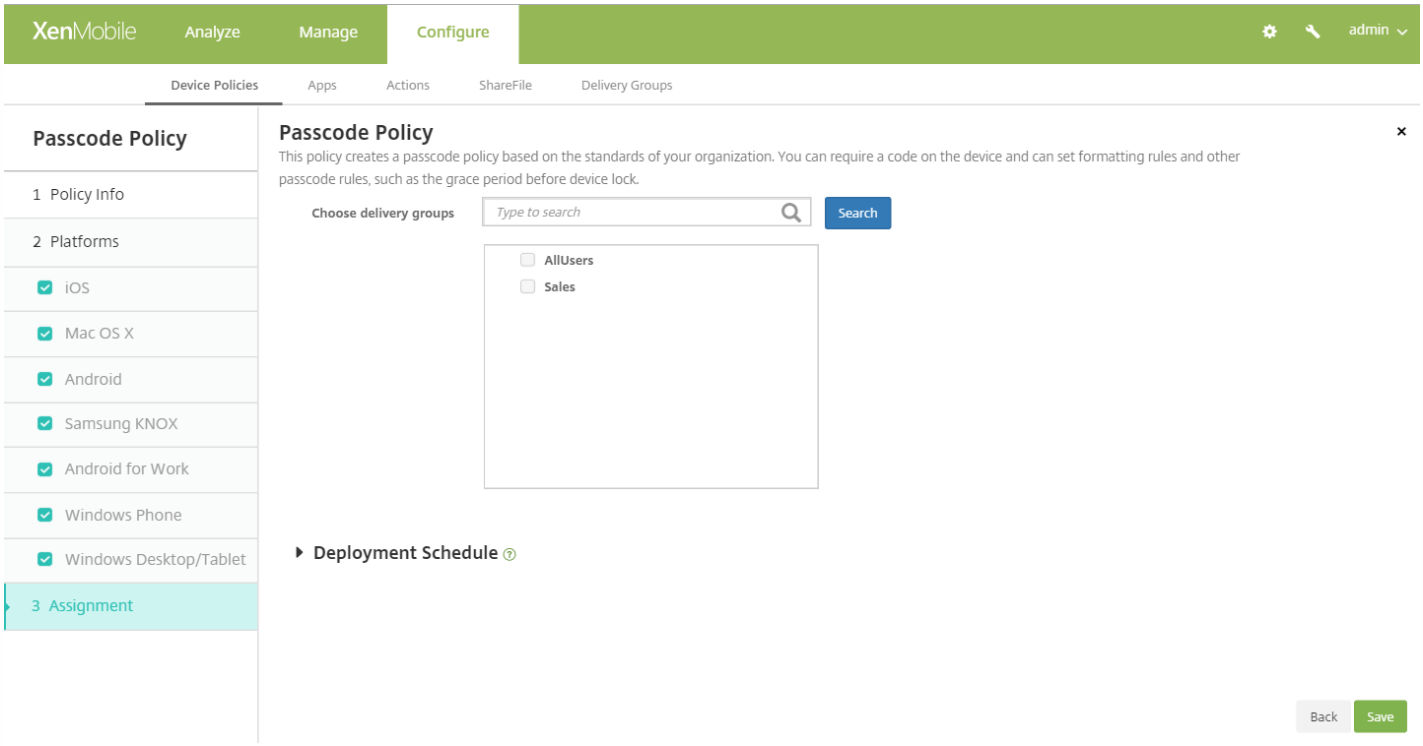


Configure these settings:

- **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

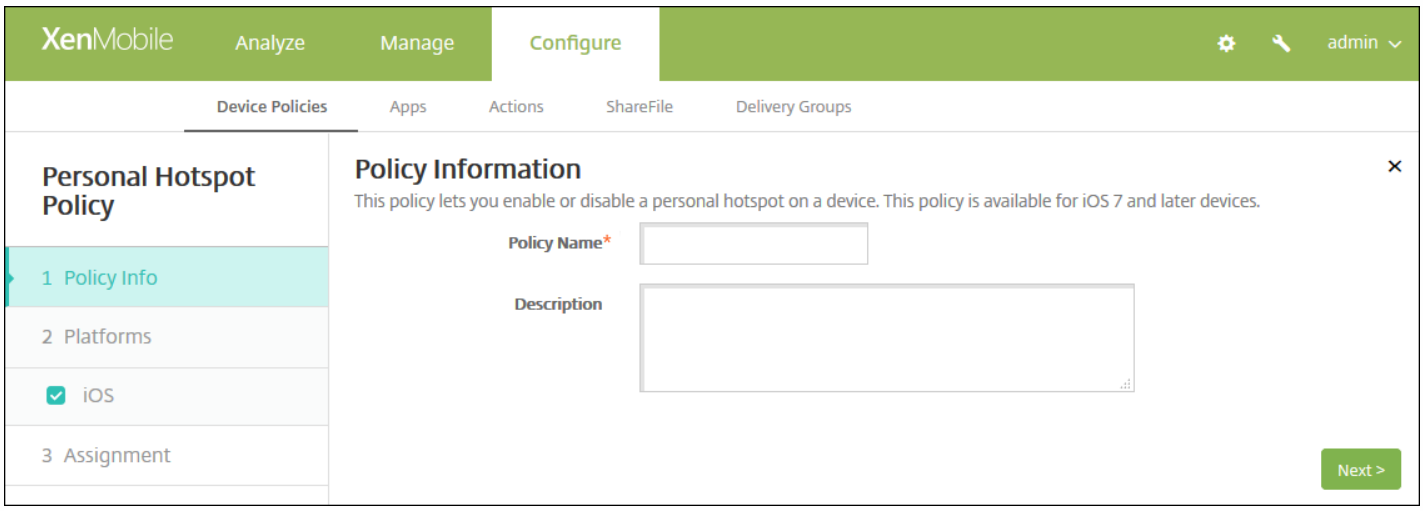
Sep 24, 2015

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.

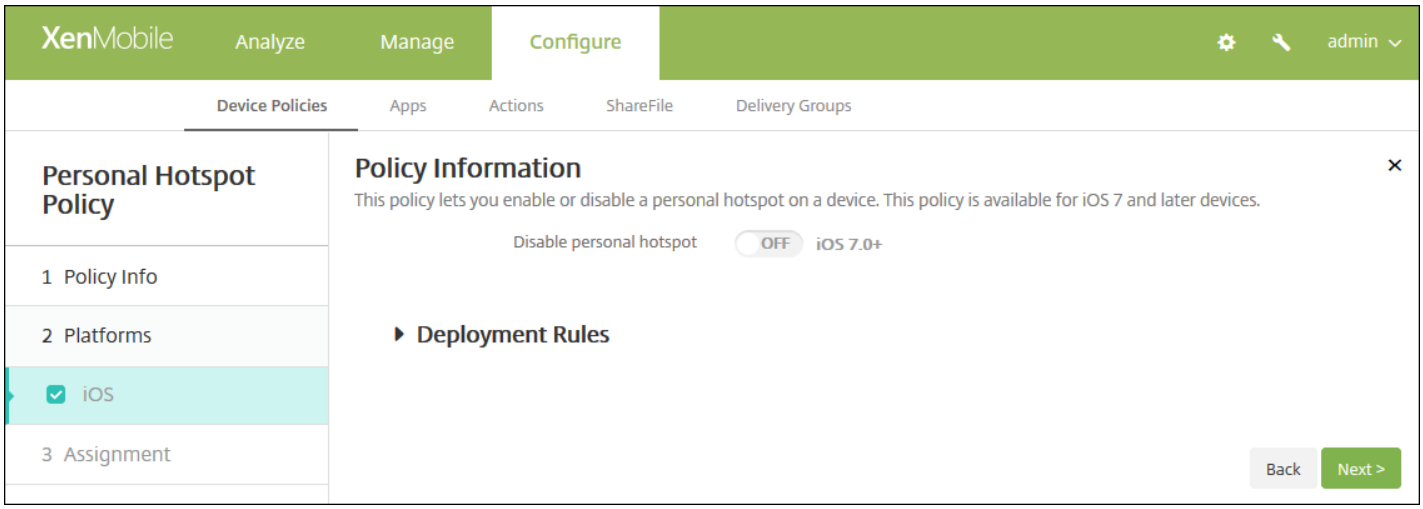
3. Expand **More**, and then under **Network Access**, click **Personal Hotspot**. The **Personal Hotspot Policy** information page appears.



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.

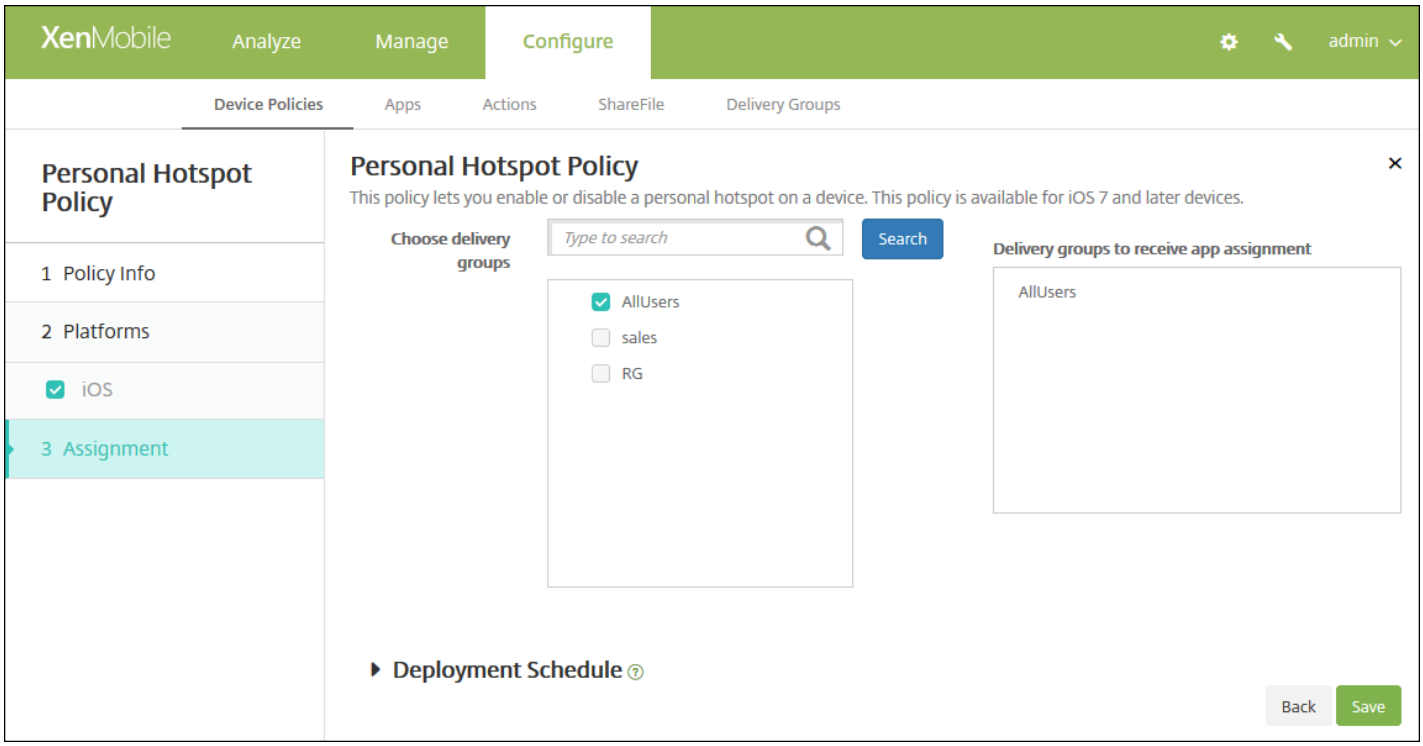


6. Configure this setting:

- **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 policies

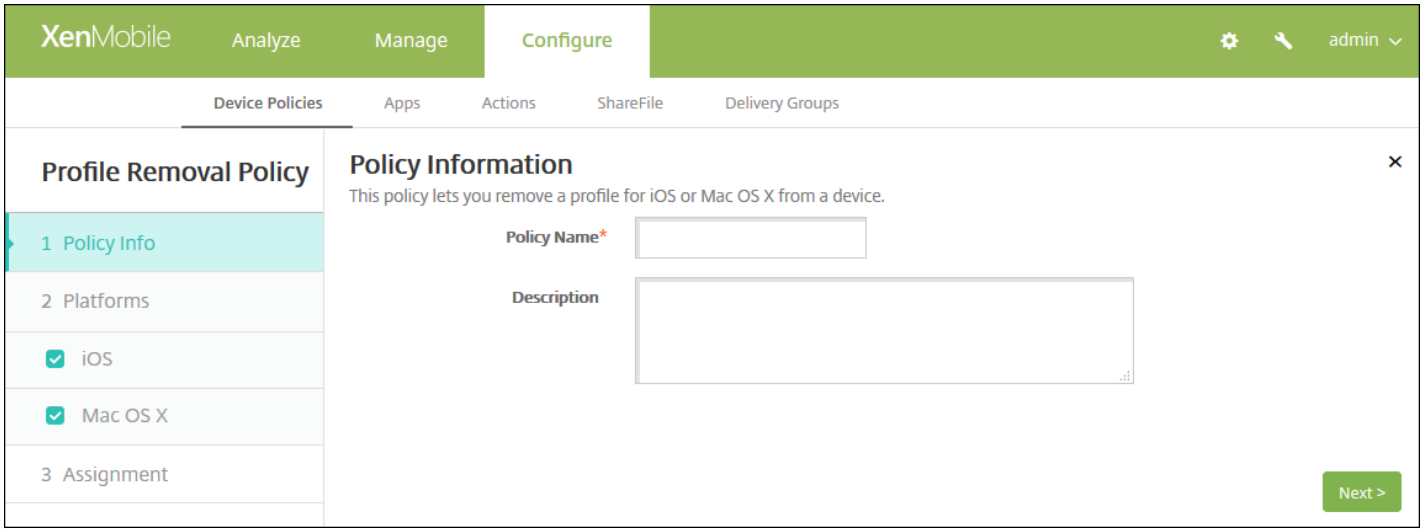
Oct 06, 2015

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:

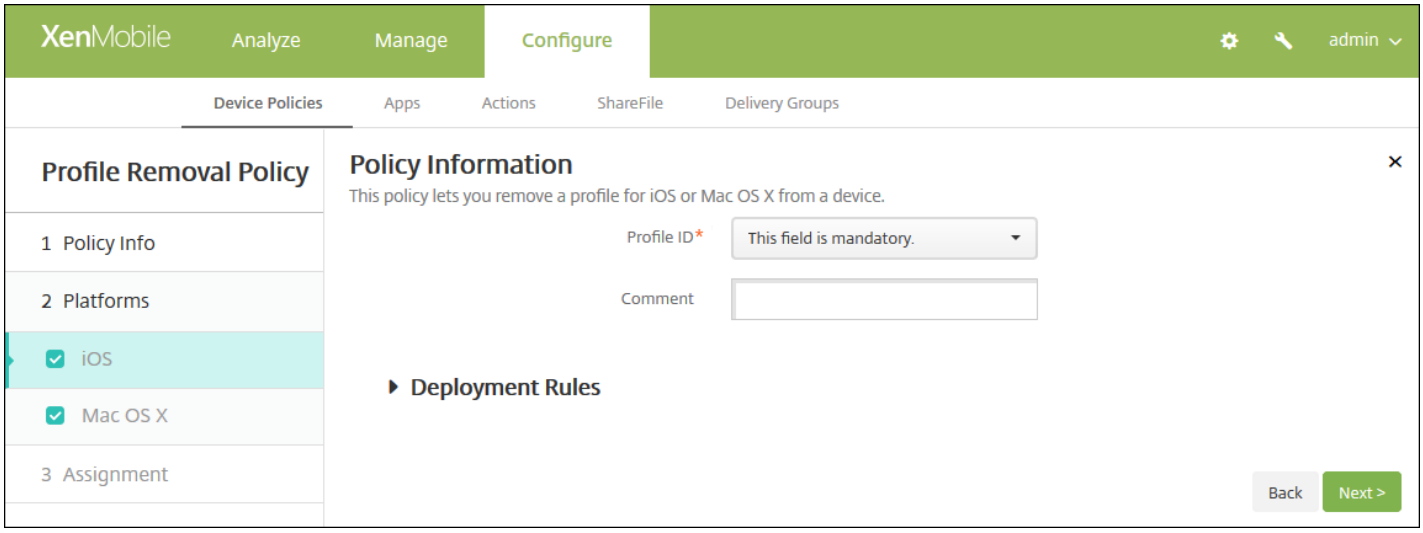
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

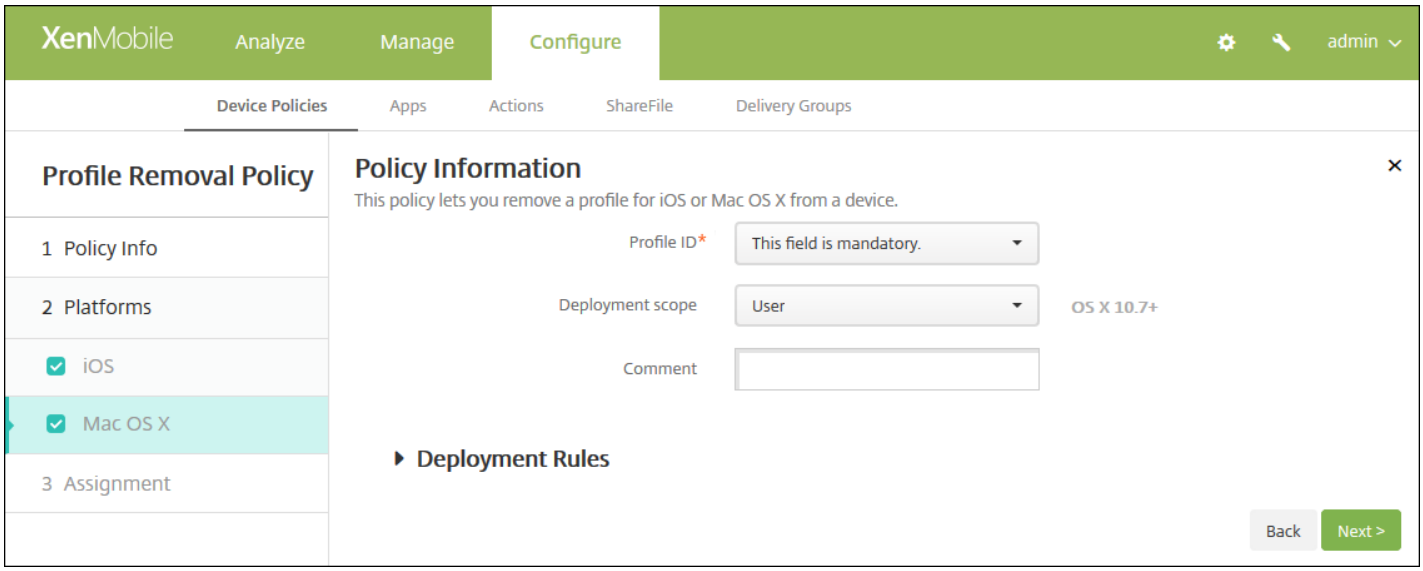
Configure iOS setting



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

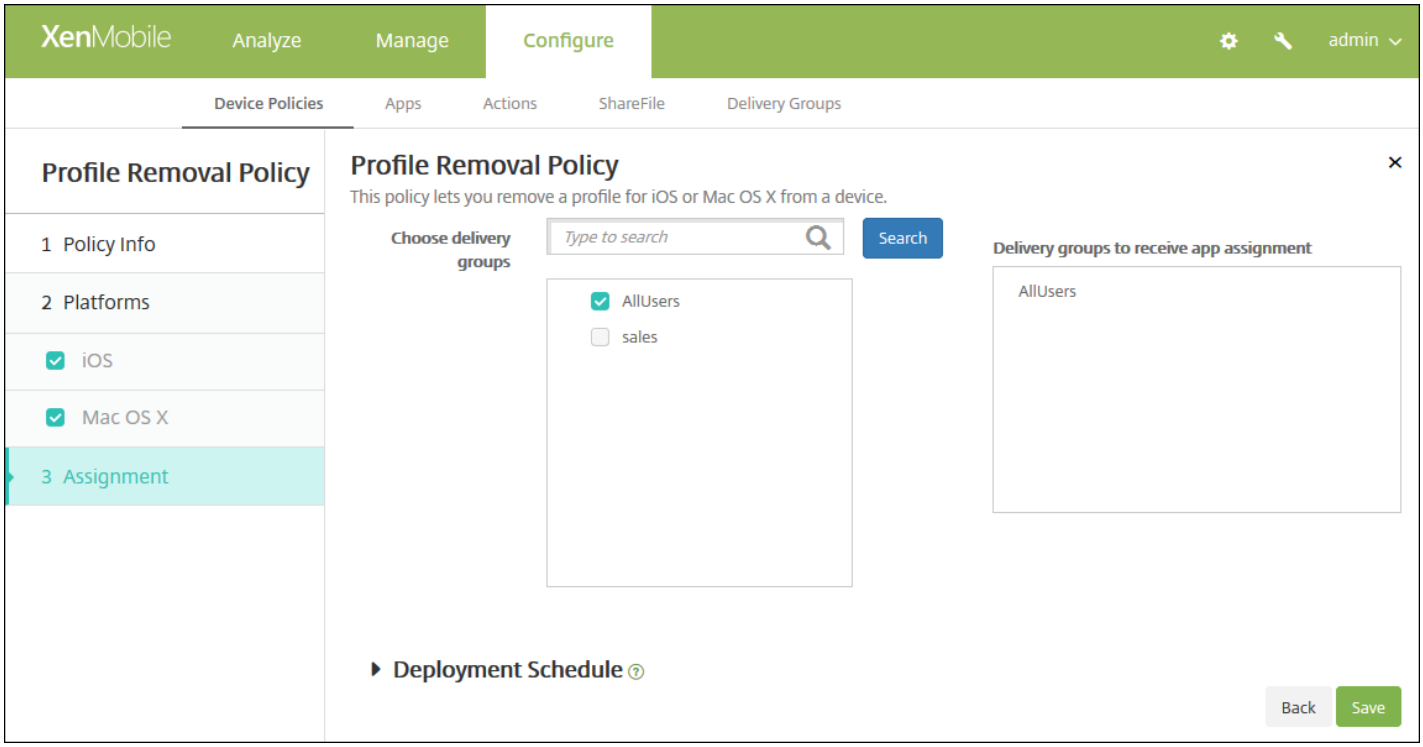


Configure these settings:

- **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

Aug 10, 2015

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.

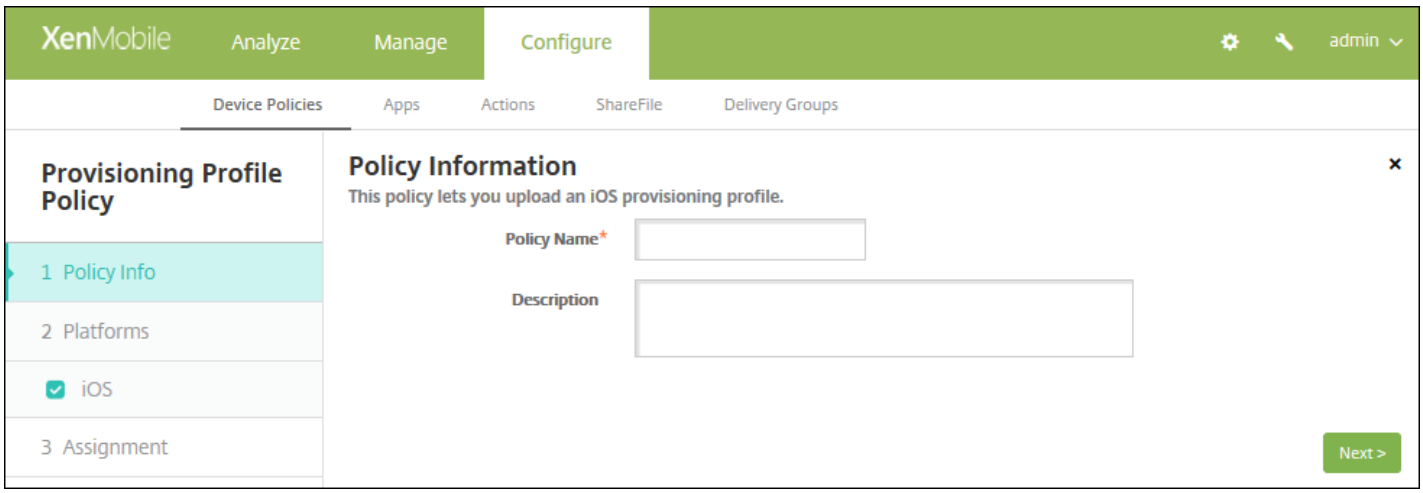
To make this process transparent to users, in XenMobile you can install and remove provisioning profiles with device policies. Missing or expired profiles are removed as necessary and the up-to-date profiles are installed on users' devices, so that tapping an app simply opens it for use.

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.

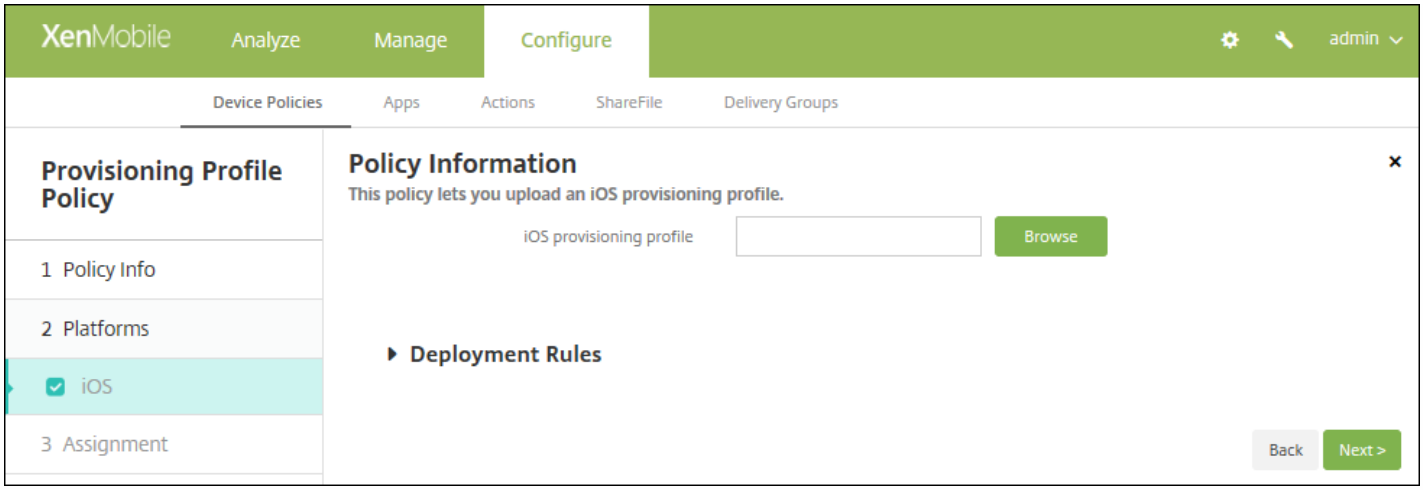
3. Expand **More** and then, under **Apps**, click **Provisioning Profile**. The **Provisioning Profile Policy** information page appears.



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.

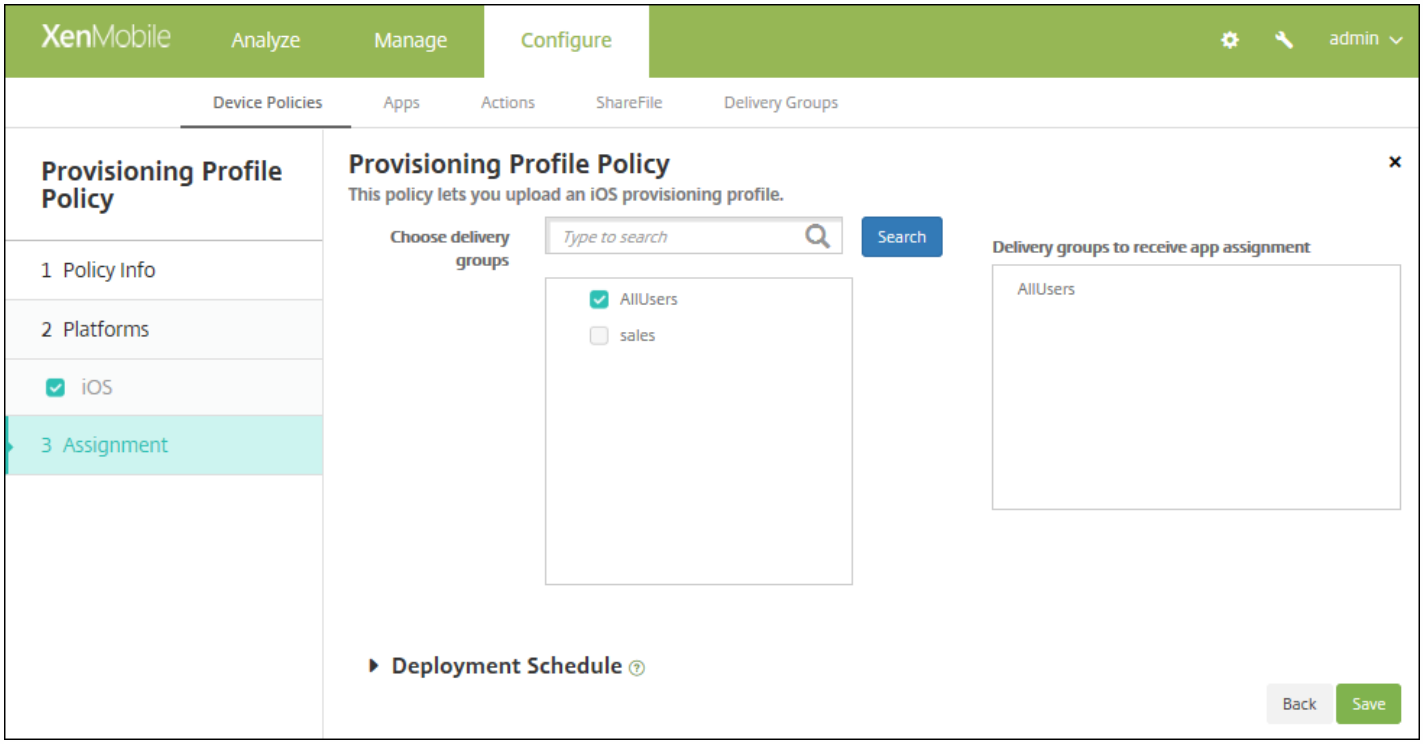


6. Configure this setiing:

- **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

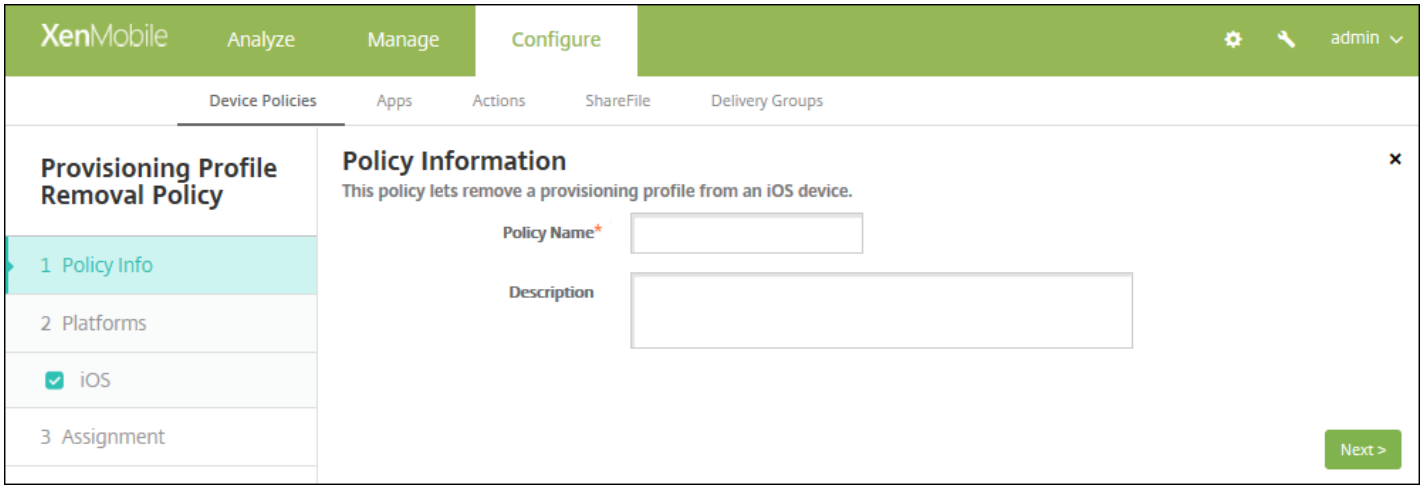
Aug 10, 2015

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.

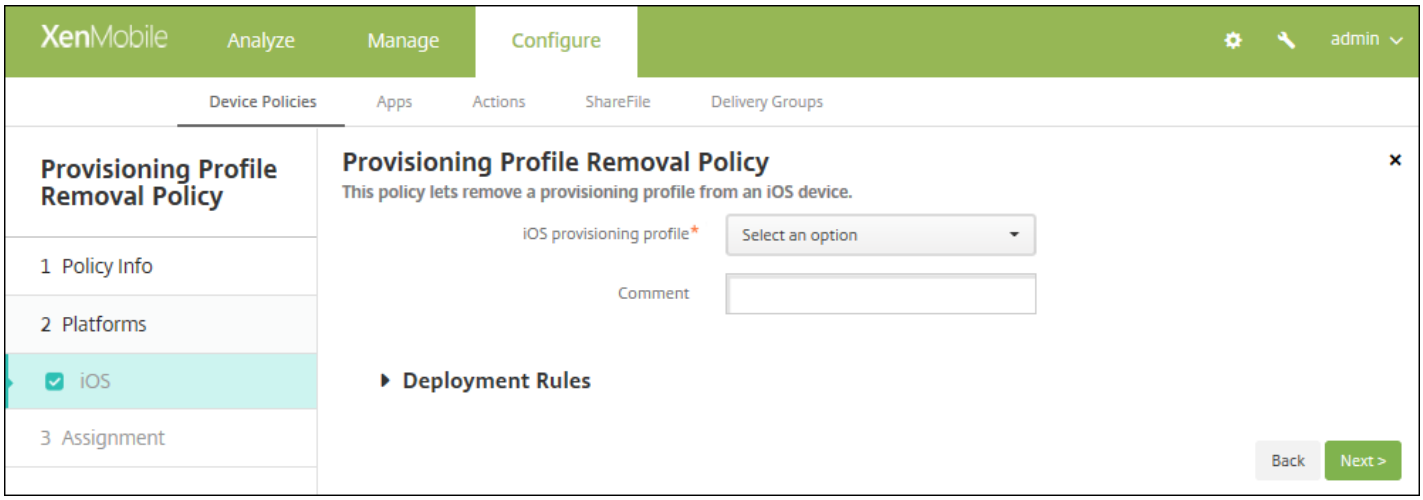
3. Expand **More** and then, under **Removal**, click **Provisioning Profile removal**. The **Provisioning Profile Removal Policy** information page appears.



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.

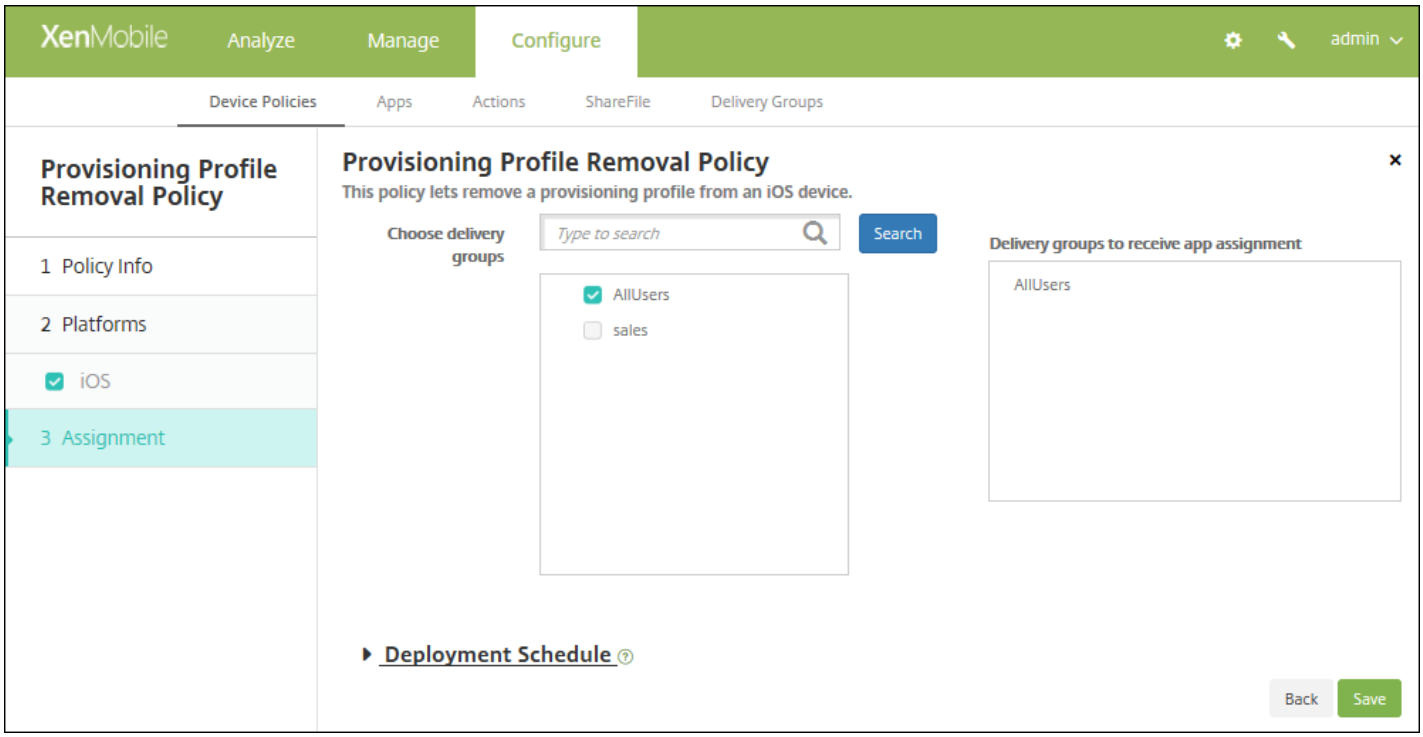


6. Configure these settings:

- **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 policies

Mar 03, 2015

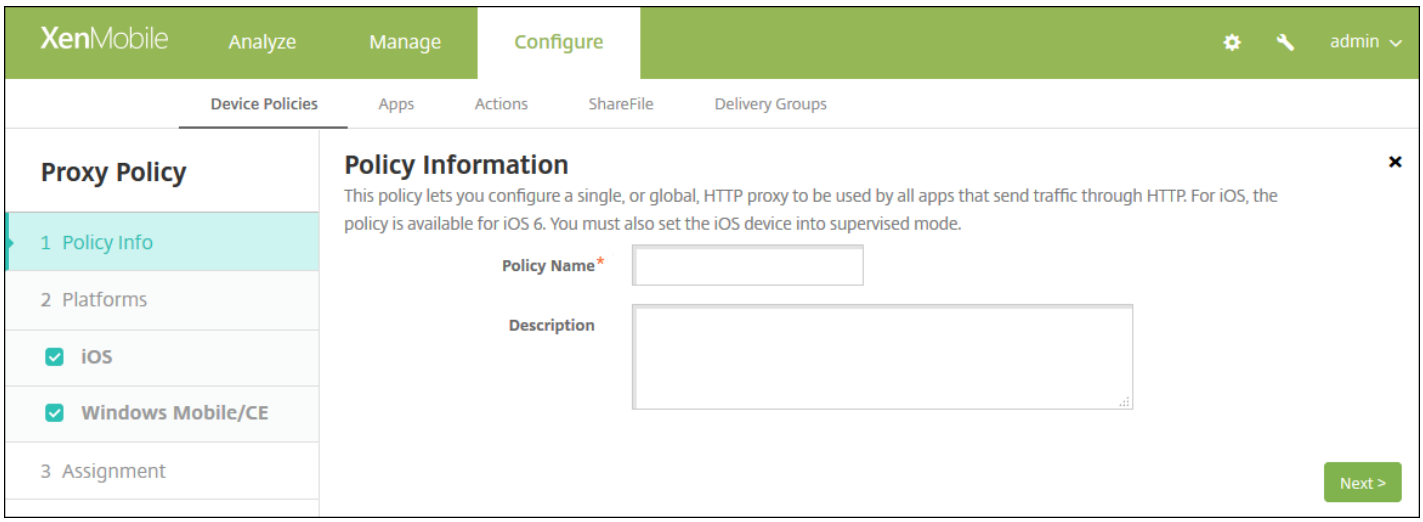
You can add a device policy in XenMobile to specify global HTTP proxy settings for devices running Windows Mobile/CE andiOS 6.0 or later. You can deploy only one global HTTP proxy policy per device.

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:

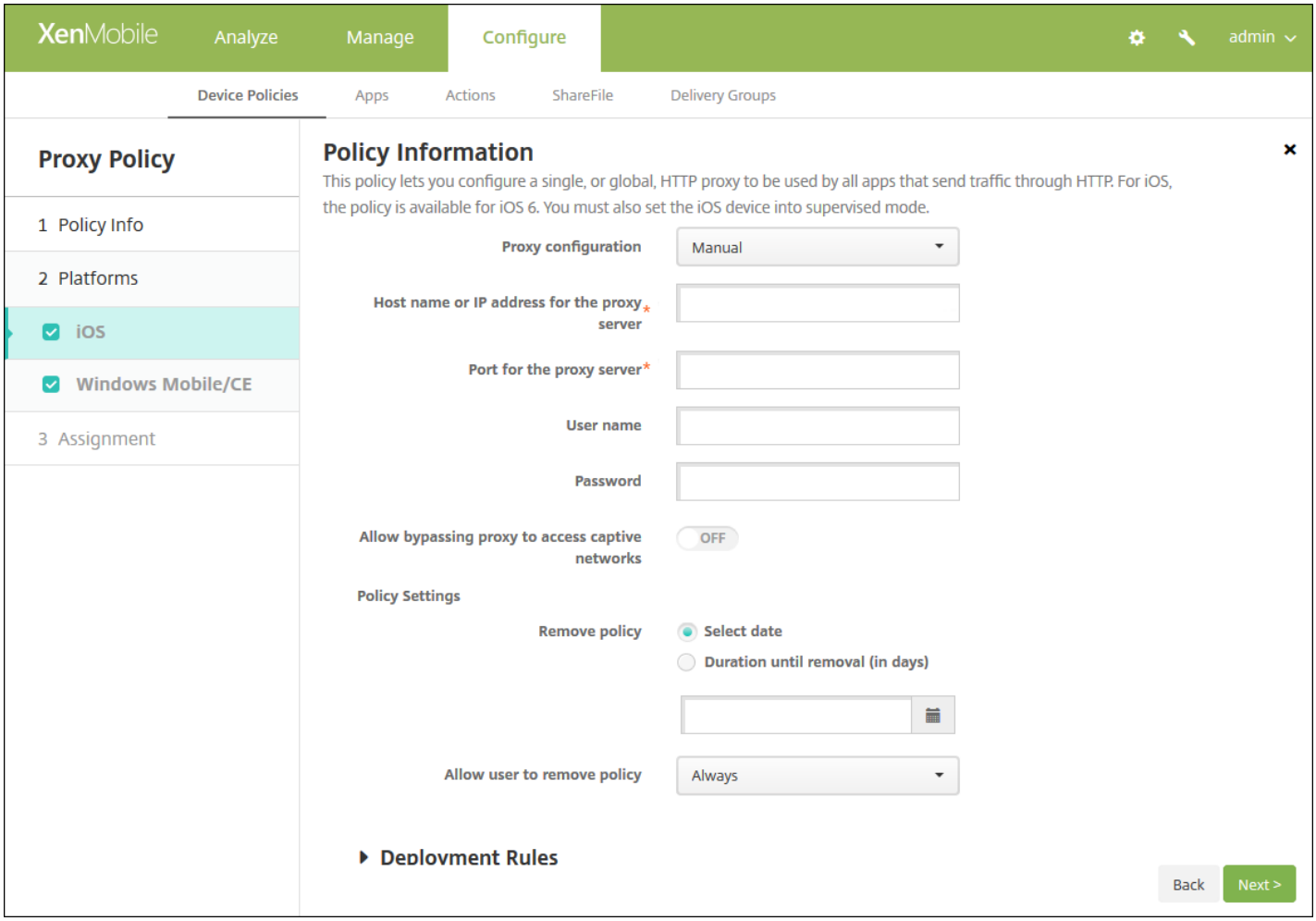
- **Policy Name**: Enter a descriptive name for the policy.
- **Description**: Optionally, enter a description of the policy.

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.

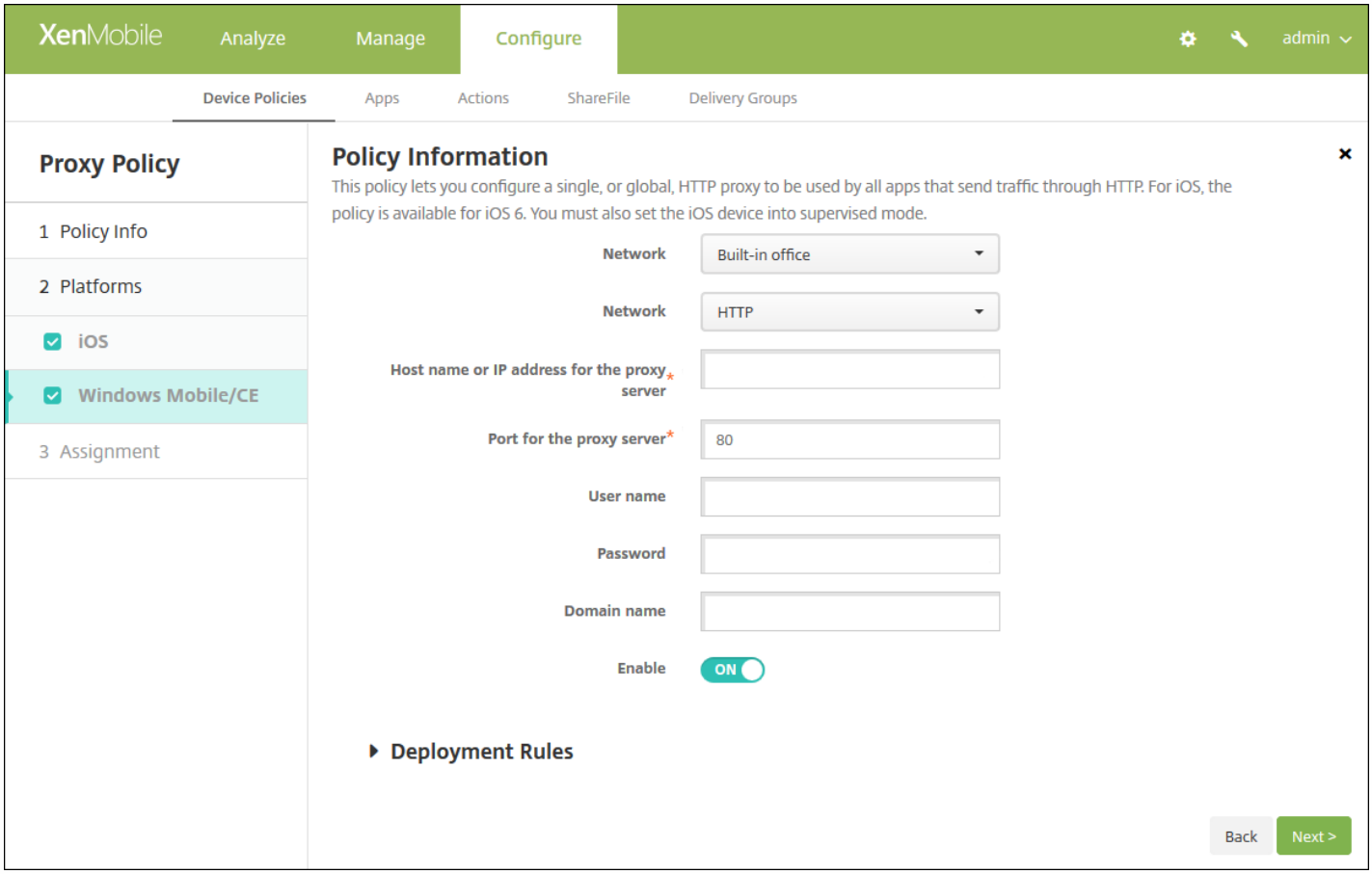
Configure iOS settings



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

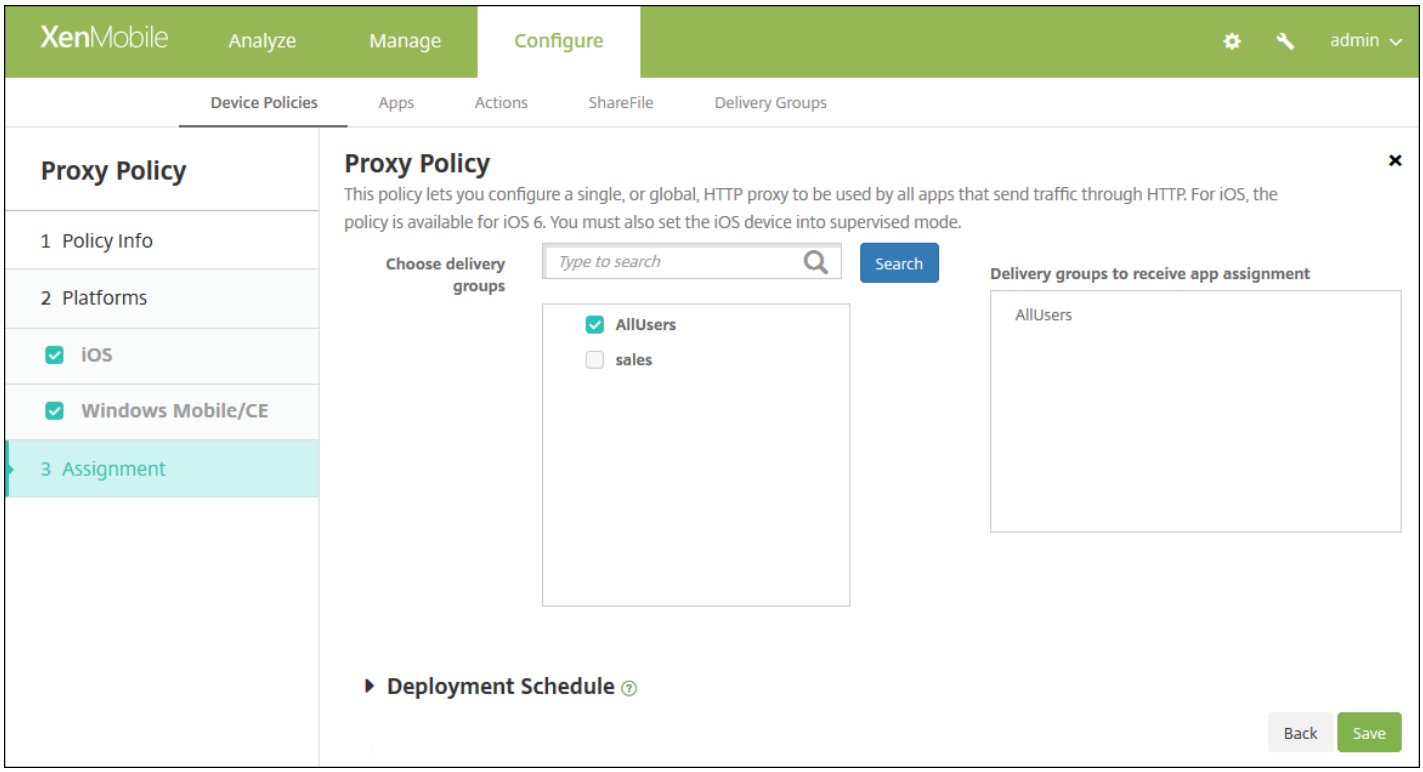


Configure these settings:

- **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

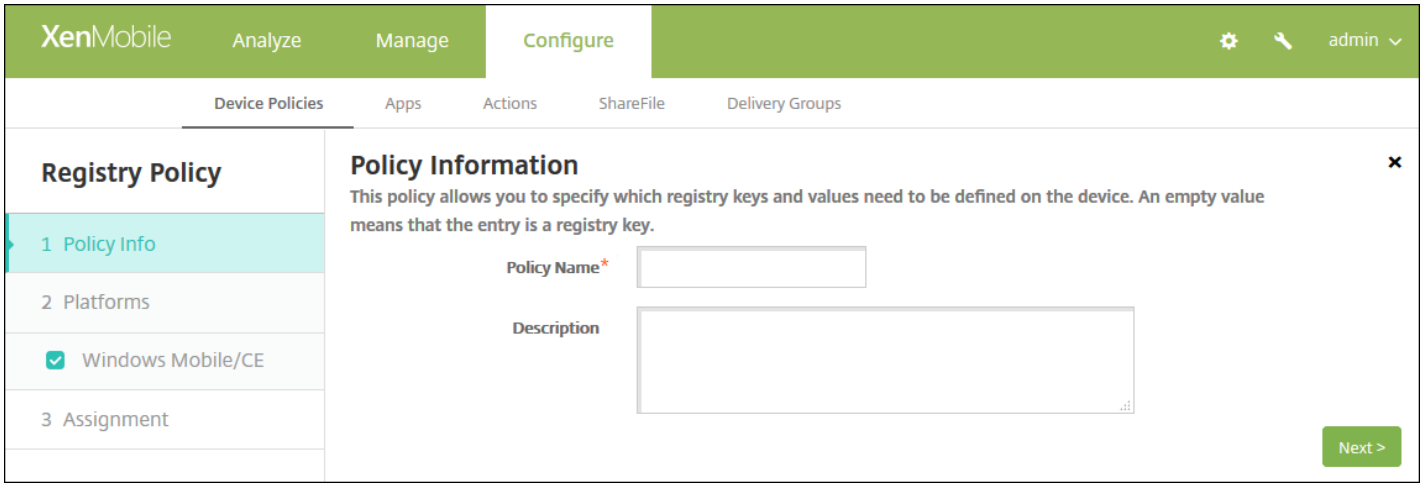
Oct 20, 2015

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.

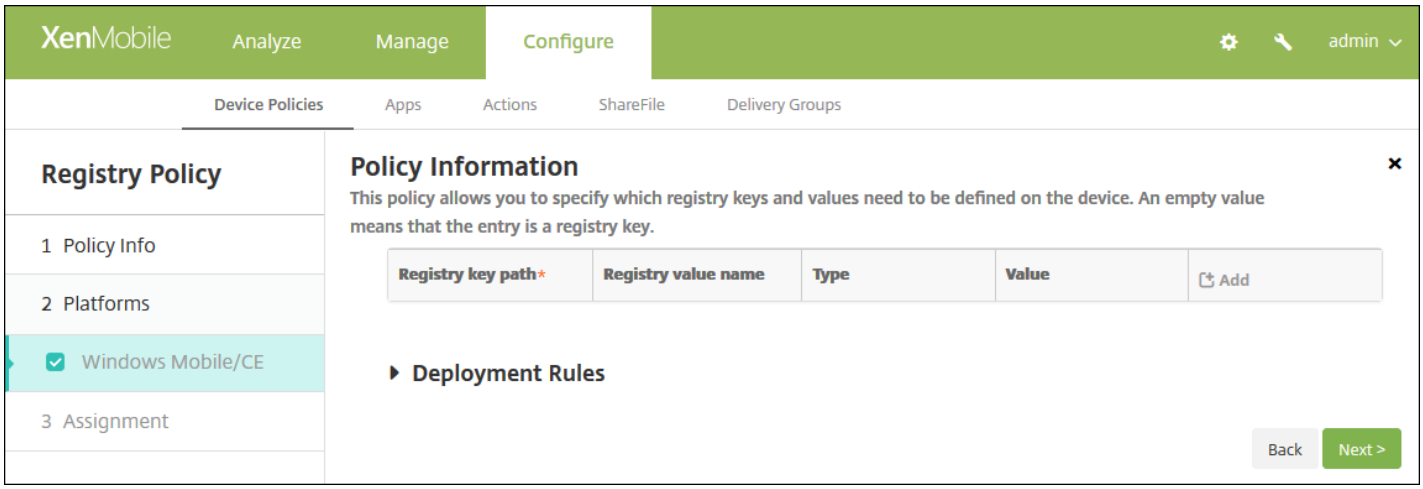
3. Expand **More** and then, under **Custom**, click **Registry**. The **Registry Policy** information page appears.



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:

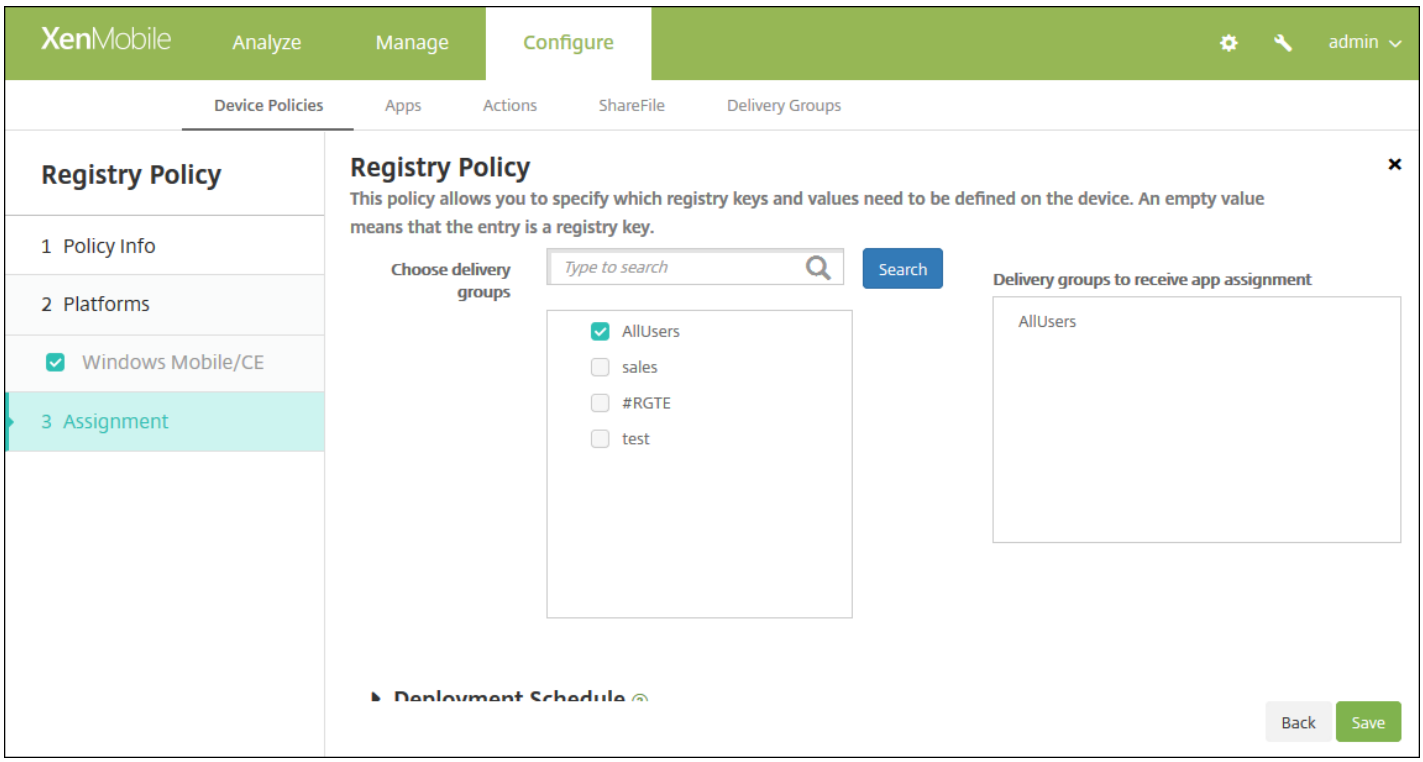
- For each registry key or registry key/value pair you want to add, click **Add** and do the following:
- **Registry key path**: Type the full path for the registry key. For example, type *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows* to specify the route to the Windows key from the HKEY_LOCAL_MACHINE 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

Feb 13, 2015

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.

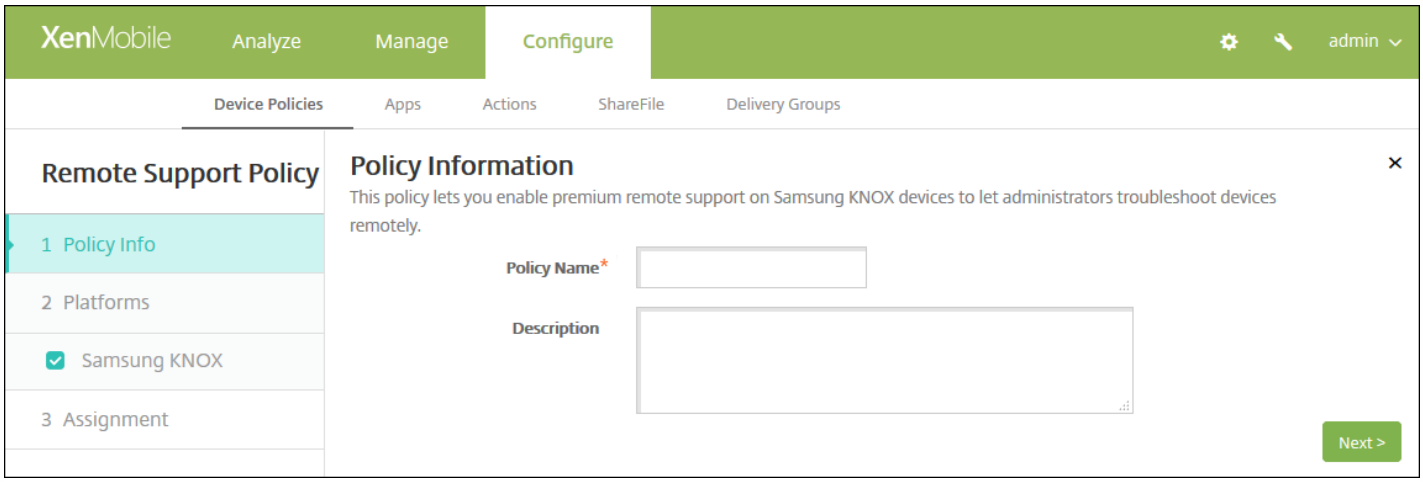
Note: To implement this policy, you must do the following:

- 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.

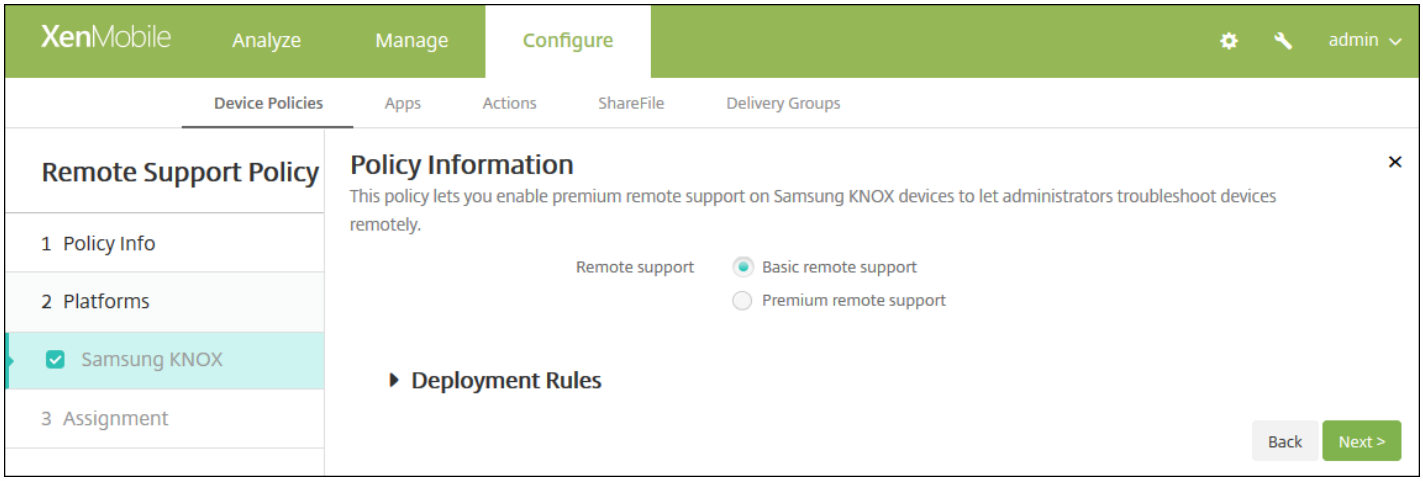
3. Expand **More** and then, under **Network access**, click **Remote Support**. The **Remote Support Policy** page appears.



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.

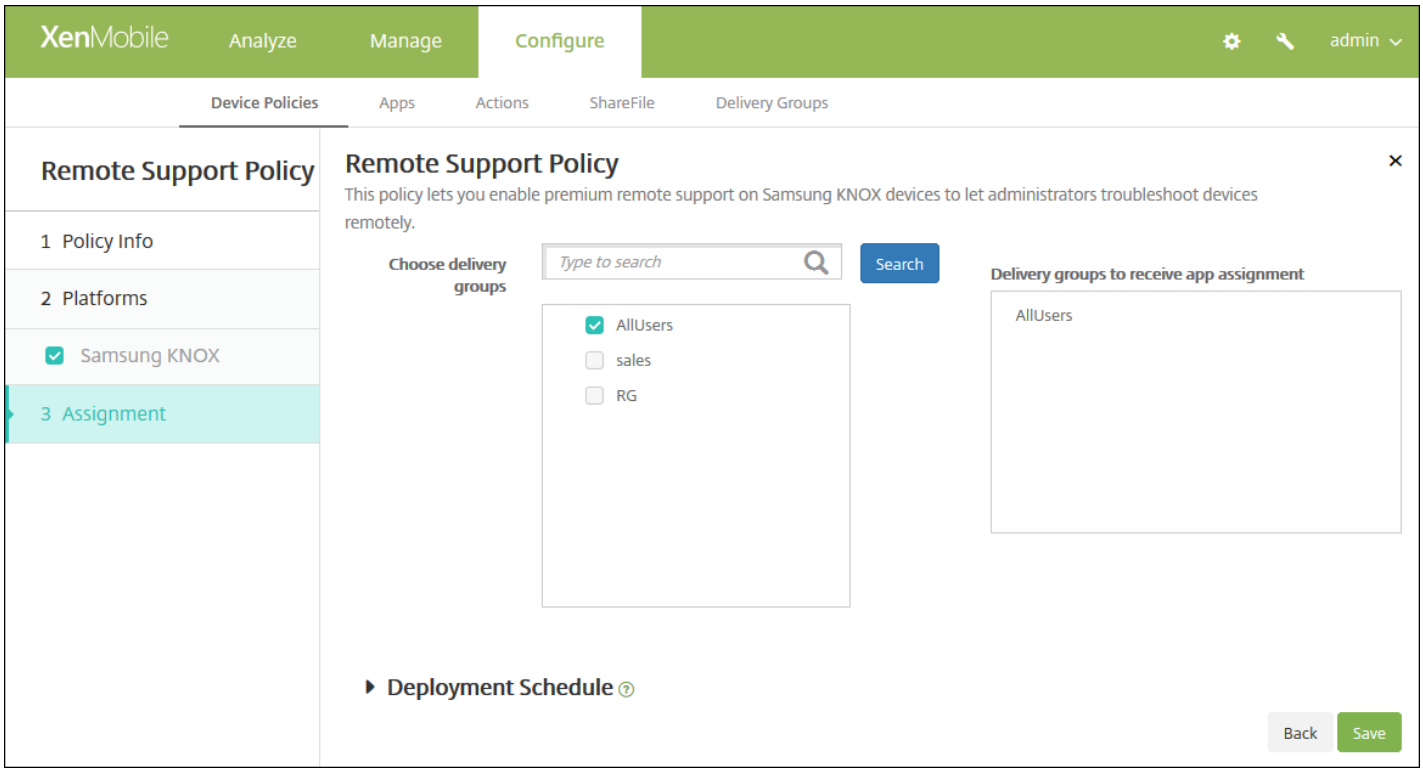


6. Configure this setting:

- **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 policies

Jul 12, 2016

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*.

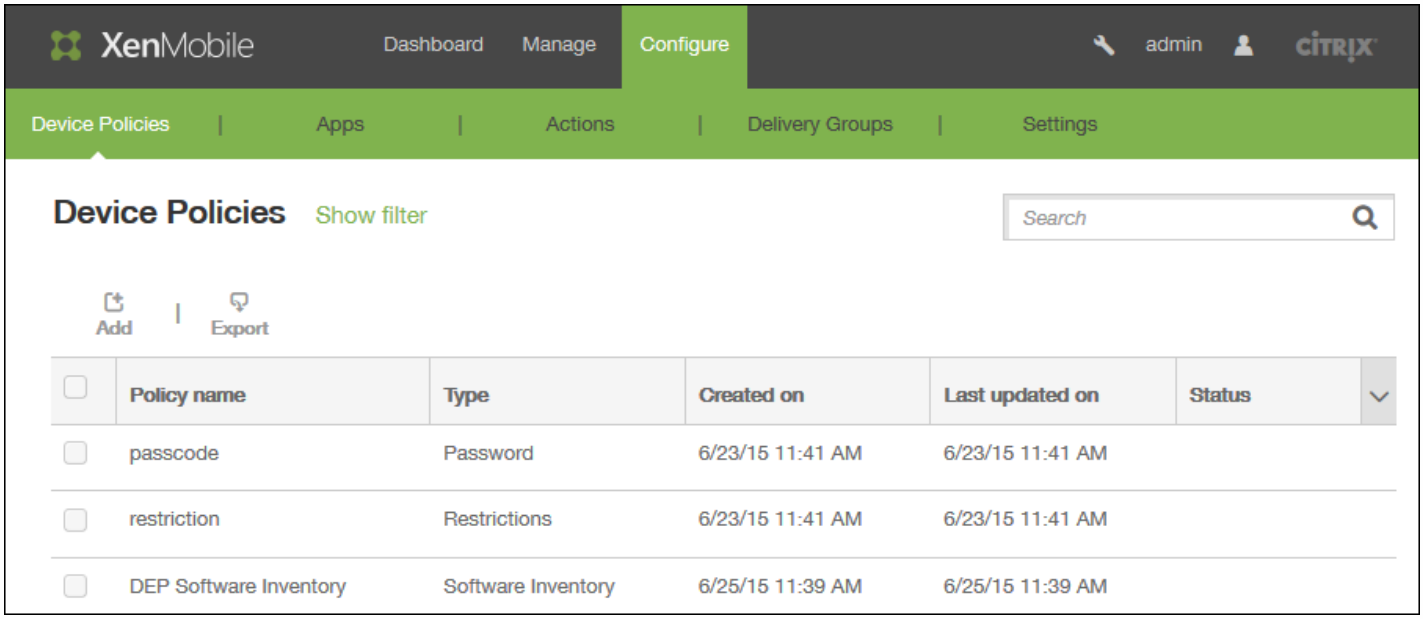
Tip: Any option for which you select **ON** means that the user

— can

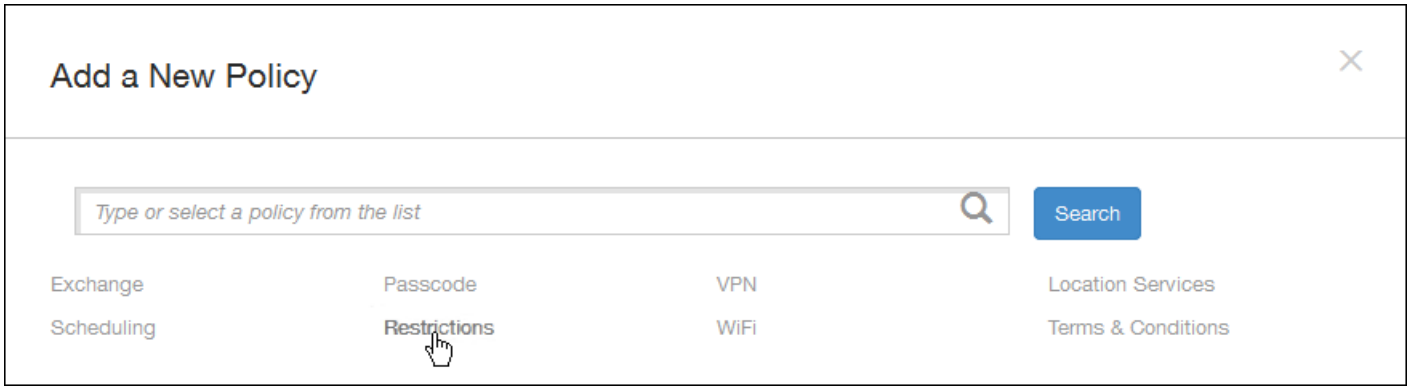
perform the operation or use the feature. For example:

- **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.

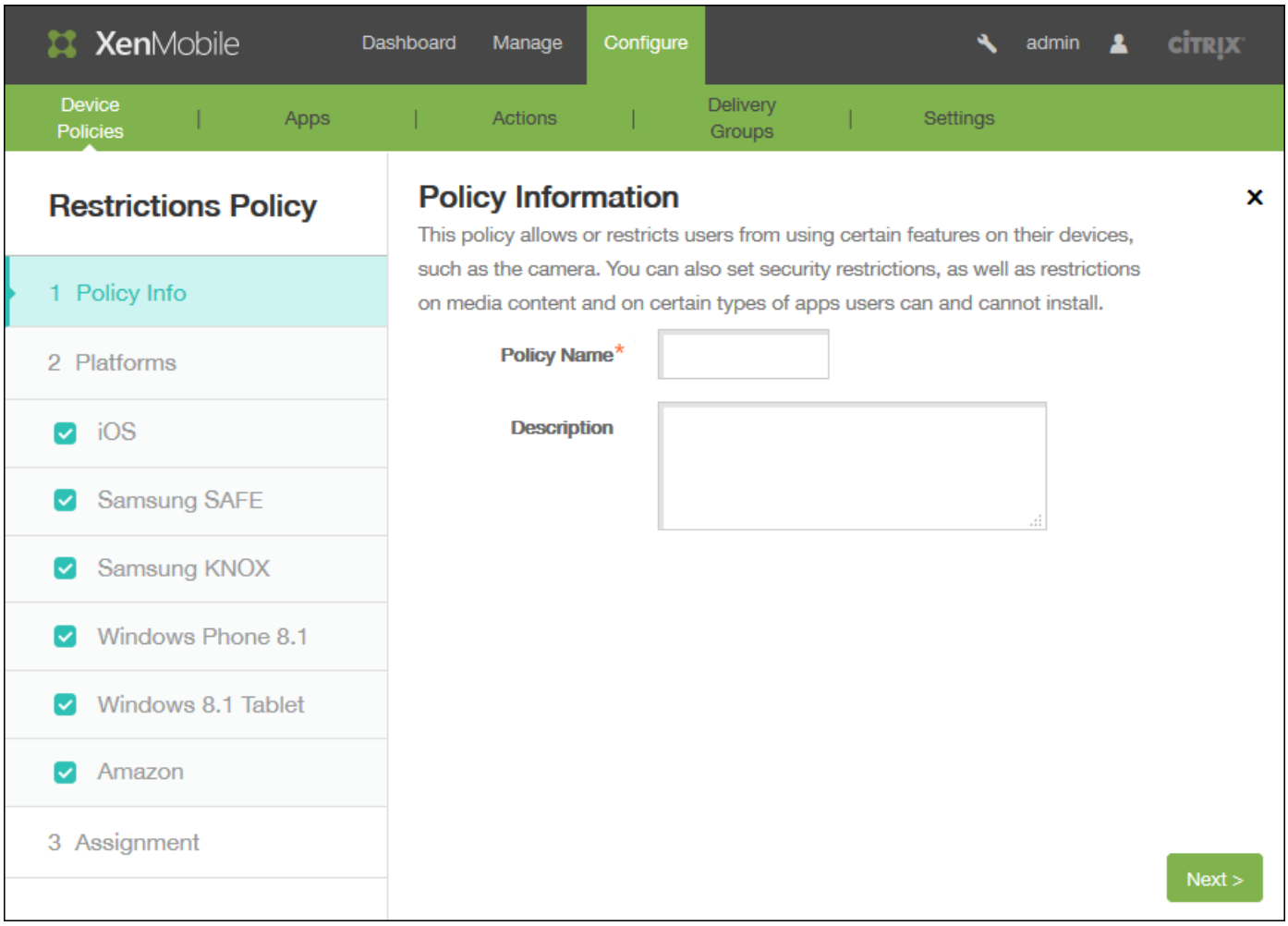
1. In the XenMobile console, click **Configure > Device Policies**. The **Device Policies** page appears.



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

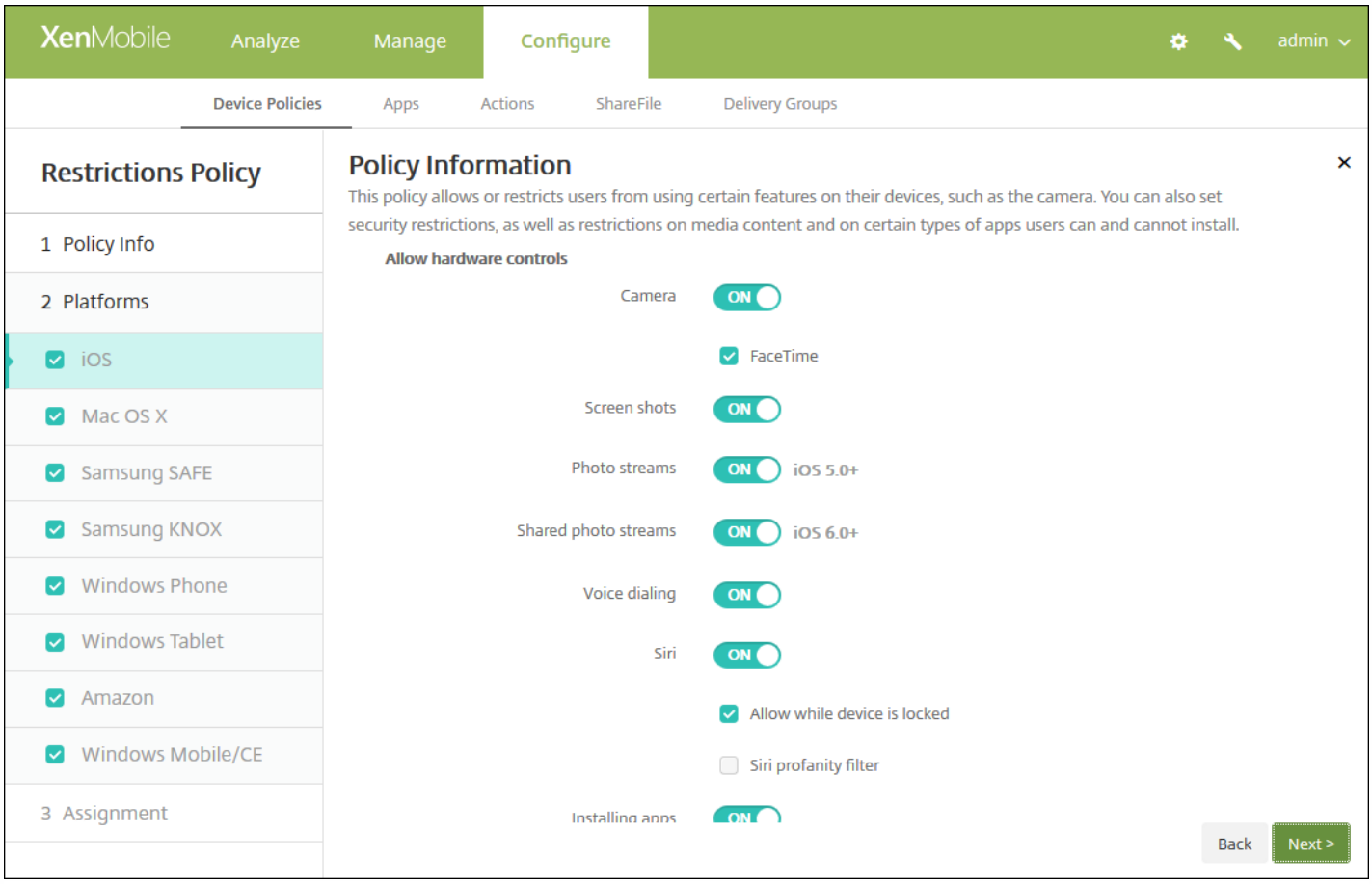
each platform you selected. Click to restrict any of the features in the following sections, which changes the setting to **OFF**. Unless otherwise noted, the default setting is to enable the feature.

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

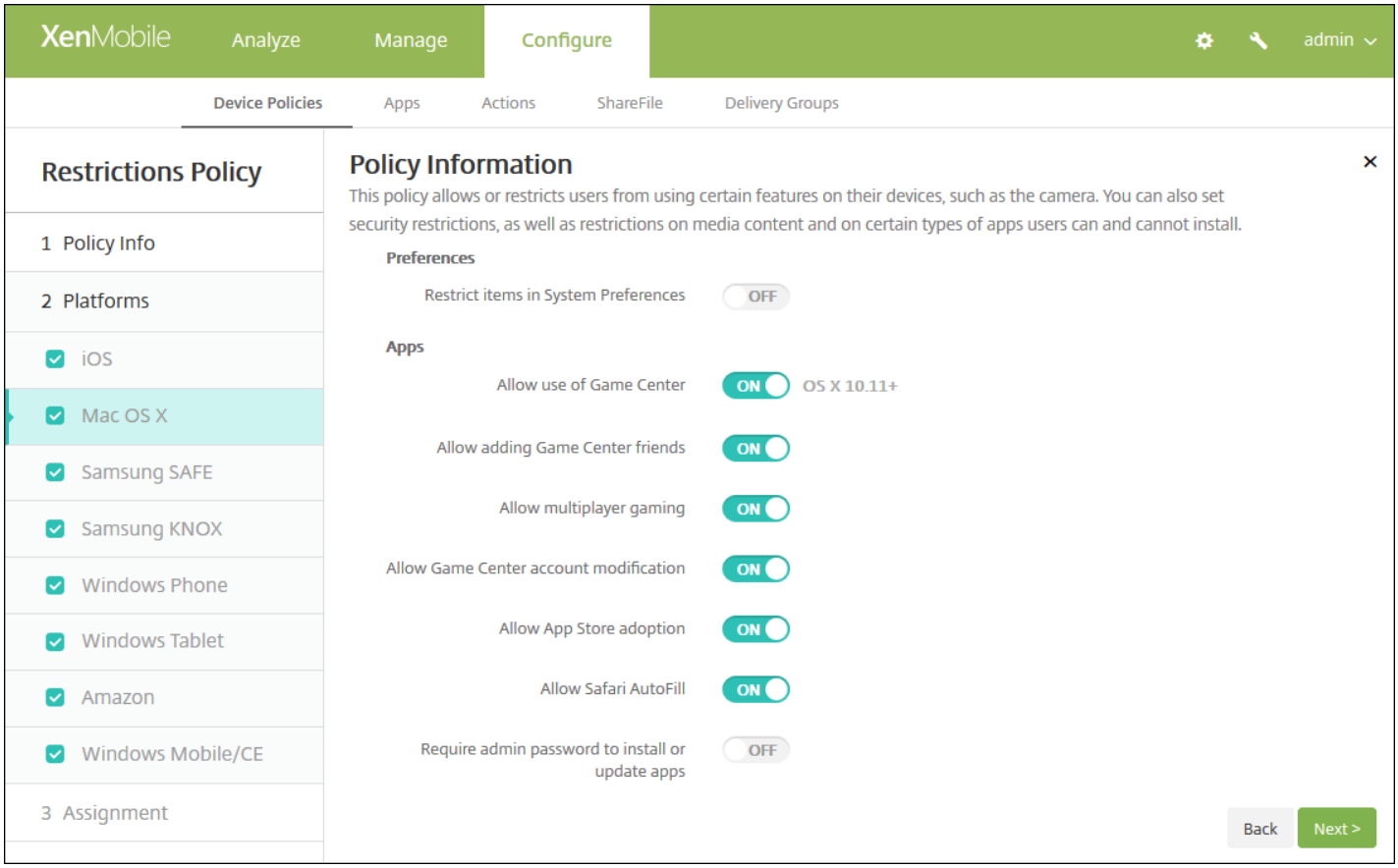
When you finish setting the restrictions for a platform, refer to Step 7 later in this article for how to set that platform's deployment rules.

If you selected iOS, configure these settings



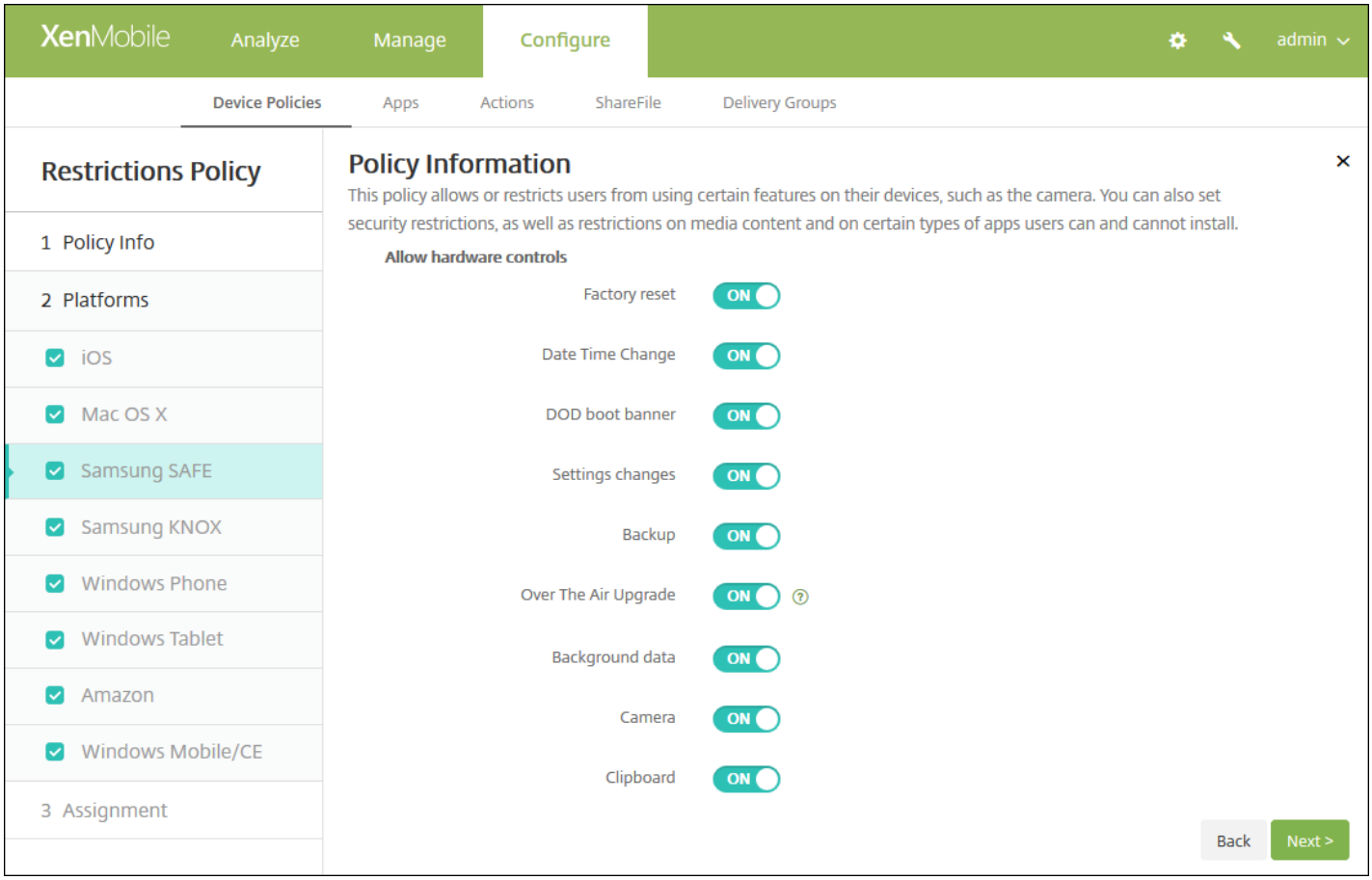
iOS settings

Configure Mac OS X settings



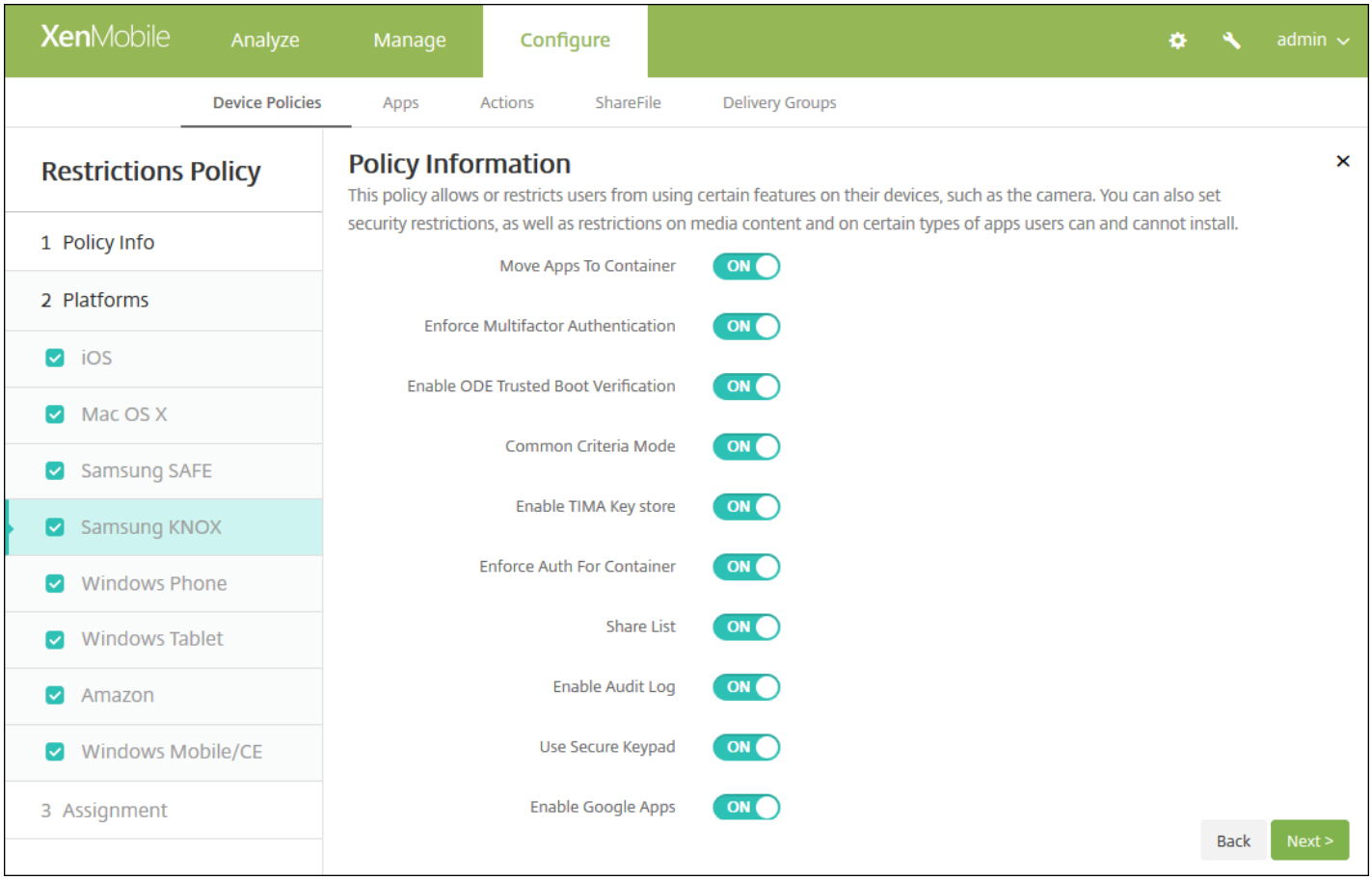
Mac OS X settings

Configure Samsung SAFE settings



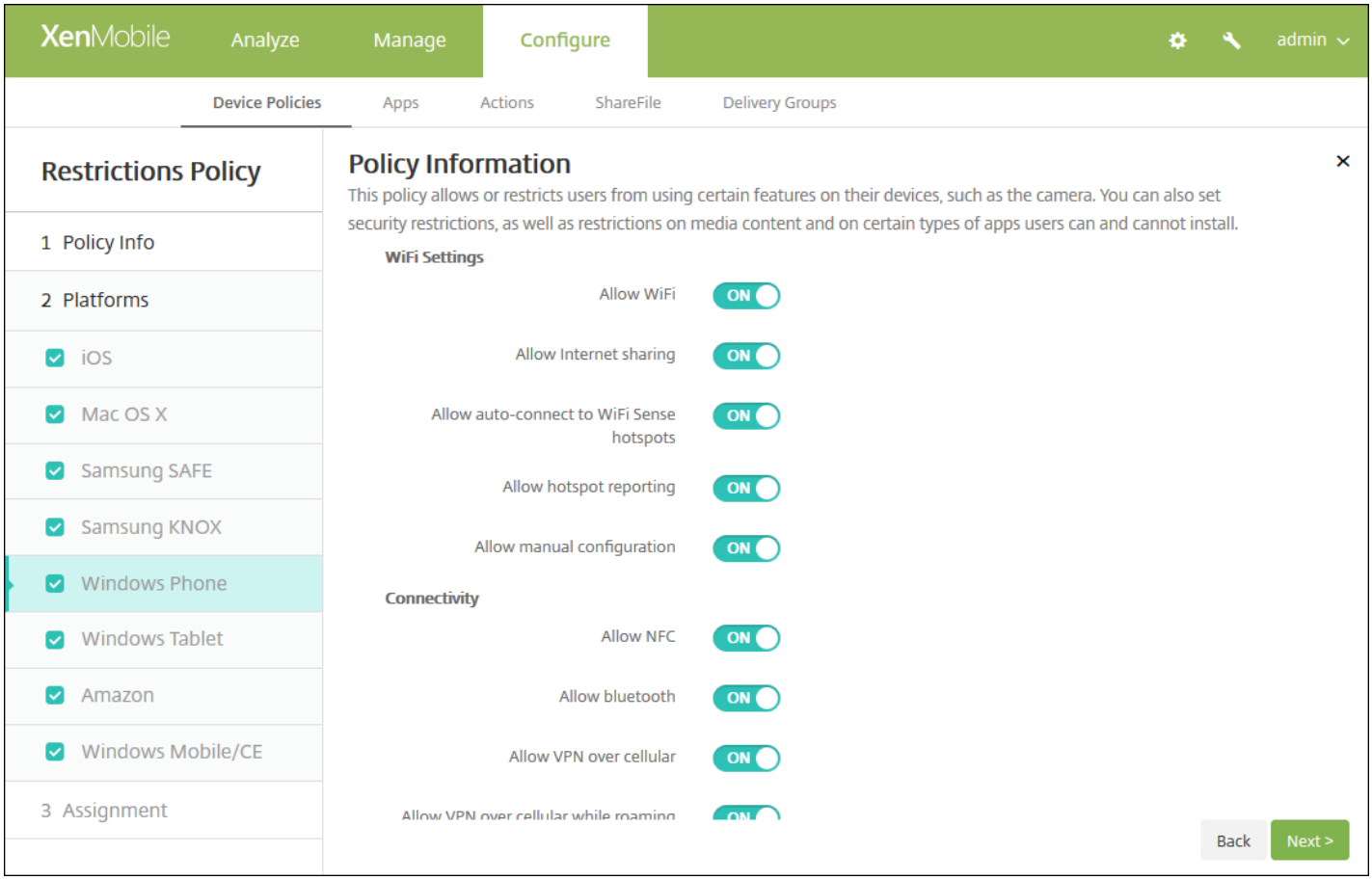
Samsung SAFE settings

Configure Samsung KNOX settings



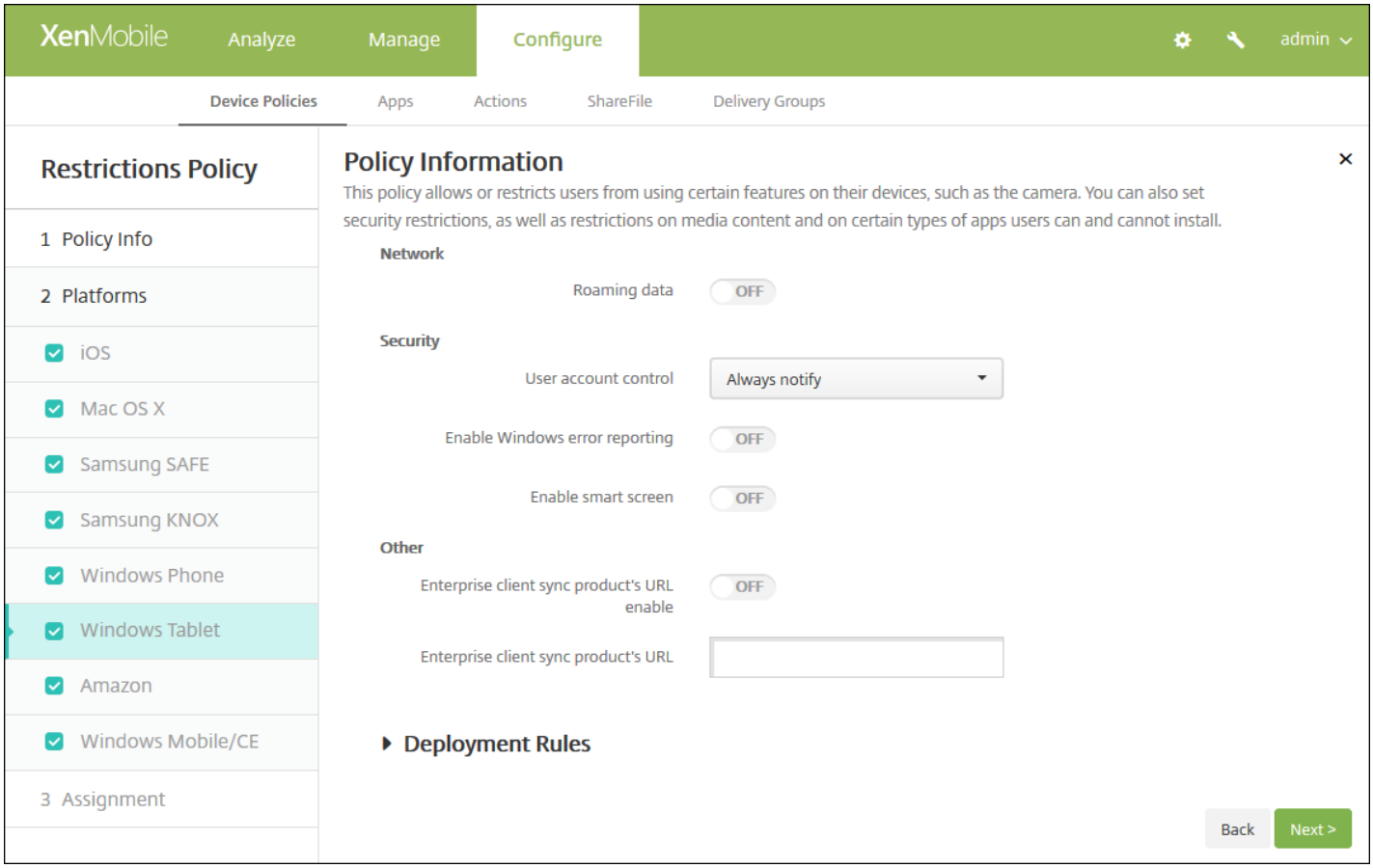
Samsung KNOX settings

Configure Windows Phone settings



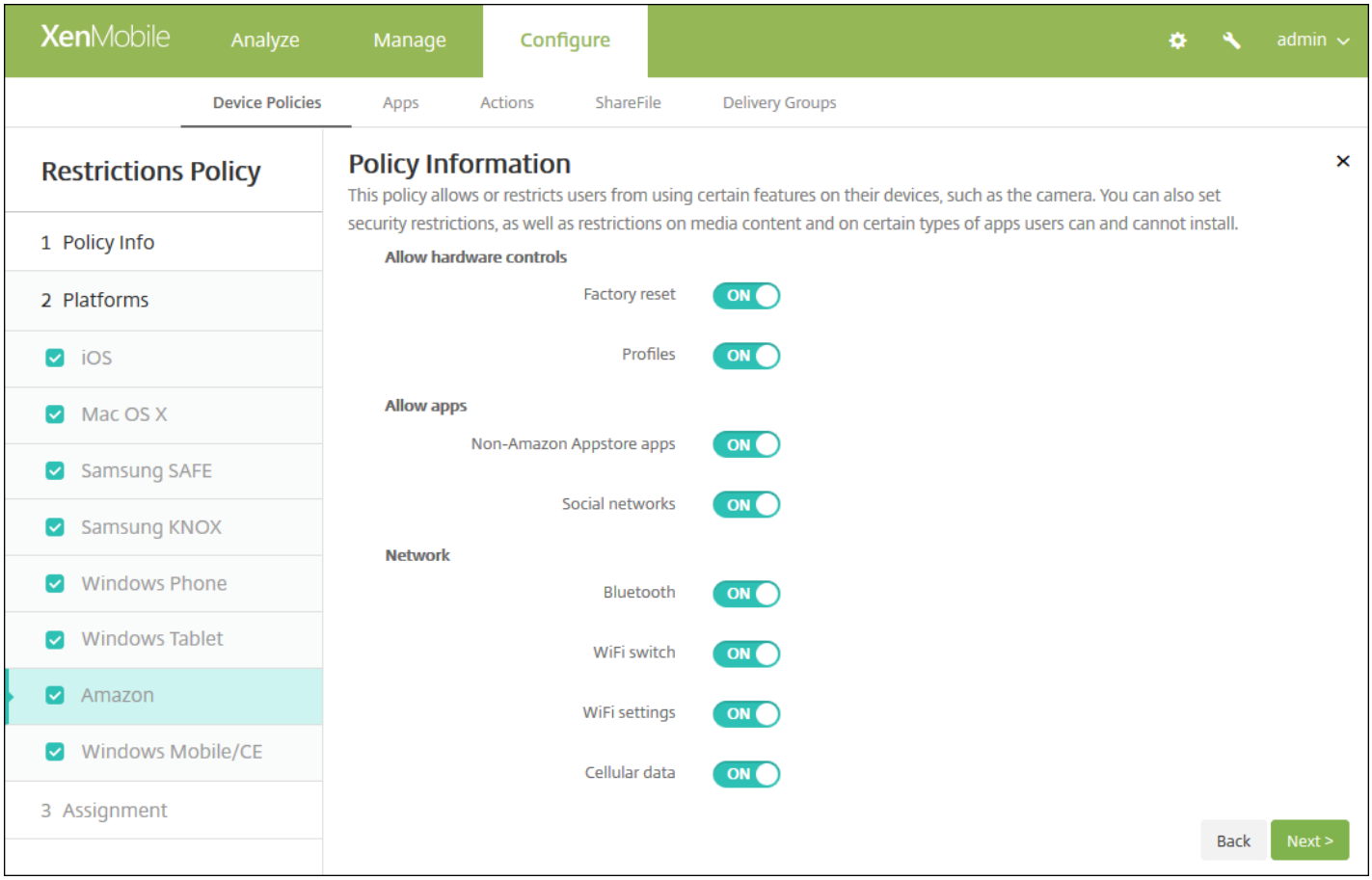
Windows Phone settings

Configure Windows Tablet settings



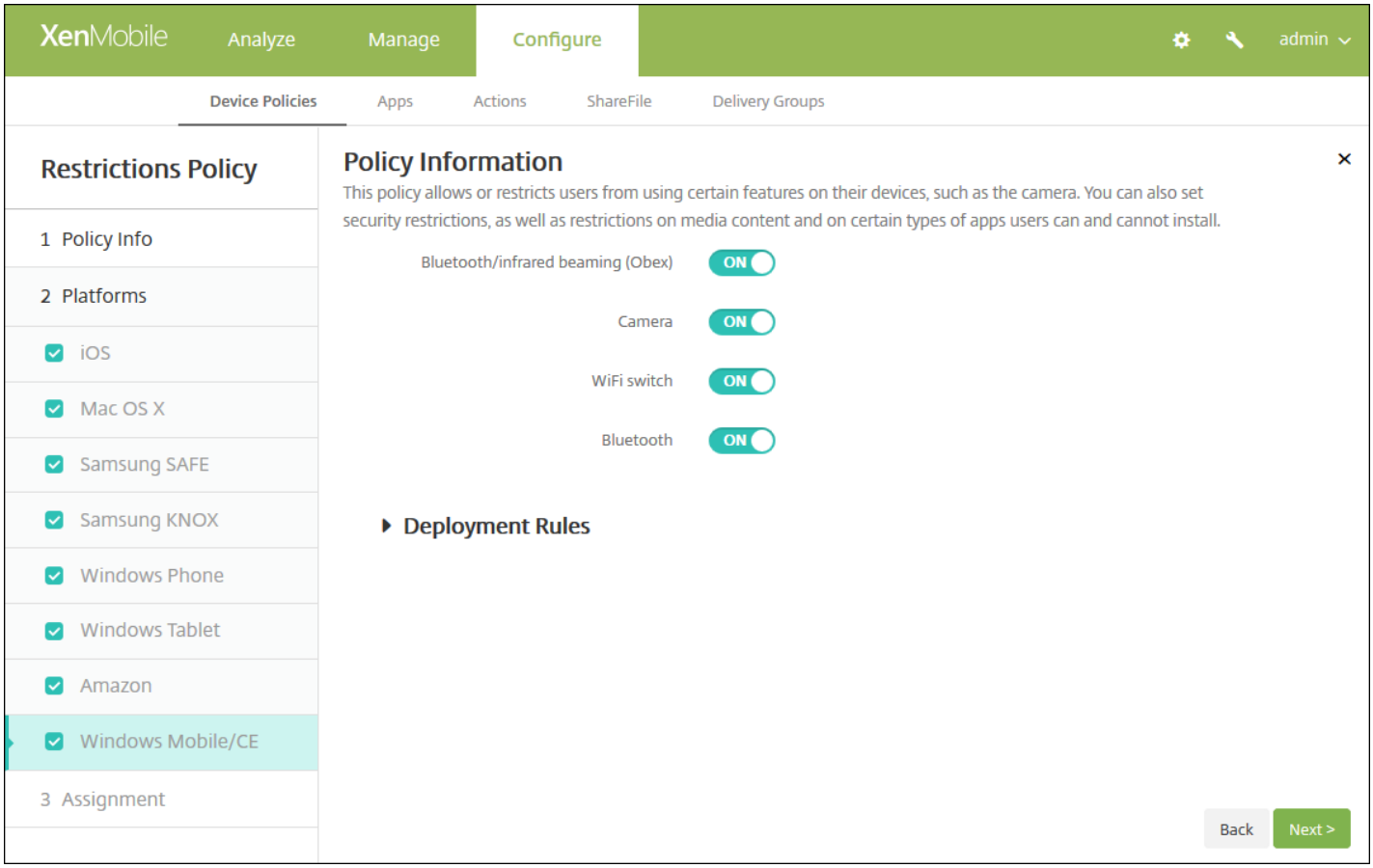
Windows Tablet settings

Configure Amazon settings



Amazon settings

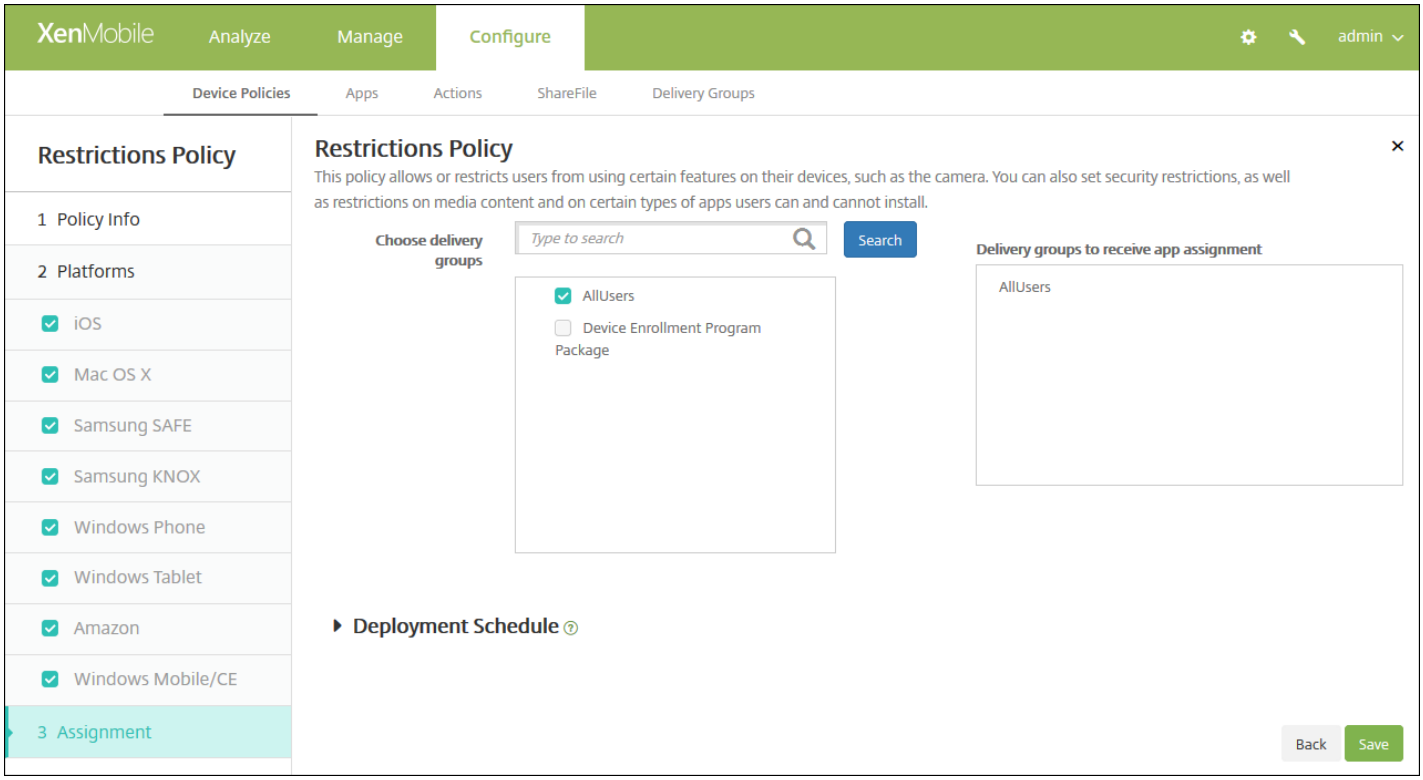
Configure Windows Mobile/CE settings



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 policies

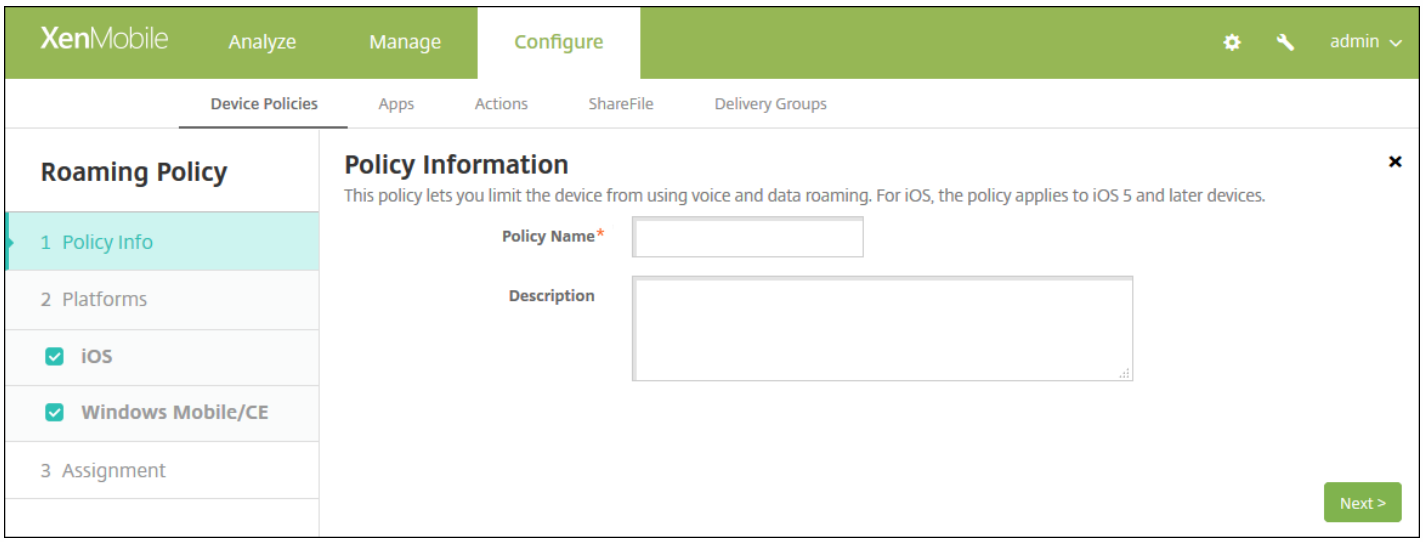
Mar 03, 2015

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:

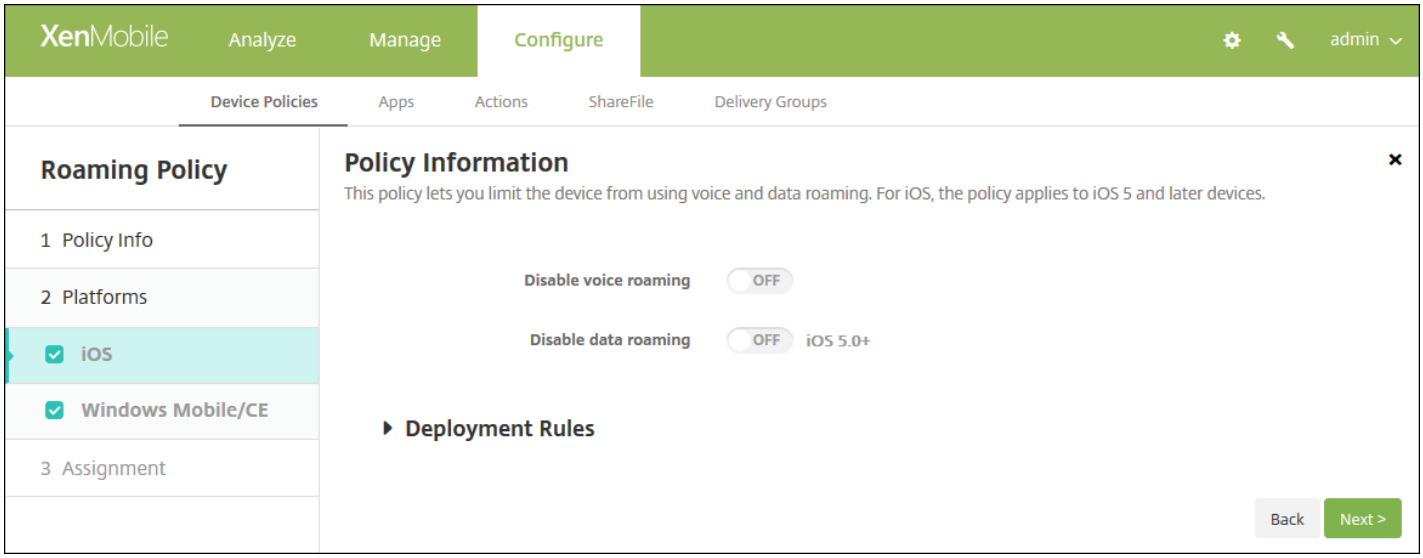
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Optionally, type a description of the policy.

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.

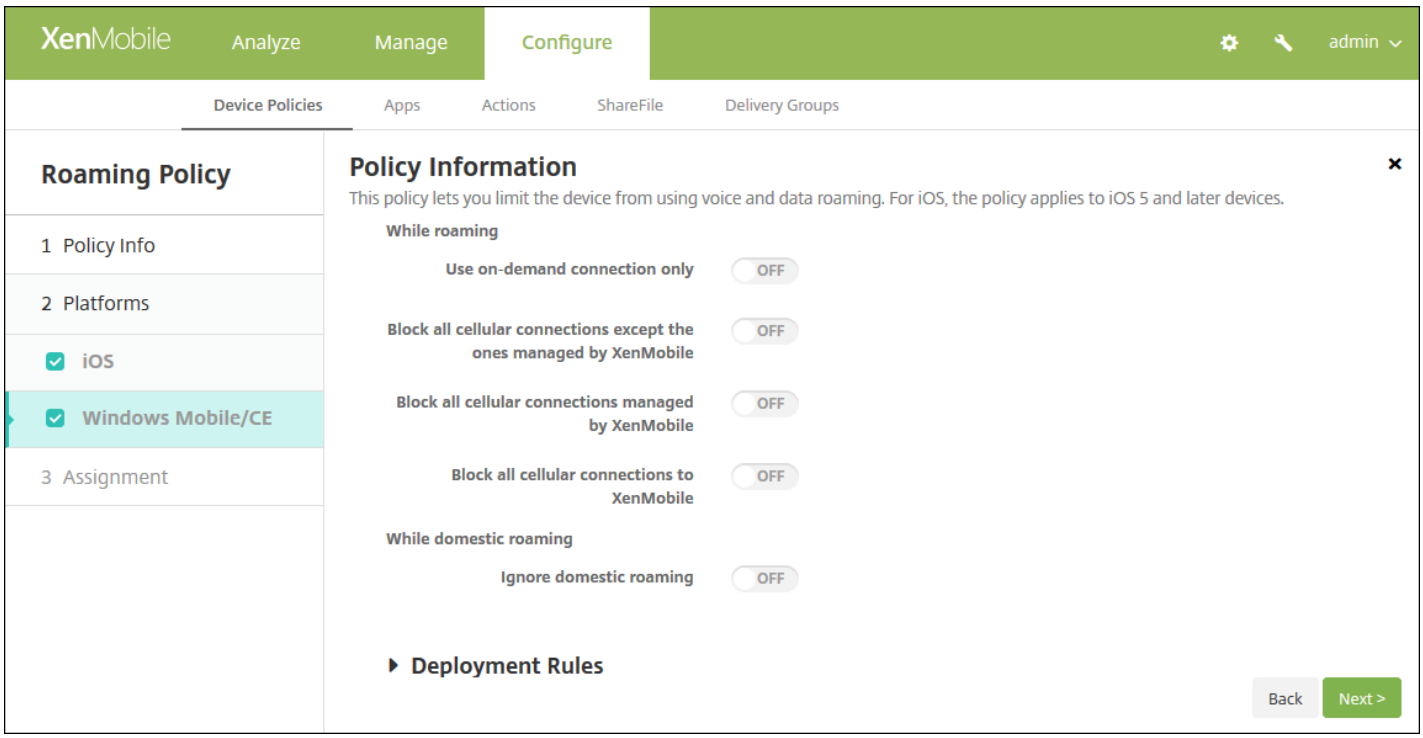
Configure iOS settings



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:

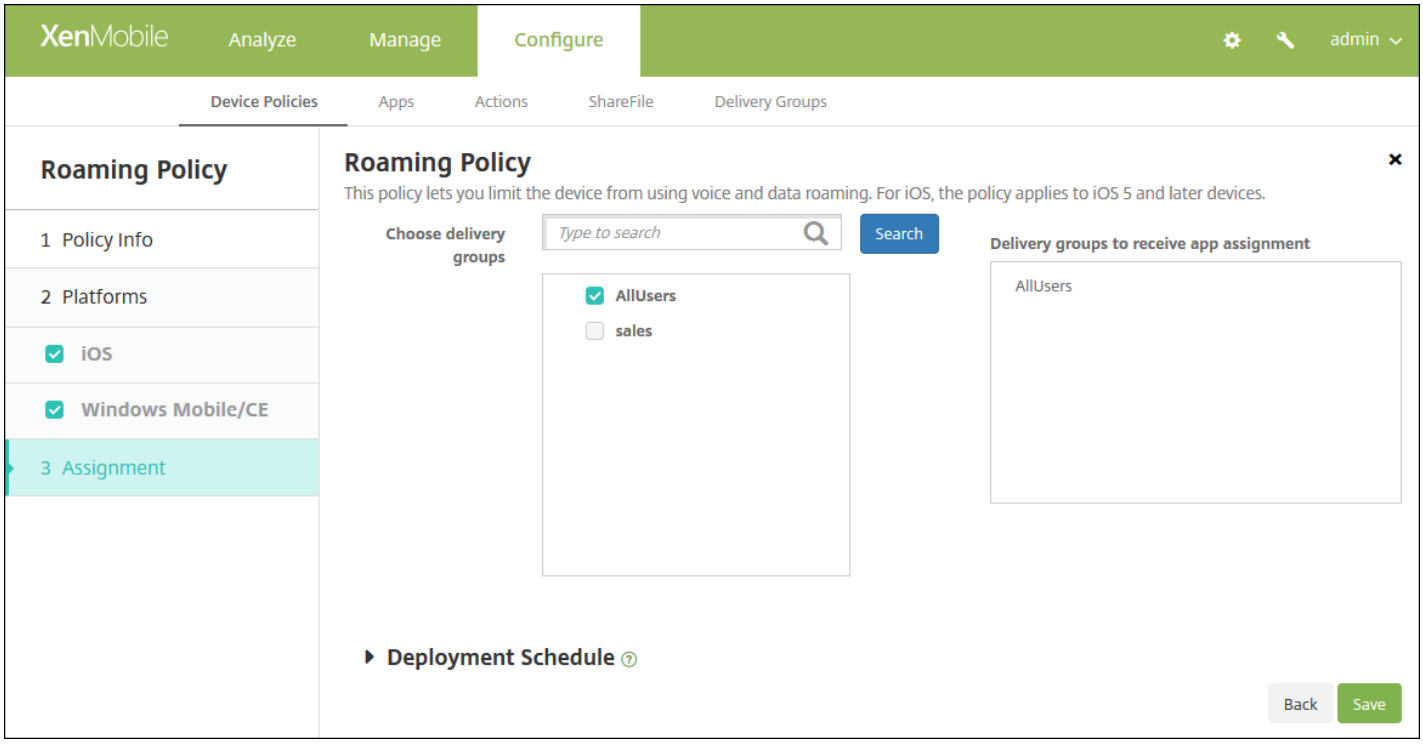
- **While roaming**

- **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 policies

Jan 06, 2017

XenMobile supports and extends both Samsung for Enterprise (SAFE) and Samsung KNOX policies. SAFE is a family of solutions that provides security and feature enhancements for business use through integration with mobile device management solutions. Samsung KNOX is a solution within the SAFE program that provides a more secure Android platform for enterprise use.

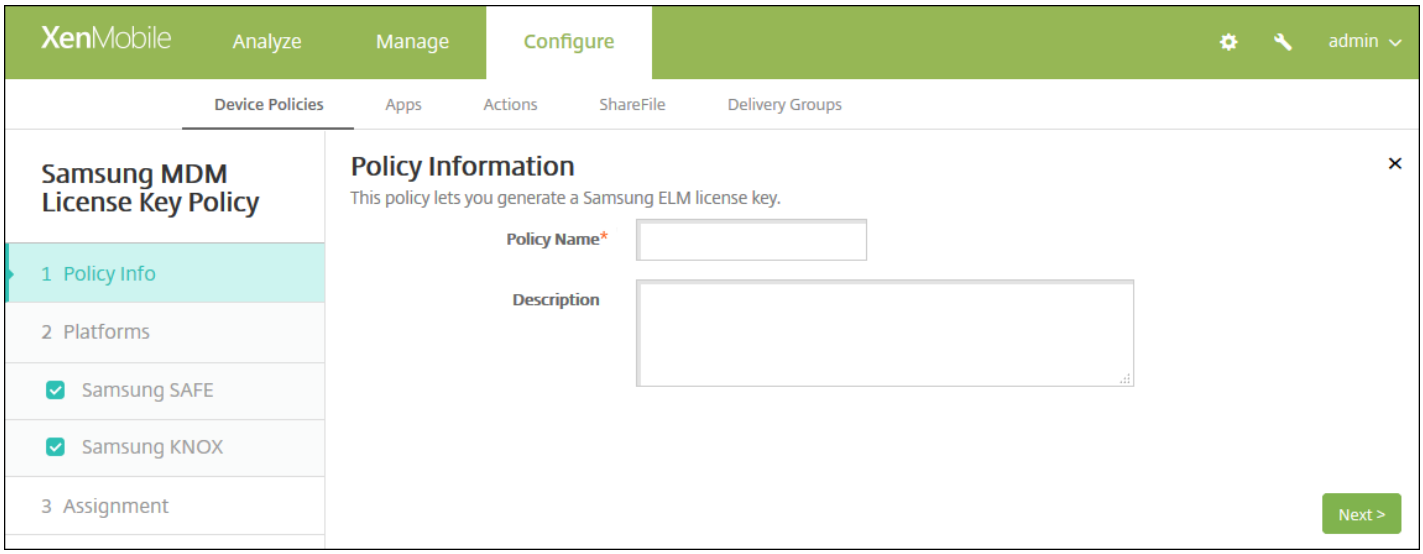
You must enable the SAFE APIs by deploying the built-in Samsung Enterprise License Management (ELM) key to a device before you can deploy SAFE policies and restrictions. To enable the Samsung KNOX API, you also need to purchase a Samsung KNOX Workspace license using the Samsung KNOX License Management System (KLMS) in addition to deploying the Samsung ELM key. The Samsung KLMS provisions valid licenses to mobile device management solutions to enable them to activate Samsung KNOX APIS on mobile devices. These licenses must be obtained from Samsung and are not provided by Citrix.

You must deploy Worx Home along with the Samsung ELM key to enable the SAFE and Samsung KNOX APIs. **Note**: Starting with version 10.4, Worx Home is renamed Secure Hub. 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:

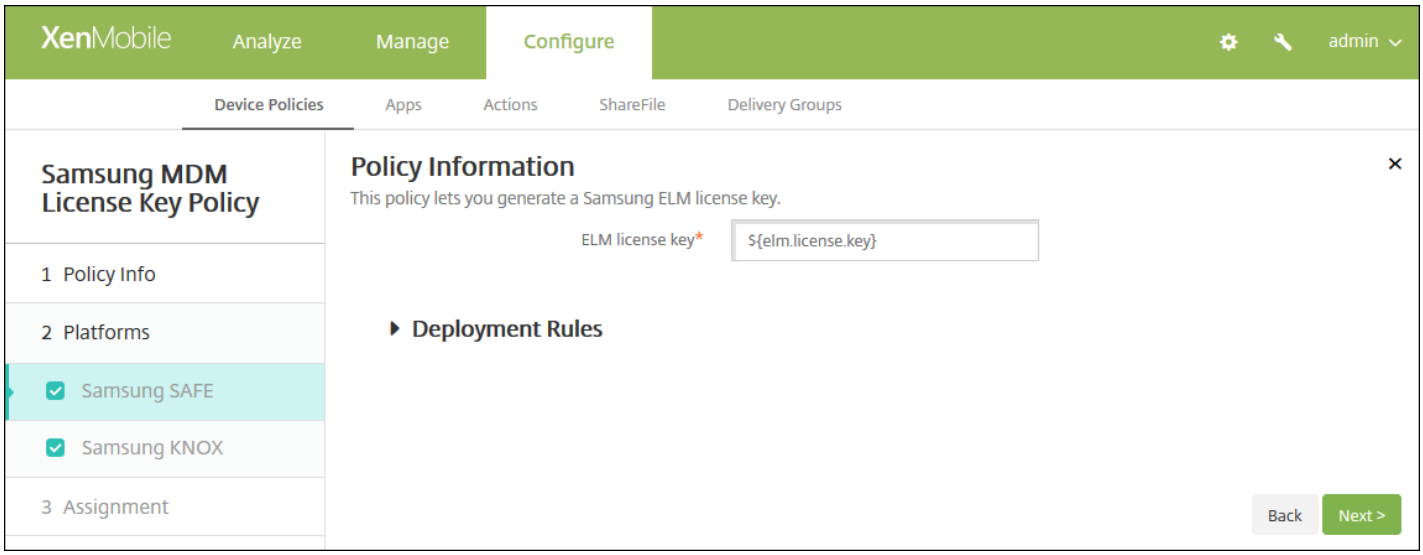
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

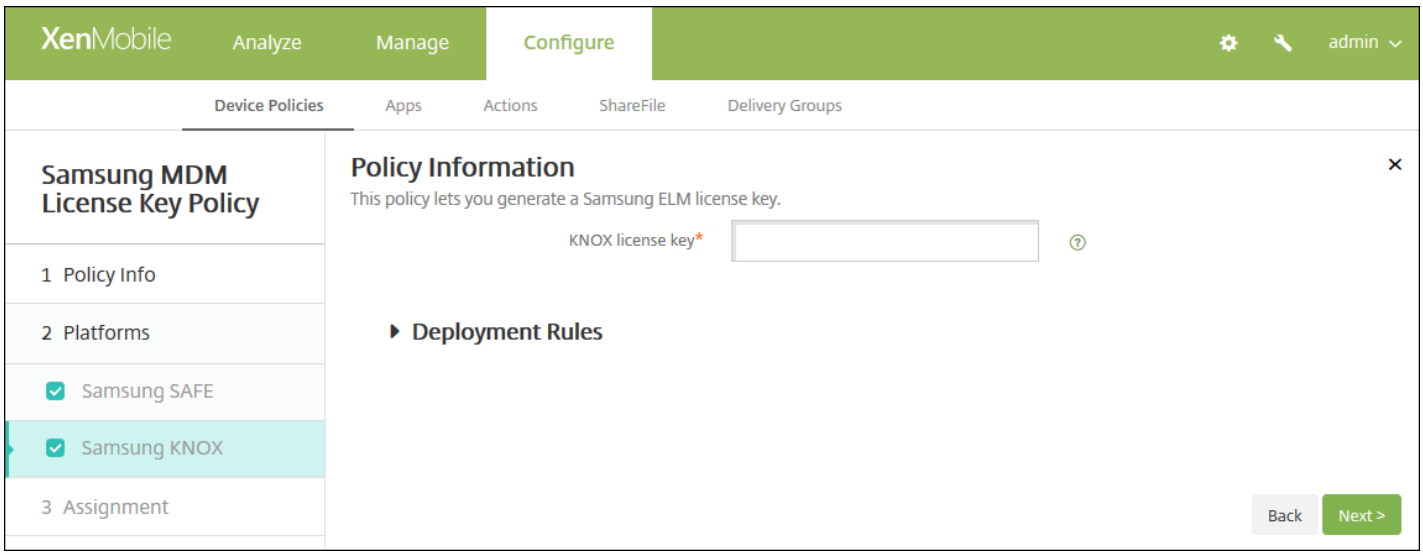
Configure Samsung SAFE settings



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 setttings

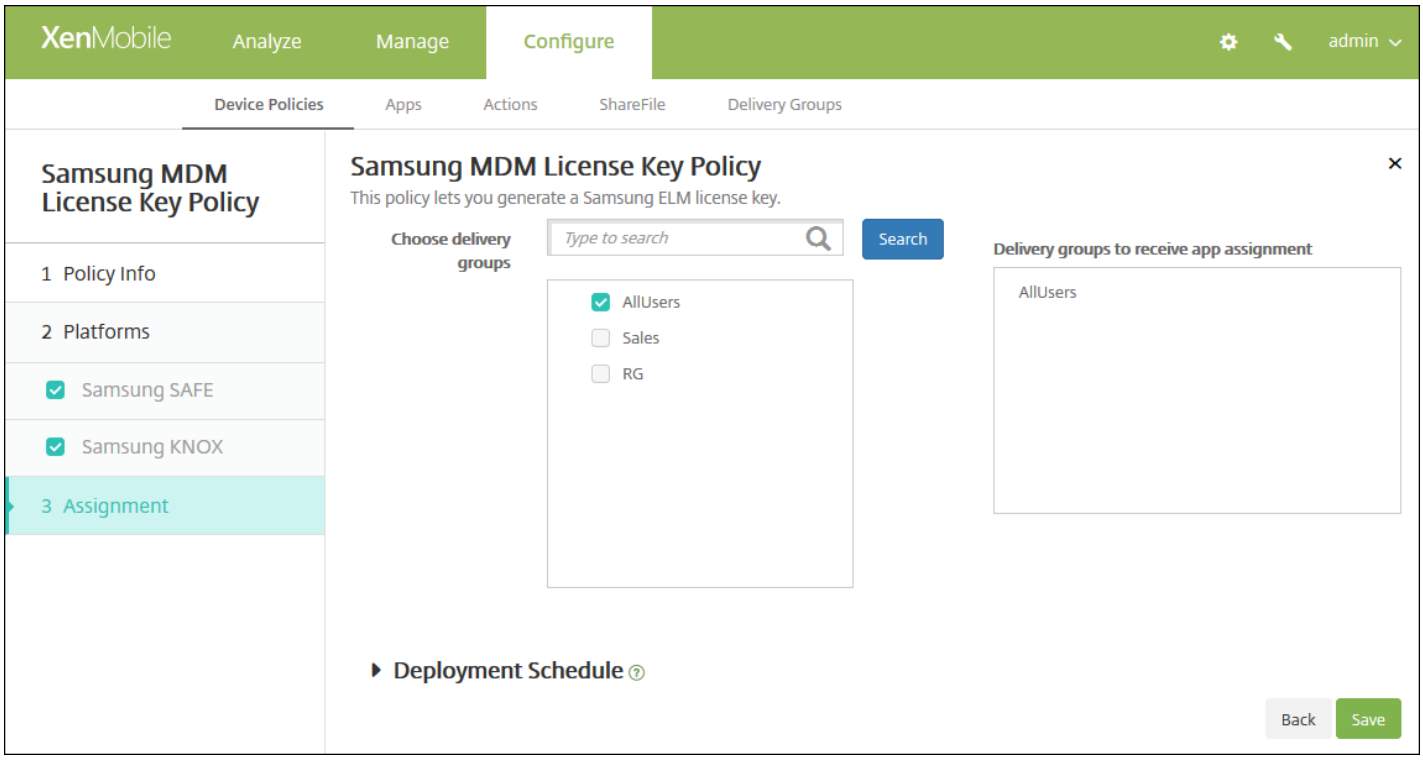


Configure this setting:

- **KNOX License key**: Type the 25-digit 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

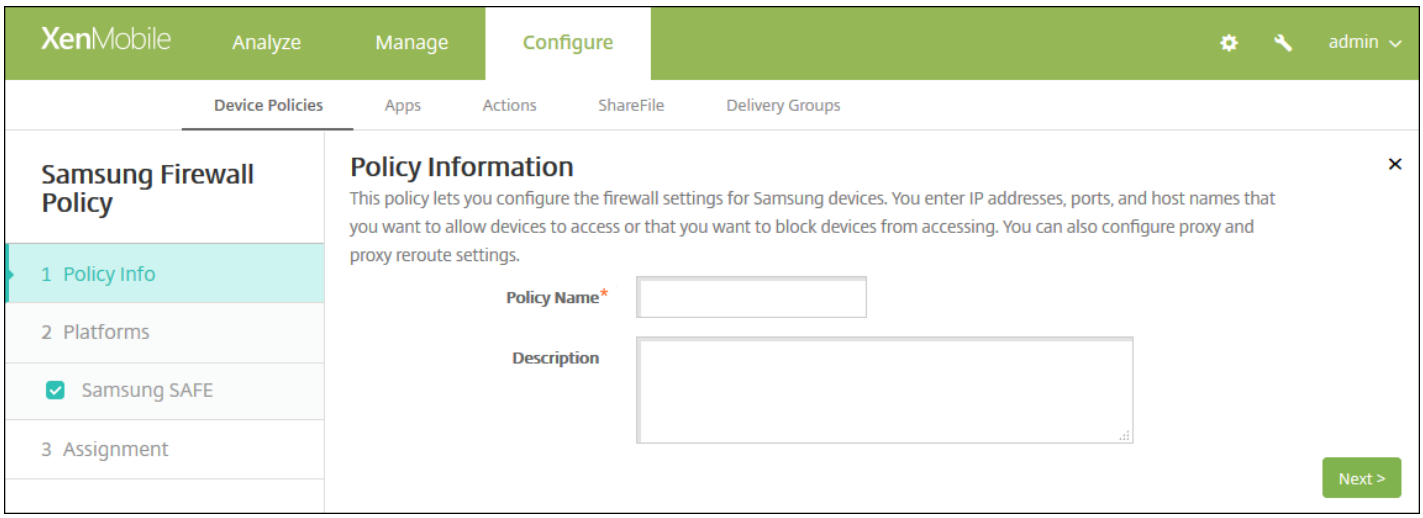
Sep 24, 2015

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.

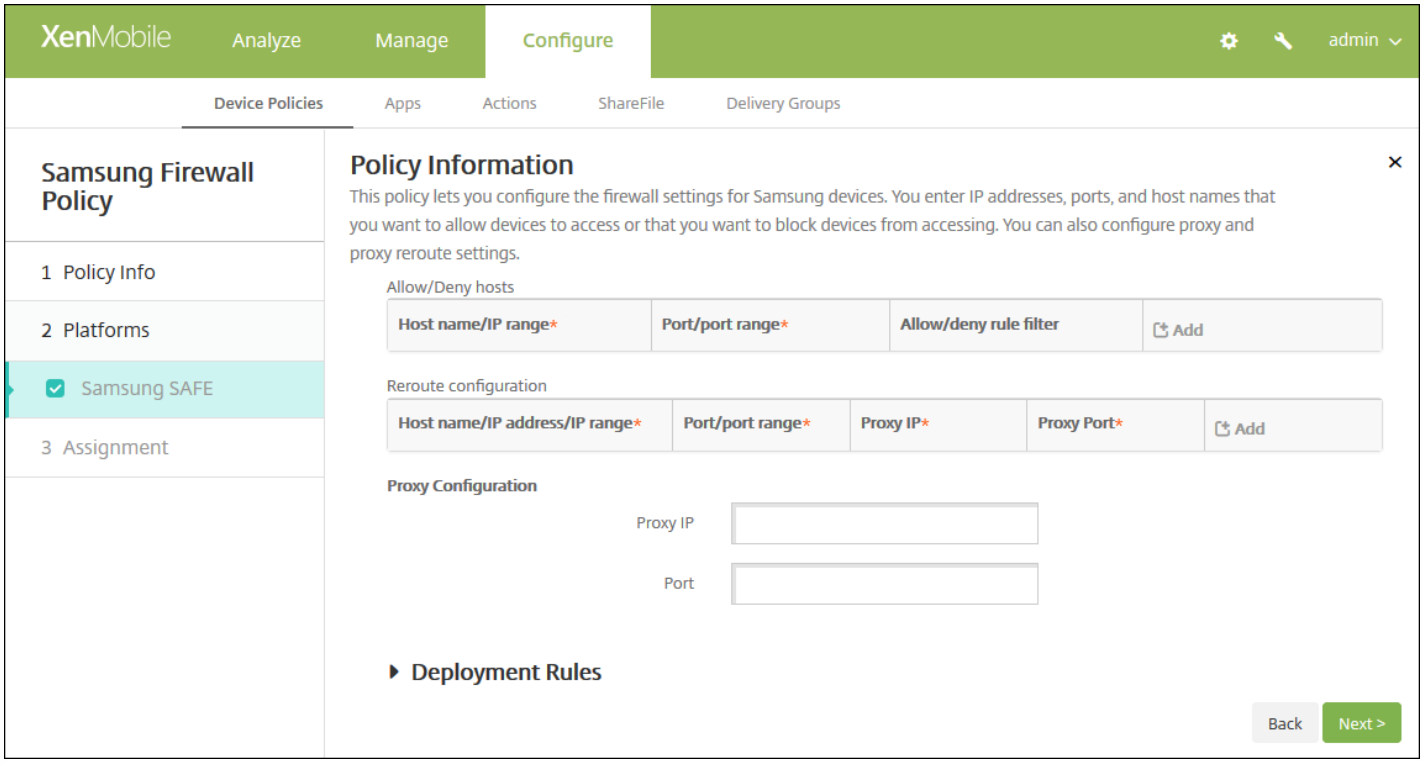
3. Expand **More** and then, under **Network access**, click **Samsung Firewall**. The **Samsung Firewall Policy** page appears.



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:

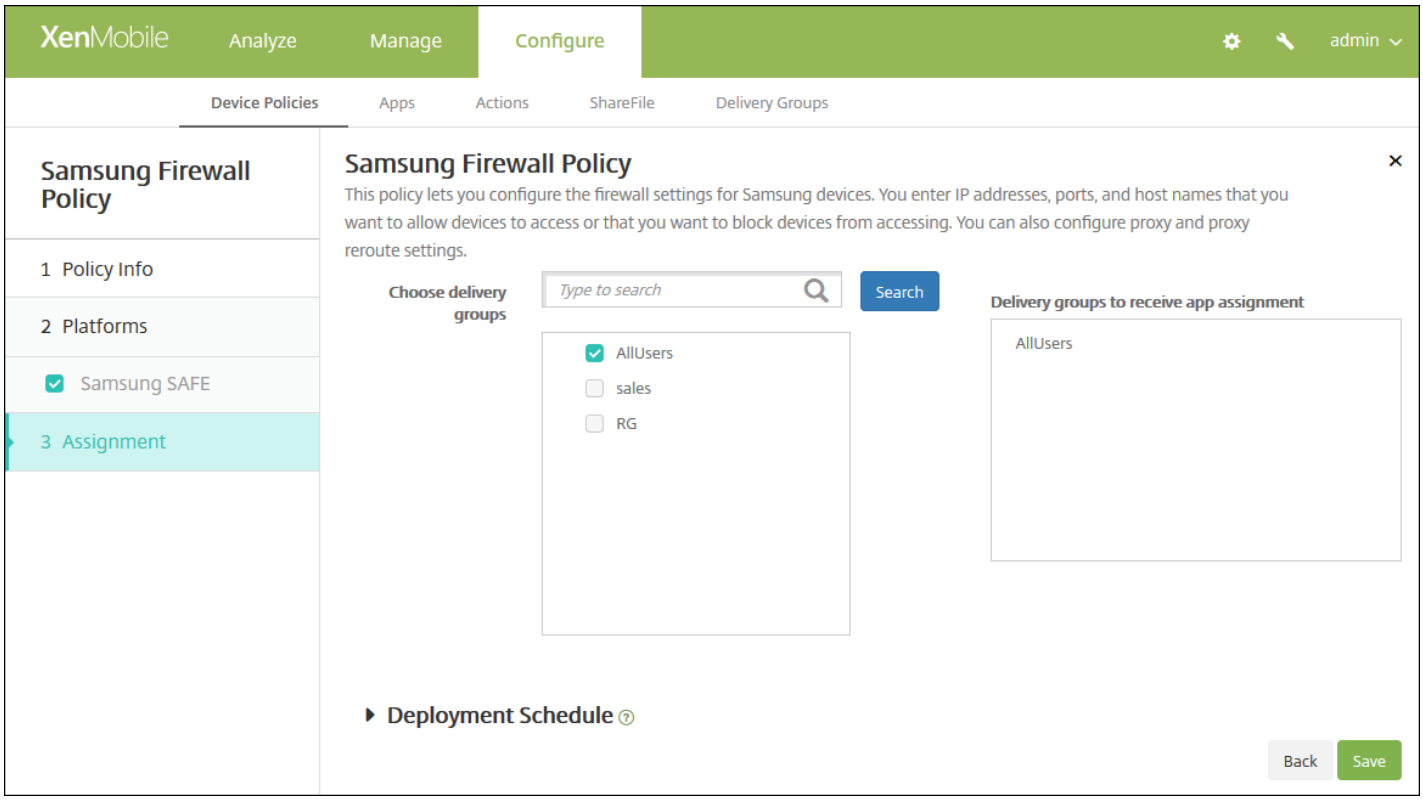
- **Allow/Deny hosts**
  - For each host to which you want to allow or deny access, click **Add** and do the following:
    - **Host name/IP range**: Type the host name or IP address range of the site you want to affect.
    - **Port/port range**: Type the port or port range.
    - **Allow/deny rule 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 policies

Jul 16, 2015

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.

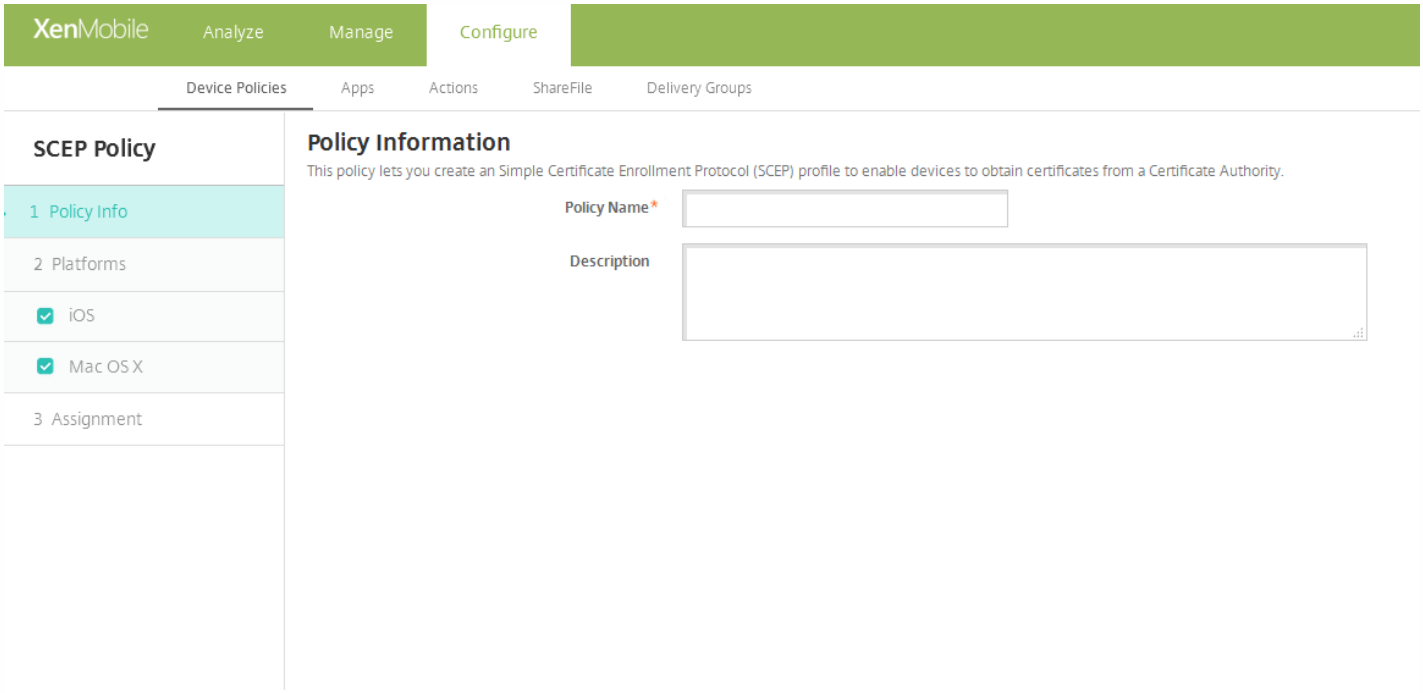
iOS settings

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:

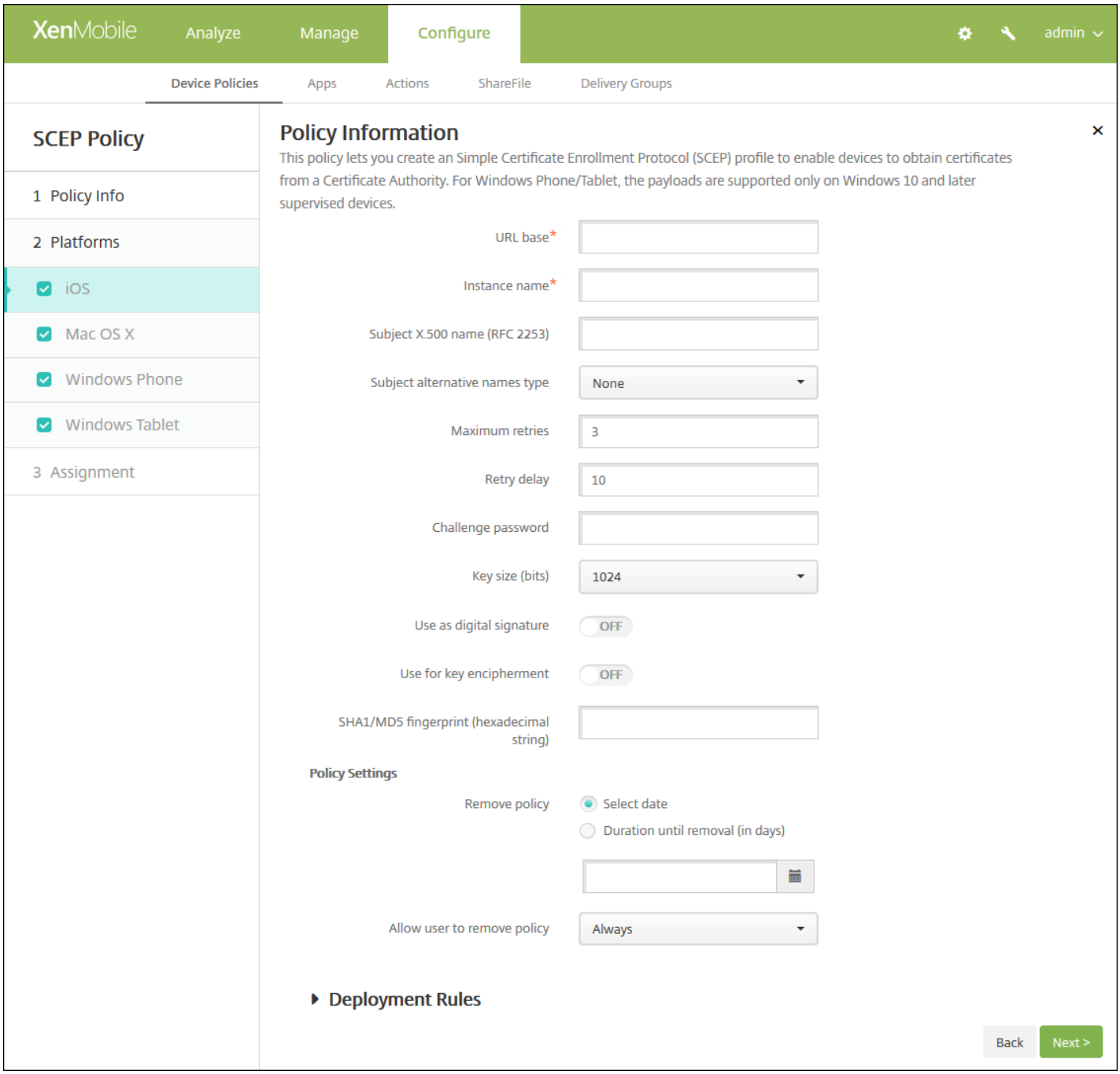
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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



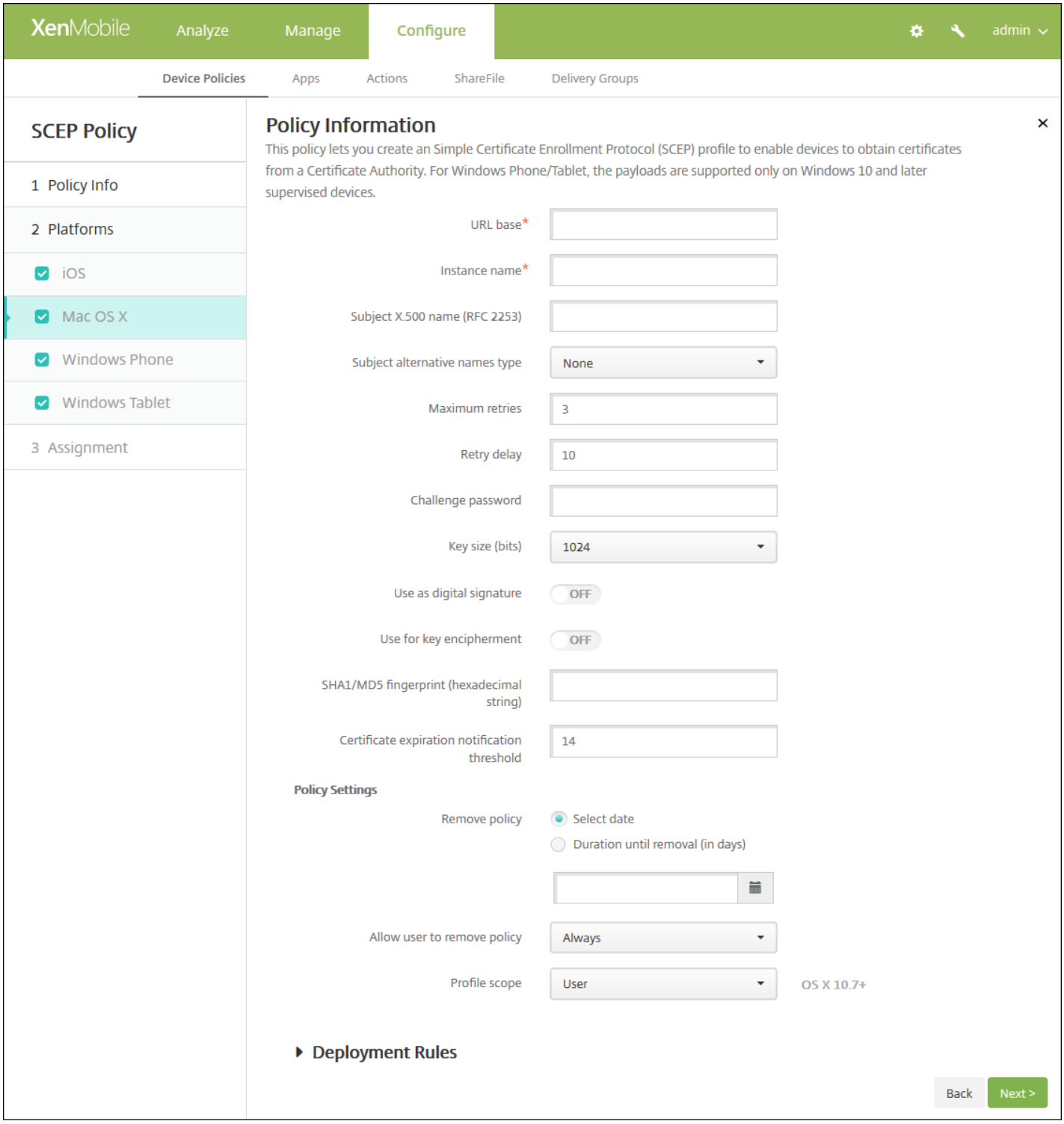
Configure these settings:

- **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

Mar 04, 2015

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.

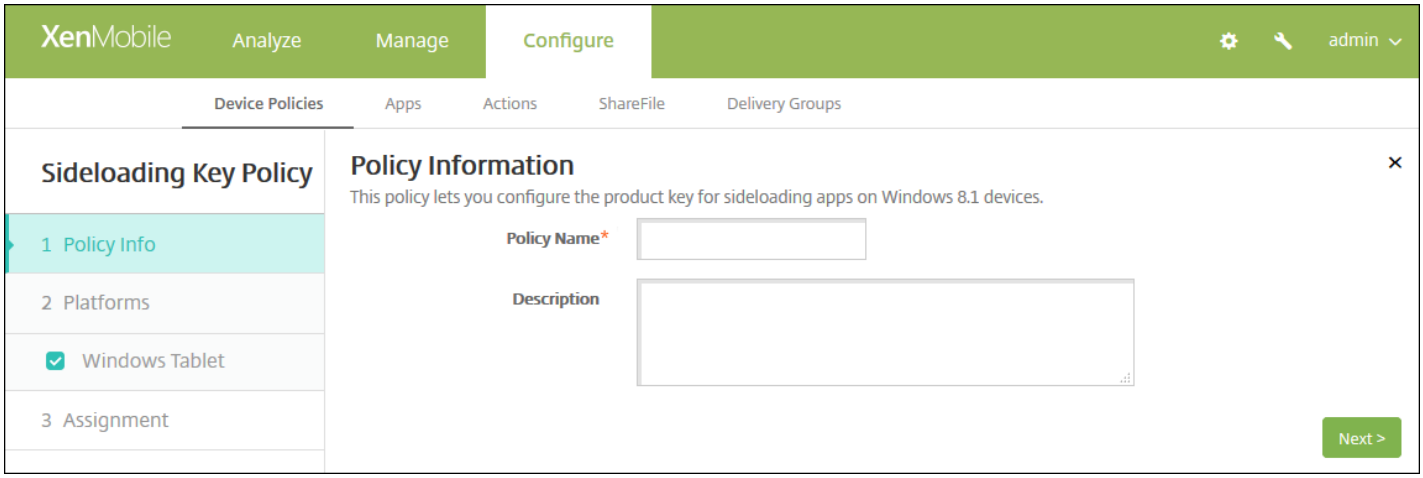
You need the following information before you can create this policy:

- 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.

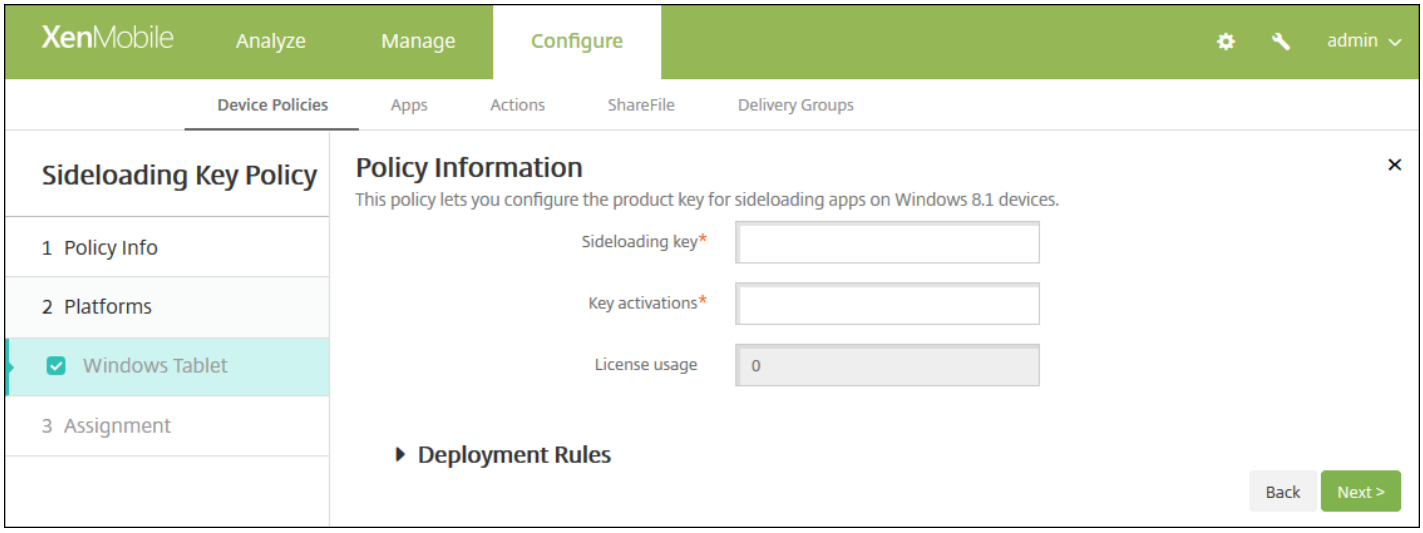
3. Expand **More**, and then under **Apps**, click **Sideloading Key**. The **Sideloading Key Policy** page appears.



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.

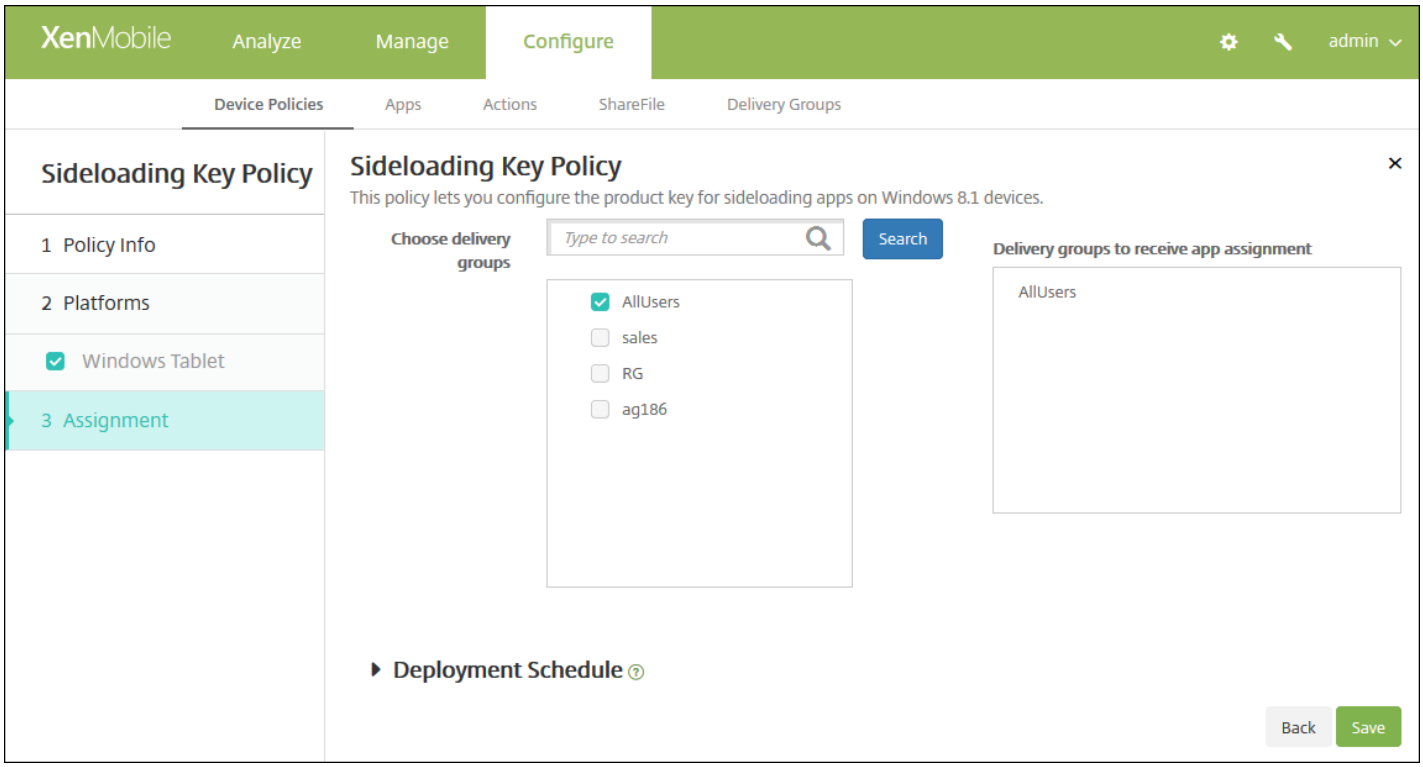


6. Configure these settings:

- **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

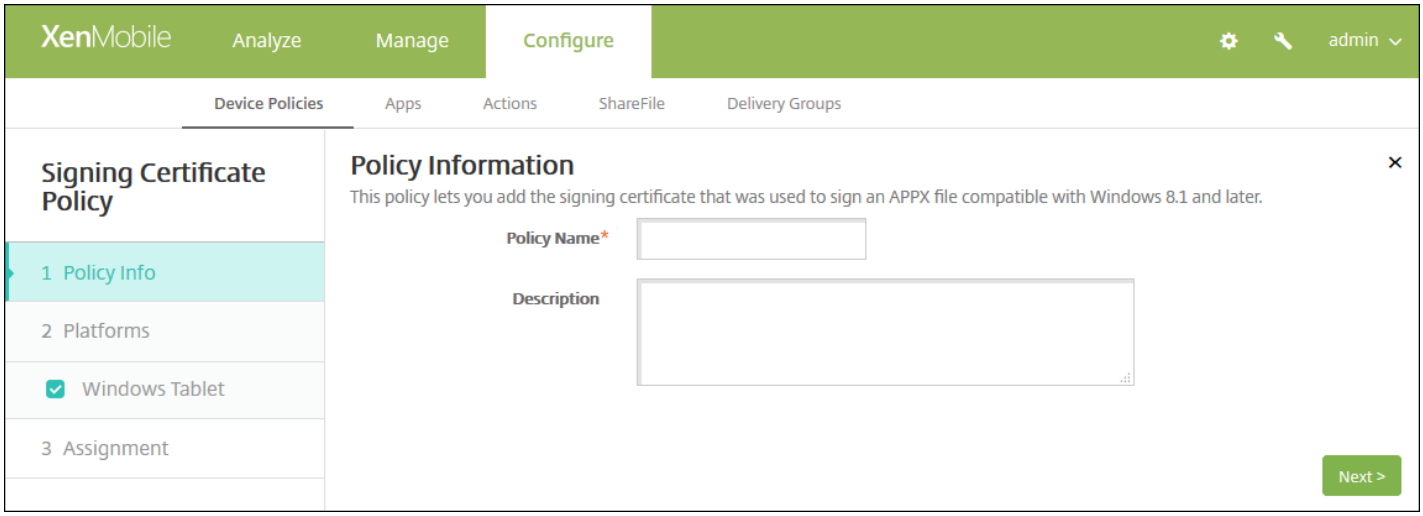
Feb 13, 2015

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.

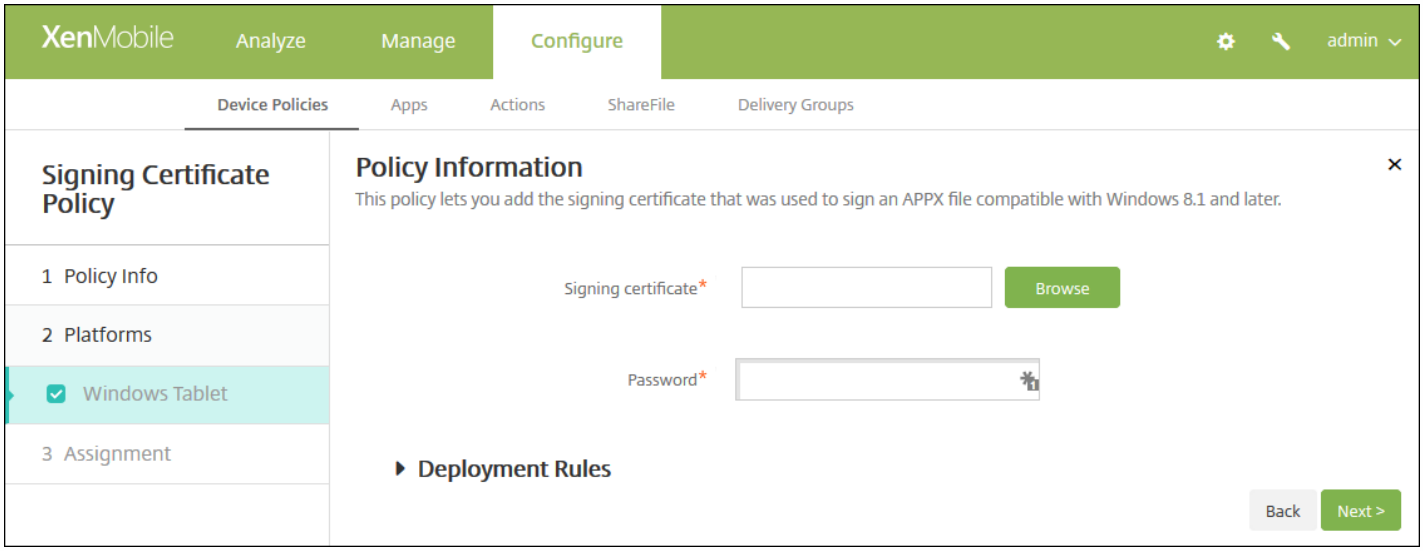
3. Click **More** and then, under **Apps**, click **Signing Certificate**. The **Signing Certificate Policy** page appears.



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.

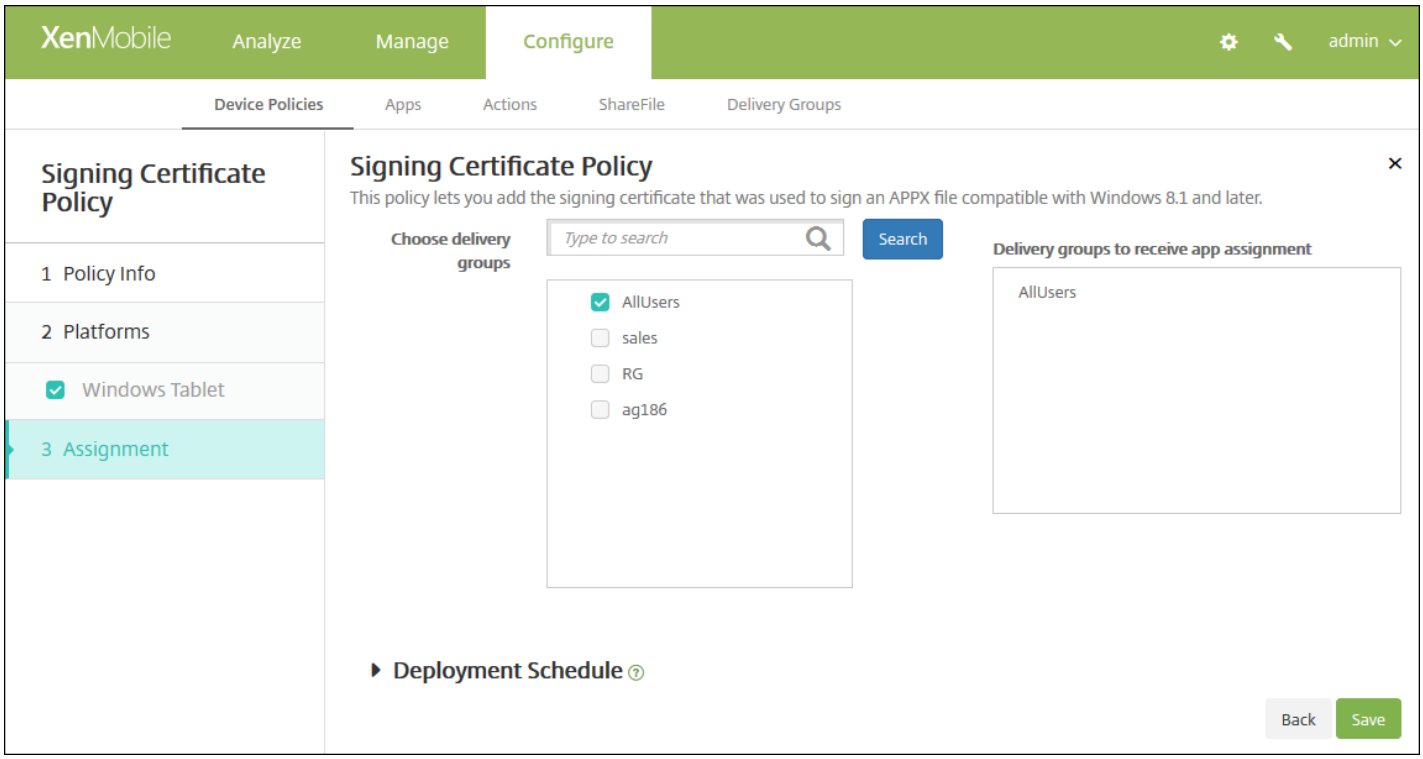


6. Configure these settings:

- **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**.

Single sign-on account device policy

Mar 03, 2015

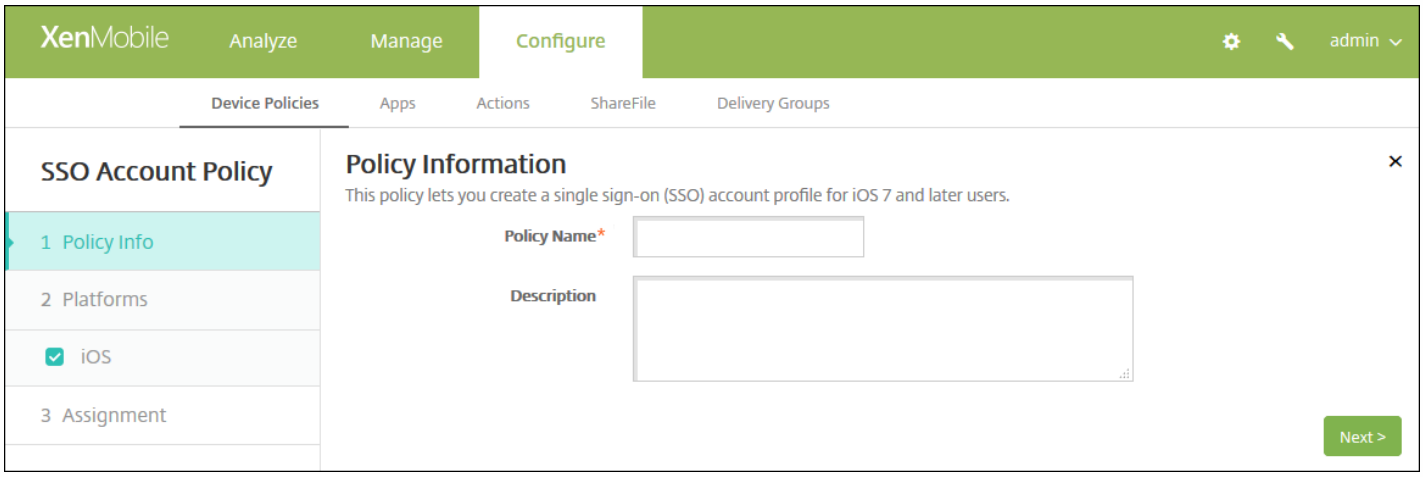
You create single sign-on (SSO) accounts in XenMobile to let users sign on one-time only to access XenMobile and your internal company resources from various apps. Users do not need to store any credentials on the device. The SSO account enterprise user credentials are used across apps, including apps 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.

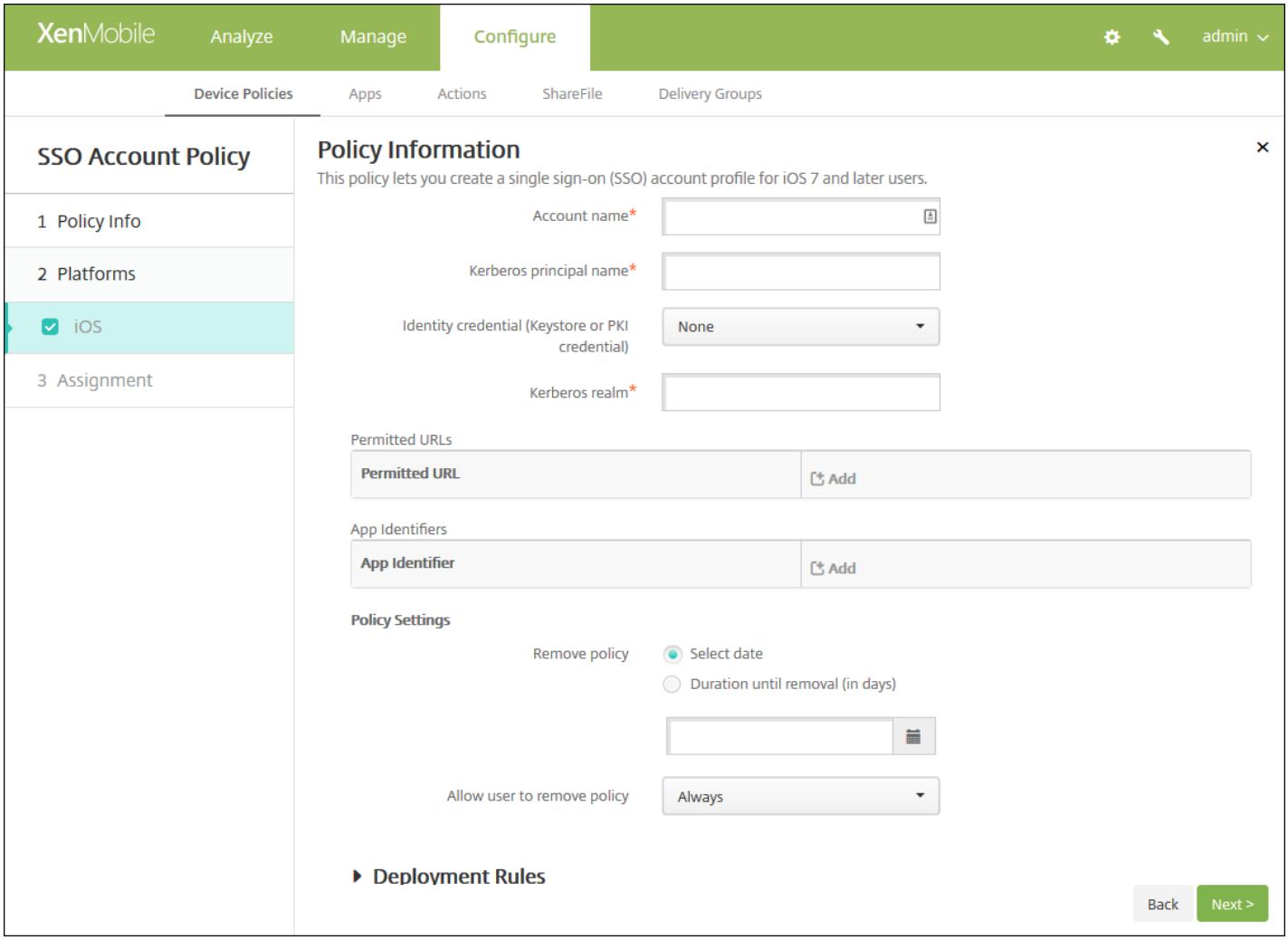
3. Click **More** and then, under **End user**, click **SSO Account**. The **SSO Account Policy** page appears.



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.

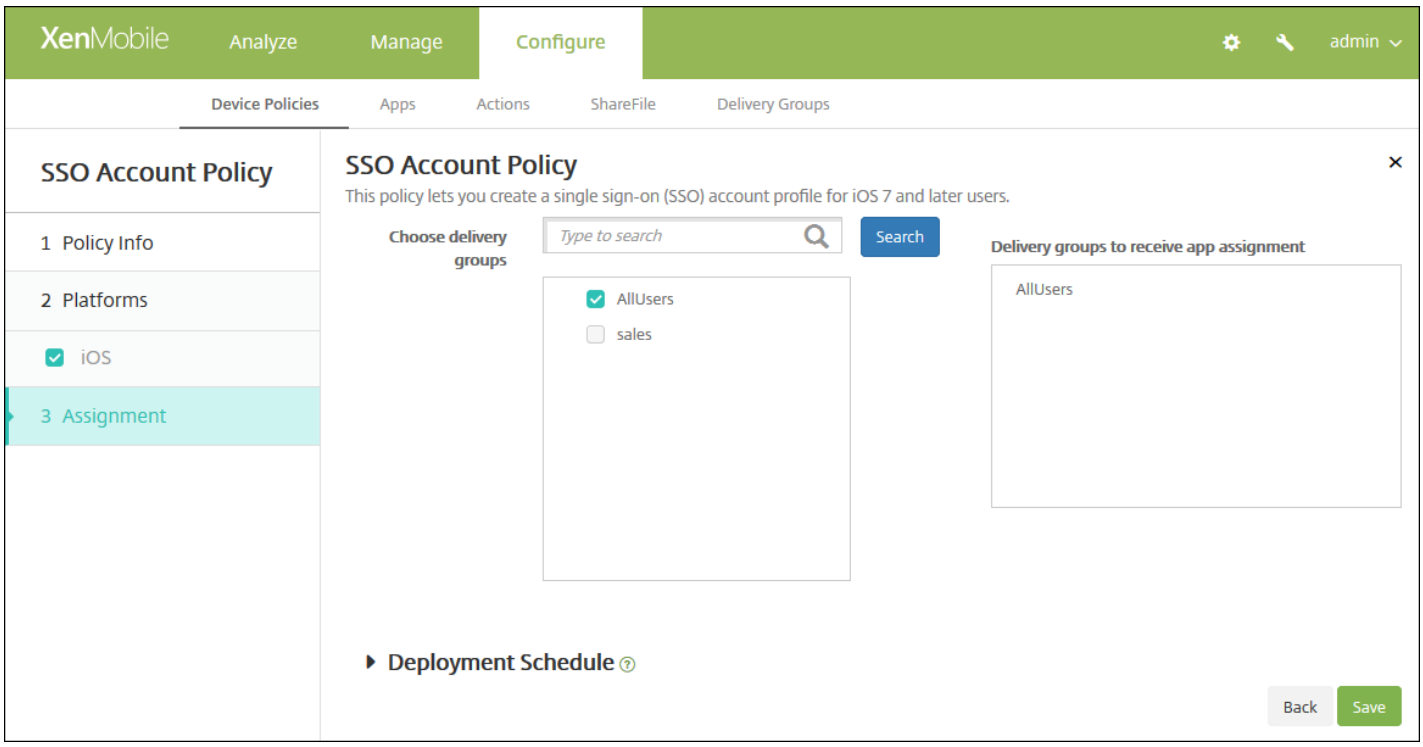
  Note: To delete an existing URL or app identifier, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing.

  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**.

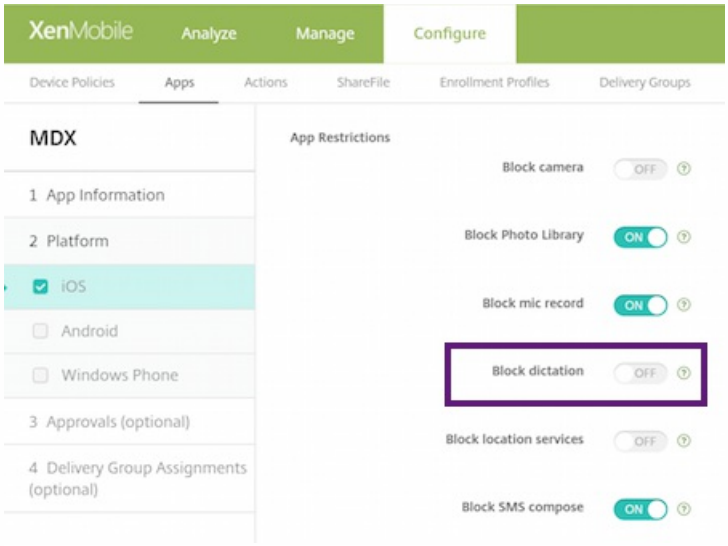
Siri and dictation policies

Jul 12, 2016

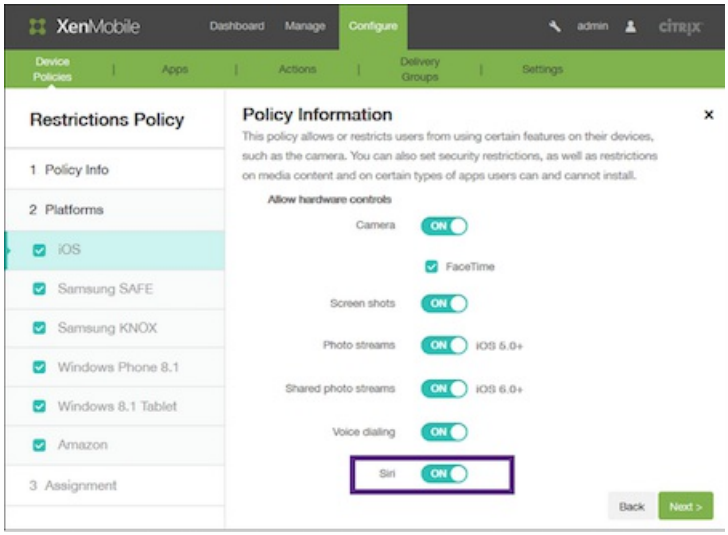
When users ask Siri something or dictate text on managed iOS devices, Apple collects the voice data for purposes of improving Siri. The voice data passes through Apple's cloud-based services, and therefore exists outside the secure XenMobile container. The text that results from dictation, however, remains 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 policies

Apr 08, 2015

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

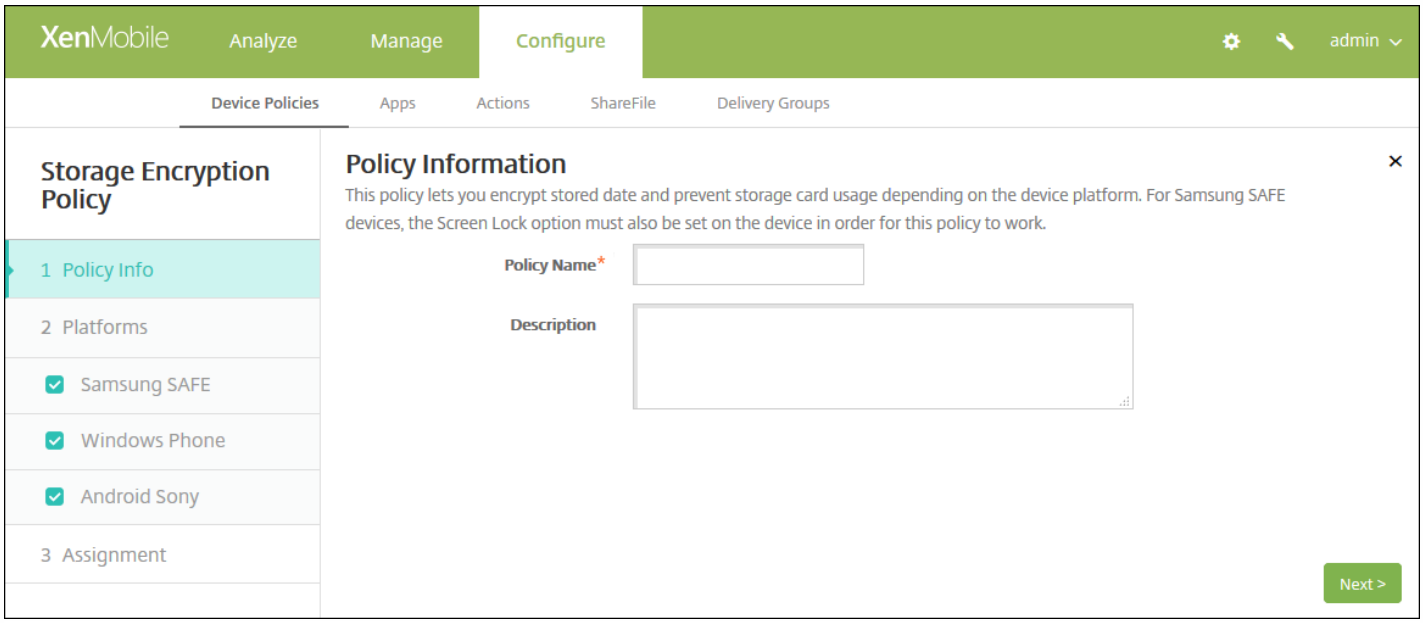
Note: For Samsung SAFE devices, before configuring this policy, make sure the following requirements are met:

- 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:

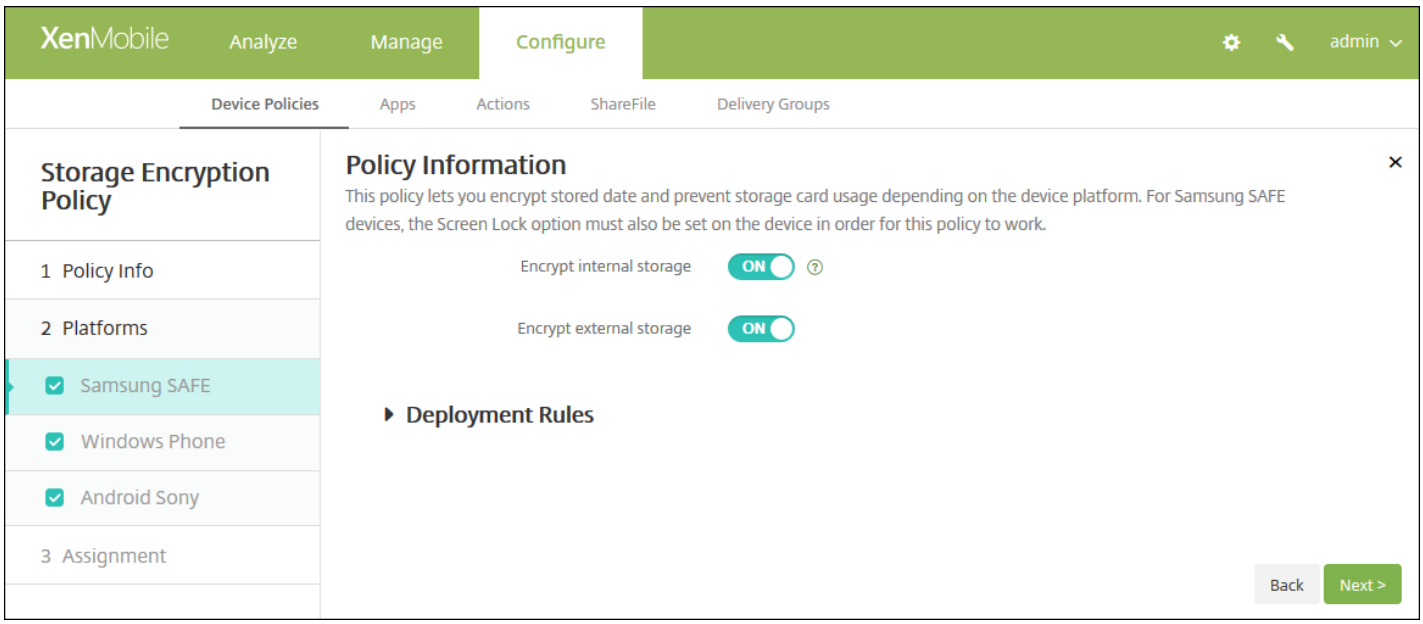
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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.

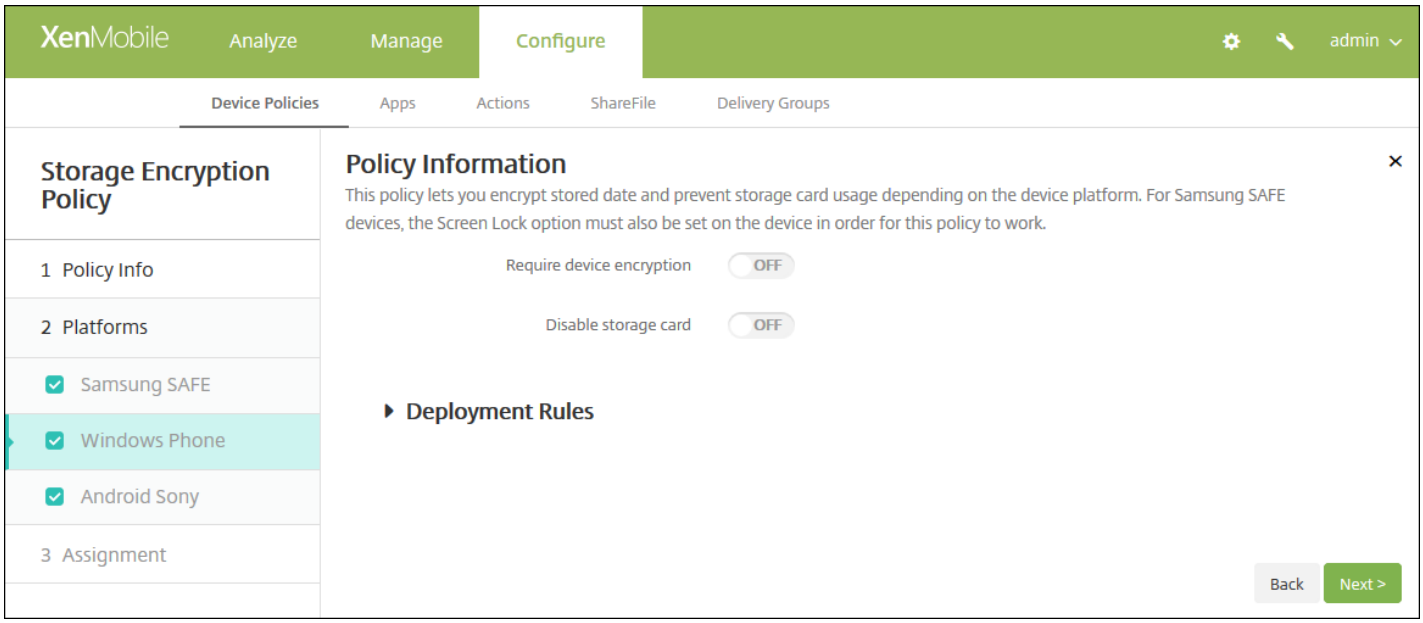
Configure Samsung SAFE settings



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**.

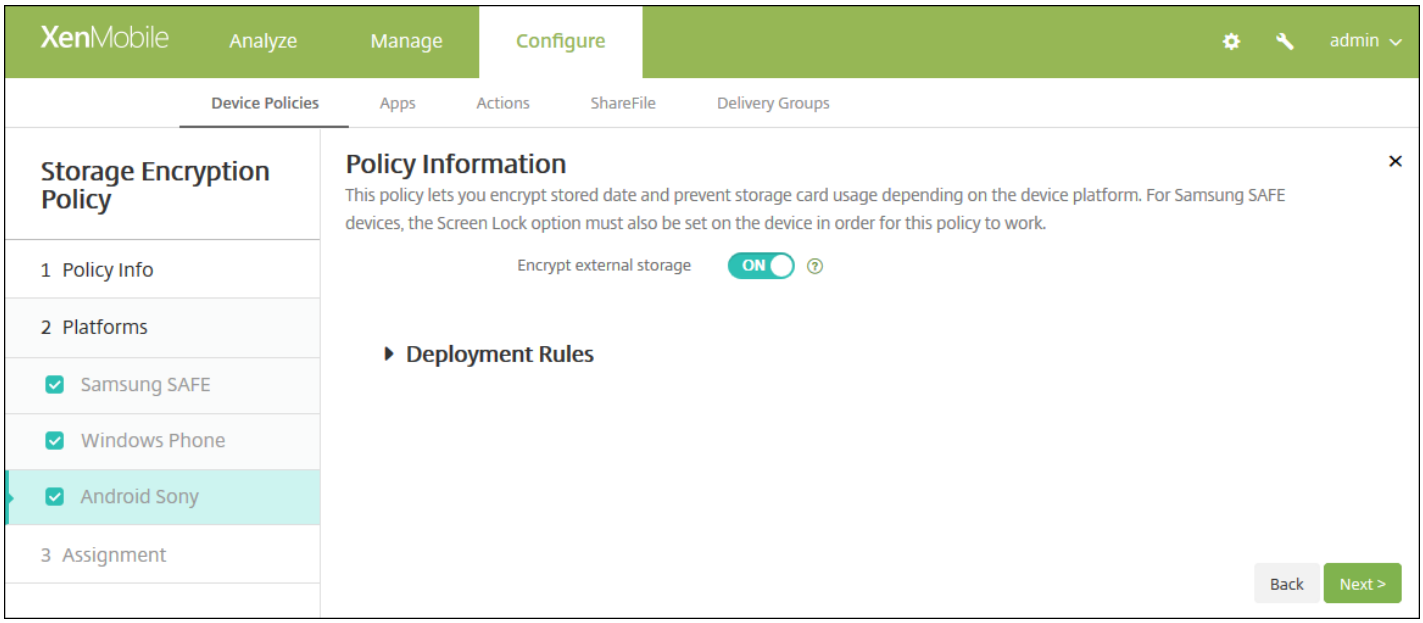
Configure Windows Phone settings



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

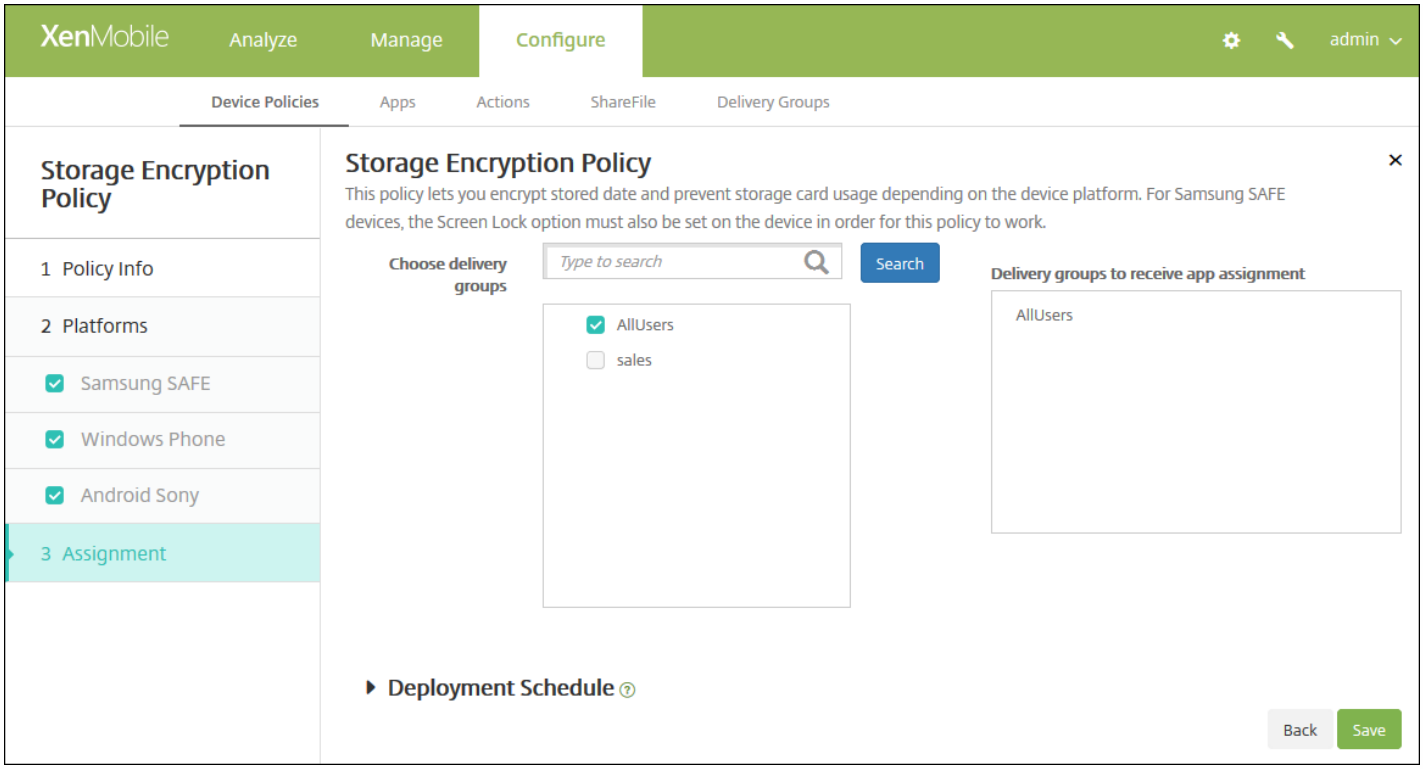


Configure this setting:

- **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

Feb 13, 2015

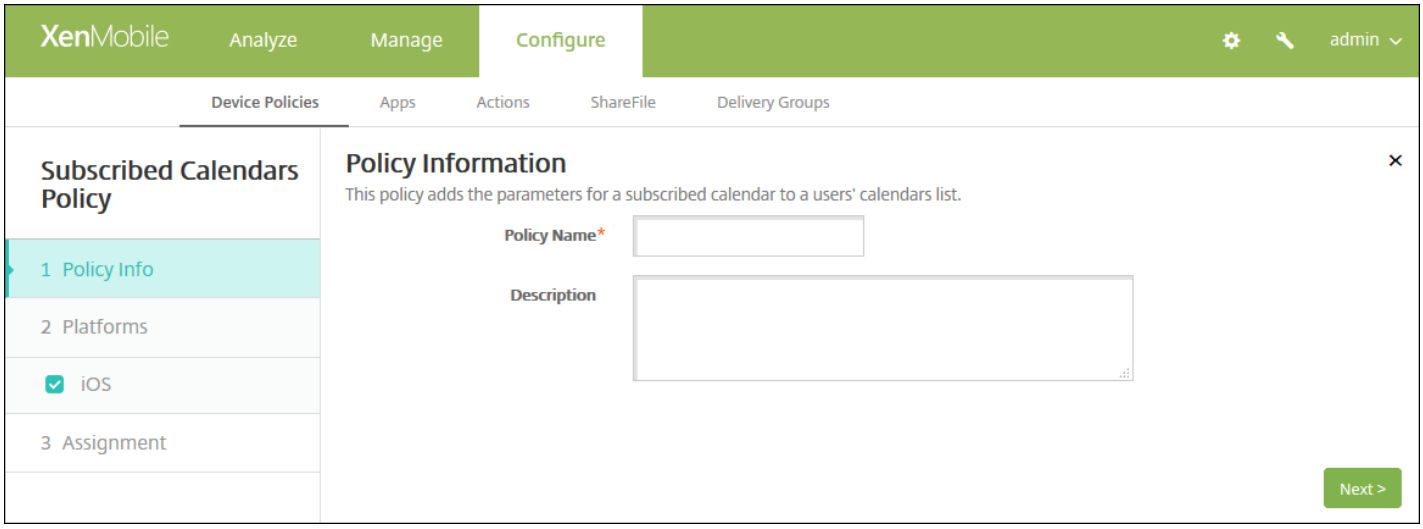
You can add a device policy in XenMobile to add a subscribed calendar to the calendars list on users' iOS devices. The list of public calendars to which you can subscribe is available at www.apple.com/downloads/macosx/calendars.

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.

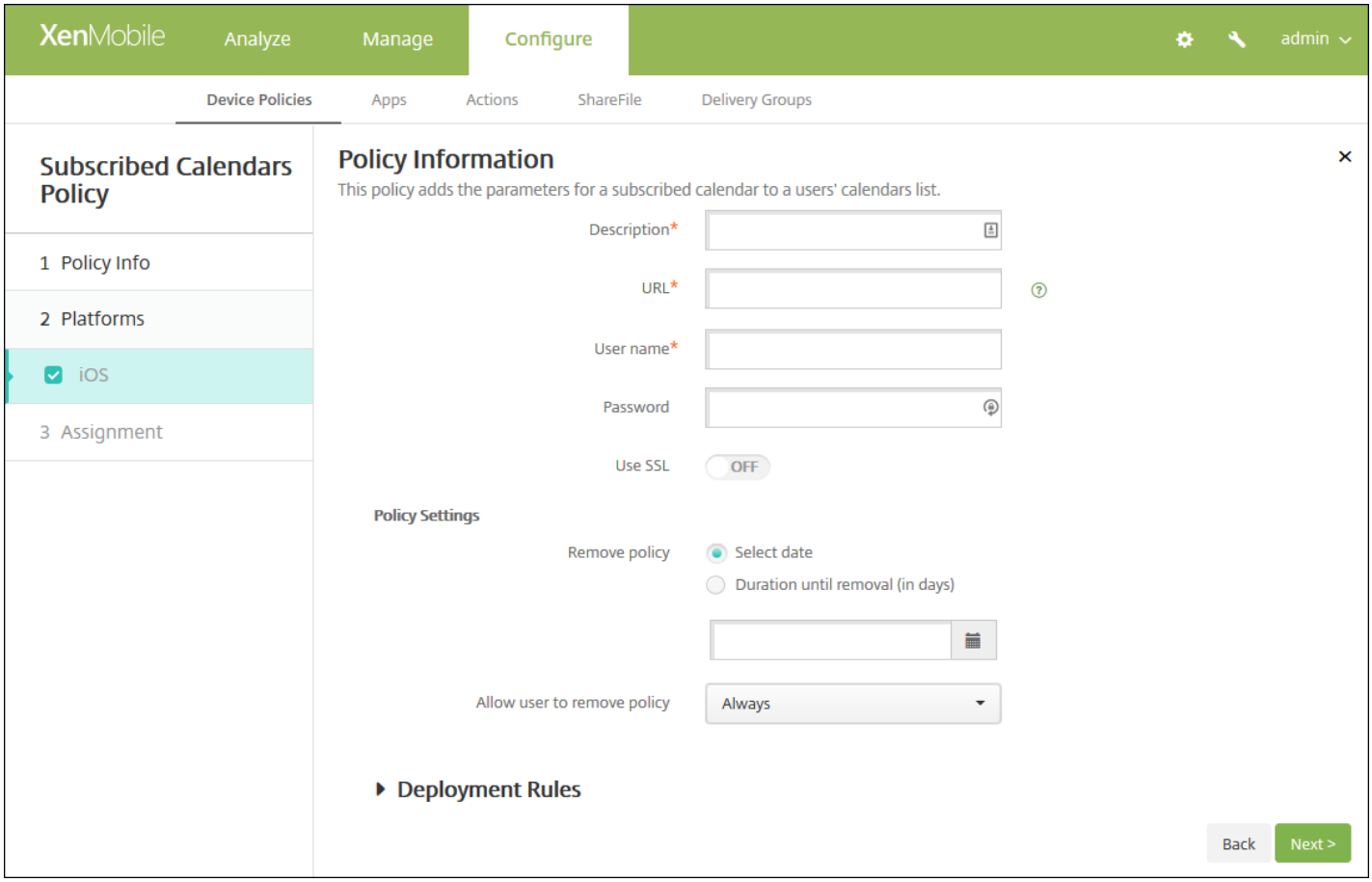
3. Click **More** and then, under **End user**, click **Subscribed Calendars**. The **Subscribed Calendars Policy** page appears.



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.

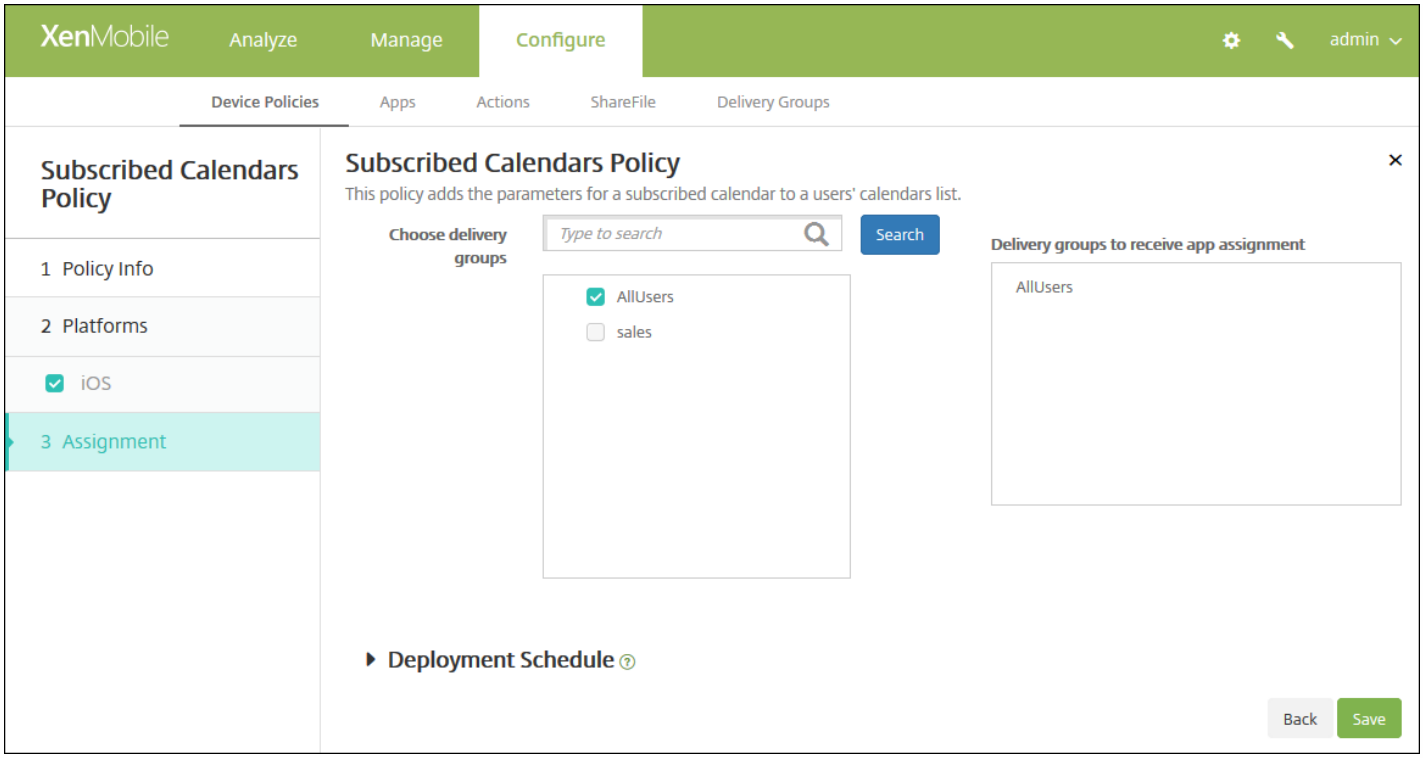


6. Configure these settings:

- **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 policies

Mar 04, 2015

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.

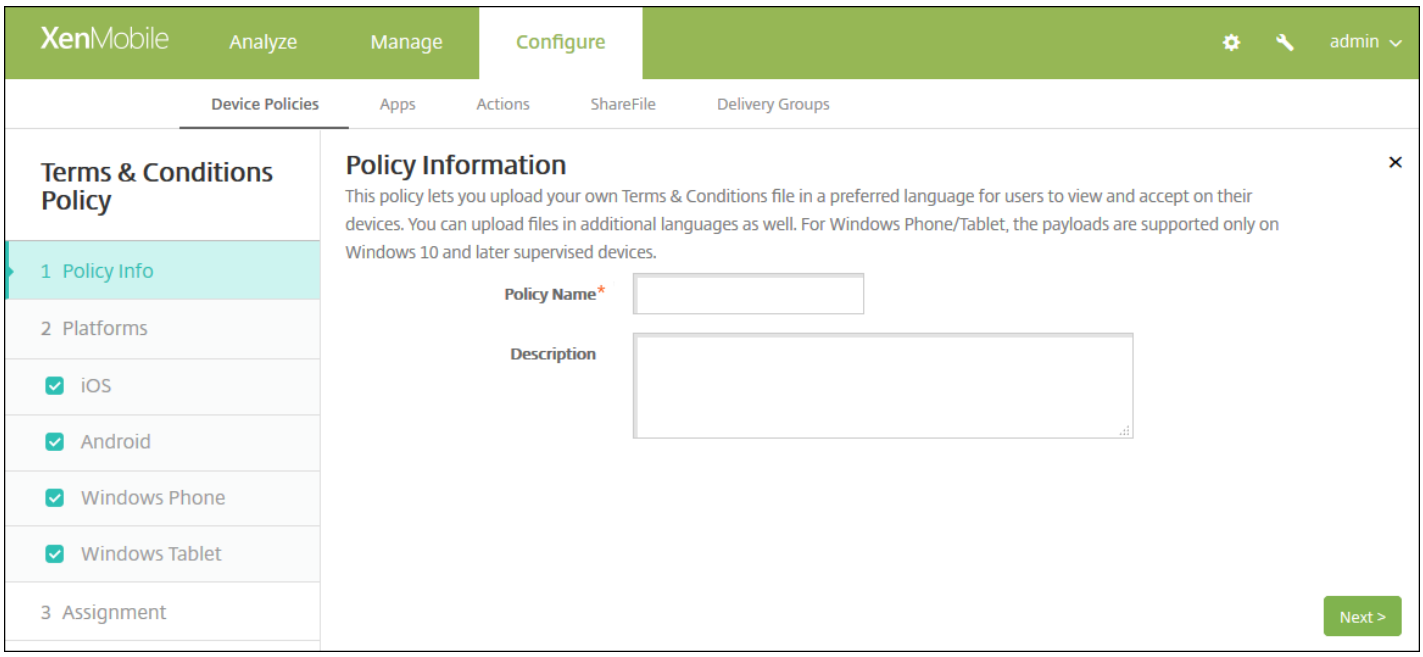
iOS and Android settings

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.

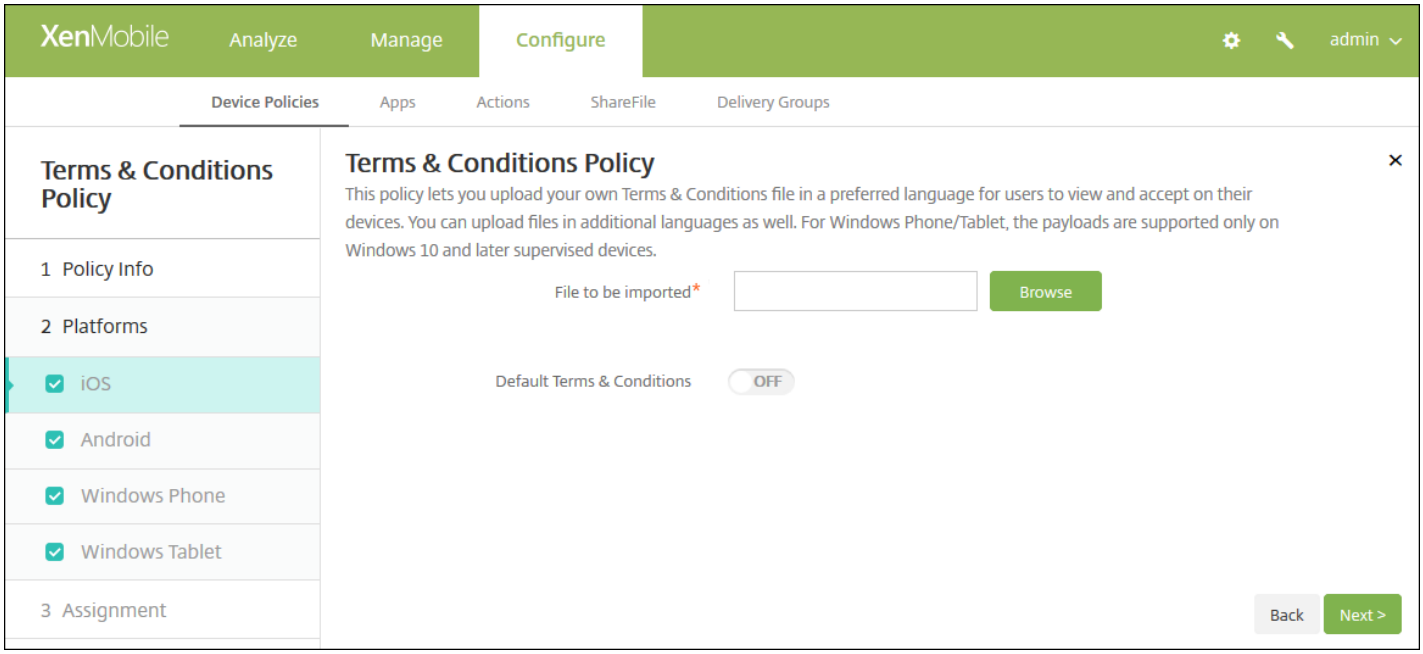
3. Click **Terms & Conditions**. The **Terms & Conditions Policy** page appears.



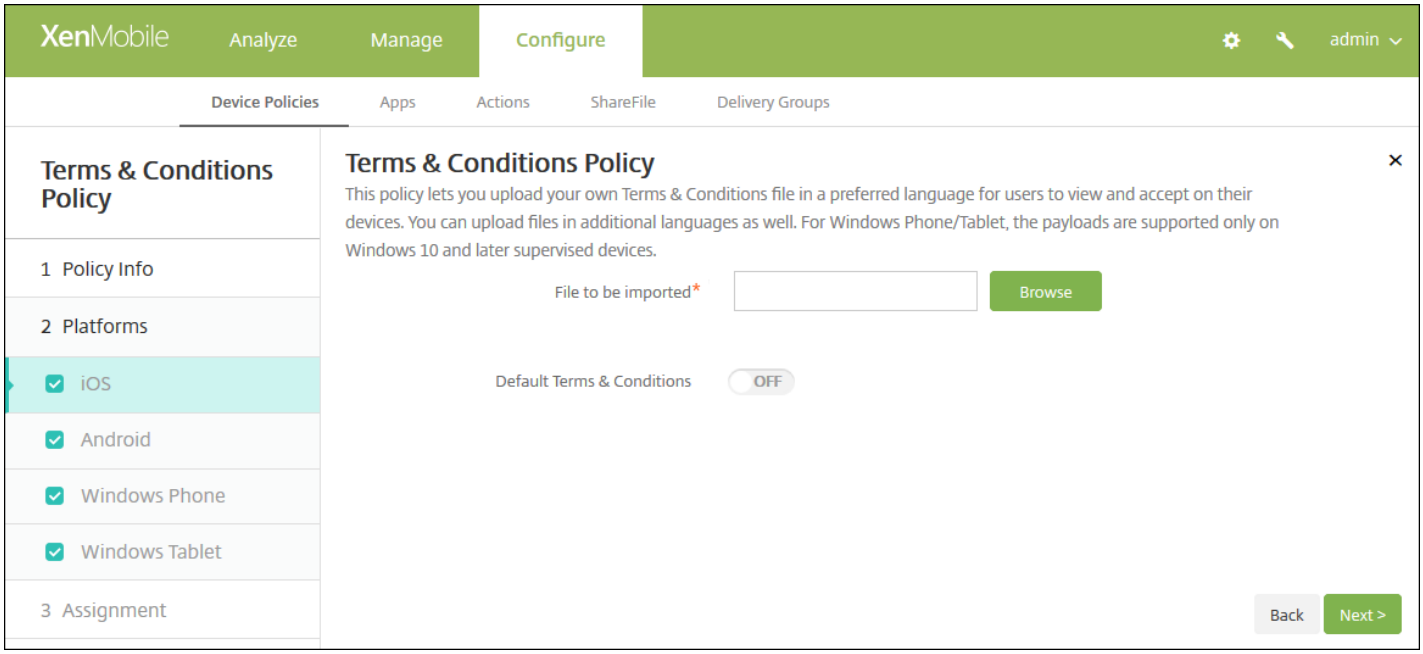
4. In the **Policy Information** pane, enter the following information:

- **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.



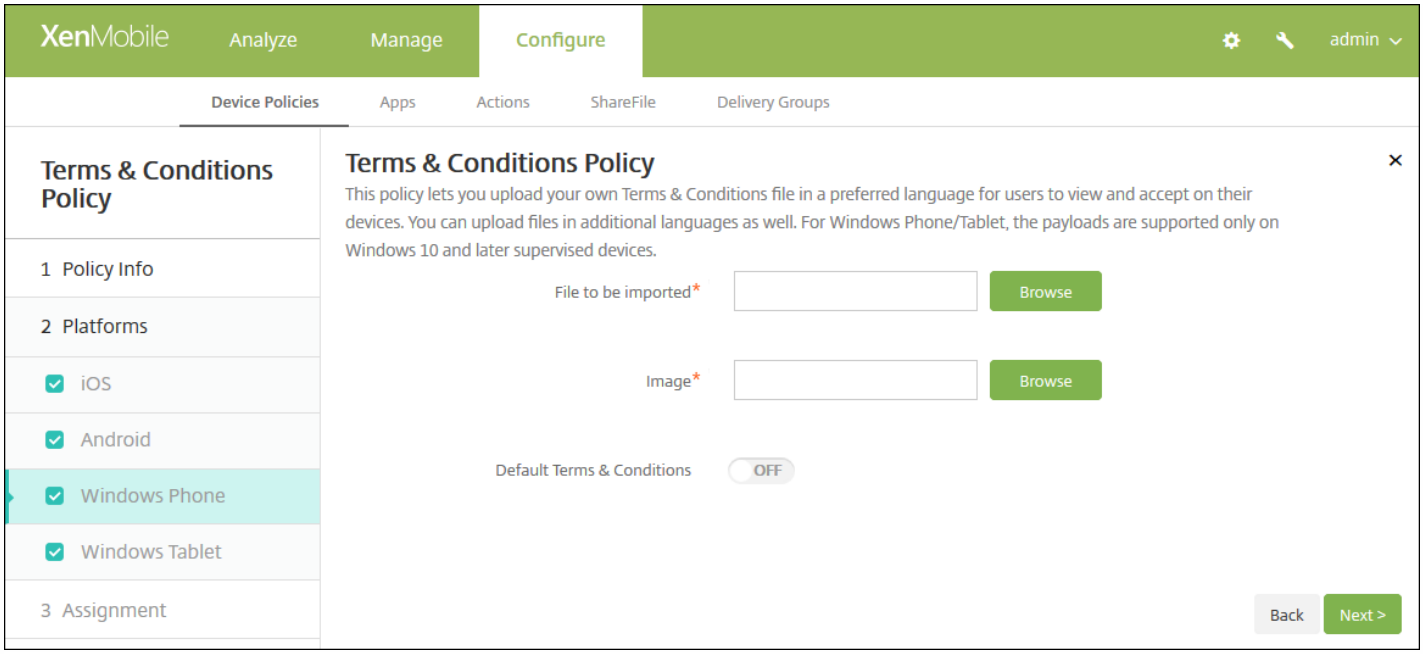
iOS and Android settings



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**.

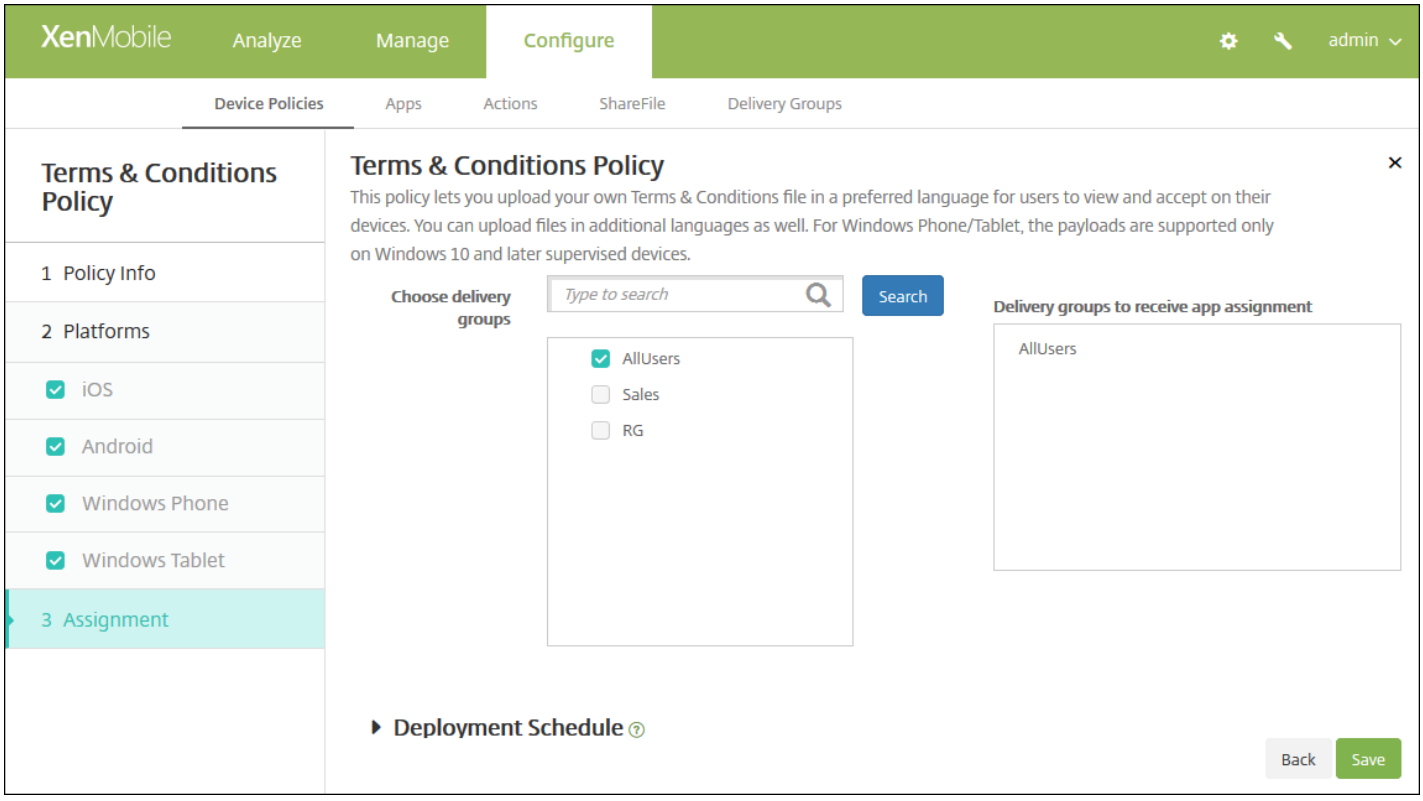
Windows Phone and Windows Tablet settings



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

Oct 21, 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 policies

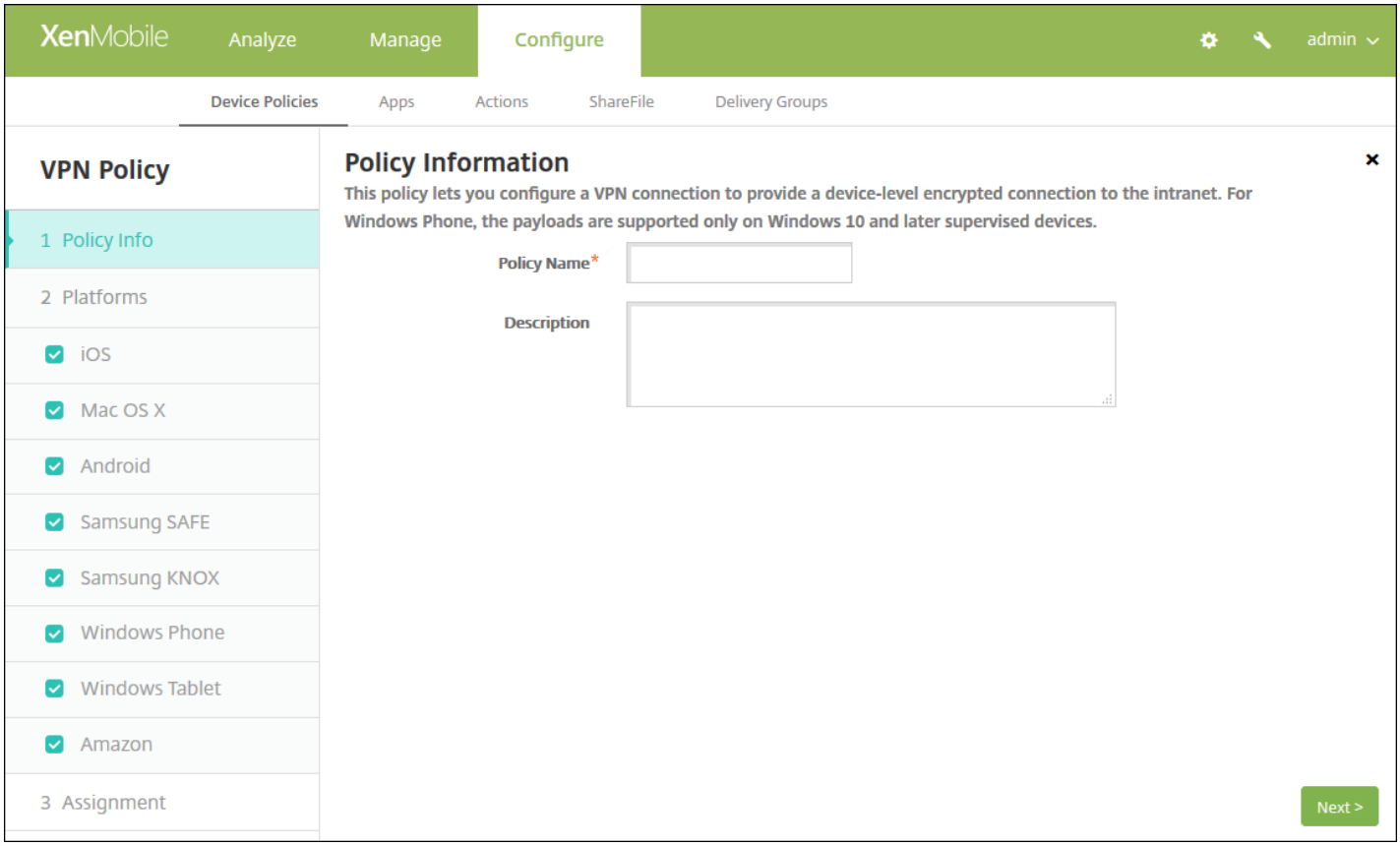
Sep 29, 2016

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:

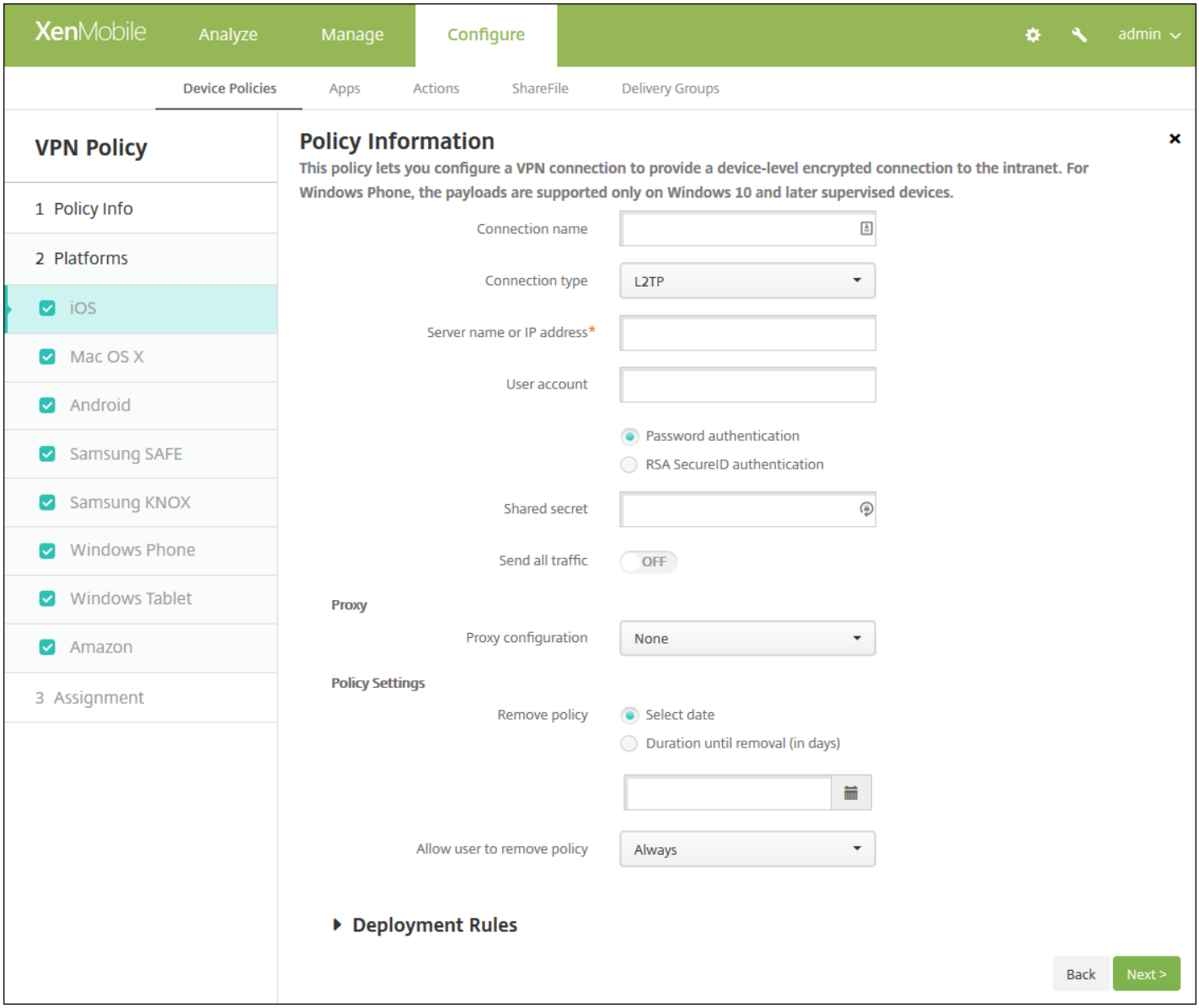
- **Policy Name**: Type a descriptive name for the policy.
- **Description**: Type an optional description of the policy.

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

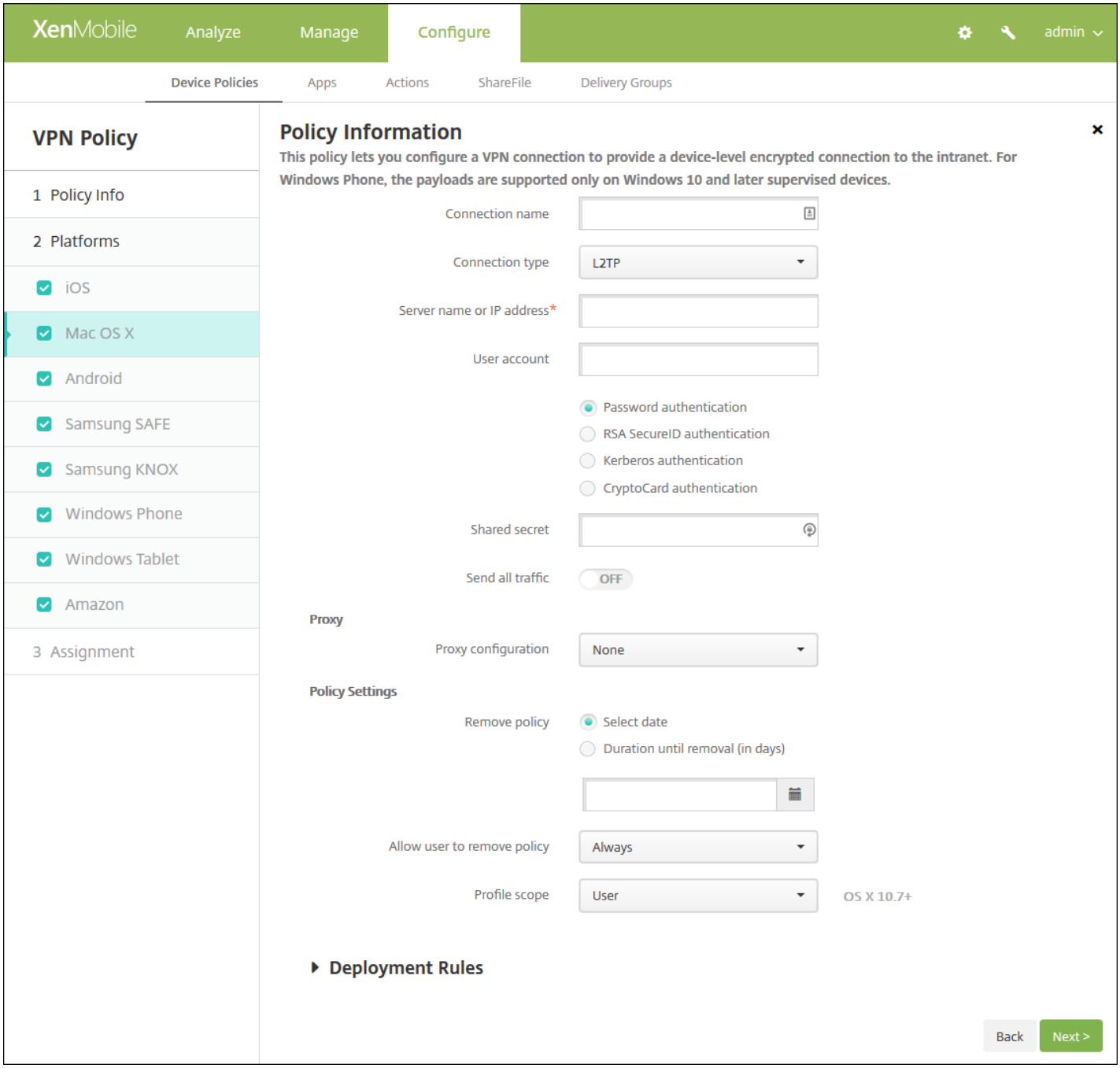
Configure Citrix VPN protocol

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

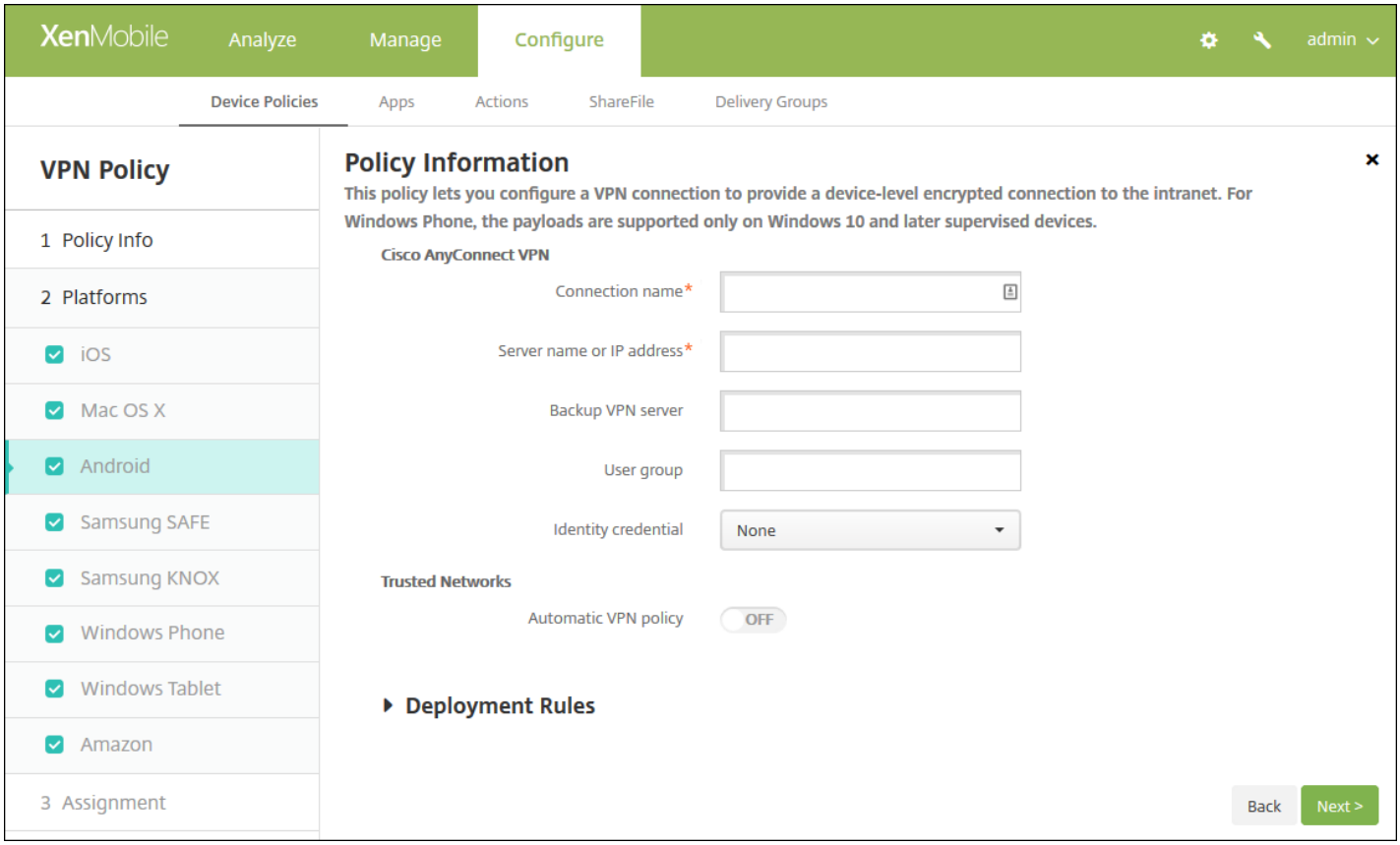
Configure Citrix VPN protocol

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:

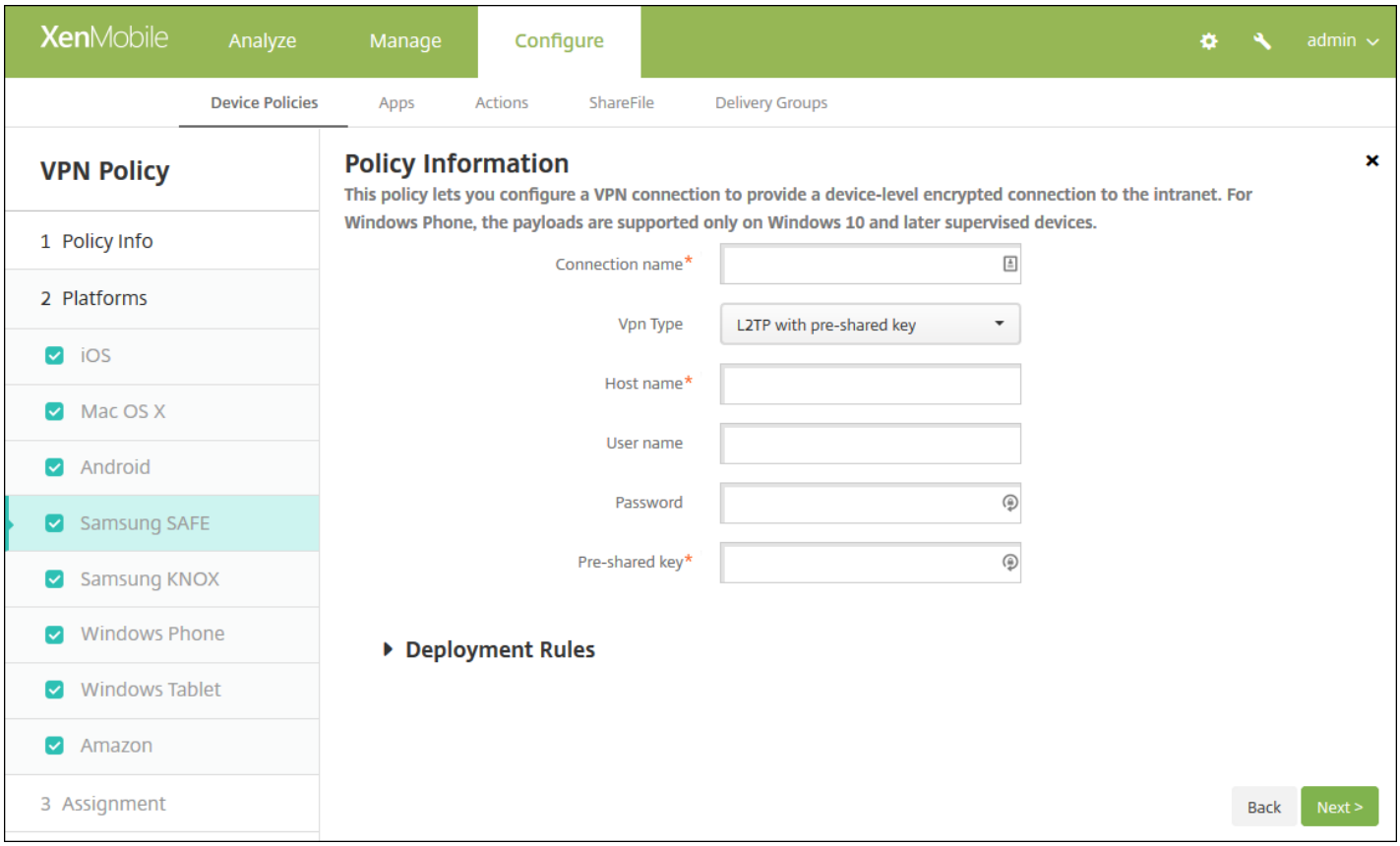
- **Domain**: Type the domain to be added.
- Click **Save** to save the domain or click **Cancel** to not save the domain.

- **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

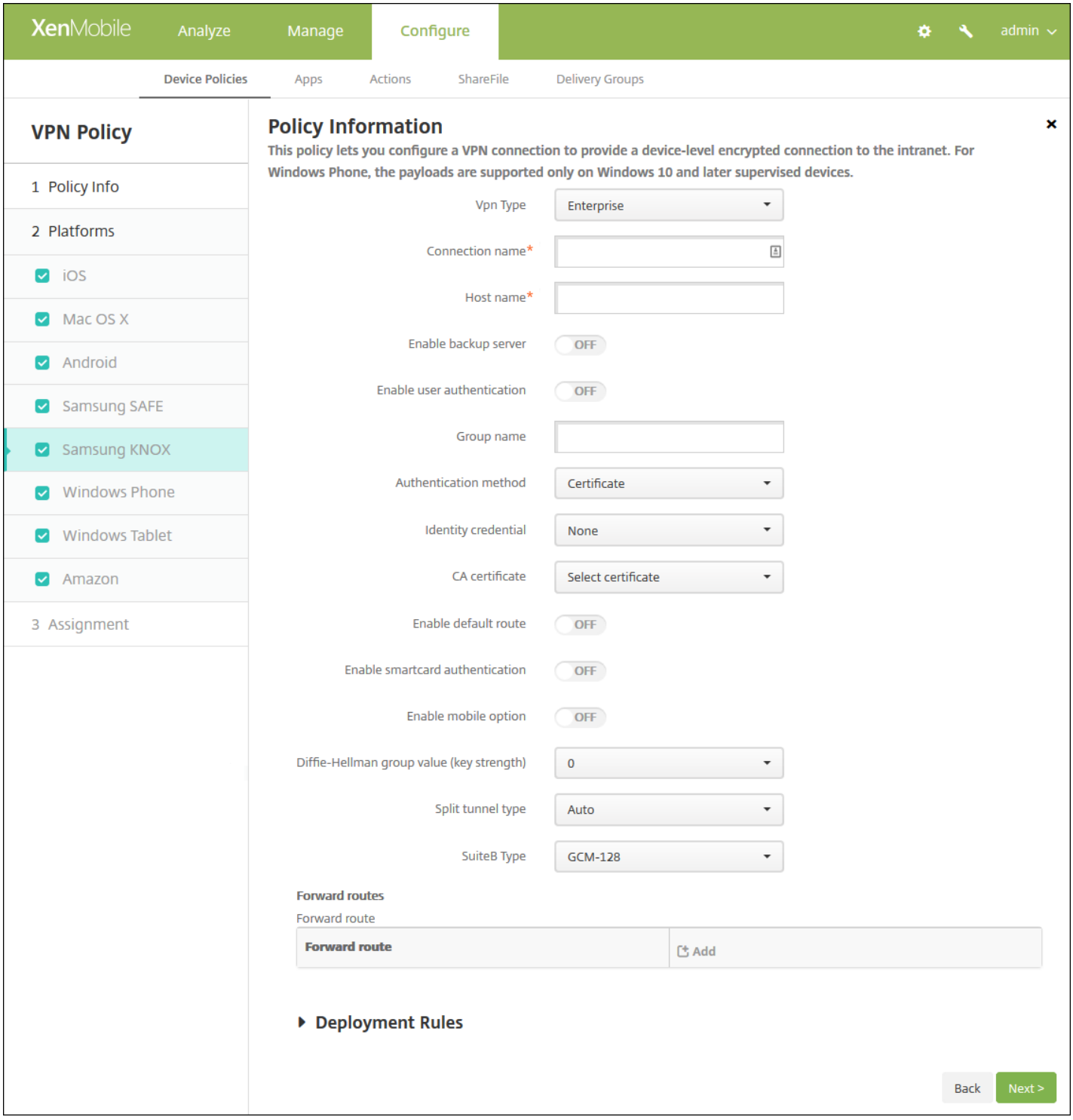
Configure L2TP with certificate protocol

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:

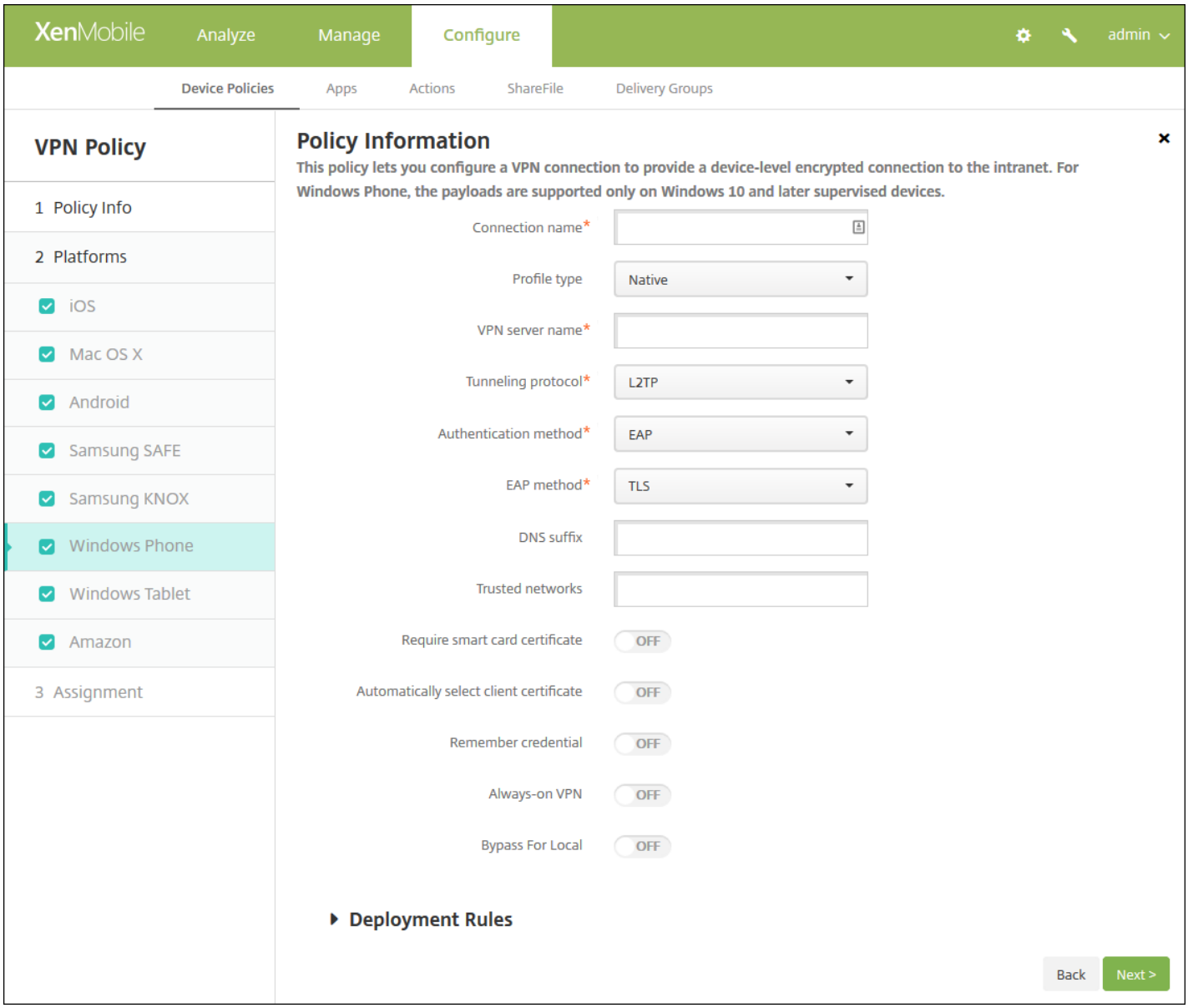
- **Vpn Type**: In the list, click either **Enterprise** (applicable to KNOX versions earlier than 2.0) or **Generic** (applicable to KNOX versions 2.0 or higher) for the type of VPN connection to configure. The default is **Enterprise**.

The following sections list the configuration options for each of the preceding connection types.

Configure Enterprise protocol

Configure generic protocol

Configure Windows Phone settings



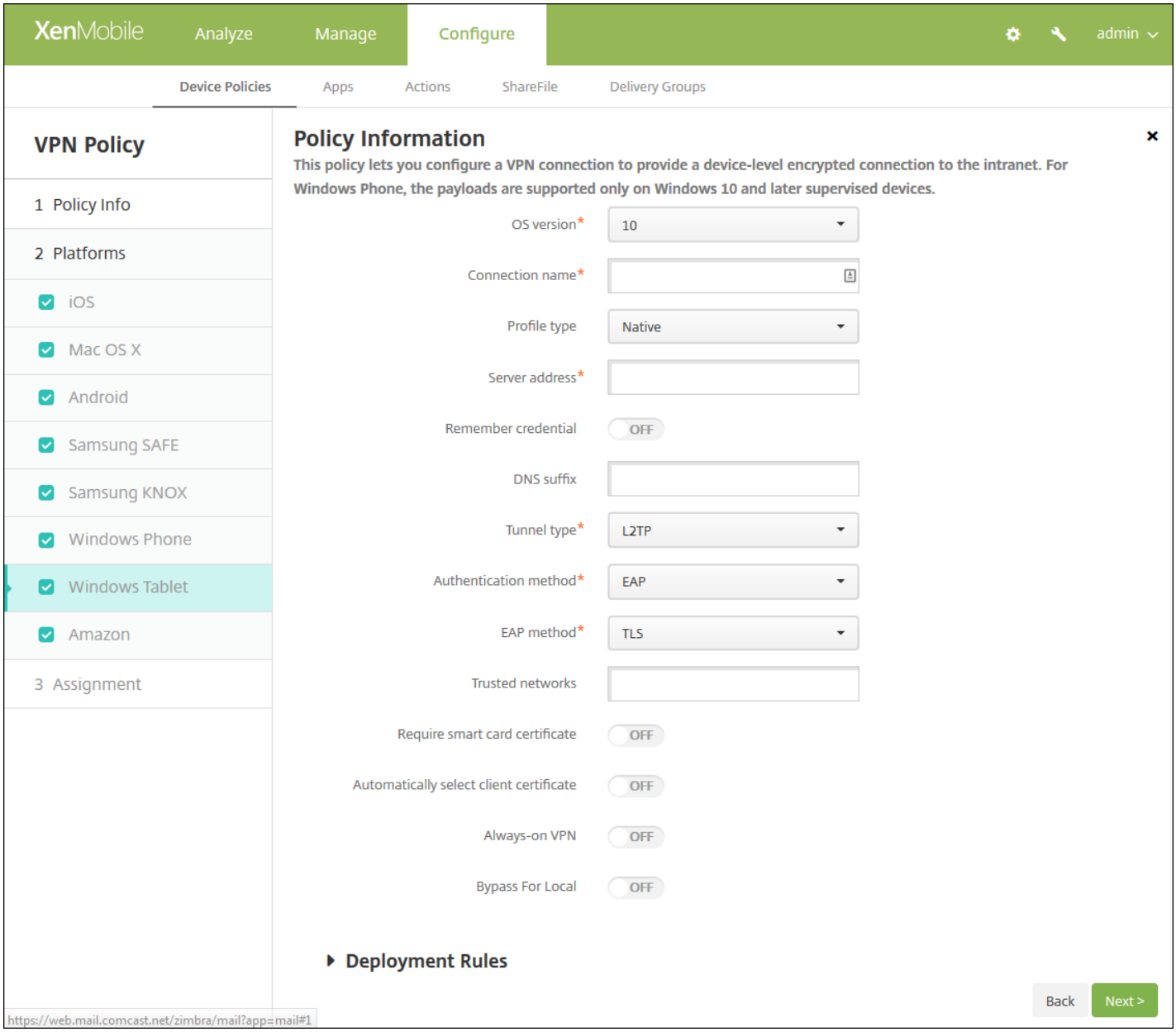
Note: These settings are supported only on Window 10 and later supervised phones.

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



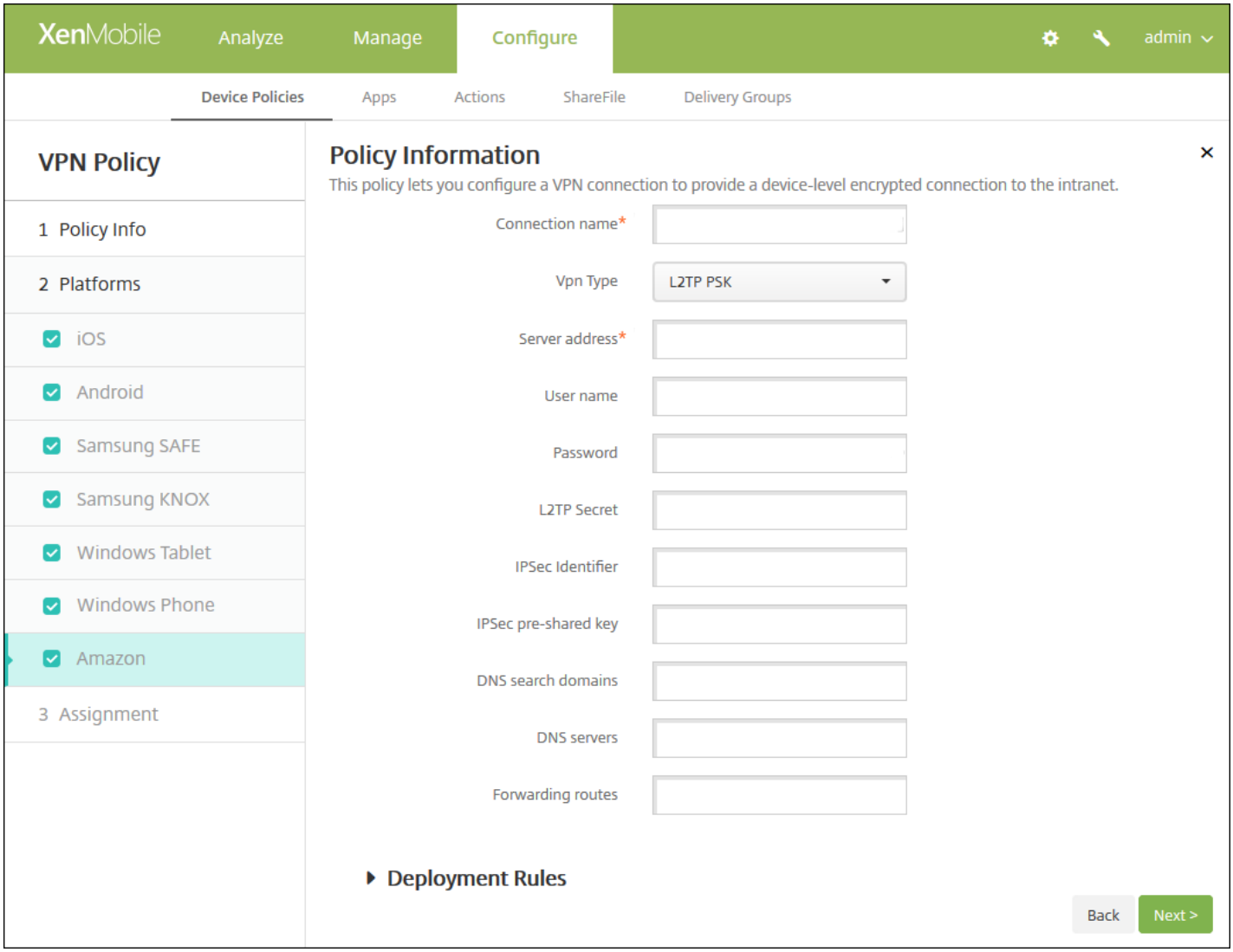
Configure these settings:

- **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

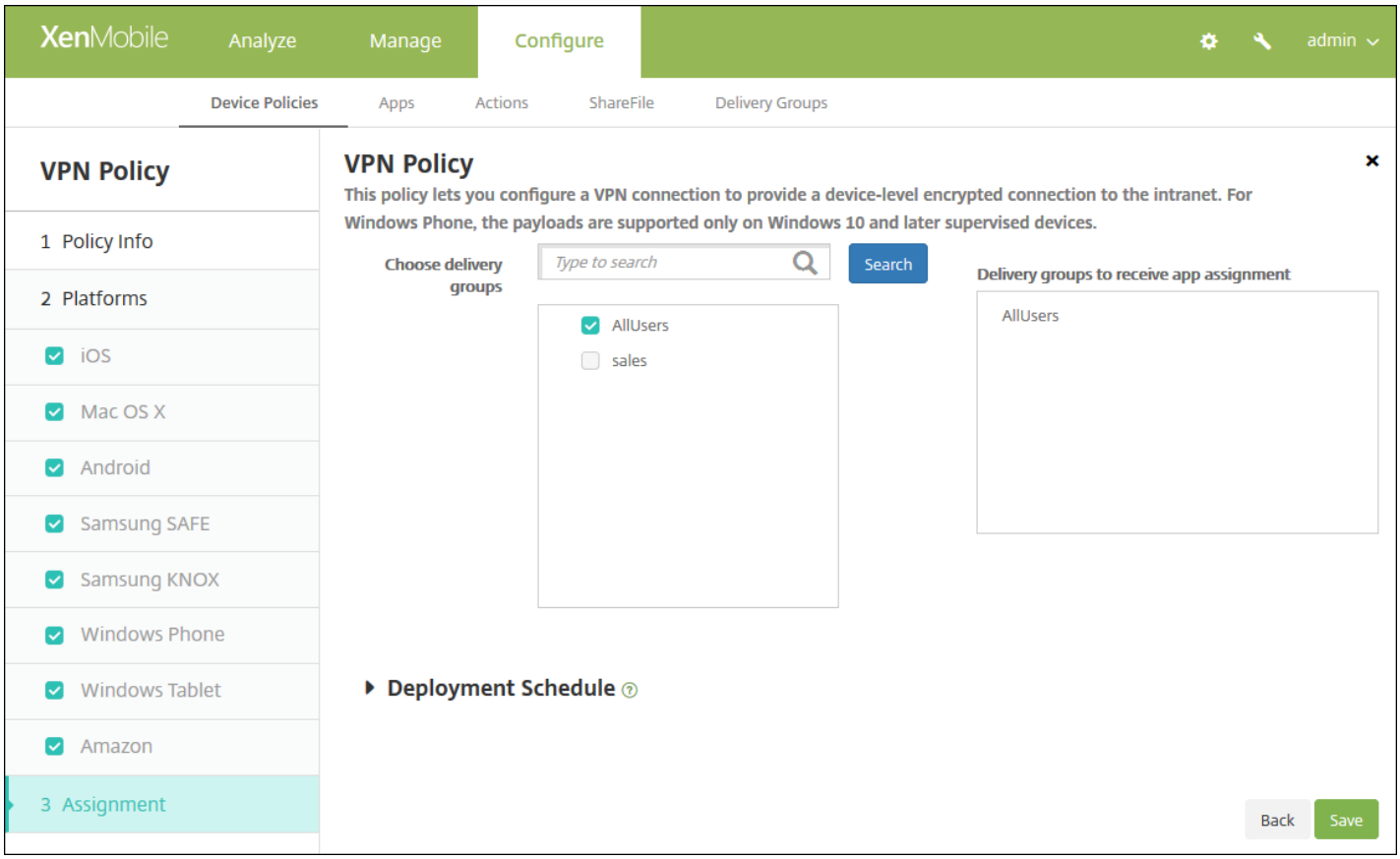
Configure IPSEC AUTH RSA settings

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

Sep 22, 2015

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.

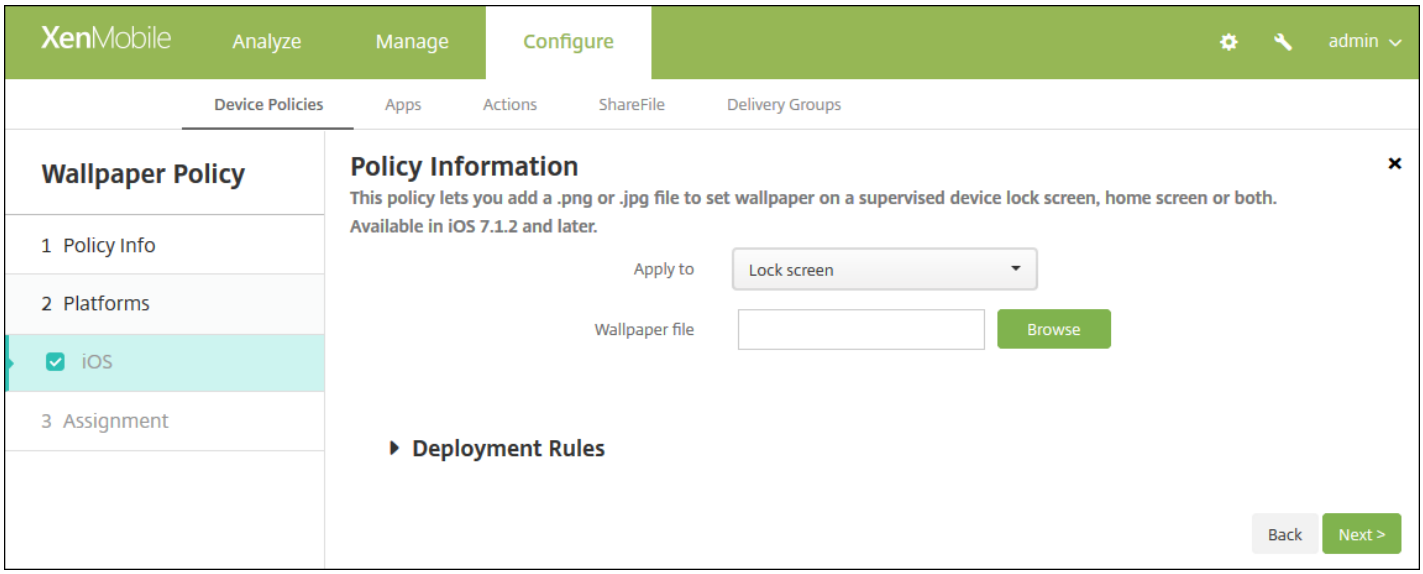
2. Click **Add**. The **Add a New Policy** dialog box appears.

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.

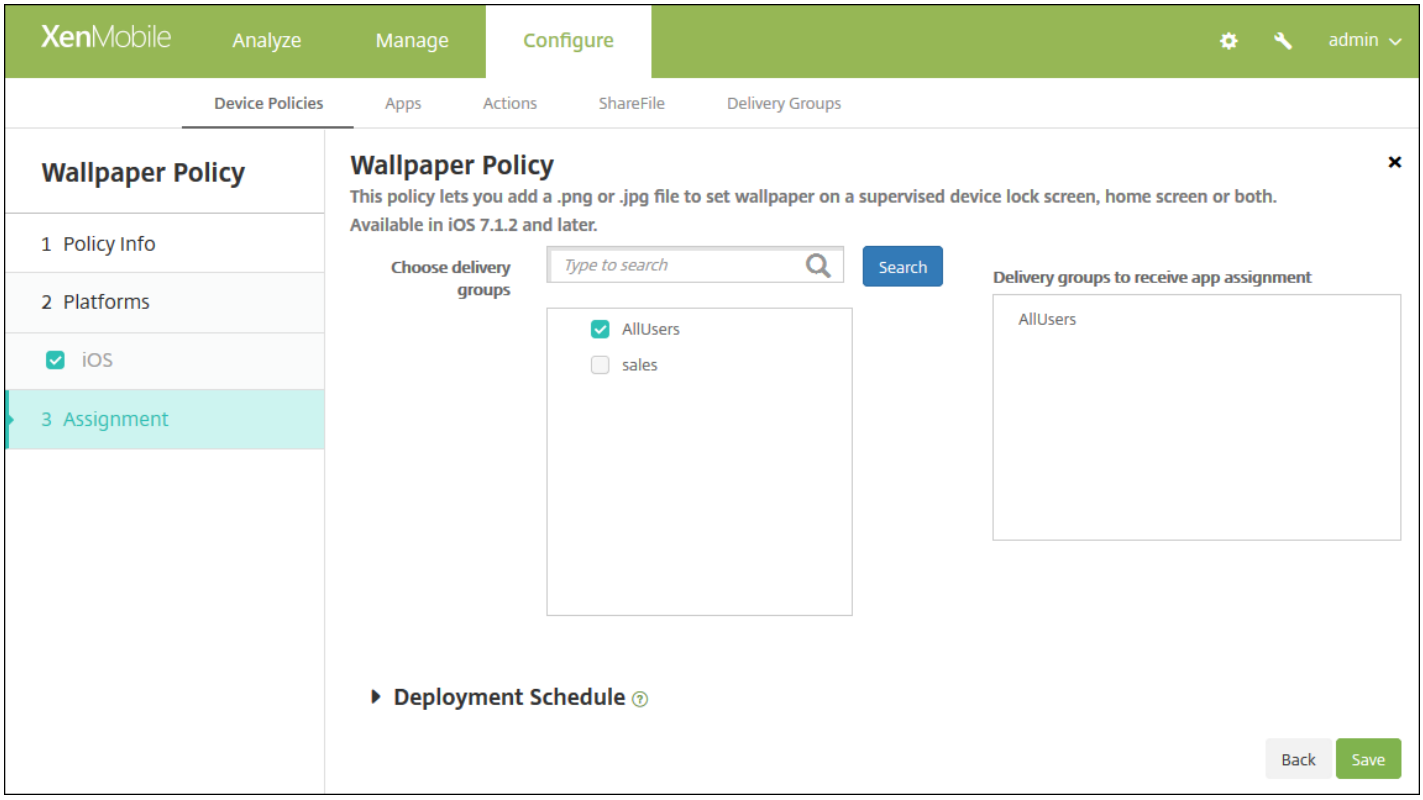


Configure these settings:

- **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 device policy

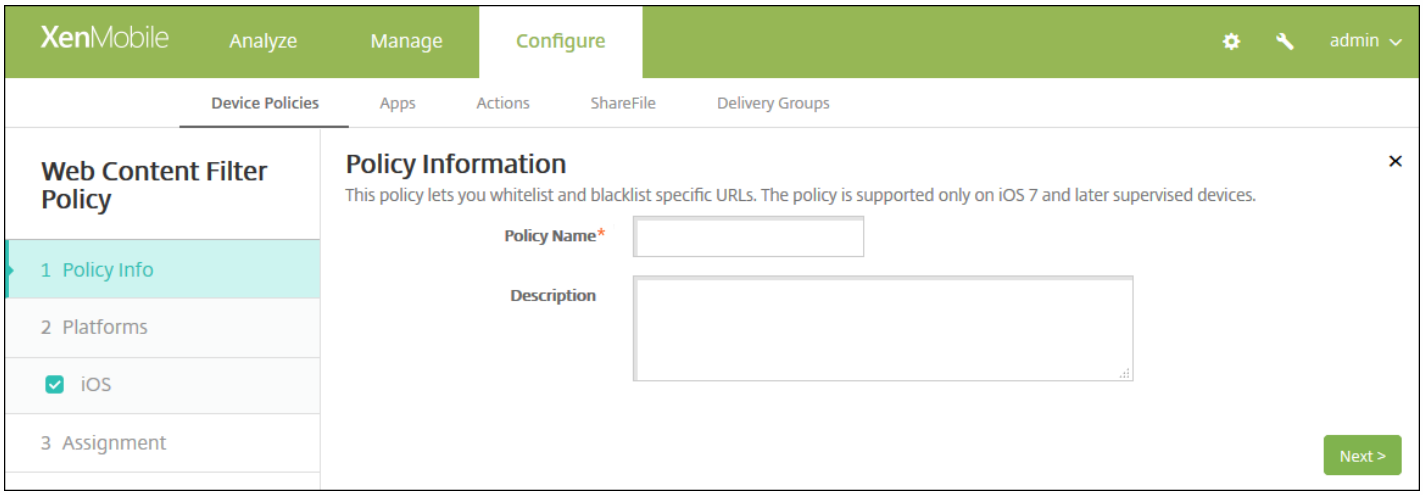
Mar 04, 2015

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.

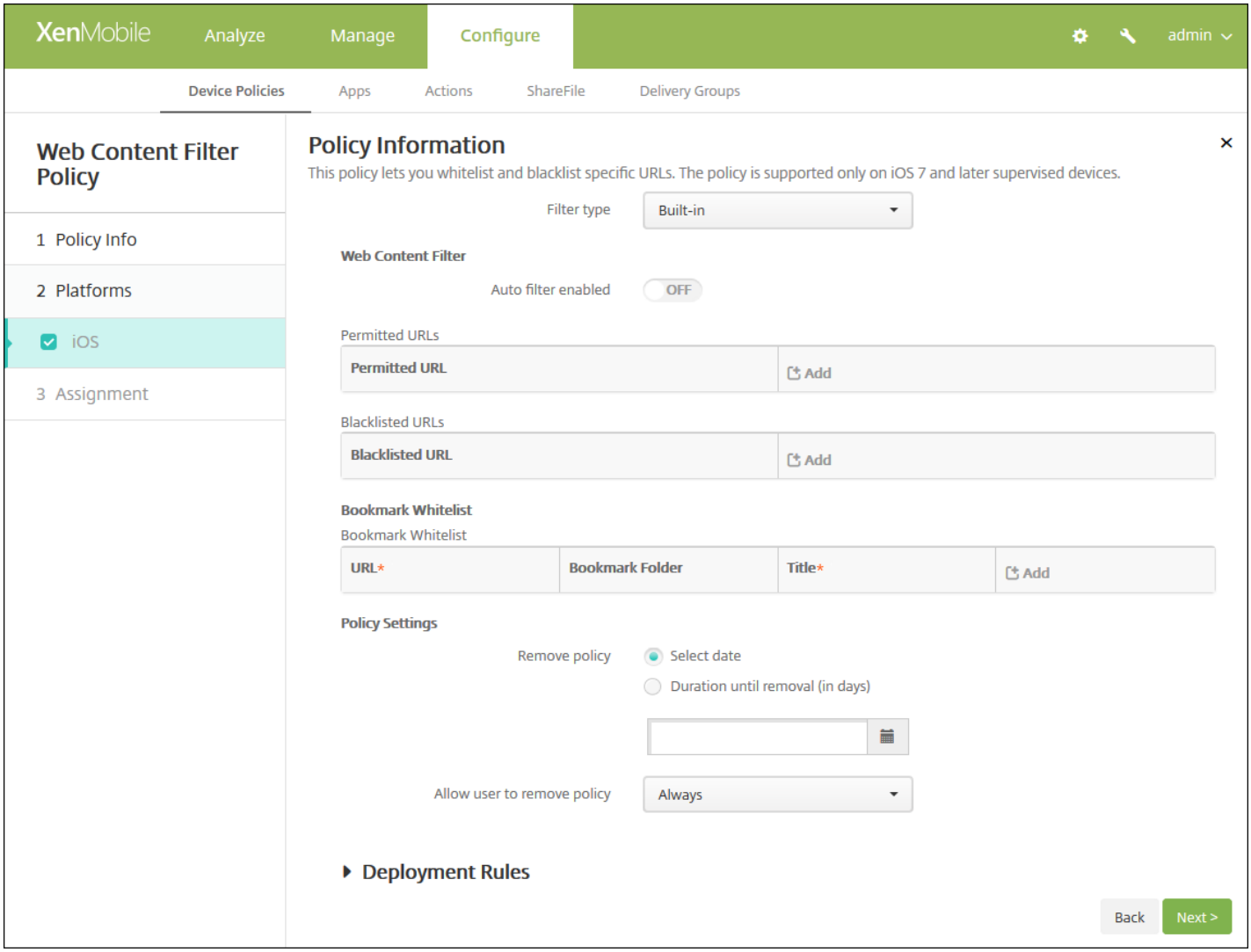
3. Click **More** and then, under **Security**, click **Web Content Filter**. The **Web Content Filter Policy** page appears.



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**.

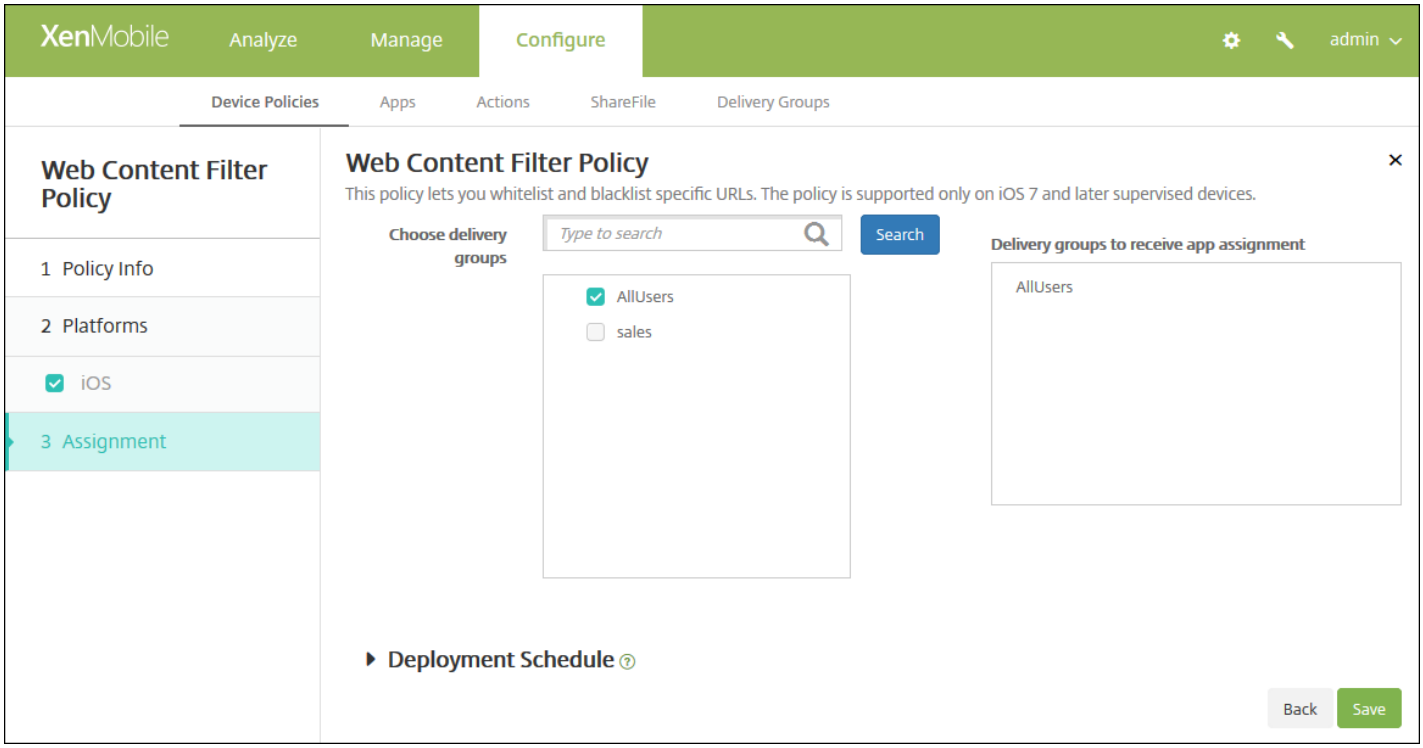
Built-in filter type settings

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.

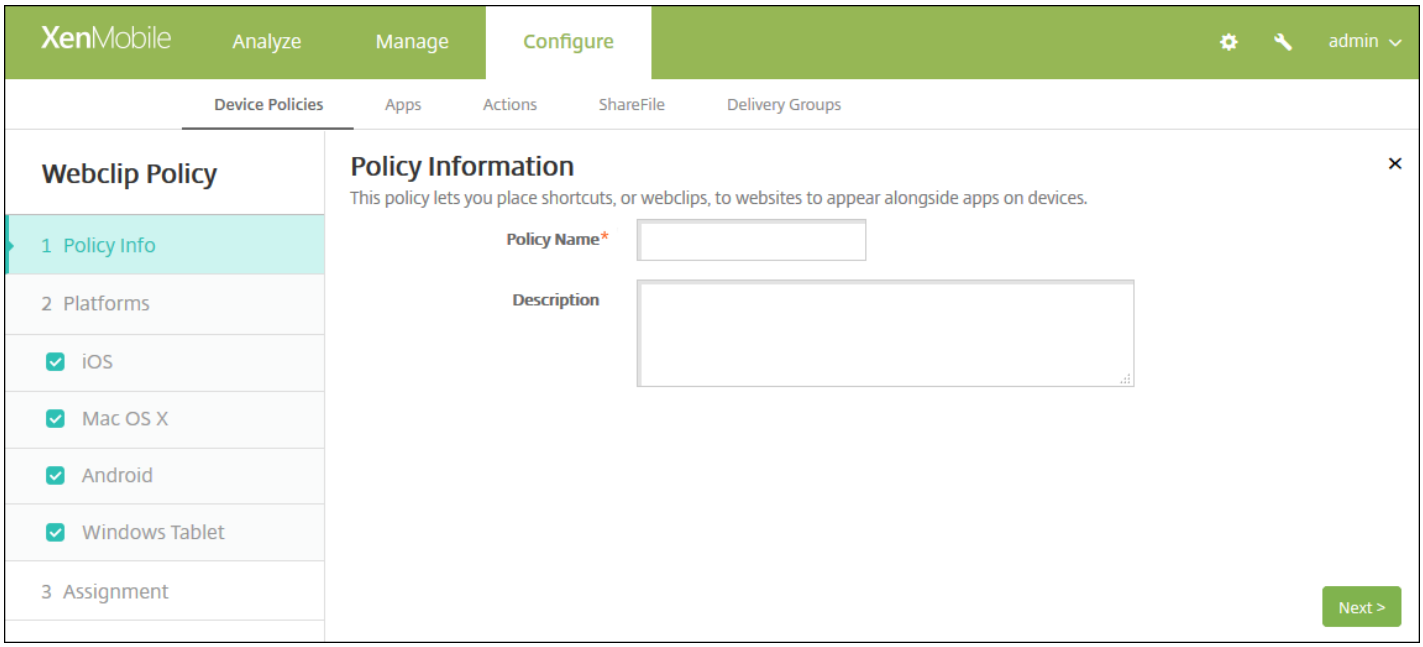
10. Expand **Deployment Schedule** and then configure the following settings:

- 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.**

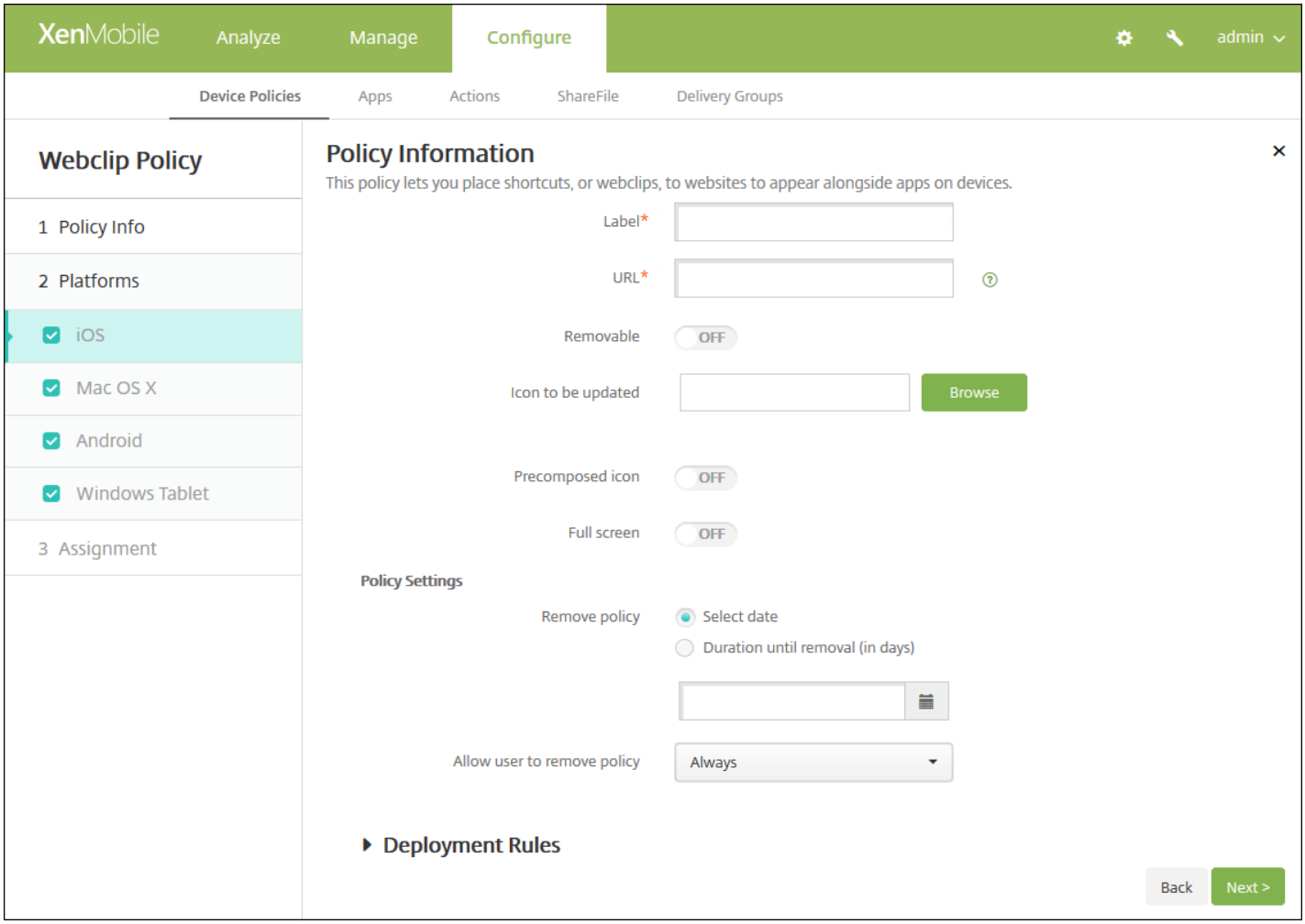
Note:

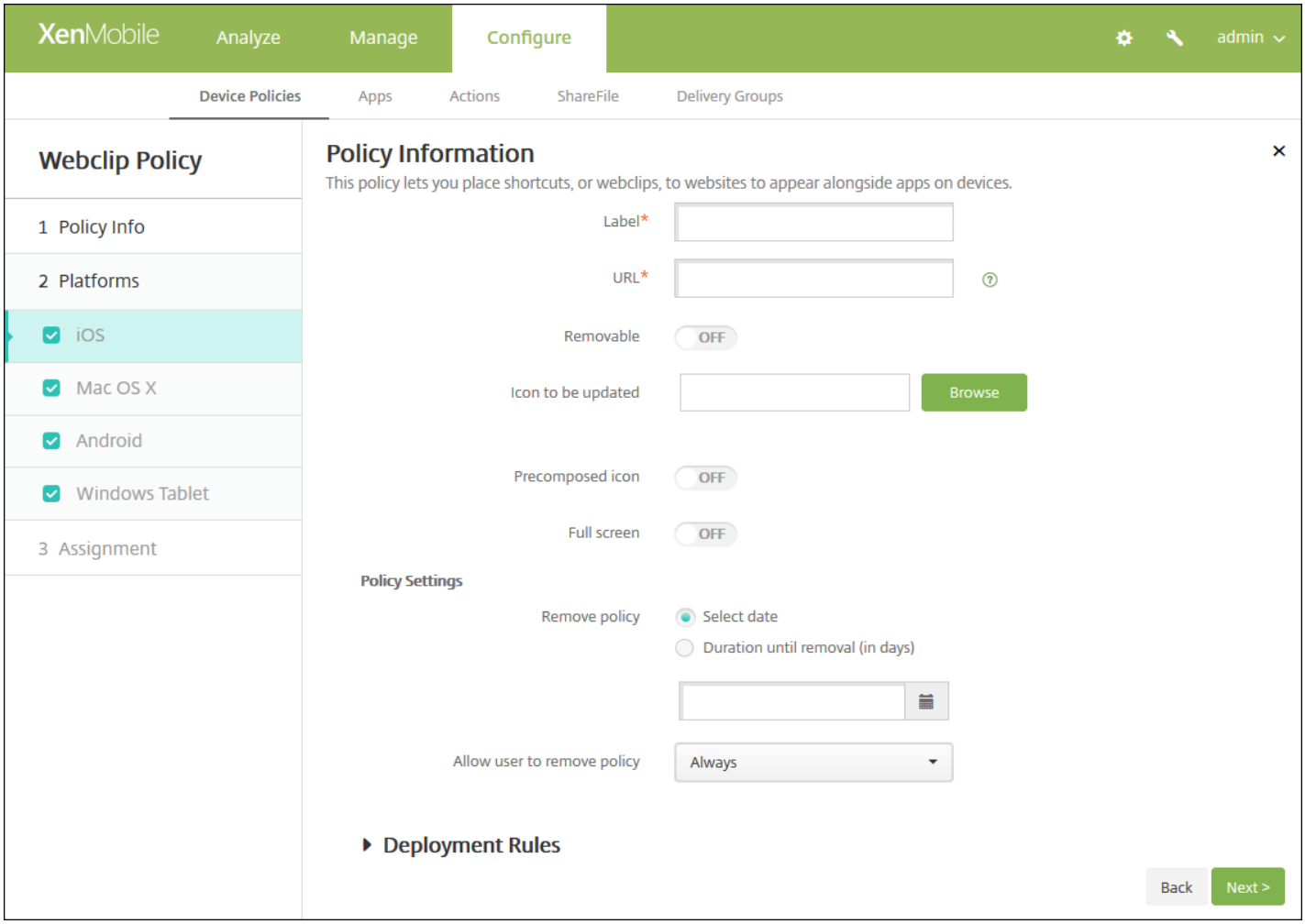
- This option applies when you have configured the scheduling background deployment key in **Settings** > **Server Properties**. The always-on option is not available for iOS devices.
- The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always on connection**, which does not apply to iOS.

11. Click **Save**.

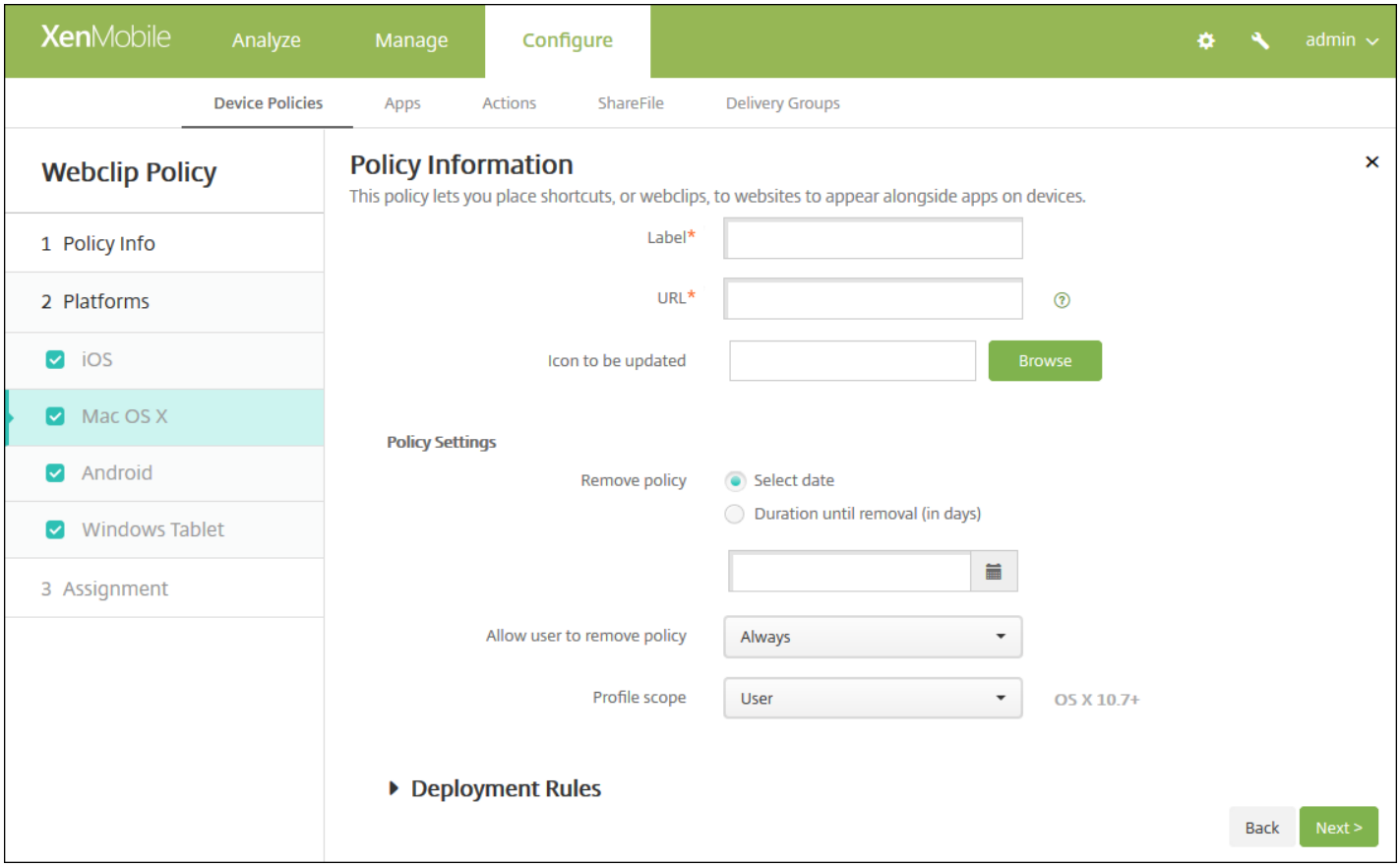


-
-

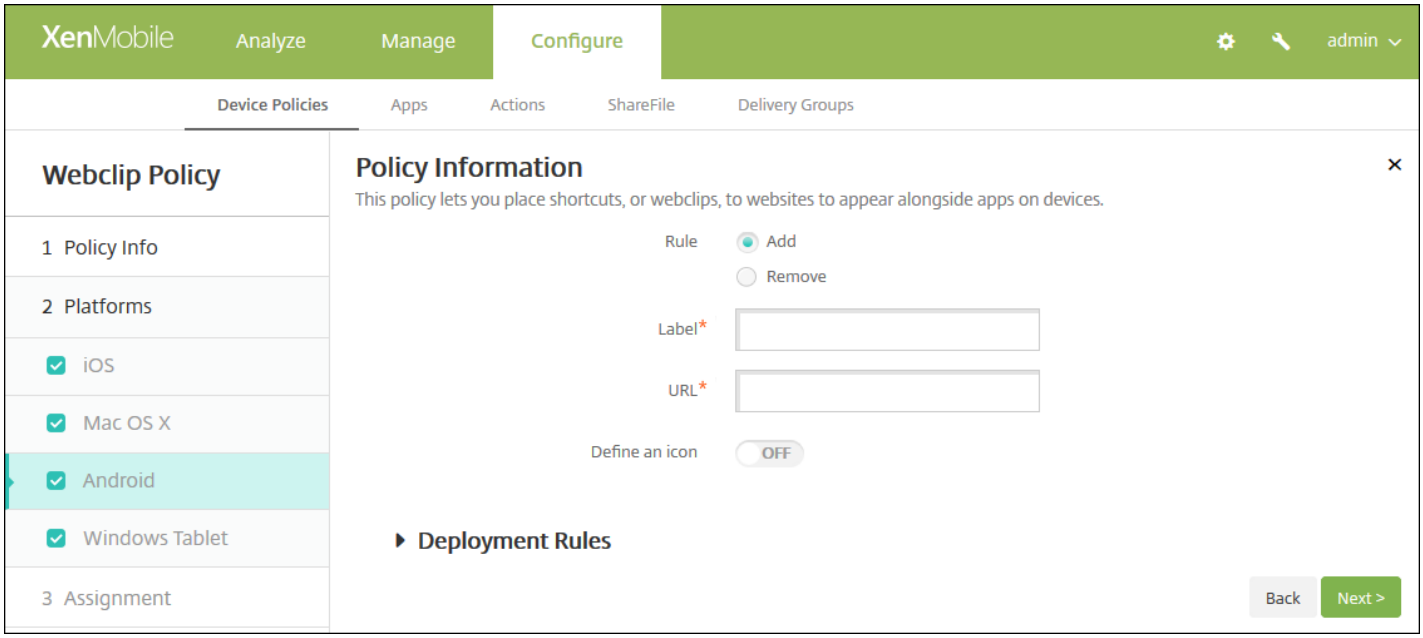




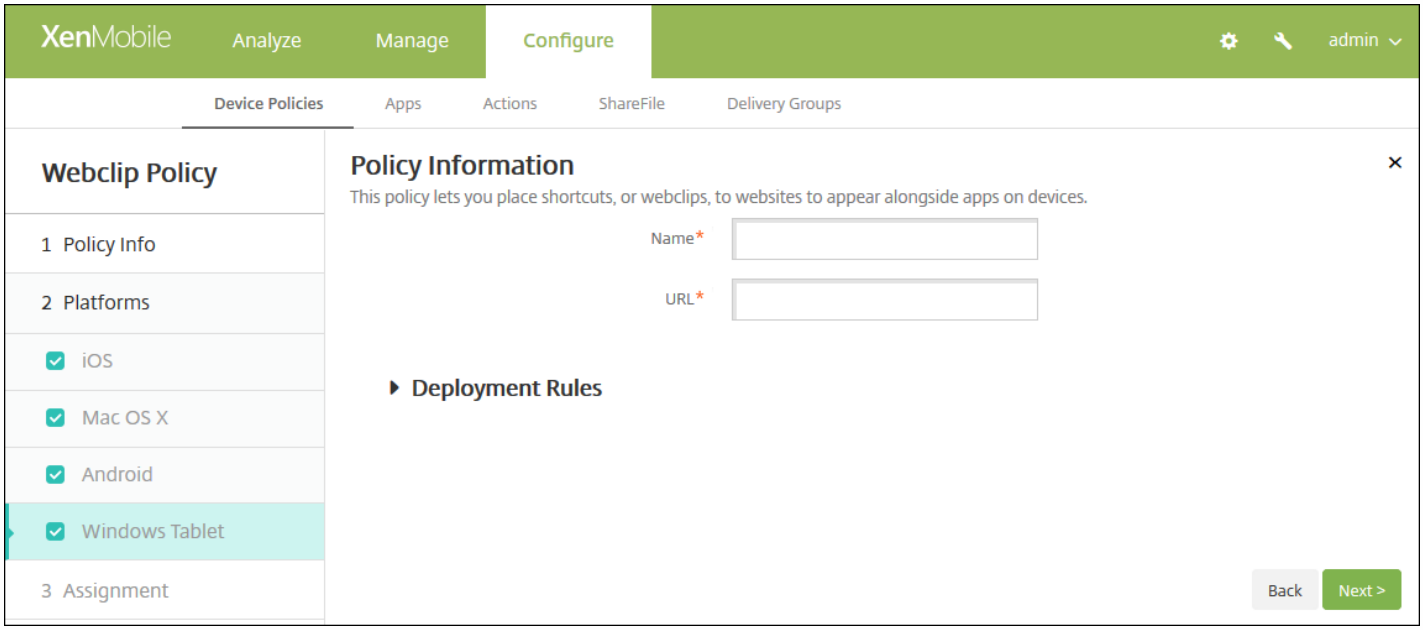
-
-
-
-
-
-
-
  -
  -
  -
  -



-
-
-
-
  -
  -
  -
  -
  -

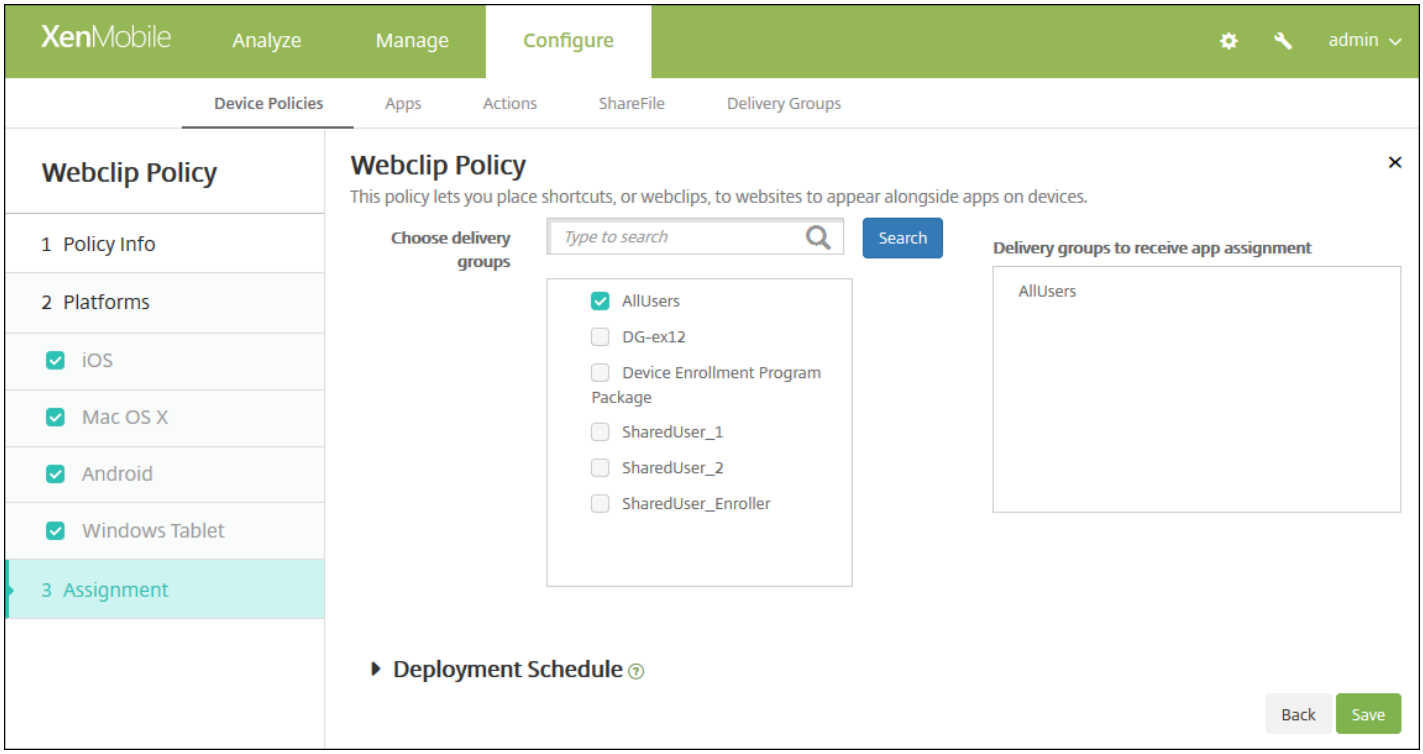


-
-
-
-
-

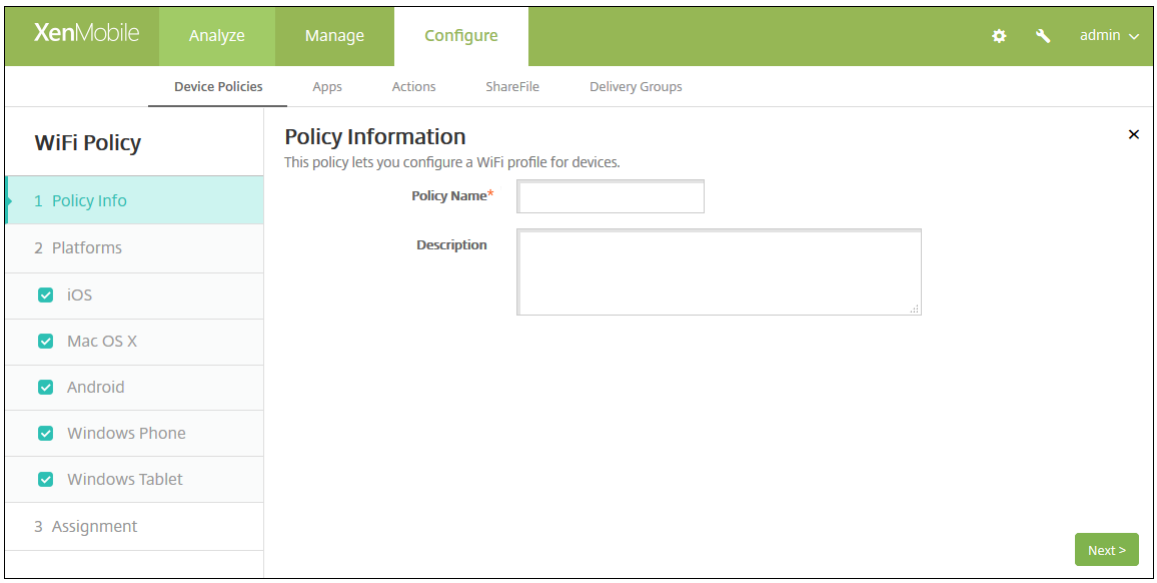


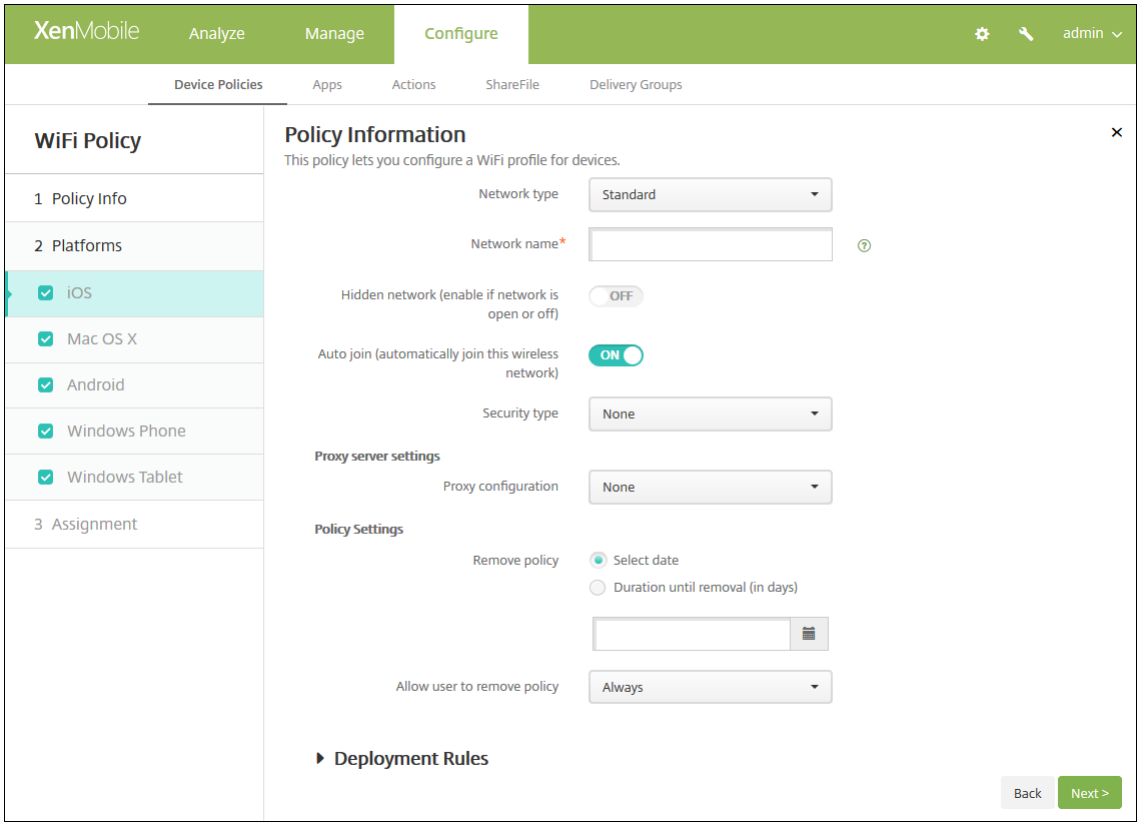
-
-

7. Configure the deployment rules



-
-
-
-
-
-
-



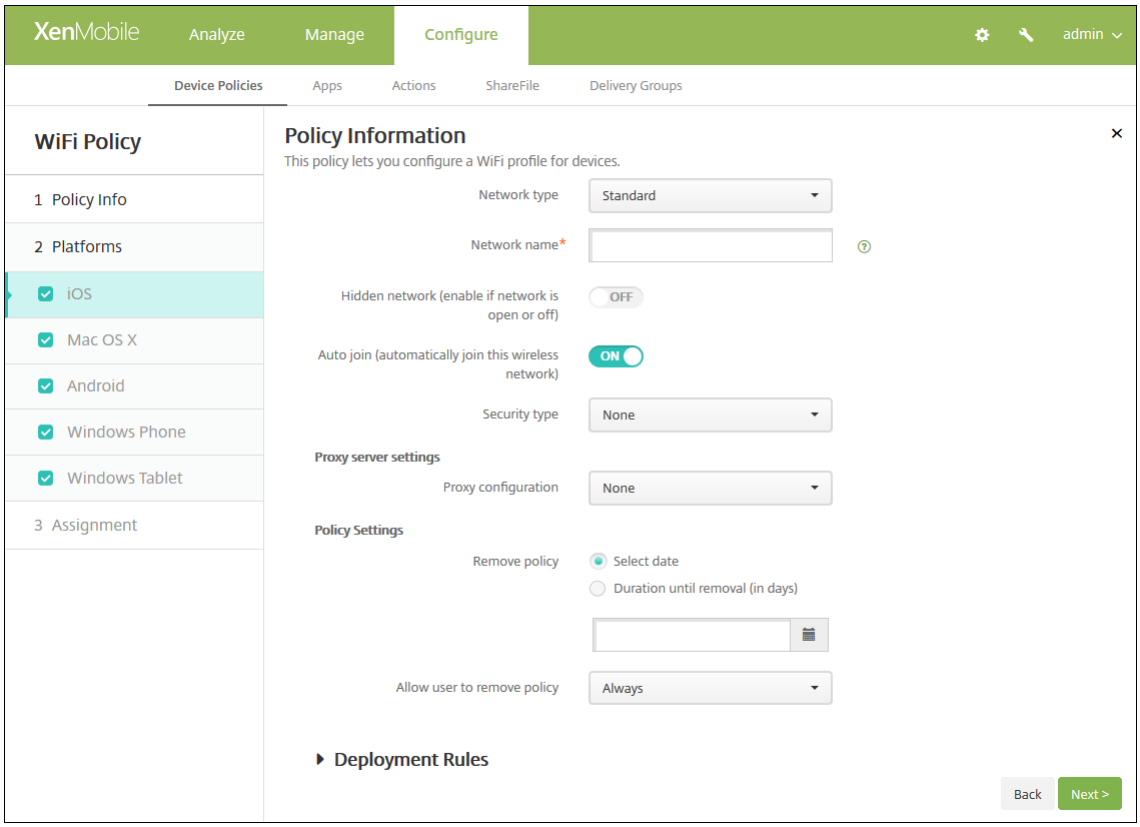


-
-
-
-
-
  -
  -
  -
  -
  -
  -
  -
  -

WPA, WPA Personal, Any (Personal)

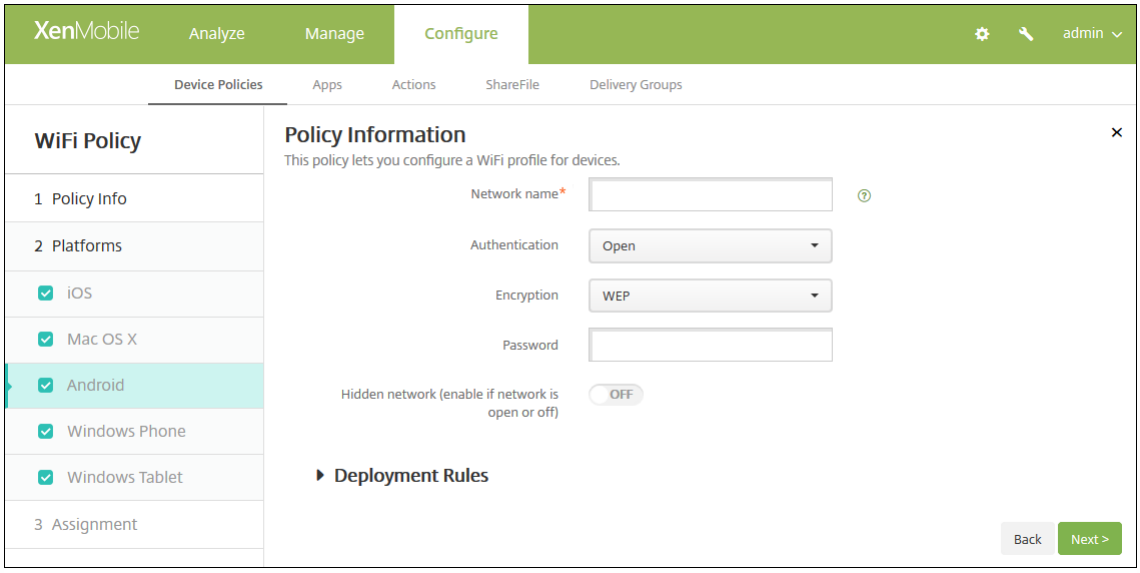
WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise)

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



WPA, WPA Personal, WPA 2 Personal, Any (Personal)

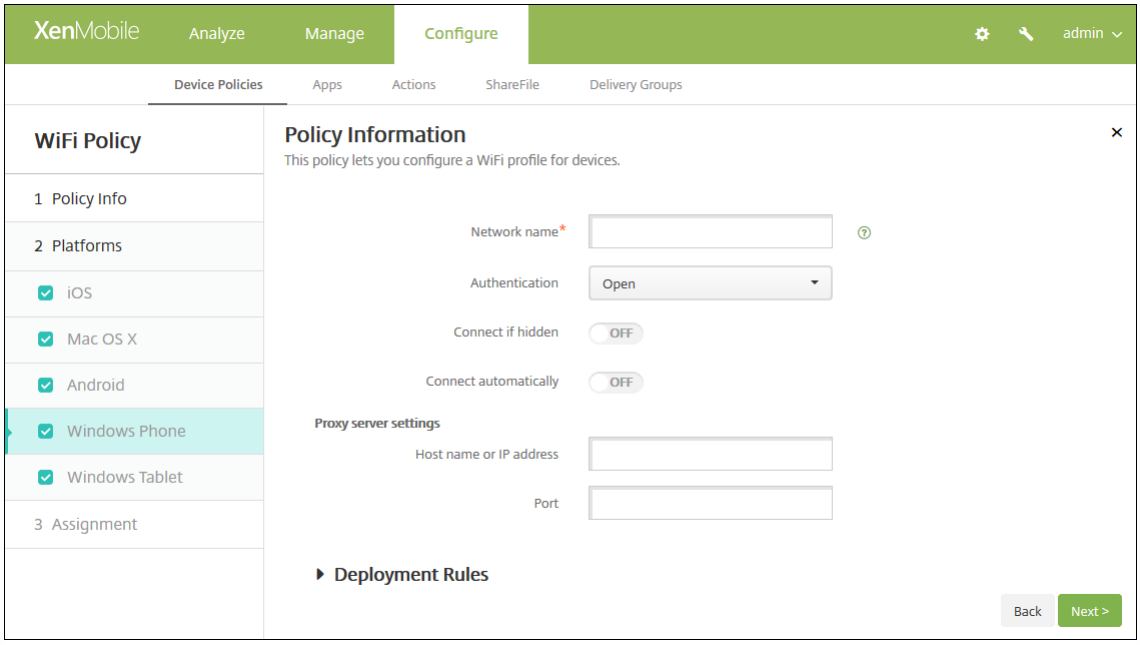
WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise)



Open, Shared

WPA, WPA-PSK, WPA2, WPA2-PSK

802.1x



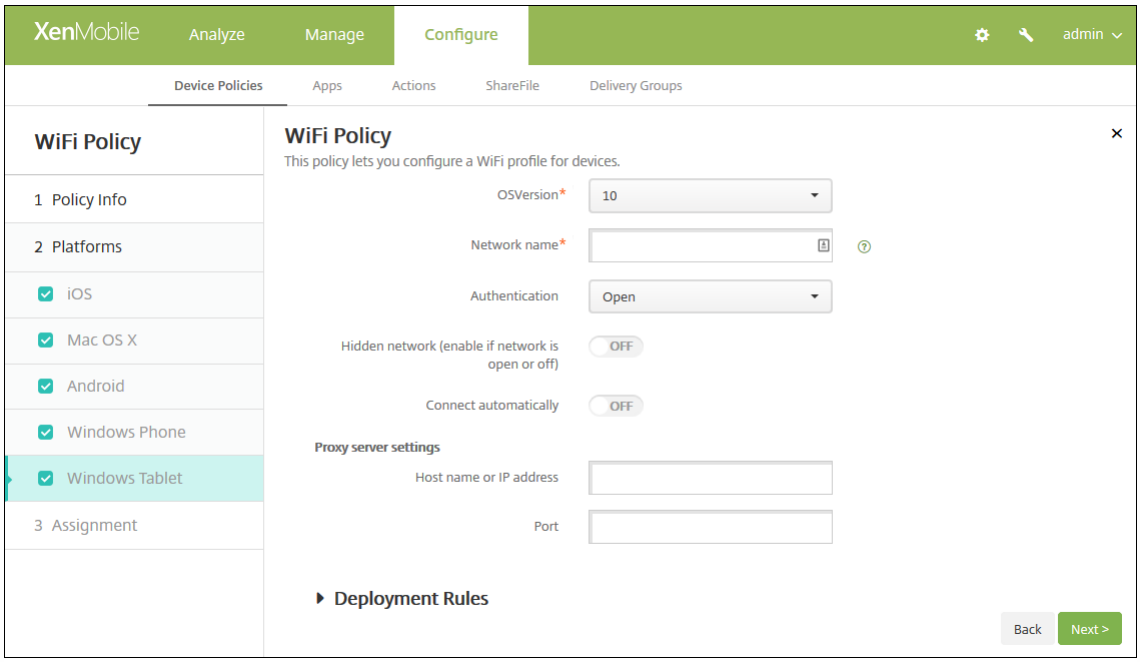
-
-
  -
  -
  -
  -

Open

WPA Personal, WPA-2 Personal

WPA-2 Entrprise

-
  -
  -



-
-
  -
  -
  -
  -
  -
  -

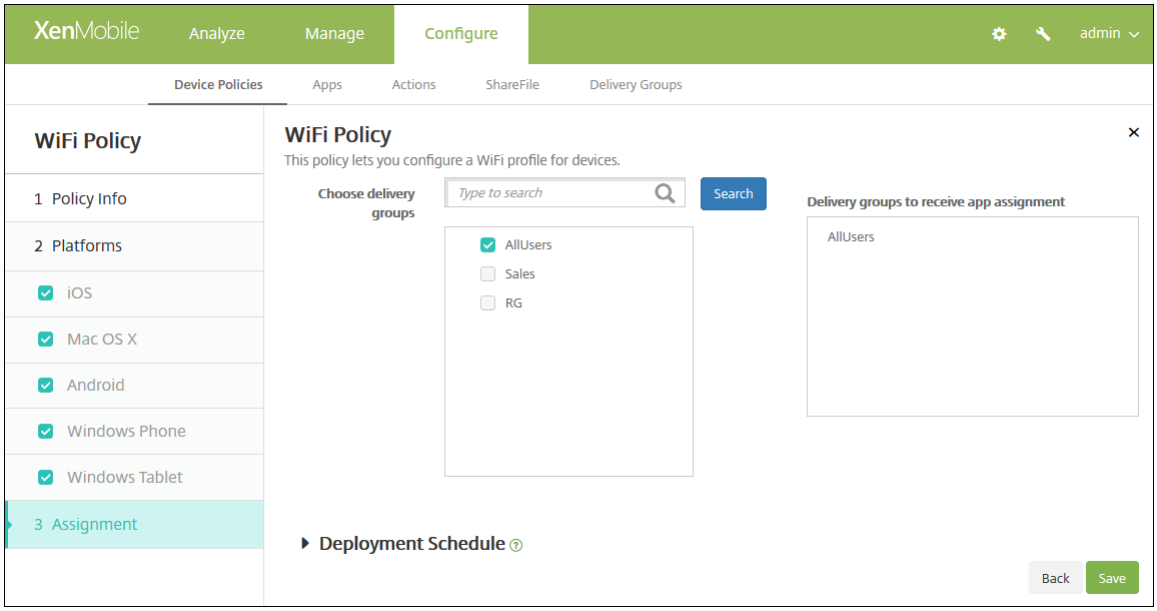
Open

WPA Personal, WPA-2 Personal

WPA-2 Enterprise

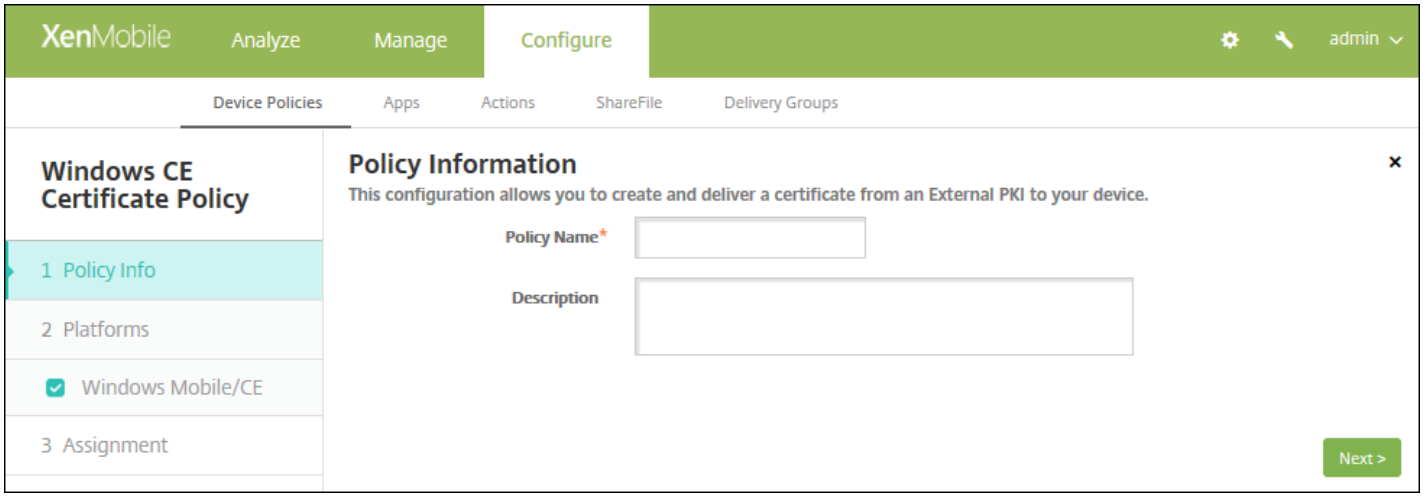
-
-
  -
  -
  -
  -
  -
-
-

7. Configure the deployment rules

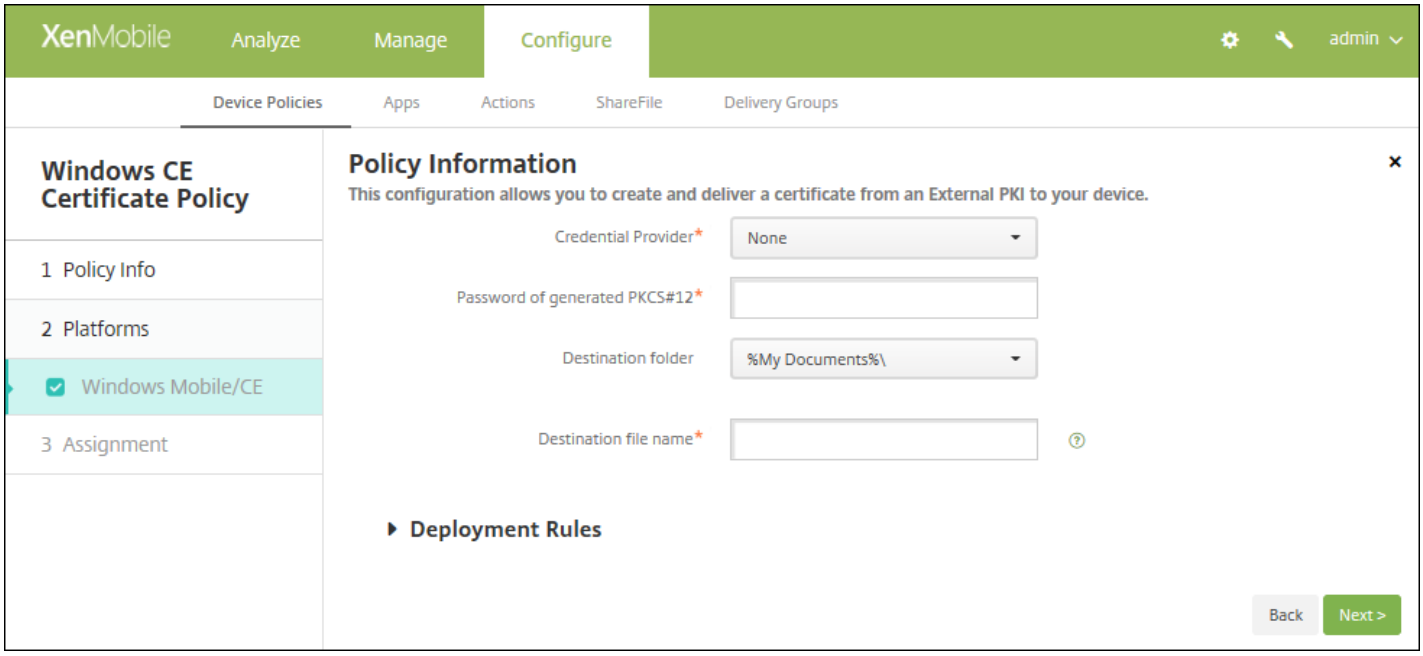


-
-
-
-
-

-
-

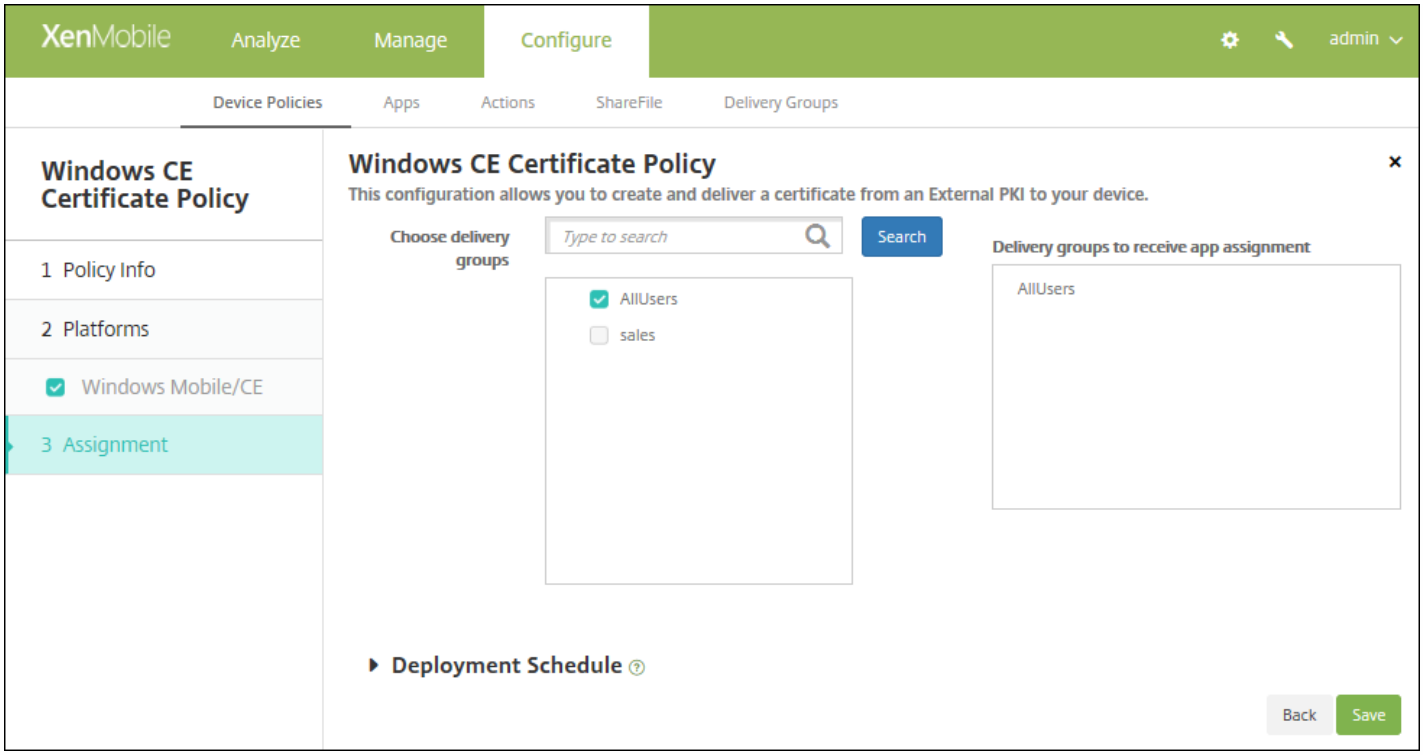


-
-

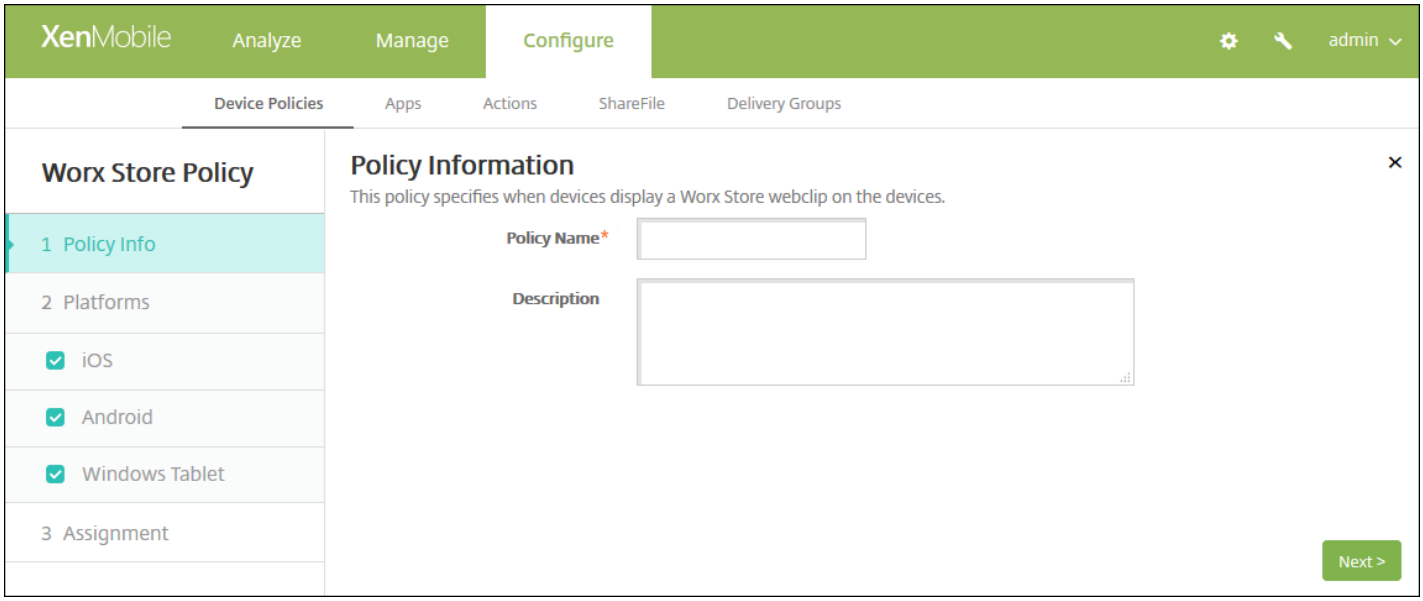


-
-
-
  -
  -
  -
  -
  -
-

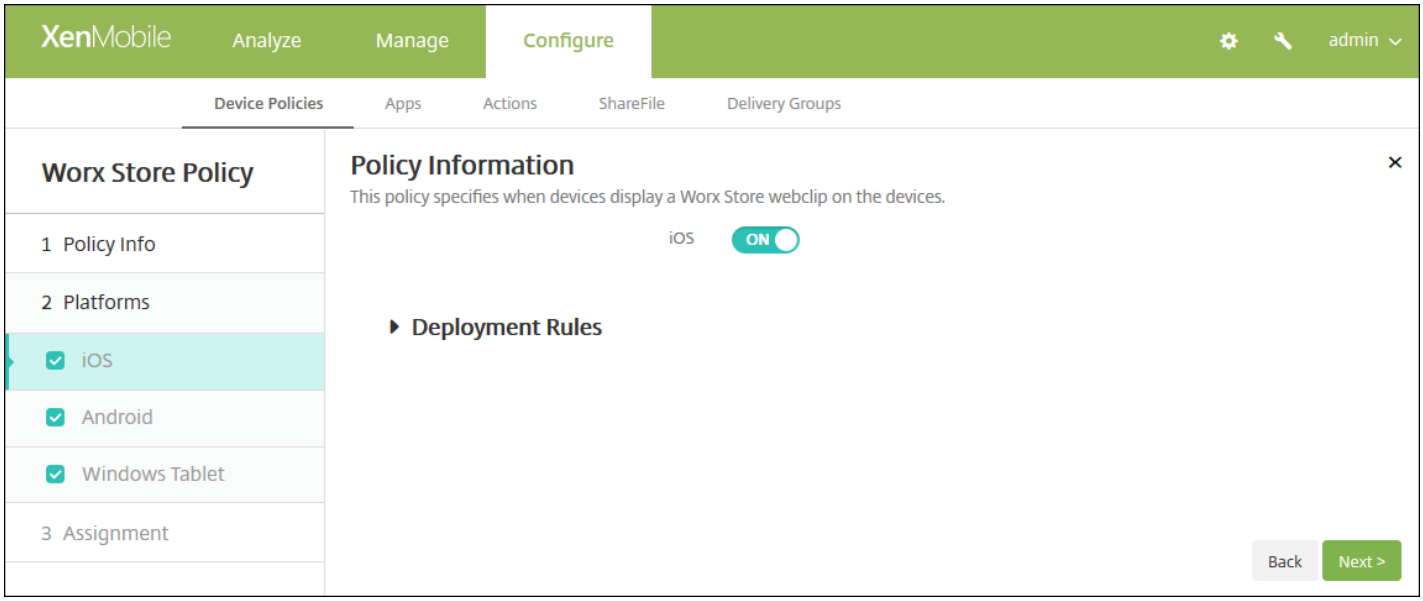
7. Configure the deployment rules



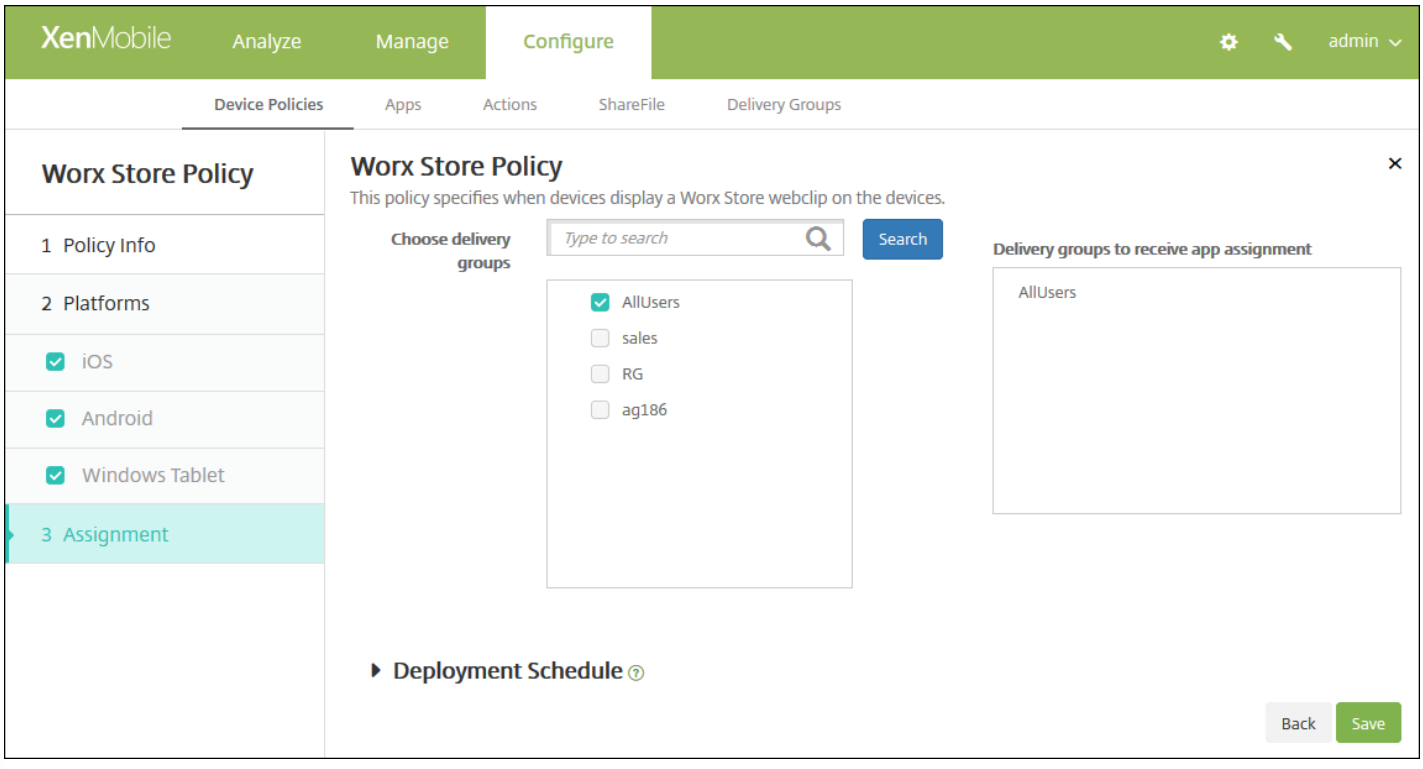
-
-
-
-
-
-
-



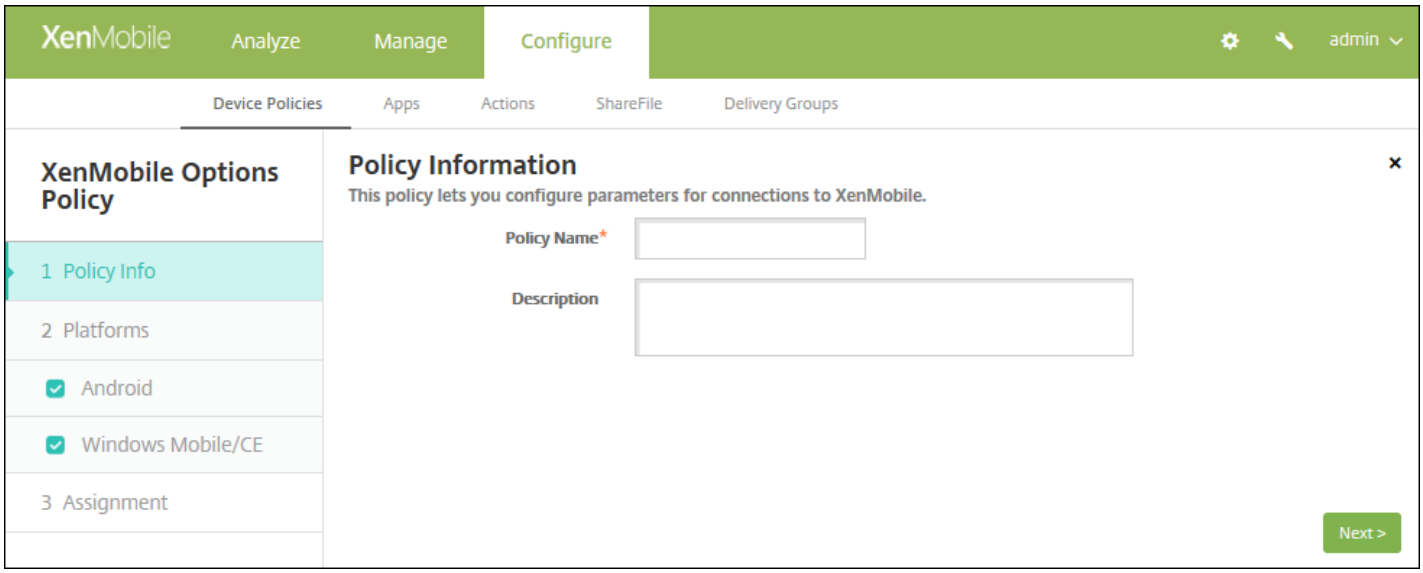
-
-



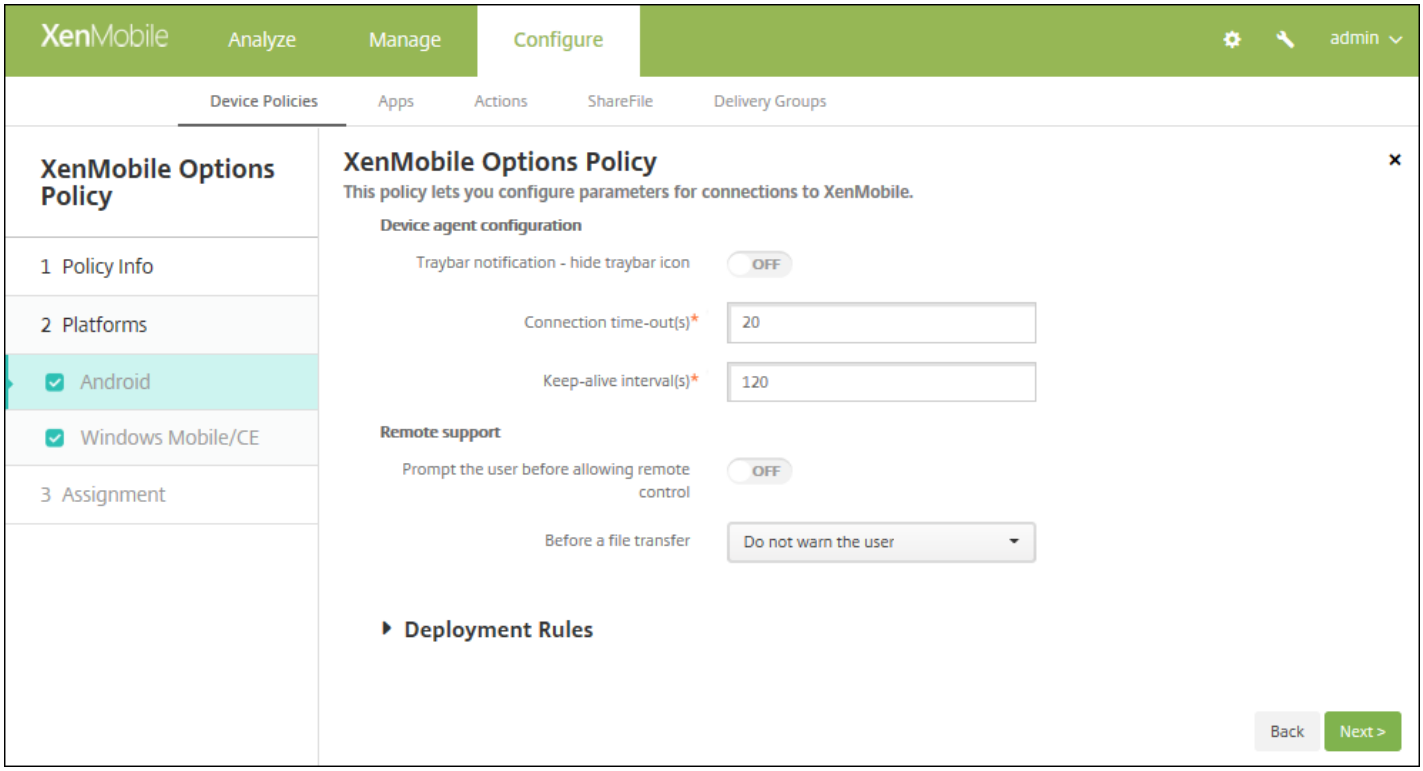
8. Configure the deployment rules



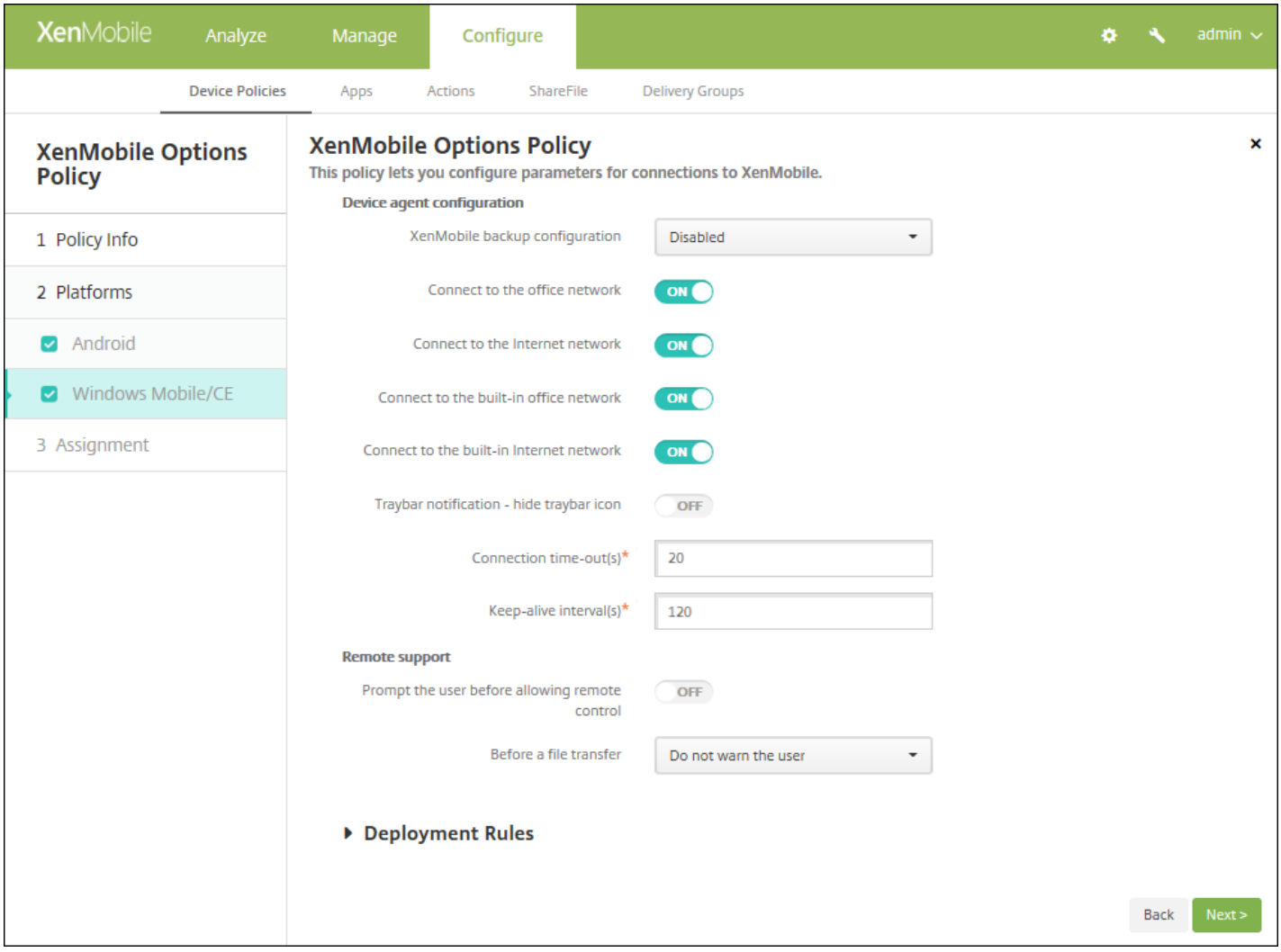
-
-
-
-
-
-
-



-
-

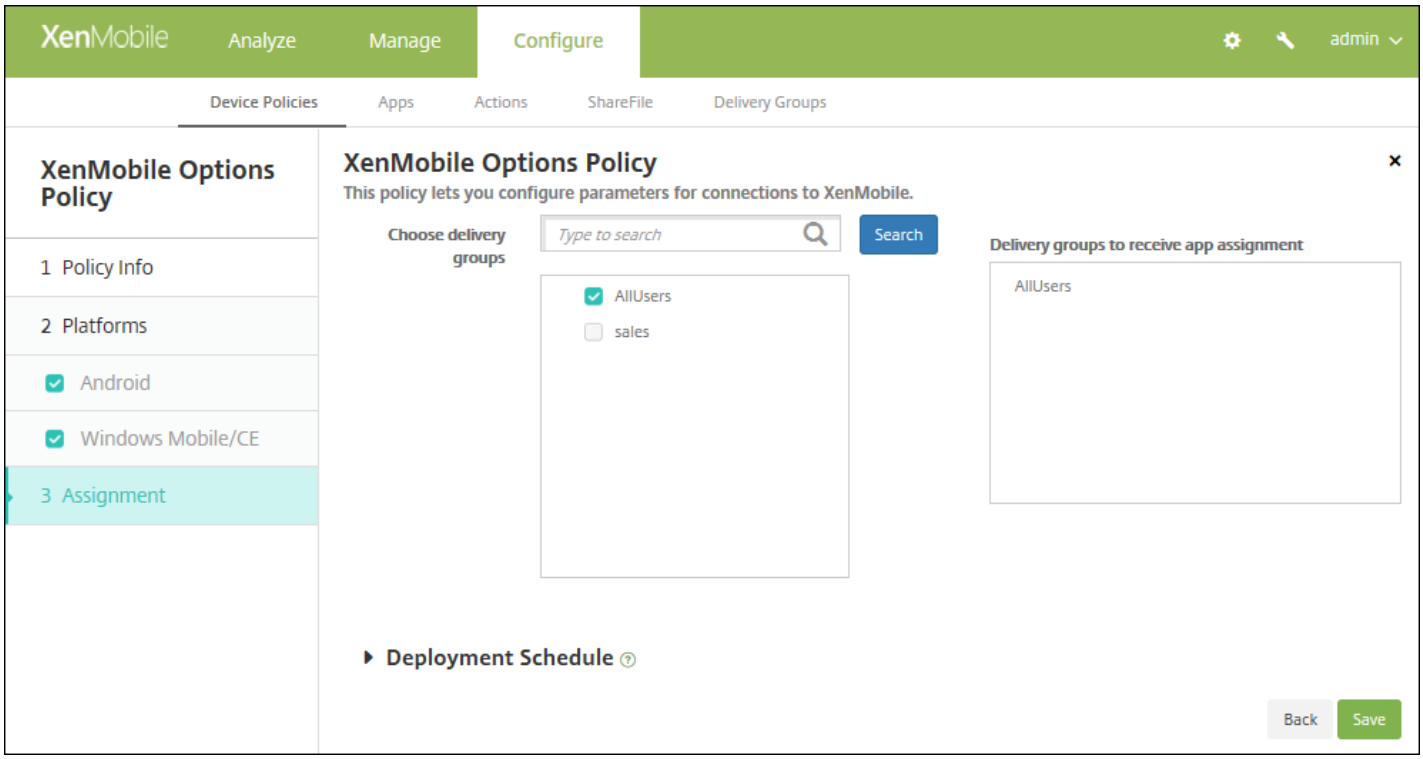


-
-
-
-
-



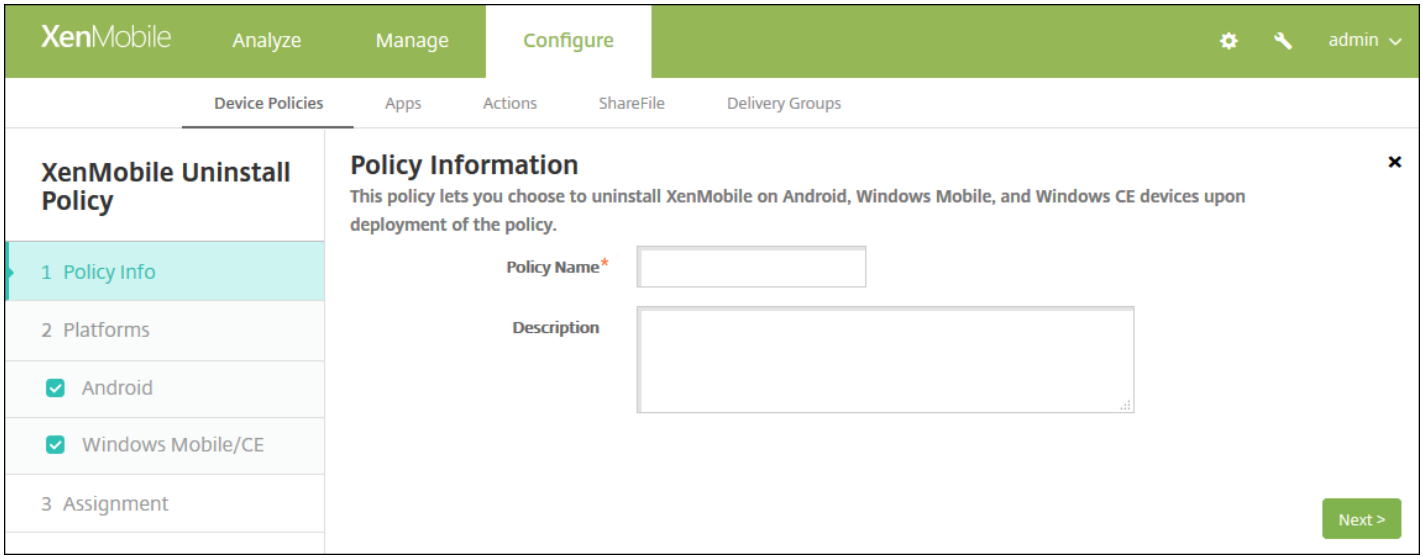
-
  -
  -

7. Configure the deployment rules

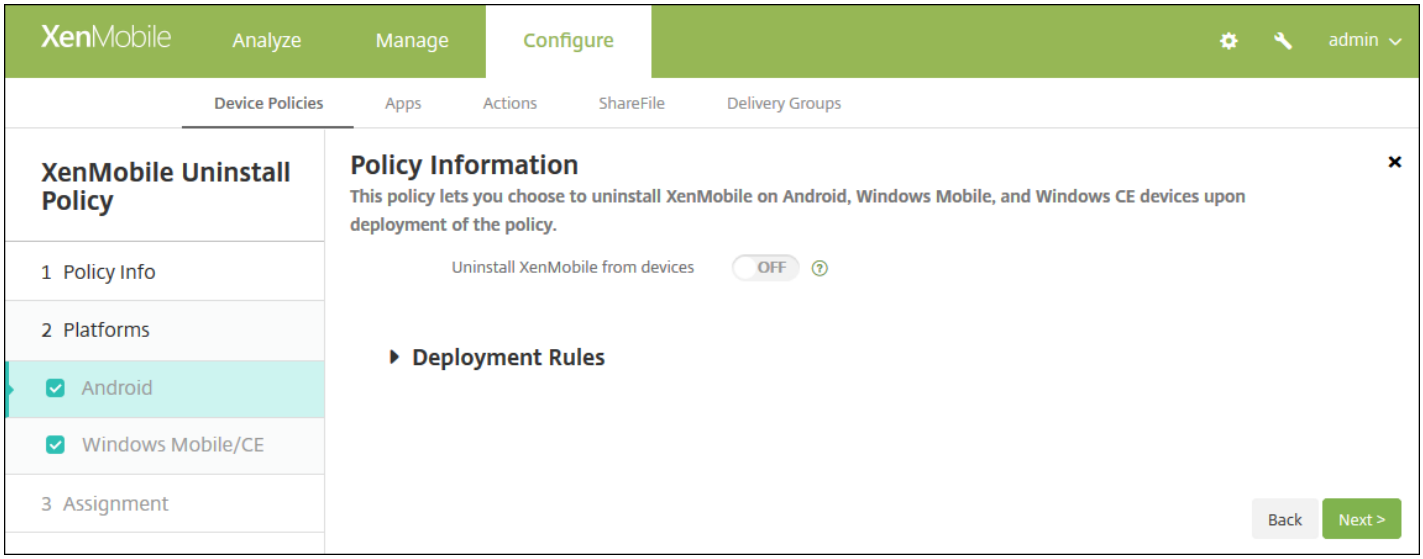


-
-
-
-

-
-

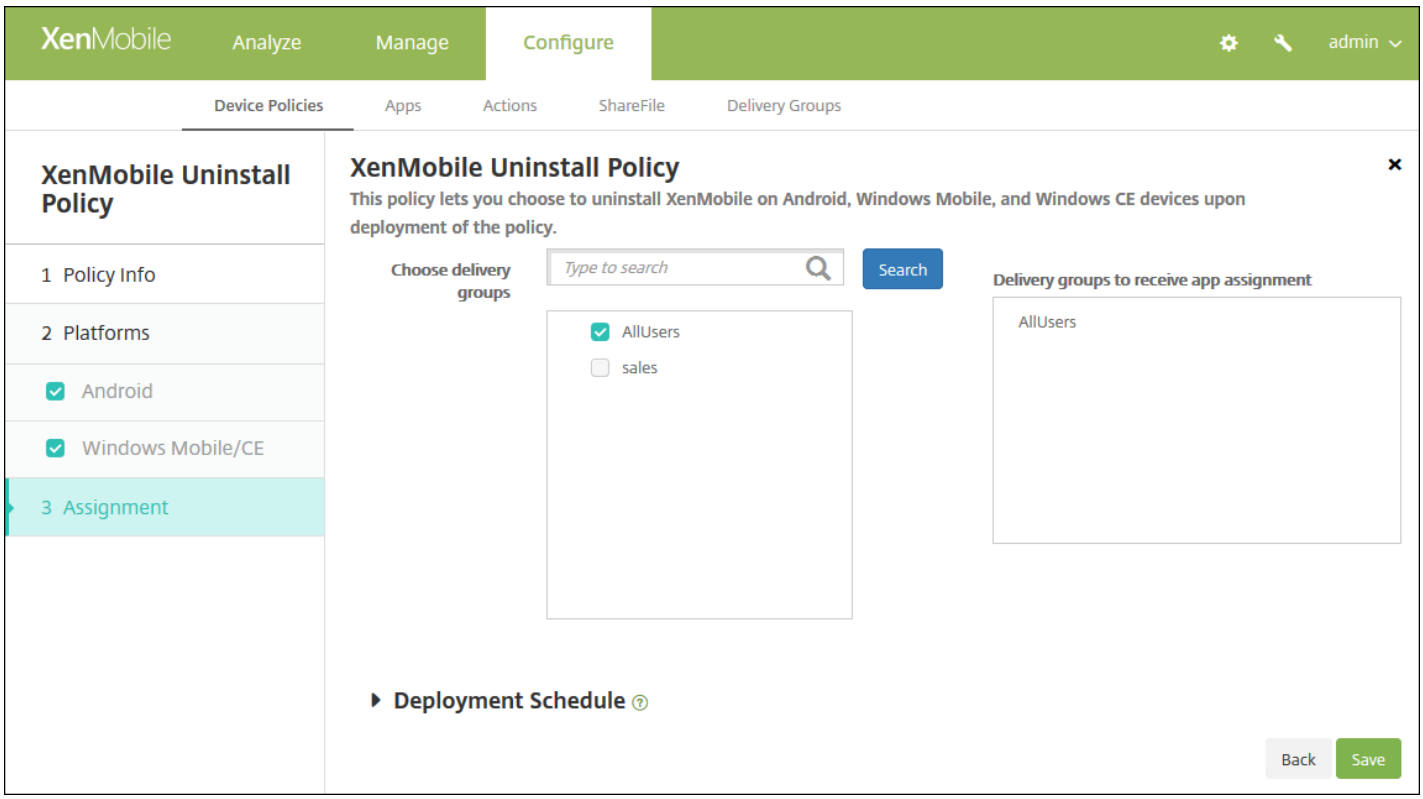


-
-



-

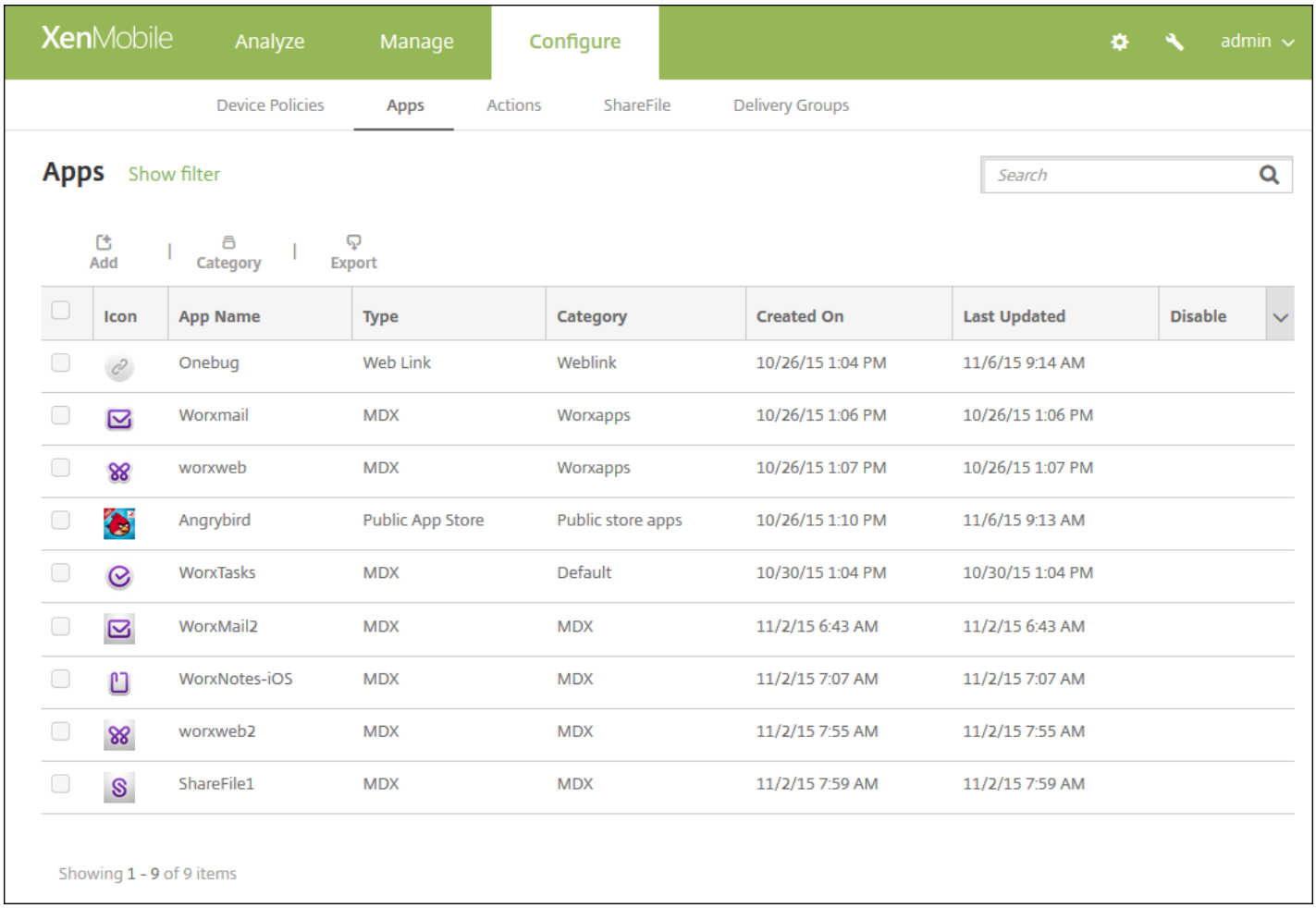
7. Configure the deployment rules

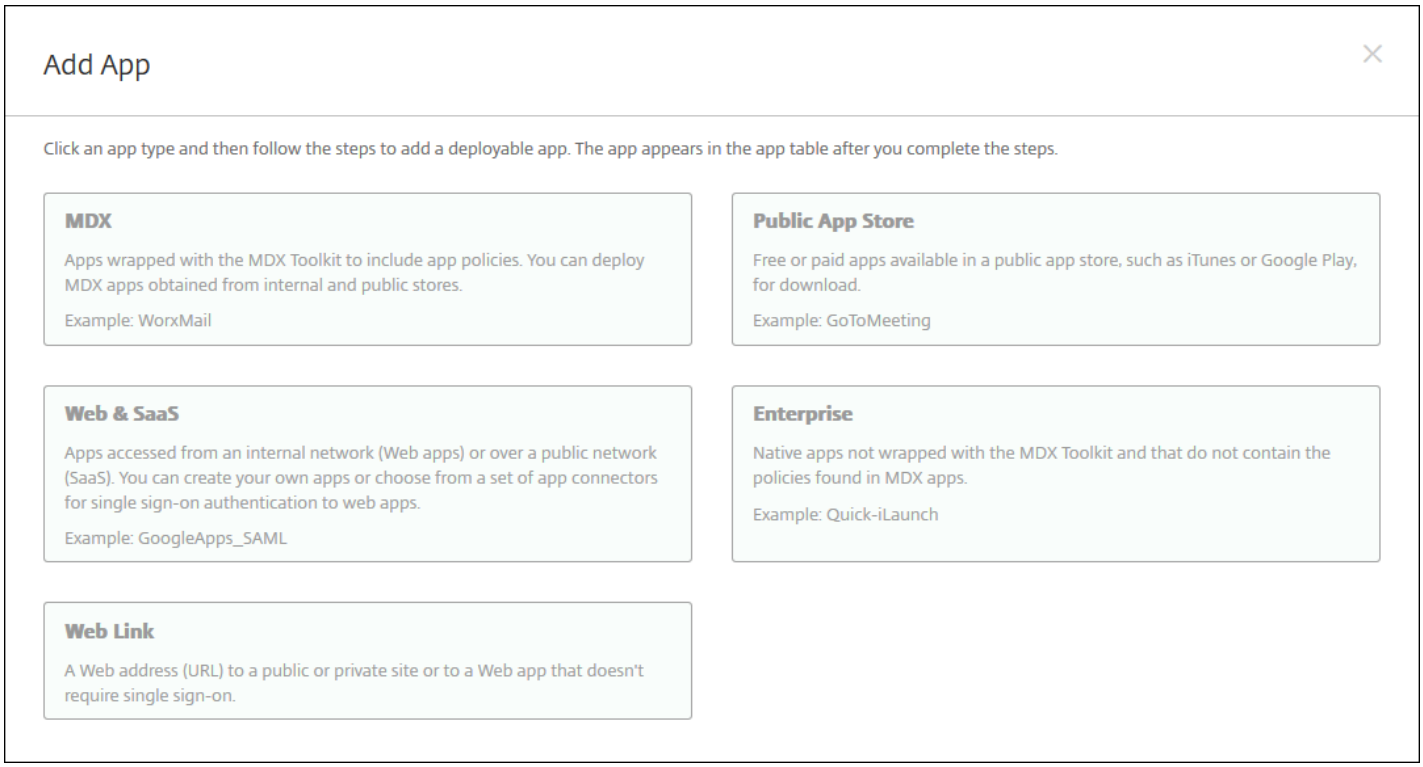


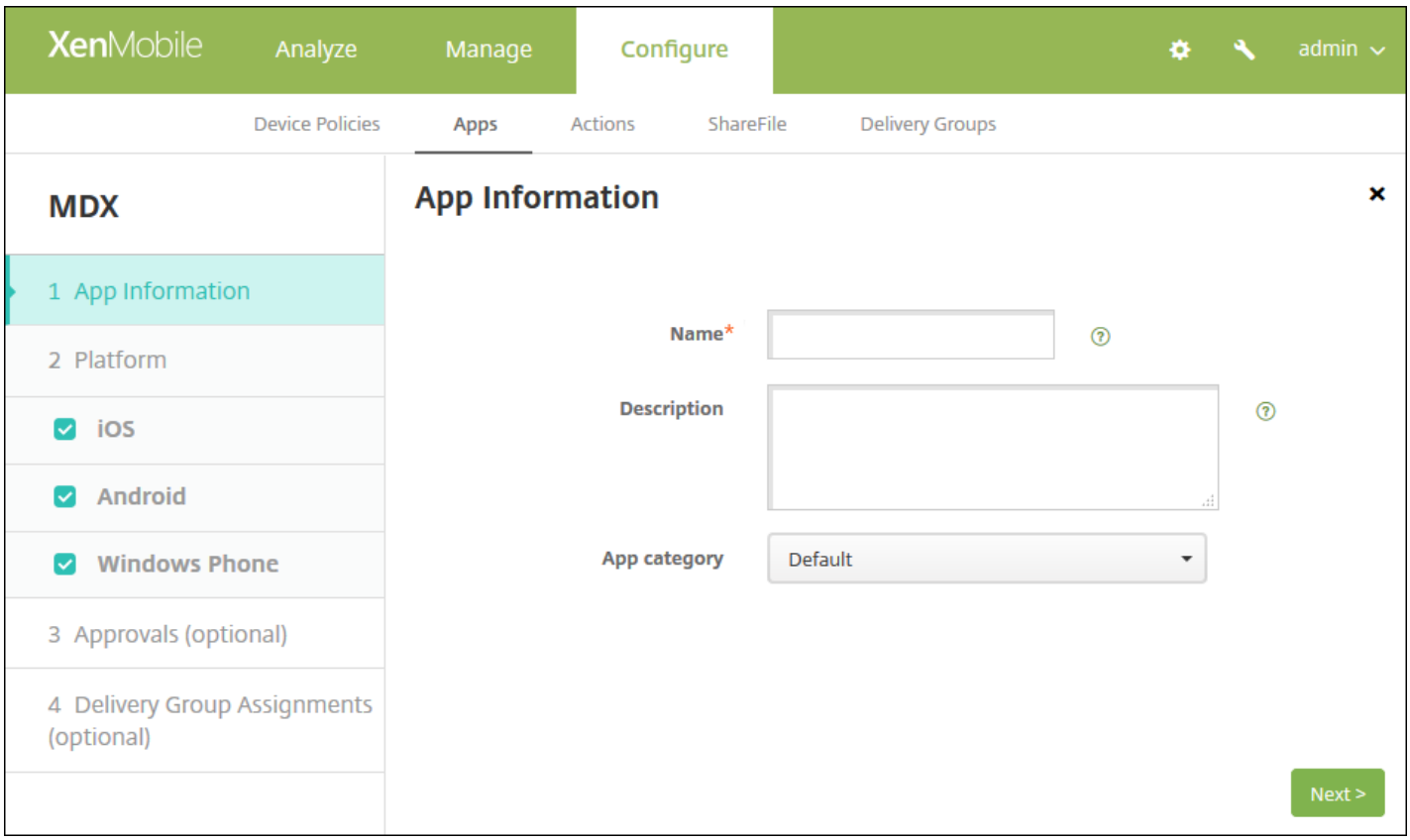
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-

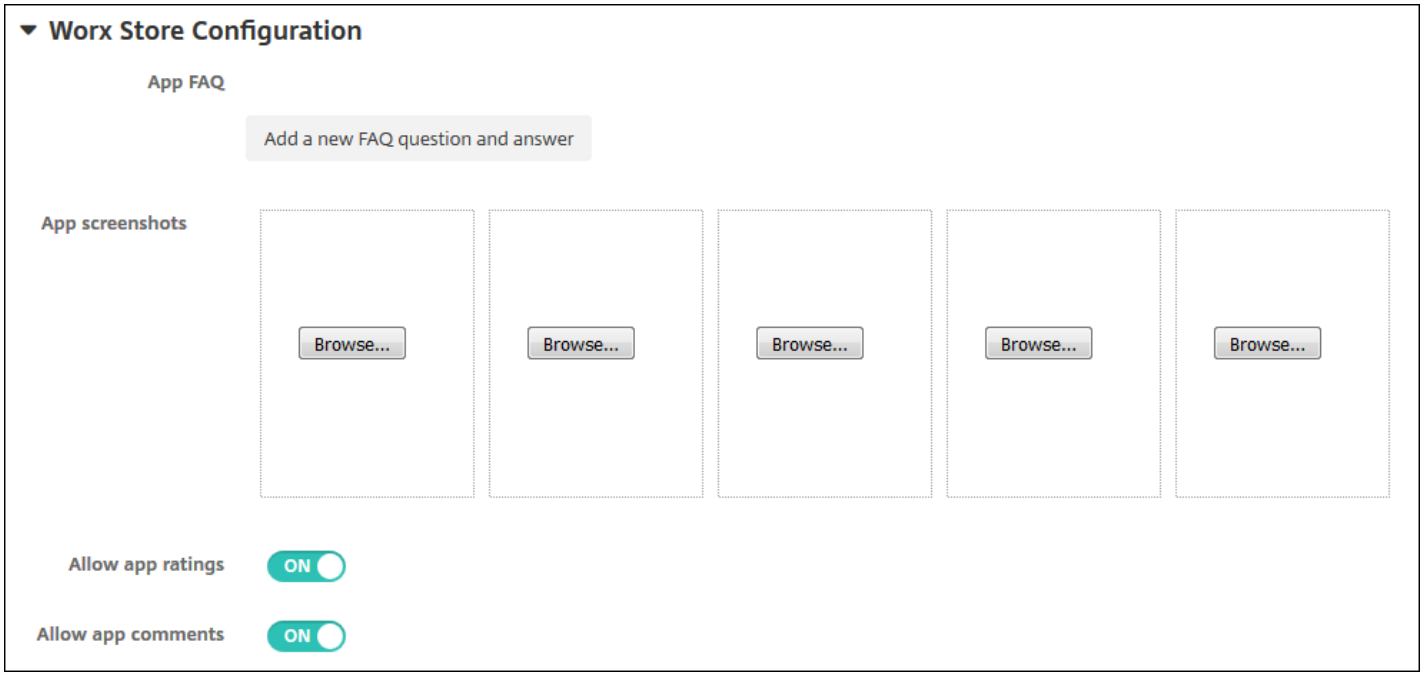
-



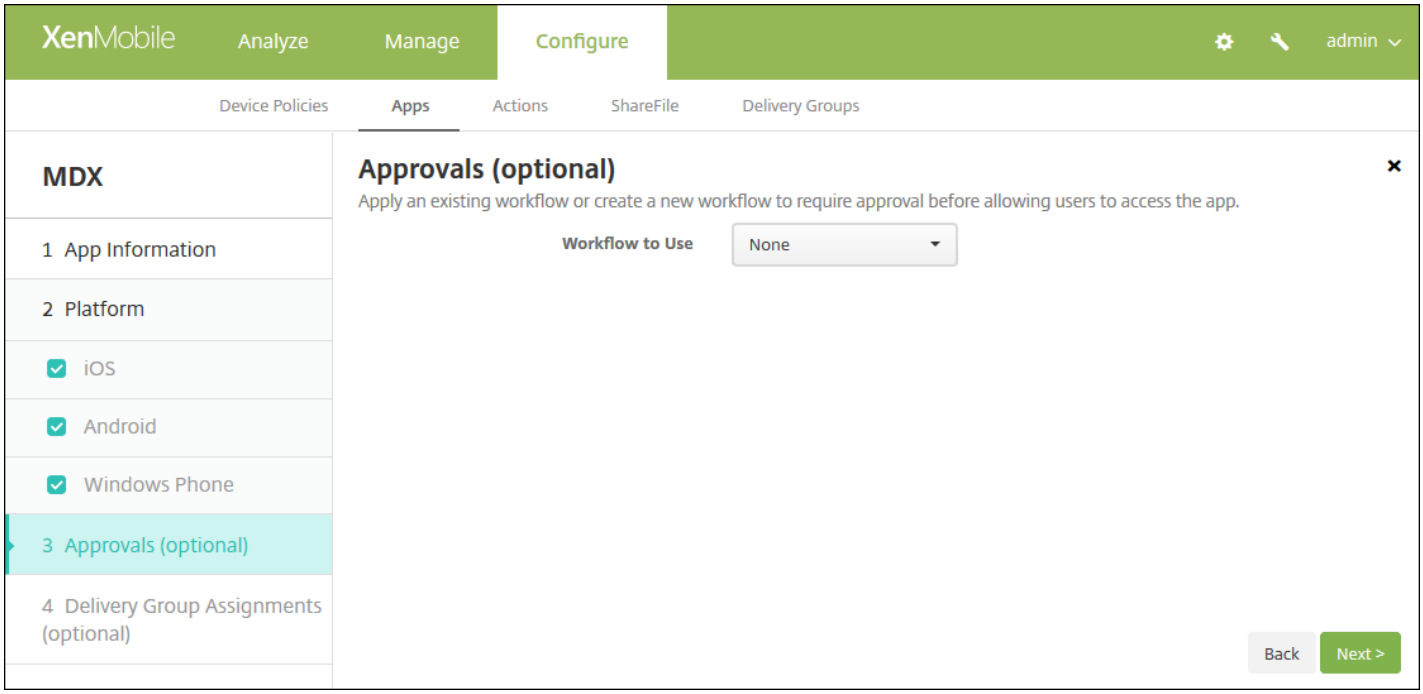




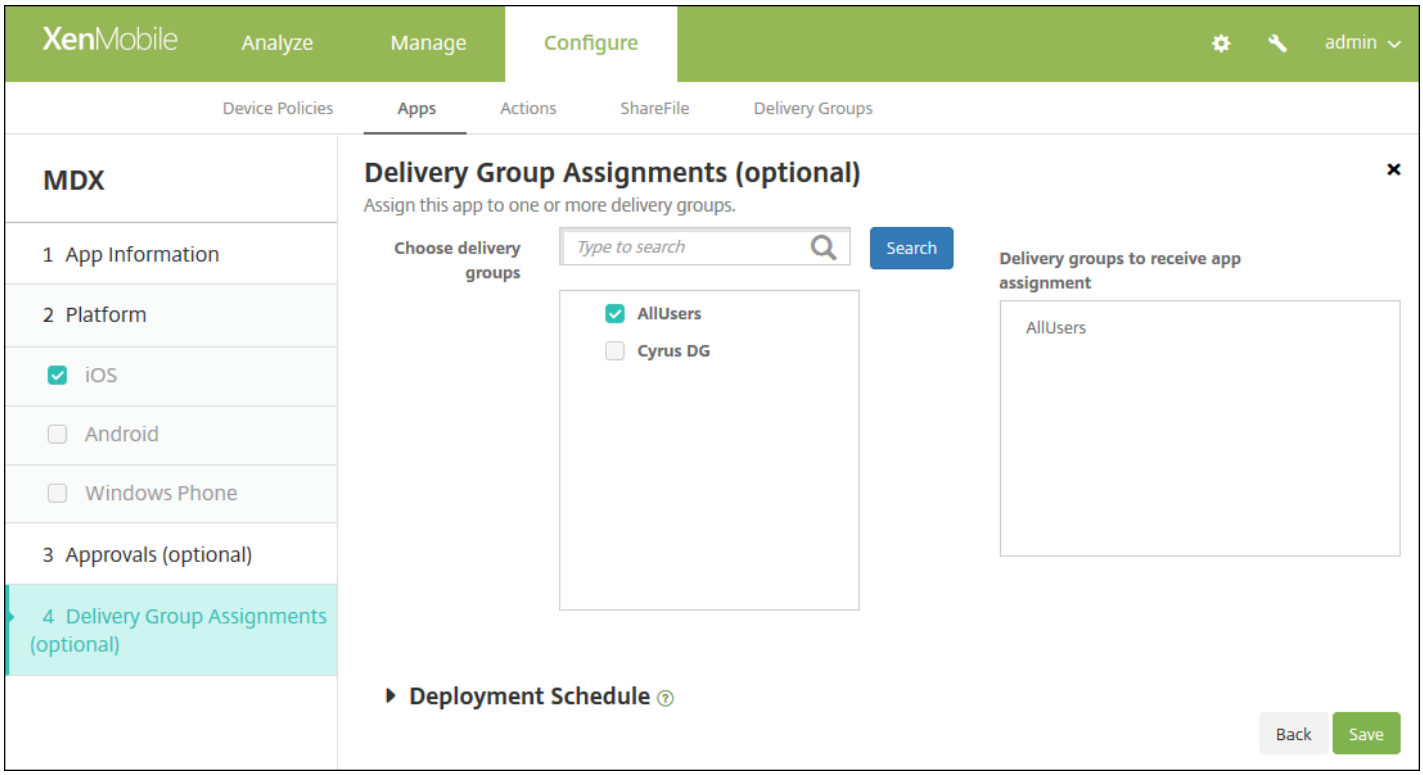
11. Configure the deployment rules

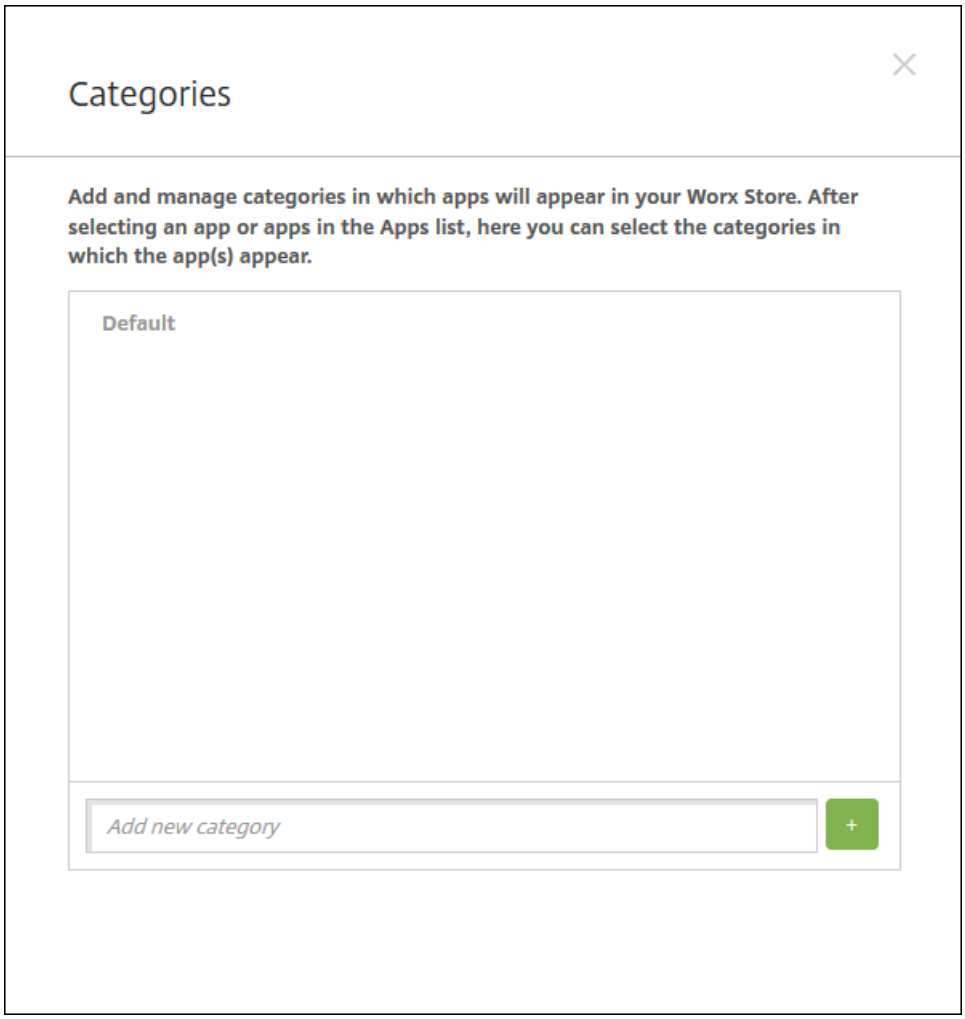


-
  -
  -
  -
  -

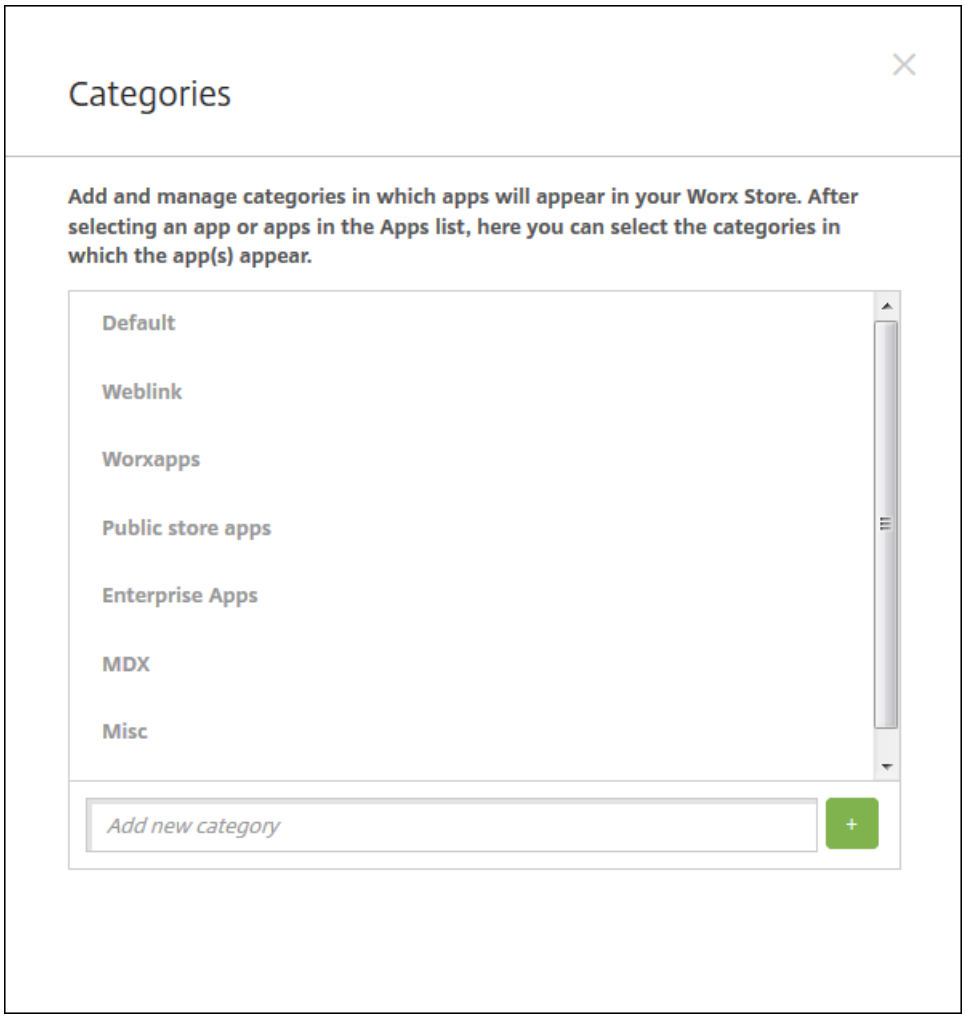


-
-
  -
  -
  -
  -
    -
    -
    -
    -
  -
  -
  -
    -
      -
      -

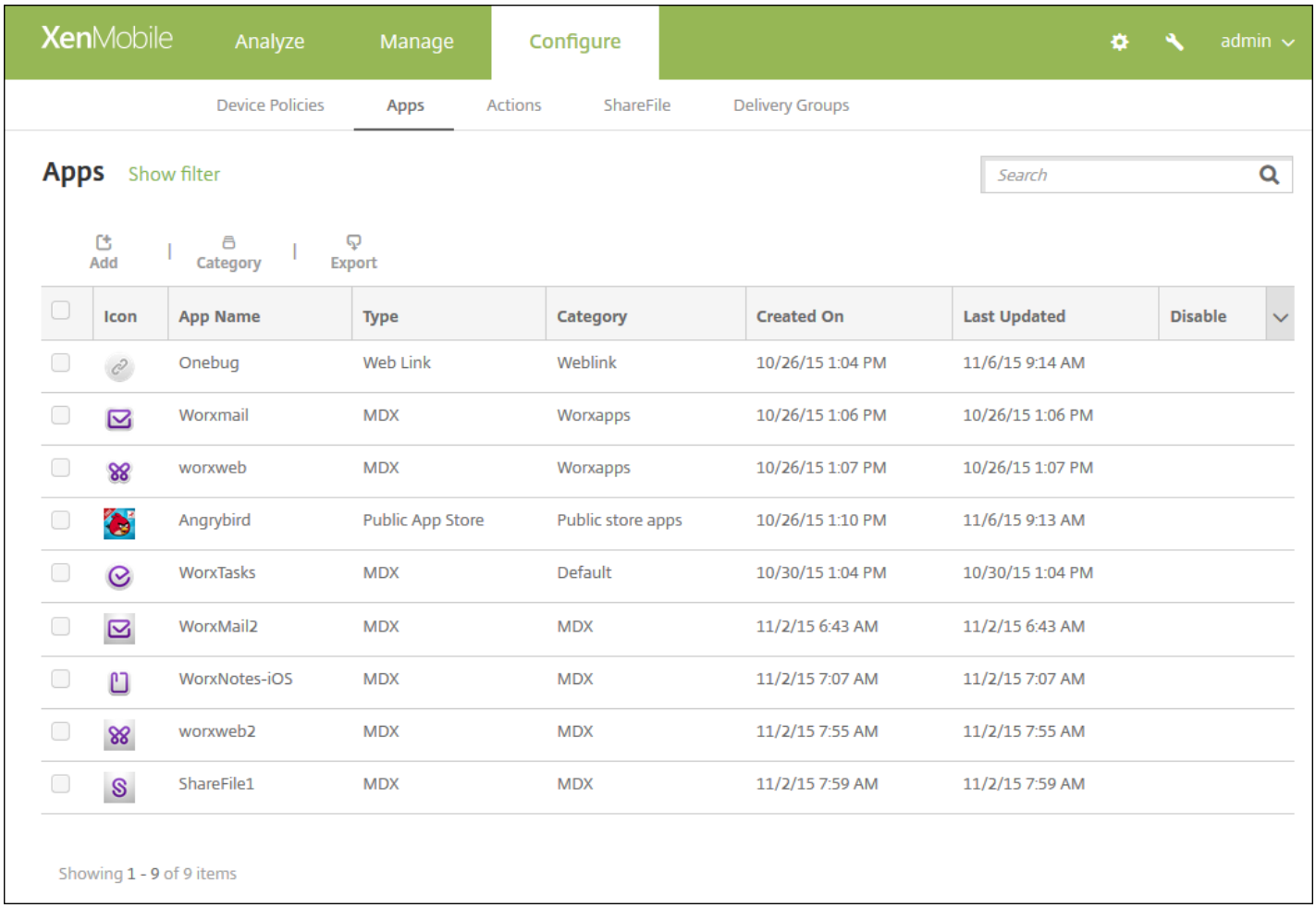


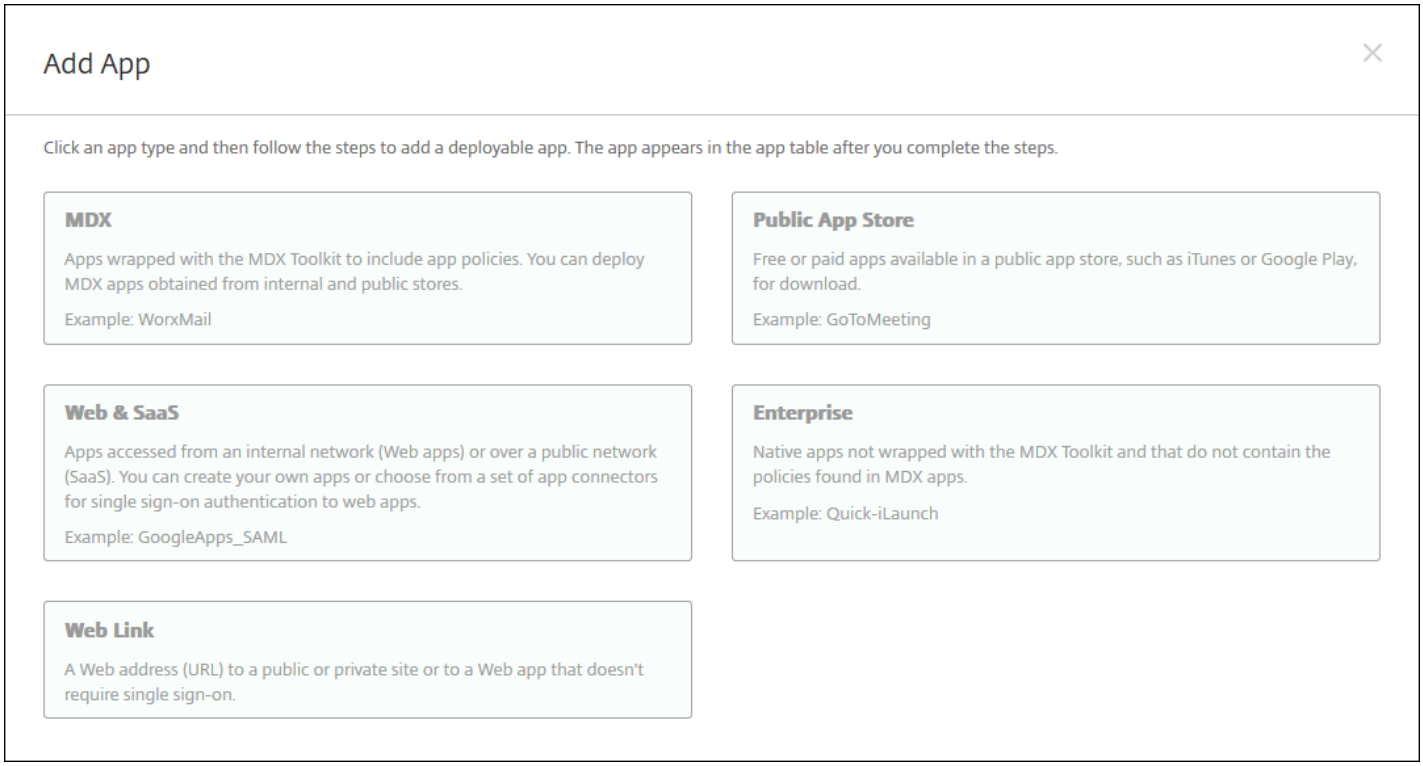


-

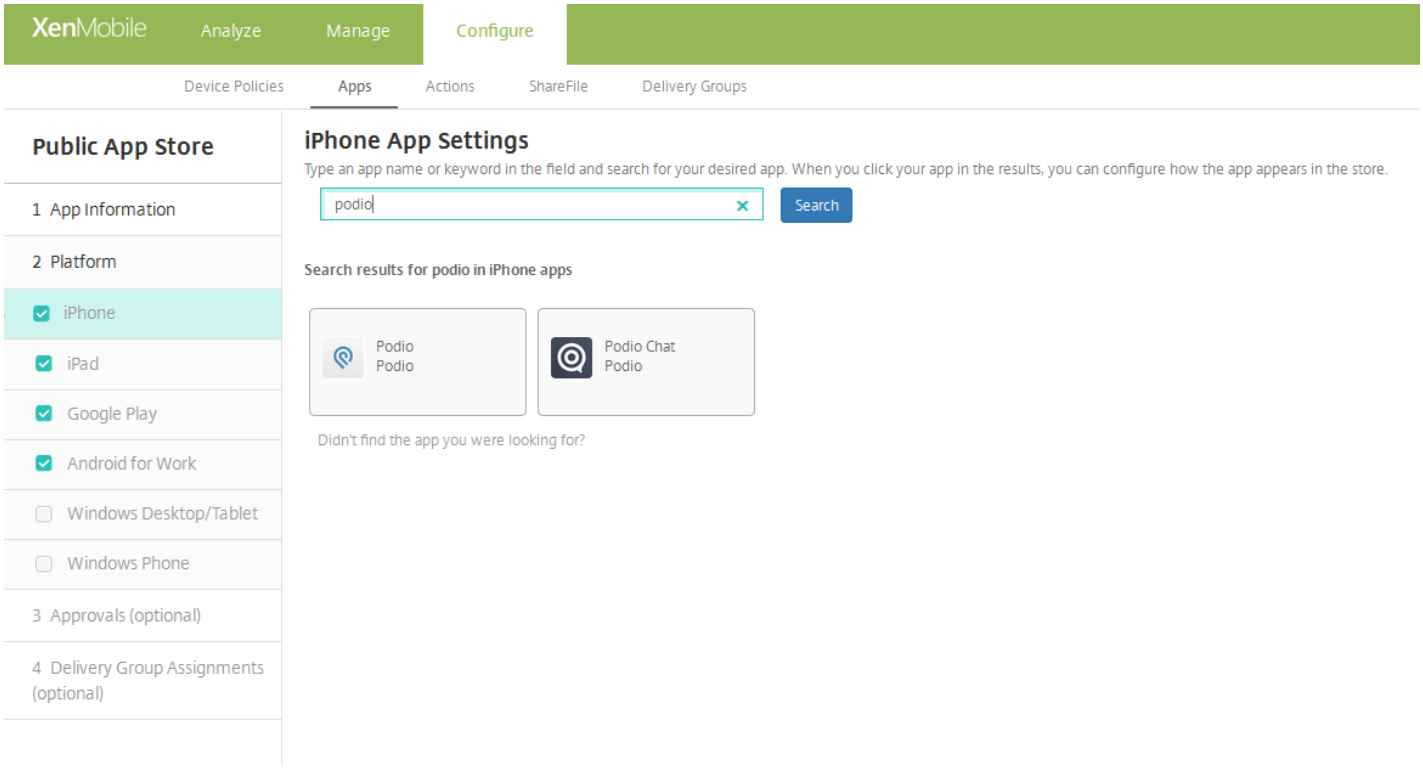


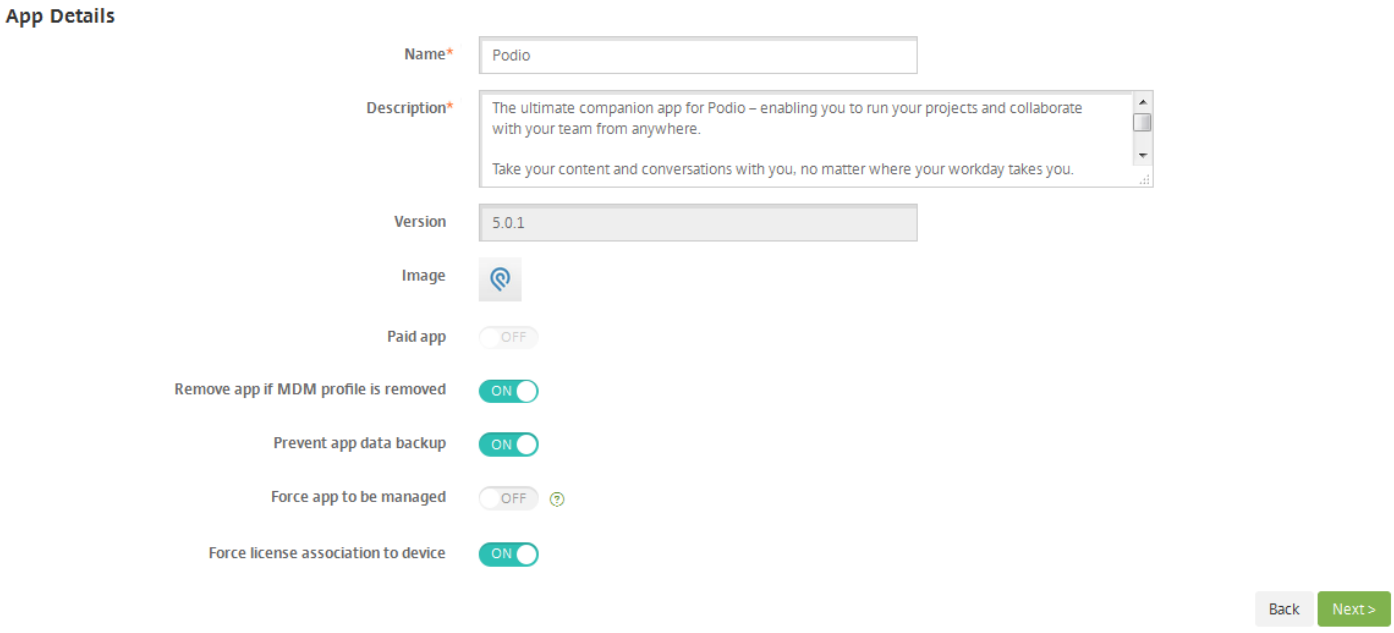
-
-
-
-
-





-
-
-

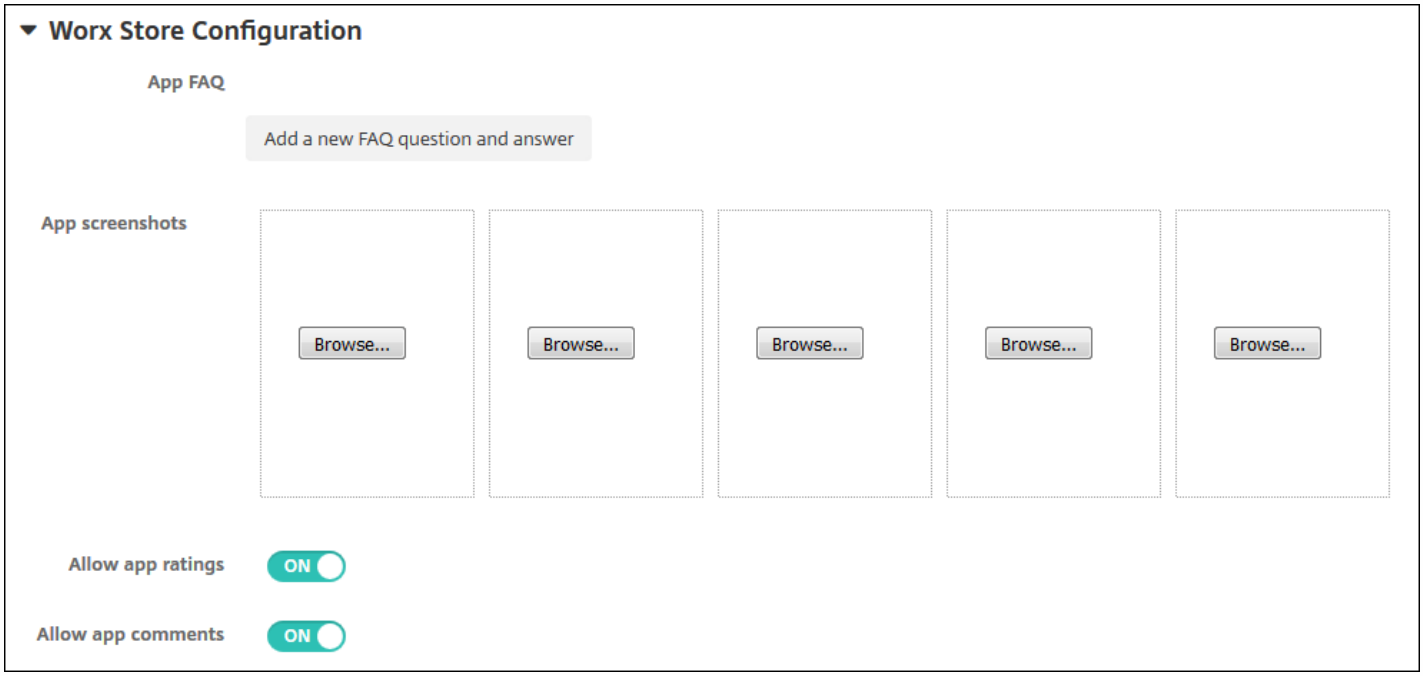




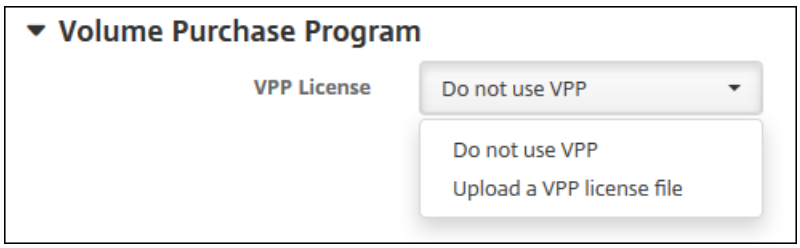
-
-

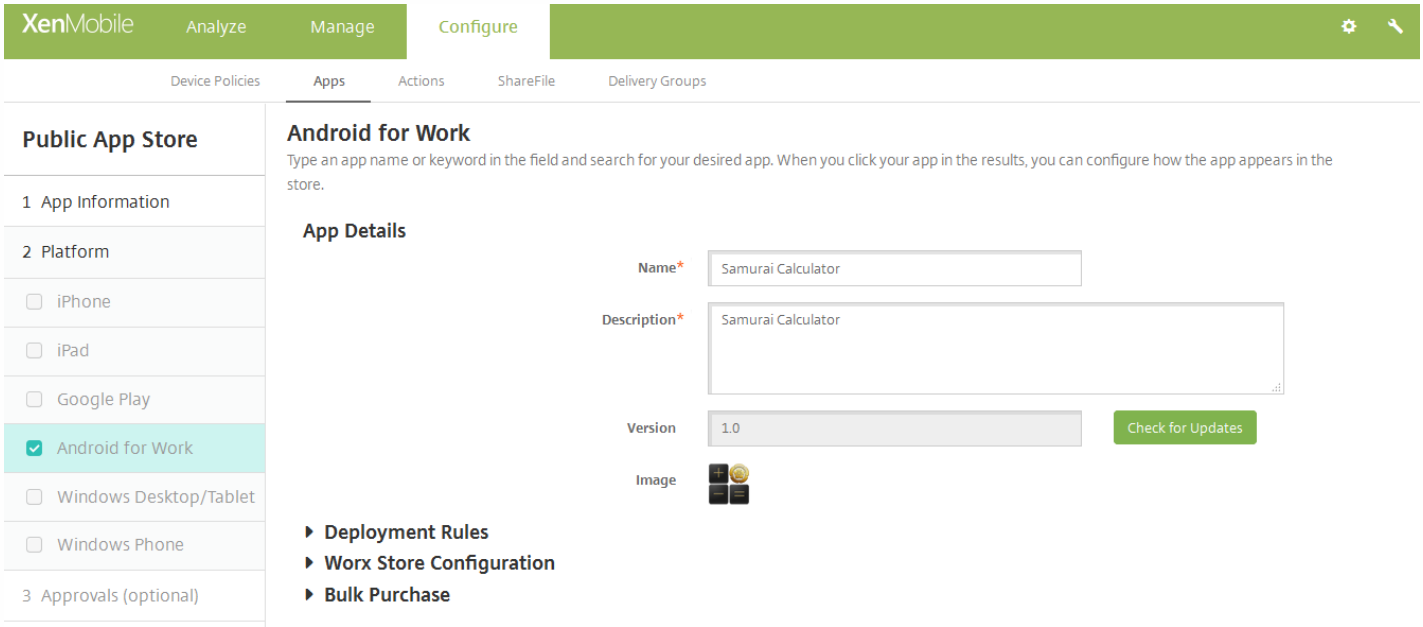
-
-
-
-

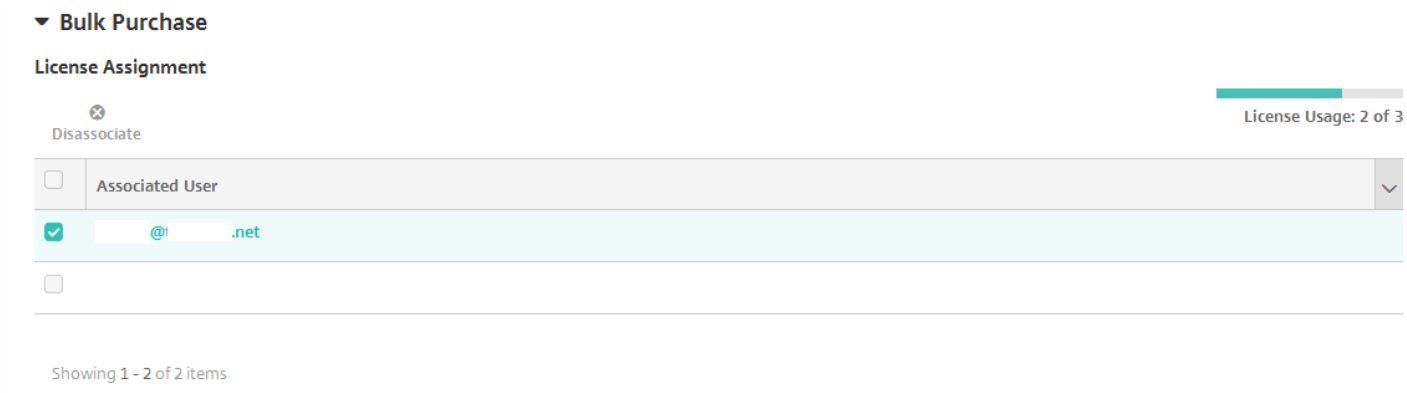
10. Configure the deployment rules



-
  -
  -
  -
  -

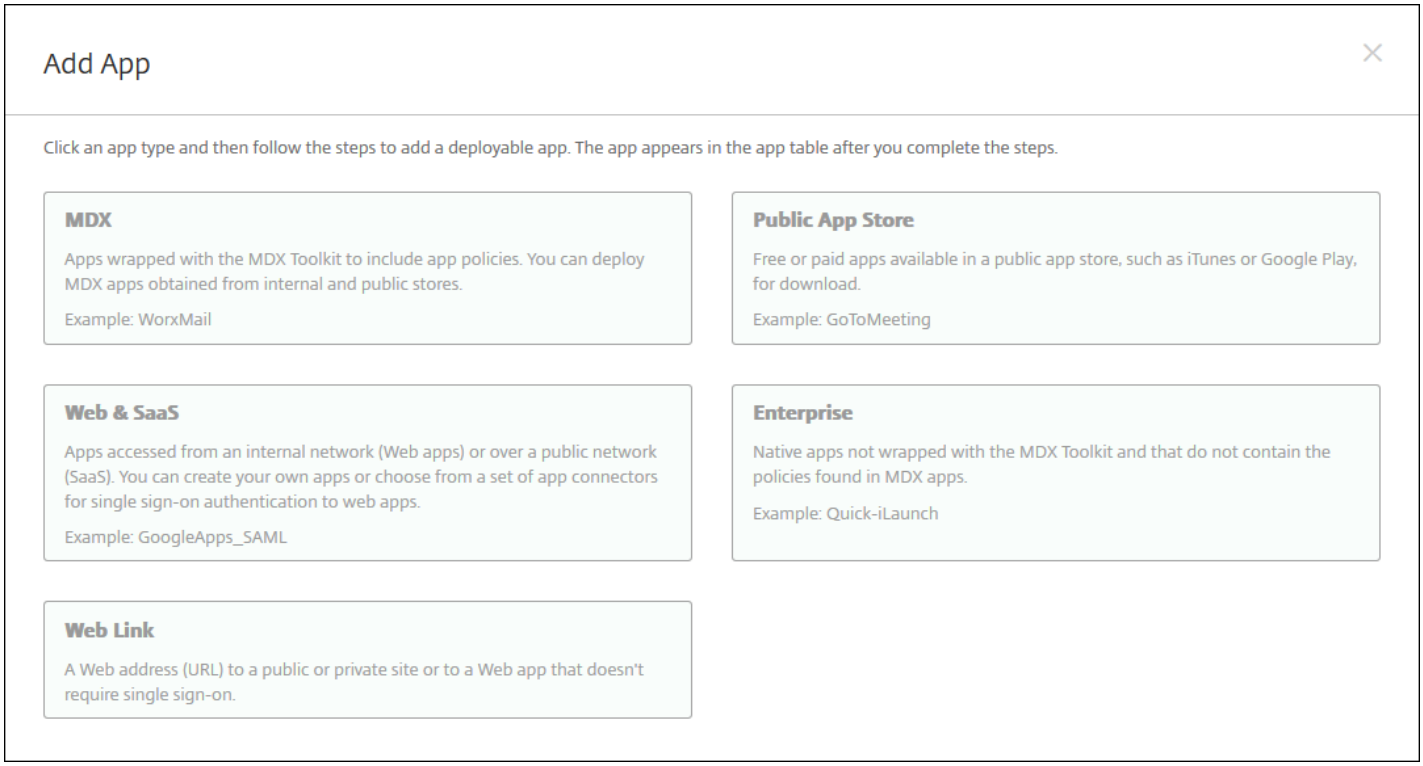


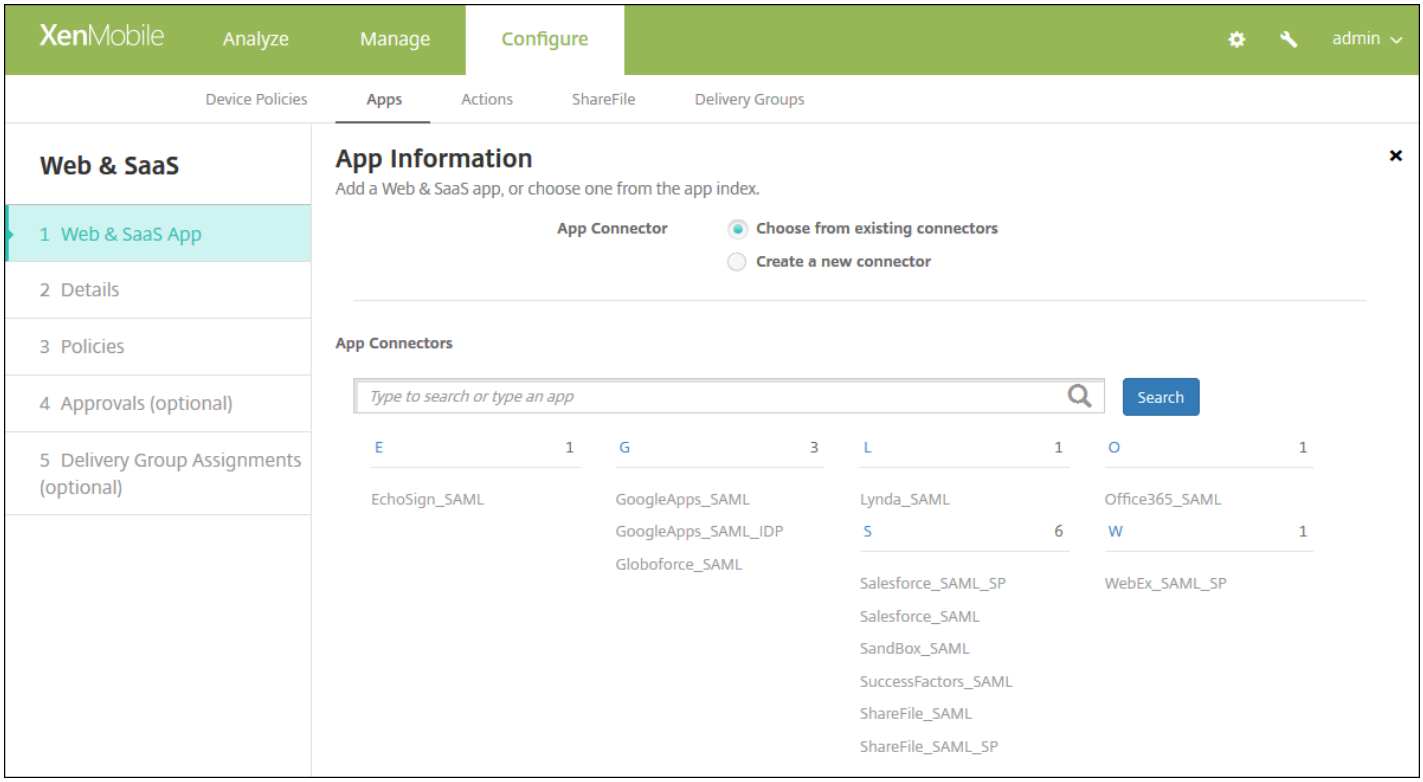


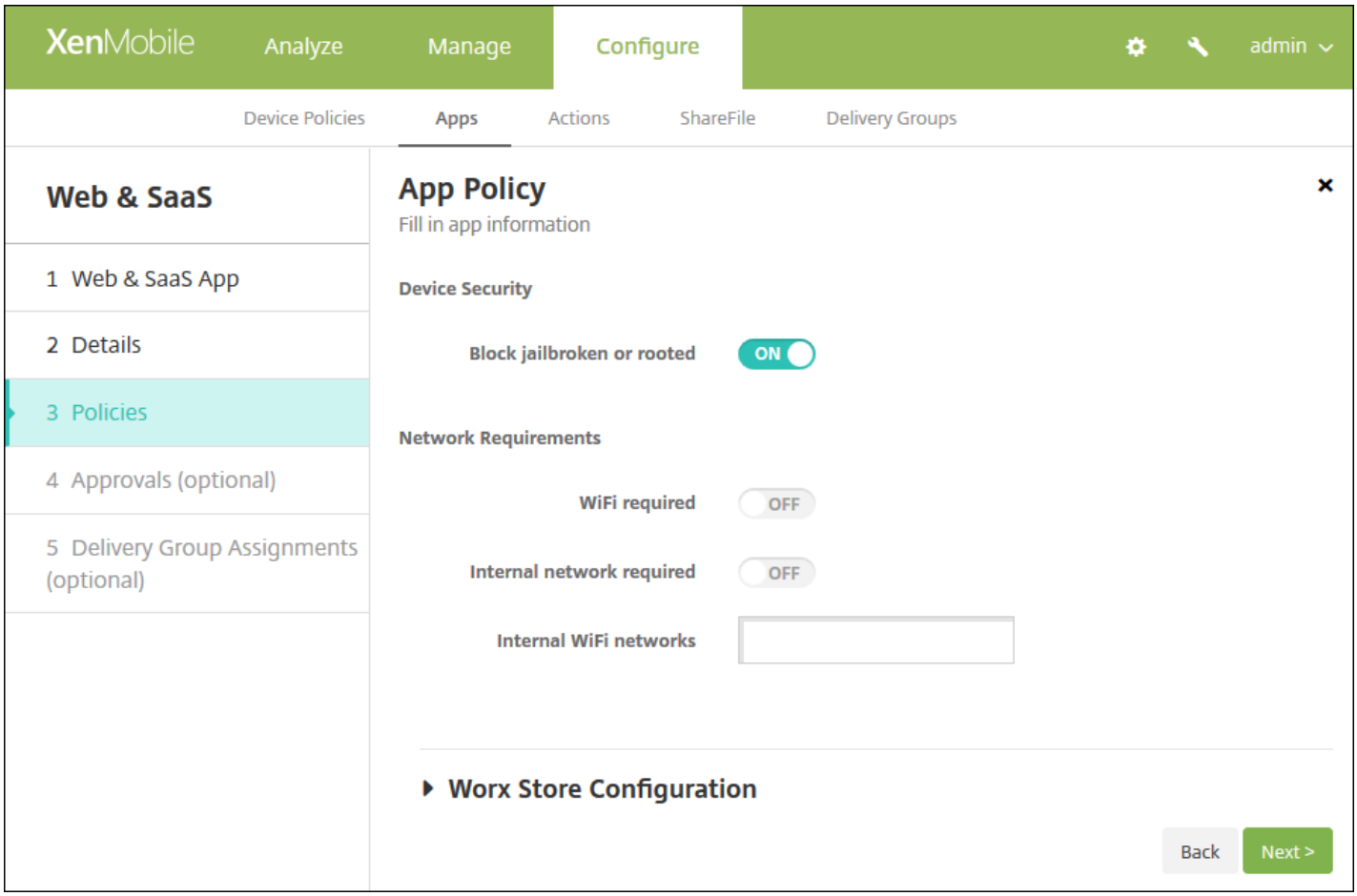


-
-
-
-
-
-
-

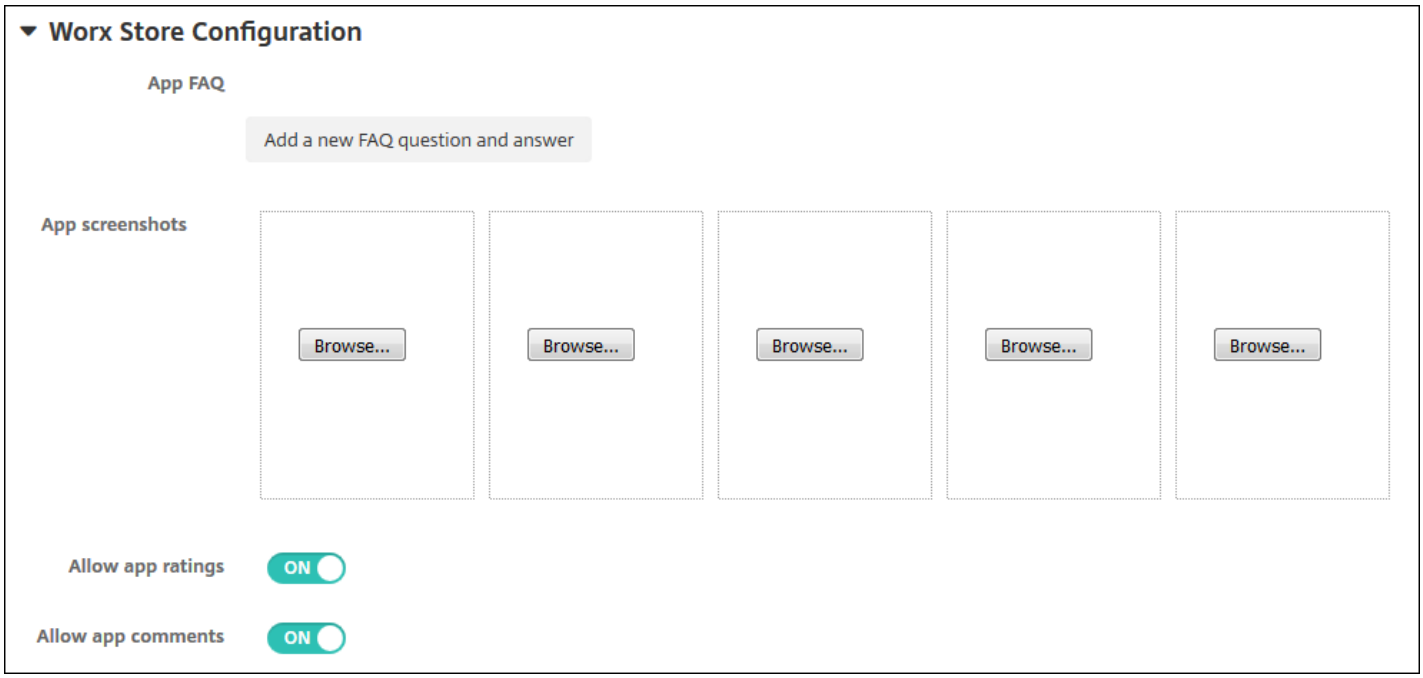
-
-
-
-
-
-
-
-



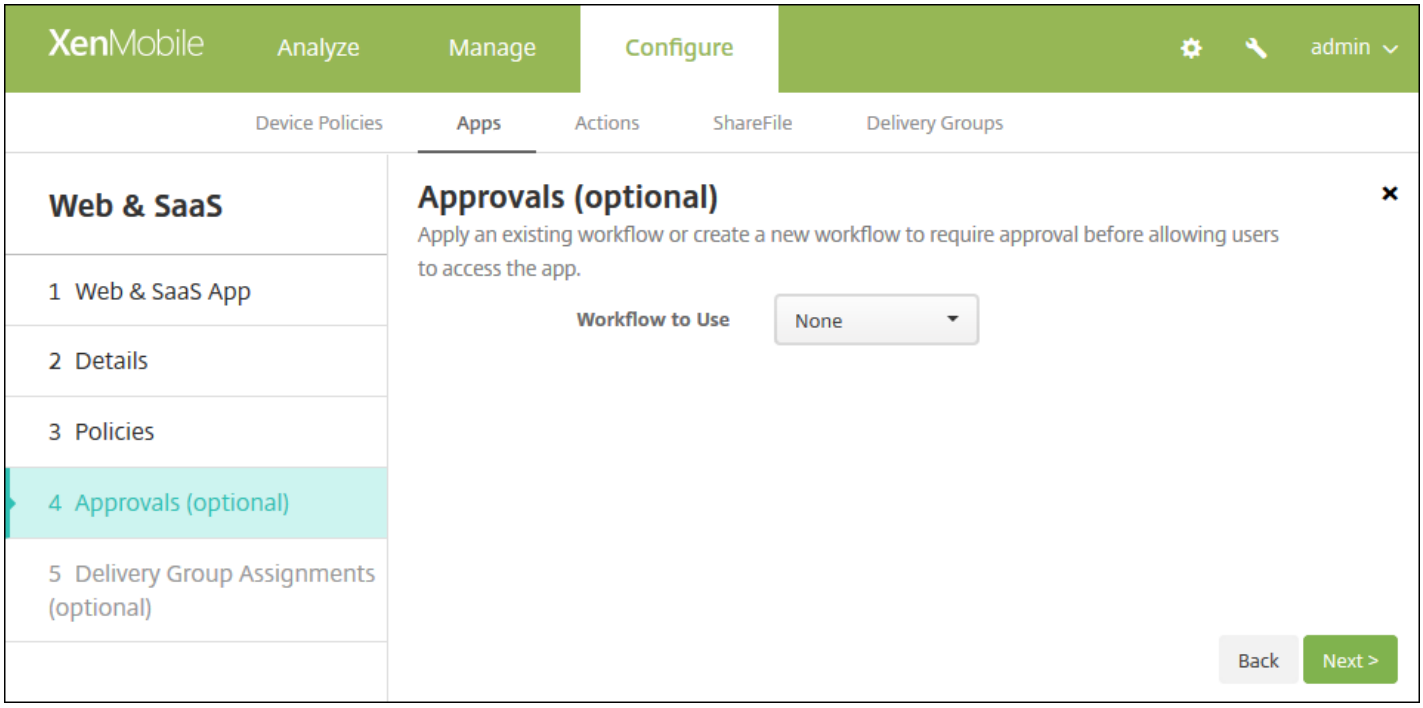


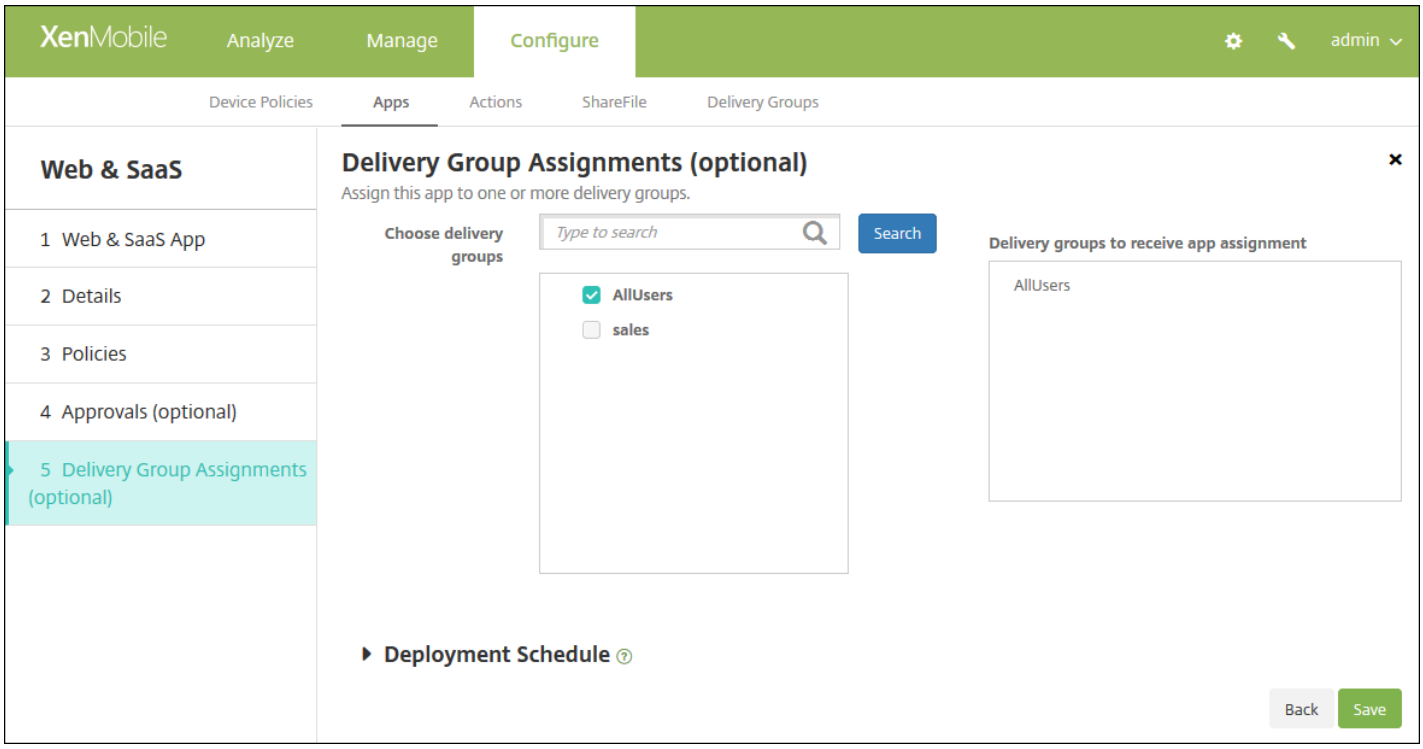


-
-

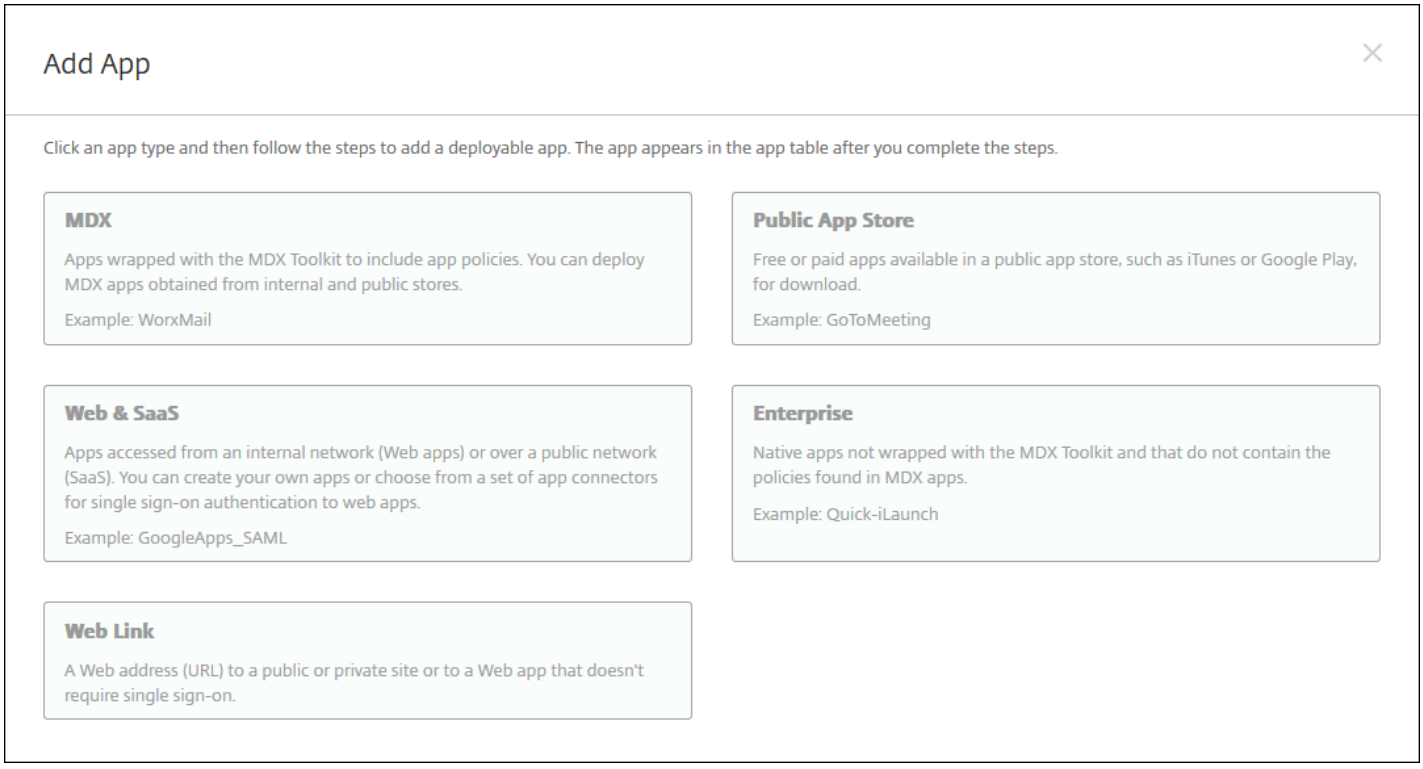


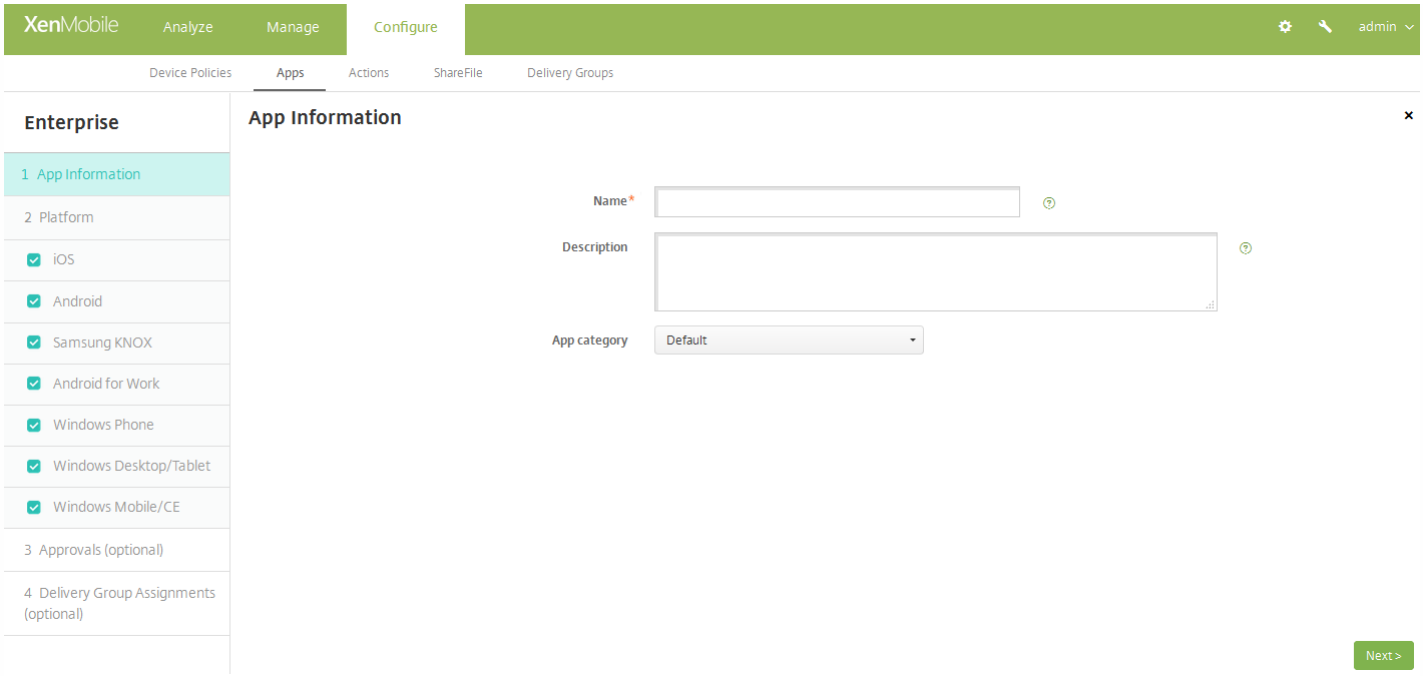
-
  -
  -
  -
  -





-
-
-
-
-
-
-



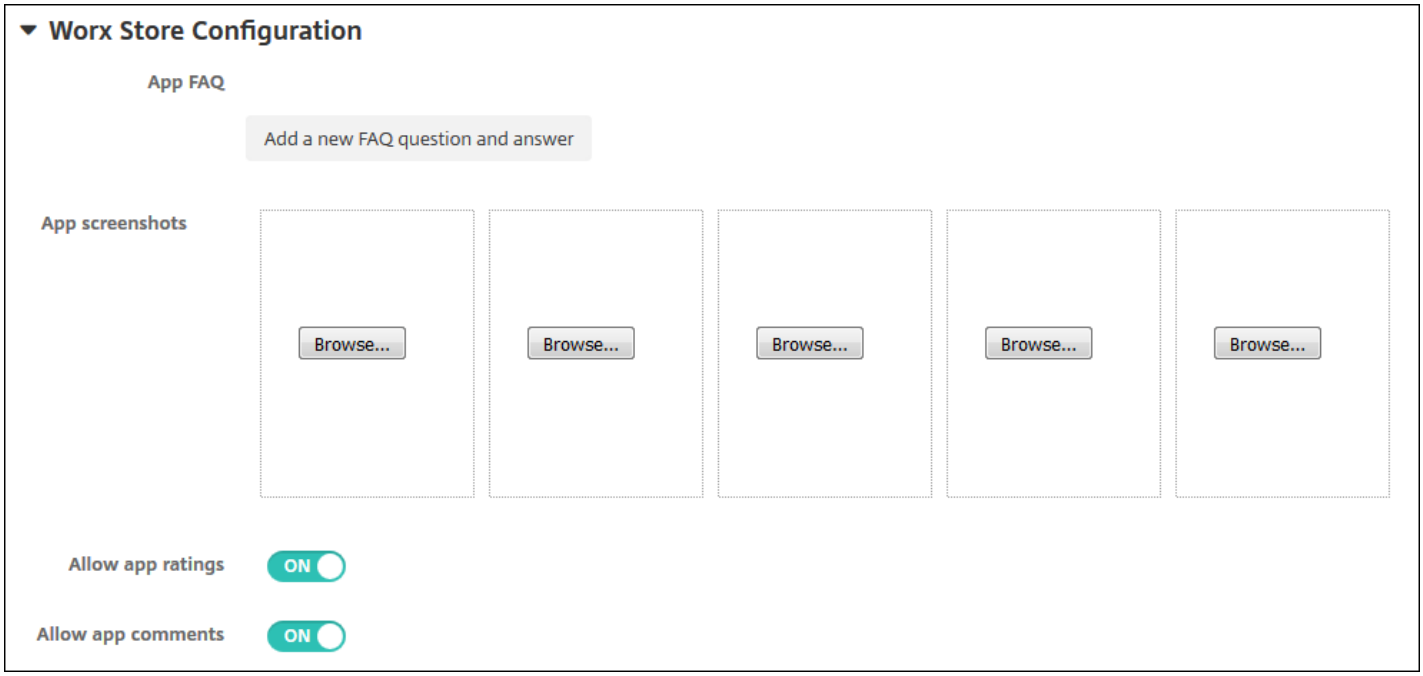


-
-
-

-
-
-
-
-
-

-
-

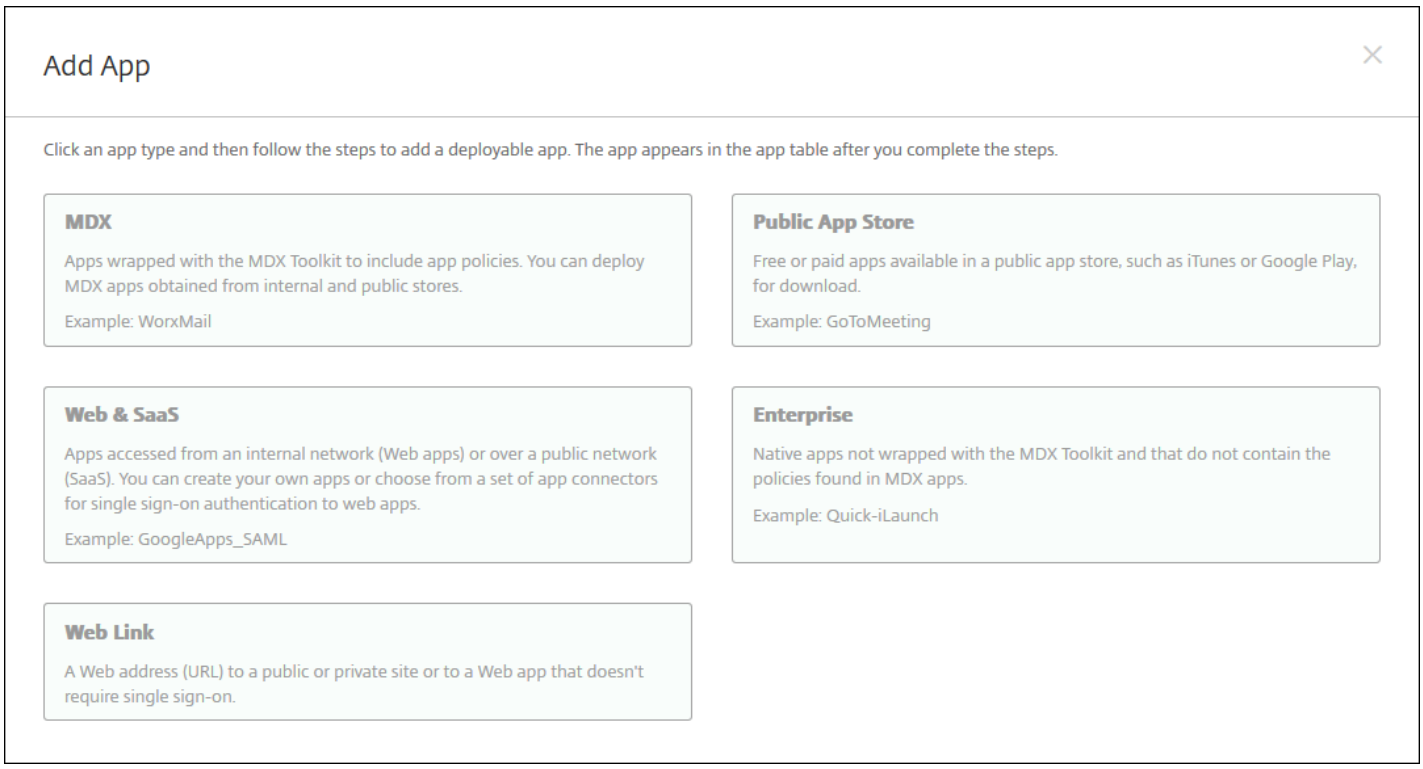
10. Configure the deployment rules

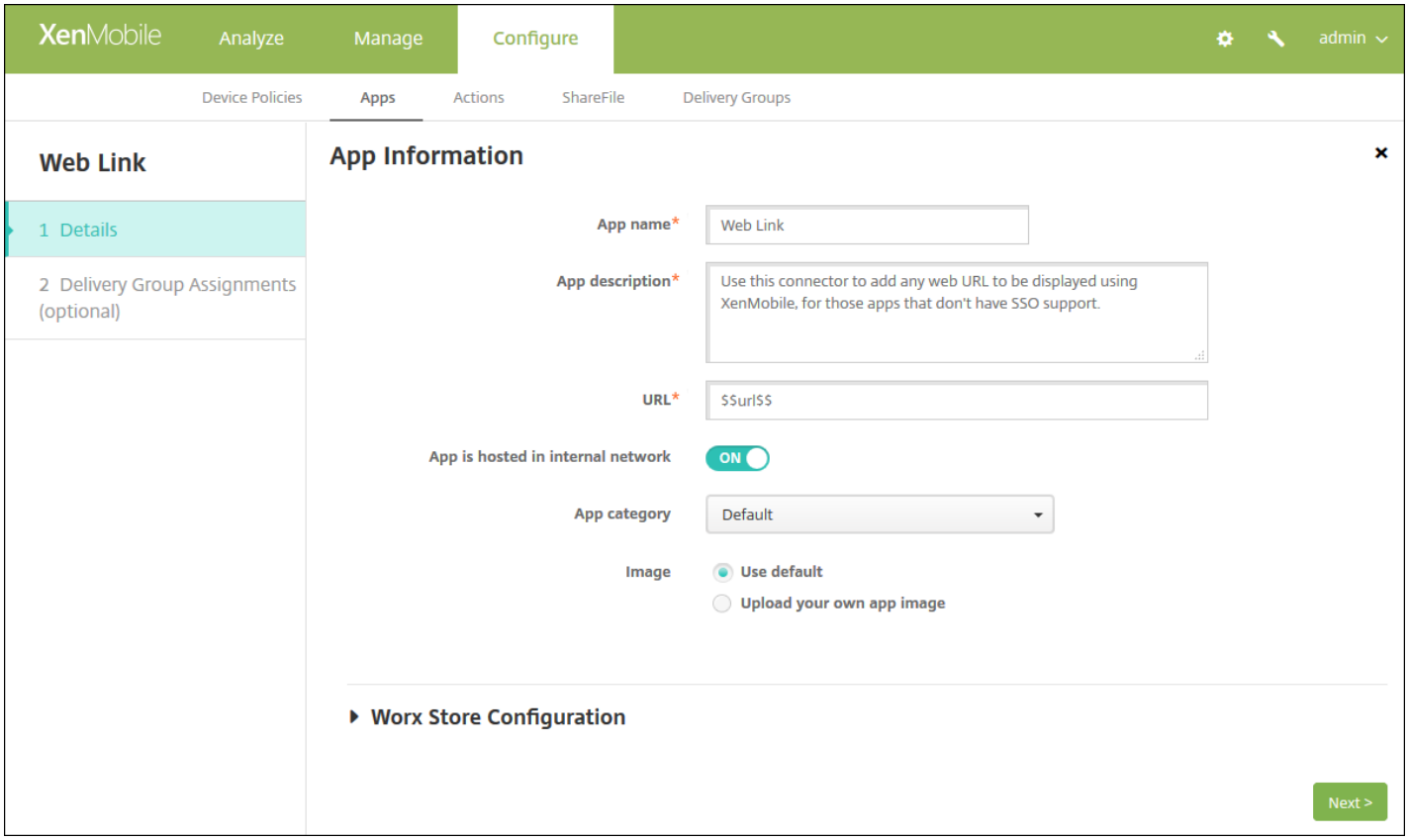


-
  -
  -
  -
  -

-

-
-
-
-
-
-

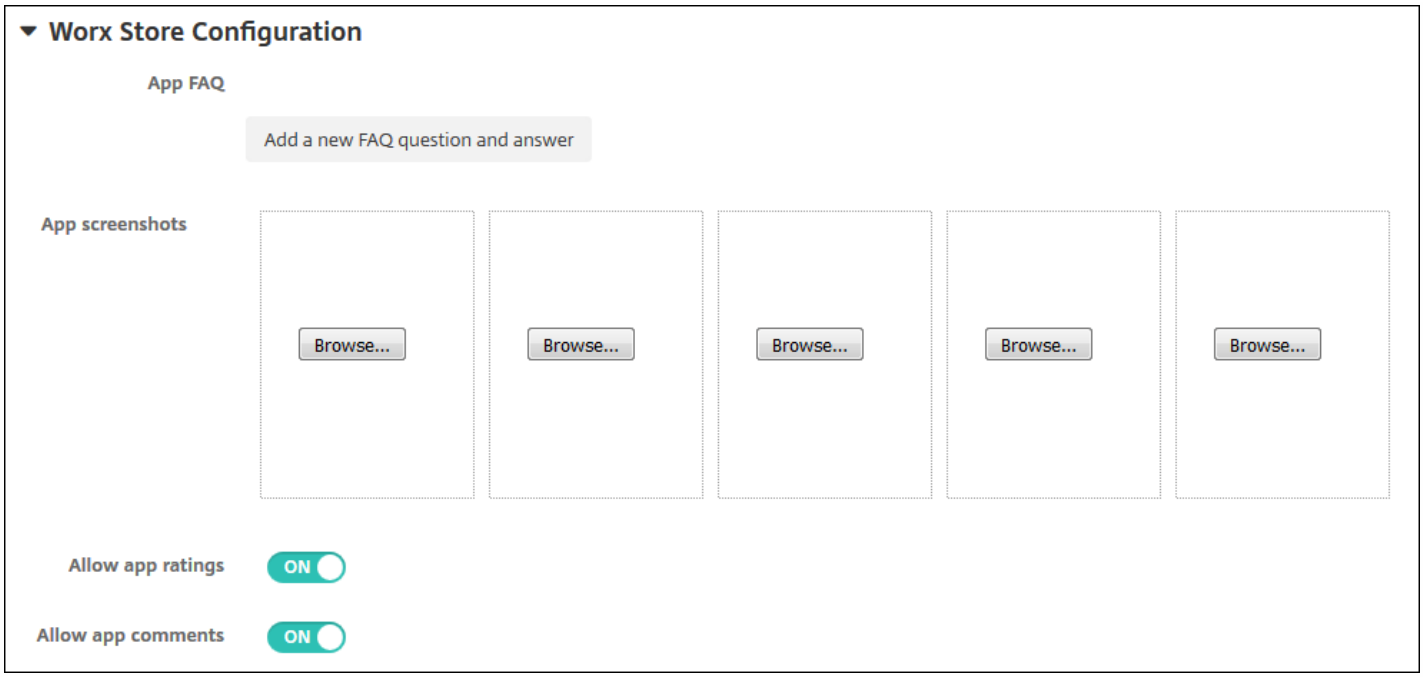




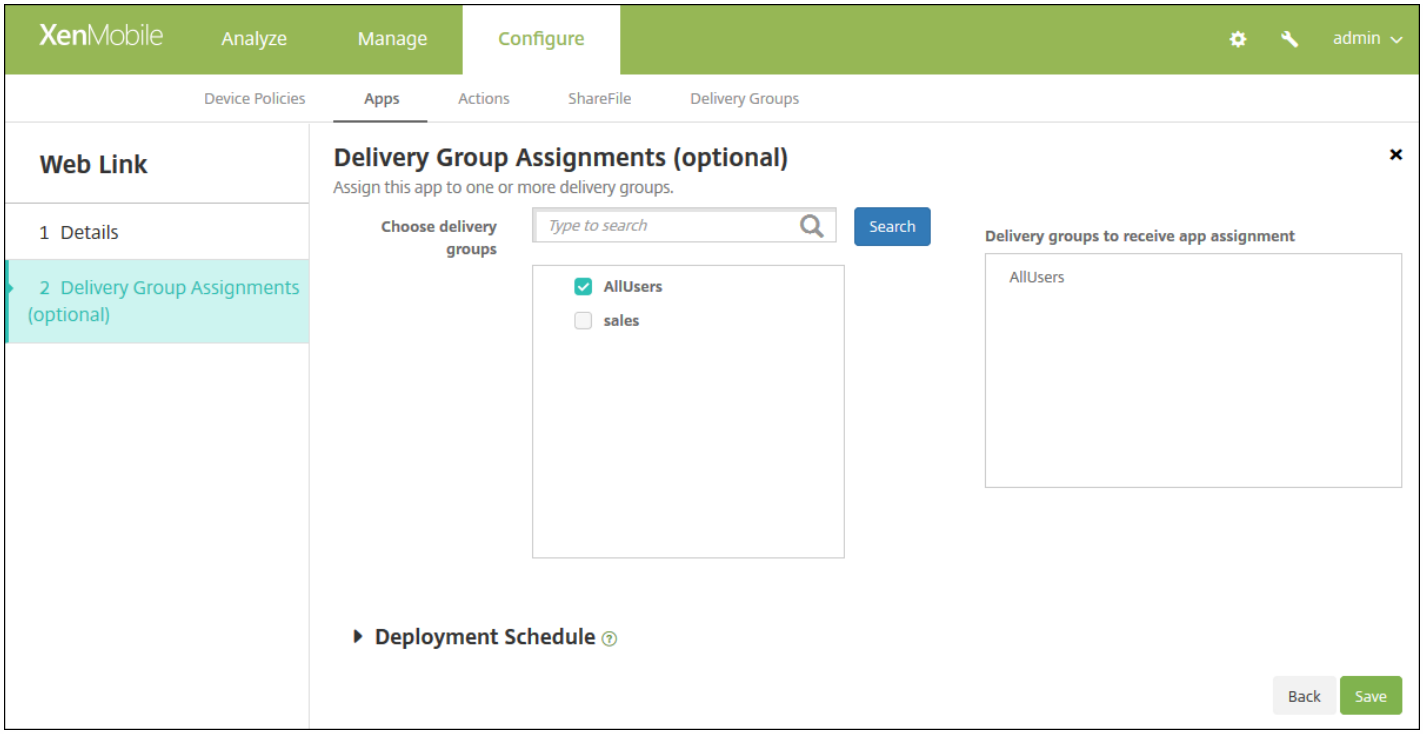
-
-
-

-

-
-

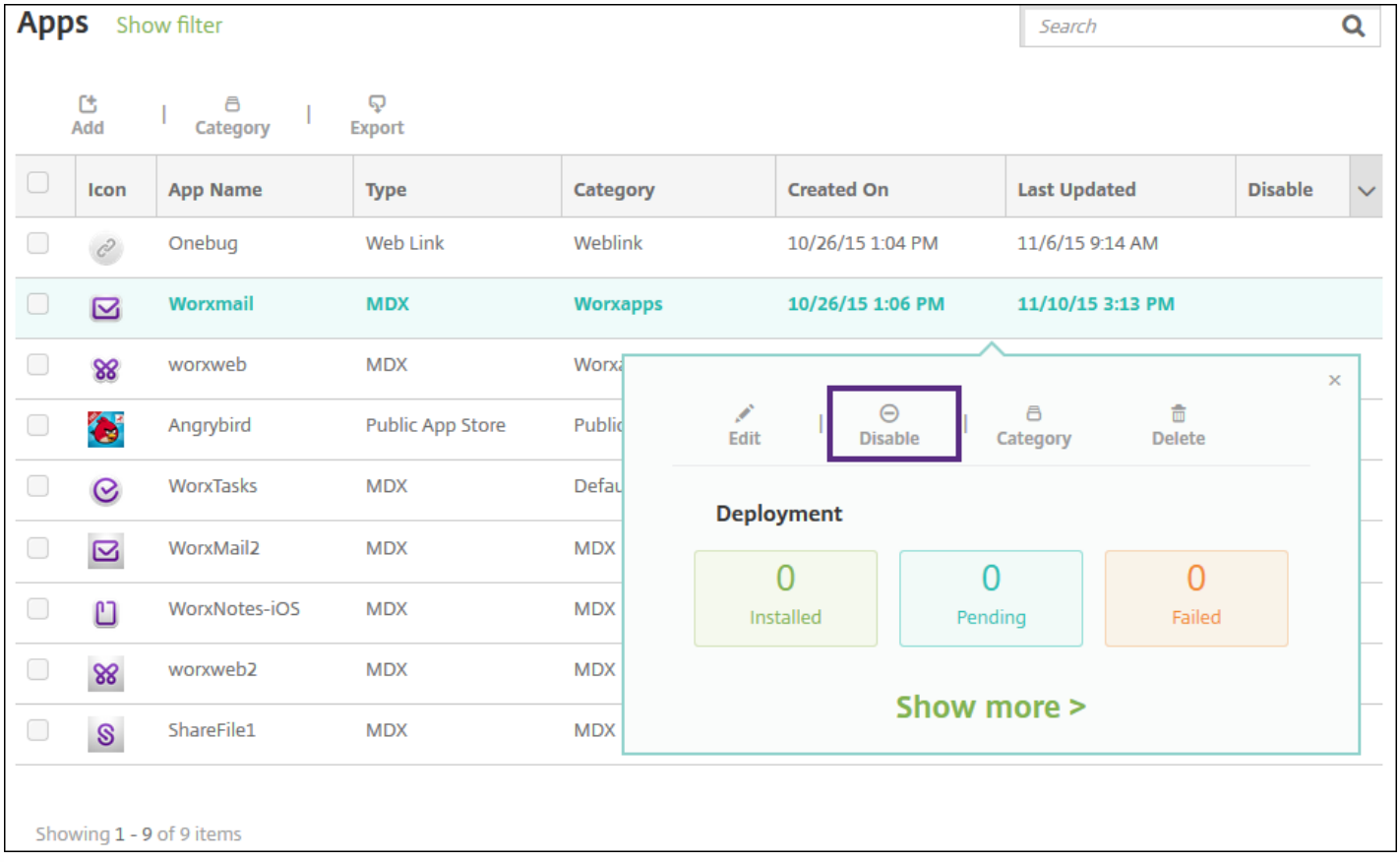


-
  -
  -
  -
  -



-
-
-
-
-
-
-

-
-

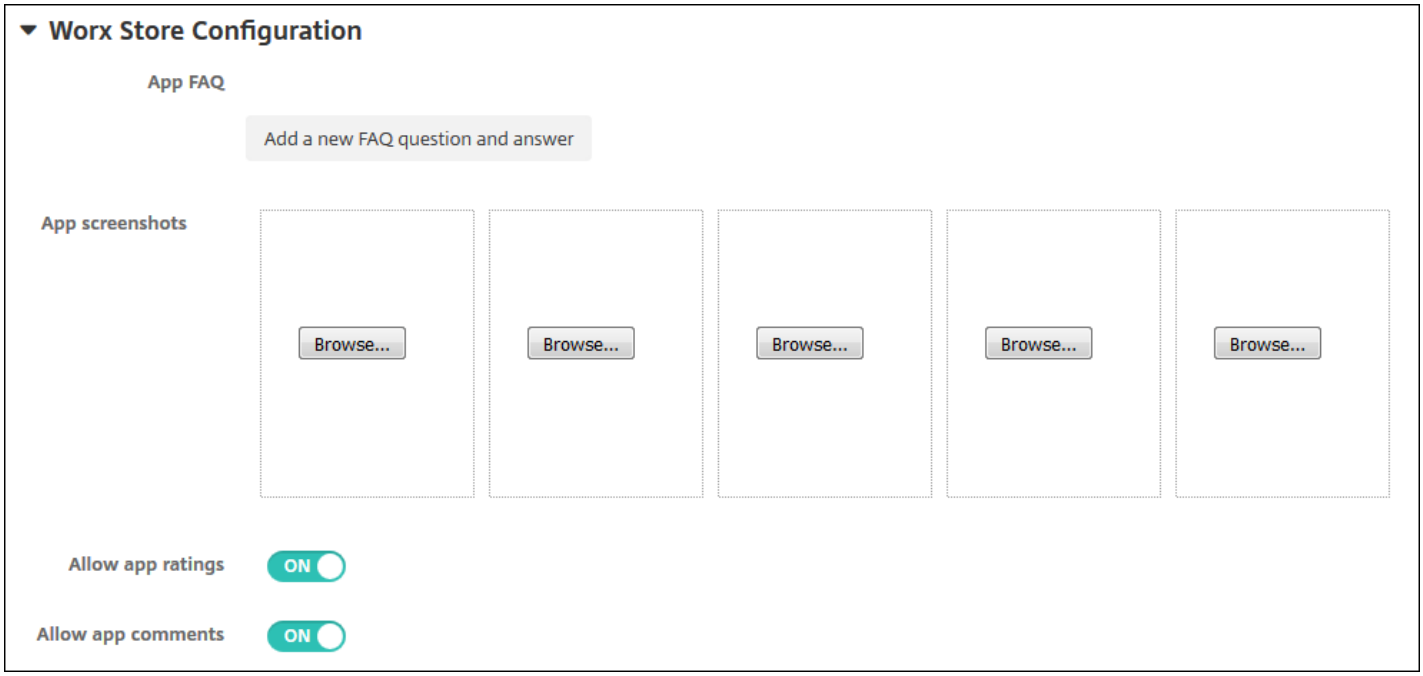


-

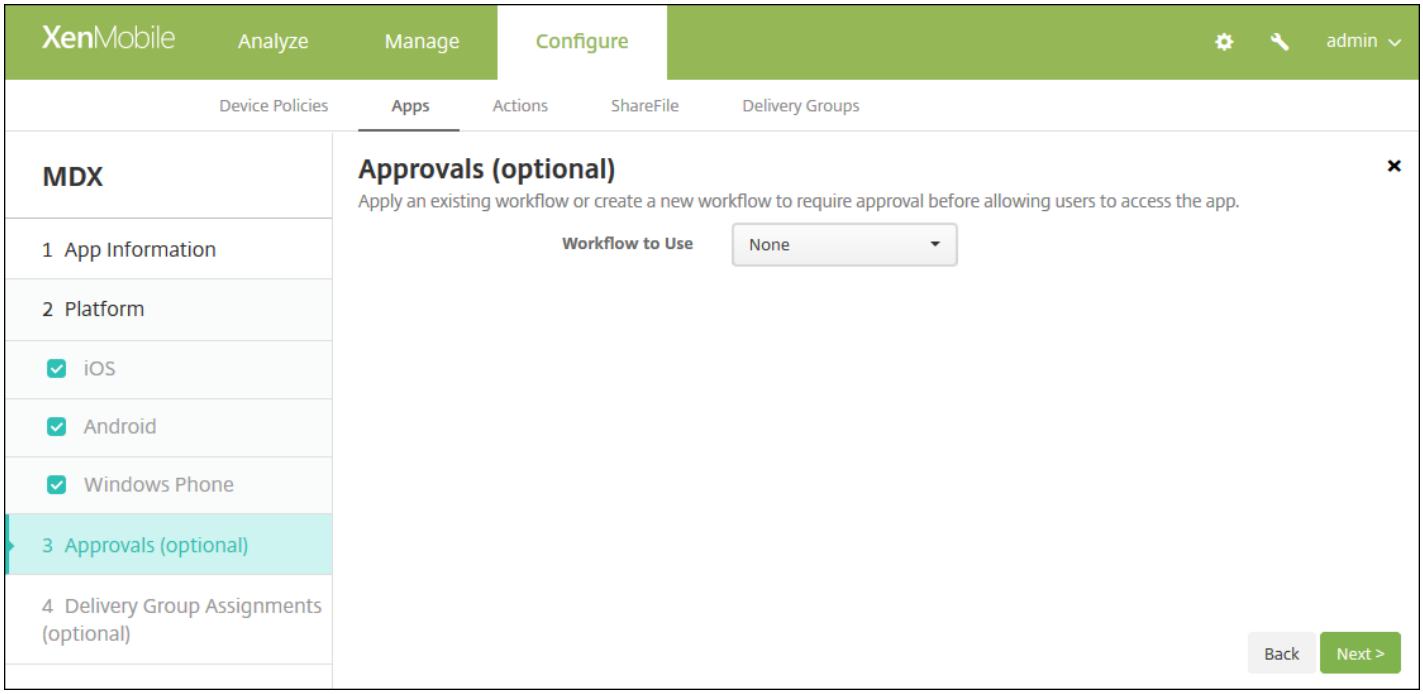
Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
	Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/11/15 8:55 AM	Disabled

-
-
-
-
-
-

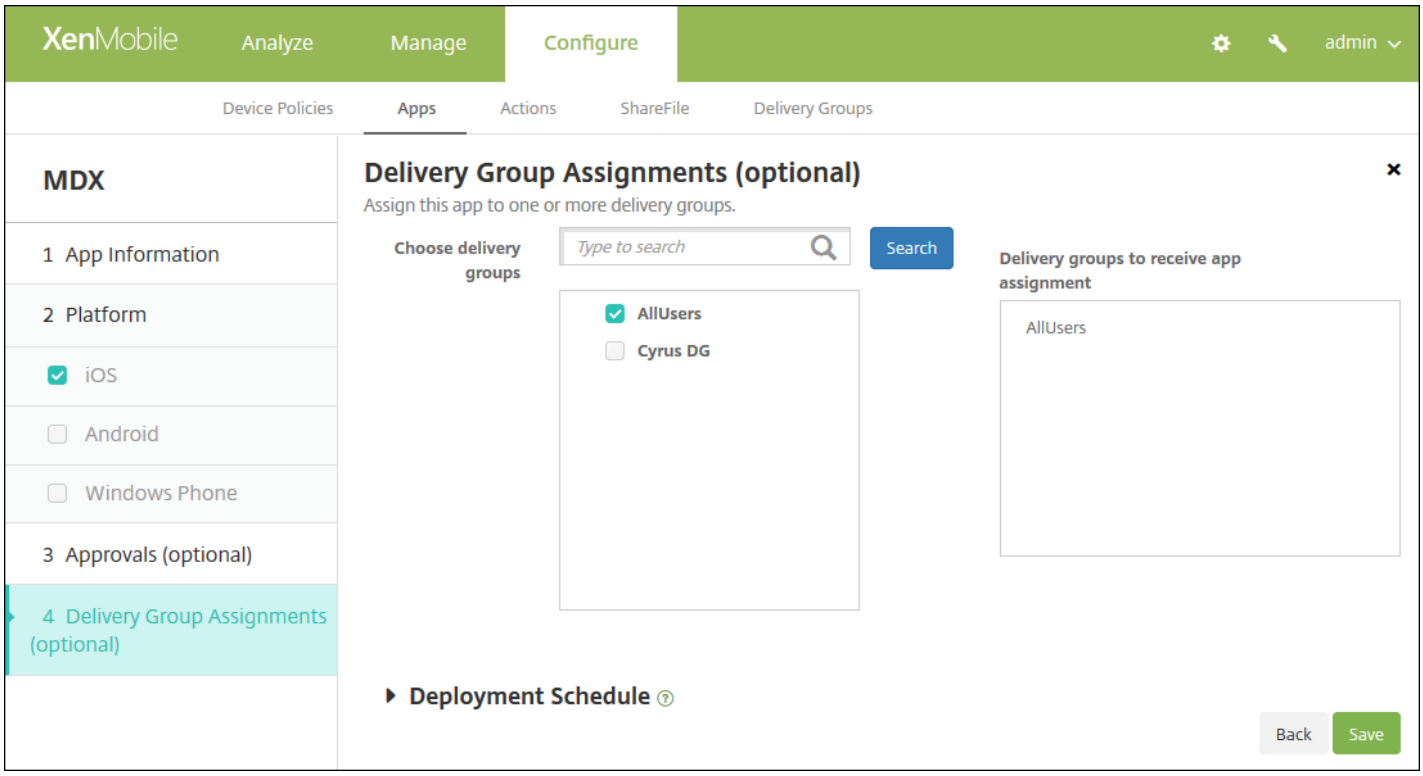
8. Configure the deployment rules



-
  -
  -
  -
  -



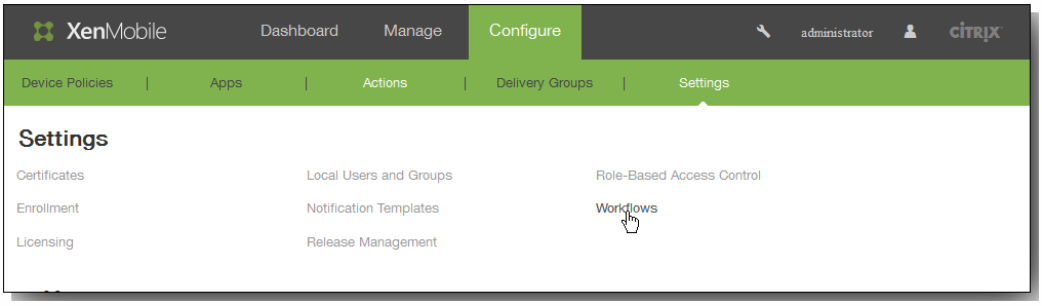
-
-
  -
  -
  -
  -
    -
    -
    -
    -
  -
  -
  -
  -
    -
    -
    -

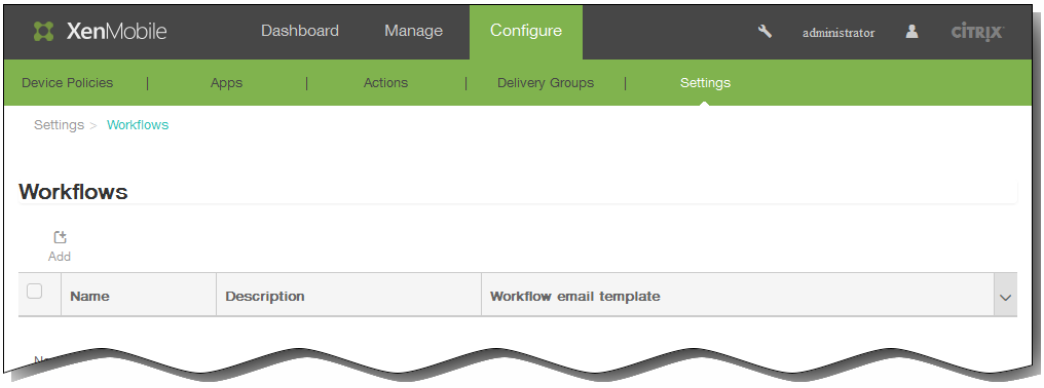


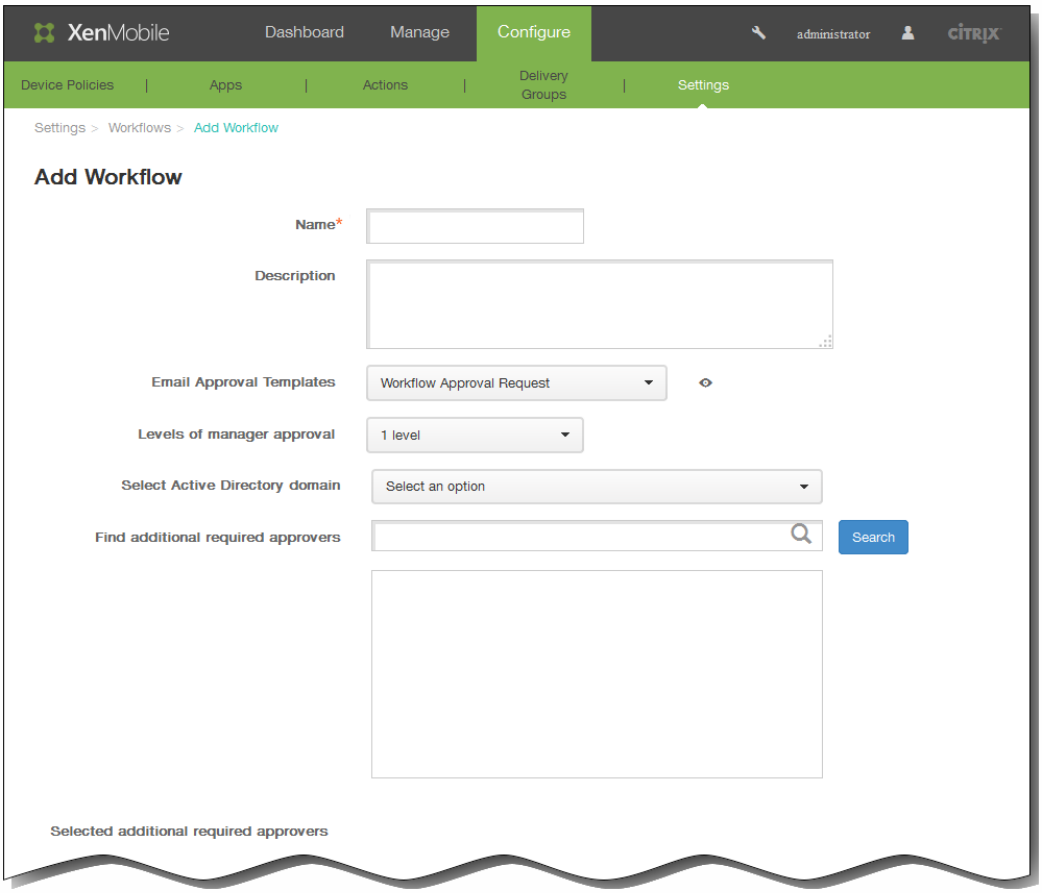
-
-
-
-
-
-
-

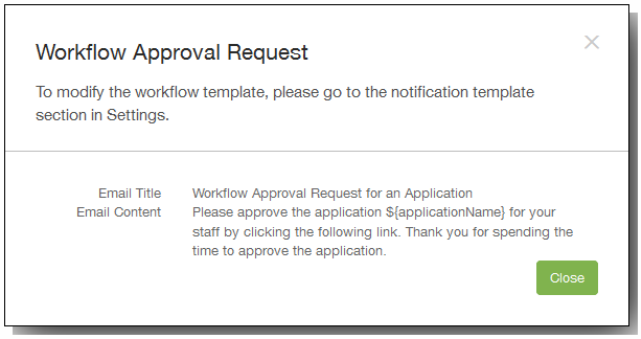
-
-

-
-





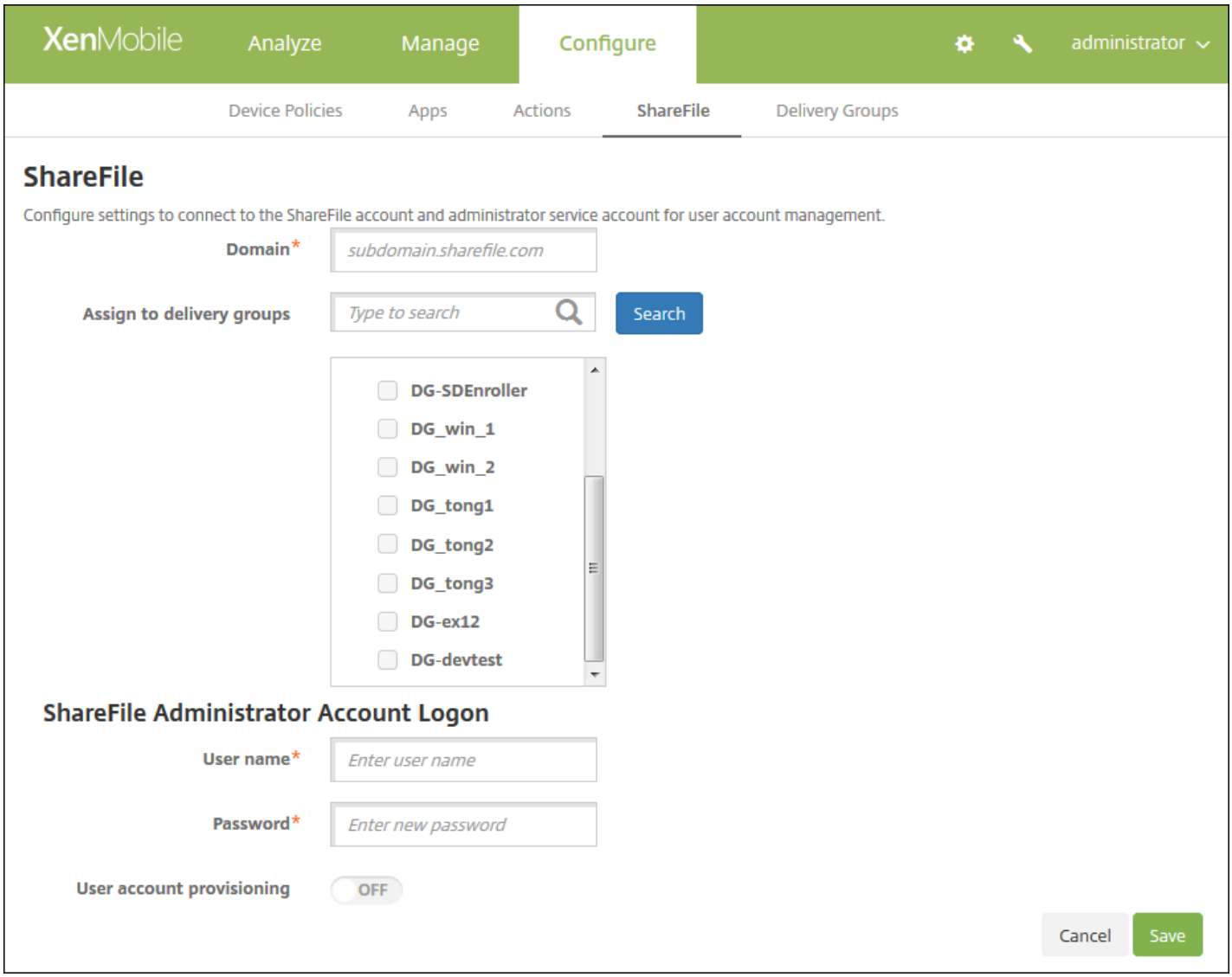




-
-

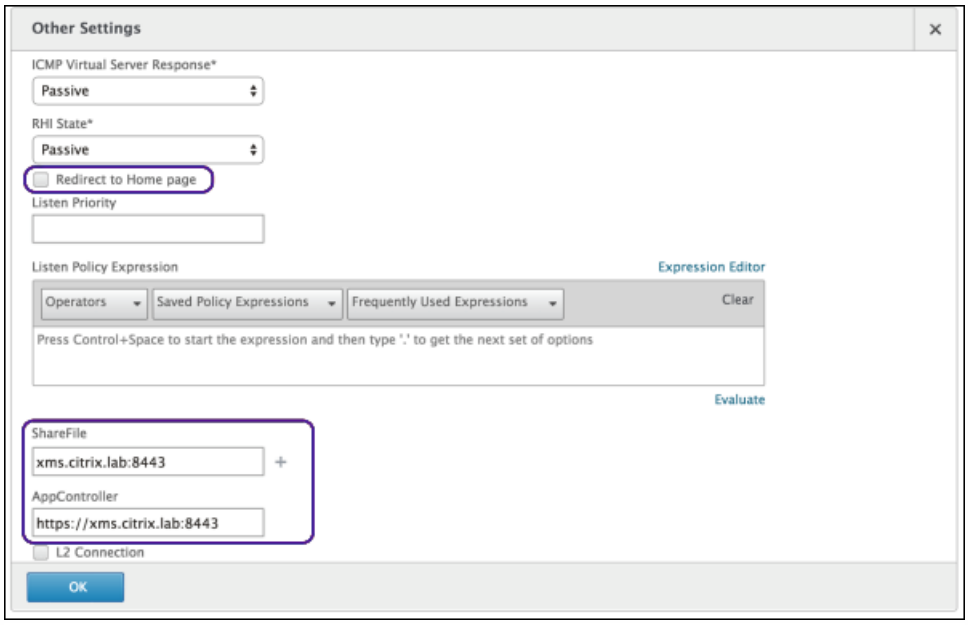
-
-

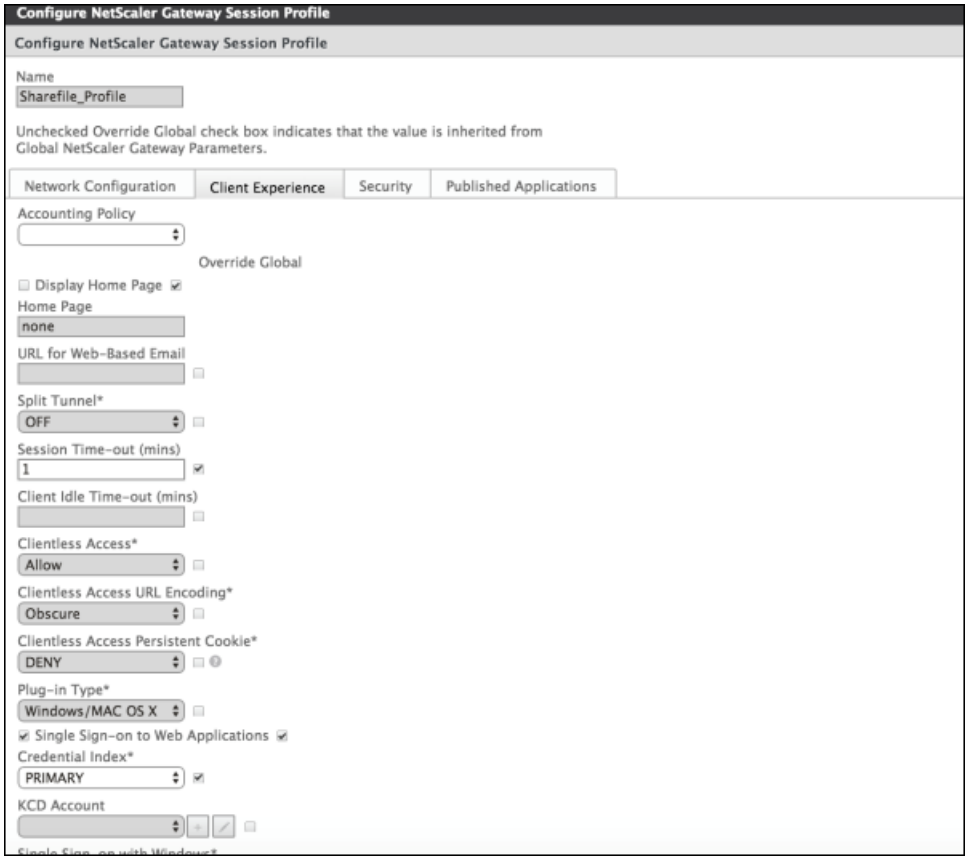
-
-
  -
  -
  -
-
-



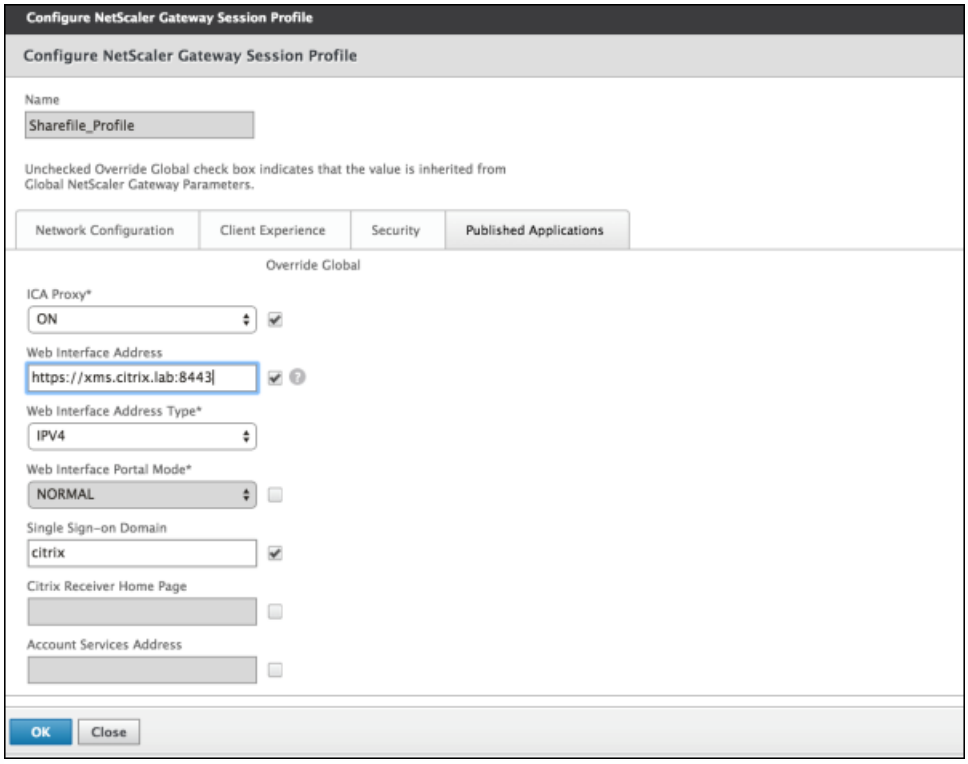
-
-
-
  -
  -
  -

-
-
-

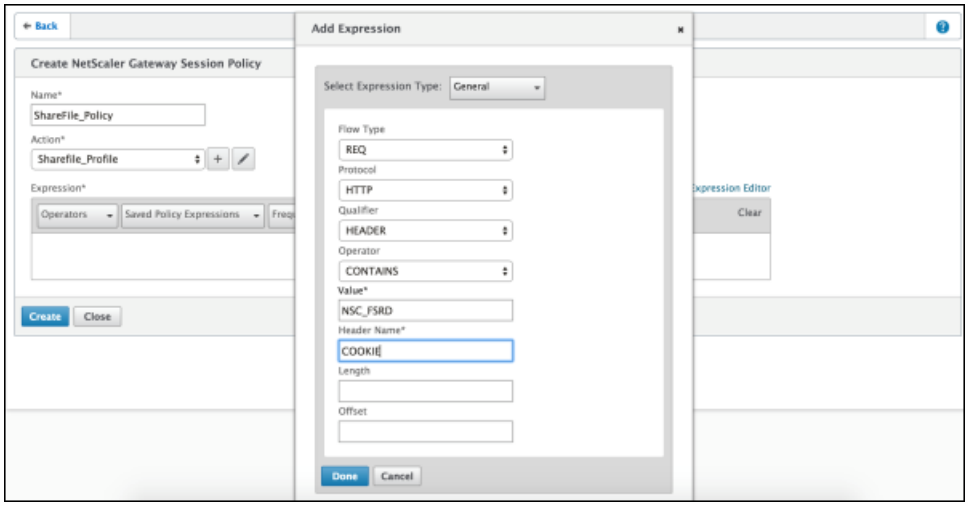




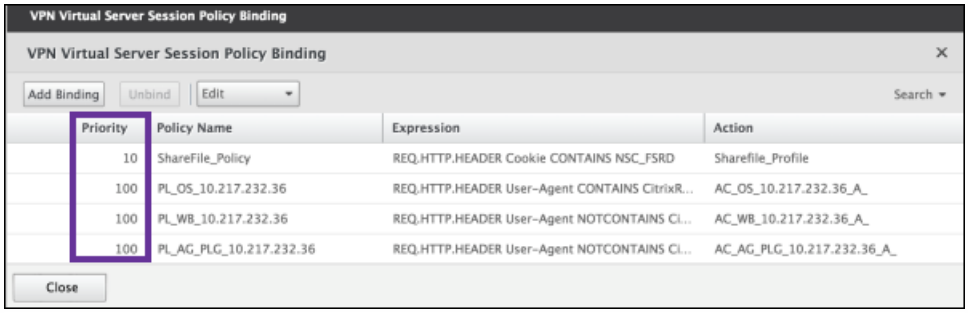
-
-
  -
  -
  -
  -
-

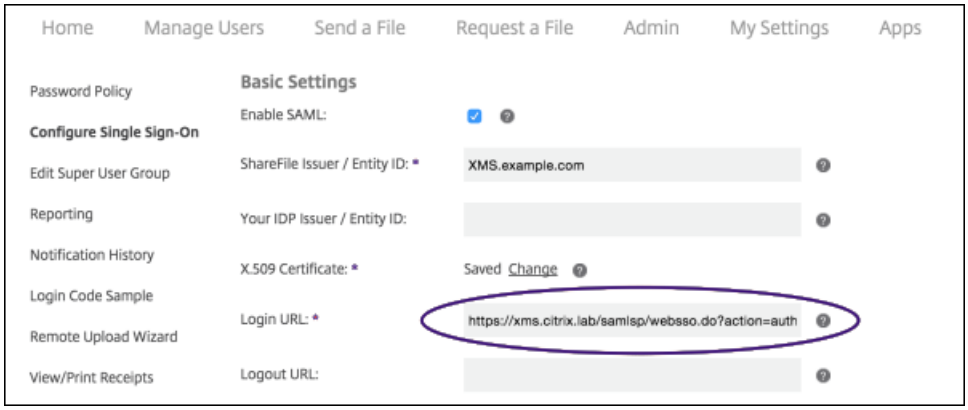


-
-
-

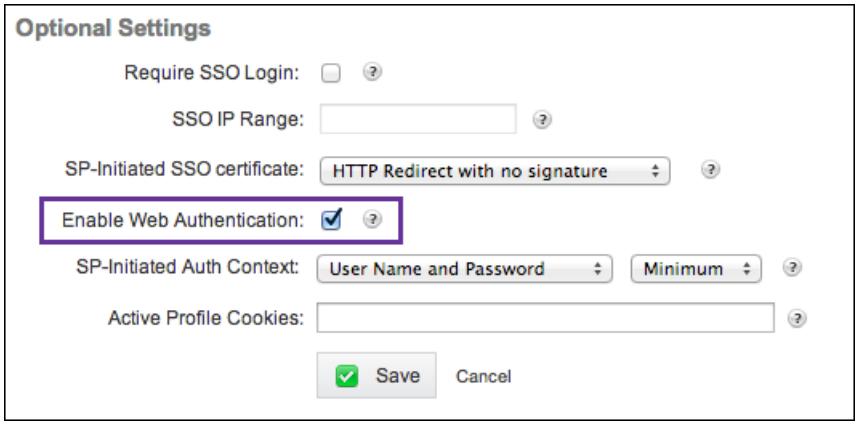


-
-
-





-
-
-



-
-
-
-

-
-

-
-

-

-
-
-
-

-
-
-
-
-
-
-
-

13. Configure deployment rules

-
-
-
-
-

Macros in XenMobile

Mar 29, 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.

XenMobile Client Settings

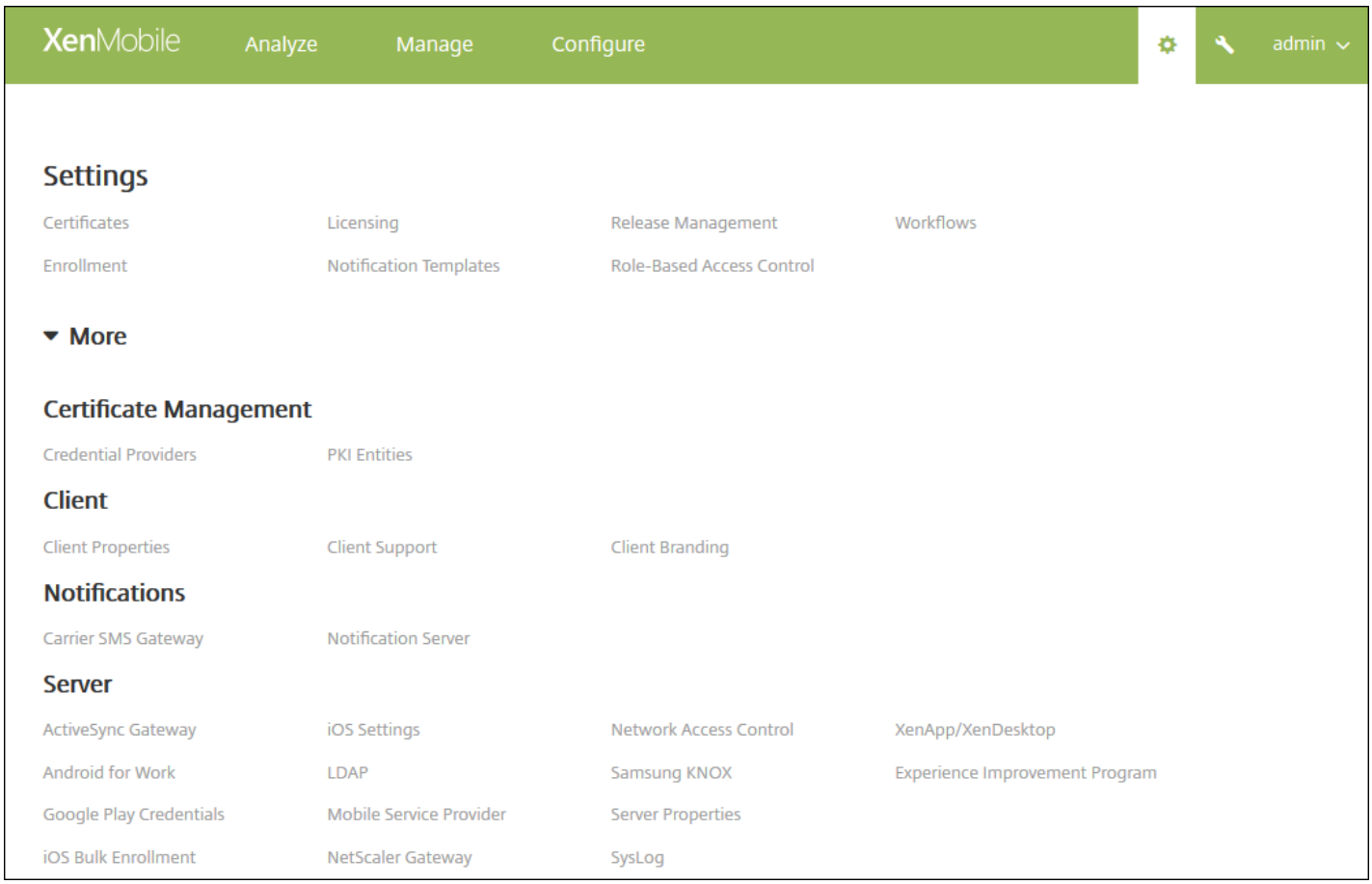
Jan 16, 2015

The XenMobile client settings you configure in the XenMobile console include:

- Client Properties
- Client Support
- Client Branding

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

3. Under **Client**, click the option you want to configure.



To create custom Worx branding for mobile devices

Jul 15, 2016

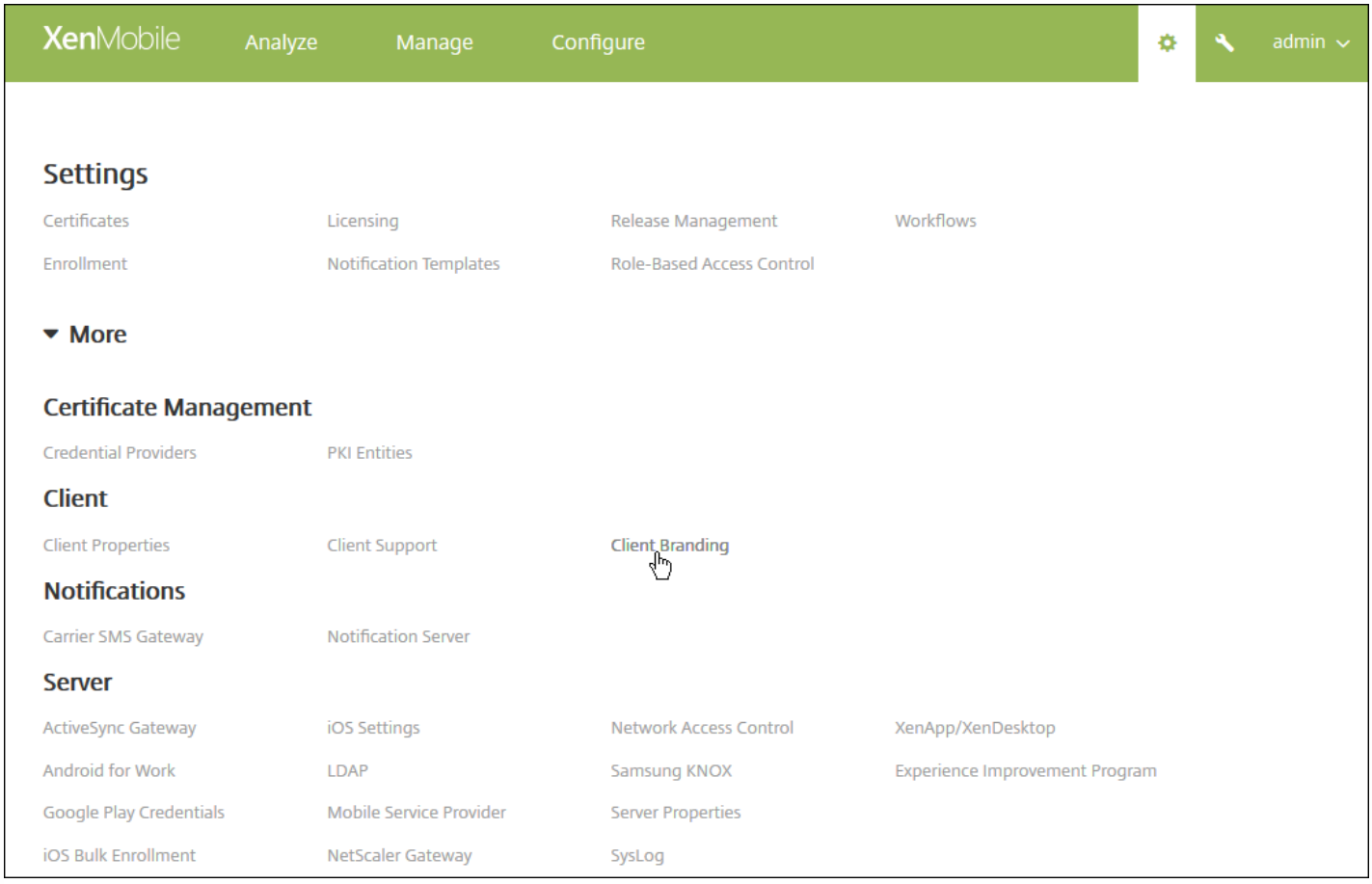
You can set the way apps appear in the store and add a logo to brand Worx Home and the WorxStore on mobile devices for iOS and Android.

Note: Before you begin, make sure you have your custom image ready and accessible.

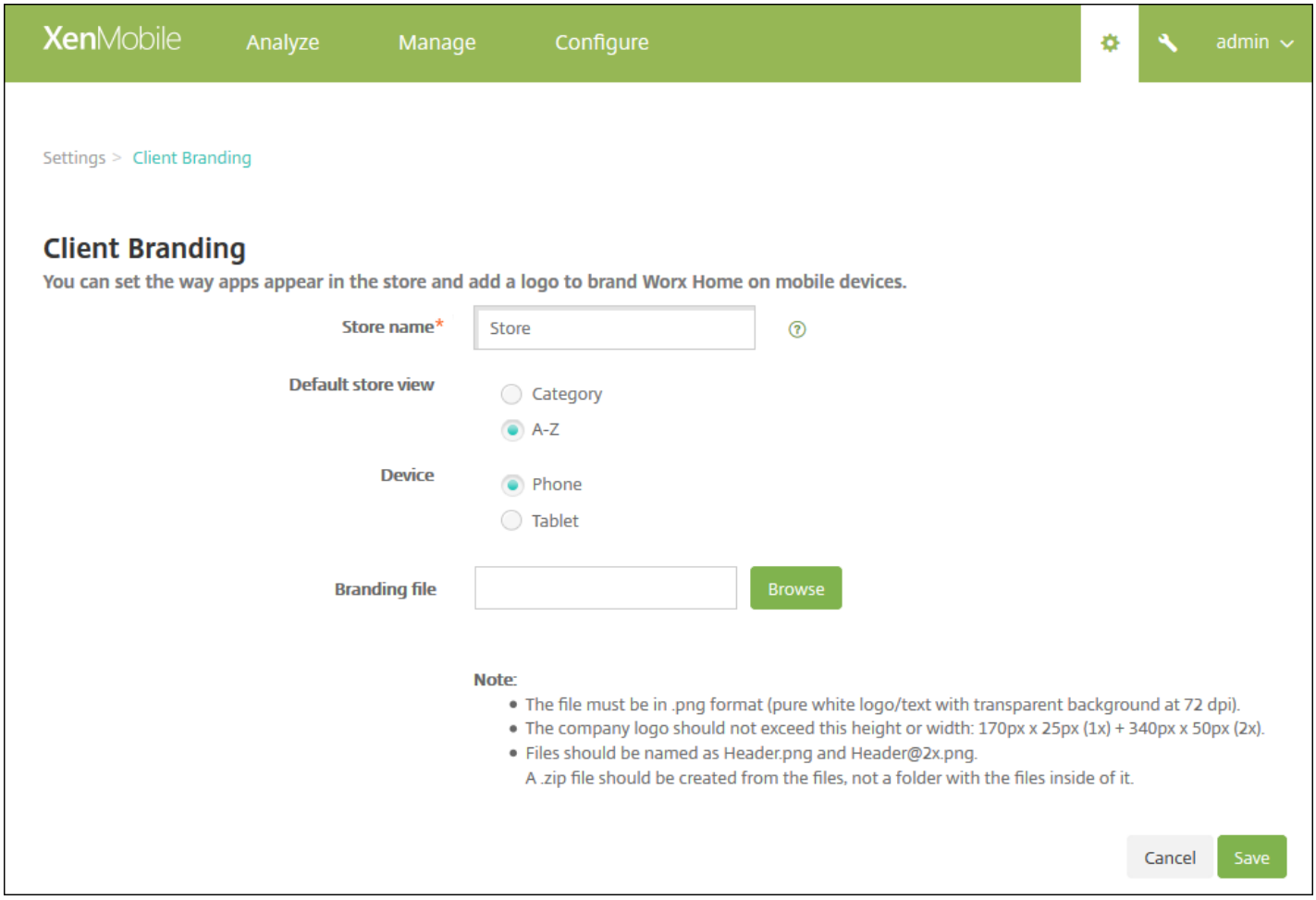
The custom image must meet these requirements:

- 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**.

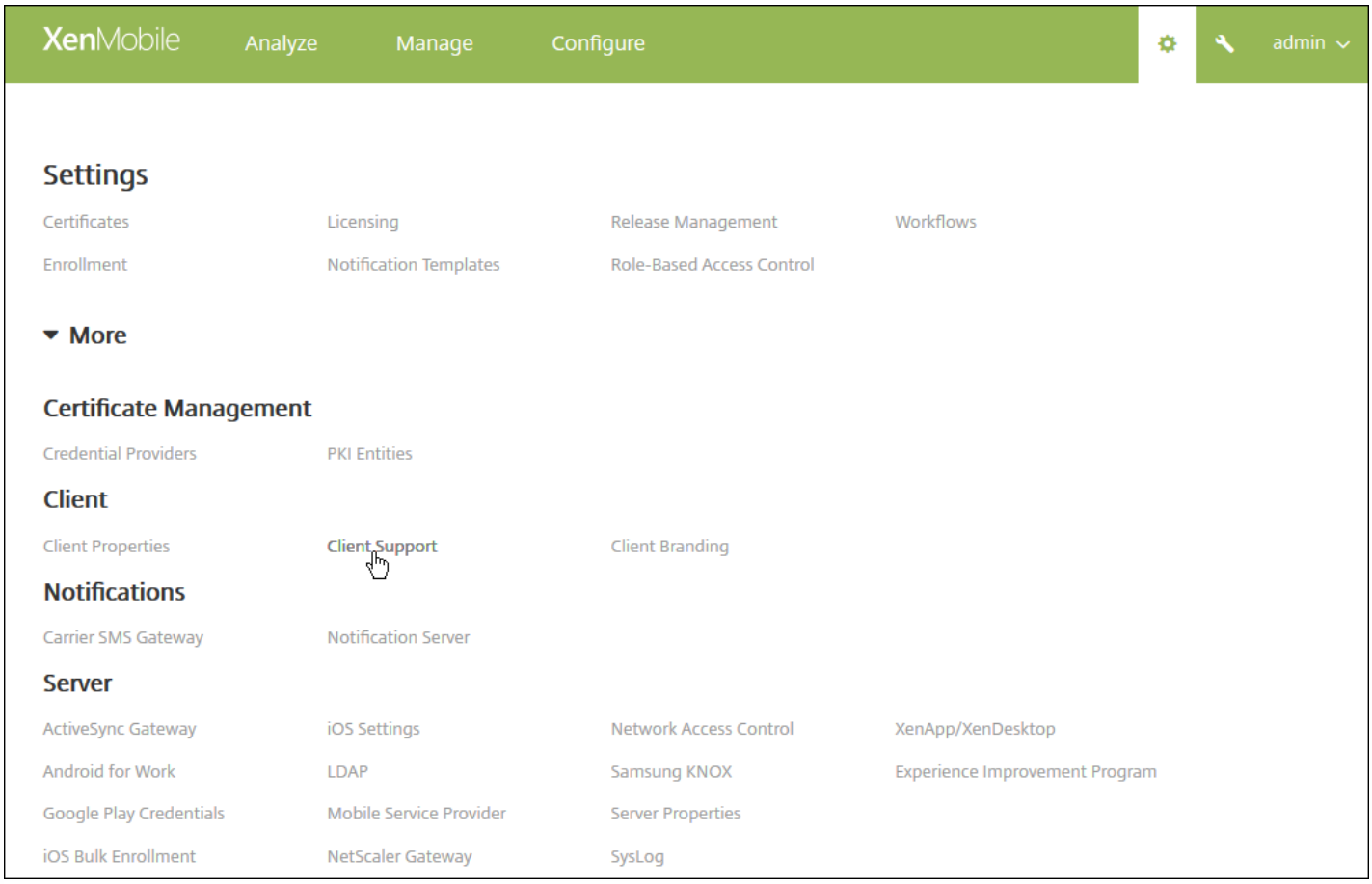
To deploy this package to users' devices, you need to create a deployment package and deploy the package to users' devices.

Creating Worx Home and GoToAssist support options

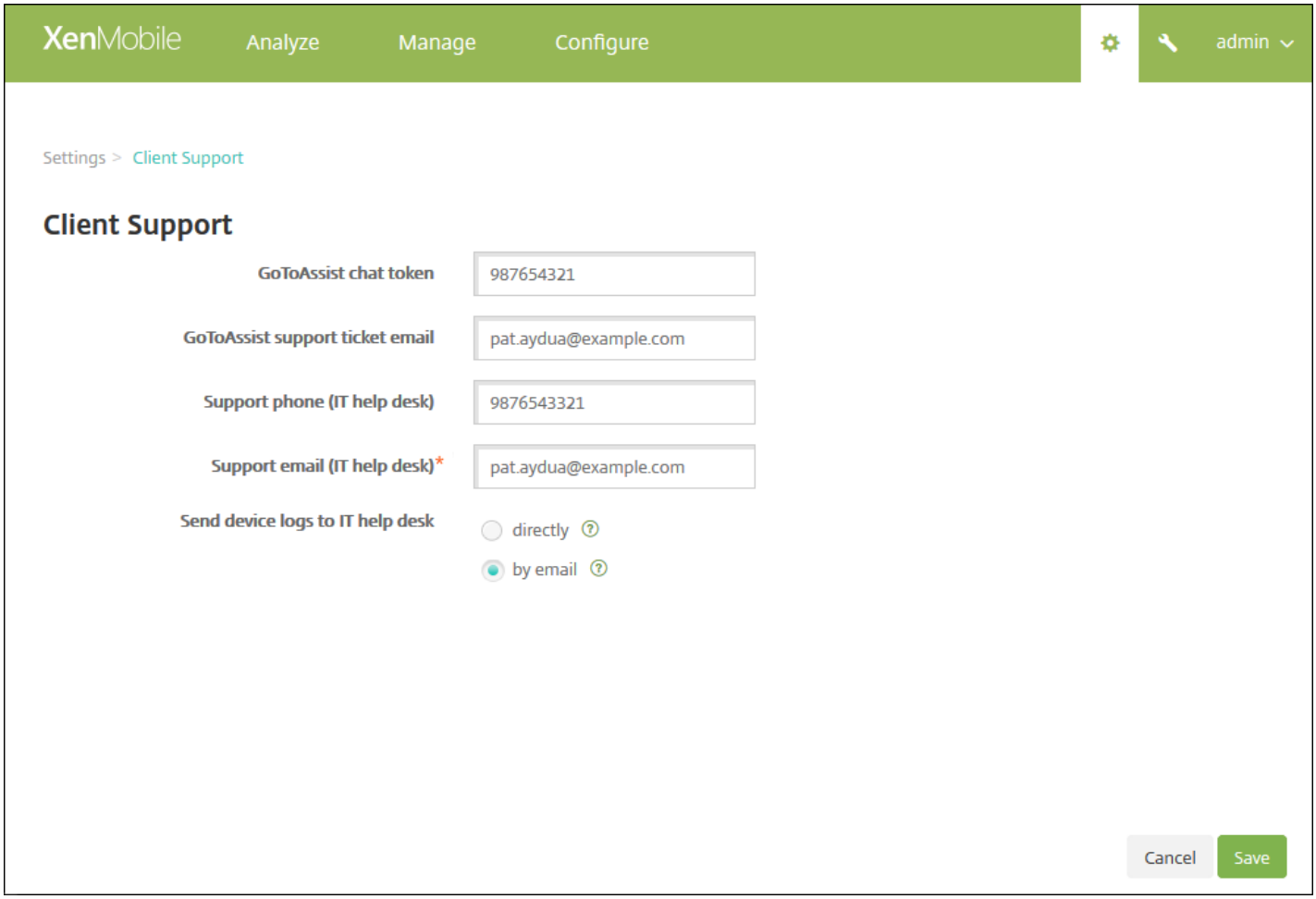
Apr 19, 2016

You can give your users different ways to contact your support staff by providing email addresses, phone numbers, and GoToAssist tokens. When users request assistance from their devices, they see the options that you have set.

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:

- **GoToAssist chat token**: Type the token users receive to initiate a GoToAssist session.
- **GoToAssist support ticket email**: Type email address users use for GoToAssist support tickets.
- **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 then sent directly to ShareFile; otherwise, they are sent to XenMobile and then emailed to the IT help desk. In addition, the **If sending directly fails, use email** option appears, which is enabled by default. You can disable this option if you do not want to use the client's email to send the logs if there is a server problem. If, however, you disable this option and there is a server problem, the logs are not sent.
  - When you enable **by email**, the client's email is always used to send the logs.

4. Click **Save**.

To add, edit, or delete client properties

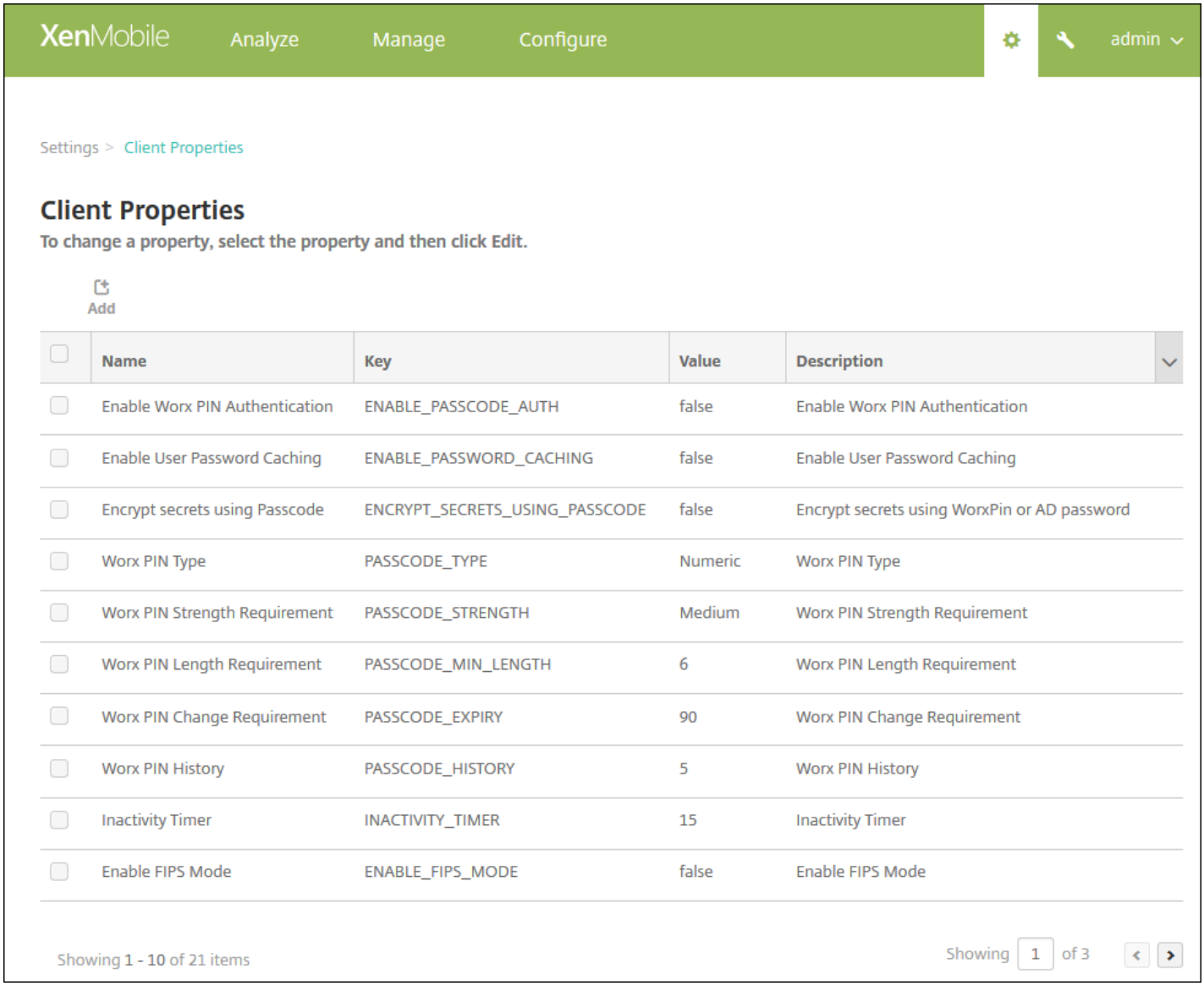
Jan 06, 2017

Client properties contain information that is provided directly to Worx Home on user devices. You can use these properties to configure advanced settings, such as the Worx PIN. You obtain client properties from Citrix support.

Note: Starting with version 10.4, Worx PIN is renamed Citrix PIN.

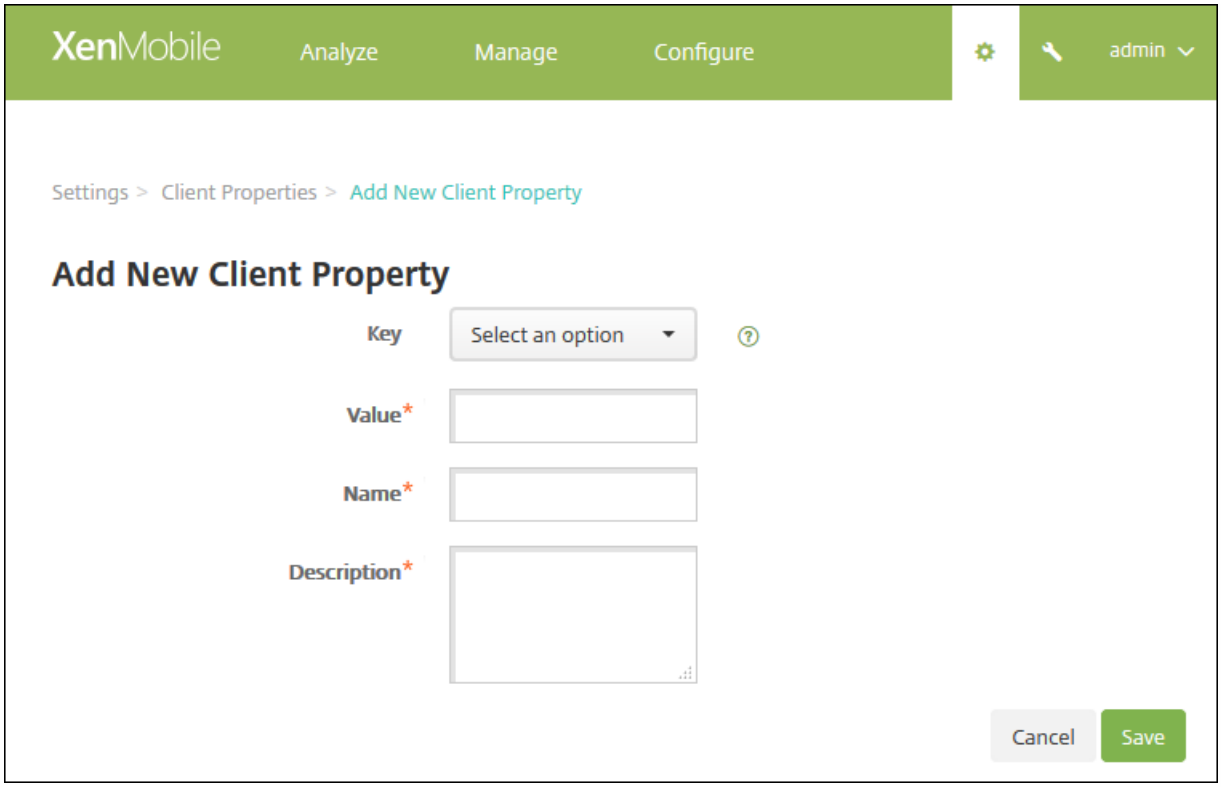
Client properties are subject to change with every release of client apps, particularly Worx Home. For more information on client properties, see Client property reference.

1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Client**, click **Client Properties**. The **Client Properties** page appears. You can add, edit, and delete client properties from this page.



To add a client property

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



2. Configure these settings:

- **Key**: In the list, click the property key you want to add. **Important**: Contact Citrix Support before making any changes or request a special key to make a change.
- **Value**: Enter the selected property's value.
- **Name**: Enter a name for the property.
- **Description**: Enter a description of the property.

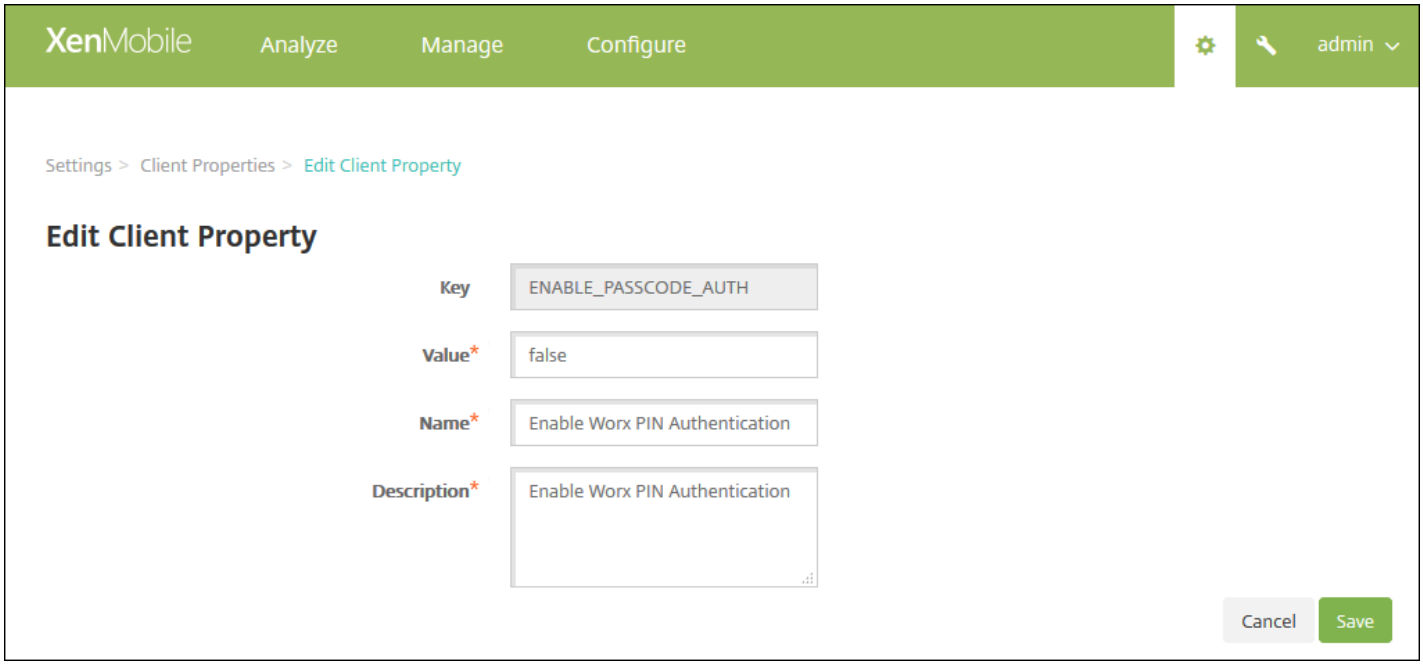
3. Click **Save**.

To edit a client property

1. In the **Client Properties** table, select the client property you want to edit.

Note: When you select the check box next to a client property, the options menu appears above the client property list; when you click anywhere else in the list, the options menu appears on the right side of the listing.

2. Click **Edit**. The **Edit Client Property** page appears.



3. Change the following information as appropriate:

- **Key**: You cannot change this field.
- **Value**: The property's value.
- **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 client property

1. In the **Client Properties** table, select the client property you want to delete.

   Note: You can select more than one property to delete by selecting the check box next to each property.

2. Click **Delete**. A confirmation dialog box appears. Click **Delete** again.

Client property reference

Mar 14, 2017

> **Note**
>
> Starting with version 10.4, Worx Mobile Apps are renamed XenMobile Apps. Most of the individual apps are renamed as well. For details, see About XenMobile Apps.

The XenMobile predefined client properties and their default settings are as follows.

CONTAINER_SELF_DESTRUCT_PERIOD

Display name: Self-Destruct

Self-destruct prevents access to Worx Home and managed apps, after a set number of days of inactivity. After the time limit, apps are no longer usable, and the user device is unenrolled from the XenMobile Server. Wiping the data includes clearing the app data for each installed app, including the app cache and user data. The inactivity time is when the server does not receive an authentication request to validate the user over a specific length of time. For example, you set 30 days for the policy. The user does not use Worx Home or other apps for more than 30 days. When this occurs, the policy takes effect.

This global security policy applies to iOS and Android platforms and is an enhancement of the existing app lock and wipe policies.

To configure this global policy, go to **Settings > Client Properties**, and add the custom key CONTAINER_SELF_DESTRUCT_PERIOD.

Value: Number of days

ENABLE_WORXHOME_CEIP

Display name: Enable Worx Home CEIP

This key turns on the Customer Experience Improvement Program. This program sends anonymous configuration and usage data to Citrix periodically. This data helps Citrix improve the quality, reliability, and performance of XenMobile.

Value: true or false

Default value: false

ENABLE_PASSCODE_AUTH

Display name: Enable Worx PIN Authentication

This key allows you to turn on Worx PIN functionality. With the Worx PIN or passcode, users are prompted to define a PIN to use instead of their Active Directory password. This setting is automatically enabled when ENABLE_PASSWORD_CACHING is enabled or when XenMobile is using certificate authentication.

If users are performing offline authentication, the Worx PIN is validated locally and users are allowed to access the

app or content they requested. If users are performing online authentication, the Worx PIN or passcode is used to unlock the Active Directory password or certificate, which is then sent to perform authentication with XenMobile.

Possible values: true or false

Default value: false

ENABLE_PASSWORD_CACHING

Display name: Enable User Password Caching

This key lets you allow the Active Directory password for a user to be cached locally on the mobile device. When you set this key to true, users are prompted to set a Worx PIN or passcode. The ENABLE_PASSCODE_AUTH key must be set to true when you set this key to true.

Possible values: true or false

Default value: false

ENCRYPT_SECRETS_USING_PASSCODE

Display name: Encrypt secrets using Passcode

This key lets sensitive data be stored on the mobile device. The data is stored in a secret vault instead of in a platform-based native store, such as the iOS keychain. This configuration key enables strong encryption of key artifacts, but also adds user entropy (a user-generated random PIN code that only the user knows).

Citrix recommends that you enable this key to help provide higher security on user devices.

Note: Enabling this key affects the user experience in terms of a greater number of authentication prompts for the Worx PIN.

Possible values: true or false

Default value: false

PASSCODE_TYPE

Display name: Worx PIN Type

This key defines whether users are able to define a numerical Worx PIN or an alphanumeric Worx passcode. When you select Numeric, users can only define a numeric Worx PIN. When you select Alphanumeric, users can use a combination of letters and numbers for the Worx passcode.

Note: When you change the setting, users are prompted to set a new Worx PIN or passcode the next time they are prompted to authenticate.

Possible values: Numeric or Alphanumeric

Default value: Numeric

PASSCODE_STRENGTH

Display name: Worx PIN Strength Requirement

This key defines the strength of Worx PIN or passcode. When you change this setting, users are prompted to set a new Worx PIN or passcode the next time they are prompted to authenticate.

Possible values: Low, Medium, or Strong

Default value: Medium

The following table describes the password rules for each strength setting based on the setting you select for PASSCODE_TYPE:

Passcode strength	Rules for numeric passcode type	Rules for alphanumeric passcode type
Low	All numbers, any sequence allowed	Must contain at least one number and one letter. Not allowed: AAAaaa, aaaaaa, abcdef Allowed: aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa
Medium (default setting)	1. All numbers cannot be the same. For example, 444444 is not allowed. 2. All numbers cannot be consecutive. For example, 123456 or 654321 is not allowed. Allowed: 444333, 124567, 136790, 555556, 788888	In addition to the rules for Low passcode strength: 1. Letters and all numbers cannot be same. For example, aaaa11, aa11aa, or aaa111 are not allowed. 2. Letters cannot be consecutive and numbers cannot be consecutive. For example, abcd12, bcd123, 123abc, xy1234, xyz345, or cba123 are not allowed. Allowed: aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~
Strong	Same as for the Medium Worx PIN passcode strength.	The passcode should include at least one number, one special symbol, one capital letter, and one small letter. Not allowed: abcd12, Abcd12, dfgh12, jkrtA2 Allowed: Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#

PASSCODE_MIN_LENGTH

Display name: Worx PIN Length Requirement

This key defines the minimum length Worx passcodes can be.

Possible values: 1-99

Default value: 6

PASSCODE_EXPIRY

Display name: Worx PIN Expiry Requirement

This key defines the time in days for which the Worx PIN or passcode is valid, after which the user is forced to change their Worx PIN or passcode. When you change this setting, the new value is set only when users' current Worx PIN or passcode expires.

Possible values: 1 or higher, but 1-99 is recommended

Default value: 90

Note: If you want users never to have to reset their PINs, set the value to 0. When you do, if you originally set an expiry period of between 1 and 99 days, during that period, the change takes effect immediately after users reauthenticate to Secure Hub.

PASSCODE_HISTORY

Display name: Worx PIN History

This key defines the number of previously used Worx PINs or passcodes that users cannot reuse when changing their Worx PIN or passcode. When you change this setting, the new value is set the next time users reset their Worx PIN or passcode.

Possible values: 1-99

Default value: 5

INACTIVITY_TIMER

Display name: Inactivity Timer

This key defines the time in minutes that users can leave their device inactive and then access an app without being prompted for a Worx PIN or passcode. To enable this setting for an MDX app, you must set the App Passcode setting to On. If the App Passcode setting is set to Off, users are redirected to Worx Home to perform a full authentication. When you change this setting, the value takes effect the next time users are prompted to authenticate.

Note: On iOS, the Inactivity Timer also governs access to Worx Home not only to MDX apps.

Possible values: Any positive integer

Default value: 15

DISABLE_LOGGING

Display name: Disable logging

This key lets you disable the ability for users to collect and upload logs from their devices. Logging is disabled for Worx Home and for all installed MDX apps. Users cannot send logs for any app from the Support page. Even though the mail composition dialog box appears, logs are not attached, but a message is appended saying that logging is disabled. In addition to the effect on devices, you cannot change log settings in the XenMobile console for Worx Home and MDX apps.

When this key is set to true, Worx Home sets Block application logs to true, ensuring that MDX apps stop logging when the new policy is applied.

Possible values: true or false

Default value: false (logging is not disabled)

ENABLE_CRASH_REPORTING

Display name: Enable Crash reporting

This key enables or disables crash reporting using Crashlytics for Worx apps.

Possible values: true or false

Default value: true

DEVICE_LOGS_TO_IT_HELP_DESK

Display name: Send device logs to IT help desk

This key enables or disables the ability to send logs to the IT help desk.

Possible values: true or false

Default value: false

ON_FAILURE_USE_EMAIL

Display name: On failure use email to send device logs to IT help desk.

This key enables or disables the ability to use email to send device logs to IT.

Possible values: true or false

Default value: true

PASSCODE_MAX_ATTEMPTS

Display name: Worx PIN Maximum Attempts

This key defines how many wrong Worx PIN or passcode attempts users can make before being prompted for full authentication. After users successfully perform a full authentication, they are prompted to create a new Worx PIN or passcode.

Possible values: Any positive integer

Default value: 15

ENABLE_TOUCH_ID_AUTH

Display name: Enable Touch ID Authentication

This key enables or disables the ability for devices (equipped with the capability) to use Touch ID authentication. User devices must have Worx PIN enabled and User Entropy set to false so that when they start an app, they are

prompted to use Touch ID.

Possible values: true or false

Default value: false

ENABLE_WORXHOME_GA

Display name: Enable Google Analytics in WorxHome

This key enables or disables the ability to collect data using Google Analytics in WorxHome. When you change this setting, the new value is set only when the user next logs on to WorxHome.

Possible values: true or false

Default value: true

XenMobile Server Settings

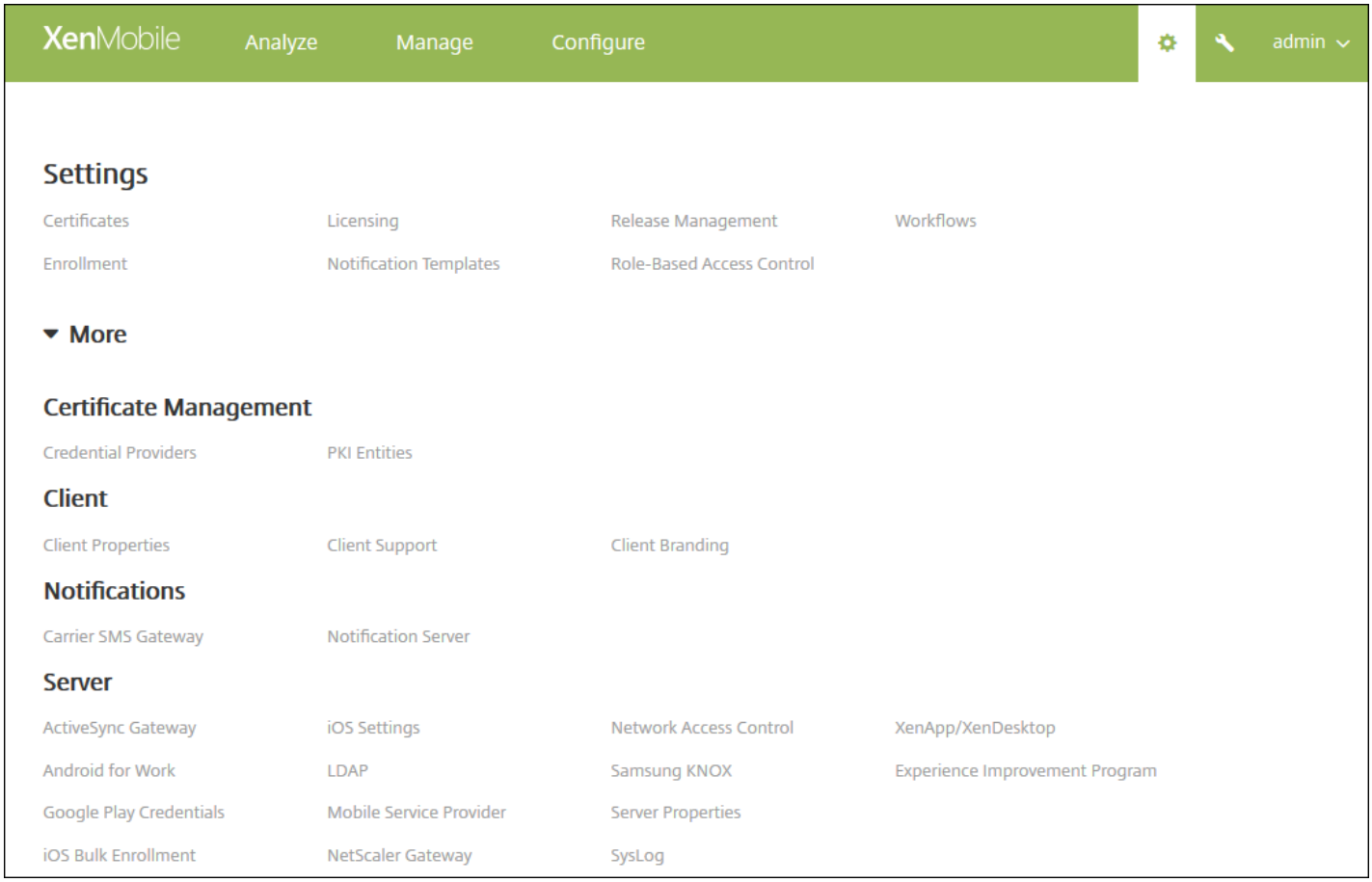
May 29, 2015

The XenMobile server settings that you configure in the XenMobile console include:

- ActiveSync Gateway
- Android for Work
- Experience Improvement Program
- Google Play Credentials
- iOS Bulk Enrollment
- iOS Settings
- LDAP
- Microsoft Azure
- Mobile Service Provider
- NetScaler Gateway
- Network Access Control
- Samsung KNOX
- Server Properties
- SysLog
- XenApp/XenDesktop

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

2. Under **Server**, click the option you want to configure.



ActiveSync Gateway in XenMobile

Mar 21, 2016

ActiveSync is a mobile data synchronization protocol developed by Microsoft. ActiveSync synchronizes data with handheld devices and desktop (or laptop) computers. You can configure ActiveSync Gateway rules in XenMobile. Based on these rules, devices can be allowed or denied access to ActiveSync data. For example, if you activate the rule Missing Required Apps, XenMobile checks the App Access Policy for required apps and denies access to ActiveSync data if the required apps are missing.

XenMobile supports the following rules:

Anonymous Devices: Checks if a device is in anonymous mode. This check is available if XenMobile can't re-authenticate the user when a device attempts to reconnect.

Failed Samsung KNOX attestation: Checks if a device failed a query of the Samsung KNOX attestation server.

Forbidden Apps: Checks if a device has forbidden apps, as defined in an App Access policy.

Implicit Allow and Deny: This action is the default for the ActiveSync Gateway, which creates a Device List of all devices that do not meet any of the other filter rule criteria and allows or denies connections based on that list. If no rule matches, the default is Implicit Allow.

Inactive Devices: Checks if a device is inactive as defined by the Device Inactivity Days Threshold setting in Server Properties.

Missing Required Apps: Checks if a device is missing required apps, as defined in an App Access policy.

Non-suggested Apps: Checks if a device has non-suggested apps, as defined in an App Access policy.

Noncompliant Password: Checks if the user password is compliant. On iOS and Android devices, XenMobile can determine whether the password currently on the device is compliant with the passcode policy sent to the device. For instance, on iOS, the user has 60 minutes to set a password if XenMobile sends a passcode policy to the device. Before the user sets the password, the passcode might be non-compliant.

Out of Compliance Devices: Checks whether a device is out of compliance, based on the Out of Compliance device property. That property is usually changed by the automated actions or by a 3rd party leveraging XenMobile APIs.

Revoked Status: Checks whether the device certificate was revoked. A revoked device cannot re-enroll until it is authorized again.

Rooted Android and Jailbroken iOS Devices: Checks whether an Android or iOS device is jailbroken.

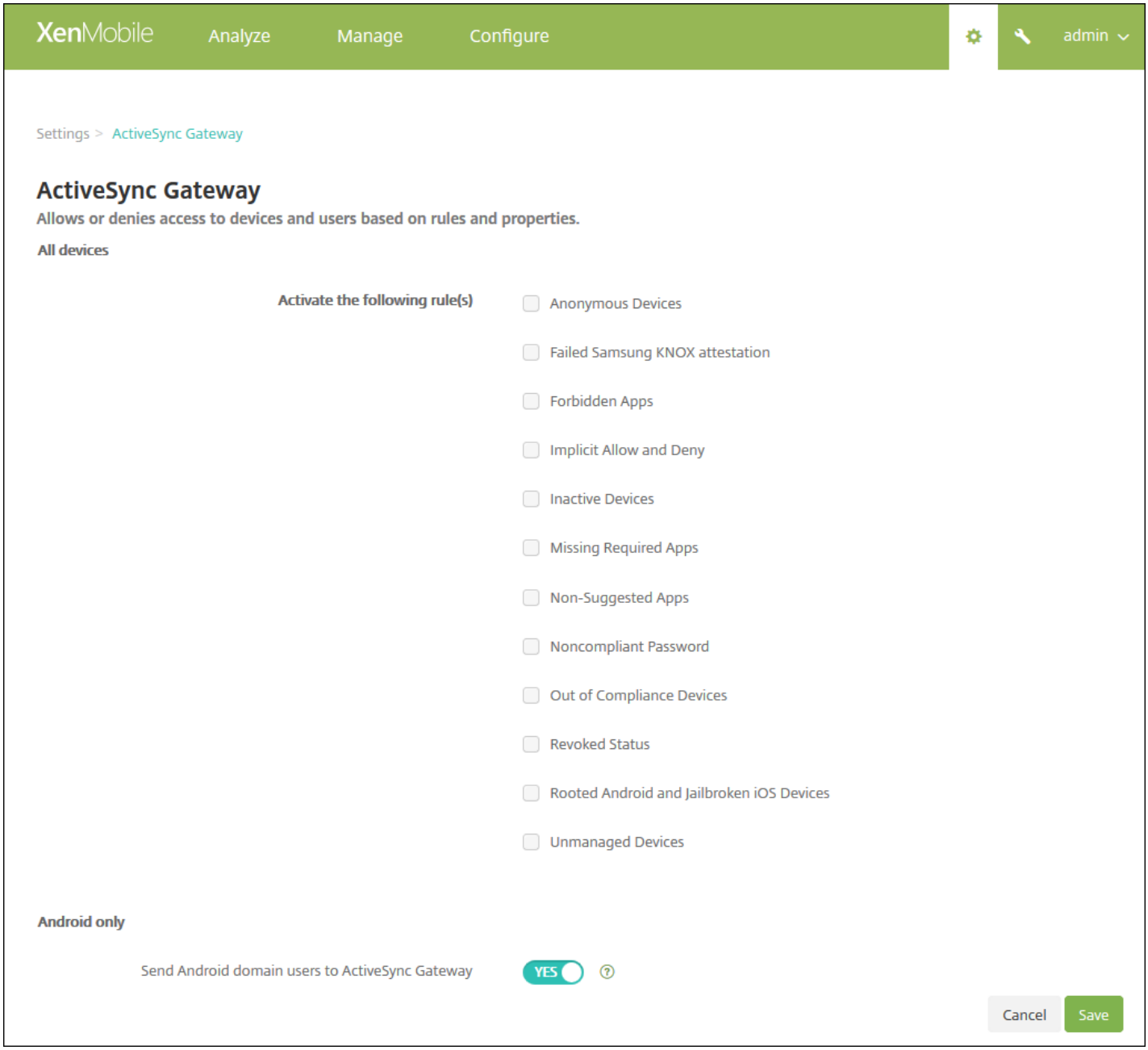
Unmanaged Devices: Check whether a device is still in a managed state, under XenMobile control. For example, a device running in MAM mode or an un-enrolled device is not managed.

Send Android domain users to ActiveSync Gateway: Click **YES** to ensure that XenMobile sends Android device information to the ActiveSync Gateway. When this option is enabled, it ensures that XenMobile sends Android device information to the ActiveSync Gateway in the event that XenMobile does not have the ActiveSync identifier for the Android device user.

To configure the ActiveSync Gateway settings

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

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



3. In **Activate the following rules**, select one or more rules you want to activate.

4. In **Android-only**, in **Send Android domain users to ActiveSync Gateway**, click **YES** to ensure that XenMobile sends Android device information to the ActiveSync Gateway.

5. Click **Save**.

Google Play Credentials

Jul 27, 2016

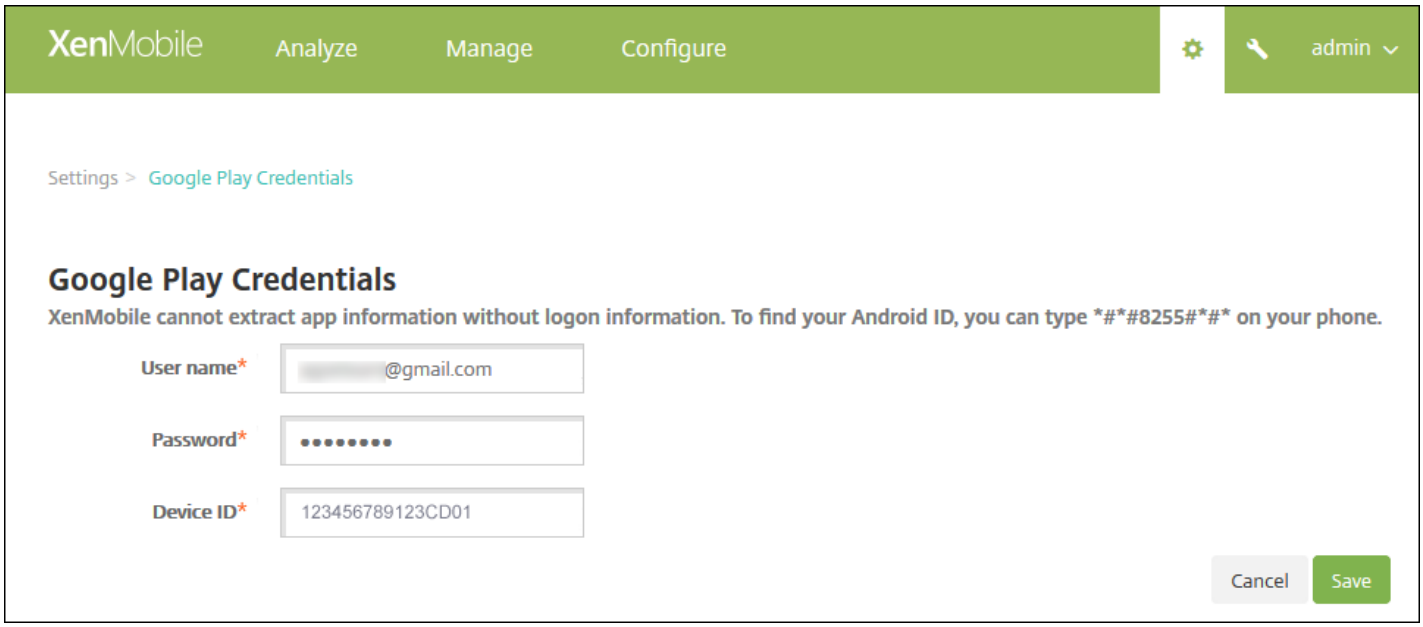
XenMobile uses Google Play credentials to extract app information for the device.

Note: To locate your Android ID, enter *#*#8255#*#* on your phone. If the code does not reveal the device ID on your device type, it may be possible to use a device ID third-party app to derive the device ID. The ID you need to retrieve is the Google Services Framework ID with the label GSF ID.

Important: To enable XenMobile to extract app information, you may need to configure your Gmail account to permit unsecure connections. For steps, see the Google support site.

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

2. Under **Server**, click **Google Play Credentials**. The **Google Play Credentials** page appears.



3. Configure these settings:

- **User name**: Type the name associated with the Google Play account.
- **Password**: Type the user password.
- **Device ID**: Type your Android ID.
  Enter *#*#8255#*#* on your phone to determine the Android ID.

3. Click **Save**.

Bulk enrollment of iOS devices

Jan 05, 2017

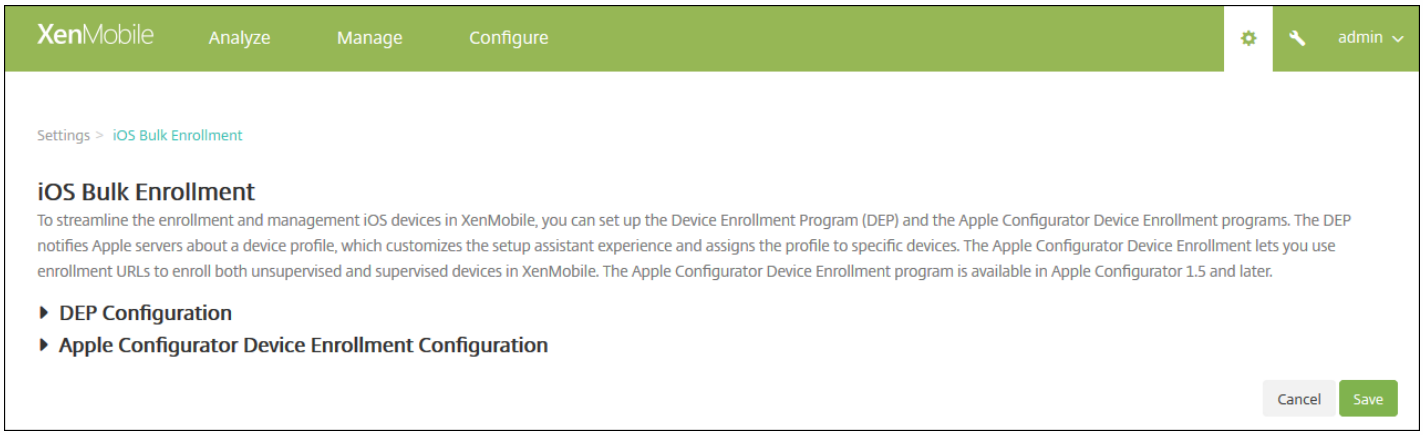
You can enroll large numbers of iOS devices in XenMobile in two ways. You can use Apple's Device Enrollment Program (DEP) to enroll devices that you buy directly from Apple or from a participating Apple Authorized Reseller or carrier; or you can use the Apple Configurator to enroll devices regardless of whether they were purchased directly from Apple.

With DEP, you do not have to touch or prepare the devices; you submit device serial numbers or purchase order numbers through DEP and the devices are configured and enrolled in XenMobile. After the devices are enrolled, you can give them to users who can start using them right out of the box. In addition, when you set up devices with DEP, you can eliminate some of the Setup Assistant steps that users would otherwise have to complete when they first start their devices. For more information on setting up DEP, see Apple's Device Enrollment Program page.

With the Apple Configurator, you attach devices to an Apple computer running OS X 10.7.2 or later and 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 on using the Apple Configurator, see Apple's Apple Configurator page.

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

2. Under **Server**, click **iOS Bulk Enrollment**. The **iOS Bulk Enrollment** page appears.



If you are configuring DEP settings, see Configuring DEP settings; if you are configuring Apple Configurator settings, see Configuring Apple Configurator settings.

Configuring DEP settings

Before you can continue, you must have created an Apple DEP account on deploy.apple.com. After you have created a DEP account, you set up a virtual MDM server to allow XenMobile and Apple to communicate. To do that, you must upload a XenMobile public key to Apple. After Apple receives the public key, it returns a server token that you import into XenMobile. Follow these steps to establish the connection between XenMobile and Apple.

1. To obtain the public key to upload to Apple, on the **iOS Bulk Enrollment** page, expand **DEP Configuration**, and then, click **Export Public Key** and save the file to your computer.

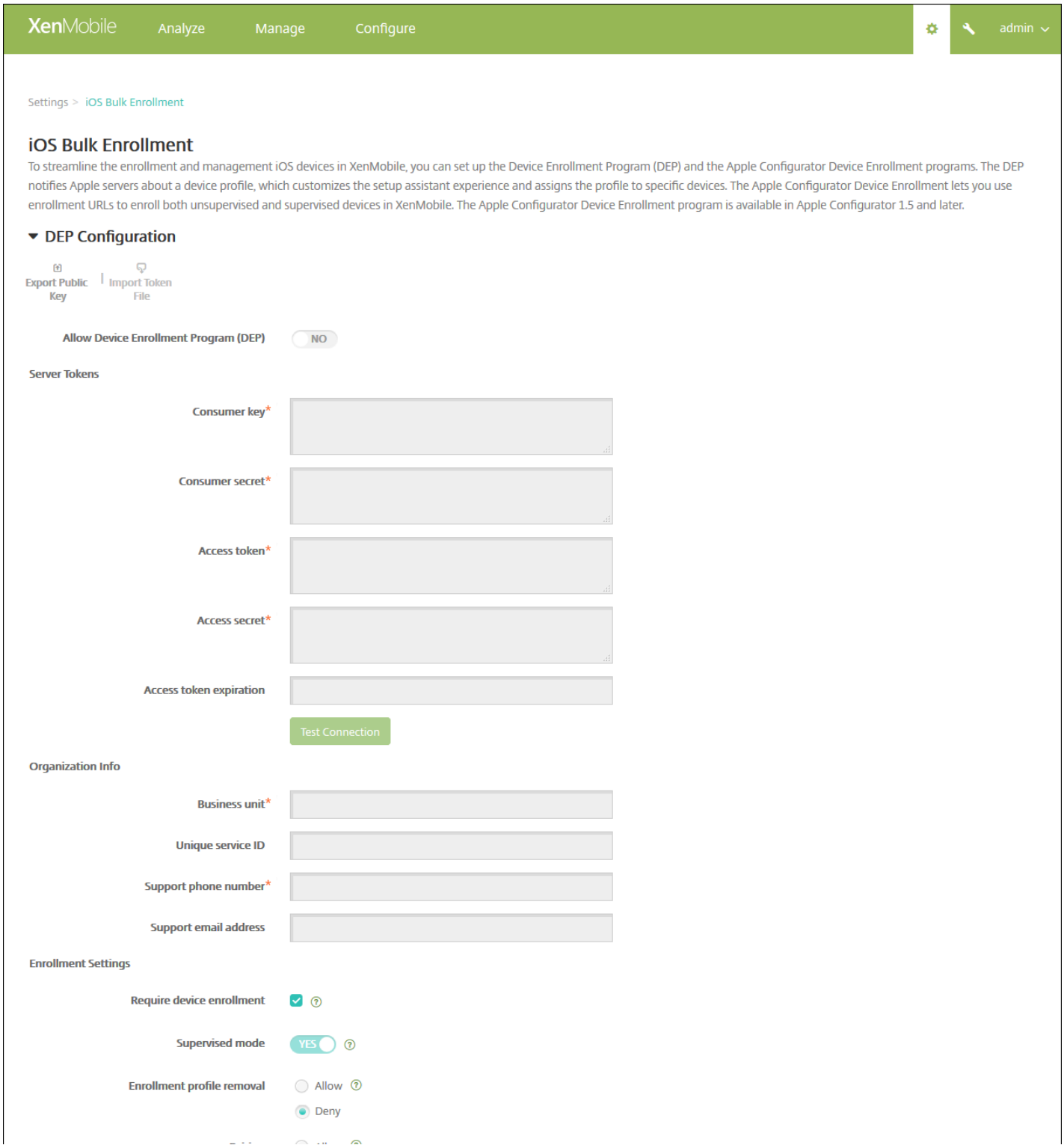
2. Go to deploy.apple.com, log in to your DEP account and follow the instructions for setting up an MDM server. As part of

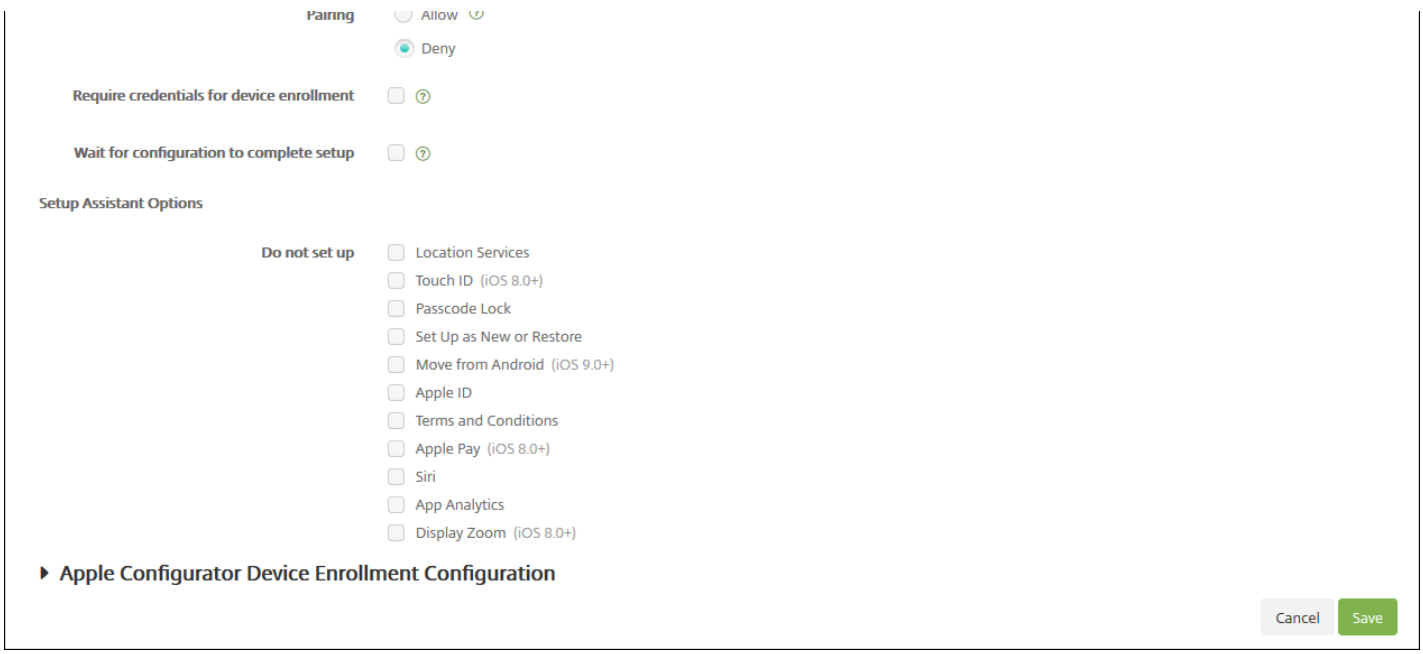
this process, Apple provides a server token.

3. On the **iOS Bulk Enrollment** page, click **Import Token File** to add the Apple server token to XenMobile.

4. The **Server tokens** fields fill automatically after the token file is uploaded to XenMobile.

5. Click **Test Connectivity** to confirm that XenMobile and Apple are able to communicate. If the connection test fails, confirm that you have opened all required ports because this is the most likely cause of the failure. For more information on the ports that must be opened in XenMobile, see Port Requirements.





6. Configure these settings to complete the DEP configuration:

Organization Information

- **Business unit**: Enter the business unit or department to which the device is assigned. This field is required.
- **Unique service ID**: Enter an optional unique ID.
- **Support phone number**: Enter a support phone number that users may call for help during setup. This field is required.
- **Support email address**: Enter an optional support email address.

Enrollment Settings

- **Require device enrollment**: Select whether to require users to enroll their devices. The default is to require enrollment.
- **Supervised mode**: Must be set to **Yes** if you are using the Apple Configurator to manage DEP enrolled devices or when **Wait for configuration to complete setup** is enabled. The default is **Yes**. For details on placing an iOS device in supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.
- **Enrollment profile removal**: Select whether to allow devices to use a profile that can be removed remotely. The default is **Deny**.
- **Pairing**: Select whether to allow devices enrolled through DEP to be managed through iTunes and the Apple Configurator. The default is **Deny**.
- **Require credentials for device enrollment**: Select whether to require users to enter their credentials during DEP set up. This is available for iOS 7.1 and higher. **Note**: When DEP is on for the first time setup and you don't select this option, the DEP components, such as DEP user, Worx Home (renamed Secure Hub starting with version 10.4), software inventory, and DEP deployment group, are created from the beginning. If you do select this option, the components are not created until the user enters their credentials. As a result, if you later clear this option, users who have not entered their credentials cannot perform the DEP enrollment because these DEP components do not exist. To add DEP components, in that case, you should disable and enable the DEP account.
- **Wait for configuration to complete setup**: Select whether to require users' devices to remain in Setup Assistant mode until all MDM resources are deployed to the device. This is available for iOS 9.0 and higher devices in supervised mode.
  - **Note**: Apple documentation states that the following commands may not work while a device is in Setup Assistant

mode:

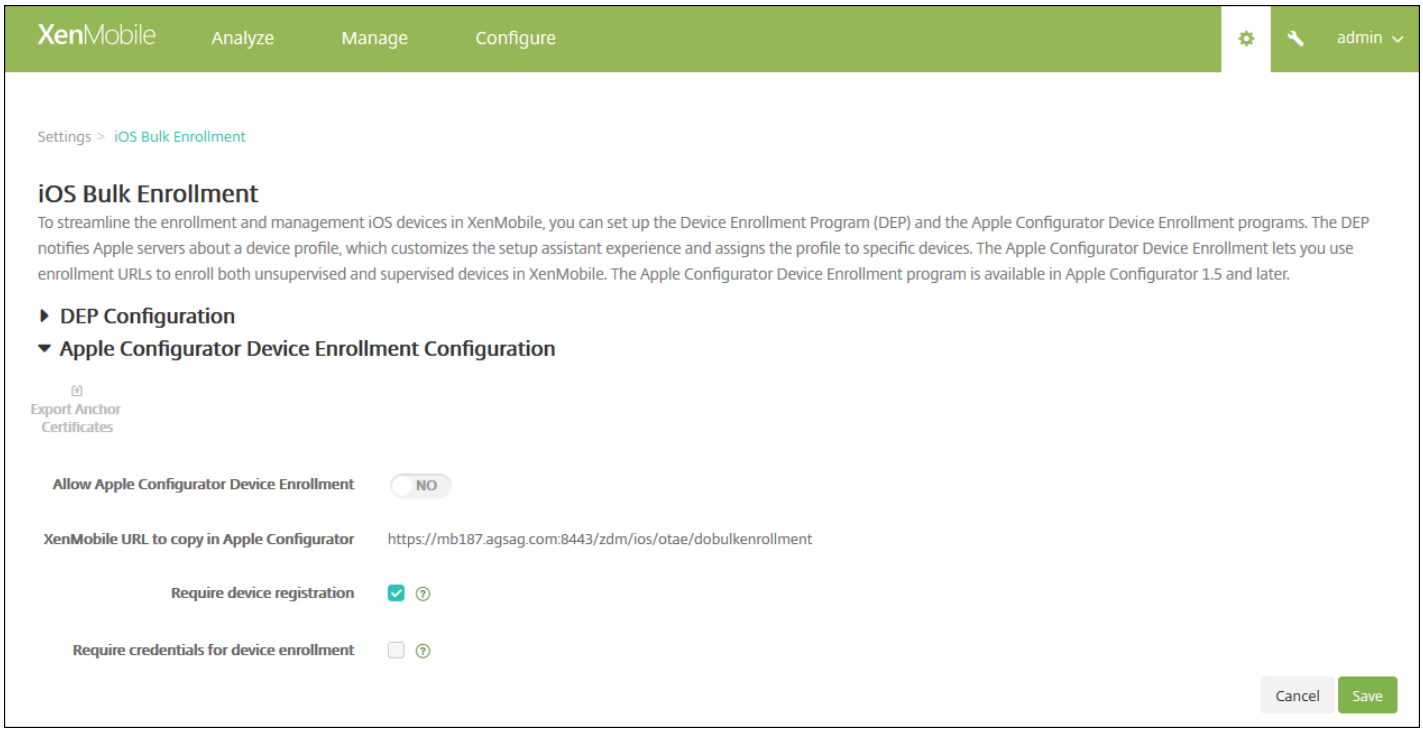
- InviteToProgram
- InstallApplication
- ApplyRedemptionCode
- InstallMedia
- RequestMirroring
- DeviceLock

Setup

Select the iOS Setup Assistant steps that your users will *not* have to take (that is, steps that are skipped) when they start their devices for first-time use.

- **Location Services**: Set up the location service on the device.
- **Touch ID**: Set up Touch ID on iOS 8.0 and later devices.
- **Passcode Lock**: Create a passcode for the device.
- **Set up as New or Restore**: Set up the device as new or from an iCloud or iTunes backup.
- **Move from Android**: Enable transferring data from an Android device to an iOS 9 or later device. This option is available only when **Set up as New or Restore** is selected (that is, the step is skipped).
- **Apple ID**: Set up an Apple ID account for the device.
- **Terms and Conditions**: Require users to accept terms and conditions for use of the device.
- **Apple Pay**: Set up Apple Pay on iOS 8.0 and later devices.
- **Siri**: Use or not use Siri on the device.
- **App Analytics:** Set up whether to share crash data and usage statistics with Apple.
- **Display Zoom**: Set up the display resolution (either standard or zoomed) on iOS 8.0 or later devices.

Configuring Apple Configurator settings



1. Expand **Apple Configurator Device Enrollment Configuration**.

2. Set **Enable Apple Configurator Device Enrollment** to **Yes**.

3. Note and configure these settings:

- **MDM server URL to copy in Apple Configurator**: This read-only field is the URL for the XenMobile server that communicates with Apple, and which you copy and paste into the Apple Configurator in a later step. In Apple Configurator 2, the enrollment URL is the fully qualified domain name (FQDN) or IP address of the XenMobile server, such as mdm.server.url.com.
- **Require device registration**: Selecting this setting requires you to add the configured devices to the **Devices** tab in XenMobile manually or through a CSV file before they can be enrolled. This ensures that no unknown devices can enroll. The default is to require adding devices.
- **Require credentials for device enrollment**: Require users of iOS 7.1 and later devices to enter their credentials when enrolling. The default is to not require credentials.

> **Note**
>
> If the XenMobile server is using a trusted SSL certificate, skip the next step.

4. Click **Export Anchor Certs** and save the certchain.pem file to the OS X keychain (login or System).

5. Start the Apple Configurator and go to **Prepare > Setup > Configure Settings.**

6. In the **Device Enrollment** setting, paste the MDM server URL from step 4 into the **MDM server URL** field in the Configurator.

7. In the **Device Enrollment** setting, copy the Root Certificate Authority and SSL Servers Certificate Authority to the **Anchor** certificates, if XenMobile is not using a trusted SSL certificate.

8. Use a Dock Connector to USB cable to connect devices to the Mac running the Apple Configurator to simultaneously configure up to 30 connected devices. If you do not have a Dock Connector, use one or more powered USB 2.0 high-speed hubs to connect the devices.

9. Click **Prepare**. For more information on preparing devices with the Apple Configurator, see the Apple Configurator help page Prepare devices.

10. In the Apple Configurator, configure the device policies you require.

11. As each device is prepared, turn it on to start the iOS Setup Assistant, which prepares the device for first-time use.

To renew or update certificates when using the Apple DEP

When the XenMobile Secure Sockets Layer (SSL) certificate is renewed, you upload a new certificate in the XenMobile console in **Settings** > **Certificates**. In the Import dialog box, in **Use as**, be sure to click **SSL Listener** so that the certificate is used for SSL. After you restart the server, XenMobile uses the new SSL certificate. For more information about certificates in XenMobile, see Uploading Certificates in XenMobile.

It is not necessary to reestablish the trust relationship between Apple DEP and XenMobile when you renew or update the

SSL certificate. You can, however, reconfigure your DEP settings at any time by following the preceding steps in this article.

For more information about Apple DEP, see the Apple documentation.

For information about a known issue and work around related to this configuration, see XenMobile Server 10.3 Known Issues.

Deploying iOS Devices Through Apple DEP

Jan 05, 2017

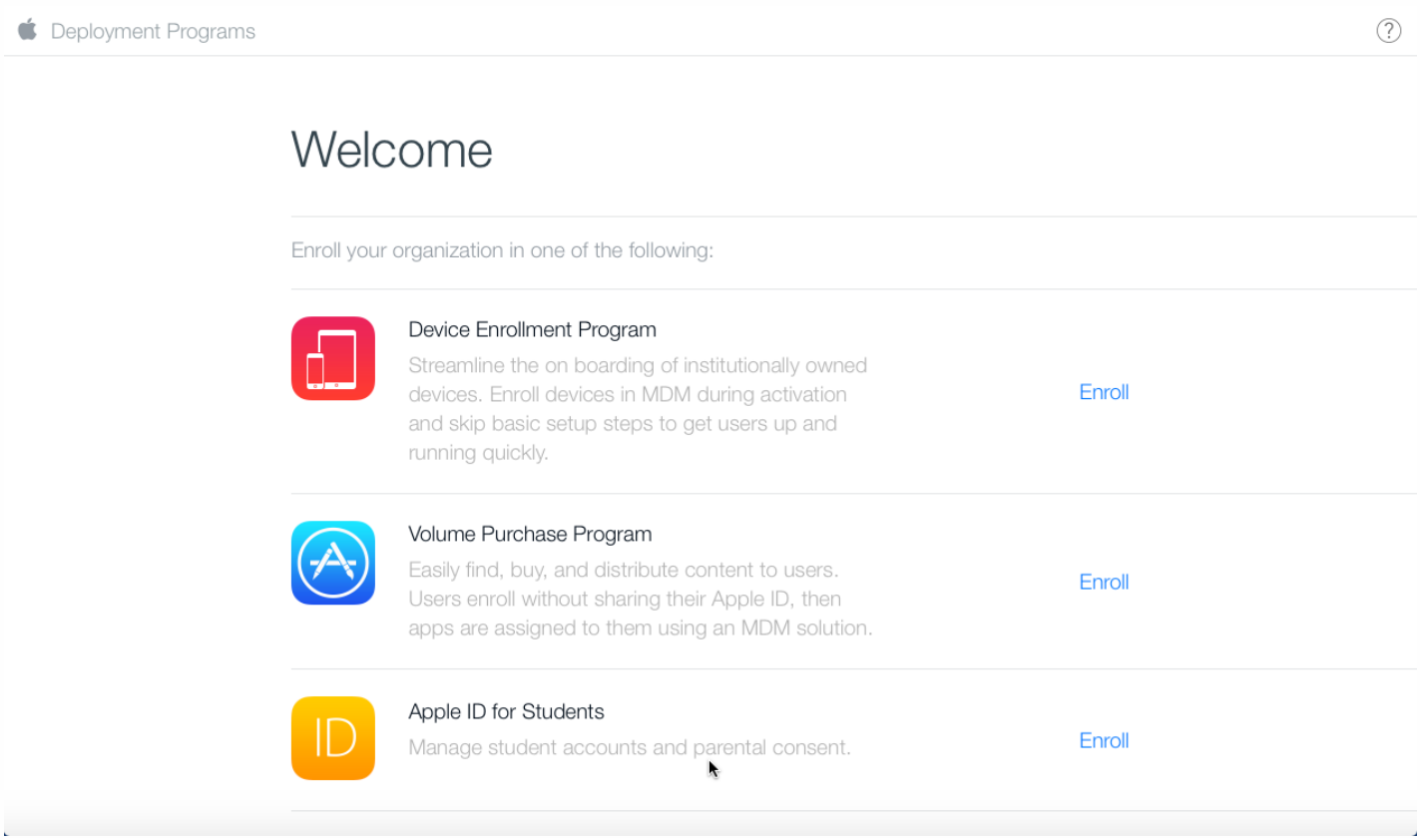
You need an Apple Developer Enterprise Program (DEP) account to be able to take advantage of the Apple DEP for IOS device enrollment and management in XenMobile. The main requirements for organizations to sign up for the Apple DEP are as follows.

- Business or institution phone number and email address
- Verification contact
- Business or institution information (D-U-N-S / tax ID)
- Apple Customer number

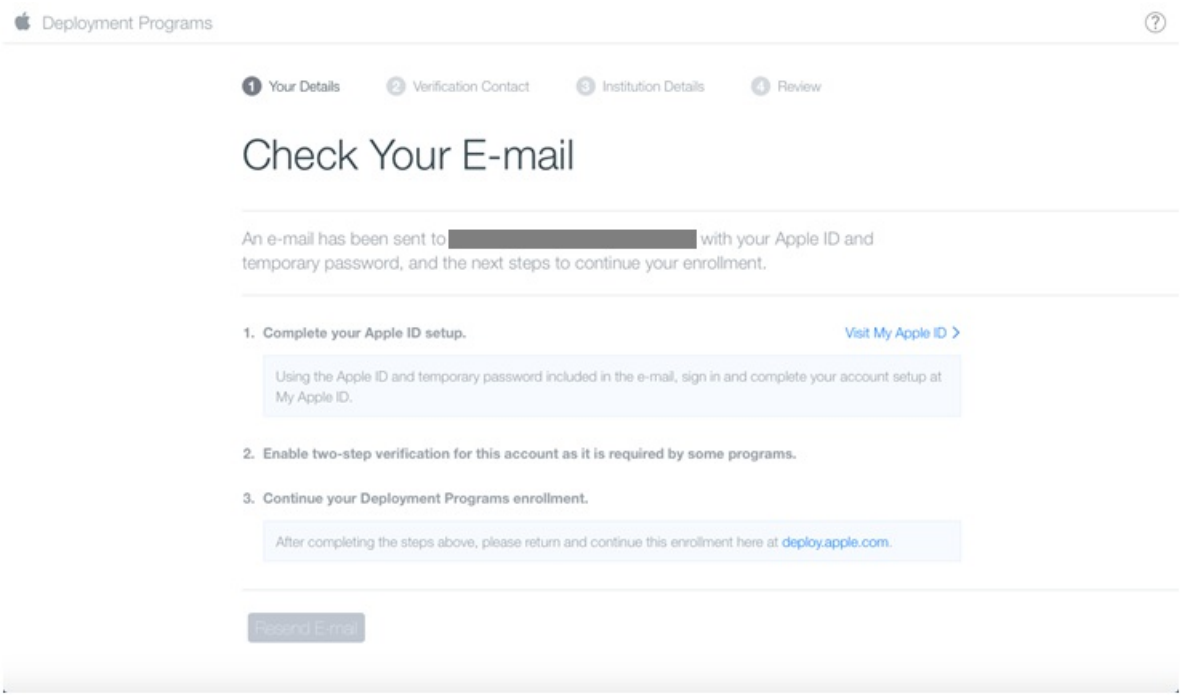
For more information about Apple DEP details, see this PDF from Apple. It is important to highlight that Apple DEP is available for organizations and not individuals. It is also important to be aware that a fair amount of corporate details and information needs to be provided to create an Apple DEP account, which means it could take time for customers to request and receive approval for their accounts.

Applying for the Apple DEP account

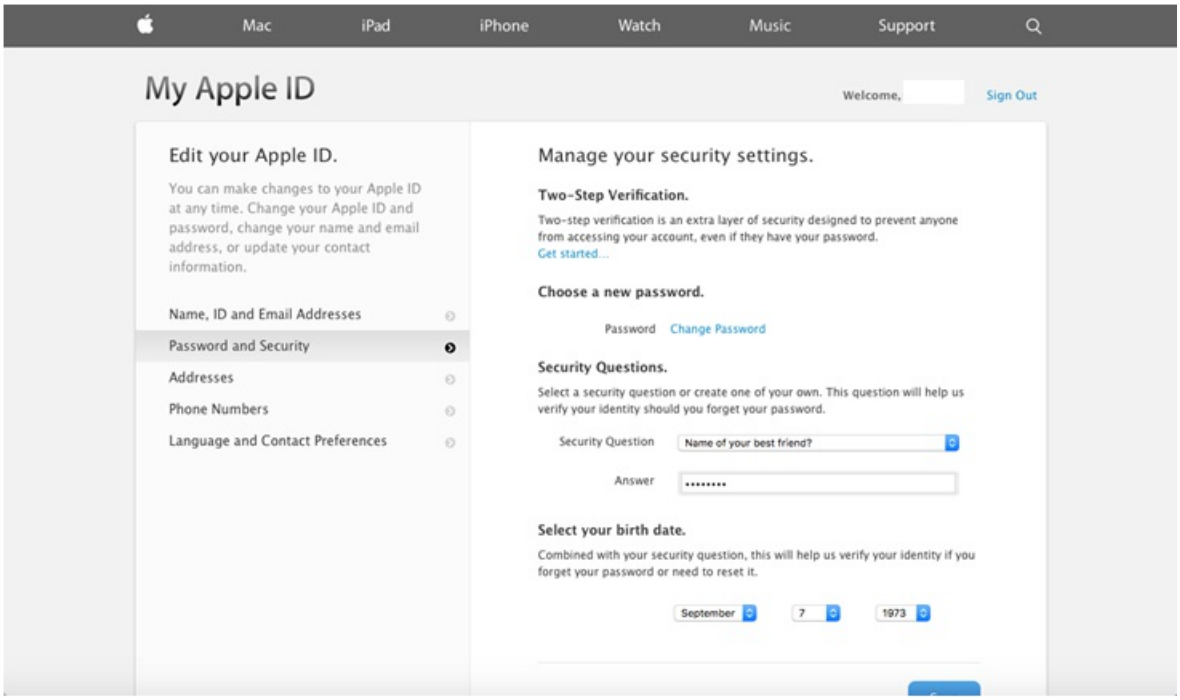
When applying for a DEP account, the best practice is to use an email address that is tied to the organization, such as dep@company.com.



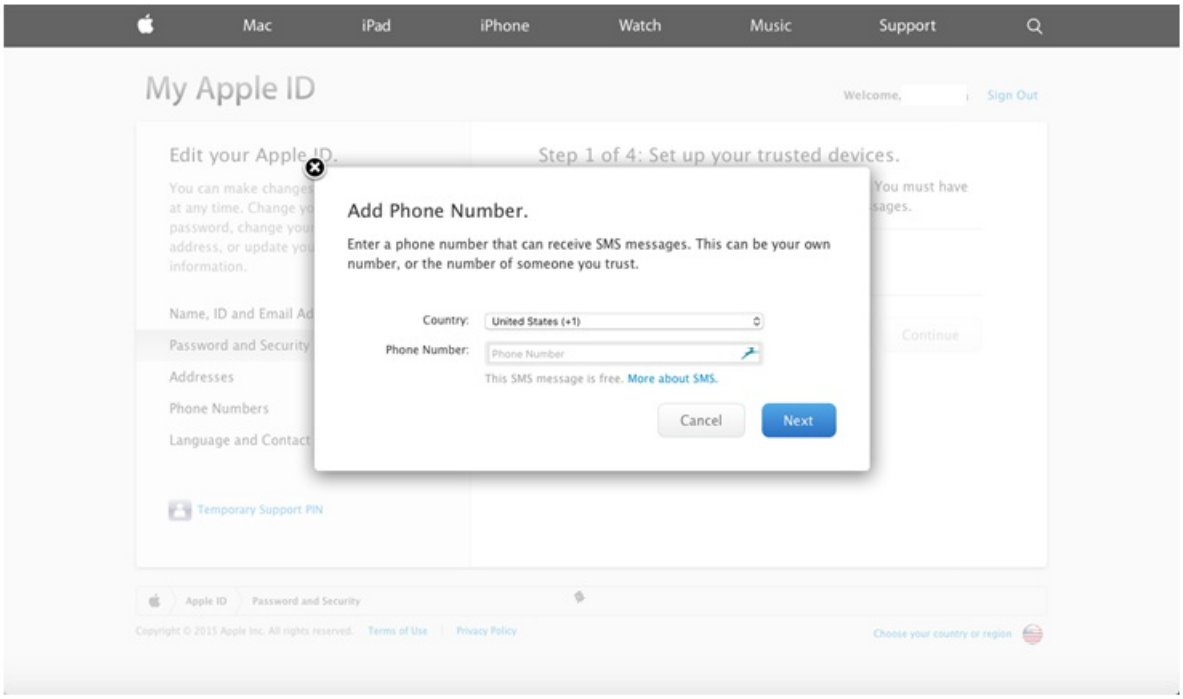
1. After you enter your organization information, you should receive a temporary password for the new Apple ID through email.



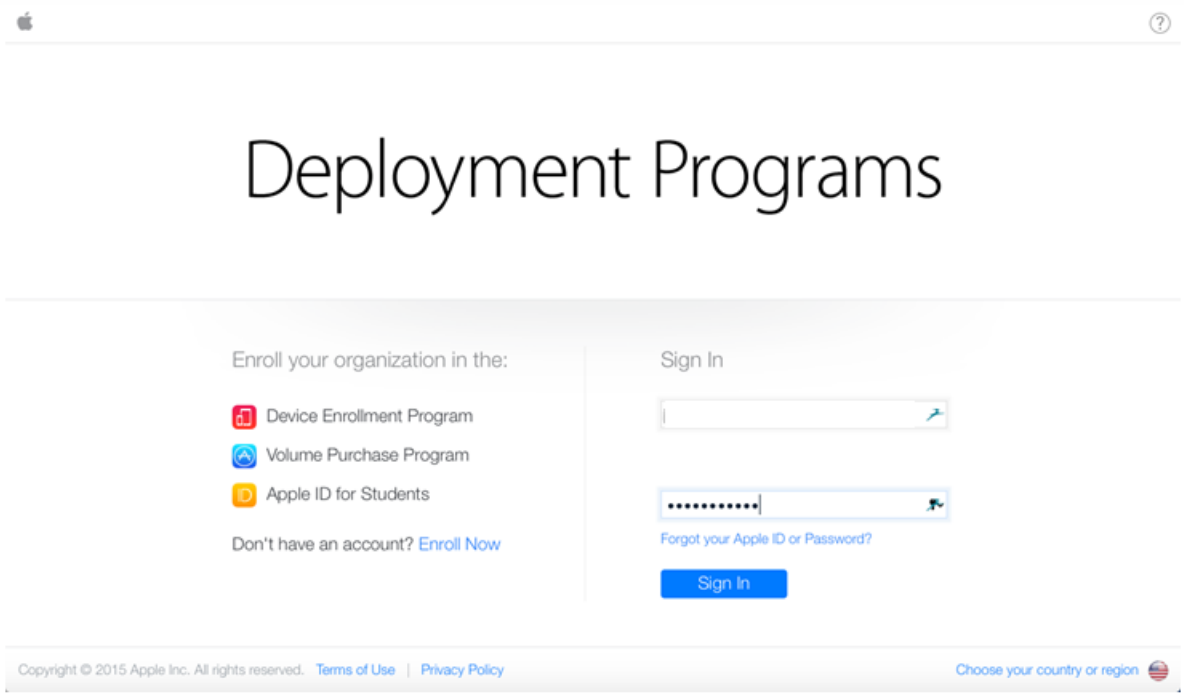
2. You then sign in with the Apple ID and complete the security settings for the account.



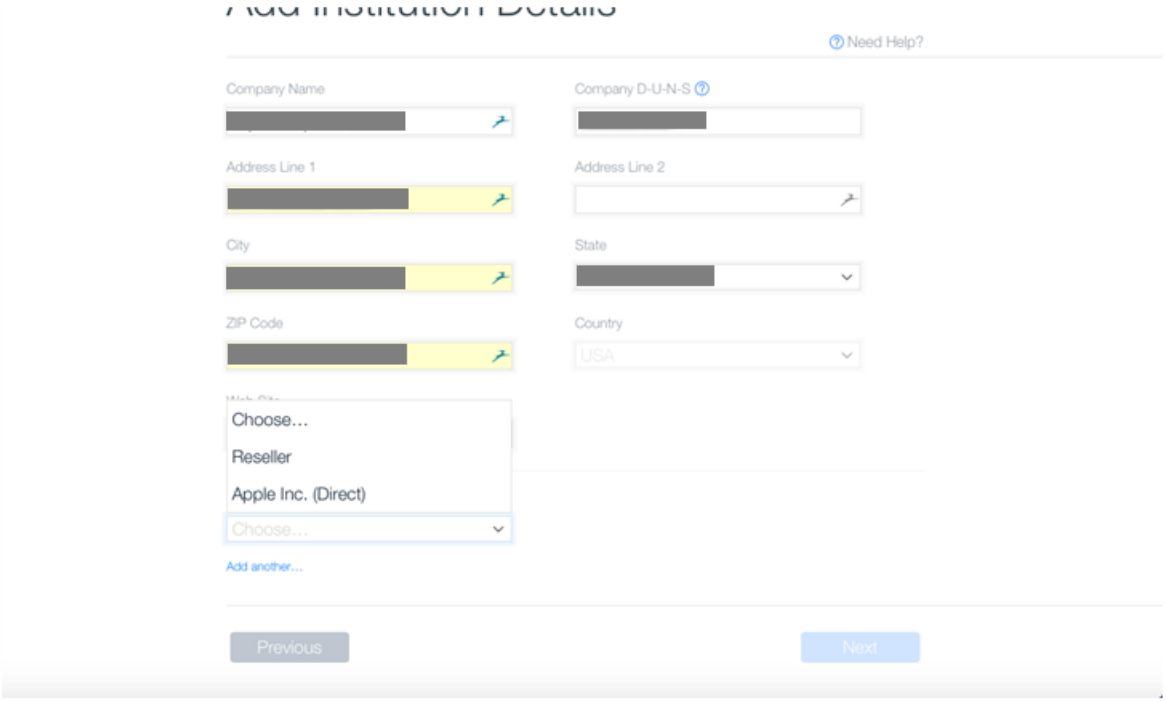
3. Configure and enable two-step verification, which is required for use with the DEP Portal. During these steps, you add a phone number where you will receive the 4-digit PIN for the two-step verification.



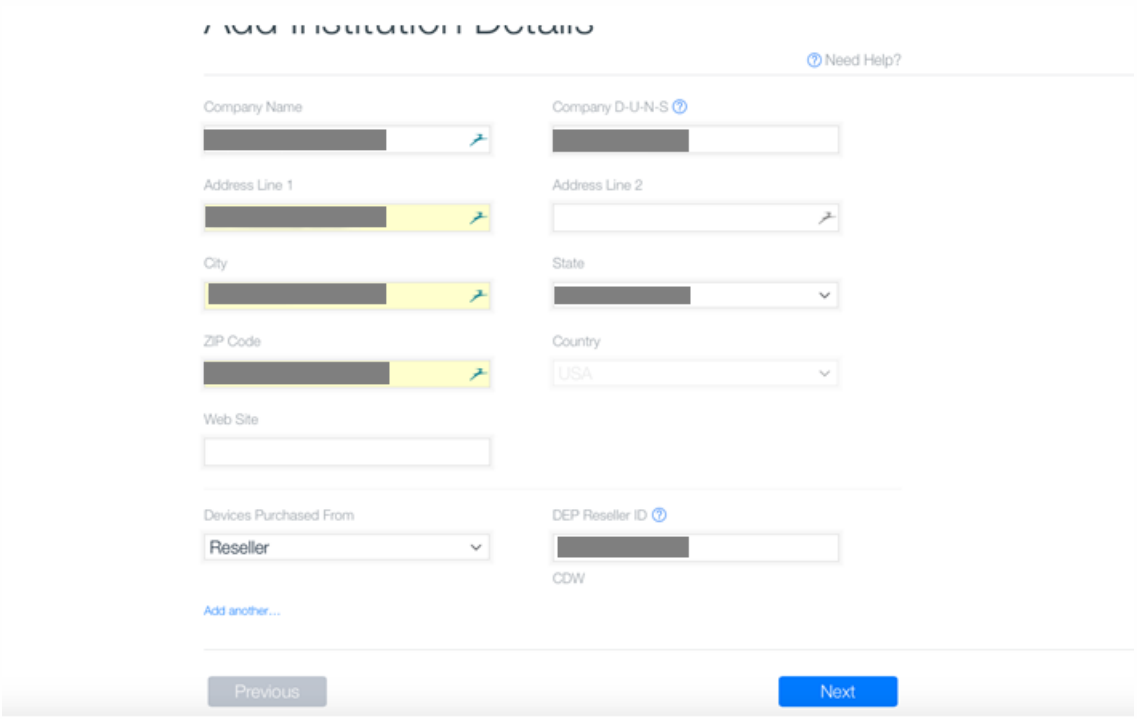
4. Log in to the DEP Portal to complete the account configuration using the two-step verification that you just set up.

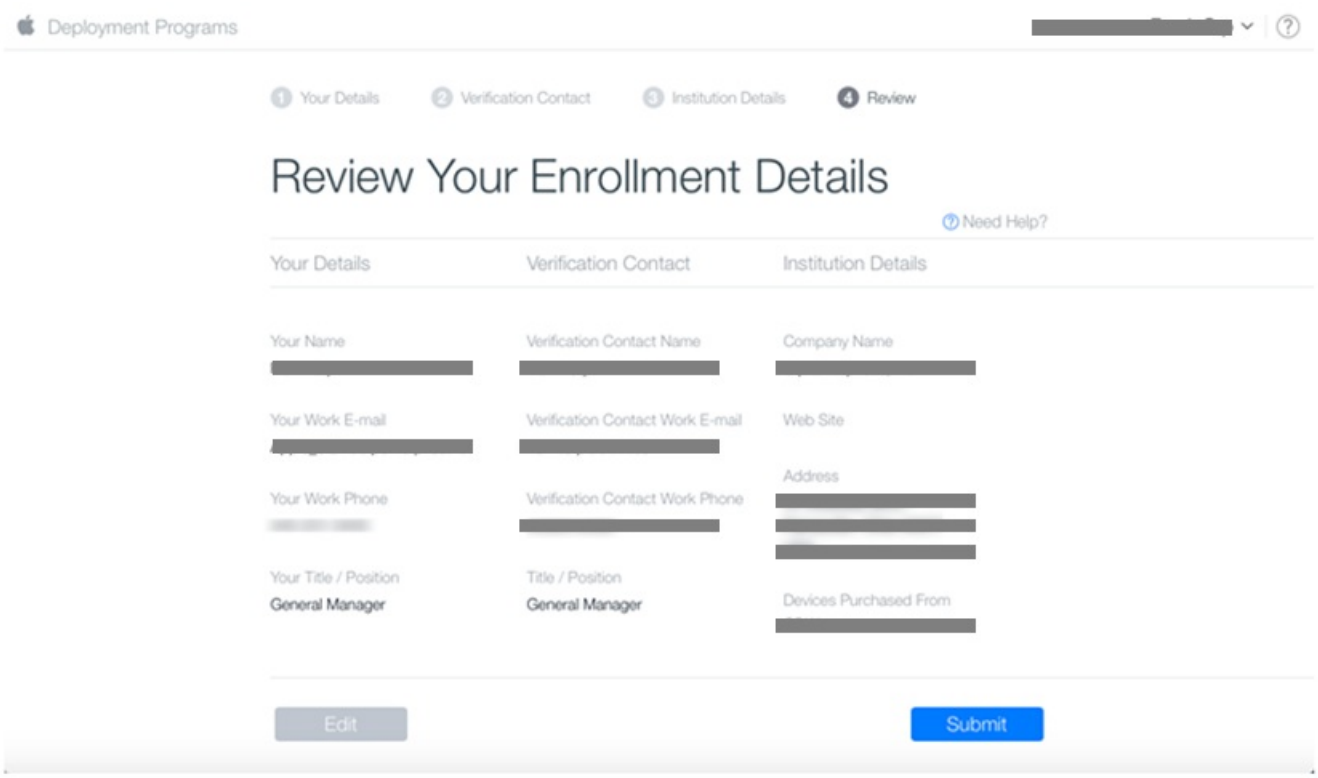


5. Add your company details and then select from where you purchase devices. For details on purchasing options, see the next section, Ordering DEP-enabled devices.

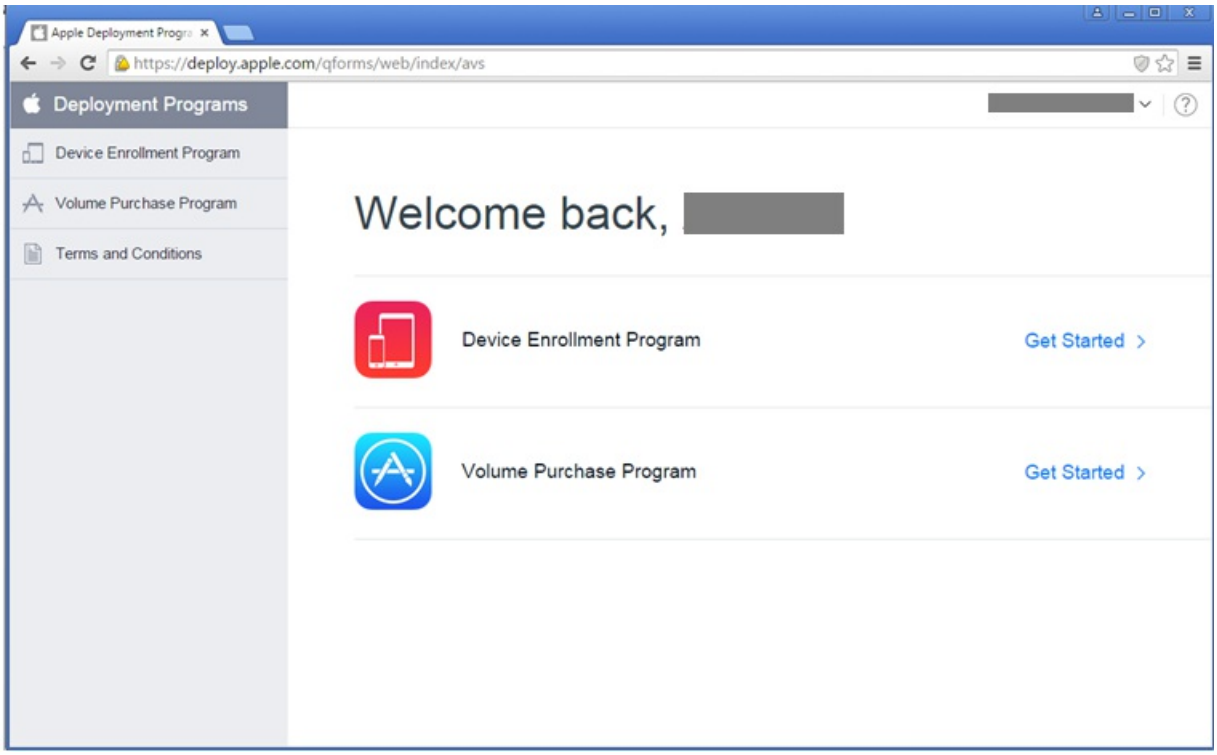


6. Add the Apple Customer Number or the DEP Reseller ID and then verify your enrollment details and wait for Apple to approve your account.





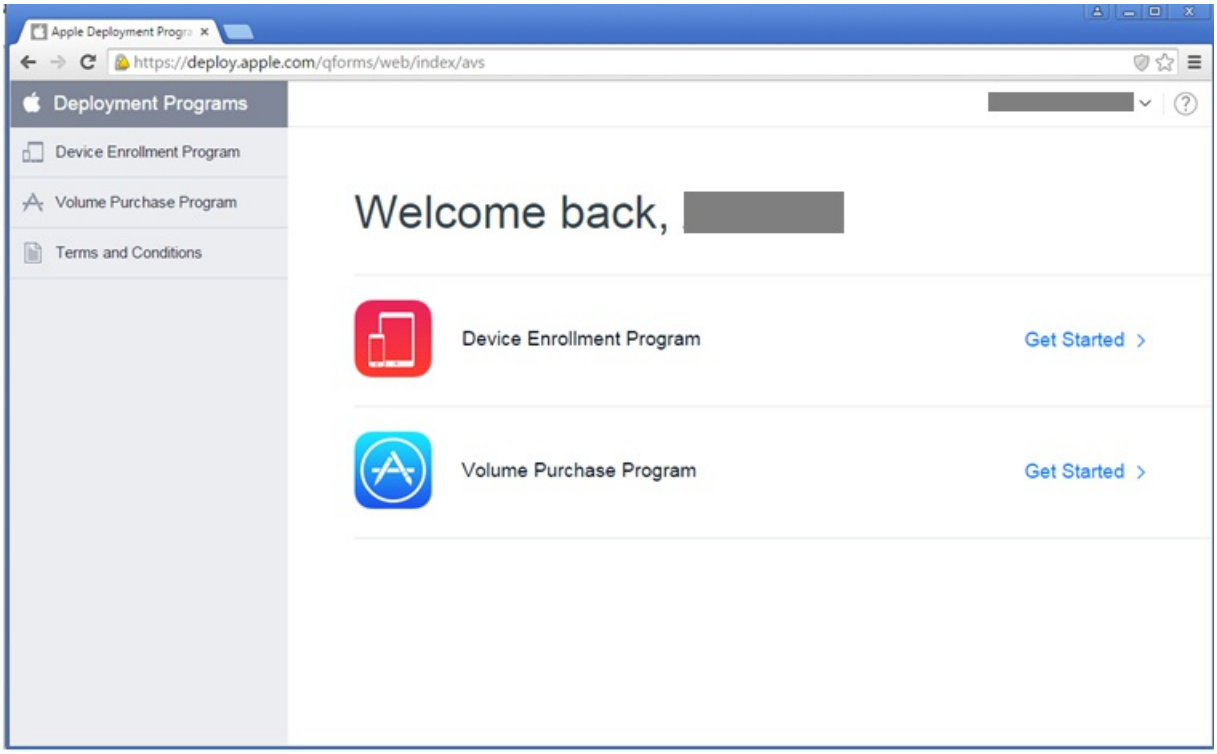
7. After you receive your logon credentials from Apple, log into the Apple DEP Portal. Then, follow the steps in the next section to connect your account with XenMobile.



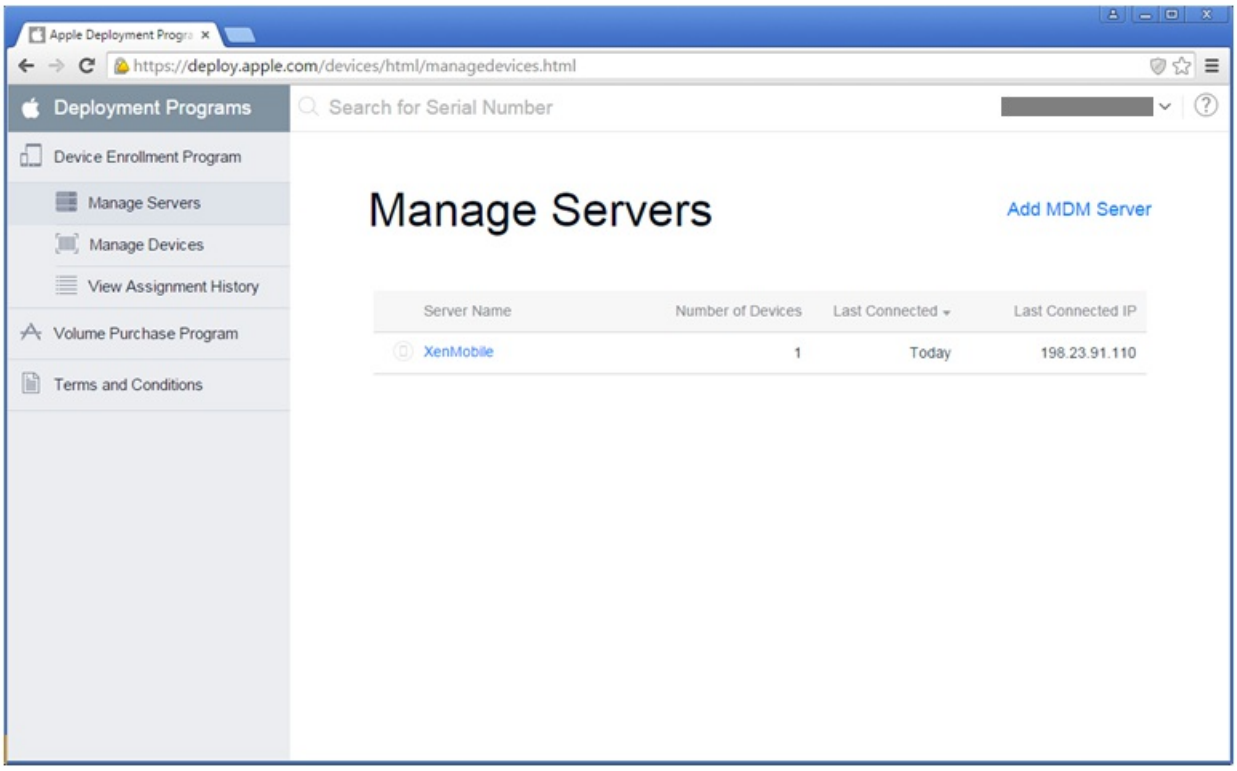
Integrating your Apple DEP account with XenMobile

Follow the steps in this section to connect your Apple DEP account with your XenMobile server deployment.

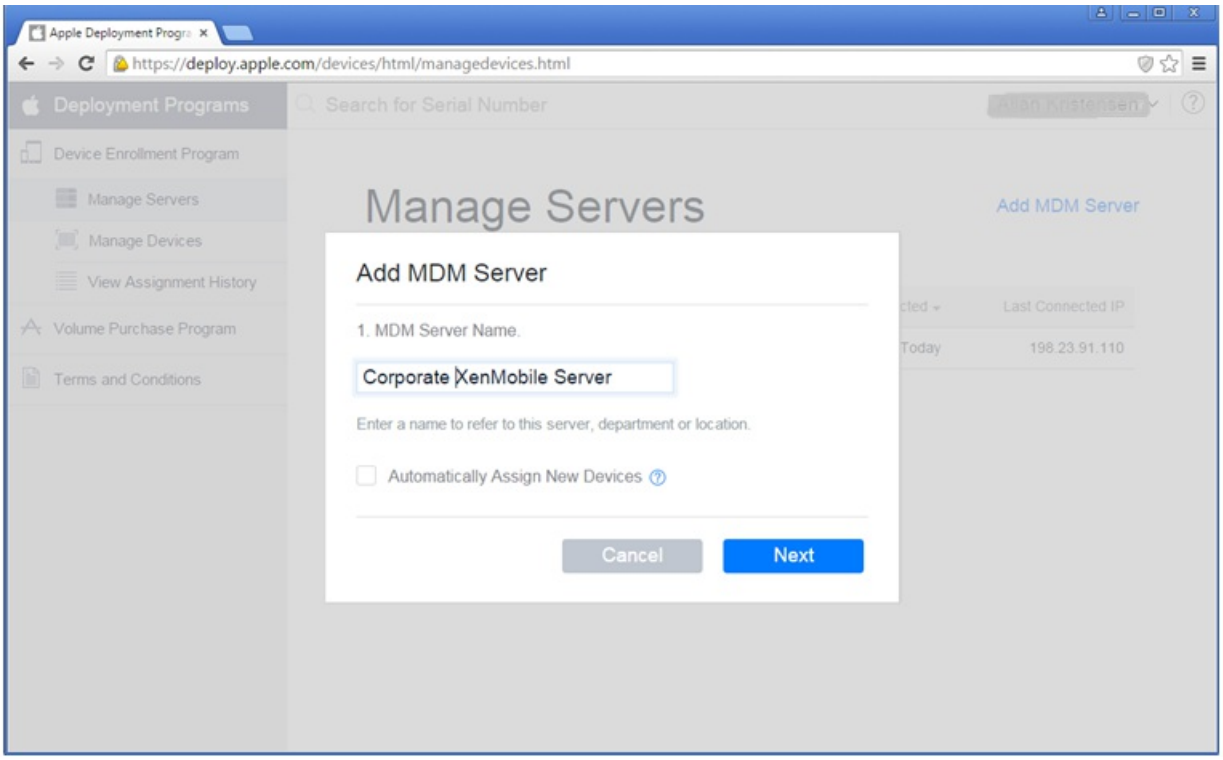
1. On the left-hand side of the Apple DEP Portal, click **Device Enrollment Program**.



2. Click **Manage Servers** and then on the right-hand side, click **Add MDM Server**.



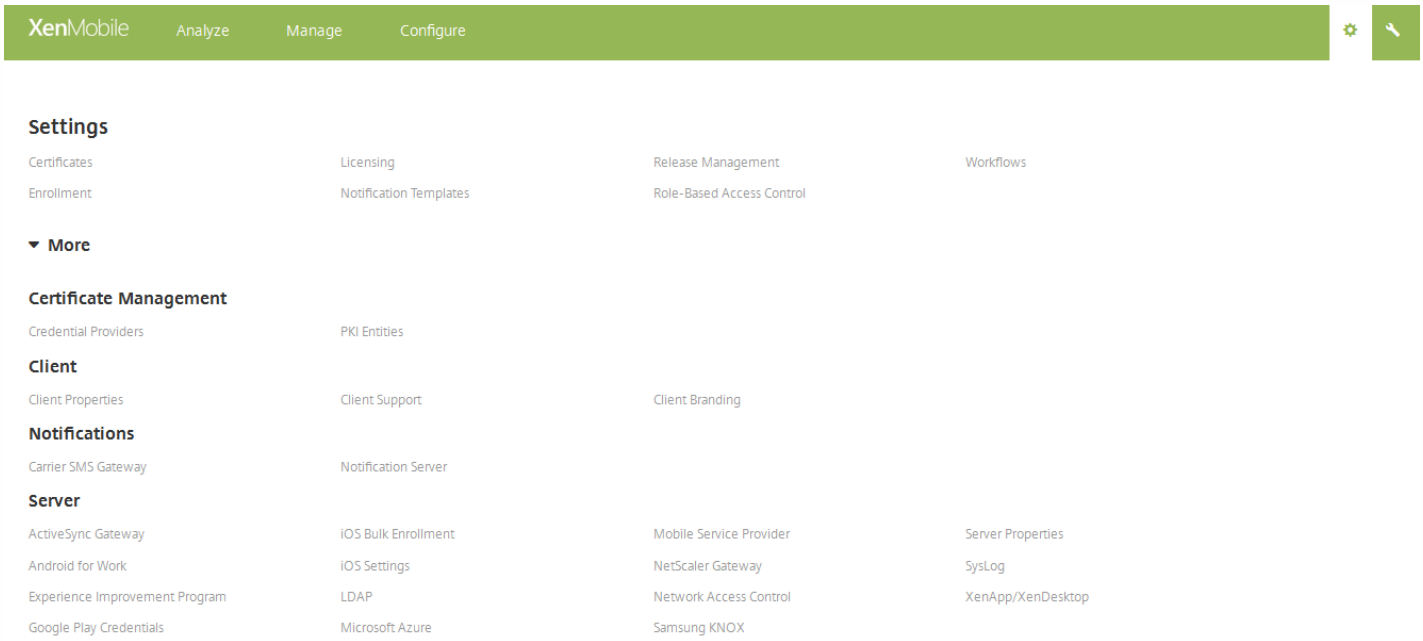
3. In **Add MDM Server**, enter a name for your XenMobile server and then click **Next**.



4. Upload a public key from your XenMobile server. To generate the key from XenMobile, do the following:

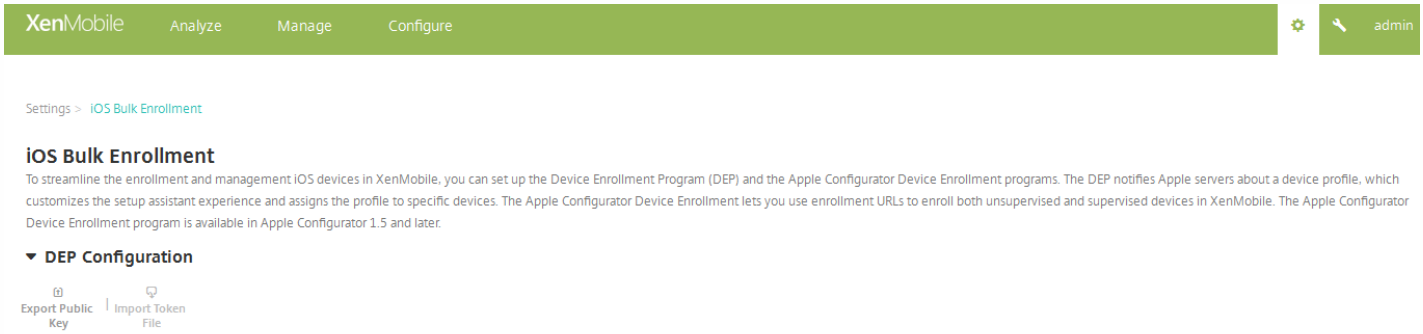
   a. Log on to the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.

   b. Under **More**, click **iOS Bulk Enrollment**.

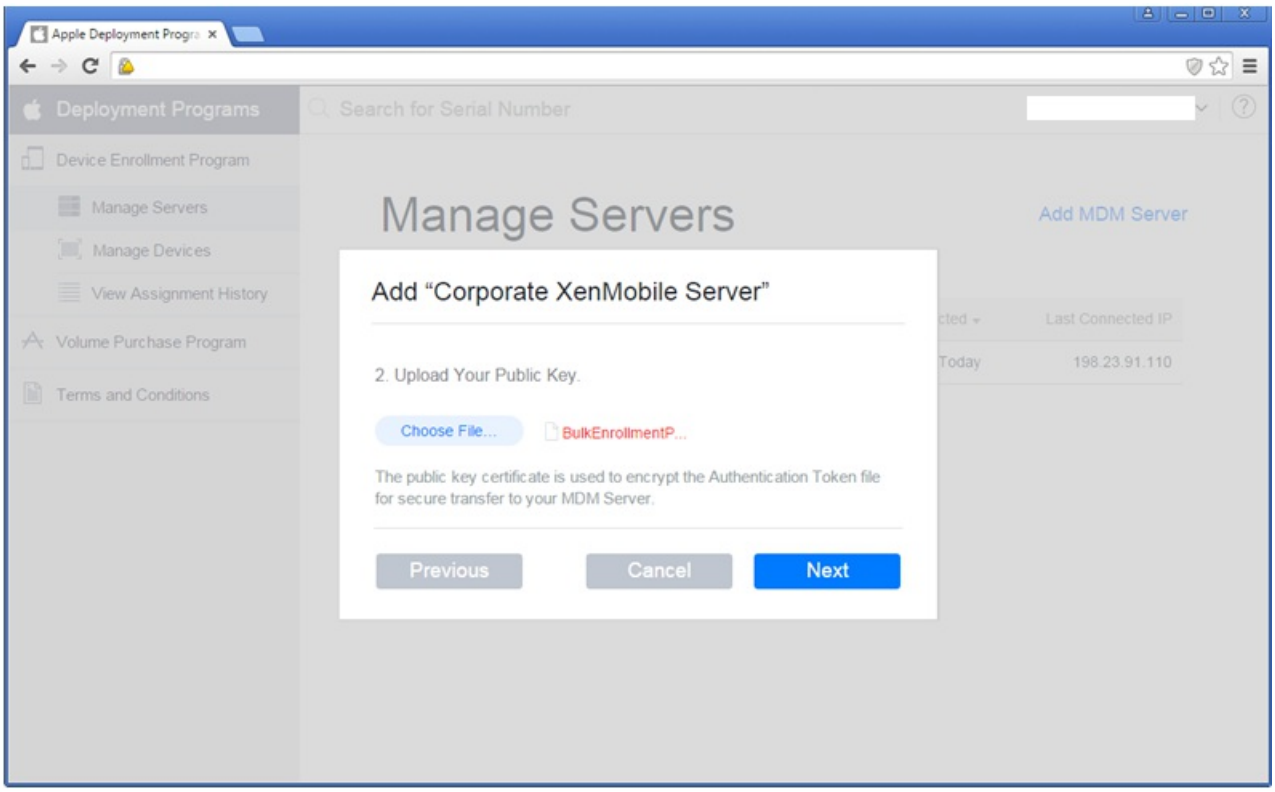


   b. On the **iOS Bulk Enrollment** page, expand **DEP Configuration** and then click **Export Public Key**. The public key is

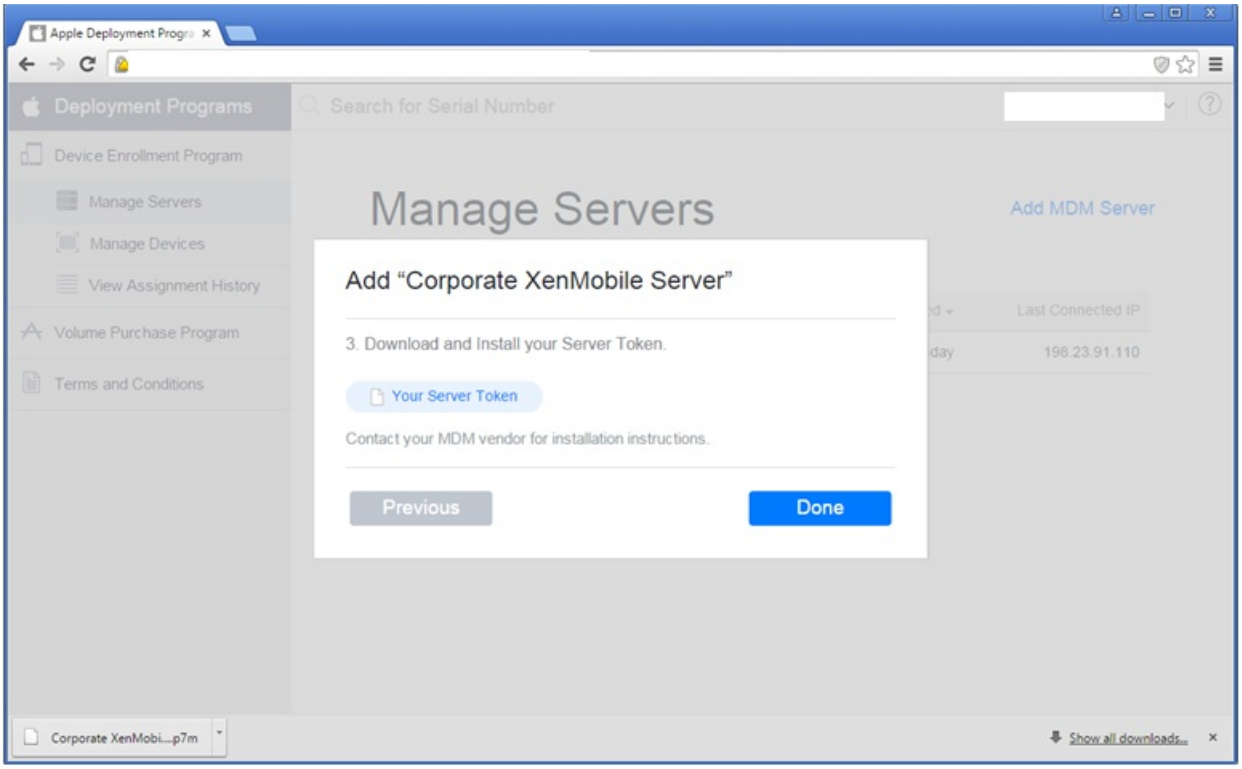
downloaded.



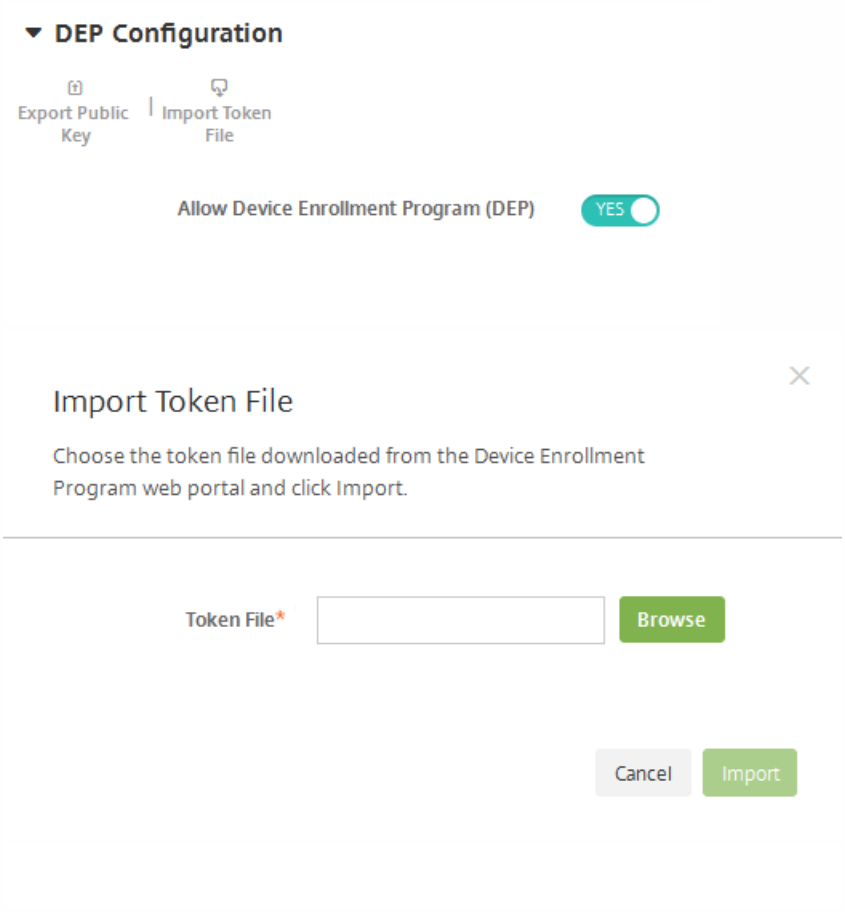
5. On the Apple DEP Portal, click **Choose file**, select the public key you just downloaded and then click **Next**.



6. Click **Your Server Token** to generate a server token, which is downloaded from the browser, and then click **Done**.

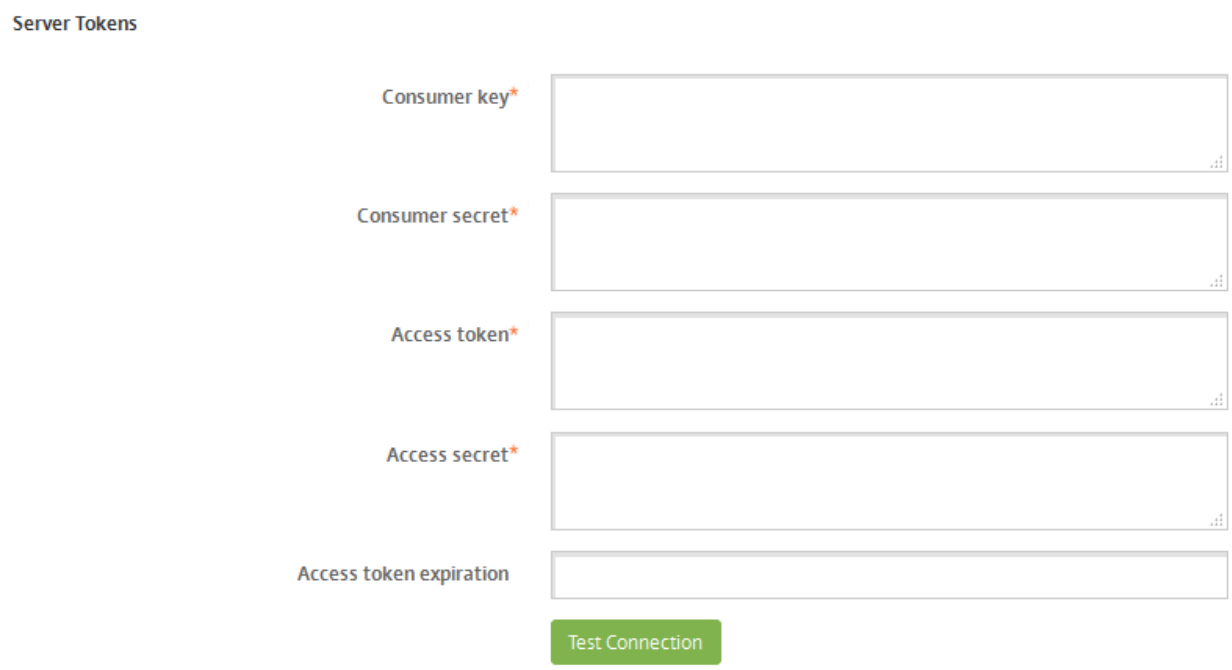


7. On the XenMobile console **iOS Bulk Enrollment** page, next to **Allow Device Enrollment Program (DEP)**, click YES, click **Import Token File** and then upload the token file you downloaded in the preceding step.



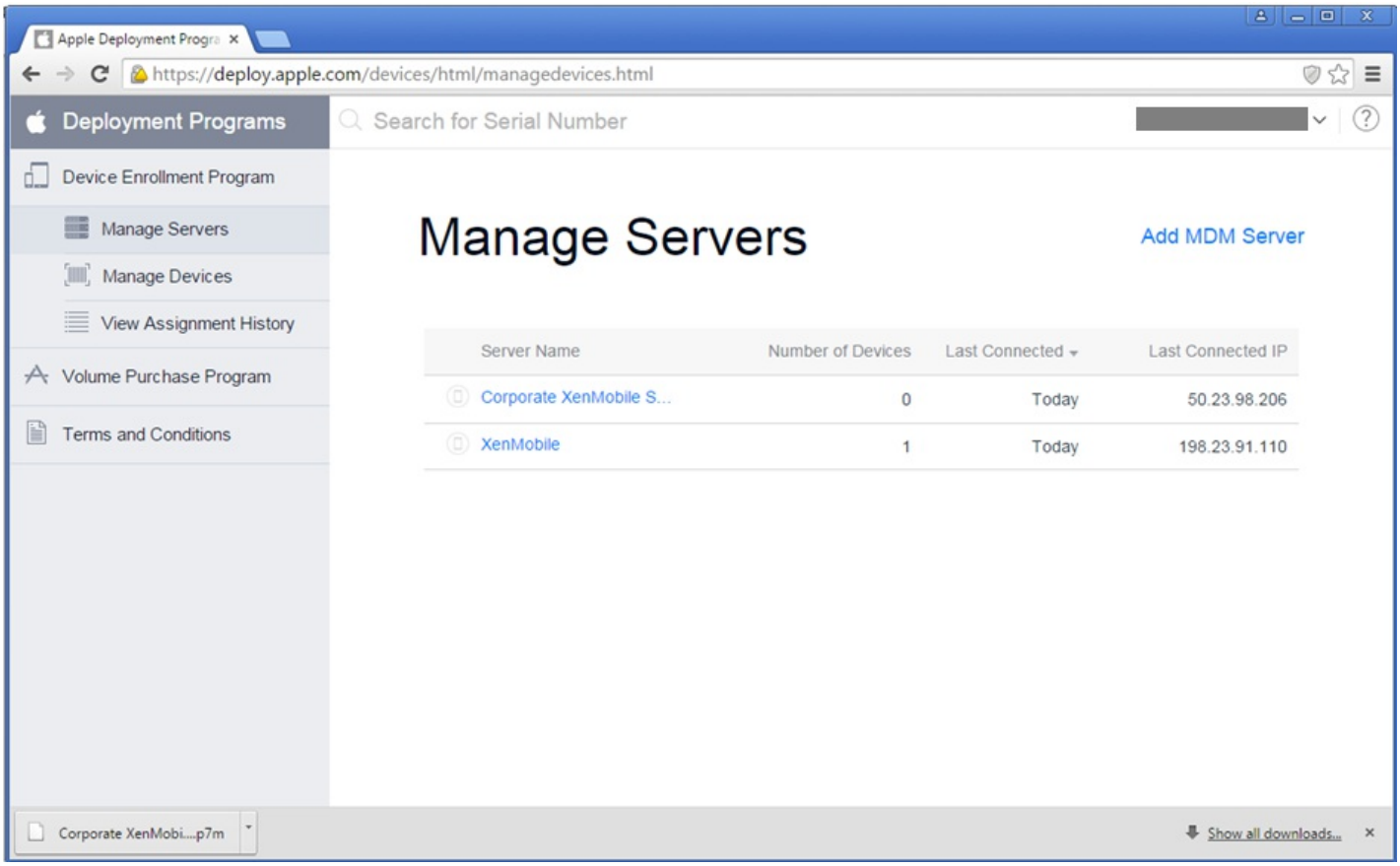
Your Apple DEP token information appears in the XenMobile console after you import the token file.

8. Click **Test Connection** to verify the Apple DEP connection with XenMobile.



9. On the **iOS Bulk Enrollment** page, complete the additional settings, select the Apple DEP controls and policies you want to implement for your Apple DEP devices and then click **Save**.

The XenMobile server appears in the Apple DEP Portal.



Ordering DEP-enabled devices

You can order DEP-enabled devices directly from Apple or DEP-enabled authorized resellers or carriers. To order from Apple, you need to provide your Apple Customer ID within the Apple DEP Portal to enable Apple to associate your device purchased with your Apple DEP account.

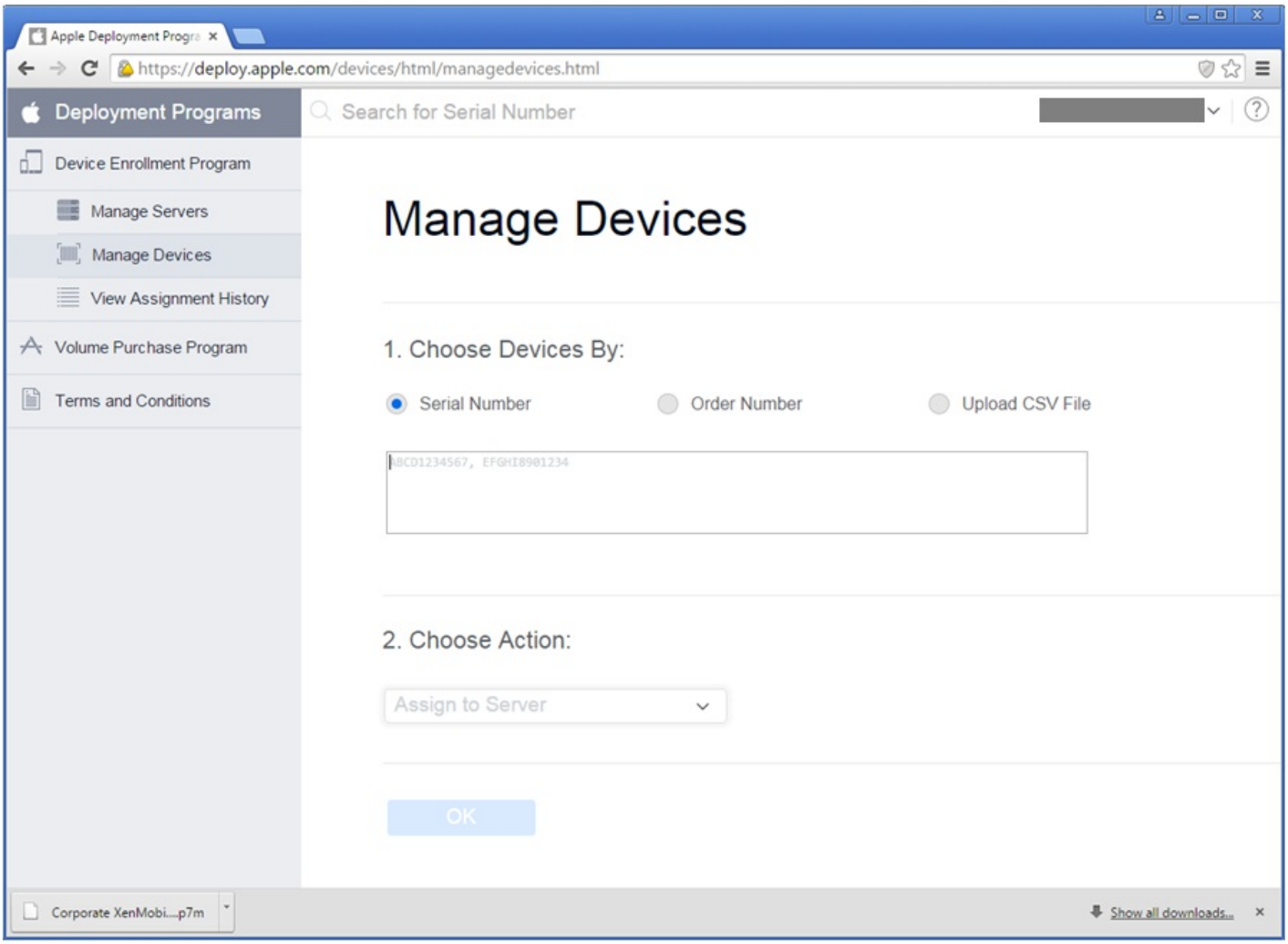
To order from your reseller or carrier, contact your Apple reseller or carrier to check if they participate in the Apple DEP. Ask for the resellers' Apple DEP ID when purchasing devices. You will need this information to add your Apple DEP reseller to your Apple DEP account. You will receive a DEP customer ID after adding the resellers' Apple DEP ID, when approved. Provide the DEP customer ID to the reseller, who will use the ID to submit information about your device purchases to Apple. For more information, see this Apple website.

Managing DEP-enabled devices

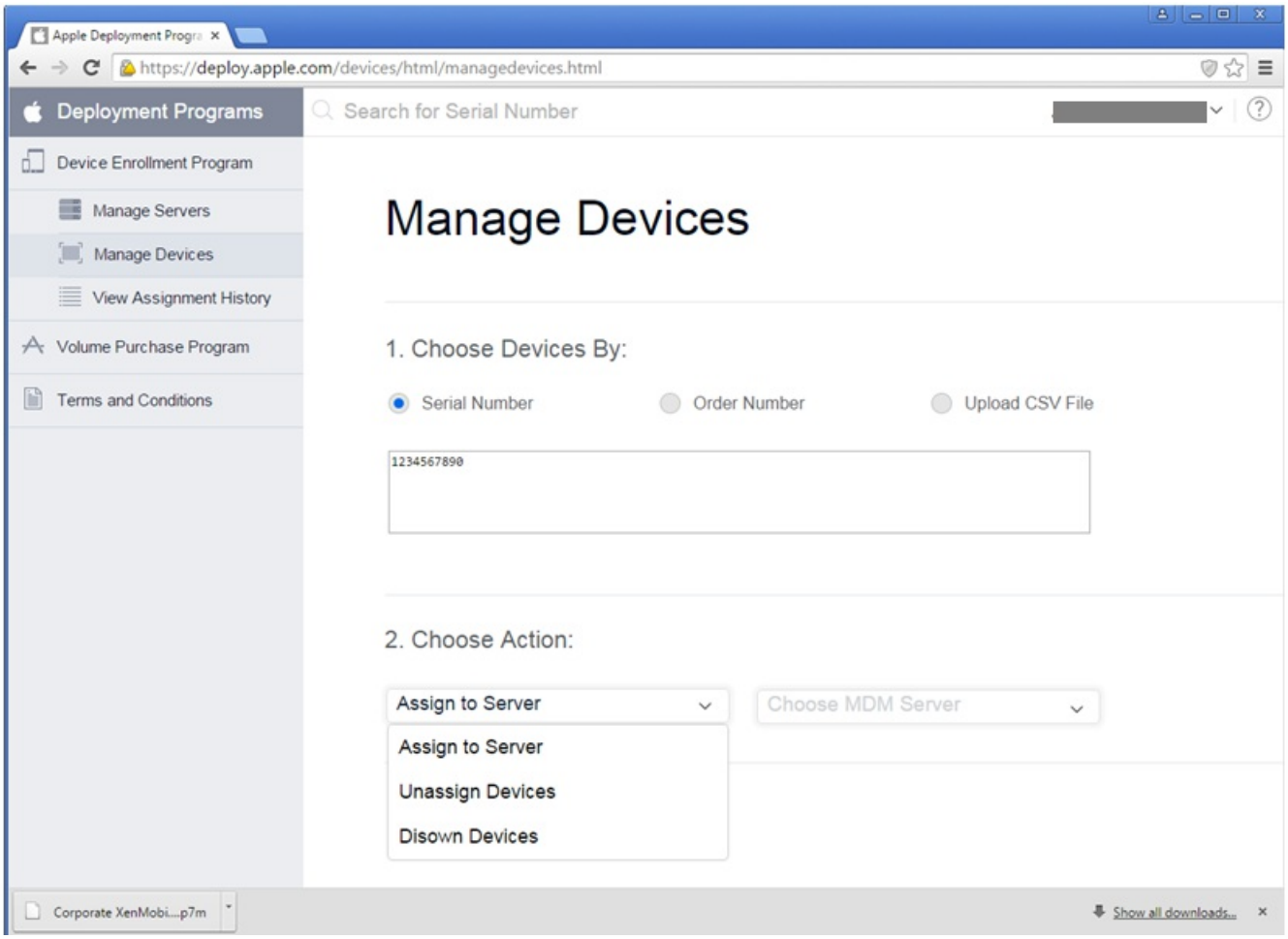
Follow these steps to associate devices with your XenMobile server within your Apple DEP account through the DEP Portal.

1. Log on to the Apple DEP Portal.

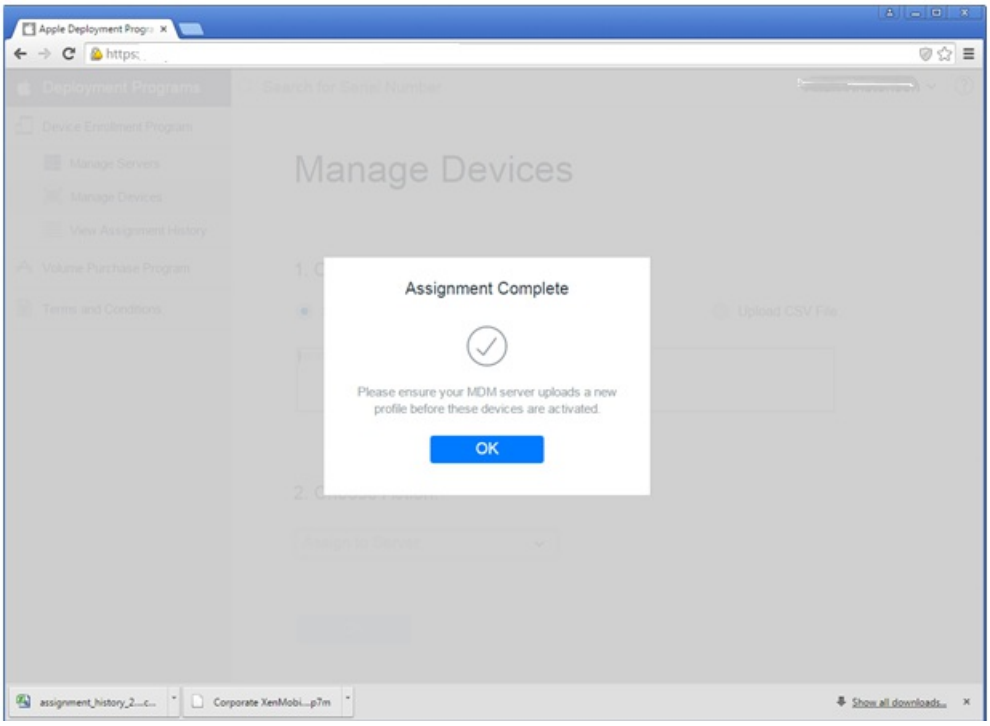
2. Click **Device Enrollment Program**, click **Manage Devices** and then in **Choose Devices By**, select the option for which you want to upload and define your Apple DEP-enabled devices - **Serial Number**, **Order Number**, or **Upload CSV File**.



3. Under **Choose Action**, to assign your devices to a XenMobile server, click **Assign to Server** and then in the list, click the name of your XenMobile server and then click **OK**.



Your Apple DEP devices are now associated with the selected XenMobile server.



User experience enrolling an Apple DEP-enabled device

When users enroll an Apple DEP-enabled device, their experience is as follows.

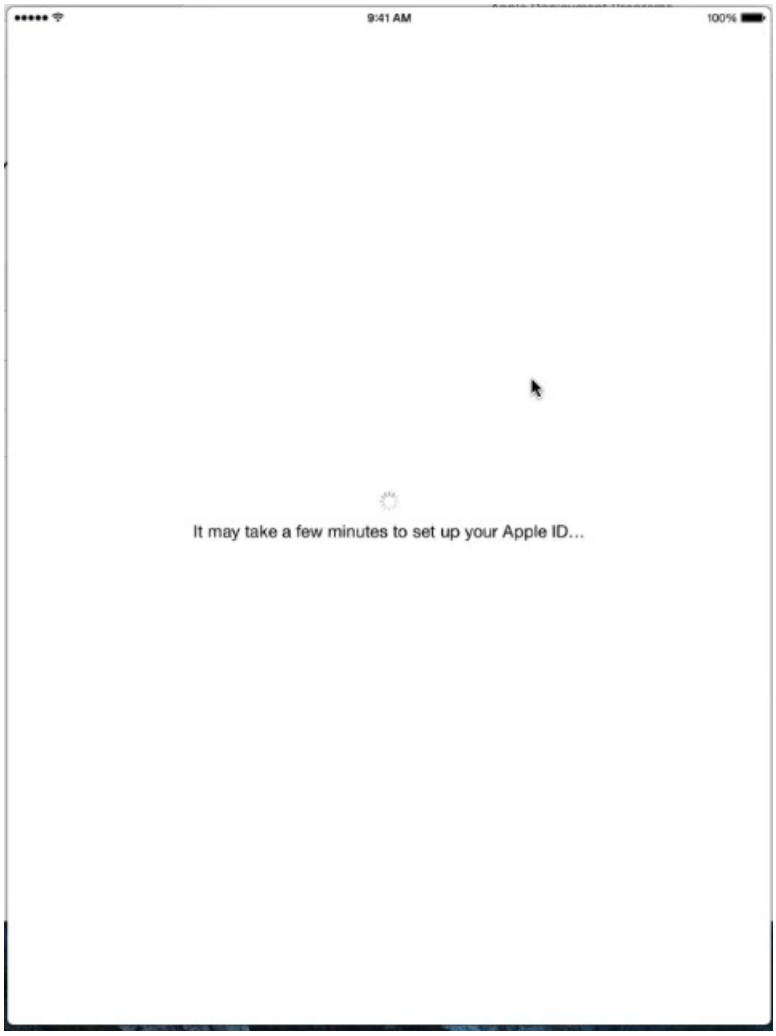
1. Users start their Apple DEP-enabled device.

2. Users the configuration wizard to configure the initial settings on their iOS device.

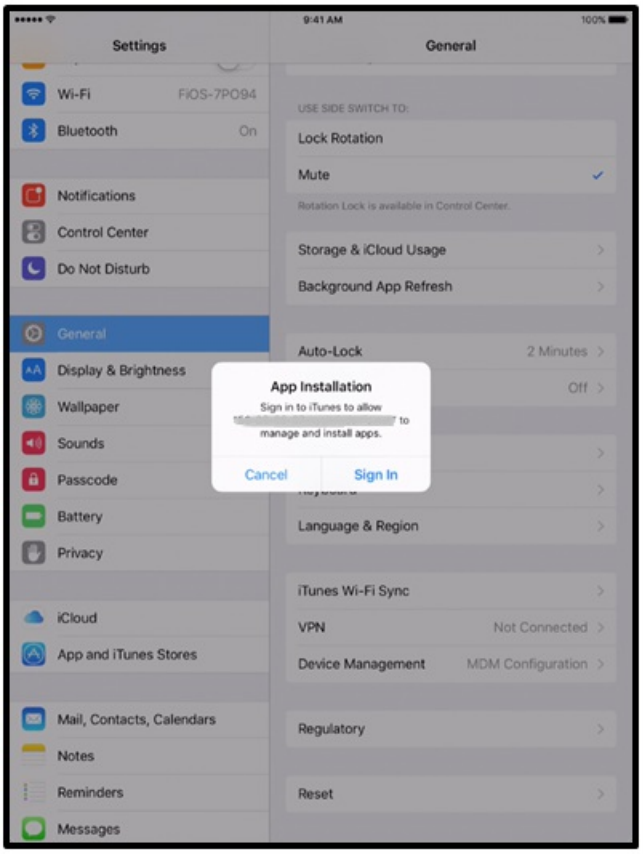
3. The device automatically starts the XenMobile device enrollment process. Users follow the wizard to enroll the device into the XenMobile server associated with the Apple DEP-enabled device.

The Apple DEP enrollment process starts automatically as part of the initial IOS configuration flow for Apple DEP enabled devices.

4. The Apple DEP configuration that you configured in the XenMobile console is delivered to the Apple DEP-enabled device. Users follow the wizard to configure the device.



5. Users may be prompted to sign into iTunes so that Worx Home can be downloaded.



6. Users open Worx Home and enter their credentials. If required by the policy, users may be prompted to create and verify a Worx PIN. **Note**: As of version 10.4, Worx Home is renamed Secure Hub and Worx PIN is renamed Citrix PIN.

The remainder of the required apps are pushed down to the device.

iOS Volume Purchase Plan Settings

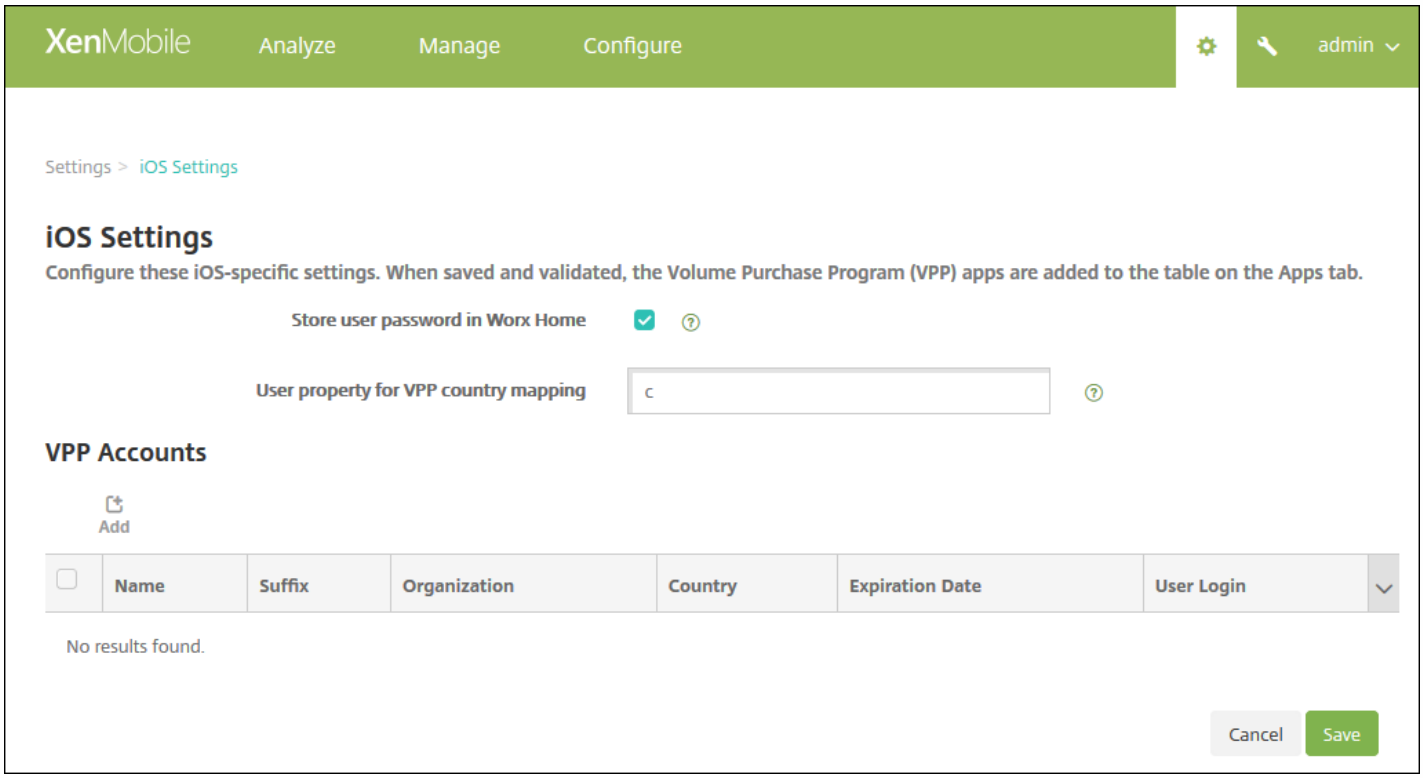
Jan 04, 2017

You can configure settings specific to the iOS Volume Purchase Plan (VPP) in XenMobile. The iOS VPP simplifies the process to find, buy, and distribute apps and other data in bulk for an organization. VPP provides a simple, scalable solution to manage an organization's content needs.

After you save and validate the iOS VPP settings in XenMobile, the purchased apps are added to the table on the Apps tab 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 **Server**, click **iOS Settings**. The **iOS Settings** configuration page appears.



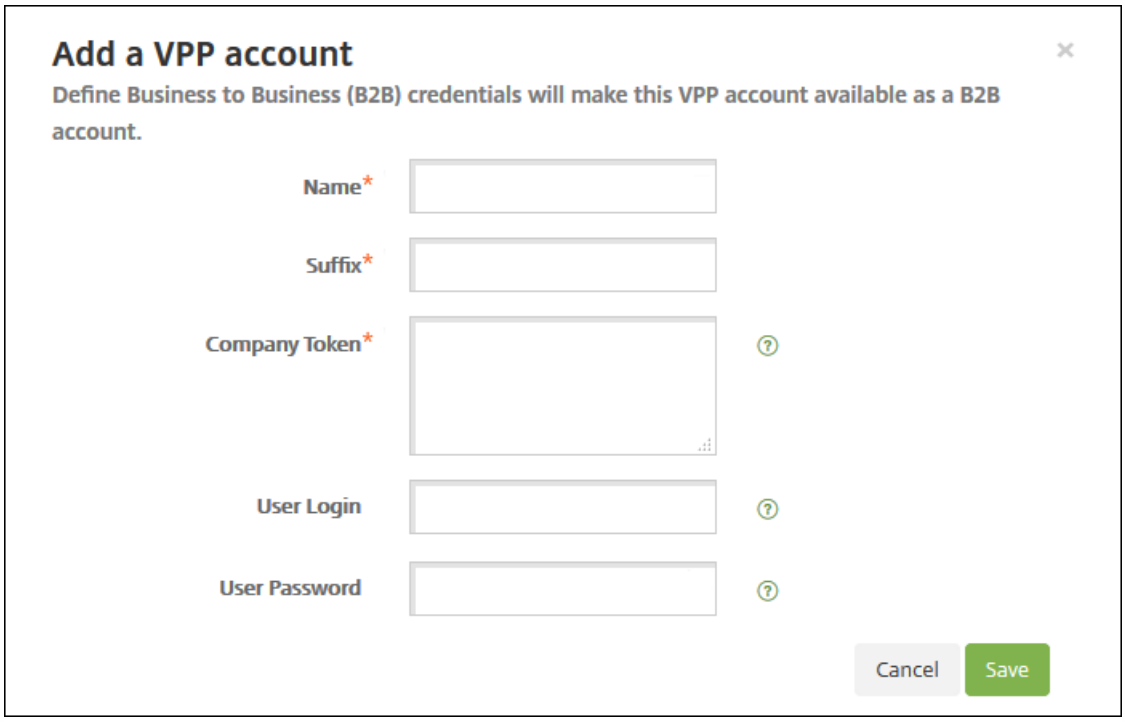
3. Configure these settings:

- **Store user password in Worx Home**: Select whether to securely store a user name and password in Worx Home for XenMobile authentication. The default is to store the information. (**Note**: Starting with version 10.4, Worx Home is renamed Secure Hub.)
- **User property for Volume Purchasing Program (VPP) country mapping**: Type a code to allow users to download apps from country-specific app stores.

  This mapping is used 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 distributed in 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:

- **Name**: Type the VPP account name.
- **Suffix**: Type the suffix that appears on apps obtained through the VPP account.
- **Company Token**: Type, or 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 user name.
- **User Password**: Type an optional VPP account user password.

5. Click **Save** to close the dialog box.

6. Click **Save** to save the iOS settings.

Mobile Service Provider

Jan 06, 2017

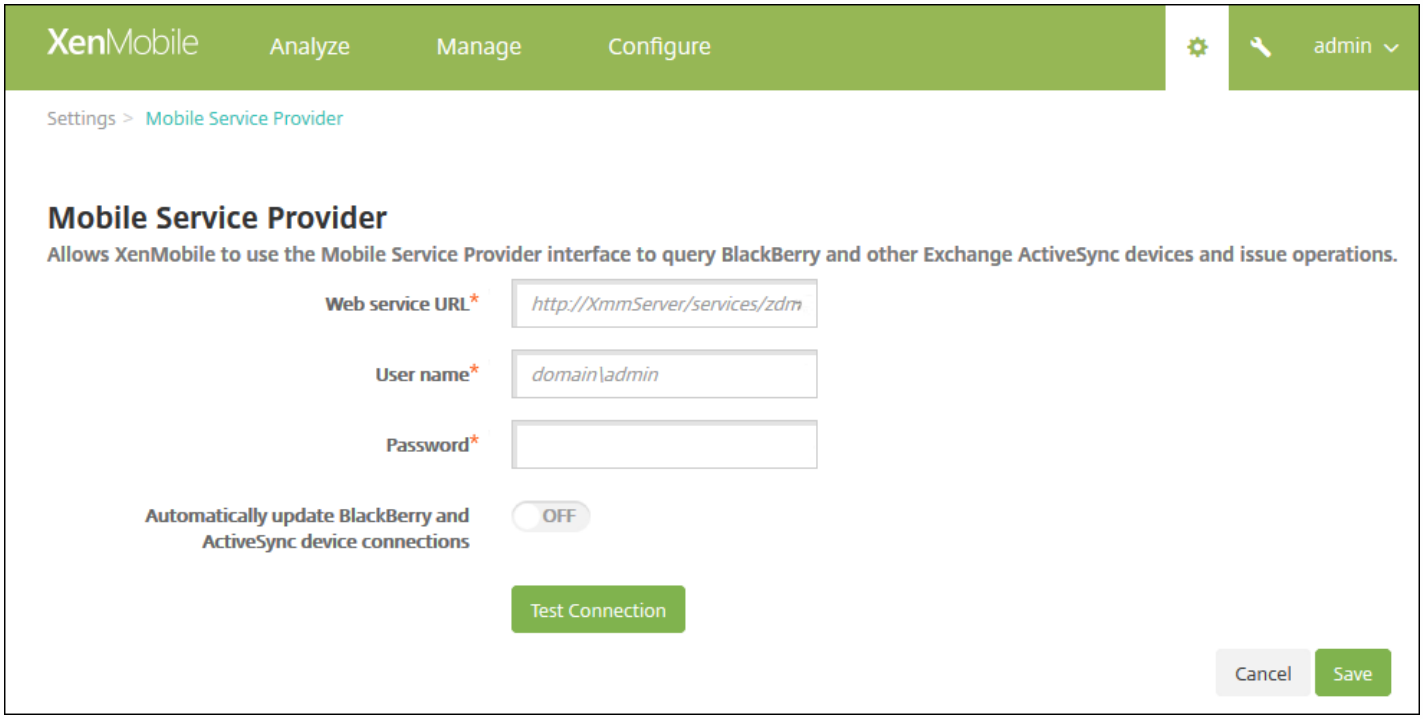
You can enable XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.

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**.

Network Access Control

Mar 21, 2016

If you have a Network Access Control (NAC) appliance set up in your network, such as a Cisco ISE, in XenMobile, you can enable filters to set devices as compliant or not compliant for NAC, based on rules or properties. If a managed device in XenMobile does not meet the specified criteria, and as a result is marked Not Compliant, the NAC appliance will block the device on your network.

In the XenMobile console, you select one or more criterion in the list to set a device as not compliant.

XenMobile supports the following NAC compliance filters:

Anonymous Devices: Checks if a device is in anonymous mode. This check is available if XenMobile can't re-authenticate the user when a device attempts to reconnect.

Failed Samsung KNOX attestation: Checks if a device failed a query of the Samsung KNOX attestation server.

Forbidden Apps: Checks if a device has forbidden apps, as defined in an App Access policy.

Implicit Allow and Deny: This action is the default for the ActiveSync Gateway, which creates a Device List of all devices that do not meet any of the other filter rule criteria and allows or denies connections based on that list. If no rule matches, the default is Implicit Allow.

Inactive Devices: Checks if a device is inactive as defined by the Device Inactivity Days Threshold setting in Server Properties.

Missing Required Apps: Checks if a device is missing required apps, as defined in an App Access policy.

Non-suggested Apps: Checks if a device has non-suggested apps, as defined in an App Access policy.

Noncompliant Password: Checks if the user password is compliant. On iOS and Android devices, XenMobile can determine whether the password currently on the device is compliant with the passcode policy sent to the device. For instance, on iOS, the user has 60 minutes to set a password if XenMobile sends a passcode policy to the device. Before the user sets the password, the passcode might be non-compliant.

Out of Compliance Devices: Checks whether a device is out of compliance, based on the Out of Compliance device property. That property is usually changed by the automated actions or by a 3rd party leveraging XenMobile APIs.

Revoked Status: Checks whether the device certificate was revoked. A revoked device cannot re-enroll until it is authorized again.

Rooted Android and Jailbroken iOS Devices: Checks whether an Android or iOS device is jailbroken.

Unmanaged Devices: Check whether a device is still in a managed state, under XenMobile control. For example, a device running in MAM mode or an un-enrolled device is not managed.

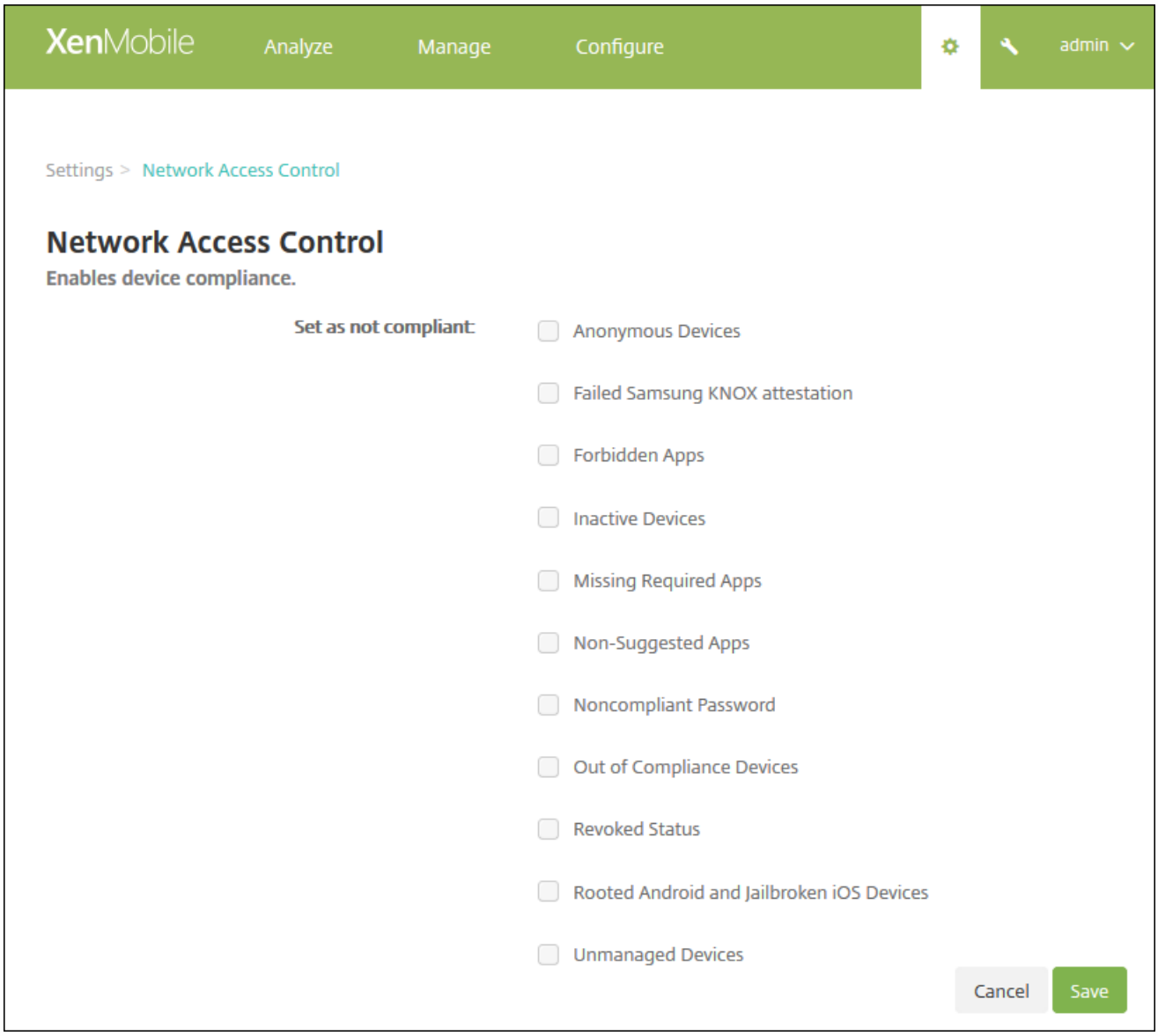
Send Android domain users to ActiveSync Gateway: Click **YES** to ensure that XenMobile sends Android device information to the ActiveSync Gateway. When this option is enabled, it ensures that XenMobile sends Android device information to the ActiveSync Gateway in the event that XenMobile does not have the ActiveSync identifier for the Android device user.

> **Note**
>
> The Implicit Compliant/Not Compliant filter sets the default value only on devices that are managed by XenMobile. For example, any devices that have a blacklisted app installed or are not enrolled, are marked as Not-Compliant and will be blocked from your network by the NAC appliance.

Configure network access control

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

2. Under **Server**, click **Network Access Control**. The **Network Access Control** page appears.



3. Select the checkboxes for the **Set as not compliant** filters you want to enable.

4. Click **Save**.

Samsung KNOX

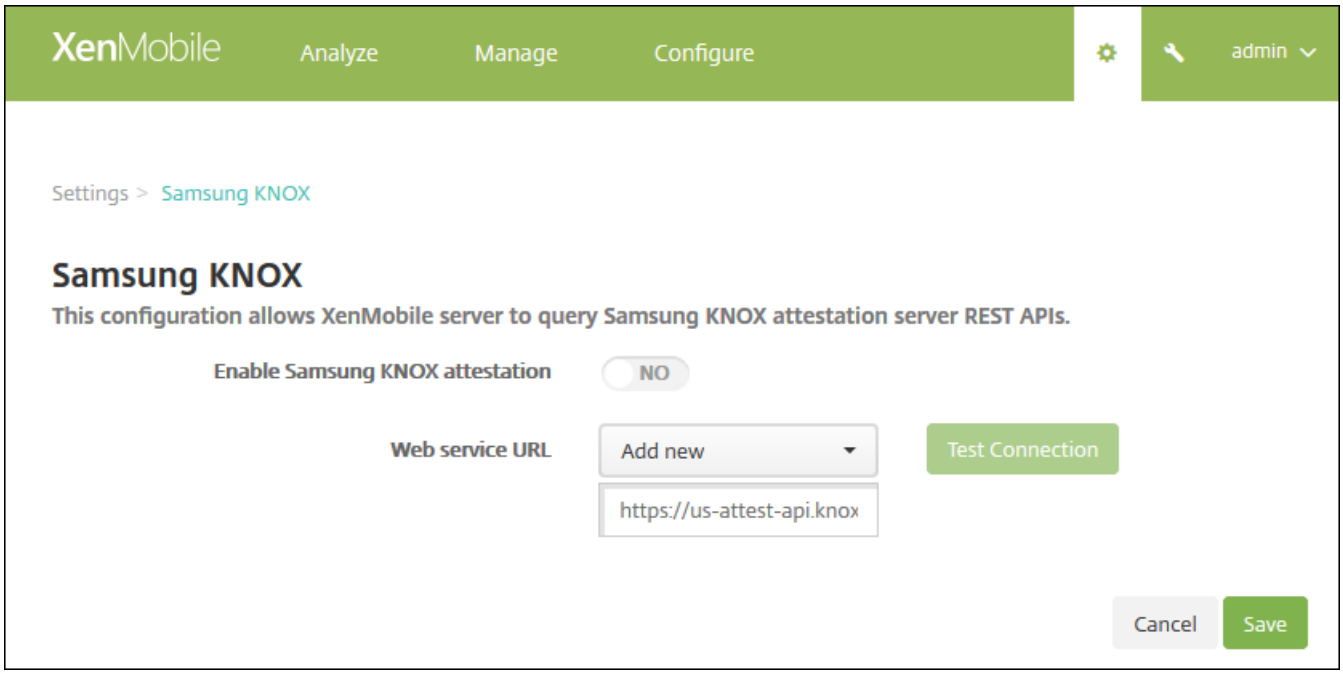
Mar 09, 2016

You can configure XenMobile to query the Samsung KNOX attestation server REST APIs.

Samsung KNOX leverages hardware security capabilities that provide multiple levels of protection for the operating system and applications. One level of this security resides at the platform through attestation. An attestation server provides verification of the mobile device's core system software (for example, the boot loaders and kernel) at runtime based on data collected during trusted boot.

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

2. Under **Server**, click **Samsung KNOX**. The **Samsung KNOX** page appears.



3. Configure these settings:

- **Enable Samsung KNOX attestation**: Select whether to enable Samsung KNOX attestation. The default is **NO**. When you enable **Enable Samsung KNOX attestation**, the **Web service URL** option is enabled.
- In the list, click the appropriate attestation server.

4. Click **Test Connection** to verify the connection.

5. Click **Save**.

Note

You can use SamSung KNOX Mobile Enrollment to enroll multiple Samsung KNOX devices into XenMobile (or any Mobile Device Manager) without manually configuring each device. For information, see Samsung KNOX Bulk Enrollment.

Server Properties

Jan 04, 2017

XenMobile has over 100 properties that apply to server-wide operations. This article describes some of the more important server properties and also details how to add, edit, or delete server properties.

Server Property Definitions

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**.

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**.

Inactivity Timeout in Minutes

The number of minutes after which an inactive administrator who used the XenMobile server Public API to access the XenMobile console or any third-party app, is logged out. A timeout of **0** means an inactive user remains logged in. Defaults to **5**.

NetScaler Single Sign-On

If **False**, disables the XenMobile callback feature during single signon from NetScaler to the XenMobile server. The callback feature is used to verify the NetScaler Gateway session ID, if the NetScaler Gateway configuration includes a callback URL. Defaults to **False**.

Session Log Cleanup (in Days)

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

Unauthenticated App Download for Android Devices

If **True**, you can download self-hosted apps to Android devices running Android for Work. This property is needed 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 Worx Home versions which don't validate one-time tickets. If **False**, you can download unauthenticated apps from XenMobile to Windows devices. Defaults to **False**.

Note: Starting with version 10.4, Worx Home is renamed Secure Hub.

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 an inactive user is logged out of the XenMobile Self Help Portal. A timeout of **0** means an inactive user remains logged in. Defaults to **30**.

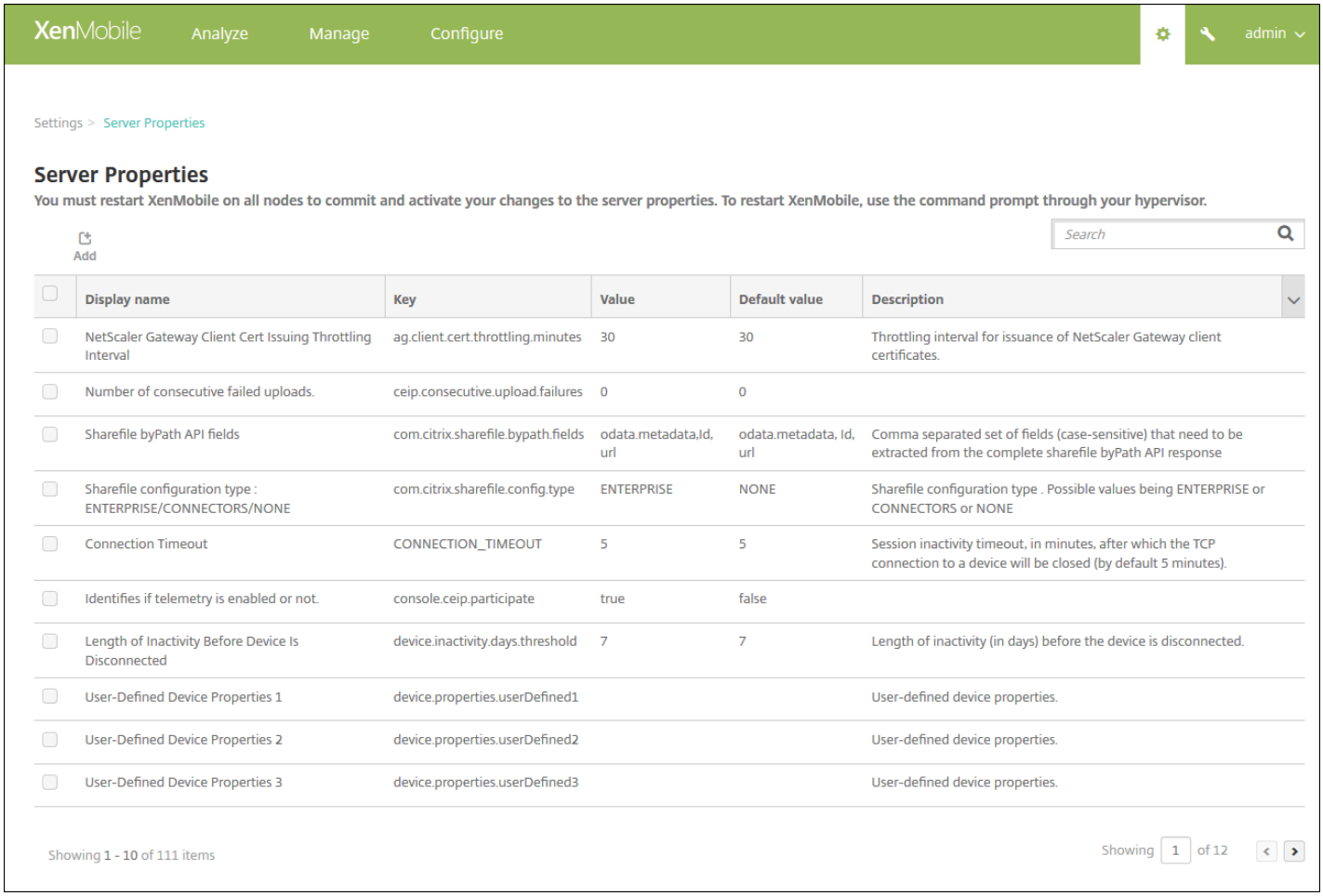
Adding, Editing, or Deleting Server Properties

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.

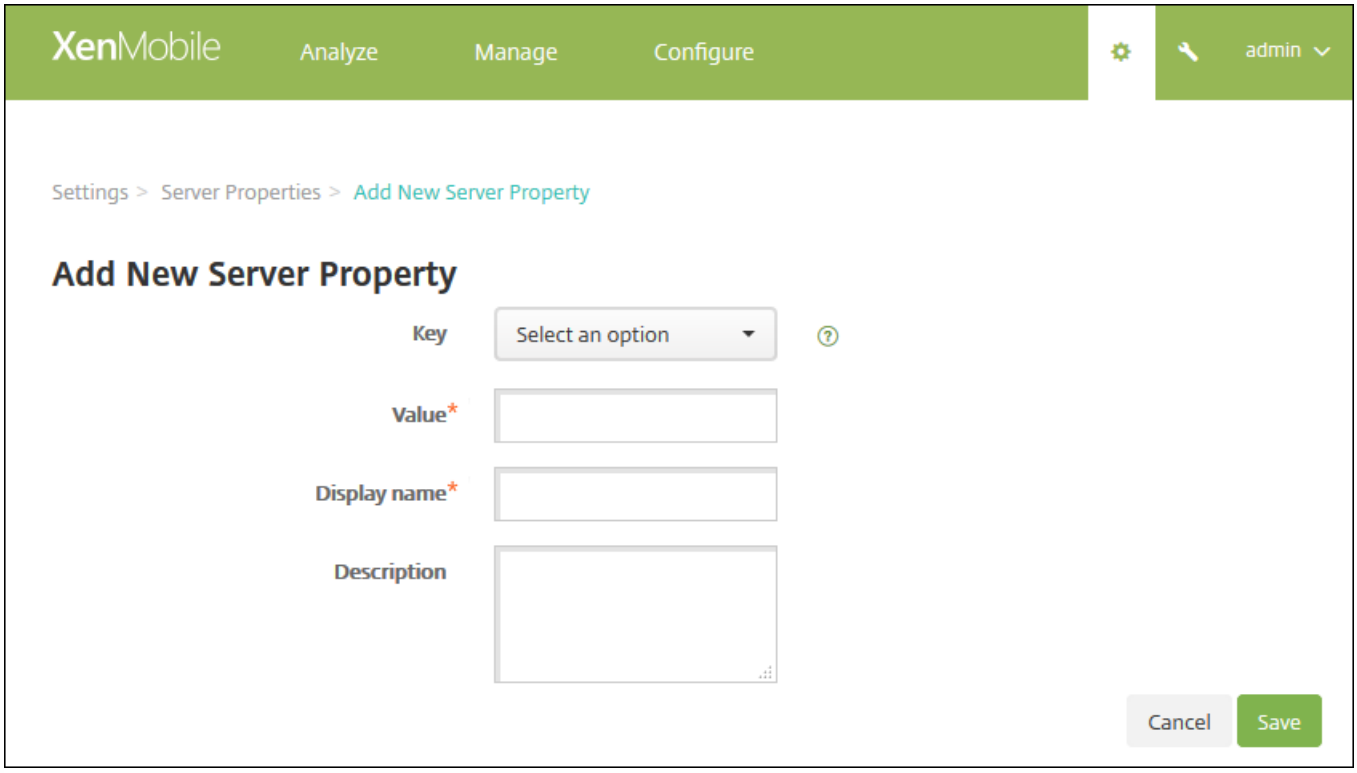
1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.

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.

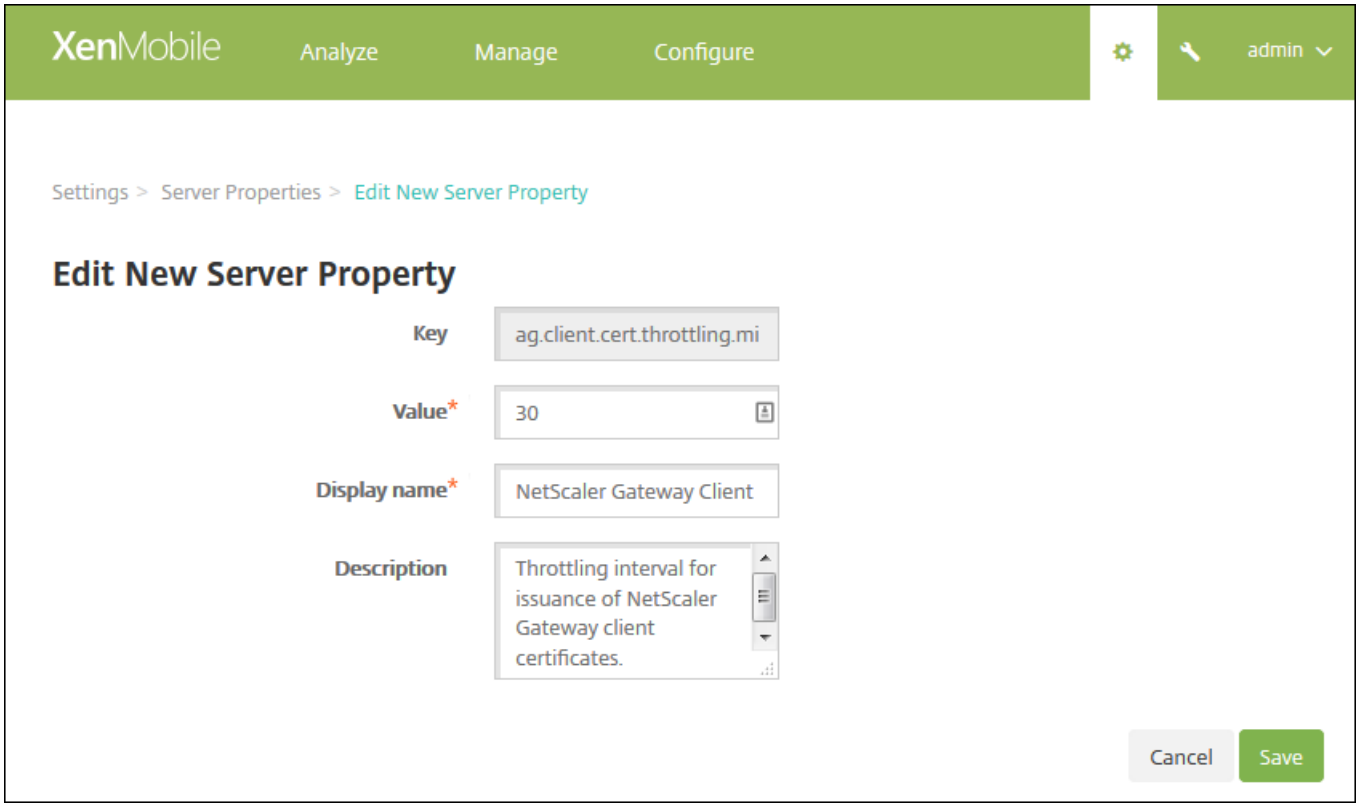
3. Click **Save**.

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.

Configuring XenMobile Server Mode

Mar 14, 2016

The XenMobile server mode is a value set in Server Properties. You can set the value to MAM, MDM, or ENT 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.

For information about setting the server mode, see To add, edit, or delete server properties.

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.

The server mode is added to the server log every time a license is activated or deleted and when the server mode is changed in Server Properties. For information about creating and viewing log files, see XenMobile Support and Maintenance.

SysLog

Apr 11, 2016

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:

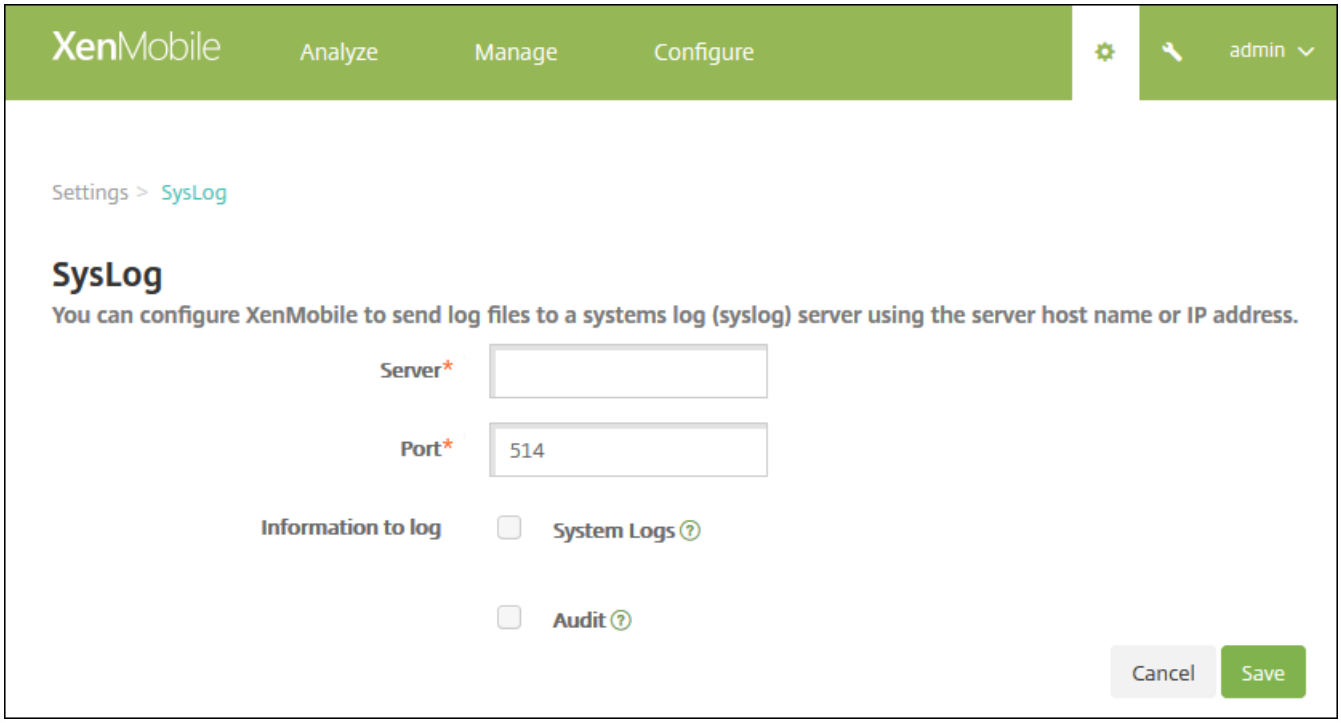
- The IP address of the appliance that generated the log message
- A time stamp
- The message type
- The log level associated with an event (Critical, Error, Notice, Warning, Informational, Debug, Alert, or Emergency)
- The message information

You can use this information to analyze the source of the alert and take corrective action if required.

> ## Note
>
> XenMobile cloud deployments, Citrix does not support syslog integration with an 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 Viewing and Analyzing 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:

- **Name**: 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**.

To configure XenApp and XenDesktop

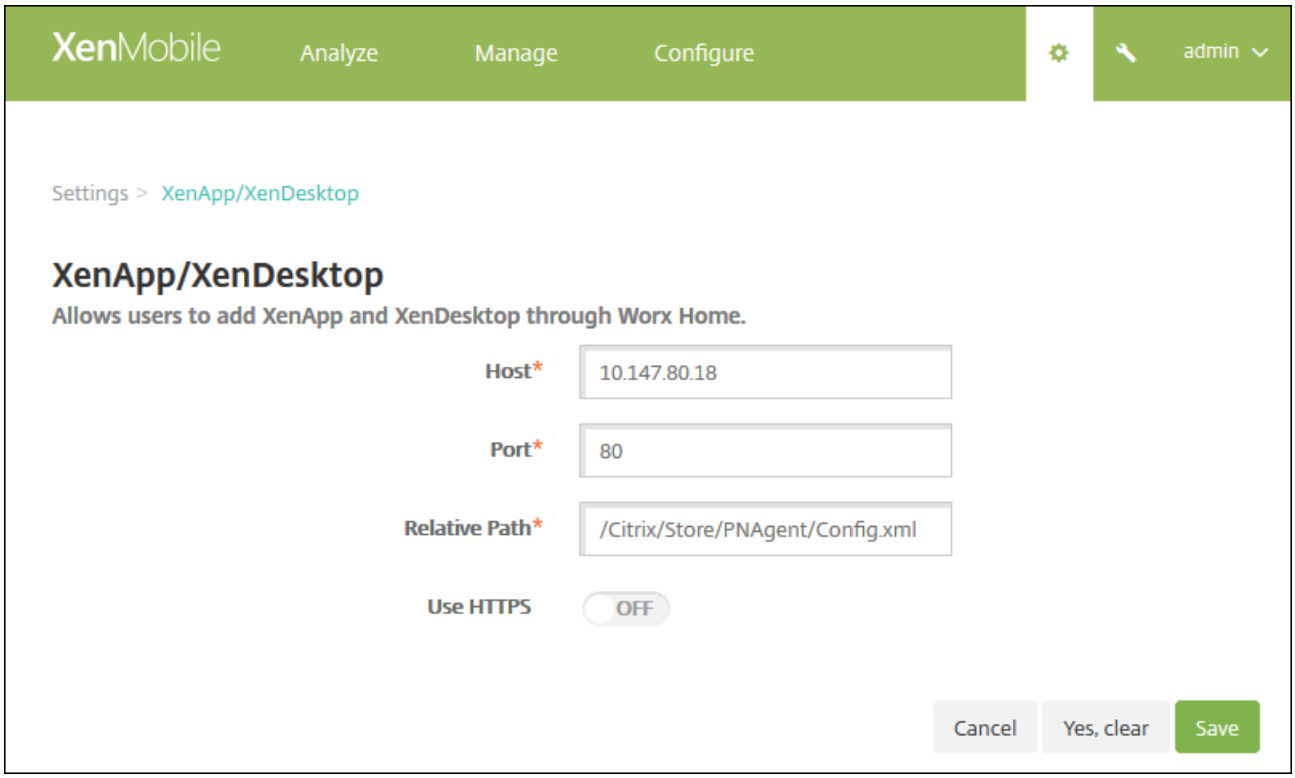
Jul 22, 2015

XenMobile can collect apps from XenApp and XenDesktop and make them available to mobile device users in Worx Store. Users subscribe to the apps directly inside Worx Store and launch them from WorxHome. Receiver must be installed on users' devices to launch the apps, but 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**.

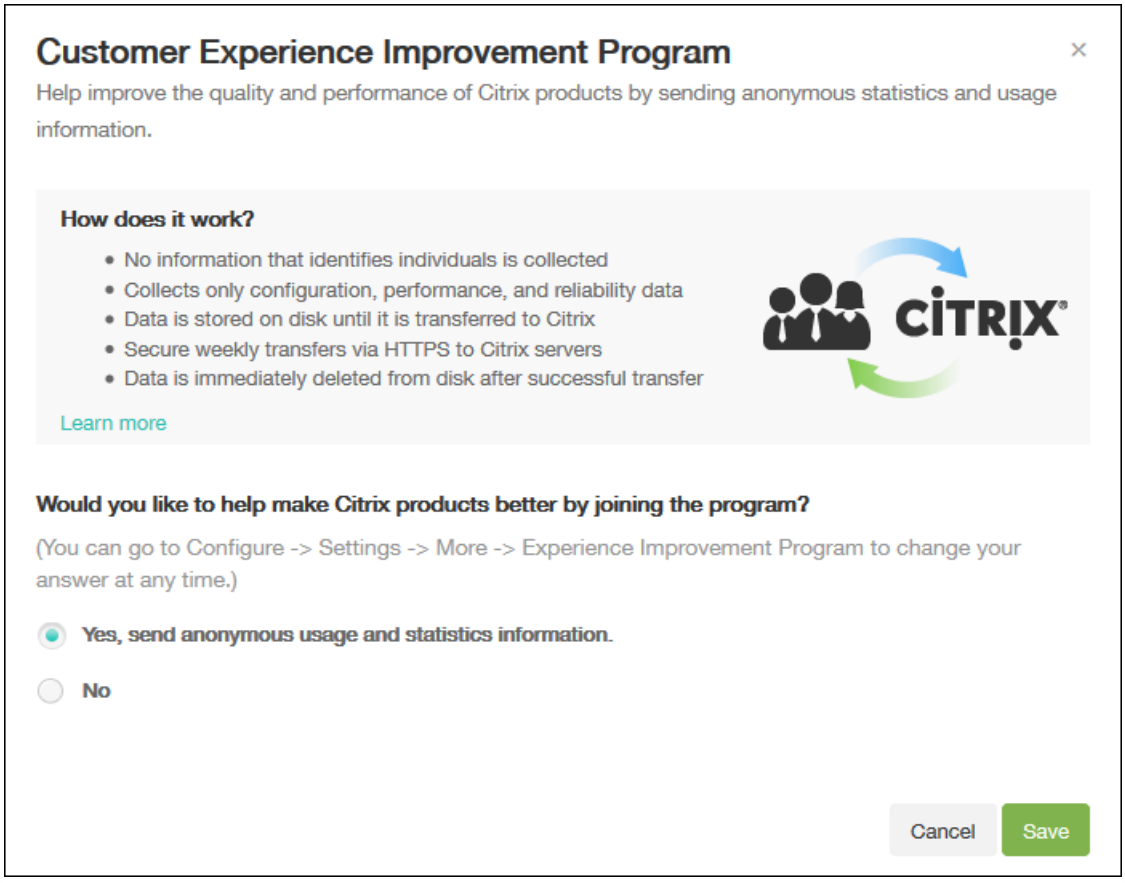
Customer Experience Improvement Program

Jul 16, 2015

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).

CEIP when installing or updating XenMobile

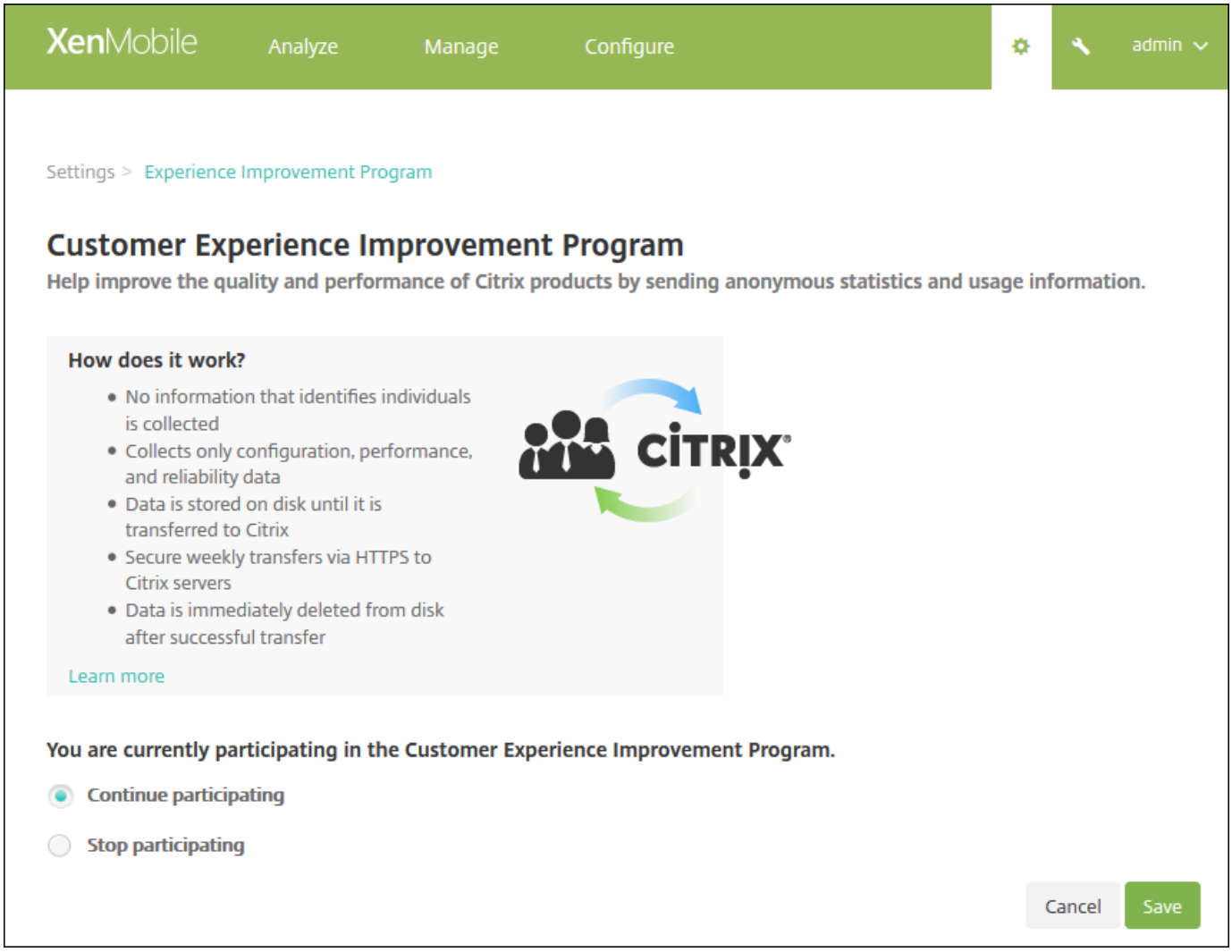
The first time you install XenMobile or when you do an update, you see the following dialog box, in which you select whether to participate and then click **Save**.



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**.

Microsoft Azure settings

Jan 06, 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.

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/

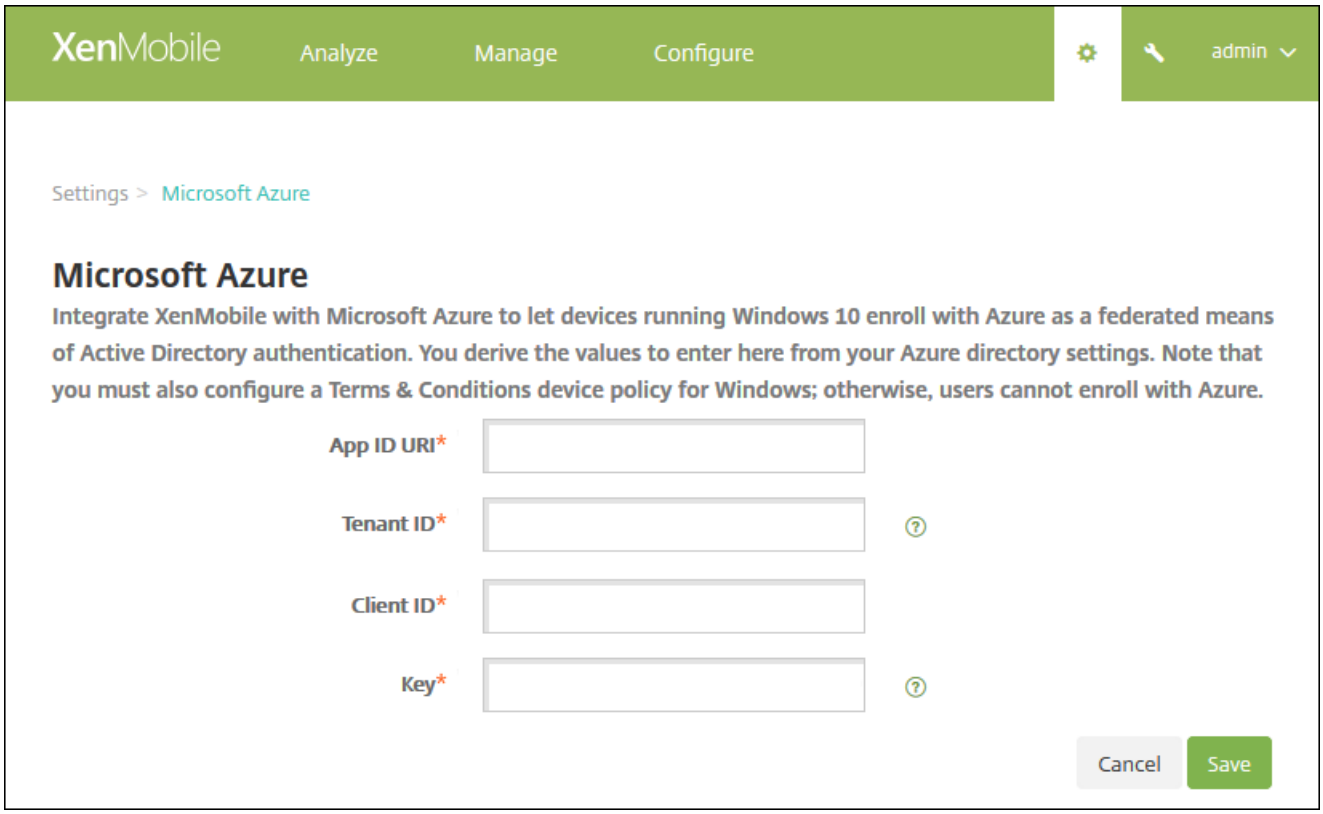
5. Select the on-premise MDM application that you created in step 3 and enable the **Manage devices for these users** option to enable MDM management for all users or any specific user group.

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 **Server**, 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 Worx 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.

Note: Starting with version 10.4, the Worx Store is renamed XenMobile Store.

Google Cloud Messaging

Jan 04, 2017

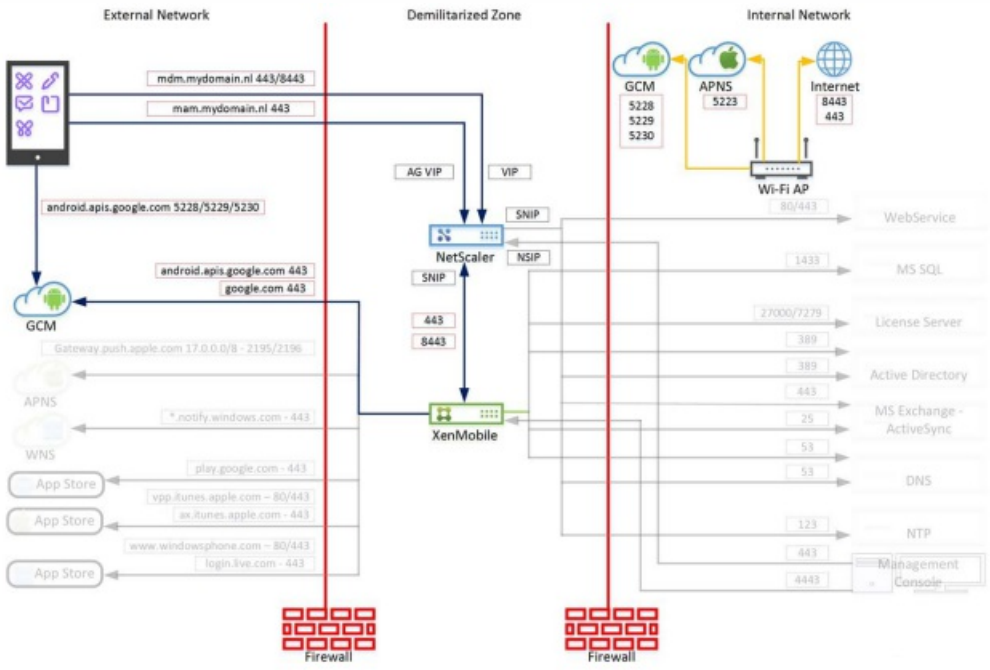
As an alternative to the MDX policy, **Active poll period**, you can use Google Cloud Messaging (GCM) to control how and when Android devices need to connect to XenMobile. With the configuration described in this article, any security action or deploy command triggers a push notification to Secure Hub to prompt the user to reconnect to the XenMobile server. (**Note**: Prior to version 10.4, Secure Hub was named Worx Home.)

Prerequisites

- XenMobile 10.3.x
- Latest Secure Hub client
- Google developer account credentials
- Open port 443 on XenMobile to Android.apis.google.com and Google.com

Architecture

This diagram shows the communication flow for GCM in the external and internal network.

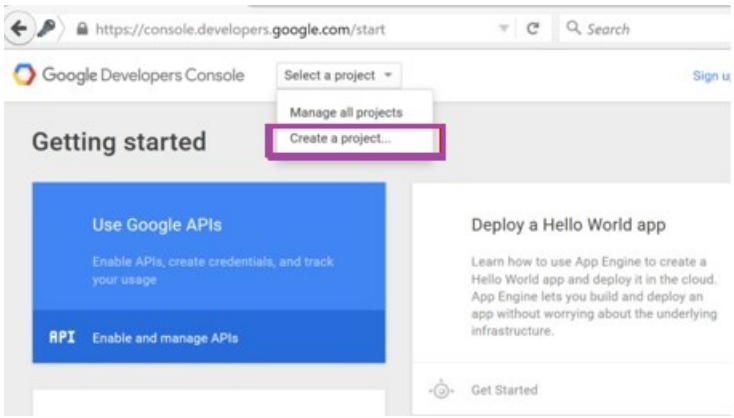


To configure your Google account for GCM

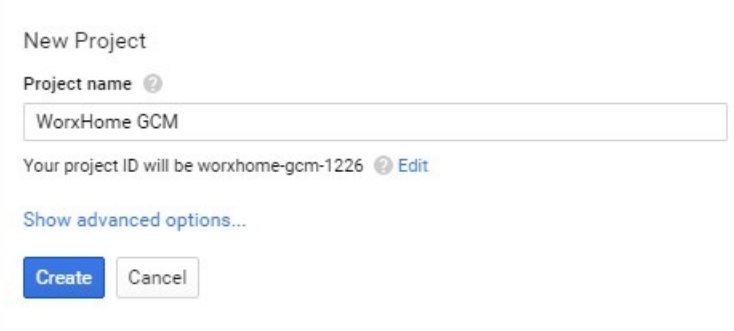
1. Log on to the following URL using your Google developer account credentials:

   https://console.developers.google.com

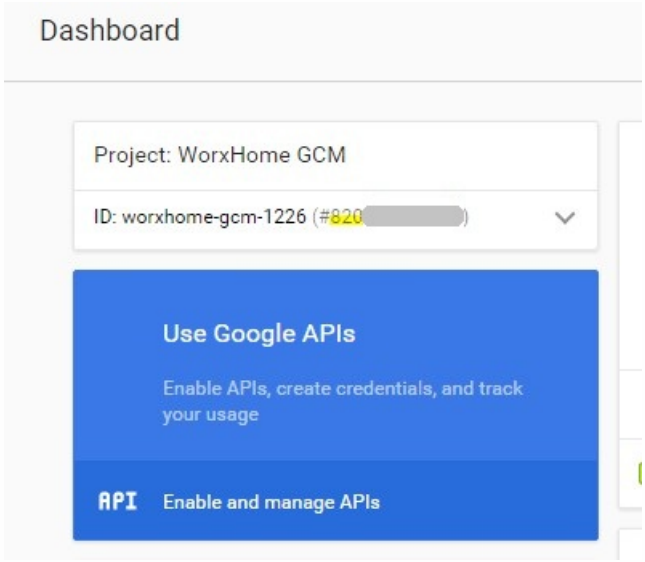
2. From **Select a project**, choose **Create a project**.



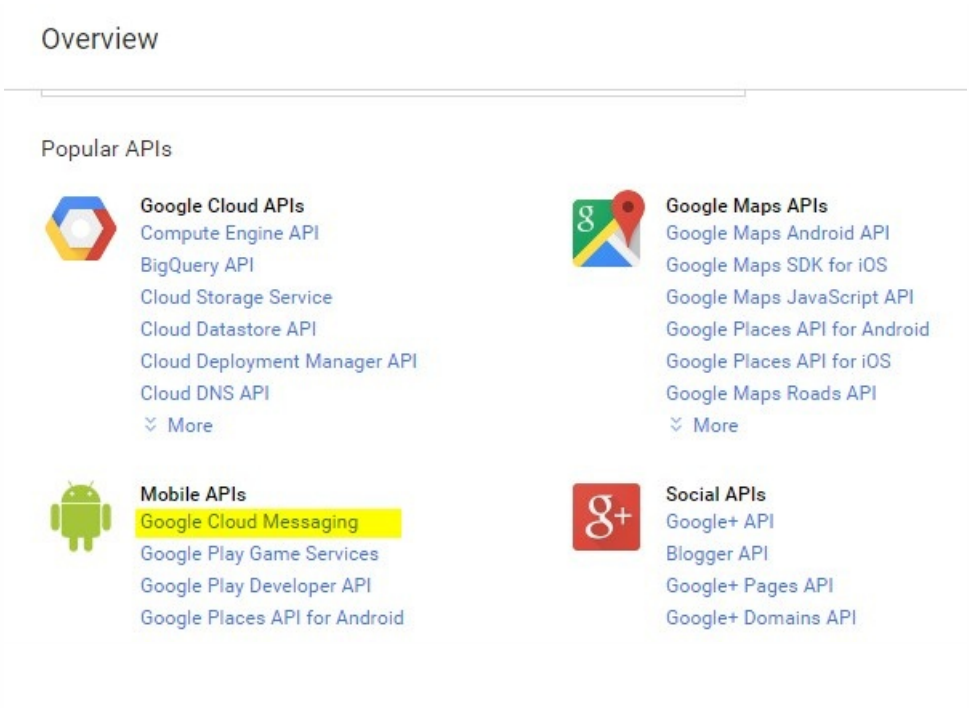
3. Enter a **Project name** and then click **Create**.



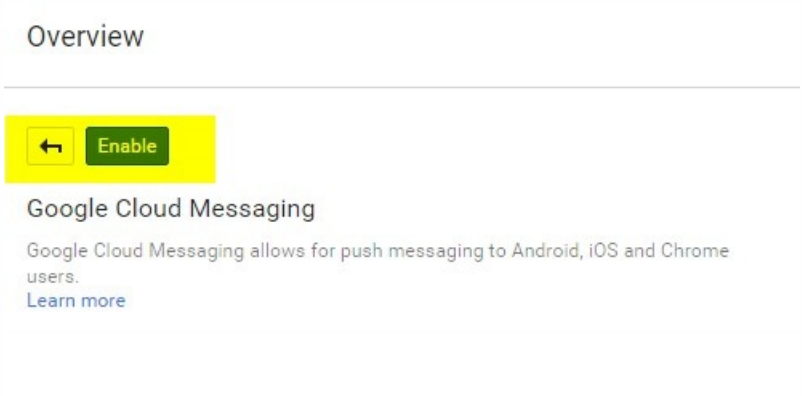
4. In the Dashboard, your Sender ID (highlighted below) is shown next to your Project ID. Record your Sender ID; you must enter it later in XenMobile server settings. Click **Use Google APIs**.



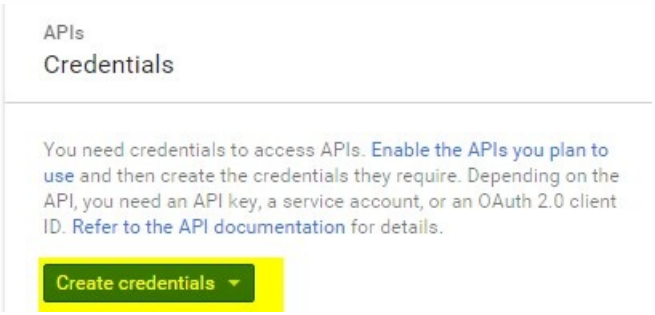
5. In the **Mobile APIs** section, click **Google Cloud Messaging**.



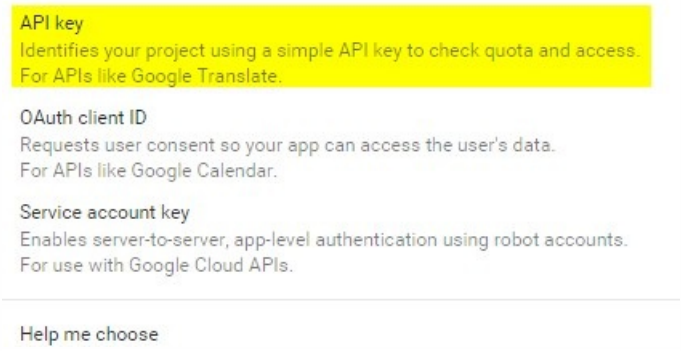
6. Click **Enable**.



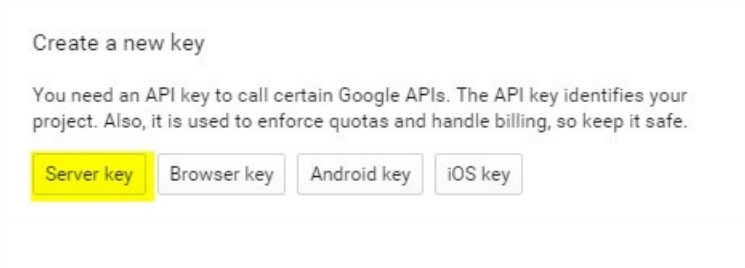
7. Under **Credentials**, click **Create credentials**.



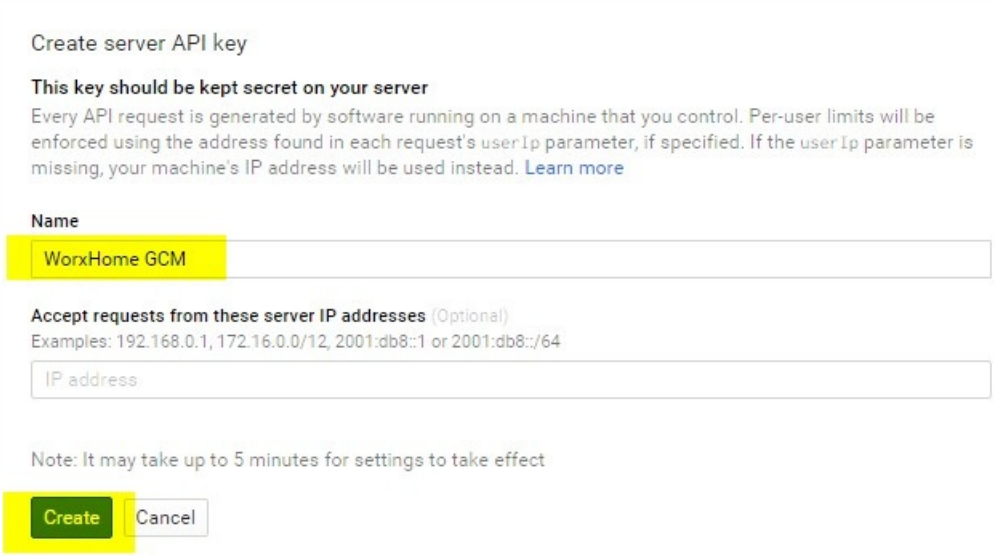
8. Click **API key**.



9. Under **Create a new key**, click **Server key**.



10. In **Create server API key**, enter a **Name** (in the example, we used the project name) and then click **Create**.



11. Record the API key. You will need it to configure XenMobile.

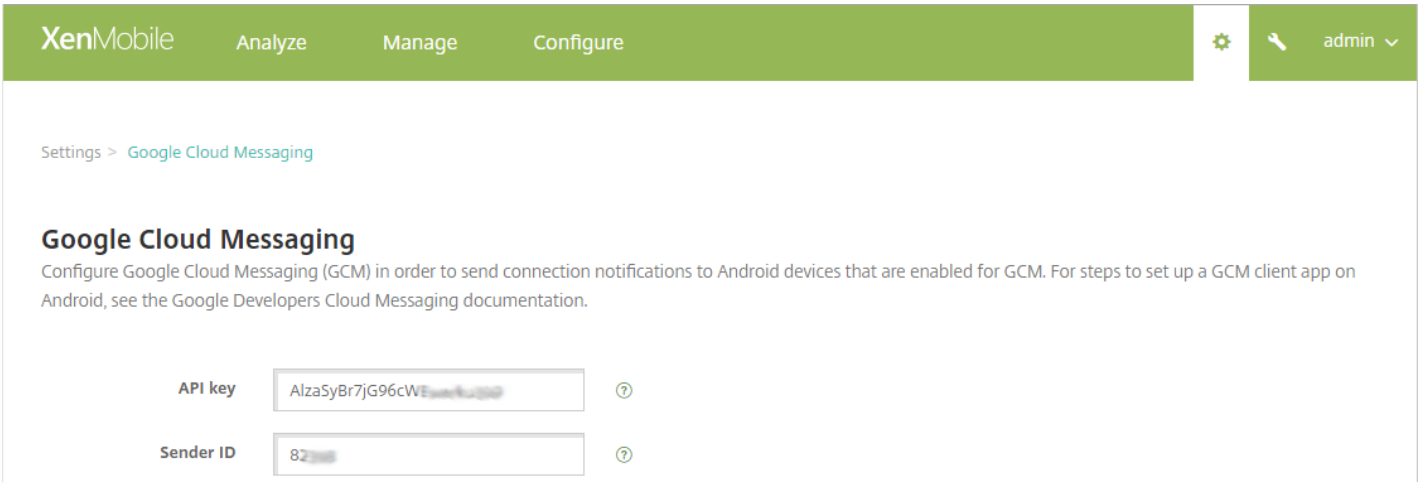
To configure XenMobile for GCM

1. Log on to XenMobile admin console and then click **Settings > Google Cloud Messaging**.

    a. In **API key**, enter the GCM API key that you copied in the last step of GCM configuration.

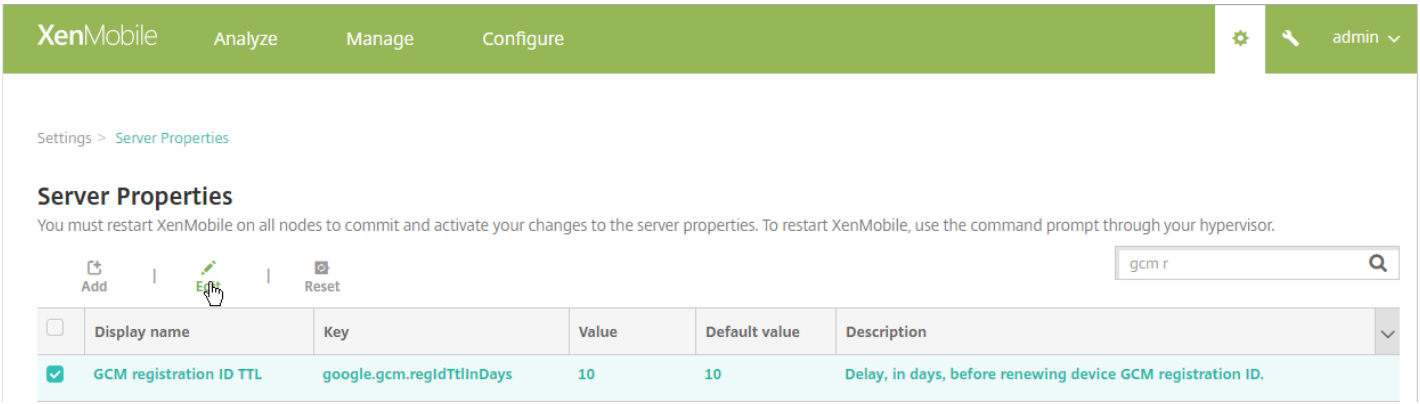
    b. In **Sender ID**, copy the Sender ID value you noted in the previous procedure and then click **Save**.

    Note: The page **Settings > Google Cloud Messaging** is new for XenMobile 10.3.6. If you aren't using the latest XenMobile release, go to **Settings > Server** to update the **API key** (google.gcm.apiKey) and **Sender ID** (google.gcm.senderid).

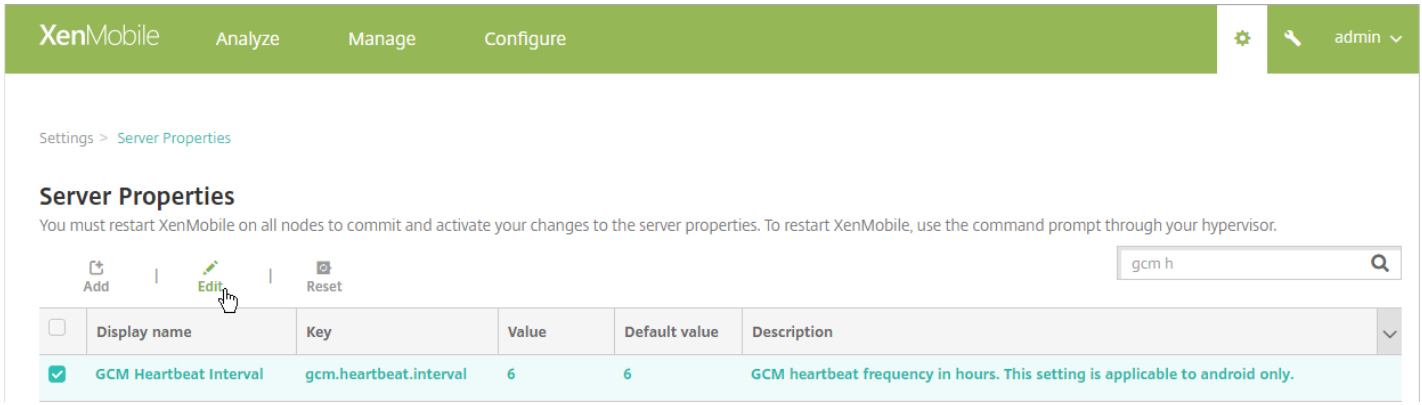


2. If you need to change the default settings for either of the following properties, click **Settings > Server Properties**.

- **GCM Registration ID TTL:** The default delay before renewing the device GCM registration ID is **10** days. To change that value, enter **gcm r** in the search box, click **GCM Registration ID TTL**, and then click **Edit**.



- **GCM Heartbeat Interval:** The default frequency that XenMobile communicates with the GCM server is **6** hours. To change that value, enter **gcm h** in the search box, click **GCM Heartbeat Interval** and then click **Edit**.

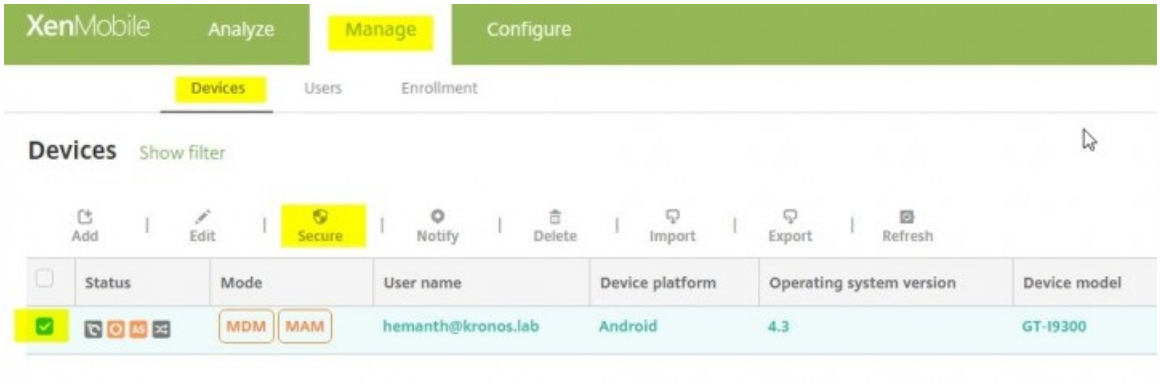


To test your configuration

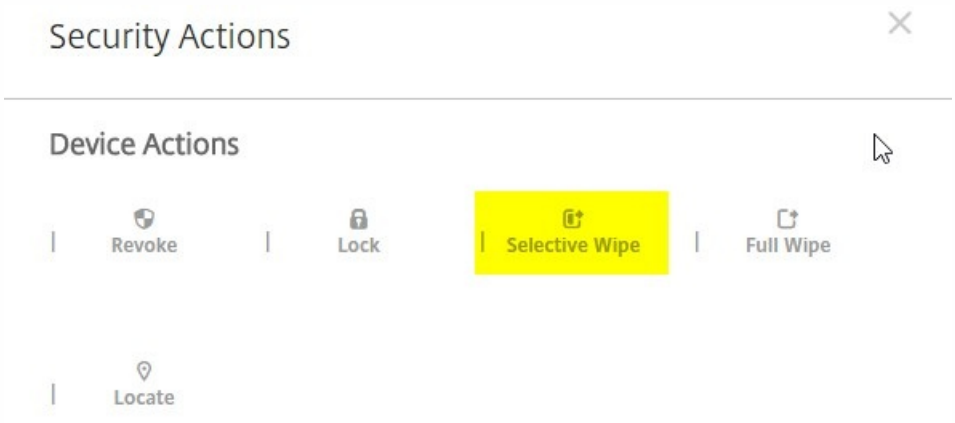
1. Enroll an Android device.

2. Leave the device idle for some time, so that it disconnects from XenMobile server.

3. Log on to the XenMobile admin console, click **Manage**, select the Android device, and then click **Secure**.



4. Under **Device Actions**, click **Selective Wipe**.



In a succcessful configuration, Selective Wipe occurs on the device without reconnecting to XenMobile.

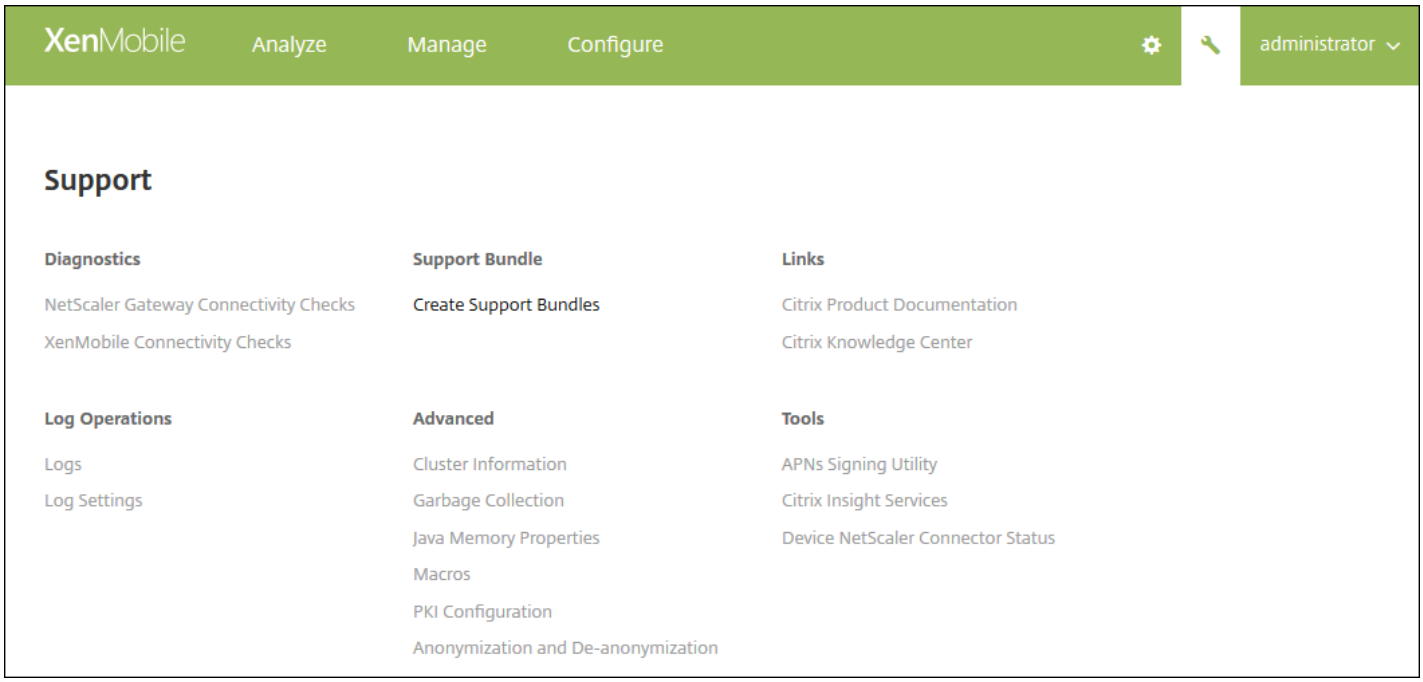
XenMobile Support and Maintenance

Jun 01, 2016

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 XenMobile 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.

Conducting Connectivity Checks

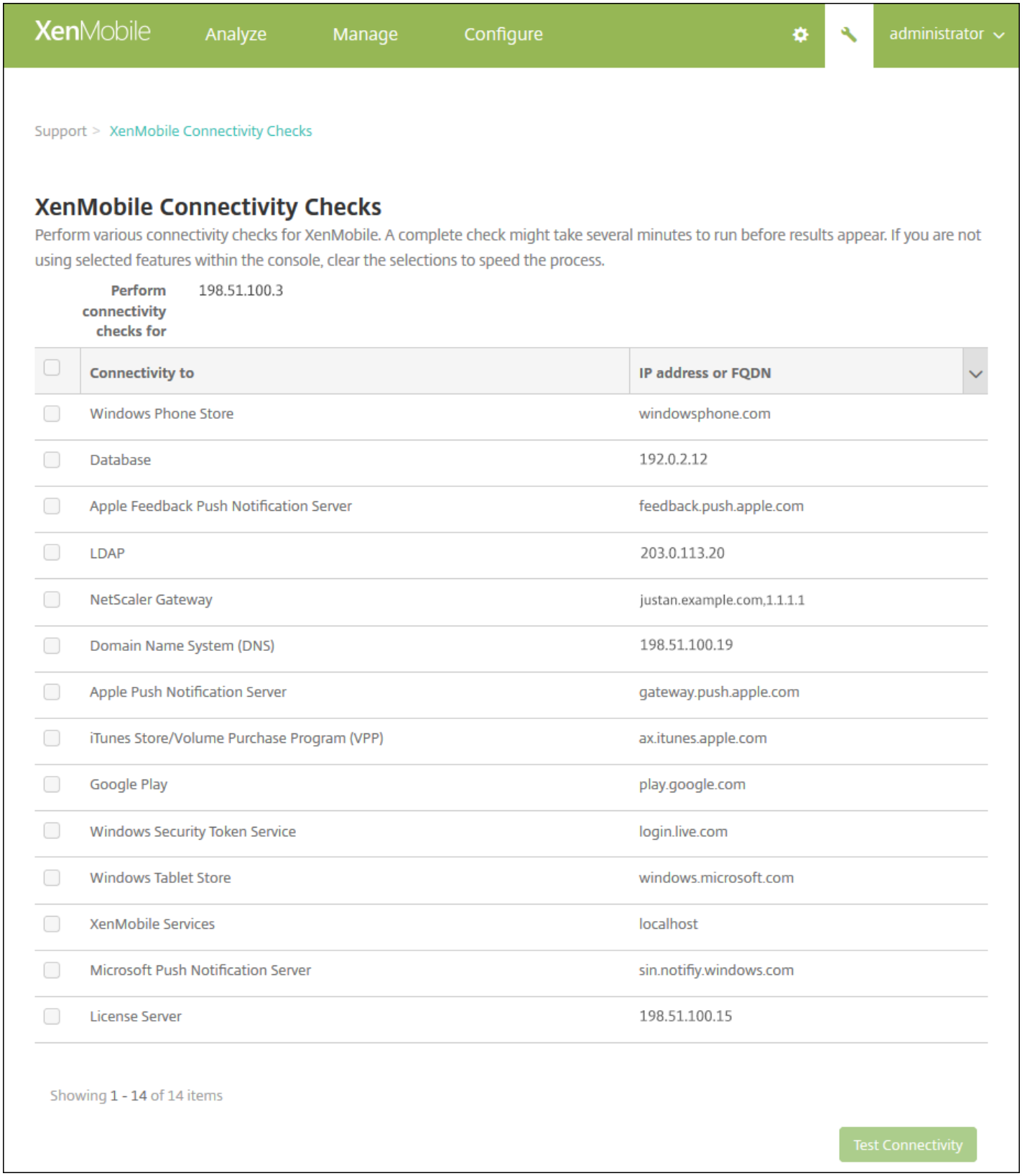
Feb 13, 2015

From the XenMobile **Support** page, you can check the XenMobile connection to NetScaler Gateway and other servers and locations.

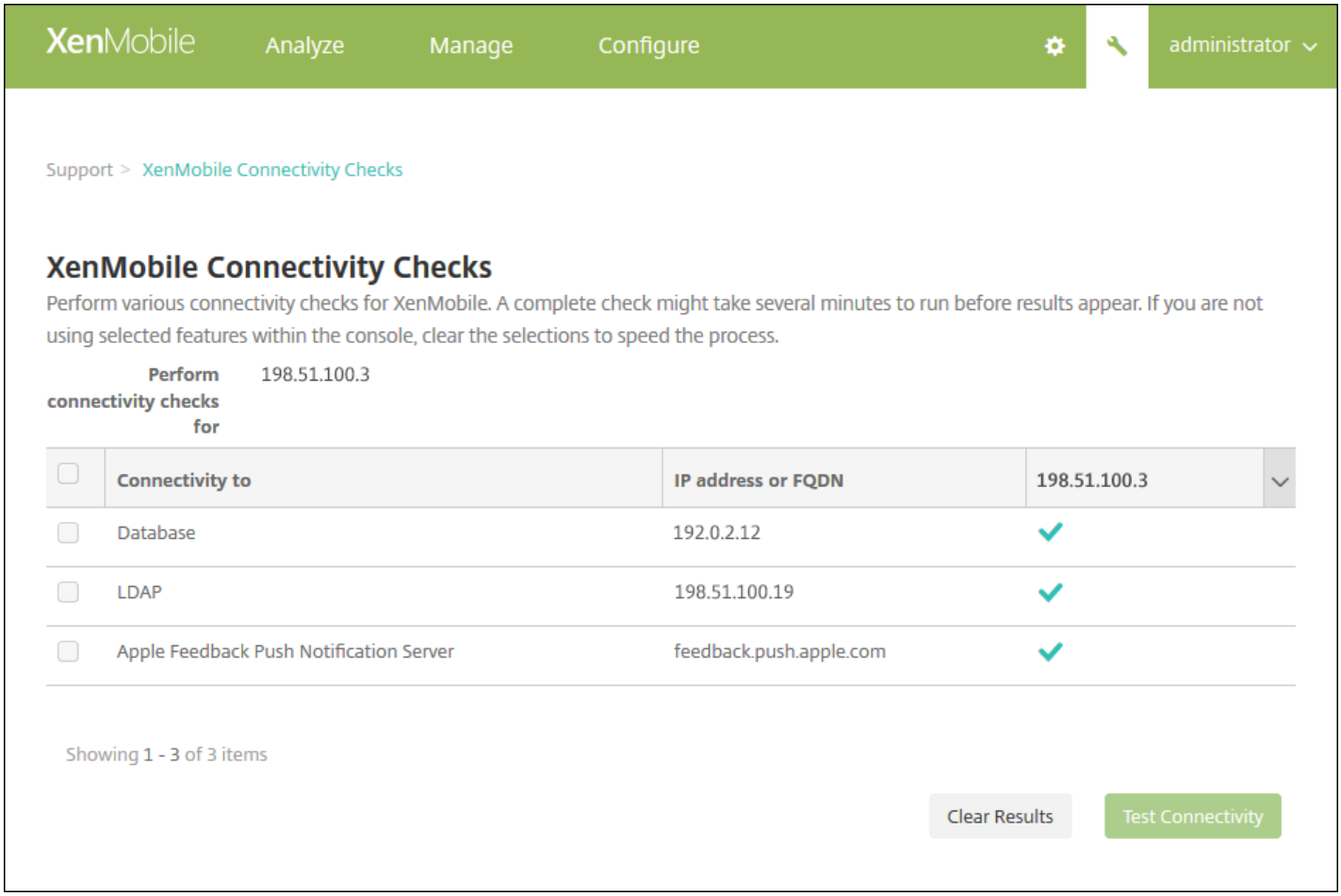
Conducting XenMobile Connectivity Checks

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

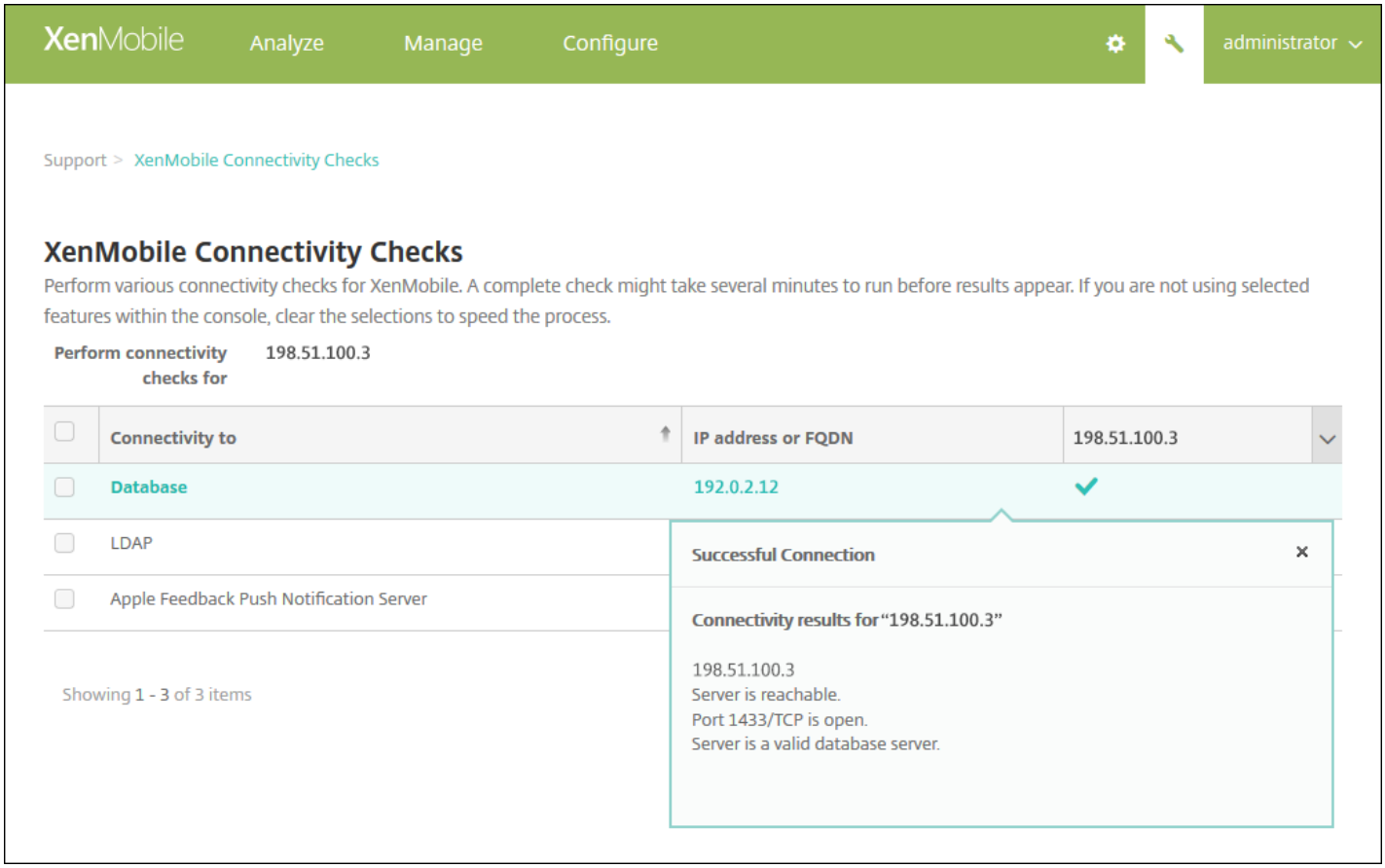
2. Under **Diagnostics**, click **XenMobile Connectivity Checks**. The **XenMobile Connectivity Checks** page appears. If your XenMobile environment contains clustered nodes, all nodes are shown.



2. Select the servers you want to include in the connectivity test and then click **Test Connectivity**. The test results page appears.

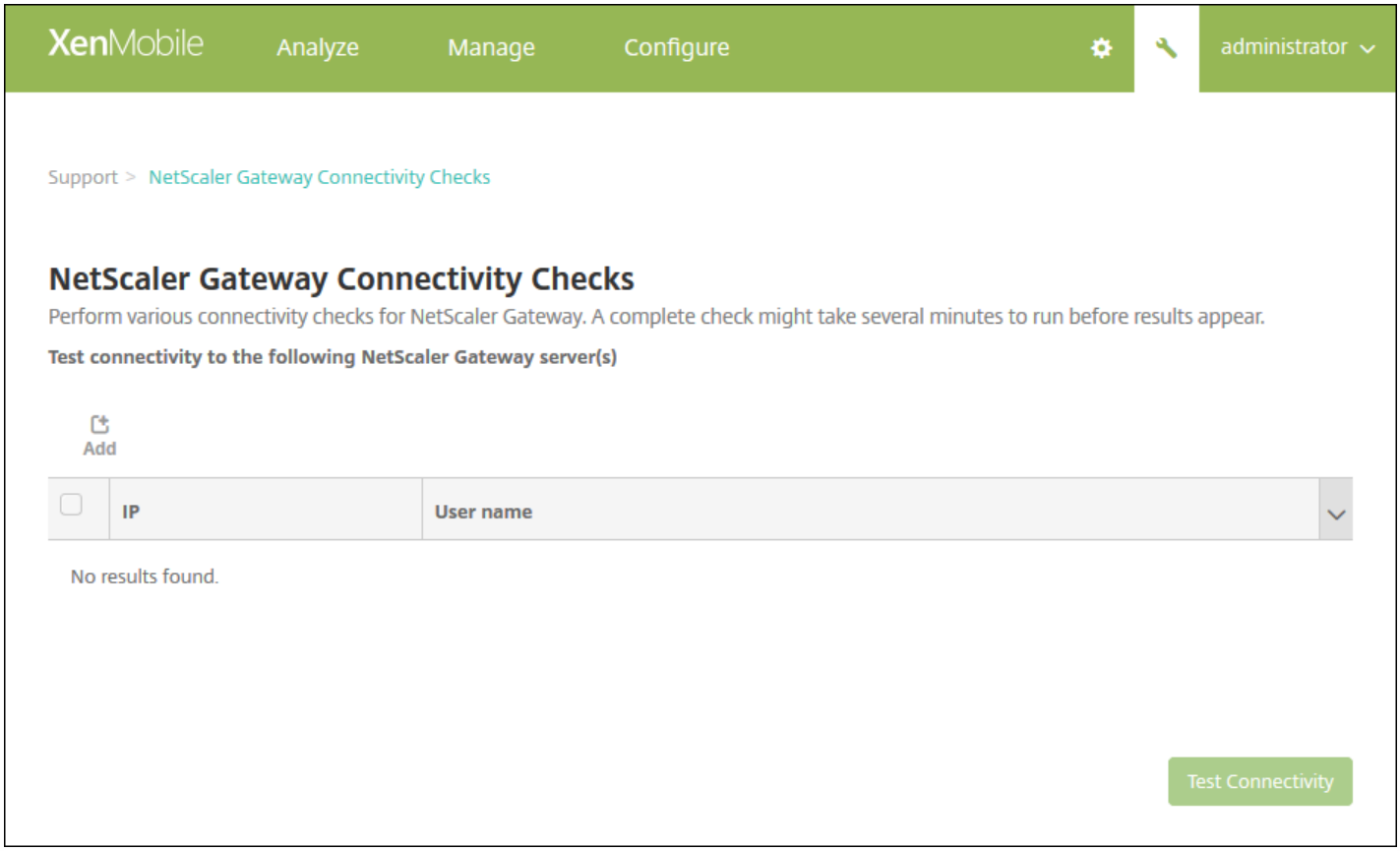


3. Select a server in the test results table to see detailed results for that server.

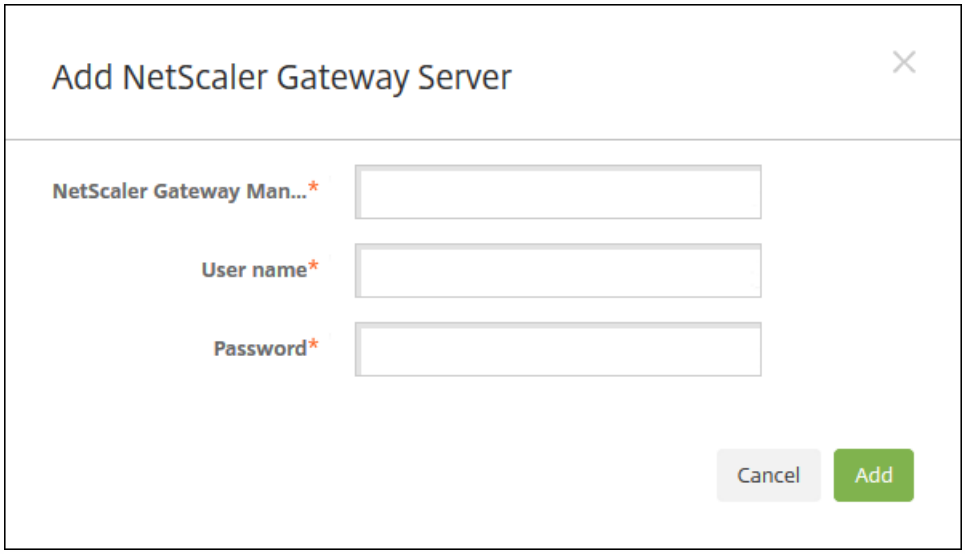


Conducting NetScaler Gateway Connectivity Checks

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 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 is already added, 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 is already added, the user name is provided.

5. Click **Add**. The NetScaler Gateway is added to the table on the **NetScaler Gateway Connectivity Checks** page.

6. 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.

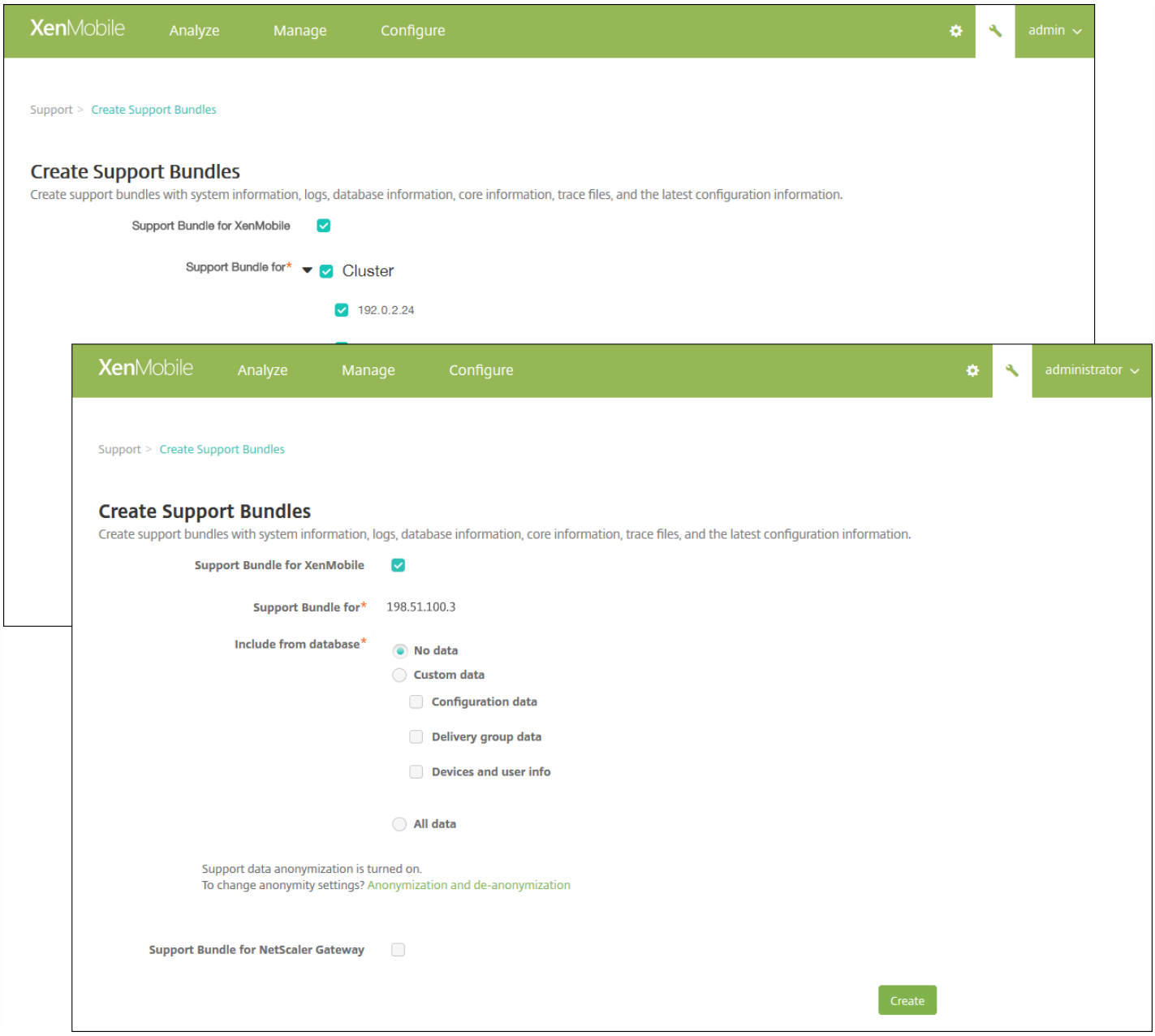
Creating Support Bundles in XenMobile

Feb 16, 2015

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.



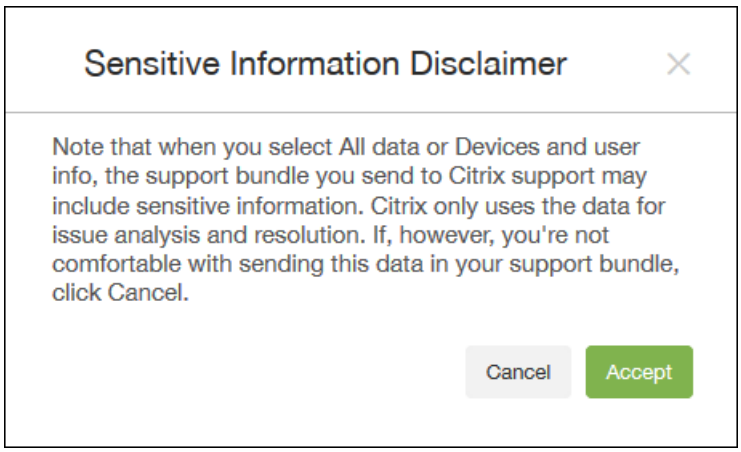
3. Make sure that the **Support Bundle for XenMobile** check box is selected.

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:
  - **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**.

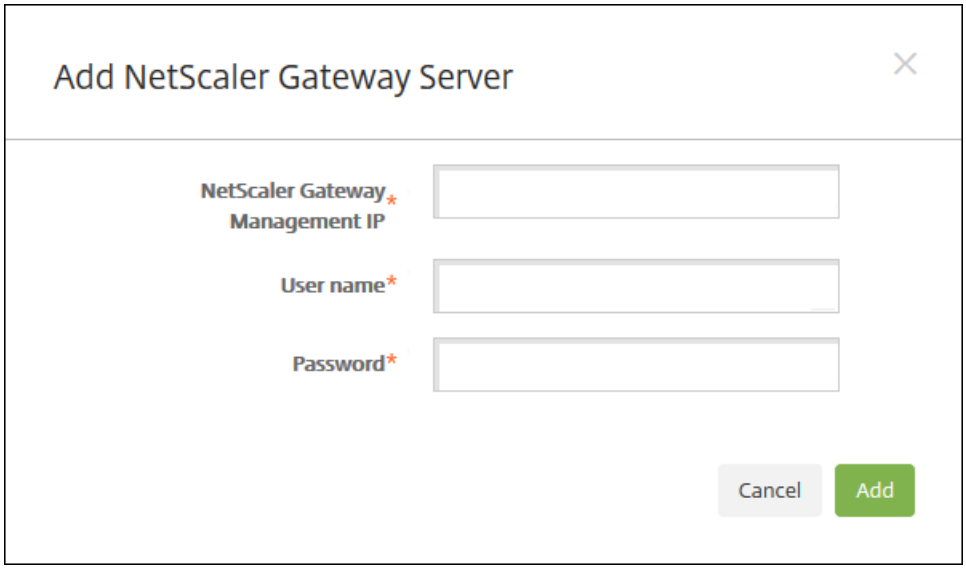
Note: If you choose **Devices and user info** or **All data**, and this is the first support bundle you have created, the **Sensitive Information Disclaimer** dialog box appears. Read the disclaimer and then click **Accept** or **Cancel**. If you click **Cancel**, the support bundle cannot be uploaded 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. Below **Include from database**, is a notice about whether sensitive user, server, and network data is made anonymous in support bundles. The default setting is to anonymize the data. You can change this setting by clicking the **Anonymization and de-anonymization** link. See Anonymizing data in support bundles for more information about data anonymization.

6. Select **Support Bundle for NetScaler Gateway** if you want to include support bundles from NetScaler Gateway and then do the following:

- Click **Add**. The **Add NetScaler Gateway Server** dialog box appears.



- 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.

- 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.

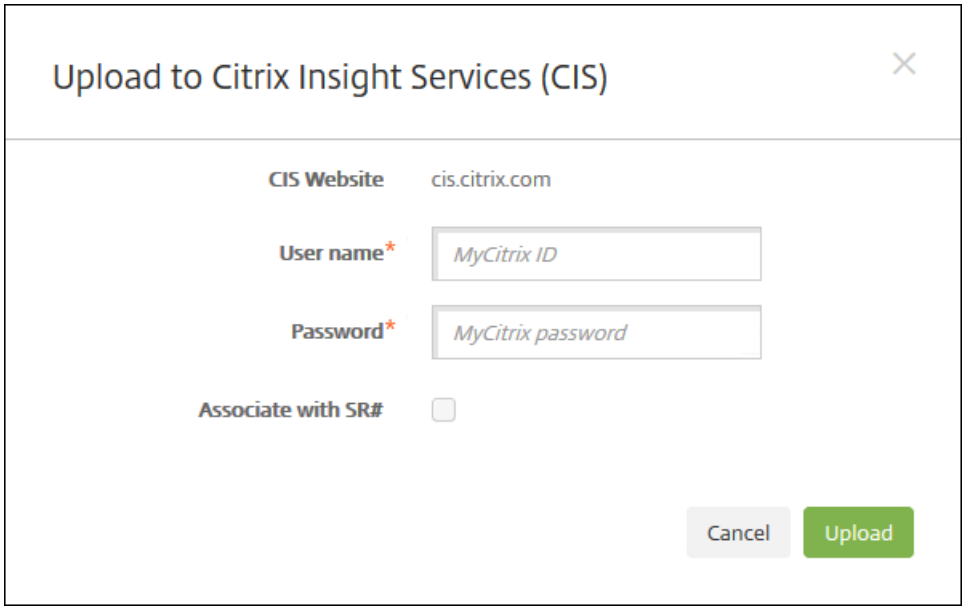
9. Click **Create**. The support bundle is created and two new buttons, **Upload to CIS** and **Download to Client**, appear.

Continue to Uploading Support Bundles to Citrix Insight Services or Downloading Support Bundles to a Client.

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 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.

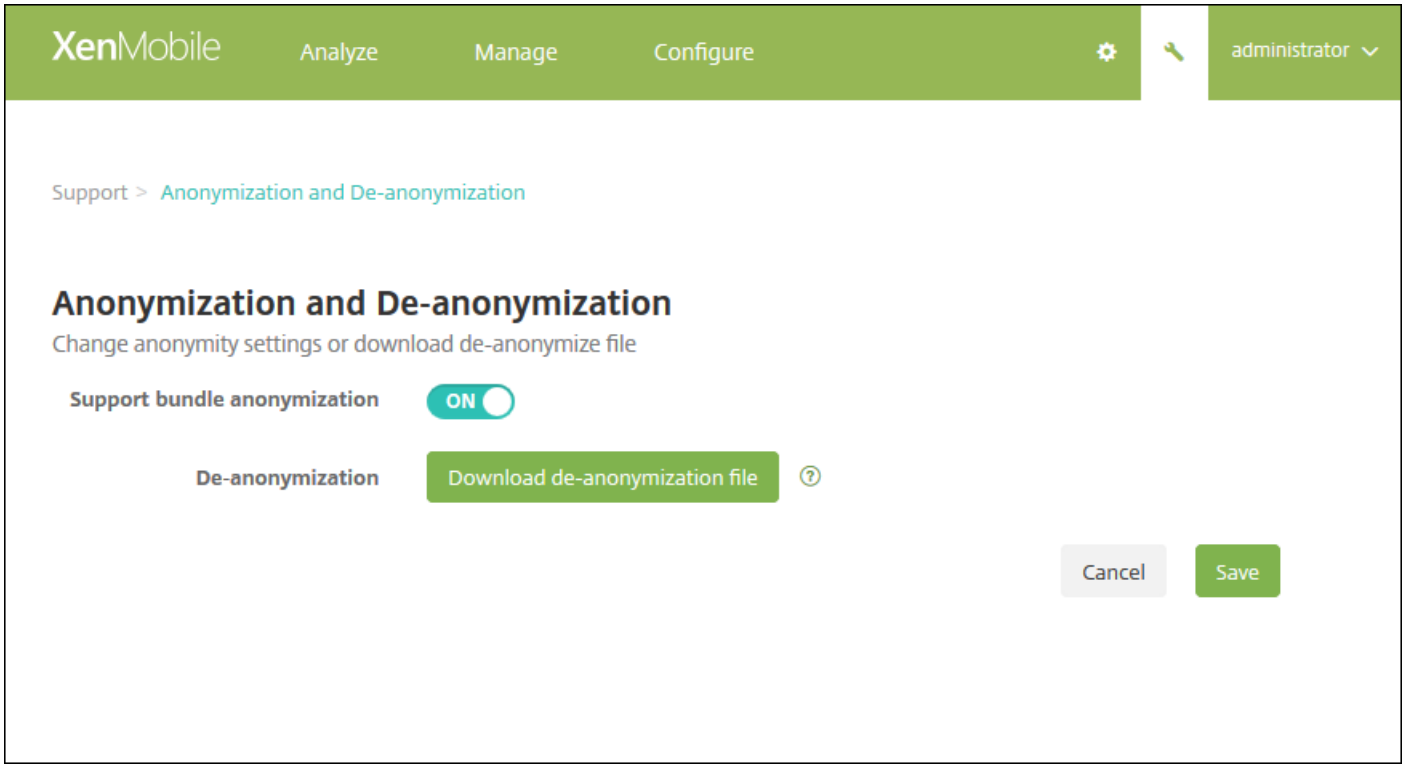
Anonymizing data in support bundles

Nov 16, 2015

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.

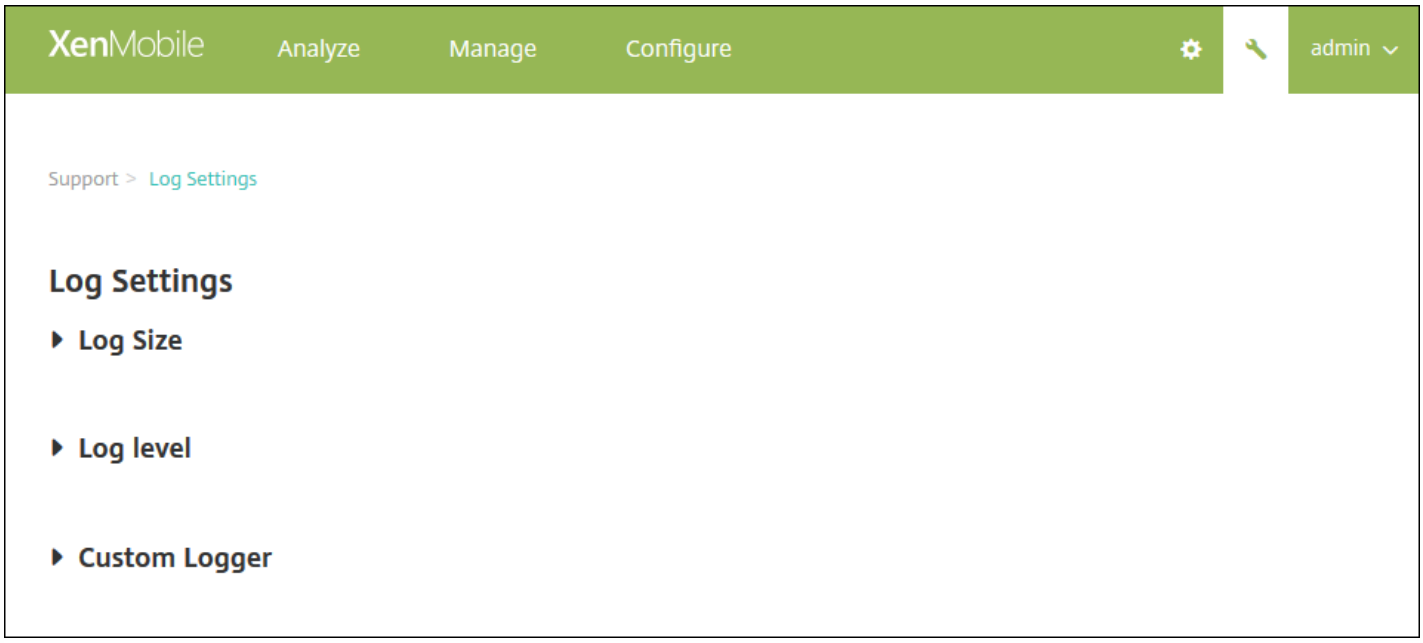
Configuring log settings

Jun 12, 2015

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.

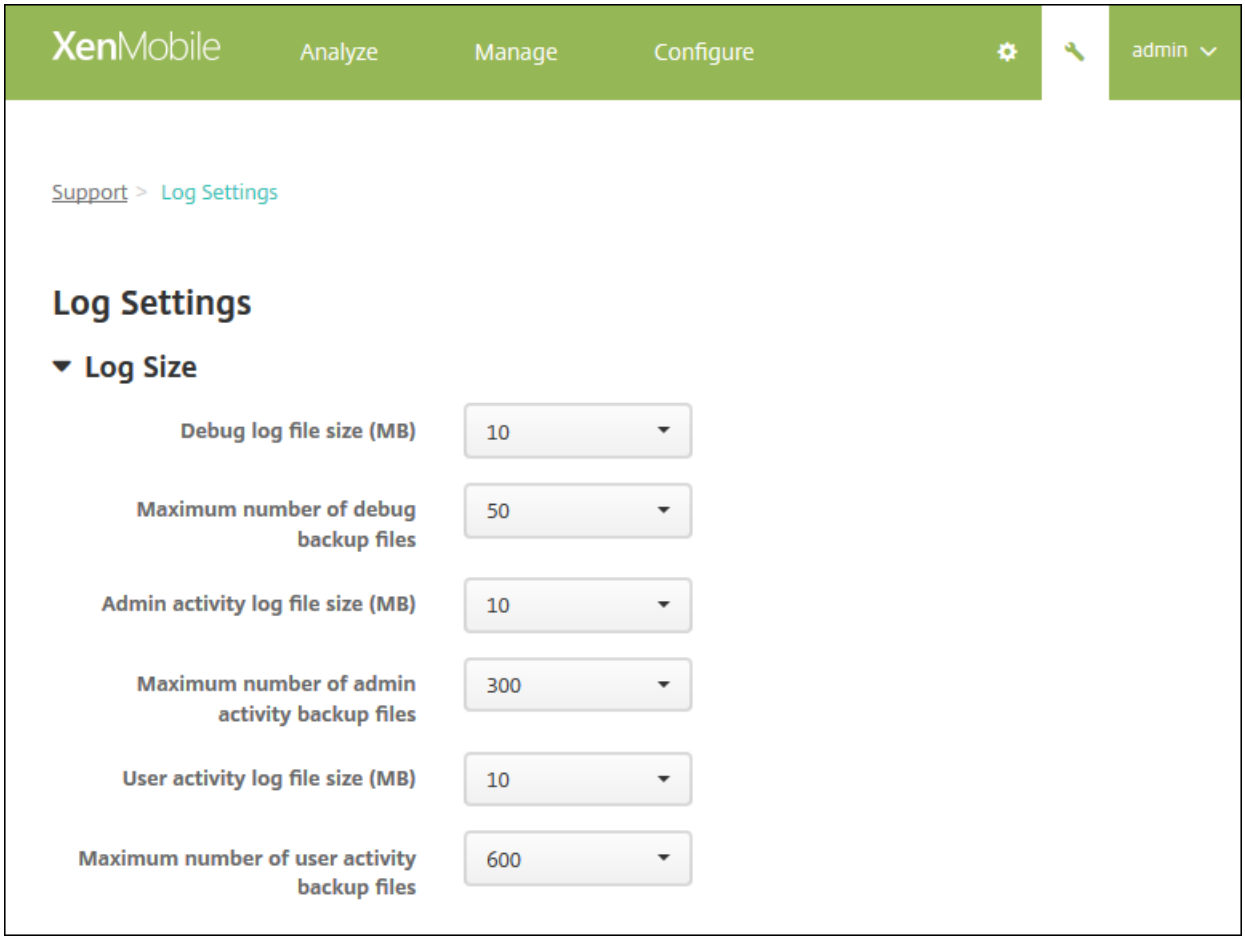


On the **Log Settings** page you can access the following options:

- **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**.



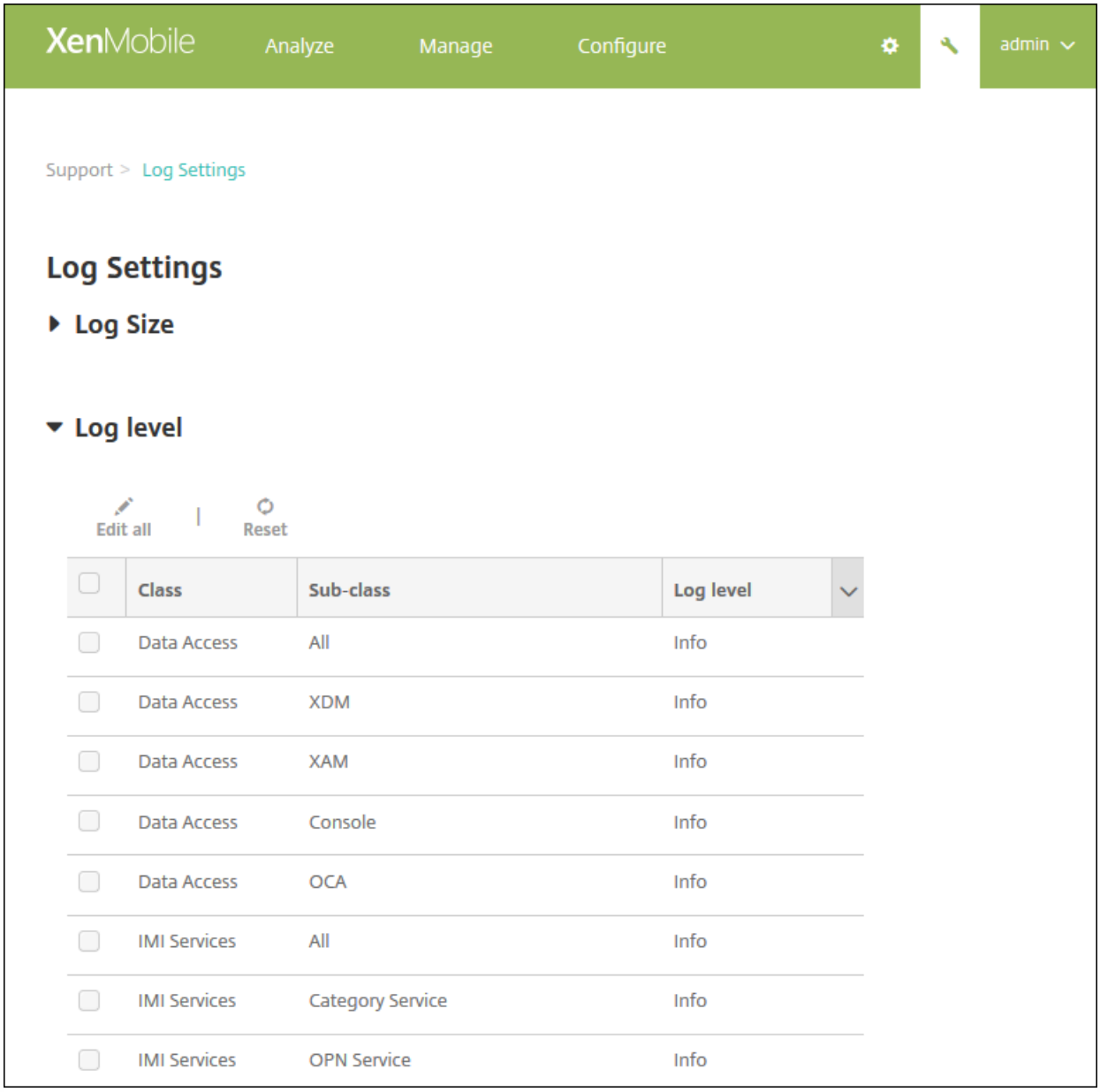
2. Configure these settings:

- **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.

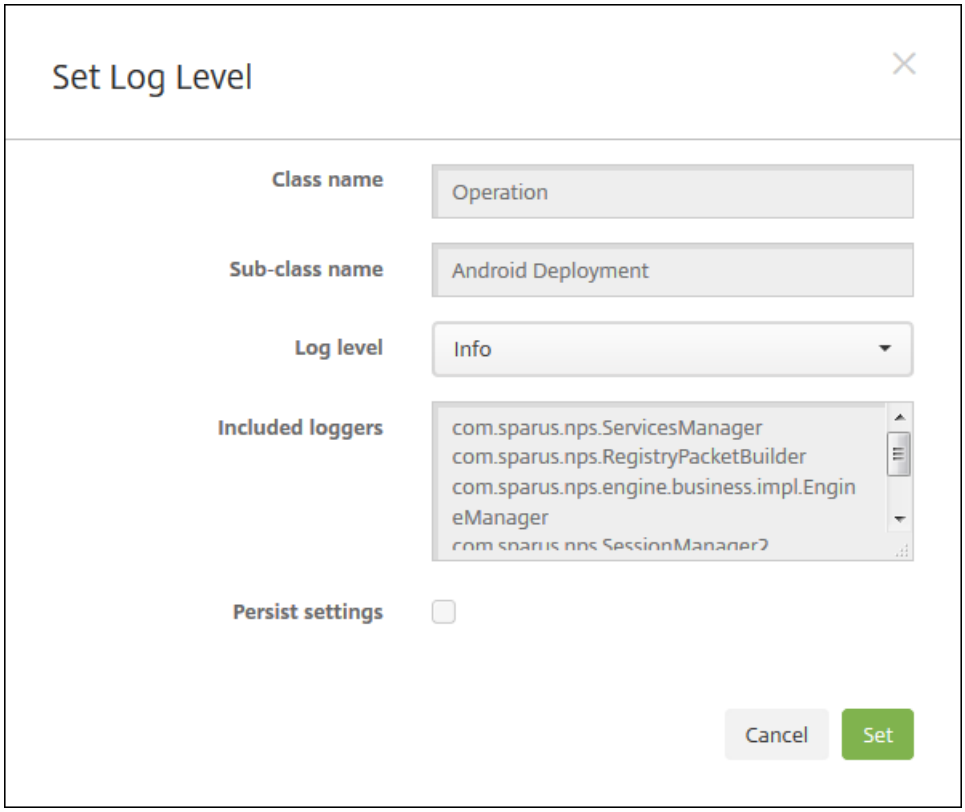
1. On the **Log Settings** page, expand **Log level**. The table of all log classes appears.



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.

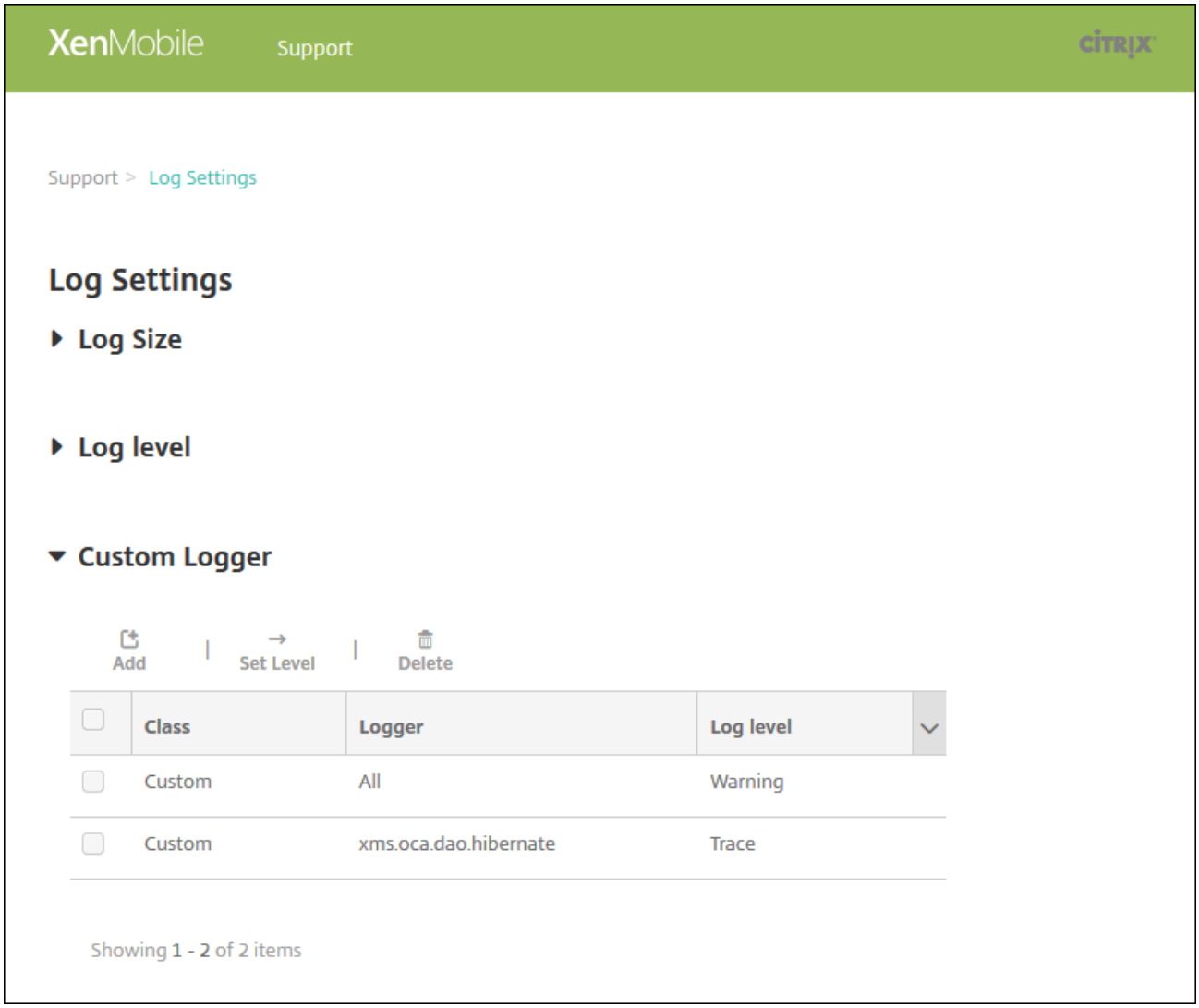


- **Class Name**: This field displays All when you are changing the log level for all classes or it displays the individual class name; it is not editable.
- **Sub-class name**: This field displays All when you are changing the log level for all classes or it displays the individual class sub-class name; 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.

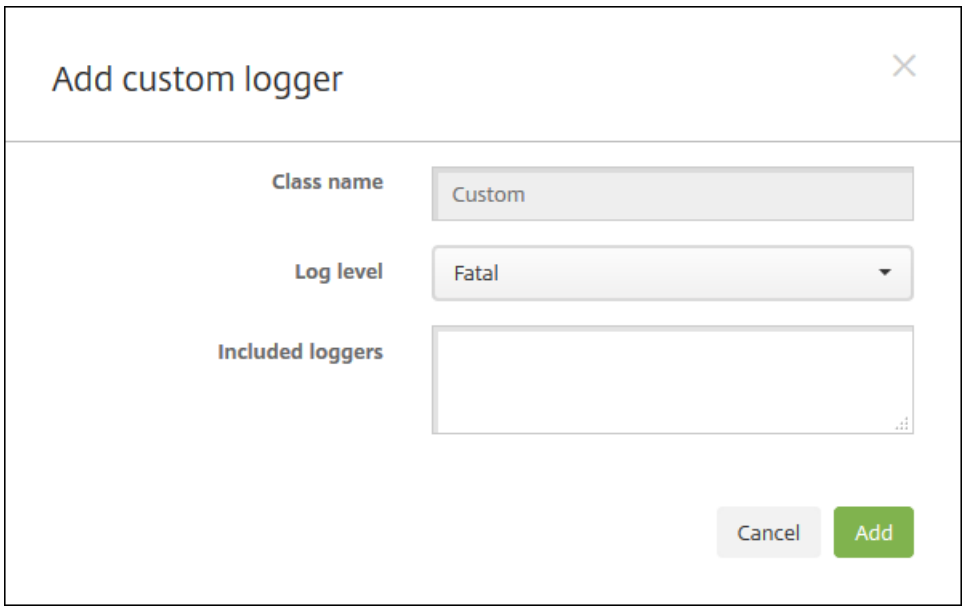
3. Click **Set** to commit your changes.

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.



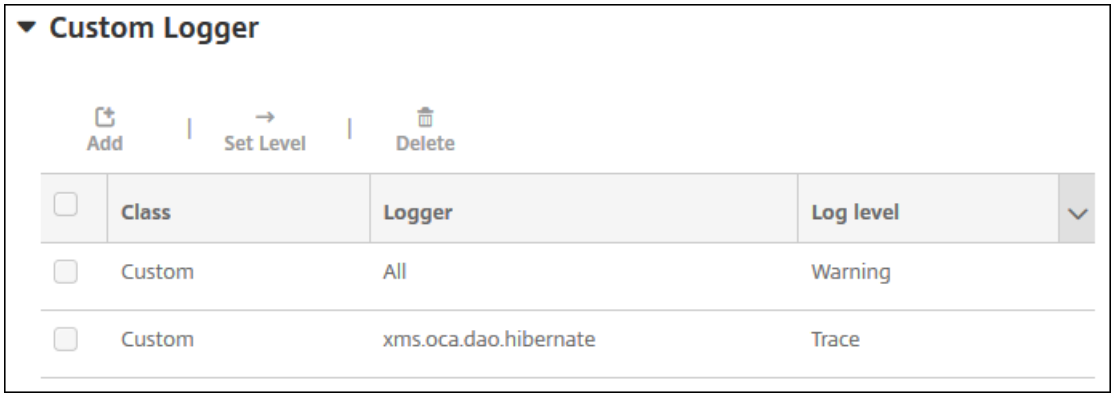
2. Click **Add**. The **Add custom logger** dialog box appears.



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.

2. Click **Delete**. A dialog box appears asking whether you want to delete the custom logger. Click **OK**.

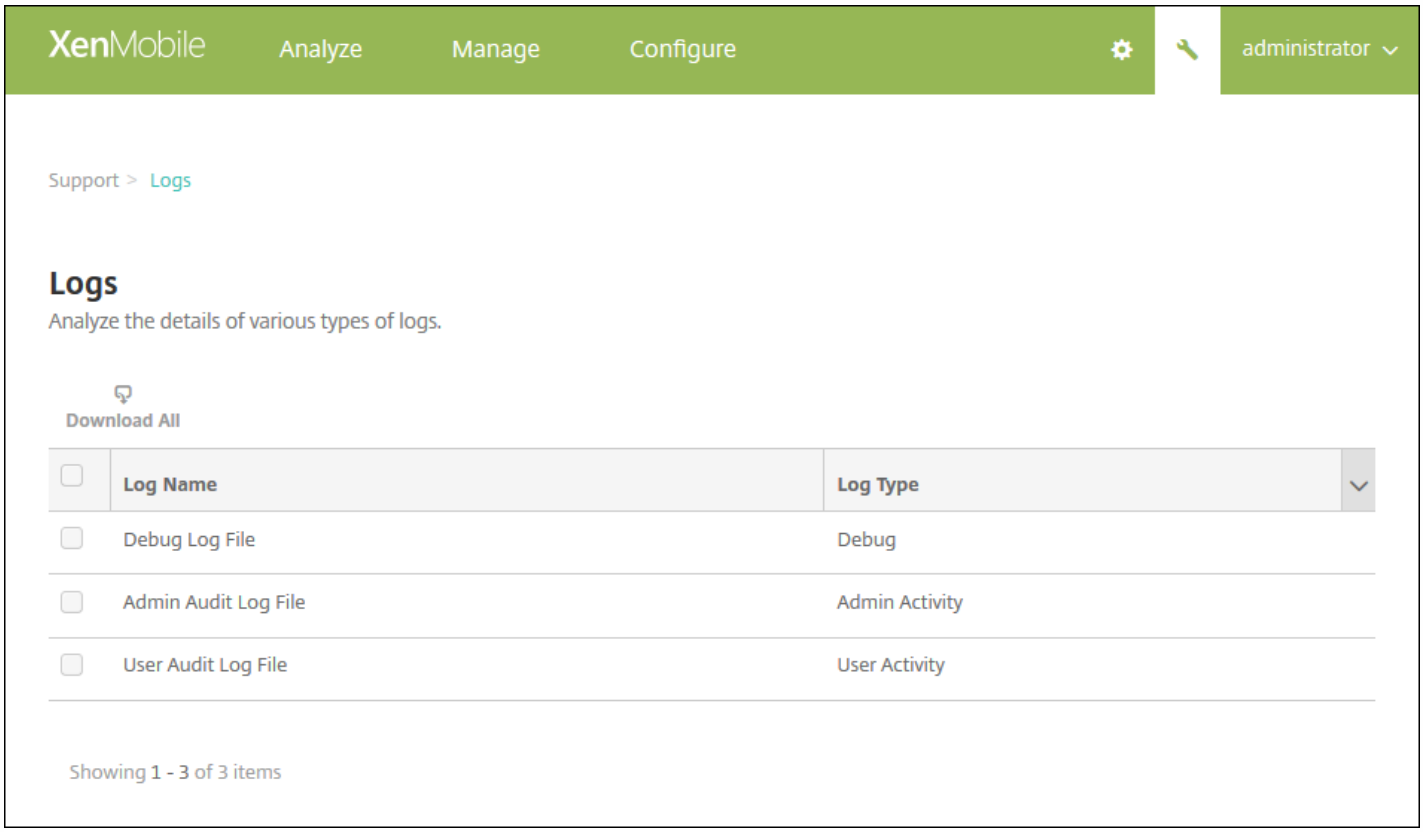
Important: You cannot undo this operation.

Viewing and Analyzing Log Files in XenMobile

May 05, 2015

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.

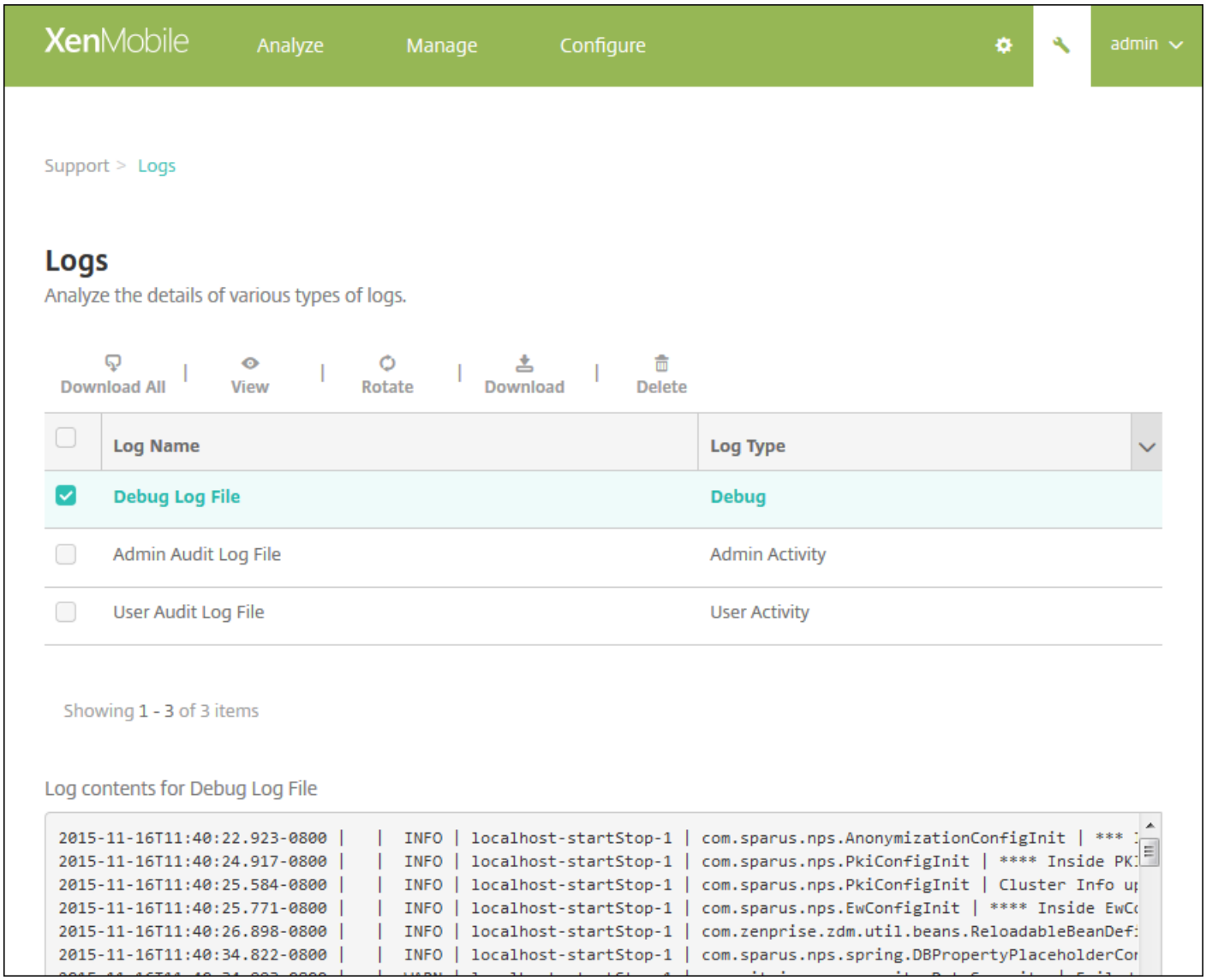
Note:

- If you select more than one log file, only **Download All** and **Delete** 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.



Remote Support

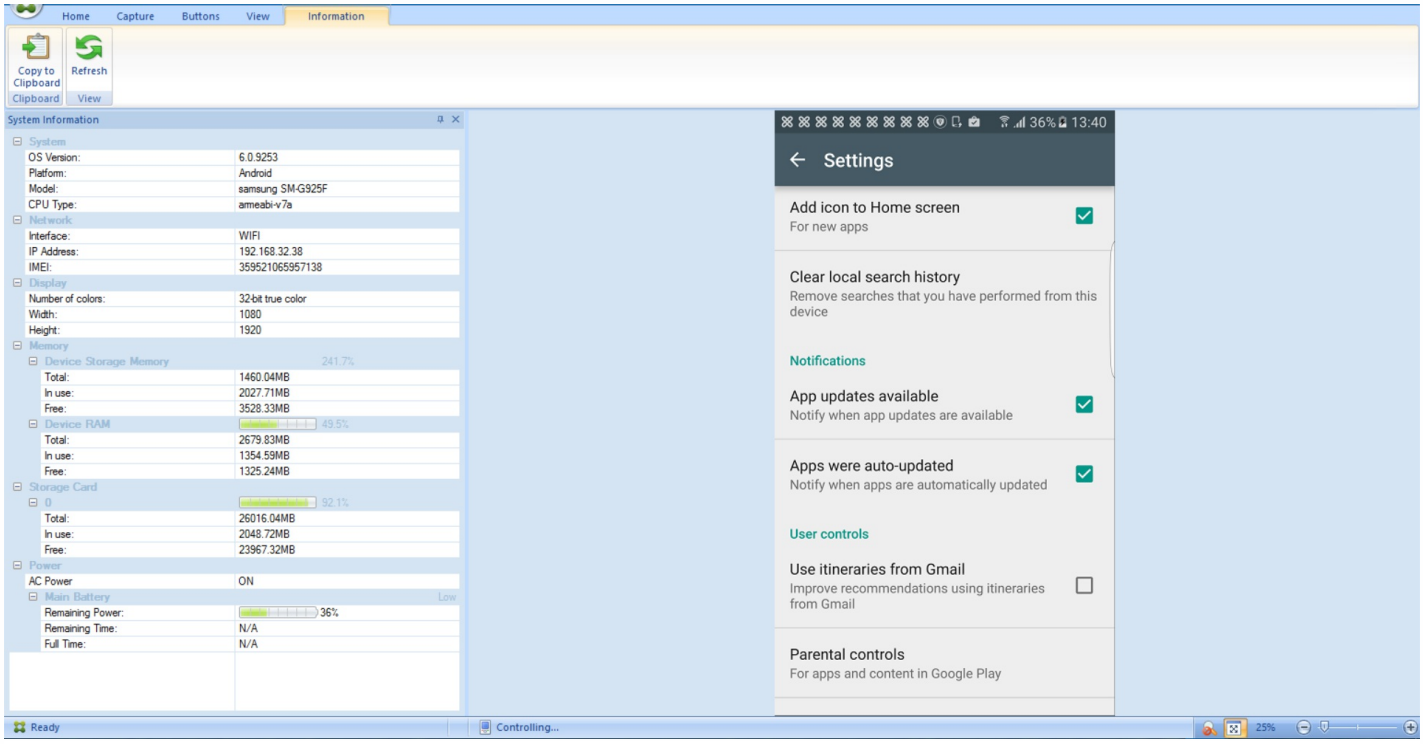
Jun 22, 2016

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. Remote control of iOS devices is not supported.

> ## Note
>
> XenMobile Remote Support is not available in XenMobile Cloud versions 10.x.

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 with a rendering of the controlled device.



With Remote Support, you can:

- Remotely log 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. If a user can't find the device, you can wipe it to ensure your sensitive data is not compromised.

Remote Support also enables support personnel to:

- Display a list of all connected devices within one or more XenMobile servers.
- 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 the XenMobile server.
- Run the device task manager where you can display and 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 between 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 filename is currently 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:

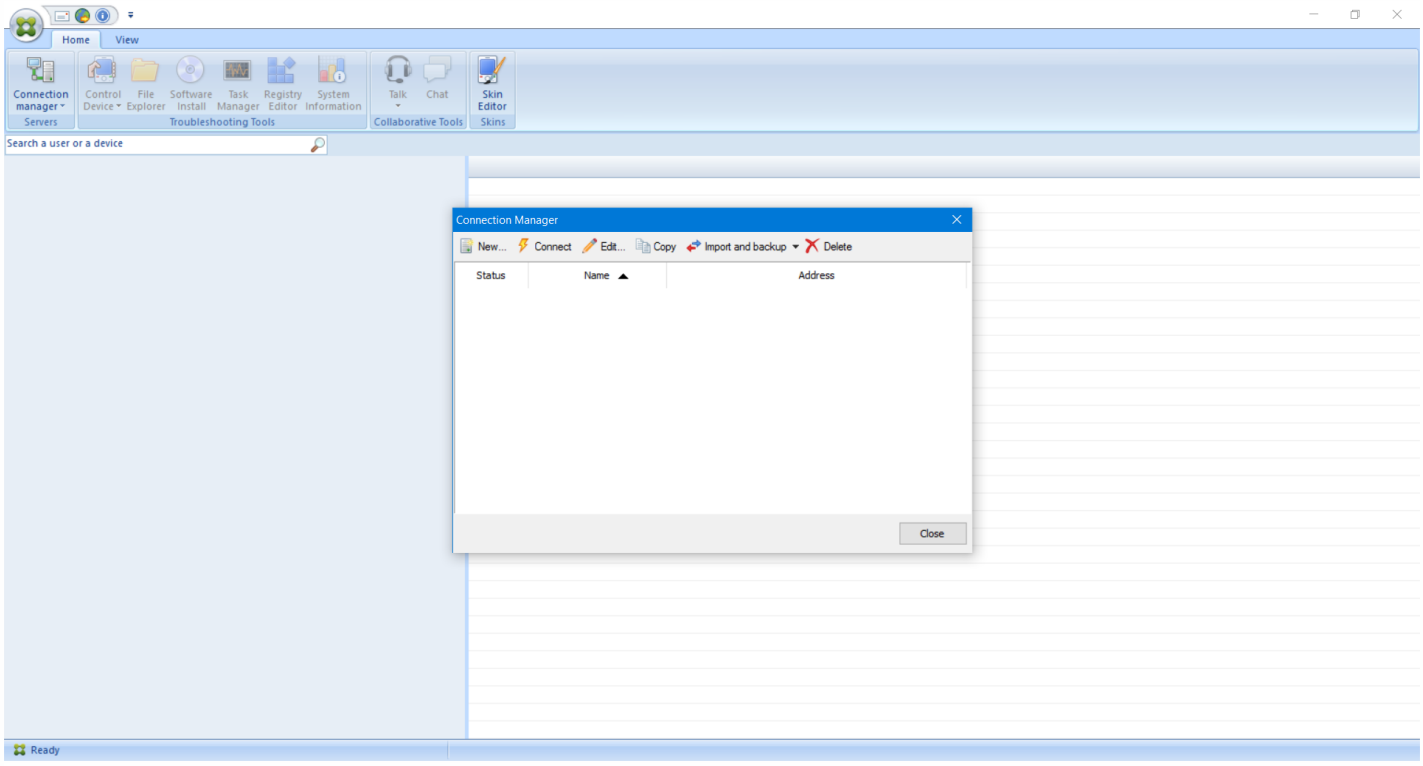
- /S: to silently install the Remote Support software with the default parameters.
- /D=dir: to specify a custom installation directory.

To connect Remote Support to XenMobile

To establish remote support connections to managed devices, you must add a connection from Remote Support to the XenMobile server(s) that manage the devices. That connection runs over an app tunnel defined in the Tunnel Policy, a device policy for Android and Windows Mobile/CE devices. The app tunnel must be defined as described in App tunneling device policies before you can connect Remote Support to XenMobile.

1. Start the Remote Support software and use your XenMobile credentials to log on.

2. In **Connection Manager**, click **New**.



3. In the **Connection Configuration** dialog box, on the **Server** tab, enter the following values:

In **Configuration name**, enter a name for the configuration entry.

In **Server IP address or name**, type the IP address or the DNS name of the XenMobile server.

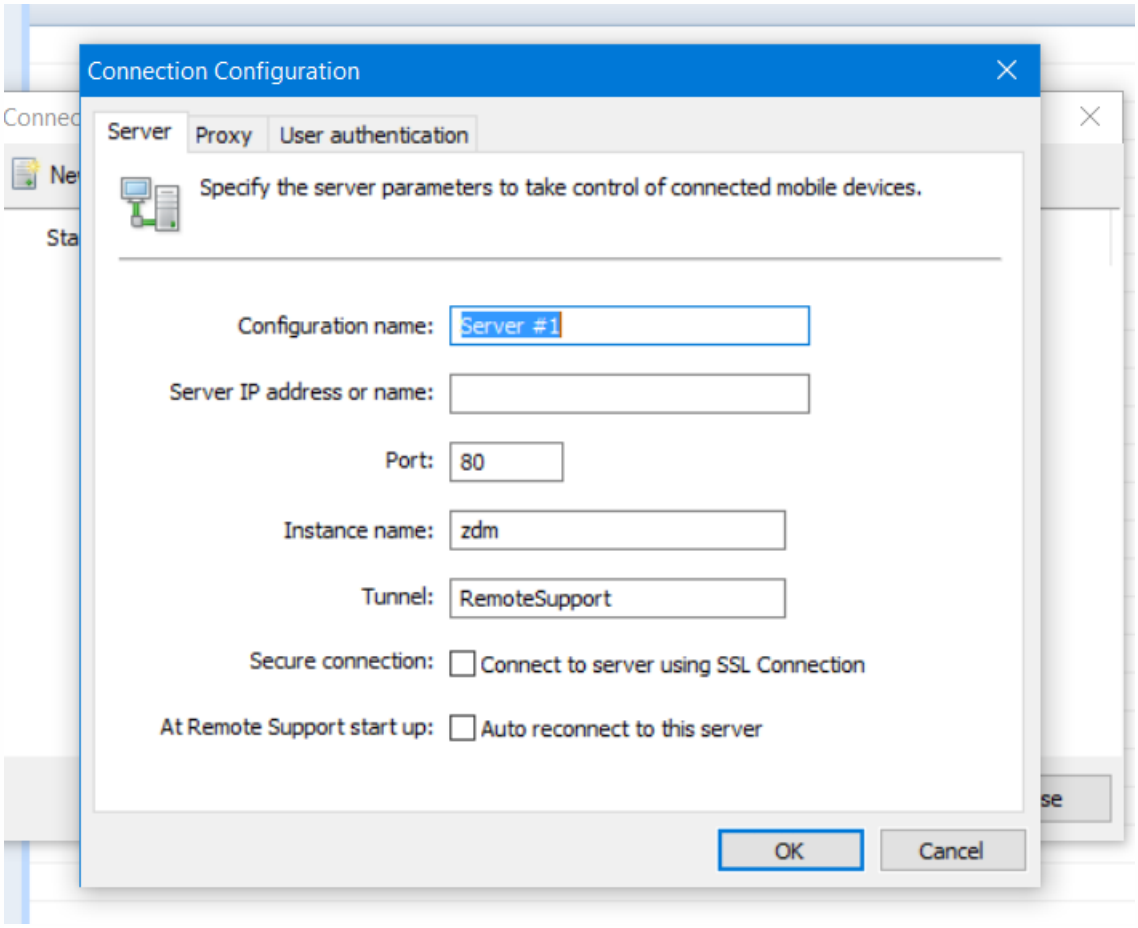
In **Port**, type a TCP port number, as defined in the XenMobile server configuration.

In **Instance name**, if XenMobile is part of a Multi-Tenant deployment, type an instance name.

In **Tunnel**, type the name of the Tunnel Policy.

Select the **Connect to server using SSL Connection** check box.

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 enter the following information:

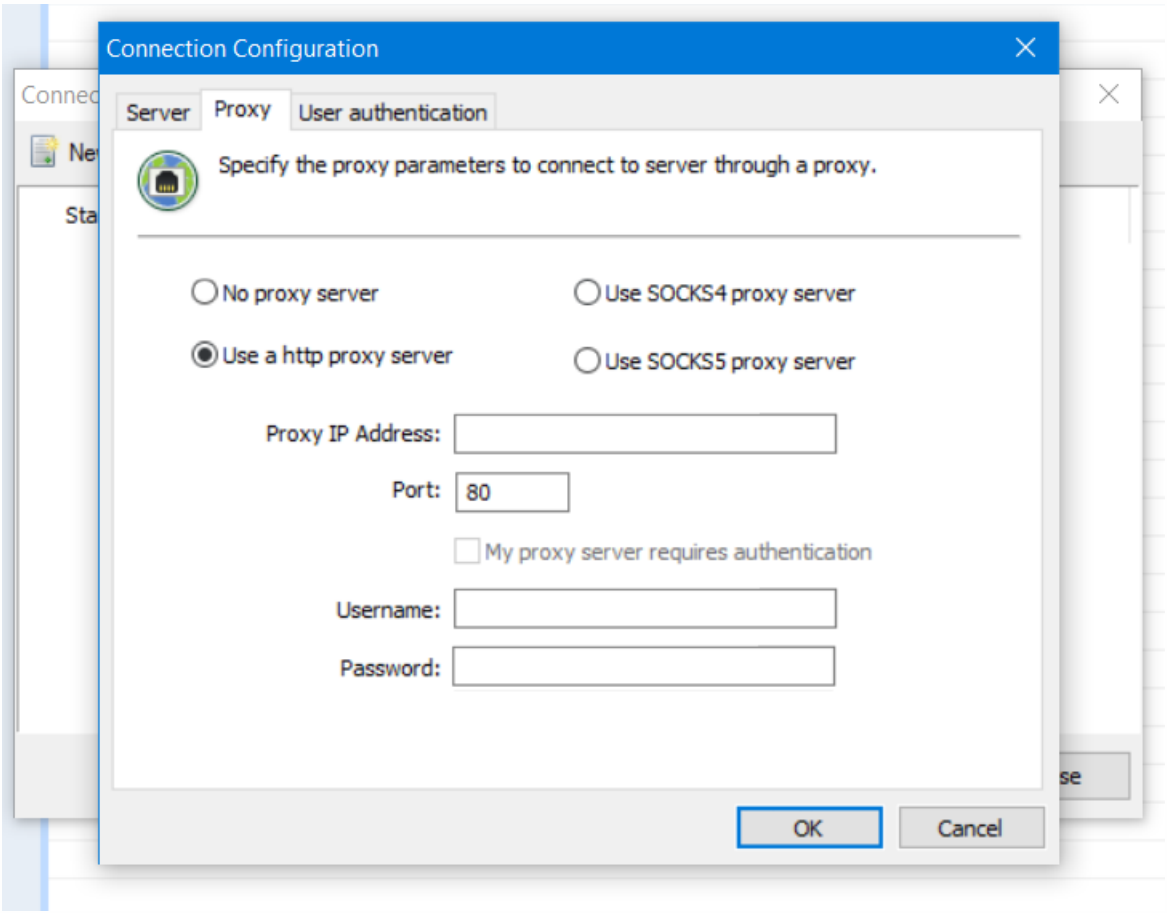
In **Proxy IP Address**, type the IP address of the proxy server.

In **Port**, type a TCP port number used by the proxy.

Select the **My proxy server requires authentication** check box if the proxy server requires authentication to allow traffic.

In **Username**, type the user name to be authenticated on the proxy server.

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.

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 defined in the XenMobile administrative console. By default, only groups containing users that are currently connected are shown. 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 click **Control Device**. A rendering of the device appears in the Remote Control window. Here are some of the ways you can interact with a controlled device:

- Control the device screen, including control with colors, in either the main window, or in a separate, floating window.
- Establish a Voice-over-IP session (VoIP) 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's local directories. Transfer files.
- Edit the device registry on Windows mobile devices.
- Display device system information and all installed software.
- Update the mobile device’s connection status with the XenMobile server.

XenMobile Command-Line Interface Options

Jun 01, 2016

At any time, you can access the following command-line interface (CLI) options on the hypervisor on which you installed XenMobile — Citrix XenServer, Microsoft Hyper-V, or VMware ESXi.

The following are the choices you can make from the Main menu and the menus that appear for each of the first four options: Configuration, Clustering, System, and Troubleshooting.

Main menu

```
------------------------------

[0] Configuration

[1] Clustering

[2] System

[3] Troubleshooting

[4] Help

[5] Log Out

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

Choice: [0 - 5]
```

Configuration Menu Options

From the main menu, when you select the Configuration option, the following menus appear:

```
[0] Back to Main Menu

[1] Network

[2] Firewall

[3] Database

[4] Listener Ports

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

Choice: [0 - 4]

------------------------------
```

When you choose the Network option, you are prompted to restart to save the changes.

When you choose the Firewall, option, you are prompted as follows:

```
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]:

Management HTTPS service

Port: 4443

Enable access (y/n) [y]:

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) [y]:

Access white list []:

Remote support tunnel

Port [8081]:

Enable access (y/n) [n]:

When you choose the Database option, you are prompted as follows:

Type: [mi]

Use SSL (y/n) [y]:

Upload Root Certificate (y/n) [y]:

Copy or Import (c/i) [c]:

Clustering Menu Options

From the main menu, when you select the Clustering option, the following menus appear:

[0] Back to Main Menu

[1] Show Cluster Status

[2] Enable/Disable cluster

[3] Cluster member white list

[4] Enable or Disable SSL offload

[5] Display Hazelcast Cluster

Choice: [0 - 5]

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.

When you choose the cluster member white list, if you disabled clustering, the following message appears:

Cluster is disabled. Please enable it.

If you have clustering enabled, the following options appear:

Current White List:

- comma separated list of hosts or network

- 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:

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.

When you select to display the Hazelcast Cluster, the following options appear:

Hazlecast Cluster Members:

[IP address listed]

NOTE: If an configured node is not part of the cluseter, please reboot that node.

System Menu Options

From the main menu, when you select the System option, the following menus appear:

---

[0] Back to Main Menu

[1] Display System Date

[2] Set Time Zone

[3] Display System Disk Usage

[4] Update Hosts File

[5] Proxy Server

[6] Admin (CLI) Password

[7] Restart Server

[8] Shutdown Server

[9] Advanced Settings

Choice: [0 - 9]

Troubleshooting Menu Options

From the main menu, when you select the Troubleshooting option, the following menus appear:

---

[0] Back to Main Menu

[1] Network Utilities

[2] Logs

[3] Support Bundle

Choice: [0 - 3]

When you choose the Network Utilities option, the following menu appears:

---

[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

Choice: [0 - 7]

When you choose the Logs option, the following menu appears:

Logs Menu

---

[0] Back to Troubleshooting Menu

[1] Display Log File

Choice: [0 - 1]

XenMobile Analyzer Tool with XenMobile 10.3

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.

> ## Note
>
> Starting with version 10.4, Worx Mobile Apps are renamed XenMobile Apps. Most of the individual XenMobile Apps are renamed as well. For details, see About XenMobile Apps.

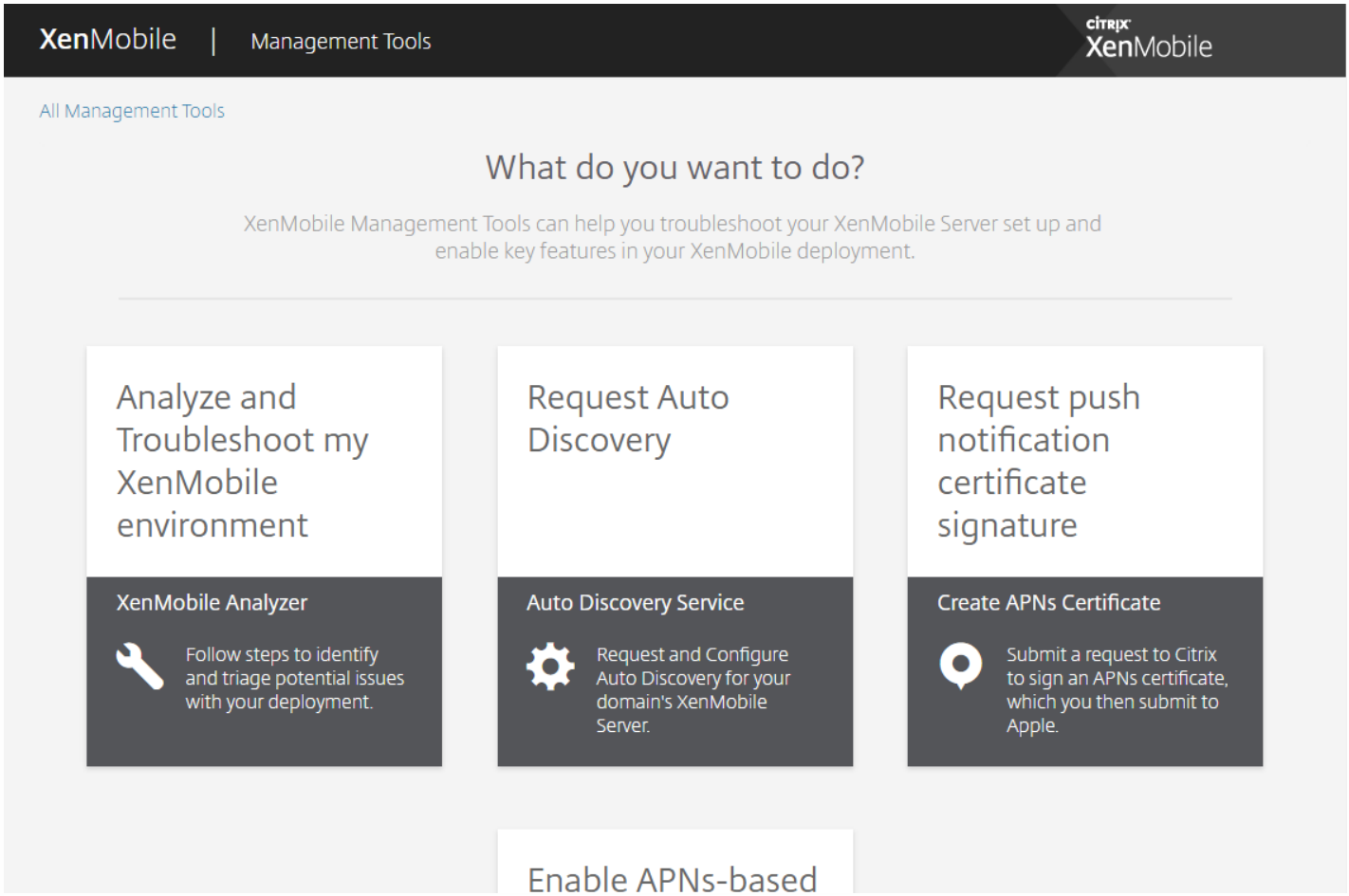
XenMobile Analyzer Key Features

- 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.
- WorxWeb tests for reachability to intranet sites.
- WorxMail Auto Discovery service checks.
- ShareFile Single Sign-On checks.
- Enables custom port support for NetScaler.
- Supports non-EN browsers.

Prerequisites

Product	Supported Version
XenMobile Server	10.3.0 - 10.3.6
NetScaler Gateway	10.5 - 11.1
Client Enrollment Simulation	iOS and Android

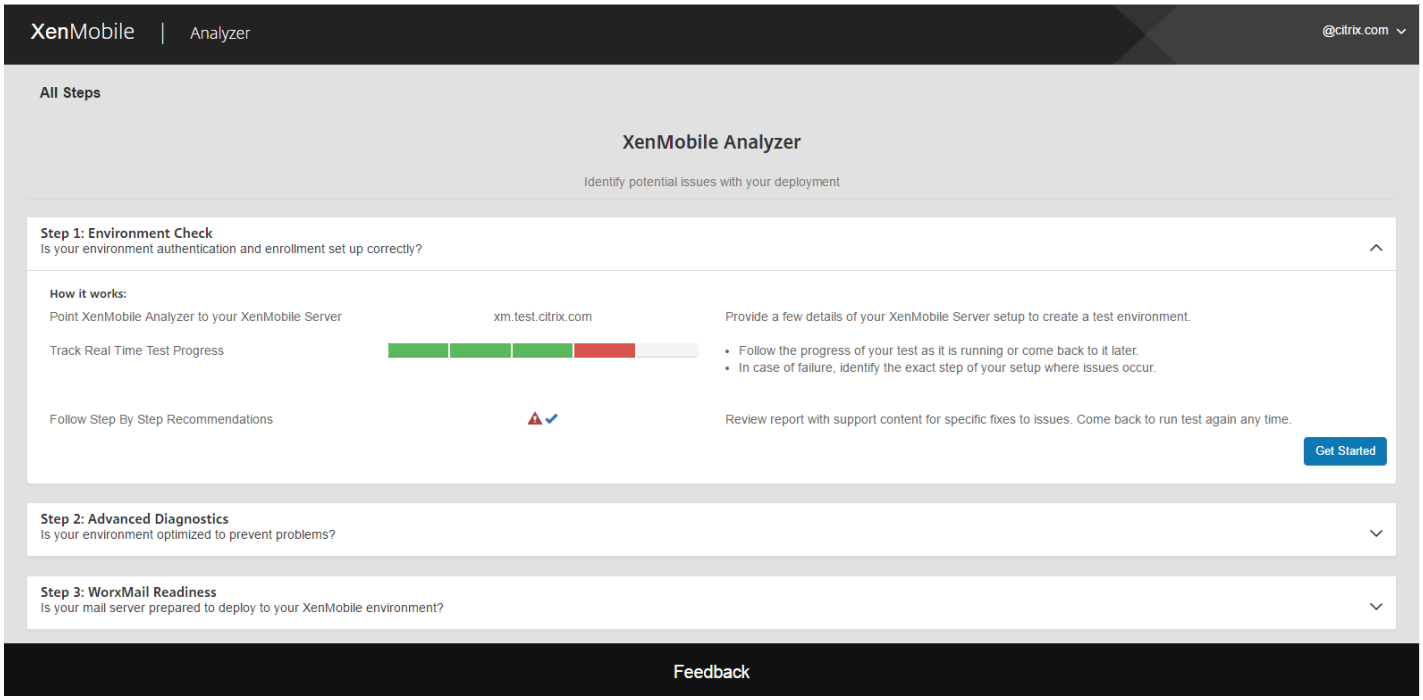
You use your MyCitrix credentials to access the tool from https://xenmobiletools.citrix.com. On the XenMobile Management Tools page that opens, to start the XenMobile Analyzer, click **Analyze and Troubleshoot my XenMobile Environment**.



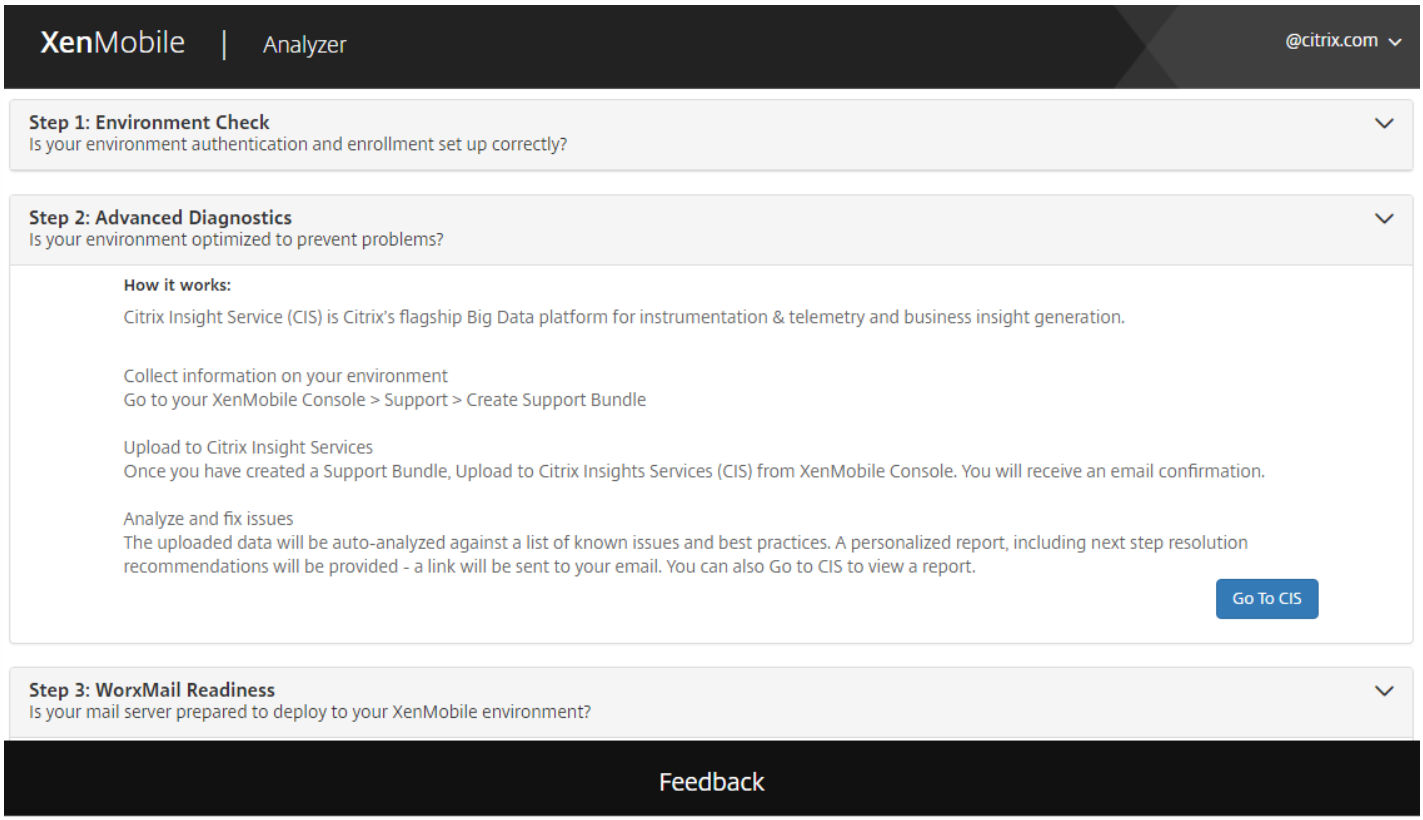
XenMobile Analyzer contains five main steps designed to lead you through the triage process and to reduce the number of support tickets, which can lower costs for everyone.

The steps are as follows:

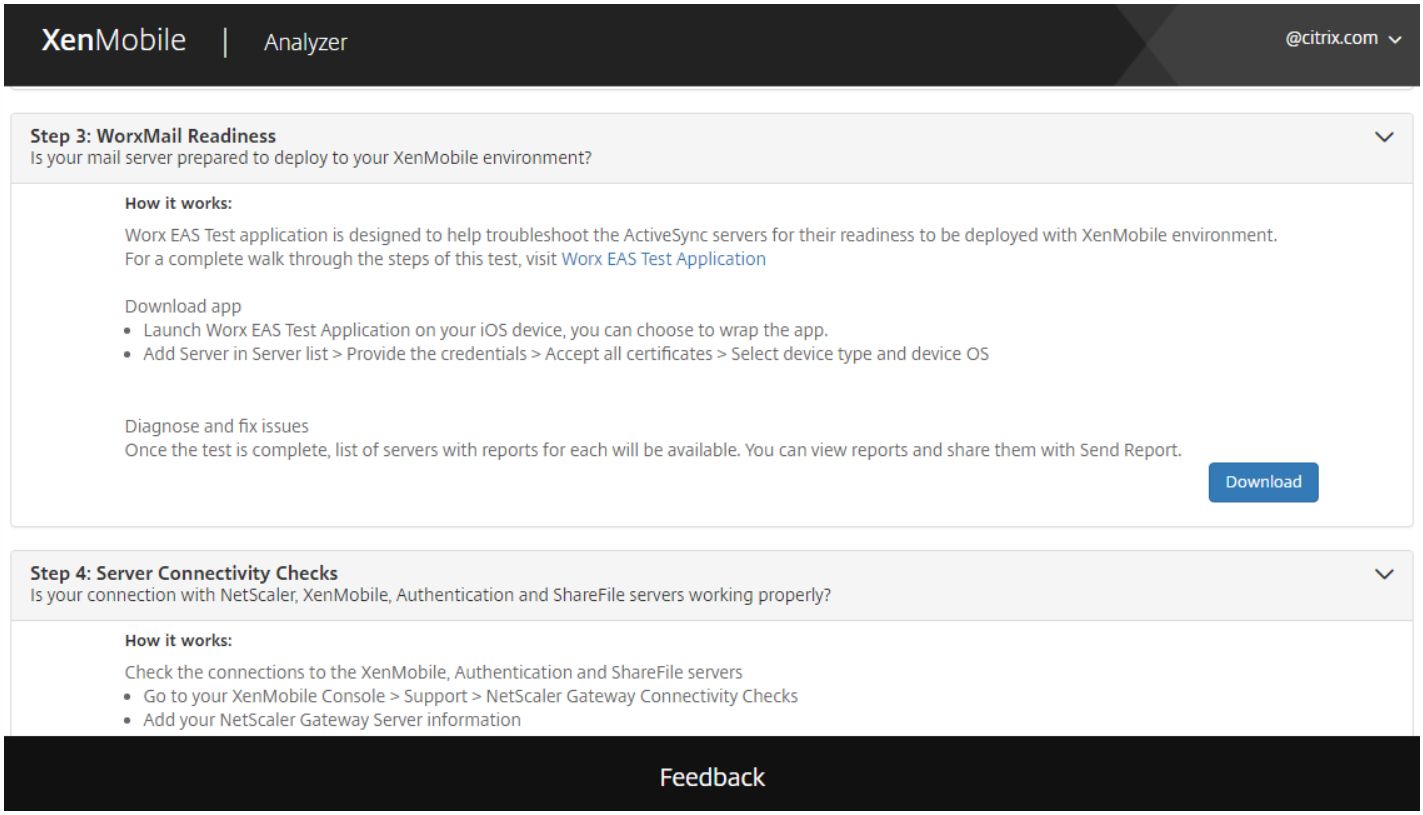
1. **Environment Check** - This step guides you in setting up tests to check your setup for issues. The step also provides recommendations and solutions on device, user enrollment, and authentication issues.



2. **Advanced Diagnostics** - This step provides information on using Citrix Insight Services to find further issues that the environment check may have missed.

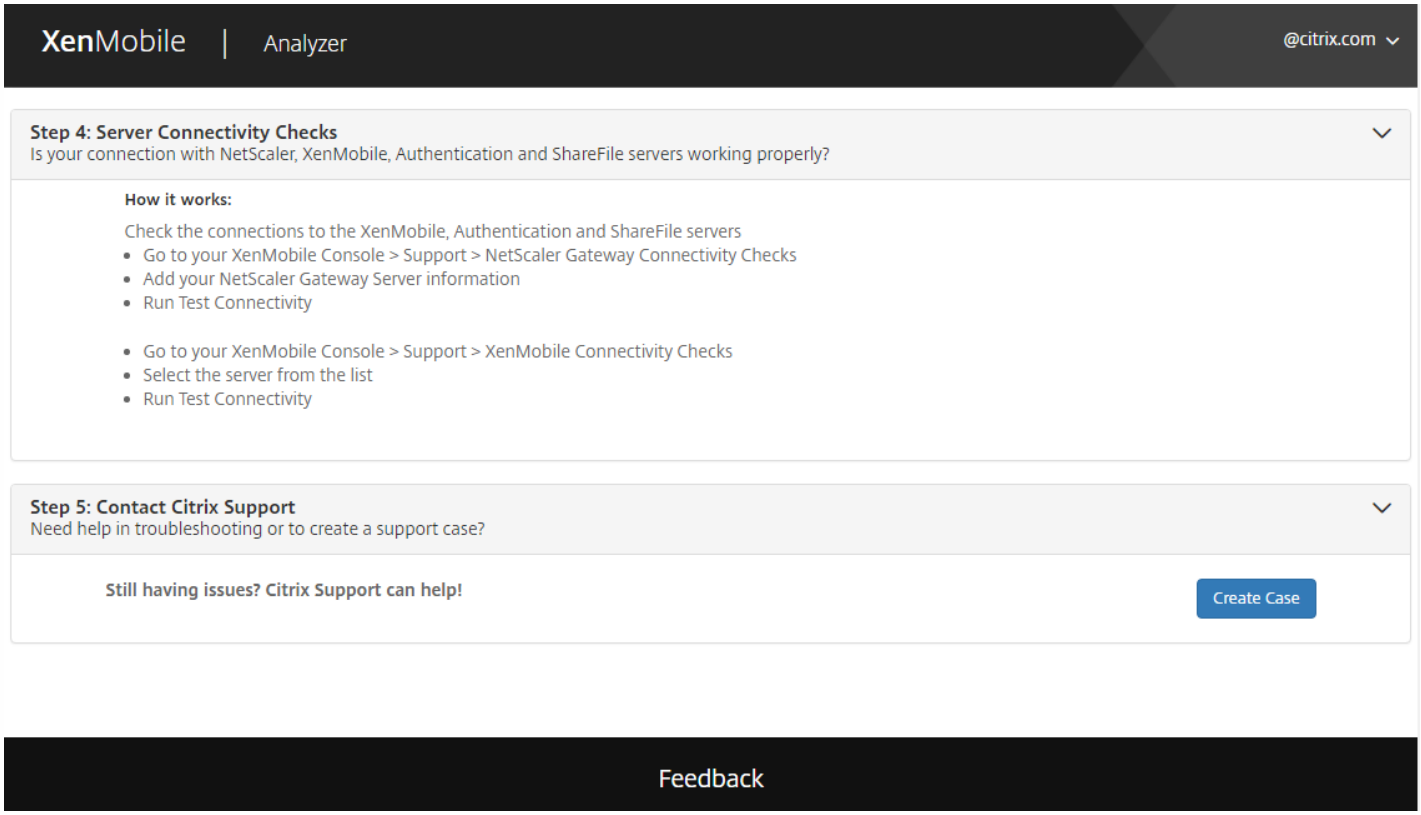


3. **WorxMail Readiness** - This step directs you to download the Worx Exchange ActiveSync Test application, which helps to troubleshoot the ActiveSync servers for their readiness to be deployed with a XenMobile environment.



4. **Server Connectivity Checks** - This step instructs you to test the connectivity of your servers.

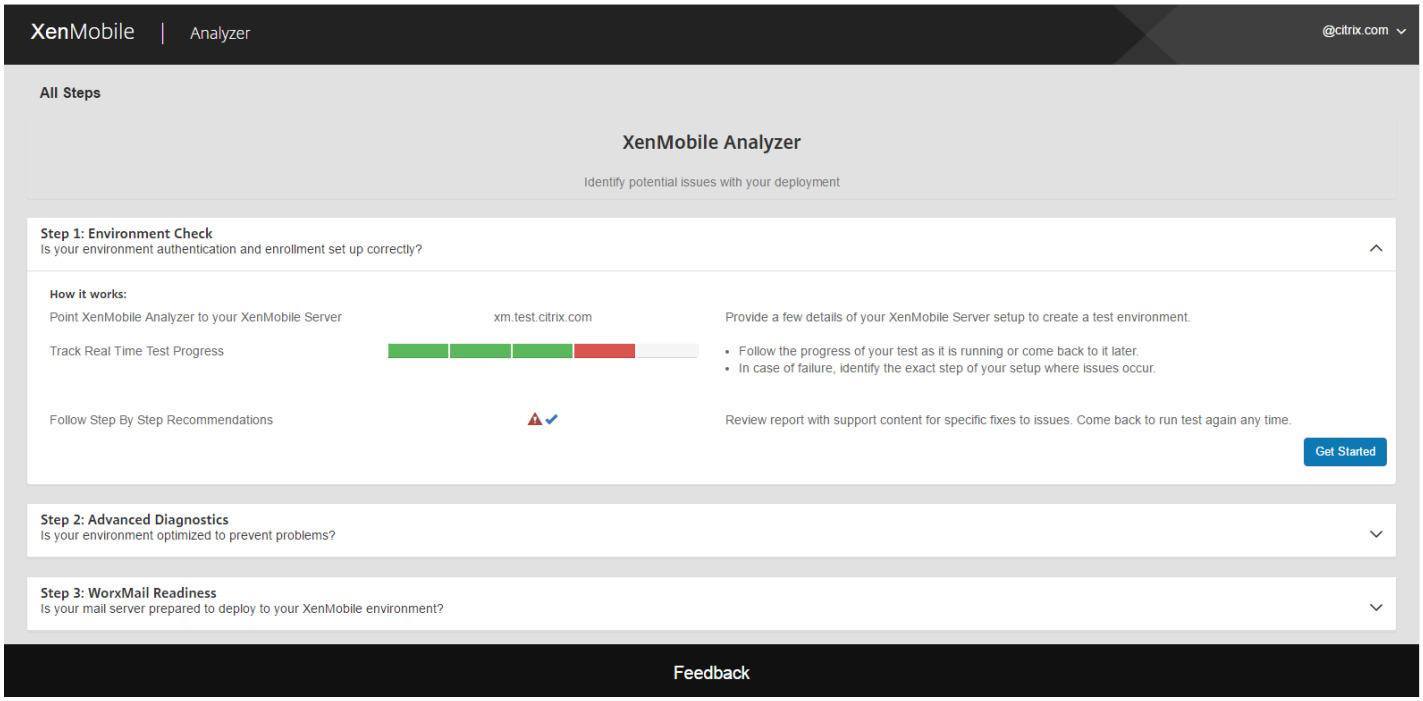
5. **Contact Citrix Support** - This step links you to the site where you can create a Citrix Support case if you're still having issues.



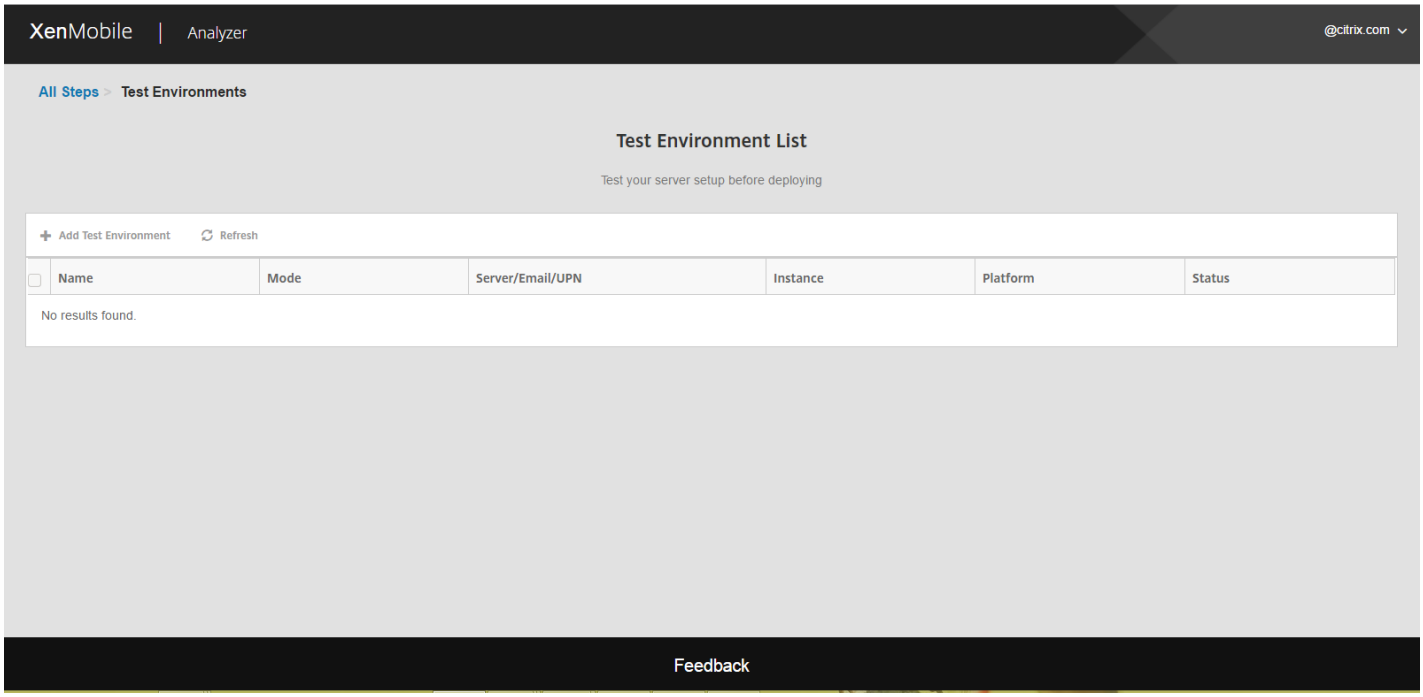
The following sections describe each step in more detail.

Performing an Environment Check

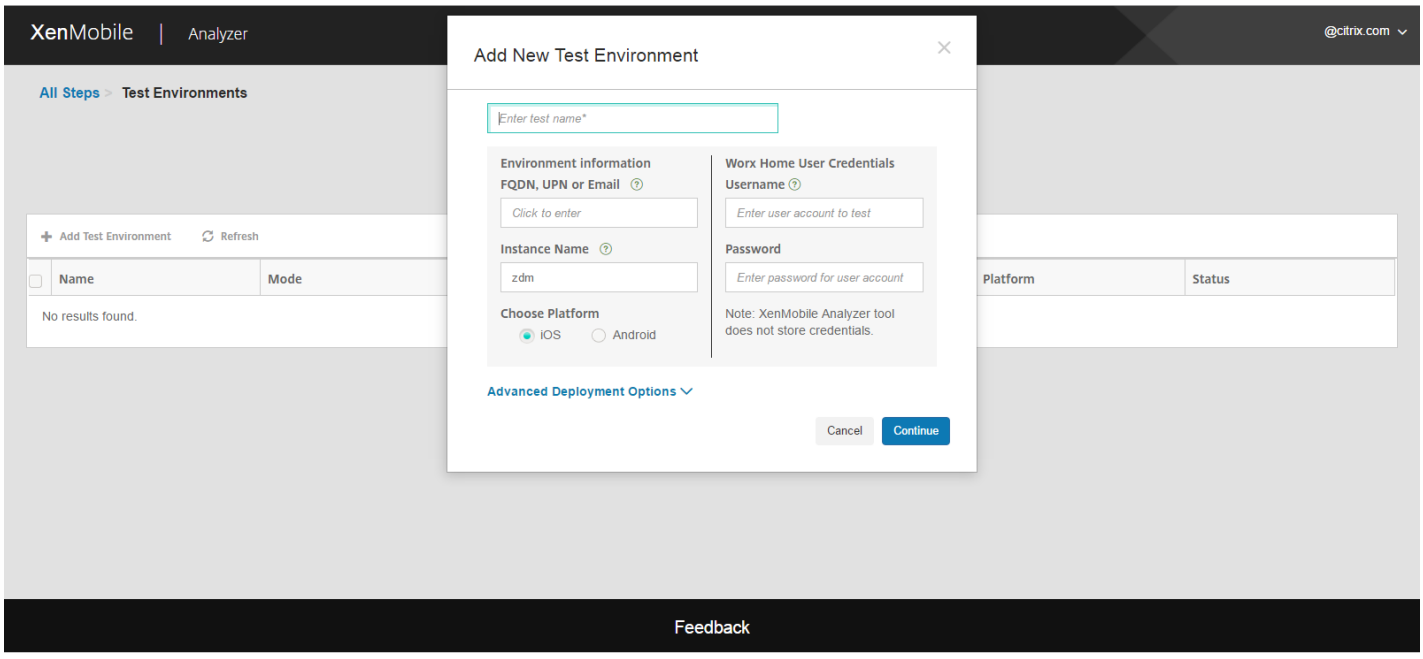
1. Log on to the XenMobile Analyzer and then click **Step 1: Environment Checks**.
2. Click **Get Started**.



3. Click **Add Test Environment**.



4. In the new **Add Test Environment** dialog box, do the following:



a. Provide a unique name for the test that will help identify the test in the future.

b. If you have an invitation URL for enrollment, click on **Advance Deployment Options**. When it expands, mark the **Do you have invitation URL** check box, and then provide the URL. Leaving the field blank will cause the tool to autodiscover the XenMobile server, user name, and other details.

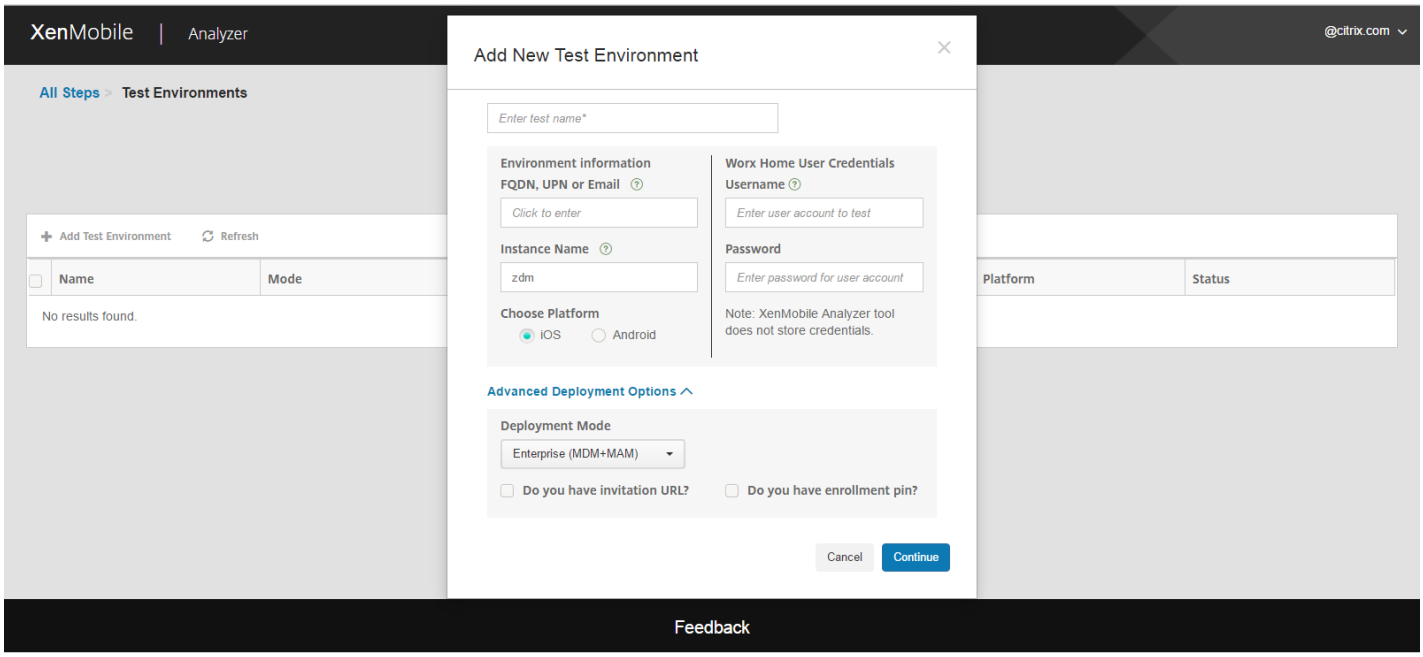
c. If you do not have an invitation URL, you can enter the server information manually.

d. In the **Deployment Mode** list, select your XenMobile deployment mode.

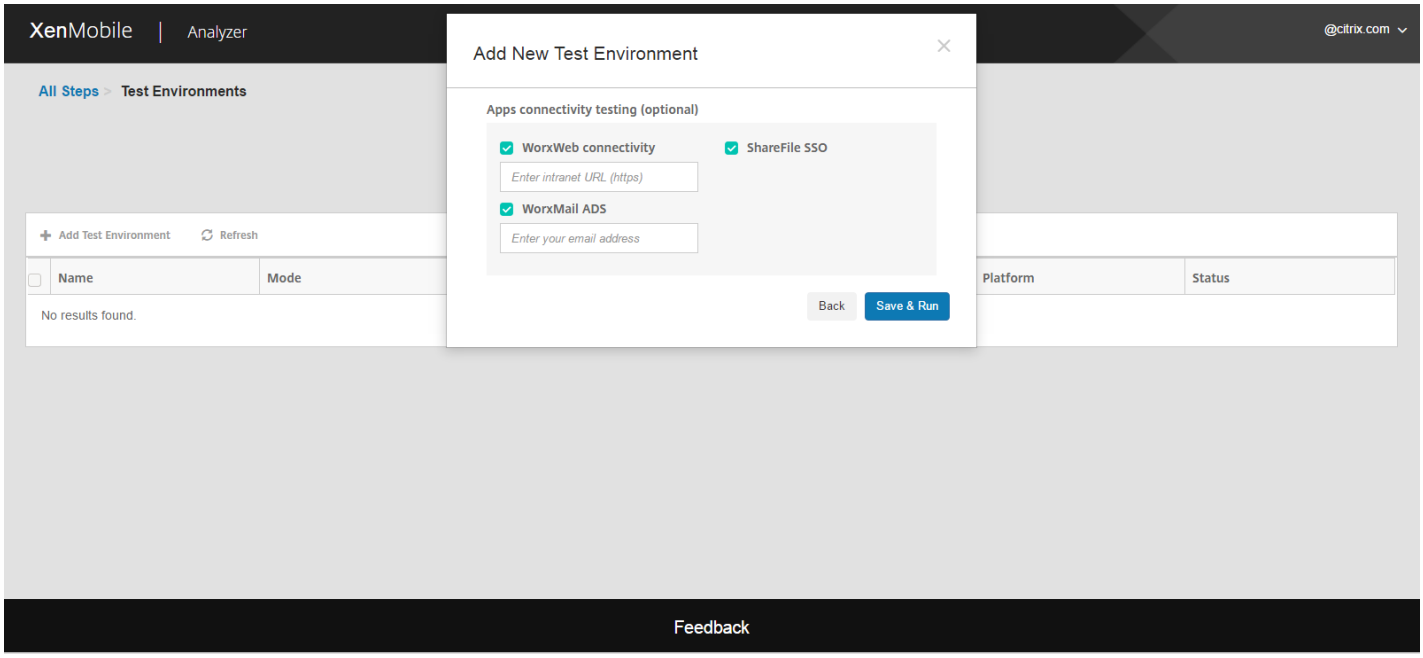
e. In **Instance Name**, if you use a custom instance, you can provide that value.

f. In **Choose Platform**, select either **iOS** or **Android** as the platform for testing.

g. In **Username** and **Password**, enter the user name and password to use for authentication. If your environment is configured for two-factor authentication, select the **Two Factor Authentication** check box and then provide the second password.



5. Click **Continue**.



6. You can choose application level tests to run. You can choose one or more of the following tests.

a. WorxWeb Connectivity. 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 WorxWeb app while trying to reach intranet URLs.

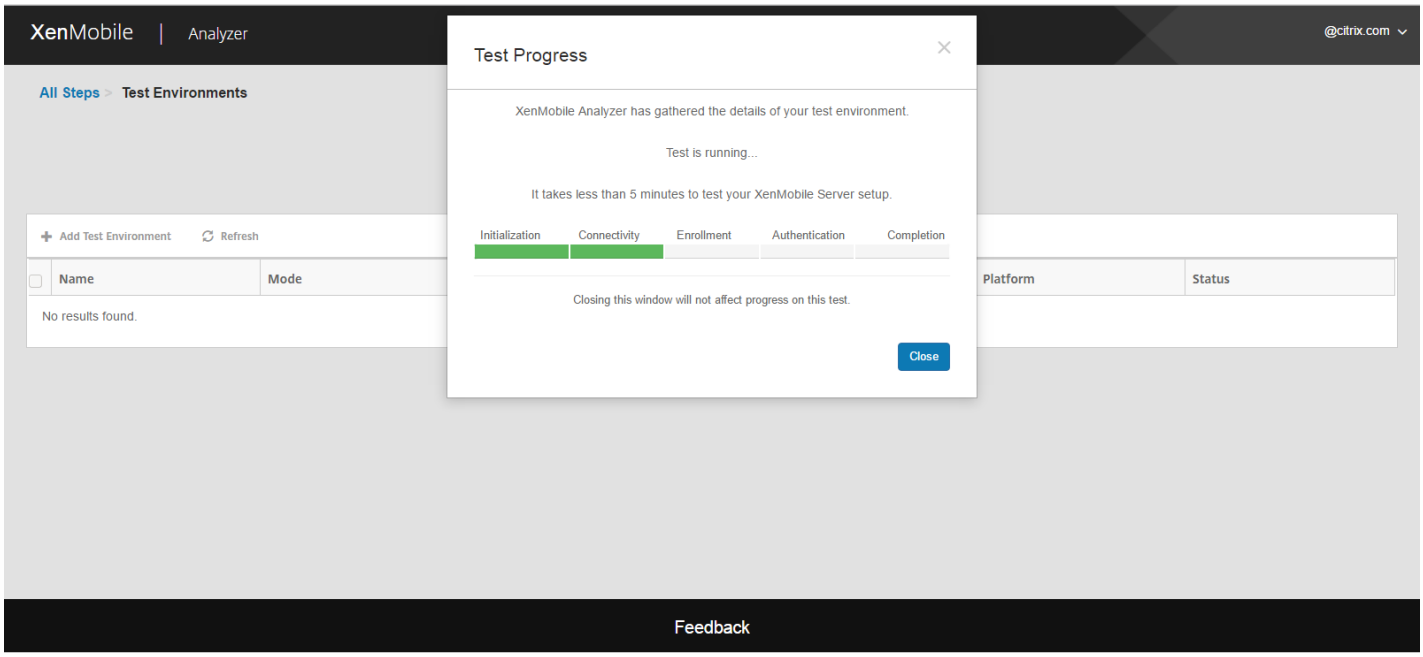
b. WorxMail ADS. Provide a user email ID. This will be used to test the autodiscovery of the Microsoft Exchange Server in your XenMobile environment. It will detect if there are any issues related to WorxMail Auto Discovery.

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 **Save & Run** to start the tests.

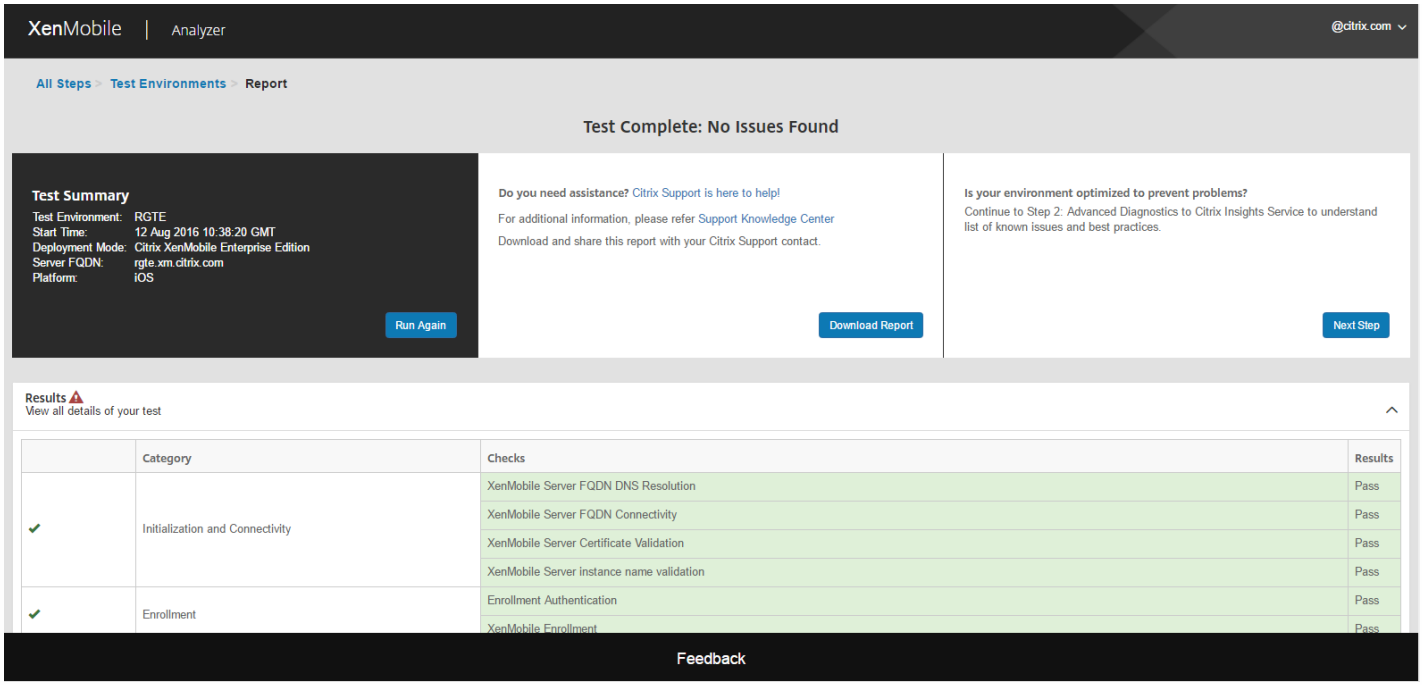
A progress notification appears. You can leave the progress dialog box open or close the dialog box and the tests will continue to run.

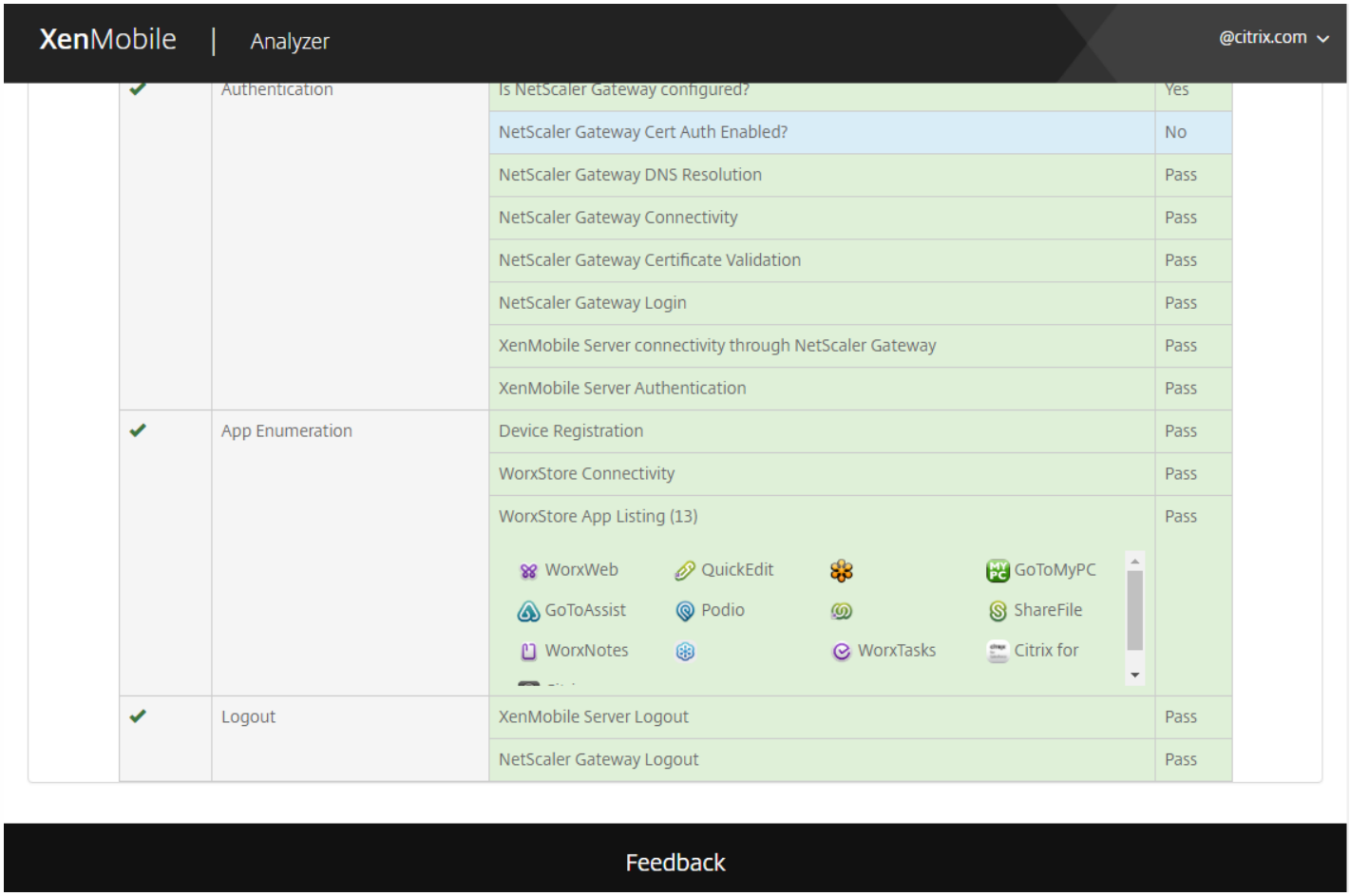
Tests that have passed appear in green. Tests that fail appear as red.



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.





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.

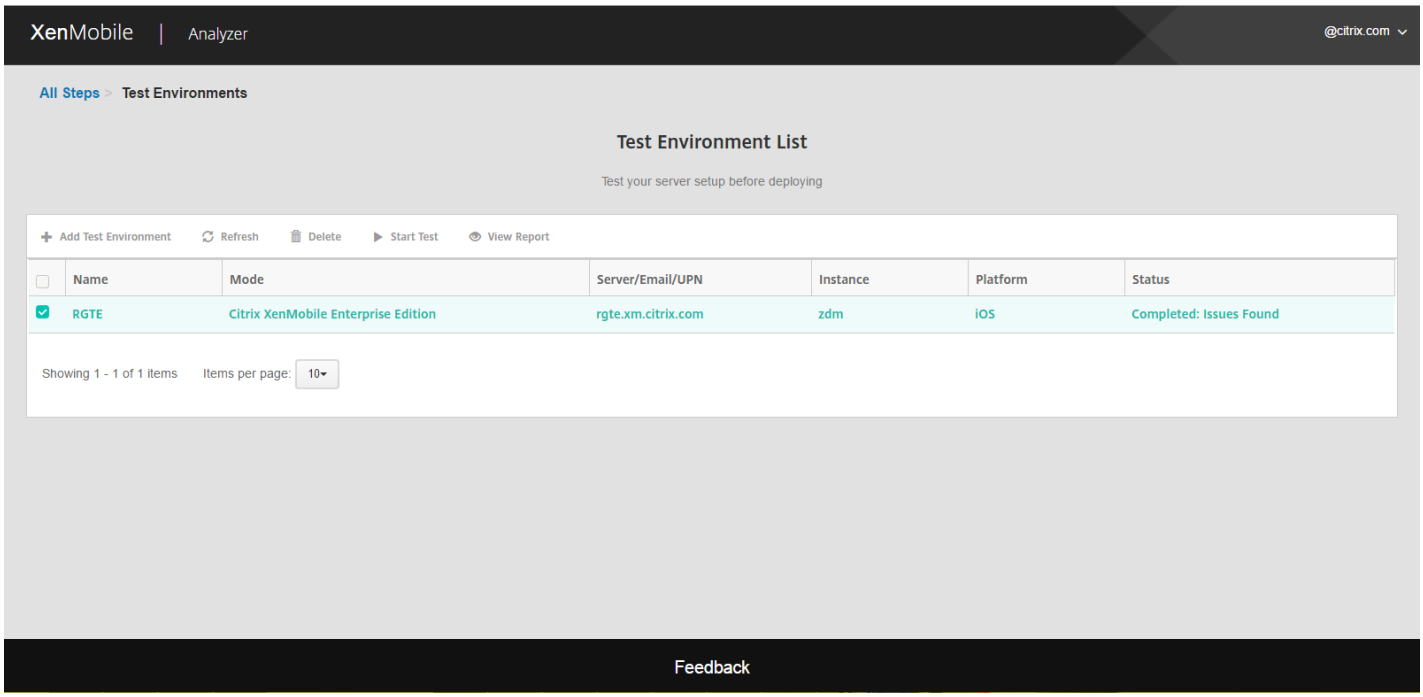
a. To download the report, click **Download Report**.

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**.



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 - WorxMail Readiness:** This step directs you to download and run the Worx 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:

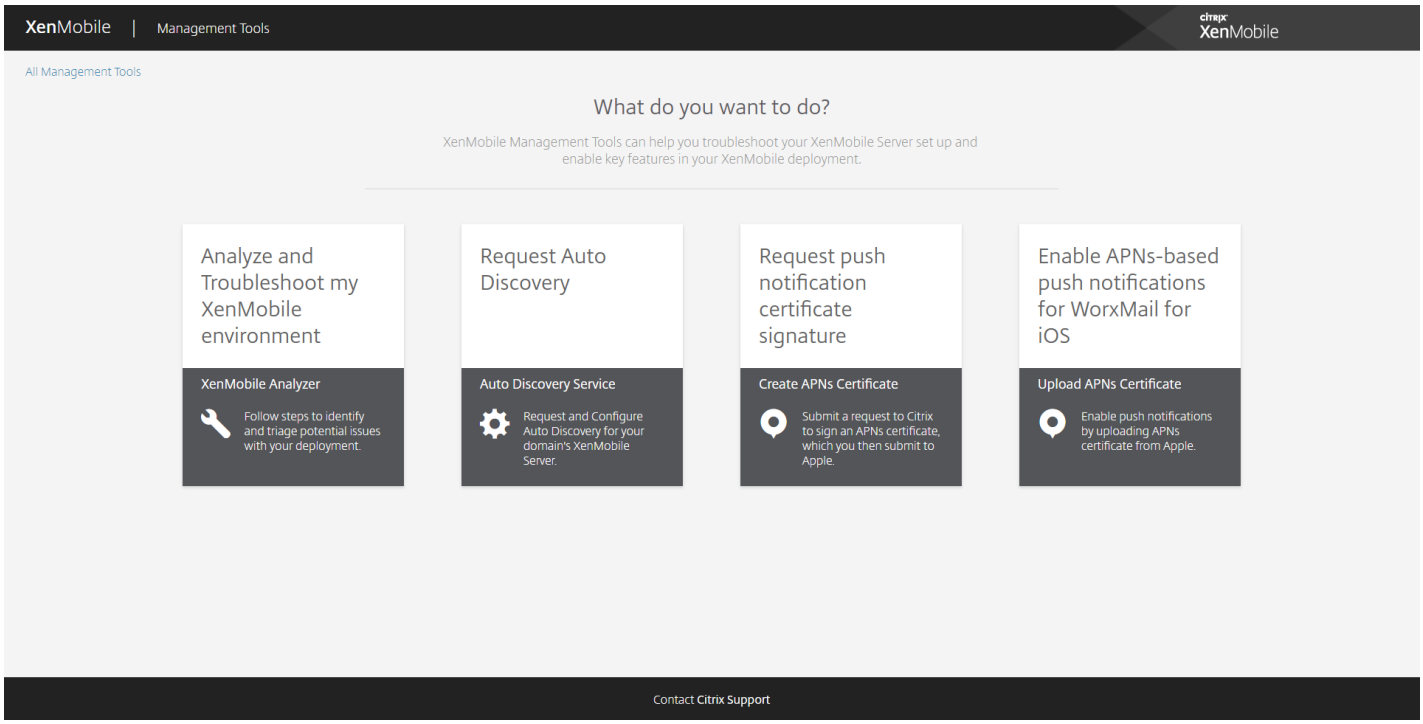
- The number of apps listed might vary based on the client if the Platform Restriction Policy is set on XenMobile Server.
- When performing the WorxWeb Intranet Connectivity checks, entering multiple URLs in the text box is not supported.
- The shared devices authentication feature of WorxHome is not supported.

XenMobile AutoDiscovery Service

Jan 05, 2017

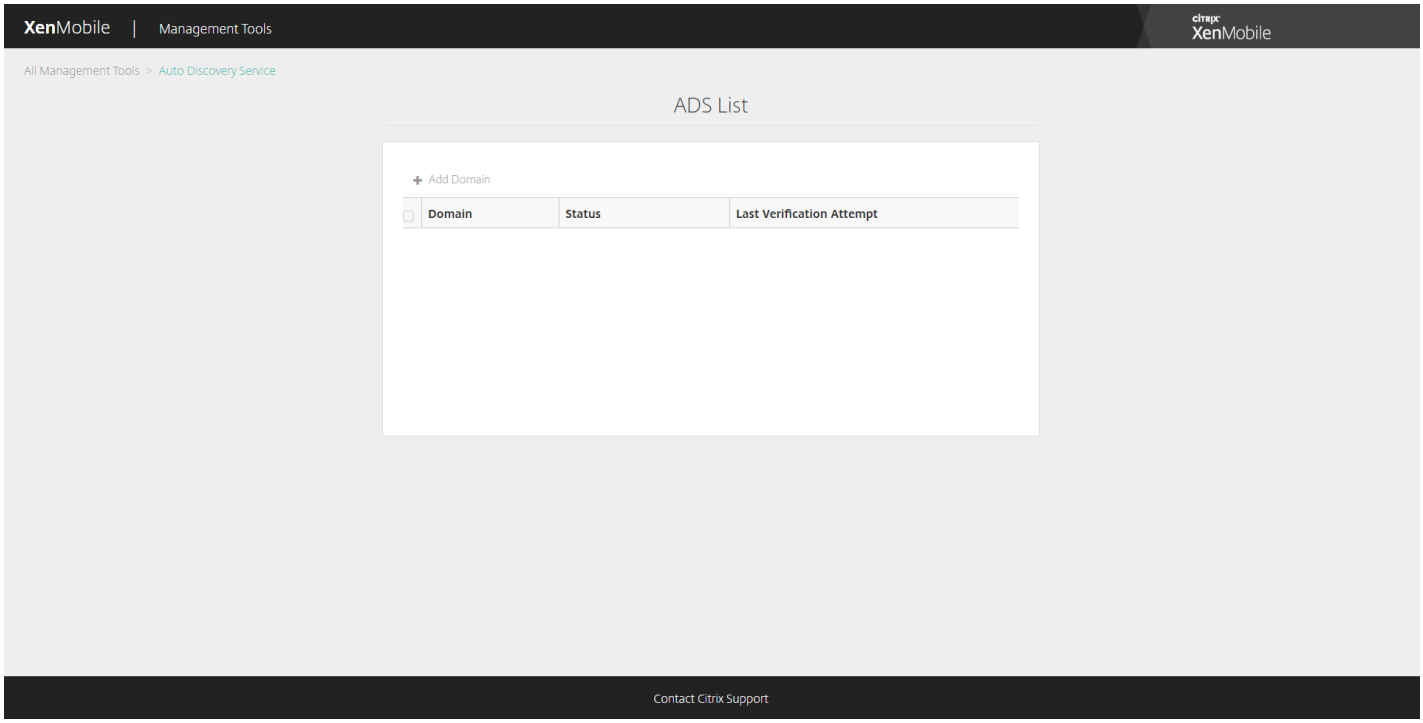
Autodiscovery is an important part of many XenMobile deployments. Autodiscovery simplifies the enrollment process for users. They can use their network user names and Active Directory passwords to enroll their devices, rather than having to also enter details about the XenMobile server. Users enter their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

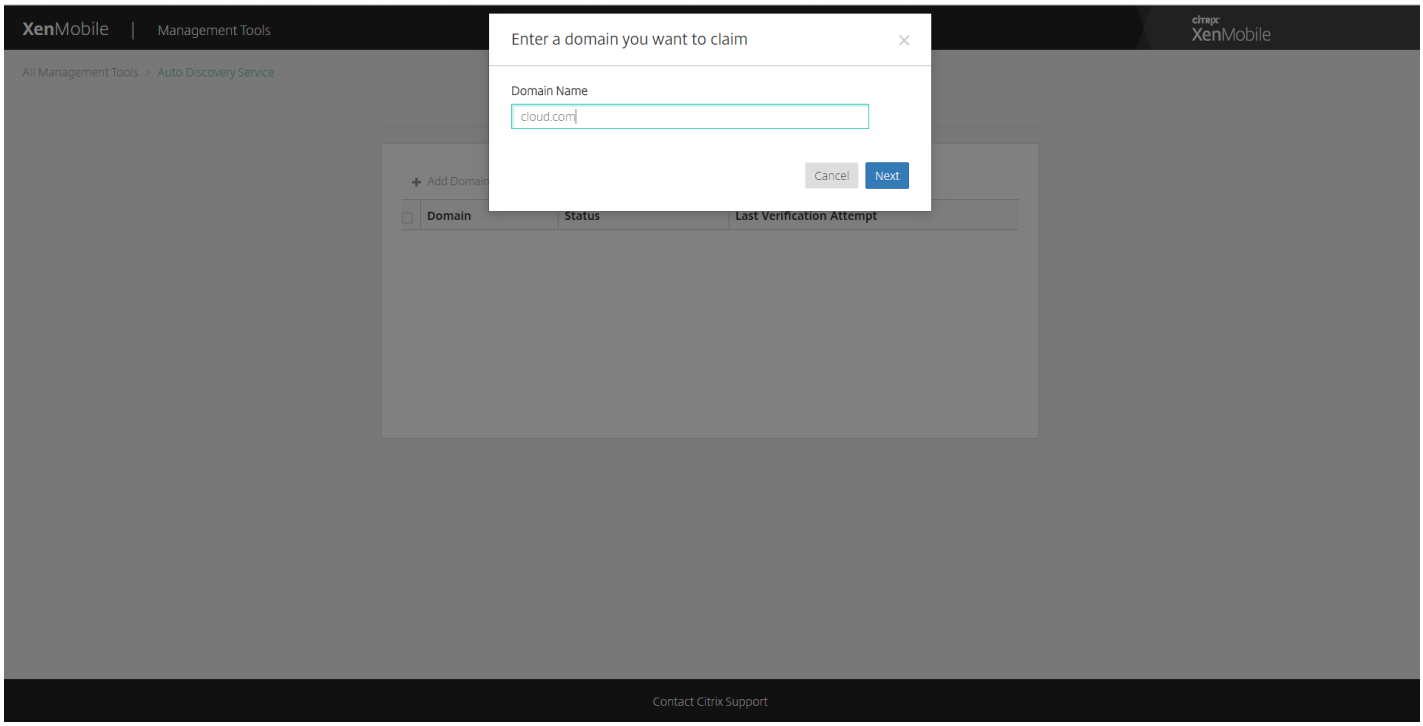


Requesting AutoDiscovery

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.

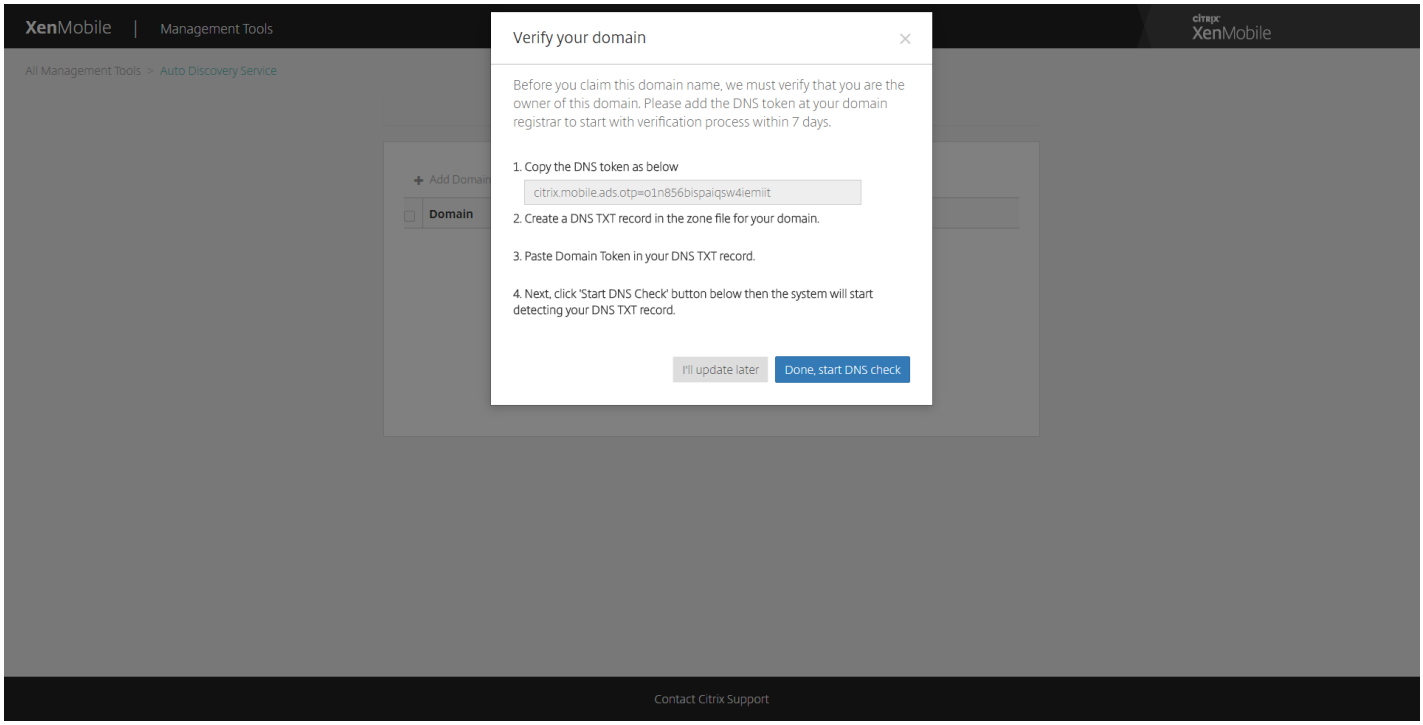
To create a DNS TXT record you need to log into the Domain Hosting Provider portal for the domain you have added in step 2 above. In the Domain Hosting portal you can edit your Domain Name Server Records and add a custom TXT record. An example below of a adding a DNS TXT entry in a hosting portal for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

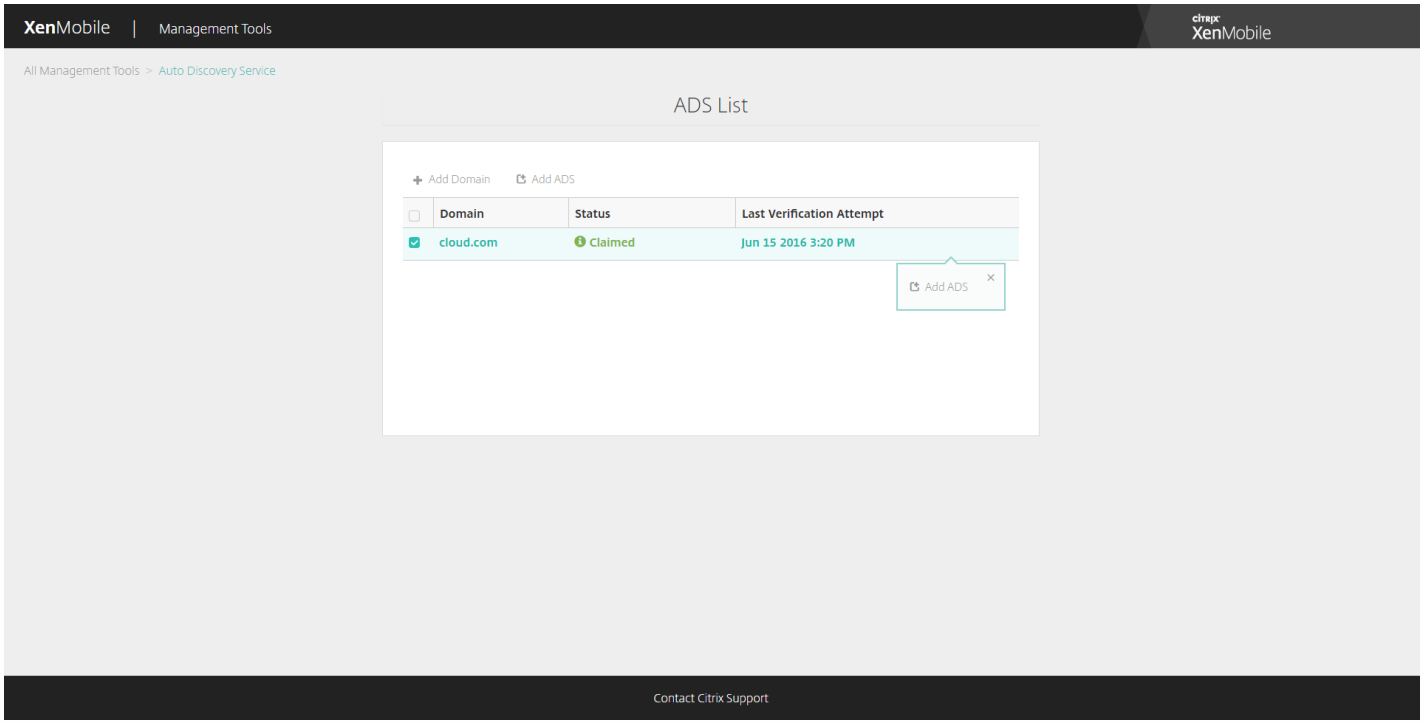
The system detects your DNS TXT record. Alternatively, you can click I'll update later, and the record is saved. The DNS check won't start until you select the Waiting record and click DNS Check.

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**.

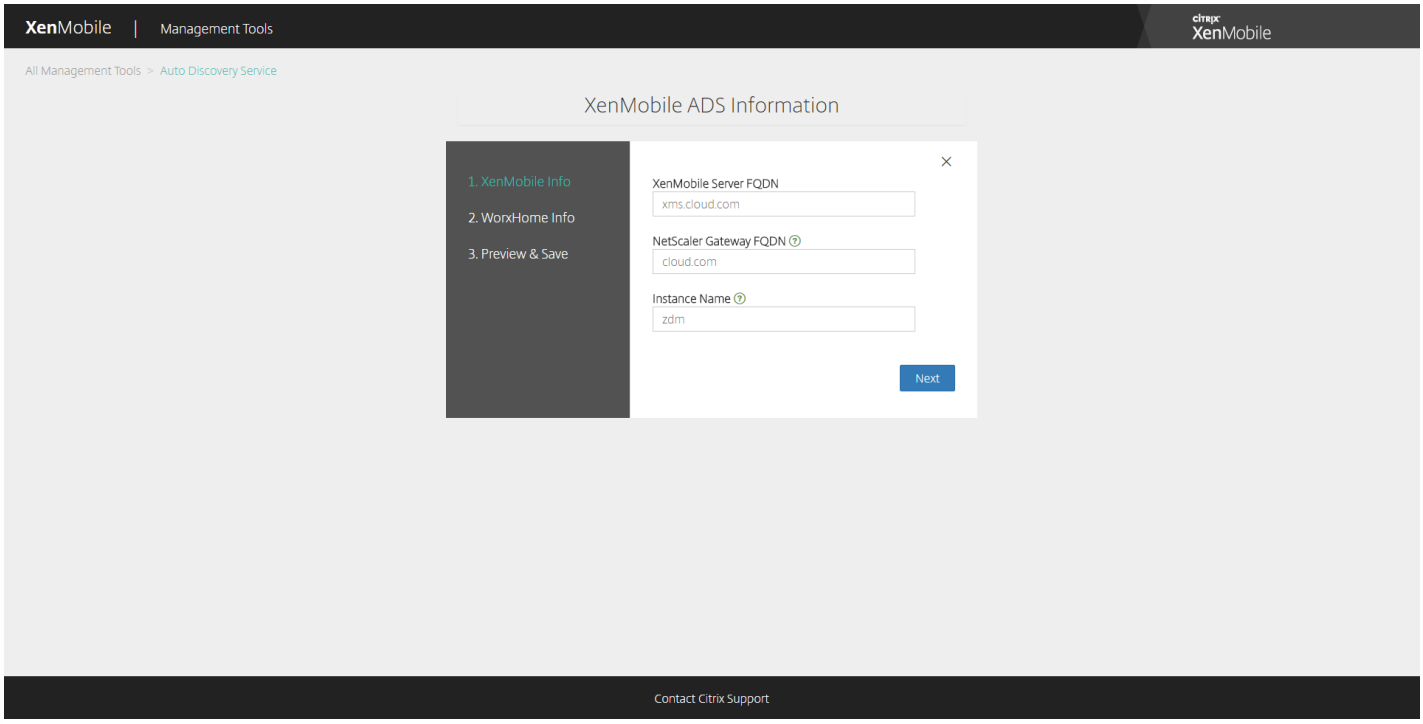
If your domain already has an AutoDiscovery record, please log a case with Citrix Technical Support to modify details as required.



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".

Note

Starting with version 10.4, Worx Home is renamed Secure Hub. For more details, see About XenMobile Apps.



6. Enter the following information for Worx Home and then click **Next**.

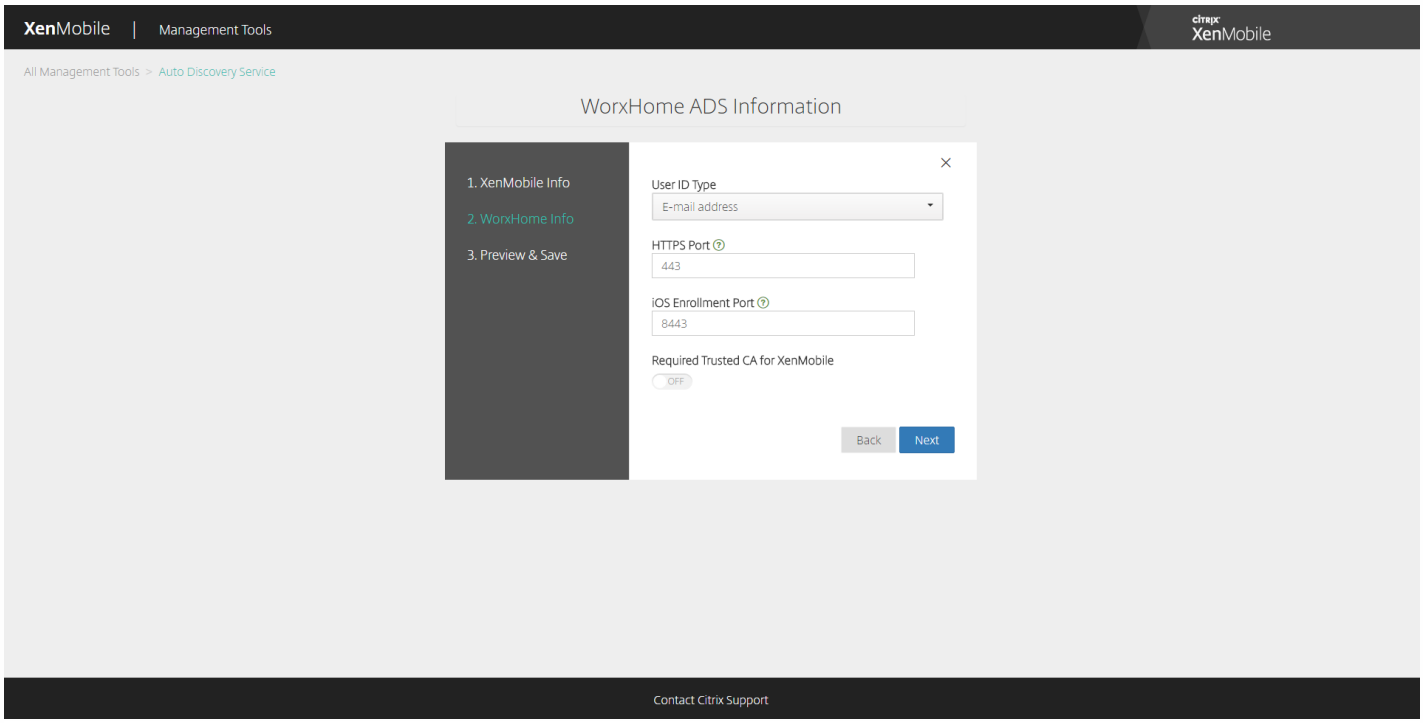
a. **User ID Type**: Select the type of ID with which users sign on as either **E-mail address** or **UPN**.

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.

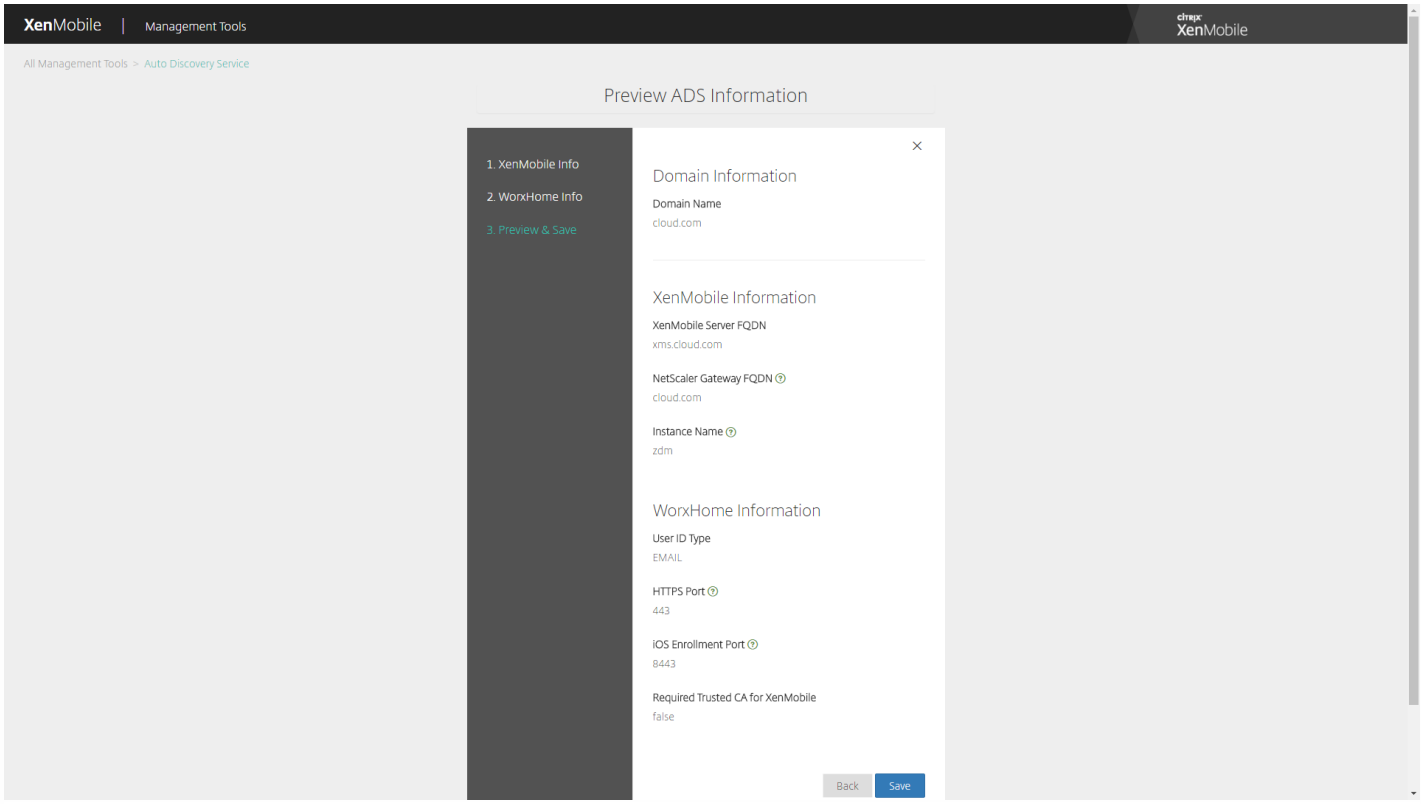
b. **HTTPS Port**: Enter the port used to access Worx Home over HTTPS. Typically, this is port 443.

c. **iOS Enrollment Port**: Enter the port used to access Worx Home 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 create the autodiscovery record and then call Citrix Support, and have certificate pinning enabled through them. To learn more about certificate pinning, see the section on certificate pinning in the Worx Home topic. To read about the ports required for certificate pinning to work, see the support article on XenMobile Port Requirements for ADS Connectivity.



7. A summary page displays all the information you entered in the preceding steps. Verify that the data is correct then click **Save**.



XenMobile REST API Reference

Jun 07, 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.

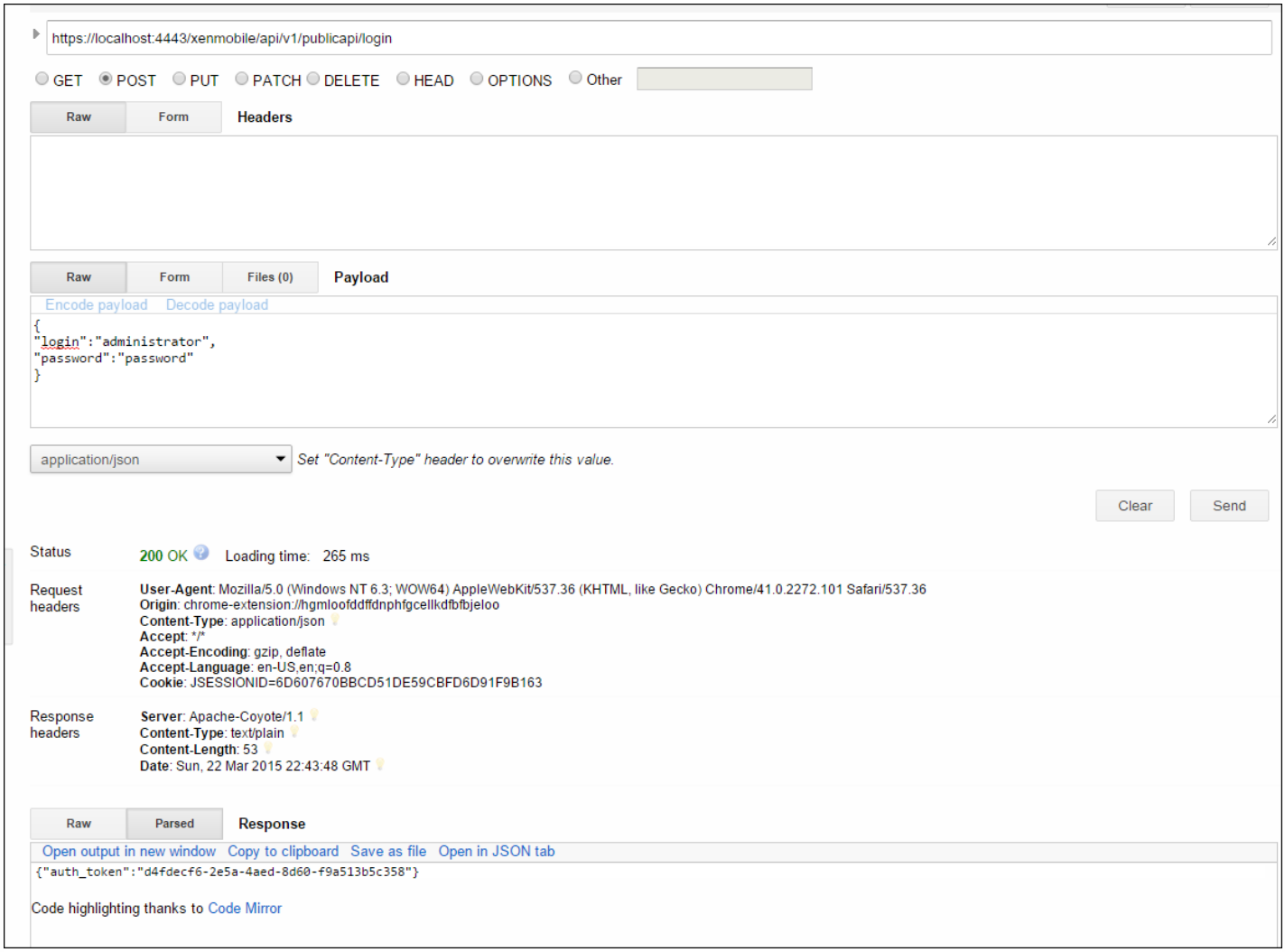
Login

URL: https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login

Request: { "login":"administrator", "password":"password" }

Method type: POST

Content type: application/json



Get Delivery Groups by filter

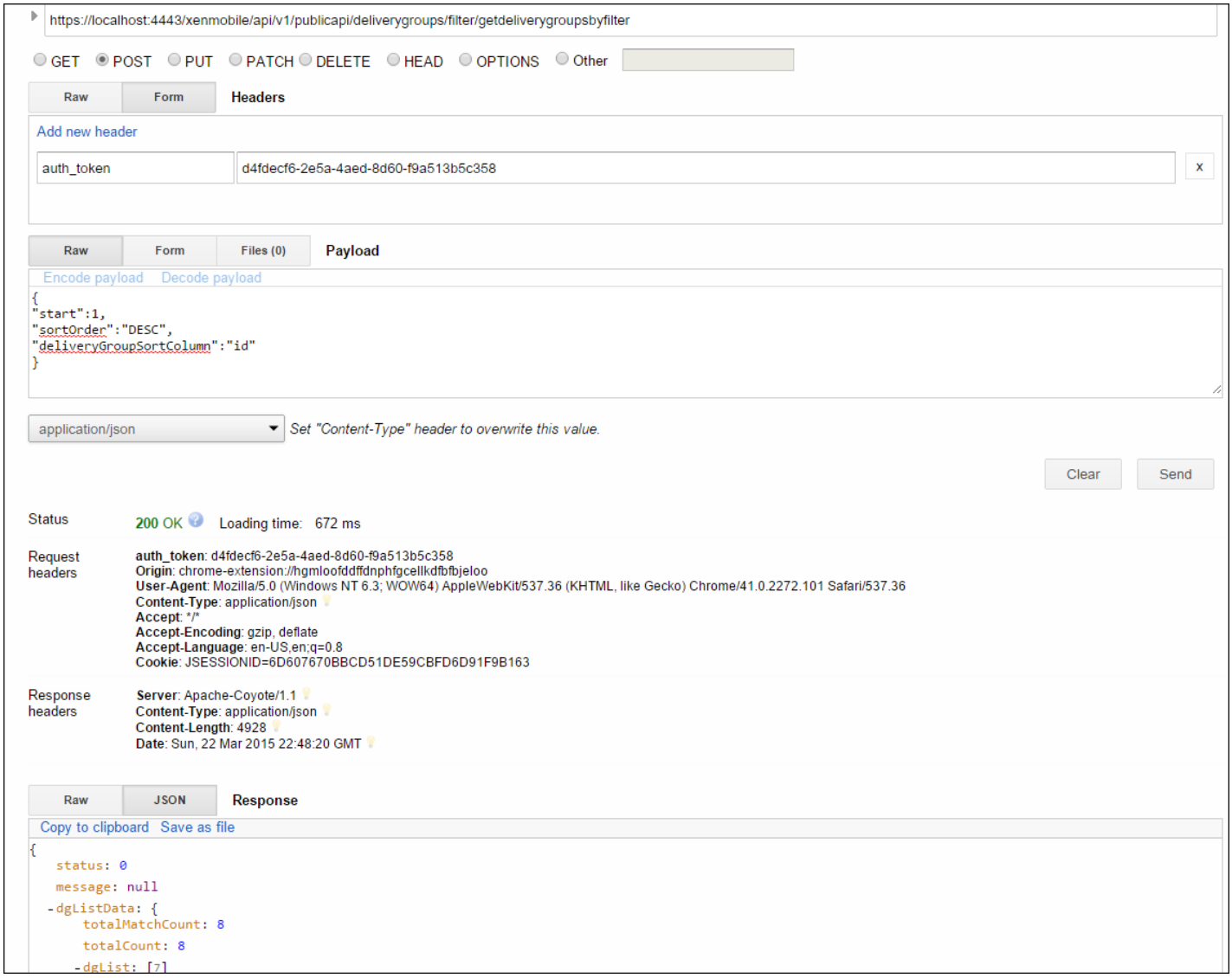
URL: /xenmobile/api/v1/deliverygroups/filter

Request COPY

```
{

    "start": 1,

    "sortOrder": "DESC",

    "deliveryGroupSortColumn":"id",

    "search":"add"

}
```

Method type: POST

Content type: application/json



REST API definitions

The following sections cover some of the APIs found in the PDF. Please refer to the PDF for the full API doc.

Remember: In the following examples, change the host name and port number to match your environment.

To log on to the public API

Accepts user credentials and uses the existing AuthenticationManager to authenticate the user. The first time the AuthenticationManager authenticates a user, it generates an authentication token that is placed in the request header.

URL: https://<host-name>:4443/xenmobile/api/v1/authentication/login

Request type: POST

Request Parameters COPY

```
{ "login":"administrator", "password":"password" }
```

Example Response COPY

```
{

    "auth-token":"q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"

}
```

To log on to the Public API through CWC

Accepts user credentials and uses the existing AuthenticationManager to authenticate the user. The first time the AuthenticationManager authenticates a user, it generates an authentication token that is placed in the request header.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/authentication/cwclogin

Request type: POST

Request header : Authorization – CWSAuth service=<ServiceKey>

Request Parameters COPY

```
{“context”:”customer or cloud”, “customerId”:”customer ID”}
```

Example Response COPY

```
{

    "auth-token":"authentication token"

}
```

To log out of the public API

Removes the authentication token issued when the user logged on and logs out the current user. Requires the user name and the authentication token.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/authentication/logout

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Request Parameters COPY

```
{“login”:”administrator”}
```

Example Response COPY

```
{"Status":"user administrator logged out successfully."}
```

To manage certificates

With certificate management operations, you can view, delete, import, and add certificates through the public API.

Get all certificates

Returns all certificates in the database.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Request Parameters: None

Example Response COPY


```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": null,
    "certificate": [
        {
            "name": "ent-root-ca",
            "description": "test description server 1",
            "validFrom": "2012-02-22",
            "validTo": "2017-02-21",
            "type": "chain",
            "isActive": false,
            "privateKey": "false",
            "ca": null,
            "id": 4656,
            "certDetails": {
                "signatureAlgo": "SHA1WithRSAEncryption",
```



```
"version": null,

"serialNum": "348237881800118418457268346483687164l3",

"issuerName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,

    "locality": null,

    "state": null,

    "country": null,

    "description": null

},

"subjectName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,

    "locality": null,
```



```
                    "state": null,
                    "country": null,
                    "description": null
                }
            }
        }
    ],
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Delete certificates

Deletes the specified certificates. Requires the certificate ID for each certificate to be deleted.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/publicapi/certificates

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Request Parameters COPY

```
{“certificateIds”:[“<certificate_id_1>”,”<certificate_id_2>”, ..., "<certificate_id_n>"]}
```

Import certificate as SAML certificate

Imports the specified certificate as a SAML certificate.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/certificate/saml

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters COPY

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'saml',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
```

```
        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```

Import certificate as server certificate

Imports the specified certificate as a server certificate.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/certificate/server

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters COPY


```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'none',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {
```

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```

Import certificate as listener certificate

Imports the specified certificate as an SSL listener certificate.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/certificate/listener

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters COPY


```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'listener',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
```

```
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Create certificate

Creates a self-signed certificate or a CSR request that requires a CA signature.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/csr

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Application/form_url_encoded

Request Parameters COPY

```
{
    "isSelfSign":true,
    "csrRequest":{
    "commonName":"your certificate name",
    "description":"certificate description",
    "org":"organization",
    "orgUnit":"organization unit",
    "locality":"location",
    "state":"CA",
    "country":"US",
    "isSelfSign":true
    },
"validDays":"60",
"keyLength":"1024",
"useAs":"none"
}
```

Example Response COPY

```
{
    status: 0
    message: "Success"
    csrRequest: ""
    apnsCheck: null
    certificate: null
    apnsCheckObj:
    {
    topicNameMismatch: false
    certExpired: false
    certNotYetValid: false
    malformed: false
    }
}
```

Export certificate

Downloads the specified certificate. The following table lists the parameters for this operation.

Parameter	Required	Description
id	Yes	The numeric certificate ID

password	Password associated with the certificate being exported.
exportPrivateKey	Flag indicating whether to export the private key.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/export

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "id": "300",
    "password": "1111",
    "exportPrivateKey": true
}
```

Example response: Displays the certificate string on successful request.

To manage keystores

You can import keystores through the public API.

Import a server keystore

Imports a server keystore.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/keystore/server

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters COPY

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
```

```
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Import SAML keystore

Imports a SAML keystore.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/keystore/saml

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Paramaters COPY

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
}
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
```

```
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```

Import APNs keystore

Imports an APNS keystore.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/keystore/apns

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters COPY

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':apns,
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Example Response COPY

```
{
    "status": 0,
```

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Import SSL listener keystore

Imports an SSL listener keystore.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/keystore/listener

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters COPY

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':"listener",
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
 uploadFile = <certificate file>
 uploadFile = <private key file>
```

Example Response COPY

```
{
    "status": 0,
```

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
"certificate": null,
"apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


To manage licenses

Lets you manage licenses through the public API.

Get license information

Lists information about all licenses.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
    status: 0
    message: "Success"
    cpLicenseServer: {
        serverAddress: "192.0.2.20"
        localPort: 0
        remotePort: 27000
        serverType: "remote"
        licenseType: "none"
        isServerConfigured: true
        gracePeriodLeft: 0
        isRestartLpeNeeded: null
        isScheduleNotificationNeeded: null
            licenseList: []
```

```
        {
            sadate: "2015.1210"
            notice: "Example Systems Inc."
            vendorString: ";LT=Retail;GP=720;UDM=U;LP=90;CL=STD,ADV,ENT;SA=1;ODP=0"
            licensesInUse: 0
            licensesAvailable: 102
            overdraftLicenseCount: 2
            p_E_M: "CXM_ENTU_UD"
            serialNumber: "cxmretailent1000user"
            licenseType: "Retail"
            expirationDate: "01-DEC-2015"
        }
        licenseNotification:
        {
            id: 1
            notificationEnabled: false
            notifyFrequency: 7
            notifyNumberDaysBeforeExpire: 60
            recepientList: ""
            emailContent: "License expiry notice"
```

```
        }

    }

}
```

Save license information

Saves all license information.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "serverAddress": "192.0.2.20",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": "remote",

    "licenseType": "none",

    "isServerConfigured": true,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": true,

    "isScheduleNotificationNeeded": true,
```

```
    "licenseList": [],
    "licenseNotification": {
        "id": 1,
        "notificationEnabled": true,
        "notifyFrequency": 20,
        "notifyNumberDaysBeforeExpire": 60,
        "recepientList": "justa.name123@example.com",
        "emailContent": "Licenseexpirynotice"
    }
}
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success"
}
```

Upload license file

Uploads the specified license file.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses/upload

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters: uploadFile = <license file to be uploaded>

Example Response COPY

```
{

   "status": 0,

   "message": "Success"

}
```

Activate license

Activates the specified license.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses/activate/{license type}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters: Append the license type to the activate license URL.

Example Response COPY

```
{

    "status": 0,

    "message": "Success"

    "cpLicenseServer": null

}
```

Remove all licenses

Removes all licenses.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses/remove

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "isConnected": null

}
```

Test license server

Performs a connectivity check on the license server.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses/testserver/

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "serverAddress": "192.0.2.7",
    "localPort": 0,
    "remotePort": 27000,
    "serverType": null,
    "licenseType": null,
    "isServerConfigured": null,
    "gracePeriodLeft": 0,
    "isRestartLpeNeeded": null,
    "isScheduleNotificationNeeded": null,
    "licenseList": [],
    "licenseNotification": null
}
```


Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "isConnected": true

}
```

Get earliest expiration date

Finds the license with the earliest expiration date.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses/getexpirationdate

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "expiredDate": 1448956800000,
    "daysBeforeExpire": 229,
    "daysInPOC": 0
}
```

To manage LDAP configurations

The following table lists the parameters used in LDAP configuration operations.

Parameter	Required	Description
primaryHost	Yes	Primary LDAP server IP address or host name. Input as IP address or FQDN.
secondaryHost	No	Secondary LDAP server IP address or host name. Input as IP address or FQDN.
port	Yes	LDAP server port number
username	Yes	Valid LDAP server user name
password	Yes	Password for username
userBaseDN	Yes	
lockoutLimit	No	
lockoutTime	No	

useSecure	No	
userSearchBy	Yes	Search for users by upn or samaccount
domain	Yes	Unique LDAP server domain name
domainAlias	Yes	Alias for the LDAP domain
globalCatalogPort	No	
gcRootContext	No	
groupBaseDN	Yes	
isDefault	No	Part of the GET response that indicates whether the LDAP configuration is the default.
name	No	Part of the GET response that is a unique identifier used to update or delete the LDAP configuration.

List LDAP configuration

Lists the entire LDAP configuration in XenMobile.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/ldap

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

    “result”: [

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"aaa@example.com","password":"1.pwd","userB

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"test@xmexample.com","password":"1.pwd","us

    ]

}
```

Add new LDAP configuration

Adds a new LDAP configuration. The domain name must be unique and cannot be the same as any other LDAP configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/ldap/msactivedirectory

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```

Example Response COPY

```
{

    “status”: 0,

    “message”: “LDAP configuration created”

}
```

Edit LDAP configuration

Edits an existing LDAP configuration with the exception that you cannot change the domain with the edit operation.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/ldap/msactivedirectory/{name}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "primaryHost":"192.0.2.7",
    "secondaryHost":"",
    "port":"389",
    "username":"aaa@example.com",
    "password":"1.pwd",
    "userBaseDN":"dc=example,dc=com",
    "groupBaseDN":"dc=example,dc=com",
    "lockoutLimit":"0",
    "lockoutTime":"1",
    "useSecure":"false",
    "userSearchBy":"upn",
    "domain":"example.com",
    "domainAlias":"exampleAlias",
    "globalCatalogPort":"0",
    "gcRootContext":""
}
```

Set default LDAP configuration

Sets the specified LDAP configuration as the default.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/ldap/default/{name}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Delete LDAP configuration

Deletes the specified LDAP configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/ldap/{name}

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

To manage NetScaler Gateway configurations

Lets you manage NetScaler Gateway configurations. The following table lists the parameters used in NetScaler Gateway operations.

Parameter	Required	Description
name	Yes	Unique NetScaler Gateway name
alias	No	
url	Yes	Publicly accessible URL for NetScaler Gateway
passwordRequired	Yes	
logonType	Yes	Valid values: domain-only, domain-token, domain-certificate, certificate-only, certificate-token, and token-only
callback	No	
default	Yes	Set to true or false when adding or editing a NetScaler Gateway configuration. If this parameter is not passed, the default is set to false.

id	No	Part of the GET response that is a unique identifier used to update or delete the NetScaler Gateway configuration.

List all NetScaler Gateway configurations

Lists the entire NetScaler Gateway configuration in XenMobile.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/netscaler

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
    “result”: [
        { "name":"displayName",
        "alias":"",
        "url":"https://externalURl.com",
        "passwordRequired":"false",
        "logonType":"domain",
        "default":"false","id":"",
        “callback”: [{“callbackUrl”:http://example.com,
        “ip”:”192.0.2.8”}]
        },
        { "name":"displayName",
        "alias":"",
```

```
        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false",

        "id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        }

    ]

}
```

Add new NetScaler Gateway configuration

Adds a new NetScaler Gateway configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/netscaler

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "name":"displayName",

    "alias":"",

    “default”:true, "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “callback”: [{“callbackUrl”:http://example.com,

    “ip”:”192.0.2.8”}]

}
```

Edit NetScaler Gateway configuration

Edit the specified NetScaler Gateway configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/netscaler/{id}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "name":"displayName",

    "alias":"",

    "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain",

    "default": true,

    "callback": [{"callbackUrl":http://ag.com,

    "ip":"192.0.2.8"}]

}
```

Delete NetScaler Gateway configuration

Delete the specified NetScaler Gateway configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/netscaler/{id}

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Set default NetScaler Gateway configuration

Set the specified NetScaler Gateway configuration as the default.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/netscaler/default/{id}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

To manage SMS and SMTP notification server configurations

You can add, edit, activate (set as default), and delete the SMS server and SMTP server configurations. The following table lists the parameters used with SMS server and SMTP server configuration operations.

Parameter	Required	Description
name	Yes	Unique SMS/SMTP configuration name.
serverType	No	Notification server type (SMS or SMTP) sent by the server in the GET request.
active	No	Indicates whether server is being used for notifications. Only one server can be active for each type.
id	No	Unique identifier used to update, delete, or activate the server.
description	No	Description of the server.
SMS parameters		
key	Yes	
secret	Yes	
virtualPhoneNumber	Yes	Must be in phone number format.
https	Yes	Default is false.
country	Yes	
carrierGateway	Yes	Default is false.
SMTP parameters		
secureChannelProtocol	Yes	The type of security protocol to use. Valid values are: None, SSL, and TLS. Default is none.

port	Yes	
authentication	Yes	Whether to use authentication. Valid values are true and false.
username	Yes, if authentication is true.	
password	Yes, if authentication is true.	
msSecurePasswordAuth	Yes	Default is false.
fromName	Yes	
fromEmail	Yes	
numOfRetries	No	An integer. Default is 5.
timeout	No	An integer. Default is 30.
maxRecipients	No	An integer. Default is 100.

List all SMS and SMTP servers

Lists all SMS and SMTP servers in XenMobile.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Accept – application/json

Example Response COPY

```
{

    “result”: [

        { "name":"serverName","serverType":"SMS,"active":"true","id":"10"},

        { "name":"serverName2","serverType":"SMTP,"active":"true","id":"10"},

        { "name":"serverName3","serverType":"SMS,"active":"false","id":"10"}

    ]

}
```

Get server details

Get details about the server by server ID.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/{id}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Accept – application/json

Example SMS Response COPY

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Example SMTP Response COPY

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.12",

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Add SMS server configuration

Add an SMS server configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/sms

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "name":"displayName",
    "description":"",
    "server":"192.0.2.9",
    "carrierGateway":"true",
    "country":"+93",
    "https":"false”,
    “key”: “123456”,
    "secret":"secretKey",
    "virtualPhoneNumber":"4085552222",
    "carrierGateway":"true"
}
```

Edit SMS server configuration

Edit the specified SMS server configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/sms/{id}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "name":"displayName",
    "description":"",
    "server":"192.0.2.9",
    "carrierGateway":"true",
    "country":"+93",
    "https":"false",
    “key”: “123456”,
    "secret":"secretKey",
    "virtualPhoneNumber":"4085552222",
    "carrierGateway":"true"
}
```

Add SMTP server configuration

Adds an SMTP server configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/smtp

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Edit SMTP configuration

Edit the specified SMTP configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/smtp/{id}

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    name":"displayName",

    "description":"Edited description",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Delete server configuration

Delete the specified SMS or SMTP server configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/{id}

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Set default SMS configuration

Set the specified SMS server configuration as the default.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/activate/sms/{id}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Set default SMTP configuration

Set the specified SMTP server configuration as the default.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/activate/smtp/{id}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

To manage local users and groups

You can manage local users and groups by using the following services.

Get all users

Get all local users.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
```

```
"status": 0,

"message": "Success",

"result": [

    {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"

        },

        "role": "ADMIN",

        "roles": null,

        "createdOn": "1/10/15 11:42 AM",

        "lastAuthenticated": "1/10/15 11:42 AM",

        "domainName": null,

        "adUser": false,

        "vppUser": false

    }
```



```
    ]

}
```

Get one user

Get the specified local user.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups/{name}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "result": {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"
```

```
            company = example
        },
        "role": "ADMIN",
        "roles": null,
        "createdOn": "1/10/15 11:42 AM",
        "lastAuthenticated": "1/10/15 11:42 AM",
        "domainName": null,
        "adUser": false,
        "vppUser": false
    }
}
```

Add user

Add a user with the specified attributes.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
        },
    "groups": [
        "MSP"
        ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

Example Response COPY

```
{
    "status": 0,
```

```
"message": "Success",

"user": {

    "userid": 0,

    "username": "justaname_XX",

    "password": "password",

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": null,

    "lastAuthenticated": null,

    "domainName": null,
```



```
        "adUser": false,

        "vppUser": false

    }

}
```

Update user

Update user attributes.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
        },
    "groups": [
        "MSP"
        ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

Example Response COPY

```
{
    "status": 0,
```

```
"message": "Success",

"user": {

    "userid": 108,

    "username": "justaname_XX",

    "password": null,

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": "3/27/15 1:10 PM",

    "lastAuthenticated": "3/27/15 1:10 PM",

    "domainName": null,
```



```
        "adUser": false,

        "vppUser": false

    }

}
```

Change user password

Reset a user's password; you can also change a user's password in the update local user call.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups/resetpassword

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "username": “administrator”,

    “password”: “newPassword”

}
```

Example Response COPY

```
Response Errors:

1250 – User id not found

1252 – Failed to reset the password

Password can also be changed in the update local user call.
```

Delete users

Delete the specified users.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups/resetpassword

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{ justaname XX }
```

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

Delete one user

Delete the specified user.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups/

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

Import provisioning file

Upload a file containing local user data. The file to be uploaded must be in .csv format. For more information on provisioning files, see Provisioning File Formats.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups/importprovisioningfile

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
importdata={"fileType:"user"}

uploadfile=<file to be uploaded.csv>
```

Example Response COPY

```
{

   "status": 0,

   "message": "Success",

   "user": null

}
```

To manage apps

You can manage apps with the following services.

Get all apps by filter

Get apps based on the specified filter parameters.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/application/filter

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on
Content type – application/json

Sample Request Data COPY

```
{
    "start": 0,
    "limit": 10,

    "applicationSortColumn": "name",
    "sortOrder": "DESC",
    "enableCount": false,
    "search": "Worx",
    "filterIds":"['application.deliverygroup#<DG_Name>@_fn_@app.dg','application.deliverygroup#<DG_Name>@_fn_@app.d
}
```

Sample Response Data COPY

```
{

  "status": 0,

  "message": "Success",

  "applicationListData": {

    "totalMatchCount": 2,

    "totalCount": 2,

    "appList": [{

      "id": 2,

      "name": "WorxNotes",

      "description": "Worx Notes Application",

      "createdOn": "6/7/16 3:55 PM",

      "lastUpdated": "6/7/16 5:11 PM",

      "disabled": false,

      "nbSuccess": 0,

      "nbFailure": 0,

      "nbPending": 0,

      "schedule": null,

      "permitAsRequired": true,

      "iconData": "iVBORw0KGgoAAAANSUhEUgAAAHgAAAB4CAYAAAA5ZDbSAAA.....",

      "appType": "MDX",
```



```
    "categories": ["Default"],
    "roles": null,
    "workflow": null,
    "vppAccount": null
  }, {
    "id": 1,
    "name": "Angry Bird",
    "description": "",
    "createdOn": "6/7/16 3:53 PM",
    "lastUpdated": "6/7/16 3:54 PM",
    "disabled": false,
    "nbSuccess": 0,
    "nbFailure": 0,
    "nbPending": 0,
    "schedule": null,
    "permitAsRequired": true,
    "iconData": "/9j/4AAQSkZJRgABAQEAAQABAAD/2wBDAAYEBQYFBAYGBQYHBwYIChA...",
    "appType": "App Store App",
    "categories": ["Default"],
    "roles": null,
```



```
        "workflow": null,
        "vppAccount": null
      }]
    }
}
```

Get mobile apps by container

Get mobile apps in the specified container.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/application/mobile/{containerId}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example response COPY

```
{
    "status": 0,
    "message": "Success",
    "result": {
        "id": 14,
        "name": "testApp",
        "description": "",
```

```
"createdOn": null,
"lastUpdated": null,
"disabled": false,
"nbSuccess": 0,
"nbFailure": 0,
"nbPending": 0,
"schedule": {
    "enableDeployment": true,
    "deploySchedule": "NOW",
    "deployScheduleCondition": "EVERYTIME",
    "deployDate": null,
    "deployTime": null,
    "deployInBackground": false
},
"iconData": "",
"appType": "MDX",
"categories": [
    "Default"
],
"roles": [],
```



```
"workflow": null,
"ios": {
    "displayName": "GoToMeeting",
    "description": "G2MW_IOS_5.3.3_075_01",
    "paid": false,
    "removeWithMdm": true,
    "preventBackup": true,
    "appVersion": "5.3.3.075",
    "minOsVersion": "",
    "maxOsVersion": "",
    "excludedDevices": "",
    "avppParams": null,
    "avppTokenParams": null,
    "rules": null,
    "appType": "mobile_ios",
    "uuid": "8e69d397-48bb-4f29-a95c-dd7b16665c1c",
   "id": 0,
    "store": {
        "rating": {
            "rating": 0,
```



```
            "reviewerCount": 0
        },
        "screenshots": [],
        "faqs": [],
        "storeSettings": {
            "rate": true,
            "review": true
        }
    },
    "policies": [
        {
            "policyName": "ReauthenticationPeriod",
            "policyValue": "480",
            "policyType": "integer",
            "policyCategory": "Authentication",
            "title": "Reauthentication period (minutes)",
            "description": "\nDefines the period before a user is challenged to authenticate again. ",
            "units": "minutes",
            "explanation": null
        }
```



```
},
{
    "policyName": "BlockJailbrokenDevices",
    "policyValue": "true",
    "policyType": "boolean",
    "policyCategory": "Device Security",
    "title": "Block jailbroken or rooted",
    "description": "\nIf On, the application is locked when the device is jailbroken or rooted.",
    "units": null,
    "explanation": null
},
{
    "policyName": "CertificateLabel",
    "policyValue": "",
    "policyType": "string",
    "policyCategory": "Network Access",
    "title": "Certificate label",
    "description": "\nThe label for the certificate.\n                                                    Default value is er
    "units": null,
    "explanation": null
```



```
                }

            ]

        },

        "android": null,

        "android_knox": null,

        "android_work": null,

        "windows": null,

        "windows_tab": null

    }

}
```

Get public store apps by container

Get public store apps from the specified container.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/application/mobile/appstore/{containerId}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Delete app container

Delete the specified app container.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/application/{containerId}

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

To manage delivery group configurations

You can manage delivery group configurations with the following services.

Get delivery groups by filter

Use the specified filter parameters to get delivery groups.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups/filter

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
{
   "start": 1,
   "sortOrder": "DESC",
   "deliveryGroupSortColumn": "id",
   “limit”:10,
   "search": "add"
}
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
```

```
"dgListData": {

"totalMatchCount": 7,

"totalCount": 10,

"dgList": [

{

"id": null,

"name": "add delivery group 6.0",

"description": "testing add delivery group 6.0",

"groups": [[{

{

"id": 1null,

"userListId": 1null,

"name": "MSPTESTLOCALGROUP",

"uniqueName": "MSPTESTLOCALGROUP",

"uniqueId": "MSPTESTLOCALGROUP",

"domainName": "local",

"primaryToken": 0null,

}"objectSid": null

],},

{
```



```
        "id": null,
        "userListId": null,
        "name": "AC08EP61S75",
        "uniqueName": "AC08EP61S75",
        "uniqueId": "AC08EP61S75",
        "domainName": "local",
        "primaryToken": null,
        "objectSid": null
    }],
    "users": [{
        "uniqueName": null,
        "domainName": "local",
        "name": null,
        "objectId": "shankar",
        "customProperties": {
            "name": "value",
            "name1": "value1"
        },
        "uniqueId": "shankar"
    }],
```



```
"zoneId": null,

"zoneDomain": null,

"rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId

"disabled": false,

"lastUpdated": 1427144713353,

"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

    {

        "name": "Web Link",

        "required": false

    },

    {

        "name": "GoogleApps_SAML",

        "required": true

    }

],

"devicePolicies": [

    "test terms conditions"

]
```



```
        ],
        "smartActions": [
            "shankar ganesh"
        ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    },
    {
        "id": null,
        "name": "add delivery group 5.0",
        "description": "testing add delivery group 5.0",
        "groups": [
            {
                "id": 1,
                "userListId": 1,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
                "domainName": "local",
```



```
                "primaryToken": 0

            }

        ],

        "zoneId": null,

        "zoneDomain": null,

        "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId

        "disabled": false,

        "lastUpdated": 1426891345698,

        "anonymousUser": true,

        "roledefLangVersionId": 1,

        "applications": [

            {

                "name": "GoogleApps_SAML",

                "required": true

            },

            {

                "name": "Web Link",

                "required": false

            }

        ],
```



```
                    "devicePolicies": [

                        "test terms conditions"

                    ],

                    "smartActions": [

                        "shankar ganesh"

                    ],

                    "nbSuccess": 0,

                    "nbFailure": 0,

                    "nbPending": 0

                }

            ]

        }



}
```


Get delivery group by name

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups/{name}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY


```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": null,
        "name": "AllUsers",
        "description": "default role",
        "groups": [],
        "zoneId": null,
        "zoneDomain": null,
        "rules": null,
        "disabled": false,
        "lastUpdated": null,
        "anonymousUser": false,
        "roledefLangVersionId": 1,
        "applications": [
            {
                "name": "test mdx",
                "required": false
            },
```



```
        {
            "name": "test all",
            "required": false
        },
        {
            "name": "justa test",
            "required": false
        },
        {
            "name": "test enterprise",
            "required": false
        },
        {
            "name": "name test",
            "required": false
        }
    ],
    "devicePolicies": [
        "test terms conditions"
    ],
```



```
        ],
        "smartActions": [
            "justa name"
        ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    }
}
```

Edit delivery group

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
{
  "name": "temp3",
  "description": "temp3 desc",
  "applications": [
```

```
{

            "name": "TESTAPP",

             "priority": -1,

             "required": false

                    }      ],

    "devicePolicies": [

        {

             "name":"test terms conditions",

             "priority":-1

         }

      ],

    "smartActions": [

        {

           "name":"Smart Action Name 1",

           "priority":-1

         }

      ],

  "groups": [

     {

  "uniqueName": "AC08EP61S75",

       "domainName": "local",

       "name": "AC08EP61S75",

       "objectSid": "AC08EP61S75",
```



```
"uniqueId": "AC08EP61S75",

"customProperties": {

    "gr1": "gr1",

    "gr2": "gr2"

  }

    }

  ],

  "users": [

    {

      "uniqueName": "testuser",

      "domainName": "local",

      "name": " testuser ",

      "objectId": " testuser "

    }

  ],

  "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\" te

}
```


Example Response COPY


```
{
      "status": 0,
      "message": "Success",
"role": {
            "id": null,
            "name": "temp4",
            "description": "temp4 desc",
            "zoneId": null,
            "zoneDomain": null,
            "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value
            "disabled": false,
            "lastUpdated": null,
            "anonymousUser": false,
            "roledefLangVersionId": null,
            "applications": [
                  {
                  "name": "TESTAPP2",
                  "priority": -1,
```



```
                "required": false

            },

{

                "name": "TESTAPP2",

                "priority": -1,

                "required": false

            }

            ],

            "devicePolicies": [

                {

                "name": "TestPolicy1",

                "priority": -1

            },

{

                "name": "TestPolicy",

                "priority": -1

            }

            ],

            "smartActions": [

{
```

```
                "name": "TestAction2",

                "priority": -1

            },

{

                "name": "TestAction3",

                "priority": -1

            }

        ],

            "nbSuccess": 0,

            "nbFailure": 0,

            "nbPending": 0,

            "groups": [{

                  "uniqueName": "AC08EP61S75",

                 "domainName": "local",

                "name": "AC08EP61S75",

                 "objectSid": "AC08EP61S75",

                "uniqueId": "AC08EP61S75",

                "customProperties": {

                  "gr1": "gr1",

                    "gr2": "gr2"
```



```
            }

        }],

        "users": [{

            "uniqueName": " tempuser ",

            "domainName": "local",

            "name": " tempuser ",

            "objectId": " tempuser ",

            "customProperties": null,

            "uniqueId": " tempuser "

        }]


    }
```

Add delivery group

Adds a delivery group.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
{

  "name": "temp3",

  "description": "temp3 desc",

  "applications": [

{

            "name": "TESTAPP",

             "priority": -1,

             "required": false

                    }     ],

    "devicePolicies": [

        {

            "name":"test terms conditions",

            "priority":-1

         }

      ],

    "smartActions": [

        {

           "name":"Smart Action Name 1",

           "priority":-1

         }

      ],

  "groups": [

    {

  "uniqueName": "AC08EP61S75",
```



```
        "domainName": "local",

        "name": "AC08EP61S75",

        "objectSid": "AC08EP61S75",

"uniqueId": "AC08EP61S75",

"customProperties": {

     "gr1": "gr1",

     "gr2": "gr2"

  }}

  ],

  "users": [

    {

      "uniqueName": "testuser",

      "domainName": "local",

      "name": "testuser",

      "objectId": "testuser"

    }

  ],

  "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"te

}
```


Example Response COPY


```
{
    "status": 0,
    "message": "Success",
"role": {
        "id": null,
        "name": "temp4",
        "description": "temp4 desc",
        "zoneId": null,
        "zoneDomain": null,
        "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value
        "disabled": false,
        "lastUpdated": null,
        "anonymousUser": false,
        "roledefLangVersionId": null,
        "applications": [
            {
            "name": "TESTAPP2",
            "priority": -1,
```



```
                "required": false
            },
{
                "name": "TESTAPP2",
                "priority": -1,
                "required": false
            }
            ],
            "devicePolicies": [
                {
                "name": "TestPolicy1",
                "priority": -1
            },
{
                "name": "TestPolicy",
                "priority": -1
            }
            ],
            "smartActions": [
{
```

```
{
                "name": "TestAction2",
                "priority": -1
            },
{
                "name": "TestAction3",
                "priority": -1
            }
        ],
            "nbSuccess": 0,
            "nbFailure": 0,
            "nbPending": 0,
            "groups": [{
                    "uniqueName": "AC08EP61S75",
          "domainName": "local",
          "name": "AC08EP61S75",
          "objectSid": "AC08EP61S75",
"uniqueId": "AC08EP61S75",
"customProperties": {
      "gr1": "gr1",
```



```
        "gr2": "gr2"

    }        }],

            "users": [{

                "uniqueName": " tempuser ",

                "domainName": "local",

                "name": " tempuser ",

                "objectId": " tempuser ",

                "customProperties": null,

                "uniqueId": " tempuser "

            }]


      }
```

Delete delivery group

Delete specified delivery groups.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
[ "add delivery group 11.0" ]
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "roleNames": [
        "add delivery group 11.0"
    ]
}
```

Enable or Disable Delivery Group

Enable or disable the specified delivery groups.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups/{delivery group name}/{enable/disable}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "roleName": "AllUsers"

}
```

To manage server properties

You can manage XenMobile server properties by using the following services.

Get all server properties

Get all current XenMobile server properties.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": [

        {

            "id": 1,

            "name": "ios.mdm.pki.ca-root.certificatefile",
```



```
        "value": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayName": "ios.mdm.pki.ca-root.certificatefile",

        "description": "",

        "defaultValue": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayFlag": false,

        "editFlag": true,

        "deleteFlag": false,

        "markDeleted": false

    } ,

    {

        "id": 2,

        "name": "ios.mdm.https.host",

        "value": "192.0.2.4",

        "displayName": "ios.mdm.https.host",

        "description": "",

        "defaultValue": "192.0.2.4",

        "displayFlag": false,

        "editFlag": false,

        "deleteFlag": false,
```



```
            "markDeleted": false

        },

        {

            "id": 3,

            "name": "ios.mdm.enrolment.checkRemoteAddress",

            "value": "false",

            "displayName": "iOS Device Management Enrollment - Check Remote Address",

            "description": "",

            "defaultValue": "false",

            "displayFlag": true,

            "editFlag": true,

            "deleteFlag": false,

            "markDeleted": false

        },

    ]

}
```


Get server properties by filter

Get server properties using the specified filter parameters.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties/filter

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "start": 0,
    "limit": 1000,
    "orderBy": "name",
    "sortOrder": "desc",
    "searchStr": "justaserver1"
}
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 154,
            "name": "justaserver123",
```

```
            "value": "justaserver1",

            "displayName": "justarserver display name",

            "description": "justaserver description",

            "defaultValue": "justaserver1",

            "displayFlag": true,

            "editFlag": true,

            "deleteFlag": true,

            "markDeleted": false

        }

    ]

}
```

Add server property

Add the specified server property.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "name": "Key 2",

    "value": "Value 1",

    "displayName": "Display Name 1",

    "description": "Description 1"

}
```

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

Edit server properties

Edit the specified server property.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 2",
    "description": "Description 2"
}
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Reset server properties

Reset the specified server properties.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties/reset

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "names": [,

        "justaname7"

        ]

}
```

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

Delete server properties

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "justaname3",
    "justaname4"
}
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

To manage devices

You can manage devices in XenMobile by using the following services.

Get Devices by Filter

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/filter

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

All **Request Parameters** are optional.

Valid values for **sortOrder** are: ASC, DSC, and DESC.

Valid values for **sortColumn** are: ID, SERIAL, IMEI, ACTIVESYNCID, WIFIMAC, BLUETOOTHMAC, OSFAMILY, SYSTEM_OEM, SYSTEM_PLATFORM, SYSTEM_OS_VERSION, DEVICE_PROPERTY, LASTAUTHDATE, INACTIVITYDAYS,ISACTIVE, LASTUSER, BLCOMPLIANT, WLCOMPLIANT, RLCOMPLIANT, MANAGED, SHAREABLE, and BULKPROFILESTATUS.

Request Parameters COPY

```
{
   "start": "0-999",
   "limit": "0-999",
   "sortOrder": "ASC",
   "sortColumn": "ID",
   "search": "Any search term",
   "enableCount": "false",
   "constraints": "{'constraintList':[{'constraint':'DEVICE_OS_FAMILY','parameters':[{'name':'osFamily','type':'STRING','value':'iO
   "filterIds": "['group#/group/MSP@_fn_@normal']"
}
```

Example Response COPY

```
{
   "id": "1-9999999",
```

```
"jailBroken": "true/false",

"managed": "true/false",

"gatewayBlocked": "true/false",

"deployFailed": "1-999",

"deployPending": "1-999",

"deploySuccess": "1-999",

"mdmKnown": "true/false",

"mamRegistered": "true/false",

"mamKnown": "true/false",

"userName": "user name",

"serialNumber": "serial number",

"imeiOrMeid": "IMEI/MEID",

"activeSyncId": "Active sync ID",

"wifiMacAddress": "WiFi MAC address",

"blueToothMacAccress": "Bluetoothi MAC address",

"devicePlatform": "Device platform",

"osVersion": "Operating system version of the device",

"deviceModel": "Device model information",

"lastAccess": "Timestamp when the device was last accessed",
```



```
    "inactivityDays": "Number of days device has been inactive",
    "shareable": "Flag indicating if the device is shareable",
    "sharedStatus": "Get shareable status of the device",
    "depRegistered": "Flag indicating if the device is DEP registered",
    "deviceName": "Name of the device",
    "deviceType": "Phone/Tablet",
    "productName": "Product name",
    "platform": "Platform of the device"
}
```

Get Devices by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/{device_id}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "device": {
  "htcMdm": true,
```

```
"managedByZMSP": true,

"serialNumber": "string",

"id": 0,

"applications": [

 {

  "resourceType": "APP_NATIVE",

  "resourceTypeLabel": "string",

  "packageInfo": "string",

  "statusLabel": "string",

  "lastUpdate": 0,

  "status": "SUCCESS",

  "name": "string"

 }

],

"smartActions": [

 {

  "resourceType": "APP_NATIVE",

  "resourceTypeLabel": "string",

  "packageInfo": "string",

  "statusLabel": "string",
```



```
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
   }
 ],
 "platform": "string",
 "osFamily": "WINDOWS",
 "nbSuccess": 0,
 "nbFailure": 0,
 "nbPending": 0,
 "deliveryGroups": [
   {
    "statusLabel": "string",
    "linkey": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
   }
 ],
 "lastAuthDate": 0,
```



```
"sharedStatus": "INACTIVE",

"managed": true,

"smgStatus": "ACCESS_ALLOWED",

"mdmKnown": true,

"mamKnown": true,

"mamRegistered": true,

"lastUsername": "string",

"imei": "string",

"activesyncid": "string",

"wifimac": "string",

"bluetoothmac": "string",

"inactivityDays": 0,

"shareable": true,

"bulkProfileStatus": "NO_BULK",

"deviceType": "string",

"softwareInventory": [

 {

   "version": "string",

   "blacklistCompliant": true,

   "suggestedListCompliant": true,
```



```
    "packageInfo": "string",
    "installCount": 0,
    "installTimeStamp": 0,
    "author": "string",
    "container": 0,
    "name": "string",
    "size": 0
  }
],
"deviceActions": [
  {
    "actionType": "WIPE",
    "failedTime": 0,
    "doneTime": 0,
    "askedTime": 0
  }
],
"managedSoftwareInventory": [
  {
    "version": "string"
```



```
    "blacklistCompliant": true,
    "suggestedListCompliant": true,
    "packageInfo": "string",
    "installCount": 0,
    "installTimeStamp": 0,
    "author": "string",
    "container": 0,
    "name": "string",
    "size": 0
  }
],
"policies": [
  {
    "resourceType": "APP_NATIVE",
    "resourceTypeLabel": "string",
    "packageInfo": "string",
    "statusLabel": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
```



```
    "name": "string"
   }
  ],
  "active": true,
  "xmlId": "string",
  "deviceUsers": [
   {
    "user": {
     "displayName": "string",
     "id": 0,
     "xmlId": "string",
     "properties": [
      {
       "displayName": "string",
       "id": 0,
       "b64": true,
       "group": "string",
       "name": "string",
       "value": "string"
      }
```



```
      ]

    },

    "lastAuthDate": 0,

    "prevAuthDate": 0,

    "userLogin": "string"

  }

],

"packageStates": [

  {

    "packageName": "string",

    "packageId": 0,

    "statusLabel": "string",

    "date": 0,

    "status": "PENDING"

  }

],

"pushState": "ENQUEUED",

"pushStateLabel": "string",

"lastPushDate": 0,

"lastSentNotification": 0,
```



```
"lastRepliedNotification": 0,

"strongId": "string",

"lastSoftwareInventoryTime": 0,

"firstConnectionDate": 0,

"lastIOSProfileInventoryTime": 0,

"lastUser": {

 "displayName": "string",

 "id": 0,

 "xmlId": "string",

 "properties": [

  {

   "displayName": "string",

   "id": 0,

   "b64": true,

   "group": "string",

   "name": "string",

   "value": "string"

  }

 ]

},
```



```
"blacklistCompliant": true,

"suggestedListCompliant": true,

"requiredListCompliant": true,

"devicePropertiesTimestamp": 0,

"revoked": true,

"mamDeviceId": "string",

"deviceToken": "string",

"typeInst": 0,

"appLock": true,

"appWipe": true,

"mamReady": true,

"validCertificates": [

 {

   "credentialProviderId": "string",

   "type": "string",

   "issuerName": "string",

   "startDate": 0,

   "endDate": 0,

   "revoked": true,

   "certificateNumber": "string"
```



```
    "certificateNumber": "string"
  }
 ],
 "revokedCertificates": [
  {
    "credentialProviderId": "string",
    "type": "string",
    "issuerName": "string",
    "startDate": 0,
    "endDate": 0,
    "revoked": true,
    "certificateNumber": "string"
  }
 ],
 "authorizeEnabled": true,
 "revokeEnabled": true,
 "lockEnabled": true,
 "cancelLockEnabled": true,
 "unlockEnabled": true,
 "cancelUnlockEnabled": true,
```



```
"containerLockEnabled": true,

"cancelContainerLockEnabled": true,

"containerUnlockEnabled": true,

"cancelContainerUnlockEnabled": true,

"containerPwdResetEnabled": true,

"cancelContainerPwdResetEnabled": true,

"wipeEnabled": true,

"cancelWipeEnabled": true,

"clearRestrictionsEnabled": true,

"cancelClearRestrictionsEnabled": true,

"corpWipeEnabled": true,

"cancelCorpWipeEnabled": true,

"sdCardWipeEnabled": true,

"cancelSdCardWipeEnabled": true,

"locateEnabled": true,

"cancelLocateEnabled": true,

"enableTrackingEnabled": true,

"disableTrackingEnabled": true,

"disownEnabled": true,

"activationLockBypassEnabled": true,
```



```
"ringEnabled": true,

"cancelRingEnabled": true,

"newPinCode": "string",

"oldPinCode": "string",

"lockMessage": "string",

"resetPinCode": true,

"scanTime": "string",

"screenSharingPwd": "string",

"iosprofileInventory": [

 {

  "iosConfigInventories": [

   {

    "description": "string",

    "type": "string",

    "organization": "string",

    "identifier": "string",

    "name": "string"

   }

  ],

  "description": "string",
```



```
    "organization": "string",
    "managed": true,
    "identifier": "string",
    "receivedDate": 0,
    "encrypted": true,
    "name": "string"
  }
],
"iosprovisioningProfileInventory": [
  {
    "managed": true,
    "uuid": "string",
    "expiryDate": 0,
    "name": "string"
  }
],
"erasedMemoryCard": true,
"gpsCoordinates": [
  {
    "gpsTimestamp": 0
```



```
    "gpsTimestamp": 0
  }
],
"lastGpsCoordinate": {
  "gpsTimestamp": 0
},
"gpsFilterStartDate": 0,
"gpsFilterEndDate": 0,
"wipePinCode": "string",
"lockPhoneNumber": "string",
"dstDevIdUsed": true,
"dstValue": "string",
"smartActionsFailure": true,
"policiesFailure": true,
"applicationsFailure": true,
"touchdownProperties": [
  {
    "category": "string",
    "name": "string",
    "value": "string"
```

```
  }
],
"appUnwipeEnabled": true,
"requestMirroringEnabled": true,
"cancelRequestMirroringEnabled": true,
"stopMirroringEnabled": true,
"cancelStopMirroringEnabled": true,
"knownByZMSP": true,
"wipeDeviceFlag": true,
"lockDeviceFlag": true,
"appWipeEnabled": true,
"appLockEnabled": true,
"appUnlockEnabled": true,
"bulkEnrolled": true,
"nbAvailable": 0,
"hasContainer": true,
"connected": true,
"properties": [
  {
    "displayName": "string",
```

```
      "id": 0,
      "b64": true,
      "group": "string",
      "name": "string",
      "value": "string"
    }
  ]
 }
}
```


Get Device Apps by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/{device_id}/apps

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "applications": [

  {

   "resourceType": "APP_NATIVE",

   "resourceTypeLabel": "string",

   "packageInfo": "string",

   "statusLabel": "string",

   "lastUpdate": 0,

   "status": "SUCCESS",

   "name": "string"

  }

 ]

}
```


Get Device Actions by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/{device_id}/actions

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY


```
{
 "status": 0,
 "message": "string",
 "actions": [
  {
   "resourceType": "APP_NATIVE",
   "resourceTypeLabel": "string",
   "packageInfo": "string",
   "statusLabel": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```


Get Device Delivery Groups by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/{device_id}/deliverygroups

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deliveryGroups": [
  {
   "statusLabel": "string",
   "linkey": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```

Get Managed Software Inventory by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/{device_id}/managedswinventory

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY


```
{
 "status": 0,
 "message": "string",
 "softwareInventory": [
  {
   "version": "string",
   "blacklistCompliant": true,
   "suggestedListCompliant": true,
   "packageInfo": "string",
   "installCount": 0,
   "installTimeStamp": 0,
   "author": "string",
   "container": 0,
   "name": "string",
   "size": 0
  }
 ]
}
```


Get Policies by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/{device_id}/policies

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "policies": [

  {

   "resourceType": "APP_NATIVE",

   "resourceTypeLabel": "string",

   "packageInfo": "string",

   "statusLabel": "string",

   "lastUpdate": 0,

   "status": "SUCCESS",

   "name": "string"

  }

 ]

}
```


Get Software Inventory by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/{device_id}/softwareinventory

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY


```
{
 "status": 0,
 "message": "string",
 "softwareInventory": [
  {
   "version": "string",
   "blacklistCompliant": true,
   "suggestedListCompliant": true,
   "packageInfo": "string",
   "installCount": 0,
   "installTimeStamp": 0,
   "author": "string",
   "container": 0,
   "name": "string",
   "size": 0
  }
 ]
}
```


Get GPS Coordinates by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/locations/{device_id}

Query Parameters:

startDate – the start date for the coordinate filter
endDate – the end date for the coordinate filter

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceCoordinates": {

  "deviceCoordinateList": {

   "deviceCoordinateList": [

    {

     "gpsTimestamp": 0

    }

   ],

   "startDate": 0,

   "endDate": 0

  }

}
```

Send Notification to a List of Devices or Users

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/notify

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
{
 "smtpFrom": "Test",
 "to": [
  {
   "deviceId": "1",
   "email": "user@test.com",
   "osFamily": "iOS",
   "serialNumber": "F7NLX6WDF196",
   "smsTo": "+123456676",
   "token": {
    "type": "apns",
     "value": "dfb2fb351a4fb068e40858ecad572e317e6c39b4fa7de6fb29ea1ad7e2254499"
   }
  }
 ],
 "smtpSubject": "This is test subject",
 "smtpMessage": "This is test message",
 "smsMessage": "This is test message",
 "agentMessage": "This is test message",
 "sendAsBCC": "true",
```



```
"smtp": "true",

"sms": "true",

"agent": "true",

"templateId": "-1",

"agentCustomProps": {

 "sound": "Casino.wav"

}
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "notificationRequests": {

  "smtpNotifRequestId": 0,

  "smsNotifRequestId": 0,

  "smsGatewayNotifRequestId": 0,

  "apnsAgentNotifRequestId": 0,

  "shtpAgentNotifRequestId": 0

 }

}
```

Authorize a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/authorize

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Apply Activation Lock Bypass on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/activationLockBypass

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Apply App Lock on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/appLock

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Apply App Wipe on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/appWipe

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Apply Container Lock on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/containerLock

Query Parameters: newPinCode – the PIN code for the Android container

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Container Lock on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/containerLock/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Apply Container Unlock on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/containerUnlock

Query Parameters: newPinCode – the PIN code for the Android container

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Container Unlock on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/containerUnlock/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Reset Container Password on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/containerPwdReset

Query Parameters: newPinCode – the PIN code for the Android container

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Reset Container Password on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/containerPwdReset/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Disown a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/disown

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Locate a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/locate

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel Locate a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/locate/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Apply GPS Tracking on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/track

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel GPS Tracking on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/track/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Lock a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/lock

Query Parameters:

newPinCode – PIN code must be between 4 and 16 characters for Android and Symbian devices. PIN code must be 4 digits for Windows devices

resetPinCode – add a reset pin code request to the lock request. Available only for Windows phone 8.1
lockMessage – add a message to the lock request. Available only for iOS 7 and later
phoneNumber – add a phone number to the lock request. Available only for iOS 7 and later

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Lock of a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/lock/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Unlock a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/unlock

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Unlock of a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/unlock/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Deploy a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/refresh

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Request AirPlay Mirroring on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/requestMirroring

Query Parameters:

dstName – destination name, as either destination name or destination device ID
dstDevId – MAC address for destination device, as either destination name or destination device ID

scanTime – number of seconds to scan
screenSharingPwd – password for screen sharing

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Request for AirPlay Mirroring on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/requestMirroring/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Stop AirPlay Mirroring on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/stopMirroring

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Stop AirPlay Mirroring on a List of Devcies

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/stopMirroring/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Clear All Restrictions on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/restrictions/clear

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Clear All Restrictions on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/restrictions/clear/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Revoke a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/revoke

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Ring a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/ring

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel Ringing a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/ring/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Wipe a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/wipe

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel Wipe of a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/wipe/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Selectively Wipe a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/selwipe

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel Selectively Wiping a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/selwipe/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Wipe the SD Cards on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/sdcardwipe

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel Wiping SD Cards on a List of Devices

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/sdcardwipe/cancel

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
[1,2]
```

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Get All Known Properties on a Device

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/knownProperties

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY


```
{
 "status": 0,
 "message": "string",
 "knownProperties": {
  "knownProperties": {
   "knownPropertyList": [
    {
     "name": "string",
     "type": "STRING",
     "displayName": "string",
     "group": "EVERYWAN",
     "groupLabel": "string"
    }
   ]
  }
}
```


Get All Used Properties on a Device

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/usedProperties

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "deviceUsedPropertiesList": {
  "deviceUsedProperties": {
   "deviceUsedPropertiesParameters": [
    {
     "name": "string",
     "type": "STRING",
     "displayName": "string"
    }
   ]
  }
 }
}
```

Get All Device Properties by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/properties/{deviceId}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
 "status": 0,
 "message": "string",
 "devicePropertiesList": {
  "deviceProperties": {
   "startIndex": 0,
   "devicePropertyParameters": [
    {
     "name": "string",
     "value": "string",
     "id": 0,
     "displayName": "string",
     "group": "string",
     "b64": true
    }
   ],
```

```
    "totalCount": 0
  }
 }
}
```

Update All Device Properties by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/properties/{deviceId}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
{
  "properties": [
    {
      "name": "ACTIVE_ITUNES",
      "value": "0"
    }
  ]
}
```

Example Response COPY

```
{

 "status": 0,

 "message": "string"

}
```

Add or Update a Device Property by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/properties/{deviceId}

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Request COPY

```
{

 "name": "PROPERTY_NAME",

 "value": "PROPERTY_VALUE"

}
```

Example Response COPY

```
{
 "status": 0,
 "message": "string"
}
```

Delete a Device Property by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/properties/{deviceId}

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
 "status": 0,
 "message": "string"
}
```

Get iOS Device MDM Status by Device ID

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/mdmStatus/{deviceId}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "deviceMdmStatus": {

  "deviceMdmStatusParameters": {

     "pushState": "ENQUEUED",

     "lastPushDate": 0,

     "lastRepliedNotification": 0,

     "lastSentNotification": 0,

     "pushStateLabel": "string"

   }

 }

}
```

Generate PIN code

URL: https://<host-name>:<port-number>/xenmobile/api/v1/device/pincode/generate

Query Parameters: pinCodeLength – the length of the requested pin code

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

 "status": 0,

 "message": "string",

 "pinCode": {

  "answer": "string"

 }

}
```


XenMobile SOAP APIs

Nov 08, 2016

> **Important**
>
> The SOAP APIs for XenMobile are deprecated. Please use the REST APIs instead. For information, see XenMobile REST API Reference.

You can use the following SOAP web services APIs in XenMobile for mobile device management. You can download the APIs and SDKs for XenMobile from the XenMobile Developer Community site.

Web Service Definition Language (WSDL) name	Calls
EveryWanDevice	addDevice
	addDevice
	authenticateUser
	authorize
	canCreateUser
	clearDeploymentHisto
	corporateDataWipeDevice
	createUser
	deploy
	deviceExists
	disableTrackingDevice
	enableTrackingDevice
	findDeviceByUdid

getAllDevices

getDeploymentHisto

getDeploymentHisto

getDeviceInfo

getDeviceInformationForUser

getDeviceProperties

getLastUser

getManagedStatus

getMasterKeyList

getSoftwareInventory

getStrongID

getUserDevices

isEnforceSSL

isEnforceStrongAuthentication

locateDevice

lockDevice

putDeviceProperties

registerDeviceForUser

removeDevice

resetDeploymentState

	revoke
	unlockDevice
	wipeDevice
	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	browseOtp
	createOtp
	getAvailableEnrollmentModes
	getOtpInfo
	revokeOtp
	triggerNotification

XenMobile Mail Manager 10.x

Aug 23, 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 and 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]

About XenMobile Mail Manager 10

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

About XenMobile Mail Manager 10

Jan 03, 2017

Known Issues

- The installed XenMobile Mail Manager version always displays as 8.5 during upgrade to XenMobile Mail Manager 10; however, the upgrade to XenMobile Mail Manager occurs. [#539520]
- Reporting of "devices found" in the minor snapshot may be confusing. The same device or devices may be reported as "new" in the successive minor snapshot summaries when the minor snapshots are run subsequent to the start of a major snapshot.
- XenMobile Mail Manager might apply local access control rules only to the first 1000 users of an Active Directory group even if the group contains more than 1000 users.

Fixed Issues

Power Shell/Exchange Management

In certain Microsoft Exchange environments (primarily Office 365), a restriction is placed on XenMobile Mail Manager that effectively limits bandwidth, preventing an app from issuing any PowerShell requests or commands. You can now use an alternate PowerShell cmdlet pathway in the Exchange configuration tab, which puts XenMobile Mail Manager into an alternate snapshot mode; this mode bypasses the original data path.

A new flag enables you to expose the AllowRedirection flag for non-Microsoft Office 365 environments. Use the Microsoft Exchange configuration tab to enable this flag.

Rules Management

LDAP local rules now support an indiscriminate number of groups for large Active Directory environments.

XenMobile duplicates device information for WorxMail clients. (**Note**: The name for WorxMail changed to Secure Mail in version 10.4.) Resolving this issue requires that you enable regular expression support in the Managed Service Provider (MSP) portion of XenMobile Mail Manager; doing so filters the record sets returned to XenMobile. Devices matching the filter are not returned to XenMobile.

MSP

Users who are removed from the Blackberry Enterprise Server (BES) database are now removed from the local database.

UI

You can now use a progress dialog class for scenarios in which a persistent process takes place. In such a process, XenMobile Mail Manager sends users feedback and provides them with an opportunity to cancel where applicable.

The default value for new Microsoft Exchange instances is now set to Shallow.

Installer

Components referring to Zenprise have been changed to reflect XenMobile Mail Manager.

The installer hangs when it fails to find the installation path.

Support binaries and scripts now reside in the Support folder after installation.

In the Windows Start menu, XenMobile Mail Manager shortcuts now reside in the \Citrix\XenMobile Mail Manager folder.

Support

The Support model provides the ability to enable troubleshooting functionality through the addition of a config.xml file. You can use this file to help Citrix troubleshoot problems. At this release of XenMobile Mail Manager, this functionality only applies to the Microsoft Exchange configuration Add and Edit screens.

Note: You can also enable this troubleshooting functionality by holding the Shift key when opening the Configure utility.

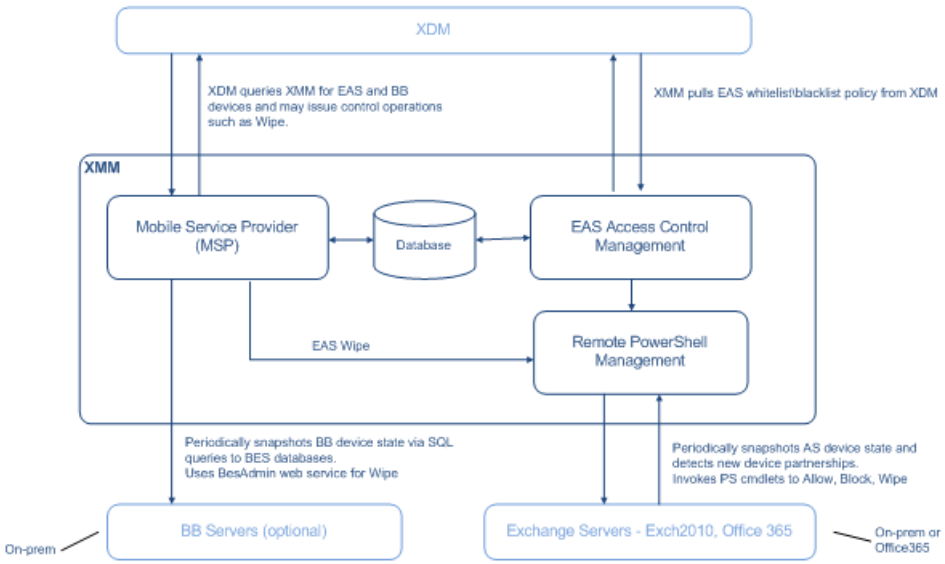
Logging

Error messages returned from PowerShell now have a GUID associated with them. Use this value to control what appears in the Snapshot History detail tab.

Architecture

Aug 12, 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

Dec 23, 2016

The following minimum system requirements are required to use XenMobile Mail Manager:

- Windows Server 2008 R2 (must be an English-based server)
- Microsoft SQL Server 2008, SQL Server 2012, SQL Server 2016, SQL Server Express 2008, SQL Server 2012, or Microsoft SQL Server 2012 Express LocalDB
- Microsoft .NET Framework 4.5
- Blackberry Enterprise Service, version 5 (optional)

Minimum supported versions of Microsoft Exchange Server

- Microsoft Office 365
- Exchanger Server 2016
- Exchanger 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 them 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. Once the connection limit is reached, XenMobile Mail Manager will not be able to connect to the 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's 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
- 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 admin has the requisite privileges.
- Exchange has many throttling policies. One of them controls how many concurrent PowerShell connections are allowed per user. The default number of simultaneous connections allowed for a user is 3 on Office 365. Once the connection limit is reached, XenMobile Mail Manager will not be able to connect to the 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.

Installing and Configuring

Jan 05, 2017

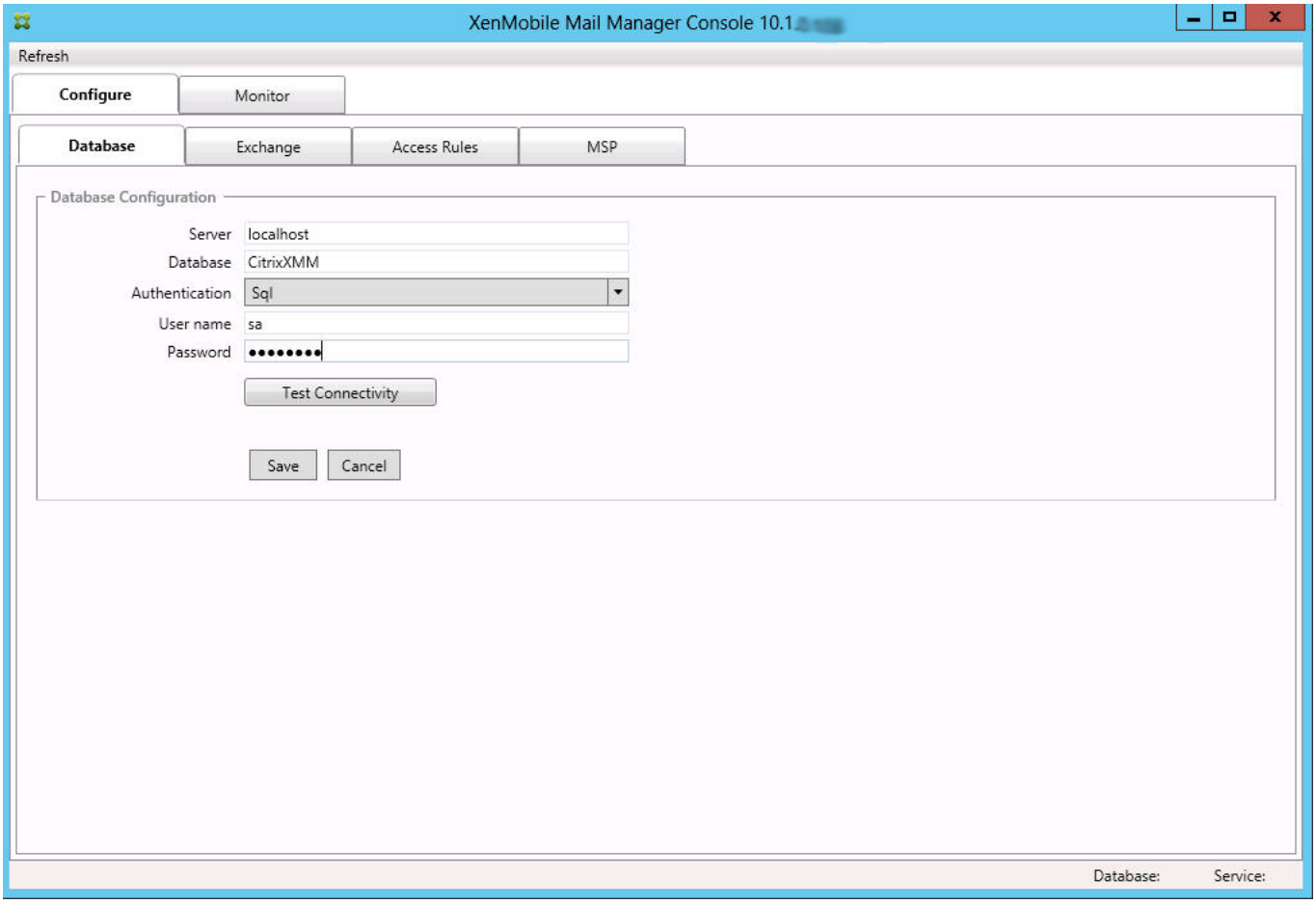
1. Click the XmmSetup.msi file and then follow the prompts in the installer to install XenMobile Mail Manager.

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**.

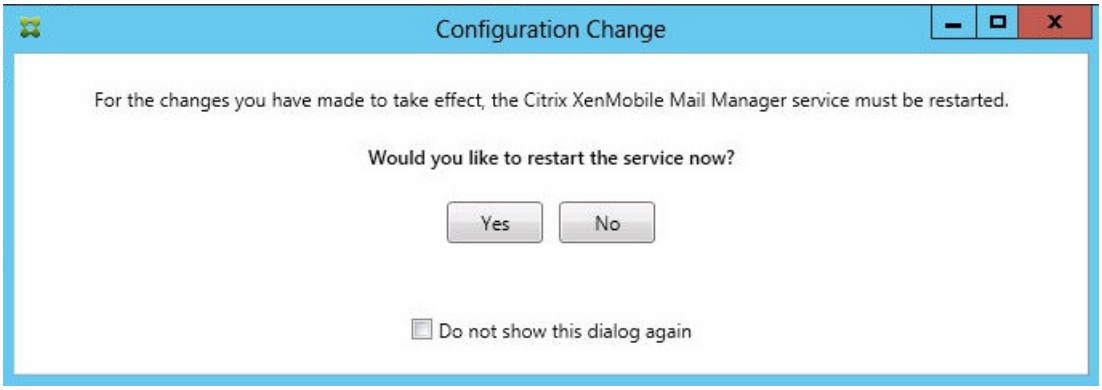
3. Configure the following database properties:
    1. Select the **Configure** > **Database** tab.
    2. Enter the name of the SQL Server (defaults to localhost).
    3. Keep the database as the default CitrixXmm.
    4. Select one of the following authentication modes used for SQL:
        - **Sql**. 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.

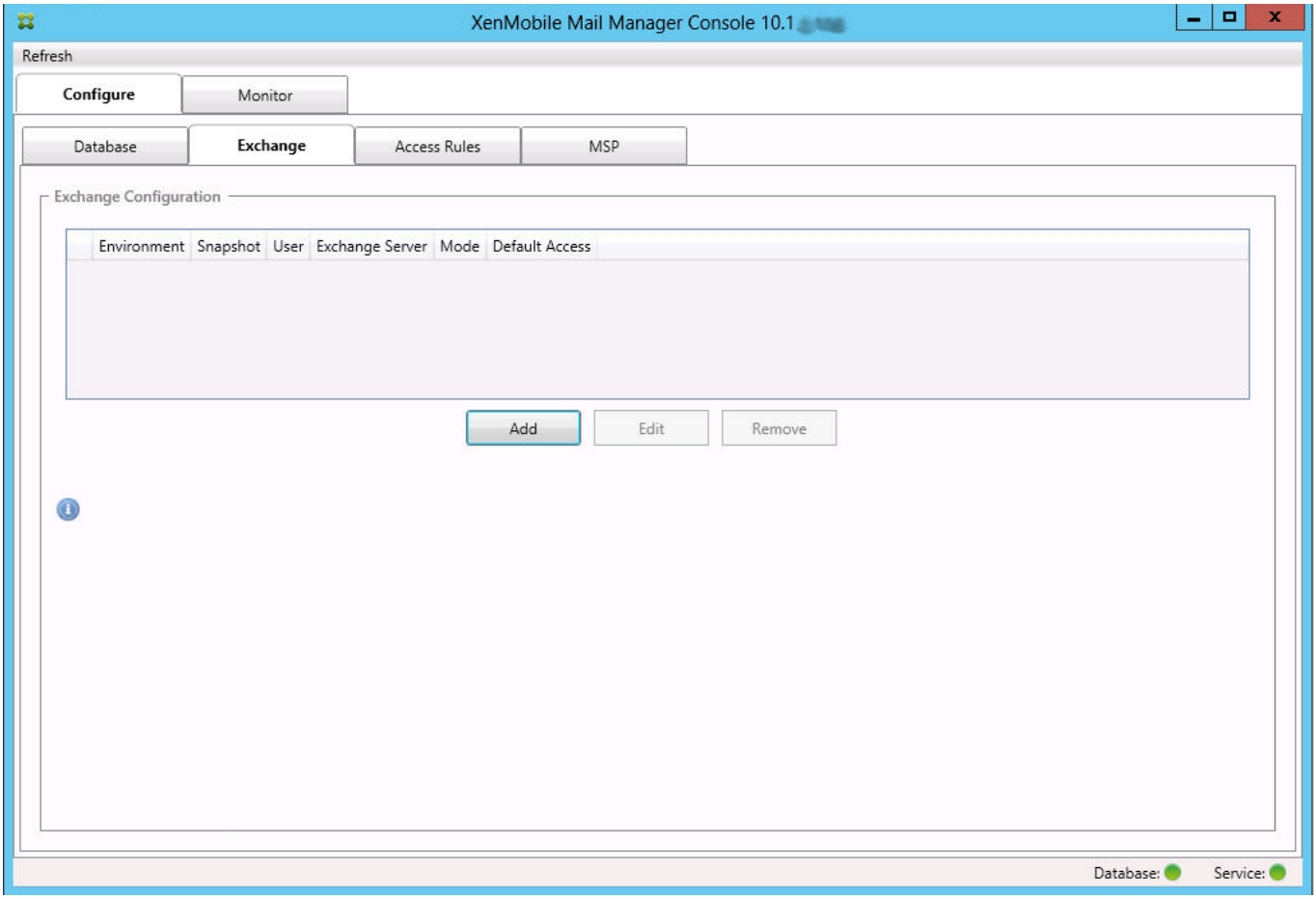
5. Click **Test Connectivity** to check that a connection can be made to the SQL Server and then click **Save**.



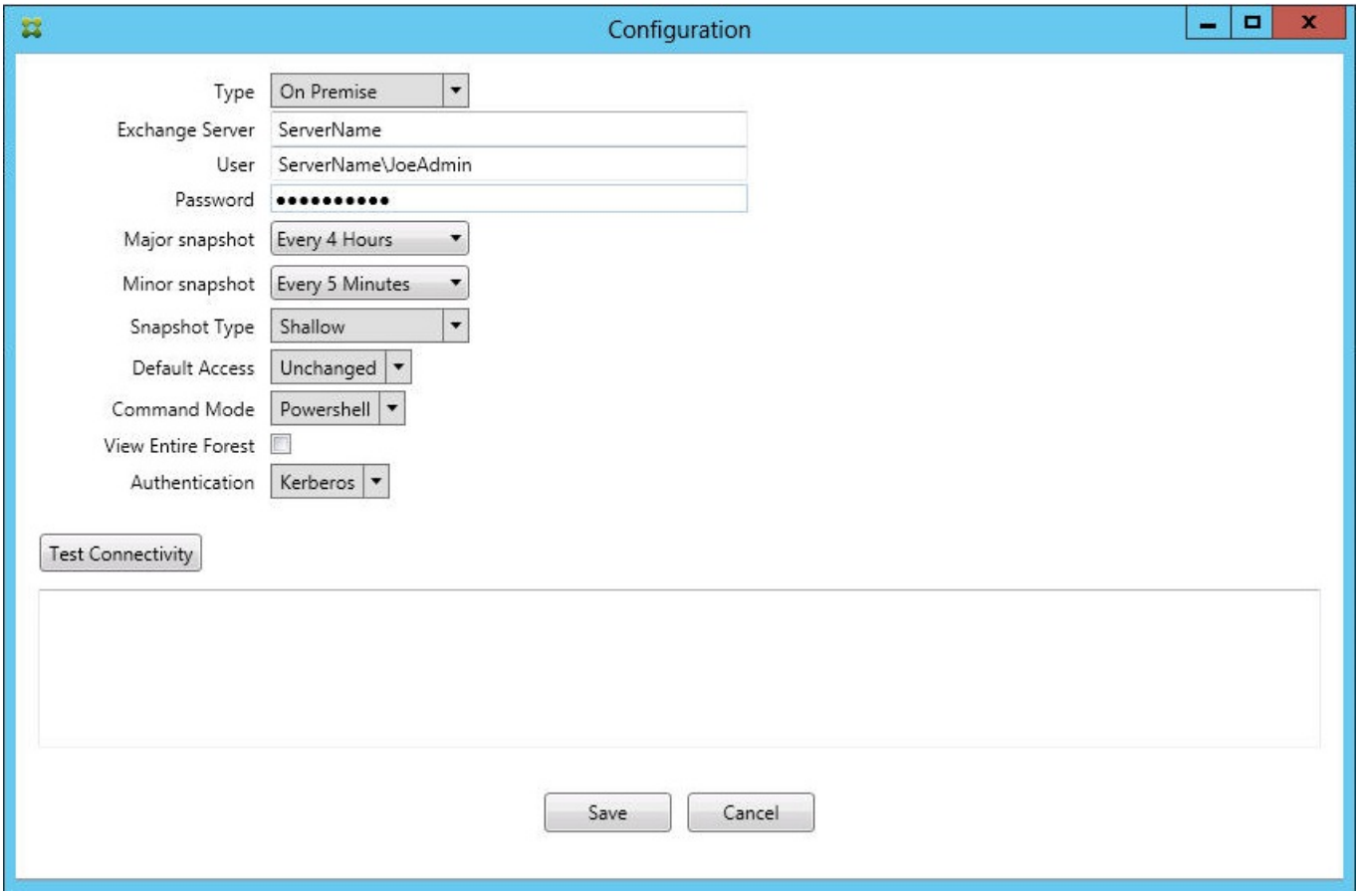
4. A message prompts you to restart the service. Click **Yes**.



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**.

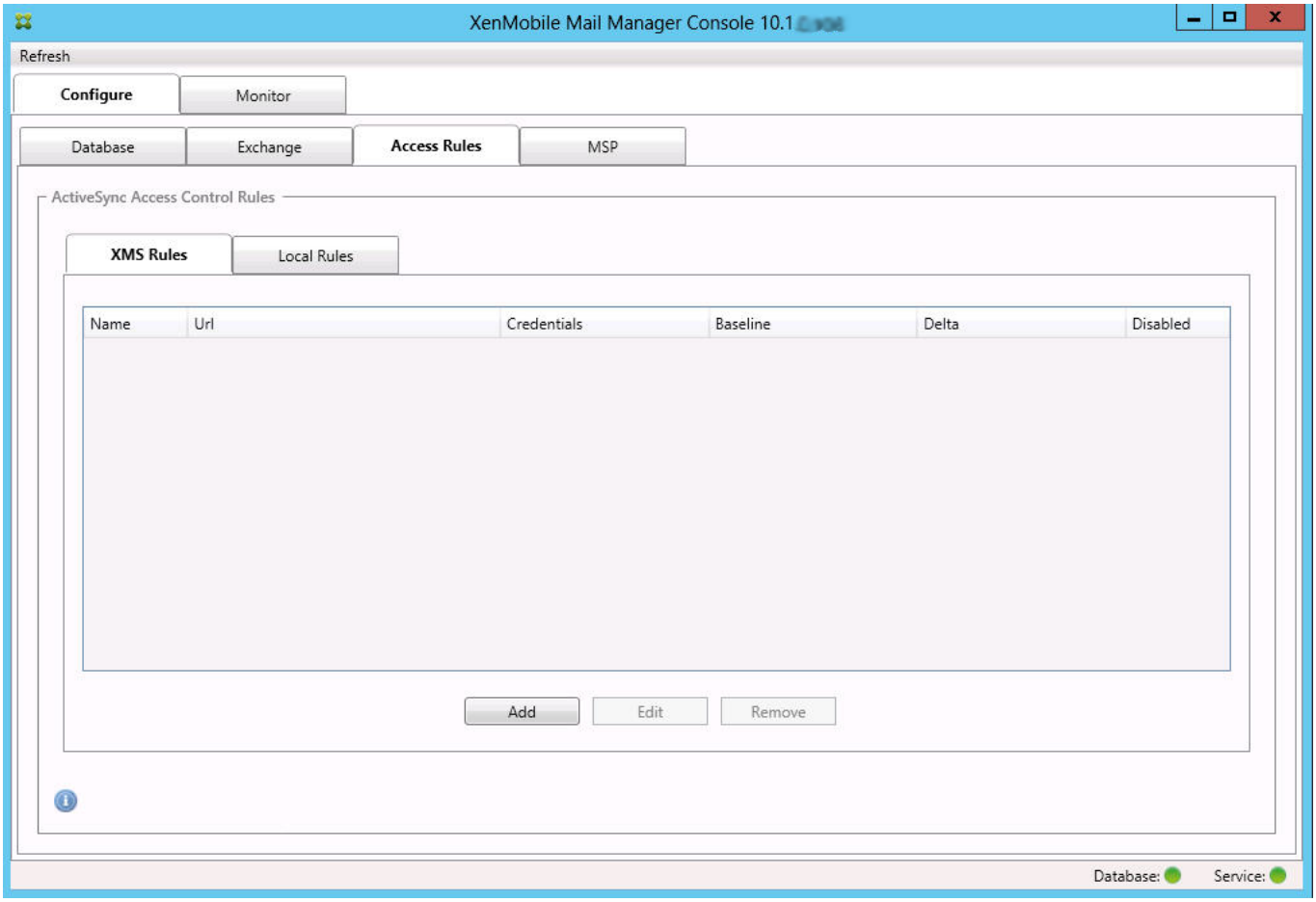


5. If you select **On Premise**, enter the name of the Exchange Server that will be used for Remote PowerShell commands.
6. Enter the user name of a Windows identity that has appropriate rights on the Exchange Server as specified within the Requirements section.
7. Enter the **Password** for the user.
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

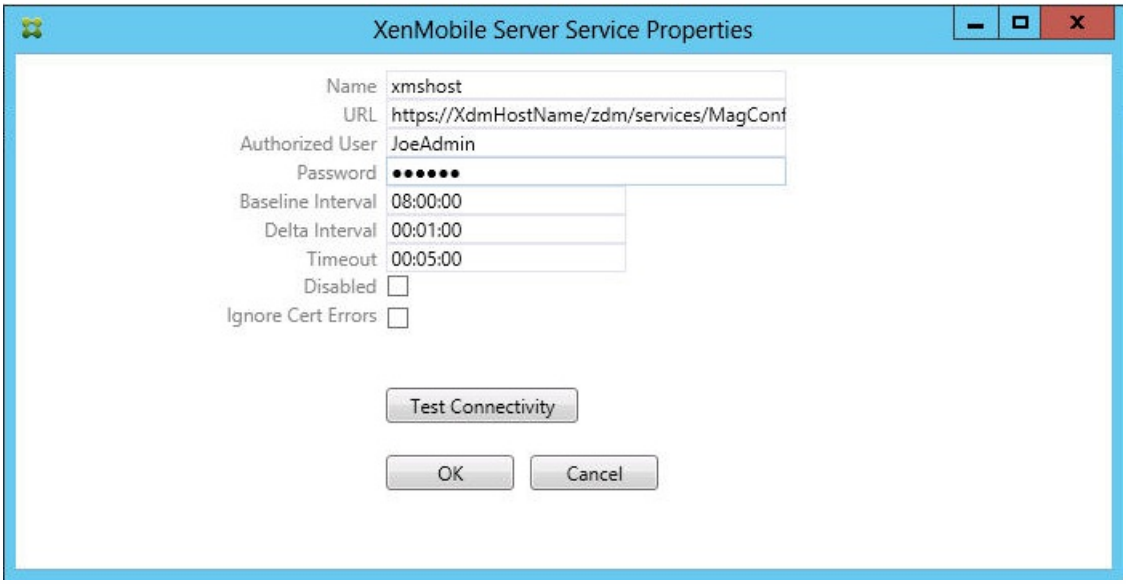
not a member of the domain in which the Exchange server resides.

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.

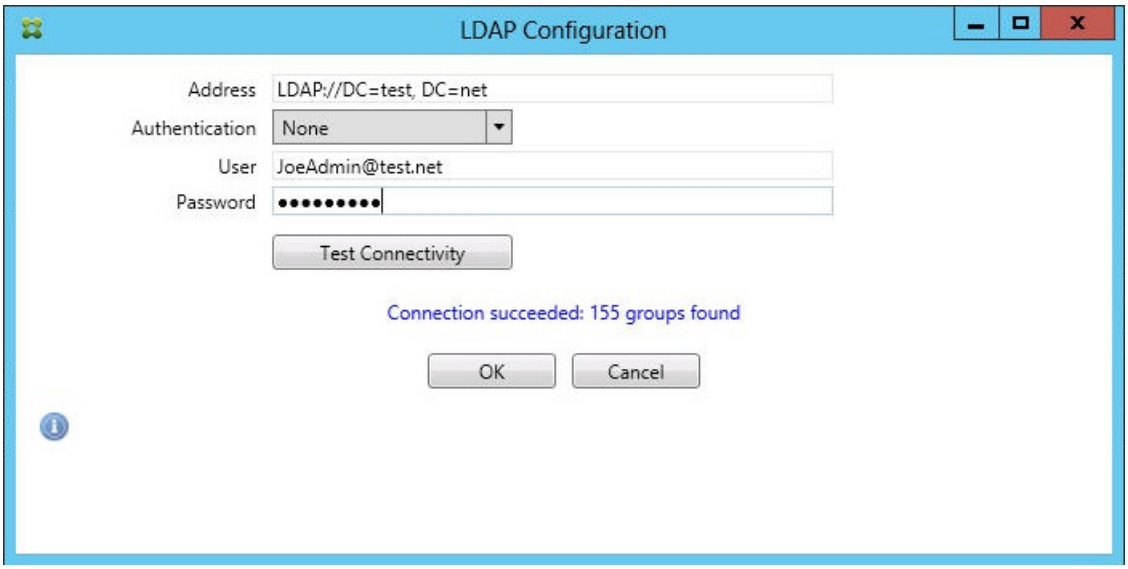


3. Click **Add**.



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.

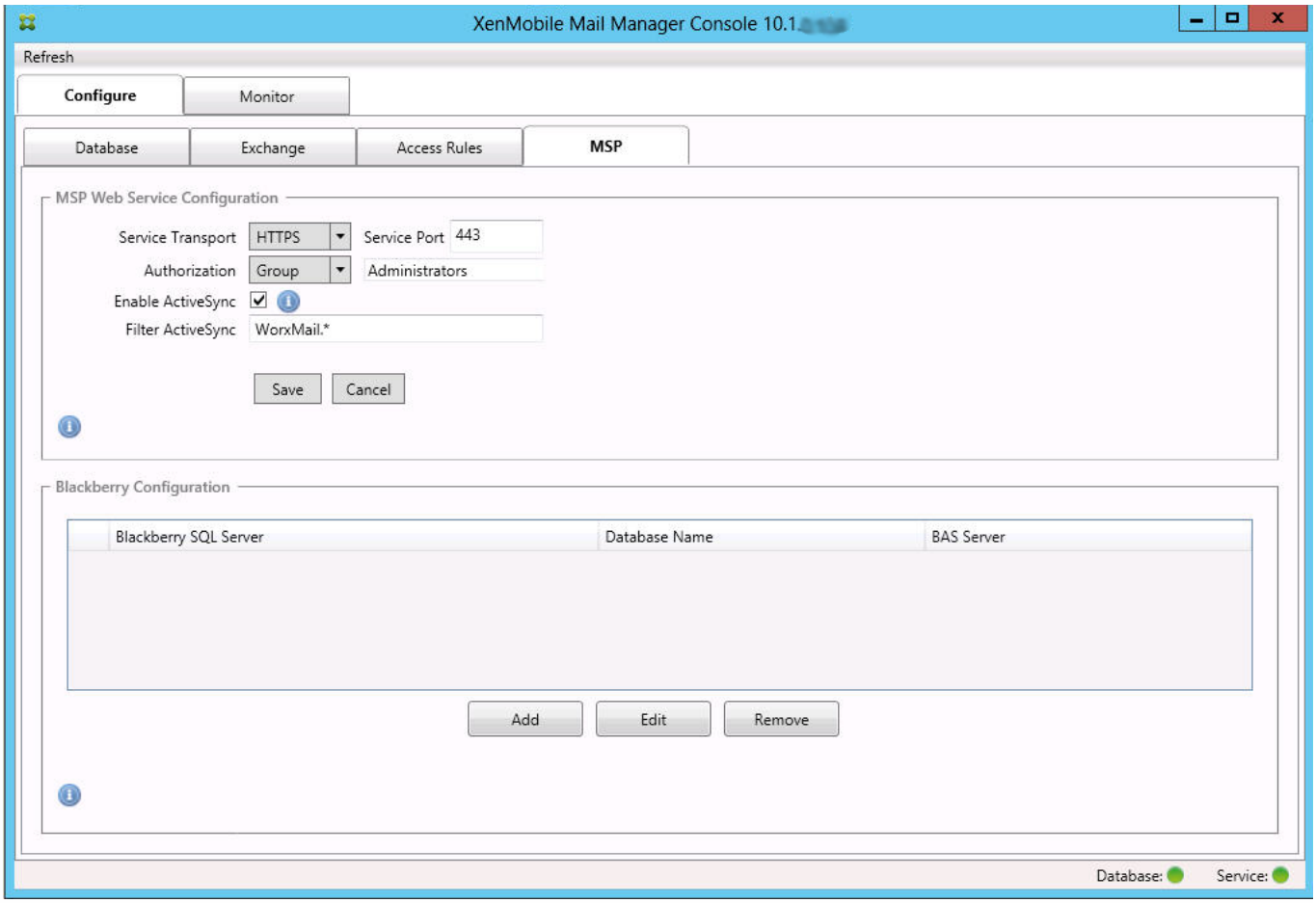


   2. You can add local rules based on **ActiveSync Device ID**, **Device Type**, **AD Grou**p, **User**, or device **UserAgent**. In the list, select the appropriate type. For details, see XenMobile Mail Manager Access Control Rules.
   3. Enter text or text fragments in the text box. Optionally, click 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.

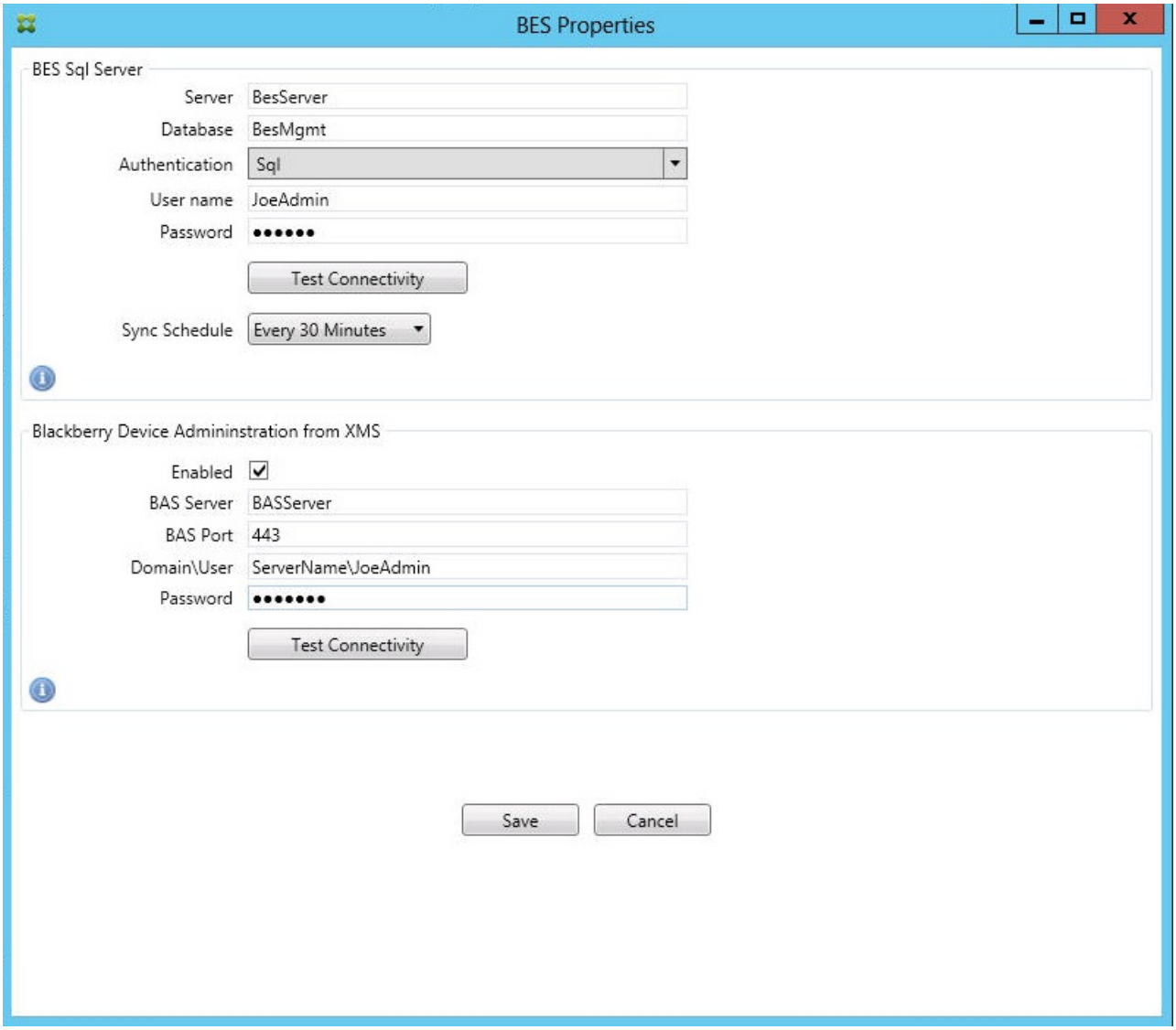
Note: The Mobile Service Provider is optional and is necessary only if XenMobile is also configured to use the Mobile Service Provider interface to query unmanaged devices.

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 WorxMail.* 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. Also please note that as of version 10.4, WorxMail is renamed Secure Mail.
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.



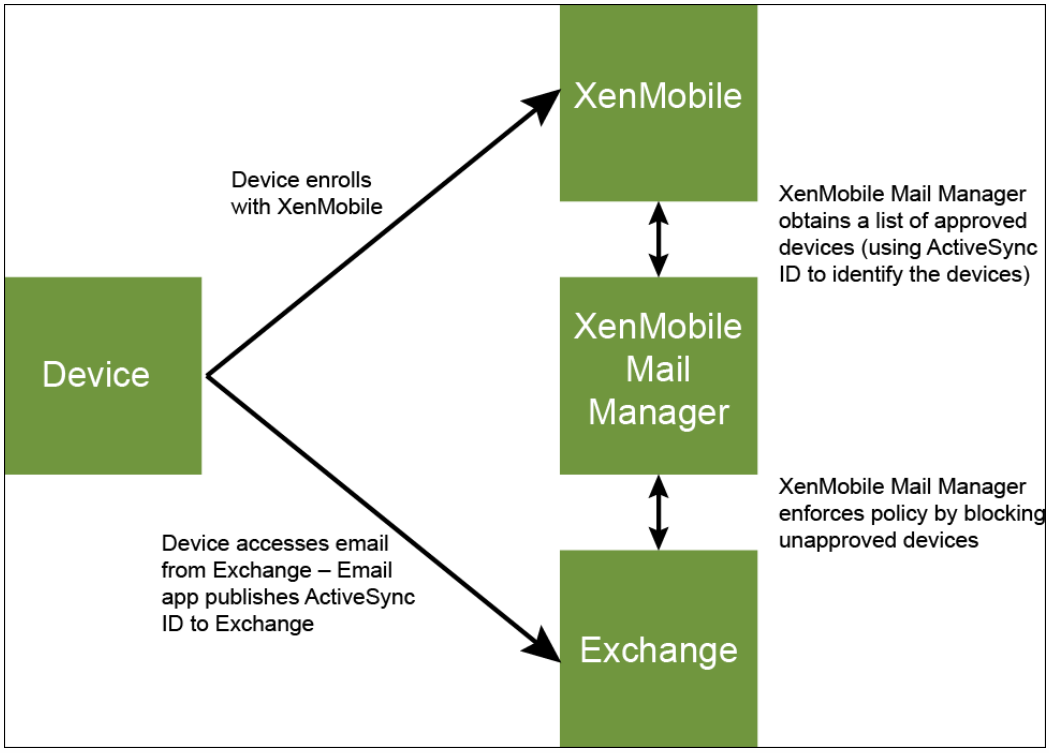
3. Enter the database name of the BES management database.
4. Select the Authentication mode. If you select Windows Integrated authentication, the user account of the XenMobile Mail Manager service is the account that is used to connect to the BES SQL Server.
   Note: If you also choose Windows Integrated 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**.

Enforcing Email Policies with ActiveSync IDs

Jan 04, 2017

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. Worx Home obtains a similar identifier and sends the identifier to XenMobile when the device is enrolled. (**Note:** Starting with version 10.4, Worx Home is renamed Secure Hub.) 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:

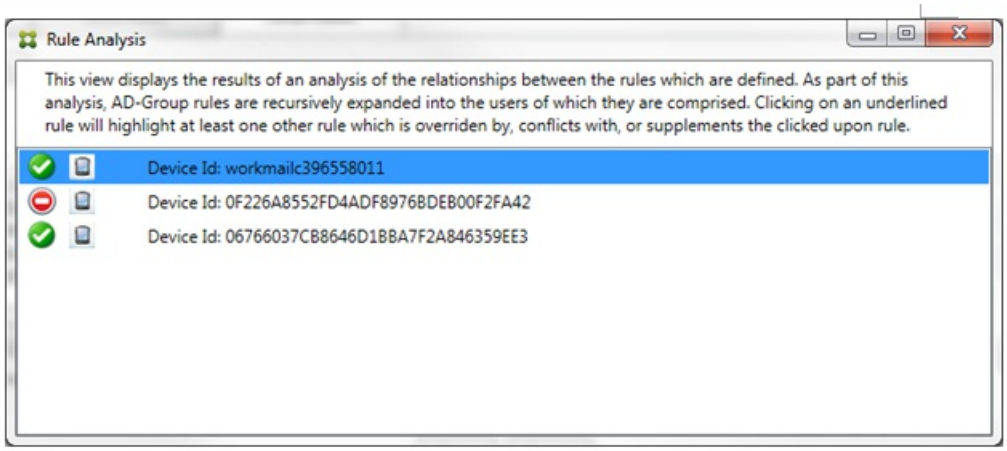
- **Overriding rule**. An override occurs when more than a single rule could apply to the same device. Because rules are evaluated by priority in the list, the later rule instance(s) which might apply might never be evaluated.
- **Conflicting rule**. A conflict occurs when more than a single rule could 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

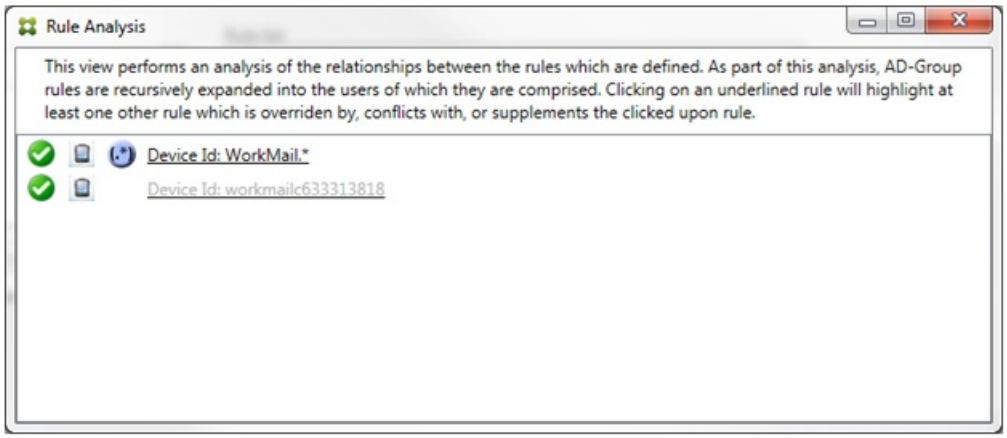
When there are no conflicts, overrides, or supplements, the Rule Analysis dialog box has no underlined entries. Clicking on

any of the items has no impact; for example, normal selected item visuals will occur.

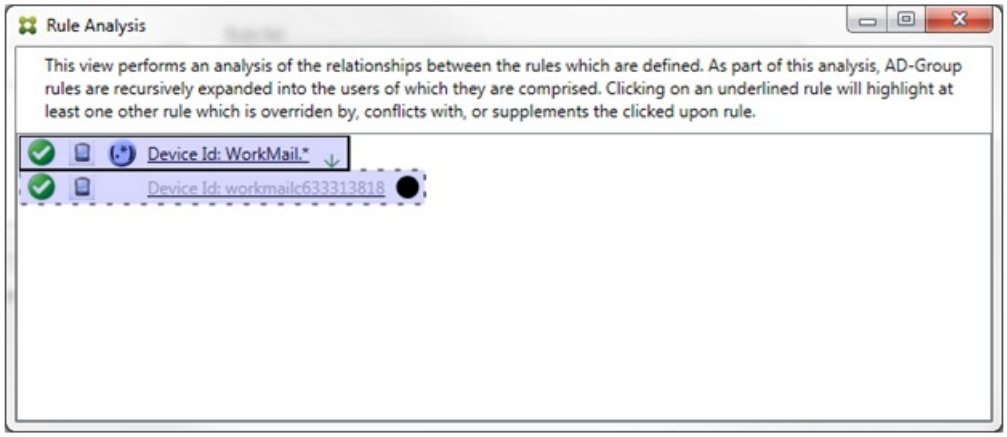
The Rule Analysis window has a check box which, when selected, displays only those rules which are conflicts, overrides, redundancies, or supplements.



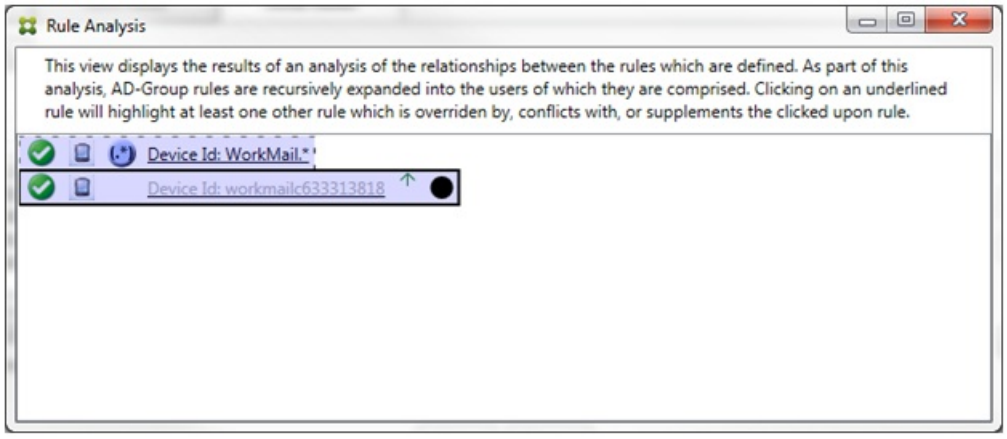
When an override occurs, at least two rules will be underlined: the primary rule and the ancillary rule or rules. At least one ancillary rule will appear in a lighter font to indicate that the rule has been overridden by a higher priority rule. You can click on the overridden rule to find out which rule 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:

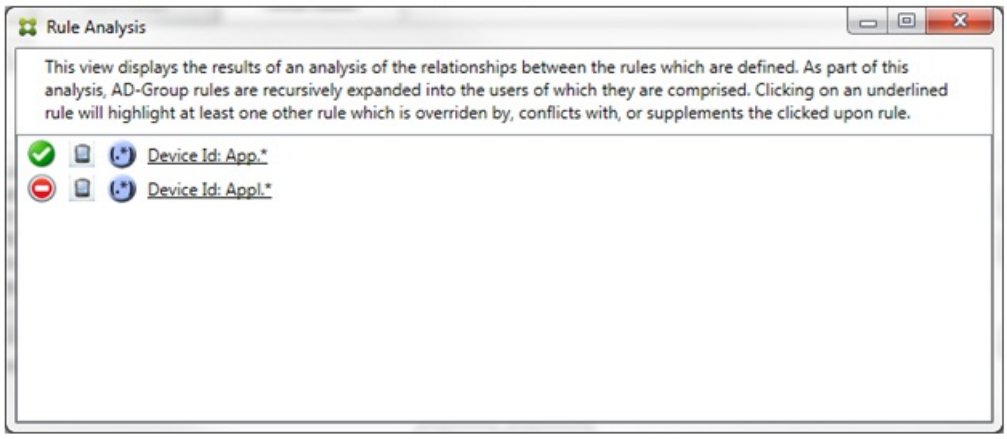


In this example, the regular expression rule WorkMail.* is the primary rule (indicated by the solid border) and the normal rule workmailc633313818 is an ancillary rule (indicated by the dashed border). The black dot next to the ancillary rule is a visual cue that further indicates that the rule is inactive (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:

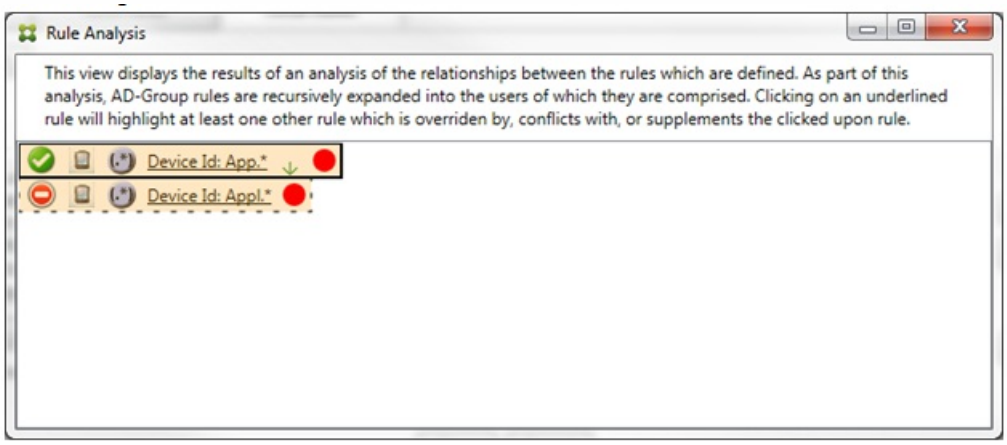


In the preceding example, the regular expression rule WorkMail.* is the ancillary rule (indicated by the dashed border) and the normal rule workmailc633313818 is a primary rule (indicated by the solid border). For this simple example, there's not much difference. For a more complicated example, see the 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:

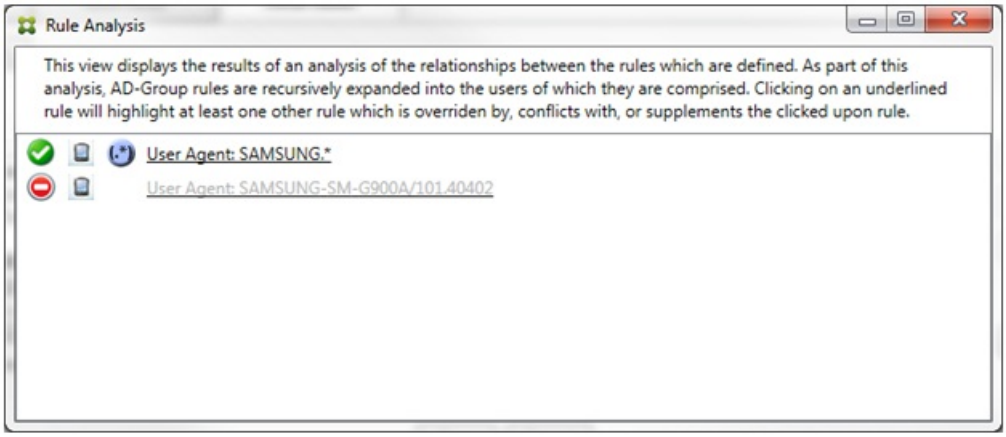


By inspecting the two regular expression rules, it's evident that the first rule allows all devices with a device ID that contains "App" and that the second rule denies all devices with a device ID that contains Appl. In addition, even though the second rule denies all devices with a device ID that contains 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:



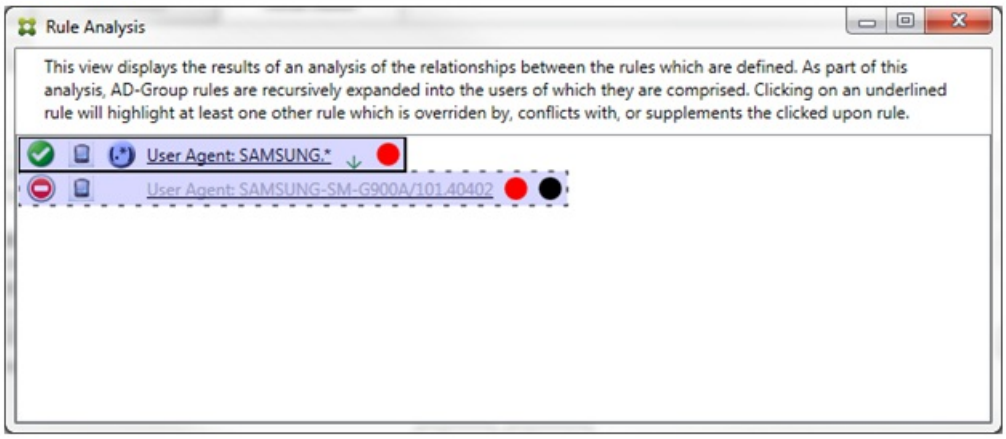
In the preceding scenario, both the primary rule (regular expression rule App.*) and the ancillary rule (regular expression rule Appl.*) are both highlighted in yellow. This is simply a visual warning to alert you to the fact that you have applied more than a single regular expression rule to a single 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.



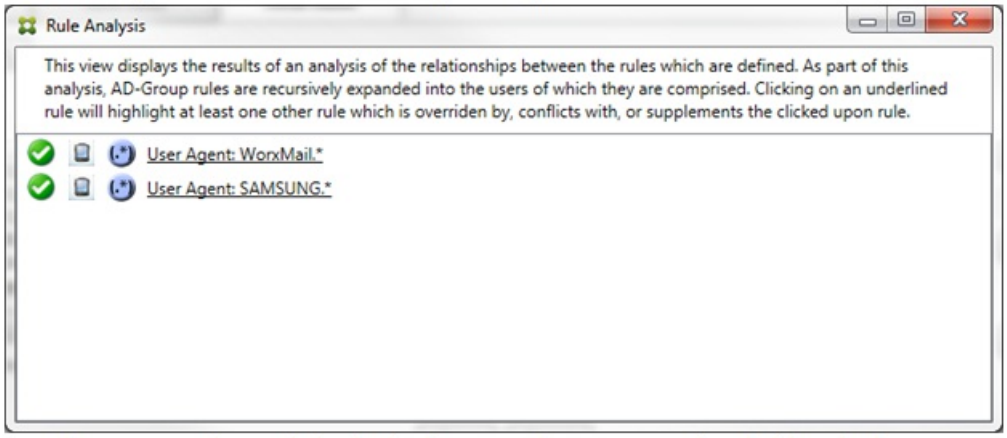
It is easy to see in the preceding example that the first rule (regular expression rule SAMSUNG.*) not only overrides the next rule (normal rule SAMSUNG-SM-G900A/101.40402), but that the two rules differ in their access (primary specifies Allow, ancillary specifies Block). The second rule (normal rule 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:

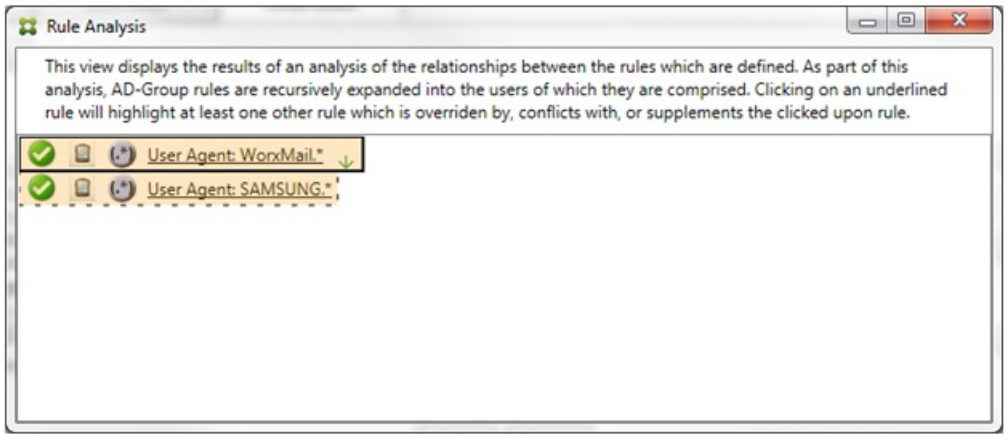


The primary rule (regular expression rule SAMSUNG.*) is followed by a red dot to indicate that its access state conflicts with one or more ancillary rules. The ancillary rule (normal rule SAMSUNG-SM-G900A/101.40402) is followed by a red dot to indicate that its access state conflicts with the primary 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:



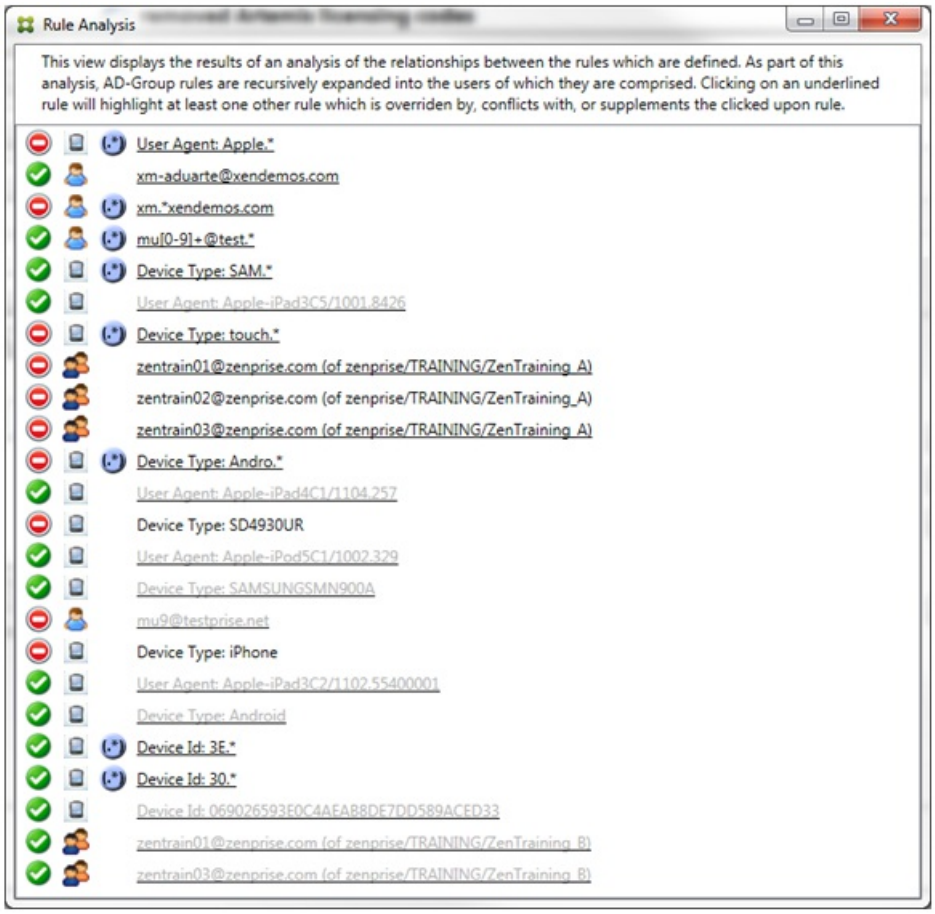
Visual inspection easily reveals that both rules are regular expression rules which have both been applied to the ActiveSync device ID field in XenMobile Mail Manager. After clicking on the first rule, the dialog box looks as follows:



The primary rule (regular expression rule WorxMail.*) is highlighted with a yellow overlay to indicate that there exists at least one additional ancillary rule which is a regular expression. (**Note**: As of version 10.4, WorxMail is renamed Secure Mail.) 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

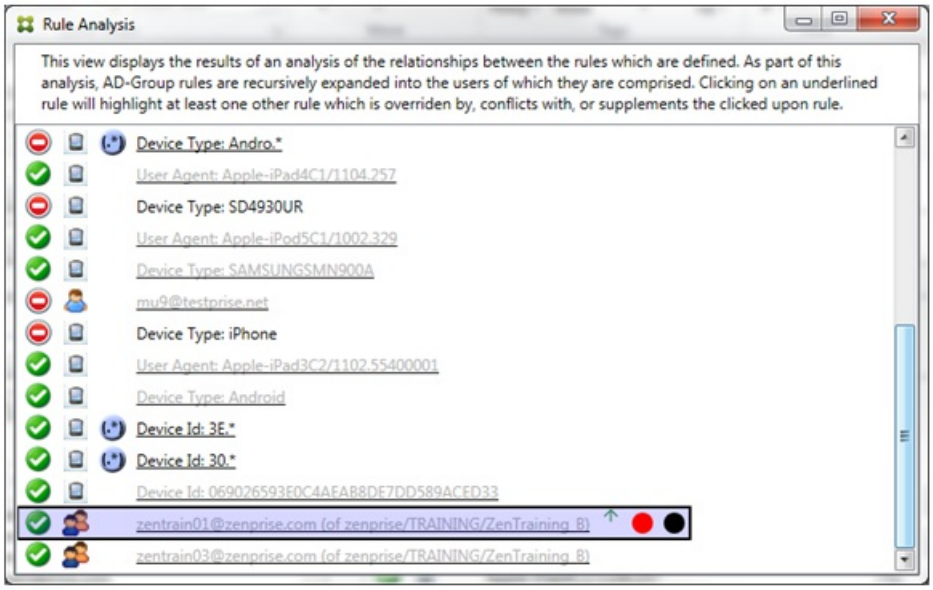
Many potential overrides, conflicts, or supplements can occur, making it impossible to give an example of all possible scenarios. The following example discusses what not to do, while also serving to illustrate the full power of the rule analysis visual construct. Most of the items are underlined in 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.

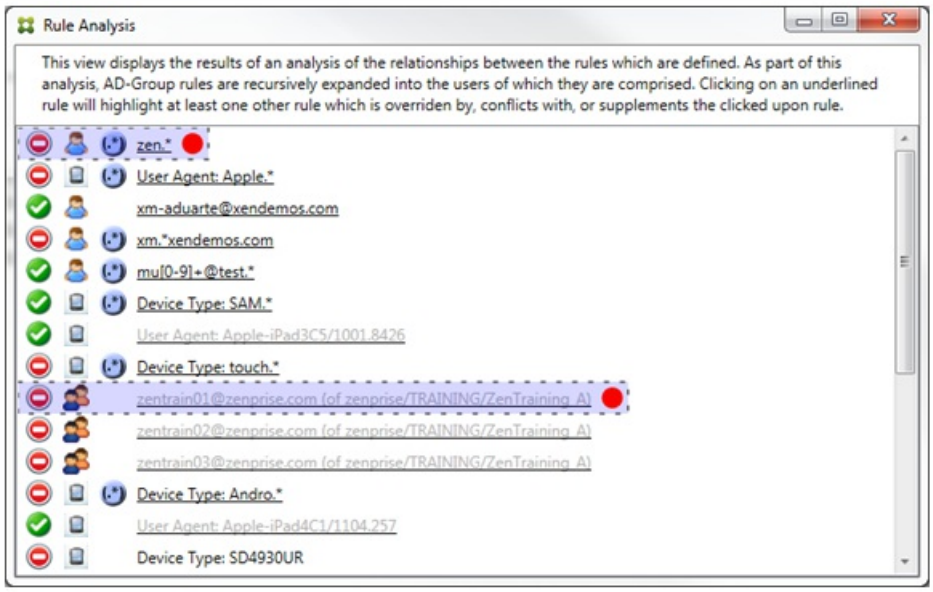
Example 1: This example examines why zentrain01@zenprise.com has been overridden.



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.

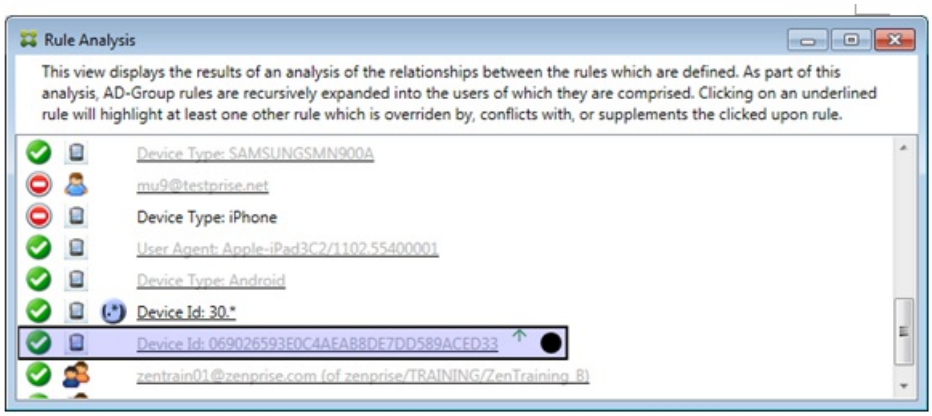
When you scroll up, you see the following:



In this case, there are two ancillary rules that override the primary rule: the regular expression rule zen.* and the normal rule

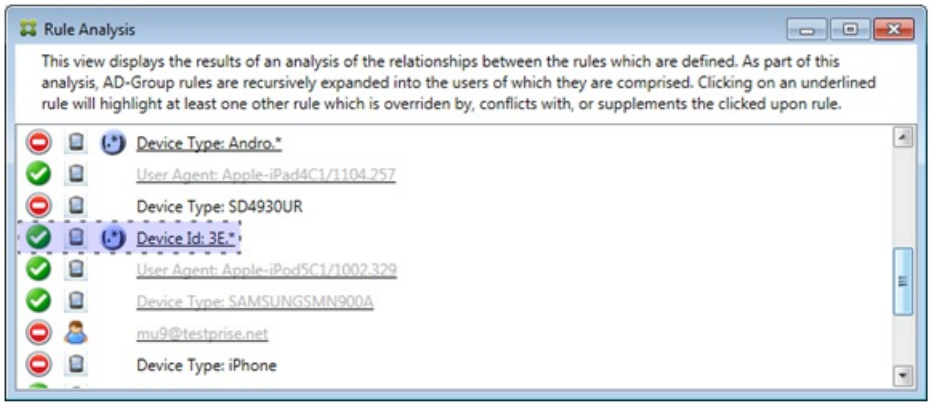
zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining A). In the case of the latter ancillary rule, what has occurred is that the Active Directory Group rule ZenTraining A contains the user zentrain01@zenprise.com, and the Active Directory Group rule ZenTraining B also contains the user zentrain01@zenprise.com. 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.

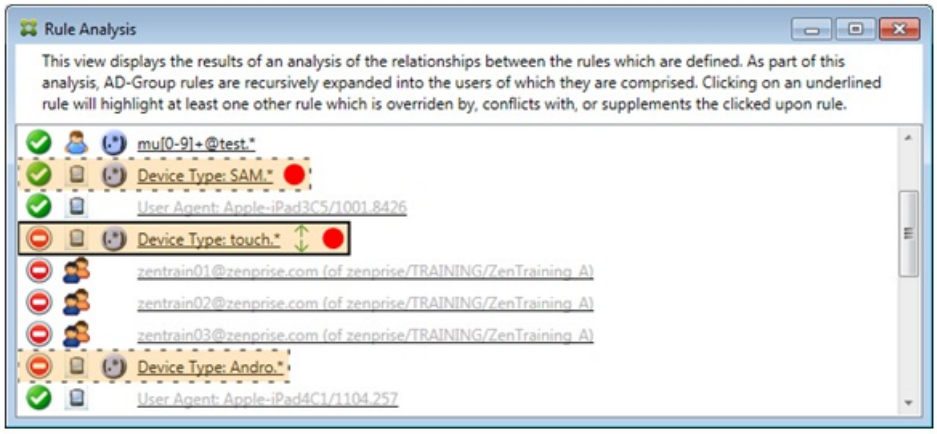


In this case, a single ancillary rule overrides the primary rule: the regular expression ActiveSync device ID rule 3E.* Because the regular expression 3E.* would match 069026593E0C4AEAB8DE7DD589ACED33, the primary rule will never be evaluated.

How to Analyze a Supplement and Conflict

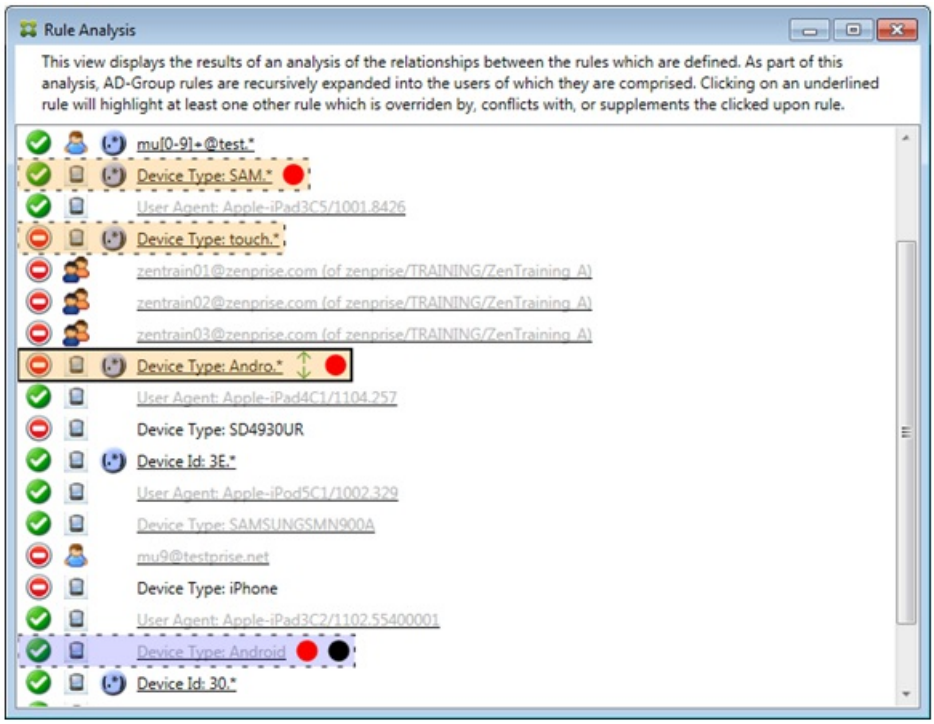
In this case, the primary rule is the regular expression ActiveSync device type rule touch.* The characteristics are as follows:

- 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

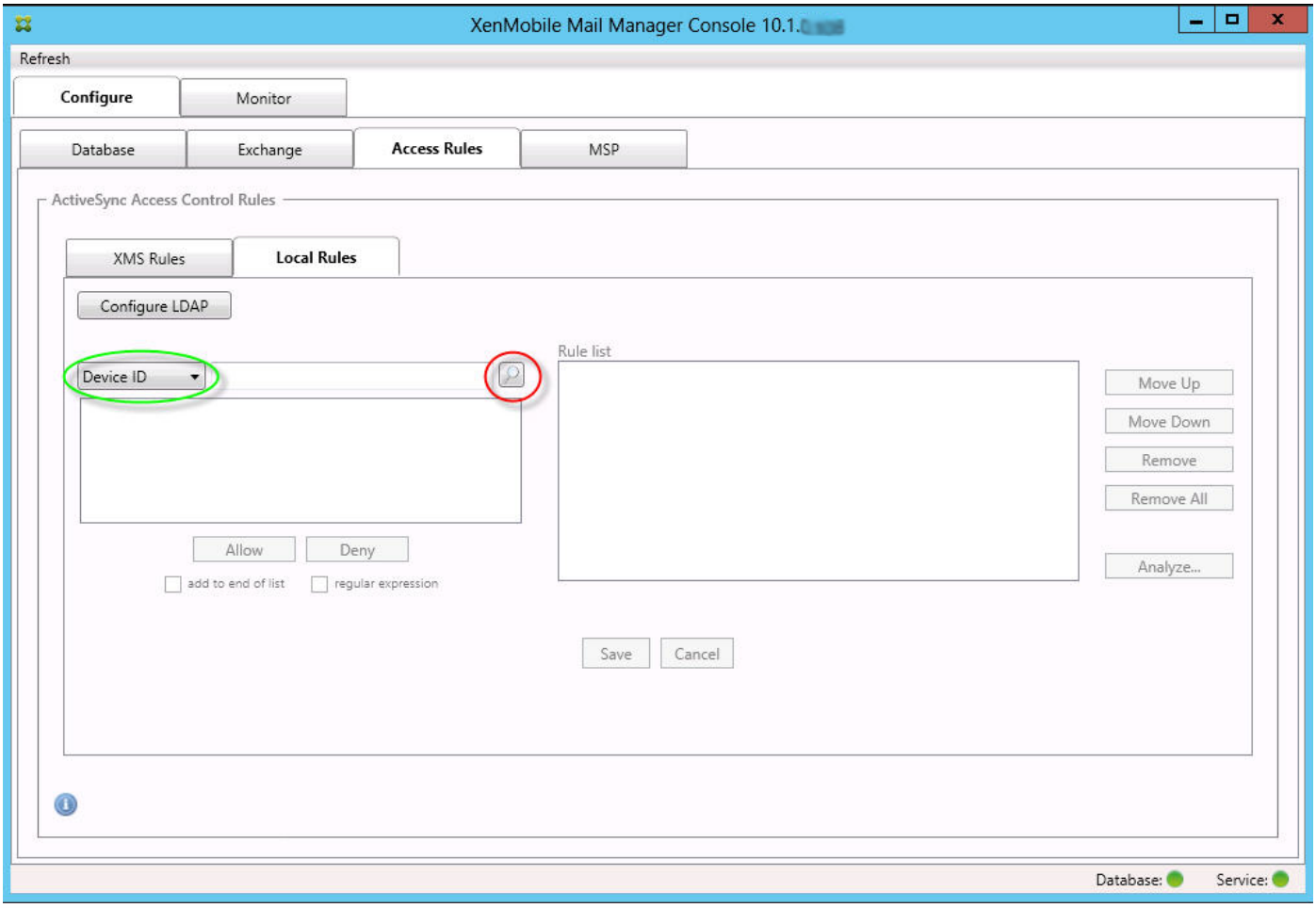
This example explores how rule relationships are always from the perspective of the primary rule. The preceding example showed how a click on the regular expression rule applied to the rule field of device type with a value of touch.* Clicking on the ancillary rule Andro.* shows a different set of ancillary rules highlighted.



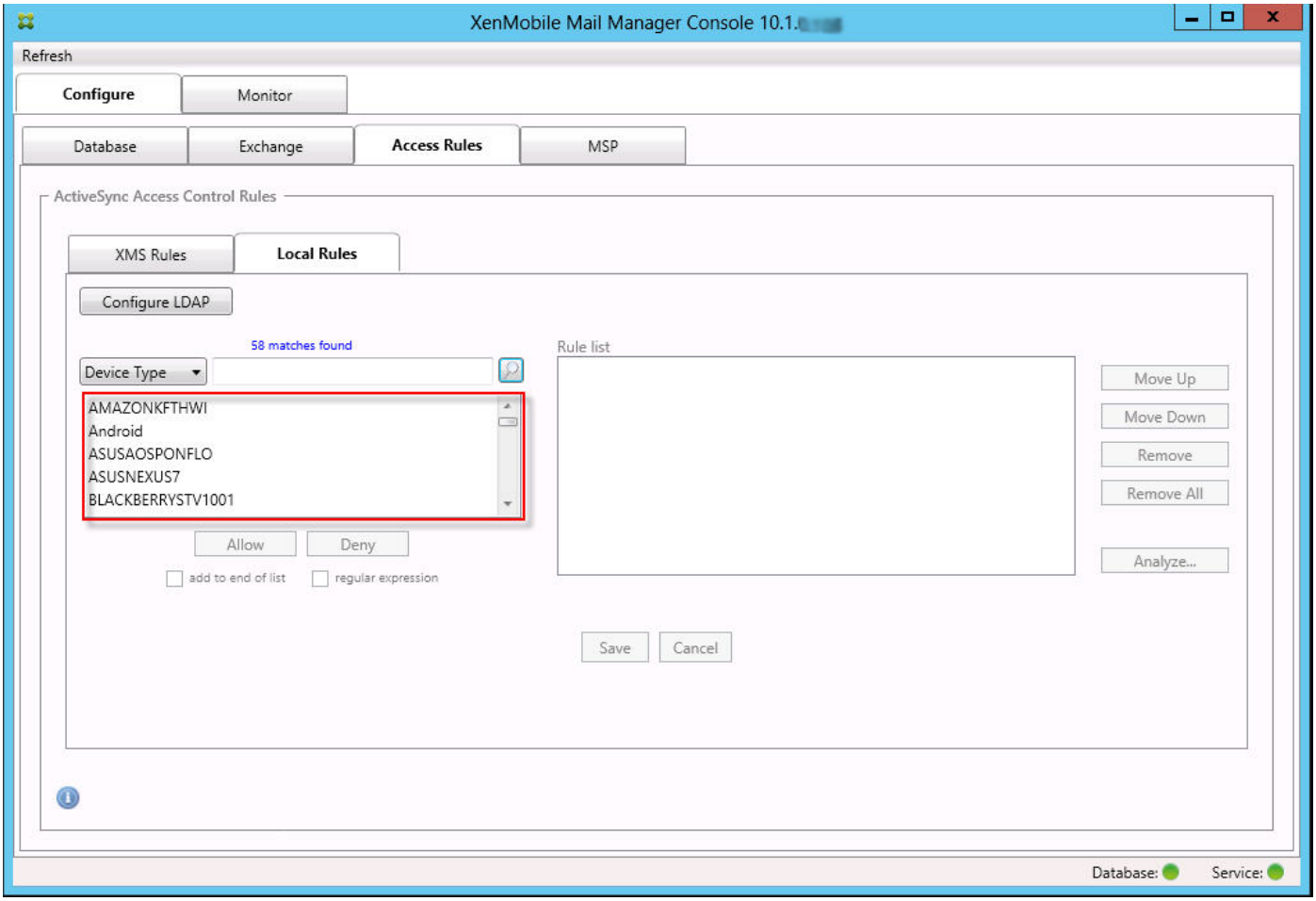
The example shows an overridden rule that is included in the rule relationship. This rule is the normal ActiveSync device type rule Android, which is overridden (indicated by the lightened font and the black circle next to it) and also conflicts in its access with the primary rule regular expression 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.

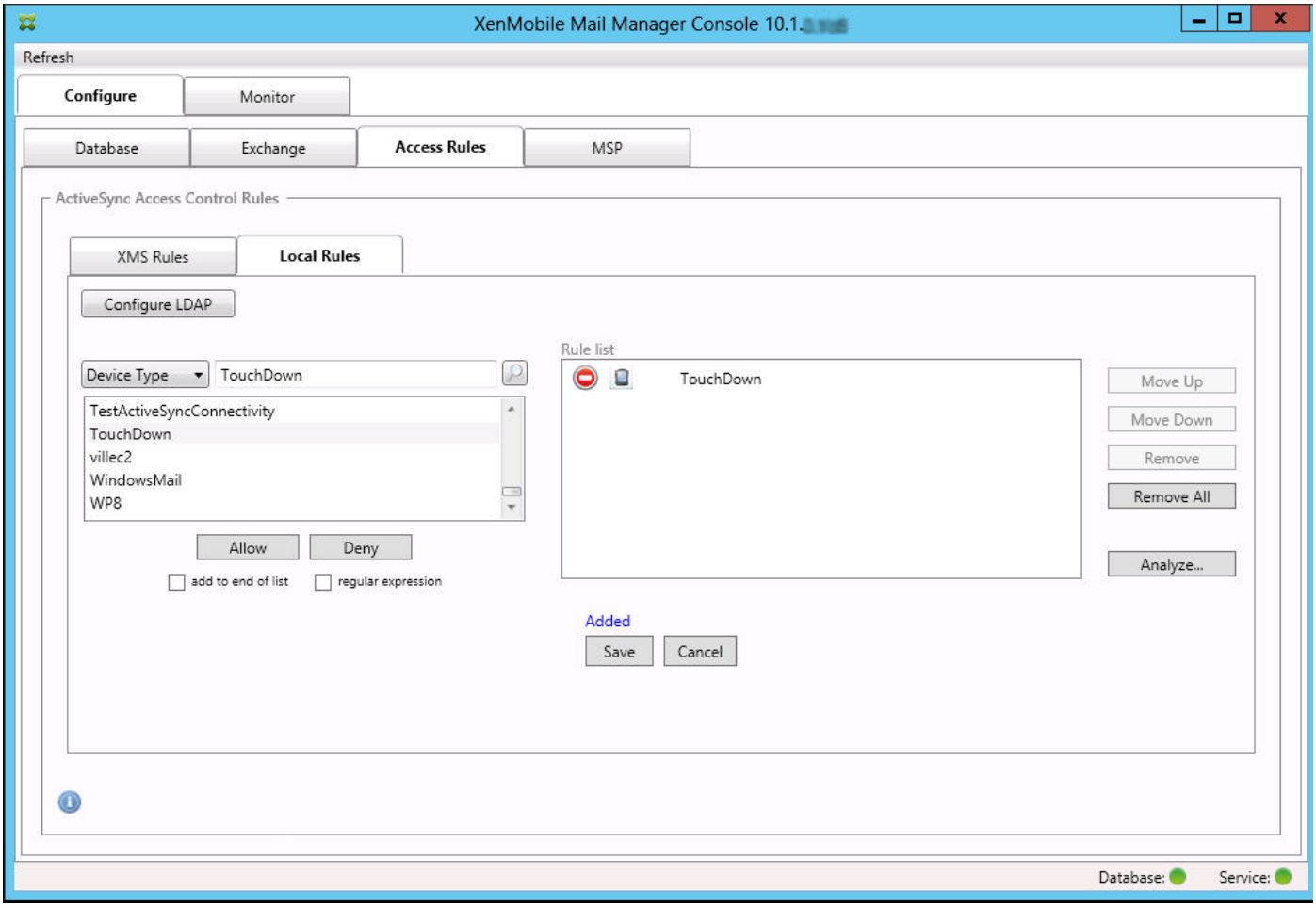


2. In the Device ID list, select the field for which you want to create a Local Rule.
3. Click on the magnifying glass icon to display all of the unique matches for the chosen field. In this example, the field Device Type has been chosen and the choices are shown below in the list box.



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.

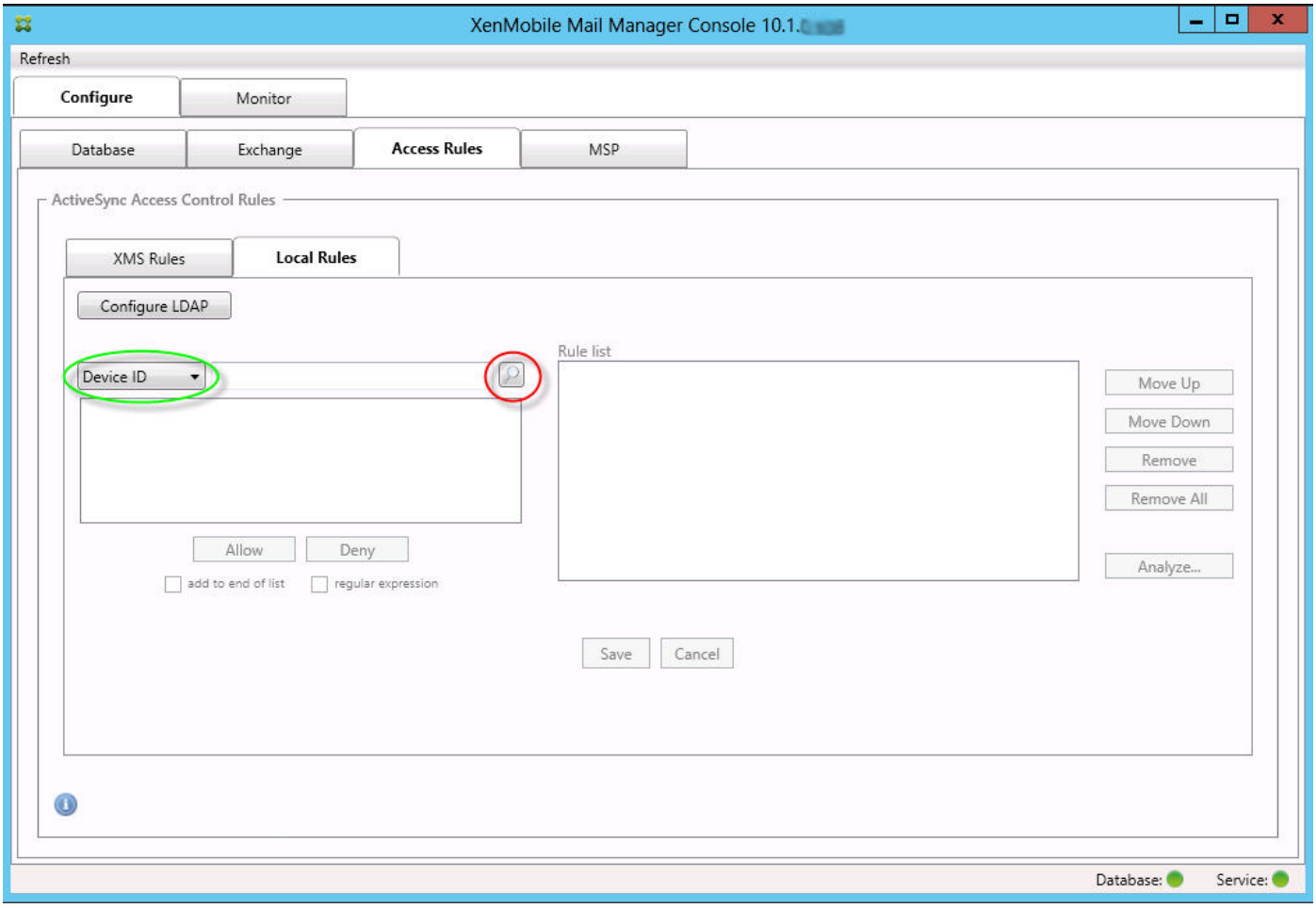


To add a regular expression

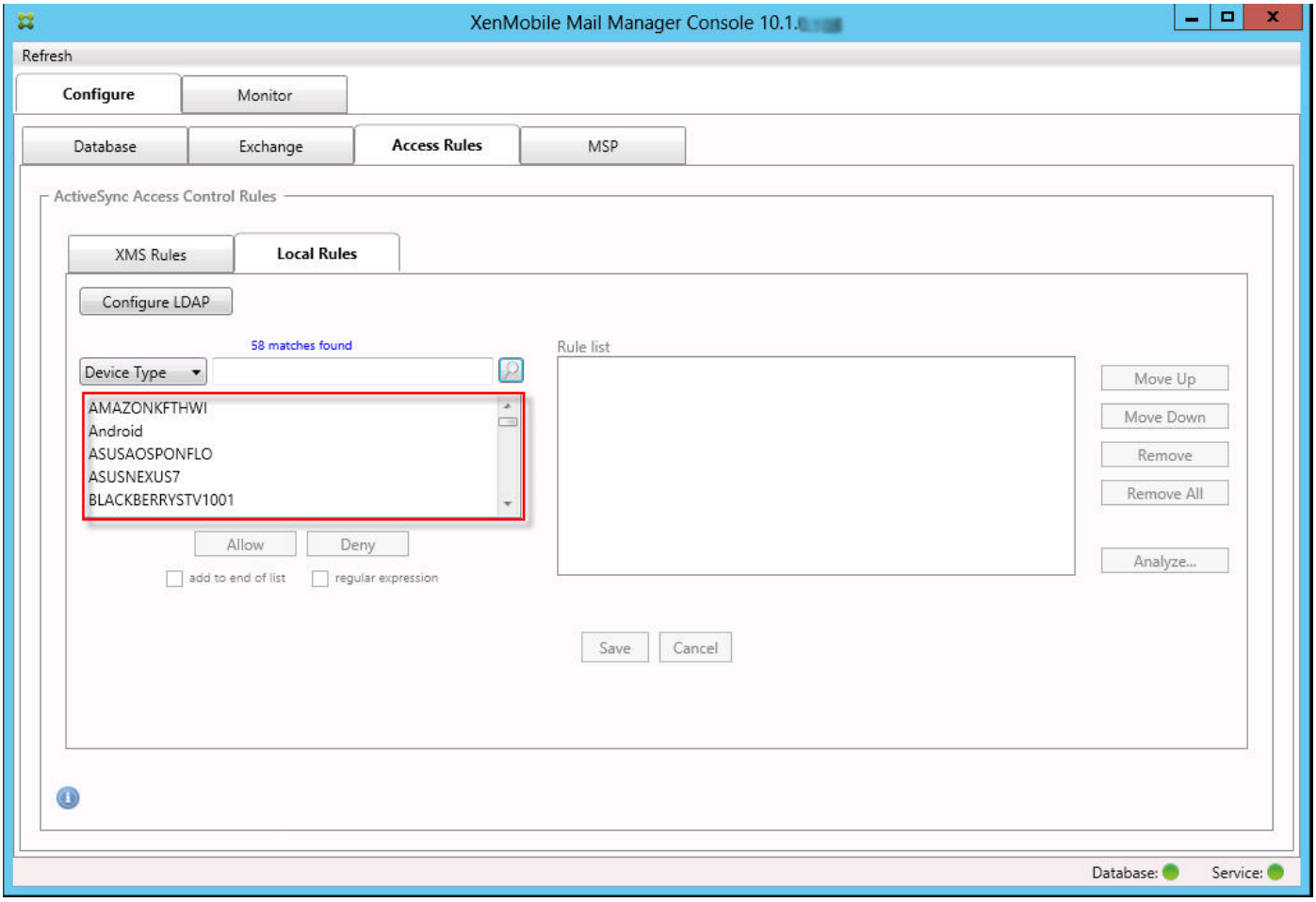
Regular expression local rules can be distinguished by the icon which appears next to them - (.*). To add a regular expression rule, you can either build a regular expression rule from an existing value from the results list for a given field (as long as a major snapshot has completed), or you can simply type in the regular expression that you want.

To build a regular expression from an existing field value

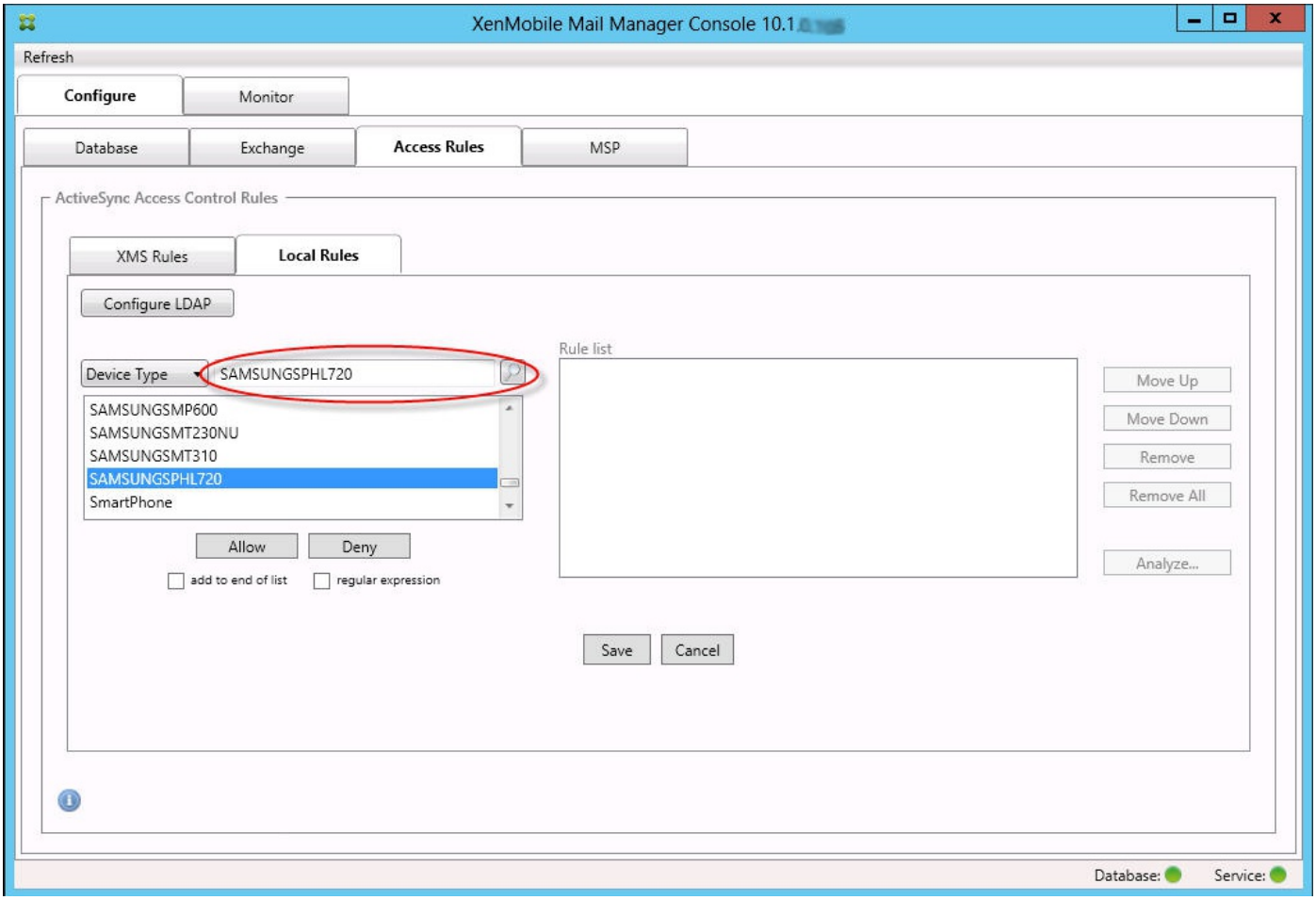
1. Click the Access Rules tab.



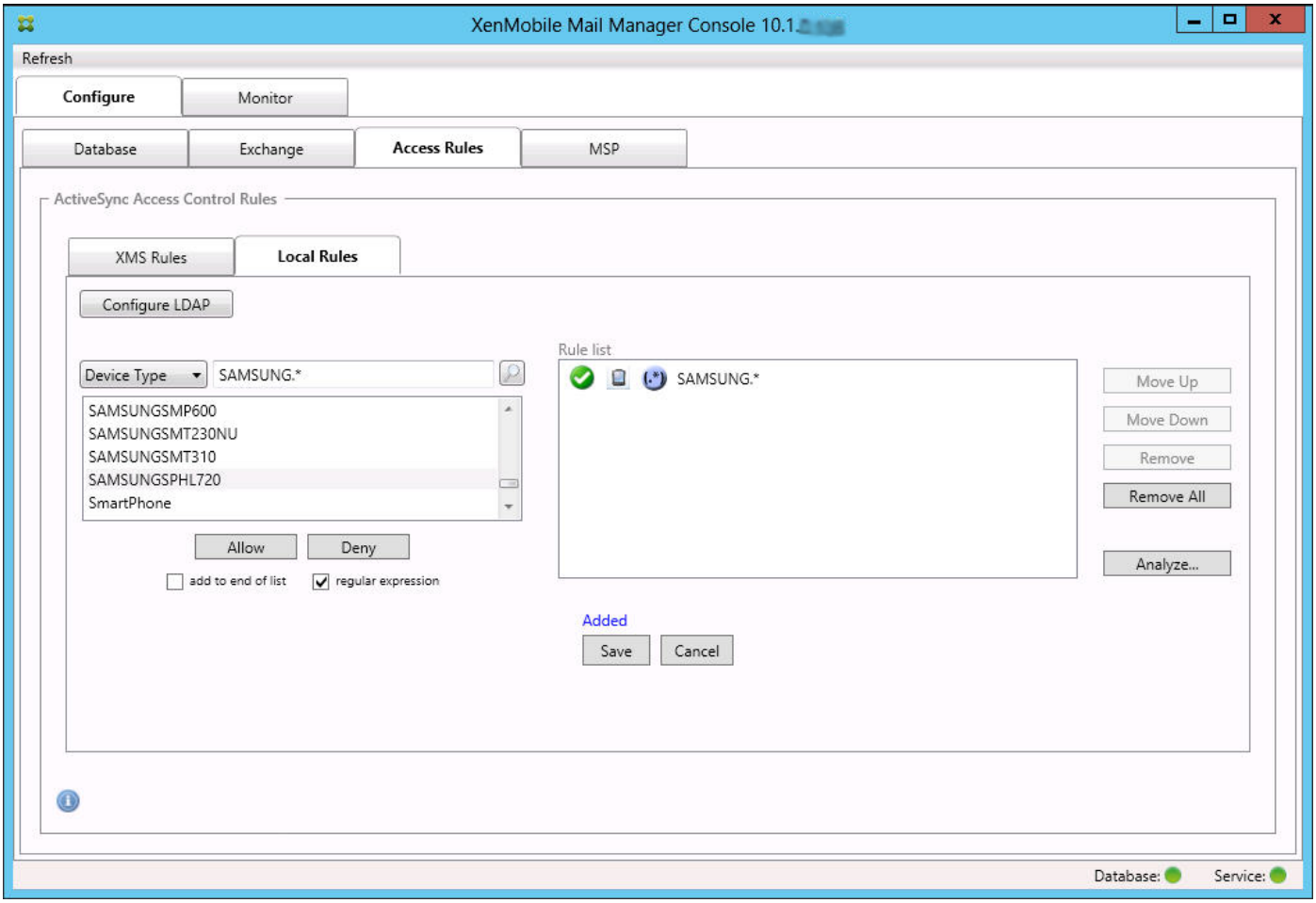
2. In the Device ID list, select the field for which you want to create a regular expression Local Rule.
3. Click on the magnifying glass icon to display all of the unique matches for the chosen field. In this example, the field Device Type has been chosen and the choices are shown below in the list 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.

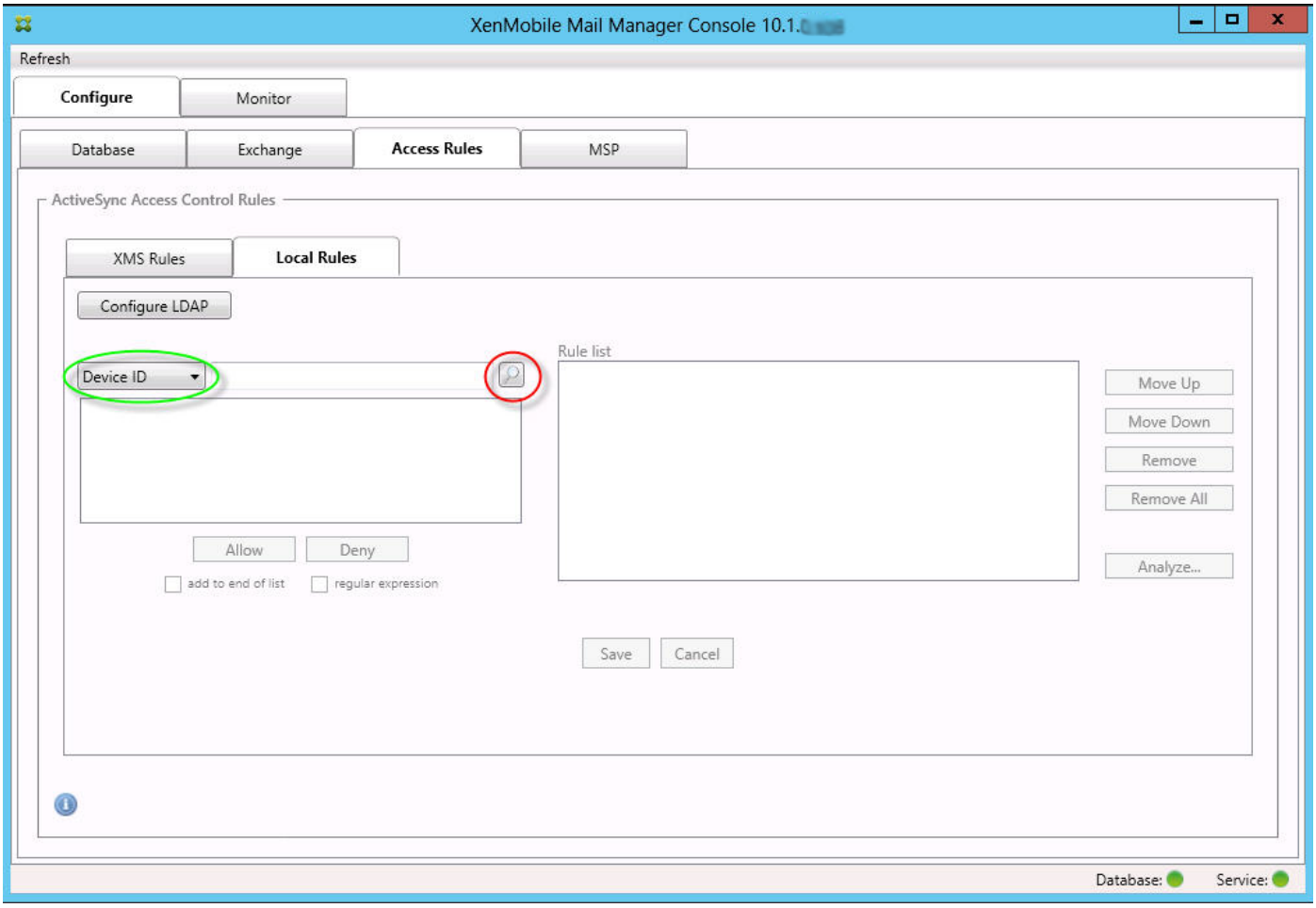


5. To allow all device types that have "Samsung" in their device type value, add a regular expression rule by following these steps:
   1. Click within the selected item text box.
   2. Change the text from SAMSUNGSPHL720 to SAMSUNG.*
   3. Make sure that the regular expression check box is selected.
   4. Click Allow.

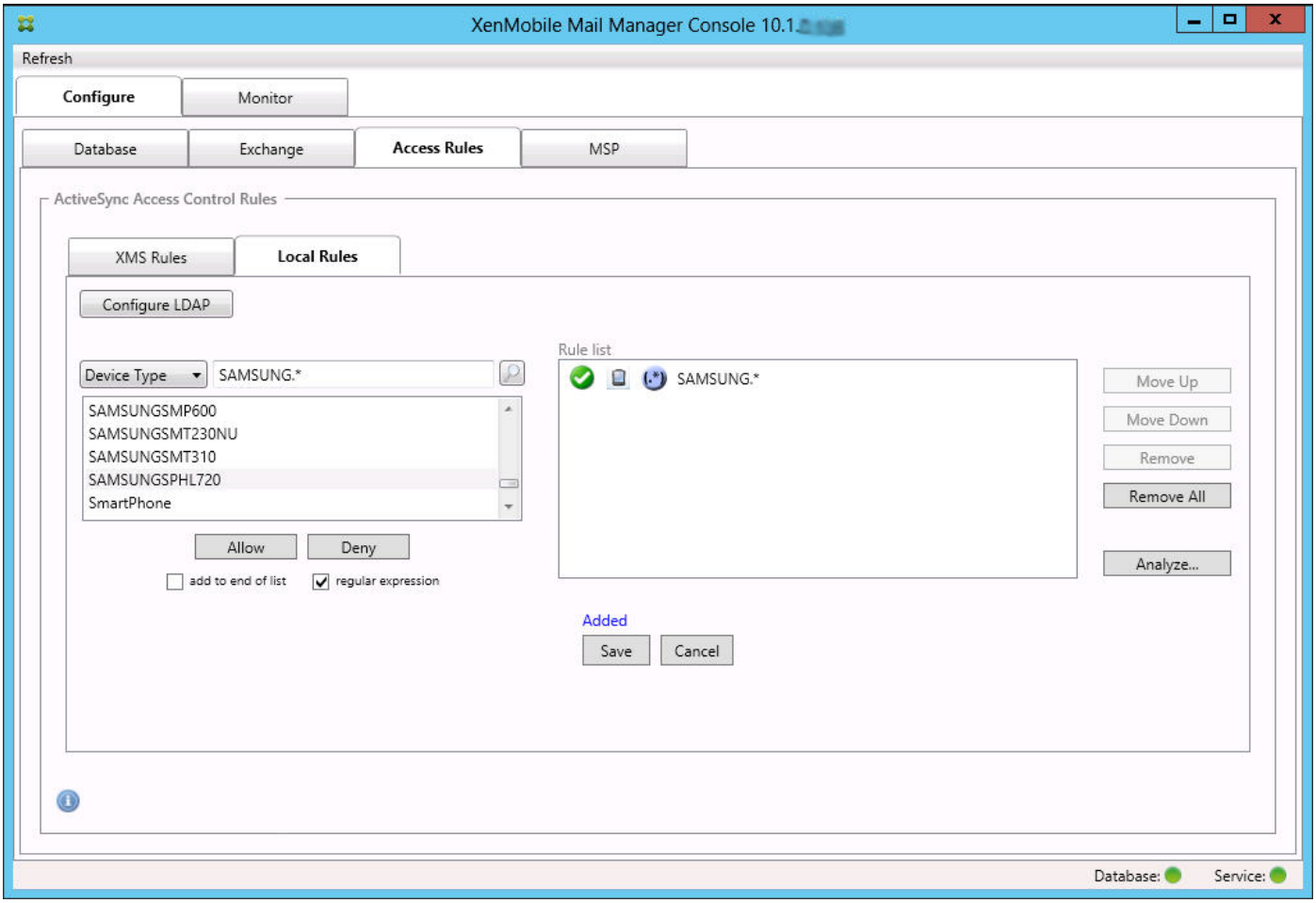


To build an access rule

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.



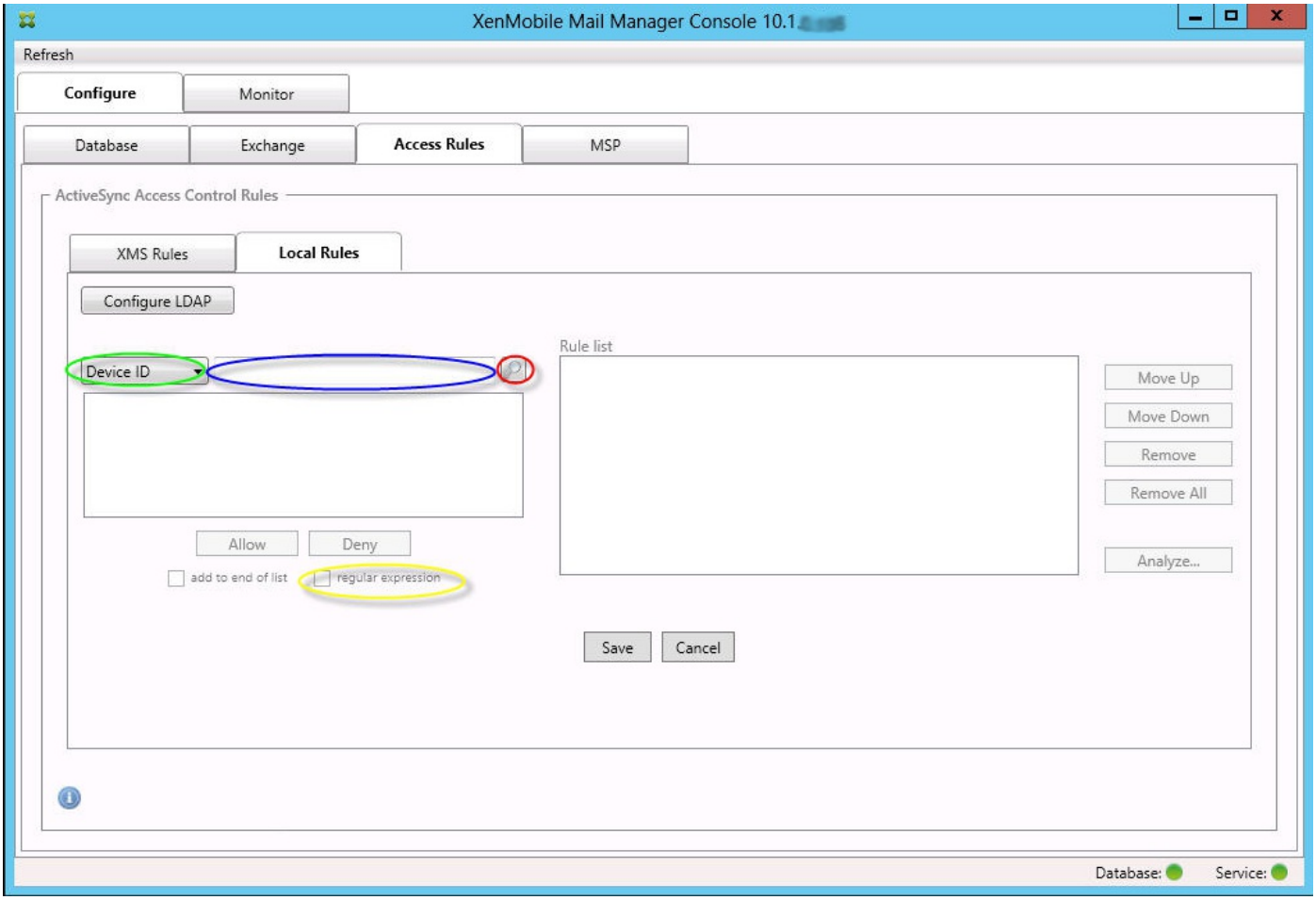
3. Select the field you want to match against. This example uses Device Type.
4. Type in the regular expression. This example uses samsung.*
5. Ensure that the regular expression check box is selected and then click Allow or Deny. In this example, the choice is Allow so that the final result is as follows:



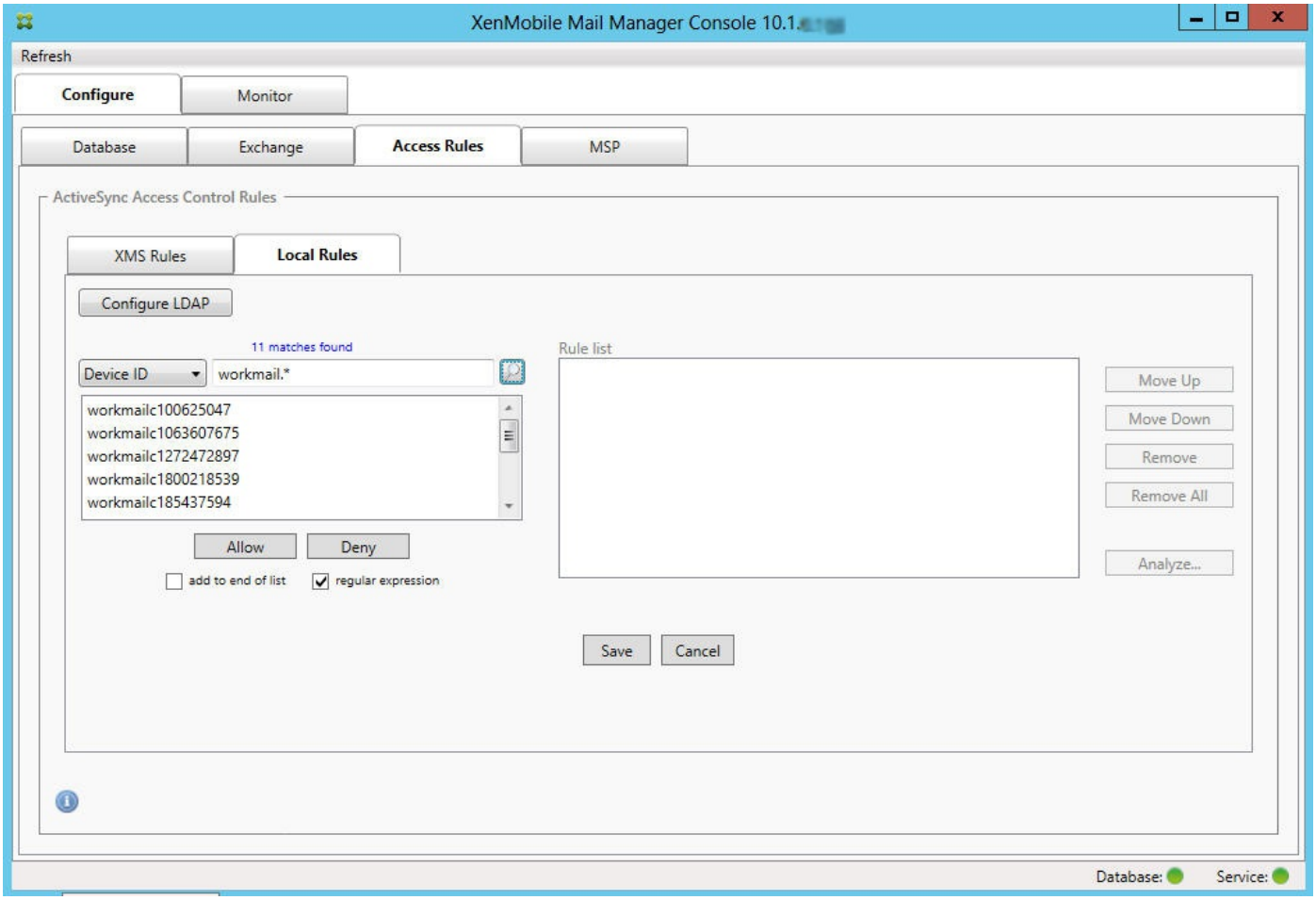
To find devices

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).



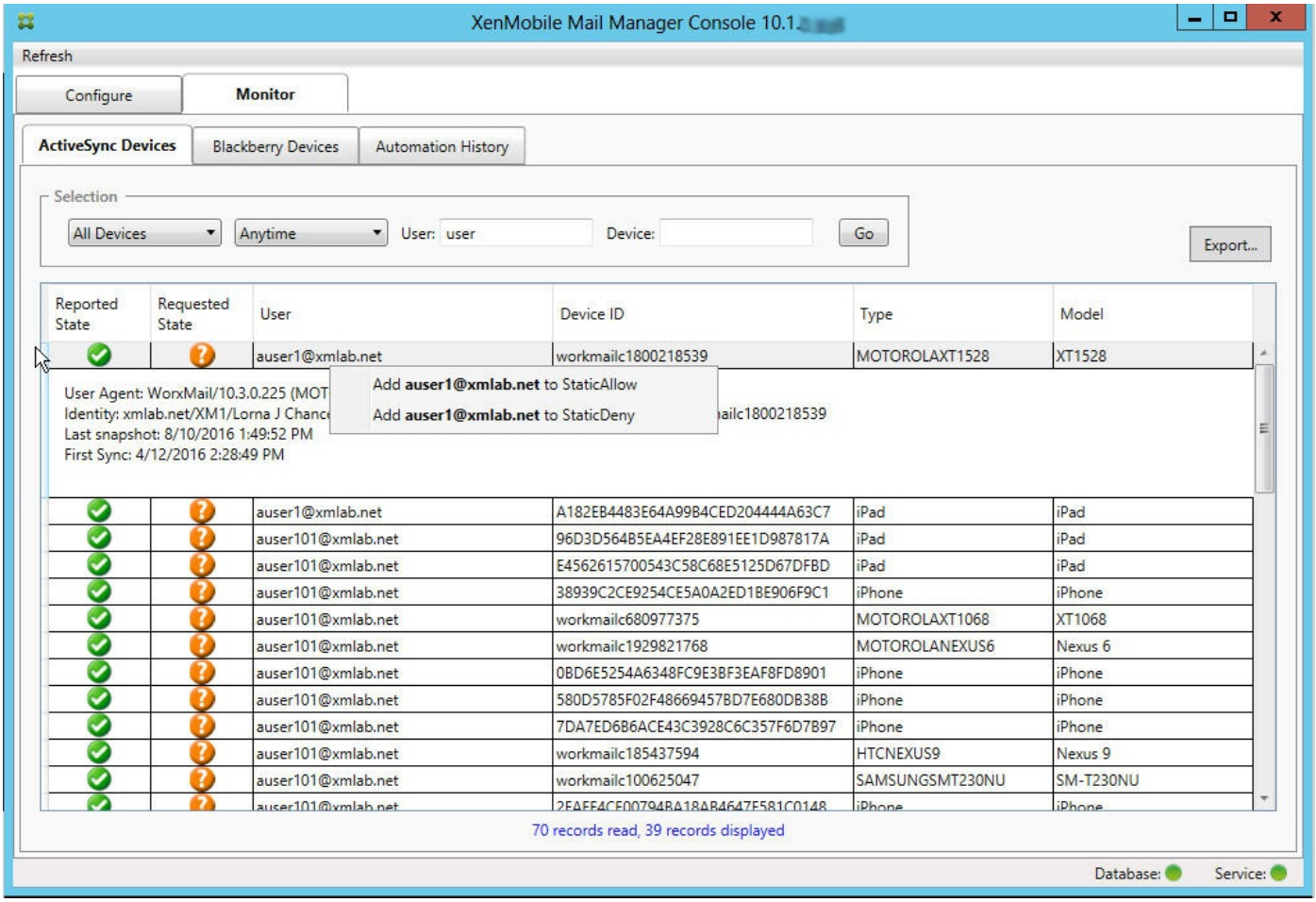
3. Click within the selected item text box (as shown in blue in the preceding figure) and then type workmail.*.
4. Make sure the regular expression check box is selected and then click the magnifying glass icon to display matches as shown in the following figure.



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

Feb 27, 2015

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

Oct 04, 2016

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.

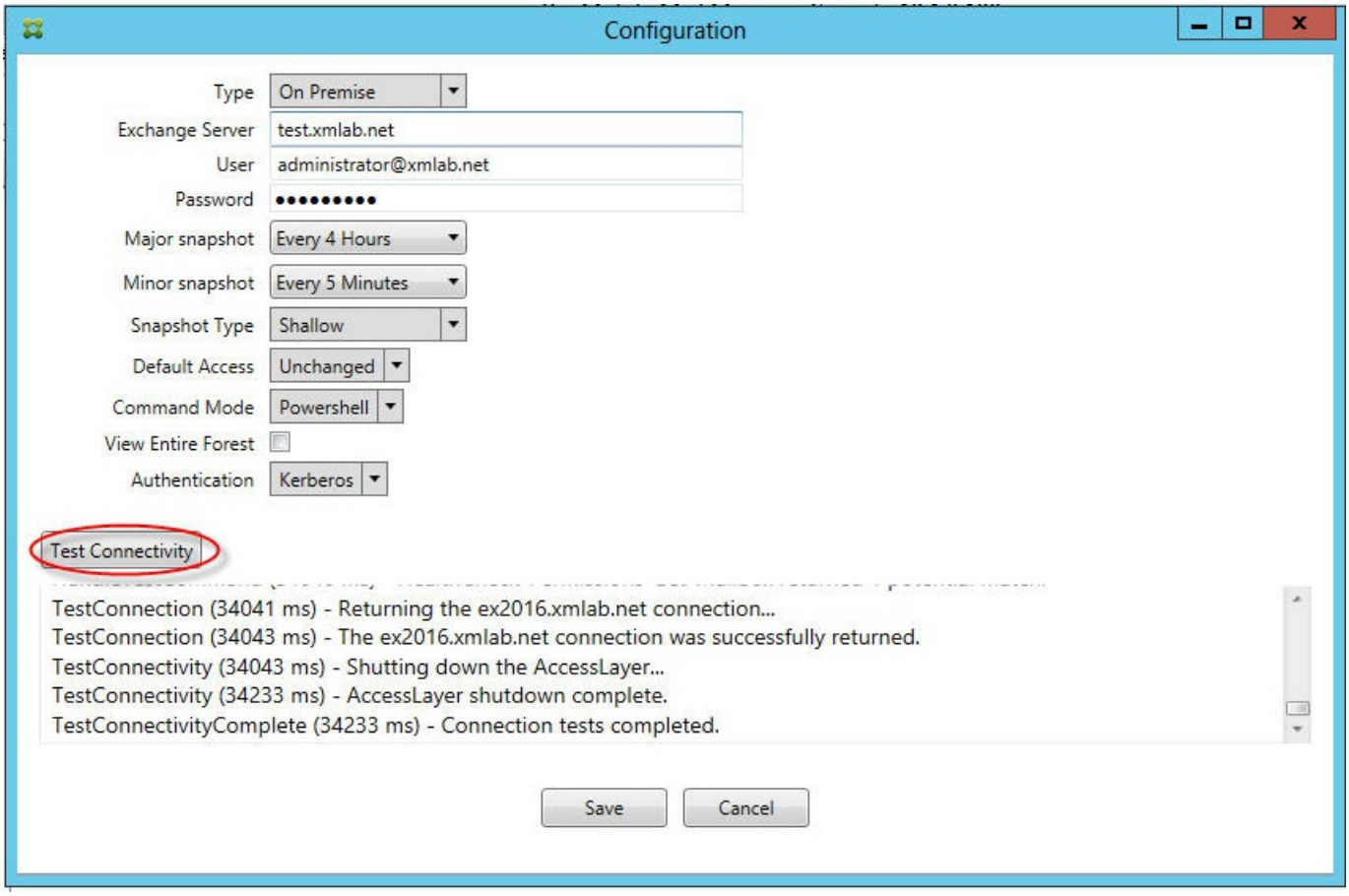
  If Windows Integrated authentication is configured, the user account of the XenMobile Mail Manager service must be an allowed SQL logon. The account of the XenMobile Mail Manager service defaults to Local System, but may be changed to any account that has local admin privileges. If SQL authentication 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

Aug 12, 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.