

About XenMobile 10

Aug 12, 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](#).

XenMobile 10 combines the App Controller and Device Manager components from XenMobile 9 and earlier versions into a unified management tool from which you can configure and manage user devices and apps.

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

For a list of fixed issues in this release, see <http://support.citrix.com/article/CTX141722>. For a list of known issues for XenMobile 10.0, see [Known Issues](#).

- **Unified infrastructure.** Mobile device management (MDM) and mobile app management (MAM) are unified within one server infrastructure.
 - You can deploy XenMobile faster due to fewer required setup steps.
 - You can manage apps and devices from one virtual server.
- **New unified XenMobile console.**
 - Designed with an easy-to-navigate user interface that simplifies administrative tasks, such as enrolling, deploying, configuring, and troubleshooting the entire mobility environment.
 - Simplified app and device policy configuration. You can configure one policy across all available device platforms.
- **Integration with NetScaler Gateway from the same console.** You can manage automated connectivity checks for multiple systems that are part of the mobility environment.
- **Beacons support deprecated.** Beacons are not supported in XenMobile 10, even though their options appear in the XenMobile console. Citrix recommends that you either connect to the XenMobile Server through NetScaler Gateway or, from within your firewall, directly to XenMobile Server.
- **Enhanced support for app authentication.** Helps to secure encryption between devices and the internal network, between the internal network and the XenMobile server, and for XenMobile console connections.
 - RSA Adaptive Authentication
 - Support for FIPS 140.2 advanced encryption

Getting Started with XenMobile 10

You start by downloading and installing the virtual image for XenMobile 10.0 Edition on a hypervisor, such as XenServer,

VMware ESXi, or Hyper-V, and then you complete the initial configuration of XenMobile on the hypervisor command-line console. For details, see [System Requirements](#), [Pre-Installation Checklist](#), and [Installing XenMobile](#).

Next, you open the web-based XenMobile console with the administrator account you set up during the initial configuration.

To help you decide where to go next in the console, see [Getting Started in the Console](#). The first set of recommendations covers initial settings you may have skipped during the installation steps.

Architecture Overview

Aug 12, 2016

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

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

- Connections to the internal network. If your users are remote, they can connect by using a VPN or micro VPN connection through NetScaler Gateway to access apps and desktops in the internal network.
- Device enrollment. Users can enroll mobile devices in XenMobile so you can manage the devices in the XenMobile console that connect to network resources.
- Web, SaaS, and mobile apps. Users can access their web, SaaS, and mobile apps from XenMobile through Worx Home.
- 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. 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.
- 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.

The following sections describe different reference architectures for the XenMobile deployment. For reference architecture diagrams, see the XenMobile Deployment Handbook sections, [Reference Architecture for On-Premises Deployments](#) and [Reference Architecture for Cloud Deployments](#). For a complete list of ports, see [XenMobile Port Requirements](#).

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](#).

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 10](#)). 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 10](#)). 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 10](#)). 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.

Scaling XenMobile 10

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 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.

Table 1. XenMobile Enterprise with Enrollment

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

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:

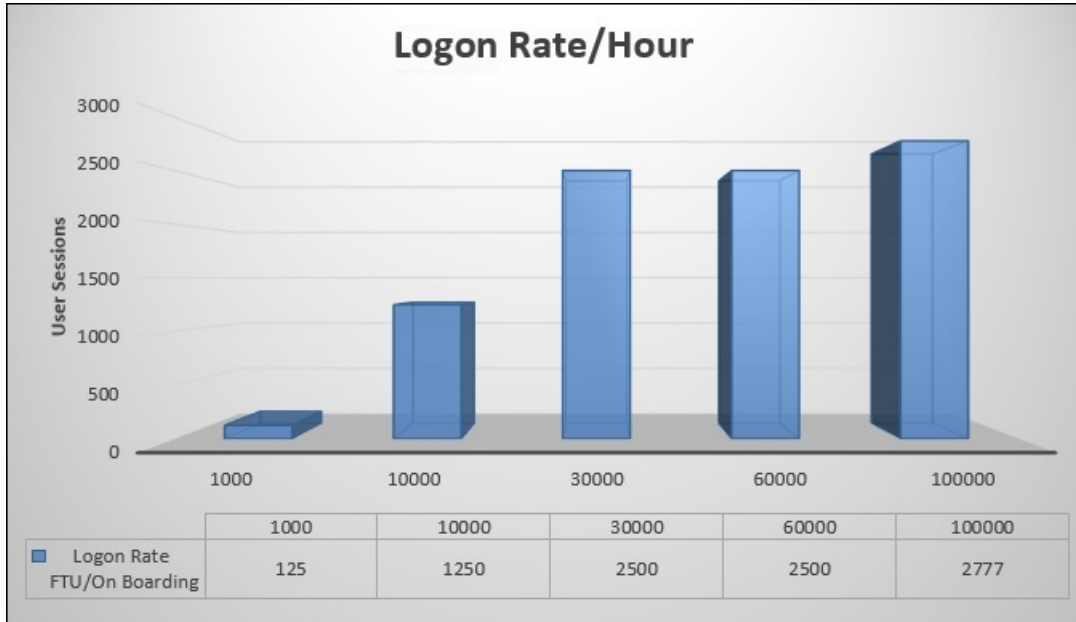
- Logon rate is an important factor in determining the scalability of a system. In addition to the initial logon, logon rates are dependent upon the authentication time-out values configured in your environment. For instance, if you set the authentication time-out value too low, users must perform more frequent logon requests. Therefore, you need to clearly understand how time-out settings affect your environment.
- 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.

Table 2. XenMobile Enterprise with Enrollment Scalability Results

Number of devices	1,000	10,000	30,000	60,000	100,000
Logon Rate					
On-boarding (FTU)	125	1,250	2,500	2,500	2,777
Existing users	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

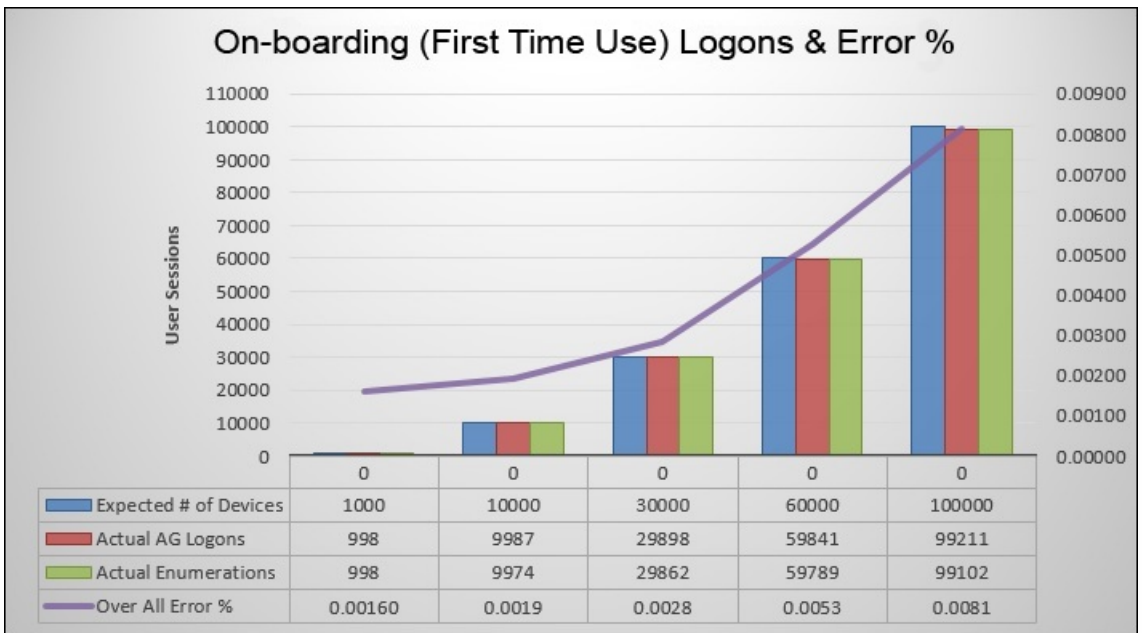
Database	External
----------	----------

The preceding 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.



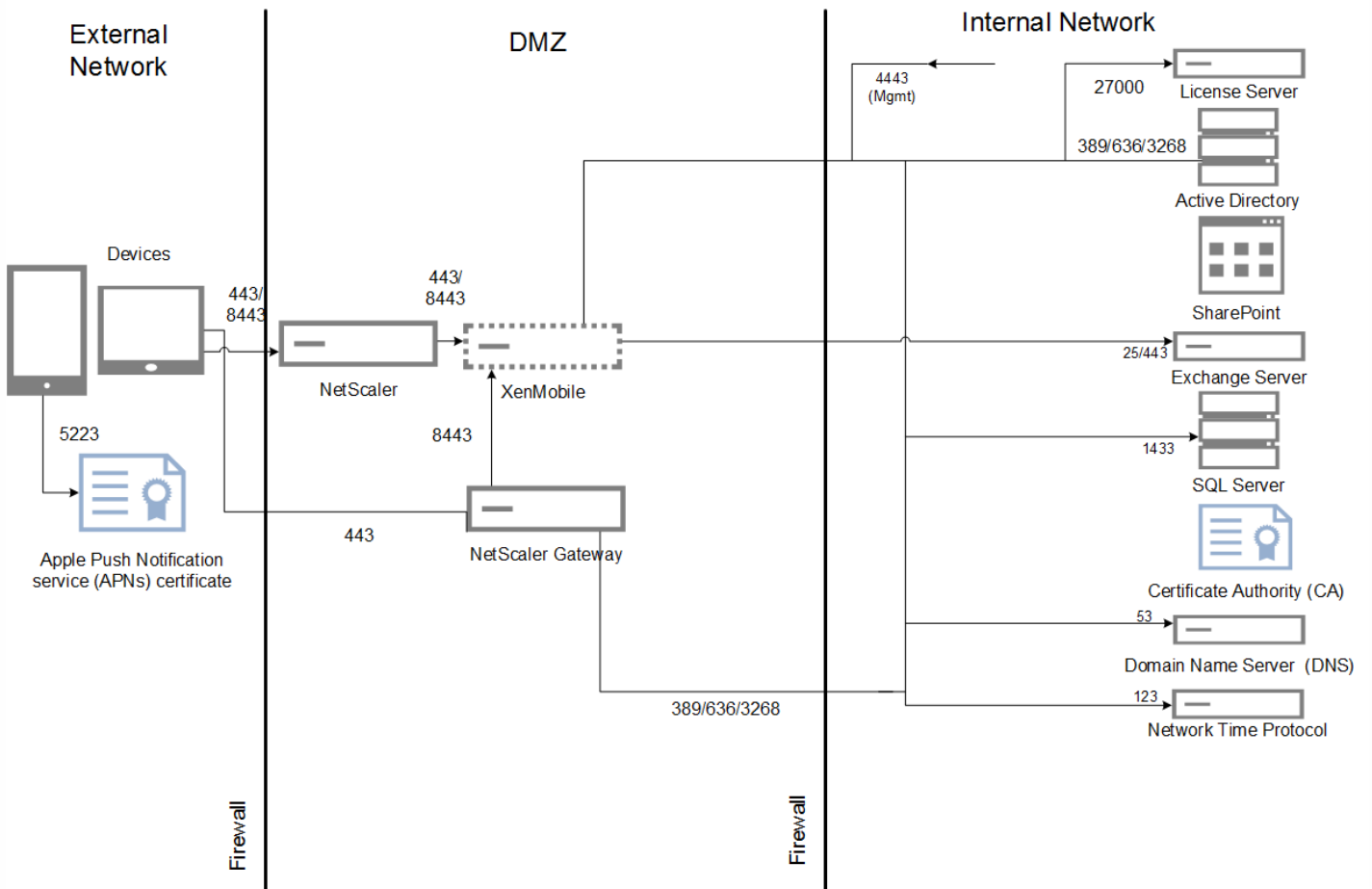
Note: You will experience the following if you exceed the recommended rates or hardware recommendations when sizing your system.

- Enrollment or logon latency (round-trip time)
 - Total average latency: > 1.5 seconds
 - Average latency for a NetScaler Gateway logon: > 440 ms
 - Average latency for a Worx Store request: > 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.

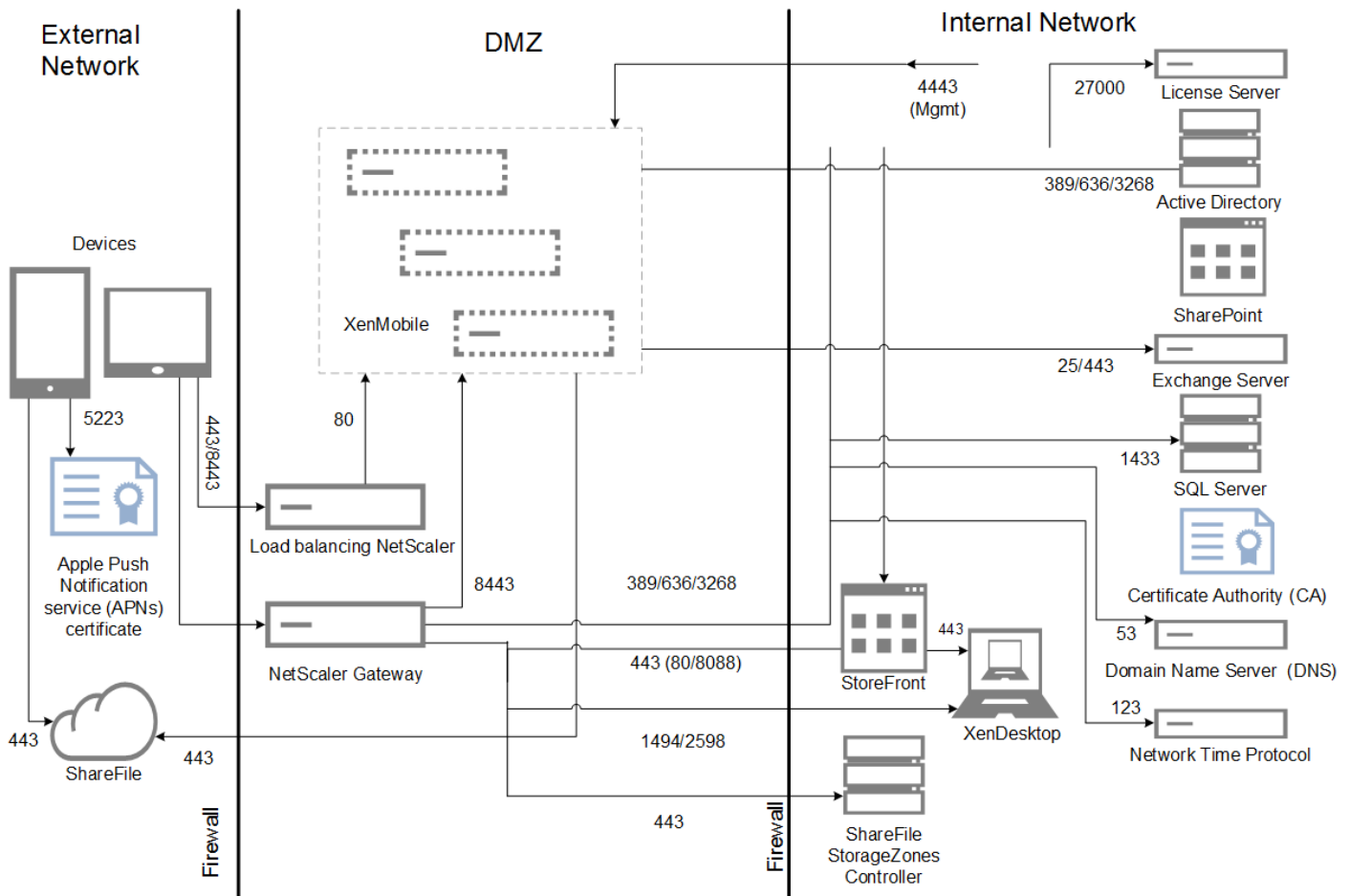


The error percentage in the preceding figure includes the overall error experienced considering requests corresponding to every operation and is not limited to logons. The error percentage is within the acceptable limit for each test run as defined in [Exit Criteria](#).

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 MDM 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 10,000 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:

Table 3. User Workload Definitions

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

sessions/devices	
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.

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)
- Minimal WorxMail and WorxWeb connections (VPN tunnels) — two connections
- Installation of required apps through XenMobile

The workload parameters included:

- 1 device registration per device
- 1 enumeration per device
- 14 apps enumerated per device
- 4 Worx Store launches per device
- 4 web/SaaS app SSOs per device
- 1 MDX app downloaded per device
- 2 required app downloads

Existing Users Workload

The following table shows the Existing Users workload. This workload simulated a user using WorxMail and WorxWeb apps. This simulation was used to measure the NetScaler Gateway port's scalability within the XenMobile configuration. For the WorxWeb app, users were accessing internal web sites, which do not trigger XenMobile SSO. Operations in this mode included:

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

WorxApps Connection Profiles

The following table shows the workload parameters for existing users.

Table 4. WorxApps Connection Profiles

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 session¹		~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).

Note: Modifications to the connection details affect analysis results. For example, if the number of connections per user is increased, then the number of NetScaler Gateway sessions supported may be reduced.

WorxMail and WorxWeb Profiles

The following tables show the WorxMail and WorxWeb profile details.

Table 5. 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

Table 6. 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.
- 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.

Table 7. XenMobile Infrastructure Components

Component	Version
NetScaler Gateway	10.5.55.8.nc
XenMobile	10.0.0.62300
External database	MS SQL Server 2008 R2 (128 GB RAM, 300 GB disk space, 24 virtual CPUs)

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

Table 8. XenServer Hardware

Vendor	GenuineIntel
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).

For additional product information and technical questions concerning this article or the products mentioned herein, see [Citrix.com](https://docs.citrix.com), search the XenMobile documentation [site](#) for the latest product documentation, or contact your local Citrix representative.

About XenMobile Cloud

Aug 12, 2016

XenMobile Cloud is a product service that offers a XenMobile enterprise mobility management (EMM) environment for managing apps and devices as well as users or groups of users. With XenMobile Cloud, Citrix handles the configuration and maintenance of the infrastructure onsite through the Citrix Cloud Operations group. This separation lets you focus exclusively on the user experience and on managing devices, policies, and apps. XenMobile Cloud also replaces the need to purchase and manage licenses with a subscription fee.

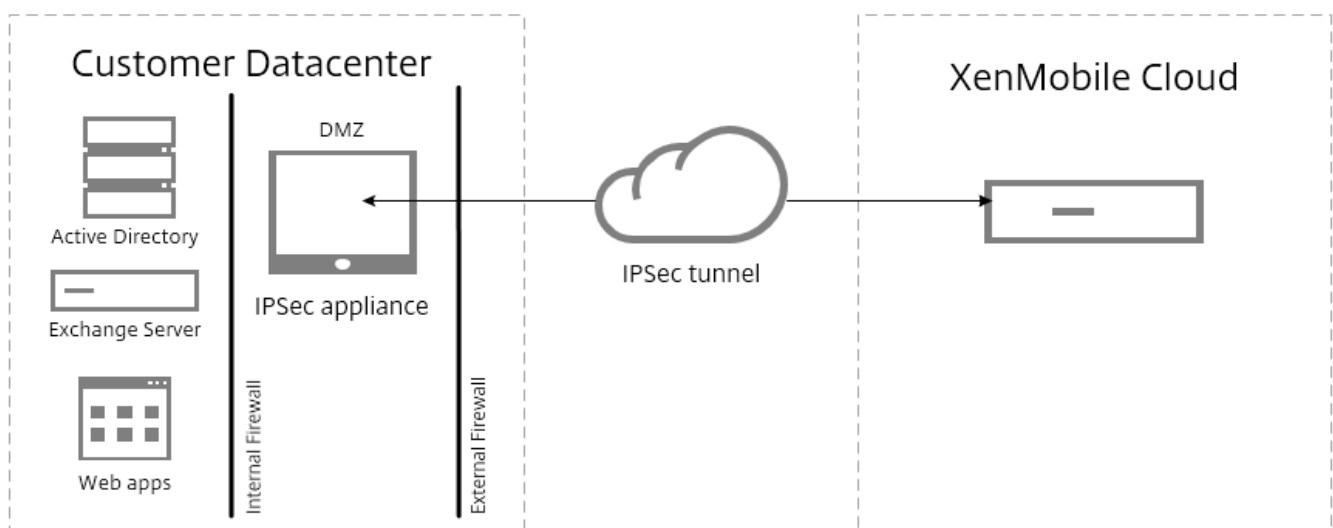
Cloud Operations administrators handle maintenance and configuration of the network connectivity, as well as the integration of Citrix products like NetScaler, XenApp, XenDesktop, StoreFront, and ShareFile. The Cloud environment is hosted in Amazon datacenters located throughout the world to deliver high performance, rapid response, and support.

To get started with XenMobile Cloud, go to <https://www.citrix.com/products/xenmobile/tech-info/cloud.html>

Note

- The Remote Support client is not available in XenMobile Cloud versions 10.x for Windows CE and Samsung Android devices.
- XenMobile Cloud server-side components are not FIPS 140-2 compliant.
- Citrix does not support syslog integration in XenMobile Cloud with an on-premises syslog server. Instead, you can download the logs from the Support page in the XenMobile console. When doing so, you must click Download All in order to get system logs. For details, see [Viewing and Analyzing Log Files in XenMobile](#).

The basic architecture of XenMobile Cloud is shown in the following figure. For detailed reference architecture diagrams, see the [XenMobile Deployment Handbook](#) section, "Reference Architecture for Cloud Deployments."



You can integrate XenMobile Cloud architecture into your existing infrastructure by installing and deploying Citrix CloudBridge or by using an existing IPsec gateway in your datacenter.

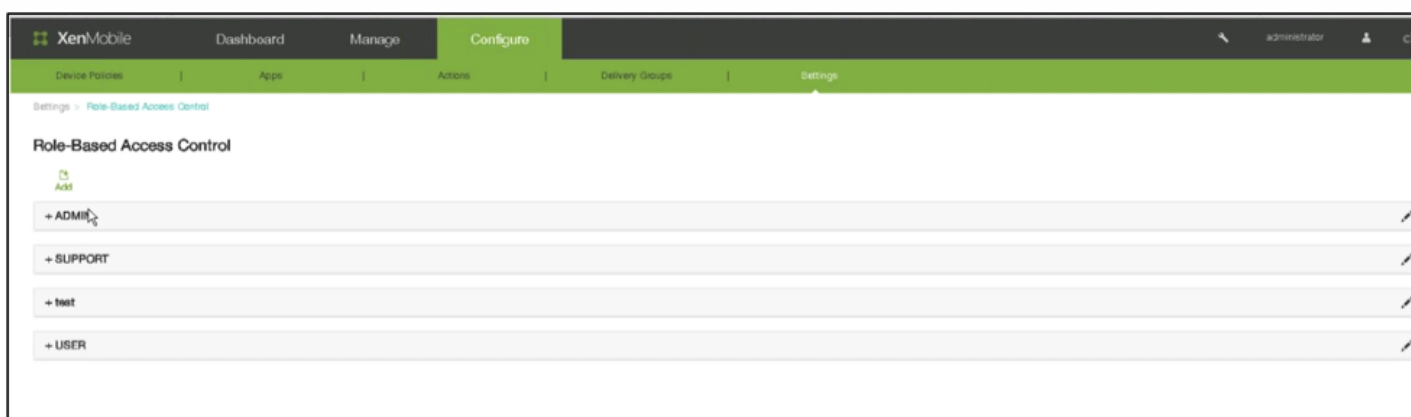
This architecture allows you to benefit from using NetScaler either in the cloud, as handled by the Cloud Operations group, or in your datacenter. When used in the datacenter, NetScaler gives you a single point of management to control access and limit actions within sessions based on both user identity and the endpoint device. This deployment provides better application security, data protection, and compliance management.

To download and install Citrix CloudBridge, go to <https://www.citrix.com/downloads/cloudbridge.html>

Roles in XenMobile Cloud

XenMobile Cloud uses the same Role Based Access Control (RBAC) as an on-premise deployment of XenMobile. The difference with XenMobile Cloud is that the Citrix Cloud Operations group handles any role, including provisioning, that deals with the infrastructure.

The following figure shows the RBAC console for XenMobile Cloud.



XenMobile implements four default user roles to logically separate access to system functions. The default roles are as follows:

- **Administrator.** Grants full system access.
- **Support.** Grants access to remote support.
- **User.** Grants users access to enrolling devices and using the Self Help Portal.
- **Provisioning.** Grants administrators the ability to provision all Windows Mobile/CE devices as a group using the Device Provisioning Tool. This role is handled by the Cloud Operation group.

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 these default roles.

You can assign roles to 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.

The following roles are available for you to assign. The Citrix Cloud Operations Group handles any role not on this list.

Main Section	Section	Page	Page Visible to
Dashboard	ALL	ALL	IT Admin
Manage	Devices	ALL	IT Admin
Manage	Enrollment	ALL	IT Admin
Configure	Device Policies	ALL	IT Admin
Configure	Apps	ALL	IT Admin
Configure	Actions	ALL	IT Admin
Configure	Delivery Groups	ALL	IT Admin
Configure	Settings	Certificates	Cloud Admin and IT Admin
Configure	Settings	Notification Templates	IT Admin
Configure	Settings	Role Based Access Control	Cloud Admin and IT Admin
Configure	Settings	Enrollment	IT Admin
Configure	Settings	Local Users and Groups	Cloud Admin and IT Admin
Configure	Settings	Release Management	Cloud Admin and IT Admin
Configure	Settings	Workflows	IT Admin
Configure	Settings	Credential Providers	IT Admin
Configure	Settings	PKI Entities	IT Admin
Configure	Settings	Client Properties	IT Admin

Configure	Settings	NetScaler Gateway	Cloud Admin Only OR IT Admin Only
Configure	Settings	Carrier SMS Gateway	IT Admin
Configure	Settings	Notification Server	Cloud Admin and IT Admin
Configure	Settings	ActiveSync Gateway	IT Admin
Configure	Settings	iOS VPP	IT Admin
Support	Log Operations	Log Settings	Cloud Admin and IT Admin and Tech Support
Configure	Settings	Server Properties	Cloud Admin and IT Admin and Tech Support
Configure	Settings	Google Play Credentials	IT Admin
Configure	Settings	LDAP	IT Admin
Configure	Settings	Network Access Control	IT Admin
Support	Support Bundle	Create Support Bundles	Cloud Admin and Tech Support
Configure	Settings	iOS Device Enrollment Program	IT Admin
Configure	Settings	Mobile Service Provider	IT Admin
Configure	Settings	Samsung KNOX	IT Admin
Configure	Settings	XenApp/ XenDesktop	IT Admin
Configure	Settings	ShareFile	IT Admin
Support	Advanced	Cluster Information	Cloud Admin and Tech Support
Support	Advanced	Garbage Collection	Cloud Admin and Tech Support

Support	Advanced	Java Memory Properties	Cloud Admin and Tech Support
Support	Advanced	Macros	IT Admin
FTU Wizard	Initial Configuration	NetScaler Gateway	Cloud Admin Only OR IT Admin Only
Configure	Settings	Worx Home Support	IT Admin
Configure	Settings	Worx Store Branding	IT Admin
Support	Diagnostics	NetScaler Gateway Connectivity Checks	Cloud Admin and IT Admin and Tech Support
Support	Diagnostics	XenMobile Connectivity Checks	Cloud Admin and IT Admin and Tech Support
Support	Log Operations	Logs	Cloud Admin and IT Admin and Tech Support
Support	Advanced	PKI Configuration	Cloud Admin and IT Admin
Support	Tools	APNS Signing Utility	Customer and Tech Support
Support	Tools	Citrix Insight Services	Cloud Admin and IT Admin and Tech Support
FTU Wizard	Initial Configuration	SSL Certificate	Cloud Admin and IT Admin
FTU Wizard	Initial Configuration	LDAP Configuration	IT Admin
FTU Wizard	Initial Configuration	Notification Server	Cloud Admin and IT Admin
FTU Wizard	Initial Configuration	Summary	Cloud Admin and IT Admin
Support	Links	Citrix Knowledge Center	Cloud Admin and IT Admin and Tech Support
Support	Tools	Device NetScaler Connector Status	IT Admin

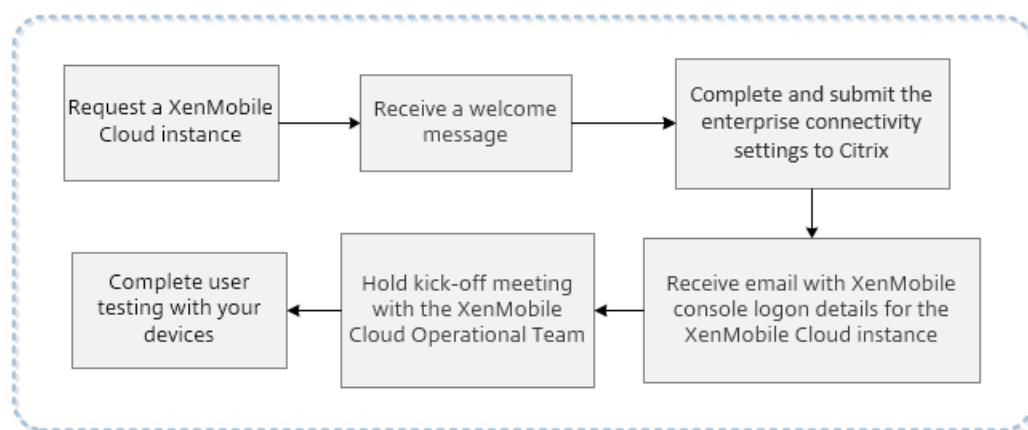
For step-by-step instructions on customizing roles, see [Configuring Roles with RBAC](#).

To request a restart of the server nodes, contact technical support at <https://www.citrix.com/contact/technical-support.html>

XenMobile Cloud Prerequisites and Administration

Feb 24, 2016

The steps that make up the onboarding process from the time you make a request for a XenMobile Cloud instance through to user testing with the devices in your organization are shown in the following figure. When you are evaluating or purchasing XenMobile Cloud, the XenMobile Cloud Operational team provides ongoing onboarding help and communication to ensure that the core XenMobile Cloud services are running and configured correctly.



Citrix hosts and delivers your XenMobile Cloud solution. Some communication and port requirements, however, are required to connect the XenMobile Cloud infrastructure to corporate services, such as Active Directory. Review the following sections to prepare for your XenMobile Cloud deployment.

XenMobile Cloud IPsec tunnel gateways

You can use a XenMobile Enterprise Connector, an IPsec tunnel to connect the XenMobile Cloud infrastructure with corporate services, such as Active Directory.

The IPsec gateways listed in the following Amazon Web Services website are officially tested and supported with the XenMobile Cloud solution: <http://aws.amazon.com/vpc/faqs/>. Scroll to the “Q. What customer gateway devices are known to work with Amazon VPC?” section to find the list of supported gateways.

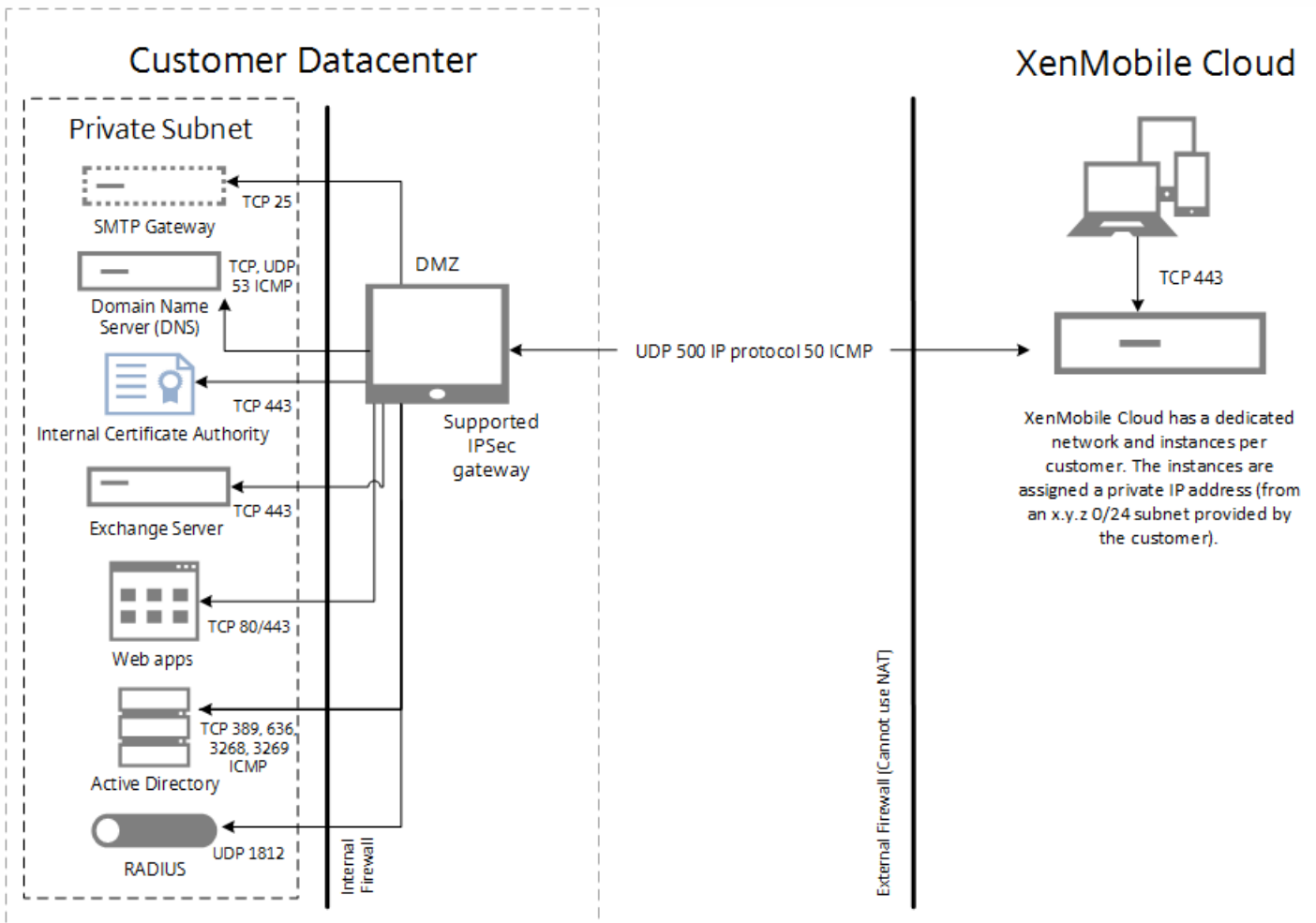
Note

If your IPsec gateway is not part of the approved list, the IPsec gateway may still work with XenMobile Cloud, but could take longer to set up, and may require you to use one of the official supported IPsec gateways as a fallback plan.

Your IPsec gateway needs to have a public IP address assigned directly to it, and the address cannot use Network Address Translation (NAT).

The following figure shows how the IPsec tunnel is configured in the XenMobile Cloud solution to connect to your

corporate services through various ports.



The following table shows communication and port requirements for a XenMobile Cloud deployment, including IPsec tunnel requirements.

Source	Destination	Protocols	Port	Description
External (edge) firewall - Inbound rules				
Public IP addresses of XenMobile cloud (AWS) IPCSEC VPN ¹	Customer IPsec appliance	UPD	500	IPsec IKE configuration.
Public IP addresses of XenMobile cloud (AWS) IPCSEC VPN ¹	Customer IPsec appliance	IP Protocol ID	50	IPsec ESP protocol.
Public IP addresses of XenMobile cloud	Customer IPsec appliance	ICMP		For troubleshooting (can be removed post-setup).

(AWS) IPCSEC VPN ¹				
External (edge) firewall - Outbound rules				
Customer DMZ subnet	Public IP addresses of XenMobile cloud (AWS) IPsec VPN ¹	UDP	500	IPsec IKE configuration.
Customer DMZ subnet	Public IP addresses of XenMobile cloud (AWS) IPsec VPN ¹	IP Protocol ID	50, 51	IPsec ESP protocol.
Customer DMZ subnet	Public IP addresses of XenMobile cloud (AWS) IPsec VPN ¹	ICMP		For Troubleshooting (can be removed post-setup).
Internal firewall - Inbound rules				
Unused and routable /24 customer subnet ²	Internal DNS servers in customer data center	TCP, UDP, ICMP	53	DNS resolution.
Unused and routable /24 customer subnet ²	Active Directory domain controllers in customer data center	LDAP(TCP)	389, 636 3268, 3269	For user Active Directory authentication and directory queries to domain controllers.
Unused and routable /24 customer subnet ²	Active Directory domain controllers in customer data center	ICMP		For troubleshooting (can be removed once the entire setup is completed).
Unused and routable /24 customer subnet ²	Exchange Servers in customer data center	SMTP (TCP)	25	Optional: For XenMobile email notification.
Unused and routable /24 customer subnet ²	Exchange Servers in customer data center	HTTP, HTTPS (TCP)	80, 443	Exchange ActiveSync, which is needed if ActiveSync traffic is sent from device to the XenMobile cloud infrastructure (through IPsec tunnel) to the Exchange Servers.

				This is NOT needed if the user device will communicate with a public ActiveSync FQDN via the Internet without a need for going through the XenMobile IPsec tunnel to the Exchange Servers.
Unused and routable /24 customer subnet ²	Application servers, such as intranet/web servers, SharePoint servers, and so on.	HTTP, HTTPS (TCP)	80, 443	Access to intranet and/or application servers from user mobile devices through the XenMobile IPsec tunnel. Each application server needs to be added to the firewall rules with the port number required to access the application (typically port 80 and/or 443).
Unused and routable /24 customer subnet ²	PKI server (if on-premise PKI is used)	HTTPS (TCP)	443	Optional (not used for XenMobile POCs): This can be leveraged to establish an integration between the XenMobile cloud infrastructure and an on-premise PKI infrastructure (such as Microsoft CA) to establish certificate-based authentication within the XenMobile solution.
Unused and routable /24 customer subnet ²	RADIUS server	UDP	1812	Optional (not used for XenMobile POCs): This can be used to establish two-factor authentication within the XenMobile solution.
Internal firewall - outbound rules				
Internal customer subnets, from where the XenMobile console needs to be available	Unused and routable /24 customer subnet ²	TCP	4443	XenMobile App Controller (MAM) console in the XenMobile Cloud infrastructure.

¹ Will be provided by the XenMobile Cloud team when the XenMobile Cloud instance and IPSec components are provisioned in the XenMobile Cloud infrastructure.

² An unused /24 subnet provided by the customer as part of the provisioning process, which does not conflict with internal subnets in the customer data center, and which is routable.

If you plan to deploy XenMobile Mail Manager or XenMobile NetScaler Connector for native email filtering, such as the ability to block or allow email connectivity from native email clients on users' mobile devices, review the following additional requirements.

XenMobile Apple APNs certificate

If you plan to manage iOS devices with your XenMobile Cloud deployment, you need an Apple APNs certificate. You should prepare the certificate before you deploy your XenMobile Cloud solution. For steps, see [Requesting an APNs certificate](#).

WorxMail for iOS push notification certificate

If you want to make use of push notification for your WorxMail deployment, you should prepare an Apple APNs certificate for iOS WorxMail push notification. For details, see [Push Notifications for WorxMail for iOS](#).

XenMobile MDX Toolkit

The MDX Toolkit is an app wrapping technology that prepares apps for secure deployment with XenMobile. If you want to wrap apps, such as Citrix WorxMail, WorxMail, WorxNotes, QuickEdit, and so on, you need to install the MDX Toolkit. For details, see [About the MDX Toolkit](#).

If you plan to wrap iOS apps, you need an Apple Developer account to create the necessary Apple distribution profiles. For details, see the MDX Toolkit [System Requirements](#) and the [Apple Developer account](#) website.

If you plan to wrap apps for Windows Phone 8.1 devices, see the [System Requirements](#).

XenMobile autodiscovery for Windows Phone enrollment

If you want to make use of XenMobile autodiscovery for your Windows Phone 8.1 enrollment, make sure you have a public SSL certificate available. For details, see [To enable autodiscovery in XenMobile for user enrollment](#).

The XenMobile console

The XenMobile Cloud solution makes use of the same web console as an on-premise XenMobile deployment. In this way, day-to-day administration of your Cloud solution, such as policy management, app management, device management and so on occurs in a similar way as an on-premise XenMobile deployment. For information about managing apps and devices in

the XenMobile console, see [Getting Started with the XenMobile Console](#).

XenMobile device enrollment

For information about XenMobile enrollment options for the different device platforms, see [Enrolling Users and Devices](#).

XenMobile support

For details on how to access supported related information and tools in the XenMobile console, see [XenMobile Support and Maintenance](#).

Supporting Mobile Platforms in XenMobile Cloud

Feb 24, 2016

After you make a request for a XenMobile Cloud instance, you can, if you like, begin preparing to support Android, iOS, and Windows platforms. As you complete the steps that apply to your environment, keep the information handy so you can use it when configuring settings in the XenMobile console.

Note that these requirements are a subset of the overall communication and port requirements that make up the XenMobile Cloud onboarding process. For details, see [XenMobile Cloud Prerequisites and Administration](#).

Android

- Create Google Play credentials. For details, see Google Play [Getting Started with Publishing](#).
- Create an Android for Work administrator account. For details, see [Managing Devices with Android for Work in XenMobile](#).
- Verify your domain name with Google. For details, see [Verify your domain for Google Apps](#).
- Enable APIs and create a service account for Android for Work. For details, see [Google for Work Android](#).

iOS

- Create an Apple ID and developer account. For details, see the [Apple Developer Program](#) website.
- Create an Apple Push Notification service (APNs) certificate. For details, see the [Apple Push Certificates Portal](#).
- Create a Volume Purchase Program (VPP) company token. For details, see [Apple Volume Purchasing Program](#).

Windows

- Create a Microsoft Windows Store developer account. For details, see the [Microsoft Windows Dev Center](#).
- Obtain a Microsoft Windows Store Publisher ID. For details, see the [Microsoft Windows Dev Center](#).
- Acquire an enterprise certificate from Symantec. For details, see the [Microsoft Windows Dev Center](#).
- Create an Application Enrollment Token (AET). For details, see the [Microsoft Windows Dev Center](#).

System Requirements

Nov 08, 2016

To run XenMobile 10, you need the following minimum system requirements:

- One of the following:
 - XenServer (supported versions: 6.2.x, 6.1.x, or 6.0.x); for details, refer to [XenServer](#)
 - VMWare (supported versions: ESXi 5.5, ESXi 5.1, ESXi 4.1); for details, refer to [VMware](#)
 - Hyper-V (supported versions: Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2); for details, refer to [Hyper-V](#)
- Dual core processor
- Two virtual CPUs
- 8 GB of RAM
- 50 GB disk space

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

- Quad core processor
- 8 GB of RAM

For system requirements for the XenMobile 10.4 release, see [System requirements](#).

NetScaler Gateway System Requirements

To run NetScaler Gateway with XenMobile 10, you need the following minimum system requirements:

- XenServer, VMWare, or Hyper-V
- 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 Database Requirements

The XenMobile repository requires a Microsoft SQL Server database running on one of the following supported versions:

- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008

Citrix XenMobile supports SQL Always on availability group and SQL Clustering for database high availability. Citrix does not support database mirroring for XenMobile database high availability. We do support database high availability with Active/Active or Active Passive mode with MS SQL Cluster deployment..

Note: If database is offline, the XenMobile server will not service any connections from devices as XenMobile server will also be offline.

Citrix recommends using Microsoft SQL remotely. PostgreSQL is included with XenMobile and should be used locally or

remotely only in test environments.

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](#)

XenMobile Compatibility

Feb 28, 2017

For a summary of XenMobile components that you can integrate, see [XenMobile Compatibility](#).

Supported Device Platforms in XenMobile

Feb 27, 2017

You can find the complete list of devices that XenMobile 10.x supports for enterprise mobility management in [Supported device operating systems](#).

Port Requirements

Sep 30, 2016

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

Opening Ports for NetScaler Gateway and XenMobile to Manage Apps

You must open the following ports to allow user connections from 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	NetScaler Gateway	XenApp or XenDesktop

	applications in the internal network using session reliability. Citrix recommends keeping this port open.		
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
443	Used for outbound connections to AutoDiscovery server.	XenMobile	https://discovery.mdm.zenprise.com
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 TCP port	Description Used for APNs outbound connections from iOS devices on Wi-Fi networks to *.push.apple.com.	Source iOS devices on WiFi networks	Destination Internet (APNs hosts using the public IP address 17.0.0.0/8)
8443	Used for enrollment of iOS and Windows Phone devices.	Internet	XenMobile
		LAN and WiFi	

Port Requirement for Auto Discovery Service Connectivity

This port configuration ensures that Android devices connecting from Worx Home for Android 10.2 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 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
	54.225.219.53
	54.243.185.79
	107.22.184.230
	107.20.173.245

discovery.mdm.zenprise.com

184.72.219.144

184.73.241.73

54.243.233.48

204.236.239.233

107.20.198.193

FIPS 140-2 Compliance

Sep 08, 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.

/

-
- [AppDNA](#)
 - [Citrix Cloud](#)
 - [Citrix Receiver](#)
 - [CloudBridge](#)
 - [CloudPortal Services Manager](#)
 - [NetScaler](#)
 - [NetScaler Gateway](#)
 - [NetScaler SD-WAN](#)
 - [ShareFile](#)
 - [Unidesk](#)
 - [VDI-in-a-Box](#)
 - [XenApp and XenDesktop](#)
 - [XenMobile](#)
 - [XenServer](#)
-
- [Advanced Concepts](#)
 - [Developer](#)
 - [Legacy Documentation](#)

Feel your pain.

This link is not here. The link might be misspelled or out dated.

Search or navigate for the content
and retry the link

Investigate

Feedback link at the bottom of [Docs.citrix.com](https://docs.citrix.com) to tell us about it

Pre-Installation Checklist

Apr 15, 2015

You can use this checklist to note the prerequisites and settings for installing XenMobile 10. Each task or note includes a column indicating the component or function for which the requirement applies. For installation steps, see [Installing XenMobile](#).

Basic Network Connectivity

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

• Prerequisite or setting	Component or function	Note the setting
Note the fully qualified domain name (FQDN) to which remote users connect.	XenMobile NetScaler Gateway	
Note the public and local IP address. You need these IP addresses to configure the firewall to set up network address translation (NAT).	XenMobile NetScaler Gateway	
Note the subnet mask.	XenMobile NetScaler Gateway	
Note the DNS IP addresses.	XenMobile NetScaler Gateway	
Write down the WINS server IP addresses (if applicable).	NetScaler Gateway	
Identify and write down the NetScaler Gateway host name. Note: This is not the FQDN. The FQDN is contained in the signed server certificate that is bound to the virtual server and to which users connect. You can configure the host name by using the Setup Wizard in NetScaler Gateway.	NetScaler Gateway	
Note the IP address of XenMobile. Reserve one IP address if you install one instance of XenMobile.	XenMobile	

<ul style="list-style-type: none"> Prerequisite or setting. If you configure a cluster, note all of the IP addresses you need. 	Component or function	Note the setting
<ul style="list-style-type: none"> • One public IP address configured on NetScaler Gateway • One external DNS entry for NetScaler Gateway 	NetScaler Gateway	
<p>Note the web proxy server IP address, port, proxy host list, and the administrator user name and password. These settings are optional if you deploy a proxy server in your network (if applicable).</p> <p>Note: You can use either the sAMAccountName or the User Principal Name (UPN) when configuring the user name for the web proxy.</p>	XenMobile NetScaler Gateway	
<p>Note the default gateway IP address.</p>	XenMobile NetScaler Gateway	
<p>Note the system IP (NSIP) address and subnet mask.</p>	NetScaler Gateway	
<p>Note the subnet IP (SNIP) address and subnet mask.</p>	NetScaler Gateway	
<p>Note the NetScaler Gateway virtual server IP address and FQDN from the certificate.</p> <p>If you need to configure multiple virtual servers, note all of the virtual IP addresses and FQDNs from the certificates.</p>	NetScaler Gateway	
<p>Note the internal networks that users can access through NetScaler Gateway.</p> <p>Example: 10.10.0.0/24</p> <p>Enter all internal networks and network segments that users need access to when they connect with Worx Home or the NetScaler Gateway Plug-in when split tunneling is set to On.</p>	NetScaler Gateway	
<p>Make sure that the network connectivity between the XenMobile server, NetScaler Gateway, the external Microsoft SQL Server, and the DNS server are reachable.</p>	XenMobile NetScaler Gateway	

Licensing

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

✔	Prerequisite	Component	Note the location
	Obtain Universal licenses from the Citrix web site . For details, see Installing NetScaler Gateway Licenses .	NetScaler Gateway XenMobile Citrix License Server	

Certificates

XenMobile and NetScaler Gateway require certificates to enable connections with other Citrix products and app and from user devices. For details, see [Certificates in XenMobile](#).

✔	Prerequisite	Component	Notes
	Obtain and install required certificates.	XenMobile NetScaler Gateway	

Ports

You need to open ports to allow communication with the XenMobile components. For a complete list of ports you need to open, see [XenMobile Port Requirements](#).

✔	Prerequisite	Component	Notes
	Open ports for XenMobile	XenMobile NetScaler Gateway	

Database

You need to configure a database connection. The XenMobile repository requires a Microsoft SQL Server database running on one of the following supported versions: Microsoft SQL Server 2014, SQL Server 2012, SQL Server 2008 R2, or SQL Server 2008. Citrix recommends using Microsoft SQL remotely. PostgreSQL is included with XenMobile and should be used locally or remotely only in test environments.

•	Prerequisite	Component	Note the setting
	Microsoft SQL Server IP address and port. Make sure the service account of the SQL Server to be used on XenMobile has the DBcreator role permission.	XenMobile	

Active Directory Settings	Prerequisite	Component	Note the setting
<ul style="list-style-type: none"> Prerequisite 		Component XenMobile NetScaler Gateway	Note the setting
<p>Note the Active Directory IP address and port for the primary and secondary servers.</p> <p>If you use port 636, install a root certificate from a CA on XenMobile, and change the Use secure connections option to Yes.</p>		XenMobile NetScaler Gateway	
<p>Note the Active Directory domain name.</p>		XenMobile NetScaler Gateway	
<p>Note the Active Directory service account, which requires a user ID, password, and domain alias.</p> <p>The Active Directory service account is the account that XenMobile uses to query Active Directory.</p>		XenMobile NetScaler Gateway	
<p>Note the User Base DN.</p> <p>This is the directory level under which users are located; for example, cn=users,dc=ace,dc=com. NetScaler Gateway and XenMobile use this to query Active Directory.</p>		XenMobile NetScaler Gateway	
<p>Note the Group Base DN.</p> <p>This is the directory level under which groups are located.</p> <p>NetScaler Gateway and XenMobile use this to query Active Directory.</p>		XenMobile NetScaler Gateway	

Connections Between XenMobile and NetScaler Gateway

✔	Prerequisite	Component	Note the setting
	<p>Note the XenMobile host name.</p>	XenMobile	
	<p>Note the FQDN or IP address of XenMobile.</p>	XenMobile	
	<p>Identify the apps users can access.</p>	NetScaler Gateway	

	Note the Callback URL. Prerequisite	XenMobile Component	Note the setting
---	--	--------------------------------------	-------------------------

User Connections: Access to XenDesktop, XenApp, and Worx Home

Citrix recommends that you use the Quick Configuration wizard in NetScaler to configure connection settings between XenMobile and NetScaler Gateway and between XenMobile and Worx Home. You create a second virtual server to enable user connections from Receiver and web browsers to connect to Windows-based applications and virtual desktops in XenApp and XenDesktop. Citrix recommends that you use the Quick Configuration wizard in NetScaler to configure these settings as well.

• Prerequisite	Component	Note the setting
Note the NetScaler Gateway host name and external URL. The external URL is the web address with which users connect.	XenMobile	
Note the NetScaler Gateway callback URL.	XenMobile	
Note the IP addresses and subnets masks for the virtual server.	NetScaler Gateway	
Note the path for Program Neighborhood Agent or a XenApp Services site.	NetScaler Gateway XenMobile	
Note the FQDN or IP address of the XenApp or XenDesktop server running the Secure Ticket Authority (STA) (for ICA connections only).	NetScaler Gateway	
Note the public FQDN for XenMobile.	NetScaler Gateway	
Note the public FQDN for Worx Home.	NetScaler Gateway	

Known Issues

Nov 20, 2015

The following are known issues for XenMobile 10.0.

For a list of fixed issues in this release, see <http://support.citrix.com/article/CTX141722>.

- Worx Home may show gray placeholders instead of icons when an iOS device is updated from iOS 7 to iOS 8 and then restarted. This is a third-party issue. [#502879]
- During enrollment, iOS devices may experience errors during or after mobile device management (MDM) profile installation. Users may see "Cocoa error 4097," on devices running iOS 8.1, or "Profile cannot be decrypted," on devices running earlier versions of iOS. If this occurs, users should try enrolling again. In some cases, it may take more than one attempt. [#507948]
- You cannot make checkUserPassword and addGroup SOAP calls in the USER group class in XenMobile 10. The User API changes appear in the database, but not on device user interfaces. [#511551, #511822]
- The ability to change the deployment order of delivery group resources from the XenMobile web console is not available. If you want to control the deployment order, rename your resources to follow the deployment protocol used by XenMobile: numerical (1, 2, 3, ...), uppercase alphabetical (A, B, C, ...), and lowercase alphabetical (a, b, c, ...). A resource with a name beginning with 24 would be deployed before a resource with a name beginning with WM, and both resources would deploy before a resource with a name beginning with tw. [#512566]
- SafeSearch is disabled and set to moderate on Windows Phone 8.1 devices when the Filter Adult Content restriction is enabled. [#513605]
- When you deploy Windows 8.1 tablet device policies, before XenMobile receives an acknowledgment from the device that the policy has executed, you may see the policies listed in the Deployed tab in Device details in the XenMobile console. [#514749]
- When re-enrolling a device, enrollment may fail if users re-enroll too soon after un-enrolling. [#516567]
- Occasionally, when users re-enroll in Worx Home, XenMobile presents a cached SSL session and users see the enrollment screen again. When this occurs, users should re-enroll again. [#517301]
- App enumeration fails when delivery groups are defined with Active Directory groups belonging to parent and child domains using the AND operator. To prevent this situation, use the OR operator when defining the delivery groups. [#518084]
- If you configure a setting or policy in the XenMobile console in which you upload a file (certificate, PDF, font, and so on), if you later view the policy or setting details, the file name does not appear. [#519552]
- XenMobile does not support authentication with a PIN in mobile app management (MAM) mode for iOS and Android devices. If you configure this mode as the default in the XenMobile console, users must enter their credentials twice in Worx Home. [#519572]
- If you disable the AllUsers group as a delivery group in the XenMobile console, users who not belong to any delivery group cannot enroll a device but can log on to the Self Help Portal. [#521393]
- Worx Home for Windows Phone 8.x, in mobile device management mode, only supports apps from public stores when they are deployed as optional. If these apps are added to the delivery group as required, they do not appear in Worx Home. [#521524]
- The Role-Based Access Control (RBAC) Role Info page appears to allow you to edit the default Admin template. Despite changes you make in the RBAC template field and elsewhere, these changes are not saved to the Admin template. The Admin template is designed to not be edited. [#521540]
- On iOS devices, the provisioning of the SAML token when users enroll in Worx Home and configure their ShareFile accounts may be out of sync. As a workaround, users can sign off and back on to Worx Home and then log on to the

ShareFile app in order to trigger the SAML token request again. [#521934]

- On most devices, when users running Android devices tap the Menu icon, the Accept and Decline menu options appear, allowing users to continue the enrollment process. On some devices running operating systems earlier than 4.0, however, such as the Samsung Tablet GT-P7510, the Menu icon does not appear on the Terms and Conditions page in default view, and users cannot complete the enrollment process. As a workaround, you can exempt the devices from the Terms and Conditions deployment. [#524039]
- Worx Home on iOS devices cannot connect to Worx Store if the default store name on the Beacons page of the XenMobile console (Configure > Settings > More > Beacons) is changed. The default setting is Store. If this setting is changed, the Discovery Service fails during logon and Worx Store cannot be found. To avoid this failure, leave the Store name setting on the Beacons page set to Store. [#523306]
- In a XenMobile configuration with load balancing and SSL offload, when you configure SAML apps, in order for single sign-on (SSO) to work when users install WorxWeb and open a Service Provider-initiated app, all references to the XenMobile server must point to port 8443 instead of to port 443. [#528680]
- When you create a Samsung KNOX passcode policy, when you configure the Lock device after (minutes of activity) setting even though the setting in the console lists minutes as the unit, the server enforces the lock in seconds. [#531204]
- You cannot configure your own SAML service and identity provider in XenMobile 10 in order to authenticate users and their devices. [#530892]
- You cannot add a single BlackBerry or Windows device in the XenMobile console. [#532844]
- If you configure a SAML app with the number sign (#) in the name, single sign-on (SSO) from Worx Home does not work and an error message appears. [#533078]
- When you add a generic PKI (GPKI) entity in the XenMobile console, you cannot test the Web Services Description Language (WSDL) URL adapter connection during the configuration. [#533871]
- Windows tablet password policies do not take effect immediately on devices and some inconsistencies in enforcement of updates to the minimum password lengths occur. This is a third-party issue. [#534088]
- When users enroll an iOS device in mobile device management (MDM) mode, the Security options in the XenMobile console on the Manage > Devices page for locating and tracking the device do not immediately appear. After a short delay, the options appear. [#534672]
- If you configure StoreFront Delivery Controller display name with a special character in the name, such as a period (.), users cannot subscribe to and open apps with XenApp through Worx Home. The error, "Cannot complete your request" appears. As a workaround, remove special characters from the name. [#535497]
- Apps do not appear in the Worx Store for iOS devices earlier than iOS 8 if you type a value in the Excluded devices field in the XenMobile console when you add and configure the app. As a workaround, you can configure a deployment rule to specify the devices that can install the app. [#537631]
- When you configure NetScaler Gateway connections with XenMobile on a port other than the default 443, mobile app management (MAM) enrollment fails on iOS devices as well as Worx Home on Windows devices. [#537368]
- Special characters like \$, @ and " are not recognized in passwords for the CLI when installing XenMobile 10 and those assigned to certificates; the special character and all characters following it are ignored and the log on fails. Subsequent to installation, the CLI password cannot be changed to include special characters. [#541997] [#542436]
- 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. [#608213]

The following are known issues for XenMobile Mail Manager 10.0.

- 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.

Installing XenMobile

Aug 25, 2016

The XenMobile virtual machine (VM) runs on Citrix XenServer, VMware ESXi, or Microsoft Hyper-V. You can use XenCenter or vSphere management consoles to install XenMobile.

Before you start: 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](#). Also, refer to the [System Requirements for XenMobile 10](#) and the [XenMobile 10 Pre-Installation Checklist](#).

Note: Ensure the hypervisor is configured with the correct time because XenMobile uses that time.

XenServer or VMware ESXi prerequisites: Before installing XenMobile on XenServer or VMware ESXi, you must do the following. For details, refer to your [XenServer](#) or [VMware](#) documentation.

- Install XenServer or VMware ESXi on a computer with adequate hardware resources.
- Install XenCenter or vSphere on a separate computer. The computer that hosts XenCenter or vSphere connects to XenServer or VMware ESXi host through the network.

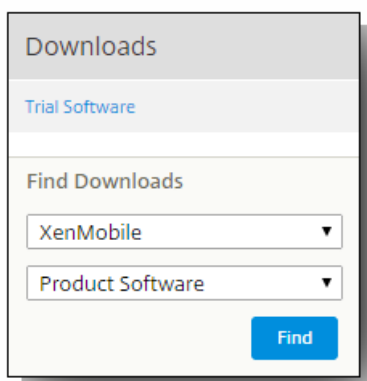
Hyper-V prerequisites: Before installing XenMobile on Hyper-V, you must do the following. For details refer to your [Hyper-V](#) documentation.

- Install Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 with Hyper-V enabled, role enabled, on a computer with adequate system resources. While installing the Hyper-V role, be sure to specify the network interface cards (NICs) on the server that Hyper-V will use to create the virtual networks. You can reserve some NICs for the host.

FIPS 140-2 mode: If you plan to install XenMobile server in FIPS mode, you need to complete a set of prerequisites, as discussed in [Configuring FIPs with XenMobile](#).

Downloading XenMobile Product Software

You can download product software from the [Citrix web site](#). You need to log on to the site and then click the Downloads link on the Citrix web page. You can then select the product and type you want to download. For example, the following figure shows XenMobile and Product Software selected from the lists:



When you click Find, a page listing the available downloads appears with the most recent version at the top of the list. You

can select your software from the available list of options.

To download the software for XenMobile

1. Go to the [Citrix web site](#).
2. Click My Account and log on.
3. Click Downloads.
4. Under Find Downloads, from the product list, click XenMobile.
5. Under Find Downloads, from the download type list, click Product Software and then click Find.
6. On the XenMobile Product Software page, click the XenMobile 10.0 edition you want to download.
7. On the XenMobile 10.0 Edition page, click Download for the appropriate virtual image in order to install XenMobile on XenServer, VMware, or Hyper-V.
8. Follow the instructions on your screen to download the software.

To download the software for NetScaler Gateway

You can use this procedure to download the NetScaler Gateway virtual appliance or software upgrades to your existing NetScaler Gateway appliance.

1. Go to the [Citrix web site](#).
2. Click My Account and log on.
3. Click Downloads.
4. Under Find Downloads, from the product list, click NetScaler Gateway.
5. Under Find Downloads, from the download type list, click Product Software and then click Find.
Note: You can also click Virtual Appliances to download NetScaler VPX. When you select this option, you receive a list of software for the virtual machine for each hypervisor.
6. On the NetScaler Gateway page, expand 10.5(4).
7. Click the appliance software version you want to download.
8. On the appliance software page for the version you want to download, click Download for the appropriate virtual appliance.
9. Follow the instructions on your screen to download the software.

Configuring XenMobile for the First-Time Use

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

1. Configure the IP address and subnet mask, default gateway, and DNS servers for XenMobile by using the XenCenter or vSphere command-line console.
2. Log on to the XenMobile management console and follow the steps in the initial logon screens.

Note

When you use a vSphere web client, it is recommended that you do not configure networking properties during the time you deploy the OVF template on the **Customize template** page. By doing so, in a high availability configuration, you avoid an issue with the IP address that occurs when you clone and then restart the second XenMobile virtual machine.

Configuring XenMobile in the Command Prompt Window

1. Import the XenMobile virtual machine into Citrix XenServer, Microsoft Hyper-V, or VMware ESXi. For details, see [XenServer](#), [Hyper-V](#), or [VMware](#) documentation.
2. In your hypervisor, select the imported XenMobile virtual machine and start the command prompt view. For details, see the documentation for your hypervisor.
3. From the hypervisor's console page, create an administrator account for XenMobile in the Command Prompt window.

```
Welcome to the XenMobile First Time Use wizard. This wizard guides you through the initial configuration of XenMobile. Accept options offered by pressing Enter/Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the command prompt.
Username: admin
New password: █
```

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

4. Provide the following:
 1. IP address
 2. Netmask
 3. Default gateway
 4. Primary DNS server
 5. Secondary DNS server (optional)

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

Commit settings [y/n]: y█
```

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

5. Type y to increase security by generating a random passphrase or n provide your own passphrase. Citrix recommends typing y to generate a random passphrase. The passphrase is used as part of the protection of the encryption keys used to secure your sensitive data. A hash of the passphrase, stored in the server file system, is used to retrieve the keys during the encryption and decryption of data. The passphrase cannot be viewed.

Note: If you intend to extend your environment and configure additional servers, you should provide your own passphrase. There is no way to view the passphrase if you selected a random passphrase.

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

6. Optionally, enable Federal Information Processing Standard (FIPS). For details about FIPS, see [XenMobile FIPS 140-2 Compliance](#). Also, be sure to complete a set of prerequisites, as discussed in [Configuring FIPs with XenMobile](#).

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

7. Configure the database connection. Your database can be local or remote. When asked Local or remote, type r or l. Important:
- Citrix recommends using Microsoft SQL remotely. PostgreSQL is included with XenMobile and should be used locally or remotely only in test environments.
 - Database migration is not supported. Databases created in a test environment cannot be moved to a production environment.

```
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:
```

Important: The default port for PostgreSQL is 5432.

```
Database connection:  
Local or remote [l/r]: l
```

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

8. Provide the fully qualified domain name (FQDN) for the server hosting XenMobile. This one host server provides both device management and app management services.

Important: You will not be able to change the FQDN without completely reinstalling the server.

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

9. Identify the communication ports. For details on ports and their uses, see [XenMobile Port Requirements](#).

Note: Accept the default ports by pressing Enter (Return on a Mac).

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


10. You are asked to provide passwords for all the Public Key Infrastructure (PKI) server certificates and given the option to use the same password for each certificate. For details on the XenMobile PKI feature, see [Uploading Certificates in XenMobile](#).

Important: If you intend to cluster nodes, or instances, of XenMobile together, you will need to provide the identical passwords for subsequent nodes.

```
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:
```

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

11. Create an administrator account for logging on to the XenMobile console with a web browser. Be sure to remember these credentials for later use.

```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile console through a web browser.
Username [administrator]: administrator
Password:
Re-enter new password:
```

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

12. When asked if this is an upgrade, type n because it is a new installation.

```
Upgrade:
Upgrade from previous release (y/n) [n]:
```

13. Copy the complete URL that appears on the screen and continue this initial XenMobile configuration in your web

```
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!

Upgrade:
Upgrade from previous release (y/n) [n]:

Stopping configuration app... [ OK ]
Starting configuration app...
application started successfully [ OK ]
Stopping main app... [ OK ]
Starting main app...
this may take a few minutes.....
.....
application started successfully [ OK ]

To access the console, from a web browser, go to the following location and
log on with your console credentials:
https://203.0.113.8:4443/

Starting monitoring... [ OK ]
```

Configuring XenMobile in a Web Browser

After completing the initial portion of the XenMobile configuration in your hypervisor Command Prompt window, complete the process in your web browser.

1. In your web browser, navigate to the location provided at the conclusion of the Command Prompt window configuration.
2. Type the XenMobile console administrator account user name and password you created in the Command Prompt window.



3. On the Get Started page, click Start. The Licensing page appears.
4. Configure the license. XenMobile comes with an evaluation license valid for 30 days. For details on adding and configuring licenses and configuring expiration notifications, see [Licensing for XenMobile](#).
Important: If you intend to cluster nodes, or instances, of XenMobile, you need to use the Citrix Licensing on a remote server.

5. On the Certificate page, click Import. The Import dialog box appears.
6. Import your APNs and SSL Listener certificate. For details on working with certificates, see [Certificates in XenMobile](#).
Note: The SSL Listener certificate requires restarting the server.
7. If appropriate to the environment, configure NetScaler Gateway. For details on configuring NetScaler Gateway, see [NetScaler Gateway and XenMobile](#) and [Configuring Settings for Your XenMobile Environment](#).
Note: You can deploy NetScaler Gateway at the perimeter of your organization's internal network (or intranet) to provide a secure single point of access to the servers, applications, and other network resources that reside in the internal network. In this deployment, all remote users must connect to NetScaler Gateway before they can access any resources in the internal network.
Note: Although NetScaler Gateway is an optional setting, after you enter data on the page, you must clear or complete the required fields before you can leave the page.
8. Complete the LDAP configuration to access users and groups from Active Directory. For details on configuring the LDAP connection, see [LDAP Configuration](#).
9. Configure the notification server to be able to send messages to users. For details on notification server configuration, see [Notifications in XenMobile](#).

Configuring FIPS with XenMobile

Nov 06, 2015

Federal Information Processing Standards (FIPS) mode in XenMobile supports U.S. federal government customers by configuring the server to use only FIPS 140-2 certified libraries for all encryption operations. Installing your XenMobile server with FIPS mode ensures that all data at rest and data in transit for both the XenMobile client and server are fully compliant with FIPS 140-2.

Before installing a XenMobile Server in FIPS mode, you need to complete the following prerequisites.

- You must use an external SQL Server 2012 or SQL Server 2014 for the XenMobile database. The SQL Server also must be configured for secure SSL communication. For instructions on configuring secure SSL communication to SQL Server, see the [SQL Server Books Online](#).
- Secure SSL communication requires that an SSL certificate be installed on your SQL Server. The SSL certificate can either be a public certificate from a commercial CA or a self-signed certificate from an internal CA. Note that SQL Server 2014 cannot accept a wildcard certificate. Citrix recommends, therefore, that you request an SSL certificate with the FQDN of the SQL Server.
- If you use a self-signed certificate for SQL Server, you will need a copy of the root CA certificate that issued your self-signed certificate. The root CA certificate must be imported to the XenMobile server during installation.

Configuring FIPS mode

You can enable FIPS mode only during the initial setup of XenMobile server. It is not possible to enable FIPS after installation is complete. Therefore, if you plan on using FIPS mode, you must install the XenMobile server with FIPS mode from the start. In addition, if you have a XenMobile cluster, all cluster nodes must have FIPS enabled; you cannot have a mix of FIPS and non-FIPS XenMobile servers in the same cluster.

There is a **Toggle FIPS mode** option in the XenMobile command-line interface that is not for production use. This option is intended for non-production, diagnostic use and is not supported on a production XenMobile server.

1. During initial setup, enable **FIPS mode**.
2. Upload the root CA certificate for your SQL Server. If you used a self-signed SSL certificate rather than a public certificate on your SQL Server, choose **Yes** for this option and then do one of the following:
 - a. Copy and paste the CA certificate.
 - b. Import the CA certificate. To import the CA certificate, you must post the certificate to a website that is accessible from the XenMobile server via an HTTP URL. For details, see the [Importing Certificates](#) section later in this article.
3. Specify the server name and port of your SQL Server, the credentials for logging into SQL Server, and the database name to create for XenMobile.

Note: You can use either a SQL logon or an Active Directory account to access SQL Server, but the logon you use must have the DBcreator role.
4. To use an Active Directory account, enter the credentials in the format domain\username.
5. Once these steps are complete, proceed with the XenMobile initial setup.

To confirm that the configuration of FIPS mode is successful, log on to the XenMobile command-line interface. The phrase **In FIPS Compliant Mode** appears in the logon banner.

Importing Certificates

The following procedure describes how to configure FIPS on XenMobile by importing the certificate, which is required when you use a VMware hypervisor.

SQL Prerequisites

1. The connection to the SQL instance from XenMobile needs to be secure and must be SQL Server version 2012 or SQL Server 2014. To secure the connection, see [How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console](#).
2. If the service does not restart properly, check the following:Open **Services.msc**.
 - a. Copy the logon account information used for the SQL Server service.
 - b. Open MMC.exe on the SQL Server.
 - c. Go to **File > Add/Remove Snap-in** and then double-click the certificates item to add the certificates snap-in. Select the computer account and local computer in the two pages on the wizard.
 - d. Click **OK**.
 - e. Expand **Certificates (Local Computer) > Personal > Certificates** and find the imported SSL certificate.
 - f. Right-click the imported certificate (selected in the SQL Server Configuration Manager) and then click **All Tasks > Manage Private Keys**.
 - g. Under **Group or User names**, click **Add**.
 - h. Enter the SQL service account name you copied in the earlier step.
 - i. Clear the **Allow Full Control** option. By default the service account will be given both Full control and Read permissions, but it only needs to be able to read the private key.
 - j. Close **MMC** and start the SQL service.
3. Ensure the SQL service is started correctly.

Internet Information Services (IIS) Prerequisites

1. Download the rootcert (base 64).
2. Copy the rootcert to the default site on the IIS server, C:\inetpub\wwwroot.
3. Check the **Authentication** check box for the default site.
4. Set **Anonymous** to **enabled**.
5. Select the **Failed Request Tracking** rules check box.
6. Ensure that .cer is not blocked.

7. Browse to the location of the .cer in an Internet Explorer browser from the local server, <http://localhost/certname.cer>. The root cert text should appear in the browser.

8. If the root cert does not appear in the Internet Explorer browser, make sure that ASP is enabled on the IIS server as follows.

- a. Open Server Manager.
- b. Navigate to the wizard in **Manage > Add Roles and Features**.
- c. In the server roles, expand **Web Server (IIS)**, expand **Web Server**, expand **Application Development** and then select **ASP**.
- d. Click **Next** until the install completes.

9. Open Internet Explorer and browse to <http://localhost/cert.cer>.

For more information, see [Internet Information Services \(IIS\) 8.5](#).

Note

You can use the use the IIS instance of the CA for this procedure.

Importing the Root Certificate During Initial FIPS Configuration

When you complete the steps to configure XenMobile for the first time in the command-line console, you must complete these settings to import the root certificate. For details on the installation steps, see [Installing XenMobile](#).

- Enable FIPS: Yes
- Upload Root Certificate: Yes
- Copy(c) or Import(i): i
- Enter HTTP URL to import: <http://FQDN of IIS server/cert.cer>
- Server: *FQDN of SQL Server*
- Port: 1433
- User name: Service account which has the ability to create the database (domain\username).
- Password: The password for the service account.
- Database Name: This is a name you choose.

XenMobile 10 MDM Upgrade Tool

Jan 24, 2017

Important

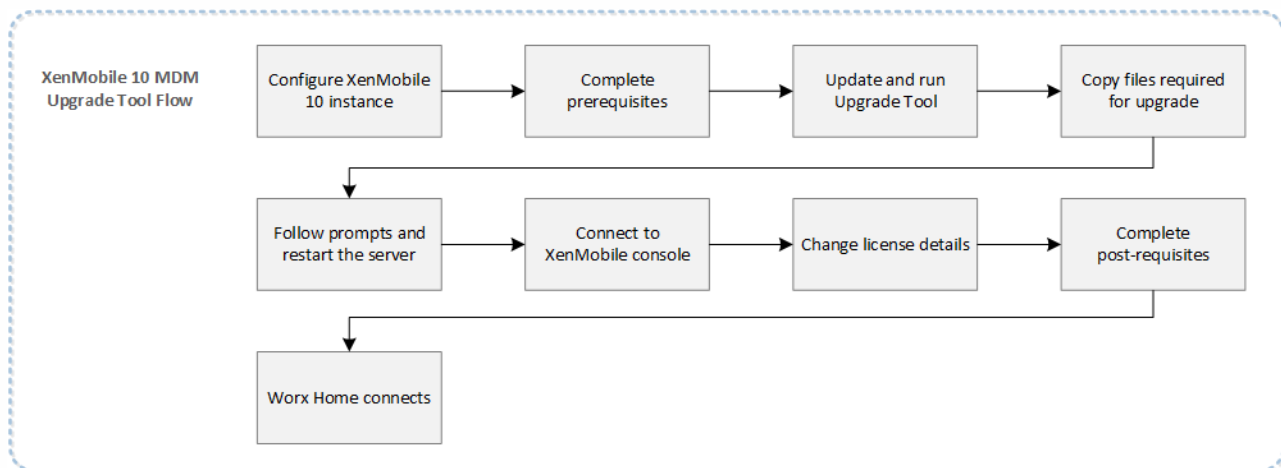
To upgrade from XenMobile 9 to the latest version, you use the Upgrade Tool built into XenMobile 10.4 or later. If you are in the process of an upgrade with an older version of the Upgrade Tool and have questions, please contact Citrix Customer Support. The older Upgrade Tool, documented in this article, is no longer available from Citrix.com.

The XenMobile 10 MDM Upgrade Tool is designed for upgrades from XenMobile 9.0 to XenMobile 10. The tool is supported for upgrades from XenMobile MDM edition deployments.

Important: Using the tool to upgrade from XenMobile App Edition or XenMobile Enterprise Edition is not supported. Likewise, you cannot use the tool to upgrade from XenMobile 8.6 or 8.7 to XenMobile 10. In addition, if the Multi-Tenant Console (MTC) is enabled on XenMobile 9.0, the MTC cannot be migrated to XenMobile 10. If your XenMobile 9.0 setup is based on named SQL instances, you need to follow steps specific to this situation. For details see, [Supporting Named SQL Instances](#).

The Upgrade Tool is built within the XenMobile 10 virtual machine. You enable the one-time only wizard through the command-line console during the initial installation of XenMobile 10.

The following diagram illustrates the basic steps you take to upgrade from XenMobile 9.0 to XenMobile 10.



See [Prerequisites](#) and [Known Issues](#) before starting the migration to XenMobile 10.

What the Upgrade Tool does

The XenMobile 10 MDM Upgrade Tool migrates configuration and user data from the XenMobile 9.0 server to a new instance of XenMobile 10 with the same fully qualified domain name (FQDN).

You can choose to test drive the upgrade or to do a full production upgrade. When you choose Test Drive in the tool, only

configuration data is migrated to XenMobile 10; no device or user data is migrated. This option lets you compare XenMobile 9.0 and XenMobile 10 without affecting your production environment.

When you choose Production Upgrade in the tool, all configuration, device, and user data is migrated. When you log on to the XenMobile 10 console after the upgrade, you see all the user and device data that was migrated from XenMobile 9.

Note: This is not an in-place migration; all data is *copied* during migration, not moved, to XenMobile 10. Everything in XenMobile 9.0 remains intact until you move the XenMobile 10 server into production. When users connect to XenMobile 10 in production, if for some reason you want to revert to XenMobile 9.0, those users must re-enroll in XenMobile 9.0.

After a successful production upgrade, to move XenMobile 10 to live production, you must do the following:

1. Update the DNS entry to map the XenMobile 9.0 FQDN to the new XenMobile 10 server IP.
2. If NetScaler is load balancing XenMobile Device Manager servers, you need to switch the XenMobile 9.0 service to the XenMobile 10 service.

What the Upgrade Tool Does Not Do

The following information is **not** migrated to XenMobile 10 when you use the Upgrade Tool:

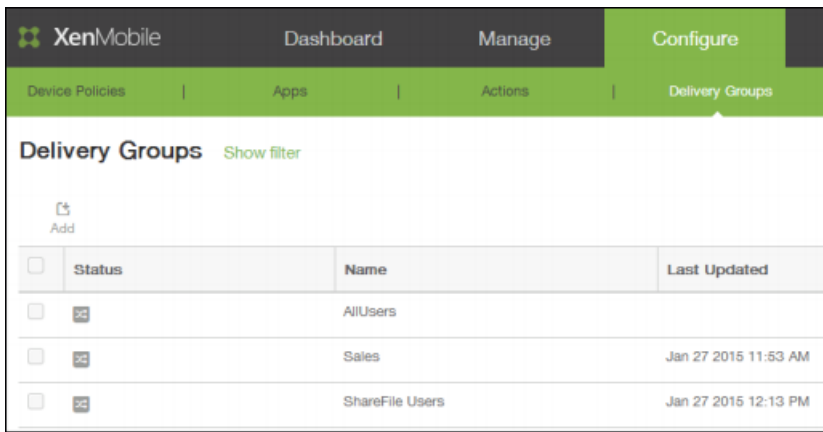
- Licensing information.
- Reports data.
- Automated actions.
- Server group policies and associated deployments.
- MSP group.
- Policies and packages related to Windows CE and Windows 8.0.
- Deployment packages not in use; for example, when no users or groups are assigned to a deployment package.
- Any other configuration or user data as described in the migration.log file.
- CXM Web (replaced by Citrix WorxWeb).
- DLP policies (replaced by Citrix Sharefile).
- Custom Active Directory attributes.
- If you have configured multiple branding policies, the branding policy is not migrated. XenMobile 10 supports one branding policy; you have to leave one branding policy in XenMobile 9.0 to successfully migrate to XenMobile 10.
- Any settings in the auth.jsp file in XenMobile 9.0 that are used to restrict access to the console. Console access restrictions in XenMobile 10 are firewall settings that you can configure in the command line interface.

Also note the following changes with XenMobile 10:

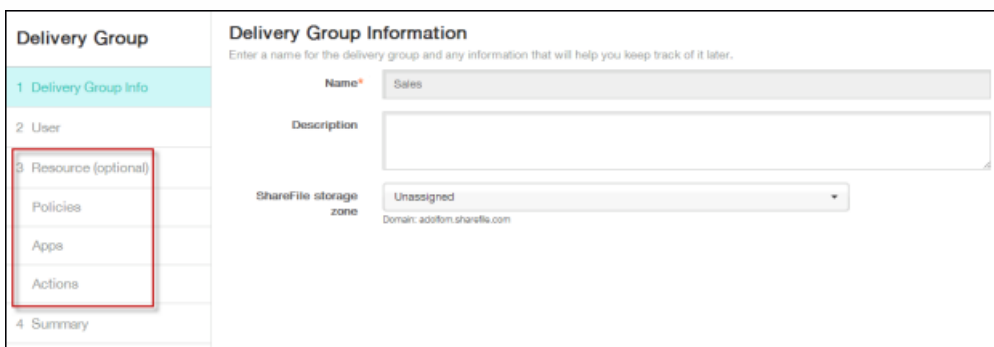
- The Upgrade Tool doesn't upgrade Active Directory users who are assigned to local groups. You can subsequently assign Active Directory users to local groups.
- XenMobile 10 doesn't support nested local groups. An upgrade from XenMobile 9 flattens the local groups hierarchy.

Terminology Change with XenMobile 10

Note that after you upgrade, deployment packages in Device Manager are now referred to as delivery groups, as shown in the following figure. For more information, see [Managing Delivery Groups](#).



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



Device Enrollment After Upgrade

Users do not need to re-enroll their devices after you upgrade to XenMobile 10. The devices should connect automatically to the XenMobile 10 server based on the heartbeat interval.

If you want to connect a device to XenMobile 10 immediately, on the device, use WorxHome > Device Info > Refresh Policy.

After the user devices connect, check to make sure you see the devices in the XenMobile console, as shown in the following figure.

XenMobile						
Dashboard		Manage		Configure		
Devices			Enrollment			
Devices Show filter						
<input type="button" value="Add"/> <input type="button" value="Import"/> <input type="button" value="Refresh"/>						
<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model
<input type="checkbox"/>		MDM	user1@training.lab	iOS	8.1.3	iPad
<input type="checkbox"/>		MDM	user2@training.lab	Android	4.1.2	GT-N8013
<input type="checkbox"/>		MDM	user3@training.lab	Windows Phone 8.x	8.10.14226.359	909

Supporting Named SQL Instances

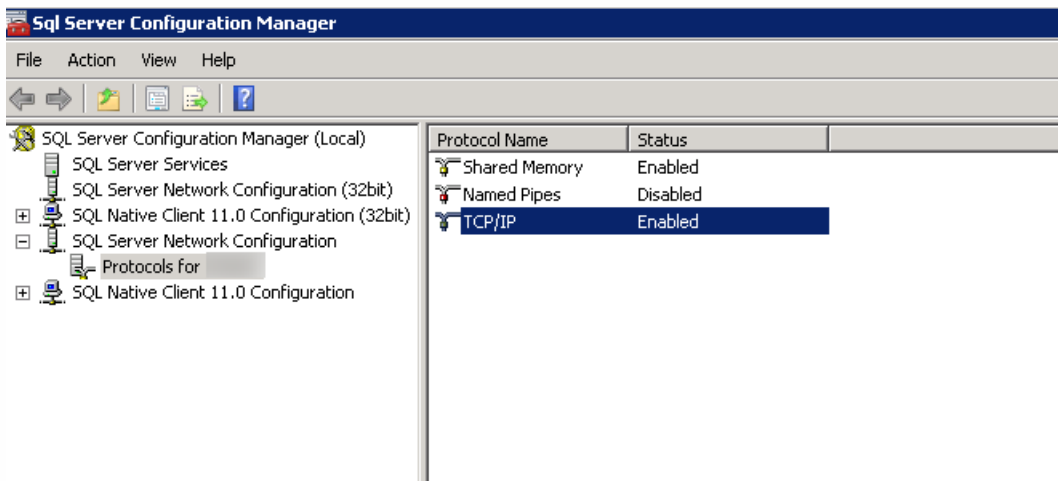
Oct 03, 2016

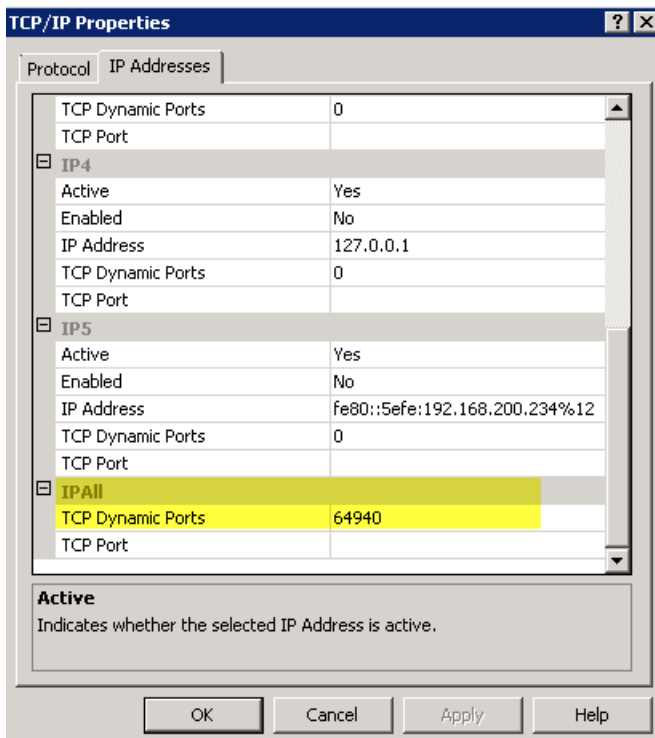
You can use the Upgrade Tool to upgrade from XenMobile 9 to XenMobile 10 and from XenMobile 9 to XenMobile 10.1. If your XenMobile 9 setup is based on named SQL instances, you need to follow steps specific to this situation. If your XenMobile 9 environment meets the following prerequisites, follow the steps in this article to upgrade.

- XenMobile 9 MDM Edition or Enterprise Edition set up with an external SQL Server database.
- SQL Server database running on a non-default named instance.
- SQL Server named instance listening on a static or dynamic TCP port. You can confirm this prerequisite by looking at the IP addresses of the TCP/IP protocol of the named instance as shown in the following figures.

Note

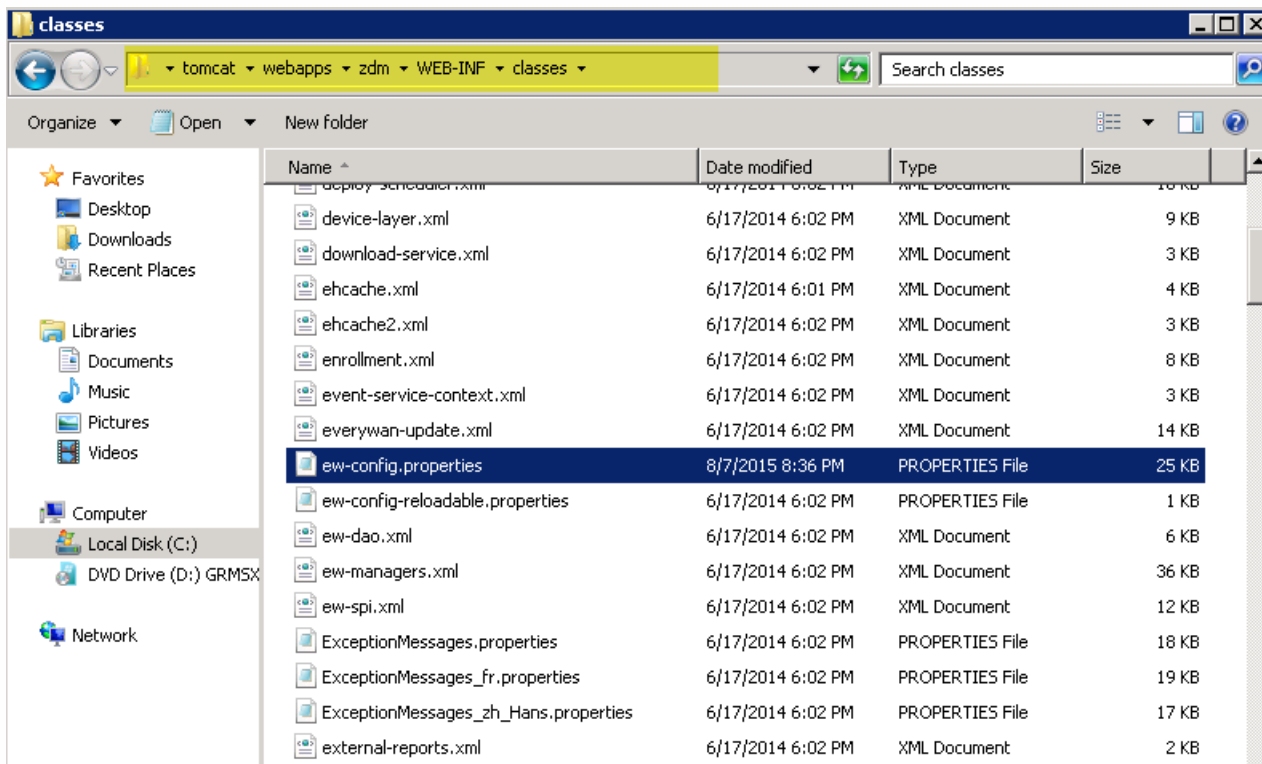
Citrix recommends that the SQL server database instance always runs on a static port, because the XenMobile server needs continuing access to the database. This connection generally traverses through a firewall. As a result, you need to open the appropriate port in the firewall; therefore, you need to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





Steps to upgrade XenMobile with a SQL Server named instance

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



2. In the ew-config.properties file, search for the following URLs in the DATASOURCE Configuration section:

pooled.datasource.url=jdbc:jt ds:sqlserver://<SQLserver_FQDN>/<DB_Name>;instance=<Instance_Name>

audit.datasource.url=jdbc:jt ds:sqlserver://<SQLserver_FQDN>/<DB_Name>;instance=<Instance_Name>

```
ew-config.properties
18 # For Microsoft SQL server url1: pooled.datasource.url=jdbc:jt ds:sqlserver://localhost:1433/everwyan
19 # For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jt ds:sqlserver://localhost/everwyan;instance=SQLExpress
20 # For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jt ds:sqlserver://localhost/everwyan;instance=SQLExpress;domain=sparus-
21 # Oracle url: pooled.datasource.url=jdbc:oracle:thin:everwyan/everwyan0//localhost:1521/everwyan
22 pooled.datasource.url=jdbc:jt ds:sqlserver://ah-234 .net/ -11aug;instance=
23 # Pooled datasource host name
24 pooled.datasource.hostname=ah-234. .net
25 # Pooled datasource database
26 pooled.datasource.database= aug
27 # Pooled datasource user
28 pooled.datasource.user=sa
29 # Pooled datasource password
30 # For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everwyan01
31 pooled.datasource.password={aes} ==
32
33 # No pooled datasource driver
34 #no.pooled.datasource.driver=org.postgresql.Driver
35 # No pooled datasource url
36 #no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everwyan
37 # No pooled datasource user
38 #no.pooled.datasource.user=everwyan
39 # No pooled datasource password
40 #no.pooled.datasource.password=everwyan
41
42 # Audit datasource driver
43 audit.datasource.driver=net.sourceforge.jt ds.jdbc.Driver
44 # Audit datasource url
45 audit.datasource.url=jdbc:jt ds:sqlserver://ah-234 / -11aug;instance=
46 # Audit datasource host name
47 audit.datasource.hostname=ah-234 .net
48 # Audit datasource database
49 audit.datasource.database= -11aug
50 # Audit datasource user
51 audit.datasource.user=sa
52 # Audit datasource password
```

3. Remove the instance name in the preceding URLs and add the port along with the SQL Server FQDN. In this case, 64940 is the required port.

pooled.datasource.url=jdbc:jt ds:sqlserver:// <SQLserver_FQDN>:64940/<DB_Name>

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

Note

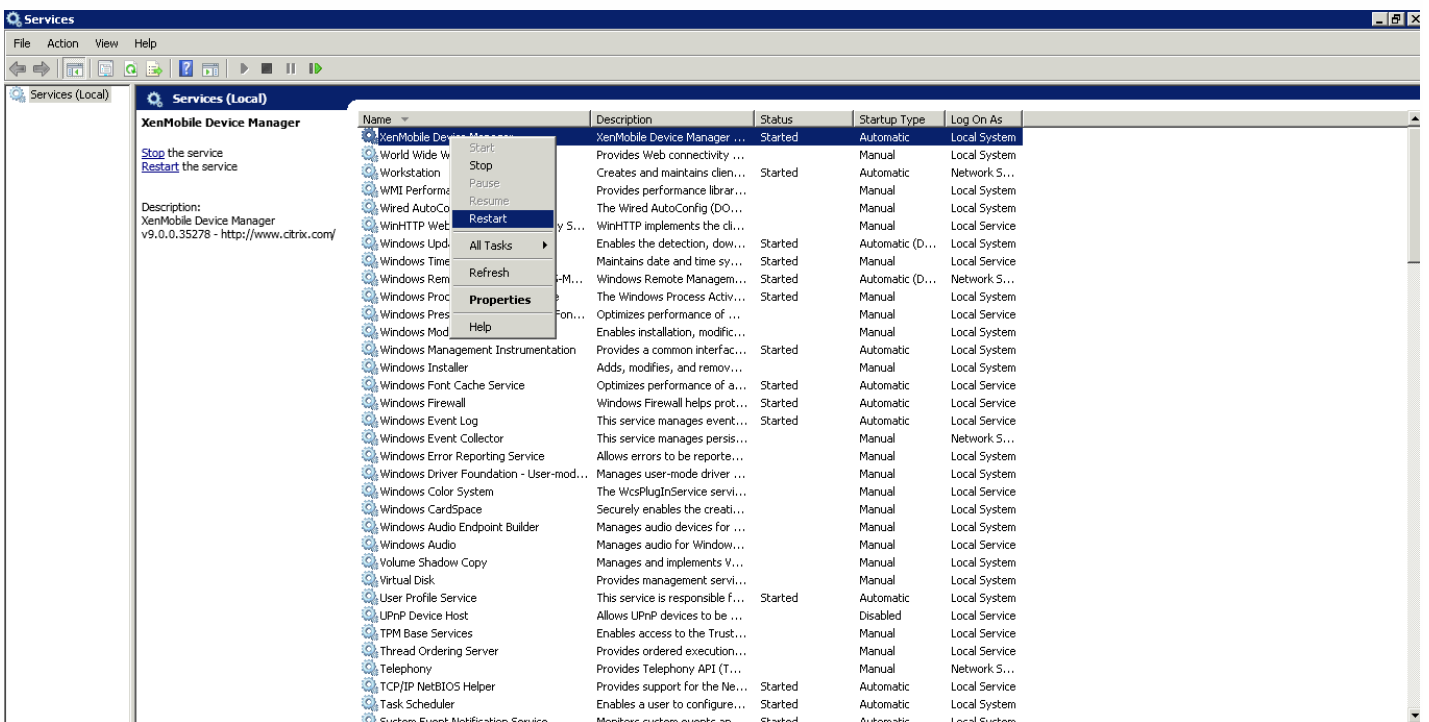
Citrix recommends that you make a backup, copy, or note of the changes you make in the ew-config.properties file. This information is helpful in case the migration fails.

```

18 # For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/verywan
19 # For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/verywan;instance=SQLExpress
20 # For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/verywan;instance=SQLExpress;domain=sparus-s
21 # Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@localhost:1521/verywan
22 pooled.datasource.url=jdbc:jtds:sqlserver://ah-234.net:1433/verywan
23 # Pooled datasource host name
24 pooled.datasource.hostname=ah-234.net
25 # Pooled datasource database
26 pooled.datasource.database=verywan-11aug
27 # Pooled datasource user
28 pooled.datasource.user=sa
29 # Pooled datasource password
30 # For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
31 pooled.datasource.password={aes}
32
33 # No pooled datasource driver
34 #no.pooled.datasource.driver=org.postgresql.Driver
35 # No pooled datasource url
36 #no.pooled.datasource.url=jdbc:postgresql://localhost:5432/verywan
37 # No pooled datasource user
38 #no.pooled.datasource.user=everywan
39 # No pooled datasource password
40 #no.pooled.datasource.password=everywan
41
42 # Audit datasource driver
43 audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
44 # Audit datasource url
45 audit.datasource.url=jdbc:jtds:sqlserver://ah-234.net:1433/verywan
46 # Audit datasource host name
47 audit.datasource.hostname=ah-234.net
48 # Audit datasource database
49 audit.datasource.database=verywan-11aug
50 # Audit datasource user
51 audit.datasource.user=sa
52 # Audit datasource password

```

4. Restart the Device Manager service. Refresh the device connections when the Device Manager instance returns.



5. Determine if the new XenMobile 10 server also needs to work with named SQL instance. If so, identify the port on which the named instance is running. If the port is a dynamic port, Citrix recommends that you convert the port to a static port; then, configure the static port on the new XenMobile server as part of the database setup.

```
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 []: ah-234.██████████.net
Port [1433]: 64940
Username [sa]:
Password:
Database name [DB_service]: DB_██████████ 11aug_Midas

Commit settings (y/n) [y]: █
```

6. Follow the steps in these articles to continue upgrading your XenMobile environment:

- To upgrade from XenMobile 9.0 App Edition or Enterprise Edition to XenMobile 10.1, you use the XenMobile Server App Edition and Enterprise Edition Upgrade Tool. For details, see [Enabling and Running the XenMobile 10.1 Upgrade Tool](#).
- To upgrade from XenMobile 9.0 MDM edition only to XenMobile 10.1, see [XenMobile 10 MDM Upgrade Tool](#).

Upgrading XenMobile in the XenMobile Console

Feb 23, 2015

When new versions of XenMobile software are available, you can upgrade to a new version. You use the Release Management page in the XenMobile console to install new versions of XenMobile software, service packs, and system patches.

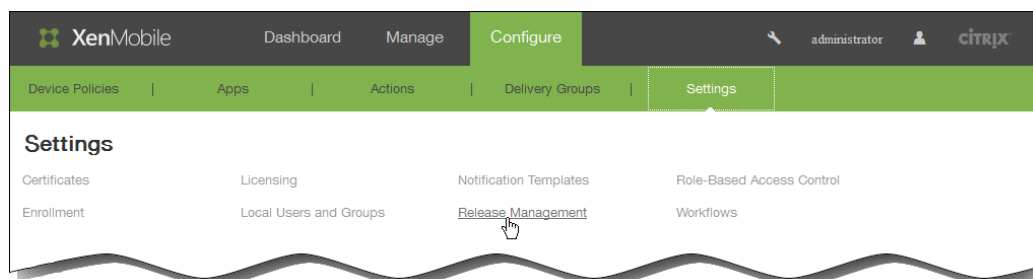
Note: When new versions or important updates are available, they are published to Citrix.com and a notice is sent to the contact on record for each customer.

Important:

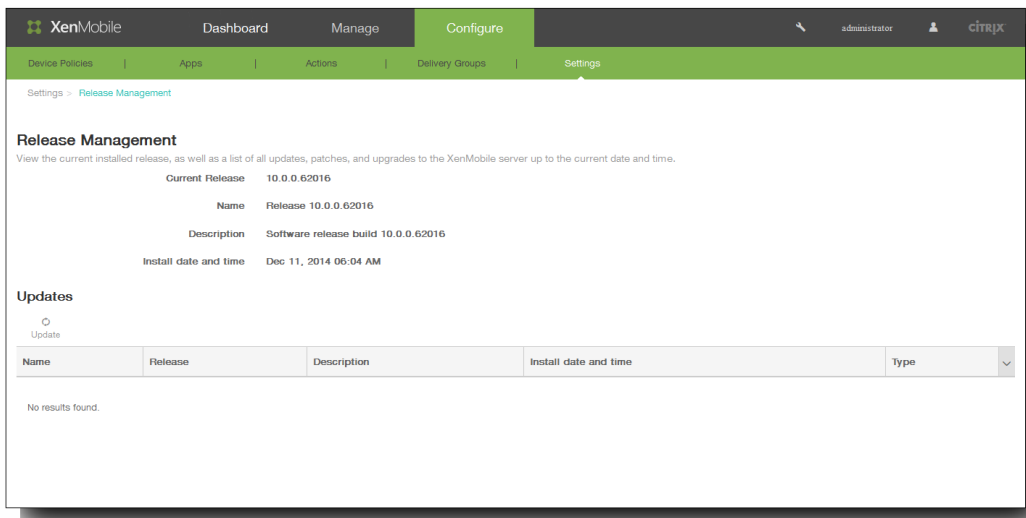
- Before you install a XenMobile update, use the facilities in your virtual machine (VM) to take a snapshot of your system.
- Backup your system configuration database.
- If you have enabled Samsung KNOX attestation on your MDM server and are planning to upgrade to XenMobile 10.0, you need to add the new custom KNOX Attestation domains prior to upgrading. For more information on enabling Samsung KNOX attestation, see [Samsung KNOX](#). The new attestation domains are:
 - China region – china-attest-api.secb2b.com.cn
 - European region – eu-attest-api.secb2b.com
 - US region – us-attest-api.secb2b.com

To upgrade XenMobile

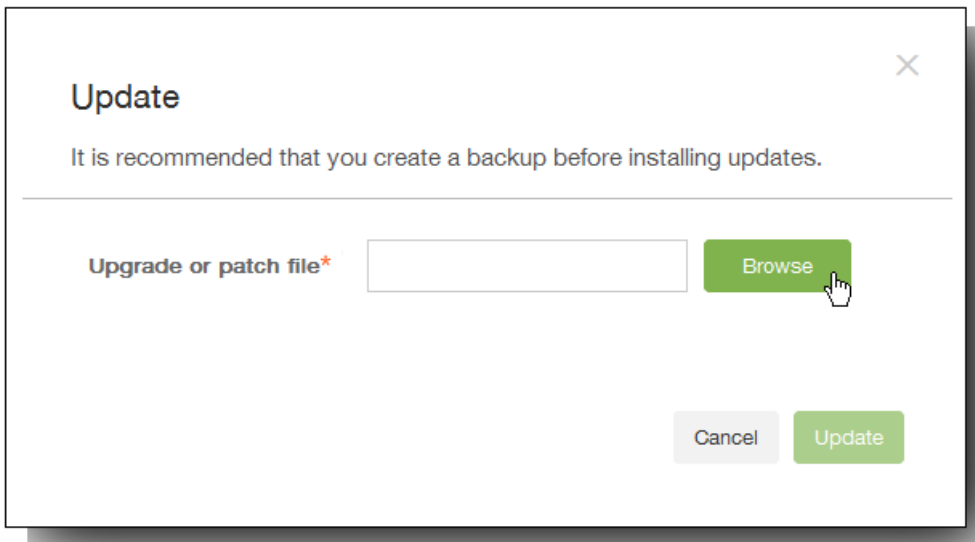
1. Log on to your account on the Citrix website and download the XenMobile Upgrade (.bin) file to an appropriate location.
2. In the XenMobile console, click Configure > Settings > Release Management.



The Release Management page appears, which displays the currently installed software version, as well as a list of any updates, patches, and upgrades you have already uploaded.



3. Under Updates, click Update. The Update dialog box appears.



4. Click Browse, navigate to the location where you saved the XenMobile upgrade file you downloaded from Citrix.com and then select the file.

5. Click Update and then if prompted, restart XenMobile.

Note: XenMobile might not require a restart after the update installs. In this case, a message indicates that the updated

installation is successful. If, however, XenMobile does require a restart, you must use the command line.

Important: If your system is configured in cluster mode, follow these steps to update each node:

- Shut down all but one node.
- Update that node.
- Confirm that the service is running before updating the next node.

If for some reason the update cannot be completed successfully, an error message appears indicating the problem. The system is reverted to its state prior to the update attempt.

Configuring Clustering for XenMobile 10

Jun 02, 2016

XenMobile 10 integrates XenMobile 9 Device Manager and App Controller. In earlier versions of XenMobile, you configure Device Manager as a cluster and App Controller as a high availability pair. High availability is not applicable to XenMobile 10. To configure clustering for XenMobile 10, therefore, you need to configure the following two load balancing virtual IP addresses on NetScaler.

- **Mobile device management (MDM) load balancing virtual IP address:** A MDM load balancing virtual IP address is required to communicate with the XenMobile nodes that are configured in a cluster. This load balancing is done in SSL Bridge mode.
- **Mobile app management (MAM) load balancing virtual IP address:** MAM load balancing virtual IP addresses are required for NetScaler Gateway to communicate with XenMobile nodes that are configured in a cluster. In XenMobile 10, by default, all traffic from NetScaler Gateway routes to the load balancing virtual IP address on port 8443.

The procedures in this article explain the method of creating a new XenMobile virtual machine (VM) and joining the new VM to an existing VM, thereby creating a cluster setup.

Prerequisites

- You have fully configured the required XenMobile node.
- Two free IP addresses to use for the load balancing virtual IP addresses.
- Server certificates.
- One free IP for NetScaler Gateway virtual IP address.

For reference architectural diagrams for XenMobile 10.x in clustered configurations, see [Architecture Overview](#).

Installing the XenMobile Cluster Nodes

Based on the number of nodes you require, you create new XenMobile VMs. You point the new VMs to the same database and provide the same PKI certificate passwords.

1. Open the command-line console of the new VM and enter the new password for the administrator account.



```
*****
*           Citrix XenMobile           *
*   (in First Time Use mode)         *
*****

Welcome to the XenMobile First Time Use wizard. This wizard guides you through t
he initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
Username: admin
New password:
Re-enter new password: _
```

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

```

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

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

```

- If you want to use the default password for data protection, type **y**; or, type **n** and then enter a new password.
Note: If you plan to add additional nodes manually to the cluster and do not plan to clone the initial XenMobile VM, you must enter a new password manually here. The sequential nodes require the same passcode. If you do not use matching passcodes, when you try to join the second node, the process fails. It is possible to clone the VM when that happens, but entering a new password prevents the failure.

```

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

```

- If you want to use FIPS, type **y**; or, type **n**.

```

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

```

- Configure the database so that you point to same database that the earlier fully configured VM pointed to. You will see the message: Database already exists.

```

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

Server []: sql2012.wg.lab
Port [1433]:
Username [sa]:
Password:
Database name [DB_service1]: DB_51

Commit settings (y/n) [y]:

Checking database status...
Database already exists.
To enable realtime communication between cluster members please open port 88 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

```

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

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

Server [l]: 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 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key Infrastructure (PKI) in first node
Do you want to use the same password for all the certificates of the PKI [y]:
```

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

```
Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key Infrastructure (PKI) in first node
Do you want to use the same password for all the certificates of the PKI [y]:
y
New password:
Re-enter new password:
Saving server and client certs password...

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

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

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

```

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

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

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

Starting monitoring... [ OK ]
xms51.wg.lab login:

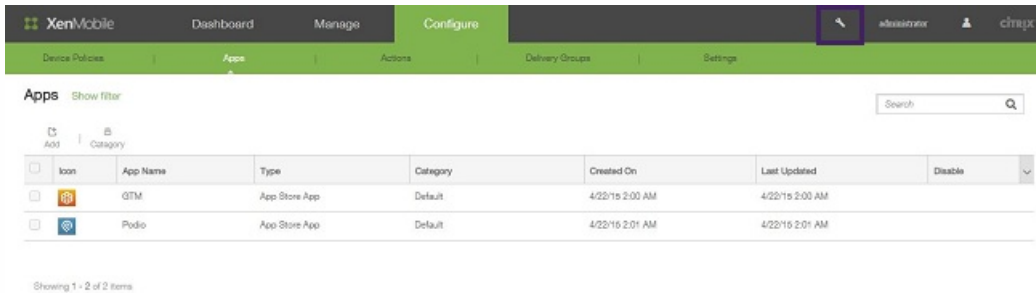
```

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

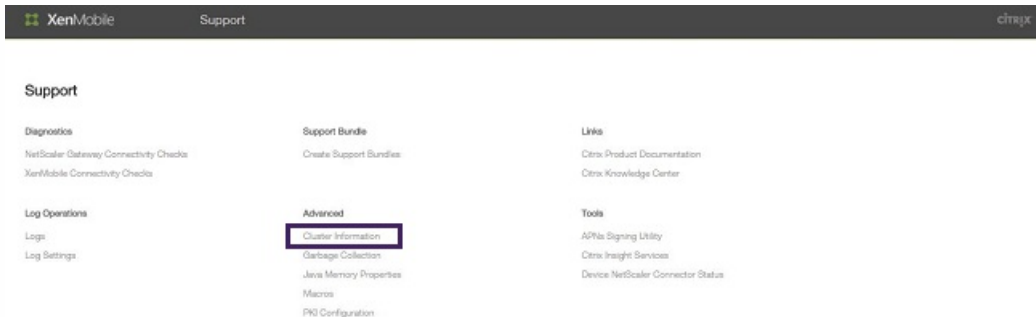
8. Use the fully qualified domain name (FQDN) of XenMobile to open the XenMobile console in a web browser.
9. On the Dashboard, click the tool icon on the upper-right of the screen.



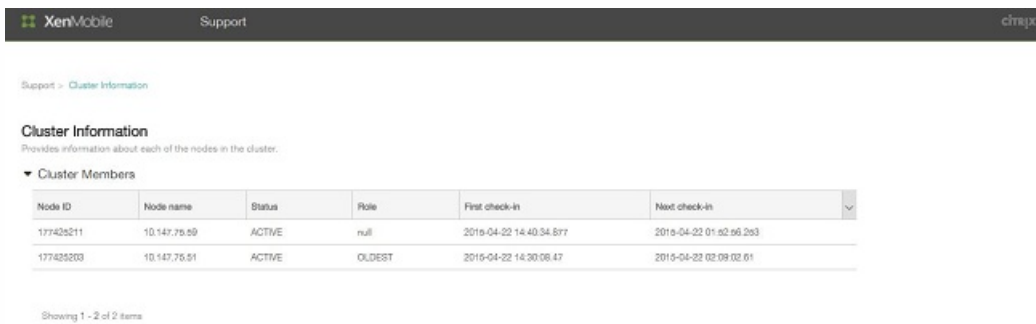
The Support page opens.



10. Under Advanced, click Cluster Information.



All of the information about the cluster, including cluster member, device connection information, tasks, and so on, appear.



Node ID	Node name	Status	Role	First check-in	Next check-in
177425211	10.147.76.59	ACTIVE	null	2015-04-22 14:40:34.877	2015-04-22 01:02:06.293
177425203	10.147.76.51	ACTIVE	OLDEST	2015-04-22 14:30:08.47	2015-04-22 02:08:02.61

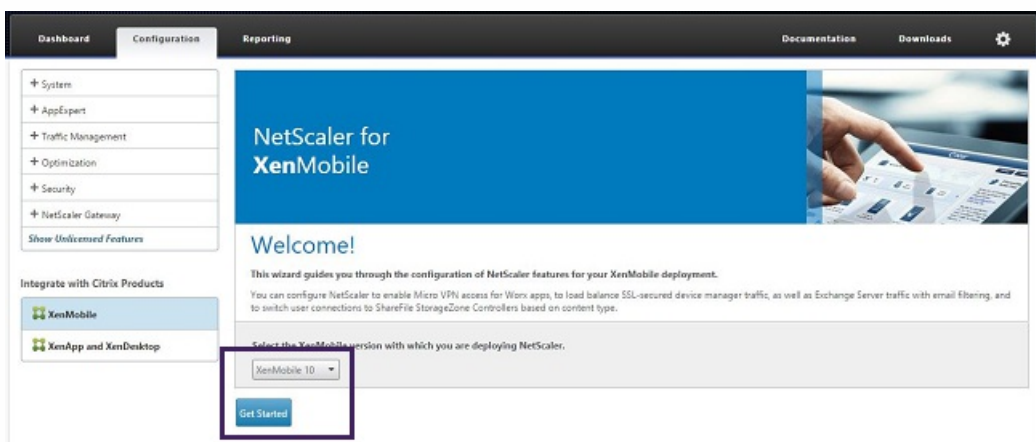
The new node is now a member of the cluster. You can add other nodes by following the same steps. To configure load balancing for the XenMobile cluster in NetScaler

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

1. Log on to NetScaler.

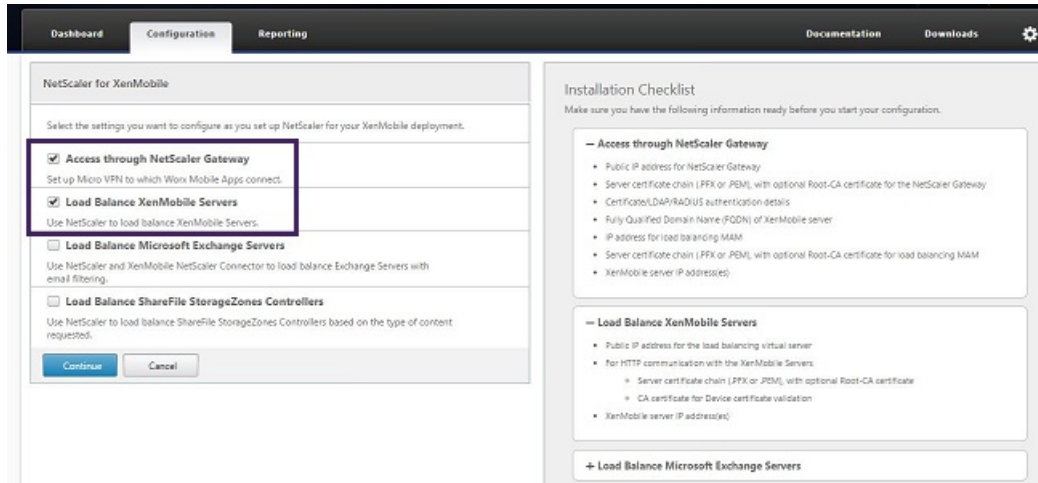


2. On the Configuration tab, click XenMobile and then click Get Started.

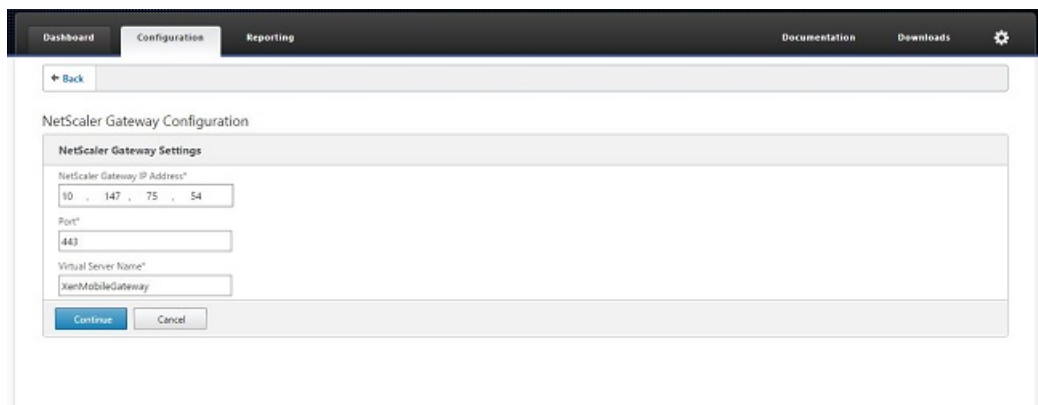


3. Select the Access through NetScaler Gateway check box and the Load Balance XenMobile Servers check box and then

click Continue.

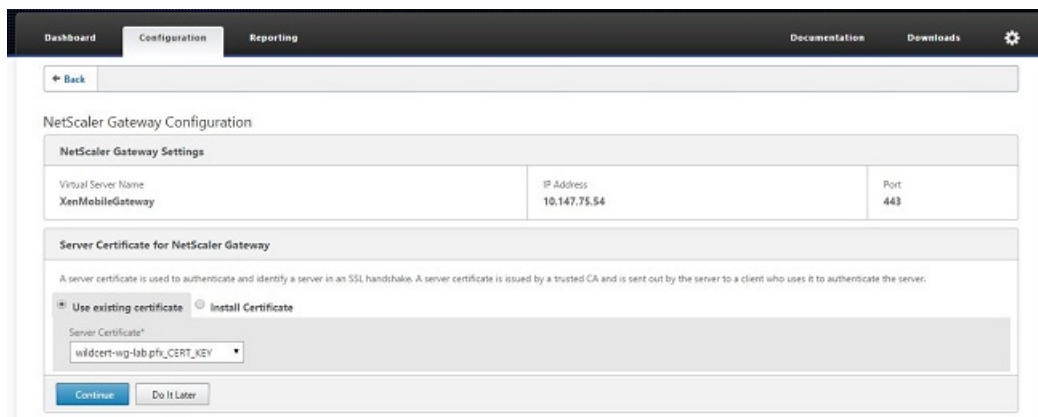


4. Enter the IP address for NetScaler Gateway and then click Continue.



5. Bind the server certificate to the NetScaler Gateway virtual IP address by doing one of the following and then click Continue.

- In Use existing certificate, choose the server certificate from the list.
- Click the Install Certificate tab to upload a new server certificate.



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

Authentication Settings

Select a primary authentication method for client connections. Primary authentication can be configured to use Active Directory/LDAP, RADIUS, or client certificate methods. For two-factor authentication, configure a secondary method from either RADIUS or Active Directory/LDAP methods.

Primary authentication method*
Active Directory/LDAP

IP Address*
10 . 147 . 75 . 240 IPv6

Port*
389

Base DN*
dc=wg,dc=lab

Service account*
administrator@wg.lab

Password*

Confirm Password*

Time out (seconds)*
3

Server Logon Name Attribute*
userPrincipalName

Secondary authentication method*
None

Note: Make sure the Server Logon Name Attribute is same as you provided in the XenMobile LDAP configuration.

- Under XenMobile settings, enter the Load Balancing FQDN for MAM and then click Continue.

XenMobile Settings

Load Balancing FQDN for MAM*
xms51.wg.lab

Load Balancing IP address for MAM*
10 . 147 . 75 . 55

Port*
8443

SSL Traffic Configuration*
 HTTPS communication to XenMobile Server
 HTTP communication to XenMobile Server

Split DNS mode for Micro VPN*
BOTH

Enable split tunneling

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

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

XenMobile Settings

Load Balancing FQDN for MAM	xms51.wg.lab	SSL Traffic Configuration	HTTPS communication to XMS Server
Load Balancing IP address for MAM	10.147.75.55	Split Tunnel	OFF
Port	8443	Split DNS	BOTH

Server Certificate for MAM Load Balancing

A server certificate is used to authenticate and identify a server in an SSL handshake. A server certificate is issued by a trusted CA and is sent out by the server to a client who uses it to authenticate the server.

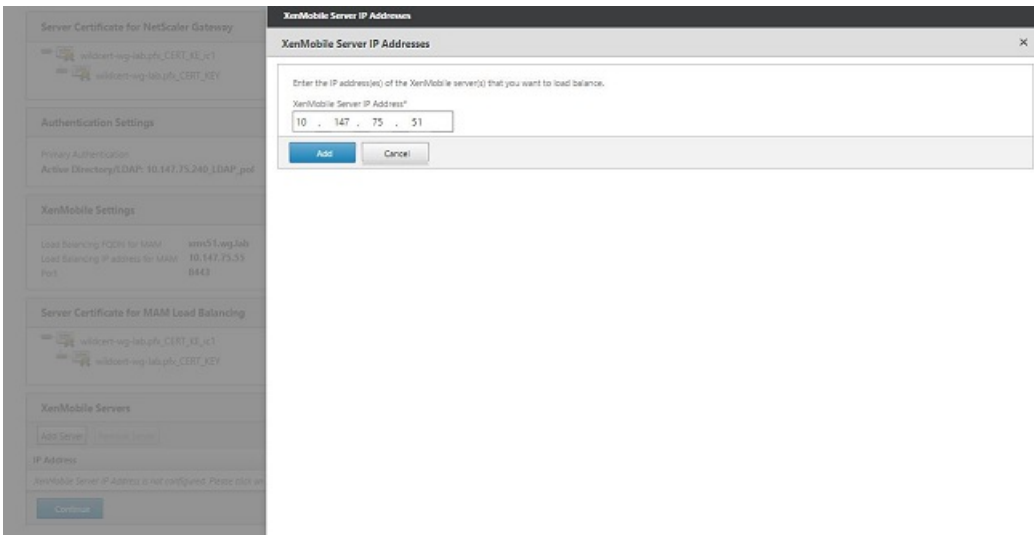
Use existing certificate Install Certificate

Server Certificate*
wildcert-wg-lab.pfx_CERT_KEY

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



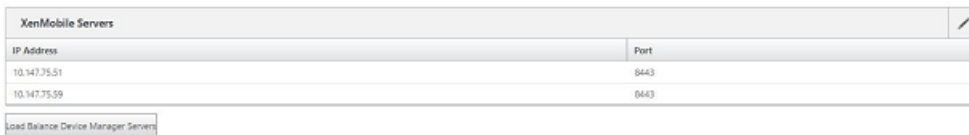
11. Enter the IP address of the XenMobile node and then click Add.



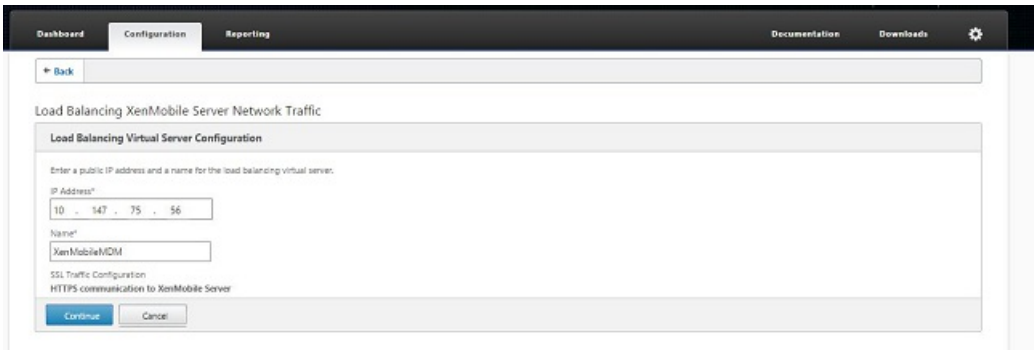
12. Repeat steps 10 and 11 to add additional XenMobile nodes that are part of the XenMobile cluster. You will see all the XenMobile nodes that you have added. Click Continue.



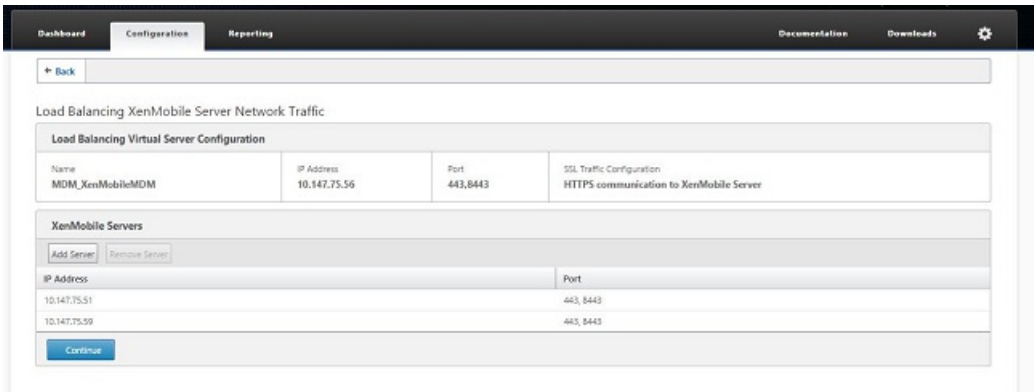
13. Click Load Balance Device Manager Servers to continue with the MDM load balancing configuration.



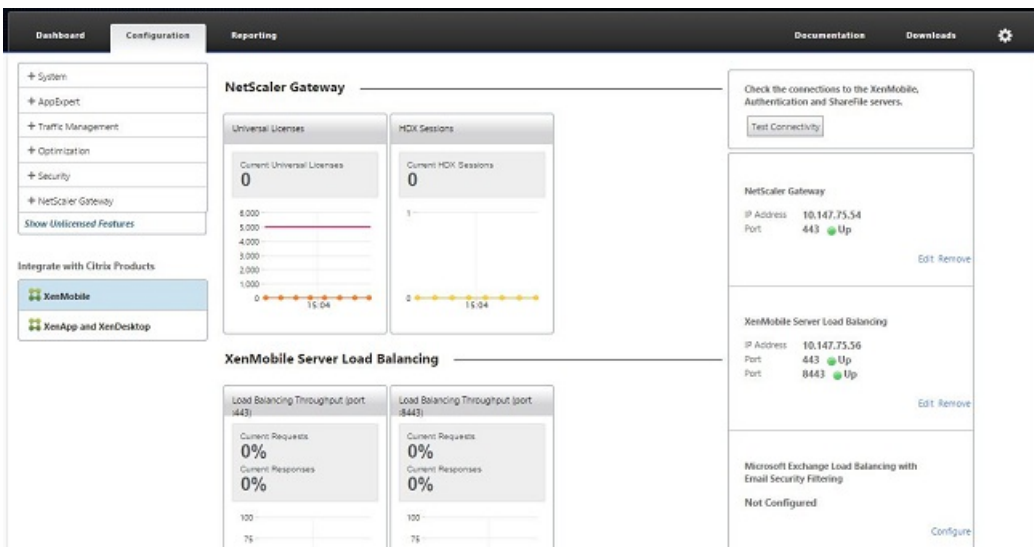
14. Enter the IP address to be used for MDM load balancing IP address and then click Continue.



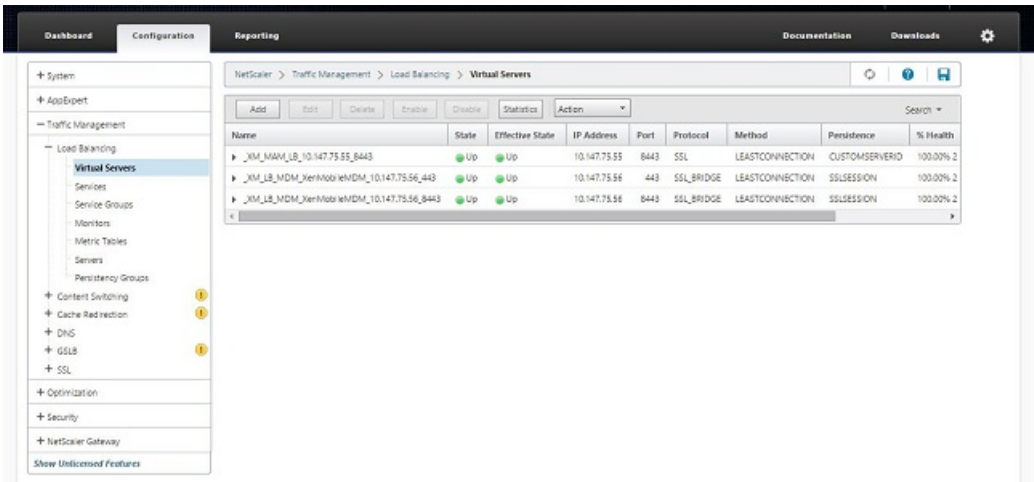
15. Once you see the XenMobile nodes in the list, click Continue and then click Done to finish the process.



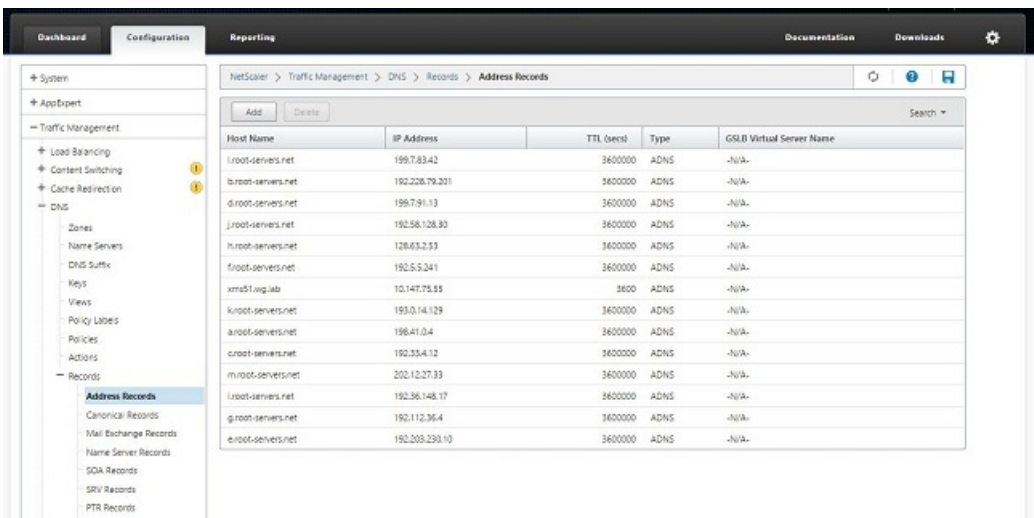
You will see the virtual IP address status on the XenMobile page.



16. To confirm if the virtual IP addresses are up and running, click the Configuration tab and then navigate to Traffic Management > Load Balancing > Virtual Servers.



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




```
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----
Choice: [0 - 5] 2
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Display System Disk Usage
[4] Update Hosts File
[5] Display Device Management Instance Name
[6] Proxy Server
[7] Admin (CLI) Password
[8] Restart Server
[9] Shutdown Server
[10] Advanced Settings
-----
```

```
-----
Choice: [0 - 10] 6
-----
Proxy Configuration Menu
-----
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
```

```
-----  
Proxy Configuration Menu  
-----  
[0] Back to System Menu  
[1] SOCKS  
[2] HTTPS  
[3] HTTP  
[4] Exclusion List  
[5] Display Configuration  
[6] Delete Proxy Configuration  
-----  
Choice: [0 - 6] 1  
  
Enter socks proxy information  
Address [1]: 203.0.113.23  
Port[]: 1080  
Target - APNS  
Proxy configuration updated successfully.  
Please restart all nodes in the cluster for the changes to take effect  
Are you sure to restart the system? [y/n]:
```

```
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
```

```
Choice: [0 - 6] 2
```

```
Enter https proxy information
```

```
Address [1]: 203.0.113.23
```

```
Port[1]: 4443
```

```
Configure username & password [y/n]: y
```

```
Username: Justaname
```

```
Password:
```

```
Target - WEB
```

```
WEB proxy configured. Override proxy settings?[y/n]: █
```


XenMobile Licensing Considerations

To find the Licensing page on the XenMobile console

Licensing

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

Default license Evaluation license

Trial period 30 day(s) left

Configure license OFF

Expiration notification OFF

To add a local license

Settings > Licenses

Licensing


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

Default license: Evaluation license

Trial period: 30 day(s) left

Configure license:

License type: Local license

 Add

Product Name	Active	Total number of licenses	Number used	Type	Expires on
No results found.					

Expiration notification:

Add New License

License File: No file chosen

License type: Local license

Add | Delete All

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

Showing 1 - 1 of 1 items

Expiration notification: OFF

To add a remote license

License type: Remote license

License server*:

Port*: 27000 Test Connection

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

To activate a different license

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

Showing 1 - 2 of 2 items

Expiration notification OFF

✓
 Activate

✓ **Activate** ✕

Are you sure you would like to activate a different license?
The currently active license will be deactivated.

To automate an expiration notification

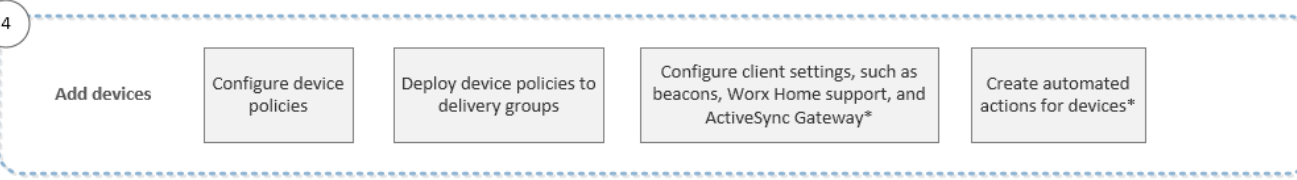
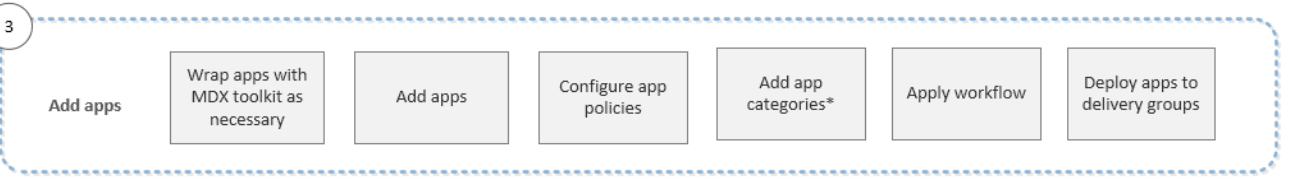
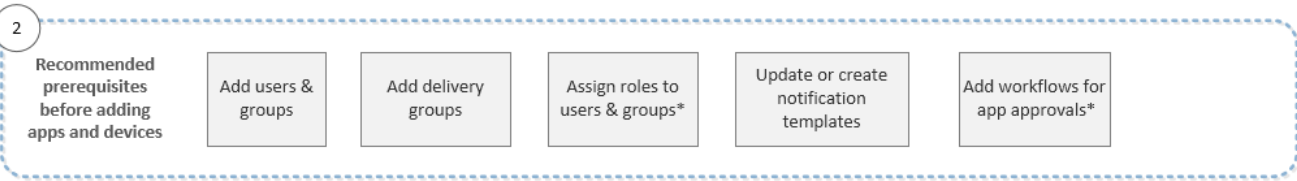
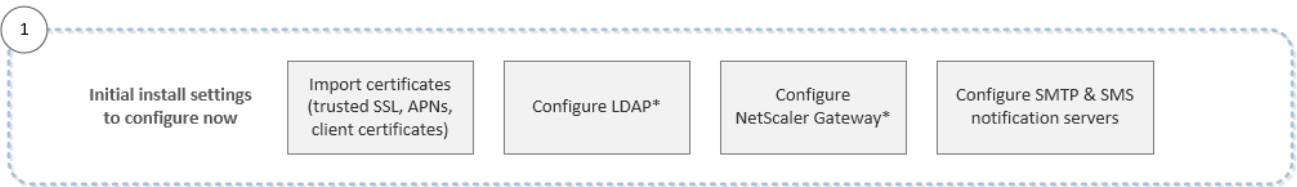
Expiration notification ON

Notify every* day(s) day(s) before expiration

Recipient*

Content*

-
-



5

Enroll user devices

Check enrollment modes for invitations

Send enrollment invitations

6

Ongoing app and device management

View notifications and monitor devices and apps on the dashboard

Issue security actions on devices as necessary

Do connectivity checks, create support bundles and view logs*

1

Initial install settings
to configure now

Import certificates
(trusted SSL, APNs,
client certificates)

Configure LDAP*

Configure
NetScaler Gateway*

Configure SMTP & SMS
notification servers

-
-
-
-

2

Recommended prerequisites before adding apps and devices

Add users & groups

Add delivery groups

Assign roles to users & groups*

Update or create notification templates

Add workflows for app approvals*

-
-
-
-
-
-

3

Add apps

Wrap apps with MDX toolkit as necessary

Add apps

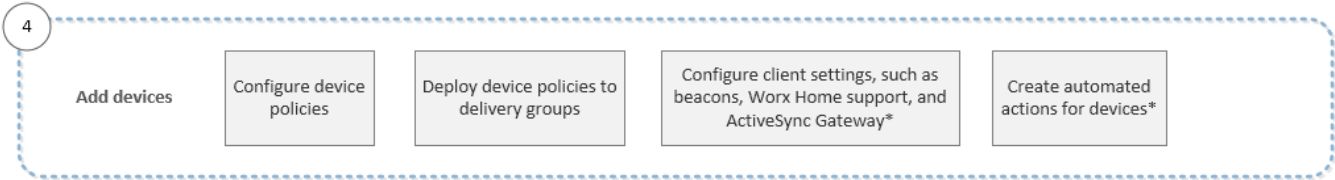
Configure app policies

Add app categories*

Apply workflow

Deploy apps to delivery groups

-
-
-
-
-
-



-
-
-
-
-

5

Enroll user devices

Check enrollment
modes for invitations

Send enrollment
invitations

-
-

6

Ongoing app and device management

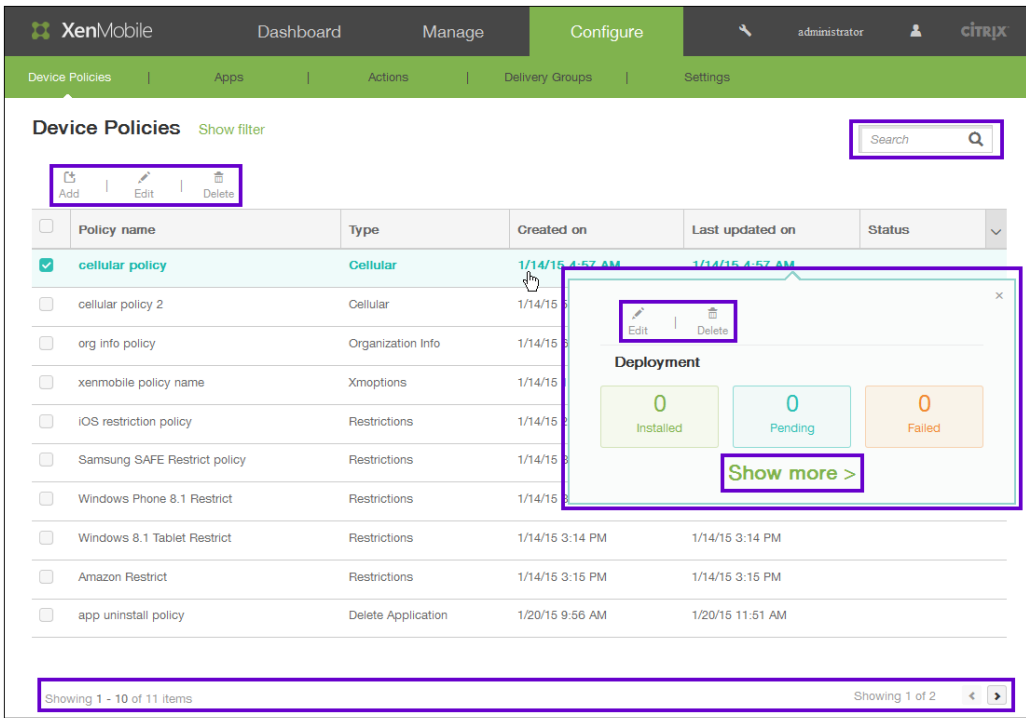
View notifications and monitor devices and apps on the dashboard

Issue security actions on devices as necessary

Do connectivity checks, create support bundles and view logs*

To view options from the tables in the XenMobile console

-
-
-
-



To filter information in the XenMobile console

Actions [Show filter](#)


Add

<input type="checkbox"/>	Name	Type	Trig
<input type="checkbox"/>	Jailbroken Device	Device property	Jailbr
<input type="checkbox"/>	Blacklisted App	Installed app name	Insta

Filter

Clear All

▼ Trigger Type

- Event 1
- User Property 0
- Device Property 1
- Application 1

▼ Action Type

- Notify 1
- Set As Out Of Compliance 1
- Selective Wipe 0
- Wipe 0
- Revoke 1

▼ Associated Delivery Group

- AllUsers 0

Actions Hide filter

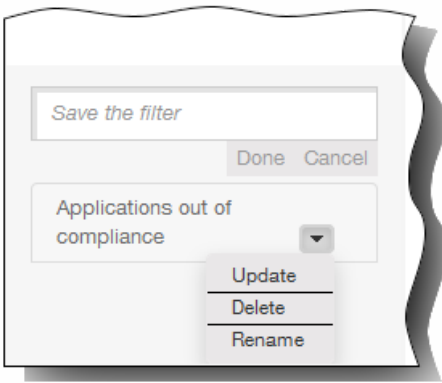
+ Add

	Name	Type
<input type="checkbox"/>	Jailbroken Device	Device prop
<input type="checkbox"/>	Blacklisted App	Instan
<input type="checkbox"/>	Out of Area	Event

Showing 1 - 3 of 3 items

Done Cancel

-
-



-

-

-

-

-

-

-

-

-

Settings > Notification Server

Notification Server

You can add and configure SMTP and SMS gatewa


[Add](#)

SMTP Server	Name
SMS Gateway	

-
-

Settings > Notification Server > Add SMTP Server

Add SMTP Server

You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP server is activated at one time.

Name*

Description

SMTP Server*

Secure channel protocol None ▼

SMTP server port*

Authentication OFF

Microsoft Secure Password Authentication (SPA) OFF

From name*

From email*

▶ Advanced Settings

-
-
-
-
-
-
-
-
-
-
-

•

•

Add a Carrier SMS Gateway

Converts email messages passing through the gateway to a pre-defined format, such as an instant message.

Carrier*

Gateway SMTP domain*

Country code*

Afghanistan +93 ▼

Email sending prefix

Cancel

Add

•

•

•

•

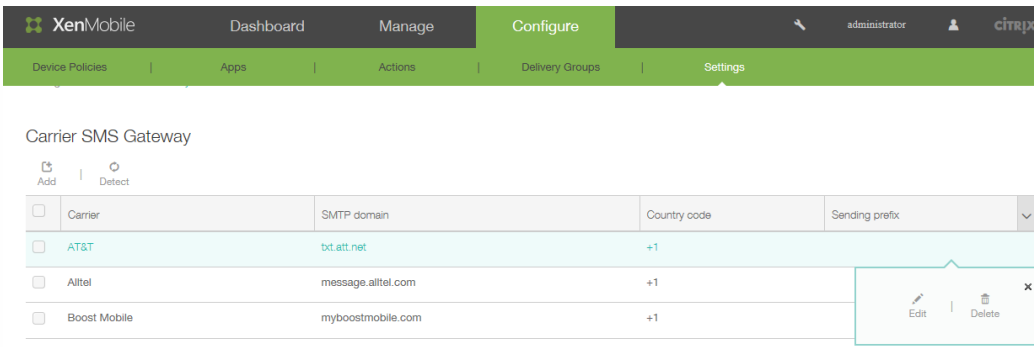
•

•

•

•

To add a Carrier SMS Gateway



The screenshot shows the XenMobile Configure page. The top navigation bar includes XenMobile, Dashboard, Manage, Configure (active), administrator, and CITRIX. Below this is a secondary navigation bar with Device Policies, Apps, Actions, Delivery Groups, and Settings. The main content area is titled "Carrier SMS Gateway" and features a table with columns for Carrier, SMTP domain, Country code, and Sending prefix. The table lists three carriers: AT&T (smtp.att.net, +1), Alltel (message.alltel.com, +1), and Boost Mobile (myboostmobile.com, +1). A context menu with Edit and Delete options is visible over the Alltel row.

Carrier	SMTP domain	Country code	Sending prefix
<input type="checkbox"/> AT&T	smtp.att.net	+1	
<input type="checkbox"/> Alltel	message.alltel.com	+1	
<input type="checkbox"/> Boost Mobile	myboostmobile.com	+1	

Add a Carrier SMS Gateway

Converts email messages passing through the gateway to a pre-defined format, such as an instant message.

Carrier*

Gateway SMTP domain*

Country code*

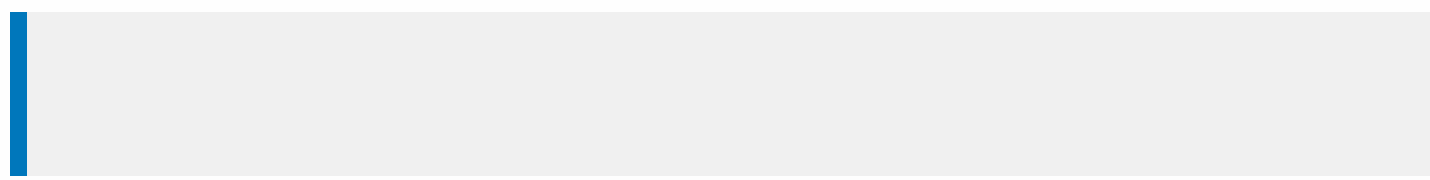
Email sending prefix

Cancel

Add

XenMobile PKI

XenMobile Certificate Expiration Policy



APNs certificate for WorxMail

APNs certificate for iOS device management

MDX Toolkit (iOS distribution certificate)

Android keystore

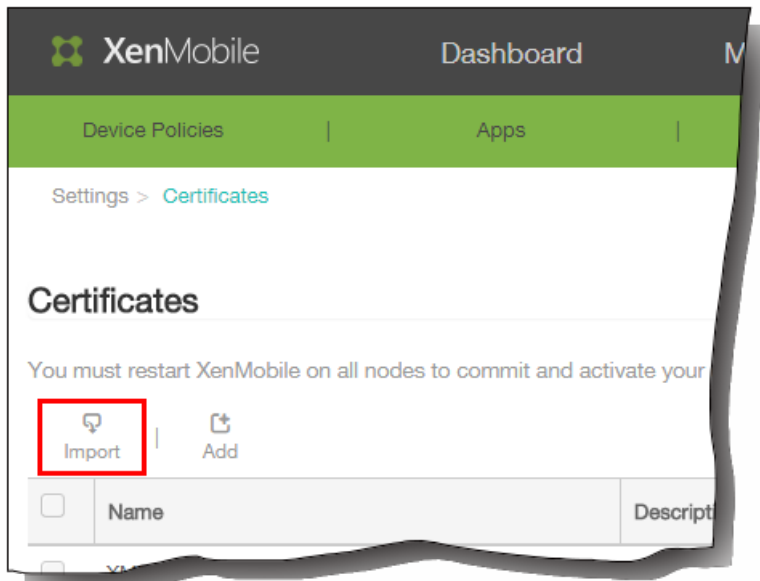
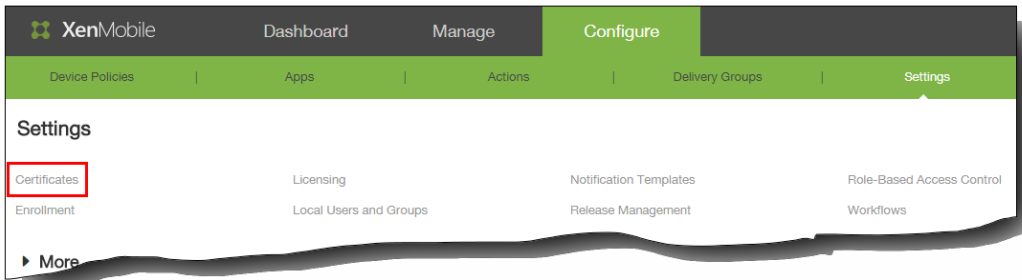
Enterprise certificate from Symantec for Windows phones

NetScaler

-

-

To import a keystore



Import ✕

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import

Keystore type

Use as

Keystore file*

Password*

Description

-
-
-
-

To import a certificate

Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import

Use as

Certificate import*

Private key file

Description

-
-
-

Updating a Certificate

-
-
-

-
-
-

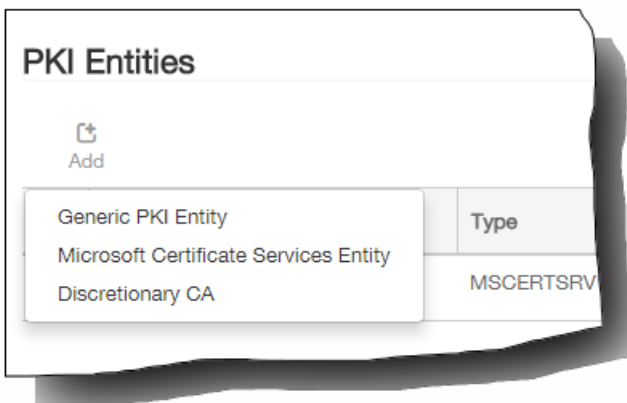
Common PKI Concepts

-
-
-

Generic PKI

-
-
-

To add a Generic PKI



Generic PKI Entity: General Information

The Generic PKI (GPKI) protocol is a proprietary XenMobile protocol running over a SOAP Web Service layer to provide uniform interfacing with various PKI solutions. The GPKI adapter, as a SOAP Web Services endpoint, publishes a self-describing Web Services Description Language (WSDL). You can create a GPKI entity to provide XenMobile with the WSDL through a URL.

Name*

WSDL URL* ?

Authentication type ?

-
-
-

Microsoft Certificate Services

To add a Microsoft Certificate Services entity

Microsoft Certificate Services Entity: General Information

Name*	<input type="text"/>	
Web enrollment service root URL*	<input type="text"/>	
certnew.cer page name*	<input type="text" value="certnew.cer"/>	?
certfnsh.asp*	<input type="text" value="certfnsh.asp"/>	?
Authentication type	<input type="text" value="Select an option"/>	?

-
-
-
-

Discretionary CAs


<https://server/instance/ocsp>

-
-
-
-
-

To add discretionary CAs

Discretionary CA: General Information

Name*

CA certificate to sign certificate requests* 

Discretionary CA: Parameters

Serial number generator*

Sequential

Next serial number

1



Certificate valid for

60

days

Key usage

Extended key usage

Name*

Add

DigitalSignature

ON

NonRepudiation

OFF

KeyEncipherment

ON

DataEncipherment

OFF

KeyAgreement

OFF

KeyCertSign

OFF

CRLSign

OFF

EncipherOnly

OFF

DecipherOnly

OFF

-

-

-
-
-
-
-
-

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

-
-

--	--	--

Certificate Revocation

-
-
-

Certificate Renewal

To create a credential provider

Credential Providers: General Information

You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.

Name*

Description

Issuing entity

Issuing method

Templates

Credential Providers: Certificate Signing Request ✕

Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.


Key algorithm:

Key size*:

Signature algorithm:

Subject name*:

Subject alternative names

Type	Value*	 Add
User Principal name	\${user.userprincipalname}	

CN=\${user.username} OU=\${user.department} O=\${user.companyname}
 C=\${user.c}\endquotation

•

•

Credential Providers: Distribution

Issuing CA certificate: CN=testprise-TESTPRISE_CA-...

Select distribution mode:

- Prefer centralized: Server-side key generation
- Prefer distributed: Device-side key generation
- Only distributed: Device-side key generation

Distributed mode uses the SCEP protocol and requires Registration Authority (RA) certificates. You may use the same RA certificate for both.

RA signing certificate*: Administrator,...

RA encryption certificate*: Administrator,...

Credential Providers: Distribution

Issuing CA certificate: CN=testprise-TESTPRISE_CA-...

Select distribution mode:

- Prefer centralized: Server-side key generation
- Prefer distributed: Device-side key generation
- Only distributed: Device-side key generation

Credential Providers: Revocation XenMobile

Configure the conditions under which XenMobile should internally flag certificates, issued through this provider configuration, as revoked.

Revoke issued certificates:

- When the certificate is renewed
- When the certificate is removed from the device
- When the certificate is wiped or revoked
- When the device is deleted from XenMobile

When certificate is revoked:

Send notification: OFF

Revoke certificate on PKI: OFF

When certificate is revoked

Send notification ON

Notification template No templates available

Revoke certificate on PKI OFF

When certificate is revoked

Send notification OFF

Revoke certificate on PKI ON

Entity No templates available

Credential Providers: Revocation PKI

Enable external revocation checks ON ?

OCSP responder CA certificate DC=net,DC=testprise,CN=testp...

When certificate is revoked Do nothing

Send notification OFF

-
-
-

-
-

-
-

Credential Providers: Renewal

Renew certificates when they expire ON

Renew when the certificate comes within* days of expiration

Do not renew certificates that have already expired

Send notification OFF

Notify when the certificate nears expiration OFF

Notify when the certificate comes within* days of expiration

-
-
-
-

-
-
-
-
-
-

--	--	--

Apple MDM Push Certificate Migration Information

-
-
-

To create a CSR by using Microsoft IIS

To create a CSR on a Mac computer

To create a CSR by using OpenSSL

To sign the CSR

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

To create a .pfx APNs certificate by using Microsoft IIS

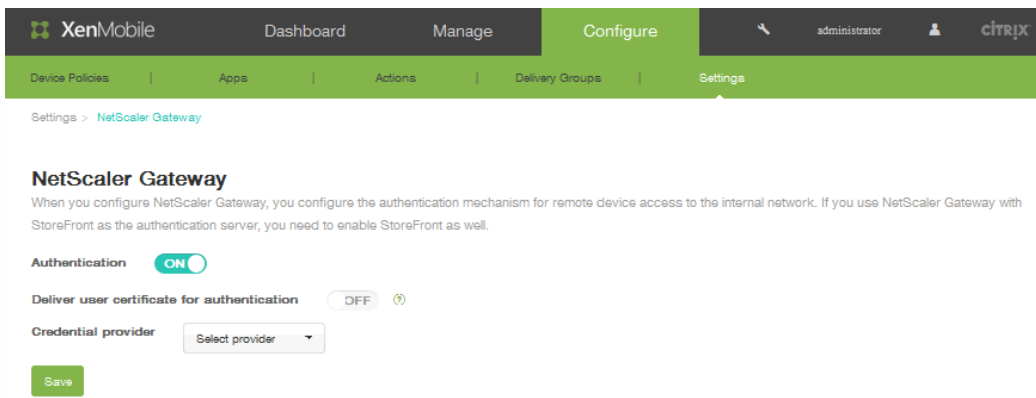
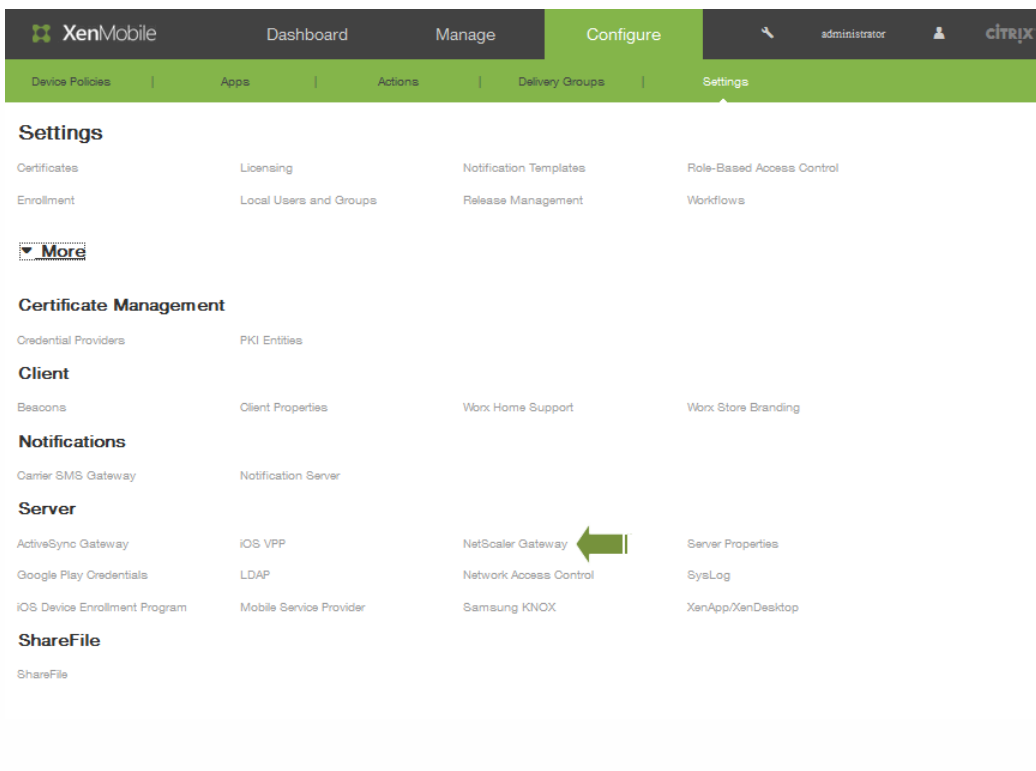
To create a .pfx APNs certificate on a Mac computer

To create a .pfx APNs certificate by using OpenSSL

To import an APNs certificate into XenMobile

To renew an APNs certificate

To configure NetScaler Gateway



To add a new NetScaler Gateway instance

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Dashboard', 'Manage', 'Configure', and 'Settings'. The 'Configure' tab is active, and the 'Settings' sub-tab is selected. The breadcrumb trail is 'Settings > NetScaler Gateway > Add New NetScaler Gateway'. The main form is titled 'Add New NetScaler Gateway' and contains the following fields and controls:

- Name***: Text input field with placeholder 'Appliance name'.
- Alias**: Text input field.
- External URL***: Text input field with placeholder 'Publicly accessible URL'.
- Logon Type**: Dropdown menu with 'Domain only' selected.
- Password Required**: Toggle switch set to 'ON'.
- Set as Default**: Toggle switch set to 'OFF'.
- Callback URL***: Text input field.
- Virtual IP***: Text input field.
- Add**: Button with a plus icon.
- Cancel** and **Save**: Buttons at the bottom right.

XenMobile Dashboard Manage **Configure** administrator CITRIX

Device Policies | Apps | Actions | Delivery Groups | Settings

Settings > NetScaler Gateway

NetScaler Gateway

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

Authentication ON

Deliver user certificate for authentication OFF (?)

Credential provider

<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs
<input type="checkbox"/>	netscalerboston	✓	https://receiver.com	Domain	0

XenMobile Dashboard Manage **Configure** Delivery Groups Settings

Settings > NetScaler Gateway > [Add New NetScaler Gateway](#)

Add New NetScaler Gateway

Name*


Alias

External URL*

Logon Type

Password Required ON

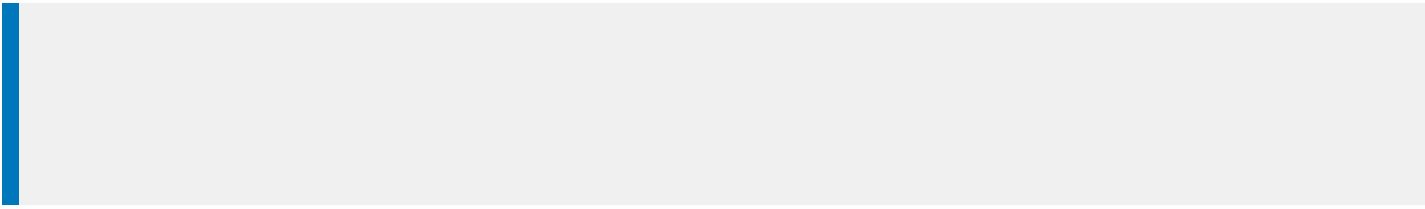
Set as Default ON

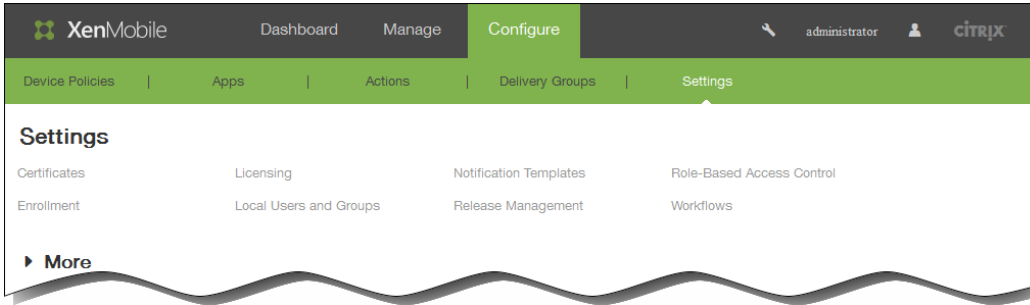
Callback URL* Virtual IP* 

Callback URL*	Virtual IP*	
<input type="text"/>	<input type="text"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

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

-
-
-
-
-





-

-
-
-
-

-
-
-

-
-

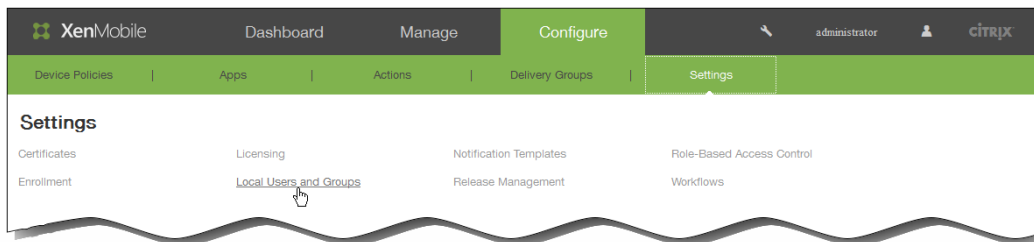
-

To add, edit, or delete local users in XenMobile

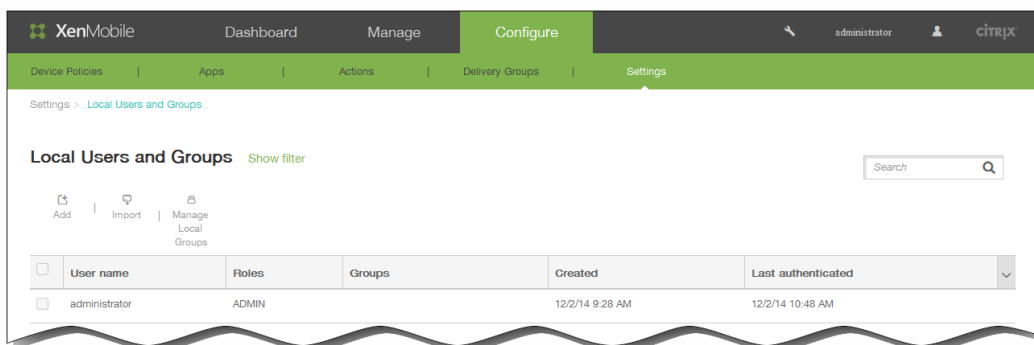
Feb 27, 2015

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 Configure > Settings > Local Users and Groups.



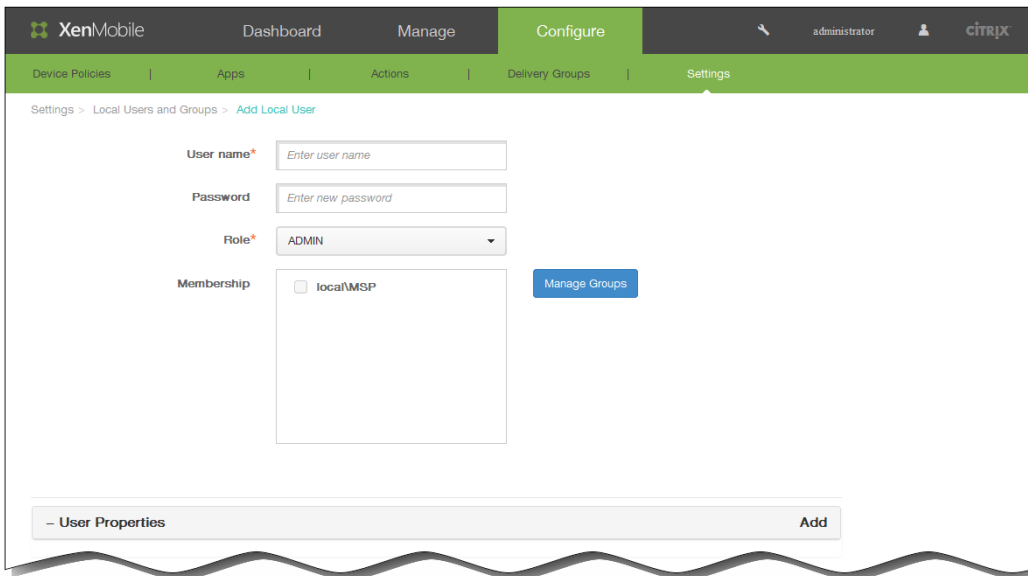
The Local Users and Groups page appears.



To add a local user

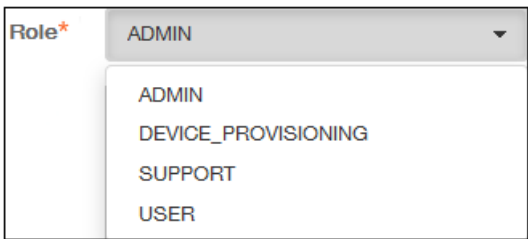
This procedure adds one user to XenMobile at a time. To add multiple users, see [To import user accounts by using a .csv provisioning file](#).

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



2. Type the following information to add a new local user:

1. User name: Type the user's name. This is a required field.
2. Password: Type an optional user password.
3. Role: In the Role list, click the user's role. For more information about roles, see [To create or update custom roles in XenMobile with RBAC](#).

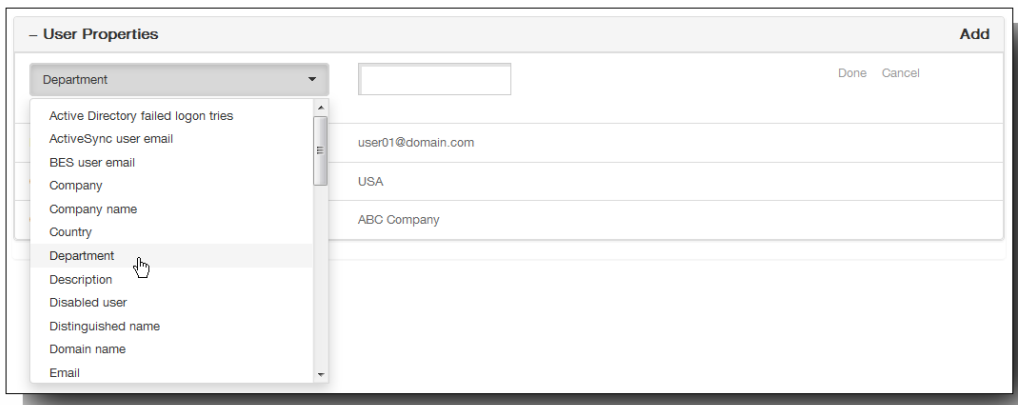


4. Membership: In the Membership list, click the group or groups to which to add the user.

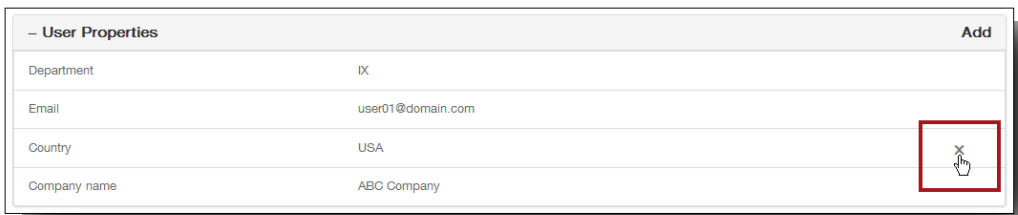


3. To optionally add user properties, follow these steps:

1. Next to User Properties, click Add.
2. In the User Properties list, click a property.
3. Type the user property attribute in the field next to the list.



4. Click Done to save the user property or click Cancel to cancel the operation.
5. Repeat steps b, c, and d for other properties you want to add.
4. Optionally, to edit a user property, do the following:
 1. Click the user property you want to edit.
 2. Change the user property attribute.
 3. Click Done to save the edit or click Cancel to cancel the edit.
5. Optionally, to delete a user property, do the following:
 1. Hover over the line containing the user property you want to delete.
 2. Click the X that appears on the right side of the line.

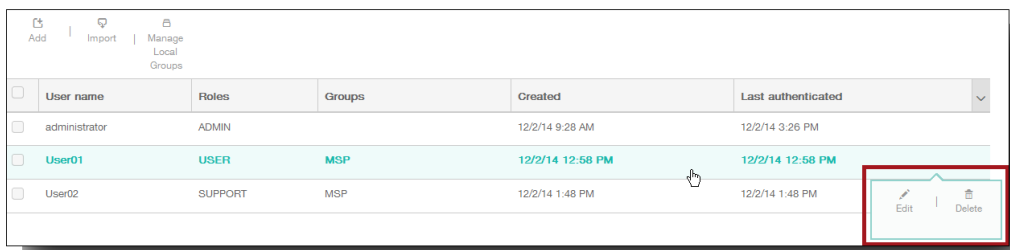


The property is deleted immediately.

6. Click Save to save the new user.

To edit a local user

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



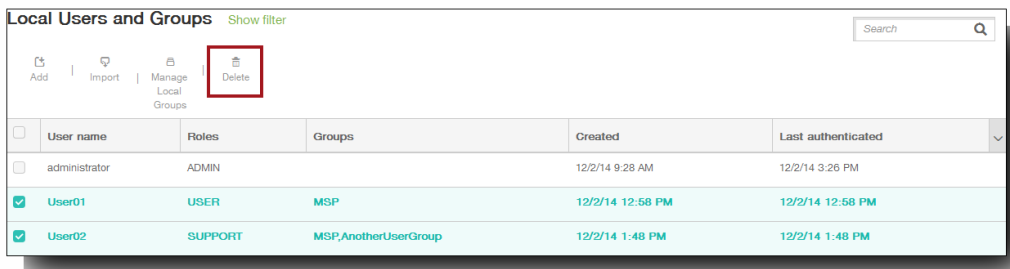
The Edit Local User page appears.

2. Change the following information as appropriate:
 1. User name: Type the user's name. This is a required field.

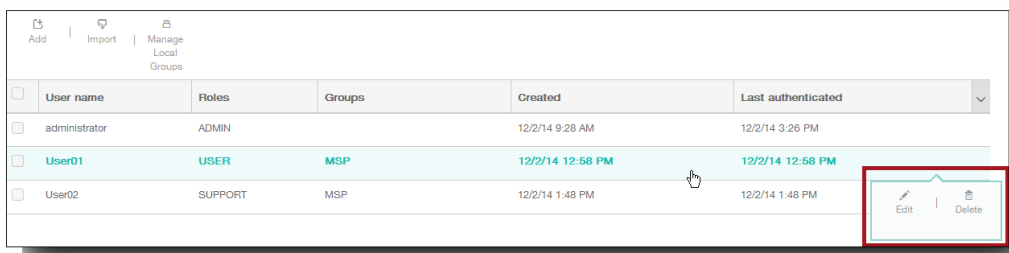
2. Password: Type an optional user password.
 3. Role: In the Role list, click the user's role.
 4. Membership: In the Membership list, click the group or groups to which to add the user.
 5. User properties: Add new or edit existing user properties.
3. Click Save to save your changes.

To delete a local user

1. On the Local Users and Groups page, in the list of users, do one of the following:
 - Select the check box next to the user or users you want to delete, and then click Delete.



- Click the line for a user you want to delete, and in the menu that appears on the right, click Delete.



A confirmation dialog appears. Click Delete to confirm the operation and remove the user or users.
 Important: You cannot undo this operation.

Importing User Accounts

Mar 06, 2015

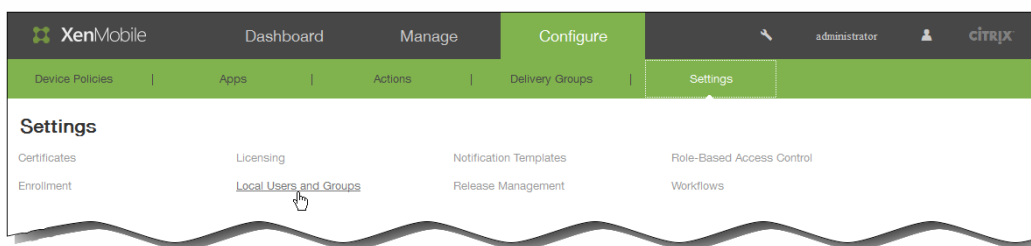
You can import user accounts and properties from a .csv file called a provisioning file, which you can create manually. See [Provisioning file formats](#) for information on formatting provisioning files.

Note:

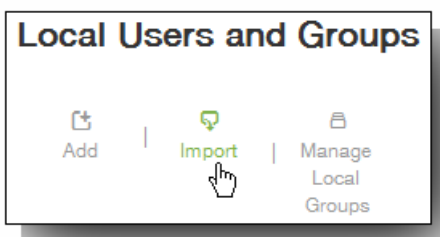
- If you are importing users from an LDAP directory, use the domain name along with the user name in the import file. For example, specify username@domain.com. This syntax prevents additional lookups that will slow the import speed.
- If importing users to the XenMobile internal user directory, disable the default domain in order to speed up the import process. You can reenble 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 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 Configure > Settings > Local Users and Groups.

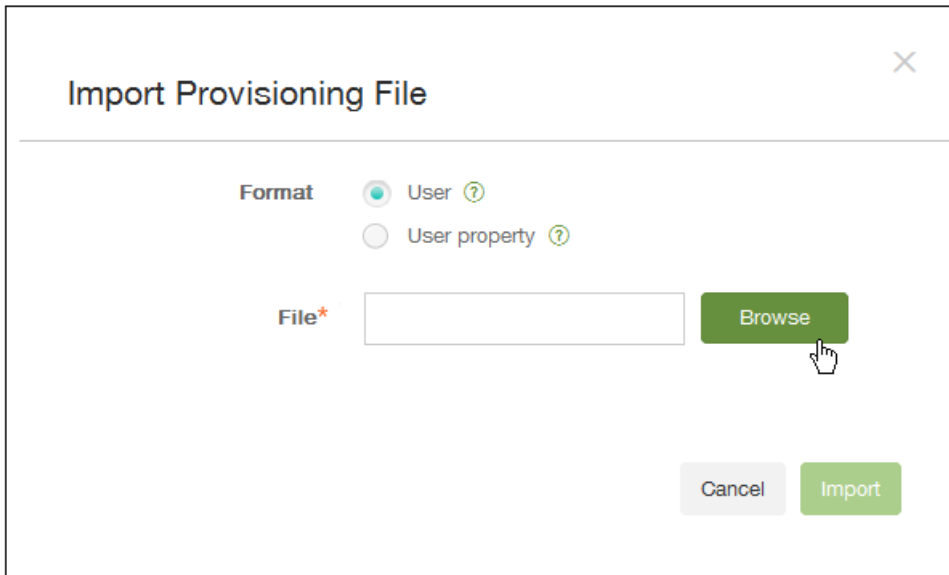


2. On the Local Users and Groups page, click Import.



The Import Provisioning File dialog box appears.

3. On the Import Provisioning File dialog box, select the format of the provisioning file you are importing.



4. Next to File, click Browse to navigate to the location of your provisioning file and then click Import.

Provisioning file formats

Mar 06, 2015

A provisioning file that you create manually and use to import user accounts and properties to XenMobile must be in the following formats:

- User provisioning file fields: user;password;role;group1;group2
- User attribute provisioning file fields: user;propertyName1;propertyValue1;propertyName2;propertyValue2

Note:

- The fields within the provisioning file are separated by a semi-colon (;). If part of a field contains a semi-colon, it must be escaped with a backslash character (\). For example, the property `propertyV;test;1;2` would 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\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01`, means:

- User: user01
- Password: pwd;01
- Role: USER
- Groups:
 - myGroup.users01
 - myGroup.users02
 - myGroup.users.users01

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: prop 2 value

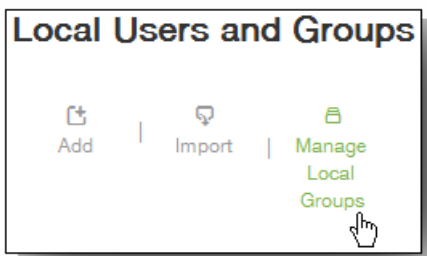
Adding or Removing Groups

Mar 06, 2015

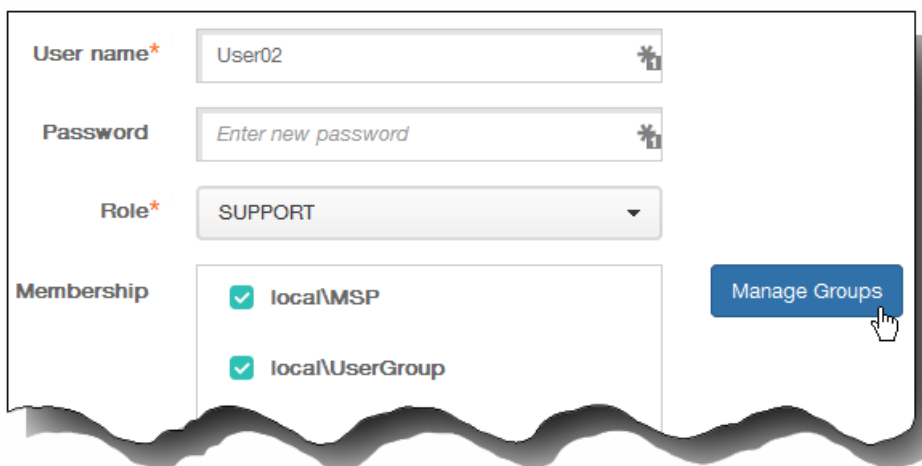
You manage groups in the Manage Groups dialog box in the XenMobile console, which you can find on the Local Users and Groups page, the Add Local User page, or the Edit Local User page. There is no group edit command. If you remove a group, keep in mind that removing a group has no effect on user accounts. 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.

To add a local group

1. Do one of the following:
 - On the Local Users and Groups page, click Manage Local Groups.

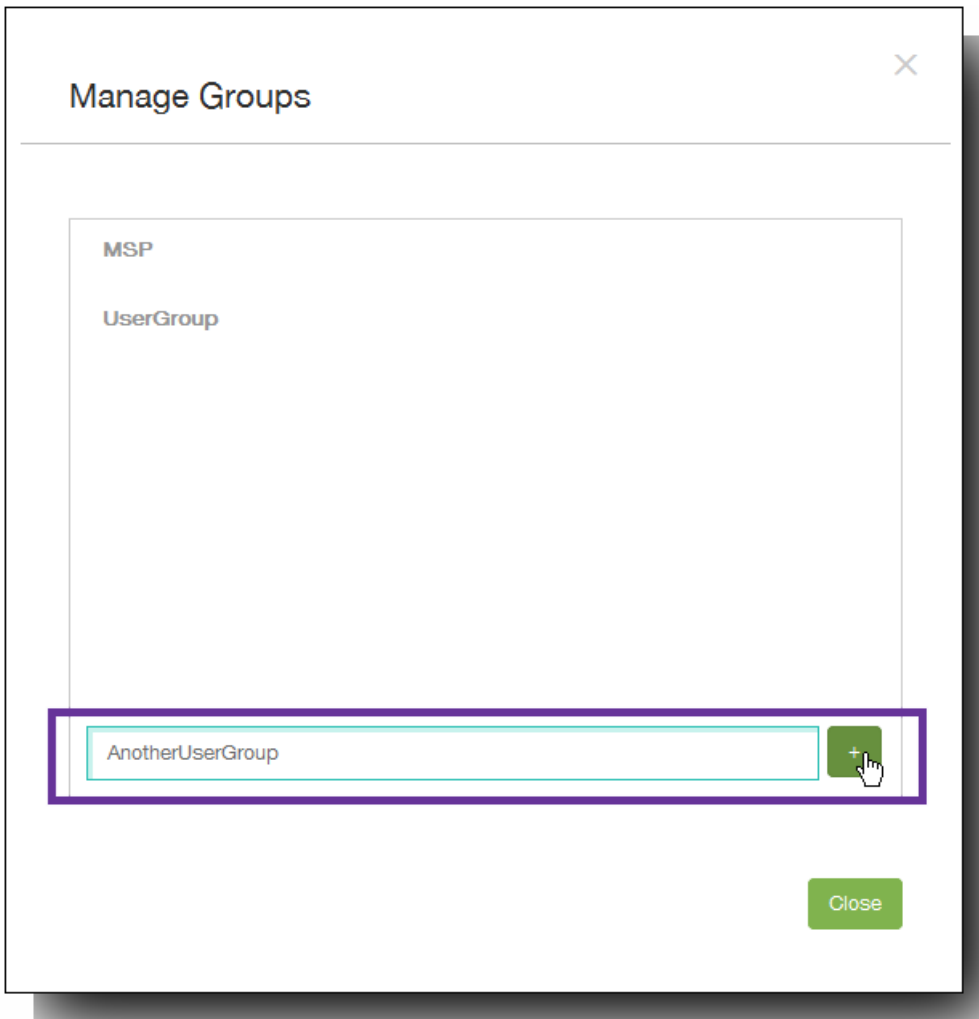


- On either the Add Local User page or the Edit Local User page, click Manage Groups.



The Manage Groups dialog box appears.

2. Below the group lists, 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

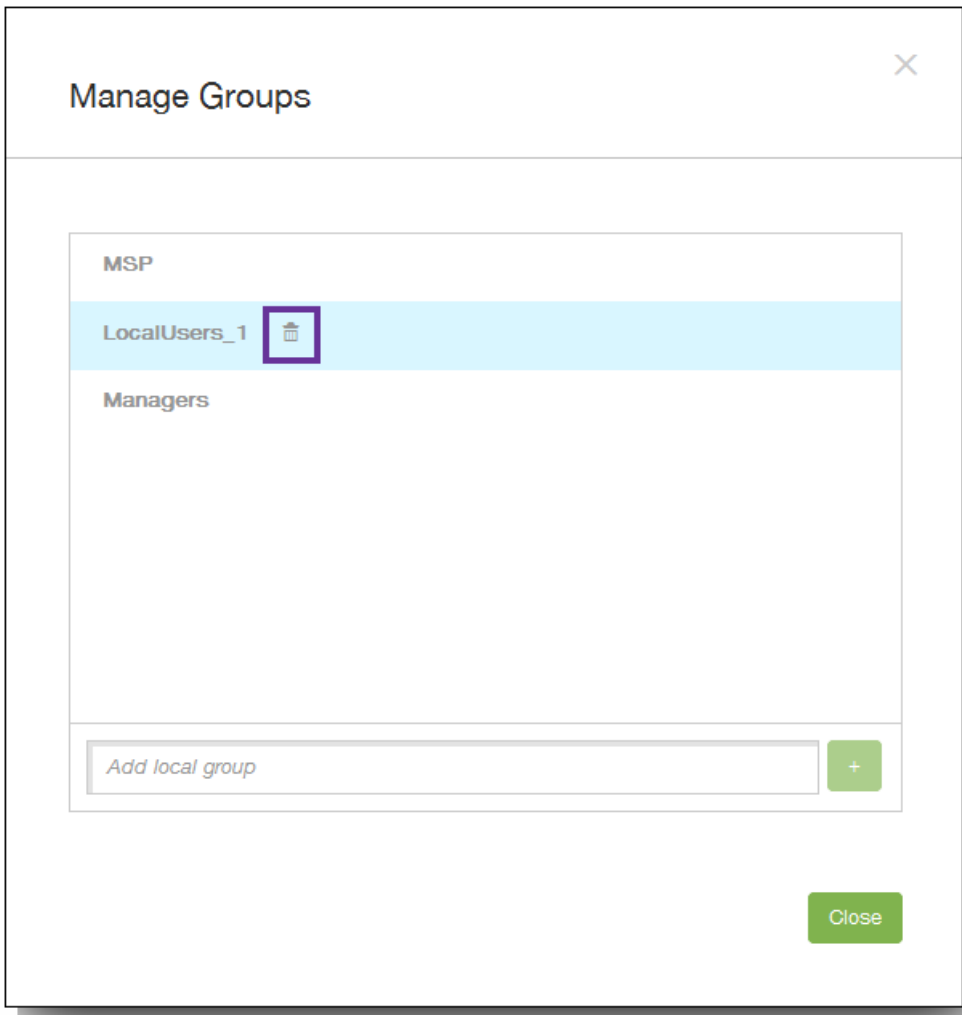
Note: Removing a group has no effect on user accounts. Removing a group simply removes the users' association with that group. Users also lose access to apps or profiles provided by the Delivery Groups that are associated with that group; any other group associations, however, remain intact. If users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

1. Do one of the following:

- On the Local Users and Groups 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.

To configure enrollment modes and enable the Self Help Portal

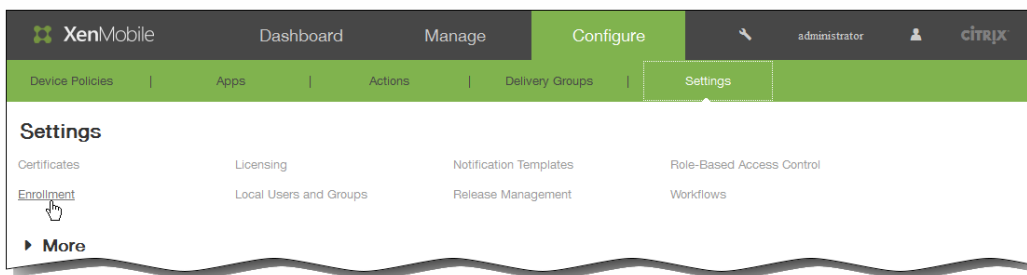
Apr 01, 2015

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.

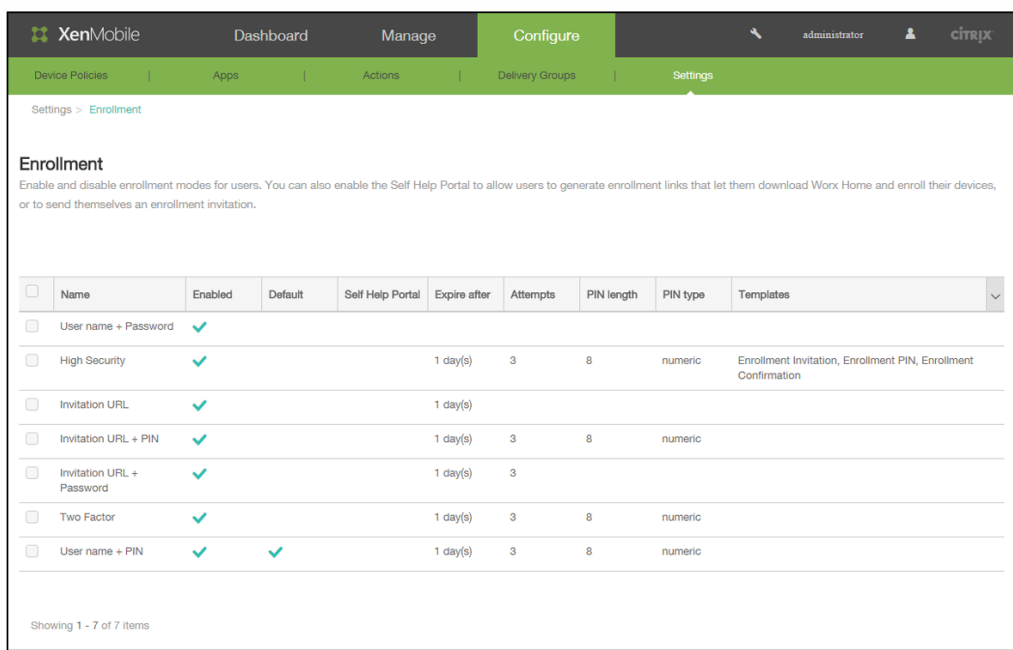
You configure enrollment modes in the XenMobile console from the Settings > Enrollment page. You send enrollment invitations in the XenMobile console from the Manage > Enrollment page (see [Enrolling Users and Devices in XenMobile](#)).

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 [To create or update notification templates in XenMobile](#).

1. On the XenMobile console, click Configure > Settings > Enrollment.

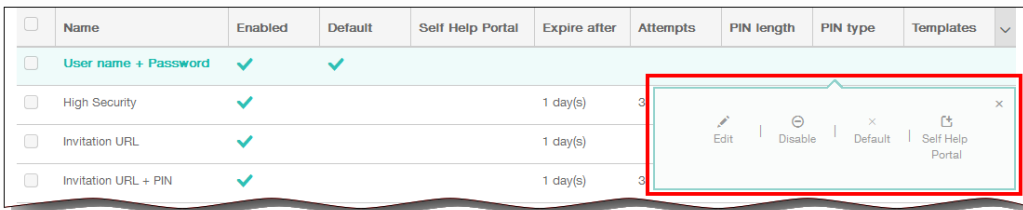
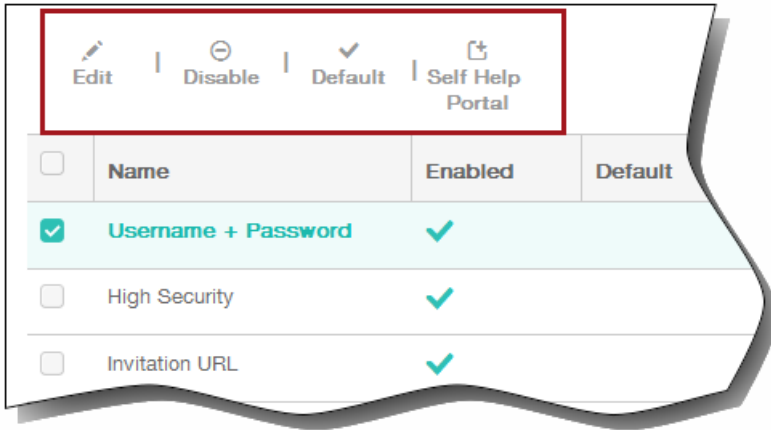


The Enrollment page appears, containing a table of all available enrollment modes.



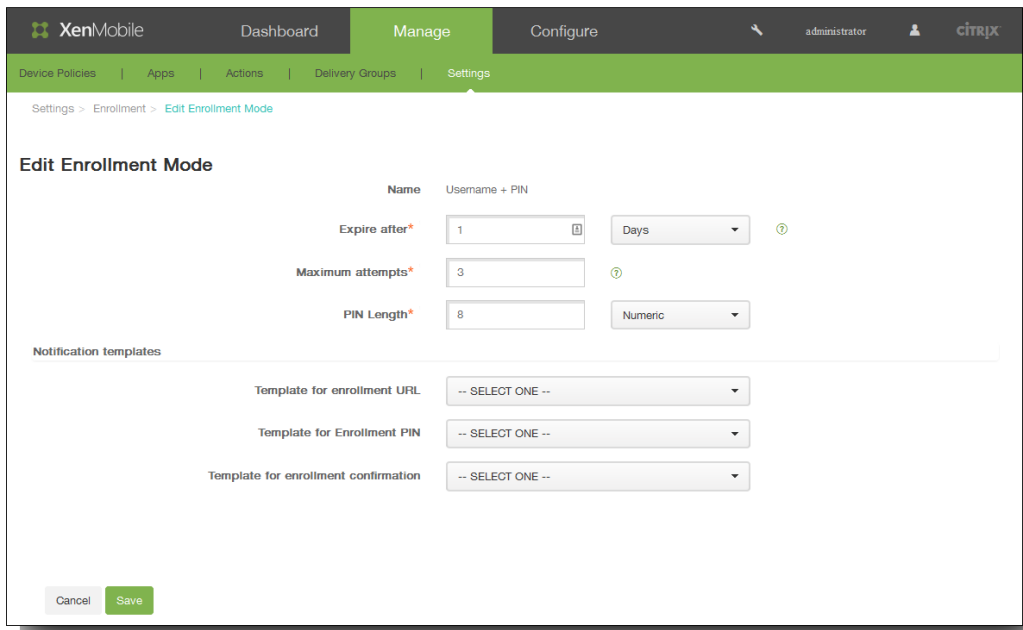
- Select any enrollment mode in the list to edit and then set the mode as the default, delete the mode, or allow users access through the Self Help Portal.

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

- In the Enrollment list, select an enrollment mode and then click Edit. Depending on the mode you select, you may see different options than the options shown in the following figure.



2. Change the following information as appropriate:
 1. Expire after: Enter an expiration deadline after which users cannot enroll their devices.
Note: Enter 0 to prevent the invitation from expiring.
 2. Days: Select Days or Hours to correspond to the expiration deadline you entered in Expire after.
 3. Maximum attempts: Enter the number of attempts to enroll that a user can make before being locked out of the enrollment process.
Note: Enter 0 to allow unlimited attempts.
 4. PIN length: Enter a numeral for how many digits/characters the generated PIN will contain.
 5. Numeric: Select Numeric or Alphanumeric for the PIN type.
3. Under Notification templates, change the following settings as appropriate:
 1. Template for enrollment URL: Select 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 [To create or update notification templates in XenMobile](#).
 2. Template for enrollment confirmation: Select a template to use to inform a user that enrollment was successful.
4. Click Save to commit your changes.

<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
<input type="checkbox"/>	Username + Password	✓							Enrollment invitation, Enrollment Confirmation

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 + Passwords, Two Factor, or Username + PIN can be set as the default enrollment mode.

1. Select one of Username + Passwords, 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.

<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
<input type="checkbox"/>	Username + Password	✓	✓						Enrollment invitation, Enrollment Confirmation

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.

<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
<input type="checkbox"/>	Username + Password								Enrollment Invitation, Enrollment Confirmation

To enable an enrollment mode on the Self Help Portal

Enabling an enrollment mode on the Self Help Portal lets users enroll their devices in XenMobile individually.

Note:

- The enrollment mode must be enabled and bound to notification templates to be made available on the Self Help Portal.
 - You can only enable one enrollment mode on the Self Help Portal at a time.
1. Select an enrollment mode.
 2. Click Self Help Portal. The enrollment mode you selected is now available to users on the Self Help Portal. Any mode already enabled on the Self Help Portal is no longer available to users.

<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
<input type="checkbox"/>	Username + Password	✓	✓	✓					Enrollment Invitation, Enrollment Confirmation

Configuring Roles with RBAC

Feb 13, 2015

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.
- **Provisioning.** Used by administrators to provision all Windows Mobile/CE devices as a group using the Device Provisioning Tool.
- **Support.** Grants access to remote support.
- **User.** Used by users who can enroll devices and access the Self Help Portal.

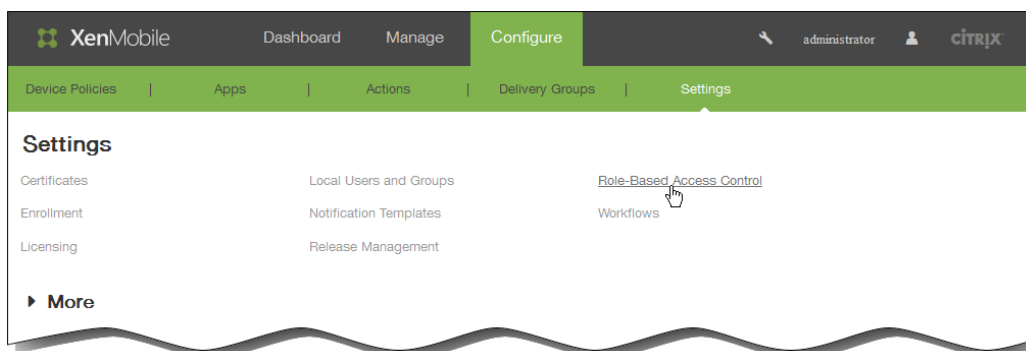
You can also create new user roles with permissions to access specific system functions beyond the functions defined by these default roles by using the default roles as templates that you customize.

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.

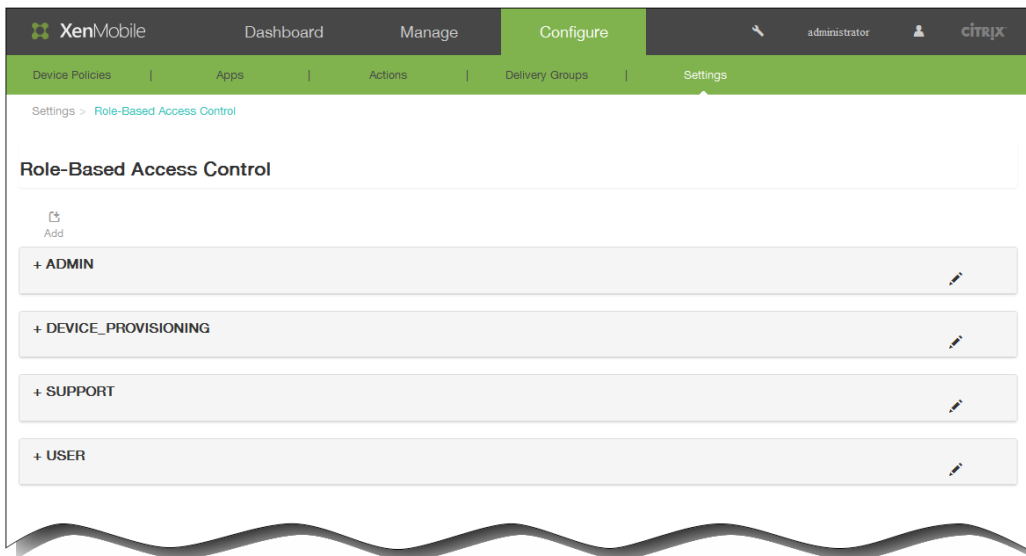
You can use the RBAC feature in XenMobile to do the following:

- Create a new role.
- Add groups to a role.
- Associate local users to roles.

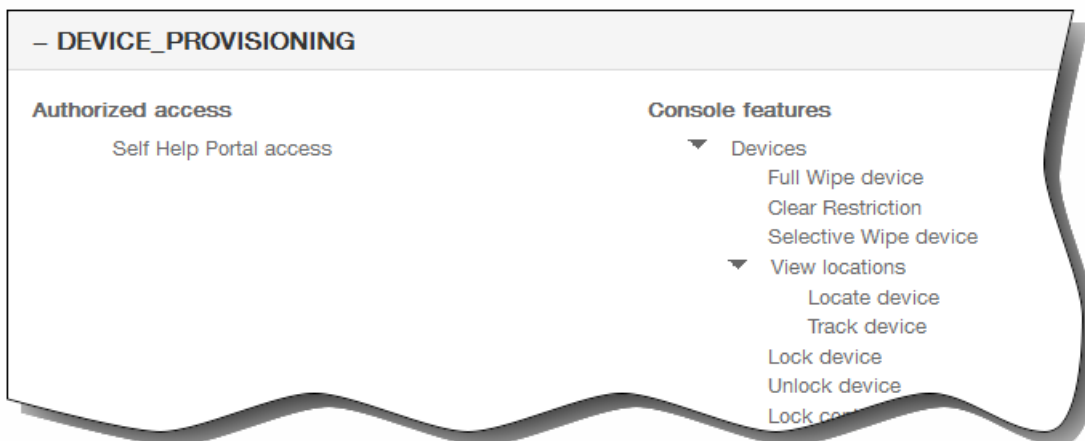
1. In the XenMobile console, click Configure > Settings > Role-Based Access Control.



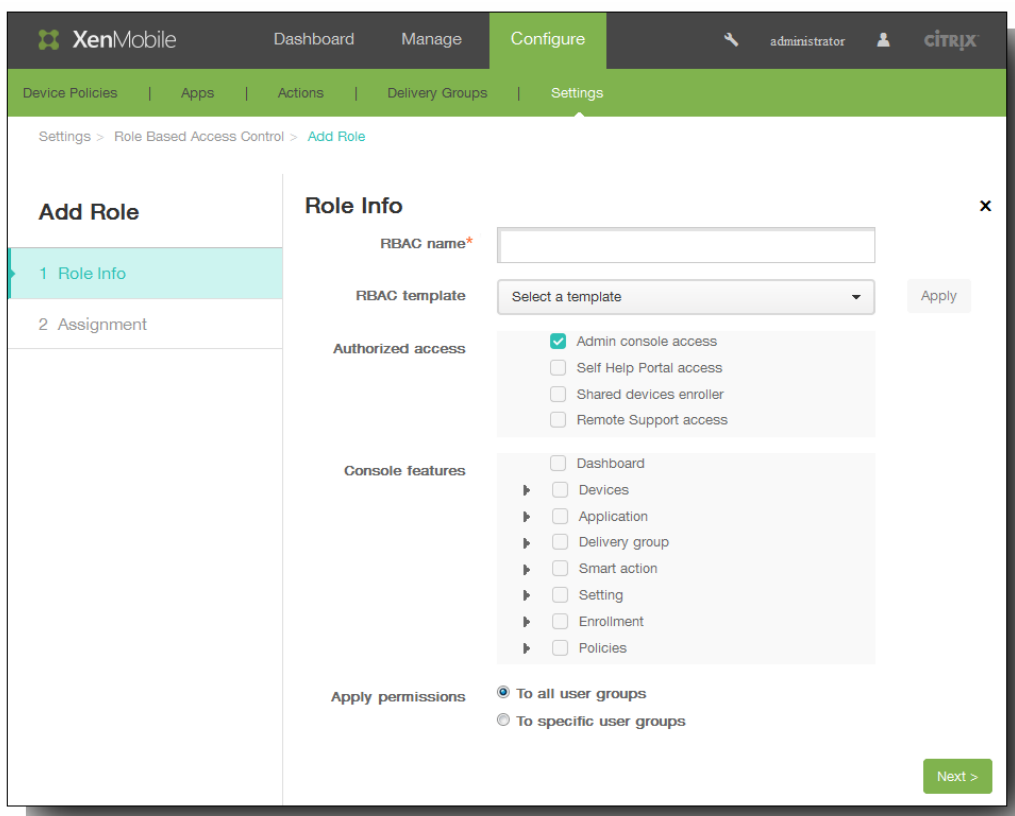
The Role page appears, which displays the four default user roles, plus any roles you have previously added.



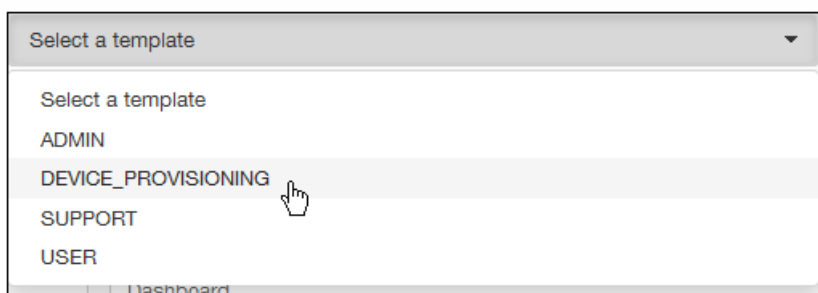
Note: If you click the plus sign (+) next to a role, the role expands to show all the permissions for that role, as shown in the following figure.



2. 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.

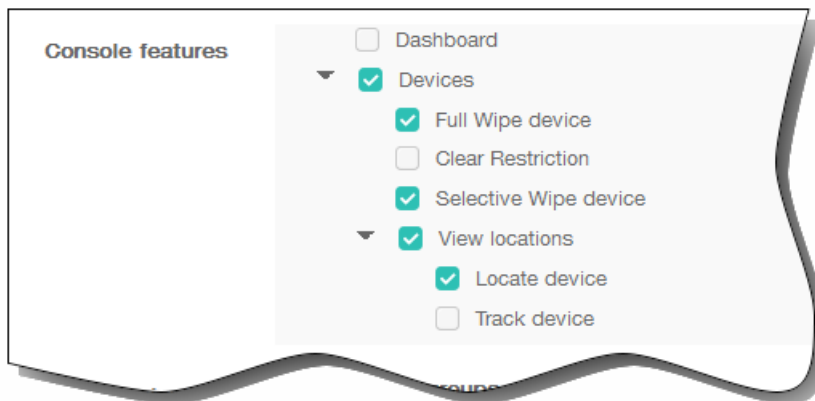


- When you click the trash can icon, a confirmation dialog appears. Click Delete to remove the selected role.
3. Enter the following information to create a new user role or to edit an existing user role:
1. RBAC name: Enter a descriptive name for the new user role. You cannot change the name of an existing role.
 2. RBAC template: Click a template as the starting point for the new role or click a new template for an existing role. Note: RBAC templates are the default user roles, plus any roles that you have previously defined. They define the access users associated with that role have to system functions. After you select an RBAC template, you can see all of the permissions associated with that role in 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.

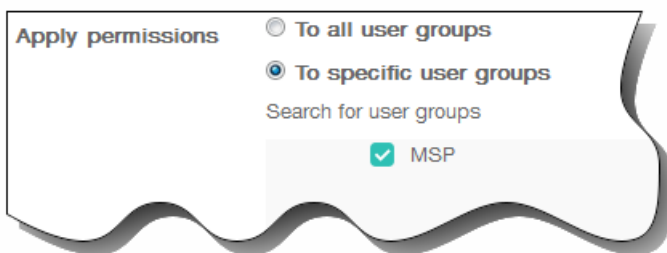


- Click Apply to populate the Authorized access and Console features check boxes with the pre-defined access and feature permissions for the selected template.
- Select and clear the check boxes in Authorized access and Console features to customize the role. Note: If you click the triangle next to a Console feature, permissions specific to that feature appear that you can

select and clear. Clicking the top-level check box allows read-only access to that console part; you must select individual options below the top level to enable write/update access for that option. For example, in the following figure, the user has read-only access to the Clear Restrictions option.

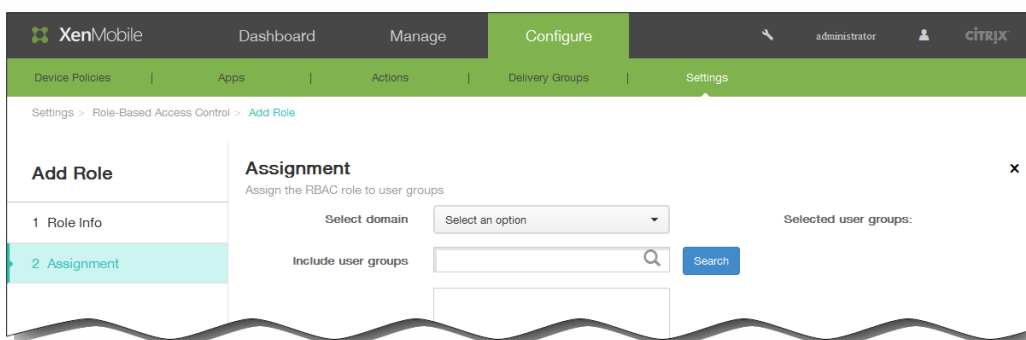


3. Apply permissions: Select the groups to which you want to apply the selected permissions.



If you click To specific user groups, a list of groups appears from which you can select one or more groups.

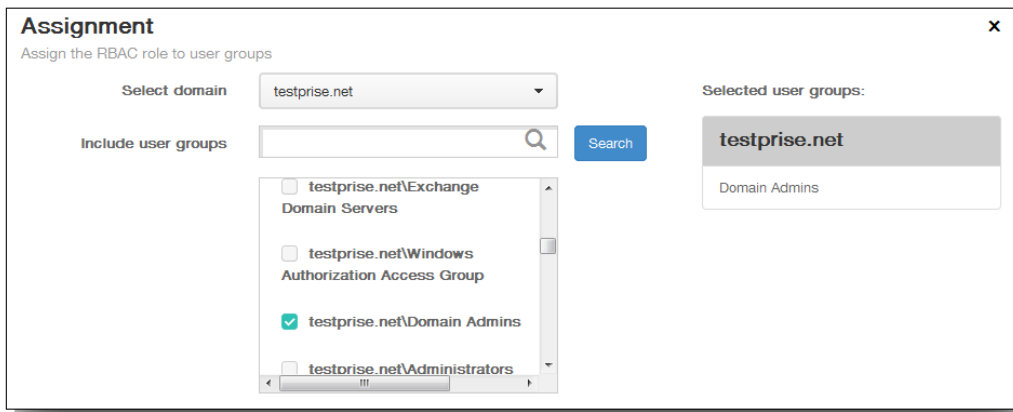
4. Click Next. The Assignment page appears.



5. Enter the following information to assign the role to user groups and then click Save.

1. Select domain: In the list, click a domain.
2. 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.
3. 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 a list of selected groups to the right of the search box.



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

- 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.

User groups in the list have check marks next to their name in the resulting list. Scroll through the list and clear the check box next to each group you want to remove.

To 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 autodiscover 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:
 1. 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.
 2. 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).

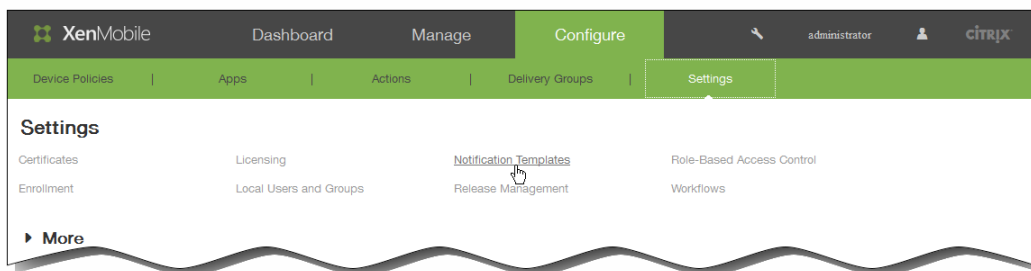
Creating and Updating Notification Templates

Feb 13, 2015

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: 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 Configure > Settings > Notification Templates.

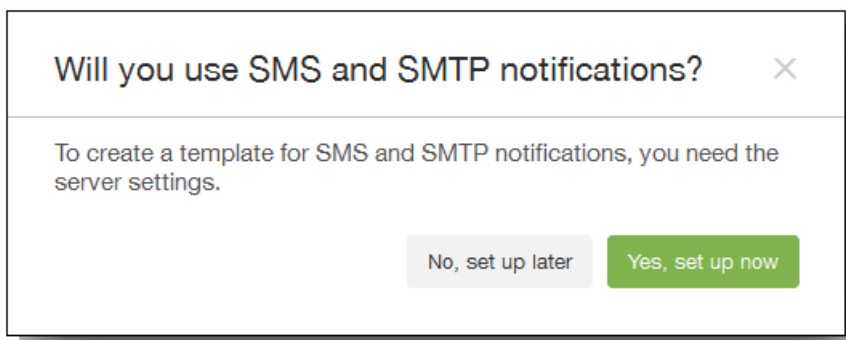


2. Do one of the following:

- Click Add to add a new notification template. 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. For details, see [Notifications in XenMobile](#).

Note: If you choose to set up SMS or SMTP server settings now, you are redirected to the Configure > Settings > Notification Server page. After setting up the channels you want to use, you can return to the Configure > Settings > 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.

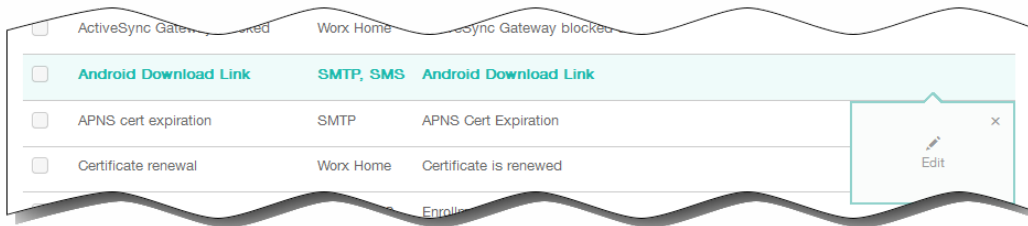


- Select an existing template to edit or delete. Click the option you want to use.

Note:

- You can delete only notification templates that you have added; you cannot delete predefined notification templates.

- When you select the check box next to a notification template, the options menu appears above the notification template list; when you click anywhere else in the list, the options menu appears on the right side of the listing.
- XenMobile includes many predefined notification templates that reflect the distinct types of events that XenMobile automatically responds to for every device in the system.



When you click to add a template, the Add Notification Template page appears.

Add Notification Template

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

Name*

Description

Type Manual sending supported

Channels

Worx Home

Message

Sound File

SMTP ⚠ Channel cannot be activated until you define the SMTP server in the [Notification Server](#) section in Settings.

Sender

Recipient

Subject

Message

SMS ⚠ Channel cannot be activated until you define the SMS server in the [Notification Server](#) section in Settings.

Recipient

Message

3. On the Add Notification Template page (or the Edit Notification Template page if you are editing an existing notification), enter or modify the following information:

1. Name: Type a descriptive name for the template.
2. Description: Type a description for the template.
3. Type: Select the notification type. Only supported channels for the selected type appear.

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 templates that use the following macros in the Subject or Message field on any channel:

- `${outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `${outofcompliance.reason(smgs_block)}`

Attention: Only one APNS Cert Expiration template is allowed, which is a predefined template. This means you cannot add a new template of this type.

4. Channels: Enter or modify 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 SMS, only users using devices with a SIM card receive the notification.
- If you choose SMTP, most users should receive the message because they will have enrolled with their email addresses.

Worx Home

1. Activate: Click to enable the notification channel.
2. Message: Type the message to be sent to the user. This field is required if you are using Worx Home.
3. Sound File: Select the notification sound the user hears when the notification is received.

SMTP

1. Click Activate to enable the notification channel.
Important: You are only able to activate the SMTP notification if you have already set up the SMTP server. For details, see [Notifications in XenMobile](#).
2. Sender: Enter an optional sender for the notification, which can be a name, an email address, or both.
3. 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](#).
4. Subject: Type a descriptive subject for the notification. This field is required if you are using SMTP.
5. Message: Type the message to be sent to the user.

SMS

1. Click Activate to enable the notification channel.
Important: You are only able to activate the SMTP notification if you have already set up the SMTP server. For details, see [Notifications in XenMobile](#).
 2. 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. To send Ad Hoc notifications, you can enter specific recipients, or you can select devices from the Manage > Devices page. For details, see [Adding Devices and Viewing Device Details in XenMobile](#).
 3. Message: Type the message to be sent to the user. This field is required if you are using SMS.
Important: You are only able to activate the SMS notification if you have already set up the SMS gateway. For details, see [Notifications in XenMobile](#).
5. Click Add to add the new template or click Save to save your edits. 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.

Managing Delivery Groups

Feb 13, 2015

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 8.1, and Windows 8.1 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.

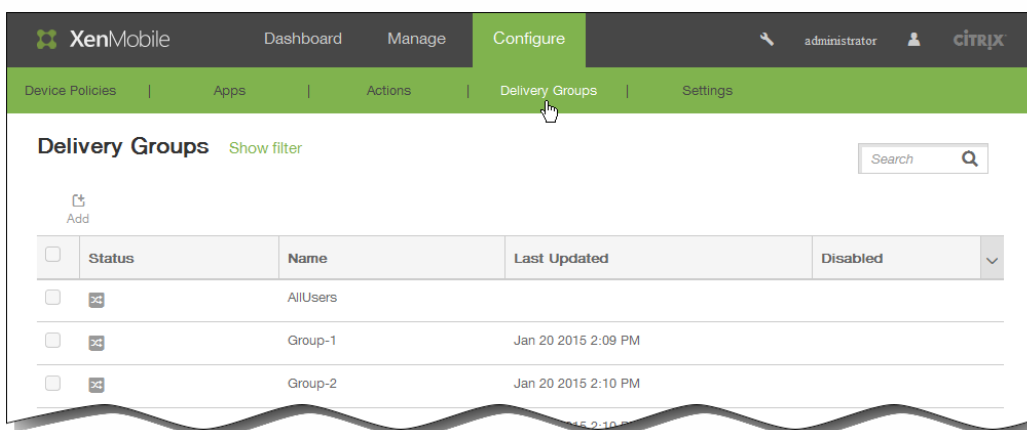
The default AllUsers delivery group is created when you install and configure XenMobile. It contains all local users and Active Directory users. You cannot delete the AllUsers group, but you can disable the group when you do not want to push resources to all users.

You can add, edit, disable, enable, deploy, and delete delivery groups in XenMobile to manage how policies, apps, and actions are deployed to your users. Each of these actions is described in detail in the following sections of this topic:

- [To add a delivery group](#)
- [To edit a delivery group](#)
- [To enable and disable the AllUsers delivery group](#)
- [To deploy delivery groups](#)
- [To delete delivery groups](#)

To begin managing your delivery groups, open the Delivery Groups page as follows:

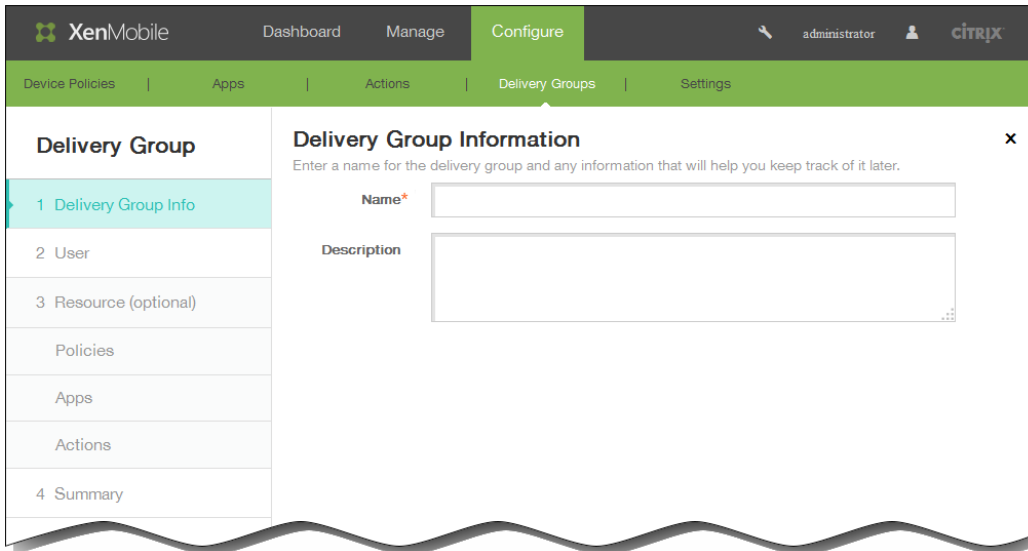
1. In the XenMobile console, click Configure > Delivery Groups.



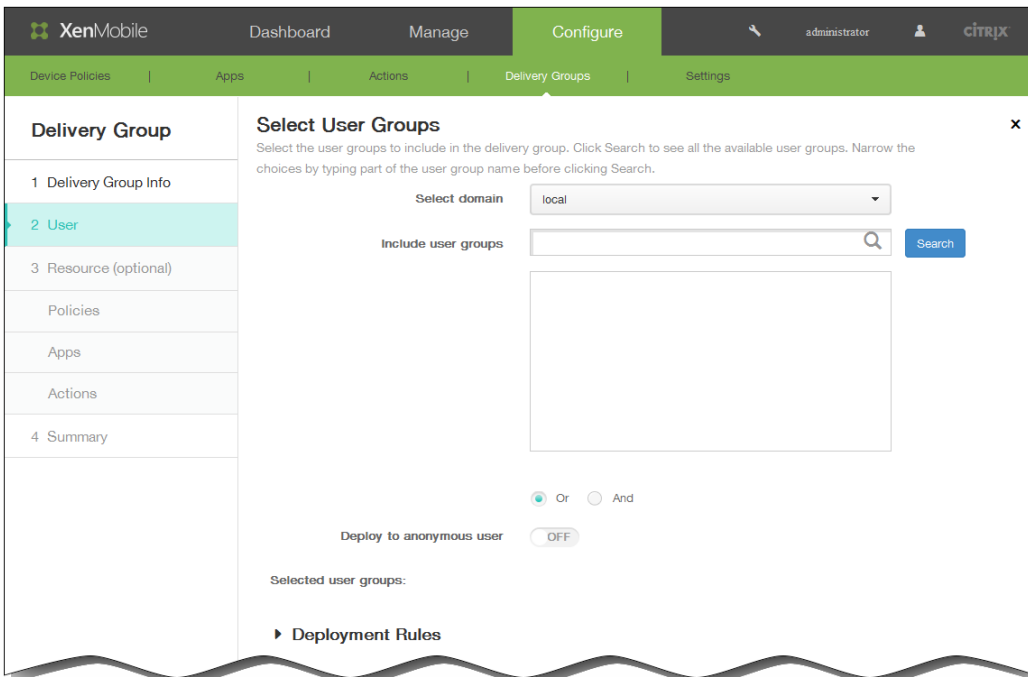
The Delivery Groups page appears. Then, refer to the specific eDocs topic for the action you want to take.

To add a delivery group

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

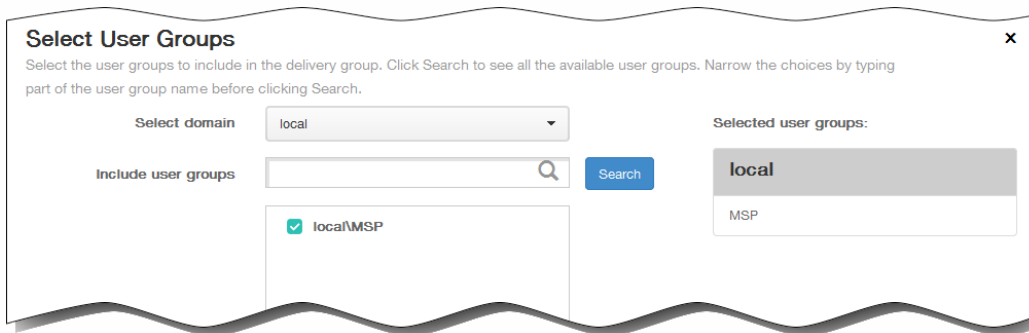


2. In the Delivery Group Information pane, enter the following information:
 1. Name: Type a descriptive name for the delivery group.
 2. Description: Type an optional description of the delivery group.
3. Click Next. The Delivery Group User page appears.



4. In the Select User Groups pane, enter the following information:
 1. Select domain: From the list, select the domain from which to choose users.
 2. Include user groups: Do one of the following:
 - 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.

3. In the list of user groups, click the groups you want to add. The selected groups appear in the Selected user groups list.



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

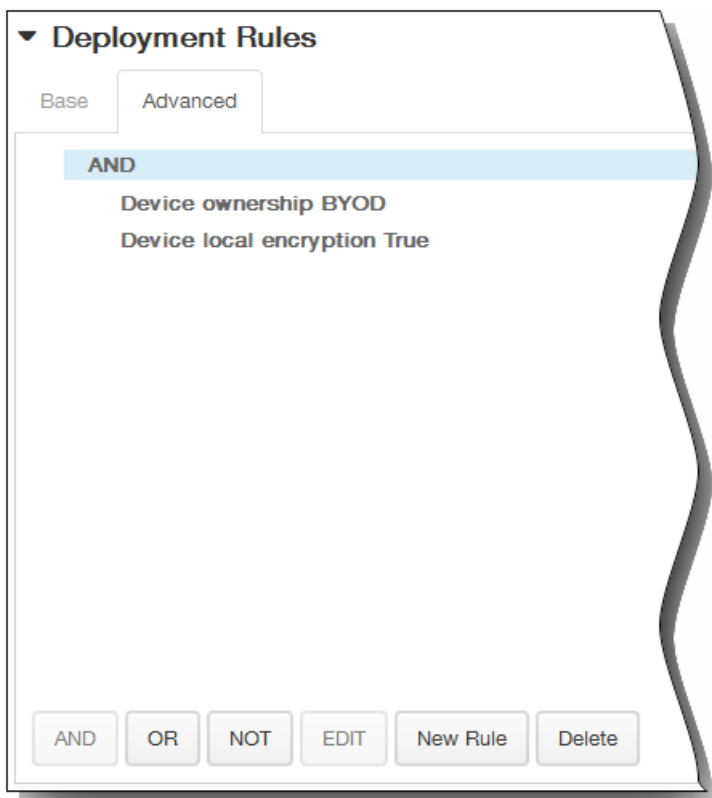
- Click Search to see a list of all user groups in the selected domain.
- Type a full or partial group name in the search box, and then click Search to limit the list of user groups.

User groups in the Selected user groups list have check marks next to their name in the resulting list. Scroll through the list and clear the check box next to each group you want to remove.

4. 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.
5. Deploy to anonymous user: Select whether to deploy to unauthenticated users in the delivery group.
Note: Unauthenticated users are users whom you were not able to authenticate, but you allowed their devices to connect to XenMobile anyway.
5. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.

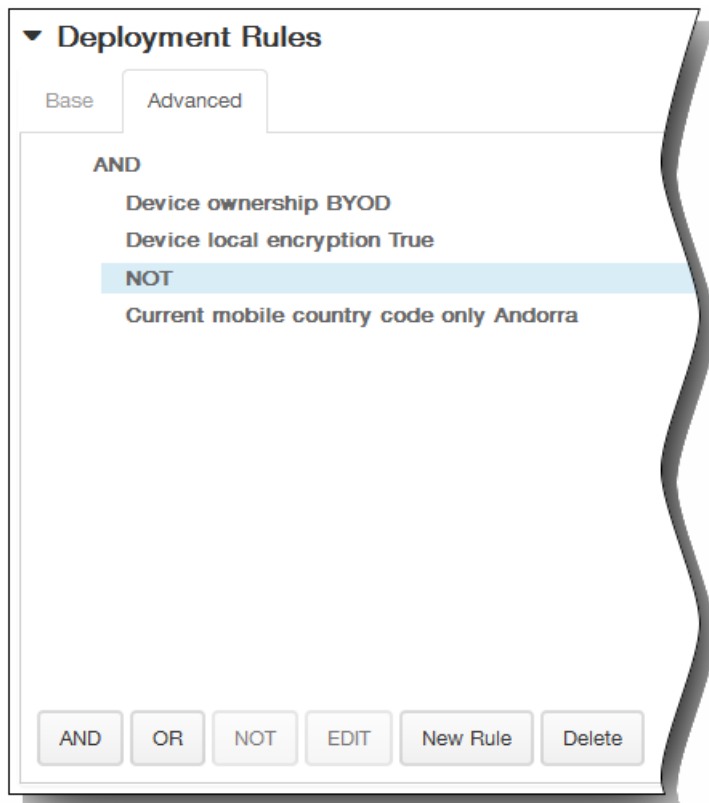
1. Click AND, OR, or NOT.

2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

3. Click New Rule again if you want to add more conditions.

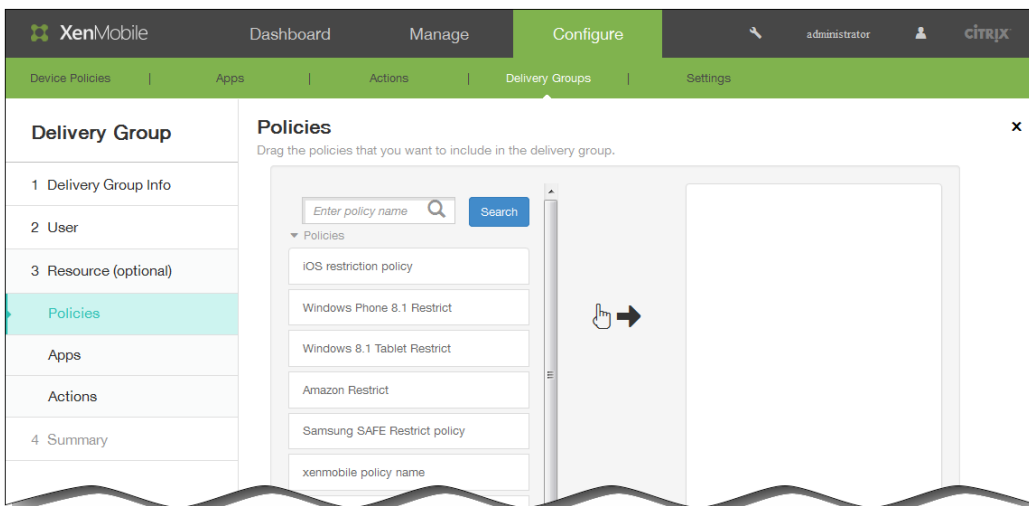
In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



- Click Next. The Delivery Group Resources page appears. You optionally add policies, apps, or actions for the delivery group here. To skip this step, under Delivery Group, click Summary to see a summary the delivery group configuration; otherwise, do the following:

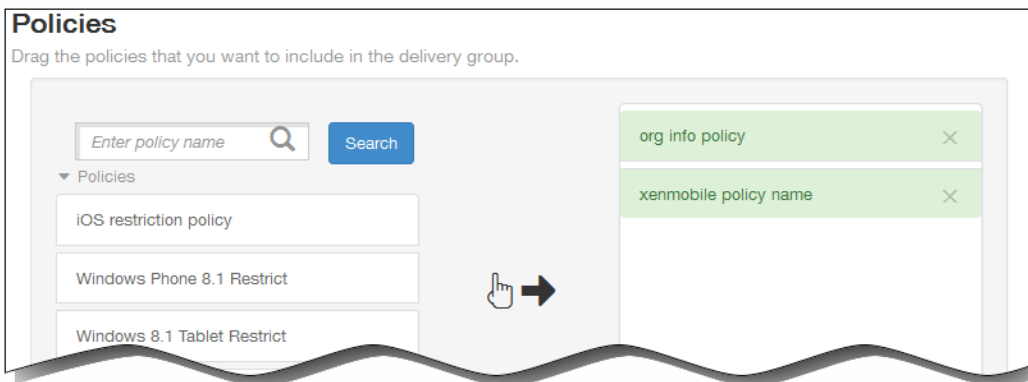
Note: To skip a resource, under Resources (optional) click the resource you want to add and follow the steps for that resource.

To add policies



- 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 a policy and drag it into the right-hand box.

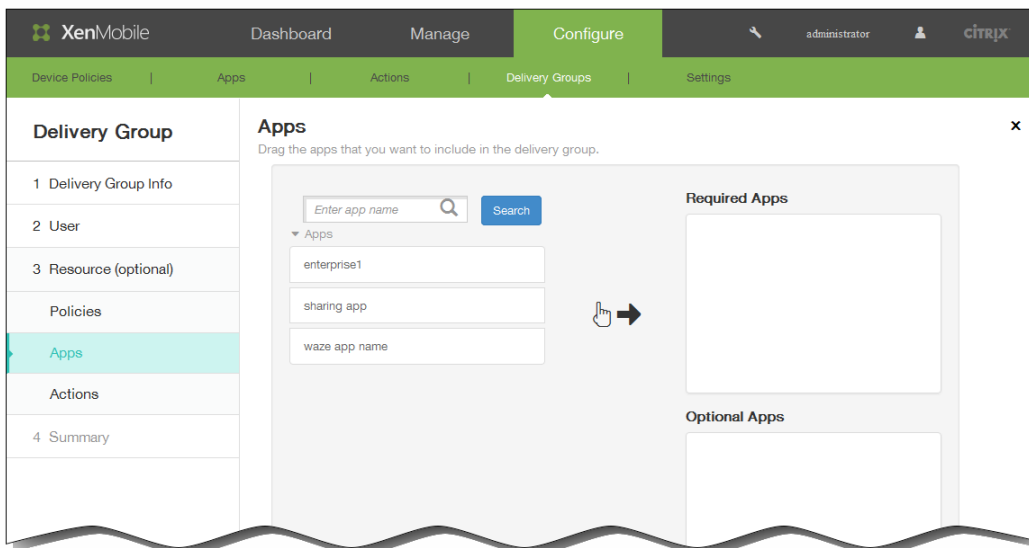
3. Repeat steps a and b to add more policies.



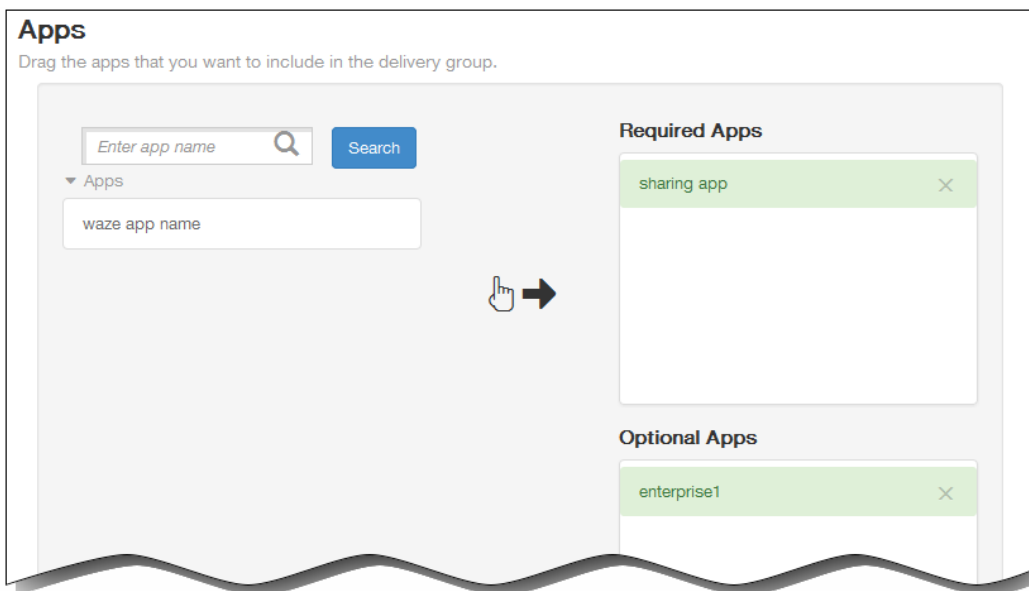
To remove a policy resource, click the X next to the policy name.

4. Click Next to move to the Apps resource page. If you are not adding more resources, under Delivery Group, click Summary. Either the Apps resource page appears or the Summary page appears.

To add Apps



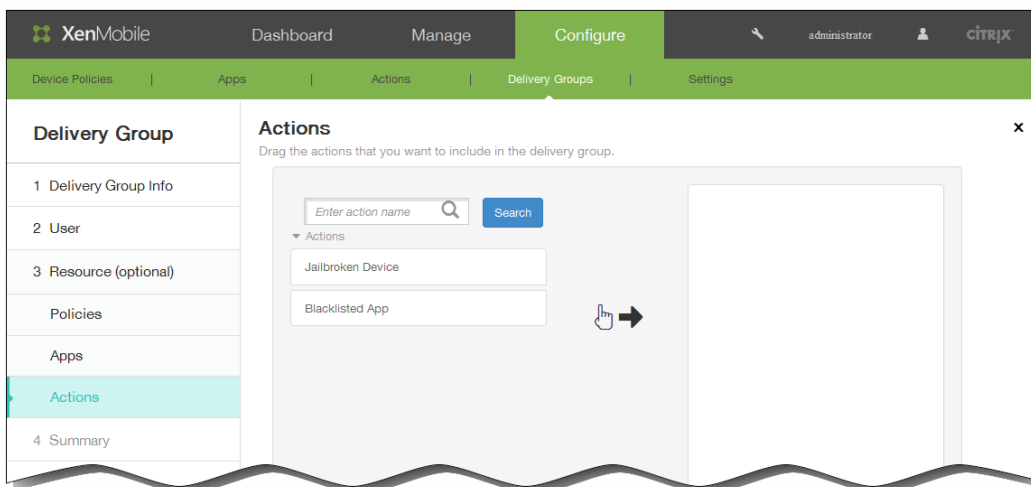
1. Scroll through the list of available apps to find the app you want to add, or to limit the list of apps, type a full or partial app name in the search box and then click Search.
2. Click an app and drag it into either the Required Apps box or the Optional Apps box.
3. Repeat steps a and b to add more apps.



To remove an app resource, click the X next to the app name.

4. Click Next to move to the Actions resource page. If you are not adding more resources, under Delivery Group, click Summary. Either the Actions resource page appears or the Summary page appears.

To add Actions

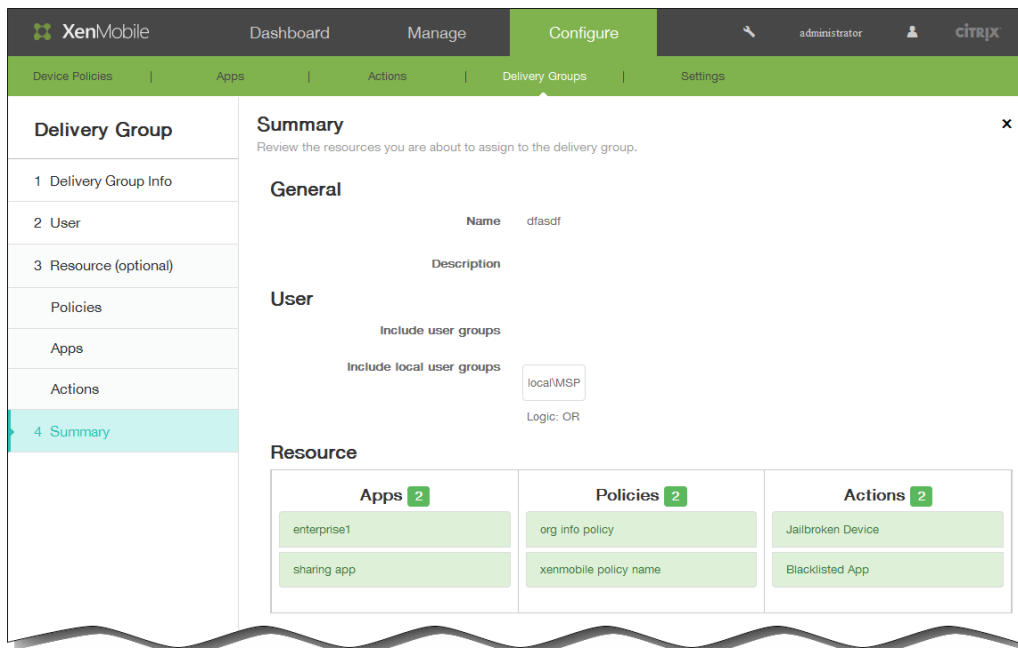


1. Scroll through the list of available actions to find the action you want to add, or to limit the list of actions, type a full or partial action name in the search box and then click Search.
2. Click an action and drag it into the right-hand box.
3. Repeat steps a and b to add more actions.



To remove an action resource, click the X next to the action name.

4. Click Next. The Summary page appears.

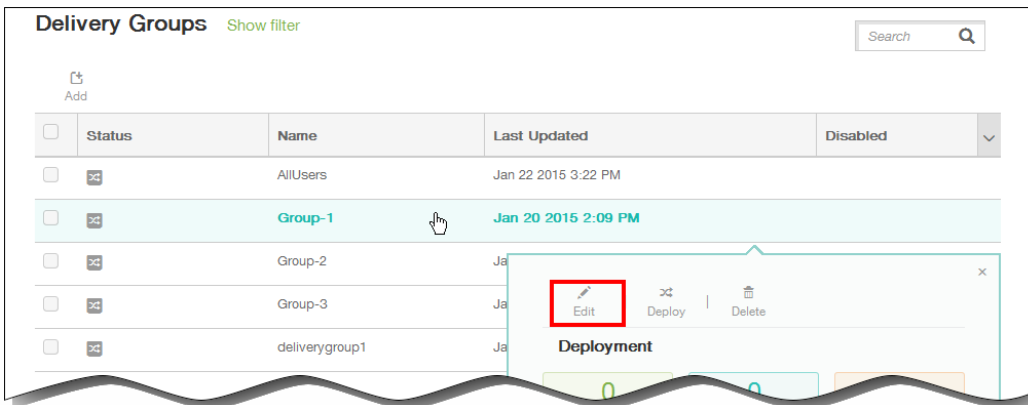
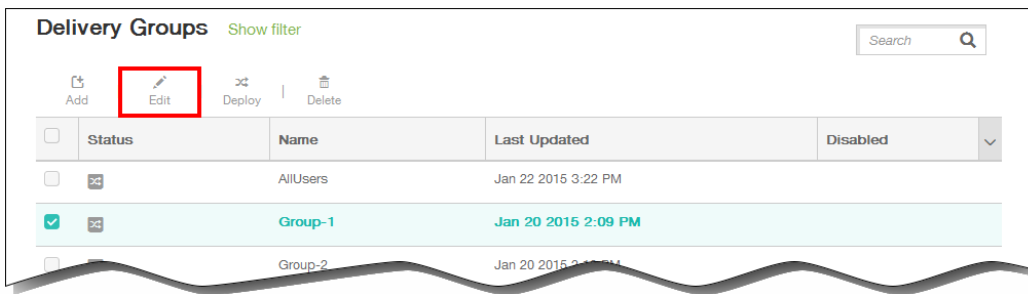


7. On the Summary page, review the options you have configured for the delivery group. Click Back to return to previous pages to make any necessary adjustments to the configuration.
8. Click Save to save the delivery group.

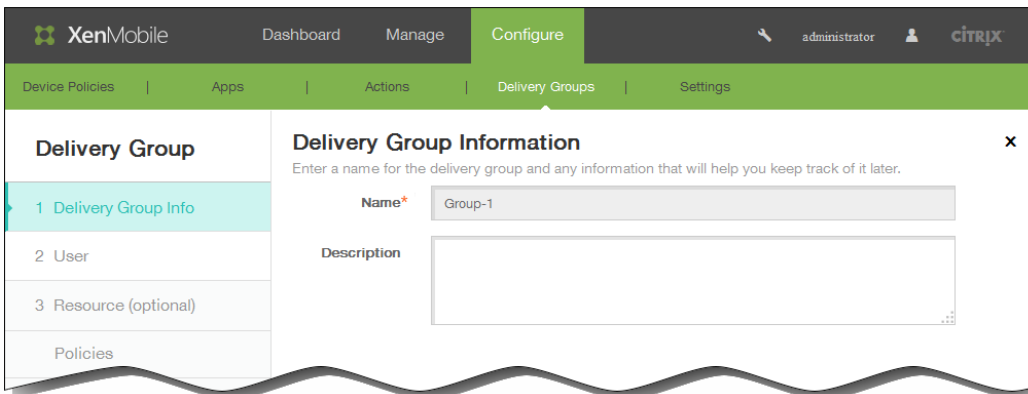
To edit a delivery group

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.
2. Click Edit.

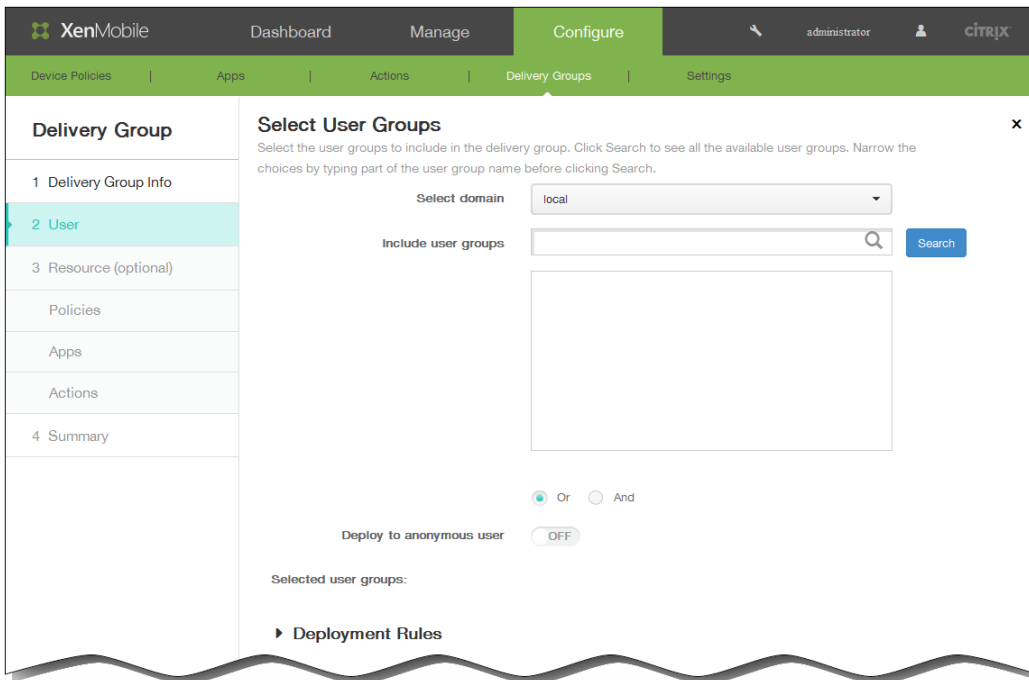
Note: Depending on how you selected the delivery group, the Edit command appears above or to the right of the delivery group.



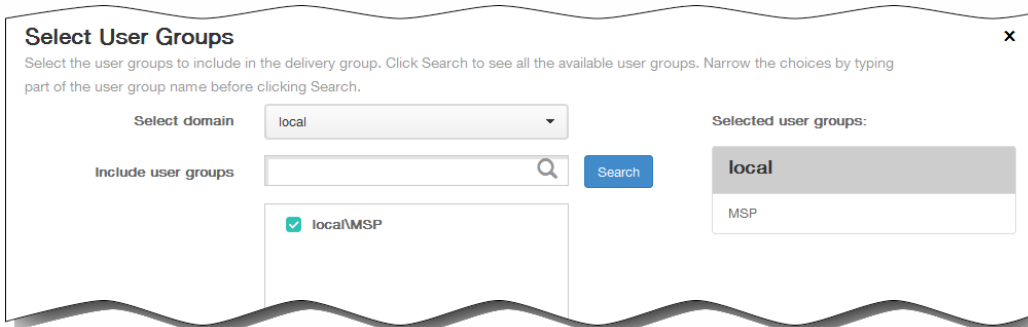
The Delivery Group Information edit page appears.



3. Add or change the Description.
Note: You cannot change the name of an existing group.
4. Click Next. The Select User Groups page appears.



5. In the Select User Groups pane, enter or change the following information:
 1. Select domain: In the list, select the domain from which to choose users.
 2. Include user groups: Do one of the following:
 - 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.
 3. In the list of user groups, click the groups you want to add. The selected groups appear in the Selected user groups list.



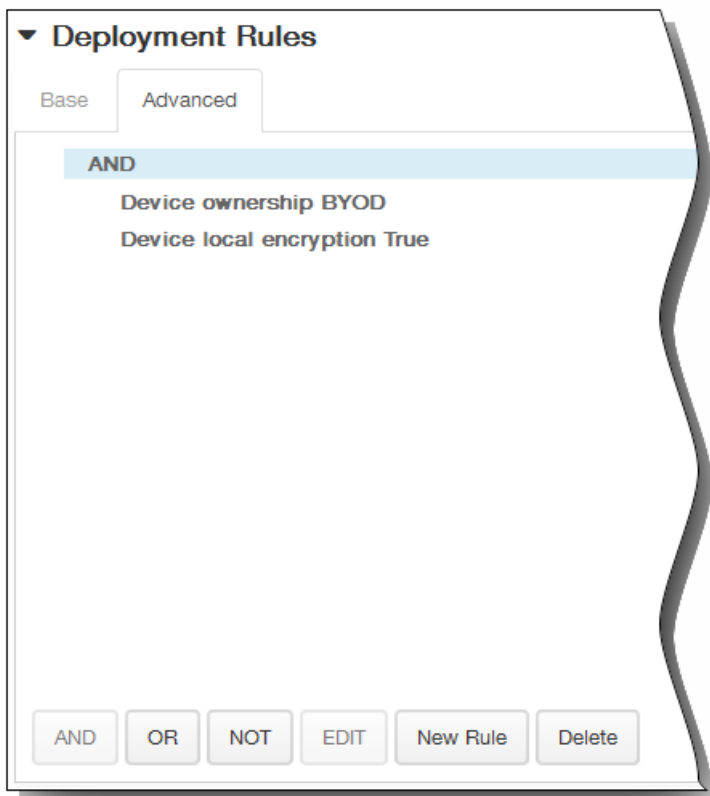
Note: To remove user groups, click Search, and then in the list of user groups, clear the check box next to the group or groups you want to remove. You can type a full or partial group name in the search box and then click Search to limit the number of user groups displayed in the list.

4. Or/And: Select whether users may be in any group (Or) or whether they must be in all groups (And) for deployment.
5. 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.
6. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

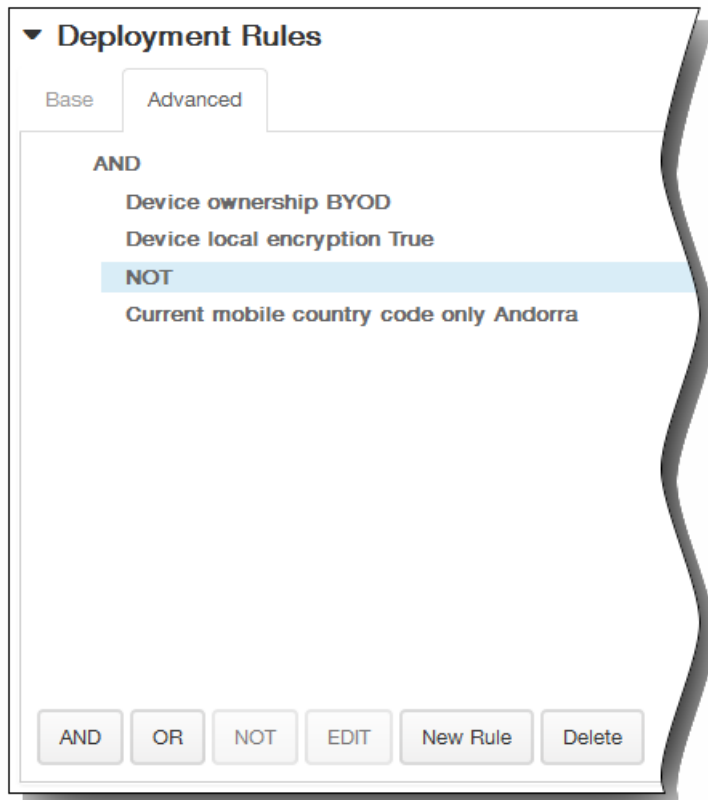


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

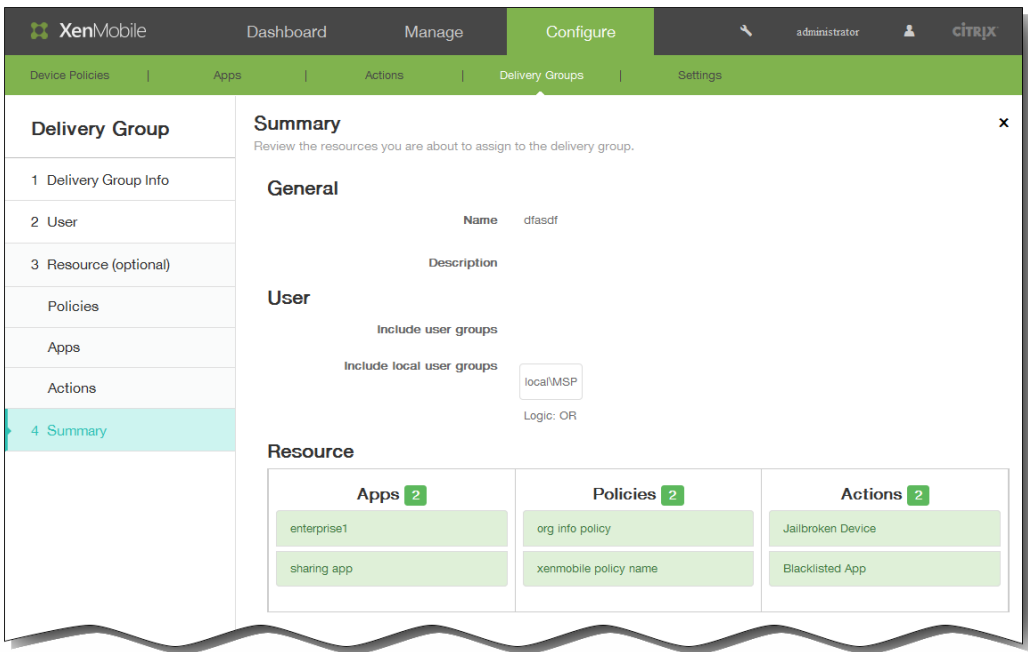
3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



7. 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. When you are done modifying a resource, click Next or under Delivery Group, click Summary.

Either the next resource page appears or the Summary page appears.



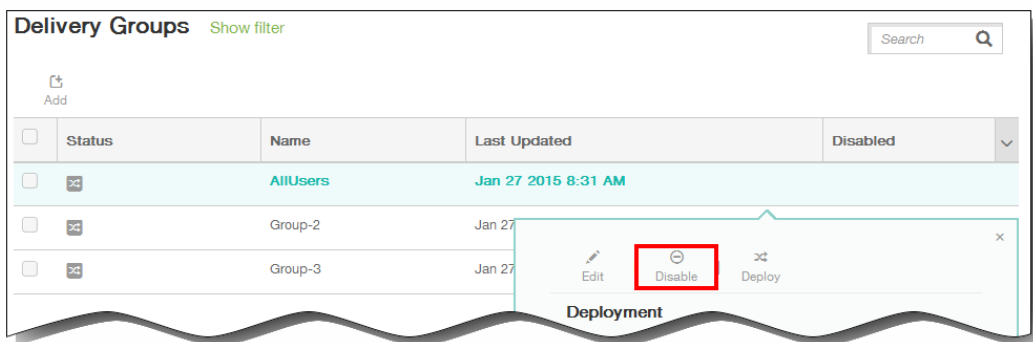
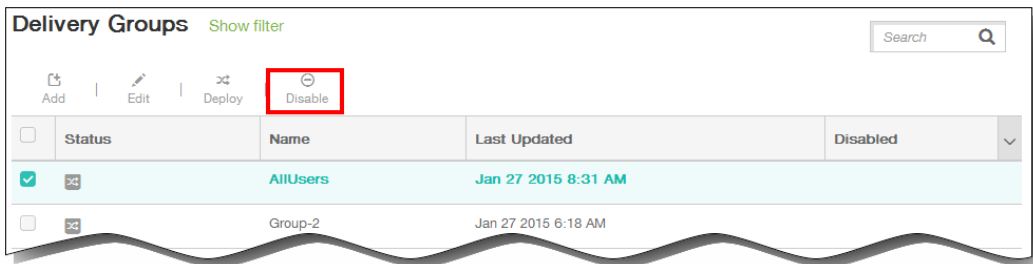
8. On the Summary page, review the changes you have made. Click Back to return to previous pages to make any necessary adjustments to the configuration.
9. Click Save to save your changes.

To enable and disable the AllUsers delivery group

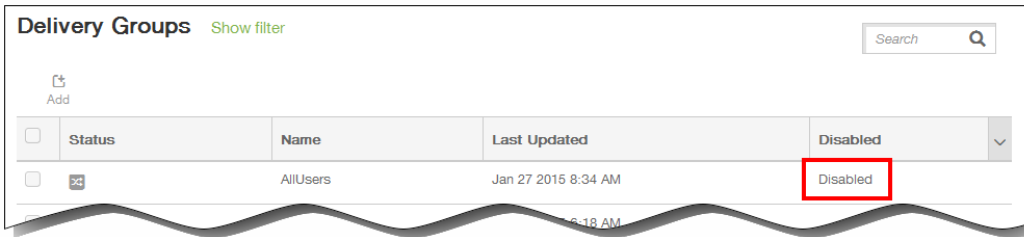
Note: AllUsers is the only delivery group that you can enable or disable.

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.

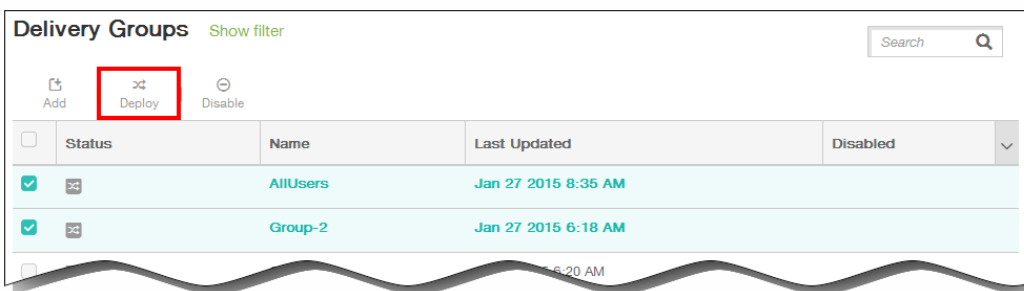
To deploy delivery groups

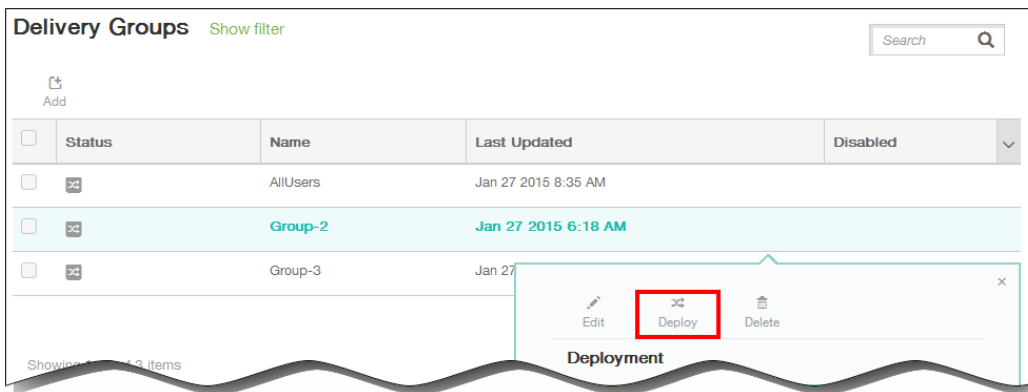
Deploying to a delivery group means sending a push notification to all users with iOS, Windows Phone 8.1, and Windows 8.1 tablet devices who belong to the delivery group to reconnect to XenMobile, so that you can reevaluate the devices and deploy apps, policies, and actions; users with other platform devices receive the resources immediately if they are already connected or, based on their scheduling policy, the next time they connect.

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.

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.



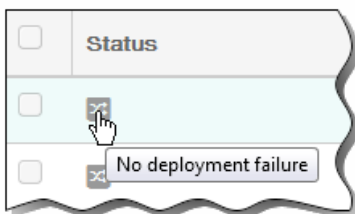


The Deploy Devices dialog box appears.

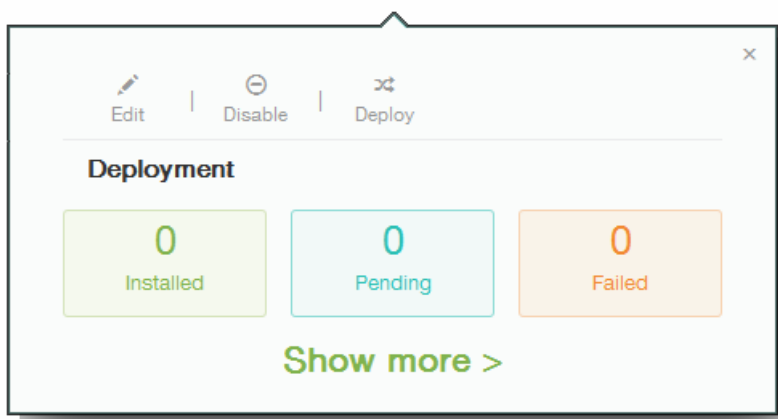
3. Verify that the groups to which you want to deploy apps, policies, and actions are listed and then click Deploy. The apps, policies, and actions are deployed to the selected groups based on device platform and scheduling policy.

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.



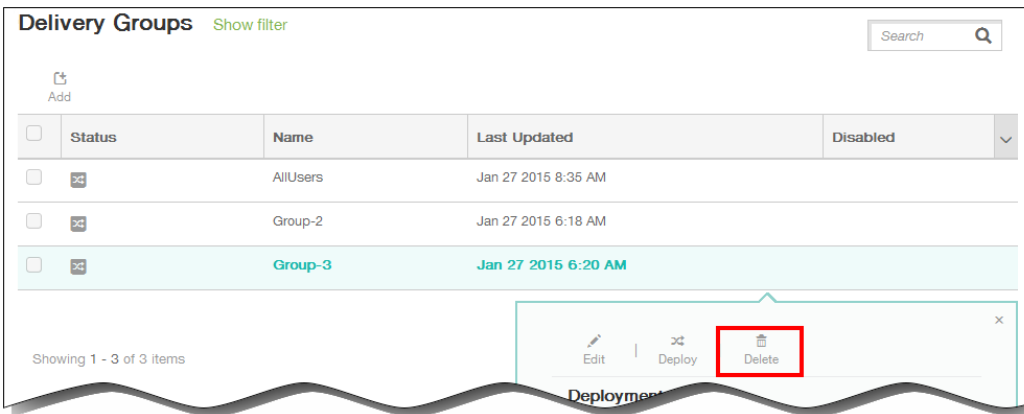
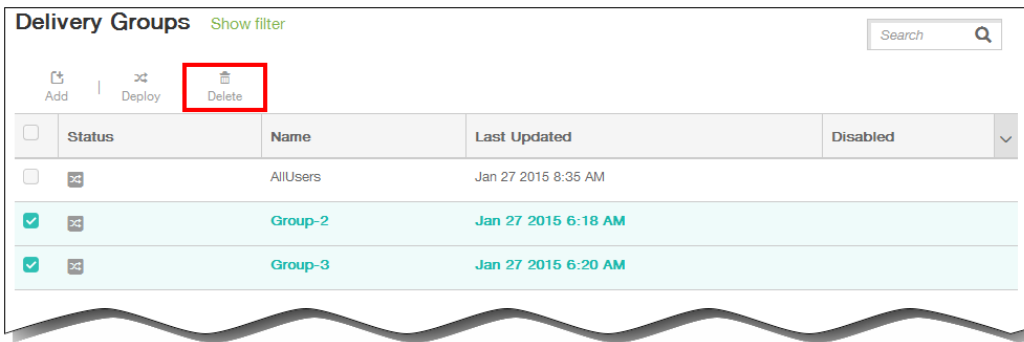
To delete delivery groups

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



- The Delete dialog box appears.
3. Click Delete on the Delete dialog box.
Important: You cannot undo this action.

Enrolling Users and Devices

Mar 09, 2015

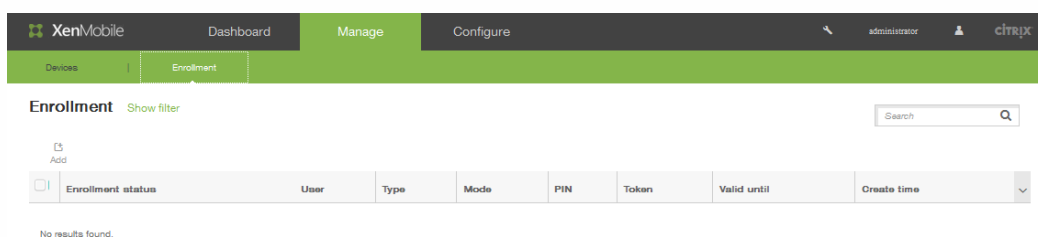
In order to manage user devices remotely and securely, user devices need to be enrolled in XenMobile. The XenMobile client software is installed on the user device and the user's identity is authenticated, and then XenMobile and the user's profile is installed. After the devices are enrolled, in the XenMobile console, you can perform device management tasks, such as applying policies, deploying apps, pushing data to the device, locking, wiping, and locating lost or stolen devices.

To enroll users, you must first add users to XenMobile, if you have not yet established an Active Directory connection. The topics in this section describe the subsequent required steps for enrolling users:

- [Configure enrollment modes \(Default, SHP\).](#)
- [Configure notification servers \(SMTP and SMS\).](#)
- [Configure the enrollment notification template.](#)
- [Send enrollment notification.](#)

Note: Before you can enroll iOS device users, you need to request an APNs certificate. See [Certificates in XenMobile](#) for more information.

You access configuration options for users and devices in the XenMobile console by clicking **Manage > Enrollment**:



Android Devices

Feb 06, 2015

1. Go to the Google Play or Amazon App store on your Android device, download the Citrix Worx Home app and then tap the app.
2. When prompted to install the app, click Next and then click Install.
3. After Worx Home installs, tap Open.
4. Enter your corporate credentials, such as the organization's XenMobile server name, User Principal Name (UPN), or email address and then click Next.
5. In the Activate device administrator screen, tap Activate.
6. Enter your corporate password and then tap Sign On.
7. Depending on the way XenMobile is configured, you may be asked to create a Worx PIN, which you can use to sign on to Worx Home and other Worx-enabled apps, such as WorxMail, WorxWeb, ShareFile, and more. On the Create Worx PIN screen, enter a PIN consisting of any series of six numbers.
8. Reenter the PIN.

You are now enrolled with your Android device. Tap the Worx Store to access your corporate app store, as well as Worx-enabled apps, such as WorxMail, WorxWeb, ShareFile, and more.

To un-enroll and re-enroll an Android device

Updated: 2015-02-12

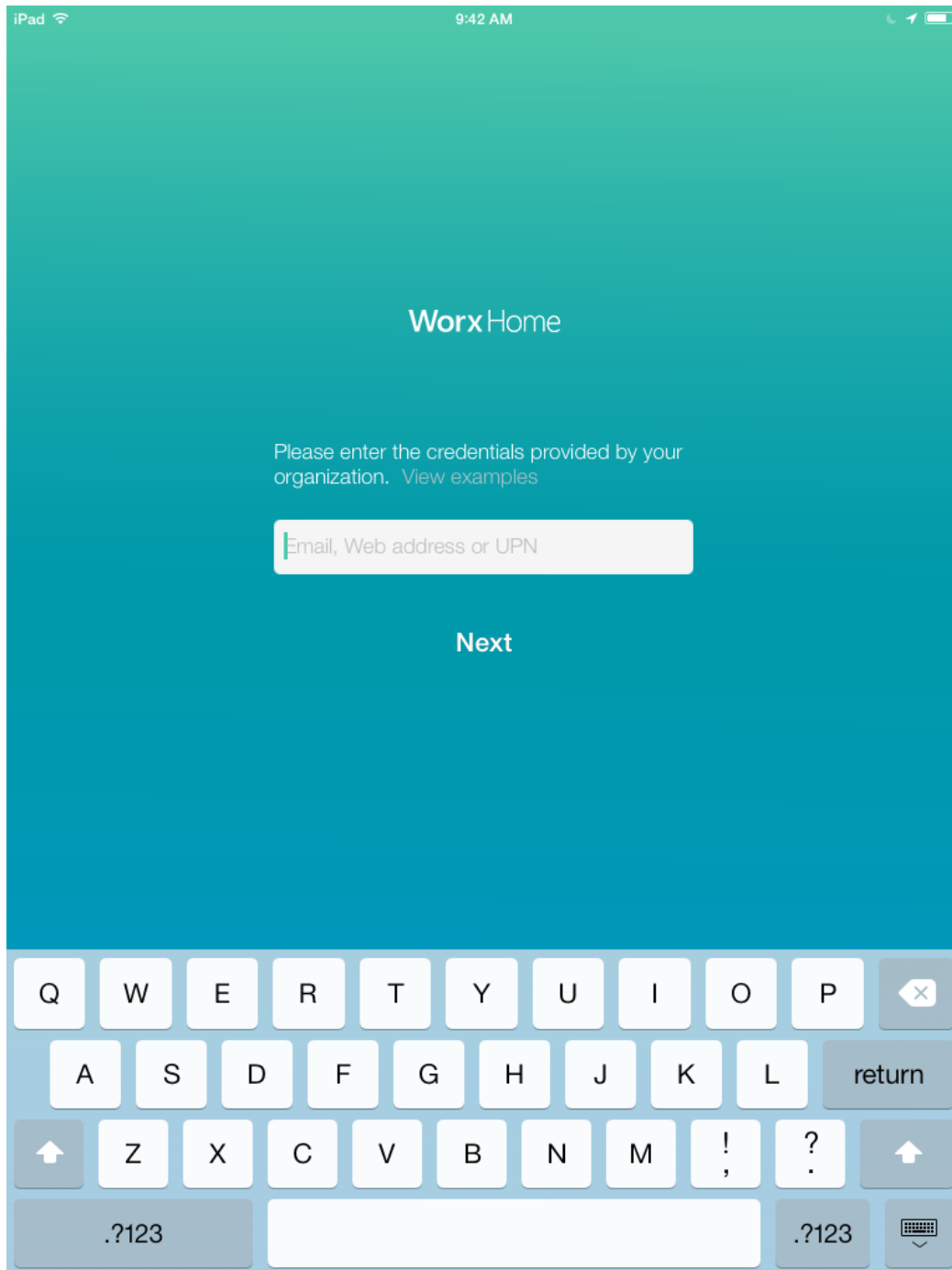
Before a device is re-enrolled, the device is first un-enrolled. During the period in which the device is un-enrolled, but not yet re-enrolled, the device is not managed by XenMobile, although it continues to appear in the device inventory list in the XenMobile console. You cannot track the device and cannot monitor the device compliance when the device is not being managed by XenMobile.

1. Tap to open the Worx Home app.
2. Tap the Settings icon in the upper-left of the app window.
3. Tap Re-Enroll. A message appears to confirm you want to re-enroll your device.
4. Tap OK. This causes your device to be un-enrolled.
5. Follow the on-screen instructions to re-enroll your device.

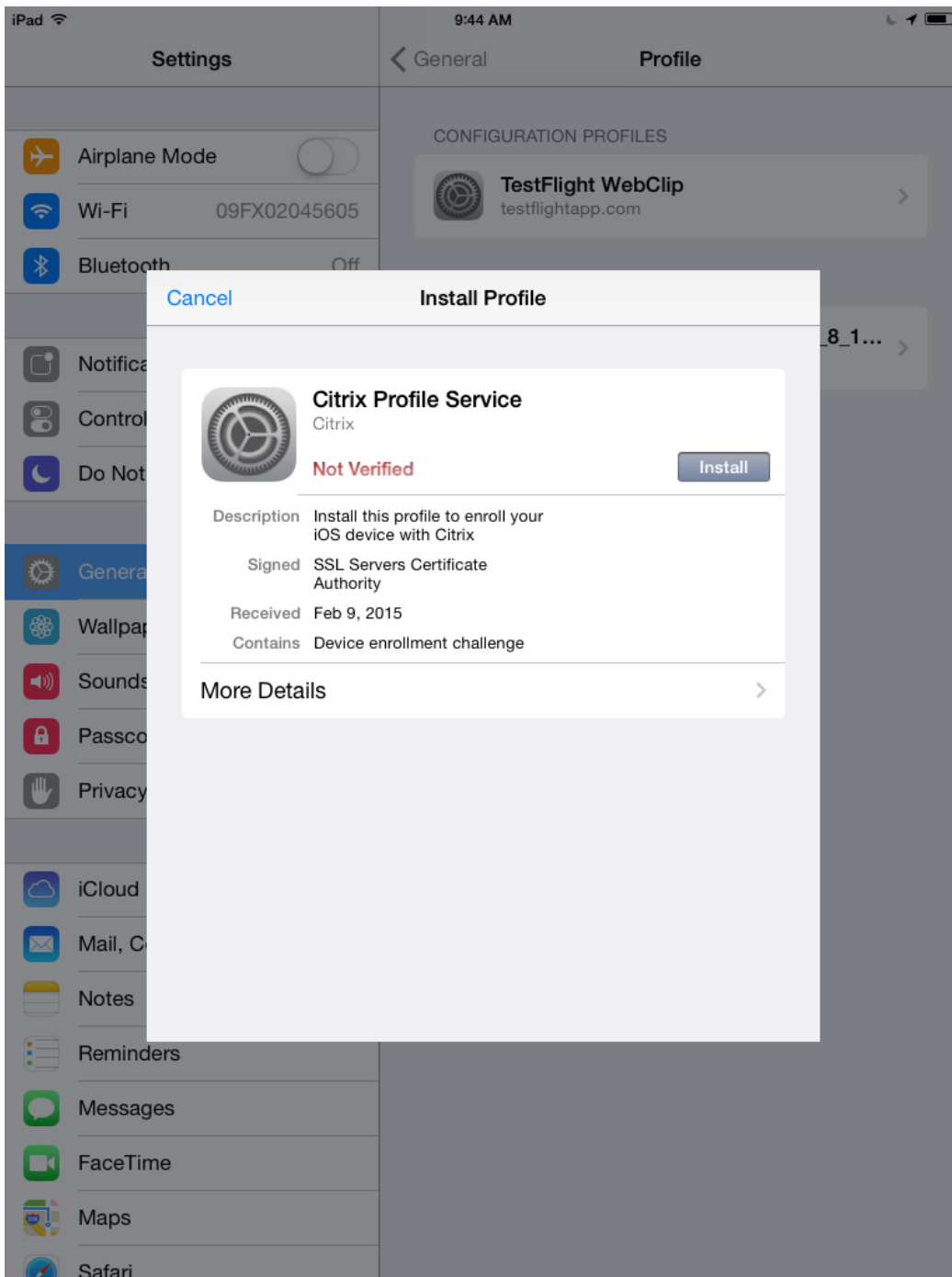
iOS Devices

Feb 13, 2015

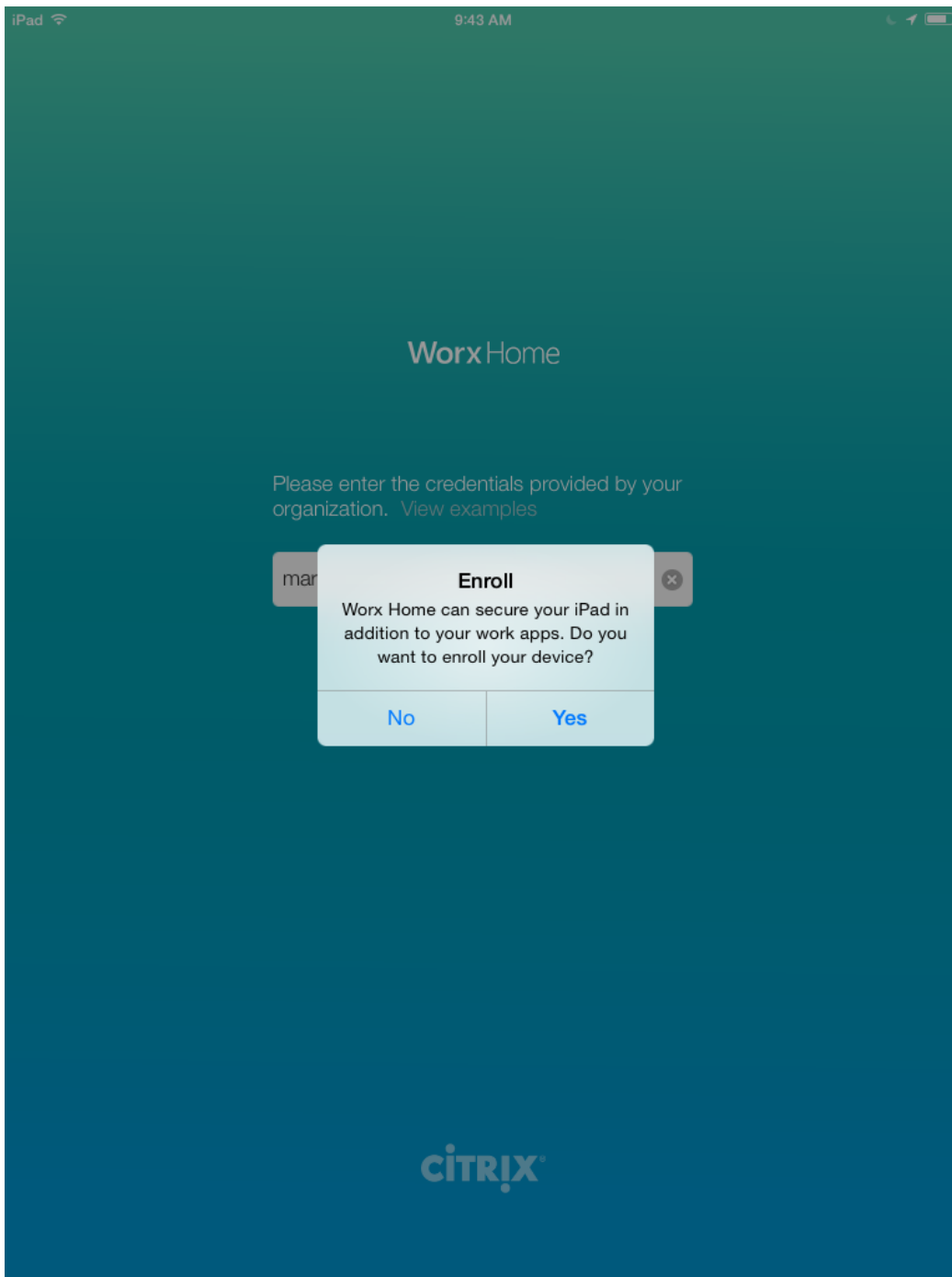
1. Download the Worx Home app from the Apple iTunes App Store on the device and then install the app on the device.
2. On the iOS device Home screen, tap the Worx Home app.
3. When the Worx Home app opens, enter your corporate credentials, such as the name of your company's XenMobile server name, User Principal Name (UPN) or your email and then click Next.



4. Type your user name and password. A browser opens to begin the enrollment process.
5. Tap Install to install the Citrix Profile Services.



6. Tap Install Now if prompted with a warning message.
7. If your device is configured with a passcode, you will be prompted to enter your passcode to install the profile.
8. Tap Install.
9. When the profile installation finishes, tap Done to complete the Company profile installation process.
10. When Worx Home appears, tap Yes to allow Worx Home to use your current location.



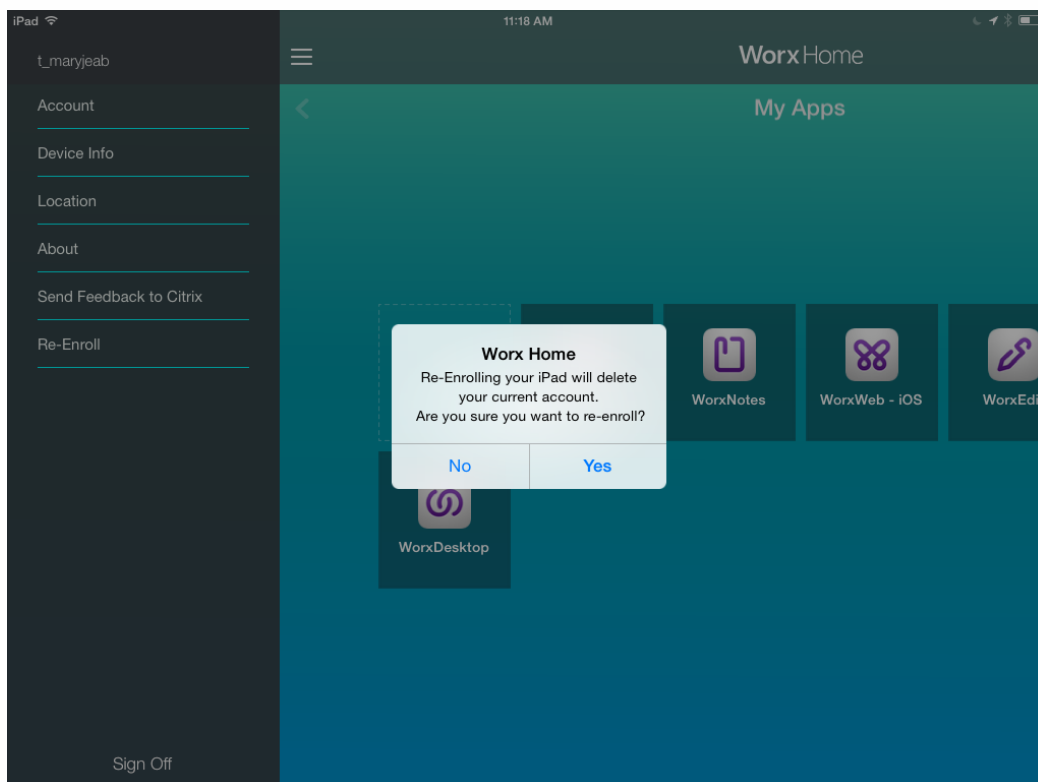
11. Depending on the way XenMobile is configured, you may be asked to create a Worx PIN, which you can use to sign on to Worx Home and other Worx-enabled apps, such as WorxMail, WorxWeb, ShareFile, and more. You will need to enter your Worx PIN twice. Worx Home opens. You can then access the Worx Store to view the apps you can install on your iOS device.
12. Tap Worx Store to open the enterprise app store.
13. If you configured XenMobile to automatically push apps to your users' devices after enrollment, messages appear prompting them to install the apps. Tap Install to install the apps.

To re-enroll an iOS device

Updated: 2015-02-13

When a device is re-enrolled, the device is first un-enrolled. During the period in which the device is un-enrolled but not yet re-enrolled, the device is not managed by XenMobile, although it continues to appear in the device inventory list in the XenMobile console. You cannot track the device or monitor the device compliance when the device is not being managed by XenMobile.

1. Tap to open the Worx Home app.
2. Tap the Settings icon in the upper-left of the app window.
3. Tap Re-enroll. A message appears to confirm you want to re-enroll your device.



4. Tap Yes. This causes the device to be un-enrolled.
5. Follow the on-screen instructions to re-enroll the device.

Enrolling Windows devices in XenMobile

Mar 07, 2016

XenMobile supports the enrollment of devices running the following Windows operating systems:

- Windows
- Windows Phone

Windows and Windows Phone users enroll directly through their devices.

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

Note

In order for Windows devices to enroll, the SSL listener certificate must be a public certificate. Enrollment fails if you've uploaded a self-signed SSL certificate

To enroll Windows 8.1 devices with autodiscovery

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

1. On the device, check for and install all available Windows Updates. This step is particularly important when upgrading from Windows 8 to Windows 8.1, because users may not be automatically notified of all available updates.
2. In the charms menu, tap Settings and then tap PC Settings > Network > Workplace.
3. Enter your corporate email address and then tap Turn on. To enroll as a local user, enter a non-existent email address with the correct domain name (for example, foo@mydomain.com). This permits you to bypass a known Microsoft limitation; in the Connecting to a service dialog box, enter the user name and password associated with the local user. The device automatically discovers a XenMobile server and starts the enrollment process.
4. Enter your password. Use the password associated with an account that is part of a user group in XenMobile.
5. In the Allow apps and services from IT admin dialog box, indicate that you agree to have your device managed and then tap Turn on.

To enroll Windows 8.1 devices without autodiscovery

It is possible to enroll Windows 8.1 devices without autodiscovery. Citrix, however, recommends that you configure autodiscovery. Because enrollment without autodiscovery results in a call to port 80 before connecting to the desired URL, it is not considered best practice for production deployment. Citrix recommends that you use this process only in test environments and proof of concept deployment.

1. On the device, check for and install all available Windows Updates. This step is particularly important when upgrading from Windows 8 to Windows 8.1, because users may not be automatically notified of all available updates.
2. In the charms menu, tap Settings and then tap PC Settings > Network > Workplace.
3. Enter your corporate email address.
4. If Automatically detect server address is on, tap to turn it off.

5. In the Enter server address field, type the server address in the following format:
`https://serverfqdn:8443/serverInstance/Discovery.svc` If a port other than 8443 is used for unauthenticated SSL connections, use that port number in place of 8443 in this address.
6. Enter your password.
7. In the Allow apps and services from IT admin dialog box, indicate that you agree to have your device managed and then tap Turn on.

To enroll Windows Phone 8.1 devices

Updated: 2015-02-11

To enroll Windows Phone 8.1 devices in XenMobile, users need their Active Directory or internal network email address, and password. If autodiscovery is not set up, users also need the server web address for the XenMobile server. Then, they follow this procedure on their devices to enroll.

Note: If you plan to deploy apps through the Windows Phone company store, before your users enroll, make sure that you have configured an Enterprise Hub policy (with a signed Citrix Worx Home, Windows Phone 8.x app).

1. On the main screen of the Windows 8.1 phone, tap the Settings icon.
2. Tap workplace.
3. On the workplace screen, tap add account.
4. On the next screen, enter an email address and password and then tap sign in. If autodiscovery is configured for your domain, the information requested in the next several steps is automatically populated. Proceed to Step 8. If autodiscovery is not configured for your domain, continue with the next step. To enroll as a local user, enter a non-existent email address with the correct domain name (for example, foo@mydomain.com). This permits you to bypass a known Microsoft limitation; in the Connecting to a service dialog box, enter the user name and password associated with the local user.
5. On the next screen, type the web address of the XenMobile server, such as: `https://<xenmobile_server>:<portnumber>/<instancename>/wpe`. For example, `https://mycompany.mdm.com:8443/zdm/wpe`. **Note:** The port number has to be adapted to your implementation, but should be the same port that you used for an iOS enrollment.
6. Enter the user name and domain if authentication is validated through a user name and domain and then tap sign in.
7. If a screen appears noting a problem with the certificate, the error is due to the use of a self-signed certificate. If the server is trusted, tap continue. Otherwise, tap Cancel.
8. When the account is added, you have the option of selecting Install company app. If your administrator has configured a Company App store, select this option and then tap done. If you clear this option, in order to receive the Company app store, you will need to reenroll.
9. On the Account Added screen, tap done.
10. To force a connection to the server, tap the refresh icon. If the device does not manually connect to the server, XenMobile attempts to reconnect. XenMobile connects to the device every 3 minutes 5 successive times, then every 2 hours afterwards. You can alter this connection rate in the Windows WNS Heartbeat Interval located in Server properties. Once enrollment is complete, Worx Home enrolls in the background. No indicator appears when the installation is complete. Open Worx Home from the All Apps screen.

Symbian Devices

Feb 16, 2015

1. Browse to the XenMobile web address for your organization. The web address is in the following format:

`https://<zdmServerName>.domain.com/<zdmInstanceName>/setup`

Note: You can use HTTPS prefix only if you have a certificate issued by a trusted authority, such as Thawte or VeriSign.

2. On the Install screen, tap OK.

3. Tap Phone Memory as the location where the XenMobile agent installs.

4. When the installation is complete, tap Yes to open XenMobile.

5. On the Security Details screen, tap OK to allow XenMobile to access the phone.

6. Enter the first four numbers of the server code as 2831 and then tap OK.

7. On the Control Request Accepted screen, tap OK.

8. Enter the user name and password, server name, port, and instance name for the XenMobile server and then tap OK. The connection information appears.

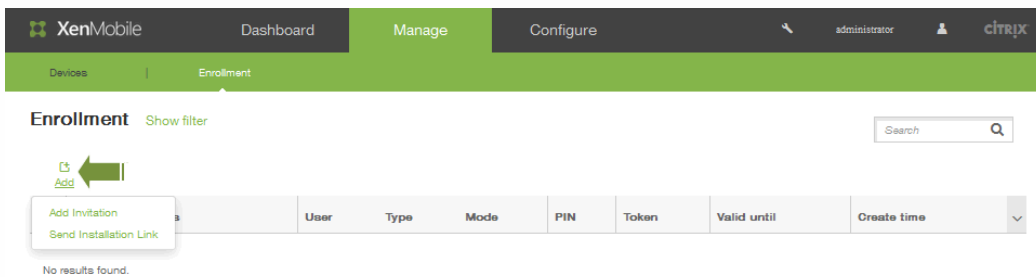
9. Tap Options to review server connection details and then tap Close to finish the setup.

Sending an enrollment invitation in XenMobile

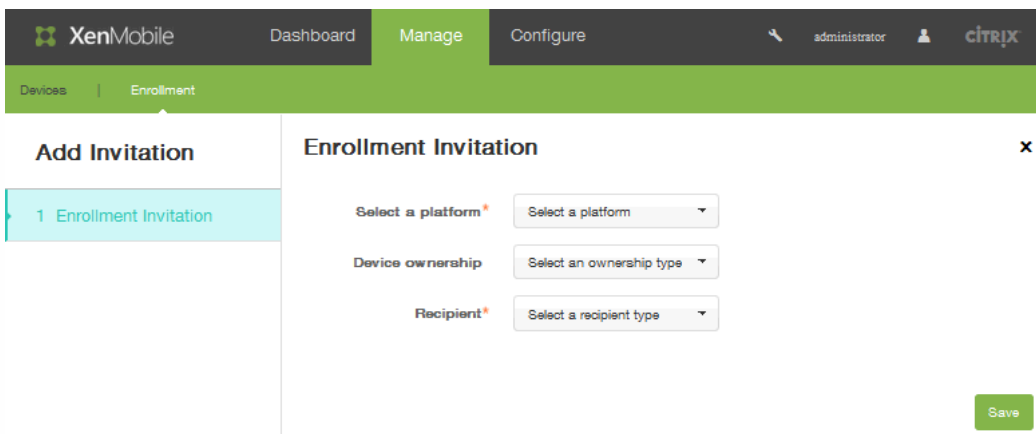
Mar 01, 2016

In the XenMobile console, you can send an enrollment invitation to users with iOS and Android devices.

1. In the XenMobile console, click Manage > Enrollment.
2. On the Enrollment screen, click Add. A menu appears listing options to add an invitation or send an installation link.



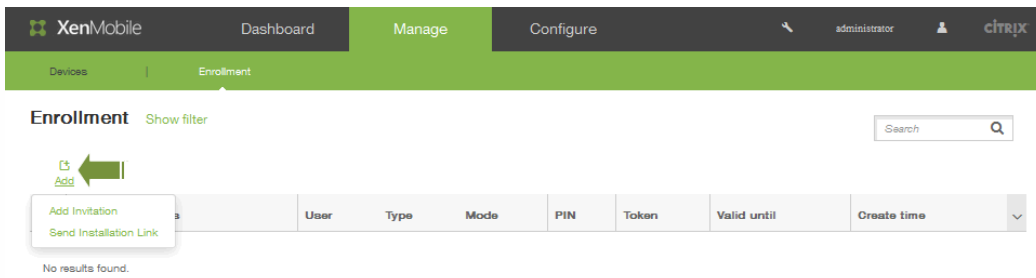
3. Click Add Invitation. The Enrollment Invitation screen appears.



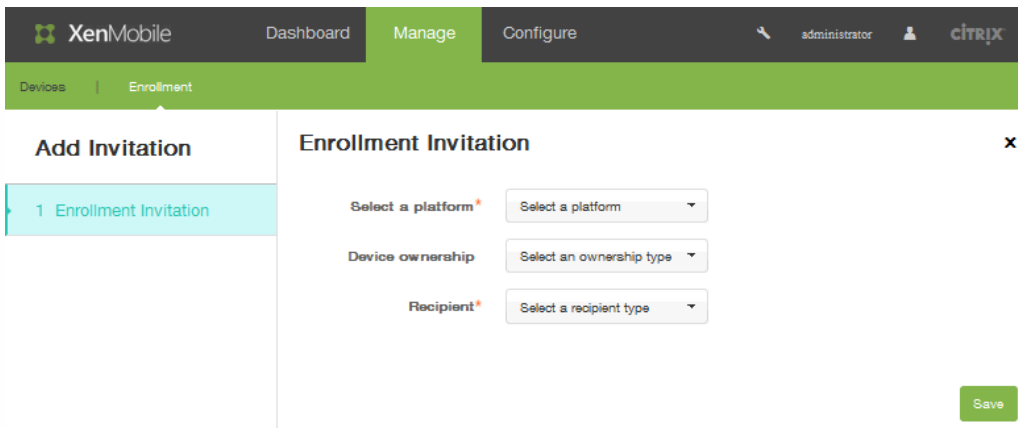
4. In the Select a platform list, click iOS or Android.
5. In the Device ownership list, click Corporate or Employee.
6. In the Recipient list, click User or Group. When you select a user as a recipient, the interface changes to display additional configuration options. Follow the steps in these topics to complete the invitation settings depending on the recipient type you select:

To send an enrollment invitation to a user

1. In the XenMobile console, click Manage > Enrollment.
2. On the Enrollment screen, click Add. A menu appears where you can choose to add an invitation or send an installation link.



3. Click Add Invitation. The Enrollment Invitation screen appears.



4. In the Select a platform list, click iOS or Android.
5. In the Device ownership list, click Corporate or Employee.
6. In the Recipient list, click User. The interface changes to display configuration options related to user enrollment.

Recipients*

Email*	Phone number*	
<input type="text"/>	<input type="text"/>	Save Cancel

7. In User name, type a user name. The user must exist in the XenMobile server as a local user or as a user in Active Directory. If the user is local, make sure the user's email property is set in order to send notifications. If the user is in Active Directory, make sure LDAP is configured.
8. In the Device info list, select Serial number, UDID, or IMEI. After you choose an option, the interface changes to display a field where you can type the corresponding value for the device:

Device info

Phone number

Carrier

Serial number

Serial number
UDID
IMEI

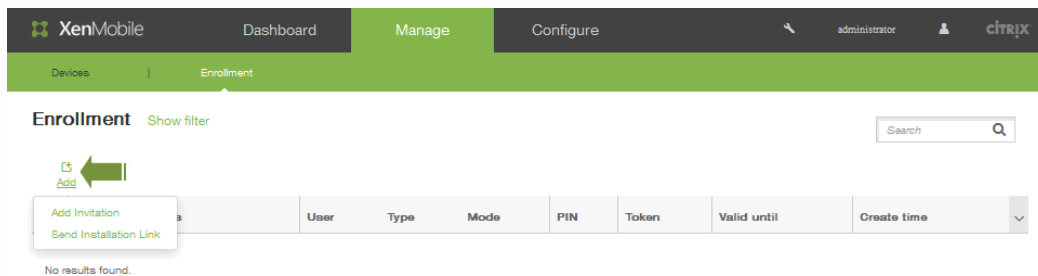
9. In Phone number, optionally enter the phone number for the user.
10. In the Carrier list, select a carrier with which to associate the user's phone number.
11. In the Enrollment mode list, select User name + Password (the default), High Security, Invitation URL, Invitation URL +

PIN, Invitation URL + Password, Two Factor, or User name + PIN.

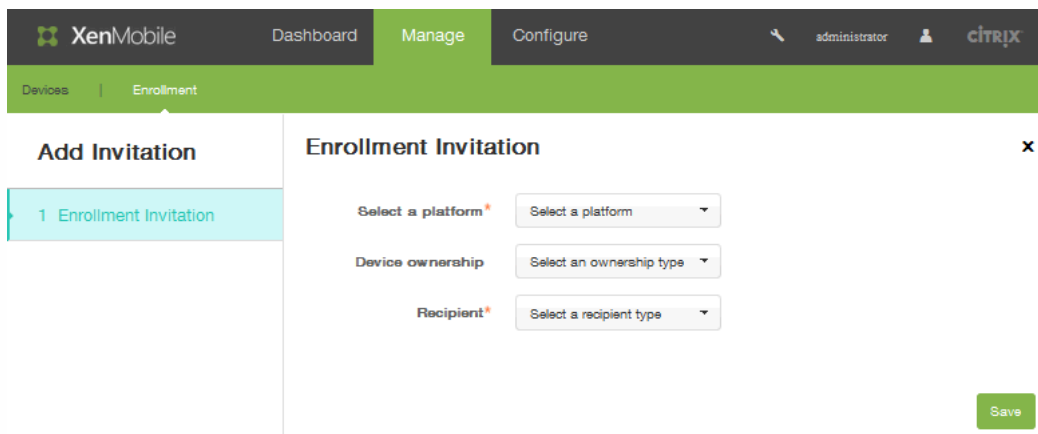
12. In the Template for agent download list, the choices for this option are based on the platform type. For example, iOS Download Link appears as an option if you selected iOS as a platform in Step 1.
13. In the Template for enrollment URL list, click Enrollment Invitation.
14. In the Template for enrollment confirmation list, click Enrollment Confirmation. The enrollment invitation expires after a period of time. The Expire after field indicates when the enrollment expires. The Maximum Attempts field illustrates the maximum number of times the enrollment process occurs.
15. In Send invitation, click ON.
16. Click Save.

To send an enrollment invitation to a group

1. In the XenMobile console, click Manage > Enrollment.
2. On the Enrollment screen, click Add. A menu appears where you can choose to add an invitation or send an installation link.



3. Click Add Invitation. The Enrollment Invitation screen appears.



4. In the Select a platform list, select iOS or Android .
5. In the Device ownership list, select Corporate or Employee.
6. In the Recipient list, select Group. The interface changes to display configuration options for group enrollment:

Enrollment Invitation

Select a platform*	Android	▼
Device ownership	Employee	▼
Recipient*	Group	▼
Domain*	Select a domain	▼
Group*	Select a group	▼
Enrollment mode*	User name + Password	▼
Template for agent download	Select a template	▼
Template for enrollment URL	Select a template	▼
Template for enrollment confirmation	Select a template	▼
Expire after	Never	
Maximum Attempts	0	
Send invitation	<input type="checkbox"/>	OFF

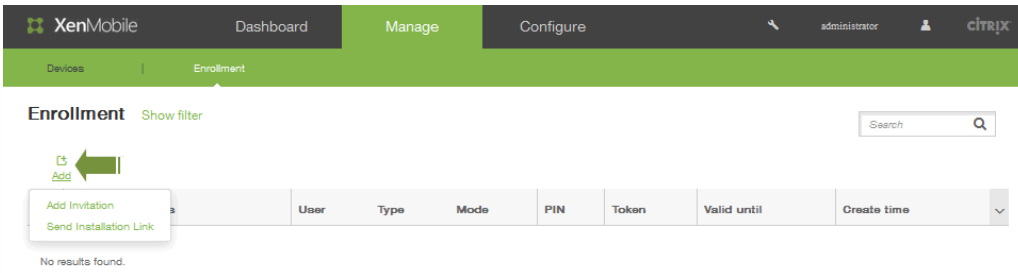


7. For Domain, choose the domain in which the group of recipients resides.
8. For Group, choose the group to which you want to send an enrollment notification.
9. In the Enrollment mode, select User name + Password (the default), High Security, Invitation URL + PIN, Invitation URL + Password, Two Factor, or User name + PIN.
10. In the Template for agent download list, the choices for this option are based on the platform type. For example, iOS Download Link appears as an option if you selected iOS in Step 1.
11. In the Template for enrollment URL, select Enrollment Invitation.
12. In the Template for enrollment confirmation list, select Enrollment Invitation. The enrollment invitation expires after a period of time. The Expire after field indicates when the enrollment expires. The Maximum Attempts field illustrates the maximum number of times the enrollment process occurs.
13. In Send invitation, click ON to send the enrollment invitation to the selected group.
14. Click Save.

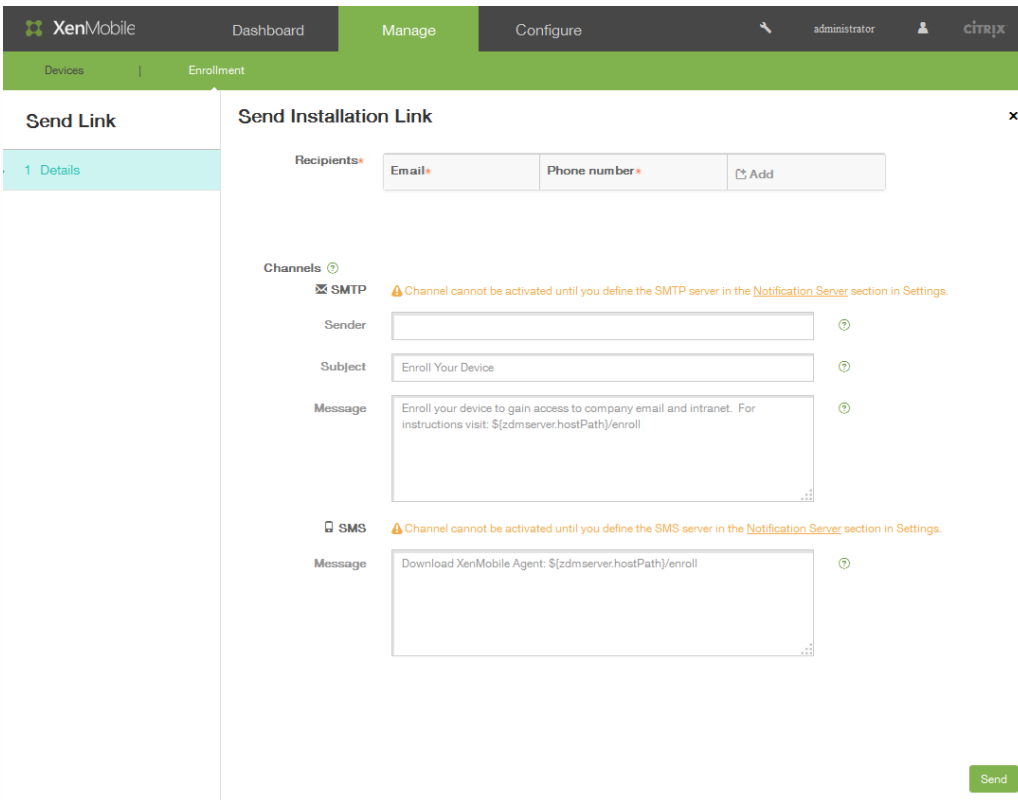
To send an enrollment installation link

Before you can send an enrollment installation link, you'll have to configure channels (SMTP or SMS) on the Notification Server: Configure > Settings > Notification Server. For more information, see [Notifications in XenMobile](#).

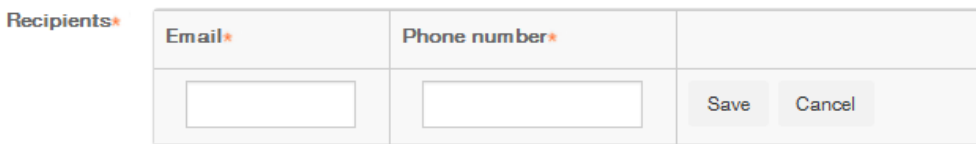
1. In the XenMobile console, click Manage > Enrollment.
2. On the Enrollment screen, click Add. A menu appears where you can choose to add an invitation or send an installation links.



3. Click Send Installation Link. The interface changes to show the Send Installation Link options.



4. In Recipient, click Add to identify a recipient to whom you want to send an installation enrollment link. The Recipient field expands to allow you to add an email address and phone number.



5. Enter an Email address, Phone number for the user receiving the enrollment invitation link. These fields are mandatory.
6. In Channels, select an appropriate channel to use for sending the enrollment installation link. Notifications are sent over SMTP or SMS. **Note:** These channels (SMTP or SMS) cannot be activated until you configure the server settings in Configure > Settings > Notification Server. For more information, see [Notifications in XenMobile](#).
7. If you are configuring the SMTP field, specify the Sender. This is an optional field used in the form field of an SMTP message. If you do not specify a sender here, the value specified in the Settings > Notification Server field is used.
8. For SMTP notifications, optionally include the Subject. For example, "enroll your device."
9. Provide a Message used for the content of the message sent to the recipient. For example, "Enroll your device to gain

access to company email and intranet."

10. To send notifications over SMS, enter a message that will be sent to the recipient. This field is required for SMS-based notification. **Note:** In North America, SMS messages that exceed 160 characters are delivered in multiple messages.
11. Click Send.

Note

If your environment leverages SAMAccountName, after users receive the invitation and click the link, they must edit the user name to complete the authentication. For example, they need to remove *domainname* in SAMAccountName@*domainname*.com.

Configuring Deployment Rules and Schedules

May 25, 2016

This section describes:

- Deployment rules - parameters that affect the deployment outcome of a package.
- Deployment schedules - options that specify when XenMobile pushes packages to a device.

Configuring Deployment Rules

You can set any number of parameters that will affect the deployment outcome of a package.

For example, your package deployment could be based on a specific operating system version, on a particular hardware platform, or some other combination. In this wizard, you will find both a Base and Advanced rule editor. The Advanced view is a free-form editor. The image below illustrates the Deployment Rules screen accessible when adding or editing an app:

▼ Deployment Rules

Base | Advanced

Deploy this app when: All conditions are met. [New Rule]

Device ownership: [BYOD]

- Deploy this resource by devi
- Device ownership
- Device local encryption
- Supervised
- Device operating system ver
- Passcode compliant
- Deploy this resource regardir

Base Deployment Rules

Base deployment rules are comprised of predefined tests and resulting actions. When possible, the results are pre-built into the example tests. For example, when basing a package deployment on a hardware platform, all existing known platforms are populated into the resulting test, drastically reducing your rule creation time and limiting possible errors.

Click **New rule** to add a rule to the package.

Note: The rule builder includes further information, specific to each test.

To create a new rule, you select a rule template, select the condition type, and then customize the rule. Customizing the rule includes modifying the description. When you finish configuring settings, you add the rule to the package.

You can add as many rules as you want. The package is deployed when all of the rules match.

Advanced Deployment Rules

If you click on the **Advanced** tab, the **Advanced Rule Editor** appears.

In this mode, you can specify what relationship is set between the rules. The operators **AND**, **OR**, and **NOT** are available.

Configuring Deployment Schedules

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 deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connections**, which does not apply to iOS.

If you do not change the deployment schedule options, deployments occur immediately on every connection. The deployment schedule options are:

Deploy: Defaults to **ON**. To prevent deployment, change this setting to **OFF**.

Deployment Schedule: Defaults to **Now**. To specify a deployment time, select **Later** and then choose a date and enter a time.

Deployment condition: Defaults to **On every connection**. To limit deployments, change this setting to **Only when previous deployment has failed**.

Deploy for always-on connections: Defaults to **OFF**. For iOS and Windows Mobile devices: If you set the device **Connection Scheduling Policy** option to **Always**, you must change **Deploy for always-on connections** to **ON**. For Android devices: The XenMobile server property, **Background Deployment** requires that you set **Deploy for always-on connections** to **ON** for each policy deployed to Android devices.

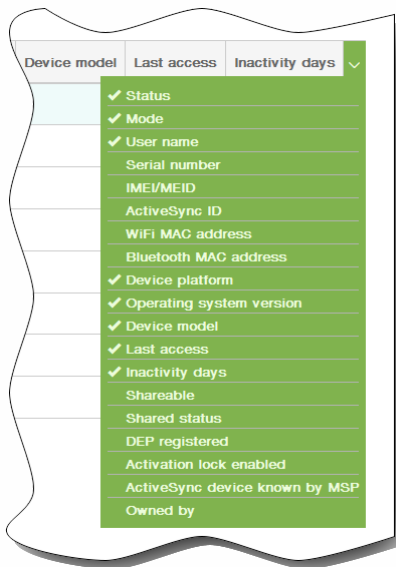
Adding Devices and Viewing Device Details

Feb 19, 2015

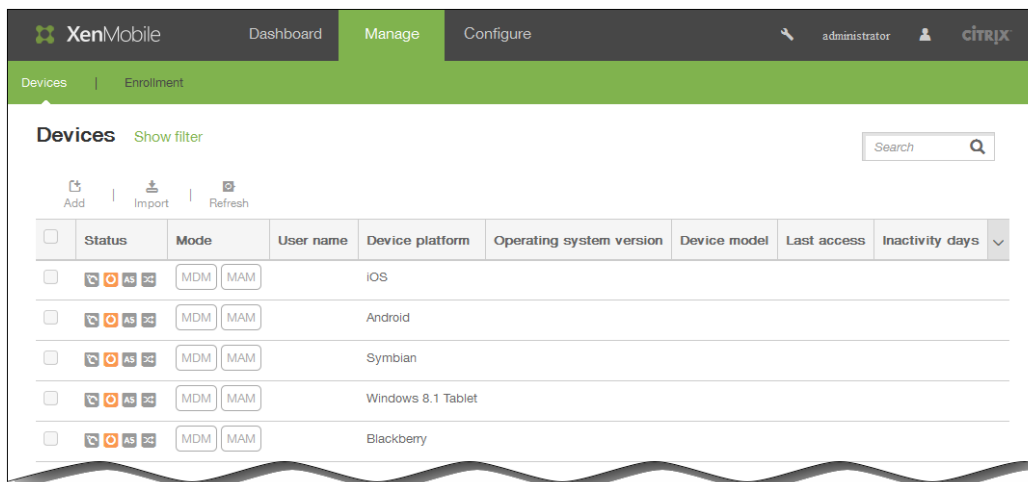
The XenMobile console server repository database stores a list of mobile devices. Each mobile device is defined by a unique serial number and/or International Mobile Station Equipment Identity (IMEI)/Mobile Equipment Identifier (MEID) identification. To populate the XenMobile console with your devices, you can add the devices manually or you can import a list of devices from a file. See [Device Provisioning File Formats](#).

On the Devices page in the console, you'll find a table listing each of the devices, along with the following information: Status (Device not jailbroken, Device not managed, Active Sync Gateway unavailable, no deployment failure), Mode, (MDM, MAM), User name, Device platform, Operating system version, Device model, Last access, and Inactivity days.

Note: The preceding headings are the defaults. You can customize what is shown in the table by clicking the down arrow on the last heading and then clicking headings you want to see or clearing those you do not want to see.

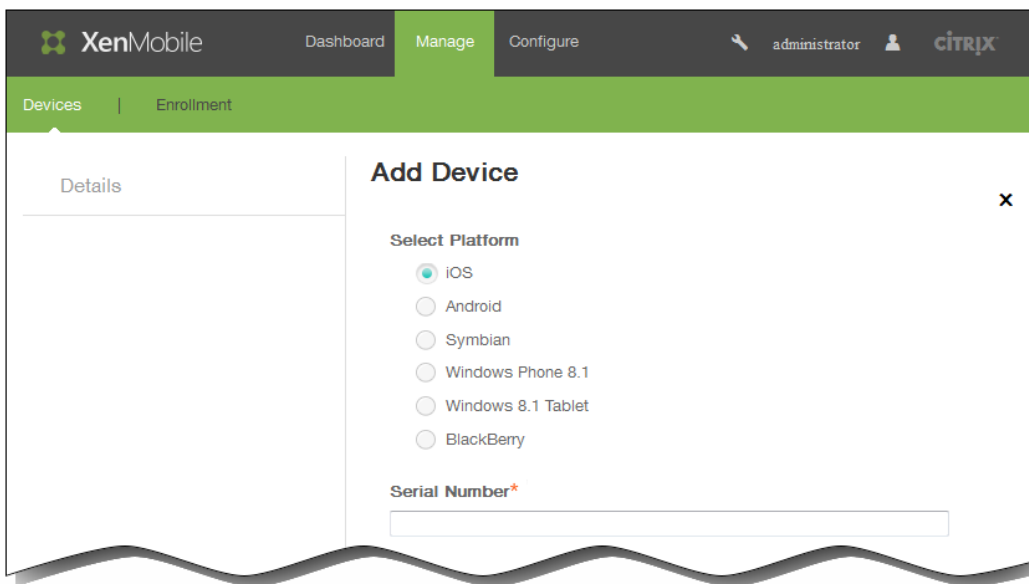


You can add a new device manually by clicking Add, or you can import a provisioning file by clicking Import. To update the table, click Refresh.

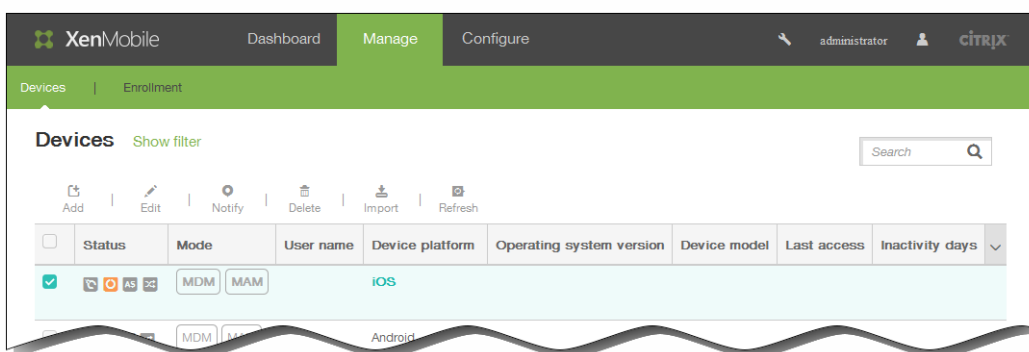


To add devices manually

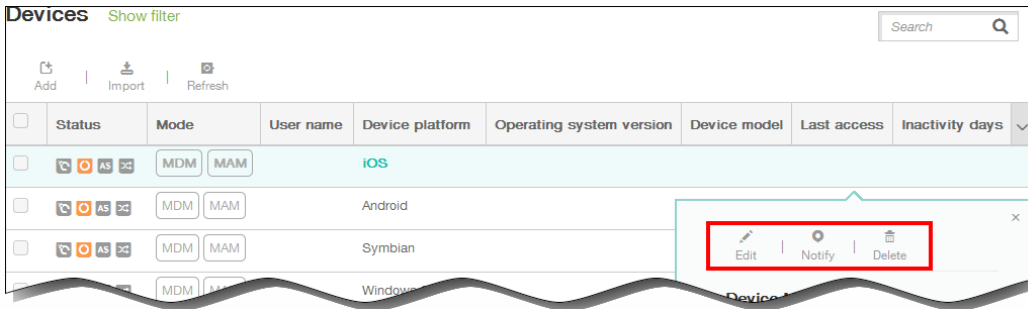
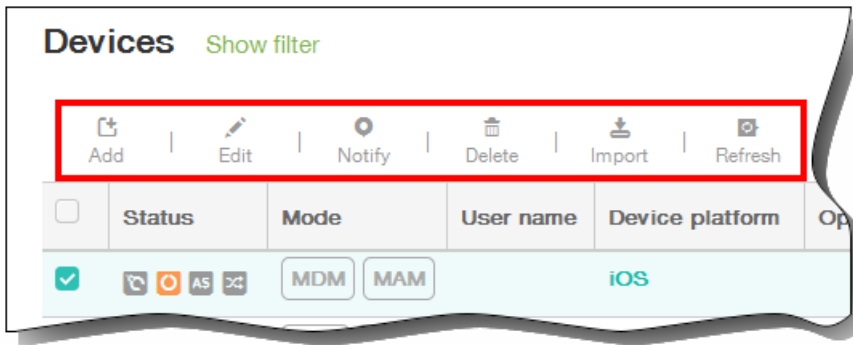
1. In the XenMobile console, click Manage > Devices and then click Add. The Add Device page appears.



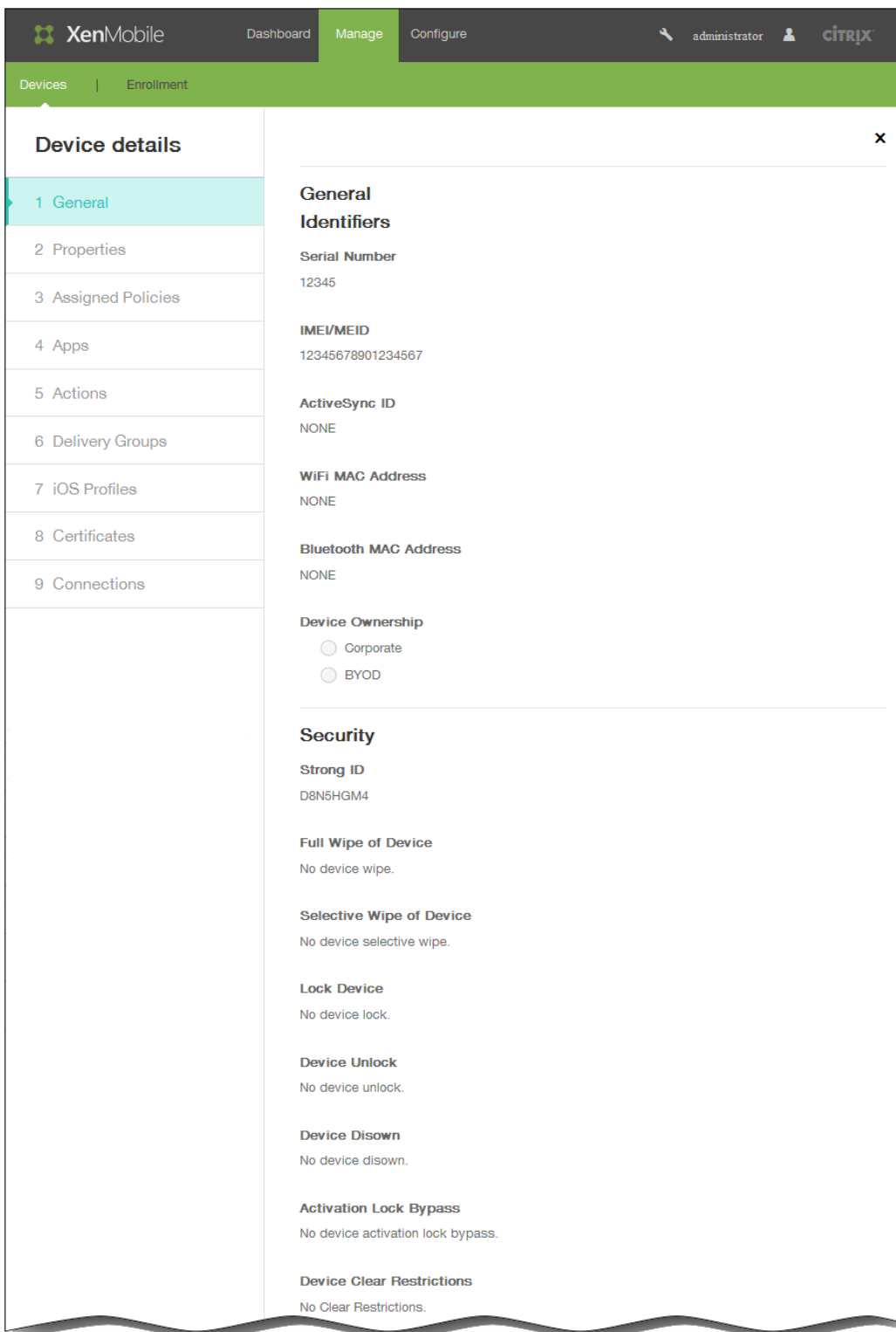
2. In Select platform, click either iOS, Android, Symbian, Windows Phone 8.1, Windows 8.1 Tablet, or BlackBerry.
3. Enter the following information:
 1. iOS: Enter the Serial Number.
 2. Android: Enter the Serial Number and IMEI/MEID.
 3. Symbian: Enter the IMEI/MEID.
 4. Windows Phone 8.1: Enter the Serial Number and IMEI/MEID.
 5. Windows 8.1 Tablet: Enter the Serial Number and IMEI/MEID.
 6. BlackBerry: Enter the Serial Number and IMEI/MEID.
4. Click Add. The Devices table appears with the device added to the bottom of the list.
5. In the list, select the device you added and then in the menu that appears, click Edit to view and confirm the device details.



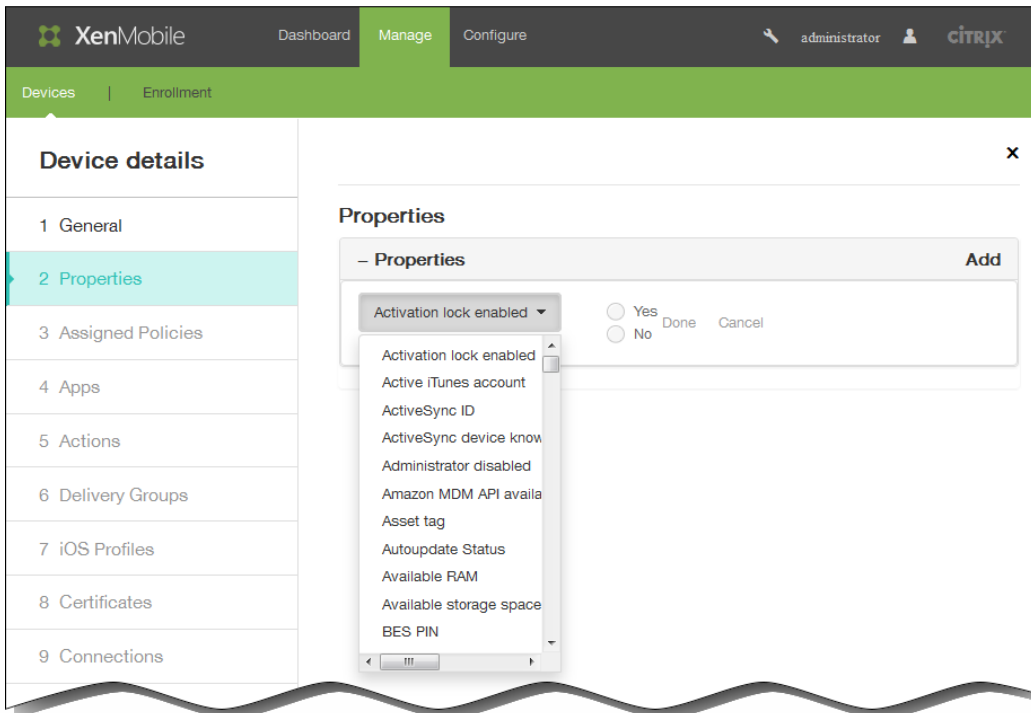
Note: When you select the check box next to a device, the options menu appears above the device list; when you click anywhere else in the list, the options menu appears on the right side of the listing.



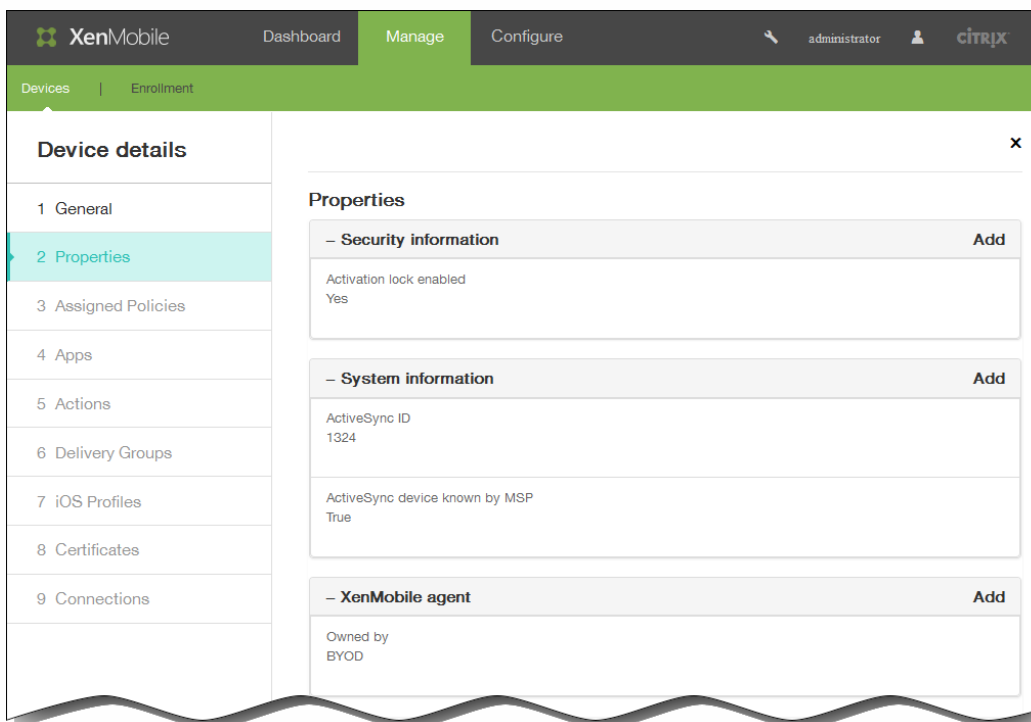
- Under General Identifiers, confirm the information displayed (the exact parameter list varies by platform type): Serial Number, IMEI/MEID, ActiveSync ID, WiFi MAC Address, Bluetooth MAC Address, Device Ownership: Corporate or BYOD.



7. Under Security, confirm the information that appears (the exact parameter list varies by platform type): Strong ID, Full Wipe of Device, Selective Wipe of Device, Lock Device, Device Unlock, Device Disown, Activation Lock Bypass, Device Clear Restrictions.
8. Click Next to add properties.
9. On the Properties page, click Add to view a list of the properties that you can provision for the device. The list of available properties appears.



10. In the list, click the property to be provisioned and then set its value. For example, in the preceding image, the property Activation lock enabled is selected with a value that you can set to either Yes or No.
 11. After configuring a property, click Done.
 12. Repeat steps 9 through 11 for each of the properties you want to provision and then click Next.
- Note: As you add properties, they are all listed under Properties. When you return to the Properties page at a later time, the properties are separated into different categories.



The **Assigned Policies** section and the sections that follow all contain summary information for the device.

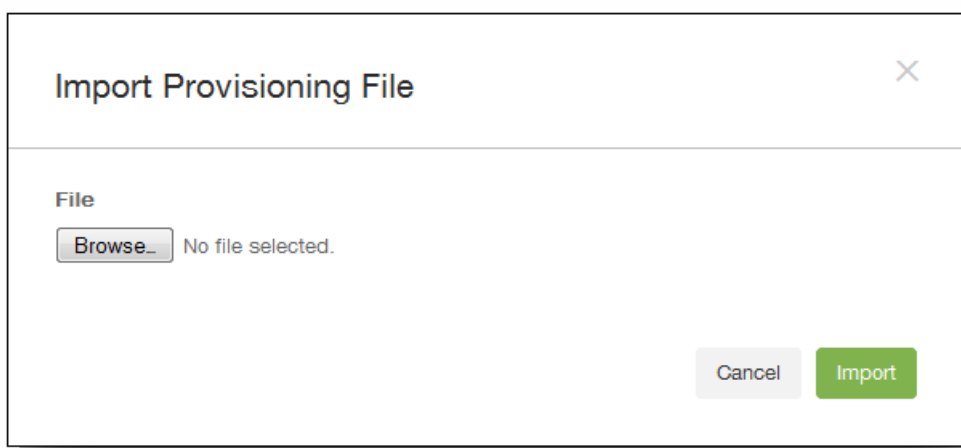
- **Assigned Policies:** Displays the number of assigned policies including the number of deployed, pending, and failed policies. The name, type and last deployed information also appear for each policy.
- **Apps:** Displays the number of apps as of the last inventory that includes the number of installed, pending, and failed apps.
 - For Installed, the following information appears: Name, Ownership, Version, Author, Size, Installed, Identifier, and Type.
 - For Pending and Failed apps, the following information appears: Name, Last deployed, Identifier, and Type.
- **Actions:** Displays the number of actions, which includes the number of deployed, pending, and failed actions. Each action displays the name and last deployed information.
- **Delivery Groups:** Displays the number of success, pending, and failed delivery groups. The Delivery Groups and time information appears for each action. In addition, more detailed information appears for the Delivery Group, including Status, Action, Owner and Date.
- **iOS Profiles (iOS devices only):** Displays the last iOS profile inventory, including Name, Type, Organization and Description.
- **Certificates:** Displays the number of valid certificates and expired or revoked certificates, including the Type, Provider, Issuer, Serial number, Valid from, and Valid to information.
- **Connections:** Displays the first connection status and the last connection status. For each connection, the User name, Penultimate authentication and Last authentication appear.
- **TouchDown (Android devices only):** Displays the last device authentication and the last user authenticated information. Each applicable Policy name and Policy value appear.

13. Click Save.

To import devices from a provisioning file

You can import a file supplied by mobile operators or device manufacturers, or you can create your own device provisioning file. See [Device Provisioning File Formats](#).

1. In the menu above the Devices table, click Import. The Import Provisioning File dialog box appears.

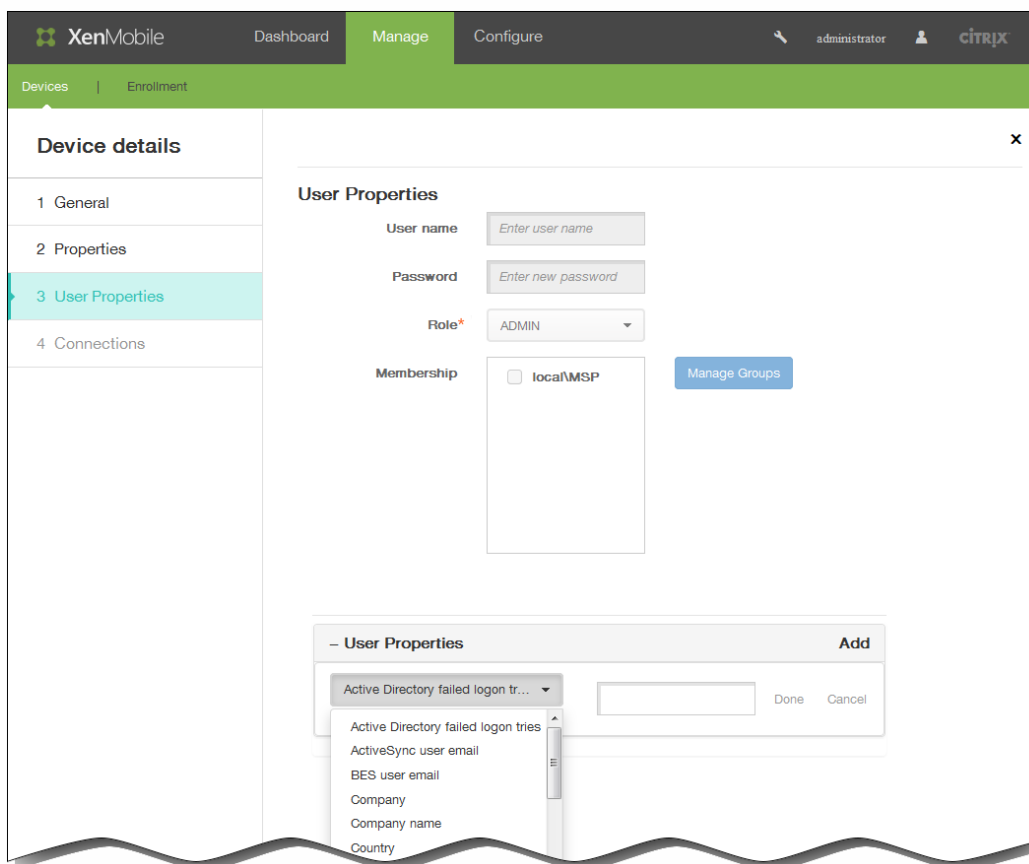


2. Select the file to import by clicking Browse and then navigating to the file's location.

3. Click Import. The imported files are added to the Devices table.

To edit devices

1. Select the device you want to edit, and then click Edit. The Device Details page appears.
2. Under General Identifiers, the only field you can change is Device Ownership, which you can set to Corporate or BYOD.
3. Click Next. The Properties page appears.
4. On the Properties page, add, edit, or delete properties as appropriate.
 - To edit a property, click the property, modify its settings, and then click Done or Cancel.
 - To delete a property, hover over the listing and then click the X on the right-hand side. The item is deleted immediately.
5. Click Next. The page that appears next depends on the selected device. For some devices you see User Properties, and for others you see Assigned Properties.
6. If you see User Properties, add, edit, or delete user properties as follows; otherwise the remaining pages contain summary information for the device. For a description of these pages, see [To add devices manually](#).



Note: The upper portion of the User Properties page cannot be edited.

- To add a user property, click Add.
 - In the list, click the property you want to add, enter the value for the property, and then click Done or Cancel. Repeat this step for each property you want to add.
 - To edit a property, click the property, modify its settings, and then click Done or Cancel.
 - To delete a property, hover over the listing and then click the X on the right-hand side. The item is deleted immediately.
7. Click Next on each of the following pages to view summary information.
 8. On the final page, click Save to save the changes to the device.

To send a notification to devices

You can send notifications to devices from the Devices page. For more information about notifications, see [To create or update notification templates in XenMobile](#)

1. Select the device or devices to which you want to send a notification.
2. Click Notify. The Notification dialog box appears. Recipients lists all the devices that are to receive the notification.

The screenshot shows a 'Notification' dialog box. It has a title bar with the text 'Notification' and a close button (X). The dialog is divided into several sections:

- Recipients:** A list of device identifiers: 12345, FG2ERG, and 123456999.
- Templates:** A dropdown menu currently showing 'Ad Hoc'.
- Channels:** Two checkboxes, 'SMTP' and 'SMS', both of which are checked.
- Message Configuration:** Two tabs, 'SMTP' and 'SMS', are visible. The 'SMTP' tab is active, showing three input fields: 'Sender', 'Subject', and 'Message'.
- Buttons:** At the bottom right, there are two buttons: 'Cancel' (disabled) and 'Notify' (active).

3. Configure the following information:
 1. Templates: In the list click the type of notification you want to send.
The Subject and Message fields are filled with the text configured for the template that you chose except for Ad Hoc.
 2. Channels: Select how to send the message. The default is SMTP
— and
SMS.
You can click the SMTP and SMS tabs to see the message format for each.
 3. Sender: Enter an optional sender.
 4. Subject: Enter a subject for an Ad Hoc message.
 5. Message: Enter the message for an Ad Hoc message.

4. Click Notify.

To delete devices

1. In the Devices table, select the device or devices you want to delete.
2. Click Delete. A confirmation dialog box appears. Click Delete again.

Important: You cannot undo this operation.

Tagging User Devices Manually

Jul 24, 2015

You can manually tag a device in XenMobile in the three following ways:

- Tag the device during the invitation-based enrollment process.
- Tag the device during the Self Help Portal enrollment process.
- Tag the device by adding device ownership as a device property.

You have the option of tagging the device as either corporate- or employee-owned. When using the Self Help Portal to self-enroll a device, you can also tag the device as either corporate- or employee-owned. As shown in the following figure, you can also tag a device manually by adding a property to the device from the **Devices** tab in the XenMobile console, adding the property named **Owned by** and choosing either **Corporate** or **BYOD** (employee-owned).

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'Dashboard', 'Manage' (active), and 'Configure'. The user is logged in as 'admin'. Below the navigation, there are two main sections: 'Devices' and 'Enrollment'. The 'Devices' section is active, showing a list of device details on the left sidebar. The main content area displays the details for a device named 'winuser3@testprise.net | Surface Pro 3'. Under the 'Properties' section, there is a 'Battery' property with an 'Add' button. Below it, the 'Owned by' property is highlighted, showing a dropdown menu and two radio buttons: 'Corporate' (selected) and 'BYOD'. There are 'Done' and 'Cancel' buttons next to the radio buttons. Below the 'Owned by' property, there are several other properties with '+ Add' buttons: '+ Memory', '+ Network information', '+ Notification Service', '+ Security information', and '+ System information'. At the bottom right, there are 'Back' and 'Next >' buttons.

Device Provisioning File Formats

Feb 12, 2015

Many mobile operators or device manufacturers provide lists of authorized mobile devices, and you can use these lists to avoid having to enter a long list of mobile devices manually. XenMobile supports an import file format that is common to all three supported device types: Android, iOS, and Windows.

A provisioning file that you create manually and use to import devices to XenMobile must be in the following format:

- `SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; ... propertyNameN;propertyValueN`

Note:

- The file charset must be UTF-8.
- 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, the property `propertyV;test;1;2` would be typed as `propertyV\;test\;1\;2` in the provisioning file.
- `SerialNumber` is required if `IMEI` is not given.
- `SerialNumber` is required for iOS devices because the serial number is the iOS device identifier.
- `IMEI` is required if `SerialNumber` is not given.
- Valid values for `OperatingSystemFamily` are: `WINDOWS`, `ANDROID`, or `iOS`.

Example of device provisioning file

The following lines each describe a device in a device provisioning file.

```
1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2
2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyN;propertyV$*&&ééétest
3050BF3F517301081610065510590393;35244201625379903;iOS;test;
4050BF3F517301081610065510590393;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;
```

The first entry means the following:

- `SerialNumber`: 1050BF3F517301081610065510590391
- `IMEI`: 15244201625379901
- `OperatingSystemFamily`: `WINDOWS`
- `ProertyName`: `propertyN`
- `PropertyValue`: `propertyV\;test\;1\;2;prop 2`

Macros in XenMobile

Nov 06, 2015

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
- iphone
- 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.

Device Policies

Apr 04, 2016

You can configure how XenMobile works with your devices by creating policies. Although many policies are common to all devices, each device has a set of policies specific to its operating system. As a result, you may find differences between iOS, Android, and Windows devices, and even between different manufacturers' devices running Android.

Before you create a new policy, be sure you complete these steps:

- Create any delivery groups you plan to use.
- Install any necessary CA certificates.

The basic steps to create a device policy are as follows:

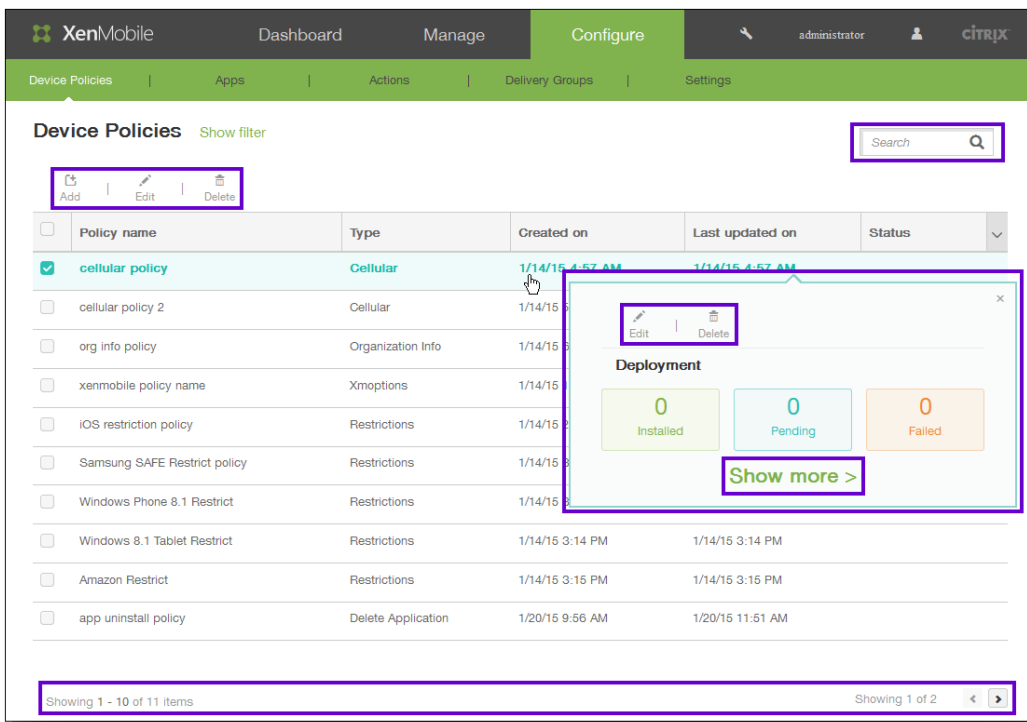
1. Name and describe the policy.
2. Configure one or more platforms.
3. Create deployment rules (optional).
4. Assign the policy to delivery groups.
5. Configure the deployment schedule (optional).

The Device Policies Page in the Console

You work with device policies on the XenMobile console Device Policies page. To get to the Device Policies page, click **Configure > Device Policies**. From here, you can add new policies, see the status of existing policies, and edit or delete policies.

The Device Policies page contains a table showing all the current policies.

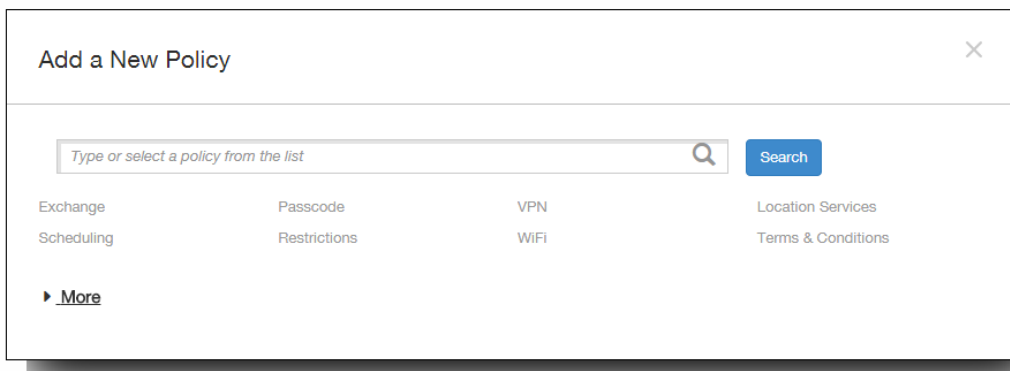
To edit or delete a policy on the Device Policies page, you can select the check box next to a policy to show the options menu above the policy list, or you click a policy in the list to show the options menu on the right side of the listing. If you click **Show More**, policy details appear.



To add a device policy

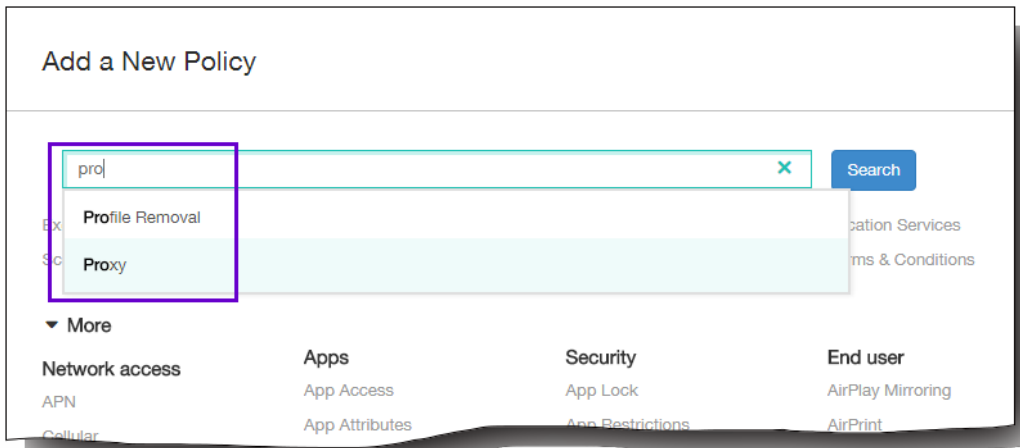
1. On the Device Policies page, click Add.

The Add a New Policy dialog box appears. You can expand More to see additional policies.

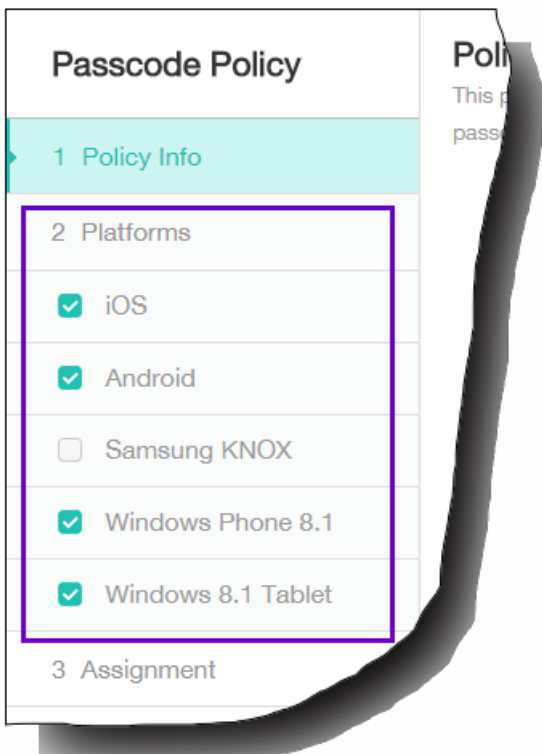


2. To find the policy you want to add, do one of the following:

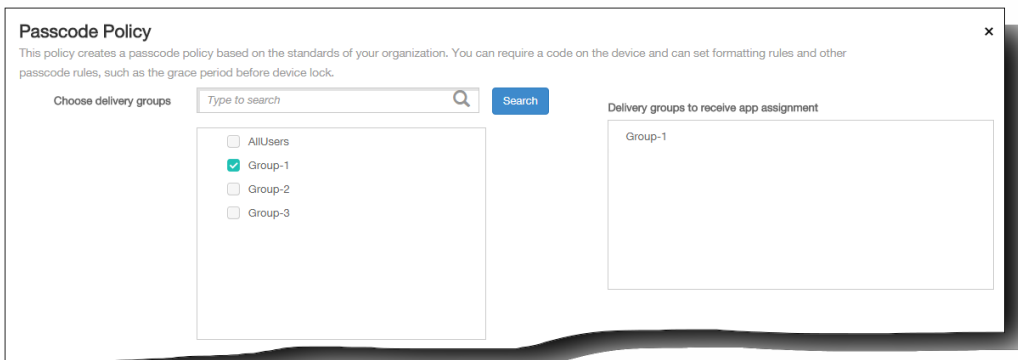
- Click the policy.
The Policy Information page for the selected policy appears.
- Type the name of the policy in the search field. As you type, potential matches appear. If your policy is in the list, click it. Only your selected policy remains in the dialog box. Click it to open the Policy Information page for that policy.
Important: If your selected policy is in the More area, it is only visible if you expand More.



3. Select the platforms you want to include in the policy. Configuration pages for the selected platforms appear in Step 5.
Note: Only those platforms supported by the policy are listed.



4. Complete the Policy Information page and then click Next. The Policy Information page collects information, such as the policy name, to help you identify and track your policies. This page is similar for all policies.
5. Complete the platform pages. Platform pages appear for each platform you selected in Step 3. These pages are different for each policy. Each policy may be different between platforms. Not all policies are supported by all platforms. Click Next to move to the next platform page or, when all the platform pages are complete, to the Assignment page.
6. On the Assignments page, select the delivery groups to which you want to apply the policy. When you click a delivery group, the group appears in the Delivery groups to receive app assignment box.
Note: The Delivery groups to receive app assignment box does not appear until you select a delivery group.



7. Click Save.

The policy is added to the Device Policies table.

To edit or delete a device policy

1. In the **Device Policies** table, select the check box next to the policy you want to edit or delete.
2. Click Edit or Delete.
 - If you click Edit, you can edit any and all settings.
 - If you click Delete, in the confirmation dialog box, click Delete again.

XenMobile Device Policies by Platform

Nov 08, 2016

The following table shows the device policies you can add and configure in XenMobile 10 for Amazon, iOS, Android, Samsung SAFE, Samsung KNOX, Symbian, Windows Phone 8.1, and Windows 8.1 tablet devices. You add and configure the device policies in the XenMobile console from Configure > Device Policies.

Note: Android Sony supports only the Storage Encryption policy. Android HTC supports only the Exchange policy.

Device policy	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 tablet
Common								
Exchange		X	X	X	X		X	
Scheduling			X			X		
Passcode		X	X		X		X	X
Restrictions	X	X		X			X	X
VPN	X	X	X	X	X			X
WiFi		X	X				X	X
Location Services		X	X					
Terms & Conditions	X	X	X	X	X	X	X	X
Network access								
APN		X	X		X			
Cellular			X					
Personal Hotspot		X						
Proxy		X						
Remote Support					X			

Device Policy	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 tablet
Samsung Firewall				X				
Tunnel			X					
	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 tablet
Custom								
Custom XML						X	X	X
Import iOS Profile		X						
Removal								
Profile Removal		X						
Apps								
App Access		X	X			X		
App Attributes		X						
App Configuration		X						
App Inventory		X	X		X	X	X	X
App Uninstall		X	X		X			X
App Uninstall Restrictions	X			X				
Files			X					
Samsung Browser				X	X			
Sideload Key								X

Signing Certificate Device policy	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows ^X 8.1 tablet
Webclip		X	X					X
Worx Store		X	X					X
	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 tablet
Security								
App Lock		X	X					
App Restrictions					X			
Contacts (CardDAV)		X						
Credentials		X	X					X
Kiosk				X				
Managed Domains		X						
SCEP		X						
Samsung MDM License Key				X	X			
Storage Encryption			X	X			X	
Web Content Filter		X						
XenMobile agent								
Enterprise Hub							X	
XenMobile Options			X			X		
XenMobile Uninstall			X					

End user Device policy	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 tablet
AirPlay Mirroring		X						
AirPrint		X						
Calendar (CalDav)		X						
Font		X						
LDAP		X						
MDM Options		X						
Mail		X						
Organization Info		X						
SSO Account		X						
Subscribed Calendars		X						

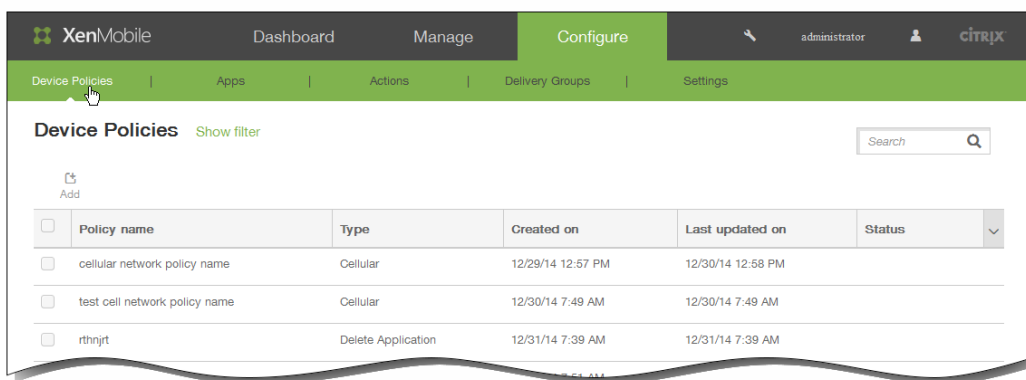
To add an app access device policy

Feb 27, 2015

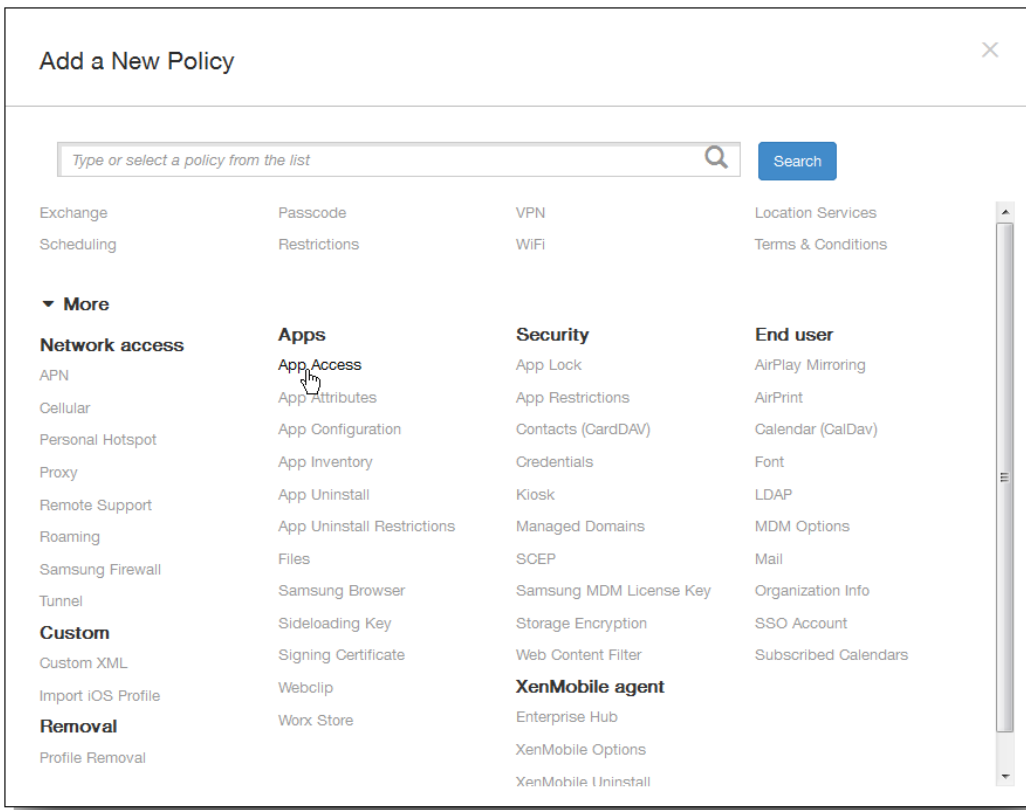
The app access device policy in XenMobile allows you to define a list of apps that are either required to be installed on the device, can be installed on the device, or must not be installed on the device. You can then create an automated action to react to the device compliance with that list of apps.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

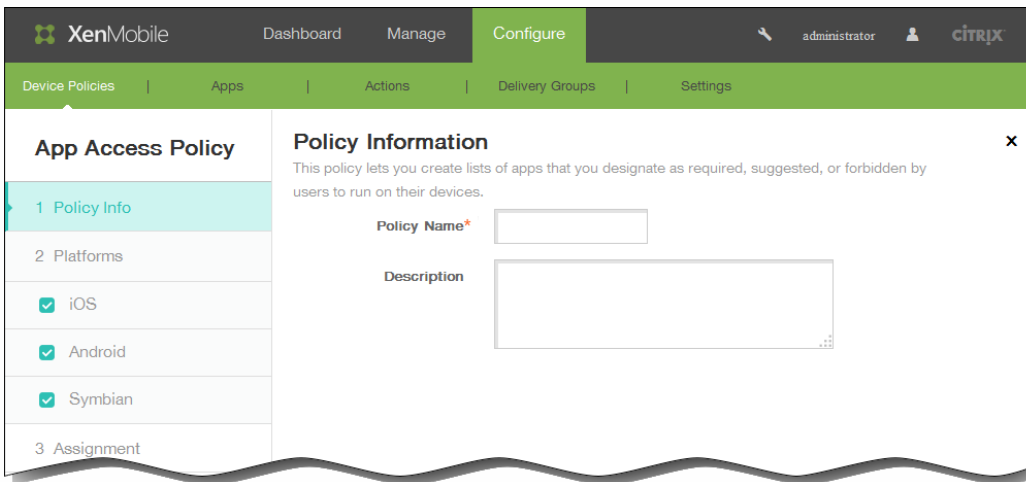
1. In the XenMobile console, click Configure > Device Policies.



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



3. Click More > App Access. The App Access Policy information page appears.

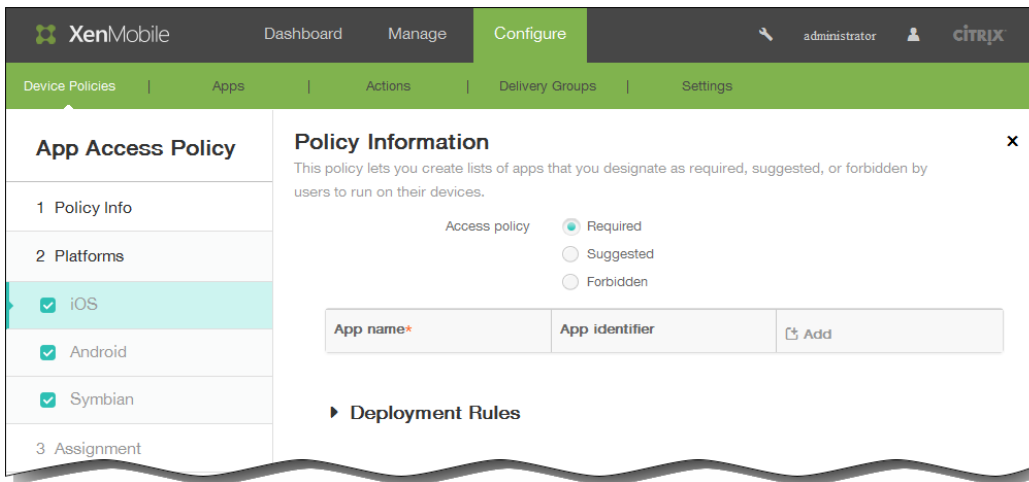


4. On the Policy Information pane, enter the following information:

1. Policy Name: Type a descriptive name for the policy.
2. Description: Type an optional 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 configuration page first.



6. Under Platforms, select the platform or platforms to want to add and then do the following for each platform:

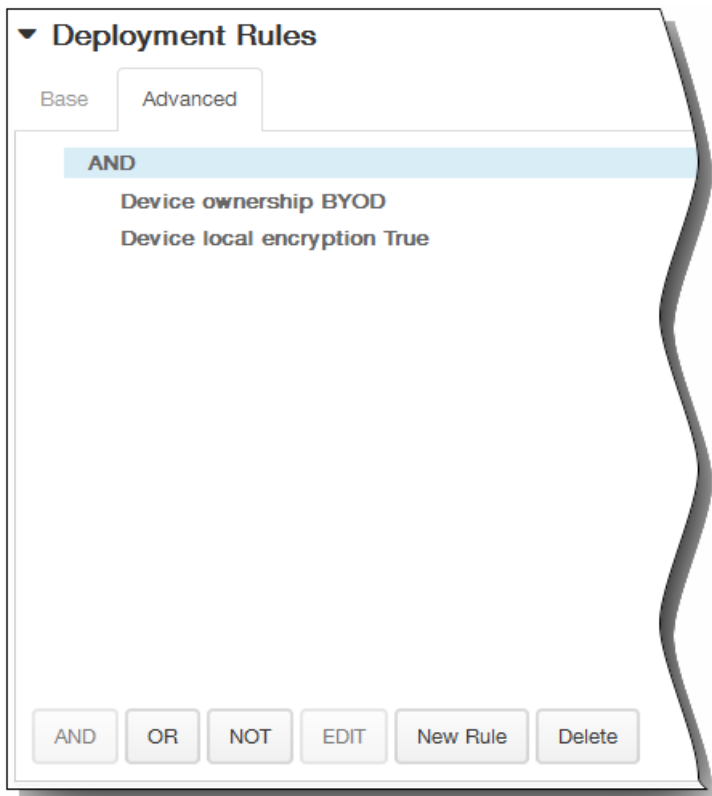
1. Access policy: Click Required, Suggested, or Forbidden. The default is Required.
2. To add one or more apps to the list, click Add and then do the following:
 1. App name: Enter an app name.
 2. App Identifier: Enter an optional app identifier.
 3. Click Save or Cancel.
 4. Repeat steps i. through iii. f 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. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

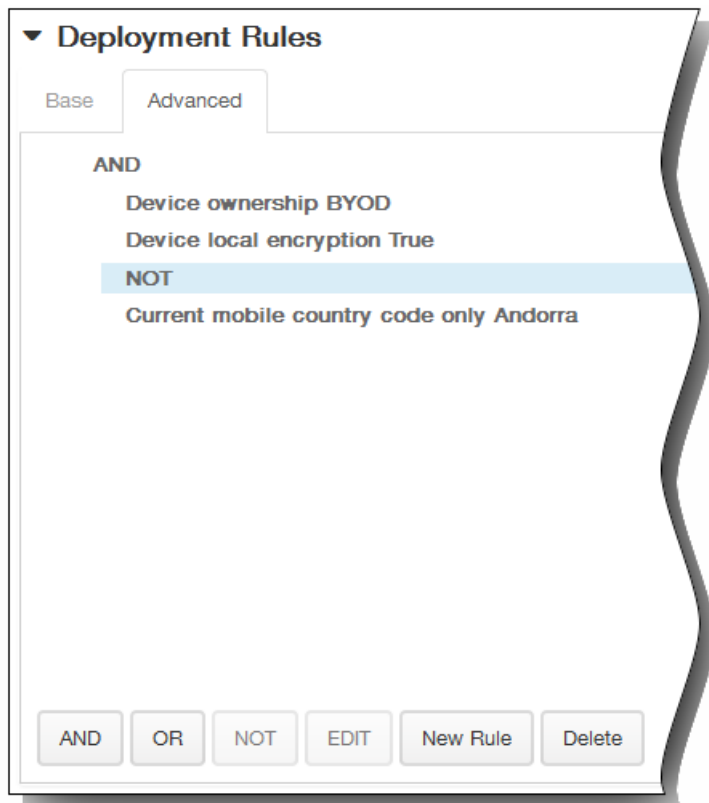


The conditions you chose on the Base tab appear.

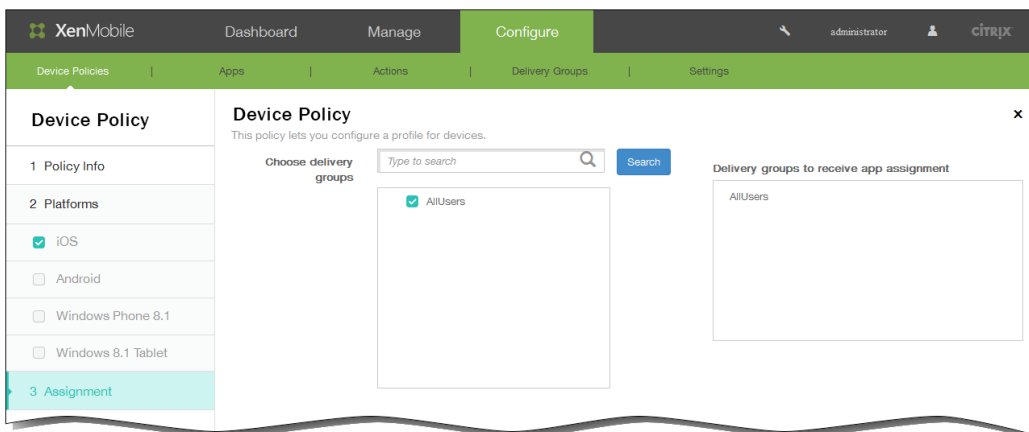
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



8. Click Next. The next platform page or Assignment policy 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.

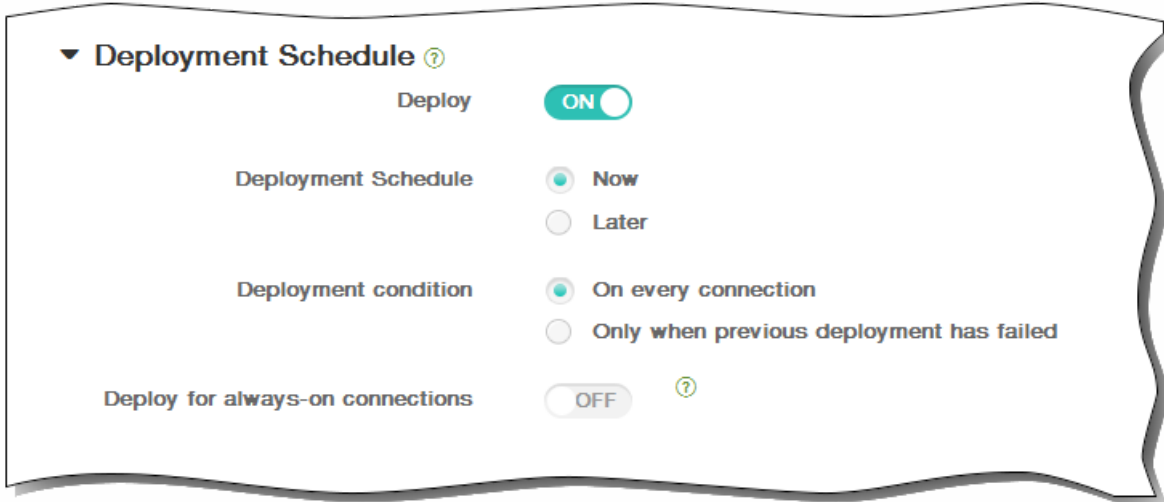


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

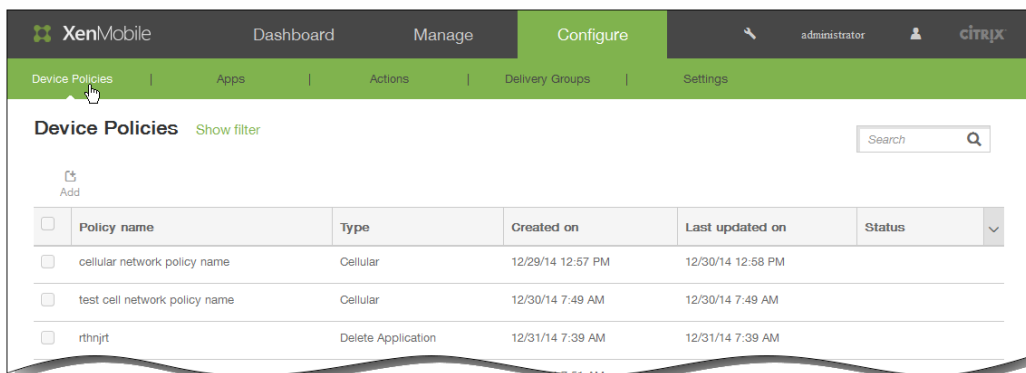
To add an app inventory device policy

Feb 25, 2015

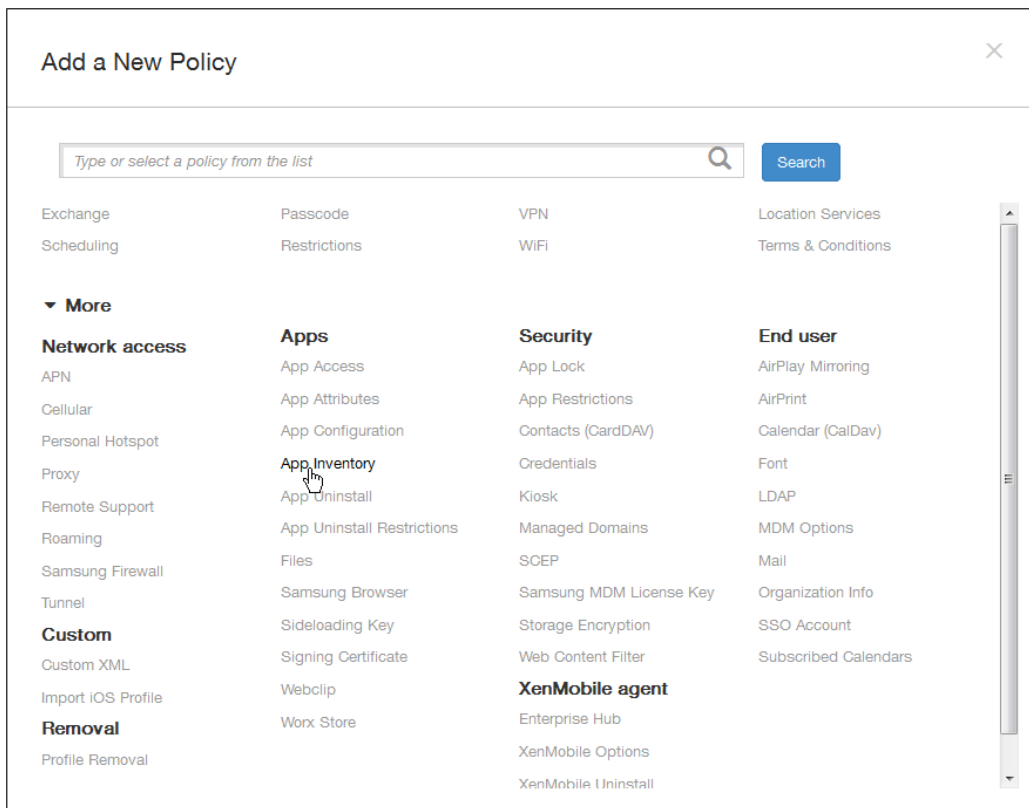
An app inventory policy in XenMobile lets you collect an inventory of the apps on managed devices, and then the inventory is compared to any app access policies deployed to those devices. In this way, you can detect apps that appear on an app blacklist (forbidden in an app access policy) or whitelist (required in an app access policy) and take action accordingly.

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.

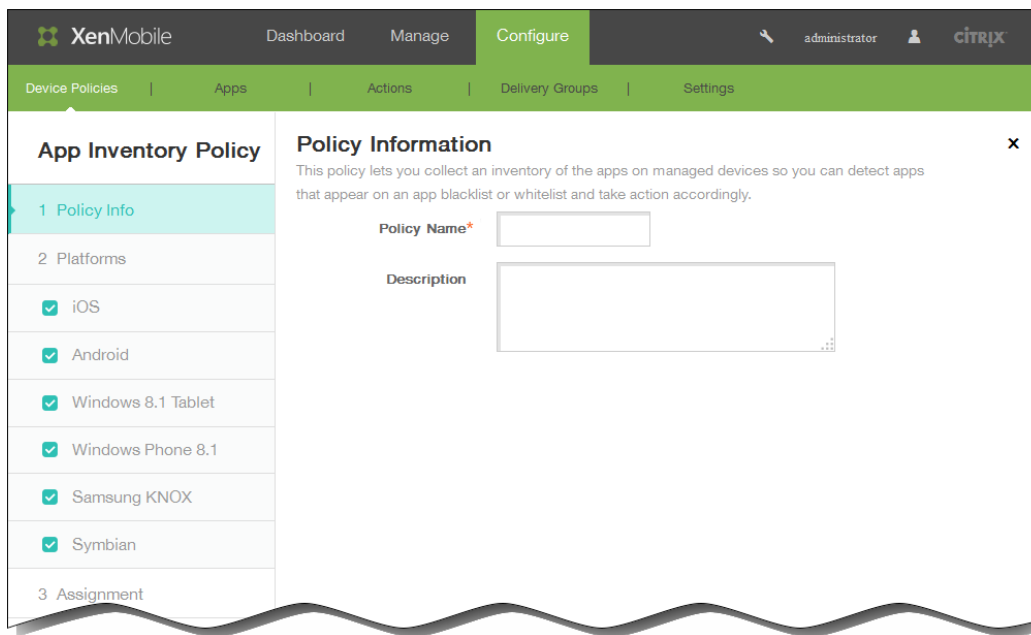
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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



3. Click More > App Inventory. The App Inventory Policy page appears.

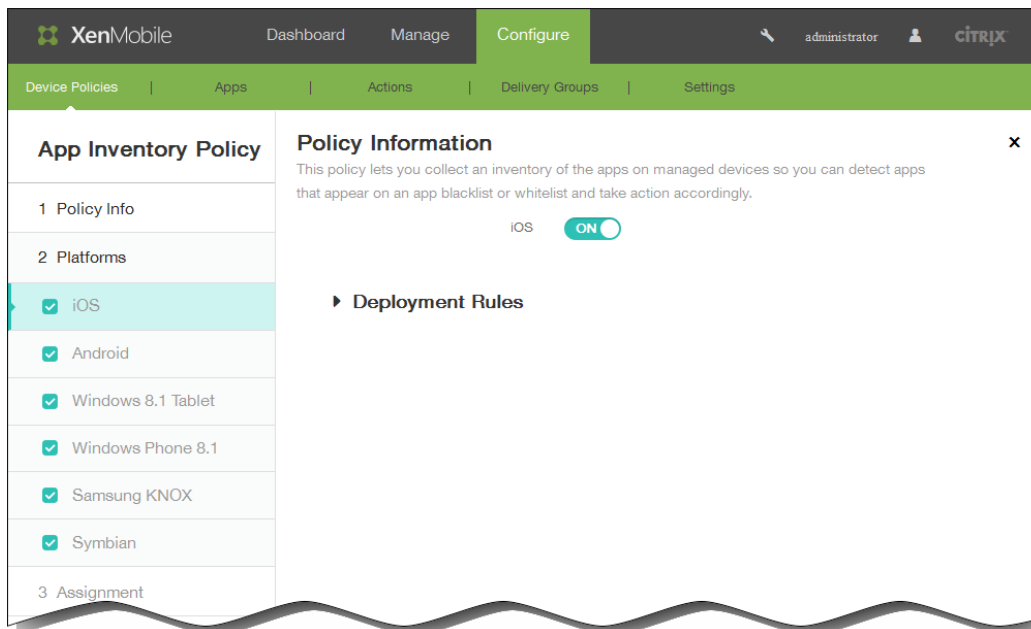


4. In the Policy Information pane, type the following information: .

1. Policy Name: Type a name for the policy.
2. Description: Type an optional 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 configuration panel first.



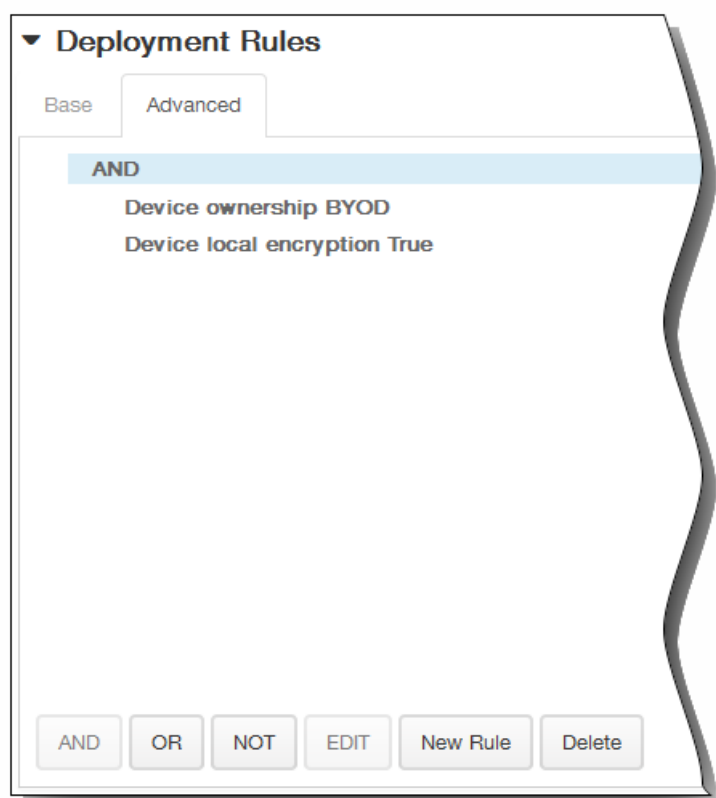
Select the platform or platforms you want to add, and then for each platform do the following:

6. Leave the default setting or change the setting to OFF. The default is ON.

7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



The conditions you chose on the Base tab appear.

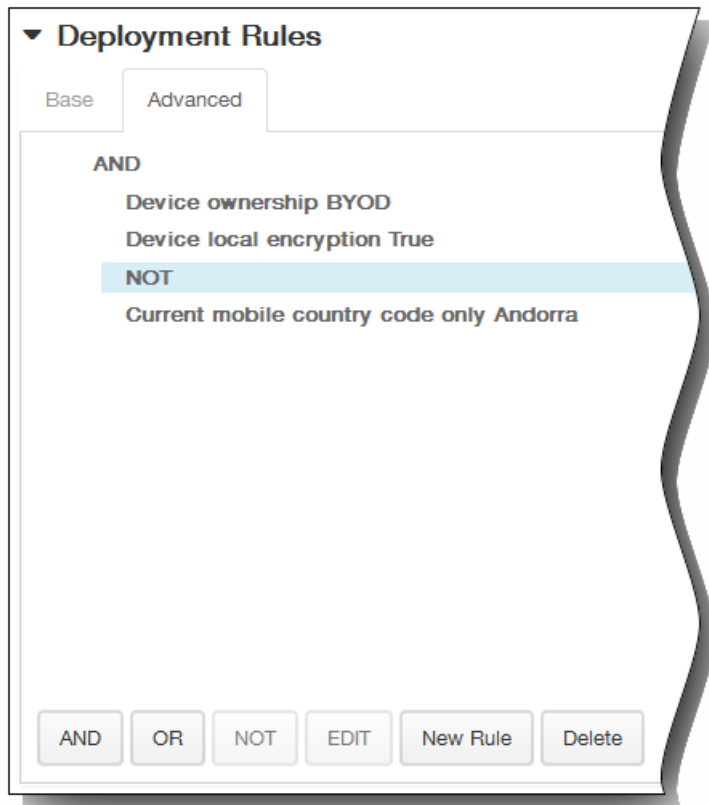
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on

the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

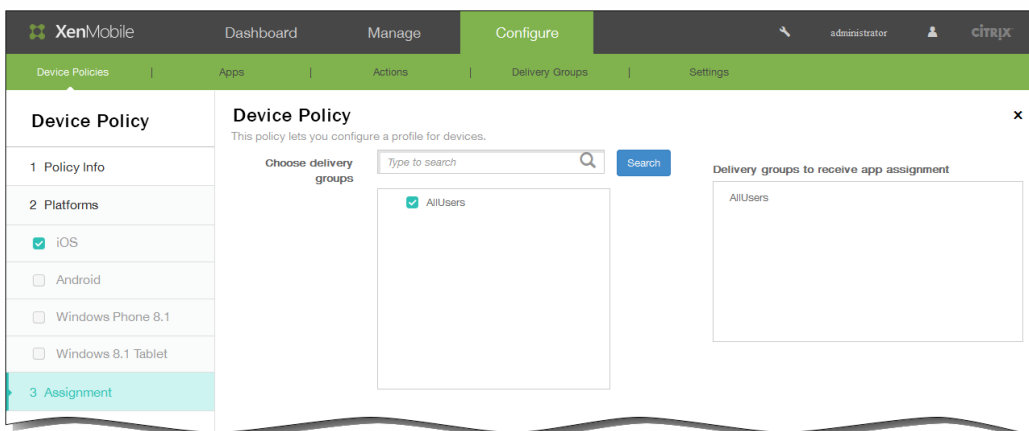
3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.

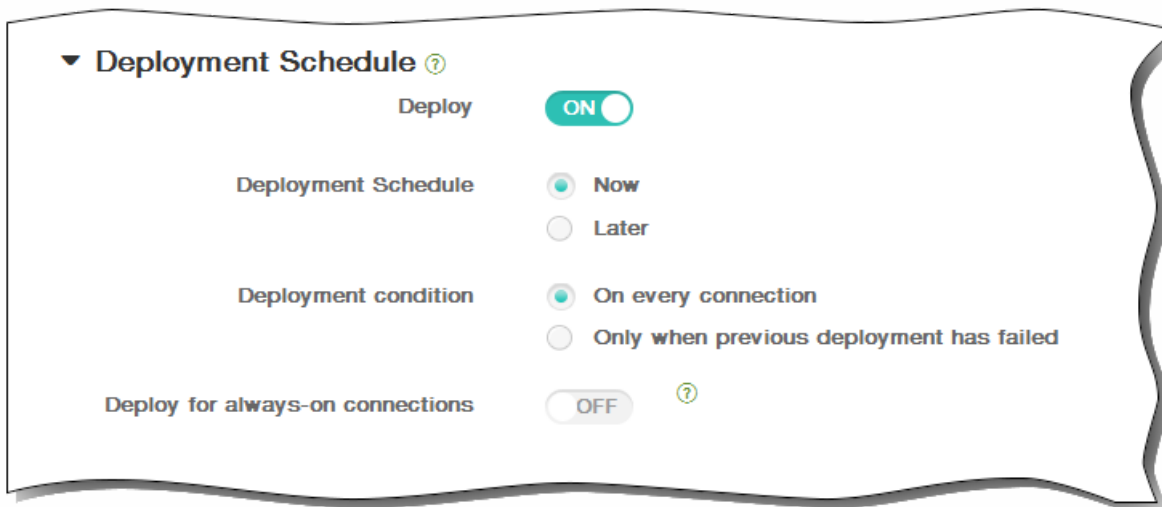


8. Click Next. The next platform page appears or the Assignment policy page appears.

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:
 1. 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.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

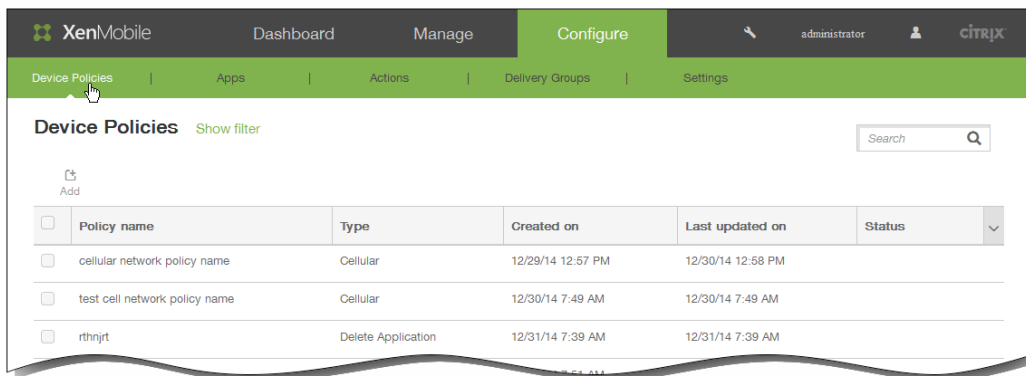
To add an app tunneling device policy for Android

Mar 31, 2015

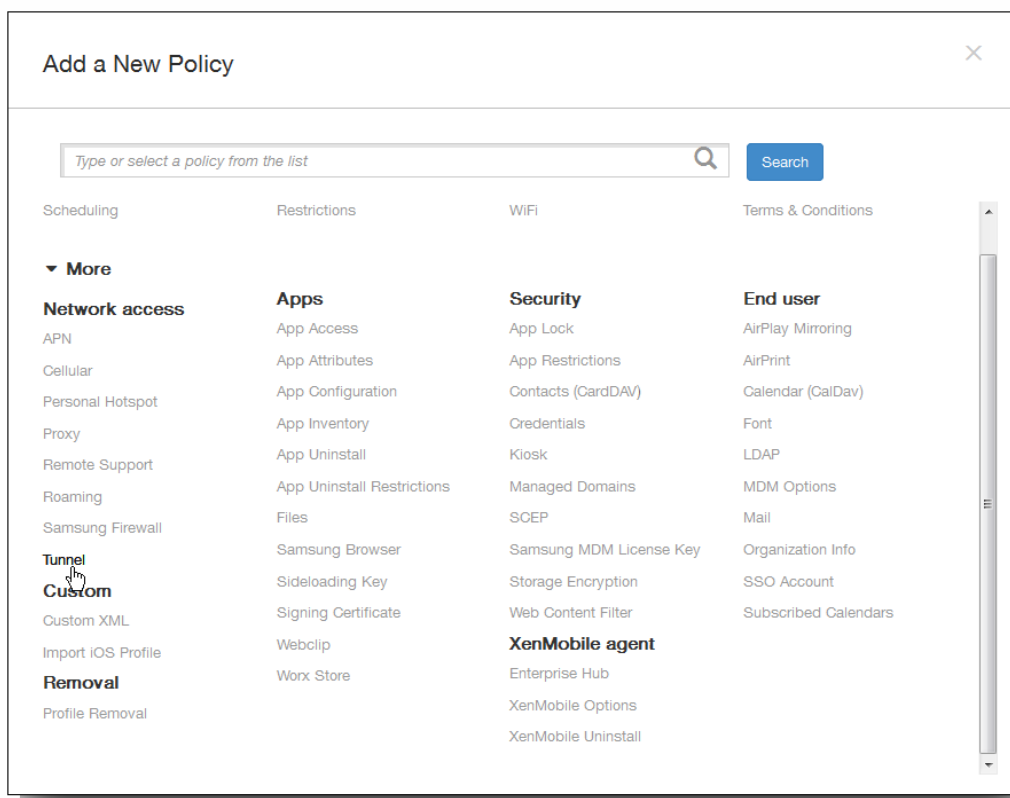
Application tunnels (app tunnels) are designed to increase service continuity and data transfer reliability for your mobile apps. App tunnels define proxy parameters between the client component of any mobile device app and the app server component. You can also use app tunnels to create remote support tunnels to a device for management support.

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.

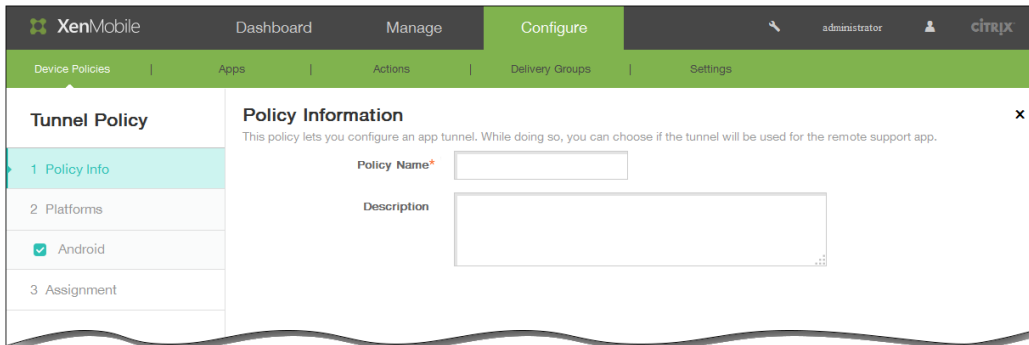
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



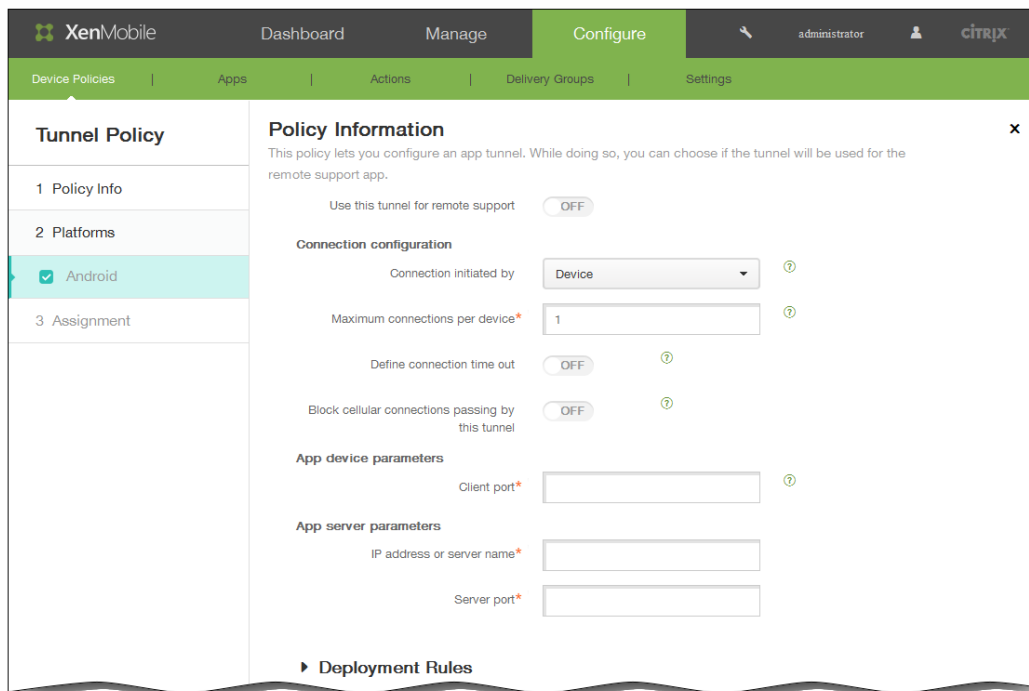
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



3. Click More and then, under Network access, click Tunnel. The Tunnel Policy page appears.



4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The Android Policy platform page appears.



6. In 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:
 1. Connection initiated by: Click Device or Server to specify the source initiating the connection.
 2. 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.
 3. Define connection time out: Select whether to set a length of time an app can be idle before the tunnel is closed.

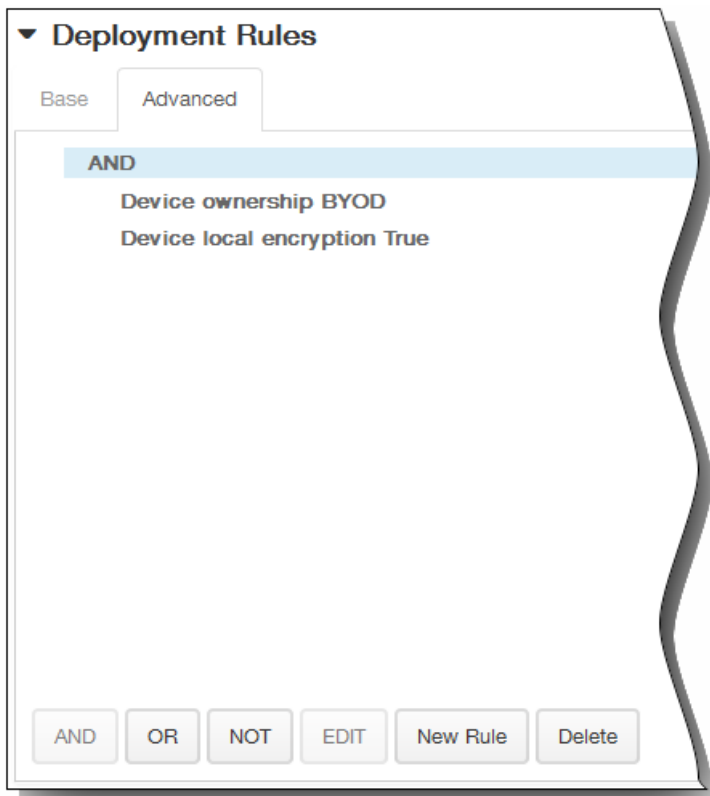
4. Connection time out: If you set Define connection time out to On, type the length of time in seconds that an app can be idle before the tunnel is closed.
5. Block cellular connections passing by this tunnel: Select whether this tunnel is blocked while roaming.
Note: WiFi and USB connections will not be blocked.
6. Client port: Type the client port number. In most cases, this value is the same as for the server port.
7. IP address or server name: Type the IP address or name of the app server. This field applies only to device-initiated connections.
8. Server port: Type the server port number.

If you **do** select remote support, do the following:

1. Use this tunnel for remote support: Set to On.
 2. Define connection time out: Select whether to set a length of time an app can be idle before the tunnel is closed.
 3. 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.
 4. Use SSL connection: Select whether to use a secure SSL connection for this tunnel.
 5. 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. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

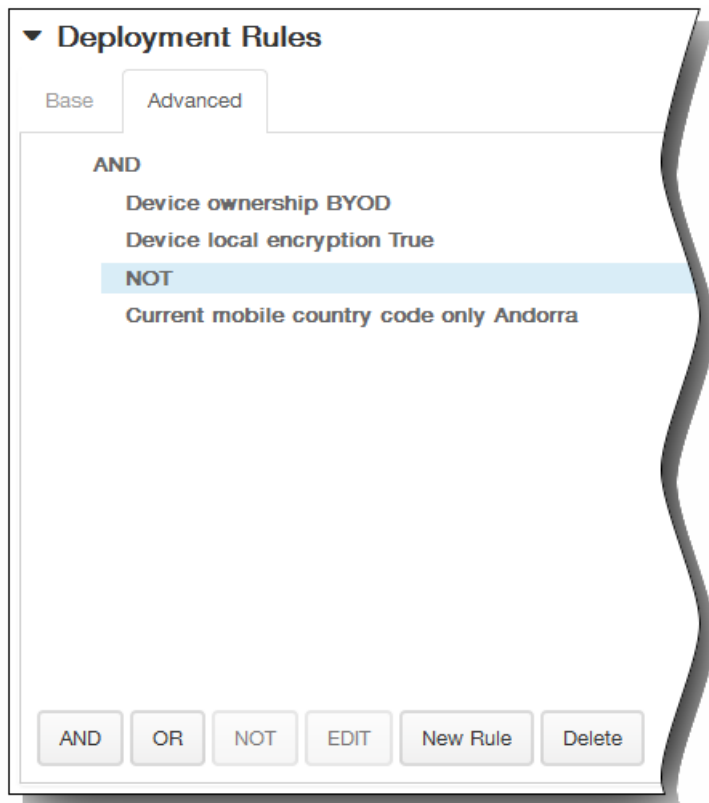


The conditions you chose on the Base tab appear.

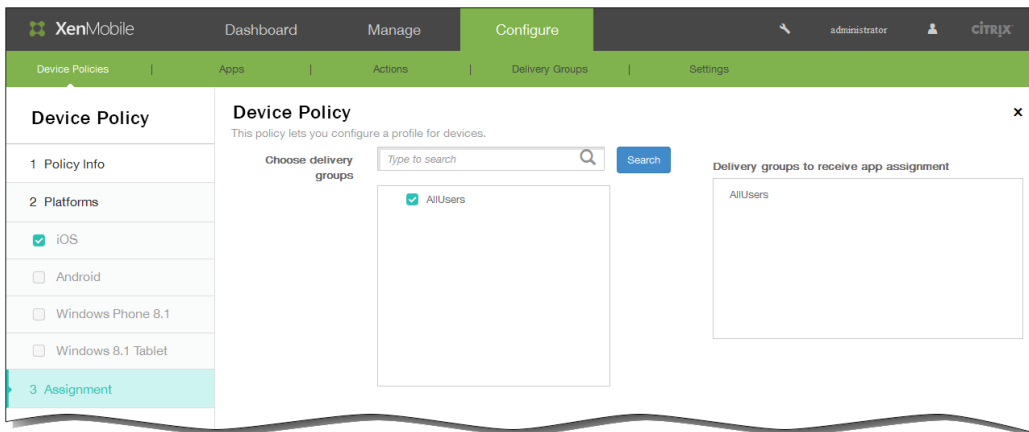
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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.

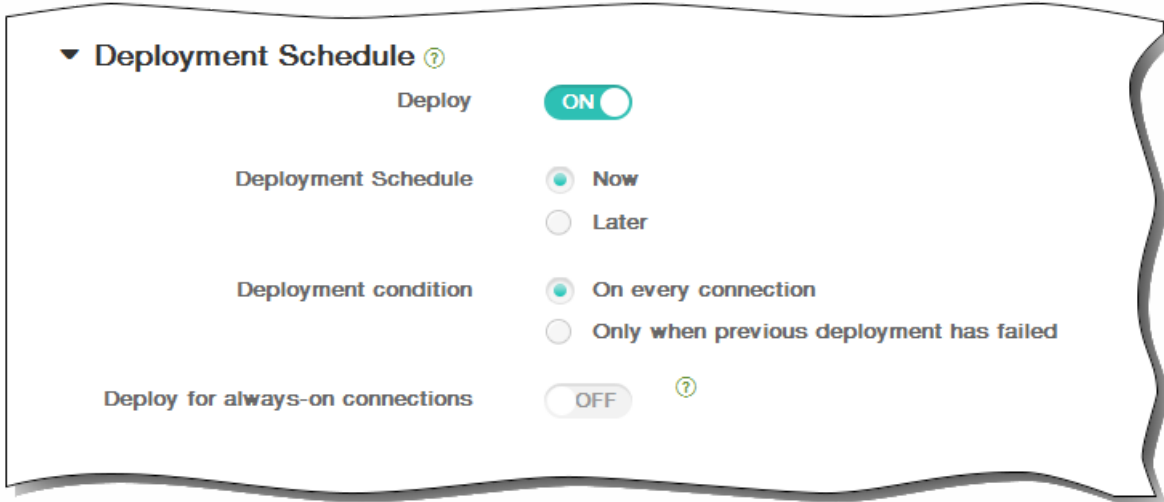


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

Custom XML device policies

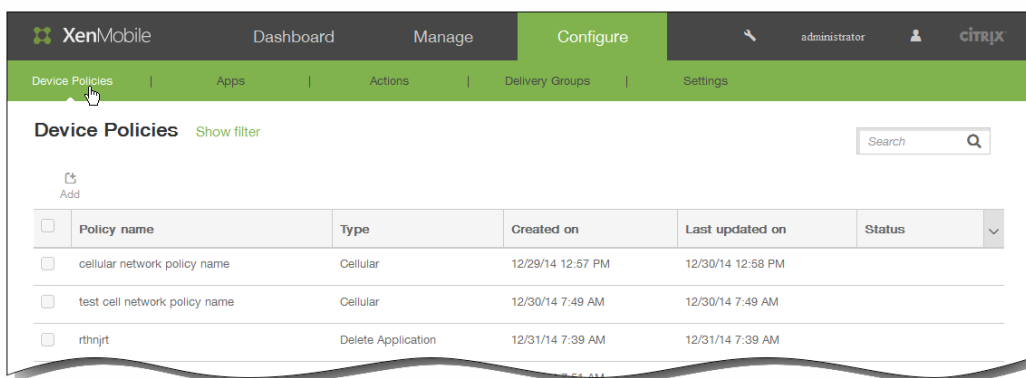
Mar 17, 2015

You can create custom XML policies in XenMobile when you want to customize the following features on Windows Phone 8.1, Windows 8.1 tablet, and Symbian devices:

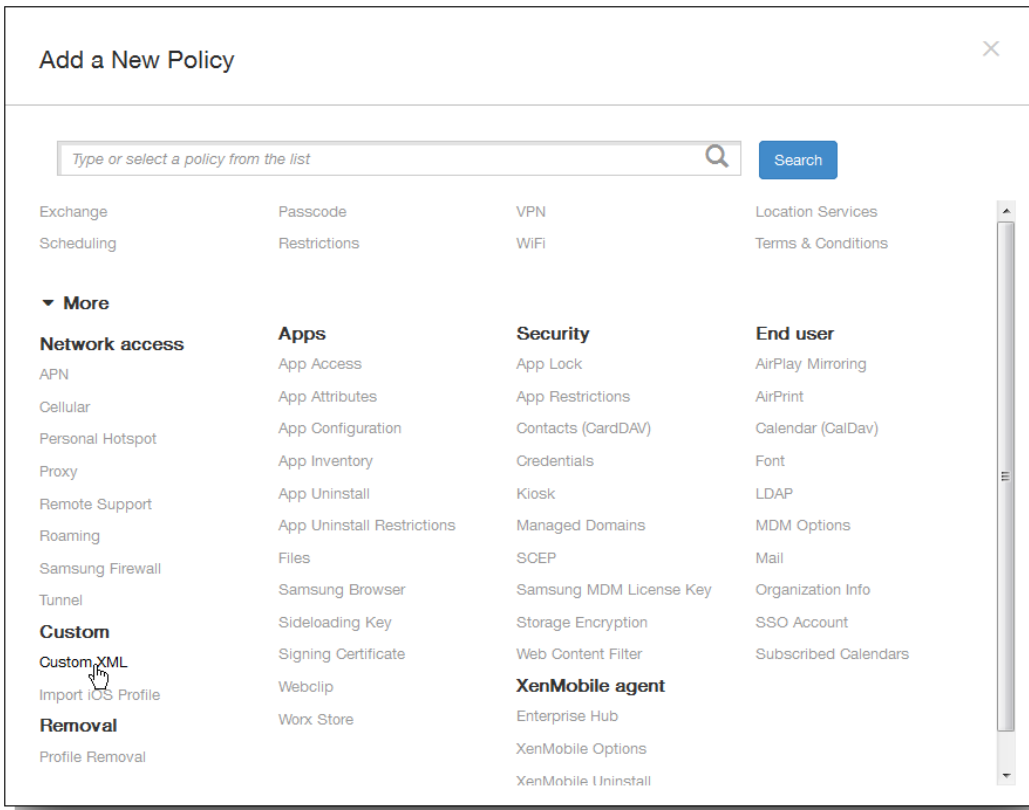
- Provisioning, which includes configuring the device, and enabling or disabling features
- Device configuration, which includes allowing users to change settings and device parameters
- Software upgrades, which includes providing new software or bug fixes to be loaded onto the device, including apps 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 8.1. 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.

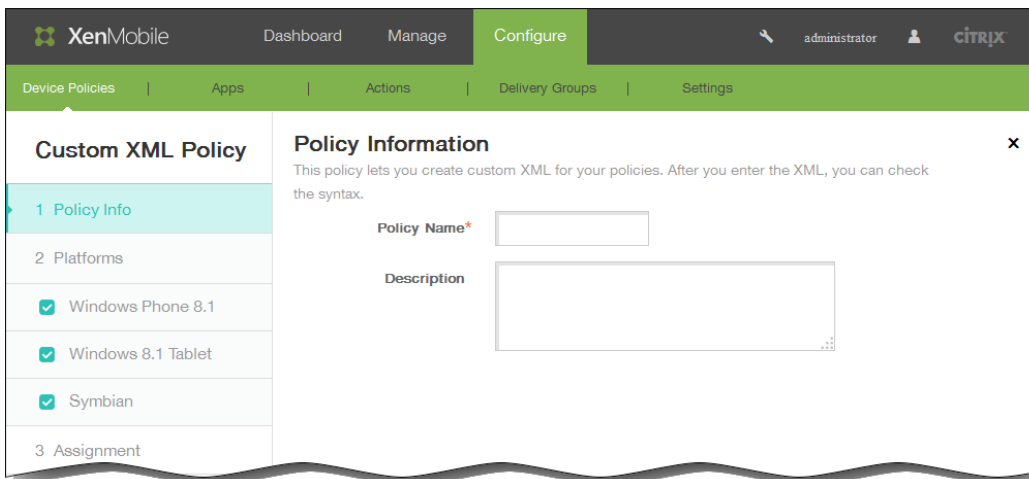
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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



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

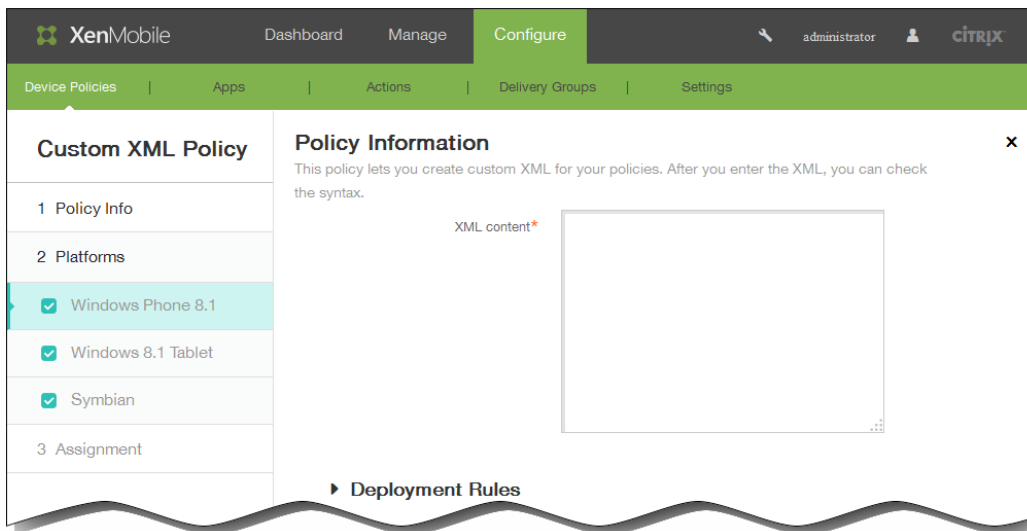


4. In the Policy Information pane, enter the following information:

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

5. Click Next. The Policy Platforms page appears.

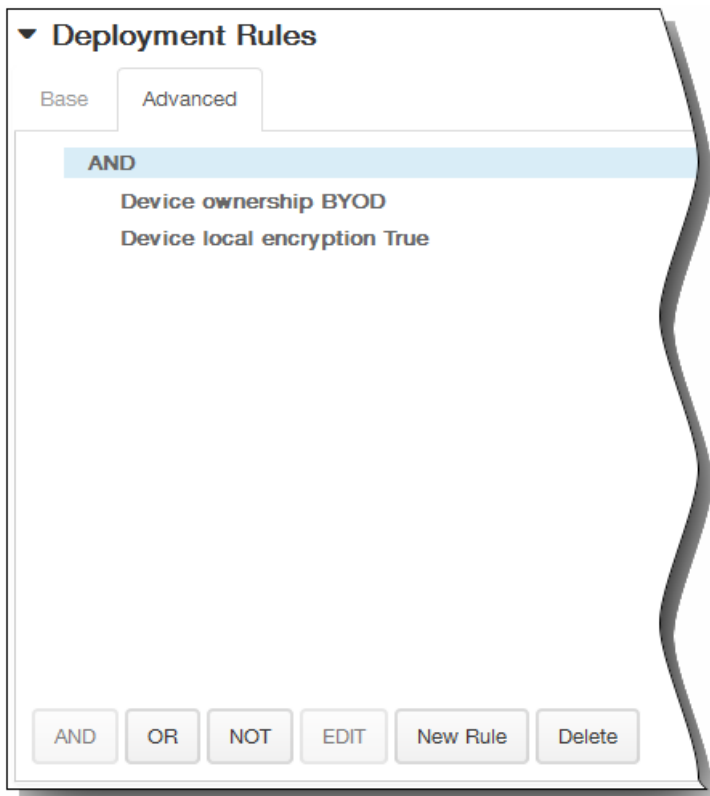
Note: When the Policy Platforms page appears, all platforms are selected and you see the Windows Phone 8.1 platform configuration panel first.



6. Under Platforms, ensure only the platforms you want to add are checked.
7. In XML content, enter the custom XML code you want to add to the policy. If the content is long, you can cut and paste the code from the source file.
8. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

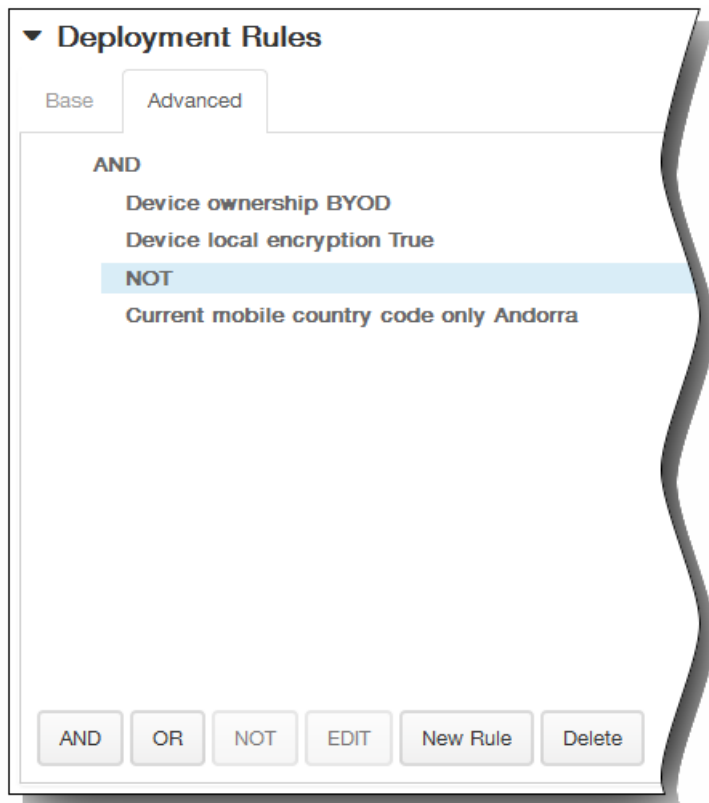


The conditions you chose on the Base tab appear.

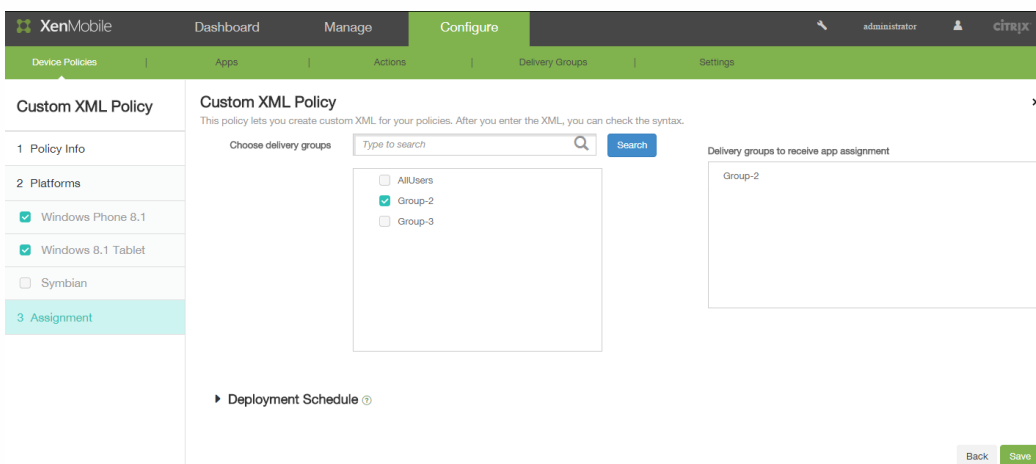
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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 right-hand Delivery groups to receive app assignment list.



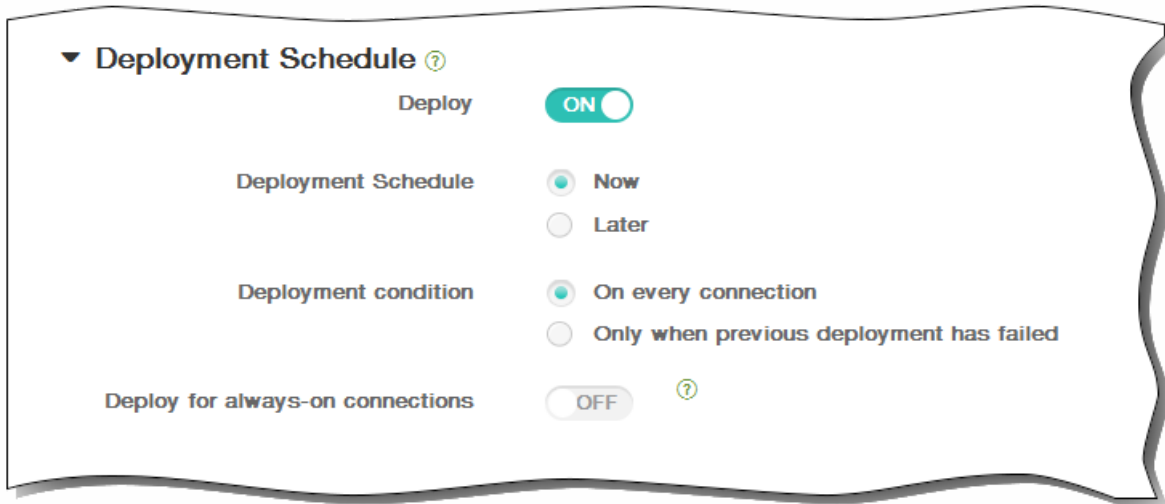
11. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The

default option is On every connection.

5. 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.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms.



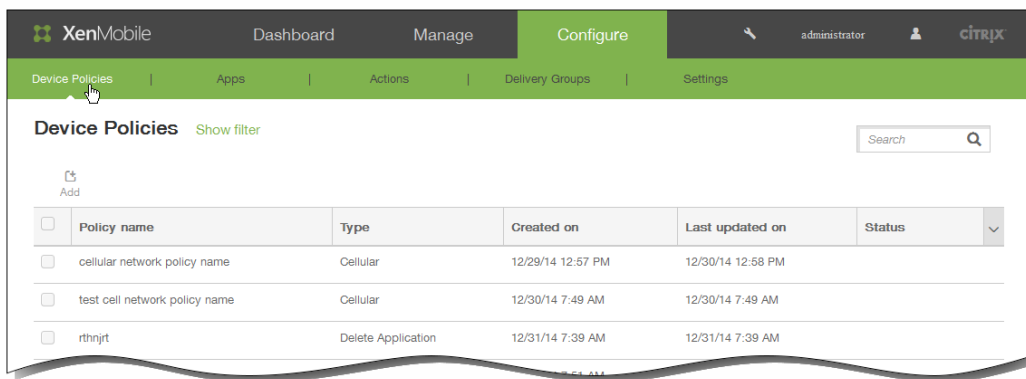
12. Click Save to save the policy.

App uninstall device policies

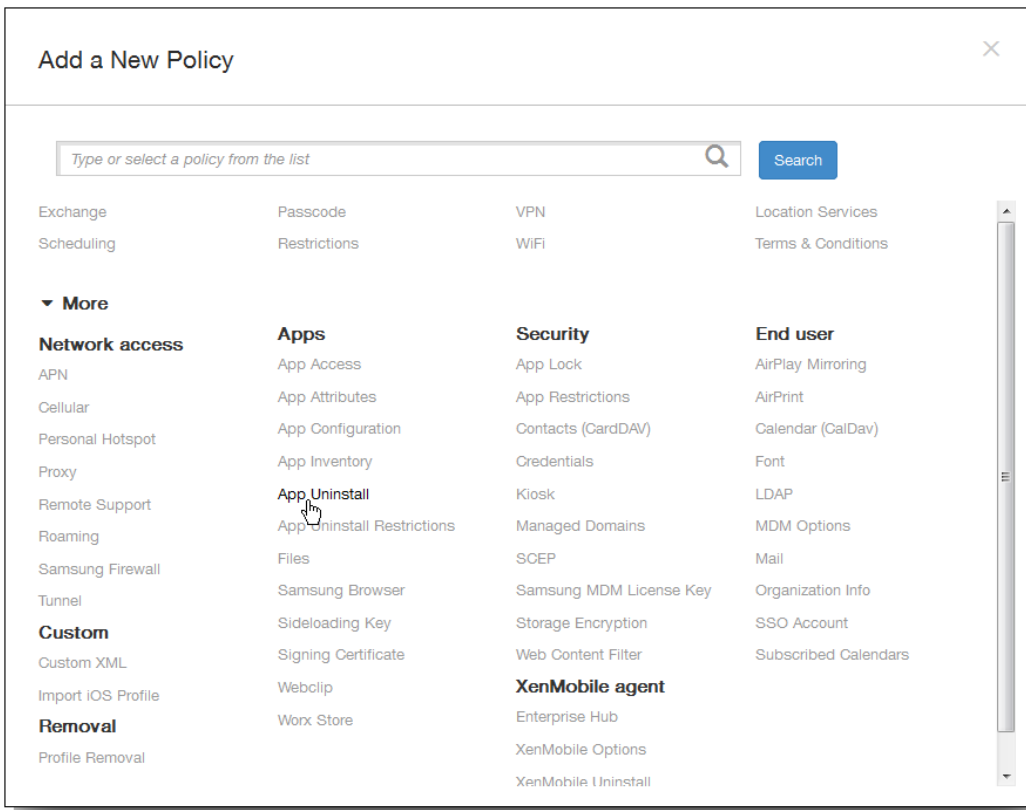
Apr 13, 2015

You can create an app uninstall policy for iOS, Android, Samsung KNOX, and Windows 8.1 Tablet 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.

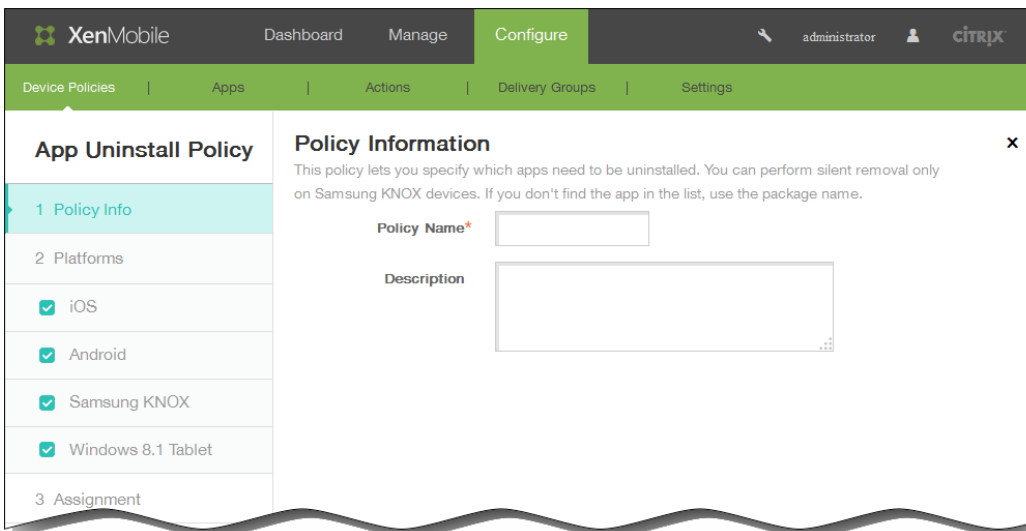
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears. On the Device Policies page, click Add.



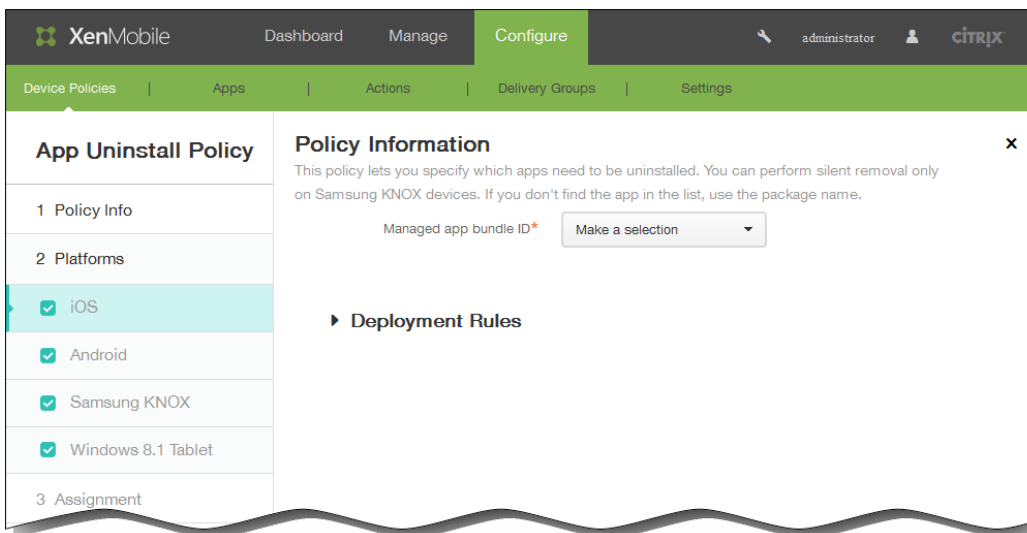
2. On the Add a New Policy dialog box, click More and then, under Apps, click App Uninstall.



3. In the App Uninstall Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Type an optional description of the policy.
 3. Click Next.



4. When the Policy Platforms page appears, all platforms are selected and you see the iOS platform configuration panel first. Under Platforms, select the platform or platforms you want to add, and de-select those you don't.

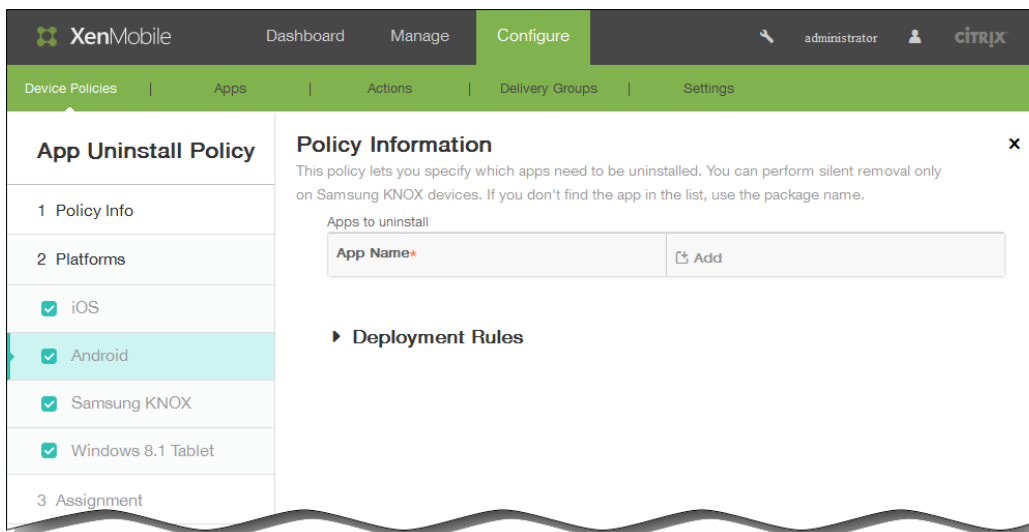


5. Configure the following settings based on the platforms you selected.

1. If you selected, iOS, in the list Managed app bundle ID, click an existing app or click Add new.

Note: 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.

2. If you chose Android, Samsung KNOX, or Windows 8.1 Tablet:



Under Apps to uninstall, click Add and then do the following:

1. App name: In the list, click an existing app or click Add new to enter a new app name.

Note: If there are no apps configured for this platform, the list will be empty and you must add new apps.

2. Click Add to add the app or click Cancel to cancel adding the app.

3. Repeat steps i. and ii. for each app you want to add to the uninstall policy.

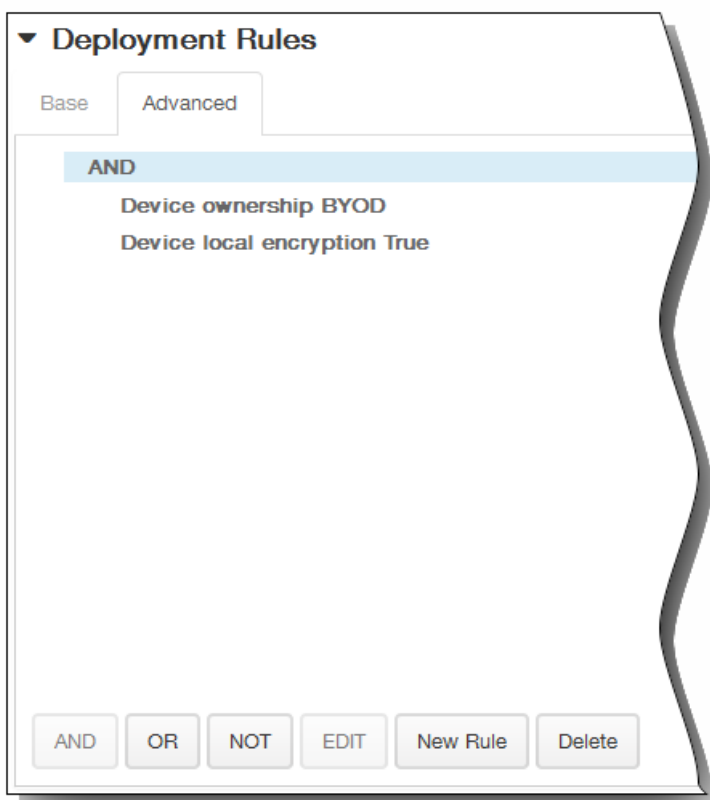
Note: To delete an existing app from the uninstall policy, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing.

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.

6. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.

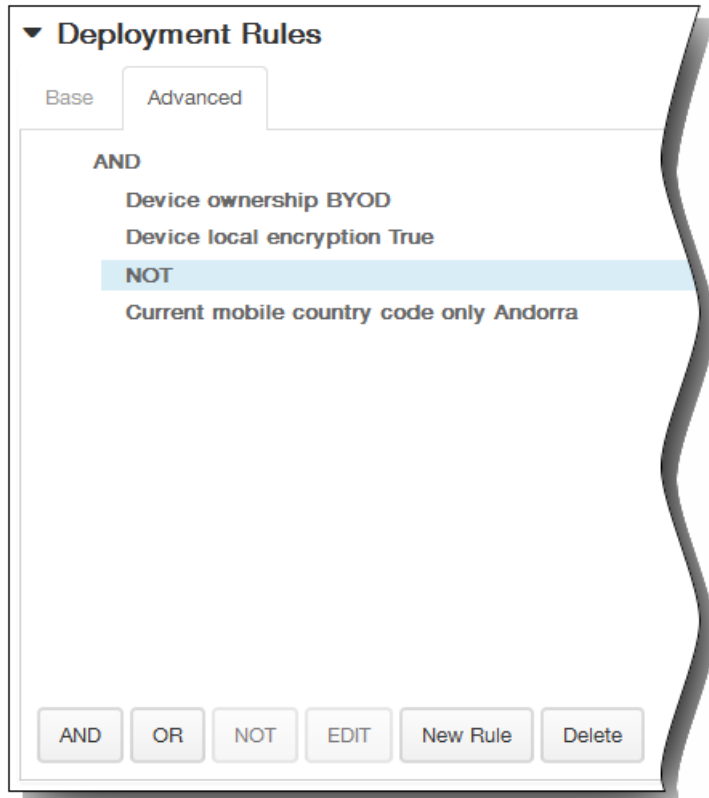


1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

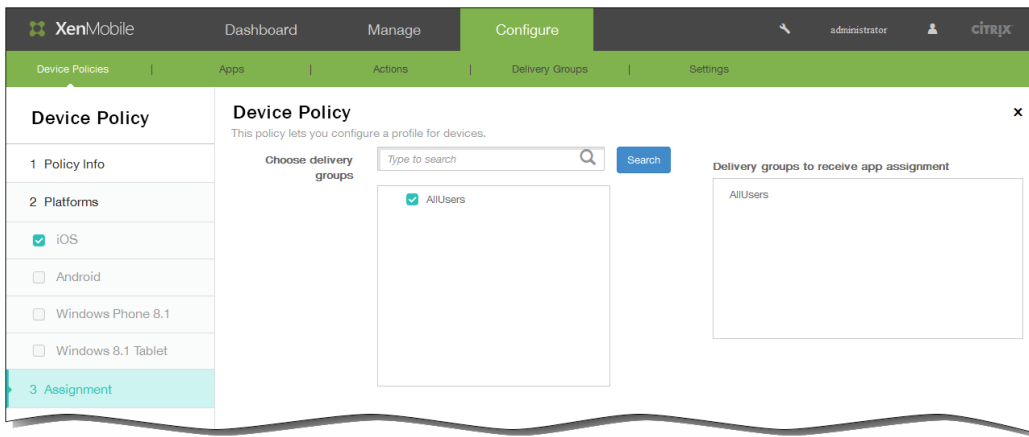


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
3. Click New Rule again if you want to add more conditions.
In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



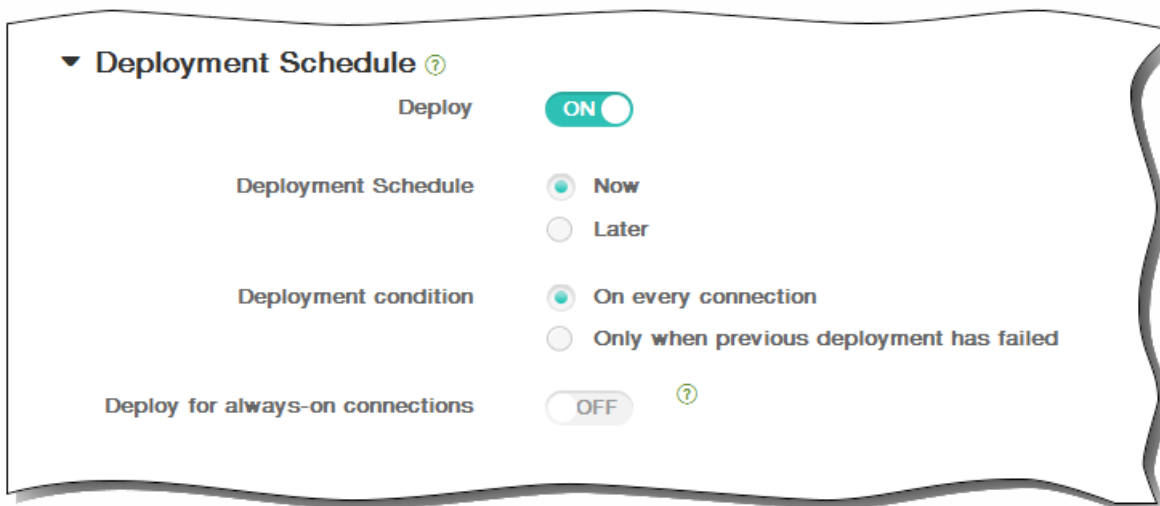
7. Click Next. The App Uninstall Policy assignment page appears.
8. Next to Choose delivery groups, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand Delivery groups to receive app assignment list.



9. Expand Deployment Schedule and then configure the following settings:


1. 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.
2. Next to Deployment schedule, click Now or Later. The default option is Now.
3. If you click Later, click the calendar icon and then select the date and time for deployment.
4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
 Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



10. Click Save to save the policy. On the Device Policies page, the Type column lists the policy you added as a Delete Application type.

Device Policies [Show filter](#)

 Add

<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status	▼
<input type="checkbox"/>	appuninstall	Delete Application	1/27/15 8:46 AM	1/27/15 8:46 AM		
<input type="checkbox"/>	test	Terms Conditions	2/11/15 8:16 AM	2/11/15 8:16 AM		
<input type="checkbox"/>	test-uninstall	Delete Application	2/17/15 10:22 AM	2/17/15 10:22 AM		
<input type="checkbox"/>	App app uninstall	Delete Application	2/17/15 10:55 AM	2/17/15 10:55 AM		

To add an APN policy

Feb 13, 2015

This policy allows you to configure a custom Access Point Name (APN) on an iOS, Android, or Samsung KNOX 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.

1. In the XenMobile console, click Configure > Device Policies > Add.
2. On the Add a New Policy page, click More and then under Network Access, click APN.
3. Select the platforms you want to include in the policy. Configuration pages for the selected platform appear in Step 5.
4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The first platform information page appears.
6. If you selected the iOS platform, on the iOS Platform Information Page, do the following:

Policy Information
This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN*

User name

Password

Server proxy address

Server proxy port

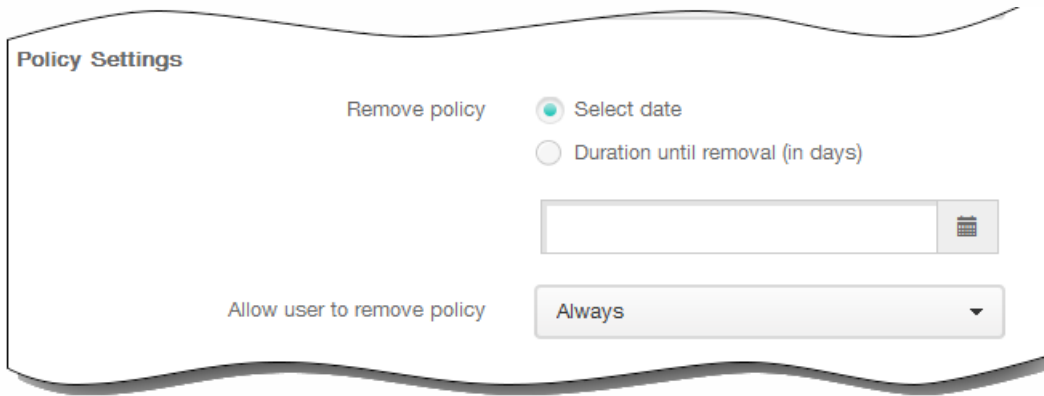
Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy

▶ Deployment Rules

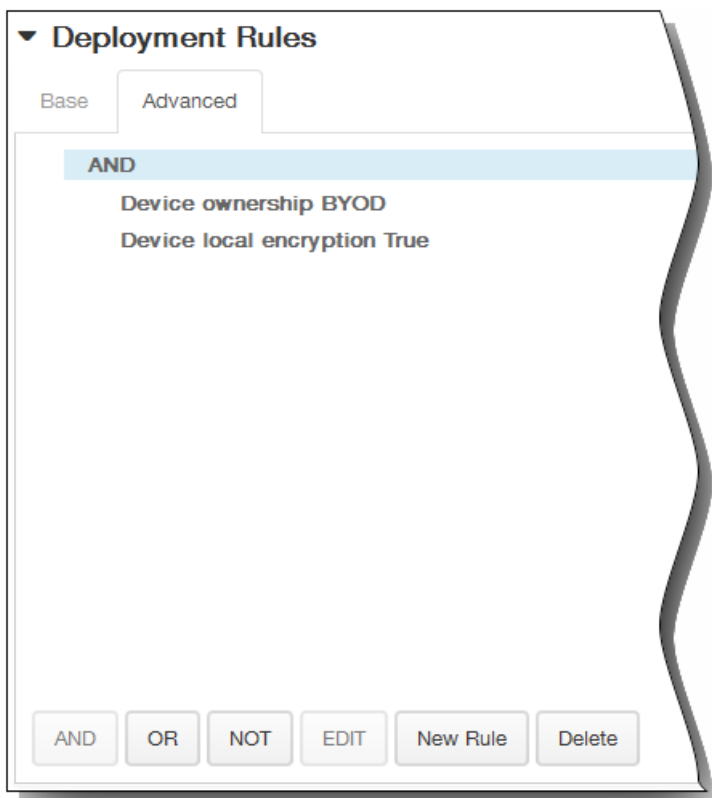
1. APN. Type the name of the access point.
2. User name. This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
3. Password. The password for the user for this APN. For obfuscation purposes, the password is encoded. If it is missing from the payload, the device prompts for the password during profile installation.
4. Server proxy address. The IP address or URL of the APN proxy.
5. Server proxy port. The port number for the APN proxy.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.

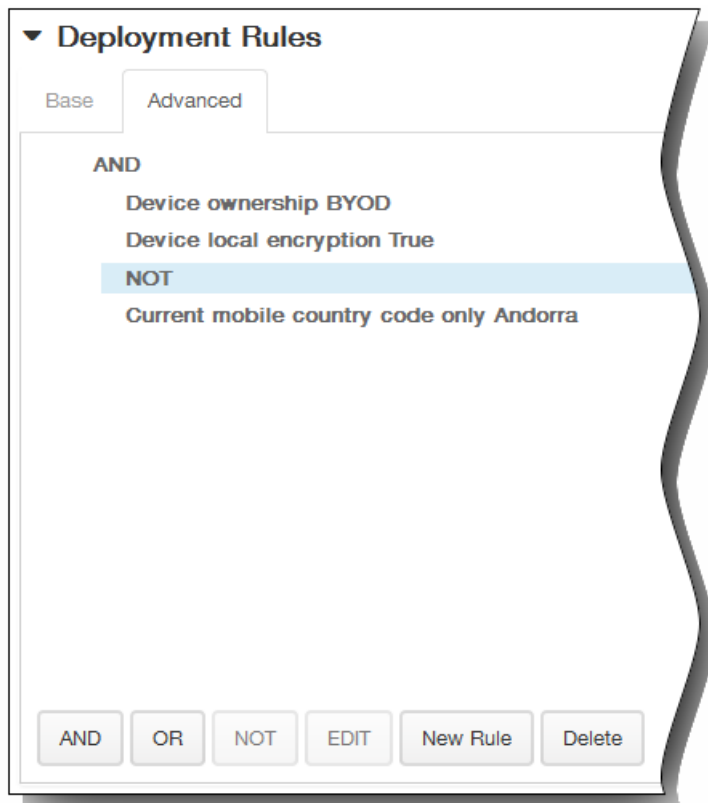
1. Click AND, OR, or NOT.

2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. If you selected the Android or Samsung KNOX platforms, on the platform information page, do the following:

Policy Information

This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN*

User name

Password

Server

APN type

Authentication type **None** ▼

Server proxy address

Server proxy port

MMS

Multimedia Messaging Server (MMS) proxy address

MMS port

► Deployment Rules

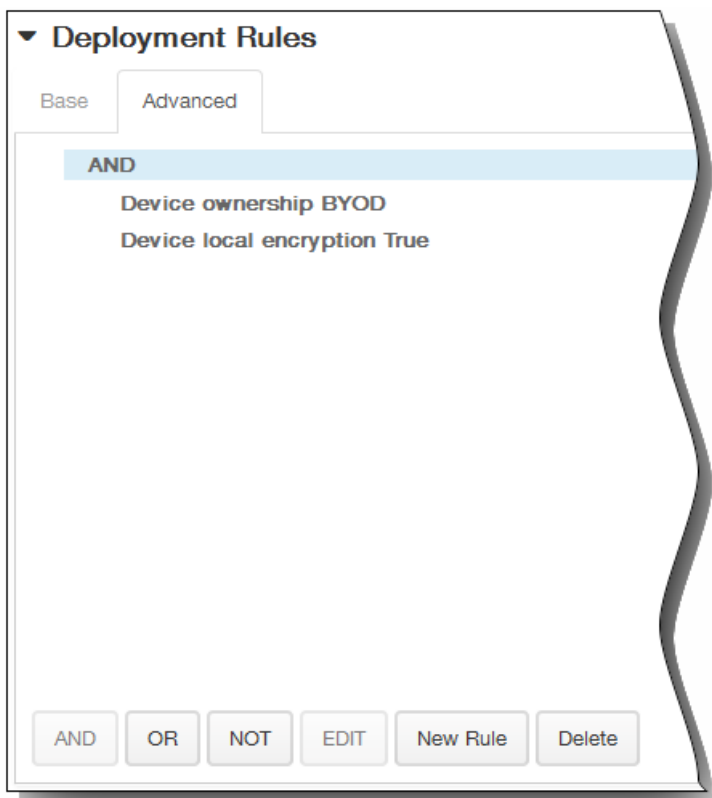
1. APN. Enter the name of the access point.
2. User name. This string specifies the user name for this APN. If the user name is missing, the device prompts for the

string during profile installation.

3. 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.
 4. Server. This setting, which predates smart phones, is usually empty. It references a Wireless Application Protocol (WAP) gateway server for phones that could not access or render standard websites.
 5. 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 an outdated and should rarely be used.
 - hipri. High priority networking.
 - fota. Firmware over the air is used for receiving firmware updates.
 6. Authentication type. Must contain either PAP, CHAP, or PAP or CHAP. Defaults to None.
 7. Server proxy address. The IP address or URL of the APN proxy.
 8. Server proxy port. The port number for the APN proxy.
 9. MMSC. This is 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).
 10. Multimedia Messaging Server (MMS) proxy address. This is an HTTP proxy server for MMS traffic.
 11. MMS port. The port used by the MMS proxy.
13. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.

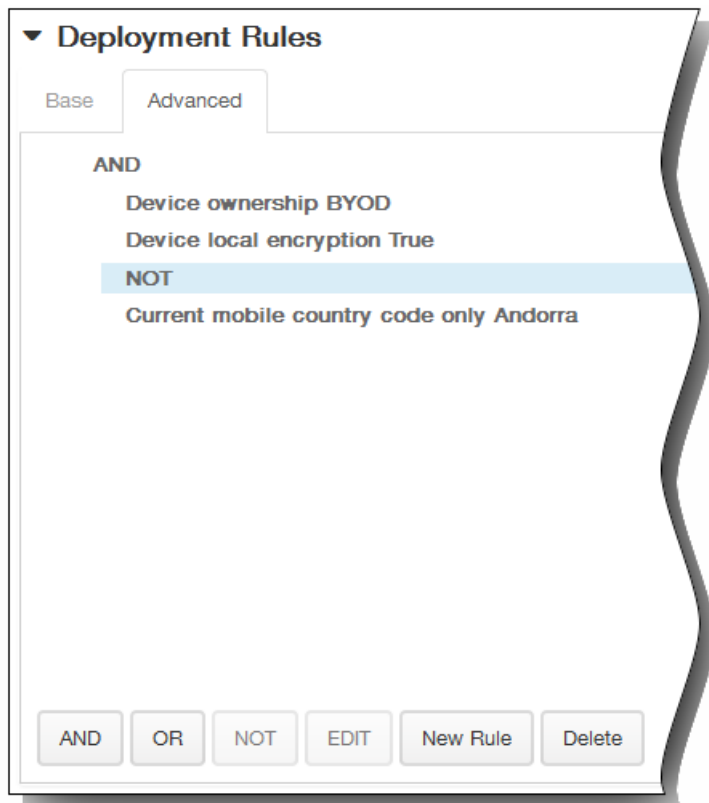
1. Click AND, OR, or NOT.

2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

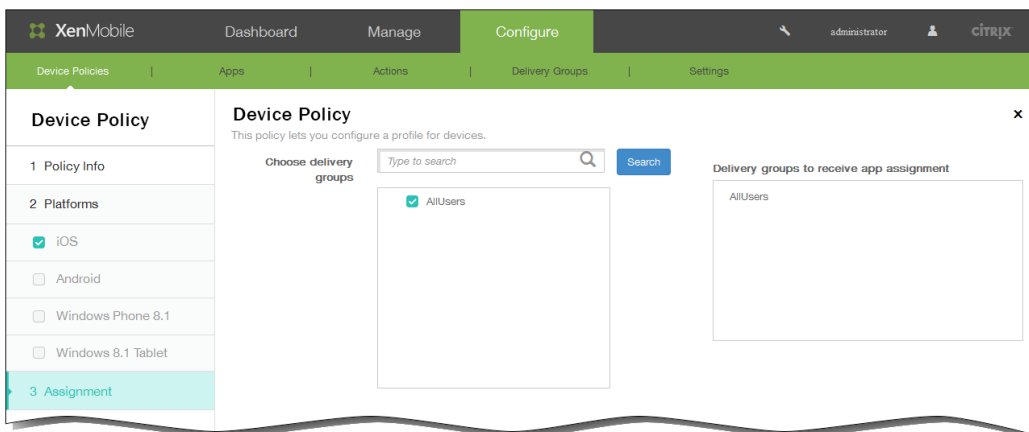
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



14. If you selected both the Android or Samsung KNOX platforms, repeat Step 8 to complete the Samsung KNOX Platform Information page and then click Next. The APN Policy Assignment page appears.
15. Next to Choose delivery groups, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand Delivery groups to receive app assignment list.



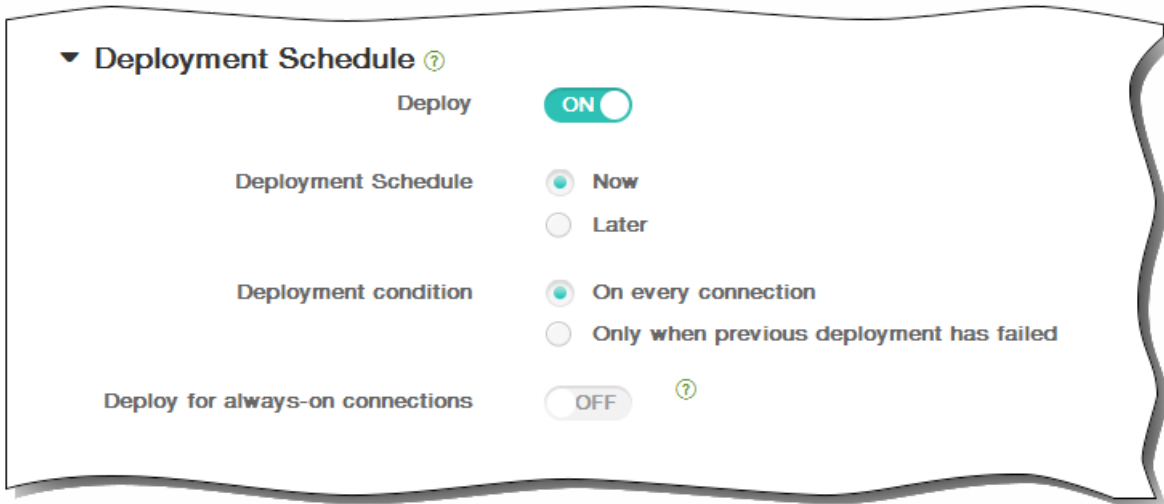
16. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The

default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



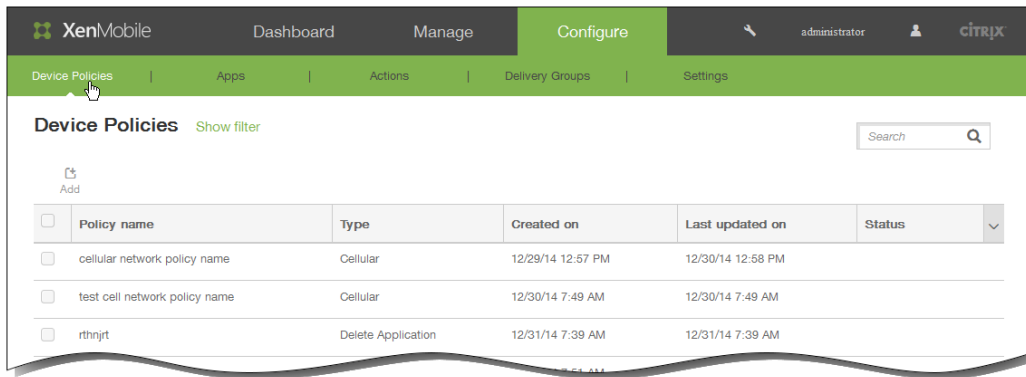
17. Click Save to save the policy.

To add a cellular device policy for iOS

Feb 27, 2015

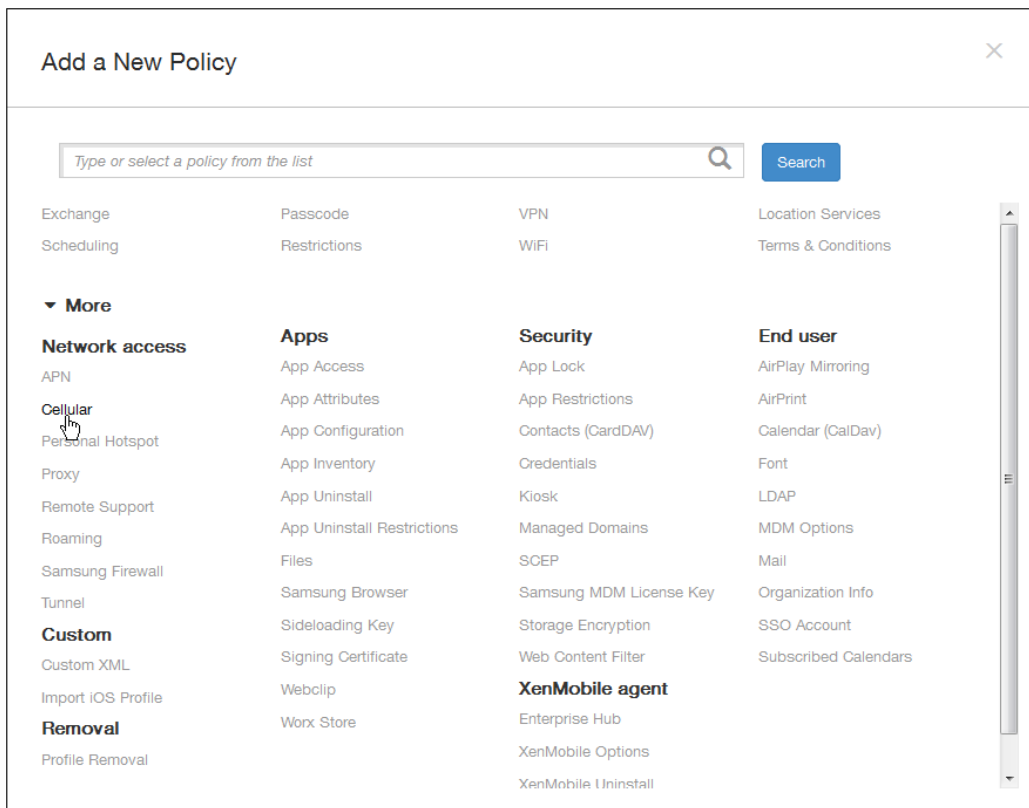
This policy allows you to configure cellular network settings on an iOS device.

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



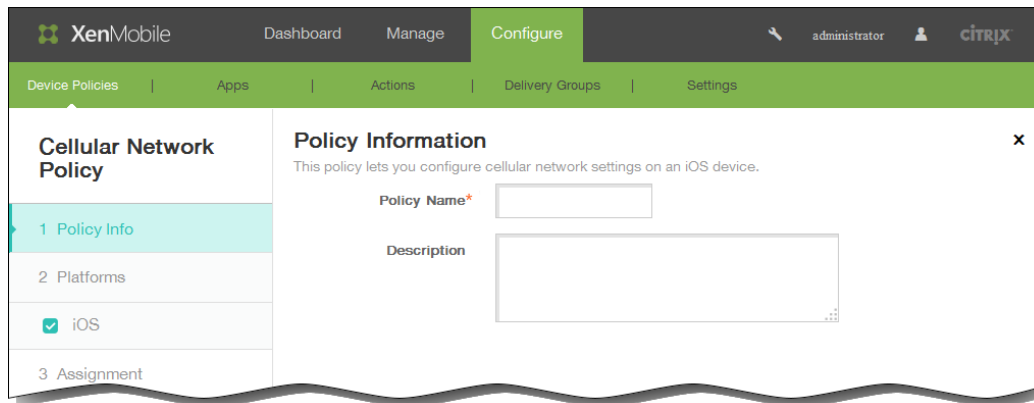
2. Click Add.

The Add a New Policy page appears.



3. On the Add a New Policy page, click More and then under Network Access, click Cellular.

The Cellular Network Policy information page appears.



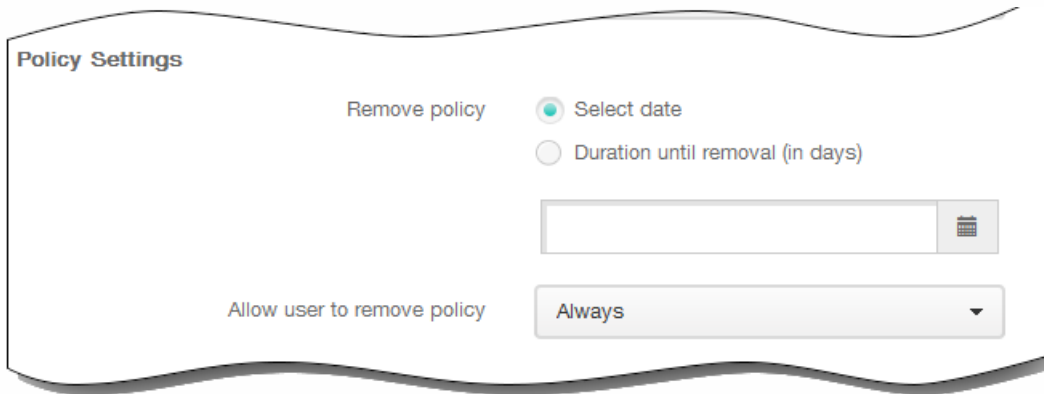
4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform information page appears.

The screenshot shows the XenMobile Configure page for Cellular Network Policy. The left sidebar has 'Cellular Network Policy' selected, with sub-items: 1 Policy Info, 2 Platforms, 3 Assignment. The 'iOS' platform is selected. The main area is titled 'Policy Information' and contains the following sections:

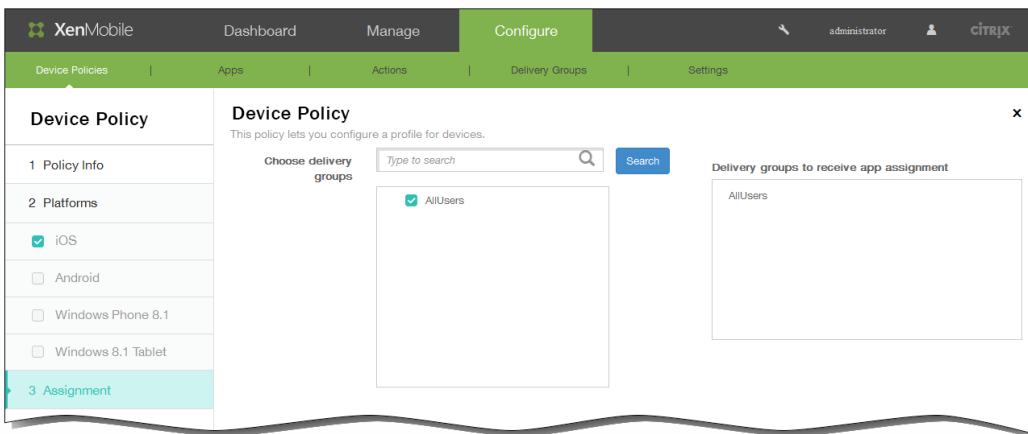
- Attach APN:** Name (text input), Authentication type (dropdown menu, PAP selected), User name (text input), Password (text input).
- APN:** Name (text input), Authentication type (dropdown menu, PAP selected), User name (text input), Password (text input), Proxy server (text input), Proxy server port (text input).
- Policy Settings:** Remove policy (radio buttons for 'Select date' and 'Duration until removal (in days)'), a calendar icon, and 'Allow user to remove policy' (dropdown menu, 'Always' selected).
- Deployment Rules:** A section header with a right-pointing arrow.

At the bottom right, there are 'Back' and 'Next >' buttons.

6. On the iOS Platform Information page, enter the following information: Under **Attach APN**:
 1. Name: Type a name for this configuration.
 2. Authentication type: In the list, click Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP). The default is PAP.
 3. User name: Type a user name used for authentication.
 4. Password: Type a password used for authentication.
- Under **APN**:
 1. Name: Type a name for the Access Point Name (APN) configuration.
 2. Authentication type: In the list, click CHAP or PAP. The default is PAP.
 3. User name: Type a user name used for authentication.
 4. Password: Type a password used for authentication.
 5. Proxy server: Type the proxy server network address.
 6. Proxy server port: Type the proxy server port.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



11. 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.



12. Expand Deployment Schedule and then configure the following settings:
 1. 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.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
 Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.

▼ **Deployment Schedule** ?

Deploy ON

Deployment Schedule Now
 Later

Deployment condition On every connection
 Only when previous deployment has failed

Deploy for always-on connections OFF ?

13. Click Save to save the policy.

To add an Enterprise Hub device policy for Windows Phone 8.1

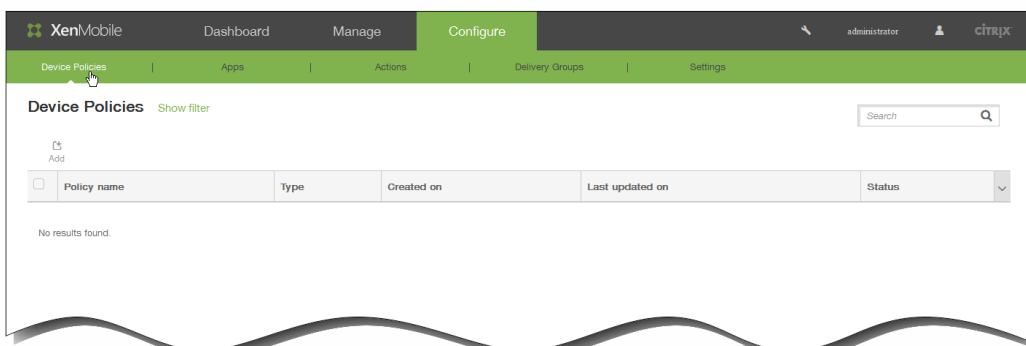
Feb 13, 2015

An Enterprise Hub device policy for Windows Phone 8.1 lets you distribute apps through the Enterprise Hub Company store.

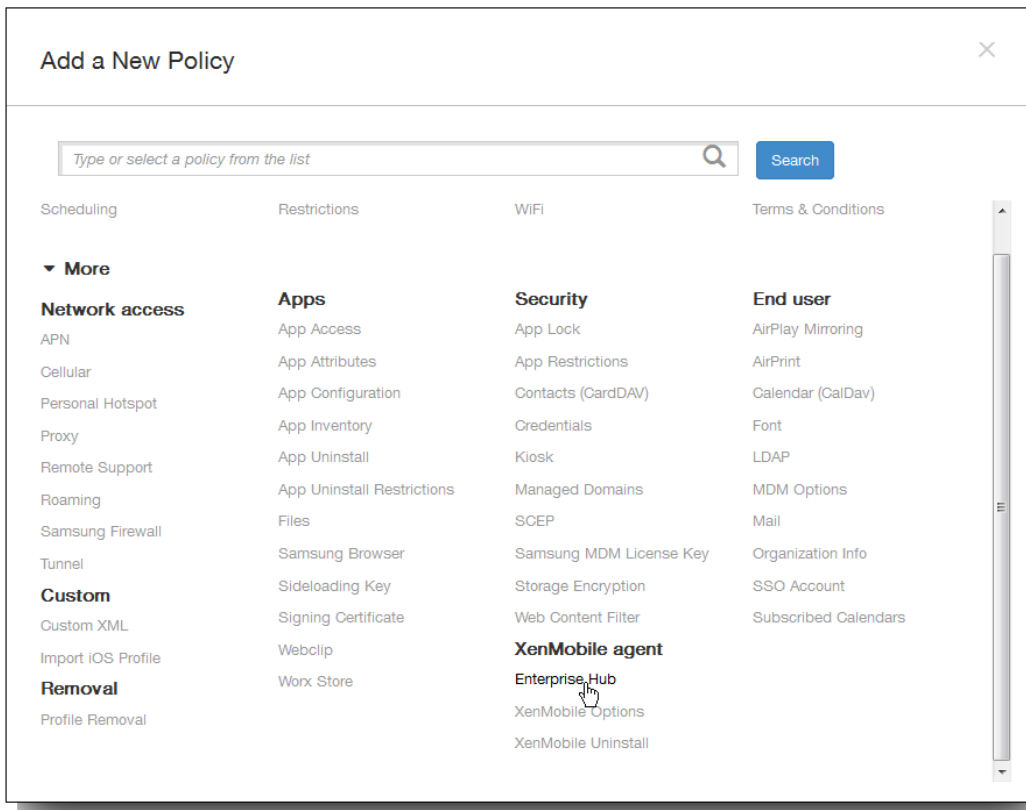
Before you can create the policy, you need the following:

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

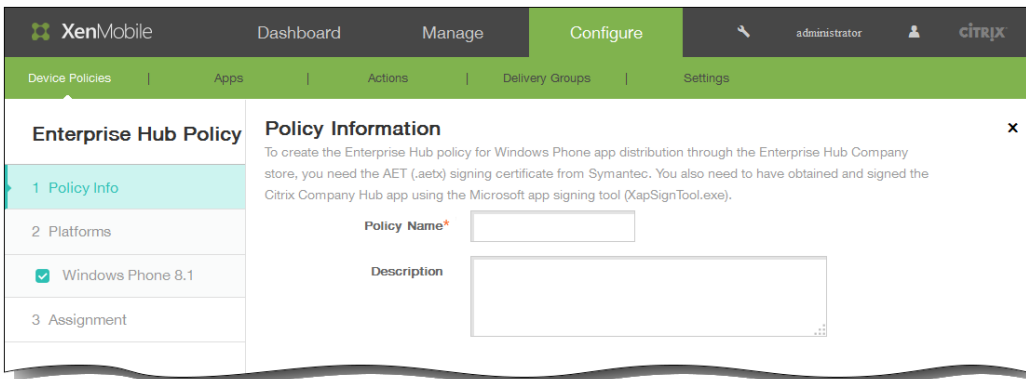
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



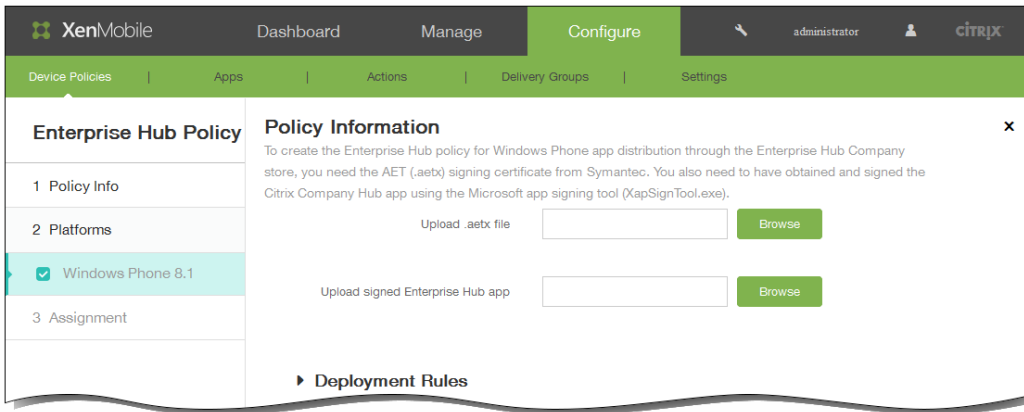
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



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



4. In the Policy Information pane, enter the following information:
 1. Policy Name: Enter a descriptive name for the policy.
 2. Description: If desired, enter a description of the policy.
5. Click Next. The Windows Phone 8.1 platform page appears.

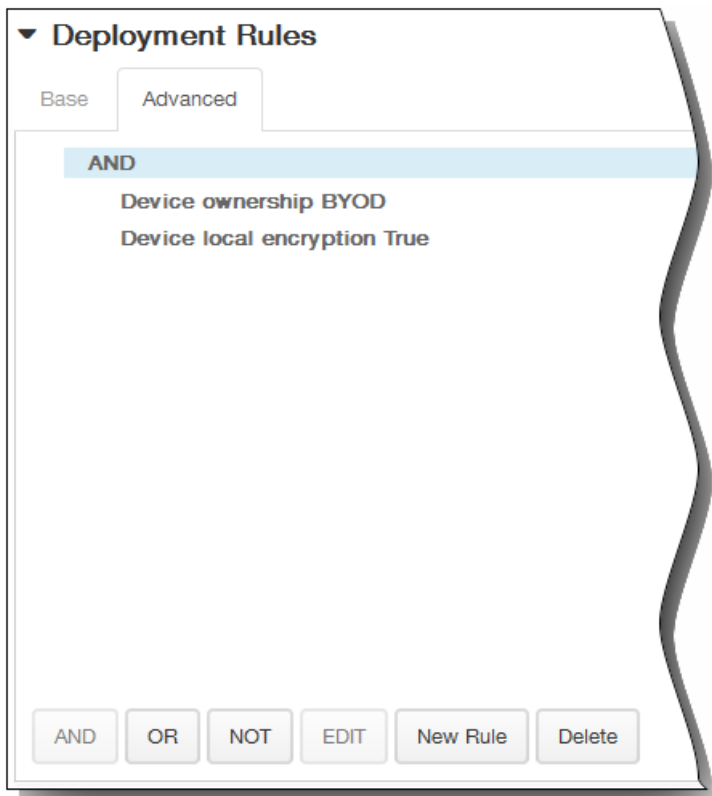


6. Configure the following settings:

1. Upload .aetx file: Browse to the location of the .aetx file and then select the file.
 2. Upload signed Enterprise Hub app: Browse to the location of the Enterprise Hub app and then select the app.
7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.

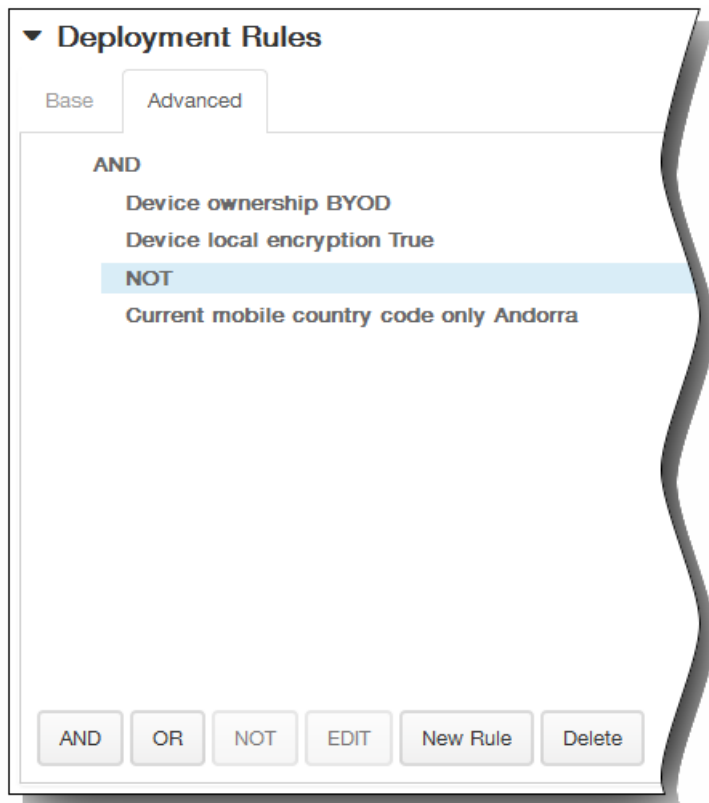
1. Click AND, OR, or NOT.

2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

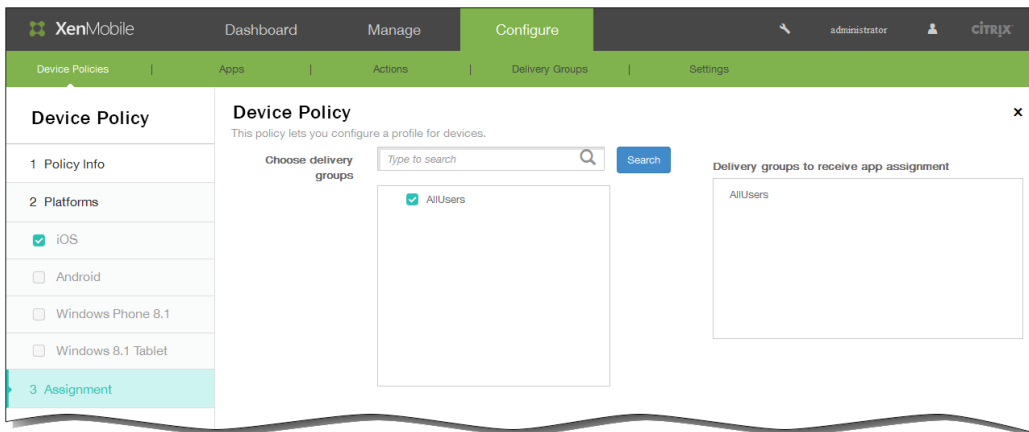
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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.

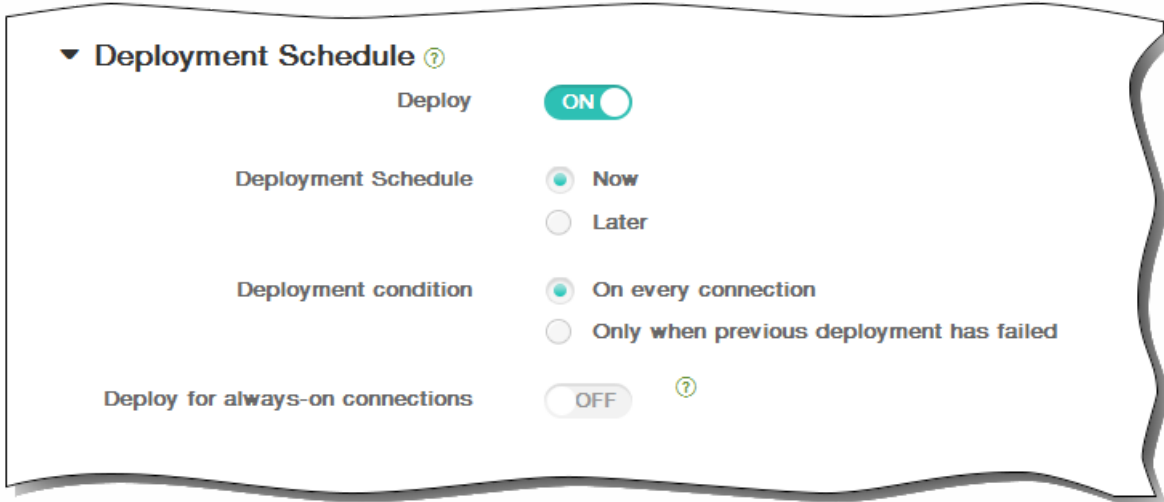


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

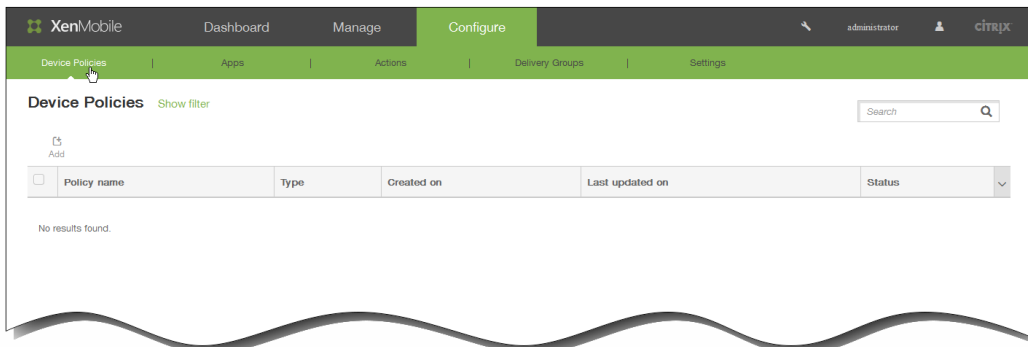
Microsoft Exchange ActiveSync device policies

Feb 13, 2015

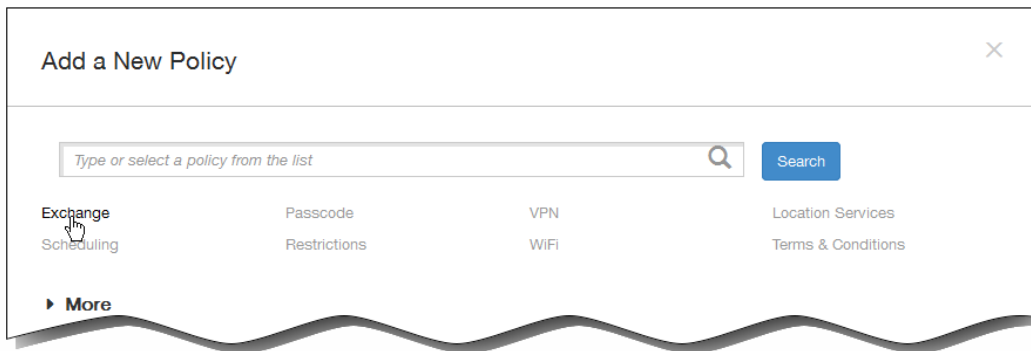
You can use the Exchange ActiveSync device policy to configure an email client on users' devices to let them access their corporate email hosted on Exchange. You can create policies for iOS, Android HTC, Android TouchDown, Samsung SAFE, Samsung KNOX, and Windows Phone 8.1. Each platform requires a different set of values, which are described in detail in the following topics:

Before you can create this policy, you will need to know the host name or IP address of the Exchange Server.

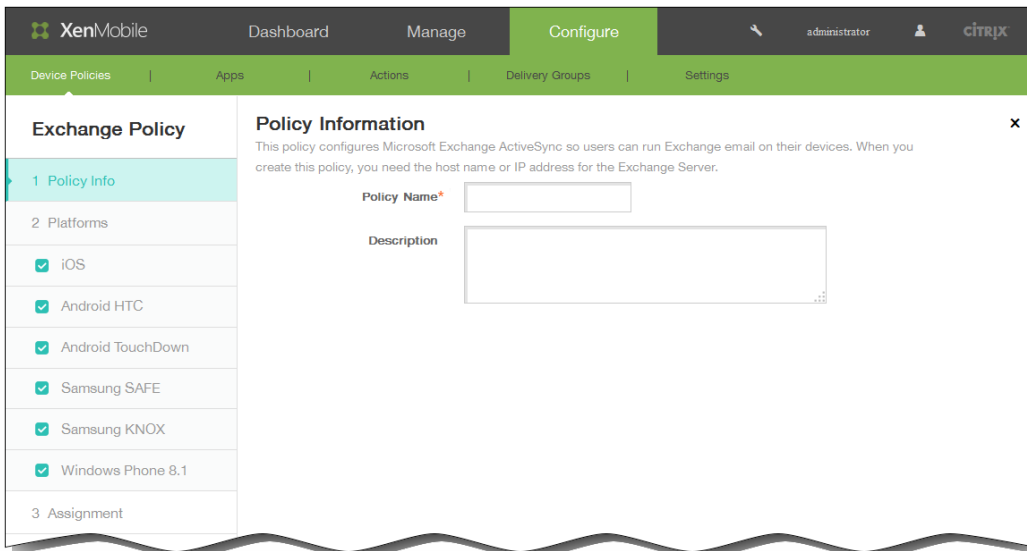
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



2. Click Add to add a new policy. The Add New Policy dialog appears.



3. Click Exchange. The Exchange Policy information page appears.

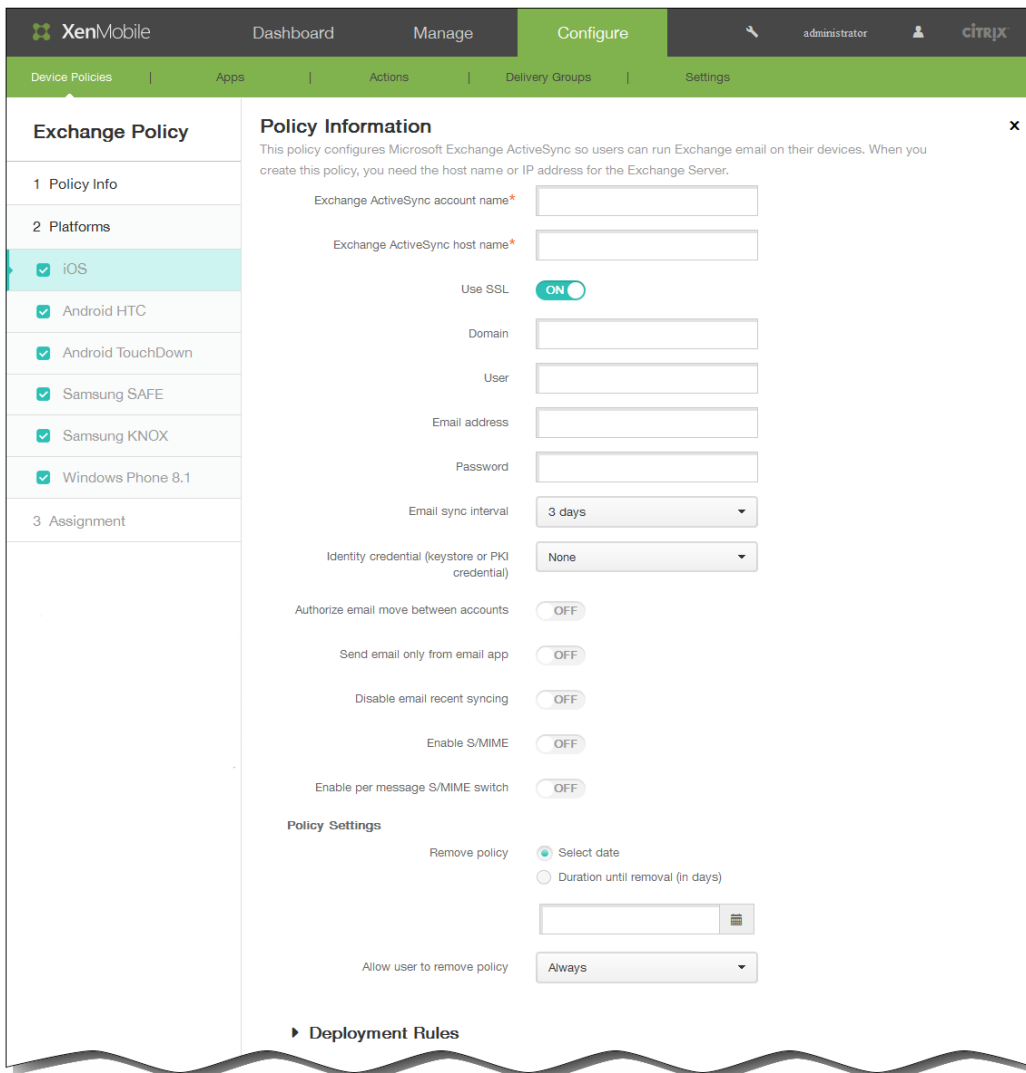


4. In the Policy Information pane, type the following information:

1. Policy Name: Type a descriptive name for the policy.
2. Description: Type an optional 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 configuration panel first.



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

- If you selected iOS, configure the following 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.

Note: 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.

Note: 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.

Note: 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.

- If you selected Android HTC, configure the following settings:

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The top navigation bar includes 'Dashboard', 'Manage', and 'Configure'. The left sidebar lists 'Device Policies', 'Apps', 'Actions', 'Delivery Groups', and 'Settings'. The main content area is titled 'Exchange Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several options are checked: iOS, Android HTC, Android TouchDown, Samsung SAFE, Samsung KNOX, and Windows Phone 8.1. The 'Policy Information' section contains the following fields: 'Configuration display name*' (text input), 'Server address*' (text input), 'User ID*' (text input), 'Password' (text input), 'Domain' (text input), 'Email address*' (text input), and 'Use SSL' (toggle switch, currently ON). A 'Deployment Rules' section is partially visible at the bottom.

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.

Note: 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.

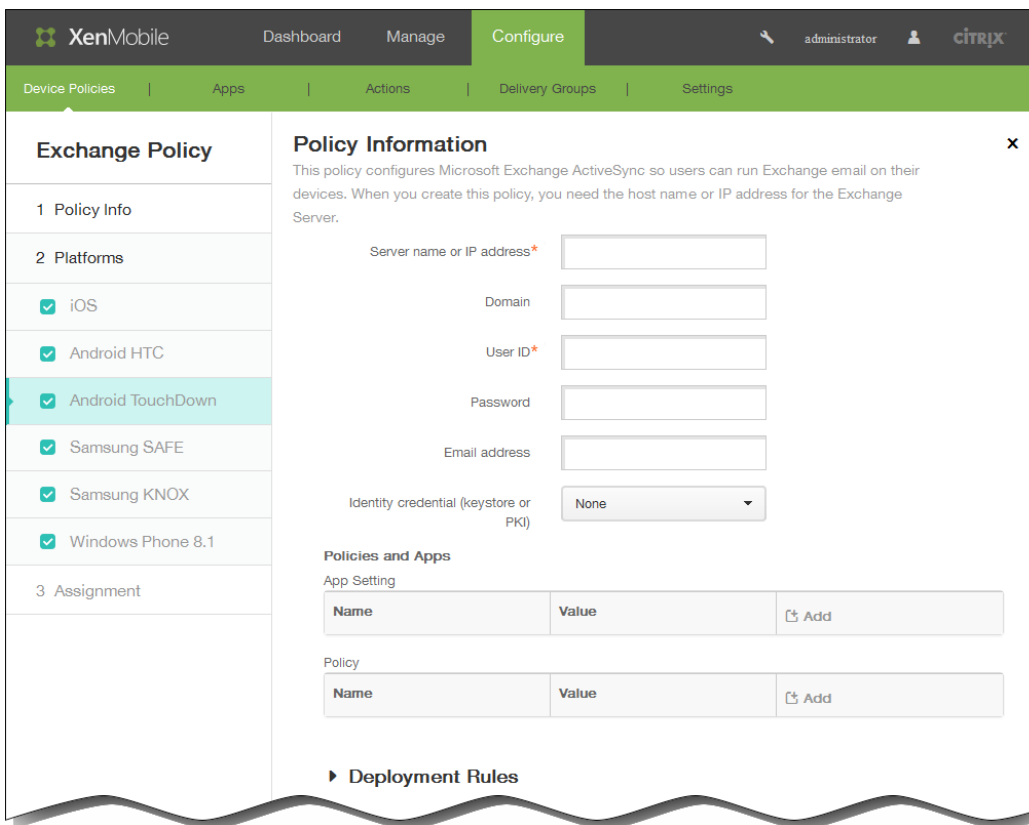
Note: You can use the system macro `${user.domainname}` in this field to automatically look up users' domain names.

Email address: Specify the user's full email address.

Note: 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.

- If you selected Android TouchDown, configure the following 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.

Note: 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.

Note: 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.

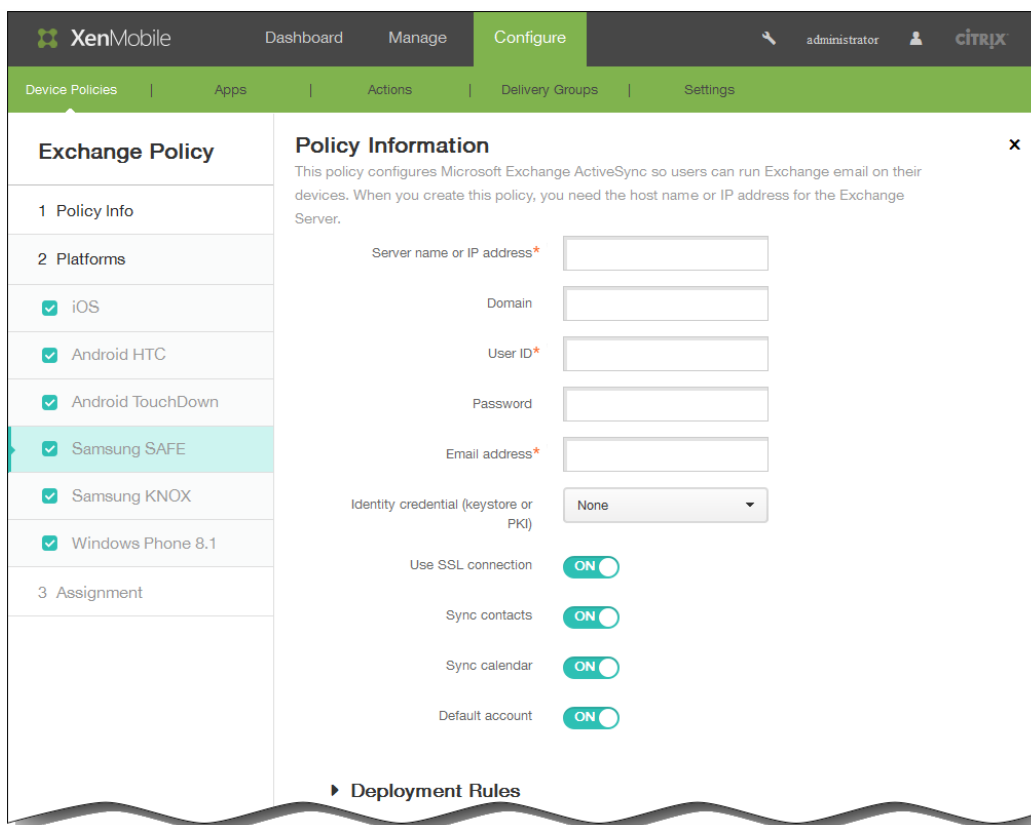
Note: You can use the system macro `${user.mail}` in this field to automatically look up users' email accounts.

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.

App Setting: Optionally, add TouchDown app settings for this policy.

Policy: Optionally, add TouchDown policies for this policy.

- If you selected Samsung SAFE or Samsung KNOX, configure the following 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.

Note: 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.

Note: 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.

Note: 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.

- If you selected Windows Phone 8.1, configure the following 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.

The screenshot shows the XenMobile 'Configure' interface for an 'Exchange Policy'. The left sidebar lists sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several options are checked: iOS, Android HTC, Android TouchDown, Samsung SAFE, Samsung KNOX, and Windows Phone 8.1. The main area is titled 'Policy Information' and contains the following fields and controls:

- Account name or display name***: Text input field.
- Server name or IP address***: Text input field.
- Domain**: Text input field.
- User ID or user name***: Text input field.
- Email address***: Text input field.
- Use SSL connection**: Toggle switch set to 'OFF'.
- Sync items**: 'Past days to sync' dropdown menu set to 'All content'.
- Sync scheduling**: 'Frequency' dropdown menu set to 'When item arrives'.
- Logging level**: Dropdown menu set to 'Disabled'.
- Deployment Rules**: A section header with a right-pointing arrow.

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.

Note: 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.

Note: 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.

Note: 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.

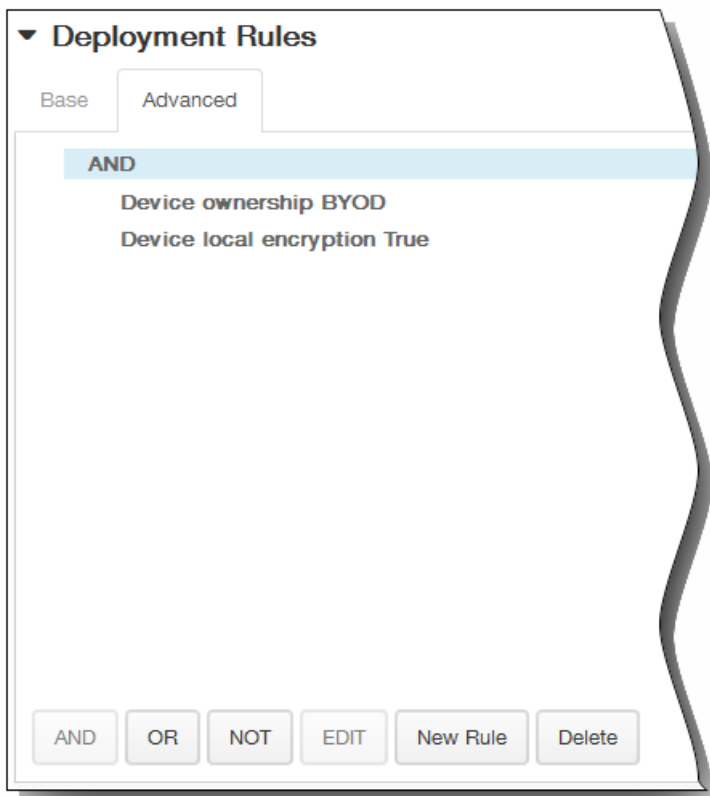
Frequency: In the list, click the schedule to use when syncing data that is sent to the device from the Exchange Server.

Logging level: In the list, click Disabled, Basic, or Advanced to specify the level of detail when logging Exchange activity.

7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

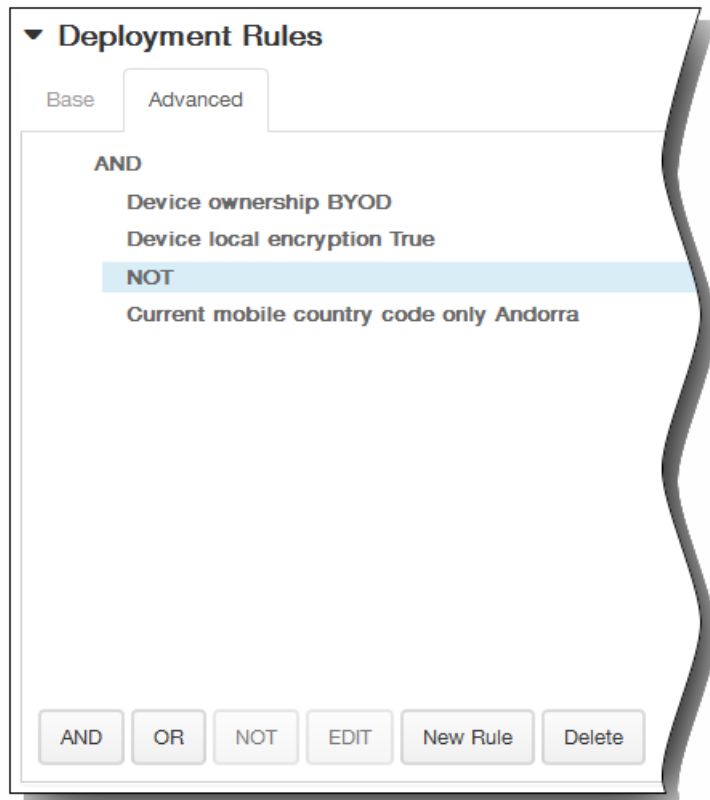


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

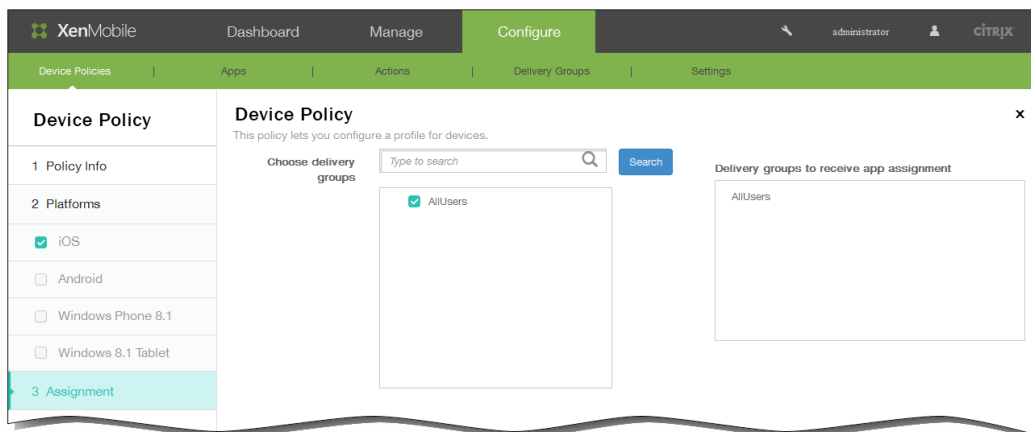
3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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 right-hand Delivery groups to receive app assignment list.

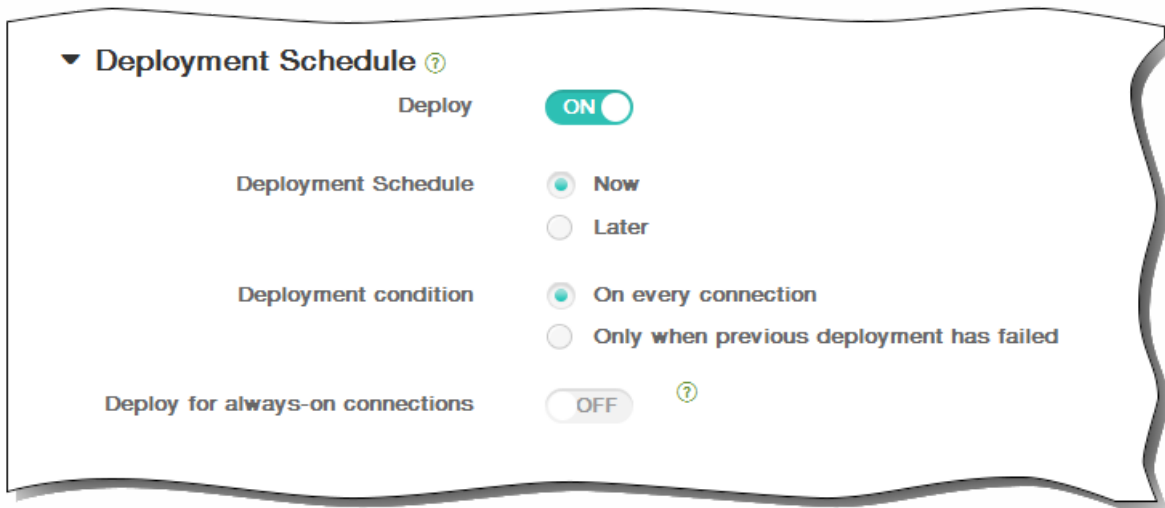


10. Expand Deployment Schedule and then configure the following settings:

1. 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.
2. Next to Deployment schedule, click Now or Later. The default option is Now.

3. If you click Later, click the calendar icon and then select the date and time for deployment.
4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save.

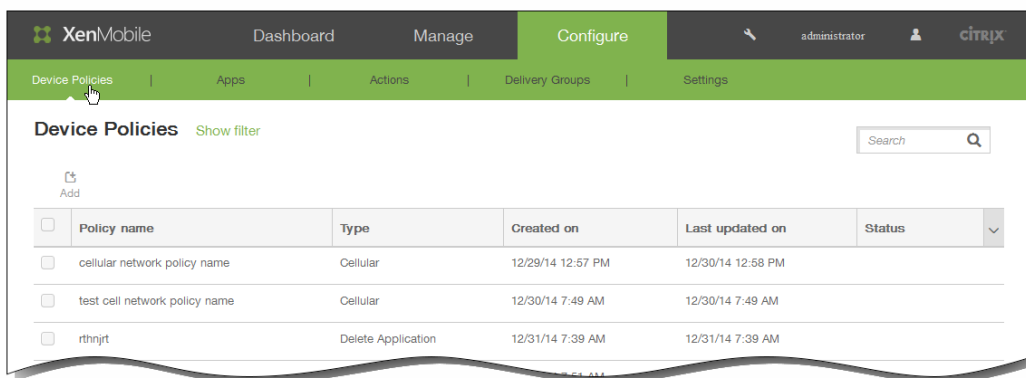
Location device policies

Apr 08, 2015

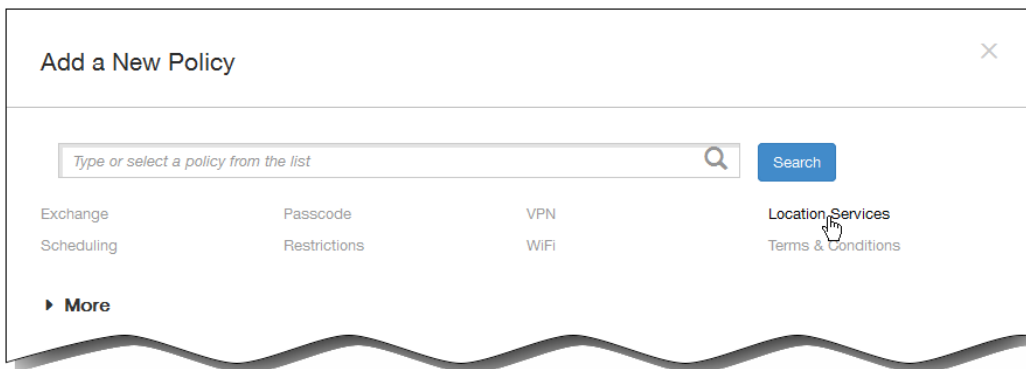
You create location device policies in XenMobile to enforce geographic boundaries, as well as to track the location and movement of users' devices. When users breach the defined boundary, also called a geofence, XenMobile can perform a selective or full wipe immediately or after a specific time period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

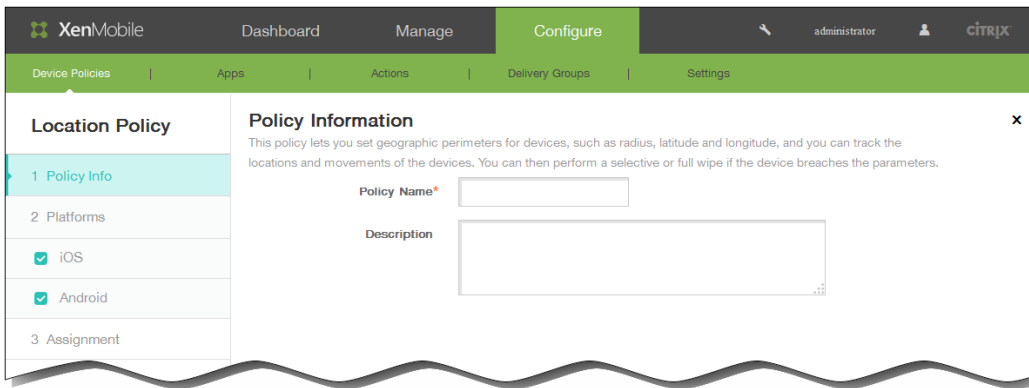
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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



3. Click Location Services. The Location Policy information page appears.

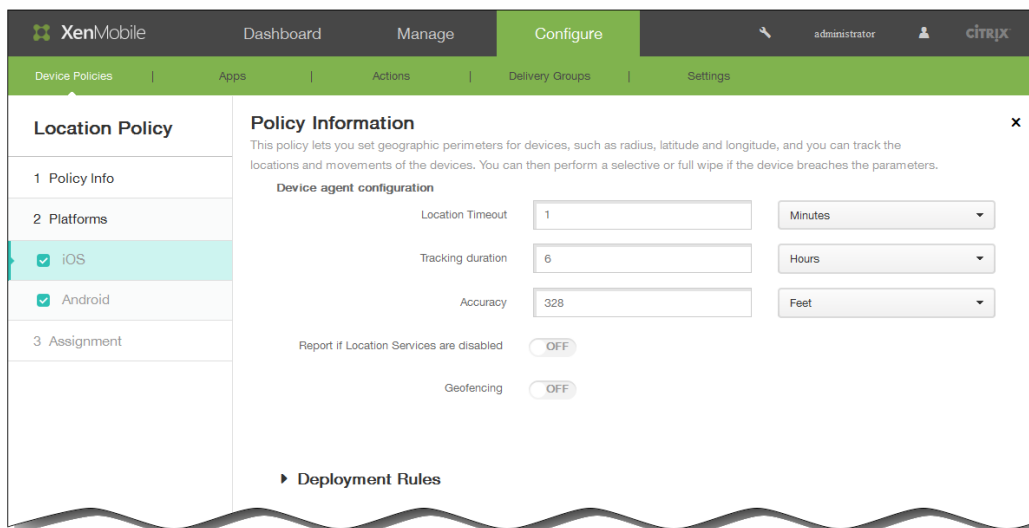


4. In the Policy Information pane, enter the following information:

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

5. Click Next. The Policy Platforms page appears.

Note: When the Policy Platforms page appears, both platforms are selected and you see the iOS platform configuration panel first.



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

- If you selected iOS, configure the following 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: Select this option to configure the following 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.
- 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.

- If you selected Android, configure these 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.
 - Note: 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: Select this option to configure the following 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.

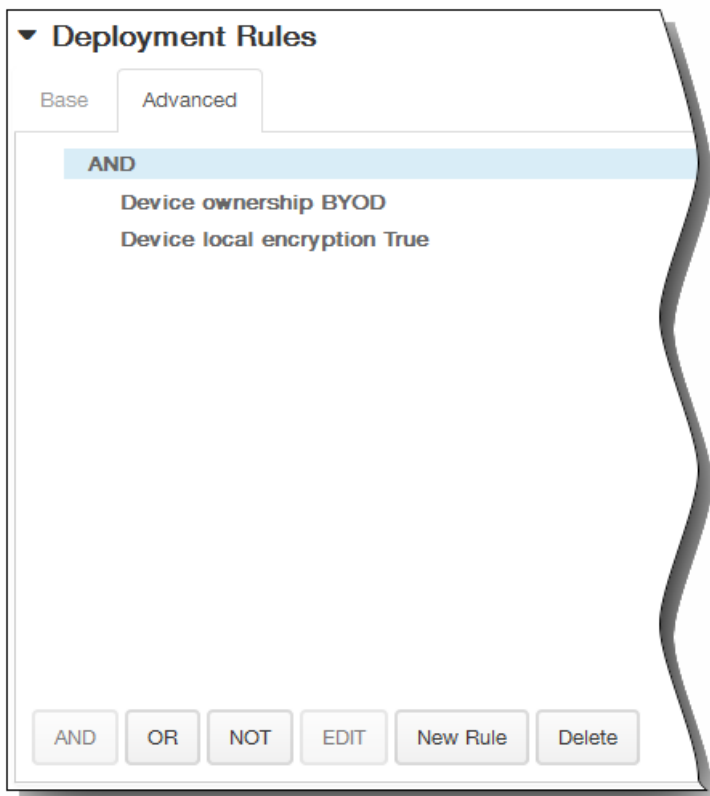
- Delay on lock: Lock users' devices after a specified length of time. When you enable this option, the Delay on lock field appears.

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. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

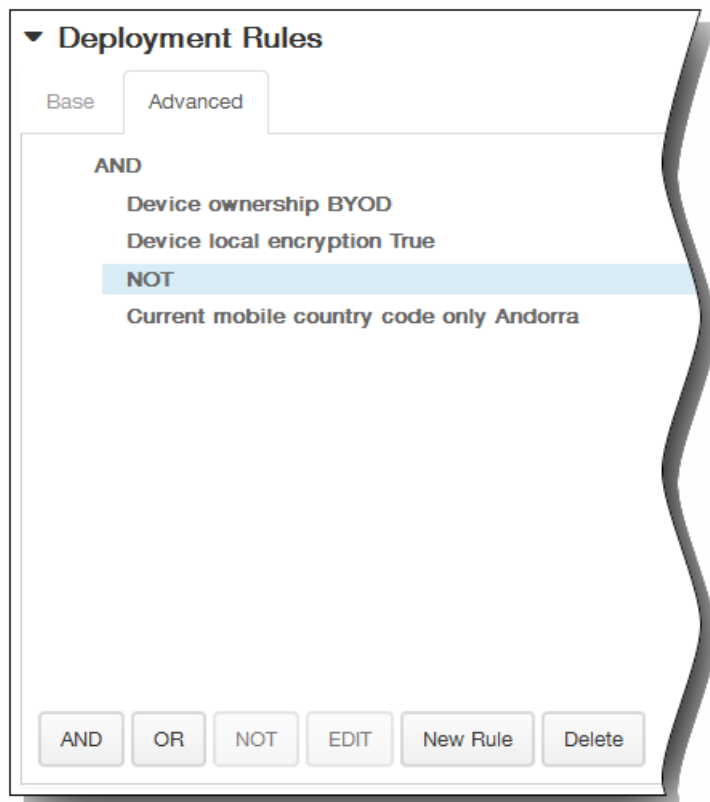


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

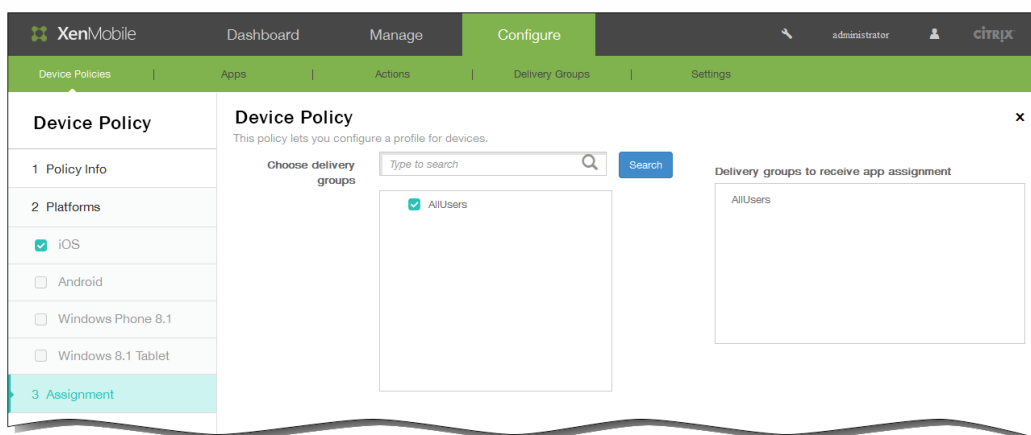
3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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 right-hand Delivery groups to receive app assignment list.

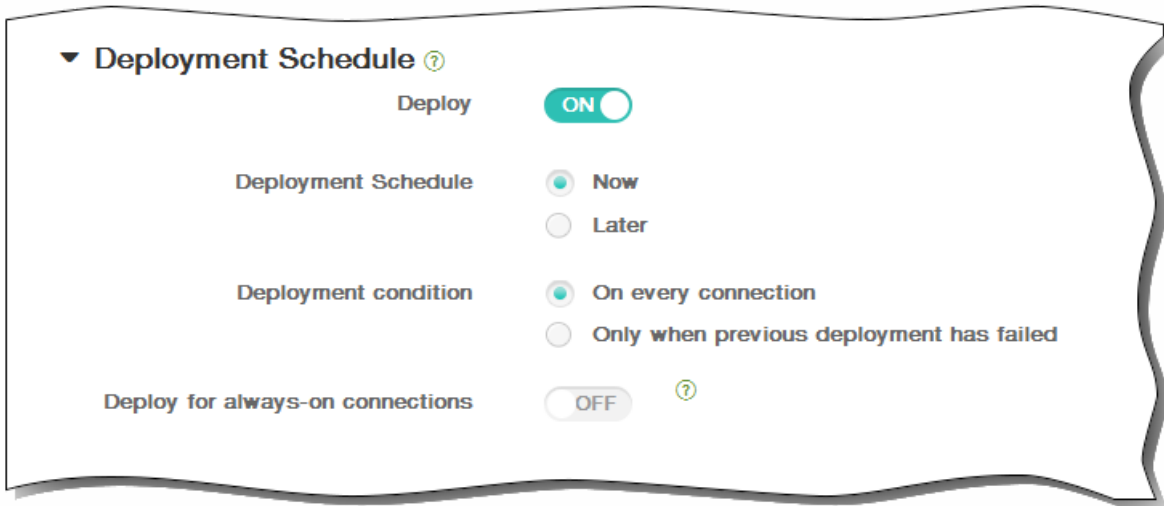


10. Expand Deployment Schedule and then configure the following settings:

1. 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.
2. Next to Deployment schedule, click Now or Later. The default option is Now.

3. If you click Later, click the calendar icon and then select the date and time for deployment.
4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



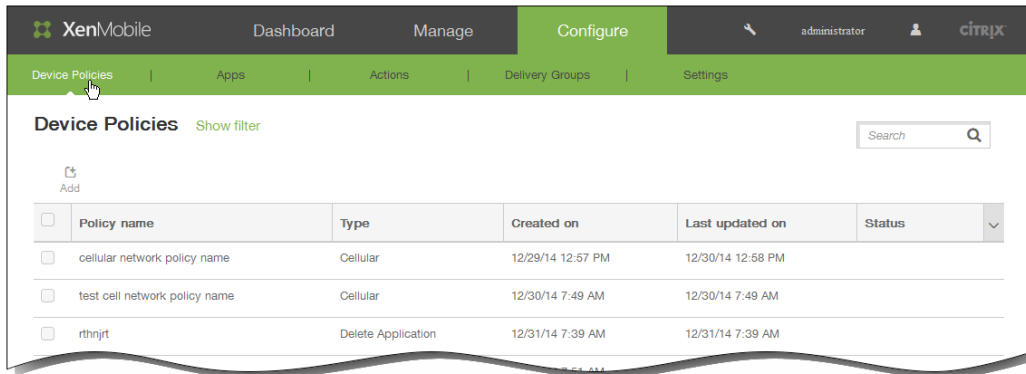
11. Click Save to save the policy.

Connection scheduling device policies

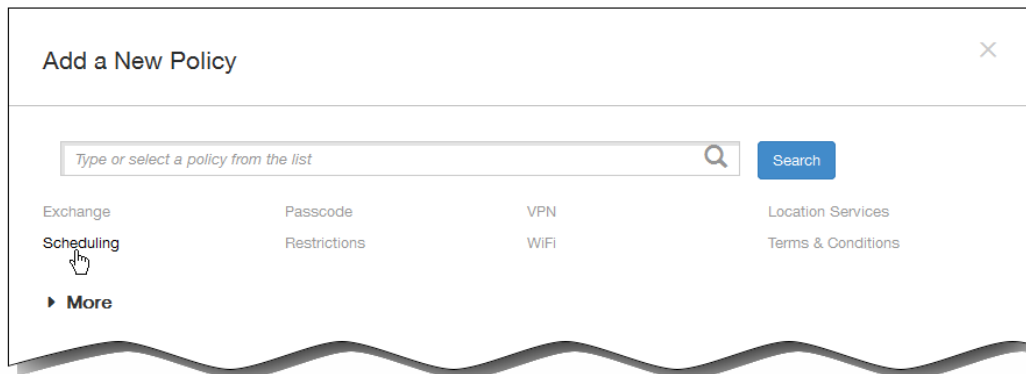
Apr 09, 2015

You create connection scheduling policies to control how and when users' Android and Symbian devices connect to XenMobile. You can specify that users connect their devices manually, that devices stay connected permanently, or that devices connect within a defined time frame.

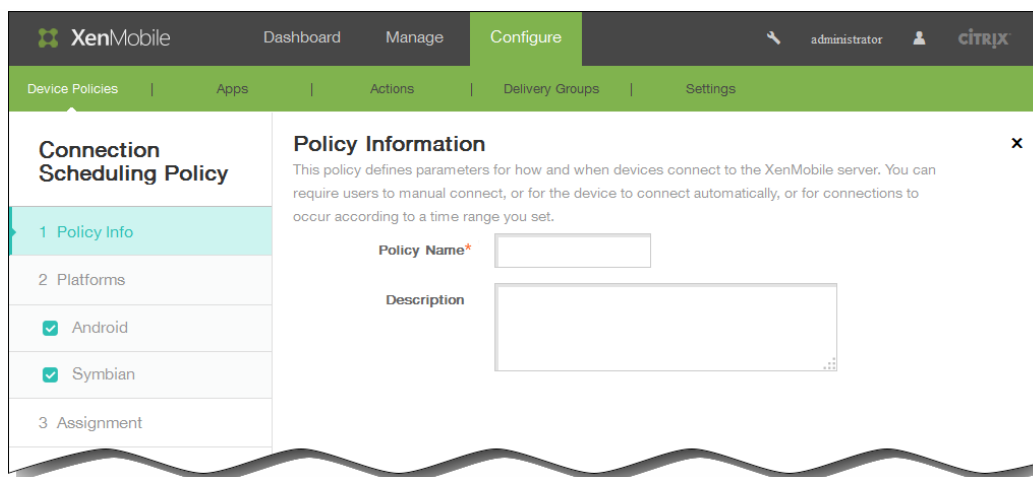
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



2. Click Add to add a new policy. The Add 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:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Type an optional description of the policy.
5. Click Next. The Policy Platforms page appears.

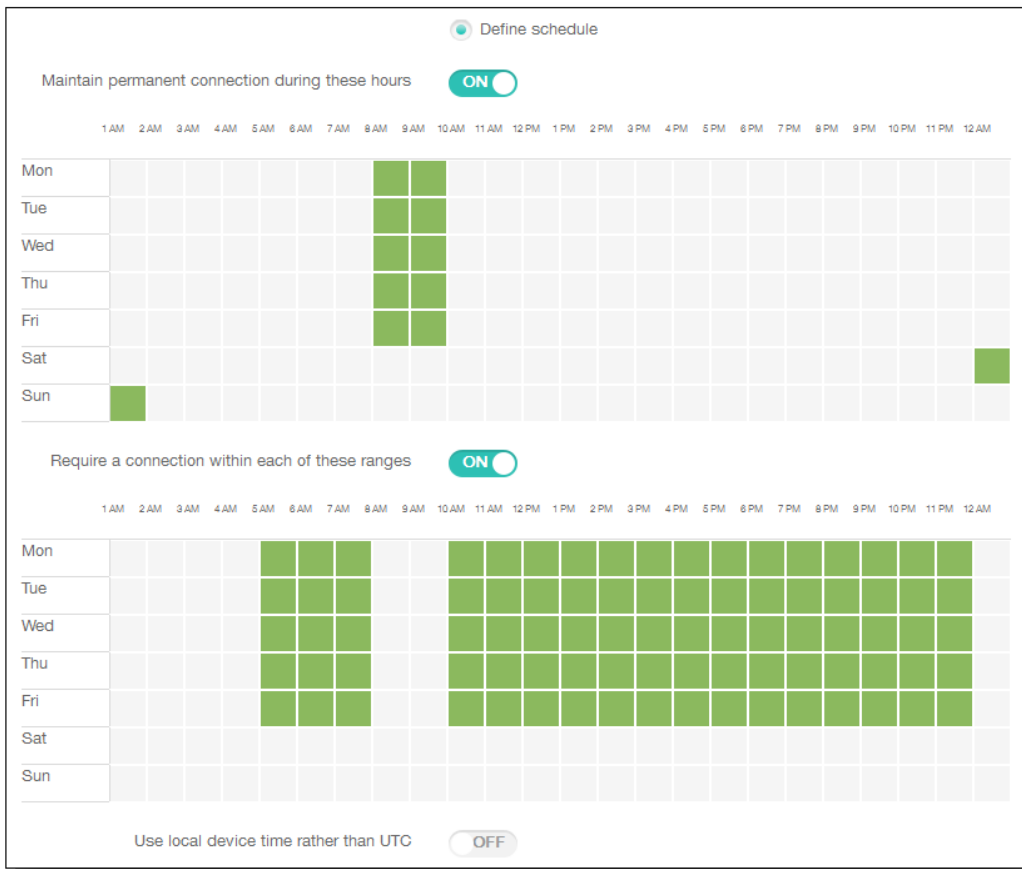
Note: When the Policy Platforms page appears, both platforms are selected and you see the Android platform configuration panel first.
6. Under Platforms, select the platforms you want to add.
7. Configure the following settings for each of the platforms you selected: Require devices to connect: Click 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.

This option is not recommended as it drains battery power and generates a lot of network traffic.
 - Never: Connect manually. Users must initiate the connection from XenMobile on their devices.
 - Every: Connect at the designated interval. Devices automatically connect after a defined number of minutes. 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: 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 within the time frame you define. The following section describes how to define a connection time frame.

To define 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.



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.

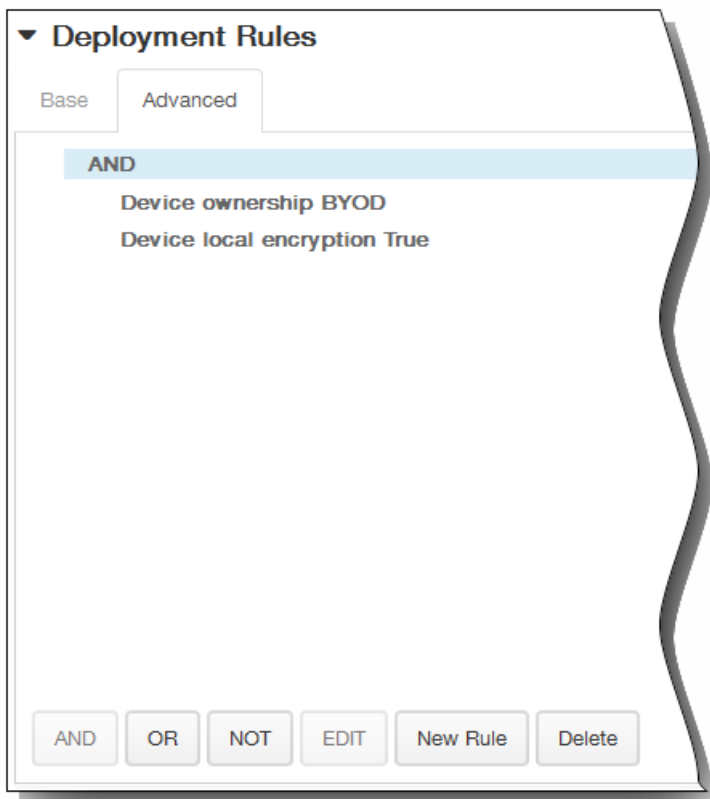
Use local device time rather than UTC: Synchronize the defined time frames to local device time rather than Coordinated Universal Time (UTC).

8. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.

3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

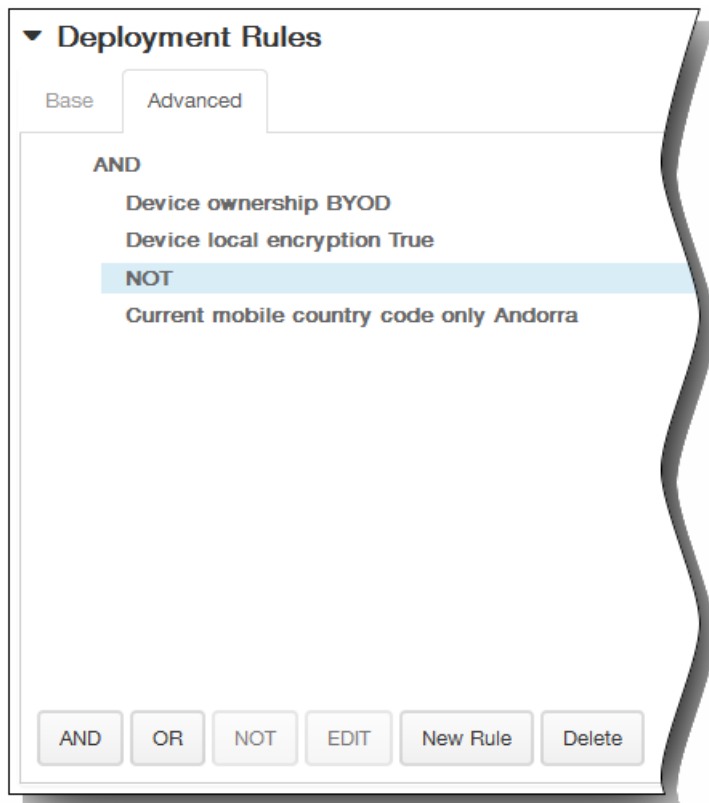


The conditions you chose on the Base tab appear.

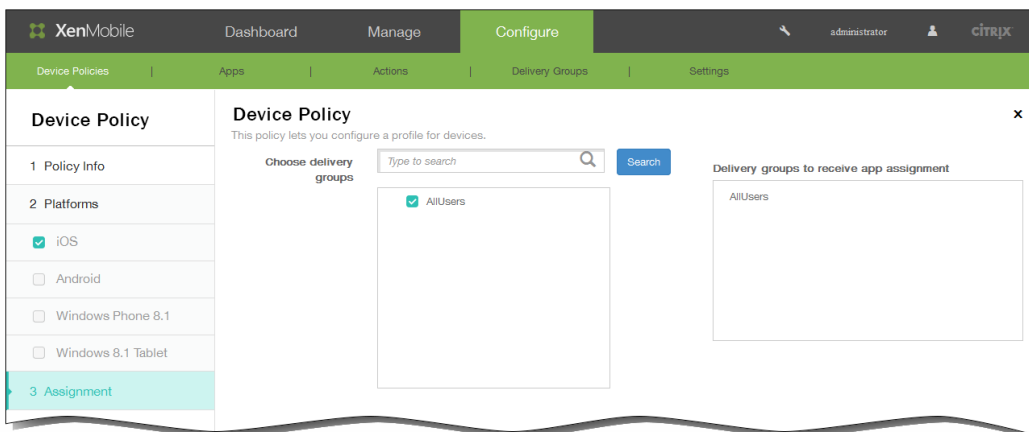
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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 right-hand Delivery groups to receive app assignment list.

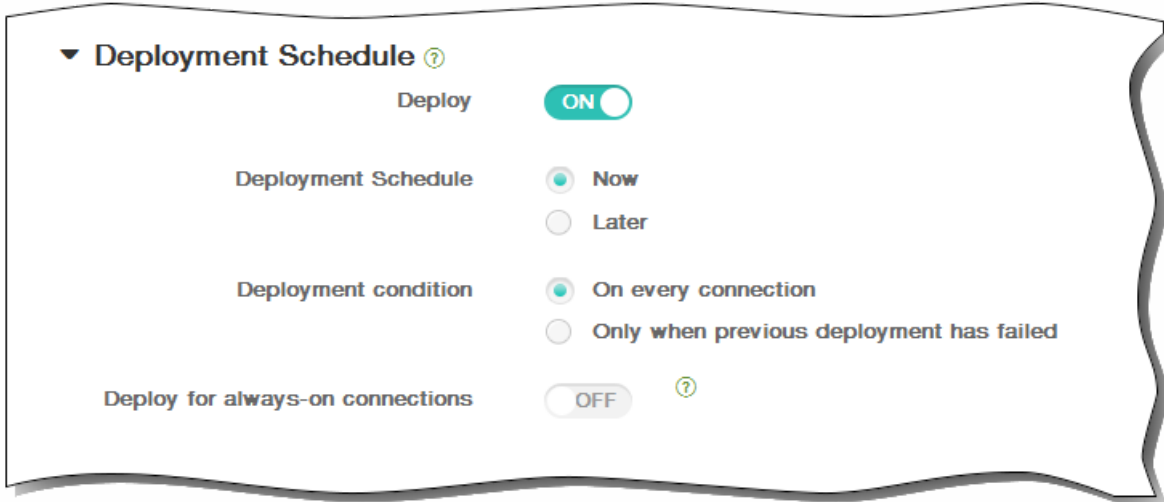


11. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



12. Click Save to save the policy.

To add an AirPlay mirroring device policy for iOS

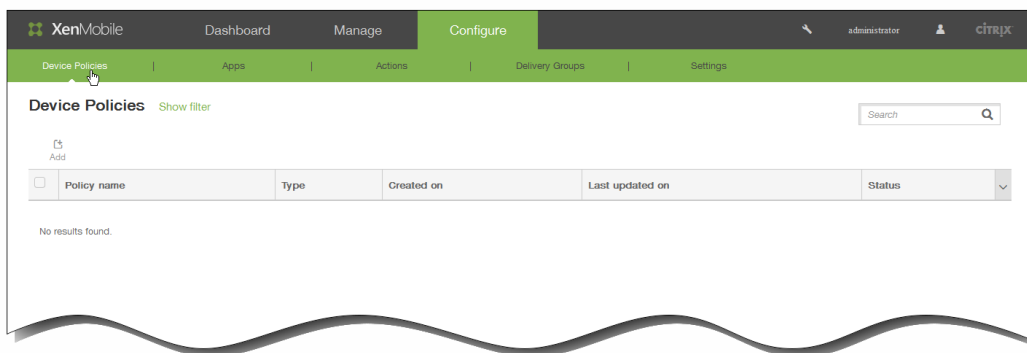
Feb 27, 2015

The Apple AirPlay feature allows users to wirelessly stream content from an iOS device to a TV screen through Apple TV, or to mirror exactly what's on a device display to a TV screen or another Mac computer.

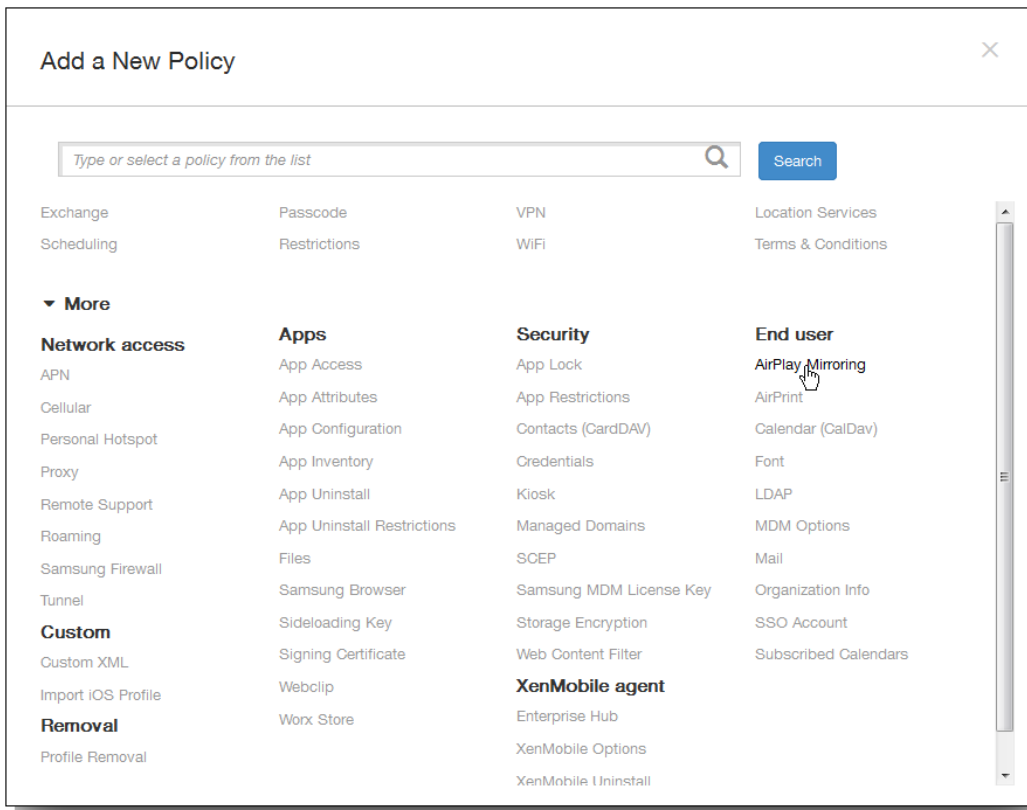
You can add a device policy in XenMobile to add specific AirPlay devices (such as Apple TV or another Mac computer) to users' iOS devices. You also have the option of adding devices to a whitelist for supervised devices, which limits users to only the AirPlay devices on the whitelist. For information about placing a device into Supervised mode, see [To place an iOS device in Supervised mode by using the Apple Configurator](#).

Note: Before proceeding, be sure to have the device IDs and any passwords for all the devices you want to add.

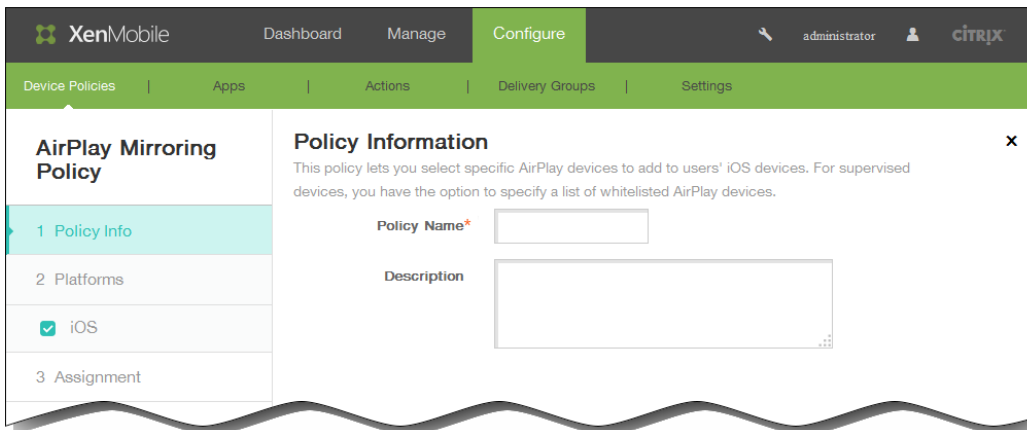
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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

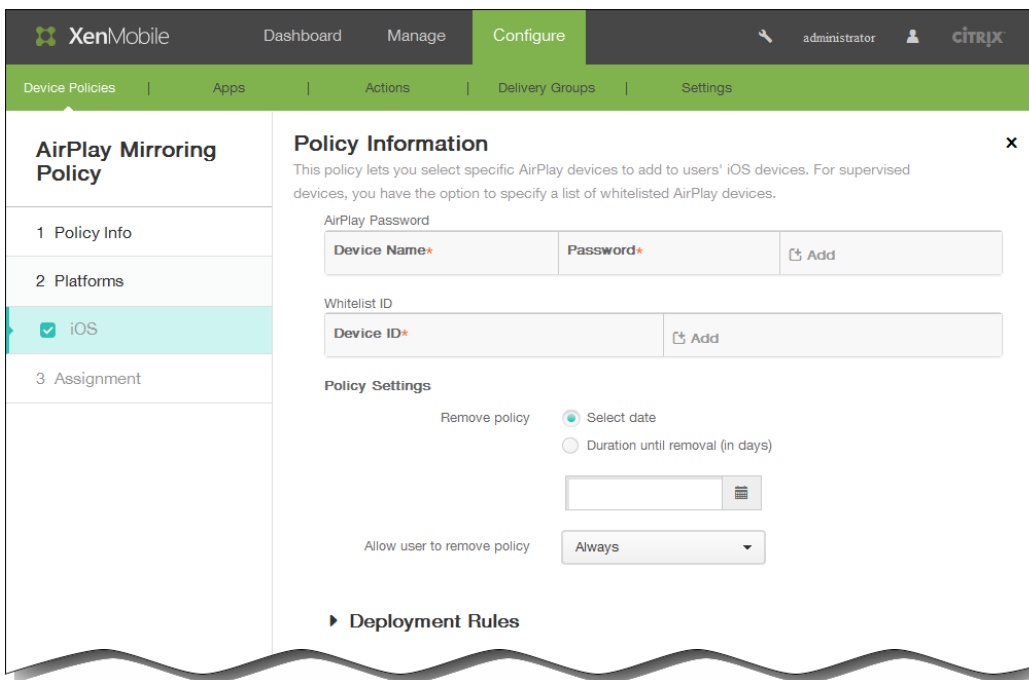


3. Click More and then, under End user, click AirPlay Mirroring. The AirPlay Mirroring Policy page appears.



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

1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform Information page appears.



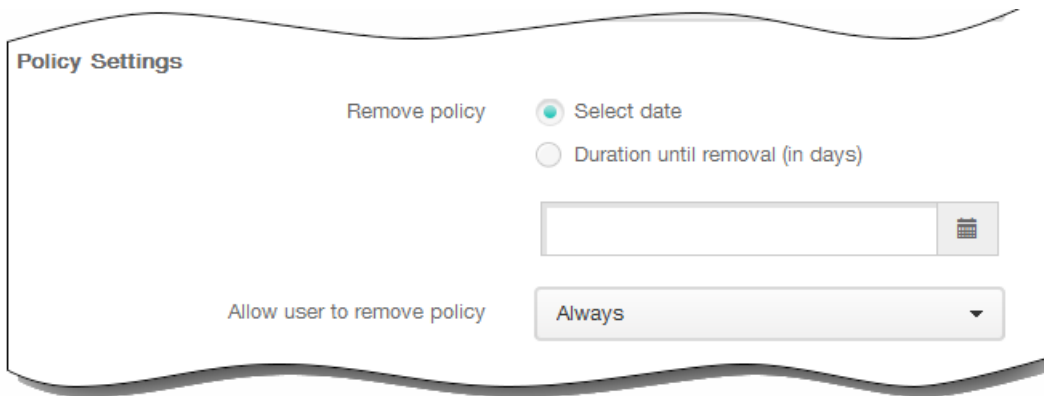
6. On the iOS Platform Information page, enter the following information:
 1. AirPlay Password: Click Add and then do the following:
 1. Device ID: Enter the device ID in xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
 2. Password: Enter an optional password for the device.
 3. Click Add to add the device or click Cancel to cancel adding the device.
 4. Repeat steps i. through iii. for each device you want to add.
 2. Whitelist ID: Click Add and then do the following to limit supervised devices to only those device IDs on the whitelist:

Note: This list is ignored for unsupervised devices.

 1. Device ID: Enter the device ID in xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
 2. Click Add to add the device or click Cancel to cancel adding the device.
 3. Repeat steps i. and ii. for each device you want to add to the whitelist.

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

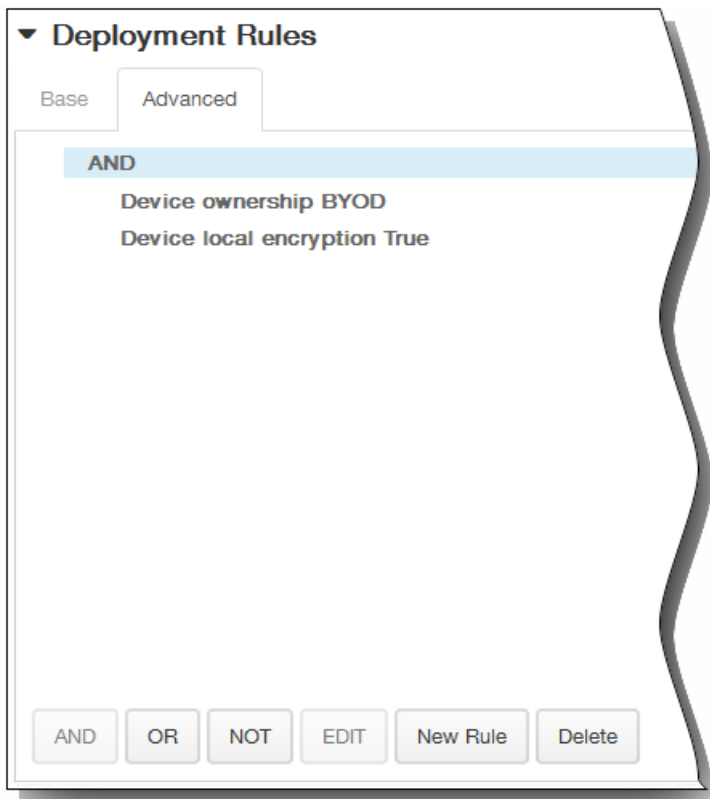
To edit an existing device, hover over the line containing the listing and click the pen icon on the right-hand side. Make any changes to the listing and then click Save to save the changed listing or Cancel to leave the listing unchanged.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.

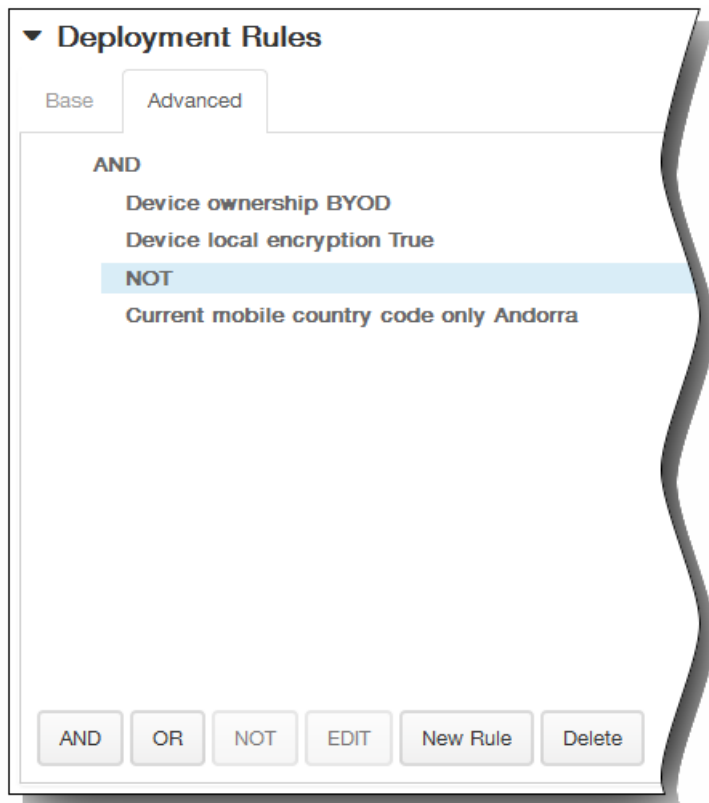
1. Click AND, OR, or NOT.

2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

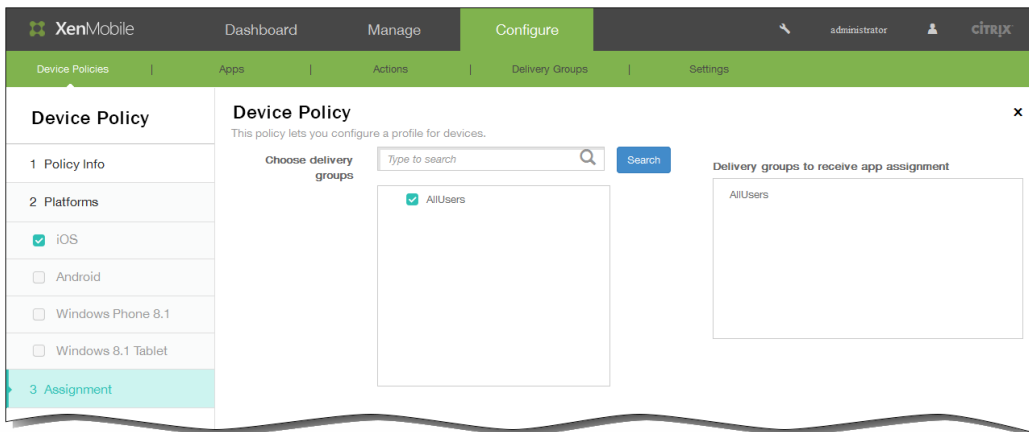
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The AirPlay Mirroring Policy assignment page appears.
13. 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.

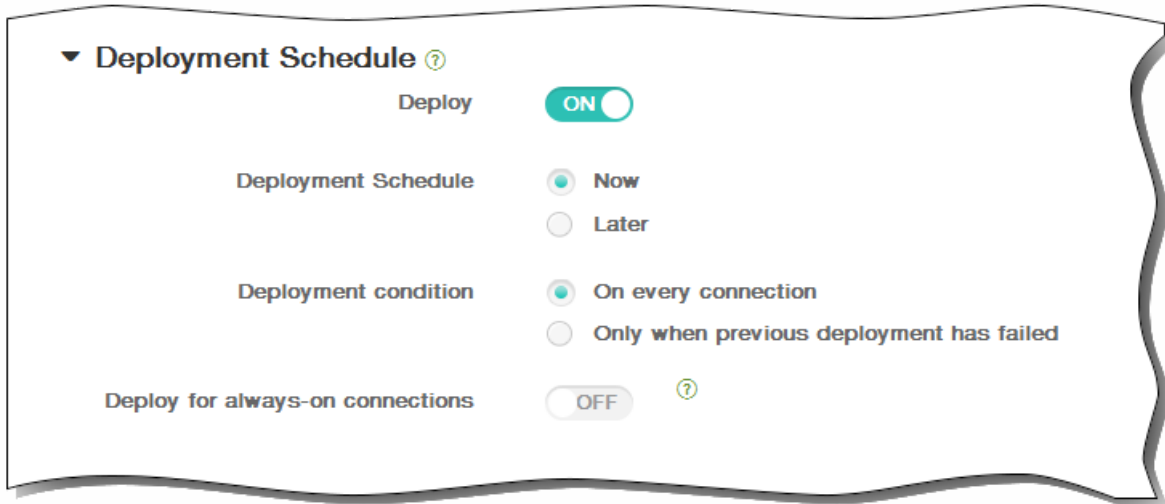


14. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



15. Click Save to save the policy.

To add an AirPrint device policy for iOS

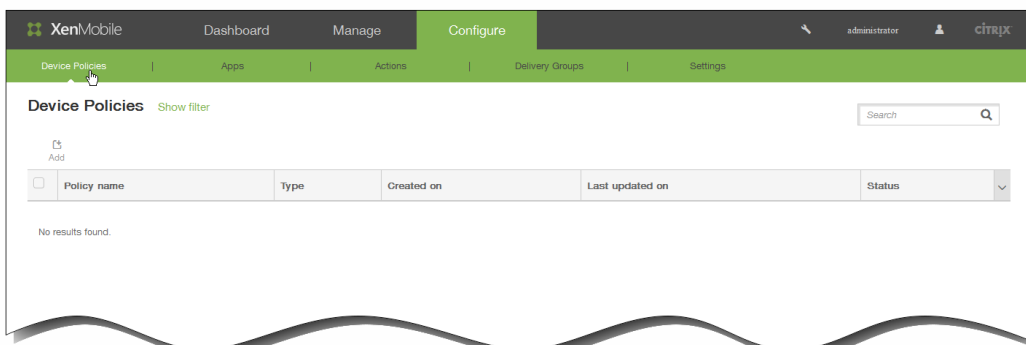
Feb 27, 2015

You can add a device policy in XenMobile to add AirPrint printers to the AirPrint printer list on users' iOS devices. This policy makes it easier to support environments where the printers and the devices are on different subnets.

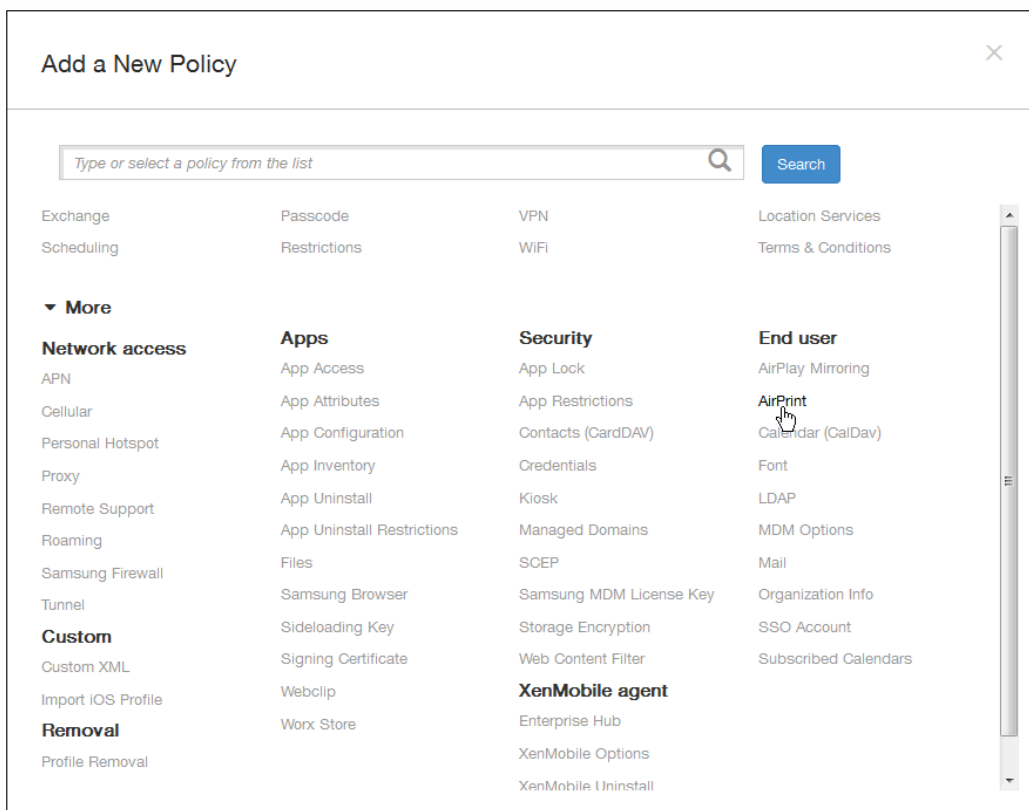
Note:

- This policy applies to iOS 7.0 and later.
- Be sure to have the IP address and resource path for each printer.

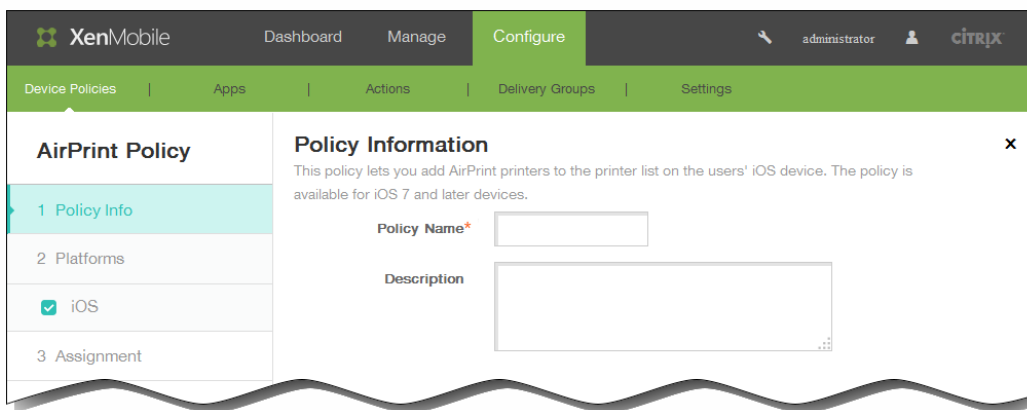
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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



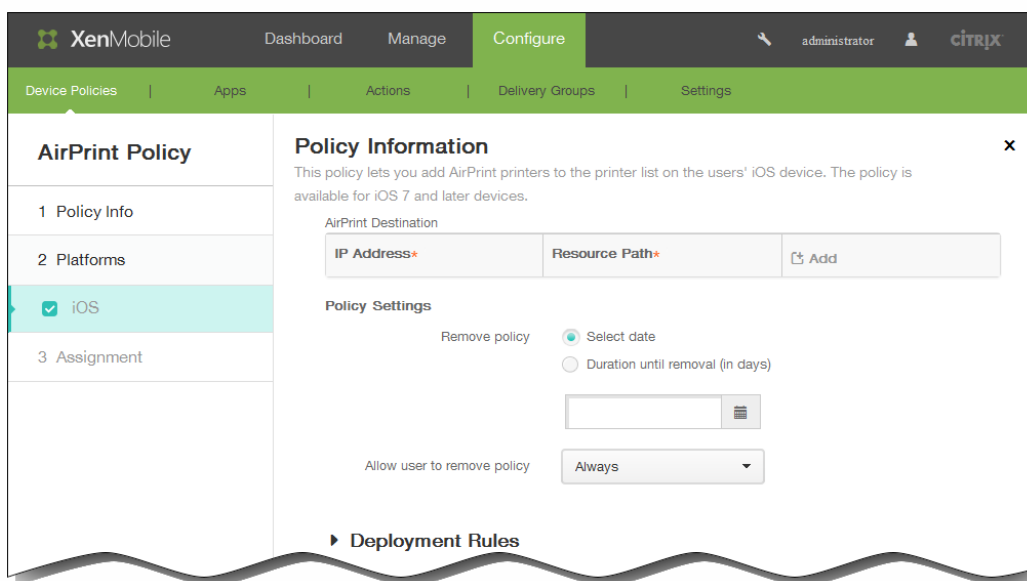
3. Click More and then, under End user, click AirPrint. The AirPrint Policy page appears.



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

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

5. Click Next. The iOS Platform Information page appears.



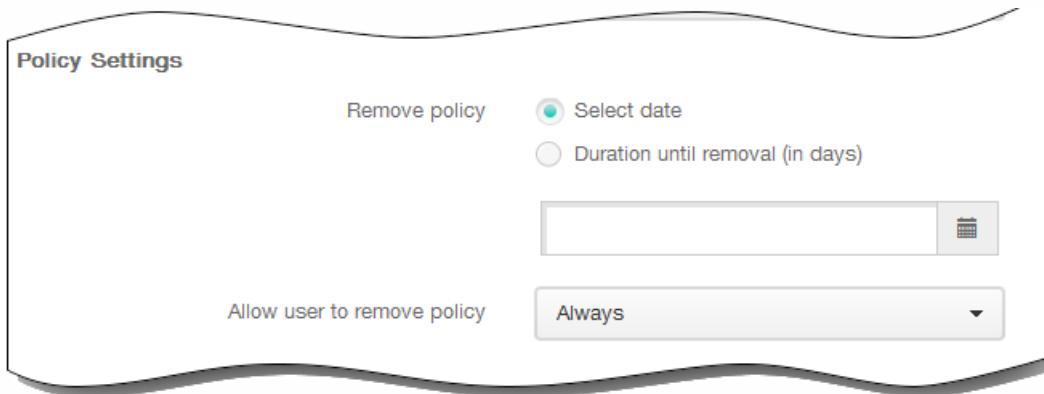
6. On the iOS Platform Information page, enter the following information:

1. AirPrint Destination: Click Add and then do the following:
 1. IP Address: Enter the AirPrint printer IP address.
 2. Resource Path: Enter the Resource Path associated with the printer. This value corresponds to the parameter of the `_ipps.tcp` Bonjour record. For example, `printers/Canon_MG5300_series` or `printers/Xerox_Phaser_7600`.
 3. Click Add to add the printer or click Cancel to cancel adding the printer.
 4. Repeat steps i. through iii. f for each device you want to add.

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

Make any changes to the listing and then click Save to save the changed listing or Cancel to leave the listing unchanged.

7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



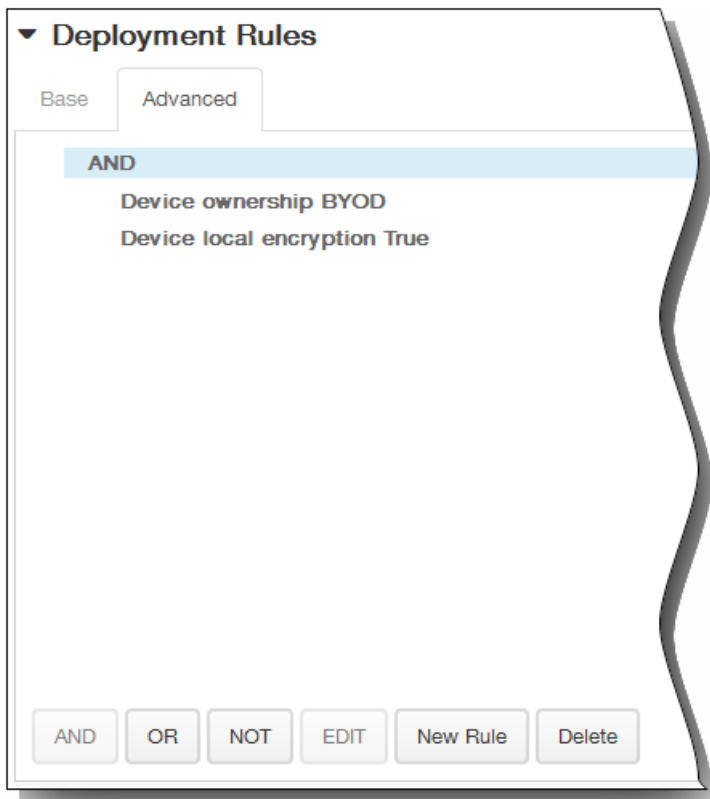
The screenshot shows the 'Policy Settings' section. Under 'Remove policy', there are two radio buttons: 'Select date' (which is selected) and 'Duration until removal (in days)'. Below these is a text input field with a calendar icon on the right. Under 'Allow user to remove policy', there is a dropdown menu currently set to 'Always'.

11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



The screenshot shows the 'Deployment Rules' section. It has two tabs: 'Base' (selected) and 'Advanced'. Under 'Deploy when', there is a dropdown menu set to 'All' and the text 'conditions are met.' followed by a 'New Rule' button. Below this, there are two more dropdown menus: 'Device ownership' and 'BYOD'. There is also a small icon on the right side of the rule configuration area.

1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

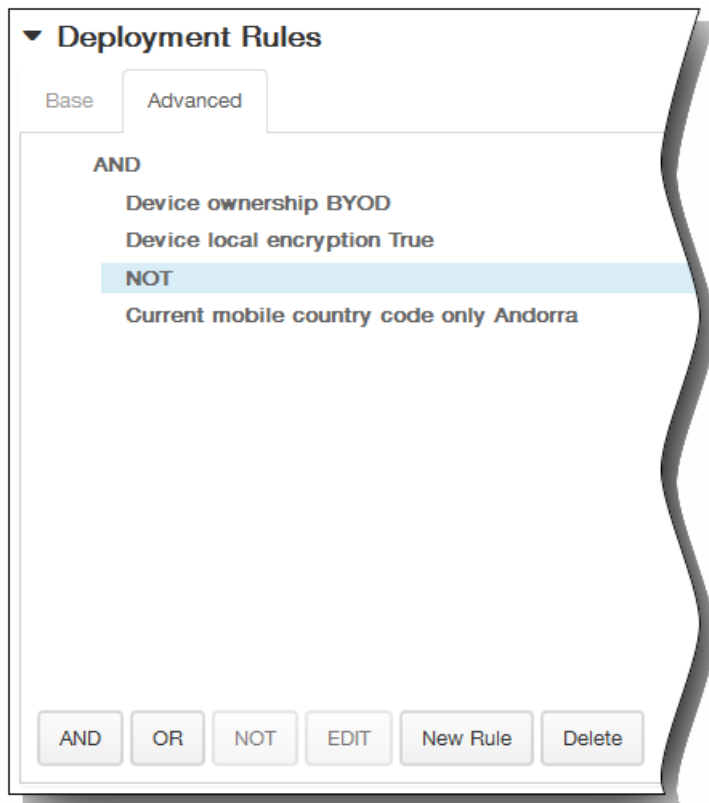


The conditions you chose on the Base tab appear.

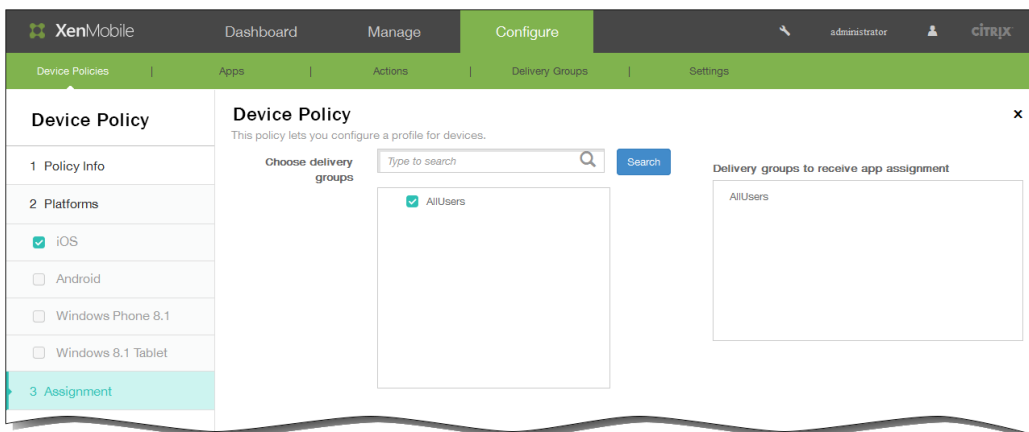
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The AirPrint Policy assignment page appears.
13. 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.

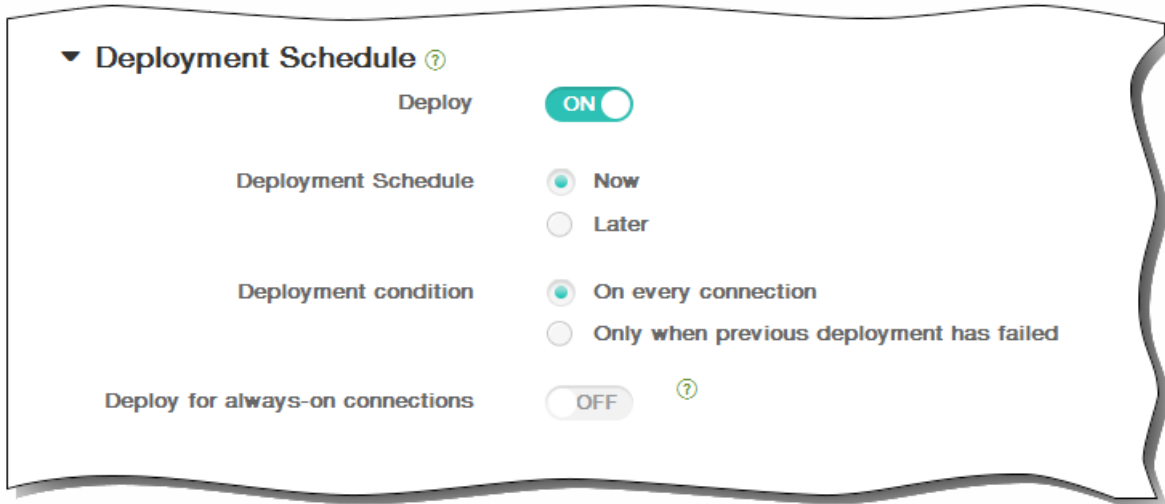


14. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



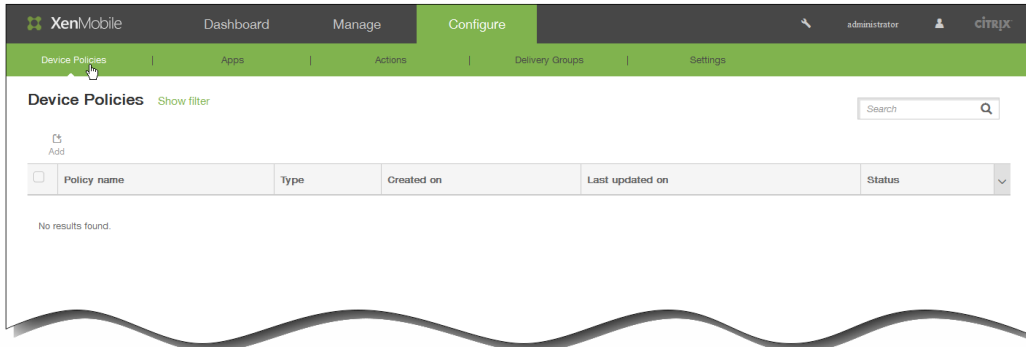
15. Click Save to save the policy.

To add a calendar (CalDav) device policy for iOS

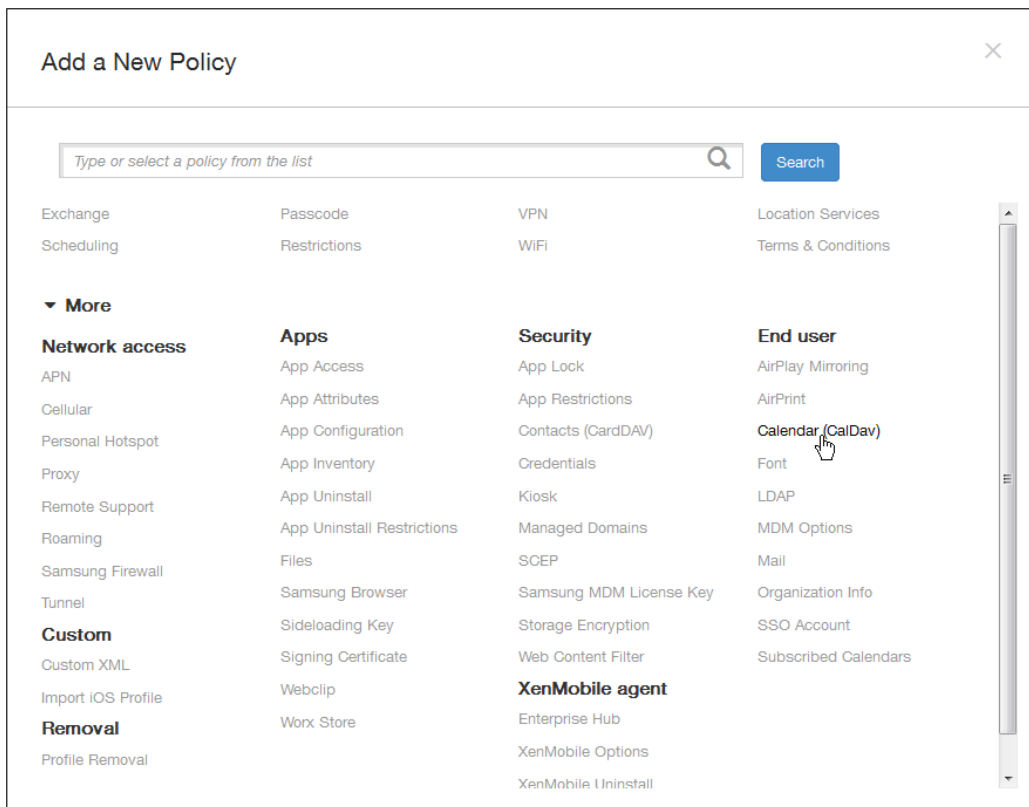
Feb 13, 2015

You can add a device policy in XenMobile to add an iOS calendar (CalDAV) account to users' iOS devices to enable them to synchronize scheduling data with any server that supports CalDAV.

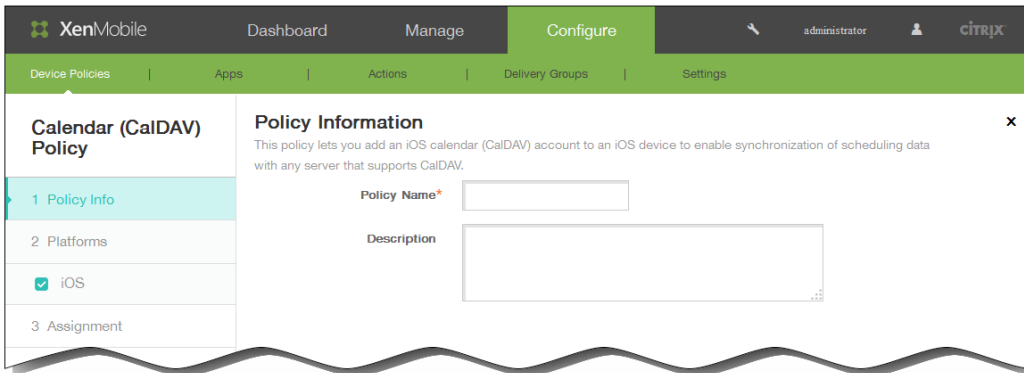
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



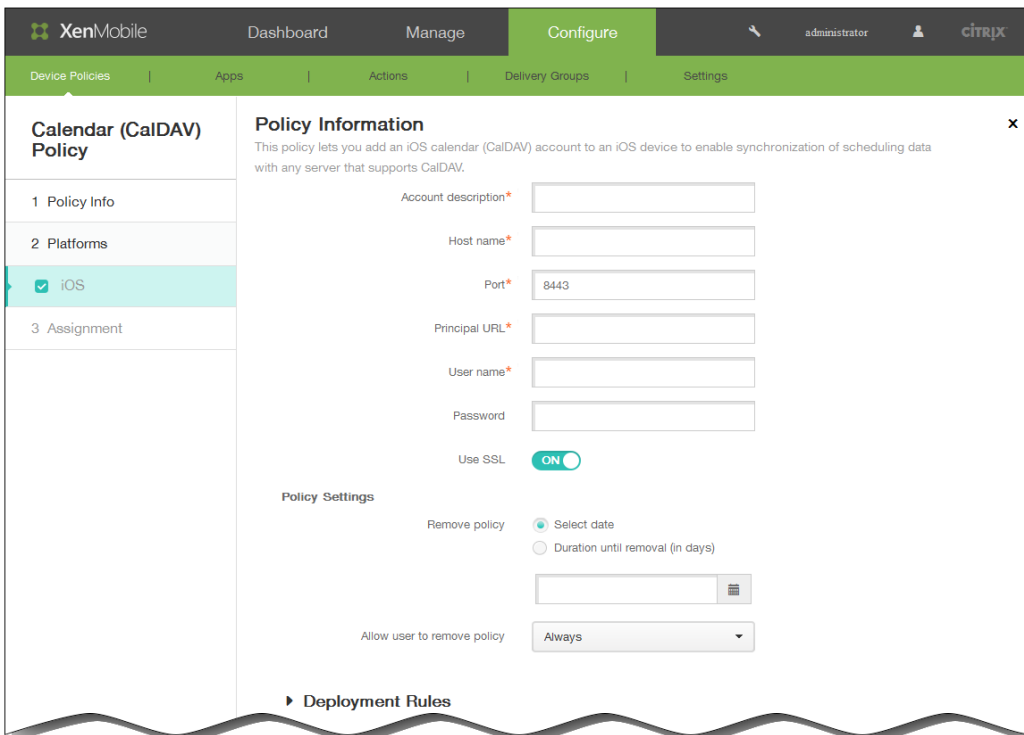
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



3. Click 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:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform Information page appears.



6. In the iOS Platform Information page, enter the following information:
 1. Account description: Type an account description. This field is required.
 2. Host name: Type the address of the CalDAV server. This field is required.
 3. Port: Type the port on which to connect to the CalDAV server. This field is required. The default is 8443.
 4. Principal URL: Type the base URL to the user's calendar.
 5. User name: Type the user's logon name. This field is required.
 6. Password: Type an optional user password.
 7. Use SSL: Select whether to use a Secure Socket Layer connection to the CalDAV server. The default is On.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).

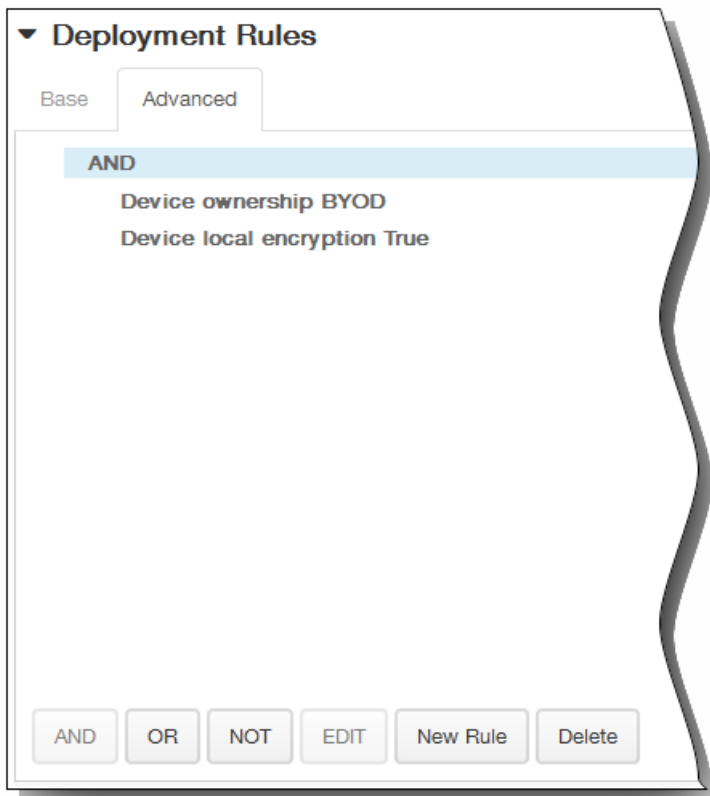
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.

The screenshot shows the 'Policy Settings' section. Under 'Remove policy', there are two radio button options: 'Select date' (which is selected) and 'Duration until removal (in days)'. Below these is a text input field with a calendar icon on the right. Under 'Allow user to remove policy', there is a dropdown menu currently set to 'Always'.

11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.

The screenshot shows the 'Deployment Rules' section. It has two tabs: 'Base' (selected) and 'Advanced'. Under 'Deploy when', there is a dropdown menu set to 'All' and the text 'conditions are met.' followed by a 'New Rule' button. Below this, there are two more dropdown menus: 'Device ownership' and 'BYOD'. There is also a small icon on the right side of the configuration area.

1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

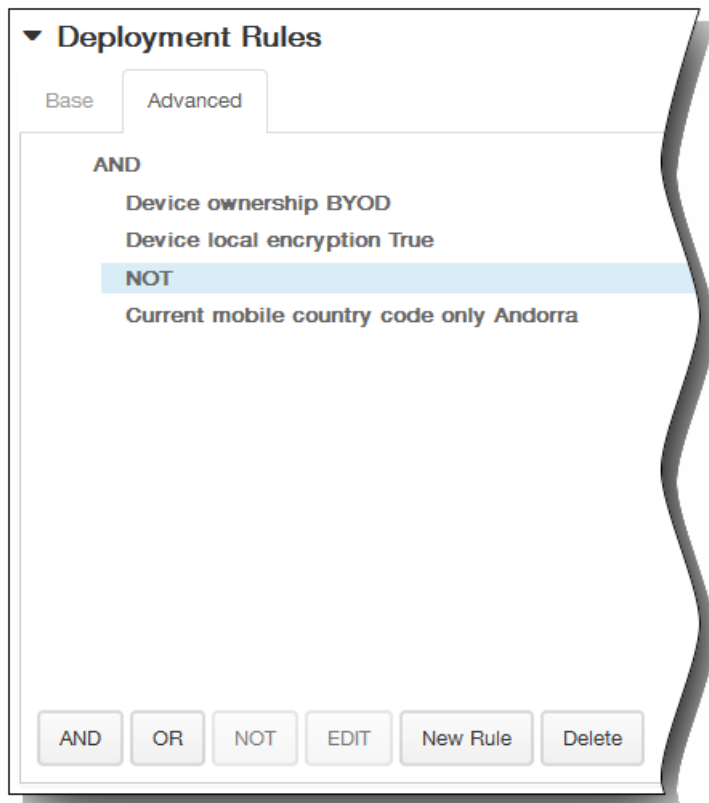


The conditions you chose on the Base tab appear.

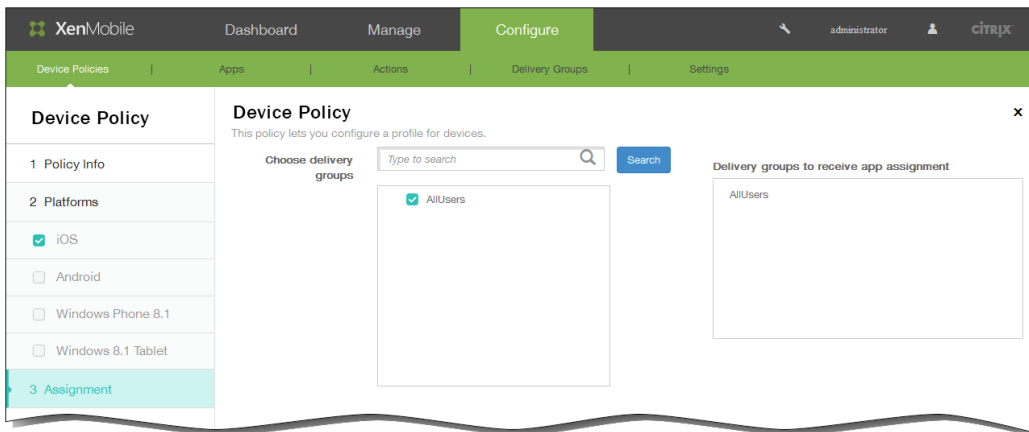
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The Calendar (CalDAV) Policy assignment page appears.
13. 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.

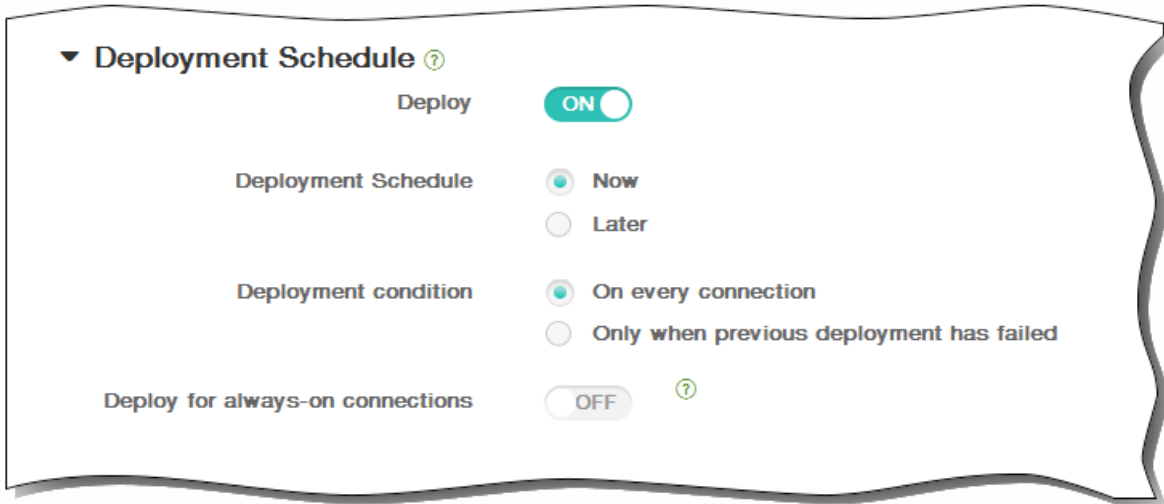


14. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



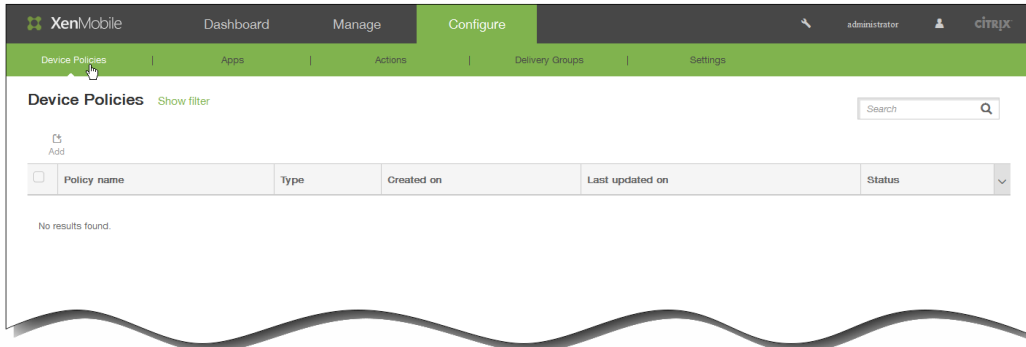
15. Click Save to save the policy.

To add a contacts (CardDAV) device policy for iOS

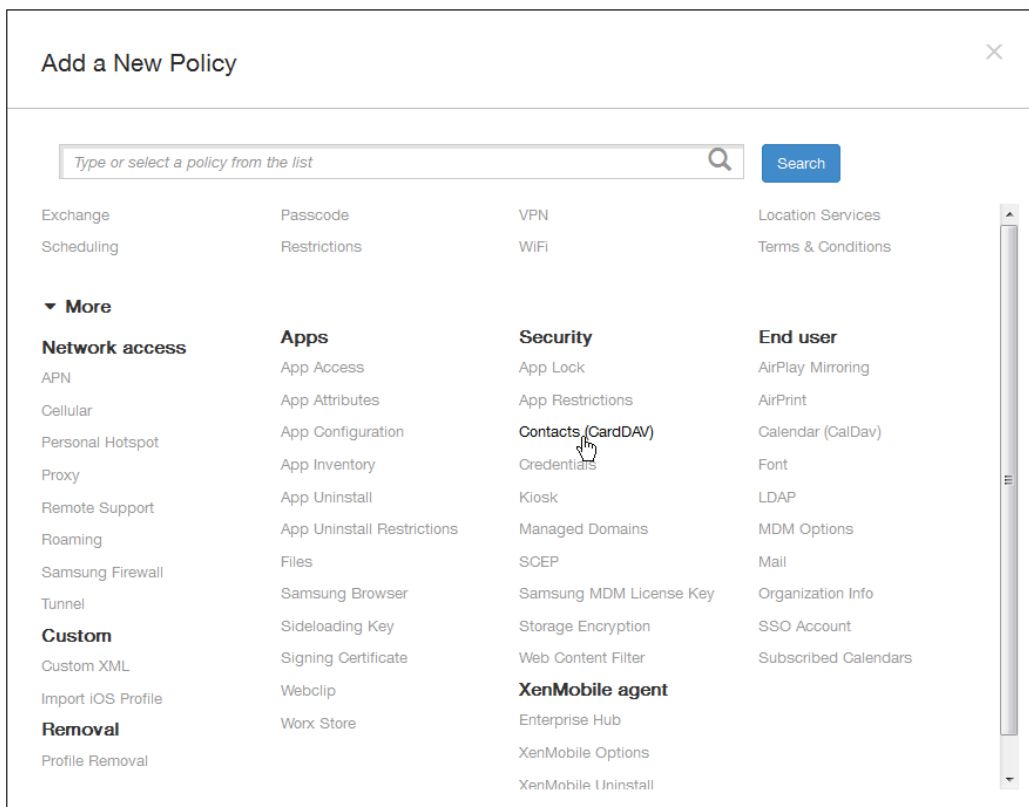
Feb 13, 2015

You can add a device policy in XenMobile to add an iOS contacts (CardDAV) account to users' iOS devices to enable them to synchronize contact data with any server that supports CardDAV.

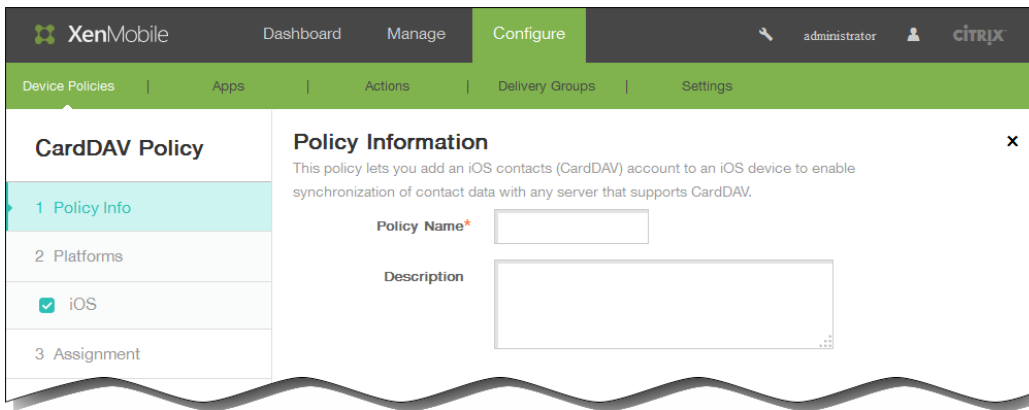
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



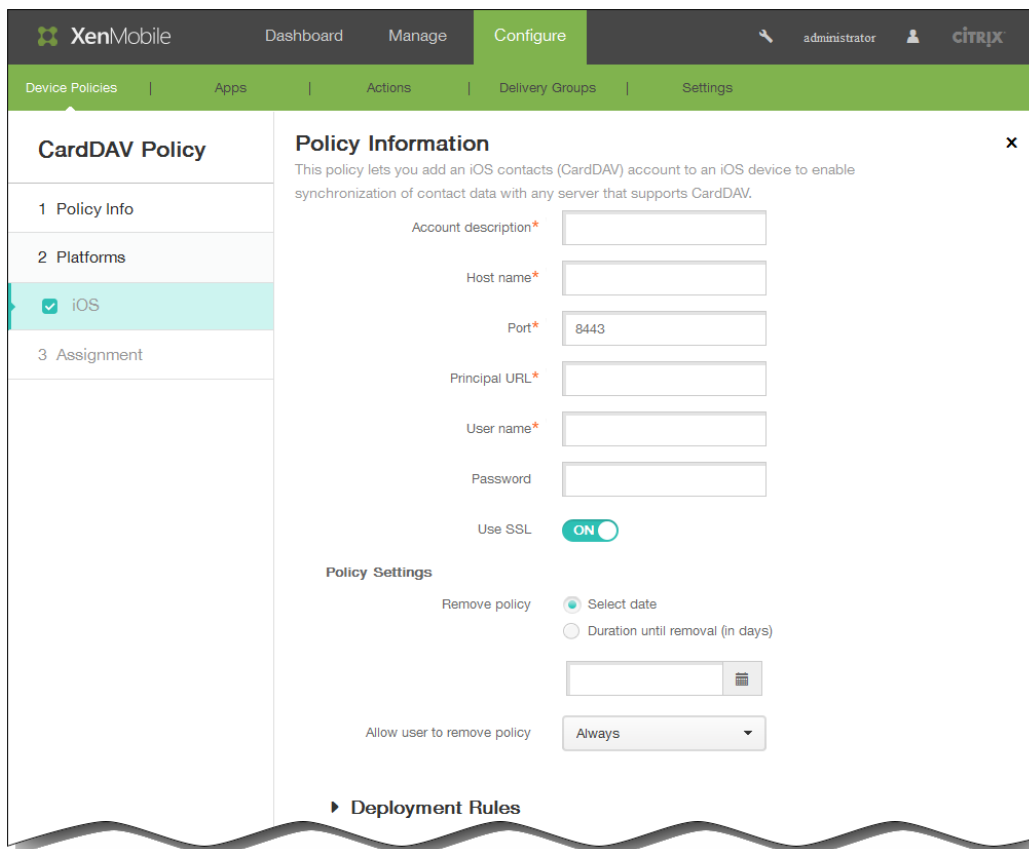
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



3. Click More and then, under Security, click Contacts CardDAV. The CardDAV Policy page appears.



4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform Information page appears.



6. In the iOS Platform Information page, enter the following information:
 1. Account description: Enter an account description. This field is required.
 2. Host name: Enter the address of the CardDAV server. This field is required.
 3. Port: Enter the port on which to connect to the CardDAV server. This field is required. The default is 8443.
 4. Principal URL: Enter the base URL to the user's calendar.
 5. User name: Enter the user's logon name. This field is required.

6. Password: Enter an optional user password.
7. Use SSL: Select whether to use a Secure Socket Layer connection to the CardDAV server. The default is ON.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.

Policy Settings

Remove policy Select date
 Duration until removal (in days)

Allow user to remove policy: Always

11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.

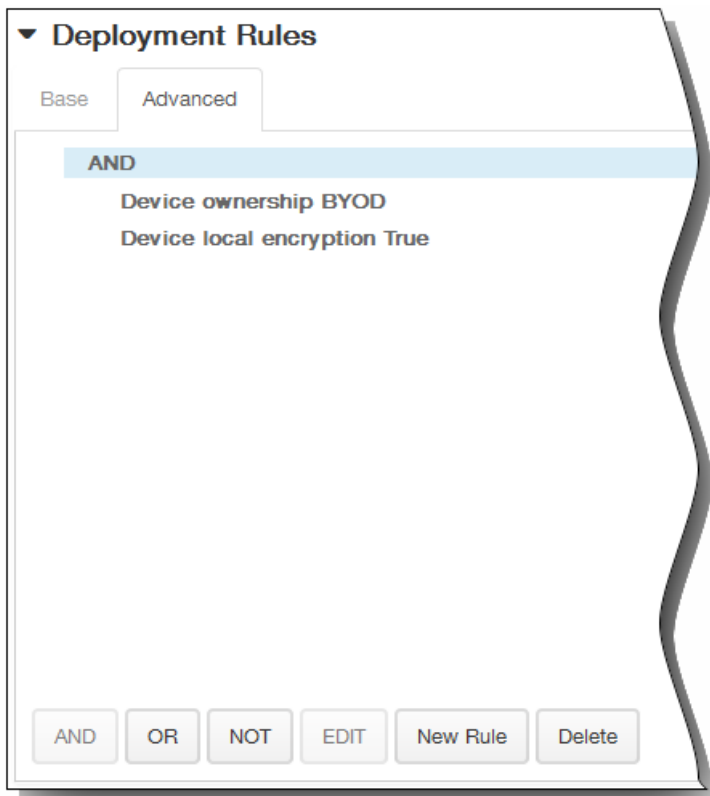
Deployment Rules

Base | Advanced

Deploy when: All conditions are met. [New Rule]

Device ownership | BYOD

1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.

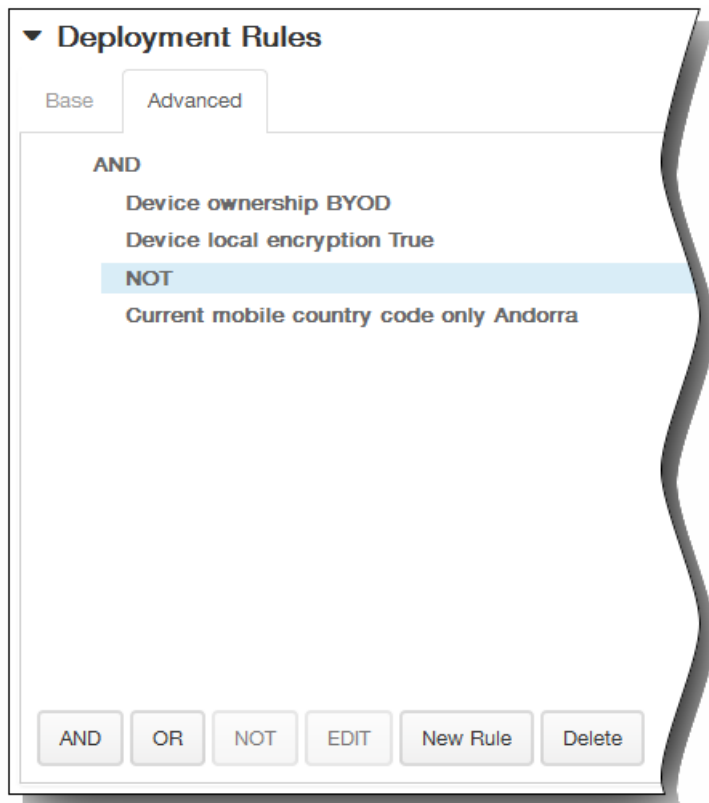
1. Click AND, OR, or NOT.

2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

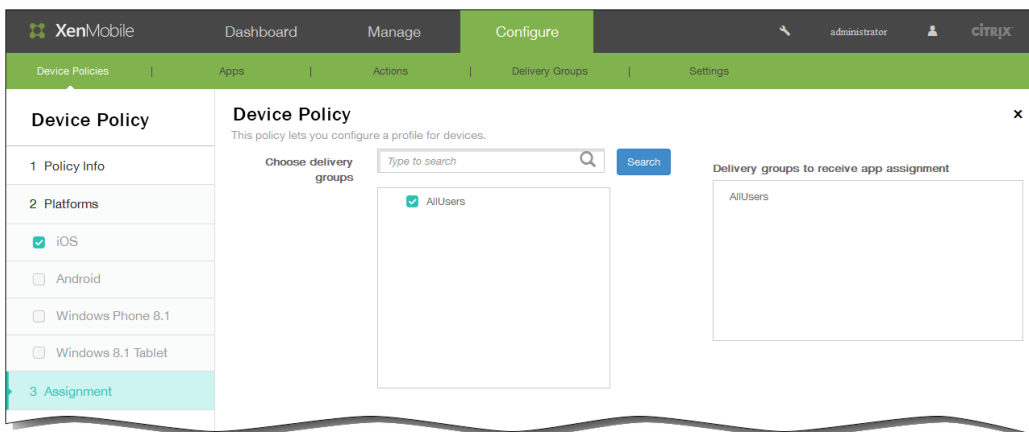
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The CardDAV Policy assignment page appears.
13. 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.

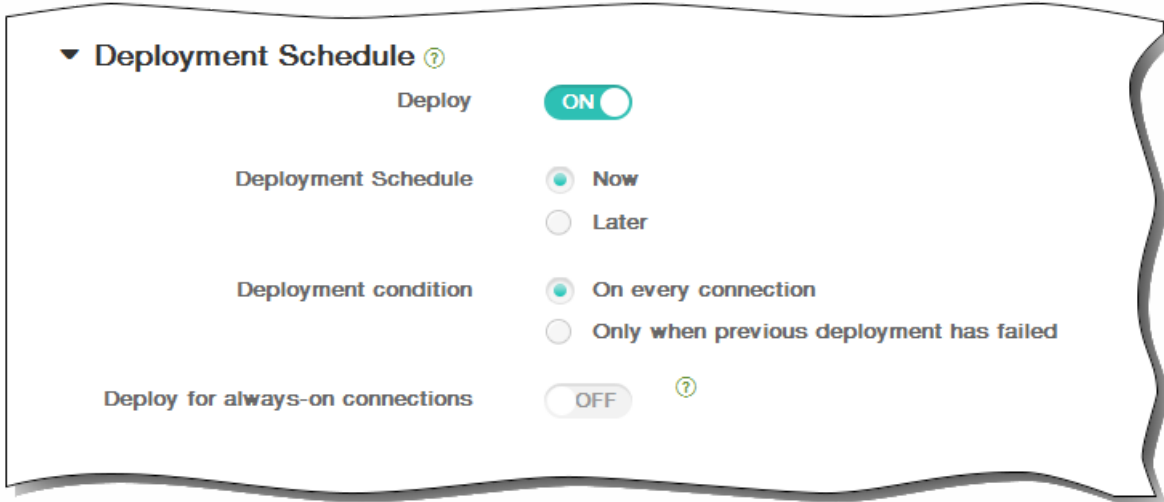


14. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



15. Click Save to save the policy.

Credentials device policies

Apr 09, 2015

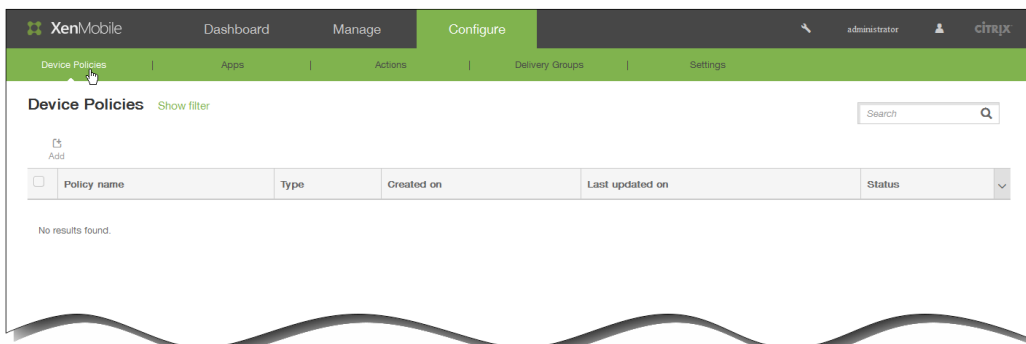
You can create credentials device policies in XenMobile to enable integrated authentication with your PKI configuration in XenMobile, such as a PKI entity, a keystore, a credential provider, or a server certificate. For more information about credentials, see [Certificates in XenMobile](#).

You can create credential policies for iOS, Android, and Windows 8.1 Tablet devices. Each platform requires a different set of values, which are described in this article.

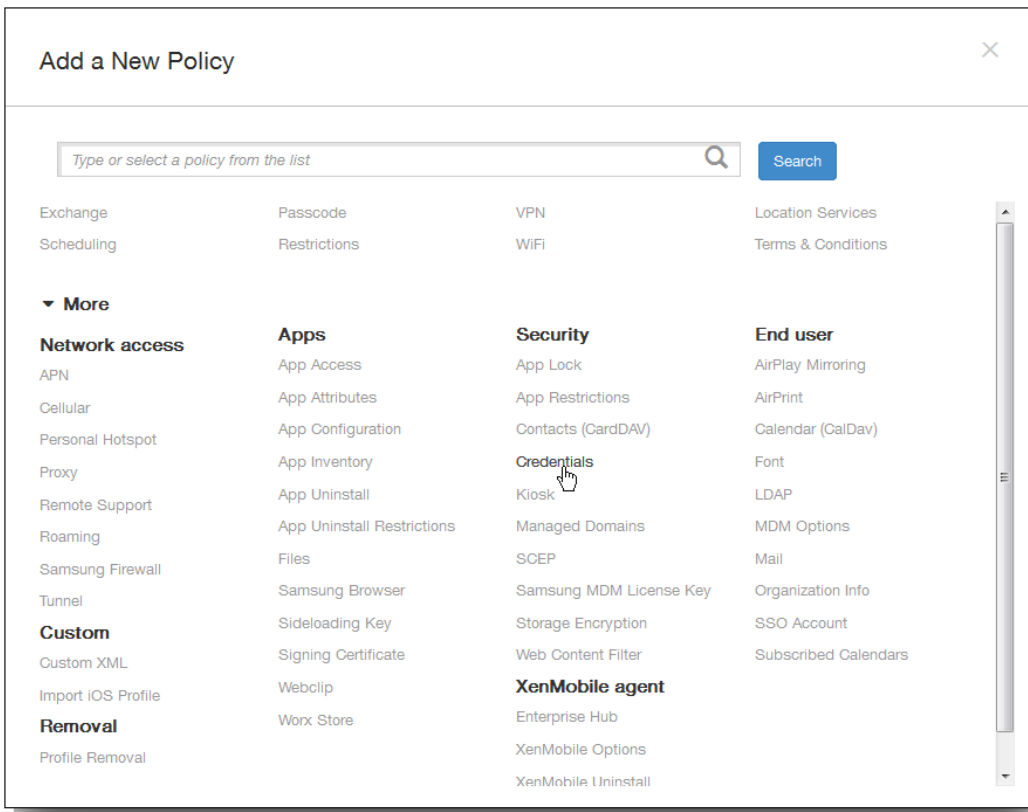
You need the following information before you can create this policy:

- The credential information you plan to use for each platform, plus any certificates and passwords.

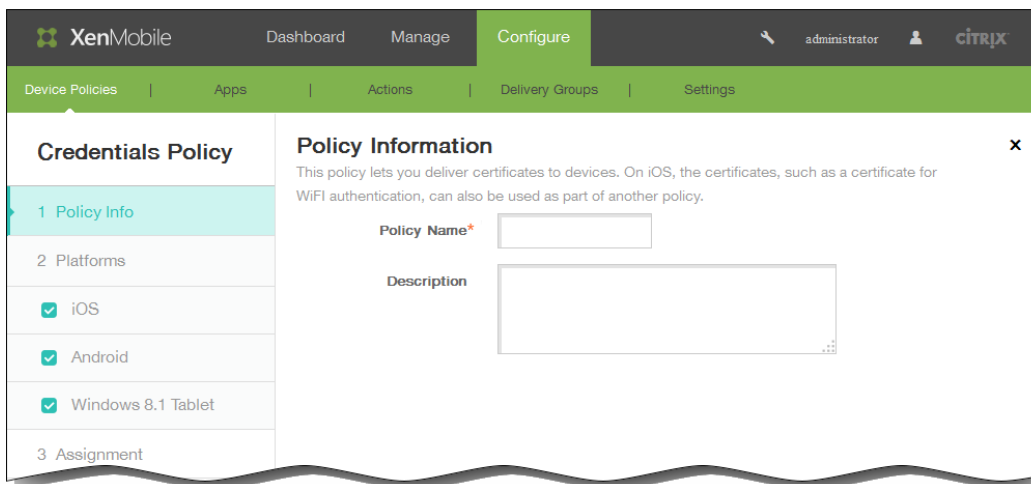
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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



3. Click More and then, under Security, click Credentials. The Credentials Policy information page appears.

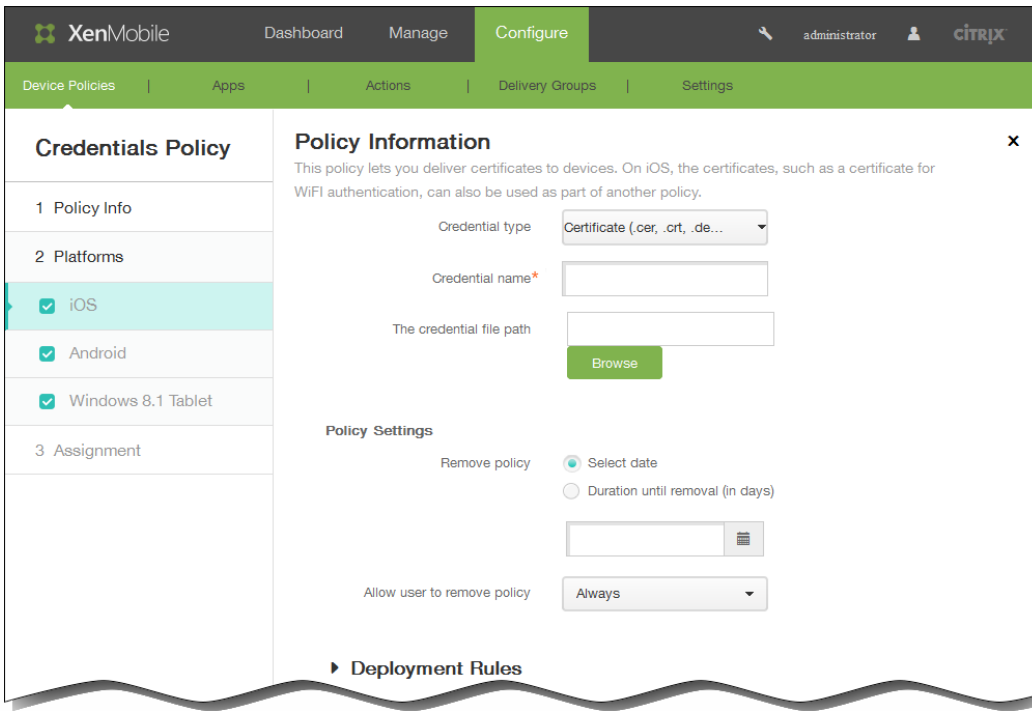


4. In the Policy Information pane, type the following information:

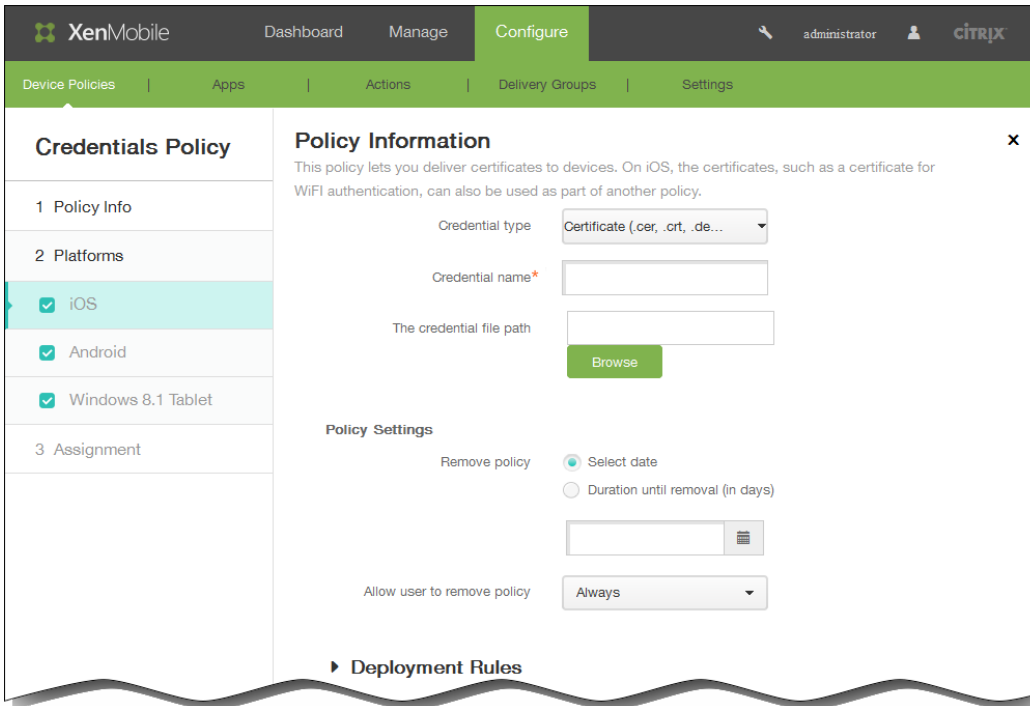
1. Policy Name: Type a descriptive name for the policy.
2. Description: Type an optional description of the policy.

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 configuration panel first.



6. Under Platforms, select the platforms you want to add.
- if you selected iOS, configure the following settings:



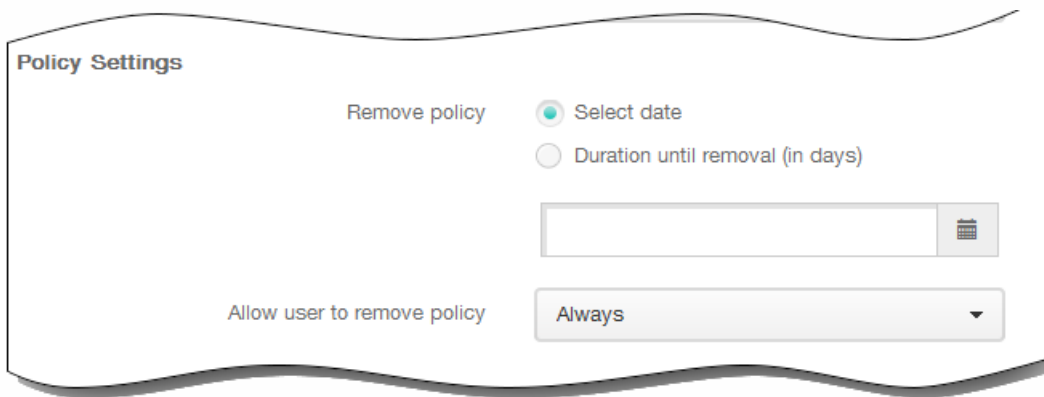
Credential type: In the list, click the type of credential to use with this policy.

Enter the following information for the selected credential:

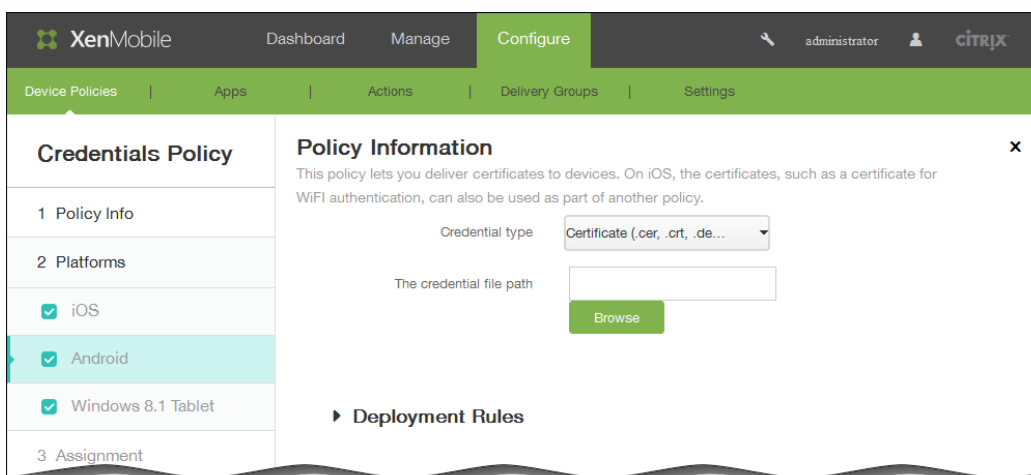
- **Certificate**
 - Credential name: Enter a unique name for the credential.

- 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



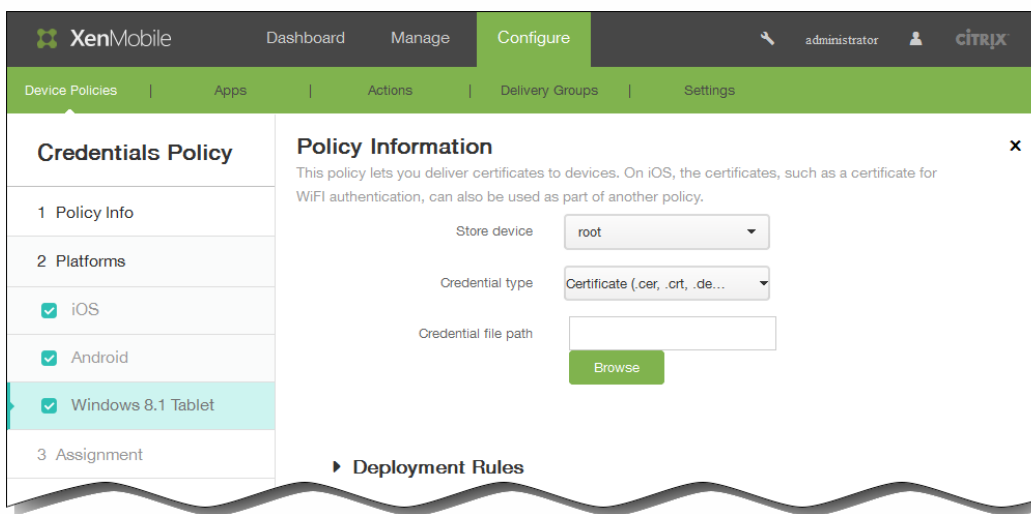
1. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
 2. If you click Select date, click the calendar to select the specific date for removal.
 3. In the Allow user to remove policy list, click Always, Password required, or Never.
 4. If you click Password required, next to Removal password, type the necessary password.
- If you selected Android, configure the following settings:



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

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.
- If you selected Windows 8.1 Tablet, configure the following 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.

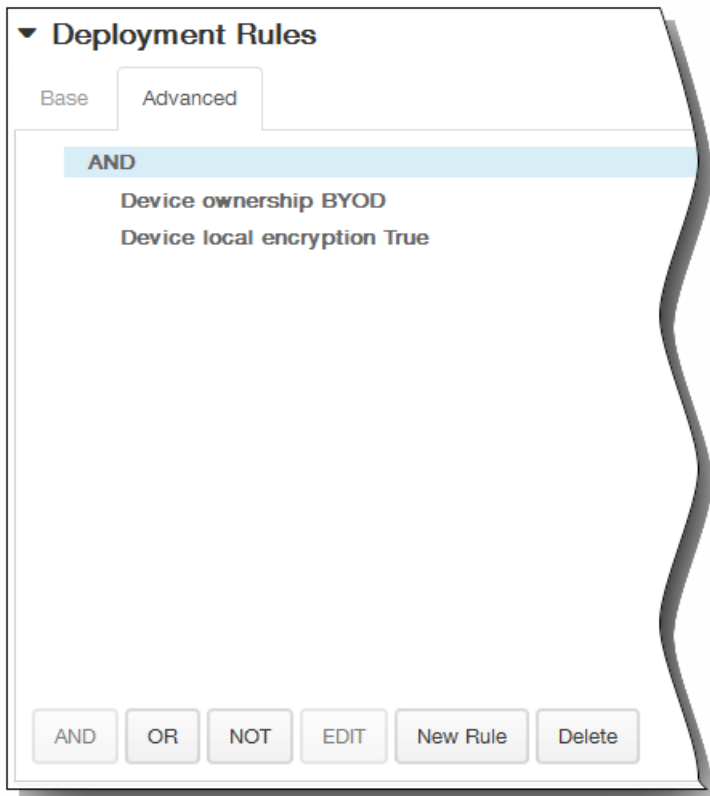
Credential type: Certificate is the only credential type for Windows 8.1 tablets.

The credential file path: Select the credential file by clicking Browse and then navigating to the file's location.

7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.

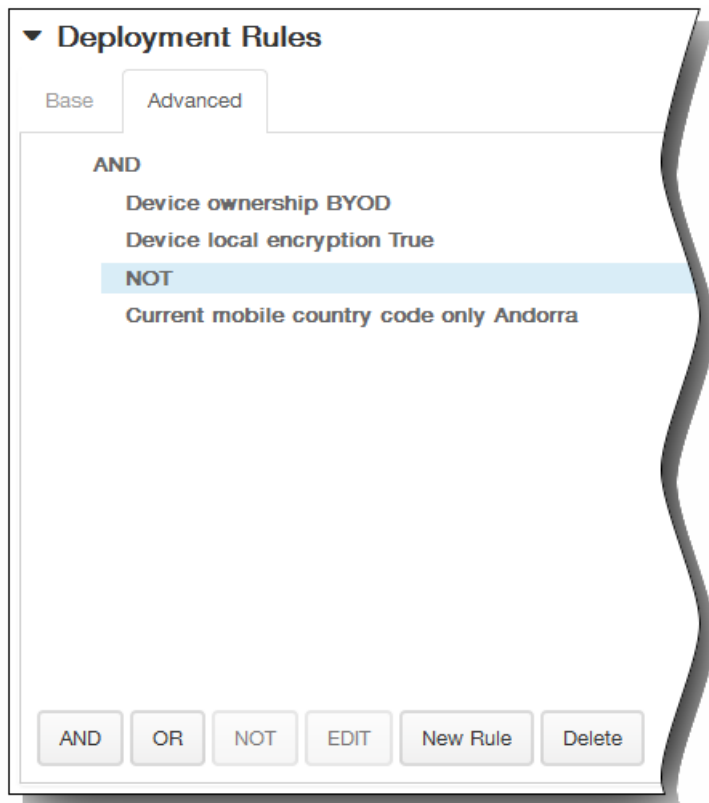


1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

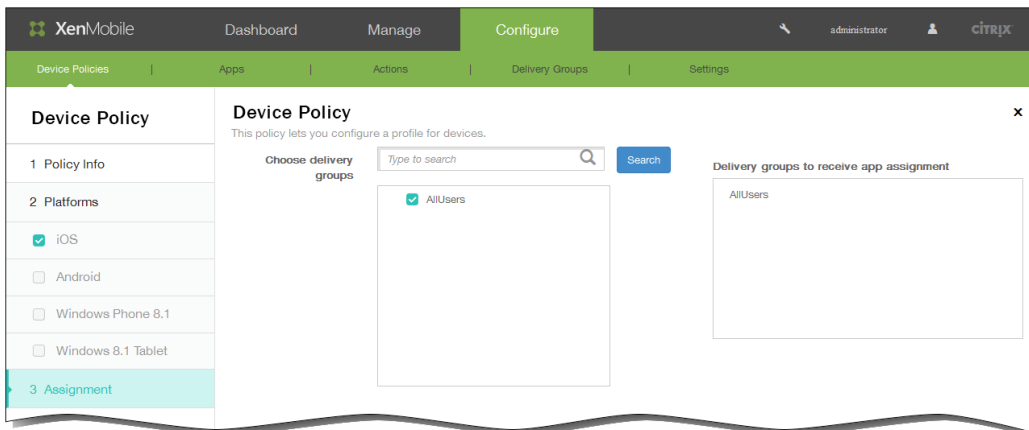


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.
In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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.

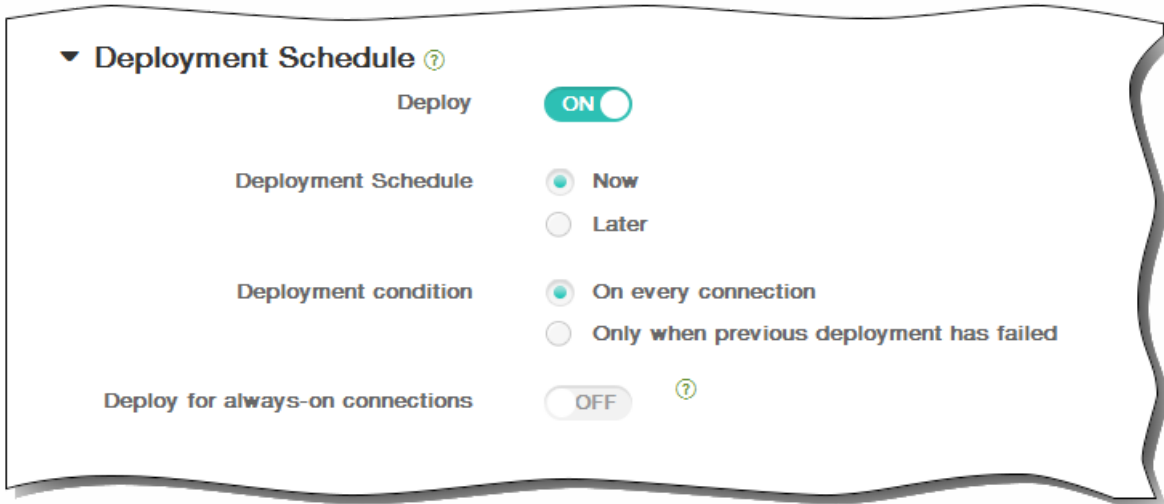


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

To add a Kiosk device policy for Samsung SAFE

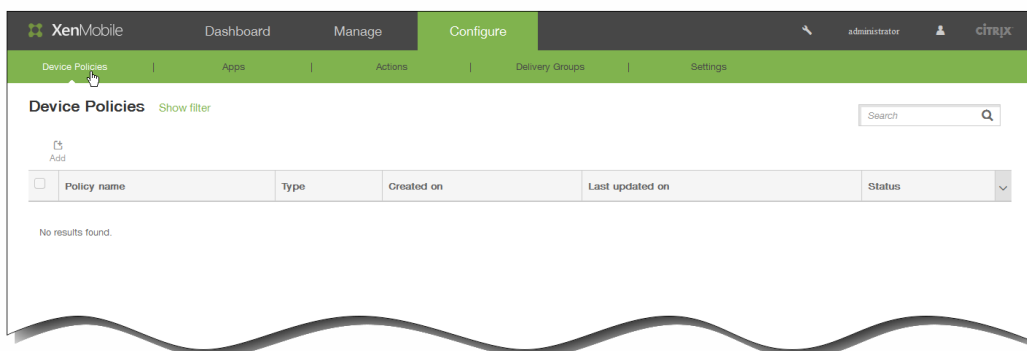
Feb 27, 2015

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.

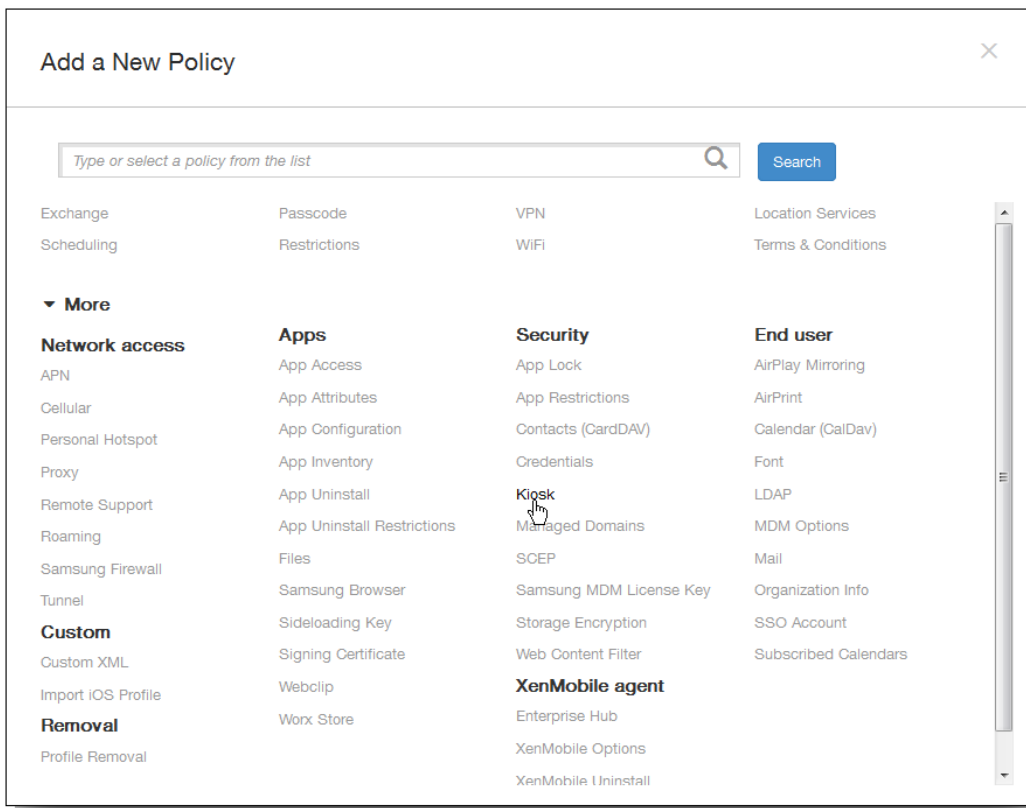
Note:

- 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 API 4.0 and later.

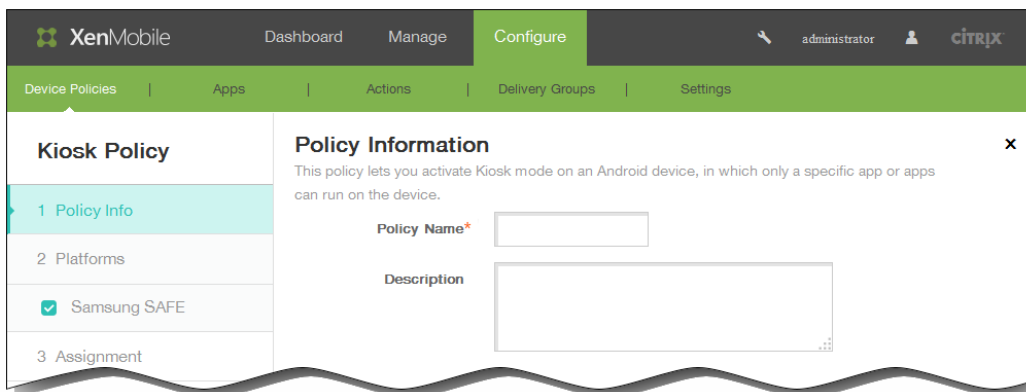
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



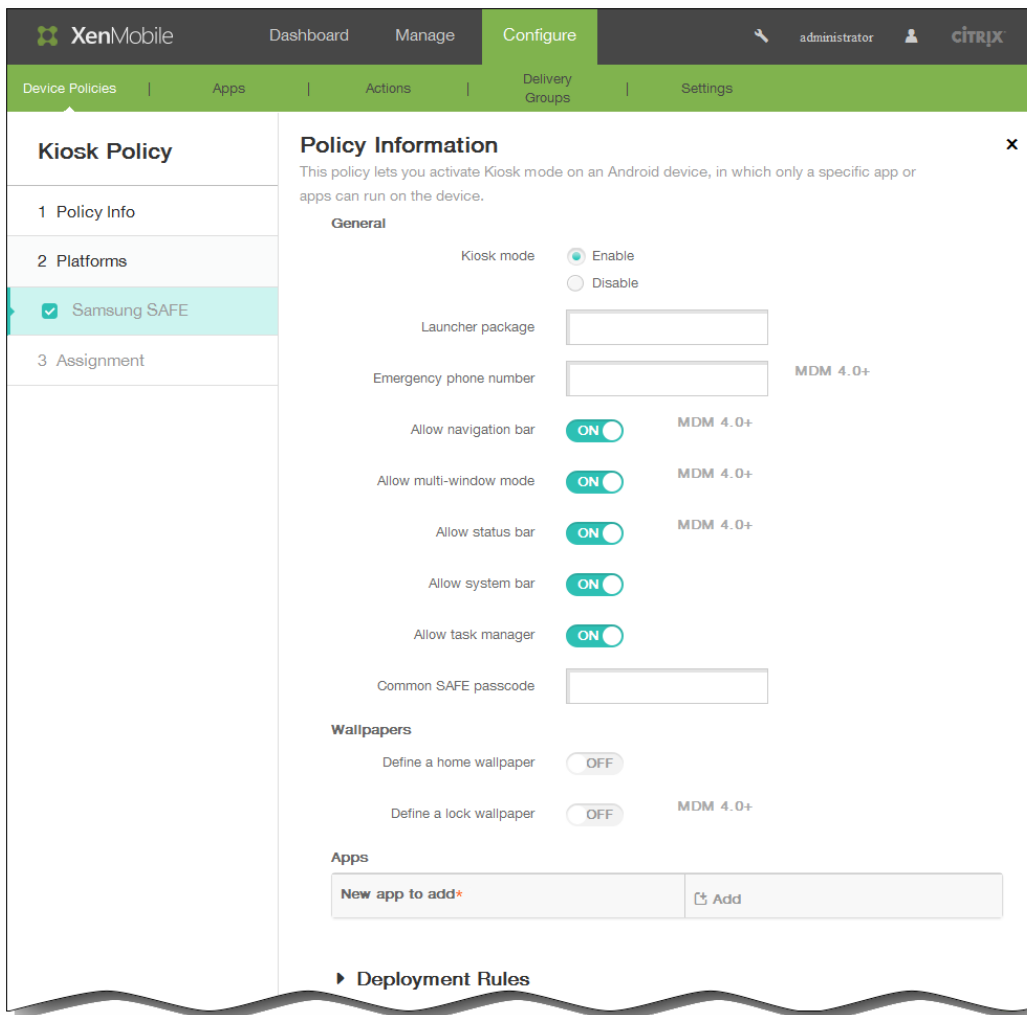
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



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

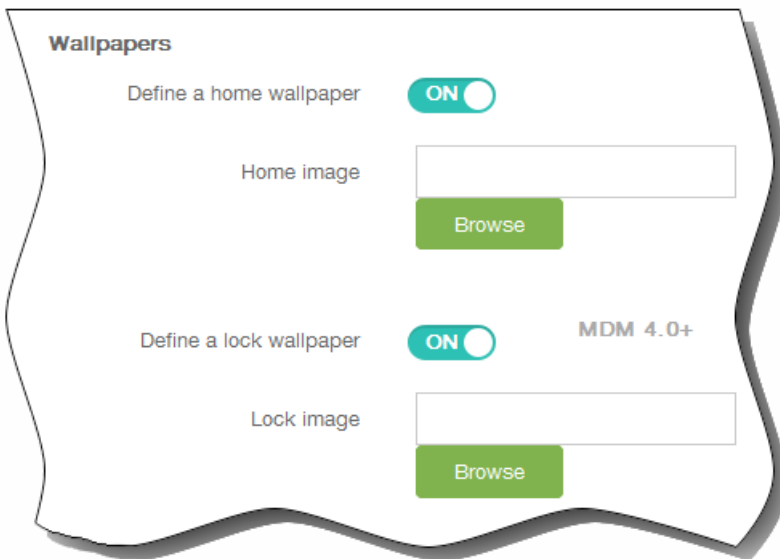


4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The Samsung SAFE Platform information page appears.



6. On the Samsung SAFE Platform information page, enter the following information:
 1. Kiosk mode: Click Enable or Disable. The default is Enable. When you click Disable, all the following options disappear.
 2. 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.
 3. 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 the Samsung Mobile Device Management API 4.0 and later.
 4. 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.
 5. Allow multi-window mode: Select whether to let users use multiple windows while in Kiosk mode. Applies only to MDM 4.0 and later.
 6. Allow status bar: Select whether to let users see the status bar while in Kiosk mode. Applies only to MDM 4.0 and later.
 7. Allow system bar: Select whether to let users see the system bar while in Kiosk mode.
 8. Allow task manager: Select whether to let users see and use the task manager while in Kiosk mode.
 9. Common SAFE passcode: If you have set a general passcode policy for all Samsung SAFE devices, enter that optional passcode in this field.
 10. Define a home wallpaper: Select whether to use a custom image for the home screen while in Kiosk mode. The default is OFF.

- Define a lock wallpaper: Select whether to use a custom image for the lock screen while in Kiosk mode. The default is OFF. Applies only to MDM 4.0 and later. When either of the preceding options is enabled, a field appears to let you select the custom image by clicking Browse and navigating to the image's location.



- Apps: 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 Add to add the app or click Cancel to cancel adding the app.
- Repeat steps i. and ii. for each app you want to add.

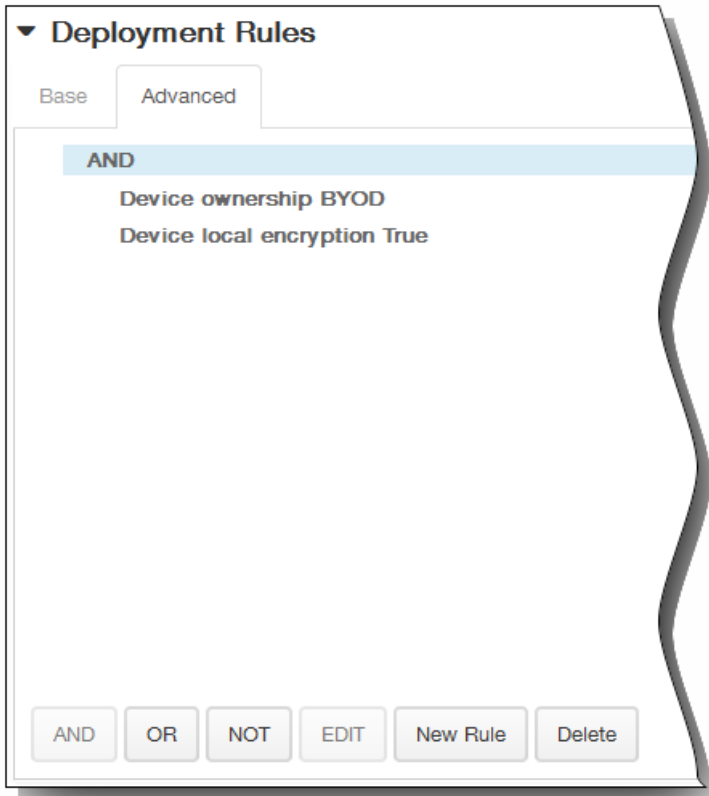
Note: To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing. To edit an existing app, hover over the line containing the listing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

- Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



- In the lists, click options to determine when the policy should be deployed.
 - You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.

2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

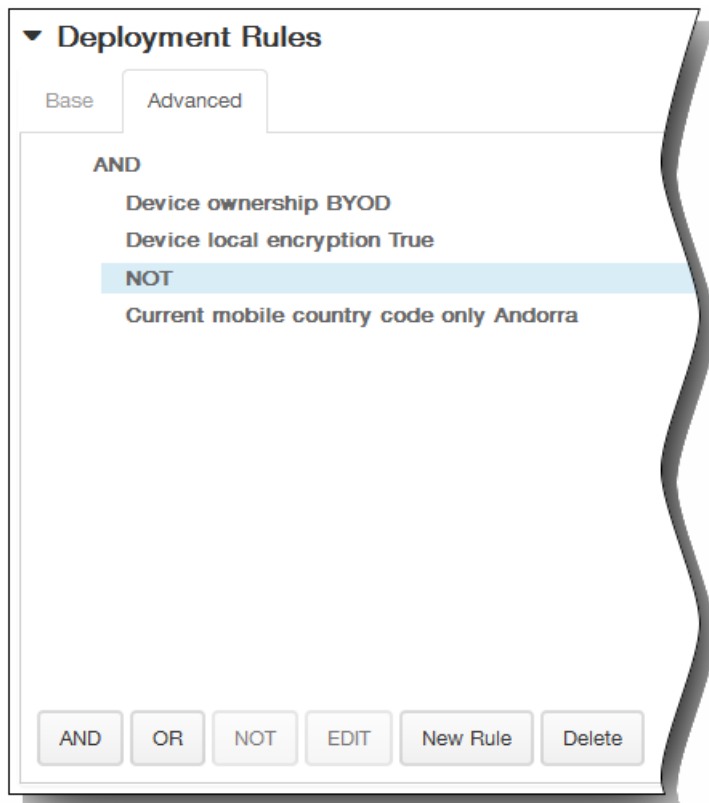


The conditions you chose on the Base tab appear.

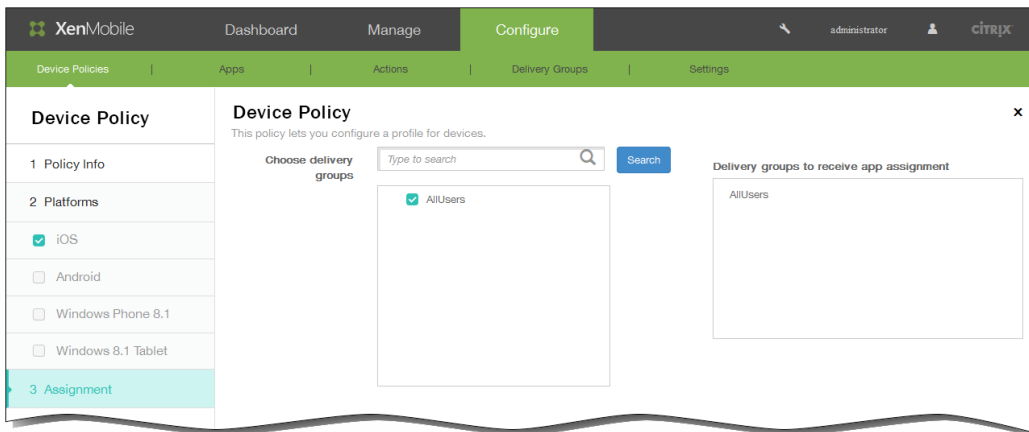
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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 right-hand Delivery groups to receive app assignment list.

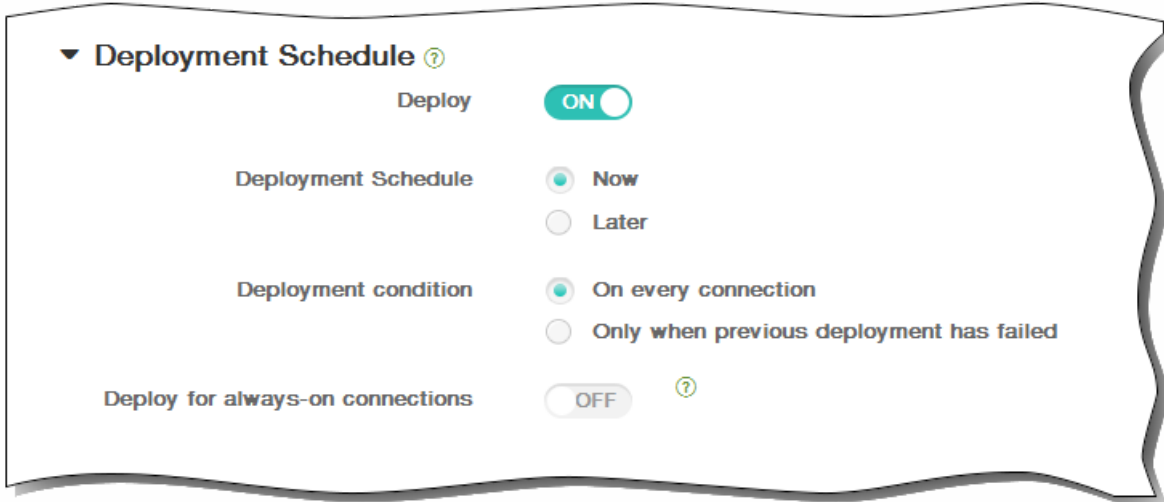


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

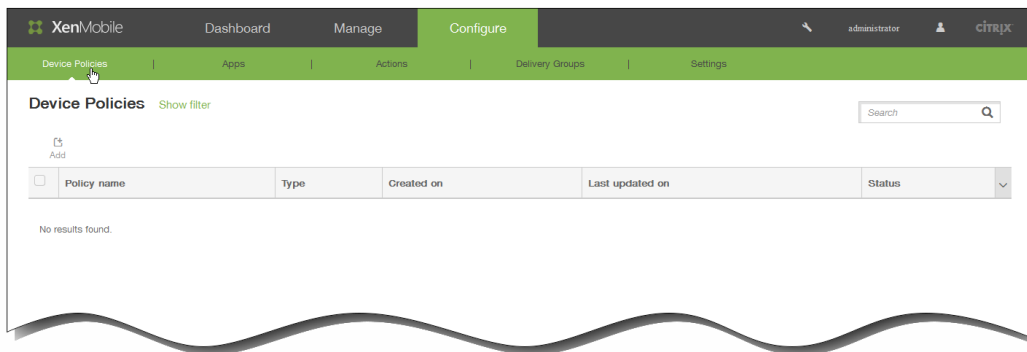
To add a font device policy for iOS

Mar 02, 2015

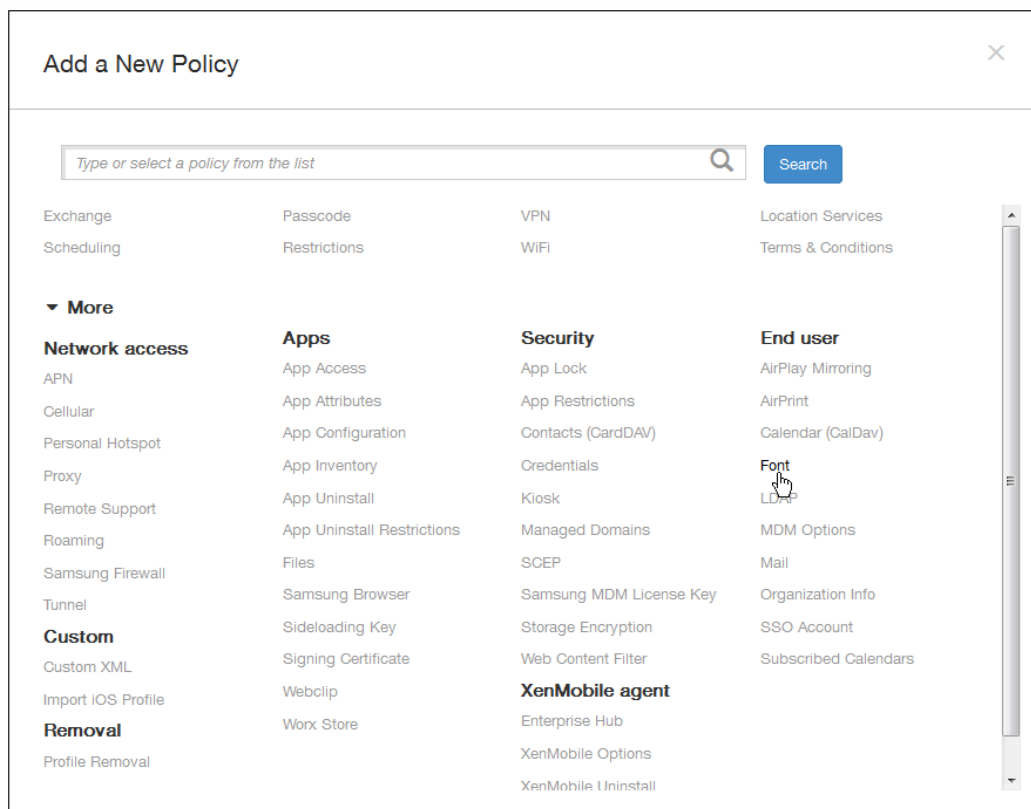
You can add a device policy in XenMobile to add additional fonts to users' devices. Fonts must be TrueType (.ttf) or OpenType (.oft) fonts. Font collections (.ttc or .otc) are not supported.

Note: This policy applies only to iOS 7.0 and later.

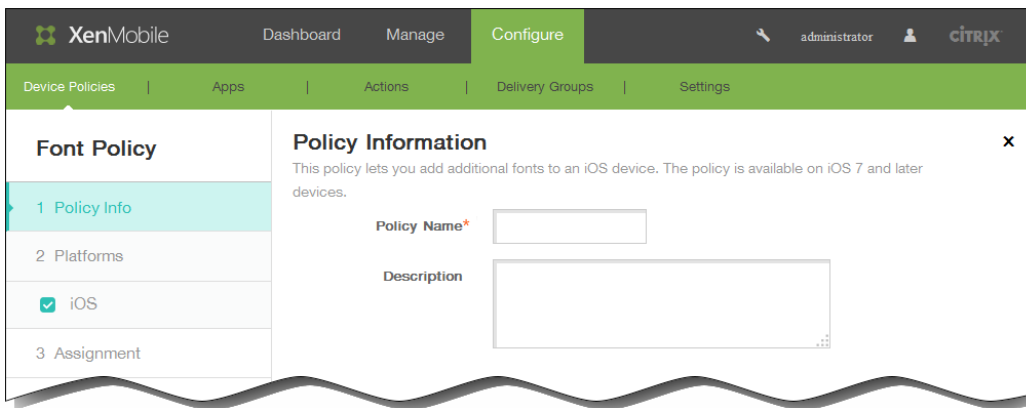
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



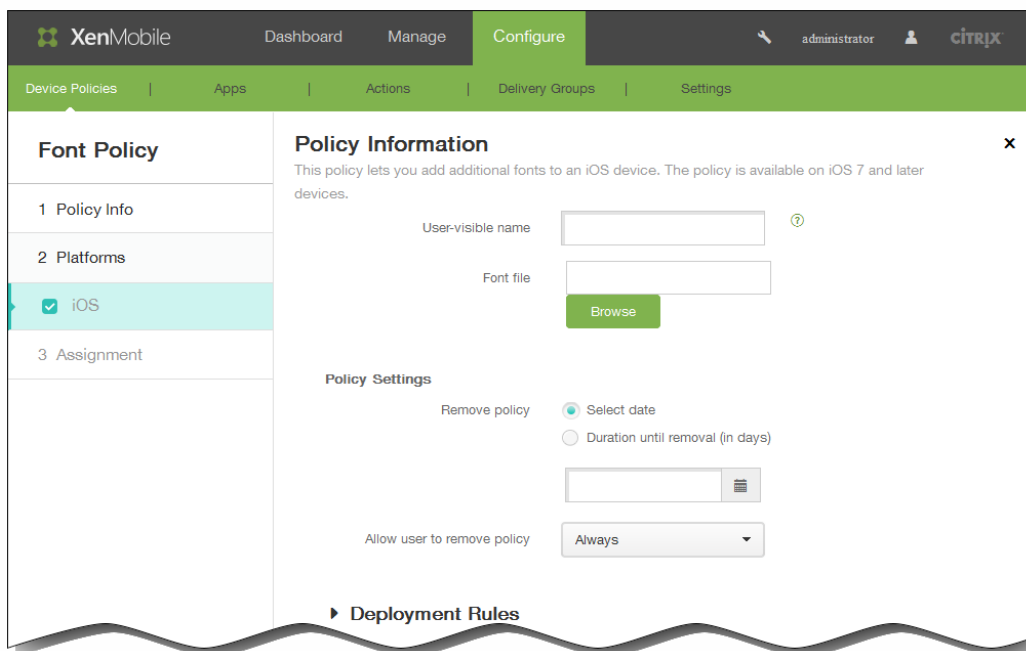
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



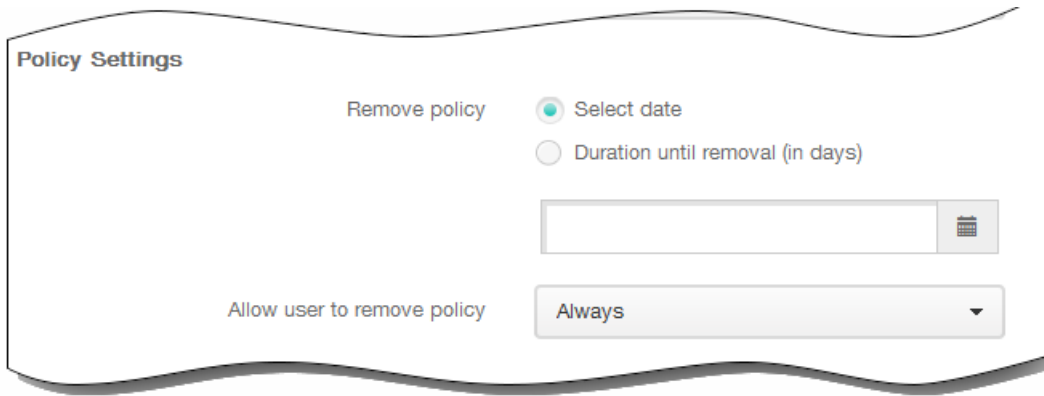
3. Click More and then, under End user, click Font. The Font Policy page appears.



4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform Information page appears.



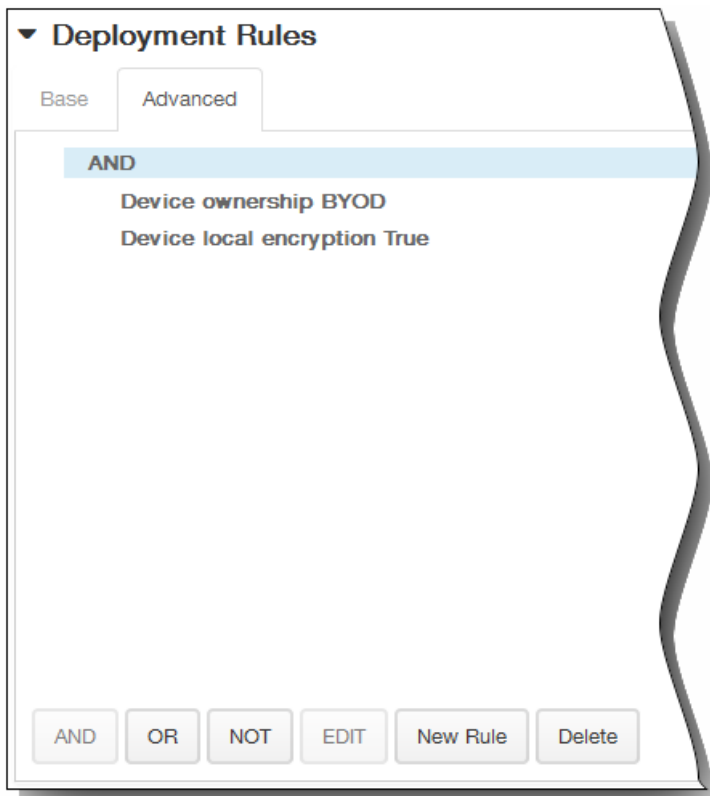
6. In the iOS Platform Information page, enter the following information:
 1. User-visible name: Enter the name that users see in their font lists.
 2. Font file: Select the font file to be added to users' devices by, clicking Browse and then navigating to the file's location.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

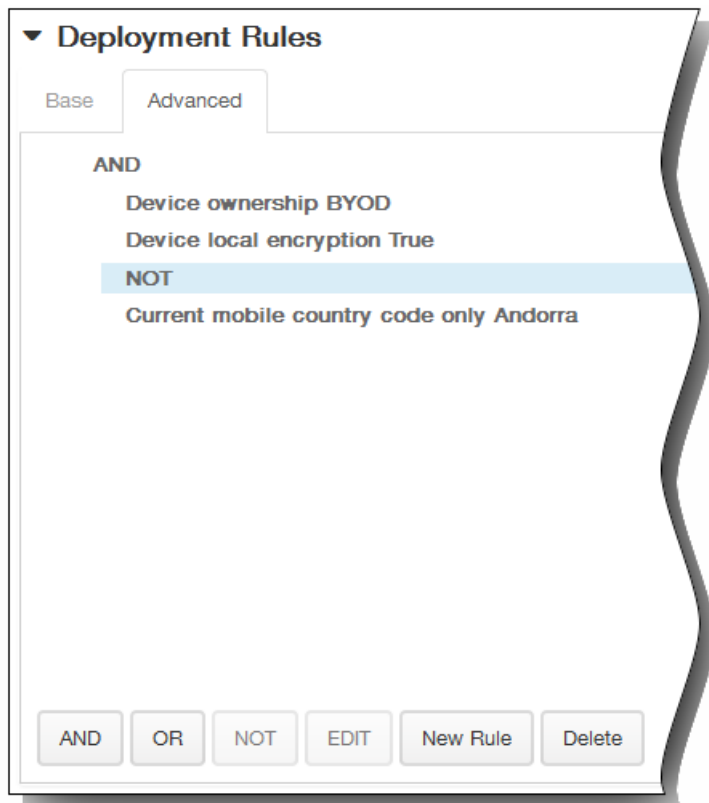


The conditions you chose on the Base tab appear.

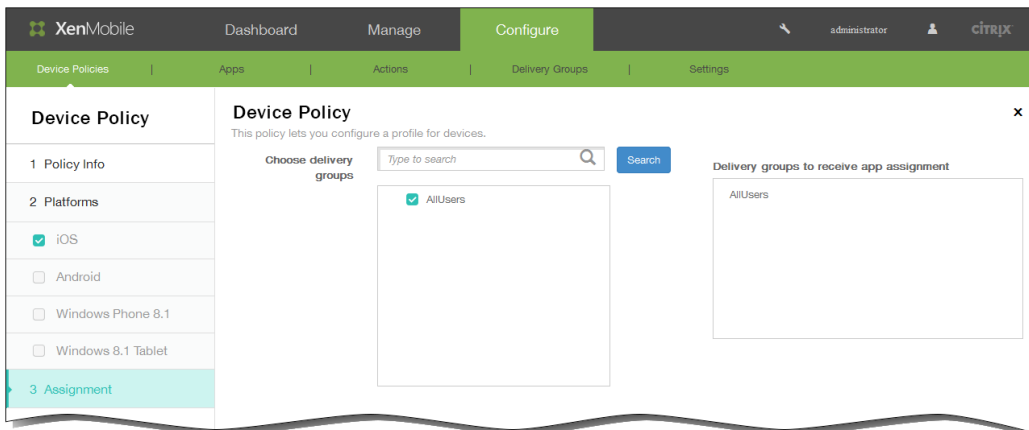
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The Font Policy assignment page appears.
13. 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.

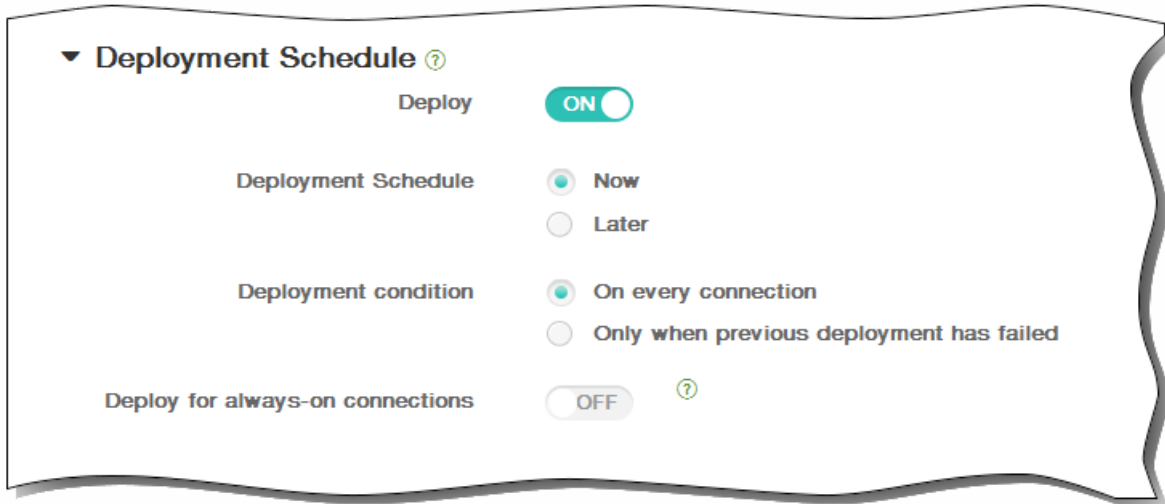


14. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



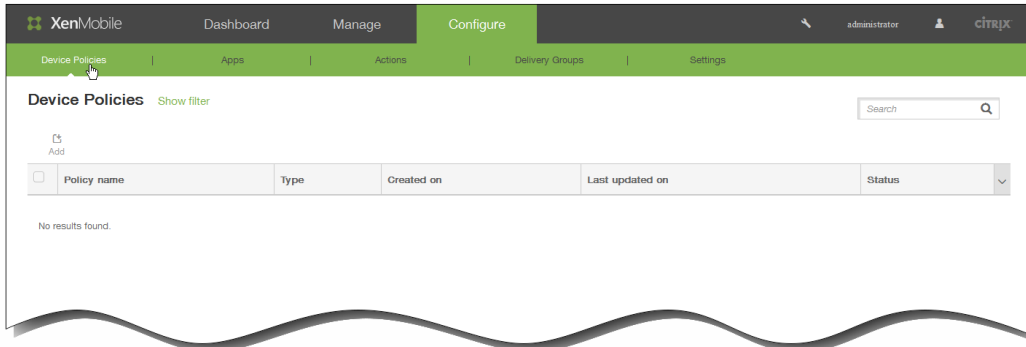
15. Click Save to save the policy.

To add a mail device policy for iOS

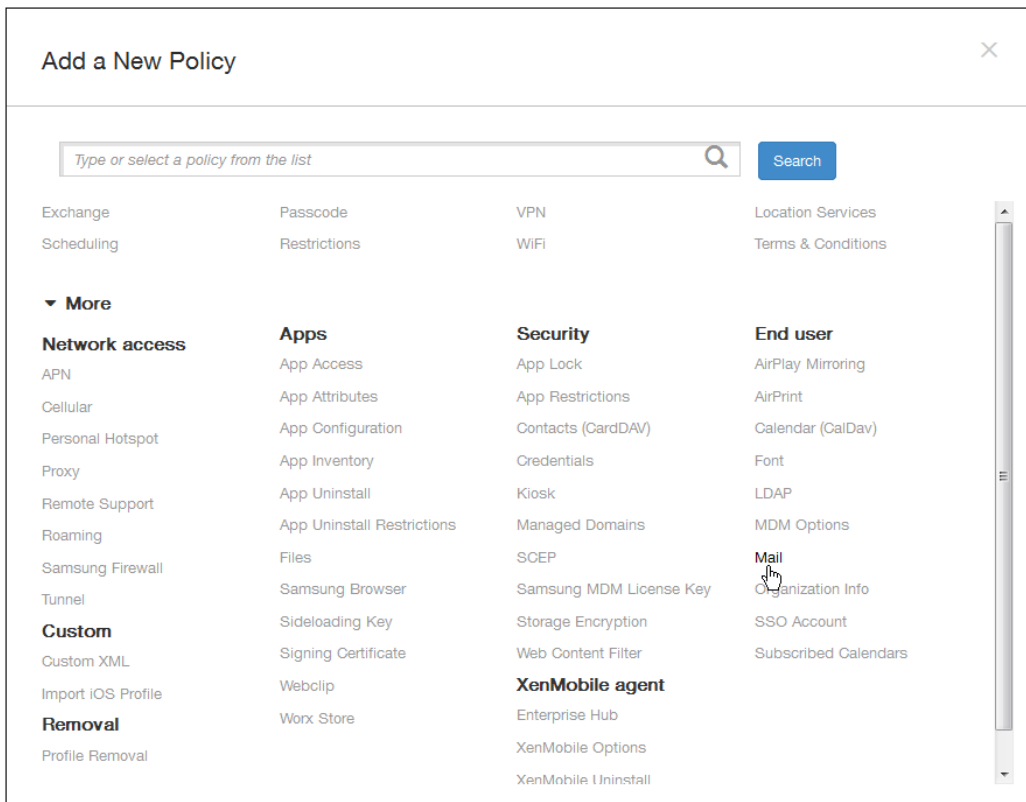
Apr 19, 2016

You can add a mail device policy in XenMobile to configure an email account on users' iOS devices.

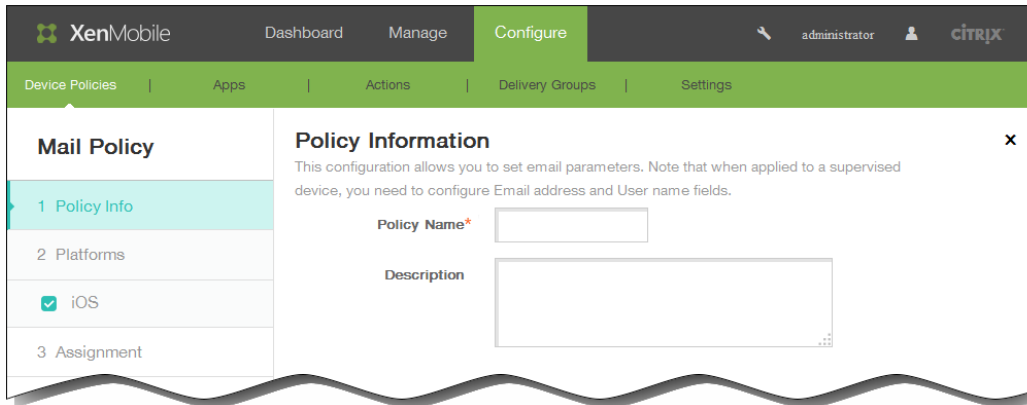
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform Information page appears.

XenMobile Dashboard Manage **Configure** administrator citrix

Device Policies | Apps | Actions | Delivery Groups | Settings

Mail Policy

- 1 Policy Info
- 2 Platforms
- iOS
- 3 Assignment

Policy Information

This configuration allows you to set email parameters. Note that when applied to a supervised device, you need to configure Email address and User name fields.

Account description*

Account type **IMAP**

Path prefix*

User display name*

Email address*

Incoming email

Email server host name*

Email server port* **143**

User name*

Authentication type **Password**

Password

Use SSL **OFF**

Outgoing email

Email server host name*

Email server port*

User name*

Authentication type **Password**

Password

Outgoing password same as incoming **OFF**

Use SSL **OFF**

Policy

Authorize email move between accounts **OFF** iOS 5.0+

Sending email only from mail app **OFF** iOS 5.0+

Disable mail recents syncing **OFF** iOS 6.0+

Enable S/MIME **OFF** iOS 5.0+

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy **Always**

► Deployment Rules

6. In the iOS Platform Information page, enter the following information:

1. Account description: Enter an account description that appears in the Mail and Settings apps. This field is required.
2. 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.
3. Path prefix: Enter INBOX or your IMAP mail account path prefix if it is not INBOX. This field is required.
4. User display name: Enter the full user name to be used for messages and so on. This field is required.
5. Email address: Enter the full email address for the account. This field is required.

Incoming email settings

6. Email server host name: Enter the incoming mail server host name or IP address. This field is required.
7. Email server port: Enter the incoming mail server port number. The default is 143. This field is required.
8. User name: Enter 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.
9. 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.
10. Password: Enter an optional password for the incoming mail server.
11. Use SSL: Select whether the incoming mail server uses Secure Socket Layer authentication. The default is OFF.

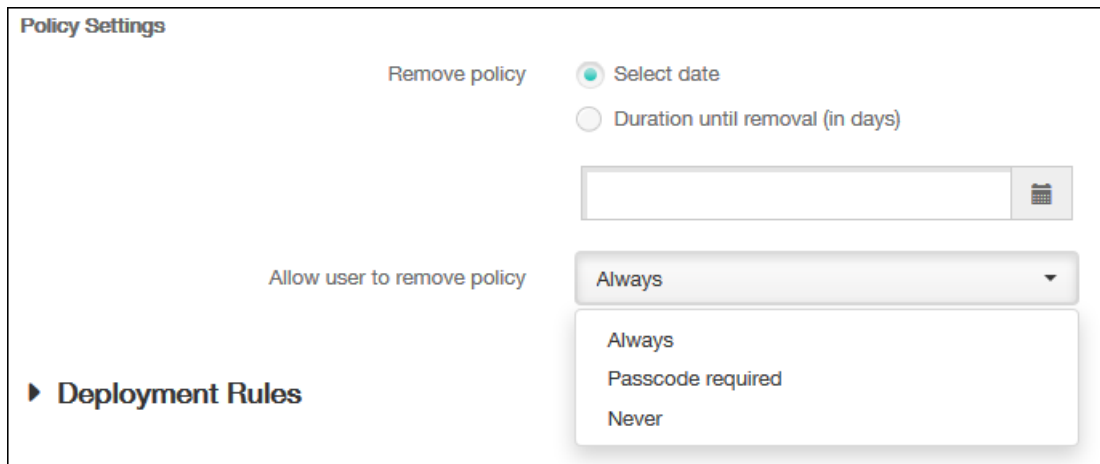
Outgoing email settings

12. Email server host name: Enter the outgoing mail server host name or IP address. This field is required.
13. Email server port: Enter the outgoing mail server port number. If not port you do not enter a port number, the default port for the given protocol is used.
14. User name: Enter 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.
15. 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.
16. Password: Enter an optional password for the outgoing mail server.
17. 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.
18. Use SSL: Select whether the outgoing mail server uses Secure Socket Layer authentication. The default is OFF.

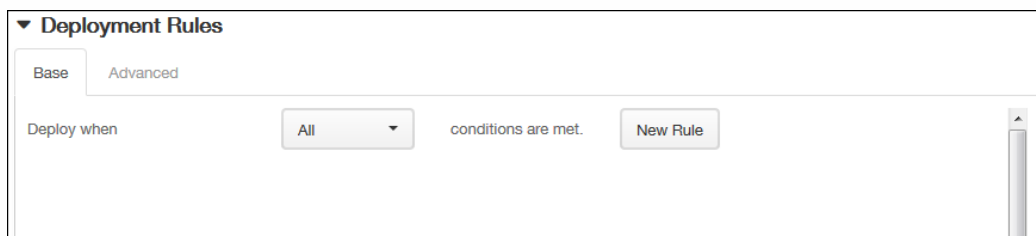
Policy settings

Note: The options apply only to iOS 5.0 and later.

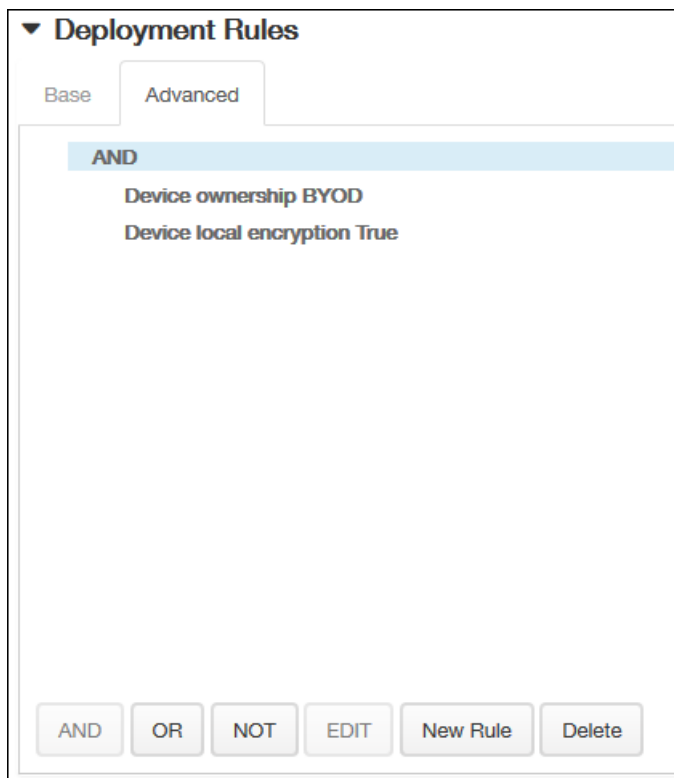
19. Authorize email move between accounts: Select whether to allow users to move email out of this account into another account and to forward and reply from a different account. The default is OFF, which allows users to move emails into another account and to forward or reply from a different account.
20. Sending email only from mail app: Select whether to restrict users to the iOS mail app for sending email.
21. 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.
22. 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.
23. Signing identity credential: In the list, select the signing credential to be used.
24. Encryption identity credential: In the list, select the encryption credential to be used.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.

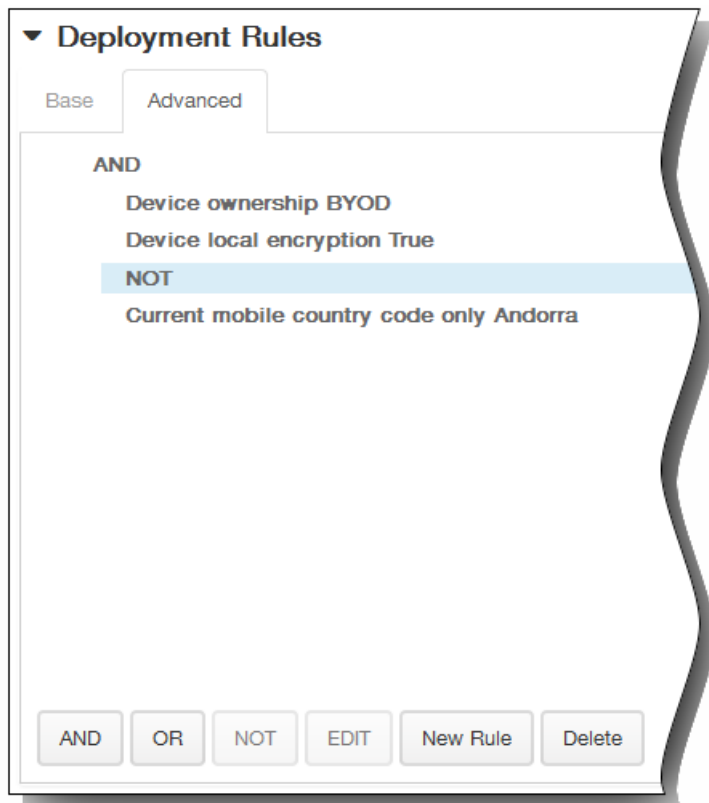
1. Click AND, OR, or NOT.

2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

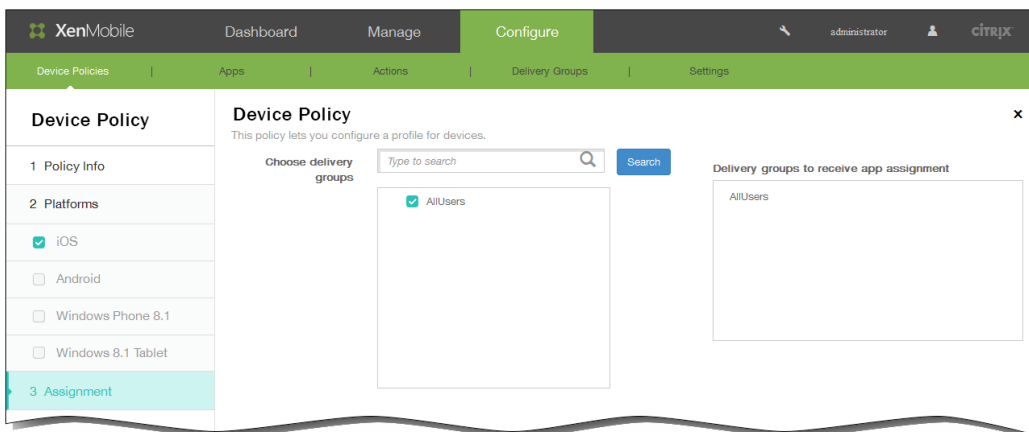
3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The Mail Policy assignment page appears.

13. 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.



14. Expand Deployment Schedule and then configure the following settings:

1. 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.
2. Next to Deployment schedule, click Now or Later. The default option is Now.
3. If you click Later, click the calendar icon and then select the date and time for deployment.

- Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 - Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.
- Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.

The screenshot shows a settings panel titled "Deployment Schedule" with a help icon. It contains four settings:

- Deploy:** A toggle switch currently set to "ON".
- Deployment Schedule:** Radio buttons for "Now" (selected) and "Later".
- Deployment condition:** Radio buttons for "On every connection" (selected) and "Only when previous deployment has failed".
- Deploy for always-on connections:** A toggle switch currently set to "OFF" with a help icon.

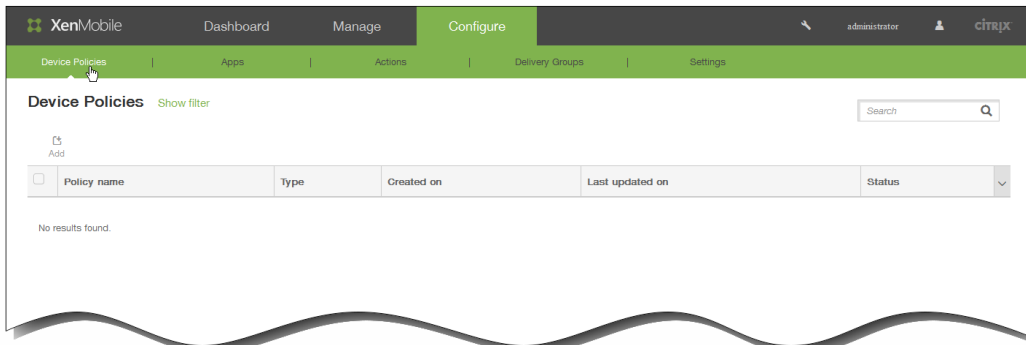
- Click Save to save the policy.

To add an organization information device policy for iOS

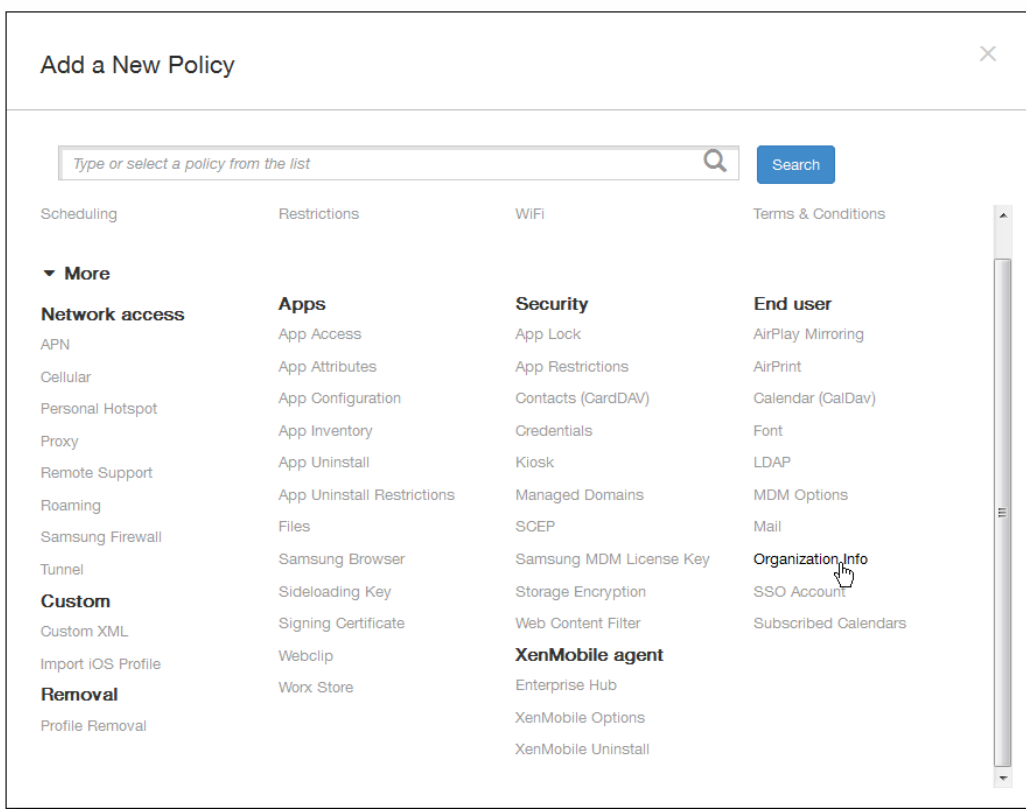
Feb 13, 2015

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.

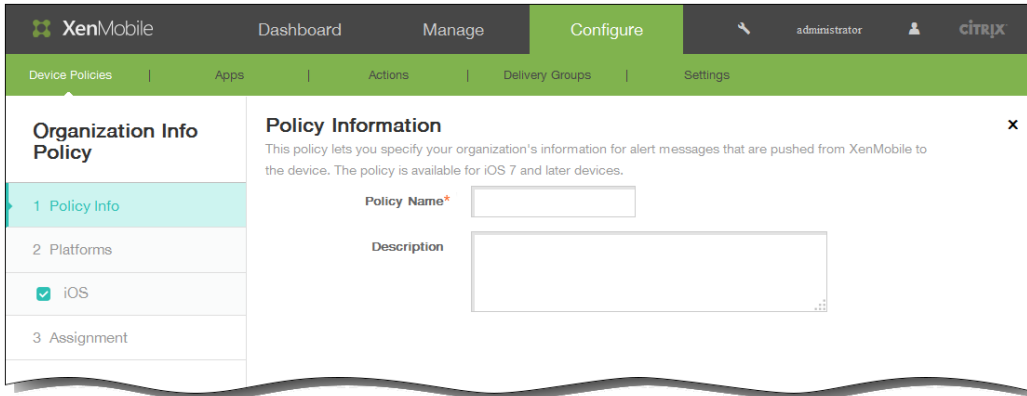
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



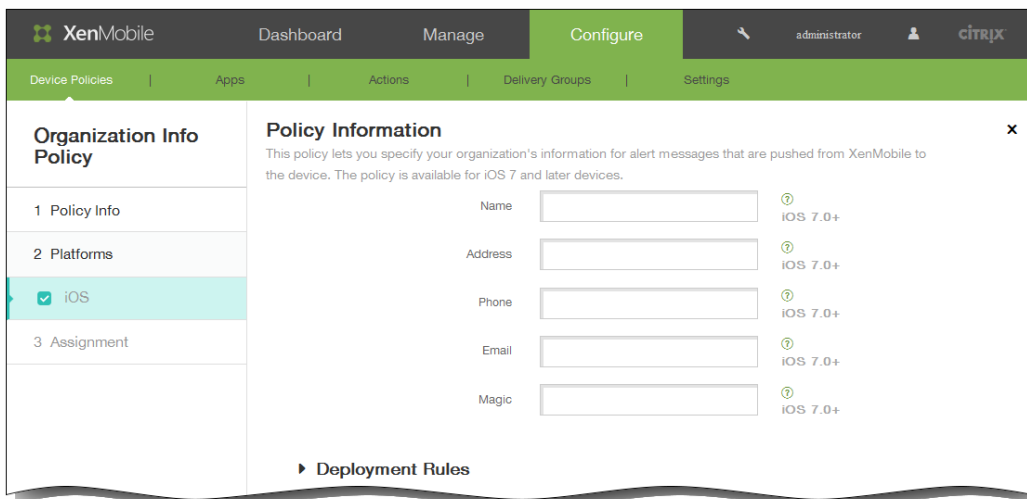
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



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



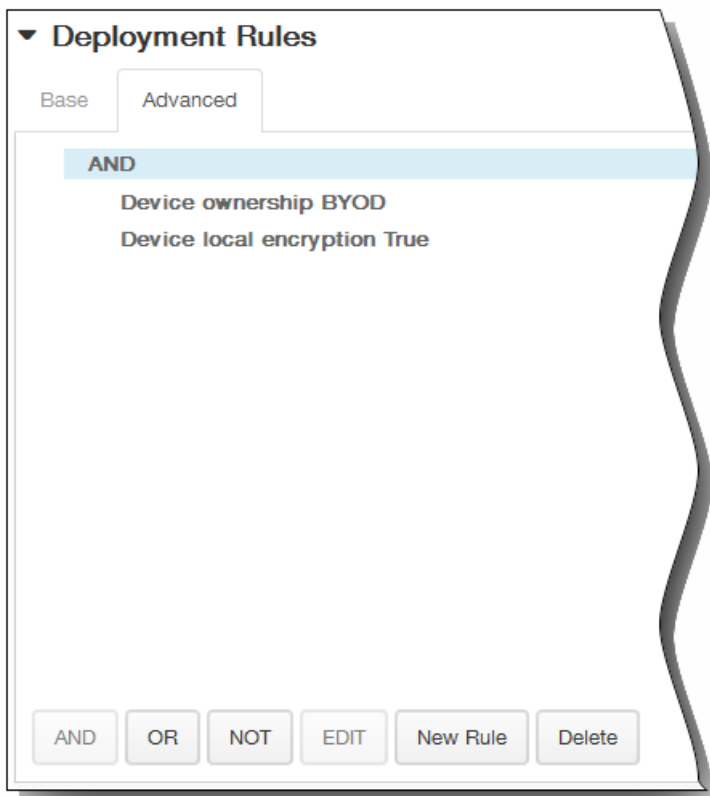
4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: If desired, type a description of the policy.
5. Click Next. The iOS Platform Information page appears.



6. In the iOS Platform Information page, enter the following information:
 1. Name: Type the name of the organization running XenMobile.
 2. Address: Type the organization's address.
 3. Phone: Type the organization's support phone number.
 4. Email: Type the support email address.
 5. Magic: Type a word or phrase that describes the services managed by the organization.
7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

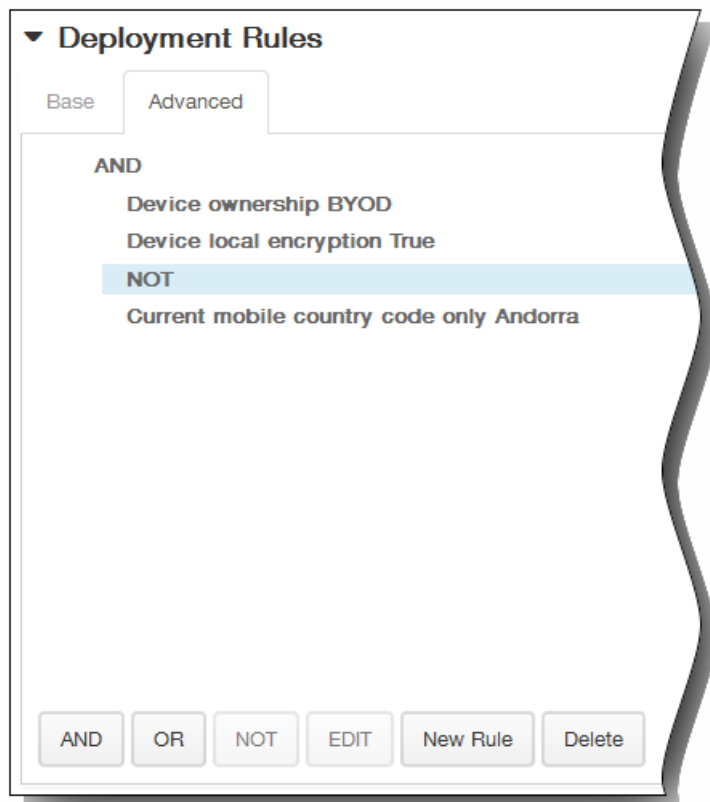


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

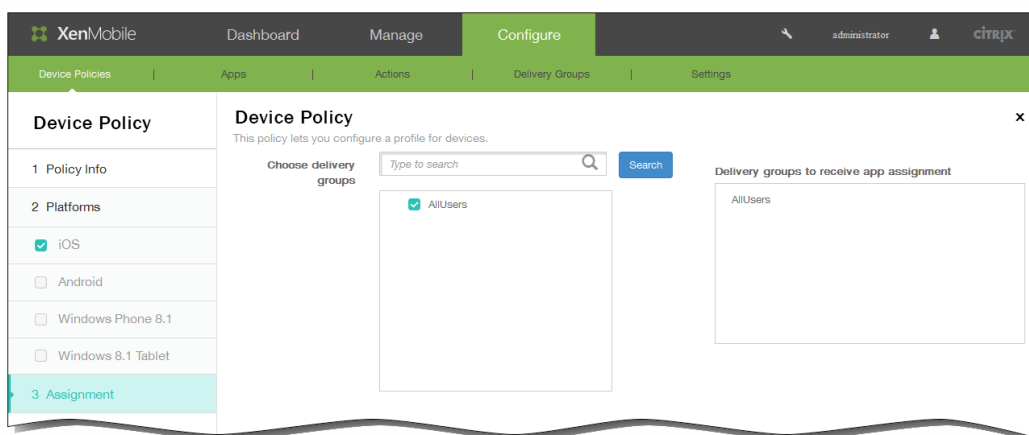
3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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 right-hand Delivery groups to receive app assignment list.

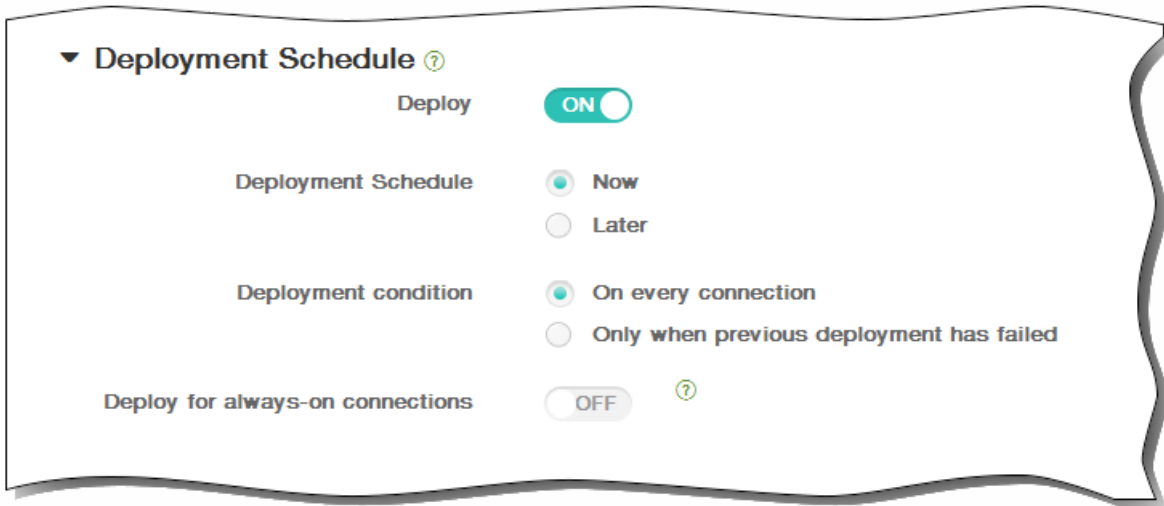


10. Expand Deployment Schedule and then configure the following settings:

1. 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.
2. Next to Deployment schedule, click Now or Later. The default option is Now.

3. If you click Later, click the calendar icon and then select the date and time for deployment.
4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

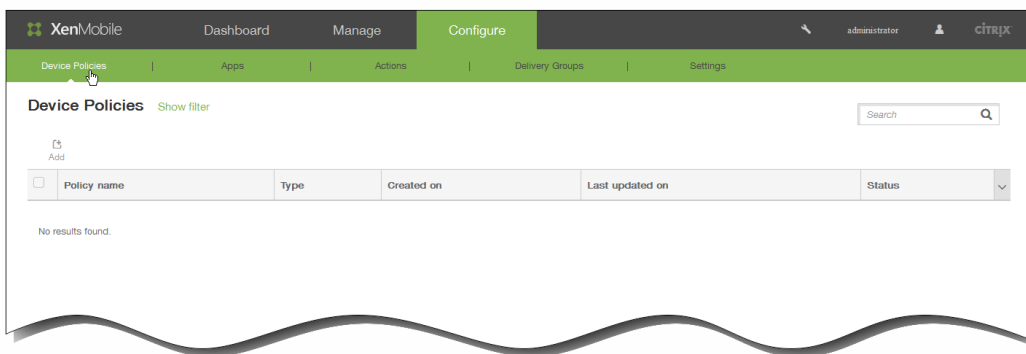
To add an LDAP device policy for iOS

Mar 03, 2015

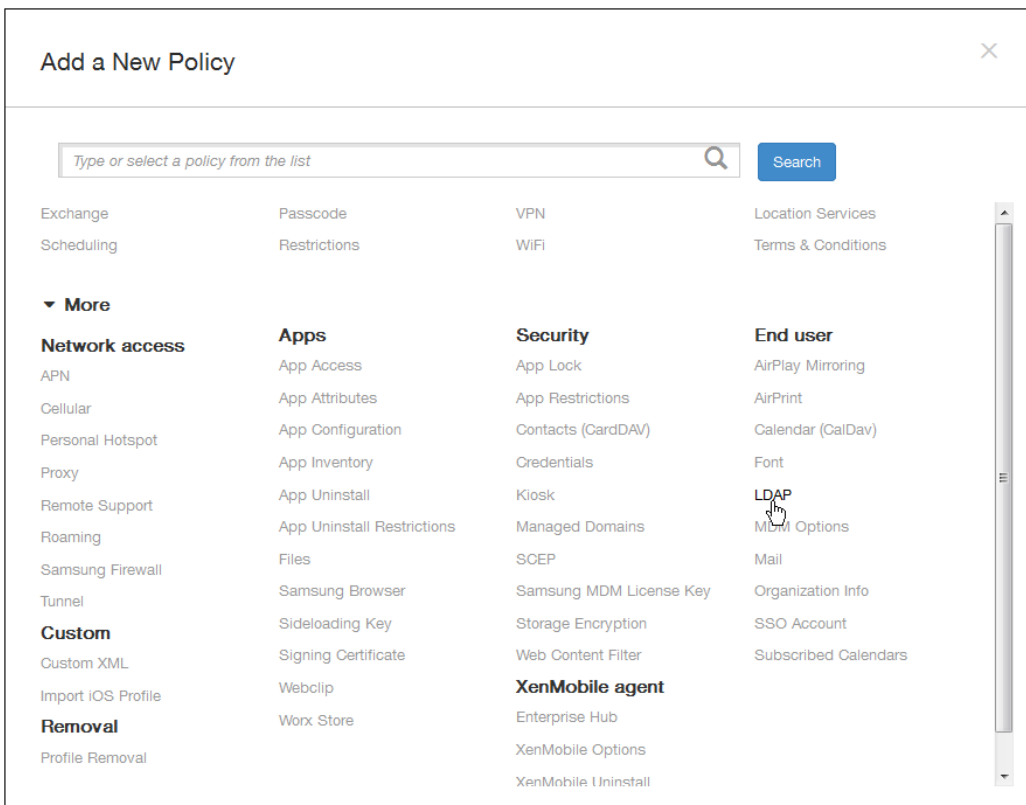
You create an LDAP policy for iOS devices in XenMobile to provide information about an LDAP server to use, including any necessary account information. The policy also provides a set of LDAP search policies to use when querying the LDAP server.

You need the LDAP host name before configuring this policy.

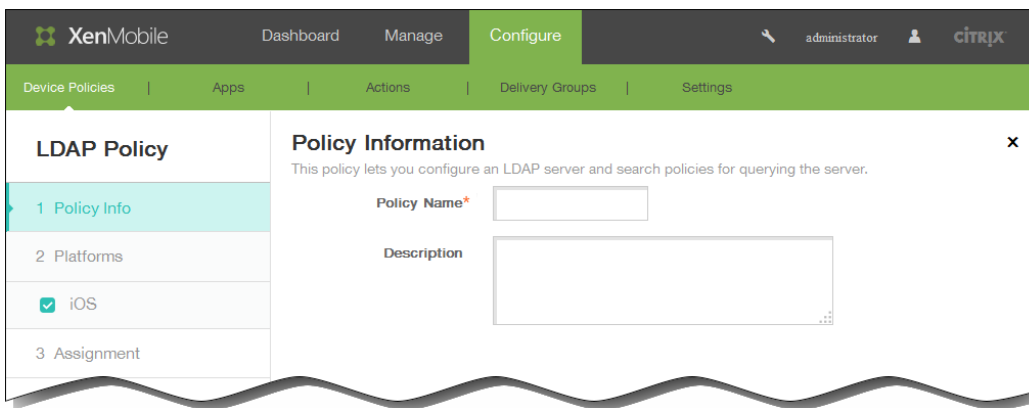
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



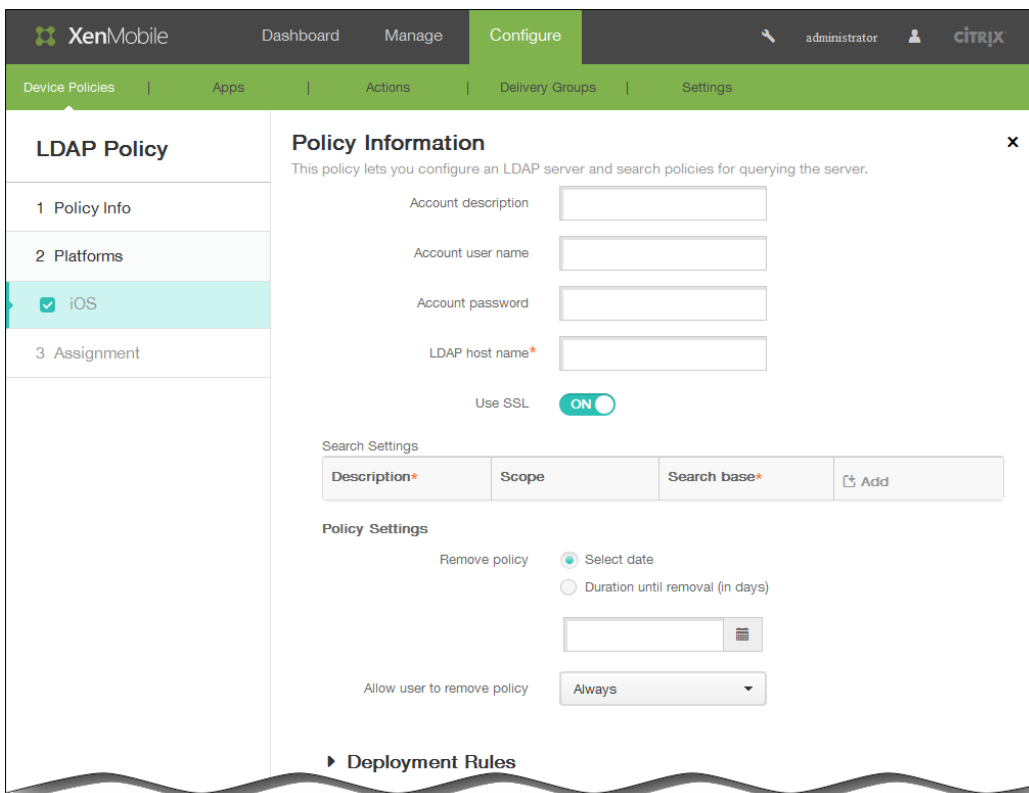
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



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



4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform information page appears.



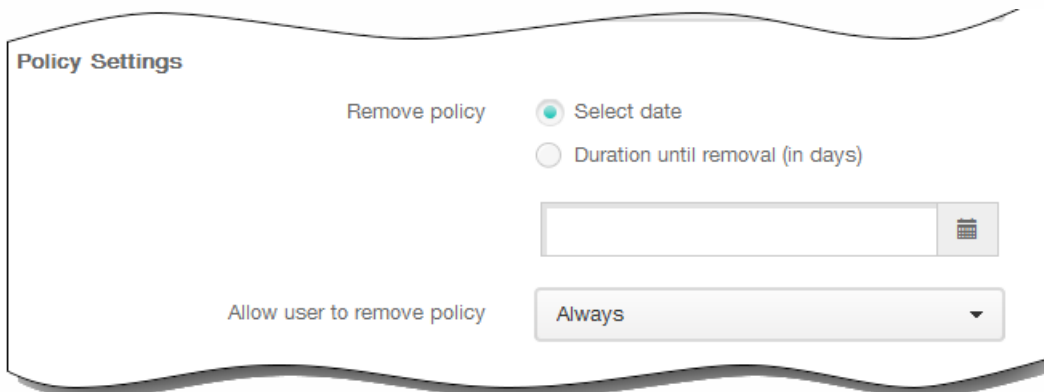
6. On the iOS Platform information page, enter the following information:
 1. Account description: Enter an optional account description.
 2. Account user name: Enter an optional user name.
 3. Account password: Enter an optional password. Use this only with encrypted profiles.
 4. LDAP host name: Enter the LDAP server host name. This field is required.

5. Use SSL: Select whether to use a Secure Socket Layer connection to the LDAP server. The default is ON.
6. Search Settings: Click Add and then do the following:

Note: You can enter as many search settings as you want, but you should add at least one search setting to make the account useful.

 1. Description: Enter a description of the search setting. This field is required.
 2. 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.
 3. Search base: Enter the path to the node at which to start searching. For example, ou=people or O=example corp. This field is required.
 4. Click Add to add the search setting or click Cancel to cancel adding the search setting.
 5. Repeat steps i. through iv. for each search setting you want to add.

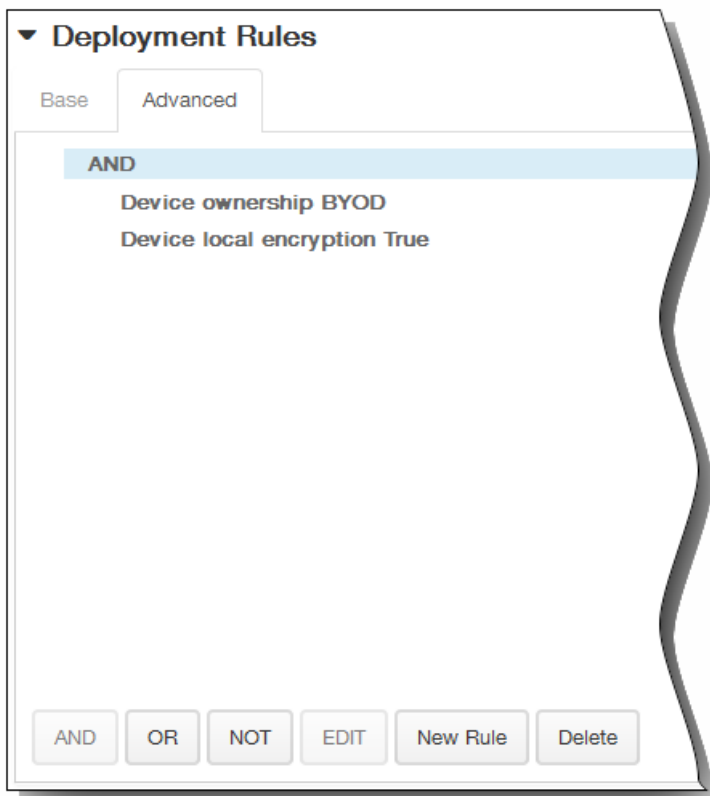
Note: To delete an existing search setting, hover over the line containing the listing and click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing. To edit an existing search setting, hover over the line containing 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.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



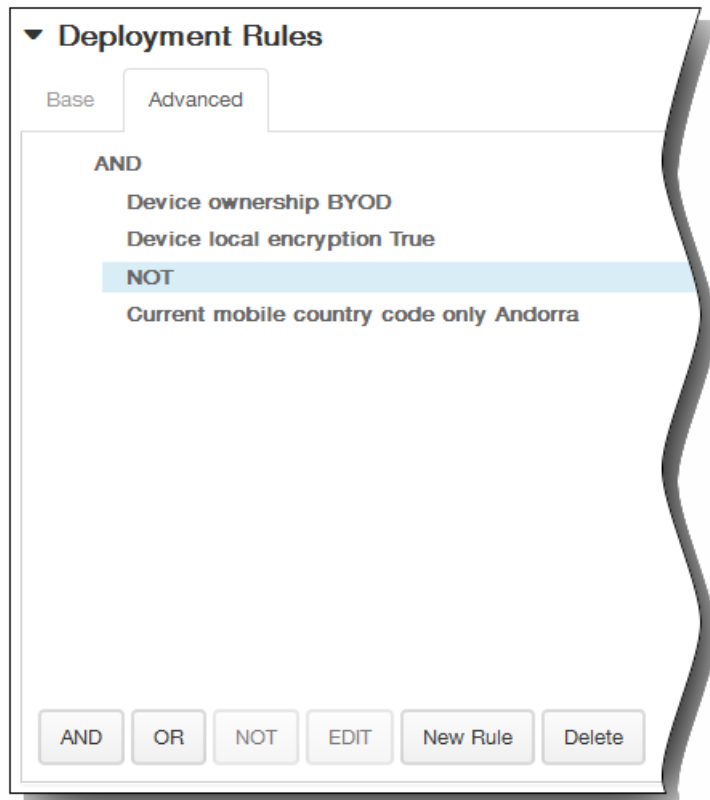
The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

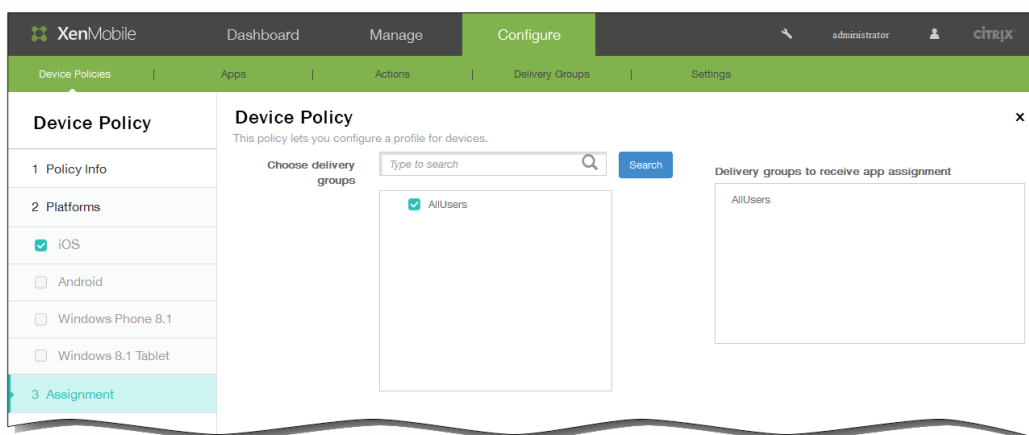
3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The LDAP Policy assignment page appears.

13. 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.

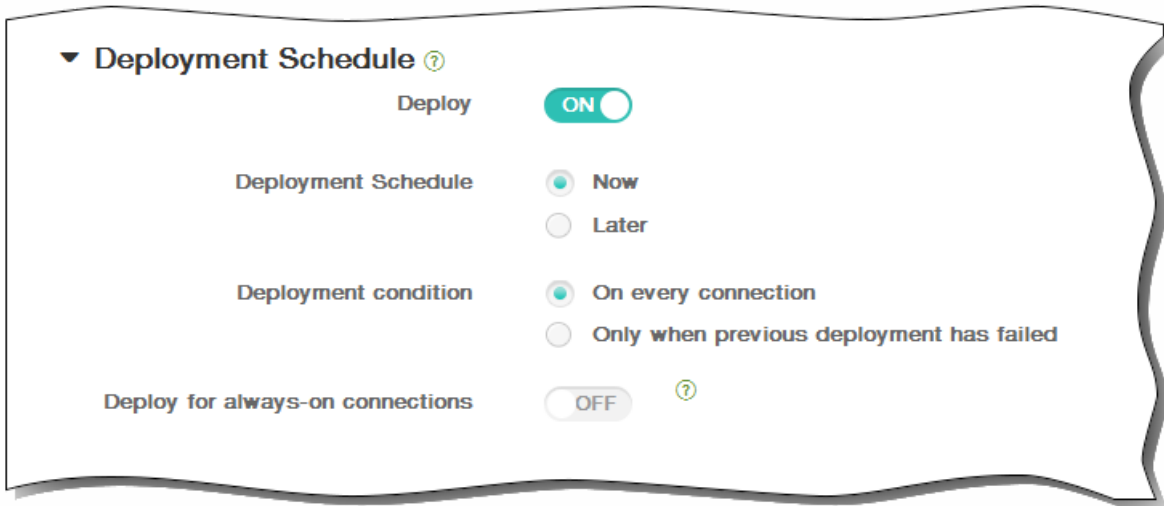


14. Expand Deployment Schedule and then configure the following settings:

1. 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.
2. Next to Deployment schedule, click Now or Later. The default option is Now.

3. If you click Later, click the calendar icon and then select the date and time for deployment.
4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



15. Click Save to save the policy.

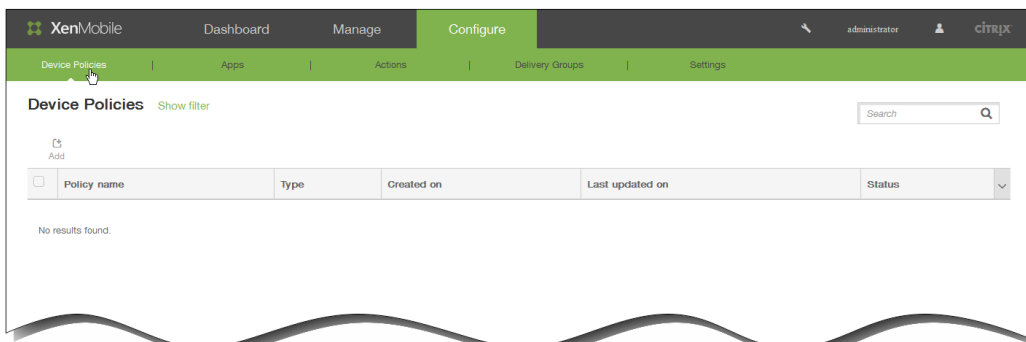
To add a single sign-on account device policy for iOS

Mar 03, 2015

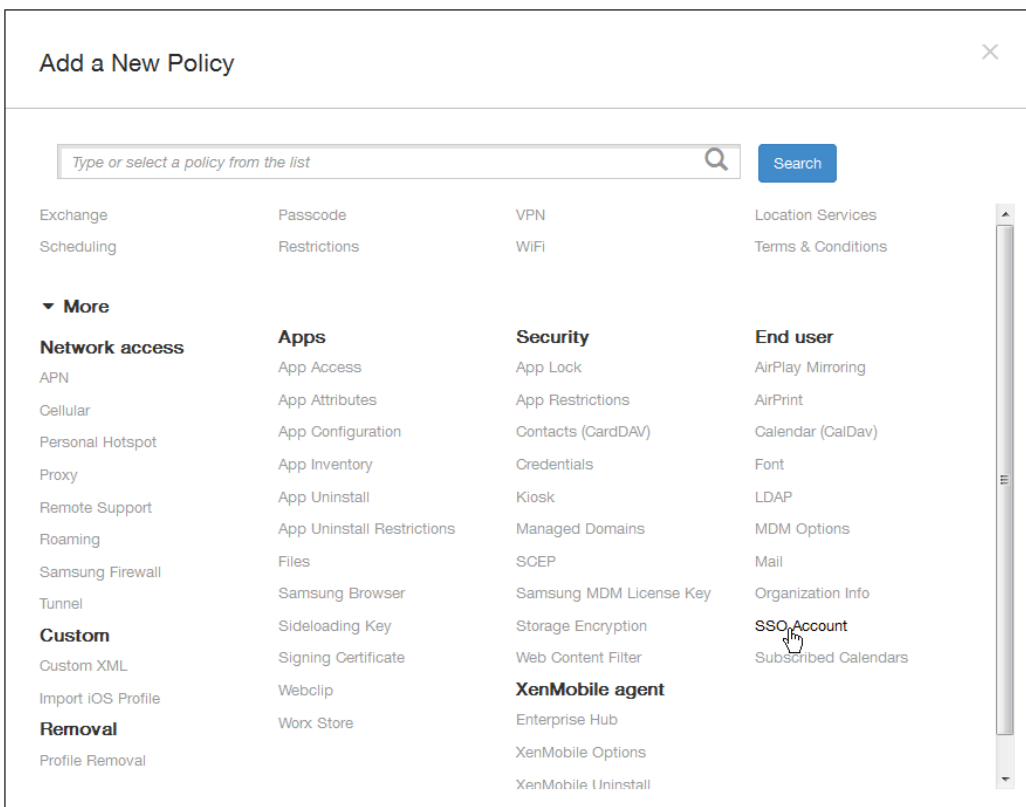
You create single sign-on (SSO) accounts in XenMobile to let users sign on one-time only to access XenMobile and your internal company resources from various apps. Users do not need to store any credentials on the device. The SSO account enterprise user credentials are used across apps, including apps 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.

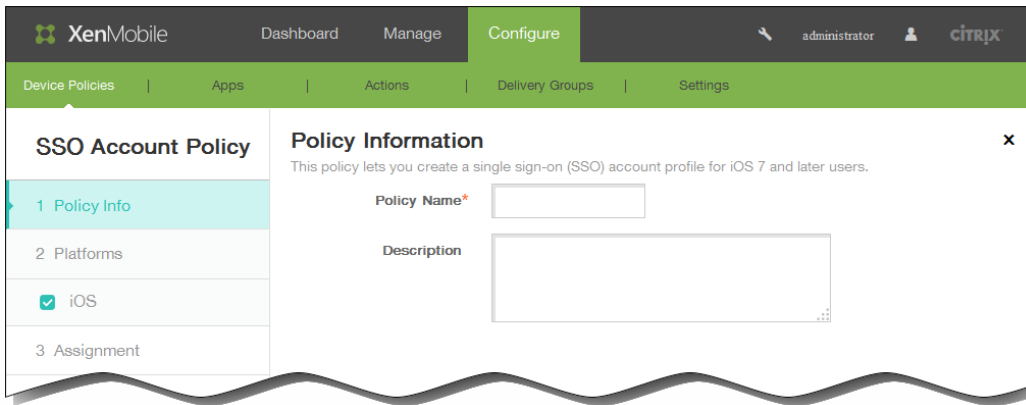
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



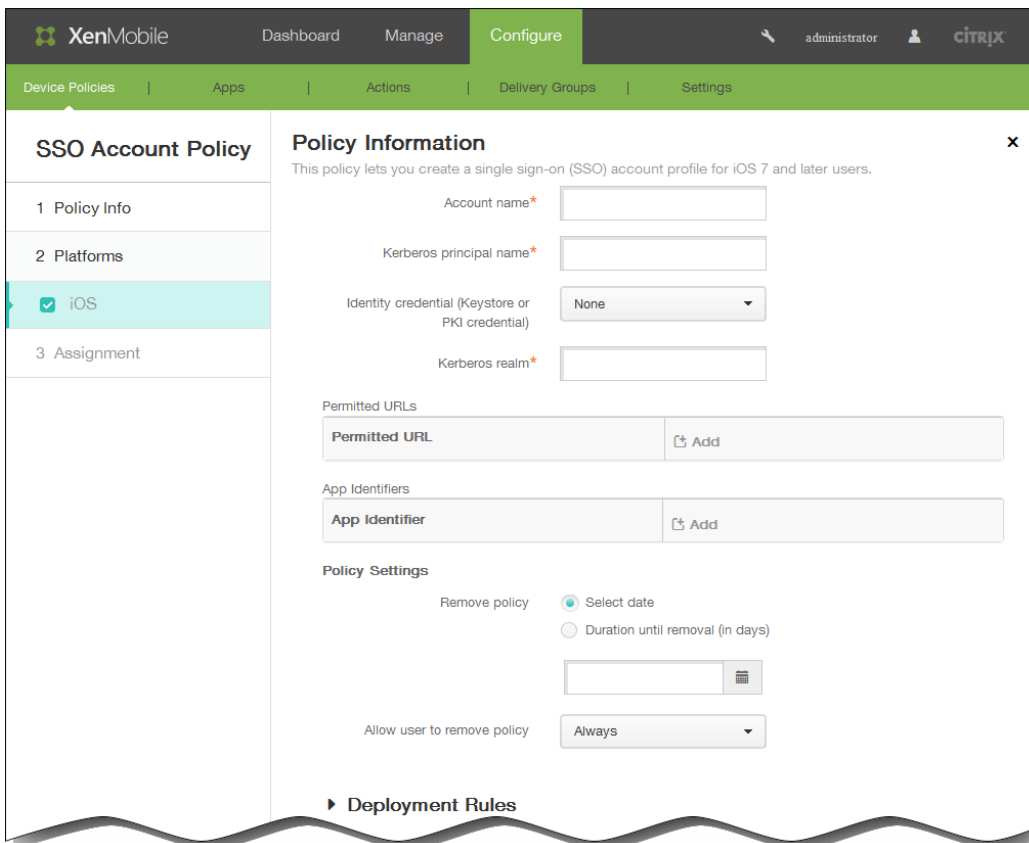
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



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:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform information page appears.

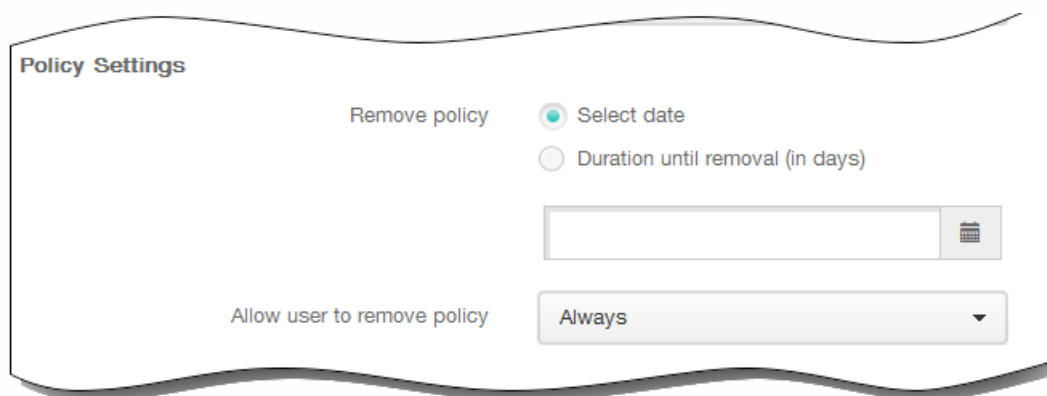


6. In the iOS Platform information page, enter the following information:
 1. Account name: Enter the Kerberos SSO account name that appears on users' devices. This field is required.
 2. Kerberos principal name: Enter the Kerberos principal name. This field is required.

3. 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.
4. 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.
5. Permitted URLs: Click Add and then do the following:
 1. Permitted URL: Enter a URL that you want to require SSO when a user visits the URL from the iOS device.
For example, when a user tries to browse to a site and the website 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.
 2. Click Add to add the URL or click Cancel to cancel adding the URL.
 3. Repeat step i. and ii. for each URL you want to add.
6. App Identifiers: Click Add and then do the following:
 1. App Identifier: Enter an app identifier for an app that is allowed to use this login.
Note: If you do not add any app identifiers, this login matches **all** app identifiers.
 2. Click Add to add the app identifier or click Cancel to cancel adding the app identifier.
 3. Repeat step i. and ii. for each app identifier you want to add.

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.

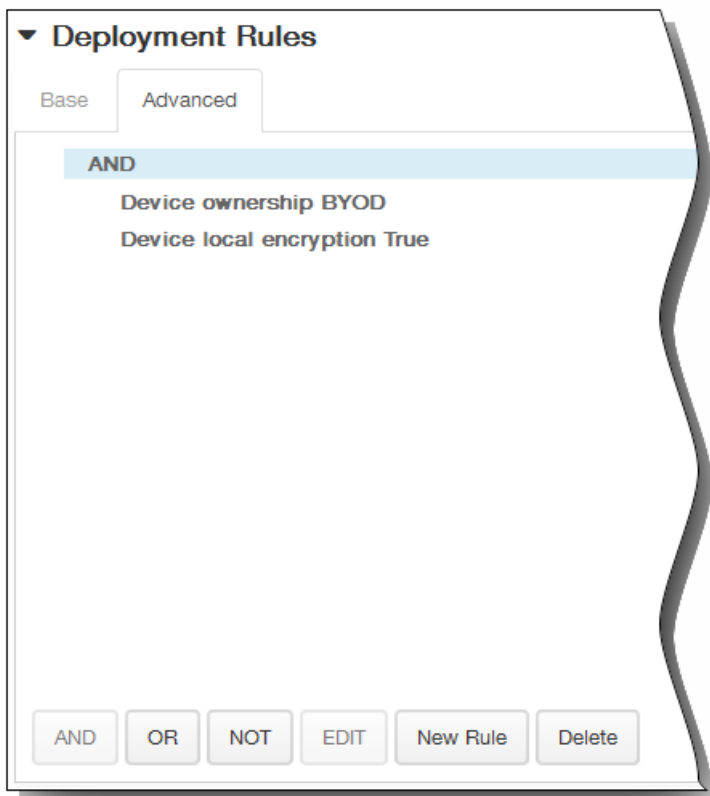
To edit an existing URL or app identifier, hover over the line containing the listing and click the pen icon on the right-hand side. Make any changes to the listing and then click Save to save the changed listing or Cancel to leave the listing unchanged.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



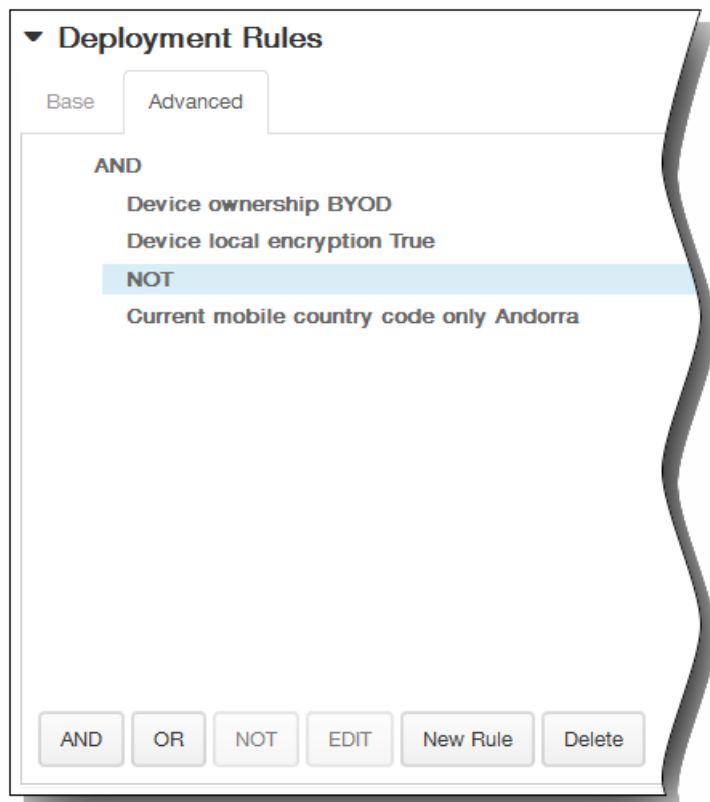
The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

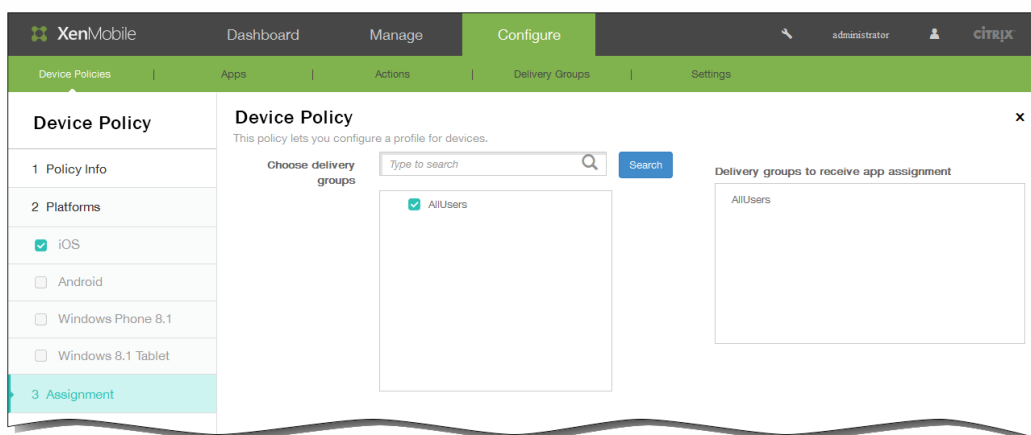
3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The SSO Account Policy assignment page appears.

13. 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.

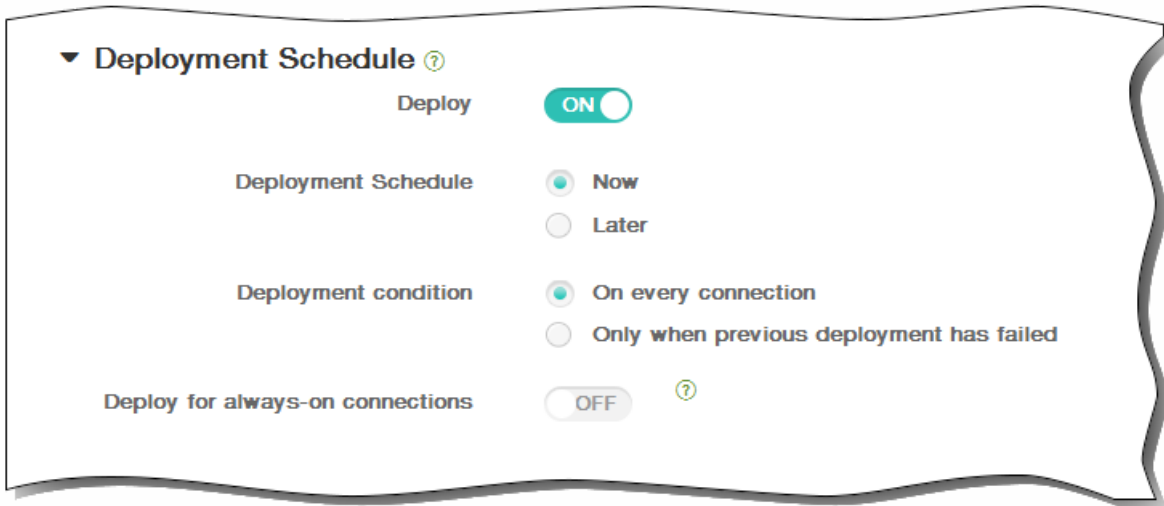


14. Expand Deployment Schedule and then configure the following settings:

1. 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.
2. Next to Deployment schedule, click Now or Later. The default option is Now.

3. If you click Later, click the calendar icon and then select the date and time for deployment.
4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



15. Click Save to save the policy.

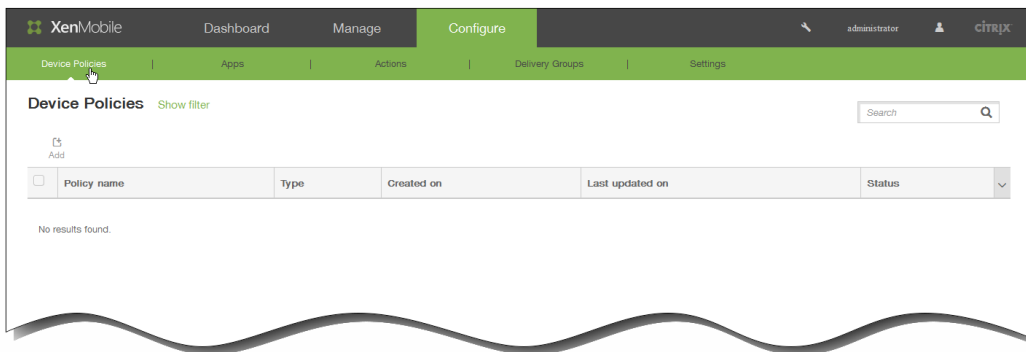
To add a subscribed calendars device policy for iOS

Feb 13, 2015

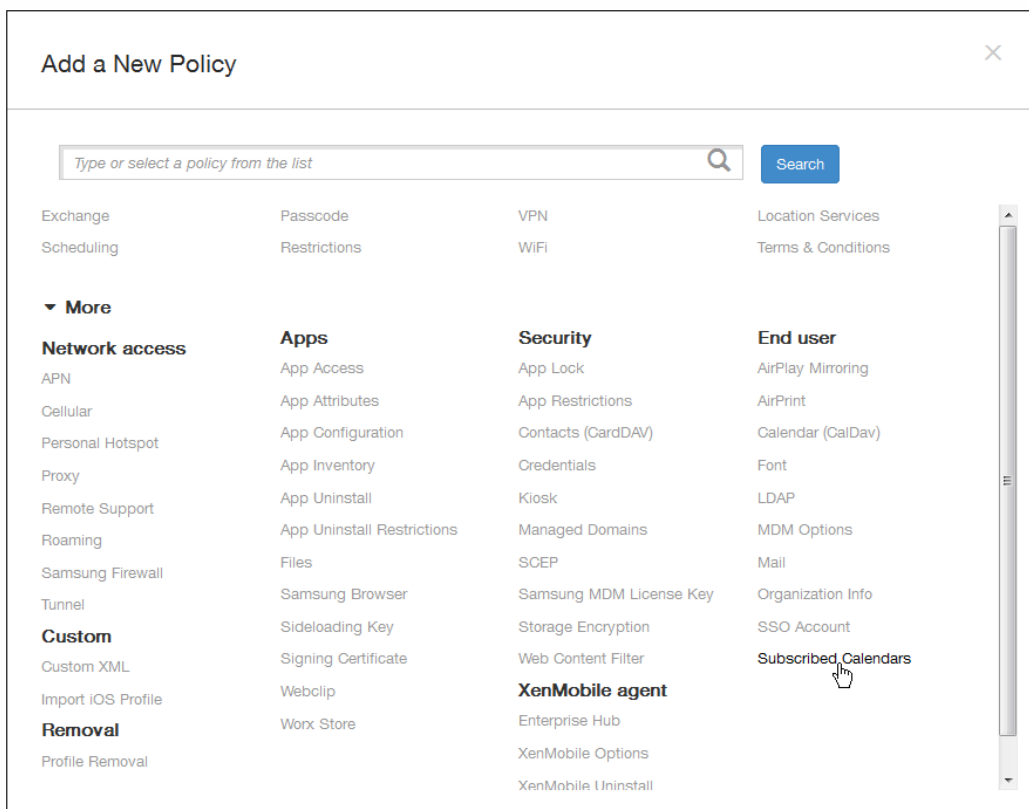
You can add a device policy in XenMobile to add a subscribed calendar to the calendars list on users' iOS devices. The list of public calendars to which you can subscribe is available at www.apple.com/downloads/macosx/calendars.

Note: You must have subscribed to a calendar before you can add it to the subscribed calendars list on users' devices.

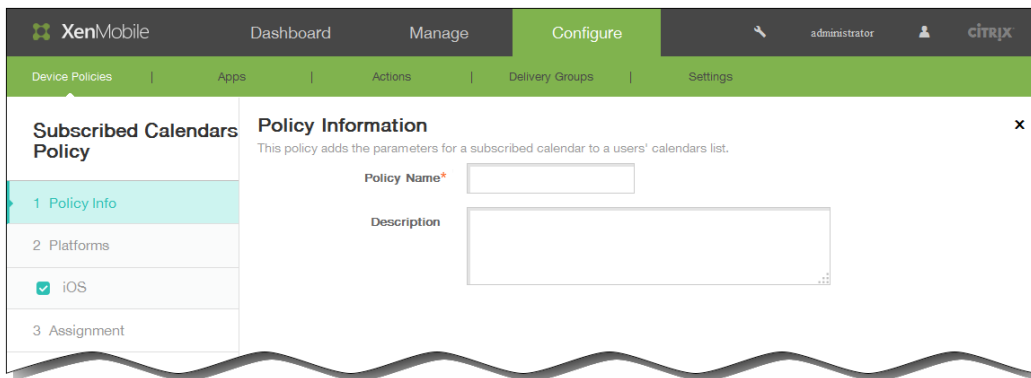
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



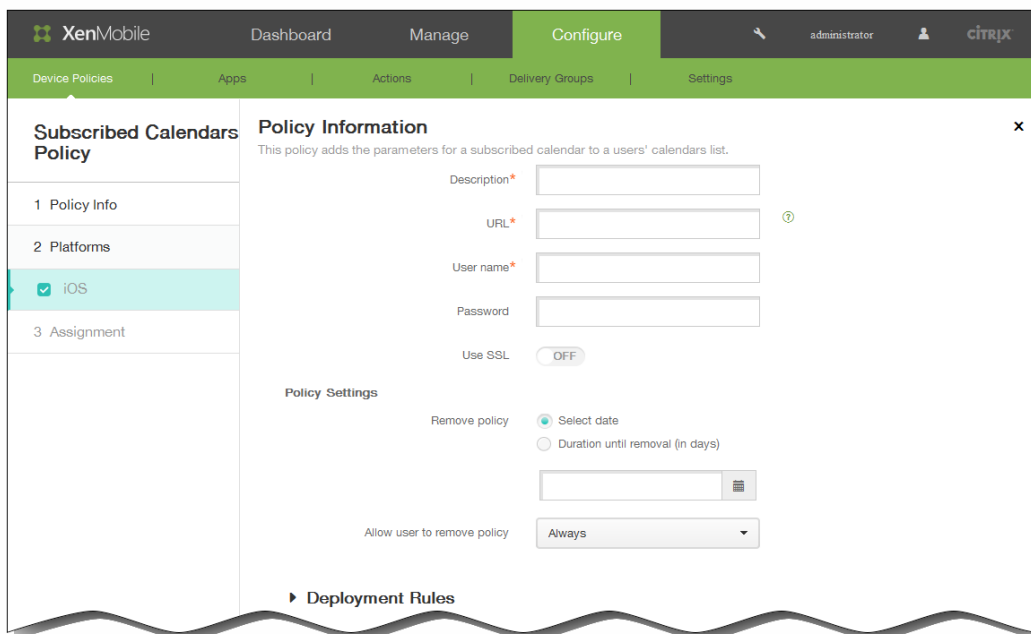
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



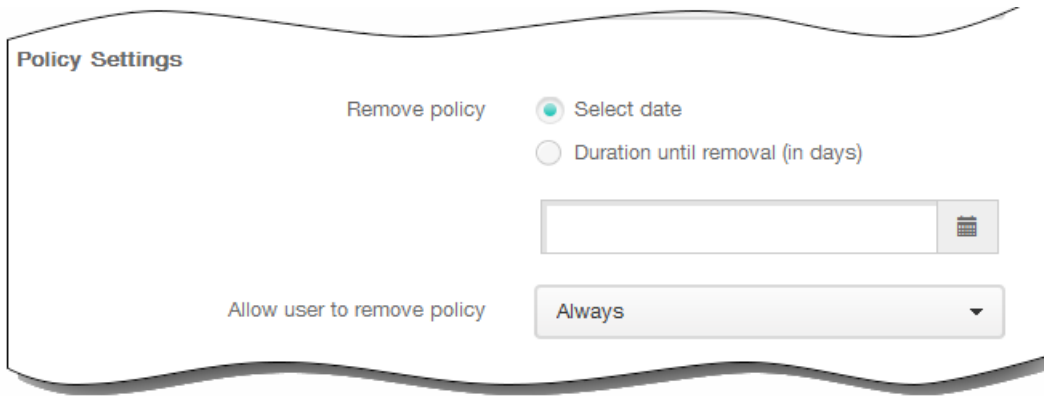
3. Click More and then, under End user, click Subscribed Calendars. The Subscribed Calendars Policy page appears.



4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform Information page appears.



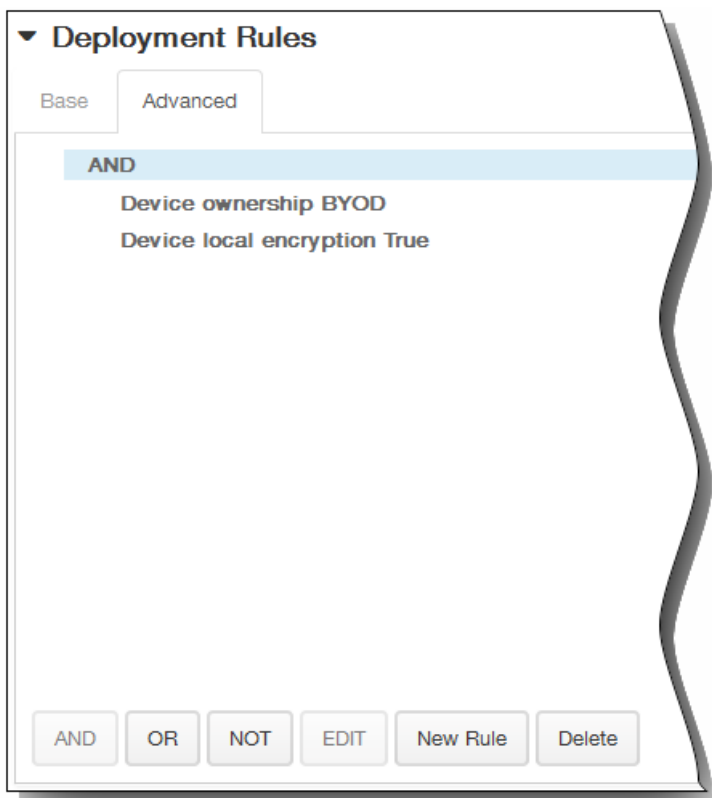
6. In the iOS Platform Information page, enter the following information:
 1. Description: Enter a description of the calendar. This field is required.
 2. URL: Enter the calendar URL. You can enter a webcal:// URL or an http:// link to an iCalendar file (.ics). This field is required.
 3. User name: Enter the user's logon name. This field is required.
 4. Password: Enter an optional user password.
 5. Use SSL: Select whether to use a Secure Socket Layer connection to the calendar. The default is Off.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

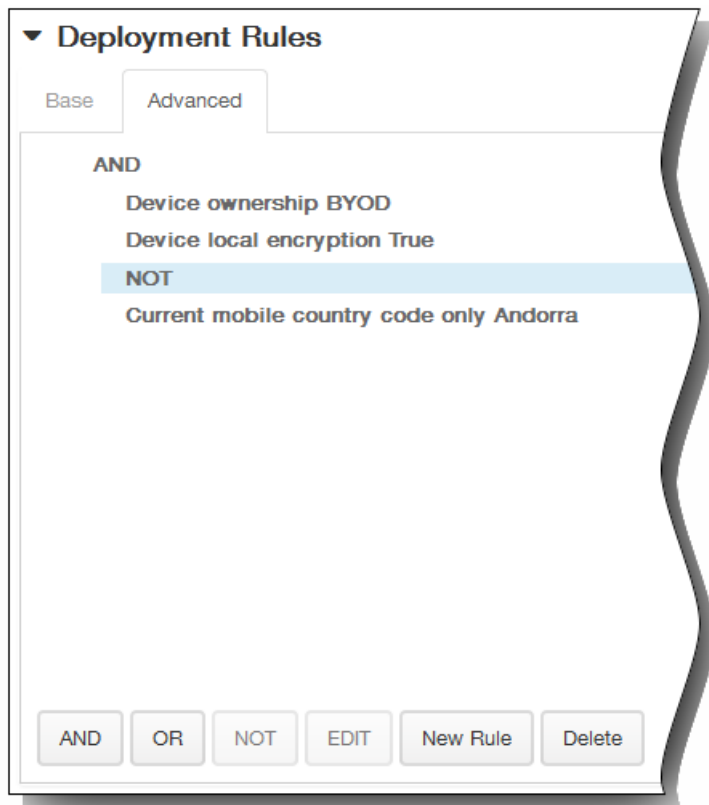


The conditions you chose on the Base tab appear.

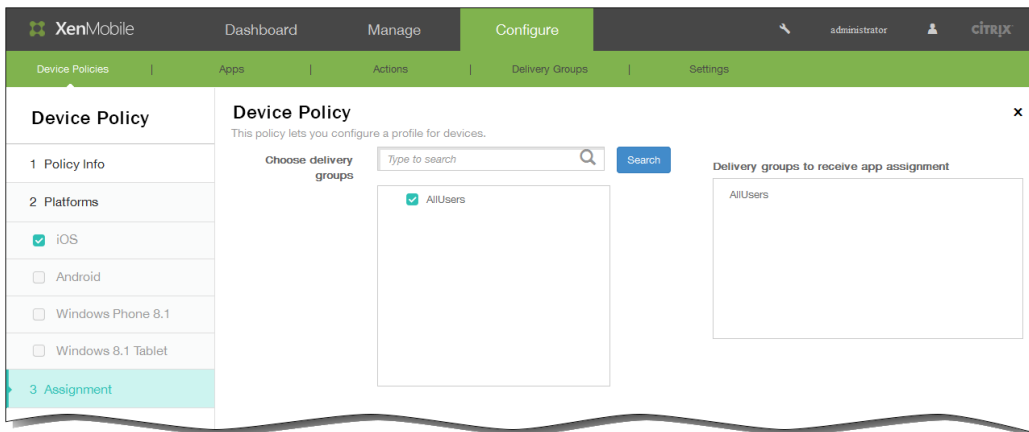
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The Subscribed Calendars Policy assignment page appears.
13. 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.

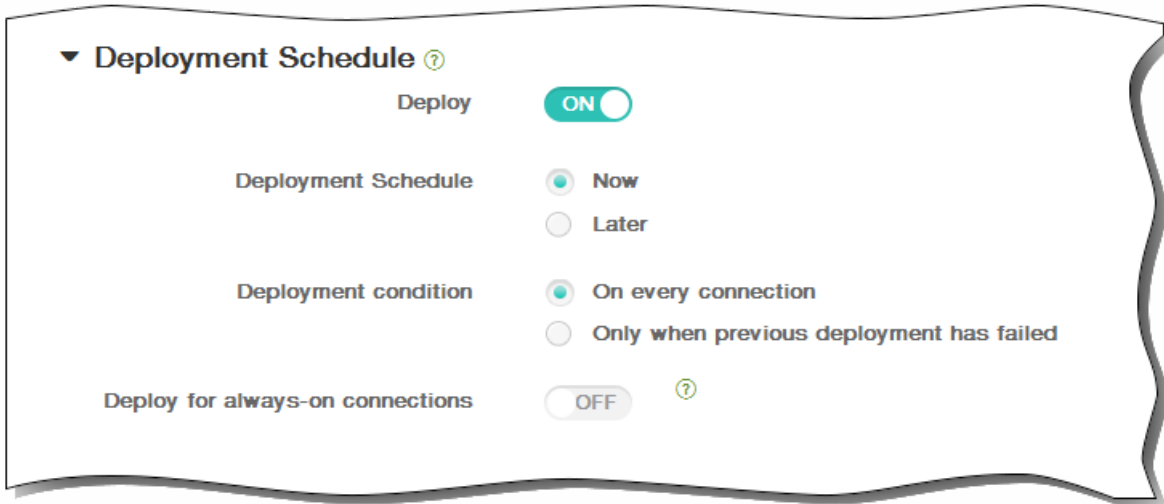


14. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



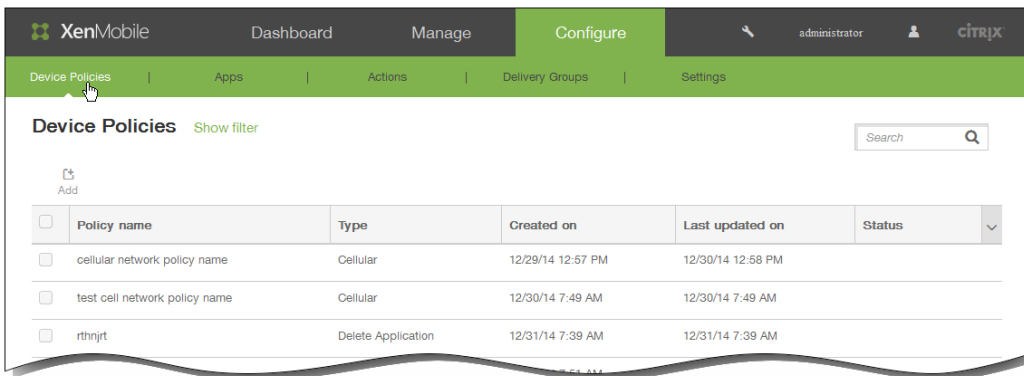
15. Click Save to save the policy.

Passcode device policies

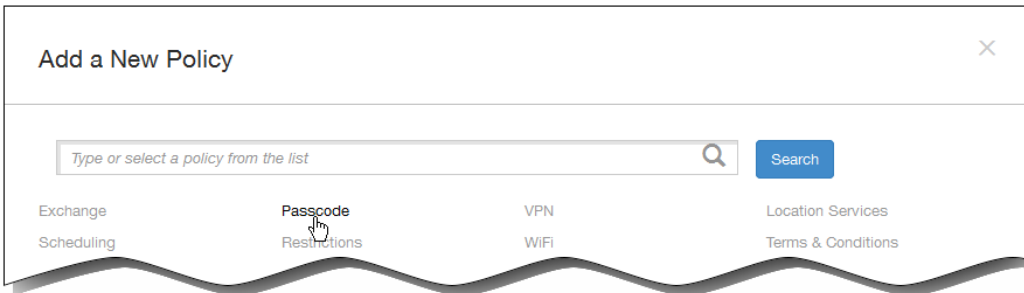
Mar 31, 2016

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, Android, Samsung KNOX, Windows Phone 8.1, and Windows 8.1 tablet. Each platform requires a different set of values, which are described in this article.

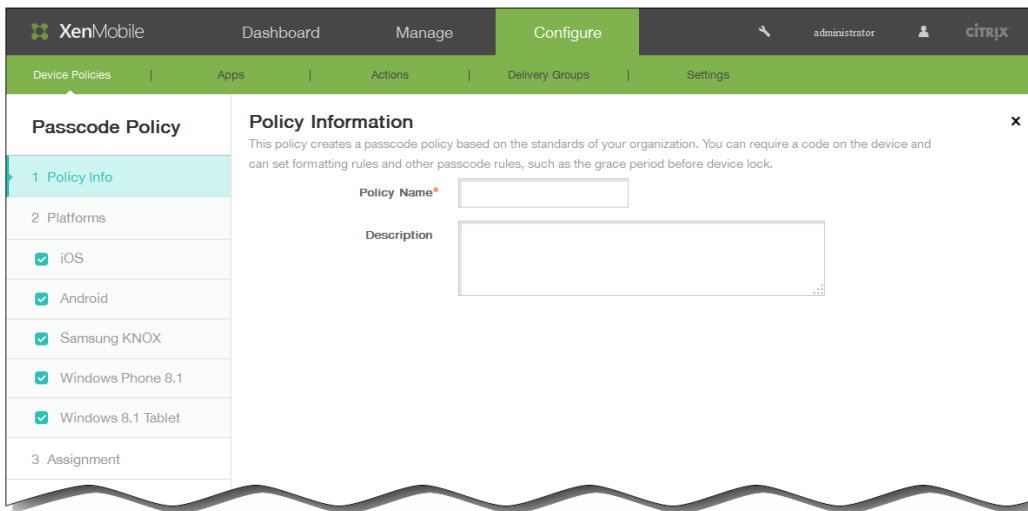
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears. Click Add to add a new policy.



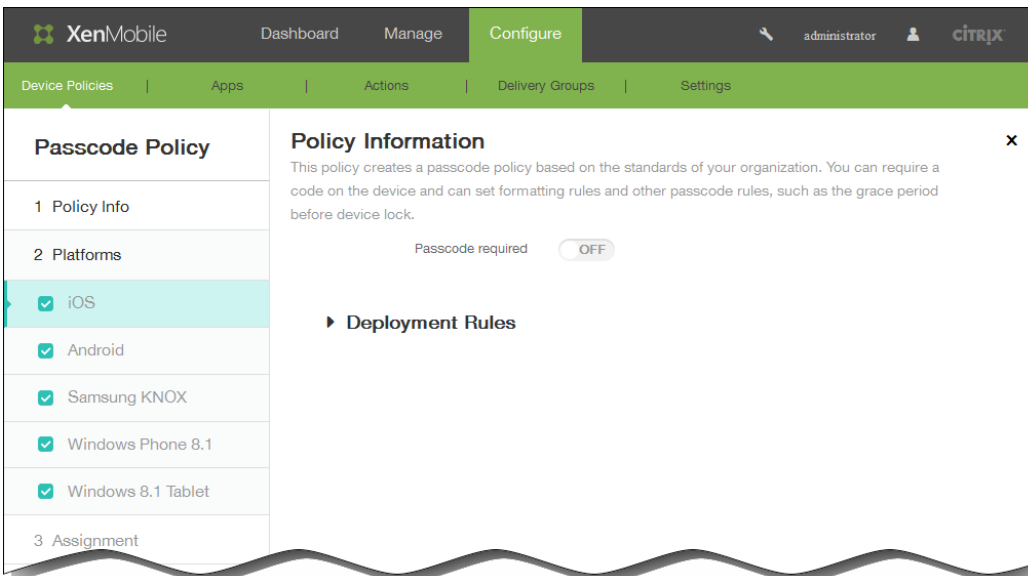
2. On the Add New Policy page, click Passcode.



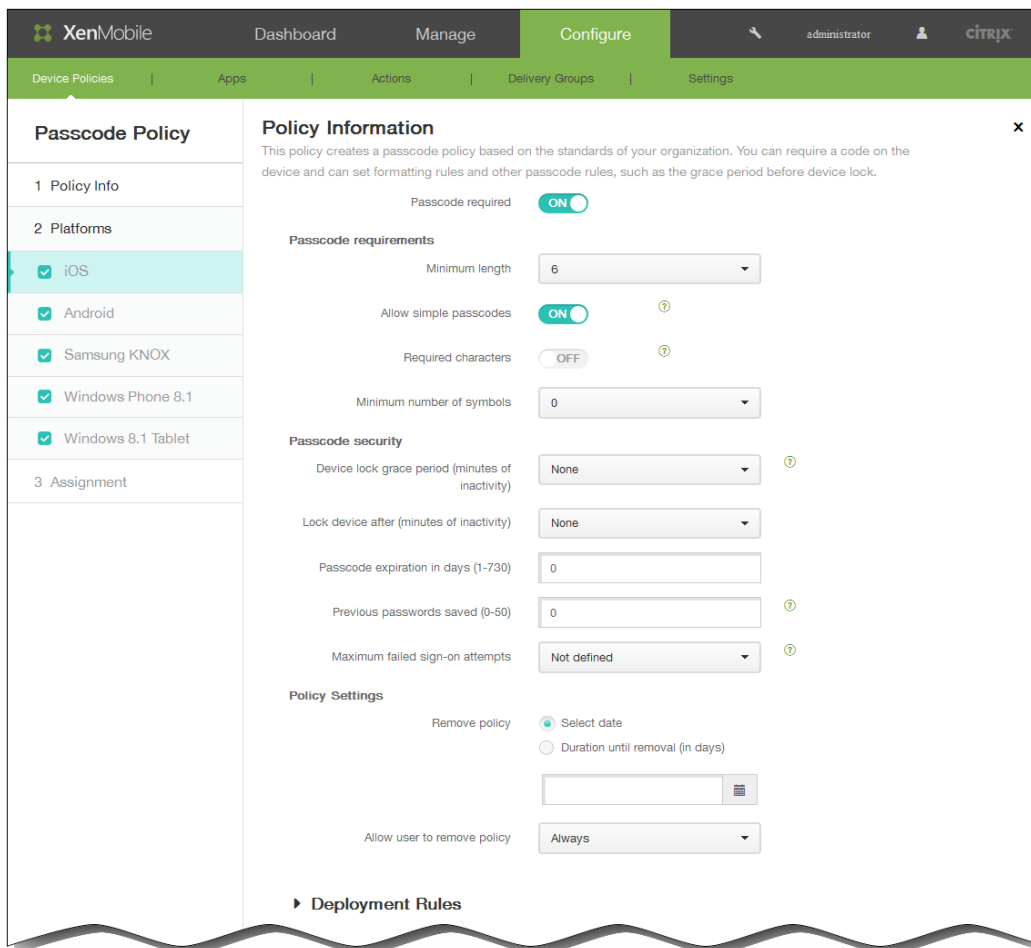
3. In the Policy Information pane, enter the following information:



1. Policy Name: Type a descriptive name for the policy.
2. Description: Type an optional description of the policy.
3. Click Next.
4. Under Platforms, select the platforms for which you want to configure this policy.
Note: When the Policy Platforms page appears, all platforms are selected and you see the iOS platform configuration panel first.



- If you selected iOS, 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.

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.

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.

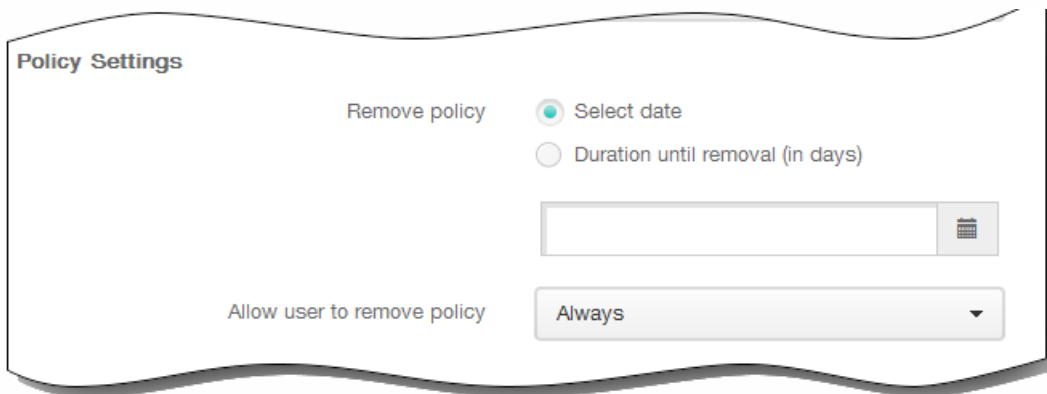
Lock device after (minutes of inactivity): In the list, click the length of time a device can be inactive before it is locked. The default is None.

Passcode expiration in days (1-730): Enter 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): Enter 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



Policy Settings

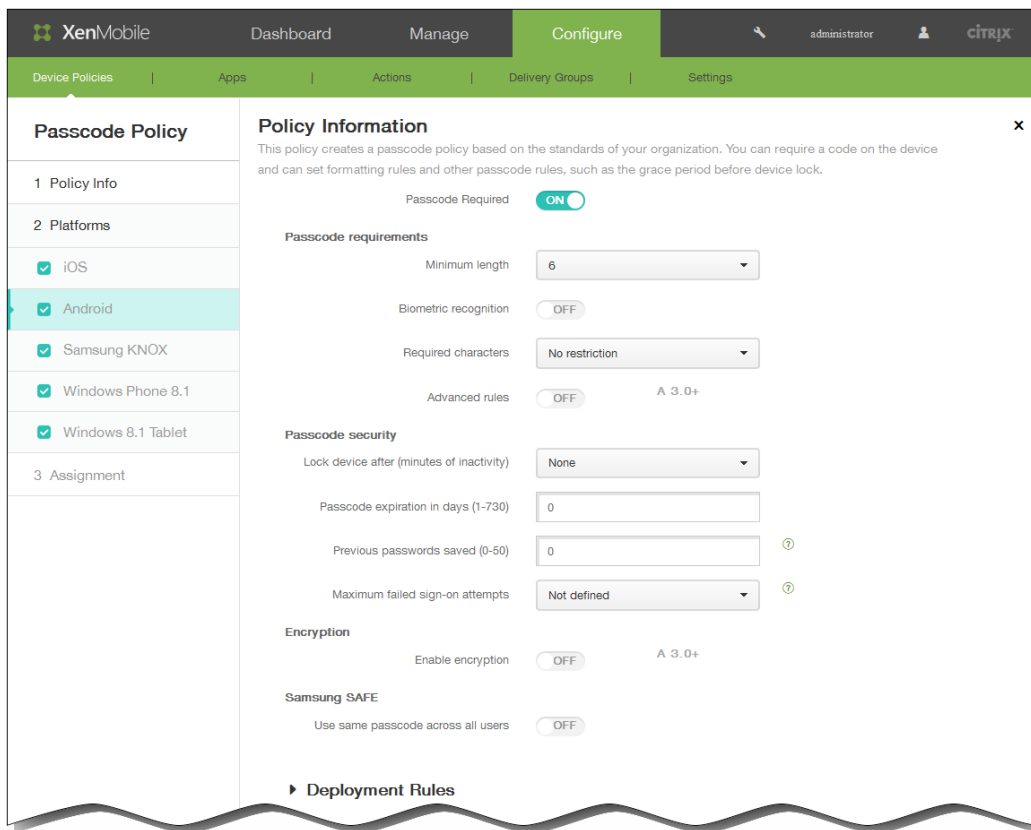
Remove policy Select date
 Duration until removal (in days)



Allow user to remove policy Always ▾

1. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
 2. If you click Select date, click the calendar to select the specific date for removal.
 3. In the Allow user to remove policy list, click Always, Password required, or Never.
 4. If you click Password required, next to Removal password, type the necessary password.
- If you selected Android, configure these settings:

Note: The default setting for Android is OFF. 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 Advanced rules is set to ON, 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): Enter 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): Enter 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.

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.

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

Enter the required passcode in the field that appears when you enable this option.

- If you selected Samsung KNOX, configure these settings:

The screenshot shows the XenMobile administration interface. The top navigation bar includes 'Dashboard', 'Manage', and 'Configure'. The 'Configure' section is active, showing a sidebar with 'Passcode Policy' selected. The main content area is titled 'Policy Information' and contains the following settings:

- Passcode requirements:**
 - Minimum length: 6
 - Allow users to make password visible: OFF
- Forbidden Strings:** A section with a table for 'Forbidden strings' and an 'Add' button.
- Minimum number of:**
 - Changed characters*: 0
 - Symbols*: 0
- Maximum number of:**
 - Number of times a character can occur*: 0
 - Alphabetic sequence length*: 0
 - Numeric sequence length*: 0
- Passcode security:**
 - Lock device after (minutes of inactivity): None
 - Passcode expiration in days (1-730): 0
 - Previous passwords saved (0-50): 0
 - Maximum failed sign-on attempts: Not defined

At the bottom, there is a section for 'Deployment Rules'.

Passcode requirements

Minimum length: In the list, click the minimum passcode length.

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. Do the one of the following:
 - **To add a forbidden string**
 1. Click Add.
 2. Type the forbidden string.
 3. Click Save to save the string or Cancel to cancel adding the string.
 4. Repeat steps i. through iii. for each forbidden string you want to add.
 - **To edit a forbidden string**
 1. Previous passwords saved (0-50): Enter 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 user can reuse passwords.
 1. Hover over the string you want to edit.
 2. Click the pen icon to the right of the listing.
 3. Make changes to the string.
 4. Click Save to save the string or Cancel to cancel changing the string.

Minimum number of

Changed characters: Enter the number of characters users must change from their previous passcode. The default is 0.

Symbols: Enter the minimum number of required symbols in a passcode. The default is 0.

Maximum number of

Number of times a character can occur: Enter the maximum number of times a character can occur in a passcode. The default is 0.

Alphabetic sequence length: Enter the maximum length of an alphabetic sequence in a passcode. The default is 0.

Numeric sequence length: Enter 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 length of time a device can be inactive before it is locked. The default is None.

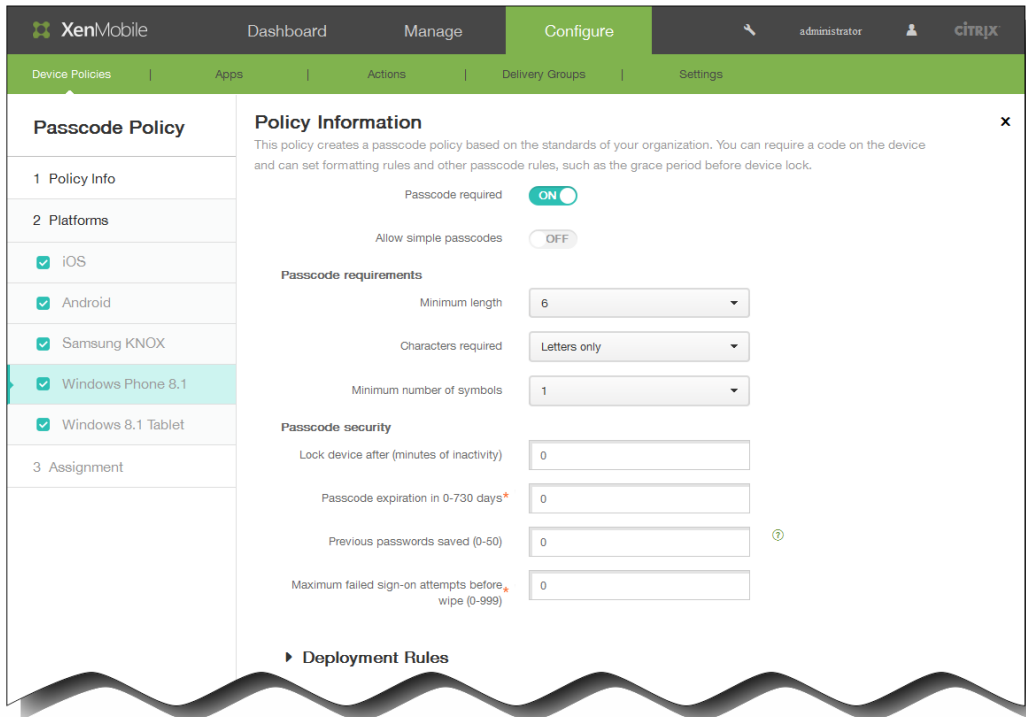
Note: Even though this field's label says "minutes of inactivity" XenMobile actually enforces the lock after the specified number of *seconds*.

Passcode expiration in days (1-730): Enter 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): Enter 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 user 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.

- If you selected Windows Phone 8.1, configure these settings:



Passcode required: Select this option to not require a passcode for Windows Phone 8.1 devices. The default setting is ON, which requires a passcode. The page collapses and the following options disappear. If you do not turn off the passcode requirement, continue configuring the following settings.

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): In the list, click the length of time a device can be inactive before it is locked. The default is 0.

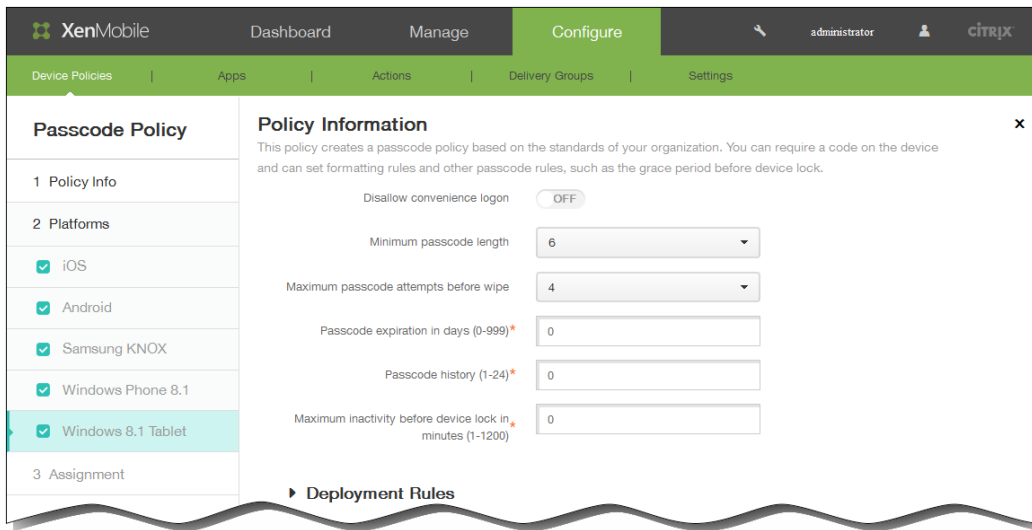
Passcode expiration in 0-730 days: Enter the number of days after which the passcode expires. Valid values are 1–730. The default is 0, which means the passcode never expires.

Previous passwords saved (0-50): Enter 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): 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 0.

- If you selected Windows 8.1 Tablet, 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 the device is wiped. The default is 4.

Passcode expiration in days (0-999): Enter the number of days after which the passcode expires. Valid values are 1–999. The default is 0, which means the passcode never expires.

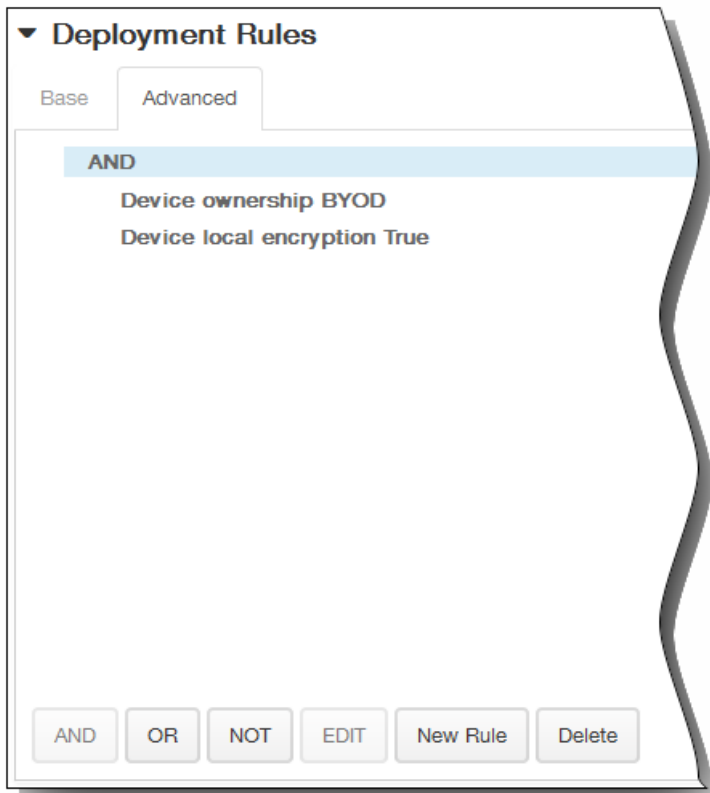
Passcode history: (1-24): Enter the number of used passcodes to save. Users are unable to use any passcode found in this list. Valid values are 1–24. You must enter a number between 1 and 24 in this field.

Maximum inactivity before device lock in minutes (1-1200): Enter the length of time in minutes that a device can be inactive before it is locked. Valid values are 1–1200. You must enter a number between 1 and 1200 in this field.

5. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.

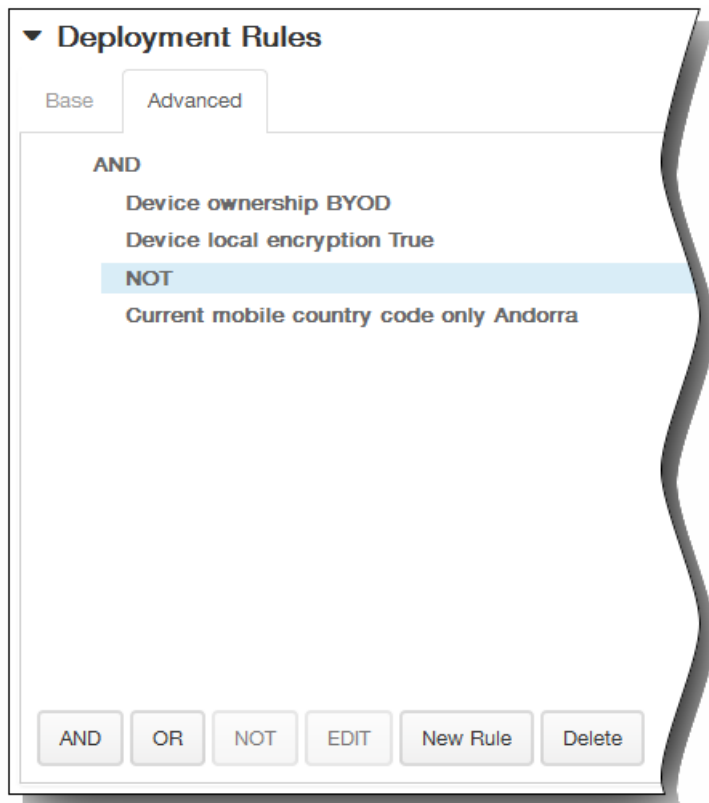


1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

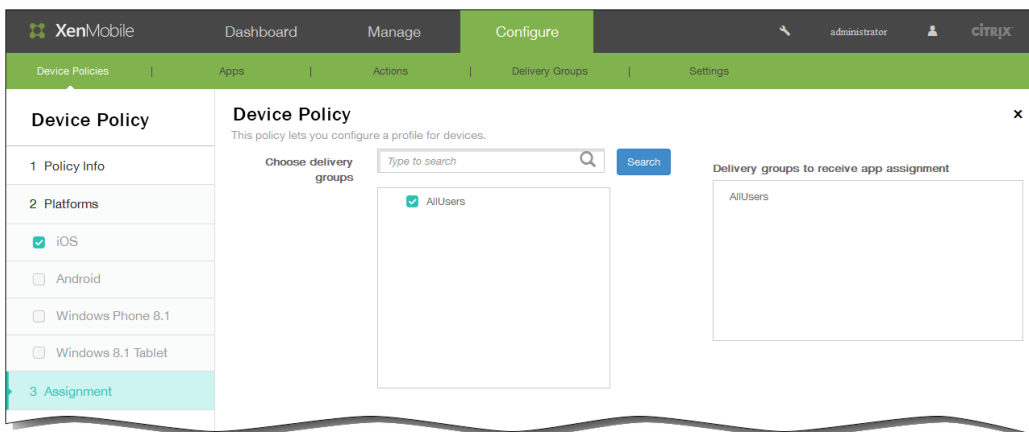


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.
In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.

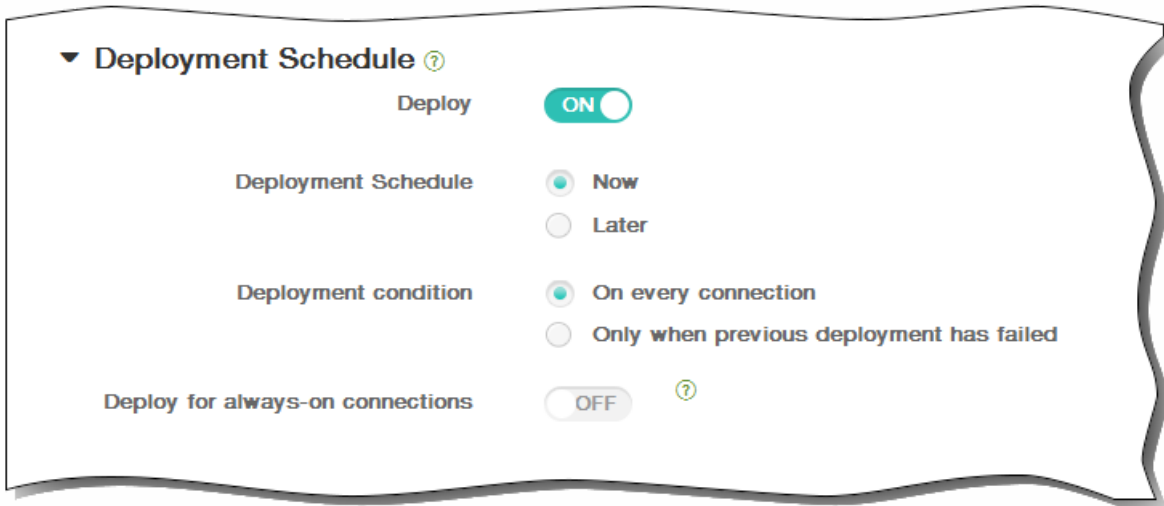


6. Click Next. The Passcode Policy assignment page appears.
7. Next to Choose delivery groups, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand Delivery groups to receive app assignment list.



8. Expand Deployment Schedule and then configure the following settings:
 1. 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.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.

- Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 - Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.
- Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



- Click Save.

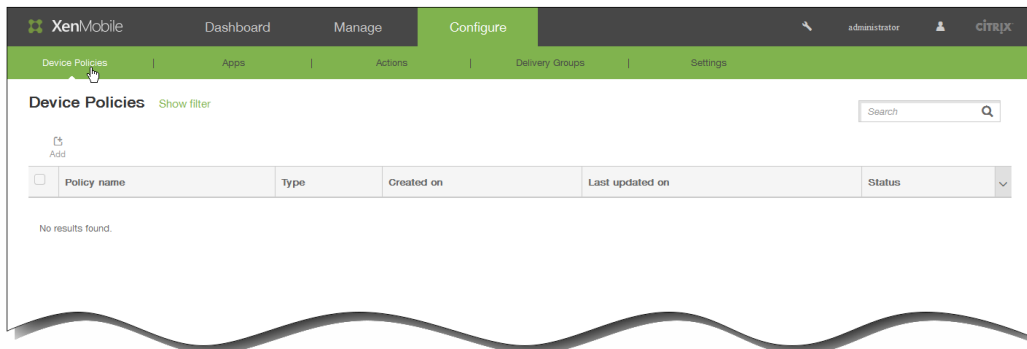
To add a proxy device policy for iOS

Mar 03, 2015

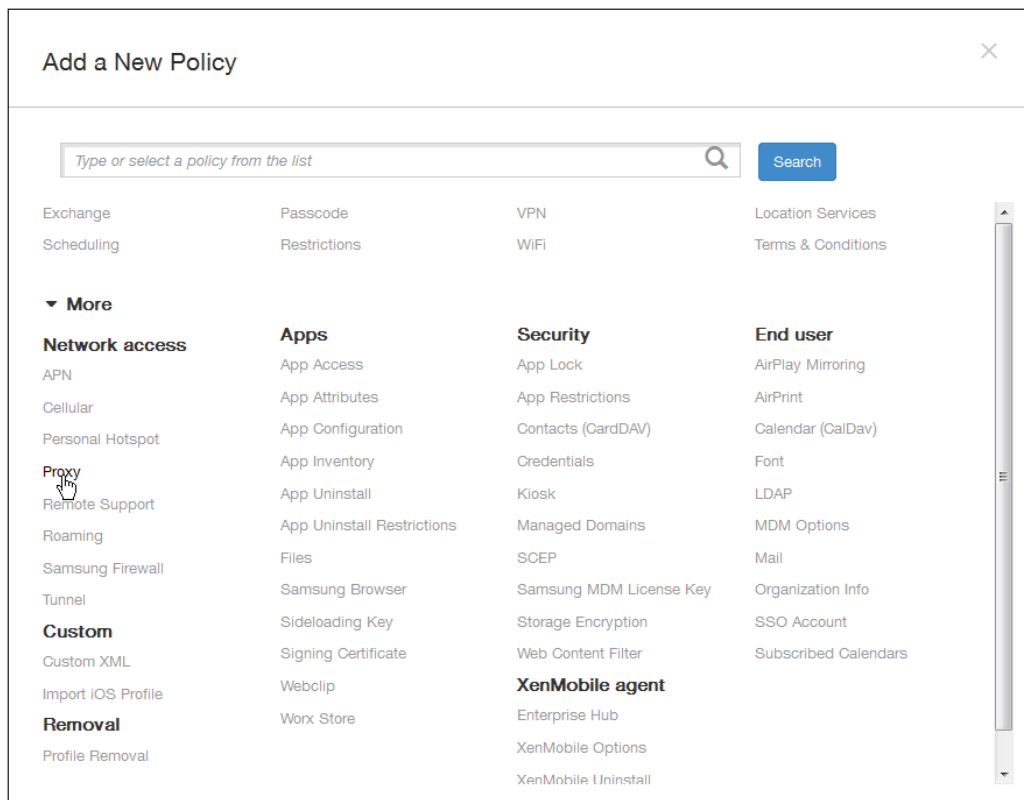
You can add a device policy in XenMobile to specify global HTTP proxy settings for devices running iOS 6.0 or later. You can deploy only one global HTTP proxy policy per device.

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](#).

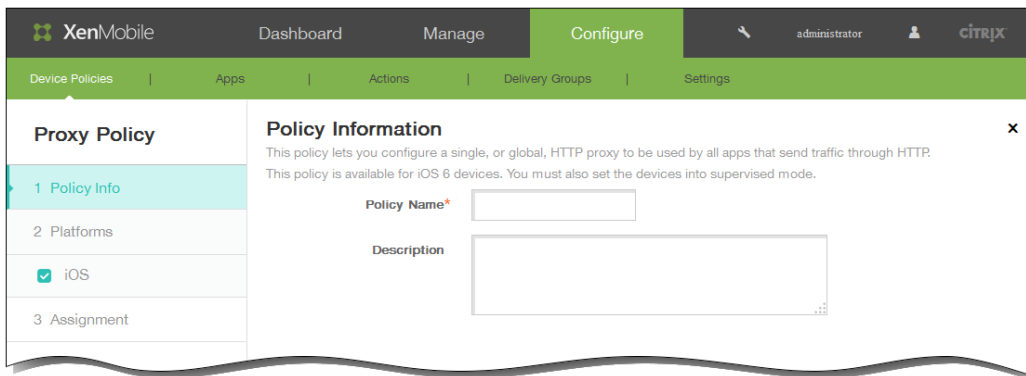
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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



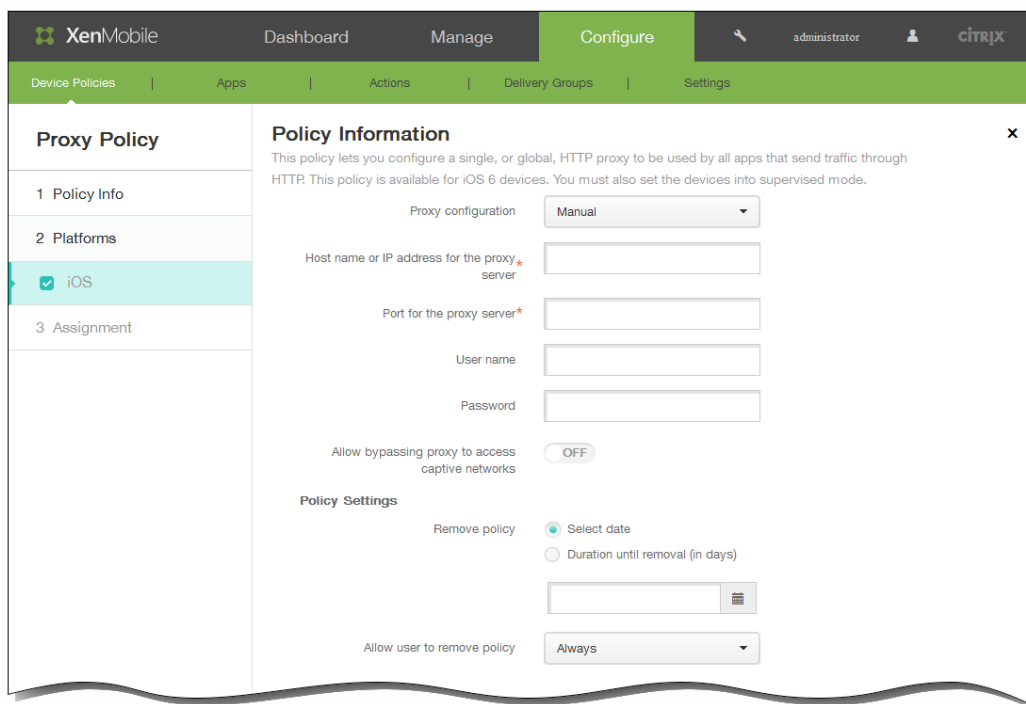
3. Click More and then, under Network access, click Proxy. The Proxy Policy page appears.



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

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

5. Click Next. The iOS Platform Information page appears.



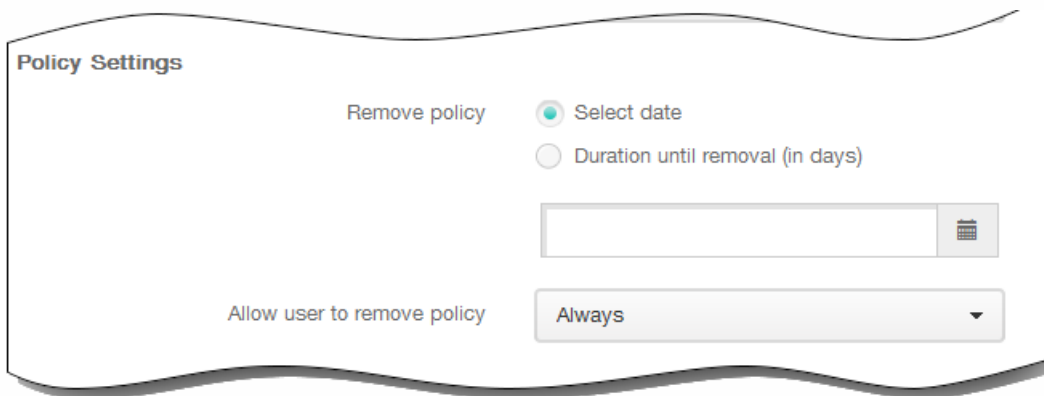
6. On the iOS Platform Information page, enter the following information:

1. Proxy configuration: Click Manual or Automatic for how the proxy will be configured on users' devices. The following table lists the options available for each proxy configuration. Each cell indicates whether the option is not applicable (-), required, or optional.

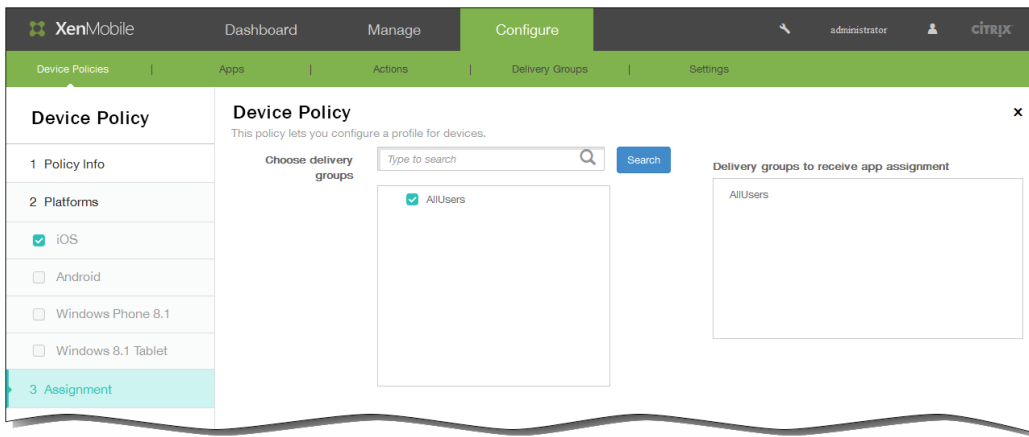
	Manual	Automatic
Host name or IP address for the proxy server	Required	-

Port for the proxy server	Manual Required	Automatic
User name	Optional	–
Password	Optional	–
Proxy PAC URL	–	Optional
Allow direct connection if PAC is unreachable	–	OFF

2. Allow bypassing proxy to access captive networks: Select whether to allow bypassing the proxy to access captive networks.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



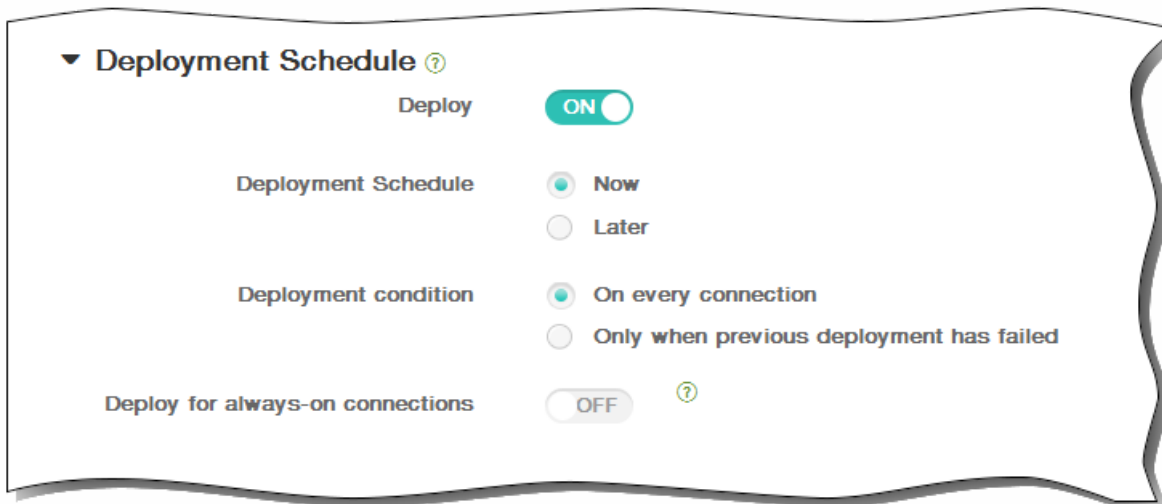
11. Click Next. The Proxy Policy assignment page appears.
12. Next to Choose delivery groups, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand Delivery groups to receive app assignment list.



13. Expand Deployment Schedule and then configure the following settings:
 1. 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.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



14. Click Save to save the policy.

To add a remote support device policy for Samsung KNOX

Feb 13, 2015

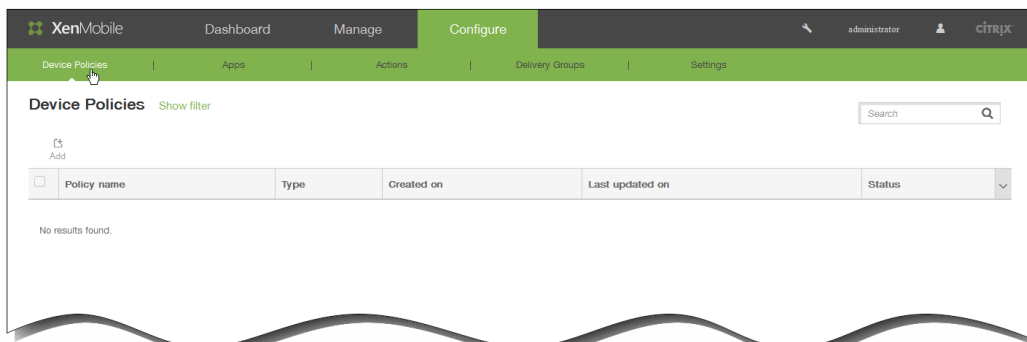
You create a remote support policy in XenMobile to give you remote access to users' Samsung KNOX devices. You can configure two types of support:

- **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.

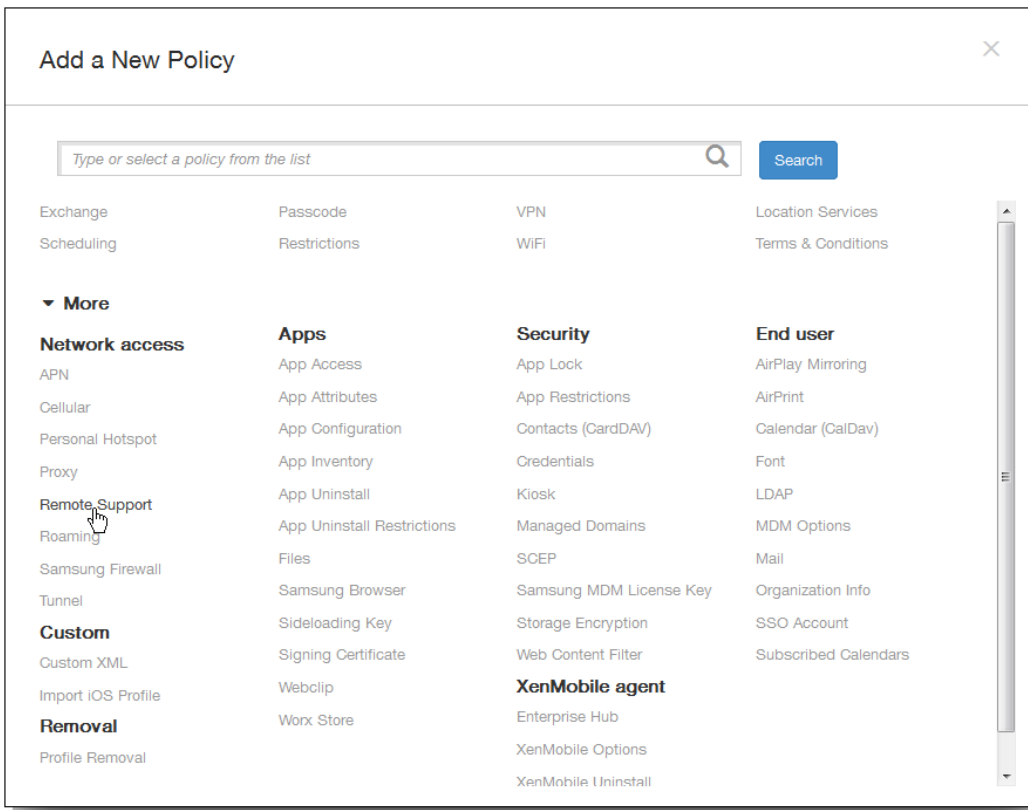
Note: To implement this policy, you must do the following:

- Install the XenMobile Remote Support app in your environment.
- Configure a remote support app tunnel. For details, see [To add an app tunneling device policy for Android](#).
- 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.

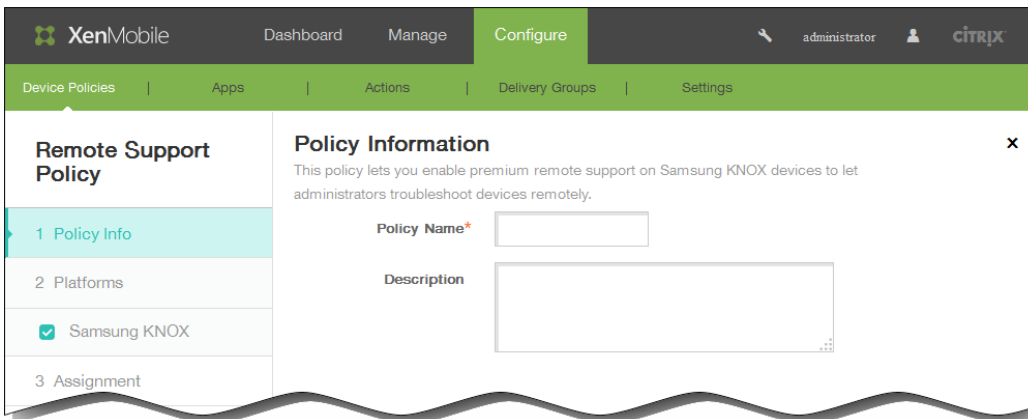
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



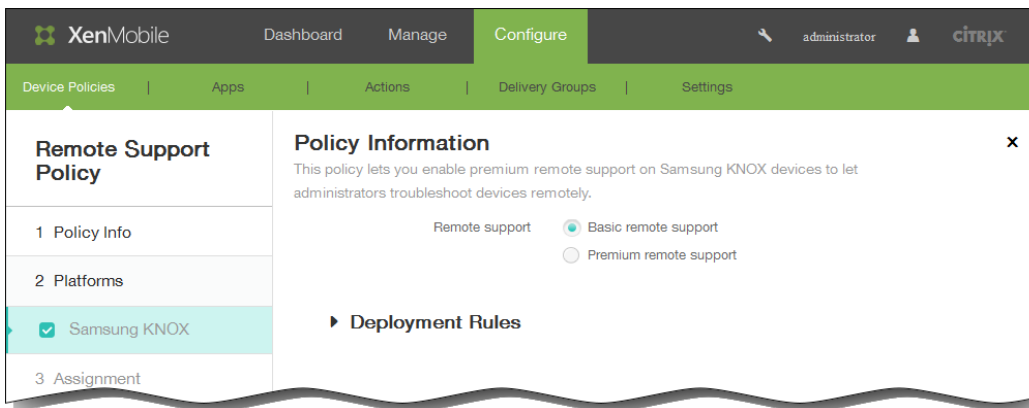
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



3. Click More and then, under Network access, click Remote Support. The Remote Support Policy page appears.



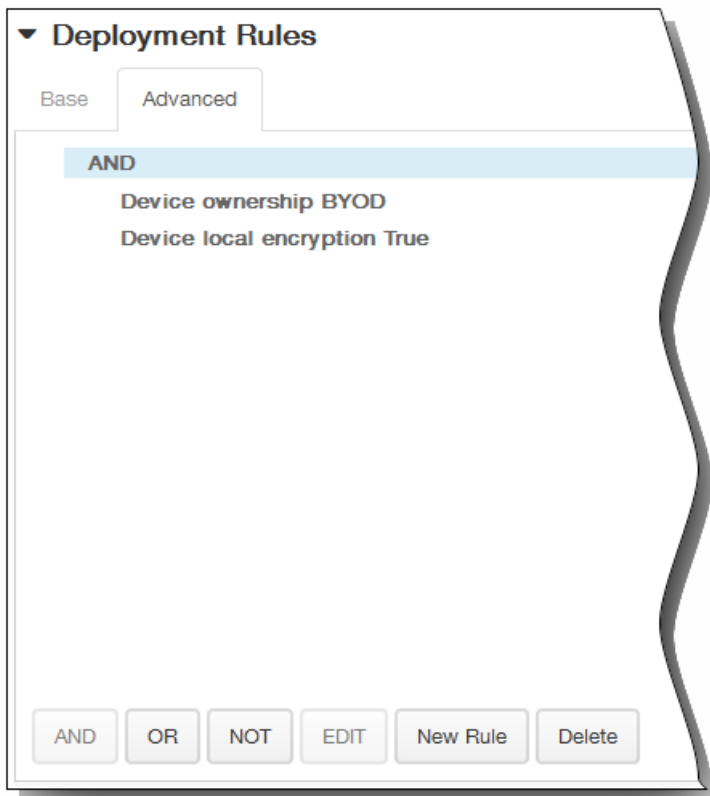
4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The Samsung KNOX platform information page appears.



6. In the Samsung KNOX platform information page, enter the following information:
 1. Remote support: Select Basic remote support or Premium remote support. The default is Basic remote support.
7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

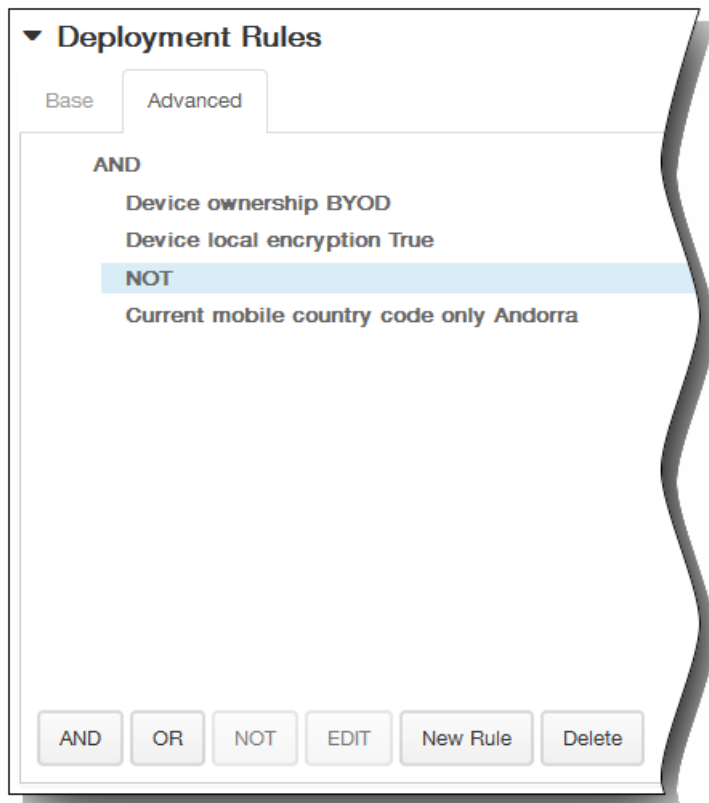


The conditions you chose on the Base tab appear.

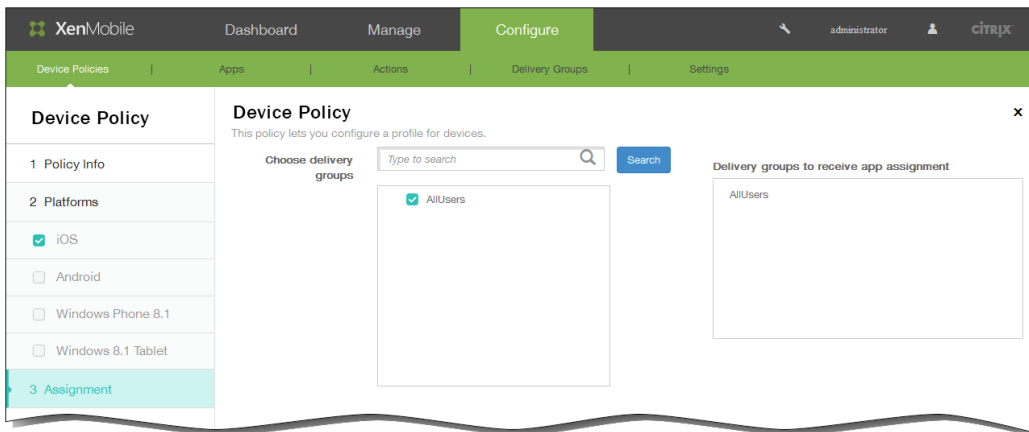
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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 right-hand Delivery groups to receive app assignment list.

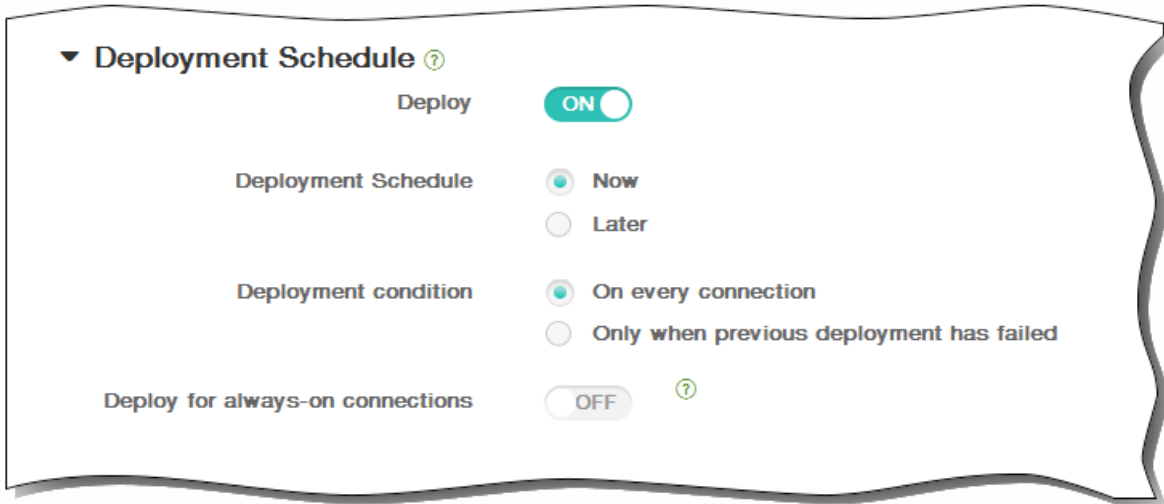


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

Restrictions device policies

Feb 27, 2015

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, Samsung SAFE, Windows 8.1 tablets, Windows Phone 8.1, and Amazon. 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 exception is the Security - Force feature, which defaults to OFF, or

— *restricts*

Tip: Any option for which you select ON means that the user

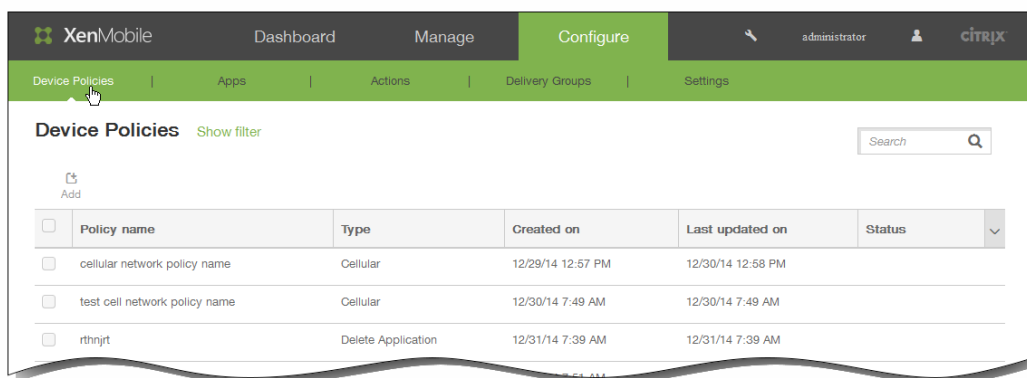
— *can*

perform the operation or use the feature. For example:

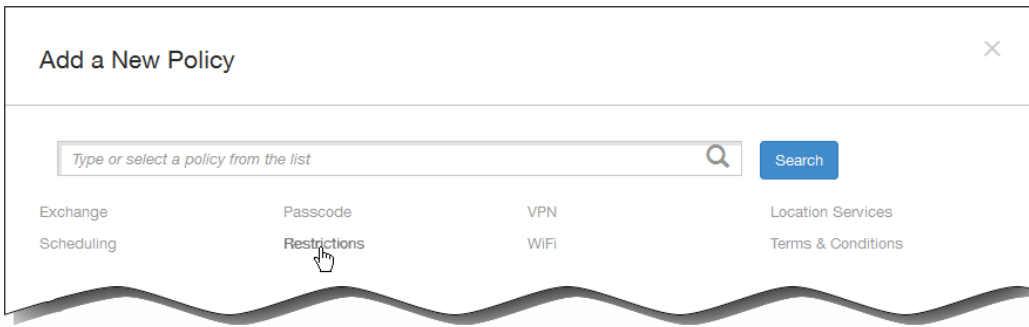
- Camera. If ON, the user can use the camera on their device. If OFF, the user cannot use the camera on their device.
- **Screen shots.** If ON, the user can take screen shots on their device. If OFF, the user cannot take screen shots on their device.

Note: Some of the iOS restrictions options apply only to specific versions of iOS (and, where applicable, these versions are noted on the XenMobile console page). Also, some options only apply if the device is placed in supervised mode. For example, the ability to allow or block AirDrop is only supported on devices running iOS 7 and later, whereas the ability to allow or block Photo streams is supported on devices running iOS 5 and later. 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](#).

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

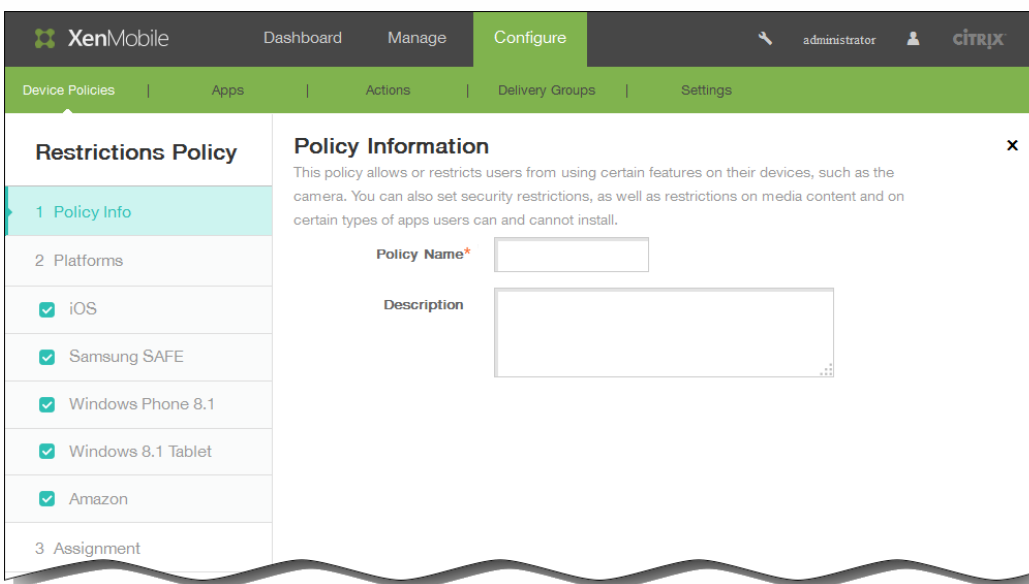


2. Click Add. The Add a New Policy page appears.



3. Click Restrictions.

The Restrictions Policy information page appears.

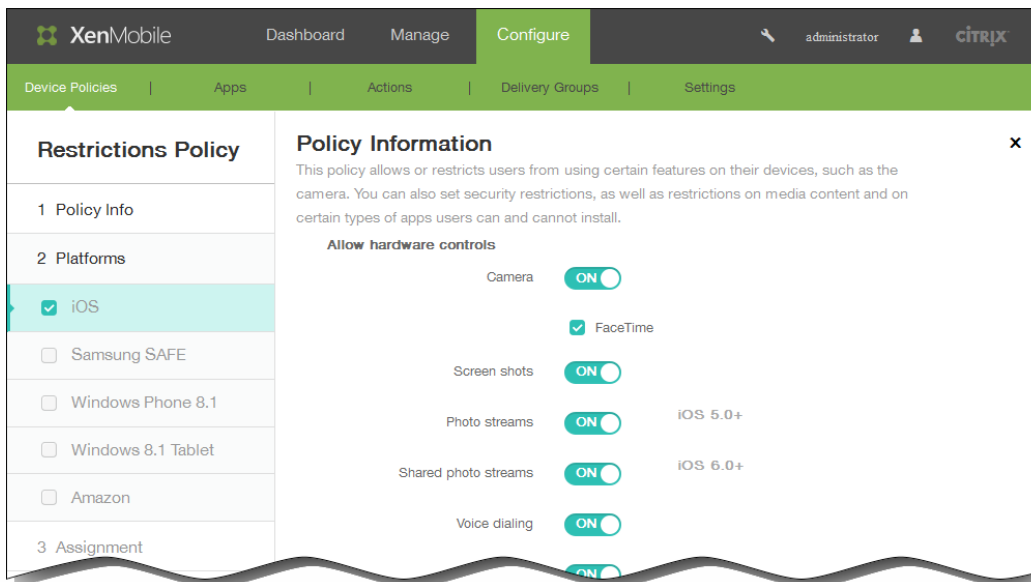


4. In the Policy Information pane, type the following information:

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

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:



- Allow hardware controls:

Camera; FaceTime

Screen shots

Photo streams (available in iOS 5.0 and later)

Shared photo streams (available in iOS 6.0 and later)

Voice dialing

Siri:

- Allow while device is locked: Leave the option selected by default or clear the check box.
- Siri profanity filter: Leave the option cleared by default or select the check box. The default is to restrict this feature.

Installing apps

- Allow apps:

YouTube

iTunes Store

In-app purchases: Require iTunes password for purchases: Leave the option cleared by default or select the check box (available in iOS 5.0 and later). The default is to restrict this feature.

Safari:

- Autofill: Leave the option selected by default or clear the check box.
- Force fraud warning: Leave the option cleared by default or select the check box. The default is to restrict this feature.
- Enable JavaScript: Leave the option selected by default or clear the check box.
- Block pop-ups: Leave the option cleared by default or select the check box. The default is to restrict this feature.

In Accept cookies, click one of the following:

- Always
- Never
- From visited sites only

The default option is Always.

- Network - Allow iCloud actions:

Documents and data sync (available in iOS 5.0 and later)

Device backup (available in iOS 5.0 and later)

Automatic sync while roaming

iCloud keychain (available in iOS 7.0 and later)

- Security - Force:

Encrypted backups The default is OFF.

Limited ad tracking (available in iOS 7.0 and later) The default is OFF.

Passcode on first Airplay pairing(available in iOS 7.0 and later) The default is OFF.

- Security - Allow:

Accepting untrusted SSL certificates (available in iOS 5.0 and later)

Automatic update to certificate trust settings (available in iOS 7.0 and later)

Documents from managed apps in unmanaged apps

Documents from unmanaged apps in managed apps

Diagnostic submission to Apple

Touch ID to unlock device (available in iOS 7.0 and later)

Passbook notifications when locked (available in iOS 6.0 and later)

Handoff (available in iOS 8.0 and later)

iCloud sync for managed apps (available in iOS 8.0 and later)

Backup for enterprise books (available in iOS 8.0 and later)

Notes and highlights sync for enterprise books (available in iOS 8.0 and later)

- Supervised only settings - Allow:

Internet results in Spotlight (available in iOS 8.0 and later)

Erase all content and settings (available in iOS 8.0 and later)

Configuring restriction (available in iOS 8.0 and later)

Installing configuration profiles (available in iOS 6.0 and later)

AirDrop (available in iOS 7.0 and later)

iMessage (available in iOS 6.0 and later)

Siri user-generated content (available in iOS 7.0 and later)

iBooks (available in iOS 6.0 and later)

Removing apps (available in iOS 7.0 and later)

Game Center (available in iOS 6.0 and later)

- Add friends: Leave the option selected by default or clear the check box.
- Multiplayer gaming: Leave the option selected by default or clear the check box.

Modifying account settings (available in iOS 7.0 and later)

Modifying app cellular data settings (available in iOS 7.0 and later)

Modifying Find My Friends settings (available in iOS 7.0 and later)

Pairing with non-Configurator hosts (available in iOS 7.0 and later)

Single App bundle ID: In App name, enter one or more apps.

- Security - Show in lock screen:

Control Center (available in iOS 7.0 and later)

Notification (available in iOS 7.0 and later)

Today view

- Media content - Allow:

Explicit music, podcasts, and iTunes U material

Explicit sexual content in iBooks (available in iOS 6.0 and later)

Ratings region: Click a country in the list. The default is United States.

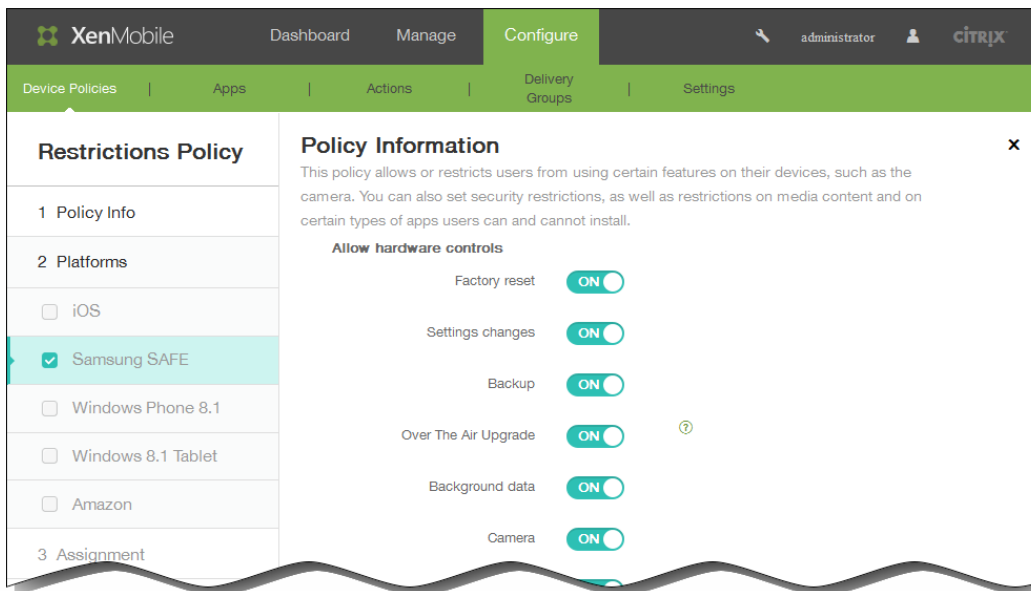
Movies: Click one of these options: Allow all movies, Block movies, G, PG, PG-13, R, NC-17; the default is Allow all movies.

TV Shows: Click one of these options: Allow all TV shows, Block TV shows, TV-Y, TV-Y7, TV-G, TV-PG, TV-PG14, TV-MA; the default is Allow all TV Shows.

Apps: Click one of these options: Allow all apps, Block apps, 4+, 9+, 12+, or 17+; the default is Allow all apps.

- If you selected Samsung SAFE, configure these settings.

Note: Some options are available only under Samsung Mobile Device Management API 4.0 and later; they are marked with (MDM 4.0 and later).



- In Allow hardware controls:

Factory Reset

Settings changes

Backup

Over The Air Upgrade (MDM 4.0 and later)

Background data

Camera

Clipboard

Clipboard share (MDM 4.0 and later)

Home key

Microphone

Mock location

NFC (Near Field Communication) (MDM 4.0 and later)

Power off (MDM 4.0 and later)

Screenshot

SD card

Voice Dialer (MDM 4.0 and later)

SBeam (MDM 4.0 and later)

SVoice (MDM 4.0 and later)

- In Allow apps:

Browser

YouTube

GooglePlay/Marketplace

Allow No-Google Play apps

Stop system app (MDM 4.0 and later)

- In Network:

Bluetooth; Tethering

WiFi; Tethering, Direct (MDM 4.0 and later)

Tethering

Cellular data

Allow roaming. The default is OFF.

Only secure connections

Android beam (MDM 4.0 and later)

Audio record (MDM 4.0 and later)

Video record (MDM 4.0 and later)

Location services

Limit by day (MB): Enter the number of MB per day users are allowed. The default is 0, which disables this feature. (MDM 4.0 and later)

Limit by week (MB): Enter the number of MB per week users are allowed. The default is 0, which disables this feature. (MDM 4.0 and later)

Limit by month (MB): Enter the number of MB per month users are allowed. The default is 0, which disables this feature. (MDM 4.0 and later)

- In Allow USB actions:

Debugging

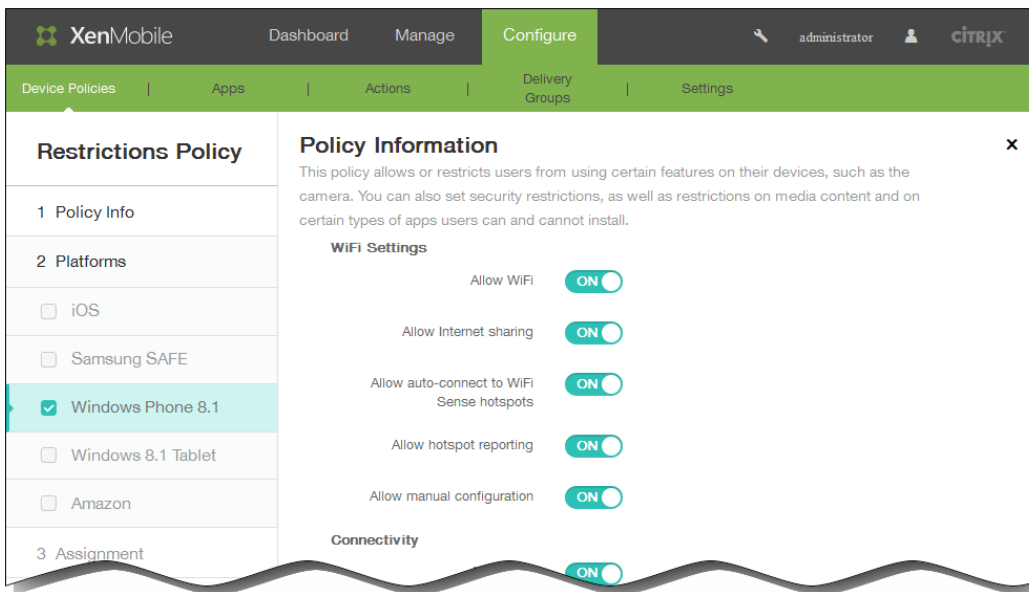
Host storage

Mass storage

Kies media player

Tethering

- If you selected Windows Phone 8.1, configure these settings:



- WiFi Settings:

Allow WiFi

Allow Internet sharing

Allow auto-connect to WiFi Sense hotspots

Allow hotspot reporting

Allow manual configuration

- Connectivity:

Allow NFC (Near Field Communication)

Allow bluetooth

Allow VPN over cellular

Allow VPN over cellular while roaming

Allow USB connection

Allow cellular data roaming

- Accounts:

Allow Microsoft account connection

Allow non-Microsoft email

- Search:

Allow search to use location

Filter adult content (The default is OFF.)

Allow Bing Vision to store images

- System:

Allow storage card

Allow location services

Allow use of camera

Telemetry: Click one of the these settings: Allowed, Not Allowed, Allowed except for secondary data request. The default is Allowed.

- Security:

Allow manual root certificate installation

Require device encryption The default is OFF.

Allow copy and paste

Allow screen capture

Allow voice recording

Allow Save As of Office files

Allow action center notifications

Allow Cortana

Allow sync of device settings

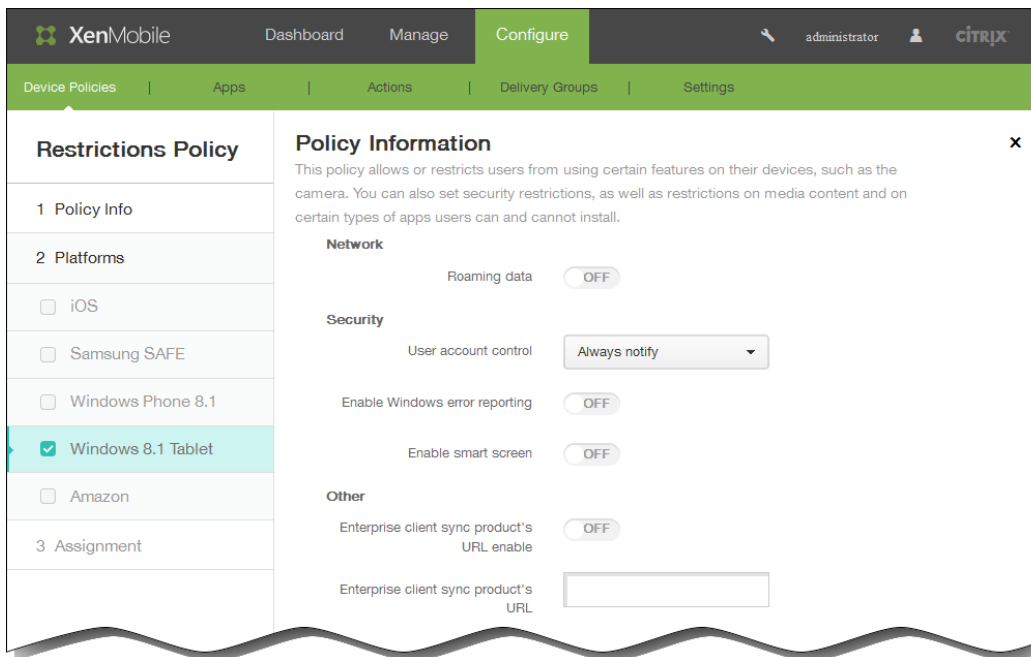
- Apps:

Allow store access

Allow developer unlock

Allow web browser access

- If you selected Windows 8.1 Tablet, configure these settings:



- Network:

Roaming data

- Security:

User account control: In the list, click one of these settings: Always notify, Notify app changes, Notify app changes (no dim), Never notify. The default is Always notify.

Enable Windows error reporting

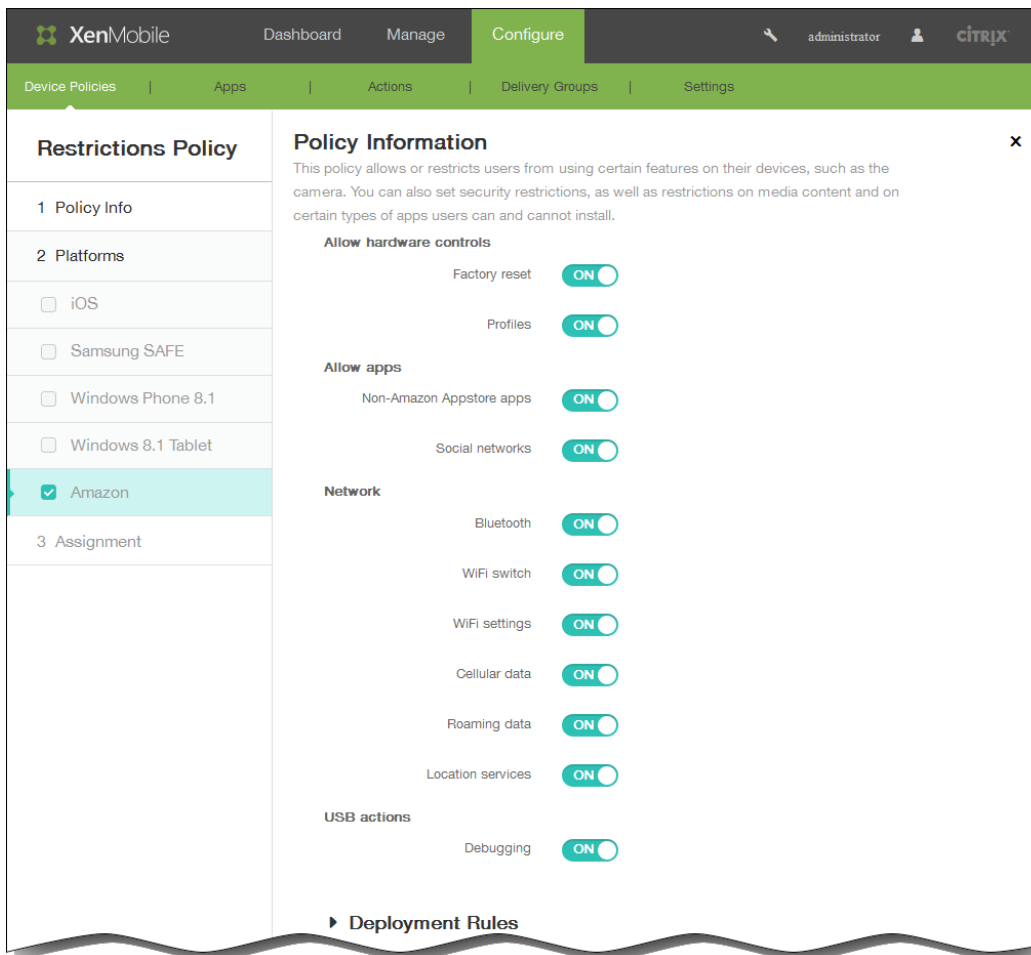
Enable smart screen

- Other:

Enterprise client sync product's URL enable

Enterprise client sync product's URL: Type a valid URL address.

- If you selected Amazon, configure these settings:



- Allow hardware controls:
 - Factory reset
 - Profiles
- Allow apps:
 - Non-Authorized Appstore apps
 - Social networks
- Network:
 - Bluetooth
 - WiFi switch
 - WiFi settings
 - Cellular data
 - Roaming data
 - Location services

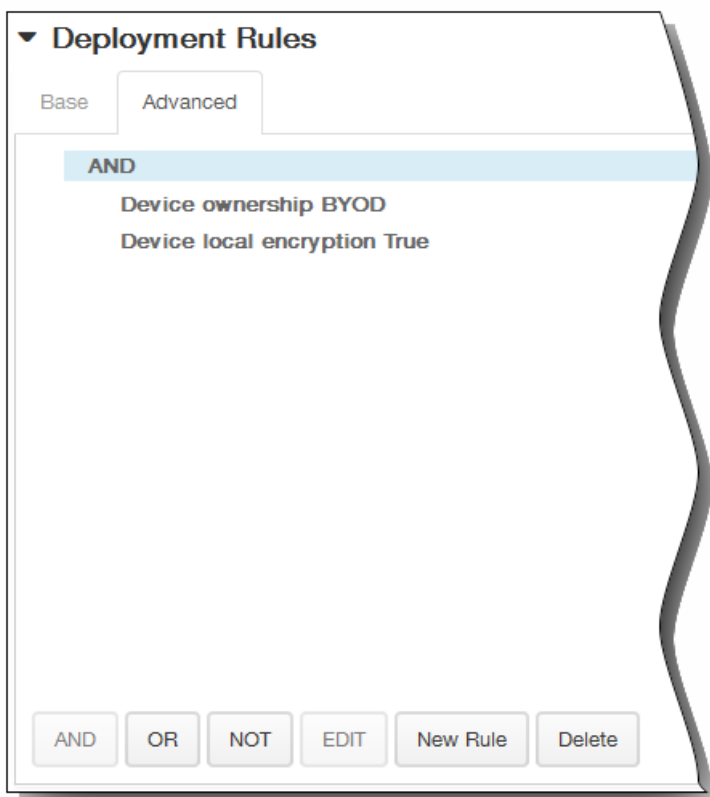
- USB actions:

Debugging

6. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.

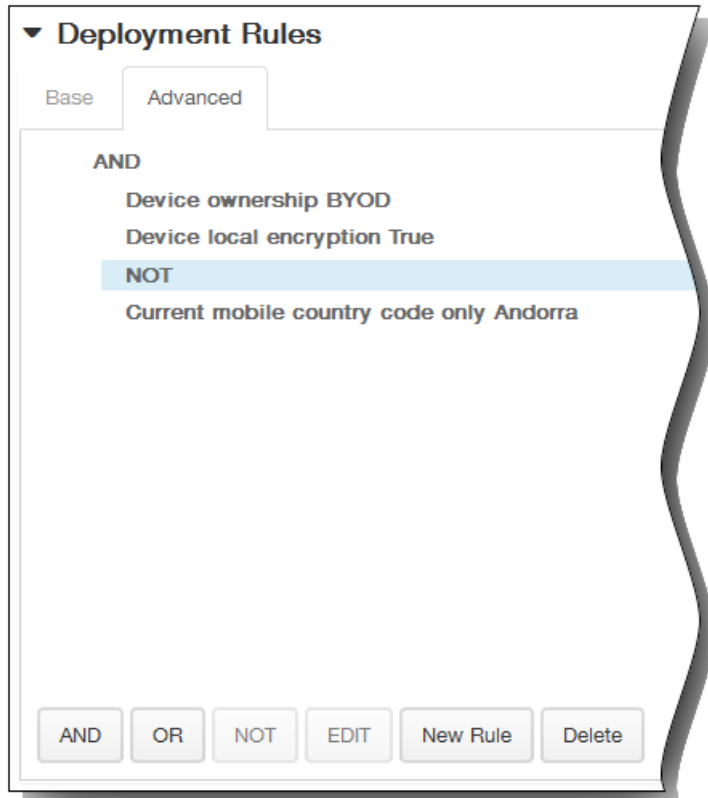


1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

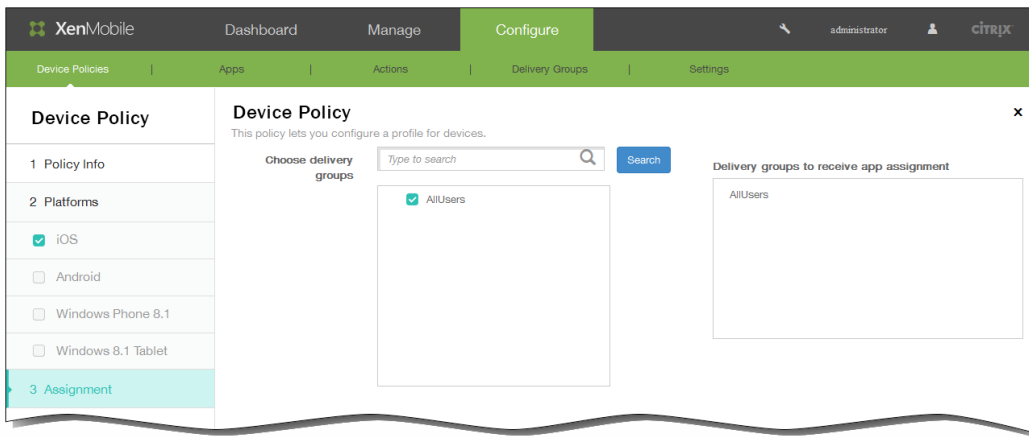


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
3. Click New Rule again if you want to add more conditions.
In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



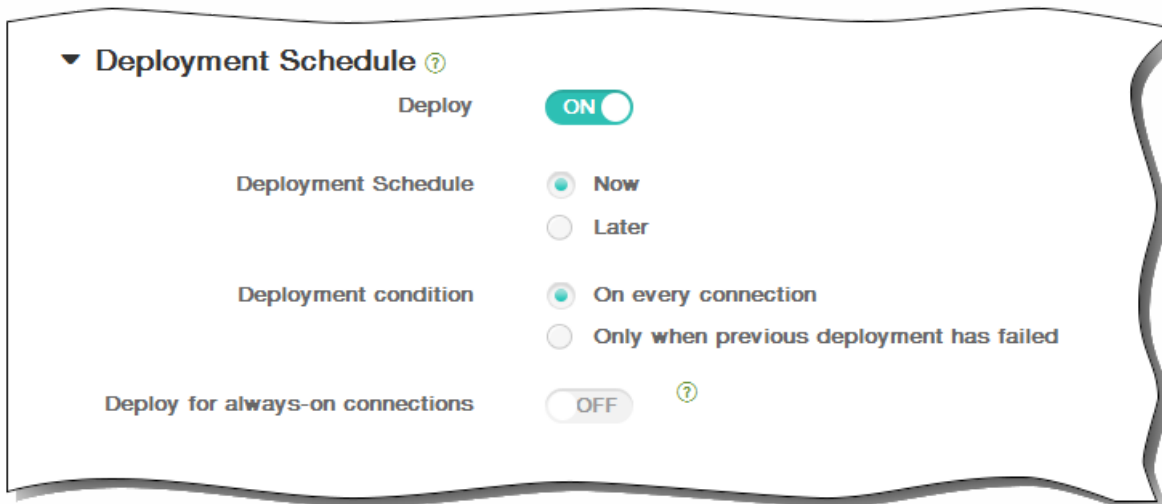
7. After you finish configuring the settings for one or more platforms, click Next and the Assignment page appears.
8. Next to Choose delivery groups, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand Delivery groups to receive app assignment list.



9. Expand Deployment Schedule and then configure the following settings:
 1. 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.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



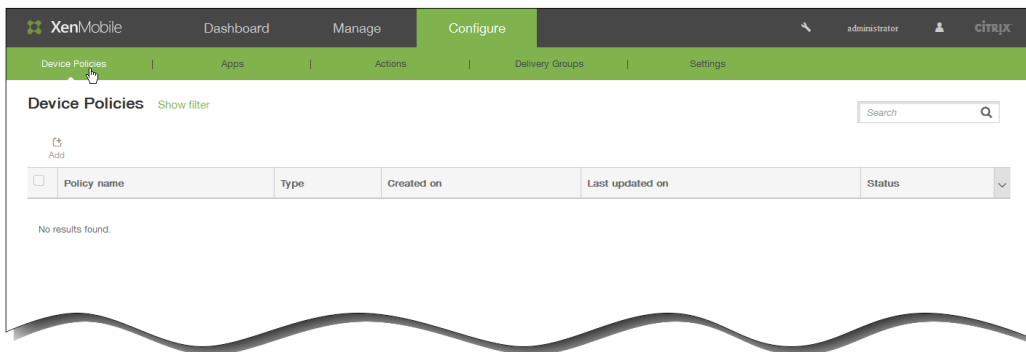
10. Click Save to save the policy.

To add a roaming device policy for iOS

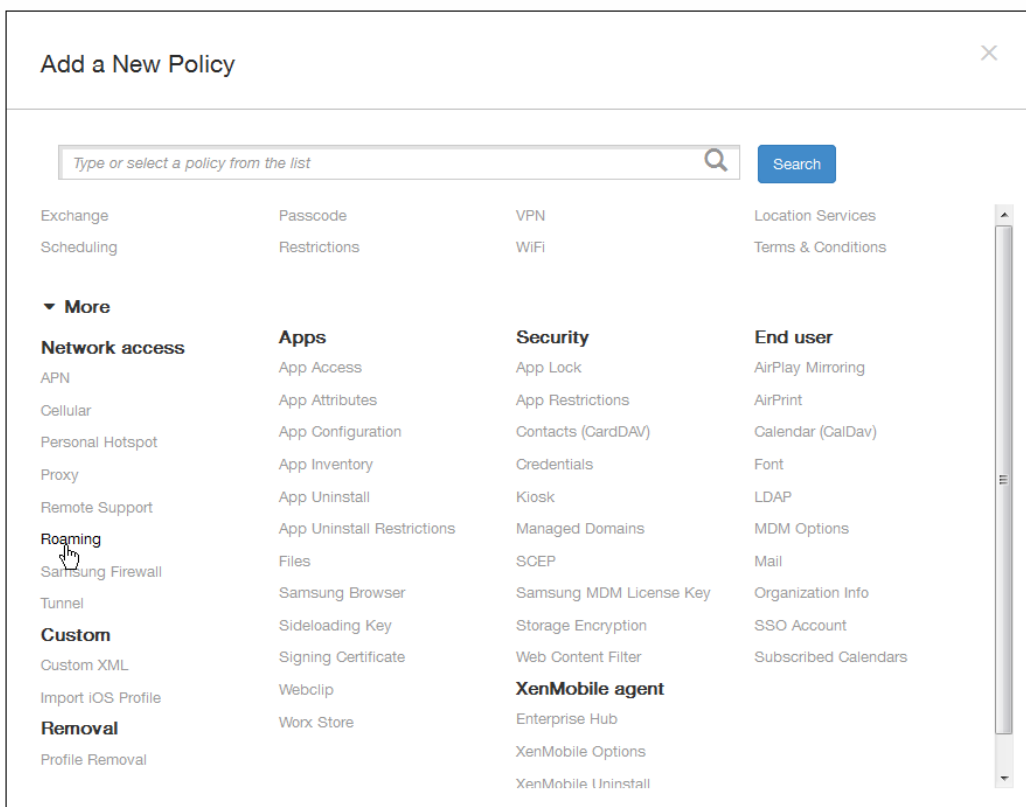
Mar 03, 2015

You can add a device policy in XenMobile to configure whether to allow voice and data roaming on users' iOS devices. When voice roaming is disabled, data roaming is automatically disabled. This policy is available only on iOS 5.0 and later devices.

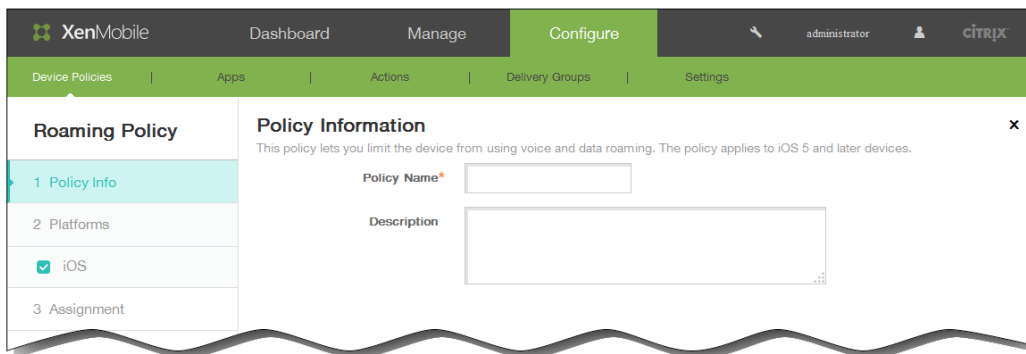
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



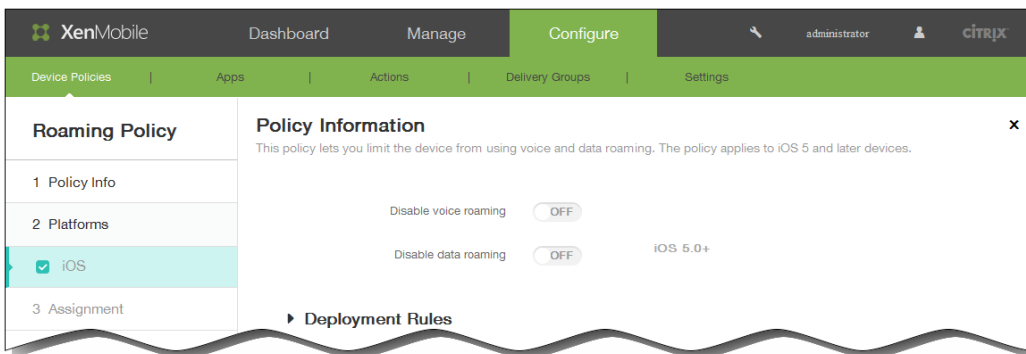
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



3. Click More and then, under Network access, click Roaming. The Roaming Info Policy page appears.



4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform Information page appears.

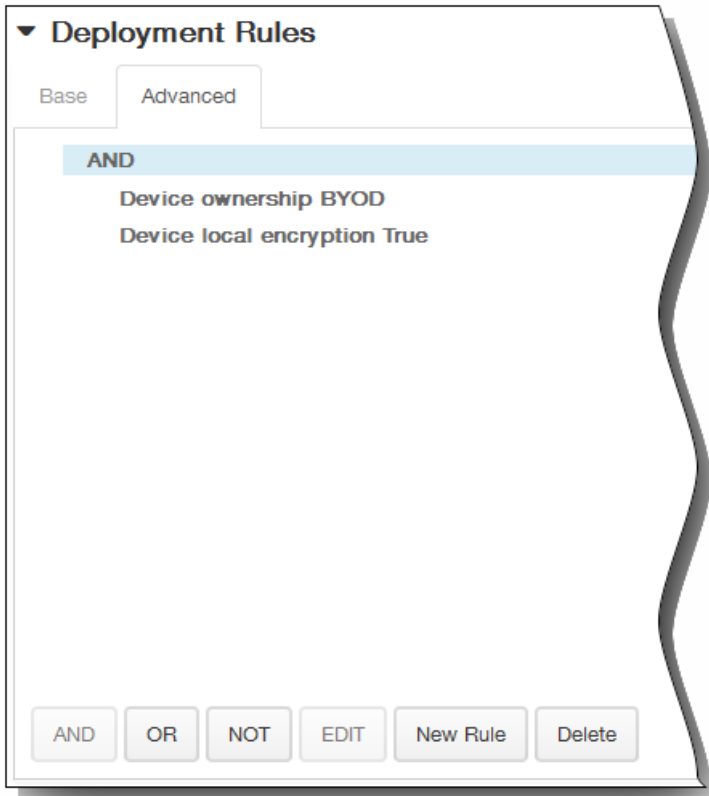


6. In the iOS Platform Information page, enter the following information:
 1. Disable voice roaming: Select whether to disable voice roaming. When this option is enabled, data roaming is automatically disabled. The default is OFF, which allows voice roaming.
 2. Disable data roaming: Select whether to disable data roaming. This option is available only when voice roaming is enabled. The default is OFF, which allows data roaming.
7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.

2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

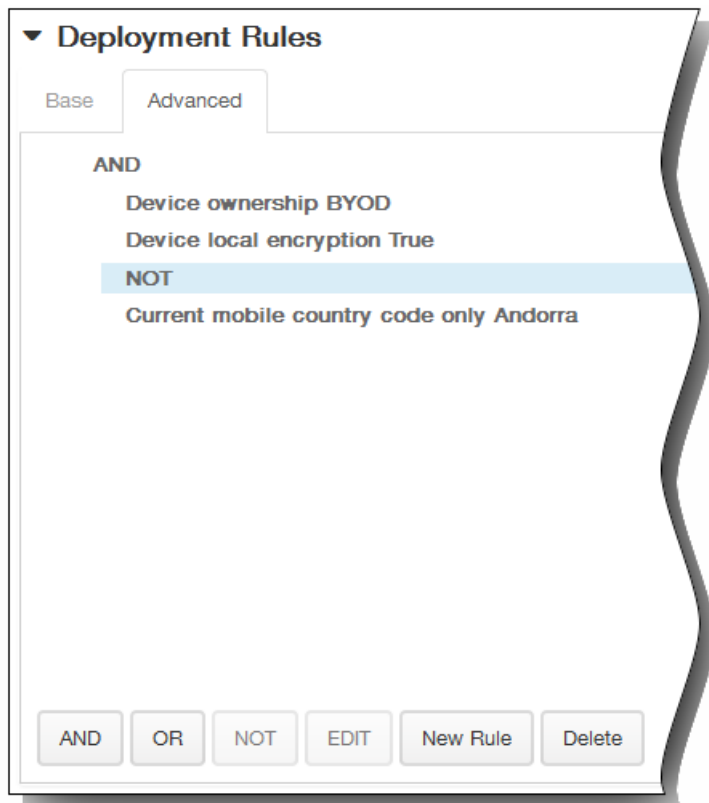


The conditions you chose on the Base tab appear.

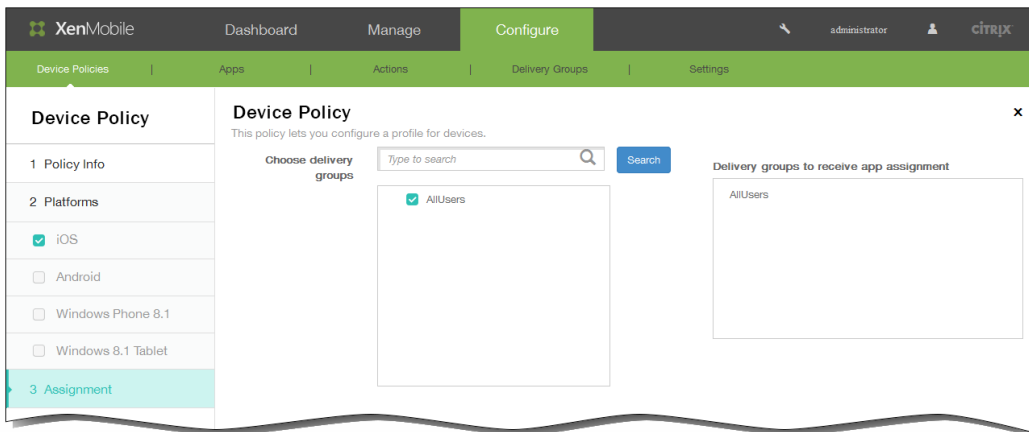
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



8. Click Next. The Roaming 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 right-hand Delivery groups to receive app assignment list.

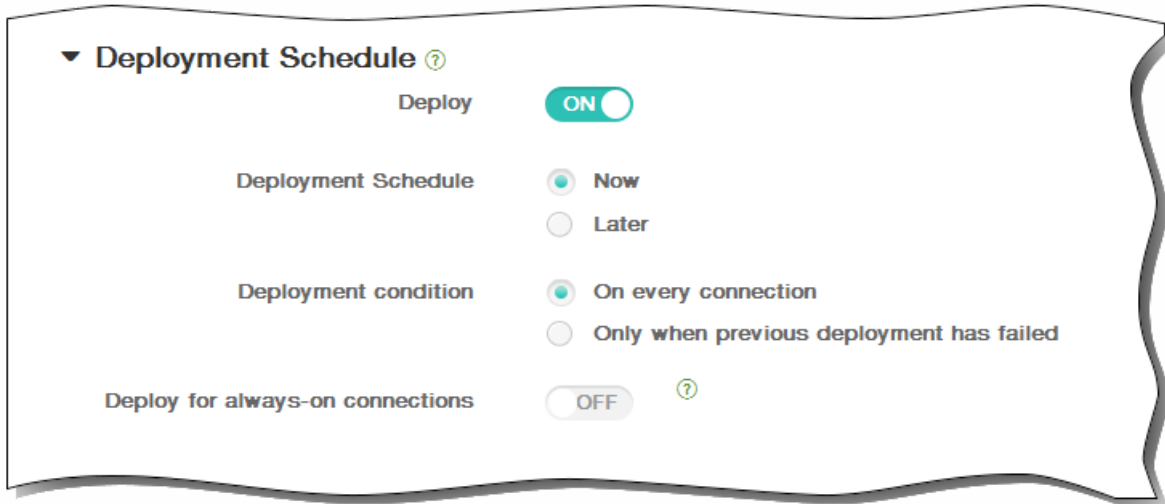


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

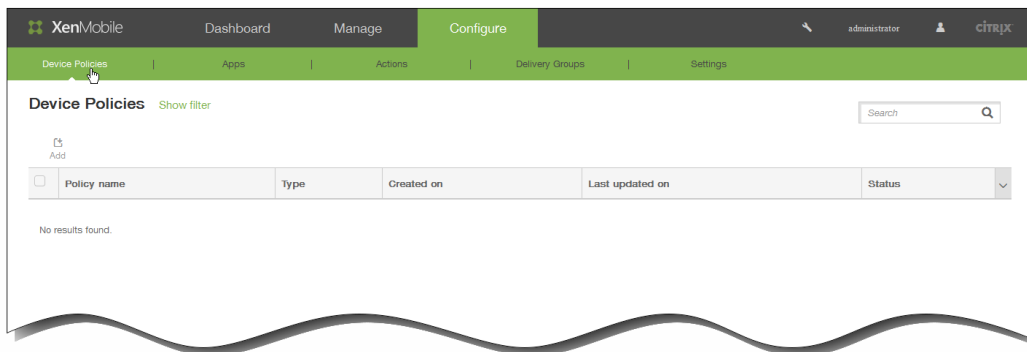
To add a SCEP device policy for iOS

Mar 04, 2015

This policy allows you to configure iOS 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](#).

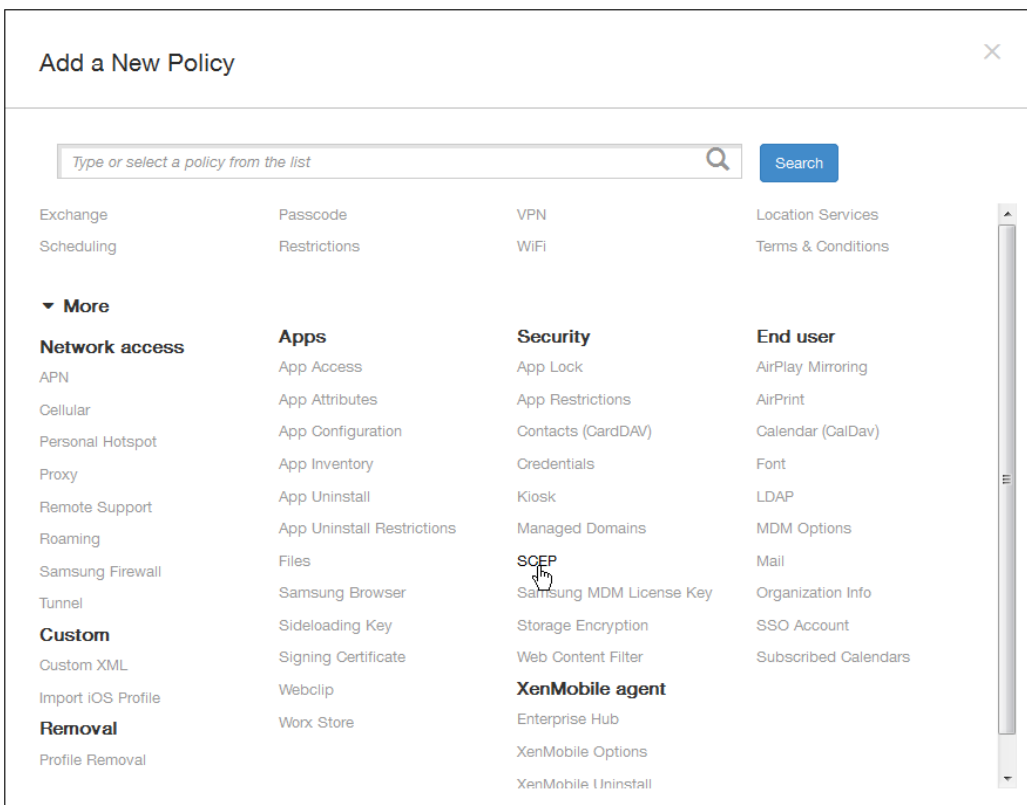
1. In the XenMobile console, click Configure > Device Policies.

The Device Policies page appears.

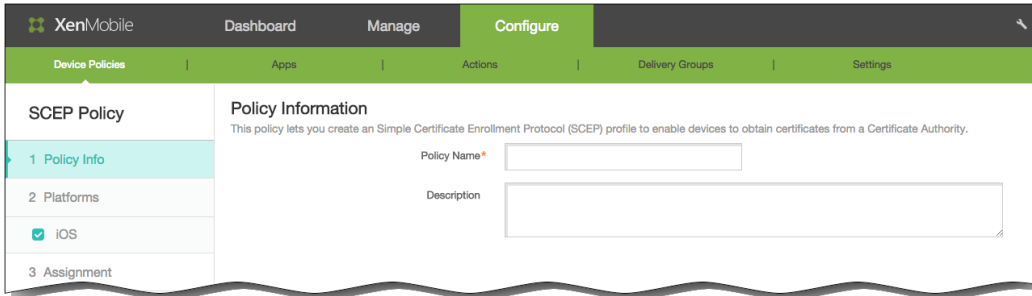


2. Click Add.

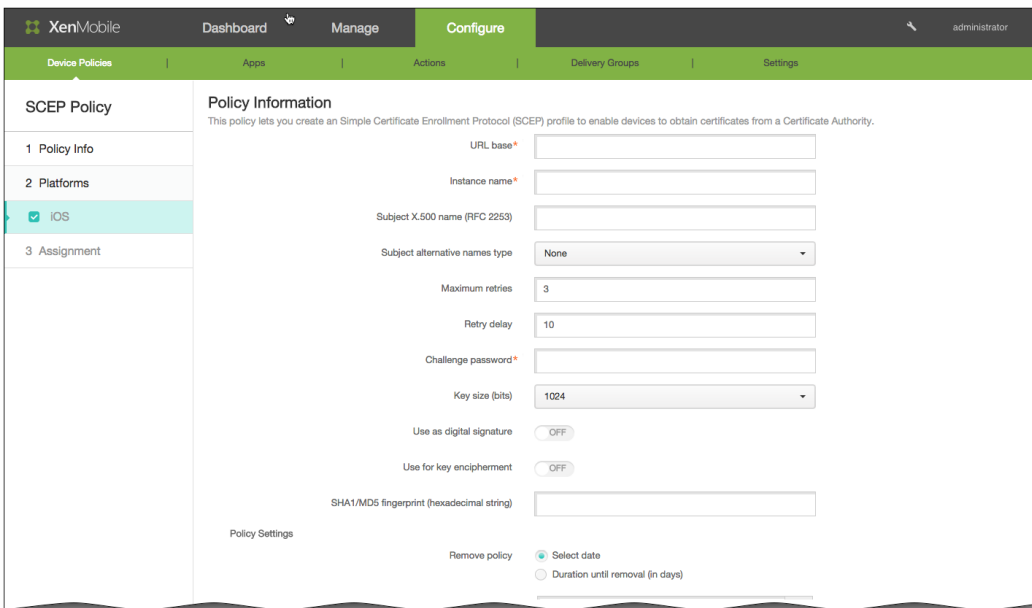
The Add a New Policy page appears.



3. On the Add a New Policy page, click More and then under Security, click SCEP. The SCEP Policy information page appears.



4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description for the policy.
5. Click Next. The iOS Platform Information page appears.



6. On the iOS Platform Information page, enter the following information:
 1. 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.
 2. 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.

3. 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).
 4. 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.
 5. Maximum retries: Type the number of retries allowed when a user enters an incorrect password. The default is 3.
 6. Retry delay: Type a time interval after which users exceed the maximum number of retries and a lockout is enforced. The default is 10.
 7. Challenge password: Enter a pre-shared secret. This step is required.
 8. Key size (bits): In the list, click the key size in bits, either 1024 or 2048. The default is 1024.
 9. 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.
 10. 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.
 11. 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.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
 8. If you click Select date, click the calendar to select the specific date for removal.
 9. In the Allow user to remove policy list, click Always, Password required, or Never.
 10. If you click Password required, next to Removal password, type the necessary password.

Policy Settings

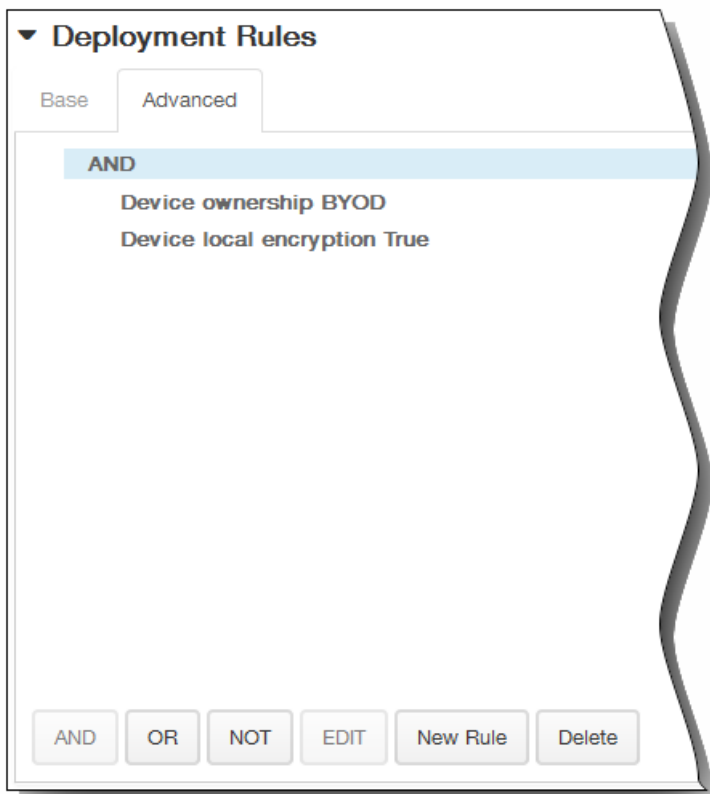
Remove policy Select date
 Duration until removal (in days)

Allow user to remove policy Always

11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



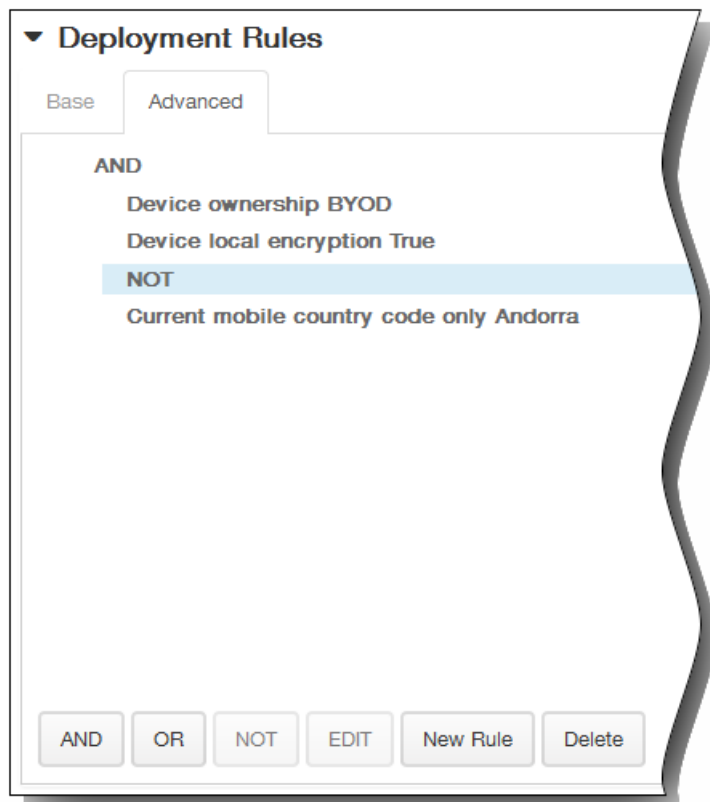
The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

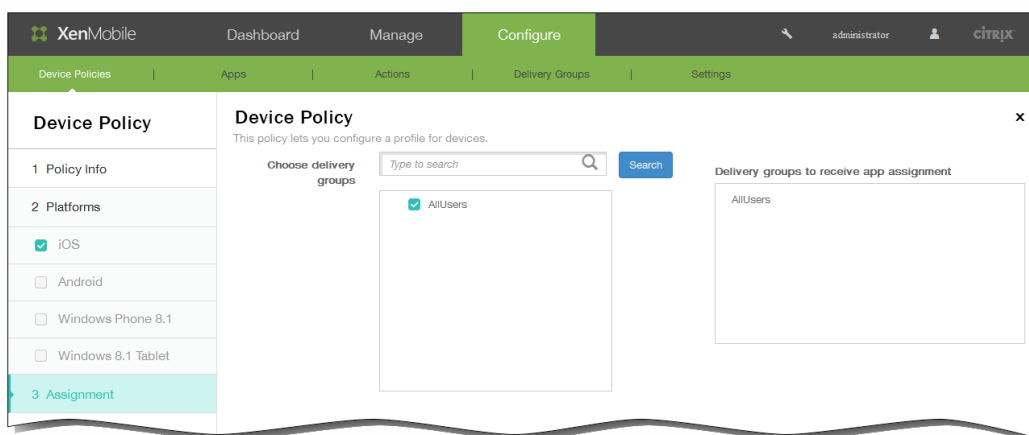
3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The SCEP Policy assignment page appears.

13. 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.

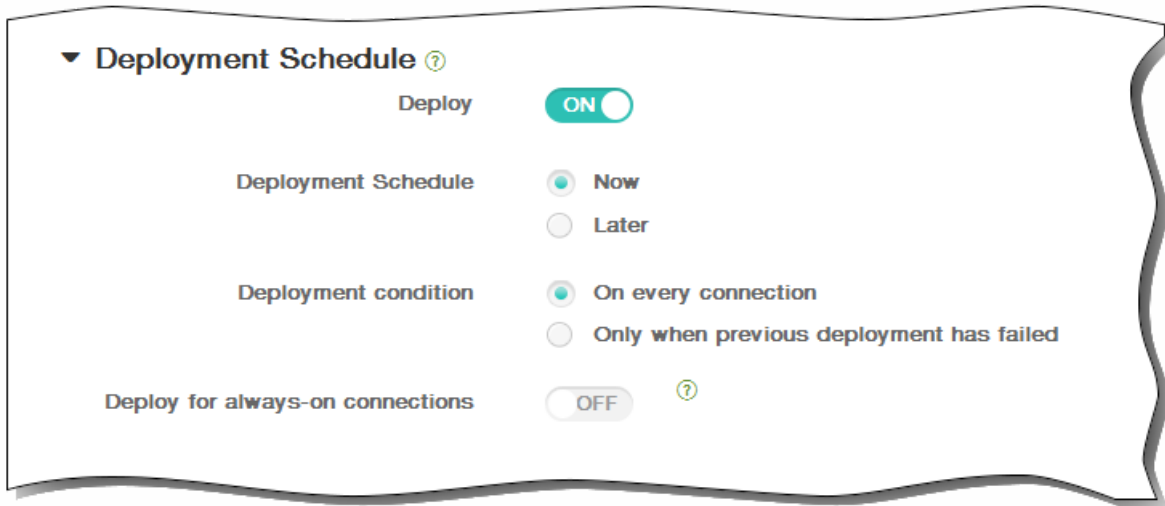


14. Expand Deployment Schedule and then configure the following settings:

1. 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.
2. Next to Deployment schedule, click Now or Later. The default option is Now.

3. If you click Later, click the calendar icon and then select the date and time for deployment.
4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



15. Click Save to save the policy.

Samsung MDM license key device policies

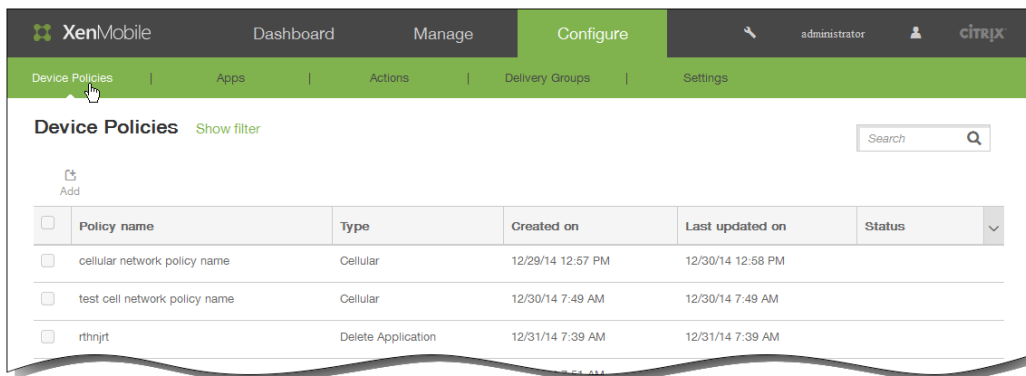
Feb 13, 2015

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.

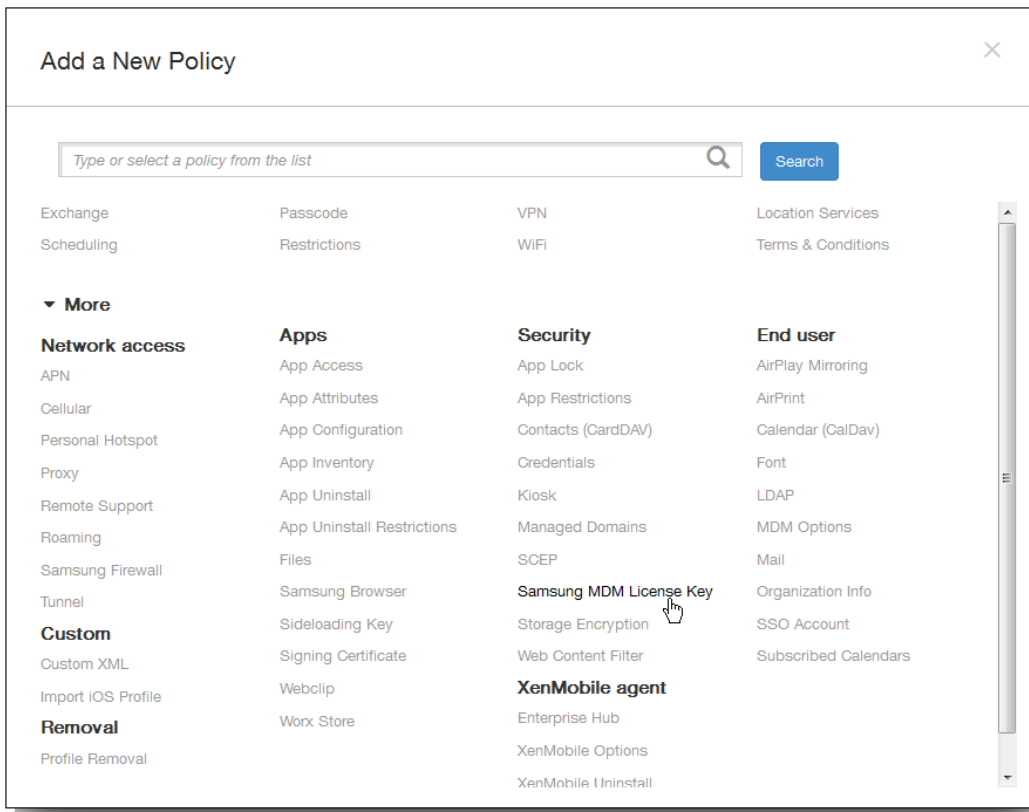
You must enable the SAFE APIs by deploying the built-in Samsung Enterprise License Management (ELM) key to a device before you can deploy SAFE policies and restrictions. To enable the Samsung KNOX API, you also need to purchase a Samsung KNOX license using the Samsung KNOX License Management System (KLMS) 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. 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.

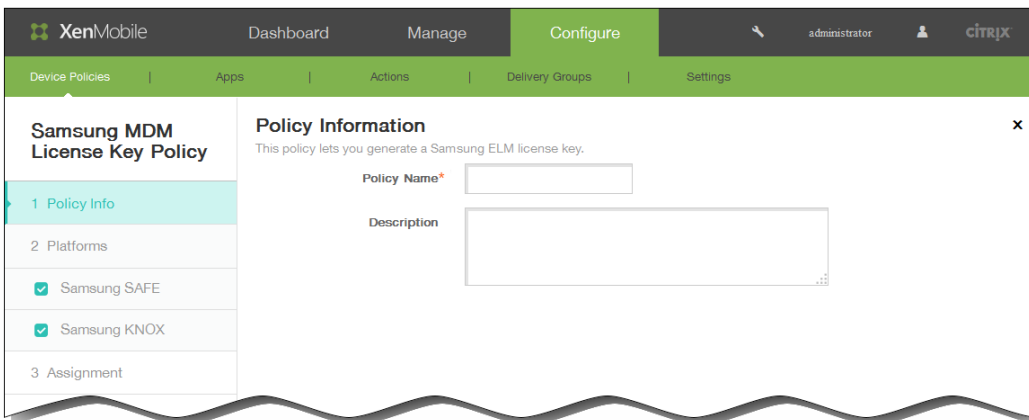
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



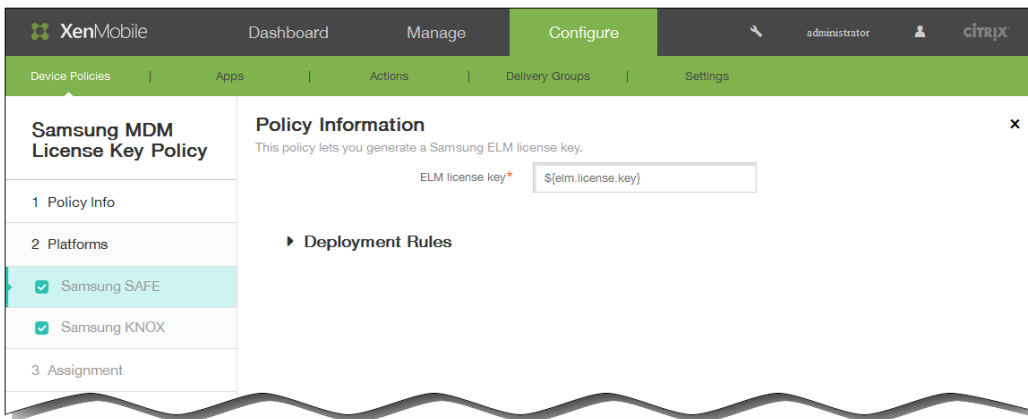
2. Click Add to add a new policy. The Add New Policy dialog appears.



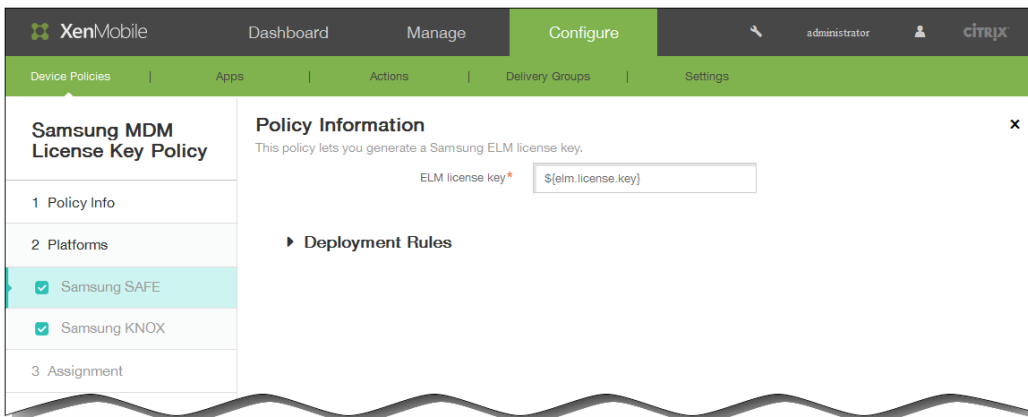
3. Click More and then under Security, click Samsung MDM Licence Key. The Samsung MDM Licence Key Policy information page appears.



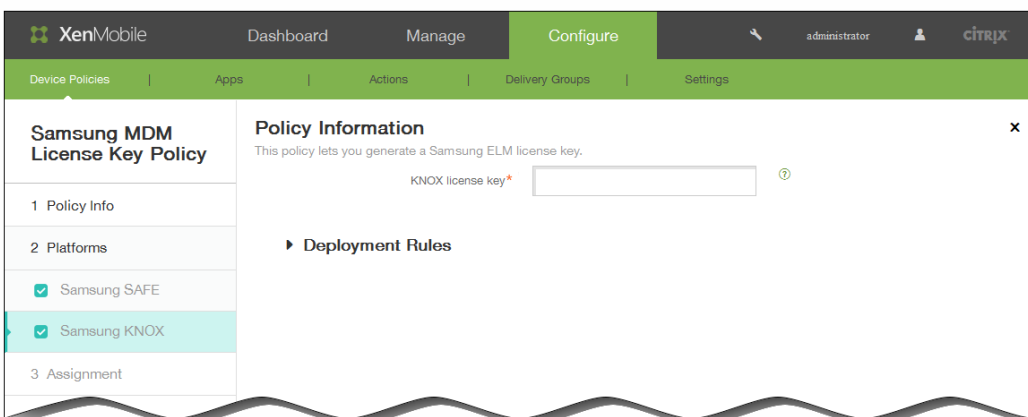
4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Type an optional description of the policy.
5. Click Next. The Policy Platforms page appears.
 Note: When the Policy Platforms page appears, both platforms are selected and you see the Samsung SAFE platform configuration panel first.



6. Under Platforms, choose the Samsung platforms for which you want to create this policy. Clear any other platform that may be selected that you don't want to include in this policy.
- If you chose Samsung SAFE, for ELM license key, enter the macro `${elm.license.key}` to generate the ELM license key. The field should already contain the macro:



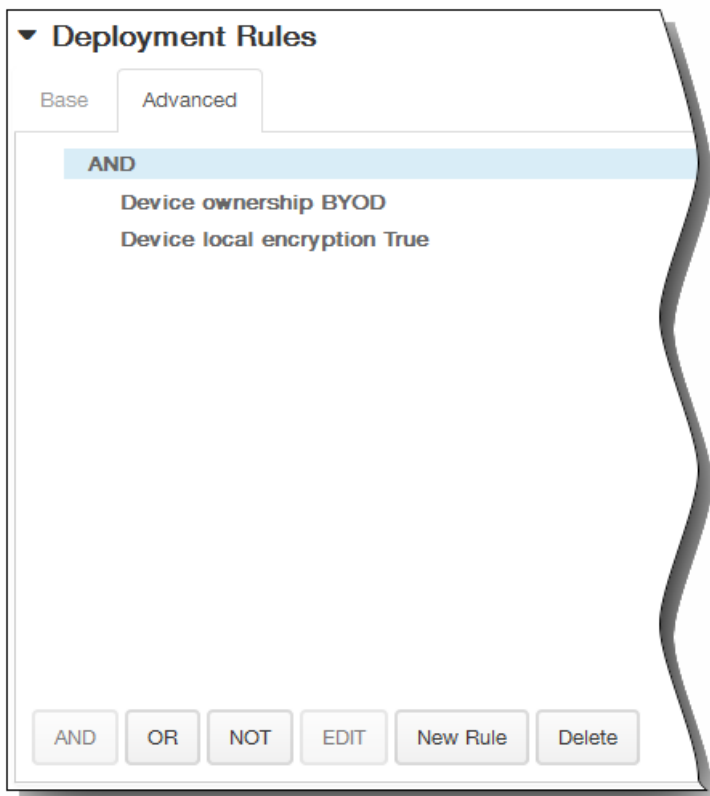
- If you chose Samsung KNOX, for KNOX license key, enter the 25-digit KNOX license key:



7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

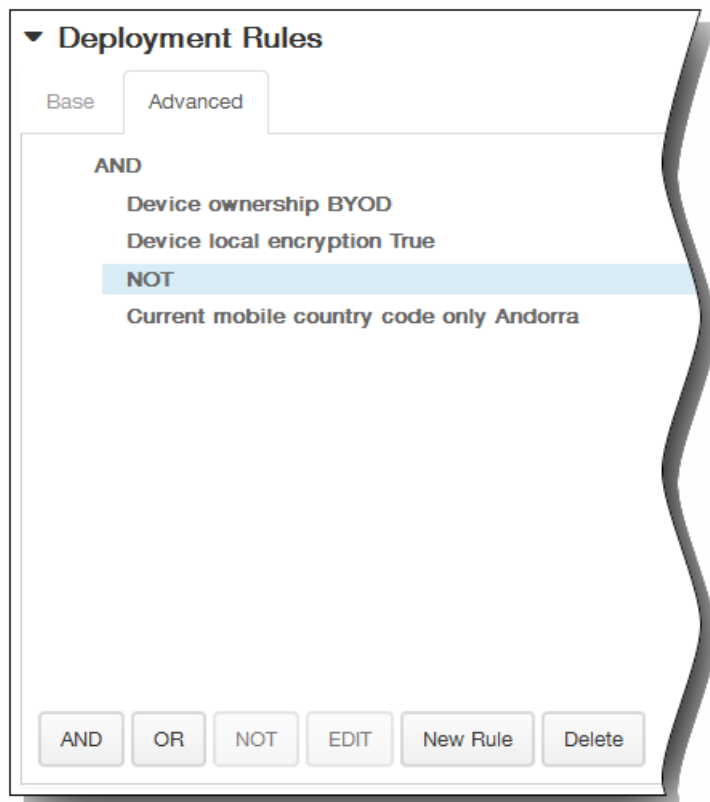


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

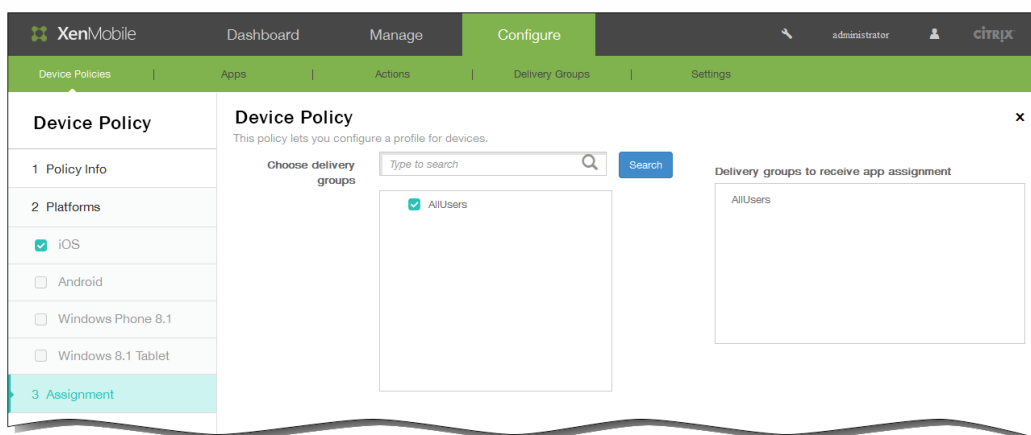
3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



8. Click Next. The Samsung MDM License Key Policy 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.

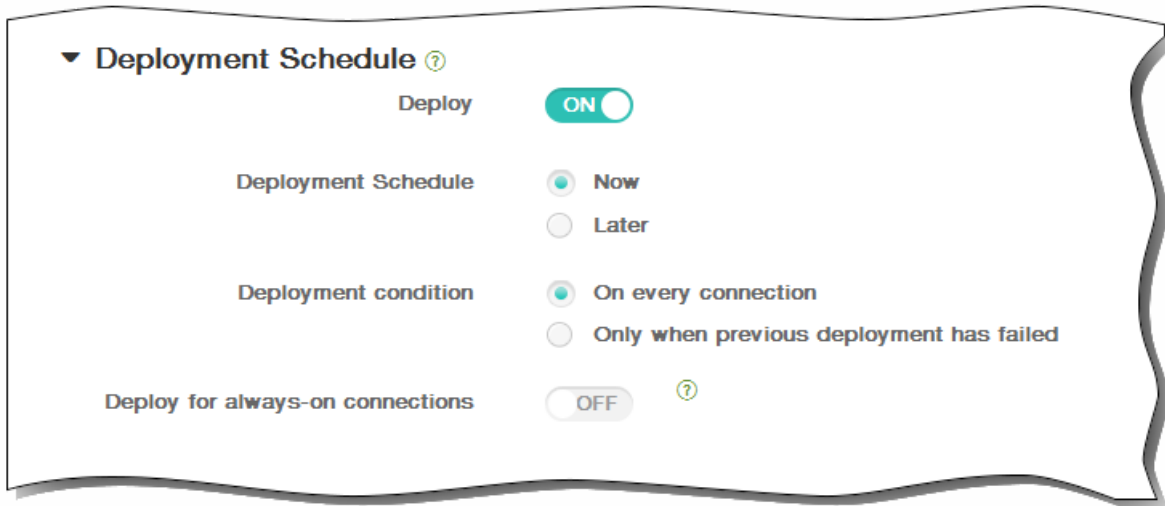


10. Expand Deployment Schedule and then configure the following settings:

1. 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.
2. Next to Deployment schedule, click Now or Later. The default option is Now.

3. If you click Later, click the calendar icon and then select the date and time for deployment.
4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

Storage encryption device policies

Apr 08, 2015

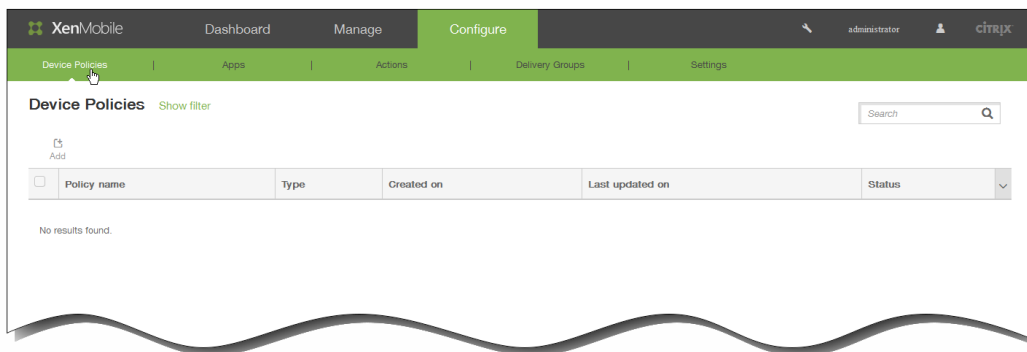
You create storage encryption device policies in XenMobile to encrypt internal and external storage, and, depending on the device, to prevent users from using a storage card on their devices.

You can create policies for Samsung SAFE, Windows 8.1 Tablet, and Android Sony devices. Each platform requires a different set of values, which are described in detail in the following steps.

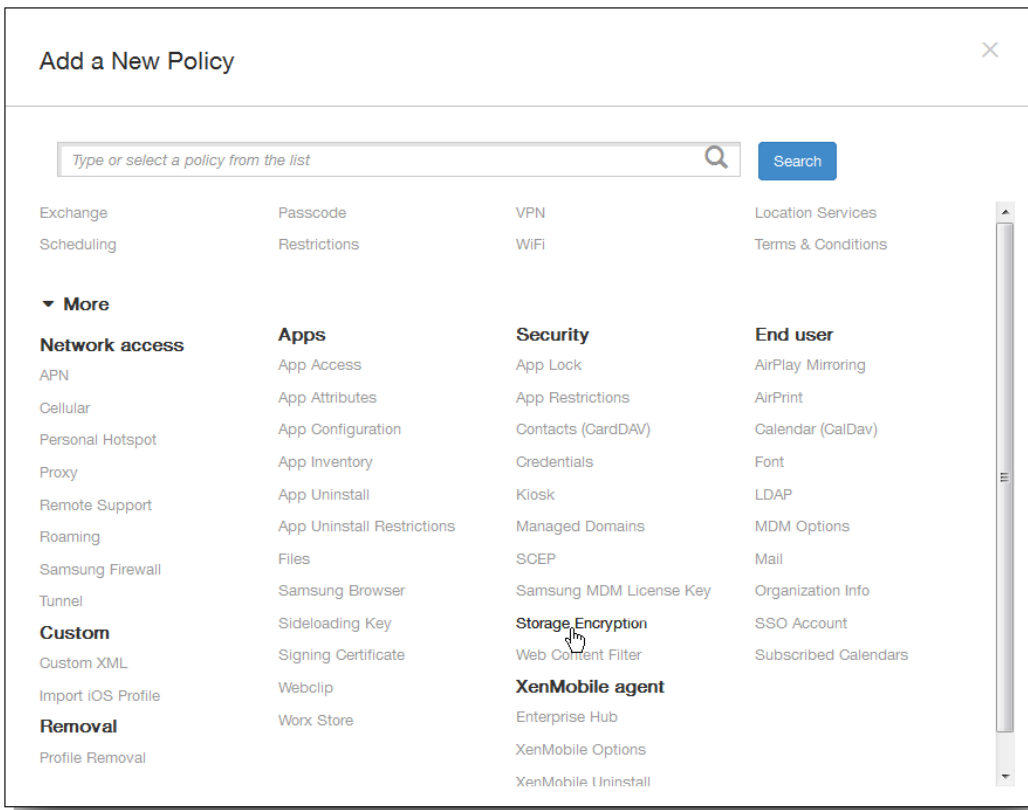
Note: For Samsung SAFE devices, before configuring this policy, make sure the following requirements are met:

- 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.

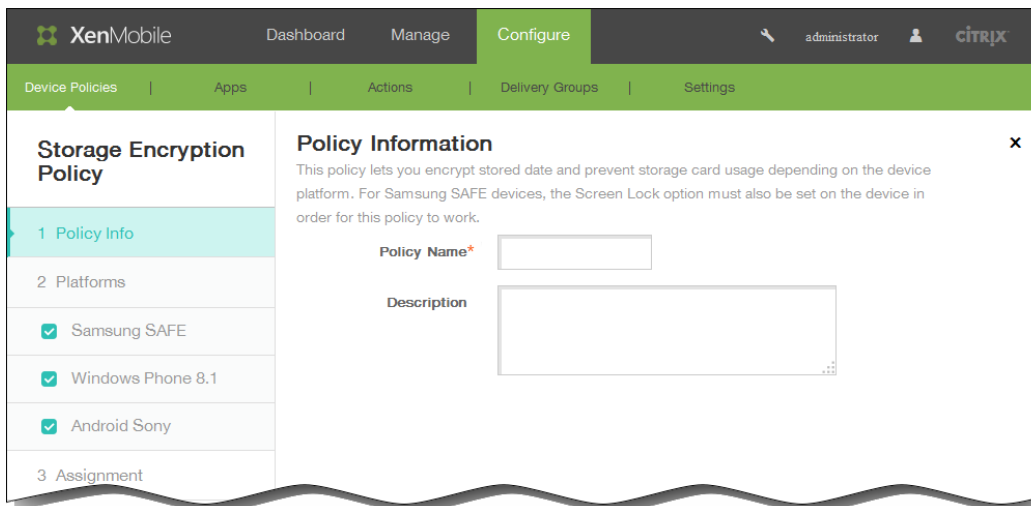
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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



3. Click More and then under Security, click Storage Encryption. The Storage Encryption Policy information page appears.

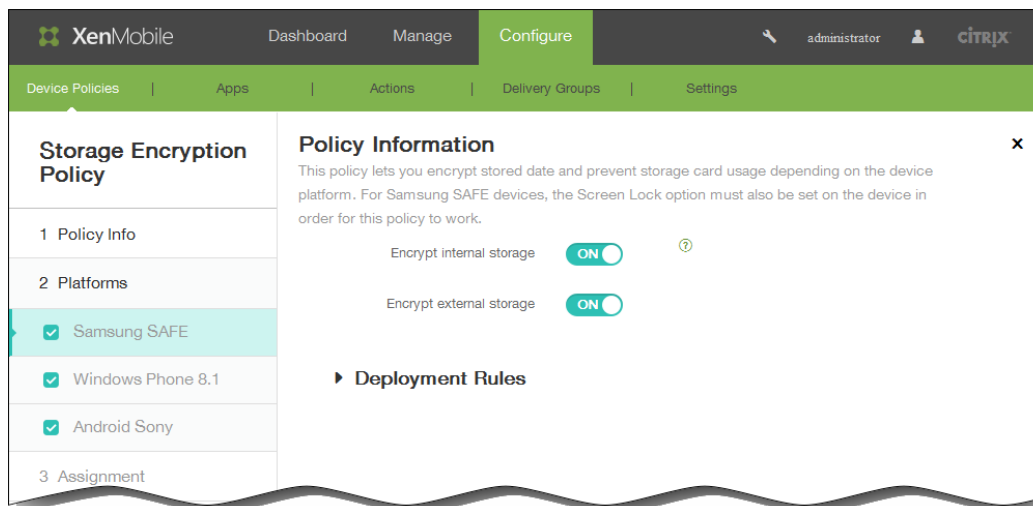


4. In the Policy Information pane, type the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Type an optional description of the policy.
5. Click Next. The Policy Platforms page appears.

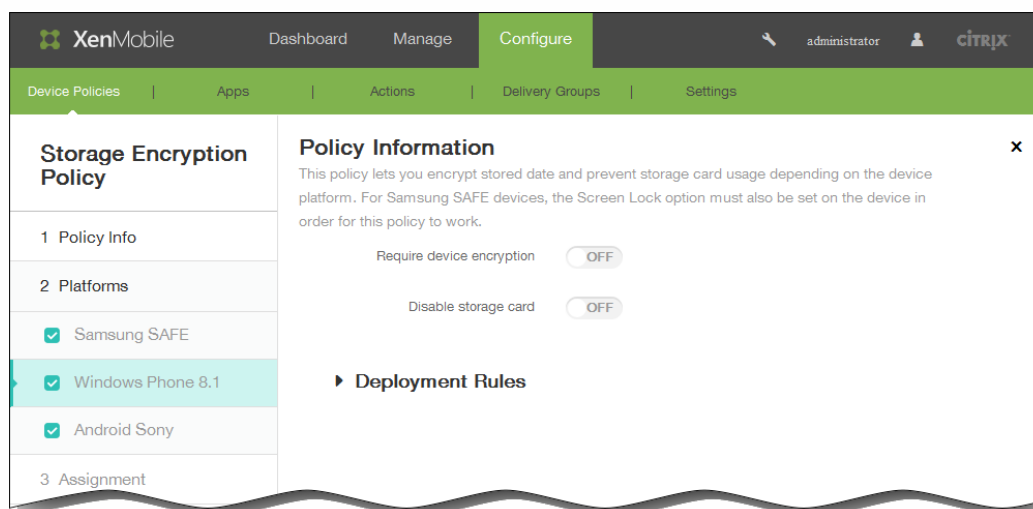
Note: When the Policy Platforms page appears, all platforms are selected and you see the Samsung SAFE platform configuration panel first.
6. Under Platforms, select the platforms for which you want to configure this policy. If this is the only platform you are

configuring, clear any other platforms that may be selected.

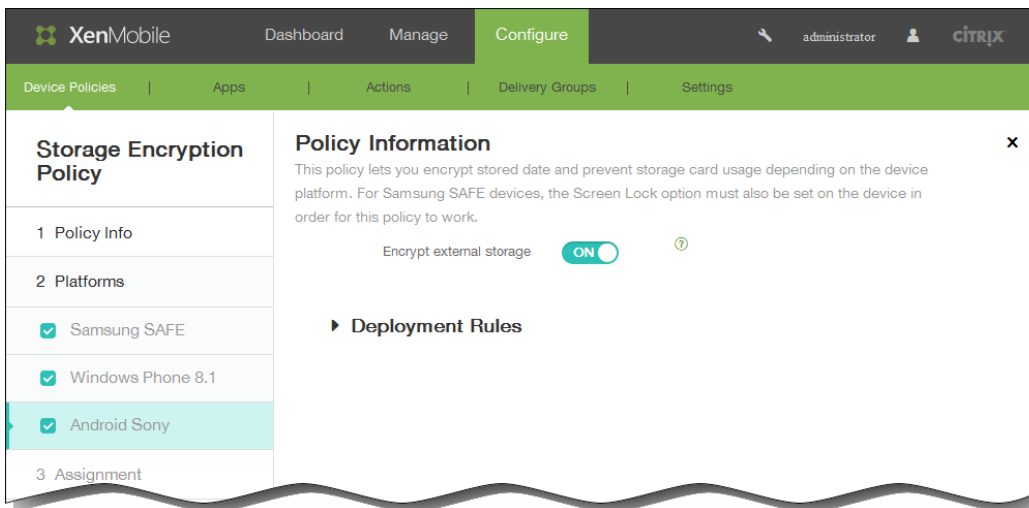
- If you select Samsung SAFE:
 - Encrypt internal storage: Select whether to encrypt internal storage on users' devices. Internal storage includes device memory and internal storage. The default is ON.
 - Encrypt external storage: Select whether to encrypt external storage on users' devices. The default is ON.



- If you select Windows Phone 8.1:
 - 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.



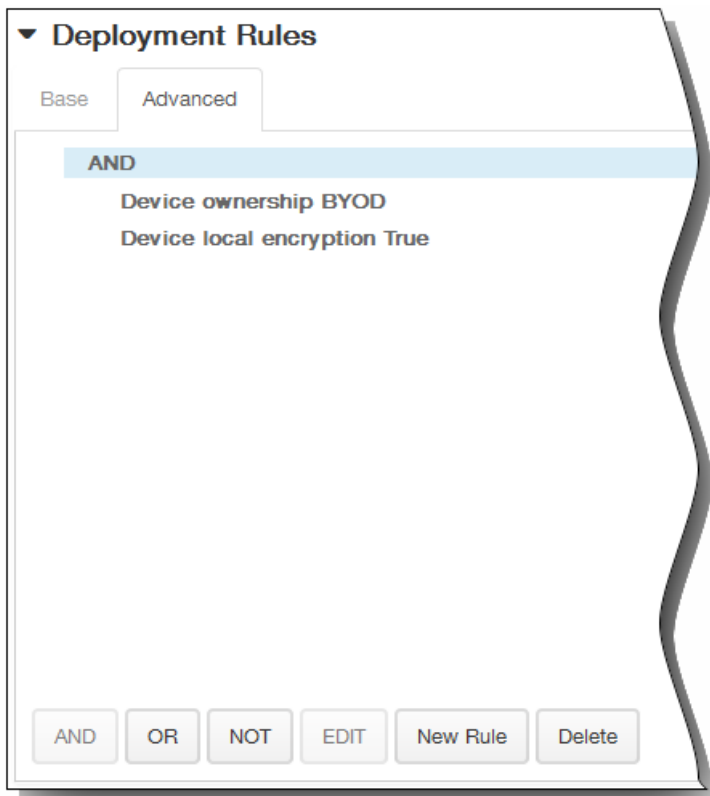
- If you select Android Sony, for Encrypt external storage, select whether to encrypt external storage on users' devices. The device must require a password containing both numbers and letters or symbols. The default is ON.



7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

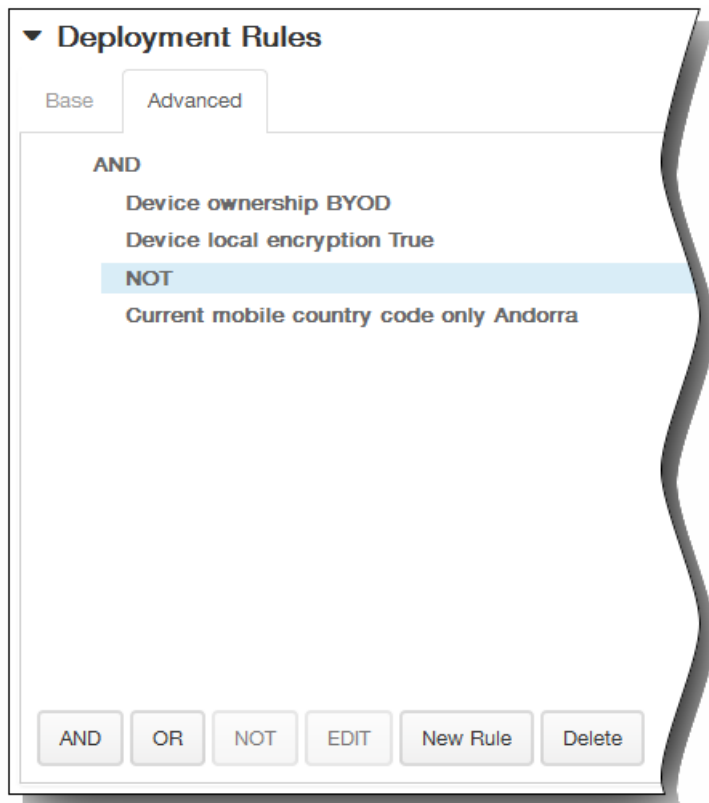


The conditions you chose on the Base tab appear.

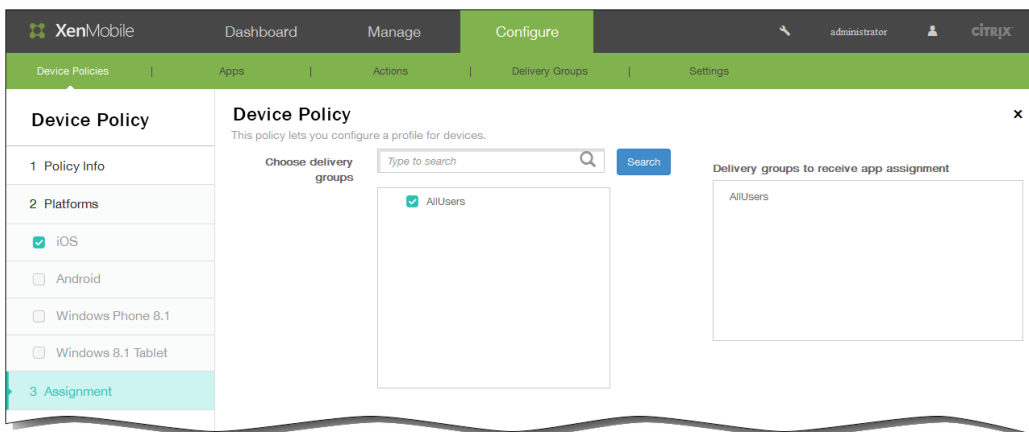
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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.

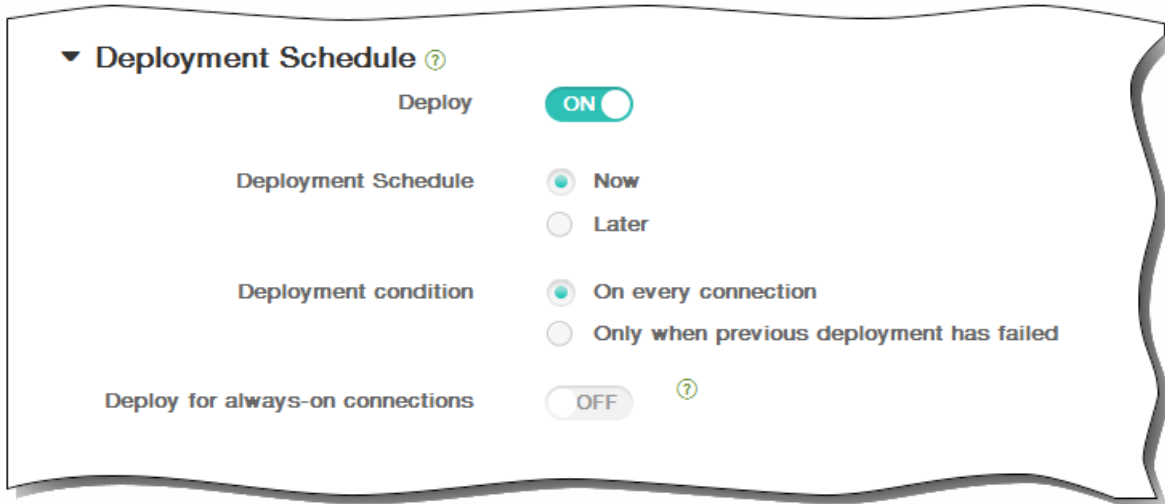


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



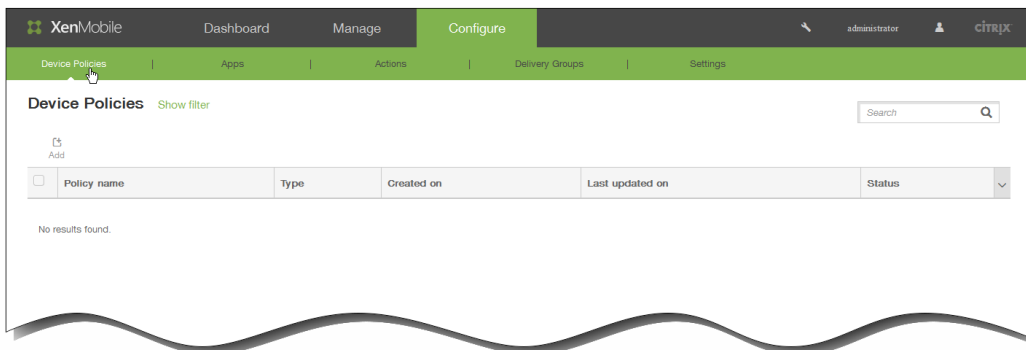
11. Click Save to save the policy.

To add a web content device policy for iOS

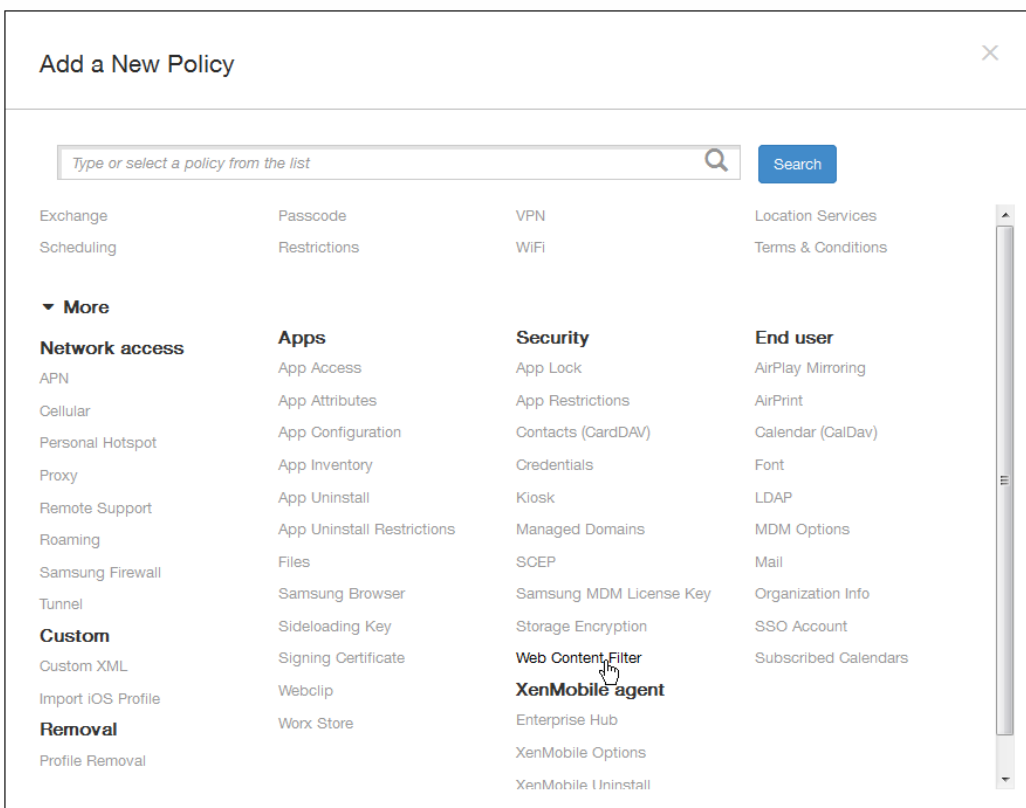
Mar 04, 2015

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](#).

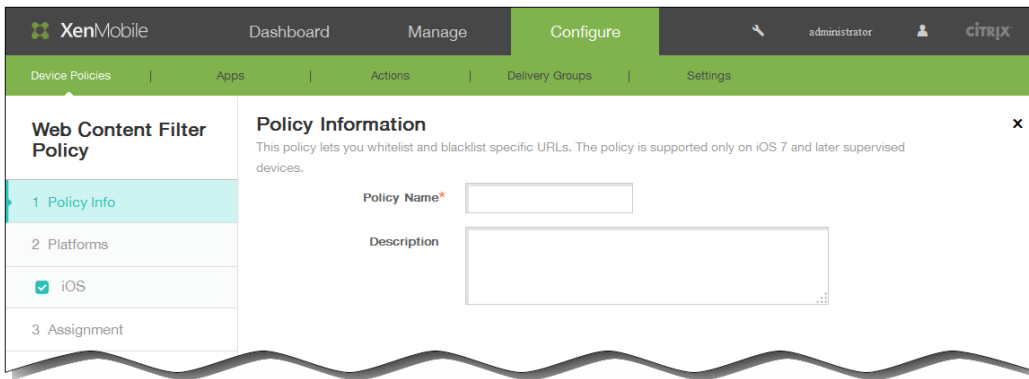
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



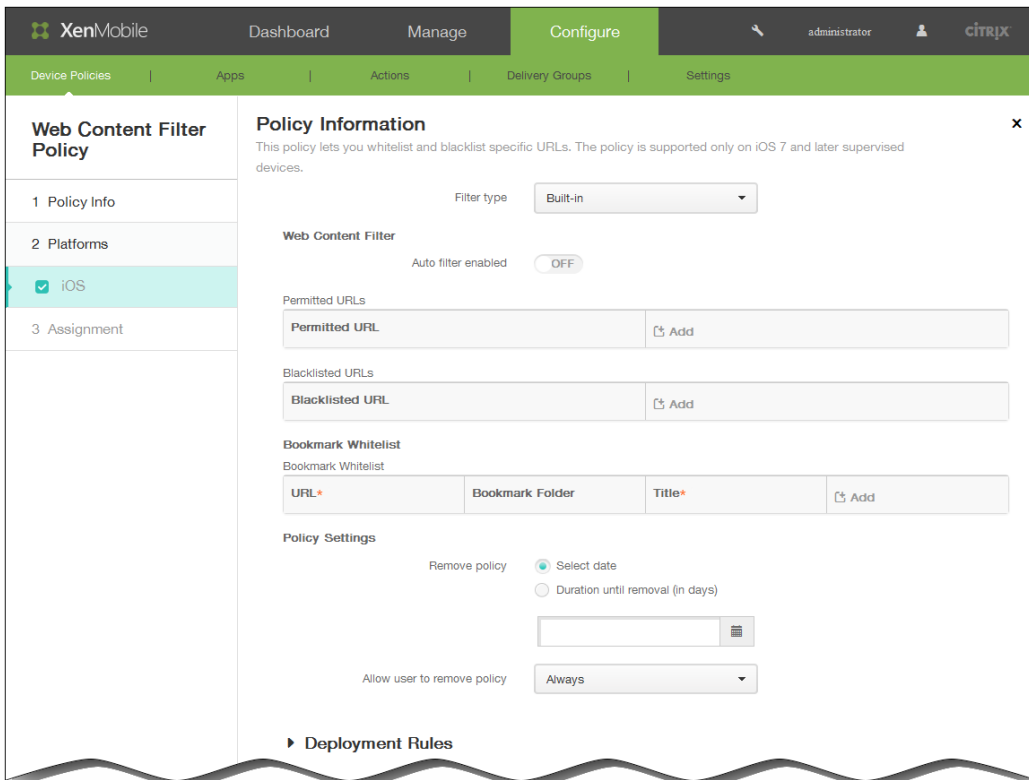
2. Click Add to add a new policy. The Add a New Policy dialog box appears.



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:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The iOS Platform information page appears.



6. In the iOS Platform Information page, in the Filter type list, do one of the following and then follow the procedures later in this topic for the option you choose:
 - Leave the default Built-in filter type.
 - Click Plug-in to configure the Plug-in filter type.

To configure the Built-in filter type

1. Auto filter enabled: Select whether to use Apple's auto-filter function to analyze websites for inappropriate content. The default is OFF.

2. Permitted URLs: This list is ignored when Auto filter enabled is set to OFF. When Auto filter enabled is set to ON, the items in this list are always accessible regardless of whether the auto filter allows access.

Click Add and then do the following to add websites to the whitelist:

1. Enter the URL of the permitted website. You must add http:// or https:// before the web address.
 2. Click Save to save the website to the whitelist or click Cancel not to save it.
 3. Repeat steps i. and ii. for each website you want to add to the whitelist.
3. Blacklisted URLs: Items in this list are always blocked.

Click Add and then do the following to add websites to the blacklist:

1. Enter the URL of the website to be blocked. You must add http:// or https:// before the web address.
 2. Click Save to save the website to the blacklist or click Cancel not to save it.
 3. Repeat steps i. and ii. for each website you want to add to the blacklist.
4. Bookmark whitelist: Items in this list are the only sites accessible to users.

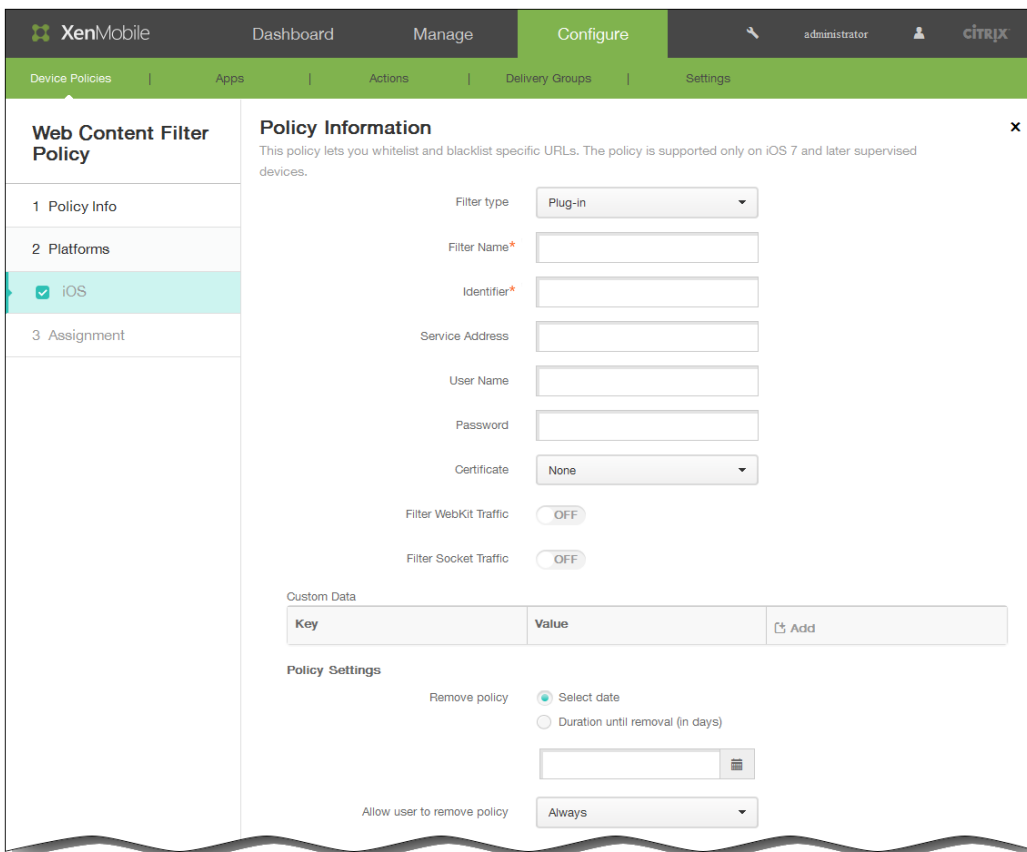
Click Add and then do the following to bookmark websites:

1. URL: Enter the URL of the website to be bookmarked. You must add http:// or https:// before the web address. This field is required.
2. Bookmark folder: Enter an optional bookmark folder name. If this field is left blank, the bookmark is added to the default bookmarks directory.
3. Title: Enter a descriptive title for the website. For example, type "Google" for the URL http://google.com.
4. Click Save to save the website to the blacklist or click Cancel not to save it.
5. Repeat steps i. through iv. for each website you want to bookmark.

Note: To delete an existing website, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing. To edit an existing website, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click Save to save the changed listing or Cancel to leave the listing unchanged.

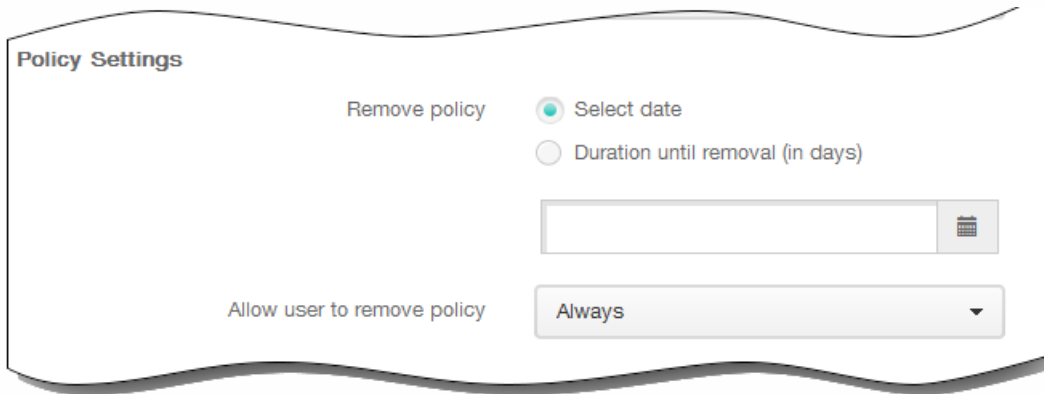
5. See Step 7 to finish configuring the Built-in filter configuration.

To configure the Plug-in filter type



1. Filter name: Enter a unique name for the filter.
2. Identifier: Enter the bundle ID of the plugin that provides the filtering service.
3. Service address: Enter an optional server address. Valid formats are IP address, hostname, or URL.
4. User name: Enter an optional user name for the service.
5. Password: Enter an optional password for the service.
6. Certificate: In the list, click an optional identity certificate to be used to authenticate the user to the service. The default is None.
7. Filter WebKit traffic: Select whether to filter WebKit traffic.
8. Filter Socket traffic: Select whether to filter socket traffic.
9. Custom Data: Click Add and then do the following to add custom data to the web content filter:
 1. Key: Enter the custom key.
 2. Value: Enter a value for the custom key.
 3. Click Save to save the custom key or click Cancel not to save it.
 4. Repeat steps i. through iii. for each custom key you want to add.

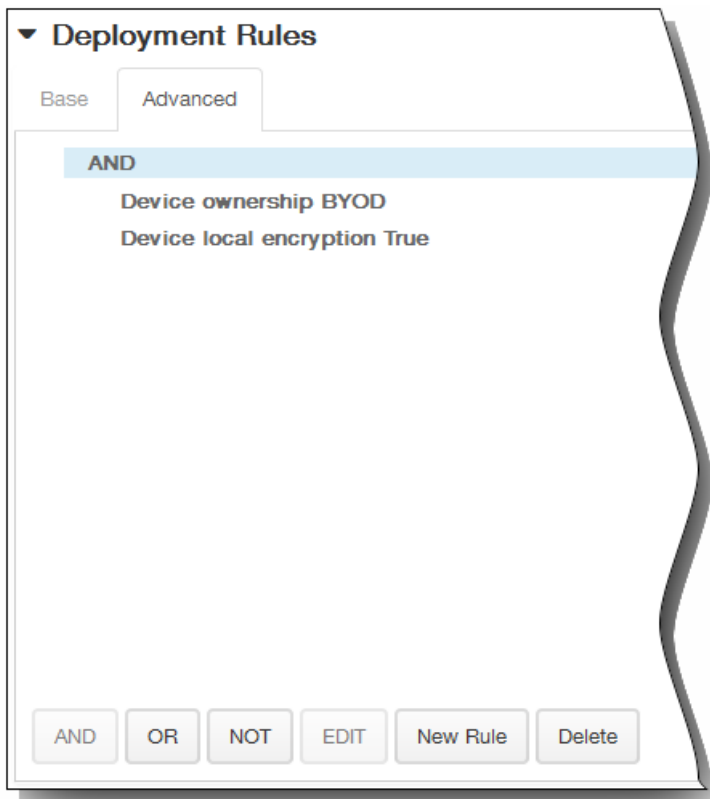
Note: To delete an existing key, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing. To edit an existing key, hover over the line containing the listing and then click the pen icon on the right-hand side. Make any changes to the listing and then click Save to save the changed listing or Cancel to leave the listing unchanged.
7. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
8. If you click Select date, click the calendar to select the specific date for removal.
9. In the Allow user to remove policy list, click Always, Password required, or Never.
10. If you click Password required, next to Removal password, type the necessary password.



11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

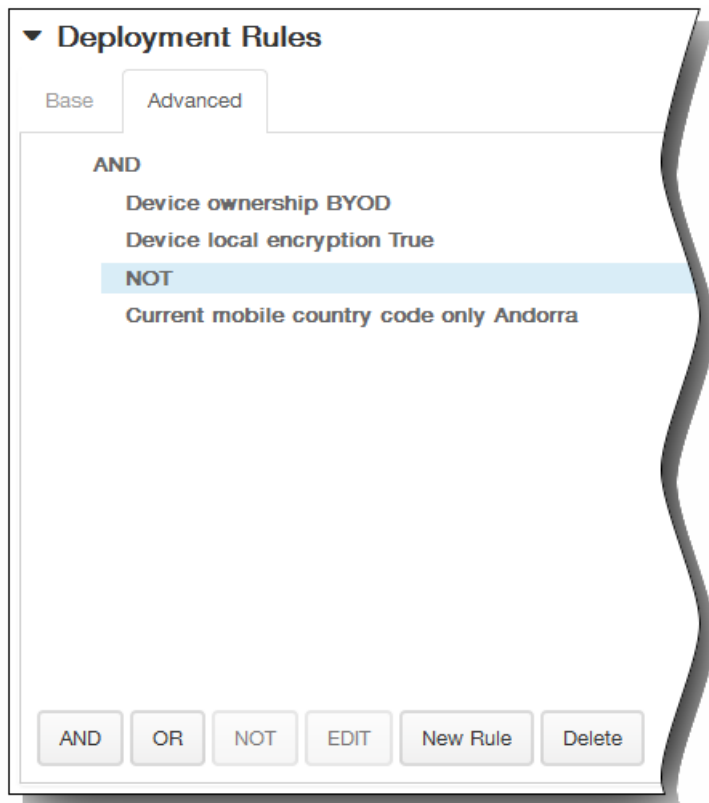


The conditions you chose on the Base tab appear.

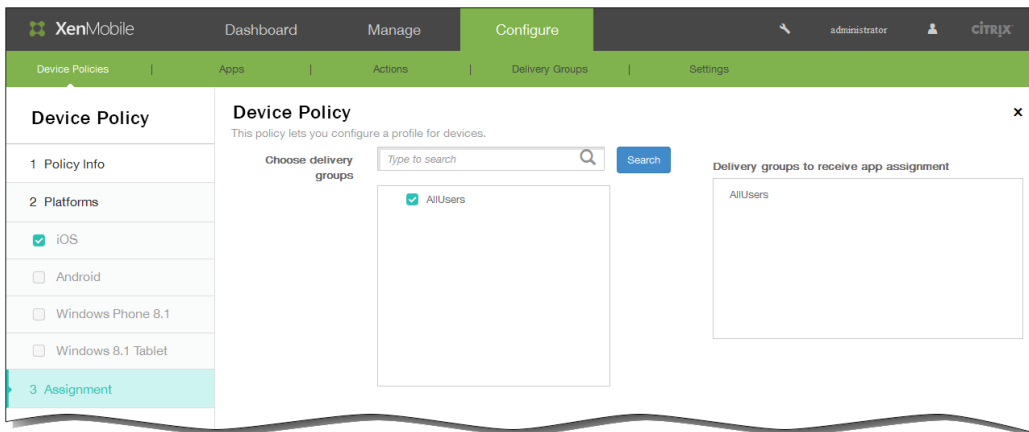
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



12. Click Next. The Web Content Filter Policy assignment page appears.
13. 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.

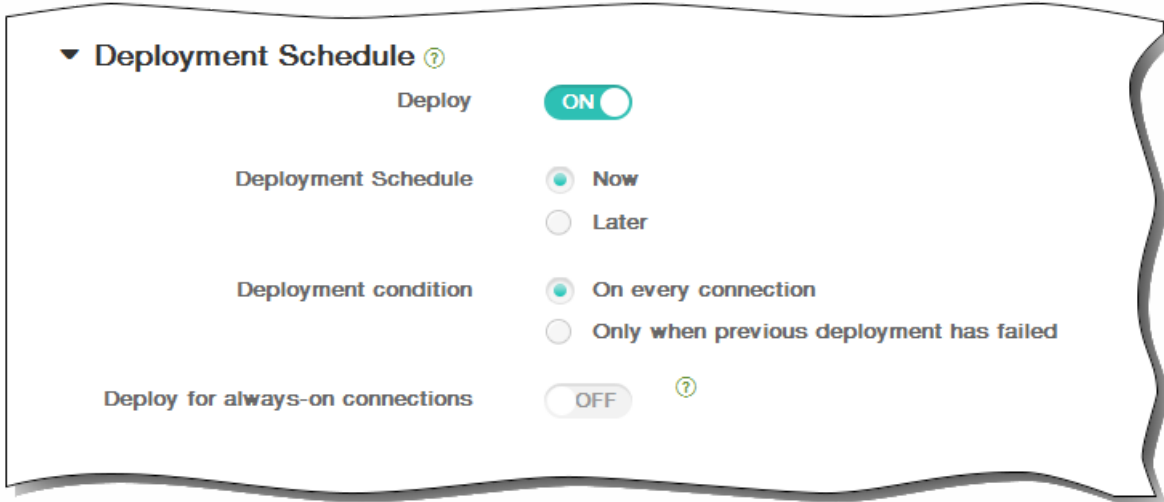


14. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



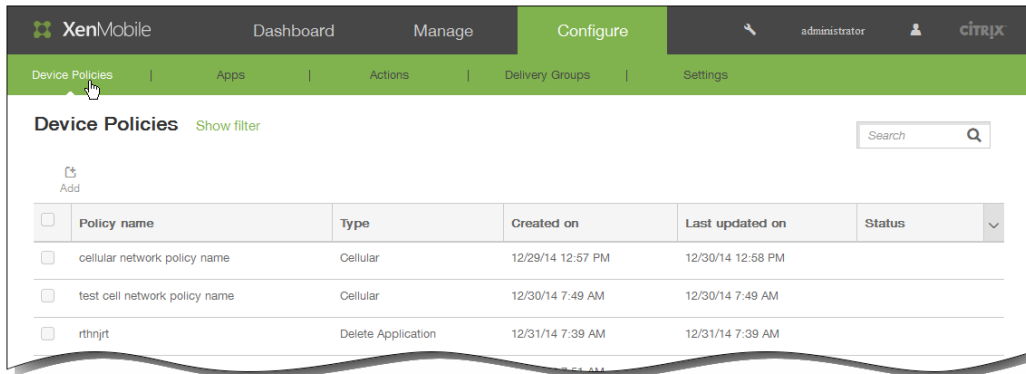
15. Click Save to save the policy.

Samsung browser device policies

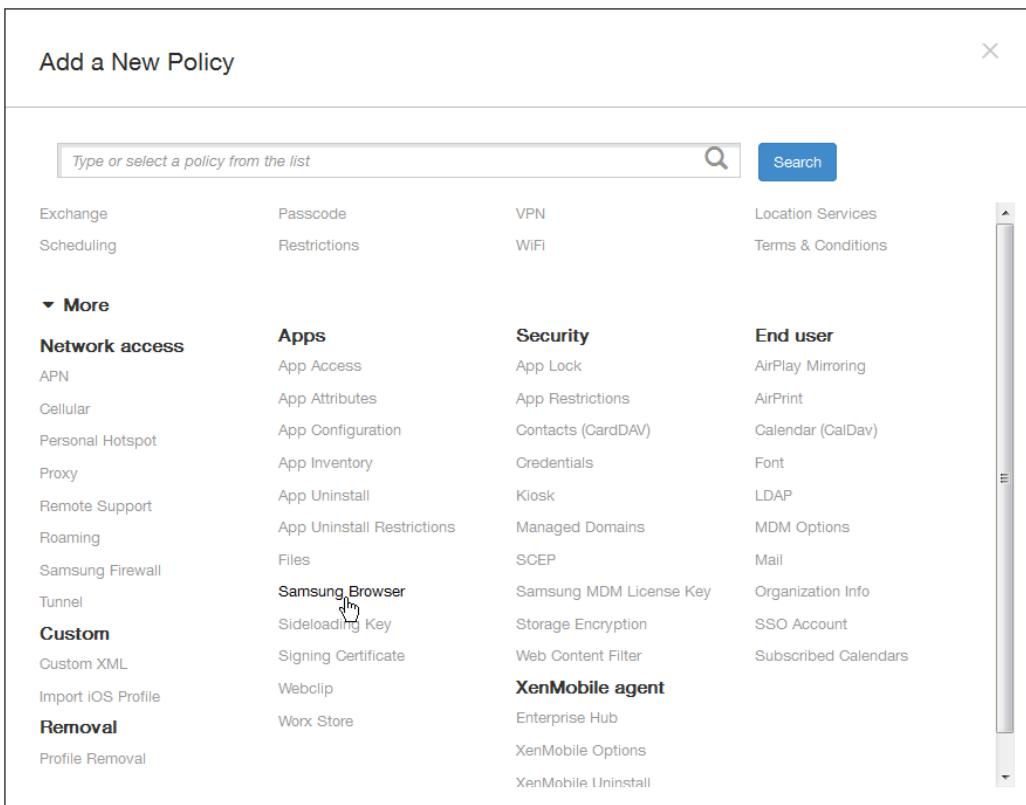
Feb 13, 2015

You can create Samsung browser device policies for Samsung SAFE and Samsung KNOX devices to define whether users' devices can use the browser or to limit which browser functions users' devices can use. You can completely disable the browser, or you can enable or disable pop-ups, Javascript, cookies, autofill, and whether to force fraud warnings.

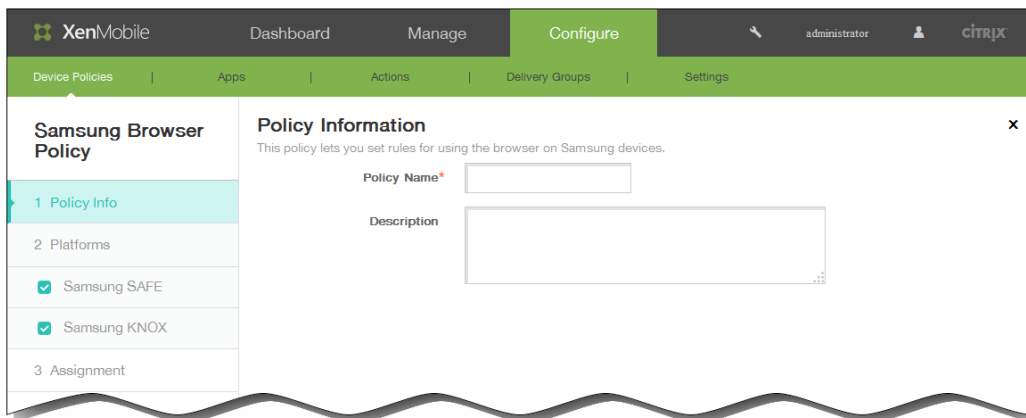
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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



3. Click More, and then under Apps, click Samsung Browser. The Samsung Browser Policy information page appears.

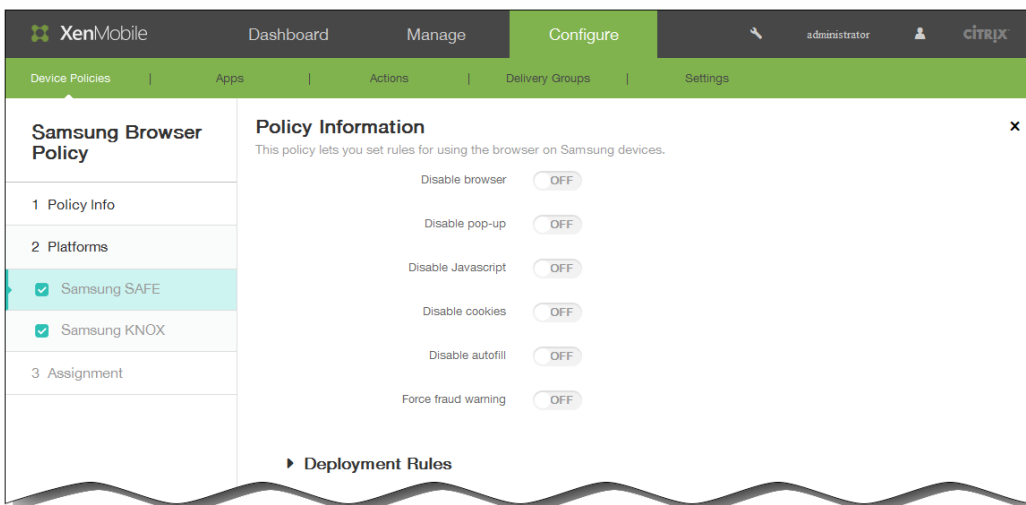


4. In the Policy Information pane, enter the following information:

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

5. Click Next. The Policy Platforms page appears.

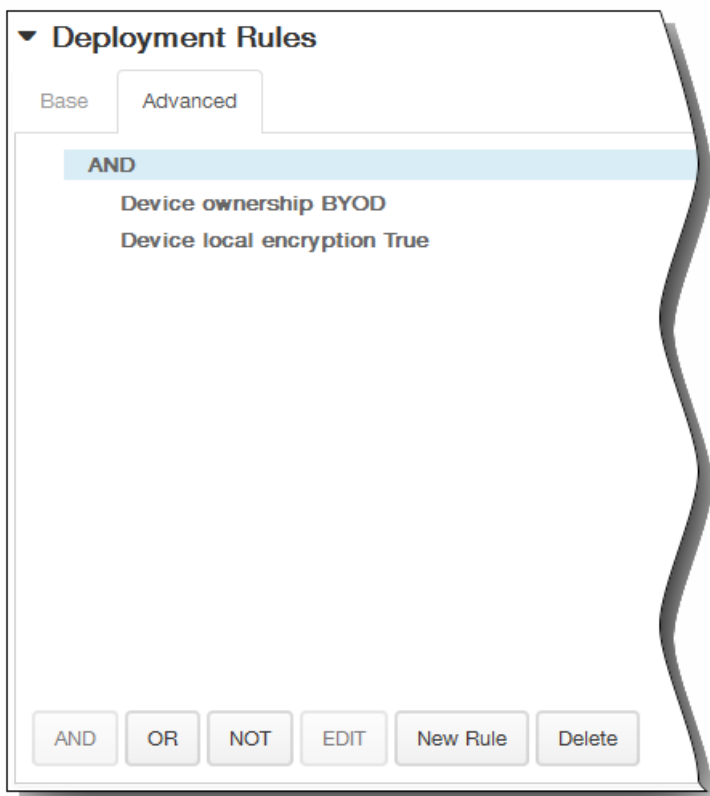
Note: When the Policy Platforms page appears, both platforms are selected and you see the Samsung SAFE platform configuration panel first.



- 6.
7. Under Platforms, select Samsung platforms you want to add. If you are only configuring for one platform, clear the other, then configure the following settings:
 1. Disable browser: Select whether to completely disable the Samsung browser on users's devices. The default is OFF, which lets users use the browser. When you disable the browser, the following options disappear.
 2. Disable pop-up: Select whether to allow pop-up messages on the browser.
 3. Disable Javascript: Select whether to allow Javascript to run on the browser.
 4. Disable cookies: Select whether to allow cookies.
 5. Disable autofill: Select whether to allow users to turn on the browser's autofill function.
 6. Force fraud warning: Select whether to display a warning when users visit a fraudulent or compromised website.
8. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



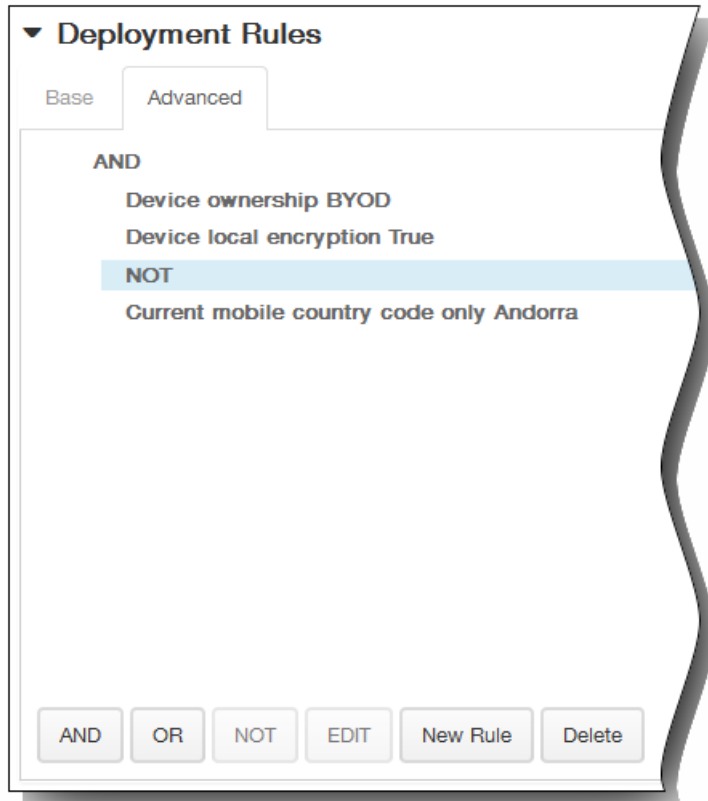
The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

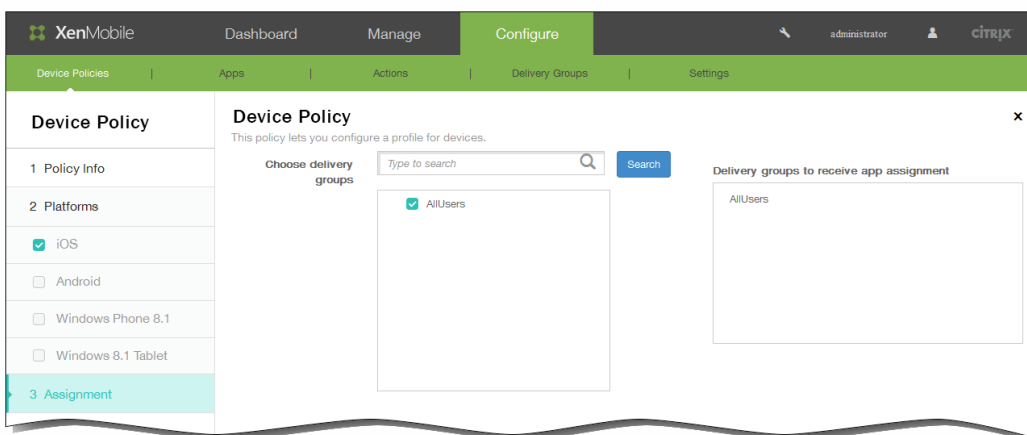
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.

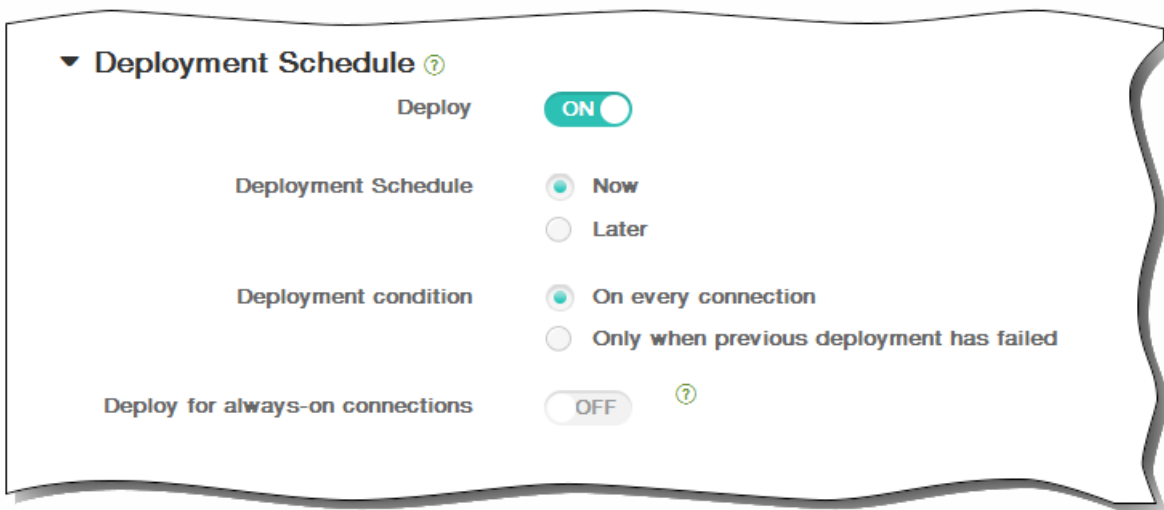


9. Click Next. The Samsung Browser Device Policy page appears.
10. Next to Choose delivery groups, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand Delivery groups to receive app assignment list.



11. Expand Deployment Schedule and then configure the following settings:

1. 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.
2. Next to Deployment schedule, click Now or Later. The default option is Now.
3. If you click Later, click the calendar icon and then select the date and time for deployment.
4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.
Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



12. Click Save to save the policy.

To add a sideloading key device policy for Windows 8.1 tablets

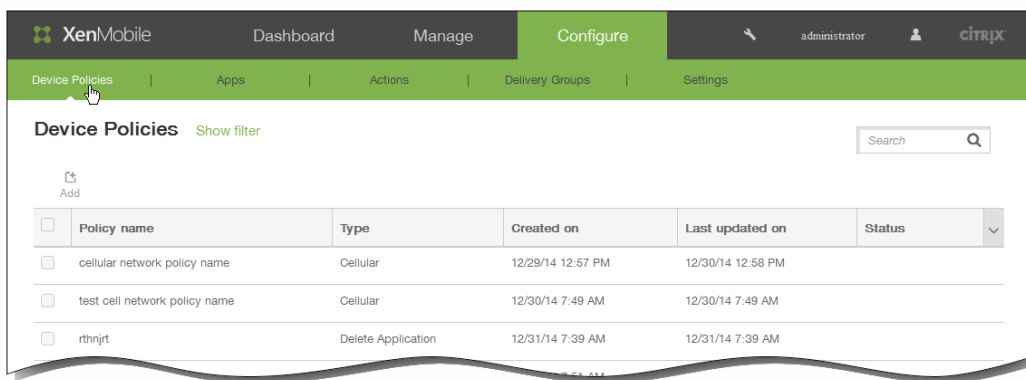
Mar 04, 2015

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.

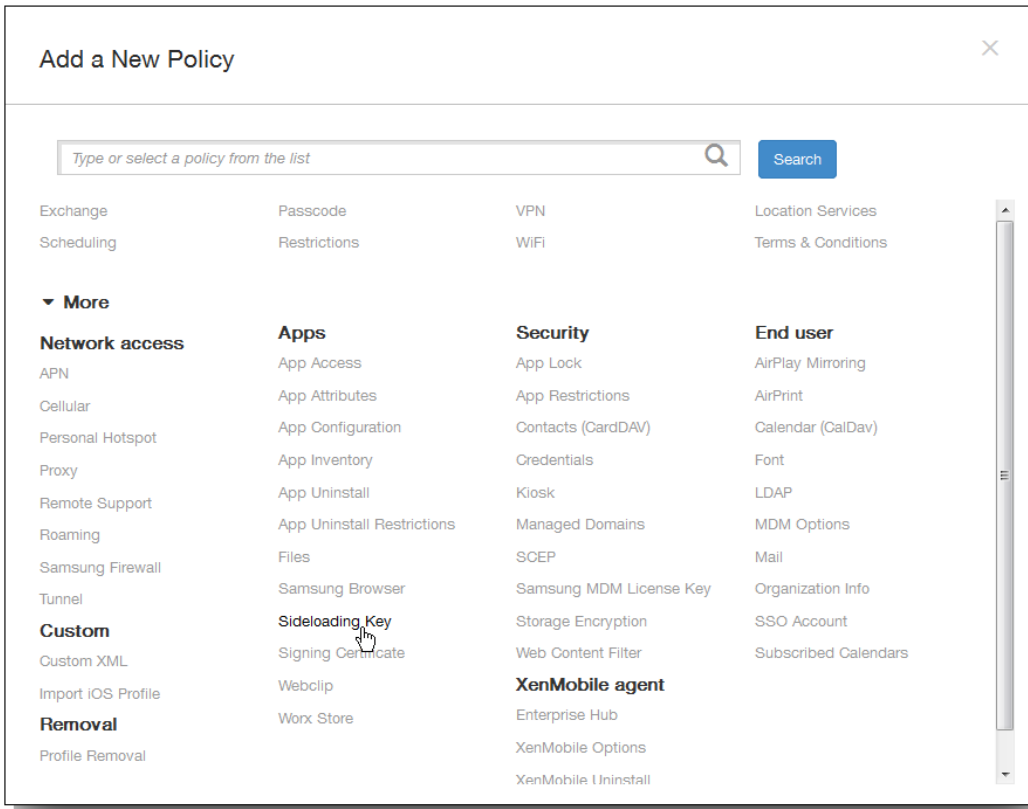
You need the following information before you can create this policy:

- 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

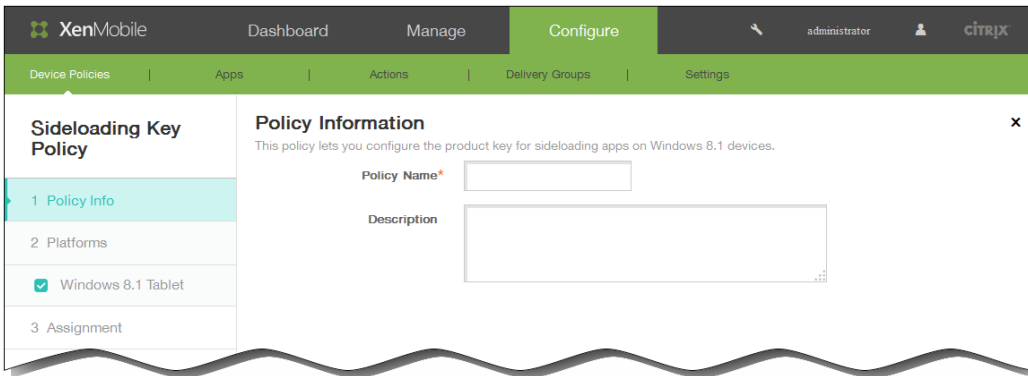
1. In the XenMobile console, click Configure > Device Policies The Device Policies page appears.



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



3. Click More, and then under Apps, click Sideload Key. The Sideload Key Policy page appears.

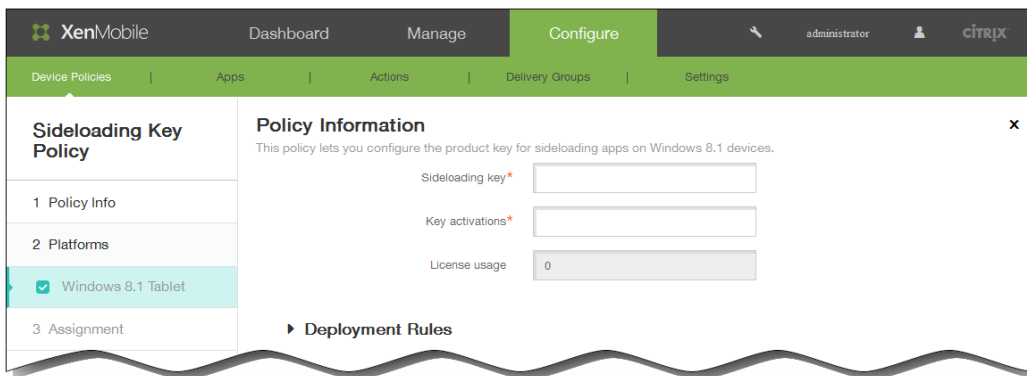


4. In the Policy Information pane, enter the following information:

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

5. Click Next.

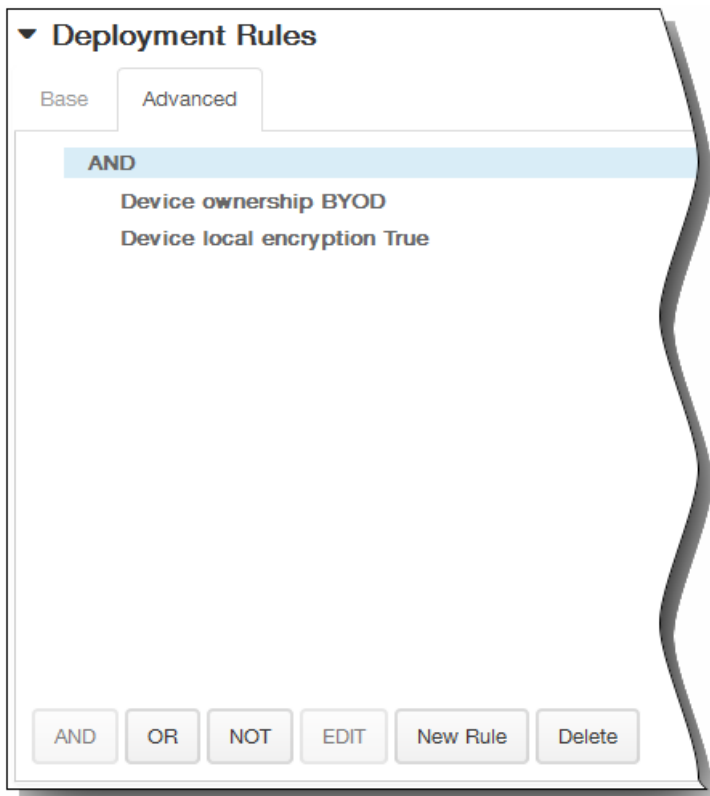
The Windows 8.1 Tablet Platform information page appears.



6. Configure the following settings:
 1. Sideload key: Type the sideloading key that you obtained from the Microsoft Volume Licensing Service Center.
 2. Key activations: Type the key activation you created for the sideloading key.
 3. License usage: XenMobile calculates this value based on the number of enrolled tablets. You cannot change this field.
7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

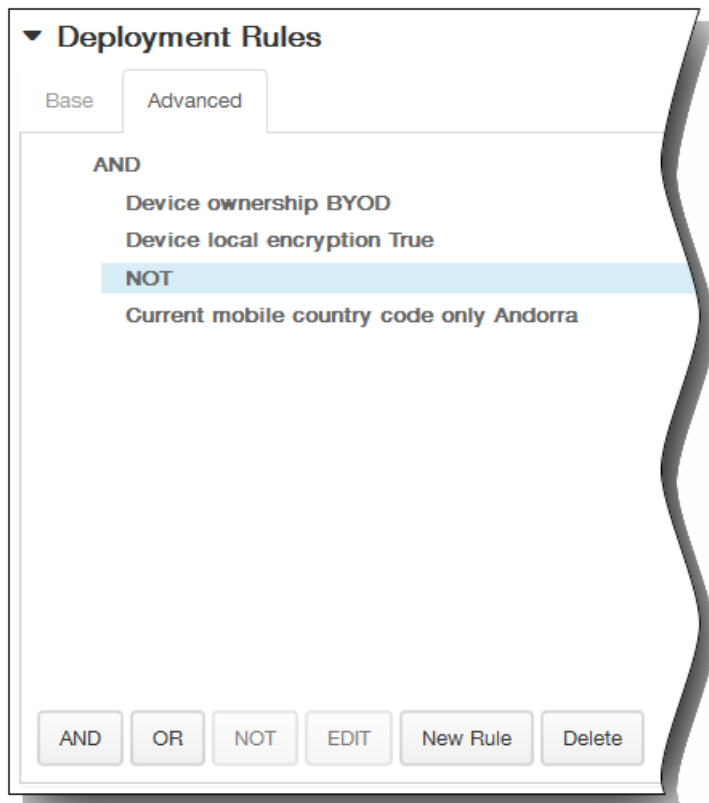


The conditions you chose on the Base tab appear.

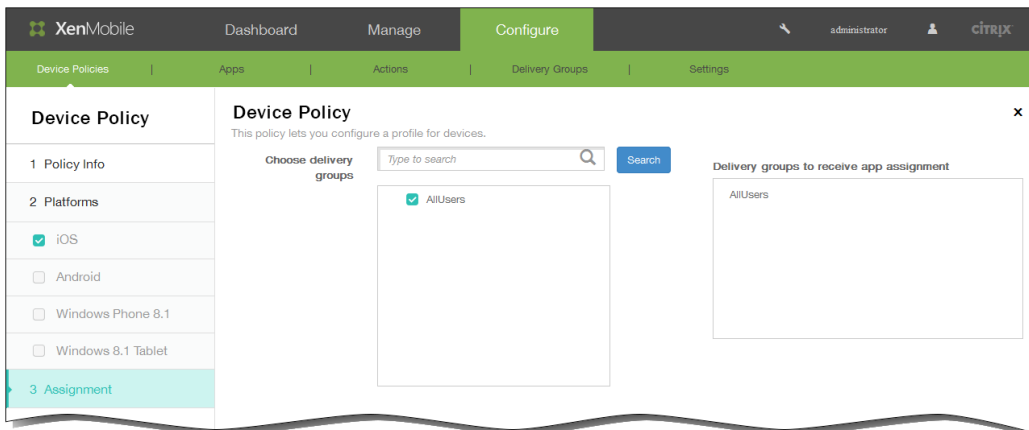
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



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 right-hand Delivery groups to receive app assignment list.

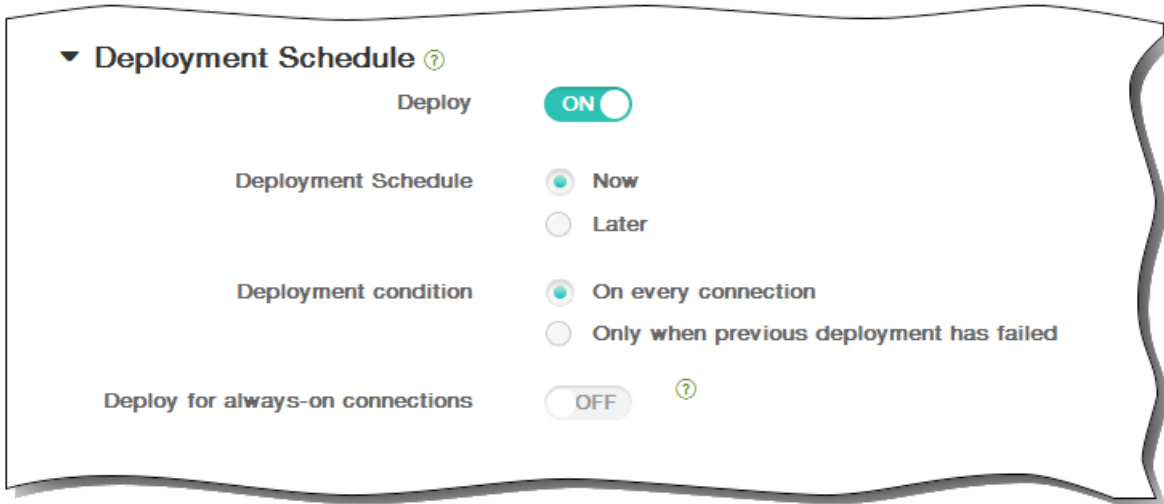


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.

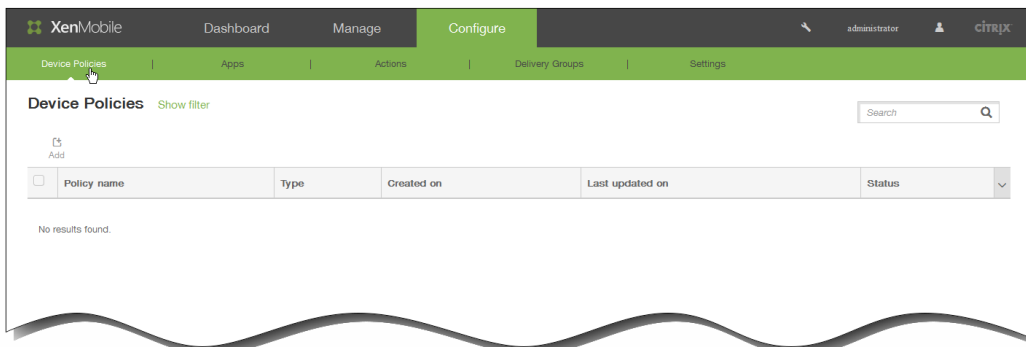


To add a signing certificate device policy for Windows 8.1 tablets

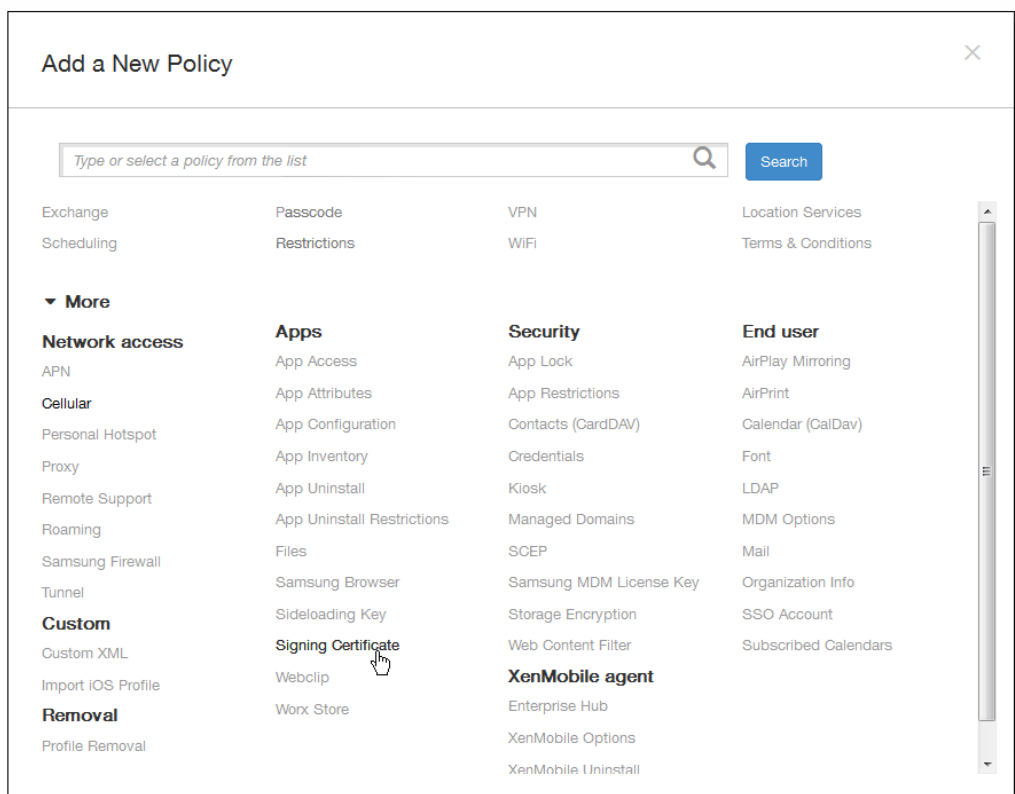
Feb 13, 2015

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 8.1 tablets.

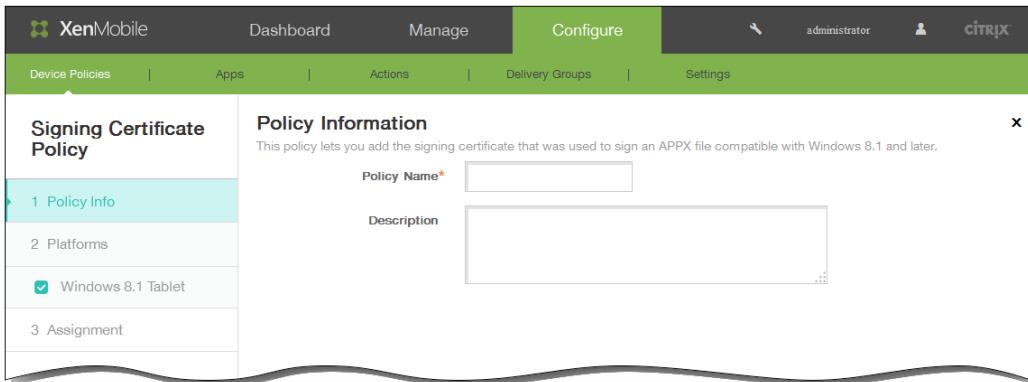
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



2. Click Add to add a new policy. When you click Add, the Add a New Policy dialog box appears.



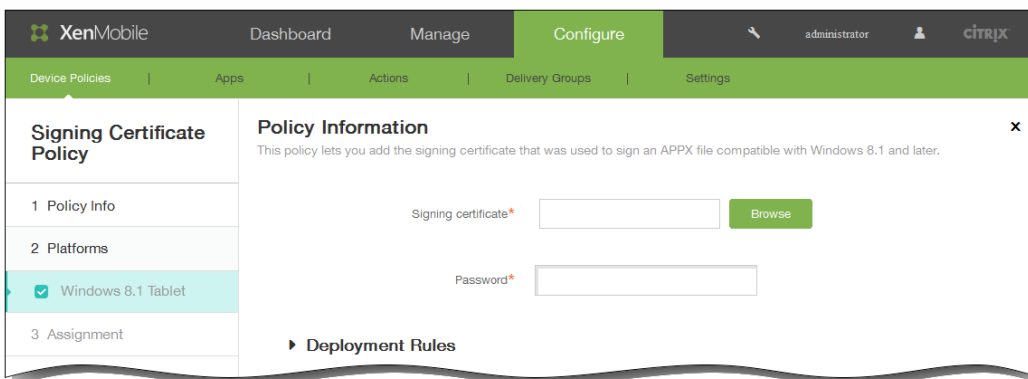
3. Click More and then, under Apps, click Signing Certificate. The Signing Certificate Policy page appears.



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

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

5. Click Next. The Platform Information page appears.



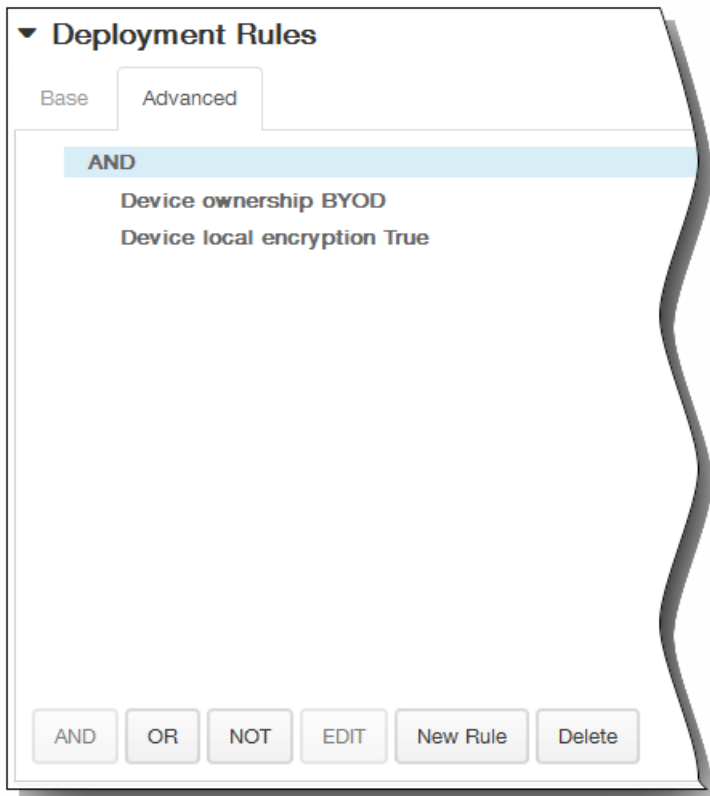
6. Configure the following settings:

1. Signing certificate: Browse to the location of the certificate that was used to sign the APPX file and then select the certificate.
2. Password: Type the password required to access the signing certificate.

7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

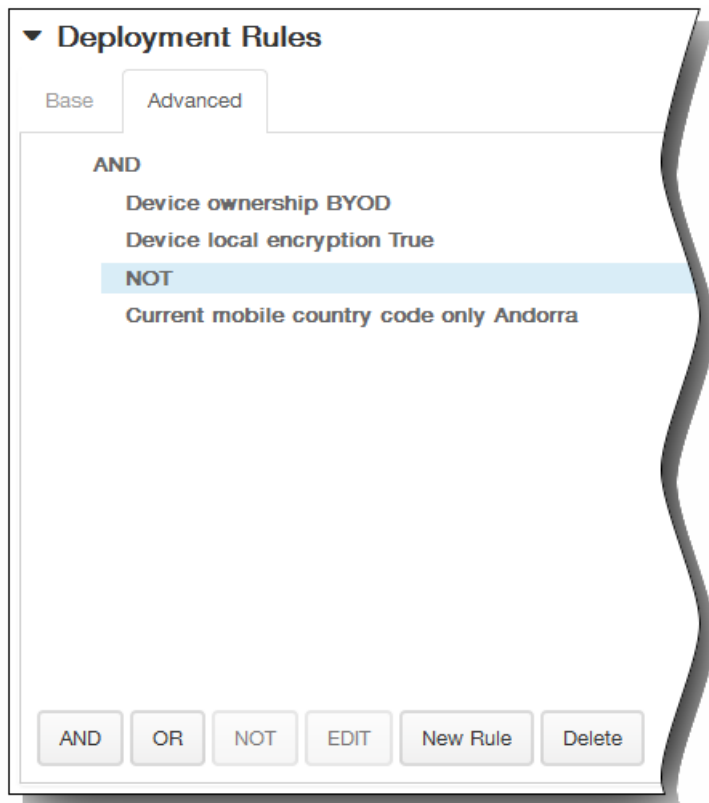


The conditions you chose on the Base tab appear.

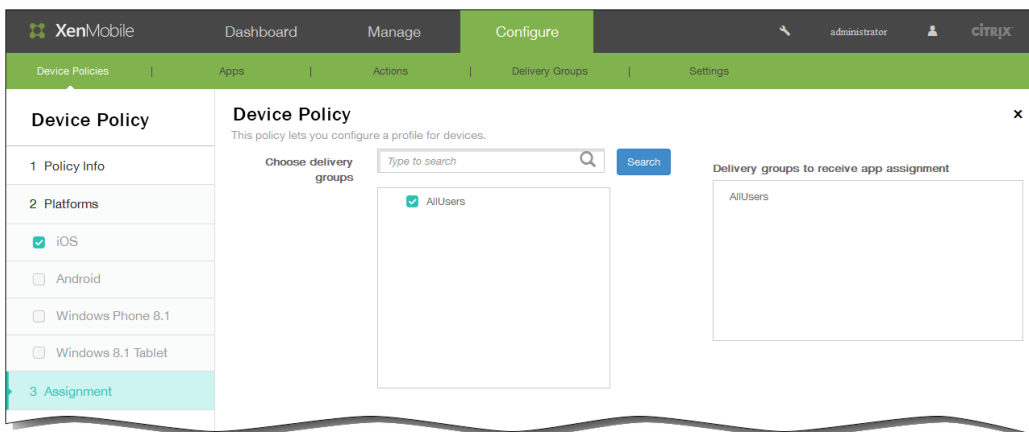
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



8. Click Next. The 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.

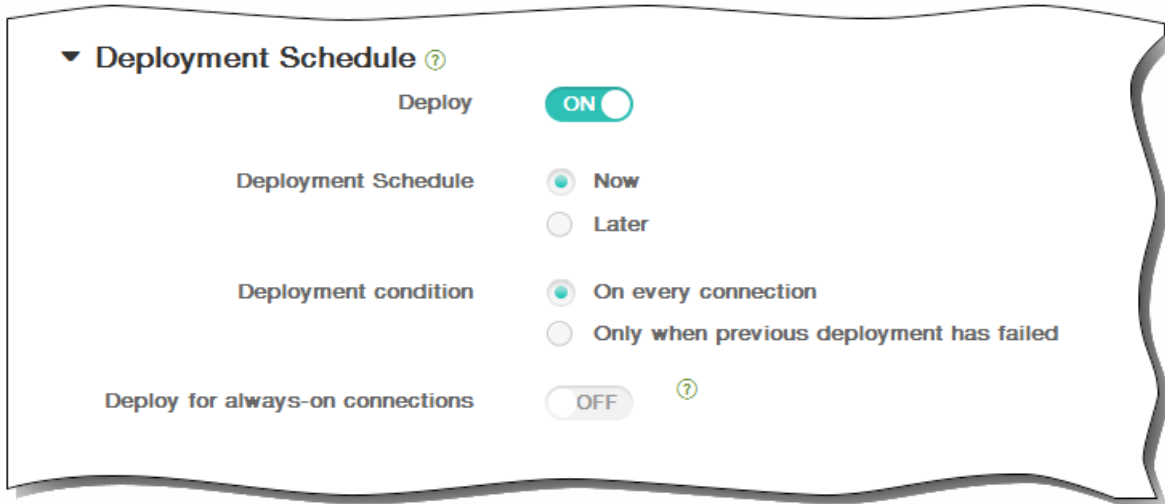


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

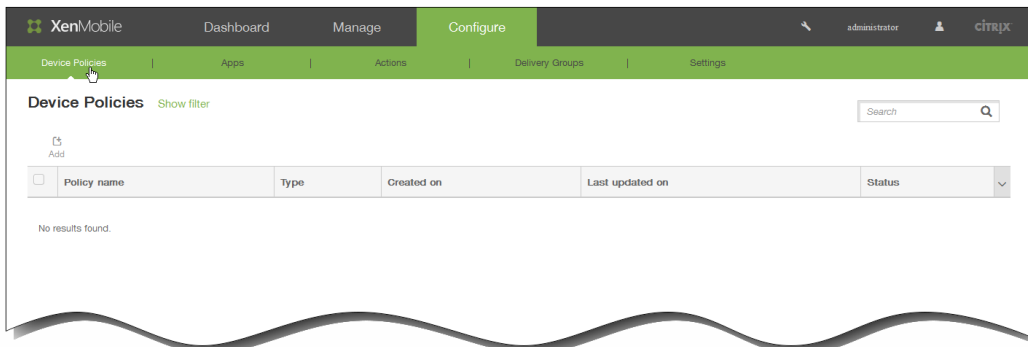
VPN device policies

Apr 10, 2015

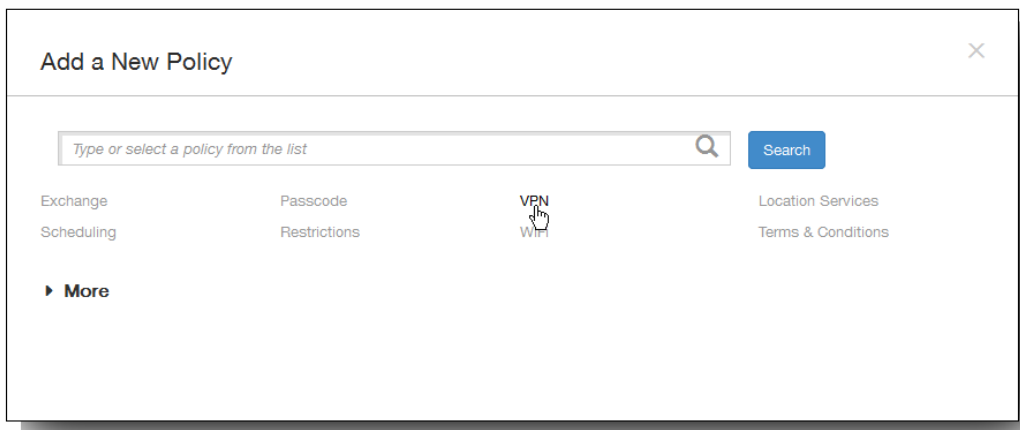
You can add a device policy in XenMobile to configure virtual private network (VPN) settings that enable users' devices to connect securely to corporate resources. You can configure the VPN policy for the following platforms: iOS, Android, Samsung SAFE, Samsung KNOX, Windows 8.1 Tablets, and Amazon. Each platform requires a different set of values, which are described in detail in this article.

To add a VPN device policy

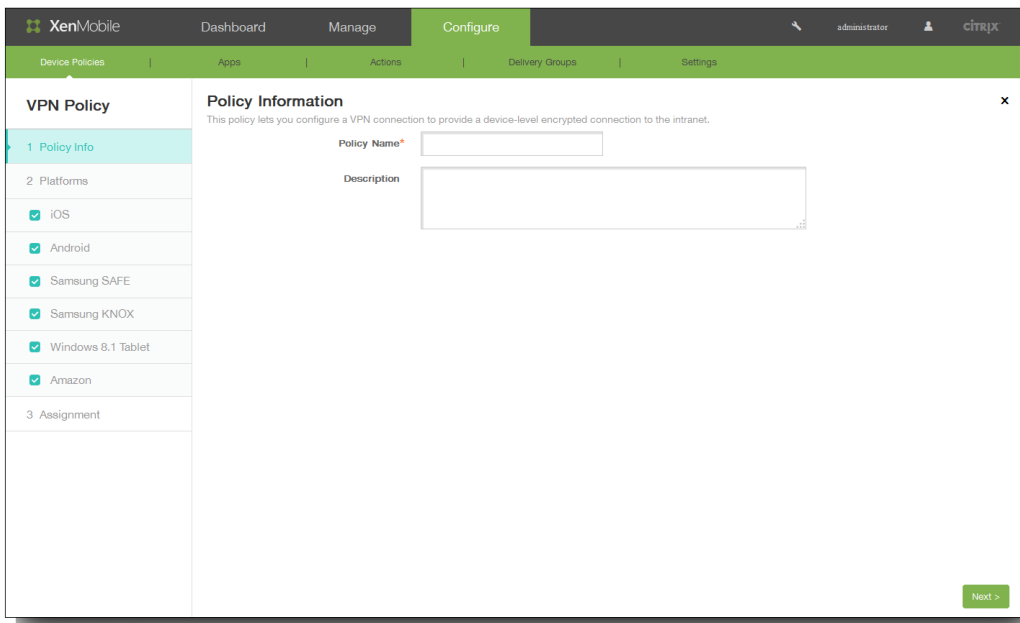
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



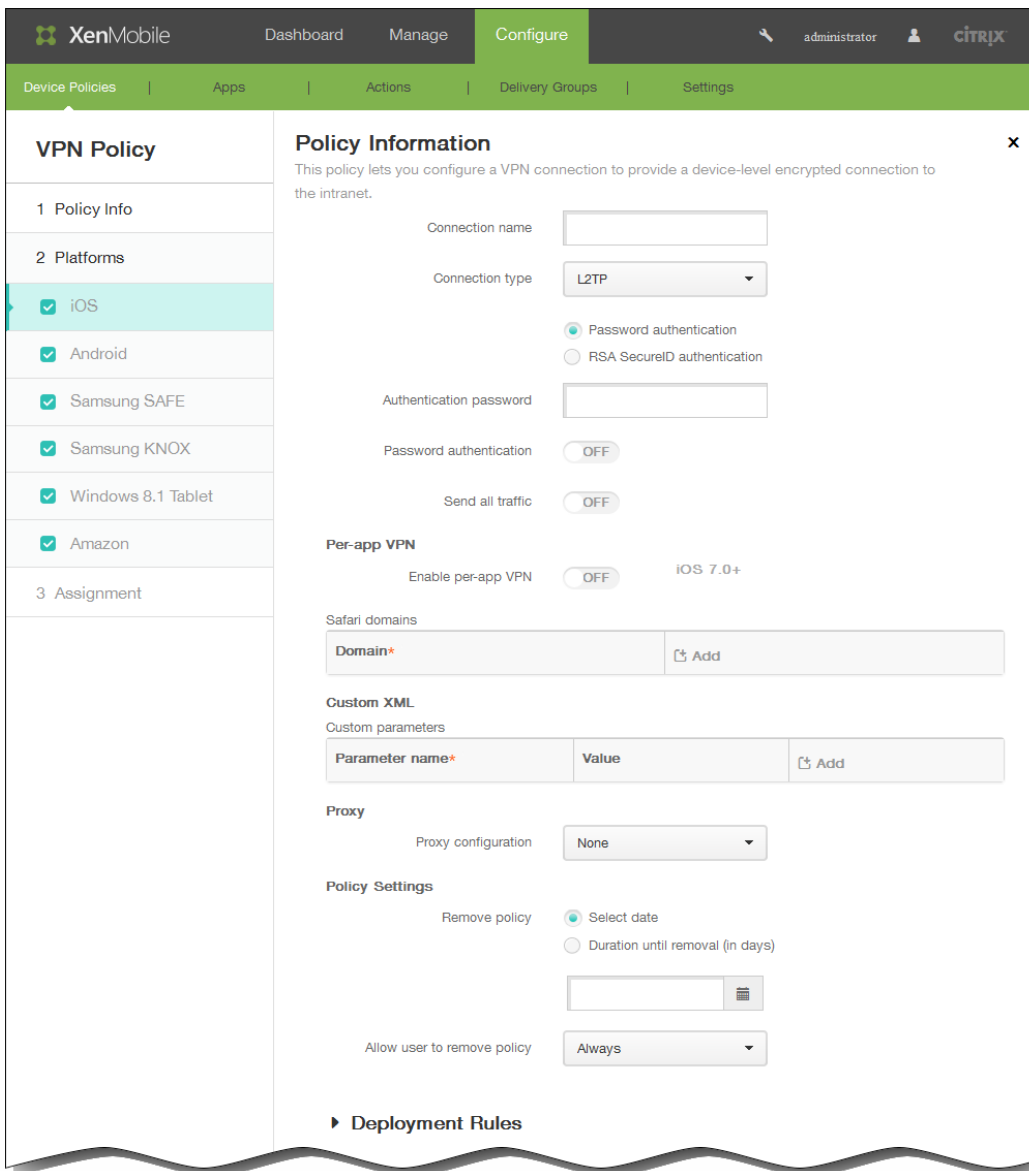
2. Click Add. The Add a New Policy dialog box appears.



3. Click VPN. The VPN Policy page appears.



4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Type an optional description of the policy.
 3. Click Next.
5. Under Platforms, select the platform or platforms you want to add.
If you selected iOS, configure these settings:



1. Connection name: Type a name for the connection.
2. Connection type: In the list, click the protocol to be used for this connection.
 - L2TP — Layer 2 Tunneling Protocol with pre-shared key authentication. This is the default setting.
 - 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.
 - CustomSSL — Custom Secure Socket Layer.

The following sections list the configuration options for each of the preceding connection types.

Configure the following options for the L2TP protocol

1. Select either Password authentication or RSA SecureID authentication.
2. Authentication password: Type an optional authentication password.
3. Password authentication: Select whether password authentication is on or off.
4. Send all traffic: Select whether to send all traffic over the VPN.

Configure the following options for the PPTP protocol

1. Select either Password authentication or RSA SecureID authentication.
2. Authentication password: Type an optional authentication password.
3. Password authentication: Select whether password authentication is on or off.
4. Encryption level: Select the desired encryption level.
5. Send all traffic: Select whether to send all traffic over the VPN.

Configure the following options for the IPSec protocol

1. Authentication password: Type an optional authentication password.
2. Authentication type for the connection: Select the type of authentication for this connection.

The following table lists the options available for each connection type. Each cell lists the default value for an option when an option exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	Password	Certificate	Shared Secret
Group name	-	-	Optional
Password authentication	OFF	OFF	OFF
Identity credential	-	None	-
Prompt for PIN when connecting	-	OFF	-
Enable VPN on demand	-	OFF	-
On Demand Domain	-	Required if Enable VPN on demand = ON	-
Use hybrid authentication	-	-	OFF
Prompt for password	-	-	OFF
Auth password	Optional	-	-

Configure the following options for the Cisco AnyConnect protocol

1. Authentication password: Type an optional authentication password.
2. Group: Type an optional group name.
3. Authentication type for the connection: Select the type of authentication for this connection.

The following table lists the options available for each connection type. Each cell lists the default value for an option when an option exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	Password	Certificate	Shared Secret
Group name	-	-	Optional
Password authentication	OFF	OFF	OFF
Identity credential	-	None	-
Prompt for PIN when connecting	-	OFF	-
Enable VPN on demand	-	OFF	-
On Demand Domain	-	Required if Enable VPN on demand = ON	-
Use hybrid authentication	-	-	OFF
Prompt for password	-	-	OFF
Auth password	Optional	-	-

Configure the following options for the Juniper SSL protocol

1. Authentication password: Type an optional authentication password.
2. Realm: Type an optional realm name.
3. Role: Type an optional role name.
4. Authentication type for the connection: Select the type of authentication for this connection.

The following table lists the options available for each connection type. Each cell lists the default value for an option when an option exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	Password	Certificate	Shared Secret
Group name	-	-	Optional
Password authentication	OFF	OFF	OFF
Identity credential	-	None	-
Prompt for PIN when connecting	-	OFF	-
Enable VPN on demand	-	OFF	-

	Password	Certificate	Shared Secret
On Demand Domain	–	Required if Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Prompt for password	–	–	OFF
Auth password	Optional	–	–

Configure the following options for the F5 SSL protocol

1. Authentication password: Type an optional authentication password.
2. Authentication type for the connection: Select the type of authentication for this connection.

The following table lists the options available for each connection type. Each cell lists the default value for an option when an option exists; otherwise, the cell indicates whether the option is not applicable (–), required, or optional.

	Password	Certificate	Shared Secret
Group name	–	–	Optional
Password authentication	OFF	OFF	OFF
Identity credential	–	None	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Required if Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Prompt for password	–	–	OFF
Auth password	Optional	–	–

Configure the following options for the SonicWALL Mobile Connect protocol

1. Authentication password: Type an optional authentication password.
2. Logon group or domain: Type an optional logon group or domain.
3. Authentication type for the connection: Select the type of authentication for this connection.

The following table lists the options available for each connection type. Each cell lists the default value for an option when an option exists; otherwise, the cell indicates whether the option is not applicable (–), required, or optional.

	Password	Certificate	Shared Secret
Group name	-	-	Optional
Password authentication	OFF	OFF	OFF
Identity credential	-	None	-
Prompt for PIN when connecting	-	OFF	-
Enable VPN on demand	-	OFF	-
On Demand Domain	-	Required if Enable VPN on demand = ON	-
Use hybrid authentication	-	-	OFF
Prompt for password	-	-	OFF
Auth password	Optional	-	-

Configure the following options for the Ariba VIA protocol

1. Authentication password: Type an optional authentication password.
2. Authentication type for the connection: Select the type of authentication for this connection.

The following table lists the options available for each connection type. Each cell lists the default value for an option when an option exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	Password	Certificate	Shared Secret
Group name	-	-	Optional
Password authentication	OFF	OFF	OFF
Identity credential	-	None	-
Prompt for PIN when connecting	-	OFF	-
Enable VPN on demand	-	OFF	-
On Demand Domain	-	Required if Enable VPN on demand = ON	-

	Password	Certificate	Shared Secret
Use hybrid authentication	–	–	OFF
Prompt for password	–	–	OFF
Auth password	Optional	–	–

Configure the following options for the IKEv2 protocol (iOS only)

1. Authentication password: Type an optional authentication password.
2. Password authentication: Select whether password authentication is on or off.
3. Always-on VPN: Select whether the VPN connection is always on.

The following options apply only when Always-on VPN = ON.

4. Server name or IP address: Type the server name or IP address for the VPN server.
5. User Account: Type an optional user account.
6. Authentication type for the connection: Select the type of authentication for this connection.

The following table lists the options available for each connection type. Each cell lists the default value for an option when an option exists; otherwise, the cell indicates whether the option is not applicable (–), required, or optional.

	Password	Certificate	Shared Secret
Group name	–	–	Optional
Shared secret	–	–	Optional
Use hybrid authentication	–	–	OFF
Prompt for password	–	–	OFF
Allow user to disable automatic connection	OFF	OFF	OFF
Local identifier	Required	Required	Required
Remote identifier	Required	Required	Required
Extended Authentication Enabled	OFF	OFF	OFF
Dead Peer Detection Interval	None	None	None
Encryption Algorithm	2DES	2DES	2DES
Integrity Algorithm	SHA1-96	SHA1-96	SHA1-96

	Password	Certificate	Shared Secret
Diffie Hellman Group	2	2	2
LifeTime in Minutes	1440	1440	1440
Voice Mail	Allow traffic via tunnel	Allow traffic via tunnel	Allow traffic via tunnel
Allow traffic from captive web sheet outside the VPN	OFF	OFF	OFF
Allow traffic from all captive networking apps outside the VPN tunnel	OFF	OFF	OFF
AirPrint	Allow traffic via tunnel	Allow traffic via tunnel	Allow traffic via tunnel
Captive networking app bundle identifiers	Optional	Optional	Optional

Configure the following options for the Custom SSL protocol

1. Custom SSL identifier (reverse DNS format): Type the SSL identifier in reverse DNS format.
2. Authentication password: Type an optional authentication password.
3. Password authentication: Select whether password authentication is on or off.
4. Authentication type for the connection: Select the type of authentication for this connection.

The following table lists the options available for each connection type. Each cell lists the default value for an option when an option exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	Password	Certificate	Shared Secret
Group name	-	-	Optional
Prompt for password	-	-	OFF
Auth password	Optional	-	OFF
Identity credential	-	None	-
Prompt for PIN when connecting	-	OFF	-
Enable VPN on demand	-	OFF	-
On Demand Domain	-	Required if Enable VPN on demand = ON	-

Use hybrid authentication	Password	Certificate	-	Shared Secret ^{OFF}
---------------------------	----------	-------------	---	------------------------------

3. Enable per-app VPN: Enable or disable per-app VPN (available for iOS 7 and later). If enabled, enable or disable On-demand match enabled.
4. Safari domains: Click Add to add a Safari domain that lets the app create a secure per-app VPN connection through Safari.
5. Custom XML: Click Add to enter Parameter name and Value pairs to customize the configuration.
6. Proxy configuration: In the list, select how the VPN connection routes through a proxy server and configure any additional options.

The following table lists the options available for Manual and Automatic; None does not require further configuration. Each cell lists the default value for an option when an option exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	Manual	Automatic
Host name or IP address fro the proxy server	Required	-
Port for the proxy server	Required	-
User name	Optional	-
Password	Optional	-
Proxy server URL	-	Required

Policy Settings

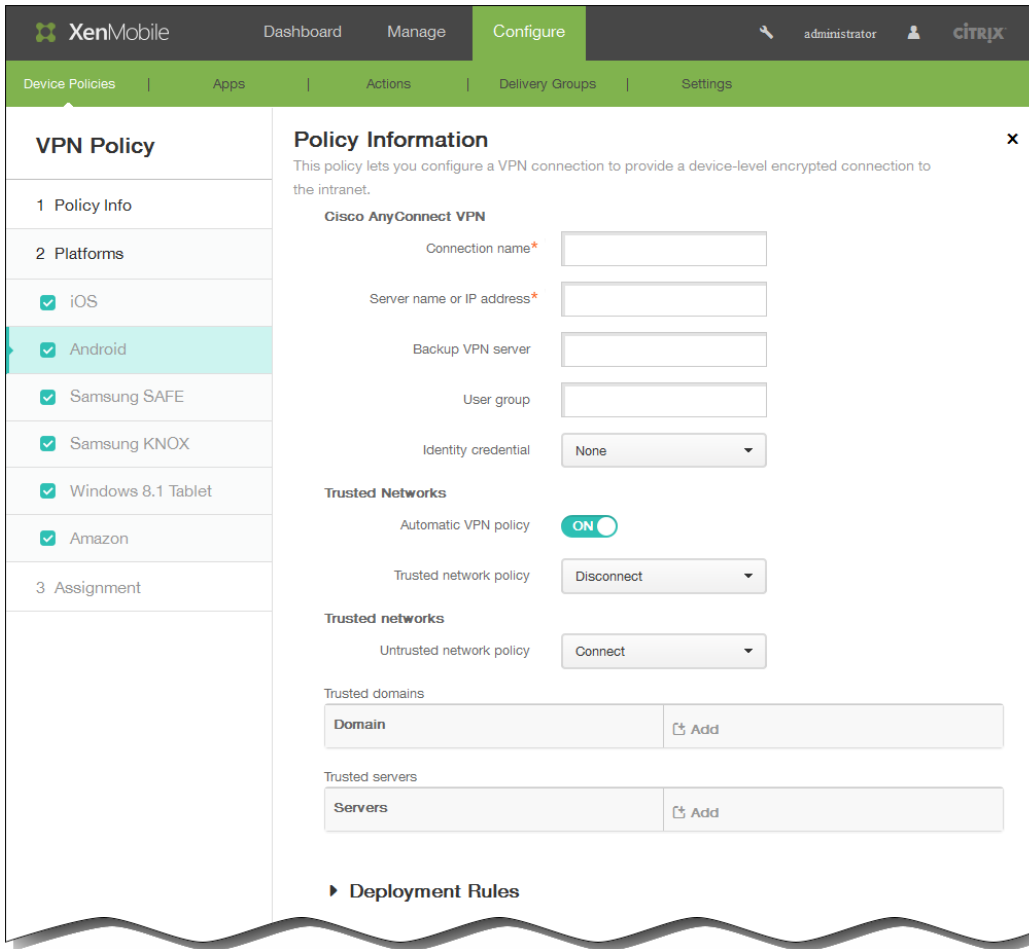
Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy Always

1. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
2. If you click Select date, click the calendar to select the specific date for removal.
3. In the Allow user to remove policy list, click Always, Password required, or Never.
4. If you click Password required, next to Removal password, type the necessary password.

If you selected Android, configure these settings:



1. Connection name: Type a name for the Cisco AnyConnect VPN connection.
2. Server name or IP address: Enter the name or IP address of the VPN server.
3. Backup VPN server: Enter the backup VPN server information.
4. User group: Enter the user group information.
5. Identity credential: In the list, select an identity credential.
6. Automatic VPN policy: Enable or disable this option to set how the VPN reacts to trusted and untrusted networks. If enabled, enter the following information:
 - Trusted network policy: In the list, click the desired policy.
 - Untrusted network policy: In the list, click the desired policy.

If you selected Samsung SAFE, configure these settings:

1. Connection name: Type a name for the connection.
2. Connection type: In the list, click the protocol to be used for this connection:
 - 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.

The following table lists the configuration options for each of the preceding connection types. Each cell lists the default value for an option when a default exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	L2TP with pre-shared key	L2TP with certificate	PPTP	Enterprise				
Host name	Required	Required	Required	Required				
Enable backup server	-	-	-	Off				
Backup VPN server	-	-	-	Required if Enable backup server = On				
User name	Optional	Optional	Optional	Optional				
Password	Optional	Optional	Optional	Optional				
Group name	-	-	-	Optional				
IPsec group ID type	-	-	-	Default				
IKE version	-	-	-	IKEv1				
Authentication method	-	-	-	Certificate (default)	Pre-shared key	Hybrid RSA	EAP MD5	EAP MSCHAPv2
Identity credential	-	Required	-	None	None	-	-	-
CA certificate	-	-	-	Select certificate				
Enable dead peer detection	-	-	-	Off				
Enable default route	-	-	-	Off				
Enable								

smartcard authentication	L2TP with pre-shared key	-	-	Enterprise					Off
Enable user authentication	L2TP-with certificate	-	PPTP	Enterprise					Off
Enable mobile option	-	-	-	Enterprise					Off
Diffie-Hellman group value (key strength)	-	-	-	Enterprise					0
IKE Phase 1 key exchange mode	-	-	-	Enterprise					Main
Perfect forwarded secrecy (PFS) value	-	-	-	Enterprise					Off
Split tunnel type	-	-	-	Enterprise					Auto
SuiteB Type	-	-	-	Enterprise					GCM-128
Pre-shared key	Required	-	-	-	Optional	-	-	-	
Enable encryption	-	-	Off	-	-	-	-	-	

3. Forward routes: Add any optional forwarding routes if your corporate VPN server supports multiple route tables. If you selected Samsung KNOX, configure these settings:

VPN Policy

Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet.

Connection name*

Host name*

Enable backup server OFF

User name

Password

Group name

IPsec group ID type

IKE version

Authentication method

Identity credential

CA certificate

Enable dead peer detection OFF

Enable default route OFF

Enable smartcard authentication OFF

Enable user authentication OFF

Enable mobile option OFF

Diffie-Hellman group value (key strength)

IKE Phase 1 key exchange mode

Perfect forward secrecy (PFS) value OFF

Split tunnel type

SuiteB Type

Forward routes

Forward route

► **Deployment Rules**

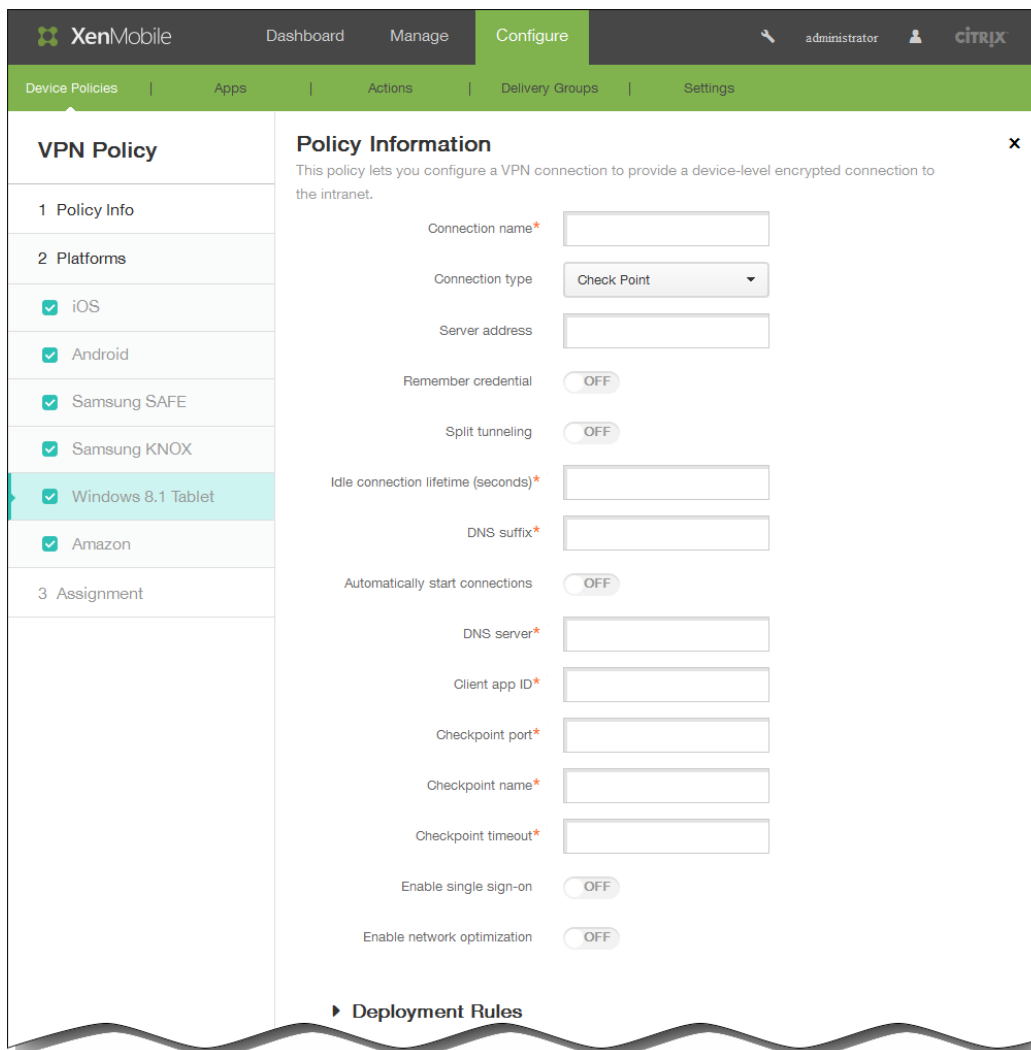
1. Connection name: Enter a name for the connection.
2. Host name: Enter the host name.
3. Enable backup server: Select whether to enable a backup VPN server. An additional field appears when you select this option. Enter the backup server information.
4. User name: Enter an optional user name.
5. Password: Enter an optional password.
6. Group name: Enter an optional group name.

7. IPsec group ID type: In the list, click the IPsec group ID type.
8. IKE version: In the list, click the IKE version.
9. Authentication method: In the list, click the authentication method.
 - Certificate — Certificate-based authentication
 - Pre-shared key — Authentication using a pre-shared key
 - Hybrid RSA — Hybrid authentication using RSA certificates
 - EAP MD5 — Extensible Authentication Protocol using MD5 hash function
 - EAP MSCHAPv2 — Extensible Authentication Protocol with Microsoft Challenge Handshake Authentication Protocol version 2

The following table lists the configuration options for each of the preceding connection types. Each cell lists the default value for an option when a default exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	Certificate	Pre-shared key	Hybrid RSA	EAP MD5	EAP MSCHAPv2
Pre-shared key	-	Required	-	-	-
Identity credential	None	None	-	-	-
CA certificate	Required	Required	Required	Required	Required
Enable dead peer detection	OFF	OFF	OFF	OFF	OFF
Enable default route	OFF	OFF	OFF	OFF	OFF
Enable smartcard authentication	OFF	OFF	OFF	OFF	OFF
Enable user authentication	OFF	OFF	OFF	OFF	OFF
Enable mobile option	OFF	OFF	OFF	OFF	OFF
Diffie-Hellman group value (key strength)	0	0	0	0	0
IKE Phase 1 key exchange mode	Main	Main	Main	Main	Main
Perfect forward secrecy (PFS) value	OFF	OFF	OFF	OFF	OFF
Split tunnel type	Auto	Auto	Auto	Auto	Auto
SuiteB Type	GCM-128	GCM-128	GCM-128	GCM-128	GCM-128

10. Forward route: Add any optional forwarding routes to your corporate VPN server supports multiple route tables. If you selected Windows 8.1 tablet, configure these settings:
- | | | | | |
|-----------|----------------|------------|---------|--------------|
| Configure | Pre-shared key | Hybrid RSA | EAP MD5 | EAP MSCHAPv2 |
|-----------|----------------|------------|---------|--------------|



1. Connection name: Enter a name for the connection.
2. Connection type: In the list, click the connection type.
 - SonicWALL — Dell unified VPN client for Windows
 - Check Point — Check Point Software Technologies SSL VPN client
 - Juniper — Juniper Networks SSL VPN client
 - Microsoft — Microsoft VPN client
 - F5 — F5 Networks SSL VPN client

The following table lists the configuration options for each of the preceding connection types. Each cell lists the default value for an option when a default exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	SonicWALL	Check Point	Juniper	Microsoft	F5
Server address	Optional	Optional	Optional	Optional	Optional

	SonicWALL	Check Point	Juniper	Microsoft	F5
Remember credential	OFF	OFF	OFF	OFF	OFF
Split tunneling	OFF	OFF	OFF	OFF	OFF
Idle connection lifetime (seconds)	Required	Required	Required	Required	Required
DNS suffix	Required	Required	Required	Required	Required
Automatically start connections	OFF	OFF	OFF	-	OFF
DNS server	Required	Required	Required	-	Required
Client app ID	Required	Required	Required	-	Required
Checkpoint port	-	Required	-	-	-
Checkpoint name	-	Required	-	-	-
Checkpoint timeout	-	Required	-	-	-
Enable single sign-on	-	OFF	-	-	-
Enable network optimization	-	OFF	-	-	-
Enable compression	OFF	-	-	-	-
Require smart card certificate	OFF	-	-	-	-
Automatically select client certificate	OFF	-	-	-	-
Enable client logging	OFF	-	-	-	-
Enable packet capture	OFF	-	-	-	-
Use single sign-on credentials	-	-	OFF	-	-
Make connection available to all users	-	-	-	OFF	-

Tunneling protocol	SonicWALL	Check Point	Juniper	Required Microsoft	F5 -
Authentication method	-	-	-	Required	-
VPN server name	-	-	-	Required	-
VPN friendly name	-	-	-	Required	-
Automatically detect settings	-	-	-	OFF	-
Bypass proxy server for local addresses	-	-	-	OFF	-
Automatically use Windows credentials	-	-	-	OFF	-
Client certificate issuer	-	-	-	-	Required

If you selected Amazon, configure these settings:

The screenshot shows the XenMobile configuration interface for a VPN Policy. The left sidebar lists the policy configuration steps: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', several options are checked, including 'Amazon'. The main area displays the 'Policy Information' for the selected platform, with a description: 'This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet.' The configuration fields are as follows:

- Connection name*:
- Connection type: L2TP PSK (dropdown)
- Server address*:
- User name:
- Password:
- L2TP Secret:
- IPSec Identifier:
- IPSec pre-shared key:
- DNS search domains:
- DNS servers:
- Forwarding routes:

At the bottom of the configuration area, there is a section for 'Deployment Rules' with a right-pointing arrow.

1. Connection name: Enter a name for the connection.

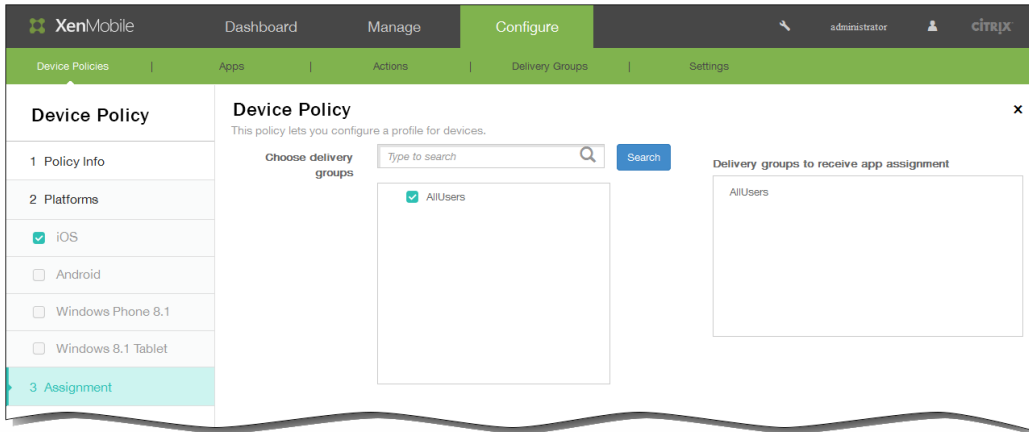
2. Connection type: Click the connection type.

- L2TP PSK — Layer 2 Tunneling Protocol with pre-shared key authentication
- L2TP RSA — Layer 2 Tunneling Protocol with RSA authentication
- IPSEC XAUTH PSK — Internet Protocol Security with pre-shared key and extended authentication
- IPSEC XAUTH RSA — Internet Protocol Security with RSA and extended authentication
- IPSEC HYBRID RSA — Internet Protocol Security with hybrid RSA authentication
- PPTP — Point-to-Point Tunneling

The following table lists the configuration options for each of the preceding connection types. Each cell lists the default value for an option when a default exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	L2TP PSK	L2TP RSA	IPSEC XAUTH PSK	IPSEC XAUTH RSA	IPSEC HYBRID RSA	PPTP
Server address	Required	Required	Required	Required	Required	Required
User name	Optional	Optional	Optional	Optional	Optional	Optional
Password	Optional	Optional	Optional	Optional	Optional	Optional
L2TP Secret	Optional	Optional	-	-	-	-
IPSec identifier	Optional	-	Optional	-	-	-
IPSec pre-shared key	Optional	-	Optional	-	-	-
DNS search domains	Optional	Optional	Optional	Optional	Optional	Optional
DNS servers	Optional	Optional	Optional	Optional	Optional	Optional
Forwarding routes	Optional	Optional	Optional	Optional	Optional	Optional
Server certificate	-	Select	-	Select	Select	-
CA certificate	-	Select	-	Select	Select	-
Identity credential	-	Required	-	Required	-	-
PPP encryption (MMPE)	-	-	-	-	-	OFF

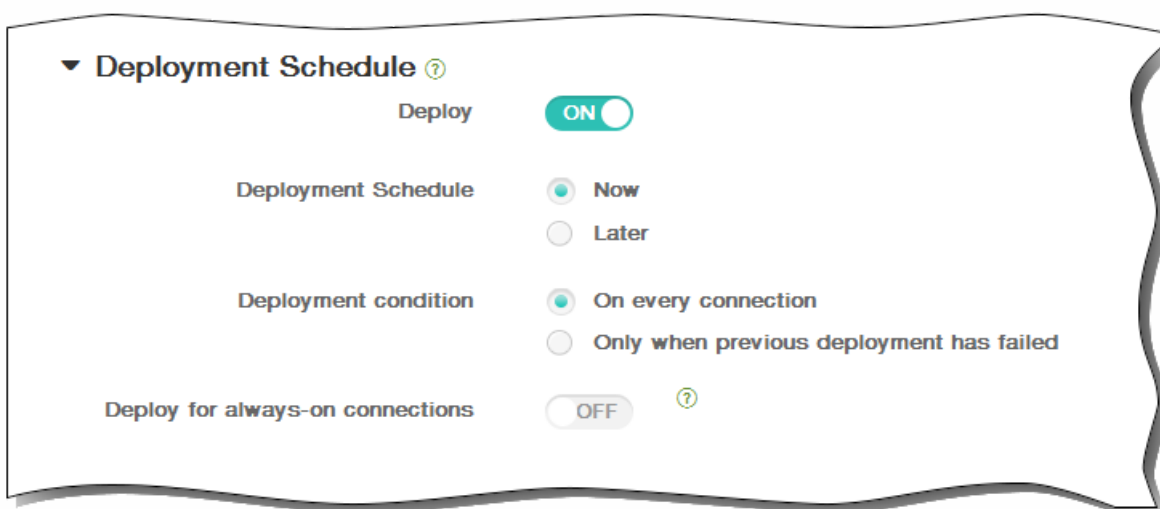
3. Forwarding route: Add any optional forwarding routes if your corporate VPN server supports multiple route tables.
6. After you finish configuring the settings for one or more platforms and then click Next, the VPN Policy assignment page appears.
7. Next to Choose delivery groups, type to find a delivery 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. Expand Deployment Schedule and then configure the following settings:
 1. 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.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



9. Click Save to save the policy.

WiFi device policies

Oct 11, 2016

You create new or edit existing WiFi device policies in XenMobile by using the Device Policies page of the XenMobile Console. WiFi policies let you manage how users connect their devices to WiFi networks by defining network names and types, authentication and security policies, whether to use proxy servers, and other WiFi-related details consistently for all users on device platforms you select.

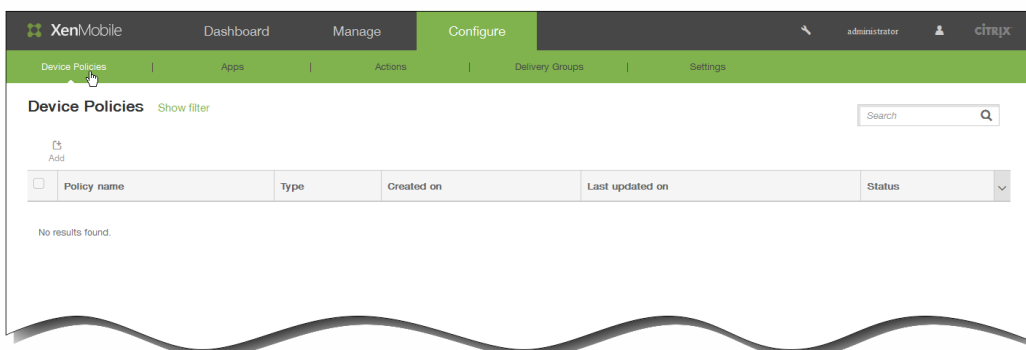
You can configure WiFi settings for users for the following platforms: iOS, Android, Windows Phone 8.1, and Windows 8.1 tablet. Each platform requires a different set of values, which are described in detail in this article.

Important: Before you create a new policy, be sure you complete these steps:

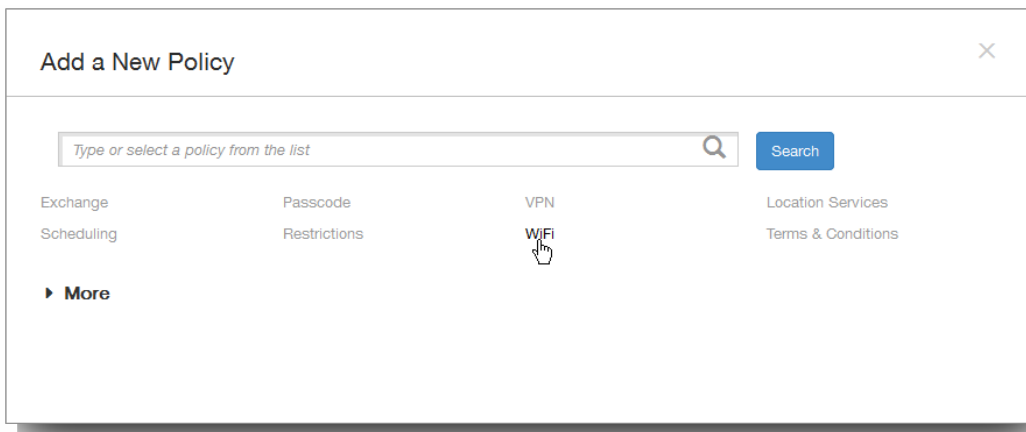
- Create any deployment groups you plan to use.
- Know the network name and type.
- Know any authentication or security types you plan to use.
- Know any proxy server information you may need.
- Install any necessary CA certificates.
- Have any necessary shared keys.

To create a new WiFi device policy

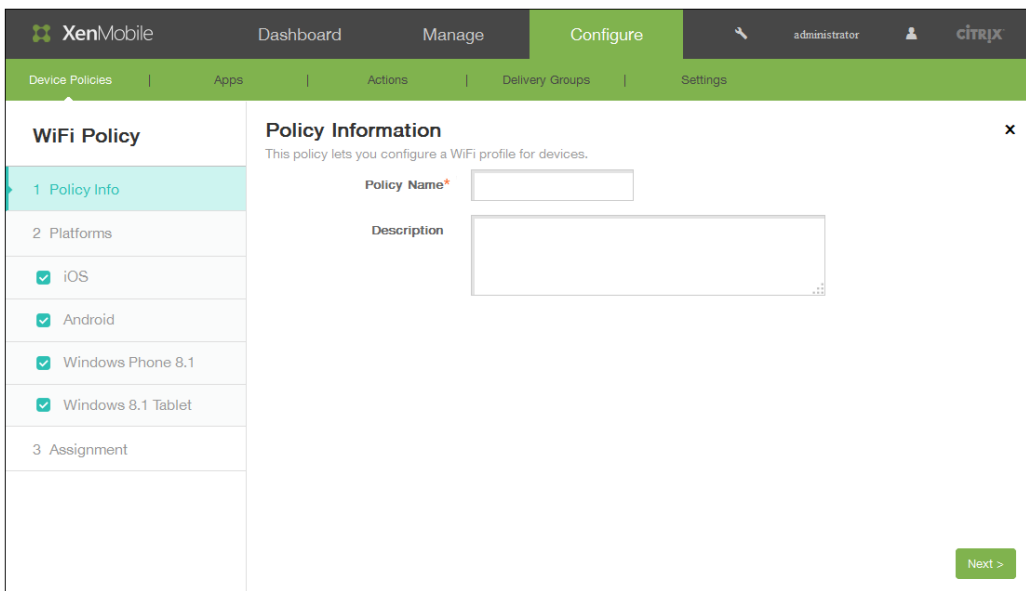
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



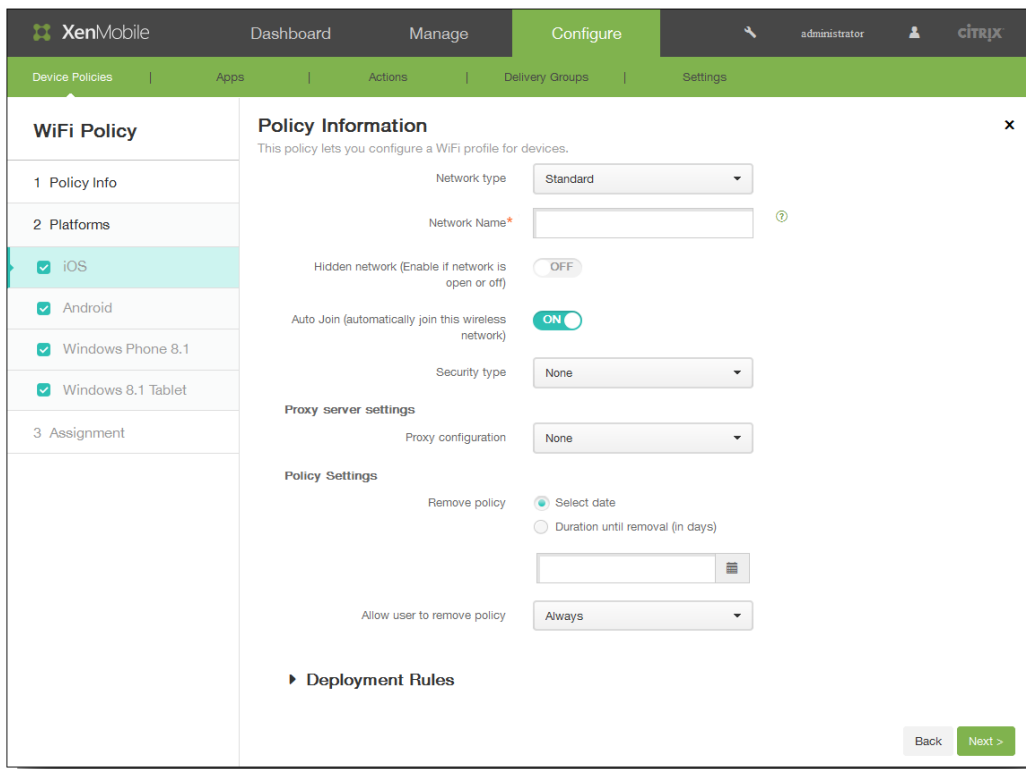
2. Click Add to add a new policy. The Add a New Policy dialog box appears. Click WiFi.



The WiFi Policy page appears.



3. In the Policy Information pane the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Type an optional description of the policy.
 3. Click Next
4. Under Platforms, select the platform or platforms you want to add or modify. Clear those platforms for which you do not want to configure.
If you selected iOS, configure these settings:



1. In the Network type list, click the network type you plan to use.
2. If you clicked Standard or Legacy Hotspot, enter the following information:
 1. Network Name: Type the SSID that is seen in the device's list of available networks.
 2. Hidden network (enable if network is open or off): Select whether the network is hidden.
 3. Auto Join: Select whether the network is joined automatically.
3. If you clicked Hotspot 2.0, enter the following information, which is listed after the Security type information:

Note: These options apply only to iOS 7.0 and later.

 1. Displayed operator name: Type the operator name to display.
 2. Domain name: Type the domain name.
 3. Allow connecting to roaming partner networks: Select whether to allow devices to connect to roaming partner networks.
 4. Roaming Consortium Organization Identifiers (OI): Optionally, add Roaming Consortium OIs.
 5. Network Access Identifier (NAI) realm names: Optionally, add NAI realm names.
 6. Mobile Country Codes (MCCs) and Mobile Network Configurations (MNCs): Optionally, add MCCs and MNCs.
4. Security type: In the list, click the type of security to use with the WiFi connection.
 - None
 - WEP
 - WPA/WPA2 Personal
 - Any (Personal)
 - WEP Enterprise
 - WPA/WPA2 Enterprise
 - Any (Enterprise)

The following table lists the options to be configured for each of the preceding connection types. Each cell lists the default value for an option when a default exists; otherwise, the cell indicates whether the option is not applicable

(-), required, or optional.

	None	WEP	WPA/WPA2 Personal	Any (Personal)	WEP Enterprise	WPA/WPA2 Enterprise	Any (Enterprise)
Password	-	Optional	Optional	Optional	-	-	-
TLS	-	-	-	-	OFF	OFF	OFF
TTLS	-	-	-	-	OFF	OFF	OFF
LEAP	-	-	-	-	OFF	OFF	OFF
PEAP	-	-	-	-	OFF	OFF	OFF
EAP-FAST	-	-	-	-	OFF	OFF	OFF
EAP-SIM	-	-	-	-	OFF	OFF	OFF
Inner authentication (TTLS)	-	-	-	-	MSCHAPv2 (when TTLS = On)	MSCHAPv2 (when TTLS = On)	MSCHAPv2 (when TTLS = On)
Outer identity	-	-	-	-	Optional (when PEAP, TTLS, or EAP-FAST = On)	Optional (when PEAP, TTLS, or EAP-FAST = On)	Optional (when PEAP, TTLS, or EAP-FAST = On)
Use PAC	-	-	-	-	OFF	OFF	OFF
Provisioning PAC	-	-	-	-	OFF (when Use PAC = On)	OFF (when Use PAC = On)	OFF (when Use PAC = On)
Provisioning PAC anonymously	-	-	-	-	OFF (when Provisioning PAC = On)	OFF (when Provisioning PAC = On)	OFF (when Provisioning PAC = ON)
User name	-	-	-	-	Optional	Optional	Optional
Per-connection password	-	-	-	-	OFF	OFF	OFF

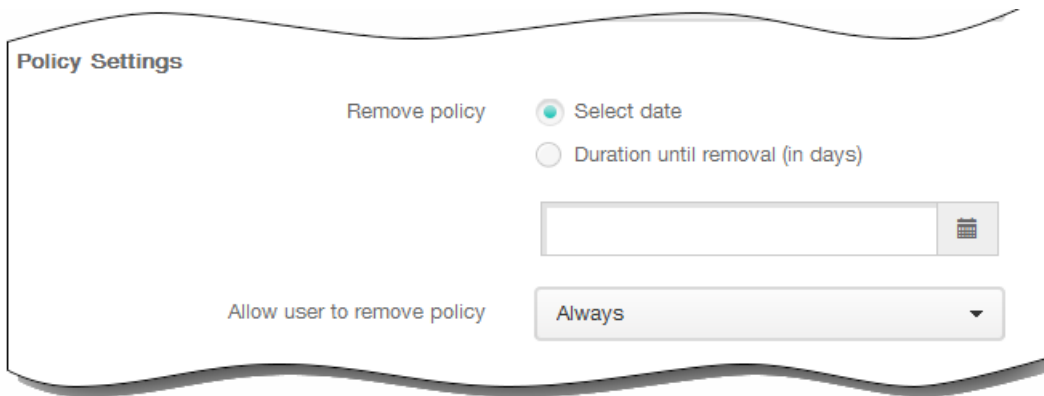
Password	None	WEP	WPA/WPA2 Personal	Any – (Personal)	Optional Enterprise	WPA/WPA2 Enterprise	Optional (Enterprise)
Identity credential (Keystore or PKI credential)	–	–	–	–	None	None	None
Requires a TLS certificate	–	–	–	–	OFF	OFF	OFF
Trusted certificates	–	–	–	–	Optional	Optional	Optional
Trusted server certificate names	–	–	–	–	Optional	Optional	Optional
Allow trust exceptions	–	–	–	–	ON	ON	ON

5. Proxy configuration: In the list, select how the VPN connection routes through a proxy server and then configure any additional options.

The following table lists the options available for Manual and Automatic; None does not require further configuration. Each cell lists the default value for an option when an option exists; otherwise, the cell indicates whether the option is not applicable (–), required, or optional.

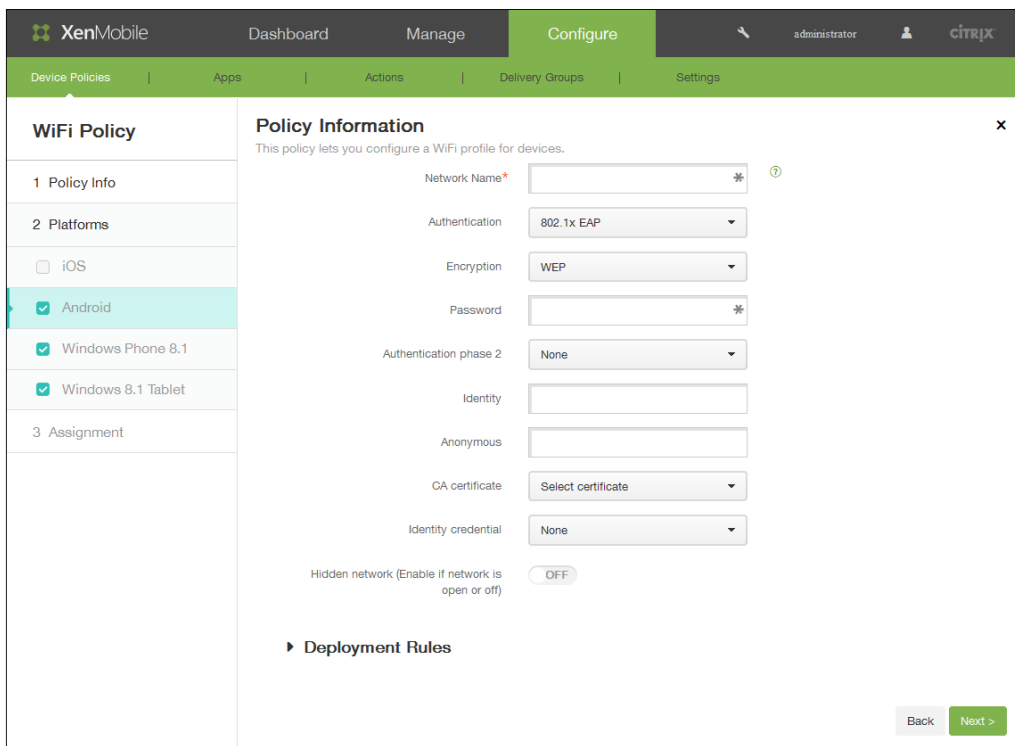
	Manual	Automatic
Host name or IP address fro the proxy server	Required	–
Port for the proxy server	Required	–
User name	Optional	–
Password	Optional	–
Proxy server URL	–	Required
Allow direct connection if PAC is unreachable	–	On (for iOS 7.0 and later)

Policy Settings



1. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
2. If you click Select date, click the calendar to select the specific date for removal.
3. In the Allow user to remove policy list, click Always, Password required, or Never.
4. If you click Password required, next to Removal password, type the necessary password.

If you selected Android, configure these settings:



1. Network name: Type the SSID that is seen in the list of available networks on the user's device.
2. Authentication: In the list, click the type of security to use with the WiFi connection.
 - Open
 - Shared

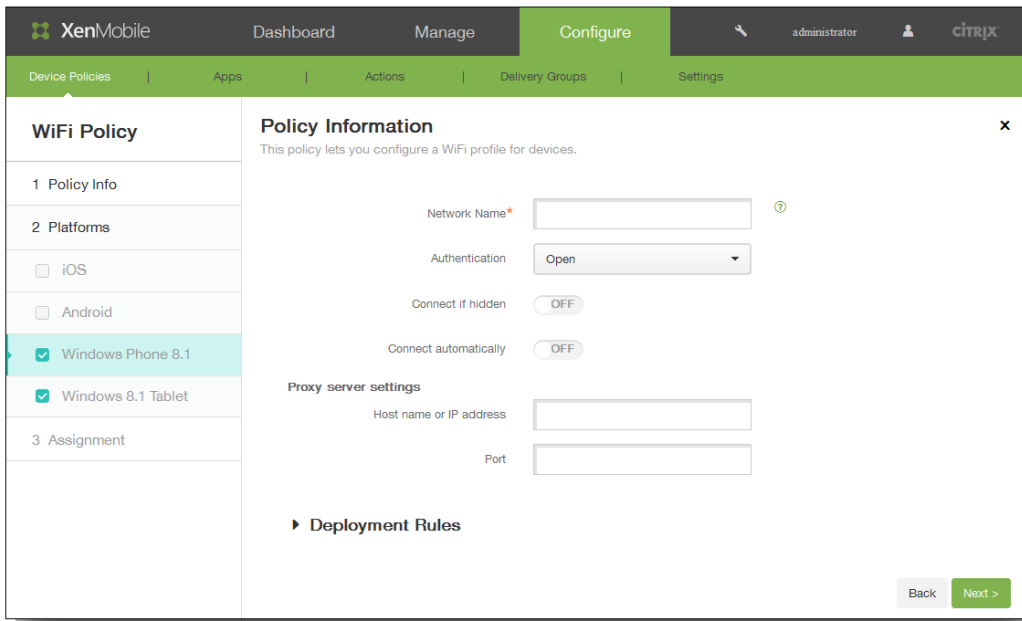
- WPA
- WPA-PSK
- WPA2
- WPA2-PSK
- 802.1x EAP

The following table lists the options to be configured for each of the preceding connection types. Each cell lists the default value for an option when a default exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

	Open	Shared	WPA	WPA-PSK	WPA2	WPA2-PSK	802.1 EAP
Encryption	TKIP	TKIP	TKIP	TKIP	TKIP	TKIP	-
Password	Optional	Optional	-	-	-	-	Optional
EAP type	-	-	-	-	-	-	PEAP
Authentication phase 2	-	-	-	-	-	-	None
Identity	-	-	-	-	-	-	Optional
Anonymous	-	-	-	-	-	-	Optional
CA certificate	-	-	-	-	-	-	Select
Identity credential	-	-	-	-	-	-	None

3. Hidden network (Enable if network is open or off): Select whether the network is hidden.

If you selected Windows Phone 8.1, configure these settings:



1. Network name: Type the SSID that is seen in the list of available networks on the user's device.
2. Authentication: In the list, click the type of security to use with the WiFi connection.

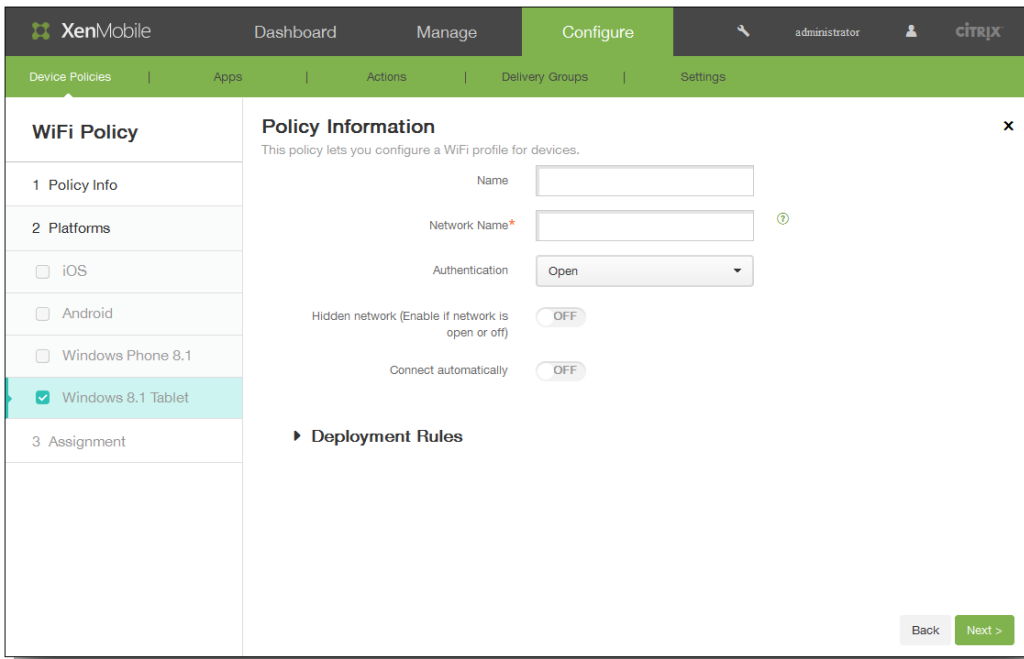
- Open
- WPA Personal
- WPA-2 Personal
- WPA-2 Enterprise

The following table lists the options to be configured for each of the preceding connection types. Each cell lists the default value for an option when a default exists; otherwise, the cell indicates whether the option is not applicable (-), required, or optional.

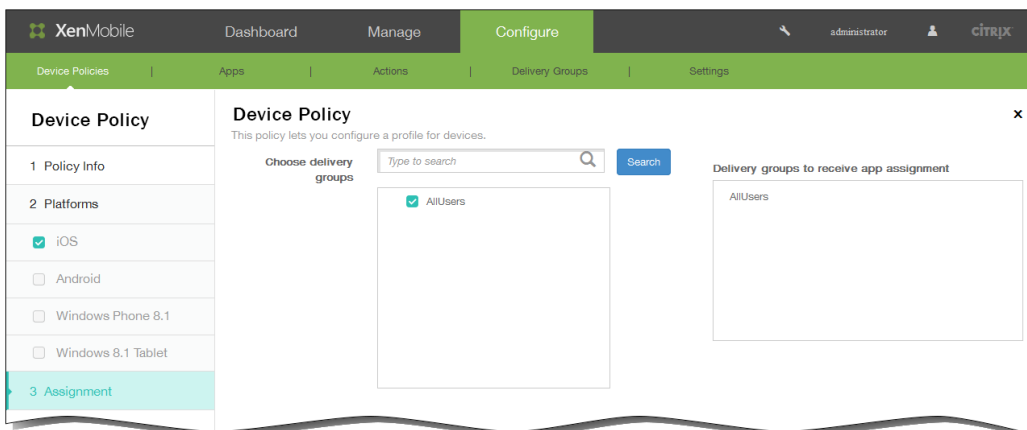
	Open	WPA Personal	WPA-2 Personal	WPA-2 Enterprise
Encryption	-	AES	AES	AES
Shared key	-	Optional	Optional	-

3. Connect if hidden: Select whether to connect when the network is hidden.
4. Connect automatically: Select whether to connect to the network automatically.
5. Host name or IP address: Type the name or IP address of a proxy server.
6. Port: Type the port number for the proxy server.

If you selected Windows 8.1 tablet, configure these settings:

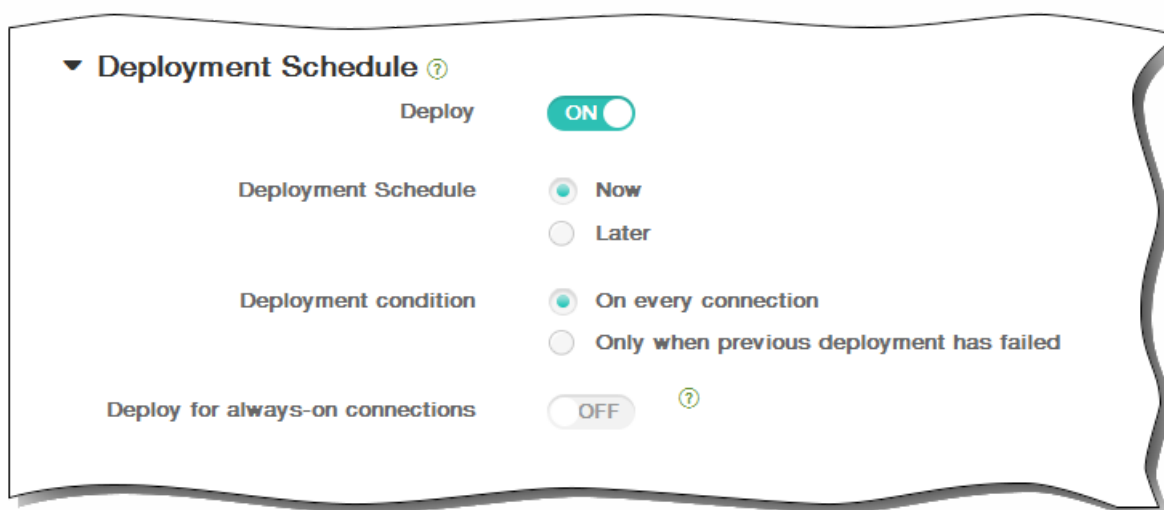


1. Name: Type a name for the network.
2. Network name: Type the SSID that is seen in the list of available networks on the user's device.
3. Authentication: In the list, click the type of security to use with the WiFi connection.
 - Open
 - WPA Personal
 - WPA-2 Personal
 - WPA Enterprise
 - WPA-2 Enterprise
4. Hidden network (Enable if network is open or off): Select whether the network is hidden.
5. Connect automatically: Select whether to connect to the network automatically.
5. After you finish configuring the settings for one or more platforms and then click Next, the Assignment page appears.
6. 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.



7. Expand Deployment Schedule and then configure the following settings:
 1. 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.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



8. Click Save to save the policy.

To add a terms and conditions device policy for all platforms

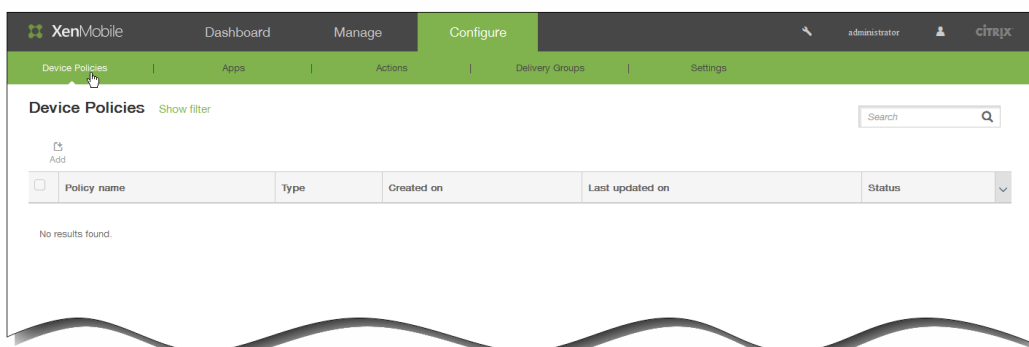
Mar 04, 2015

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.

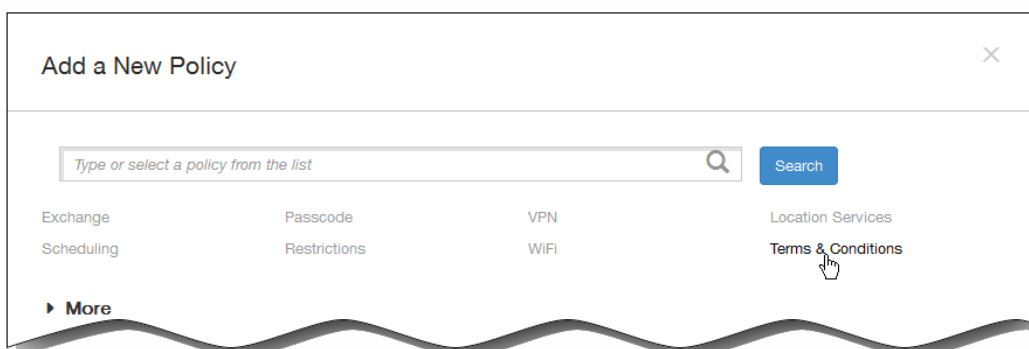
You can create different policies for terms and conditions in different languages if your company has international users and you want them to accept terms and conditions in their native languages.

Note: Terms and conditions files must be in PDF format.

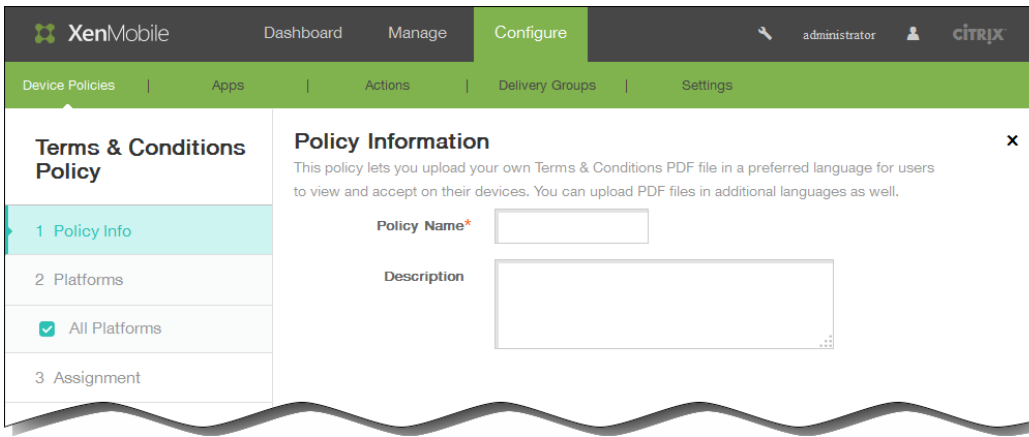
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



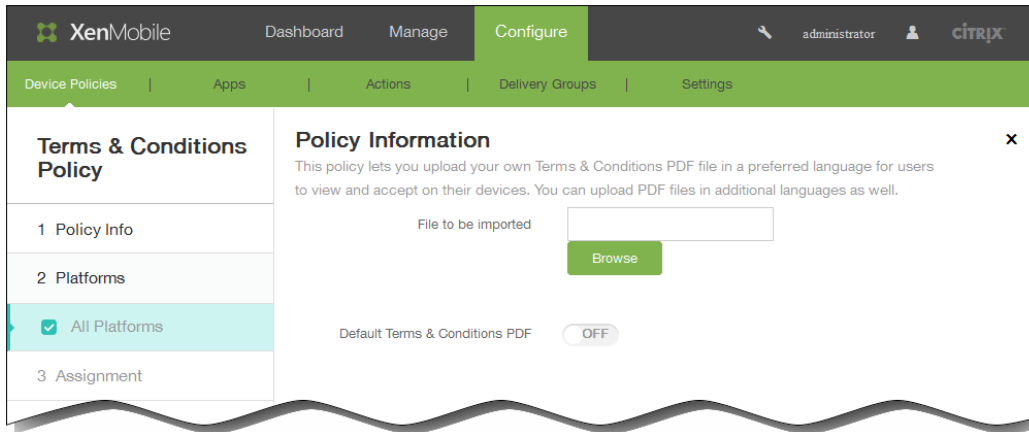
2. Click Add. The Add a New Policy dialog box appears.



3. Click Terms & Conditions. The Terms & Conditions Policy page appears.



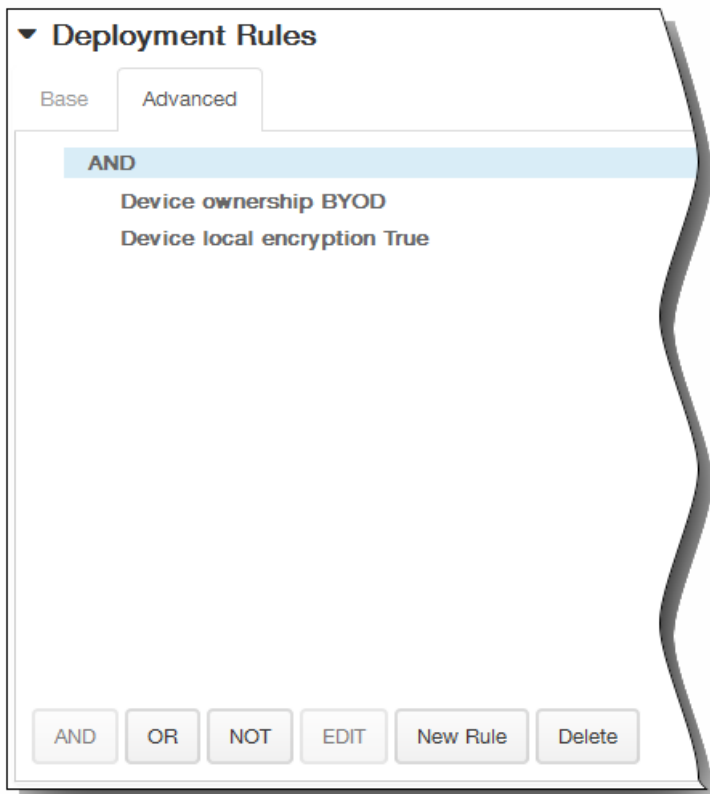
4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The All Platforms information page appears.



6. In the All Platforms information page, enter the following information:
 1. File to be imported: Select the terms and conditions file to import by clicking Browse and then navigating to the file's location.
 2. Default Terms & Conditions PDF: 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.
7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.

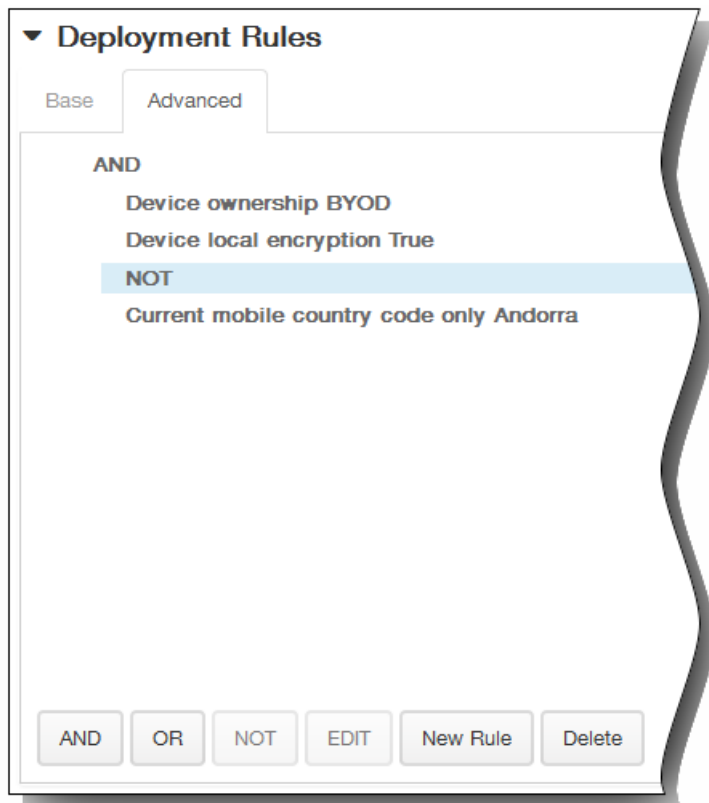


1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

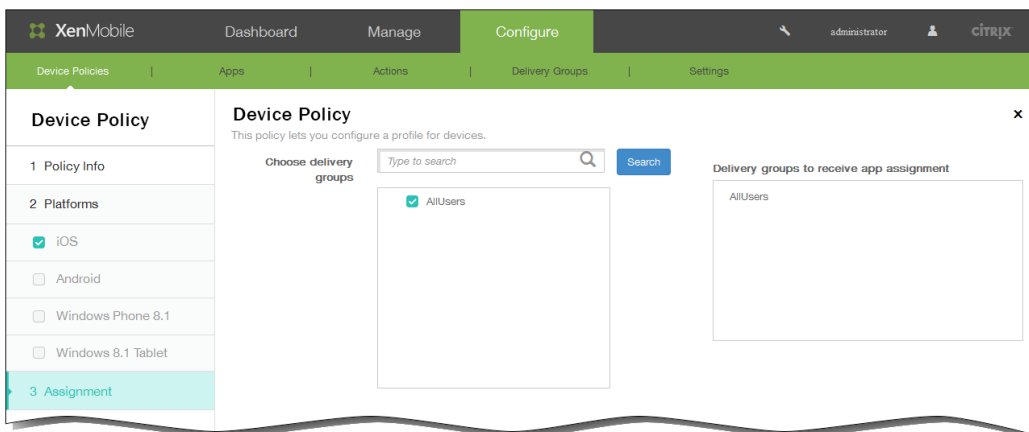


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.
In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



8. Click Next. The Terms & Conditions 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.

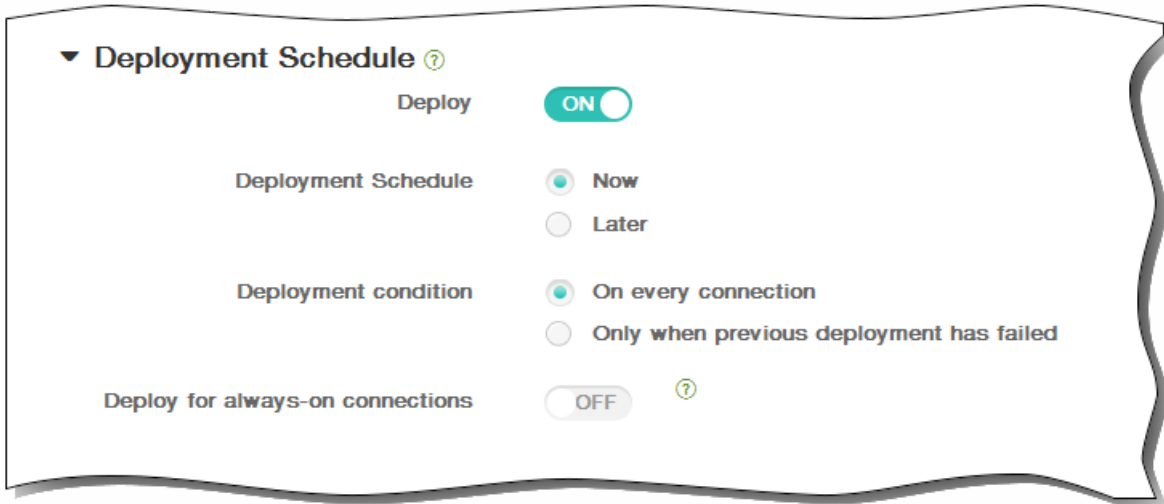


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



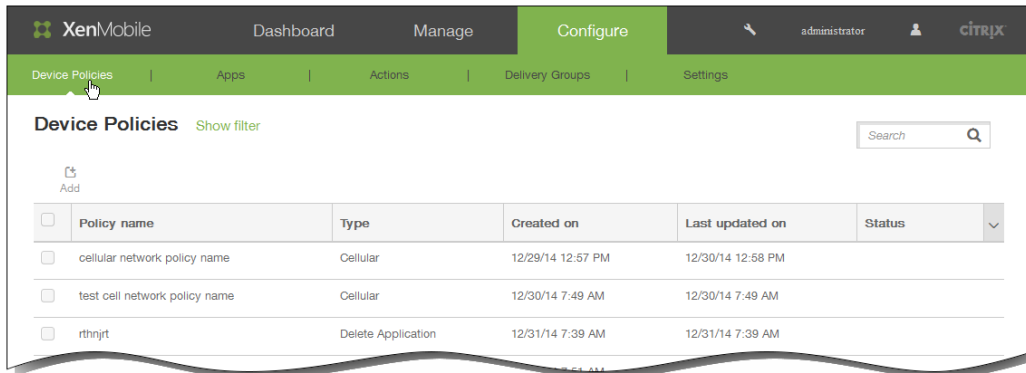
11. Click Save to save the policy.

To add a Worx Store device policy

Feb 13, 2015

This policy specifies when devices display a Worx Store webclip on the devices. The policy can apply to the following platforms: iOS, Android, or Windows 8.1 Tablet.

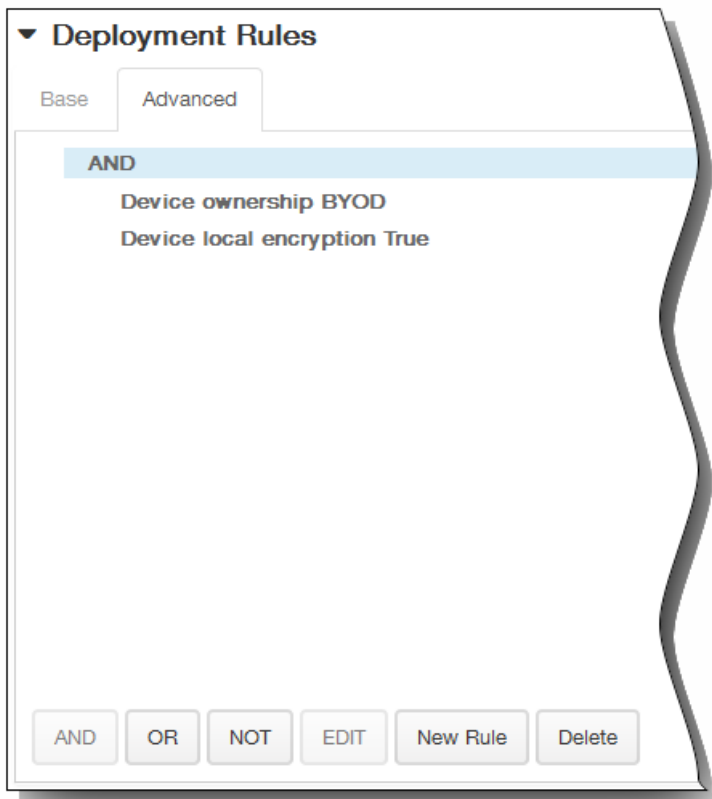
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



2. On the Add a New Policy page, click More > Worx Store.
3. On the Worx Store Policy page, on the Policy Information panel, enter the following information and then click Next.
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Type an optional description of the policy.
4. Under Platforms, select the platform or platforms you want to add.
5. For each platform you select, leave the default of ON or click OFF if you do not want a Worx Store webclip to appear on the devices.
6. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

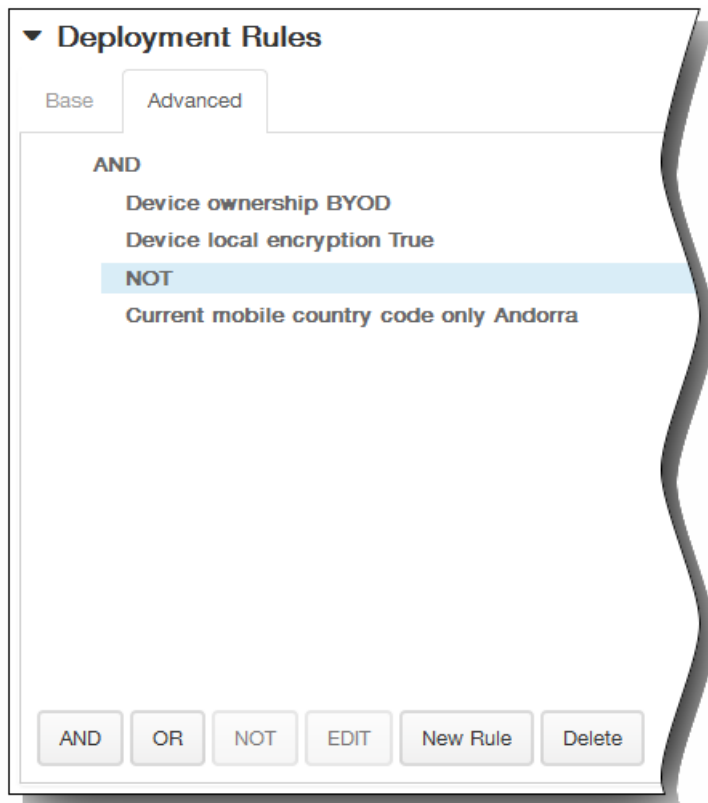


The conditions you chose on the Base tab appear.

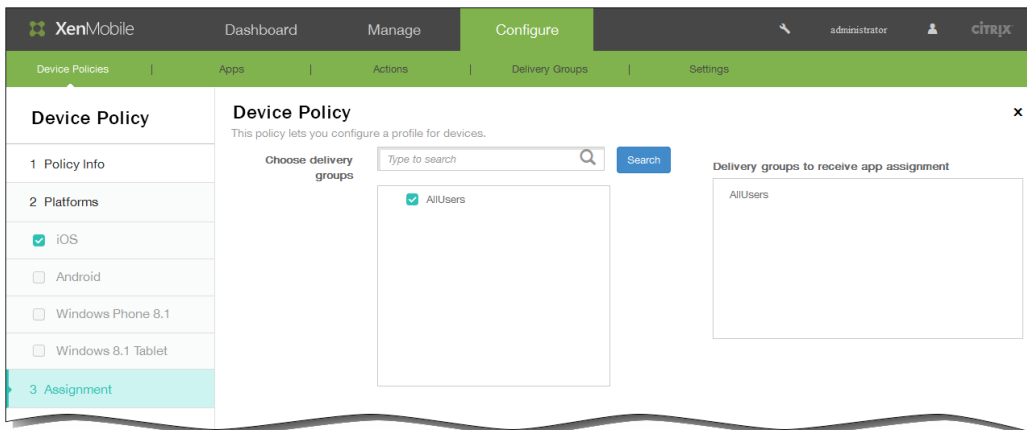
3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



7. After you finish configuring the settings for the selected platforms, click Next, the Assignment page appears.
8. 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.

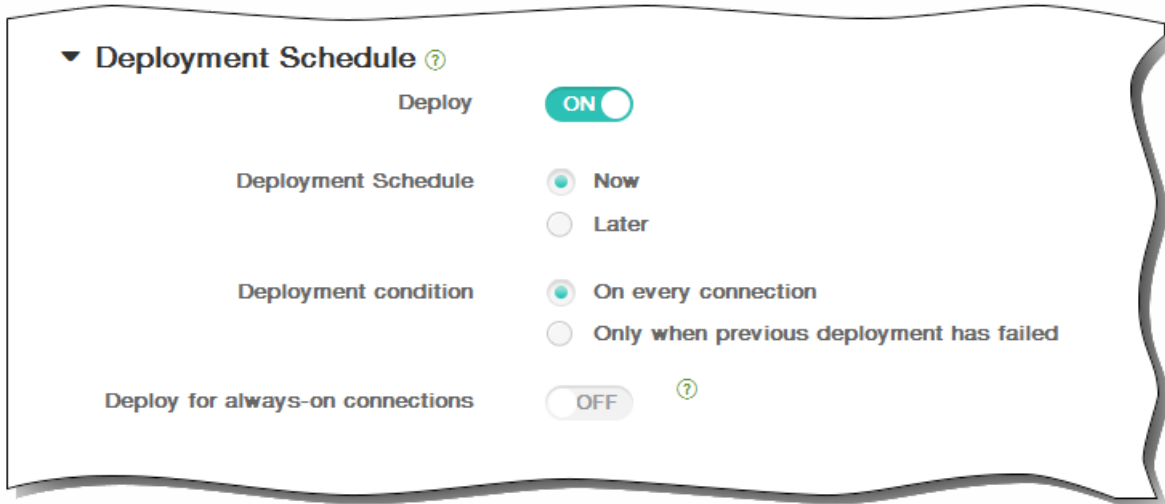


9. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



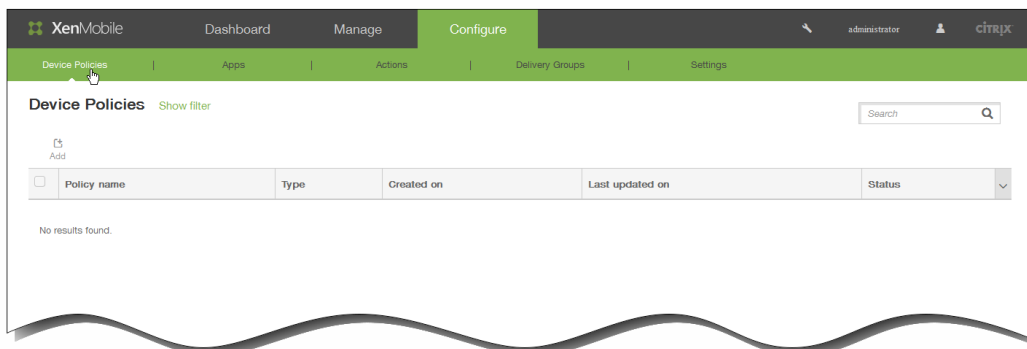
10. Click Save to save the policy.

XenMobile options device policies

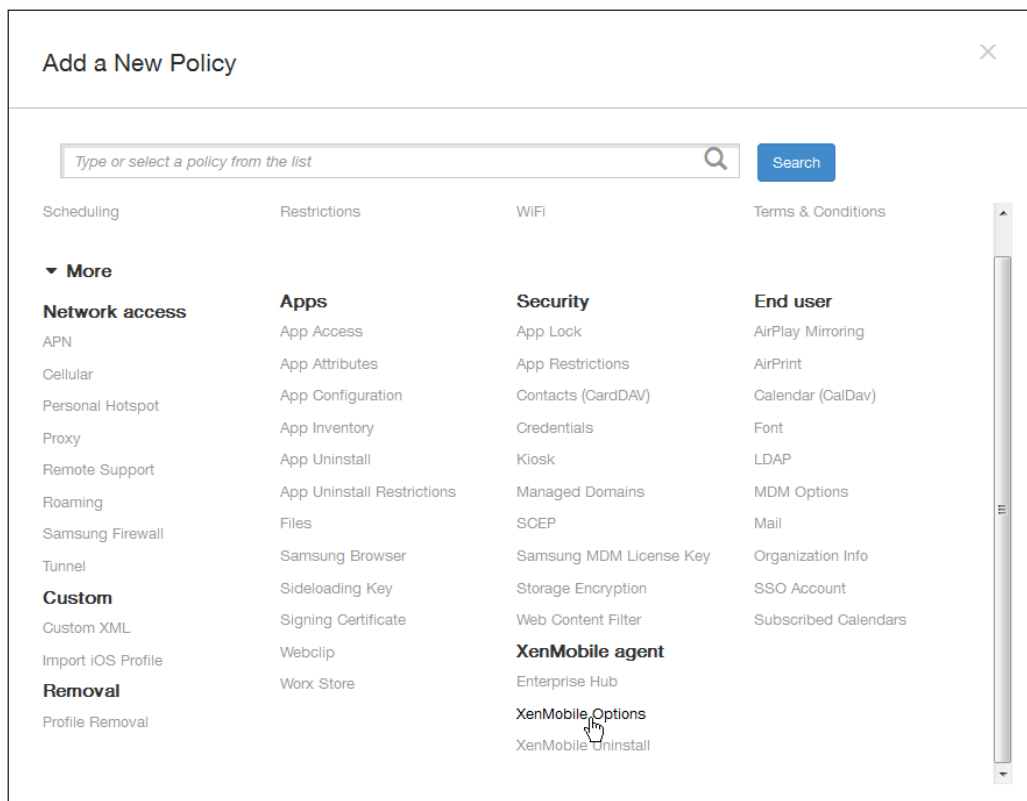
Mar 04, 2015

You add a XenMobile options policy to configure Worx Home behavior when connecting to XenMobile from Android and Symbian devices.

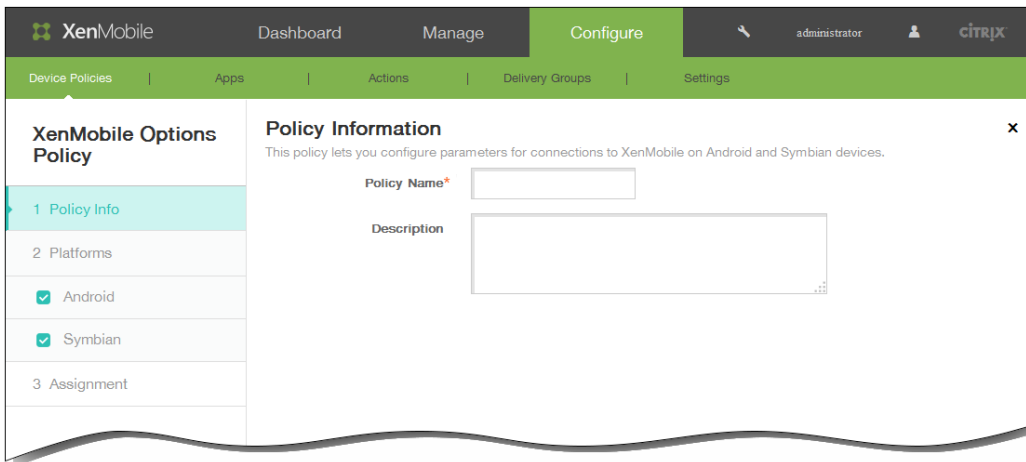
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



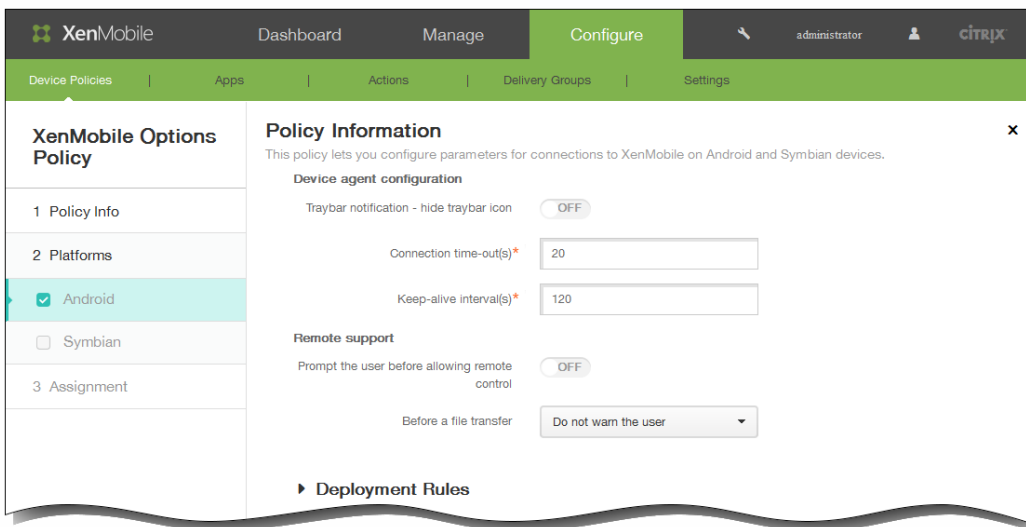
2. Click Add. The Add a New Policy dialog box appears.



3. Click More and then, under XenMobile agent, click XenMobile Options. The XenMobile Options Policy page appears.

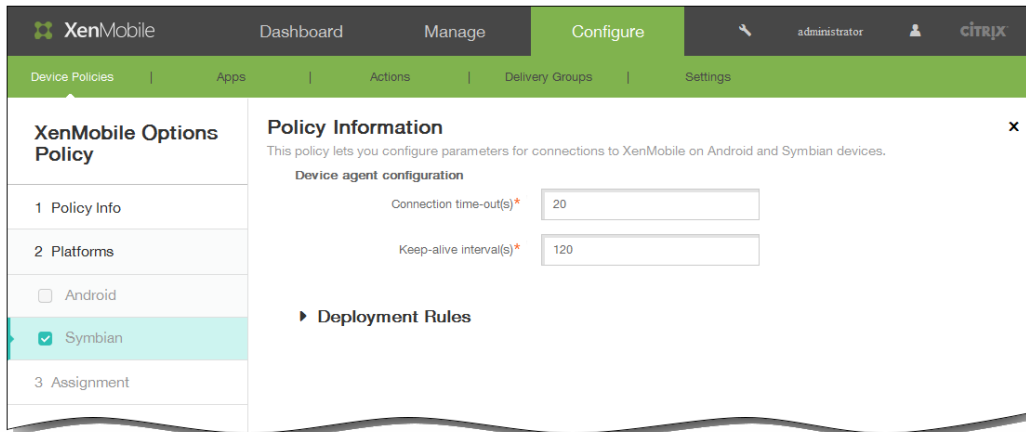


4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Type an optional description of the policy.
 3. Click Next.
5. Under Platforms, select the platform or platforms you want to add.
If you selected Android, configure these settings:

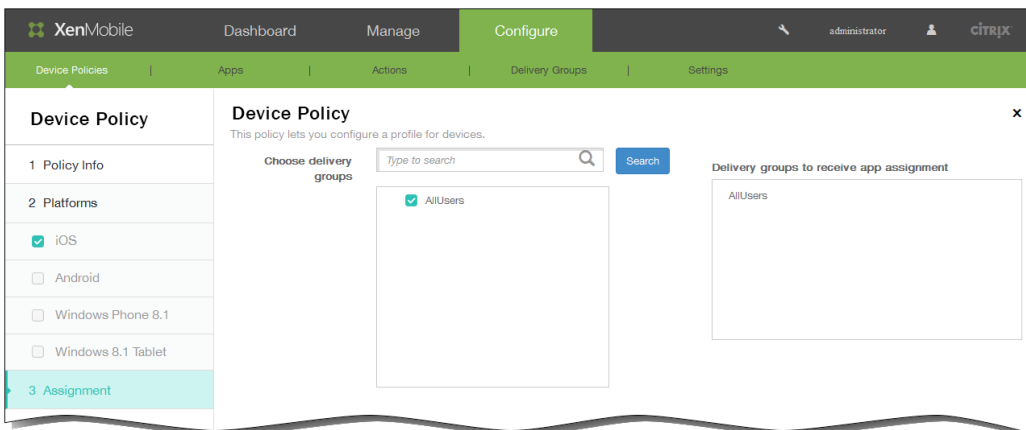


1. Traybar notification - hide traybar icon: Select whether the traybar icon is hidden or visible.
2. Connection: time-out(s): Type the length of time in seconds that a connection can be idle before the connection times out. The default is 20 seconds.
3. Keep-alive interval(s): Type the length of time in seconds to keep a connection open. The default is 120 seconds.
4. Prompt the user before allowing remote control: Select whether to prompt the user before allowing remote support control.
5. Before a file transfer: In the list, click whether to warn the user about a file transfer or whether to ask the user for permission.

If you selected Symbian, configure these settings:



1. Connection time-outs: Type the length of time in seconds that a connection can be idle before it times out. The default is 20 seconds.
2. Keep-alive interval(s): Type the length of time in seconds to keep a connection open. The default is 120 seconds.
6. After you finish configuring the settings for one or more platforms and then click Next, the 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. Expand Deployment Schedule and then configure the following settings:
 1. 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.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
 Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.
- Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.

▼ **Deployment Schedule** ?

Deploy ON

Deployment Schedule Now
 Later

Deployment condition On every connection
 Only when previous deployment has failed

Deploy for always-on connections OFF ?

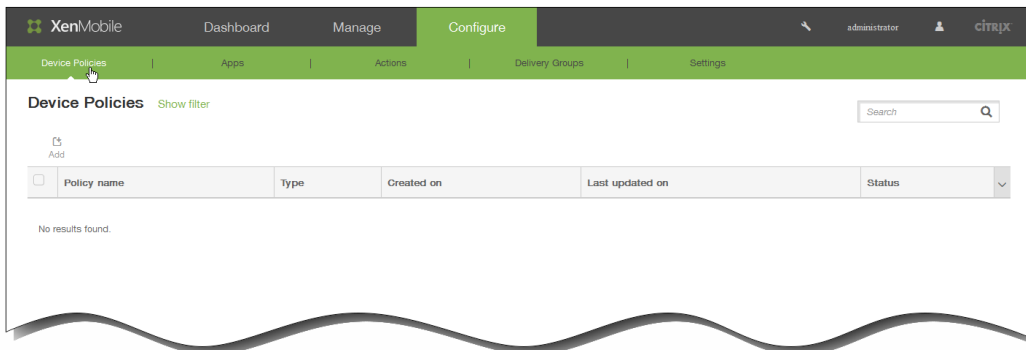
9. Click Save to save the policy.

To add a XenMobile uninstall device policy for Android

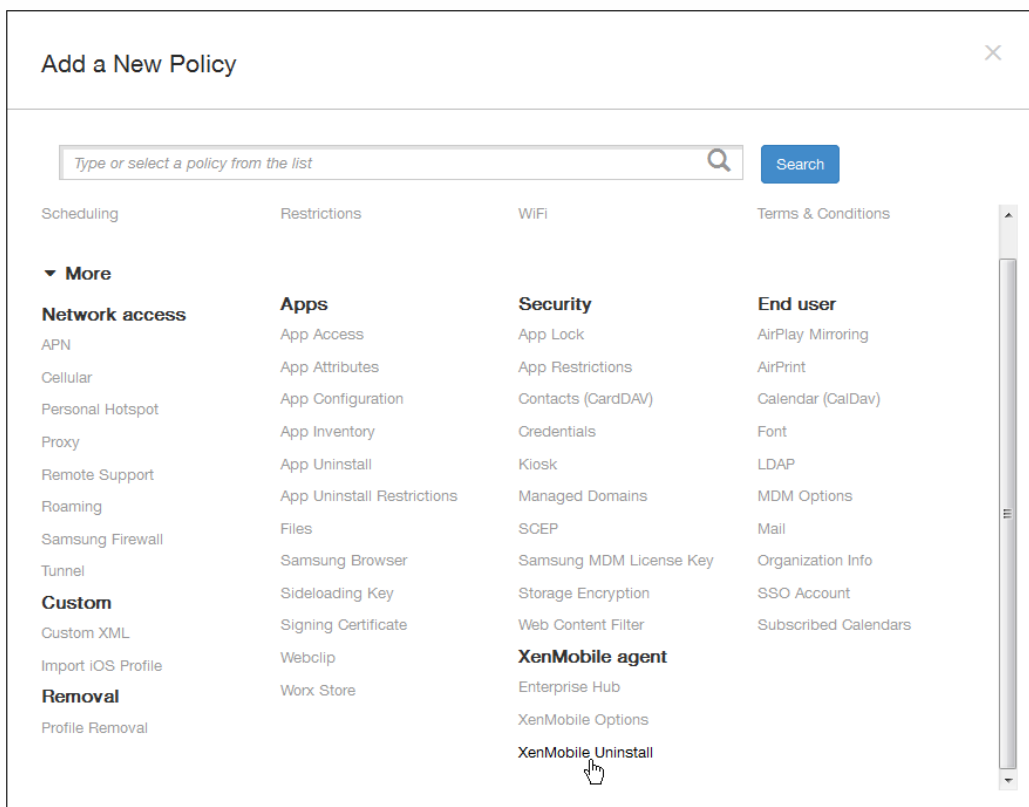
Mar 06, 2015

You can add a device policy in XenMobile to uninstall XenMobile from Android devices. When deployed, this policy removes XenMobile on all Android devices in the deployment group.

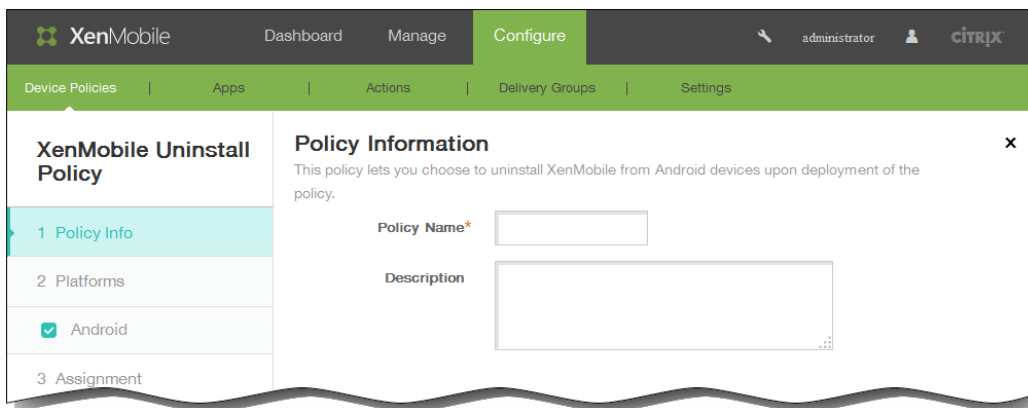
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



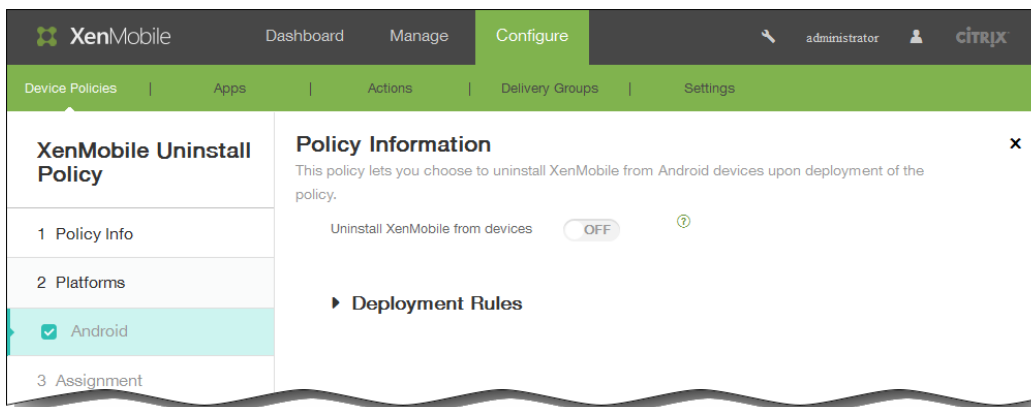
2. Click Add. The Add a New Policy dialog box appears.



3. Click More and then, under XenMobile agent, click XenMobile Uninstall. The XenMobile Uninstall Policy page appears.



4. In the Policy Information pane, enter the following information:
 1. Policy Name: Type a descriptive name for the policy.
 2. Description: Optionally, type a description of the policy.
5. Click Next. The Android Platform information page appears.

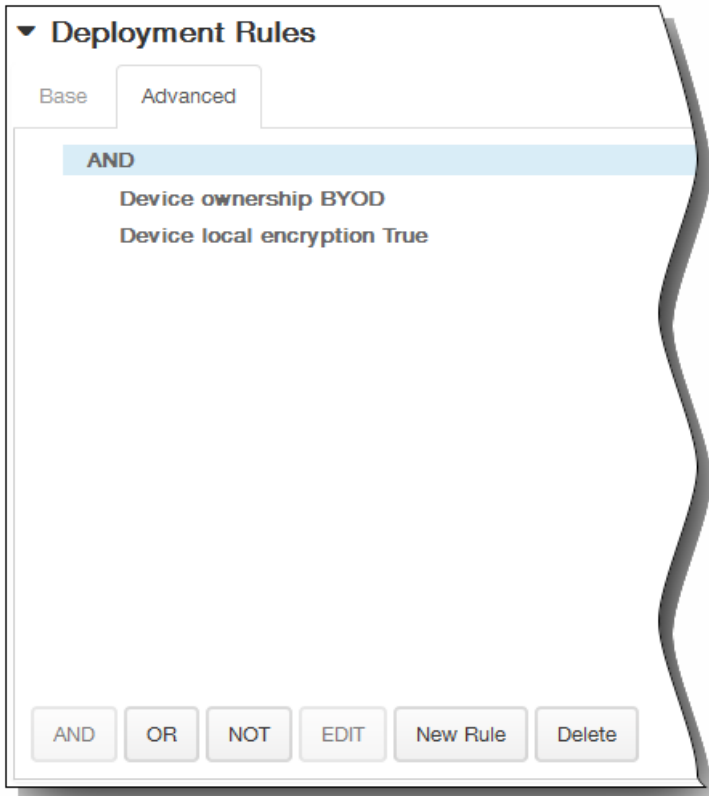


6. In the Android Platform information page, enter the following information:
 1. Uninstall XenMobile from devices: Select whether to uninstall XenMobile from Android devices. The default is OFF.
7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



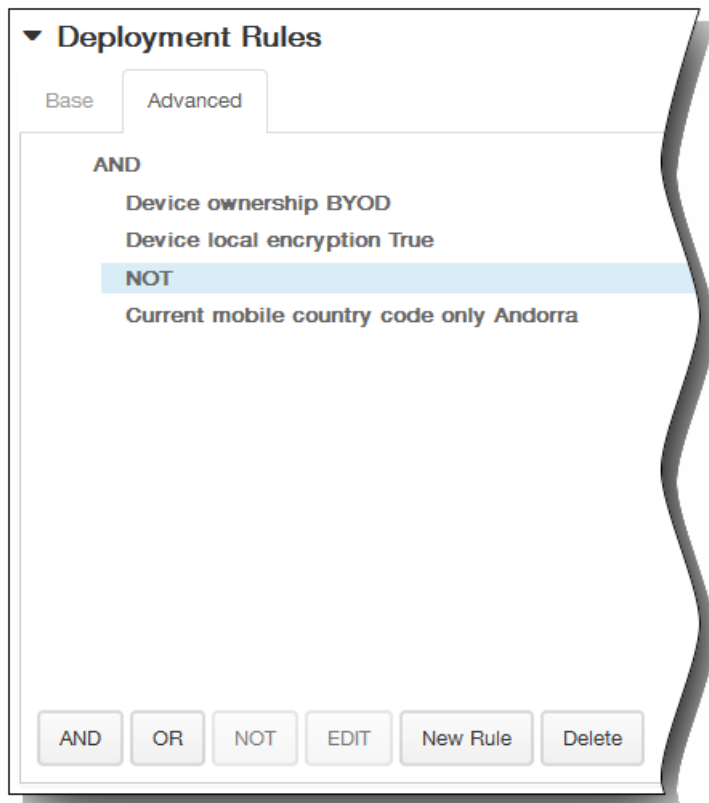
1. In the lists, click options to determine when the policy should be deployed.
 1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.

2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

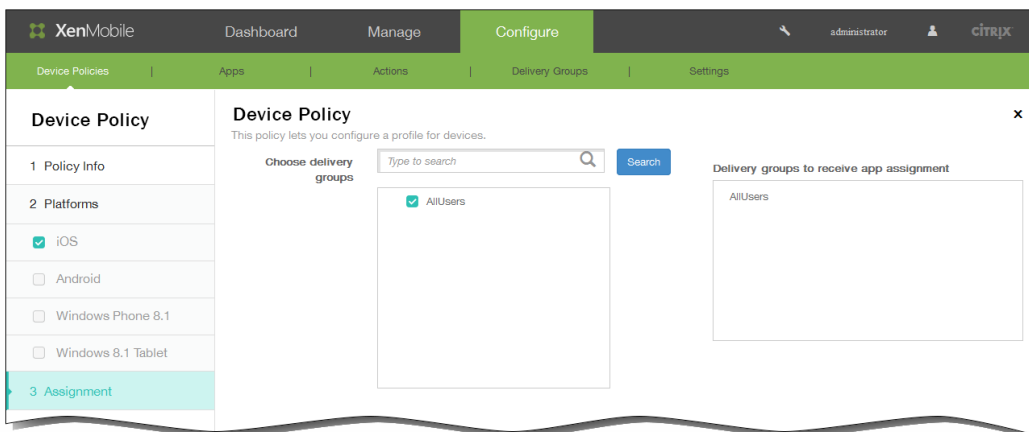


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.
In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



8. Click Next. The XenMobile Uninstall Policy assignment page appears.
9. Next to Choose delivery groups, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand Delivery groups to receive app assignment list.

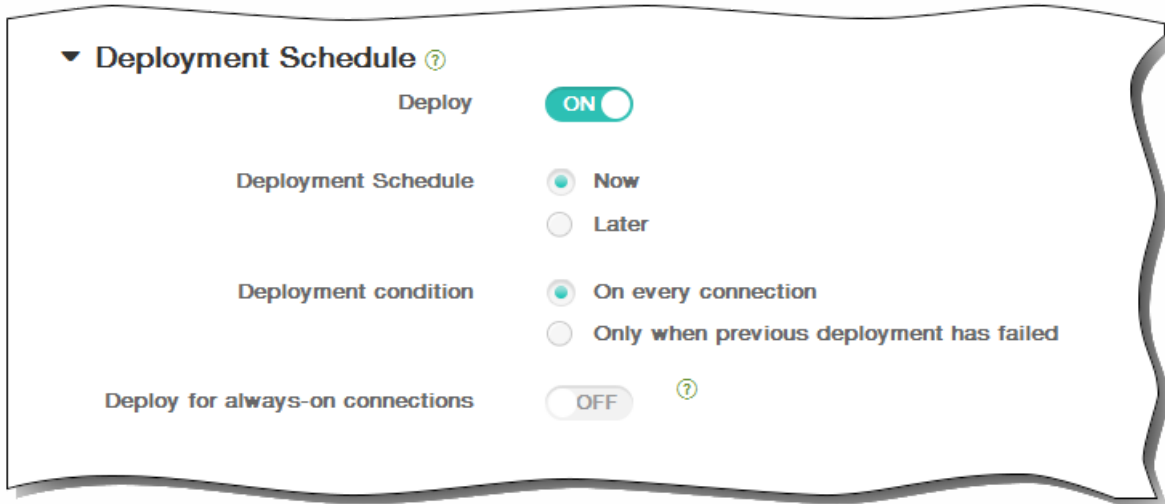


10. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.

5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



11. Click Save to save the policy.

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.

Adding Apps

Feb 13, 2015

You add apps to XenMobile for management. You add the apps to the XenMobile console, where you can then arrange the apps in categories and deploy the apps to users. Follow the procedure later in this topic to add app categories.

You can add the following types of apps to XenMobile:

- **MDX.** Apps wrapped with the MDX Toolkit (and associated policies). You deploy MDX apps obtained from internal and public stores. For example, WorxMail.
- **Public App Store.** These apps include free or paid apps available in a public store, such as iTunes or Google Play. For example, GoToMeeting.
- **Web and SaaS.** These apps include apps accessed from an internal network (web apps) or over a public network (SaaS). You can create your own apps, or choose from a set of app connectors for single sign-on authentication to existing Web apps. For example, GoogleApps_SAML.
- **Enterprise.** These apps represent native apps that are not wrapped with the MDX Toolkit and do not contain the policies associated with MDX apps.
- **Web Link.** A Web address (URL) to a public or private site or to a web app that does not require single sign-on.

How Mobile and MDX Apps Work

XenMobile supports iOS, Android, and Windows Phone 8.x apps, including Worx Apps, such as Worx Home, WorxMail and WorxWeb, and the use of MDX policies. Using the XenMobile web console, you can upload mobile apps and then deliver the apps to user devices. In addition to the Worx apps, you can add the following types of mobile apps:

- Apps you develop for your users.
- Apps in which you want to allow or restrict device features by using MDX policies.

Citrix provides the MDX Toolkit that wraps mobile apps for iOS, Android, and Windows Phone 8.x devices with Citrix logic and policies. The tool can securely wrap an app that was created within your organization or a mobile app made outside the company.

How Web and SaaS Apps Work

XenMobile comes with a set of application connectors, which are templates that you can configure for single sign-on (SSO) to web and Software as a Service (SaaS) applications, and in some cases for user account creation and management. XenMobile includes Security Assertion Markup Language (SAML) connectors. SAML connectors are used for web applications that support SAML protocol for SSO and user account management. XenMobile supports SAML 1.1 and SAML 2.0.

You can also build your own enterprise SAML connectors.

How Enterprise Apps Work

You can create your own application connector in XenMobile. This type of application typically resides in your internal network. Users can connect to the apps by using Worx Home. When you add an enterprise app, you create the application connector at the same time.

How the Public App Store Works

You can configure settings to retrieve mobile app names and descriptions from the Apple App Store, Google Play, and the

Windows Store. When you retrieve the app information from the store, XenMobile overwrites the existing name and description.

How Web Links Work

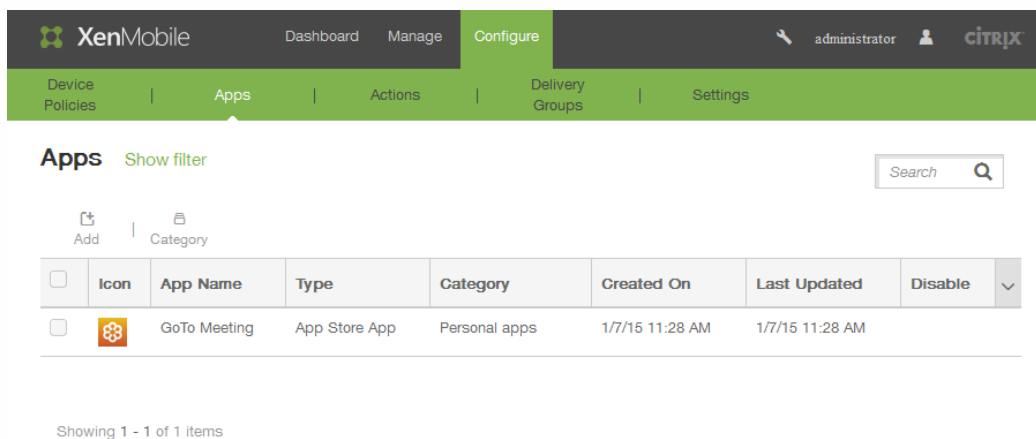
A web link is a web address to an Internet or intranet site. A web link can also point to a web application that doesn't require SSO. When you finish configuring a web link, the link appears as an icon in the Worx Store. When users log on with Worx Home, the link appears with the list of available apps and desktops.

Adding an app using the console consists of the following four steps:

- Adding information about the app.
- Selecting and configuring the app for each supported platform, such as iOS or Android.
- Defining an optional approval method.
- Setting optional delivery group assignments.

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

The Apps page appears.



Note: When connecting to the XenMobile console for the first time, the Apps table is empty; the only available options are **Add** and **Category**.

2. Click Add and then follow the steps in these eDocs topics for the type you want to add:

- [To add an MDX app to XenMobile](#)
- [To add a public app store app to XenMobile](#)
- [To add a Web and SaaS app to XenMobile](#)
- [To add an enterprise app to XenMobile](#)
- [To add a Web Link app to XenMobile](#)

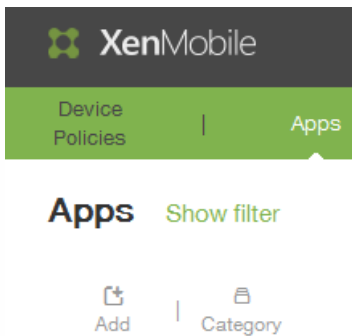
Note: After you add an app, the app appears in the table on the Apps page, where you can edit or categorize the app at any time.

To add app categories

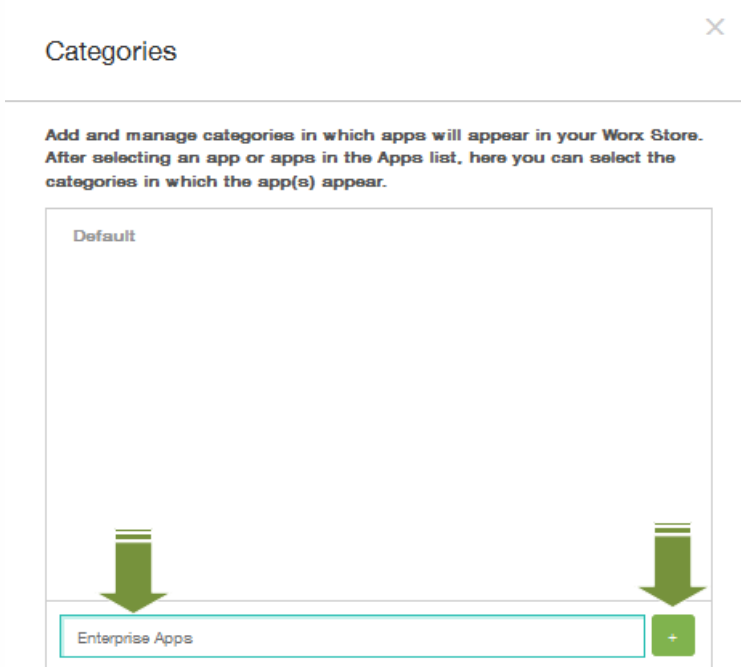
When users log on to Worx Home, they receive a list of the apps, web links, and stores that you have added and configured in XenMobile. You can use app categories to allow users to access only the apps, stores, or web links that you want. For example, you can create a Finance category and then add apps to the category that only pertain to finance. Or, you can configure a Sales category to which you assign sales apps. You can also configure an Apple category for the App Store. You configure categories on the Apps page in the XenMobile console. Then, when you configure or edit an app, web link, or

store, you can add the app to one of the categories you've configured.

1. In the XenMobile console, click Configure > Apps. The Apps page appears.
2. On the Apps page, click Category.



3. In the Categories dialog box, enter the name of the category you want to add and then click the Plus sign (+). For example, enter *Enterprise Apps* and then click the Plus sign (+).



The newly created category is added and appears in the same Categories dialog box. If no categories are currently configured, only the **Default** category appears

4. Repeat step 3 to add as many new categories as you want and then close the Categories dialog box.
5. On the Apps page, you can categorizing an existing app into a new category. Select the app you want to categorize.

Apps [Show filter](#)

Add | Edit | Disable | Category | Delete

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		waze app name	Web Link	Default	1/14/15 6:36 AM	1/14/15 6:53 AM	
<input checked="" type="checkbox"/>		enterprise1	Enterprise	Default	1/15/15 8:48 AM	1/15/15 8:48 AM	

6. Click Edit to categorize the app.

Apps [Show filter](#)

Add | Edit | Disable | Category | Delete

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		waze app name	Web Link	Default	1/14/15 6:36 AM	1/14/15 6:53 AM	
<input checked="" type="checkbox"/>		enterprise1	Enterprise	Default	1/15/15 8:48 AM	1/15/15 8:48 AM	

The App Information page appears.

7. In App category list, apply the category by selecting the category check box.

XenMobile Dashboard Manage Configure administrator CITRIX

Device Policies | Apps | Actions | Delivery Groups | Settings

Enterprise

- 1 App Information
- 2 Platform
 - iOS
 - Android
 - Samsung KNOX
 - Windows Phone
 - Windows Tablet
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

App Information

Name*

Description


App category



- Default
- Enterprise Apps



8. Click Next to step through the remaining pages of the app configuration.

9. Click Save on the last page to apply the category. The newly created category is applied to the app and appears in the App table.

Apps [Show filter](#)

 Add |  Category

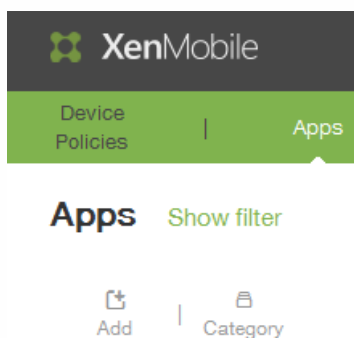
<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	▼
<input type="checkbox"/>		waze app name	Web Link	Default	1/14/15 6:36 AM	1/14/15 6:53 AM		
<input type="checkbox"/>		enterprise1	Enterprise	Enterprise Apps	1/15/15 8:48 AM	1/16/15 12:40 PM		

To add an MDX app to XenMobile

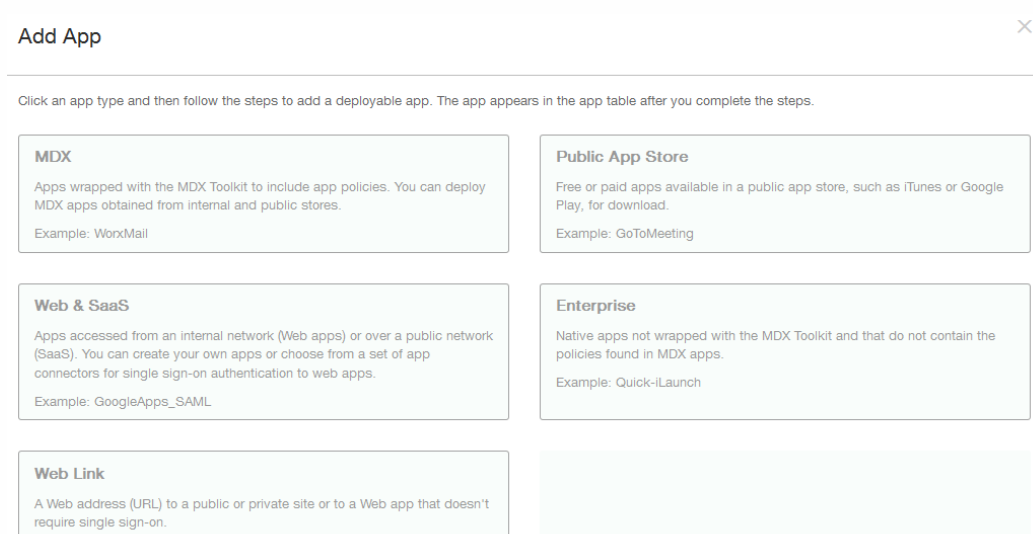
Feb 24, 2015

When you receive a wrapped MDX mobile app for an iOS, Android, or Windows Phone device, you can upload the app to XenMobile. After you upload the app, you can configure app details and policy settings. For more information about the app policies that are available for each device platform type, see [MDX Policies at a Glance for iOS, Android, and Windows Phone](#).

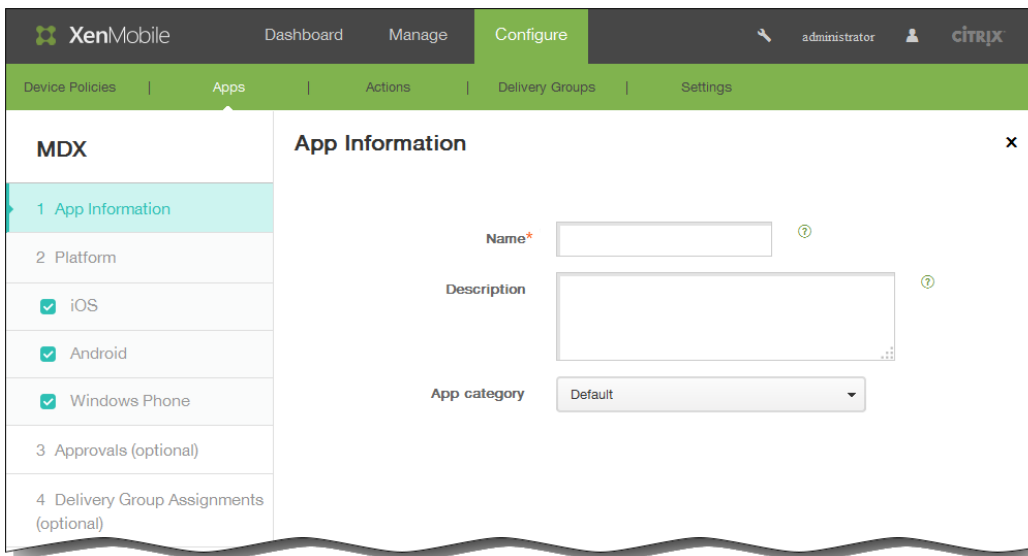
1. In the XenMobile console, click Configure > Apps. The Apps page appears.
2. Click Add.



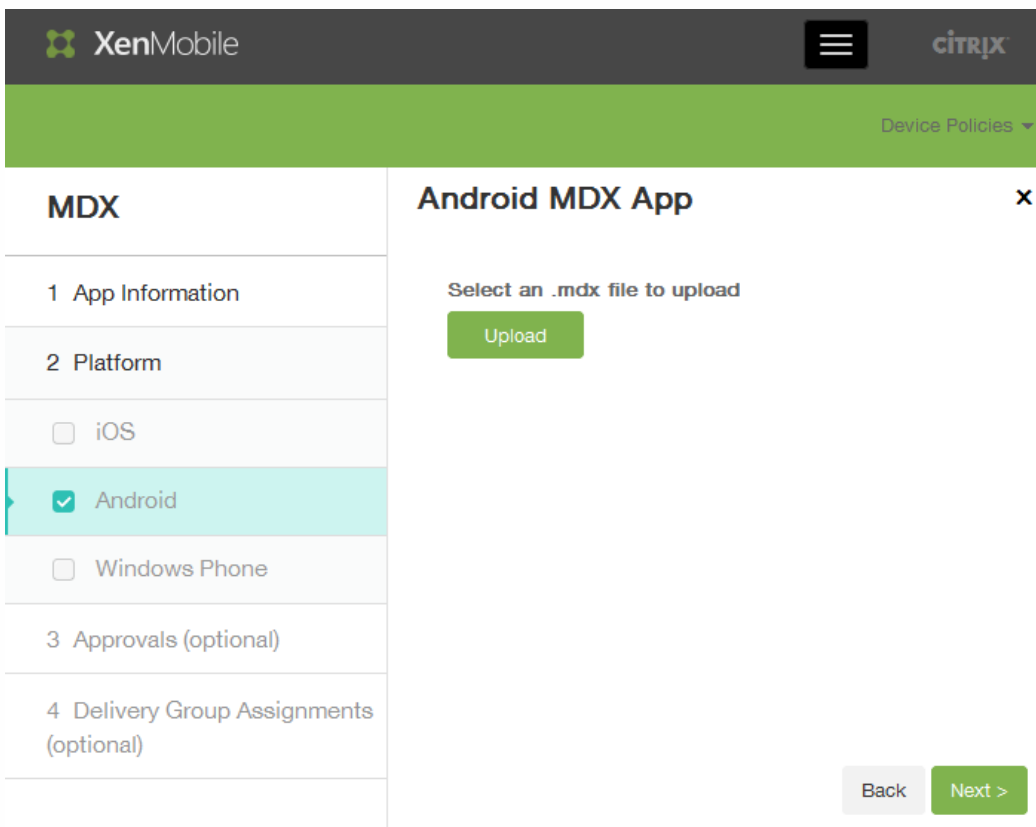
3. In the Add App screen, click MDX.



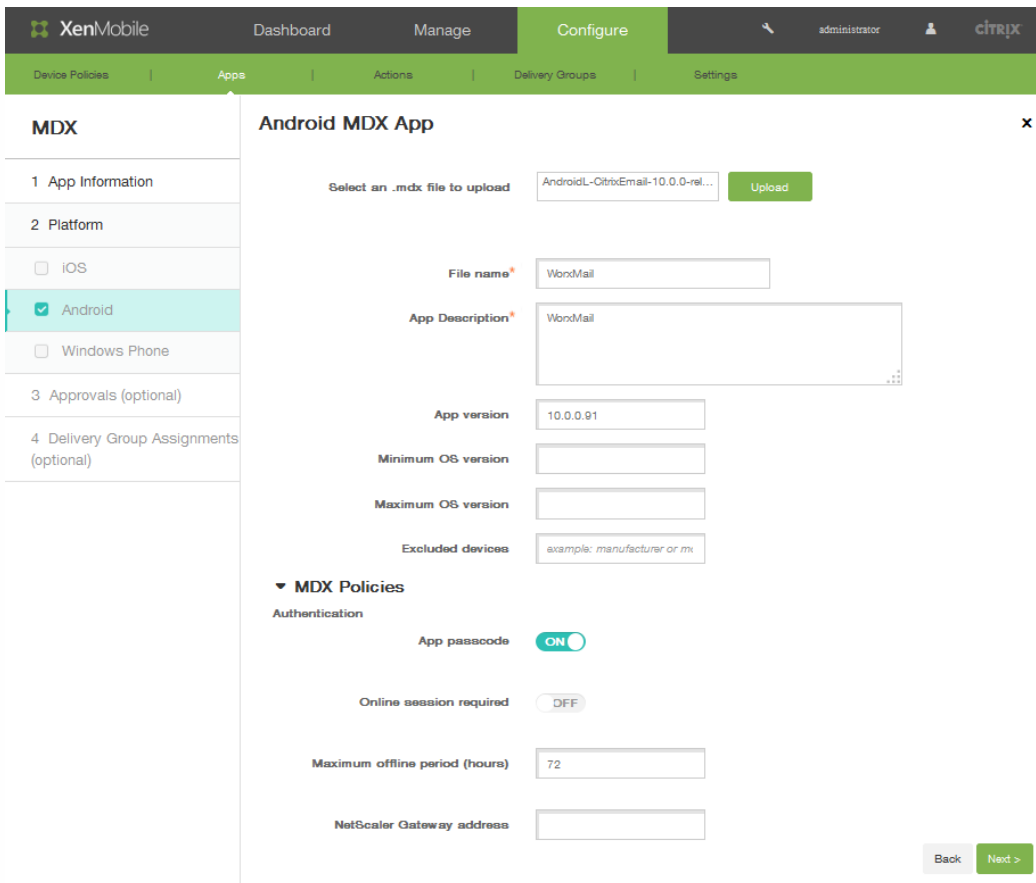
4. On the App Information page, enter a Name and then provide an optional Description for the app. These fields are used for internal purposes. If you are adding apps for multiple devices, use the check boxes in the left portion of the screen to select them.



5. In the App category list, click the App category. See [Adding a Category](#) for additional information.
6. Click Next.
7. Click Upload to select an .mdx file to upload and then click Next.



The app details and MDX policies fields appear.



8. Configure the following settings:

1. File name: Enter the file name associated with the app.
2. App Description: Enter a description for the app.
3. Minimum OS version: Enter the oldest operating system version that the device can run in order to use the app.
4. Maximum OS version: Enter the most recent operating system that the device must run in order to use the app.
5. Excluded devices: Enter the manufacturer or models of devices that cannot run the app.

9. In the MDX Policies section, configure policy settings that the Worx Store enforces in the area of authentication, device security, network requirements and access, encryption, app interaction, and app restrictions, and more.

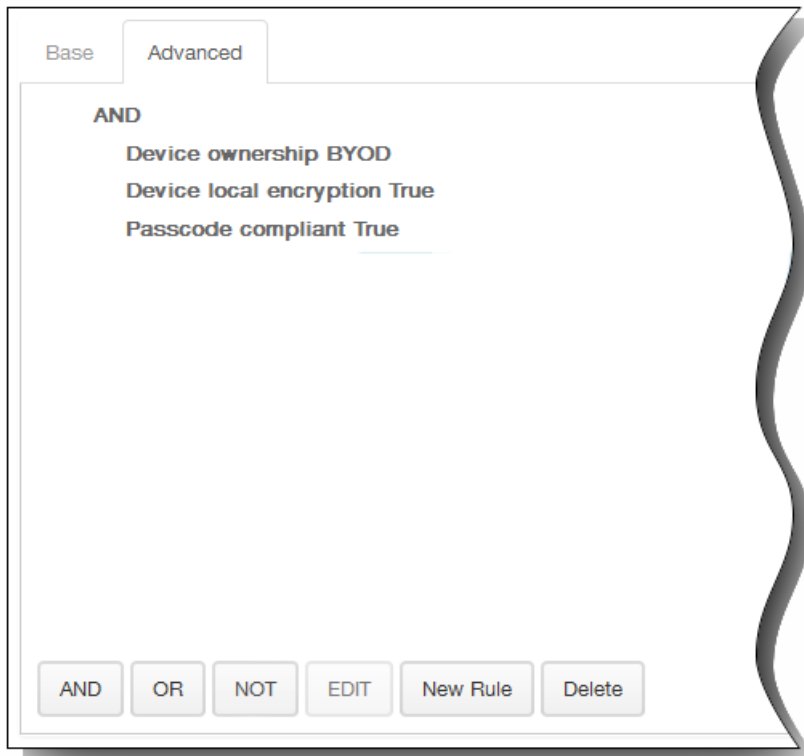
Note: In the console, you can hover over the policy name to view a description of the policy. For more information about app policies for MDX apps, such as a table showing which policies apply to which platform types, see [MDX Policies at a Glance for iOS, Android, and Windows Phone](#).

10. Expand Deployment Rules. The Base tab appears by default.



1. In the lists, click options to determine when the app should be deployed.

1. You can choose to deploy the app when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

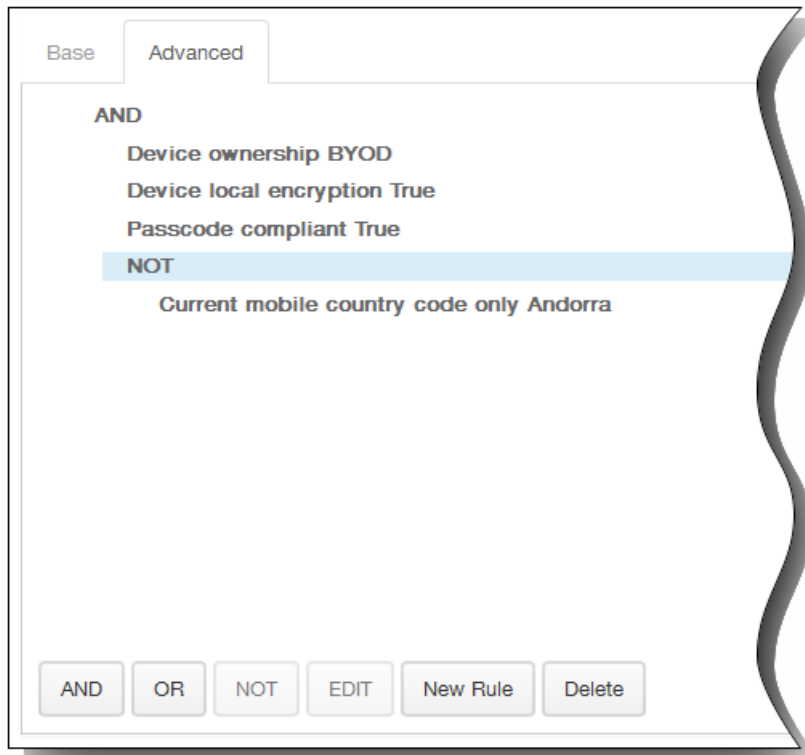


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
 3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, the device must be passcode compliant, and the device mobile country code cannot be only Andorra.



- Expand Worx Store Configuration to add an FAQ for the app, or add screen captures to help classify the app in the Worx Store. The graphic you upload must be of the type PNG. You cannot upload a GIF or JPEG image.

▼ **Worx Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

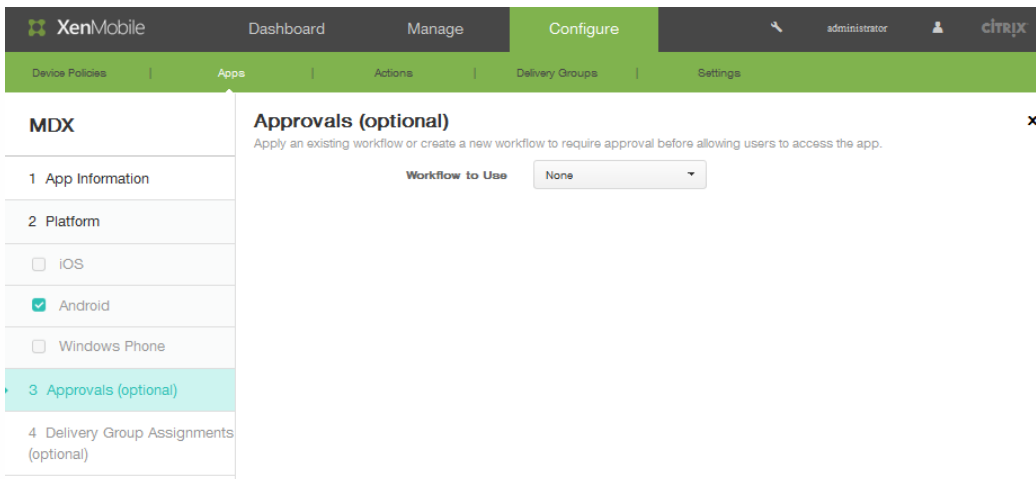


Allow app ratings

Allow app comments

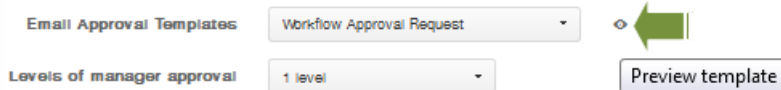
In Allow app ratings, click ON to permit a user to rate the app.

- In Allow app comments, click ON to permit users to comment about the selected app.
- Click Next. The Approvals screen appears.

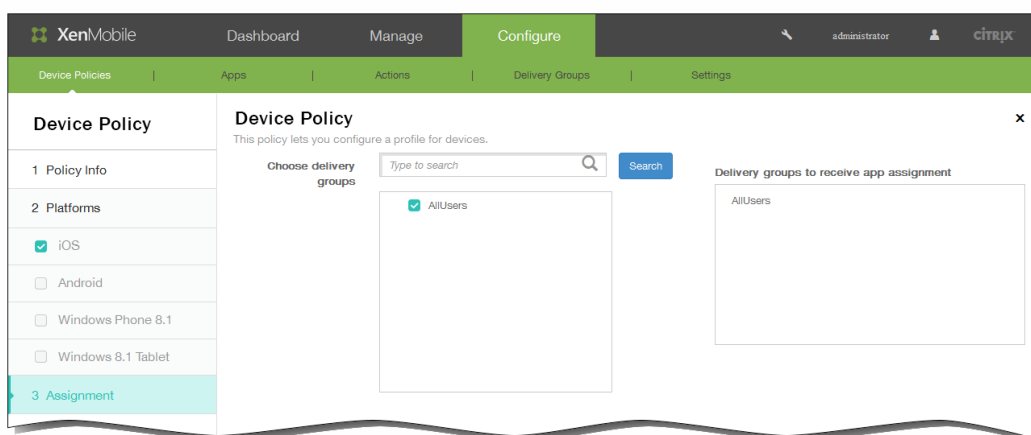


14. When you create a new workflow, the XenMobile console changes to display configuration options for the approval process. Each of these fields is described in the following steps. Configure these fields if you need approval for creating user account.

1. Specify a **name** for the workflow.
2. Optionally enter a **description**.
3. In **Email Approval Templates** field, click a notification option. Click the eye icon to preview the template you chose.



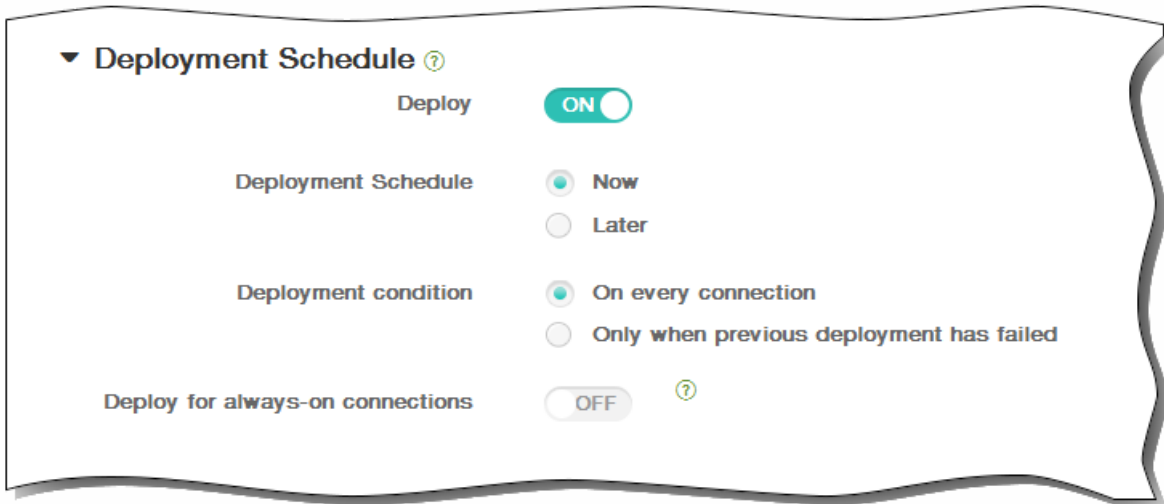
4. In **Levels of manager approval**, click the level from None to 3. .
 5. In **Select Active Directory domain**, click the domain.
 6. In Find additional required approvers, optionally enter additional required approvers and then click Search.
15. Click Next.
16. Next to Choose delivery groups, type 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.



17. Expand Deployment Schedule and then configure the following settings:
 1. 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.

2. Next to Deployment schedule, click Now or Later. The default option is Now.
3. If you click Later, click the calendar icon and then select the date and time for deployment.
4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



18. Click Save. The XenMobile console applies the app information.

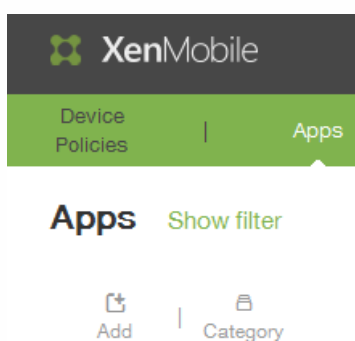
Creating App Categories in XenMobile

Feb 13, 2015

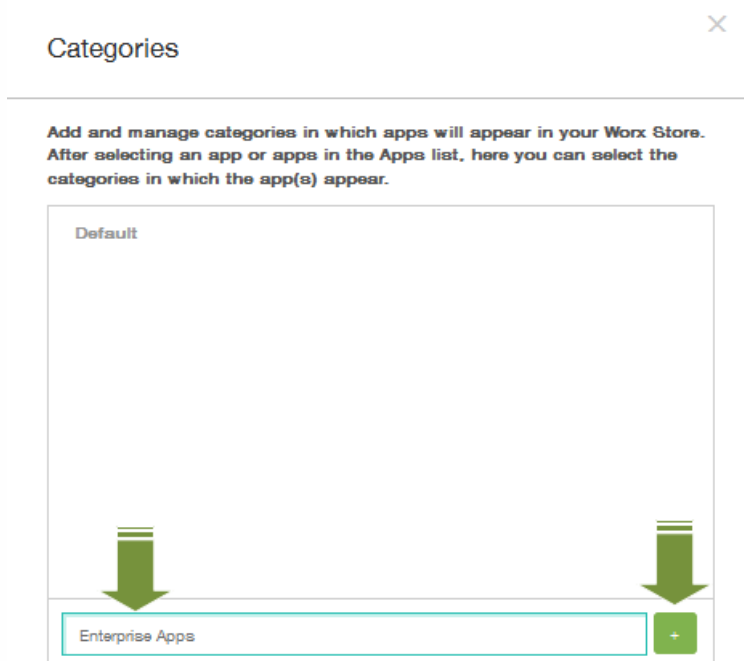
When users log on to Worx Home, they receive a list of the apps, web links, and stores that you have added and configured in XenMobile. You can use app categories to allow users to access only the apps, stores, or web links that you want. For example, you can create a Finance category and then add apps to the category that only pertain to finance. Or, you can configure a Sales category to which you assign sales apps. You can also configure an Apple category for the App Store. You configure categories on the Apps page in the XenMobile console. Then, when you configure or edit an app, web link, or store, you can add the app to one of the categories you've configured.

To add a category

1. In the XenMobile console, click Configure > Apps. The Apps page appears.
2. On the Apps page, click Category.



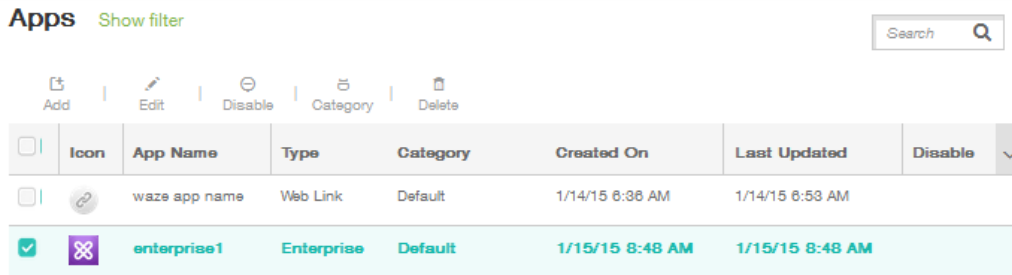
3. In the Categories dialog box, enter the name of the category you want to add and then click the Plus sign (+). For example, enter *Enterprise Apps* and then click the Plus sign (+).



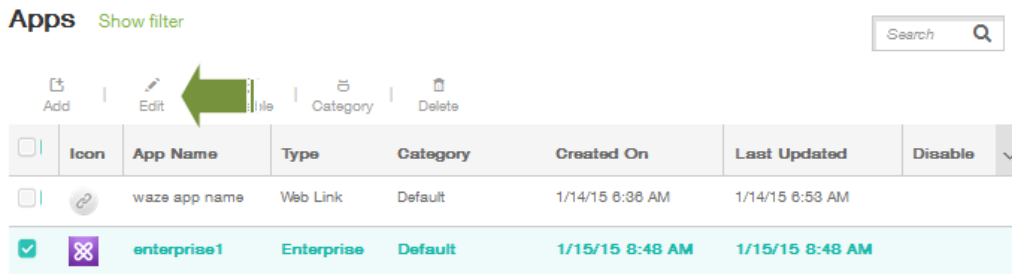
The newly created category is added and appears in the same Categories dialog box. If no categories are currently

configured, only the **Default** category appears.

- Repeat step 3 to add as many new categories as you want and then close the Categories dialog box.
- On the Apps page, you can categorizing an existing app into a new category. Select the app you want to categorize.



- Click Edit to categorize the app.



The App Information page appears.

- In App category list, apply the category by selecting the category check box.

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'Dashboard', 'Manage', and 'Configure'. The 'Configure' tab is active, and the 'Apps' sub-tab is selected. The left sidebar shows a navigation menu with 'Enterprise' selected, and '1 App Information' is the active step. The main area displays the 'App Information' form with the following fields:

- Name:** enterprise1
- Description:** (empty text area)
- App category:** A dropdown menu showing 'Default, Enterprise Apps' with a list of options: 'Default' and 'Enterprise Apps', both of which are checked.

Other steps in the configuration process include '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'.

8. Click Next to step through the remaining pages of the app configuration.
9. Click Save on the last page to apply the category. The newly created category is applied to the app and appears in the App table.

Apps [Show filter](#)

[Add](#) | [Category](#)

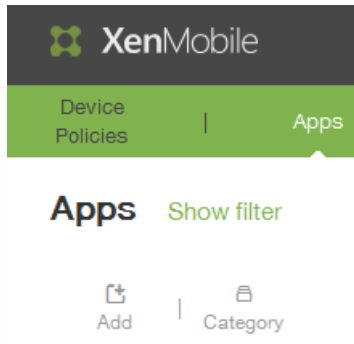
<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		waze app name	Web Link	Default	1/14/15 6:38 AM	1/14/15 6:53 AM	
<input type="checkbox"/>		enterprise1	Enterprise	Enterprise Apps	1/15/15 8:48 AM	1/16/15 12:40 PM	

To add a public app store app to XenMobile

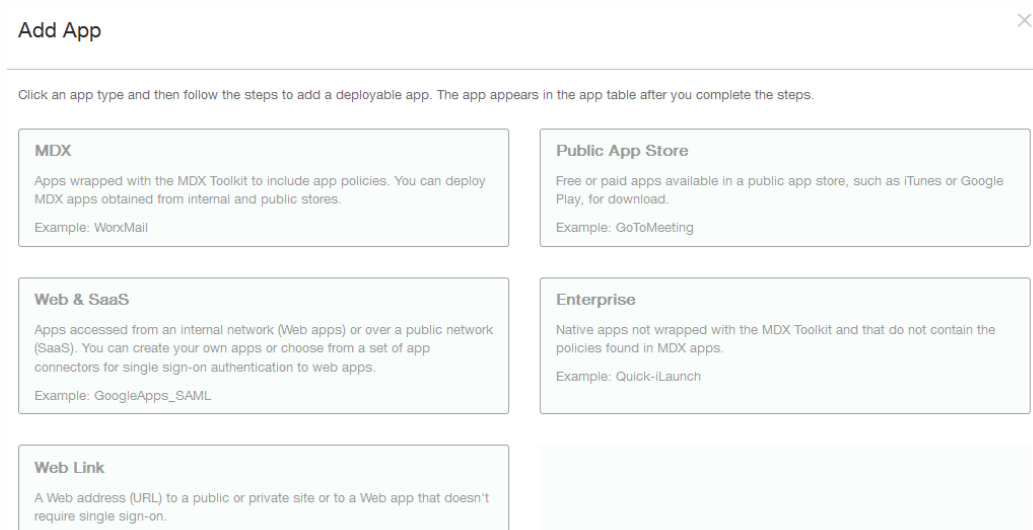
Feb 25, 2015

You can add free or paid apps to XenMobile that are available in a public app store, such as iTunes or GooglePlay. For example, GoToMeeting.

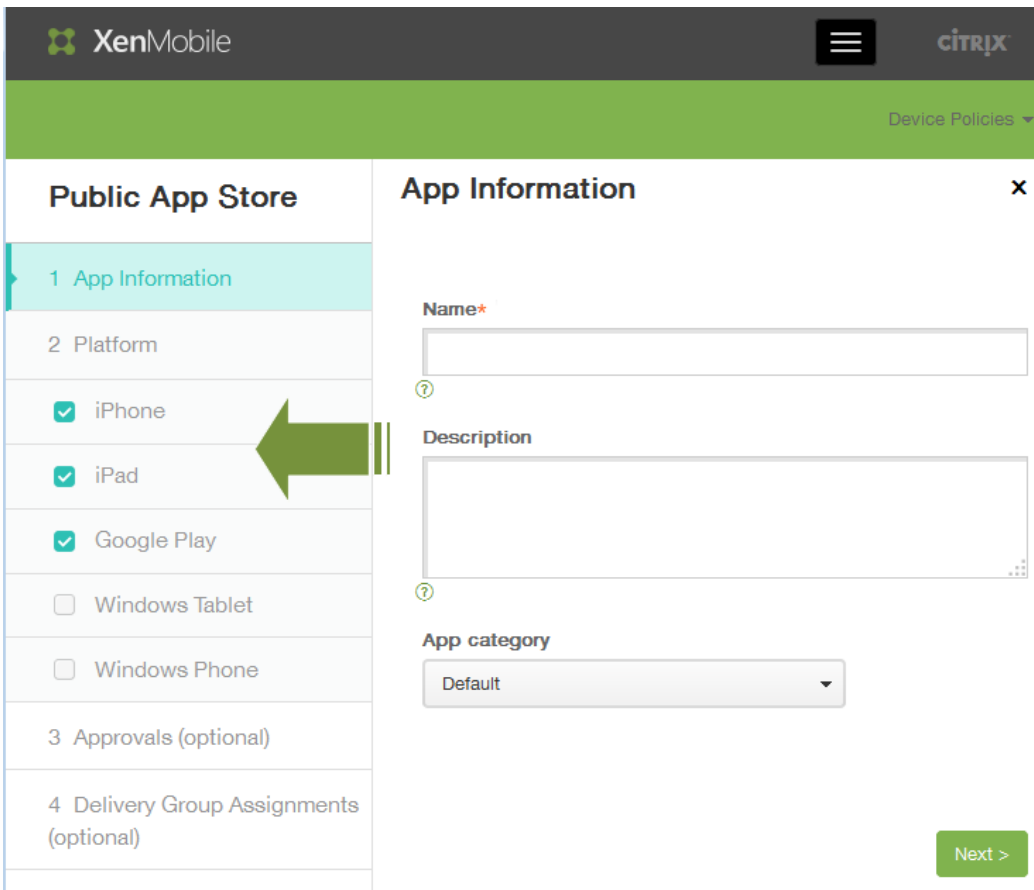
1. In the XenMobile console, click Configure > Apps. The Apps screen appears.



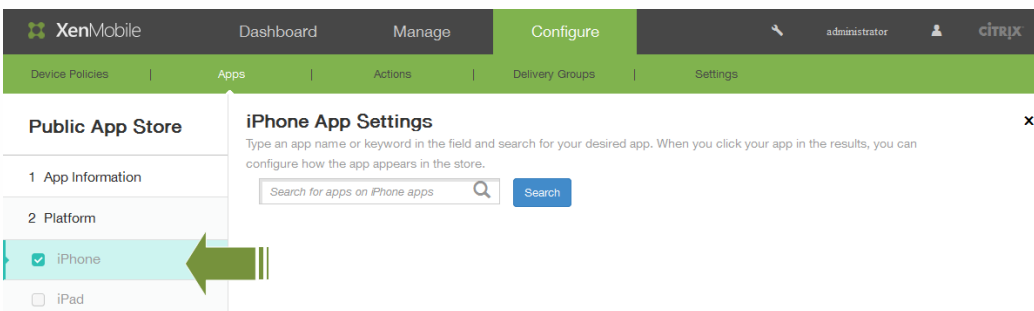
2. Click Add.
3. In the Add App screen, click Public App Store.



4. On the App Information page, enter a Name and then provide a Description for the app. These fields are used for internal purposes. If you are adding apps for multiple devices (for example, iPhone, iPad, and GooglePlay), use the check boxes in the left portion of the screen to select them.



5. In the App category list, click the App category.
6. Click Next.
7. On the Platform screen for the platform type, in the search field, type an app name or keyword to locate the app you want to add. For example, if you chose to add an iPhone app, the XenMobile console searches for apps related to iPhone devices. If you chose to add apps for multiple platforms, results appear for each one.

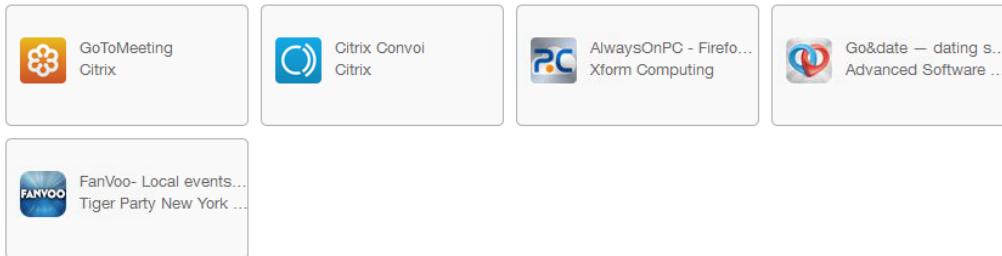


In the following figure, apps matching the search criteria appear (for example, GoToMeeting).

iPhone App Settings

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

Search results for goto meeting in iPhone apps



Didn't find the app you were looking for?

8. Click an app in the results to configure how it appears in the store. On the App Details screen, the fields are pre-populated with information related to the chosen app (including the name, description, version number and image associated). If necessary, change the name and description for the app.

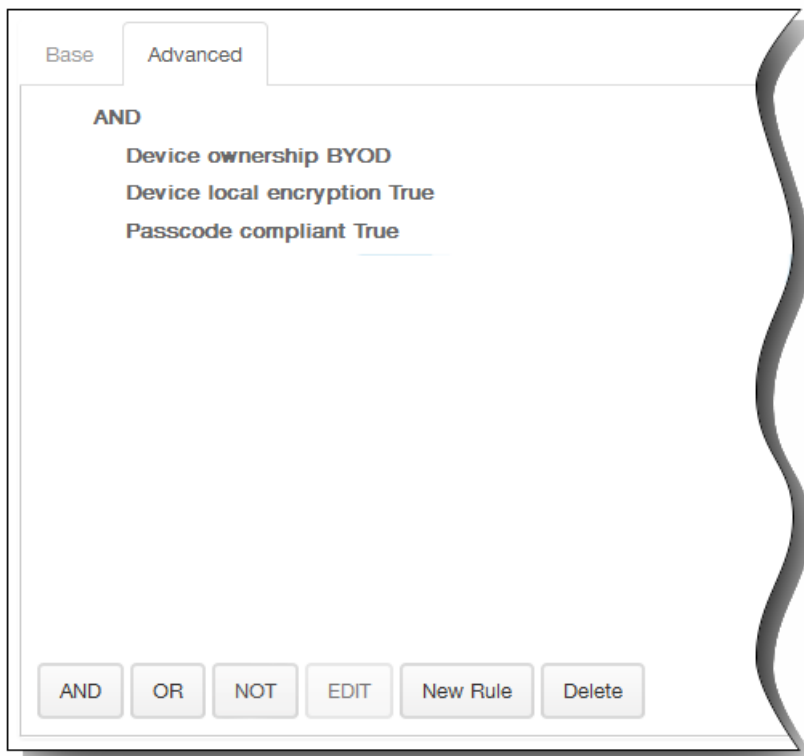
App Details

Name*	<input type="text" value="GoToMeeting"/>
Description*	<input type="text" value="Download the free GoToMeeting app and join, host or schedule a GoToMeeting session right from your iPhone, iPad or iPod touch."/>
Version	<input type="text" value="6.3.0.671"/>
Image	
Remove app if MDM profile is removed	<input checked="" type="checkbox"/>
Prevent app data backup	<input checked="" type="checkbox"/>
Paid app	<input type="checkbox"/>

1. In Remove app if MDM profile is removed, click ON if you would like to remove the app if the MDM profile is removed. By default, this option is ON.
2. In Prevent app data backup, click ON if you would like to prevent the app from backing up data. By default, this option is ON.
3. In **Paid app**, the field is preconfigured and cannot be changed.
9. Expand Deployment Rules. The Base tab appears by default.



1. In the lists, click options to determine when the app should be deployed.
 1. You can choose to deploy the app when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.

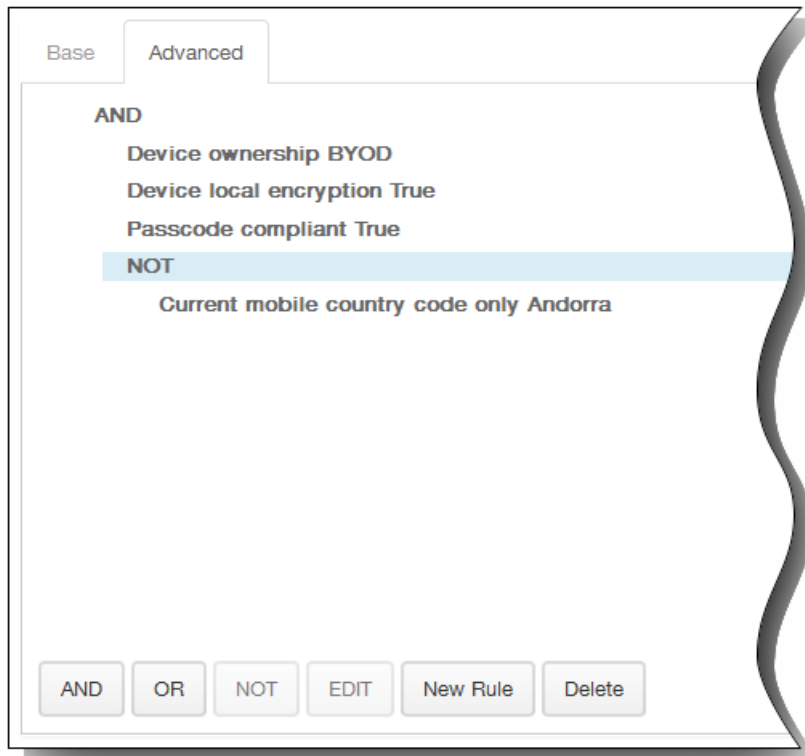


The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, the device must be passcode compliant, and the device mobile country code cannot be only Andorra.



10. Expand Worx Store Configuration to add an FAQ for the app, or add screen captures to help classify the app in the Worx Store. The graphic you upload must be of the type PNG. You cannot upload a GIF or JPEG image.

▼ Worx Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots



Allow app ratings

Allow app comments

In Allow app ratings, click ON to permit a user to rate the app.

11. In Allow app comments, click ON to permit users to comment about the selected app.

12. Expand Volume Purchase Program and then in the VPP license list, click Upload a VPP license file if you want to enable XenMobile to apply a VPP license for the app.

▼ Volume Purchase Program

VPP License

Do not use VPP

- Click Next and then repeat steps 7 to 16 for each platform type for which you want to add public apps.
- On the Approvals page, in the Workflow to use list, optionally click a workflow or click Create a new workflow.

Public App Store

1 App Information

2 Platform

iPhone

iPad

Google Play

Windows Tablet

Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

Approvals (optional)

Apply an existing workflow or create a new workflow to require approval before allowing users to access the app.

Workflow to Use: Create a new workflow

Name:

Description:

Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level

Select Active Directory domain: Select an option

Find additional required approvers: Search

Selected additional required approvers:

Back Next >

- When you create a new workflow, the XenMobile console changes to display configuration options for the approval process. Each of these fields is described in the following steps. Configure these fields if you need approval for creating user account. The uploaded VPP file only applies to the legacy Volume Purchase Program from Apple. For the new program, the license handling is automatic based on licenses purchased by the company. This information is configured in **Settings > iOS VPP**.

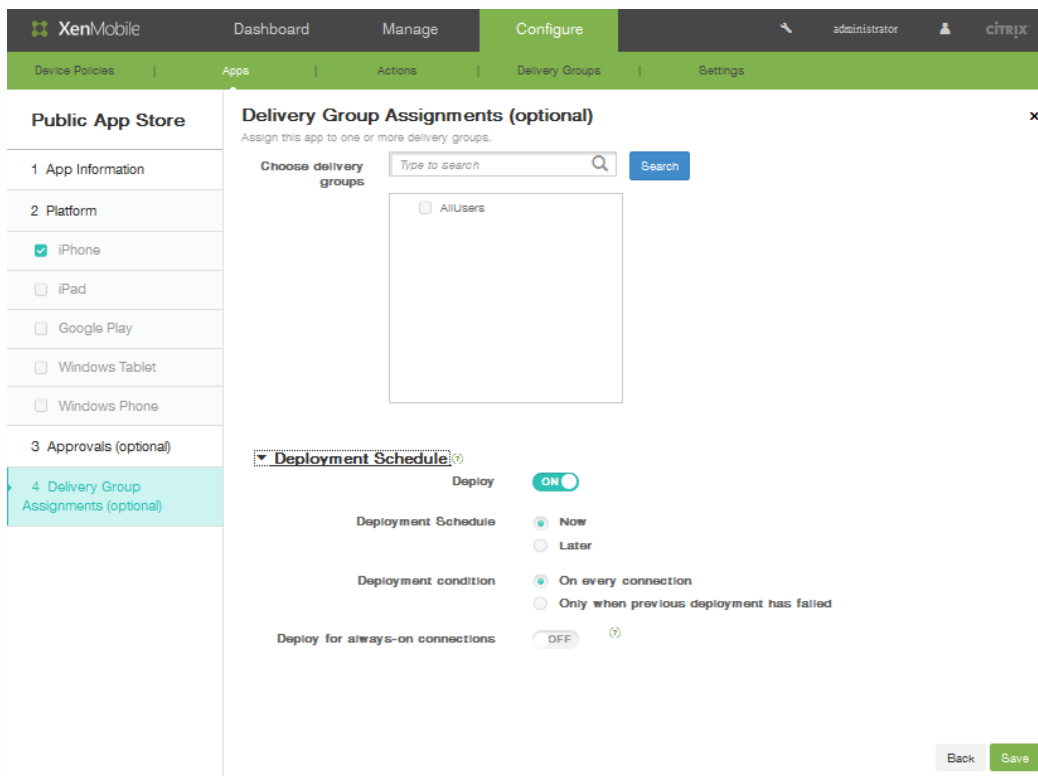
- Specify a **name** for the workflow.
- Optionally enter a **description**.
- In **Email Approval Templates** field, click a notification option. Click the eye **icon** to preview the template you chose.

Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level

Preview template

- In **Levels of manager approval**, click the level from None to 3. .
 - In **Select Active Directory domain**, click the domain.
 - In Find additional required approvers, optionally enter additional required approvers and then click Search.
- Click Next.
 - On the **Delivery Groups Assignment** page, optionally assign the app to one or more delivery groups.



18. In Choose delivery groups, search for a delivery group (or groups). Select the **All Users** checkbox to assign the app to each XenMobile user.
19. Expand Deployment Schedule to further refine the delivery group.
 1. Deploy: Click ON to enable a deployment schedule.
 2. Deployment Schedule: Click Now or Later to set the deployment schedule .
 3. Deployment condition: Click to deploy the app on every connection, or only when the previous deployment has failed.
 4. In Deploy for always-on connections, click ON to deploy when the always-on connection policy is set.
 Note: This option applies when you have also configured global background deployment keys in the Server Properties section in the Settings area of the XenMobile console. The always-on scheduled policy is not available for iOS devices
20. Click Save. The XenMobile console applies the app information.

To add a Web and SaaS app to XenMobile

Feb 13, 2015

Using the XenMobile console, you can provide users with single sign-on (SSO) to your mobile, enterprise, web, and SaaS apps. You can enable apps for SSO by using application connector templates. For a list of connector types available in XenMobile, see [List of Application Connector Types](#).

You can also you build your own connector in XenMobile.

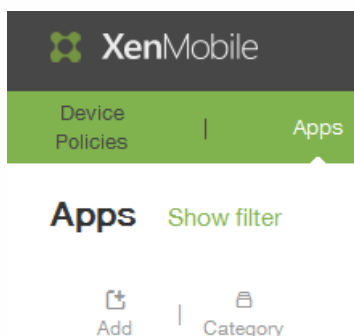
You configure a connector by providing the following parameters:

- Different names (optional). Use any app connector displayed in the console. Box connector is no longer supported.
- Description of the app.
- Web address by using the fully qualified domain name (FQDN). For example, if you want to add LinkedIn to your app list, you go to <http://www.linkedin.com> and then click Sign in. When the logon page appears, you use the web address, <https://www.linkedin.com> when configuring the app.
- Location of the app, either on the Internet or in your internal network.
- Credentials for SSO. Users can use the app credentials.
- Category for the app. Categories allow you to organize apps in Worx Home.
- App policies for each app you configure in XenMobile.
- Workflow approval settings for all apps that include specifying the individuals who can approve the user account.
- A delivery group of users to which you want to assign the app.

If an app is available for SSO only, when you finish configuring the preceding settings, you save the settings and the app appears on the Apps tab in the XenMobile console.

To add an app connector in XenMobile

1. In the XenMobile web console, click Configure > Apps. The Apps page opens.
2. On the Apps page, click **Add**.



3. On the **Add App** page, click **Web & SaaS**.

Add App



Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

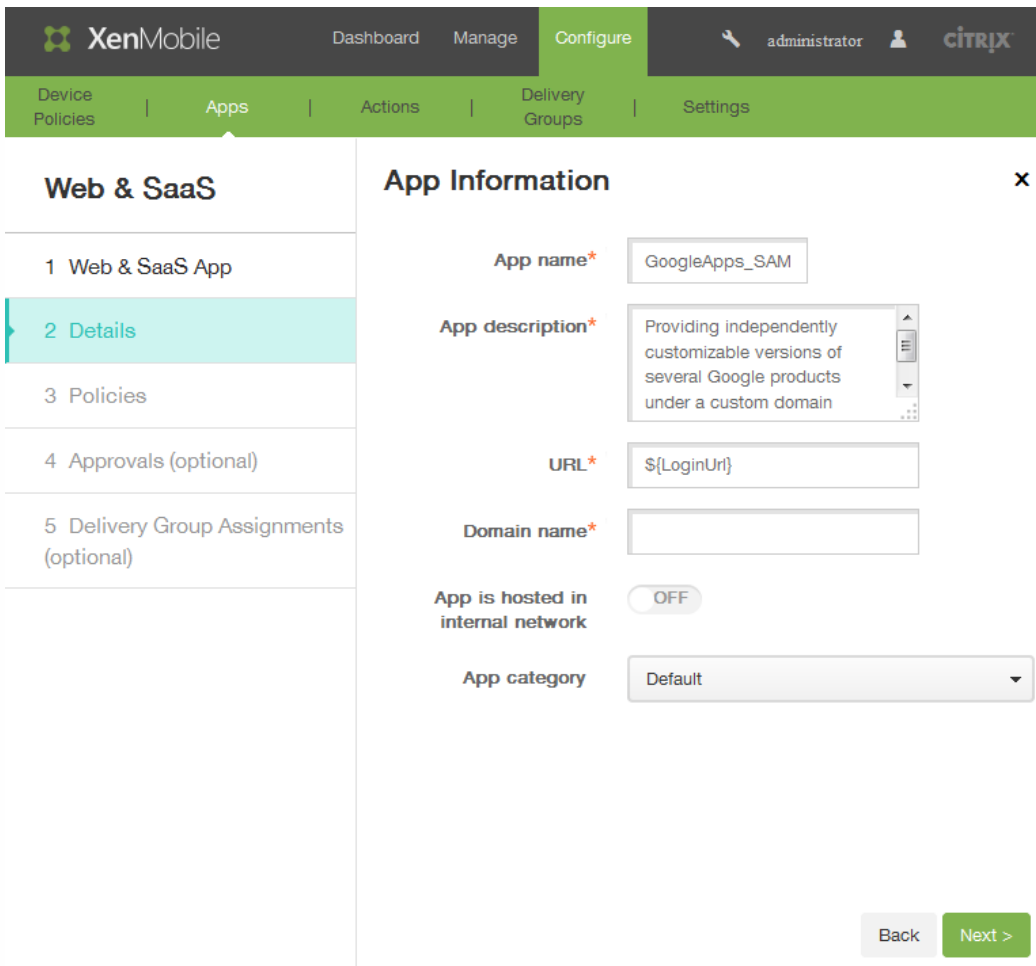
4. On the App Information page, click Choose from existing connector or Create a new connector.

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'Dashboard', 'Manage', and 'Configure'. The left sidebar has 'Web & SaaS' selected, with sub-items: '1 Web & SaaS App', '2 Details', '3 Policies', '4 Approvals (optional)', and '5 Delivery Group Assignments (optional)'. The main content area is titled 'App Information' and contains the following elements:

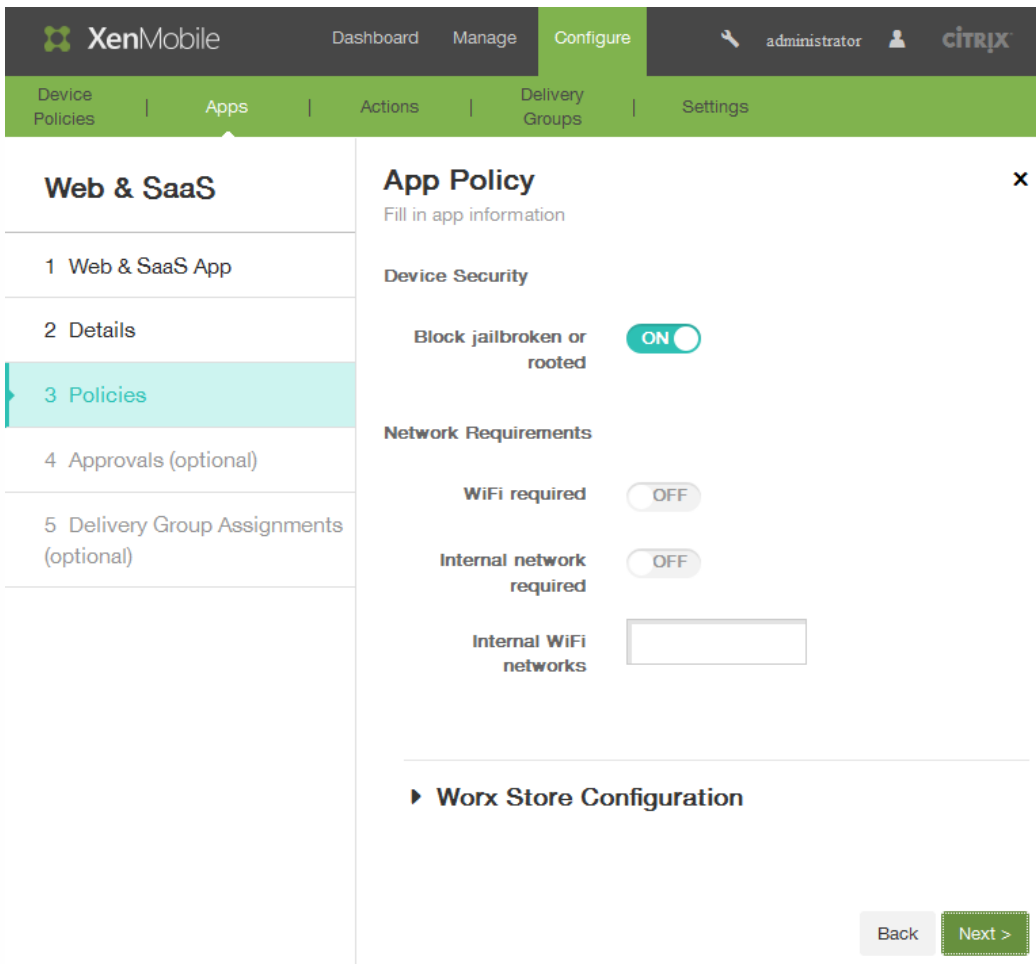
- App Connector** section with two radio buttons: 'Choose from existing connectors' (selected) and 'Create a new connector'.
- App Connectors** section with a search bar and a 'Search' button.
- A table listing app connectors with their counts:

Connector Name	Count
E	1
EchoSign_SAML	
G	3
GoogleApps_SAML	
GoogleApps_SAML_JDP	
Globoforce_SAML	
L	1
Lynda_SAML	

5. If you click an app in the list, the Details page opens. The App name, Description, and URL are pre-populated.



1. In URL, if applicable, type the Web address of the app or keep the default address.
2. In App is hosted in internal network, click ON if the app is running on a server in your internal network. If users connect from a remote location to the internal app, they must connect through NetScaler Gateway. Setting this option to ON adds the VPN keyword to the app and allows users to connect through NetScaler Gateway.
3. In the App category list, click a category.
4. In the Enable user management for provisioning click On. If you are using the Globalforce_SAML connector, you must turn on Enable user management for provisioning to ensure seamless SSO integration.
6. Click Next. The Policies page appears.



7. In Device Security in Block jailbroken or rooted, click ON.
8. In Network Requirements, configure the following settings:
 1. In WiFi required, click ON and then specify internal WiFi networks.
 2. In Internal network required, click ON if an internal network is required to run the app.
9. Expand Worx Store Configuration to add an FAQ for the app, or add screen captures to help classify the app in the Worx Store. The graphic you upload must be of the type PNG. You cannot upload a GIF or JPEG image.

▼ Worx Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

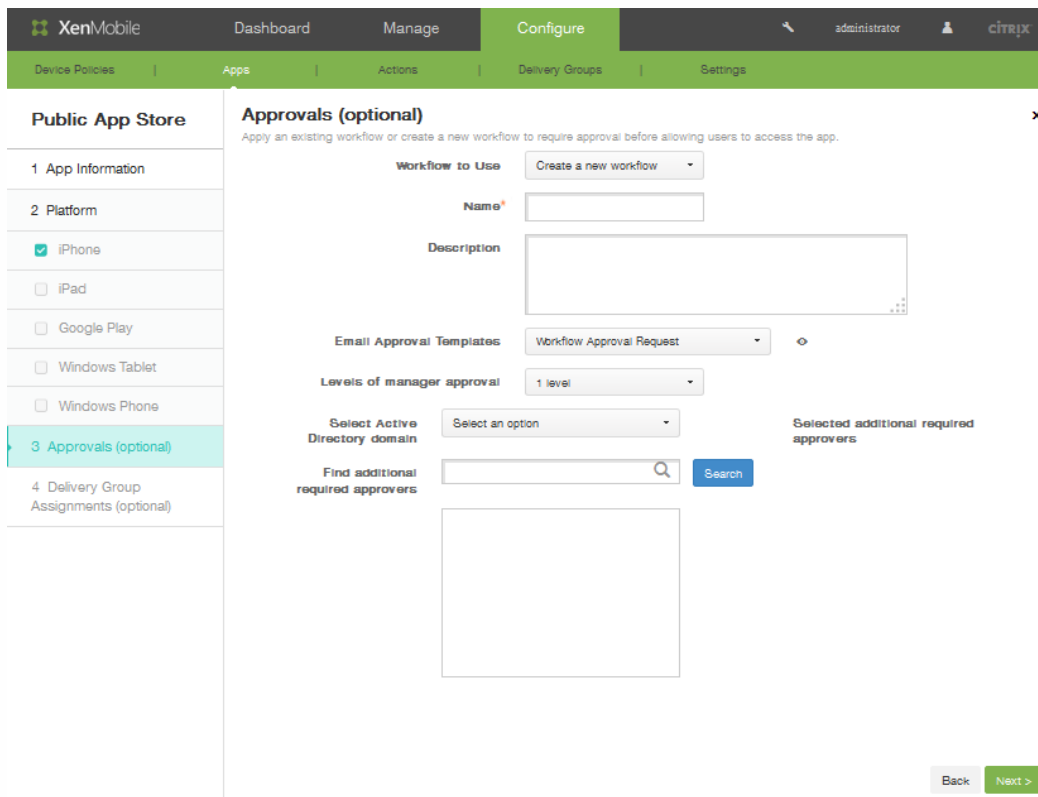
Browse...	Browse...	Browse...	Browse...	Browse...
-----------	-----------	-----------	-----------	-----------

Allow app ratings

Allow app comments

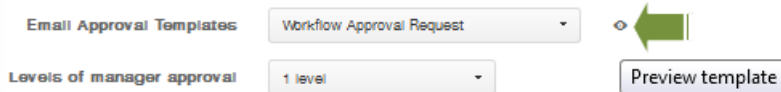
In Allow app ratings, click ON to permit a user to rate the app.

10. In Allow app comments, click ON to permit users to comment about the selected app.
11. Click Next.
12. On the Approvals page, in the Workflow to use list, optionally click a workflow or click Create a new workflow.



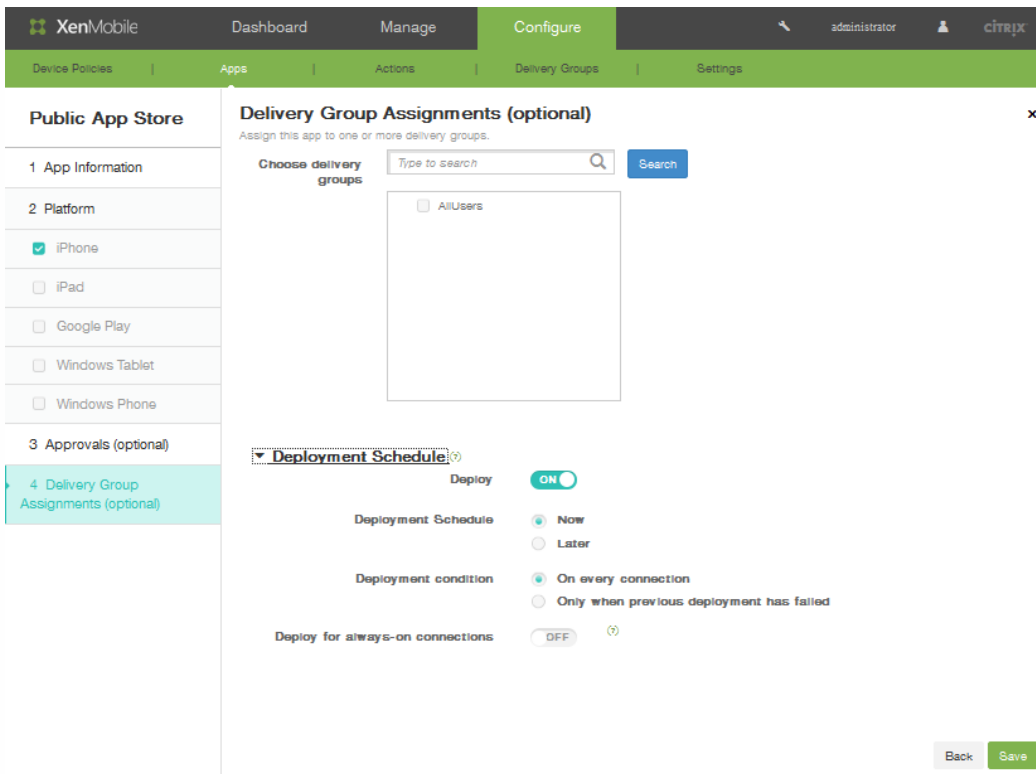
13. When you create a new workflow, the XenMobile console changes to display configuration options for the approval process. Each of these fields is described in the following steps. Configure these fields if you need approval for creating user account.

1. Specify a **name** for the workflow.
2. Optionally enter a **description**.
3. In **Email Approval Templates** field, click a notification option. Click the eye **icon** to preview the template you chose.

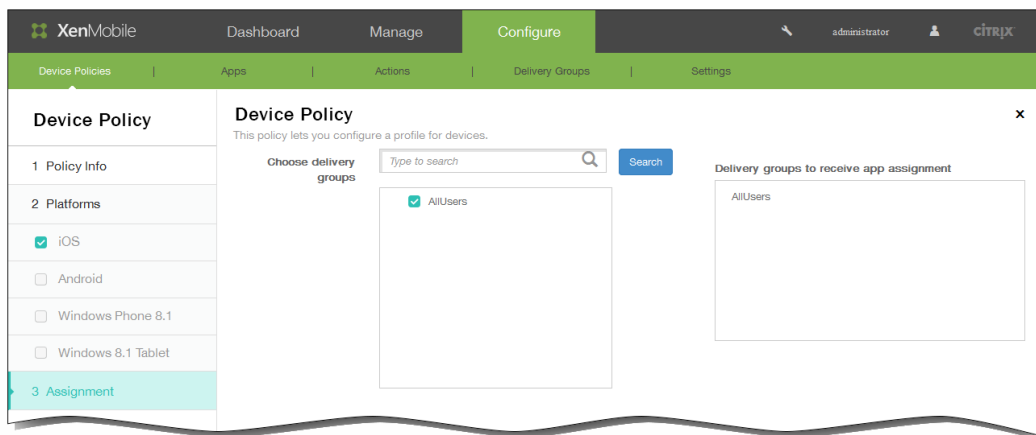


4. In **Levels of manager approval**, click the level from None to 3.
5. In **Select Active Directory domain**, click the domain.
6. In Find additional required approvers, optionally enter additional required approvers and then click Search.

14. Click Next.
15. On the **Delivery Groups Assignment** page, optionally assign the app to one or more delivery groups.

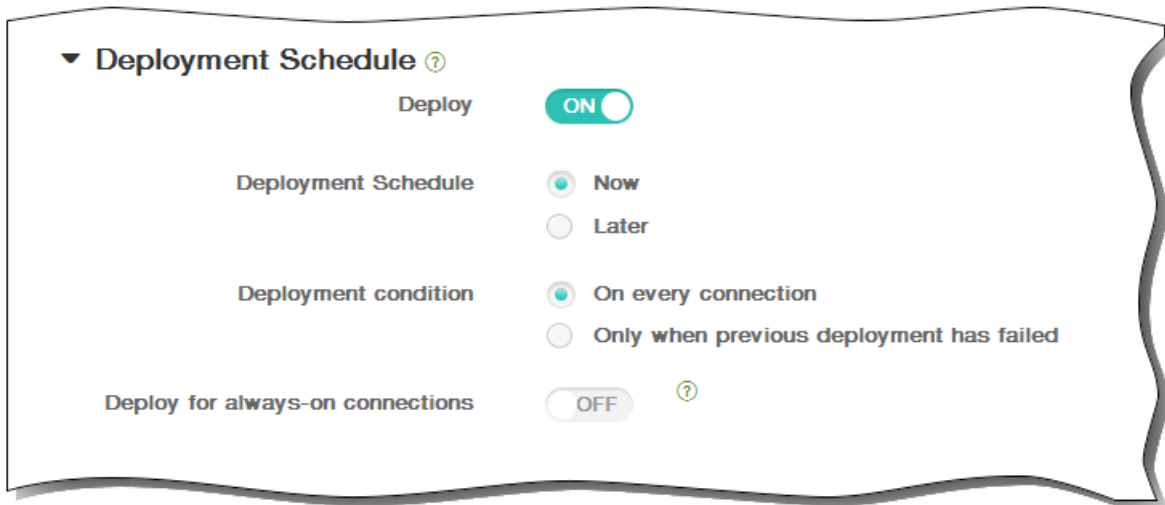


16. Next to Choose delivery groups, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand Delivery groups to receive app assignment list.



17. Expand Deployment Schedule and then configure the following settings:
 1. 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.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
 Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



The screenshot shows a configuration panel titled "Deployment Schedule" with a help icon. It contains four settings:

- Deploy**: A toggle switch set to "ON".
- Deployment Schedule**: Radio buttons for "Now" (selected) and "Later".
- Deployment condition**: Radio buttons for "On every connection" (selected) and "Only when previous deployment has failed".
- Deploy for always-on connections**: A toggle switch set to "OFF" with a help icon.

18. Click **Save**.

List of Application Connector Types

Feb 11, 2015

The following table lists the connectors and the types of connectors that are available within XenMobile. The table also indicates if the connector supports user account management, which enables you to create new accounts automatically or by using a workflow.

Connector name	SSO SAML	Supports user account management
EchoSign_SAML	Y	Y
Globoforce_SAML		Note: When using this connector, you must enable User Management for Provisioning to ensure seamless SSO integration.
GoogleApps_SAML	Y	Y
GoogleApps_SAML_IDP	Y	Y
Lynda_SAML	Y	Y
Office365_SAML	Y	Y
Salesforce_SAML	Y	Y
Salesforce_SAML_SP	Y	Y
SandBox_SAML	Y	
SuccessFactors_SAML	Y	
ShareFile_SAML	Y	
ShareFile_SAML_SP	Y	
WebEx_SAML_SP	Y	Y

To add an enterprise app to XenMobile

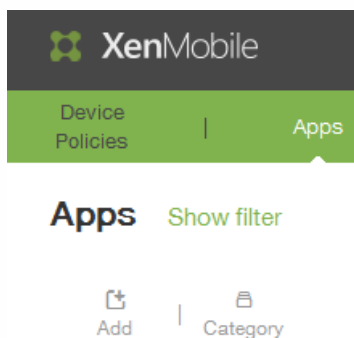
Feb 26, 2015

Enterprise apps in XenMobile represent native apps that are not wrapped with the MDX Toolkit and do not contain the policies associated with MDX apps. You can upload an enterprise app on the Apps tab in the XenMobile console. Enterprise apps support the following platforms (and corresponding file types):

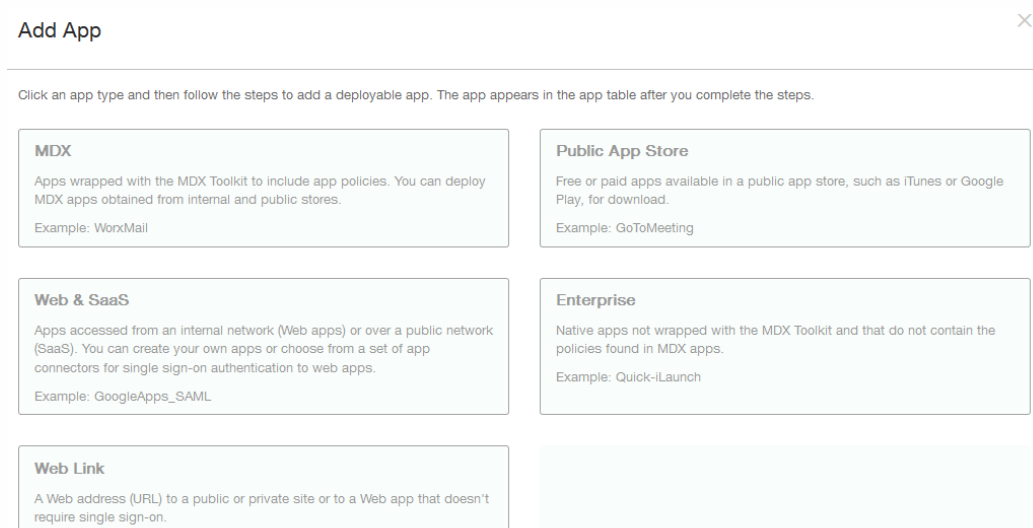
- iOS (.ipa file)
- Android (.apk file)
- Samsung KNOX (.apk file)
- Windows Phone (.xap or .appx file)
- Windows Tablet (.appx file)

To create an enterprise application

1. In the XenMobile console, click the Configure > Apps.
2. On the Apps page, click **Add**.

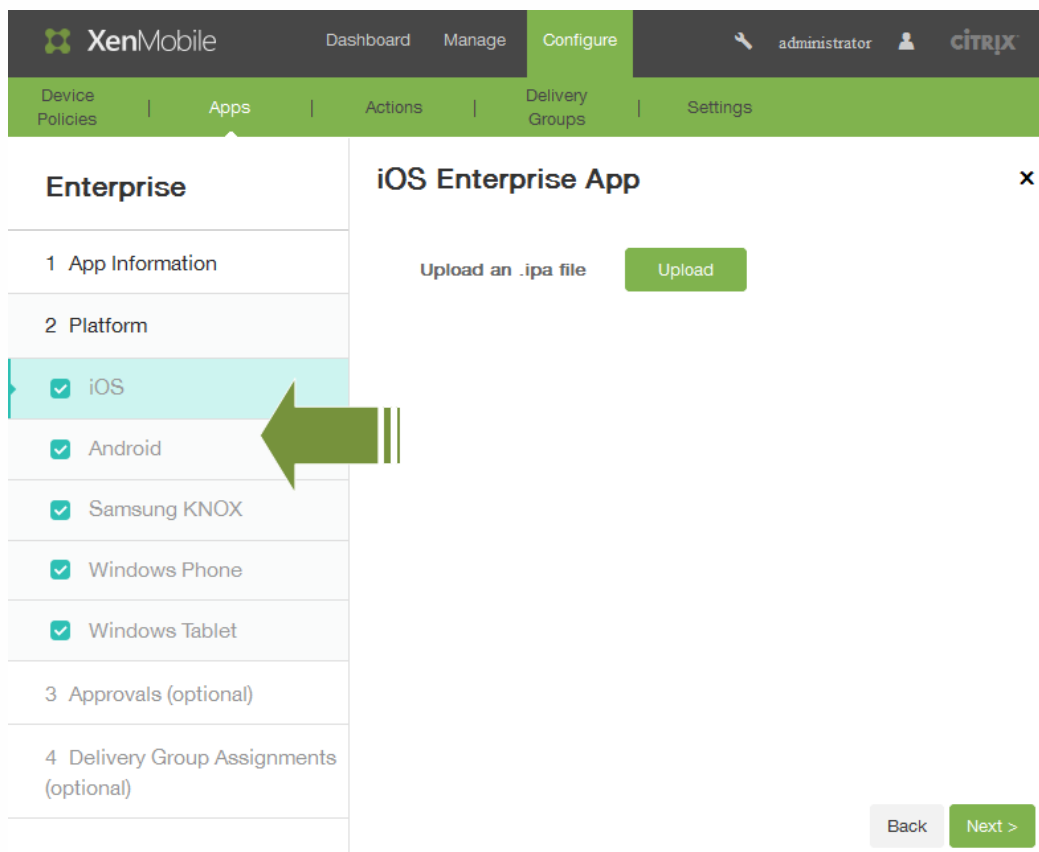


3. On the Add App page, click **Enterprise**.

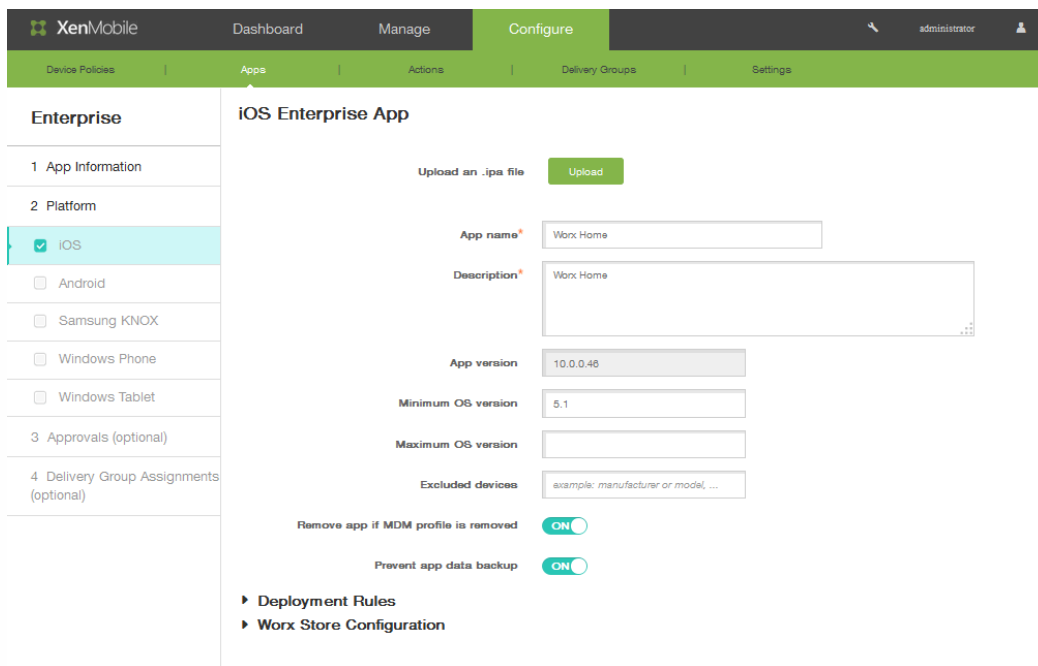


4. In the catalog, click New enterprise app.
5. On the App Information page, complete the following:

1. Name: Type a name for the app.
2. Description: Type a description for the app.
Note: If you want to configure a second app with the same web address, you must give the app a different name.
3. In **App category**, click a category and then click Next.
6. In the Platform area on the left-hand side of the page, select the device platforms for which you want to add the app (for example, iOS or Android).



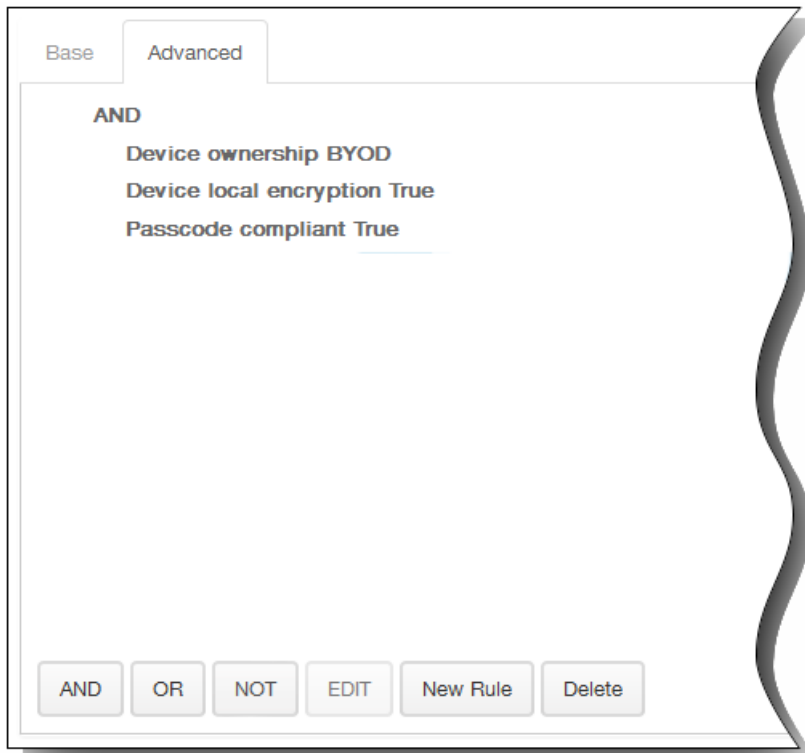
7. Click Upload to browse to the location of the file and then click Next. The app information page appears for the platform type. The fields are pre-populated with information related to the chosen app (including the name, description, version number and image associated). If necessary, change the name and description for the app.



8. In Remove app if MDM profile is removed, click ON if you would like to remove the app if the MDM profile is removed. By default, this option is ON.
9. In Prevent app data backup, click ON if you would like to prevent the app from backing up data. By default, this option is ON.
10. Expand Deployment Rules. The Base tab appears by default.



1. In the lists, click options to determine when the app should be deployed.
 1. You can choose to deploy the app when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.

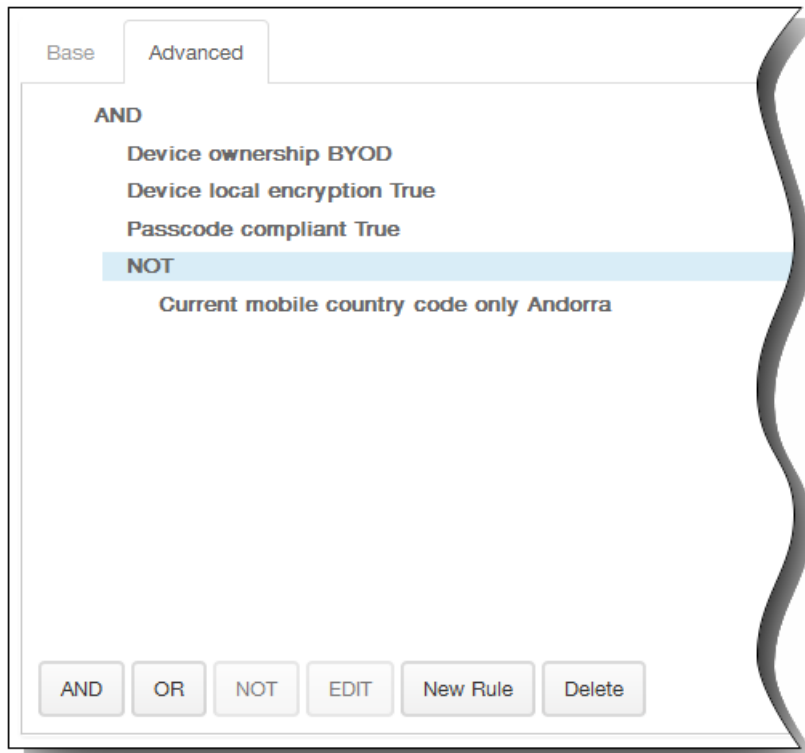
1. Click AND, OR, or NOT.

2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, the device must be passcode compliant, and the device mobile country code cannot be only Andorra.



- Expand Worx Store Configuration to add an FAQ for the app, or add screen captures to help classify the app in the Worx Store. The graphic you upload must be of the type PNG. You cannot upload a GIF or JPEG image.

▼ Worx Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

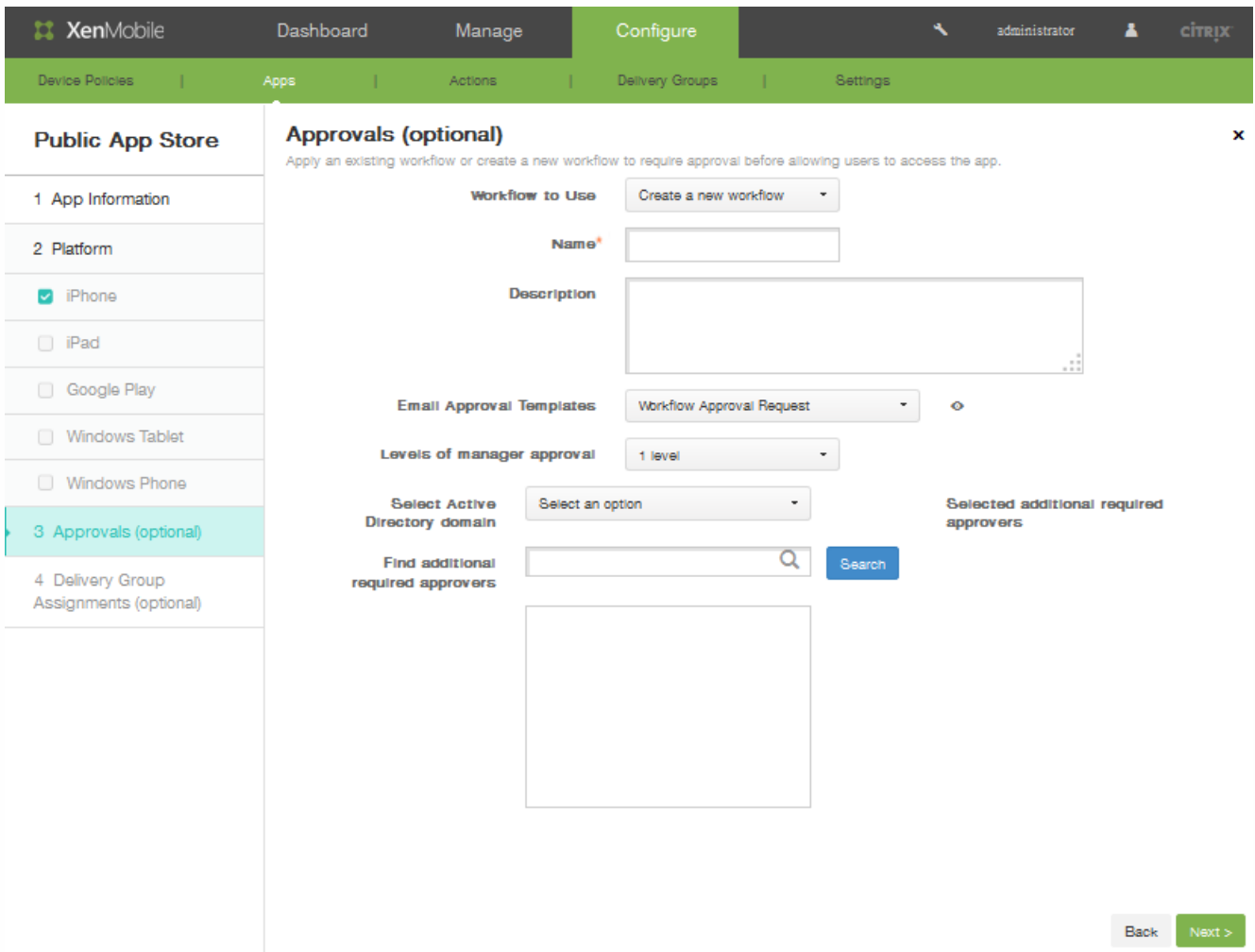
Browse...	Browse...	Browse...	Browse...	Browse...
-----------	-----------	-----------	-----------	-----------

Allow app ratings ON

Allow app comments ON

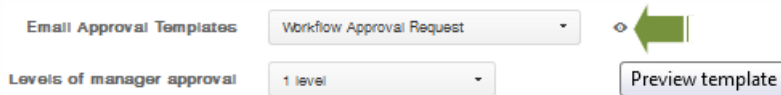
In Allow app ratings, click ON to permit a user to rate the app.

- In Allow app comments, click ON to permit users to comment about the selected app.
- Click Next.
- On the Approvals page, in the Workflow to use list, optionally click a workflow or click Create a new workflow.

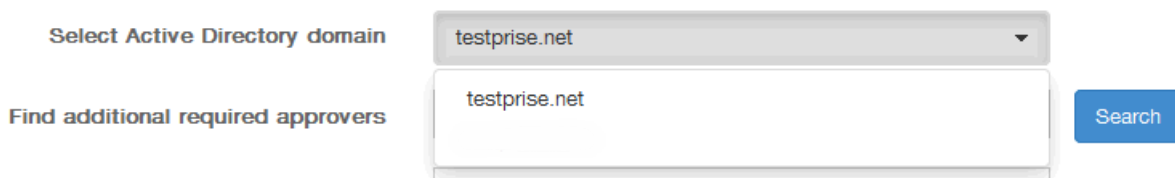


15. When you create a new workflow, the XenMobile console changes to display configuration options for the approval process. Each of these fields is described in the following steps. Configure these fields if you need approval for creating user account.

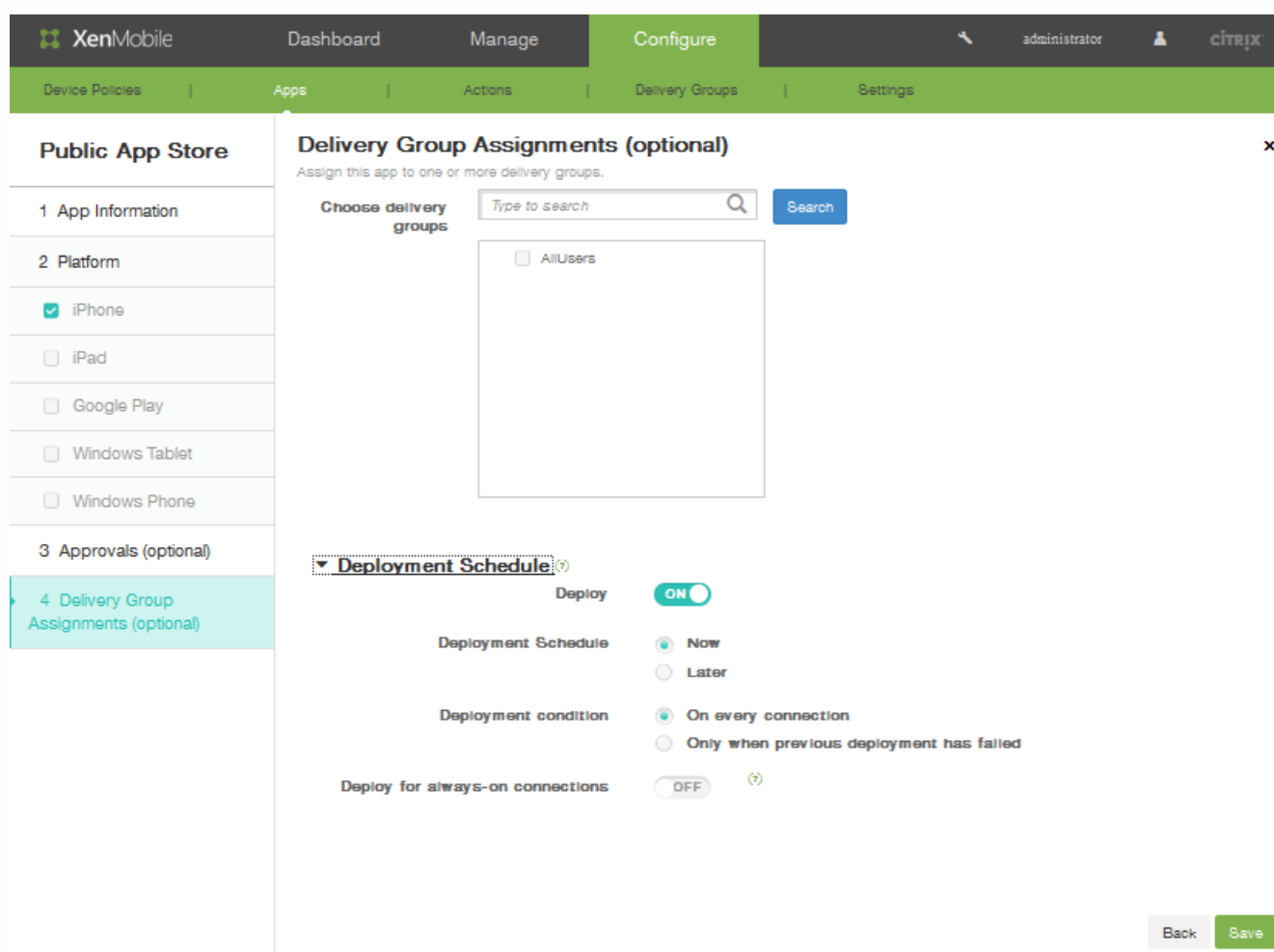
1. Specify a **name** for the workflow.
2. Optionally enter a **description**.
3. In **Email Approval Templates** field, click a notification option. Click the eye **icon** to preview the template you chose.



4. In **Levels of manager approval**, click the level from None to 3.
5. In **Select Active Directory domain**, select the domain from the drop down menu; only joined Active Directory domains appear in this list (for example, testprise.net):



6. In Find additional required approvers, optionally enter additional required approvers and then click Search.
16. On the **Delivery Groups Assignment** page, optionally assign the app to one or more delivery groups.



17. In Choose delivery groups, search for a delivery group (or groups). Select the **All Users** checkbox to assign the app to each XenMobile user.
18. Expand Deployment Schedule to further refine the delivery group.
 1. Deploy: Click ON to enable a deployment schedule.
 2. Deployment Schedule: Click Now or Later to set the deployment schedule .
 3. Deployment condition: Click to deploy the app on every connection, or only when the previous deployment has failed.
 4. In Deploy for always-on connections, click ON to deploy when the always-on connection policy is set.
 Note: This option applies when you have also configured global background deployment keys in the Server Properties section in the Settings area of the XenMobile console. The always-on scheduled policy is not available for iOS devices.
19. Click Save.

To add a Web Link app to XenMobile

Feb 13, 2015

In XenMobile, you can establish a Web address (URL) to a public or private site, or to a Web app that doesn't require single sign-on (SSO).

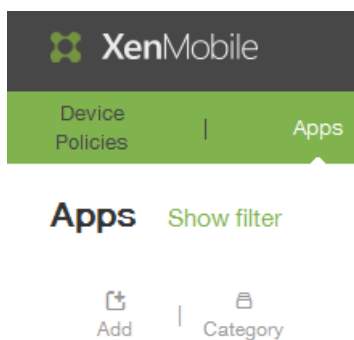
You can configure web links from the Apps tab in the XenMobile console. When you finish configuring the web link, the link appears as a link icon in the list in the Apps table. When users log on with Worx Home, the link appears with the list of available apps and desktops.

To add the link, you provide the following information:

- Name for the link
- Description of the link
- Web address (URL)
- Category
- Role
- Image in .png format (optional)

To add a Web link in XenMobile

1. Configure > Apps. The Apps page opens.
2. On the Apps page, click Add.



3. On the Add App page, click Web Link.

Add App



Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

The App Information page appears.

- The App name, Description, and URL are pre-populated.

The screenshot shows the XenMobile interface with the 'Configure' tab selected. The 'App Information' section is active, displaying the following fields:

- App name:** Web Link
- App description:** Use this connector to add any web URL to be displayed using XenMobile App Controller, for those apps that don't have SSO support.
- URL:** \$\$url\$\$
- App is hosted in internal network:** ON (toggle switch)
- App category:** Default (dropdown menu)
- Image:** Use default, Upload your own app image

A 'Next >' button is located at the bottom right of the form.

- In URL, if applicable, type the Web address of the app or keep the default address.
- In App is hosted in internal network, click ON if the app is running on a server in your internal network. If users connect from a remote location to the internal app, they must connect through NetScaler Gateway. Setting this option to ON adds the VPN keyword to the app and allows users to connect through NetScaler Gateway.
- In the App category list, click a category.
- If you want to associate your own thumbnail image with the connector, select Upload your own app image. Click Browse to locate the desired image:

Image

- Use default
- Upload your own app image

No file selected.



Images must be of the type PNG.

- Expand Worx Store Configuration to add an FAQ for the app, or add screen captures to help classify the app in the Worx Store. The graphic you upload must be of the type PNG. You cannot upload a GIF or JPEG image.

▼ Worx Store Configuration

App FAQ

App screenshots

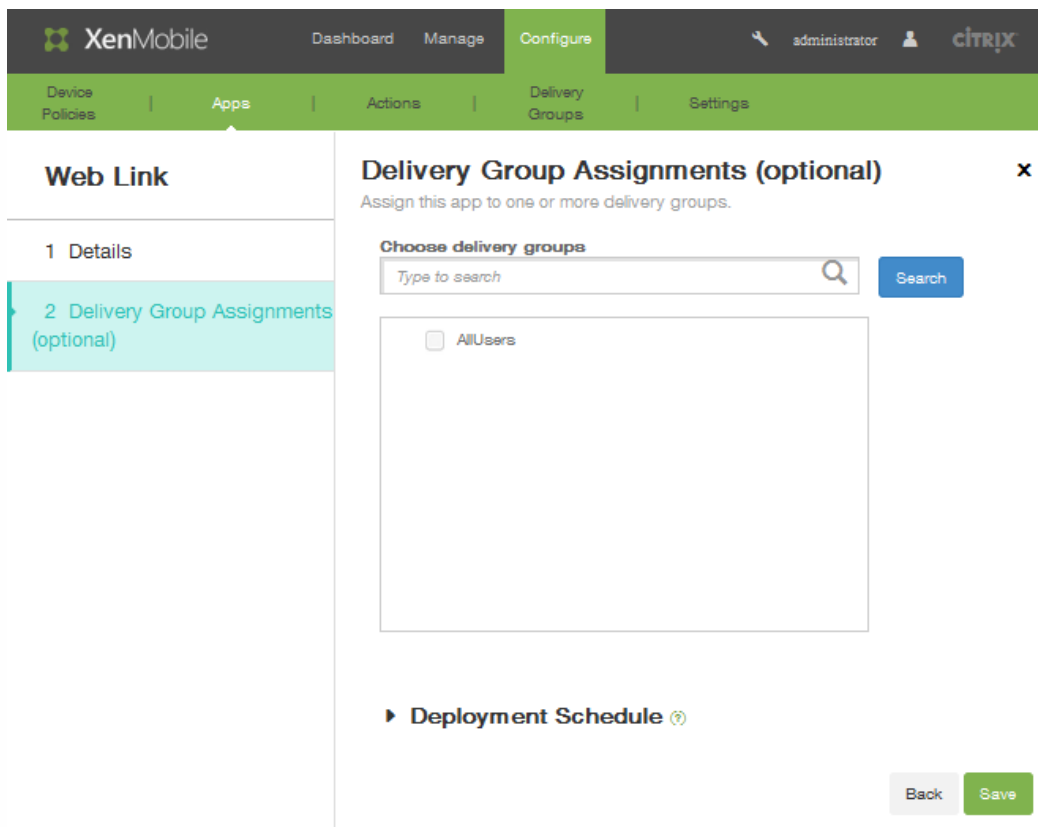
<input type="button" value="Browse..."/>	<input type="button" value="Browse..."/>	<input type="button" value="Browse..."/>	<input type="button" value="Browse..."/>	<input type="button" value="Browse..."/>
--	--	--	--	--

Allow app ratings

Allow app comments

In Allow app ratings, click ON to permit a user to rate the app.

- In Allow app comments, click ON to permit users to comment about the selected app.
- Click Next.
- On the **Delivery Groups Assignment** page, optionally assign the app to one or more delivery groups.



9. In Choose delivery groups, search for a delivery group (or groups). Select the **All Users** checkbox to assign the app to each XenMobile user.
10. Expand Deployment Schedule to further refine the delivery group.



1. Deploy: Click ON to enable a deployment schedule.
2. Deployment Schedule: Click Now or Later to set the deployment schedule.
3. Deployment condition: Click to deploy the app on every connection, or only when the previous deployment has failed.
4. In Deploy for always-on connections, click ON to deploy when the always-on connection policy is set.
Note: This option applies when you have also configured global background deployment keys in the Server Properties section in the Settings area of the XenMobile console. The always-on scheduled policy is not available for iOS devices.
11. Click Save.

To create and manage workflows

Feb 13, 2015

You can use workflows to manage the creation and removal of user accounts. Before you can use a workflow, you need to identify individuals in your organization who have the authority to approve user account requests. Then, you can use the workflow template to create and approve user account requests.

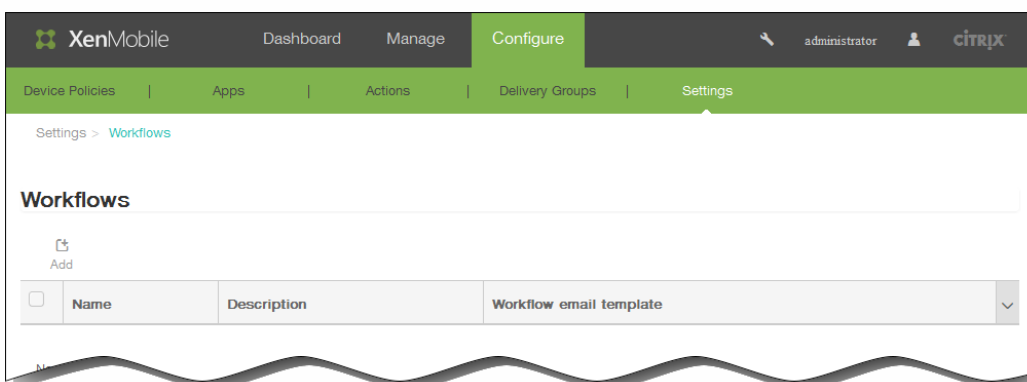
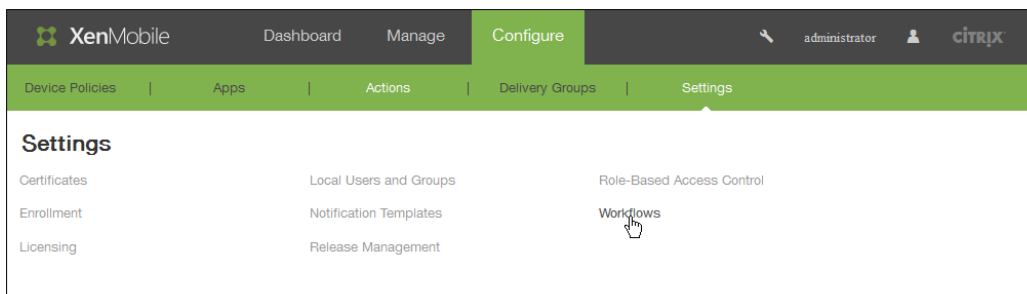
When you configure XenMobile for the first time, you configure workflow email settings. You must configure workflow email settings to use workflows. You can change workflow email settings at any time. These settings include the email server, port, email address, and whether the request to create the user account requires approval or not.

You can configure workflows in two places in XenMobile:

- In the Workflows page in the XenMobile console. On the Workflows page, you can configure multiple workflows for use with app configurations. When you configure workflows on the Workflows page, you can select the workflow when you configure the app.
- When you configure an application connector, in the app, you provide a workflow name and then configure the individuals who can approve the user account request. See [Adding Apps to XenMobile](#).

You can assign up to three levels for manager approval of user accounts. If you need other people to approve the user account, you can search and select additional people to approve by using the person's name or email address. When XenMobile finds the person, you then add the him or her to the workflow. All individuals in the workflow receive emails to approve or deny the new user account.

1. In the XenMobile console, click Configure > Settings > Workflows.



The Workflows page appears.

2. On the Workflows page, click Add. The Add Workflow page appears.

3. On the Add Workflow page, in the Name field, type a unique name for the workflow.
4. In Description, optionally type a description for the workflow.
5. In the Email Approval Templates list, select the email approval template to be assigned. You create email templates in the Notification Templates section under Settings in the XenMobile console. When you click the eye icon to the right of this field, the following tip appears.

Email Title	Email Content
Workflow Approval Request for an Application	Please approve the application \${applicationName} for your staff by clicking the following link. Thank you for spending the time to approve the application.

6. In the Levels of manager approval list, select the number of levels of manager approval required for this workflow.
7. In the Select Active Directory domain list, select the appropriate Active Directory domain to be used for the workflow.

8. Next to Find additional required approvers, type the additional required person's name in the search field and then click Search. Names originate in Active Directory.
9. When the person's name appears in the field, select the check box next to his or her name. The person's name and email address appear in the Selected additional required approvers list. To remove a person from the Selected additional required approvers list, do one of the following:
 - Click Search to see a list of all the people in the selected domain.
 - Type a full or partial name in the search box, and then click Search to limit the search results.Persons in the Selected additional required approvers list have check marks next to their name in the search results list. Scroll through the list and clear the check box next to each name you want to remove.
10. Click Save.
The created workflow appears on the Workflows page.

After you create the workflow, you can view the workflow details, view the apps associated with the workflow, or delete the workflow. You cannot edit a workflow after you create the workflow. If you need a workflow with different approval levels or approvers, you must create a new workflow.

To view details and delete a workflow

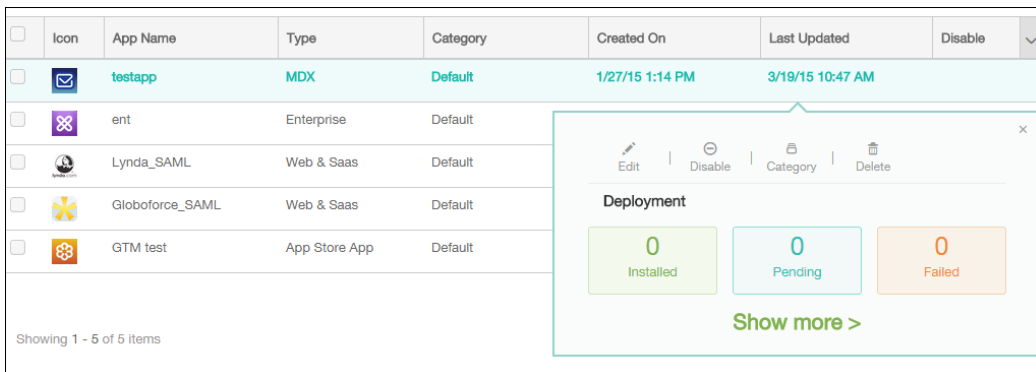
1. On the Workflows page, in the list of existing workflows, select a specific workflow by clicking the row in the table or by checking the check box next to workflow.
2. To delete a workflow, click Delete. A confirmation dialog box appears. Click Delete again.
Important: You cannot undo this operation.

Upgrading an App in XenMobile

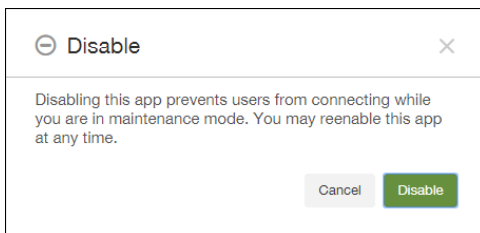
Mar 23, 2015

To upgrade an app in XenMobile, you disable the app in the XenMobile console, and then you upload the new version of the app.

1. In the XenMobile console, click Configure > Apps.
2. For managed devices (devices enrolled in XenMobile for mobile device management), skip to step 3. For unmanaged devices (devices enrolled in XenMobile for enterprise app management purposes only), do the following:
 1. In the Apps table, click to select the app you want to update and then in the menu that appears, click Disable.



2. On the confirmation dialog box, click Disable.



The app shows the status of Disabled in the Apps table.

Note: Disabling an app puts the app in maintenance mode. Users cannot connect to the app again after they log off, while an app is disabled. Disabling an app is an optional setting, but Citrix recommends disabling the app to avoid issues with app functionality. Issue may arise due to policy updates, for example, or if users request a download at the same time you are uploading the app to XenMobile.

3. Click to select the app and then in the menu that appears, click Edit. The platform you originally chose for the app appears selected.
4. On the App Information page, optionally you can change the Name, Description, or App category, and then click Next.
5. Click Upload to select the file you want to upload to replace the current app and then click Next.

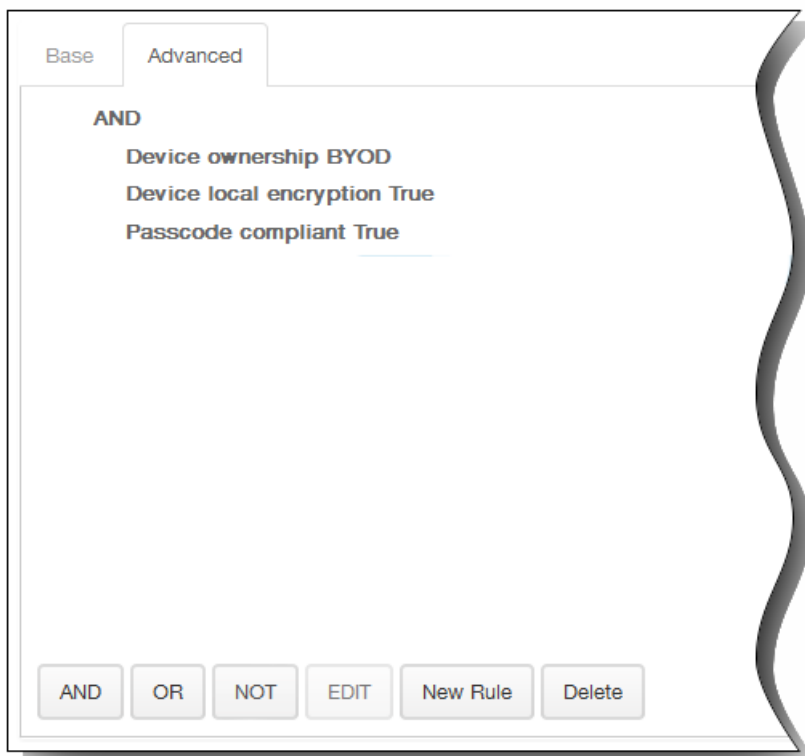


The app uploads to XenMobile. Optionally, you can change the app details and policy settings.

6. Click Next and then in Steps 8 through 14, leave the settings as is, or make changes related to the upgrade.
7. Expand Deployment Rules. The Base tab appears by default.



1. In the lists, click options to determine when the app should be deployed.
 1. You can choose to deploy the app when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



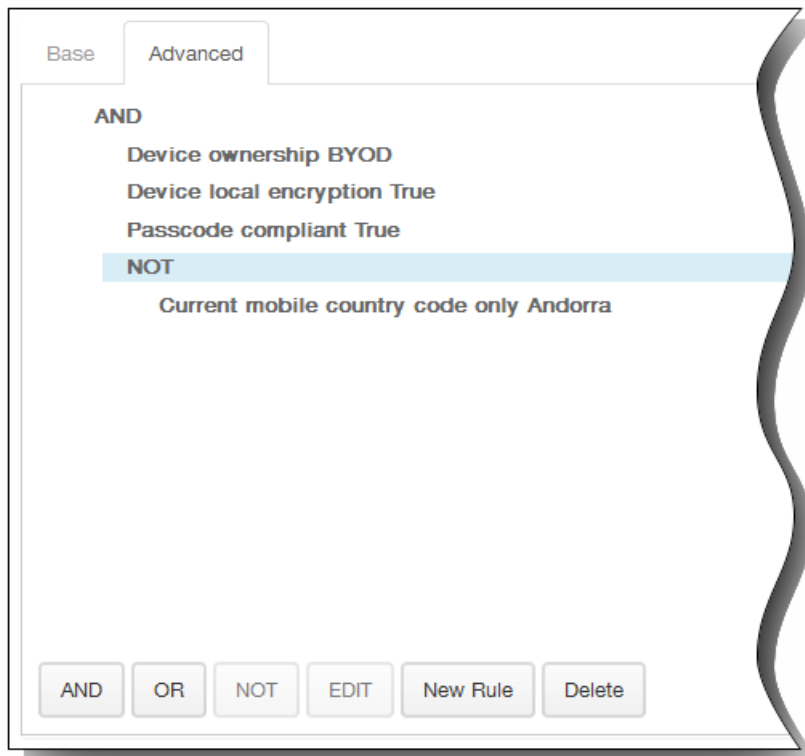
The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.
 1. Click AND, OR, or NOT.
 2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove

the condition.

3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, the device must be passcode compliant, and the device mobile country code cannot be only Andorra.



8. Expand Worx Store Configuration to add an FAQ for the app, or add screen captures to help classify the app in the Worx Store. The graphic you upload must be of the type PNG. You cannot upload a GIF or JPEG image.

▼ Worx Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots



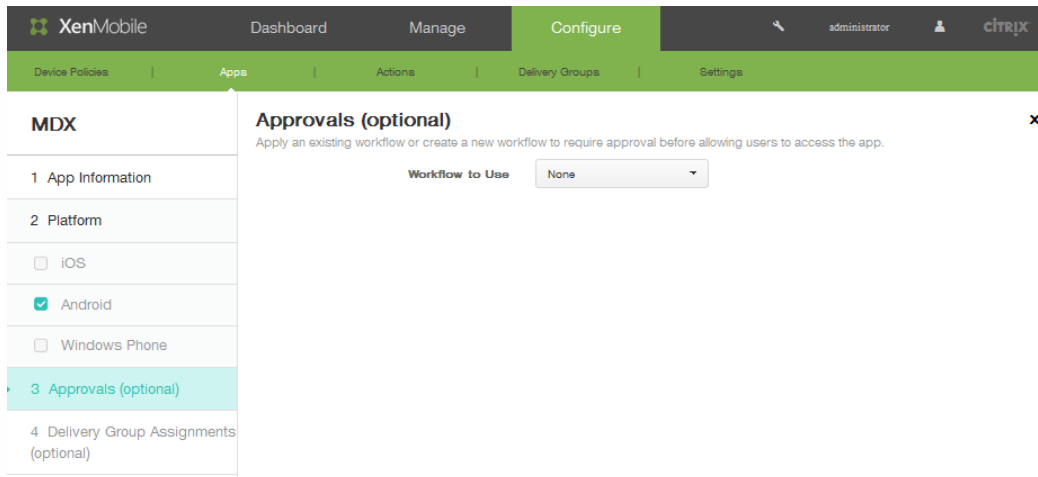
Allow app ratings

Allow app comments

In Allow app ratings, click ON to permit a user to rate the app.

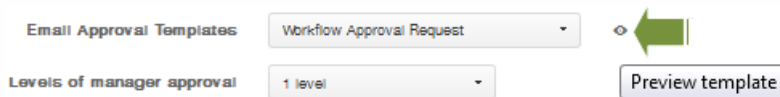
9. In Allow app comments, click ON to permit users to comment about the selected app.

10. Click Next. The Approvals screen appears.

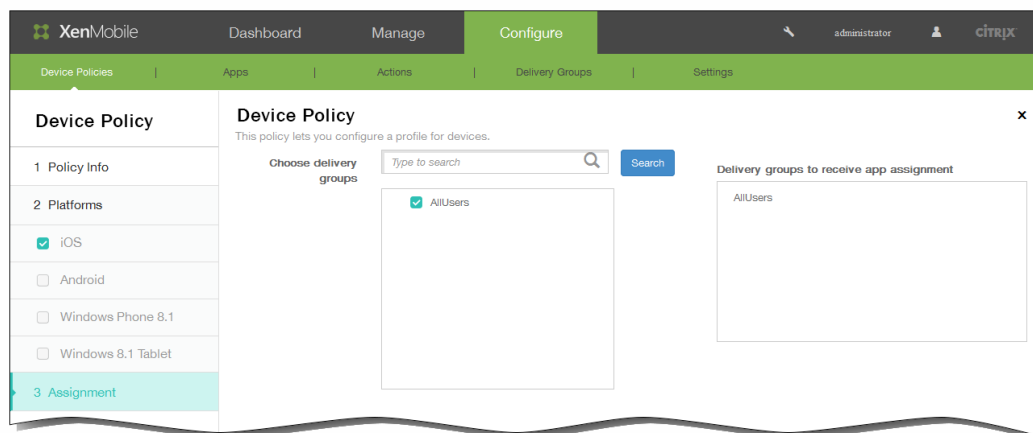


11. When you create a new workflow, the XenMobile console changes to display configuration options for the approval process. Each of these fields is described in the following steps. Configure these fields if you need approval for creating user accounts.

1. Specify a **name** for the workflow.
2. Optionally enter a **description**.
3. In **Email Approval Templates** field, click a notification option. Click the **eye icon** to preview the template you chose.

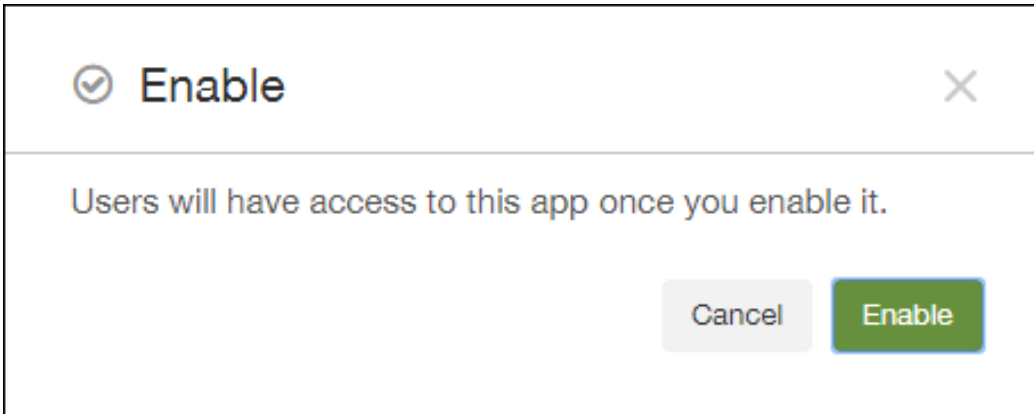


4. In **Levels of manager approval**, click the level from None to 3. .
 5. In **Select Active Directory domain**, click the domain.
 6. In Find additional required approvers, optionally enter additional required approvers and then click Search.
12. Click Next.
13. Next to Choose delivery groups, type 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.



14. Click Save. The Apps page appears.

15. If you disabled the app in step 2, do the following:
 1. In the Apps table, click to select the app you updated and then in the menu that appears, click Enable.
 2. In the confirmation message that appears, click Enable.



Users can now access the app again and receive a notification prompted them to upgrade the app.

MDX App Policies at a Glance

Feb 12, 2016

For a table listing the MDX app policies for iOS, Android, and Windows Phone with notes on restrictions and Citrix recommendations, see [MDX Apps Policies at a Glance](#) in the MDX Toolkit documentation.

Note: Worx Home refreshes policies during certain actions. For details, see [Administering Worx Home](#).

Automated Actions

Mar 09, 2015

You create automated actions in XenMobile to program a reaction to events, user or device properties, or the existence of apps on user devices. When you create an automated action, you establish the effect on the user's device when it is connected to XenMobile based on triggers in the action. When an event is triggered, you can send a notification to the user to correct an issue before more serious action is taken.

For example, if you want to detect an app that you have previously blacklisted (for example, Words with Friends), you can specify a trigger that sets the user's device out of compliance when Words with Friends is detected on their device. The action then notifies them that they must remove the app to bring their device back into compliance. You can set a time limit for how long to wait for the user to comply before taking more serious action, such as selectively wiping the device.

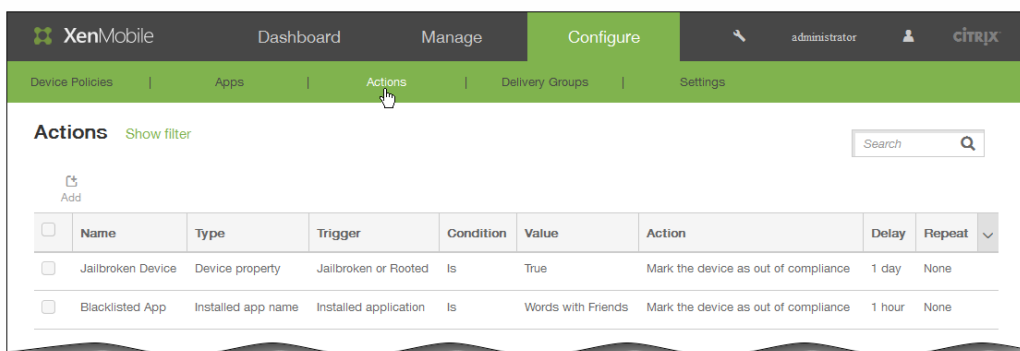
The effects that you set to happen automatically range from the following:

- Fully or selectively wiping the device.
- Setting the device to out of compliance.
- Revoking the device.
- Sending a notification to the user to correct an issue before more severe action is taken.

Note: Before you can notify users, you must have configured notification servers in Settings for SMTP and SMS so that XenMobile can send the messages, see [Notifications in XenMobile](#). Also, set up any notification templates you plan to use before proceeding. For details on setting up notification templates, see [To create or update notification templates in XenMobile](#).

This topic explains how to add, edit, and filter automated actions in XenMobile.

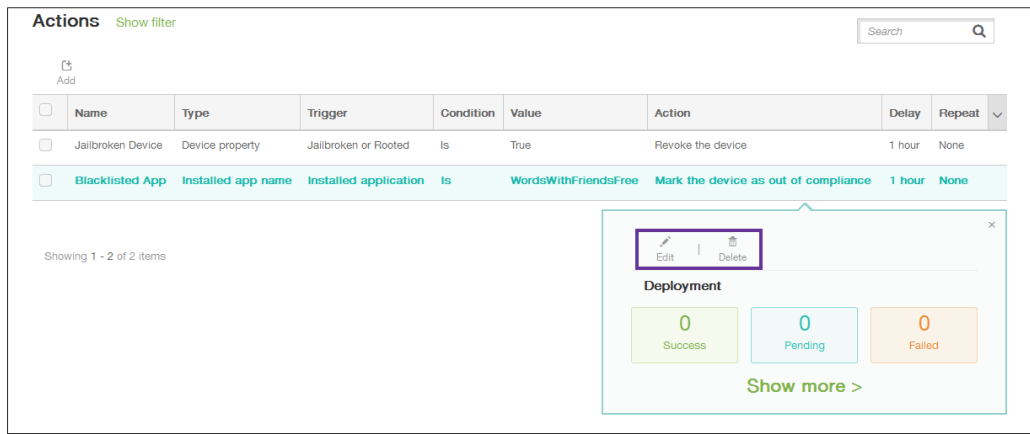
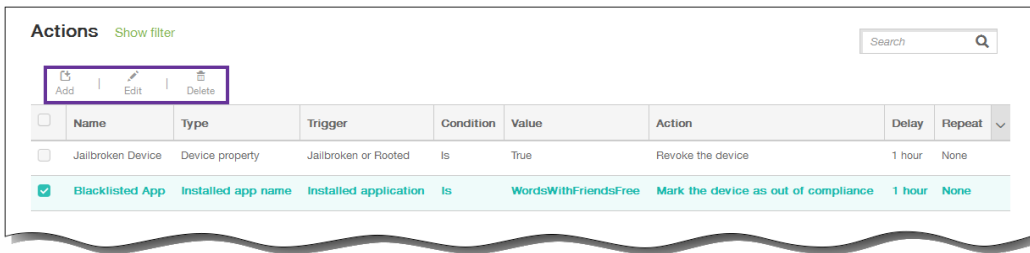
1. From the XenMobile console, click Configure > Actions. The Actions page appears.



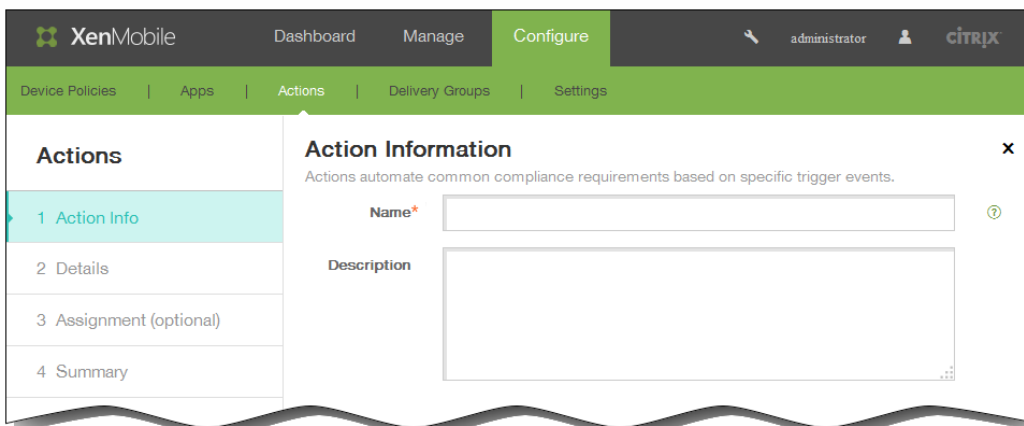
2. On the Actions page, do one of the following:

- Click Add to add a new action.
- Select an existing action to edit or delete. Click the option you want to use.

Note: When you select the check box next to an action, the options menu appears above the action list; when you click anywhere else in the list, the options menu appears on the right side of the listing.



The Action Information page appears.

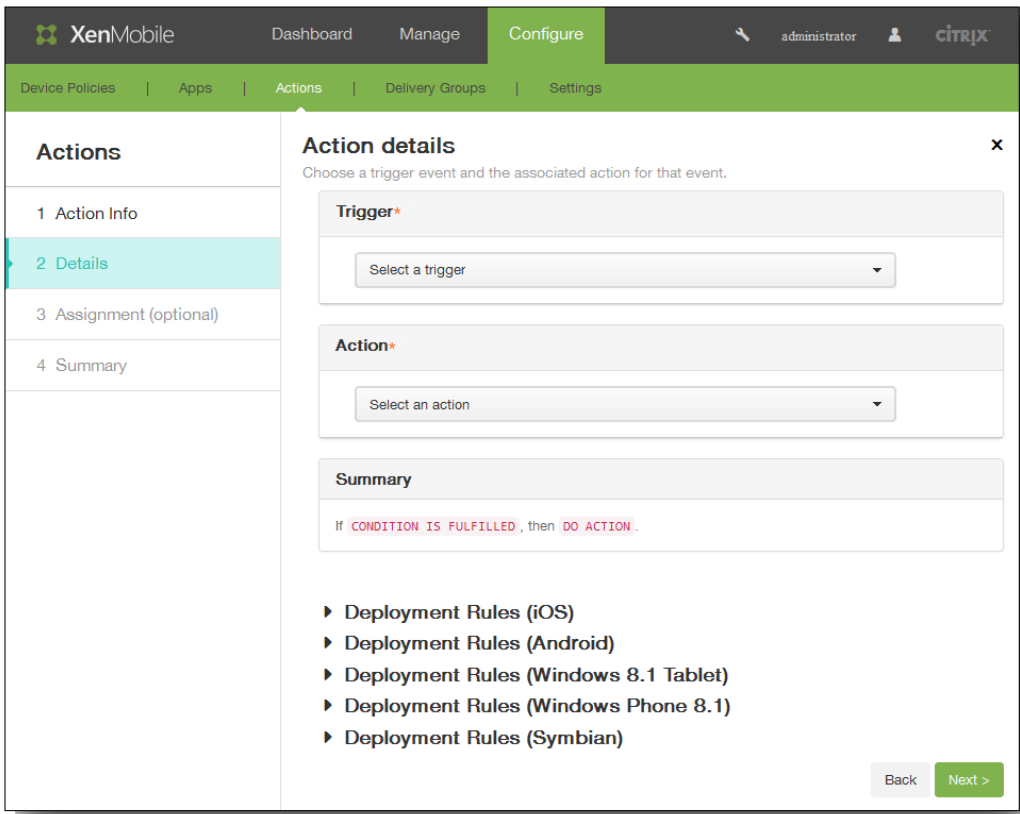


3. On the Action Information page, enter or modify the following information:

1. Name: Type a name to uniquely identify the action. This field is required.
2. Description: Describe what the action is meant to do.

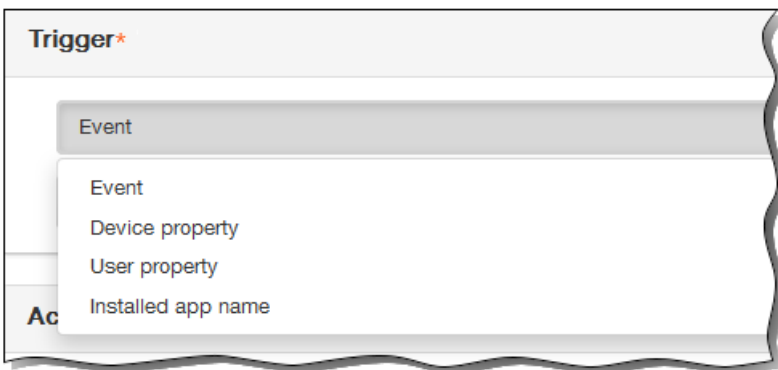
4. Click Next. The Action details page appears.

Note: The following example shows how to set up an Event trigger. If you select a different trigger, the resulting options will be different from those shown here.

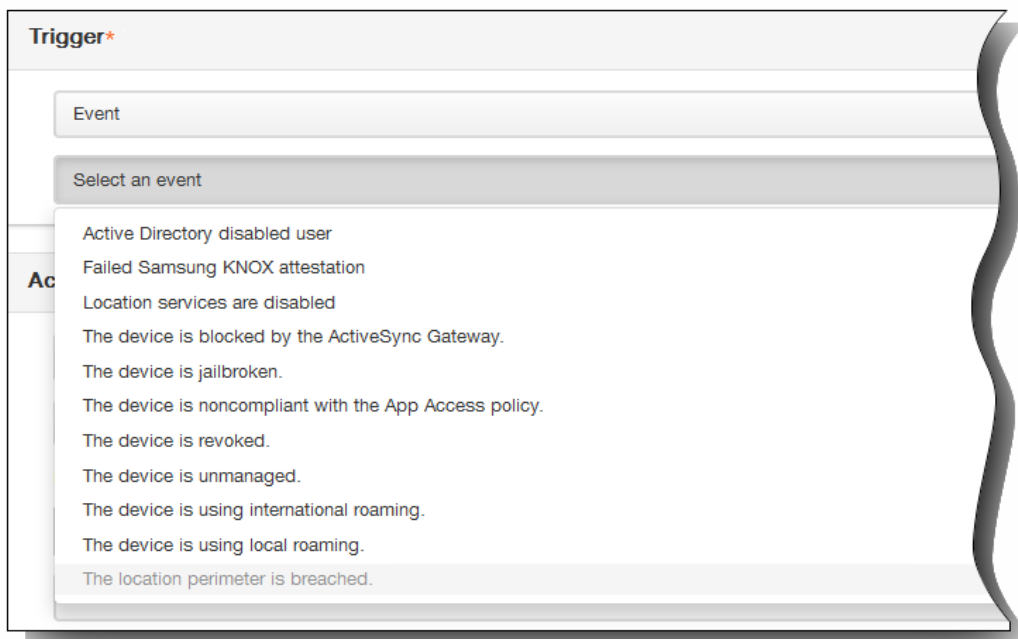


5. On the Action details page, enter or modify the following information:

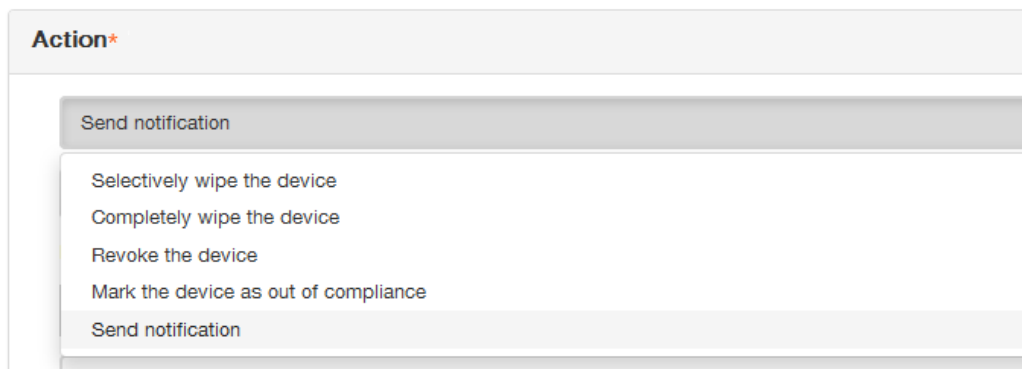
1. In the Trigger list, click the event trigger type for this action. The meaning of each trigger is as follows:
 - Event: Reacts to a predefined event.
 - Device property: Checks for a device attribute on the device gathered in MDM mode and reacts to it.
 - User property: Reacts to a user attribute, usually from Active Directory.
 - Installed app name: Reacts to an app being installed. Requires the app inventory policy to be enabled on the device. The app inventory policy is enabled on all platforms by default. For details, see [To add an app inventory device policy](#).



2. In the next list, click the response to the trigger.



3. In the Action list, click the action to be performed when the trigger criterion is met. With the exception of Send notification, you choose a time frame in which users can resolve the issue that caused the trigger. If the issue is not resolved within that time frame, the selected action is taken.



The remainder of this procedure explains how to send a notification action.

4. In the next list, select the template to use for the notification. Notification templates relevant to the selected event appear.

Note: Before you can notify users, you must have configured notification servers in Settings for SMTP and SMS so that XenMobile can send the messages, see [Notifications in XenMobile](#). Also, set up any notification templates you plan to use before proceeding. For details on setting up notification templates, see [To create or update notification templates in XenMobile](#).

Action*

Send notification

Select a template

Location perimeter breach

Note: After you select the template, you can preview the notification by clicking Preview notification message.

- In the following fields, set the delay in days, hours, or minutes before taking action and the interval at which the action repeats until the user addresses the triggering issue.

Action*

Send notification

Select a template

1

Hours

1

Hours

Minutes

Hours

Days

Su

If The location perimeter has been breached., then notify the administrator U

- In Summary verify that you created the automated action as you intended.

Summary

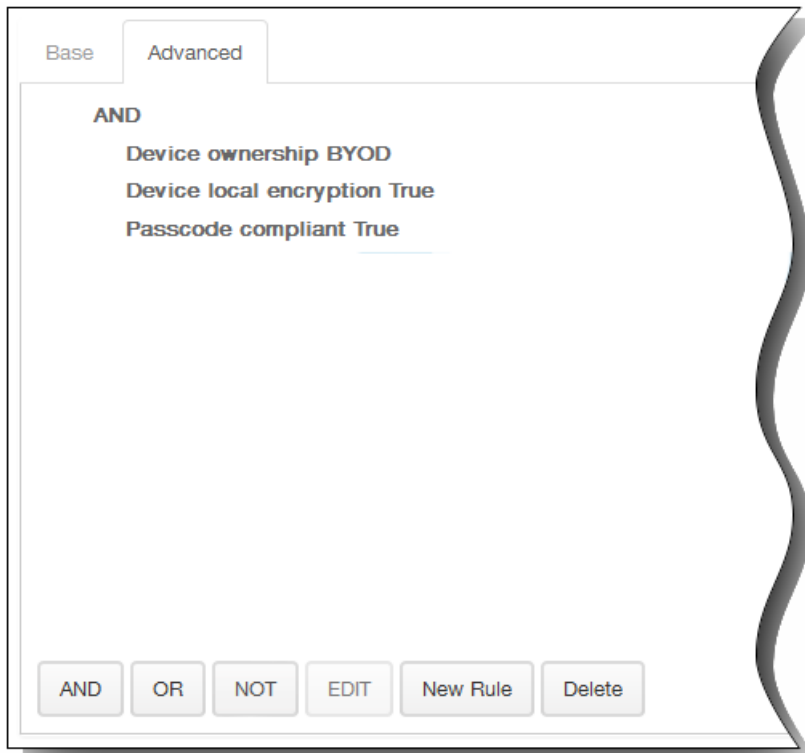
If The location perimeter has been breached., then notify the administrator using the template "Location perimeter breach" after 1 hour(s), repeating after every 1 hour(s).

After you configure the action details, you can configure deployment rules for each platform individually—iOS, Android, Windows 8.1 Tablet, Windows Phone 8.1, and Symbian. To do so, follow steps 6 through 9 for each platform you choose.

- ▶ **Deployment Rules (iOS)**
- ▶ **Deployment Rules (Android)**
- ▶ **Deployment Rules (Windows 8.1 Tablet)**
- ▶ **Deployment Rules (Windows Phone 8.1)**
- ▶ **Deployment Rules (Symbian)**

6. Expand Deployment Rules. The Base tab appears by default.

1. In the lists, click options to determine when the action should be deployed.
 1. You can choose to deploy the action when all conditions are met or when any conditions are met. The default option is All.
 2. Click New Rule to define the conditions.
 3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
 4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



The conditions you chose on the Base tab appear.

3. You can use more advanced Boolean logic to combine, edit, or add rules.

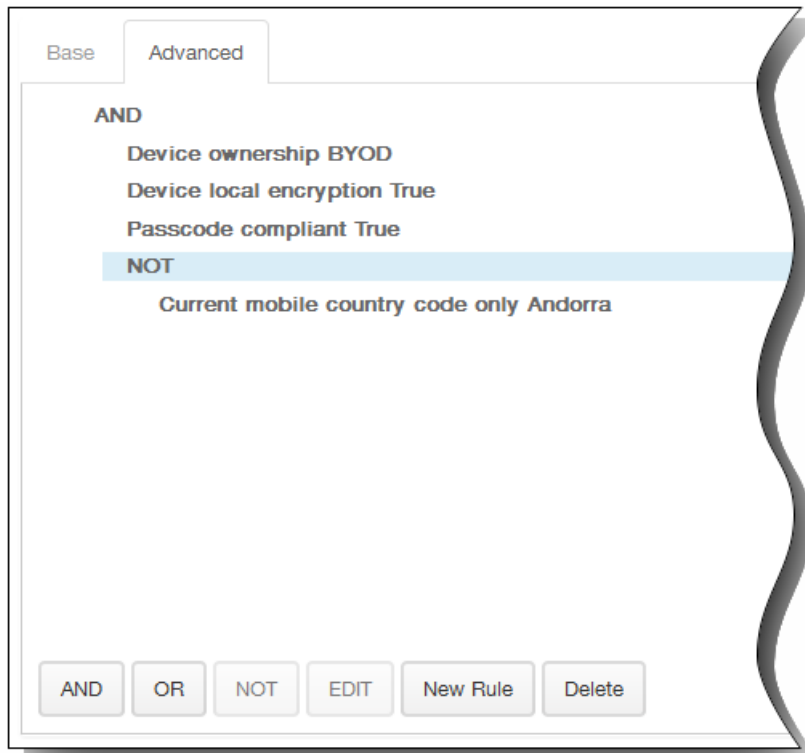
1. Click AND, OR, or NOT.

2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.

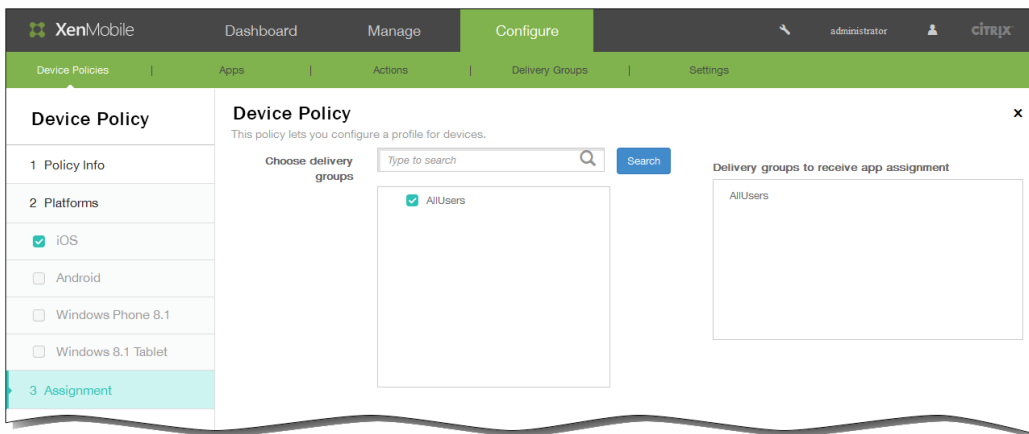
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

3. Click New Rule again if you want to add more conditions.

In this example, the device ownership must be BYOD, the device local encryption must be True, the device must be passcode compliant, and the device mobile country code cannot be only Andorra.



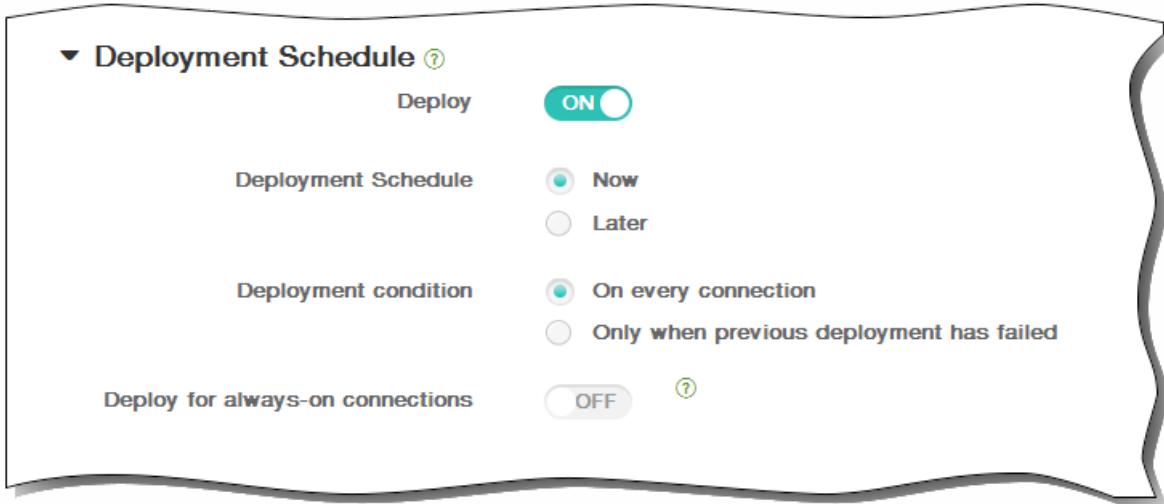
7. When you are done configuring the platform deployment rules for the action, click Next. The Actions assignment page appears, where you assign the action to a delivery group or groups. This step is optional.
8. Next to Choose delivery groups, type to find a delivery group or select a group or groups 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.



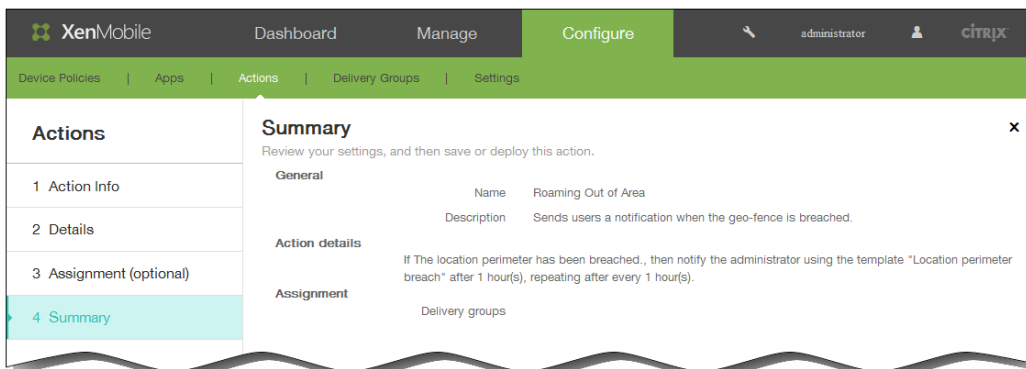
9. Expand Deployment Schedule and then configure the following settings:
 1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
 2. Next to Deployment schedule, click Now or Later. The default option is Now.
 3. If you click Later, click the calendar icon and then select the date and time for deployment.
 4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
 5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.

Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



10. Click Next. The Summary page appears, where you can verify the action configuration.



11. Click Save to save the action.

XenMobile Client Settings

Jan 16, 2015

You can configure XenMobile client settings in the XenMobile web console.

1. In the XenMobile console, click **Configure** and then click **Settings**.
The **Settings** page appears.
2. Click **More**.
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 file name 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) + 340 px x 50 px (2x).
 - Name the file as Header.png and Header@2x.png.
 - Create a .zip file from the files, not a folder with the files inside of it.
1. In the XenMobile console, click Configure > Settings > More > Worx Store Branding.
 2. Next to Default store view, select either Category or A-Z.
 3. Next to Device option, select either Phone or Tablet.
 4. Next to Branding file, click Browse to select an image or .zip file of images to use for the branding and then click Save.

To deploy this package to users' devices, you need to create a deployment package and deploy the package.

To create Worx Home and GoToAssist support options

Dec 26, 2014

1. In the XenMobile console, click Configure > Settings > More > Worx Home Support.
2. On the Worx Home Support page, type a value for the following fields:
 1. Support email (IT help desk)
 2. Support phone (IT help desk)
 3. Token for GoToAssist chat
 4. GoToAssist support ticket email

The Worx Home Support information you create appears in the Client Properties list in the XenMobile console associated with the following keys: SUPPORT_EMAIL, SUPPORT_PHONE, GTA_CHAT and GTA_TICKET.

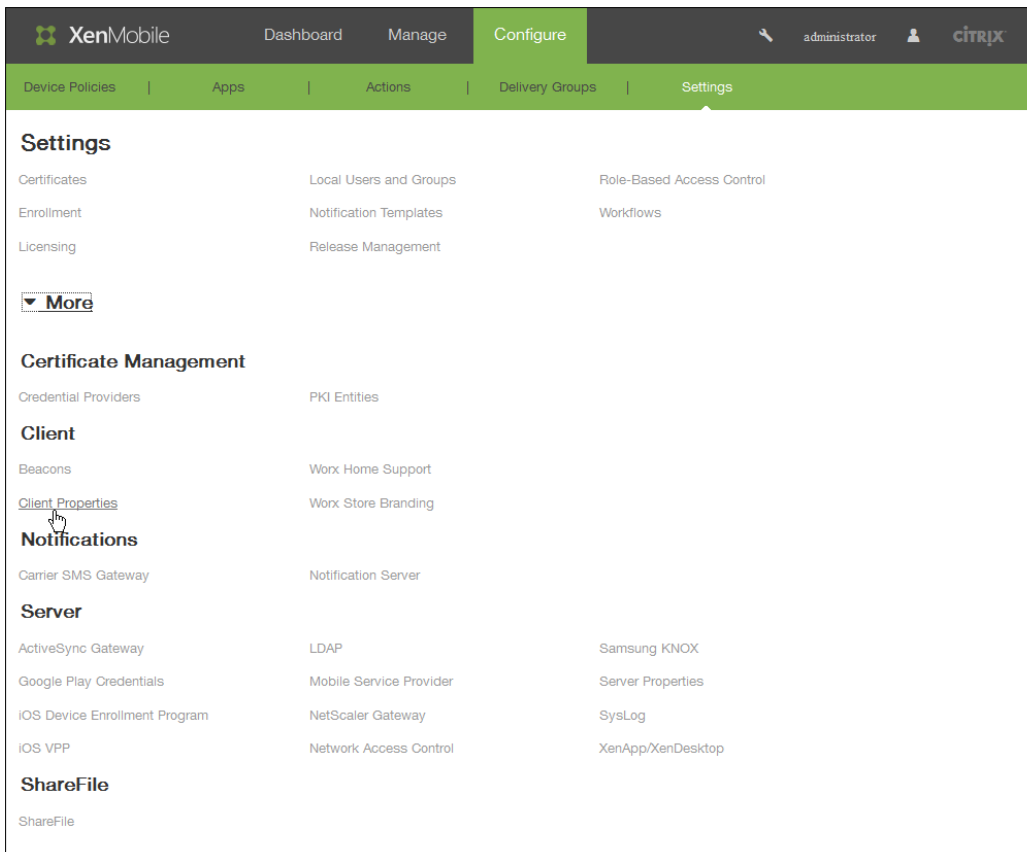
To add, edit, or delete client properties

Feb 13, 2015

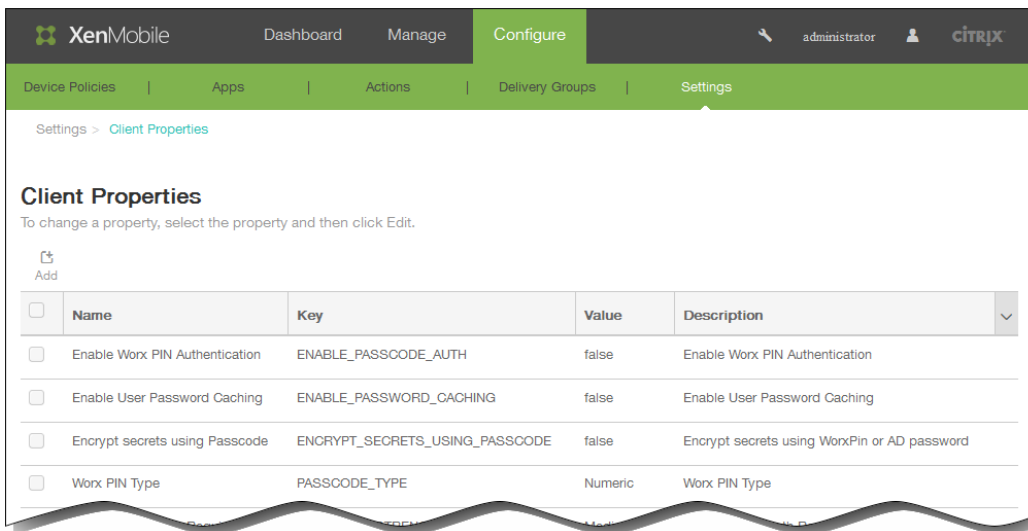
Client properties contain information that is provided directly to Worx Home on users' devices. These properties are used to configure advanced settings, such as the Worx PIN. You obtain client properties from Citrix support.

Note: Client properties are subject to change with every release of client apps, particularly Worx Home.

1. In the XenMobile console, click Configure > Settings > More > Client Properties.

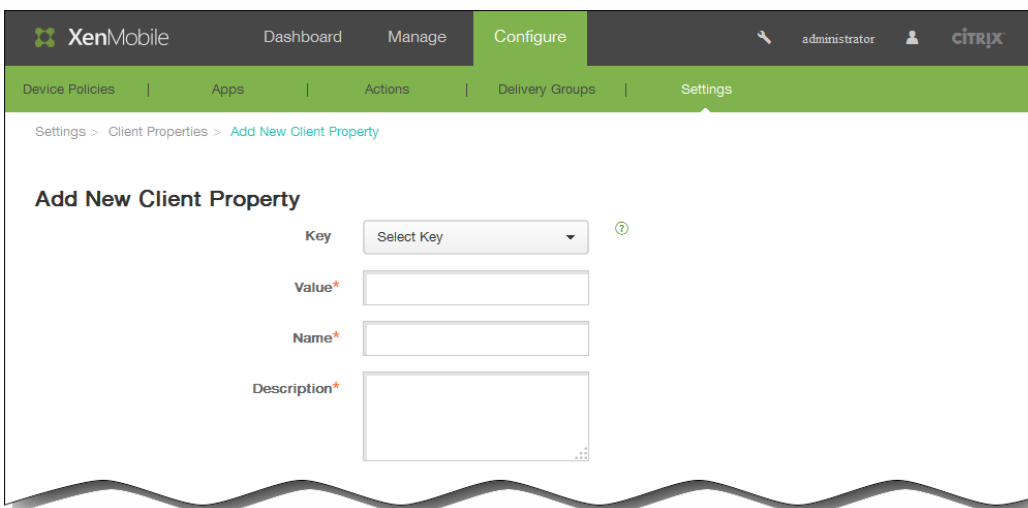


The Client Properties page appears. You can add, edit, and delete client properties from this page.



To add a client property

1. In the Client Properties page, click Add. The Add New Client Property page appears.



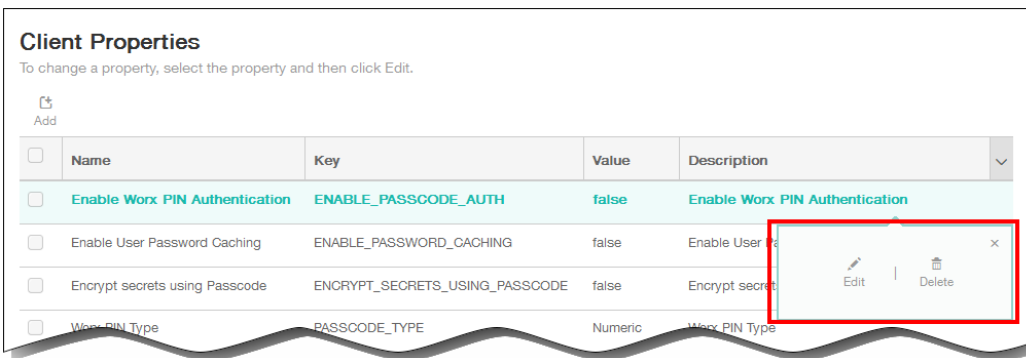
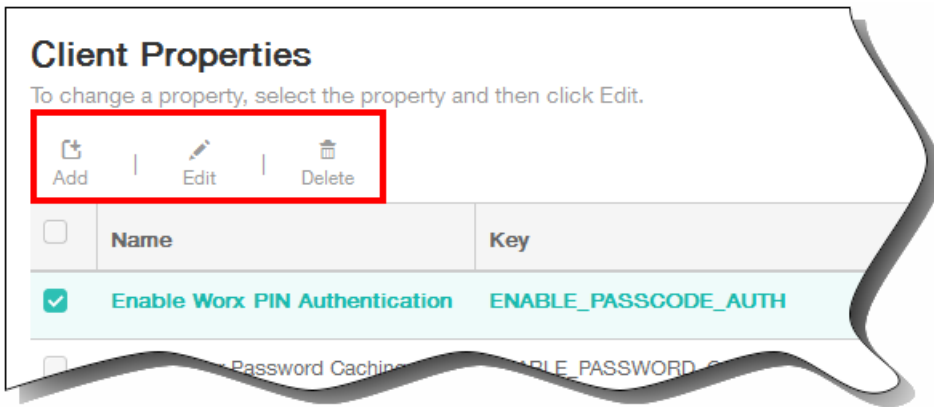
2. In the Add New Client Property page, enter the following information:

Note: All fields are required.

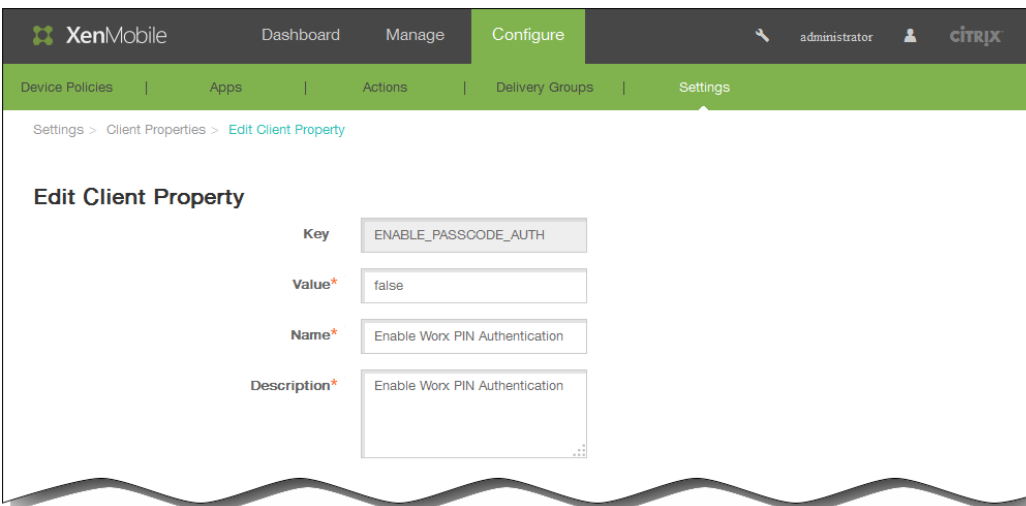
1. Key: In the list, click the property key you want to add.
Important: Contact Citrix Support before making any changes or request a special key to make a change.
2. Value: Enter the selected property's value.
3. Name: Enter a name for the property.
4. Description: Enter a description of the property.

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:
 1. Value: The selected property value.
 2. Name: The name for the property.
 3. Description: The description of the property.
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

May 06, 2016

The XenMobile predefined client properties and their default settings are as follows.

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 users' Active Directory password to be cached locally on the mobile device. When you set this key to true, users are prompted to set a 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 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 artefacts, but also adds user entropy (a user-generated random PIN code that only the user knows).

Citrix recommends 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_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: 1-99

Default value: 90

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

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

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

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#

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

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 users' devices, you cannot modify 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)

XenMobile Server Settings

Feb 13, 2015

You can configure XenMobile server settings in the XenMobile web console.

Server configuration options include:

ActiveSync Gateway	iOS VPP	NetScaler Gateway	Server Properties
Google Play Credentials	LDAP	Network Access Control	SysLog
iOS Device Enrollment Program	Mobile Service Provider	Samsung KNOX	XenApp/XenDesktop

1. In the XenMobile console, click Configure and then click Settings.
The Settings page appears.

The screenshot shows the XenMobile web console interface. At the top, there is a navigation bar with 'XenMobile' logo, 'Dashboard', 'Manage', and 'Configure' (highlighted with a green arrow). Below the navigation bar, there is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'Delivery Groups', and 'Settings' (highlighted with a green arrow). The main content area is titled 'Settings' and contains several sections: 'Certificate Management' (with sub-items: Credential Providers, PKI Entities), 'Client' (with sub-items: Beacons, Client Properties, Wox Home Support, Wox Store Branding), 'Notifications' (with sub-items: Carrier SMS Gateway, Notification Server), and 'Server' (with sub-items: ActiveSync Gateway, Google Play Credentials, iOS Device Enrollment Program, iOS VPP, LDAP, Mobile Service Provider, NetScaler Gateway, Network Access Control, Samsung KNOX, Server Properties, SysLog, XenApp/XenDesktop). A 'More' button is located below the 'Certificate Management' section, with a green arrow pointing to it.

2. Click More.
3. 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.

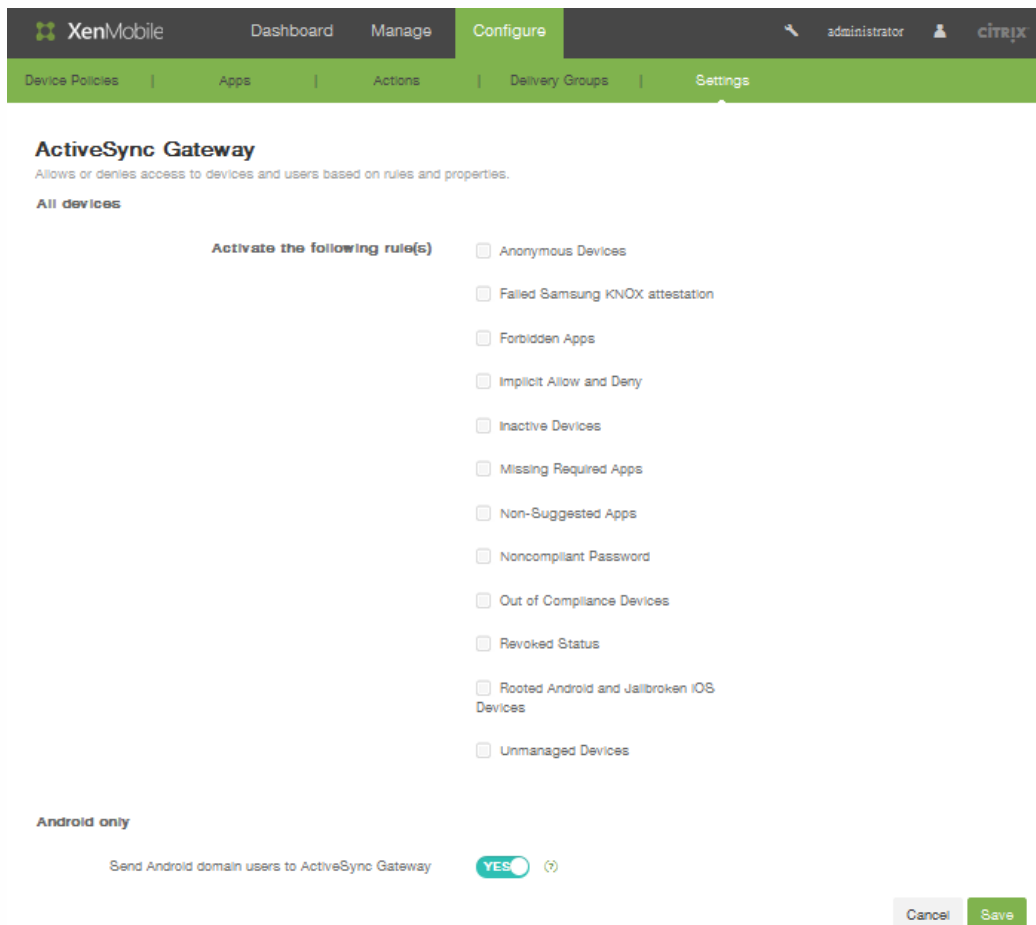
Rooted Android and jailbroken iOS Devices: Checks whether an Android or iOS device is jailbroken.

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 an ActiveSync Gateway in XenMobile

1. In the XenMobile console, click **Configure > Settings > More > ActiveSync Gateway**. The **ActiveSync Gateway** configuration page appears.



2. In **Activate the following rules**, select one or more rules you want to activate.
3. In **Android-only**, in **Send Android domain users to ActiveSync Gateway**, click **YES** to ensure that XenMobile sends Android device information to the Secure Mobile Gateway.
4. Click **Save**.

Google Play Credentials

Feb 20, 2015

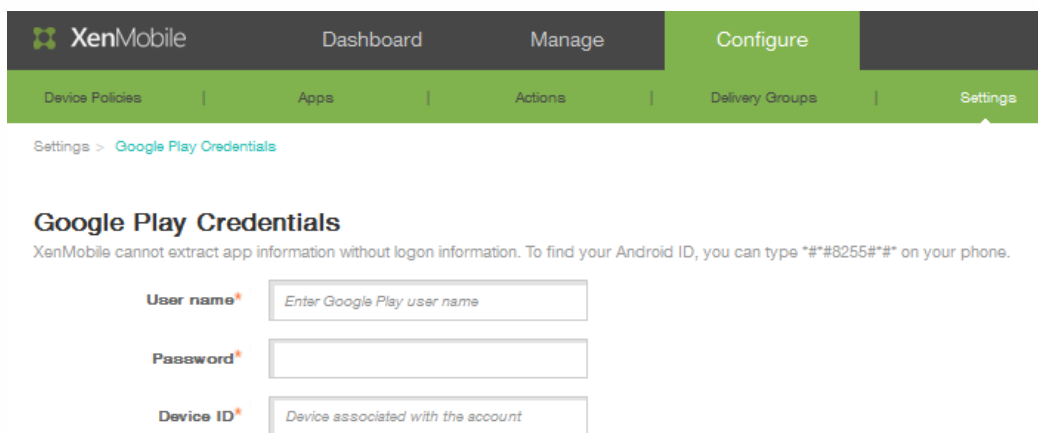
XenMobile uses Google Play credentials to extract app information for the device.

Note: To locate your Android ID, enter `*##8255##*` on your phone.

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.

To configure XenMobile to use Google Play credentials

1. In the XenMobile web console, click Configure > Settings > More > Google Play Credentials. The Google Play Credentials configuration screen appears.



The screenshot shows the XenMobile web console interface. The top navigation bar includes 'XenMobile', 'Dashboard', 'Manage', and 'Configure'. Below this is a secondary navigation bar with 'Device Policies', 'Apps', 'Actions', 'Delivery Groups', and 'Settings'. The 'Settings' menu is expanded to show 'Google Play Credentials'. The main content area is titled 'Google Play Credentials' and contains a message: 'XenMobile cannot extract app information without logon information. To find your Android ID, you can type `*##8255##*` on your phone.' Below the message are three input fields: 'User name*' with a placeholder 'Enter Google Play user name', 'Password*', and 'Device ID*' with a placeholder 'Device associated with the account'.

2. In User name, enter the name associated with the Google Play account.
3. In Password, enter the user password.
4. In Device ID, enter your Android ID.
Enter `*##8255##*` on your phone to determine the Android ID.
5. Click Save.

iOS Device Enrollment Program

Feb 13, 2015

You can set up an iOS Device Enrollment Program in XenMobile for mobile devices running iOS. The feature lets iOS devices notify Apple servers about a profile that customizes the experience of the device setup assistant which can then be assigned to specific devices.

To configure the iOS Device Enrollment Program in XenMobile

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 Device Enrollment Program** page under **Settings > More**, 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 Device Enrollment Program** page, set **Device enrollment** to **Yes** and then 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](#).

The screenshot shows the XenMobile web interface for configuring the iOS Device Enrollment Program. The top navigation bar includes 'XenMobile', 'Dashboard', 'Manage', and 'Configure'. The 'Configure' section is active, showing a breadcrumb trail: 'Settings > iOS Device Enrollment Program'. Below the navigation, the page title is 'iOS Device Enrollment Program' with a subtitle: 'Notifies Apple servers about a profile that customizes the experience of the device setup assistant and then can be assigned to specific devices.' There are two action buttons: 'Export Public Key' and 'Import Token File'. The main configuration area has a 'Device enrollment' toggle set to 'NO'. Below this are five text input fields: 'Consumer key*', 'Consumer secret*', 'Access token*', 'Access secret*', and 'Access token expiration'. A green 'Test Connection' button is located below the input fields. At the bottom, there is a 'Device Setup' link and 'Cancel' and 'Save' buttons.

In **Details**, configure the following settings to complete the DEP configuration:

- Device enrollment: Click YES.
- Consumer key: Enter the consumer key.
- Consumer secret: Enter a consumer secret.
- Access token: Specify the access token.
- Access secret: Enter the secret for the access token.
- Access token expiration: Optionally, specify the access token expiration.
- Click Test Connection to verify connectivity.

- Expand Device Setup and then configure the following settings:
 - Business unit: Enter the name associated with the Business unit.
 - Support phone number: Enter the phone number for support.
 - Support email address: Optionally, enter the Support email address.
 - Unique service ID: Optionally include a unique service ID.

- In Device Settings, configure the following device settings that are associated with the iOS Device Enrollment Program:
 - Allow or deny pairing: Click Allow to enable the device to be managed through Apple Tools, such as iTunes and the Apple Configurator.

Note

If you allow pairing and use the Apple Configurator, in **Supervised mode**, select **YES**

- • Device profile removal: If you want the device to use a profile that can be removed remotely, click Allow.
- Require device enrollment: Select this check box to prevent users from skipping the enrollment process.

- In Device Setup Steps, configure the following settings:
 - Location services: Click Set up to enable the device to share the location or click Skip to prevent the device from sharing its location.
 - Restore from backup: Click Set up to enable a device to restore data from a backup file.
 - Apple and iCloud: Click Set up if you want the device to use the Apple ID and iCloud.
 - Terms and Conditions: Click Set up.
 - Passcode: Click Set up to use a passcode for device enrollment.
 - Siri: Click Set up to enable a device to use Siri.
 - Touch ID: Click Set up to use Touch ID for the device.
 - Apple Pay: Click Set up to enable Apple Pay for the device.
 - Zoom: Click Set up to enable zoom.
 - Diagnostics: Click Set up to allow the device to share diagnostics.

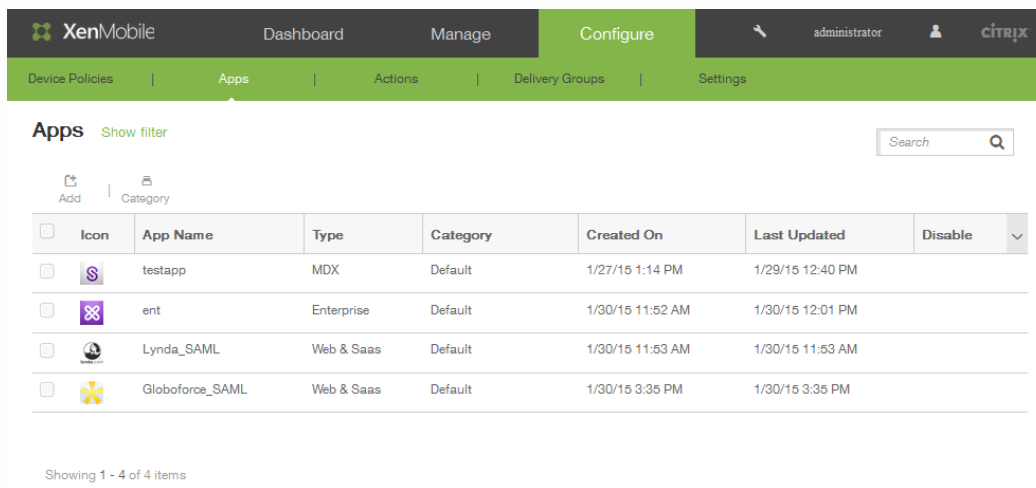
- Click Save.





iOS VPP

Feb 13, 2015

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.

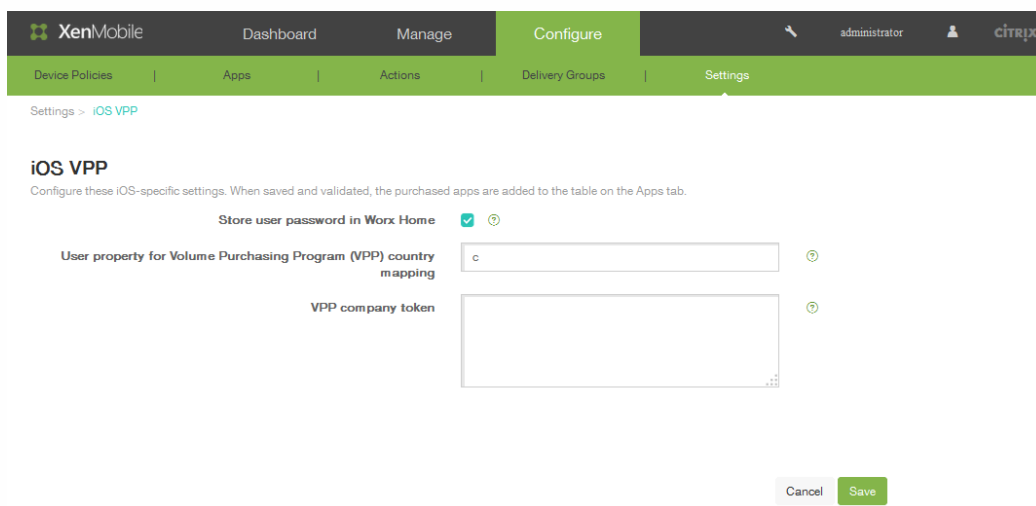


<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	
<input type="checkbox"/>		testapp	MDX	Default	1/27/15 1:14 PM	1/29/15 12:40 PM		
<input type="checkbox"/>		ent	Enterprise	Default	1/30/15 11:52 AM	1/30/15 12:01 PM		
<input type="checkbox"/>		Lynda_SAML	Web & Saas	Default	1/30/15 11:53 AM	1/30/15 11:53 AM		
<input type="checkbox"/>		Globoforce_SAML	Web & Saas	Default	1/30/15 3:35 PM	1/30/15 3:35 PM		

Showing 1 - 4 of 4 items

To configure iOS VPP in XenMobile

1. In the XenMobile web console, click Configure > Settings > More > iOS VPP. The iOS VPP configuration screen appears.



Settings > iOS VPP

iOS VPP
Configure these iOS-specific settings. When saved and validated, the purchased apps are added to the table on the Apps tab.

Store user password in Worx Home ⓘ

User property for Volume Purchasing Program (VPP) country mapping ⓘ

VPP company token ⓘ

Cancel Save

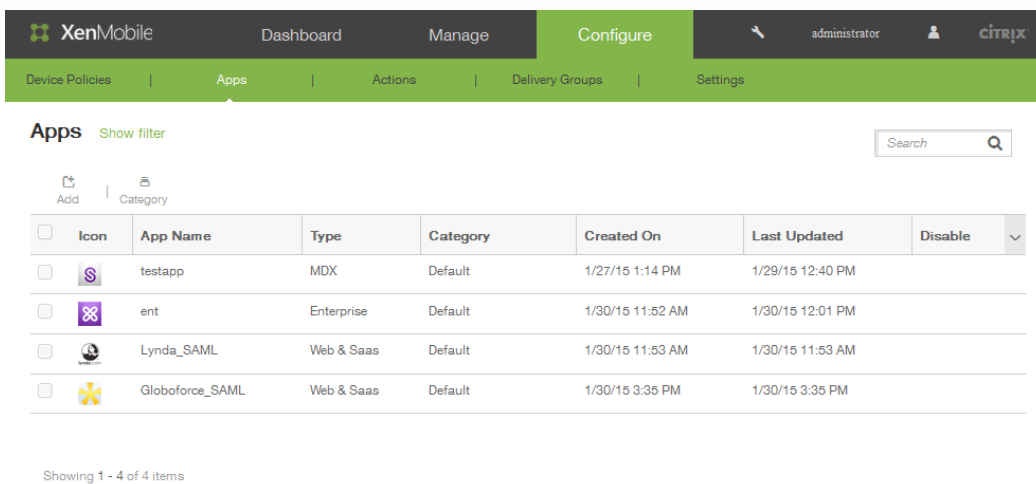
2. In Store user password in Worx Home, select the check box to securely store a user name and password in Worx Home

for XenMobile authentication.





3. In User property for Volume Purchasing Program (VPP) country mapping, enter 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.

4. In VPP company token, enter a token that represents the VPP service token generated when a user buys something from the Apple App Store through a company-based account. The token is used to validate the VPP license. For example, if you have an Apple VPP account for Business, visit <https://vpp.itunes.com>, click **Business**, and log in with your Apple VPP account credentials to retrieve the appropriate information.
5. Click Save. The information is then displayed in the Apps table:



The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Dashboard', 'Manage', and 'Configure'. The 'Configure' section is active, and the 'Apps' tab is selected. Below the navigation bar, there are tabs for 'Device Policies', 'Apps', 'Actions', 'Delivery Groups', and 'Settings'. The 'Apps' section displays a table with the following data:

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	▼
<input type="checkbox"/>		testapp	MDX	Default	1/27/15 1:14 PM	1/29/15 12:40 PM		
<input type="checkbox"/>		ent	Enterprise	Default	1/30/15 11:52 AM	1/30/15 12:01 PM		
<input type="checkbox"/>		Lynda_SAML	Web & Saas	Default	1/30/15 11:53 AM	1/30/15 11:53 AM		
<input type="checkbox"/>		Globoforce_SAML	Web & Saas	Default	1/30/15 3:35 PM	1/30/15 3:35 PM		

Showing 1 - 4 of 4 items

Mobile Service Provider

Jan 06, 2017

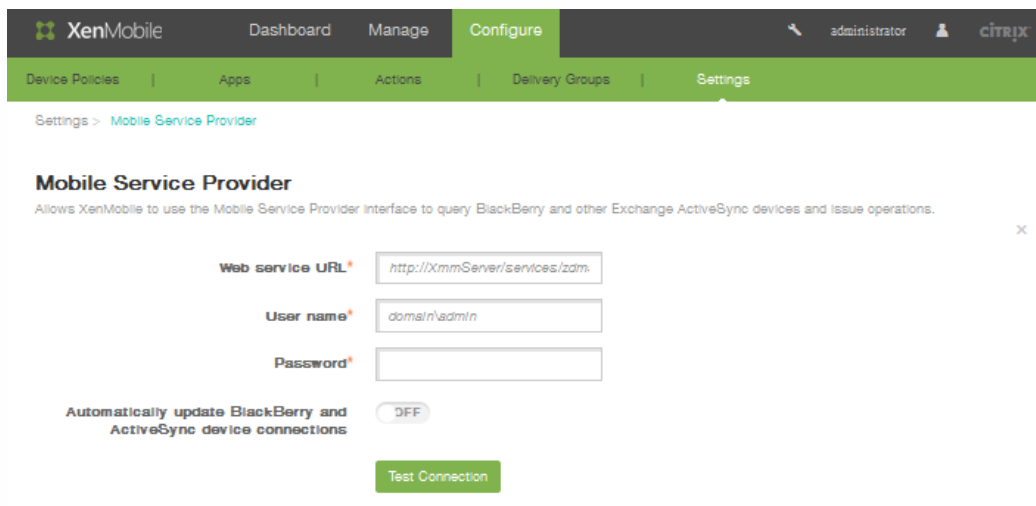
You can enable XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.

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.

To configure the Mobile Service Provider

1. In the XenMobile web console, click Configure > Settings > More > Mobile Service Provider. The Mobile Service Provider configuration page appears.



The screenshot shows the XenMobile web console interface. The top navigation bar includes 'XenMobile', 'Dashboard', 'Manage', and 'Configure'. Below this is a secondary navigation bar with 'Device Policies', 'Apps', 'Actions', 'Delivery Groups', and 'Settings'. The 'Settings' page is open, showing the 'Mobile Service Provider' configuration. The page title is 'Mobile Service Provider' with a subtitle: 'Allows XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and Issue operations.' The configuration fields are: 'Web service URL' (http://XmmServer/services/zdm), 'User name' (domain\admin), and 'Password' (empty). There is a toggle for 'Automatically update BlackBerry and ActiveSync device connections' set to 'OFF'. A 'Test Connection' button is visible at the bottom.

2. In Web service URL, enter the URL of the Web service, such as `http://XmmServer/services/xdmService`
3. In User name, enter the user name in the format `domain\admin`
4. In Password, enter the password.
5. In Automatically update BlackBerry and ActiveSync device connections, click **ON** if you want to enable this option. The default setting is **OFF**.
6. Click Test connection to verify connectivity.
7. 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.

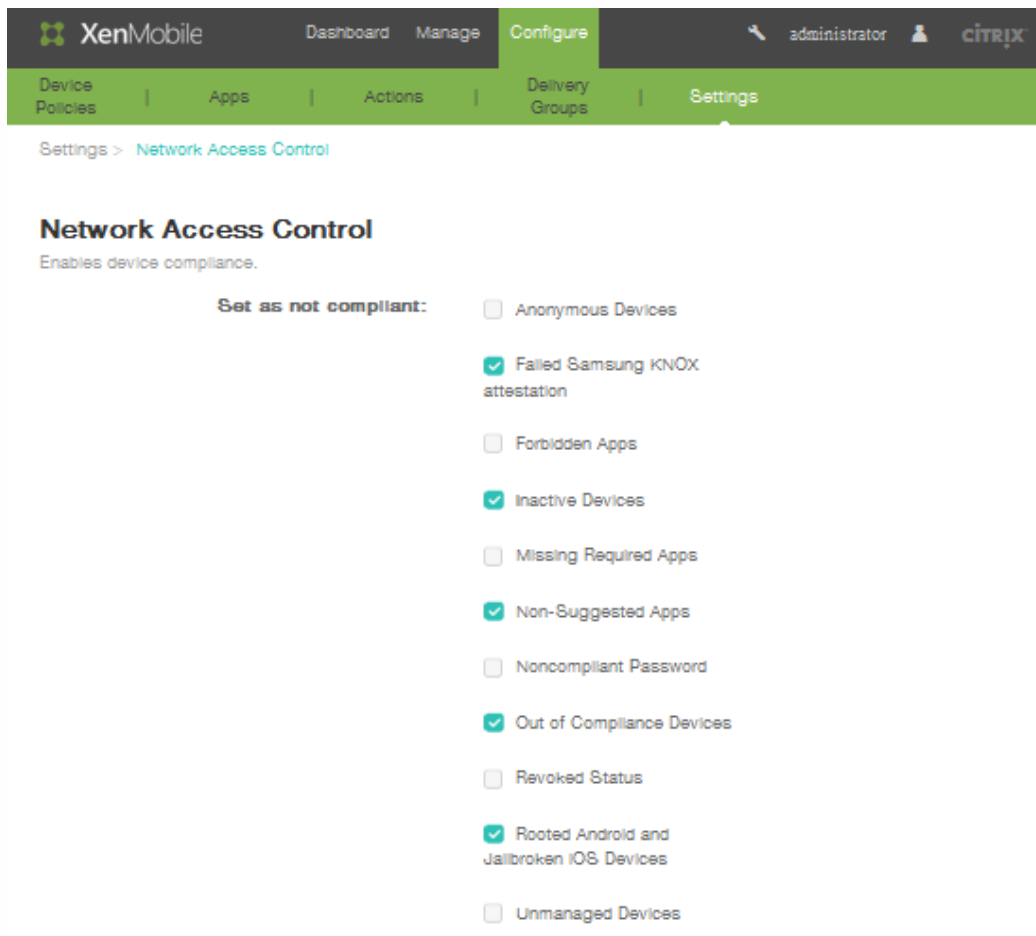
Send Android domain users to ActiveSync Gateway: Click **YES** to ensure that XenMobile sends Android device information to the ActiveSync Gateway. When this option is enabled, it ensures that XenMobile sends Android device information to the ActiveSync Gateway in the event that XenMobile does not have 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 and/or are not enrolled, are marked as Not-Compliant and will be blocked from your network by the NAC appliance.

To configure Network Access Control in XenMobile

1. In the XenMobile web console, click **Configure > Settings > More > Network Access Control**. The **Network Access Control** configuration page appears.



2. Select the checkboxes for the **Set as not compliant** filters you want to enable.
3. Click **Save**.

Samsung KNOX

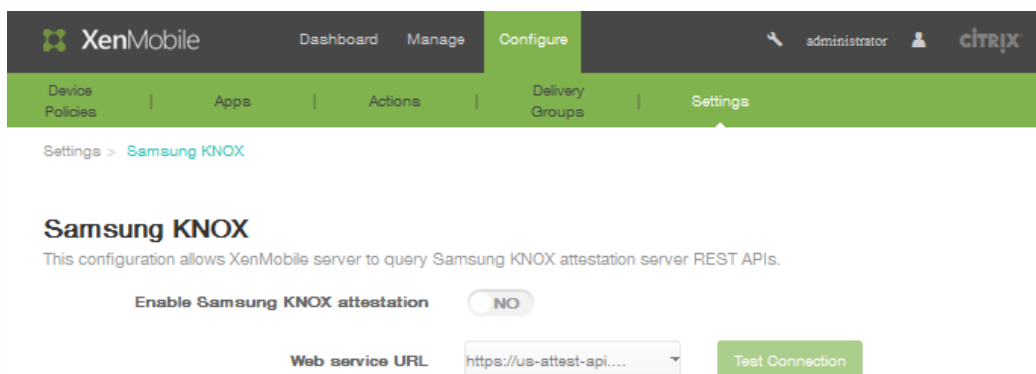
Feb 13, 2015

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.

To enable Samsung KNOX attestation

1. In the XenMobile web console, click Configure > Settings > More > Samsung KNOX.
The Samsung KNOX configuration page appears.



2. In Enable Samsung KNOX attestation, click **YES**.
3. When you click YES in step 2, 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**.

Server Properties

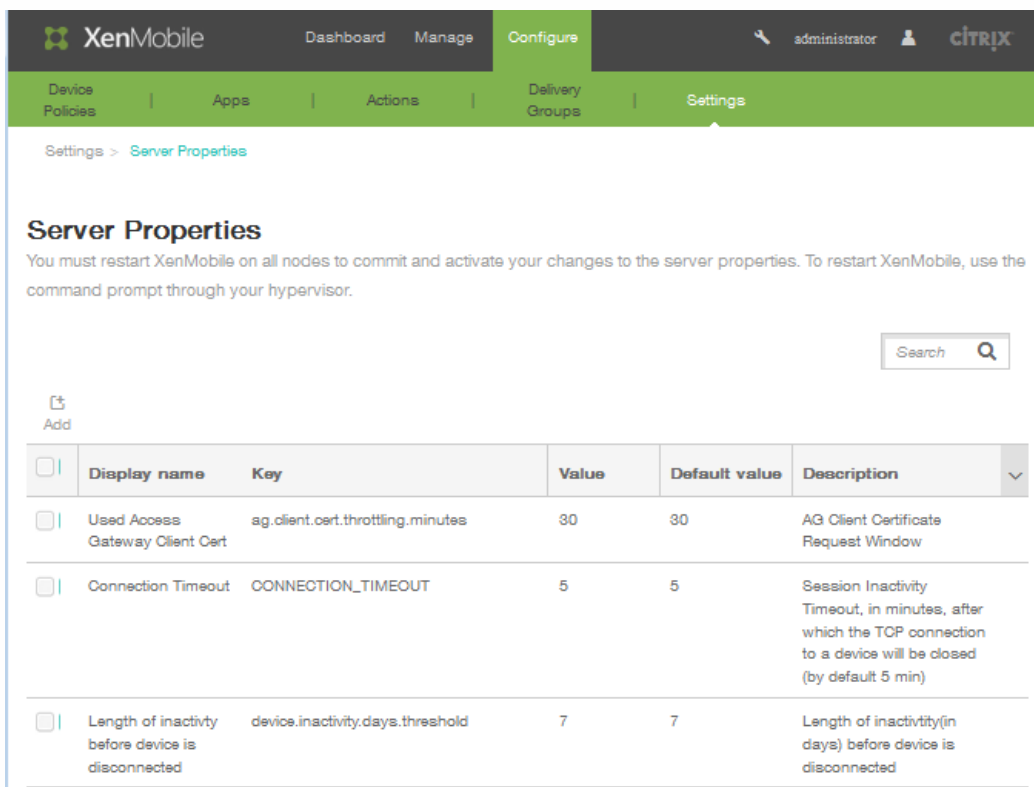
Feb 16, 2015

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.

To configure server properties in XenMobile

1. In the XenMobile web console, click Configure > Settings > More > Server Properties.
The Server Properties configuration page appears.



<input type="checkbox"/>	Display name	Key	Value	Default value	Description
<input type="checkbox"/>	Used Access Gateway Client Cert	ag_client.cert.throttling.minutes	30	30	AG Client Certificate Request Window
<input type="checkbox"/>	Connection Timeout	CONNECTION_TIMEOUT	5	5	Session Inactivity Timeout, in minutes, after which the TCP connection to a device will be closed (by default 5 min)
<input type="checkbox"/>	Length of inactivity before device is disconnected	device.inactivity.days.threshold	7	7	Length of inactivity(in days) before device is disconnected

2. Do one of the following:
 - Click Add to add a new server property.
 - In the table, click to select an existing property and then in the menu that appears, click Edit.
3. If you clicked Add in step 2, configure the following fields:
 - **Key:** In the list, select the appropriate key.
Note: 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, include a description for the new server property and then click Save.

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.

You can configure the server to collect the following types of information:

- System logs represent actions taken by XenMobile.
- Audit logs represent 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

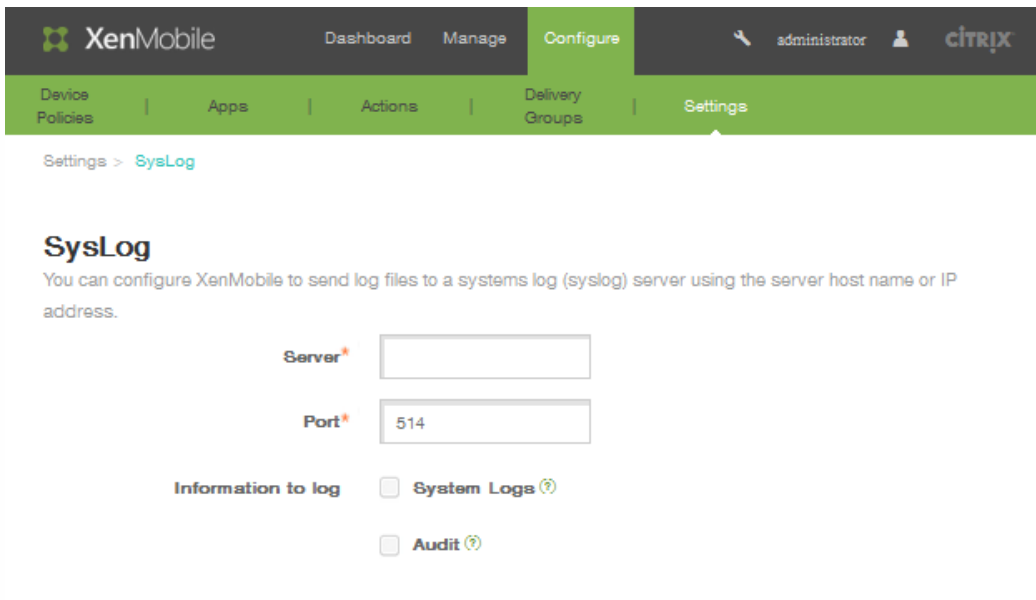
You can use this information to analyze the source of the alert and take corrective action if required.

Note

XenMobile cloud deployments, Citrix does not support syslog integration with an 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](#).

To configure a syslog server in XenMobile

1. In the XenMobile web console, click Configure > Settings > More > Syslog.
The Syslog configuration page appears.



2. In Name, enter either an IP address or fully qualified domain name (FQDN) of your syslog server.
3. In Port, enter the port number. By default, the port is set to 514.
4. In Information to log, select or clear System Logs and Audit.
 - System logs represent actions taken by XenMobile.
 - Audit logs represent a chronological record of system activities for XenMobile.
5. Click **Save**.

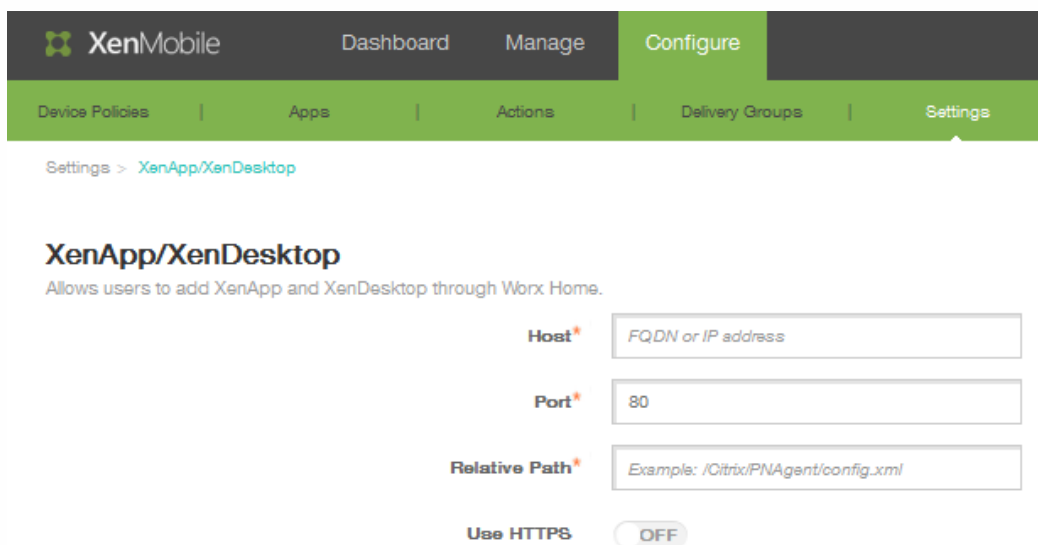
To configure XenApp and XenDesktop

Aug 12, 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 StoreFront or the Web Interface site.

1. In the XenMobile web console, click **Configure > Settings > More > XenApp/XenDesktop**.
The XenApp/XenDesktop configuration page appears.



The screenshot shows the XenMobile web console interface. At the top, there is a navigation bar with 'XenMobile' logo and tabs for 'Dashboard', 'Manage', and 'Configure'. Below this is a secondary navigation bar with 'Device Policies', 'Apps', 'Actions', 'Delivery Groups', and 'Settings'. The 'Settings' tab is active, and the breadcrumb trail shows 'Settings > XenApp/XenDesktop'. The main content area is titled 'XenApp/XenDesktop' and includes a description: 'Allows users to add XenApp and XenDesktop through Worx Home.' Below the description are four configuration fields: 'Host' (with a red asterisk and placeholder 'FQDN or IP address'), 'Port' (with a red asterisk and value '80'), 'Relative Path' (with a red asterisk and placeholder 'Example: /Citrix/PNAgent/config.xml'), and 'Use HTTPS' (a toggle switch currently set to 'OFF').

2. In Host, enter the fully qualified domain name (FQDN) or IP address for StoreFront or the Web Interface site.
3. In Port, enter the port number for StoreFront or the Web Interface site. The default is 80.
4. In Relative Path, enter the path. For example, /Citrix/Store/PNAgent/config.xml
5. In Use HTTPS, select ON to enable secure authentication between StoreFront or the Web Interface site and the client device. The default is OFF.
6. Click **Save**.

XenMobile Support and Maintenance

Jun 01, 2016

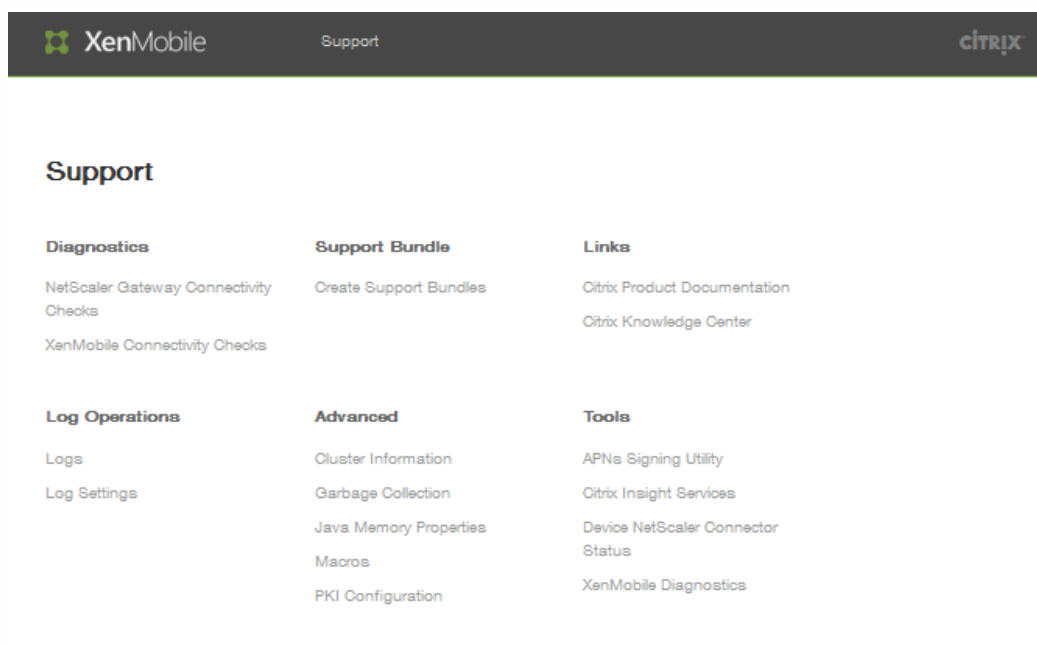
Use the XenMobile Support page to access a number of support-related information and tools. You can also carry out actions from the command-line interface. For details, see [XenMobile Command-Line Interface Options](#).

To access the Support page

In the XenMobile console, click the wrench icon  in the upper-right corner of the console:



The Support page appears in a separate browser tab:



Use the XenMobile Support page to:

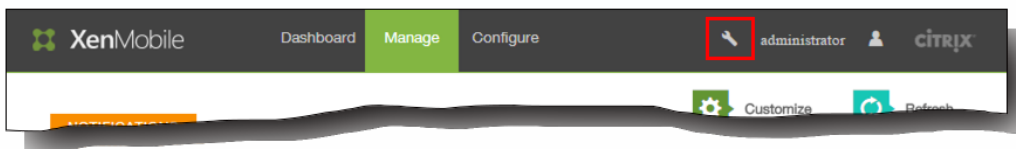
- Access diagnostics.
- Create support bundles.
- Access links to Citrix Product Documentation and the Knowledge Center.
- Access log operations.
- Select from a set of advanced information and configuration options.
- Access a set of tools and utilities.

Conducting Connectivity Checks

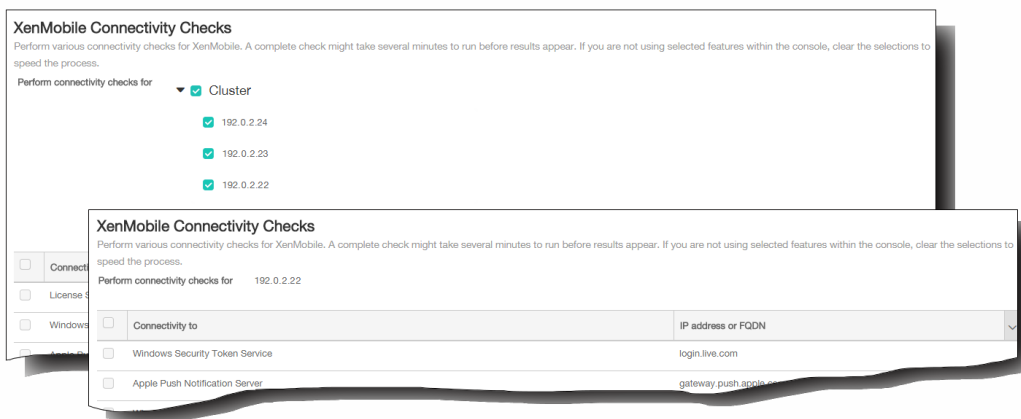
Feb 13, 2015

From the XenMobile Support page, you can check the XenMobile connection to NetScaler Gateway and other servers and locations. To get to the Support page, do the following:

1. From the XenMobile console, click the wrench icon in the right upper-hand corner. The wrench icon is available from any page of the XenMobile console. You may be asked for your user name and password.



A new browser tab, XenMobile Support, opens. If your XenMobile environment contains clustered nodes, all nodes are shown.



Conducting XenMobile Connectivity Checks

1. On the Support page, click XenMobile Connectivity Checks. The XenMobile Connectivity Checks page appears.
2. Select the servers you want to include in the connectivity test and then click Test Connectivity. The results appear.
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, click NetScaler Gateway Connectivity Checks. The NetScaler Gateway Connectivity Checks page appears.
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 are 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 are 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.

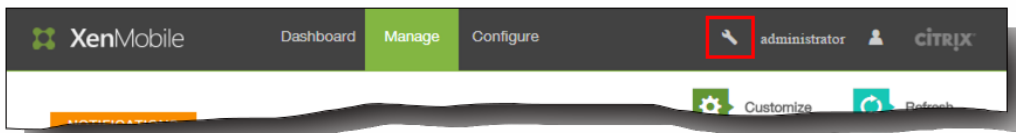
Creating Support Bundles in XenMobile

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).

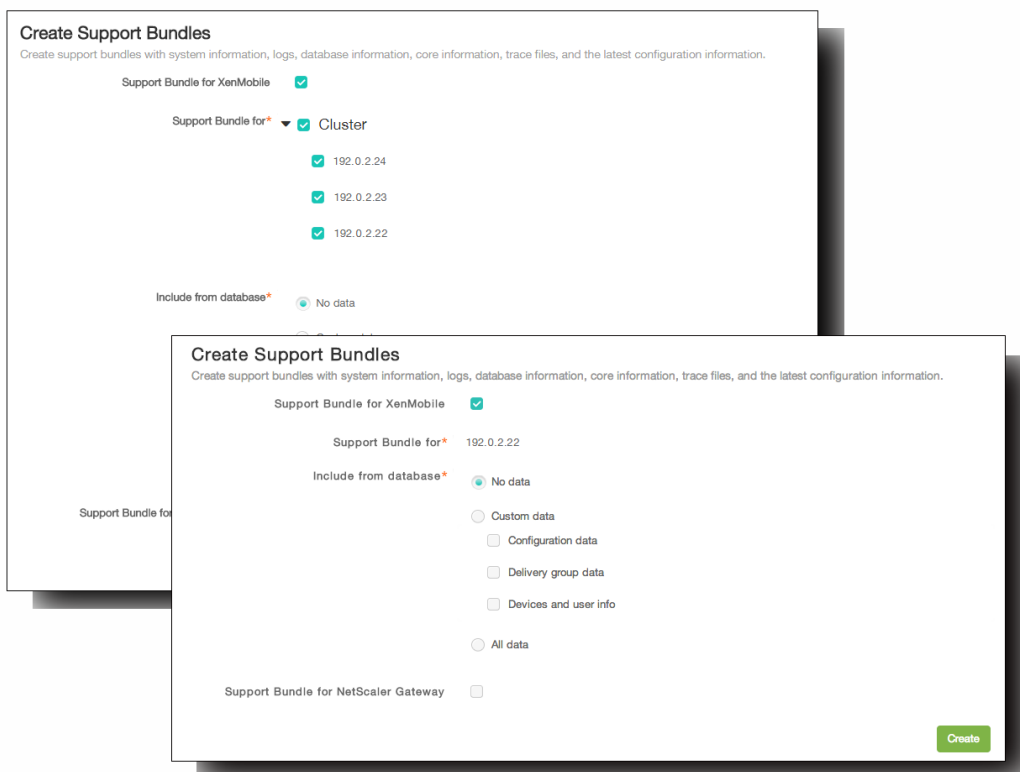
1. In the XenMobile console, click the wrench icon in the right upper-hand corner. The wrench icon is available from any page of the XenMobile console.

Note: You may be asked for your user name and password.



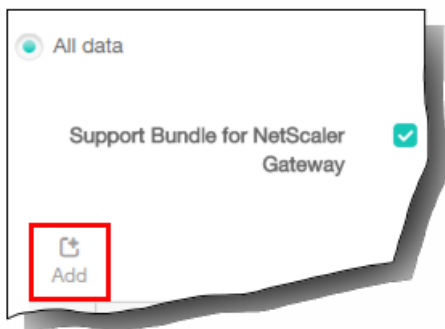
XenMobile Support opens in a new browser tab.

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. Ensure 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 to draw data from.
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 groups information, containing app types and app delivery policy details.
 - Devices and user info. Includes device policies, apps, actions, and delivery groups.
 - Click All data.
6. Select the Support Bundle for NetScaler Gateway if you want to include support bundles from NetScaler Gateway and then do the following:
1. Click Add.

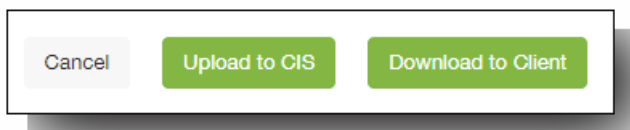


The Add NetScaler Gateway Server dialog box appears.

2. In NetScaler Gateway Management IP, type the NetScaler management IP address for the NetScaler Gateway you want to draw your support bundle from.

Note: If you are creating a bundle from a NetScaler Gateway server that is already added, the IP address is provided.
3. 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.
4. Click Add. The new NetScaler Gateway support bundle is added to the table.
5. Repeat Step 6 to add additional NetScaler Gateway support bundles as needed.
7. Click Create. The support bundle is created and two new buttons, Upload to CIS and Download to Client, appear.



Continue to the procedures for **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.

1. On the Create Support Bundles page, click Upload to CIS. The Upload to Citrix Insight Services (CIS) dialog box appears.

Upload to Citrix Insight Services (CIS)

CIS Website cis.citrix.com

User name* MyCitrix ID

Password* MyCitrix password

Associate with SR#

Cancel Upload

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:
 1. In SR#, type the eight-digit service request number you want to associate this bundle with.
 2. In SR Description, type a description of the SR.
5. Click Upload. The support bundle is uploaded to CIS.

Downloading Support Bundles to Your Computer

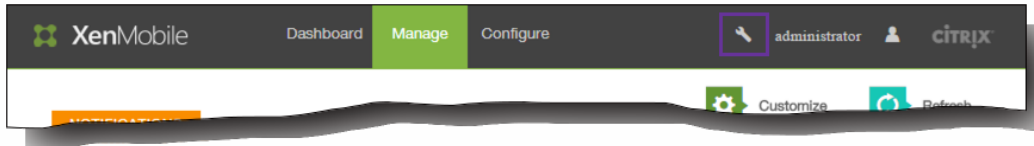
After you create a support bundle, you can upload the bundle to CIS or download the bundle to your computer. If you would like to troubleshoot the problem on your own, download the support bundle to your computer. On the Create Support Bundles page, click Download to Client. The bundle is downloaded to your computer.

To view the debug log file

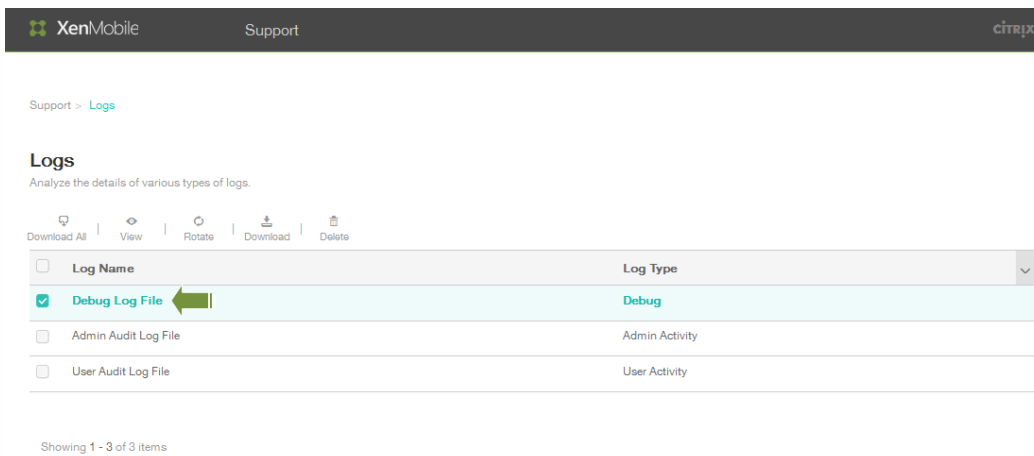
Mar 20, 2015

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 wrench icon is available from any page of the XenMobile console.



2. On the Support page, click Logs. The Logs screen appears.



3. Select Debug Log File and then click View to display the contents of the log.

Support > Logs

Logs

Analyze the details of various types of logs.

Download All Rotate Download Delete

<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Debug Log File

```

2015-01-27T06:13:25.54-0800 | INFO | localhost-startStop-1 | com.sparus.nps.PkiConfigInit | **** Inside Pki Config Initialize Method. pki.xml file created from DB ***
2015-01-27T06:13:25.524-0800 | INFO | localhost-startStop-1 | com.sparus.nps.PkiConfigInit | Cluster Info updated
2015-01-27T06:13:26.691-0800 | INFO | localhost-startStop-1 | com.sparus.nps.EwConfigInit | **** Inside EwConfig Initialize Method ****
2015-01-27T06:13:33.882-0800 | ERROR | localhost-startStop-1 | com.citrix.xms.security.OnPremiseDataSecurity | Failed to encrypt. Empty Input
2015-01-27T06:13:33.882-0800 | ERROR | localhost-startStop-1 | com.citrix.xms.security.OnPremiseDataSecurity | Failed to encrypt. Empty Input
2015-01-27T06:13:33.901-0800 | ERROR | localhost-startStop-1 | com.citrix.xms.security.OnPremiseDataSecurity | Failed to encrypt. Empty Input
2015-01-27T06:13:33.901-0800 | ERROR | localhost-startStop-1 | com.citrix.xms.security.OnPremiseDataSecurity | Failed to encrypt. Empty Input
2015-01-27T06:13:33.980-0800 | INFO | localhost-startStop-1 | com.sparus.nps.spring.DBPropertyPlaceholderConfigurer | Loading properties file from class path resource
2015-01-27T06:13:34.39-0800 | INFO | localhost-startStop-1 | com.sparus.nps.spring.DBPropertyPlaceholderConfigurer | Read zdm.awareness.http-plain.host property from
2015-01-27T06:13:34.41-0800 | INFO | localhost-startStop-1 | com.sparus.nps.spring.DBPropertyPlaceholderConfigurer | Read zdm.awareness.http-plain.port property from
2015-01-27T06:13:34.41-0800 | INFO | localhost-startStop-1 | com.sparus.nps.spring.DBPropertyPlaceholderConfigurer | Read zdm.awareness.http-plain.instancepath proper
2015-01-27T06:13:34.42-0800 | INFO | localhost-startStop-1 | com.sparus.nps.spring.DBPropertyPlaceholderConfigurer | Read zdm.awareness.https-no-auth.host property fr
2015-01-27T06:13:34.42-0800 | INFO | localhost-startStop-1 | com.sparus.nps.spring.DBPropertyPlaceholderConfigurer | Read zdm.awareness.https-no-auth.port property fr

```

After analyzing the log file, use the Download File option to save the data, or click Delete to remove the contents of the log from the database.

To configure log settings

Mar 24, 2015

You can configure log settings to customize the output of logs generated by XenMobile. In the XenMobile console, click Support > Log Settings to 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 the user activity log).
- **Log Level.** Use this option to change the class name, the sub-class name, 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. Click Support > Log Settings and then expand Log Size.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with the XenMobile logo and the word 'Support'. Below this, a breadcrumb trail reads 'Support > Log Settings'. The main heading is 'Log Settings'. Underneath, a dropdown menu labeled 'Log Size' is expanded. This menu contains six items, each with a label and a corresponding dropdown menu:

Debug log file size (MB)	10
Maximum number of debug backup files	50
Admin activity log file size (MB)	10
Maximum number of admin activity backup files	300
User activity log file size (MB)	10
Maximum number of user activity backup files	600

2. In the Debug log file size (MB) list, select a size between 5 and 20 MB to change the maximum size of the debug file. By default, the size of the file is set to 10 MB.
3. In the Maximum number of debug backup files list, select from 5 through 300 debug files to change the maximum number of debug files retained by the server. By default, XenMobile retains 50 backup files on the server.
4. In the Admin activity log list, select a size between 5 and 20 MB. By default, the size of the file is set to 10 MB.
5. In the Maximum number of admin backup files list, select from 5 through 300 debug files as the maximum number of admin activity backup files retained by the server. By default, XenMobile retains 300 backup files on the server.
6. In the User activity log size list, select a size between 5 and 20 MB. By default, the size of the file is set to 10 MB.
7. In the Maximum number of admin backup files list, select from 5 through 300 debug files as the maximum number of admin activity backup files retained by the server. By default, XenMobile retains 300 backup files on the server.

To configure Log Level options

1. Click Support > Log Settings and then expand Log level to display configuration options. Click Edit all to configure elements of the log level.

▼ Log level



The Set Log Level screen appears.

Set Log Level ×

Class name

Sub-class name

Log level

Included loggers

Persist settings

2. Enter the Class Name. By default, this field is set to All.
3. Enter the Sub-class name. By default, this field is set to All
4. In the Log level list, select a log level. The supported log levels include Fatal, Error, Warning, Info, Debug, Trace, or Off. The Included Loggers field displays currently configured log levels for each configured class.
5. If you want to persist the log level settings, select the Persist settings check box.
6. Click Set to commit your changes.

To add a custom logger

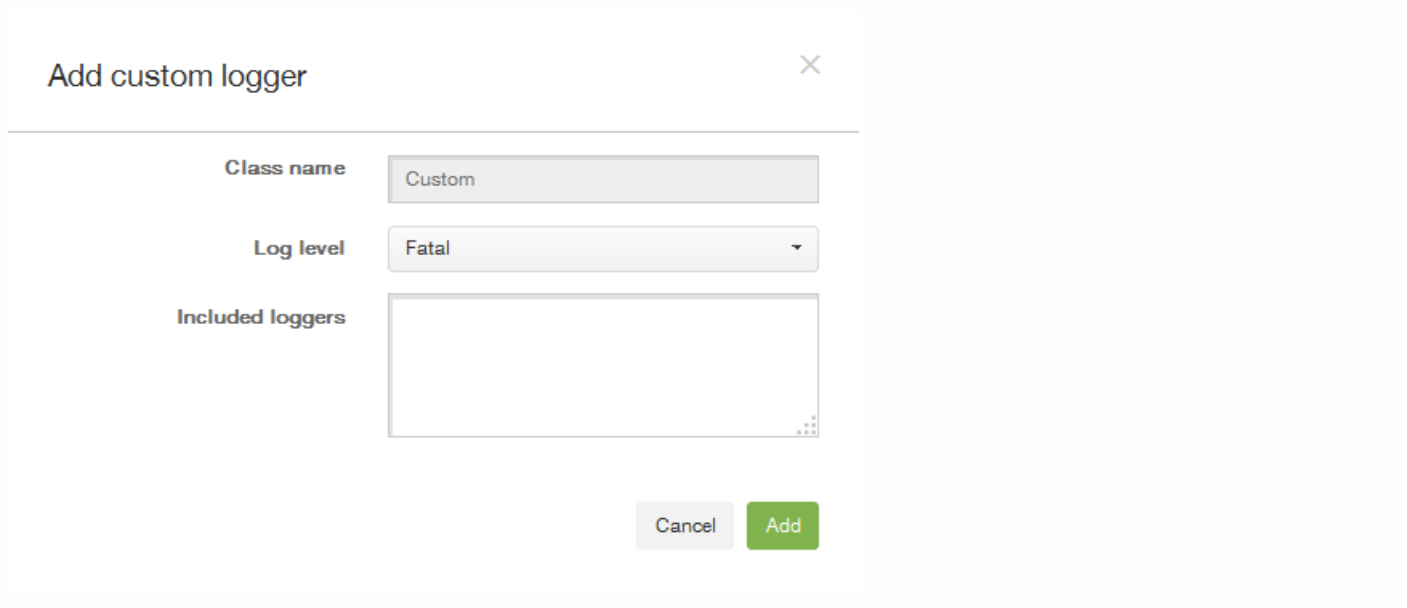
1. To add a Custom Logger, click Add.

▼ Custom Logger



Add

The Add custom logger screen appears.

A dialog box titled "Add custom logger" with a close button (X) in the top right corner. The dialog contains three fields: "Class name" with a text input field containing "Custom"; "Log level" with a dropdown menu showing "Fatal"; and "Included loggers" with an empty list box. At the bottom of the dialog are two buttons: "Cancel" and "Add".

Add custom logger ×

Class name Custom

Log level Fatal ▼


Included loggers

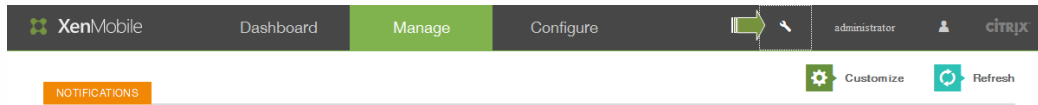
Cancel Add

2. Specify a Class name.
3. In the Log level list, select a log level. The supported log levels include Fatal, Error, Warning, Info, Debug, Trace, or Off. The Included Loggers field displays currently configured log levels for each configured class.
4. Click Add.

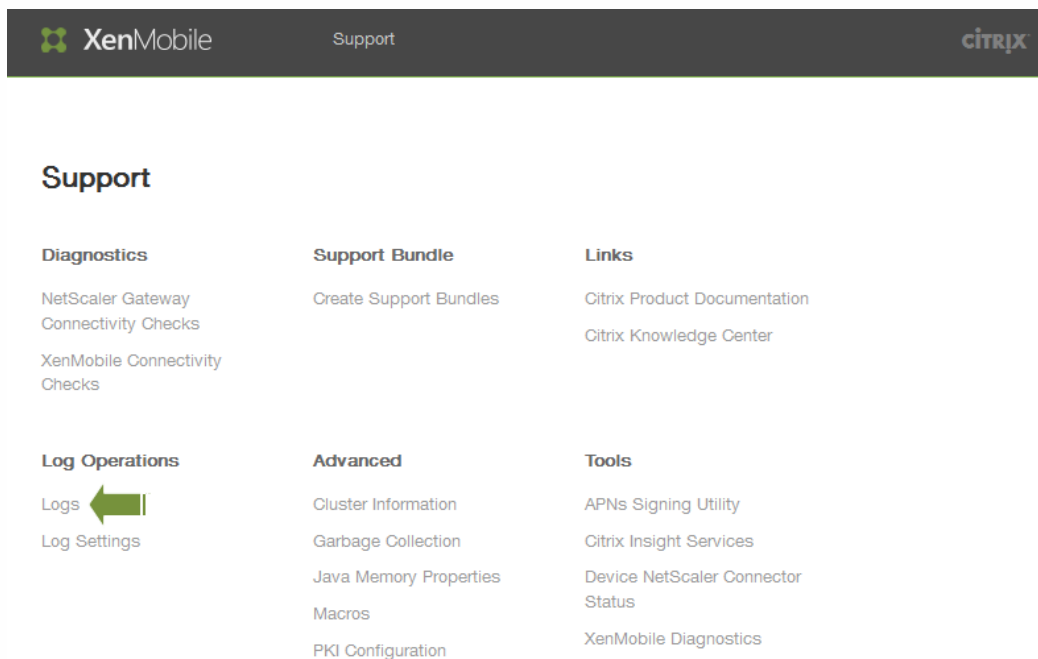
Viewing and Analyzing Log Files in XenMobile

Feb 13, 2015

1. In the XenMobile console, click the wrench icon  in the upper-right corner of the console. The Support page opens in a new browser window.



2. Under Log Operations, click **Logs**. The **Logs** screen appears. Individual logs appear in a table.



3. Select the log you want to view. A debug log contains information useful for Citrix Support; it contains useful information such as error messages, and server-related actions. User activity logs display information related to each configured user. The **Logs** screen appears. Individual logs appear in a table.

Support > [Logs](#)

Logs

Analyze the details of various types of logs.

Download All |
 View |
 Rotate |
 Download

<input type="checkbox"/>	Log Name	Log Type
<input type="checkbox"/>	DebugLog	Debug
<input type="checkbox"/>	AdminActivityLog	Admin Activity
<input checked="" type="checkbox"/>	UserActivityLog	User Activity

Showing 1 - 3 of 3 items

4. Use the actions at the top of the table to do the following:

- Download All logs: The console downloads all the logs present on the system (including debug, user/admin activity, server logs, and so on). Click Download allows you to save only those logs selected; it also downloads archived logs).

Logs

Analyze the details of various types of logs.


Download All |
 View |
 Rotate |
 Download

<input type="checkbox"/>	Log Name
<input type="checkbox"/>	Debug Log File
<input type="checkbox"/>	Admin Audit Log File
<input checked="" type="checkbox"/>	User Audit Log File

- View: Shows the contents of the log below the table.

Logs

Analyze the details of various types of logs.

   
Download | **View** | Rotate | Download

<input type="checkbox"/>	Log Name	Log Type
<input type="checkbox"/>	Debug Log File	Debug
<input checked="" type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Admin Audit Log File

```
2015-01-13T12:04:01.691-0800 "" "FF652948C084E77D" "" "ZdmService_Login" "Success" "" "Login with [UserName = administrator] response successful"
2015-01-13T12:04:13.328-0800 "administrator" "4550D7E54CC3A112" "10.252.56.85" "UserService_DeleteUserProperty" "Success" "" "Mozilla/5.0 (Macintosh; Intel
2015-01-13T12:04:13.528-0800 "administrator" "4550D7E54CC3A112" "10.252.56.85" "UserService_DeleteUserProperty" "Success" "" "Mozilla/5.0 (Macintosh; Intel
2015-01-13T12:04:19.5-0800 "administrator" "4550D7E54CC3A112" "10.252.56.85" "Licensing_SaveLicenseInfo" "Success" "" "Mozilla/5.0 (Macintosh; Intel Mac OS
2015-01-13T12:04:19.778-0800 "administrator" "4550D7E54CC3A112" "10.252.56.85" "UserService_DeleteUserProperty" "Success" "" "Mozilla/5.0 (Macintosh; Intel
2015-01-13T12:04:24.919-0800 "administrator" "4550D7E54CC3A112" "10.252.56.85" "General_SaveInitialConfig" "Success" "" "Mozilla/5.0 (Macintosh; Intel Mac OS
2015-01-13T12:05:15.236-0800 "administrator" "4550D7E54CC3A112" "10.252.56.85" "ZdmService_Login" "Success" "" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5
```

- Delete: Permanently removes a selected log file.
- 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.

Rotate Logs ✕

Are you sure you want to archive the current log file and create a new file to capture log entries?

XenMobile Command-Line Interface Options

Feb 13, 2015

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 cluser, 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]

/

-
- [AppDNA](#)
 - [Citrix Cloud](#)
 - [Citrix Receiver](#)
 - [CloudBridge](#)
 - [CloudPortal Services Manager](#)
 - [NetScaler](#)
 - [NetScaler Gateway](#)
 - [NetScaler SD-WAN](#)
 - [ShareFile](#)
 - [Unidesk](#)
 - [VDI-in-a-Box](#)
 - [XenApp and XenDesktop](#)
 - [XenMobile](#)
 - [XenServer](#)
-
- [Advanced Concepts](#)
 - [Developer](#)
 - [Legacy Documentation](#)

Feel your pain.

This link is not here. The link might be misspelled or outdated.

Search or navigate for the content
and retry the link

Investigate

Feedback link at the bottom of [Docs.citrix.com](https://docs.citrix.com) to tell us about it

XenMobile Mail Manager 10

Feb 20, 2015

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.

The following are known and fixed issues in the current release of XenMobile Mail Manager 10.0. To download XenMobile Mail Manager, go to the Server Components section under XenMobile 10 Server on Citrix.com.

- 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.

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. 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.

System Requirements and Prerequisites

Jan 13, 2017

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 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
- Exchange Server 2013
- Exchange Server 2010 SP2

Device email clients

Not all email clients consistently return the same ActiveSync ID for a device. Because XenMobile Mail Manager expects a unique ActiveSync ID for each device, only email clients that consistently generate the same, unique ActiveSync ID for each device are supported. These email clients have been tested by Citrix and performed without errors:

- HTC native email client
 - Samsung native email client
 - iOS native email client
 - Touchdown for Smartphones
-
- Windows Management Framework must be installed.
 - PowerShell V4, V3, and V2
 - 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-Premise Computer Running Exchange

- **Permissions.** Exchange Role-Based Access Control (RBAC) is beyond the scope of this documentation. That being said, at a minimum, 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:
 - Get-CASMailbox
 - Set-CASMailbox
 - Get-Mailbox
 - Get-ActiveSyncDevice
 - Get-ActiveSyncDeviceStatistics
 - Clear-ActiveSyncDevice
- 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 <http://technet.microsoft.com/en-us/library/dd315349.aspx>, 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, <http://blogs.msdn.com/b/powershell/archive/2009/11/23/you-don-t-have-to-be-an-administrator-to-run-remote-powershell-commands.aspx>, `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

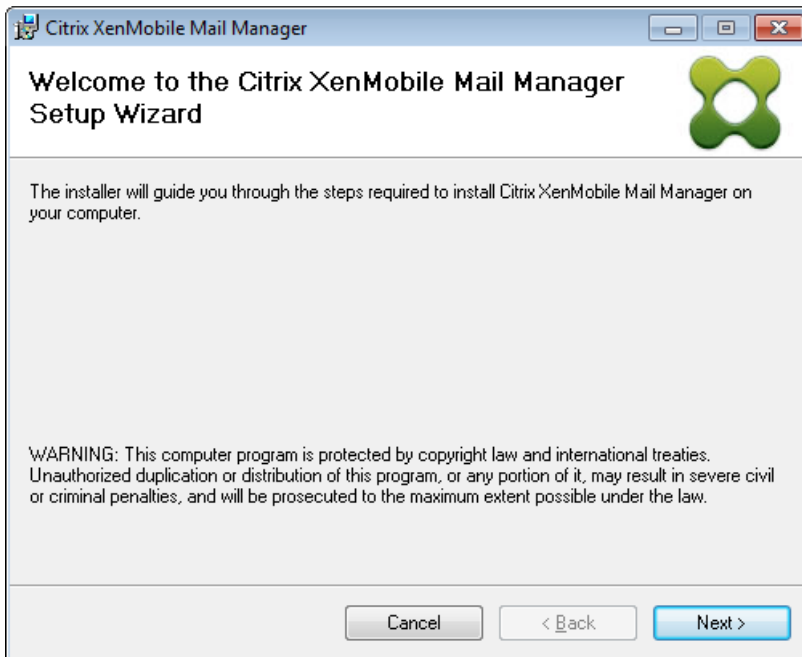
- **Permissions.** Exchange Role-Based Access Control (RBAC) is beyond the scope of this documentation. That being said, at a minimum, the credentials specified in the Exchange Configuration UI must be able to connect to Office 365 and be given full access to execute the following Exchange-specific PowerShell cmdlets:
 - `Get-CASMailbox`
 - `Set-CASMailbox`
 - `Get-Mailbox`
 - `Get-ActiveSyncDevice`
 - `Get-ActiveSyncDeviceStatistics`
 - `Clear-ActiveSyncDevice`
- 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

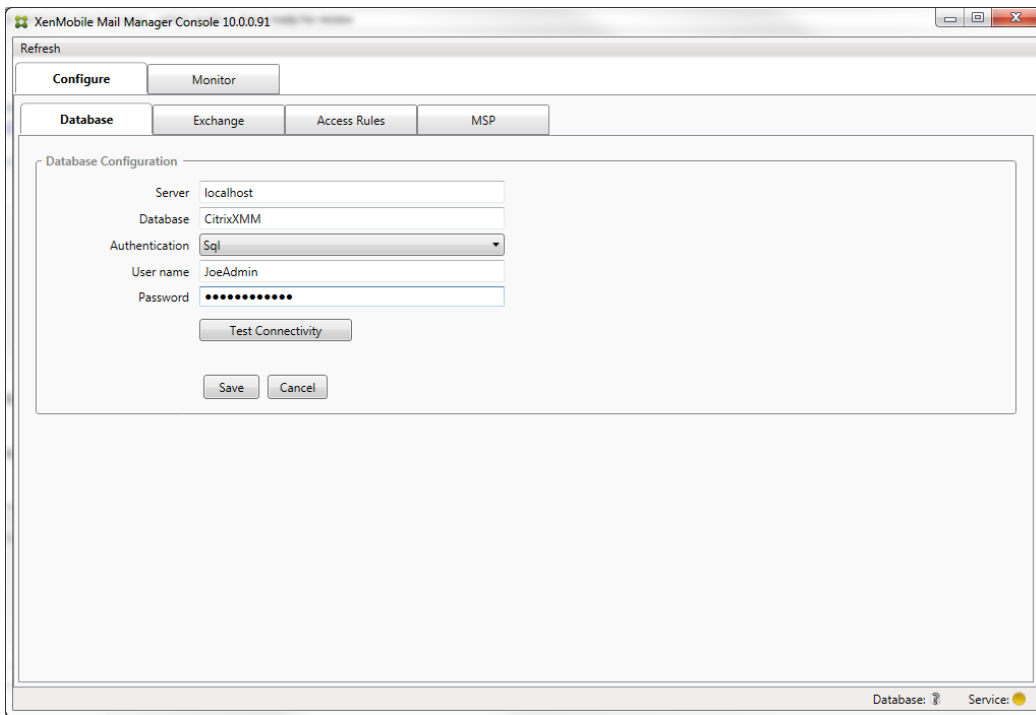
Apr 17, 2015

Follow these steps to install and configure XenMobile Mail Manager. Before starting, be sure you review the system requirements and prerequisites. For details, see [XenMobile Mail Manager System Requirements and Prerequisites](#).

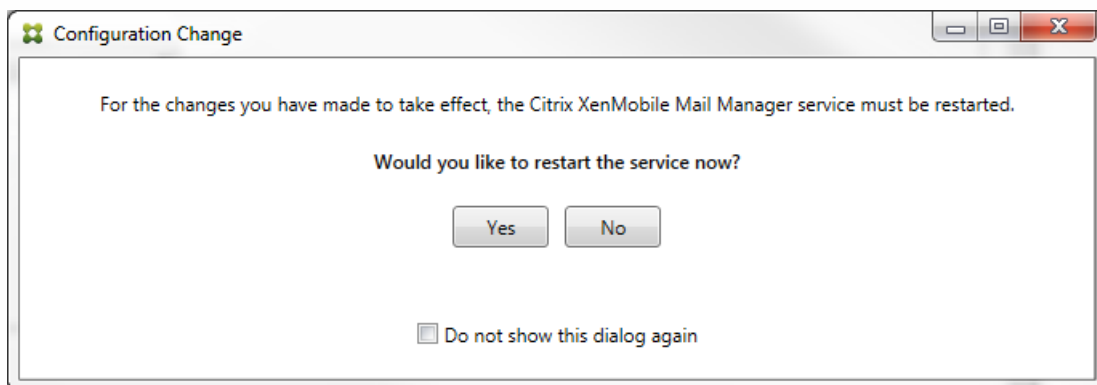
1. Click the XmmSetup.msi file and then follow the prompts in the installer to install XenMobile Mail Manager.



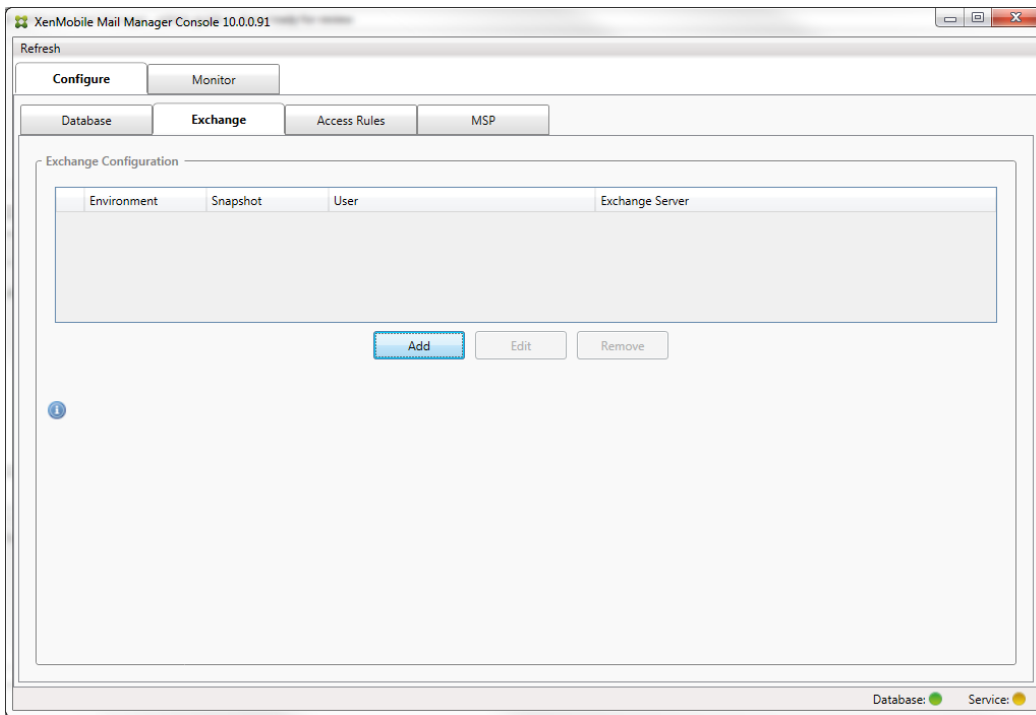
2. From the Start menu, open XenMobile Mail Manager.
3. Configure the following database properties:
 1. Select the Configure > Database tab.
 2. Enter the name of the SQL Server (defaults to localhost).
 3. Keep the database as the default CitrixXmm.
 4. Select one of the following Authentication modes 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.



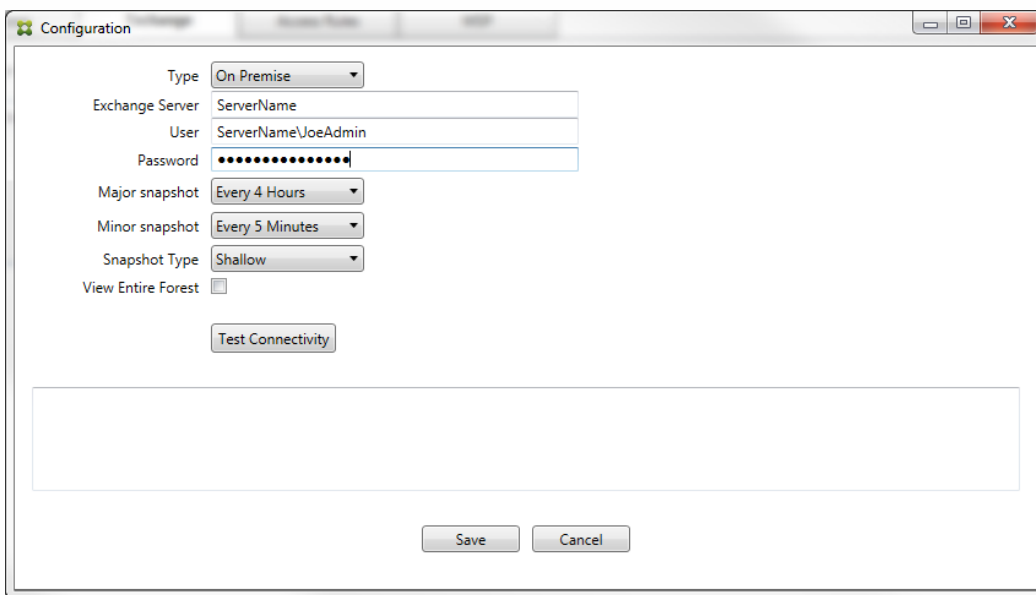
5. Click Test Connectivity to check that a connection can be made to the SQL Server and then click Save.
4. A message prompts you to restart the service. Click Yes.



5. Configure one or more Exchange Server:
 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.



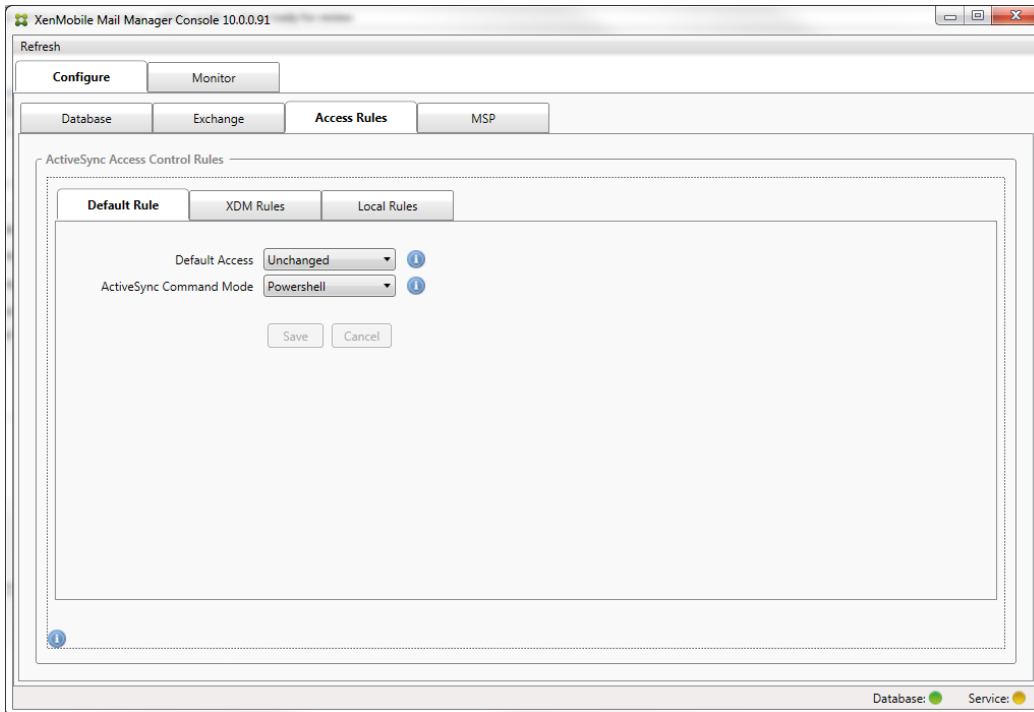
3. Click Add.
4. Select the type of Exchange Server environment: On Premise or Office 365.



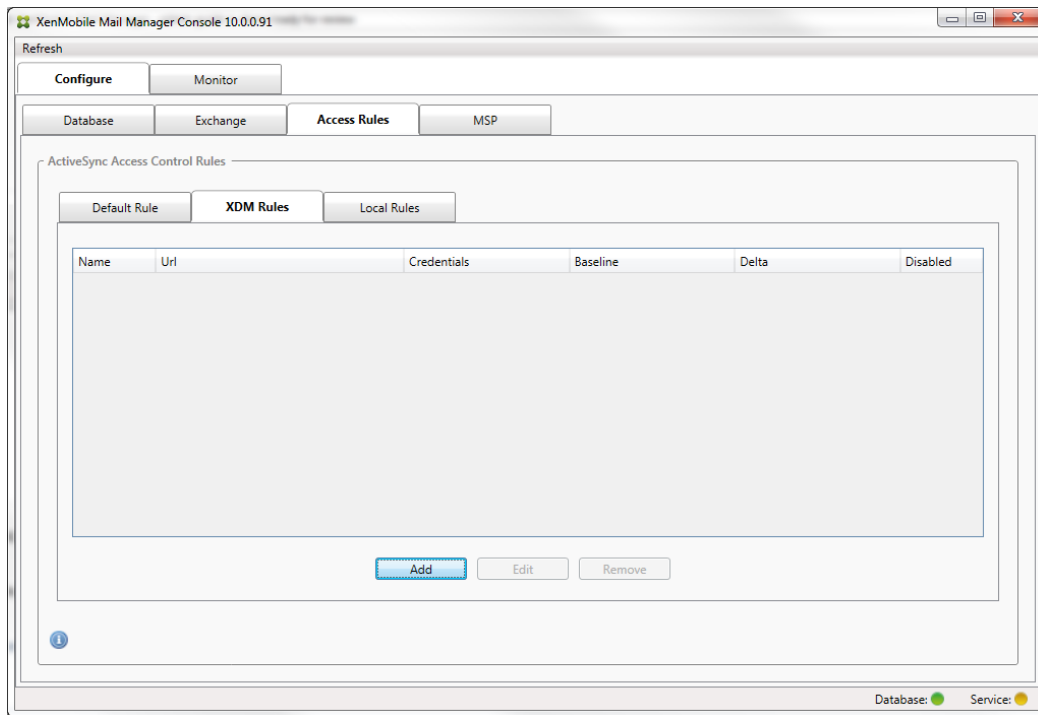
5. If you select On Premise, enter the name of the Exchange Server that will be used for Remote PowerShell commands.
6. Enter the user name of a Windows identity that has appropriate rights on the Exchange Server as specified within the Requirements section.
7. Enter the Password for the user.
8. Select 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.

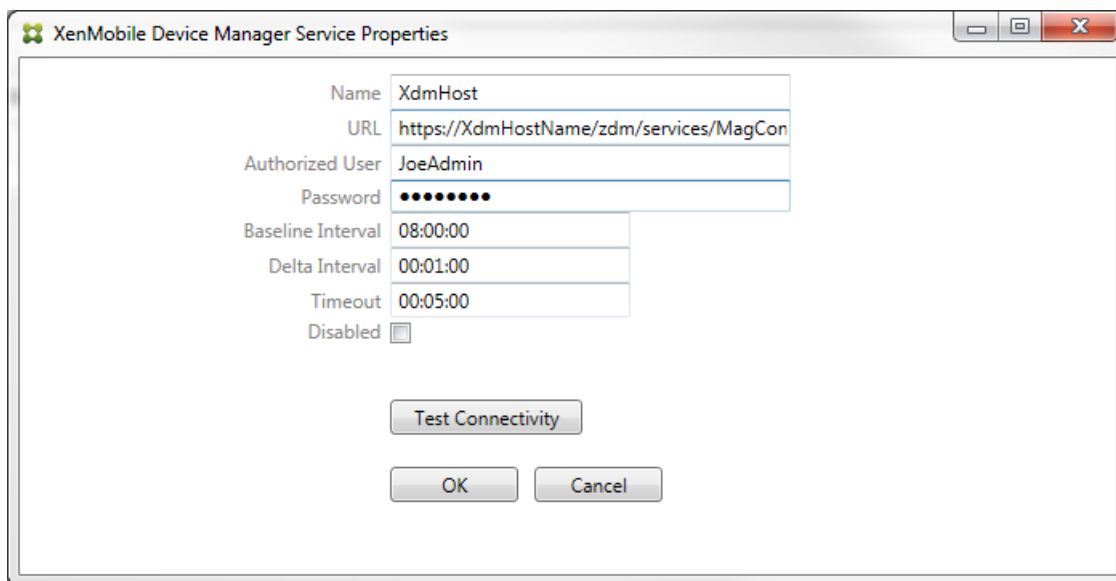
11. Click Test Connectivity to check that a connection can be made to the Exchange Server and then click Save.
 12. A message prompts you to restart the service. Click Yes.
6. Configure the access rules:
1. Select the Configure > Access Rules tab.



2. 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 select Unchanged, no change will be made.
 3. 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.
 4. Click Save.
7. Click the XDM Rules tab.

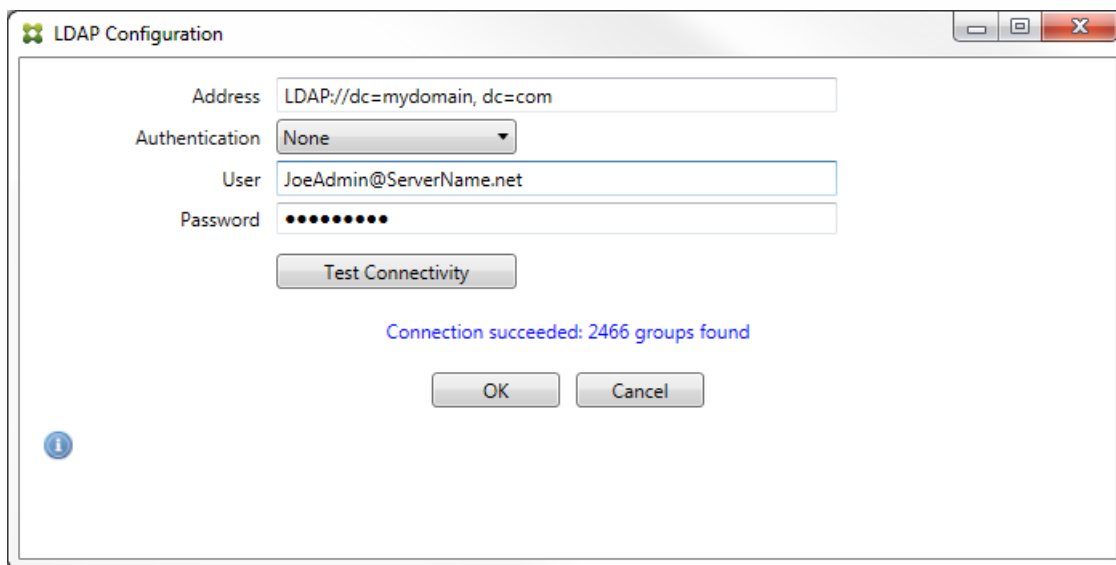


1. Click Add.
2. Enter a name for the XDM rules, such as XdmHost.

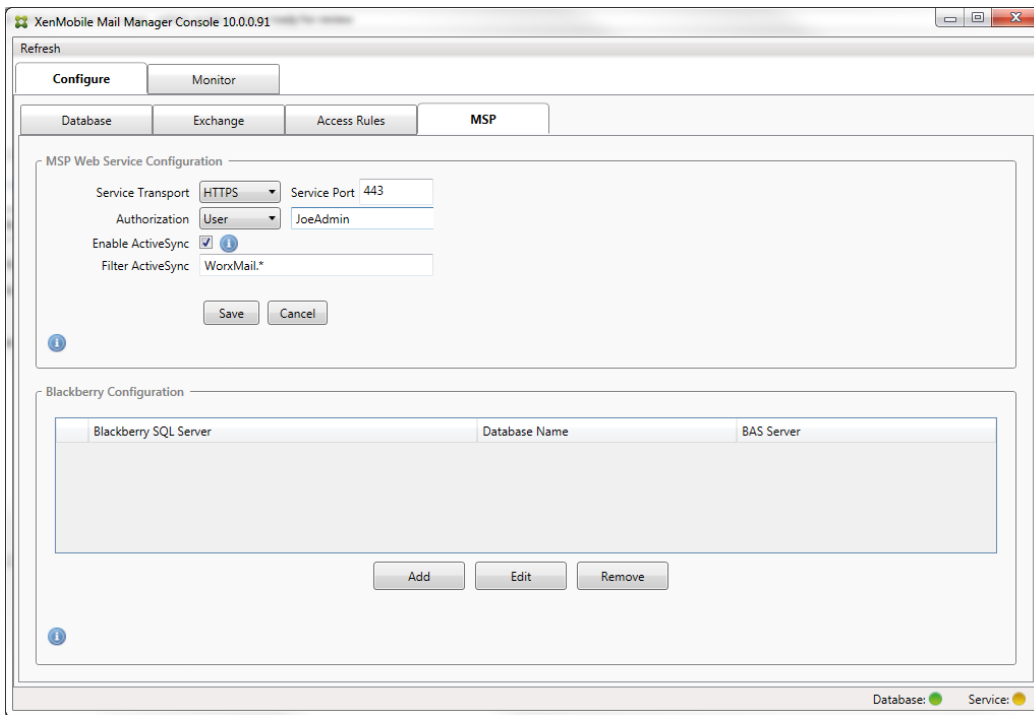


3. Modify the URL string to refer to the XenMobile server; for example, if the server name is XdmHost, enter http://XdmHostName/zdm/services/MagConfigService.
4. Enter an authorized user on the server.
5. Enter the password of the user.
6. Keep the default values for the Baseline Interval, Delta Interval, and Timeout values.
7. 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.
8. Click OK.
8. Click the Local Rules tab.

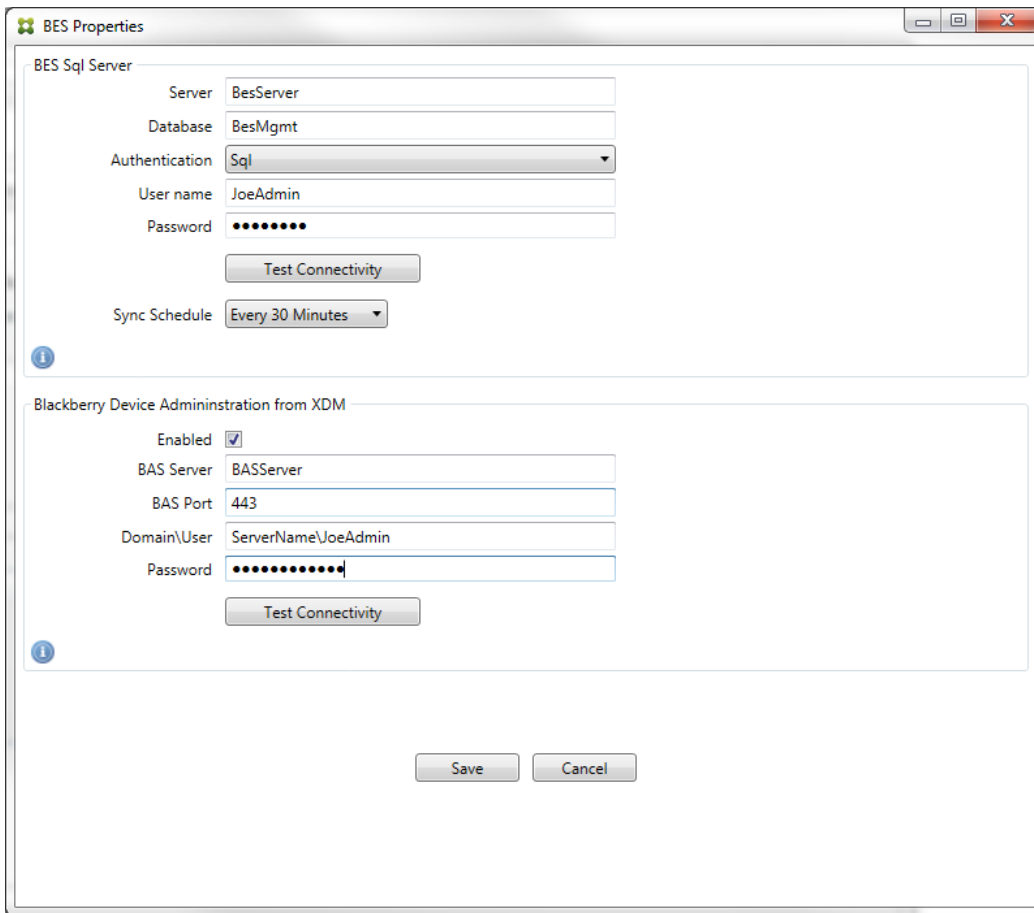
1. If you want to construct local rules that operate on Active Directory Groups, click Configure LDAP and then configure the LDAP connection properties.



2. You can add local rules based on ActiveSync Device ID, Device Type, AD Group, 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.
9. 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 Configure > 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.
7. Click Save.
10. Optionally, configure one or more BlackBerry Enterprise Server (BES):
 1. Click Add.
 2. Enter the server name of the BES SQL Server.



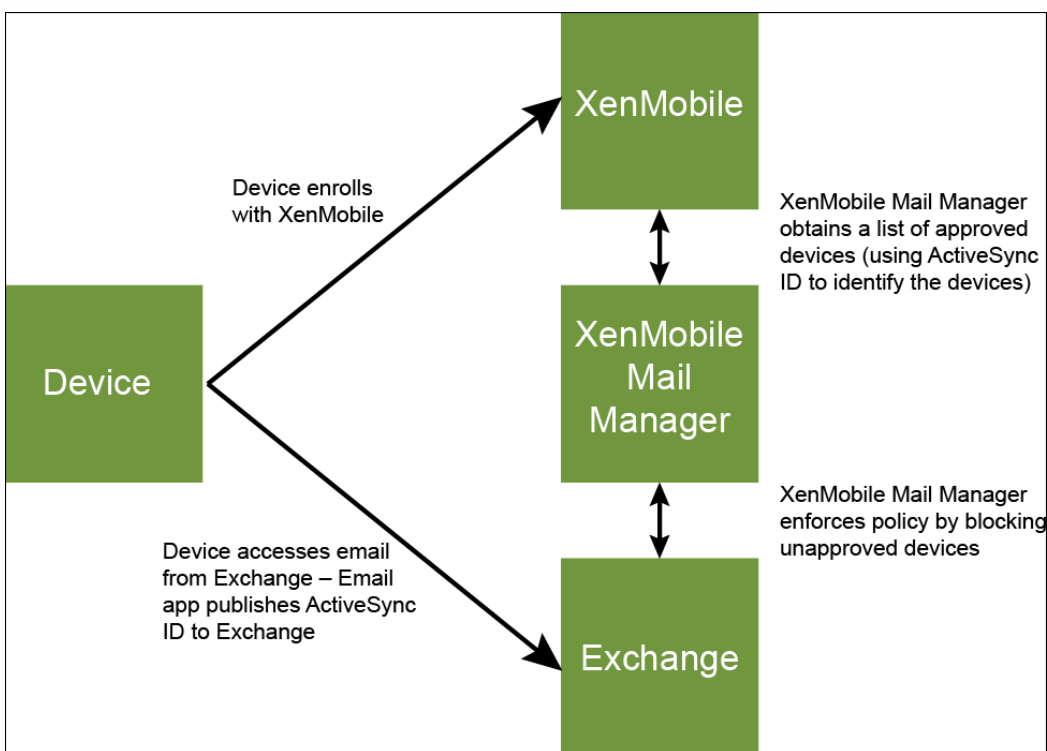
3. Enter the database name of the BES management database.
4. Select the Authentication mode. If you select Windows Integrated authentication, the user account of the XenMobile Mail Manager service is the account that is used to connect to the BES SQL Server.
Note: If you also choose Windows Integrated 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

May 08, 2015

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. Work Home obtains a similar identifier and sends the identifier to XenMobile when the device is enrolled. By comparing the two device IDs, XenMobile Mail Manager can determine whether a specific device should have corporate email access. The following figure illustrates this concept:



If XenMobile sends XenMobile Mail Manager an ActiveSync ID that is different from the ID the device publishes to Exchange, XenMobile Mail Manager cannot indicate to Exchange what to do with the device.

Matching ActiveSync IDs works reliably on most platforms; however, Citrix has found that on some Android implementations, the ActiveSync ID from the device is different from the ID that the mail client advertises to Exchange. To mitigate this problem, you can do the following:

- On the Samsung SAFE platform, push the device ActiveSync configuration from XenMobile.
- On all other Android platforms, push both the Touchdown app and the Touchdown ActiveSync configuration from XenMobile.

This does not, however, prevent an employee from installing an email client other than Touchdown on an Android device. To guarantee that your corporate email access policy is enforced properly, you can adopt a defensive security stance and

configure XenMobile Mail Manager to block emails by setting the static policy to Deny by default. This means that if an employee does configure an email client on an Android device other than Touchdown, and if ActiveSync ID detection does not work properly, the employee is denied corporate email access.

Access Control Rules

Jan 23, 2017

XenMobile Mail Manager provides a rule-based approach for dynamically configuring access control for Exchange ActiveSync devices. A XenMobile Mail Manager access control rule consists of two parts: a matching expression and a desired access state (Allow or Block). A rule may be evaluated against a given Exchange ActiveSync device to determine if the rule applies to, or matches the device. There are multiple kinds of matching expressions; for example, a rule may match all devices of a given Device Type, or a specific Exchange ActiveSync device ID, or all devices of a specific user, and so on. At any point during the adding, removing, and rearranging of the rules in the rule list, clicking the Cancel button will revert the rules list back to the state at which it was when first opened. Unless you click Save, any changes made to this window are lost if you close the Configure tool.

XenMobile Mail Manager has three types of rules: local rules, 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 XDM 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.

XDM rules: XDM 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 XDM 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 XDM rule will be allowed.
- **Default Access – Block.** Any device that is not matched by either a Local or XDM rule will be blocked.
- **Default Access - Unchanged.** Any device that is not matched by either a Local or XDM 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
- XDM 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 XDM 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.

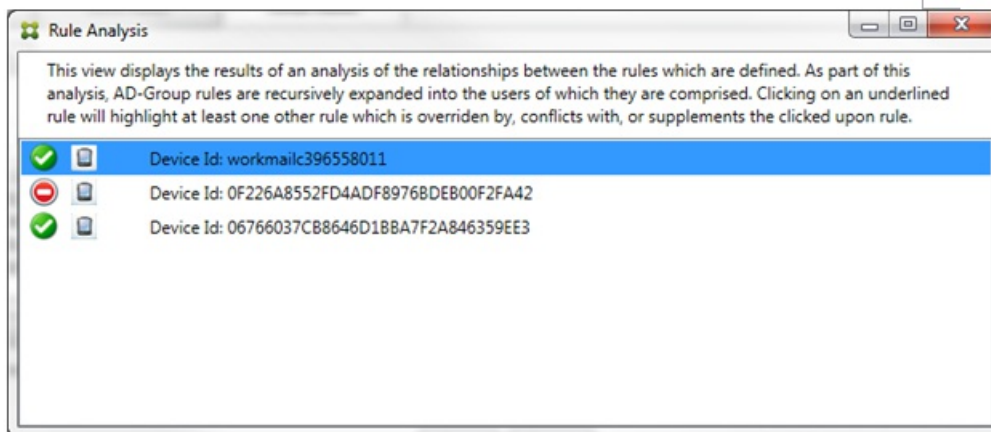
Rule terminology:

- **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

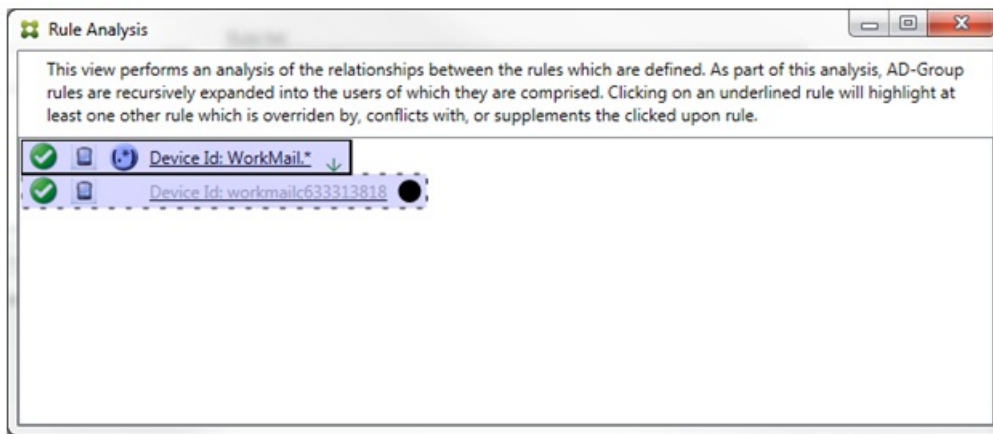
any of the items has no impact; for example, normal selected item visuals will occur.



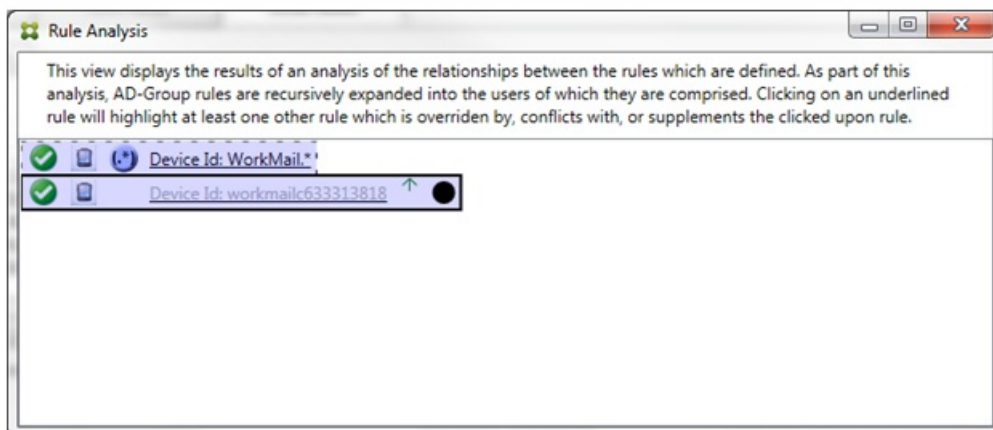
When an override occurs, at least two rules will be underlined: the primary rule and the ancillary rule or rules. At least one ancillary rule will appear in a lighter font to indicate that the rule has been overridden by a higher priority rule. You can click on the overridden rule to find out which rule or rules have overridden the rule. Any time an overridden rule has been highlighted either as a result of the rule being the primary or ancillary rule, a black circle 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:

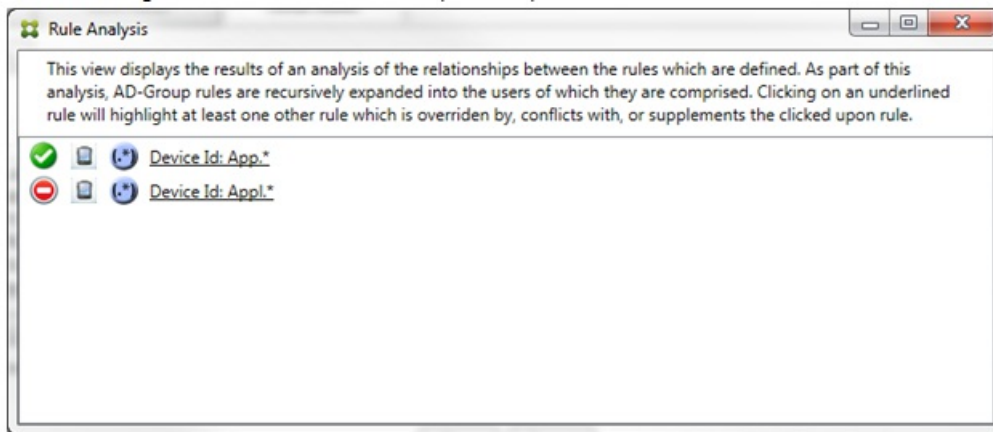


In this example, the regular expression rule WorkMail.* is the primary rule (indicated by the solid border) and the normal rule workmail633313818 is an ancillary rule (indicated by the dashed border). The black dot next to the ancillary rule is a visual cue that further indicates that the rule is inactive (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:

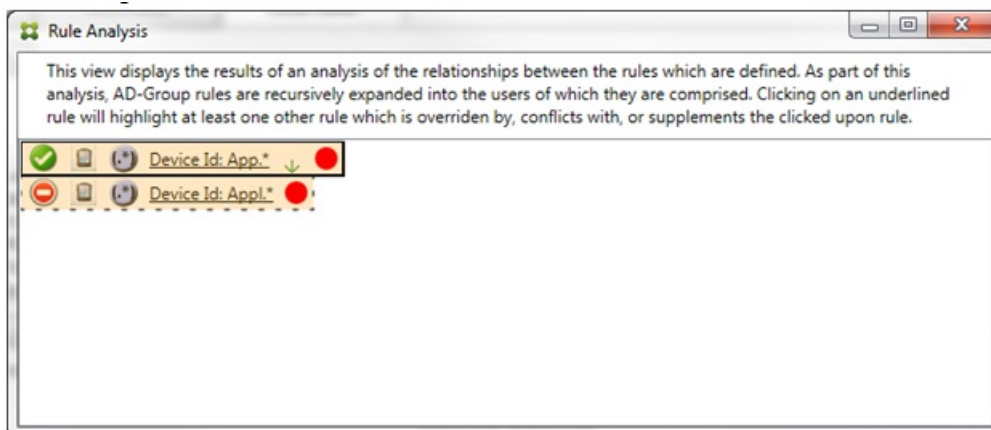


In the preceding example, the regular expression rule WorkMail.* is the ancillary rule (indicated by the dashed border) and the normal rule workmail633313818 is a primary rule (indicated by the solid border). For this simple example, there's not much difference. For a more complicated example, see the 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:

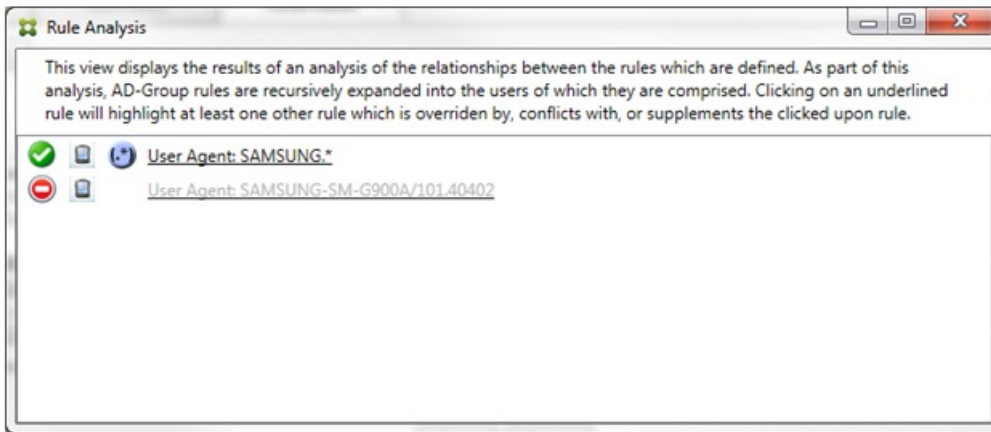


By inspecting the two regular expression rules, it's evident that the first rule allows all devices with a device ID that contains "App" and that the second rule denies all devices with a device ID that contains Appl. In addition, even though the second rule denies all devices with a device ID that contains 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:



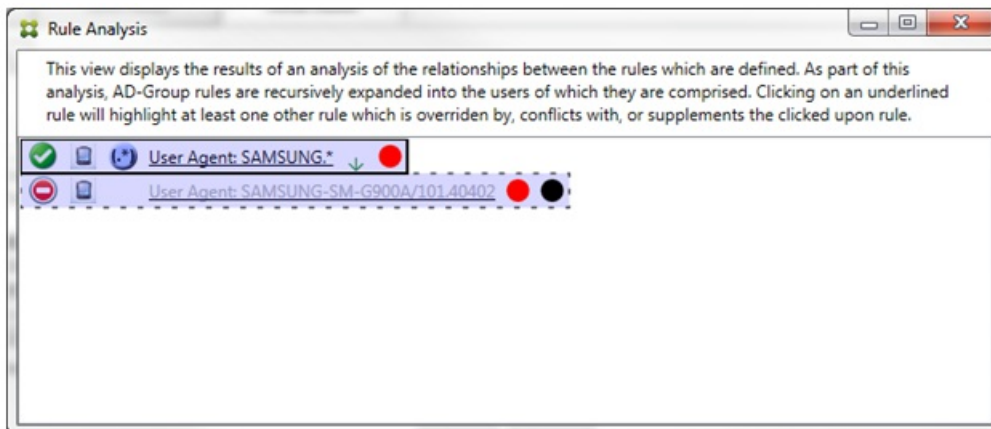
In the preceding scenario, both the primary rule (regular expression rule App.*) and the ancillary rule (regular expression rule Appl.*) are both highlighted in yellow. This is simply a visual warning to alert you to the fact that you have applied more than a single regular expression rule to a single 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.



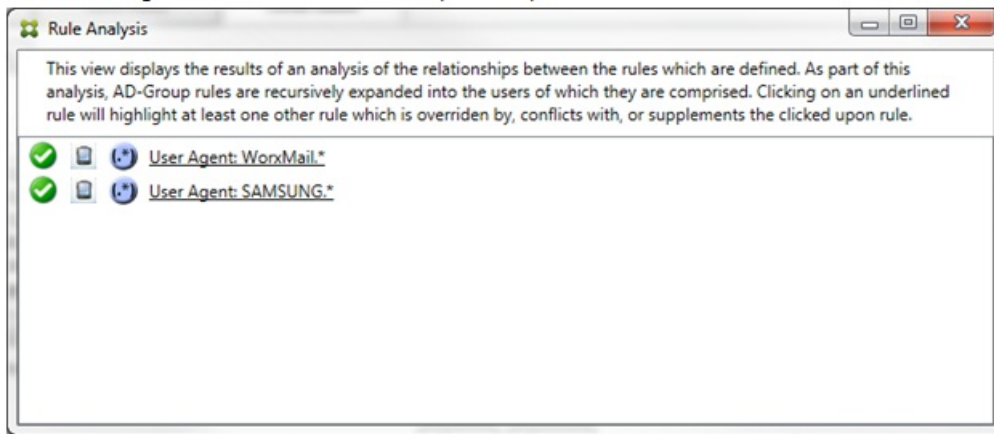
It is easy to see in the preceding example that the first rule (regular expression rule SAMSUNG.*) not only overrides the next rule (normal rule SAMSUNG-SM-G900A/101.40402), but that the two rules differ in their access (primary specifies Allow, ancillary specifies Block). The second rule (normal rule 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:

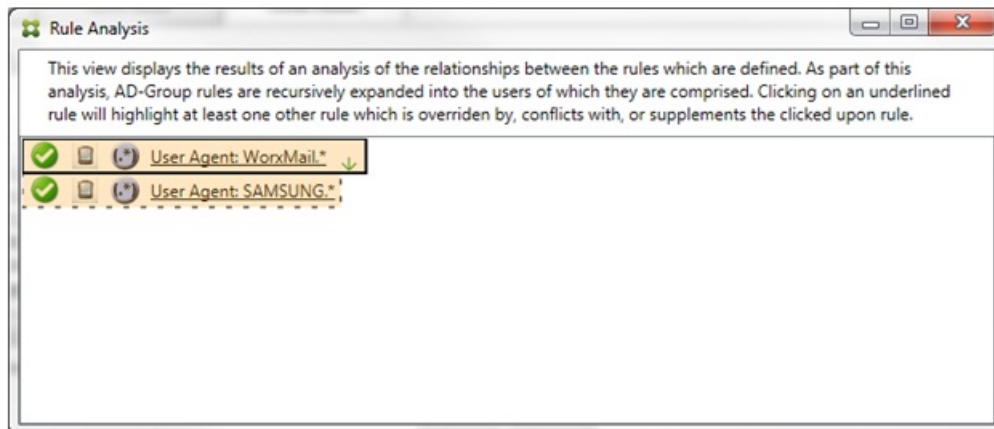


The primary rule (regular expression rule SAMSUNG.*) is followed by a red dot to indicate that its access state conflicts with one or more ancillary rules. The ancillary rule (normal rule SAMSUNG-SM-G900A/101.40402) is followed by a red dot to indicate that its access state conflicts with the primary 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:




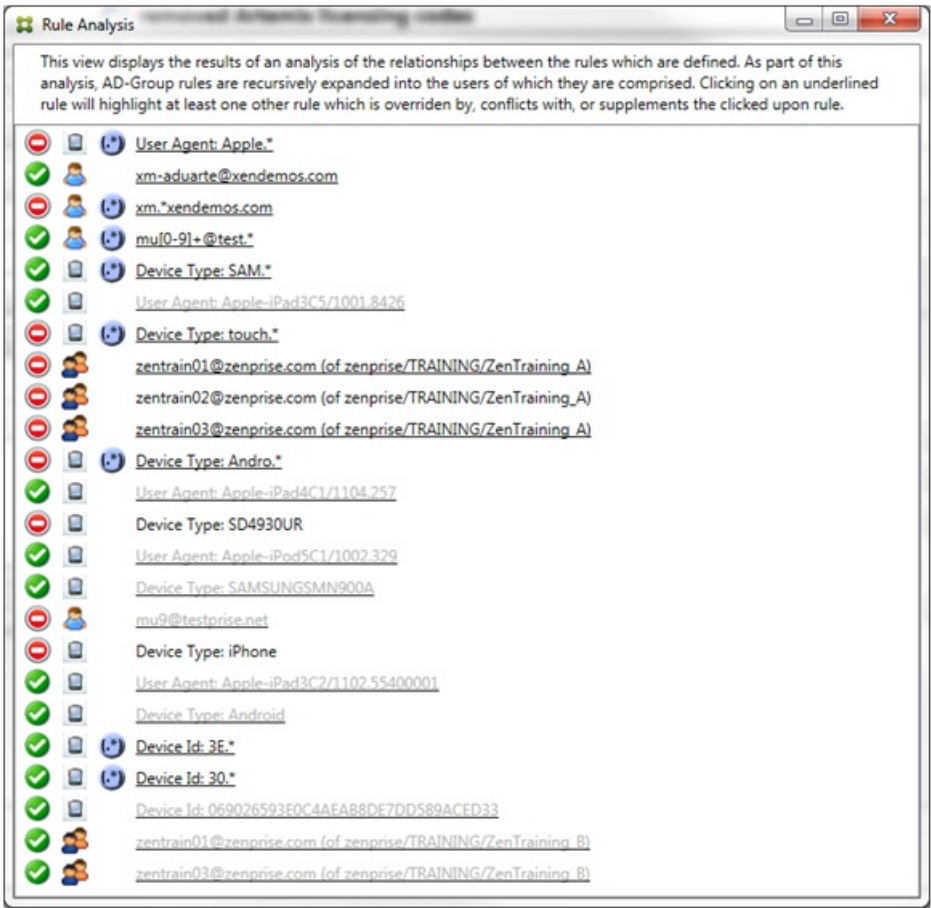
Visual inspection easily reveals that both rules are regular expression rules which have both been applied to the ActiveSync device ID field in XenMobile Mail Manager. After clicking on the first rule, the dialog box looks as follows:



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. 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

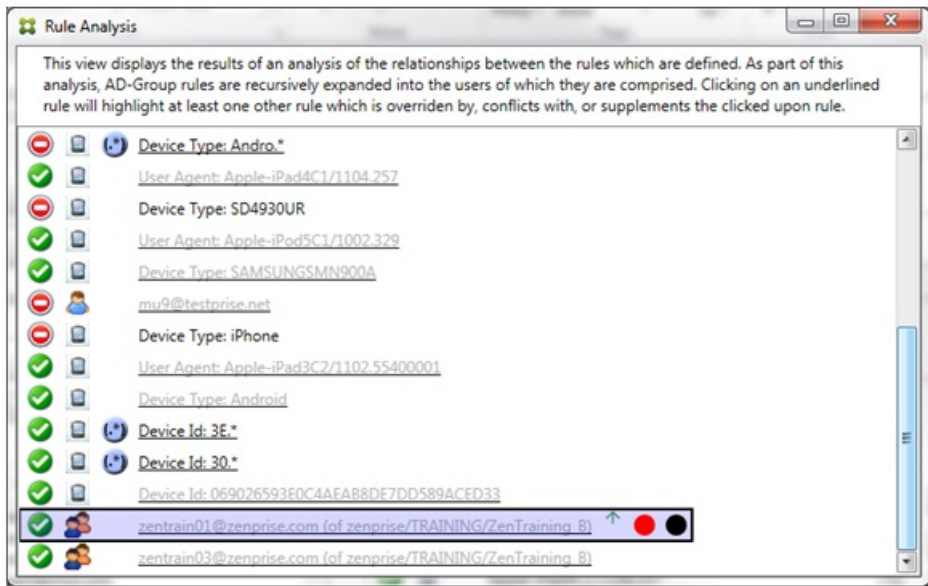
Many potential overrides, conflicts, or supplements can occur, making it impossible to give an example of all possible scenarios. The following example discusses what not to do, while also serving to illustrate the full power of the rule analysis visual construct. Most of the items are underlined in 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.

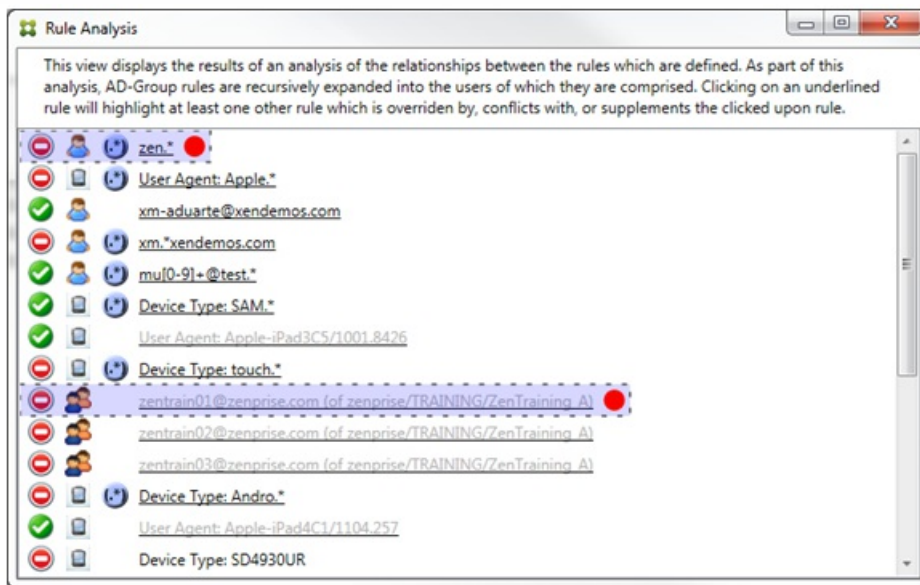
Example 1: This example examines why zetrain01@zenprise.com has been overridden.



The primary rule (AD-Group rule zenprise/TRAINING/ZenTraining B, of which zentra01@zenprise.com is a member) has the following characteristics:

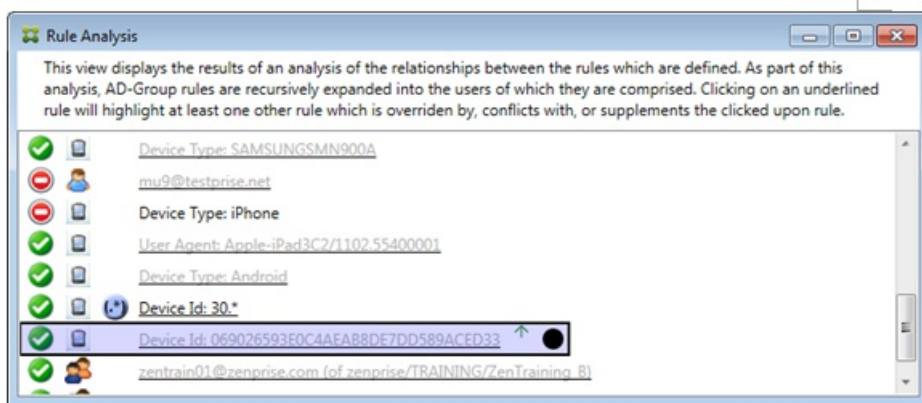
- Is highlighted in blue and has a solid border.
- Has an upwards pointing green arrow (to indicate that the ancillary rule or rules are all to be found above it).
- Is followed by both a red circle and black circle to indicate respectively that one or more ancillary rule conflicts with its access and that the primary rule has been overridden and is hence inactive.

When you scroll up, you see the following:



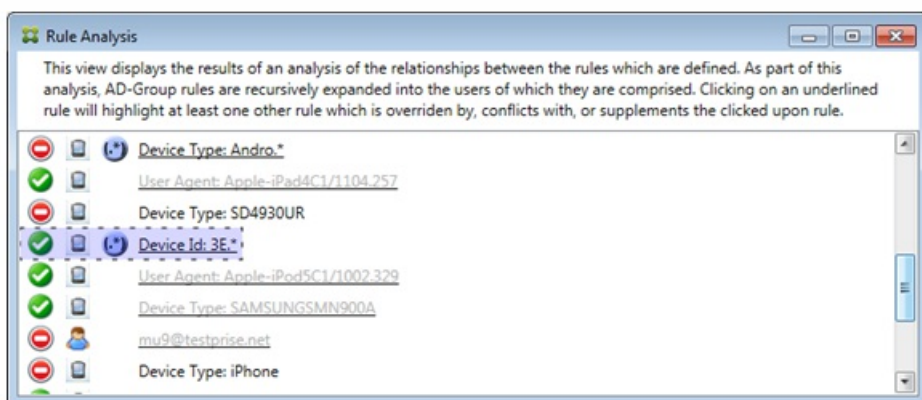
In this case, there are two ancillary rules that override the primary rule: the regular expression rule zen.* and the normal rule zentra01@zenprise.com (of zenprise/TRAINING/ZenTraining A). In the case of the latter ancillary rule, what has occurred is that the Active Directory Group rule ZenTraining A contains the user zentra01@zenprise.com, and the Active Directory Group rule ZenTraining B also contains the user zentra01@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.

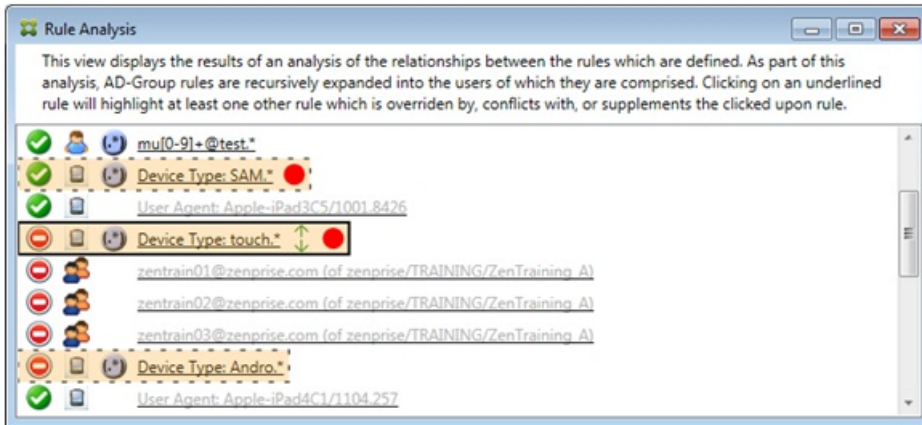
How to Analyze a Supplement and Conflict

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

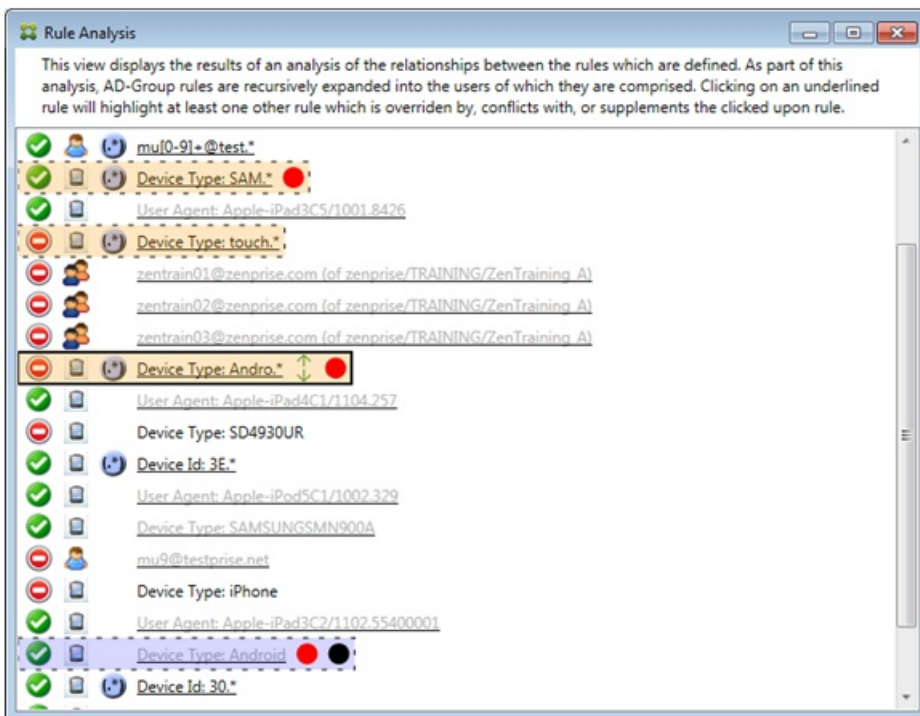
ActiveSync device type rule Andro.*

- Both of the ancillary rules are bordered with dashes to indicate that they are ancillary.
- Both of the ancillary rules are overlaid 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.



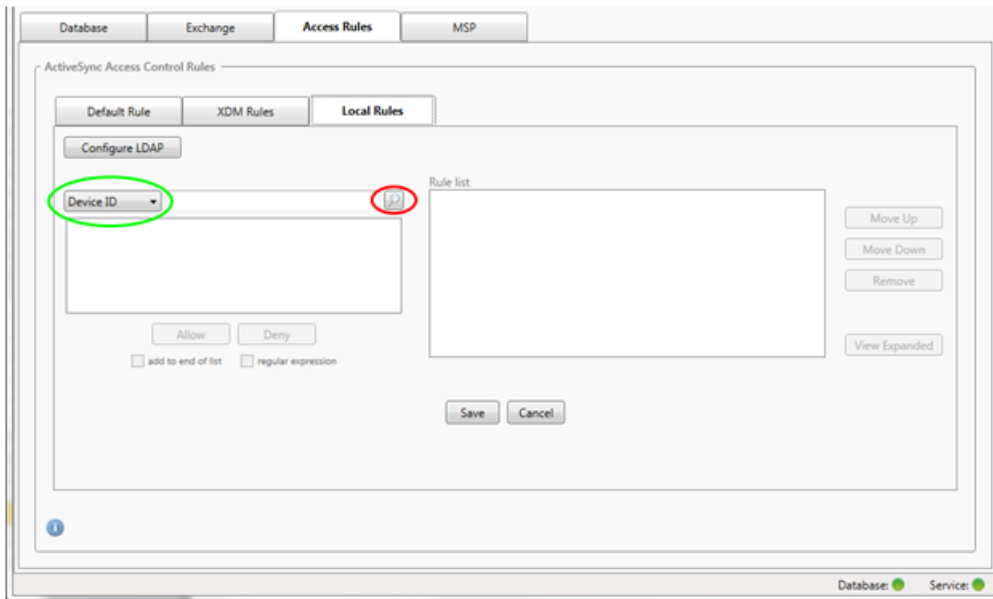
How to Further Analyze the Rules

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.

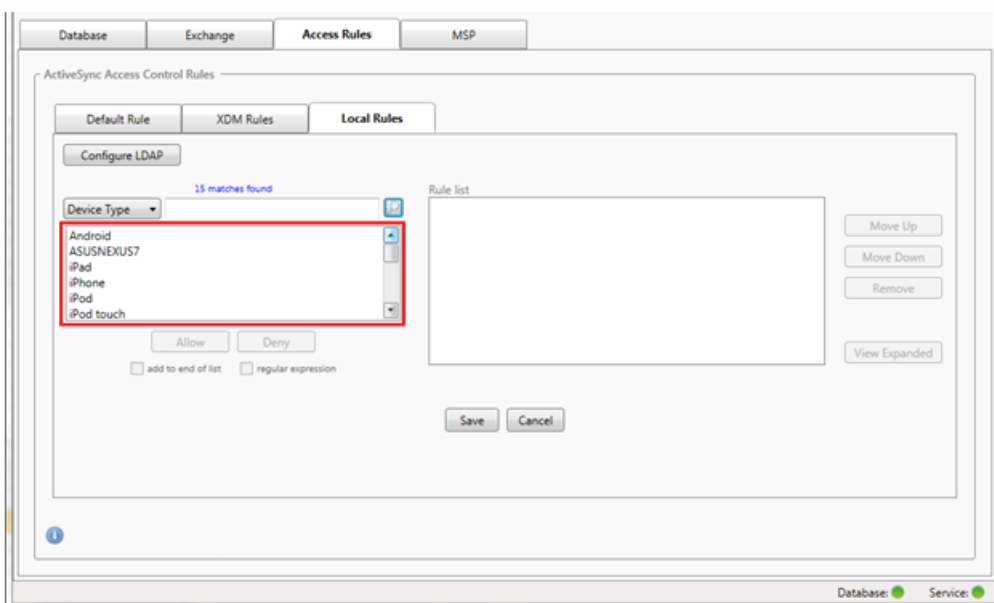


The example shows an overridden rule that is included in the rule relationship. This rule is the normal ActiveSync device type rule Android, which is overridden (indicated by the lightened font and the black circle next to it) and also conflicts in its access with the primary rule regular expression 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.

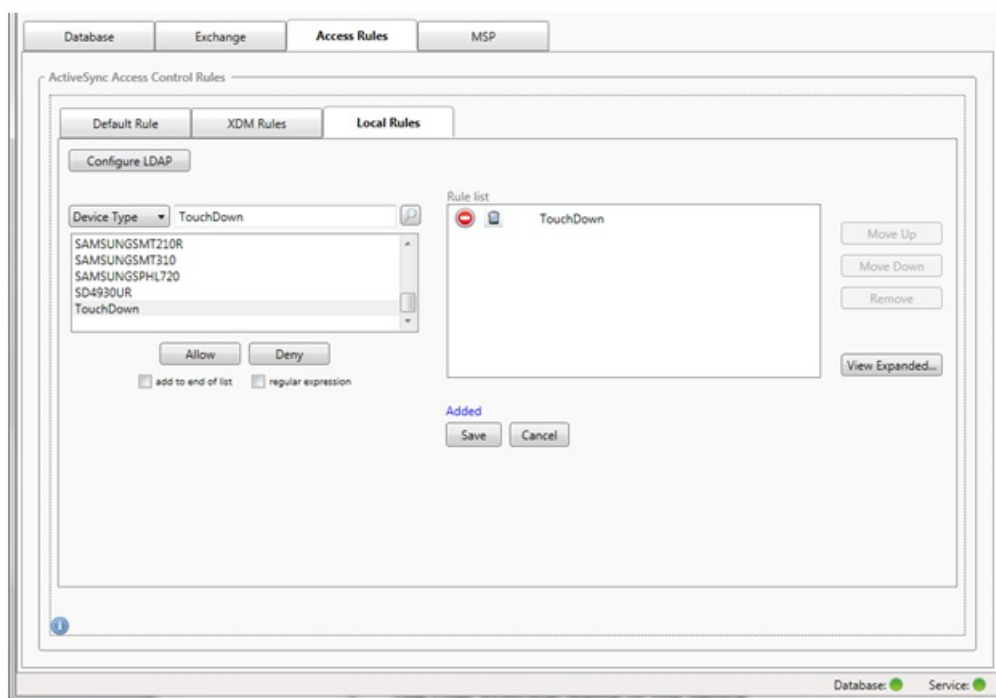
1. Click the Access Rules tab.




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.



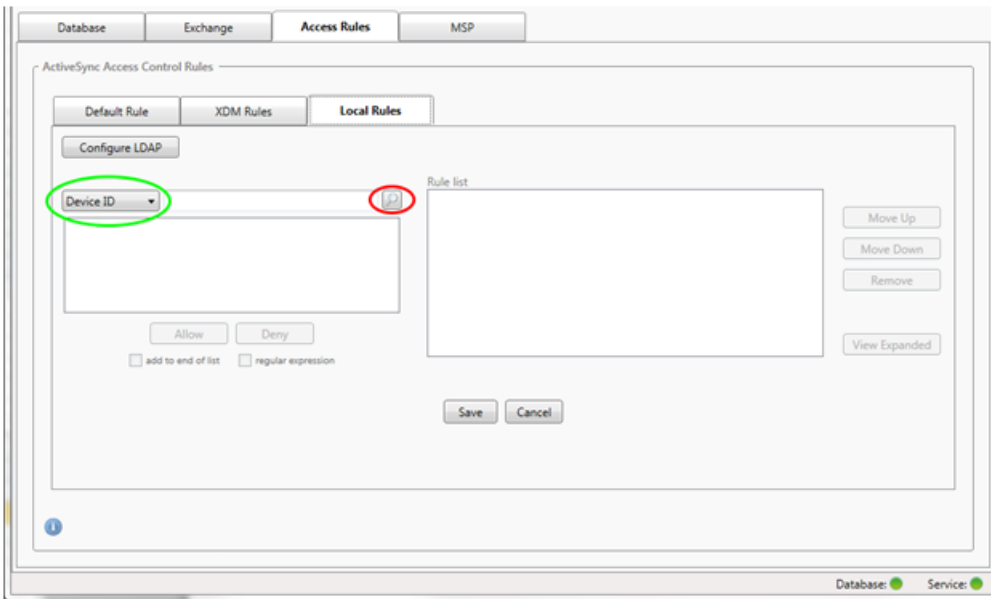
4. Click one of the items in the results list box and then click one of the following options:
- Allow means that Exchange will be configured to allow ActiveSync traffic for all matching devices.
 - Deny means that Exchange will be configured to deny ActiveSync traffic for all matching devices.
- In this example, all devices that have a device type of TouchDown are denied access.



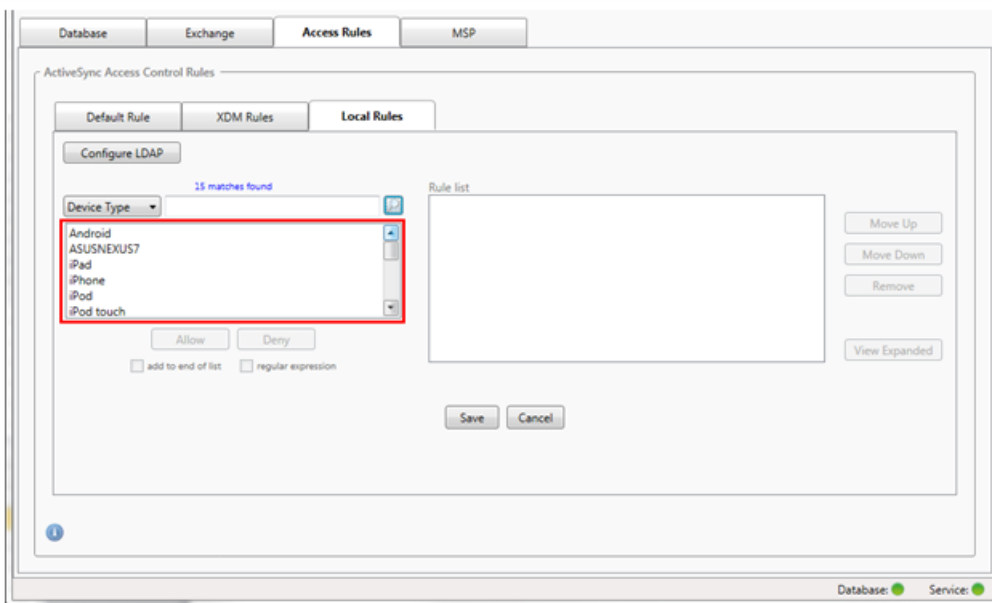
Regular expression local rules can be distinguished by the icon which appears next to them - . To add a regular expression rule, you can either build a regular expression rule from an existing value from the results list for a given field (as long as a major snapshot has completed), or you can simply type in the regular expression that you want.

To build a regular expression from an existing field value

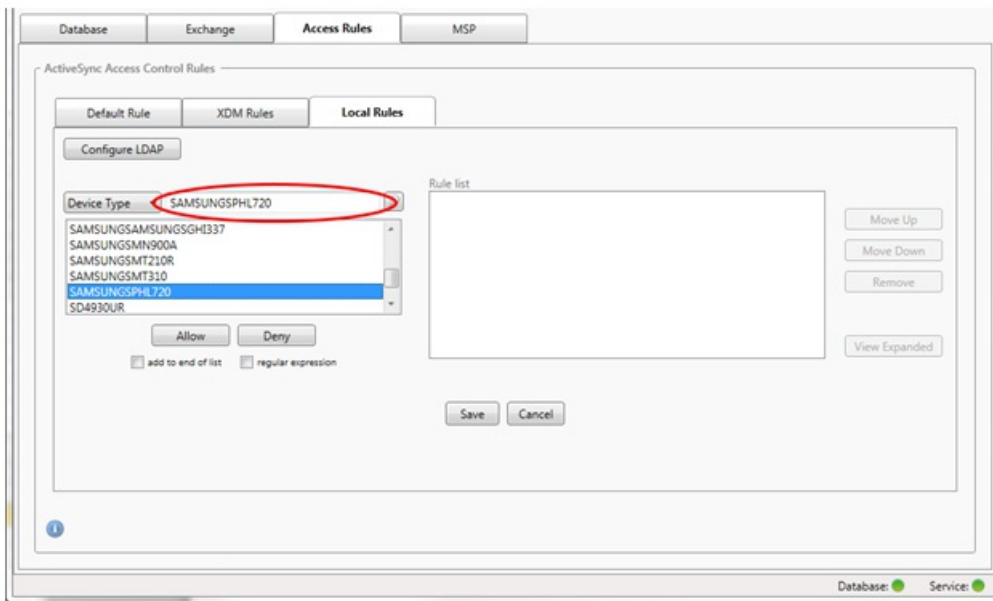
1. Click the Access Rules tab.



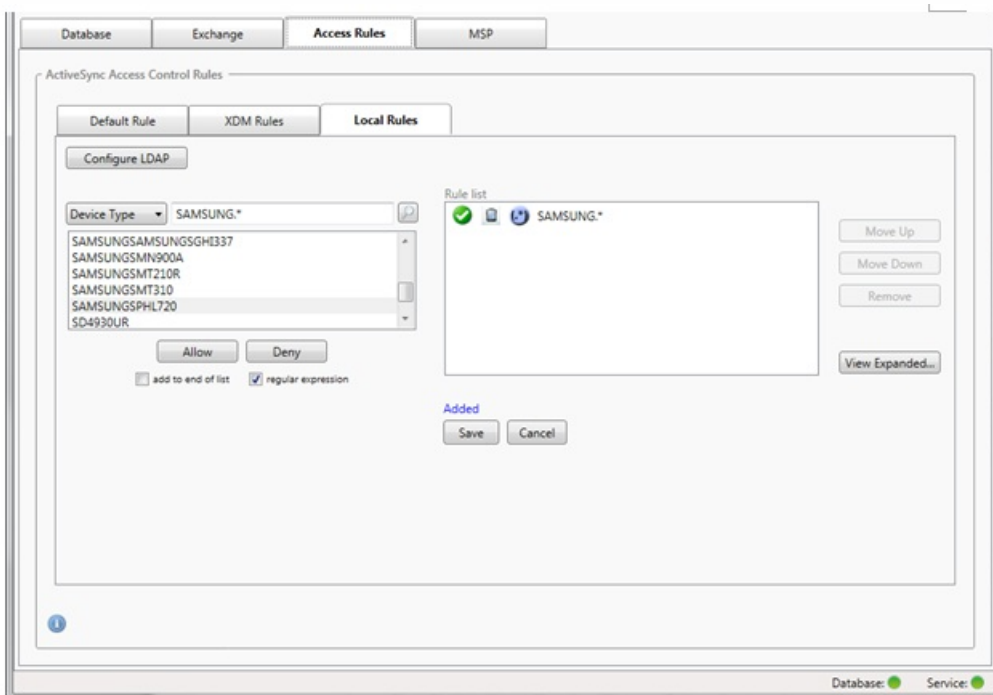
2. In the Device ID list, select the field for which you want to create a regular expression Local Rule.
3. Click on the magnifying glass icon to display all of the unique matches for the chosen field. In this example, the field Device Type has been chosen and the choices are shown below in the list box.



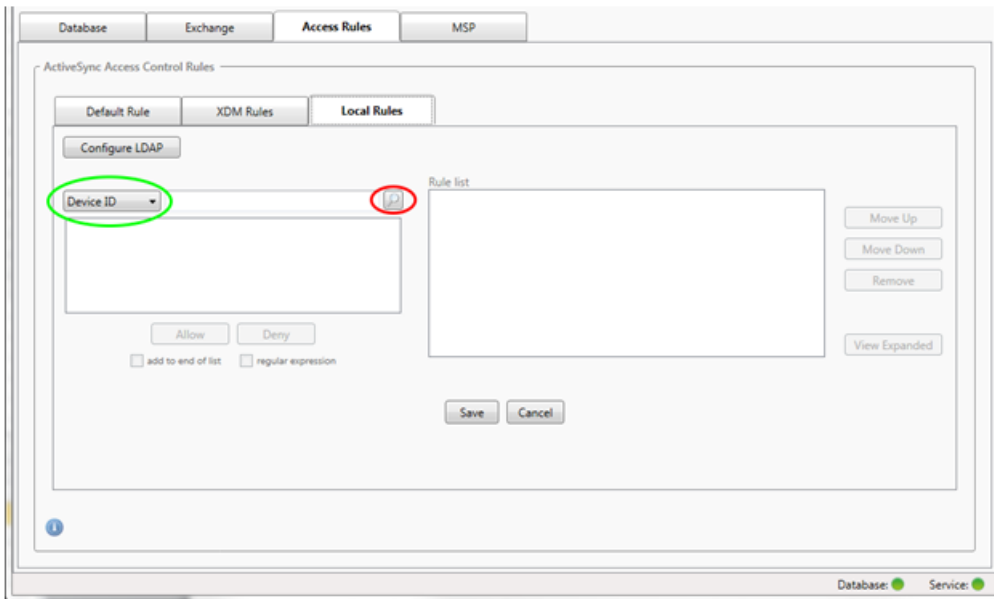
4. Click one of the items in the results list. In this example, SAMSUNGSPHL720 has been selected and appears in the text box adjacent to Device Type.



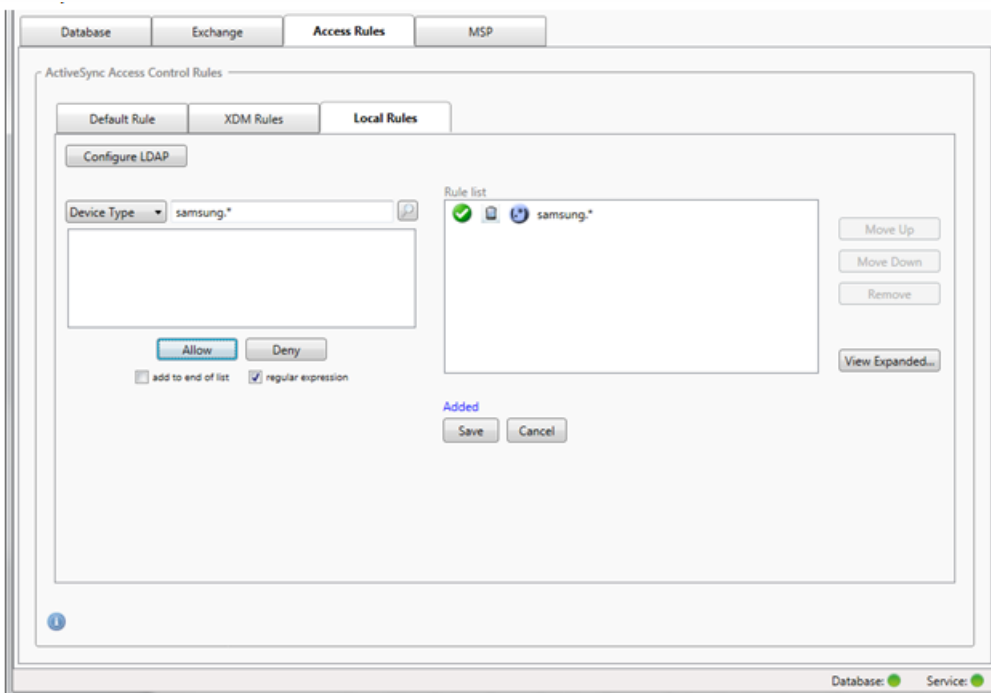
5. To allow all device types that have "Samsung" in their device type value, add a regular expression rule by following these steps:
 1. Click within the selected item text box.
 2. Change the text from SAMSUNGSPHL720 to SAMSUNG.*
 3. Make sure that the regular expression check box is selected.
 4. Click Allow.



1. Click the Local Rules tab.
2. To enter the regular expression, you need to make use of both the Device ID list and the selected item text box.

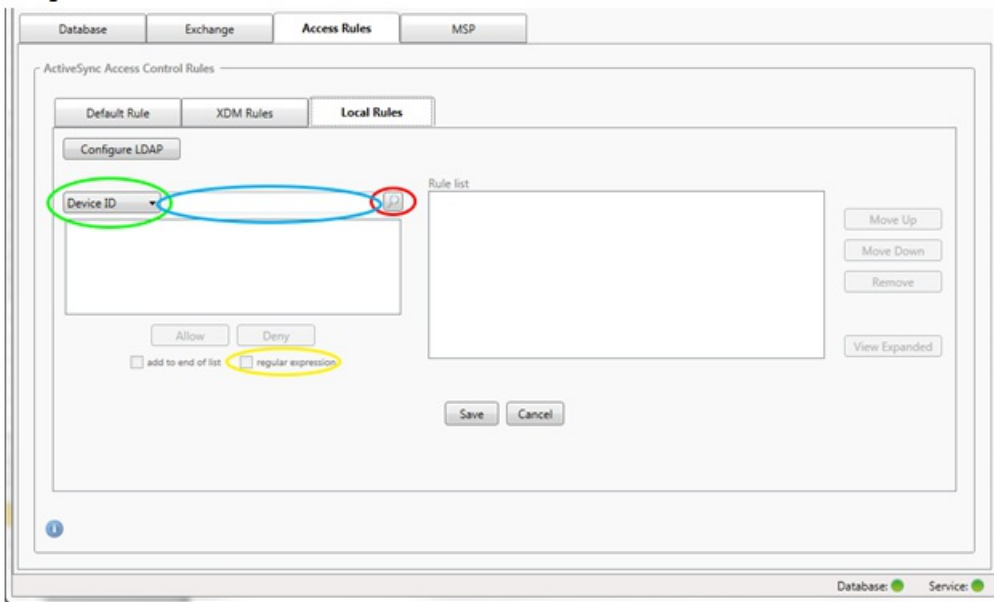


3. Select the field you want to match against. This example uses Device Type.
4. Type in the regular expression. This example uses `samsung.*`
5. Ensure that the regular expression check box is selected and then click Allow or Deny. In this example, the choice is Allow so that the final result is as follows:

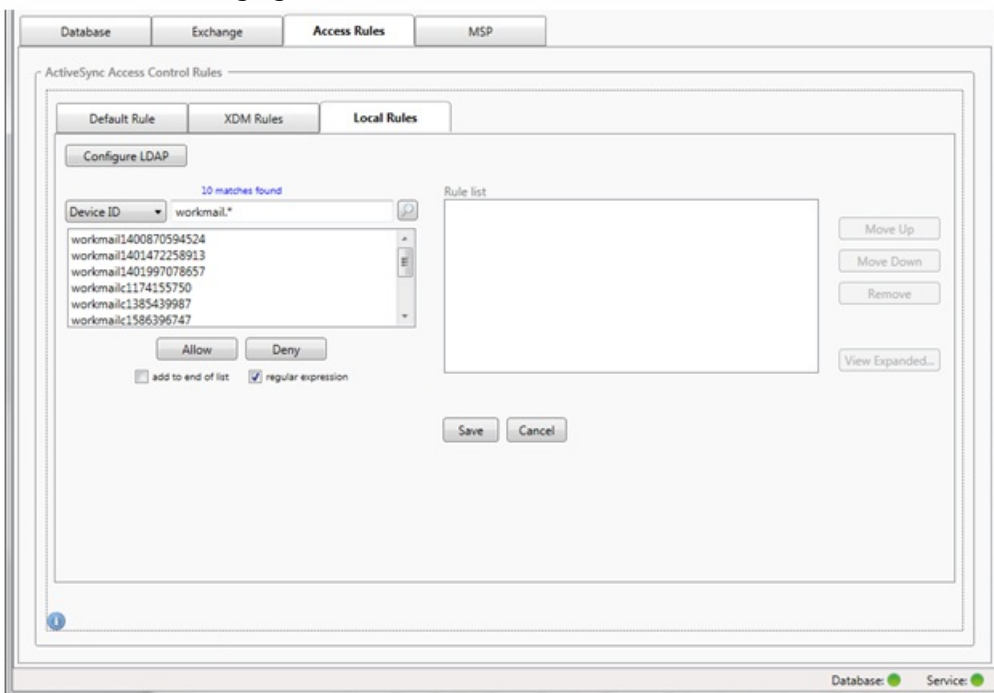


By selecting the regular expression check box, you can run searches for specific devices that match the given expression. This feature is only available if a major snapshot has successfully completed. You can use this feature even if there is no plan to use regular expression rules. For example, assume that you want to find all devices that have the text "workmail" in their ActiveSync device ID. To do so, follow this procedure.

1. Click the Access Rules tab.
2. Ensure that the device match field selector is set to Device ID (the default).



3. Click within the selected item text box (as shown in blue in the preceding figure) and then type workmail.*.
4. Make sure the regular expression check box is selected and then click the magnifying glass icon to display matches as shown in the following figure.



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.

XenMobile Mail Manager Console 10.0.0.86

Refresh

Configure **Monitor**

ActiveSync Devices BlackBerry Devices Automation History

Selection

All Devices Anytime User: Device: Go Export...

Reported State	Requested State	User	Device ID	Type	Model
✓	?	user1@citrix.lab	711138644465147739D4AACFC31A3415F	iPad	iPad
✓	?	user1 Add user1@citrix.lab , to StaticAllow	1003061	SAMSUNGSAMSUNGSMG900A	SAMSUNG-SM-G900A
✓	?	user2 Add user1@citrix.lab , to StaticDeny	1003061	SAMSUNGSAMSUNGSMG900A	SAMSUNG-SM-G900A
✓	?	user2@citrix.lab,	883A681FEB514D1098A3C81712ACB876	iPhone	iPhone

4 records read, 4 records displayed

Database: Service:

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

Mar 06, 2015

XenMobile Mail Manager logs errors and other operational information to its log file: <Install Folder>\log\XmmWindowsService.log. XenMobile Mail Manager also logs significant events to the Windows Event Log.

The following list includes common errors:

XenMobile Mail Manager service doesn't start

Check the log file and the Windows Event Log for errors. Typical causes are as follows:

- The XenMobile Mail Manager service cannot access the SQL Server. This may be caused by these issues:

- The SQL Server service is not running.
- Authentication failure.

If Windows Integrated authentication is configured, the user account of the XenMobile Mail Manager service must be an allowed SQL logon. The account of the XenMobile Mail Manager service defaults to Local System, but may be changed to any account that has local 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.

XenMobile NetScaler Connector

Aug 12, 2016

XenMobile NetScaler Connector is a solution that controls access to corporate email, calendar, and contacts from mobile devices. XenMobile NetScaler Connector allows customers to send a list of compliant devices from XenMobile to NetScaler, which in turn controls which mobile devices are allowed to sync with the corporate Exchange Server.

XenMobile provides complete protection for mobile apps, network, and data, and ensures end-to-end security and compliance. NetScaler optimizes, secures, and controls the delivery of all enterprise and cloud services. Together, the two Citrix products provide the ability to scale, ensure high availability for apps, and maintain security while reducing mobility deployment and management costs.

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.

XenMobile provides whitelisting (approved) and blacklisting (forbidden) policies for devices based on compliance with high-level policies, such as detection of jailbroken devices or detection of specific apps. XenMobile NetScaler Connector local rules are typically used to augment the XenMobile rules in cases where specific overrides are required; for example, to block all devices using a specific operating system version.

The key features of XenMobile NetScaler Connector are:

- **Access control of HTTP ActiveSync requests.** XenMobile NetScaler Connector can control the HTTP ActiveSync requests that mobile devices make of Exchange Servers. You can build filters in XenMobile NetScaler Connector that enable you to allow or block user devices, based on rules and criteria that you specify. When you set the rules in XenMobile NetScaler Connector, you can turn on and off the rules in XenMobile, which then manages the ability for devices to access email within the organization.
- **Remote configuration.** XenMobile controls the baseline and delta intervals used by XenMobile NetScaler Connector.
- **Logging.** On the **Log** tab of the XenMobile NetScaler Connector configuration utility, you can view when the encryption is enabled for a given user device at the request level, in addition to devices that are allowed or blocked.

XenMobile NetScaler Connector provides the following capabilities:

- **Filter-based rules to allow or block access.** XenMobile NetScaler Connector evaluates a particular client request routed through NetScaler against the organization's rules. The end result is a binary state of *allowed*, in which the client is permitted to contact the Microsoft Exchange 2010 Client Access Server (CAS), or *blocked*, in which the client request is dropped and access to the Exchange CAS is not permitted. Paired with settings in the XenMobile console, you can prevent Exchange ActiveSync email access to device users based on compliance criteria, such as when a blacklisted app is installed on the device, if the device is jailbroken, and so on.
- **A two-tiered filter model.** The first tier parses the incoming HTTP requests based on path-specific information. The second tier filters based on user- or device-specific information. You can configure both tiers.
- **Filter rules stored in configuration files.** Specific filter rules pertaining to the user accounts and devices in your organization are stored in the gateway's XML configuration files.

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

Deploying XenMobile NetScaler Connector

May 06, 2015

XenMobile NetScaler Connector enables you to use NetScaler to proxy and load balance XenMobile server communication with XenMobile managed devices. XenMobile NetScaler Connector communicates periodically with XenMobile to synchronize policies. XenMobile NetScaler Connector and XenMobile can be clustered, together or independently, and can be load balanced by NetScaler.

XenMobile NetScaler Connector consists of the following four components:

- XenMobile NetScaler Connector service. This provides a REST web service interface that can be invoked by NetScaler to determine if an ActiveSync request from a device is authorized.
- XenMobile configuration service. This service communicates with Device Manager to synchronize Device Manager policy changes with XenMobile NetScaler Connector.
- XenMobile notification service. This service sends notifications of unauthorized device access to Device Manager so that Device Manager can take appropriate measures, such as notifying the user why the device was blocked.
- XenMobile NetScaler configuration utility. This application allows the administrator to configure and monitor XenMobile NetScaler Connector.

In order for XenMobile NetScaler Connector to be able to receive requests from NetScaler to authorize ActiveSync traffic, you need to specify the port on which XenMobile NetScaler Connector listens to NetScaler web service calls.

1. From the Start menu, select the XenMobile NetScaler configuration utility.
2. Click the Web Service tab and then type the listening addresses for the XenMobile NetScaler Connector web service. You can select HTTP and/or HTTPS. If XenMobile NetScaler Connector is co-resident with XenMobile (installed on the same server), select port values that do not conflict with XenMobile.
3. After the values are configured, click Save and then click Start Service to start the web service.

To configure the access control policy you want to apply to your managed devices, do the following:

1. In the XenMobile NetScaler configuration utility, click the Path Filters tab.
2. Select the first row, Microsoft-Server-ActiveSync is for ActiveSync and then click Edit.
3. From the Policy list, select the desired policy. For a policy that is inclusive of XenMobile policies, select Static + ZDM: Permit Mode or Static + ZDM: Block Mode. These policies combine local (or, static) rules with the rules from XenMobile. Permit Mode means that all devices not explicitly identified by the rules will be permitted access to ActiveSync. Block Mode means that such devices will be blocked.
4. After setting the policies, click Save.

In this task, you will specify the name and properties of the XenMobile server (also known as a Config Provider) that you want to use with XenMobile NetScaler Connector and NetScaler.

Note: This task assumes that you have already installed and configured XenMobile.

1. In the XenMobile NetScaler Connector configuration utility, click the Config Providers tab and then click Add.
2. Enter the name and URL of the XenMobile server you are using in this deployment. If you have multiple XenMobile servers deployed in a Multi-Tenant deployment, this name must be unique for each server instance. For example, for Name, you could type XMS.
3. In Url, enter the Web address of the XenMobile GlobalConfig Provider (GCP), typically in the format `https://DeviceManagerHost/zdm/services/MagConfigService`. The MagConfigService name is case-sensitive.
4. In Password, enter the password that will be used for basic HTTP authorization with the XenMobile web server.
5. In Managing Host, enter the server name where you installed XenMobile NetScaler Connector.
6. In Baseline Interval, specify a time period for when a new refreshed dynamic ruleset is pulled from XenMobile.
7. In Request Timeout, specify the server request timeout interval.
8. In Config Provider, select if the config provider server instance is providing the policy configuration.
9. In Events Enabled, enable this option if you want Secure Mobile Gateway to notify XenMobile when a device is blocked. This option is required if you are using Secure Mobile Gateway rules in any of your Device Manager Automated Actions.
10. Once the server is configured, click Test Connectivity to test the connection to the XenMobile server.
11. When connectivity has been established, click Save.

If you want to scale your XenMobile NetScaler Connector and XenMobile deployment, you can install instances of XenMobile NetScaler Connector on multiple Windows Servers, all pointing to the same XenMobile instance, and then you can use NetScaler to load balance the servers.

There are two modes for the XenMobile NetScaler Connector configuration:

- In non-shared mode, each XenMobile NetScaler Connector instance communicates with a XenMobile server and keeps its own private copy of the resulting policy. For example, if you had a cluster of XenMobile servers, you could run a XenMobile NetScaler Connector instance on each XenMobile server and XenMobile NetScaler Connector would get policies from the local XenMobile instance.
- In shared mode, one XenMobile NetScaler Connector node is designated the primary node and it communicates with XenMobile. The resulting configuration is shared among the other nodes either by a Windows network share or by Windows (or third-party) replication.

The entire XenMobile NetScaler Connector configuration is in a single folder (consisting of a few XML files). The XenMobile NetScaler Connector process detects changes to any file in this folder and automatically reloads the configuration. There is no failover for the primary node in shared mode. But the system can tolerate the primary server being down for a few minutes (for example, to restart) because the last known good configuration is cached in the XenMobile NetScaler Connector process.

XenMobile NetScaler Connector System Requirements

Feb 24, 2017

XenMobile NetScaler Connector communicates with NetScaler over an SSL bridge configured on the NetScaler appliance that enables the appliance to bridge all secure traffic directly to XenMobile. XenMobile NetScaler Connector requires the following minimum system configuration:

Component	Requirement
Computer and processor	733 MHz Pentium III 733 MHz or higher processor. 2.0 GHz Pentium III or higher processor (recommended)
NetScaler	NetScaler appliance with software version 10
Memory	1 GB
Hard disk	NTFS-formatted local partition with 150 MB of available hard-disk space
Operating system	Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 SP2, Microsoft Windows Server 2012 R2
Other devices	Network adapter compatible with the host operating system for communication with the internal network
Display	VGA or higher-resolution monitor

The host computer for XenMobile NetScaler Connector requires the following minimum available hard disk space:

- Application. 10 -15 MB (100 MB recommended)
- Logging. 1 GB (20 GB recommended)

For information about platform support for XenMobile NetScaler Connector, see [Supported Device Platforms in XenMobile](#).

Device email clients

Not all email clients consistently return the same ActiveSync ID for a device. Because XenMobile NetScaler Connector 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

Installing XenMobile NetScaler Connector

May 02, 2014

You can install XenMobile NetScaler Connector on its own server or on the same server where you installed XenMobile.

You can consider installing XenMobile NetScaler Connector on its own server (separate from XenMobile) for the following reasons:

- If your XenMobile server is hosted remotely in the cloud (physical location).
- If you do not want XenMobile NetScaler Connector to be affected by restarts of the XenMobile server (availability).
- If you want a server's system resources to be devoted entirely to XenMobile NetScaler Connector (performance).

The CPU load that XenMobile NetScaler Connector puts on a server depends on how many devices are managed, but a general rule of thumb is to provision for one additional CPU core if XenMobile NetScaler Connector is deployed on the same server as XenMobile. For large numbers of devices (more than 50,000), you may need to provision additional cores if you do not have a clustered environment. The memory footprint of XenMobile NetScaler Connector is not significant enough to warrant additional memory.

To install, upgrade, or uninstall XenMobile NetScaler Connector

May 02, 2014

1. Run XncInstaller.exe with an administrator account to install XenMobile NetScaler Connector (XNC) or allow for upgrade or removal of an existing XenMobile NetScaler Connector.
2. Follow the onscreen instructions to complete the installation, upgrade, or uninstallation.

After you install XenMobile NetScaler Connector, you must manually restart the XenMobile configuration service and the notification service.

To uninstall the XNC

Feb 22, 2014

1. Run XncInstaller.exe with an administrator account.
2. Follow the onscreen instructions to complete the uninstallation.

Managing XenMobile NetScaler Connector

May 02, 2014

You can use XenMobile NetScaler Connector to build access control rules to either allow or block access to ActiveSync connection requests from managed devices, based on device status, app blacklists or whitelists, and other compliance conditions.

By using the XenMobile NetScaler Connector configuration utility, you can build dynamic and static rules that enforce corporate email policies, allowing you to block users who are in violation of compliance standards. You can also set up email attachment encryption, so that all attachments that pass through your Exchange Server to managed devices are encrypted and only viewable on managed devices by authorized users.

Choosing a Security Model for XenMobile NetScaler Connector

Apr 19, 2016

Establishing a security model is essential to a successful mobile device deployment for organizations of any size. Although it is not uncommon to use protected or quarantined network control to allow access to a user, computer, or device by default, it is not always a good practice. Every organization that manages IT security may have a slightly different or tailored approach to security for mobile devices.

The same logic applies to mobile device security. The vast numbers of mobile devices and types, quantities of mobile devices per user, and the array of operating system platforms and apps available make the very idea of using a permissive model a weak choice. In most organizations, the restrictive model will be the most logical choice.

The configuration scenarios that Citrix allows for integrating XenMobile NetScaler Connector with XenMobile are as follows:

The permissive security model operates on the premise that everything is either allowed or granted access by default. Only in the case of rules and filtering will something be blocked and a restriction applied. The permissive security model is good for organizations that have a relatively loose security concern about mobile devices and only applies restrictive controls to deny access where appropriate (when a policy rule is failed).

The restrictive security model is based on the premise that nothing is allowed or granted access by default. Everything passing through the security check point is filtered and inspected, and is denied access unless the rules allowing access are passed. The restrictive security model is good for organizations that have a relatively tight security criterion about mobile devices. The mode only grants access for use and functionality with the network services when all rules to allow access have passed.

Configuring XenMobile NetScaler Connector

May 02, 2014

You can configure XenMobile NetScaler Connector to selectively block or allow ActiveSync requests based on the following properties: Active Sync Service ID, Device type, User Agent (device operating system), Authorized user, and ActiveSync Command.

The default configuration supports a combination of static and dynamic groups. You maintain static groups by using the SMG Controller Configuration utility. The static groups may consist of known categories of devices, such as all devices using a given user agent.

Dynamic groups are maintained by an external source called a Gateway Configuration Provider and collected by XenMobile NetScaler Connector on a periodic basis. XenMobile can export groups of allowed and blocked devices and users to XenMobile NetScaler Connector.

A policy is an ordered list of groups in which each group has an associated action (allow or block) and a list of group members. A policy may have any number of groups. Group ordering within a policy is important because when a match is found the action of the group is taken, and subsequent groups are not evaluated.

A member defines a way to match the properties of a request. It can match a single property, such as device ID, or multiple properties, such as device type and user agent.

Configuring XenMobile NetScaler Connector Policy Modes

Jan 13, 2015

XenMobile NetScaler Connector can run in the following six modes:

- Allow All. This policy mode grants access for all traffic passing through XenMobile NetScaler Connector. No other filtering rules are used.
- Deny All. This policy mode blocks access for all traffic passing through XenMobile NetScaler Connector. No other filtering rules are used.
- Static Rules: Block Mode. This policy mode executes static rules with an implicit deny or block statement at the end. Devices that are not allowed or permitted via other filter rules are blocked by XenMobile NetScaler Connector.
- Static Rules: Permit Mode. This policy mode executes static rules with an implicit permit or allow statement at the end. Devices that are not blocked or denied via other filter rules are allowed through XenMobile NetScaler Connector.
- Static + ZDM Rules: Block Mode. This policy mode executes static rules first, followed by dynamic rules from XenMobile with an implicit deny or block statement at the end. Devices are permitted or denied based on defined filters and Device Manager rules. Any devices that do not match on defined filters and rules are blocked.
- Static + ZDM Rules: Permit Mode. This policy mode executes static rules first, followed by dynamic rules from XenMobile with an implicit permit or allow statement at the end. Devices are permitted or denied based on defined filters and XenMobile rules. Any devices that do not match on defined filters and rules are allowed.

The XenMobile NetScaler Connector process permits or blocks for dynamic rules based on unique ActiveSync IDs for iOS and Windows-based mobile devices received from XenMobile. Android devices differ in their behavior based on the manufacturer and some do not readily expose a unique ActiveSync ID. To compensate, XenMobile sends user ID information for Android devices to make a permit or block decision. As a result, if a user has only one Android device, permits and blocks function normally. If the user has multiple Android devices, all the devices are allowed because Android devices cannot be definitively differentiated. The gateway can still be configured to statically block these devices by ActiveSyncID, if they are known, and can also be configured to block based on device type or user agent.

To specify the policy mode, in the SMG Controller Configuration utility, do the following:

1. Click the Path Filters tab and then click Add.
2. In the Path Properties dialog box, select a policy mode from the Policy drop-down list and then click Save.

You can review rules on the Policies tab of the configuration utility. The rules are processed on XenMobile NetScaler Connector from top to bottom. The Allow policies are displayed with green checkmark. The Deny policies are shown as a red circle with a line through it. To refresh the screen and see the most updated rules, click Refresh. You can also modify the ordering of rules in the config.xml file.

To test rules, click the Simulator tab. Specify values in the fields. These can also be obtained from the logs. A result message will appear specifying Allow or Block.

To configure static rules

May 02, 2014

You must enter static rules with values that are read by the ISAPI filtering of the ActiveSync connection HTTP request. Static rules enable XenMobile NetScaler Connector to permit or block traffic by the following criteria:

- **User.** XenMobile NetScaler Connector uses the authorized user value and name structure that was captured during device enrollment. This is commonly found as domain\username as referenced by the server running XenMobile connected to Active Directory via LDAP. The Log tab within the XenMobile NetScaler Connector configuration utility will show the values that are passed through XenMobile NetScaler Connector if the value structure needs to be determined or is different.
- **Deviceid (ActiveSyncID).** Also known as the ActiveSyncID of the connected device. This value is commonly found within the specific device properties page in the XenMobile console. This value can also be screened from the Log tab in the XenMobile NetScaler Connector configuration utility.
- **DeviceType.** XenMobile NetScaler Connector can determine if a device is an iPhone, iPad, or other device type and can permit or block based on that criteria. As with other values, the XenMobile NetScaler Connector configuration utility can reveal all connected device types being processed for the ActiveSync connection.
- **UserAgent.** Contains information on the ActiveSync client that is used. In most cases, the value specified corresponds to a specific operating system build and version for the mobile device platform.

The XenMobile NetScaler Connector configuration utility running on the server always manages the static rules.

1. In the SMG Controller Configuration utility, click the Static Rules tab and then click Add.
2. In the Static Rule Properties dialog box, specify the values that you want to use as criteria. For example, you can enter a user to allow access by entering the user name (for example, AllowedUser) and then clearing the Disabled check box.
3. Click Save. The static rule is now in effect. Additionally, you can use regular expressions to define values, but you must enable the rule processing mode in the config.xml file.

To configure dynamic rules

May 02, 2014

Dynamic rules are defined by device policies and properties in Device Manager and can trigger a dynamic XenMobile NetScaler Connector or filter based on the presence of a policy violation or property setting. The XenMobile NetScaler Connector filters work by analyzing a device for a given policy violation or property setting. If the device meets the criteria, the device is placed in a Device List. This Device List is neither an allow list or a block list. It is a list of devices that meets the criteria defined. The following configuration options enable you to define whether you want to allow or deny the devices in the Device List by using XenMobile NetScaler Connector.

Note: These dynamic rules must be configured in the XenMobile console.

1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Server**, click **ActiveSync Gateway**. The ActiveSync Gateway page appears.
3. In **Activate the following rules**, select one or more rules you want to activate.
4. In Android-only, in **Send Android domain users to ActiveSync Gateway**, click **YES** to ensure that XenMobile sends Android device information to the Secure Mobile Gateway. When this option is enabled, it ensures that XenMobile sends Android device information to the XenMobile NetScaler Connector in the event that XenMobile does not have the ActiveSync identifier for the Android device user.

To configure custom policies by editing the XenMobile NetScaler Connector XML file

May 02, 2014

You can view the basic policies in the default configuration on the Policies tab of the XenMobile NetScaler Connector configuration utility. If you want to create custom policies, you can edit the XenMobile NetScaler Connector XML configuration file (config\config.xml).

1. Find the PolicyList section in the file and then add a new Policy element.
2. If a new group is also required, such as an additional static group or a group to support an additional GCP, add the new Group element to the GroupList section.
3. Optionally, you can change the ordering of groups within an existing policy by rearranging the GroupRef elements.

Configuring the XenMobile NetScaler Connector XML File

May 02, 2014

The XenMobile NetScaler Connector uses an XML configuration file to dictate the actions of XenMobile NetScaler Connector. Among other entries, the file specifies the group files and associated actions the filter will take when evaluating HTTP requests. By default, the file is named config.xml and can be found at the following location: ..\Program Files\Citrix\XenMobile NetScaler Connector\config\.

The GroupRef nodes define the logical group names - by default, the AllowGroup and the DenyGroup.

Note: The order of the GroupRef nodes as they appear in the GroupRefList node is significant.

The ID value of a GroupRef node identifies a logical container or collection of members that are used for matching specific user accounts or devices. The action attributes specifies how the filter will treat a member that matches a rule in the collection. For example, a user account or device that matches a rule in the AllowGroup set will "pass" (be allowed to access the Exchange CAS), while a user account or device that matches a rule in the DenyGroup set will be "rejected" (not allowed to access the Exchange CAS).

When a particular user account/device or combination meets rules in both groups, a precedence convention is used to direct the request's outcome. Precedence is embodied in the order of the GroupRef nodes in the config.xml file from top to bottom. The GroupRef nodes are ranked in priority order. Rules for a given condition in the Allow group will always take precedence over rules for the same condition in the Deny group.

Additionally, the config.xml defines Group nodes. These nodes link the logical containers AllowGroup and DenyGroup to external XML files. Entries stored in the external files form the basis of the filter rules.

Note: In this release, only external XML files are supported.

The default installation implements two XML file in the configuration - allow.xml and deny.xml.

To import a policy from XenMobile

May 02, 2014

1. In the XenMobile NetScaler Configuration configuration utility, click the Config Providers tab and then click Add.
2. In the Config Providers dialog box, in Name, enter a user name that will be used for basic HTTP authorization with the XenMobile server and that has administrative privileges.
3. In Url, enter the web address of the XenMobile Gateway Configuration Service (GCS), typically in the format `https://xdmHost/xdm/services/MagConfigService`. The MagConfigService name is case-sensitive.
4. In Password, enter the password that will be used for basic HTTP authorization with the XenMobile server.
5. Click Test Connectivity to test gateway-to-configuration provider connectivity. If the connection fails, check that your local firewall settings allow the connection or check with your administrator.
6. When a connection is successfully made, clear the Disabled check box and then click Save.
7. In Managing Host, leave the default DNS name of the local host computer. This setting used to coordinate communication with XenMobile when multiple Forefront Threat Management Gateway (TMG) servers are configured in an array.

After you save the settings, open the GCS.

To configure a connection to XenMobile NetScaler Connector

May 02, 2014

XenMobile NetScaler Connector communicates with XenMobile and other remote configuration providers through secure web services.

1. In the XenMobile NetScaler Connector configuration utility, click the Config Providers tab and then click Add.
2. In the Config Providers dialog box, in Name, enter a user name that has administrative privileges and will be used for basic HTTP authorization with the XenMobile server.
3. In Url, enter the web address of the XenMobile GCS, typically in the format `https://ZdmHost/zdm/services/MagConfigService`. The `MagConfigService` name is case-sensitive.
4. In Password, enter the password that will be used for basic HTTP authorization with the XenMobile server.
5. In Managing Host, enter the XenMobile NetScaler Connector server name.
6. In Baseline Interval, specify a time period for when a new refreshed dynamic ruleset is pulled from Device Manager.
7. In Delta interval, specify a time period for when an update of dynamic rules is pulled.
8. In Request Timeout, specify the server request timeout interval.
9. In Config Provider, select if the configuration provider server instance is providing the policy configuration.
10. In Events Enabled, enable this option if you want XenMobile NetScaler Connector to notify XenMobile when a device is blocked. This option is required if you are using the XenMobile NetScaler Connector rules in any of your XenMobile Automated Actions.
11. Click Save and then click Test Connectivity to test gateway-to-configuration provider connectivity. If the connection fails, check that the local firewall settings allow the connection or contact your administrator.
12. When the connection succeeds, clear the Disabled check box and then click Save.

When you add a new configuration provider, XenMobile NetScaler Connector automatically creates one or more policies associated with the provider. These policies are defined by a template definition contained in `config\policyTemplates.xml` in the `NewPolicyTemplate` section. For each `Policy` element defined within this section, a new policy is created. The operator may add, remove, or modify policy elements provided that the policy element conforms to the schema definition, and that the standard substitution strings (enclosed in braces) are not modified. Next, add new groups for the provider and update the policy to include the new groups.

Choosing Filters for XenMobile NetScaler Connector

May 02, 2014

The XenMobile NetScaler Connector filters work by analyzing a device for a given policy violation or property setting. If the device meets the criteria, the device is placed in a Device List. This Device List is neither an allow list or a block list. It is a list of devices that meet the criteria defined. The following filters are available for XenMobile NetScaler Connector within XenMobile.

- **Blacklisted Apps.** Allows or denies devices based on the Device List defined by blacklist policies and the presence of blacklisted apps.
- **Whitelisted Apps only.** Allows or denies devices based on the Device List defined by whitelist policies and the presence of non-whitelisted apps.
- **Unmanaged Devices.** Creates a Device List of all devices in the XenMobile database. The Mobile Application Gateway needs to be deployed in a Block Mode.
- **Rooted Android /Jailbroken iOS Devices.** Creates a Device List of all devices flagged as rooted and allows or denies based on rooted status.
- **Out of Compliance Devices.** Allows you to deny or allow devices that meet your own internal IT compliance criteria. Compliance is an arbitrary setting defined by the device property named Out of Compliance, which is a Boolean flag that can be either True or False. (You can create this property manually and set the value, or you can use Automated Actions to create this property on a device if the device does or does not meet specific criteria.)
 - **Out of Compliance = True.** If a device does not meet the compliance standards and policy definitions set by your IT department, the device is out of compliance.
 - **Out of Compliance = False.** If a device does meet the compliance standards and policy definitions set by your IT department, the device is compliant.
- **Noncompliant password.** Creates a Device List of all devices that do not have a passcode on the device.
- **Revoked Status.** Creates a Device List of all revoked devices and allows or denies based on revoked status.
- **Inactive devices.** Creates a Device List of devices that have not communicated with XenMobile within a specified period of time and are thus considered inactive and allows or denies the devices accordingly.
- **Anonymous Devices.** Allows or denies devices that are enrolled in XenMobile but the user's identity is unknown. For example, this could be a user who was enrolled, but the user's Active Directory password is expired, or a user who enrolled with unknown credentials.
- **Implicit Allow/Deny.** Creates a Device List of all devices that do not meet any of the other filter rule criteria and allows or denies based on that list. The Implicit Allow/Deny option ensures that the XenMobile NetScaler Connector status in the Devices tab is enabled and shows the XenMobile NetScaler Connector status for your devices. The Implicit Allow/Deny option also controls all of the other XenMobile NetScaler Connector filters that have not been selected. For example, Blacklists Apps will be denied (blocked) by XenMobile NetScaler Connector, whereas all other filters will be allowed because the Implicit Allow/Deny option is selected to Allow.

To simulate ActiveSync traffic with XenMobile NetScaler Connector

May 02, 2014

You can use the XenMobile NetScaler Connector to simulate what ActiveSync traffic will look like in conjunction with your policies. In the XenMobile NetScaler Connector configuration utility, select the Simulations tab. The results show you how your policies will apply according to the rules you have configured.

Monitoring XenMobile NetScaler Connector

May 02, 2014

The XenMobile NetScaler Connector configuration utility provides detailed logging that you can use to view all traffic passing through your Exchange Server that is either allowed or blocked by Secure Mobile Gateway.

Use the Log tab to view the history of the ActiveSync requests forwarded to XenMobile NetScaler Connector by NetScaler for authorization.

Also, to make sure the XenMobile NetScaler Connector web service is running, you can load the following URL into a browser on the XenMobile NetScaler Connector server `http://<host:port>/services/ActiveSync/Version`. If the URL returns the product version as a string, the web service is responsive.