About XenMobile Server 10.1

Aug 12, 2016

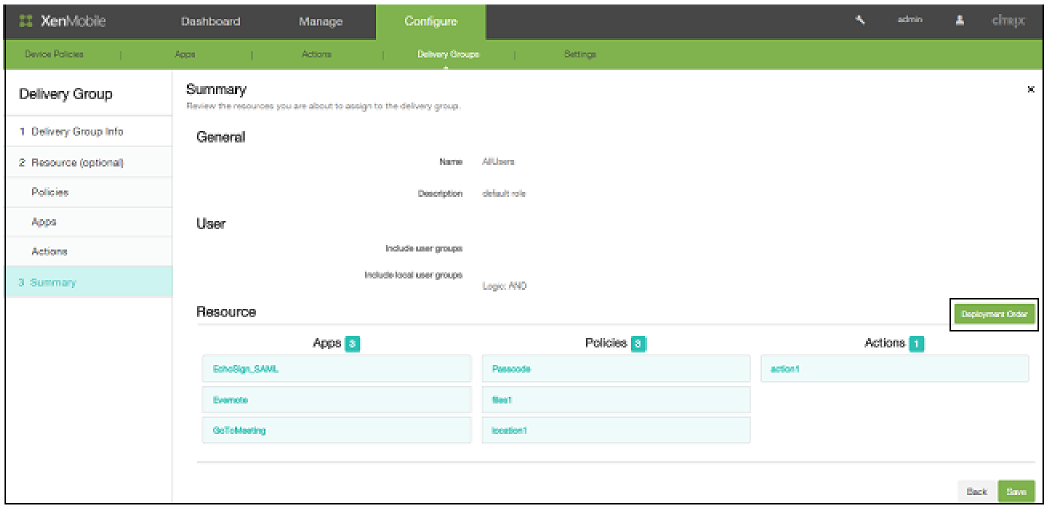
> ## Note
>
> Citrix supports the current version of XenMobile Server and the prior two versions. We keep the product documentation for versions earlier than those versions as PDFs in the Archive List of Legacy Documents.
>
> For product documentation on the current release, see XenMobile Server.

You can upgrade XenMobile 10 to XenMobile 10.1 in the XenMobile console. To perform the upgrade, you use the xms_10.1.0.62986.bin. In the XenMobile console, go to **Settings** > **Release Management**. Click **Upgrade** and then upload the xms_10.1.0.62986.bin file. For more information about upgrades in the console, see Upgrading XenMobile.

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

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

Resource deployment ordering. In XenMobile MDM Edition, you can change the order in which resources are deployed within a delivery group. In the XenMobile console, you change the deployment order in Configure > Delivery Groups. When you add or edit a delivery group, on the Summary page, next to Resources, you click Deployment Order, where you can change the position of the resources that appear in the list to set your preferred order.



Summary

Review the resources you are about to assign to the delivery group.

General

Name AllUsers

Description default role

User

Include user groups

Include local user groups

Logic: AND

Resource

Apps 3	Policies 3	Actions 1
EchoSign_SAML	Passcode	action1
Evernote	files1	
GoToMeeting	location1	

Notes:

- The resources you can order for deployment must be resources that XenMobile fully manages, such as policies and apps.

However, in this release in XenMobile MDM Edition, you cannot yet order actions.

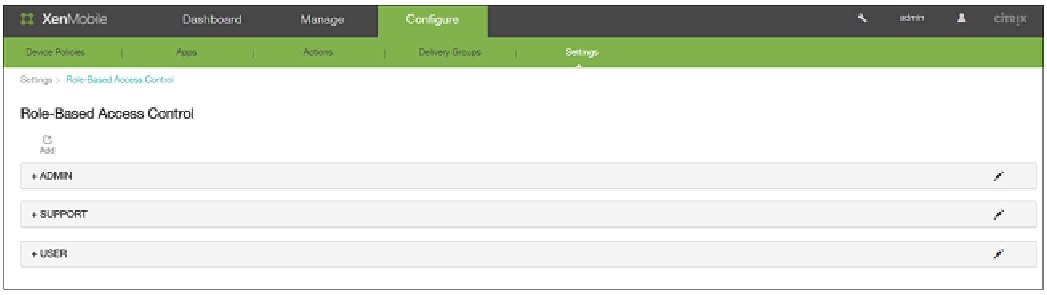
- This feature is not supported for Windows Phone and Windows Tablet. To enforce a deployment schedule for resources on those devices, you must carry out multiple deployments.

Exporting table data. For every table in the XenMobile console - Apps, Policies, Actions, Delivery Groups, Local Users and Groups, Enrollment, and Devices - you can click Export to create a .csv file containing all displayed columns.

REST APIs. XenMobile supports public APIs for REST services to let you call the services that are exposed through XenMobile through any REST client directly. You can do the following with the APIs that are supported in XenMobile 10.1:

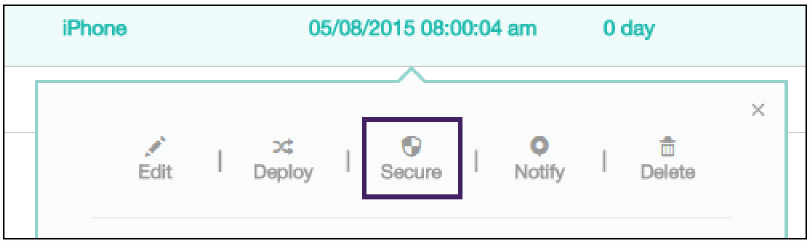
- Configure licenses, NetScaler Gateway, LDAP, certificate management during initial installation.
- Retrieve delivery group details with assigned resources and groups.
- Reset the administrator password.
- Export a PKI certificate.
- Configure notification server settings, such as adding and editing the SMS and SMTP server, deleting the server, and activating the server.
- Retrieve app details and delete apps.
- Set the host fully qualified domain name (FQDN).

RBAC. The DEVICE_PROVISIONING role is removed from XenMobile 10.1, and the Support console feature is added. In XenMobile 10, this feature was available automatically for the ADMIN role; in XenMobile 10.1, the feature is only available when you select Support for the role.

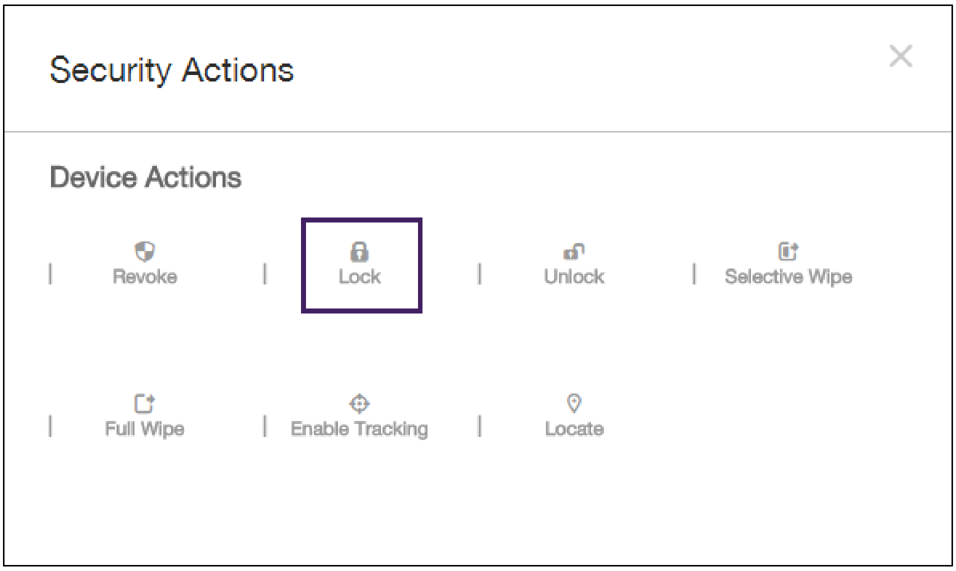


Device lock security action. You can lock a device with an accompanying display of a message and phone number that appears on the device lock screen. You can lock a device in the XenMobile console in Manage > Devices.

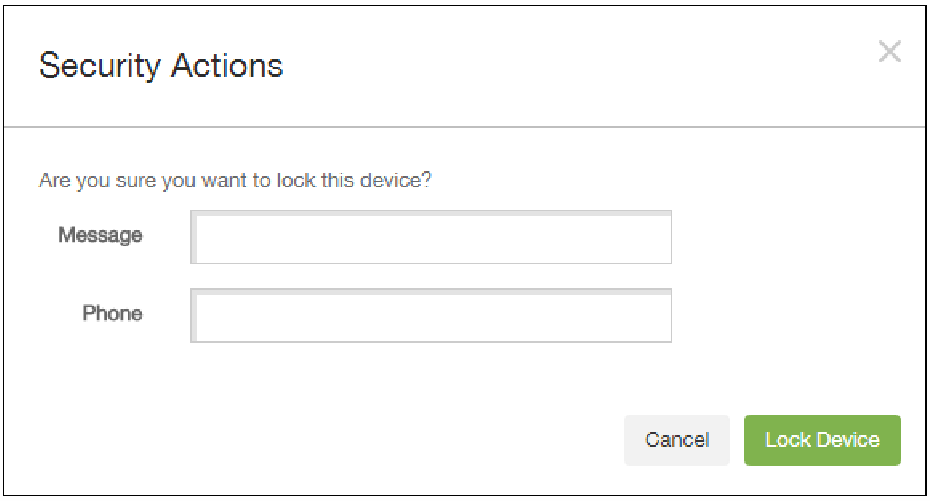
After you select an iOS device in the list, in the dialog box that appears, you click Secure.



In the Security Actions dialog box, you click Lock.



Then, in the confirmation message, you can optionally enter a message and phone number and then click Lock Device. This feature is supported on iOS 7 and 8 devices.

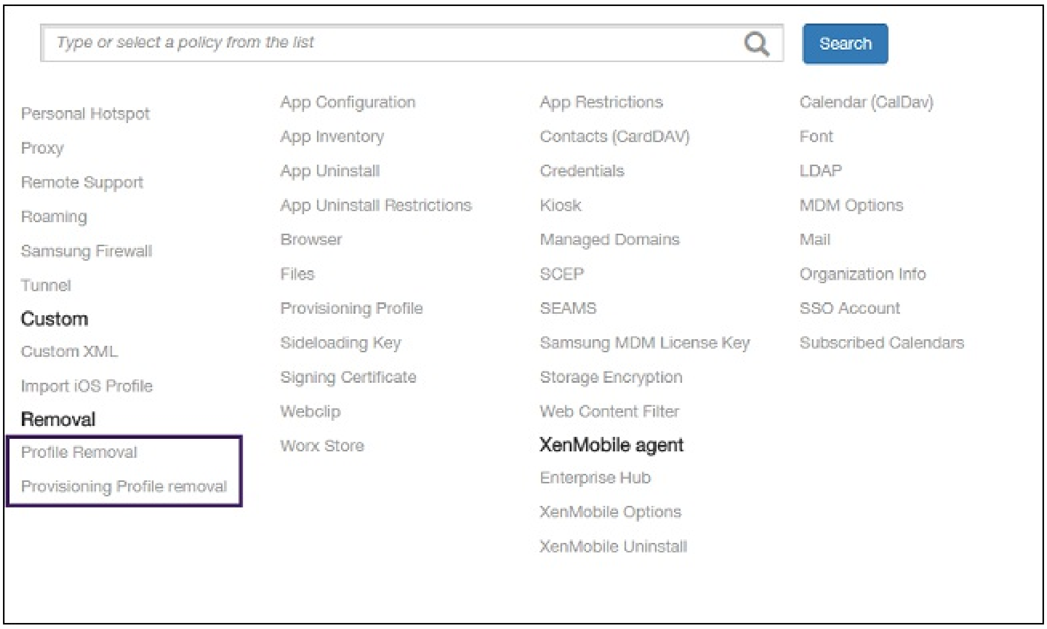


Note: The message and phone only appear on a locked device if you have also set the Passcode policy in the XenMobile console, or if users have enabled the passcode manually on the device.

VPP enhancements. The following features extend the capabilities of the Volume Purchasing Program (VPP) within XenMobile.

- Allows you to import multiple VPP tokens into XenMobile; for example, for tokens purchased in multiple locations, or for multiple organizations, business units, or divisions that require different VPP tokens.
- Partners can create and deploy B2B apps to users with iOS devices from a private business-to-business (B2B) app stores by adding the logon credentials to the VPP configuration in the XenMobile console in Settings.
- Supports the management of multiple VPP/B2B apps for organizations who use XenMobile to manage apps and devices for several VPP customers and multinational companies. Apps from all VPP/B2B accounts are automatically uploaded to XenMobile and are automatically updated. You can assign particular VPP/B2B apps to users in the XenMobile console, where you can also view the VPP/B2B account to which an app applies.

Provisioning profile policies and device details. In XenMobile 10 and earlier, you distribute the profile to user devices by using an email attachment; users add the profile on their iOS device by clicking the attachment. XenMobile 10.1 supports the following provisioning profile policies and device details that make it easier to track the provisioning profile status for enterprise apps on iOS devices, and no longer require users to install the profiles on their devices manually.



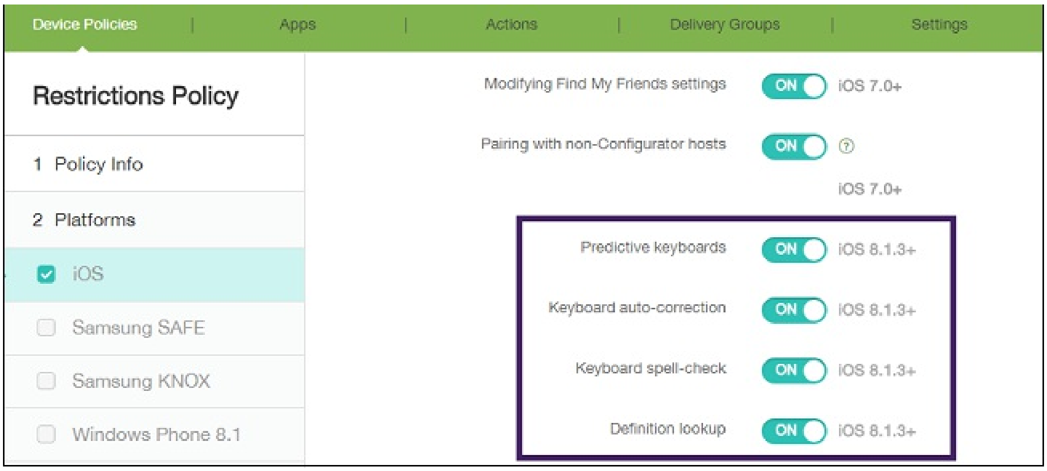
- **iOS Provisioning Profile policy**. Lets you remotely install a provisioning profile on an iOS device. When you configure the policy, you upload an iOS provisioning profile and then deploy the profile to user devices.
- **iOS Provisioning Profile Removal policy**. Lets you remove a provisioning profile from an iOS device. You configure these device policies in the XenMobile console in Configure > Device Policies.
- **iOS provisioning profile lists**. You can view an inventory iOS profiles for the device and a list of provisioning profiles that are installed on the device, listing the universally unique identifier (UUID), expiration date, and managed status for each profile. You view these details in the XenMobile console in Manage > Devices.

Apple Device Enrollment Program (DEP) pre-enrollment. Lets resellers pre-enroll devices in the DEP in order to install managed apps on devices before distributing the devices to users.

Integration with Apple Configurator. Simplifies the large-scale enrollment of corporate-owned devices. Devices can connect to an Apple Configurator and are automatically configured to install a pre-generated XenMobile profile.

New restriction device policies for iOS supervised devices.

- Allows or prevents predictive keyboards, keyboard auto-correction, keyboard spell check, and keyboard definition lookup. Available for iOS 8.1.3 on supervised devices only.



Restrictions Policy

1 Policy Info

2 Platforms

☑ iOS

□ Samsung SAFE

□ Samsung KNOX

□ Windows Phone 8.1

Modifying Find My Friends settings ON iOS 7.0+

Pairing with non-Configurator hosts ON iOS 7.0+

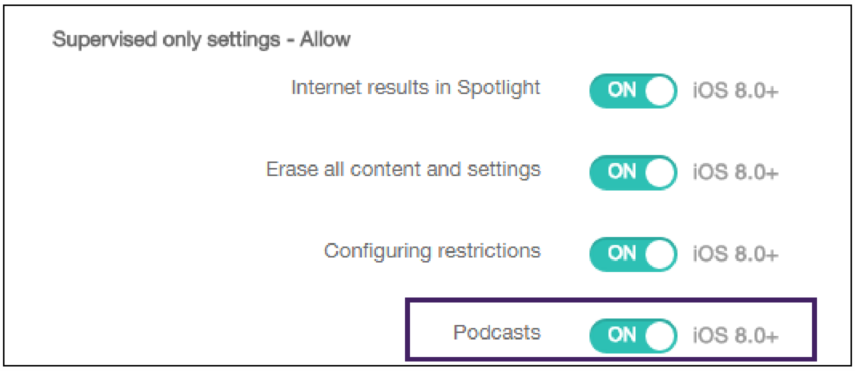
Predictive keyboards ON iOS 8.1.3+

Keyboard auto-correction ON iOS 8.1.3+

Keyboard spell-check ON iOS 8.1.3+

Definition lookup ON iOS 8.1.3+

- Allows or prevents podcasts. Available for iOS 8.0 and later versions on supervised devices only.



Supervised only settings - Allow

Internet results in Spotlight ON iOS 8.0+

Erase all content and settings ON iOS 8.0+

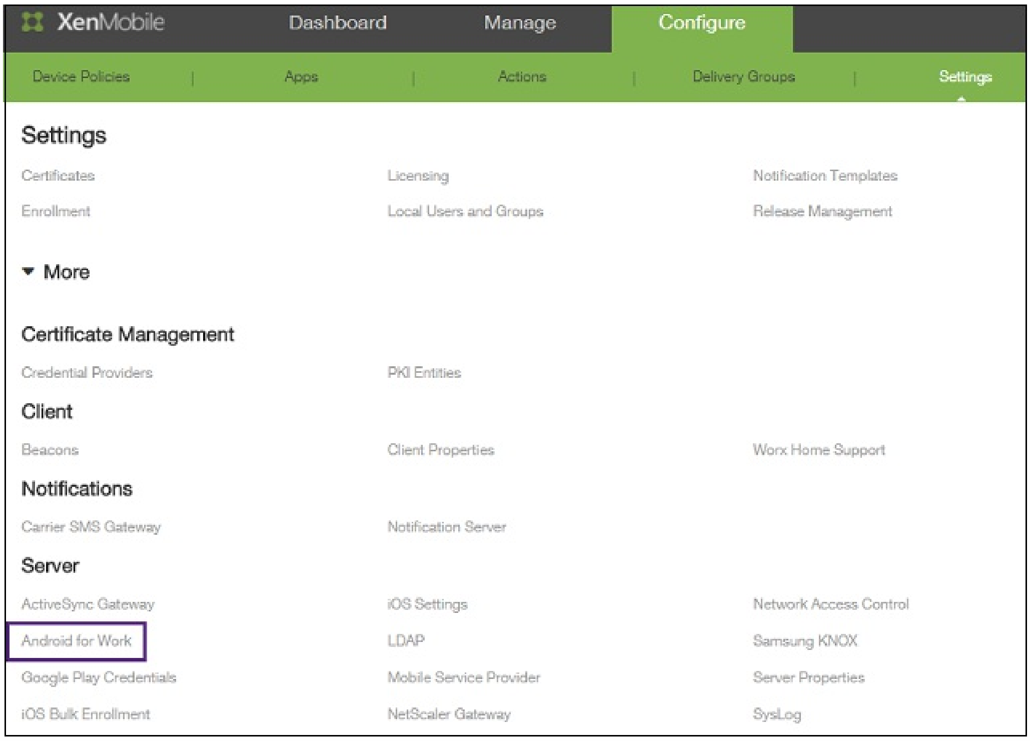
Configuring restrictions ON iOS 8.0+

Podcasts ON iOS 8.0+

Android for Work. A secure workspace on devices that separates corporate apps and data from personal apps and data. Organizations can set up an Android for Work account with Google. You can then deploy approved apps from the Google Play for Work store to user devices. You can also set app restriction policies to control access and functionality. You configure Android for Work settings in the XenMobile console in Settings > Server > Android for Work, and in Device Policies > Security > Android for Work App Restrictions.

Note

Android for Work does not support wrapped apps. Users must install Worx Home on their Android device and then add Android for Work apps to Worx Home.



Settings

Certificates | Licensing | Notification Templates
Enrollment | Local Users and Groups | Release Management

▼ More

Certificate Management

Credential Providers | PKI Entities

Client

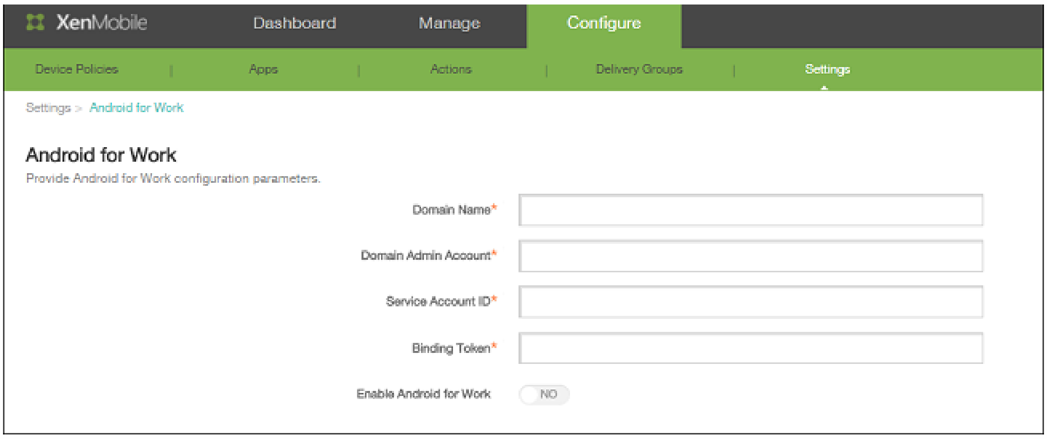
Beacons | Client Properties | Worx Home Support

Notifications

Carrier SMS Gateway | Notification Server

Server

ActiveSync Gateway | iOS Settings | Network Access Control
Android for Work | LDAP | Samsung KNOX
Google Play Credentials | Mobile Service Provider | Server Properties
iOS Bulk Enrollment | NetScaler Gateway | SysLog



Settings > Android for Work

Android for Work

Provide Android for Work configuration parameters.

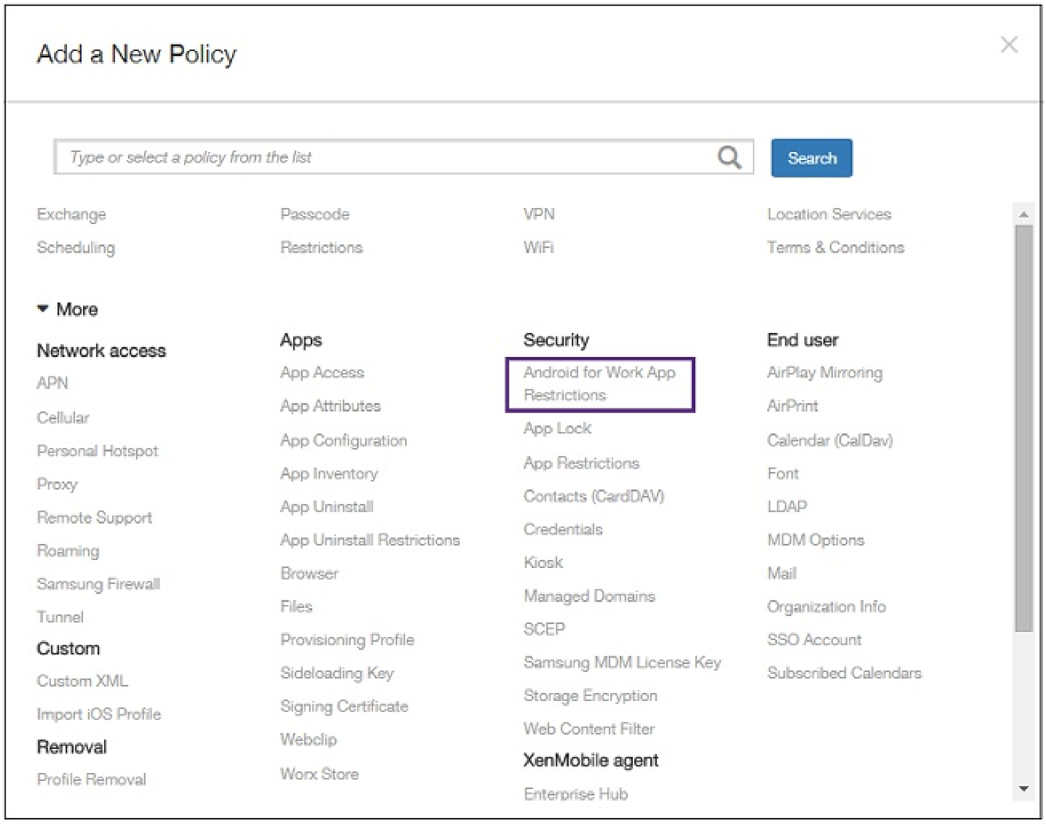
Domain Name*

Domain Admin Account*

Service Account ID*

Binding Token*

Enable Android for Work NO



Samsung KNOX container. The following table lists the MDM policies for the Samsung KNOX container and the operating system to which they apply. The Samsung KNOX container is a secure workspace on devices that separates corporate apps and data from personal apps and data. You configure these policy settings in the XenMobile console in Configure > Device Policies > Restrictions.

Policy	Applies to Samsung KNOX Standard; previously applied to Samsung SAFE	Applies to Samsung KNOX Premium (KNOX 2.0)
Allows for the use of the Samsung SAFE API to configure Access Point Name (APN) and General Packet Radio service (GPRS) settings on an Android device.	X	X
Enables or disables the use of Common Access Card (CAC) authentication in the KNOX container that includes the authentications necessary for email and browser use in the container.		X
Sets the Unlock method as the combination of a fingerprint and a password.		X
Enables or disables whether users can move applications inside the KNOX container.		X
Enables or disables the use of non-secure keyboard in the KNOX container.		X

Policy	Applies to Samsung KNOX Standard; previously applied to Samsung SAFE	Applies to Samsung KNOX Premium (KNOX 2.0)
Enables or disables sharing through a list in the KNOX container.		X
Allows or prevents users from sending or receiving Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages	X	
Allows or prevents users from changing the date and time manually.	X	
Allows users to install apps that are already installed in their personal area to the KNOX container.		X
Enables or disables GMS apps in the KNOX container.		X
Enables or disables the device to be placed into the Common Criteria configuration.		X
Enables or disables the TIMA keystore that provides TrustZone-based secure key storage for the symmetric keys.		X
Enables or disables the device to log events to be used for forensic analysis of the device.		X

XenMobile Server 10.1 Fixed Issues

Oct 30, 2015

Compared to: XenMobile Server 10.

The following issues were fixed in XenMobile 10.1:

- When you add a Generic PKI Entity (GPKI) with the client authentication type, the WSDL URL is not sent to the certificate server to carry out the authentication.

  [#501945]

- To remove Active Directory groups already configured in a delivery group, first search for the Active Directory groups and then clear the check boxes for the groups.

  [#512990]

- You can now configure Microsoft Certificate Authority using basic authentication.

  [#526705]

- You cannot add a single BlackBerry or Windows device in the XenMobile console.

  [#532844]

- You can now install VPN profiles on iOS devices.

  [#533770]

- When using the subject or SAN macro $user.distinguishedname, an extra CN= is no longer added to the name that is imported into the client certificate.

  [#533837]

- RBAC: admins with view-only rights now can only view. They can no longer see options not available to them.

  [#534184]

- Account creation fails on iOS when NetScaler Gateway is listening on non-default port.

  [#537368]

- In the XenMobile console in MDX policies under Authentication, the App Passcode or Online session required setting is now saved.

  [#543397]

- The SSO Account and VPN policy for iOS now works.

  [#549924]

- You can now publish custom-developed Android applications.

[#550111]

- Special characters like $, @ and " are not recognized in passwords for the command-line interface (CLI) when installing XenMobile 10 and those assigned to certificates; the special character and all characters following it are ignored and log on fails. Subsequent to installation, the CLI password cannot be changed to include special characters.

  [#541997] [#542436]

- On enrolled Windows Phone 8.1 devices, no managed apps appear in the software inventory list.

  [#506143]

- 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]

- Automatic synchronization with ShareFile cloud does not occur at the set time each day. As a result, any users that the ShareFile administrator provisioned manually in the cloud since the last successful synchronization are not reconciled.

  [#542494]

- When you configure a Background network services app policy, the character space is limited for your list of FQDN and port of service addresses.

  [#542891]

- When XenMobile is installed on a hypervisor, the time on the XenMobile server may be off by several hours.

  [#543668]

- When an Active Directory user group name contains a dot (.), you cannot save the delivery group.

  [#547957]

- Enterprise apps, such as XenDesktop and XenApp apps, do not appear when users try to access them from the Worx Store through Worx Home when users enroll with an alternate User Principal Name (UPN).

  [#548339]

- If the list of Active Directory groups exceeds 255 characters, the list is truncated and user group memberships are not saved. As a consequence, users may not be able to enroll and delivery groups may not deploy.

  [#548762, #557918]

- On an Android or iOS device running Citrix Receiver, in some cases, users cannot open StoreFront apps from Worx Home.

  [#549824]

- When you configure a VPN device policy in the XenMobile console with the Connection type of IPSec, you cannot configure a shared secret. In addition, if you set the Enable VPN on demand setting to ON, in the On Demand Domain Action list, you cannot specify an action.

[#550560, #550844, #553296]

- In the XenMobile console, when you configure an iOS Secure Actions Lock option, the Message and Phone Number fields allow strings longer than can be displayed properly on the device. In addition, if you click the Lock button, you receive an error message if the Message field contains a question mark character (?). Finally, after you configure the Message and Phone Number fields, and you configure another Lock command, the Message and Phone Number fields sometimes contain the previous configuration information.

  [#551200, #551201, #554811]

- You cannot create and deploy an Exchange ActiveSync device policy when the port number follows the server address, such as mail.example.com:8443.

  [#551313]

- If you configure LDAP authentication, if the length of the user name and password exceeds 76 characters, when you request a CA certificate, an error occurs.

  [#553276]

- When configuring a PKI entity, if you use a distinguished name in the subject name of the certificate that you upload to XenMobile, the certificate name includes "CN" in the name, such as CN = CN=Admin, Joe.

  [#553280]

- When creating an enrollment confirmation template, if you configure a macro for the Recipient of ${device.imei} to return the device IMEI, the macro continually returns the IMEI of the users' first enrolled device and not the IMEI of the users' subsequent devices. The issue occurs when users have the same logon credentials for each enrolled device.

  [#553282]

- When you configure a new NetScaler Gateway instance, when you set the Logon Type to Domain only, you cannot set the Password Required setting to OFF.

  [#553628]

- The Samsung Restriction device policies for Allow Hardware Controls and Add Profiles under WiFi have no effect on devices.

  [#555938]

- You cannot wrap custom-developed .apk Android files. When trying to upload the .apk app to XenMobile, an invalid package type error occurs.

  [#557089]

- In the XenMobile console, the filter for Android for Work is missing from the Device Policies page.

  [#558298]

- In the XenMobile console, when you issue a lock on a device enrolled in Android for Work mode, you see an option to lock the device with a passcode.

[#559098]

- When you re-enroll a device with a different user in Android for Work, the Google Directory Primary Email field is not updated with the new user information.

  [#559161]

- Pushing the Google Play app to an Android for Work device fails.

  [#559174]

- After deploying an Android for Work App Restrictions policy, the Devices tab in the XenMobile console is inaccessible. In addition, you are not able to edit the newly created policy.

  [#560225]

- You are able to upload an unapproved public app on the Android for Work platform.

  [#560390]

- When you select the deployment condition of Only when previous deployment has failed, after you deploy wrapped apps and the apps are installed on enrolled devices, when users access the Worx Store a subsequent time, the apps do not appear. The app icon no longer appears on the device springboard either.

  [#560500]

- In the XenMobile console, when you configure a Generic GPKI Entity, if you set the backend PKI adapter server without authentication, the GPKI does not connect to HTTPS ports. The following error appears: Could not locate the WSDL with the URL you provided. Check the WSDL URL and try again.

  [#560707]

- When Android for Work server settings are incorrect, you can enable Android for Work.

  [#561475]

- You are able to add a self-hosted Android for Work app to a delivery group as a required app.

  [#561485]

- In the XenMobile console, when you configure an iOS Secure Actions Lock option, the Phone Number field allows multiple plus signs (+) to be entered.

  [#561792]

- In the XenMobile console, when you save a Samsung KNOX device restriction policy, an error message appears.

  [#562607]

- When you save an Android for Work configuration without having first imported an Android for Work certificate, a configuration error occurs.

  [#562983]

- When you create an App uninstall device policy for Samsung KNOX and then deploy the policy to remove a particular app, the app is removed from the KNOX container and the icon is removed from the device springboard, but the app appears again after about 3 to 4 seconds.

[#562713]

- When you configure an Android for Work Samsung Browser device policy, bookmark URLs are not validated.

  [#565379]

- In the XenMobile console, when you create a Samsung SAFE device restriction policy, an error message appears when you save the policy.

  [#565697]

XenMobile Server 10.1 Known Issues

Jun 21, 2016

The following issues are known in XenMobile 10.1.

- In XenMobile 10.x you can search for group names only by their pre-Windows 2000 name because the XenMobile console shows the sAMAccountName instead of the CN.
- Due to IIS on servers running Windows 2008 that have an SSL handshake flaw in the TLS v1 implementation, problems occur with Java 8:

  [#492269]

- XenMobile Server 10.1 is supported on Windows 2008 R2 Certificate Authorities with a workaround. To enable TLSv1.1 and TLSv1.2 support, follow the instructions in the Microsoft KB article https://support.microsoft.com/en-us/kb/245030, in the section "SCHANNEL\Protocols subkey."
- XenMobile Server 10.1 is not supported with Windows 2008 "vanilla" Certificate Authorities.
- 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]
- When re-enrolling a device, enrollment may fail if users re-enroll too soon after un-enrolling.
  [#516567]
- 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]
- When you create an action in which the Disabled user is True, when the issue is triggered, the action you configure does not occur.
  [#531024]
- When you configure XenMobile server with a uppercase letter in the host name, such as ABC.Xms.com, the Worx Store does not open on devices after the devices enroll.
  [#545527]
- On an Android device in Android for Work mode, when you add a PKI entity with a GPKI credential provider or Microsoft Certificate Services and associate credential in a Credentials device policy with another device policy, when users refresh the device policies from Worx Home, the certificate is revoked and regenerated in error. As a workaround, deploy the certificate only one time.
  [#547905]
- When you create an Exchange device policy for Windows Phone 8.1 devices and you set the Logging level to Basic, deployment fails. This is a third-party issue.
  [#555923]
- In the XenMobile console, when you configure a Browser device policy for Android for Work, for the URLs in the blacklist, the policy is enforced for exact matches. For example, if you list http://www.example.com, only that URL is blocked, but

not https://www.example.com or http://www.example.com.pk.
[#560963]

- Windows Phone 8.1 devices cannot connect to XenMobile server after certificate renewal. This is a third-party issue.
[#561511]

- You can choose a full wipe action in the XenMobile console from the dashboard for Android for Work devices, but the devices do not support the full wipe action. When you choose this action, the Android for Work devices are selectively wiped and users cannot re-enroll in XenMobile, unless you delete the device from XenMobile.
[#562642]

- On Worx Home for iOS, when launching a Windows app hosted on a XenApp delivery controller with a display name configured with special characters (#%^), you may see the error "Access to your company network not available."
[#564069]

- When you create a Password device policy and set the complexity as Alphanumeric or Numeric, after deploying the policy to Windows Phone 8.1 devices, users cannot choose letters on the keypad. This is a third-party issue.
[#565682]

- On Windows Phone 8.1 devices, if users choose not to install Worx Home while enrolling, required enterprise apps are deployed and installed automatically on the device in error.
[#566166]

- In the XenMobile console, when configuring RBAC settings, when you add a role, in Authorized access, you must clear the Admin console access check box, or in Console features, select one or more option. If not, you can still add the role, but an error appears when users sign on to the console.
[#567076]

- Requiring iTunes passwords on IOS 8.3+ devices is not enforced.
[#567434]

- Cert based enrollment of Worx Home fails on Windows Phone 8.1. For a workaround, see http://support.citrix.com/article/CTX141541.

  [#567812]

- After migrating data in a XenMobile enterprise deployment to XenMobile 10.1, the following issues occur with enrolled Windows Phone 8.1 devices:
  - Users with Windows Phone 8.1 devices cannot log on to the Worx Store.
  - users cannot open installed enterprise apps from Worx Home, but they can open the apps from the main menu.
  - Users cannot open the Worx Store.

  [#568316]

- When creating advanced deployment rules, if you add a rule for Limit by known device property name and you set the property value as True or False, the rule doesn't work as expected. For example, the rule for Supervised equal to False does not work. As a workaround, the property value you should choose for the Limit by known device property name rule should be a Boolean value: 0 to indicate False and a -1 to indicate True.
[#568964]

- Not all required iOS apps are pushed to all users after enrolling Worx Home do to a delay in APNS.
[#569978]

- When providing a host name for the command line interface, no error is indicated when you enter invalid characters. The host name cannot have a - as the first character and cannot contain the following characters: **$? /**

  [#570147]

- On the XenMobile console, when you open Settings -> NetScaler Gateway, you see the following instruction: "If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well." This is incorrect. You do not need to do anything with StoreFront.
  [#570820]

- When you configure a single device policy for both Android and Android for Work platforms, the policy for the Android device also takes effect on an Android for Work device. As a workaround, configure a separate policy for each platform and assign different users to each policy. That is, assign users with Android devices to the Android policy and assign users with Android for Work devices to the Android for Work policy.
  [#570828]

- In the XenMobile console, when configuring your connection to ShareFile, if the ShareFile admin password contains the characters **%** or **^**, you will get an error or see other spurious behavior. To avoid this, change the ShareFile admin account password so it does not include the characters **%** or **^** .
  [#571283]

- Users cannot enroll devices running Android for Work with the enrollment method "User Name + PIN" This setting appears in the XenMobile console in Configure -> Settings -> Enrollment -> User name + PIN.

  [#571919]

- When you configure LDAP with sAMAccountName as the means for user searches, Android devices cannot enroll in Android for Work mode. This is a third-party issue.
  [#571927]

- In cloud deployments, NetScaler Gateway connectivity checks under Support Page may incorrectly show STA status as Fail.
  [#573564]

- Devices running Android M may have problems re-enrolling. This is a third-party issue.

  [#574746]

- If you are using SSL on the SQL Server, upload the Trusted Root CA Certificate through the XenMobile 10.0 Console prior to upgrading. Failure to do so causes a reboot loop.

  [#574751]

- Schedule the shutting down cluster nodes in Maintenance mode because there could be a two-minute window of outage.
  [#575644]

- Join new nodes only after bringing up the first node in the cluster.

  [#575671]

- An invalid profile error occurs when you try to configure the iOS Device Enrollment Program in the XenMobile console.

This is a third-party issue.

[#607143]

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

  [#633854]

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. See About the MDX Toolkit.
- StoreFront (optional). You can provide access to Windows-based apps and virtual desktops from StoreFront through connections with Receiver.
- ShareFile Enterprise (optional). If you deploy ShareFile, you can enable enterprise directory integration through XenMobile, which acts as a Security Assertion Markup Language (SAML) identity provider. For more information about configuring identity providers for ShareFile, see the ShareFile support site.

XenMobile supports an integrated solution that provides device management, as well as app management through the XenMobile console. This section describes the reference architecture for the XenMobile deployment.

In a production environment, Citrix recommends deploying the XenMobile solution in a cluster configuration for both scalability, as well as server redundancy purposes. Also, leveraging the NetScaler SSL Offload capability can further reduce the load on the XenMobile server and increase throughput. For more information about how to setup clustering for XenMobile 10.x by configuring two load balancing virtual IP addresses on NetScaler, see Configuring Clustering for

XenMobile 10.

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

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

Mobile device management (MDM) mode

XenMobile MDM Edition provides mobile device management for iOS, Android, Amazon, and Windows Phone (see Supported Device Platforms in XenMobile). You deploy XenMobile in MDM mode if you plan to use only the MDM features of XenMobile. For example, you need to manage a corporate-issued device through MDM in order to deploy device policies, apps and to retrieve asset inventories and be able to carry out actions on devices, such as a device wipe.

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

Mobile app management (MAM) mode

MAM supports iOS and Android devices, but not Windows Phone devices (see Supported Device Platforms in XenMobile). You deploy XenMobile in MAM mode (also referred to as MAM-only mode) if you plan to use only the MAM features of XenMobile without having devices enroll for MDM. For example, you want to secure apps and data on BYO mobile devices; you want to deliver enterprise mobile apps and be able to lock apps and wipe their data. The devices cannot be MDM enrolled.

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

MDM+MAM mode

Using the MDM and MAM modes together provides mobile app and data management as well as mobile device management for iOS, Android, and Windows Phone (see Supported Device Platforms in XenMobile). You deploy XenMobile in ENT (enterprise) mode if you plan to use MDM+MAM features of XenMobile. For example, you want to manage a corporate-issued device via MDM; you want to deploy device policies and apps, retrieve an asset inventory, and be able to wipe devices. You also want to deliver enterprise mobile apps and be able to lock apps and wipe the data on devices.

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

XenMobile in the internal network

You can deploy an architecture with XenMobile in the internal network, rather than in the DMZ, to meet one or more of the following requirements:

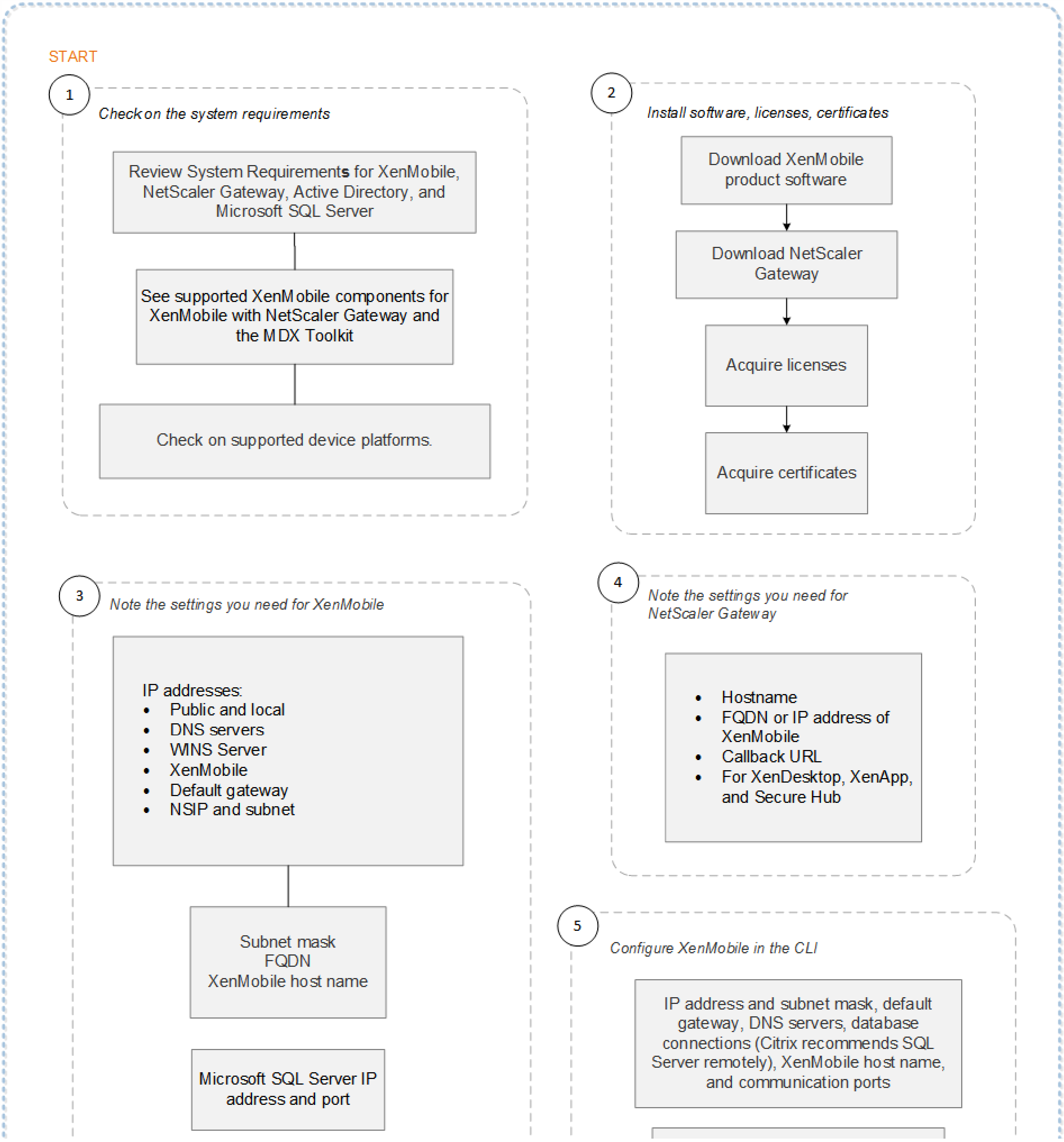
- You do not have or are not allowed to have a hypervisor in the DMZ.
- Your DMZ can only contain network appliances.

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

Flowchart for Deploying XenMobile with NetScaler Gateway

May 05, 2016

You can use this flowchart to guide you through the main steps for deploying XenMobile 10.1 with NetScaler Gateway. Links to topics on each step follow the figure.



START

1 Check on the system requirements

Review System Requirements for XenMobile, NetScaler Gateway, Active Directory, and Microsoft SQL Server

See supported XenMobile components for XenMobile with NetScaler Gateway and the MDX Toolkit

Check on supported device platforms.

2 Install software, licenses, certificates

Download XenMobile product software

Download NetScaler Gateway

Acquire licenses

Acquire certificates

3 Note the settings you need for XenMobile

IP addresses:

- Public and local
- DNS servers
- WINS Server
- XenMobile
- Default gateway
- NSIP and subnet

Subnet mask
FQDN
XenMobile host name

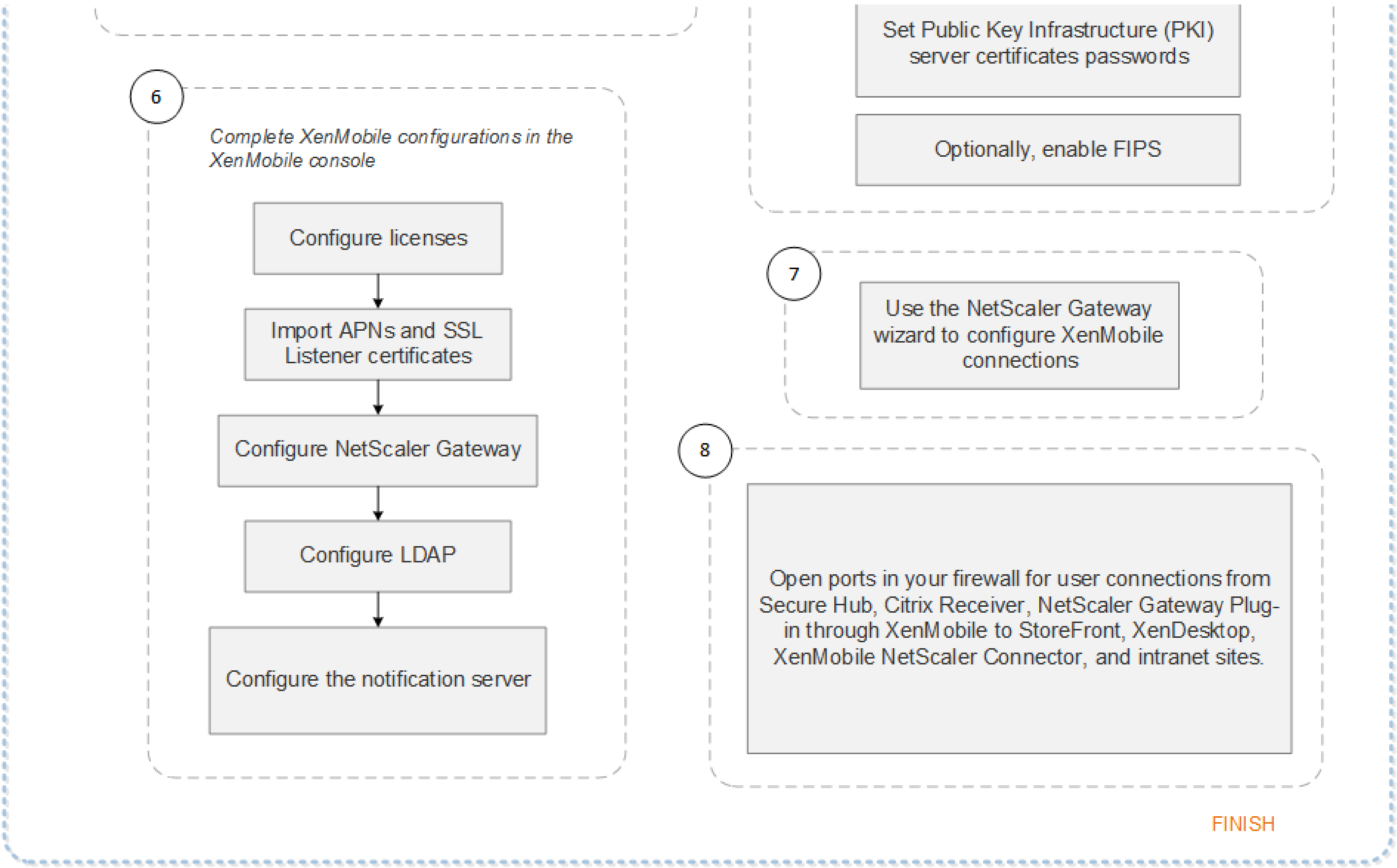
Microsoft SQL Server IP address and port

4 Note the settings you need for NetScaler Gateway

- Hostname
- FQDN or IP address of XenMobile
- Callback URL
- For XenDesktop, XenApp, and Secure Hub

5 Configure XenMobile in the CLI

IP address and subnet mask, default gateway, DNS servers, database connections (Citrix recommends SQL Server remotely), XenMobile host name, and communication ports


Set Public Key Infrastructure (PKI) server certificates passwords
Optionally, enable FIPS
6
Complete XenMobile configurations in the XenMobile console
Configure licenses
Import APNs and SSL Listener certificates
Configure NetScaler Gateway
Configure LDAP
Configure the notification server
7
Use the NetScaler Gateway wizard to configure XenMobile connections
8
Open ports in your firewall for user connections from Secure Hub, Citrix Receiver, NetScaler Gateway Plug-in through XenMobile to StoreFront, XenDesktop, XenMobile NetScaler Connector, and intranet sites.
FINISH

1

- System Requirements for XenMobile 10.1
- XenMobile Compatibility
- Supported Device Platforms in XenMobile 10.1

2

- Installing XenMobile
- Certificates in XenMobile
- Licensing for XenMobile

3

- XenMobile Pre-Installation Checklist

4

- XenMobile Pre-Installation Checklist

5

- Configuring XenMobile in the Command Prompt Window

6

- Configuring XenMobile in a Web Browser

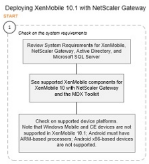
7

- Configuring Settings for Your XenMobile Environment

8

- XenMobile Port Requirements

Click the thumbnail image to download the flowchart in PDF format.



Deploying XenMobile 10.1 with NetScaler Gateway

START

1 Check on the system requirements

Review System Requirements for XenMobile, NetScaler Gateway, Active Directory, and Microsoft SQL Server

See supported XenMobile components for XenMobile 10 with NetScaler Gateway and the MDX Toolkit

Check on supported device platforms. Note that Windows Mobile and CE devices are not supported in XenMobile 10.1; Android must have ARM-based processors; Android x86-based devices are not supported.

Scaling XenMobile

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.

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

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.

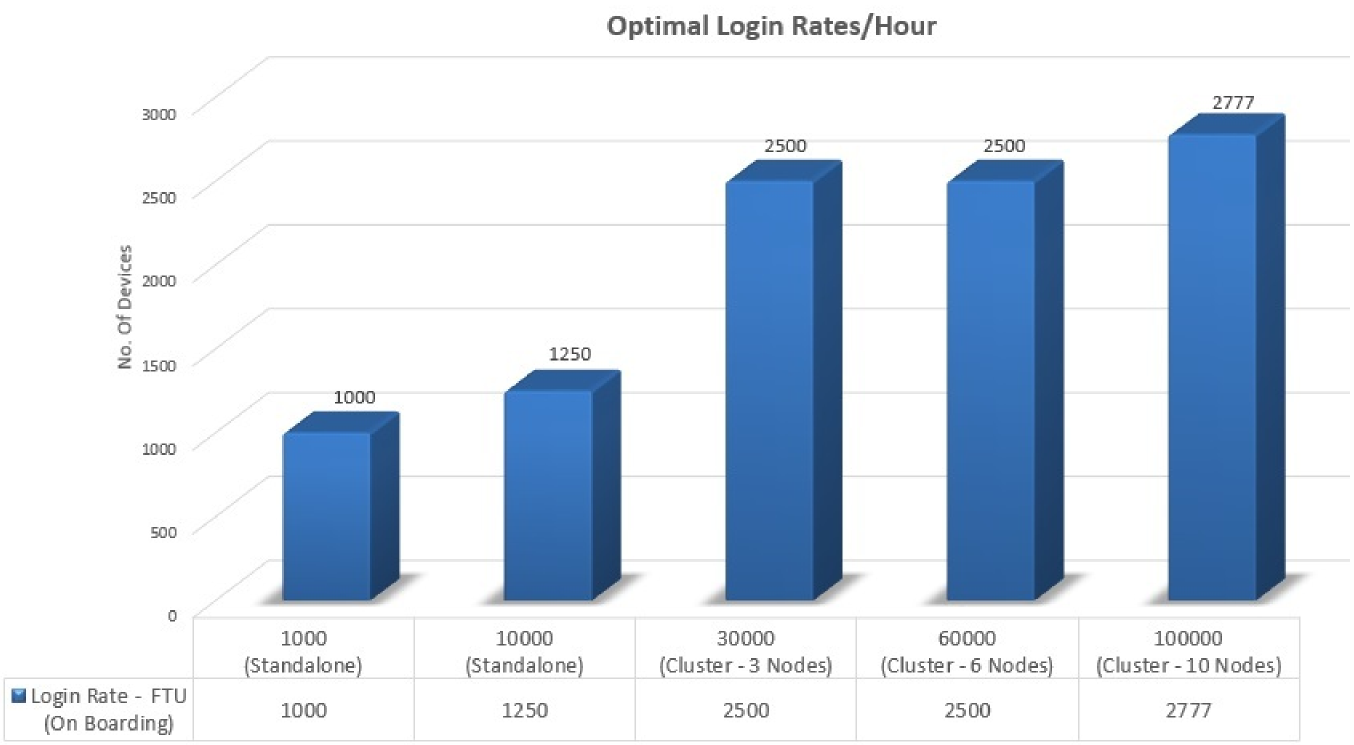
Table 2. XenMobile Enterprise with Enrollment Scalability Results

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	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.

Figure 1. XenMobile Enterprise with Enrollment — Logon Rate per Hour

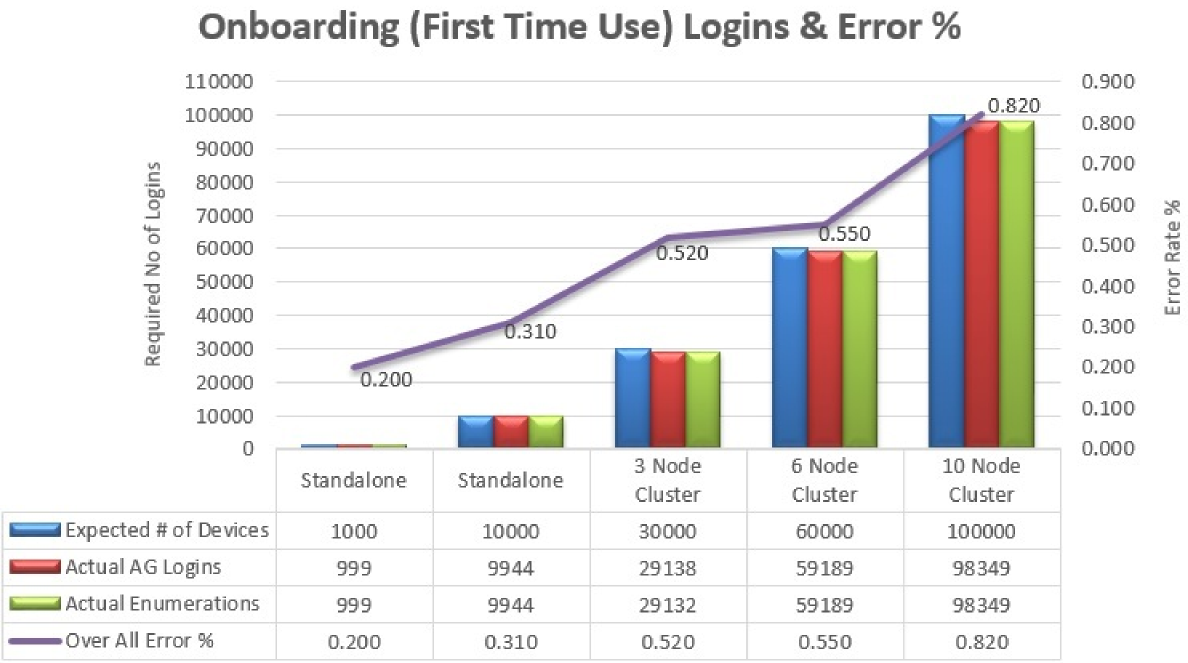


Note: You will experience the following if you exceed the recommended rates or hardware recommendations when sizing your system.

- 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.

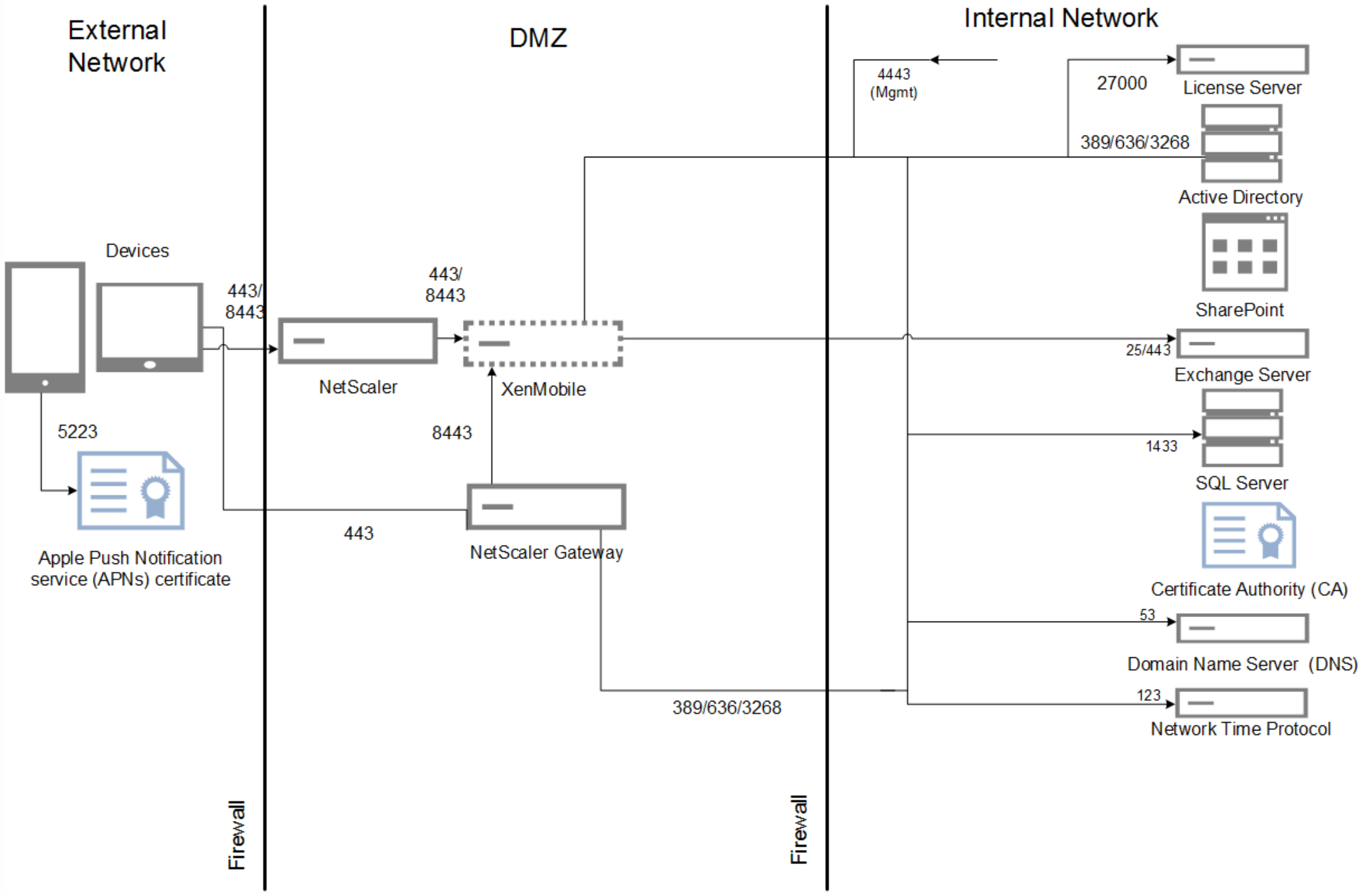
Figure 2. On-boarding (FTU) Logons and Error Percentage with Enrollment



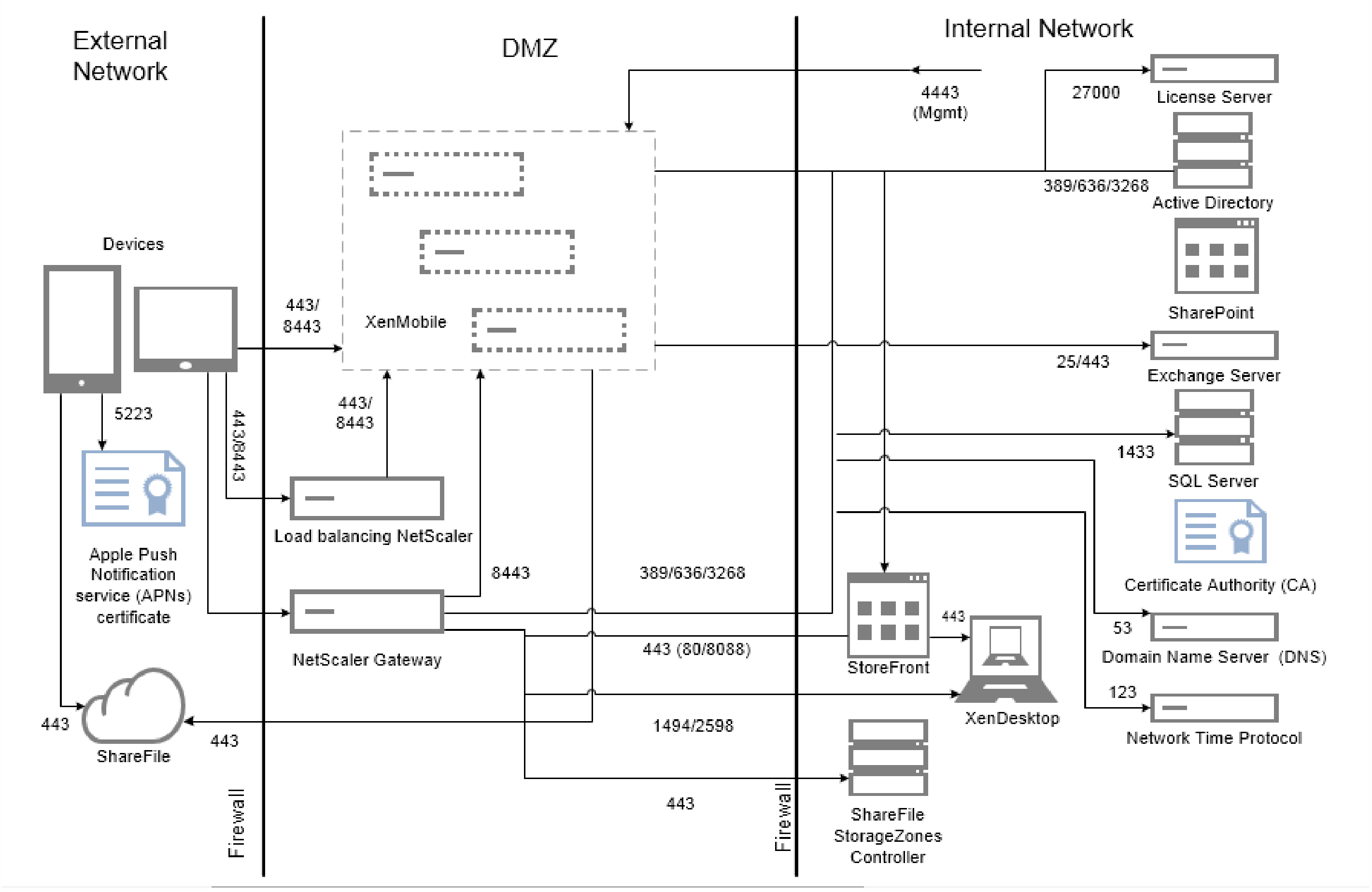
	Standalone	Standalone	3 Node Cluster	6 Node Cluster	10 Node Cluster
🟦 Expected # of Devices	1000	10000	30000	60000	100000
🟥 Actual AG Logins	999	9944	29138	59189	98349
🟩 Actual Enumerations	999	9944	29132	59189	98349
— Over All Error %	0.200	0.310	0.520	0.550	0.820

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 MAM over HTTP that supports 10,000 or more devices.



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

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

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

User workloads are defined as follows:

Table 3. User Workload Definitions

User sessions/devices	Includes NetScaler Gateway logons, enumerations, device registration, and so on for each session.
Worx Store	Users launch Worx Store multiple times and each time they subscribe to or install more than one app

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

Notes and Assumptions

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

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

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

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

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

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

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

- Policy Push to device is not tested.
- Android Connected Devices not tested.
- Package deployment is not tested.
- Windows platform is not tested.

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

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

On-Boarding (FTU) Workload

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

- Auto discovery
- Enrollment
- Authentication
- Device registration
- Application delivery (web, SaaS, and mobile MDX apps)
  - App subscription (including images and icon downloads)
  - Installation of the subscribed MDX apps
- App launch (web, SaaS, and mobile MDX apps)
- 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 session[1]		~19.7 MB	~ 40.7 MB

1. **Per session**: 8 hours.

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

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

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.

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.

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

Table 8. XenMobile Infrastructure Components

Component	Version
NetScaler Gateway	10.5-57.4.nc
XenMobile	10.1.0.63030
External database	MS SQL Server 2014 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 9. XenServer Hardware

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

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

For additional product information and technical questions concerning this article or the products mentioned herein, see Citrix.com, search the XenMobile documentation site for the latest product documentation, or contact your local Citrix representative.

About XenMobile Cloud

Aug 12, 2016

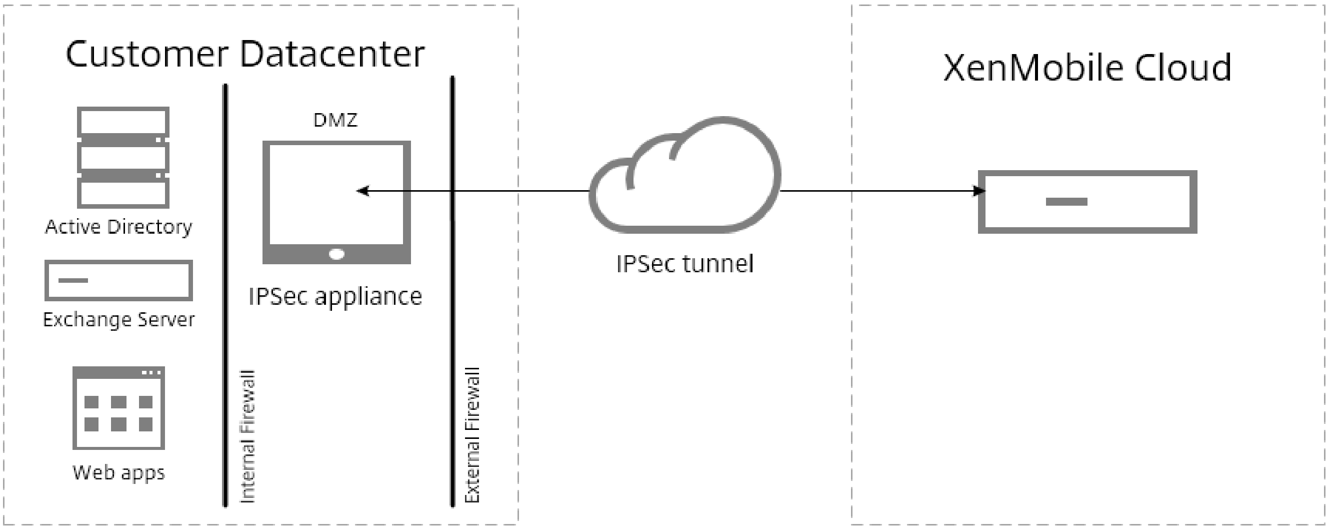
XenMobile Cloud is a product service that offers a XenMobile enterprise mobility management (EMM) environment for managing apps and devices as well as users or groups of users. With XenMobile Cloud, Citrix handles the configuration and maintenance of the infrastructure onsite through the Citrix Cloud 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 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 you existing infrastructure by installing and deploying Citrix CloudBridge or by using an existing IPsec gateway in your datacenter.

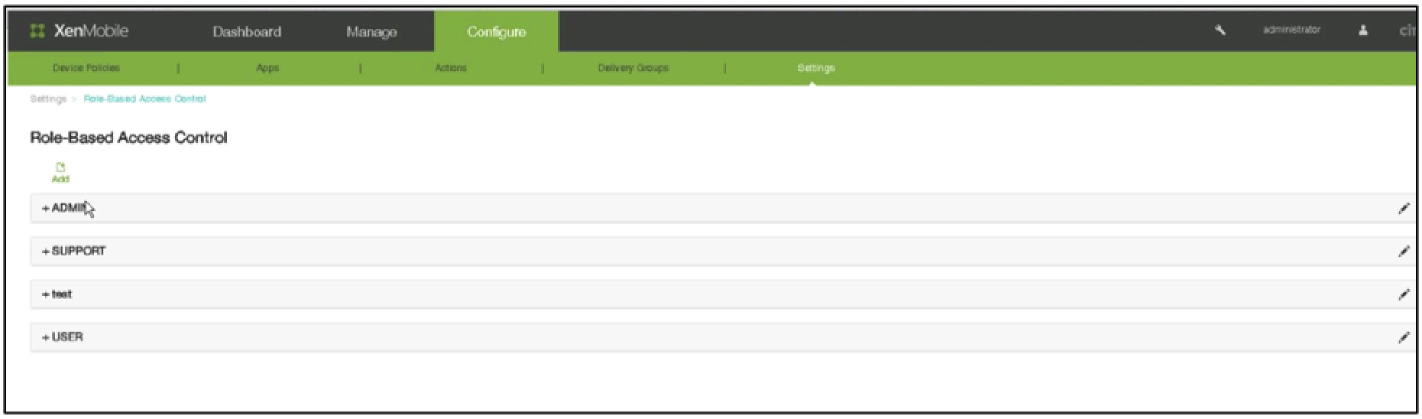
This architecture allows you to benefit from using NetScaler either in the cloud, as handled by the Cloud Operations group, or in your datacenter. When used in the datacenter, NetScaler gives you a single point of management to control access and limit actions within sessions based on both user identity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

Support	Log Operations	Log Settings->Log Size	Cloud Admin and Tech Support

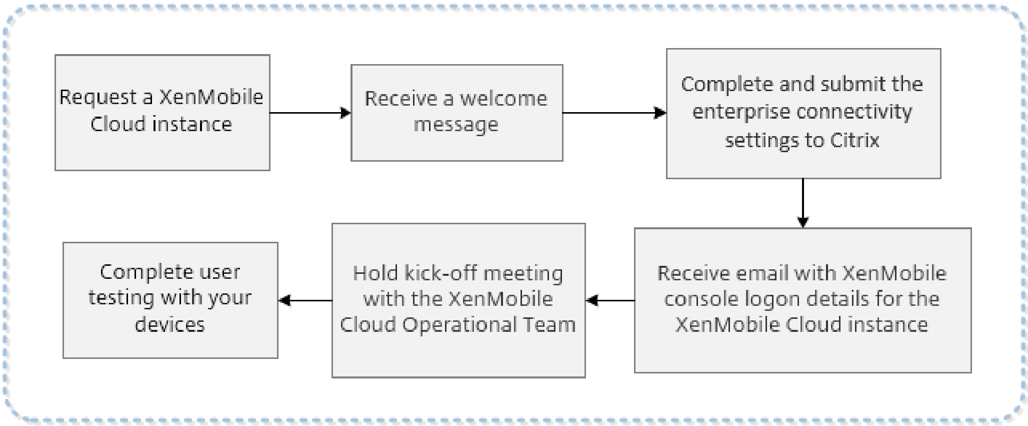
For step-by-step instructions on customizing roles, see Configuring Roles with RBAC.

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.


Request a XenMobile Cloud instance
Receive a welcome message
Complete and submit the enterprise connectivity settings to Citrix
Receive email with XenMobile console logon details for the XenMobile Cloud instance
Hold kick-off meeting with the XenMobile Cloud Operational Team
Complete user testing with your devices

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

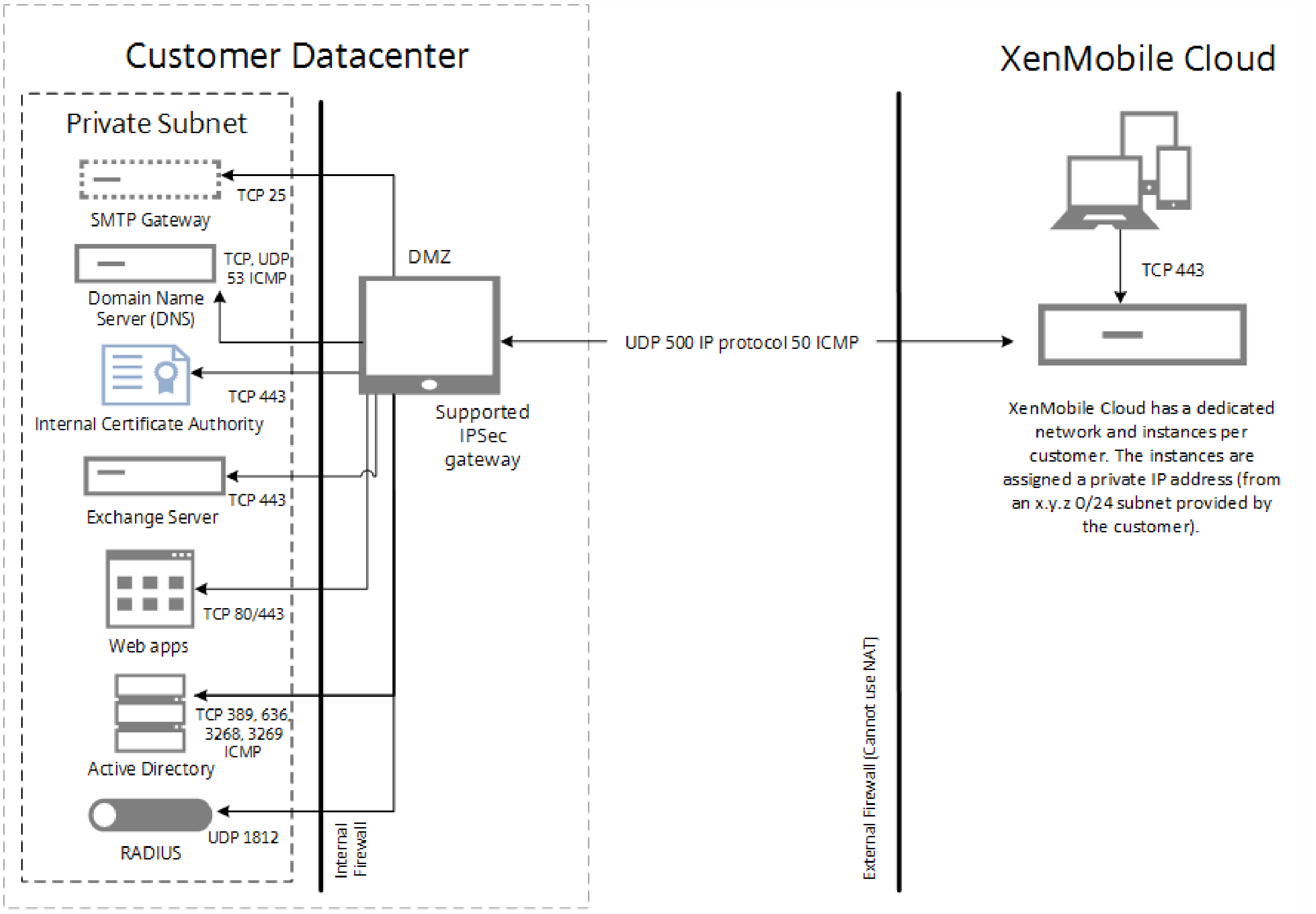
You can use a XenMobile Enterprise Connector, an IPsec tunnel to connect the XenMobile Cloud infrastructure with corporate services, such as Active Directory.

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.



Customer Datacenter
Private Subnet
TCP 25
SMTP Gateway
TCP, UDP 53 ICMP
Domain Name Server (DNS)
TCP 443
Internal Certificate Authority
TCP 443
Exchange Server
TCP 80/443
Web apps
TCP 389, 636, 3268, 3269 ICMP
Active Directory
UDP 1812
RADIUS
Internal Firewall
DMZ
Supported IPSec gateway
UDP 500 IP protocol 50 ICMP
External Firewall (Cannot use NAT)
XenMobile Cloud
TCP 443
XenMobile Cloud has a dedicated network and instances per customer. The instances are assigned a private IP address (from an x.y.z 0/24 subnet provided by the customer).

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, UPP, 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

Sep 25, 2015

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.

- 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.

- 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.

- 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

Dec 05, 2016

To run XenMobile 10.1, you need the following minimum system requirements:

- One of the following:
  - XenServer (supported versions: 6.5.x, 6.2.x, 6.1.x, or 6.0.x); for details, refer to XenServer
  - VMWare (supported versions: ESXi 4.1, ESXi 5.1, or ESXi 5.5); 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
- 4 GB of RAM
- 50 GB disk space

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

- Quad core processor
- 16 GB of RAM

To run NetScaler Gateway with XenMobile 10.1, you need the following minimum system requirements:

- One of the following:
  - XenServer (supported versions: 6.2.x, 6.1.x, or 6.0.x)
  - VMWare (supported versions: ESXi 4.1, ESXi 5.1, or ESXi 5.5)
  - Hyper-V (supported versions: Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2)
- Two virtual CPUs
- 2 GB of RAM
- 20 GB disk space

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

XenMobile requires one of the following databases:

- Microsoft SQL Server

  The XenMobile repository supports a Microsoft SQL Server database running on one of the following supported versions (for more information about Microsoft SQL Server databases, see Microsoft SQL Server):

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

  XenMobile 10.1 supports SQL AlwaysOn Availability Groups and SQL Clustering for database high availability.

Citrix recommends using Microsoft SQL remotely.

Note: Make sure the service account of the SQL Server to be used on XenMobile has the DBcreator role permission. For more information about SQL Server service accounts, see the following pages on the Microsoft Developer Network site (these links point to information for SQL Server 2014. If you are using a different version, select your server version from the **Other Versions** list):
Server Configuration - Service Accounts

Configure Windows Service Accounts and Permissions

Server-Level Roles

- PostgreSQL

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

  Note: All XenMobile editions support Remote PostgreSQL 9.3.11 for Windows with the following limitations:

  - Support for up to 300 devices

    Use on-premises SQL Server for more than 300 devices.

  - No support for clustering

XenMobile 10.1 supports the following mail servers:

- Exchange 2013
- Exchange 2010

XenMobile Compatibility

Feb 11, 2016

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

Supported Device Platforms

Feb 10, 2016

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

Port Requirements

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.

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

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

443	Used for connections to StoreFront from Citrix Receiver or Receiver for Web to XenApp and XenDesktop.	Internet	NetScaler Gateway
	Used for connections to XenMobile for web, mobile, and SaaS app delivery.	Internet	NetScaler Gateway
	Used for general device communication to XenMobile server	XenMobile	XenMobile
	Used for connections from mobile devices to XenMobile for enrollment.	Internet	XenMobile
	Used for connections from XenMobile to XenMobile NetScaler Connector.	XenMobile	XenMobile NetScaler Connector
	Used for connections from XenMobile NetScaler Connector to XenMobile.	XenMobile NetScaler Connector	XenMobile
	Used for Callback URL in deployments without certificate authentication.	XenMobile	NetScaler Gateway
514	Used for connections between XenMobile and a syslog server.	XenMobile	Syslog server
636	Used for secure LDAP connections.	NetScaler Gateway XenMobile	LDAP authentication server or Active Directory
1494	Used for ICA connections to Windows-based applications in the internal network. Citrix recommends keeping this port open.	NetScaler Gateway	XenApp or XenDesktop
1812	Used for RADIUS connections.	NetScaler Gateway	RADIUS authentication server
2598	Used for connections to Windows-based applications in the internal network using session reliability. Citrix recommends keeping this port open.	NetScaler Gateway	XenApp or XenDesktop

3268	Used for Microsoft Global Catalog insecure LDAP connections.	NetScaler Gateway XenMobile	LDAP authentication server or Active Directory
3269	Used for Microsoft Global Catalog secure LDAP connections.	NetScaler Gateway XenMobile	LDAP authentication server or Active Directory
9080	Used for HTTP traffic between NetScaler and the XenMobile NetScaler Connector.	NetScaler	XenMobile NetScaler Connector
9443	Used for HTTPS traffic between NetScaler and the XenMobile NetScaler Connector.	NetScaler	XenMobile NetScaler Connector
45000 80	Used for communication between two XenMobile VMs when deployed in a cluster.	XenMobile	XenMobile
8443	Used for enrollment, XenMobile Store and mobile app management (MAM).	XenMobile NetScaler Gateway Devices Internet	XenMobile
4443	Used for accessing the XenMobile console by an administrator through the browser.	Access point (browser)	XenMobile
	Used for downloading logs and support bundles for all XenMobile cluster nodes from one node.	XenMobile	XenMobile
27000	Default port used for accessing the external Citrix License Server	XenMobile	Citrix License Server
7279	Default port used for checking Citrix licenses in and out.	XenMobile	Citrix Vendor Daemon

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, 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)
	Used for outbound connections between XenMobile and Nexmo SMS Notification Relay.		Nexmo SMS Relay Server
443	Used for outbound connections to AutoDiscovery server.	XenMobile	https://discovery.mdm.zenprise.com
	Used for enrollment and agent setup for Android and Windows devices, the XenMobile web console, and MDM Remote Support Client.	Internal LAN and WiFi	
	Used for enrollment and agent setup for Android and Windows Mobile.	Internet	XenMobile
1433	Used by default for connections to a remote database server (optional).	XenMobile	SQL Server
2195	Used for Apple Push Notification service (APNs) outbound connections to gateway.push.apple.com for iOS device notifications and device policy push.	XenMobile	Internet (APNs hosts using the public IP address 17.0.0.0/8)
2196	Used for APNs outbound connections to feedback.push.apple.com for iOS device notification and device policy push.		
5223	Used for APNs outbound connections from iOS devices on Wi-Fi networks to *.push.apple.com.	iOS devices on WiFi networks	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	

This port configuration ensures that Android devices connecting from Worx Home for Android, versions 10.2 and 10.3, can access the Citrix Auto Discovery Service (ADS) from within the internal network. The ability to access the ADS is important when downloading any security updates made available through the ADS.

Note: ADS connections might not work with your proxy server. In this scenario, allow the ADS connection to bypass the proxy server.

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

- **Collect XenMobile Server and NetScaler certificates**. The certificates need to be in PEM format and must be a public certificate and not the private key.
- **Contact Citrix Support and place a request to enable certificate pinning**. During this process, you are asked for your certificates.

New certificate pinning improvements require that devices connect to ADS before the device enrolls. This ensures that the latest security information is available to Worx Home for the environment in which the device is enrolling. Worx Home will not enroll a device that cannot reach the ADS. Therefore, opening up ADS access within the internal network is critical to enabling devices to enroll.

To allow access to the ADS for Worx Home 10.2 for Android, open port 443 for the following FQDN and IP addresses:

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

107.20.198.193

FIPS 140-2 Compliance

Sep 07, 2015

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

Important: You can enable XenMobile FIPS mode only during initial installation.

Note: XenMobile mobile device management-only, XenMobile mobile app management-only, and XenMobile Enterprise are all FIPS compliant as long as no HDX apps are used.

All data-at-rest and data-in-transit cryptographic operations at XenMobile Device Manager use cryptographic modules provided by OpenSSL validated as FIPS compliant. (See the following details for recent developments.) 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 validated cryptographic modules end-to-end.

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.

XenMobile Language Support

Feb 10, 2016

Citrix Worx apps and the XenMobile console are adapted for use in languages other than English. This includes support for non-English characters and keyboard input even when the app is not localized in the users' preferred language.

The following table shows the languages into which the most recent versions of the Worx apps are translated with an X to indicate language support.

User Interface Languages	Japanese	Simplified Chinese	German	French	Spanish	Korean	Portuguese	Dutch	Italian	Danish	Swedish
Apple iPhone/iPad											
Worx Home	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X			
Android Phone/Tablet											
Worx Home	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X			
WinPhone											
Worx Home			X	X	X				X	X	X

WorxMail	X	X	X				X	X	X
WorxWeb	X	X	X				X	X	X

For the complete globalization status of Citrix products, see the Citrix Knowledge Center.

The following table summarizes the XenMobile console translation status with an X to indicate language availability.

Languages	Simplified Chinese	French
XenMobile console	X	X

Pre-Installation Checklist

Nov 02, 2015

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

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	

	Prerequisite or setting	Component or function	Note the setting
	If you configure a cluster, note all of the IP addresses you need. ● One public IP address configured on NetScaler Gateway ● One external DNS entry for NetScaler Gateway	NetScaler Gateway	
	Note the web proxy server IP address, port, proxy host list, and the administrator user name and password. These settings are optional if you deploy a proxy server in your network (if applicable). Note: You can user either the sAMAccountName or the User Principal Name (UPN) when configuring the user name for the web proxy.	XenMobile NetScaler Gateway	
	Note the default gateway IP address.	XenMobile NetScaler Gateway	
	Note the system IP (NSIP) address and subnet mask.	NetScaler Gateway	
	Note the subnet IP (SNIP) address and subnet mask.	NetScaler Gateway	
	Note the NetScaler Gateway virtual server IP address and FQDN from the certificate. If you need to configure multiple virtual servers, note all of the virtual IP addresses and FQDNs from the certificates.	NetScaler Gateway	
	Note the internal networks that users can access through NetScaler Gateway. Example: 10.10.0.0/24 Enter all internal networks and network segments that users need access to when they connect with Worx Home or the NetScaler Gateway Plug-in when split tunneling is set to On.	NetScaler Gateway	
	Make sure that the network connectivity between the XenMobile server, NetScaler Gateway, the external Microsoft SQL Server, and the DNS server are reachable.	XenMobile NetScaler Gateway	

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	

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	

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	

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	

•	Prerequisite	Component	Note the setting
	Before installing a XenMobile server in FIPS mode, you need to complete prerequisites with SQL Server. For details, see Configuring FIPS with XenMobile.		

•	Prerequisite	Component	Note the setting
	Note the Active Directory IP address and port for the primary and secondary servers. If you use port 636, install a root certificate from a CA on XenMobile, and change the Use secure connections option to Yes.	XenMobile NetScaler Gateway	
	Note the Active Directory domain name.	XenMobile NetScaler Gateway	
	Note the Active Directory service account, which requires a user ID, password, and domain alias. The Active Directory service account is the account that XenMobile uses to query Active Directory.	XenMobile NetScaler Gateway	
	Note the User Base DN. This is the directory level under which users are located; for example, cn=users,dc=ace,dc=com. NetScaler Gateway and XenMobile use this to query Active Directory.	XenMobile NetScaler Gateway	
	Note the Group Base DN. This is the directory level under which groups are located. NetScaler Gateway and XenMobile use this to query Active Directory.	XenMobile NetScaler Gateway	

✓	Prerequisite	Component	Note the setting
	Note the XenMobile host name.	XenMobile	
	Note the FQDN or IP address of XenMobile.	XenMobile	

✓	Prerequisite	Component	Note the setting
	Identify the apps users can access.	NetScaler Gateway	
	Note the Callback URL.	XenMobile	

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	

Installing XenMobile

Oct 09, 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 10.1 and the XenMobile Pre-Installation Checklist.

Note: Ensure that the hypervisor is configured with the correct time because XenMobile uses that time. Also, be sure that the XenMobile virtual machine is configured to synchronize guest time with the host in the Virtual Machine properties.
XenServer or VMware ESXi prerequisites: Before installing XenMobile on XenServer or VMware ESXi, you must do the following. For details, refer to your XenServer or VMware documentation.

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

FIPs mode prerequisites: Before installing a XenMobile Server in FIPS mode, you need to complete prerequisites with SQL Server. For details, see Configuring FIPS with XenMobile.

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.
- If you install Windows Server 2008 R2 or Windows Server 2012, do the following:
  - Delete the file Virtual Machines/<build-specific UUID>.xml
  - Move the file Legacy/<build-specific UUID>.exp into Virtual Machines

  These steps are necessary because there are two different versions of the Hyper-V manifest file representing the VM configuration (.exp and .xml). The Windows Server 2008 R2 and Windows Server 2012 releases support only .exp. For these releases, you must have only the .exp manifest file in place before installation.

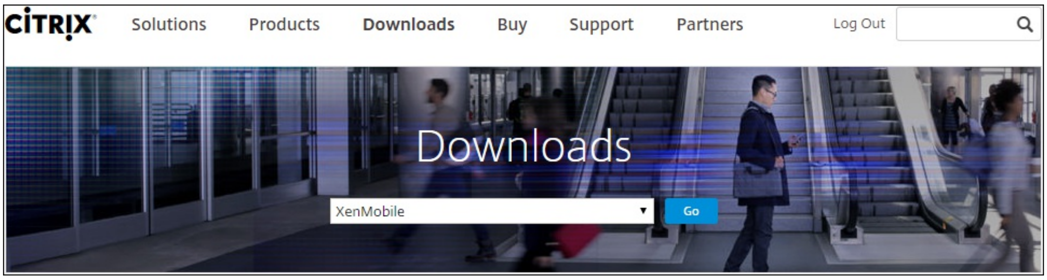
  Windows Server 2012 R2 does not require these extra steps.

You can download product software from the Citrix web site. You need to log on to the site first and then use the Downloads link on the Citrix web page to navigate to the page containing the software you want to download.

To download the software for XenMobile

1. Go to the Citrix web site.
2. Next to the Search box, click Log On and log on to your account.
3. Click the Downloads tab.

4. On the Downloads page, from the select product list, click XenMobile.



5. Click Go. The XenMobile page appears.
6. Expand XenMobile 10.
7. Click XenMobile 10.0 Server.
8. On the XenMobile 10.0 Server edition page, click Download next to the appropriate virtual image to use to install XenMobile on XenServer, VMware, or Hyper-V.
9. Follow the instructions on your screen to download the software.

To download the software for NetScaler Gateway

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

1. Go to the Citrix web site.
2. If you are not already logged on to the Citrix web site, next to the Search box, click Log On and log on to your account.
3. Click the Downloads tab.
4. On the Downloads page, from the select product list, click NetScaler Gateway.
5. Click Go. The NetScaler Gateway page appears.
6. On the NetScaler Gateway page, expand 10.5.
7. Under Firmware, click the appliance software version you want to download.
   Note: You can also click Virtual Appliances to download NetScaler VPX. When you select this option, you receive a list of software for the virtual machine for each hypervisor.
8. Click the appliance software version you want to download.
9. On the appliance software page for the version you want to download, click Download for the appropriate virtual appliance.
10. Follow the instructions on your screen to download the software.

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

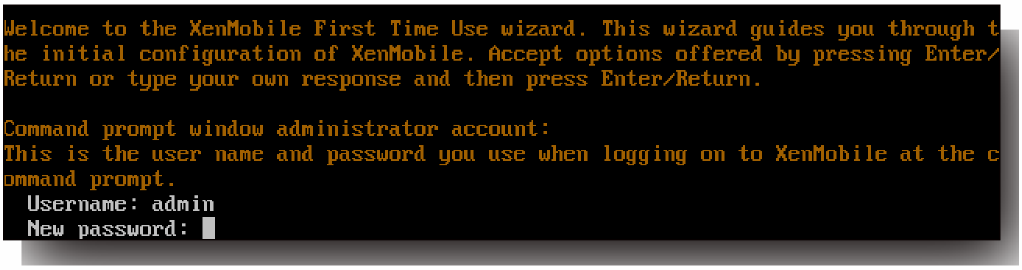
1. Configure the IP address and subnet mask, default gateway, DNS servers, and so on for XenMobile by using the XenCenter or vSphere command-line console.
2. Log on to the XenMobile management console and follow the steps in the initial logon screens.

> ### Note
>
> When you use a vSphere web client, it is recommended that you do not configure networking properties during the time you deploy

the OVF template on the **Customize template** page. By doing so, in a high availability configuration, you avoid an issue with the IP address that occurs when you clone and then restart the second XenMobile virtual machine.

Configuring XenMobile in the Command Prompt Window

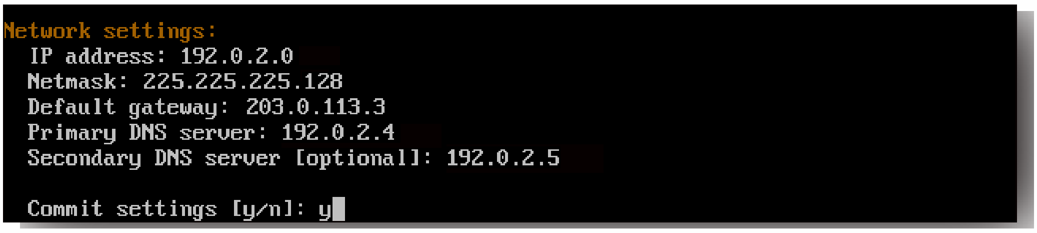
1. Import the XenMobile virtual machine into Citrix XenServer, Microsoft Hyper-V, or VMware ESXi. For details, see XenServer, Hyper-V, or VMware documentation.
2. In your hypervisor, select the imported XenMobile virtual machine and start the command prompt view. For details, see the documentation for your hypervisor.
3. From the hypervisor's console page, create an administrator account for XenMobile in the command prompt window by typing the administrator user name and password.
   Important:
   When you create or changed passwords for the command prompt administrator account, Public Key Infrastructure (PKI) server certificates, and FIPS, XenMobile enforces the following rules for all users except Active Directory users whose passwords are managed outside of XenMobile:
   - The password must be at least 8 characters long and must meet at least three of the following complexity criteria:
     - Uppercase letters (A through Z)
     - Lowercase letters (a through z)
     - Numerals (0 through 9)
     - Special characters (such as, !, #, $, %)



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

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

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

4. Provide the following network information and then, type y to commit the settings:
   1. IP address
   2. Netmask
   3. Default gateway
   4. Primary DNS server
   5. Secondary DNS server (optional)

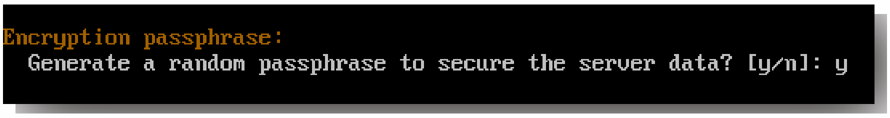


```
Network settings:
  IP address: 192.0.2.0
  Netmask: 225.225.225.128
  Default gateway: 203.0.113.3
  Primary DNS server: 192.0.2.4
  Secondary DNS server [optional]: 192.0.2.5

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

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

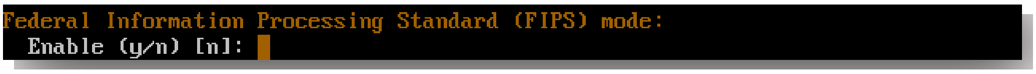
5. Type y to increase security by generating a random encryption passphrase or n to provide your own passphrase. Citrix recommends typing y to generate a random passphrase. The passphrase is used as part of the protection of the encryption keys used to secure your sensitive data. A hash of the passphrase,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

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



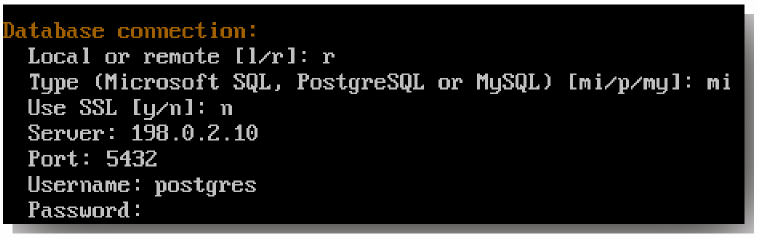
```
Encryption passphrase:
  Generate a random passphrase to secure the server data? [y/n]: y
```

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]:
```

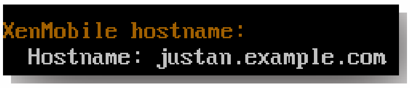
7. Provide the following information to configure the database connection:



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

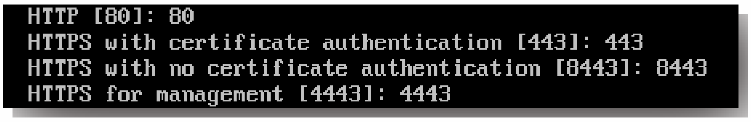
   1. Your database can be local or remote. Type l for local or r for remote.
   2. Select the database type. Type mi for Microsoft SQL or type p for PostgreSQL.
      Important:
      - Citrix recommends using Microsoft SQL remotely. PostgreSQL is included with XenMobile and should be used locally or remotely only in test environments.
      - Database migration is not supported. Databases created in a test environment cannot be moved to a production environment.
   3. Optionally, type y to use SSL authentication for your database.
   4. Provide the fully qualified domain name (FQDN) for the database server. This one host server provides both device management and app management services.
   5. Type your database port number if it is different from the default port number. The default port for Microsoft SQL is 1433 and the default port for PostgreSQL is 5432.
   6. Type your database administrator user name.
   7. Type your data base administrator password.
   8. Type the database name.
   9. Press Enter to commit the database settings.
8. Optionally, type y to enable clustering XenMobile nodes, or instances.
   Important: If you enable a XenMobile cluster, after system configuration is complete, be sure to open port 80 to enable real time communication between cluster members.
9. Type the XenMobile server fully qualified domain name (FQDN). The XenMobile server FQDN must be identical to the SSL Listener certificate common name.

   Note: The XenMobile server FQDN is the public DNS for XenMobile enrollment and cannot be changed after the installation.



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

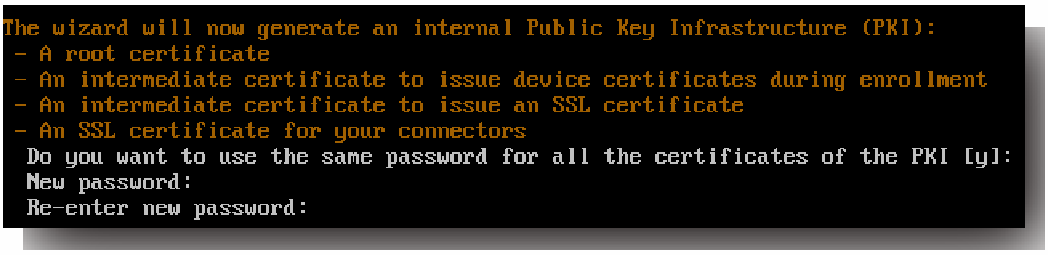
10. Press Enter to commit the settings.
11. Identify the communication ports. For details on ports and their uses, see XenMobile Port Requirements.
    Note: Accept the default ports by pressing Enter (Return on a Mac).



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

12. Skip the next question about upgrading from a previous XenMobile release because you are installing XenMobile for the first time.

13. Type y if you want to use the same password for each Public Key Infrastructure (PKI) certificate. For details on the XenMobile PKI feature, see Uploading Certificates in XenMobile.

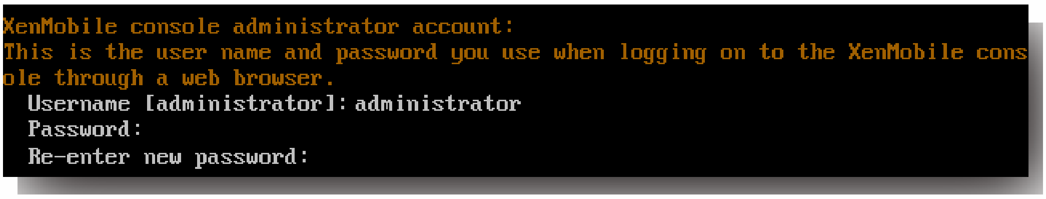


```
The wizard will now generate an internal Public Key Infrastructure (PKI):
 - A root certificate
 - An intermediate certificate to issue device certificates during enrollment
 - An intermediate certificate to issue an SSL certificate
 - An SSL certificate for your connectors
  Do you want to use the same password for all the certificates of the PKI [y]:
  New password:
  Re-enter new password:
```

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

14. Type the new password and then, re-enter the new password to confirm it.
Note: No characters, such as asterisks, are shown when you type the new password. Nothing appears.

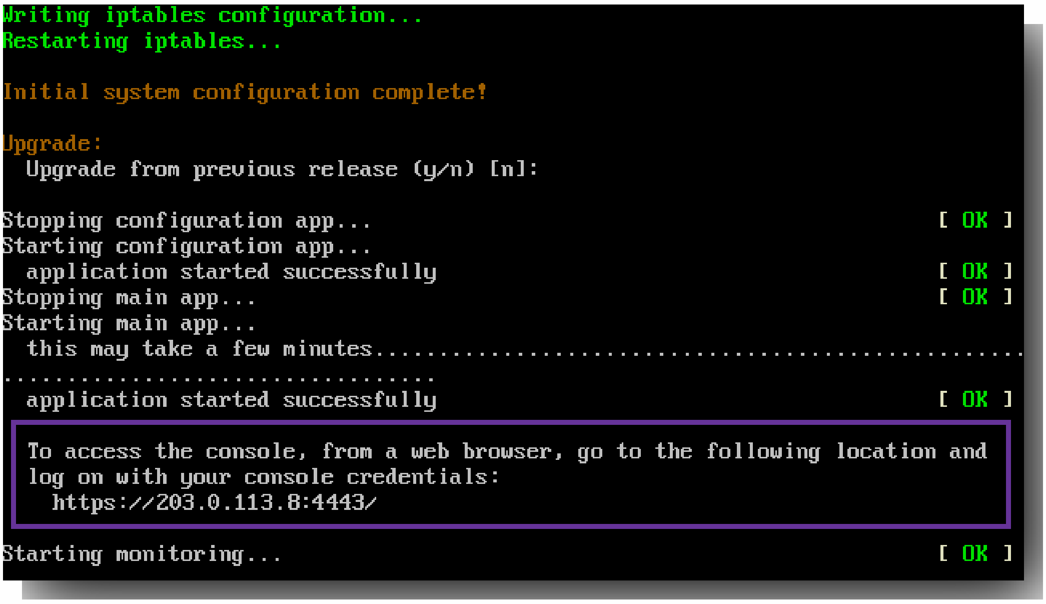
15. Press Enter to commit the settings.
16. Create an administrator account for logging on to the XenMobile console with a web browser. Be sure to remember these credentials for later use.



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

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

17. Press Enter to commit the settings. The initial system configuration is saved.
18. When asked if this is an upgrade, type n because it is a new installation.
19. Copy the complete URL that appears on the screen and continue this initial XenMobile configuration in your web browser.

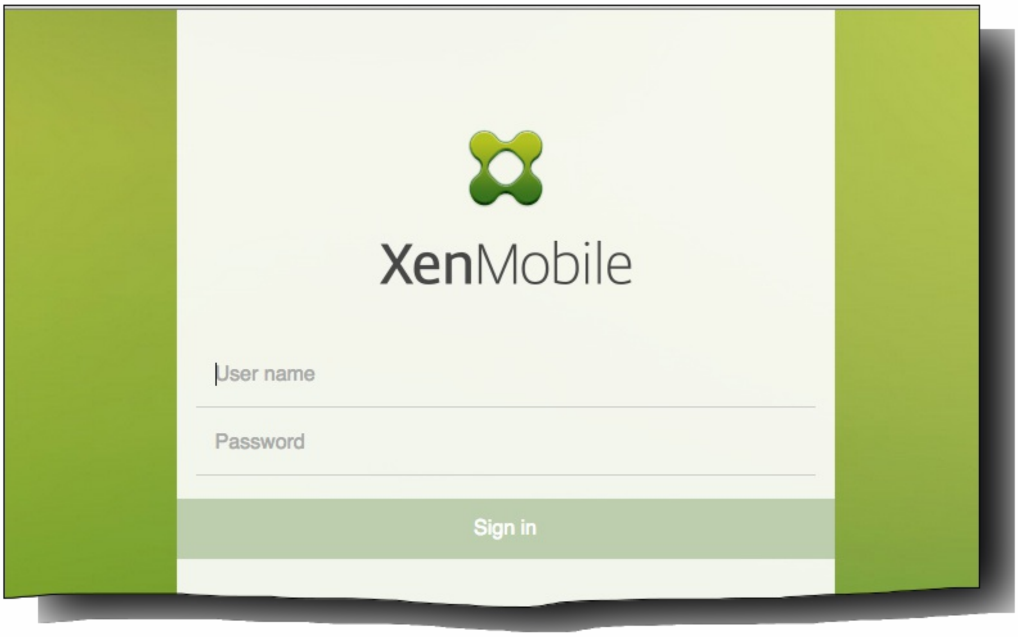


```
Writing iptables configuration...
Restarting iptables...

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

Configuring FIPS with XenMobile

Oct 27, 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.

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.

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

SQL Prerequisites

1. The connection to the SQL instance from XenMobile needs to be secure and must be SQL Server version 2012 or SQL Server 2014. To secure the connection, see How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console.

2. If the service does not restart properly, check the following:Open **Services.msc**.

a. Copy the logon account information used for the SQL Server service.

b. Open MMC.exe on the SQL Server.

c. Go to **File** > **Add/Remove Snap-in** and then double-click the certificates item to add the certificates snap-in. Select the computer account and local computer in the two pages on the wizard.

d. Click **OK**.

e. Expand **Certificates (Local Computer)** > **Personal** > **Certificates** and find the imported SSL certificate.

f. Right-click the imported certificate (selected in the SQL Server Configuration Manager) and then click **All Tasks** > **Manage Private Keys**.

g. Under **Group or User names**, click **Add**.

h. Enter the SQL service account name you copied in the earlier step.

i. Clear the **Allow Full Control** option. By default the service account will be given both Full control and Read permissions, but it only needs to be able to read the private key.

j. Close **MMC** and start the SQL service.

3. Ensure the SQL service is started correctly.

Internet Information Services (IIS) Prerequisites

1. Download the rootcert (base 64).

2. Copy the rootcert to the default site on the IIS server, C:\inetpub\wwwroot.

3. Check the **Authentication** check box for the default site.

4. Set **Anonymous** to **enabled**.

5. Select the **Failed Request Tracking** rules check box.

6. Ensure that .cer is not blocked.

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

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

a. Open Server Manager.

b. Navigate to the wizard in **Manage** > **Add Roles and Features**.

c. In the server roles, expand **Web Server (IIS)**, expand **Web Server**, expand **Application Development** and then select **ASP**.

d. Click **Next** until the install completes.

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

For more information, see Internet Information Services (IIS) 8.5.

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

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.

Upgrading XenMobile

Dec 22, 2016

When new versions of XenMobile software are available, you can upgrade to a new version. You have two options for upgrading depending on your scenario:

- To install new versions of XenMobile 10.1 software, service packs, and system patches, you use the Release Management page in the XenMobile console as described later in this article.
- To upgrade from XenMobile 9 to the latest version, you use the Upgrade Tool built into XenMobile 10.4 or later. For details, including known and fixed issues, see Upgrade.
- 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.

Note

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.

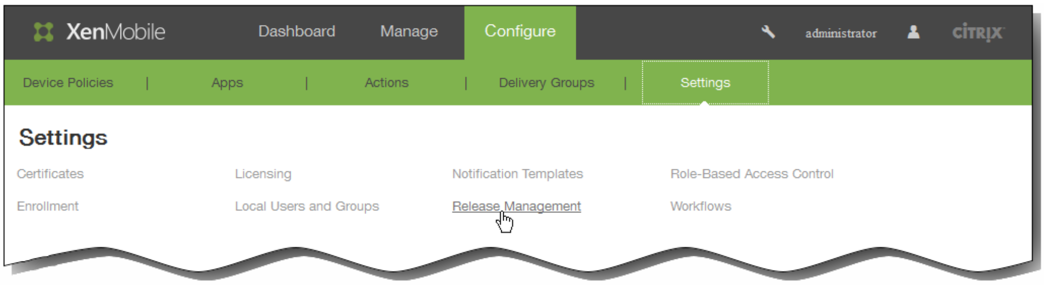
Important

- Be aware of this XenMobile 10.1 known issue, because it is likely that your XenMobile 9.0 host name may have an uppercase letter. In this case, after upgrading to XenMobile 10.1, devices cannot access the Worx Store. When you configure XenMobile server with an uppercase letter in the host name, such as ABC.Xms.com, the Worx Store does not open on devices after the devices enroll. [#545527]
- After upgrading to XenMobile 10.1, when you update Worx Mobile Apps in XenMobile 10.1 that you configured in an earlier release, the app settings no longer appear in the XenMobile console. You need to edit and configure the settings for these apps again. You do not need to reinstall the apps. You only need to do this step one time; the values will stay intact for future updates if you update the app or update the server.

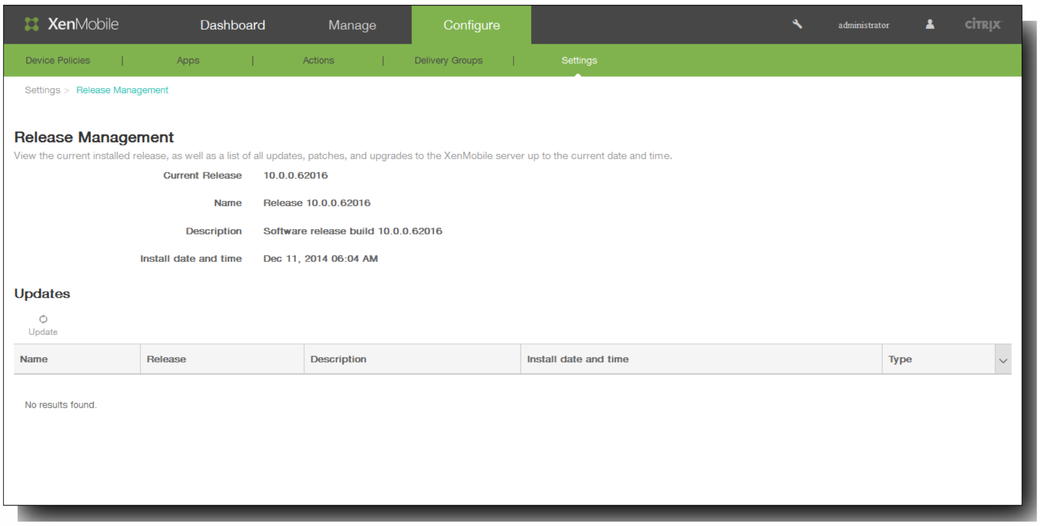
Prerequisites:

- Before you install a XenMobile update, use the facilities in your virtual machine (VM) to take a snapshot of your system.
- Back up your system configuration database.
- Review the system requirements.

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.



Release Management

View the current installed release, as well as a list of all updates, patches, and upgrades to the XenMobile server up to the current date and time.

Current Release 10.0.0.62016

Name Release 10.0.0.62016

Description Software release build 10.0.0.62016

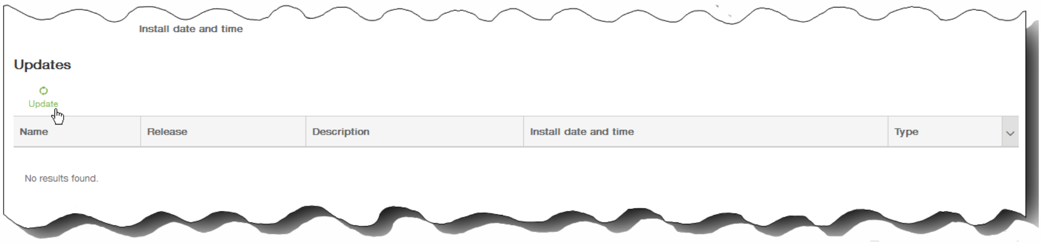
Install date and time Dec 11, 2014 06:04 AM

Updates

Name	Release	Description	Install date and time	Type

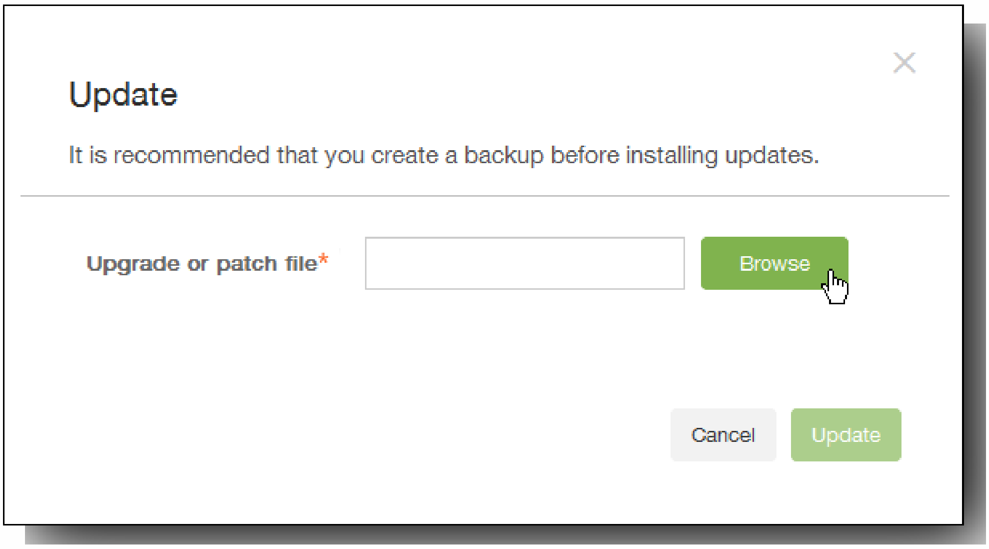
No results found.

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



Name	Release	Description	Install date and time	Type

No results found.



Update

It is recommended that you create a backup before installing updates.

Upgrade or patch file*

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.

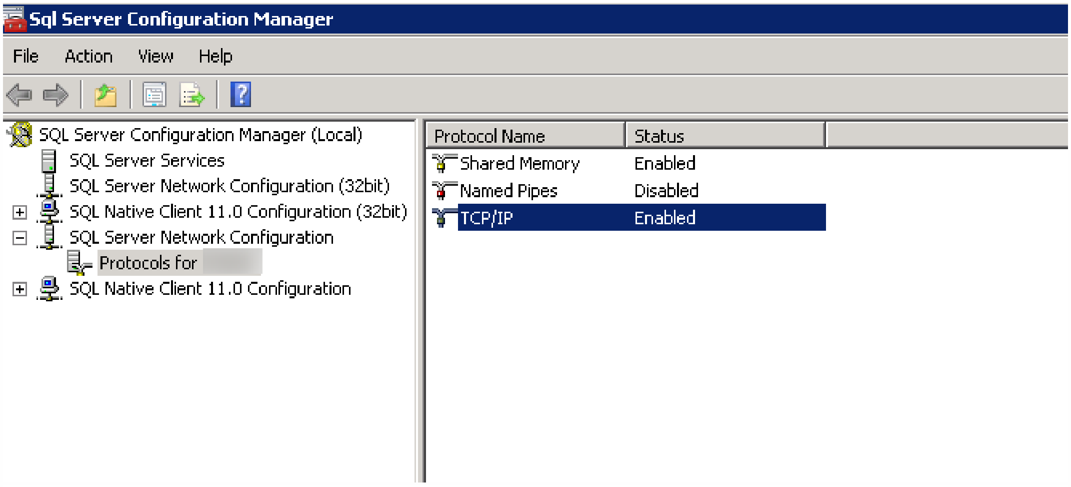
Supporting Named SQL Instances

Feb 11, 2016

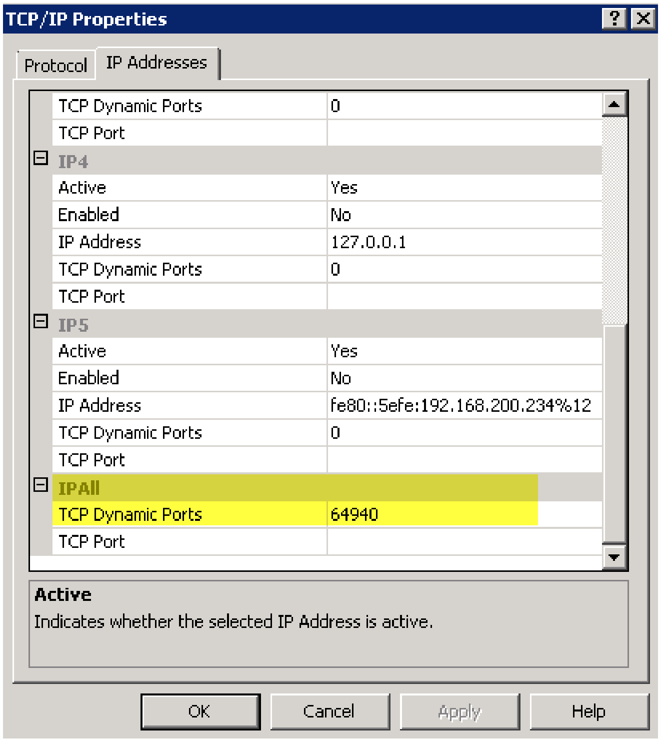
You can use the Upgrade Tool to upgrade from XenMobile 9 to XenMobile 10 and from XenMobile 9 to XenMobile 10.1. If your XenMobile 9 setup is based on named SQL instances, you need to follow steps specific to this situation. If your XenMobile 9 environment meets the following prerequisites, follow the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


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 11.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for [redacted]
SQL Native Client 11.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled

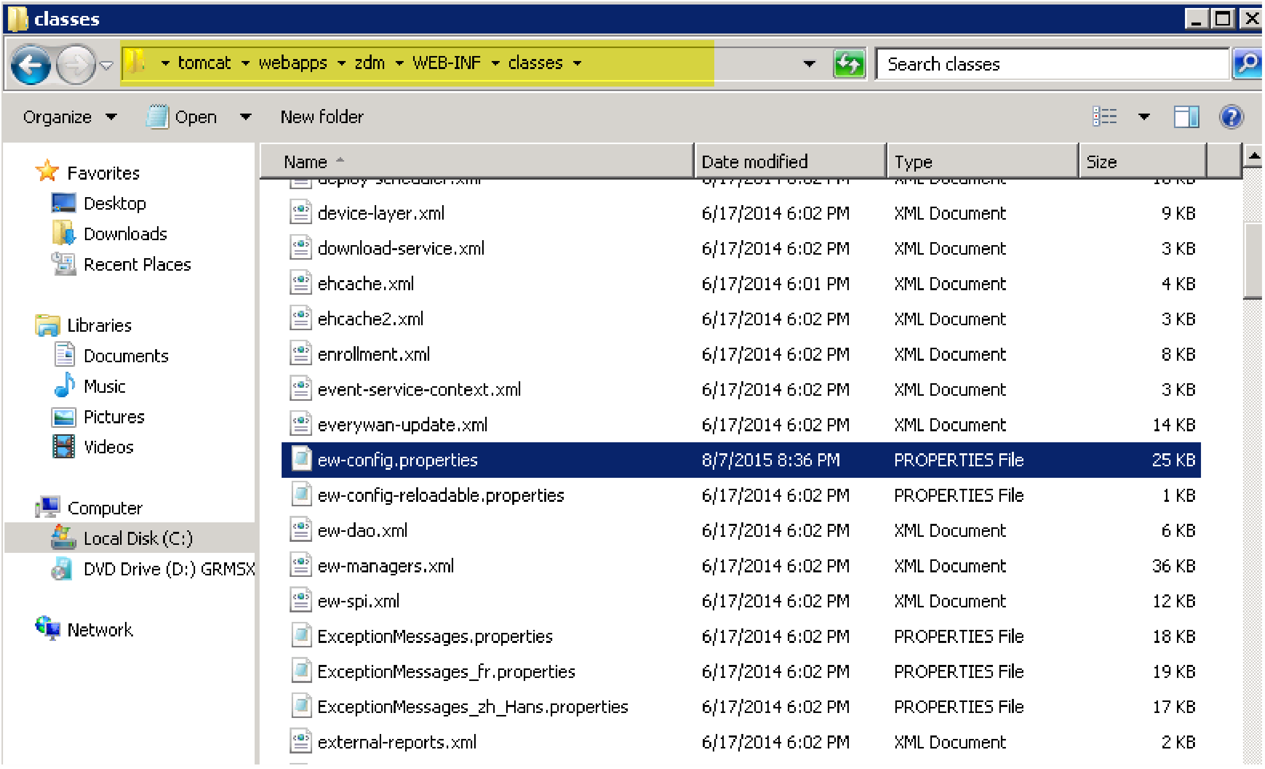


TCP/IP Properties

TCP Dynamic Ports	0
TCP Port	
IP4	
Active	Yes
Enabled	No
IP Address	127.0.0.1
TCP Dynamic Ports	0
TCP Port	
IP5	
Active	Yes
Enabled	No
IP Address	fe80::5efe:192.168.200.234%12
TCP Dynamic Ports	0
TCP Port	
IPAll	
TCP Dynamic Ports	64940
TCP Port	

Active
Indicates whether the selected IP Address is active.

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



classes

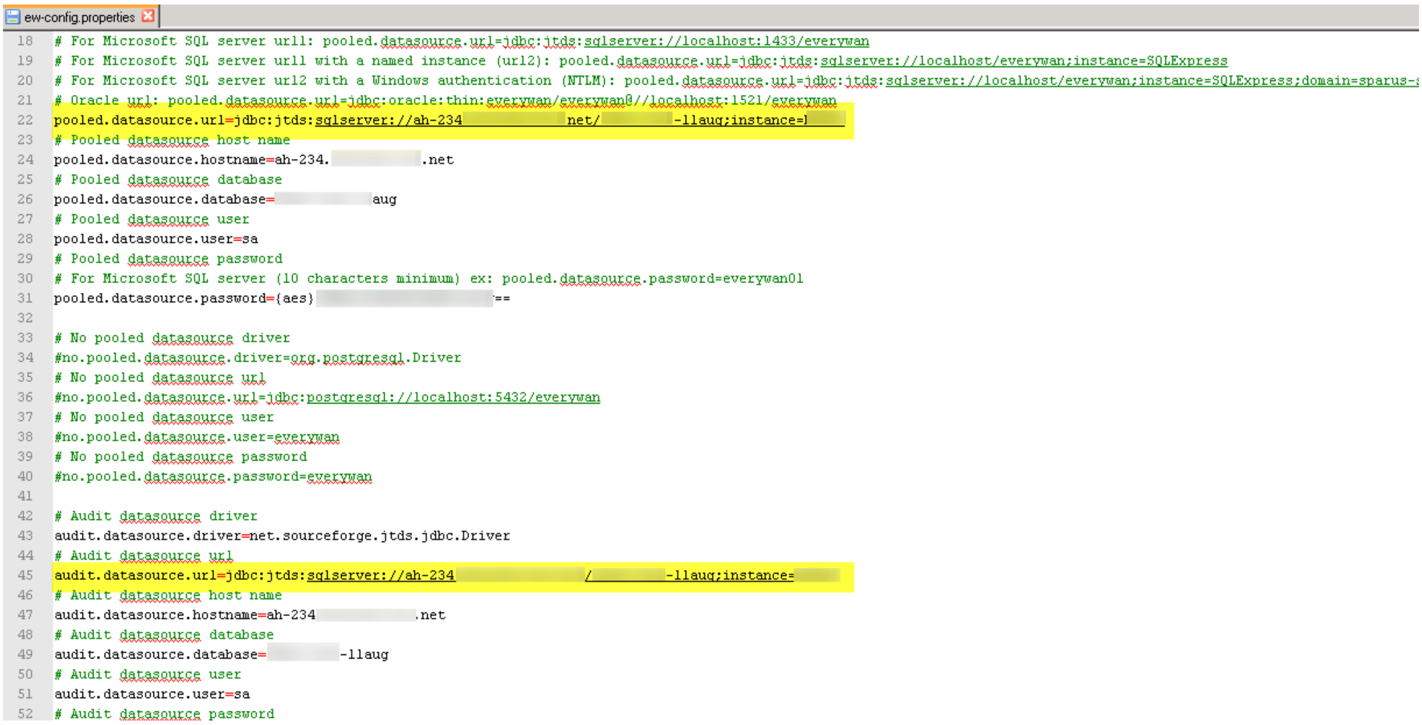
tomcat ▸ webapps ▸ zdm ▸ WEB-INF ▸ classes

Name	Date modified	Type	Size
device-layer.xml	6/17/2014 6:02 PM	XML Document	9 KB
download-service.xml	6/17/2014 6:02 PM	XML Document	3 KB
ehcache.xml	6/17/2014 6:01 PM	XML Document	4 KB
ehcache2.xml	6/17/2014 6:02 PM	XML Document	3 KB
enrollment.xml	6/17/2014 6:02 PM	XML Document	8 KB
event-service-context.xml	6/17/2014 6:02 PM	XML Document	3 KB
everywan-update.xml	6/17/2014 6:02 PM	XML Document	14 KB
ew-config.properties	8/7/2015 8:36 PM	PROPERTIES File	25 KB
ew-config-reloadable.properties	6/17/2014 6:02 PM	PROPERTIES File	1 KB
ew-dao.xml	6/17/2014 6:02 PM	XML Document	6 KB
ew-managers.xml	6/17/2014 6:02 PM	XML Document	36 KB
ew-spi.xml	6/17/2014 6:02 PM	XML Document	12 KB
ExceptionMessages.properties	6/17/2014 6:02 PM	PROPERTIES File	18 KB
ExceptionMessages_fr.properties	6/17/2014 6:02 PM	PROPERTIES File	19 KB
ExceptionMessages_zh_Hans.properties	6/17/2014 6:02 PM	PROPERTIES File	17 KB
external-reports.xml	6/17/2014 6:02 PM	XML Document	2 KB

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

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

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



ew-config.properties

```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234[redacted]net/[redacted]-llaug;instance=l[redacted]
# Pooled datasource host name
pooled.datasource.hostname=ah-234.[redacted].net
# Pooled datasource database
pooled.datasource.database=[redacted]aug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}[redacted]==

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

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://ah-234[redacted]/[redacted]-llaug;instance=[redacted]
# Audit datasource host name
audit.datasource.hostname=ah-234[redacted].net
# Audit datasource database
audit.datasource.database=[redacted]-llaug
# Audit datasource user
audit.datasource.user=sa
# Audit datasource password
```

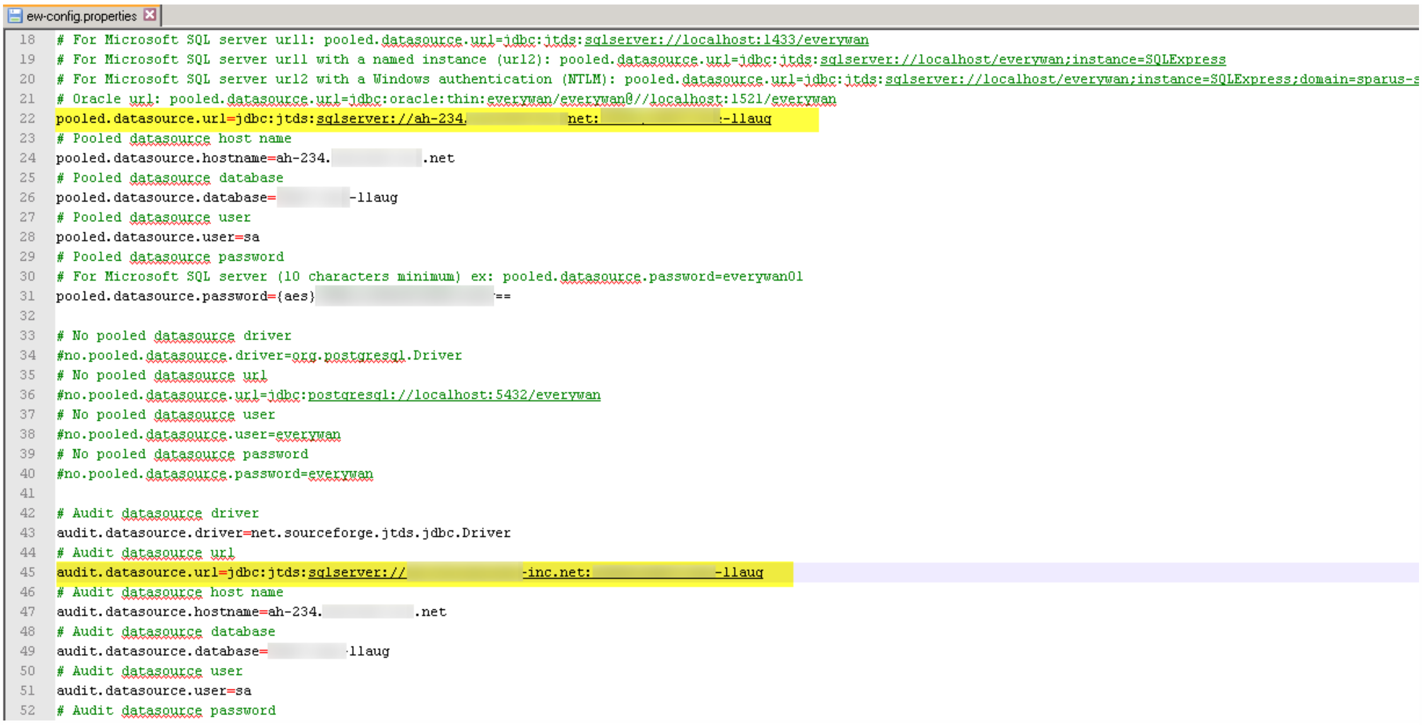
3. Remove the instance name in the preceding URLs and add the port along with the SQL Server FQDN. In this case, 64940 is the required port.

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

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

Add ";domain=<DomainSuffix>" to the end of URL if the user account belongs to a domain.

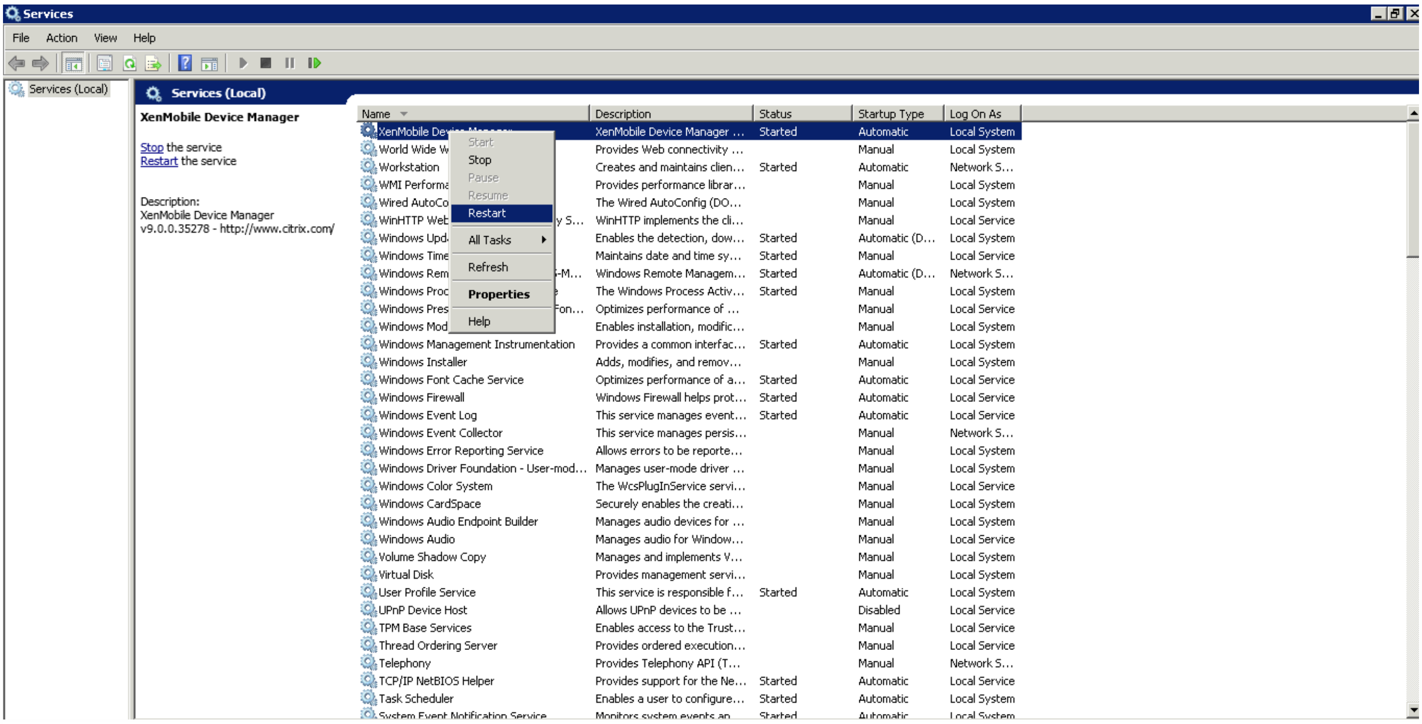
> ## Note
>
> Citrix recommends that you make a backup, copy, or note of the changes you make in the ew-config.properties file. This information is helpful in case the migration fails.



ew-config.properties

```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-s
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234.[redacted]net:[redacted]-llaug
# Pooled datasource host name
pooled.datasource.hostname=ah-234.[redacted].net
# Pooled datasource database
pooled.datasource.database=[redacted]-llaug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}[redacted]==

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

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://[redacted]-inc.net:[redacted]-llaug
# Audit datasource host name
audit.datasource.hostname=ah-234.[redacted].net
# Audit datasource database
audit.datasource.database=[redacted]llaug
# Audit datasource user
audit.datasource.user=sa
# Audit datasource password
```

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



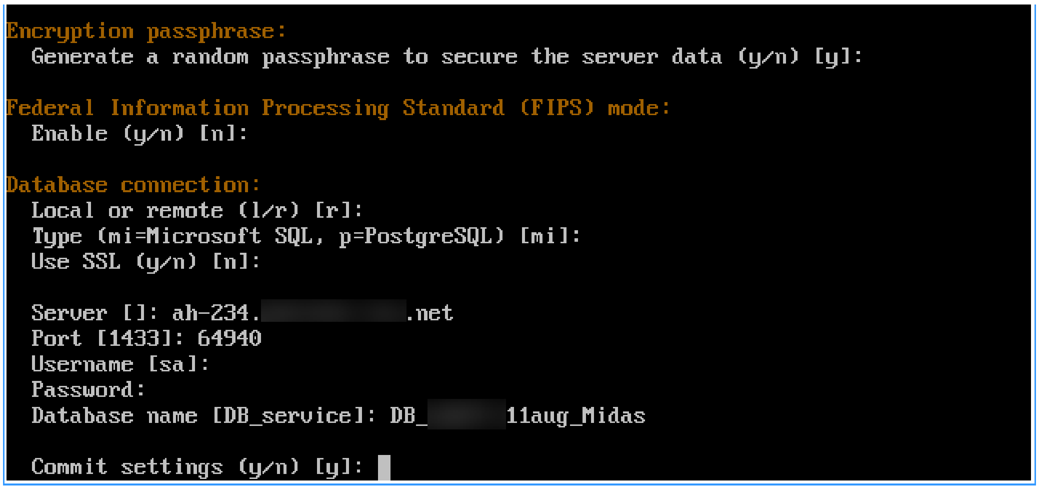
XenMobile Device Manager

Stop the service
Restart the service

Description:
XenMobile Device Manager
v9.0.0.35278 - http://www.citrix.com/

Name	Description	Status	Startup Type	Log On As
XenMobile Dev	XenMobile Device Manager …	Started	Automatic	Local System
World Wide W	Provides Web connectivity …		Manual	Local System
Workstation	Creates and maintains clien…	Started	Automatic	Network S…
WMI Performa	Provides performance librar…		Manual	Local System
Wired AutoCo	The Wired AutoConfig (DO…		Manual	Local System
WinHTTP Web y S…	WinHTTP implements the cli…		Manual	Local Service
Windows Upd	Enables the detection, dow…	Started	Automatic (D…	Local System
Windows Time	Maintains date and time sy…	Started	Manual	Local Service
Windows Rem -M…	Windows Remote Managem…	Started	Automatic (D…	Network S…
Windows Proc e	The Windows Process Activ…	Started	Manual	Local System
Windows Pres Fon…	Optimizes performance of …		Manual	Local Service
Windows Mod	Enables installation, modific…		Manual	Local System
Windows Management Instrumentation	Provides a common interfac…	Started	Automatic	Local System
Windows Installer	Adds, modifies, and remov…		Manual	Local System
Windows Font Cache Service	Optimizes performance of a…	Started	Automatic	Local Service
Windows Firewall	Windows Firewall helps prot…	Started	Automatic	Local Service
Windows Event Log	This service manages event…	Started	Automatic	Local Service
Windows Event Collector	This service manages persis…		Manual	Network S…
Windows Error Reporting Service	Allows errors to be reporte…		Manual	Local System
Windows Driver Foundation - User-mod…	Manages user-mode driver …		Manual	Local System
Windows Color System	The WcsPlugInService servi…		Manual	Local Service
Windows CardSpace	Securely enables the creati…		Manual	Local System
Windows Audio Endpoint Builder	Manages audio devices for …		Manual	Local System
Windows Audio	Manages audio for Window…		Manual	Local Service
Volume Shadow Copy	Manages and implements V…		Manual	Local System
Virtual Disk	Provides management servi…		Manual	Local System
User Profile Service	This service is responsible f…	Started	Automatic	Local System
UPnP Device Host	Allows UPnP devices to be …		Disabled	Local Service
TPM Base Services	Enables access to the Trust…		Manual	Local Service
Thread Ordering Server	Provides ordered execution…		Manual	Local Service
Telephony	Provides Telephony API (T…		Manual	Network S…
TCP/IP NetBIOS Helper	Provides support for the Ne…	Started	Automatic	Local Service
Task Scheduler	Enables a user to configure…	Started	Automatic	Local System
System Event Notification Service	Monitors system events an	Started	Automatic	Local System

5. Determine if the new XenMobile 10 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.[redacted].net
  Port [1433]: 64940
  Username [sa]:
  Password:
  Database name [DB_service]: DB_[redacted]11aug_Midas

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

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

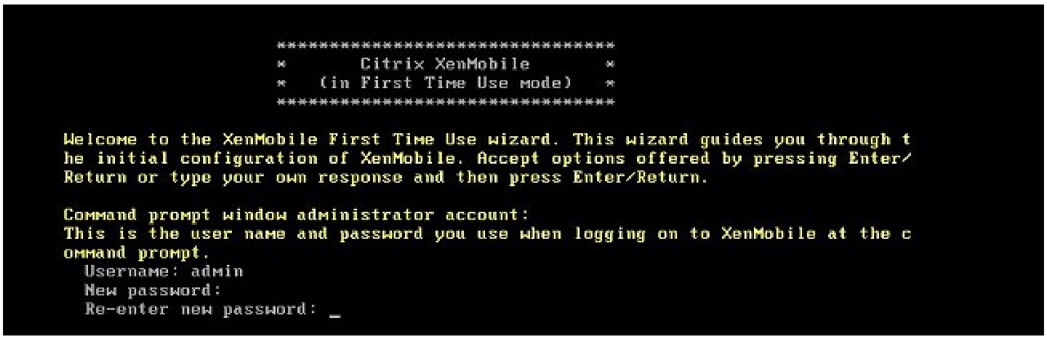
- To upgrade from XenMobile 9.0 App Edition or Enterprise Edition to XenMobile 10.1, you use the XenMobile Server App Edition and Enterprise Edition Upgrade Tool. For details, see Enabling and Running the XenMobile 10.1 Upgrade Tool.
- To upgrade from XenMobile 9.0 MDM edition only to XenMobile 10.1,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

-

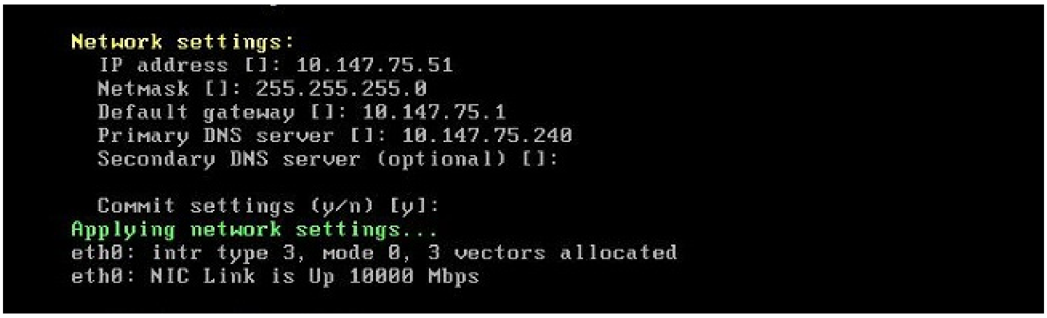
-

-
-
-
-

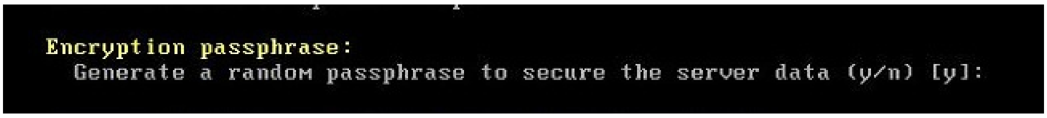
Installing the XenMobile Cluster Nodes



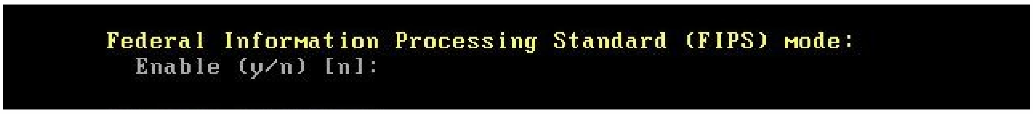
```
                    **********************************
                    *        Citrix XenMobile        *
                    *    (in First Time Use mode)    *
                    **********************************

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

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



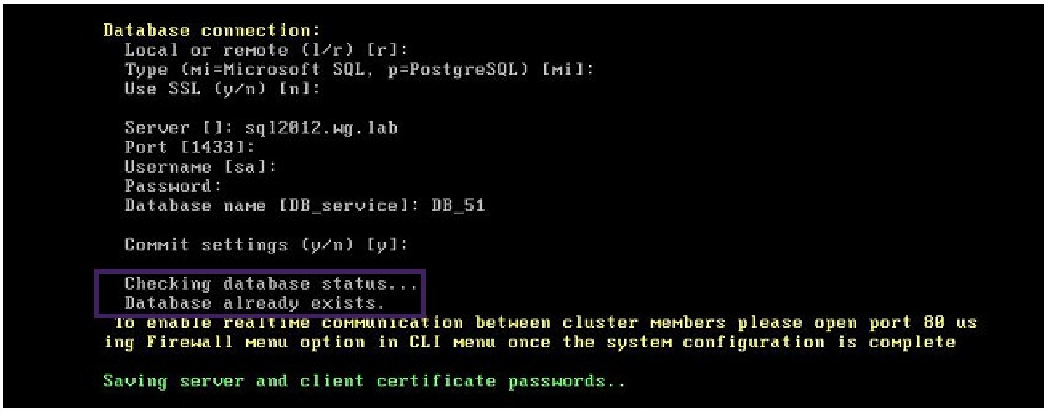
```
Network settings:
  IP address []: 10.147.75.51
  Netmask []: 255.255.255.0
  Default gateway []: 10.147.75.1
  Primary DNS server []: 10.147.75.240
  Secondary DNS server (optional) []:

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



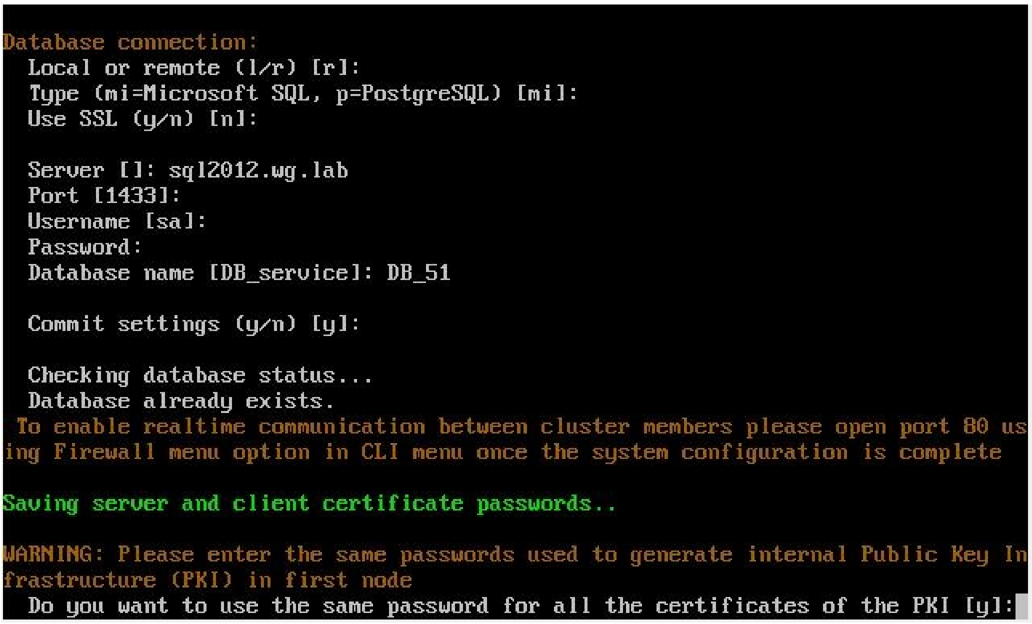
```
Encryption passphrase:
  Generate a random passphrase to secure the server data (y/n) [y]:
```



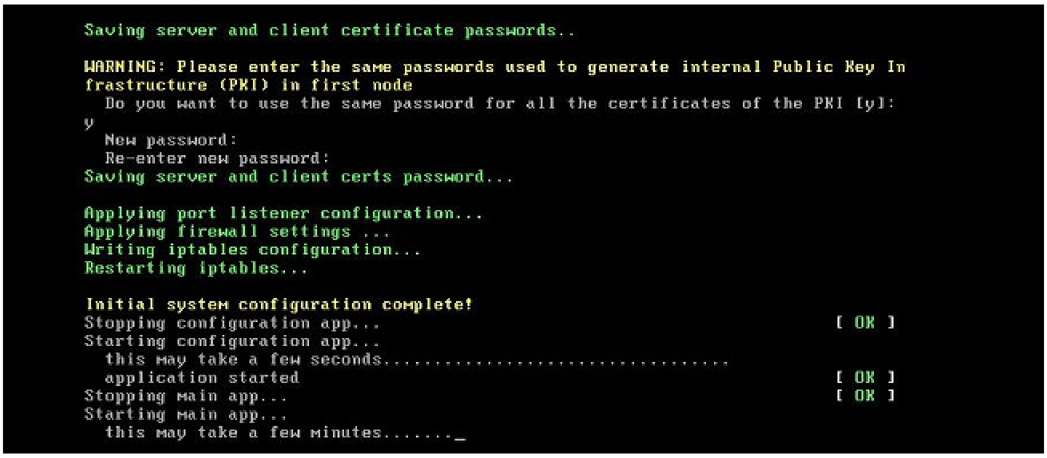
```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```



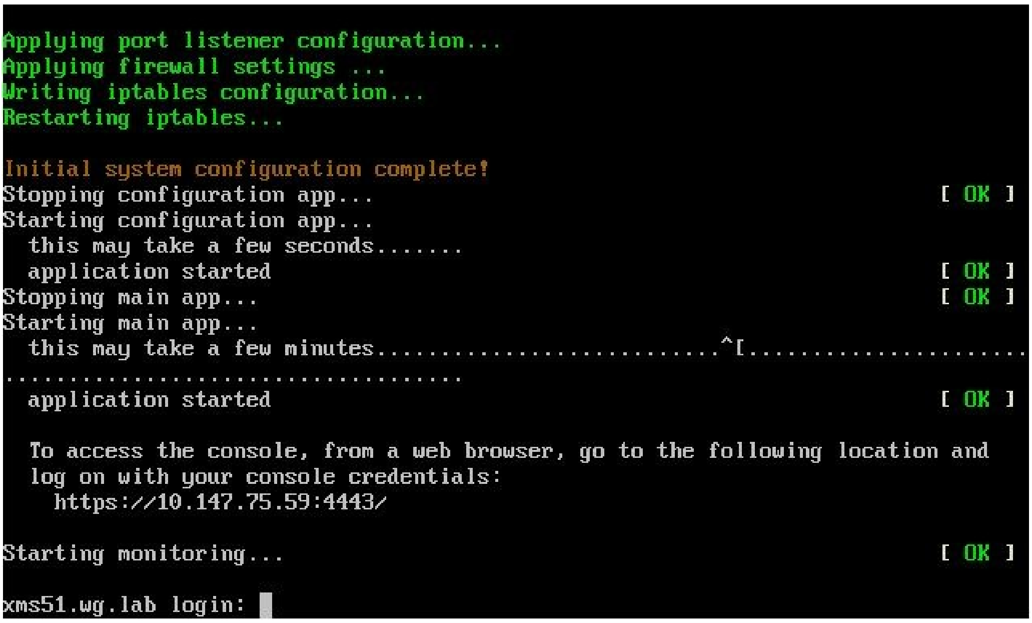
```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

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

  Commit settings (y/n) [y]:

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

Saving server and client certificate passwords..
```



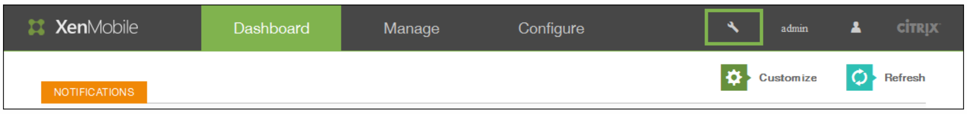
```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

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

  Commit settings (y/n) [y]:

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

Saving server and client certificate passwords..

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

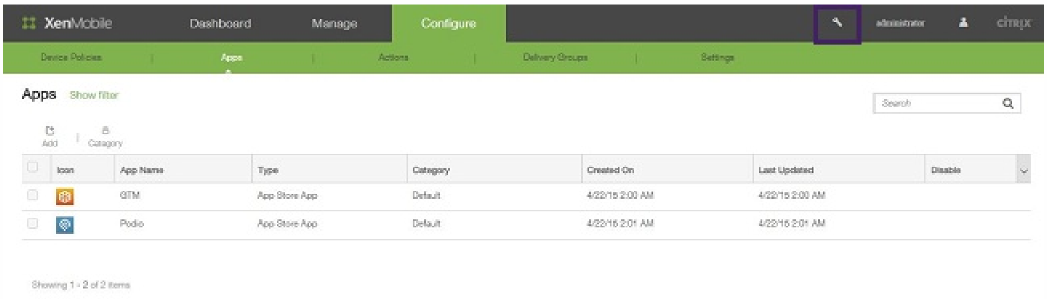


```
Saving server and client certificate passwords..

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

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

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



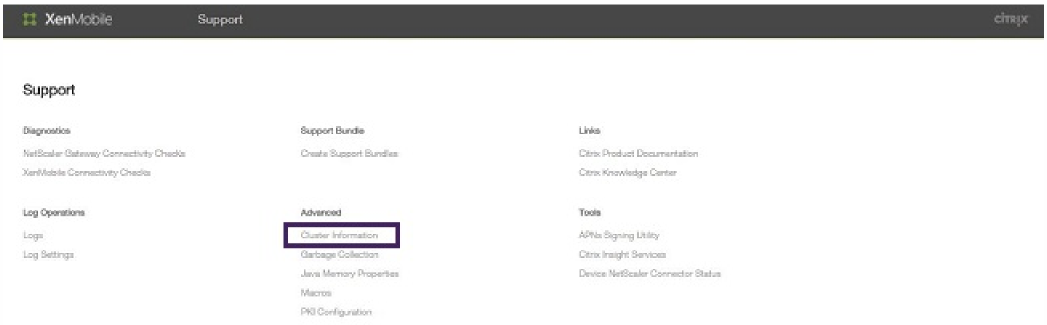
```
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

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: 
```





□	Icon	App Name	Type	Category	Created On	Last Updated	Disable
□		GTM	App Store App	Default	4/22/15 2:00 AM	4/22/15 2:00 AM	
□		Podio	App Store App	Default	4/22/16 2:01 AM	4/22/16 2:01 AM	

Showing 1 - 2 of 2 items



Support

Diagnostics
NetScaler Gateway Connectivity Checks
XenMobile Connectivity Checks

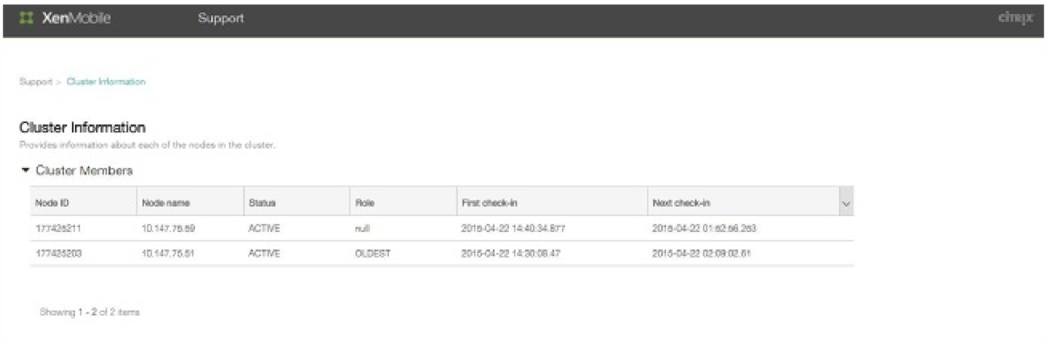
Support Bundle
Create Support Bundles

Links
Citrix Product Documentation
Citrix Knowledge Center

Log Operations
Logs
Log Settings

Advanced
Cluster Information
Garbage Collection
Java Memory Properties
Macros
PKI Configuration

Tools
APNs Signing Utility
Citrix Insight Services
Device NetScaler Connector Status



Support > Cluster Information

Cluster Information

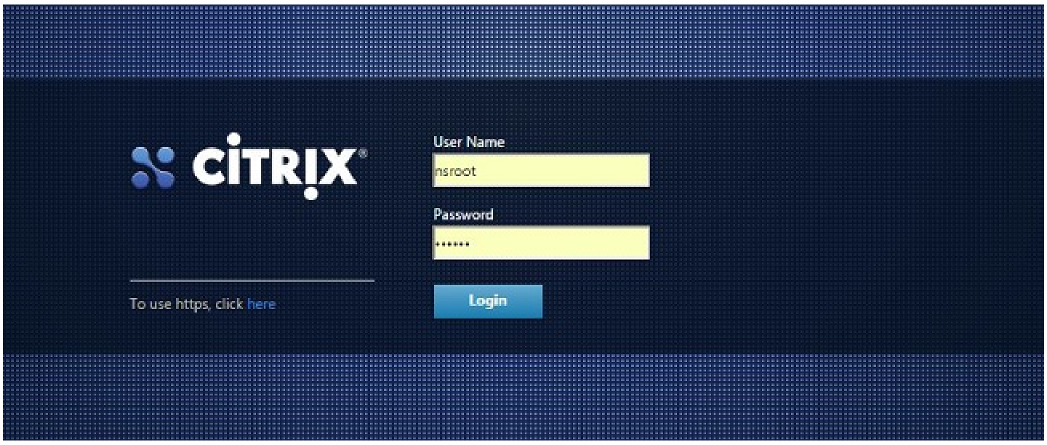
Provides information about each of the nodes in the cluster.

▾ Cluster Members

Node ID	Node name	Status	Role	First check-in	Next check-in
177426211	10.147.75.59	ACTIVE	null	2016-04-22 14:40:34.877	2016-04-22 01:52:56.263
177426203	10.147.75.51	ACTIVE	OLDEST	2016-04-22 14:30:08.47	2016-04-22 02:09:02.61

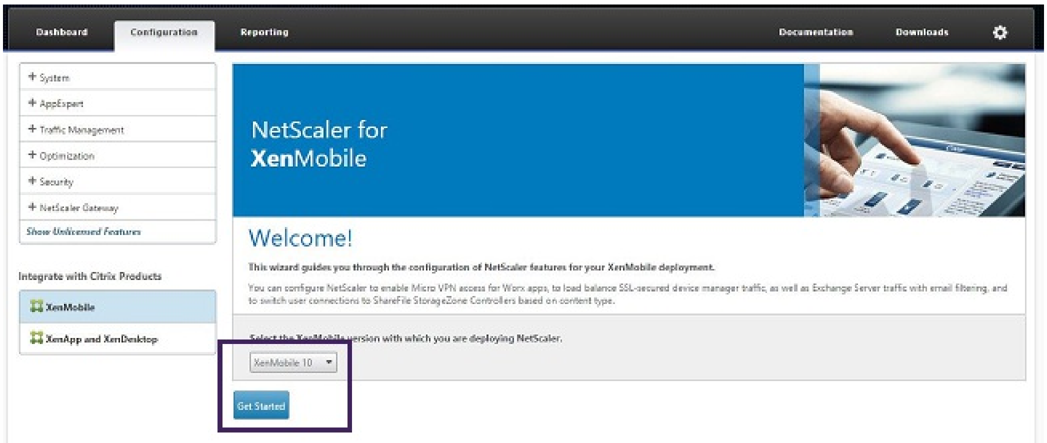
Showing 1 - 2 of 2 items

To configure load balancing for the XenMobile cluster in NetScaler



User Name: nsroot

Password: ••••••



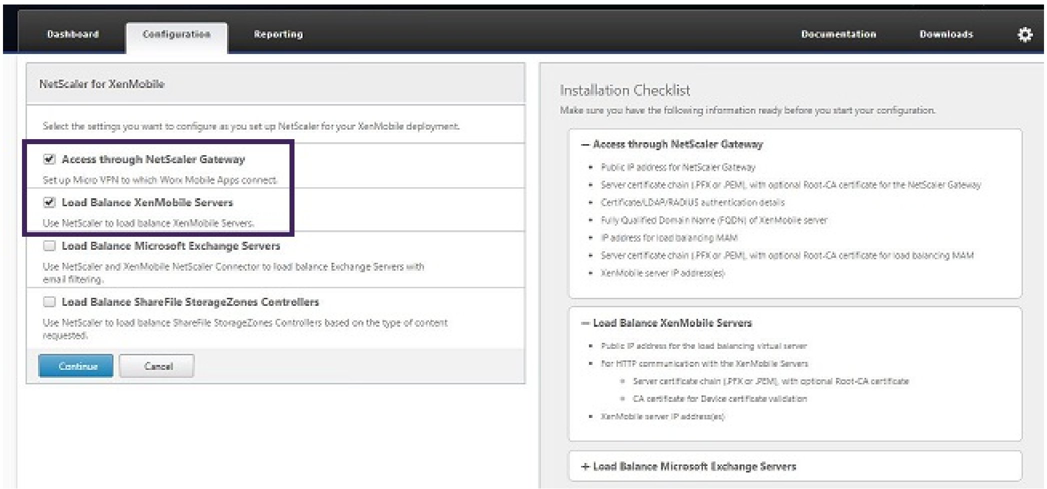
Welcome!

This wizard guides you through the configuration of NetScaler features for your XenMobile deployment.

You can configure NetScaler to enable Micro VPN access for Worx apps, to load balance SSL-secured device manager traffic, as well as Exchange Server traffic with email filtering, and to switch user connections to ShareFile StorageZone Controllers based on content type.

Select the XenMobile version with which you are deploying NetScaler.

XenMobile 10



NetScaler for XenMobile

Select the settings you want to configure as you set up NetScaler for your XenMobile deployment.

☑ **Access through NetScaler Gateway**

Set up Micro VPN to which Worx Mobile Apps connect.

☑ **Load Balance XenMobile Servers**

Use NetScaler to load balance XenMobile Servers.

□ **Load Balance Microsoft Exchange Servers**

Use NetScaler and XenMobile NetScaler Connector to load balance Exchange Servers with email filtering.

□ **Load Balance ShareFile StorageZones Controllers**

Use NetScaler to load balance ShareFile StorageZones Controllers based on the type of content requested.

Installation Checklist

Make sure you have the following information ready before you start your configuration.

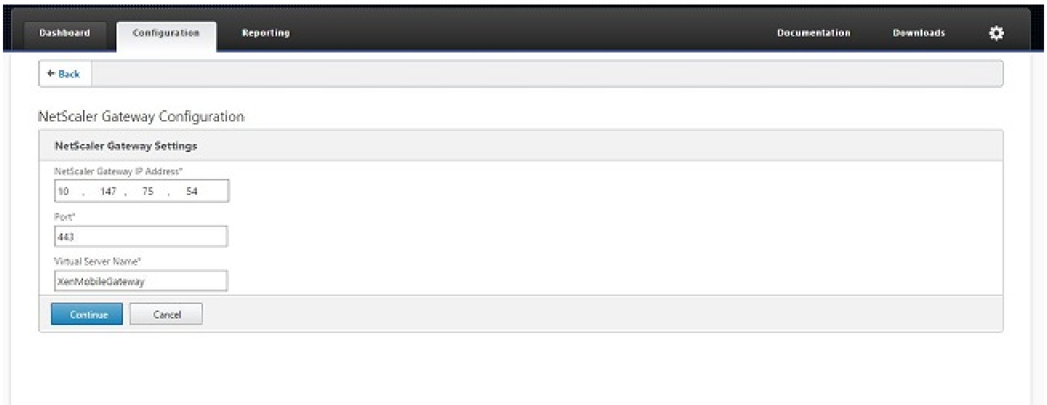
— Access through NetScaler Gateway

- Public IP address for NetScaler Gateway
- Server certificate chain (.PFX or .PEM), with optional Root-CA certificate for the NetScaler Gateway
- Certificate/LDAP/RADIUS authentication details
- Fully Qualified Domain Name (FQDN) of XenMobile server
- IP address for load balancing MAM
- Server certificate chain (.PFX or .PEM), with optional Root-CA certificate for load balancing MAM
- XenMobile server IP address(es)

— Load Balance XenMobile Servers

- Public IP address for the load balancing virtual server
- For HTTP communication with the XenMobile Servers
  - Server certificate chain (.PFX or .PEM), with optional Root-CA certificate
  - CA certificate for Device certificate validation
- XenMobile server IP address(es)

+ Load Balance Microsoft Exchange Servers



NetScaler Gateway Configuration

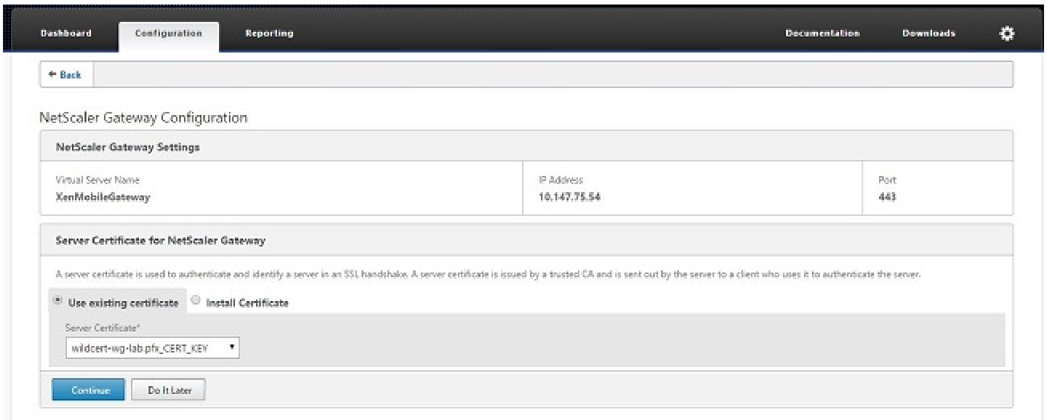
NetScaler Gateway Settings

NetScaler Gateway IP Address*: 10 . 147 . 75 . 54

Port*: 443

Virtual Server Name*: XenMobileGateway

-
-



NetScaler Gateway Configuration

NetScaler Gateway Settings

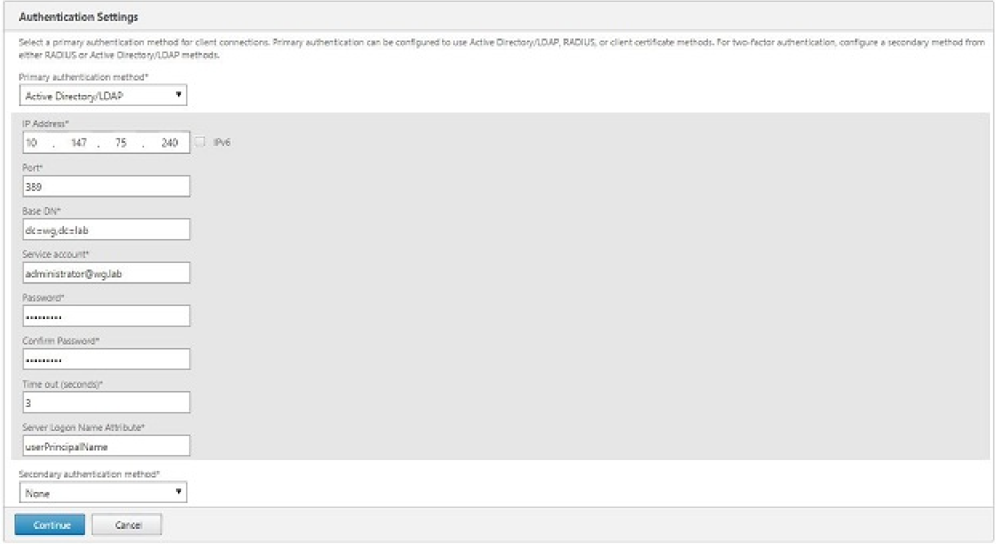
Virtual Server Name	IP Address	Port
XenMobileGateway	10.147.75.54	443

Server Certificate for NetScaler Gateway

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

● Use existing certificate ○ Install Certificate

Server Certificate*: wildcert-wg-lab.pfx_CERT_KEY



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

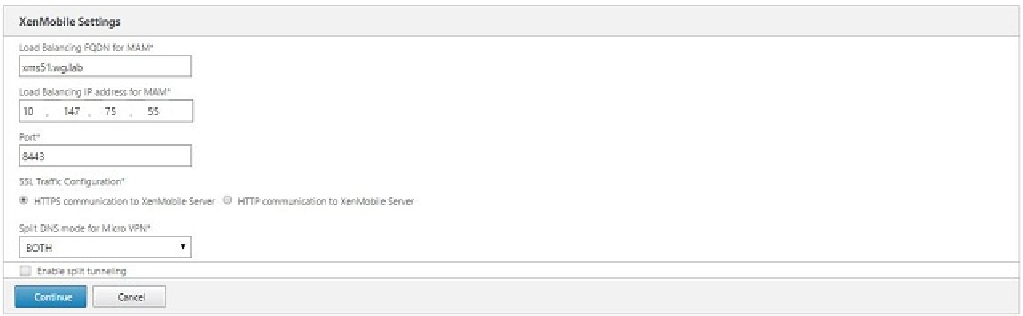
Password*: •••••••••

Confirm Password*: •••••••••

Time out (seconds)*: 3

Server Logon Name Attribute*: userPrincipalName

Secondary authentication method*: None



XenMobile Settings

Load Balancing FQDN for MAM*: xms51.wg.lab

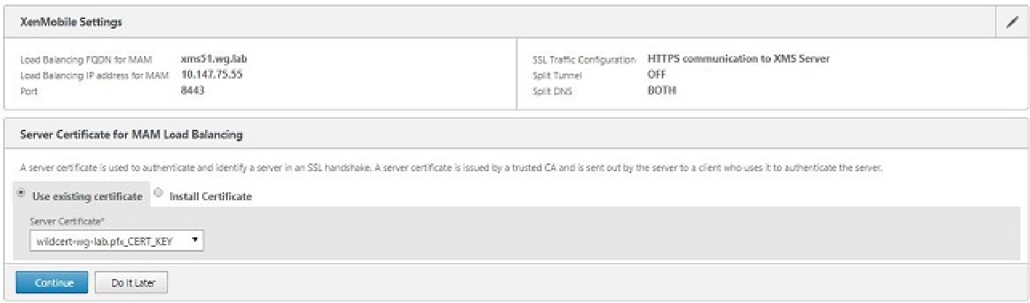
Load Balancing IP address for MAM*: 10 . 147 . 75 . 55

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



XenMobile Settings

Load Balancing FQDN for MAM: xms51.wg.lab
Load Balancing IP address for MAM: 10.147.75.55
Port: 8443

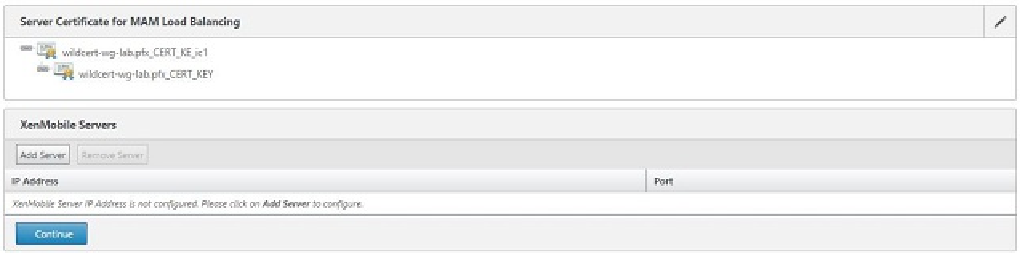
SSL Traffic Configuration: HTTPS communication to XMS Server
Split Tunnel: OFF
Split DNS: BOTH

Server Certificate for MAM Load Balancing

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

● Use existing certificate ○ Install Certificate

Server Certificate*: wildcert-wg-lab.pfx_CERT_KEY



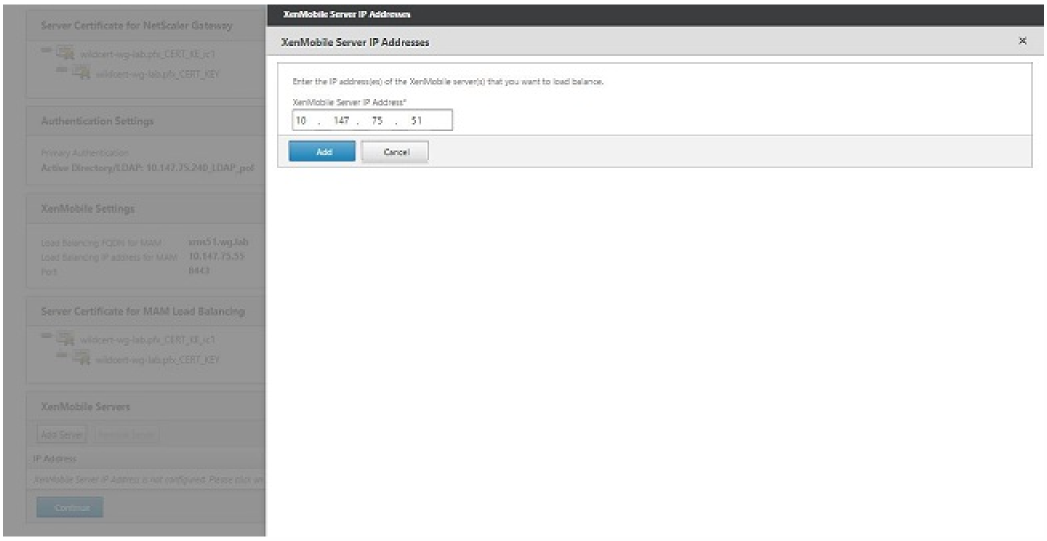
Server Certificate for MAM Load Balancing

wildcert-wg-lab.pfx_CERT_KE_ic1

wildcert-wg-lab.pfx_CERT_KEY

XenMobile Servers

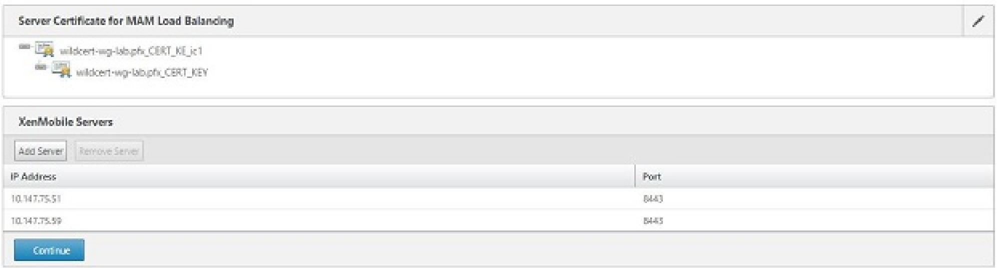
IP Address	Port
*XenMobile Server IP Address is not configured. Please click on **Add Server** to configure.*	



XenMobile Server IP Addresses

Enter the IP address(es) of the XenMobile server(s) that you want to load balance.

XenMobile Server IP Address*: 10 . 147 . 75 . 51



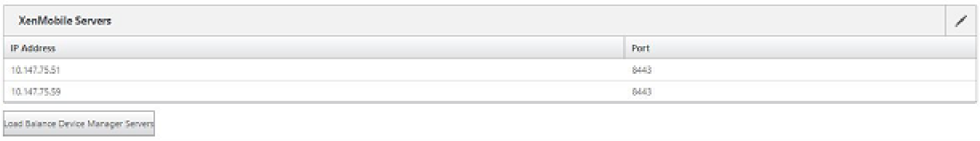
Server Certificate for MAM Load Balancing

wildcert-wg-lab.pfx_CERT_KE_ic1

wildcert-wg-lab.pfx_CERT_KEY

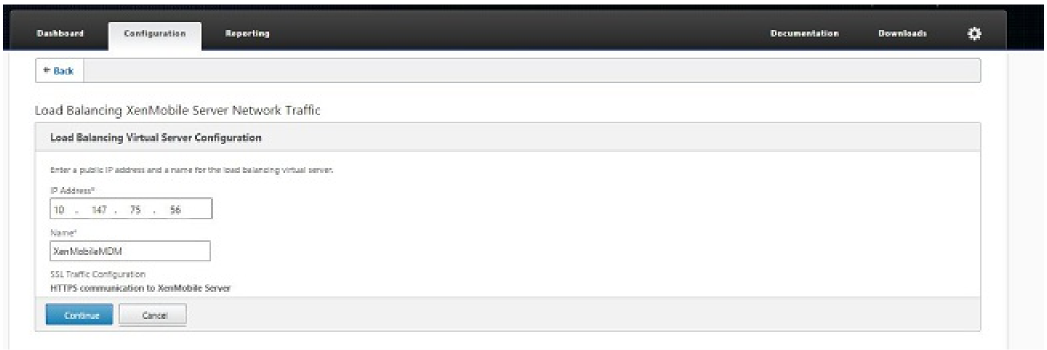
XenMobile Servers

IP Address	Port
10.147.75.51	8443
10.147.75.59	8443



XenMobile Servers

IP Address	Port
10.147.75.51	8443
10.147.75.59	8443



Load Balancing XenMobile Server Network Traffic

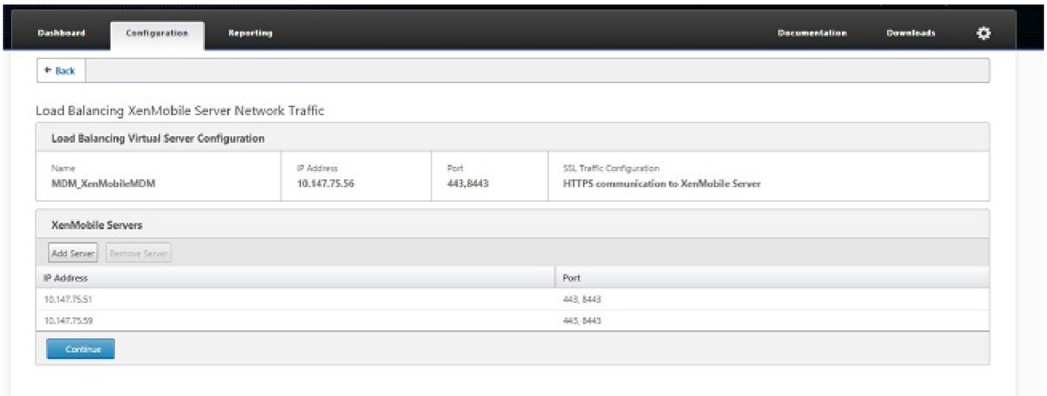
Load Balancing Virtual Server Configuration

Enter a public IP address and a name for the load balancing virtual server.

IP Address*: 10 . 147 . 75 . 56

Name*: XenMobileMDM

SSL Traffic Configuration: HTTPS communication to XenMobile Server



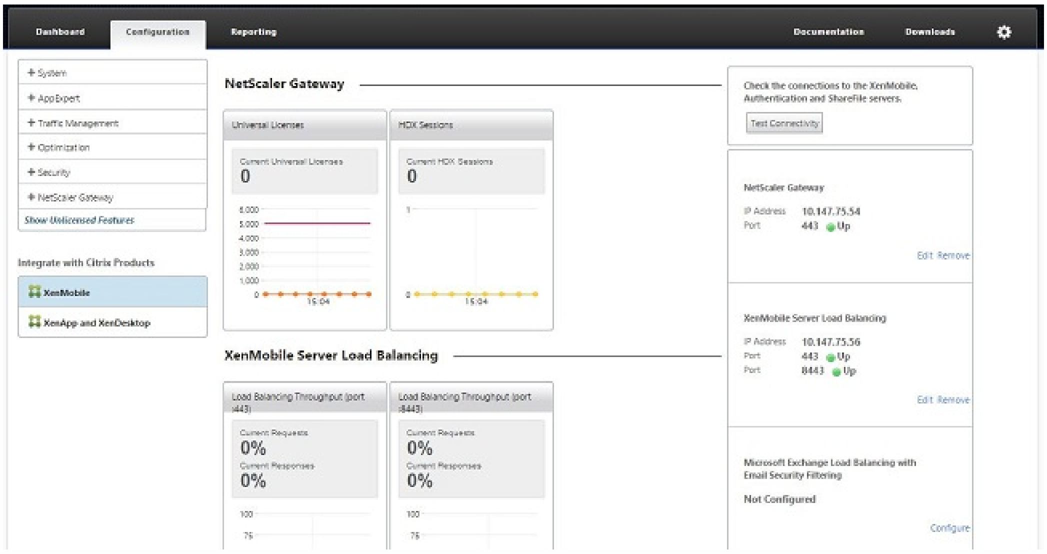
Load Balancing XenMobile Server Network Traffic

Load Balancing Virtual Server Configuration

Name	IP Address	Port	SSL Traffic Configuration
MDM_XenMobileMDM	10.147.75.56	443,8443	HTTPS communication to XenMobile Server

XenMobile Servers

IP Address	Port
10.147.75.51	443, 8443
10.147.75.59	443, 8443



NetScaler Gateway

Universal Licenses — Current Universal Licenses: 0

HDX Sessions — Current HDX Sessions: 0

XenMobile Server Load Balancing

Load Balancing Throughput (port :443) — Current Requests: 0% — Current Responses: 0%

Load Balancing Throughput (port :8443) — Current Requests: 0% — Current Responses: 0%

Check the connections to the XenMobile, Authentication and ShareFile servers.

NetScaler Gateway

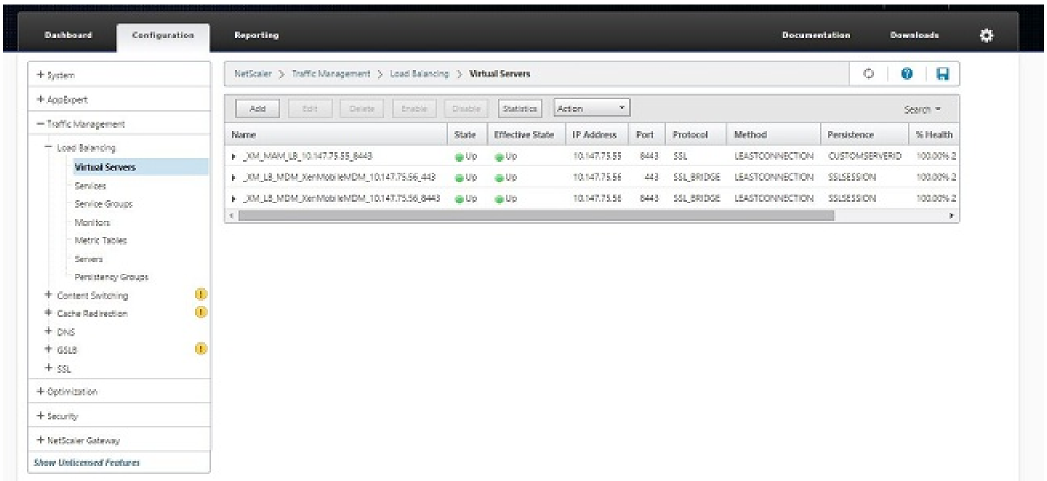
IP Address 10.147.75.54
Port 443 ● Up

XenMobile Server Load Balancing

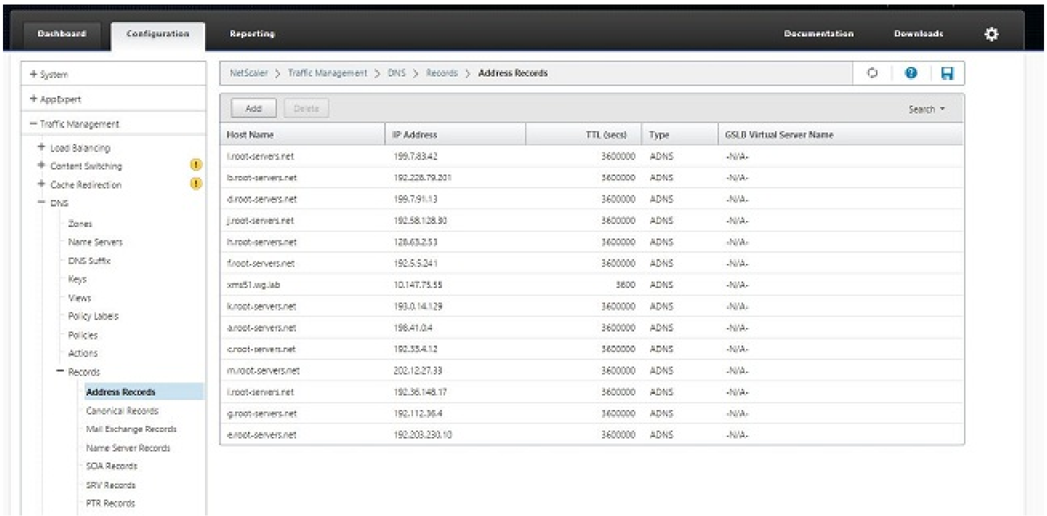
IP Address 10.147.75.56
Port 443 ● Up
Port 8443 ● Up

Microsoft Exchange Load Balancing with Email Security Filtering

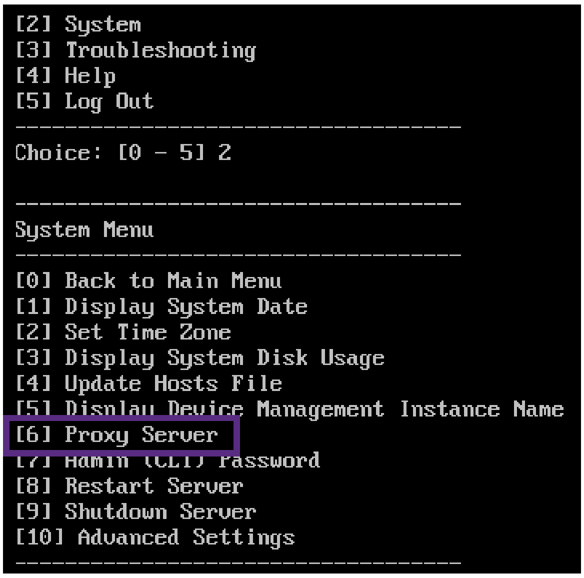
Not Configured



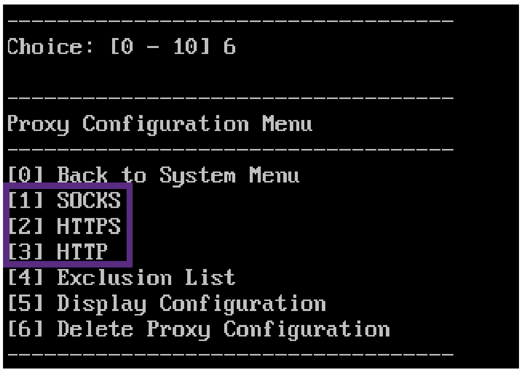
Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health
_XM_MAM_LB_10.147.75.55_8443	● Up	● Up	10.147.75.55	8443	SSL	LEASTCONNECTION	CUSTOMSERVERID	100.00% 2
_XM_LB_MDM_XenMobileMDM_10.147.75.56_443	● Up	● Up	10.147.75.56	443	SSL_BRIDGE	LEASTCONNECTION	SSLSESSION	100.00% 2
_XM_LB_MDM_XenMobileMDM_10.147.75.56_8443	● Up	● Up	10.147.75.56	8443	SSL_BRIDGE	LEASTCONNECTION	SSLSESSION	100.00% 2



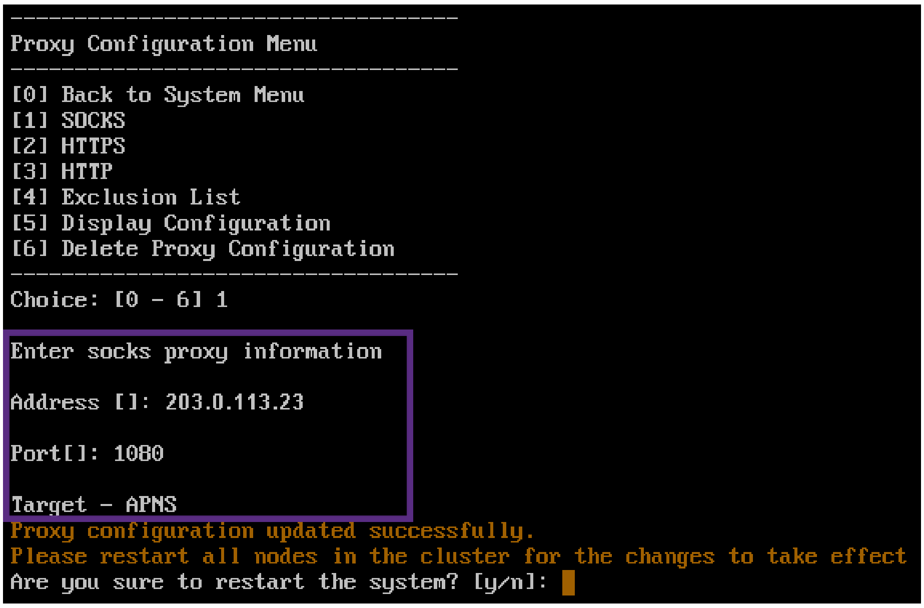
Host Name	IP Address	TTL (secs)	Type	GSLB Virtual Server Name
l.root-servers.net	199.7.83.42	3600000	ADNS	-N/A-
b.root-servers.net	192.228.79.201	3600000	ADNS	-N/A-
d.root-servers.net	199.7.91.13	3600000	ADNS	-N/A-
j.root-servers.net	192.58.128.30	3600000	ADNS	-N/A-
h.root-servers.net	128.63.2.53	3600000	ADNS	-N/A-
f.root-servers.net	192.5.5.241	3600000	ADNS	-N/A-
xms51.wg.lab	10.147.75.55	3600	ADNS	-N/A-
k.root-servers.net	193.0.14.129	3600000	ADNS	-N/A-
a.root-servers.net	198.41.0.4	3600000	ADNS	-N/A-
c.root-servers.net	192.33.4.12	3600000	ADNS	-N/A-
m.root-servers.net	202.12.27.33	3600000	ADNS	-N/A-
i.root-servers.net	192.36.148.17	3600000	ADNS	-N/A-
g.root-servers.net	192.112.36.4	3600000	ADNS	-N/A-
e.root-servers.net	192.203.230.10	3600000	ADNS	-N/A-



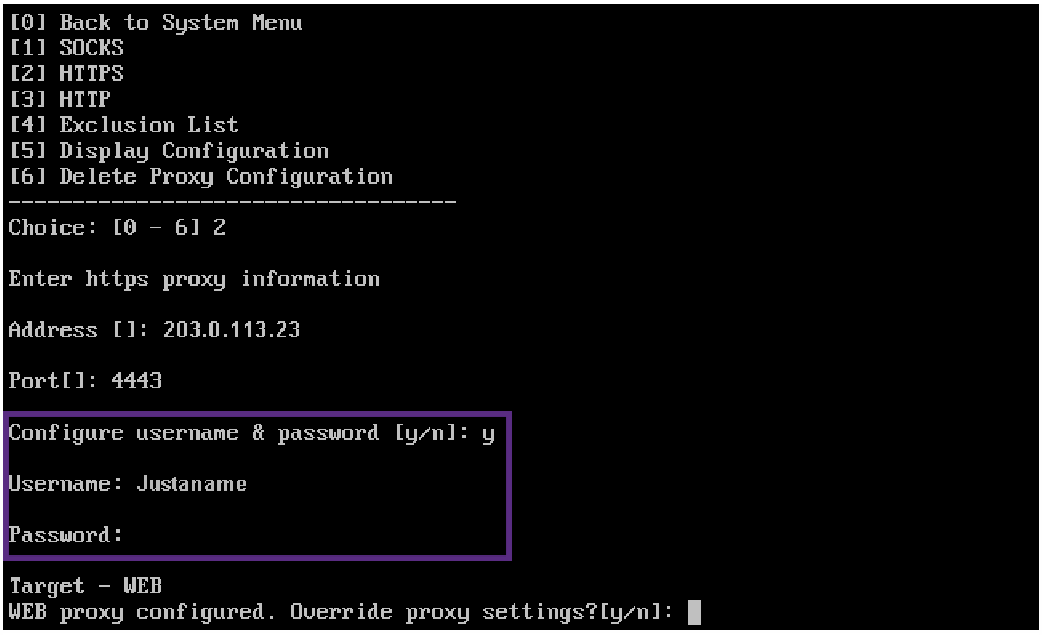
```
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----------------------------------
Choice: [0 - 5] 2

-----------------------------------
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
-----------------------------------
```



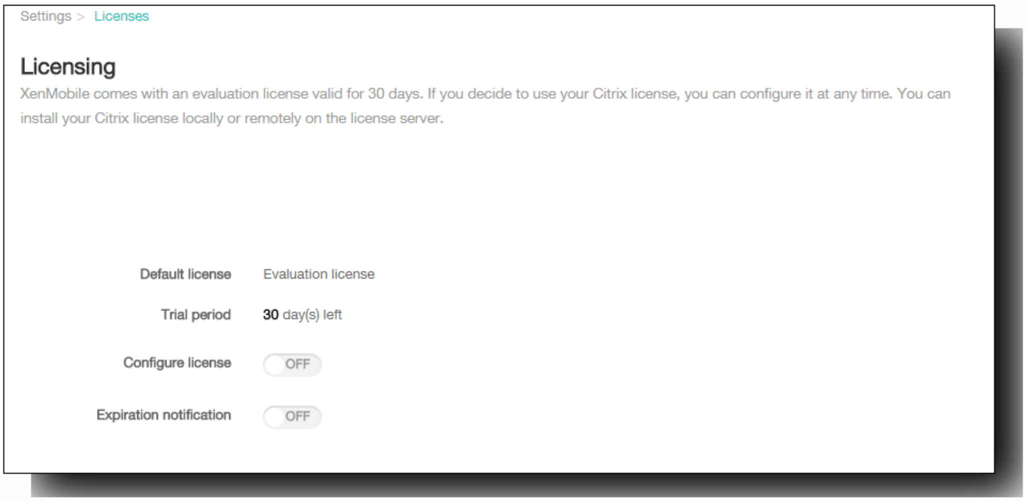
```
-----------------------------------
Choice: [0 - 10] 6

-----------------------------------
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 []: 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 []: 203.0.113.23

Port[]: 4443

Configure username & password [y/n]: y

Username: Justaname

Password:

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

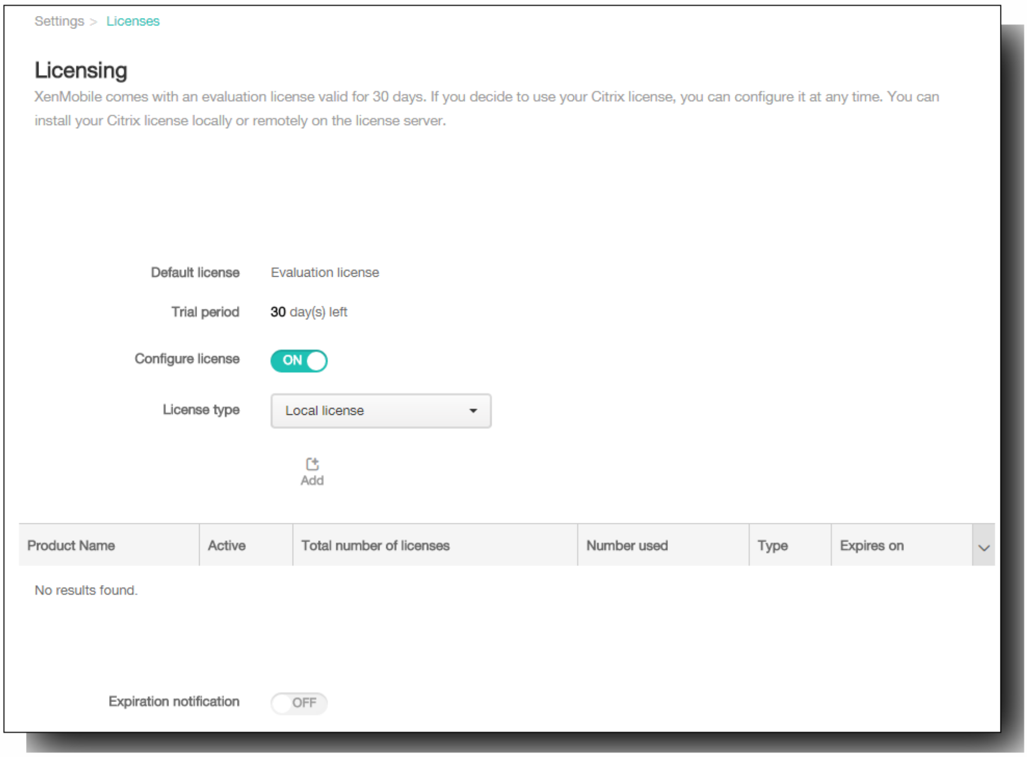

Settings > Licenses

Licensing

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

Default license	Evaluation license
Trial period	30 day(s) left
Configure license	OFF
Expiration notification	OFF

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

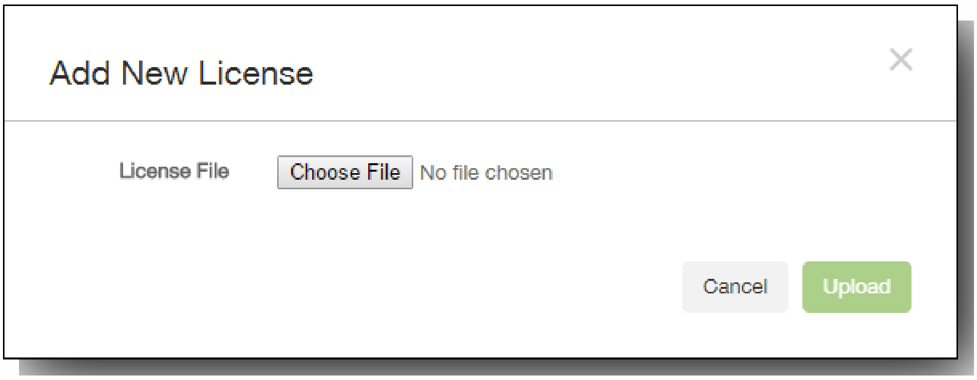
Configure license: ON

License type: Local license

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

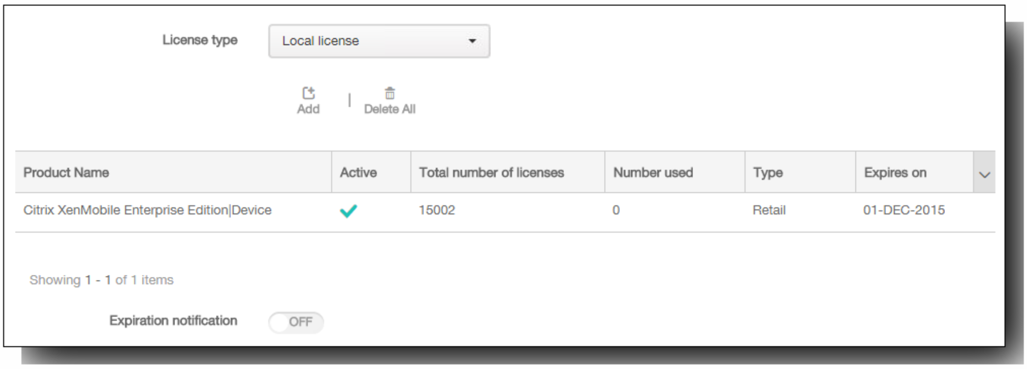
No results found.

Expiration notification: OFF



Add New License

License File: Choose File No file chosen



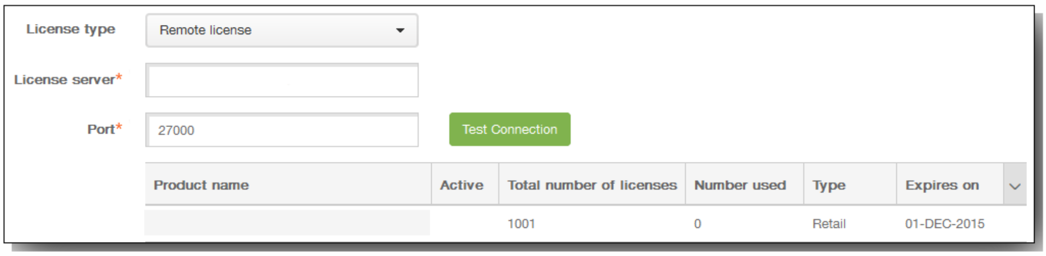
License type	Local license

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

Showing 1 - 1 of 1 items

Expiration notification OFF

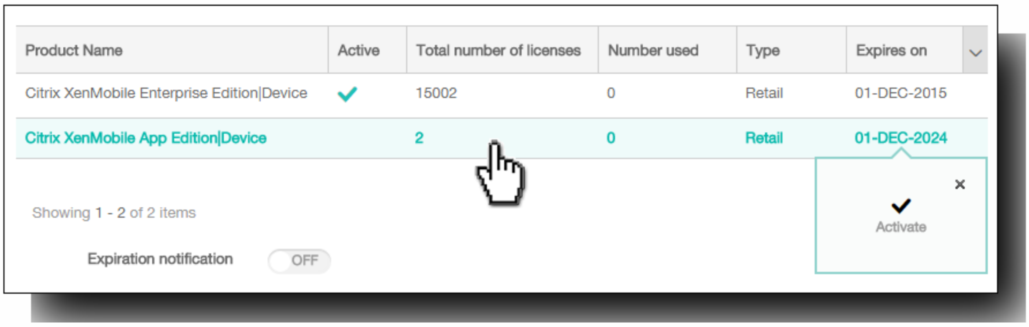
To add a remote license



License type	Remote license
License server*	
Port*	27000

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

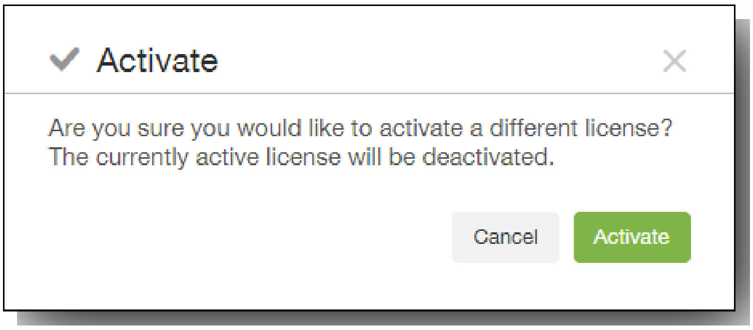
To activate a different license



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

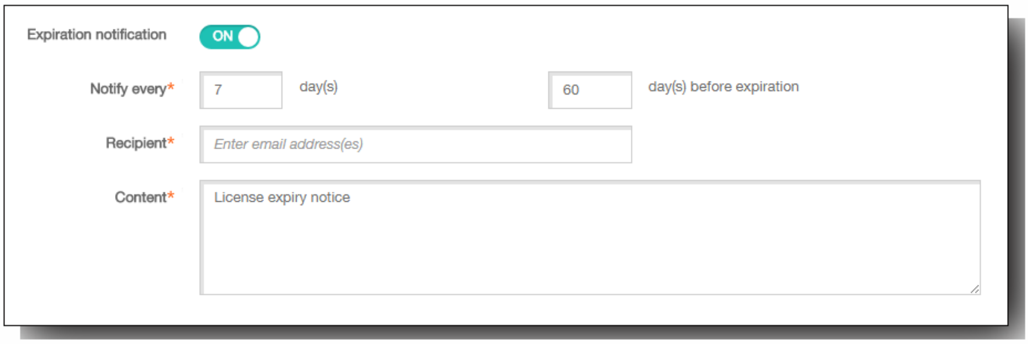
Expiration notification OFF



Activate

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

To automate an expiration notification



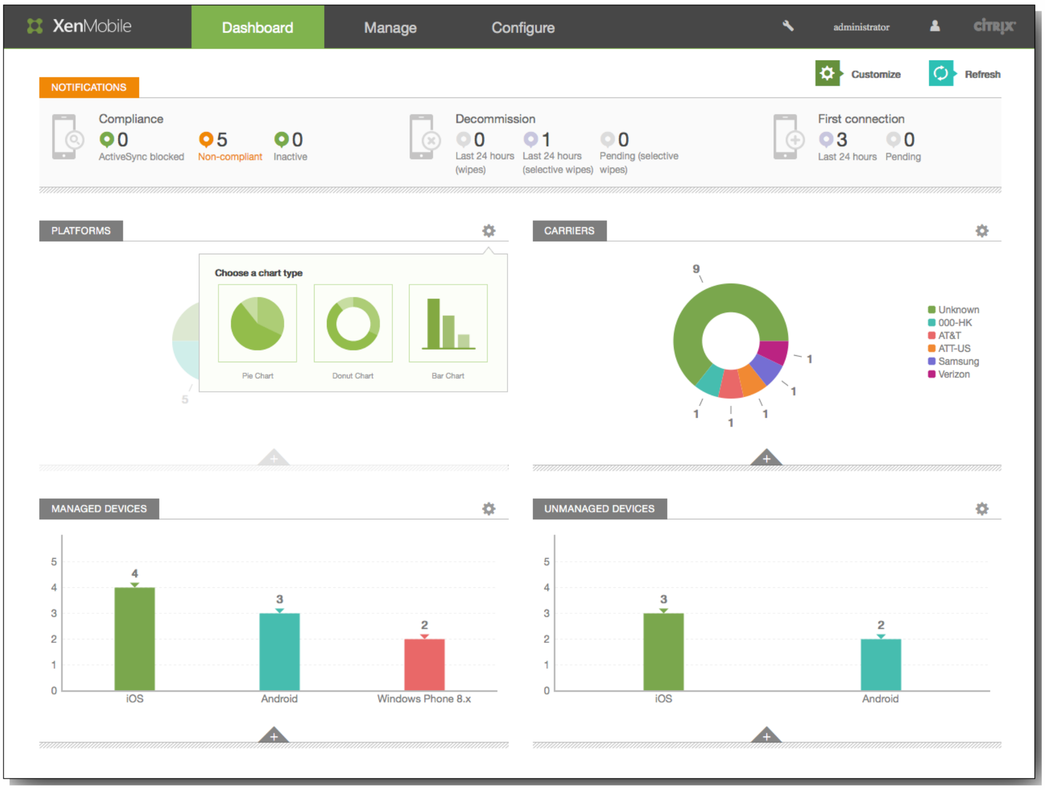
Expiration notification ON

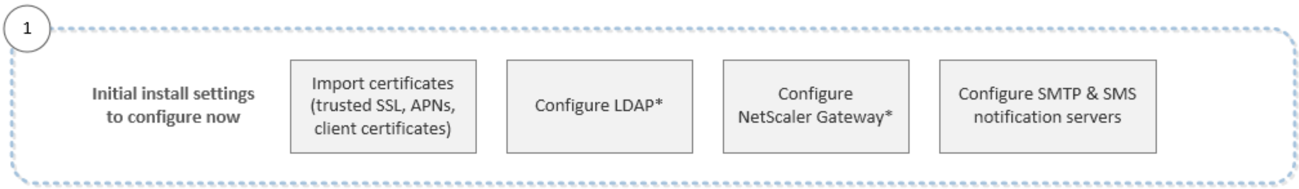
Notify every* 7 day(s) 60 day(s) before expiration

Recipient* Enter email address(es)

Content* License expiry notice

-
-




1

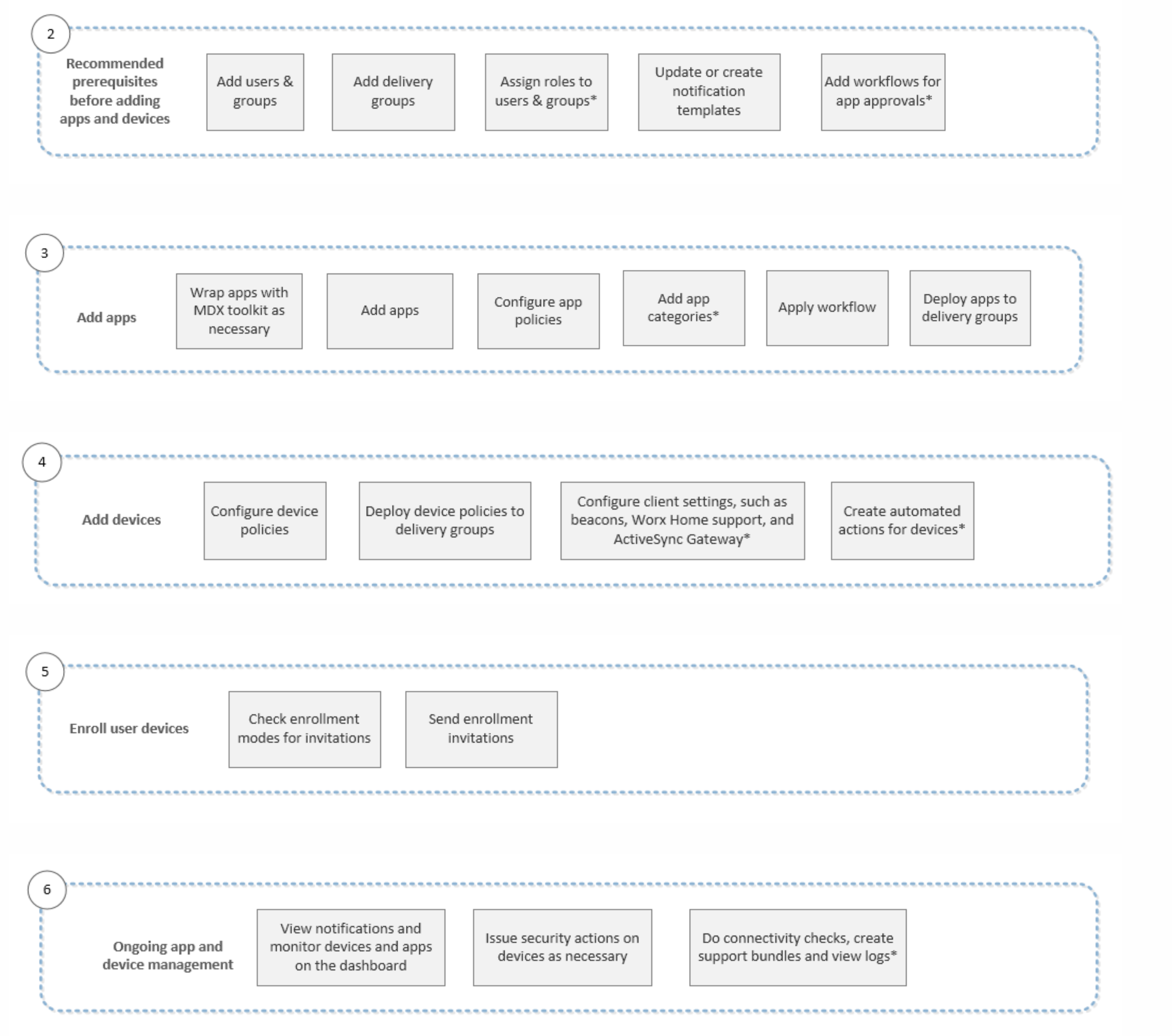
Initial install settings to configure now

Import certificates (trusted SSL, APNs, client certificates)

Configure LDAP*

Configure NetScaler Gateway*

Configure SMTP & SMS notification servers



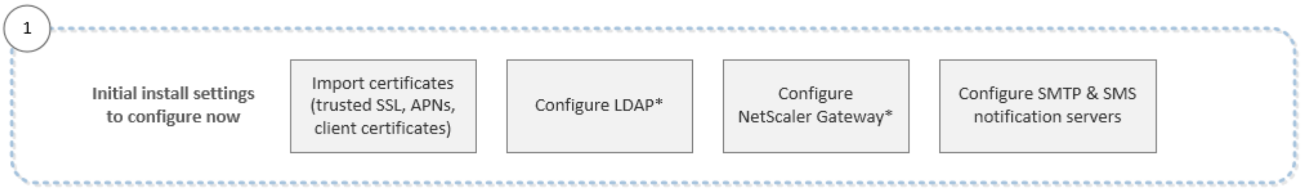
2
Recommended prerequisites before adding apps and devices
Add users & groups
Add delivery groups
Assign roles to users & groups*
Update or create notification templates
Add workflows for app approvals*

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

4
Add devices
Configure device policies
Deploy device policies to delivery groups
Configure client settings, such as beacons, Worx Home support, and ActiveSync Gateway*
Create automated actions for devices*

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

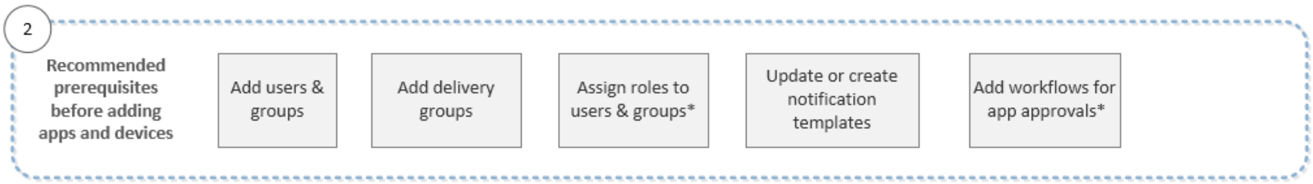
Initial install settings to configure now

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

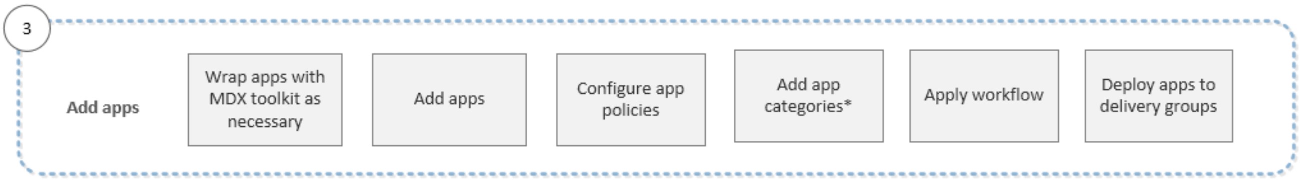
Add users & groups

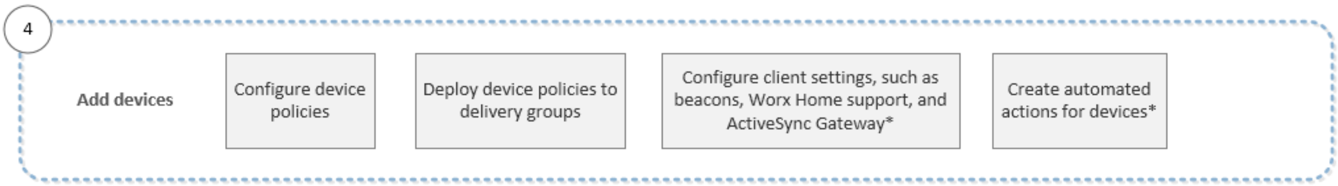
Add delivery groups

Assign roles to users & groups*

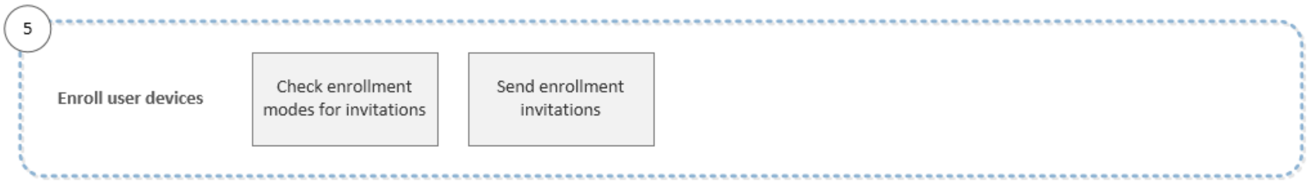
Update or create notification templates

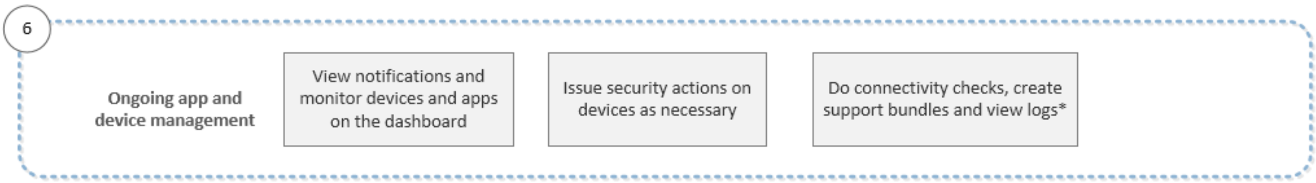
Add workflows for app approvals*


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

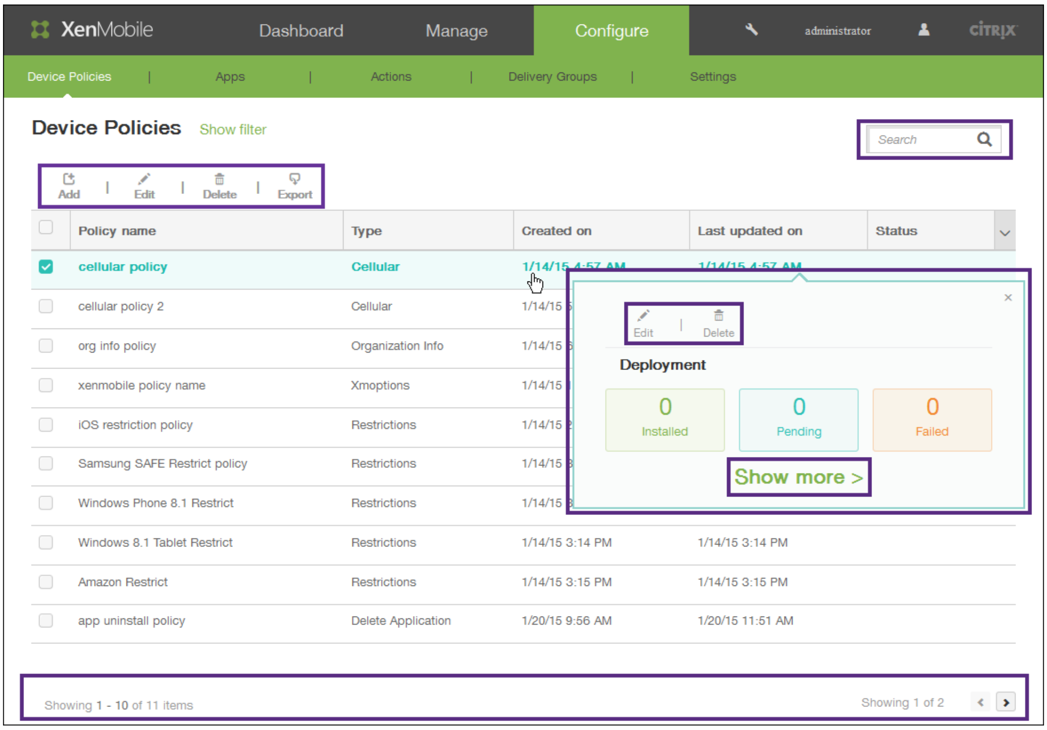

4
Add devices
Configure device policies
Deploy device policies to delivery groups
Configure client settings, such as beacons, Worx Home support, and ActiveSync Gateway*
Create automated actions for devices*

-
-
-
-
-


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



XenMobile | Dashboard | Manage | Configure | administrator | CITRIX

Device Policies | Apps | Actions | Delivery Groups | Settings

Device Policies Show filter

Search

Add | Edit | Delete | Export

☐	Policy name	Type	Created on	Last updated on	Status
☑	cellular policy	Cellular	1/14/15 4:57 AM	1/14/15 4:57 AM	
☐	cellular policy 2	Cellular	1/14/15		
☐	org info policy	Organization Info	1/14/15		
☐	xenmobile policy name	Xmoptions	1/14/15		
☐	iOS restriction policy	Restrictions	1/14/15		
☐	Samsung SAFE Restrict policy	Restrictions	1/14/15		
☐	Windows Phone 8.1 Restrict	Restrictions	1/14/15		
☐	Windows 8.1 Tablet Restrict	Restrictions	1/14/15 3:14 PM	1/14/15 3:14 PM	
☐	Amazon Restrict	Restrictions	1/14/15 3:15 PM	1/14/15 3:15 PM	
☐	app uninstall policy	Delete Application	1/20/15 9:56 AM	1/20/15 11:51 AM	

Edit | Delete

Deployment

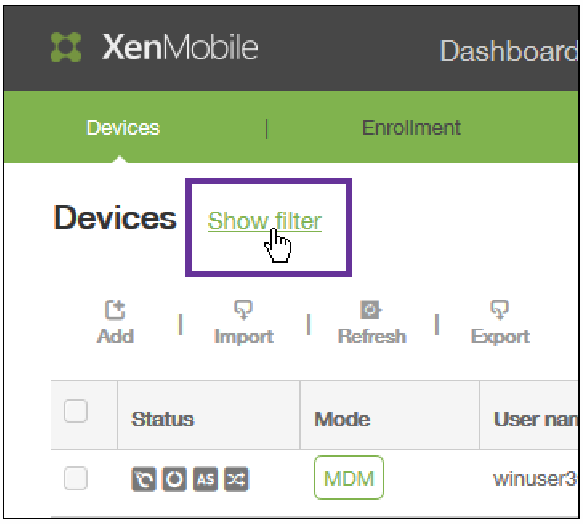
0 Installed | 0 Pending | 0 Failed

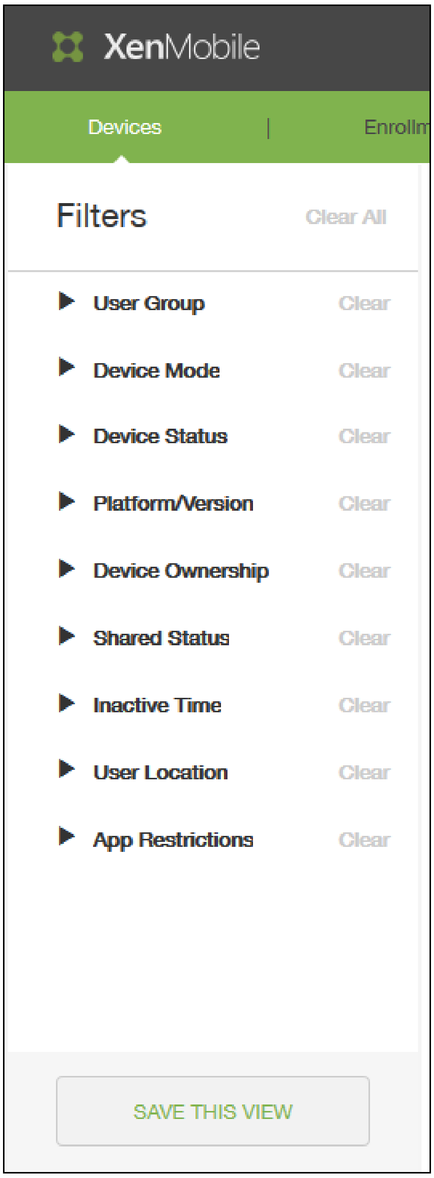
Show more >

Showing 1 - 10 of 11 items

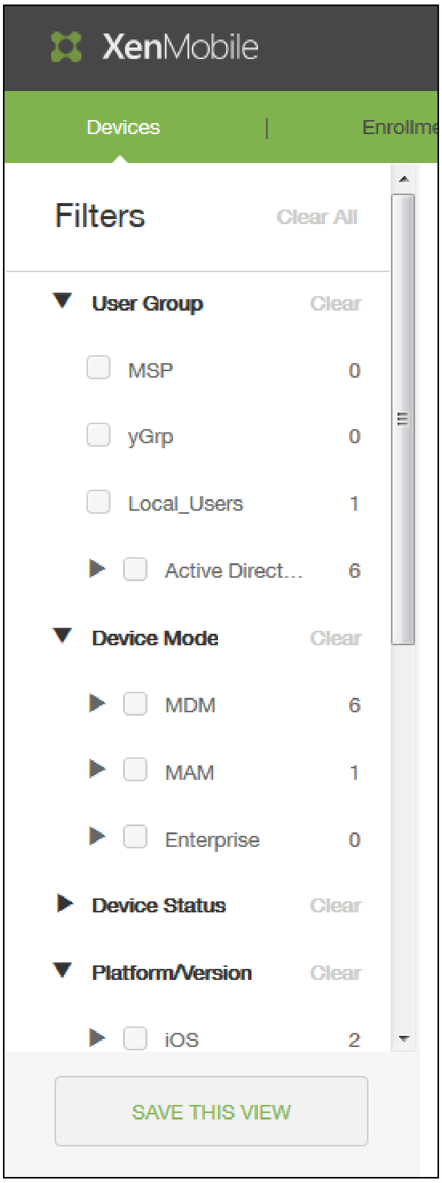
Showing 1 of 2

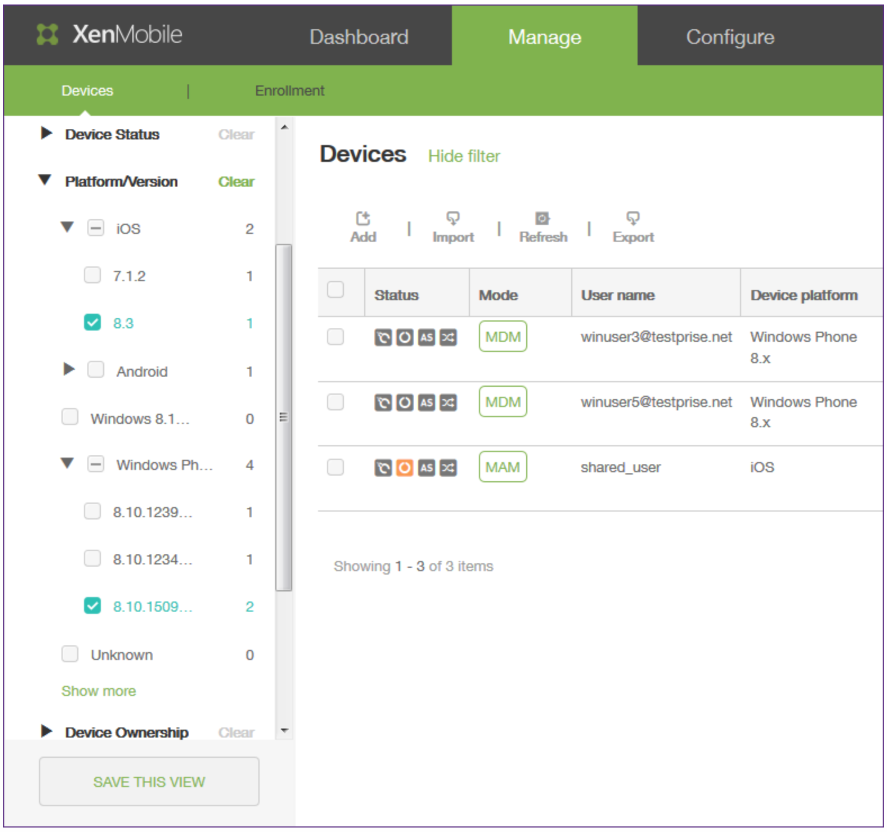
To filter information in the XenMobile console


XenMobile
Dashboard
Devices
Enrollment
Devices
Show filter
Add
Import
Refresh
Export
Status
Mode
User nam
MDM
winuser3



XenMobile
Devices
|
Enrollm
Filters
Clear All
User Group
Clear
Device Mode
Clear
Device Status
Clear
Platform/Version
Clear
Device Ownership
Clear
Shared Status
Clear
Inactive Time
Clear
User Location
Clear
App Restrictions
Clear
SAVE THIS VIEW

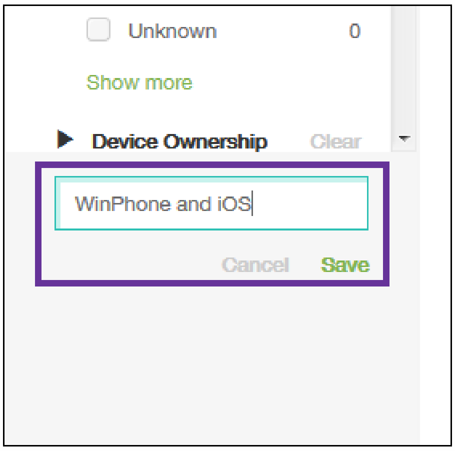

XenMobile
Devices
Enrollme
Filters
Clear All
User Group
Clear
□ MSP 0
□ yGrp 0
□ Local_Users 1
▶ □ Active Direct… 6
Device Mode
Clear
▶ □ MDM 6
▶ □ MAM 1
▶ □ Enterprise 0
Device Status
Clear
Platform/Version
Clear
▶ □ iOS 2
SAVE THIS VIEW

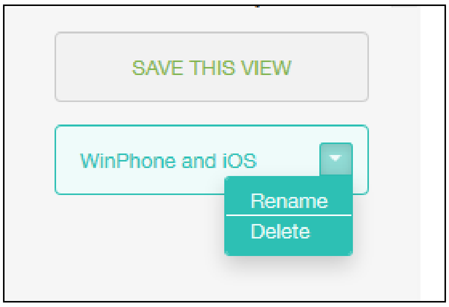


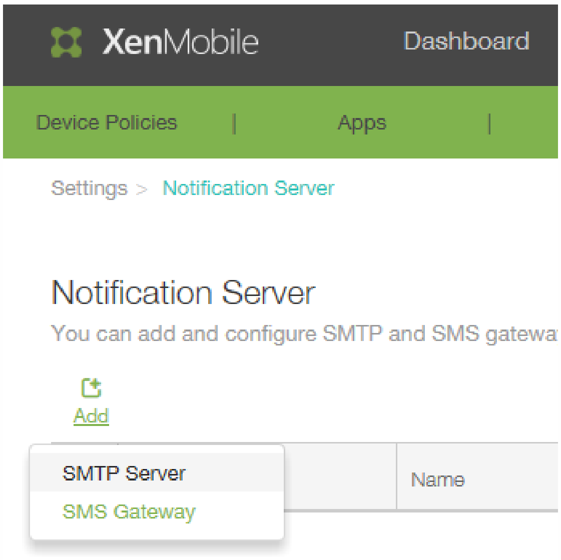
☐	Status	Mode	User name	Device platform
☐		MDM	winuser3@testprise.net	Windows Phone 8.x
☐		MDM	winuser5@testprise.net	Windows Phone 8.x
☐		MAM	shared_user	iOS

Showing 1 - 3 of 3 items

-
-
-



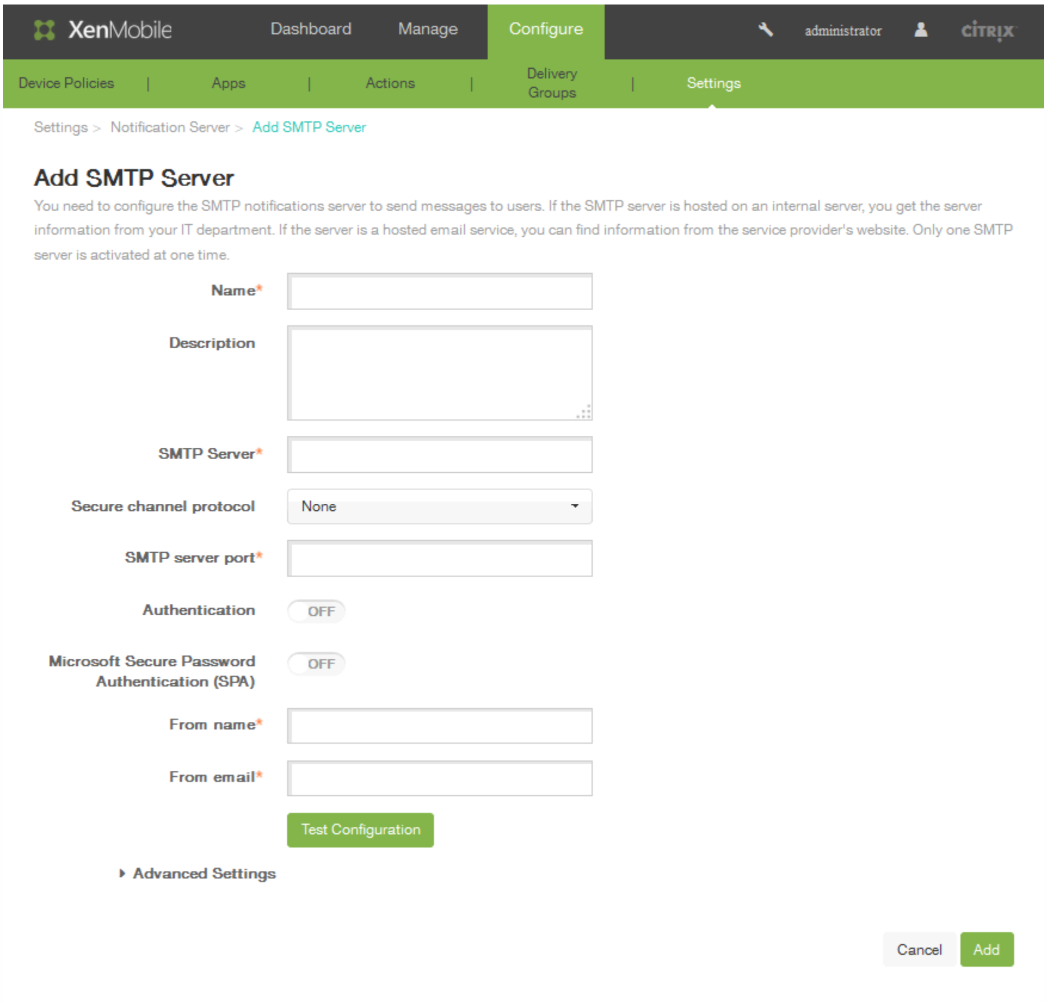

SAVE THIS VIEW
WinPhone and iOS
Rename
Delete



Notification Server

You can add and configure SMTP and SMS gatewa

-
-



Add SMTP Server

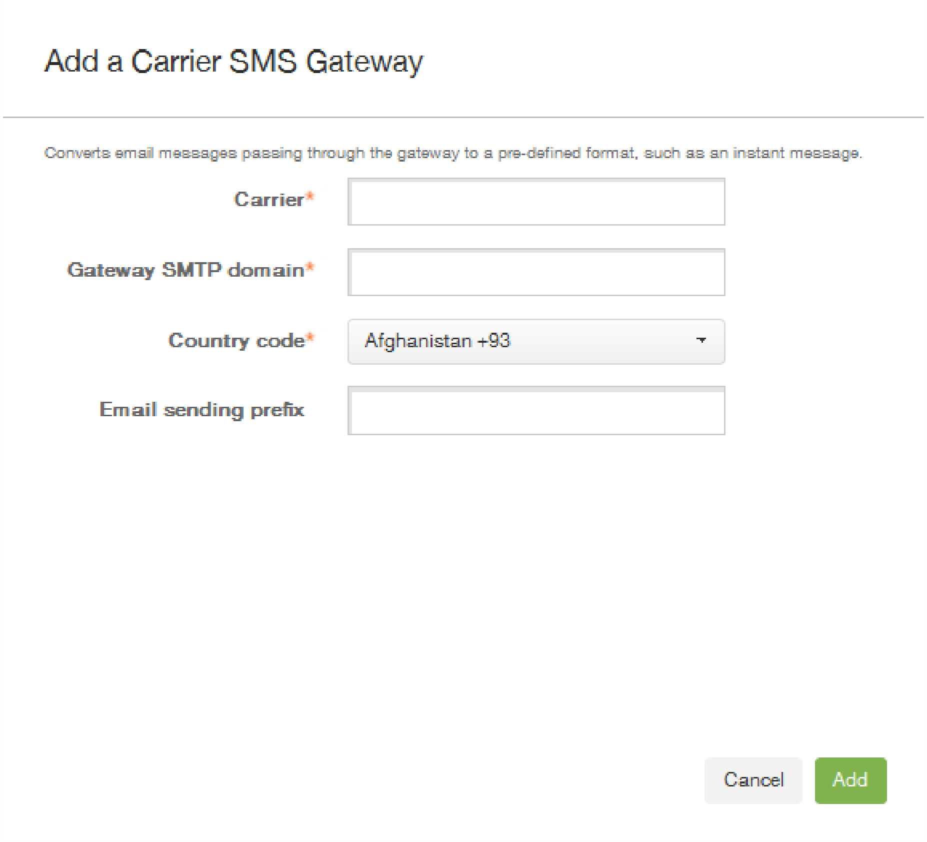
You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP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

-
-
-
-
-
-
-
-
-
-
-

-

-



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	

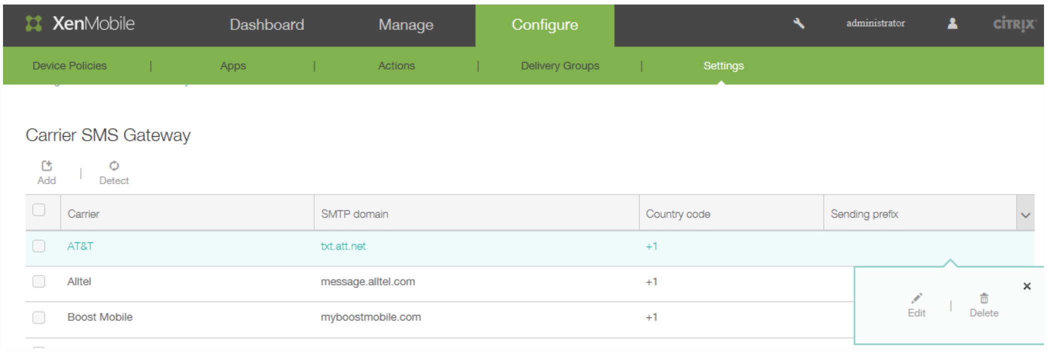
-
-
-
-

-

-
-

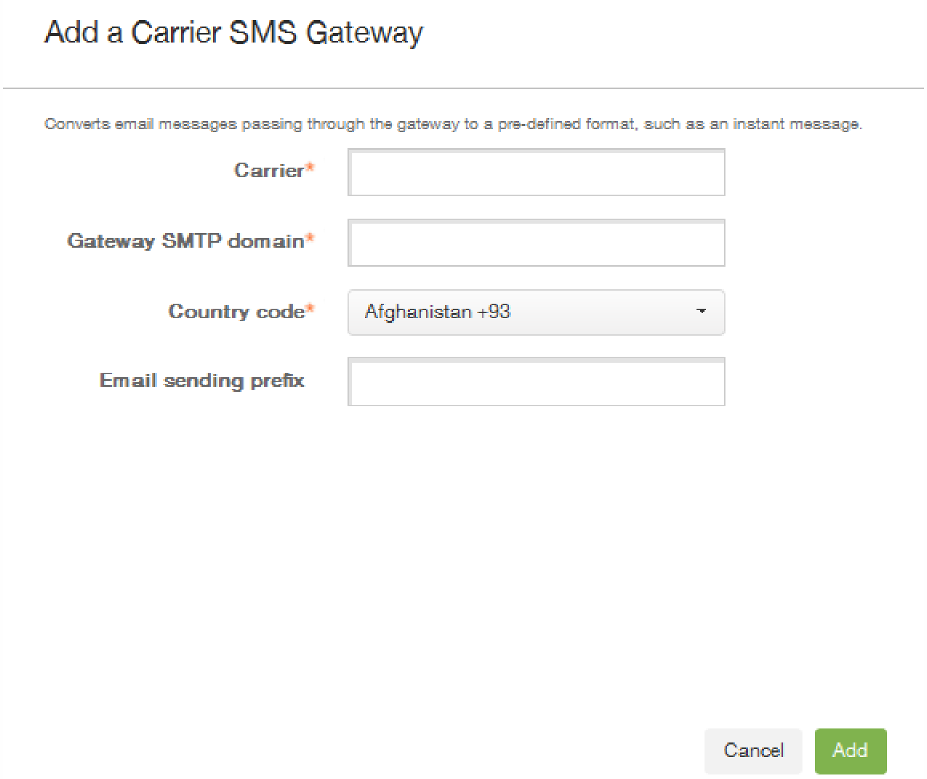
-

To add a Carrier SMS Gateway



Carrier SMS Gateway

Carrier	SMTP domain	Country code	Sending prefix
AT&T	txt.att.net	+1	
Alltel	message.alltel.com	+1	
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*	Afghanistan +93
Email sending prefix	

Configuring Client Certificates for Authentication

XenMobile PKI

XenMobile Certificate Expiration Policy

APNs certificate for WorxMail

APNs certificate for iOS device management

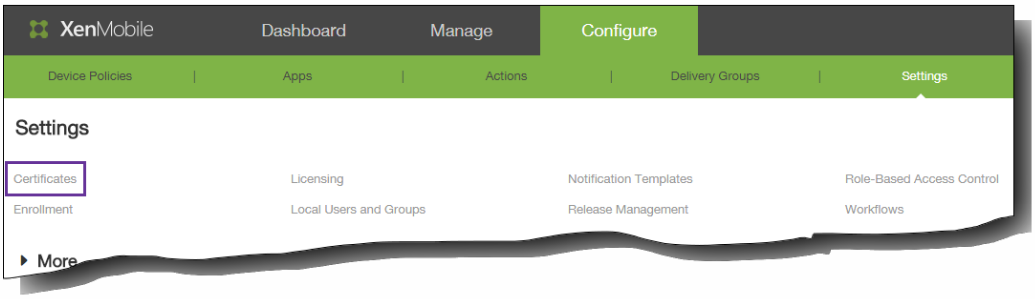
MDX Toolkit (iOS distribution certificate)

Android keystore

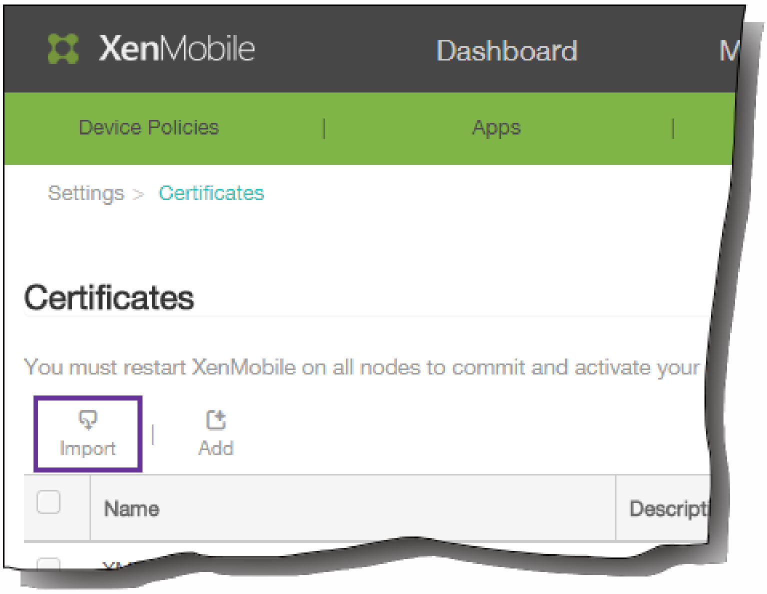
Enterprise certificate from Symantec for Windows phones

-
-

To import a keystore

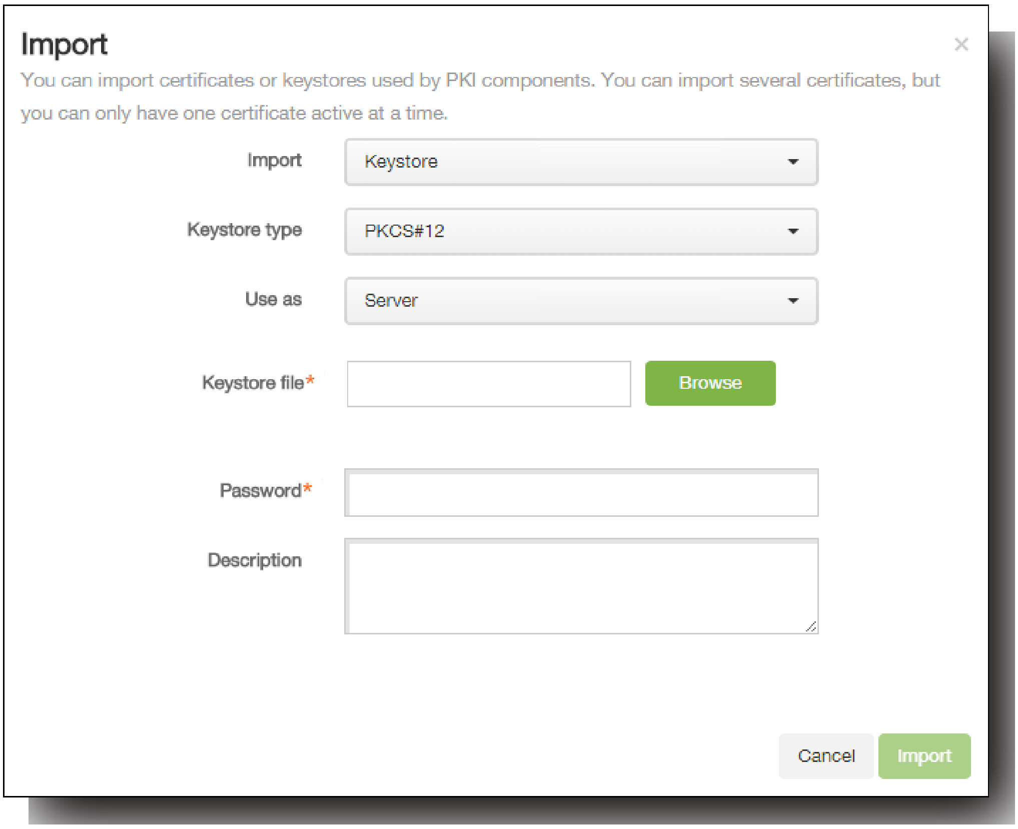


Settings



Certificates

You must restart XenMobile on all nodes to commit and activate your



Import

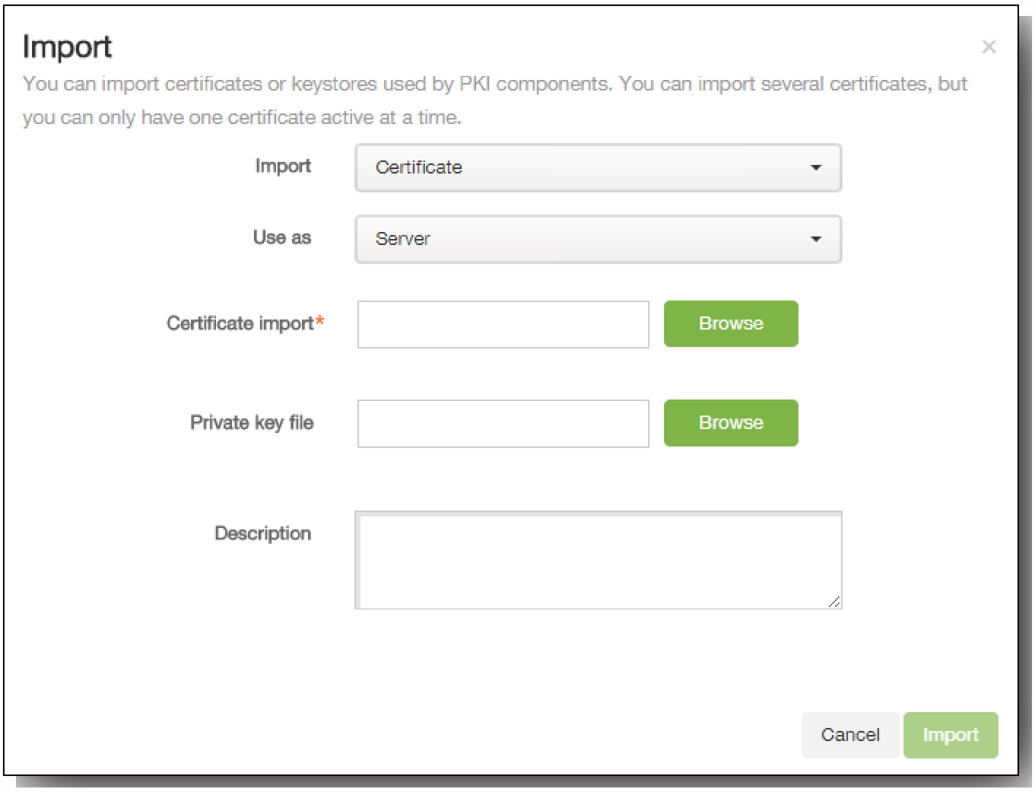
You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import	Keystore
Keystore type	PKCS#12
Use as	Server
Keystore file*	
Password*	
Description	

-
-
-
-

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: Certificate

Use as: Server

Certificate import*

Private key file

Description

-
-
-

Updating a Certificate

-
-
-

-
-
-

Common PKI Concepts

-
-
-

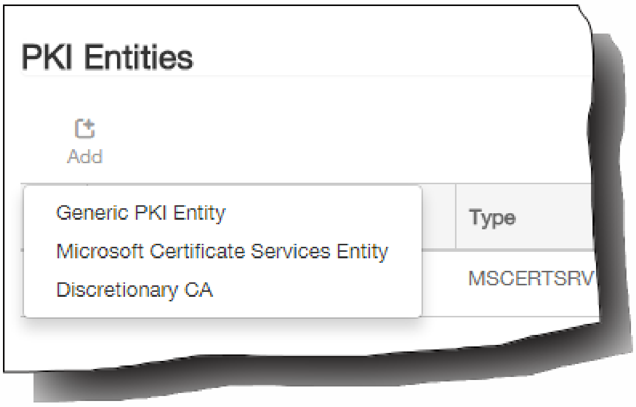
Generic PKI

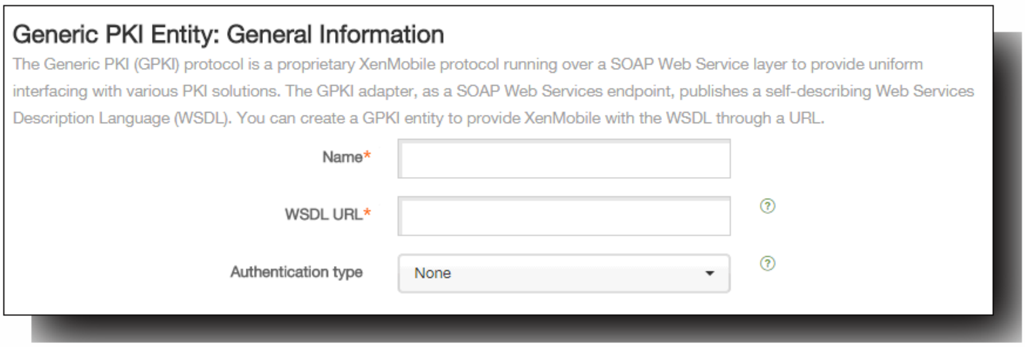
-

-

-

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.

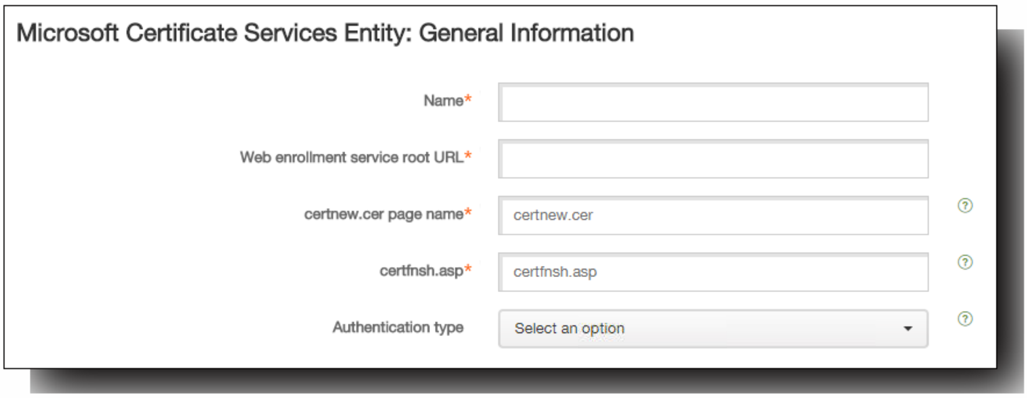
Name*

WSDL URL*

Authentication type: None

Microsoft Certificate Services

To add a Microsoft Certificate Services entity



Microsoft Certificate Services Entity: General Information

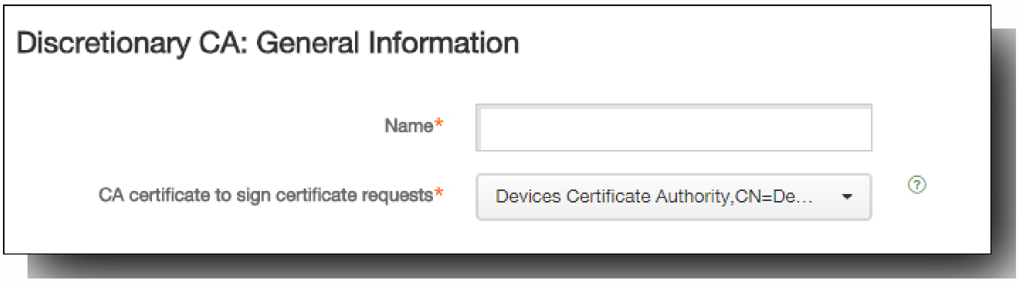
Name*	
Web enrollment service root URL*	
certnew.cer page name*	certnew.cer
certfnsh.asp*	certfnsh.asp
Authentication type	Select an option

Discretionary CAs

https://server/instance/ocsp

-
-
-
-
-

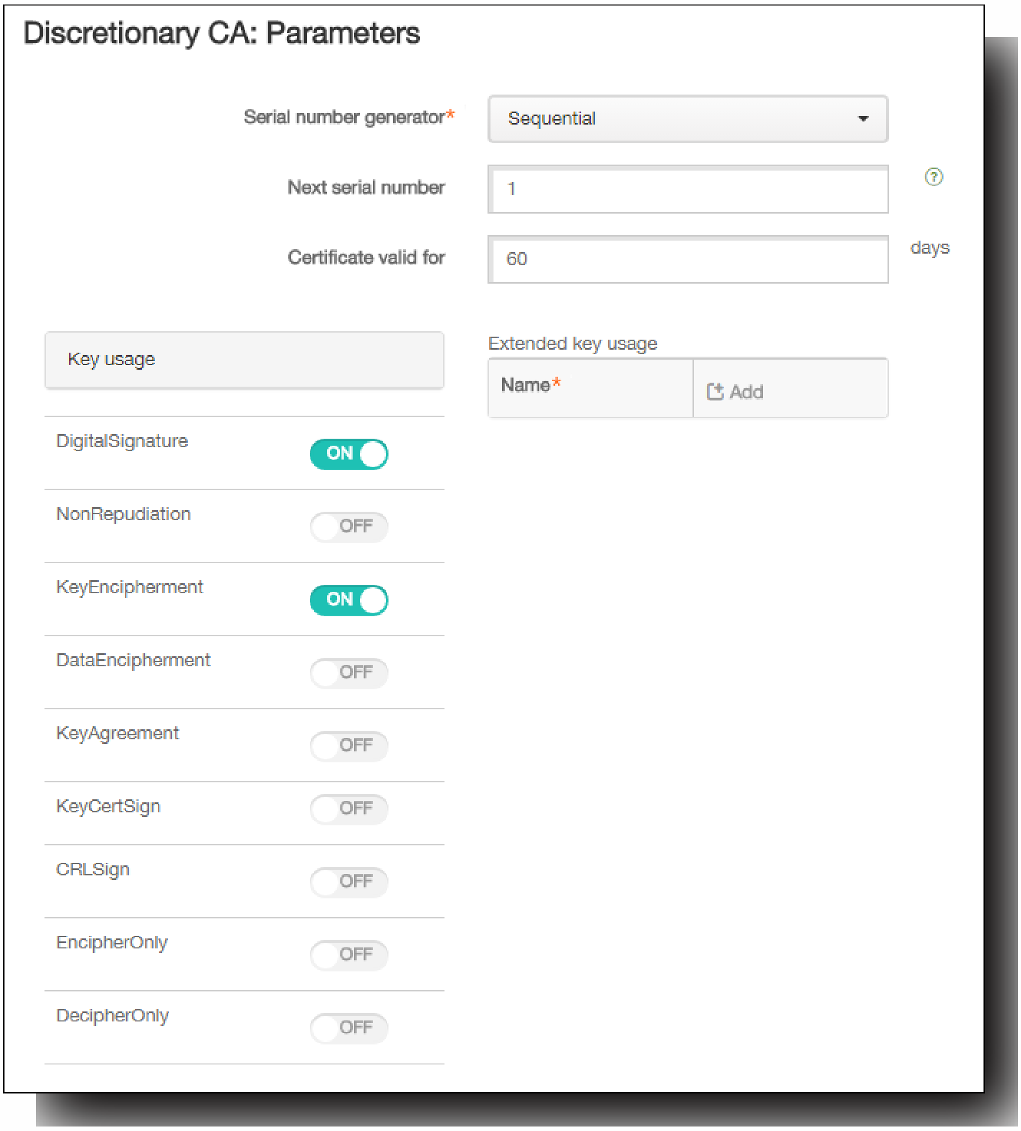
To add discretionary CAs



Discretionary CA: General Information

Name*

CA certificate to sign certificate requests* Devices Certificate Authority,CN=De...



Discretionary CA: Parameters

Serial number generator* Sequential

Next serial number 1

Certificate valid for 60 days

Key usage

DigitalSignature	ON
NonRepudiation	OFF
KeyEncipherment	ON
DataEncipherment	OFF
KeyAgreement	OFF
KeyCertSign	OFF
CRLSign	OFF
EncipherOnly	OFF
DecipherOnly	OFF

Extended key usage

Name* Add

-
-

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

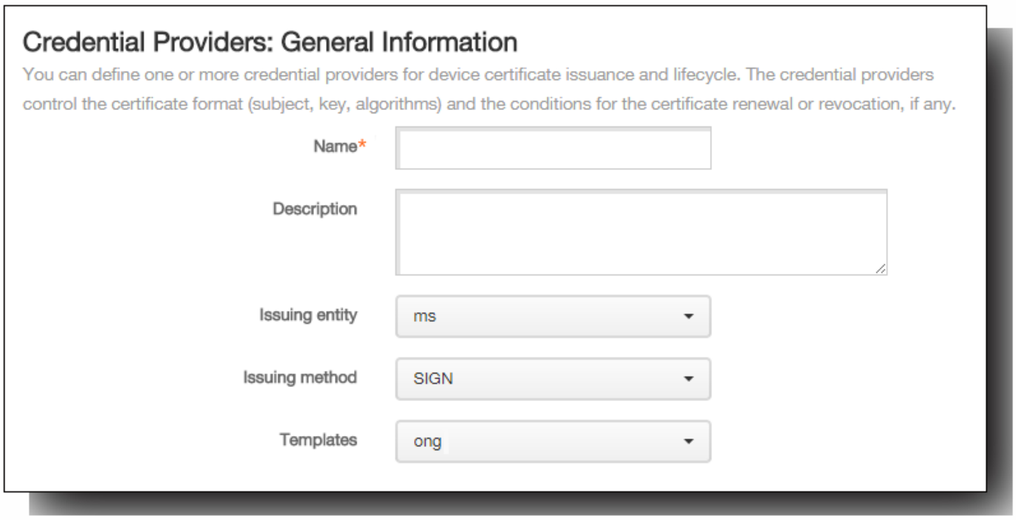
-

-

-

Certificate Renewal

To create a credential provider

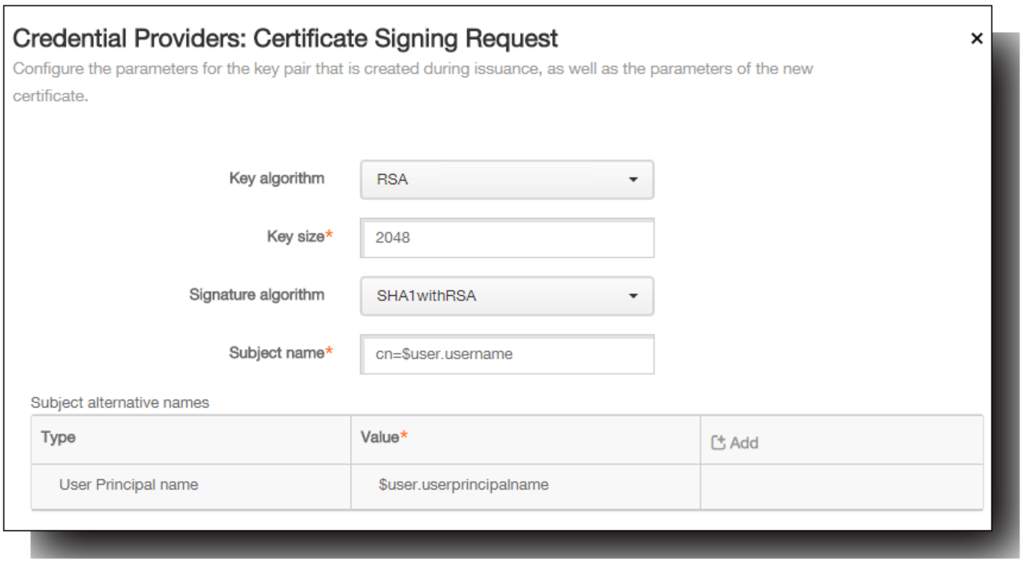


Credential Providers: General Information

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	ms
Issuing method	SIGN
Templates	ong

-



Credential Providers: Certificate Signing Request

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

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

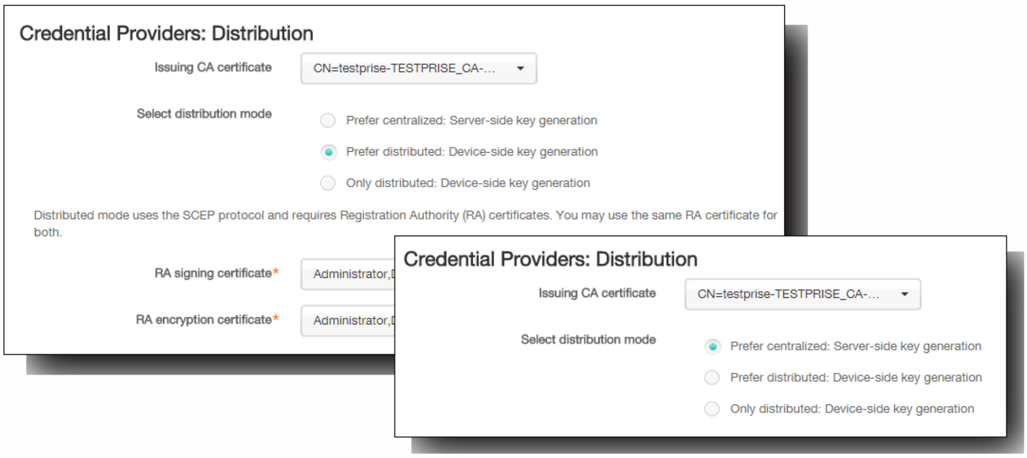
Subject alternative names

Type	Value*	Add
User Principal name	$user.userprincipalname	

```
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

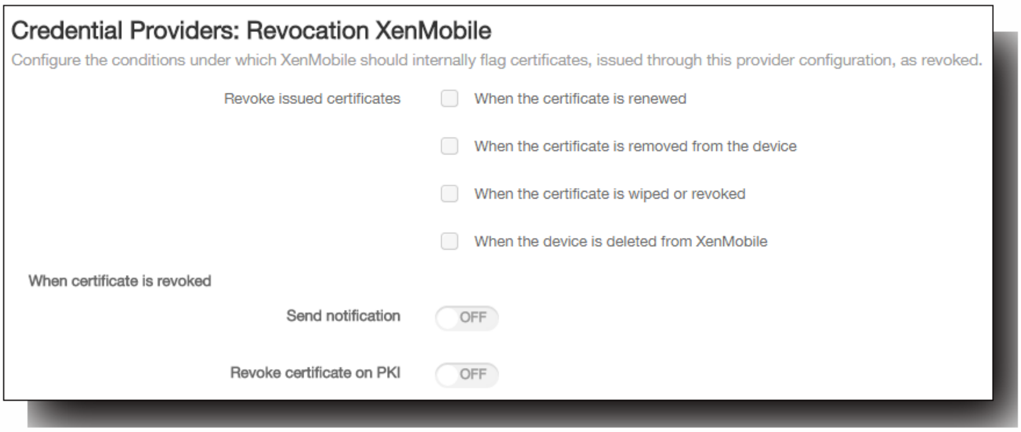
Issuing CA certificate: CN=testprise-TESTPRISE_CA-...

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

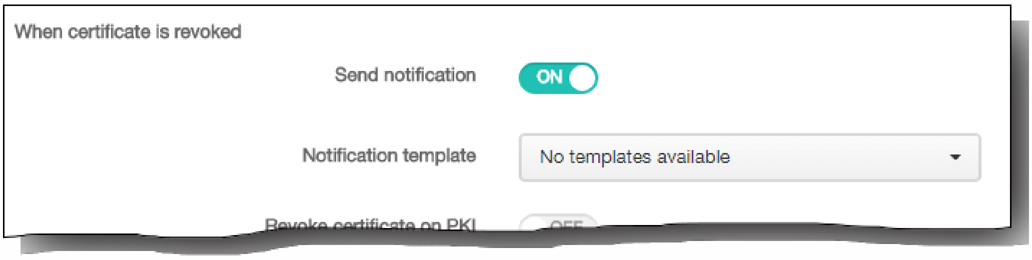
☐ When the certificate is wiped or revoked

☐ When the device is deleted from XenMobile

When certificate is revoked

Send notification: OFF

Revoke certificate on PKI: OFF

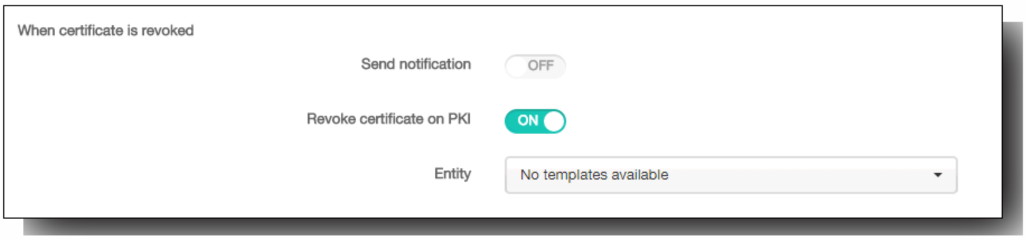


When certificate is revoked

Send notification ON

Notification template No templates available

Revoke certificate on PKI OFF

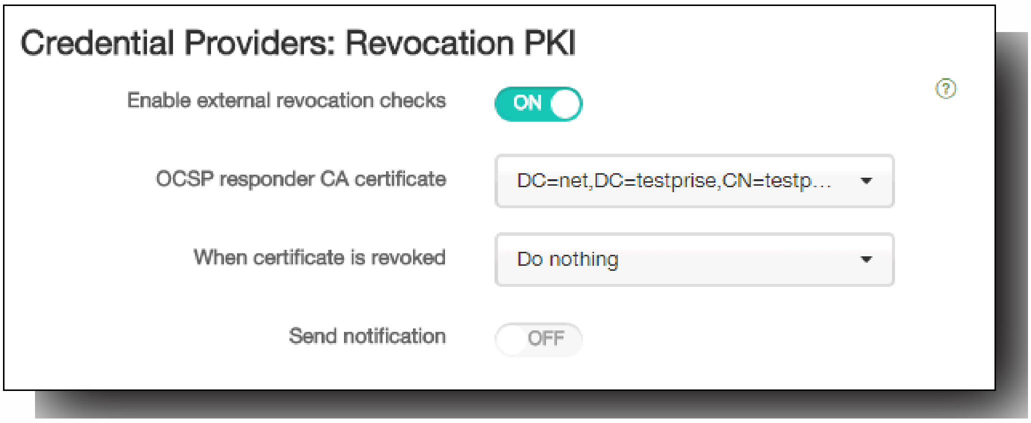


When certificate is revoked

Send notification OFF

Revoke certificate on PKI ON

Entity No templates available



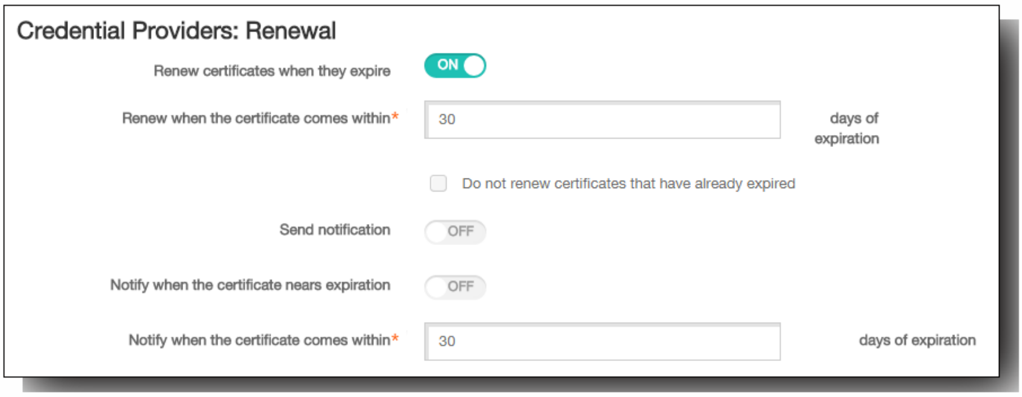
Credential Providers: Revocation PKI

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*: 30 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*: 30 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

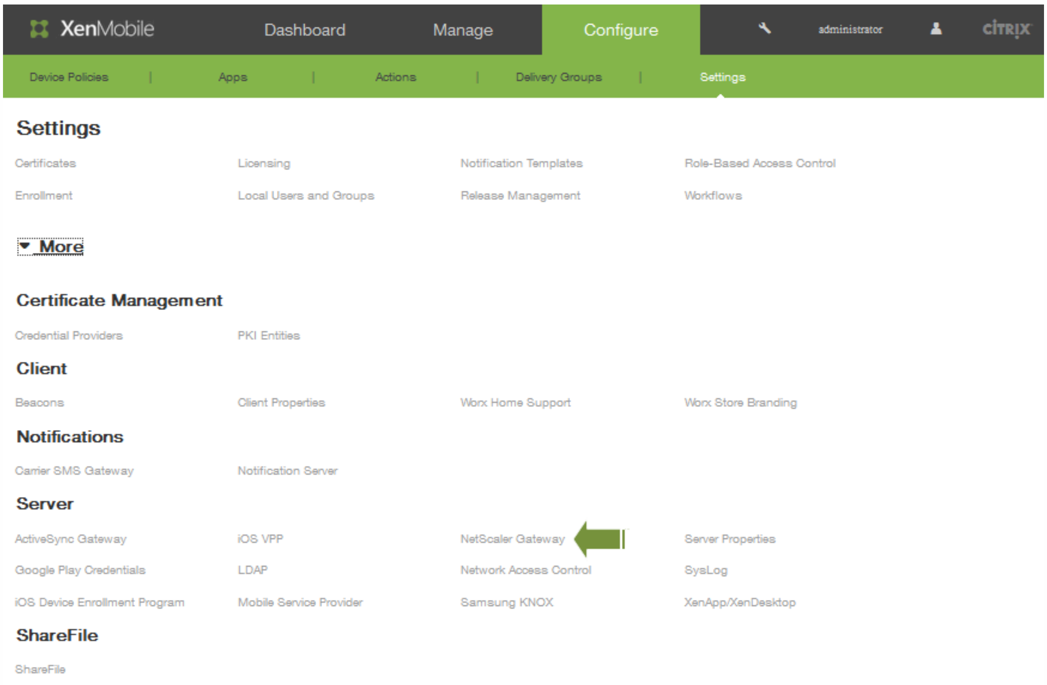
To create a .pfx APNs certificate on a Mac computer

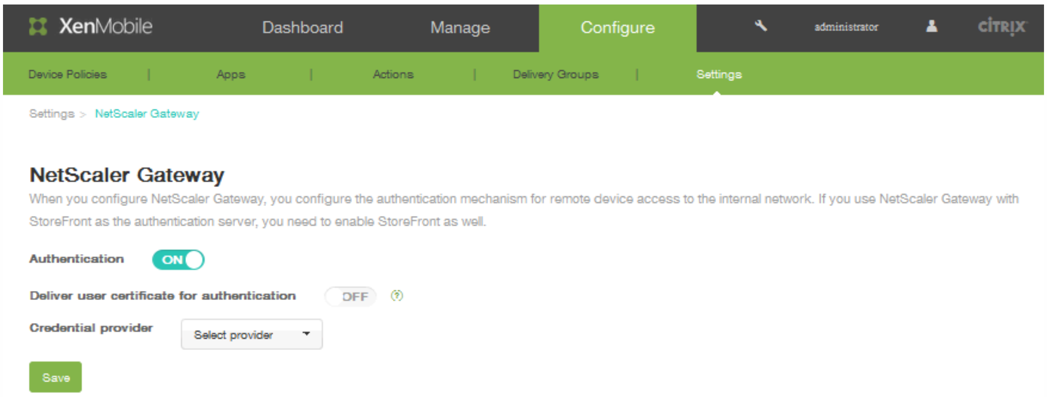
To create a .pfx APNs certificate by using OpenSSL

To import an APNs certificate into XenMobile

To renew an APNs certificate

To configure NetScaler Gateway





NetScaler Gateway

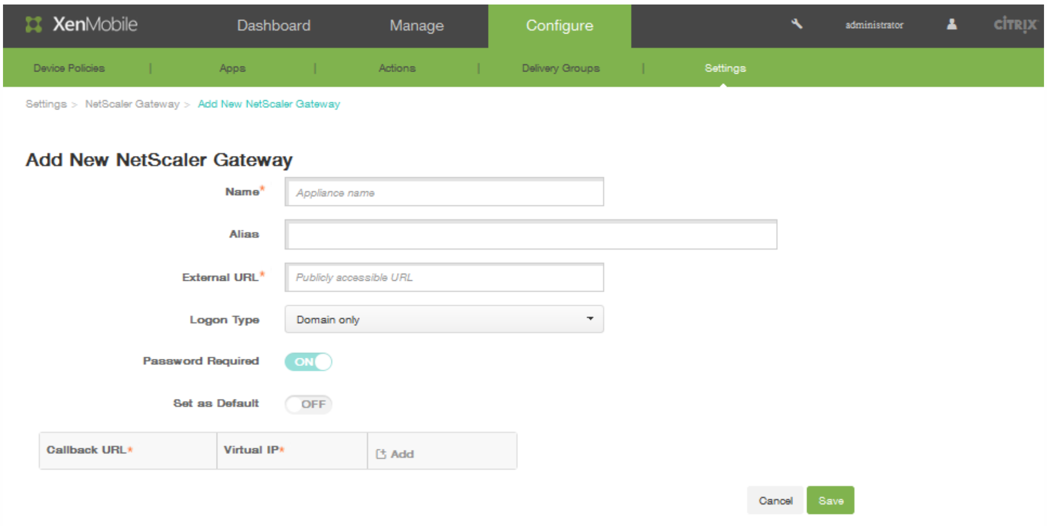
When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication ON

Deliver user certificate for authentication OFF

Credential provider Select provider

To add a new NetScaler Gateway instance



Add New NetScaler Gateway

Name* Appliance name

Alias

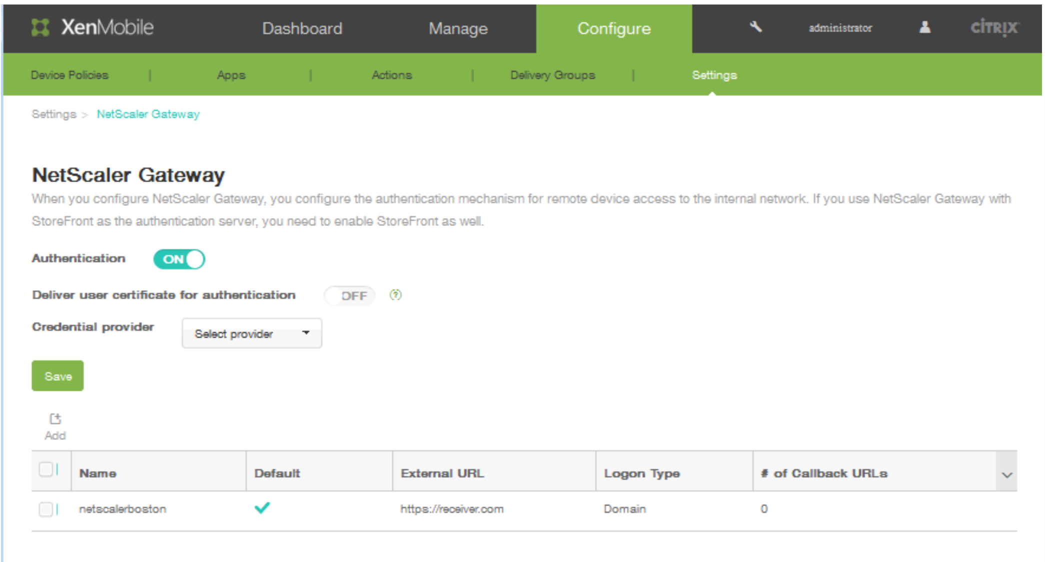
External URL* Publicly accessible URL

Logon Type Domain only

Password Required ON

Set as Default OFF

Callback URL*	Virtual IP*	Add



NetScaler Gateway

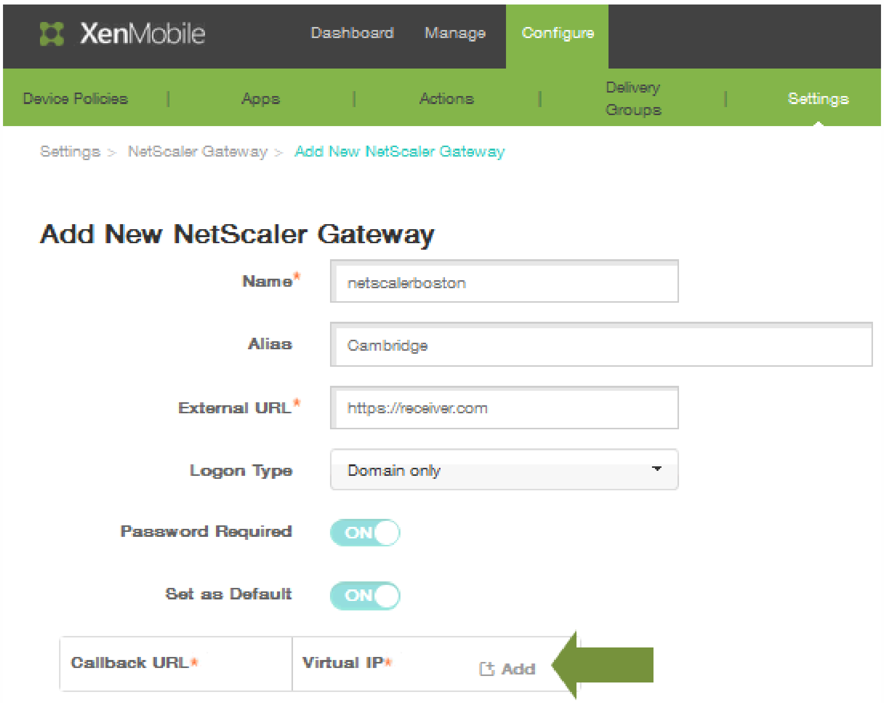
When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication: ON

Deliver user certificate for authentication: OFF

Credential provider: Select provider

□	Name	Default	External URL	Logon Type	# of Callback URLs
□	netscalerboston	✓	https://receiver.com	Domain	0



Add New NetScaler Gateway

Name*: netscalerboston

Alias: Cambridge

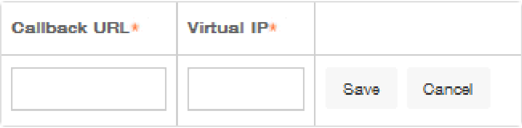
External URL*: https://receiver.com

Logon Type: Domain only

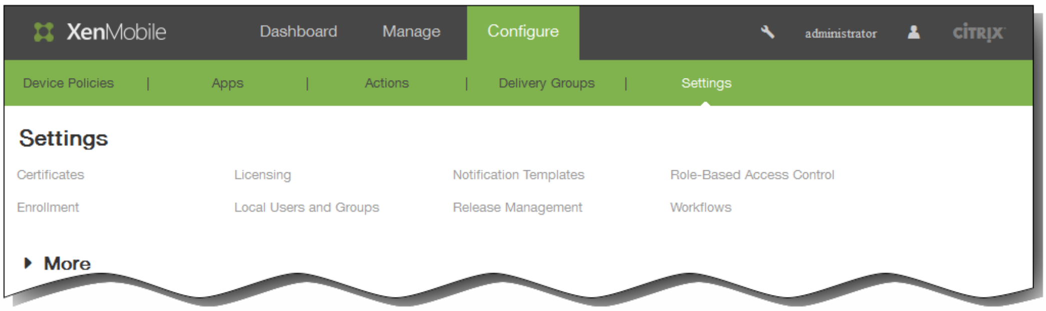
Password Required: ON

Set as Default: ON

Callback URL*	Virtual IP*	Add



Callback URL*	Virtual IP*	
		Save Cancel

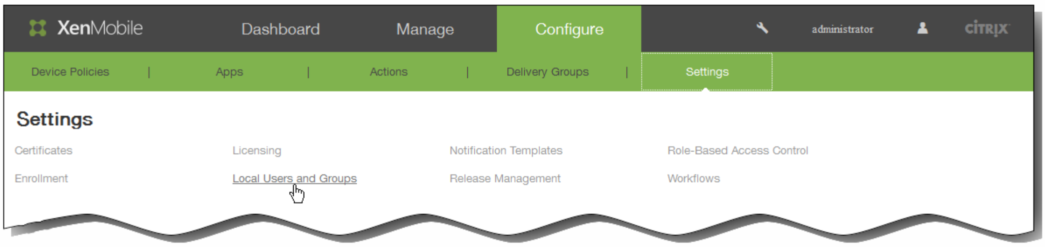

XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies
Apps
Actions
Delivery Groups
Settings
Settings
Certificates
Licensing
Notification Templates
Role-Based Access Control
Enrollment
Local Users and Groups
Release Management
Workflows
More

To add, edit, or delete local users in XenMobile

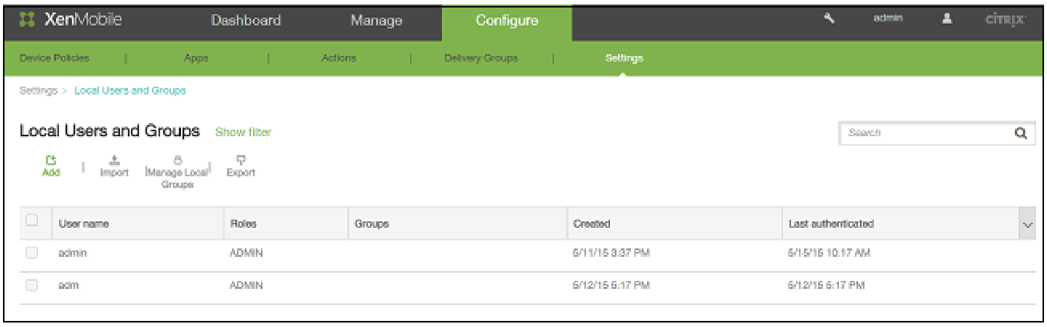
May 15, 2015

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

1. In the XenMobile console, click Configure > Settings > Local Users and Groups.



The Local Users and Groups page appears.

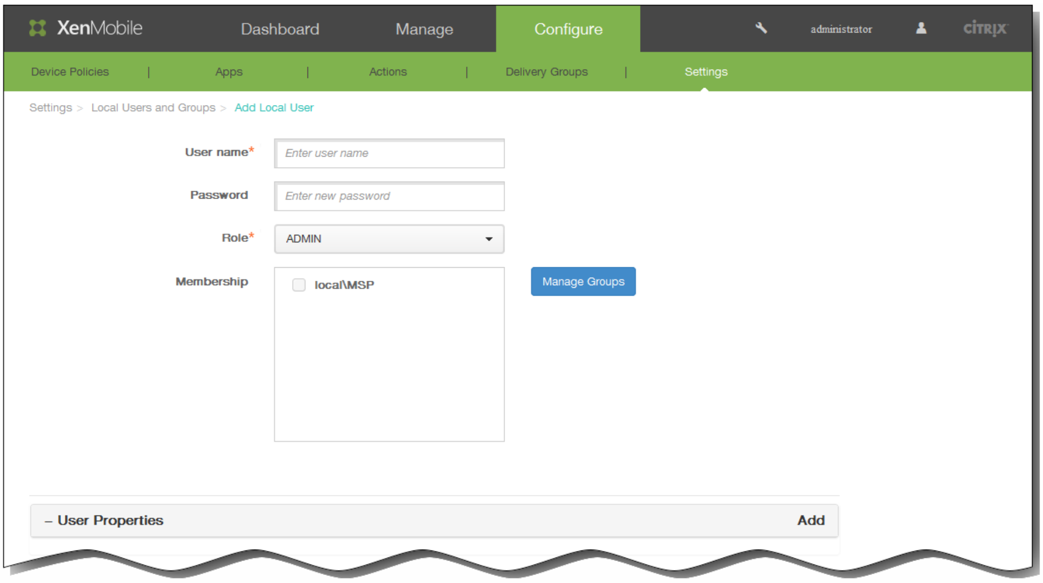


□	User name	Roles	Groups	Created	Last authenticated
□	admin	ADMIN		5/11/15 3:37 PM	5/15/15 10:17 AM
□	adm	ADMIN		5/12/15 5:17 PM	5/12/15 5:17 PM

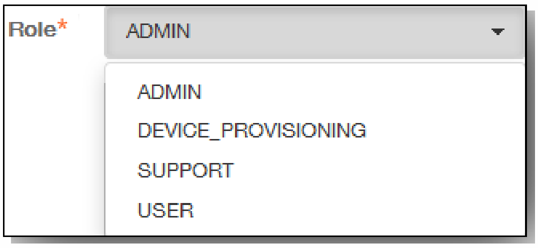
To add a local user

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.

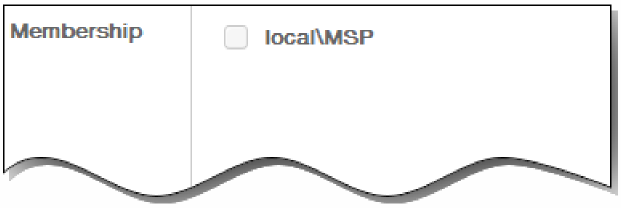
1. On the Local Users and Groups page, click Add. The Add Local User page appears.



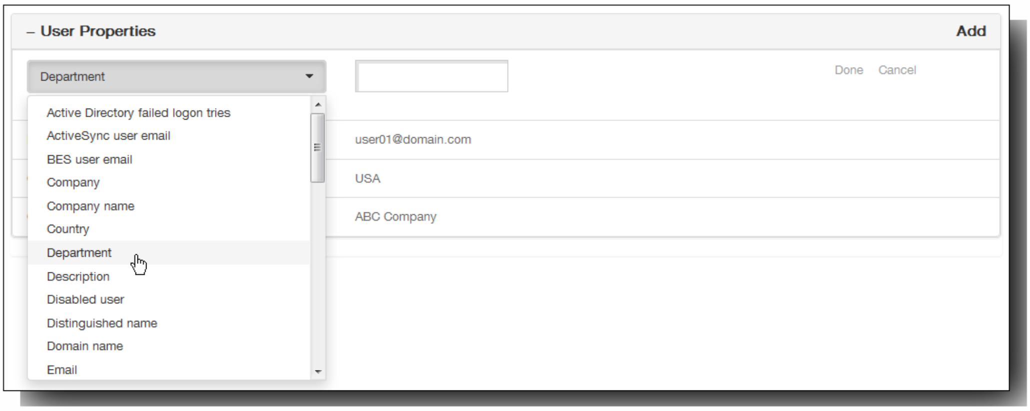
2. Type the following information to add a new local user:
   1. User name: Type the user's name. This is a required field.
   2. Password: Type an optional user password.
   3. Role: In the Role list, click the user's role. For more information about roles, see To create or update custom roles in XenMobile 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.



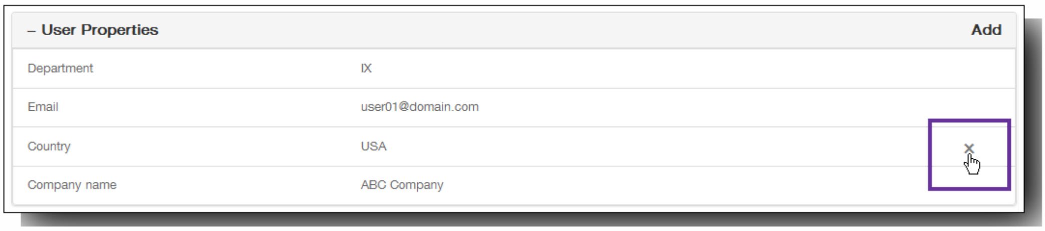
user01@domain.com

USA

ABC Company

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.



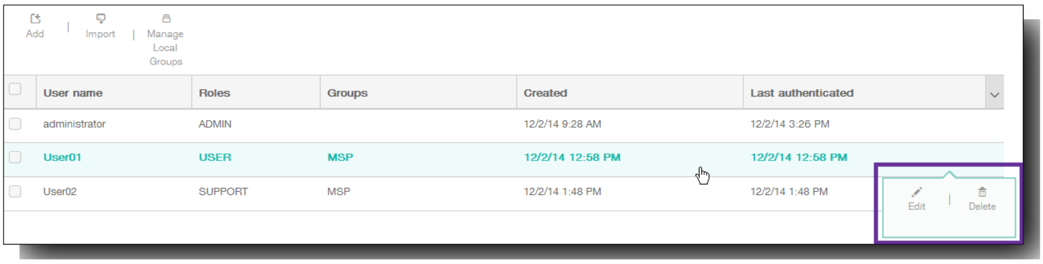
Department	IX
Email	user01@domain.com
Country	USA
Company name	ABC Company

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.



□	User name	Roles	Groups	Created	Last authenticated
□	administrator	ADMIN		12/2/14 9:28 AM	12/2/14 3:26 PM
□	User01	USER	MSP	12/2/14 12:58 PM	12/2/14 12:58 PM
□	User02	SUPPORT	MSP	12/2/14 1:48 PM	12/2/14 1:48 PM

The Edit Local User page appears.

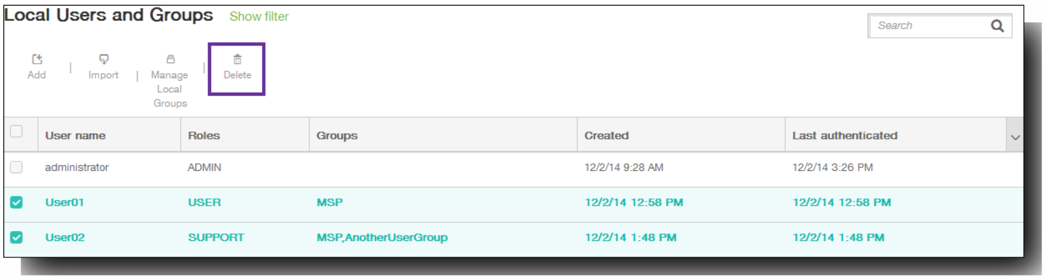
2. Change the following information as appropriate:
   1. User name: Type the user’s name. This is a required field.
   2. Password: Type an optional user password.

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.

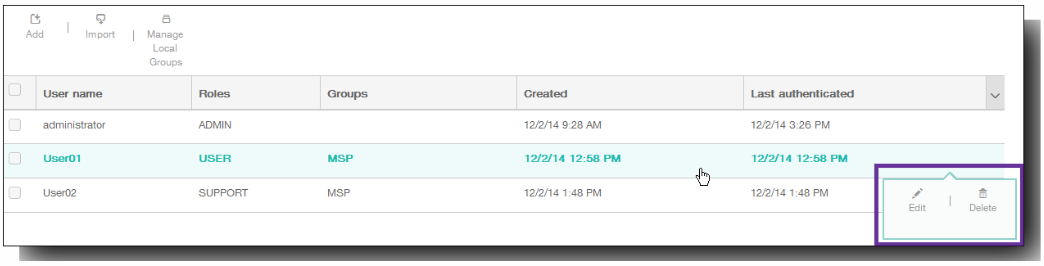
To delete a local user

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.



	User name	Roles	Groups	Created	Last authenticated
□	administrator	ADMIN		12/2/14 9:28 AM	12/2/14 3:26 PM
☑	User01	USER	MSP	12/2/14 12:58 PM	12/2/14 12:58 PM
☑	User02	SUPPORT	MSP,AnotherUserGroup	12/2/14 1:48 PM	12/2/14 1:48 PM

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



	User name	Roles	Groups	Created	Last authenticated
□	administrator	ADMIN		12/2/14 9:28 AM	12/2/14 3:26 PM
□	User01	USER	MSP	12/2/14 12:58 PM	12/2/14 12:58 PM
□	User02	SUPPORT	MSP	12/2/14 1:48 PM	12/2/14 1:48 PM

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

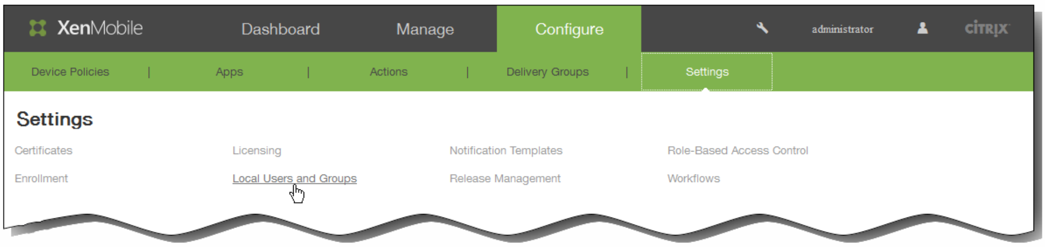
You can import user accounts and properties from a .csv file called a provisioning file, which you can create manually. See Provisioning file formats for information on formatting provisioning files.

Note:

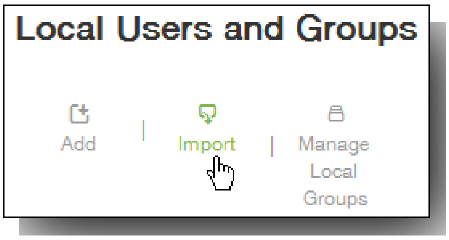
- If you are importing users from an LDAP directory, use the domain name along with the user name in the import file. For example, specify username@domain.com. This syntax prevents additional lookups that will slow the import speed.
- If importing users to the XenMobile internal user directory, disable the default domain in order to speed up the import process. You can reenable the default domain after the import of internal users is completed.
- Local users can be in User Principal Name (UPN) format, but Citrix recommends that you 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.

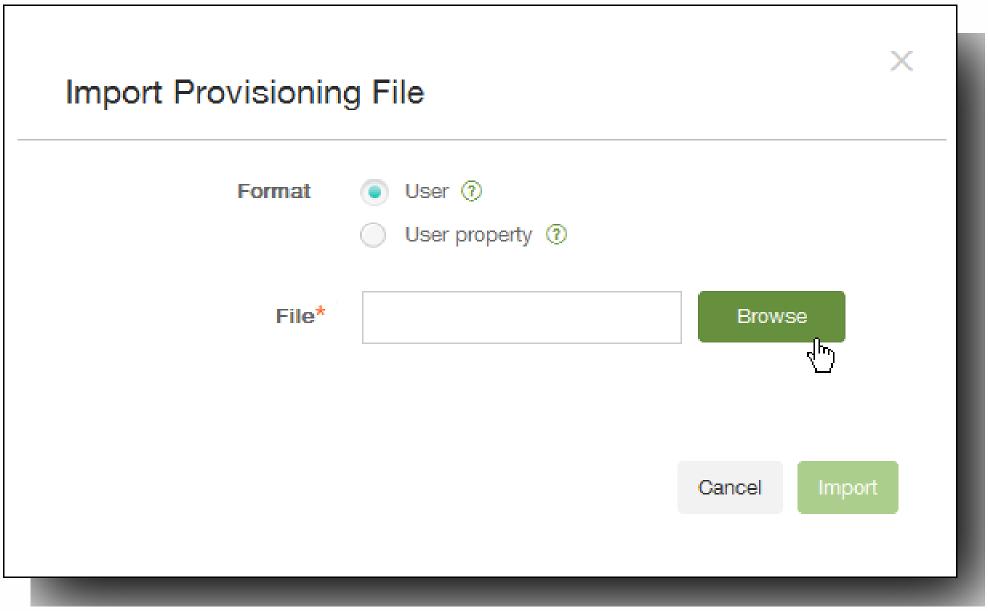


2. On the Local Users and Groups page, click Import.



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.



Format ● User ○ User property

File*

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.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

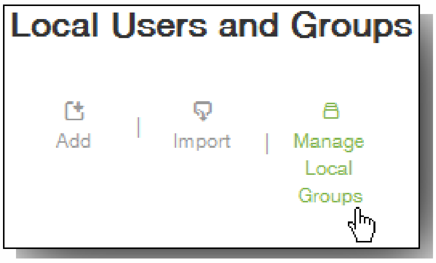
Adding or Removing Groups

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.

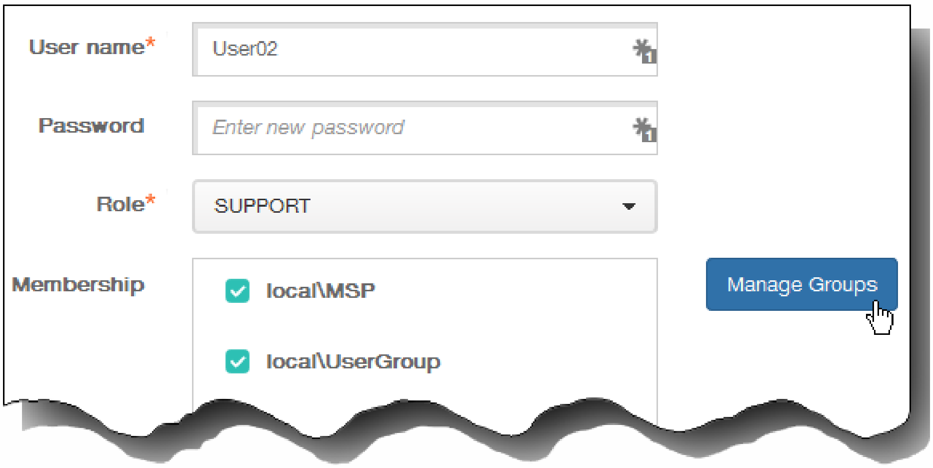
To add a local group

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



Local Users and Groups

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



User name* User02

Password Enter new password

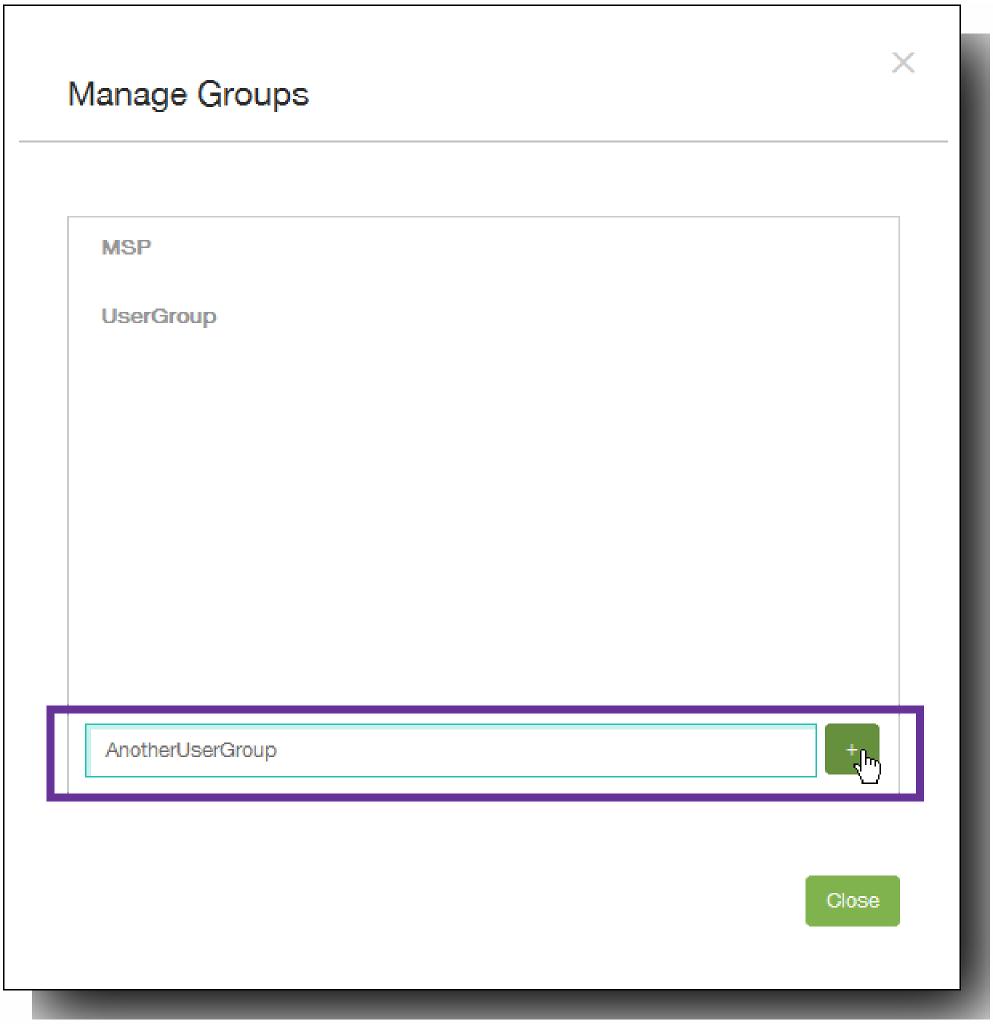
Role* SUPPORT

Membership

☑ local\MSP

☑ local\UserGroup

   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.

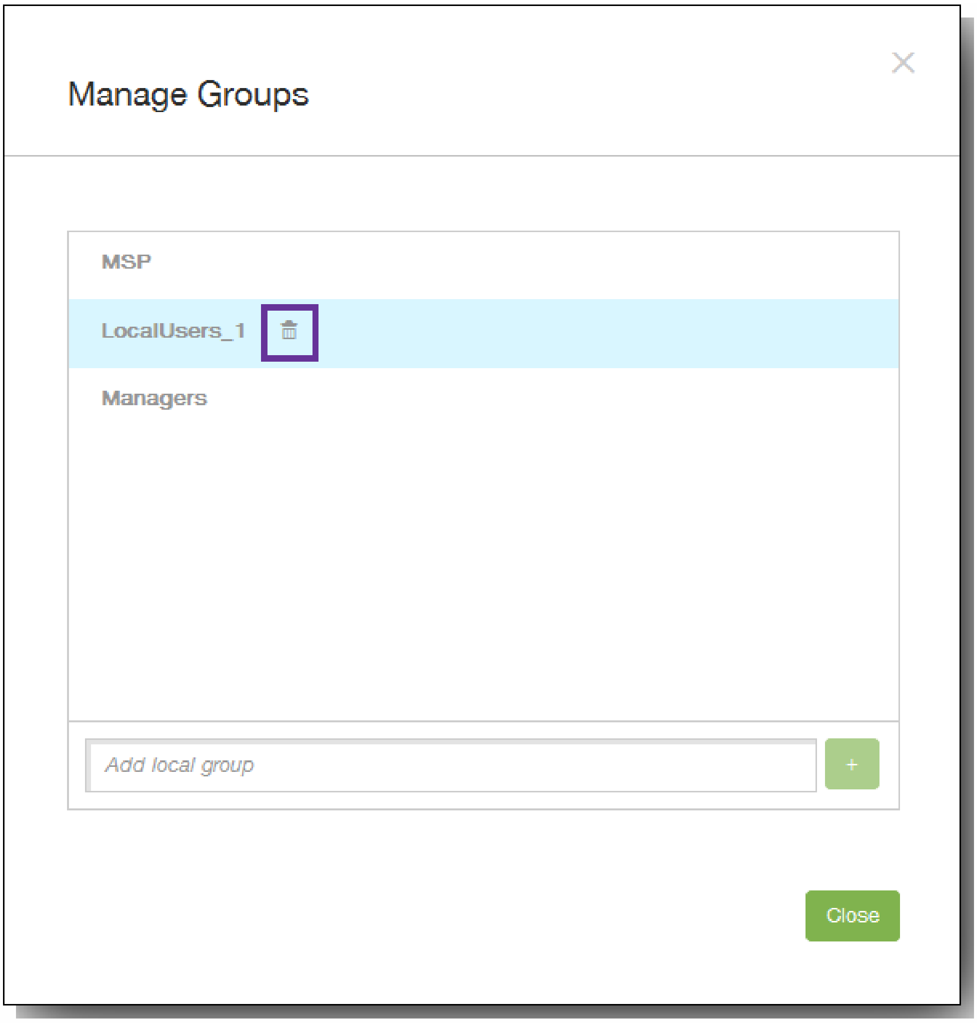
3. Click Close.

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

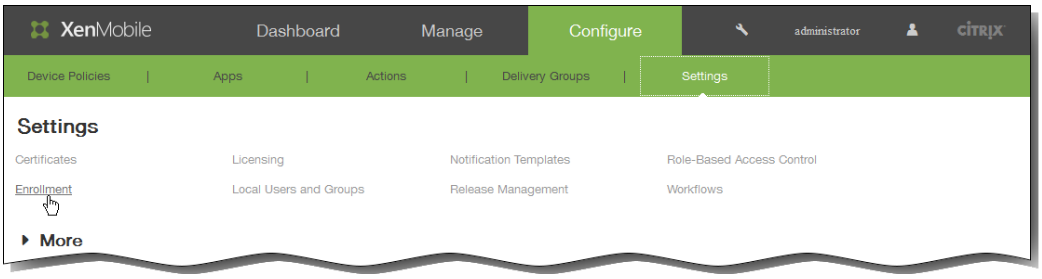
Apr 01, 2015

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.

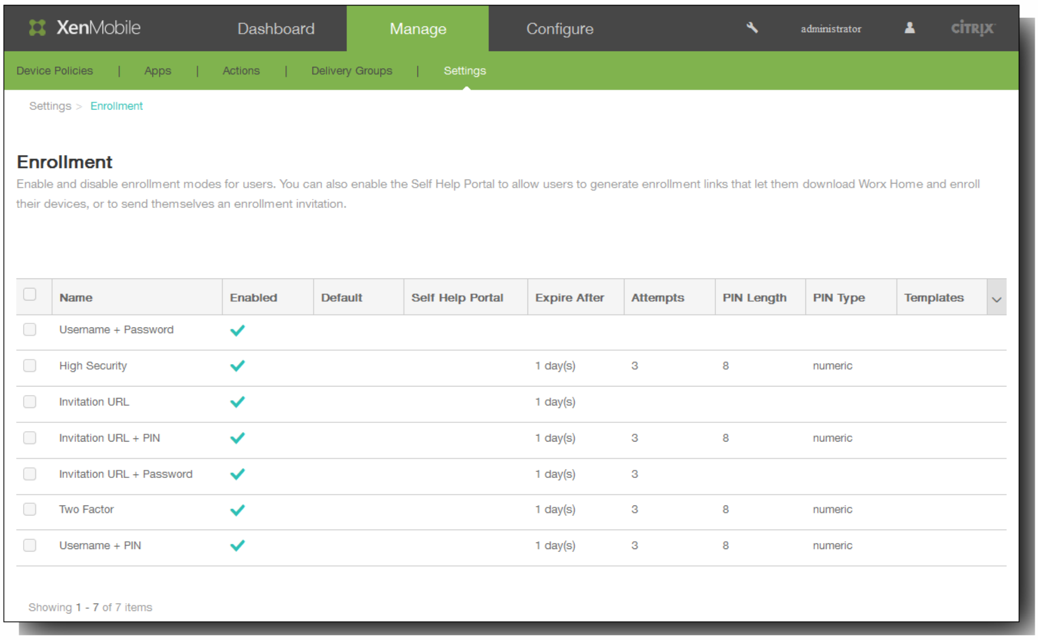
You configure enrollment modes in the XenMobile console from the Settings > Enrollment page. You send enrollment invitations in the XenMobile console from the Manage > Enrollment page (see Enrolling Users and Devices in XenMobile).

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.



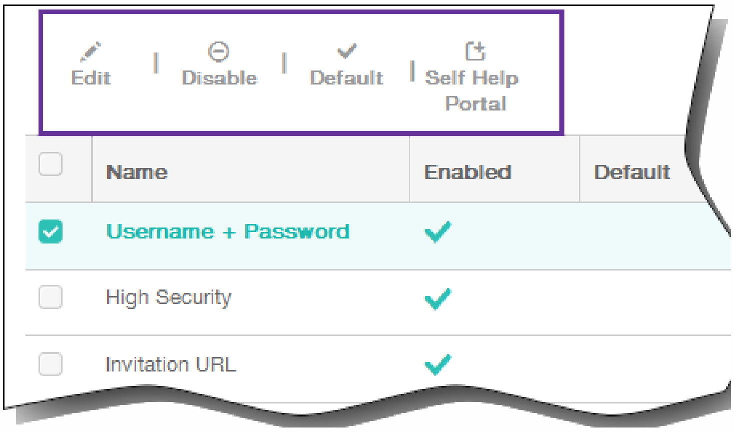
Enrollment

Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Worx Home and enroll their devices, or to send themselves an enrollment invitation.

□	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
□	Username + Password	✓							
□	High Security	✓			1 day(s)	3	8	numeric	
□	Invitation URL	✓			1 day(s)				
□	Invitation URL + PIN	✓			1 day(s)	3	8	numeric	
□	Invitation URL + Password	✓			1 day(s)	3			
□	Two Factor	✓			1 day(s)	3	8	numeric	
□	Username + PIN	✓			1 day(s)	3	8	numeric	

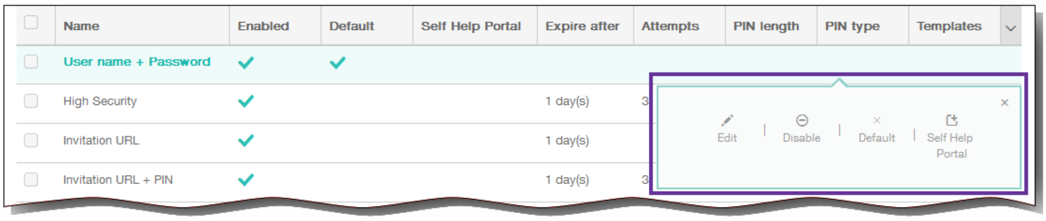
Showing 1 - 7 of 7 items

2. 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.



Edit | Disable | Default | Self Help Portal

□	Name	Enabled	Default
☑	Username + Password	✓	
□	High Security	✓	
□	Invitation URL	✓	

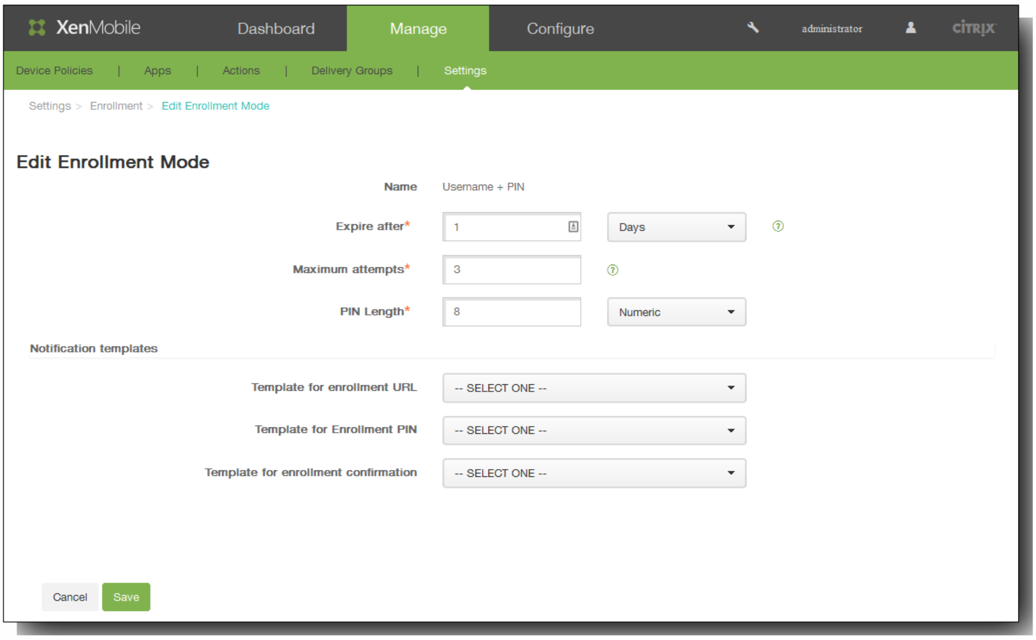


□	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates
□	User name + Password	✓	✓						
□	High Security	✓			1 day(s)	3			
□	Invitation URL	✓			1 day(s)				
□	Invitation URL + PIN	✓			1 day(s)	3			

Edit | Disable | Default | Self Help Portal

To edit an enrollment mode

1. 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.



XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings
Settings > Enrollment > Edit Enrollment Mode

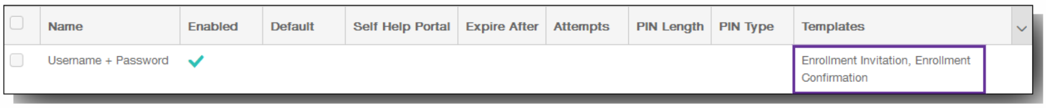
Edit Enrollment Mode

Name	Username + PIN
Expire after*	1 Days
Maximum attempts*	3
PIN Length*	8 Numeric

Notification templates

Template for enrollment URL	-- SELECT ONE --
Template for Enrollment PIN	-- SELECT ONE --
Template for enrollment confirmation	-- SELECT ONE --

2. Change the following information as appropriate:
    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.



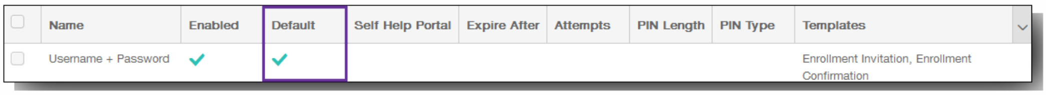
☐	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
☐	Username + Password	✓							Enrollment Invitation, Enrollment Confirmation

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.

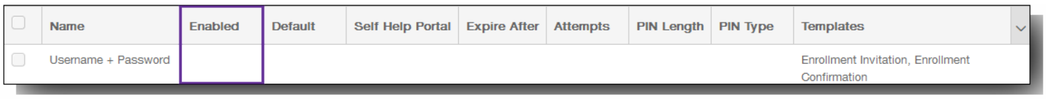


☐	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
☐	Username + Password	✓	✓						Enrollment Invitation, Enrollment Confirmation

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.



□	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
□	Username + Password								Enrollment Invitation, Enrollment Confirmation

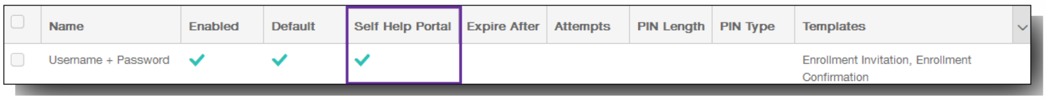
To enable an enrollment mode on the Self Help Portal

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.



□	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
□	Username + Password	✓	✓	✓					Enrollment Invitation, Enrollment Confirmation

Configuring Roles with RBAC

May 20, 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:

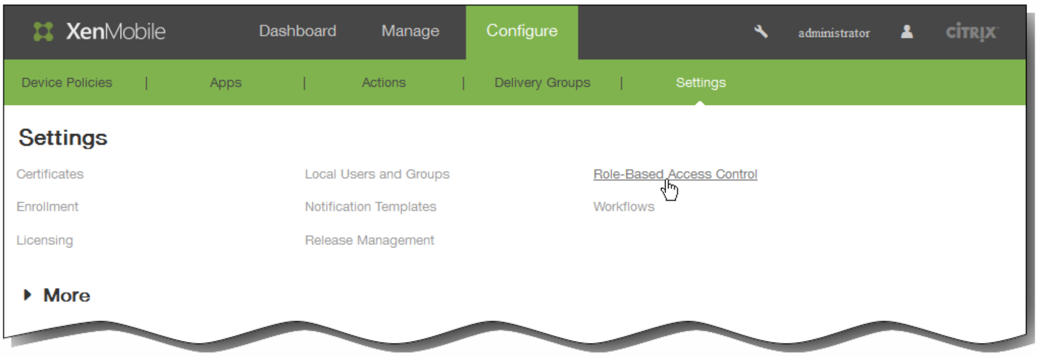
- **Administrator**. Grants full system access.
- **Support**. Grants access to remote support.
- **User**. Used by users who can enroll devices and access the Self Help Portal.

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.

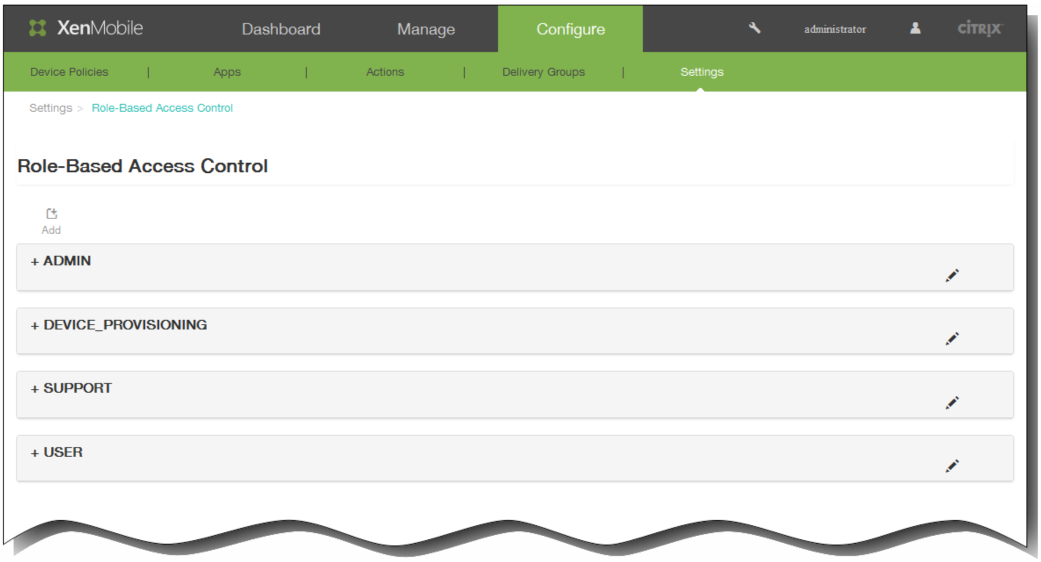
Roles can be assigned to local users (at the user level) or to Active Directory groups (all users in that group have the same permissions). If a user belongs to several Active Directory groups, all the permissions are merged together to define the permissions for that user. For example, if ADGroupA users 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.



Role-Based Access Control

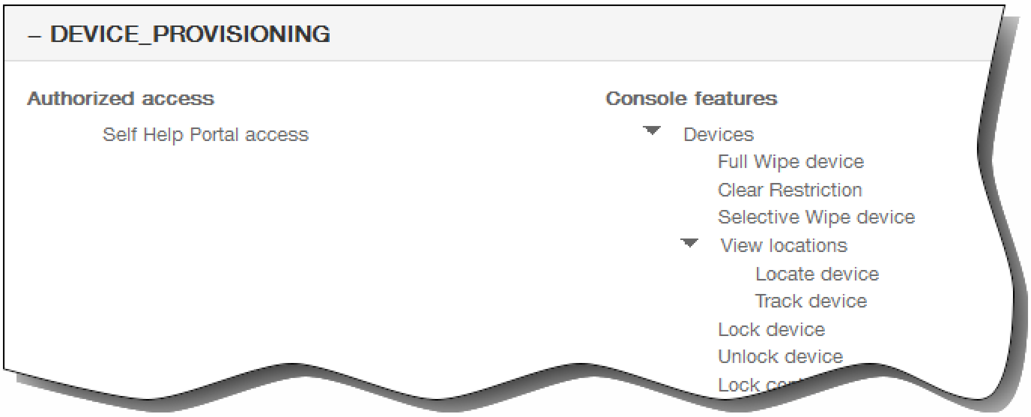
+ ADMIN

+ DEVICE_PROVISIONING

+ SUPPORT

+ USER

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.



– DEVICE_PROVISIONING

Authorized access

Self Help Portal access

Console features

Devices

Full Wipe device

Clear Restriction

Selective Wipe device

View locations

Locate device

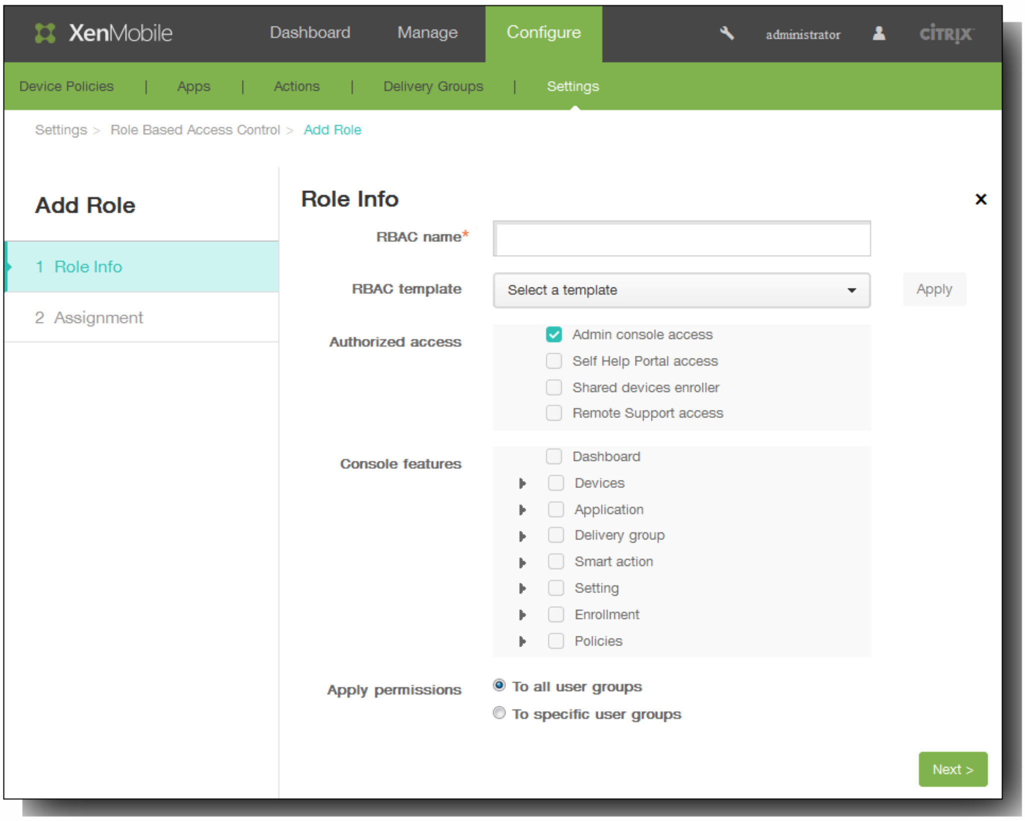
Track device

Lock device

Unlock device

Lock co

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.


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings
Settings > Role Based Access Control > Add Role
Add Role
1 Role Info
2 Assignment
×
Apply
Next >

Role Info

RBAC name*

RBAC template: Select a template

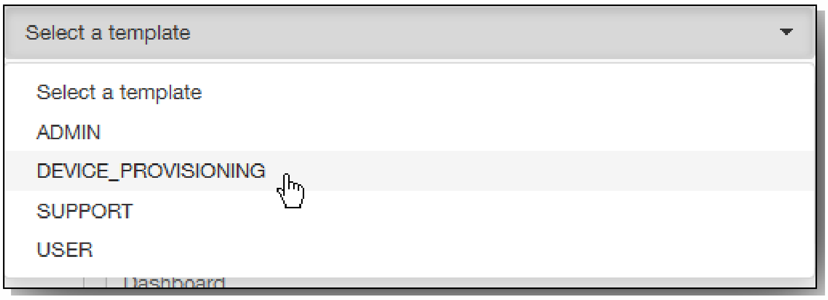
Authorized access:
☑ Admin console access
□ Self Help Portal access
□ Shared devices enroller
□ Remote Support access

Console features:
□ Dashboard
▶ □ Devices
▶ □ Application
▶ □ Delivery group
▶ □ Smart action
▶ □ Setting
▶ □ Enrollment
▶ □ Policies

Apply permissions:
● To all user groups
○ To specific user groups

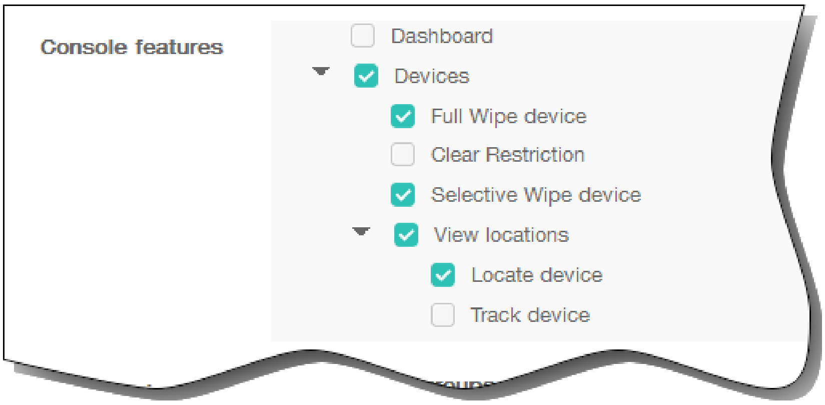
- When you click the trash can icon, a confirmation dialog appears. Click Delete to remove the selected role.

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.

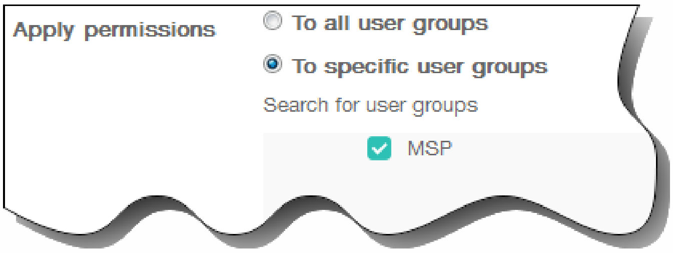
- Select and clear the check boxes in Authorized access and Console features to customize the role.
  Note: If you click the triangle next to a Console feature, permissions specific to that feature appear that you can select and clear. Clicking the top-level check box allows read-only access to that 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.



Console features

- □ Dashboard
- ☑ Devices
  - ☑ Full Wipe device
  - □ Clear Restriction
  - ☑ Selective Wipe device
  - ☑ View locations
    - ☑ Locate device
    - □ Track device

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



Apply permissions

○ To all user groups

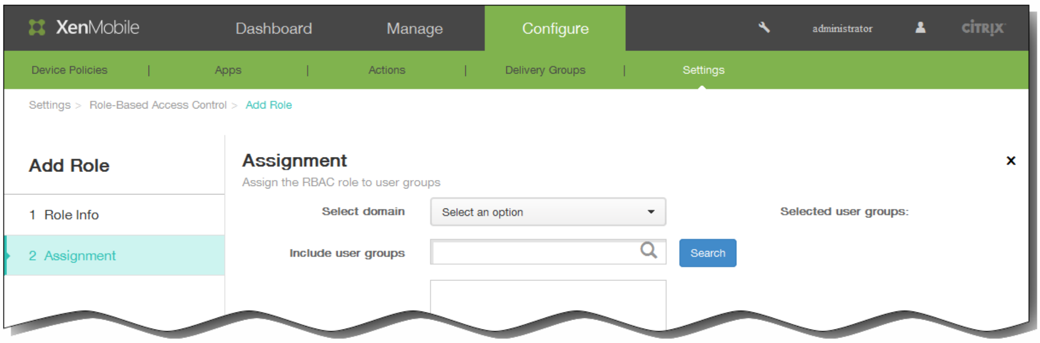
● To specific user groups

Search for user groups

☑ MSP

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.



XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings
Settings > Role-Based Access Control > Add Role
Add Role
1 Role Info
2 Assignment
×
Search

Assignment

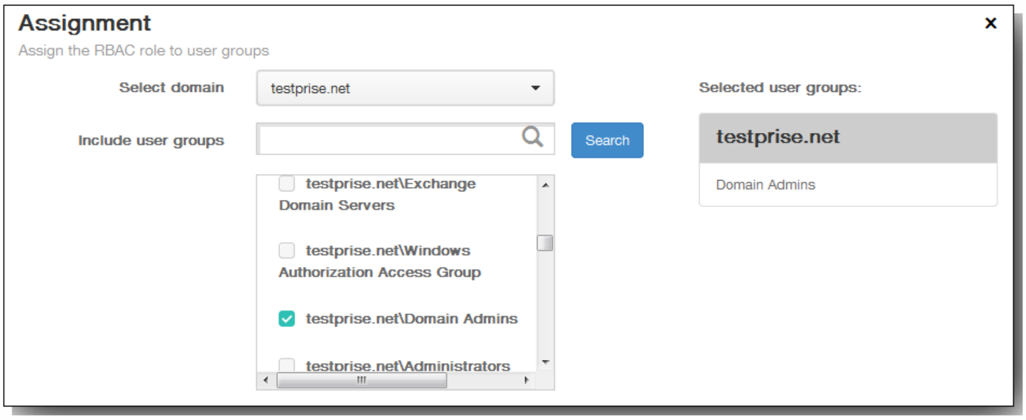
Assign the RBAC role to user groups

Select domain: Select an option

Include user groups:

Selected user groups:

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 the Selected user groups list.



Assignment

Assign the RBAC role to user groups

Select domain: testprise.net

Include user groups:

□ testprise.net\Exchange Domain Servers

□ testprise.net\Windows Authorization Access Group

☑ testprise.net\Domain Admins

□ testprise.net\Administrators

Selected user groups:

testprise.net

Domain Admins

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.

RBAC Roles and Permissions

Jul 28, 2015

Each predefined role-based access control (RBAC) role has certain access and feature permissions associated with the role. This article describes what each of those permissions does. For more information on how to configure RBAC roles, see Configuring roles with RBAC.

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 autodiscovery using the Autodiscovery Service portal at https://xenmobiletools.citrix.com, open a Technical Support case using the Citrix Support portal and then provide the following information:
   - The domain containing the accounts with which users will enroll.
   - The XenMobile server fully qualified domain name (FQDN).
   - The XenMobile instance name. By default, the instance name is zdm and is case-sensitive.
   - User ID Type, which can be either UPN or Email. By default, the type is UPN.
   - The port used for iOS enrollment if you changed the port number from the default port 8443.
   - The port through which the XenMobile server accepts connections if you changed the port number from the default port 443.
   - Optionally, an email address for your XenMobile administrator.
2. If you plan to enroll Windows devices, do the following:
   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).

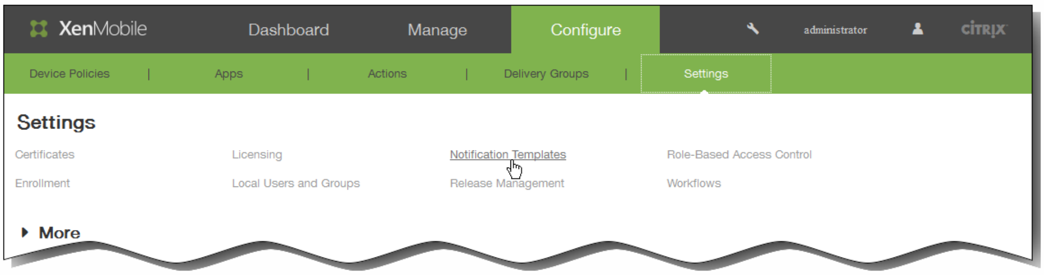
Creating and Updating Notification Templates

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.

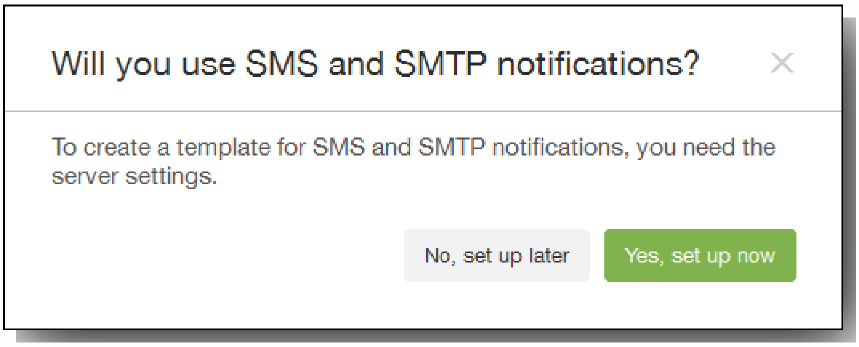
1. In the XenMobile console, click Configure > Settings > Notification Templates.



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.



Will you use SMS and SMTP notifications?

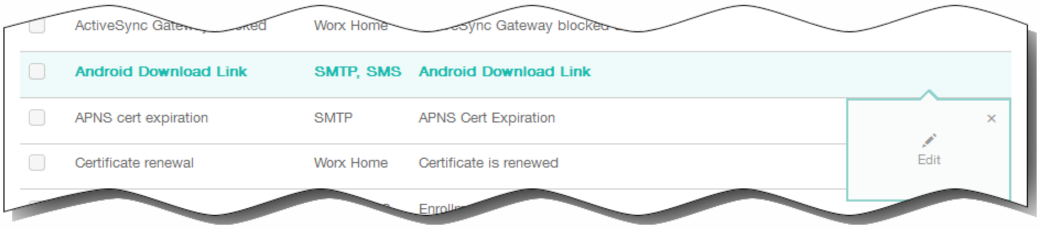
To create a template for SMS and SMTP notifications, you need the server settings.

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

     Note:

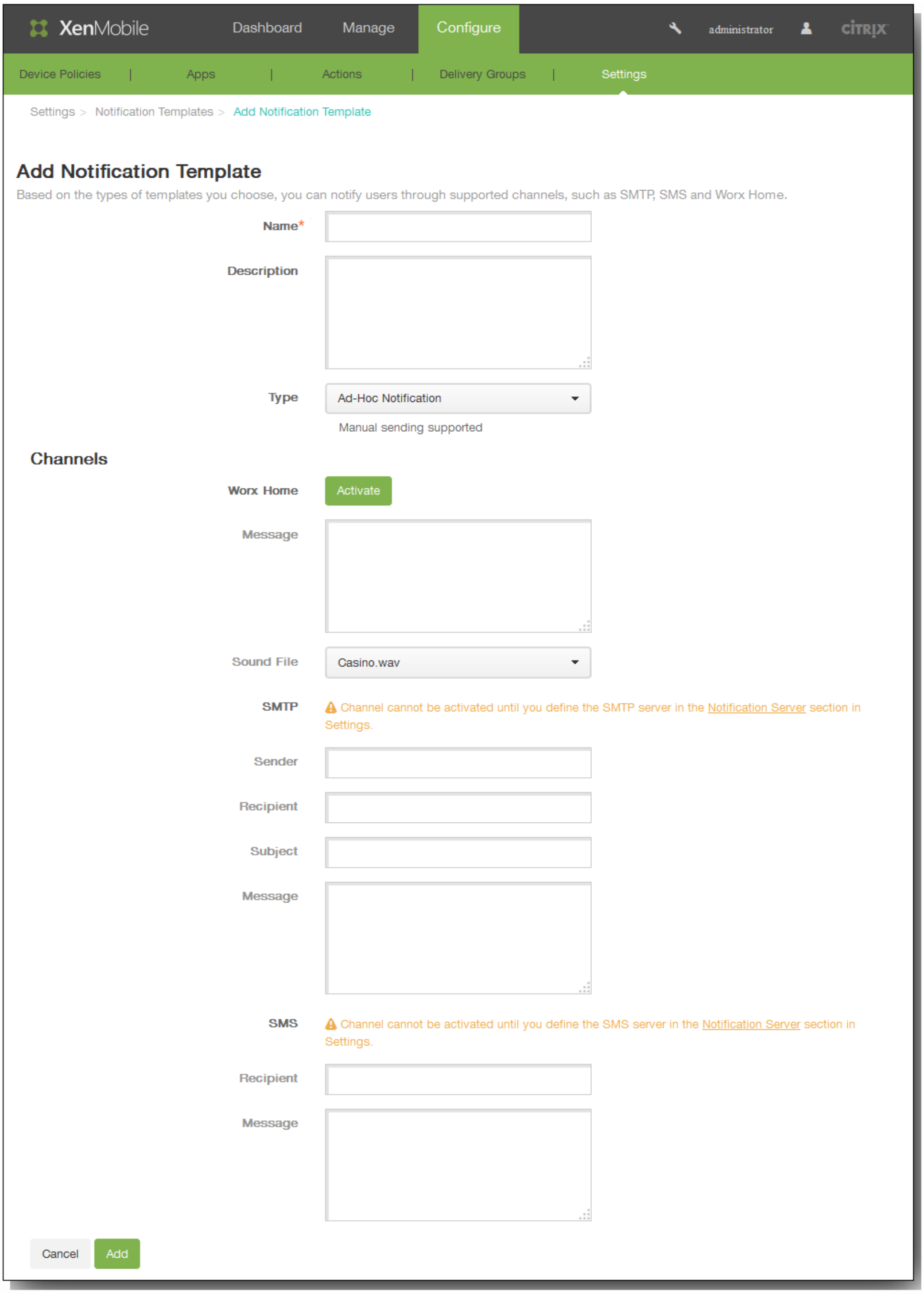
     - You can delete only notification templates that you have added; you cannot delete predefined notification templates.

- 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.



☐	ActiveSync Gate… ked	Worx Home	…Sync Gateway blocked
☐	Android Download Link	SMTP, SMS	Android Download Link
☐	APNS cert expiration	SMTP	APNS Cert Expiration
☐	Certificate renewal	Worx Home	Certificate is renewed
			Enroll…

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


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings
Settings > Notification Templates > Add Notification Template

Add Notification Template

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

Name*

Description

Type: Ad-Hoc Notification

Manual sending supported

Channels

Worx Home: Activate

Message

Sound File: Casino.wav

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(smg_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

May 02, 2016

Device configuration and management typically involves creating resources (policies and apps) and actions in the XenMobile console and then packaging them using delivery groups. The order in which XenMobile pushes resources and actions in a delivery group to devices is referred to as the deployment order. This article describes how to add, manage, and deploy delivery groups; how to change the deployment order of resources and actions in delivery groups; and how XenMobile determines deployment order when a user is in multiple delivery groups that have duplicate or conflicting policies.

Delivery groups specify the category of users to whose devices you deploy combinations of policies, apps, and actions. Inclusion in a delivery group is usually based on users' characteristics, such as company, country, department, office address, title, and so on. Delivery groups give you greater control over who gets what resources and when they get them. You can deploy a delivery group to everyone or to a more narrowly defined group of users.

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

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

Deployment Ordering

Deployment order is the sequence in which XenMobile pushes resources to devices. When determining deployment order, XenMobile applies filters and control criteria, such as deployment rules and deployment schedule, to policies, apps, actions, and delivery groups. Before adding delivery groups, consider how the information in this section relates to your deployment goals.

Here's a summary of the main concepts related to deployment order:

- **Deployment order:** The sequence in which XenMobile pushes resources (policies and apps) and actions to a device.
- **Deployment rules:** XenMobile uses the deployment rules that you specify for device properties to filter policies, apps, actions, and delivery groups. For example, a deployment rule might specify to push the deployment package when a domain name matches a particular value.
- **Deployment schedule:** XenMobile uses the deployment schedule that you specify for actions, apps, and device policies to control deployment of those items. You can specify that a deployment occurs immediately, on a particular date and time, or according to deployment conditions.

The following table shows those and other criteria that you can associate with specific objects or resources to filter them or control their deployment.

Object/Resource	**Filter/Control Criteria**
	Device platform

Device policy	Deployment rule (based on device properties) Deployment schedule
App	Device platform Deployment rule (based on device properties) Deployment schedule
Action	Deployment rule (based on device properties) Deployment schedule
Delivery group	User/Groups Deployment rule (based on device properties)

It is very likely that, in a typical environment, multiple delivery groups become assigned to a single user, with the following possible results:

- Duplicate objects exist within the delivery groups.
- A specific policy is configured differently in more than one delivery group that is assigned to a user.

When either of those situations occur, XenMobile calculates a deployment order for all of the objects that it must deliver to a device or act upon. The calculation steps are independent of the device platform.

Calculation steps:

1. Determine all of the delivery groups for a specific user, based upon the filters of user/groups and the deployment rules.
2. Create an ordered list of all resources (policies, actions and apps) within the selected delivery groups that apply based on the filters of device platform, deployment rules and deployment schedule. The ordering algorithm is as follows:

a. Place resources from delivery groups that have a user-defined deployment order ahead of those without one. The rationale for this is described after these steps.

b. As a tie-breaker among delivery groups, order resources from delivery groups by delivery group name. For example, place resources from delivery group A ahead of those from delivery group B.

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

d. If the same resource appears more than once, then remove the duplicate resource.

Resources that have a user-defined order associated with them deploy prior to resources without a user-defined order. A resource can exist in multiple delivery groups assigned to user. As indicated in the steps above, the calculation algorithm removes redundant resources and only delivers the first resource in this list. By removing duplicate resources in that way, XenMobile enforces the order defined by the XenMobile administrator.

For example, suppose that you have two delivery groups as follows:

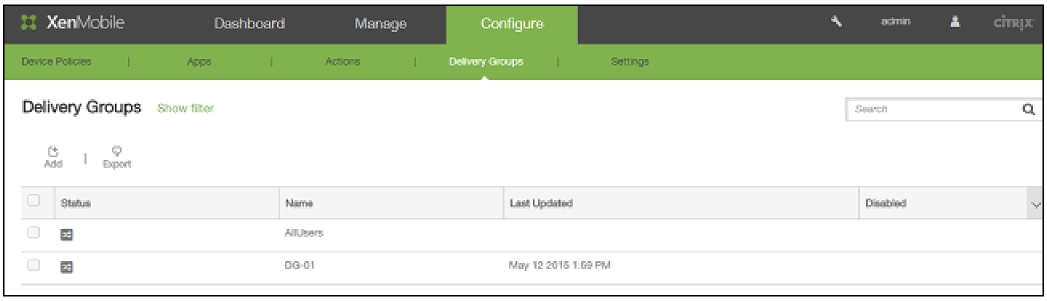
- Delivery group A: With **unspecified** order for resources (RES); contains RES1 and RES2.
- Delivery group B: With **specified** order for resources; contains RES3 and RES2. In this case, you want to deliver RES3 before RES2.

If the calculation algorithm only ordered deployment groups by name, XenMobile would perform the deployment in this order: RES1, RES2, RES3. XenMobile would ignore RES2, a duplicate, from delivery group B.

However, the calculation algorithm places resources from delivery group B higher in the list over those from delivery group A, so that XenMobile deploys in this order: RES3, RES2, RES1. XenMobile ignores RES2 from delivery group A, as it is a duplicate. That algorithm therefore respects the order specified by the XenMobile administrator.

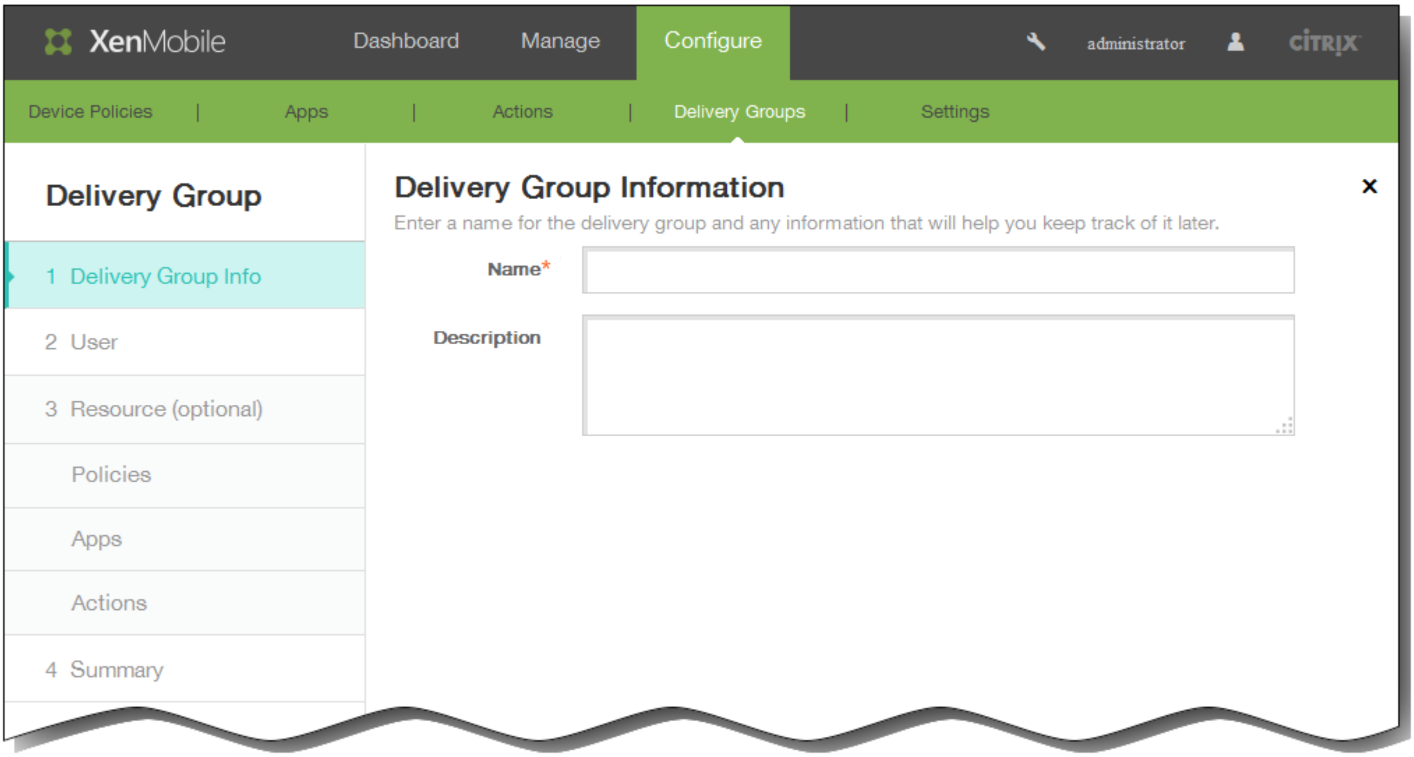
To add a delivery group

1. In the XenMobile console, click **Configure > Delivery Groups**. The **Delivery Groups** page appears.



□	Status	Name	Last Updated	Disabled
□		AllUsers		
□		DG-01	May 12 2016 1:59 PM	

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

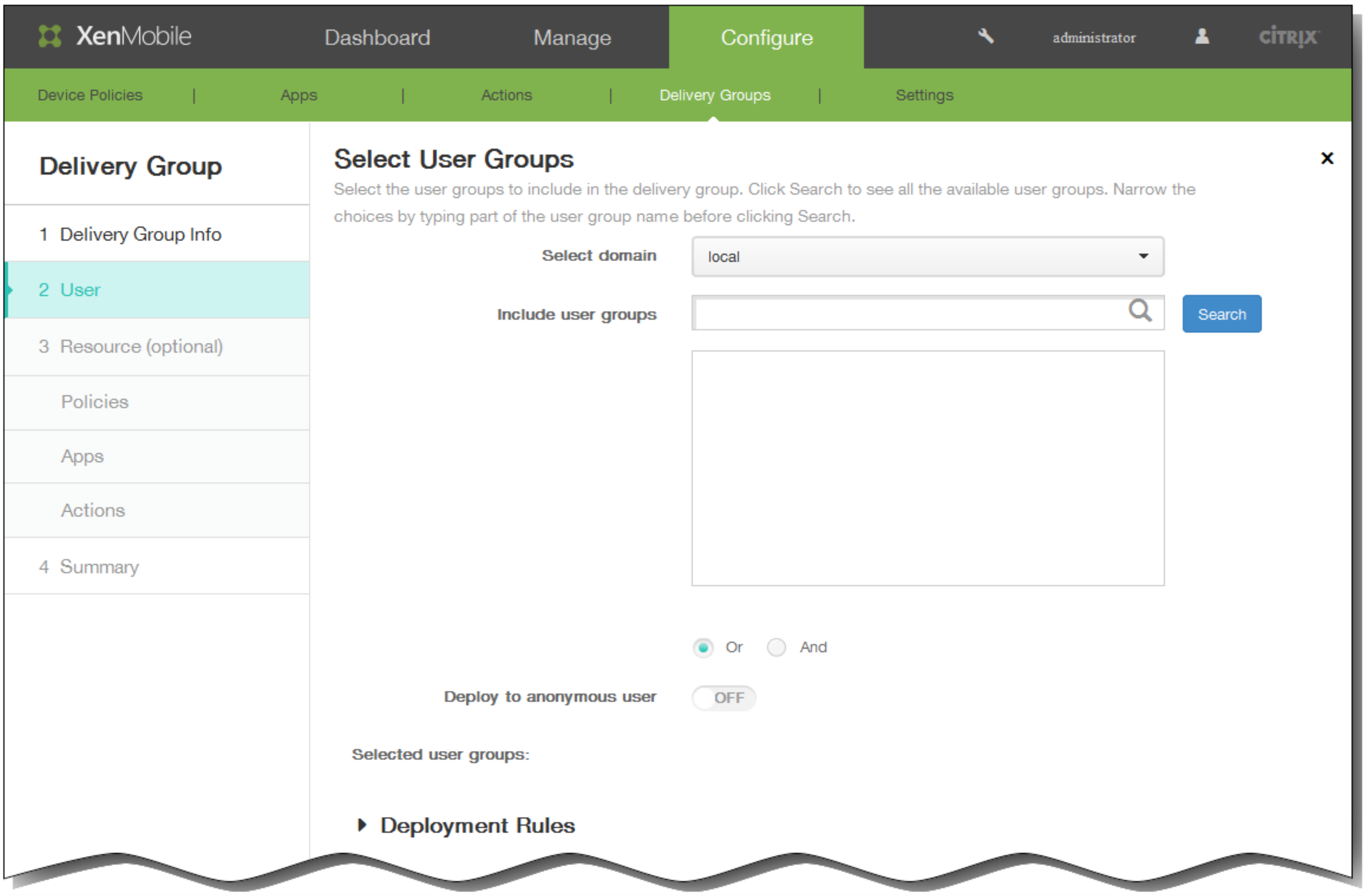


3. In the **Delivery Group Information** page, enter the following information:

Name: Type a descriptive name for the delivery group.

Description: Type an optional description of the delivery group.

4. Click **Next**. The **Delivery Group User** page appears.



Select User Groups

Select the user groups to include in the delivery group. Click Search to see all the available user groups. Narrow the choices by typing part of the user group name before clicking Search.

Select domain: local

Include user groups:

● Or ○ And

Deploy to anonymous user: OFF

Selected user groups:

▸ Deployment Rules

5. In the **Select User Groups** page, enter the following information:

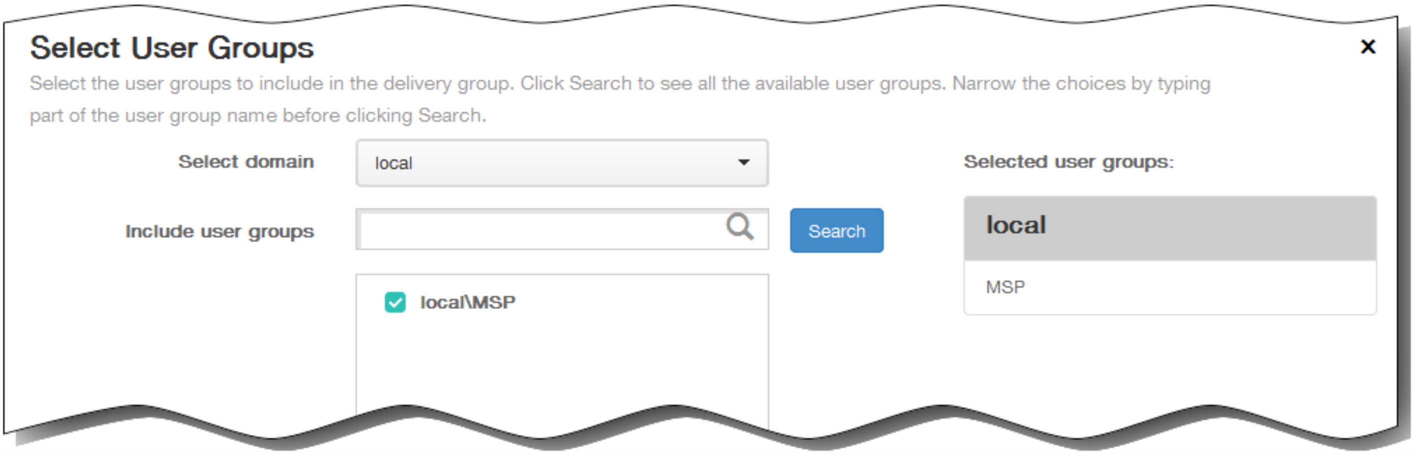
a. **Select domain**: From the list, select the domain from which to choose users.

b. **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.

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



Select User Groups

Select the user groups to include in the delivery group. Click Search to see all the available user groups. Narrow the choices by typing part of the user group name before clicking Search.

Select domain: local

Include user groups:

☑ local\MSP

Selected user groups:

local

MSP

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.

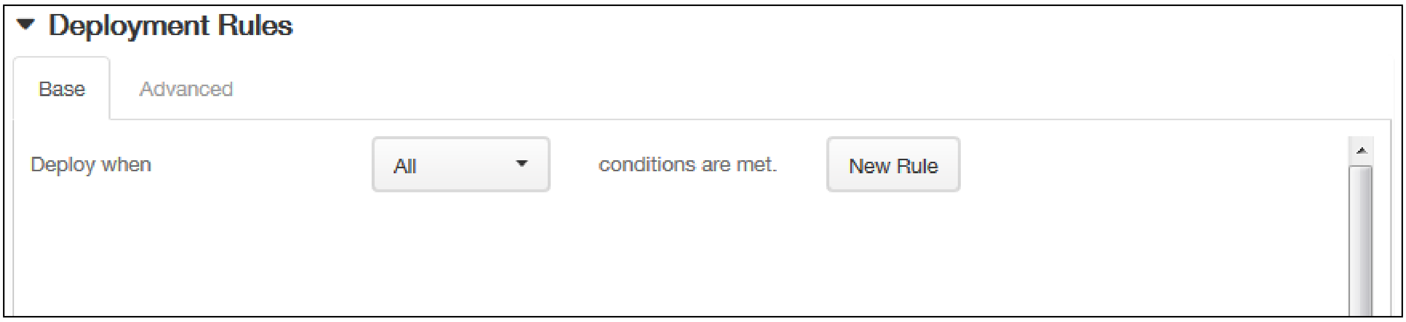
User groups in the **Selected user groups** list have check marks next to their name in the resulting list. Scroll through the list and clear the check box next to each group you want to remove.

d. **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.

e. **Deploy to anonymous user**: Select whether to deploy to unauthenticated users in the delivery group.

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

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



Deployment Rules

Deploy when All conditions are met.

a. In the lists, click options to determine when the policy should be deployed.

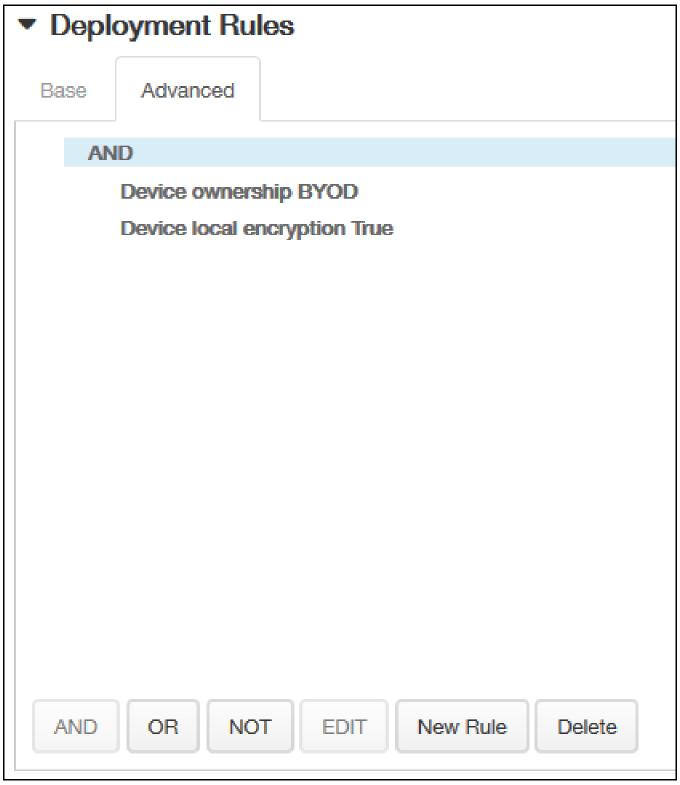
(1) You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is **All**.

(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.

b. Click the **Advanced** tab to combine the rules with Boolean options.



The conditions you chose on the **Base** tab appear.

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

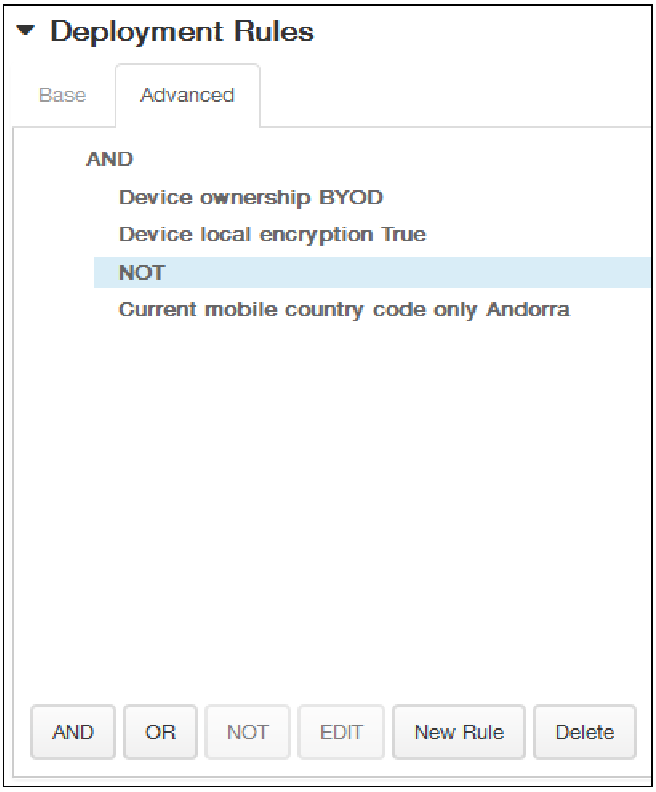
(1) Click **AND**, **OR**, or **NOT**.

(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**.

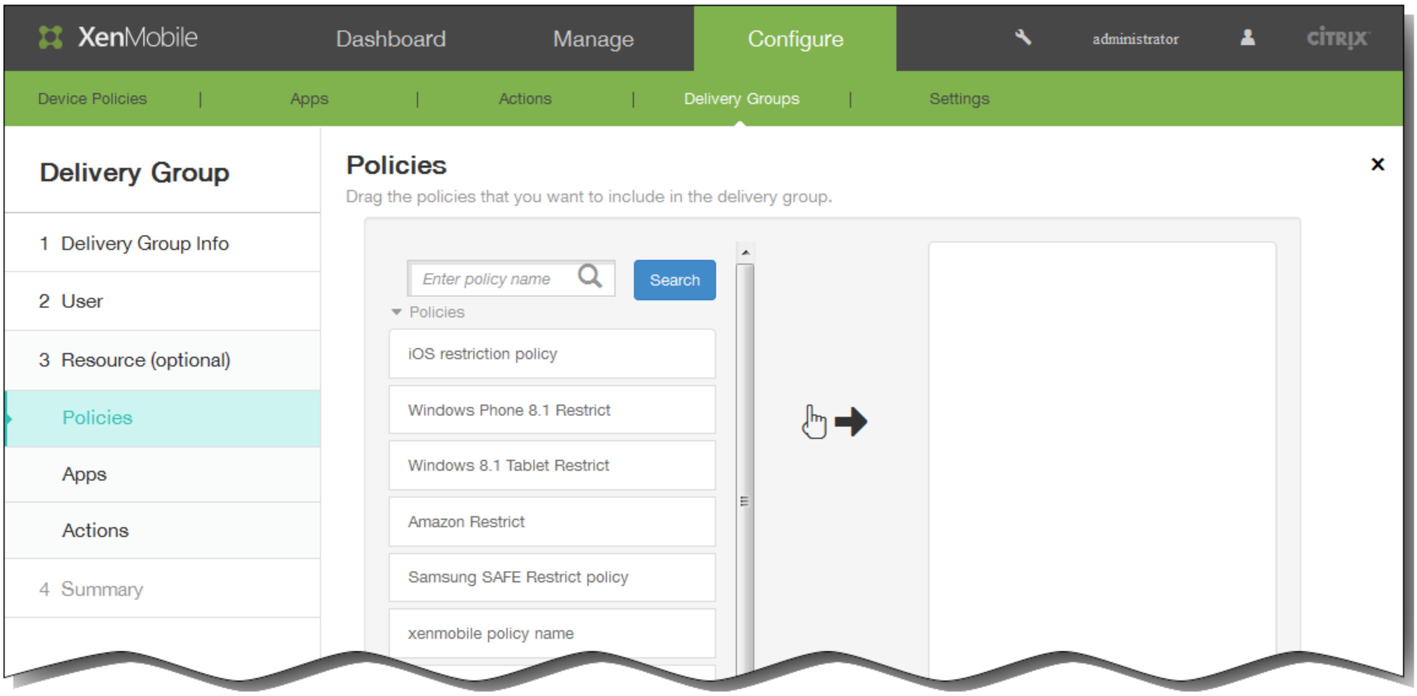


AND
Device ownership BYOD
Device local encryption True
NOT
Current mobile country code only Andorra

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



Policies

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

iOS restriction policy

Windows Phone 8.1 Restrict

Windows 8.1 Tablet Restrict

Amazon Restrict

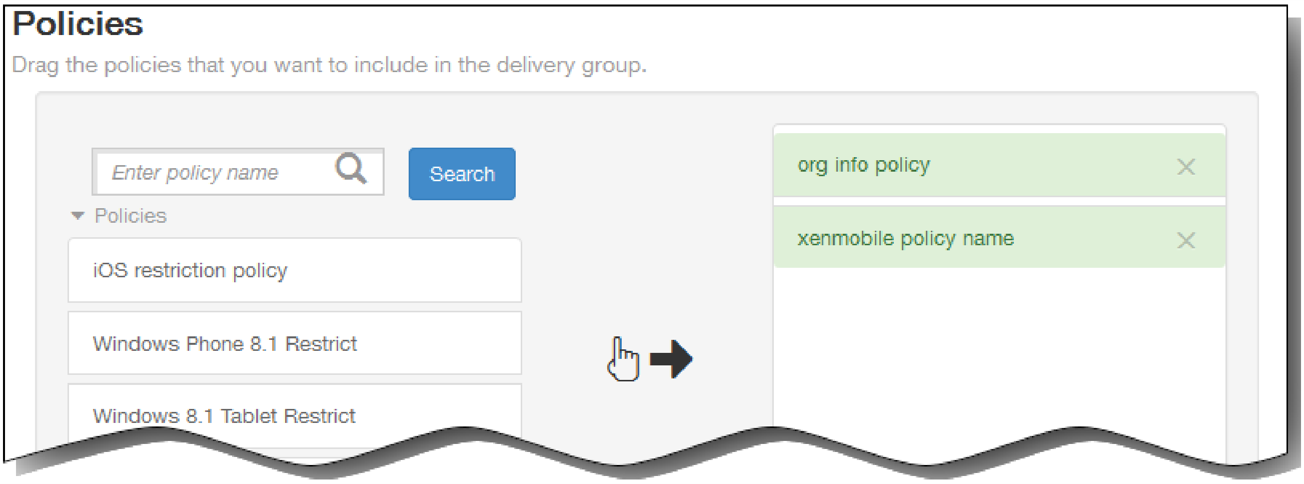
Samsung SAFE Restrict policy

xenmobile policy name

a. Scroll through the list of available polices 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**.

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

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



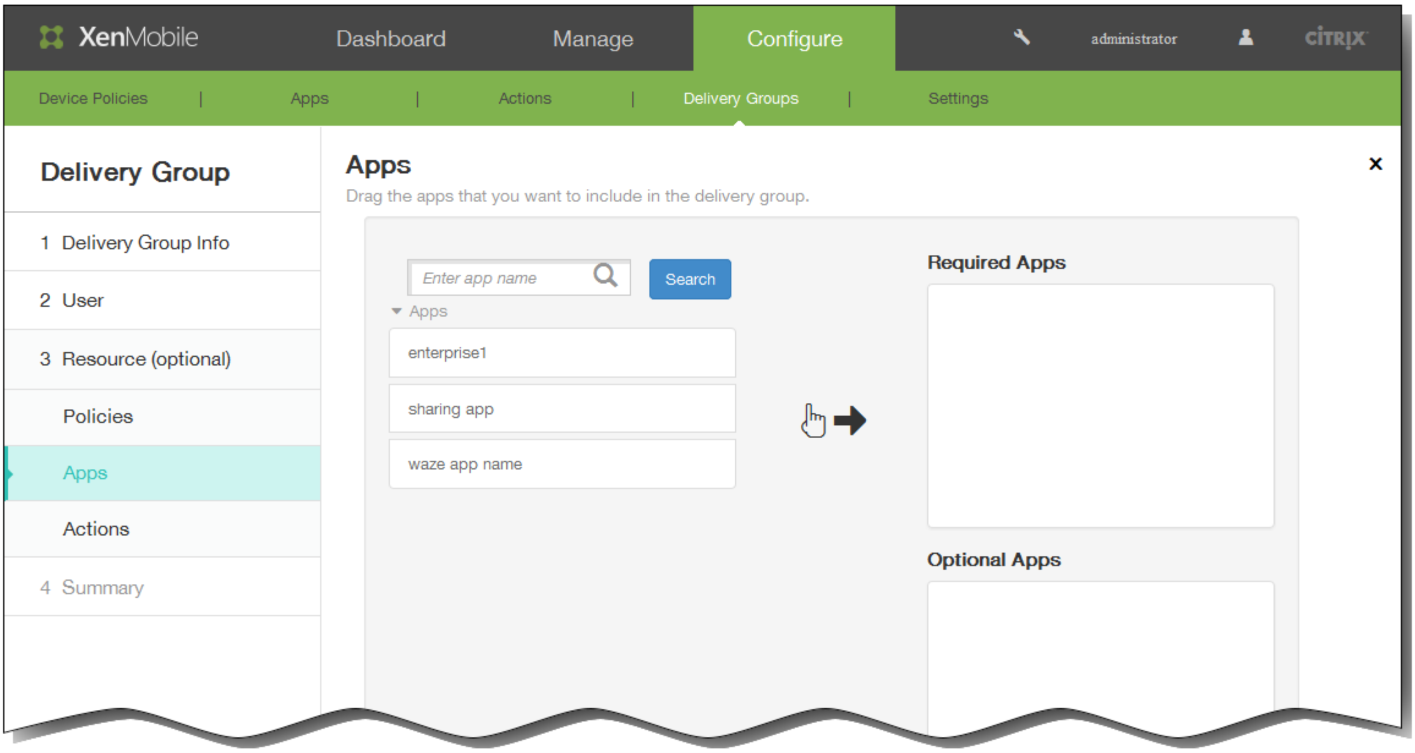
Policies

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

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

e. 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.

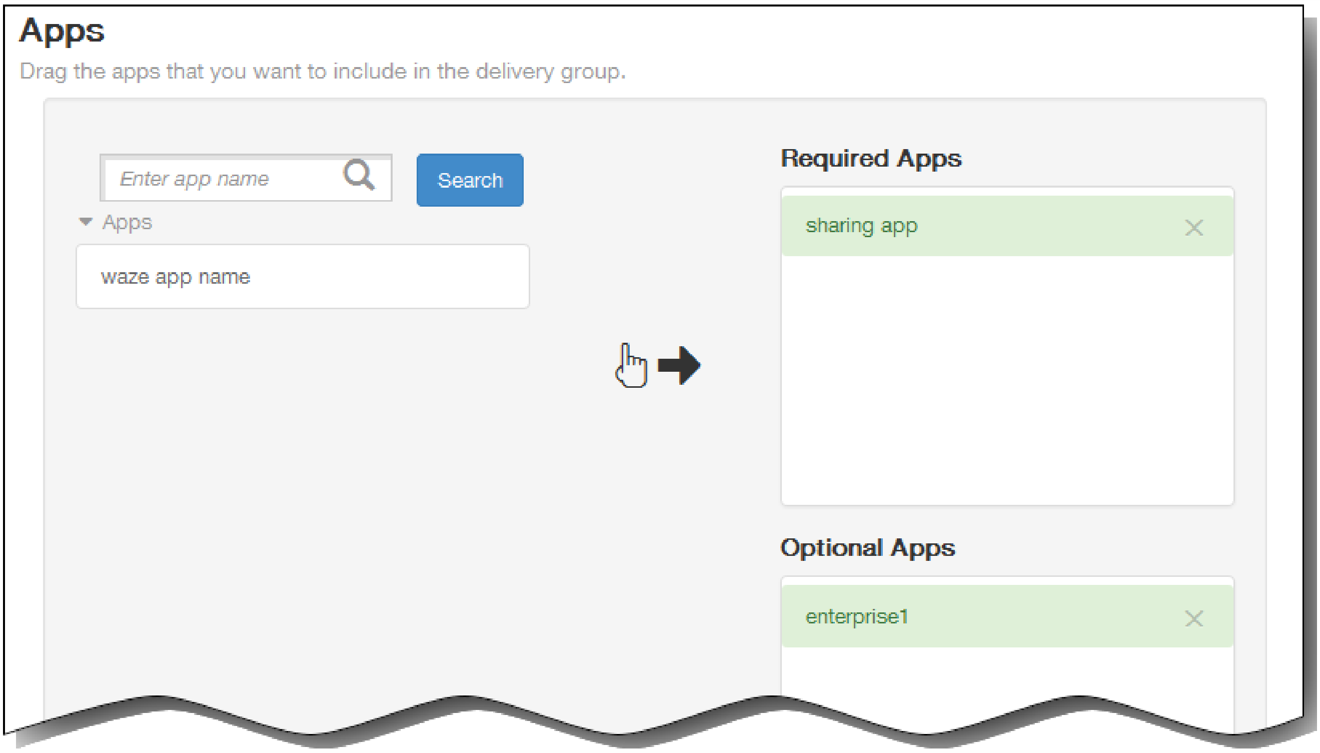
To add Apps



a. 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**.

b. Click an app and drag it into either the **Required Apps** box or the **Optional Apps** box.

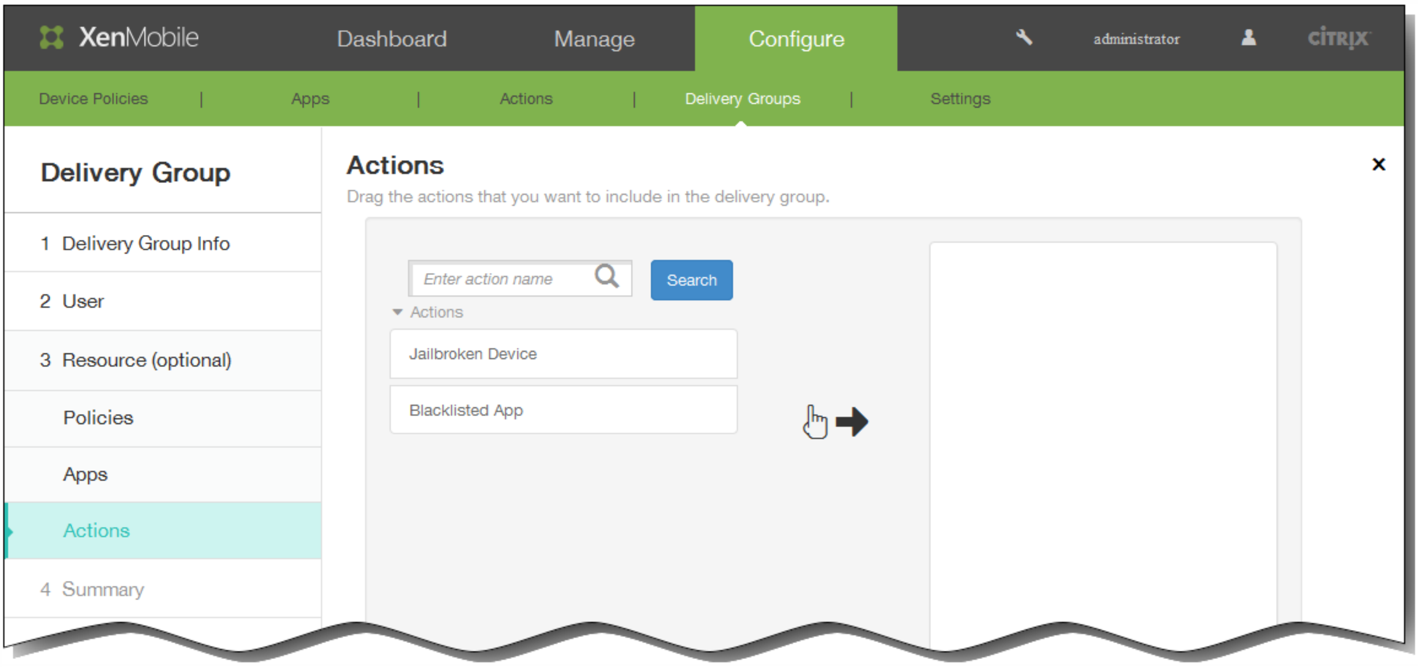
c. Repeat steps a and b to add more apps.



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

e. 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.

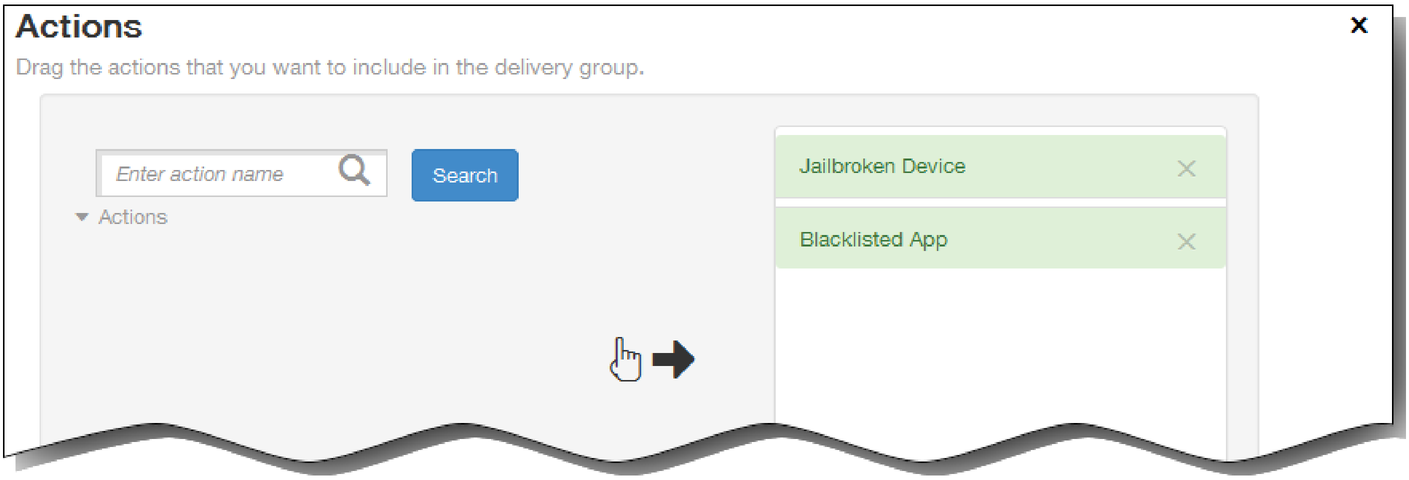
To add Actions



a. 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**.

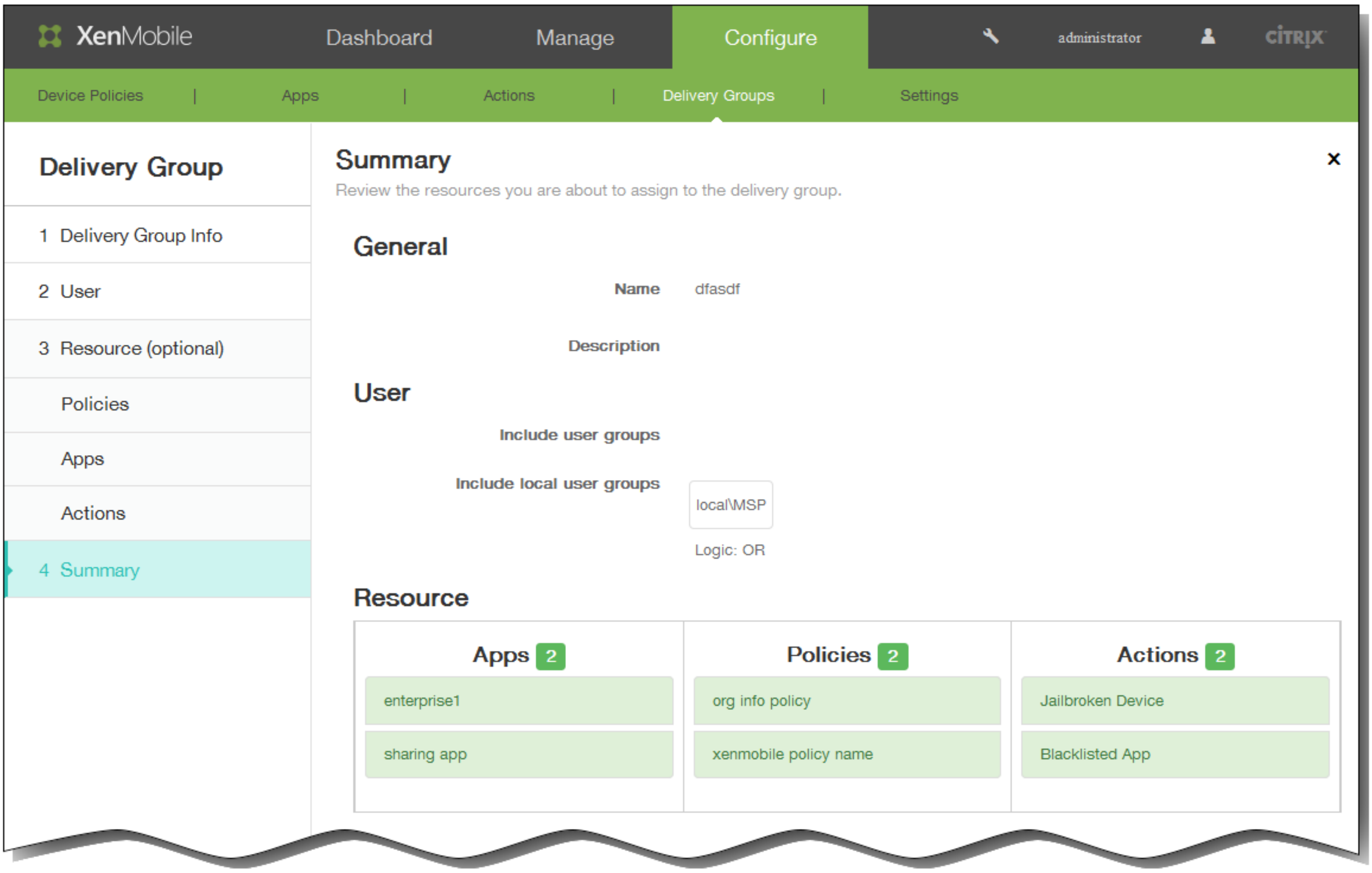
b. Click an action and drag it into the right-hand box.

c. Repeat steps a and b to add more actions.



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

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



Summary

Review the resources you are about to assign to the delivery group.

General

Name: dfasdf

Description:

User

Include user groups:

Include local user groups: local\MSP

Logic: OR

Resource

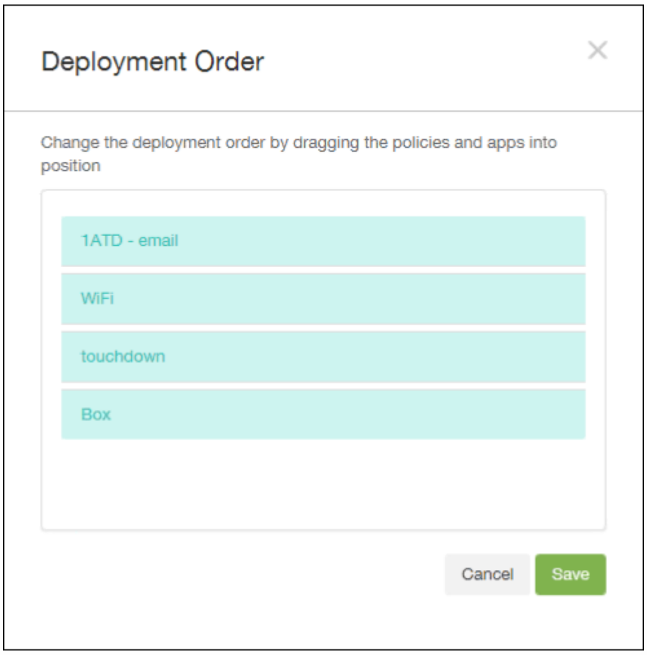
Apps 2	Policies 2	Actions 2
enterprise1	org info policy	Jailbroken Device
sharing app	xenmobile policy name	Blacklisted App

8. On the **Summary** page, you can review the options you have configured for the delivery group and change the deployment order of resources. Click **Back** to return to previous pages to make any necessary adjustments to the configuration. Click **Deployment Order** to reorder the resource deployment order; for more information on changing deployment order, see To change deployment order.

9. Click **Save** to save the delivery group.

To change deployment order

1. Click the **Deployment Order** button. The **Deployment Order** dialog box appears.



Deployment Order

Change the deployment order by dragging the policies and apps into position

1ATD - email

WiFi

touchdown

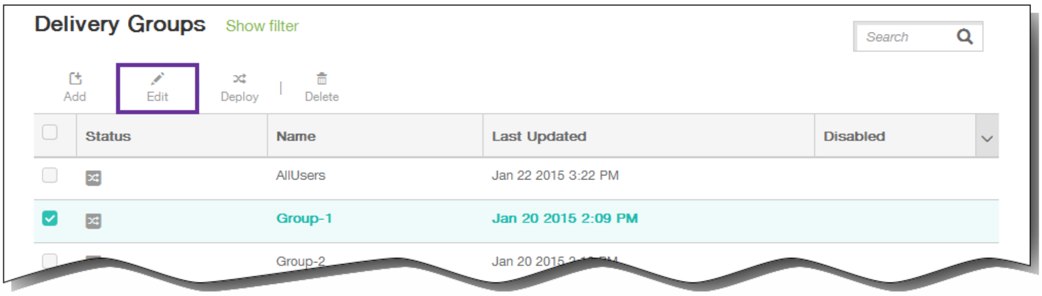
Box

2. Click on a resource and drag it to the location from which you want it deployed. After you change the deployment order, XenMobile deploys resources in the list from top to bottom.

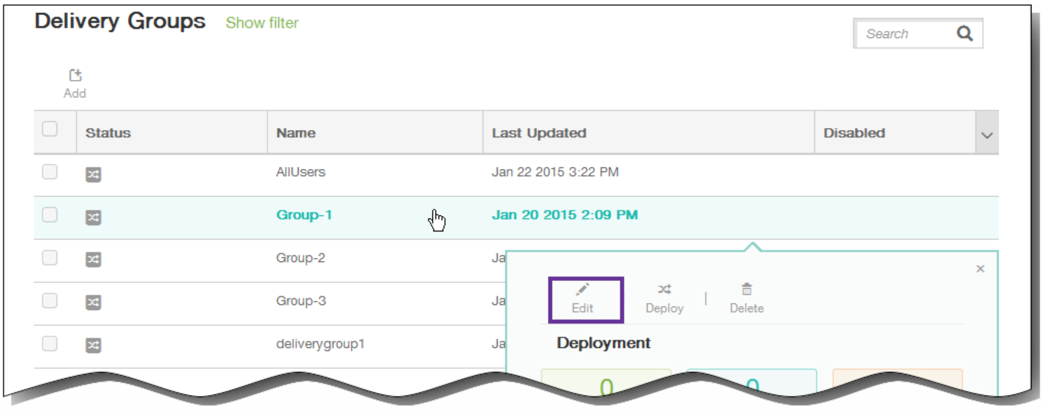
3. Click **Save** to save the deployment order.

To edit a delivery group

1. On the Delivery Groups page, choose the delivery group you want to edit by selecting the check box next to its name or by clicking in the line containing its name.
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.

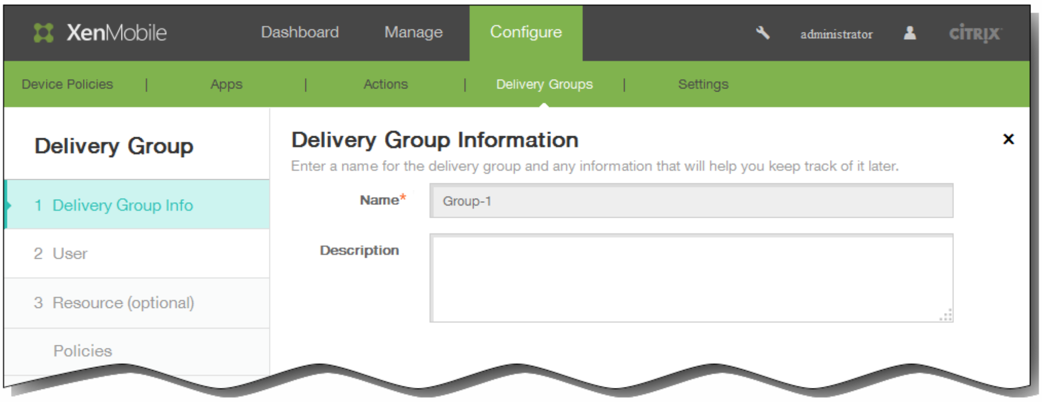


□	Status	Name	Last Updated	Disabled
□		AllUsers	Jan 22 2015 3:22 PM	
☑		Group-1	Jan 20 2015 2:09 PM	
□		Group-2	Jan 20 2015	



Status	Name	Last Updated	Disabled
	AllUsers	Jan 22 2015 3:22 PM	
	Group-1	Jan 20 2015 2:09 PM	
	Group-2	Ja	
	Group-3	Ja	
	deliverygroup1	Ja	

The Delivery Group Information edit page appears.



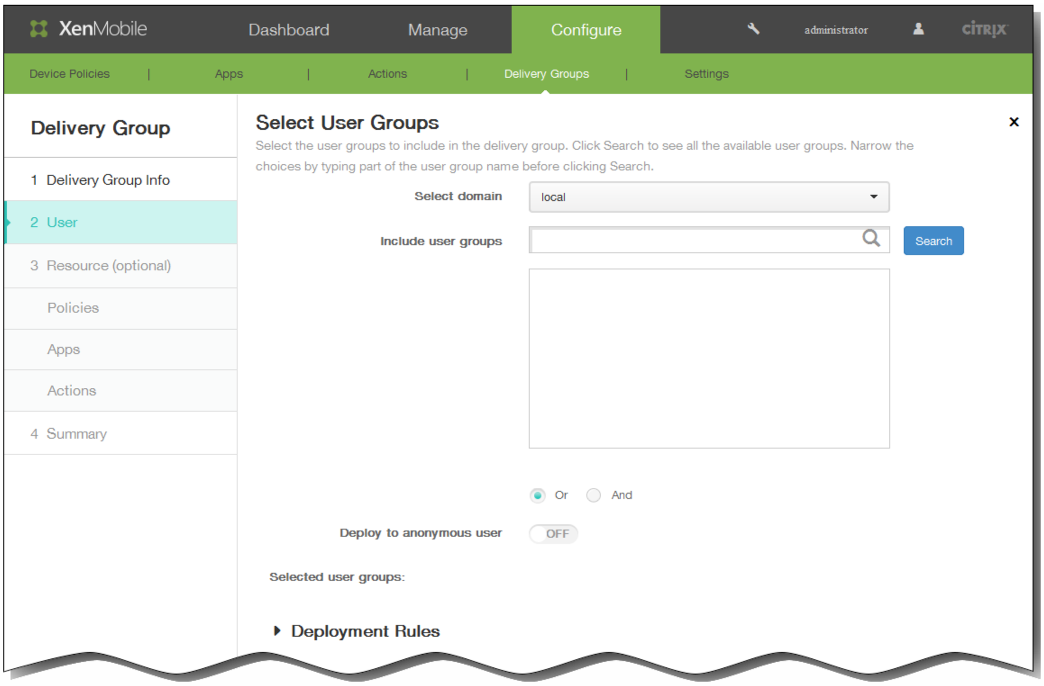
Delivery Group Information

Enter a name for the delivery group and any information that will help you keep track of it later.

Name* Group-1

Description

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.



Select User Groups

Select the user groups to include in the delivery group. Click Search to see all the available user groups. Narrow the choices by typing part of the user group name before clicking Search.

Select domain: local

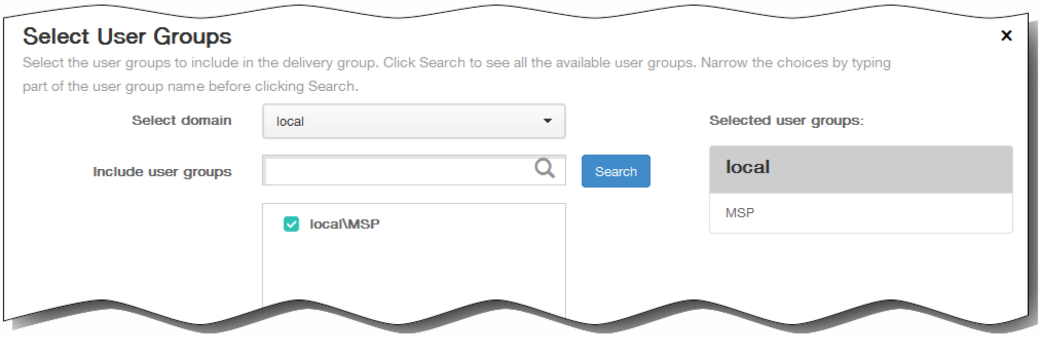
Include user groups:

● Or ○ And

Deploy to anonymous user: OFF

Selected user groups:

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.



Select User Groups

Select the user groups to include in the delivery group. Click Search to see all the available user groups. Narrow the choices by typing part of the user group name before clicking Search.

Select domain: local

Include user groups:

☑ local\MSP

Selected user groups:

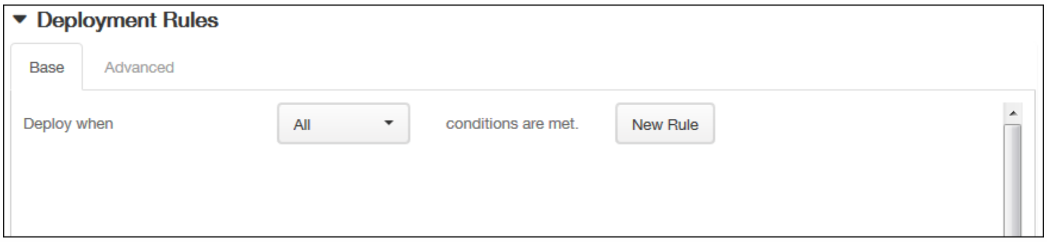
local

MSP

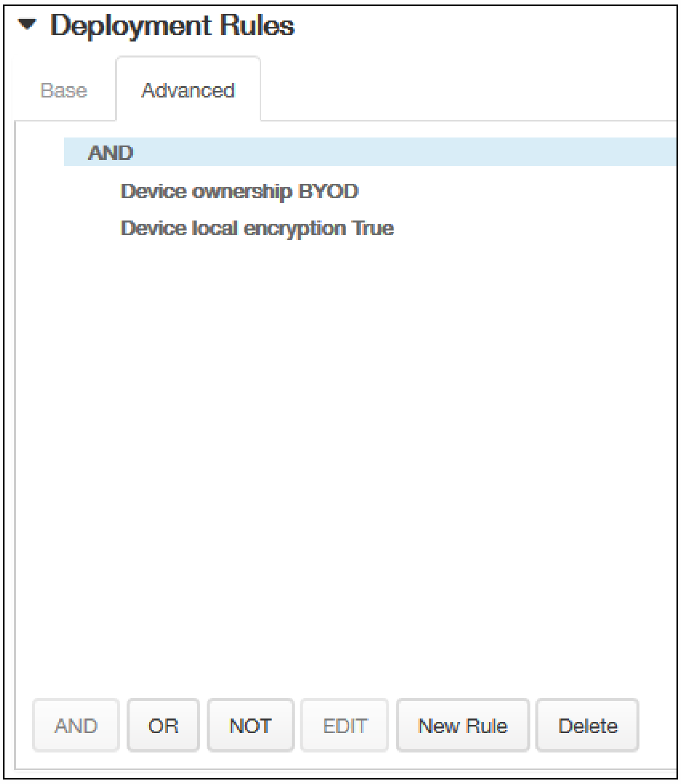
   Note: To remove user groups, click Search, and then in the list of user groups, clear the check box next to the group or groups you want to remove. You can type a full or partial group name in the search box and then click Search to limit the number of user groups displayed in the list.

   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.



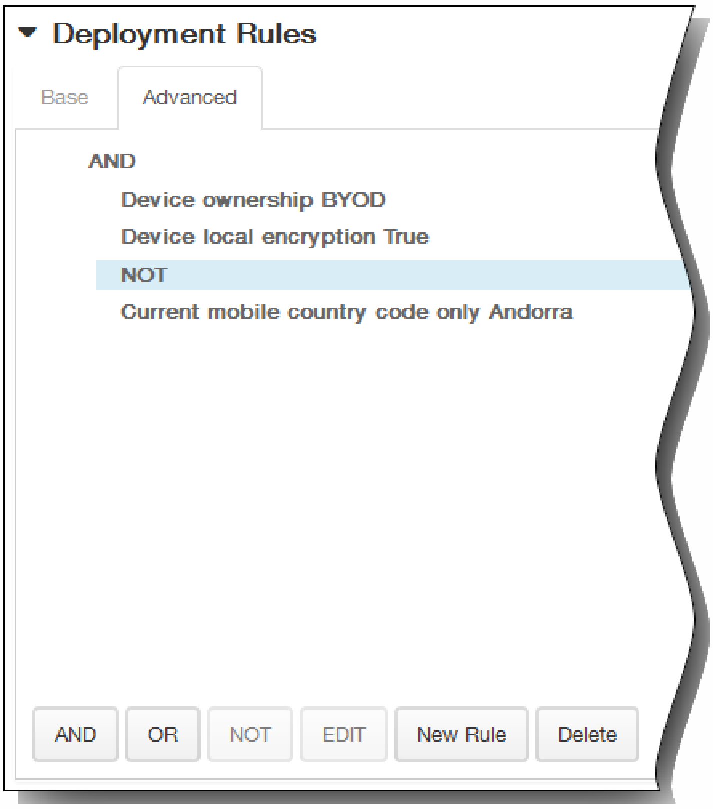
1. In the lists, click options to determine when the policy should be deployed.
   1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
   2. Click New Rule to define the conditions.
   3. In the lists, click the conditions, such 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.

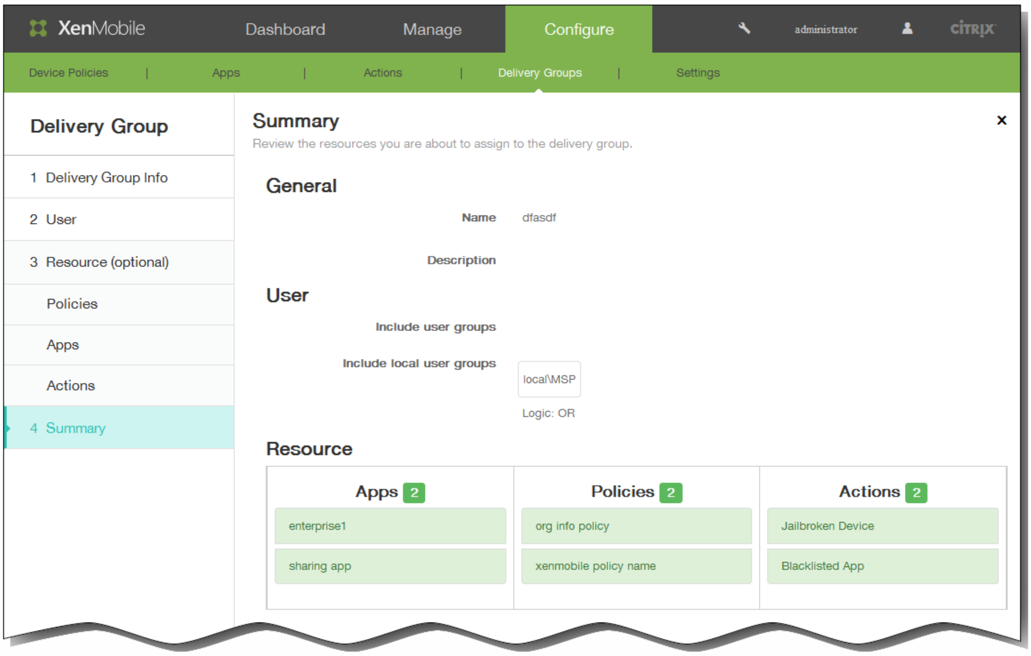
At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.

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.


XenMobile
Dashboard
Manage
Configure
administrator
Device Policies | Apps | Actions | Delivery Groups | Settings
×

Delivery Group

1 Delivery Group Info
2 User
3 Resource (optional)
Policies
Apps
Actions
4 Summary

Summary

Review the resources you are about to assign to the delivery group.

General

Name: dfasdf

Description:

User

Include user groups:

Include local user groups: local\MSP

Logic: OR

Resource

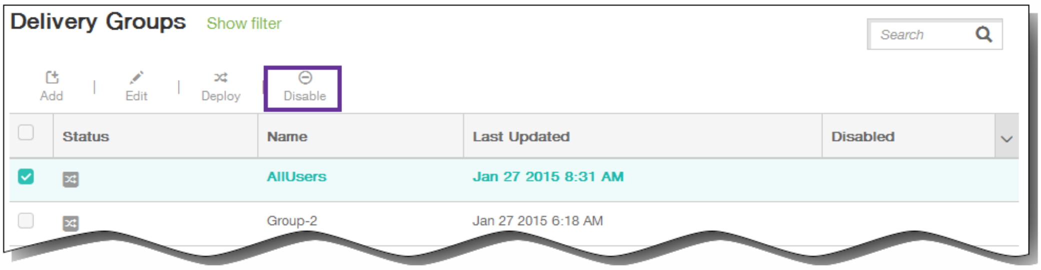
Apps 2	Policies 2	Actions 2
enterprise1	org info policy	Jailbroken Device
sharing app	xenmobile policy name	Blacklisted App

8. On the Summary page, you can review the options you have configured for the delivery group and change the deployment order of resources. Click Back to return to previous pages to make any necessary adjustments to the configuration. Click Deployment Order to reorder the resource deployment order; for more information on changing deployment order, see To change deployment order.
9. Click Save to save your changes.

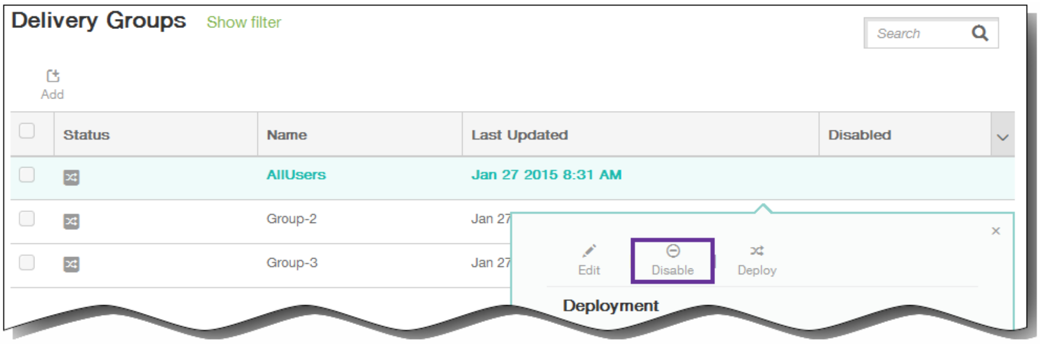
To enable and disable the AllUsers delivery group

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.

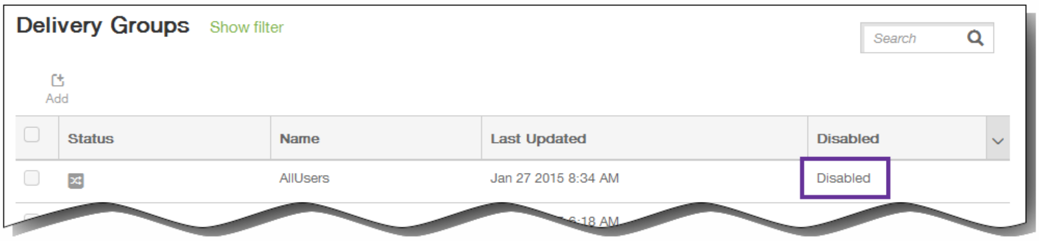


□	Status	Name	Last Updated	Disabled
☑		AllUsers	Jan 27 2015 8:31 AM	
□		Group-2	Jan 27 2015 6:18 AM	



	Status	Name	Last Updated	Disabled
□		AllUsers	Jan 27 2015 8:31 AM	
□		Group-2	Jan 27	
□		Group-3	Jan 27	

- 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.



	Status	Name	Last Updated	Disabled
□		AllUsers	Jan 27 2015 8:34 AM	Disabled

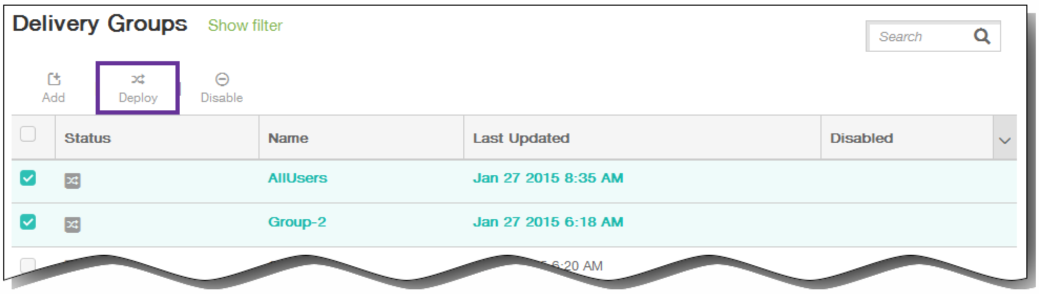
- Click Enable to enable the AllUsers delivery group. This command is only available if AllUsers is currently disabled. Disabled disappears from under the Disabled heading in the delivery group table.

To deploy delivery groups

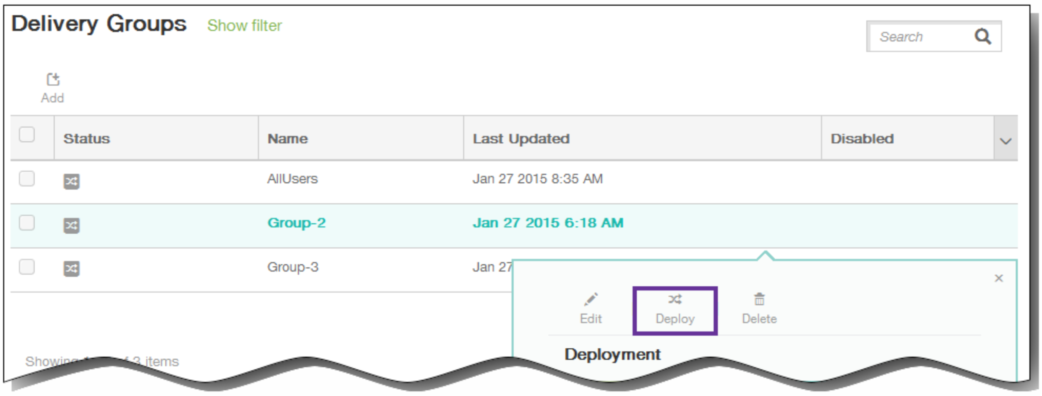
Deploying to a delivery group means sending a push notification to all users with iOS, Windows Phone 8.1, and Windows 8.1 tablet devices who belong to the delivery group to reconnect to XenMobile, so that you can reevaluate the devices and deploy apps, policies, and actions; users with other platform 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.



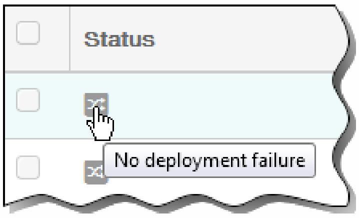
	Status	Name	Last Updated	Disabled
☑		AllUsers	Jan 27 2015 8:35 AM	
☑		Group-2	Jan 27 2015 6:18 AM	



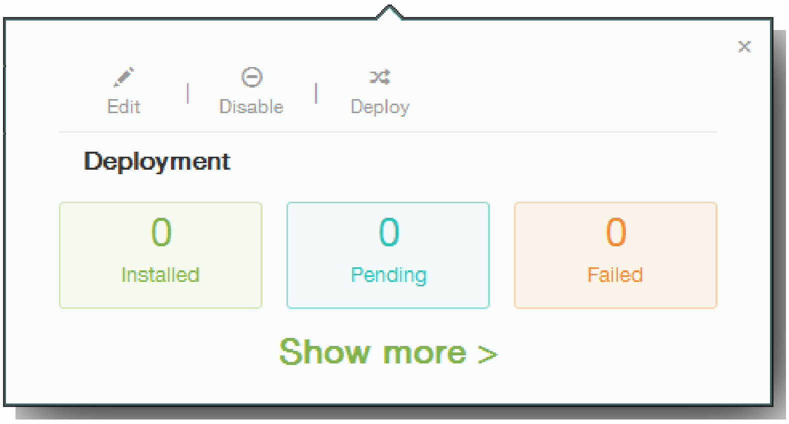
Status	Name	Last Updated	Disabled
	AllUsers	Jan 27 2015 8:35 AM	
	Group-2	Jan 27 2015 6:18 AM	
	Group-3	Jan 27	

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

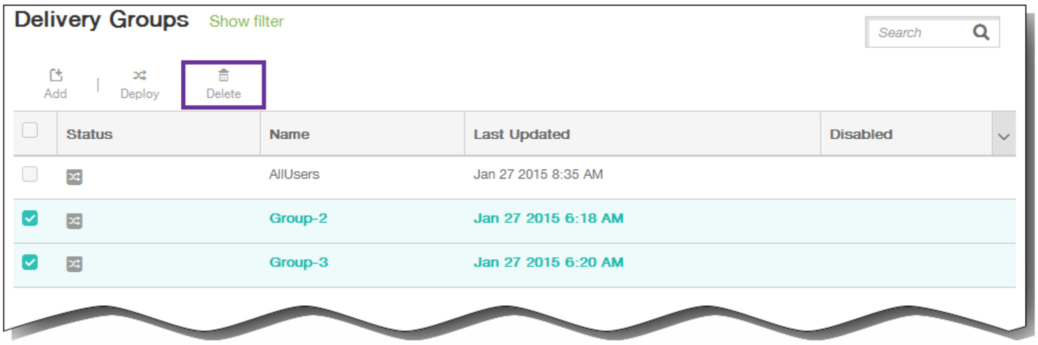
Note: You cannot delete the AllUsers delivery group, but you can disable the group when you do not want to push resources to all users.

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.

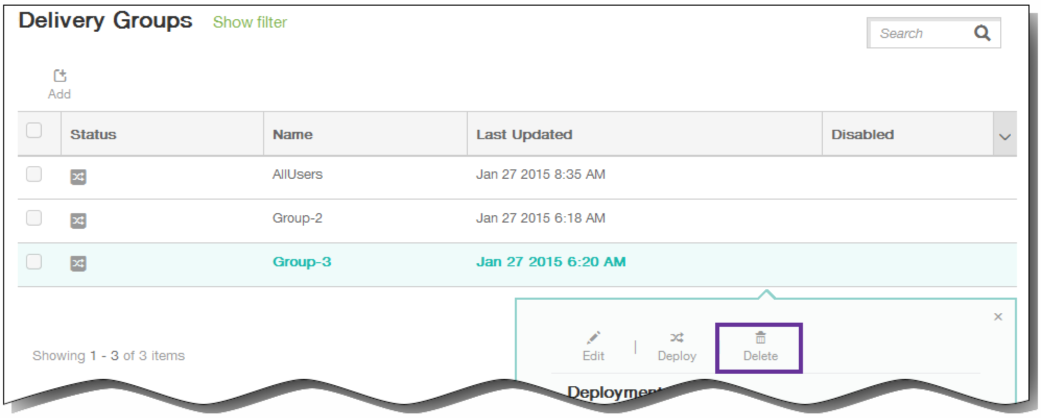
- To delete a single delivery group, either select the check box next to its name or click the line containing its name.

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.



☐	Status	Name	Last Updated	Disabled
☐		AllUsers	Jan 27 2015 8:35 AM	
☑		Group-2	Jan 27 2015 6:18 AM	
☑		Group-3	Jan 27 2015 6:20 AM	



☐	Status	Name	Last Updated	Disabled
☐		AllUsers	Jan 27 2015 8:35 AM	
☐		Group-2	Jan 27 2015 6:18 AM	
☐		Group-3	Jan 27 2015 6:20 AM	

Showing 1 - 3 of 3 items

The Delete dialog box appears.

3. Click Delete on the Delete dialog box.

   Important: You cannot undo this action.

Enrolling Users and Devices

May 15, 2015

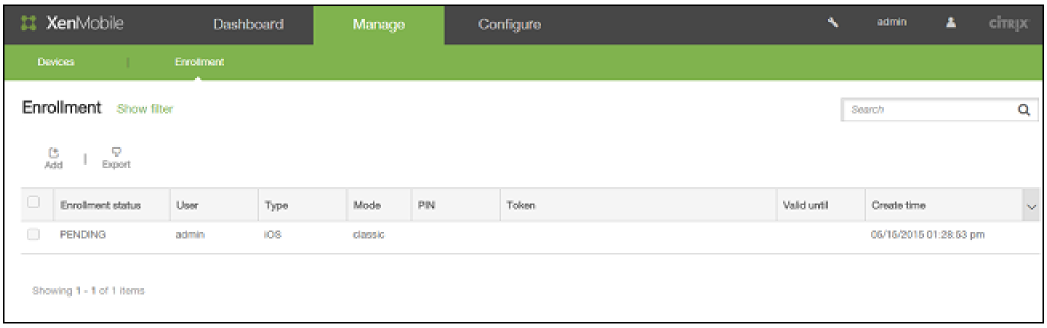
In order to manage user devices remotely and securely, user devices need to be enrolled in XenMobile. The XenMobile client software is installed on the user device and the user's identity is authenticated, and then XenMobile and the user's profile is installed. After the devices are enrolled, in the 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**:



Enrollment Show filter

☐	Enrollment status	User	Type	Mode	PIN	Token	Valid until	Create time
☐	PENDING	admin	iOS	classic				06/16/2015 01:28:53 pm

Showing 1 - 1 of 1 items

Android Devices

Jun 16, 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. You will need to enter your Worx PIN twice. On the Create Worx PIN screen screen, enter a PIN consisting of any series of six numbers.
8. Reenter the PIN. Worx Home opens. You can then access the Worx Store to view the apps you can install on your Android device.
9. 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 un-enroll and re-enroll an Android device

Updated: 2015-02-12

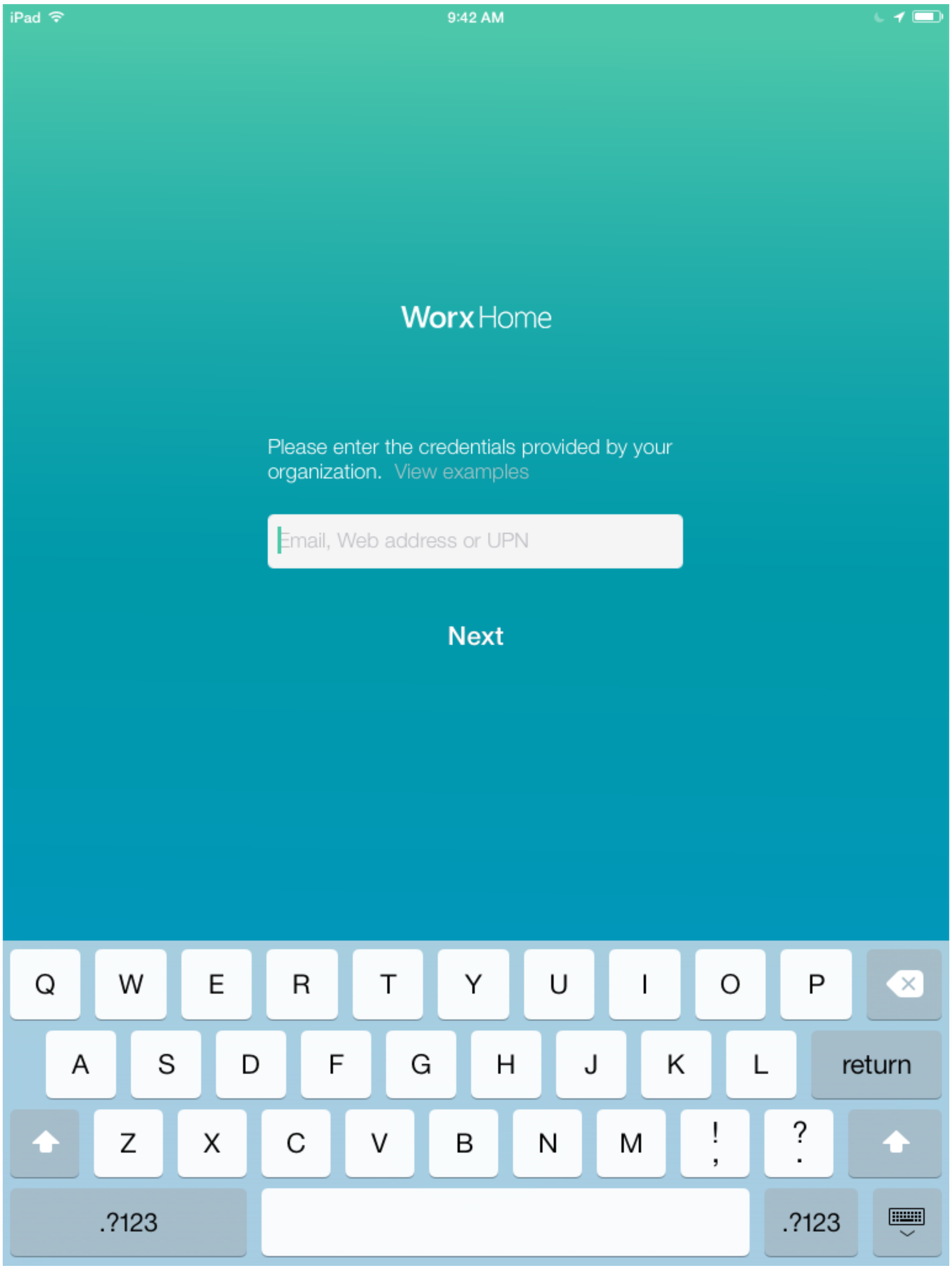
Before a device is re-enrolled, the device is first un-enrolled. During the period in which the device is un-enrolled, but not yet re-enrolled, the device is not managed by XenMobile, although it continues to appear in the device inventory list in the XenMobile console. You cannot track the device and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

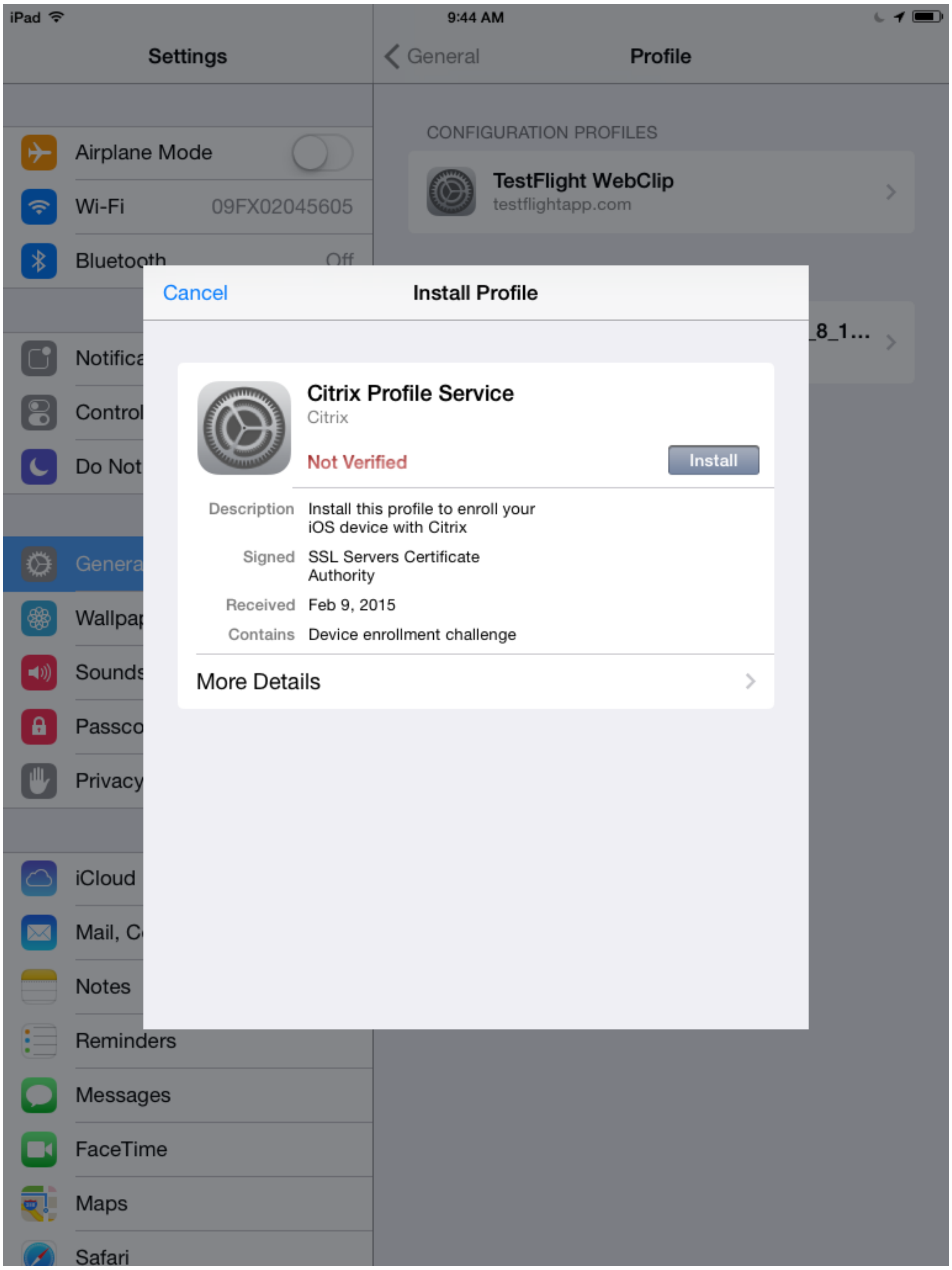
Feb 13, 2015

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.



Please enter the credentials provided by your organization. View examples

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



Citrix Profile Service
Citrix
Not Verified

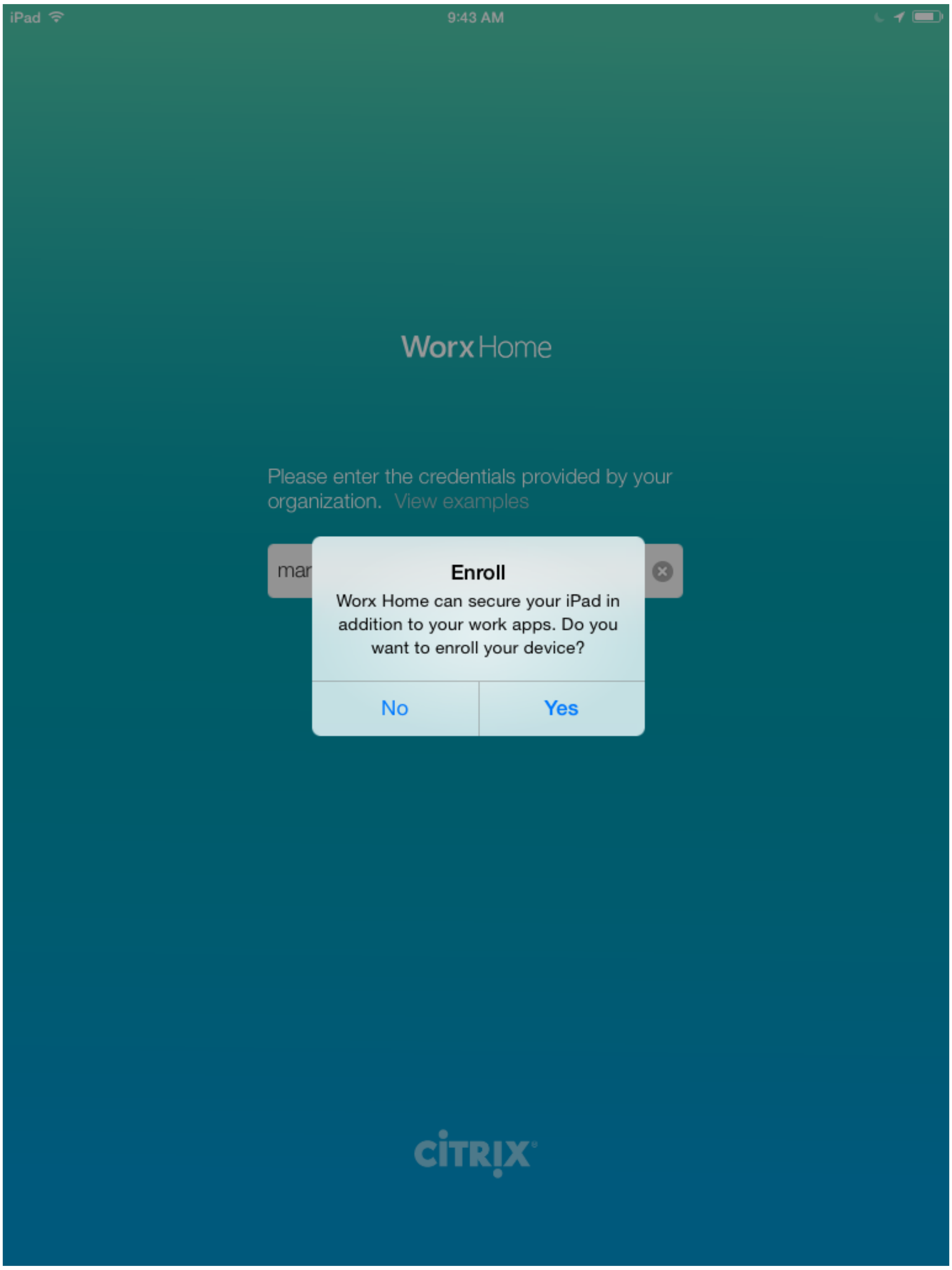
Description: Install this profile to enroll your iOS device with Citrix

Signed: SSL Servers Certificate Authority

Received: Feb 9, 2015

Contains: Device enrollment challenge

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.


iPad
9:43 AM
Worx Home
Please enter the credentials provided by your organization. View examples
mar

Enroll

Worx Home can secure your iPad in addition to your work apps. Do you want to enroll your device?

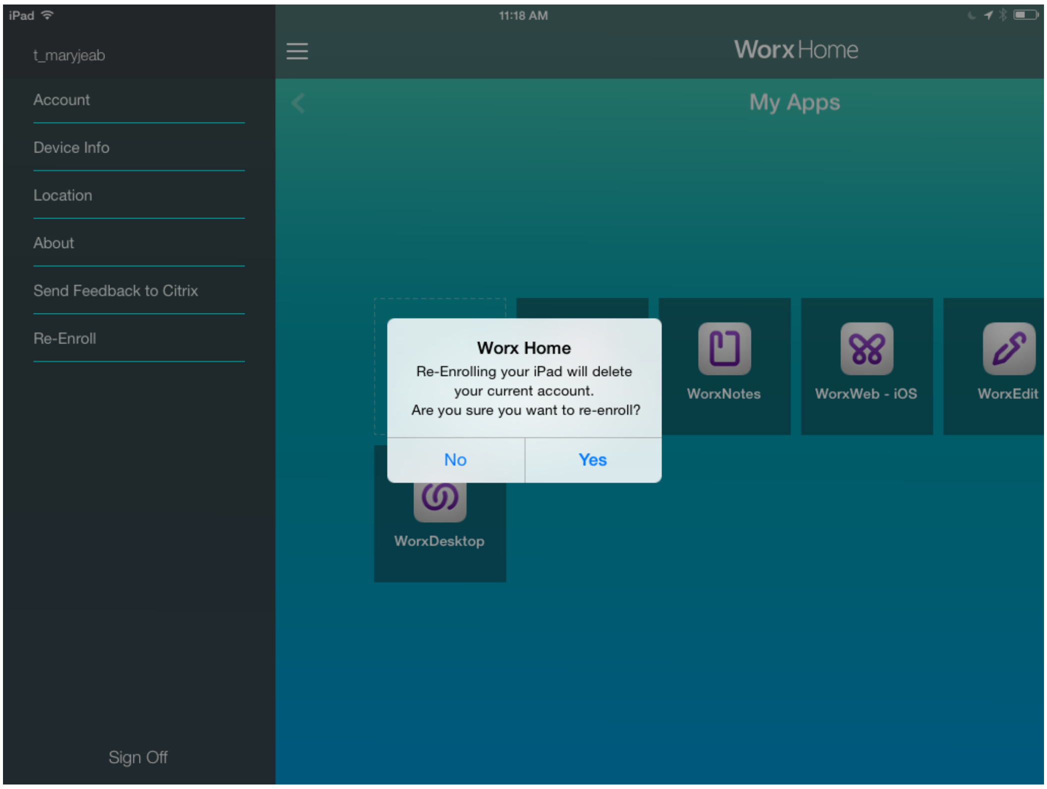
11. Depending on the way XenMobile is configured, you may be asked to create a Worx PIN, which you can use to sign on to Worx Home and other Worx-enabled apps, such as WorxMail, WorxWeb, ShareFile, and more. You will need to enter your Worx PIN twice. Worx Home opens. You can then access the Worx Store 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.



Worx Home
Re-Enrolling your iPad will delete your current account.
Are you sure you want to re-enroll?

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

Windows Devices

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 in 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

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 Window 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 inServer 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

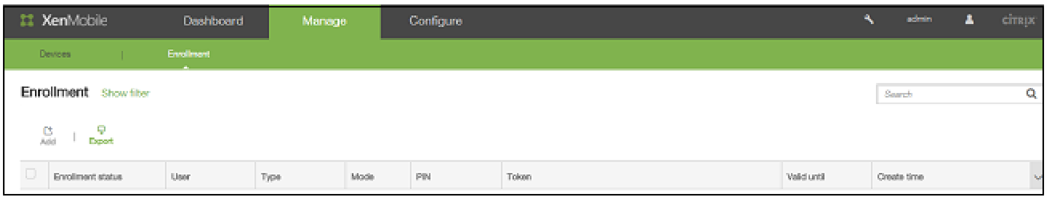
1. Browse to the XenMobile web address for your organization. The web address is in the following format:
   https://<zdmServerName>.domain.com/<zdmInstanceName>/setup
   Note: You can use HTTPS prefix only if you have a certificate issued by a trusted authority, such as Thawte or VeriSign.
2. On the 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

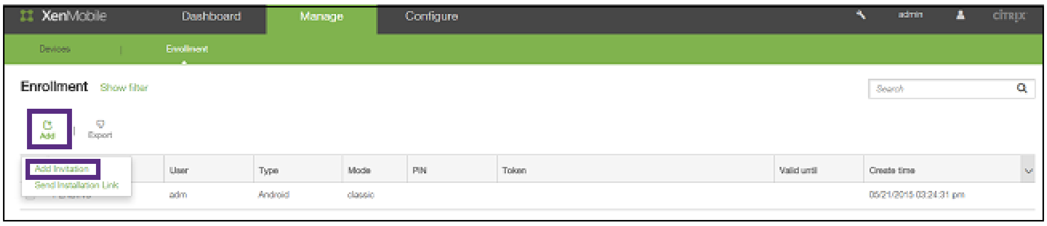
Mar 01, 2016

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

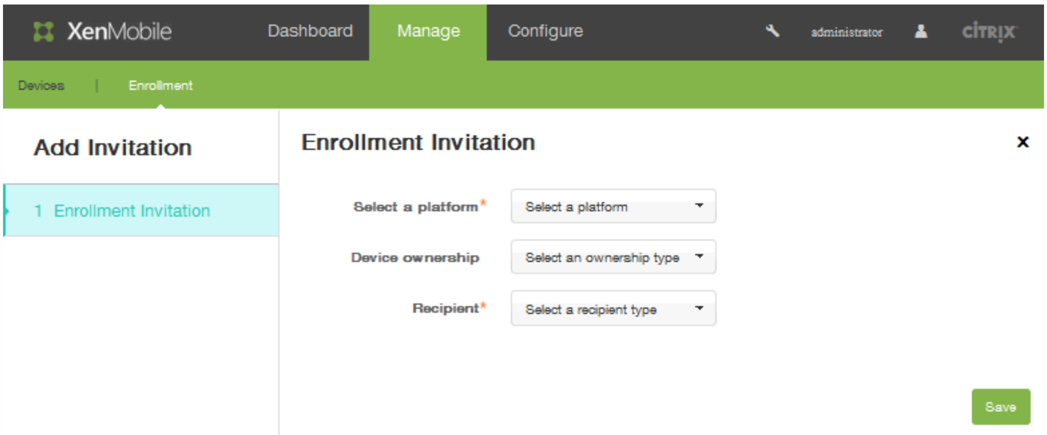
1. In the XenMobile console, click Manage > Enrollment.



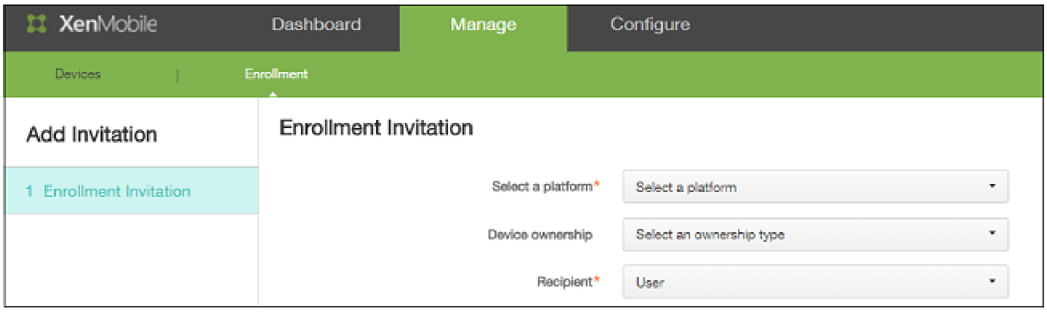
2. On the Enrollment screen, click Add. A menu appears listing options to add an invitation or send an installation link.
3. Click Add Invitation.



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.



Select a platform* Select a platform

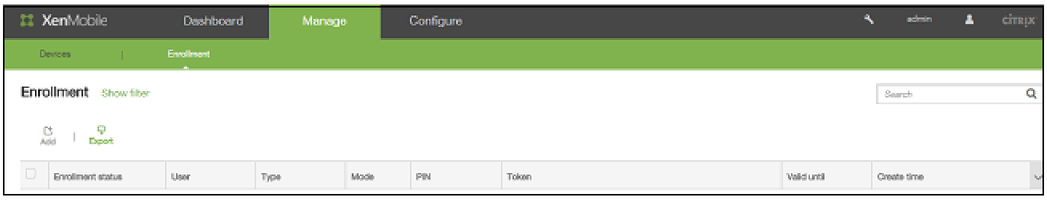
Device ownership Select an ownership type

Recipient* User

When you select a user as a recipient, additional configuration options appear. Follow the steps in these topics to complete the invitation settings depending on the recipient type you select.

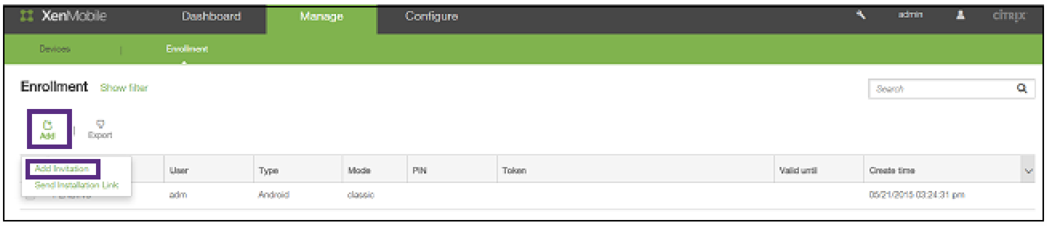
To send an enrollment invitation to a user

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

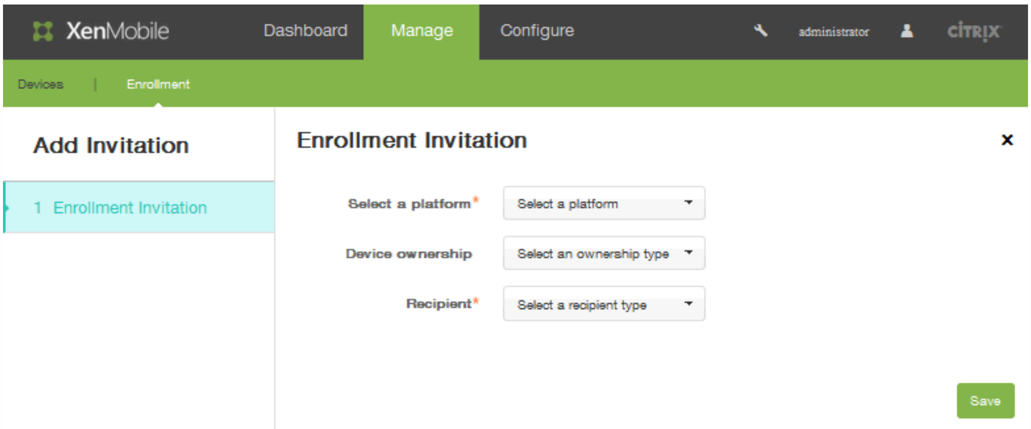


2. On the Enrollment screen, click Add. A menu appears where you can choose to add an invitation or send an installation link.

3. Click Add Invitation.



The Enrollment Invitation screen appears.

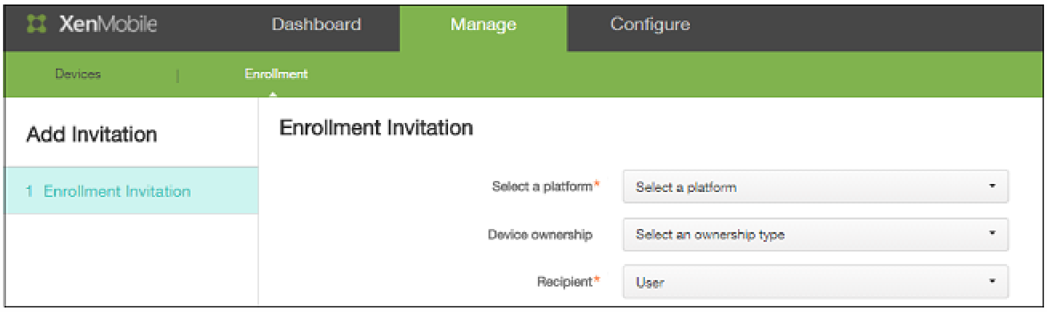


Select a platform* Select a platform

Device ownership Select an ownership type

Recipient* Select a recipient type

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.



Add Invitation

1 Enrollment Invitation

Enrollment Invitation

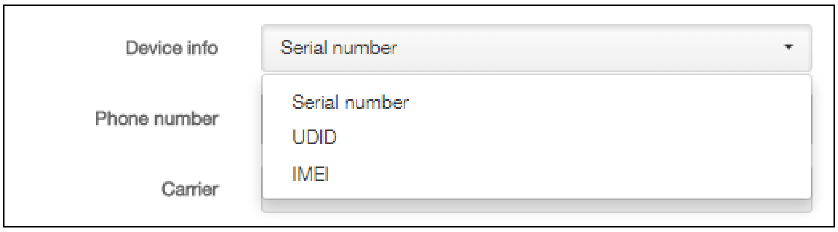
Select a platform* Select a platform

Device ownership Select an ownership type

Recipient* User

Additional configuration options appear related to user enrollment.

7. In User name, type a user name.
   Note: 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.



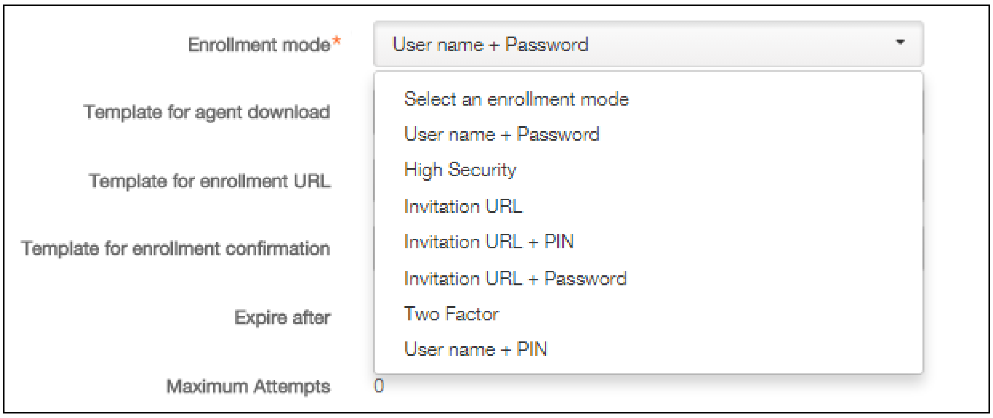
Device info: Serial number

Phone number

Carrier

After you choose an option, a field appears where you can type the corresponding value for the device.

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.



Enrollment mode*: User name + Password

Template for agent download

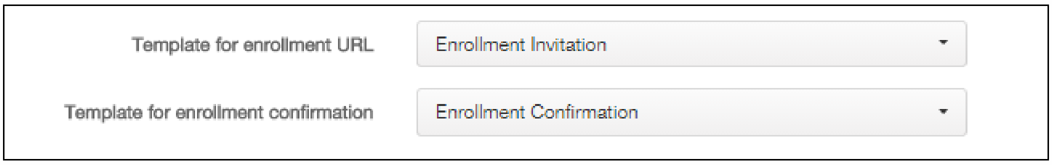
Template for enrollment URL

Template for enrollment confirmation

Expire after

Maximum Attempts: 0

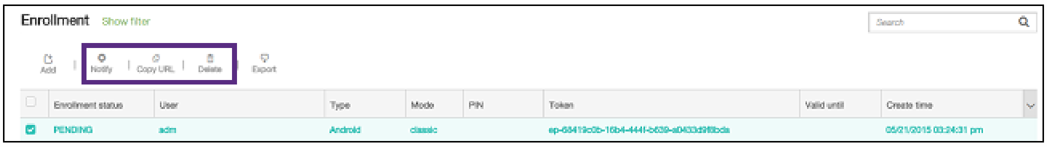
12. In the Template for agent download list, the choices for this option are based on the platform type. For example, iOS Download Link appears as an option if you selected iOS as a platform in Step 1.



Template for enrollment URL: Enrollment Invitation

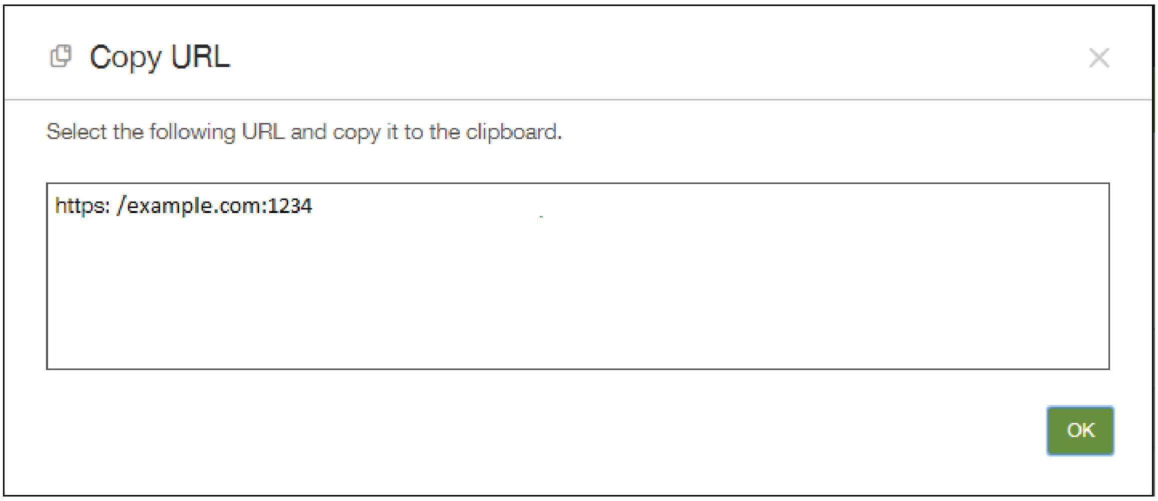
Template for enrollment confirmation: Enrollment Confirmation

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, do one of the following:
    - Click ON and then click Save & Send.
    - Leave the option as OFF and then click Save.
16. The invitation you added appears in the table on the Enrollment page. From here, if you click to select an invitation, several new options appear above the table: Notify, Copy URL, and Delete.



□	Enrollment status	User	Type	Mode	PIN	Token	Valid until	Create time
☑	PENDING	adm	Android	classic		ep-68419c0b-16b4-4441-b629-a0433d9f8bda		05/21/2015 03:24:31 pm

1. Click Notify to send a pending invitation.
2. Click Copy URL to copy the invitation URL in case you want to send the invitation in email. When the notification appears, you select the URL, copy it and then click OK.



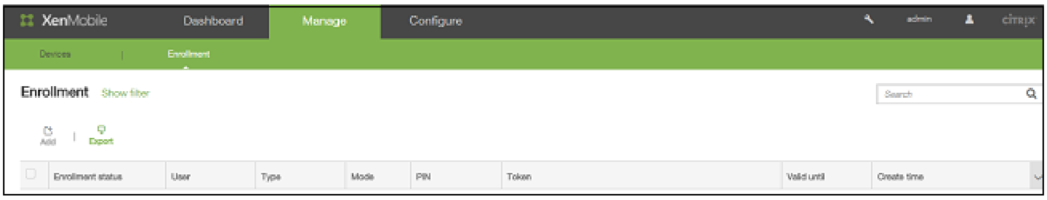
Select the following URL and copy it to the clipboard.

https: /example.com:1234

3. Click Delete to delete the invitation.

To send an enrollment invitation to a group

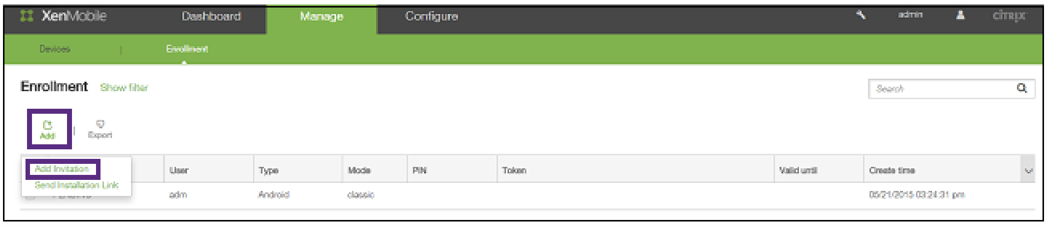
1. In the XenMobile console, click Manage > Enrollment.



□	Enrollment status	User	Type	Mode	PIN	Token	Valid until	Create time

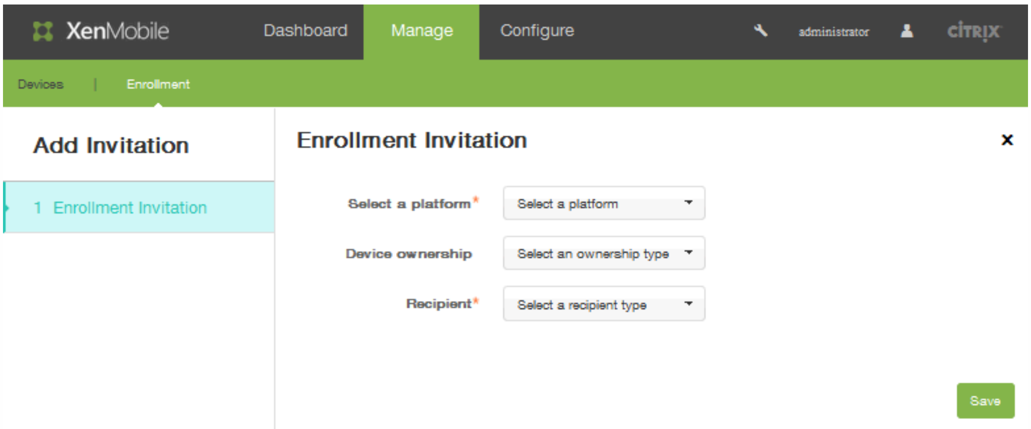
2. On the Enrollment screen, click Add. A menu appears where you can choose to add an invitation or send an installation link.

3. Click Add Invitation.



User	Type	Mode	PIN	Token	Valid until	Create time
adm	Android	classic				05/21/2015 03:24:31 pm

The Enrollment Invitation screen appears.

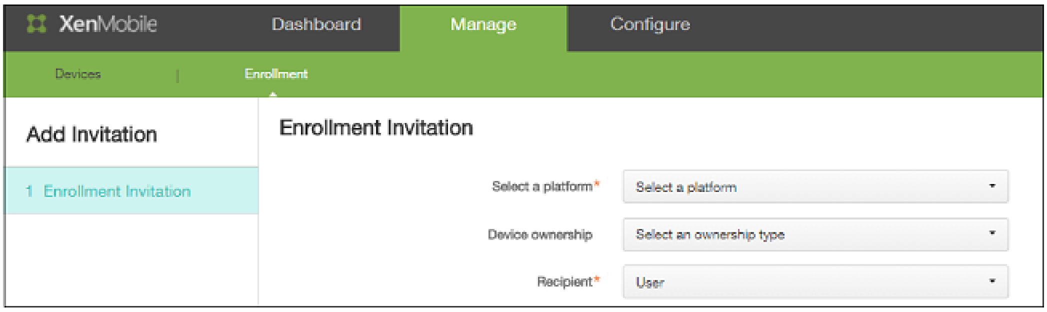


Select a platform* Select a platform

Device ownership Select an ownership type

Recipient* Select a recipient type

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. Configuration options appear for group enrollment.

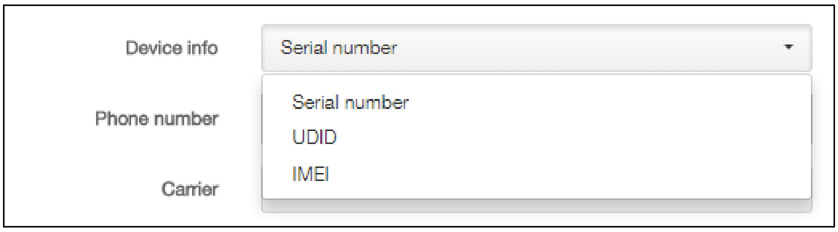


Select a platform* Select a platform

Device ownership Select an ownership type

Recipient* User

7. In User name, type a user name.
   Note: 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, a field appears where you can enter the corresponding value for the device.



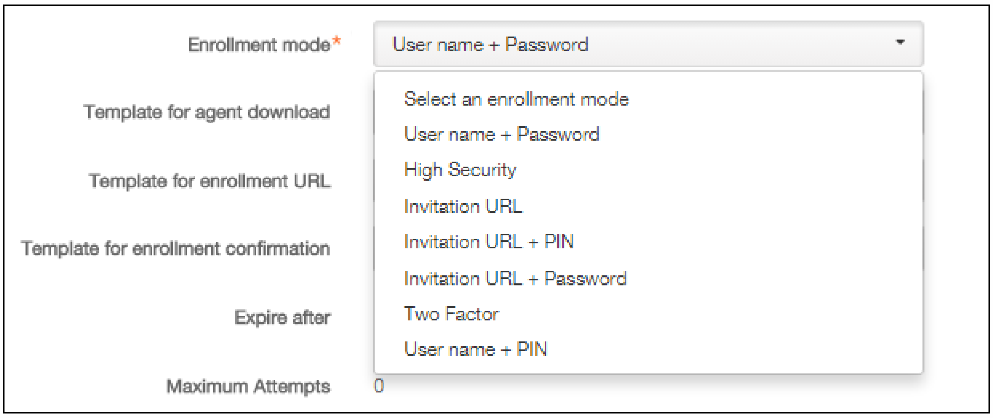
Device info Serial number

Phone number

Carrier

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, select User name + Password (the default), High Security, Invitation URL + PIN, Invitation URL + Password, Two Factor, or User name + PIN.



Enrollment mode* User name + Password

Template for agent download

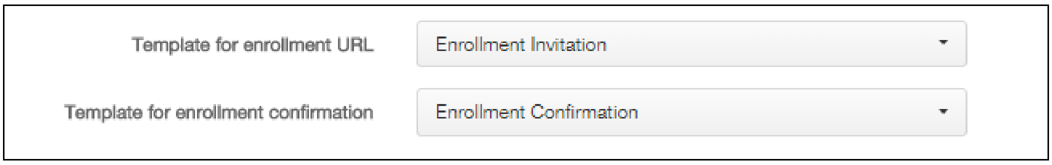
Template for enrollment URL

Template for enrollment confirmation

Expire after

Maximum Attempts 0

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 in Step 1.



Template for enrollment URL: Enrollment Invitation

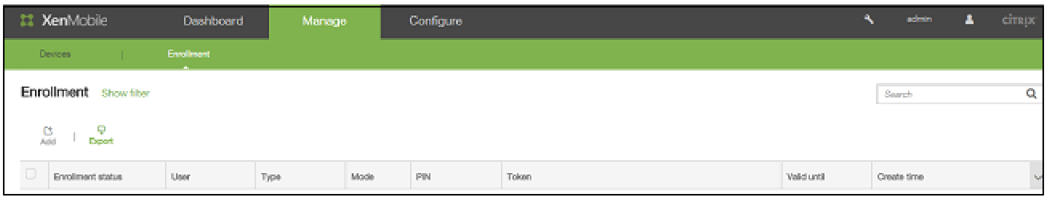
Template for enrollment confirmation: Enrollment Confirmation

13. In the Template for enrollment URL, select Enrollment Invitation.
14. 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.
15. In Send invitation, click ON and then click Save & Send.

To send an enrollment installation link

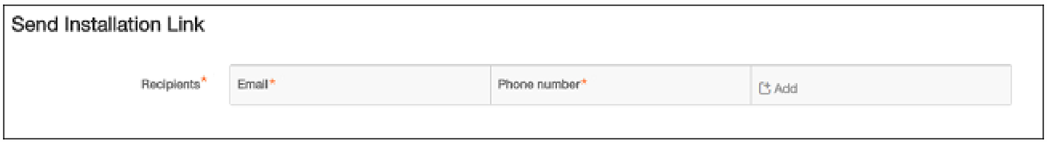
Before you can send an enrollment installation link, you must configure channels (SMTP or SMS) on the notification server from Configure > Settings > Notification Server. For details, see Notifications in XenMobile.

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.

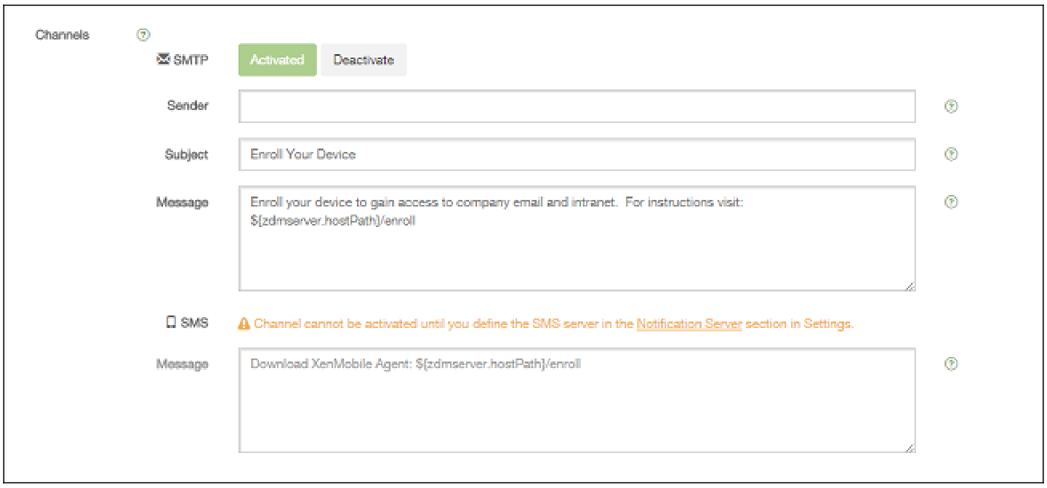
3. Click Send Installation Link. The Send Installation Link options appear.



Send Installation Link

Recipients*

4. In Recipient, click Add to add the email address and phone number for a recipient to whom you want to send an installation enrollment link and then click Save. You can repeat this step to add additional recipients one by one.
5. In Channels, select an appropriate channel to use for sending the enrollment installation link. Notifications are send over SMTP or SMS.

   Subject: Enroll Your Device

   Message: Enroll your device to gain access to company email and intranet. For instructions visit: ${zdmserver.hostPath}/enroll

   SMS: Channel cannot be activated until you define the SMS server in the Notification Server section in Settings.

   Message: Download XenMobile Agent: ${zdmserver.hostPath}/enroll

   Note: These channels cannot be activated until you configure the server settings in Configure > Settings > Notification Server. For details, see Notifications in XenMobile
6. 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.
7. For SMTP notifications, in Subject, optionally include the subject of the message. For example, "Enroll your device."
8. In Message, optionally add the content of the message to be sent to the recipient. For example, "Enroll your device to gain access to organizational apps and email."
9. 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.
10. 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.

Managing Devices with Android for Work in XenMobile

Jul 27, 2015

Android for Work is a secure workspace available on Android devices running Android 5.0 and later that isolates business accounts, apps, and data from personal accounts, apps, and data. In XenMobile 10.1, you manage both bring your own device (BYOD) and company-owned Android devices by having users create a separate work profile on their devices that, combined with hardware encryption and the policies you deploy, securely separates a device's corporate and personal areas. You can remotely manage all corporate policies, apps, and data, and you can wipe the policies, apps, and data from the device without affecting the user's personal area. For more information about supported Android devices, see Google's devices page.

In XenMobile 10.1, you can also manage devices running Android 4.0 - 4.4 by having users download and install the Android for Work app, which supplies the same secure workspace functionality built into devices running Android 5.0 and later.

You use Google Play for Work to add, buy, and approve apps for deployment to a device's Android for Work workspace. You can use Google Play for Work to deploy your private Android apps, as well as public and third-party apps.

Requirements for Android for Work:

- A publically accessible domain
- A Google admin account
- Devices running Android 5.0+ Lollipop with managed profile support or devices running Android 4.0 - 4.4 (Ice Cream Sandwich, Jelly Bean and KitKat) with the Android for Work app
- A Google account with Google Play installed in the user's personal profile
- A Work profile set up on the device

Before you can set Android for Work app restrictions, you must do the following:

- Complete Android for Work setup tasks on Google.
- Create a set of Google Play Credentials.
- Configure Android for Work server settings.
- Create at least one Android for Work device policy.
- Add, buy, and approve Android for Work apps in the Google Play for Work app store.

You can use the following links when managing Android for Work:

- Google admin console: https://admin.google.com/AdminHome
- Play for Work admin console: https://play.google.com/work/apps
- Play publish for private channel and self-hosted applications: https://play.google.com/apps/publish
- Google Developer's Console for creating service account: https://console.developers.google.com

Android for Work Prerequisites

Before you can administer Android for Work in XenMobile, you must:

- Create an Android for Work account
- Set up a service account

- Download an Android for Work certificate
  Enable and authorize the Google Admin SDK and MDM APIs
- Authorize your service account to use the directory and Google Play
- Obtain a binding token.

The following sections describe how to do each of these tasks. After you have completed these tasks, you can create a set of Google Play Credentials, configure Android for Work settings, and manage Android for Work apps in XenMobile.

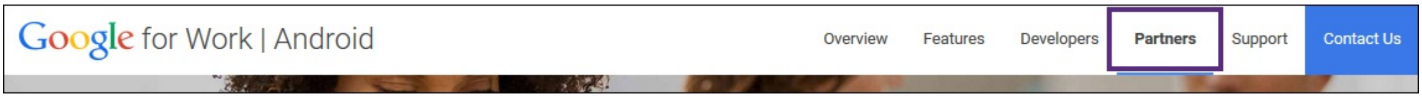
Create an Android for Work Account

You must meet the following prerequisites before you can set up an Android for Work account:

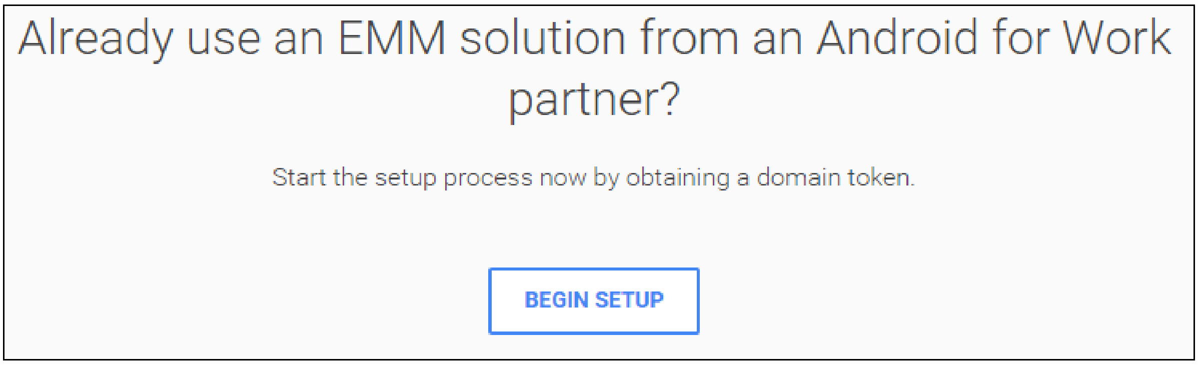
- You must own a domain name; for example, example.com.
- You must let Google verify that you own the domain.
- You must enable and administer Android for Work through an enterprise mobility management (EMM) provider (XenMobile 10.1 or later).

If you have already verified your domain name with Google, you can skip to Set up an Android for Work service account and download an Android for Work certificate.

1. Go to the Google Android for Work portal (https://www.google.com/work/android/partners/) and navigate to the **Partners** page.

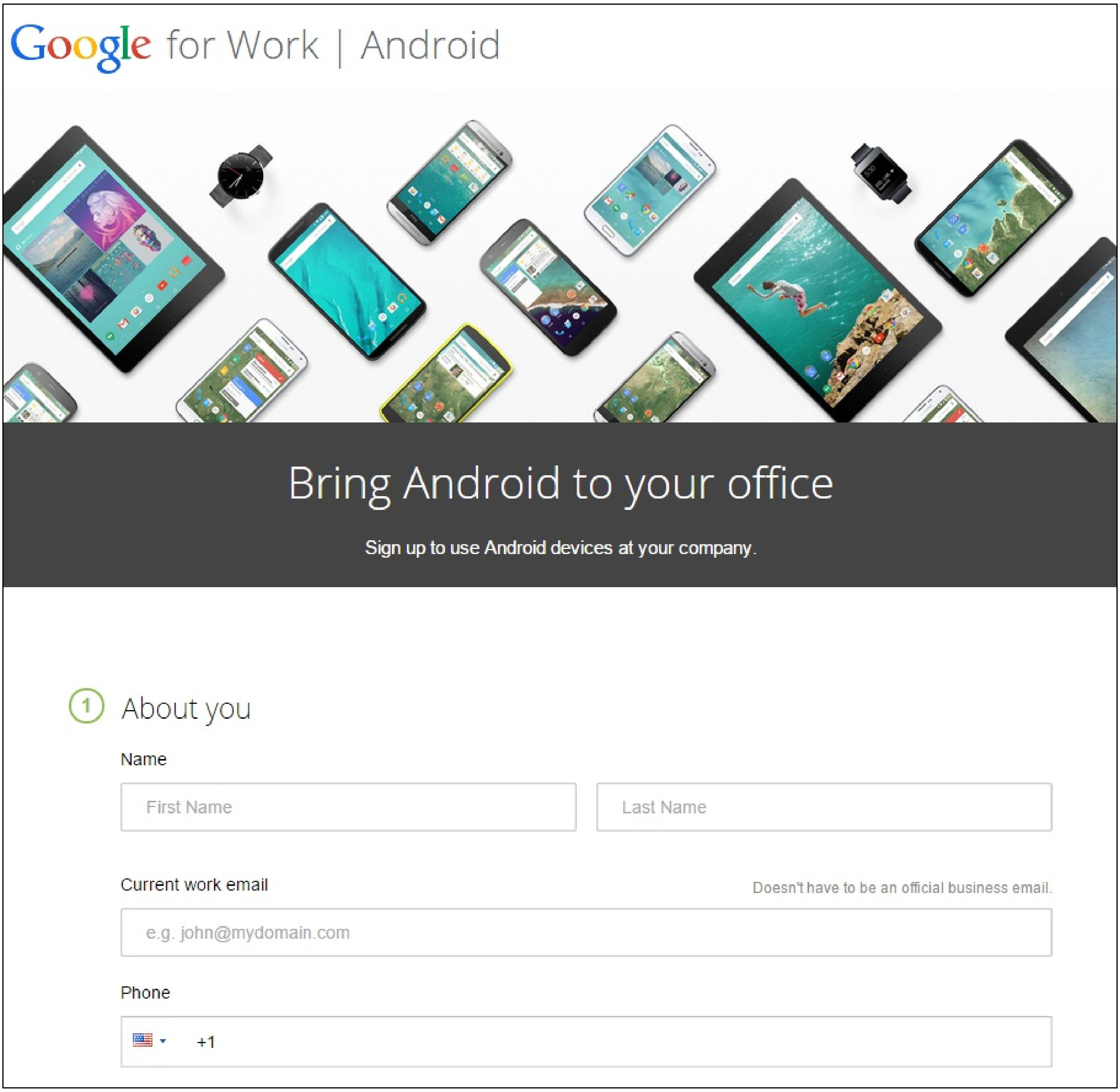


2. Click **Begin Setup**.


Already use an EMM solution from an Android for Work partner?

Start the setup process now by obtaining a domain token.

You are redirected to the following page where you enter your administrator information and company information.



Google for Work | Android

Bring Android to your office

Sign up to use Android devices at your company.

1 About you

Name

First Name

Last Name

Current work email

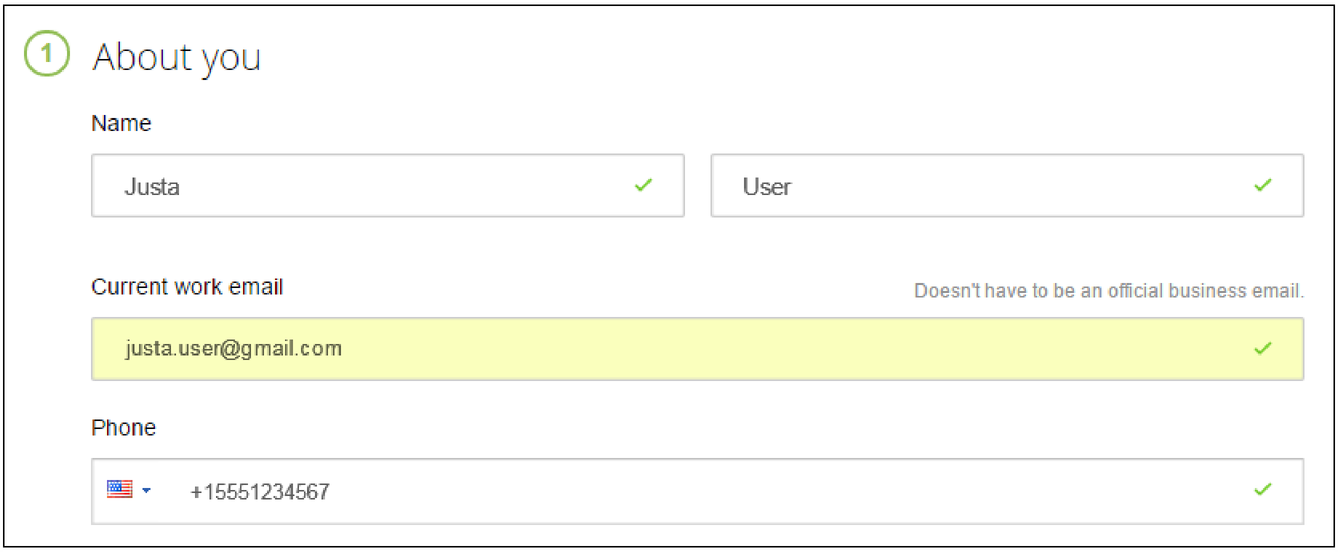
Doesn't have to be an official business email.

e.g. john@mydomain.com

Phone

+1

2. Enter your administrator user information.



1 About you

Name

Justa ✓ User ✓

Current work email

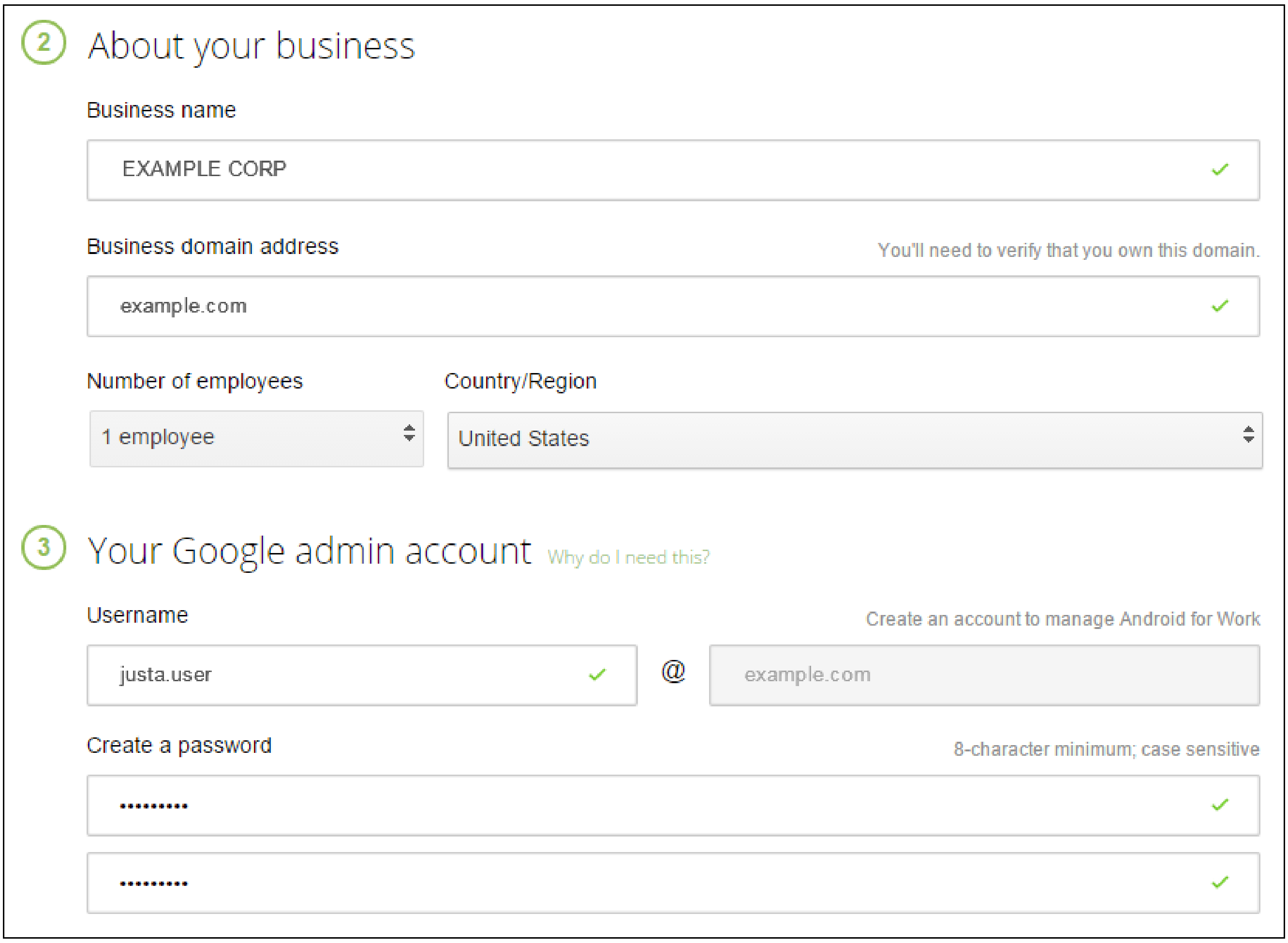
Doesn't have to be an official business email.

justa.user@gmail.com ✓

Phone

+15551234567 ✓

3. Enter your company information, as well as your admin account information.



2 About your business

Business name

EXAMPLE CORP ✓

Business domain address

You'll need to verify that you own this domain.

example.com ✓

Number of employees

1 employee

Country/Region

United States

3 Your Google admin account Why do I need this?

Username

Create an account to manage Android for Work

justa.user ✓ @ example.com

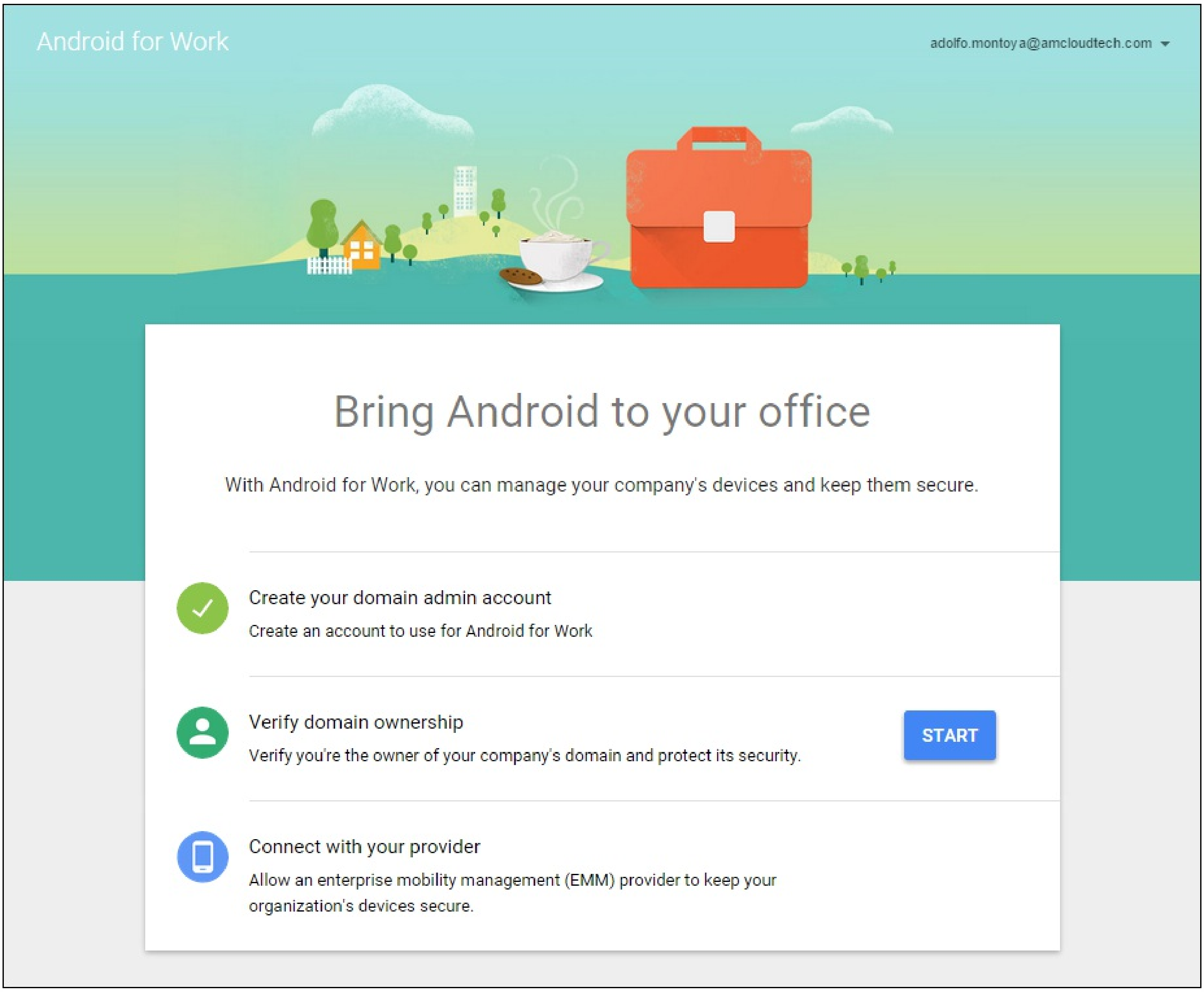
Create a password

8-character minimum; case sensitive

••••••••• ✓

••••••••• ✓

The first step in the process is complete and you see the following page.



Android for Work

adolfo.montoya@amcloudtech.com

Bring Android to your office

With Android for Work, you can manage your company's devices and keep them secure.

✓ Create your domain admin account

Create an account to use for Android for Work

Verify domain ownership

Verify you're the owner of your company's domain and protect its security.

Connect with your provider

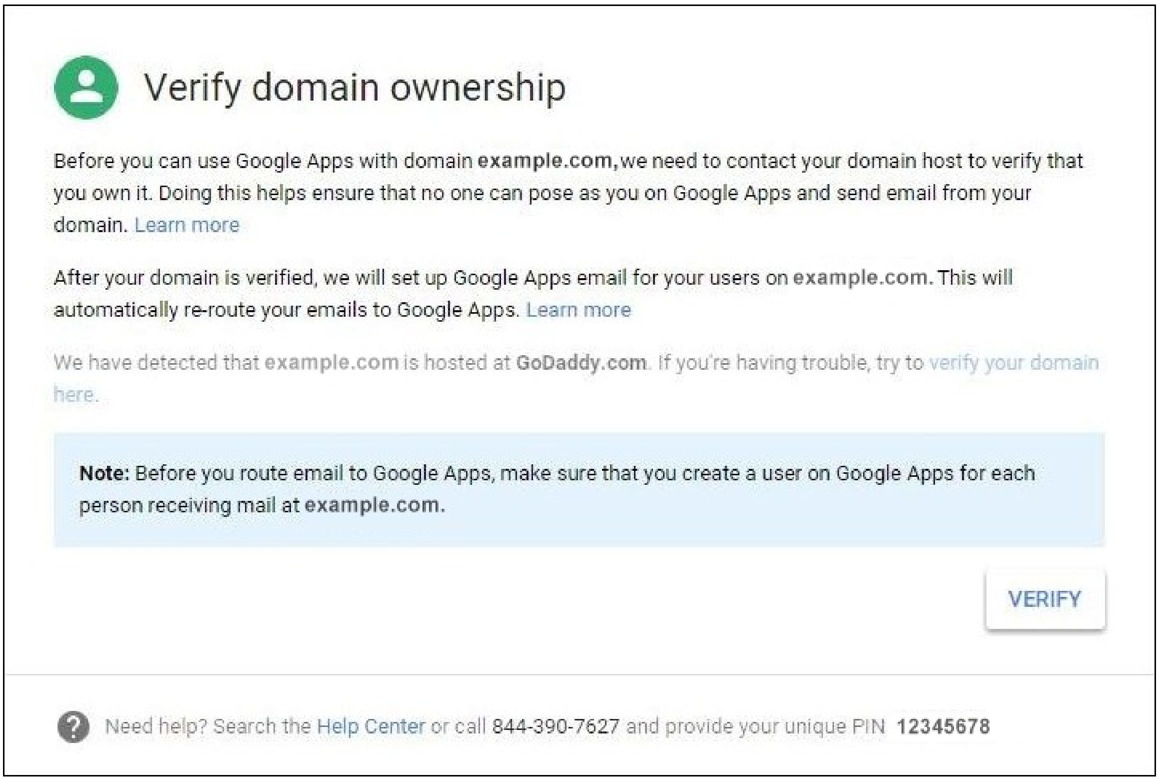
Allow an enterprise mobility management (EMM) provider to keep your organization's devices secure.

Verify domain ownership

You must now allow Google to verify your domain. There are three ways to verify your domain: add a TXT or CNAME record to your domain host's website, upload an HTML file to your domain's web server, or add a <meta> tag to your home page. Google recommends the first method. The steps to verify your domain ownership are not covered in this article, but you can find the information you need here: https://support.google.com/a/answer/6095407/.

1. Click **Start** to begin verification of your domain. The **Verify domain ownership** page appears. Follow the instructions there to verify your domain.

2. When you are done, click **Verify**.



Verify domain ownership

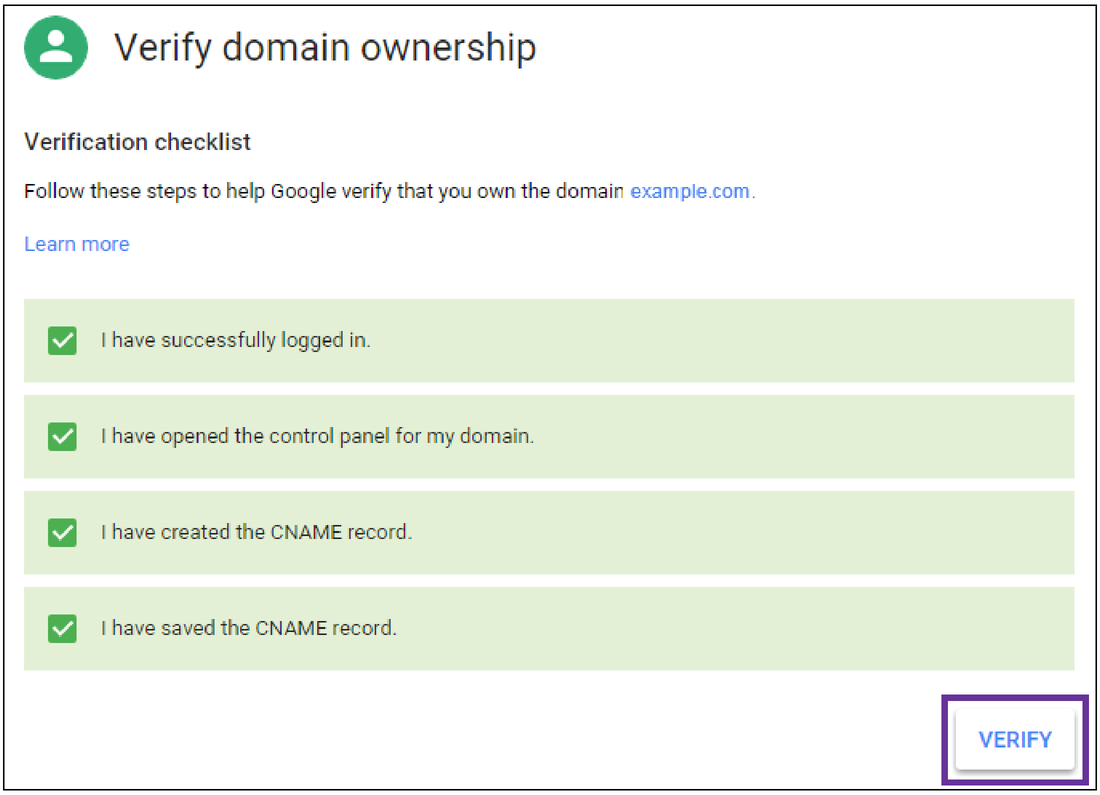
Before you can use Google Apps with domain **example.com,** we need to contact your domain host to verify that you own it. Doing this helps ensure that no one can pose as you on Google Apps and send email from your domain. Learn more

After your domain is verified, we will set up Google Apps email for your users on **example.com**. This will automatically re-route your emails to Google Apps. Learn more

We have detected that **example.com** is hosted at **GoDaddy.com**. If you're having trouble, try to verify your domain here.

Note: Before you route email to Google Apps, make sure that you create a user on Google Apps for each person receiving mail at **example.com**.

Need help? Search the Help Center or call 844-390-7627 and provide your unique PIN **12345678**



Verify domain ownership

Verification checklist

Follow these steps to help Google verify that you own the domain example.com.

Learn more

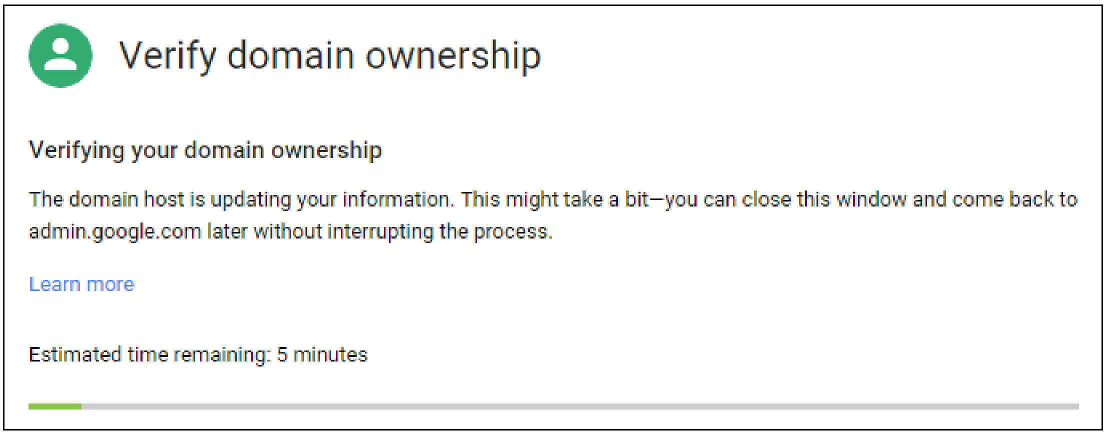
☑ I have successfully logged in.

☑ I have opened the control panel for my domain.

☑ I have created the CNAME record.

☑ I have saved the CNAME record.

7. Google verifies your domain ownership.



Verify domain ownership

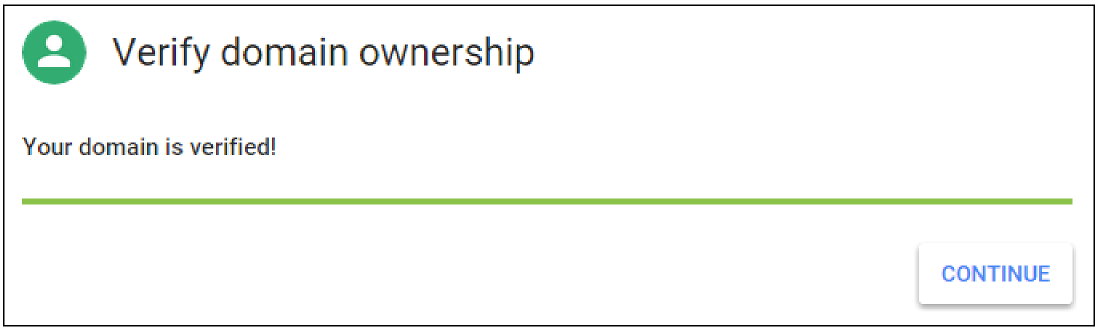
Verifying your domain ownership

The domain host is updating your information. This might take a bit—you can close this window and come back to admin.google.com later without interrupting the process.

Learn more

Estimated time remaining: 5 minutes

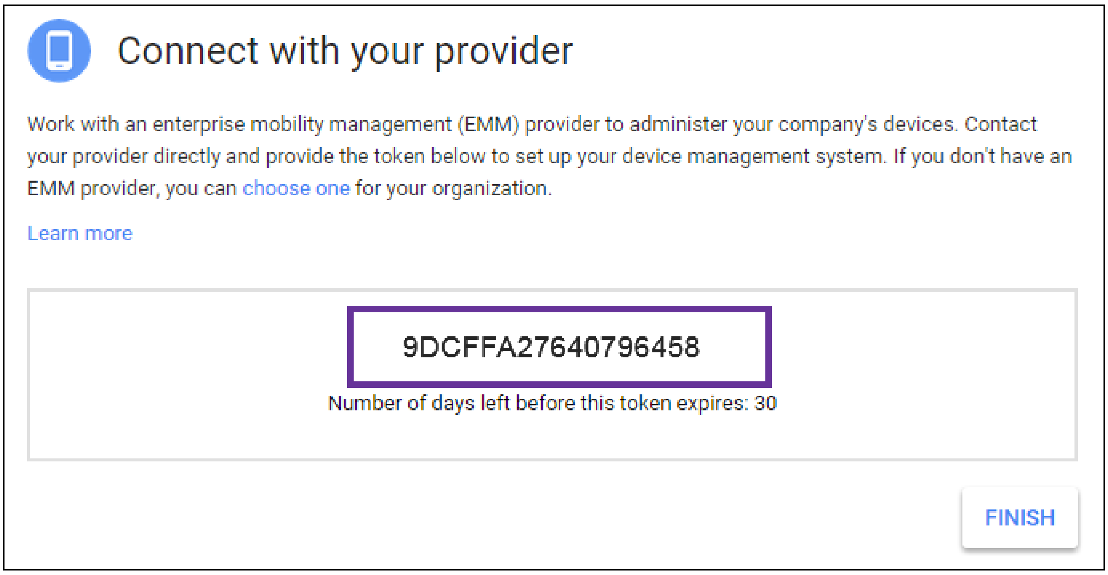
8. You see the following page after successful verification. Click **Continue**.



Verify domain ownership

Your domain is verified!

9. Google creates an EMM binding token that you provide to Citrix and use when you configure Android for Work settings. Copy and save the token; you will need it later in the set-up procedure.



Connect with your provider

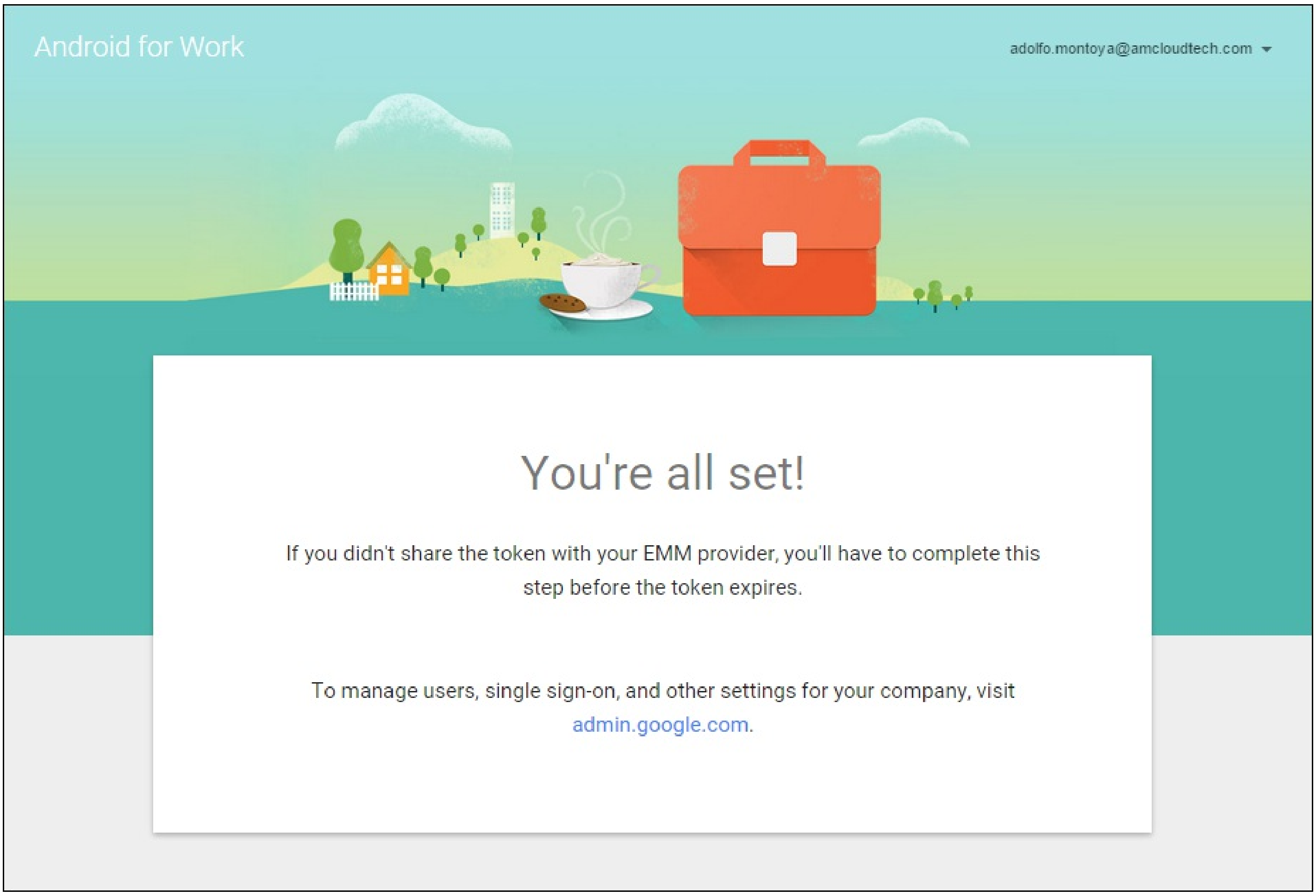
Work with an enterprise mobility management (EMM) provider to administer your company's devices. Contact your provider directly and provide the token below to set up your device management system. If you don't have an EMM provider, you can choose one for your organization.

Learn more

9DCFFA27640796458

Number of days left before this token expires: 30

10. Click **Finish** to complete setting up Android for Work.



You're all set!

If you didn't share the token with your EMM provider, you'll have to complete this step before the token expires.

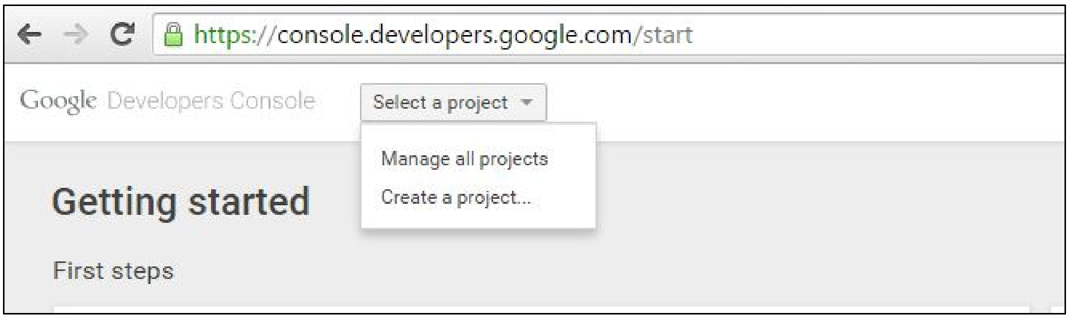
To manage users, single sign-on, and other settings for your company, visit admin.google.com.

After you create an Android for Work service account, you can log on to the Google Admin console to manage your Android for Work mobility management settings.

Set up an Android for Work service account and download an Android for Work certificate

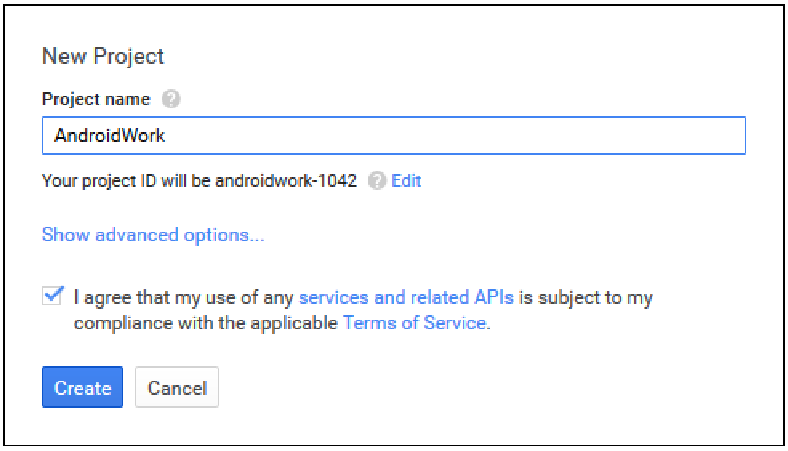
To allow XenMobile to contact Google Play and Directory services, you must create a new service account using Google's Project portal for developers. This service account is used for server-to-server communication between XenMobile and Google services for Android for Work. For more information about the authentication protocol being used, go to https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

1. In a web browser, go to https://console.developers.google.com/project and log on with your Google admin credentials.



3. In the **Select a project** list, click **Create a Project**.

4. Type a project name, click the check box to agree to the Terms of Service and then, click **Create**.



New Project

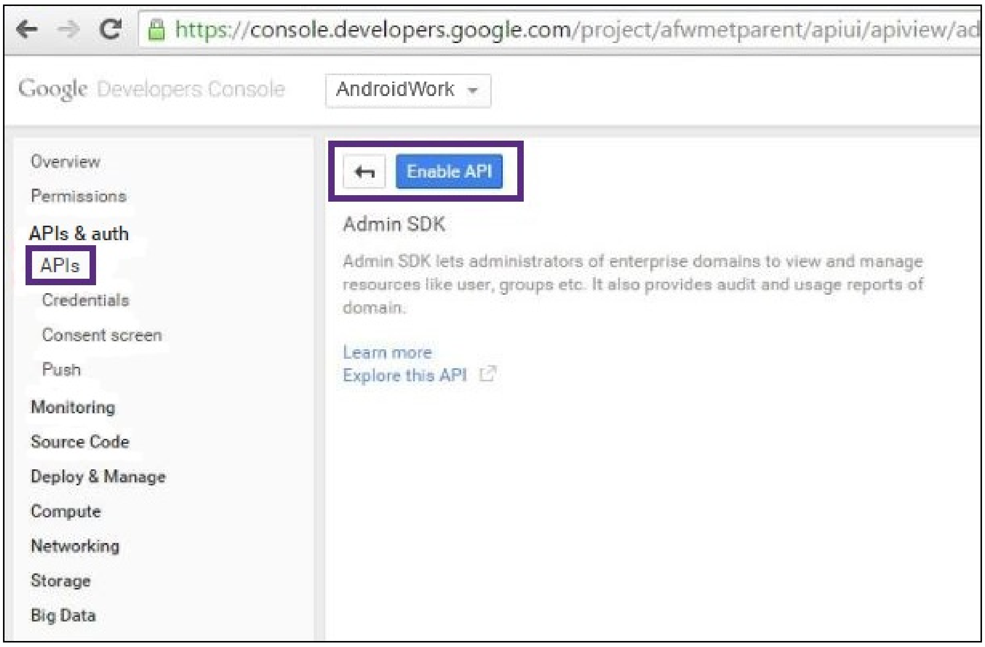
Project name: AndroidWork

Your project ID will be androidwork-1042 Edit

Show advanced options...

☑ I agree that my use of any services and related APIs is subject to my compliance with the applicable Terms of Service.

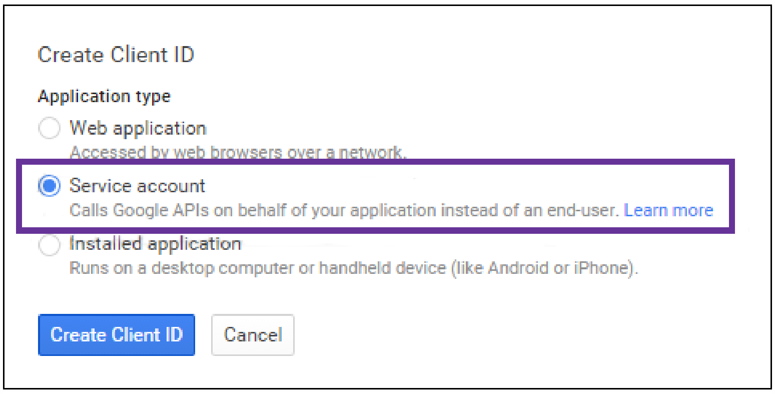
5. In the left-hand pane, click **APIs & auth**, and then click **APIs**.



https://console.developers.google.com/project/afwmetparent/apiui/apiview/ad

Admin SDK

Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.



Create Client ID

Application type

○ Web application
Accessed by web browsers over a network.

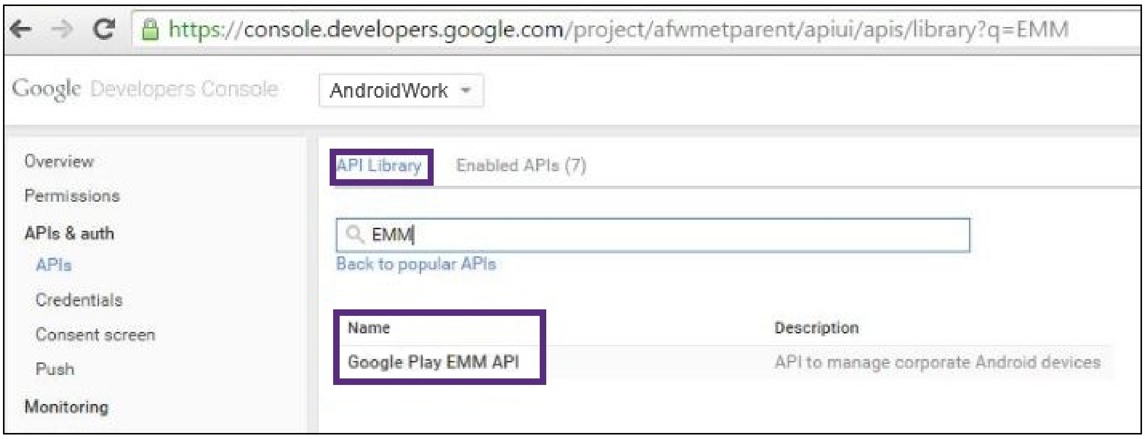
● Service account
Calls Google APIs on behalf of your application instead of an end-user. Learn more

○ Installed application
Runs on a desktop computer or handheld device (like Android or iPhone).

6. Under **Google Apps APIs**, click **Admin SDK**. Alternatively, you can type "Admin SDK" in the search field and then click **Admin SDK** on the search results page.

7. Click **Enable API**.

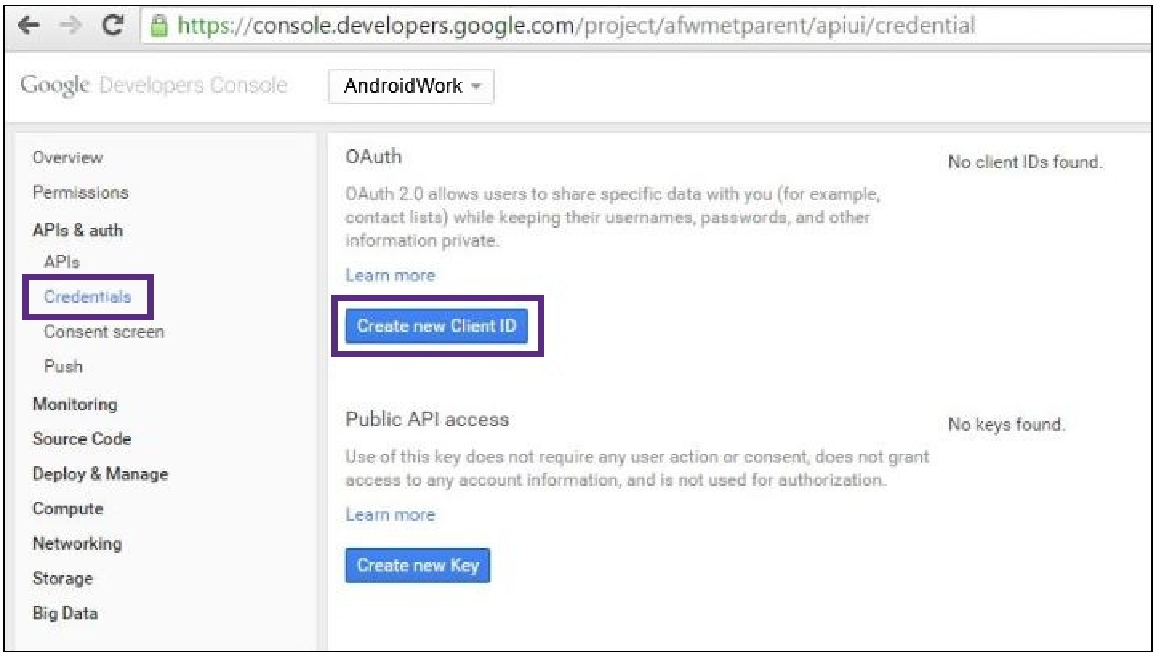
8. Under **API Library**, search for **EMM** and select **Google Play EMM API.**



Name	Description
Google Play EMM API	API to manage corporate Android devices

9. Click **Enable API.**

10. On the same page, in the left-hand pane under **APIs & auth**, click **Credentials**.



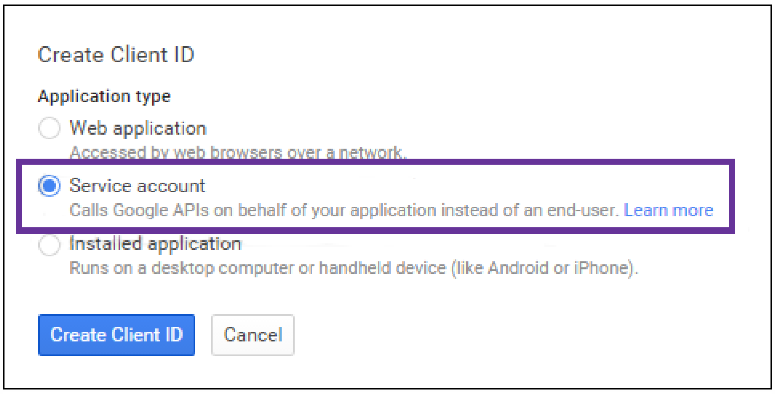
OAuth 2.0 allows users to share specific data with you (for example, contact lists) while keeping their usernames, passwords, and other information private.

No client IDs found.

Use of this key does not require any user action or consent, does not grant access to any account information, and is not used for authorization.

No keys found.

11. In the right-hand pane, click **Create new Client ID**. The **Create Client ID** dialog box appears.



Create Client ID

Application type

○ Web application
Accessed by web browsers over a network.

● Service account
Calls Google APIs on behalf of your application instead of an end-user. Learn more

○ Installed application
Runs on a desktop computer or handheld device (like Android or iPhone).

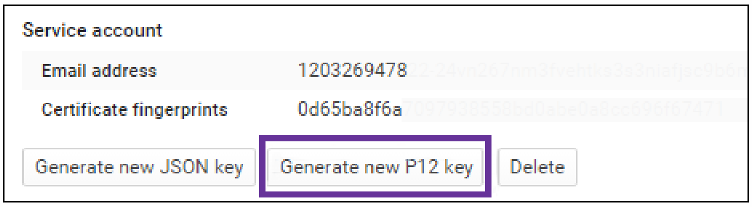
12. Select **Service account** and click **Create Client ID**.

13. Click **Okay, got it**. After you click Okay, got it, a json file is downloaded to your computer. Be sure to save the file to a secure location.

Under **Service account**, note the email address and the certificate fingerprints (password). You will need both in later steps.

The email address is the service account that you use when binding XenMobile as your EMM provider and to enable API client access.

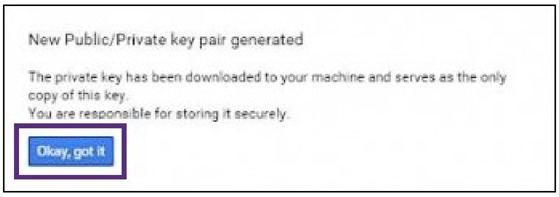
14. Under **Service account**, click **Generate new P12 key**. The certificate (P12 file) is downloaded to your computer. Be sure to save the certificate in a secure location.



Service account

Email address	1203269478
Certificate fingerprints	0d65ba8f6a

15. Click **Okay, got it**.

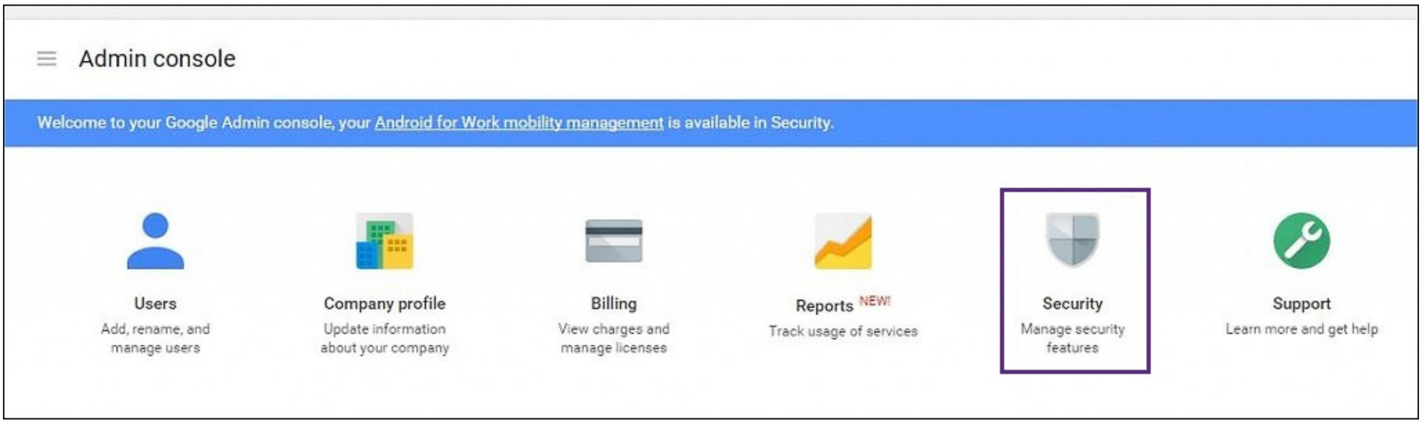


New Public/Private key pair generated

The private key has been downloaded to your machine and serves as the only copy of this key.
You are responsible for storing it securely.

16. Log on to the Google Admin portal at https://admin.google.com with your Google Android for Work administrator credentials.

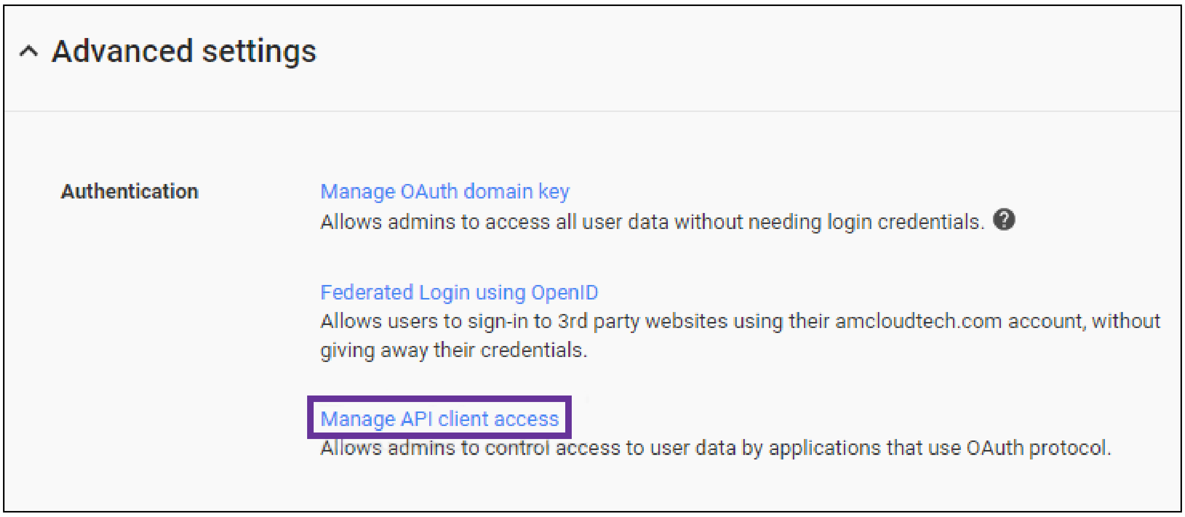
17. Click **Security**.



Admin console

Welcome to your Google Admin console, your Android for Work mobility management is available in Security.

18. Click **Advanced Settings** and then click **Manage API client** access.



Advanced settings

Authentication

Manage OAuth domain key
Allows admins to access all user data without needing login credentials.

Federated Login using OpenID
Allows users to sign-in to 3rd party websites using their amcloudtech.com account, without giving away their credentials.

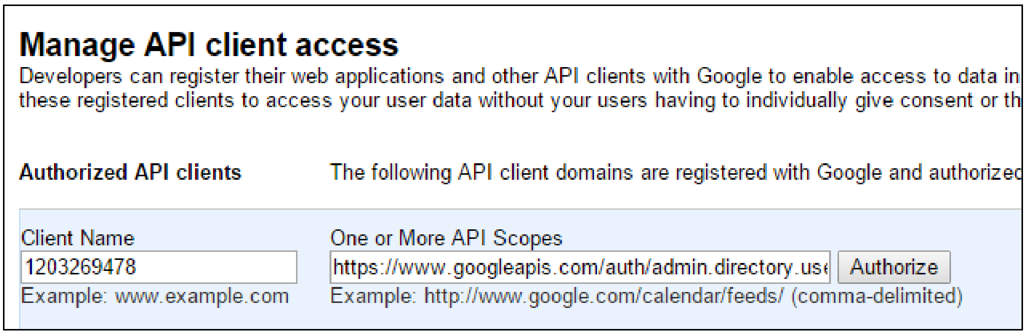
Manage API client access
Allows admins to control access to user data by applications that use OAuth protocol.

19. Click **Authorized API clients**. The **Manage API client access** page appears.

20. In **Client Name**, type the client ID generated in step 14.

21. In **One or More API Scopes**, enter "https://www.googleapis.com/auth/admin.directory.user" (without quotation marks).

22. Click **Authorize**.



Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in these registered clients to access your user data without your users having to individually give consent or th

Authorized API clients

The following API client domains are registered with Google and authorizec

Client Name: 1203269478
Example: www.example.com

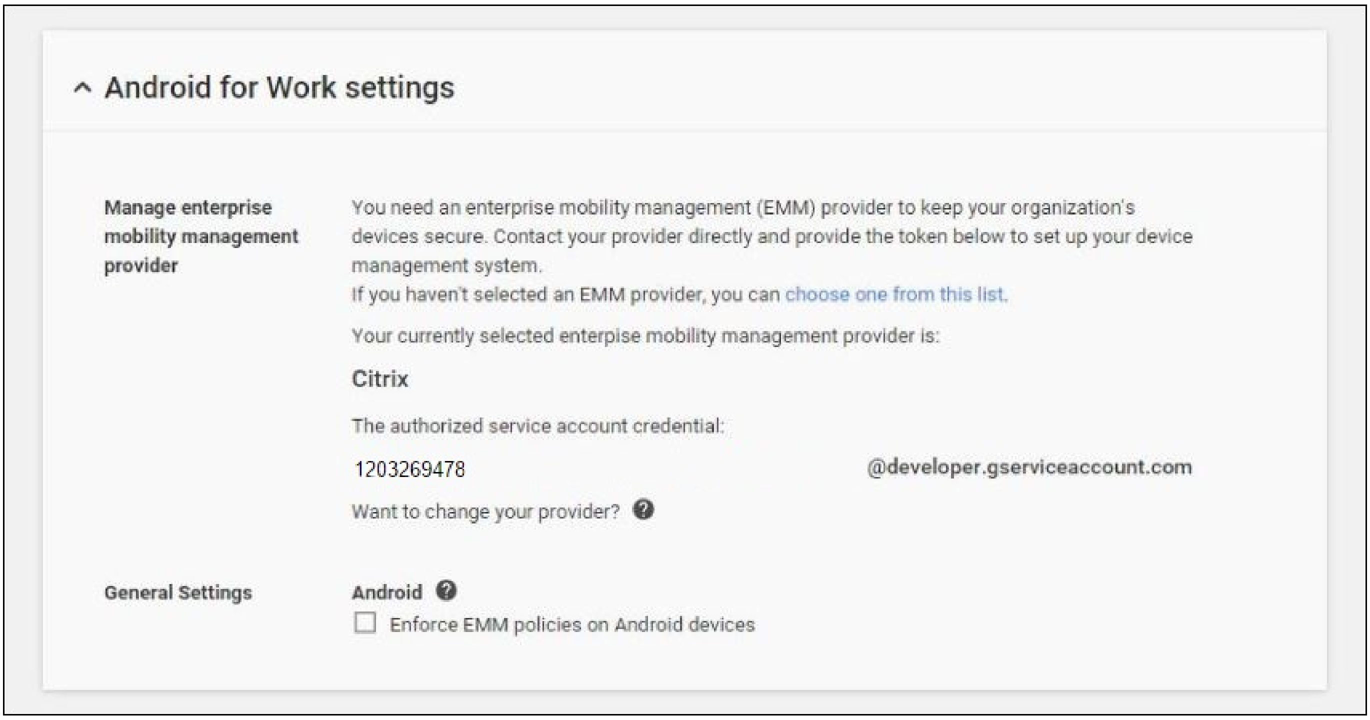
One or More API Scopes: https://www.googleapis.com/auth/admin.directory.use
Example: http://www.google.com/calendar/feeds/ (comma-delimited)

Binding to EMM

Before you can use the XenMobile to manage your Android for Work devices, you must contact Citrix Technical Support (https://www.citrix.com/contact/technical-support.html) and provide your domain name, service account, and binding token. Citrix will bind the token to XenMobile as your Enterprise Mobility Management (EMM) provider.

1. To confirm the binding, log on to the Google Admin portal and click **Security**.

2. Click **Android for Work settings**. You will see that your Google Android for Work account is bound to Citrix as your EMM provider.



^ Android for Work settings

Manage enterprise mobility management provider

You need an enterprise mobility management (EMM) provider to keep your organization's devices secure. Contact your provider directly and provide the token below to set up your device management system.
If you haven't selected an EMM provider, you can choose one from this list.

Your currently selected enterprise mobility management provider is:

Citrix

The authorized service account credential:

1203269478 @developer.gserviceaccount.com

Want to change your provider?

General Settings

Android

☐ Enforce EMM policies on Android devices

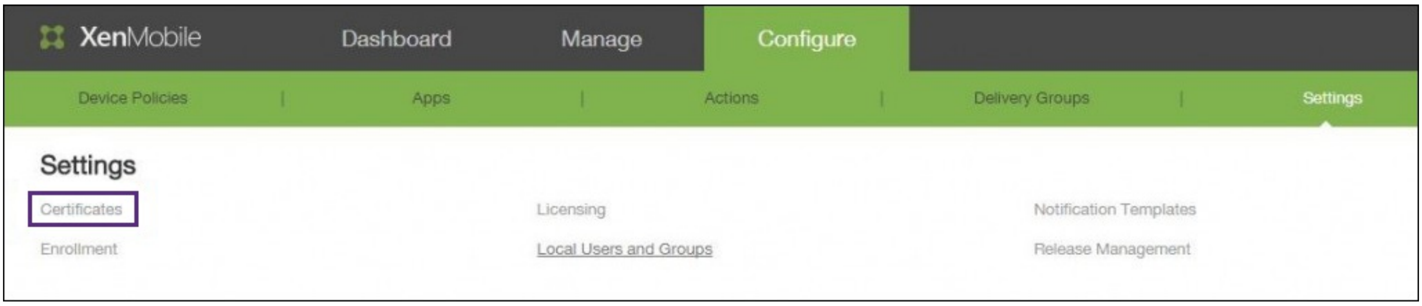
After you confirm the token binding, you can start using the XenMobile to manage your Android for Work devices. You have to import the P12 certificate you generated in step 14, set up Android for Work server settings, enable SAML-based single-sign-on, and define at least one Android for Work device policy.

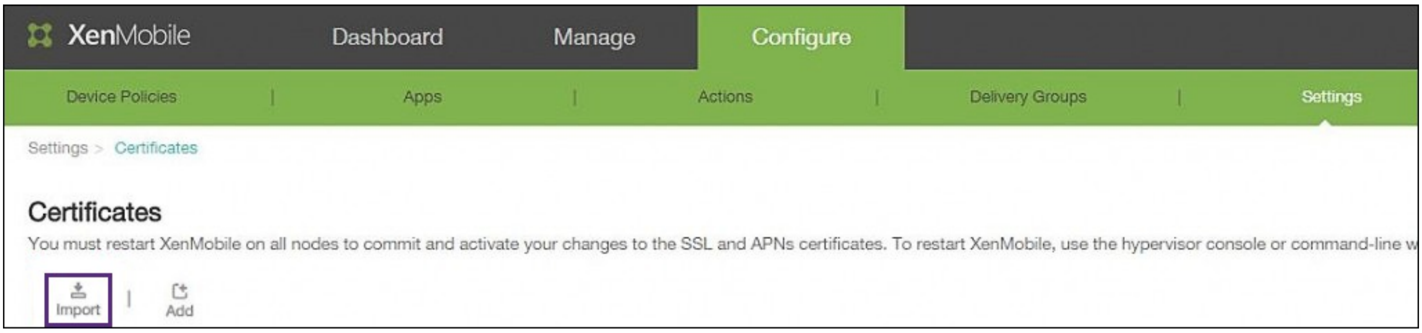
Import P12 certificate

Follow these steps to import your Android for Work P12 certificate:

1. Log on to the XenMobile 10.1 console.

2. Click **Configure->Settings->Certificate**. The **Certificates** page appears.

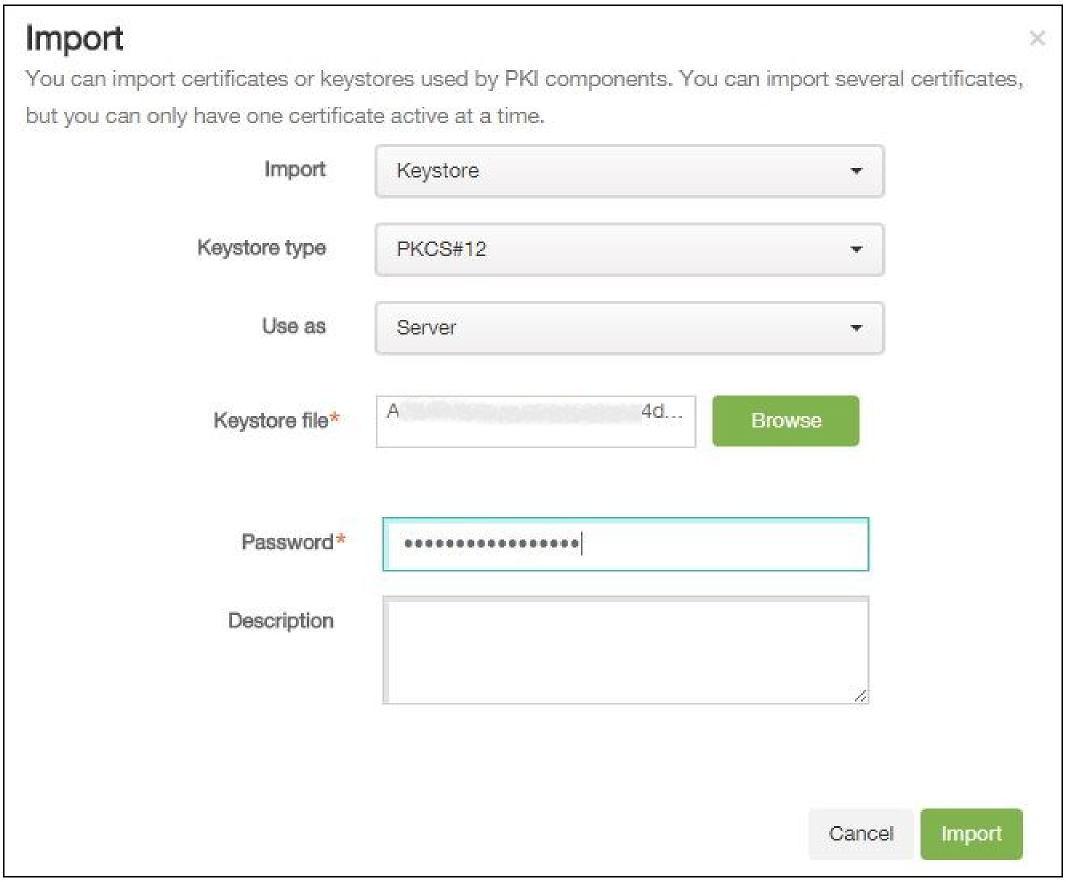




Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and APNs certificates. To restart XenMobile, use the hypervisor console or command-line w

3. Click **Import**. The **Import** dialog box appears. Configure the following settings:



Import

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

Import: Keystore

Keystore type: PKCS#12

Use as: Server

Keystore file*: A[redacted]4d...

Password*: ••••••••••••••••

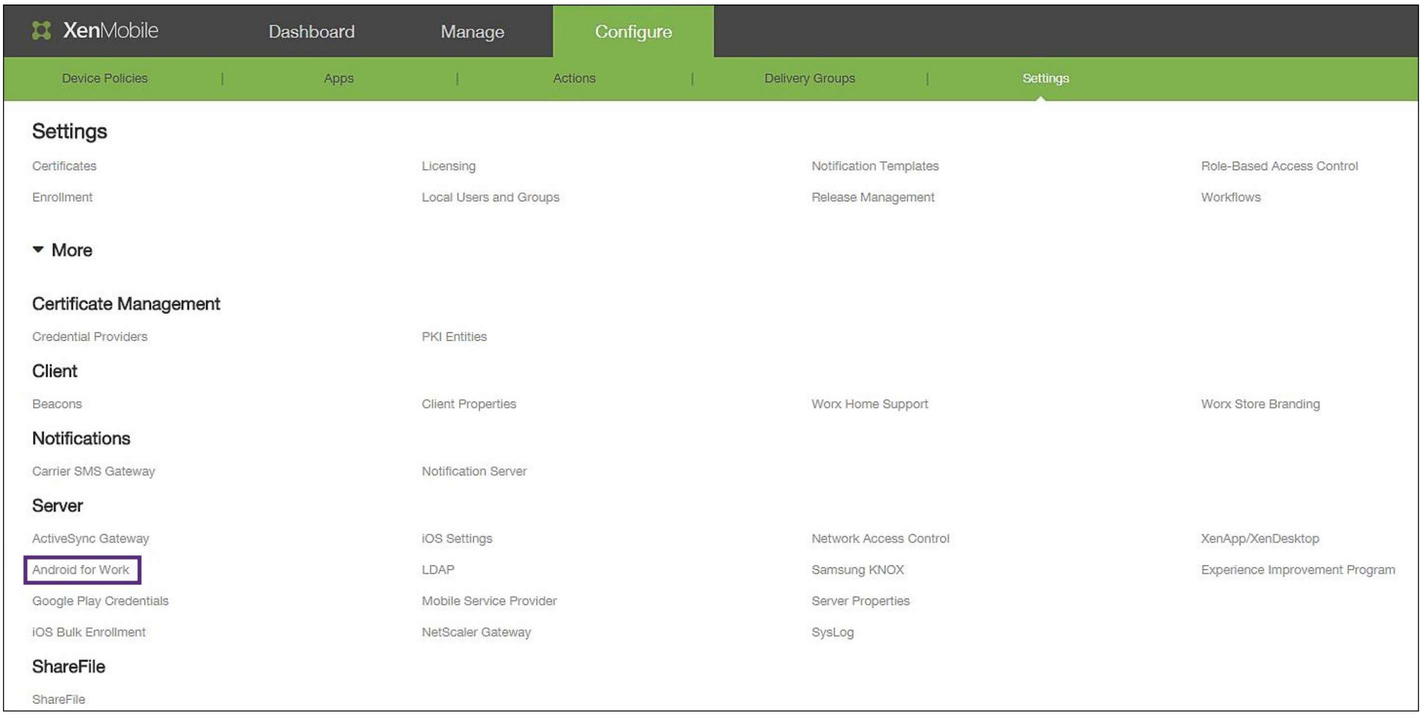
Description:

- **Import**: In the list, click Keystore.
- **Keystore type**: In the list, click PKCS#12.
- **Use as**: In the list, click Server.
- **Keystore file**: Click Browse and navigate to the P12 certificate.
- **Password**: Type the keystore password.
- **Description**: Optionally, type a description of the certificate.

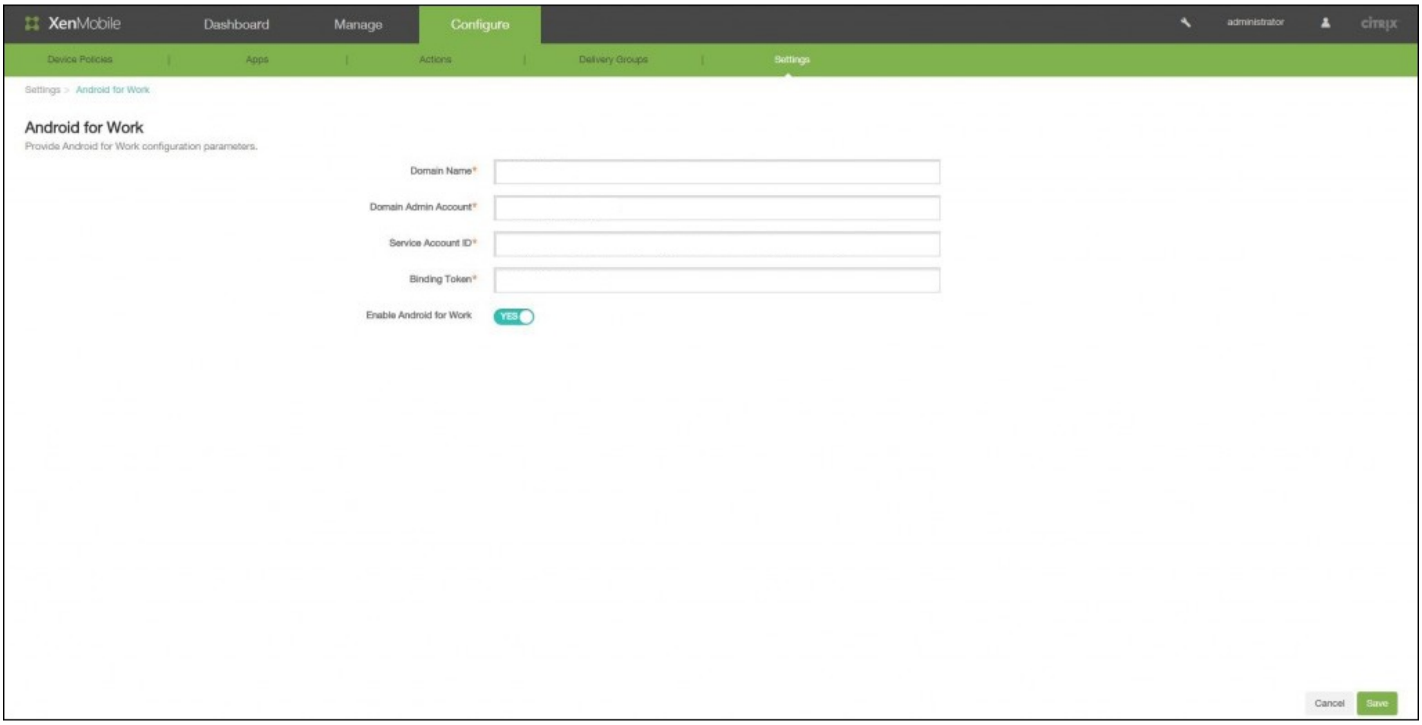
4. Click **Import**.

Set up Android for Work server settings

1. Click **Configure->Settings** and then expand **More**.



2. Under **Server**, click **Android for Work**. The **Android for Work** page appears. Configure the following settings:



Android for Work

Provide Android for Work configuration parameters.

Domain Name*

Domain Admin Account*

Service Account ID*

Binding Token*

Enable Android for Work: YES

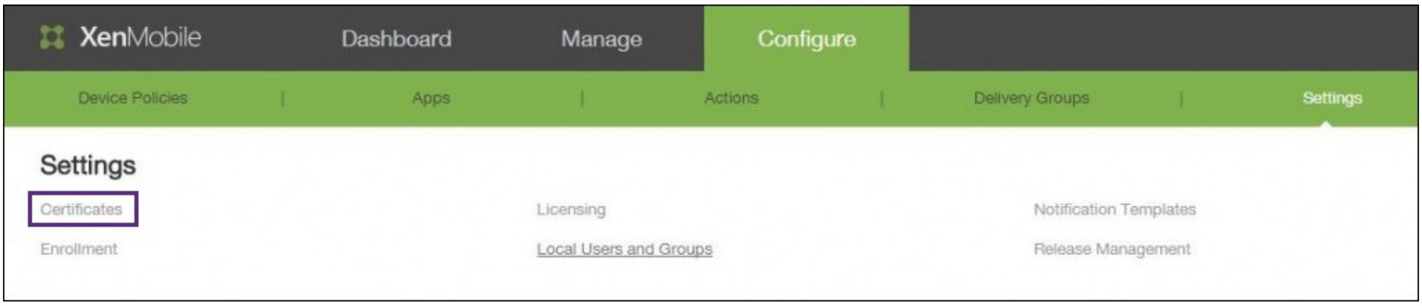
- **Domain name**: Type your Android for Work domain name.
- **Domain Admin Account**: Type your domain administrator user name.
- **Service Account ID**: Type your service account ID.
- **Binding Token**: Type, or copy and paste, the binding token.
- **Enable Android for Work**: Click to enable or disable Android for Work.

3. Click **Save**.

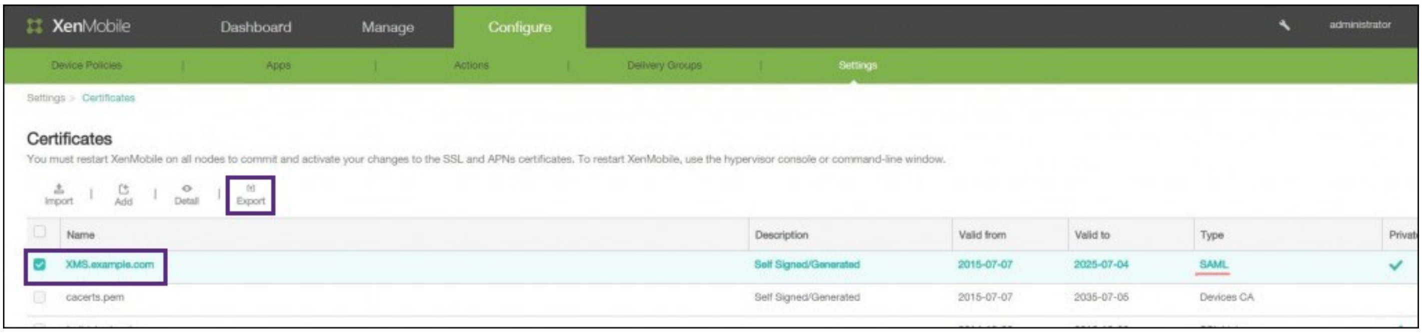
Enable SAML-based single-sign-on

1. Log on to the XenMobile 10.1 console.

2. Click **Configure->Settings->Certificate**. The **Certificates** page appears.



3. On the **Certificates** page, in the list of certificates, click the SAML certificate.



Certificates

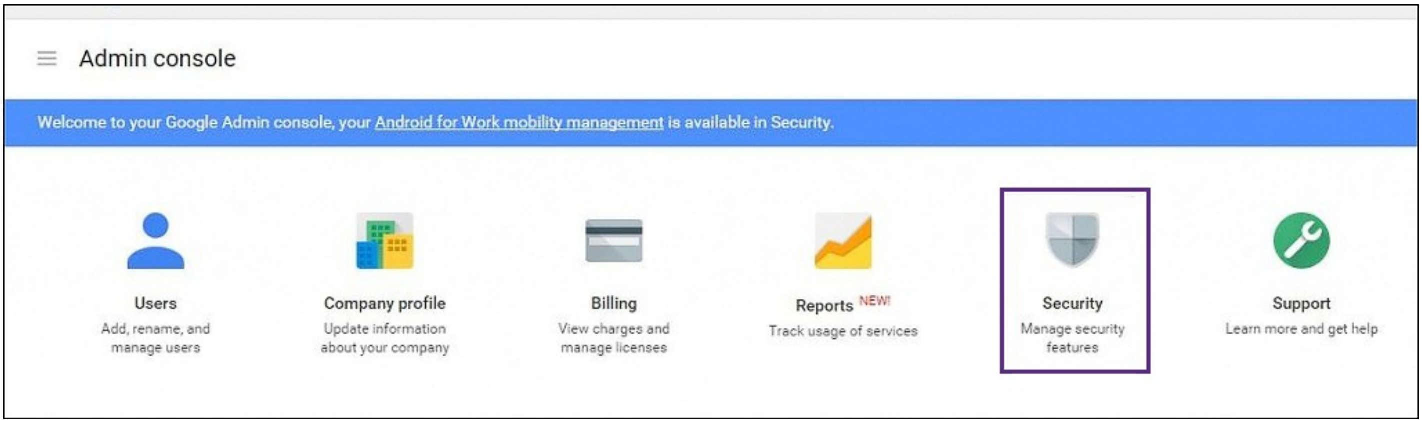
You must restart XenMobile on all nodes to commit and activate your changes to the SSL and APNs certificates. To restart XenMobile, use the hypervisor console or command-line window.

	Name	Description	Valid from	Valid to	Type	Privat
☑	XMS.example.com	Self Signed/Generated	2015-07-07	2025-07-04	SAML	✓
□	cacerts.pem	Self Signed/Generated	2015-07-07	2035-07-05	Devices CA	

4. Click **Export** and save the certificate to your computer.

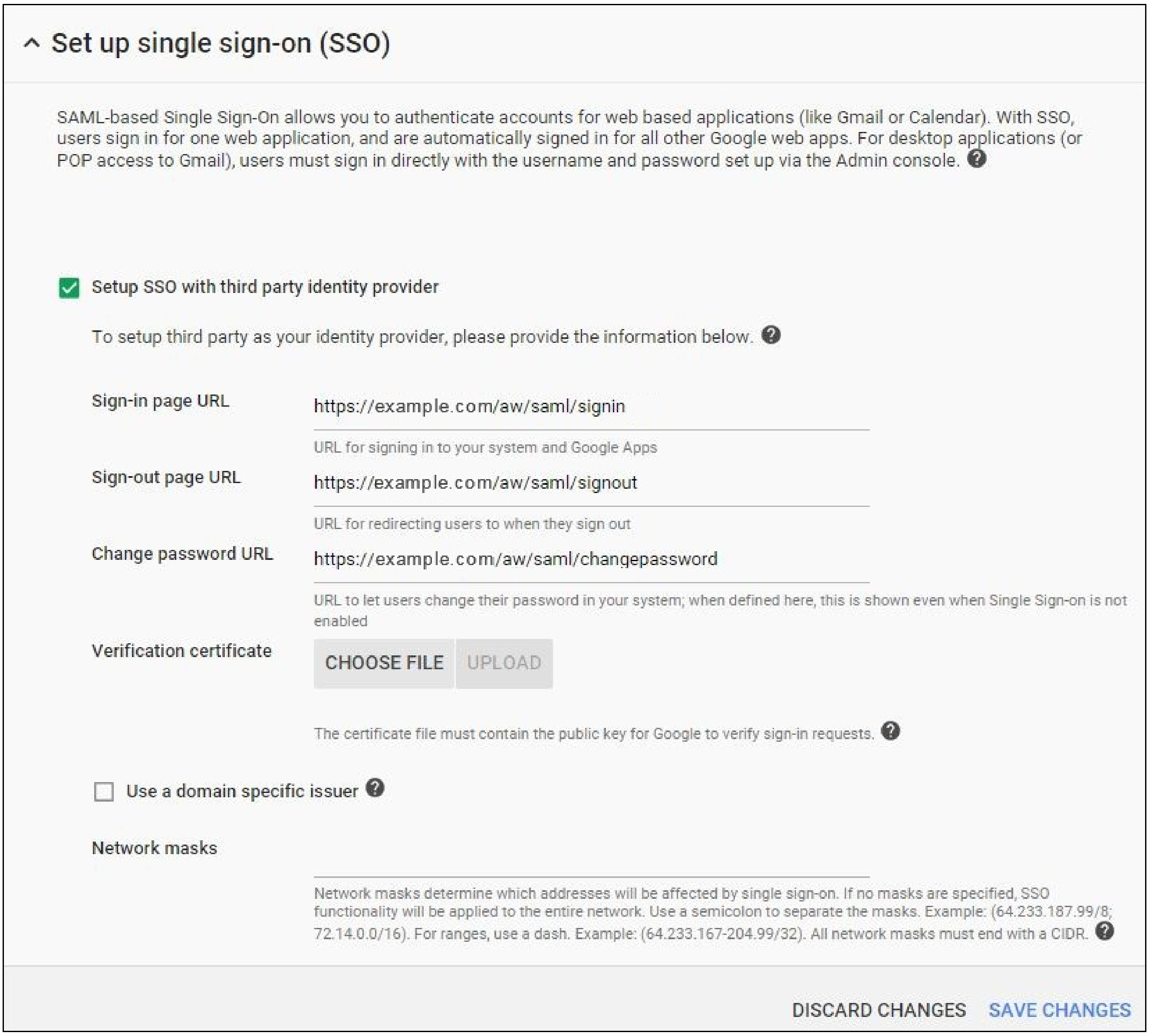
5. Log on to the Google Admin portal (https://admin.google.com) with your Android for Work administrator credentials.

6. Click **Security**.



Welcome to your Google Admin console, your Android for Work mobility management is available in Security.

7. Under **Security**, click **Set up single sign-on (SSO)** and configure the following settings:



^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

☑ Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL: https://example.com/aw/saml/signin

URL for signing in to your system and Google Apps

Sign-out page URL: https://example.com/aw/saml/signout

URL for redirecting users to when they sign out

Change password URL: https://example.com/aw/saml/changepassword

URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate

The certificate file must contain the public key for Google to verify sign-in requests. ?

□ Use a domain specific issuer ?

Network masks

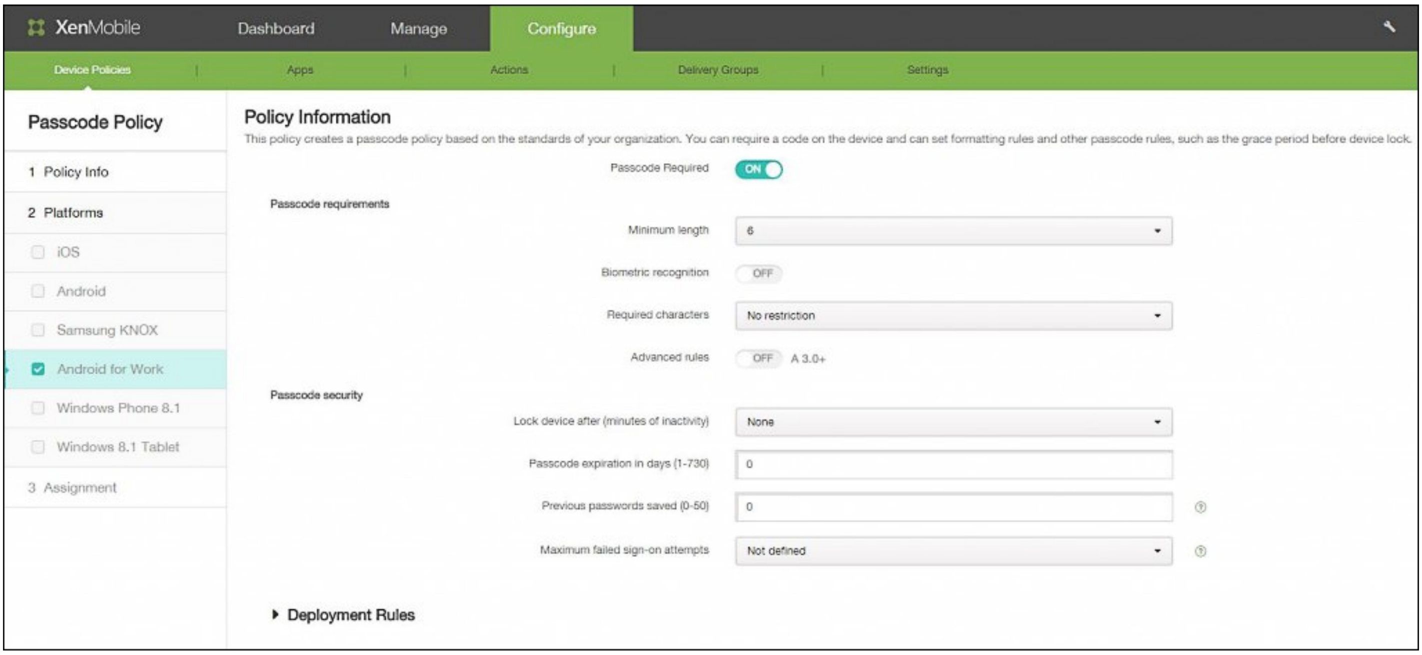
Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

- **Sign-in page URL**: Type the URL for users signing in to your system and Google Apps. For example: https://<Xebmobile-FQDN>/aw/saml/signin.
- **Sign-out page URL**: Type the URL to which users are redirected when the sign out. For example: https://<Xebmobile-FQDN>/aw/saml/signout.
- **Change password URL**: Type the URL to let users change their password in your system. For example: https://<Xebmobile-FQDN>/aw/saml/changepassword. When defined here, users see this even if SSO is not available.
- **Verification certificate**: Click CHOOSE FILE and navigate to the SAML certificate exported from XenMobile.

8. Click **SAVE CHANGES**.

Set up an Android for Work device policy

You can set up any device policy you want, but it is wise to set up a passcode policy so that users are required to establish a passcode on their devices when they first enroll.



Policy Information

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode Required: ON

Passcode requirements

Minimum length: 6

Biometric recognition: OFF

Required characters: No restriction

Advanced rules: OFF A 3.0+

Passcode security

Lock device after (minutes of inactivity): None

Passcode expiration in days (1-730): 0

Previous passwords saved (0-50): 0

Maximum failed sign-on attempts: Not defined

The basic steps to setting up any device policy are:

1. Log on to the XenMobile 10.1 console.

2. Click **Configure->Device Policies**.

3. Click **Add** and then select the policy you want to add from the **Add a New Policy** dialog box (in this example, you would click **Passcode**).

4. Complete the **Policy Information** page.

5. Click **Android for Work** and configure the settings for the policy.

6. Assign the policy to a delivery group.

For more information on setting up device policies, see Device Policies.

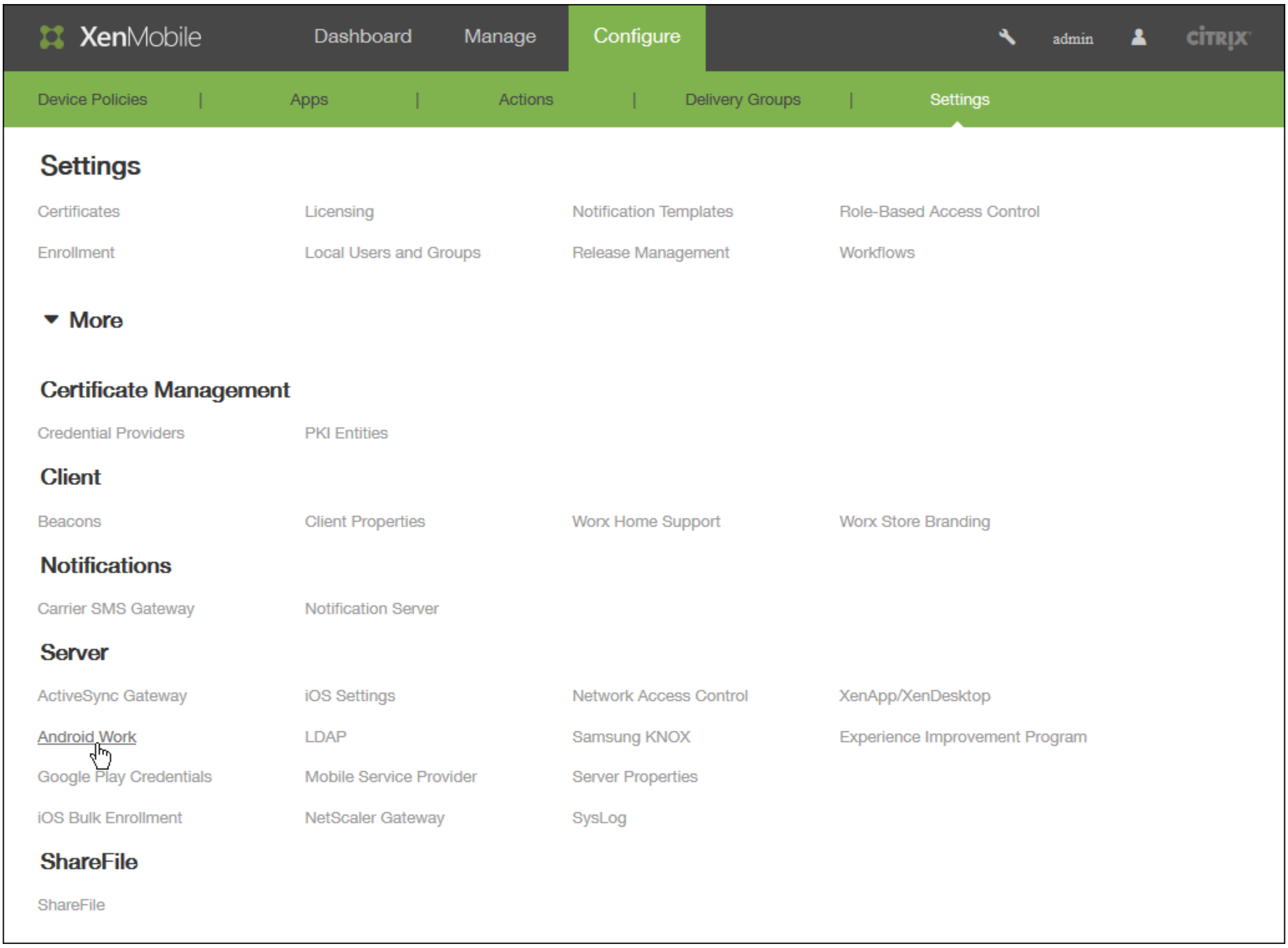
Your users can now download the Worx Home app from the Google Play store and enroll their devices in XenMobile (be sure to use user principal name for enrollment). After the devices successfully enroll, Worx Home will install the Android for Work profile so that users can access their Android for Work apps. Users may be asked to encrypt their devices during this process before they can continue.

Configure Android for Work account settings

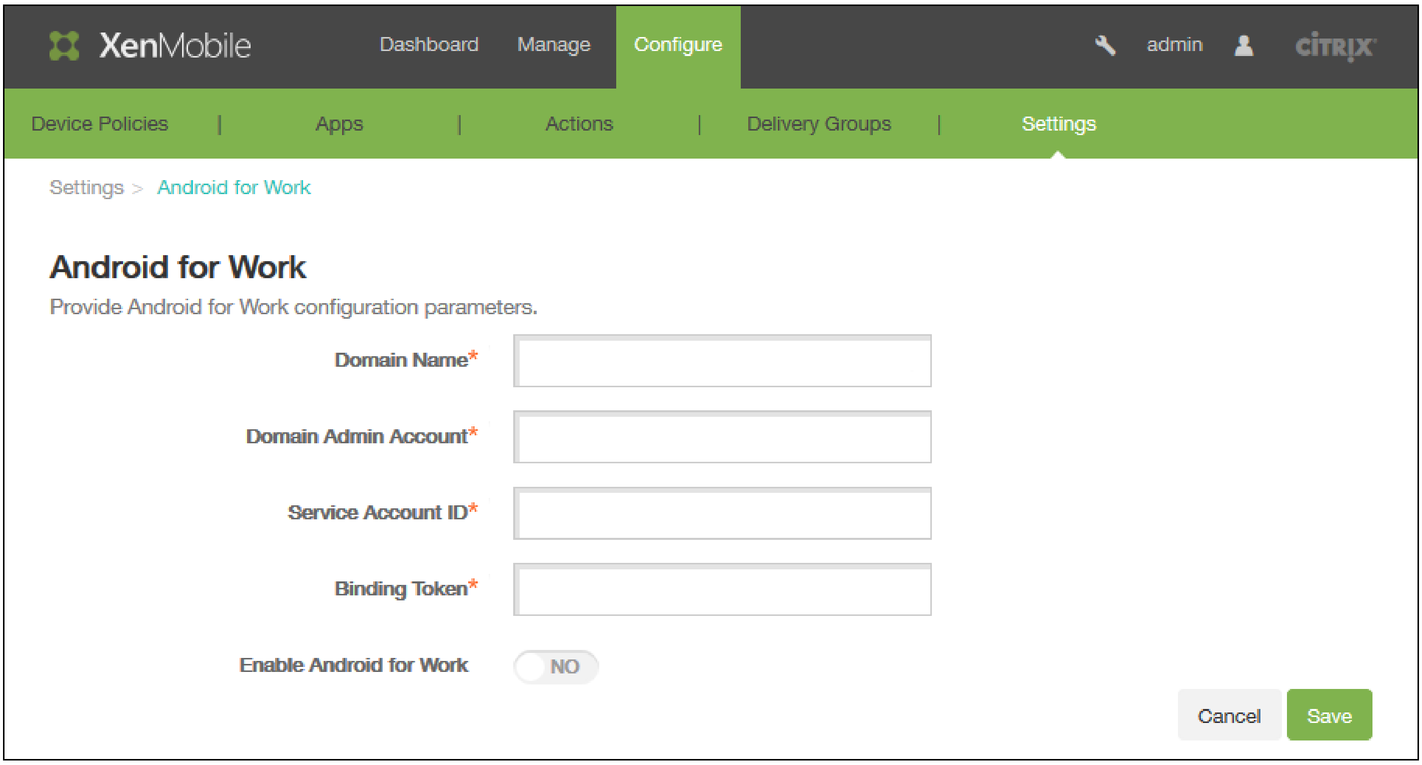
Jul 28, 2015

Before you can start managing Android for Work apps and policies on users' devices you must set up Android for Work domain and account information in XenMobile. Before doing that, however, you must complete Android for Work setup tasks on Google to set up a domain administrator, and obtain a service account ID and a binding token. For more information on Android for Work setup tasks on Google, see Managing Devices with Android for Work.

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



2. Expand **More** and then under **Server**, click **Android for Work**. The **Android for Work** page appears.



Android for Work

Provide Android for Work configuration parameters.

Domain Name*

Domain Admin Account*

Service Account ID*

Binding Token*

Enable Android for Work NO

3. On the **Android for Work** page, configure the following settings:

- **Domain Name**: Type your domain name.
- **Domain Admin Account**: Type your domain administrator user name.
- **Service Account ID**: Type your Google Service Account ID.
- **Binding Token**: Type, or paste, the binding token you received from Google when you set up your Android for Work account.
- **Enable Android for Work**: Select whether to enable Android for Work.

4. Click **Save**.

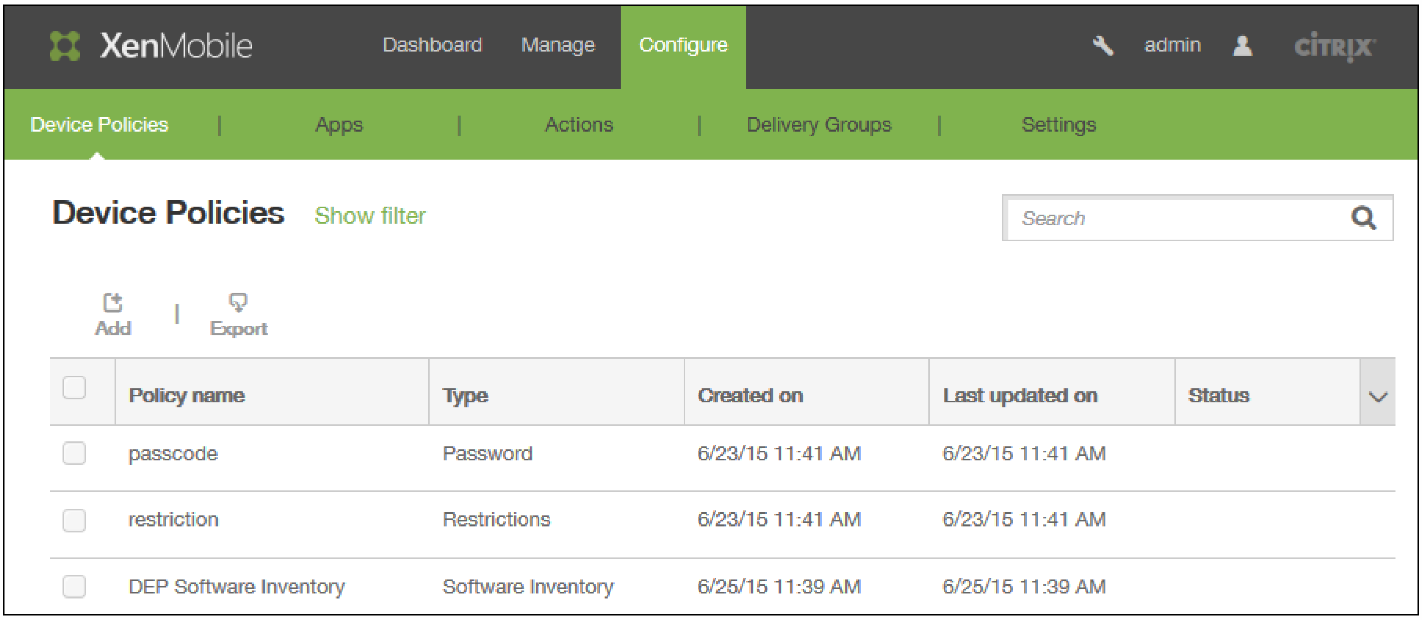
Android for Work app restriction policy

Jul 13, 2015

You can modify the restrictions associated with Android for Work apps, but before you can do so, you must meet the following prerequisites:

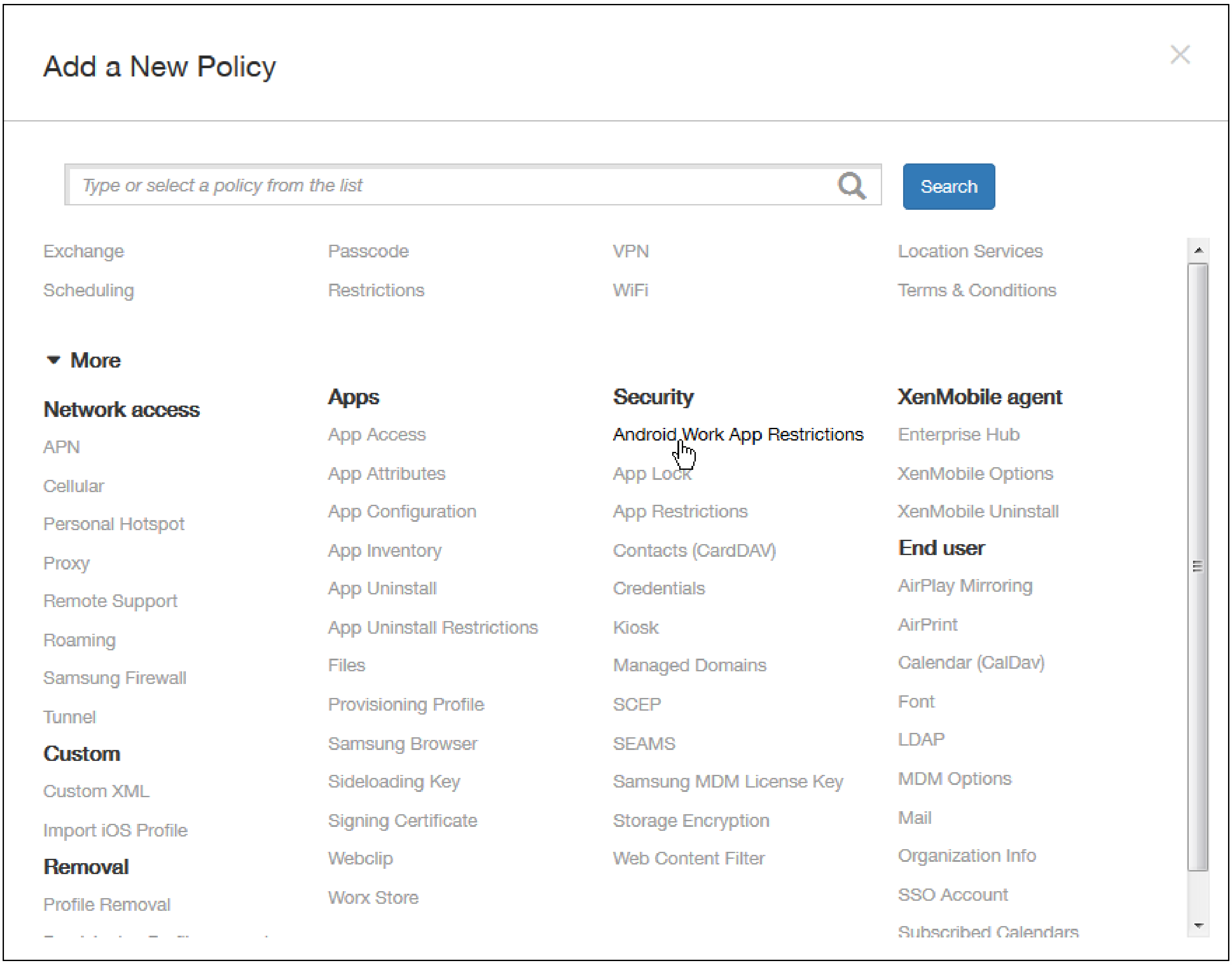
- Complete Android for Work setup tasks on Google. For more information, see Managing Devices with Android for Work.
- Create a set of Google Play Credentials. For more information, see Google Play Credentials.
- Configure Android for Work account settings. For more information, see Configure Android for Work account settings.
- Add Android for Work apps to XenMobile. For more information, see Adding Apps to XenMobile.

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

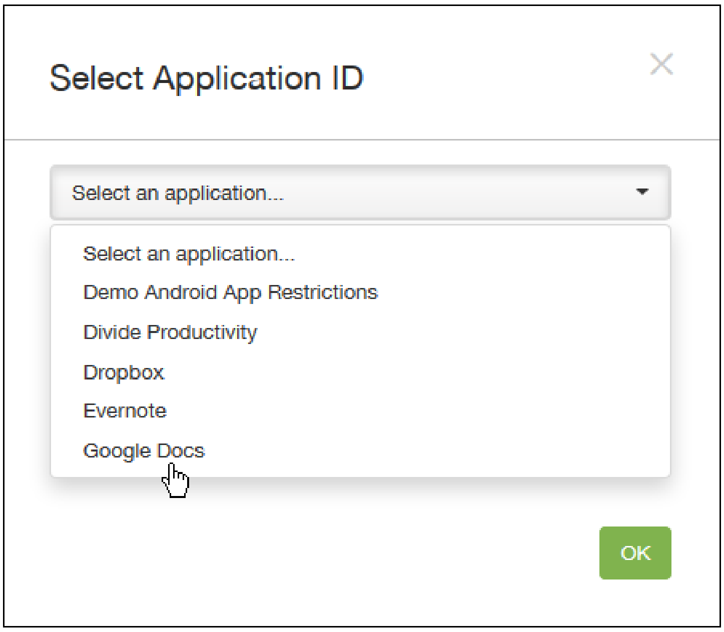


□	Policy name	Type	Created on	Last updated on	Status
□	passcode	Password	6/23/15 11:41 AM	6/23/15 11:41 AM	
□	restriction	Restrictions	6/23/15 11:41 AM	6/23/15 11:41 AM	
□	DEP Software Inventory	Software Inventory	6/25/15 11:39 AM	6/25/15 11:39 AM	

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



3. On the **Add a New Policy** page, click **More** and then under **Security**, click **Android for Work App Restrictions**. A dialog box appears asking you to select an app.



Select Application ID

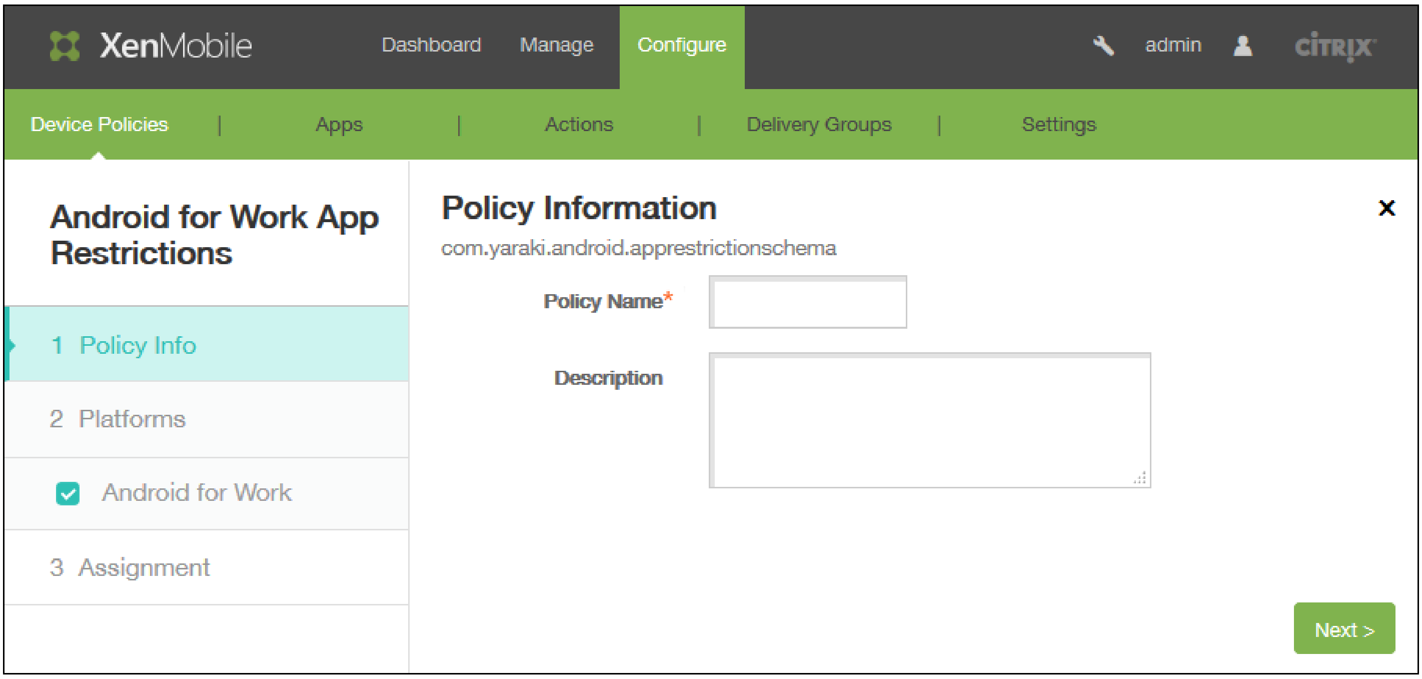
Select an application...

Select an application...
Demo Android App Restrictions
Divide Productivity
Dropbox
Evernote
Google Docs

OK

4. In the list, select the app to which you want to apply restrictions and then click **OK**.

- If there are no Android for Work apps added to XenMobile, you cannot proceed. For more information about adding apps to XenMobile, see Adding Apps to XenMobile.
- If the app has no restrictions associated with it, a notification to that effect appears. Click **OK** to dismiss the dialog box.
- If the app has restrictions associated with it, the **Android for Work App Restrictions Policy** information page appears.



Policy Information

com.yaraki.android.apprestrictionschema

Policy Name*

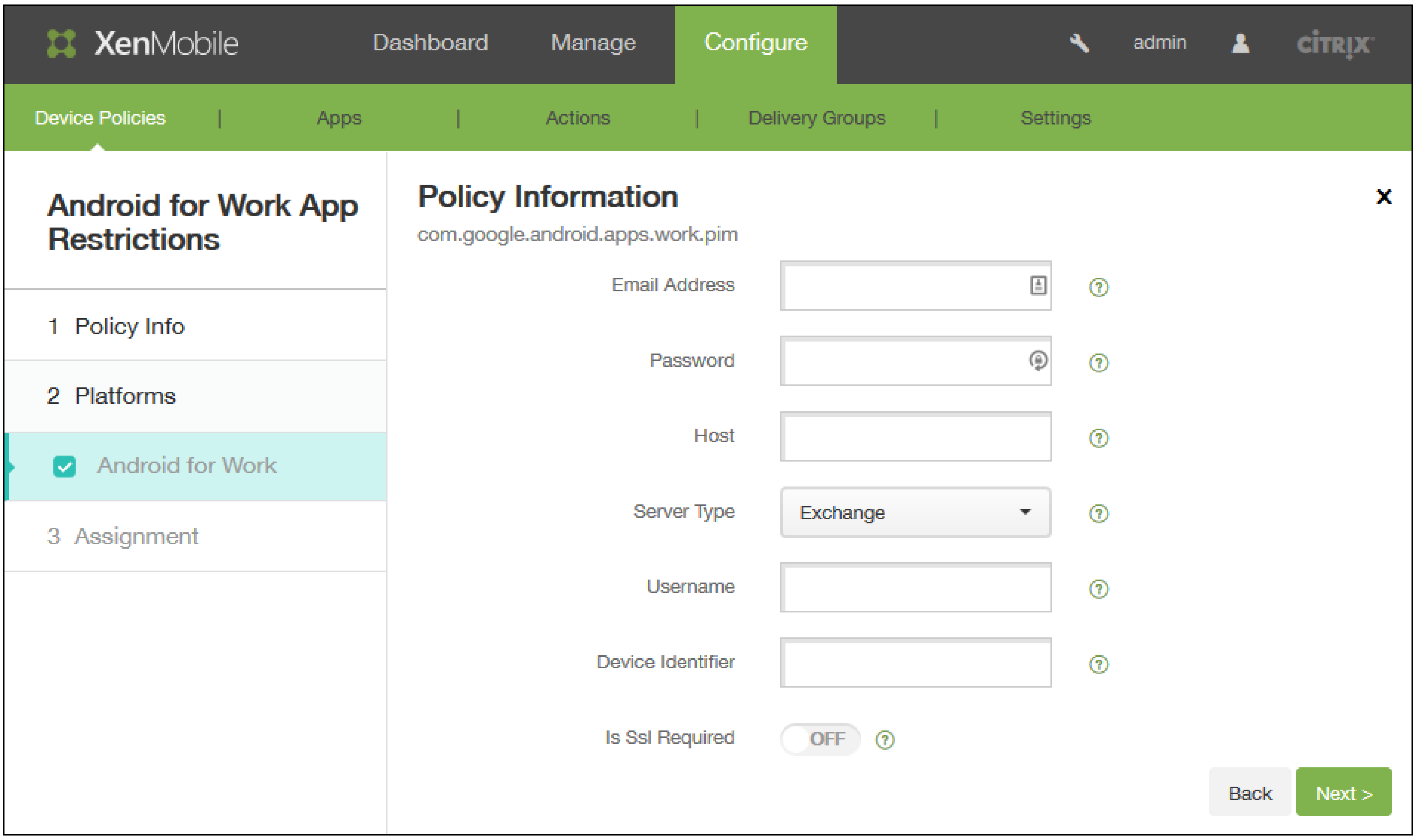
Description

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

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

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

7. Under **Platforms**, in the **Android for Work** policy information pane, configure the settings for the app you selected. The settings you see depend on the restrictions associated with the selected app. The following figure shows some of the options available for the Google Docs app.



Policy Information

com.google.android.apps.work.pim

Email Address

Password

Host

Server Type: Exchange

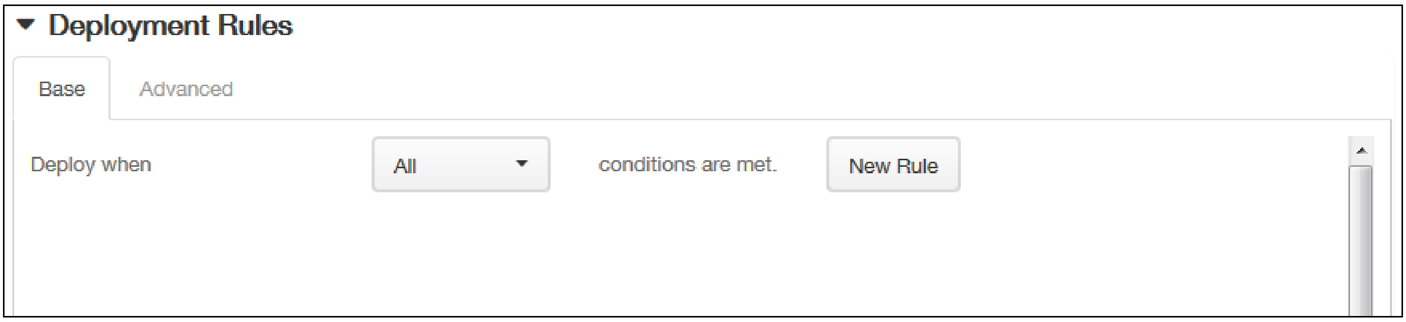
Username

Device Identifier

Is Ssl Required: OFF

8. Expand **Deployment Rules** and then configure the following settings:

The **Base** tab appears by default.



Deploy when All conditions are met.

- In the lists, click options to determine when the policy should be deployed.

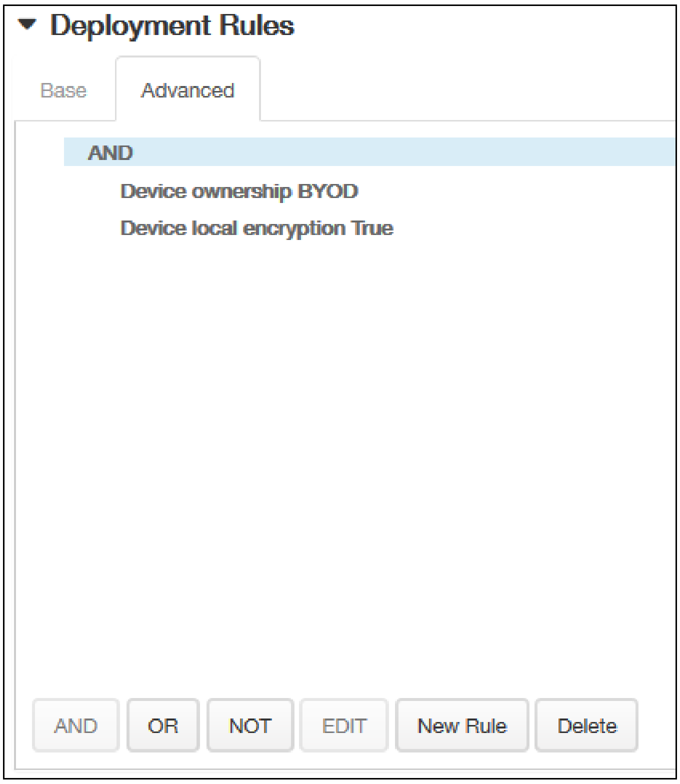
i. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is **All**.

ii. Click **New Rule** to define the conditions.

iii. In the lists, click the conditions, such as **Device ownership** and **BYOD**, as shown in the preceding figure.

iv. Click **New Rule** again if you want to add more conditions. You can add as many conditions as you would like.

- Click the **Advanced** tab to combine the rules with Boolean options.



AND

Device ownership BYOD

Device local encryption True

The conditions you chose on the Base tab appear.

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

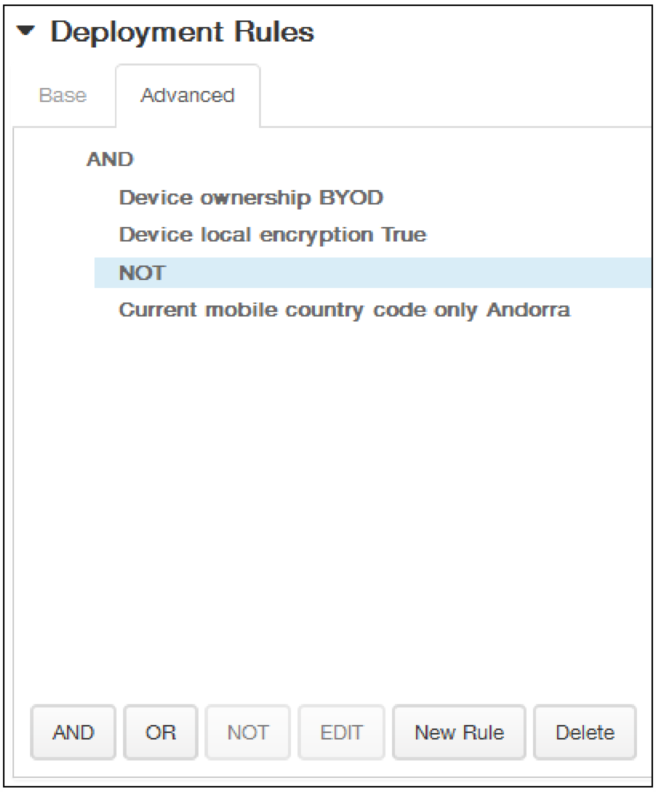
i. Click **AND**, **OR**, or **NOT**.

ii. 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.

iii. 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.



Deployment Rules

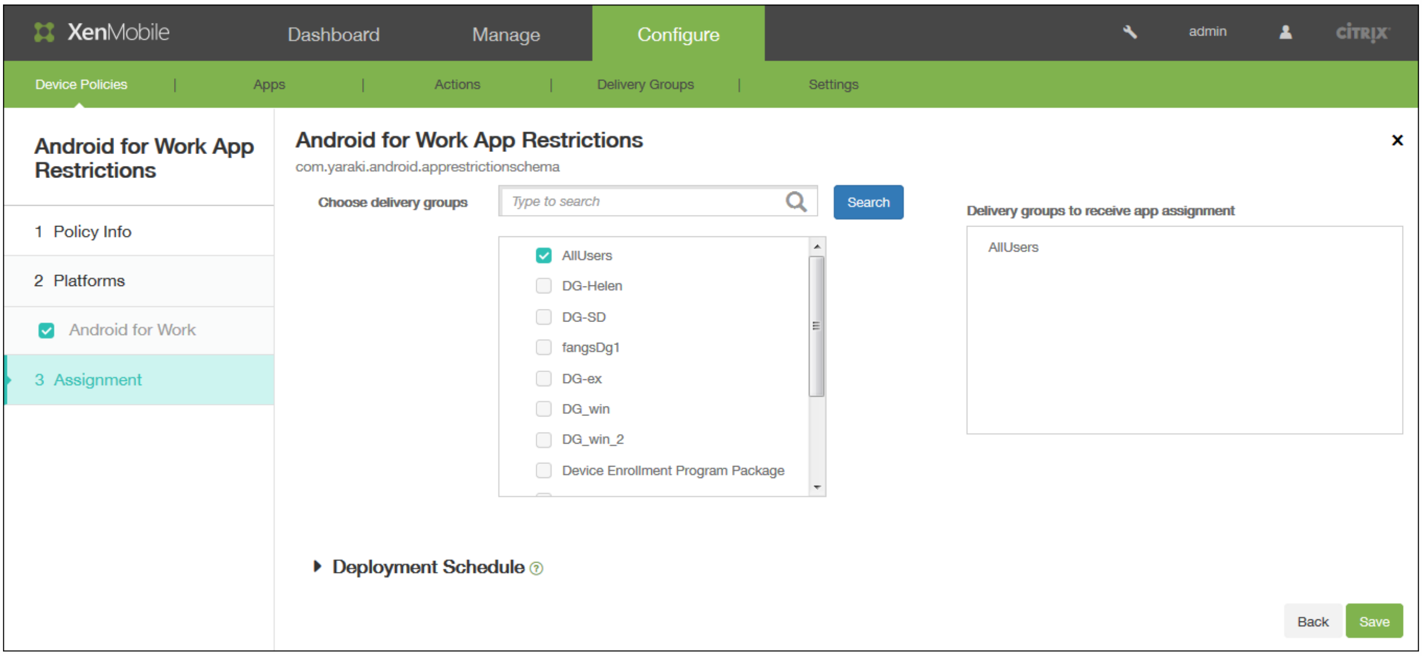
AND
Device ownership BYOD
Device local encryption True
NOT
Current mobile country code only Andorra

9. Click **Next**.

The **Android for Work App Restrictions Policy** assignment page appears.

10. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list to which you want to assign the policy.

The groups you select appear in the **Delivery groups to receive app** assignment list.



Android for Work App Restrictions
com.yaraki.android.apprestrictionschema

Choose delivery groups: Type to search

☑ AllUsers
□ DG-Helen
□ DG-SD
□ fangsDg1
□ DG-ex
□ DG_win
□ DG_win_2
□ Device Enrollment Program Package

Delivery groups to receive app assignment: AllUsers

Deployment Schedule

11. Expand **Deployment Schedule** and then configure the following settings:

- Next to **Deploy**, click **ON** to schedule deployment or click **OFF** to prevent deployment. The default option is **ON**. If you choose **OFF**, no other options need to be configured.
- Next to **Deployment schedule**, click **Now** or **Later**. The default option is **Now**.
- If you click **Later**, click the calendar icon and then select the date and time for deployment.
- Next to **Deployment condition**, click **On every connection** or click **Only when previous deployment has failed**. The default option is **On every connection**.
- Next to **Deploy for always-on connection**, click **ON** or **OFF**. The default option is **OFF**.

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

Configuring Deployment Rules and Schedules

May 25, 2016

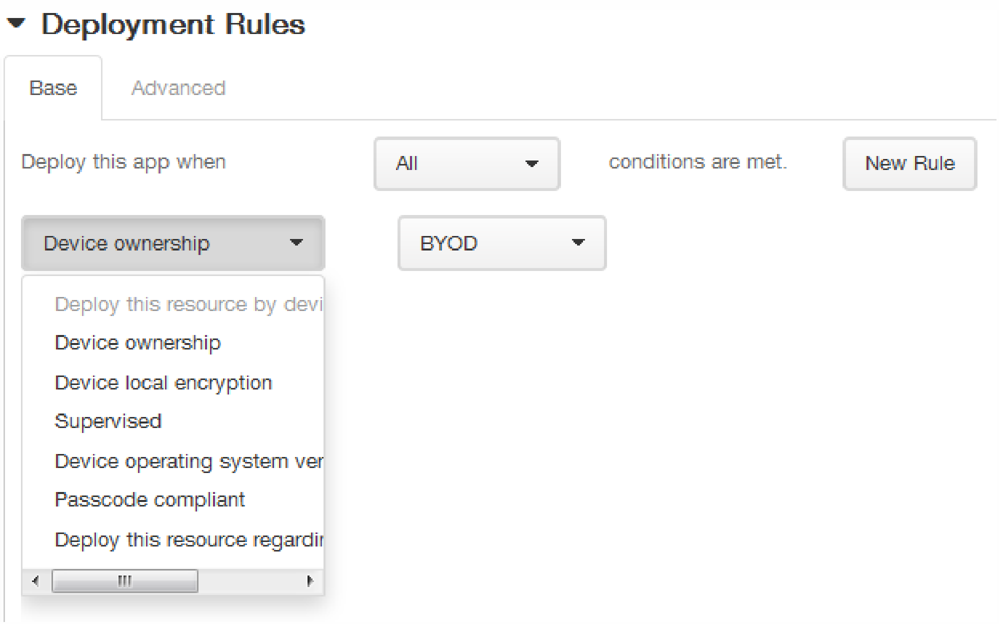
This section describes:

- 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

Deployment rules are parameters that affect the deployment outcome of a package. You can specify deployment rules for device properties, apps, and actions. XenMobile uses the deployment rules that you specify for device properties to filter policies, apps, actions, and delivery groups when determining the deployment order of a package. For more information, see Deployment Ordering.

You can based a package deployment on a specific operating system version, on a particular hardware platform, or some other combination. In this wizard used to add and edit device properties, apps, and actions are both a Baseand 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:



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.

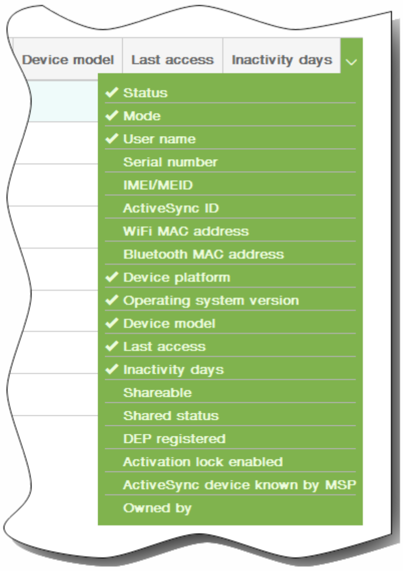
Adding Devices and Viewing Device Details

Sep 01, 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.

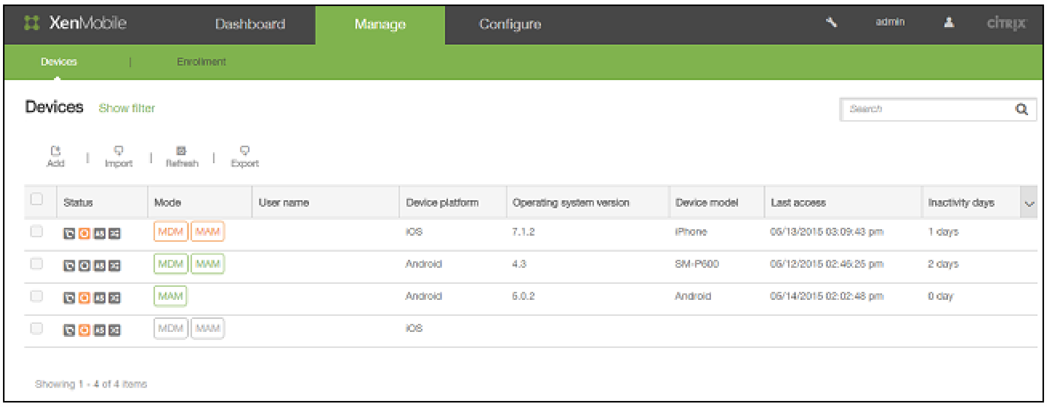
On the Devices page in the console, you'll find a table listing each of the devices, along with the following information: Status (Device not jailbroken, Device not managed, Active Sync Gateway unavailable, no deployment failure), Mode, (MDM, MAM), User name, Device platform, Operating system version, 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 from the many possible headings you want to see in the table or clearing those you do not want to see.



- ✓ Status
- ✓ Mode
- ✓ User name
- Serial number
- IMEI/MEID
- ActiveSync ID
- WiFi MAC address
- Bluetooth MAC address
- ✓ Device platform
- ✓ Operating system version
- ✓ Device model
- ✓ Last access
- ✓ Inactivity days
- Shareable
- Shared status
- DEP registered
- Activation lock enabled
- ActiveSync device known by MSP
- Owned by

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.

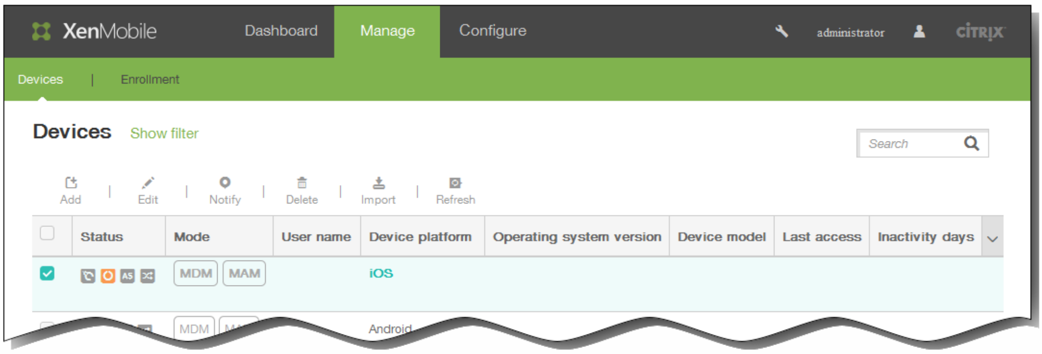


□	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days
□		MDM MAM		iOS	7.1.2	iPhone	06/13/2015 03:09:43 pm	1 days
□		MDM MAM		Android	4.3	SM-P600	06/12/2015 02:46:25 pm	2 days
□		MAM		Android	5.0.2	Android	06/14/2015 02:02:48 pm	0 day
□		MDM MAM		iOS				

Showing 1 - 4 of 4 items

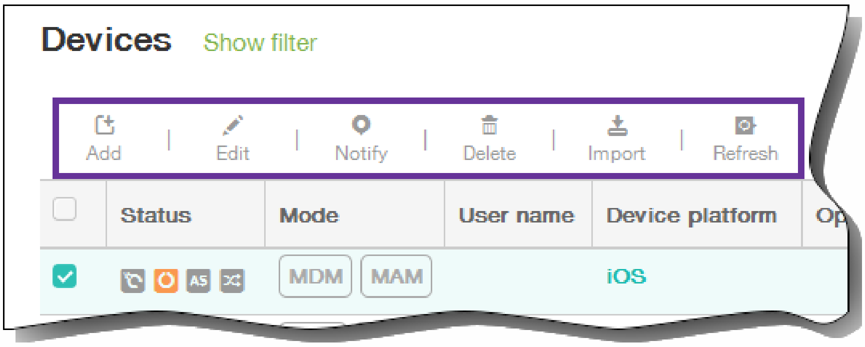
1. In the XenMobile console, click Manage > Devices and then click Add. The Add Device page appears.

2. In Select platform, click either iOS, Android, or Symbian.
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. 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.



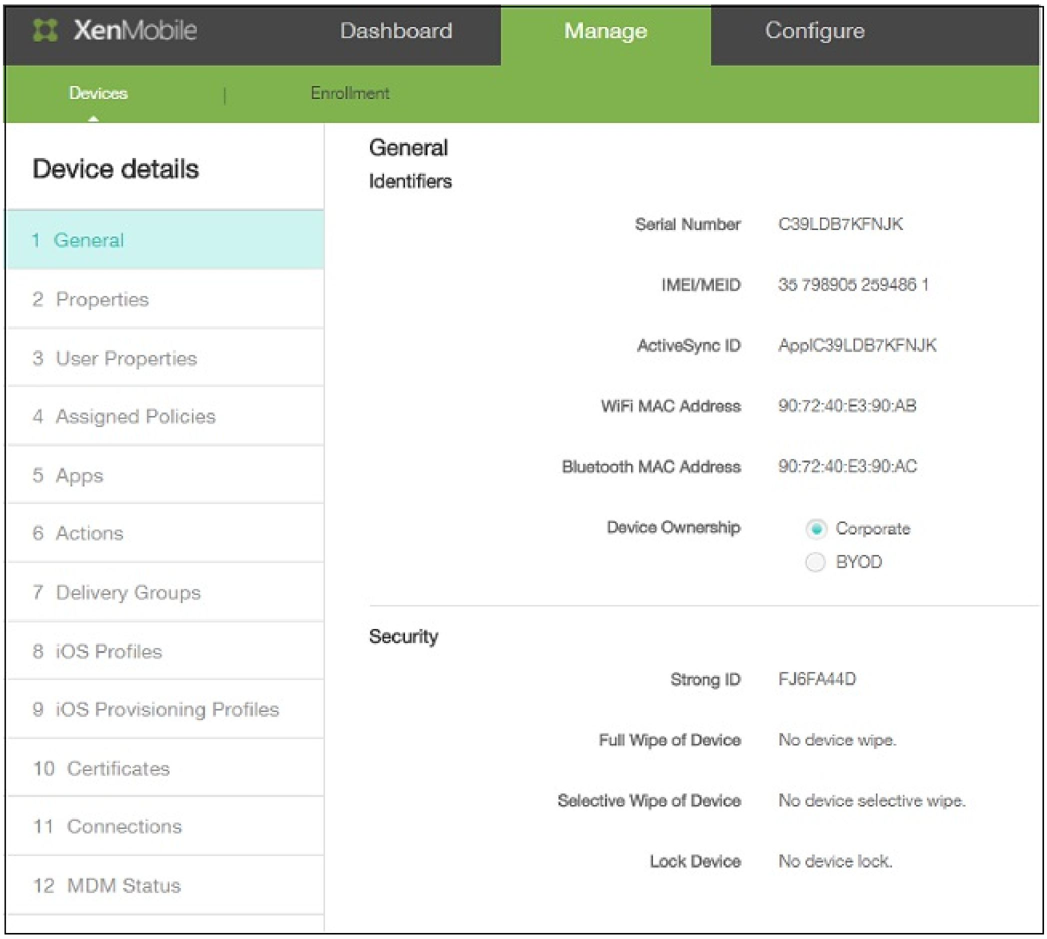
☐	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days
☑		MDM MAM		iOS				
		MDM MA		Android				

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.



☐	Status	Mode	User name	Device platform	Op
☑		MDM MAM		iOS	

6. 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.



General

Identifiers

Serial Number C39LDB7KFNJK

IMEI/MEID 35 798905 259486 1

ActiveSync ID ApplC39LDB7KFNJK

WiFi MAC Address 90:72:40:E3:90:AB

Bluetooth MAC Address 90:72:40:E3:90:AC

Device Ownership ● Corporate ○ BYOD

Security

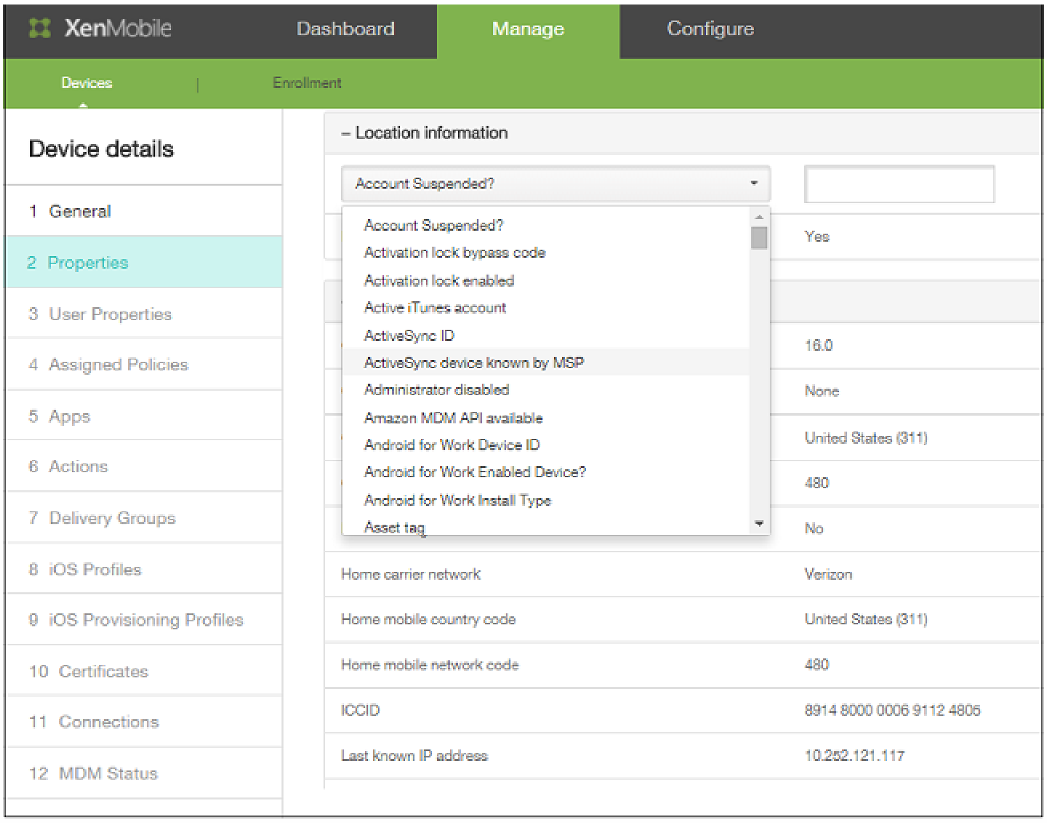
Strong ID FJ6FA44D

Full Wipe of Device No device wipe.

Selective Wipe of Device No device selective wipe.

Lock Device No device lock.

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.



Home carrier network Verizon

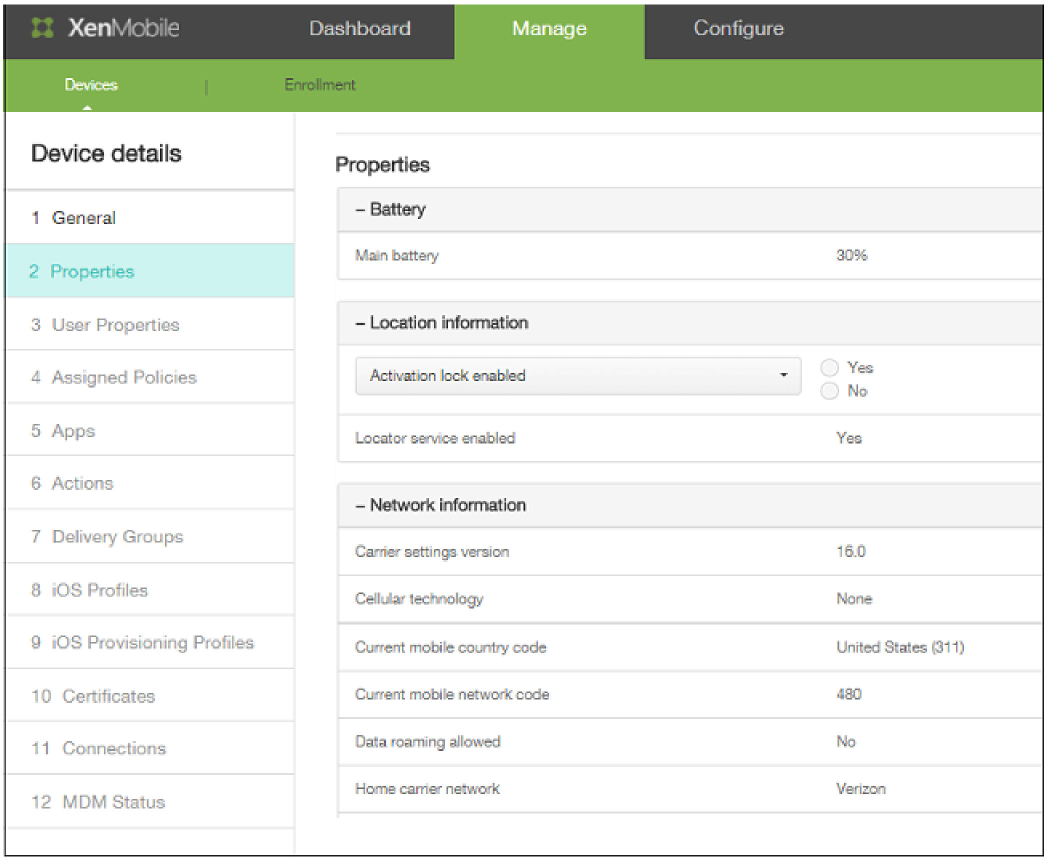
Home mobile country code United States (311)

Home mobile network code 480

ICCID 8914 8000 0006 9112 4806

Last known IP address 10.252.121.117

10. In the list, click the property to be provisioned and then set its value. For example, you can select the property Activation lock enabled and can set the value 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.



Properties

– Battery

Main battery	30%

– Location information

Activation lock enabled	○ Yes ○ No
Locator service enabled	Yes

– Network information

Carrier settings version	16.0
Cellular technology	None
Current mobile country code	United States (311)
Current mobile network code	480
Data roaming allowed	No
Home carrier network	Verizon

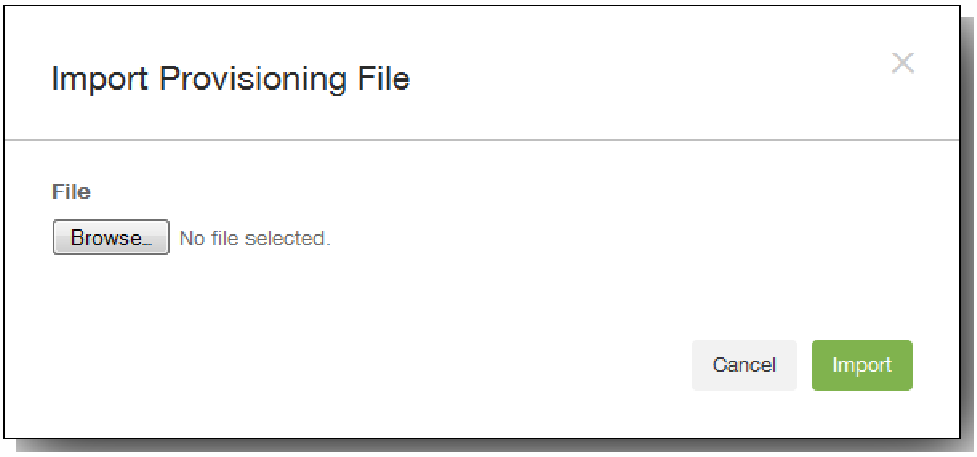
The **Assigned Policies** section and the sections that follow all contain summary information for the device.

- 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.

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.

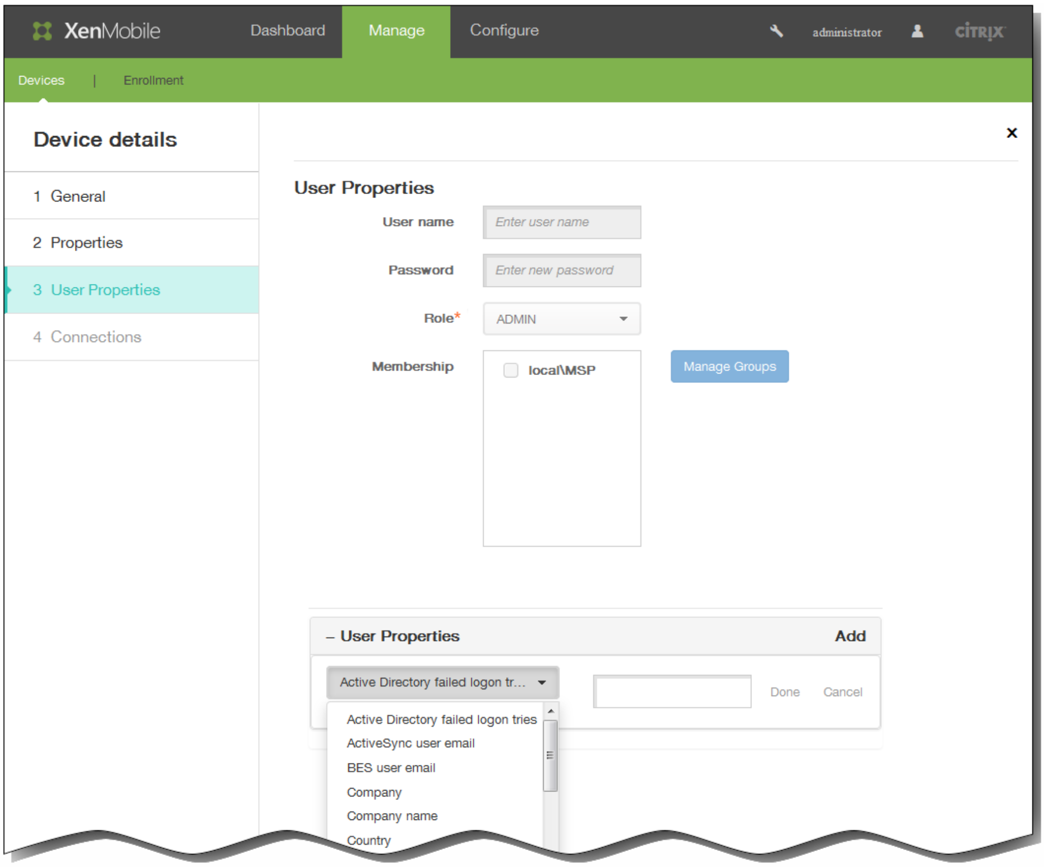


Import Provisioning File

File

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.

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.



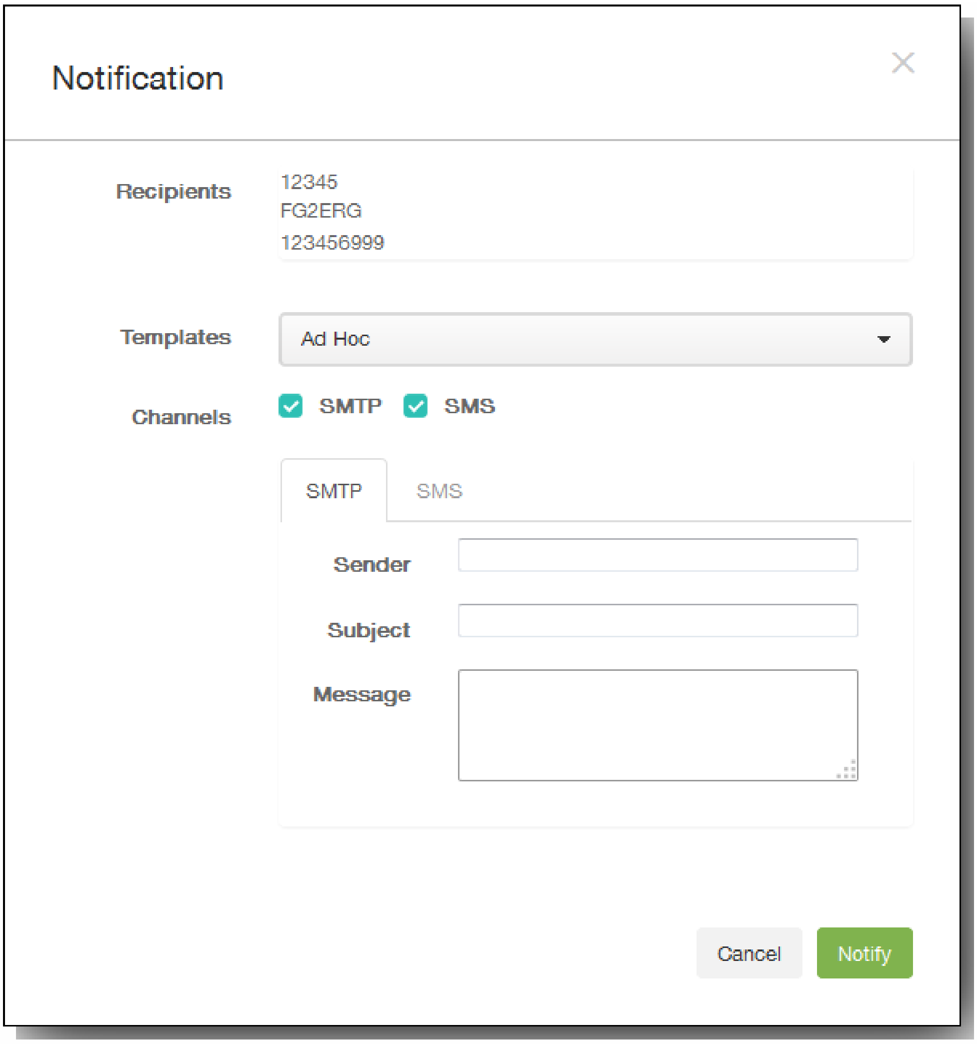
Note: The upper portion of the User Properties page cannot be edited.

- 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.

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.


Notification

Recipients: 12345
FG2ERG
123456999

Templates: Ad Hoc

Channels: ☑ SMTP ☑ SMS

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.

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.

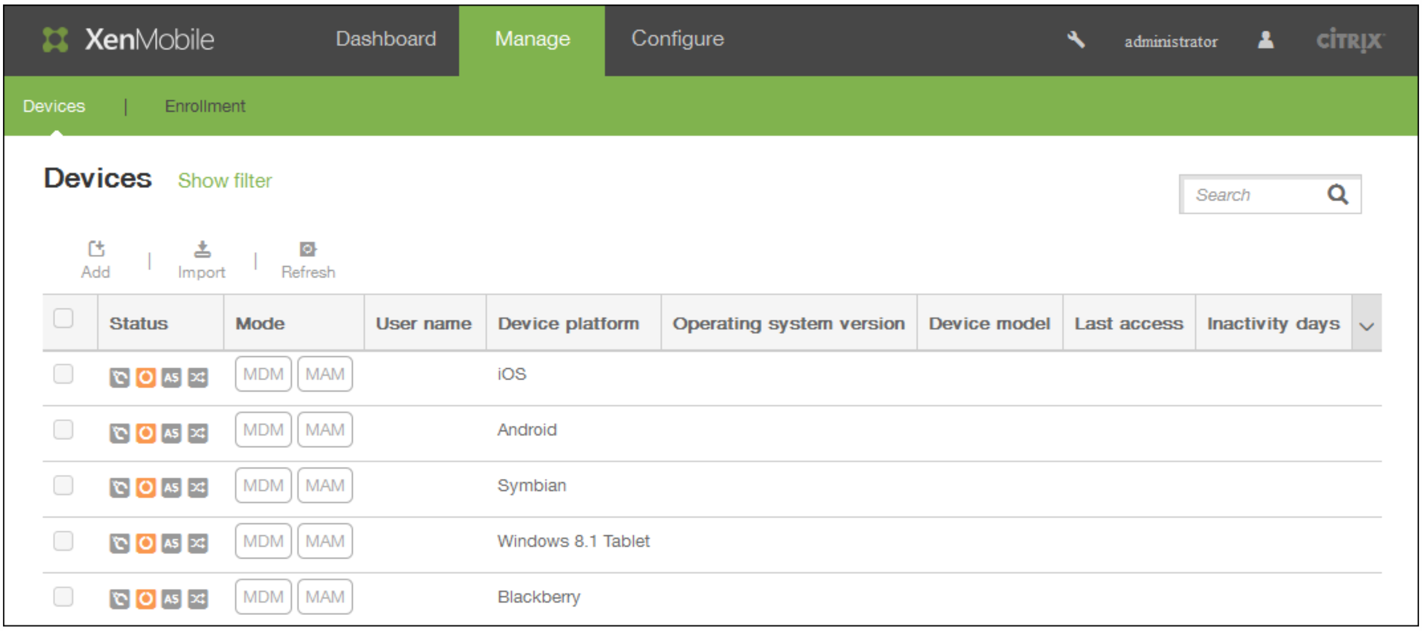
To lock an iOS device

Jul 24, 2015

You can lock an iOS device with an accompanying display of a message and phone number that appears on the device lock screen. This feature is supported on iOS 7 and 8 devices.

If you choose to include a message and phone number for the lock screen, the message and phone number only appears on a locked device if you have also set the Passcode policy in the XenMobile console, or if users have enabled the passcode manually on the device.

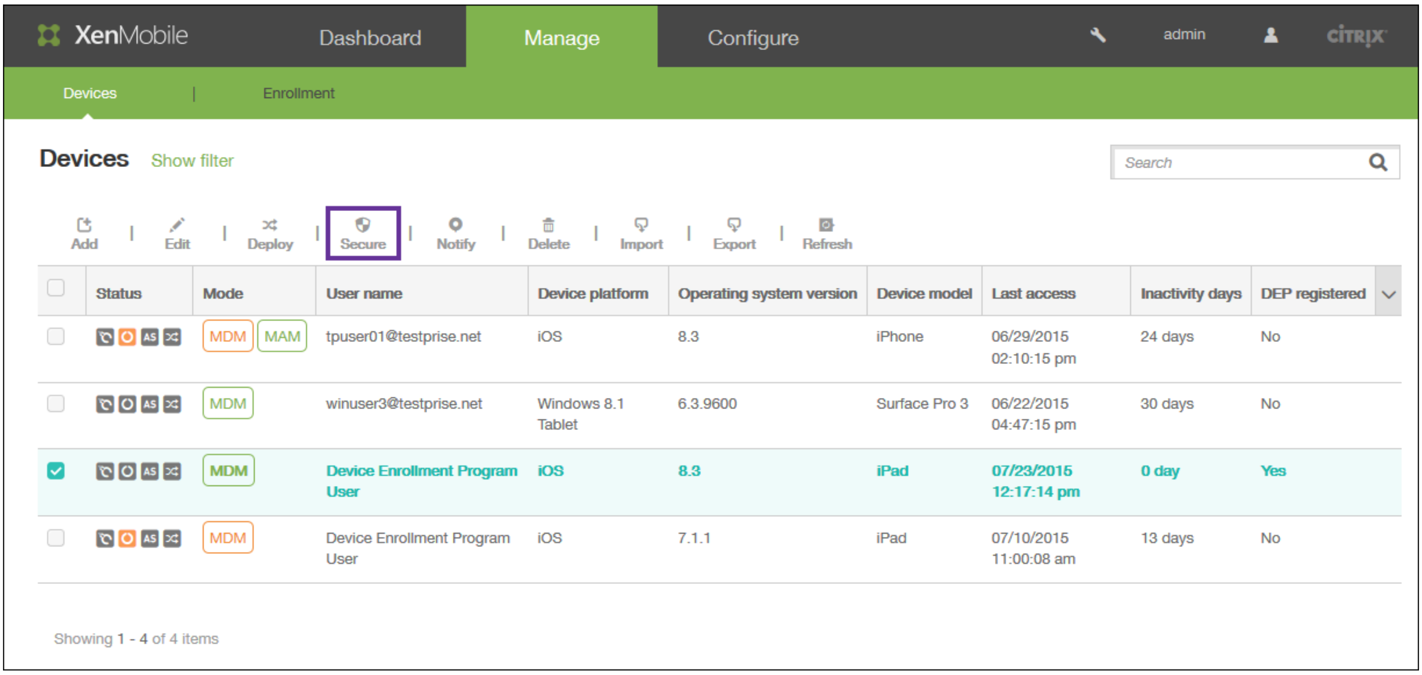
1. In the XenMobile console, click **Manage > Devices**. The **Devices** page appears.



☐	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days
☐	AS	MDM MAM		iOS				
☐	AS	MDM MAM		Android				
☐	AS	MDM MAM		Symbian				
☐	AS	MDM MAM		Windows 8.1 Tablet				
☐	AS	MDM MAM		Blackberry				

2. Select the iOS device you want to lock.

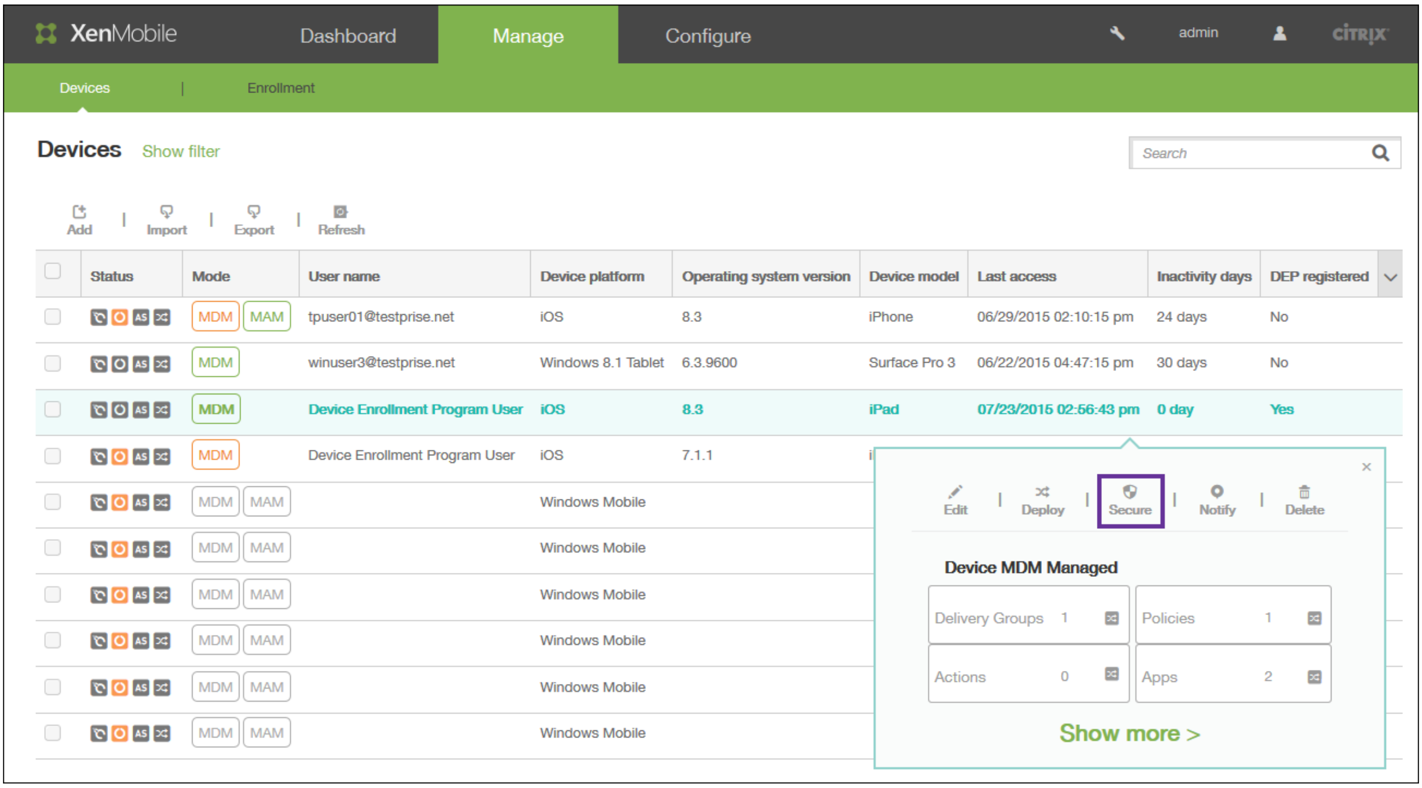
When you select the check box next to a device, the options menu appears above the device list; when you click anywhere else in the list, the options menu appears on the right side of the listing.



Devices

	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP registered
□		MDM MAM	tpuser01@testprise.net	iOS	8.3	iPhone	06/29/2015 02:10:15 pm	24 days	No
□		MDM	winuser3@testprise.net	Windows 8.1 Tablet	6.3.9600	Surface Pro 3	06/22/2015 04:47:15 pm	30 days	No
☑		MDM	Device Enrollment Program User	iOS	8.3	iPad	07/23/2015 12:17:14 pm	0 day	Yes
□		MDM	Device Enrollment Program User	iOS	7.1.1	iPad	07/10/2015 11:00:08 am	13 days	No

Showing 1 - 4 of 4 items



Devices

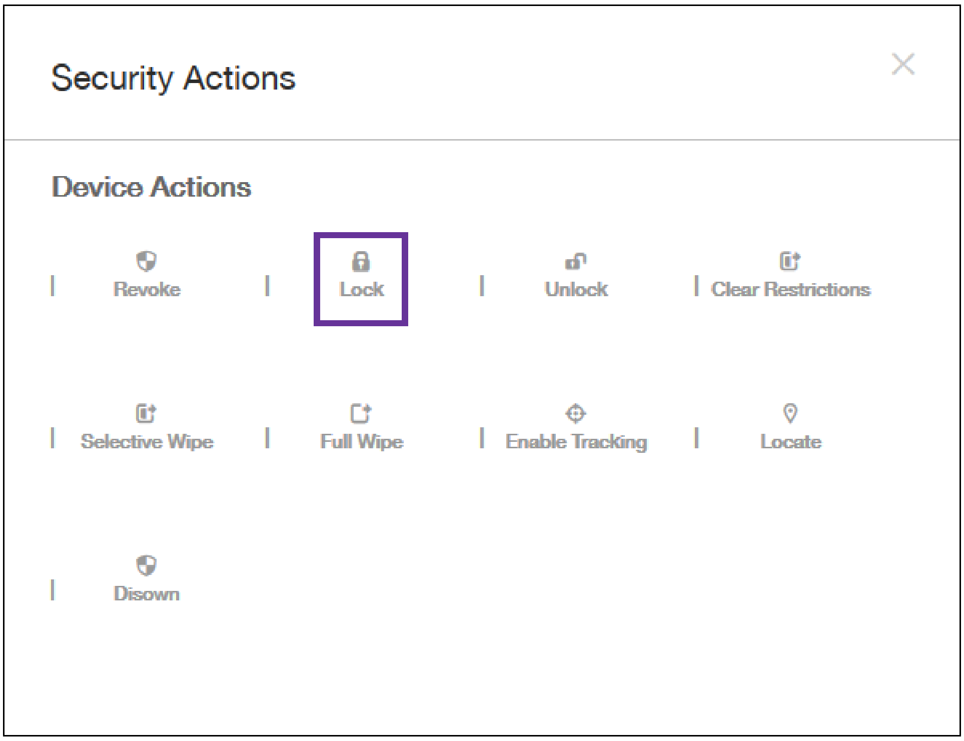
	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP registered
□		MDM MAM	tpuser01@testprise.net	iOS	8.3	iPhone	06/29/2015 02:10:15 pm	24 days	No
□		MDM	winuser3@testprise.net	Windows 8.1 Tablet	6.3.9600	Surface Pro 3	06/22/2015 04:47:15 pm	30 days	No
□		MDM	Device Enrollment Program User	iOS	8.3	iPad	07/23/2015 02:56:43 pm	0 day	Yes
□		MDM	Device Enrollment Program User	iOS	7.1.1	i			
□		MDM MAM		Windows Mobile					
□		MDM MAM		Windows Mobile					
□		MDM MAM		Windows Mobile					
□		MDM MAM		Windows Mobile					
□		MDM MAM		Windows Mobile					
□		MDM MAM		Windows Mobile					

Device MDM Managed

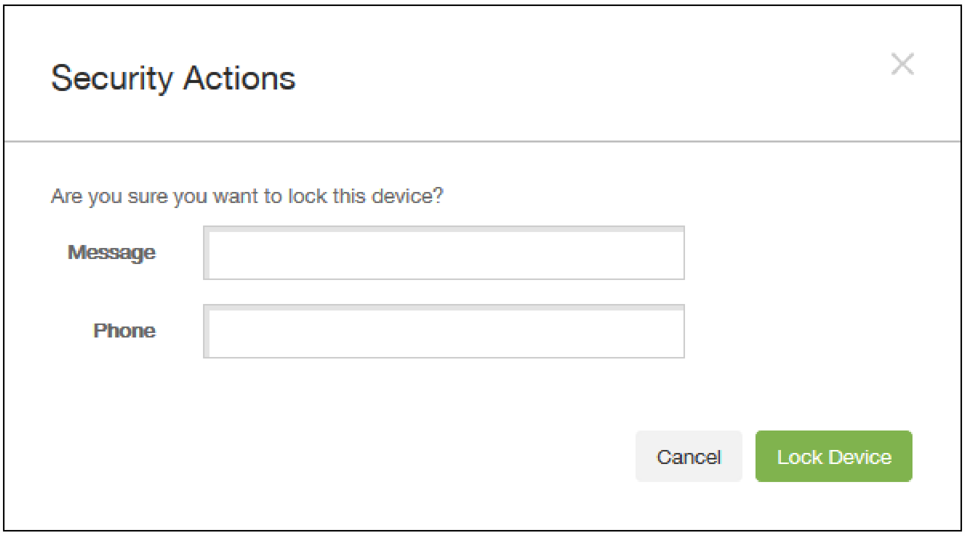
Delivery Groups 1	Policies 1
Actions 0	Apps 2

Show more >

3. In the options menu, select **Secure**. The **Security Actions** dialog box appears.



4. Select **Lock**. The **Security Actions** confirmation dialog box appears.



Are you sure you want to lock this device?

5. Optionally, enter a message and phone number that will appear on the device's lock screen.

6. Click **Lock Device**.

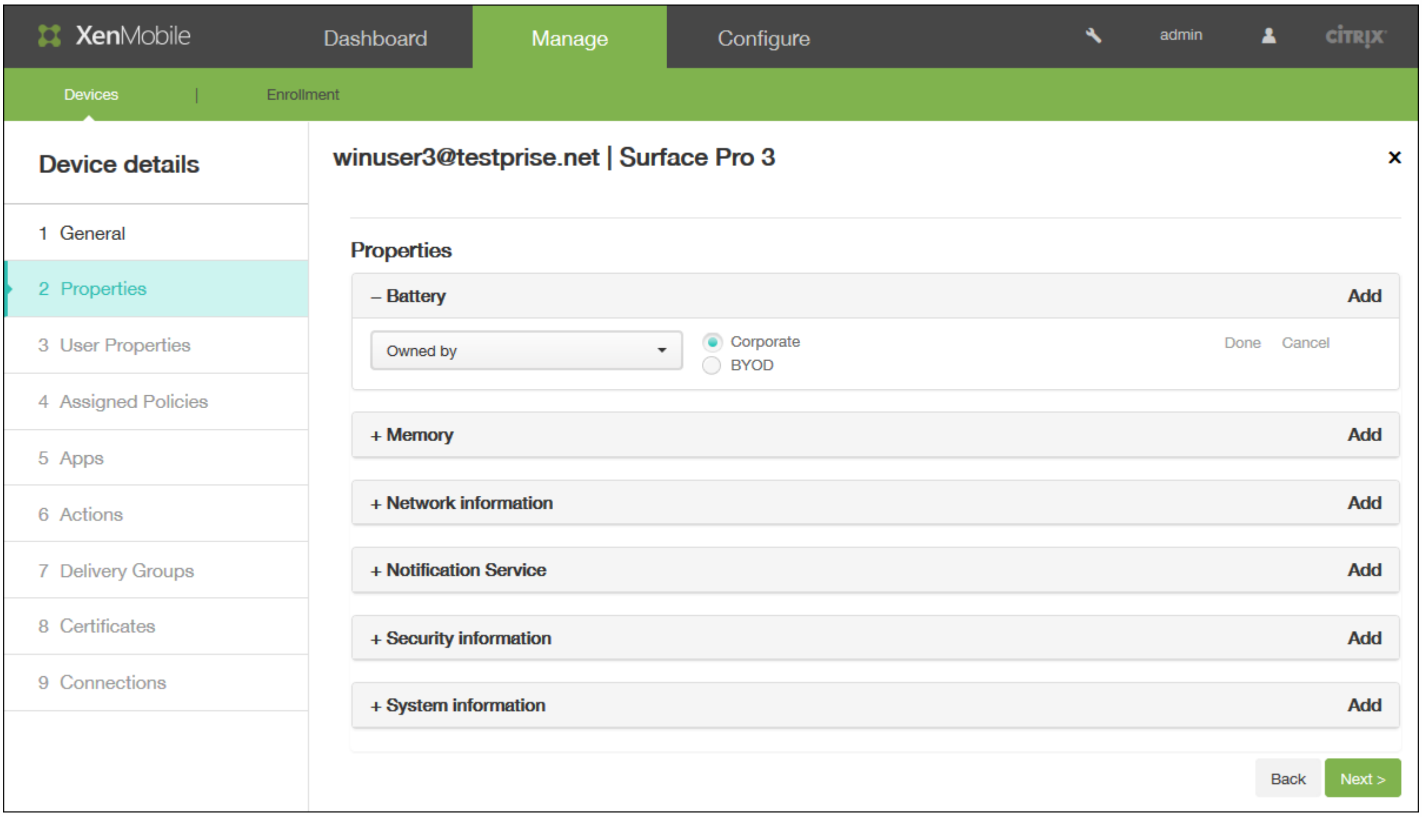
Tagging User Devices Manually

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).



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.

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.

The following user macros are always available:

- loginname (username plus domainname)
- username (loginname minus the domain, if any)
- domainname (domain name, or the default domain)

The following administrator-defined properties may be available:

- c
- cn
- company
- companyname
- department
- description
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename
- postalcode
- postofficebox

- telephonenumber
- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname (overrides property described previously)

Additionally, if the user is authenticated by using an authentication server, such as LDAP, all the properties associated with the user in that store are available.

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

Jul 13, 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.

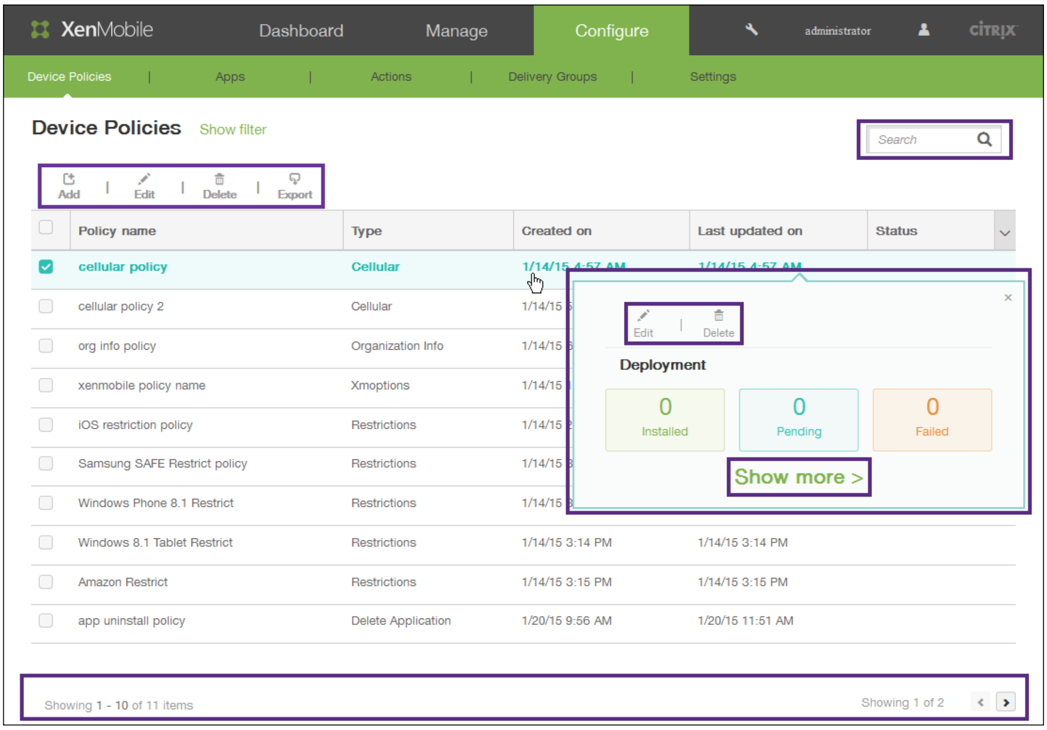
The basic steps to create a device policy are as follows:

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).

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.

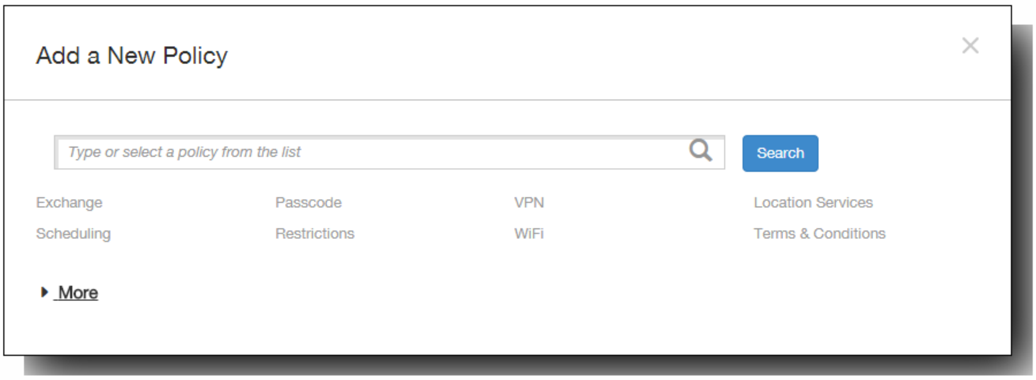


Device Policies

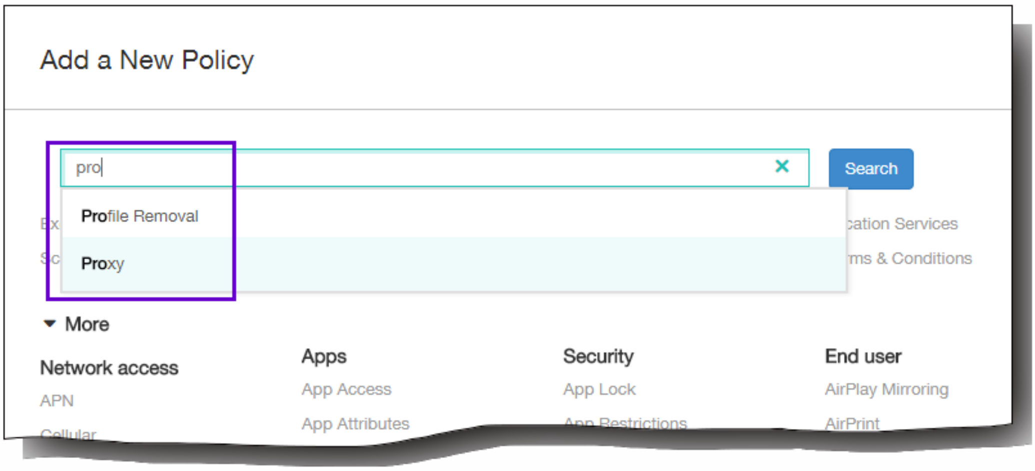
☐	Policy name	Type	Created on	Last updated on	Status
☑	cellular policy	Cellular	1/14/15 4:57 AM	1/14/15 4:57 AM	
☐	cellular policy 2	Cellular	1/14/15		
☐	org info policy	Organization Info	1/14/15		
☐	xenmobile policy name	Xmoptions	1/14/15		
☐	iOS restriction policy	Restrictions	1/14/15		
☐	Samsung SAFE Restrict policy	Restrictions	1/14/15		
☐	Windows Phone 8.1 Restrict	Restrictions	1/14/15		
☐	Windows 8.1 Tablet Restrict	Restrictions	1/14/15 3:14 PM	1/14/15 3:14 PM	
☐	Amazon Restrict	Restrictions	1/14/15 3:15 PM	1/14/15 3:15 PM	
☐	app uninstall policy	Delete Application	1/20/15 9:56 AM	1/20/15 11:51 AM	

Showing 1 - 10 of 11 items

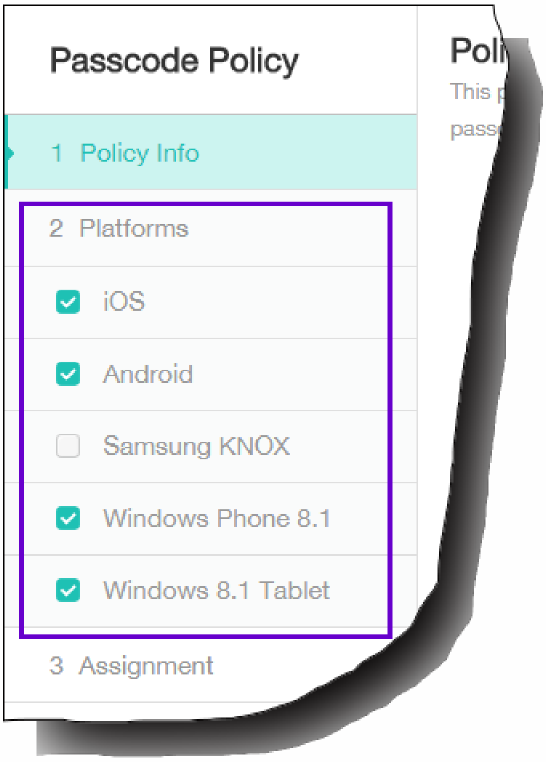
1. On the Device Policies page, click Add.
   The Add a New Policy dialog box appears. You can expand More to see additional policies.



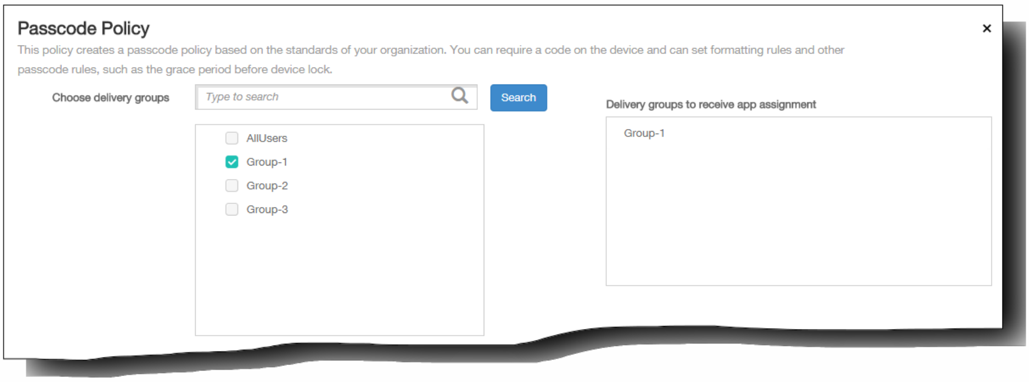
2. To find the policy you want to add, do one of the following:
   - Click the policy.
     The Policy Information page for the selected policy appears.
   - Type the name of the policy in the search field. As you type, potential matches appear. If your policy is in the list, click it. Only your selected 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.



Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Choose delivery groups: Type to search

- □ AllUsers
- ☑ Group-1
- □ Group-2
- □ Group-3

Delivery groups to receive app assignment: Group-1

7. Click Save.
   The policy is added to the Device Policies table.

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

Jun 24, 2015

You can configure device policies in XenMobile for Amazon, iOS, Android, Android for Work, 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	Android for Work	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 tablet
Common									
Exchange		X	X	X	X	X		X	
Scheduling			X	X			X		
Passcode		X	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		
Network access									
APN		X	X			X			
Cellular		X	X						
Personal		X							

Hotspot									
Proxy		X							
Remote Support						X			
Roaming		X							
Samsung Firewall					X				
Tunnel			X						
	Amazon	**iOS**	**Android**	**Android for Work**	**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							
Provisioning 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			X
App Uninstall Restrictions	X				X				
Files			X						
Browser				X	X	X			
Provisioning Profile		X							
Sideloading Key									X
Signing Certificate									X
Webclip		X	X						X
Worx Store		X	X						X
	Amazon	**iOS**	**Android**	**Android for Work**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1 tablet**
Security									
Android for Work App Restrictions				X					
App Lock		X	X						

App Restrictions						X			
Contacts (CardDAV)		X							
Credentials		X	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									

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							

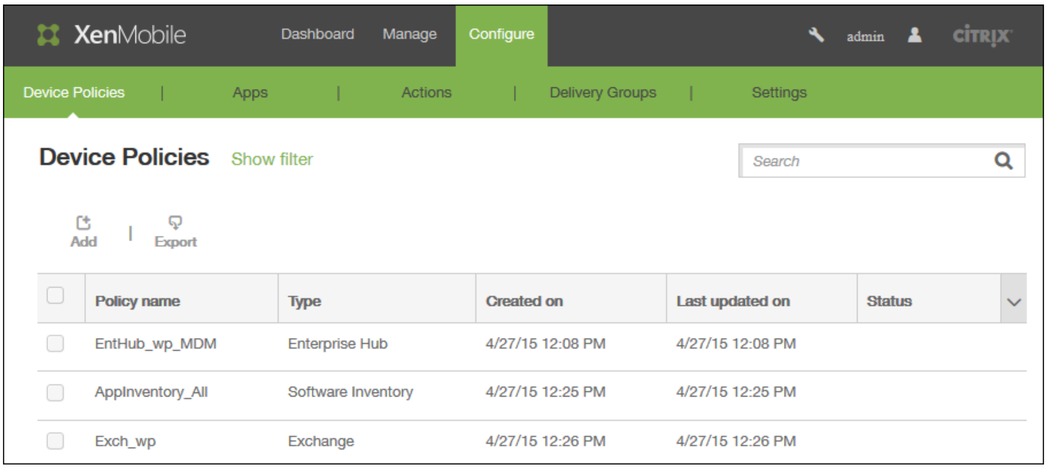
To add an app access device policy

Apr 24, 2015

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

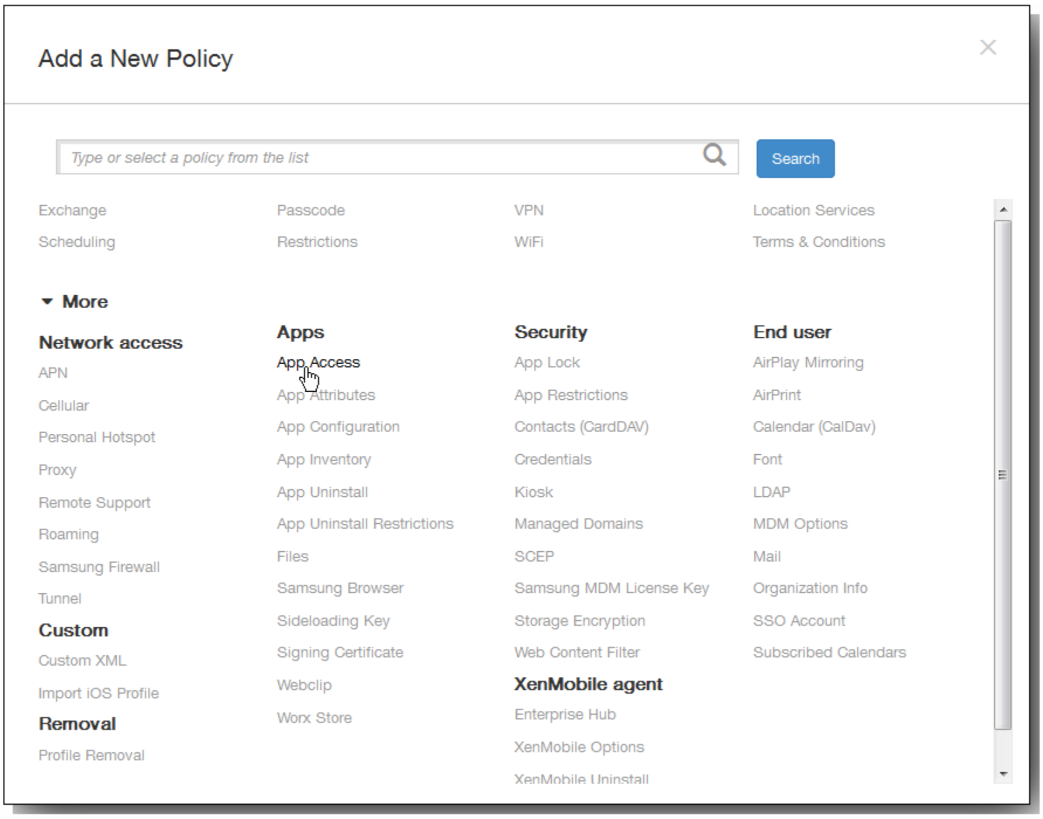
1. In the XenMobile console, click Configure > Device Policies.



Device Policies

Policy name	Type	Created on	Last updated on	Status
EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	

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



Add a New Policy

Type or select a policy from the list

Search

Exchange
Scheduling

Passcode
Restrictions

VPN
WiFi

Location Services
Terms & Conditions

▾ More

Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel

Custom
Custom XML
Import iOS Profile

Removal
Profile Removal

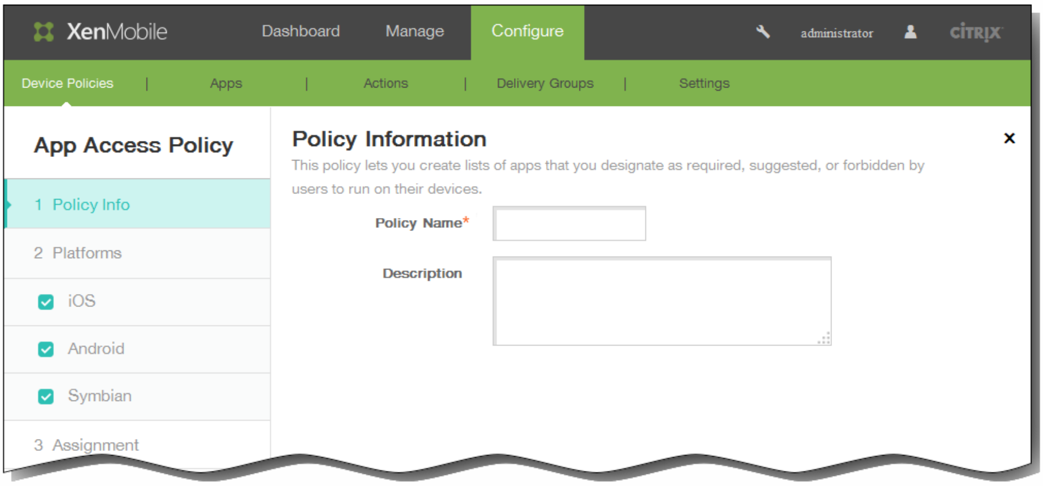
Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store

Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter

XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall

End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars

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



XenMobile | Dashboard | Manage | Configure | administrator | CITRIX

Device Policies | Apps | Actions | Delivery Groups | Settings

App Access Policy

1 Policy Info
2 Platforms
☑ iOS
☑ Android
☑ Symbian
3 Assignment

Policy Information

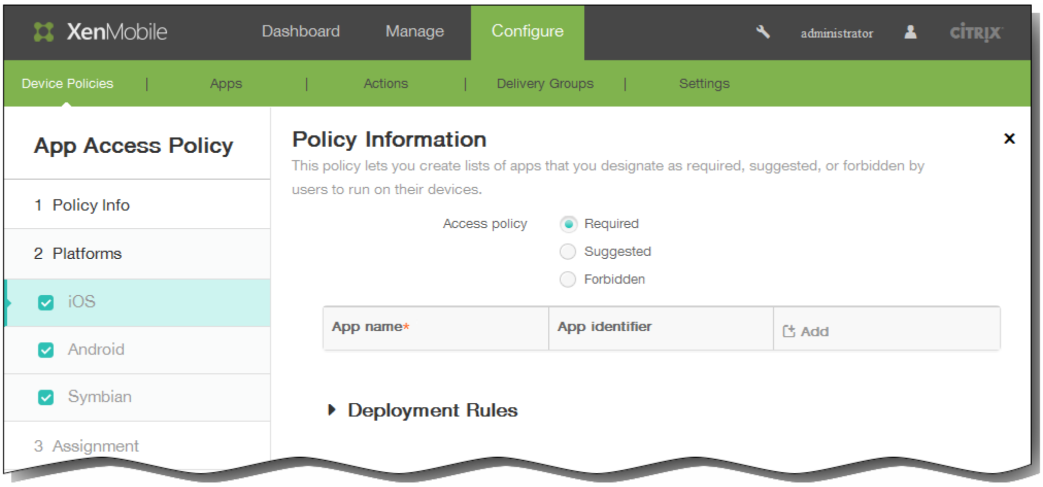
This policy lets you create lists of apps that you designate as required, suggested, or forbidden by users to run on their devices.

Policy Name*

Description

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.



Policy Information

This policy lets you create lists of apps that you designate as required, suggested, or forbidden by users to run on their devices.

Access policy ● Required ○ Suggested ○ Forbidden

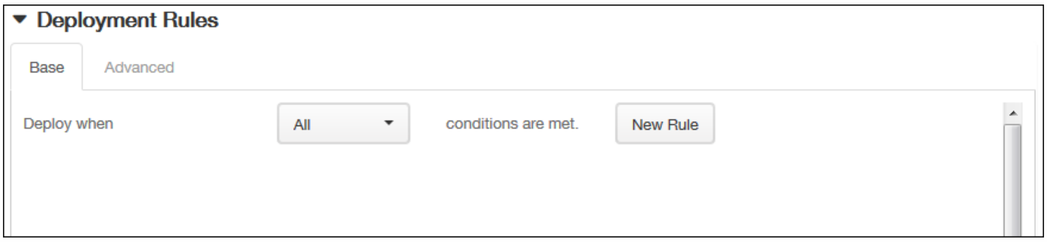
App name*	App identifier	Add

Deployment Rules

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. for each app you want to add.

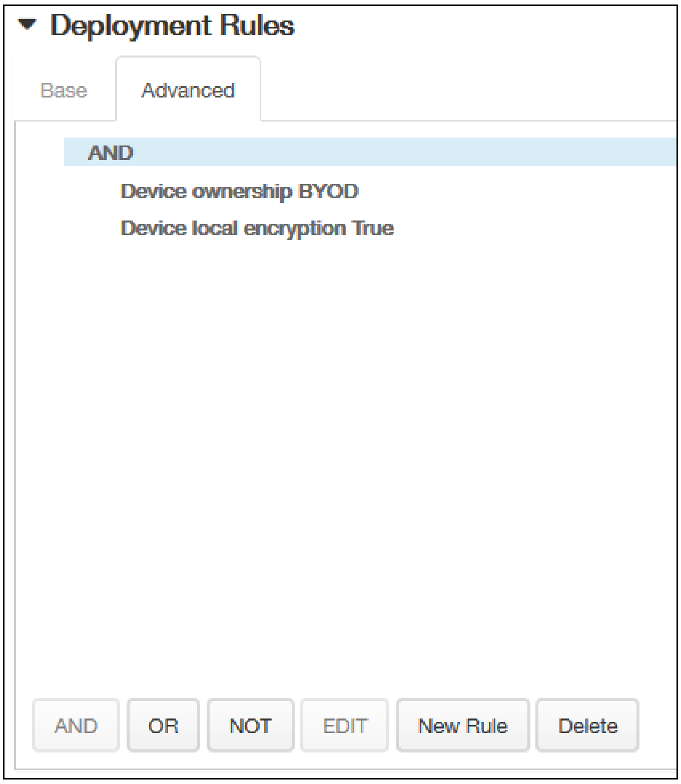
      Note: To delete an existing app, hover over the line containing the listing and then click the trash can icon on the right-hand side. A confirmation dialog box appears. Click Delete to delete the listing or Cancel to keep the listing. To edit an existing app, hover over the line containing the listing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



Deploy when All conditions are met.

   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.



AND

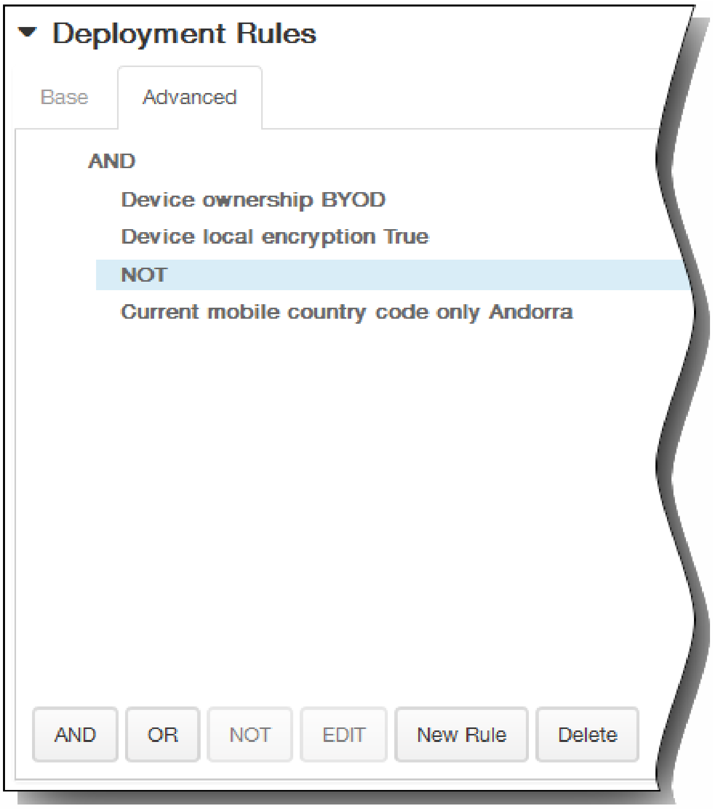
Device ownership BYOD

Device local encryption True

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.

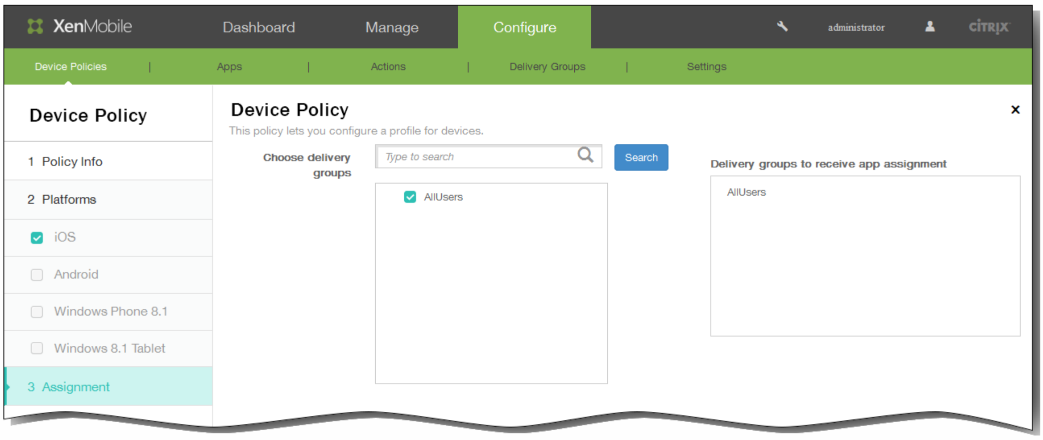
   3. Click New Rule again if you want to add more conditions.
      In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



Deployment Rules

AND
Device ownership BYOD
Device local encryption True
NOT
Current mobile country code only Andorra

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



Device Policy

This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

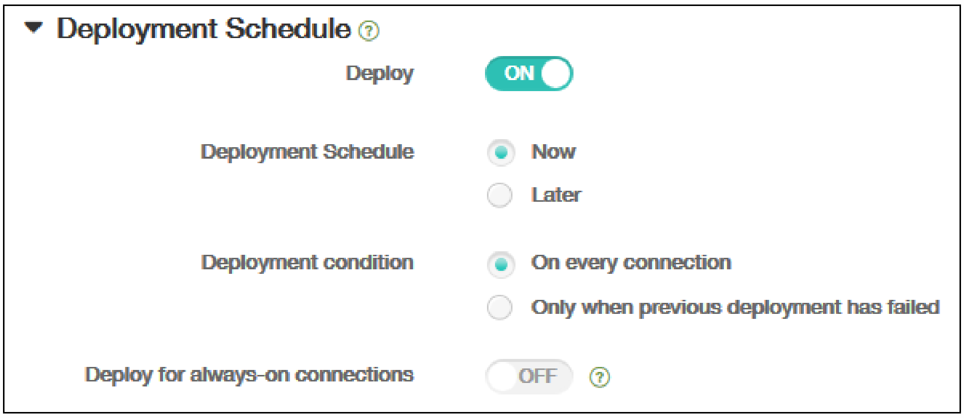
☑ AllUsers

Delivery groups to receive app assignment: AllUsers

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.



▾ 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

11. Click Save to save the policy.

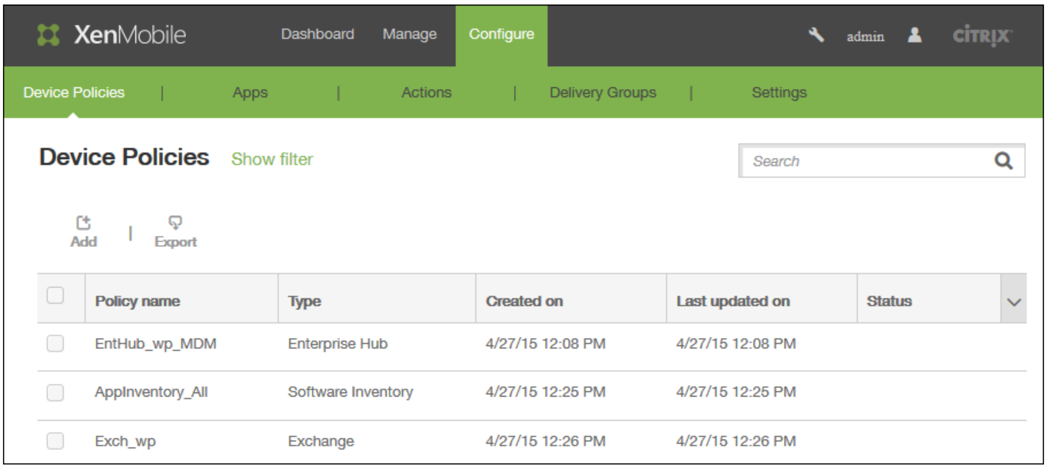
To add an app inventory device policy

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.

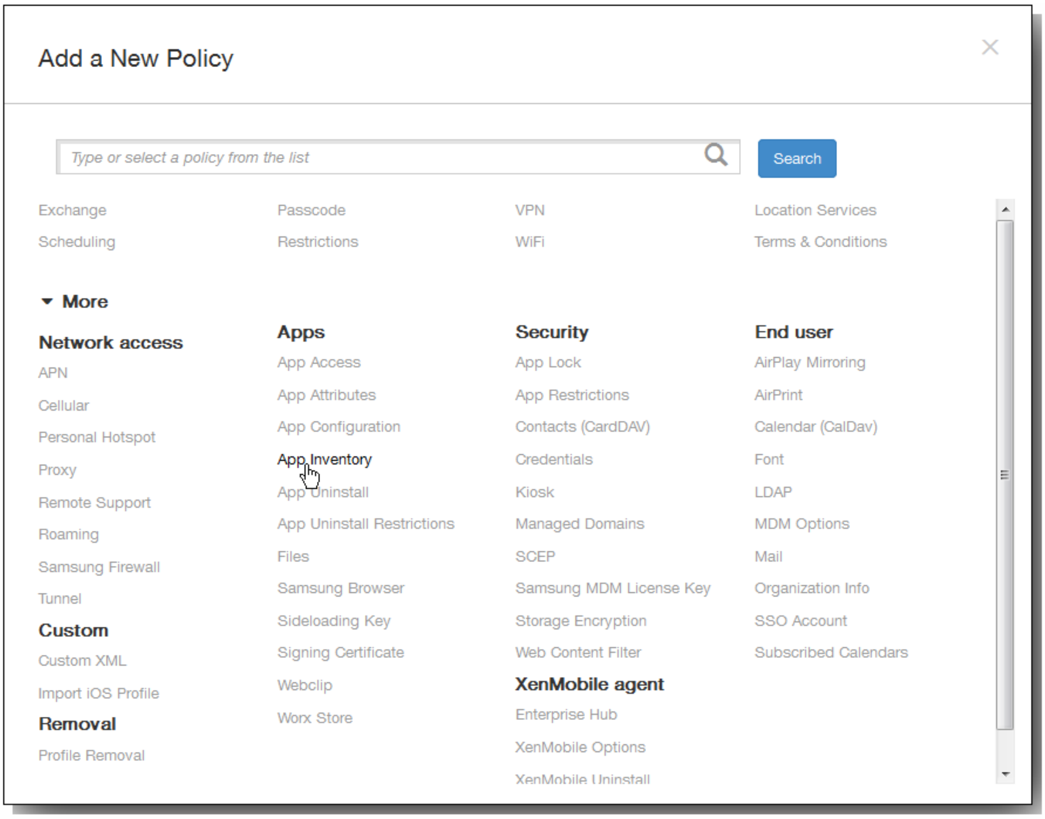
Important: For updated apps to appear in the Updates Available list in the Worx Store on users' Android devices, you must first deploy this policy to the users' devices.

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

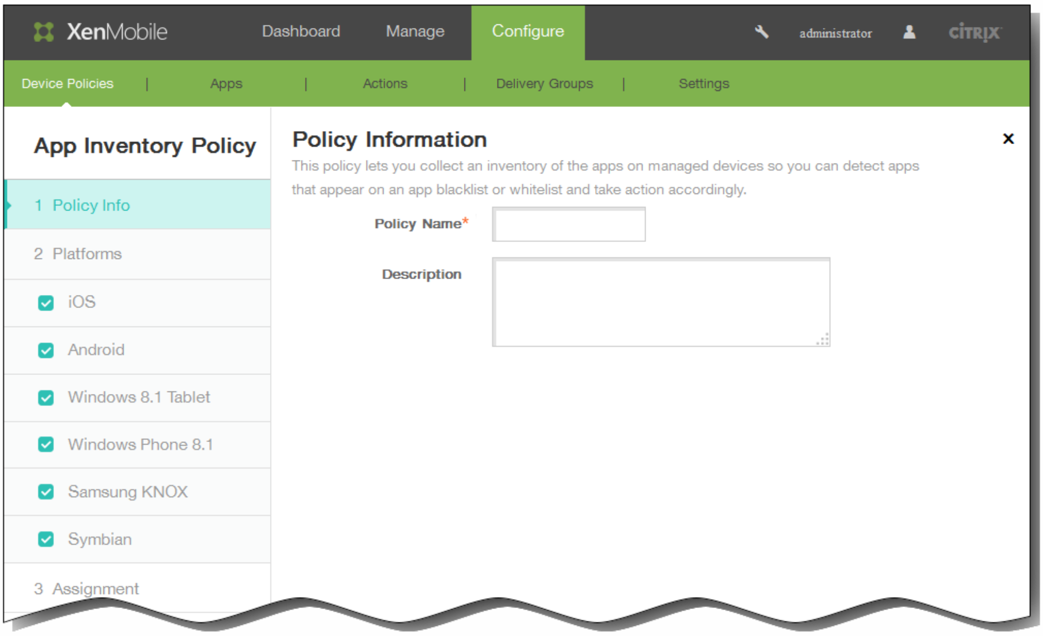


Policy name	Type	Created on	Last updated on	Status
EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	

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



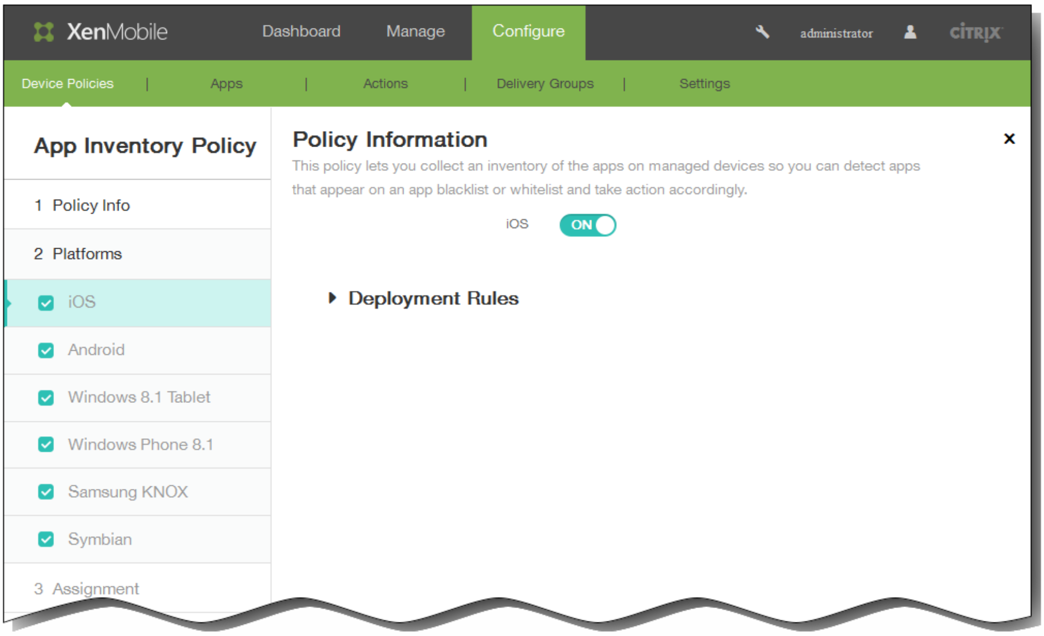
3. Click More > App Inventory. The App Inventory Policy page appears.



This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.

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.

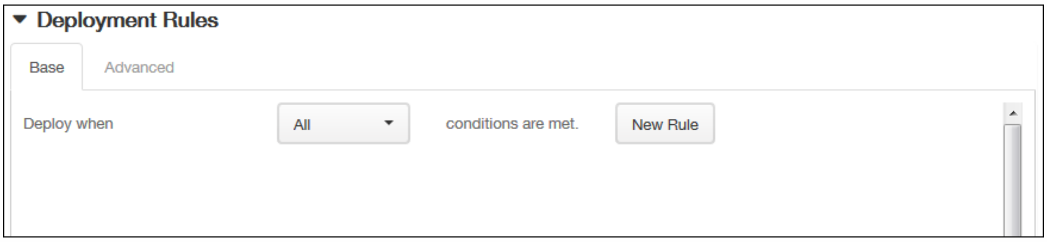


This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.

iOS ON

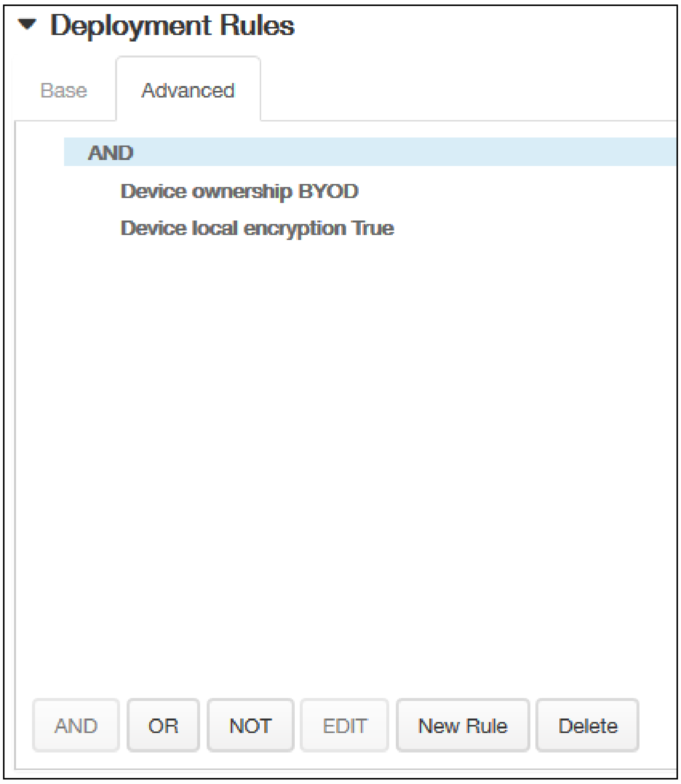
Select the platform or platforms you want to add, and then for each platform do the following:

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.



Deploy when All conditions are met.

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.



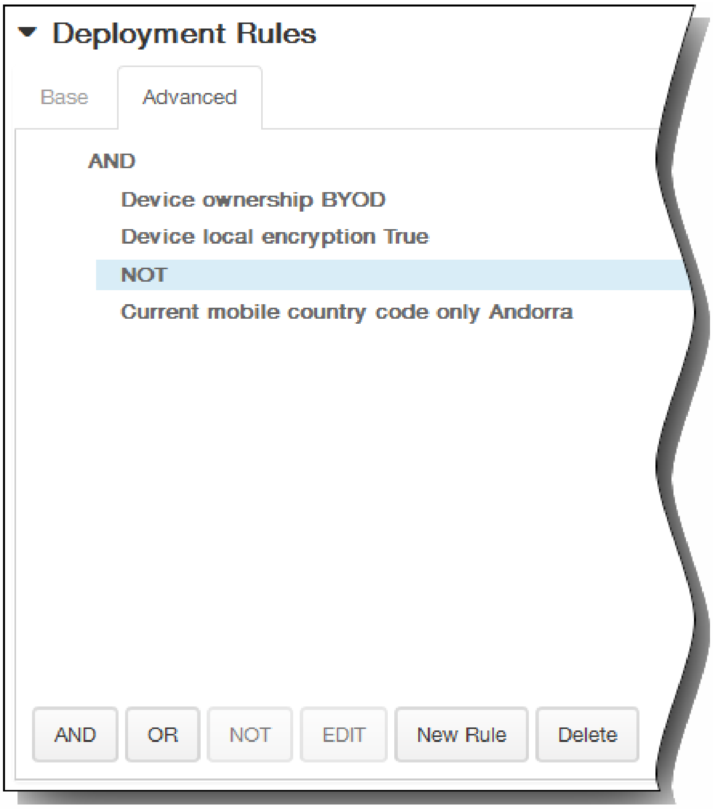
AND

Device ownership BYOD

Device local encryption True

The conditions you chose on the Base tab appear.

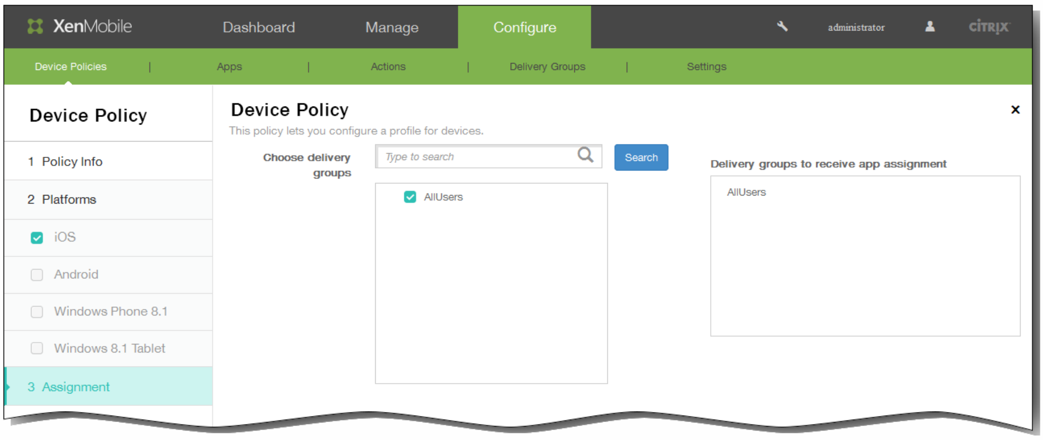
3. You can use more advanced Boolean logic to combine, edit, or add rules.
   1. Click AND, OR, or NOT.
   2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
      At any time, you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



Deployment Rules

AND
Device ownership BYOD
Device local encryption True
NOT
Current mobile country code 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.



☑ iOS
□ Android
□ Windows Phone 8.1
□ Windows 8.1 Tablet

Device Policy

This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

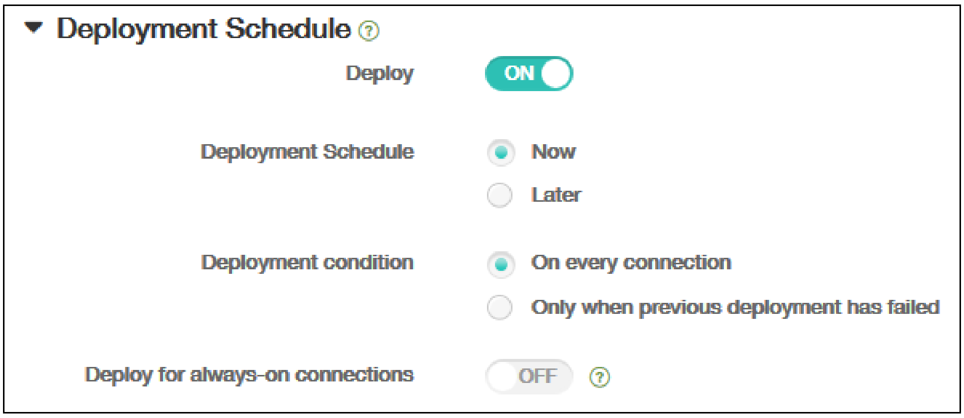
☑ AllUsers

Delivery groups to receive app assignment: AllUsers

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.



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

11. Click Save to save the policy.

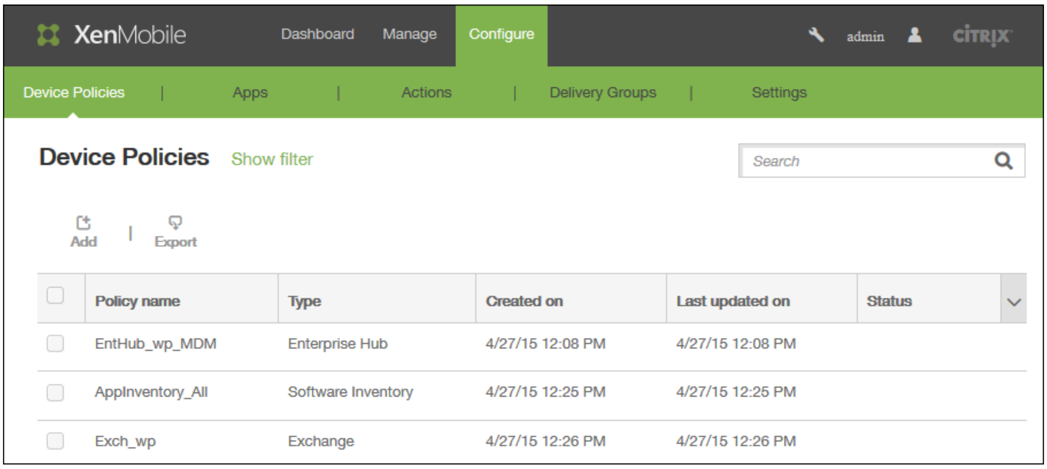
To add an app tunneling device policy for Android

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.

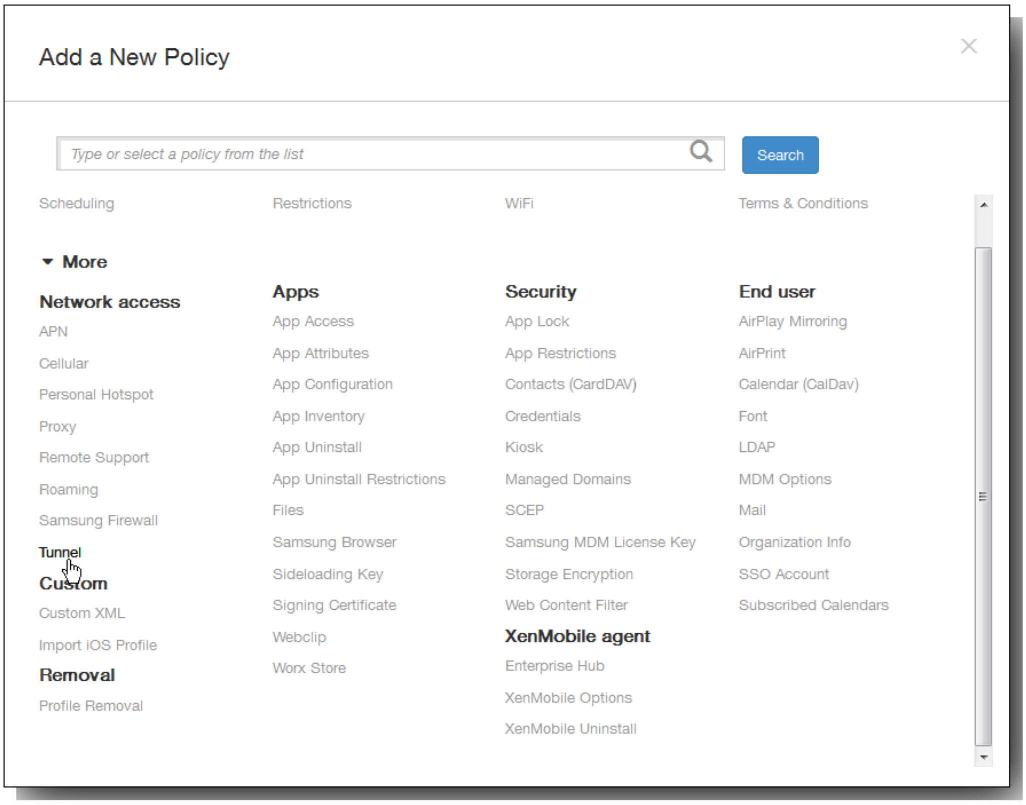
Note: Any app traffic sent through a tunnel that you define in this policy goes through XenMobile before being redirected to the server running the app.

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



☐	Policy name	Type	Created on	Last updated on	Status
☐	EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
☐	AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
☐	Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	

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



Add a New Policy

Type or select a policy from the list

Search

Scheduling

Restrictions

WiFi

Terms & Conditions

More

Network access

APN

Cellular

Personal Hotspot

Proxy

Remote Support

Roaming

Samsung Firewall

Tunnel

Custom

Custom XML

Import iOS Profile

Removal

Profile Removal

Apps

App Access

App Attributes

App Configuration

App Inventory

App Uninstall

App Uninstall Restrictions

Files

Samsung Browser

Sideloading Key

Signing Certificate

Webclip

Worx Store

Security

App Lock

App Restrictions

Contacts (CardDAV)

Credentials

Kiosk

Managed Domains

SCEP

Samsung MDM License Key

Storage Encryption

Web Content Filter

XenMobile agent

Enterprise Hub

XenMobile Options

XenMobile Uninstall

End user

AirPlay Mirroring

AirPrint

Calendar (CalDav)

Font

LDAP

MDM Options

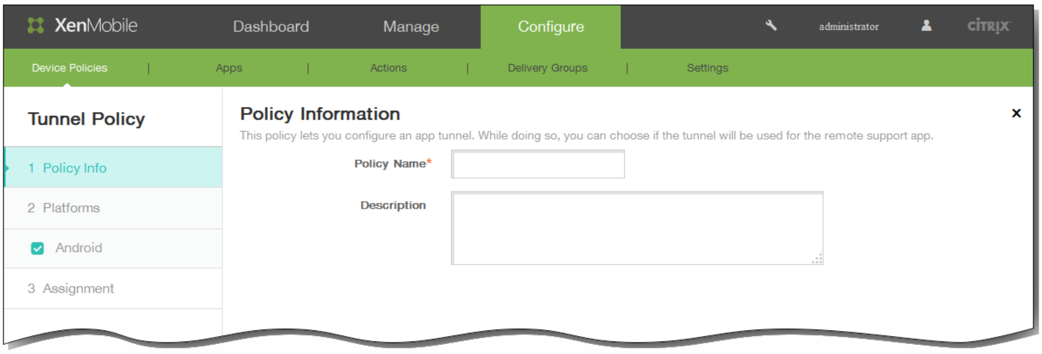
Mail

Organization Info

SSO Account

Subscribed Calendars

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



Tunnel Policy

1 Policy Info

2 Platforms

☑ Android

3 Assignment

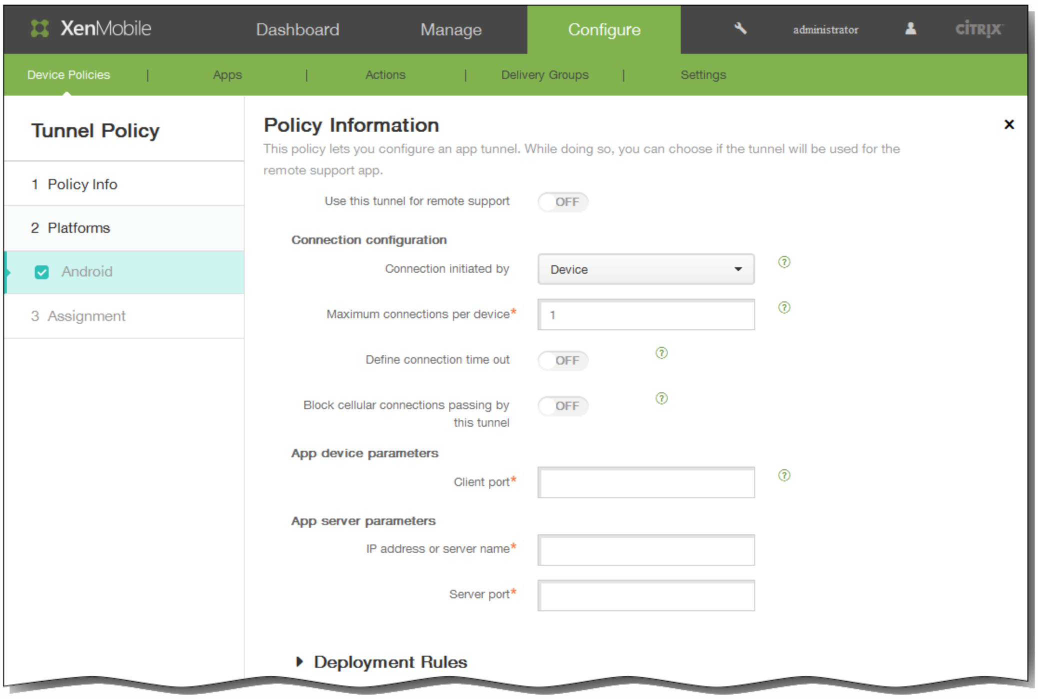
Policy Information

This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.

Policy Name*

Description

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.



Policy Information

This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.

Use this tunnel for remote support: OFF

Connection configuration

Connection initiated by: Device

Maximum connections per device*: 1

Define connection time out: OFF

Block cellular connections passing by this tunnel: OFF

App device parameters

Client port*:

App server parameters

IP address or server name*:

Server port*:

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:

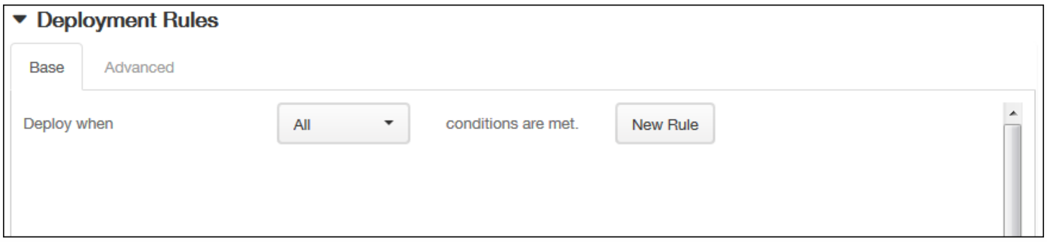
   1. Connection initiated by: Click Device or Server to specify the source initiating the connection.
   2. Maximum connections per device: Type a number to specify how many concurrent TCP connections the app can establish. This field applies only to device-initiated connections.
   3. Define connection 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.

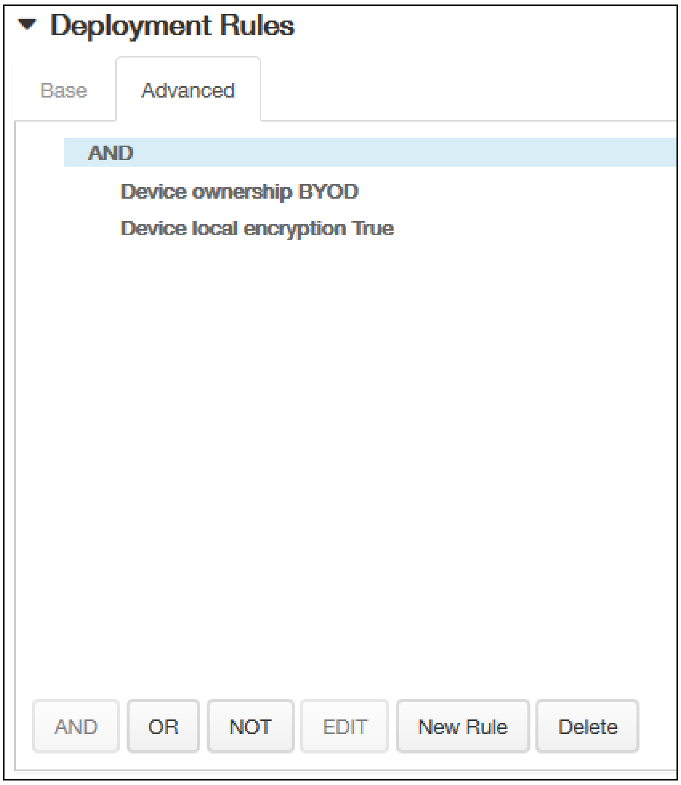
   If you **do** select remote support, do the following:

   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.



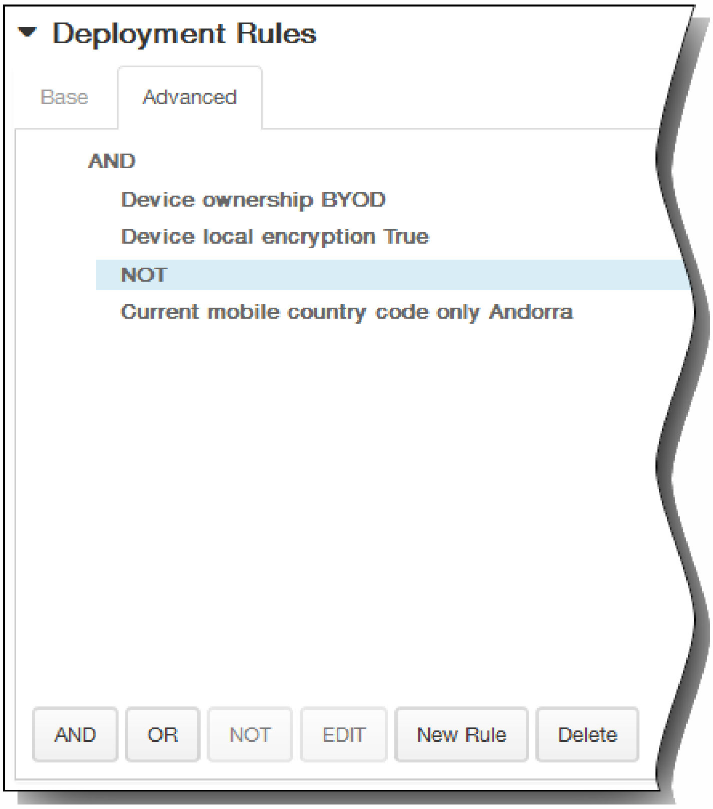
1. In the lists, click options to determine when the policy should be deployed.
   1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
   2. Click New Rule to define the conditions.
   3. In the lists, click the conditions, such 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

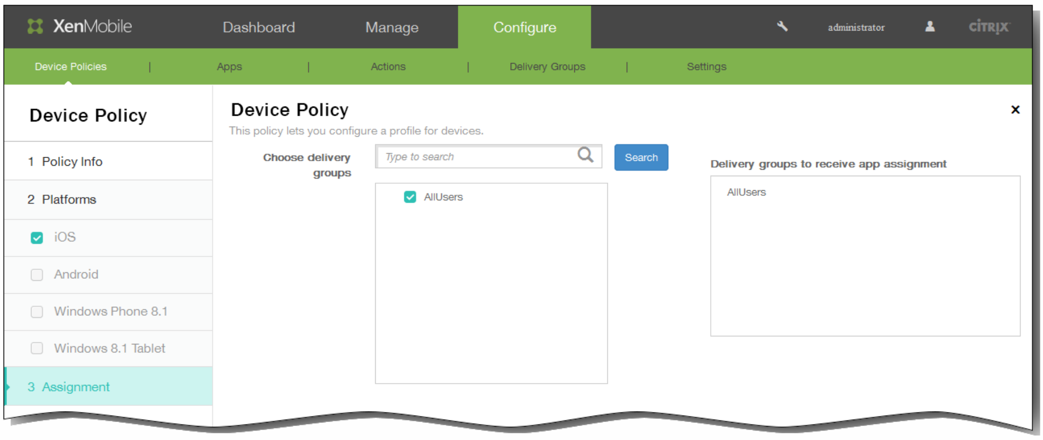
mobile country code cannot be only Andorra.



Deployment Rules

AND
Device ownership BYOD
Device local encryption True
NOT
Current mobile country code 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.



Device Policy

This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

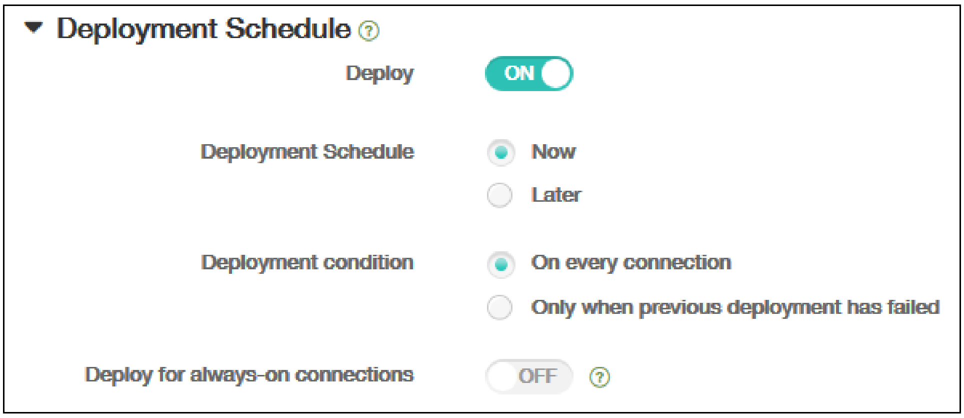
Delivery groups to receive app assignment: AllUsers

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.



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

11. Click Save to save the policy.

Custom XML device policies

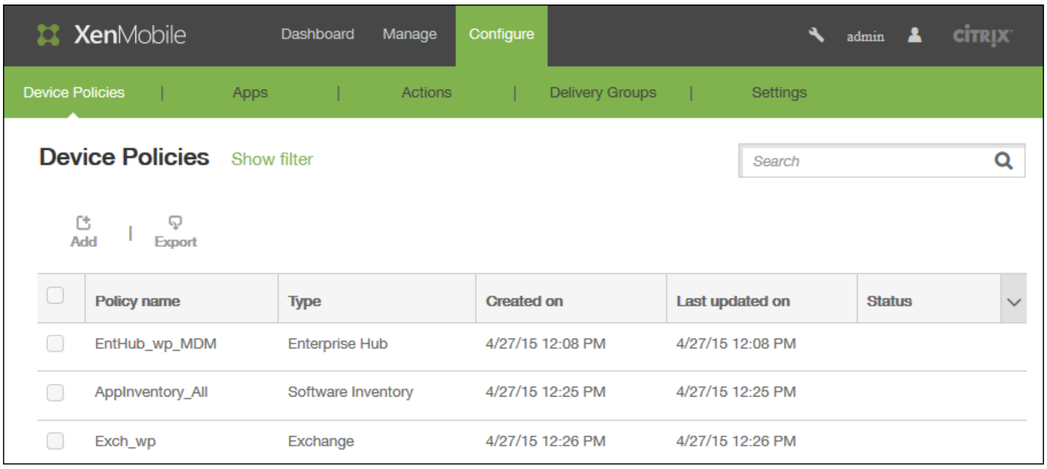
Mar 17, 2015

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

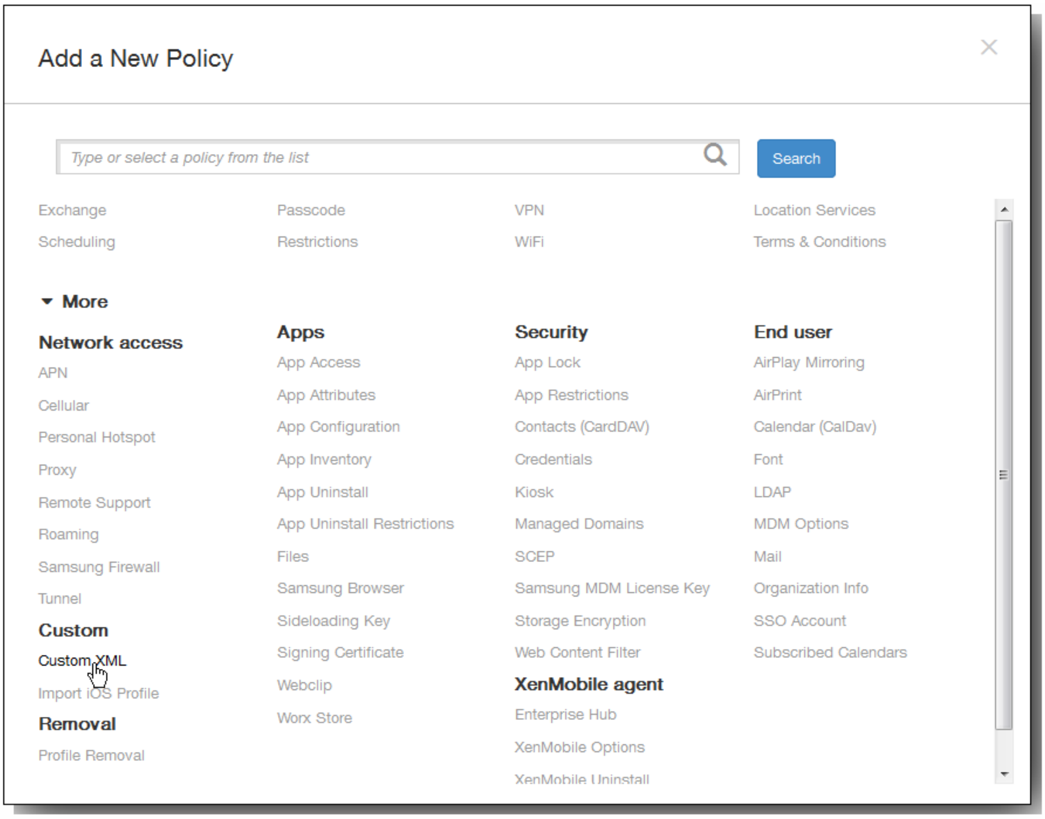
You create your custom XML configuration by using the Open Mobile Alliance Device Management (OMA DM) API in Windows 8.1. Creating custom XML with the OMA DM API is beyond the scope of this topic. For more information about using the OMA DM API, see OMA Device Management on the Microsoft Developer Network site.

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



☐	Policy name	Type	Created on	Last updated on	Status
☐	EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
☐	AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
☐	Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	

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



Add a New Policy

Type or select a policy from the list

Search

Exchange
Scheduling

Passcode
Restrictions

VPN
WiFi

Location Services
Terms & Conditions

More

Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel

Custom
Custom XML
Import iOS Profile

Removal
Profile Removal

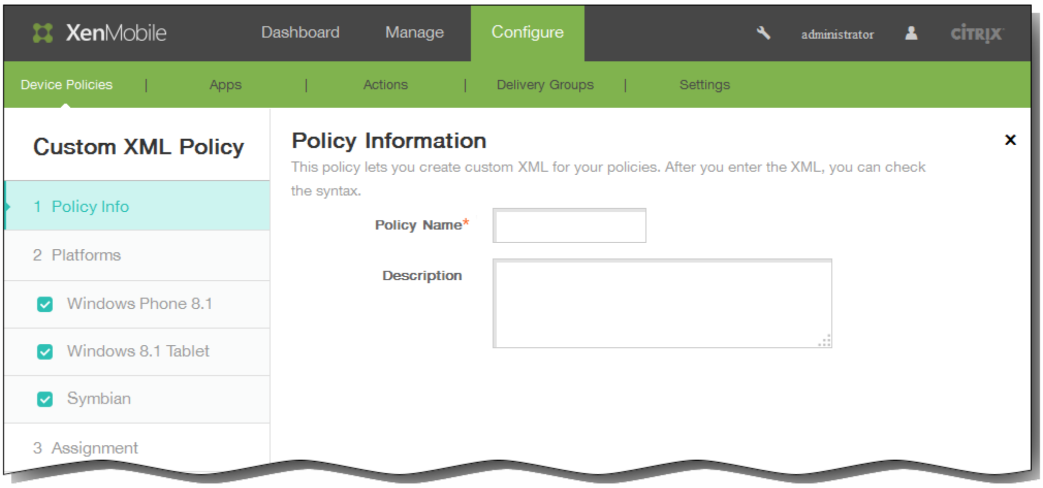
Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store

Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter

XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall

End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars

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



XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings

Custom XML Policy

1 Policy Info
2 Platforms
☑ Windows Phone 8.1
☑ Windows 8.1 Tablet
☑ Symbian
3 Assignment

Policy Information

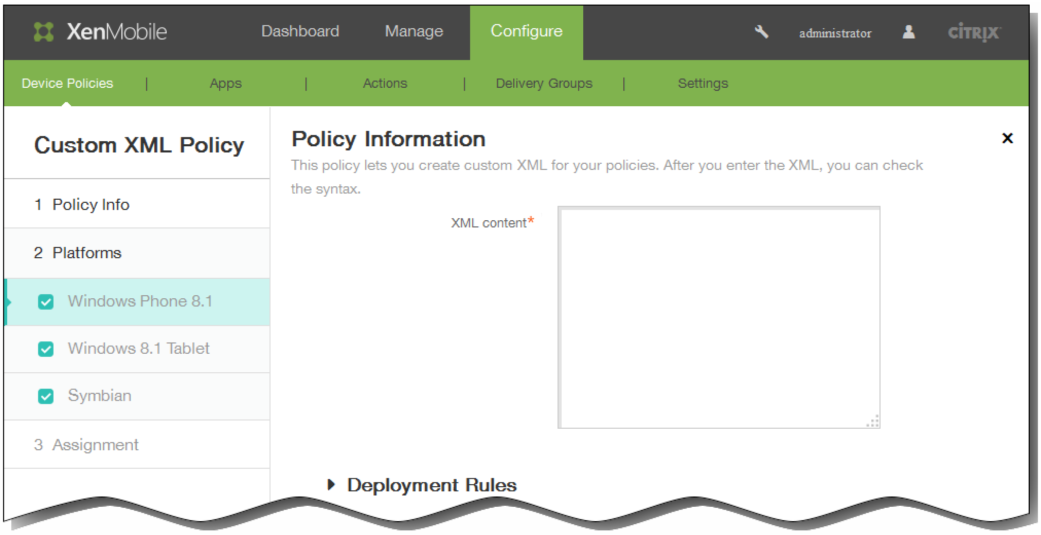
This policy lets you create custom XML for your policies. After you enter the XML, you can check the syntax.

Policy Name*

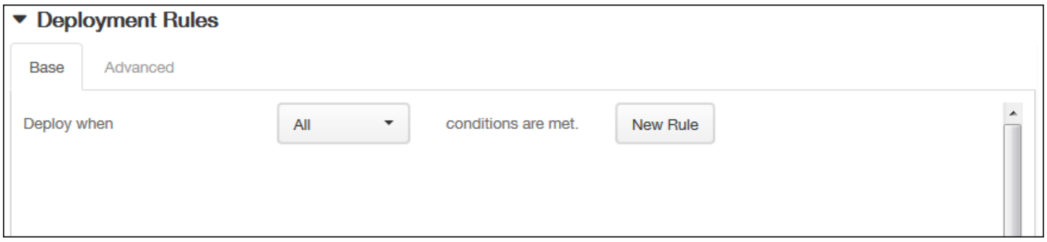
Description

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.

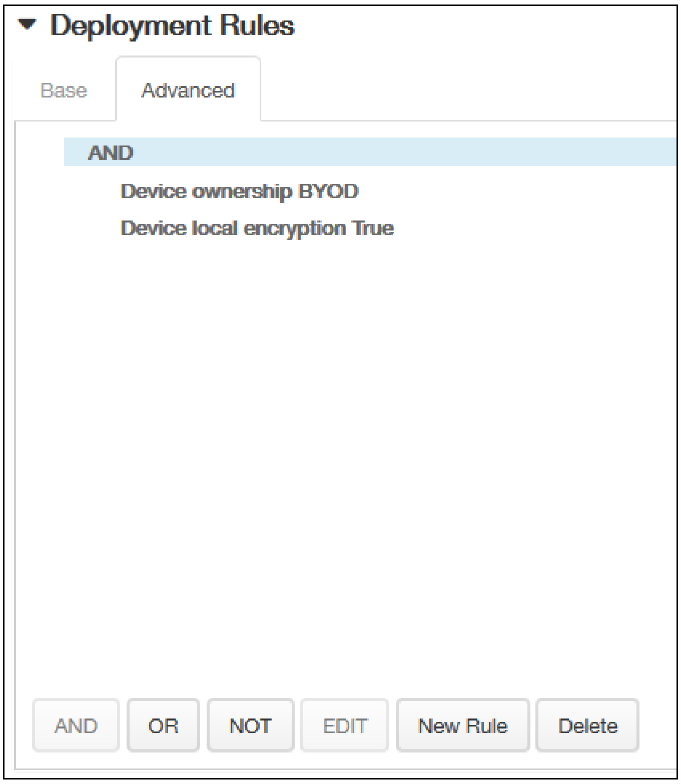
   Note: When the Policy Platforms page appears, all platforms are selected and you see the Windows Phone 8.1 platform configuration panel first.



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.



AND

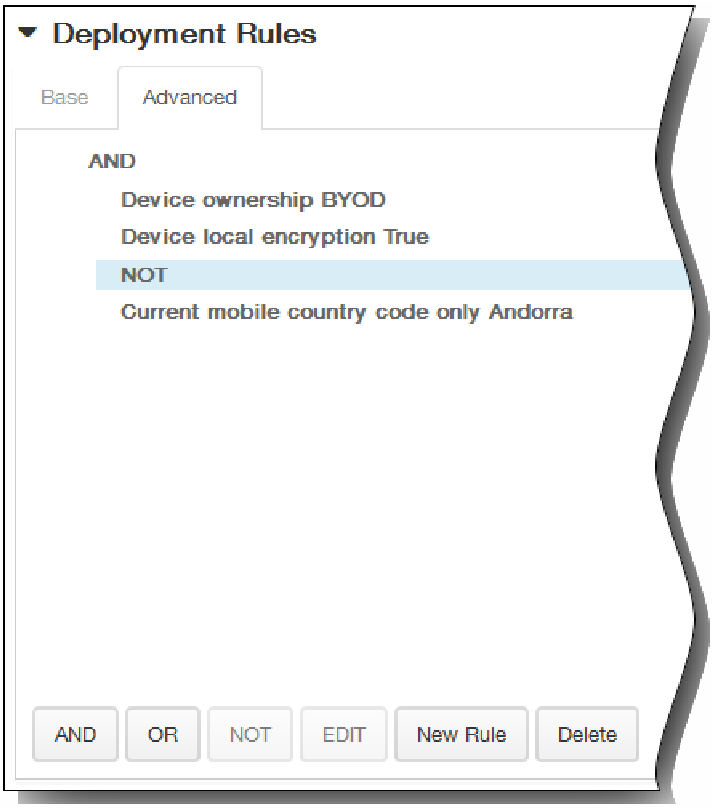
Device ownership BYOD

Device local encryption True

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.

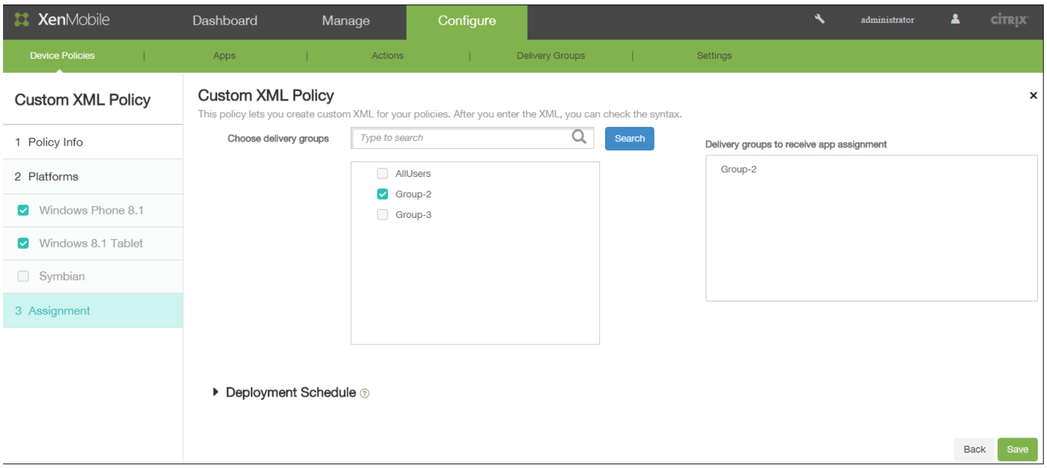
   3. Click New Rule again if you want to add more conditions.
      In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



AND
Device ownership BYOD
Device local encryption True
NOT
Current mobile country code 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.



Custom XML Policy

1 Policy Info
2 Platforms
☑ Windows Phone 8.1
☑ Windows 8.1 Tablet
□ Symbian
3 Assignment

Custom XML Policy

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

Choose delivery groups: Type to search

□ AllUsers
☑ Group-2
□ Group-3

Delivery groups to receive app assignment

Group-2

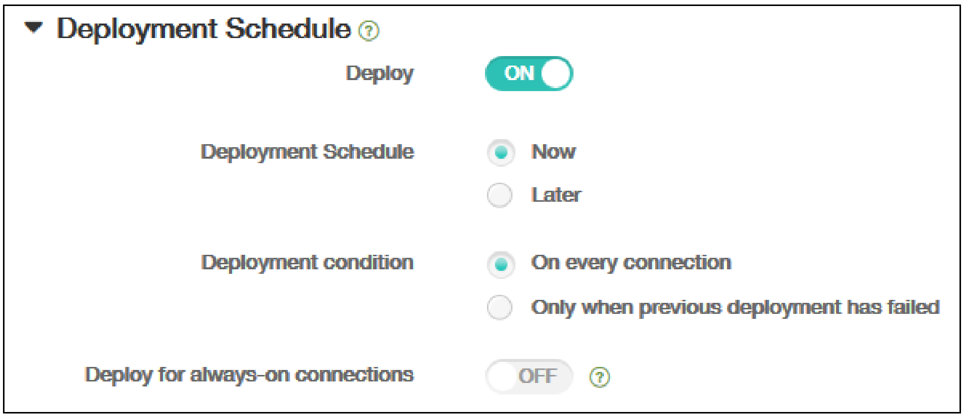
▸ Deployment Schedule

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.



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

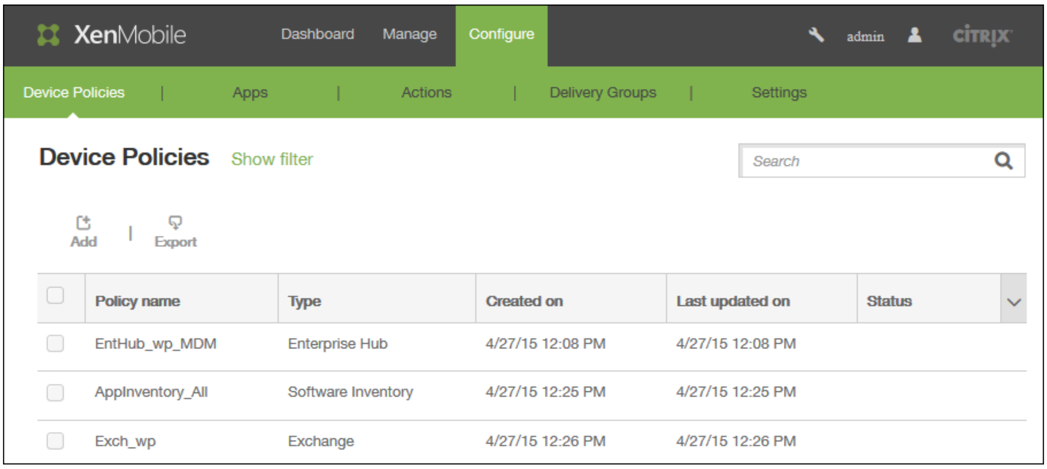
12. Click Save to save the policy.

App uninstall device policies

Jun 23, 2015

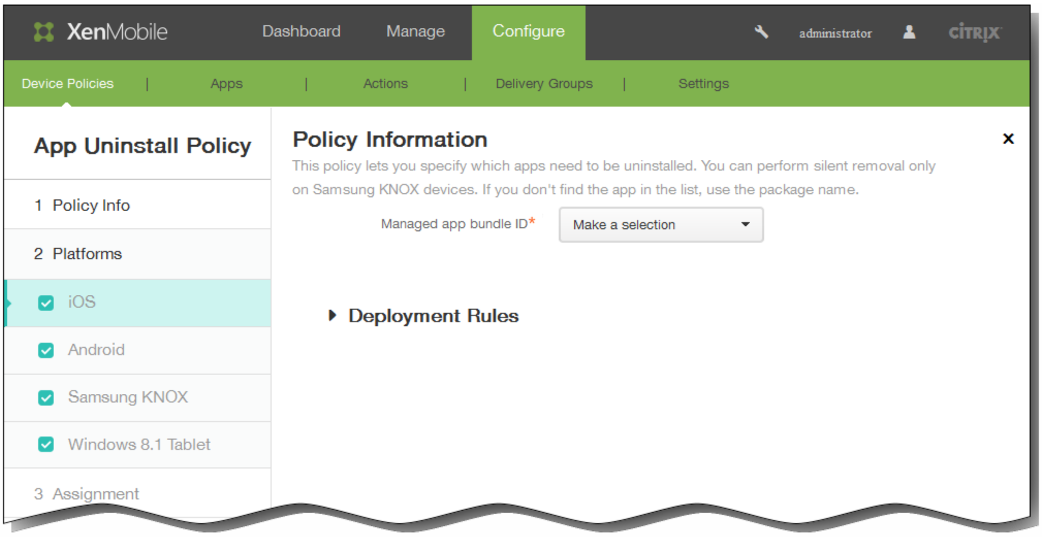
You can create an app uninstall policy for iOS, Android, Samsung KNOX, Android for Work, and Windows 8.1 Tablet platforms. An app uninstall policy lets you remove apps from users' devices for any number of reasons. It may be that you no longer want to support certain apps, your company may want to replace 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.



□	Policy name	Type	Created on	Last updated on	Status
□	EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
□	AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
□	Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	

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.

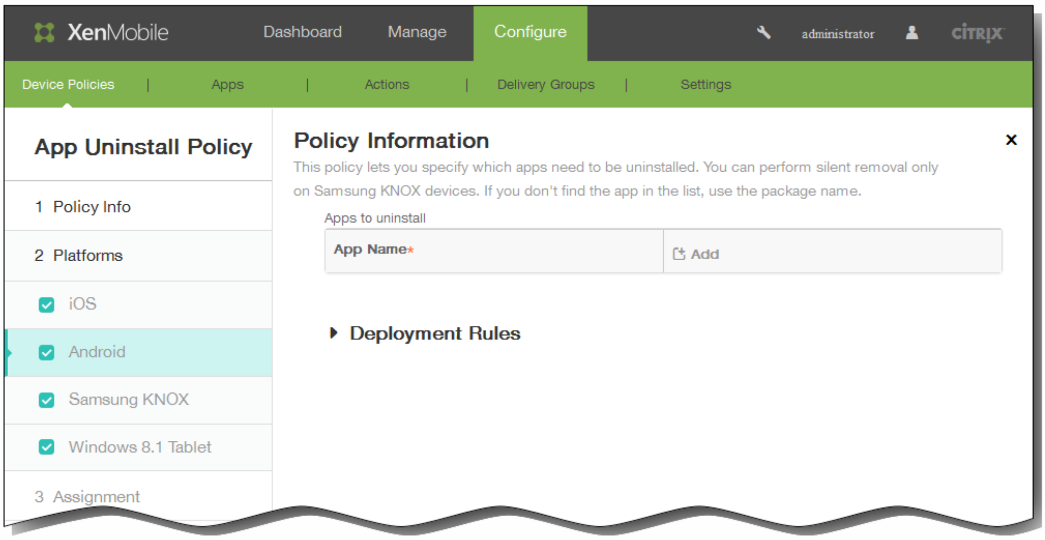


Policy Information

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

Managed app bundle ID* Make a selection

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, Android for Work, or Windows 8.1 Tablet:



Policy Information

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

Apps to uninstall

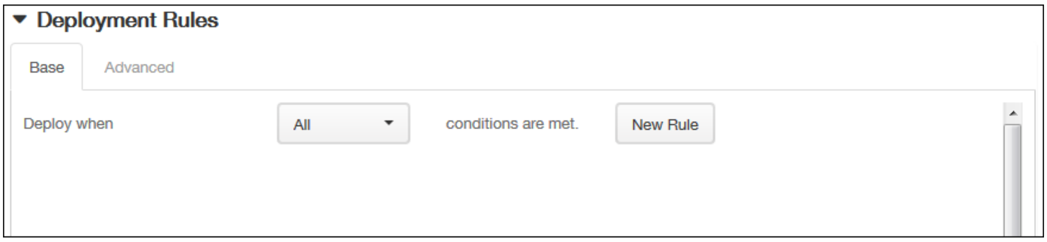
App Name*

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

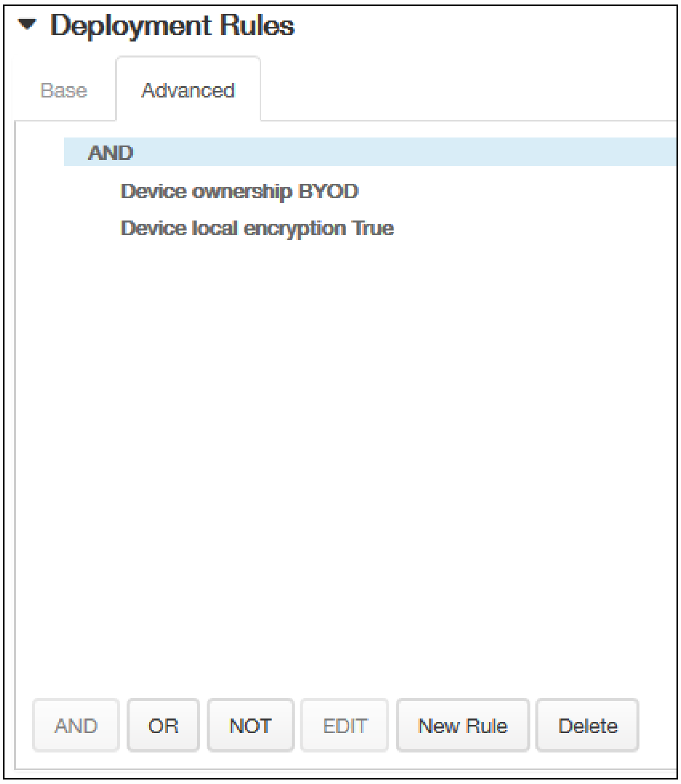
1. App name: In the list, click an existing app or click Add new to enter a new app name.
   Note: If there are no apps configured for this platform, the list will be empty and you must add new apps.
2. Click Add to add the app or click Cancel to cancel adding the app.
3. Repeat steps i. and ii. for 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.

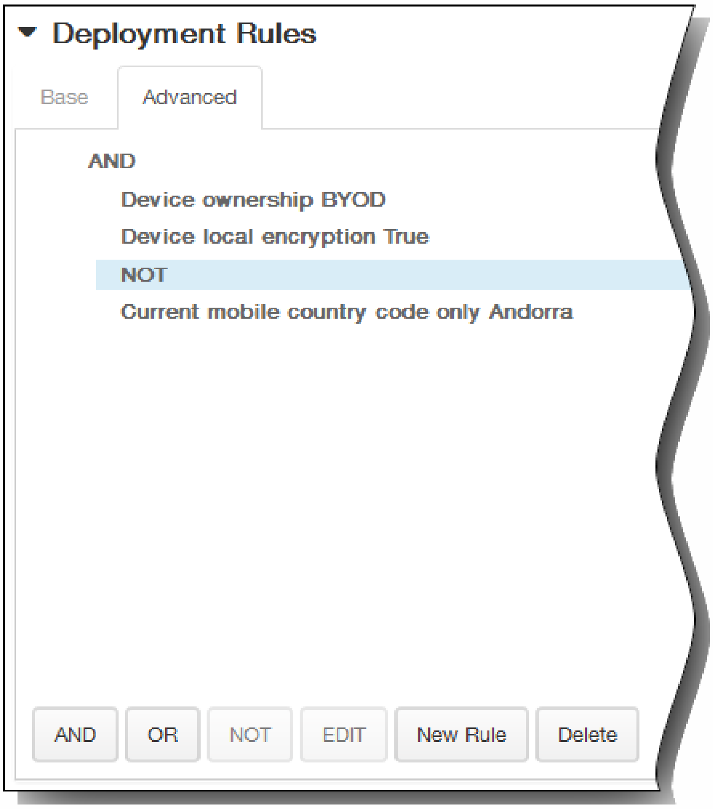


1. In the lists, click options to determine when the policy should be deployed.
   1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
   2. Click New Rule to define the conditions.
   3. In the lists, click the conditions, such 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.



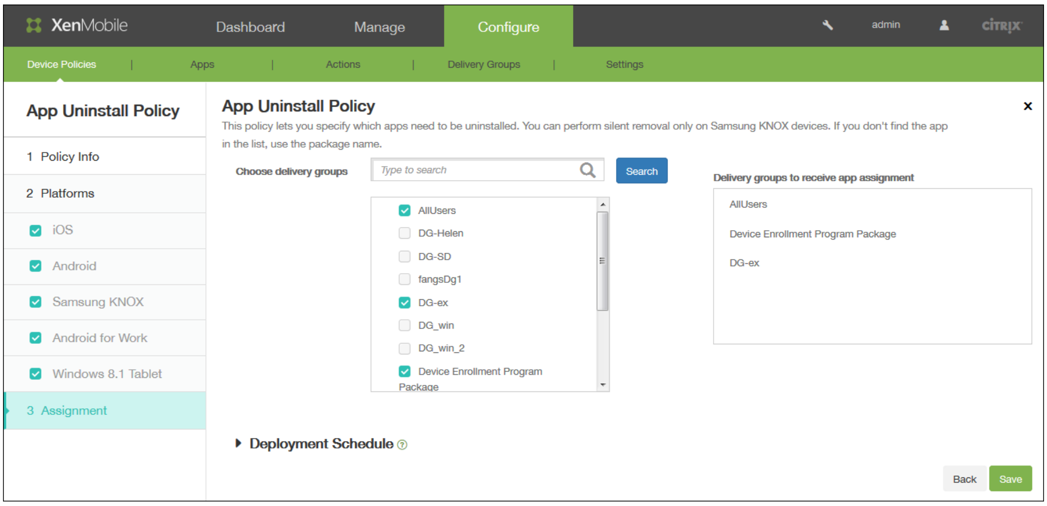
The conditions you chose on the Base tab appear.

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.



AND
Device ownership BYOD
Device local encryption True
NOT
Current mobile country code 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.


XenMobile
Dashboard
Manage
Configure
admin
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings
Back
Save
Search

App Uninstall Policy

1 Policy Info
2 Platforms
☑ iOS
☑ Android
☑ Samsung KNOX
☑ Android for Work
☑ Windows 8.1 Tablet
3 Assignment

App Uninstall Policy

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

Choose delivery groups: Type to search

☑ AllUsers
□ DG-Helen
□ DG-SD
□ fangsDg1
☑ DG-ex
□ DG_win
□ DG_win_2
☑ Device Enrollment Program Package

Delivery groups to receive app assignment

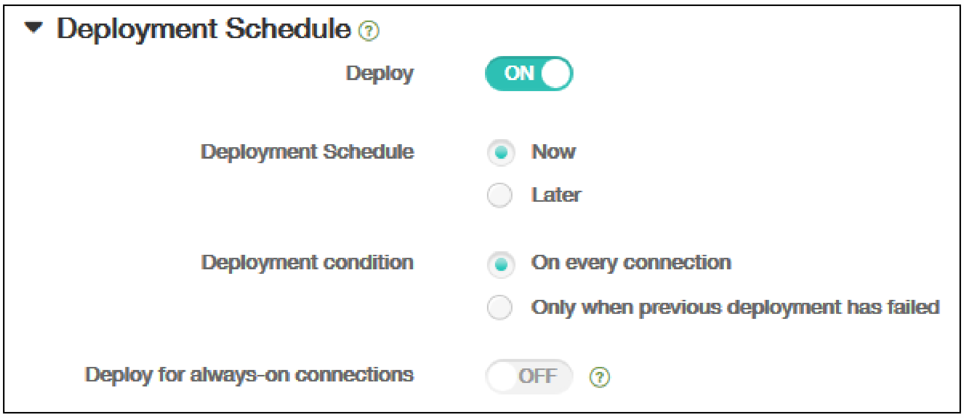
AllUsers
Device Enrollment Program Package
DG-ex

▸ Deployment Schedule

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.



▾ 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

10. Click Save to save the policy.

To add a files device policy for Android

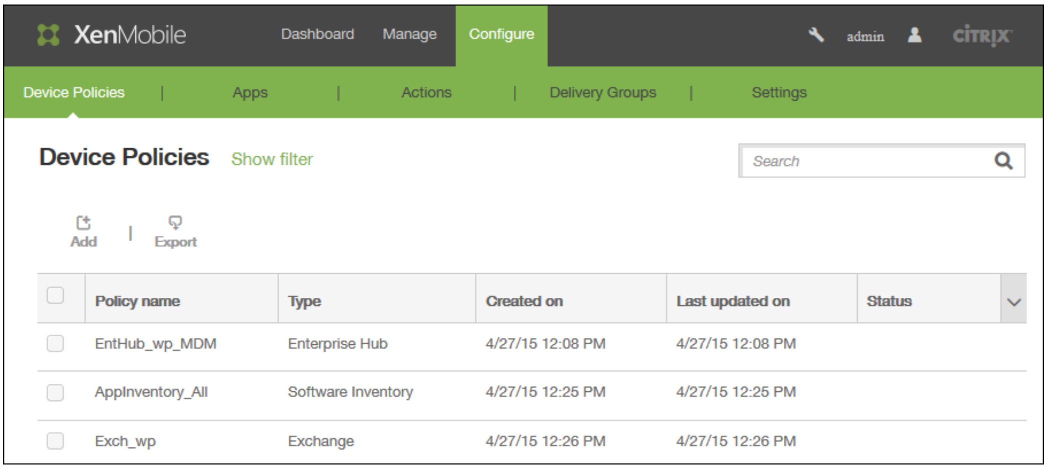
Jun 20, 2016

You can add script files to XenMobile that perform certain functions for users, or you can add document files that you want Android device users to be able to access on their devices. When you add the file, you can also specify the directory in which you want the file to be stored on the device. For example, if you want Android users to receive a company document or .pdf file, you can deploy the file to the device and let users know where the file is located.

You can add the following file types with this policy:

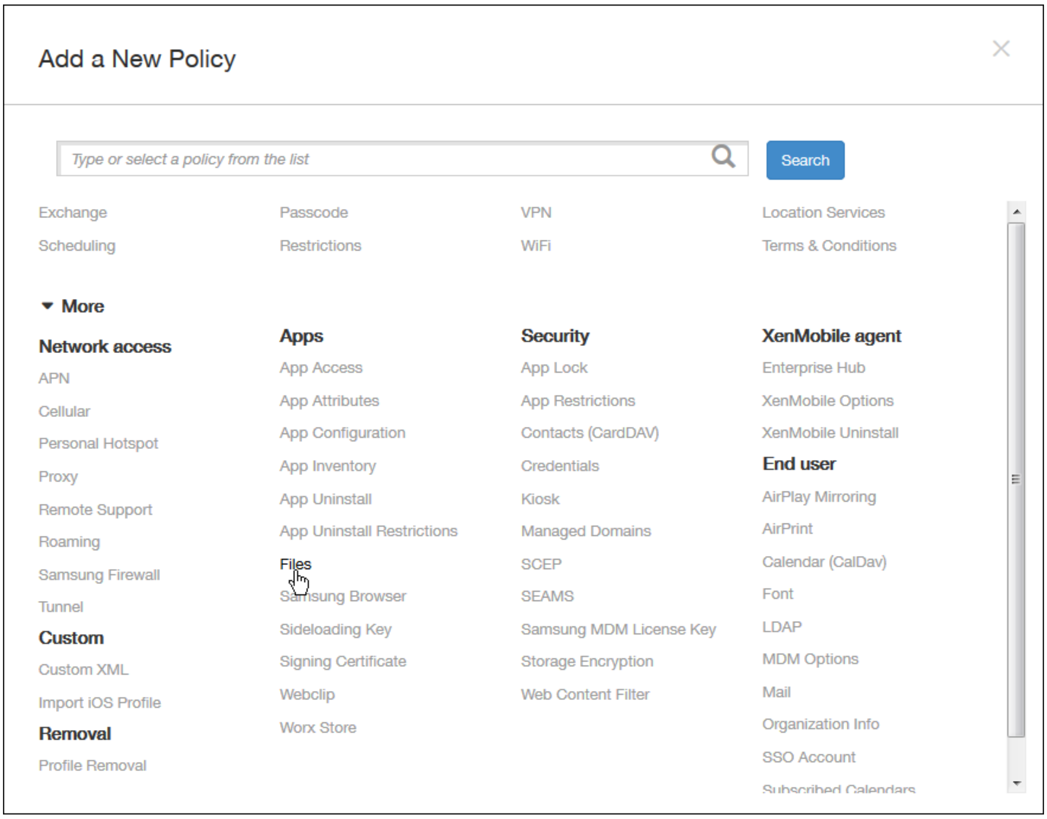
- Text-based files (.xml, .html, .py, and so on)
- Other files, such as documents, pictures, spreadsheets, or presentations
- For Windows Mobile and Windows CE only: Script files created with MortScript

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

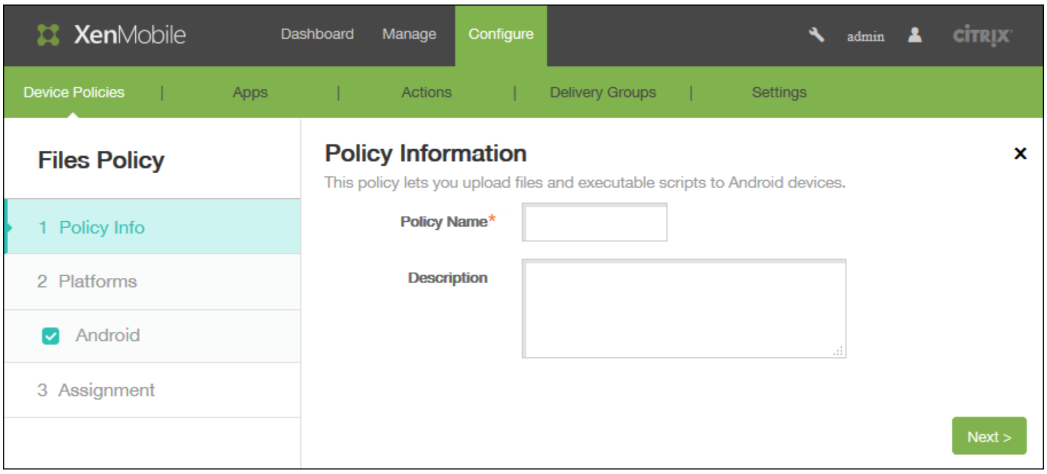


□	Policy name	Type	Created on	Last updated on	Status
□	EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
□	AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
□	Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	

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



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



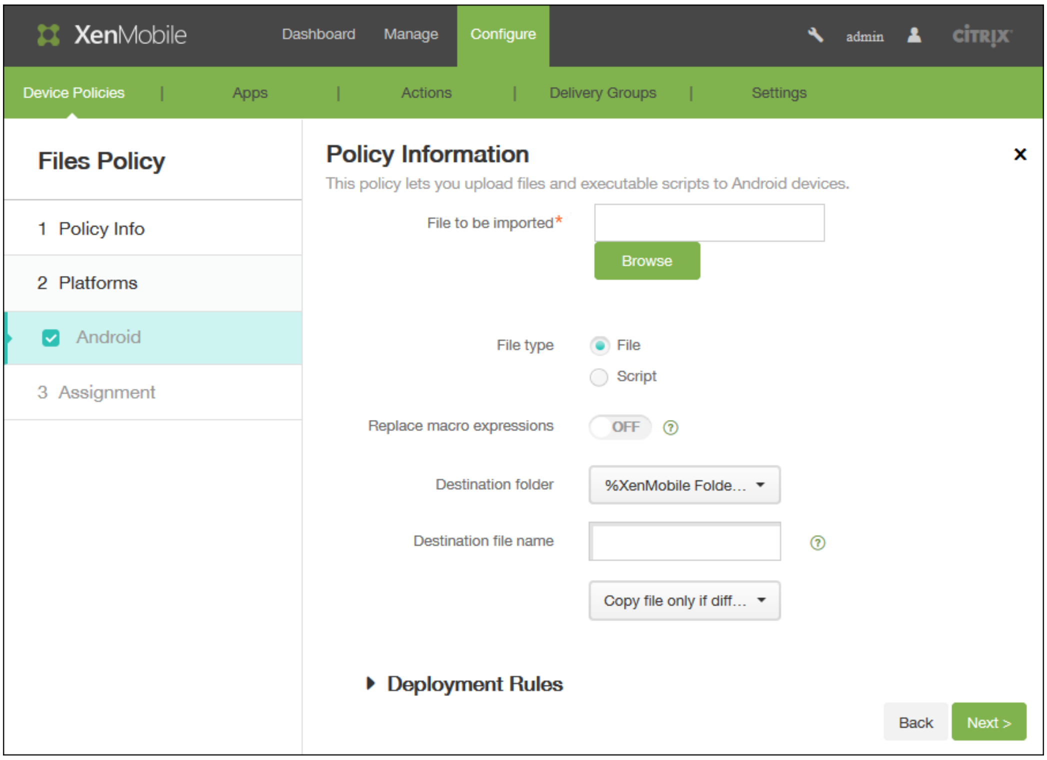
Policy Information

This policy lets you upload files and executable scripts to Android devices.

Policy Name*

Description

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.



Policy Information

This policy lets you upload files and executable scripts to Android devices.

File to be imported*

File type ● File ○ Script

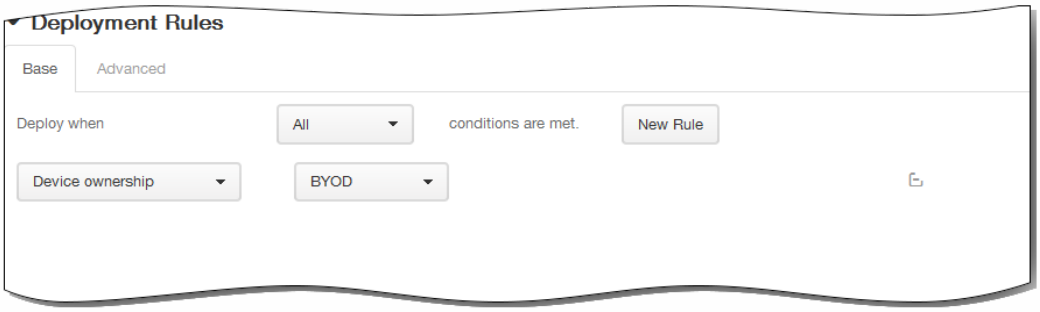
Replace macro expressions OFF

Destination folder %XenMobile Folde...

Destination file name

Copy file only if diff...

6. In the Android Platform information page, enter the following information:
   1. File to be imported: Select the file to import by clicking Browse and navigating to the file's location.
   2. File type: Select either File or Script. When you select Script, Execute immediately appears. Select whether the script is executed as soon as the file is uploaded. The default is OFF.
   3. Replace macro expressions: Select whether to replace macro token names in a script with a device or user property.
   4. Destination folder: In the list, select the location in which to store the uploaded file.
   5. Destination file name: Optionally, type a different name for the file if it must be changed before being deployed on a device.
   6. Copy file only if different: In the list, select whether to copy the file if it is different from the existing file or to overwrite the existing file.
7. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.

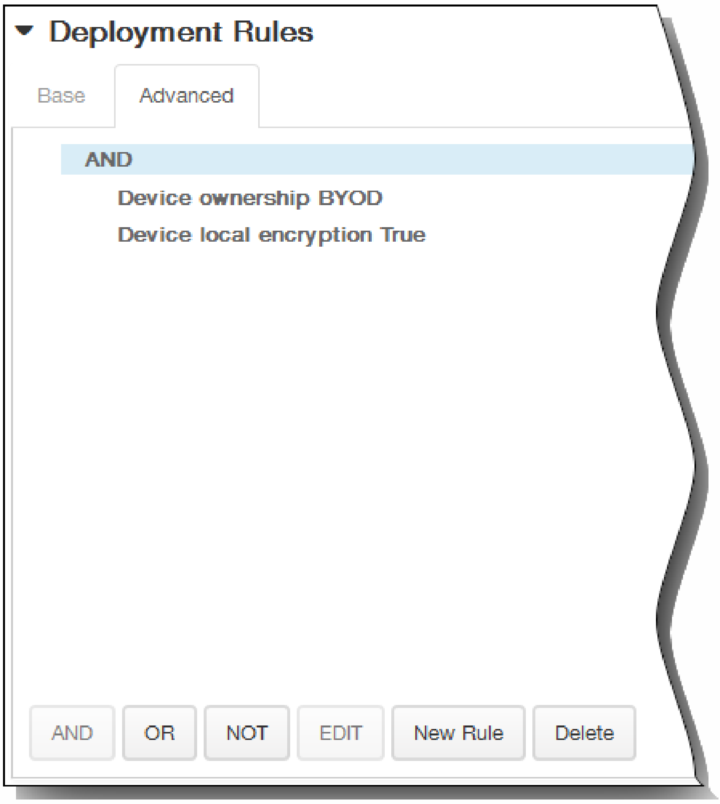


Deploy when All conditions are met.

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.

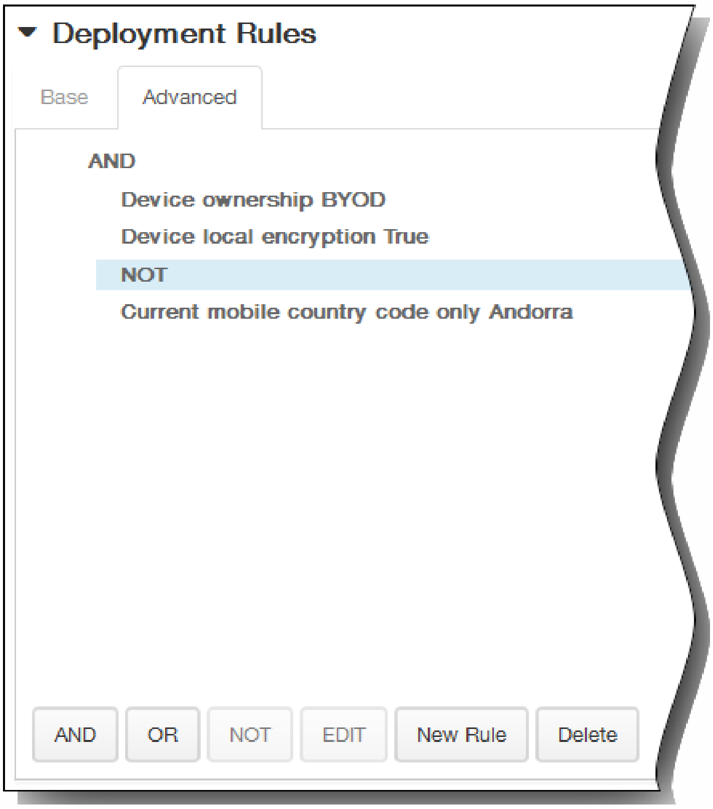
   3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
   4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



AND
Device ownership BYOD
Device local encryption True

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.



AND

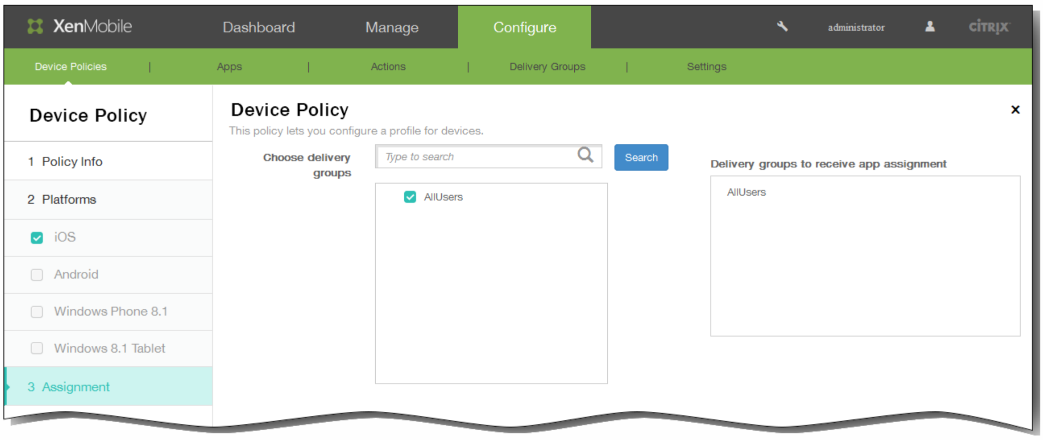
Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra

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



Device Policy

This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

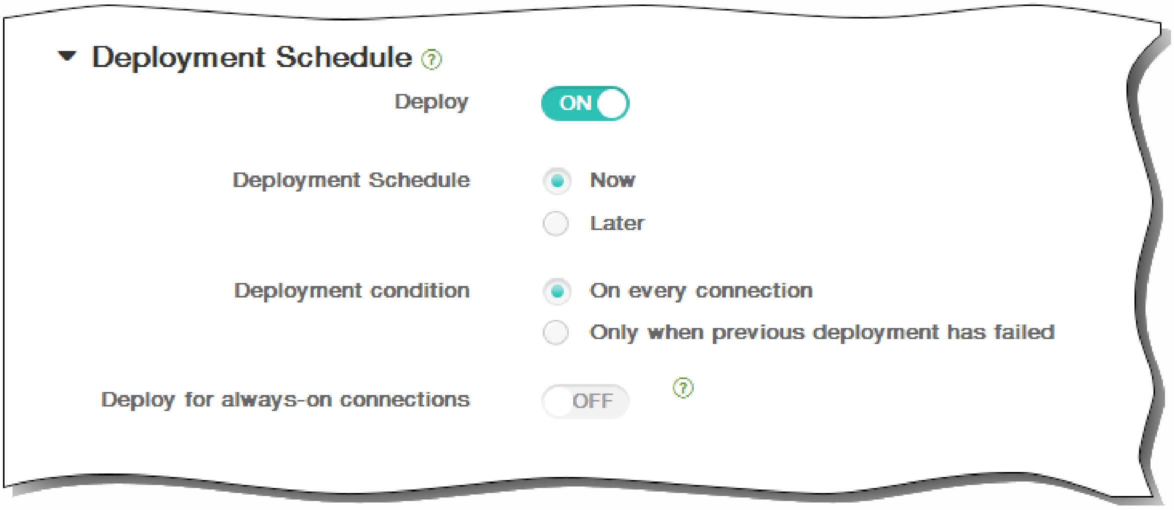
Delivery groups to receive app assignment

AllUsers

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.



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

11. Click Save to save the policy.

APN device policies

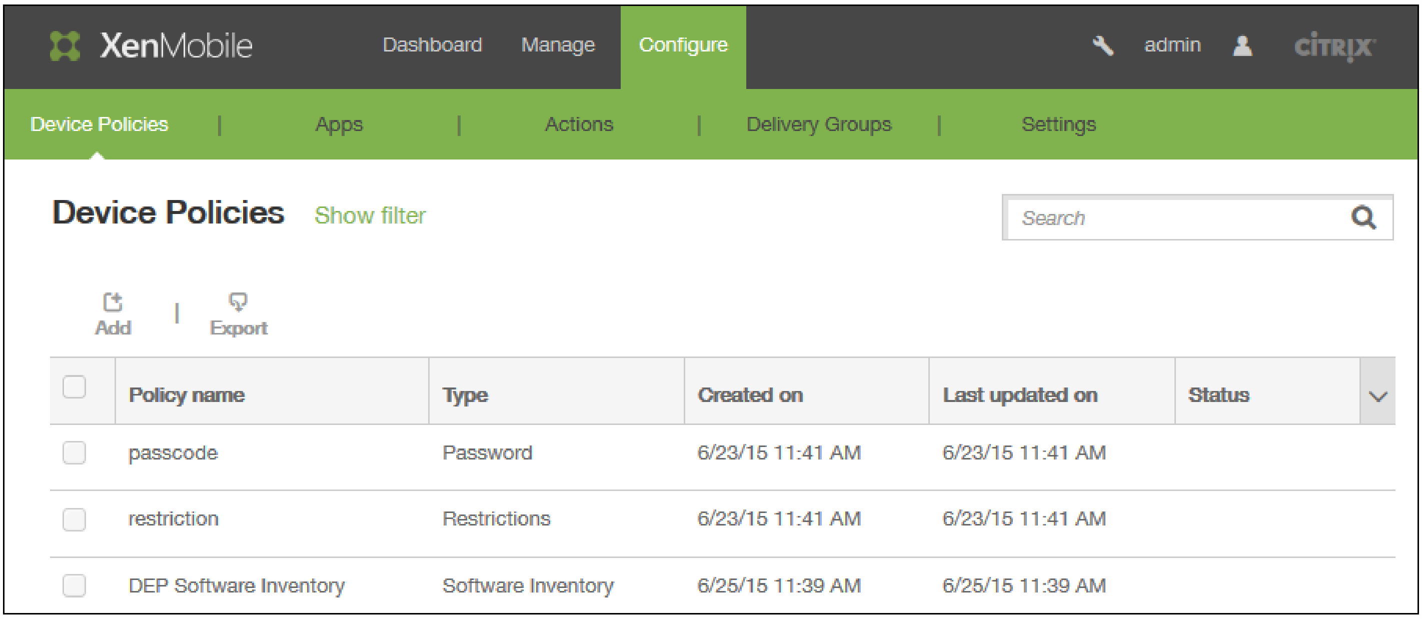
Jun 15, 2015

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

iOS settings

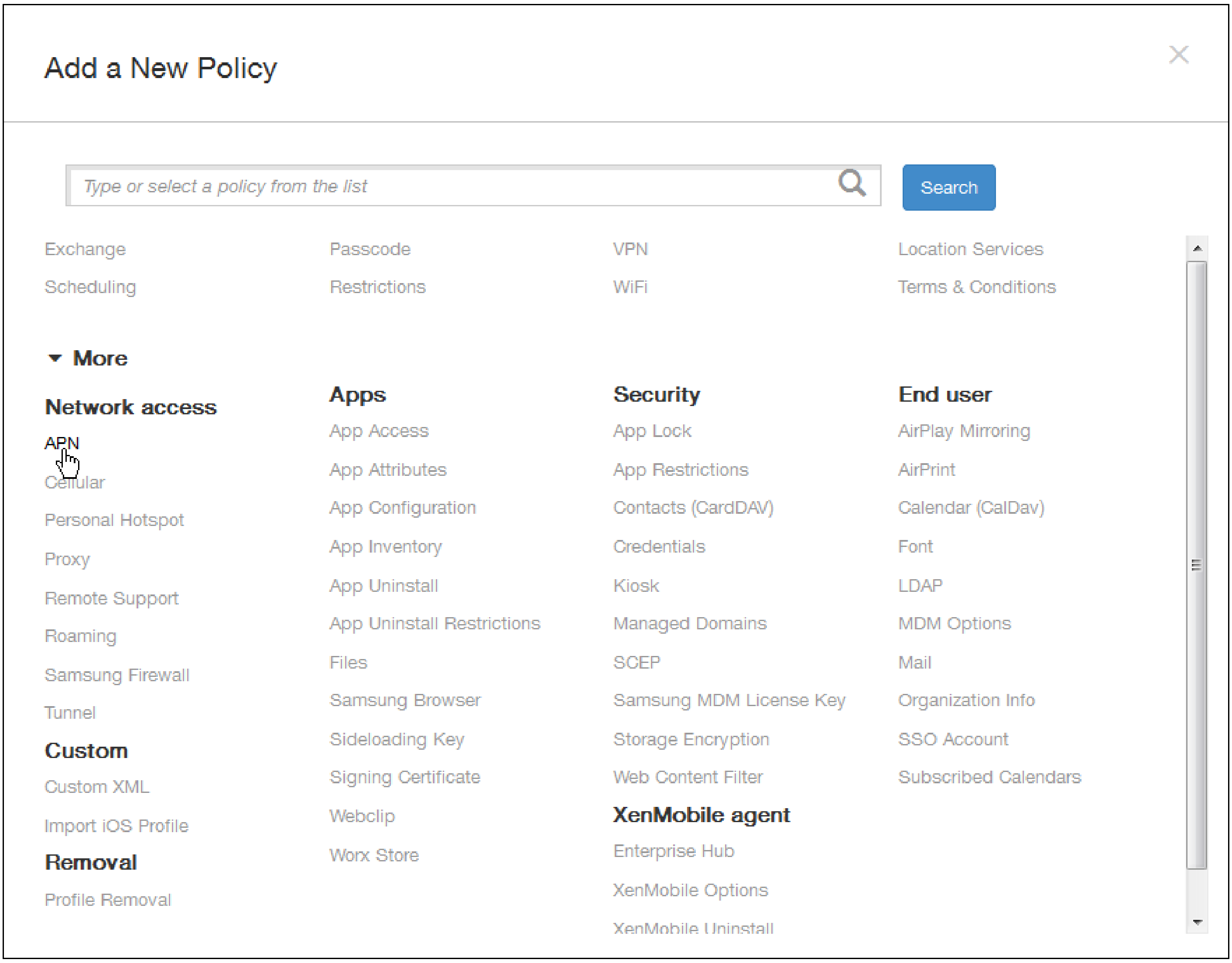
Android settings

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

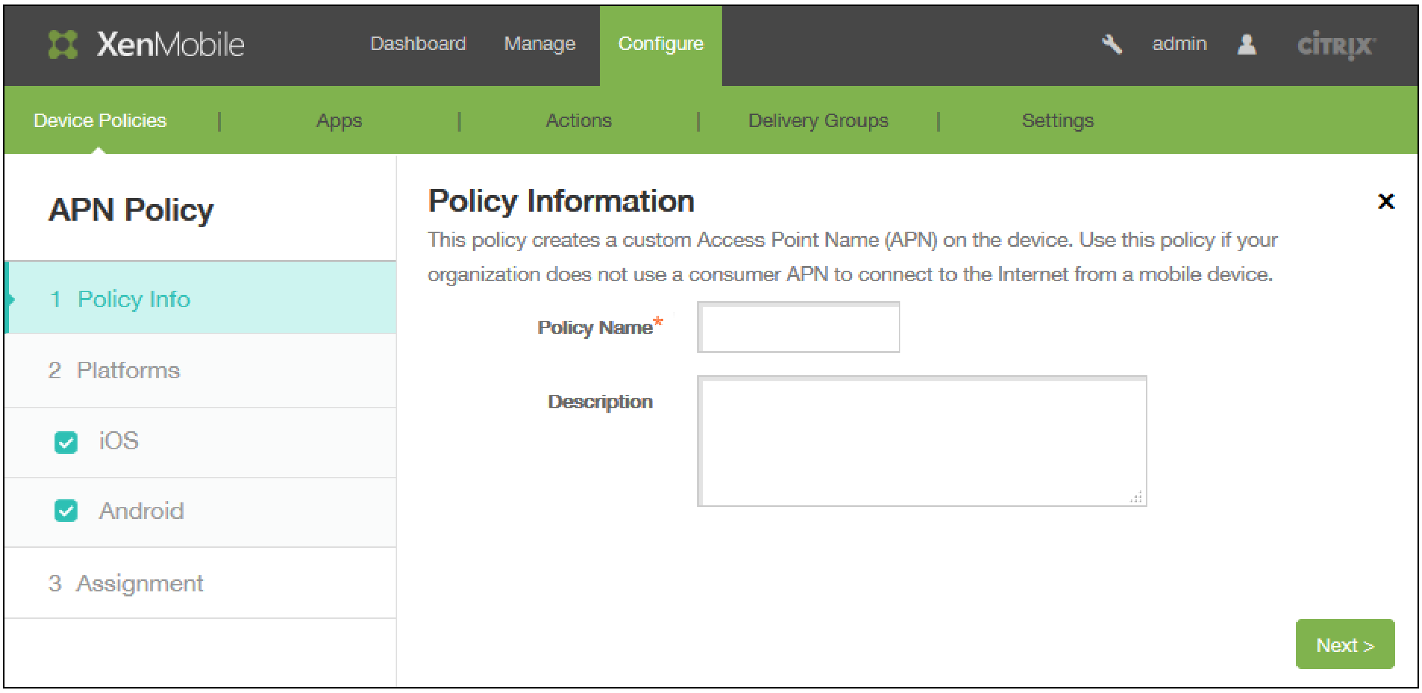


□	Policy name	Type	Created on	Last updated on	Status
□	passcode	Password	6/23/15 11:41 AM	6/23/15 11:41 AM	
□	restriction	Restrictions	6/23/15 11:41 AM	6/23/15 11:41 AM	
□	DEP Software Inventory	Software Inventory	6/25/15 11:39 AM	6/25/15 11:39 AM	

2. Click **Add** to add a new policy. The **Add a new Policy** page appears.



3. On the **Add a New Policy** page, click **More** and then under **Network access**, click **APN**. The **APN Policy** information page appears.



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.

Policy Name*

Description

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

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

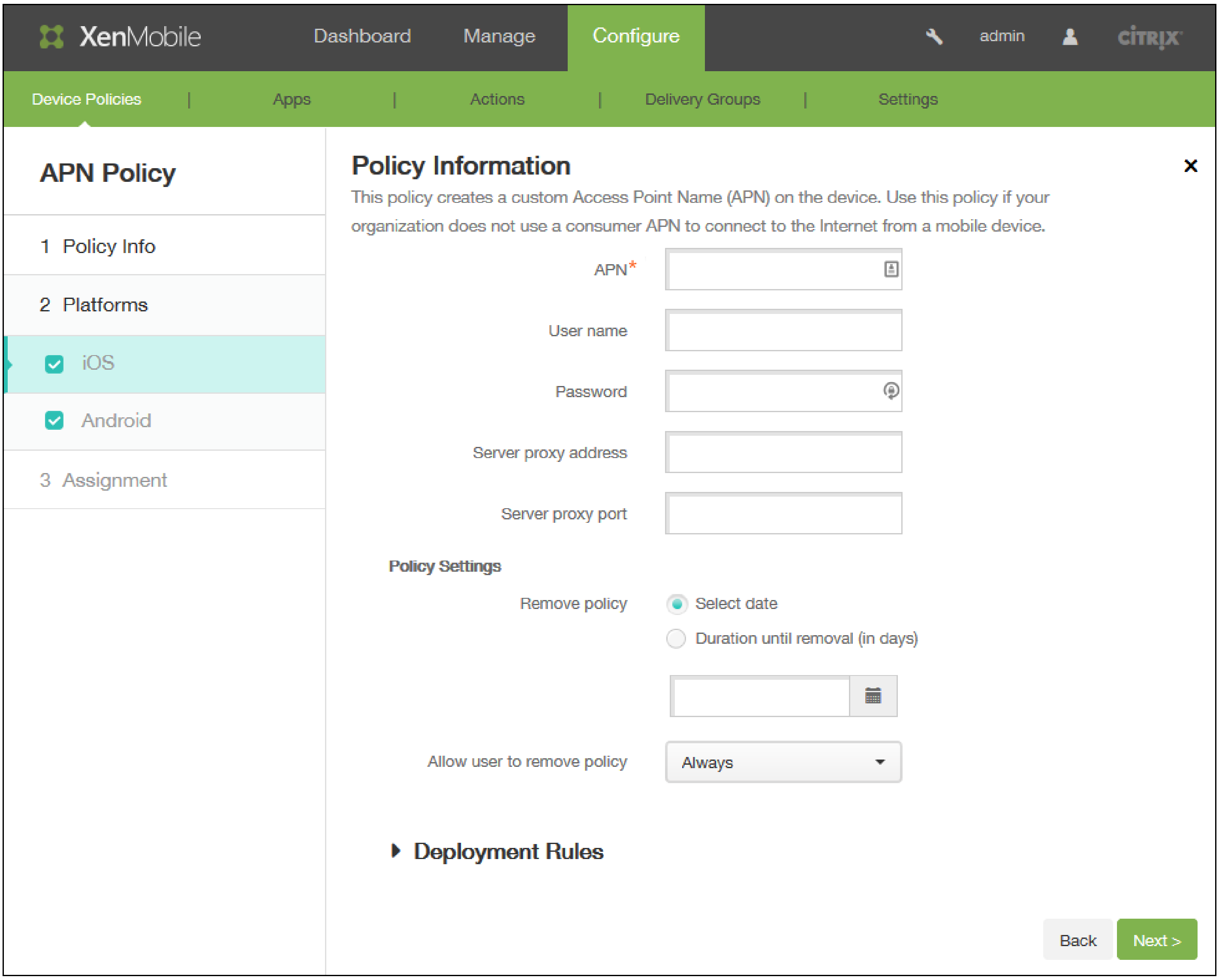
5. Click **Next**. The **Policy Platforms** page appears.

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

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

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

iOS settings



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

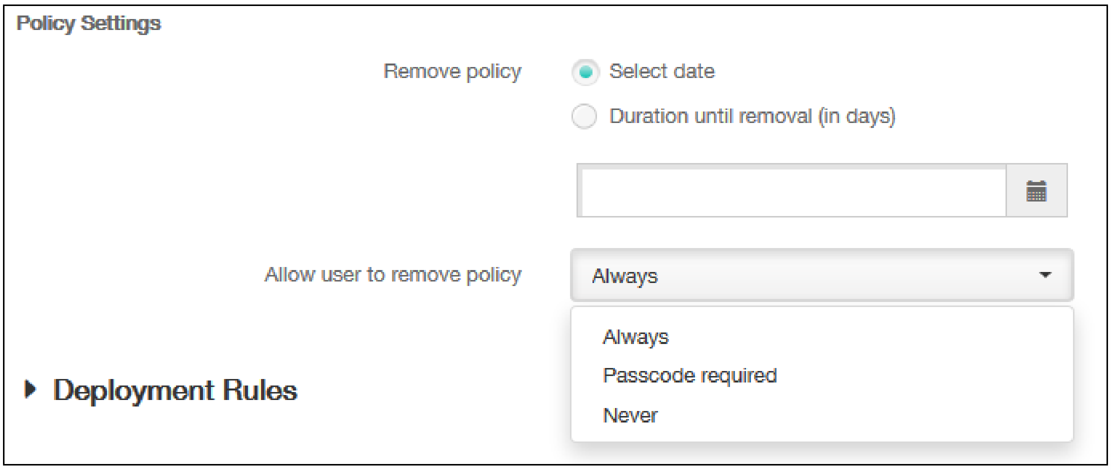
Server proxy port

Policy Settings

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

Allow user to remove policy: Always

- **APN**: Type the name of the access point. This must match a an accepted iOS APN or the policy will fail.
- **User name**: This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
- **Password**: The password for the user for this APN. For obfuscation purposes, the password is encoded. If it is missing from the payload, the device prompts for the password during profile installation.
- **Server proxy address**: The IP address or URL of the APN proxy.
- **Server proxy port**: The port number for the APN proxy. This is required if you entered a server proxy address.
- Under **Policy Settings**, next to **Remove policy**, click either **Select date** or **Duration until removal (in days)**.
  - If you click **Select date**, click the calendar to select the specific date for removal.
  - In the **Allow user to remove policy list**, click **Always**, **Password required**, or **Never**.
  - If you click **Password required**, next to **Removal password**, type the necessary password.



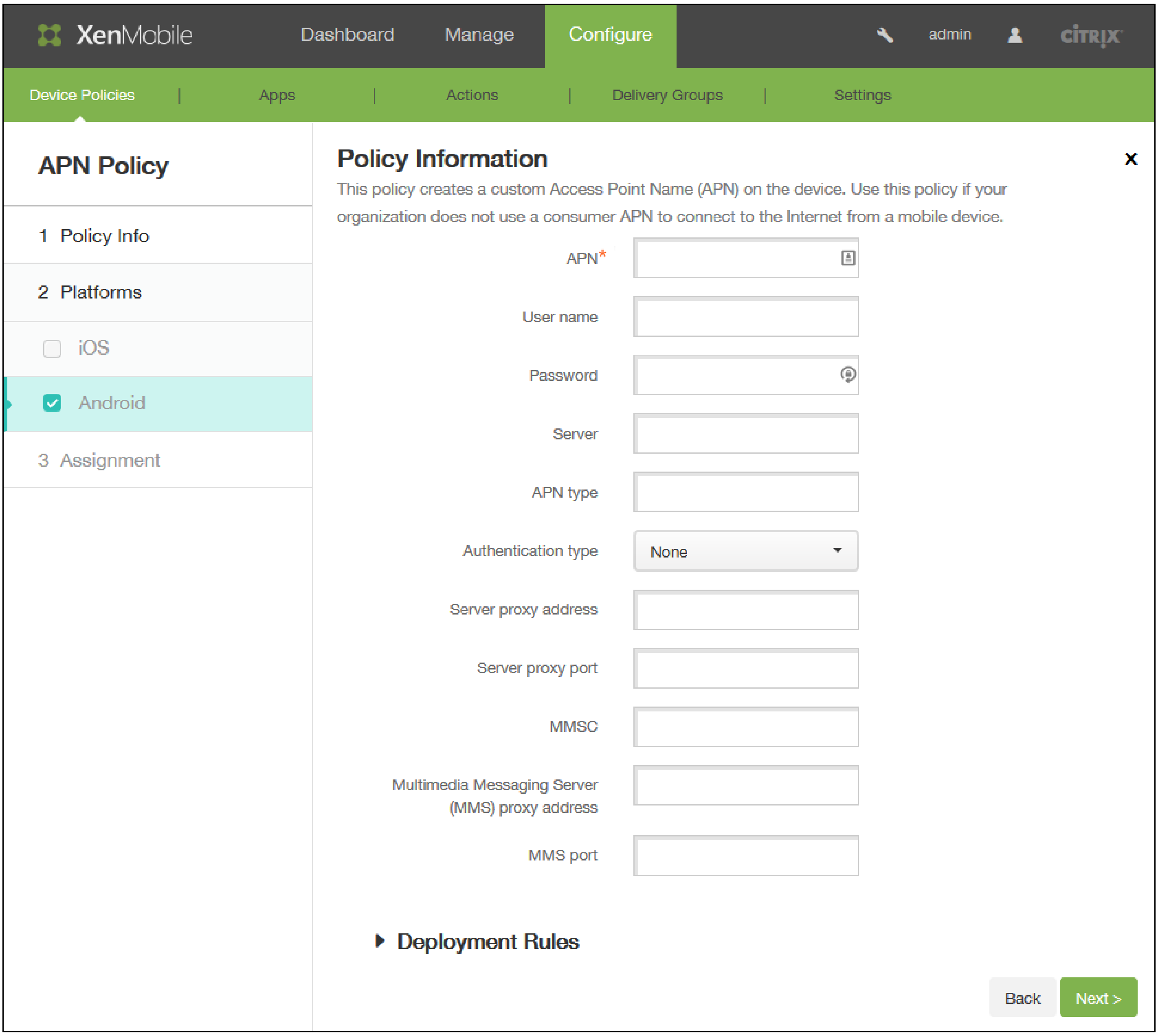
Policy Settings

Remove policy ● Select date

○ Duration until removal (in days)

Allow user to remove policy: Always

Android settings



Policy Information

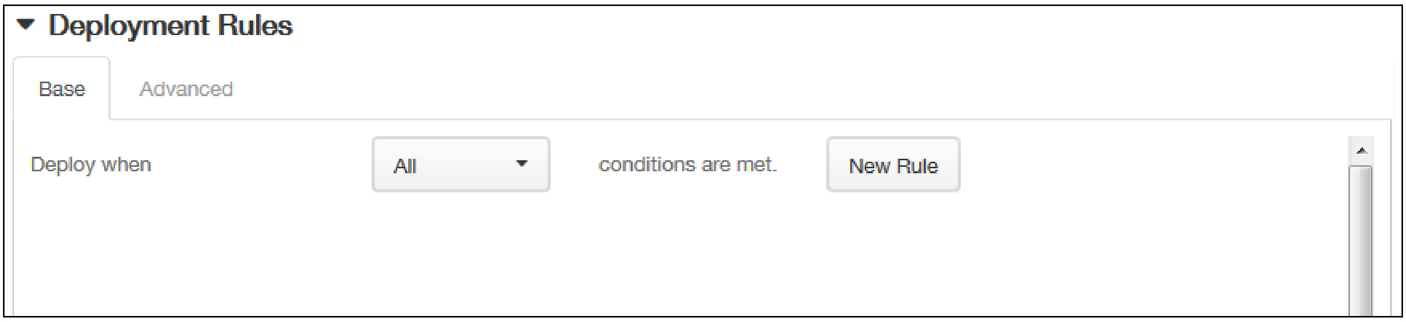
This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN*	
User name	
Password	
Server	
APN type	
Authentication type	None
Server proxy address	
Server proxy port	
MMSC	
Multimedia Messaging Server (MMS) proxy address	
MMS port	

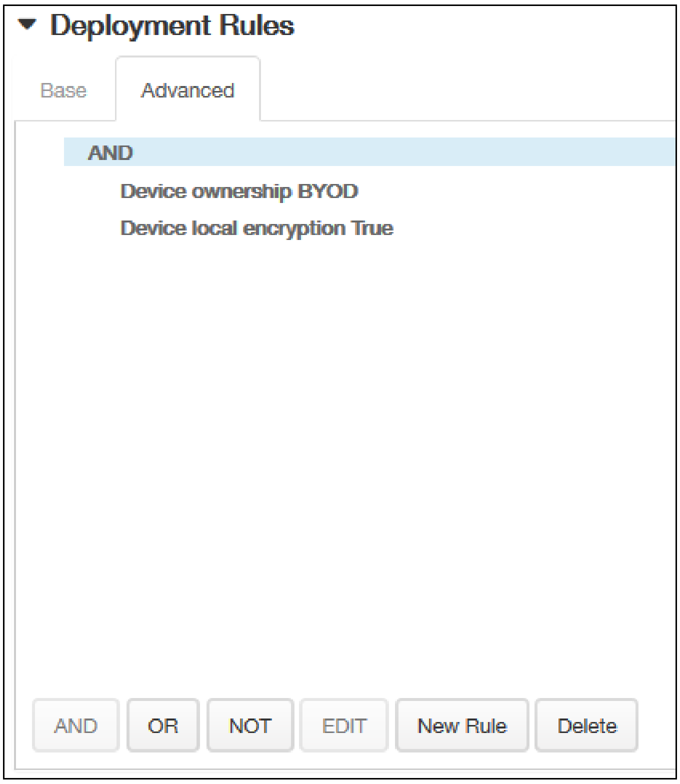
- **APN**: Type the name of the access point. This must match a an accepted Android APN or the policy will fail.
- **User name**: This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
- **Password**: The password for the user for this APN. For obfuscation purposes, the password is encoded. If it is missing from the payload, the device prompts for the password during profile installation.
- **Server**: This setting, which predates smart phones, is usually empty. It references a Wireless Application Protocol (WAP) gateway server for phones that could not access or render standardweb sites.
- **APN type**: This setting must match the carrier's intended use for the access point. It is a comma separated string of APN service specifiers and must match the wireless carrier's published definitions. Examples include:
  - *. All traffic goes through this access point.
  - mms. Multimedia traffic goes through this access point.
  - default. All traffic, including multimedia, goes through this access point.
  - supl. Secure User Plane Location is associated with assisted GPS.

  - dun. Dial Up Networking is outdated and should rarely be used.
  - hipri. High priority networking.
  - fota. Firmware over the air is used for receiving firmware updates.
- **Authentication type**: In the list, click the type of authentication to be used. Defaults to None.
- **Server proxy address**: The IP address or URL of the carrier's APN HTTP proxy.
- **Server proxy port**: The port number for the APN proxy. This is required if you entered a server proxy address.
- **MMSC**: The MMS Gateway Server address provided by the carrier.
- Multimedia Messaging Server (MMS) proxy address: This is the multimedia messaging service server for MMS traffic. MMS succeeded SMS for sending larger messages with multimedia content, such as pictures or videos. These servers require specific protocols (such as MM1, ... MM11).
- **MMS port**: The port used for the MMS proxy.

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



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



AND

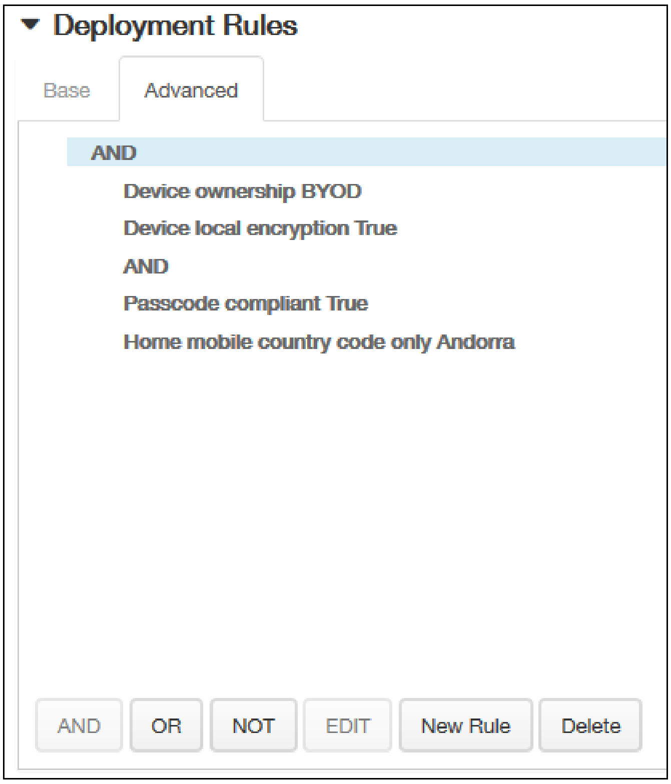
Device ownership BYOD

Device local encryption True

- You can use more advanced Boolean logic to combine, edit, or add rules.
  - Click **AND**, **OR**, or **NOT**.
  - 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.
  - 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.



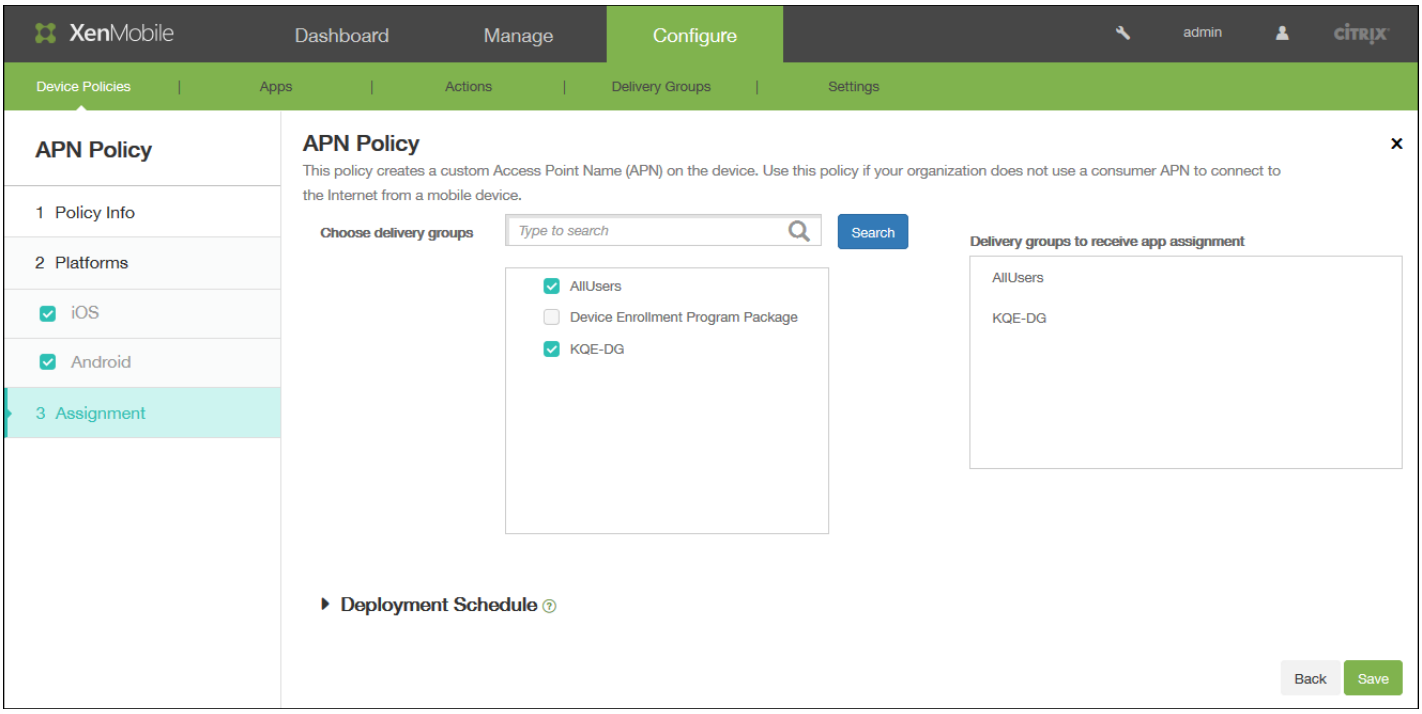
Deployment Rules

Base | Advanced

AND
- Device ownership BYOD
- Device local encryption True
- AND
- Passcode compliant True
- Home mobile country code only Andorra

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

9. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the **Delivery groups to receive app** assignment list.



APN Policy

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

Choose delivery groups: Type to search

- ☑ AllUsers
- □ Device Enrollment Program Package
- ☑ KQE-DG

Delivery groups to receive app assignment

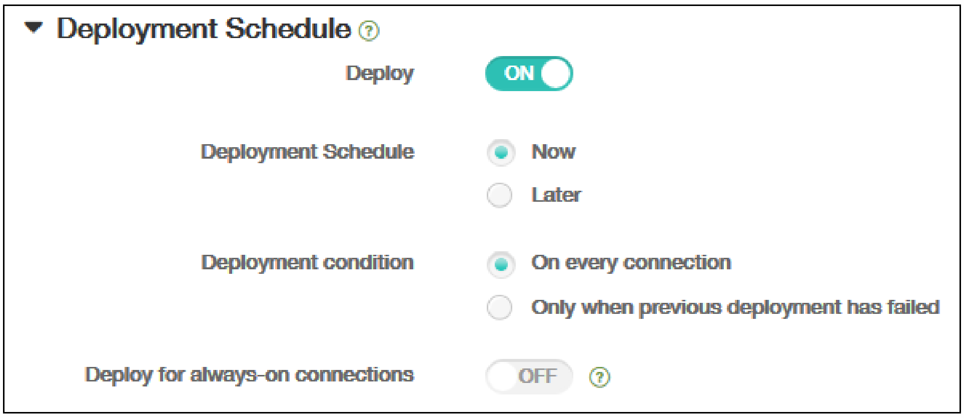
- AllUsers
- KQE-DG

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

- Next to **Deploy**, click **ON** to schedule deployment or click **OFF** to prevent deployment. The default option is **ON**. If you choose **OFF**, no other options need to be configured.
- Next to **Deployment schedule**, click **Now** or **Later**. The default option is **Now**.
- If you click **Later**, click the calendar icon and then select the date and time for deployment.
- Next to **Deployment condition**, click **On every connection** or click **Only when previous deployment has failed**. The default option is **On every connection**.
- Next to **Deploy for always-on connection**, click **ON** or **OFF**. The default option is **OFF**.

Note:

> This option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**. The always-on option is not available for iOS devices.
>
> The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always on connection**, which does not apply to iOS.



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

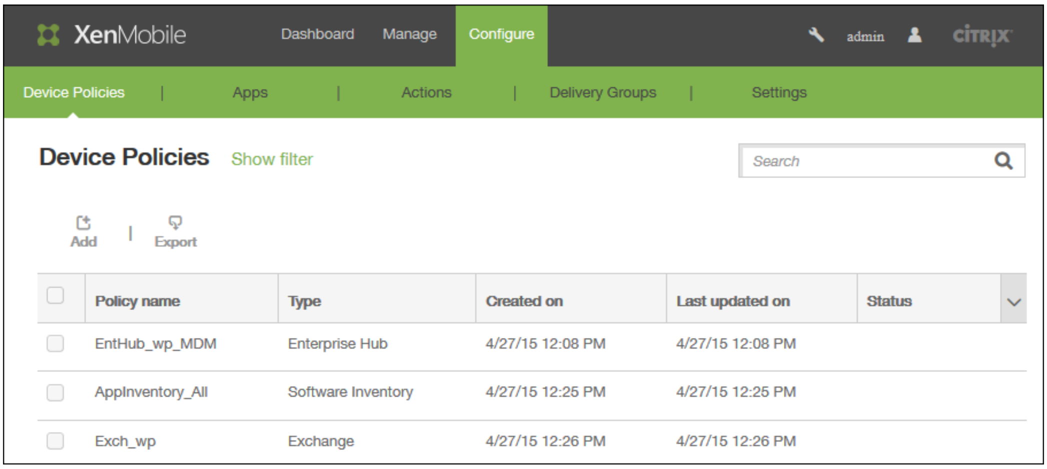
11. Click **Save** to save the policy.

To add a cellular device policy for iOS

Feb 27, 2015

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

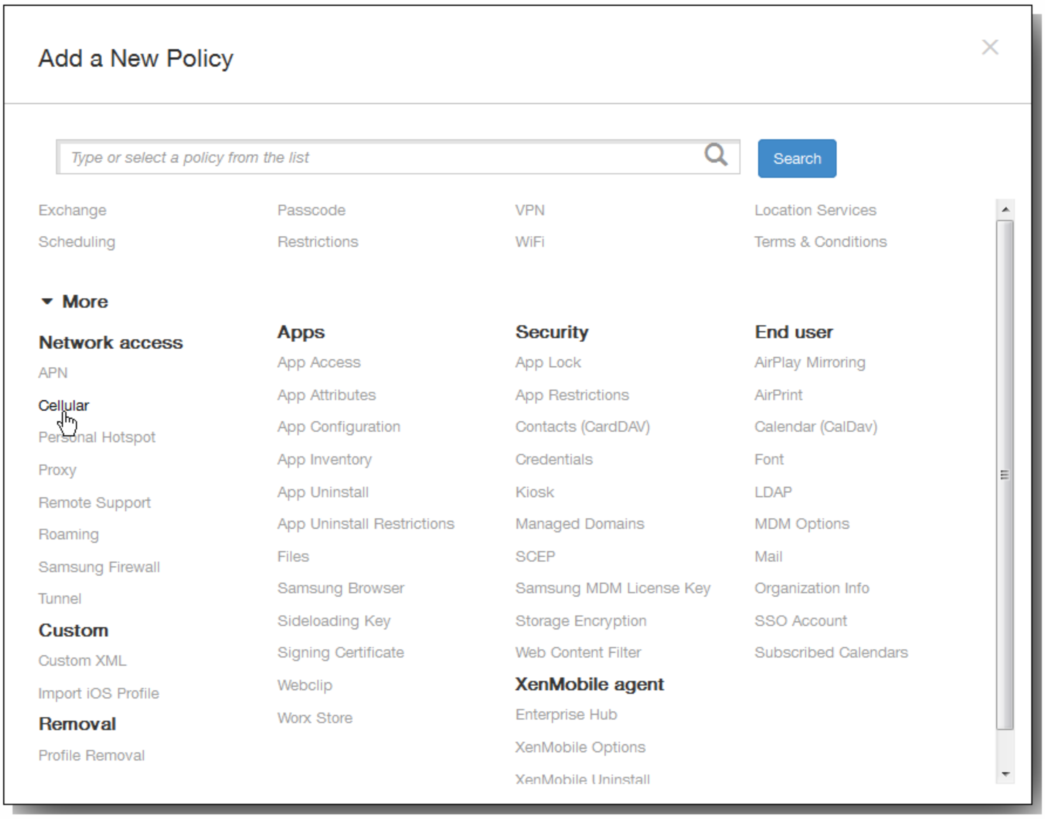
1. In the XenMobile console, click Configure > Device Policies.



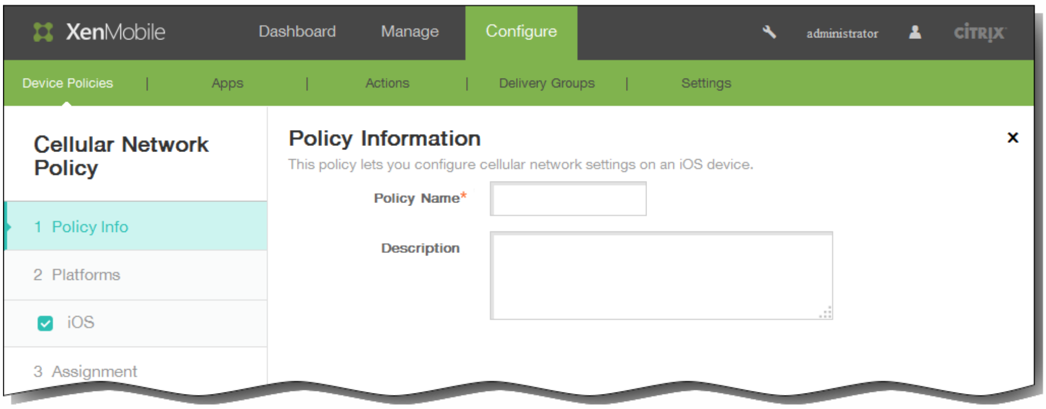
□	Policy name	Type	Created on	Last updated on	Status
□	EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
□	AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
□	Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	

2. Click Add.

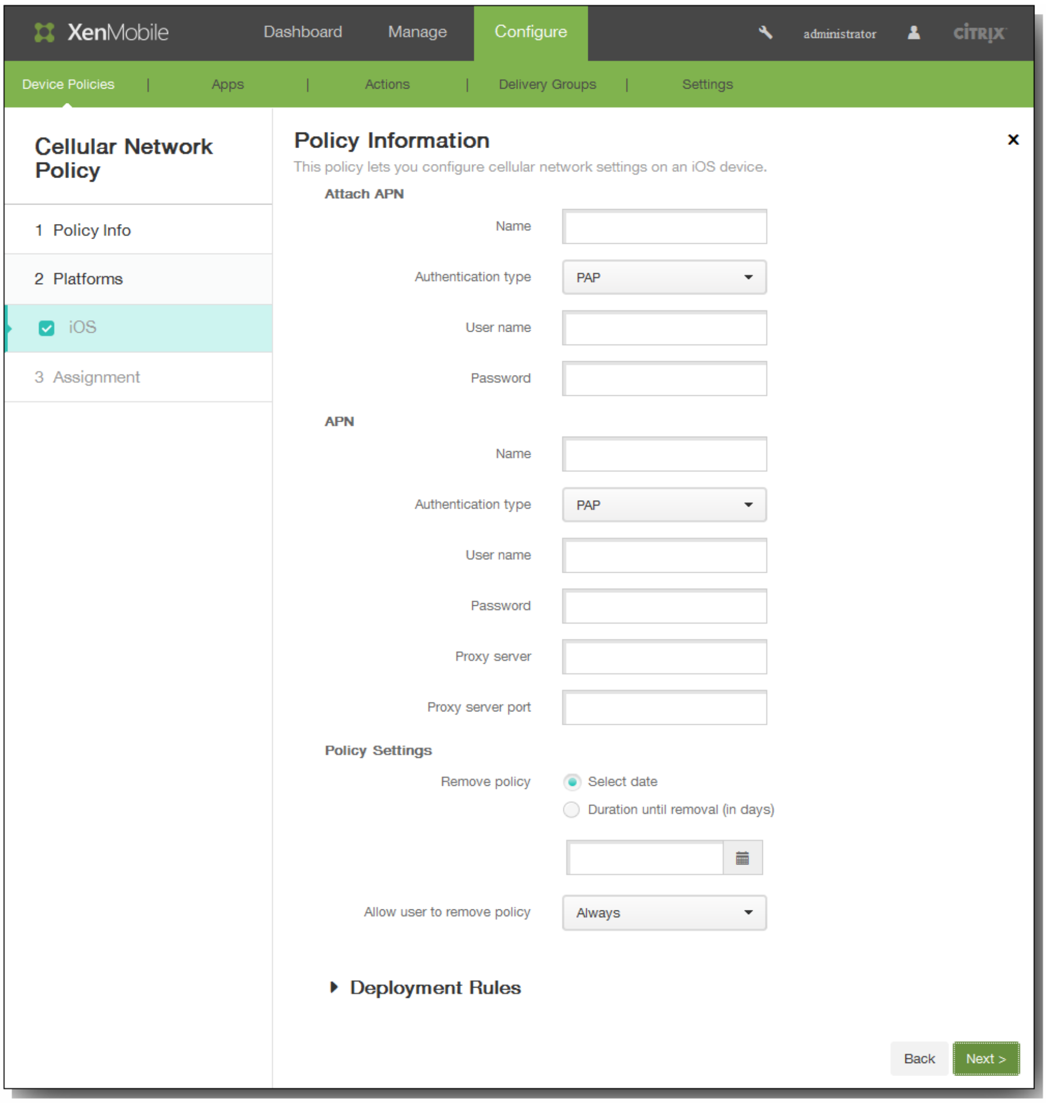
   The Add a New Policy page appears.



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.



Policy Information

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

Attach APN

Name

Authentication type: PAP

User name

Password

APN

Name

Authentication type: PAP

User name

Password

Proxy server

Proxy server port

Policy Settings

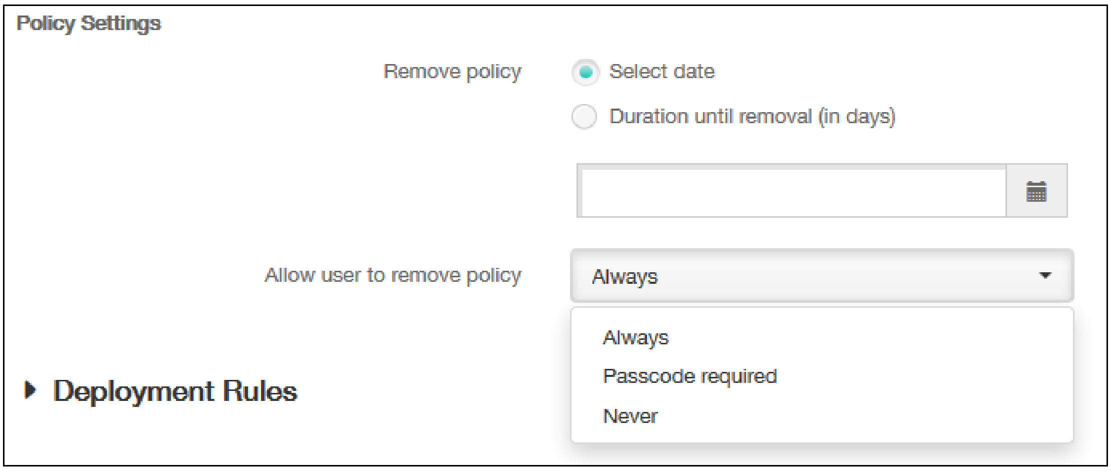
Remove policy: ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always

▸ **Deployment Rules**

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.

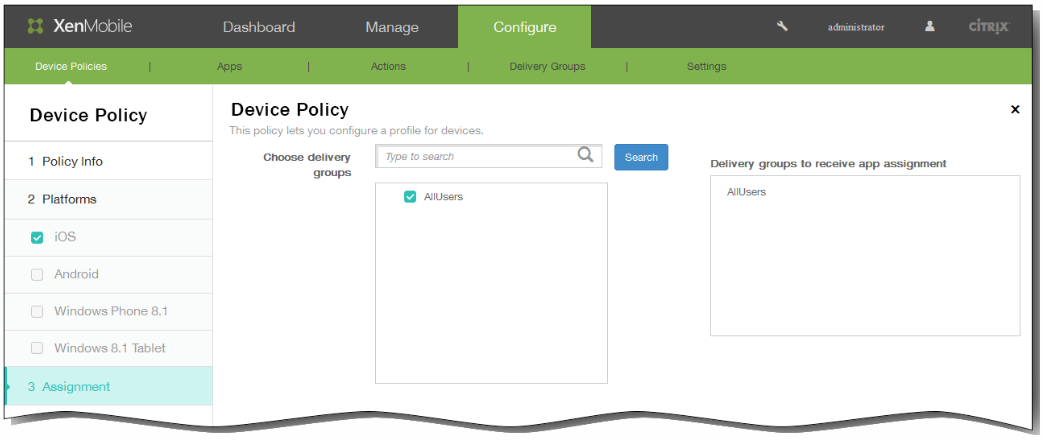


Policy Settings

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

Allow user to remove policy: Always

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.



Device Policy

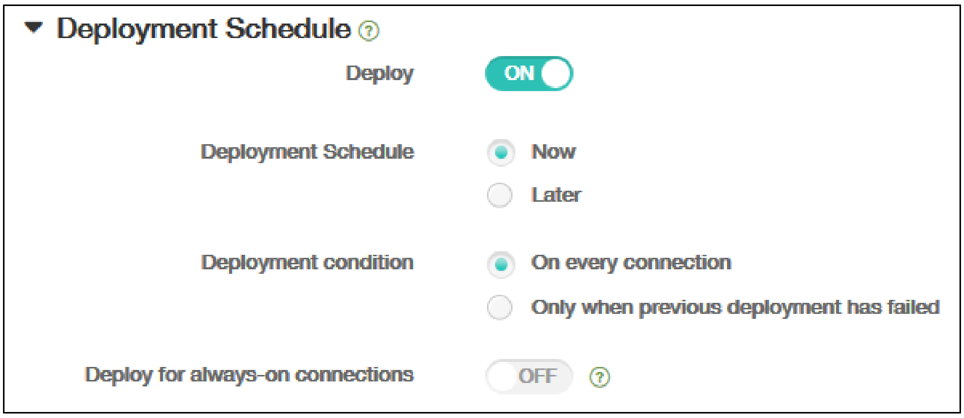
This policy lets you configure a profile for devices.

Choose delivery groups: ☑ AllUsers

Delivery groups to receive app assignment: AllUsers

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

Jun 24, 2015

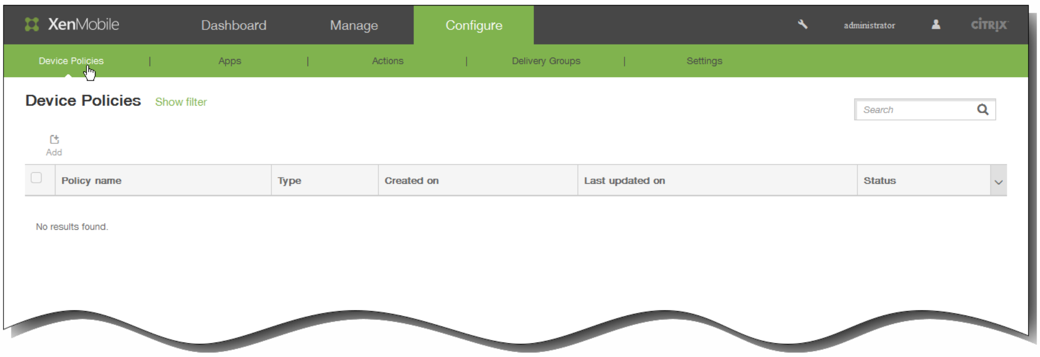
An Enterprise Hub device policy for Windows Phone 8.1 lets you distribute apps through the Enterprise Hub Company store.

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

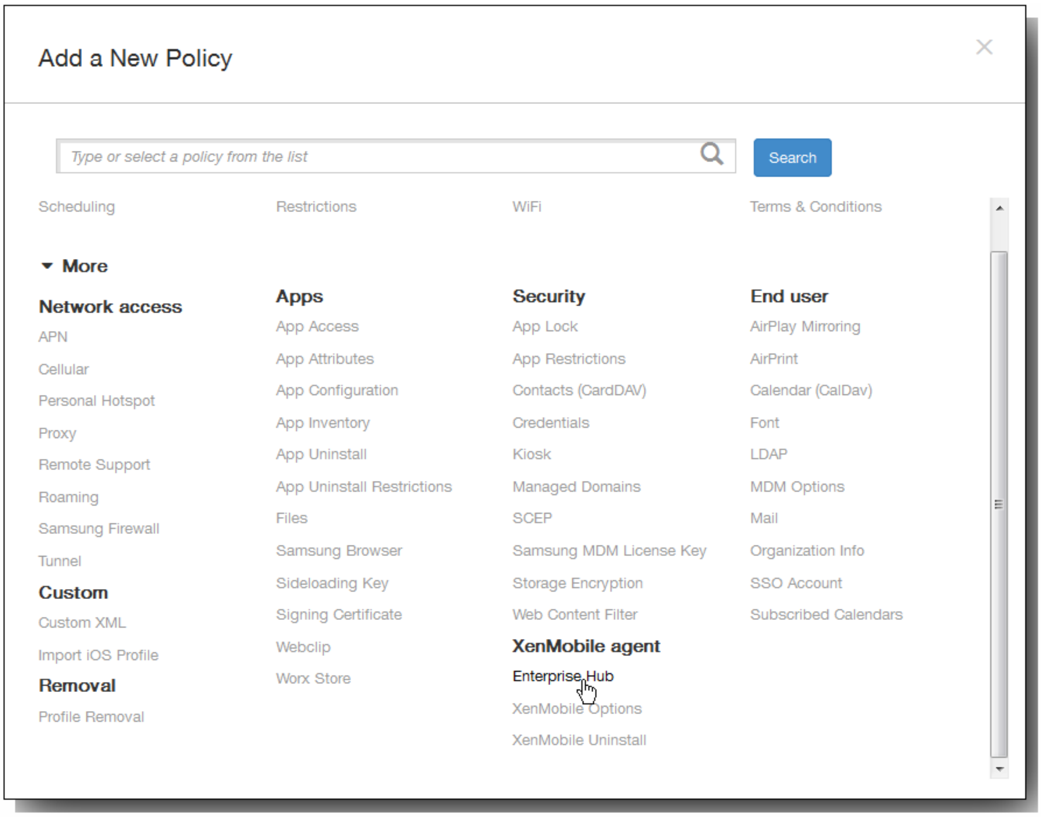
- An AET (.aetx) signing certificate from Symantec
- The Citrix Company Hub app signed by using the Microsoft app signing tool (XapSignTool.exe)

Note: XenMobile supports only one Enterprise Hub policy for one mode of Windows Phone 8.1 Worx Home. For example, to upload Windows Phone 8.1 Worx Home for XenMobile Enterprise Edition, you should not create multiple Enterprise Hub policies with different versions of Work Home for XenMobile Enterprise Edition. You can only deploy the initial Enterprise Hub policy during device enrollment.

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.



Add a New Policy

Type or select a policy from the list

Search

Scheduling Restrictions WiFi Terms & Conditions

More

Network access
- APN
- Cellular
- Personal Hotspot
- Proxy
- Remote Support
- Roaming
- Samsung Firewall
- Tunnel

Custom
- Custom XML
- Import iOS Profile

Removal
- Profile Removal

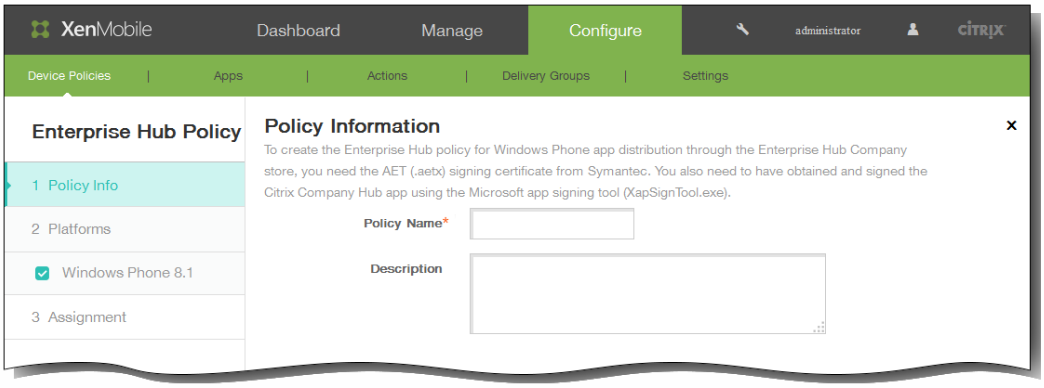
Apps
- App Access
- App Attributes
- App Configuration
- App Inventory
- App Uninstall
- App Uninstall Restrictions
- Files
- Samsung Browser
- Sideloading Key
- Signing Certificate
- Webclip
- Worx Store

Security
- App Lock
- App Restrictions
- Contacts (CardDAV)
- Credentials
- Kiosk
- Managed Domains
- SCEP
- Samsung MDM License Key
- Storage Encryption
- Web Content Filter

XenMobile agent
- Enterprise Hub
- XenMobile Options
- XenMobile Uninstall

End user
- AirPlay Mirroring
- AirPrint
- Calendar (CalDav)
- Font
- LDAP
- MDM Options
- Mail
- Organization Info
- SSO Account
- Subscribed Calendars

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



Enterprise Hub Policy

1 Policy Info

2 Platforms

☑ Windows Phone 8.1

3 Assignment

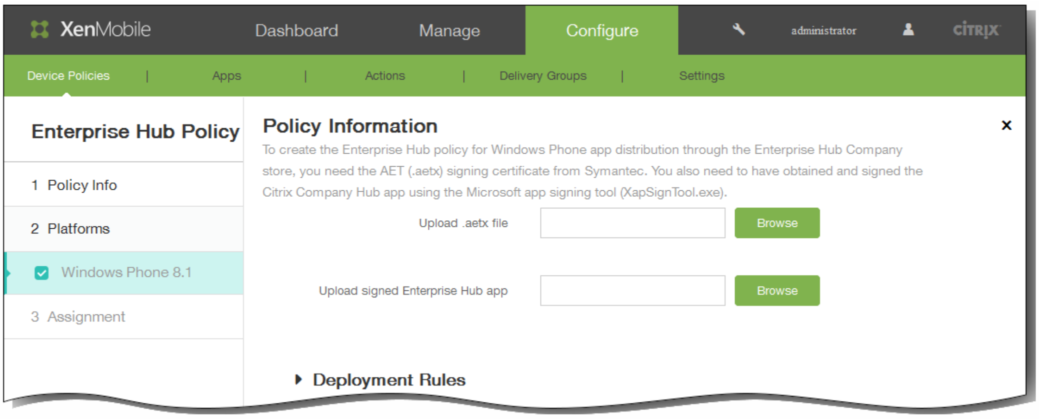
Policy Information

To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe).

Policy Name*

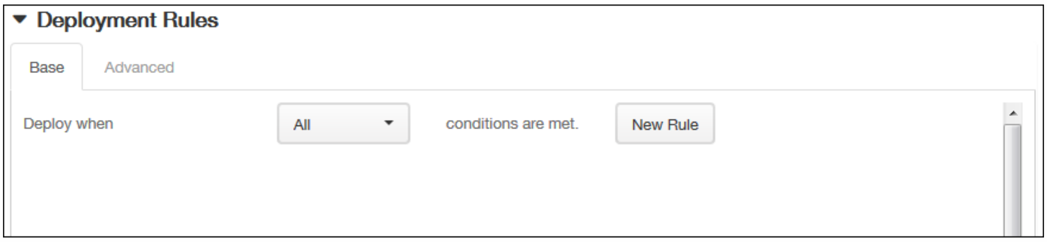
Description

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.

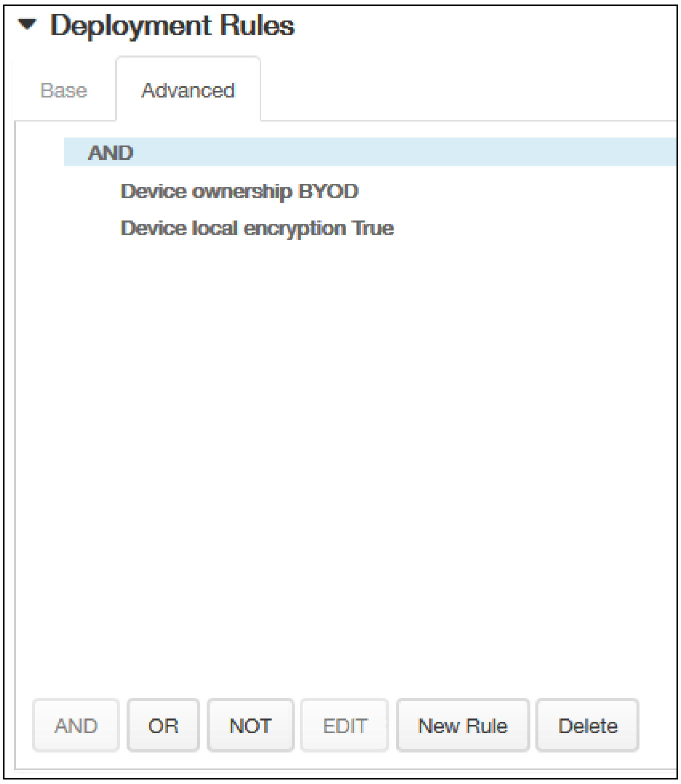


To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe).

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.



Deployment Rules

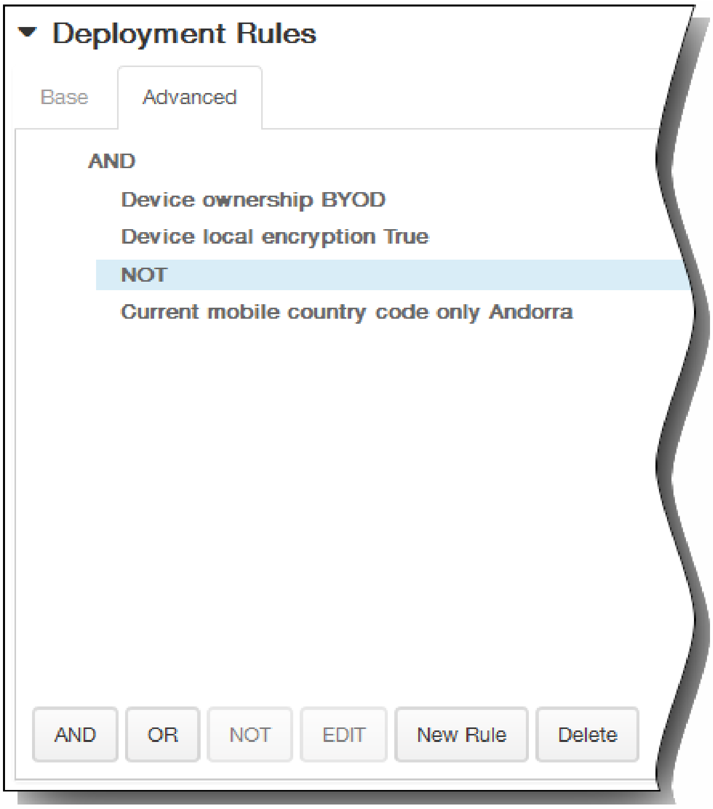
AND

Device ownership BYOD

Device local encryption True

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.



Deployment Rules

AND

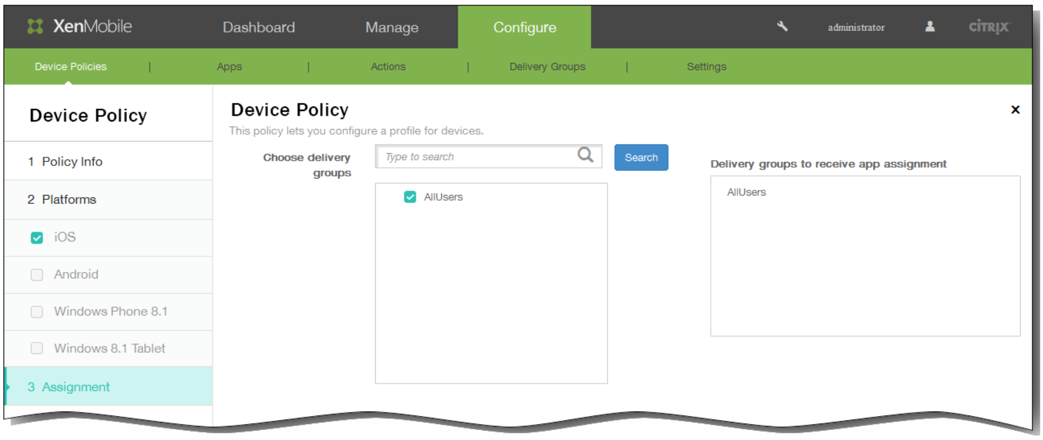
Device ownership BYOD

Device local encryption True

NOT

Current mobile country code 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.



Device Policy

This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

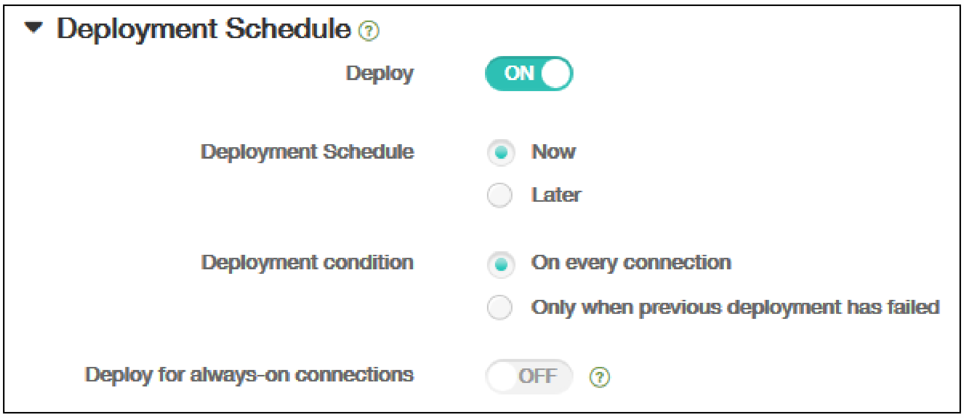
AllUsers

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.



▾ 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

11. Click Save to save the policy.

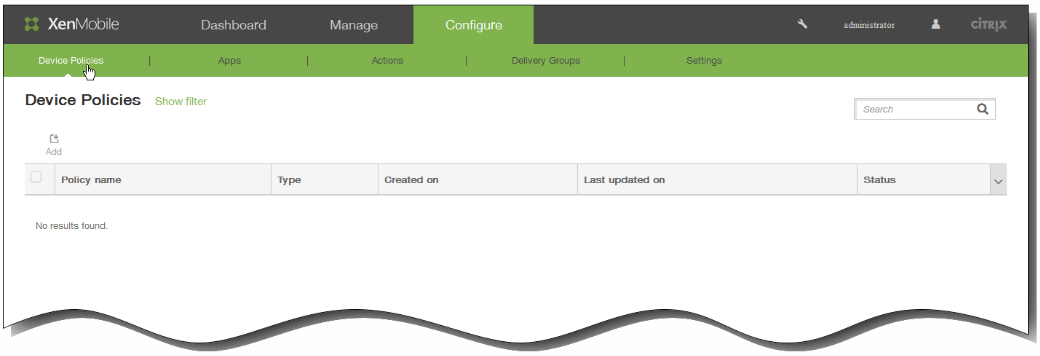
Microsoft Exchange ActiveSync device policies

Jun 23, 2015

You can use the Exchange ActiveSync device policy to configure an email client on users' devices to let them access their corporate email hosted on Exchange. You can create policies for iOS, Android HTC, Android TouchDown, Android for Work, 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.

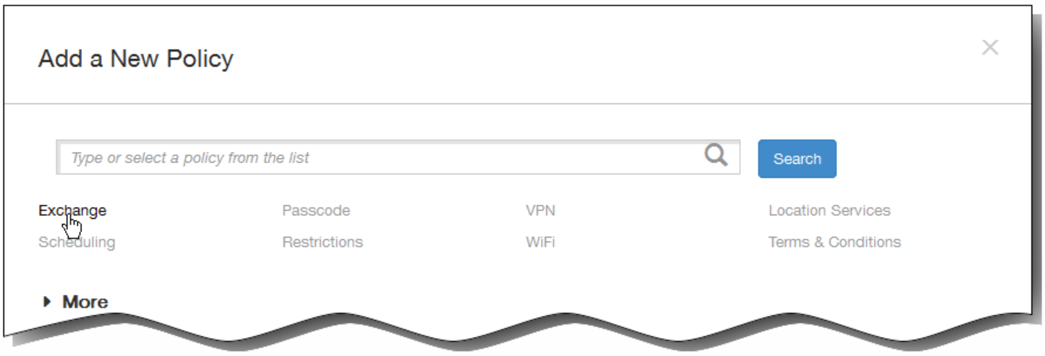
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



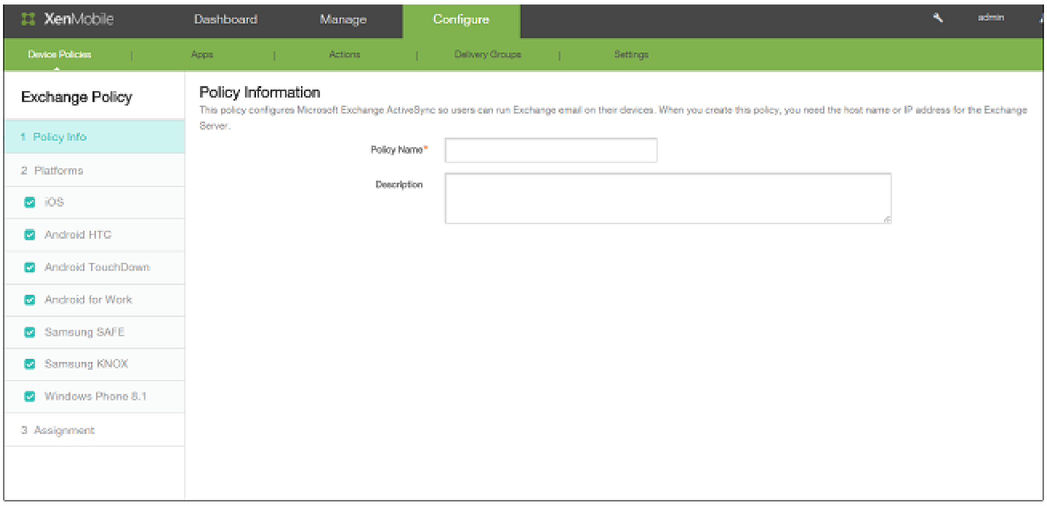
□	Policy name	Type	Created on	Last updated on	Status

No results found.

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



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



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

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:

      Exchange ActiveSync account name: Type any Exchange Server account name.

      Exchange ActiveSync host name: Type the Exchange Server host name or IP address.

      Use SSL: Select whether to secure connections between users' devices and the Exchange Server. The default is On.

      Domain: Enter the domain in which the Exchange Server resides.
      Note: You can use the system macro **${user.domainname}** in this field to automatically look up users' domain names.

      User: Specify the user name for the Exchange user account.
      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.

      Password: Enter an optional password for the Exchange user account.

      Email sync interval: Select any sync interval value from dropdown box.

      Identity credential (keystore or PKI credential): Optional. Select configured Cert/PKI credential from dropdown box.

      Authorize email move between accounts: Optional. Select On/Off. The default is Off.

      Send email only from email app: Optional. Select On/Off. The default is Off.

Disable email recent syncing: Optional. Select On/Off. The default is Off.

Enable S/MIME: Optional. Select On/Off. The default is Off.

Enable per message S/MIME switch: Optional. Select On/Off. The default is Off.

- If you selected Android HTC, 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 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. Default is 'None'.

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

  Policy: Optionally, add TouchDown policies for this policy.

- If you selected **Android for Work**, 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. Can be added in doc default is 'None'.

- 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. The default is 'None'.

  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.
  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.

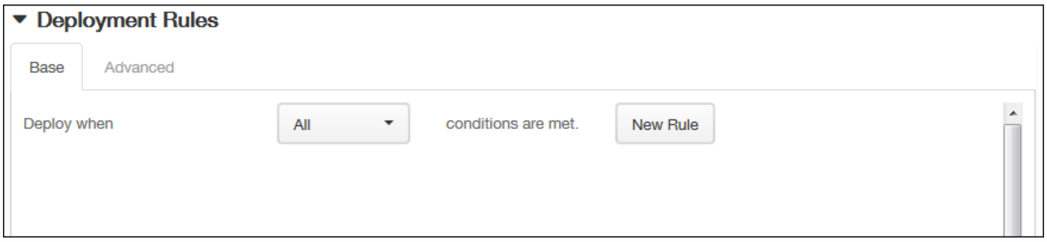
Domain: Enter the domain in which the Exchange Server resides.
Note: You can use the system macro ${user.domainname} in this field to automatically look up users' domain names.
User ID or user name: Specify the user name for the Exchange user account.
Note: You can use the system macro ${user.username} 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.

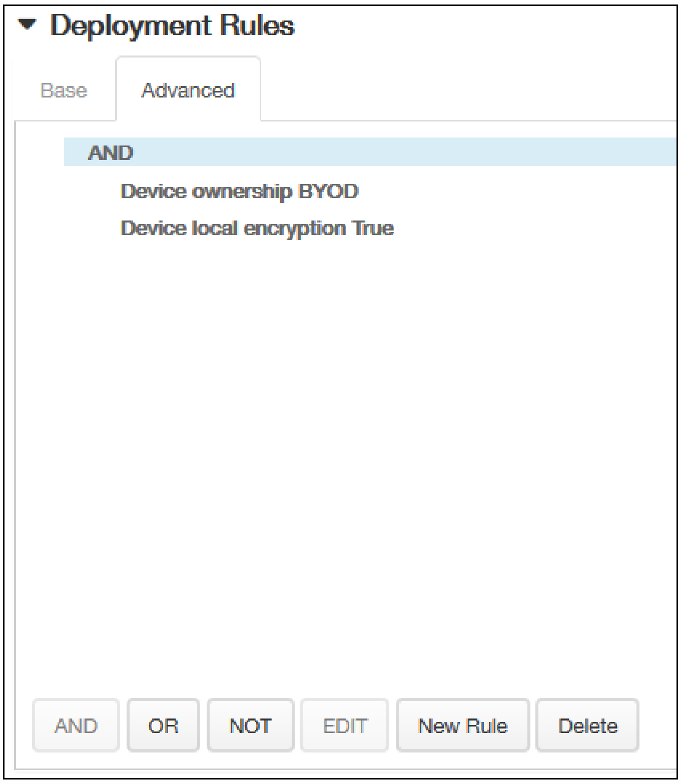
Frequency: In the list, click the schedule to use when syncing data that is sent to the device from the Exchange Server.

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.



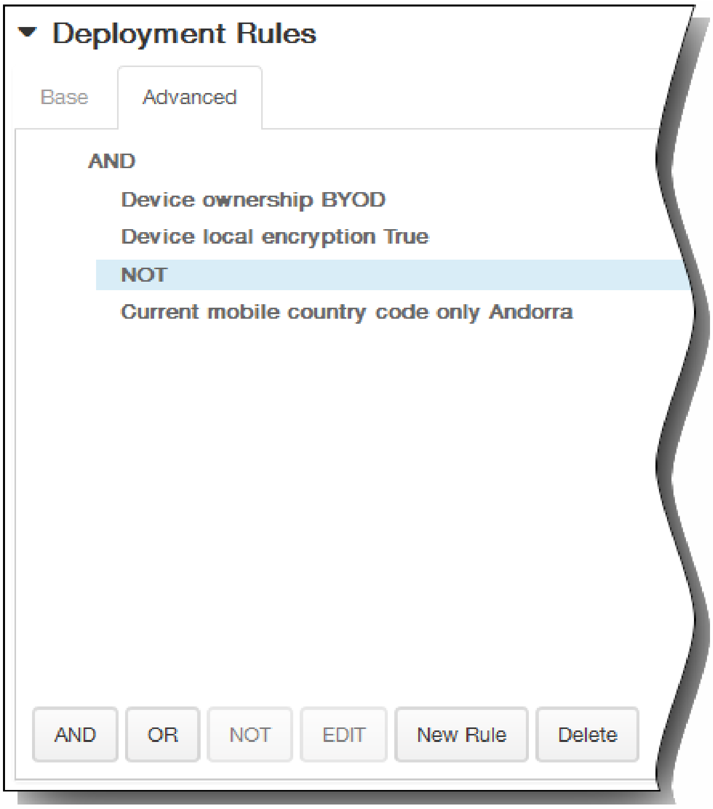
AND

Device ownership BYOD

Device local encryption True

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.



Deployment Rules

AND

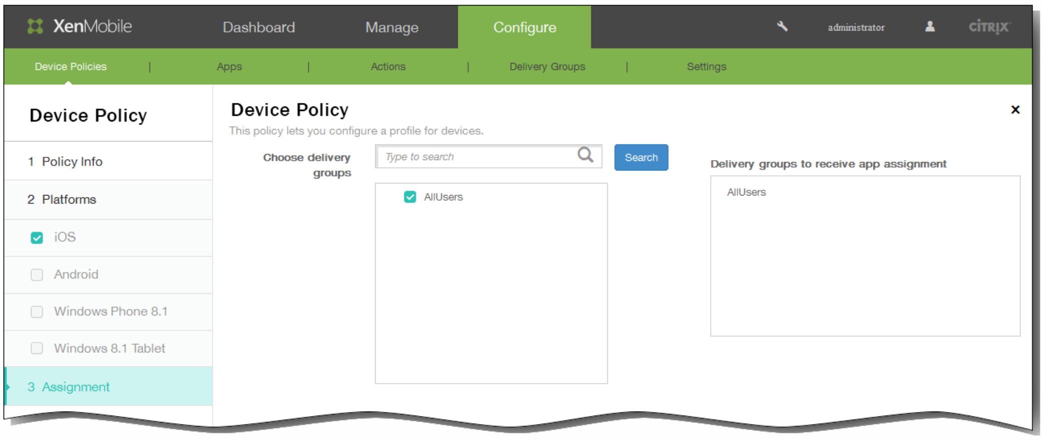
Device ownership BYOD

Device local encryption True

NOT

Current mobile country code 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.



Device Policy

This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

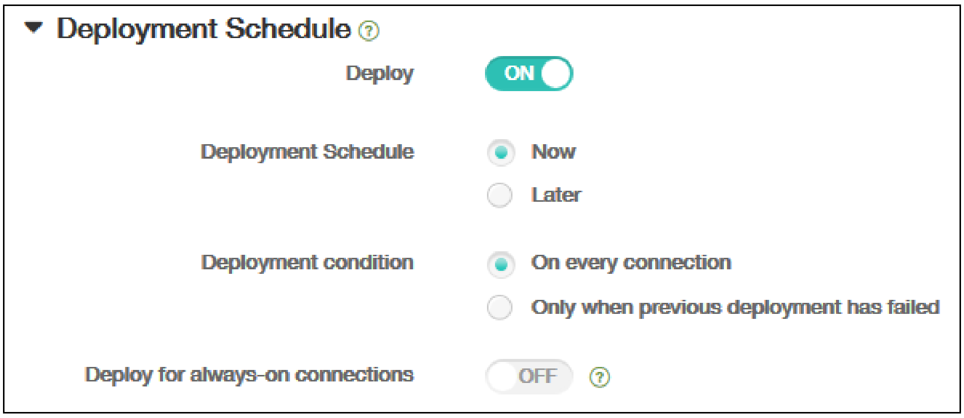
Delivery groups to receive app assignment

AllUsers

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.



▼ 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

11. Click Save.

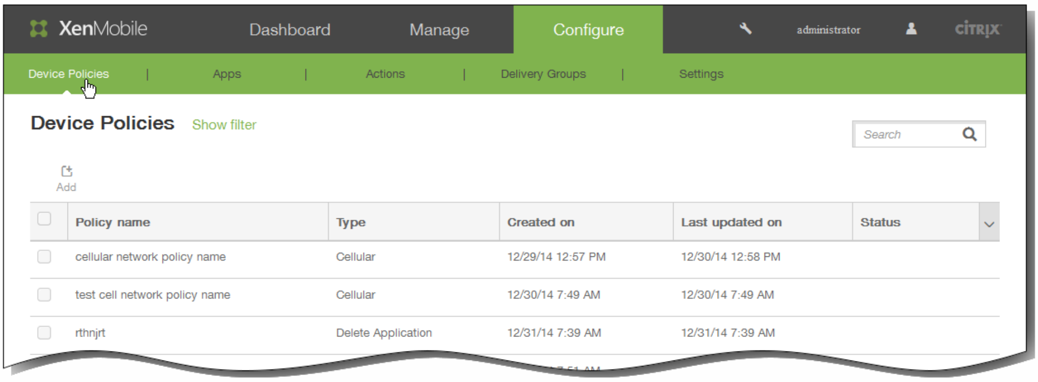
Location device policies

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.

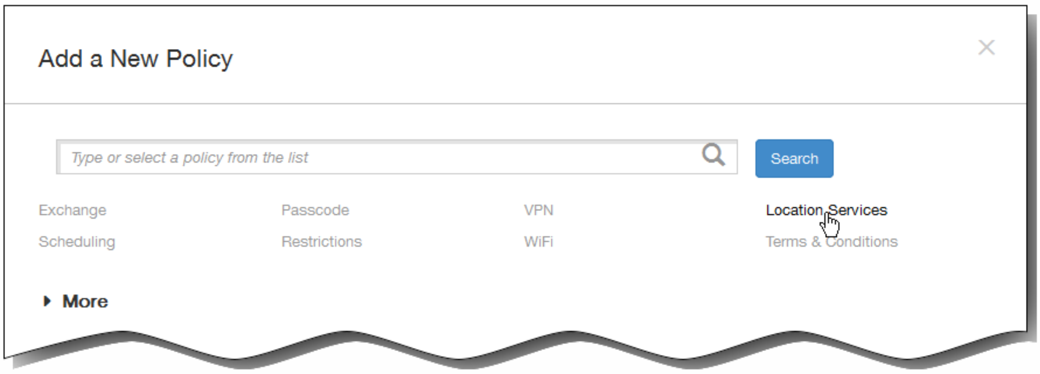
You can create location device policies for iOS and Android. Each platform requires a different set of values, which are described in this article.

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

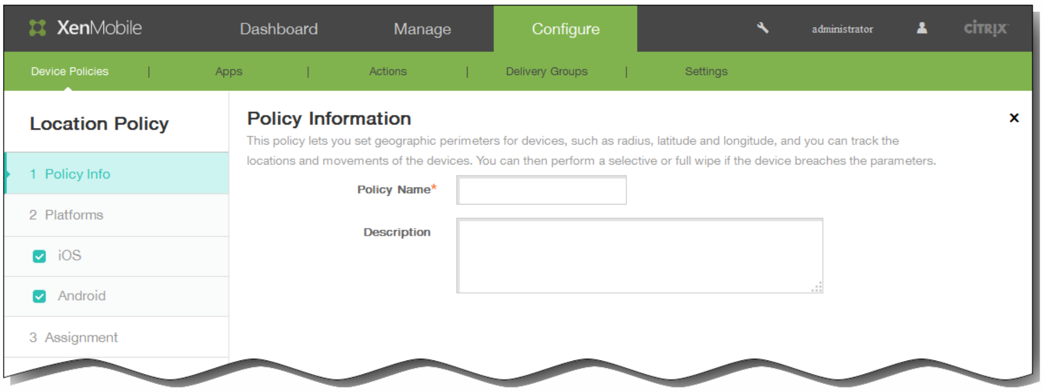


□	Policy name	Type	Created on	Last updated on	Status
□	cellular network policy name	Cellular	12/29/14 12:57 PM	12/30/14 12:58 PM	
□	test cell network policy name	Cellular	12/30/14 7:49 AM	12/30/14 7:49 AM	
□	rthnjrt	Delete Application	12/31/14 7:39 AM	12/31/14 7:39 AM	

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.



Policy Information

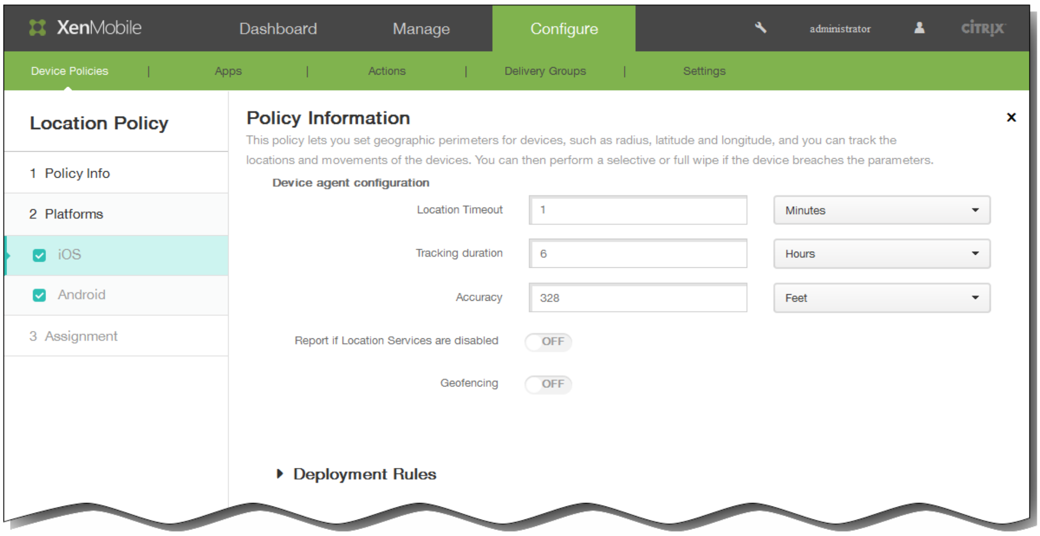
This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.

Policy Name*

Description

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.



Policy Information

This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.

Device agent configuration

Location Timeout: 1 Minutes

Tracking duration: 6 Hours

Accuracy: 328 Feet

Report if Location Services are disabled: OFF

Geofencing: OFF

6. Under Platforms, select the platforms you want to add.
    - If you selected iOS, configure the following settings:

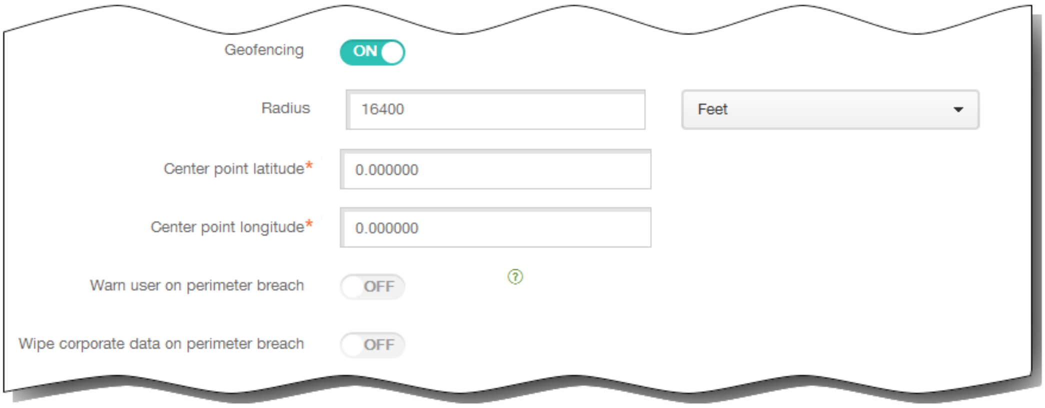
      Location timeout: Type a numeral and then, in the list, click Seconds or Minutes to set how often XenMobile attempts to fix the device's location. Valid values are 60–900 seconds or 1–15 minutes. The default is 1 minute.

      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:



Geofencing ON

Radius 16400 Feet

Center point latitude* 0.000000

Center point longitude* 0.000000

Warn user on perimeter breach OFF

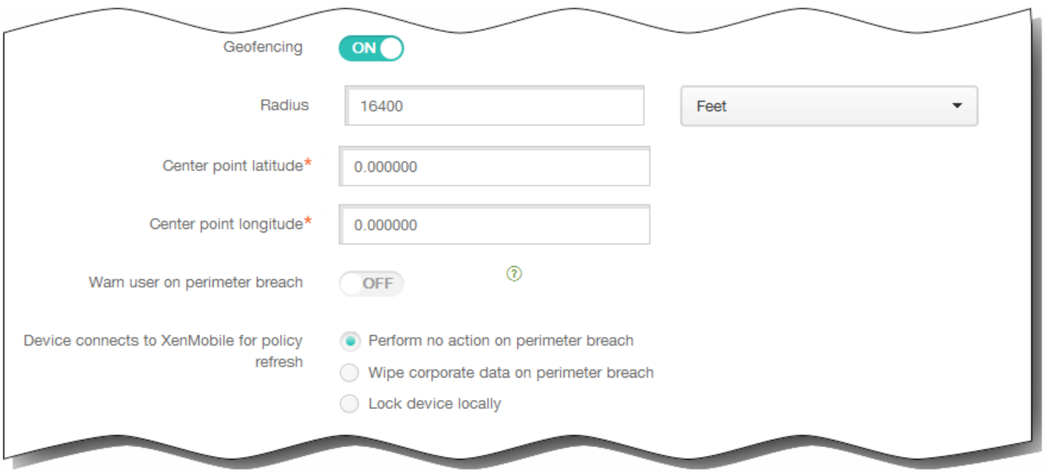
Wipe corporate data on perimeter breach OFF

- 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 that 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:



Geofencing: ON

Radius: 16400 Feet

Center point latitude*: 0.000000

Center point longitude*: 0.000000

Warn user on perimeter breach: OFF

Device connects to XenMobile for policy refresh:
- ● Perform no action on perimeter breach
- ○ Wipe corporate data on perimeter breach
- ○ Lock device locally

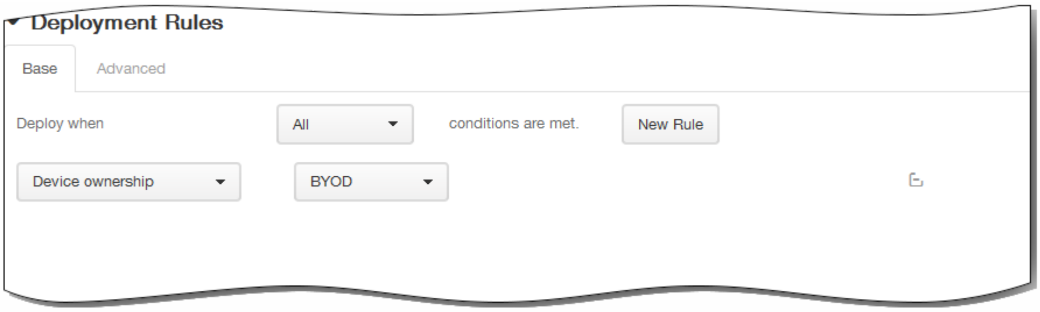
- Radius: Type a numeral and then, in the list, click the units to be used to measure the radius. The default is 16,400 feet.
  Valid values for radius are:
  - 164–164000 feet
  - 1–50 kilometers
  - 50–50000 meters
  - 54–54680 yards
  - 1–31 miles
- Center point latitude: Type a latitude, such as 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.

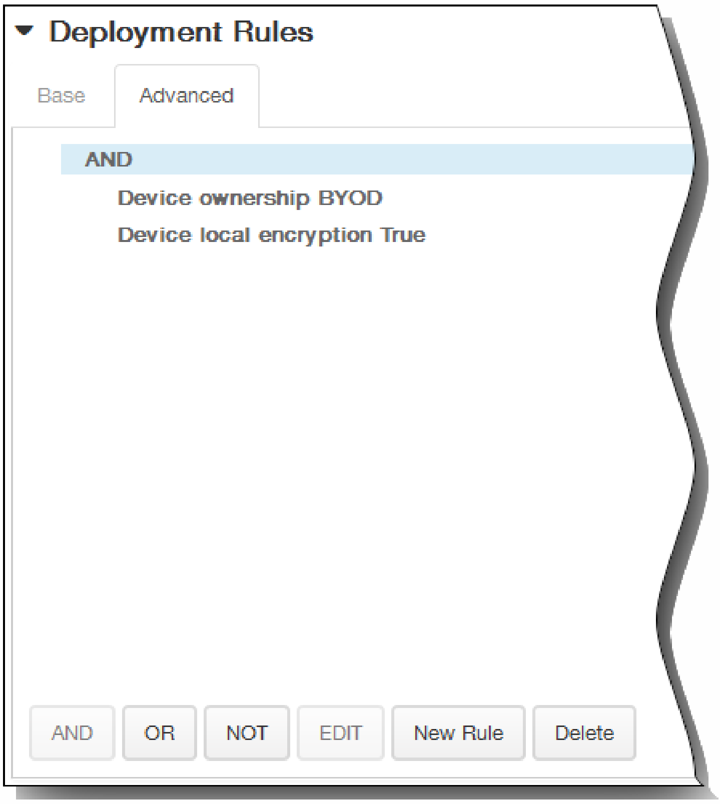
  - Delay on lock: Lock users' devices after a specified length of time.
    When you enable this option, the Delay on lock field appears.

    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.



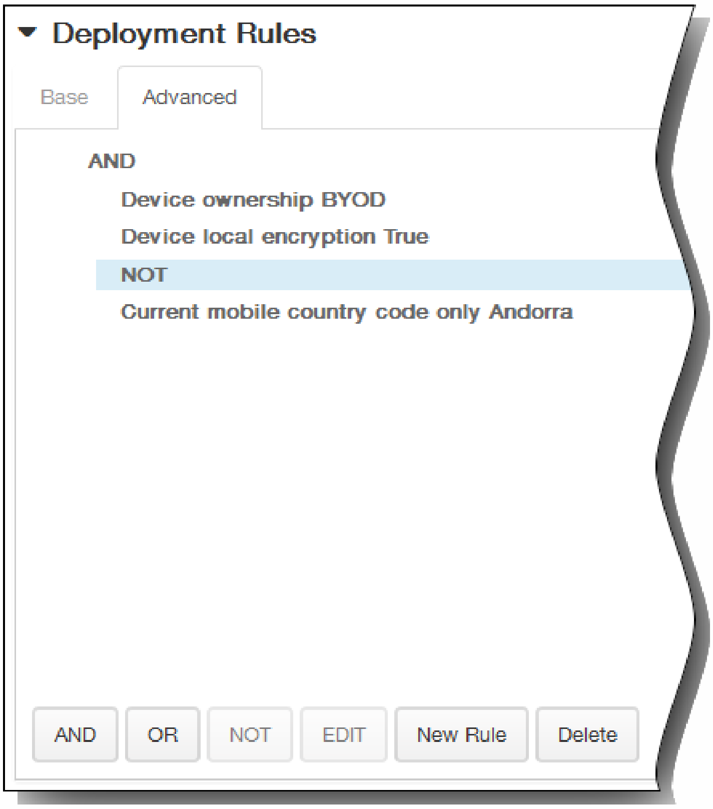
1. In the lists, click options to determine when the policy should be deployed.
   1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
   2. Click New Rule to define the conditions.
   3. In the lists, click the conditions, such 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.



Deployment Rules

Base | Advanced

AND

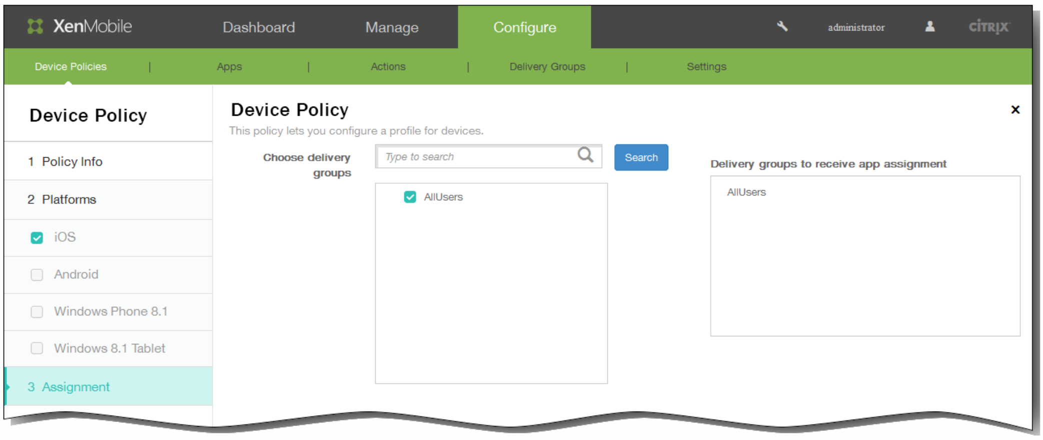
Device ownership BYOD

Device local encryption True

NOT

Current mobile country code 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.



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

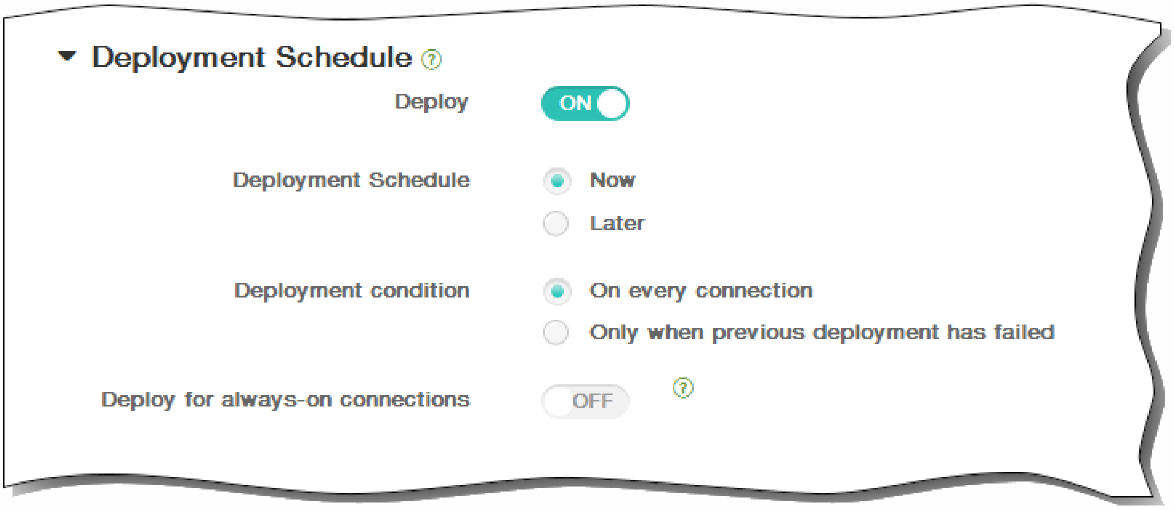
Delivery groups to receive app assignment

AllUsers

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.



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

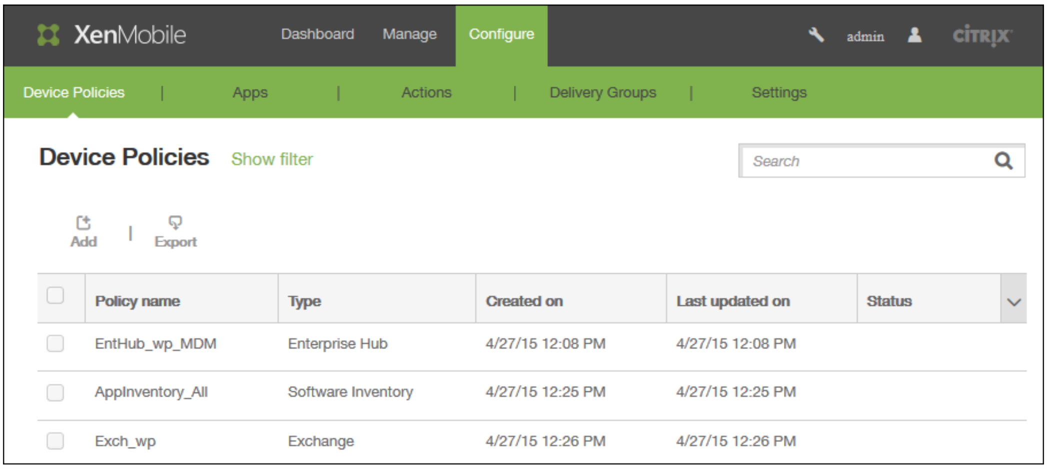
11. Click Save to save the policy.

Connection scheduling device policies

Jun 23, 2015

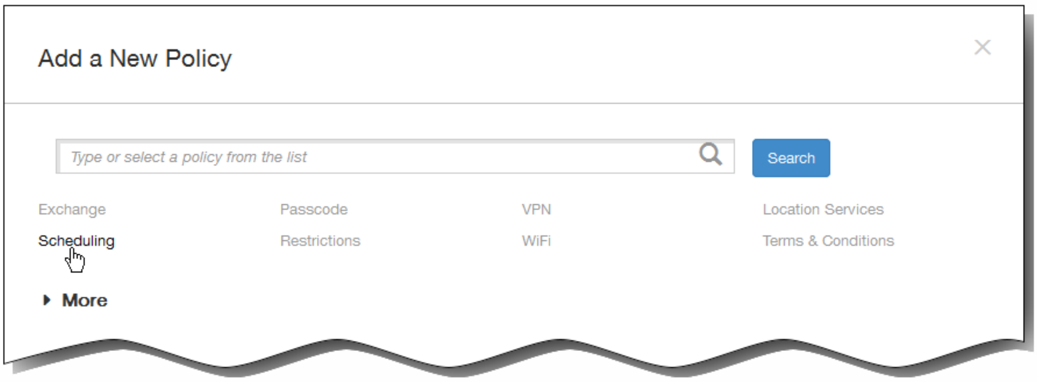
You create connection scheduling policies to control how and when users' Android and Symbian devices connect to XenMobile. You can specify that users connect their devices manually, that devices stay connected permanently, or that devices connect within a defined time frame.

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



	Policy name	Type	Created on	Last updated on	Status
□	EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
□	AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
□	Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	

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.

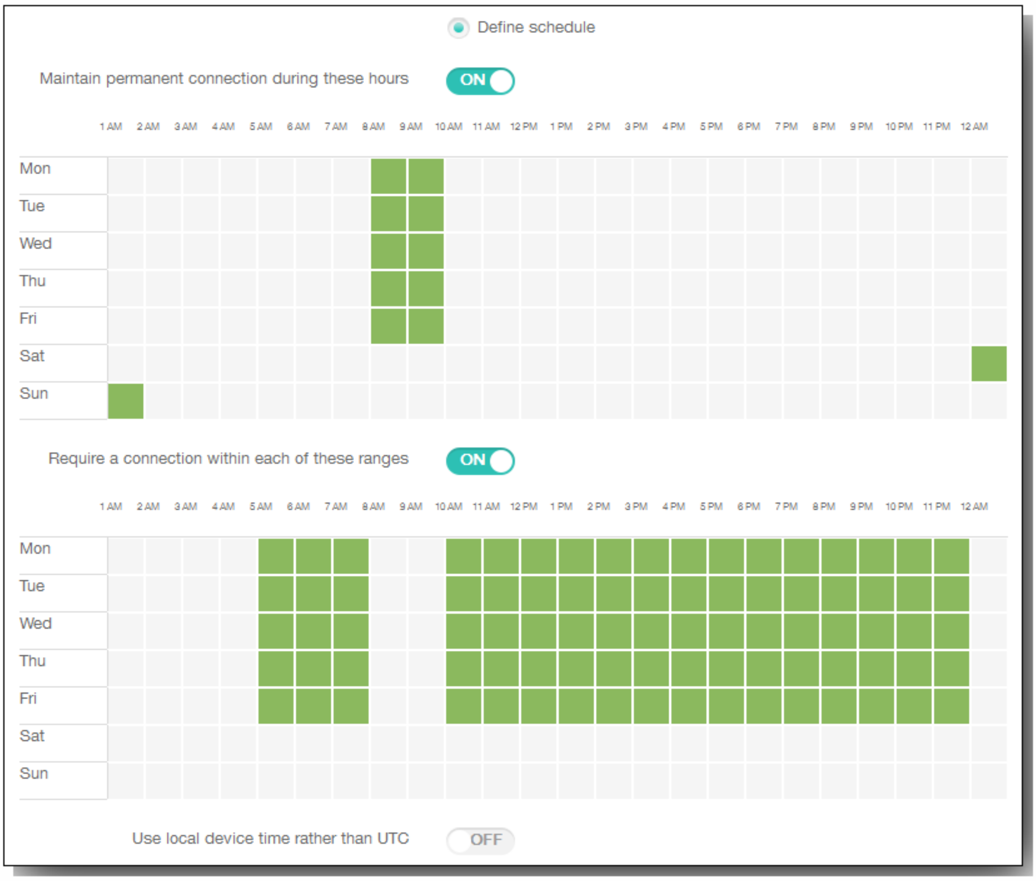
   Note: When the Policy Platforms page appears, both platforms are selected and you see the Android platform configuration panel first.
6. Under Platforms, select the platforms you want to add.
7. Configure the following settings for each of the platforms you selected: Require devices to connect: Click 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.



○ Define schedule

Maintain permanent connection during these hours ON

	1 AM	2 AM	3 AM	4 AM	5 AM	6 AM	7 AM	8 AM	9 AM	10 AM	11 AM	12 PM	1 PM	2 PM	3 PM	4 PM	5 PM	6 PM	7 PM	8 PM	9 PM	10 PM	11 PM	12 AM
Mon								🟩	🟩															
Tue								🟩	🟩															
Wed								🟩	🟩															
Thu								🟩	🟩															
Fri								🟩	🟩															
Sat																								🟩
Sun	🟩																							

Require a connection within each of these ranges ON

	1 AM	2 AM	3 AM	4 AM	5 AM	6 AM	7 AM	8 AM	9 AM	10 AM	11 AM	12 PM	1 PM	2 PM	3 PM	4 PM	5 PM	6 PM	7 PM	8 PM	9 PM	10 PM	11 PM	12 AM
Mon					🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Tue					🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Wed					🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Thu					🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Fri					🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Sat																								
Sun																								

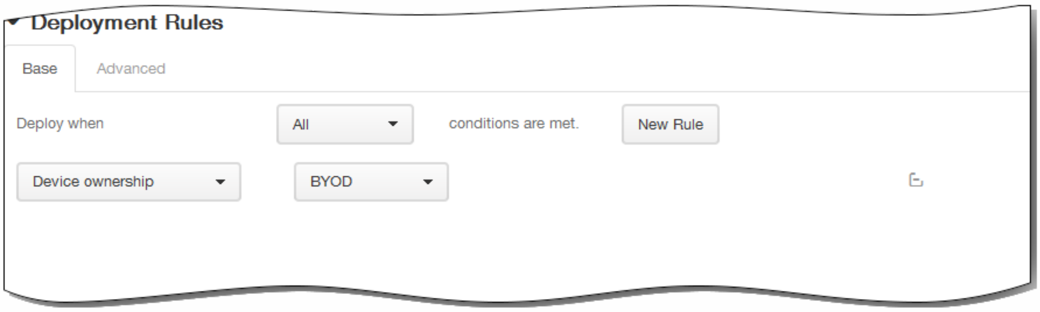
Use local device time rather than UTC OFF

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.



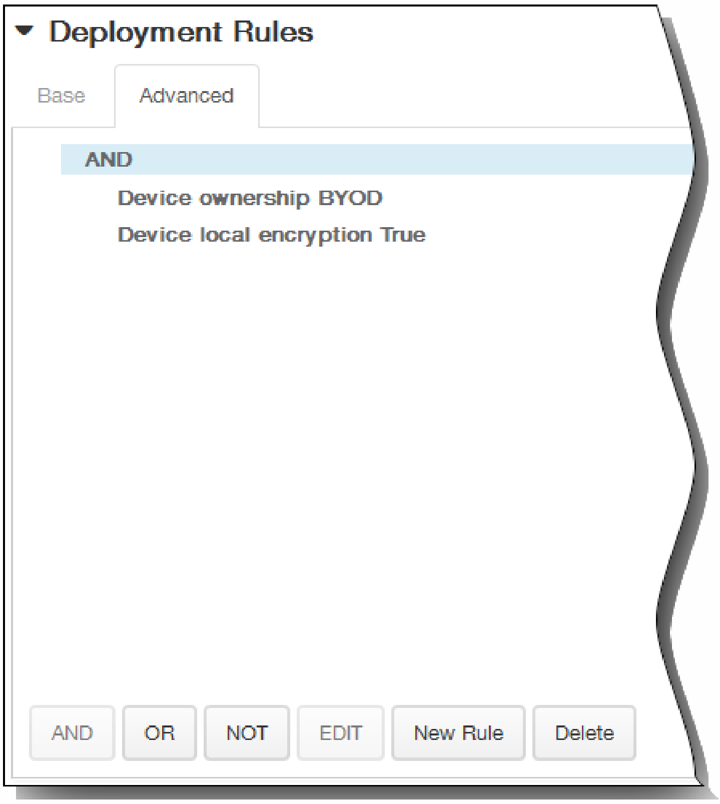
Deployment Rules

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.

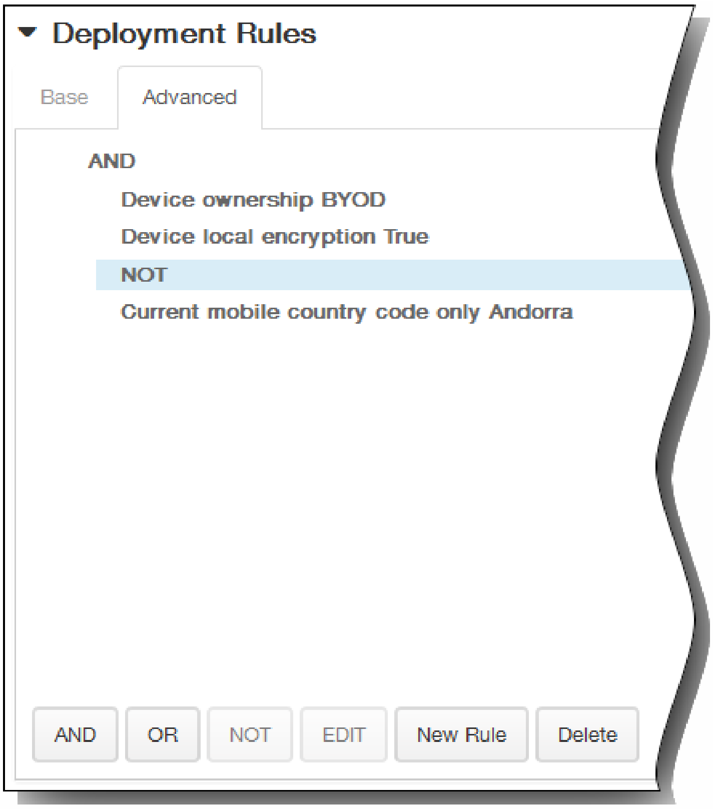
   3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
   4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



AND
Device ownership BYOD
Device local encryption True

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.



AND

Device ownership BYOD

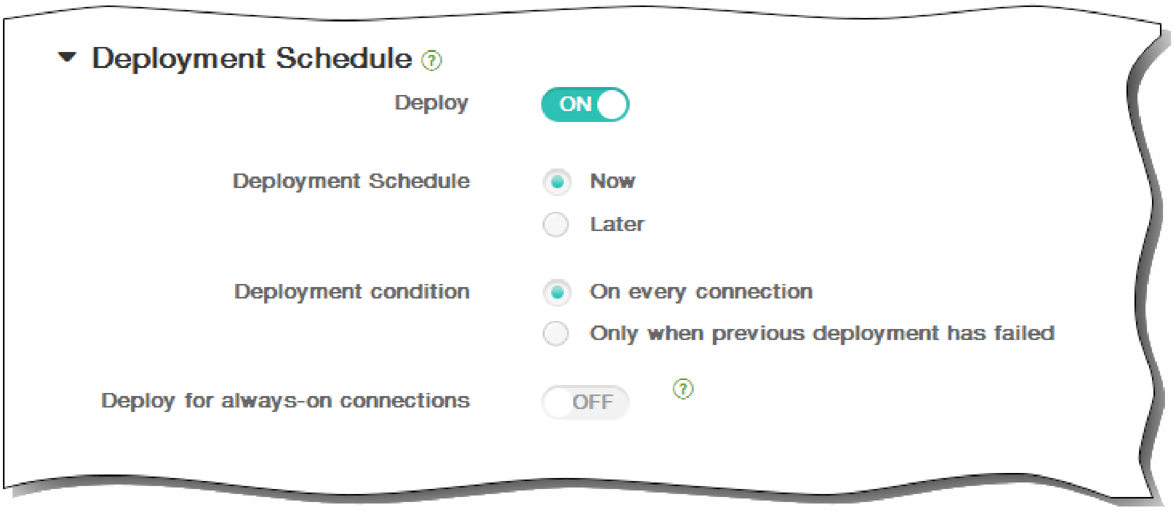
Device local encryption True

NOT

Current mobile country code 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.



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

12. Click Save to save the policy.

To add an AirPlay mirroring device policy for iOS

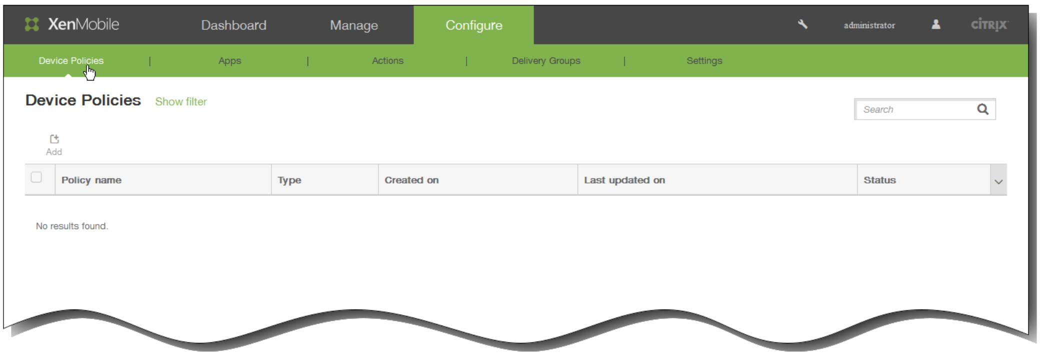
Apr 24, 2015

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.

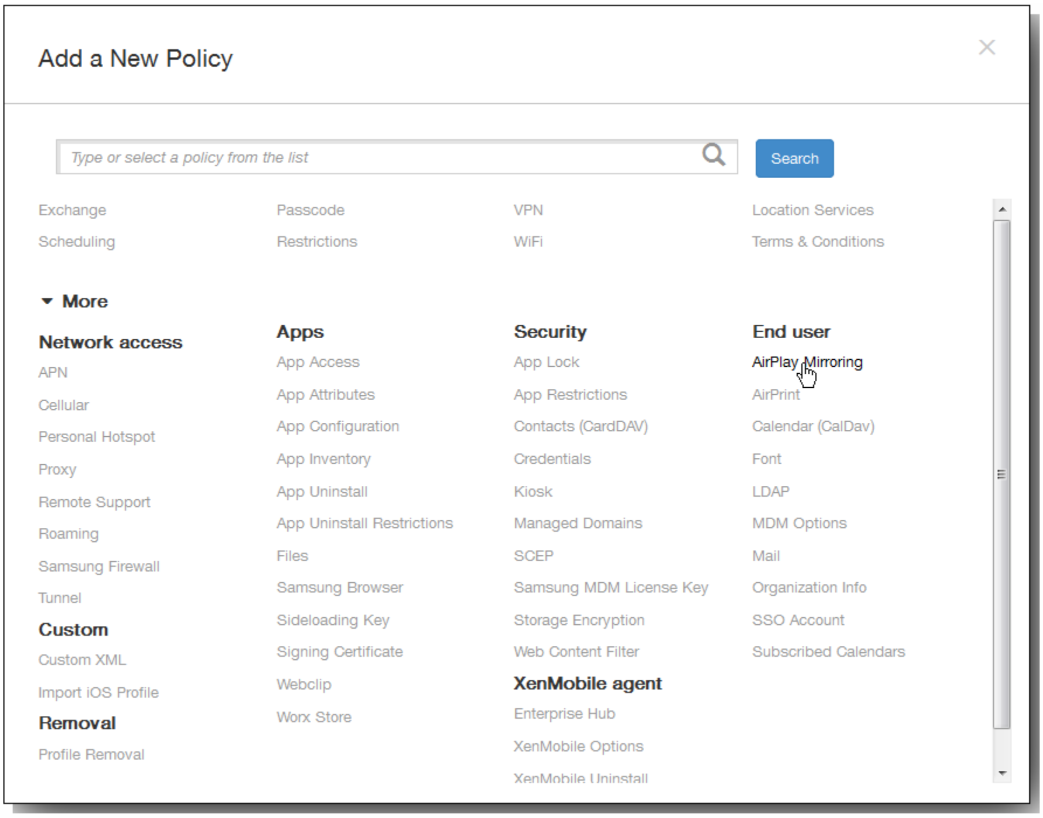
You can add a device policy in XenMobile to add specific AirPlay devices (such as Apple TV or another Mac computer) to users' iOS devices. You also have the option of adding devices to a whitelist for supervised devices, which limits users to only the AirPlay devices on the whitelist. For information 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.

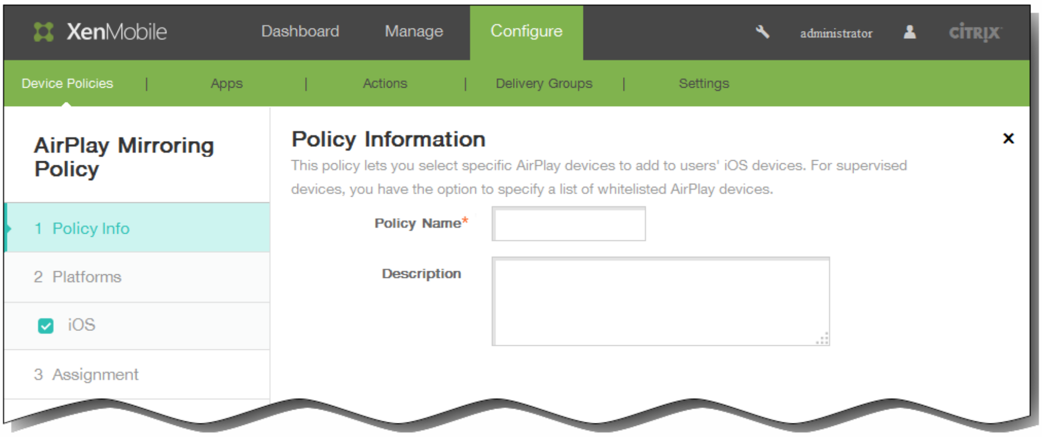
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears.



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.



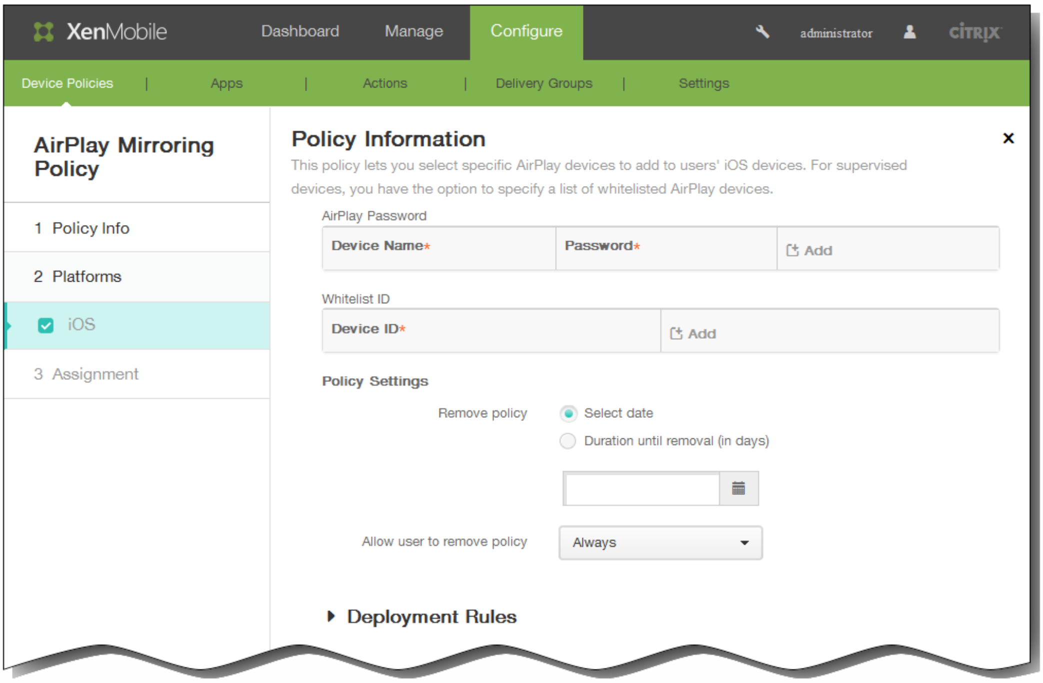
Policy Information

This policy lets you select specific AirPlay devices to add to users' iOS devices. For supervised devices, you have the option to specify a list of whitelisted AirPlay devices.

Policy Name*

Description

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.

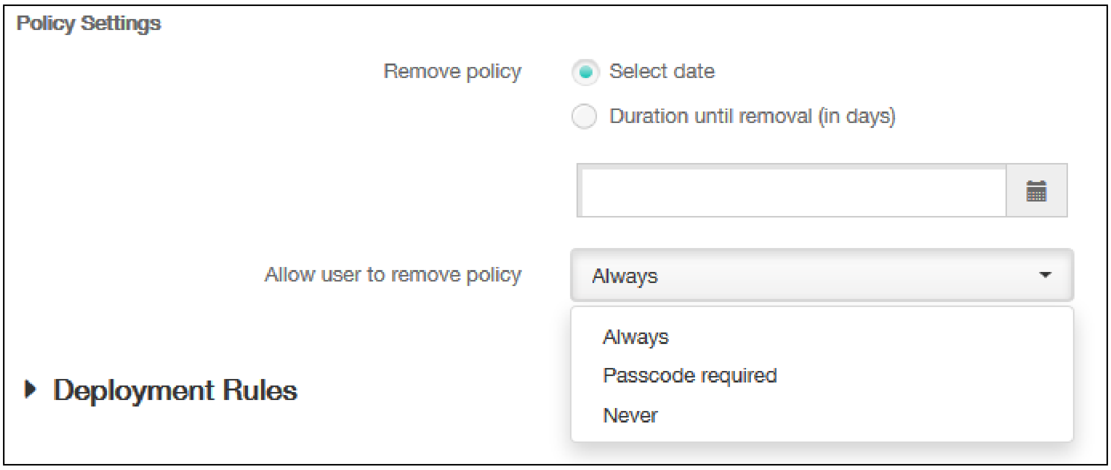


This policy lets you select specific AirPlay devices to add to users' iOS devices. For supervised devices, you have the option to specify a list of whitelisted AirPlay devices.

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.

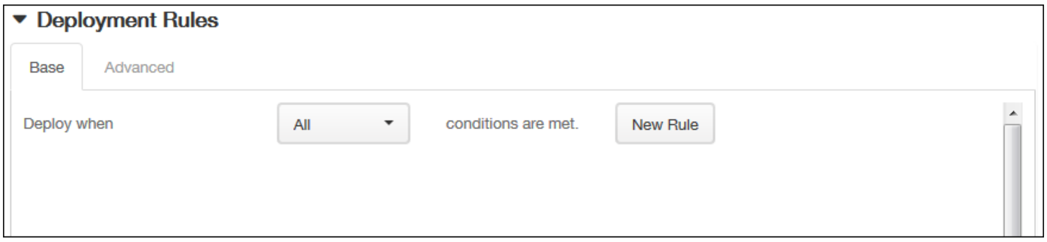


Policy Settings

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

Allow user to remove policy: Always

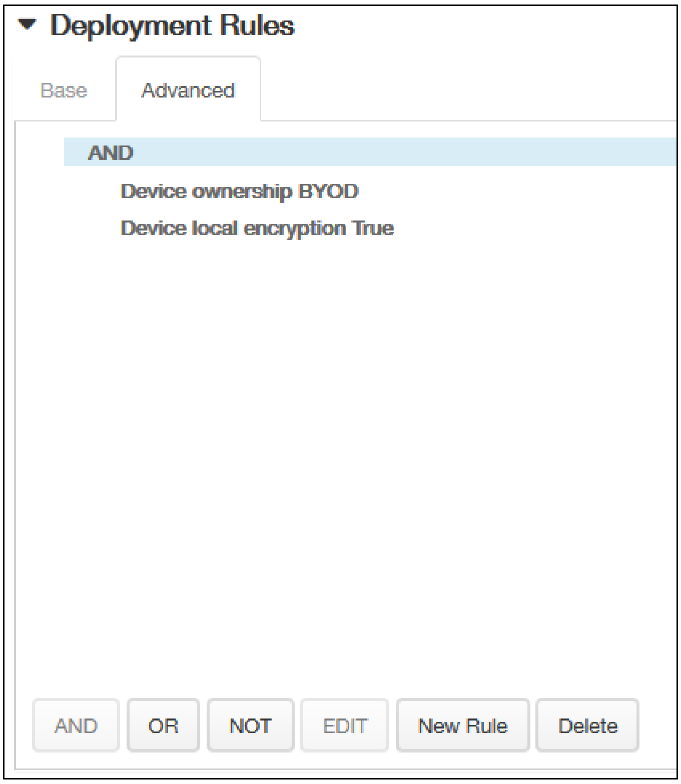
11. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.



Deployment Rules

Deploy when All conditions are met.

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.



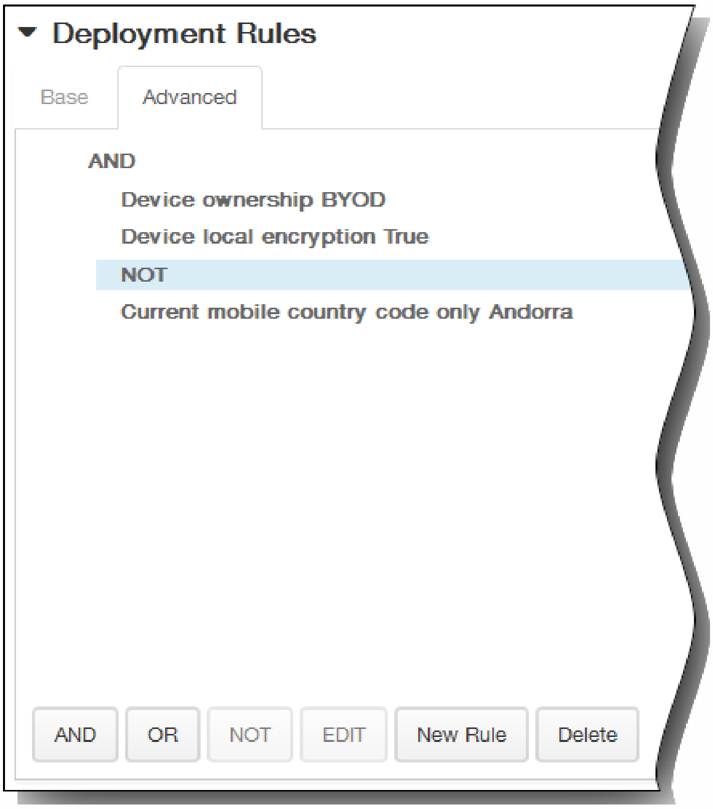
Device ownership BYOD

Device local encryption True

The conditions you chose on the Base tab appear.

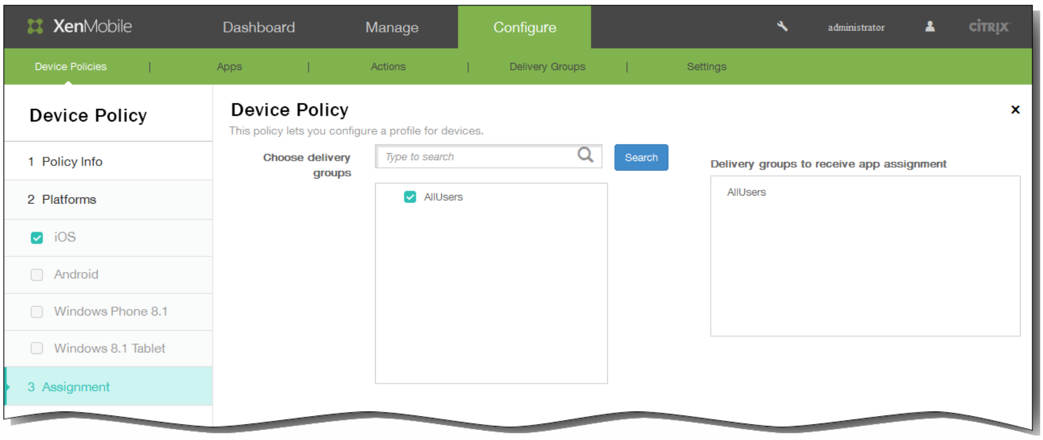
3. You can use more advanced Boolean logic to combine, edit, or add rules.
   1. Click AND, OR, or NOT.
   2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
      At any time, you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



AND
Device ownership BYOD
Device local encryption True
NOT
Current mobile country code 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.



Device Policy

This policy lets you configure a profile for devices.

☑ iOS
□ Android
□ Windows Phone 8.1
□ Windows 8.1 Tablet

Choose delivery groups

☑ AllUsers

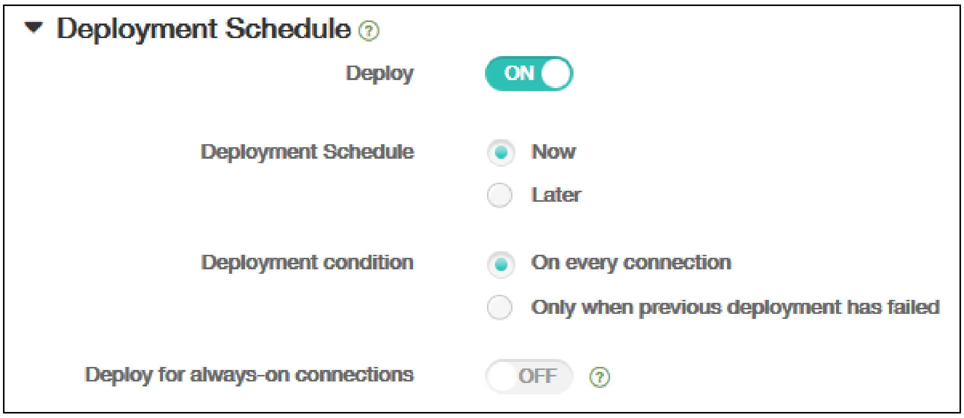
Delivery groups to receive app assignment

AllUsers

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.



Deployment Schedule

Deploy: ON

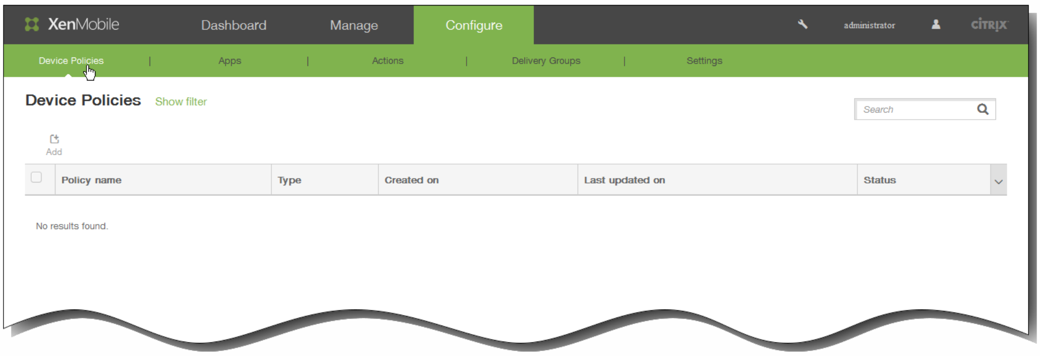
Deployment Schedule: ● Now ○ Later

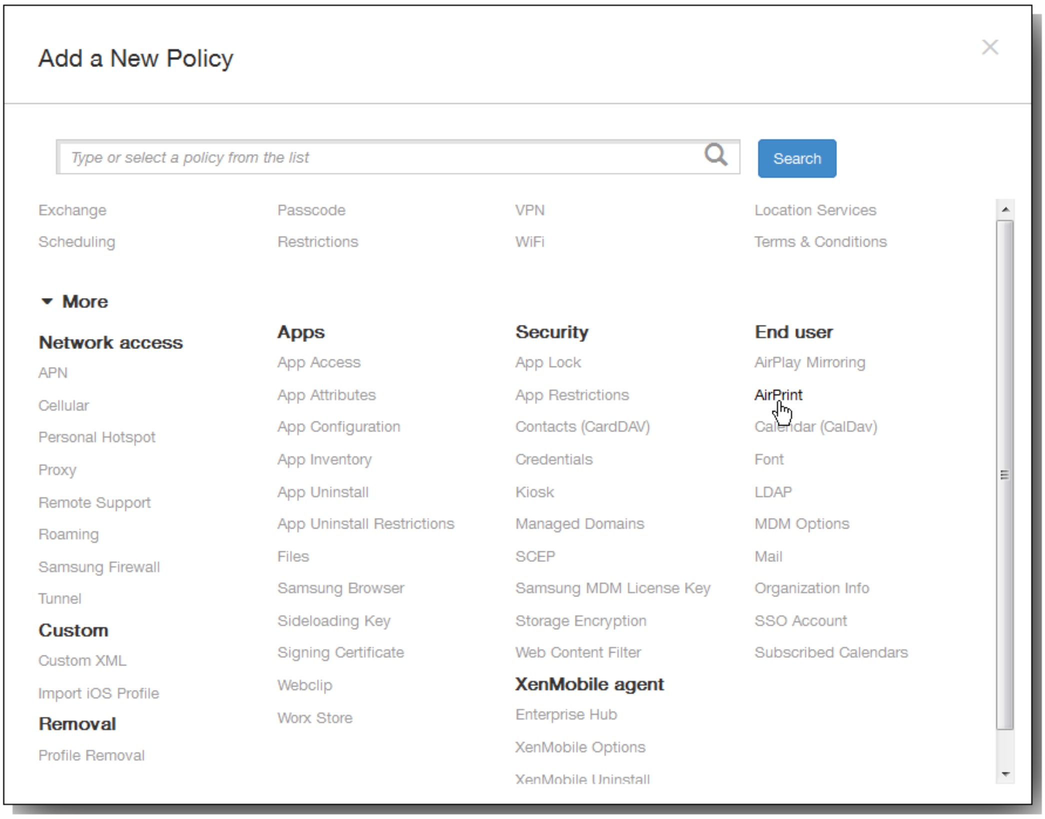
Deployment condition: ● On every connection ○ Only when previous deployment has failed

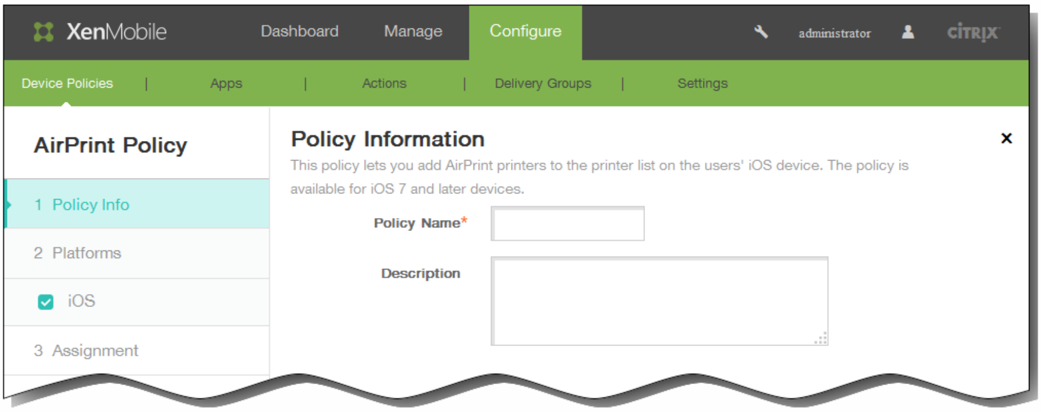
Deploy for always-on connections: OFF

15. Click Save to save the policy.

-
-


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies
Apps
Actions
Delivery Groups
Settings
Device Policies
Show filter
Search
Add
Policy name
Type
Created on
Last updated on
Status
No results found.


Add a New Policy
Type or select a policy from the list
Search
Exchange
Scheduling
Passcode
Restrictions
VPN
WiFi
Location Services
Terms & Conditions
More
Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel
Custom
Custom XML
Import iOS Profile
Removal
Profile Removal
Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store
Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter
XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall
End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars

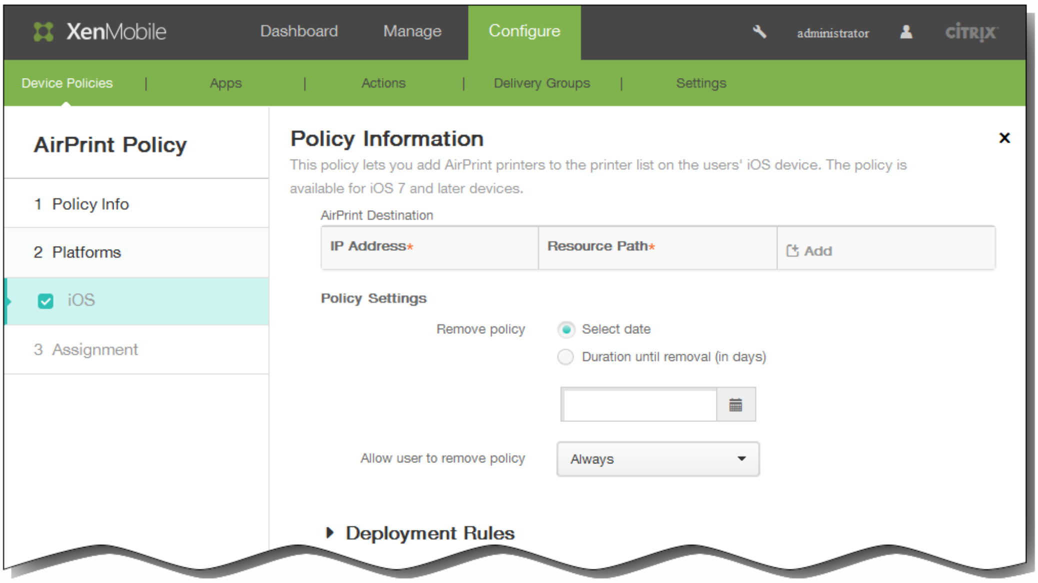


Policy Information

This policy lets you add AirPrint printers to the printer list on the users' iOS device. The policy is available for iOS 7 and later devices.

Policy Name*

Description



Policy Information

This policy lets you add AirPrint printers to the printer list on the users' iOS device. The policy is available for iOS 7 and later devices.

AirPrint Destination

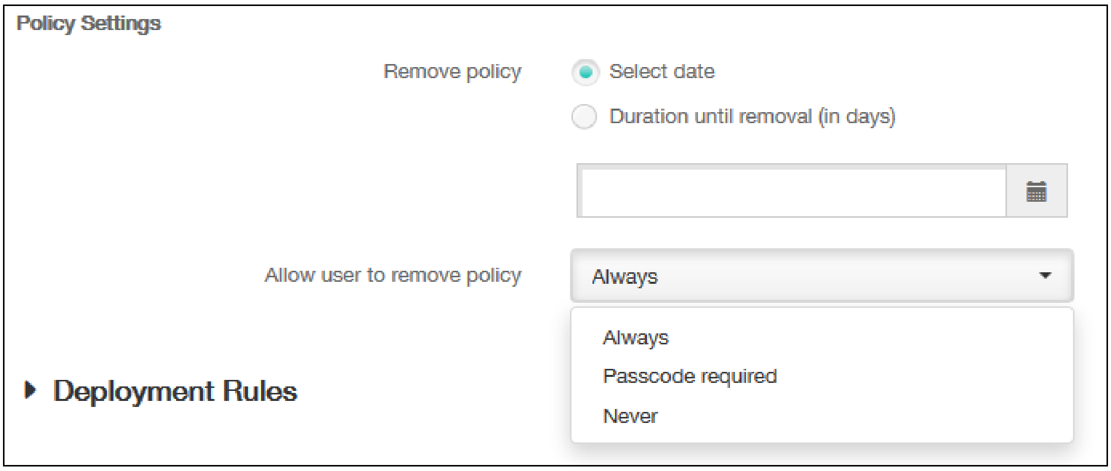
IP Address*	Resource Path*

Policy Settings

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

Allow user to remove policy: Always

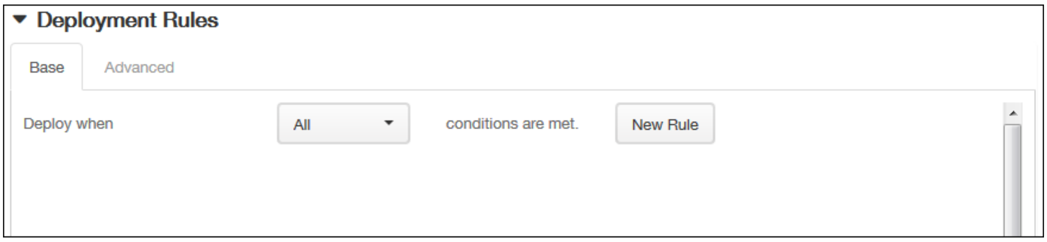
Deployment Rules



Policy Settings

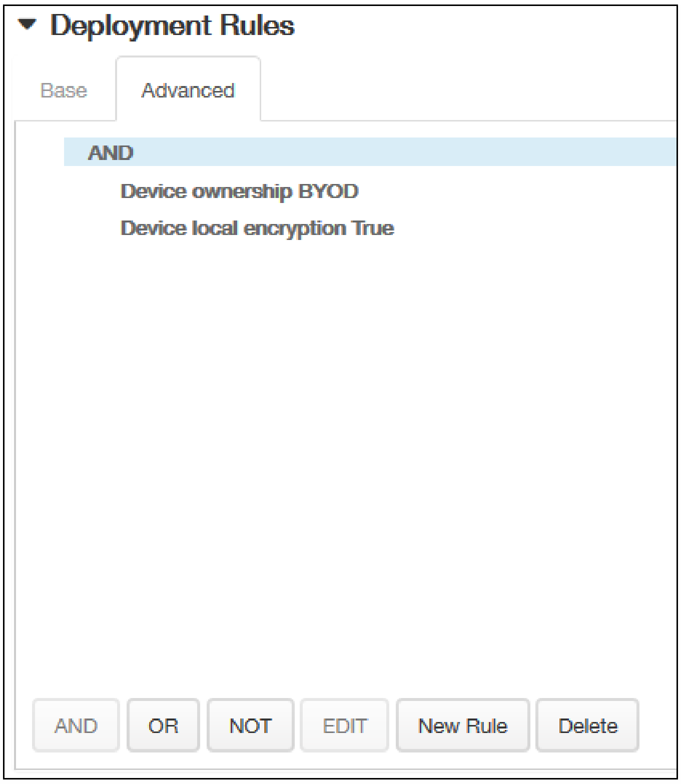
Remove policy: ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always



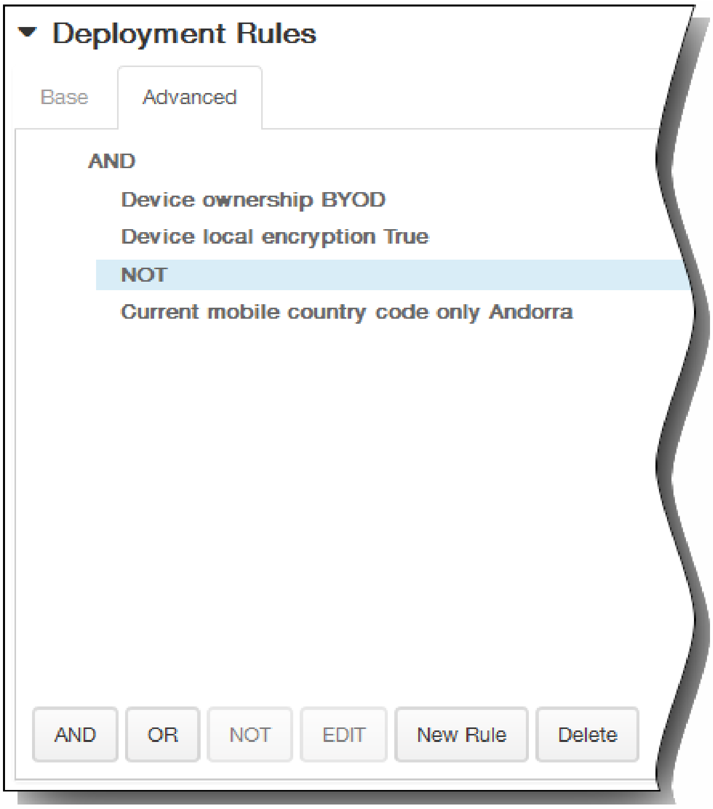
Deployment Rules

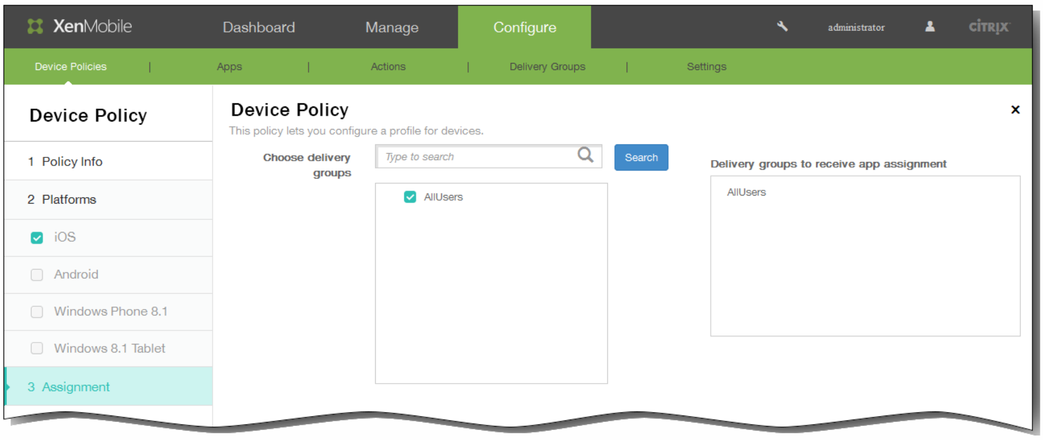
Deploy when All conditions are met.

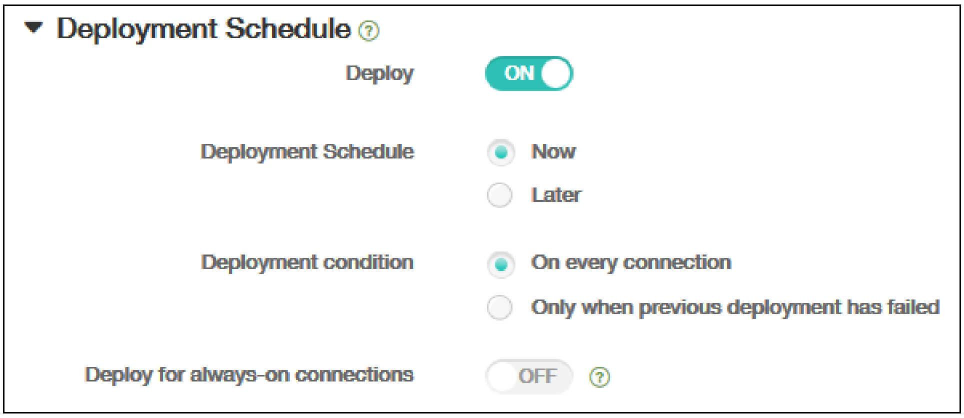


Device ownership BYOD

Device local encryption True


Deployment Rules
Base
Advanced
AND
Device ownership BYOD
Device local encryption True
NOT
Current mobile country code only Andorra
AND
OR
NOT
EDIT
New Rule
Delete


XenMobile
Dashboard
Manage
Configure
administrator
Device Policies
Apps
Actions
Delivery Groups
Settings
Device Policy
1 Policy Info
2 Platforms
☑ iOS
□ Android
□ Windows Phone 8.1
□ Windows 8.1 Tablet
3 Assignment
Device Policy
This policy lets you configure a profile for devices.
Choose delivery groups
Type to search
Search
☑ AllUsers
Delivery groups to receive app assignment
AllUsers



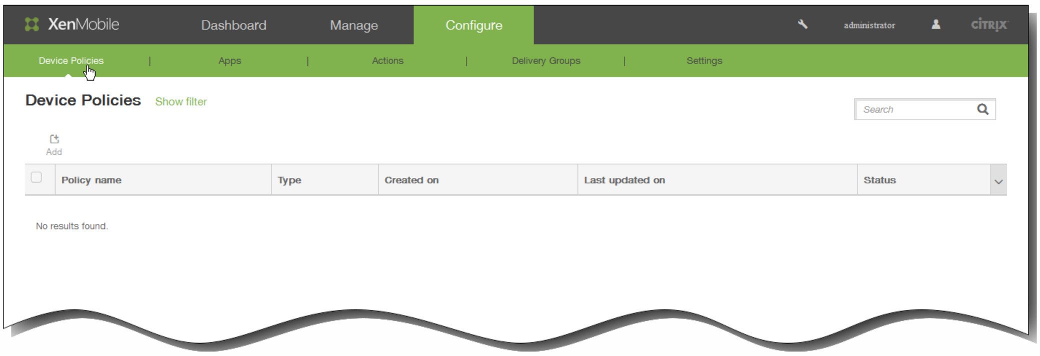
Deployment Schedule

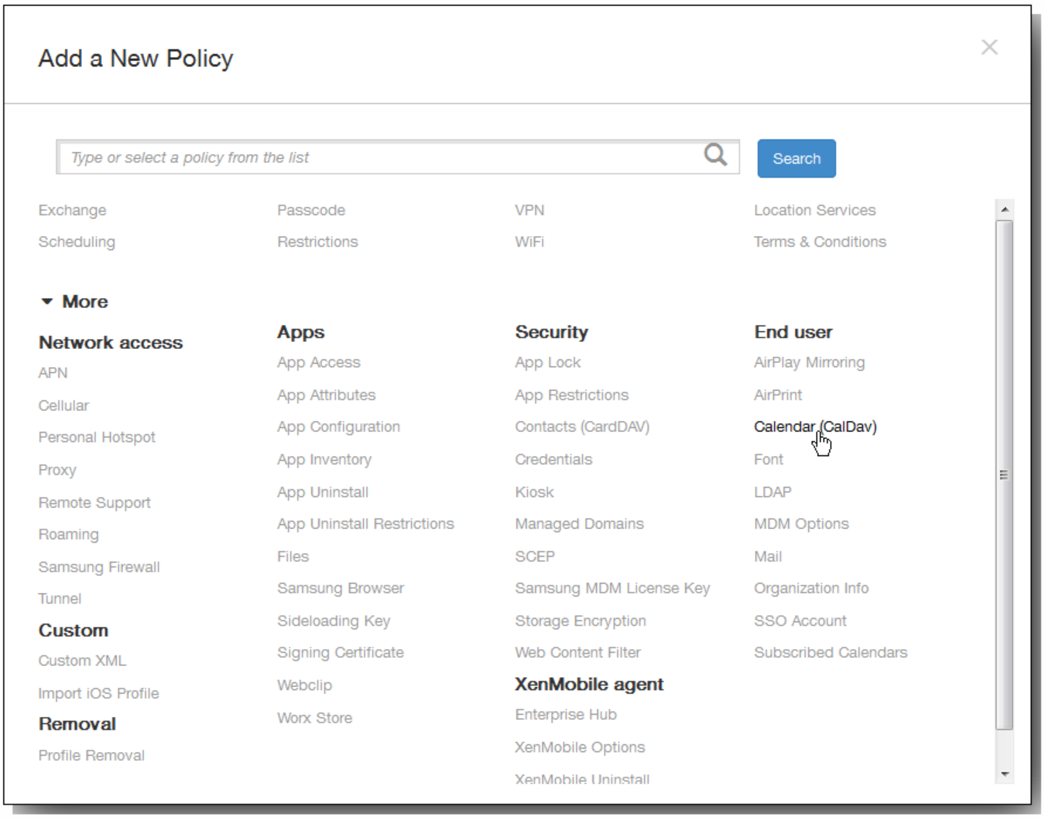
Deploy: ON

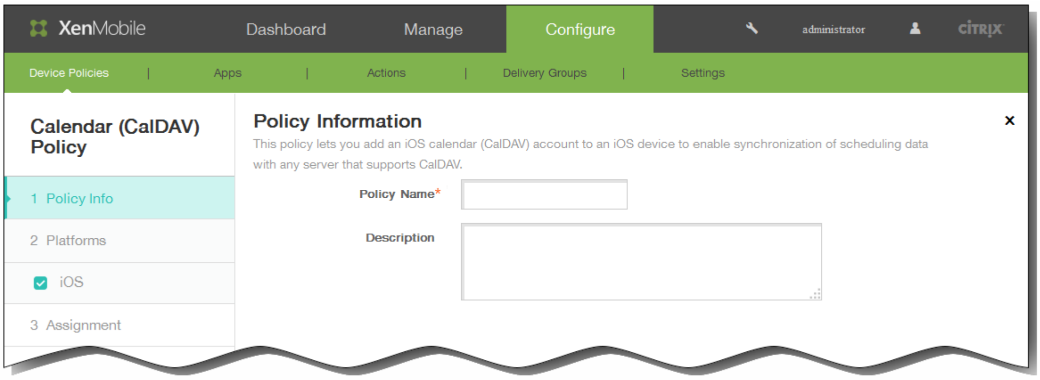
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings
Device Policies
Show filter
Search
Add
Policy name
Type
Created on
Last updated on
Status
No results found.


Add a New Policy
Type or select a policy from the list
Search
Exchange
Scheduling
Passcode
Restrictions
VPN
WiFi
Location Services
Terms & Conditions
More
Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel
Custom
Custom XML
Import iOS Profile
Removal
Profile Removal
Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store
Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter
XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall
End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars



Calendar (CalDAV) Policy

1 Policy Info

2 Platforms

☑ iOS

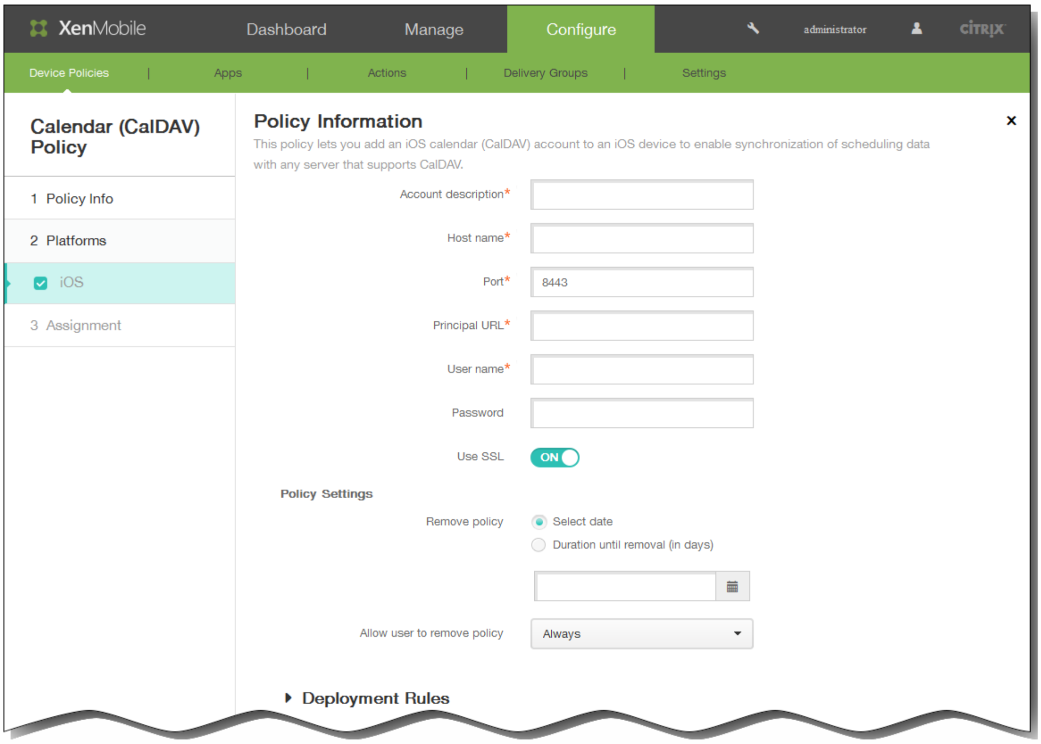
3 Assignment

Policy Information

This policy lets you add an iOS calendar (CalDAV) account to an iOS device to enable synchronization of scheduling data with any server that supports CalDAV.

Policy Name*

Description



Calendar (CalDAV) Policy

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

Policy Information

This policy lets you add an iOS calendar (CalDAV) account to an iOS device to enable synchronization of scheduling data with any server that supports CalDAV.

Account description*

Host name*

Port* 8443

Principal URL*

User name*

Password

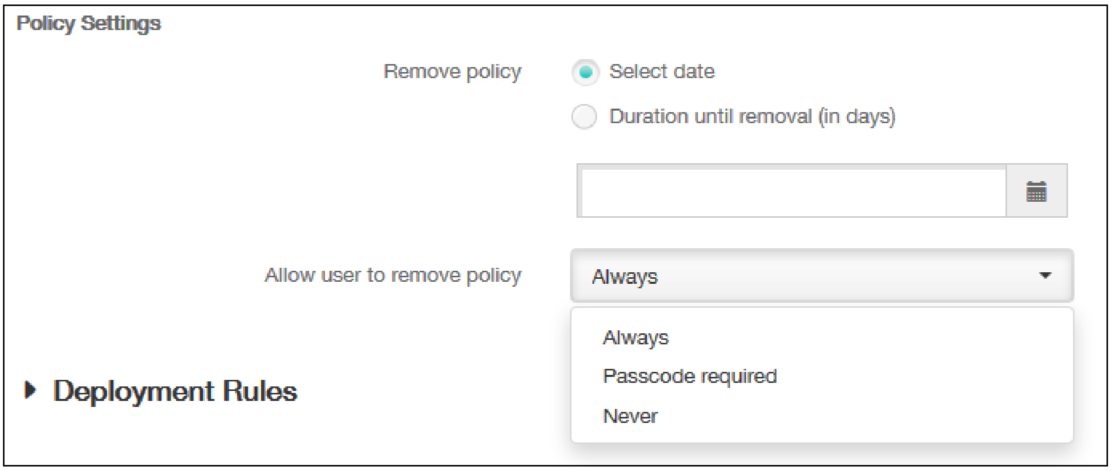
Use SSL ON

Policy Settings

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

Allow user to remove policy Always

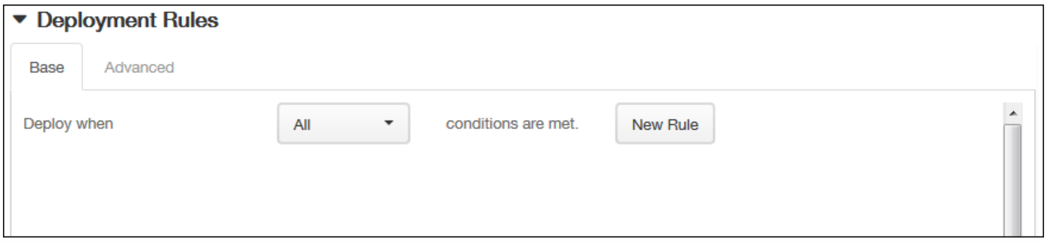
Deployment Rules



Policy Settings

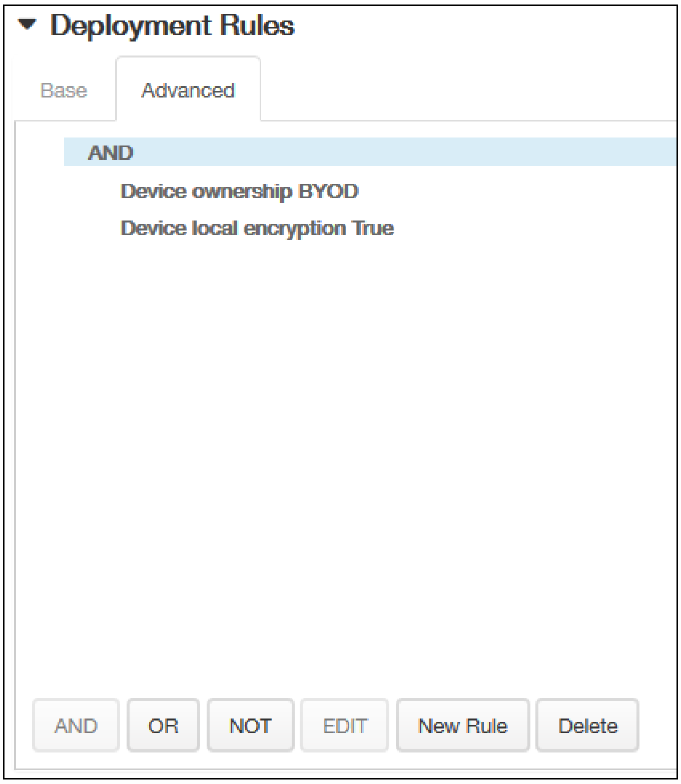
Remove policy ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always



Deployment Rules

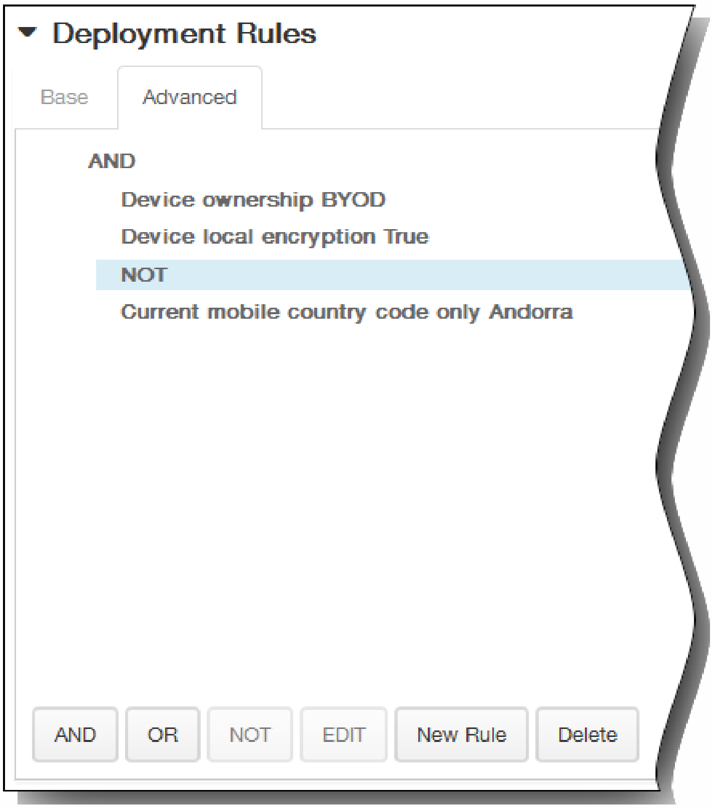
Deploy when All conditions are met.



AND

Device ownership BYOD

Device local encryption True



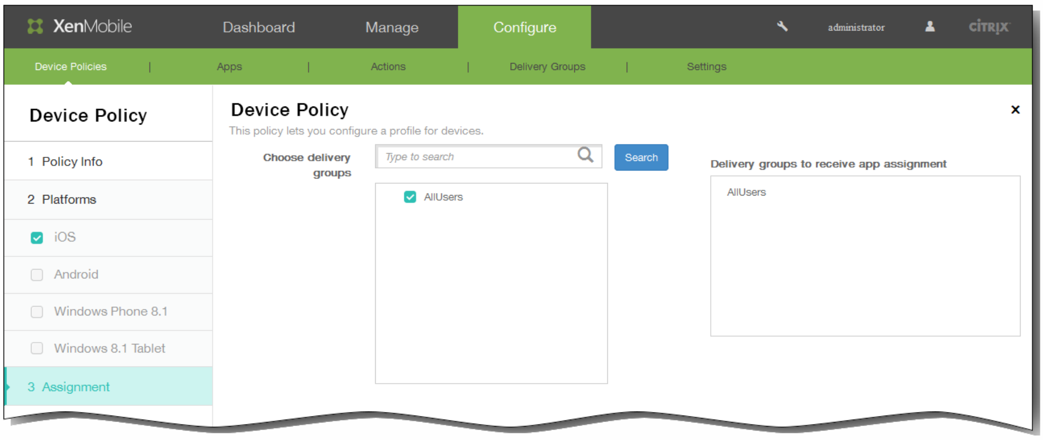
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

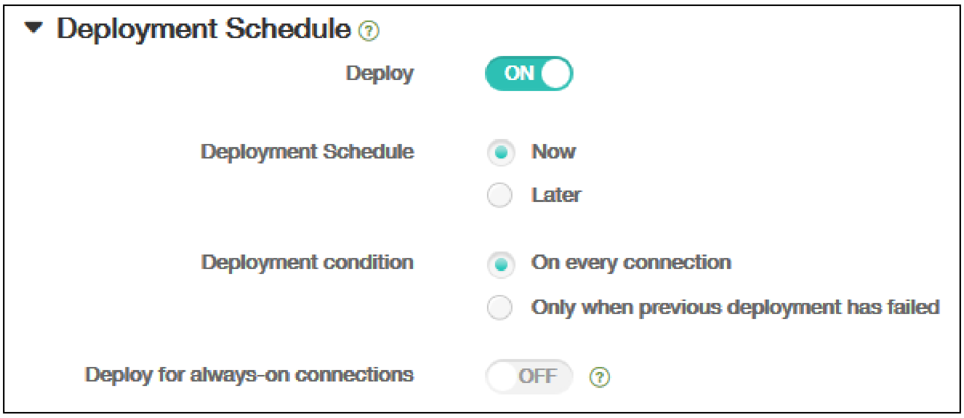
3 Assignment

Device Policy

This policy lets you configure a profile for devices.

Choose delivery groups: ☑ AllUsers

Delivery groups to receive app assignment: AllUsers



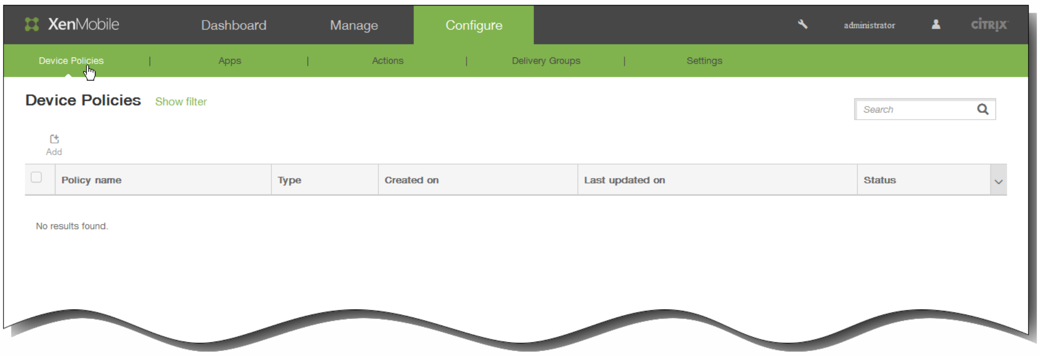
Deployment Schedule

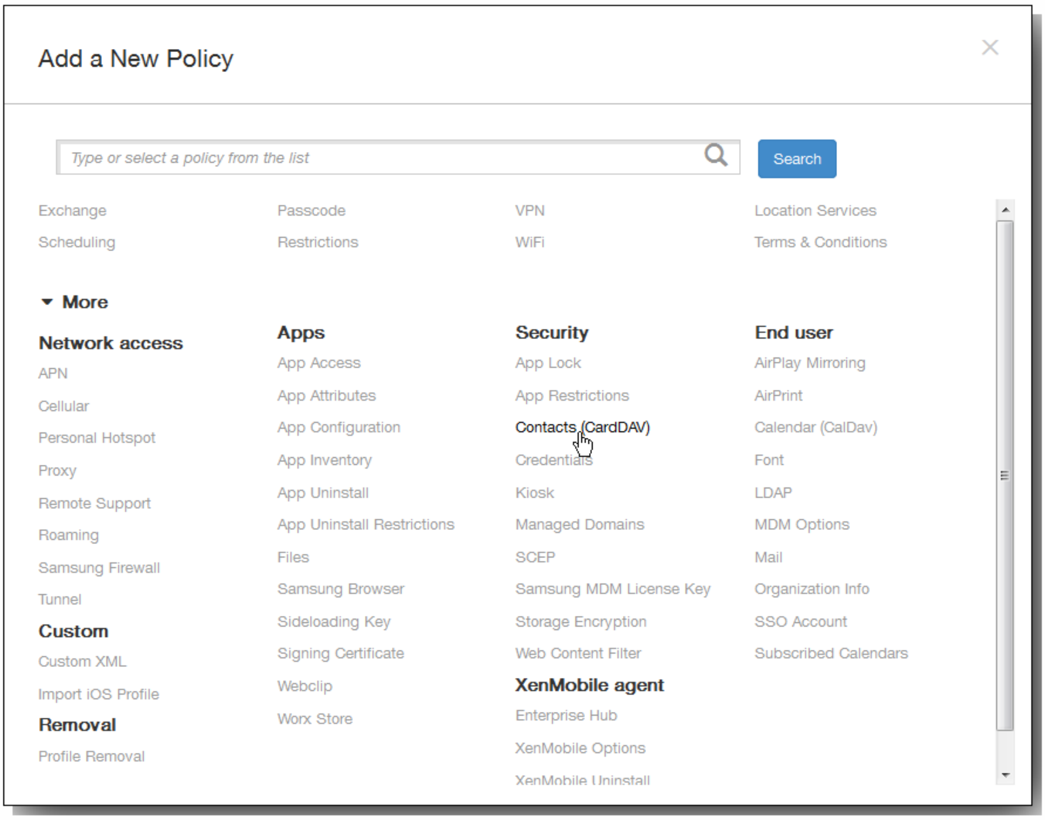
Deploy: ON

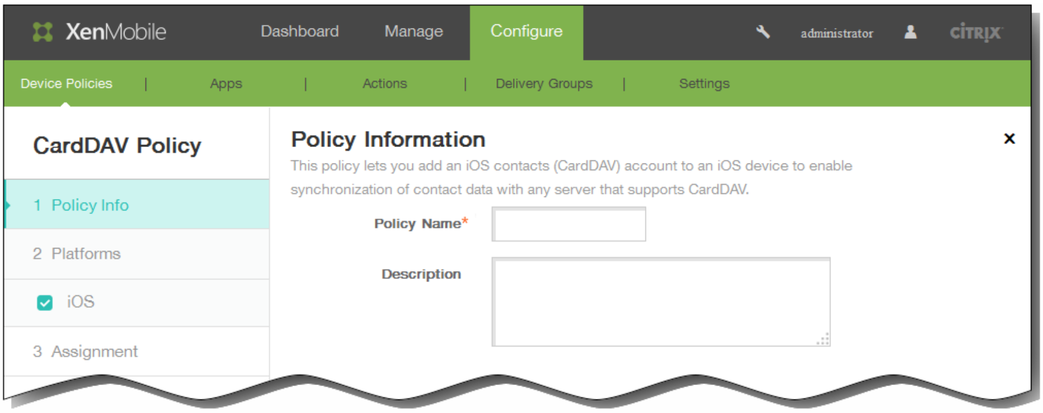
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies
Apps
Actions
Delivery Groups
Settings
Device Policies
Show filter
Search
Add
Policy name
Type
Created on
Last updated on
Status
No results found.


Add a New Policy
Type or select a policy from the list
Search
Exchange
Scheduling
Passcode
Restrictions
VPN
WiFi
Location Services
Terms & Conditions
More
Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel
Custom
Custom XML
Import iOS Profile
Removal
Profile Removal
Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store
Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter
XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall
End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars


XenMobile
Dashboard
Manage
Configure
administrator
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings

CardDAV Policy

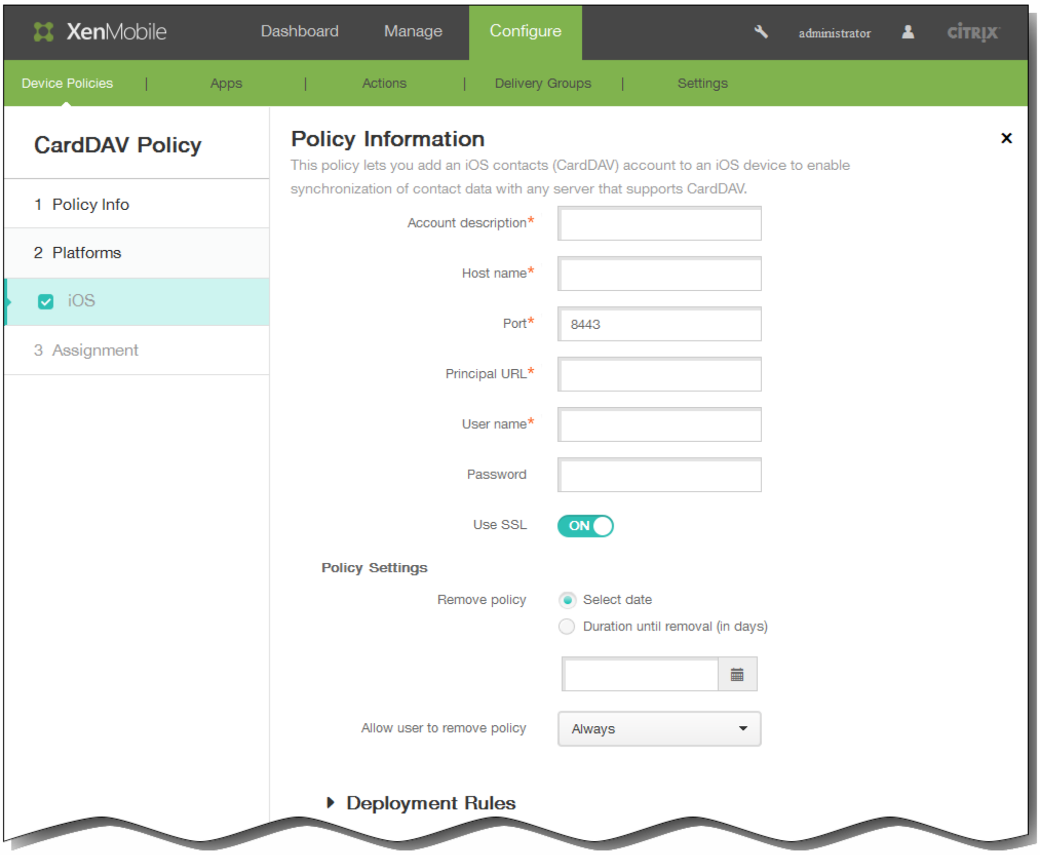
1 Policy Info
2 Platforms
☑ iOS
3 Assignment

Policy Information

This policy lets you add an iOS contacts (CardDAV) account to an iOS device to enable synchronization of contact data with any server that supports CardDAV.

Policy Name*

Description


XenMobile
Dashboard
Manage
Configure
administrator
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings

CardDAV Policy

1 Policy Info
2 Platforms
☑ iOS
3 Assignment

Policy Information

This policy lets you add an iOS contacts (CardDAV) account to an iOS device to enable synchronization of contact data with any server that supports CardDAV.

Account description*

Host name*

Port* 8443

Principal URL*

User name*

Password

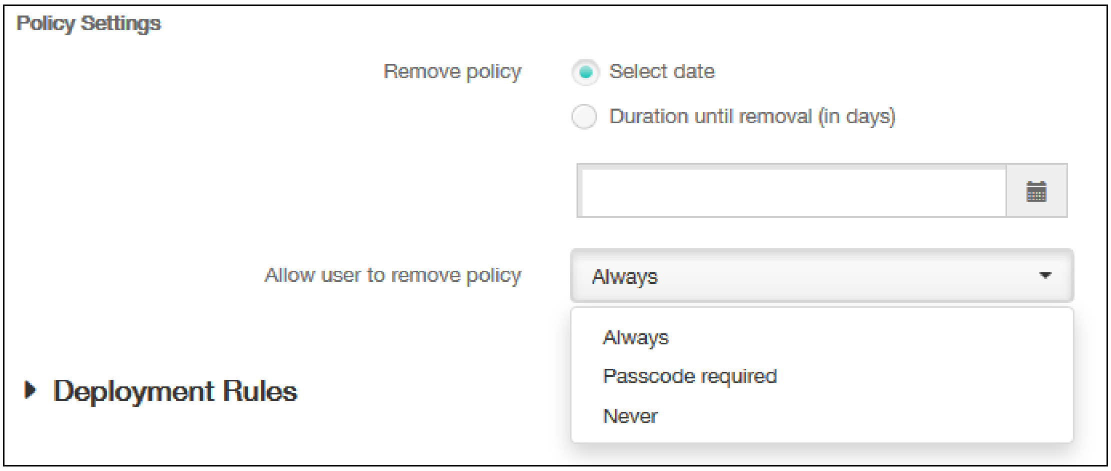
Use SSL ON

Policy Settings

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

Allow user to remove policy Always

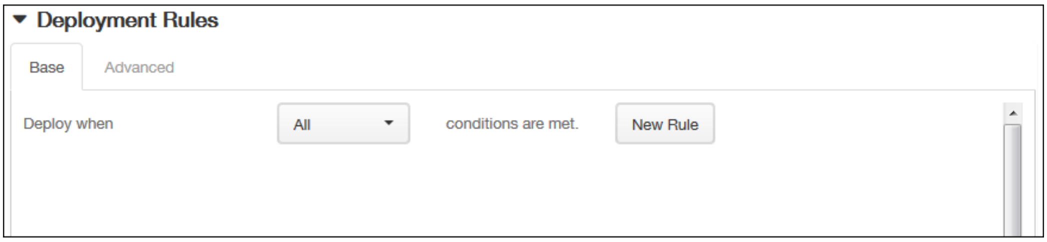
Deployment Rules



Policy Settings

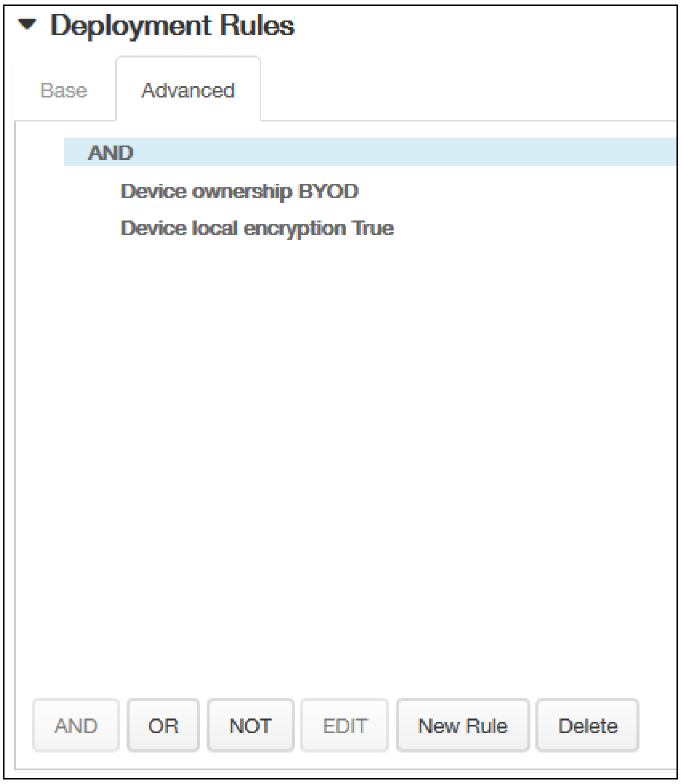
Remove policy ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always



Deployment Rules

Deploy when All conditions are met.

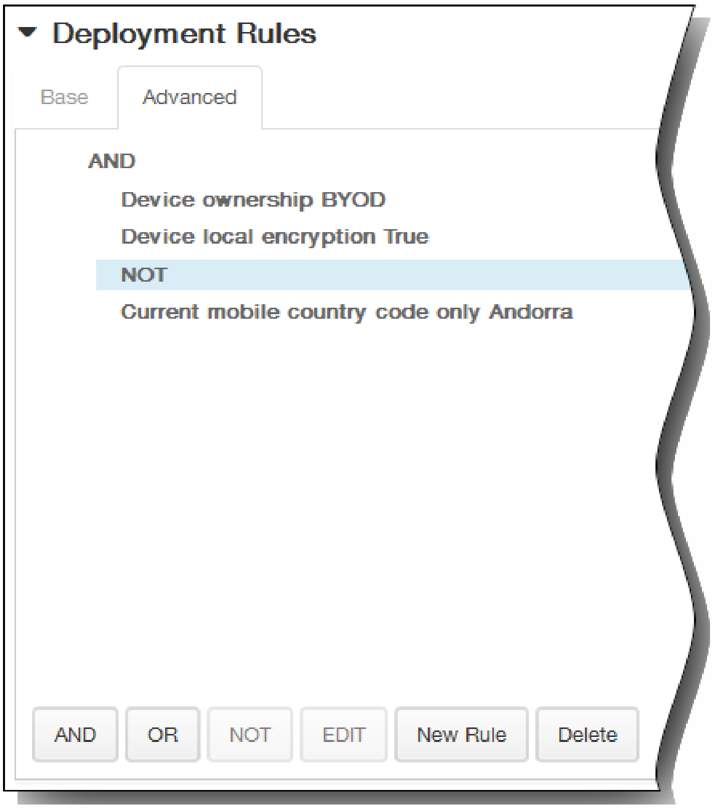


Deployment Rules

AND

Device ownership BYOD

Device local encryption True



Deployment Rules

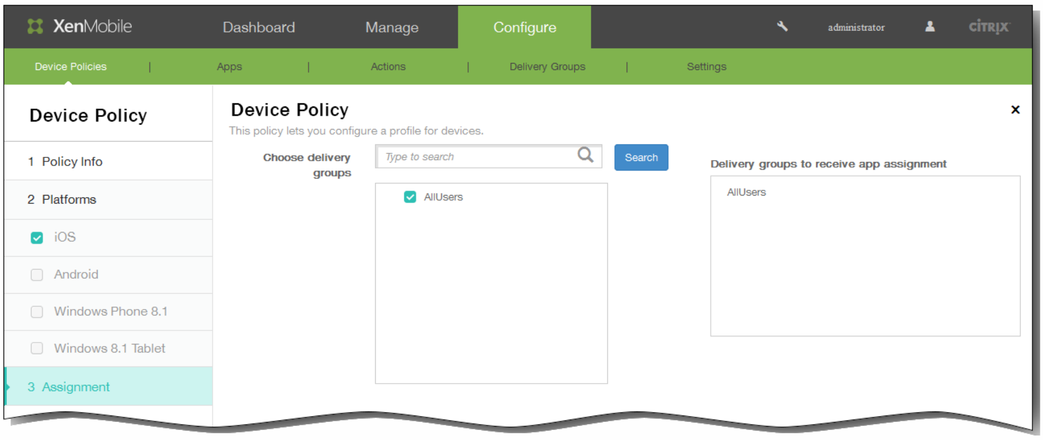
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

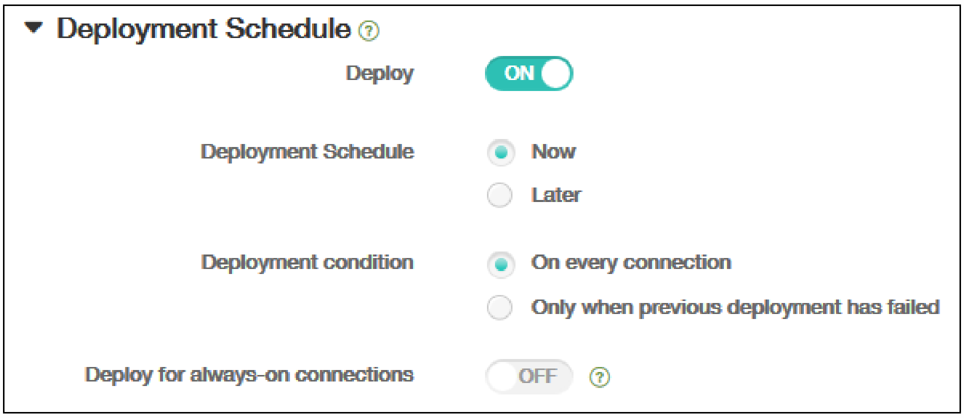
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



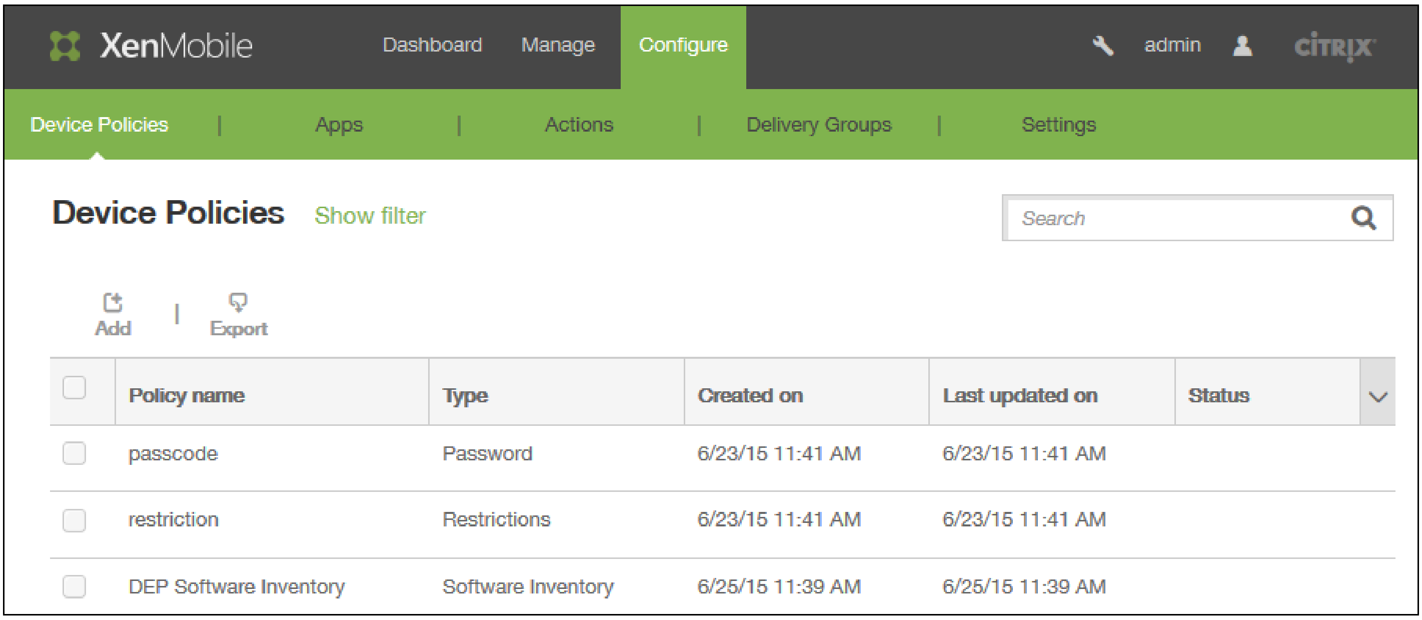
▼ Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

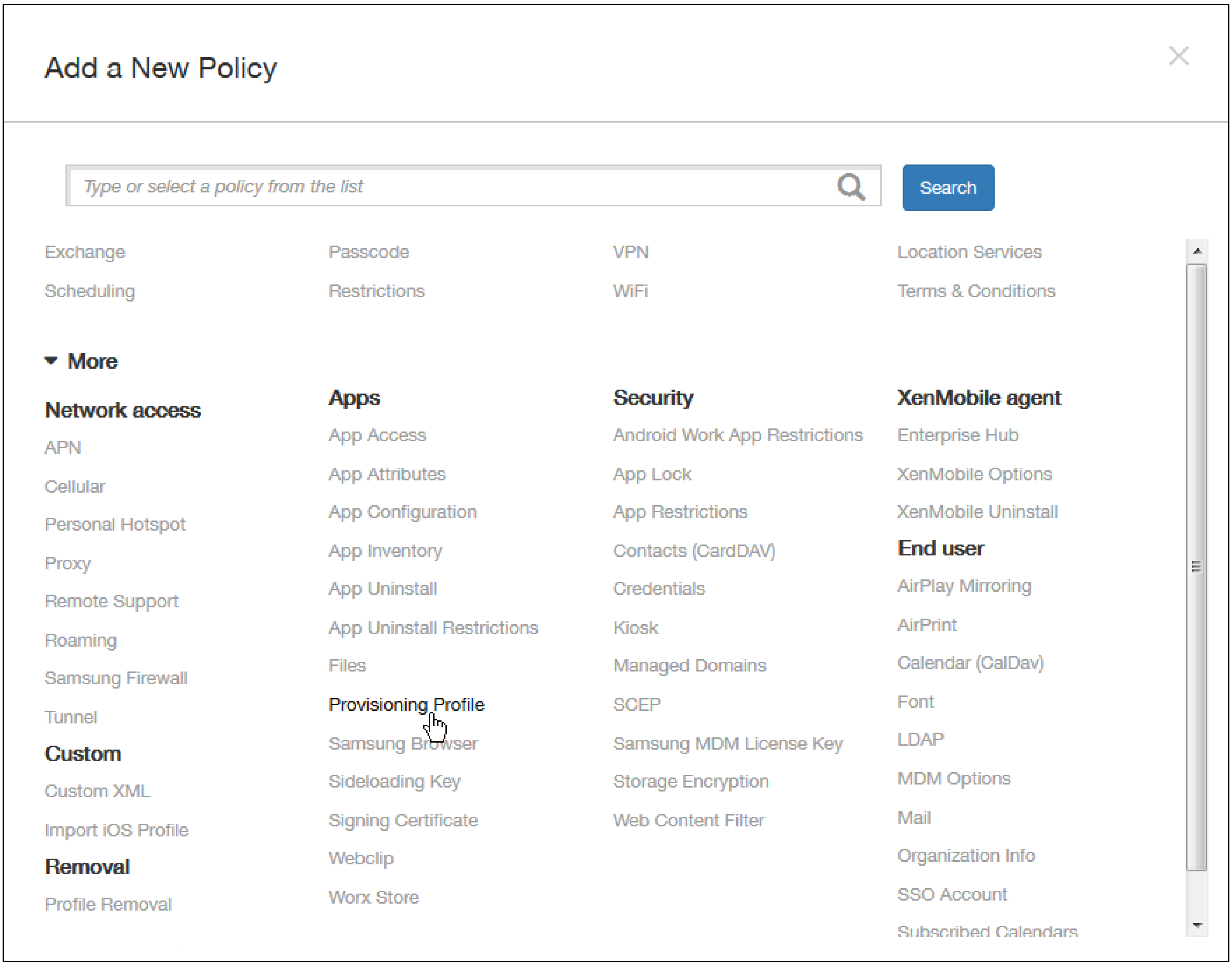
Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF



Device Policies

□	Policy name	Type	Created on	Last updated on	Status
□	passcode	Password	6/23/15 11:41 AM	6/23/15 11:41 AM	
□	restriction	Restrictions	6/23/15 11:41 AM	6/23/15 11:41 AM	
□	DEP Software Inventory	Software Inventory	6/25/15 11:39 AM	6/25/15 11:39 AM	



Add a New Policy

Type or select a policy from the list

Search

Exchange
Scheduling

Passcode
Restrictions

VPN
WiFi

Location Services
Terms & Conditions

▾ More

Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel

Custom
Custom XML
Import iOS Profile

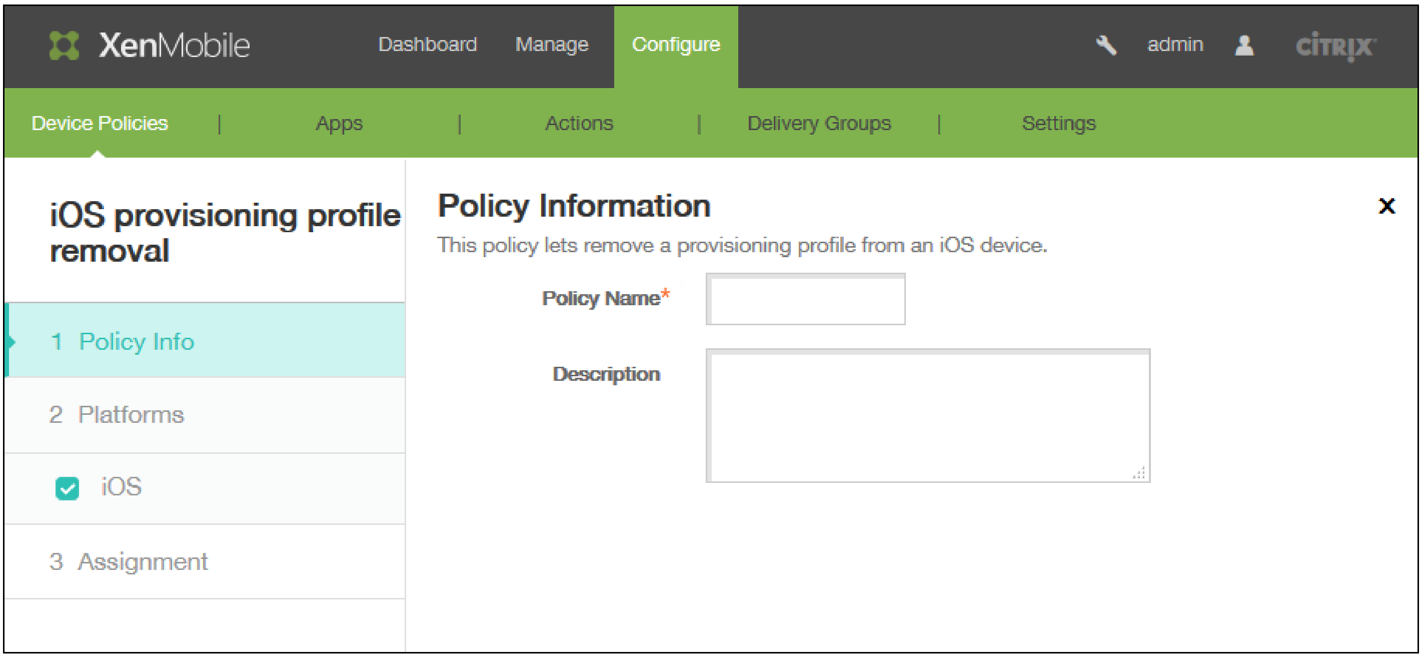
Removal
Profile Removal

Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Provisioning Profile
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store

Security
Android Work App Restrictions
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter

XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall

End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars



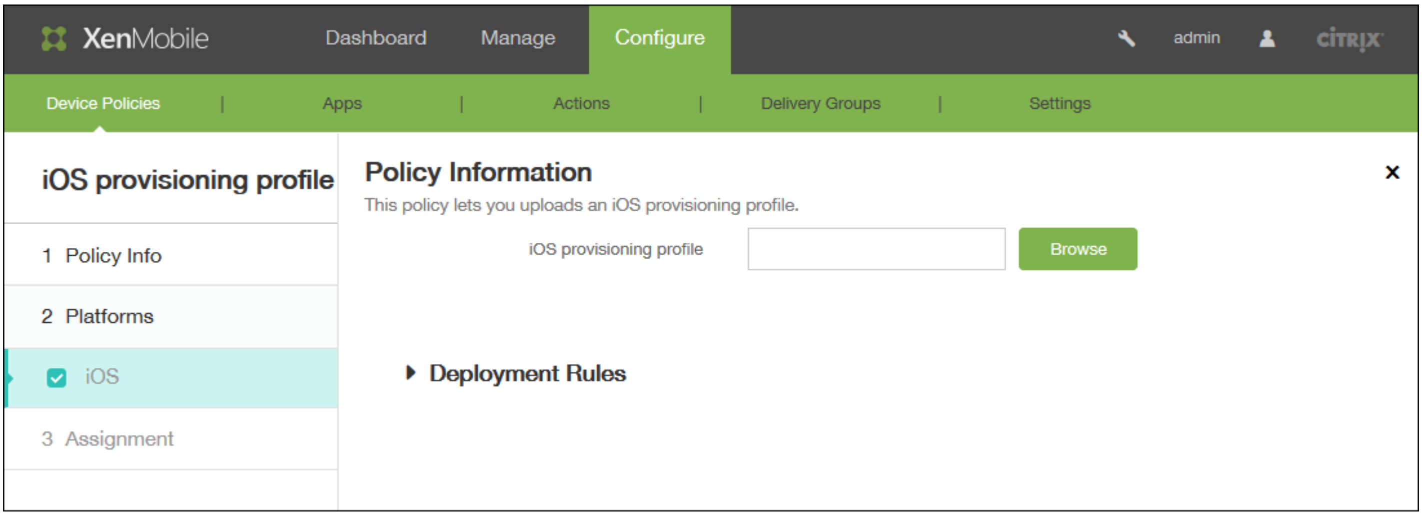
Policy Information

This policy lets remove a provisioning profile from an iOS device.

Policy Name*

Description

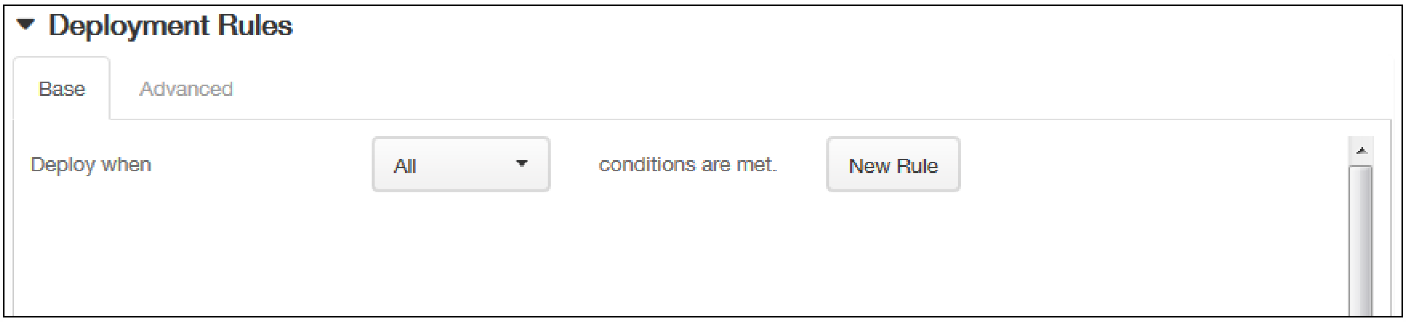
-
-



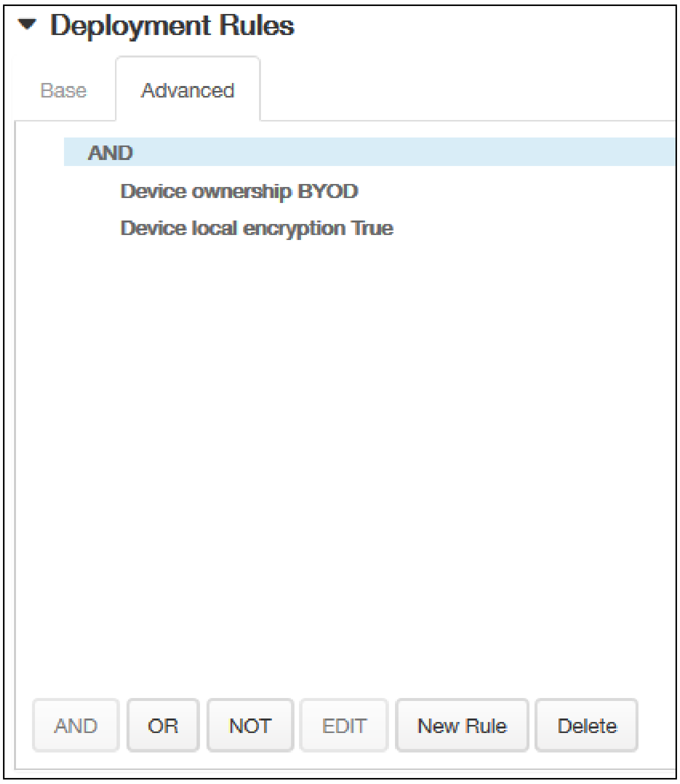
Policy Information

This policy lets you uploads an iOS provisioning profile.

iOS provisioning profile



Deploy when All conditions are met.

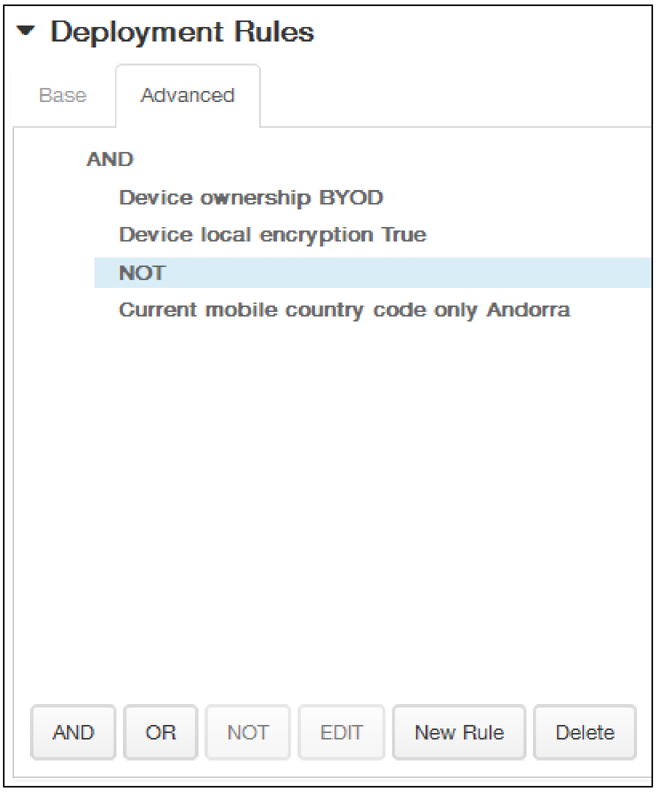


AND

Device ownership BYOD

Device local encryption True

-
-
-
-



Deployment Rules

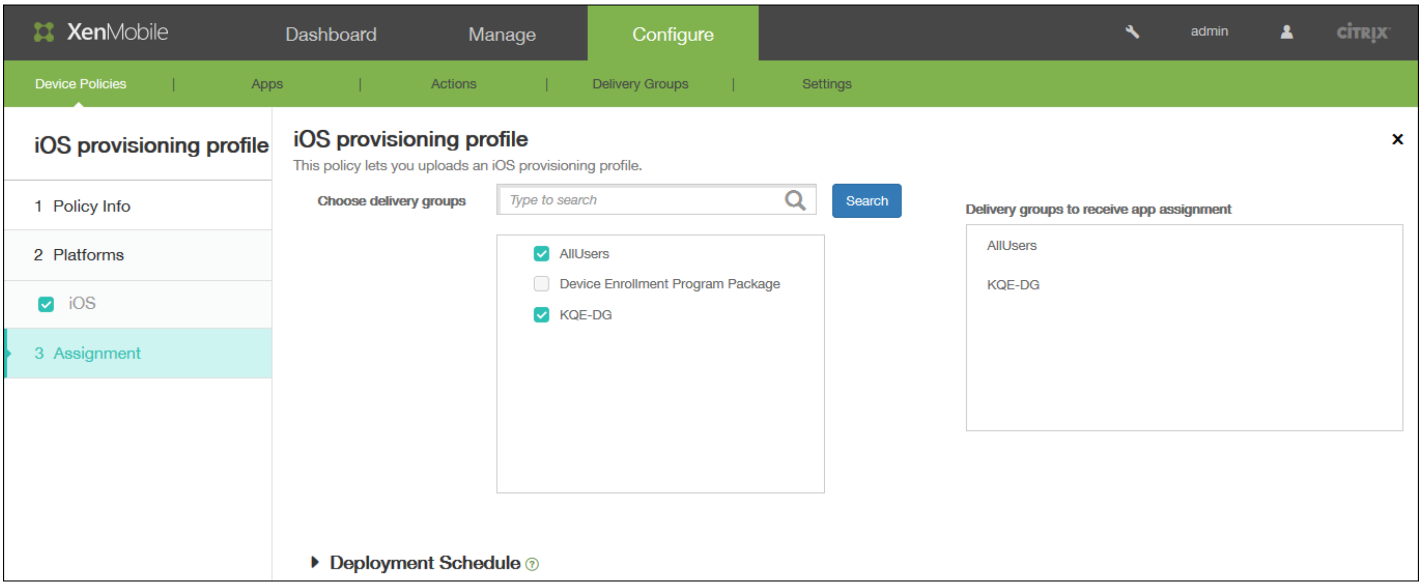
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



iOS provisioning profile

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

iOS provisioning profile

This policy lets you uploads an iOS provisioning profile.

Choose delivery groups: Type to search | Search

☑ AllUsers
□ Device Enrollment Program Package
☑ KQE-DG

Delivery groups to receive app assignment

AllUsers
KQE-DG

▸ Deployment Schedule ?

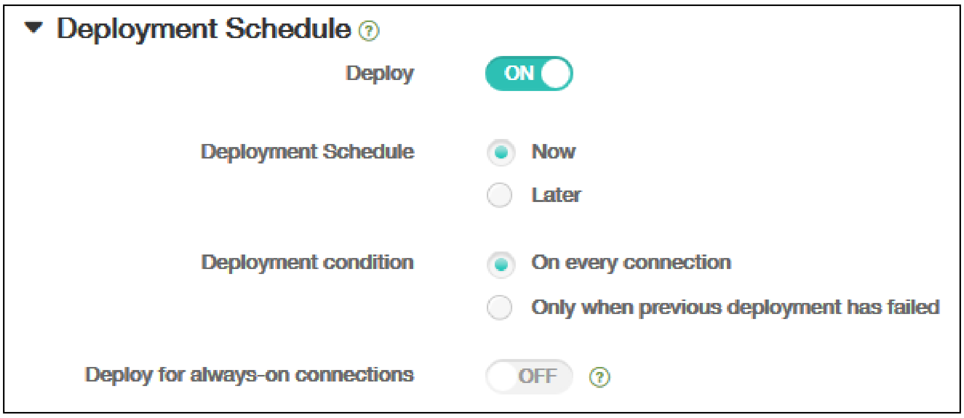
•

•

•

•

•



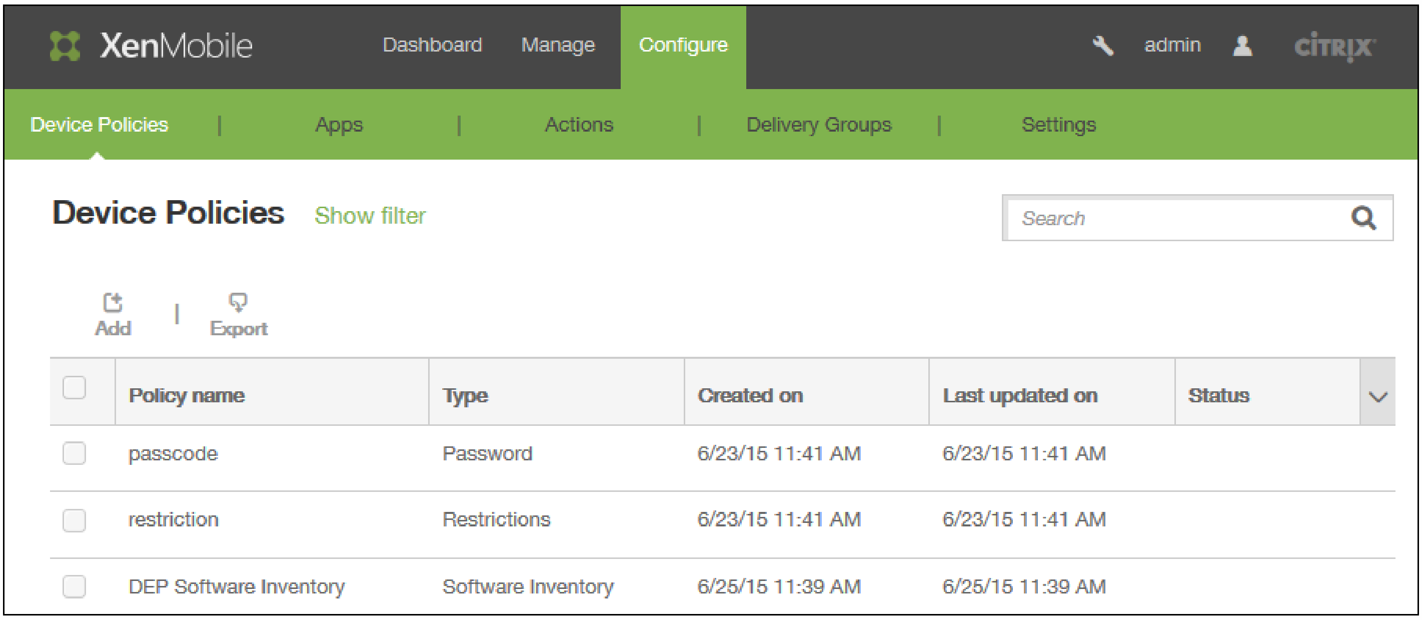
▾ Deployment Schedule ?

Deploy: ON

Deployment Schedule: ● Now ○ Later

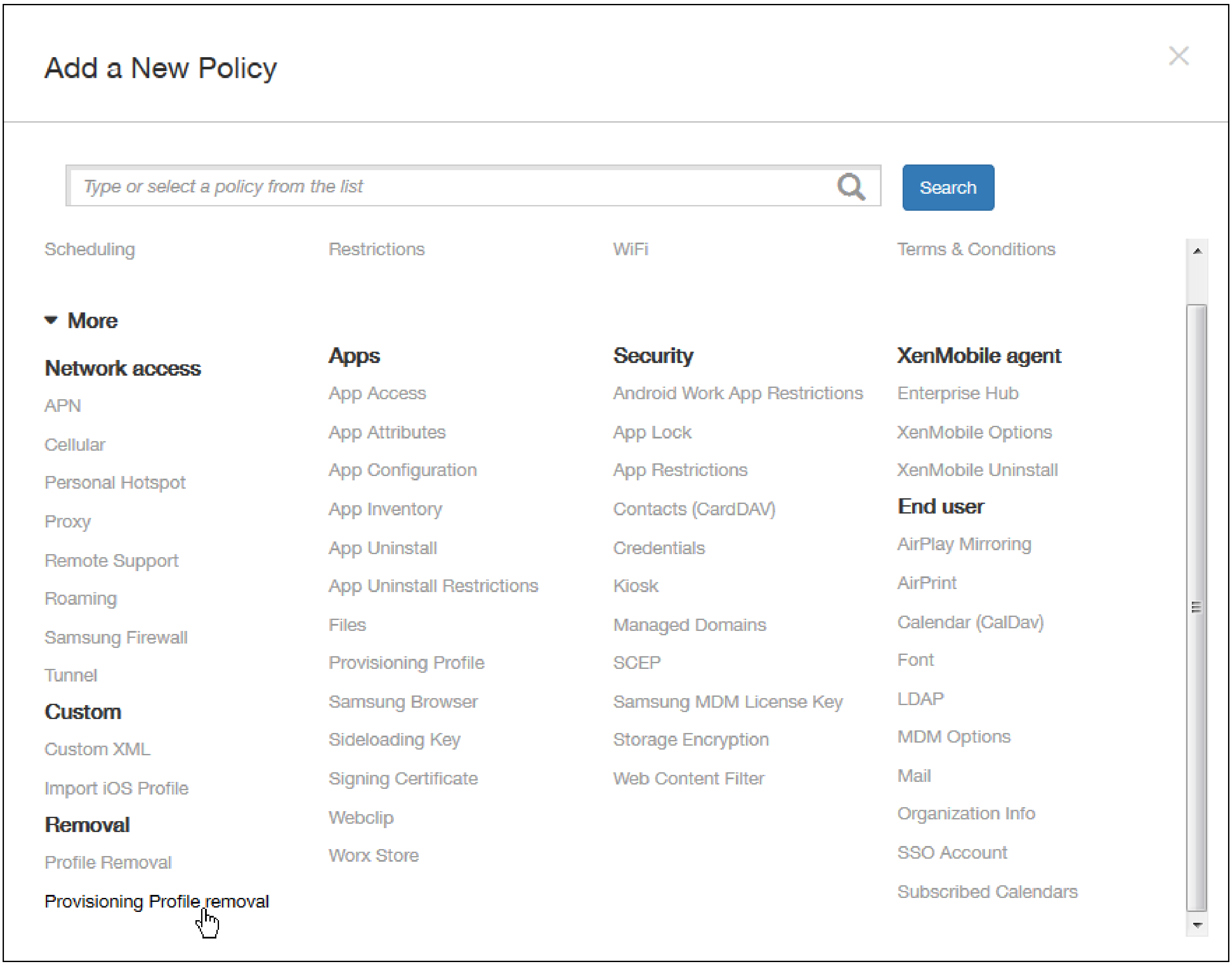
Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF ?



Device Policies Show filter

□	Policy name	Type	Created on	Last updated on	Status
□	passcode	Password	6/23/15 11:41 AM	6/23/15 11:41 AM	
□	restriction	Restrictions	6/23/15 11:41 AM	6/23/15 11:41 AM	
□	DEP Software Inventory	Software Inventory	6/25/15 11:39 AM	6/25/15 11:39 AM	



Add a New Policy

Scheduling

Restrictions

WiFi

Terms & Conditions

▾ More

Network access

- APN
- Cellular
- Personal Hotspot
- Proxy
- Remote Support
- Roaming
- Samsung Firewall
- Tunnel

Custom

- Custom XML
- Import iOS Profile

Removal

- Profile Removal
- Provisioning Profile removal

Apps

- App Access
- App Attributes
- App Configuration
- App Inventory
- App Uninstall
- App Uninstall Restrictions
- Files
- Provisioning Profile
- Samsung Browser
- Sideloading Key
- Signing Certificate
- Webclip
- Worx Store

Security

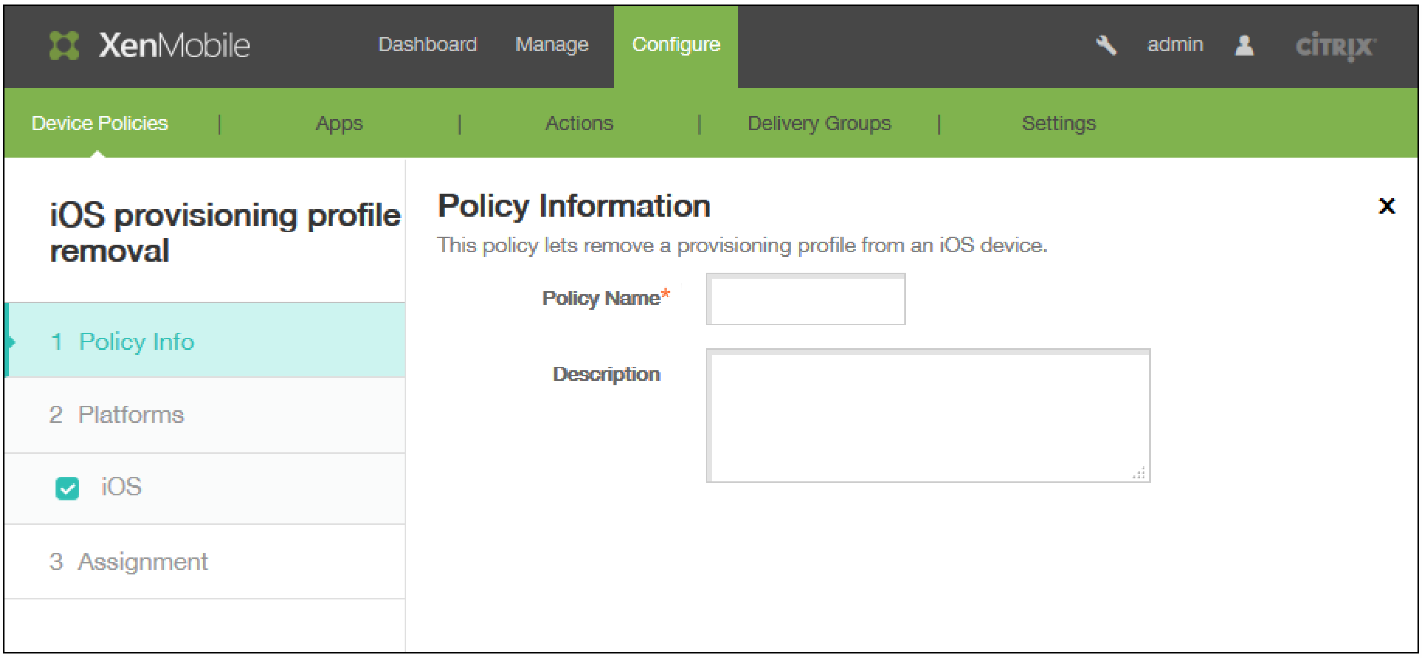
- Android Work App Restrictions
- App Lock
- App Restrictions
- Contacts (CardDAV)
- Credentials
- Kiosk
- Managed Domains
- SCEP
- Samsung MDM License Key
- Storage Encryption
- Web Content Filter

XenMobile agent

- Enterprise Hub
- XenMobile Options
- XenMobile Uninstall

End user

- AirPlay Mirroring
- AirPrint
- Calendar (CalDav)
- Font
- LDAP
- MDM Options
- Mail
- Organization Info
- SSO Account
- Subscribed Calendars



iOS provisioning profile removal

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

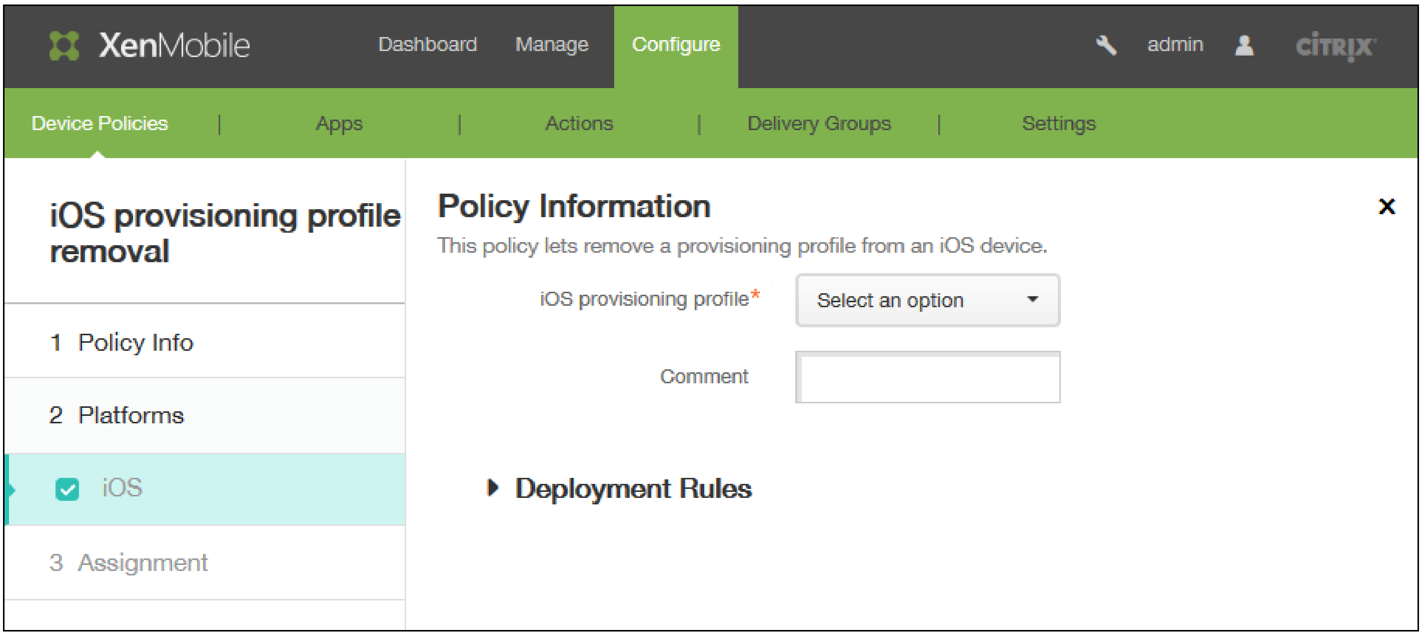
Policy Information

This policy lets remove a provisioning profile from an iOS device.

Policy Name*

Description

-
-



iOS provisioning profile removal

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

Policy Information

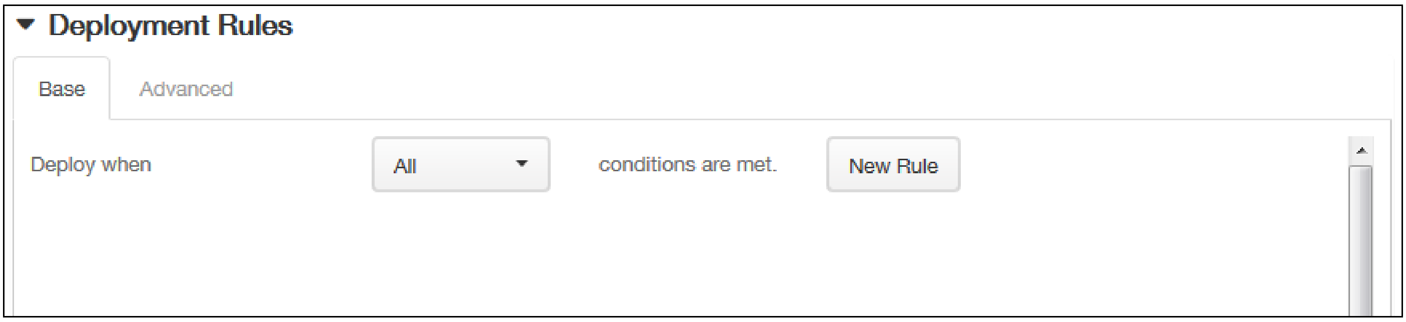
This policy lets remove a provisioning profile from an iOS device.

iOS provisioning profile* Select an option

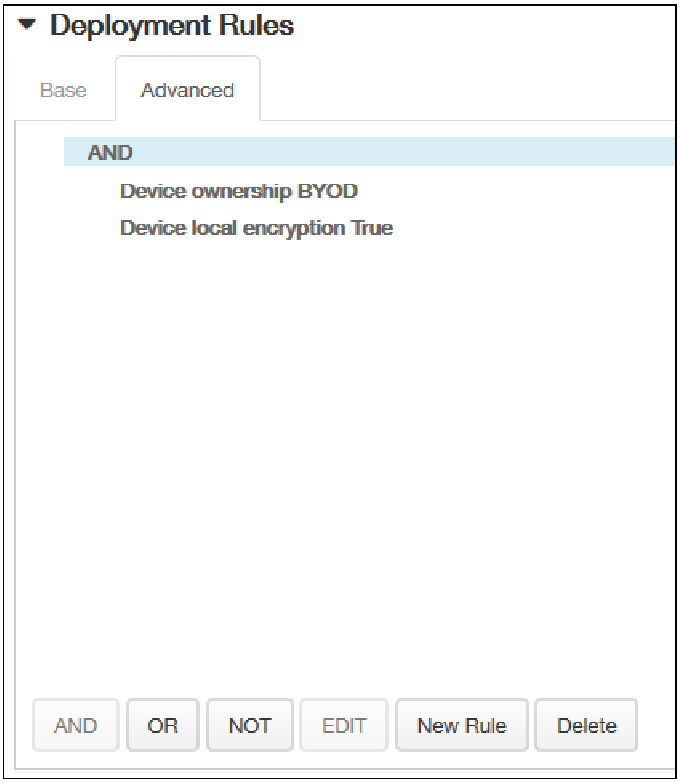
Comment

Deployment Rules

-
-



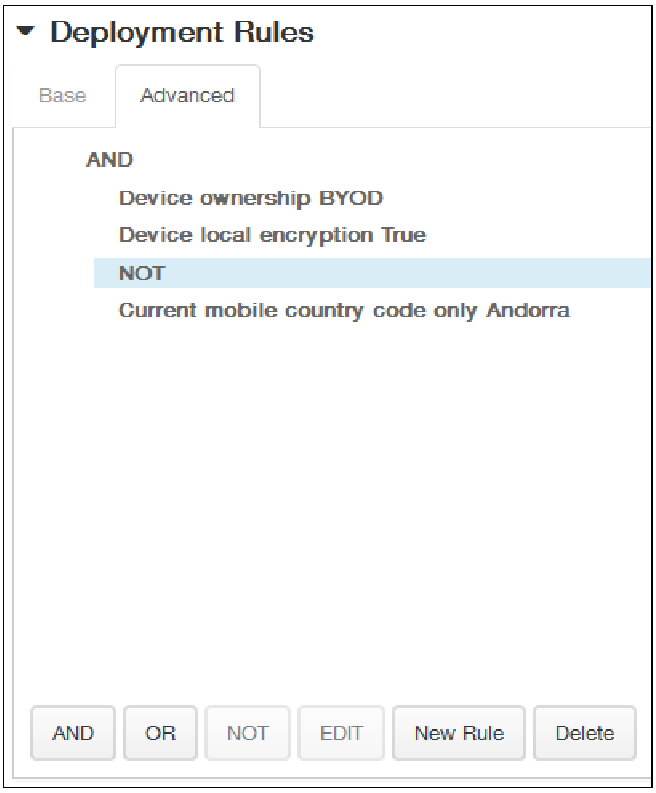
Deploy when All conditions are met. New Rule



AND

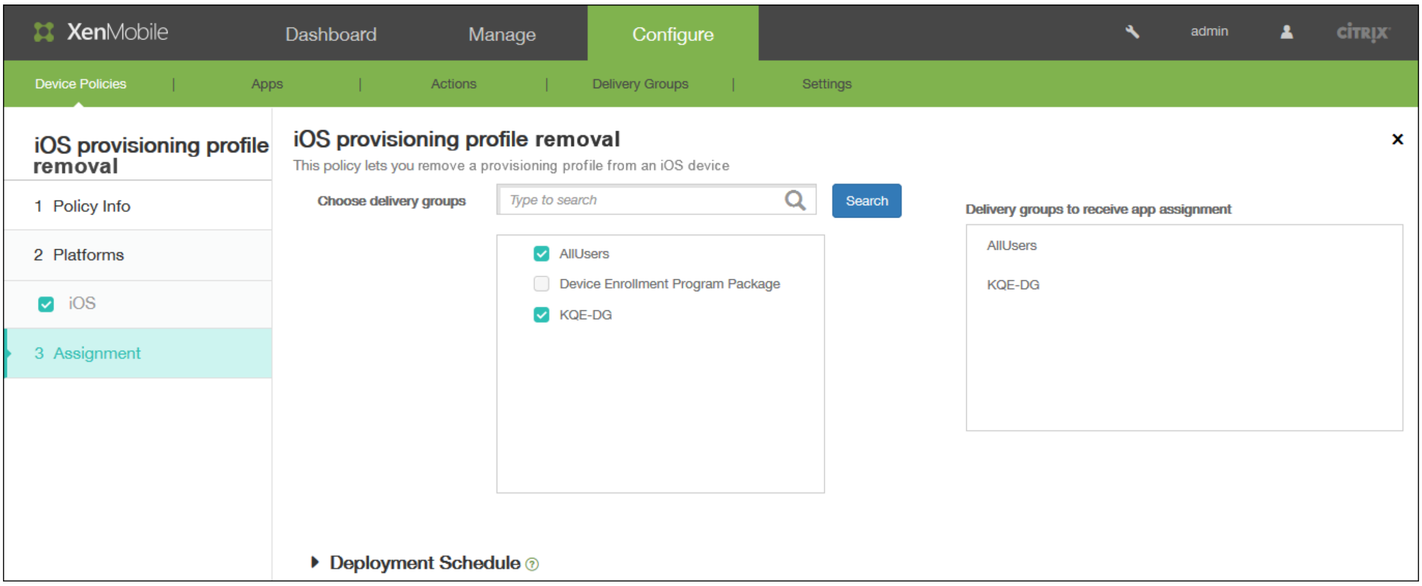
Device ownership BYOD

Device local encryption True



Deployment Rules

AND
Device ownership BYOD
Device local encryption True
NOT
Current mobile country code only Andorra



iOS provisioning profile removal

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

iOS provisioning profile removal

This policy lets you remove a provisioning profile from an iOS device

Choose delivery groups: Type to search [Search]

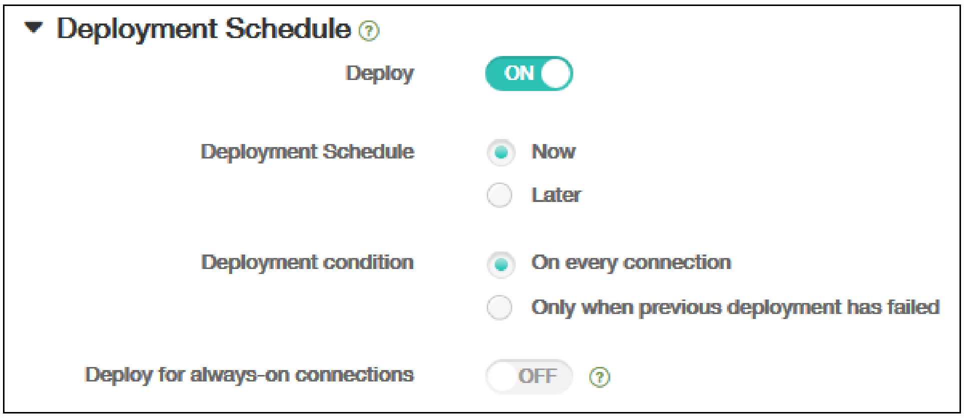
☑ AllUsers
□ Device Enrollment Program Package
☑ KQE-DG

Delivery groups to receive app assignment

AllUsers
KQE-DG

Deployment Schedule

-
-
-
-
-



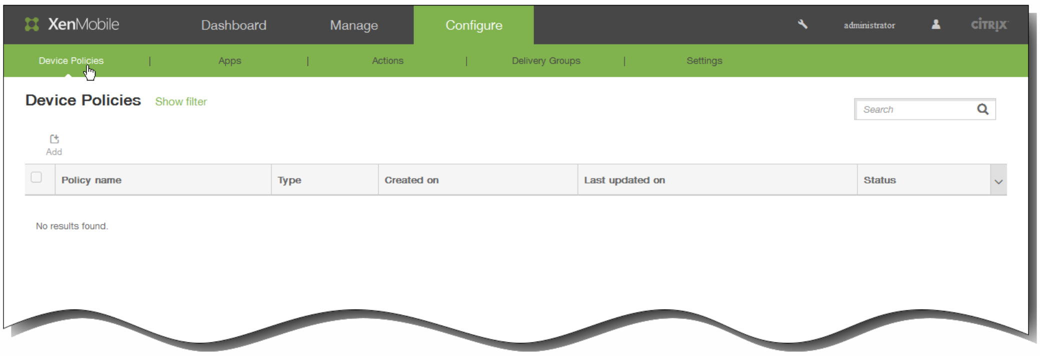
Deployment Schedule

Deploy: ON

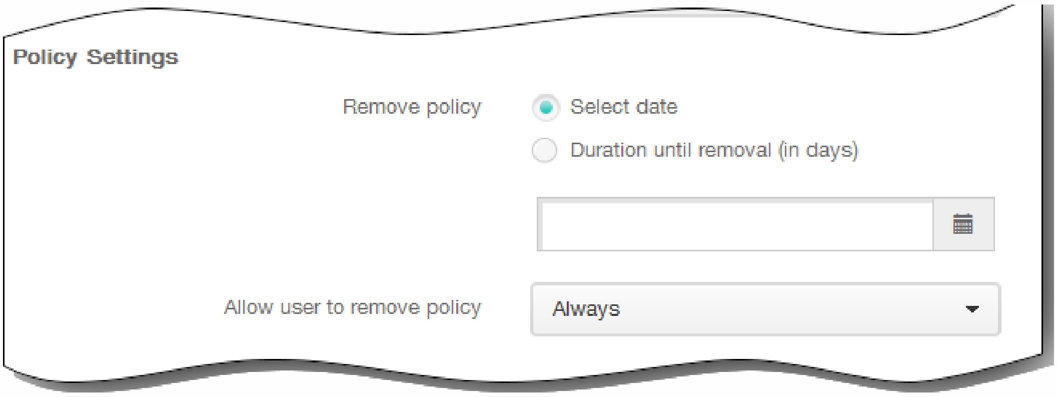
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF



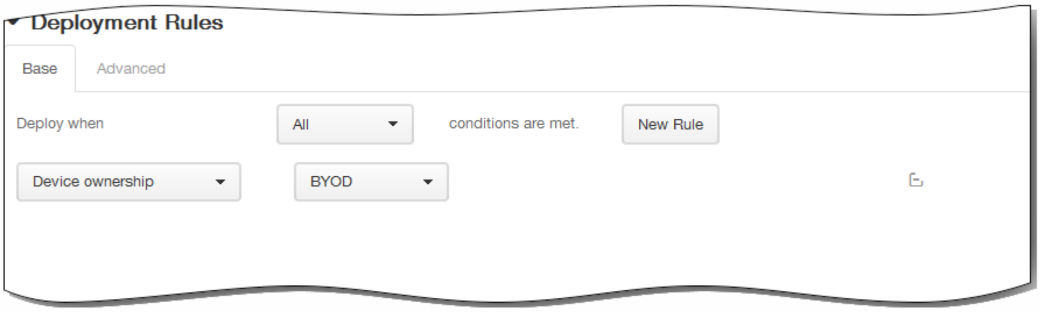
No results found.



Policy Settings

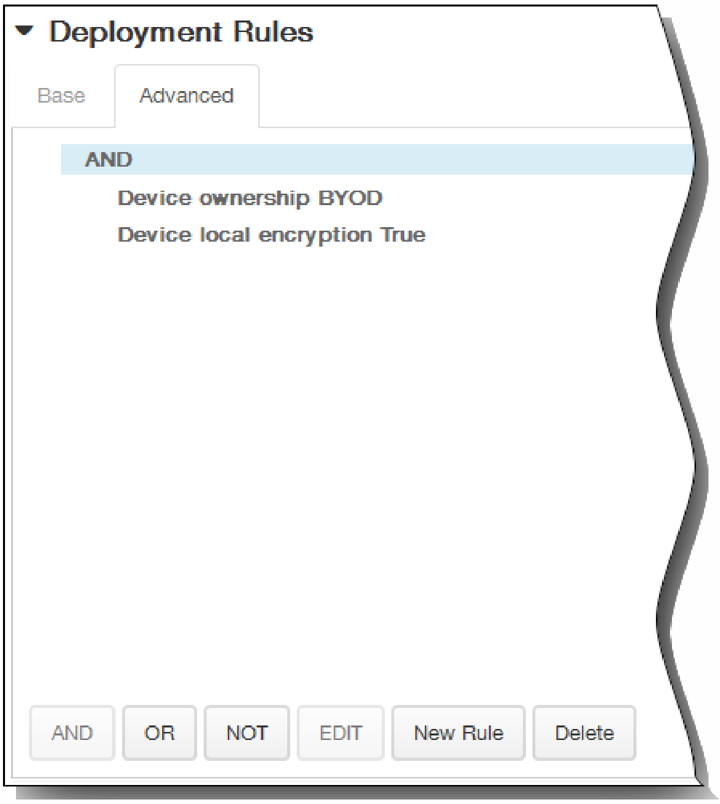
Remove policy ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always



Deploy when All conditions are met.

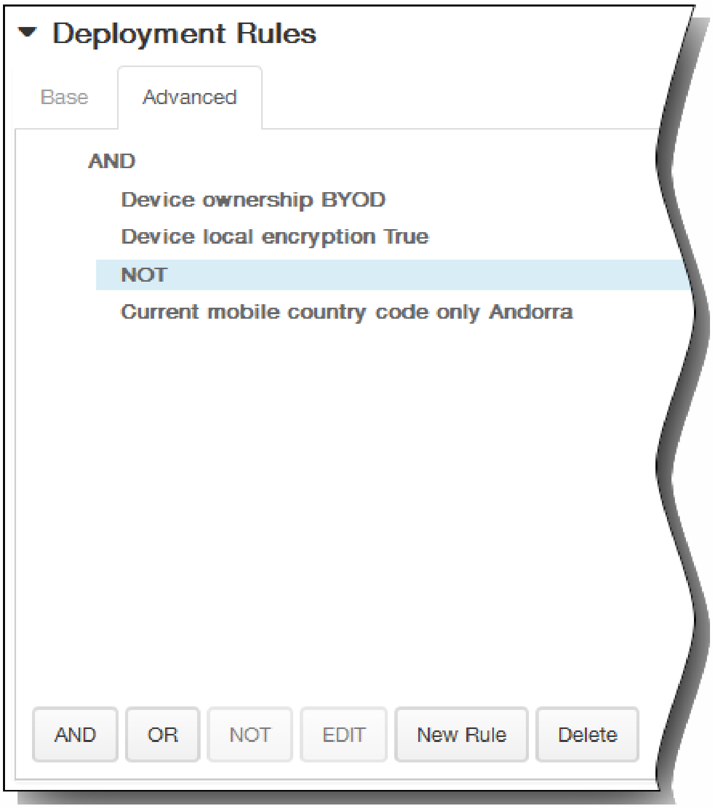
Device ownership BYOD



AND

Device ownership BYOD

Device local encryption True



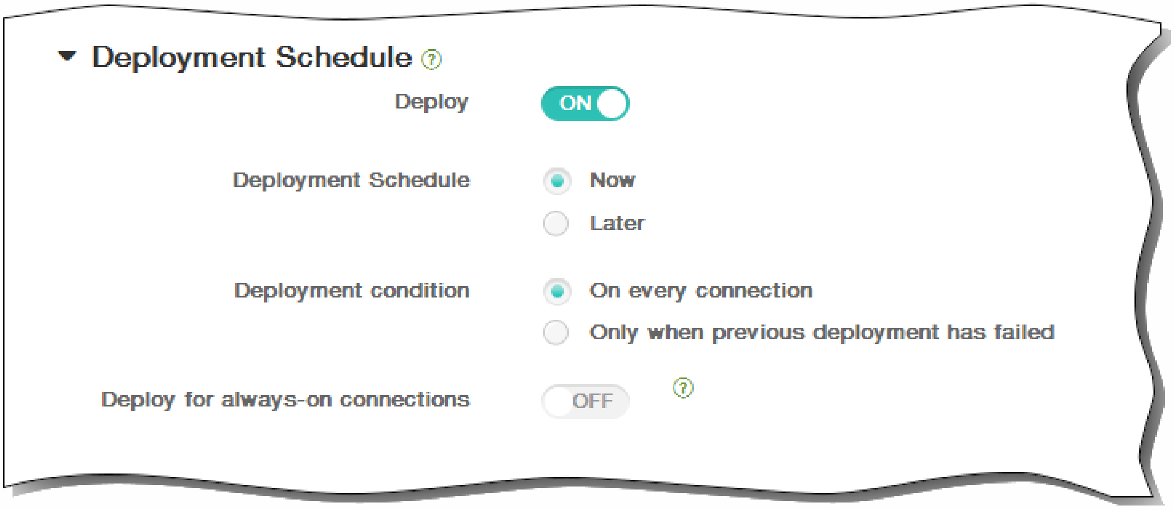
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



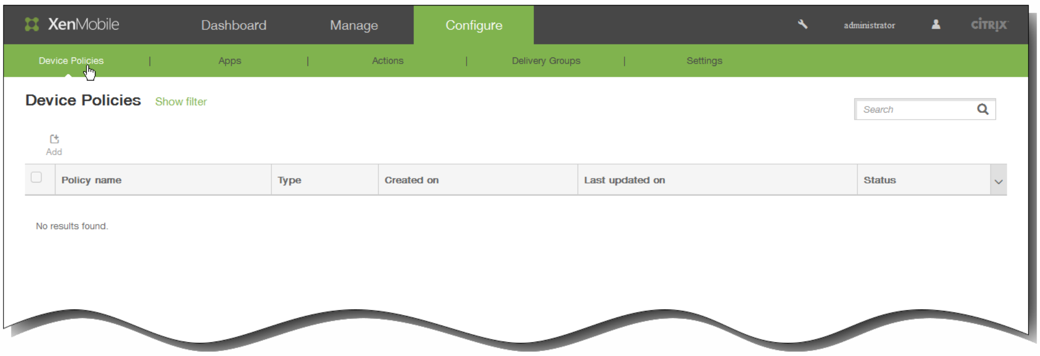
Deployment Schedule

Deploy: ON

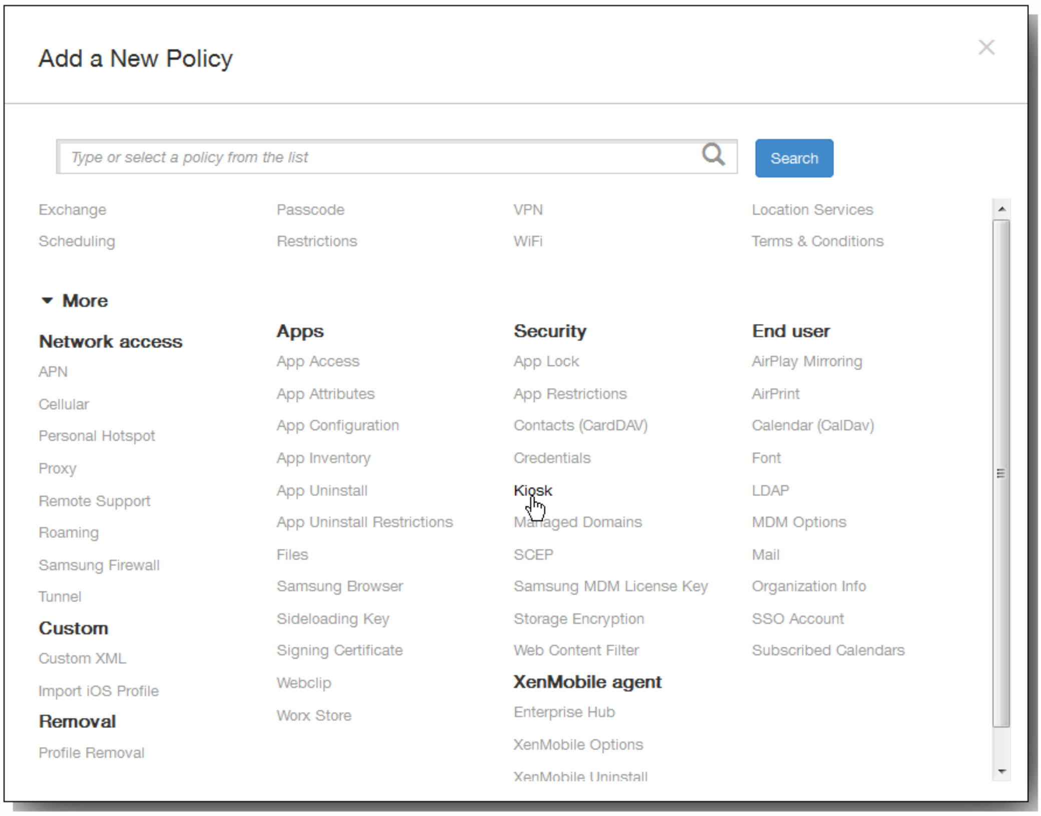
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF



No results found.



Add a New Policy

Type or select a policy from the list | Search

Exchange | Passcode | VPN | Location Services
Scheduling | Restrictions | WiFi | Terms & Conditions

▾ More

Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel

Custom
Custom XML
Import iOS Profile

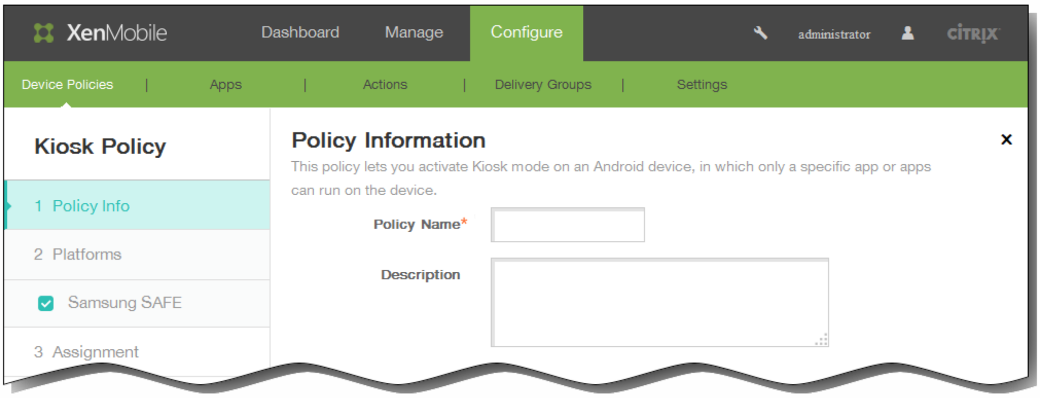
Removal
Profile Removal

Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store

Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter

XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall

End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars



Kiosk Policy

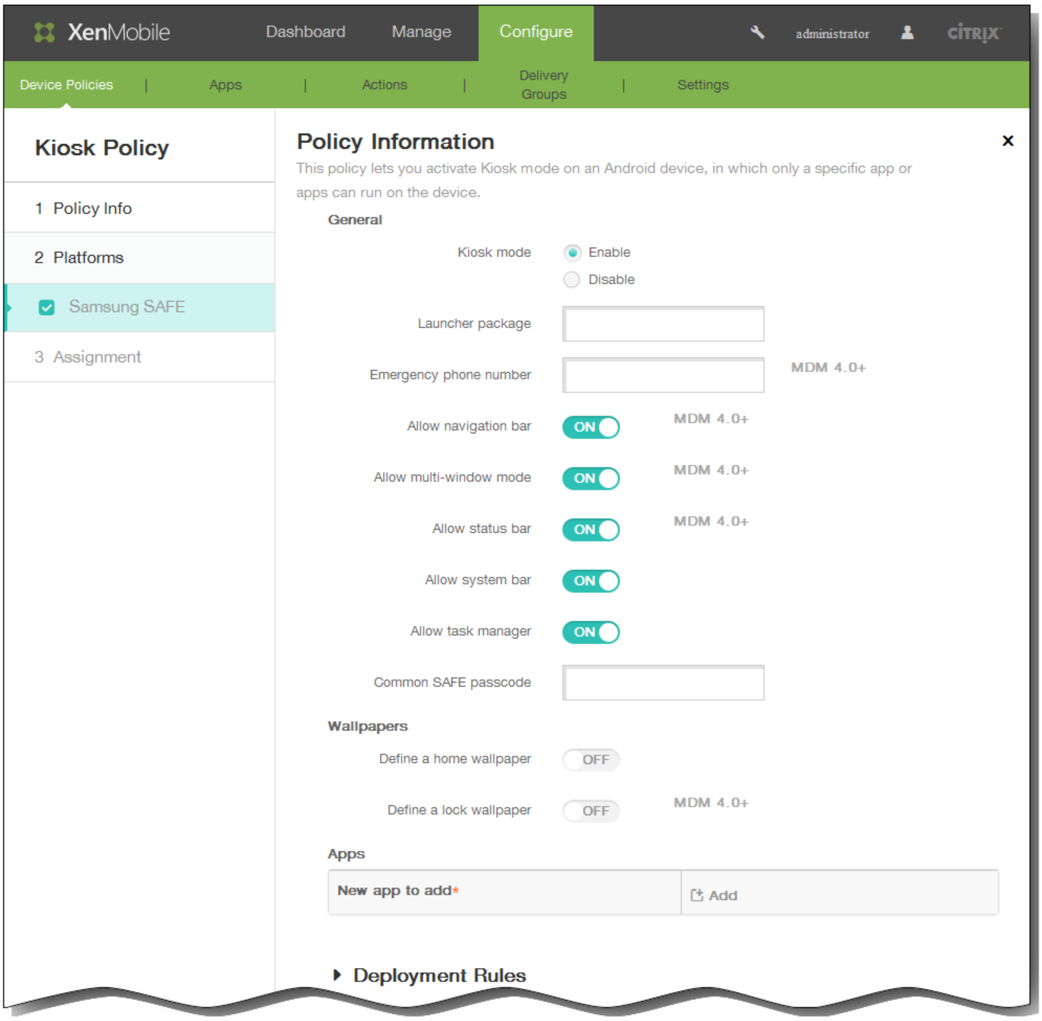
1 Policy Info
2 Platforms
☑ Samsung SAFE
3 Assignment

Policy Information

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

Policy Name*

Description



Kiosk Policy

1 Policy Info

2 Platforms

☑ Samsung SAFE

3 Assignment

Policy Information

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

General

Kiosk mode: ● Enable ○ Disable

Launcher package:

Emergency phone number: MDM 4.0+

Allow navigation bar: ON MDM 4.0+

Allow multi-window mode: ON MDM 4.0+

Allow status bar: ON MDM 4.0+

Allow system bar: ON

Allow task manager: ON

Common SAFE passcode:

Wallpapers

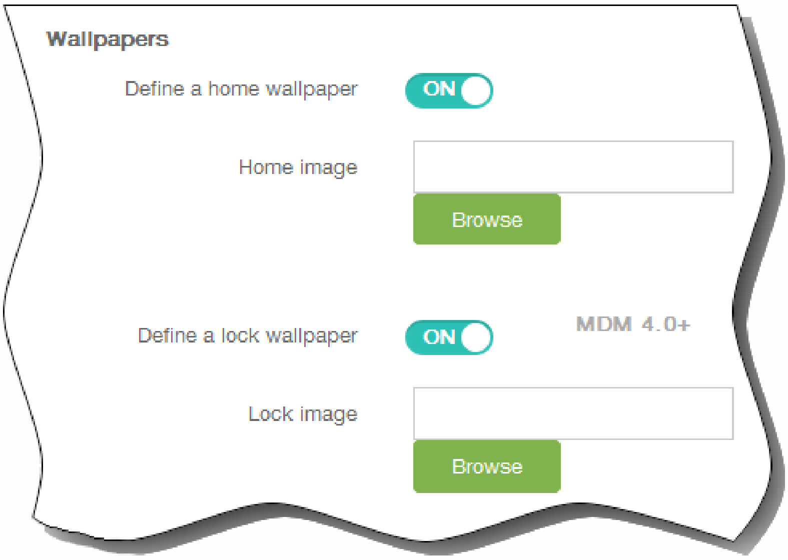
Define a home wallpaper: OFF

Define a lock wallpaper: OFF MDM 4.0+

Apps

New app to add*	Add

▸ Deployment Rules



Wallpapers

Define a home wallpaper: ON

Home image

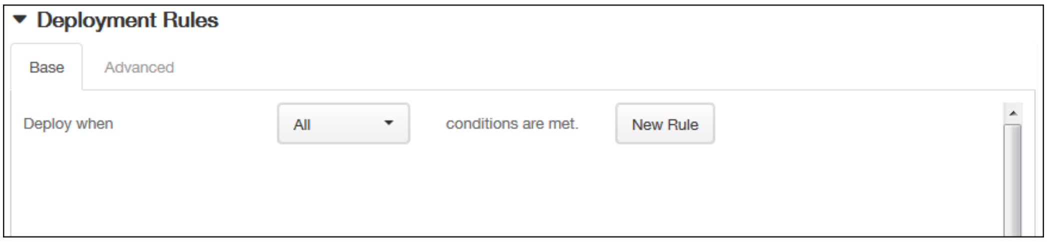
Browse

Define a lock wallpaper: ON

MDM 4.0+

Lock image

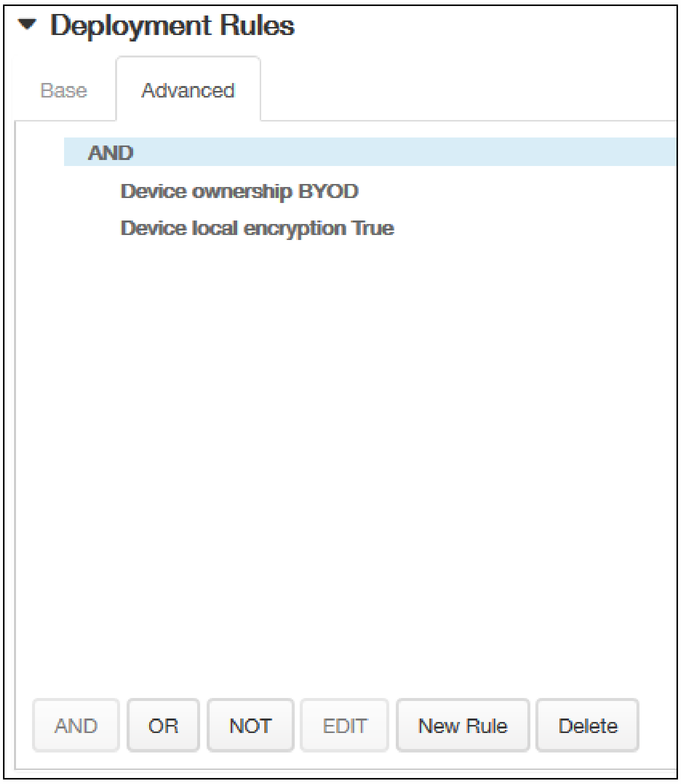
Browse



Deployment Rules

Base | Advanced

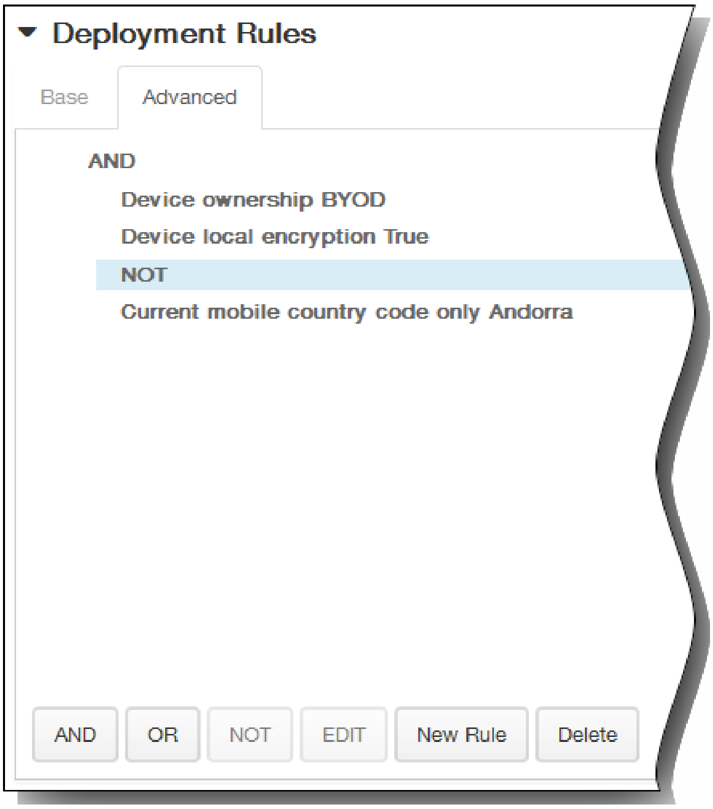
Deploy when All conditions are met.



AND

Device ownership BYOD

Device local encryption True



Deployment Rules

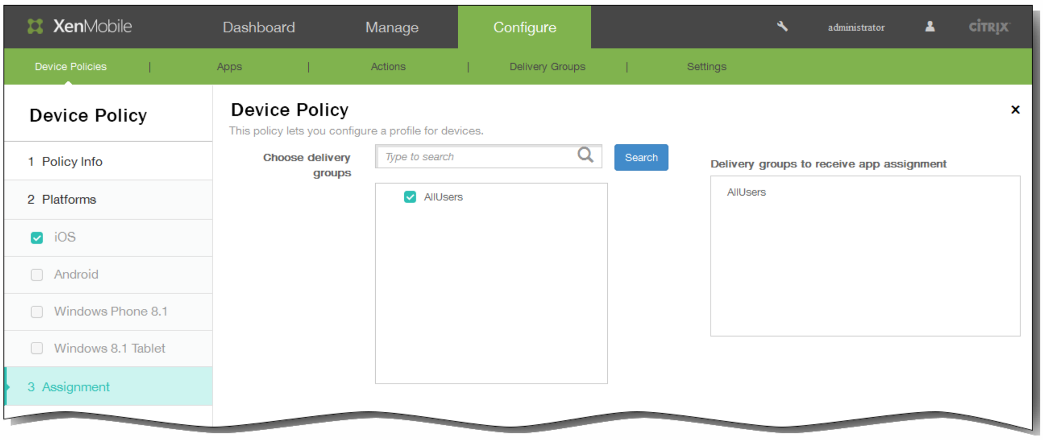
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

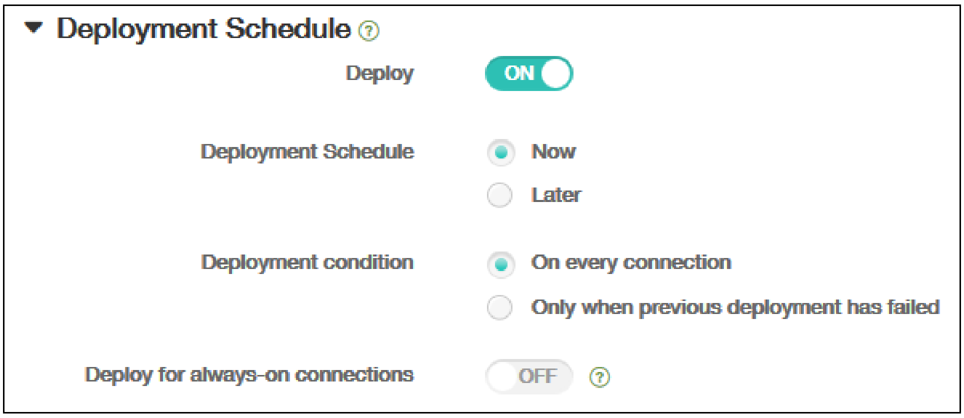
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



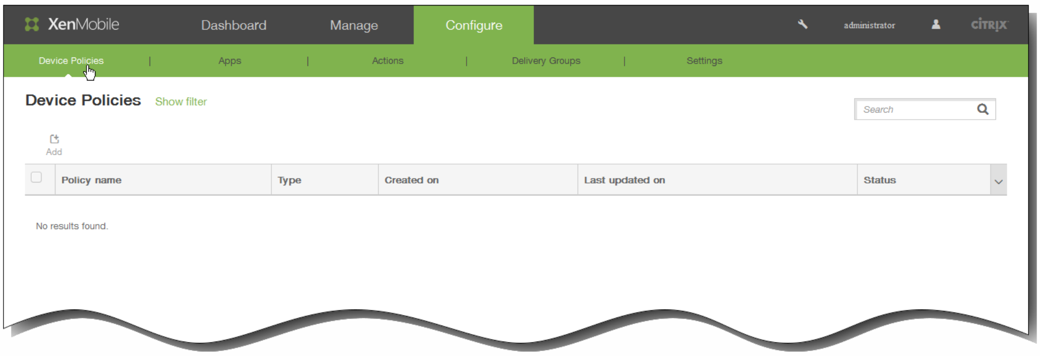
Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

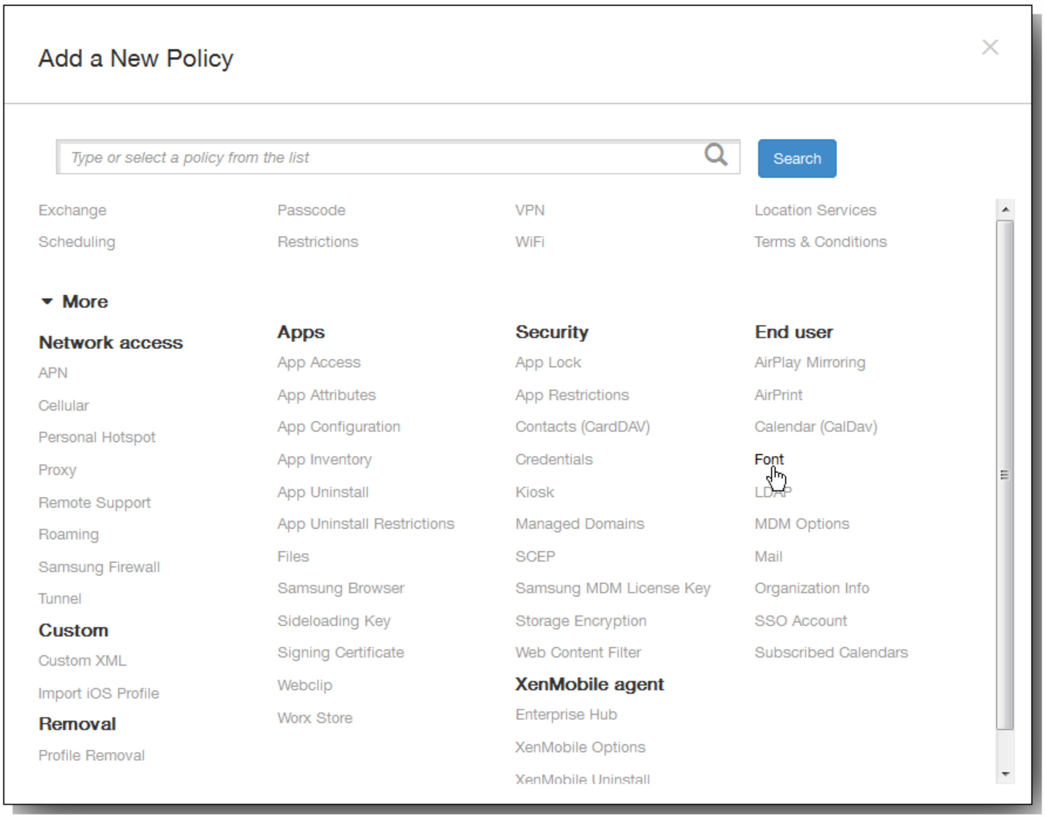
Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF

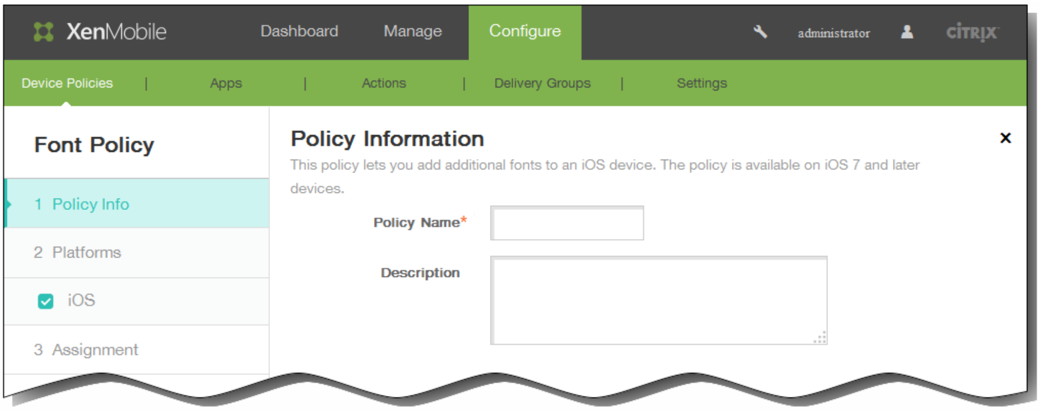


Device Policies

No results found.



Add a New Policy



XenMobile
Dashboard
Manage
Configure
administrator
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings

Font Policy

1 Policy Info

2 Platforms

☑ iOS

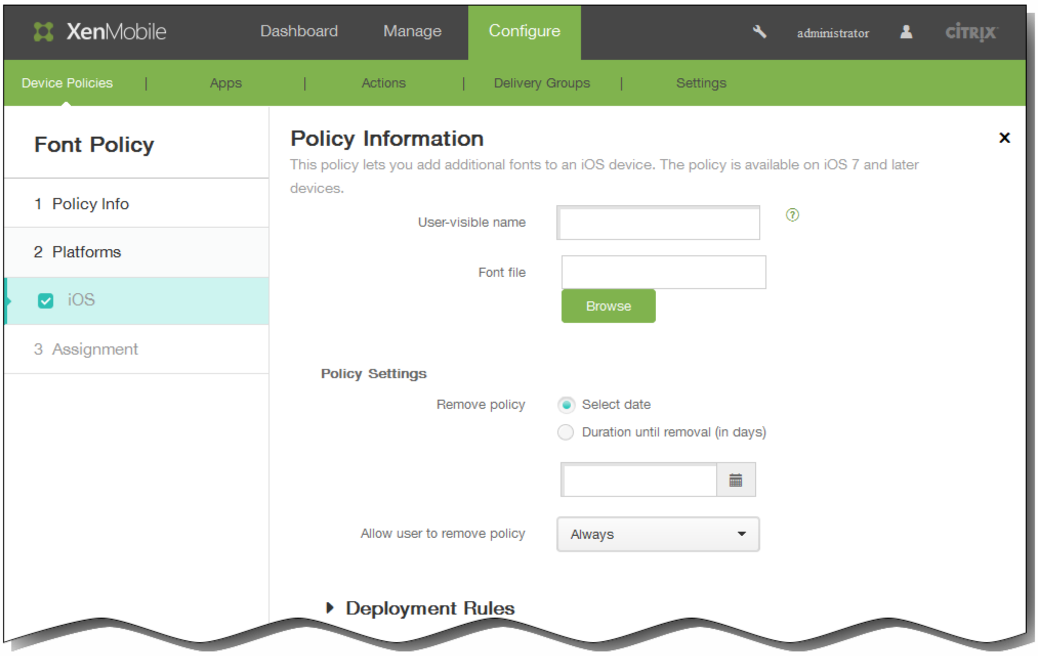
3 Assignment

Policy Information

This policy lets you add additional fonts to an iOS device. The policy is available on iOS 7 and later devices.

Policy Name*

Description



XenMobile
Dashboard
Manage
Configure
administrator
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings

Font Policy

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

Policy Information

This policy lets you add additional fonts to an iOS device. The policy is available on iOS 7 and later devices.

User-visible name

Font file

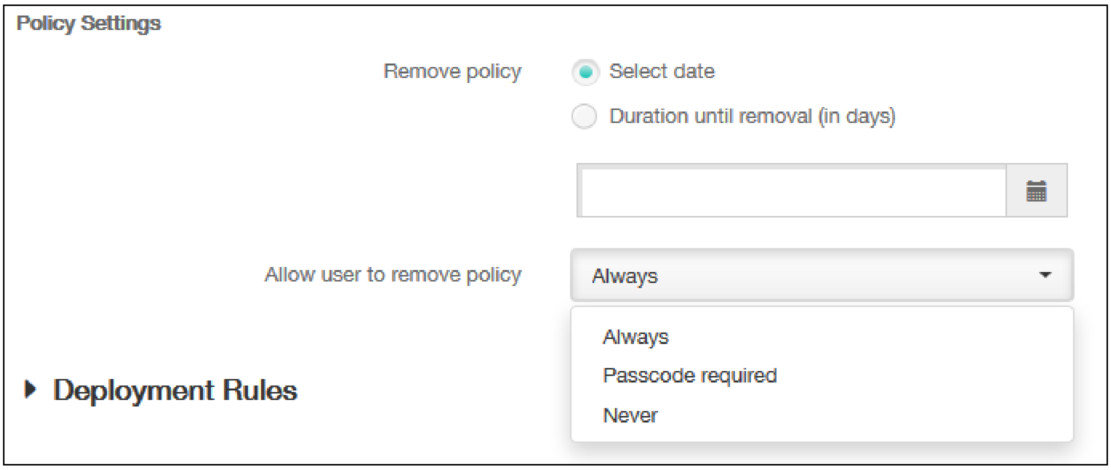
Browse

Policy Settings

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

Allow user to remove policy: Always

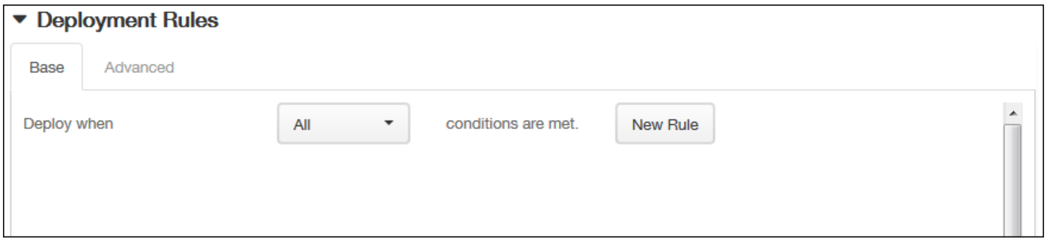
Deployment Rules



Policy Settings

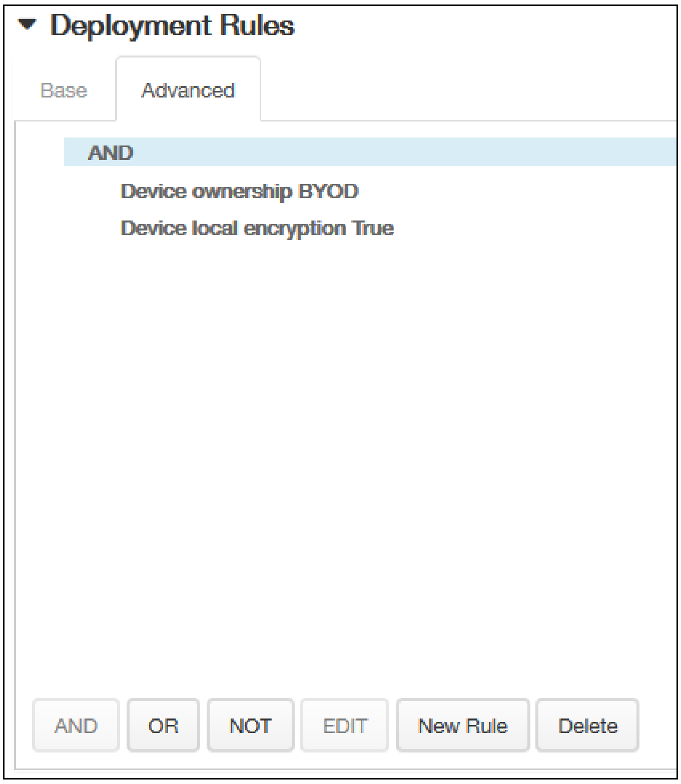
Remove policy ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always



Deployment Rules

Deploy when All conditions are met.



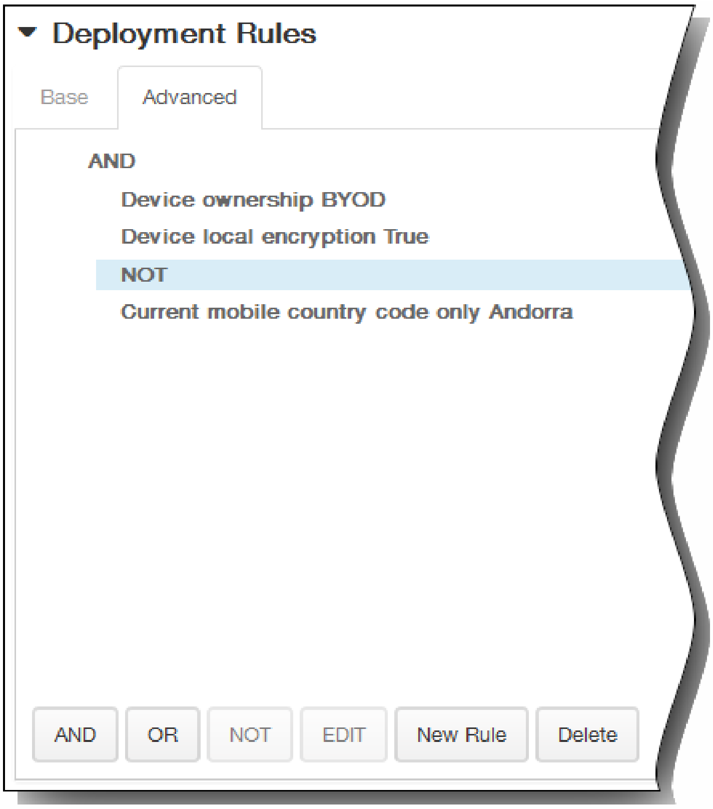
Deployment Rules

Base | Advanced

AND

Device ownership BYOD

Device local encryption True



Deployment Rules

Base | Advanced

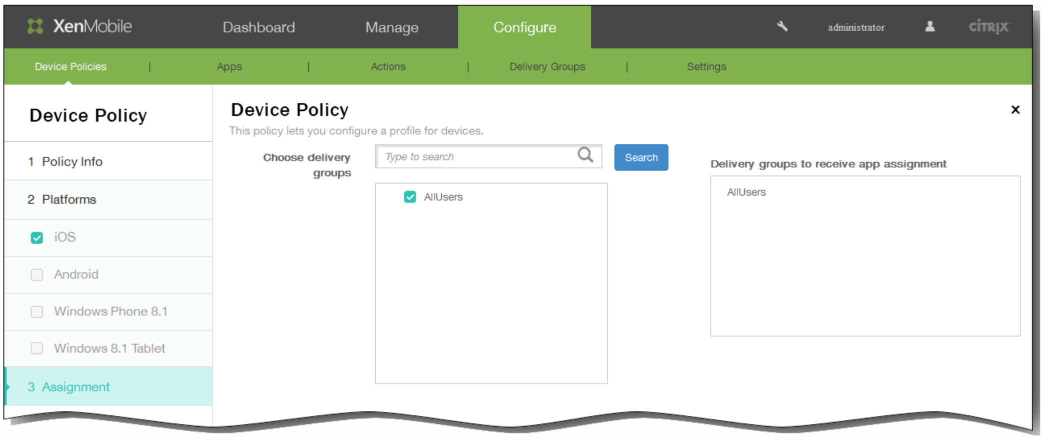
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

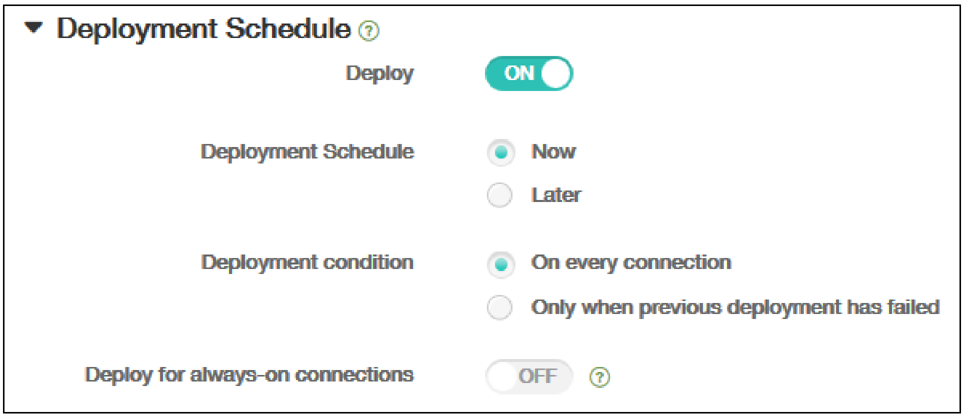
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search | Search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers

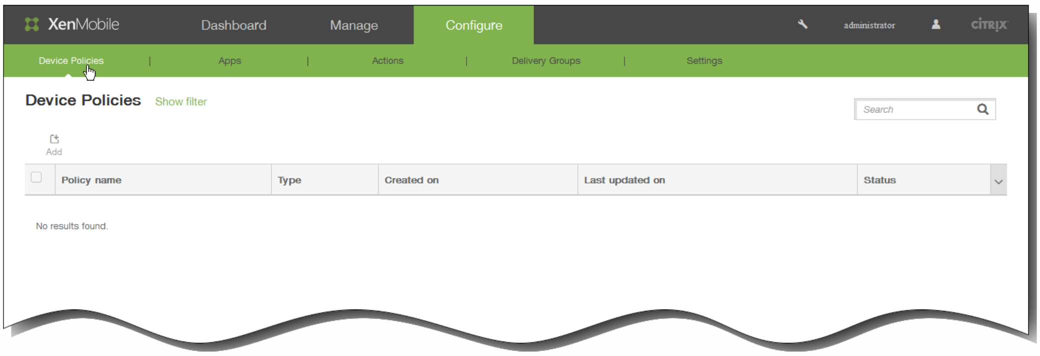


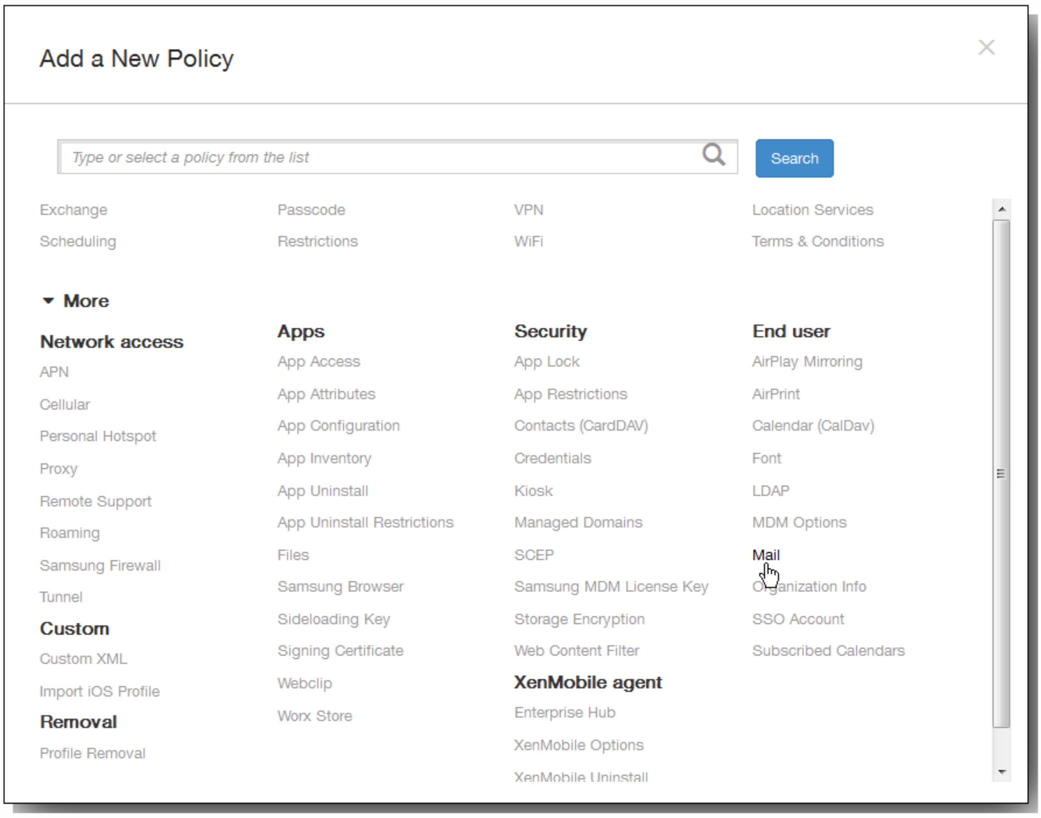
Deploy: ON

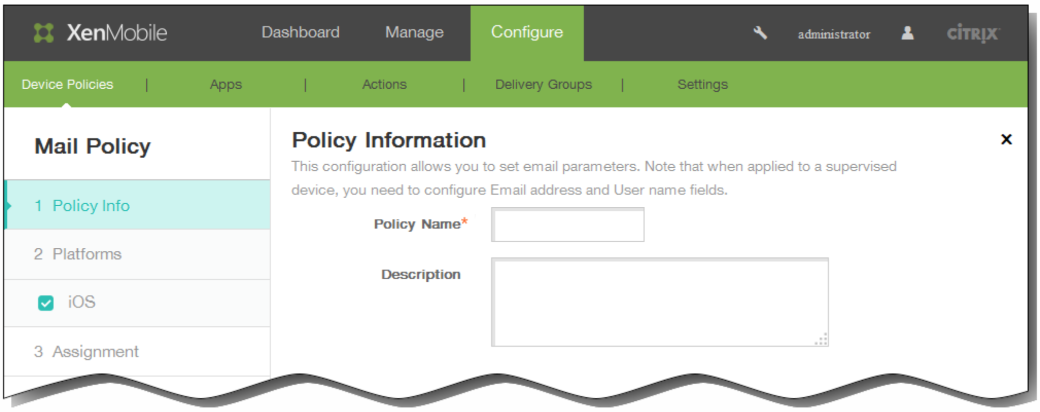
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF ?


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies
Apps
Actions
Delivery Groups
Settings
Device Policies
Show filter
Search
Add
Policy name
Type
Created on
Last updated on
Status
No results found.


Add a New Policy
Type or select a policy from the list
Search
Exchange
Scheduling
Passcode
Restrictions
VPN
WiFi
Location Services
Terms & Conditions
More
Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel
Custom
Custom XML
Import iOS Profile
Removal
Profile Removal
Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store
Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter
XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall
End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars

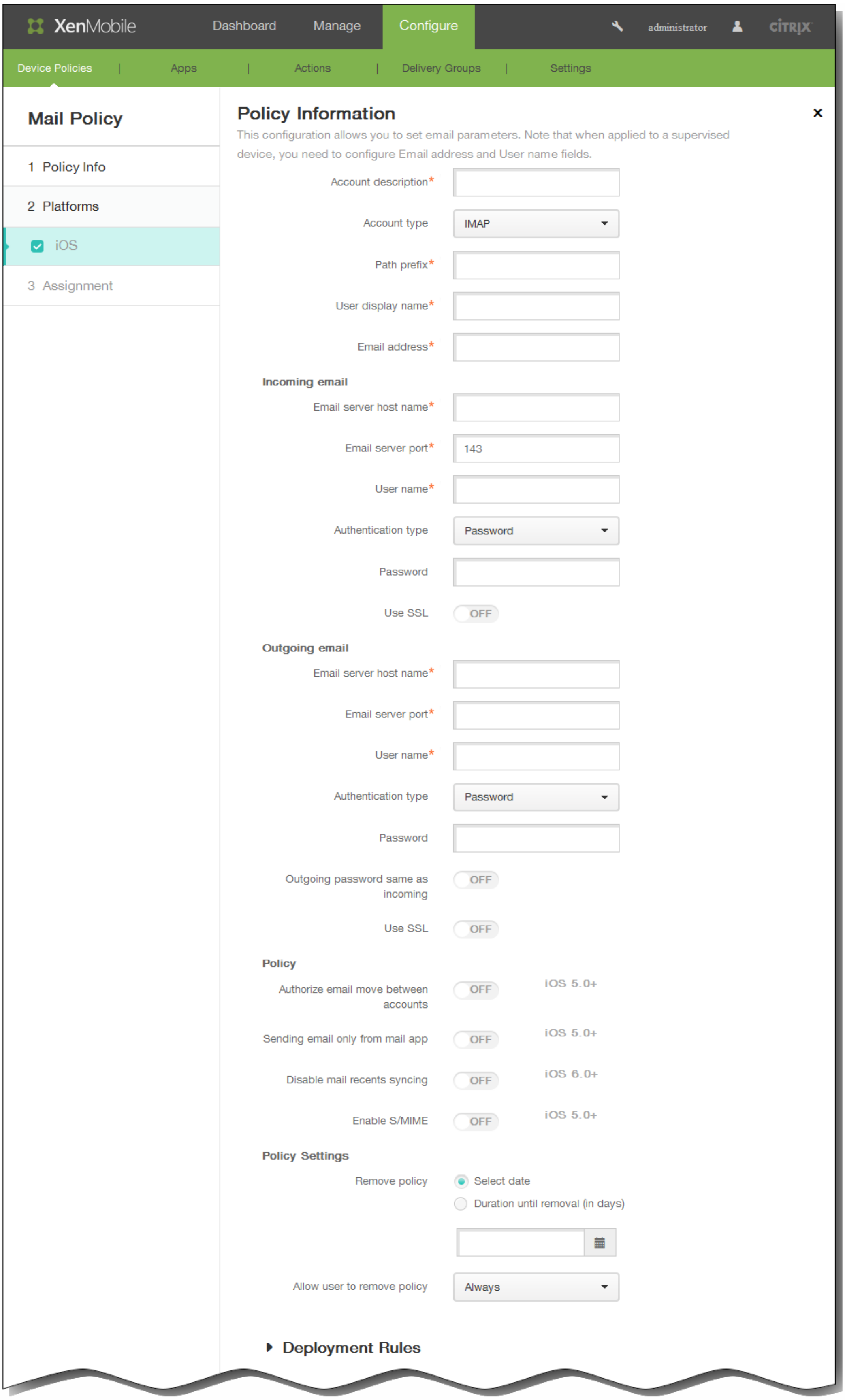


Policy Information

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.

Policy Name*

Description



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

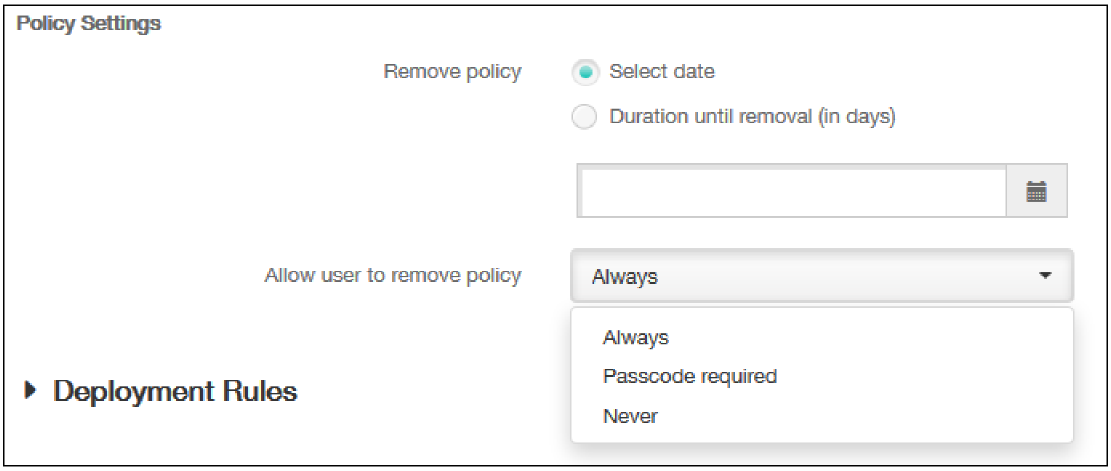
Authorize email move between accounts	OFF	iOS 5.0+
Sending email only from mail app	OFF	iOS 5.0+
Disable mail recents syncing	OFF	iOS 6.0+
Enable S/MIME	OFF	iOS 5.0+

Policy Settings

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

Allow user to remove policy: Always

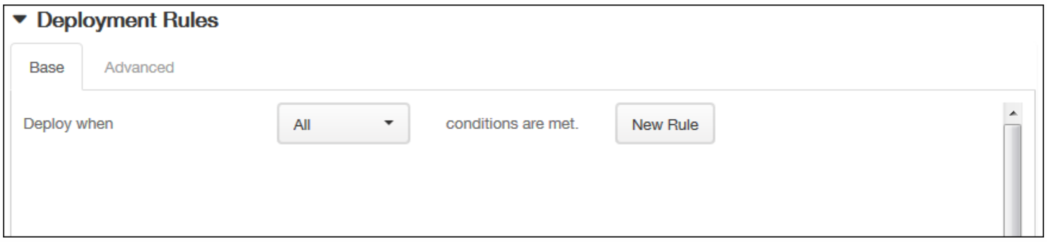
▸ Deployment Rules



Policy Settings

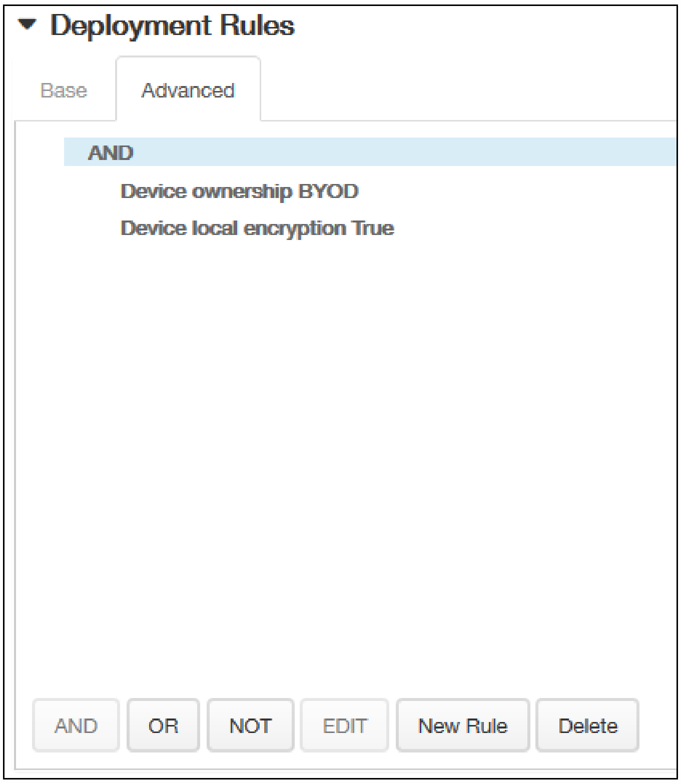
Remove policy ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always



Deployment Rules

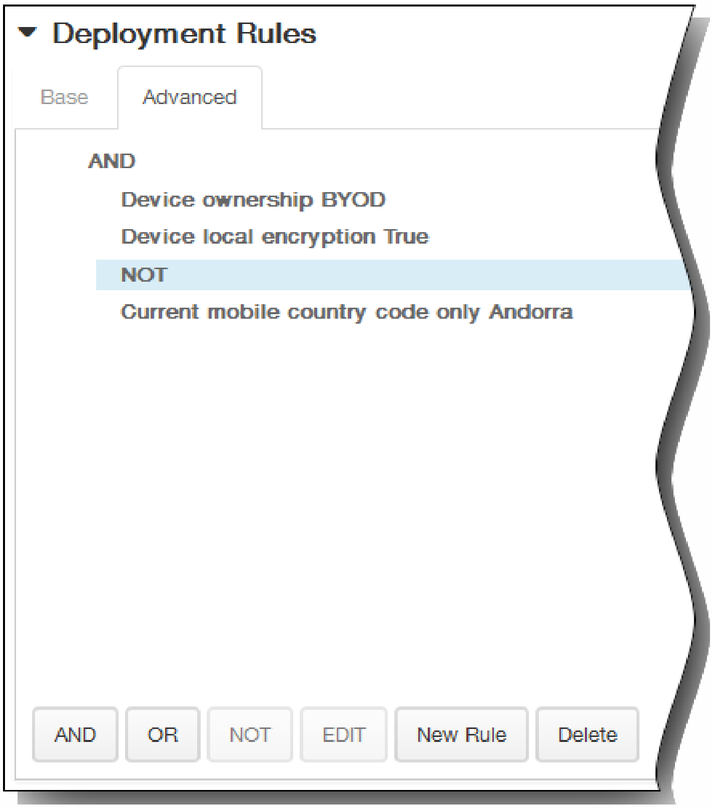
Deploy when All conditions are met.



AND

Device ownership BYOD

Device local encryption True


Deployment Rules

Base | Advanced

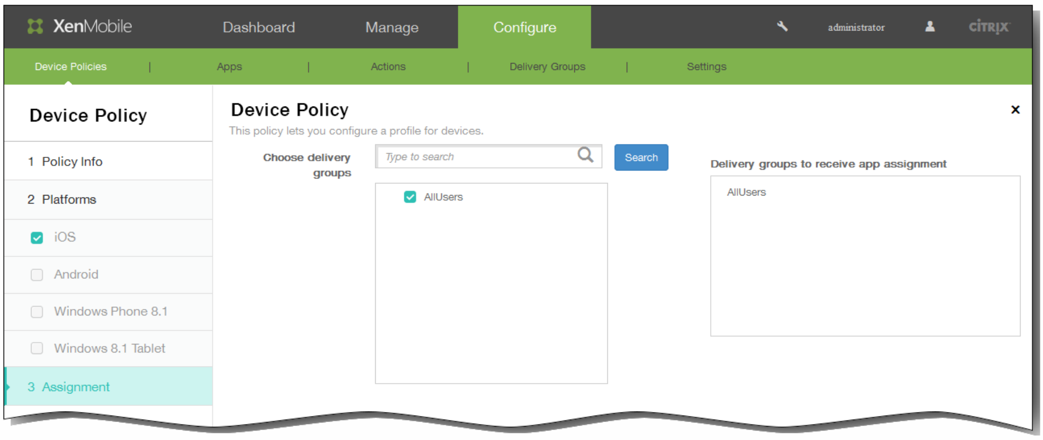
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

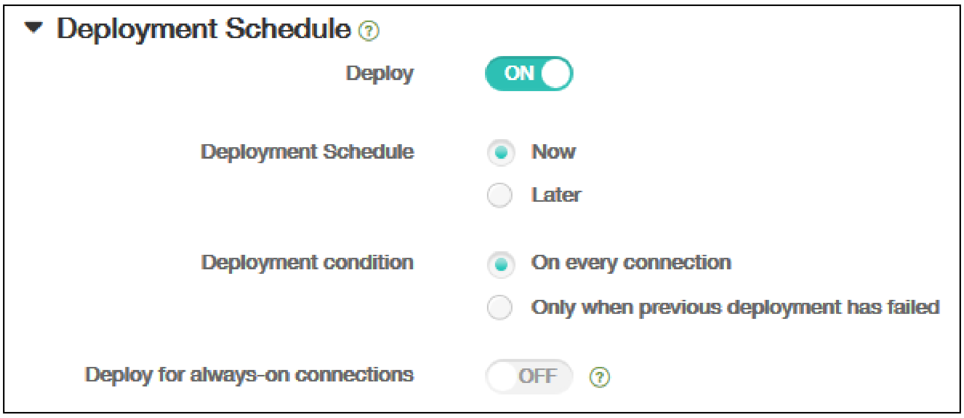
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



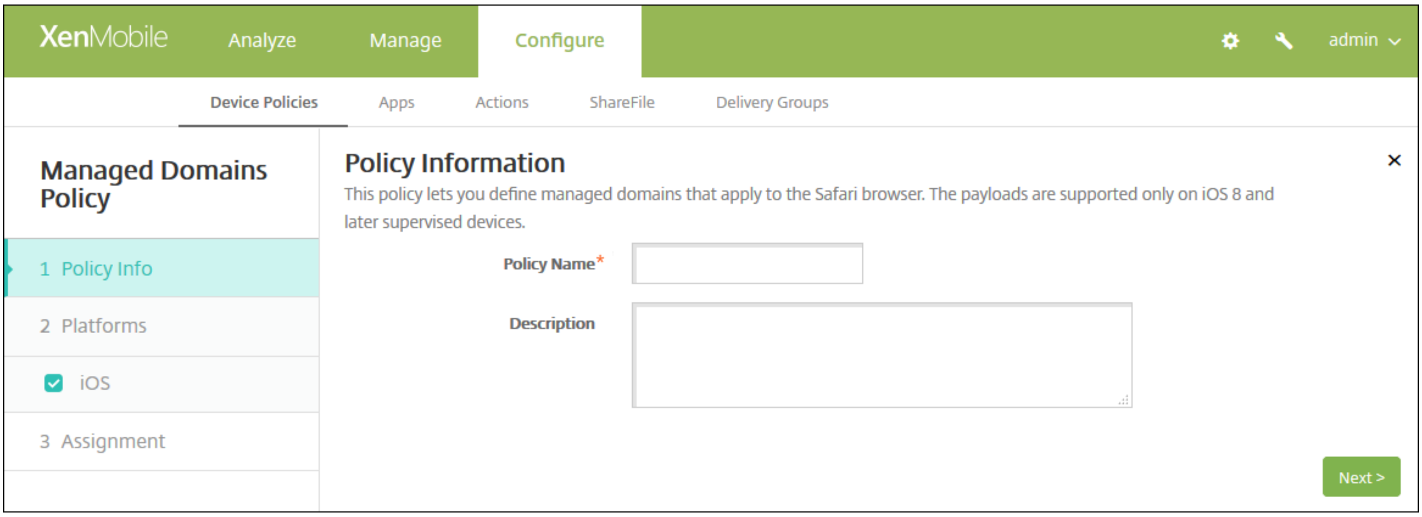
▼ Deployment Schedule ?

Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF ?



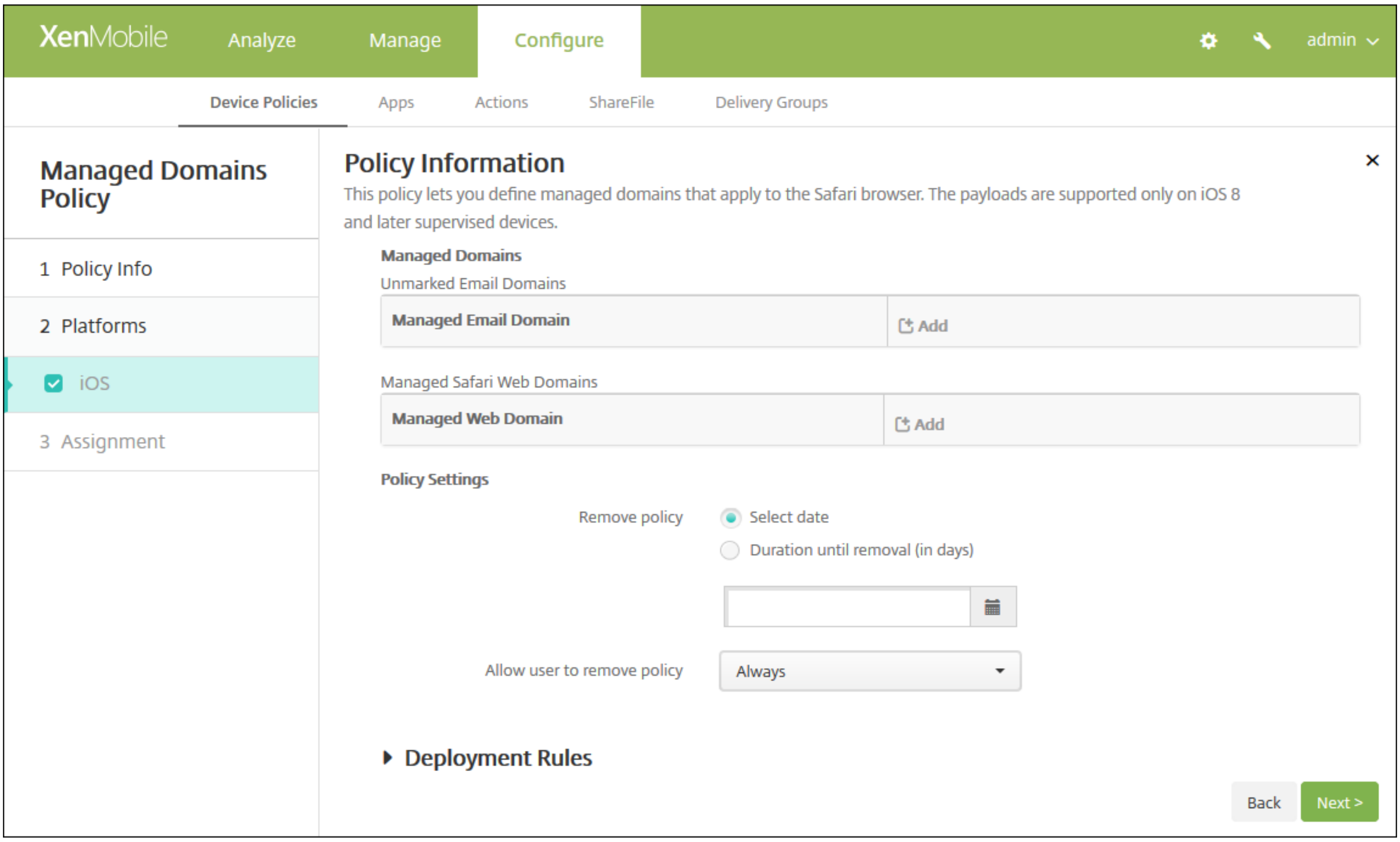
Managed Domains Policy

Policy Information

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

Policy Name*

Description



Policy Information

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

Managed Domains

Unmarked Email Domains

Managed Email Domain	Add

Managed Safari Web Domains

Managed Web Domain	Add

Policy Settings

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

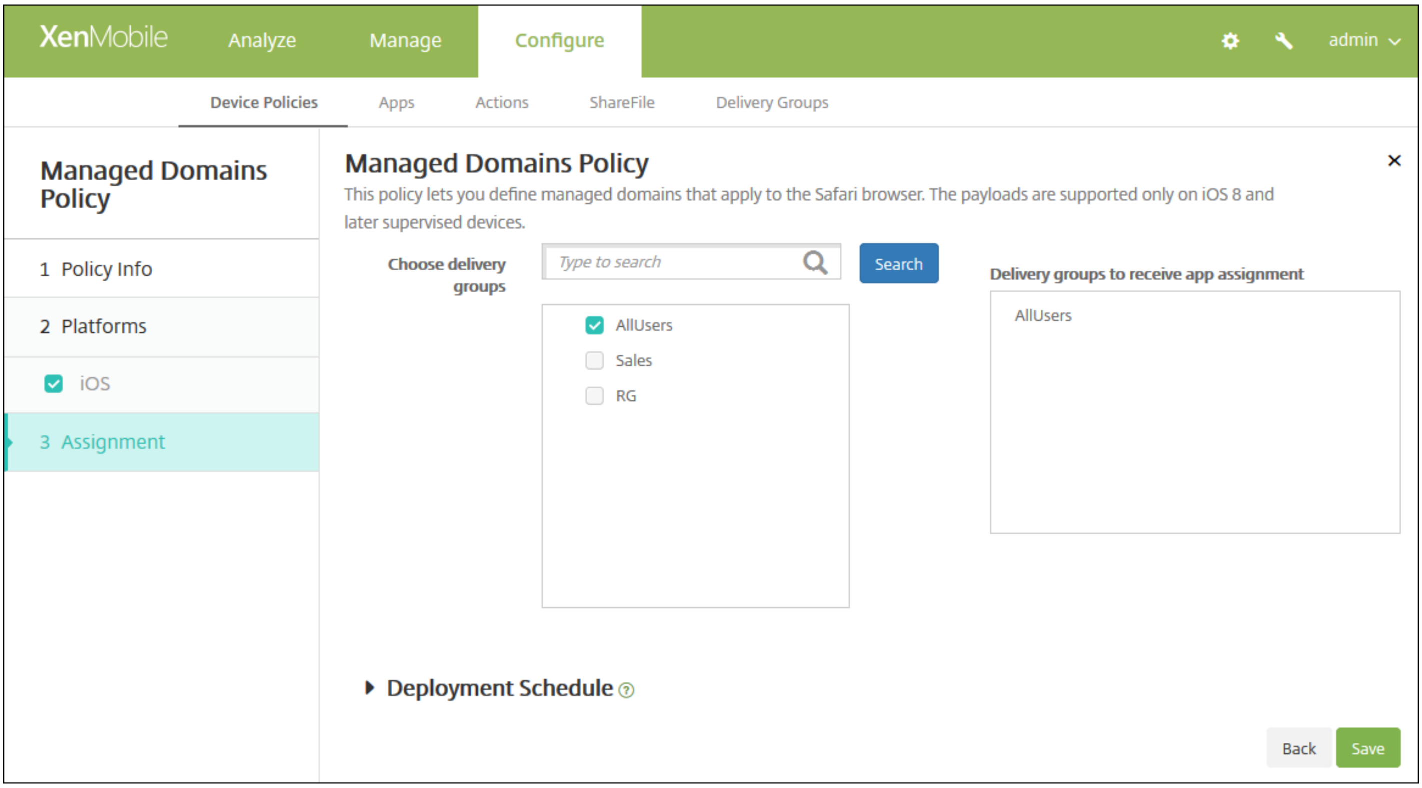
Allow user to remove policy: Always

Deployment Rules

How to specify domains

-
-
-

7. Configure the deployment rules



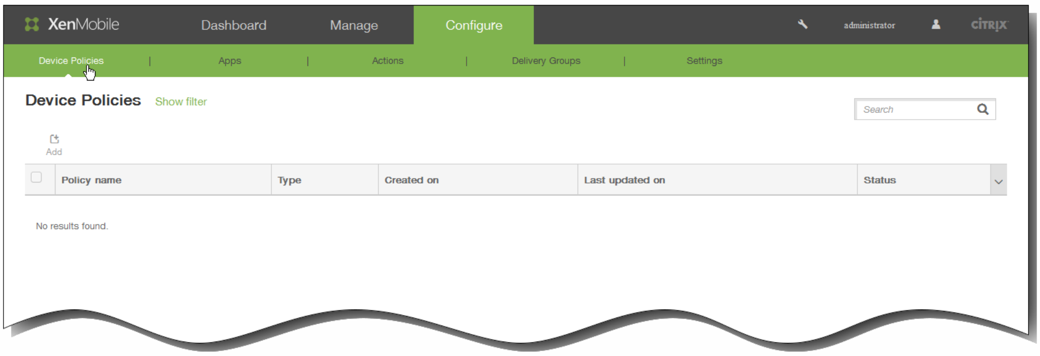
Managed Domains Policy

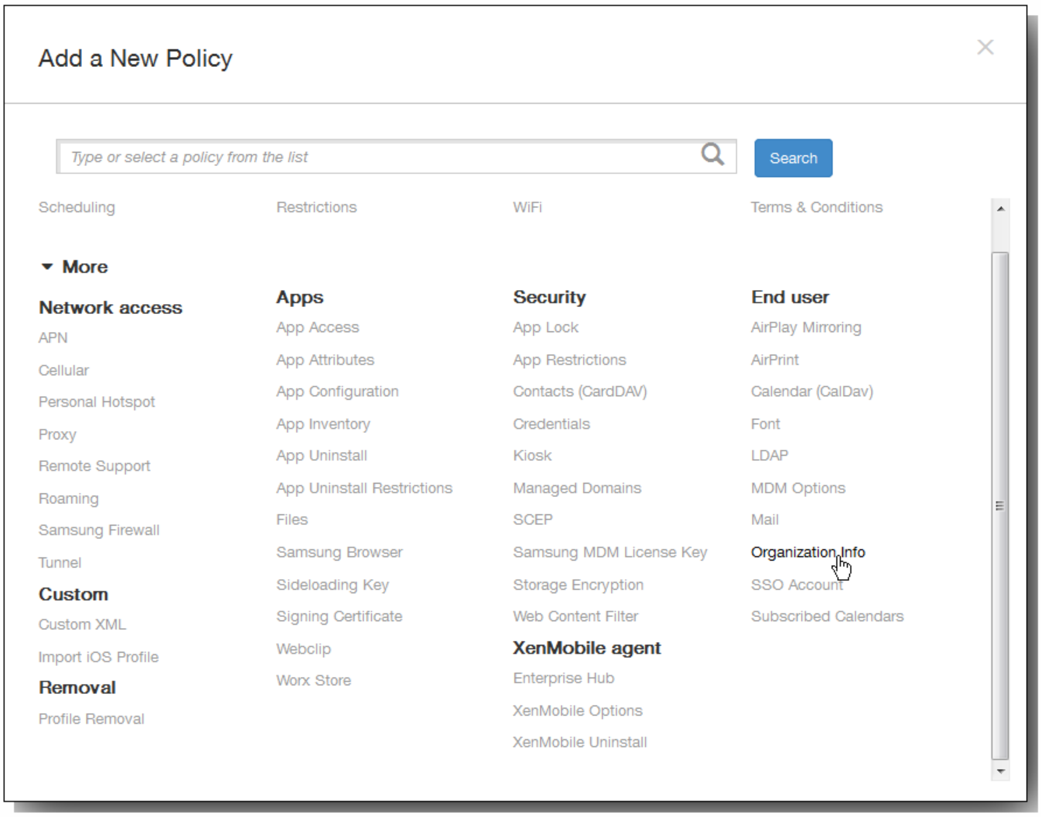
This policy lets you define managed domains that apply to the Safari browser. The payloads are supported only on iOS 8 and later supervised devices.

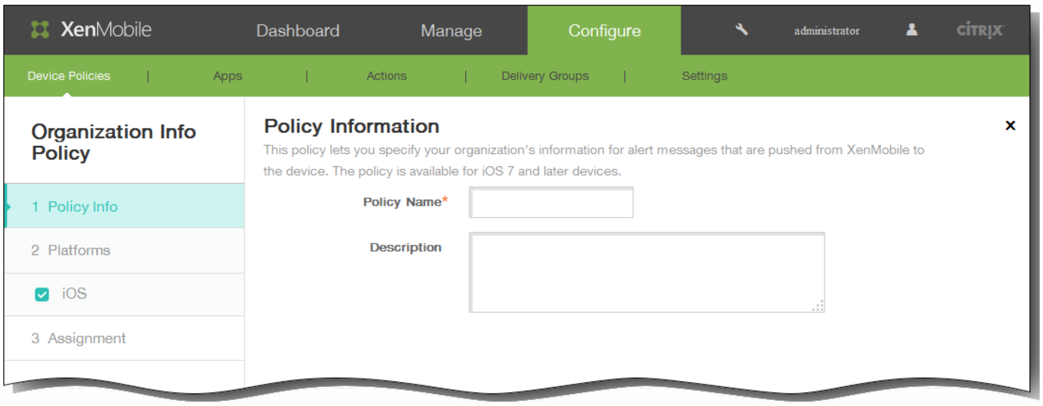
Choose delivery groups: ☑ AllUsers, □ Sales, □ RG

Delivery groups to receive app assignment: AllUsers

-
-
-
-
-
-
-


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies
Apps
Actions
Delivery Groups
Settings
Device Policies
Show filter
Search
Add
Policy name
Type
Created on
Last updated on
Status
No results found.


Add a New Policy
Type or select a policy from the list
Search
Scheduling
Restrictions
WiFi
Terms & Conditions
More
Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel
Custom
Custom XML
Import iOS Profile
Removal
Profile Removal
Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store
Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter
XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall
End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars



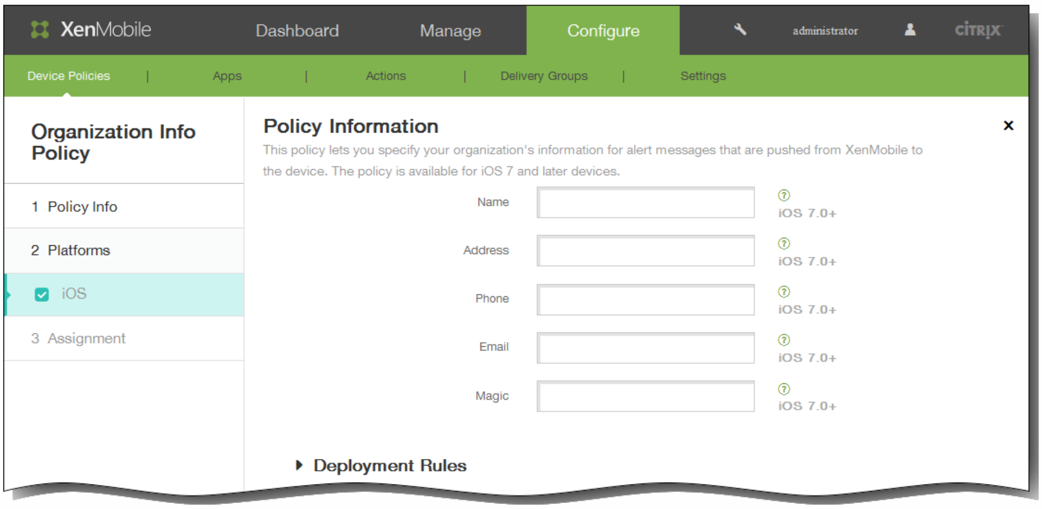
Organization Info Policy

Policy Information

This policy lets you specify your organization's information for alert messages that are pushed from XenMobile to the device. The policy is available for iOS 7 and later devices.

Policy Name*

Description

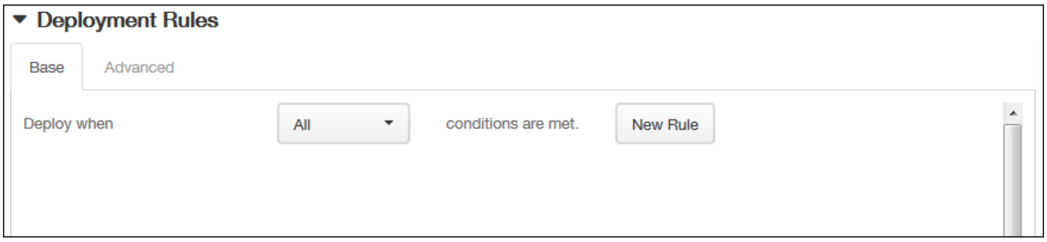


Organization Info Policy

Policy Information

This policy lets you specify your organization's information for alert messages that are pushed from XenMobile to the device. The policy is available for iOS 7 and later devices.

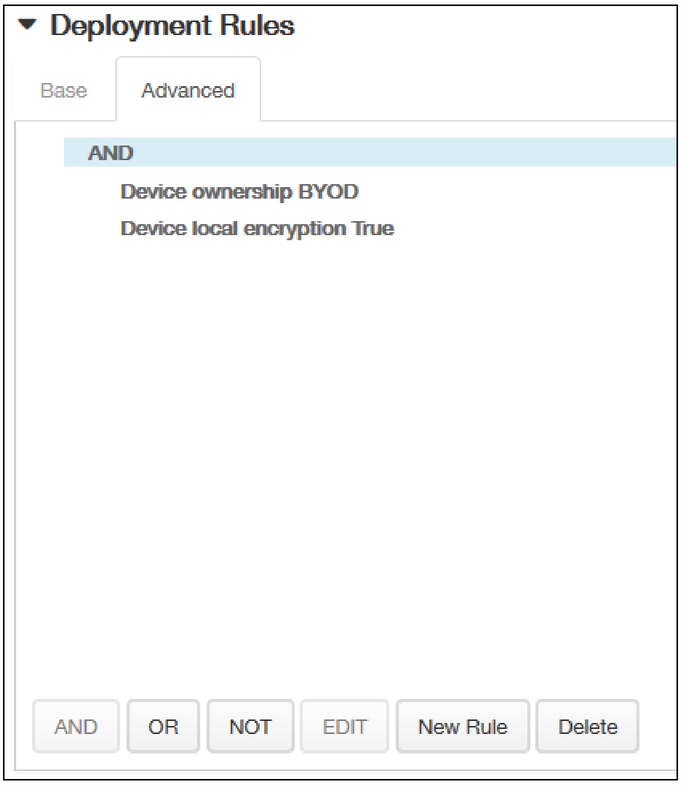
Name	iOS 7.0+
Address	iOS 7.0+
Phone	iOS 7.0+
Email	iOS 7.0+
Magic	iOS 7.0+



Deployment Rules

Base | Advanced

Deploy when All conditions are met.



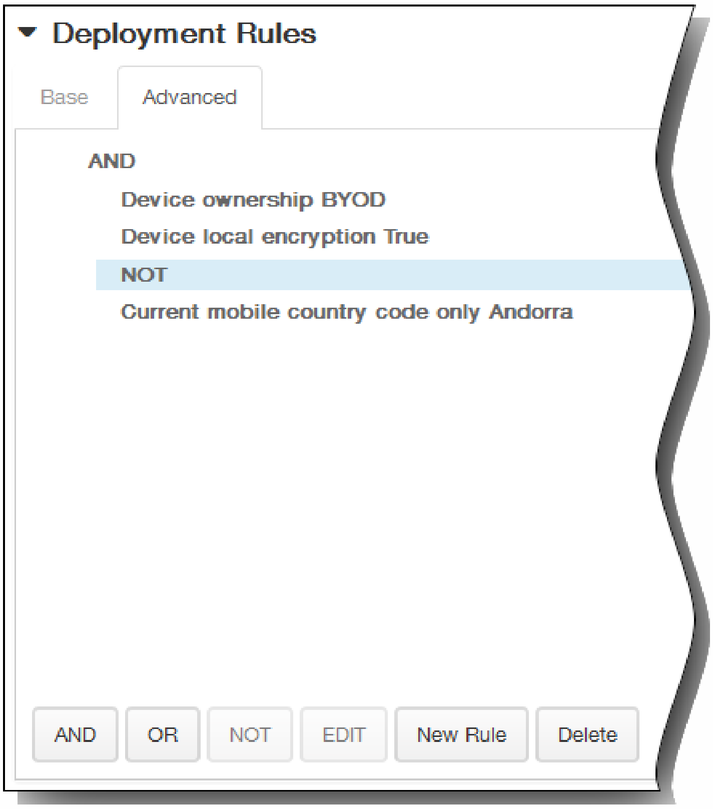
Deployment Rules

Base | Advanced

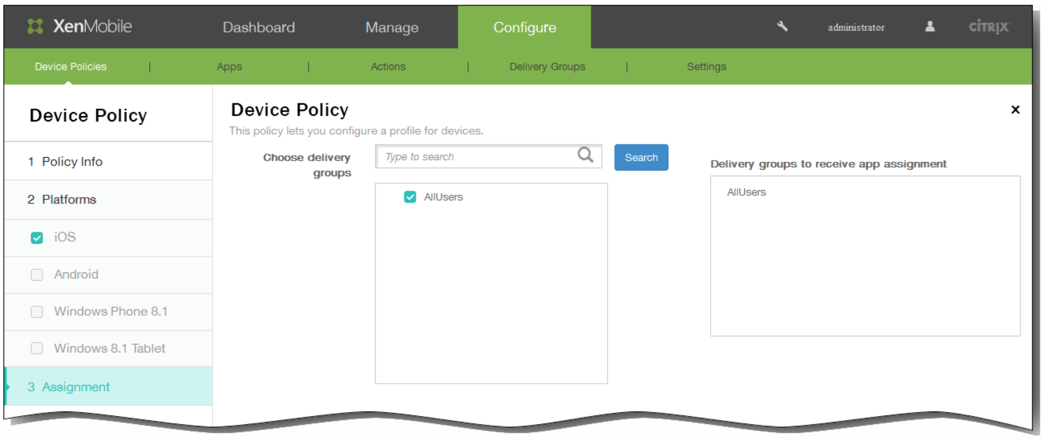
AND

Device ownership BYOD

Device local encryption True



AND
  Device ownership BYOD
  Device local encryption True
  NOT
  Current mobile country code only Andorra

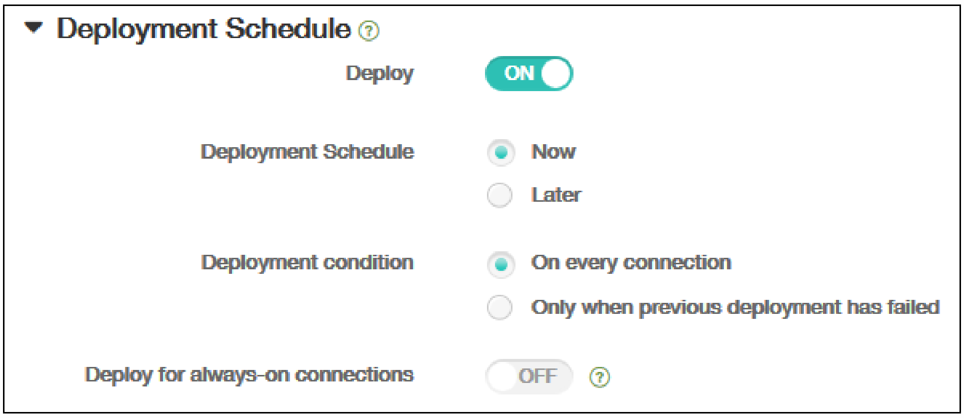


Device Policy

This policy lets you configure a profile for devices.

Choose delivery groups: ☑ AllUsers

Delivery groups to receive app assignment: AllUsers



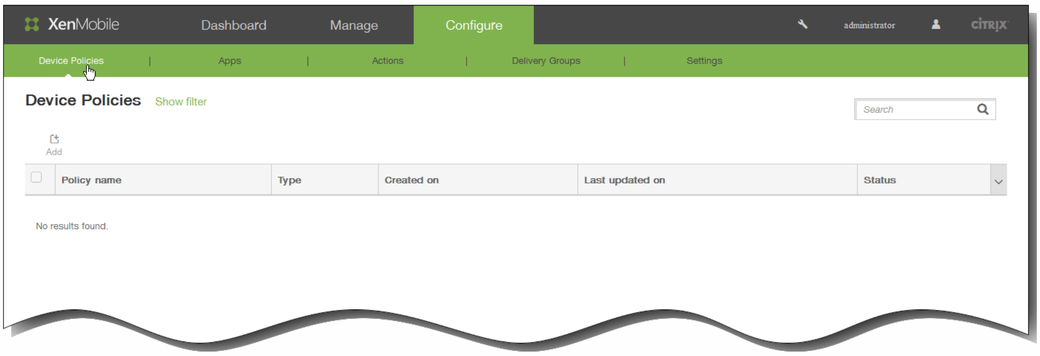
Deployment Schedule ?

Deploy: ON

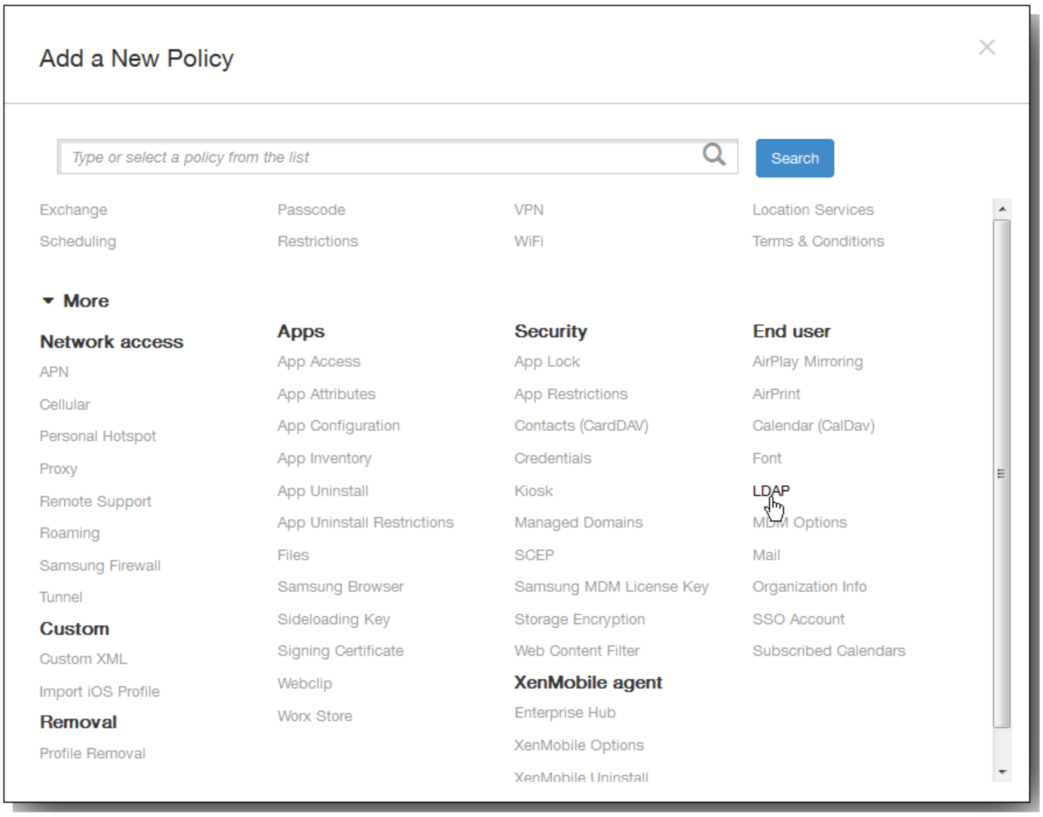
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

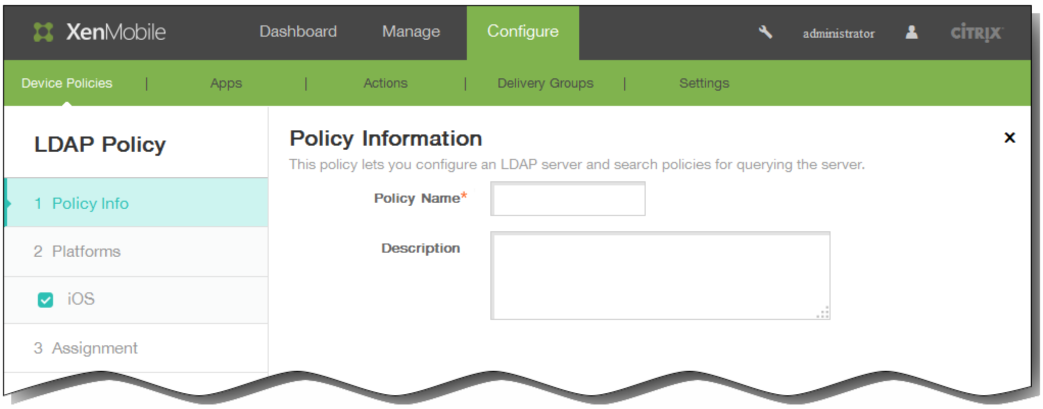
Deploy for always-on connections: OFF ?



XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies
Apps
Actions
Delivery Groups
Settings
Device Policies
Show filter
Search
Add
Policy name
Type
Created on
Last updated on
Status
No results found.



Add a New Policy
Type or select a policy from the list
Search
Exchange
Scheduling
Passcode
Restrictions
VPN
WiFi
Location Services
Terms & Conditions
More
Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel
Custom
Custom XML
Import iOS Profile
Removal
Profile Removal
Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store
Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter
XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall
End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings

LDAP Policy

1 Policy Info

2 Platforms

☑ iOS

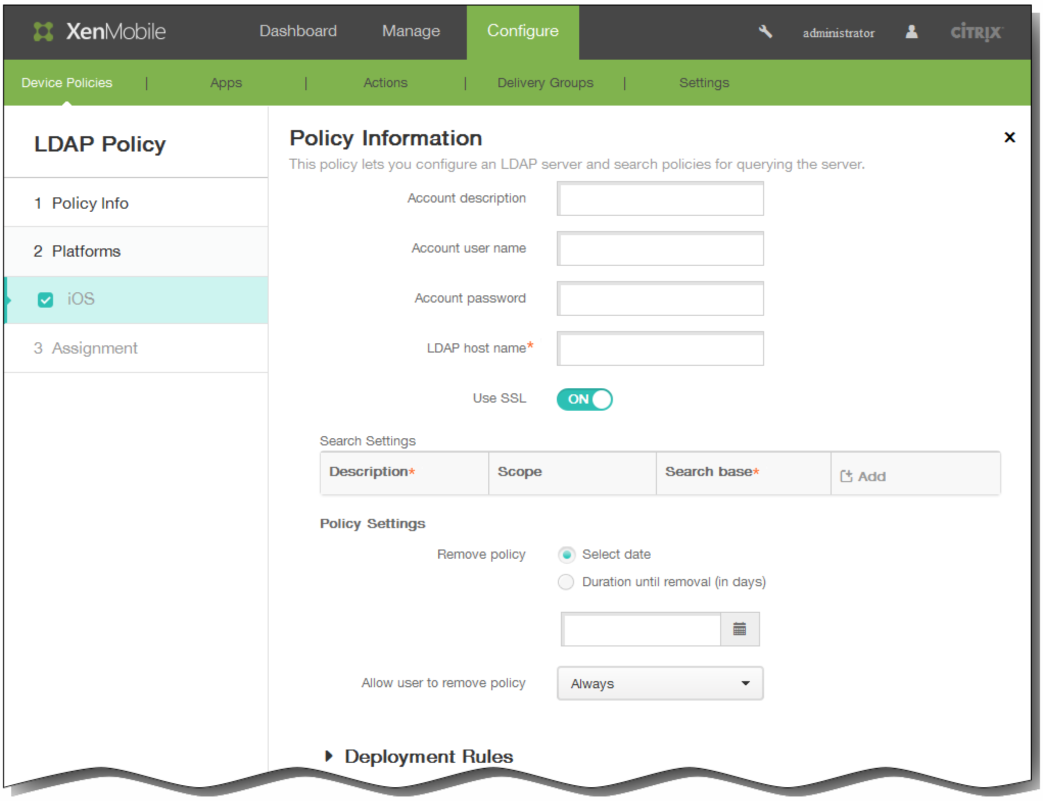
3 Assignment

Policy Information

This policy lets you configure an LDAP server and search policies for querying the server.

Policy Name*

Description


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings

LDAP Policy

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

Policy Information

This policy lets you configure an LDAP server and search policies for querying the server.

Account description

Account user name

Account password

LDAP host name*

Use SSL ON

Search Settings

Description*	Scope	Search base*	Add

Policy Settings

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

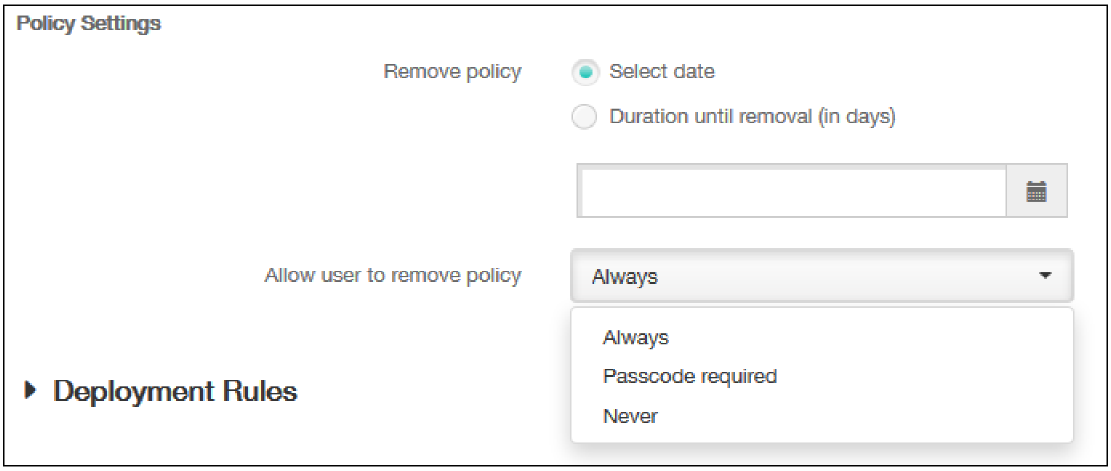
Allow user to remove policy Always

Deployment Rules

-
-
-

ou=people

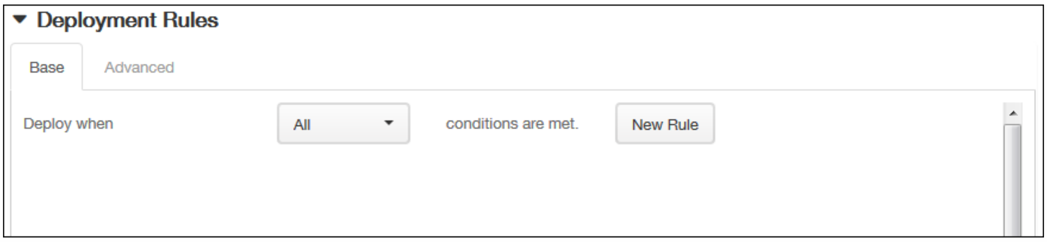
0=example corp



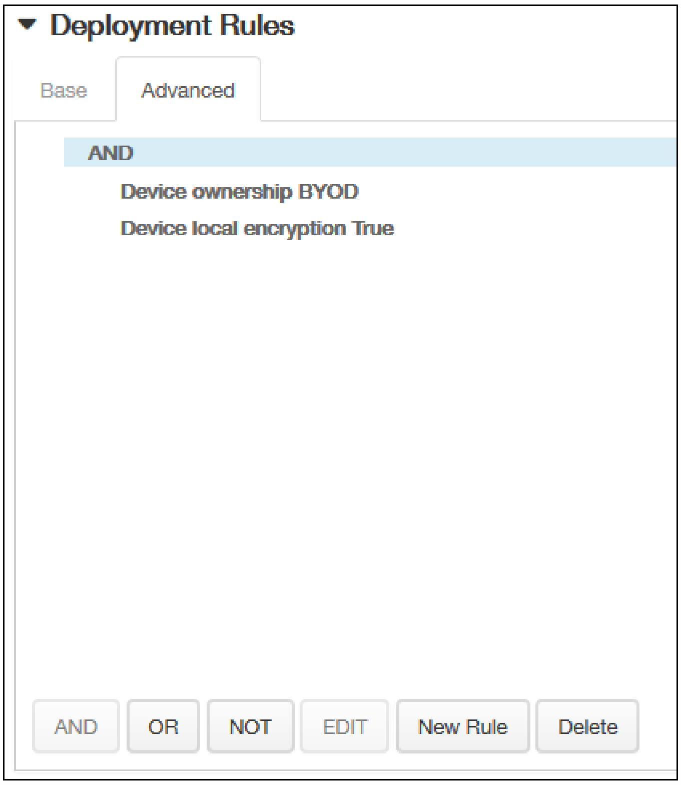
Policy Settings

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

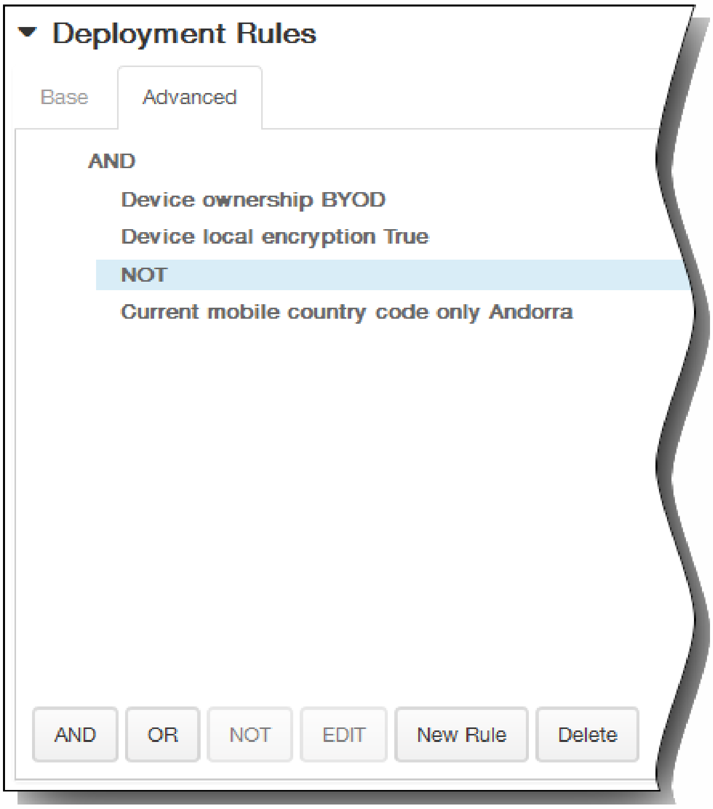
Allow user to remove policy: Always



Deploy when All conditions are met.



AND
Device ownership BYOD
Device local encryption True



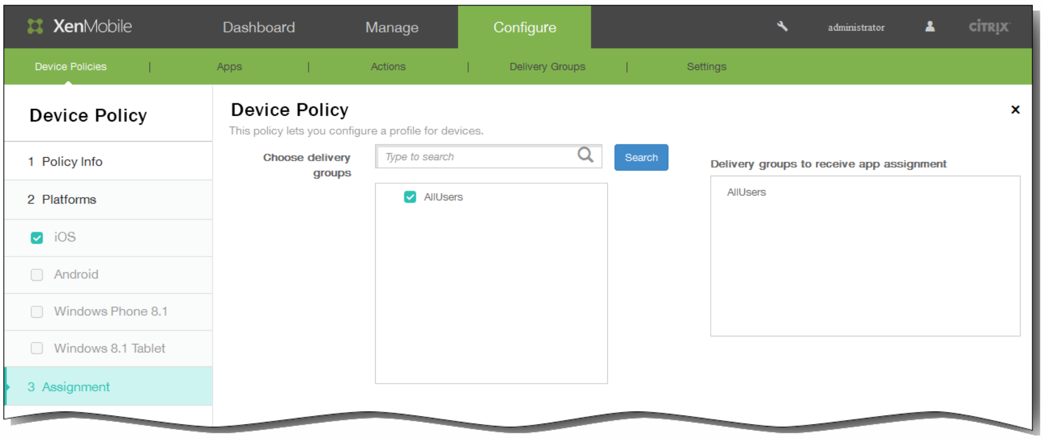
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

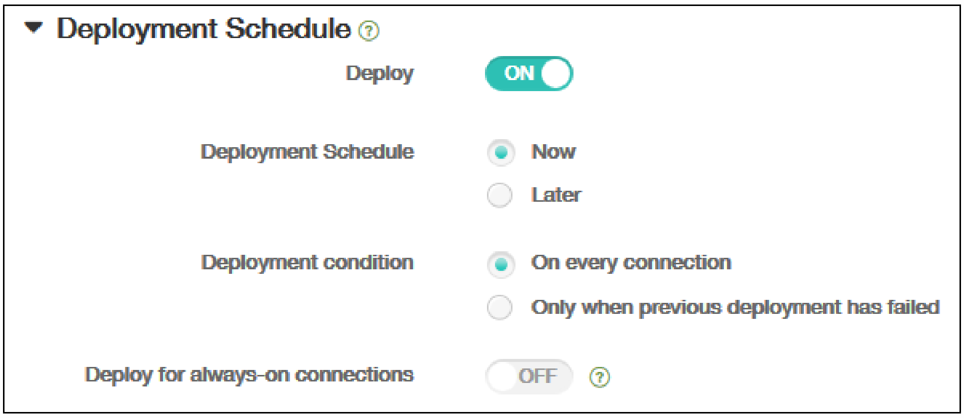
This policy lets you configure a profile for devices.

Choose delivery groups

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



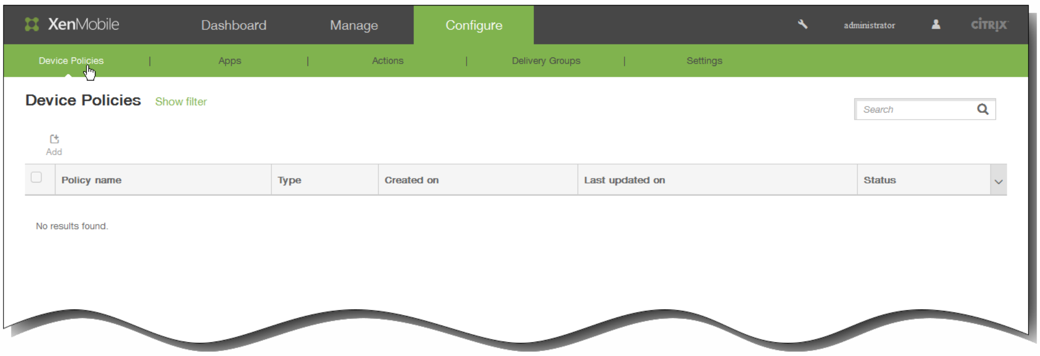
▼ Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

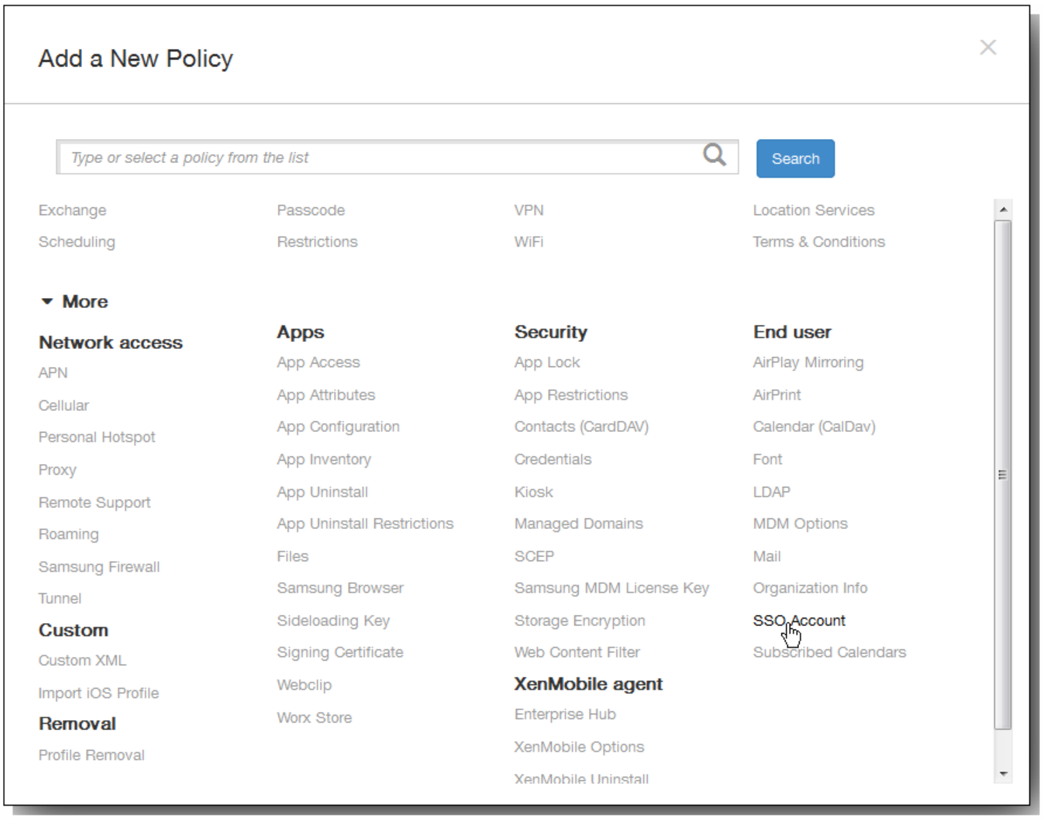
Deploy for always-on connections: OFF



Device Policies

☐	Policy name	Type	Created on	Last updated on	Status

No results found.



Add a New Policy

Type or select a policy from the list

Search

Exchange
Scheduling

Passcode
Restrictions

VPN
WiFi

Location Services
Terms & Conditions

More

Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel

Custom
Custom XML
Import iOS Profile

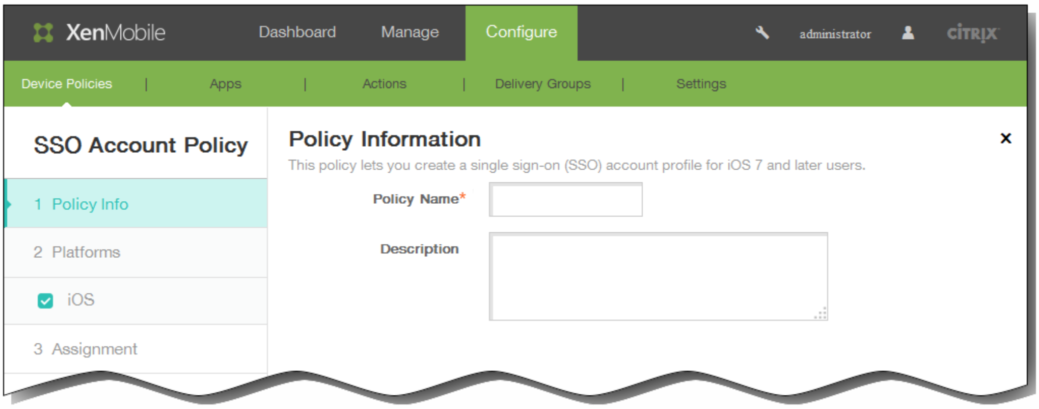
Removal
Profile Removal

Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store

Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter

XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall

End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars



XenMobile | Dashboard | Manage | Configure | administrator

Device Policies | Apps | Actions | Delivery Groups | Settings

SSO Account Policy

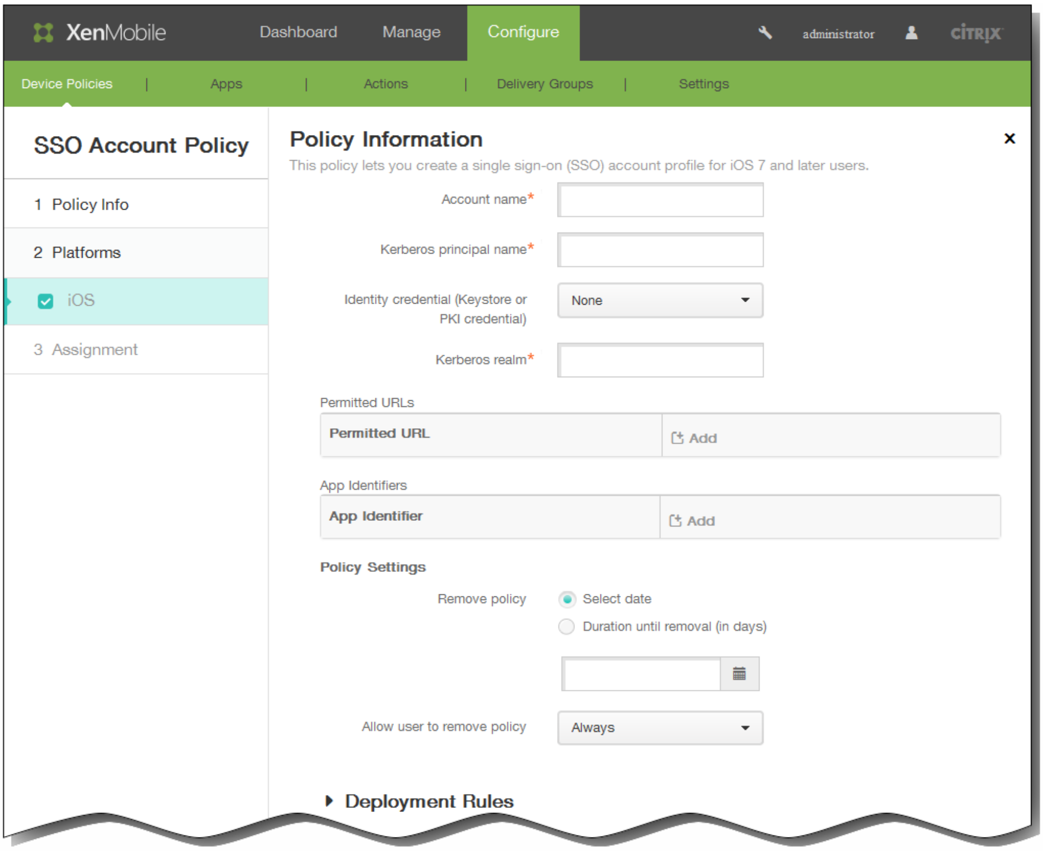
1 Policy Info
2 Platforms
☑ iOS
3 Assignment

Policy Information

This policy lets you create a single sign-on (SSO) account profile for iOS 7 and later users.

Policy Name*

Description



XenMobile
Dashboard
Manage
Configure
administrator
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings

SSO Account Policy

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

Policy Information

This policy lets you create a single sign-on (SSO) account profile for iOS 7 and later users.

Account name*

Kerberos principal name*

Identity credential (Keystore or PKI credential) None

Kerberos realm*

Permitted URLs

Permitted URL	Add

App Identifiers

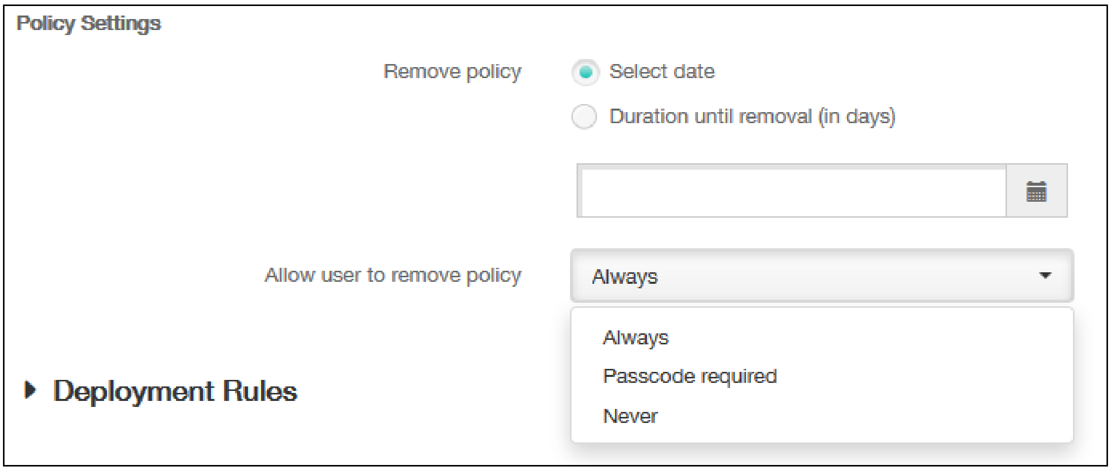
App Identifier	Add

Policy Settings

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

Allow user to remove policy Always

Deployment Rules

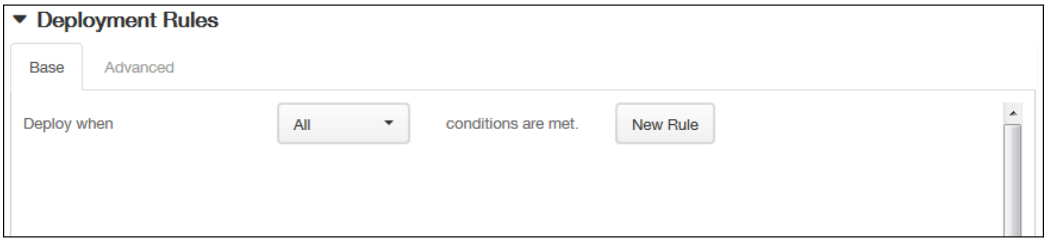


Policy Settings

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

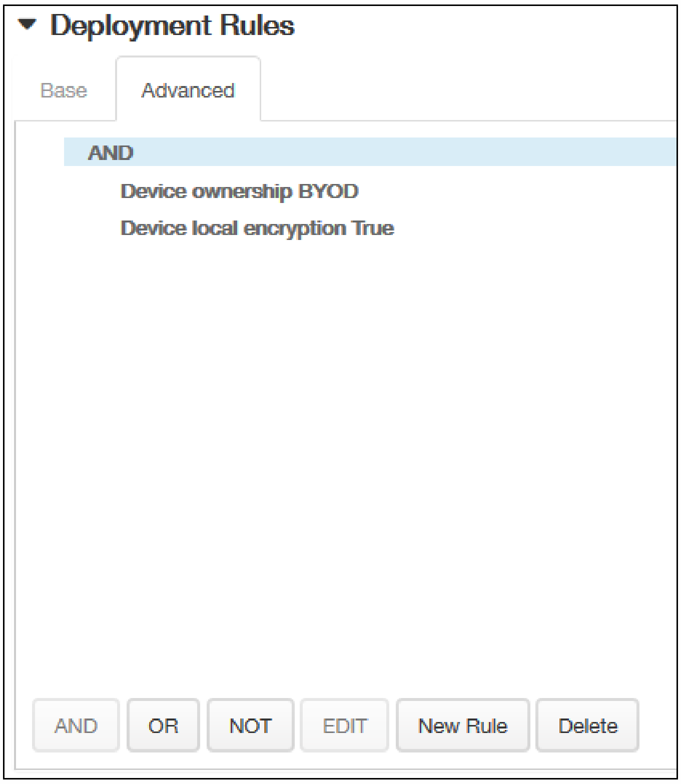
Allow user to remove policy: Always

▸ Deployment Rules



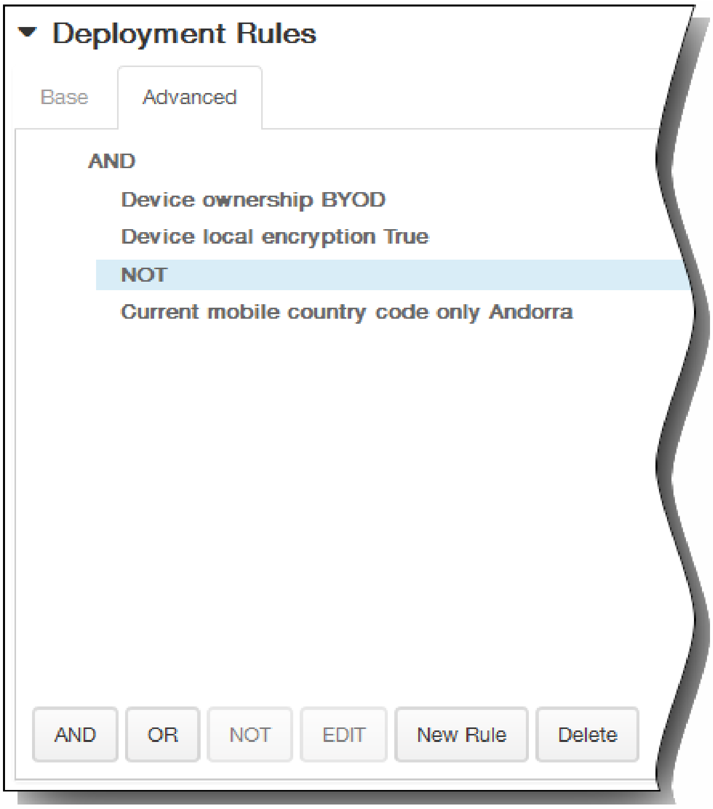
▾ Deployment Rules

Deploy when All conditions are met.



Device ownership BYOD

Device local encryption True



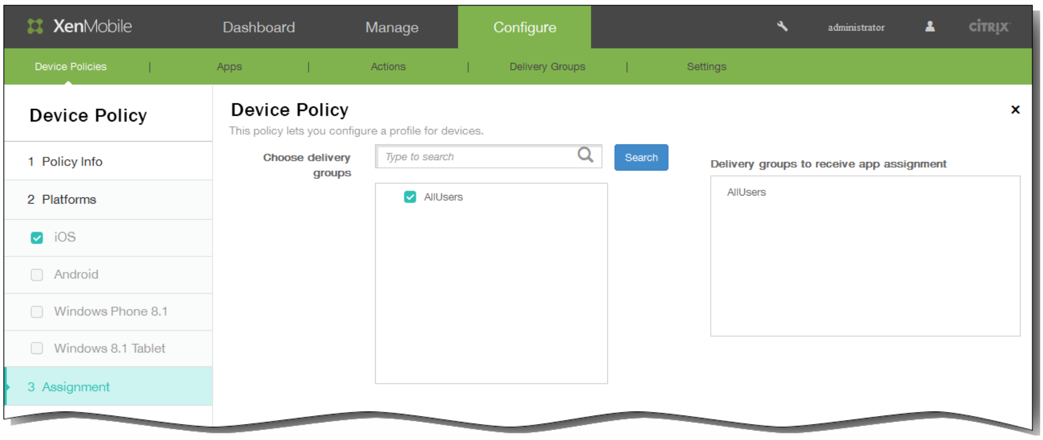
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

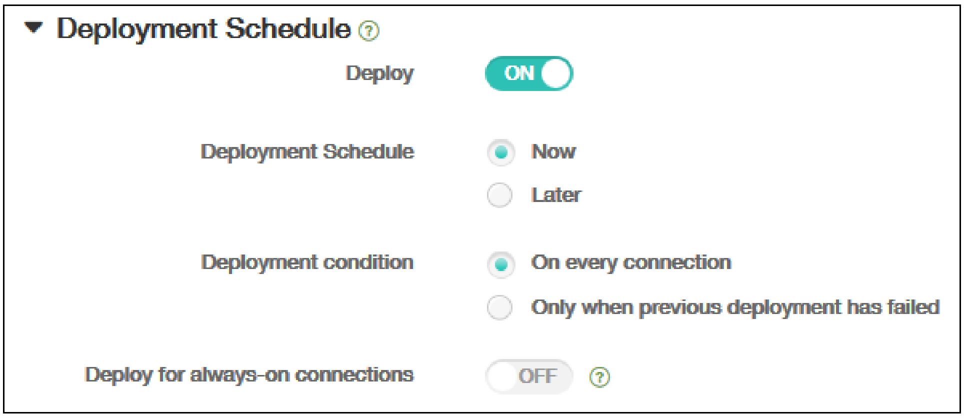
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



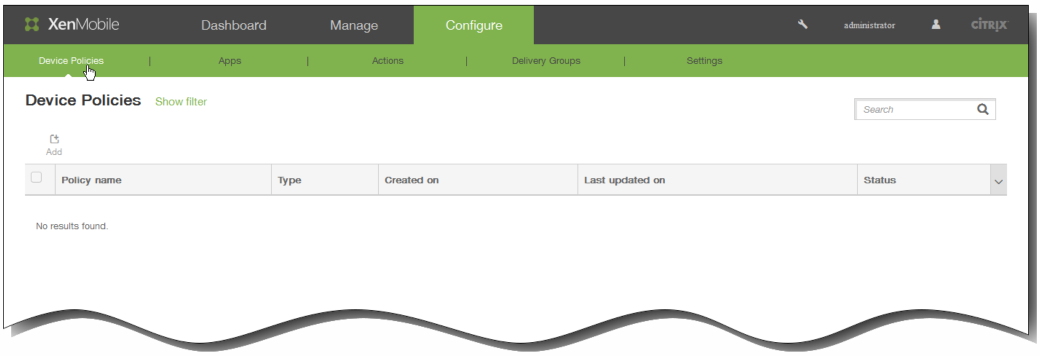
Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

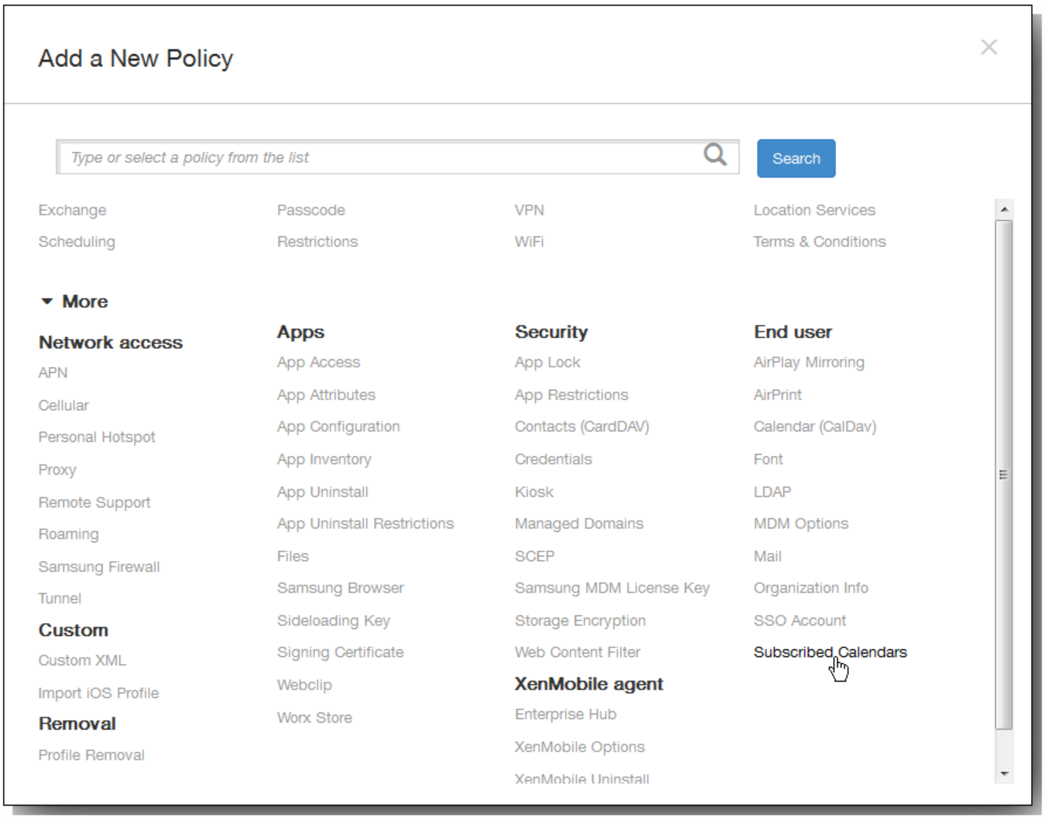
Deploy for always-on connections: OFF



Device Policies

□	Policy name	Type	Created on	Last updated on	Status

No results found.



Add a New Policy

Type or select a policy from the list

Search

Exchange
Scheduling

Passcode
Restrictions

VPN
WiFi

Location Services
Terms & Conditions

▼ More

Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel

Custom
Custom XML
Import iOS Profile

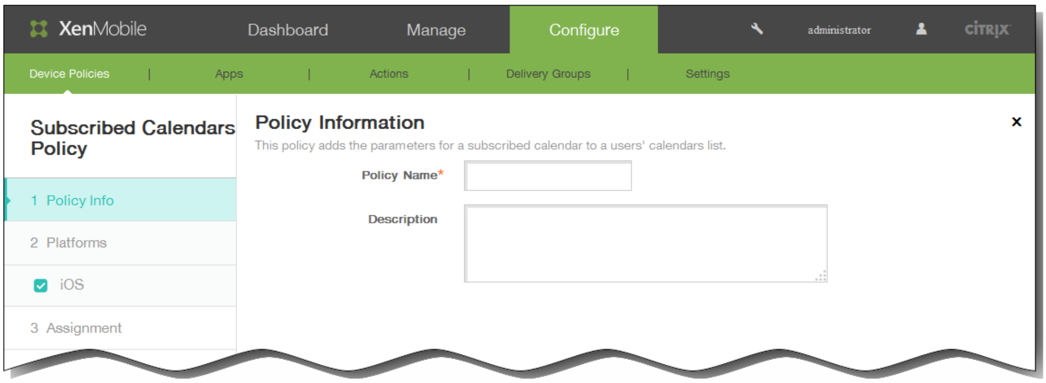
Removal
Profile Removal

Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store

Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter

XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall

End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars



XenMobile | Dashboard | Manage | Configure | administrator | CITRIX

Device Policies | Apps | Actions | Delivery Groups | Settings

Subscribed Calendars Policy

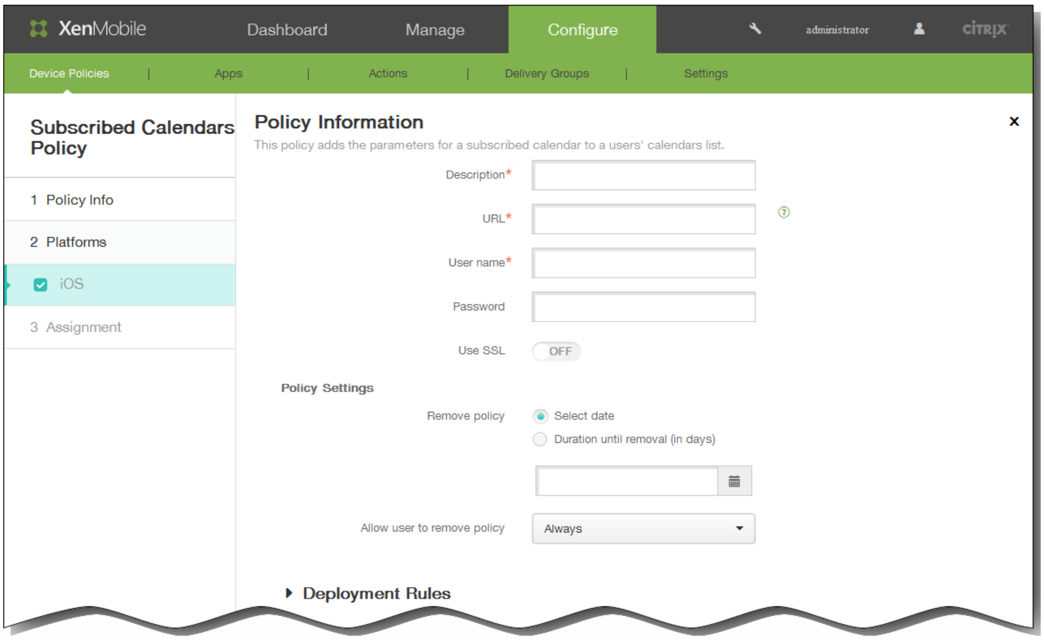
1 Policy Info
2 Platforms
☑ iOS
3 Assignment

Policy Information

This policy adds the parameters for a subscribed calendar to a users' calendars list.

Policy Name*

Description



Policy Information

This policy adds the parameters for a subscribed calendar to a users' calendars list.

Description*

URL*

User name*

Password

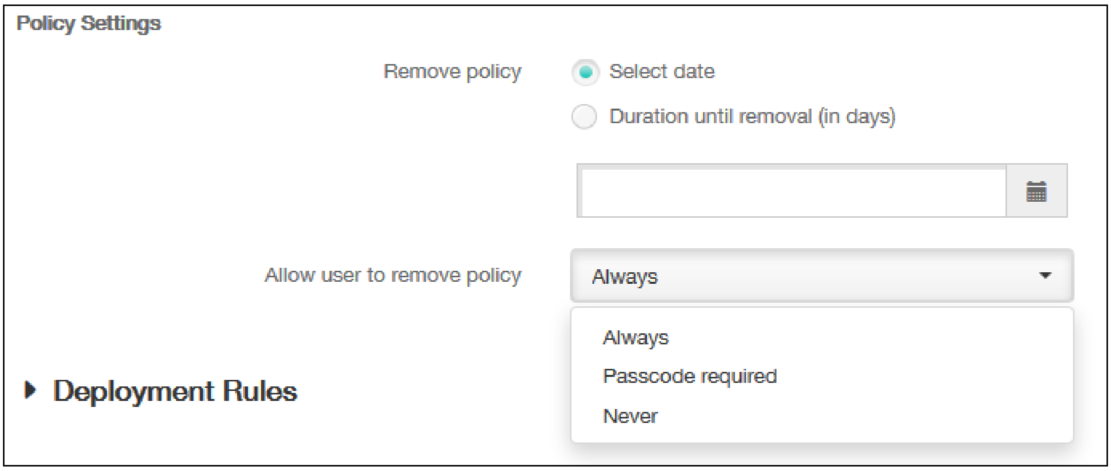
Use SSL OFF

Policy Settings

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

Allow user to remove policy Always

Deployment Rules

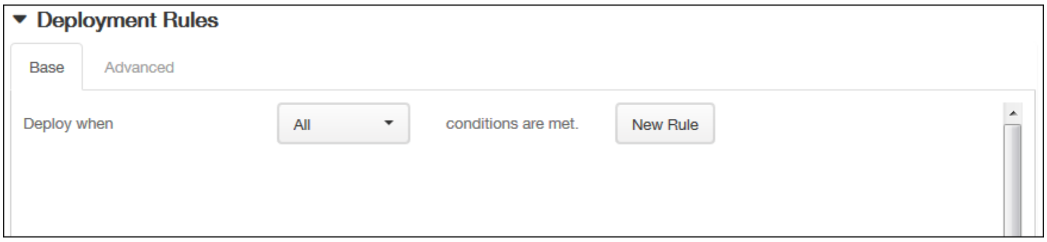


Policy Settings

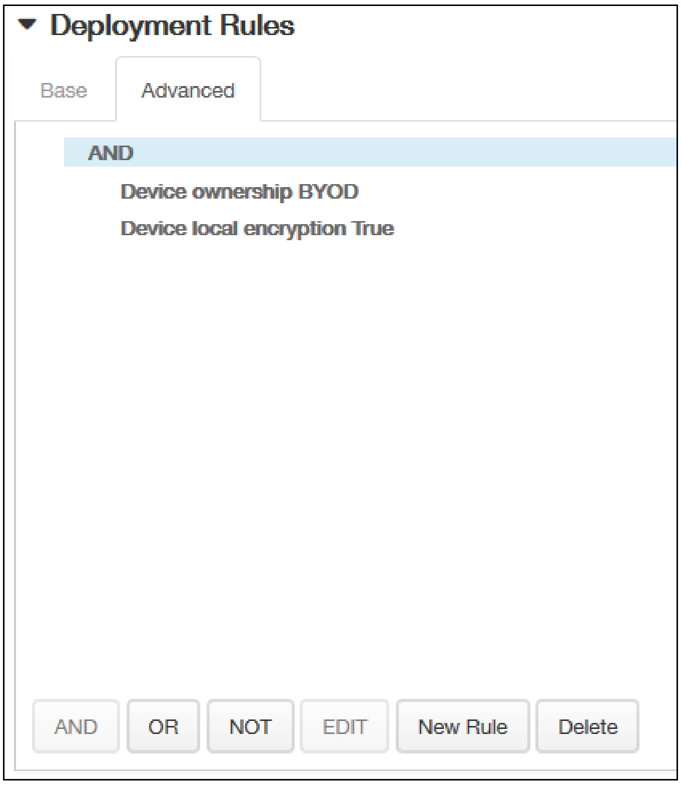
Remove policy ● Select date ○ Duration until removal (in days)

Allow user to remove policy Always

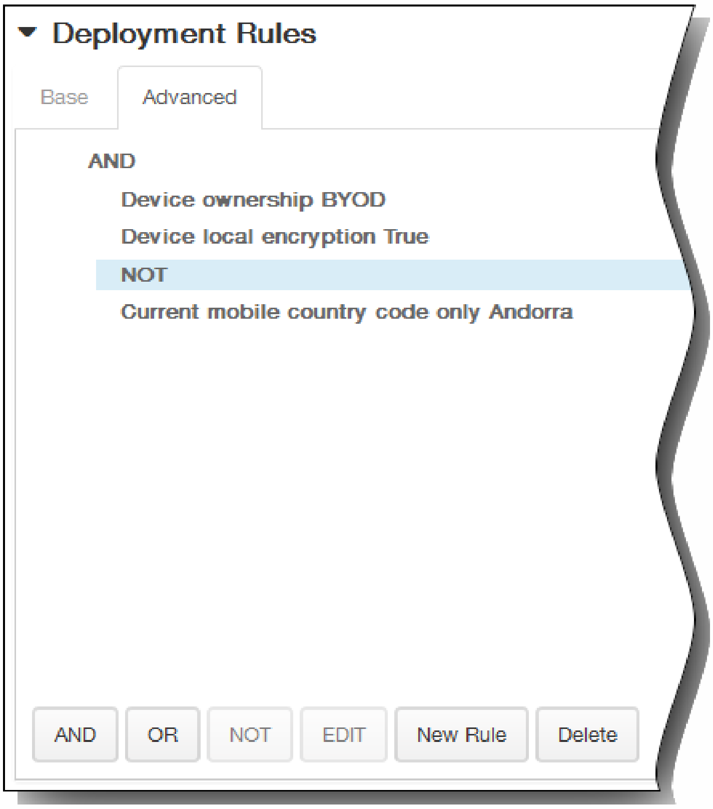
Deployment Rules



Deployment Rules
Base
Advanced
Deploy when
All
conditions are met.
New Rule



Deployment Rules
Base
Advanced
AND
Device ownership BYOD
Device local encryption True
AND
OR
NOT
EDIT
New Rule
Delete



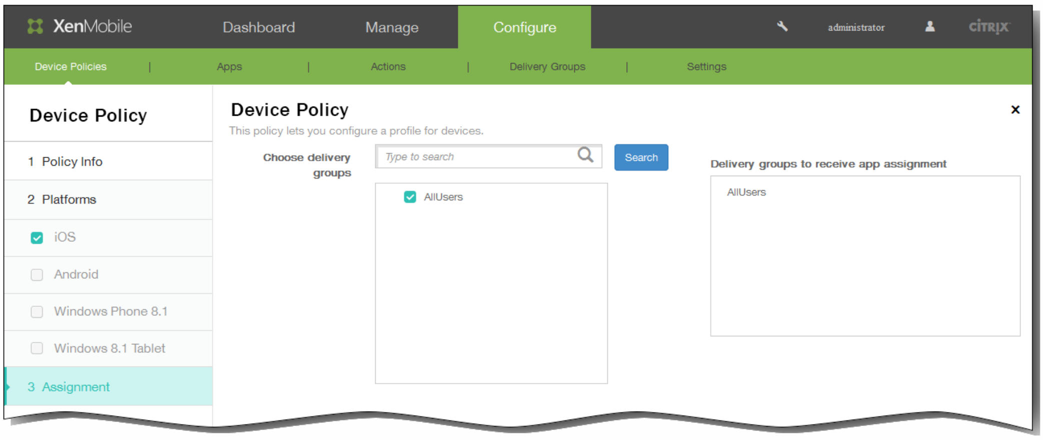
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

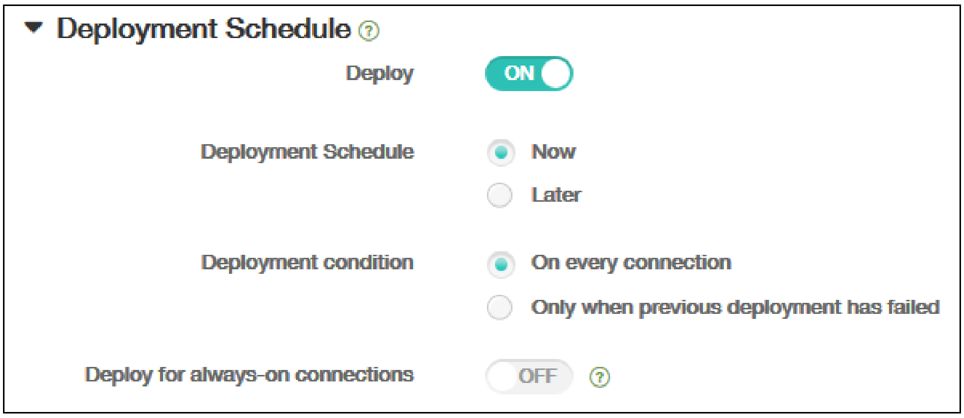
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



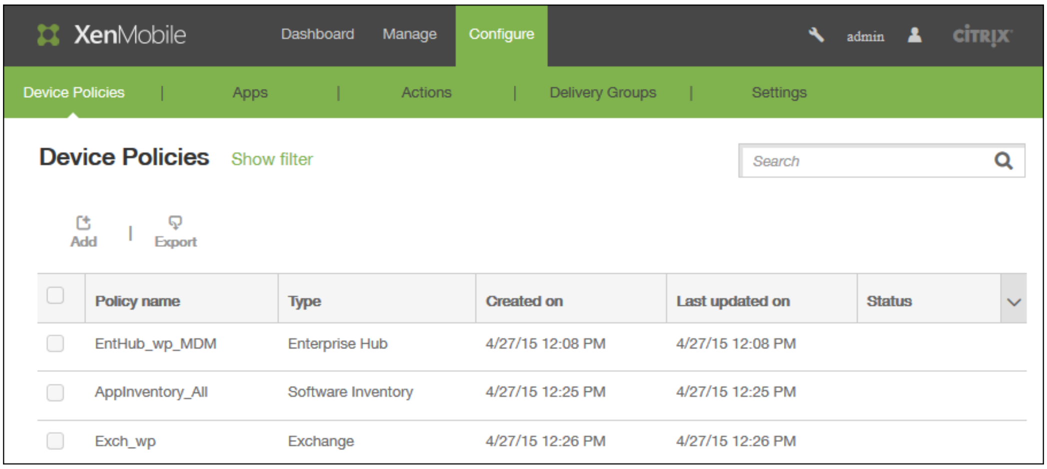
Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

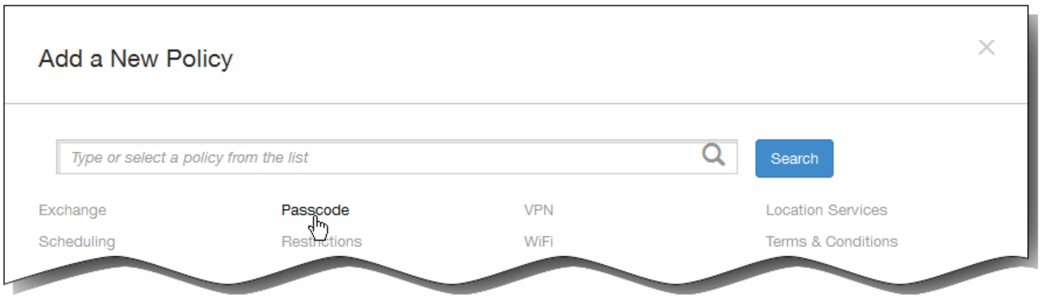
Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF

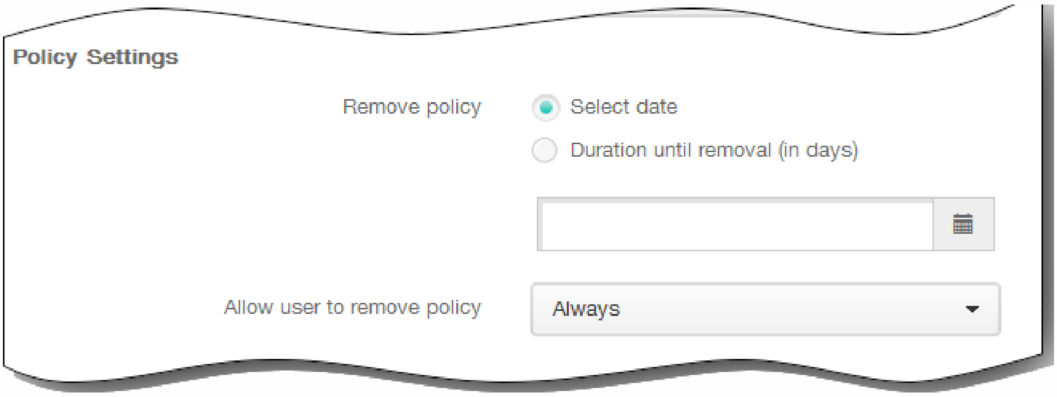


Device Policies

☐	Policy name	Type	Created on	Last updated on	Status
☐	EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
☐	AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
☐	Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	



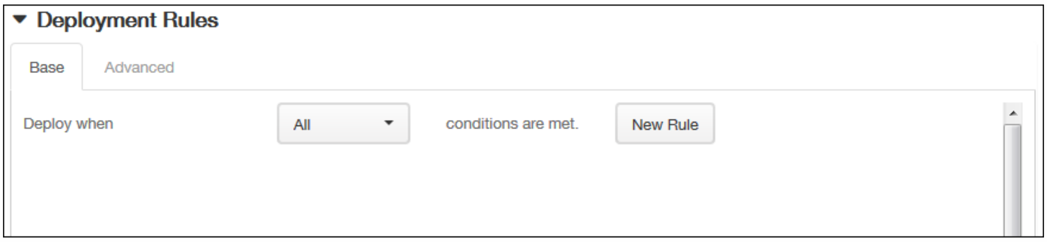
-



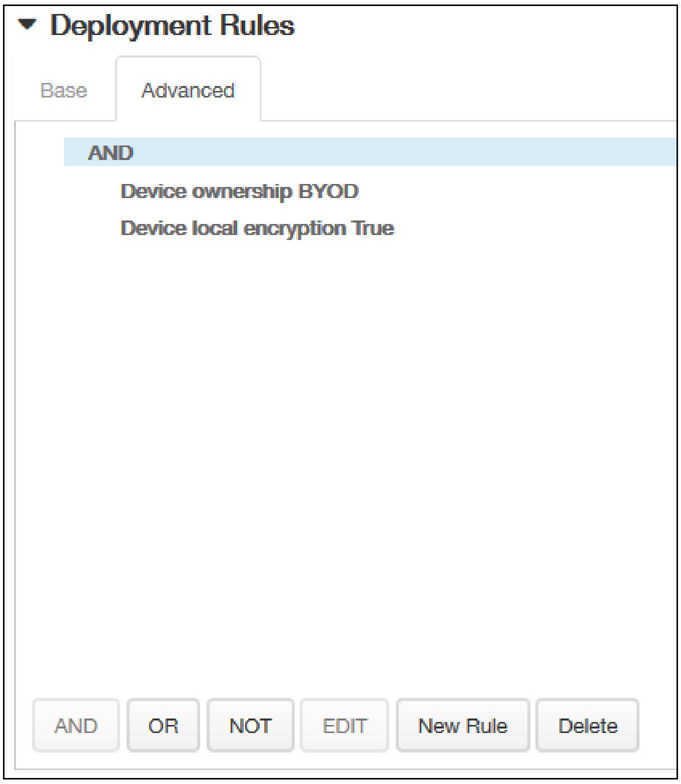
Policy Settings

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

Allow user to remove policy: Always



Deployment Rules
Base
Advanced
Deploy when
All
conditions are met.
New Rule

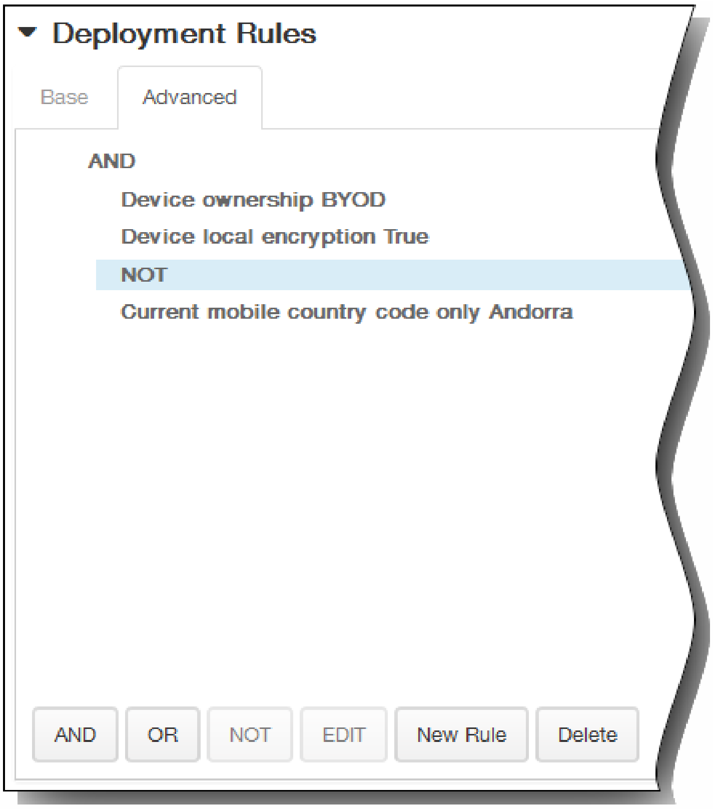


Deployment Rules

AND

Device ownership BYOD

Device local encryption True



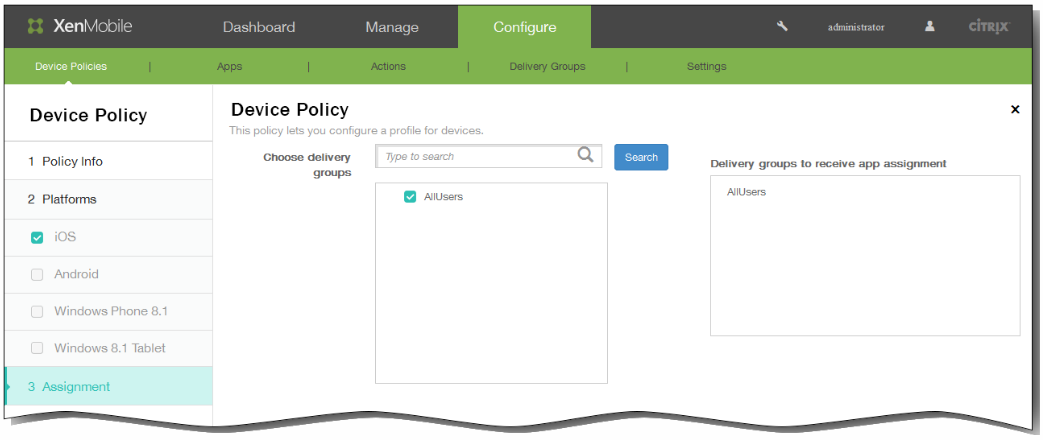
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

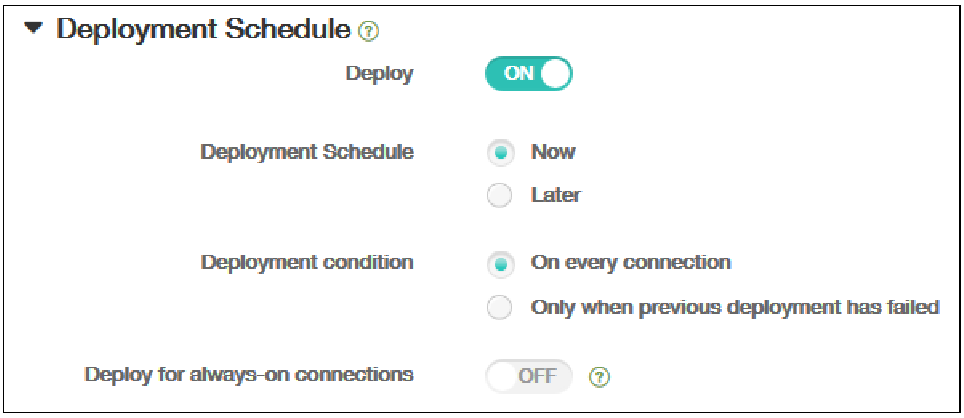
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search [Search]

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



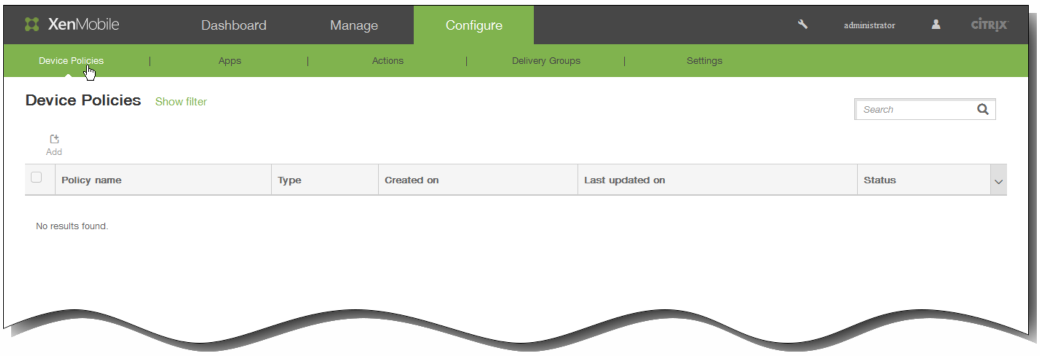
Deployment Schedule

Deploy: ON

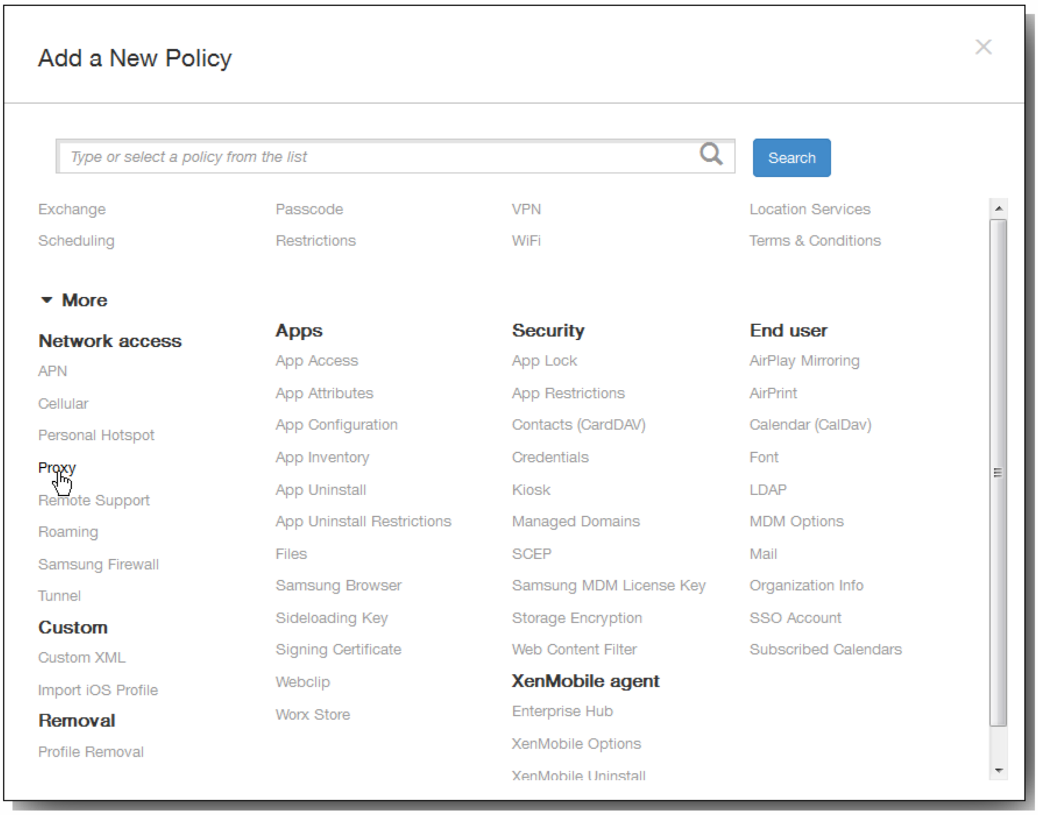
Deployment Schedule: ● Now ○ Later

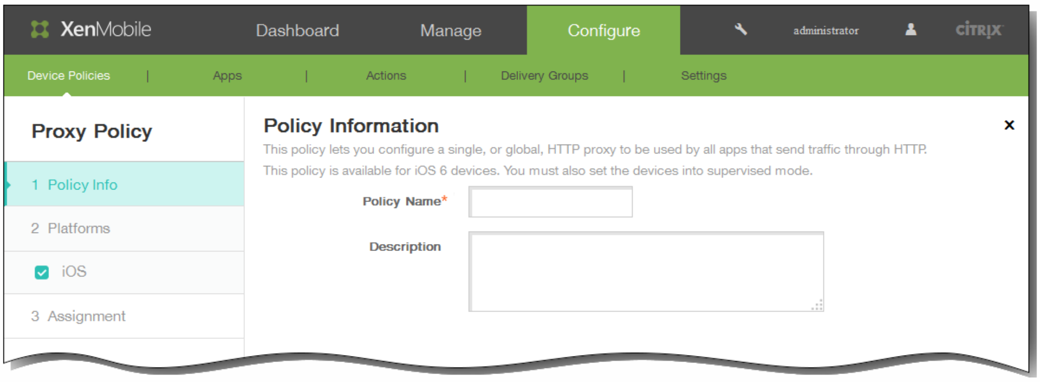
Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF



No results found.





XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings

Proxy Policy

1 Policy Info

2 Platforms

☑ iOS

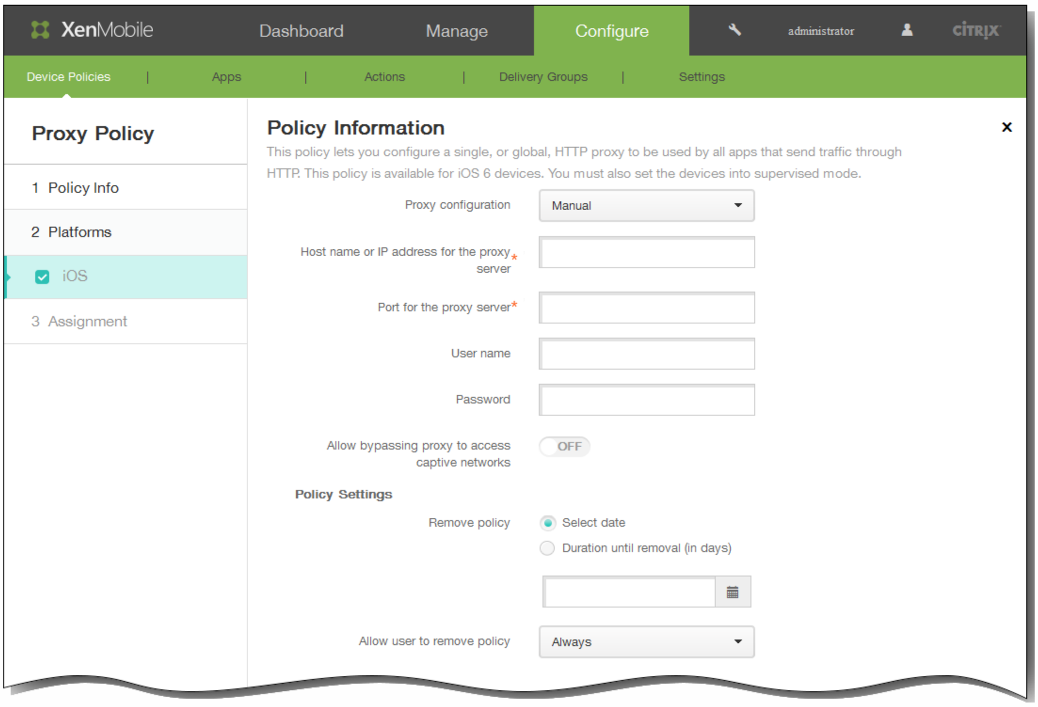
3 Assignment

Policy Information

This policy lets you configure a single, or global, HTTP proxy to be used by all apps that send traffic through HTTP. This policy is available for iOS 6 devices. You must also set the devices into supervised mode.

Policy Name*

Description



XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings

Proxy Policy

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

Policy Information

This policy lets you configure a single, or global, HTTP proxy to be used by all apps that send traffic through HTTP. This policy is available for iOS 6 devices. You must also set the devices into supervised mode.

Proxy configuration: Manual

Host name or IP address for the proxy server*

Port for the proxy server*

User name

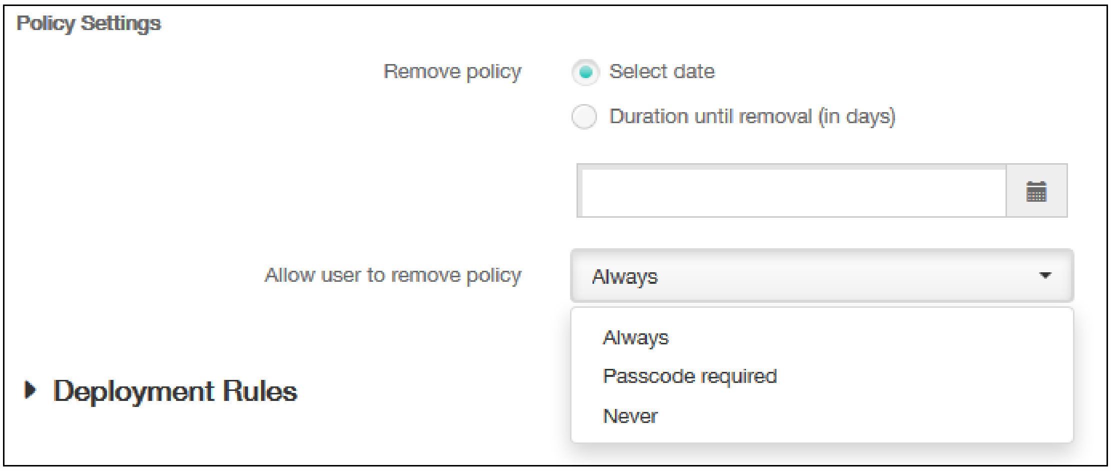
Password

Allow bypassing proxy to access captive networks: OFF

Policy Settings

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

Allow user to remove policy: Always

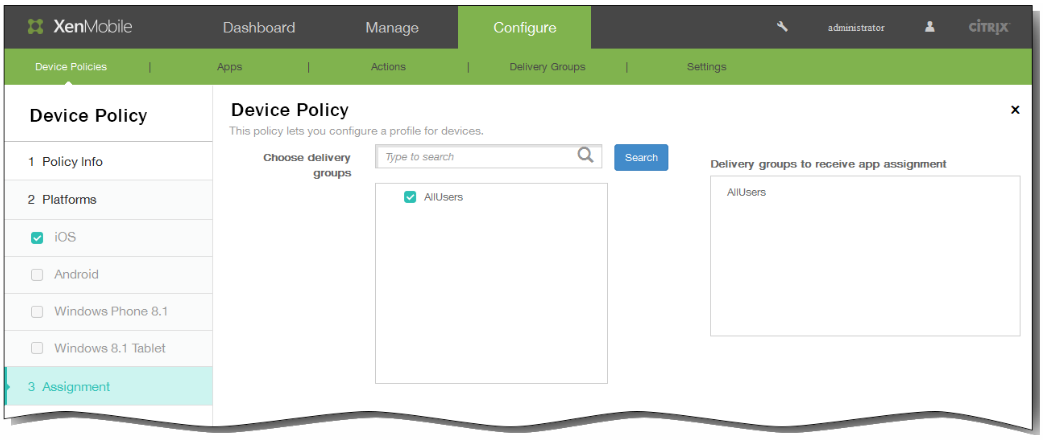


Policy Settings

Remove policy ● Select date

○ Duration until removal (in days)

Allow user to remove policy: Always



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

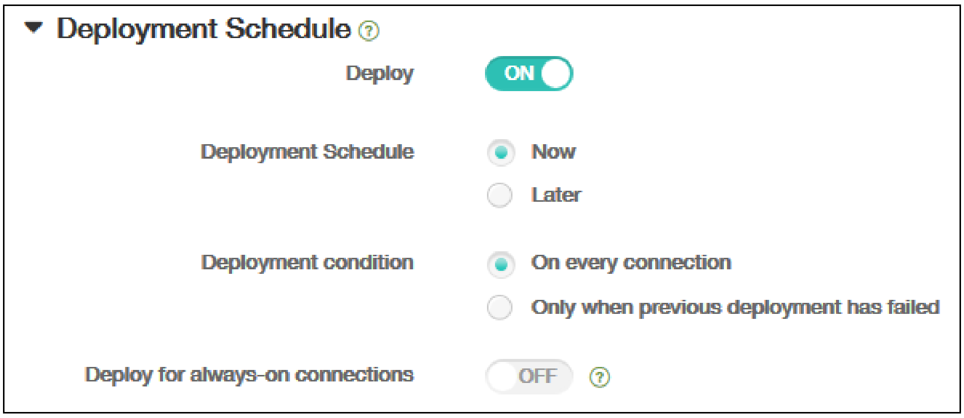
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search [Search]

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



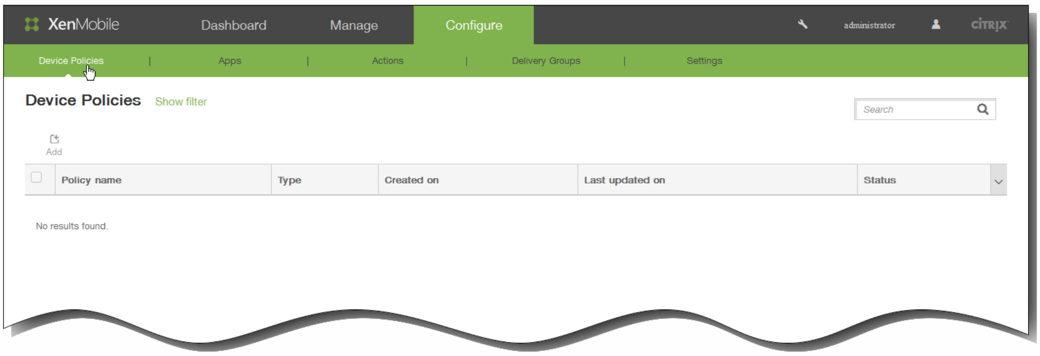
Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

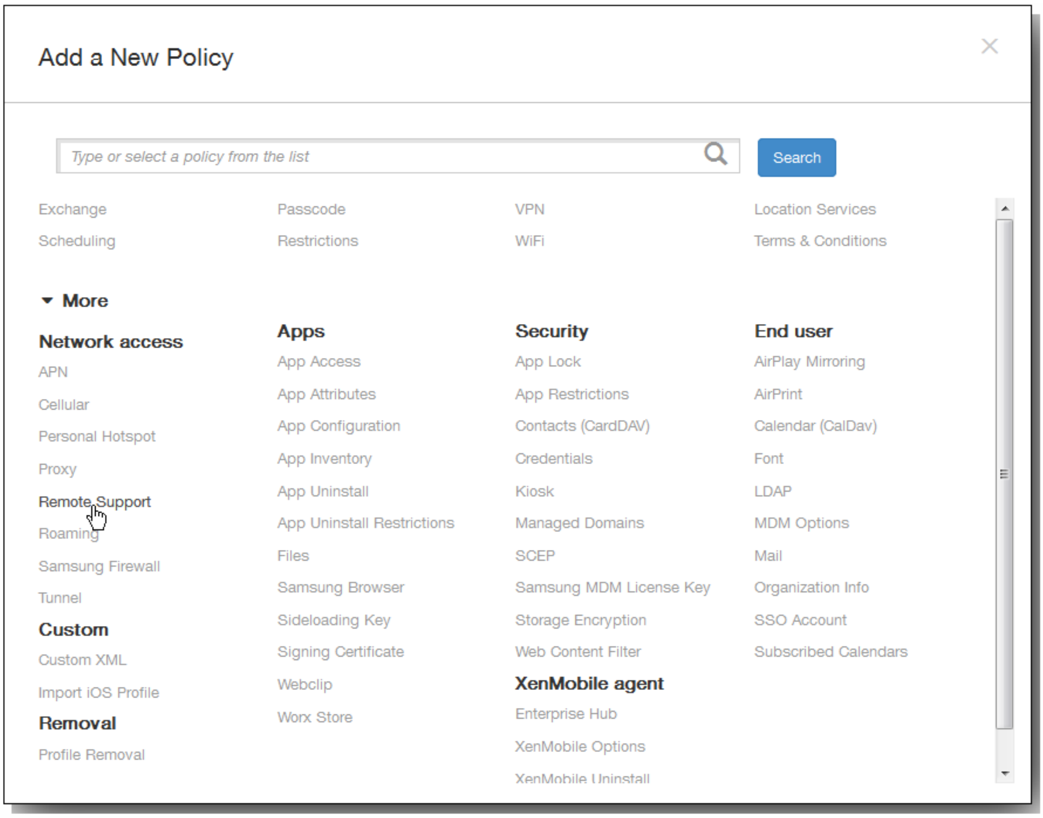
Deploy for always-on connections: OFF



Device Policies

☐	Policy name	Type	Created on	Last updated on	Status

No results found.



Add a New Policy

Type or select a policy from the list

Search

Exchange

Scheduling

Passcode

Restrictions

VPN

WiFi

Location Services

Terms & Conditions

▾ More

Network access

APN

Cellular

Personal Hotspot

Proxy

Remote Support

Roaming

Samsung Firewall

Tunnel

Custom

Custom XML

Import iOS Profile

Removal

Profile Removal

Apps

App Access

App Attributes

App Configuration

App Inventory

App Uninstall

App Uninstall Restrictions

Files

Samsung Browser

Sideloading Key

Signing Certificate

Webclip

Worx Store

Security

App Lock

App Restrictions

Contacts (CardDAV)

Credentials

Kiosk

Managed Domains

SCEP

Samsung MDM License Key

Storage Encryption

Web Content Filter

XenMobile agent

Enterprise Hub

XenMobile Options

XenMobile Uninstall

End user

AirPlay Mirroring

AirPrint

Calendar (CalDav)

Font

LDAP

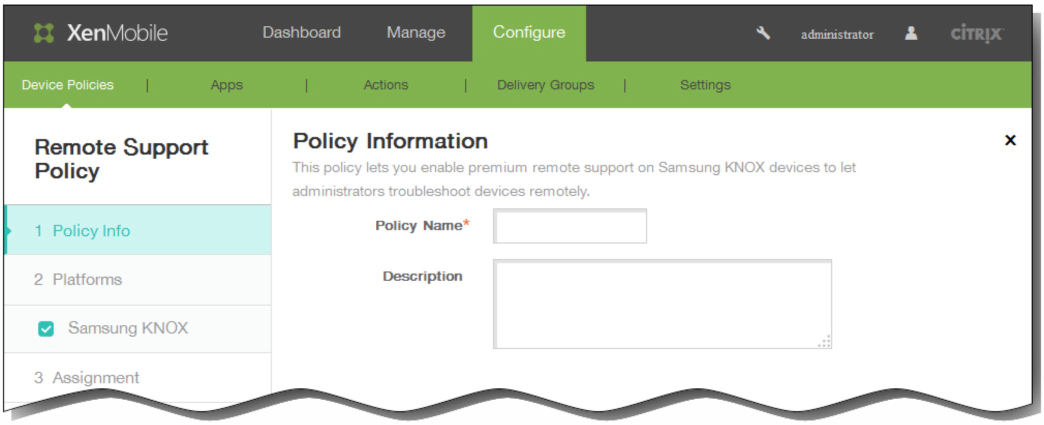
MDM Options

Mail

Organization Info

SSO Account

Subscribed Calendars



XenMobile | Dashboard | Manage | Configure | administrator | CITRIX

Device Policies | Apps | Actions | Delivery Groups | Settings

Remote Support Policy

1 Policy Info

2 Platforms

☑ Samsung KNOX

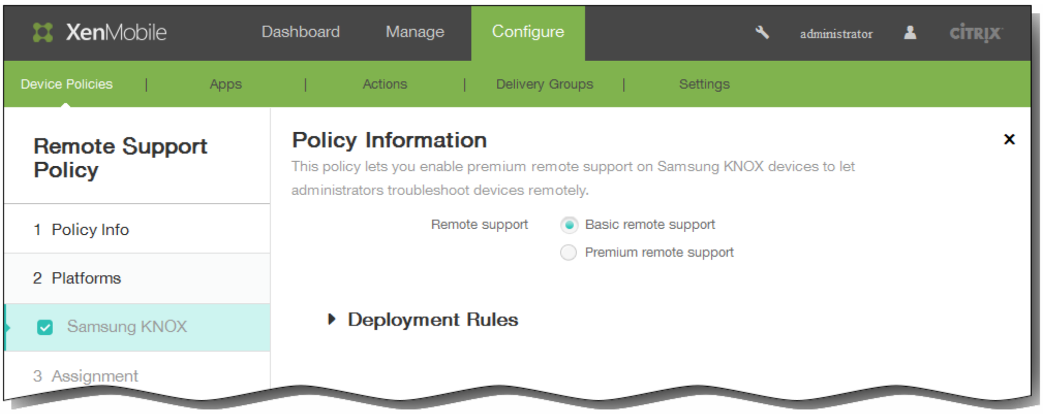
3 Assignment

Policy Information

This policy lets you enable premium remote support on Samsung KNOX devices to let administrators troubleshoot devices remotely.

Policy Name*

Description



XenMobile | Dashboard | Manage | Configure | administrator

Device Policies | Apps | Actions | Delivery Groups | Settings

Remote Support Policy

1 Policy Info

2 Platforms

☑ Samsung KNOX

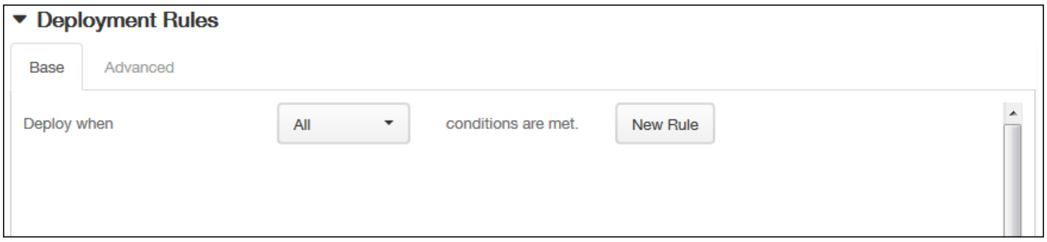
3 Assignment

Policy Information

This policy lets you enable premium remote support on Samsung KNOX devices to let administrators troubleshoot devices remotely.

Remote support ● Basic remote support
○ Premium remote support

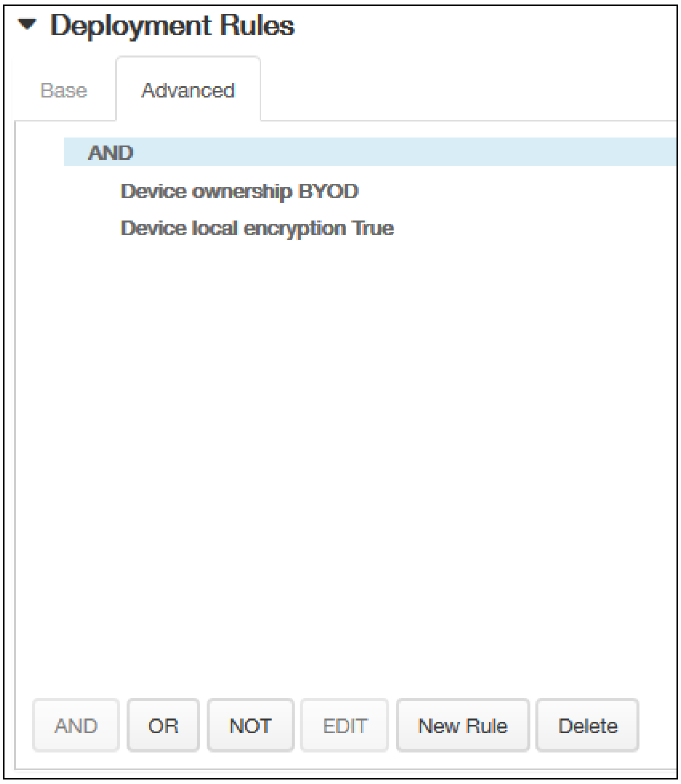
▸ Deployment Rules



▾ Deployment Rules

Base | Advanced

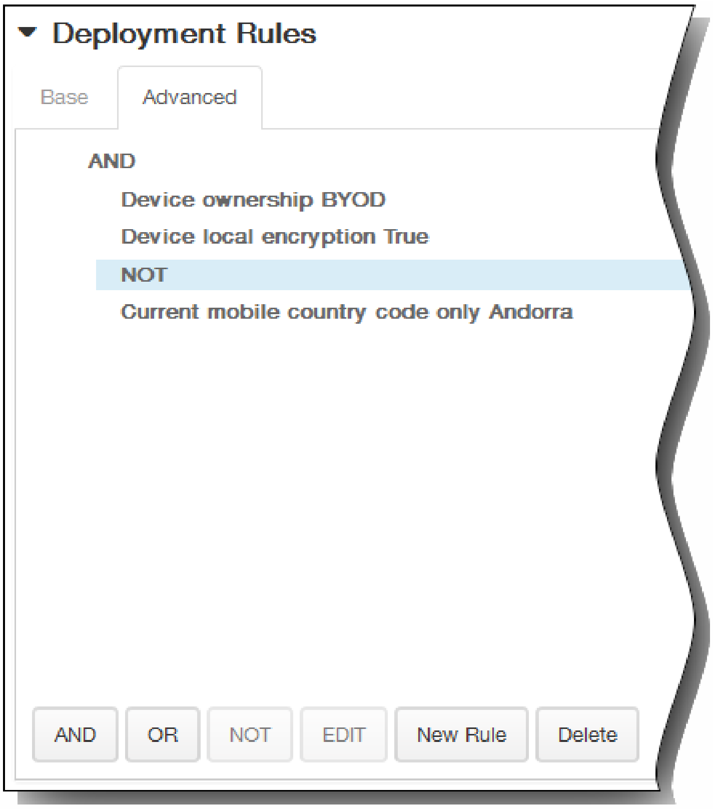
Deploy when All conditions are met. New Rule



AND

Device ownership BYOD

Device local encryption True



Deployment Rules

Base | Advanced

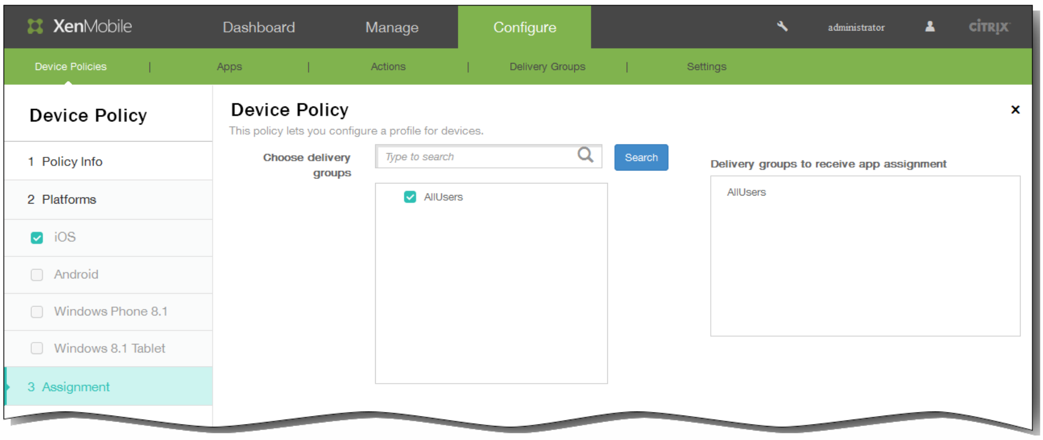
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

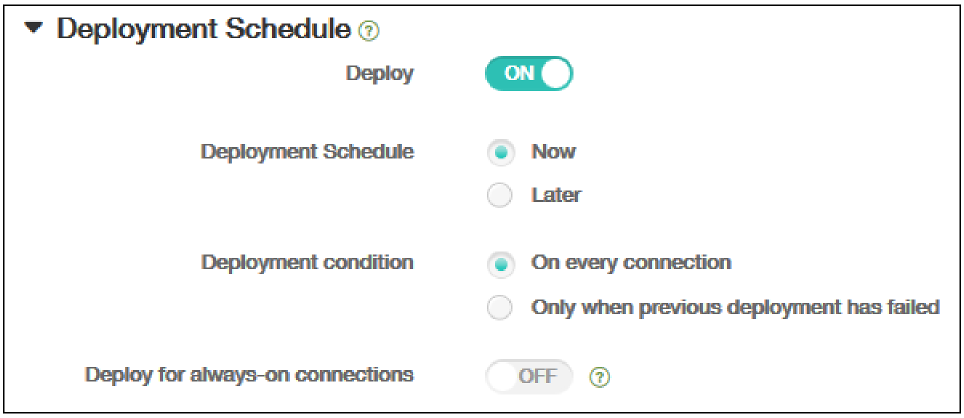
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



Deployment Schedule

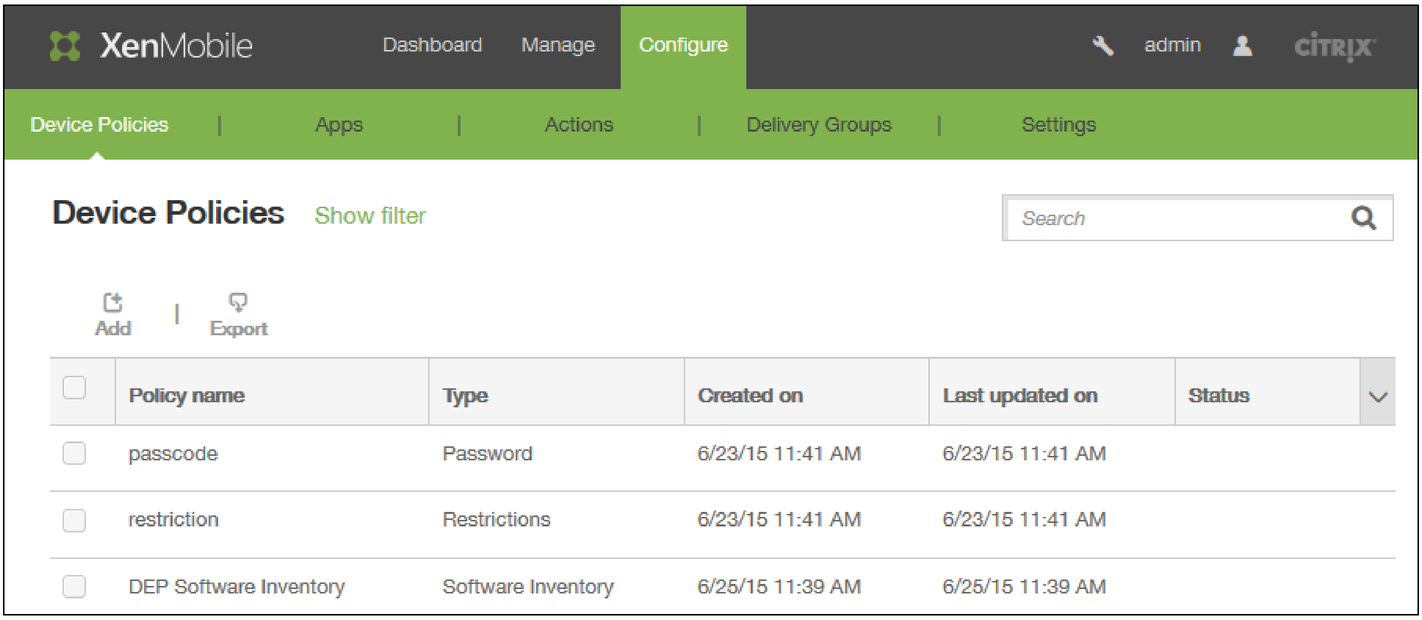
Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

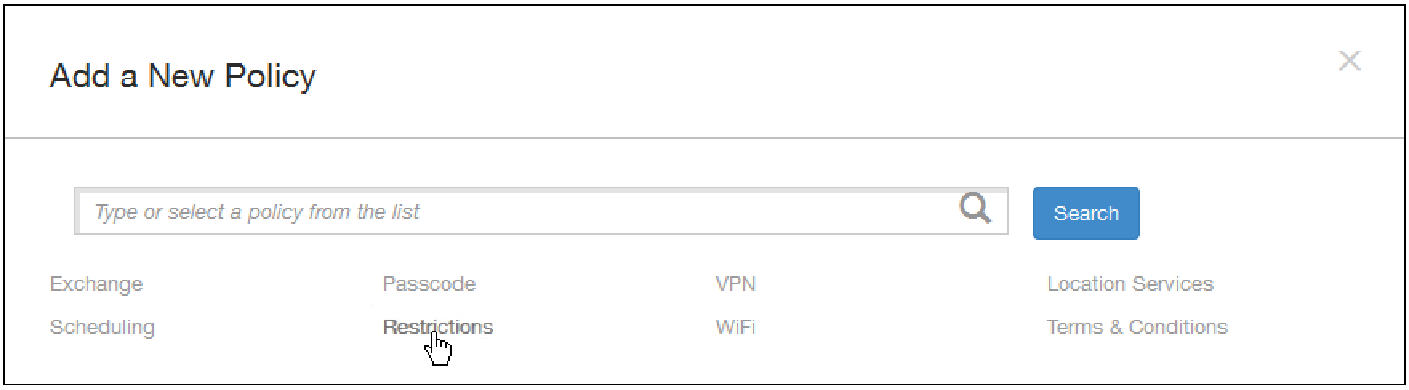
Deploy for always-on connections: OFF

-
-



Device Policies

☐	Policy name	Type	Created on	Last updated on	Status
☐	passcode	Password	6/23/15 11:41 AM	6/23/15 11:41 AM	
☐	restriction	Restrictions	6/23/15 11:41 AM	6/23/15 11:41 AM	
☐	DEP Software Inventory	Software Inventory	6/25/15 11:39 AM	6/25/15 11:39 AM	

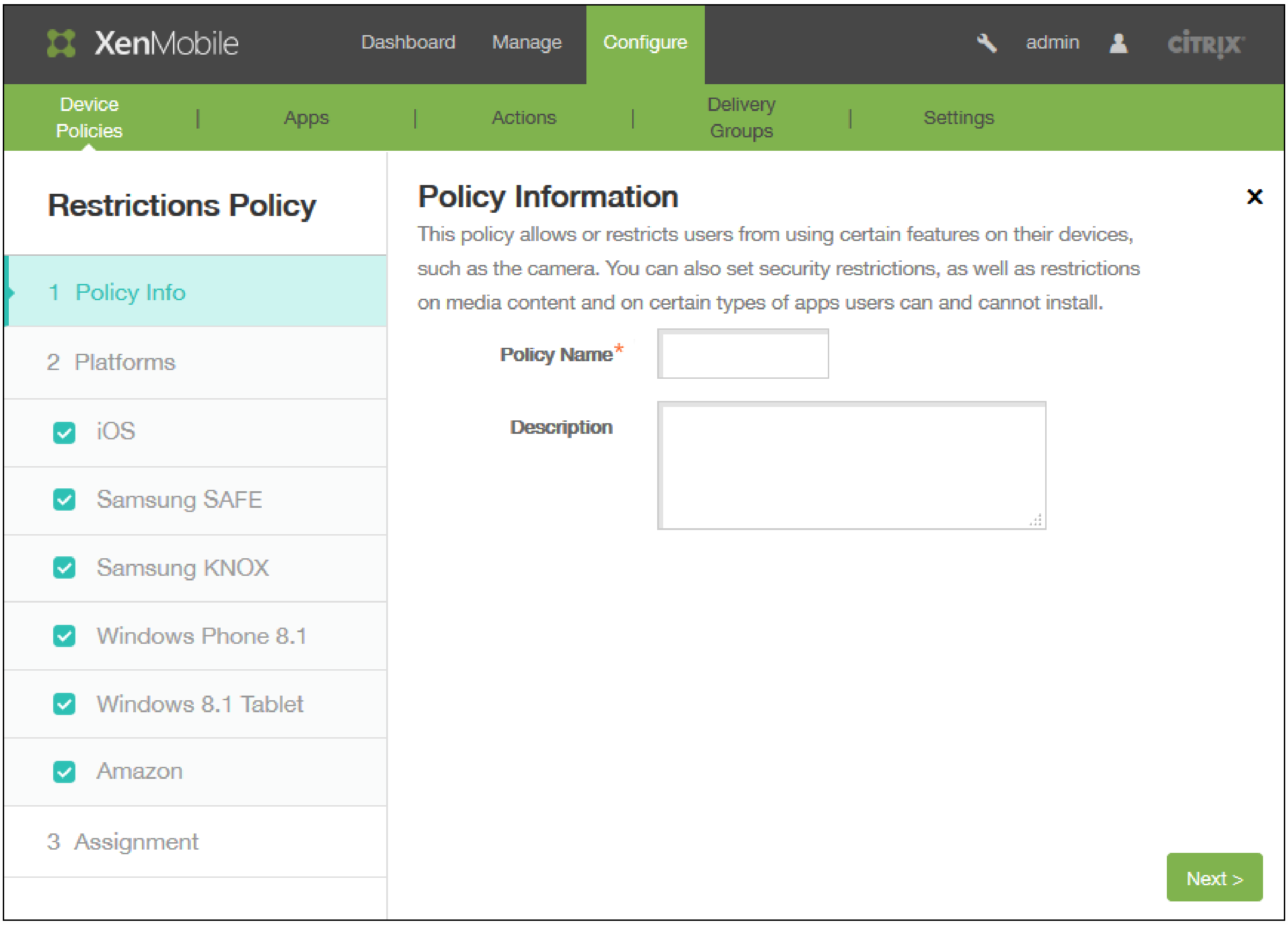


Add a New Policy

Type or select a policy from the list

Search

Exchange	Passcode	VPN	Location Services
Scheduling	Restrictions	WiFi	Terms & Conditions



Restrictions Policy

1 Policy Info

2 Platforms

- ☑ iOS
- ☑ Samsung SAFE
- ☑ Samsung KNOX
- ☑ Windows Phone 8.1
- ☑ Windows 8.1 Tablet
- ☑ Amazon

3 Assignment

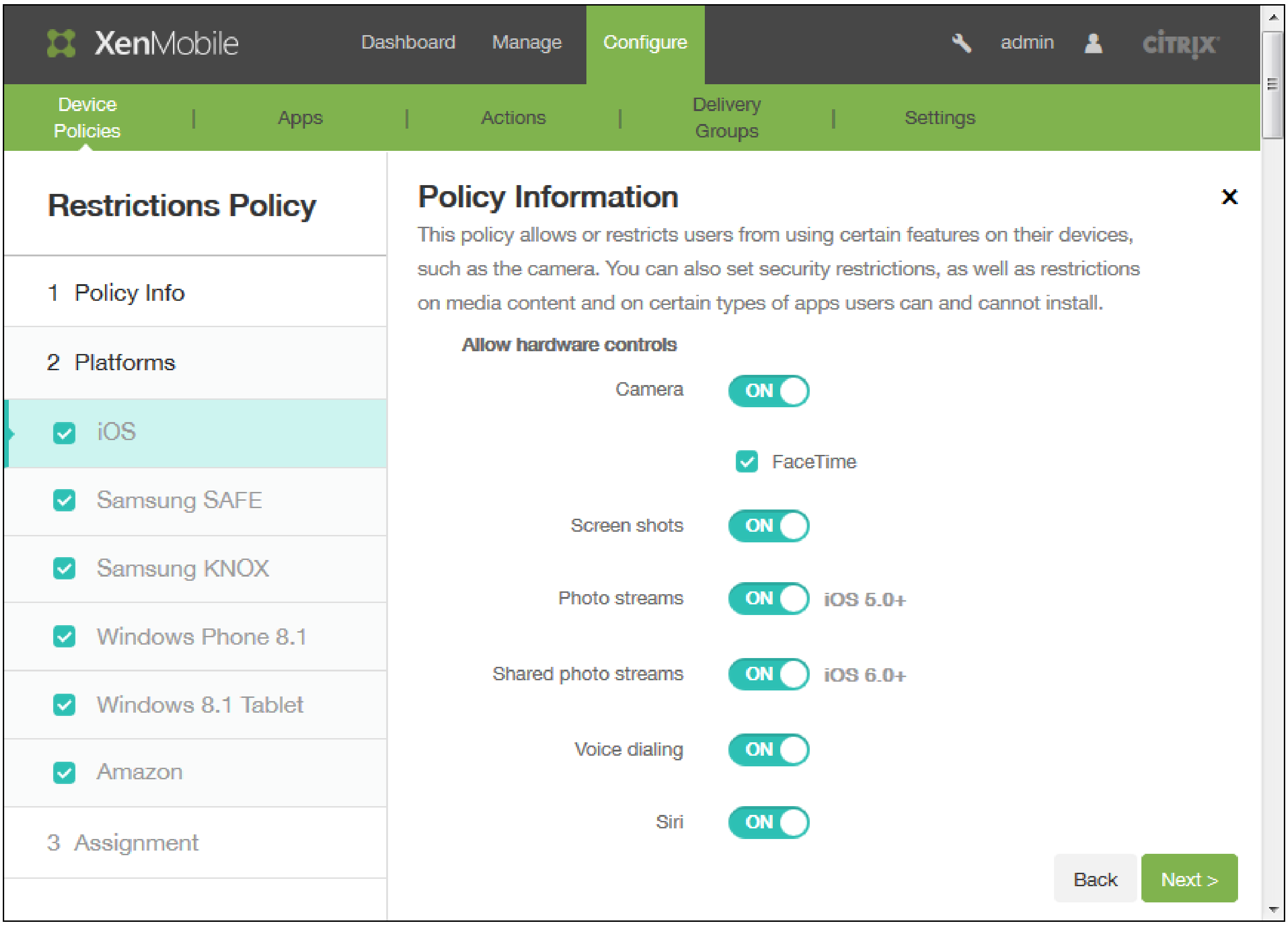
Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Policy Name*

Description

Next >



Restrictions Policy

1 Policy Info

2 Platforms

☑ iOS

☑ Samsung SAFE

☑ Samsung KNOX

☑ Windows Phone 8.1

☑ Windows 8.1 Tablet

☑ Amazon

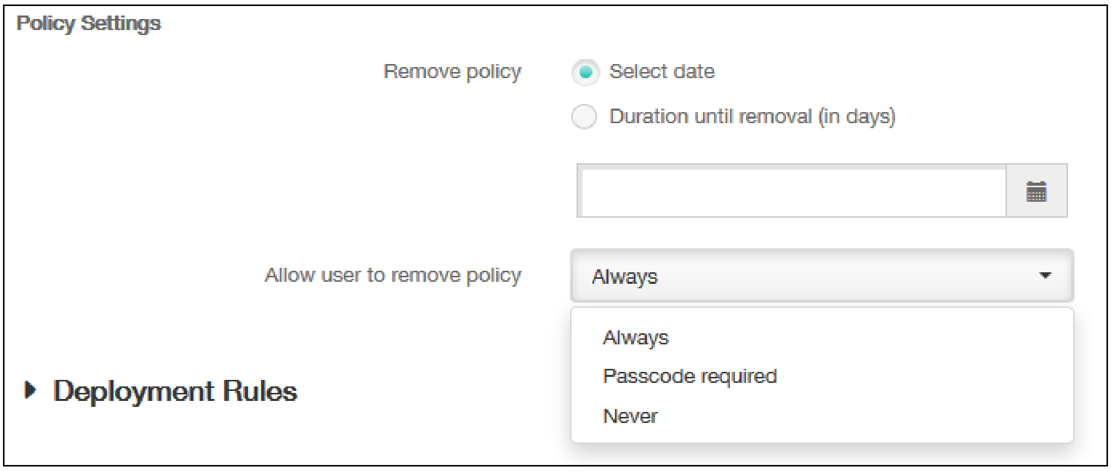
3 Assignment

Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Allow hardware controls

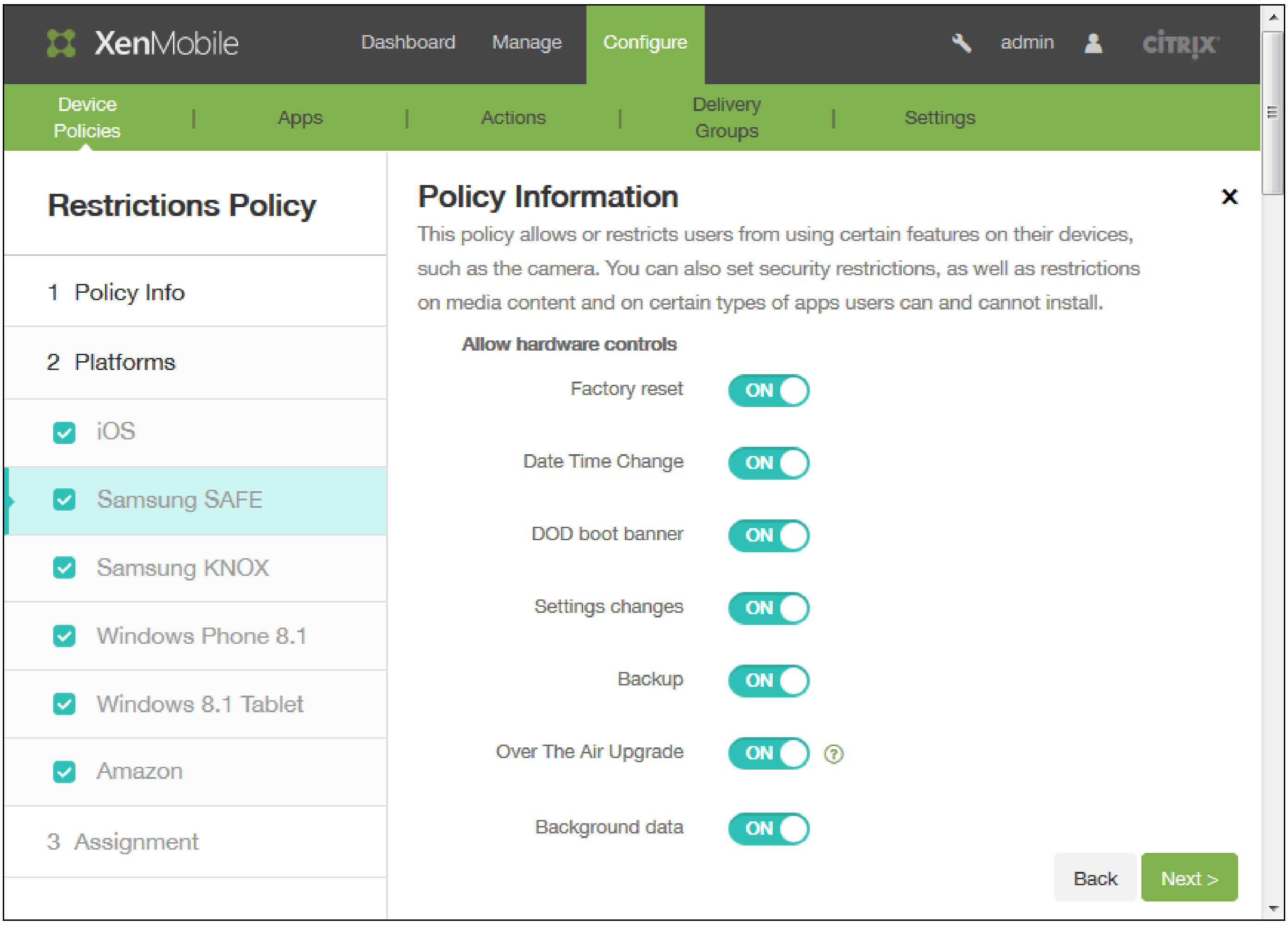
Camera	ON	
	☑ FaceTime	
Screen shots	ON	
Photo streams	ON	iOS 5.0+
Shared photo streams	ON	iOS 6.0+
Voice dialing	ON	
Siri	ON	



Policy Settings

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

Allow user to remove policy: Always



Restrictions Policy

1 Policy Info

2 Platforms

- ☑ iOS
- ☑ Samsung SAFE
- ☑ Samsung KNOX
- ☑ Windows Phone 8.1
- ☑ Windows 8.1 Tablet
- ☑ Amazon

3 Assignment

Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Allow hardware controls

Factory reset: ON

Date Time Change: ON

DOD boot banner: ON

Settings changes: ON

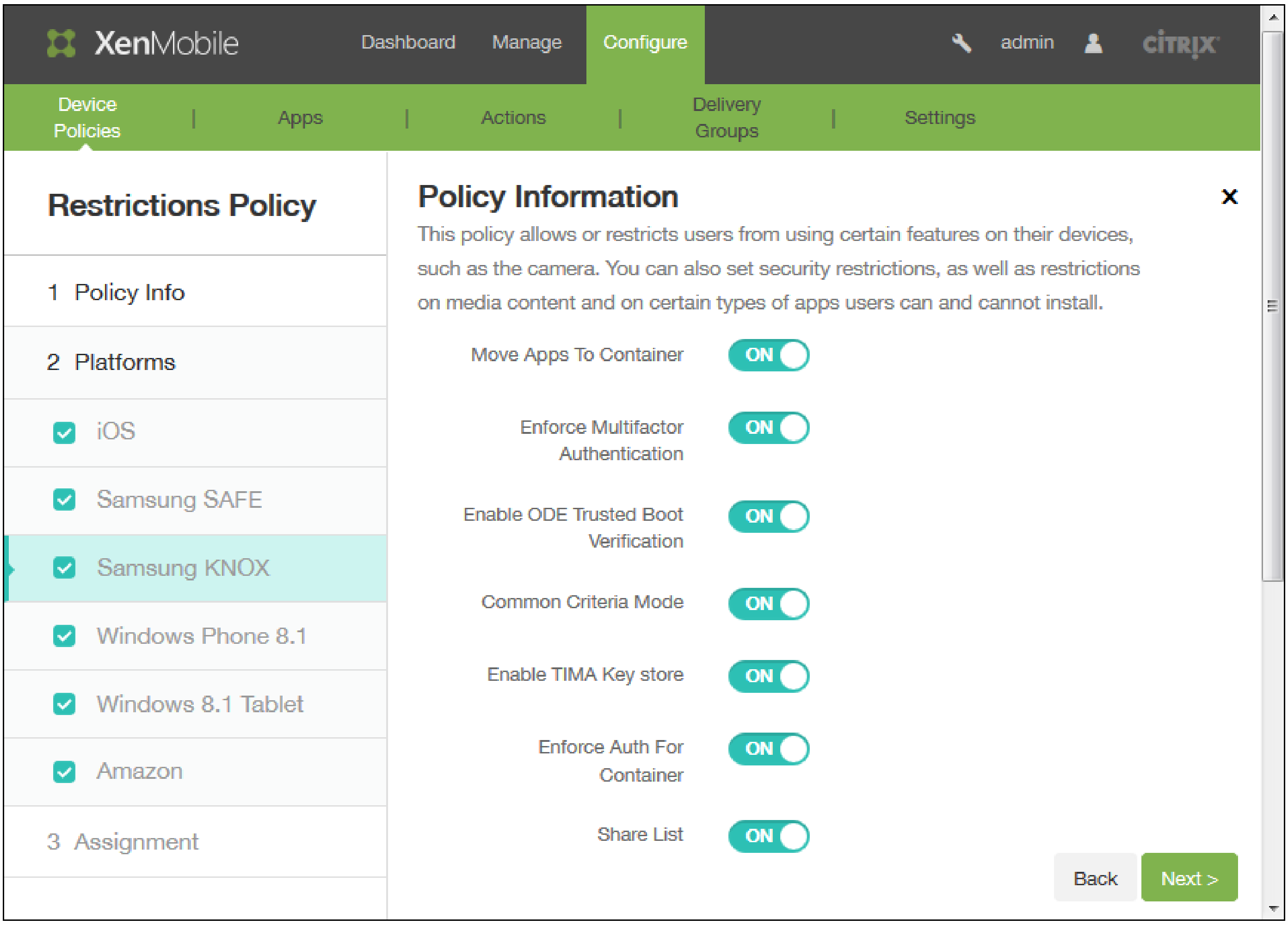
Backup: ON

Over The Air Upgrade: ON

Background data: ON

    -

-
    -
    -
    -
    -
    -



Restrictions Policy

1 Policy Info

2 Platforms

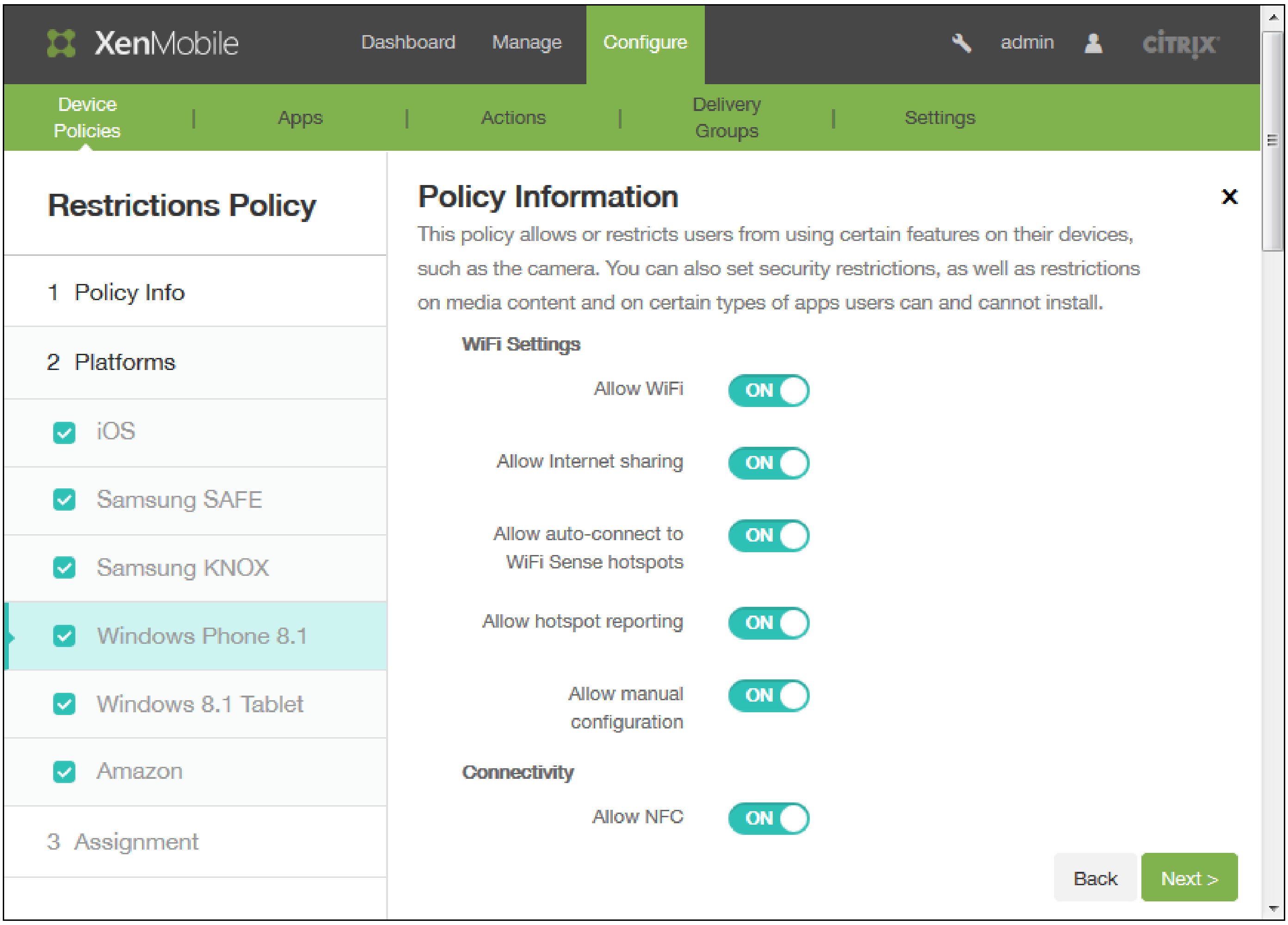
- ☑ iOS
- ☑ Samsung SAFE
- ☑ Samsung KNOX
- ☑ Windows Phone 8.1
- ☑ Windows 8.1 Tablet
- ☑ Amazon

3 Assignment

Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Move Apps To Container	ON
Enforce Multifactor Authentication	ON
Enable ODE Trusted Boot Verification	ON
Common Criteria Mode	ON
Enable TIMA Key store	ON
Enforce Auth For Container	ON
Share List	ON



Restrictions Policy

1 Policy Info

2 Platforms

☑ iOS

☑ Samsung SAFE

☑ Samsung KNOX

☑ Windows Phone 8.1

☑ Windows 8.1 Tablet

☑ Amazon

3 Assignment

Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

WiFi Settings

Allow WiFi ON

Allow Internet sharing ON

Allow auto-connect to WiFi Sense hotspots ON

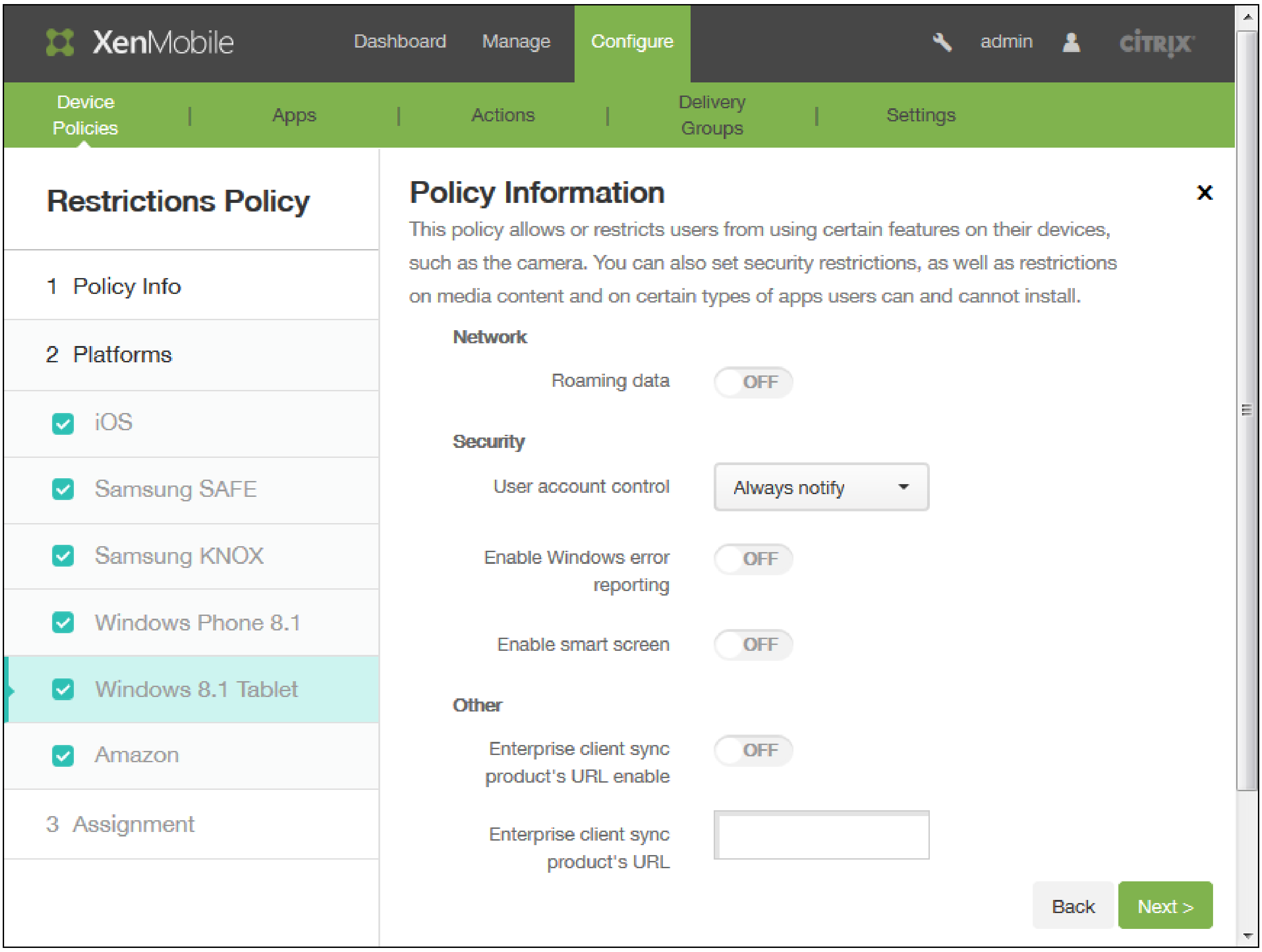
Allow hotspot reporting ON

Allow manual configuration ON

Connectivity

Allow NFC ON

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



Restrictions Policy

1 Policy Info

2 Platforms

- ☑ iOS
- ☑ Samsung SAFE
- ☑ Samsung KNOX
- ☑ Windows Phone 8.1
- ☑ Windows 8.1 Tablet
- ☑ Amazon

3 Assignment

Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Network

Roaming data: OFF

Security

User account control: Always notify

Enable Windows error reporting: OFF

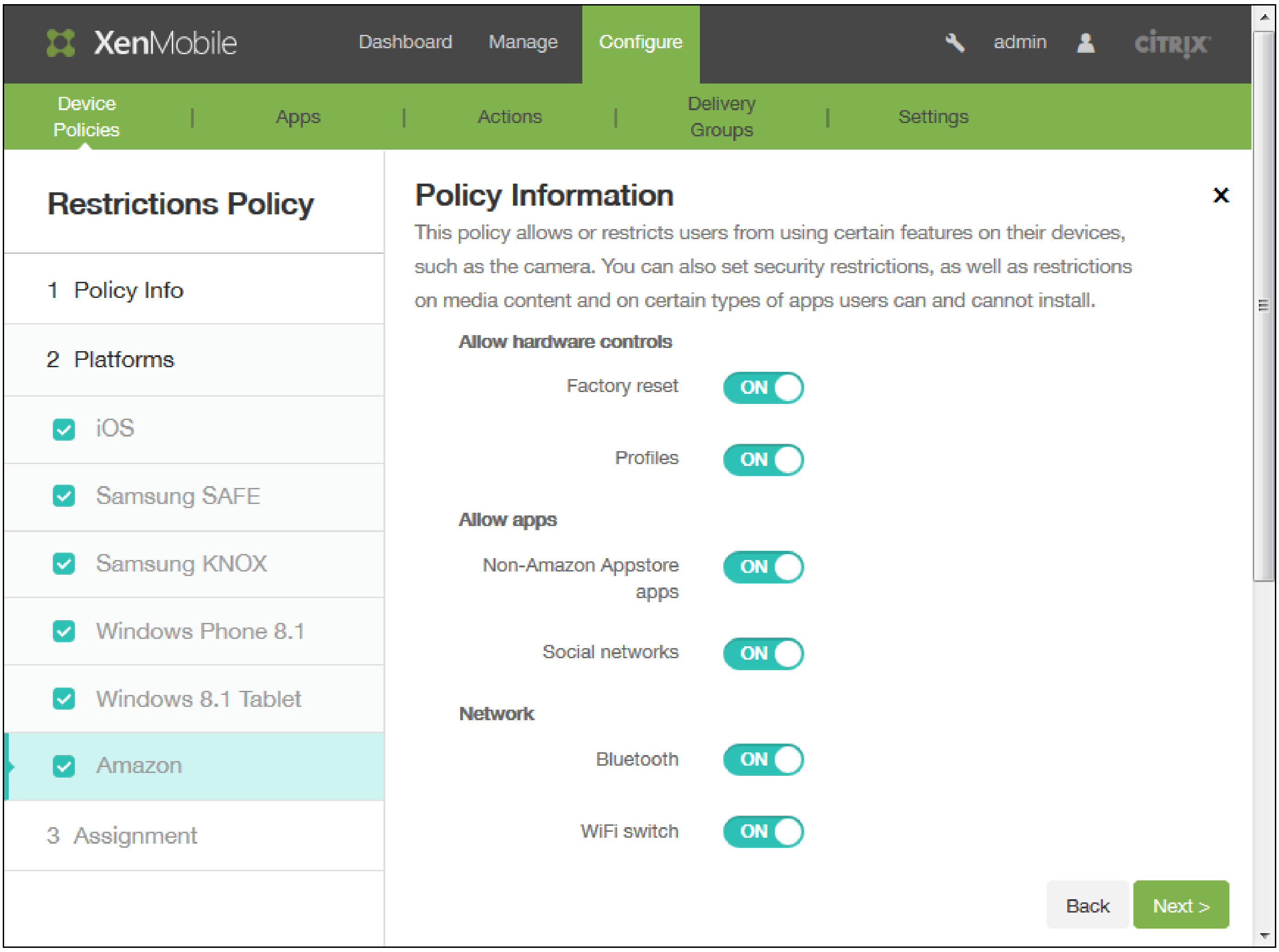
Enable smart screen: OFF

Other

Enterprise client sync product's URL enable: OFF

Enterprise client sync product's URL:

  -
  -



Restrictions Policy

1 Policy Info

2 Platforms

☑ iOS

☑ Samsung SAFE

☑ Samsung KNOX

☑ Windows Phone 8.1

☑ Windows 8.1 Tablet

☑ Amazon

3 Assignment

Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Allow hardware controls

Factory reset ON

Profiles ON

Allow apps

Non-Amazon Appstore apps ON

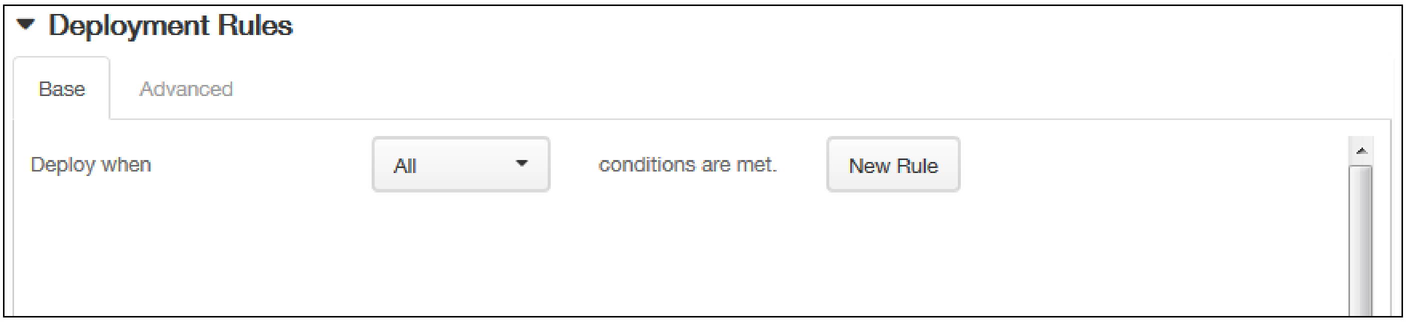
Social networks ON

Network

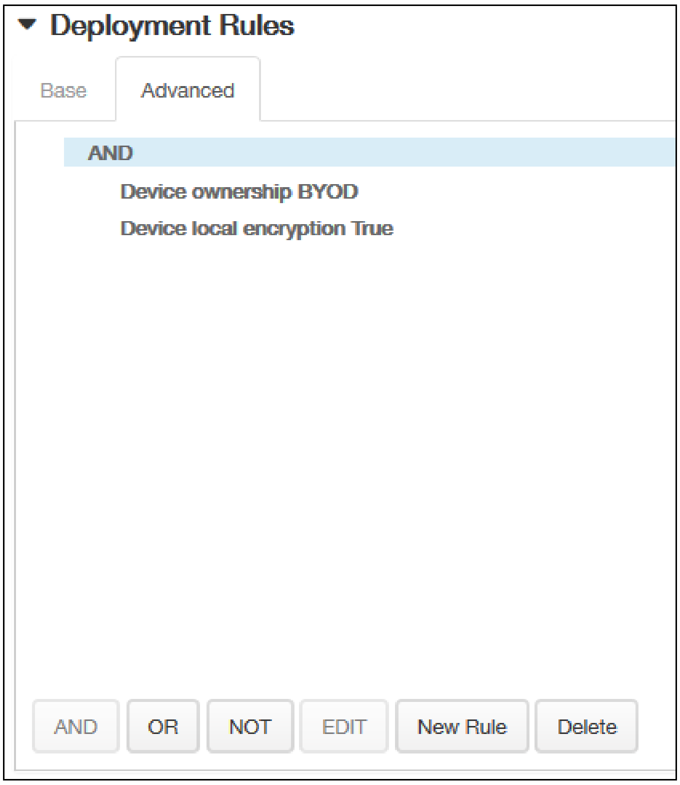
Bluetooth ON

WiFi switch ON

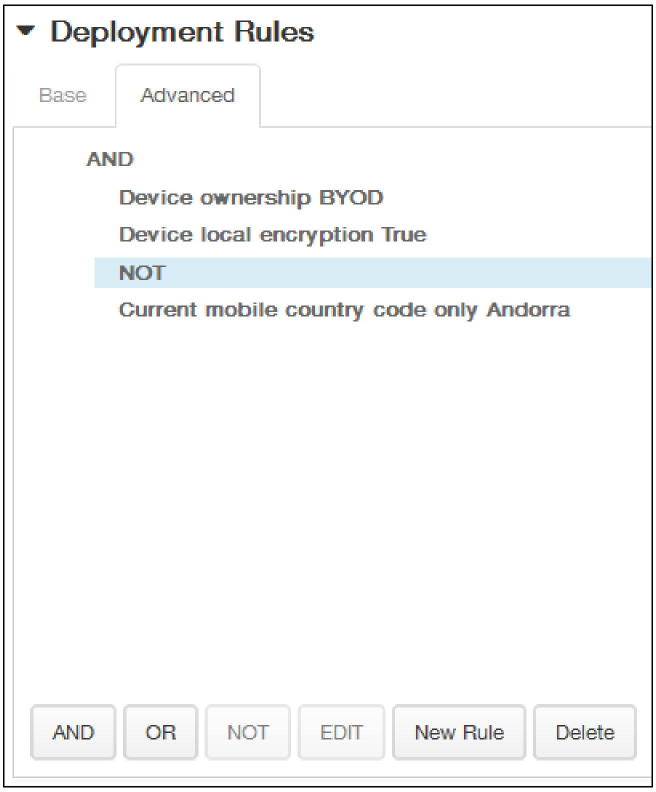
-
  -
  -
-
  -
  -
-
  -
  -
  -
  -
  -



Deployment Rules
Base
Advanced
Deploy when
All
conditions are met.
New Rule



Deployment Rules
Base
Advanced
AND
Device ownership BYOD
Device local encryption True
AND
OR
NOT
EDIT
New Rule
Delete



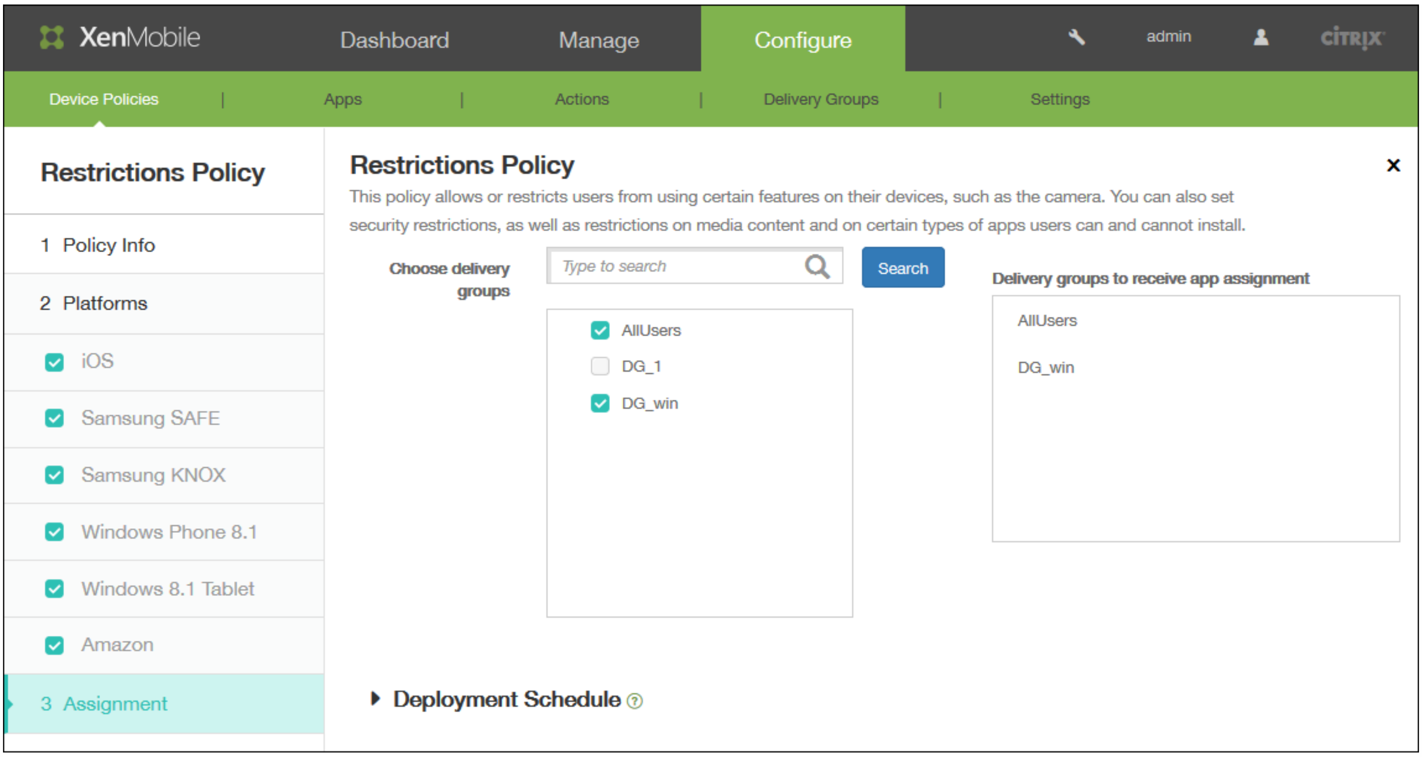
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Restrictions Policy

1 Policy Info

2 Platforms

☑ iOS

☑ Samsung SAFE

☑ Samsung KNOX

☑ Windows Phone 8.1

☑ Windows 8.1 Tablet

☑ Amazon

3 Assignment

Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Choose delivery groups: Type to search [Search]

☑ AllUsers

☐ DG_1

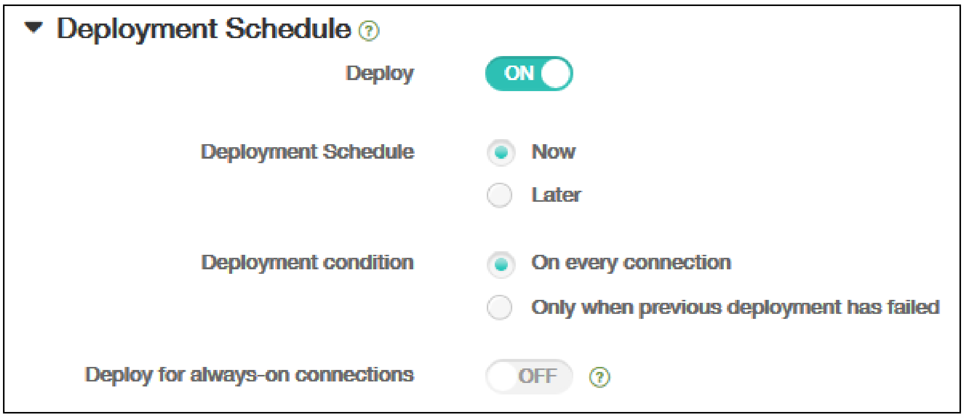
☑ DG_win

Delivery groups to receive app assignment

AllUsers

DG_win

▸ Deployment Schedule



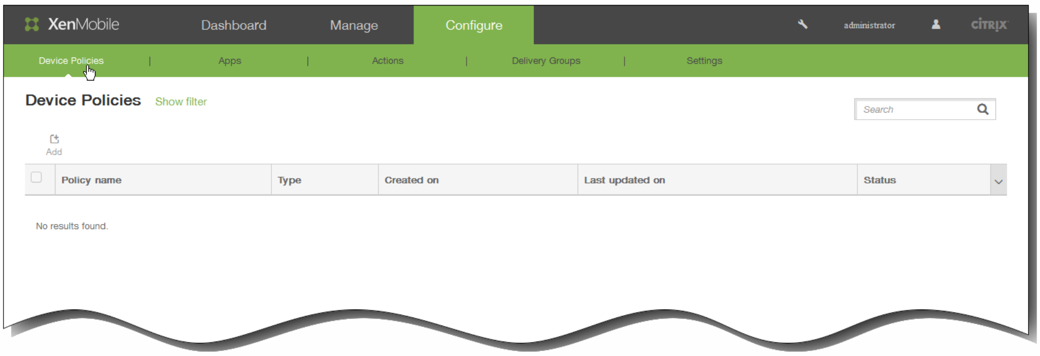
Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

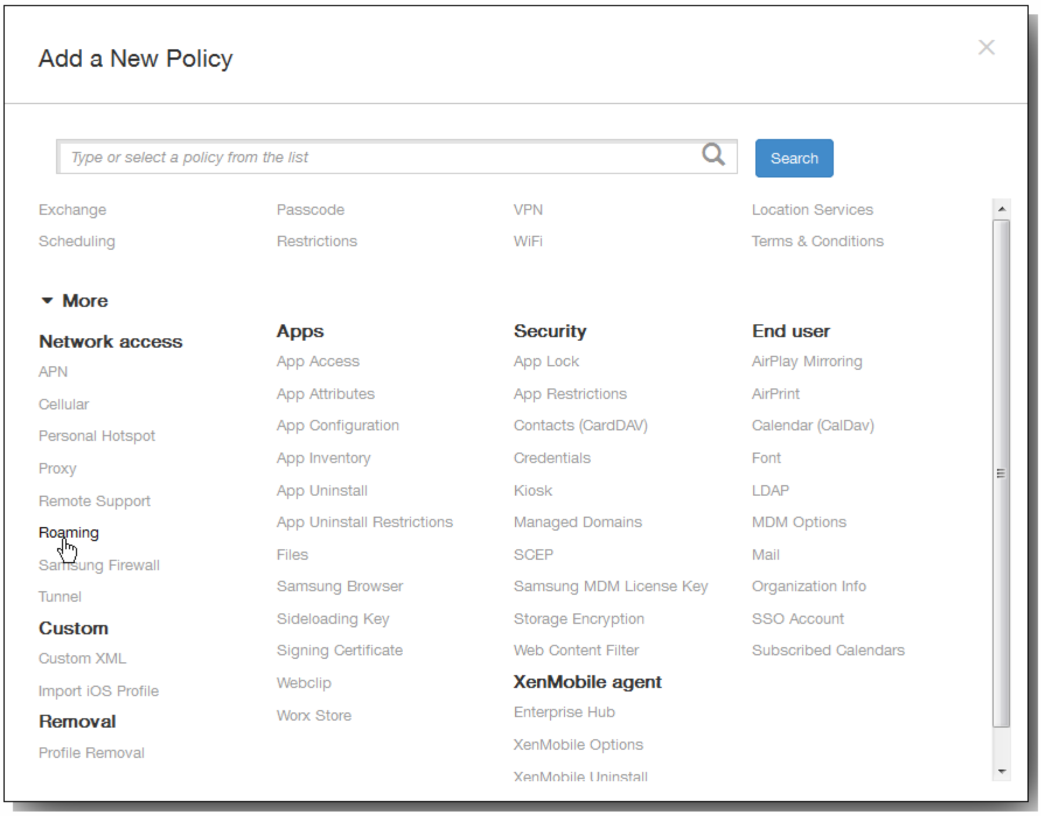
Deployment condition: ● On every connection ○ Only when previous deployment has failed

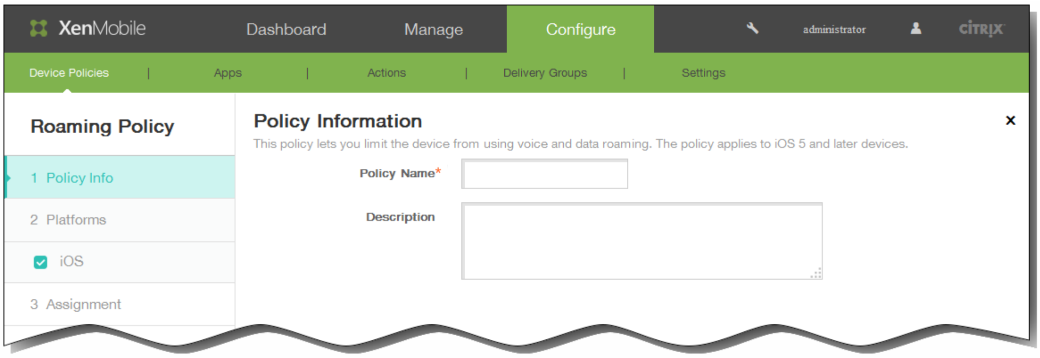
Deploy for always-on connections: OFF



	Policy name	Type	Created on	Last updated on	Status

No results found.



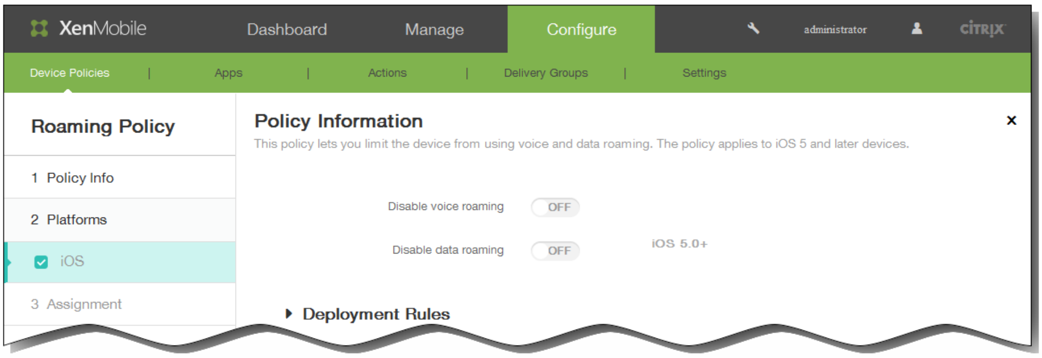


Policy Information

This policy lets you limit the device from using voice and data roaming. The policy applies to iOS 5 and later devices.

Policy Name*

Description



Policy Information

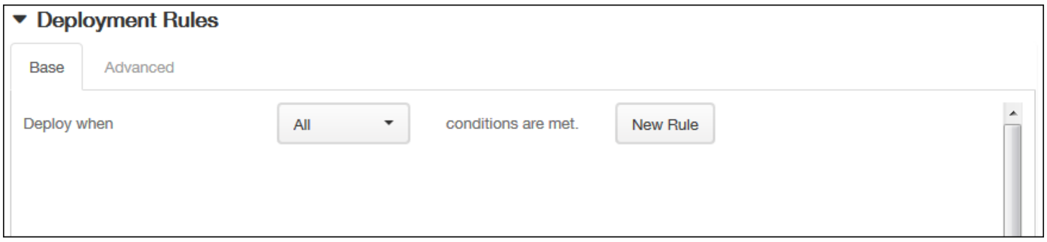
This policy lets you limit the device from using voice and data roaming. The policy applies to iOS 5 and later devices.

Disable voice roaming OFF

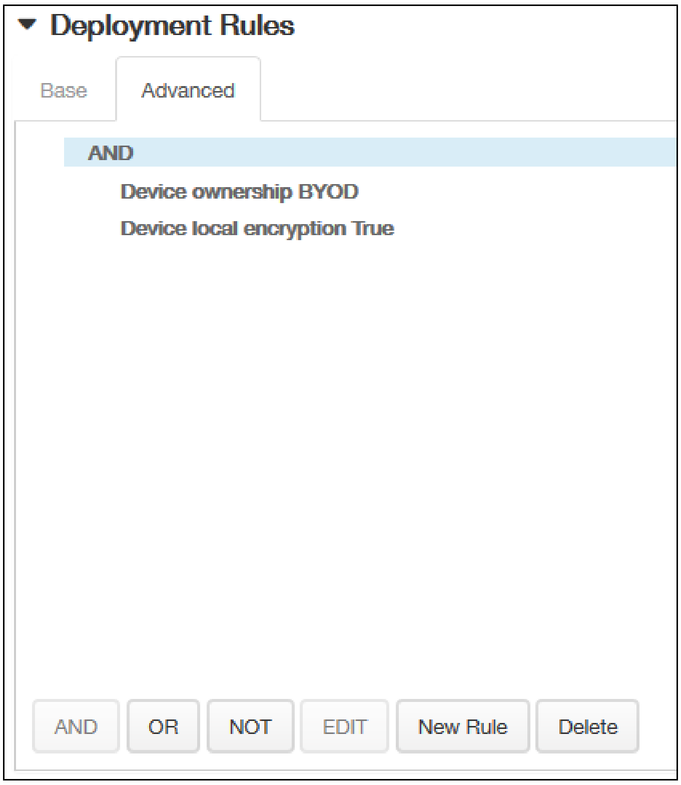
Disable data roaming OFF

iOS 5.0+

Deployment Rules



Deploy when All conditions are met.

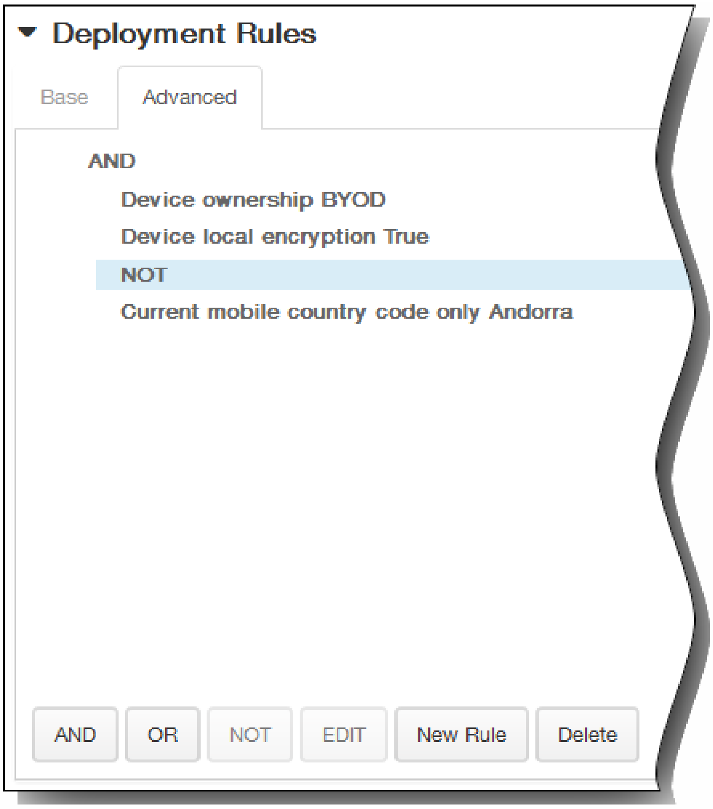


Deployment Rules

AND

Device ownership BYOD

Device local encryption True



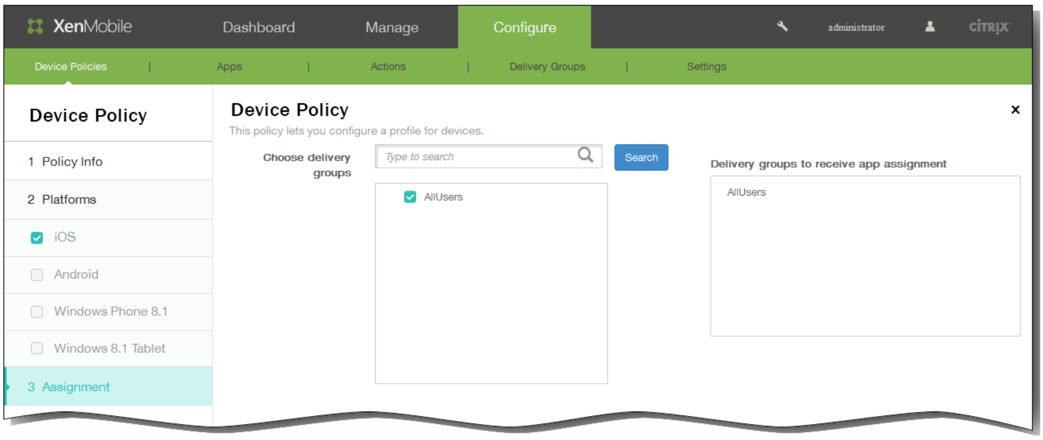
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

Device Policy

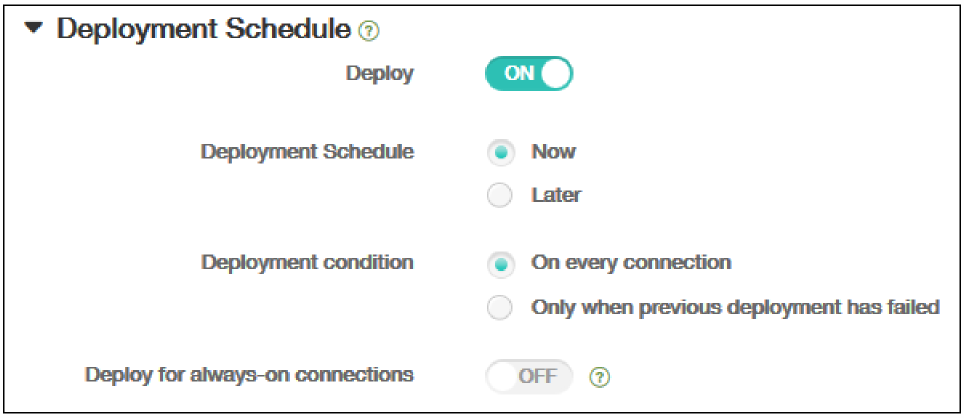
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



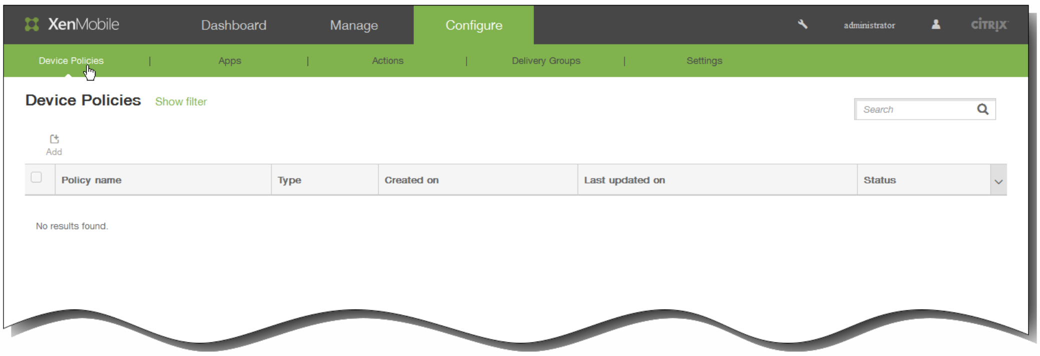
Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

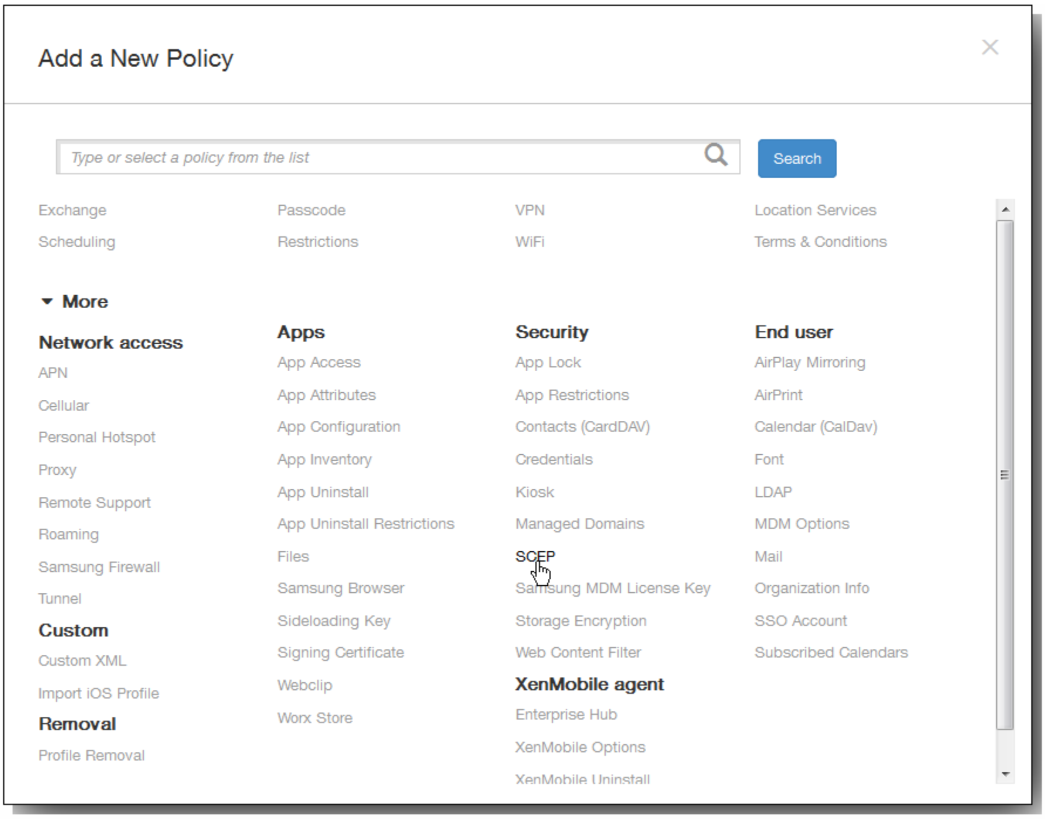
Deploy for always-on connections: OFF

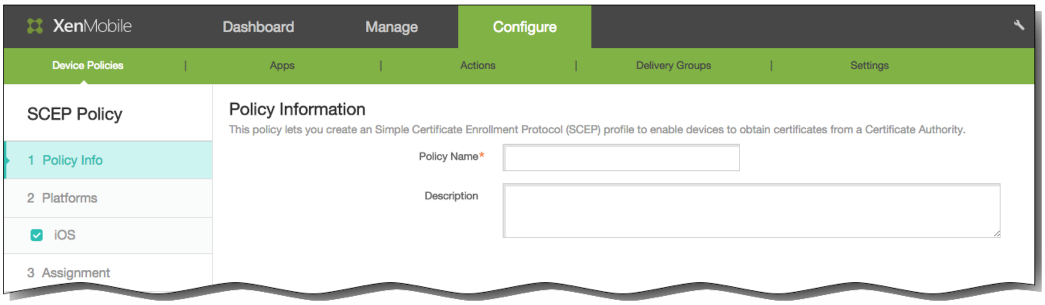


Device Policies

	Policy name	Type	Created on	Last updated on	Status

No results found.



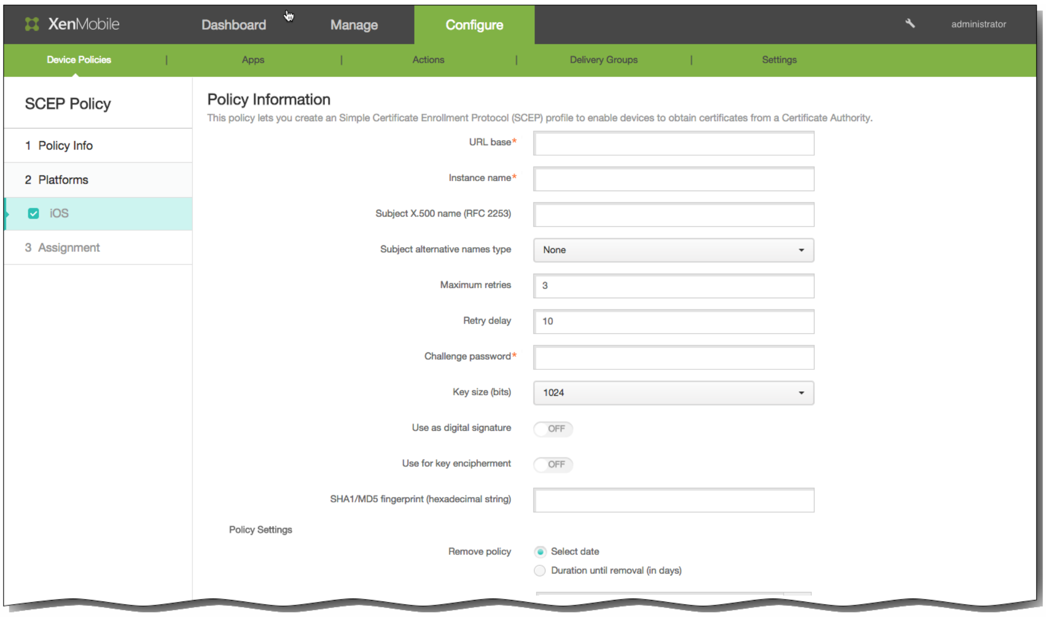


Policy Information

This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.

Policy Name*

Description



Policy Information

This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.

URL base*

Instance name*

Subject X.500 name (RFC 2253)

Subject alternative names type: None

Maximum retries: 3

Retry delay: 10

Challenge password*

Key size (bits): 1024

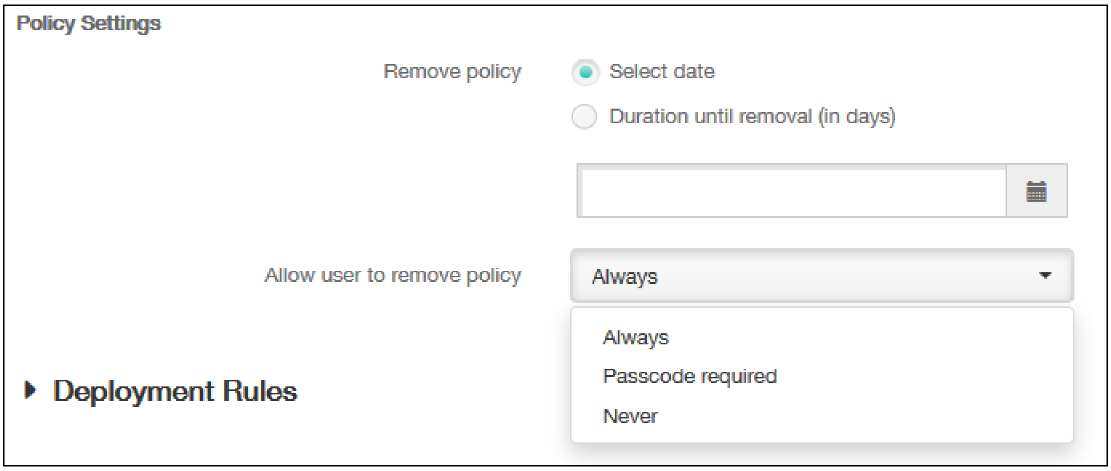
Use as digital signature: OFF

Use for key encipherment: OFF

SHA1/MD5 fingerprint (hexadecimal string)

Policy Settings

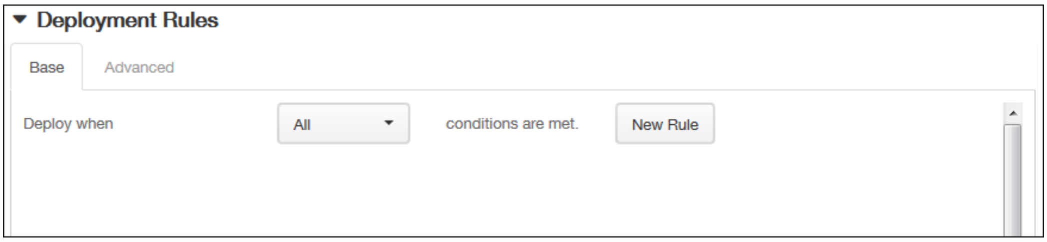
Remove policy: ● Select date ○ Duration until removal (in days)



Policy Settings

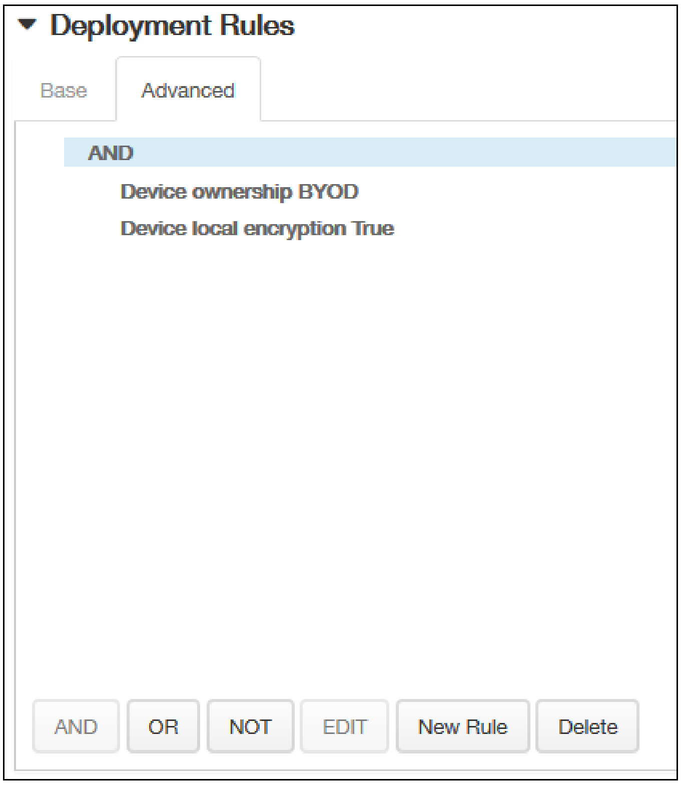
Remove policy ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always



Deployment Rules

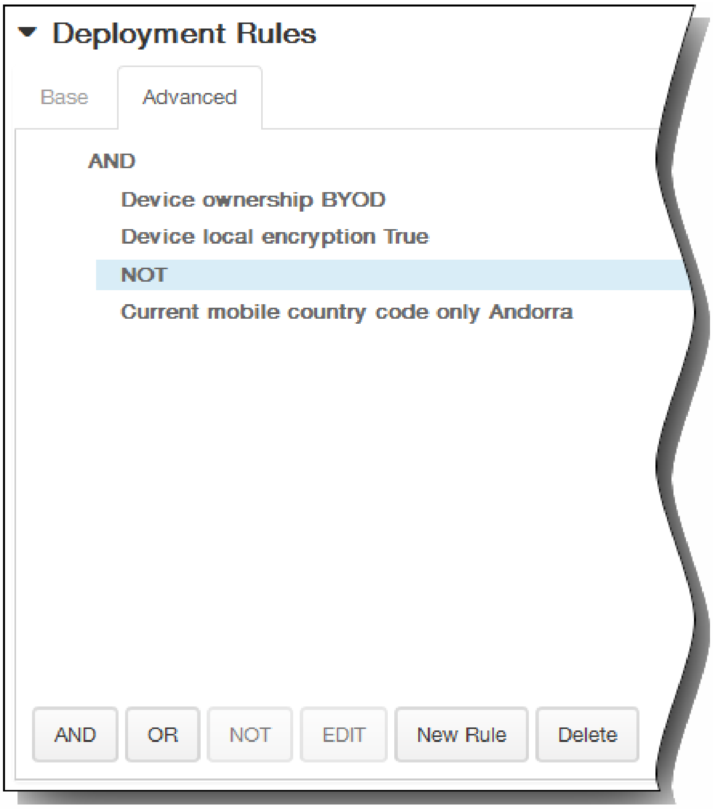
Deploy when All conditions are met.



AND

Device ownership BYOD

Device local encryption True



Deployment Rules

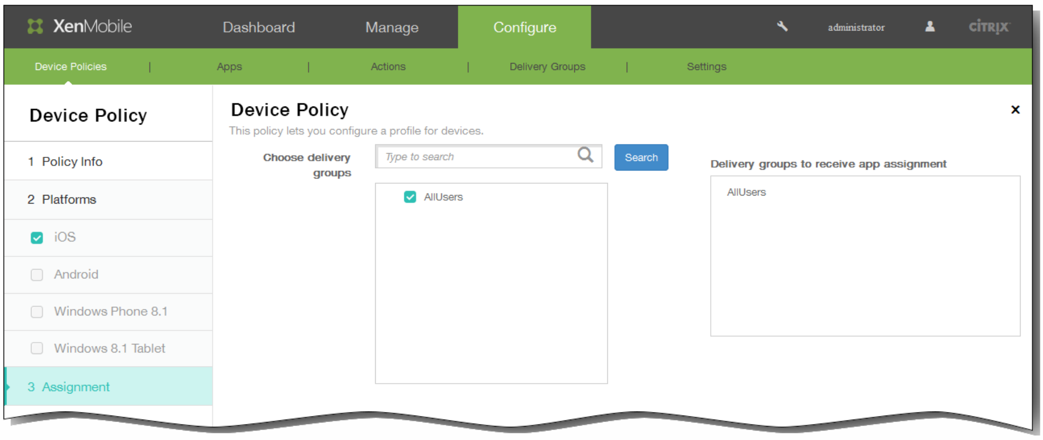
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

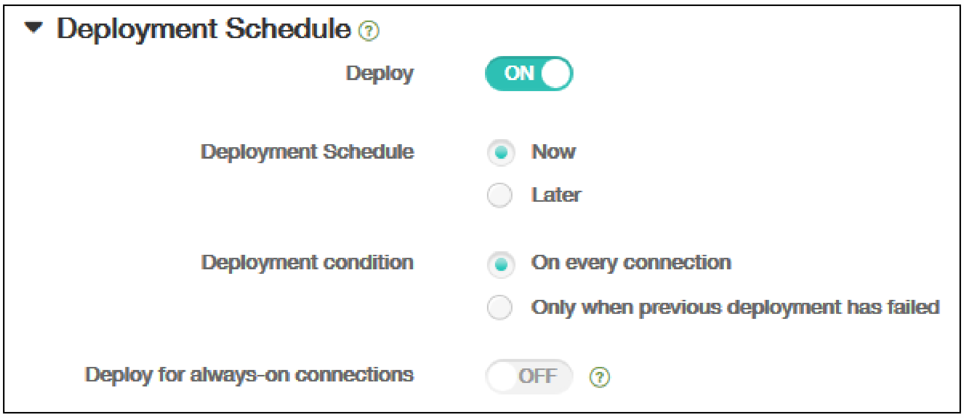
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



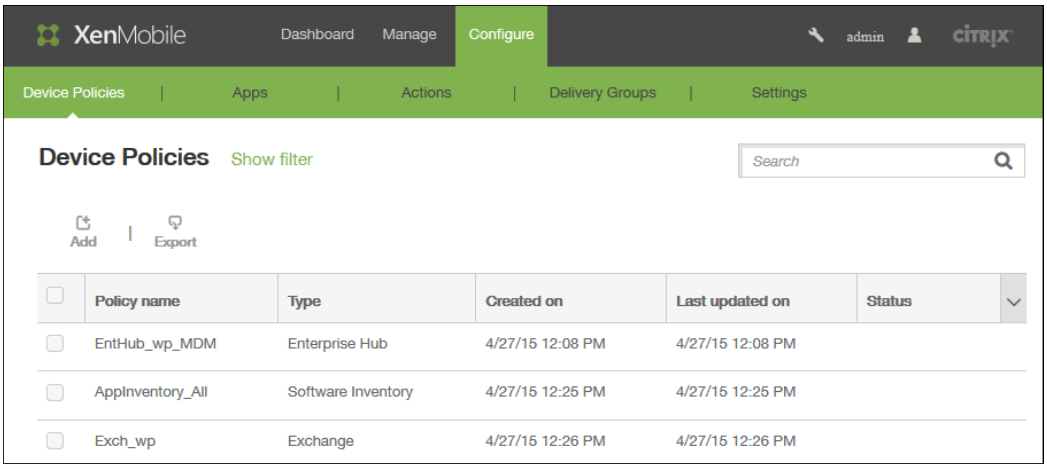
▾ Deployment Schedule ?

Deploy: ON

Deployment Schedule: ● Now ○ Later

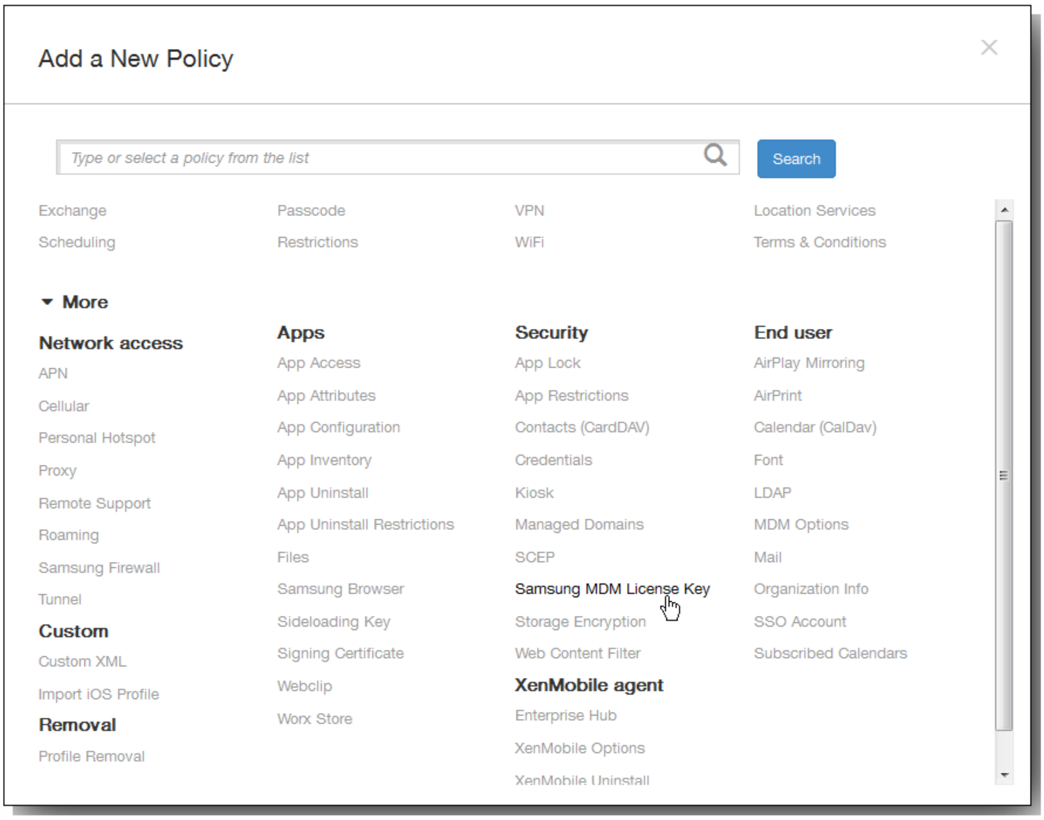
Deployment condition: ● On every connection ○ Only when previous deployment has failed

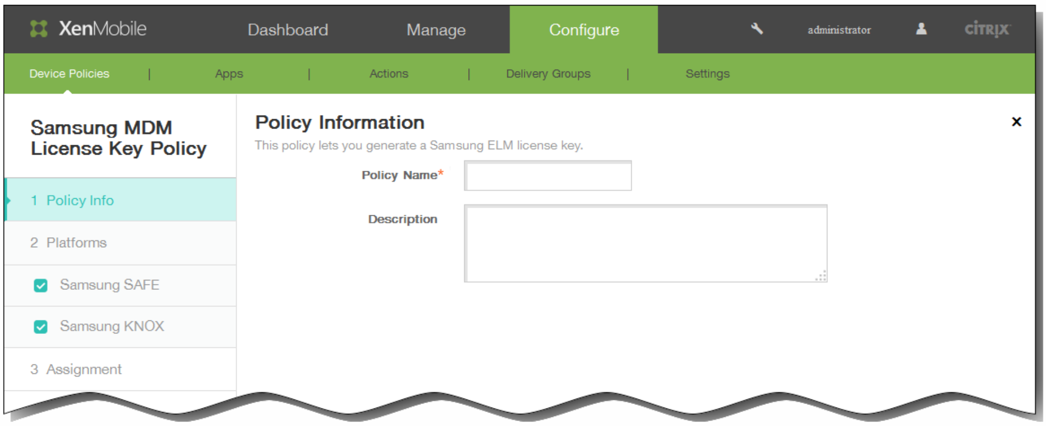
Deploy for always-on connections: OFF ?



Device Policies

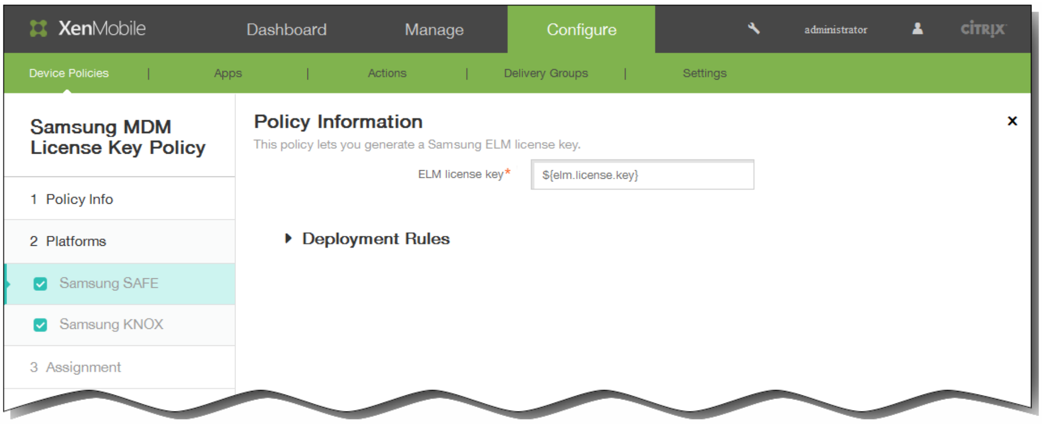
□	Policy name	Type	Created on	Last updated on	Status
□	EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
□	AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
□	Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	





Policy Information

This policy lets you generate a Samsung ELM license key.



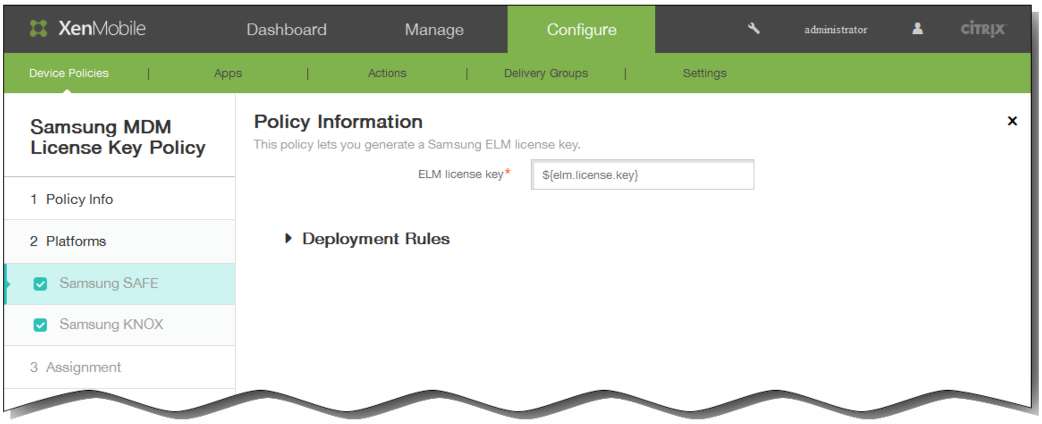
Samsung MDM License Key Policy

Policy Information

This policy lets you generate a Samsung ELM license key.

ELM license key* ${elm.license.key}

-



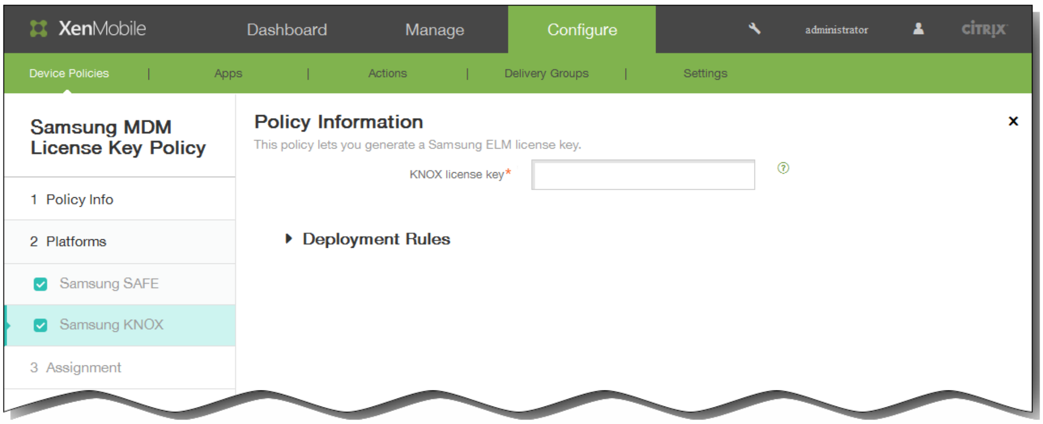
Samsung MDM License Key Policy

Policy Information

This policy lets you generate a Samsung ELM license key.

ELM license key* ${elm.license.key}

-

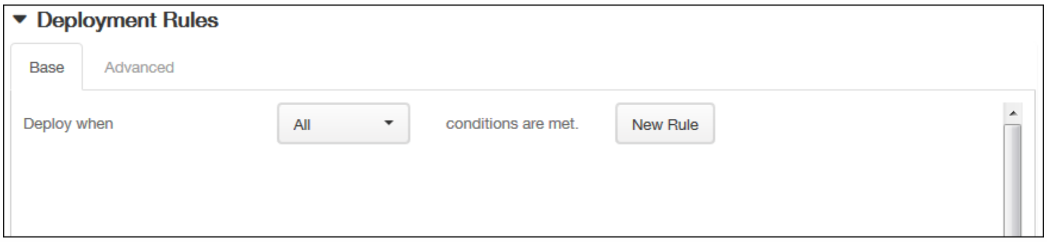


Samsung MDM License Key Policy

Policy Information

This policy lets you generate a Samsung ELM license key.

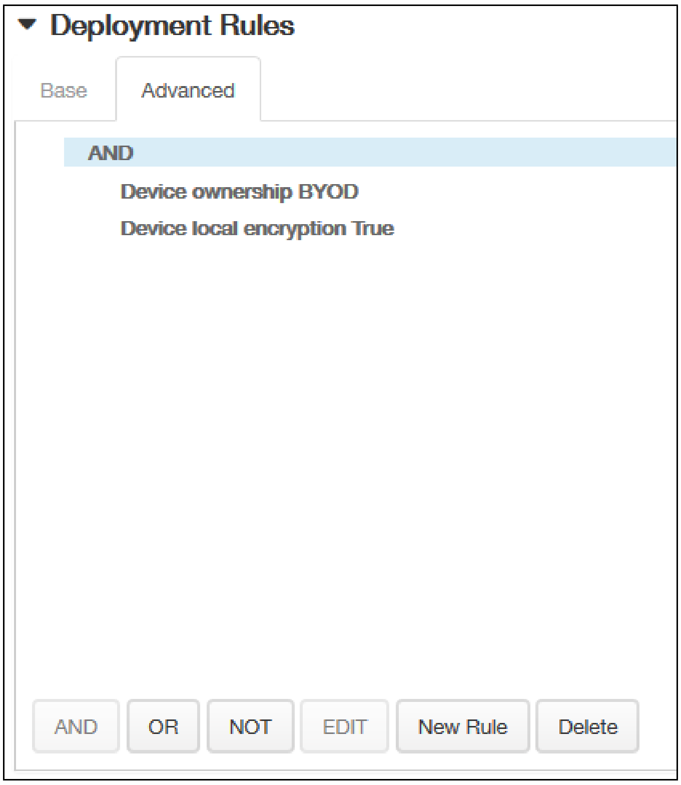
KNOX license key*



Deployment Rules

Base | Advanced

Deploy when All conditions are met. New Rule



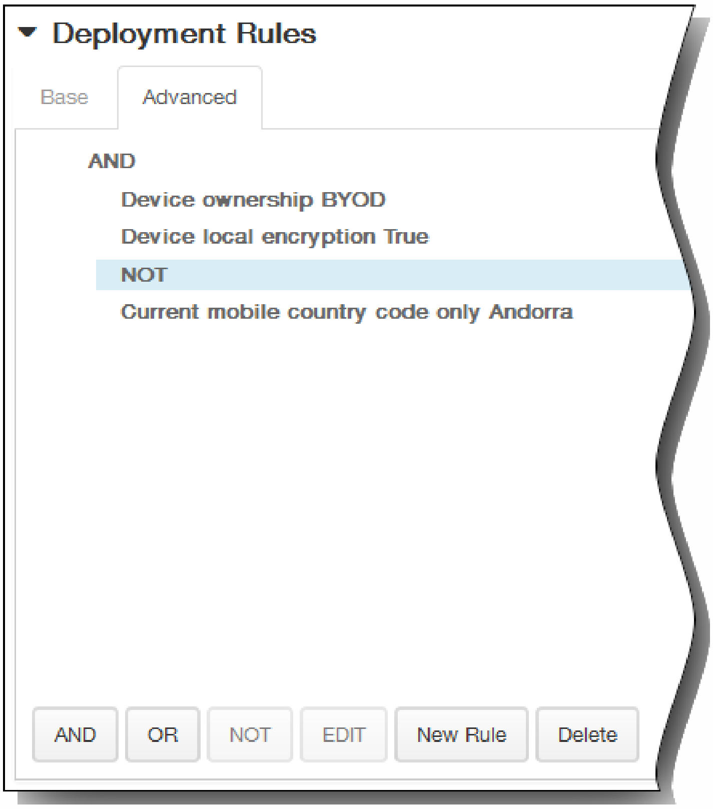
Deployment Rules

Base | Advanced

AND

Device ownership BYOD

Device local encryption True



Deployment Rules

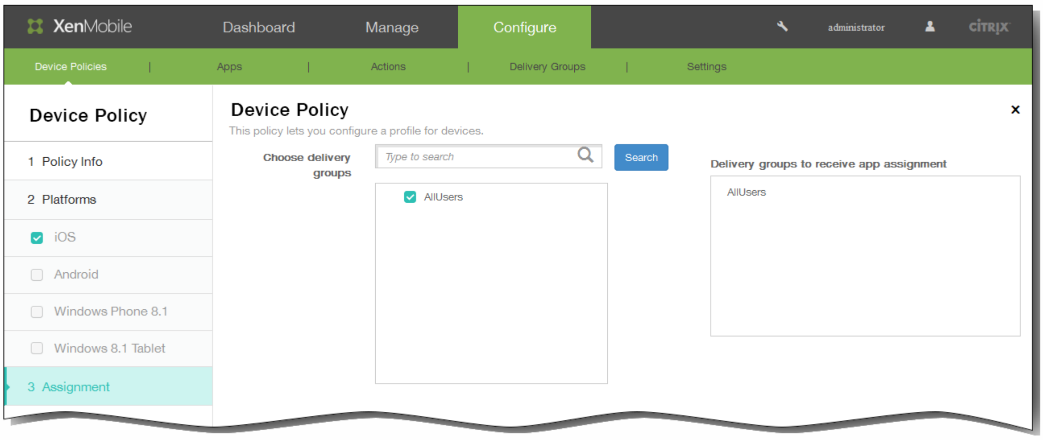
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

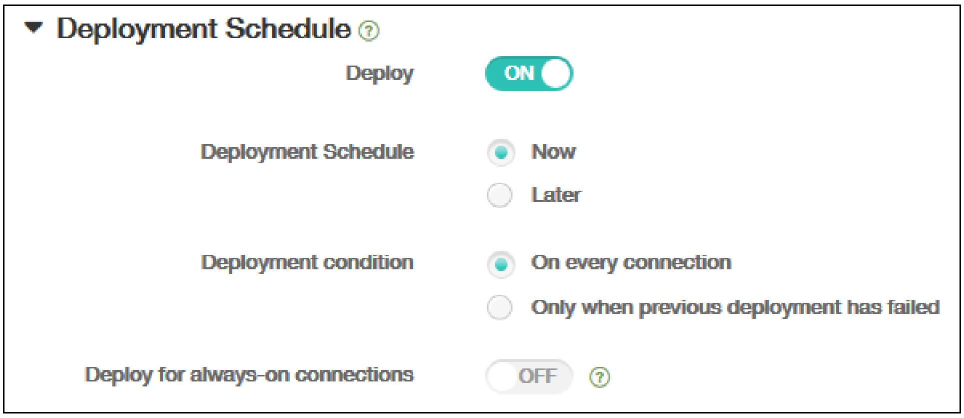
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



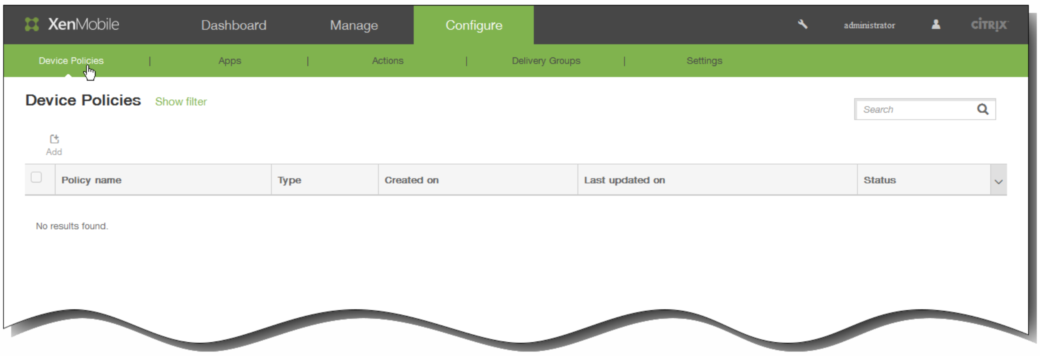
Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

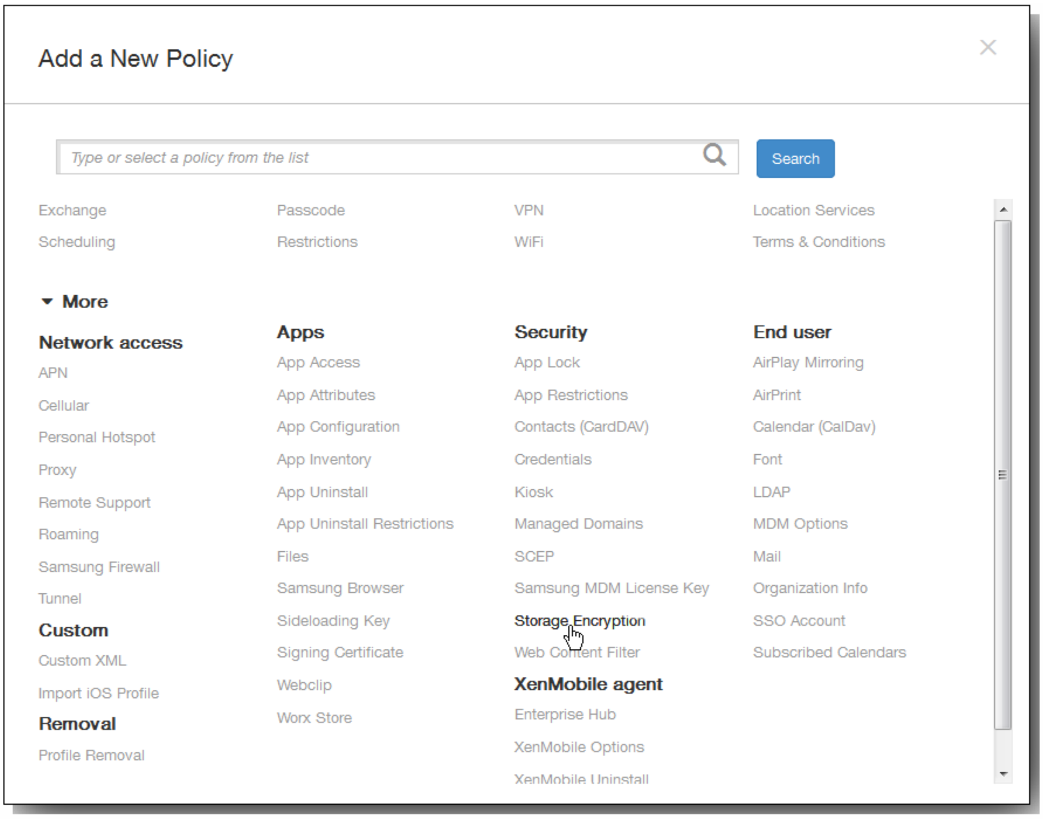
Deployment condition: ● On every connection ○ Only when previous deployment has failed

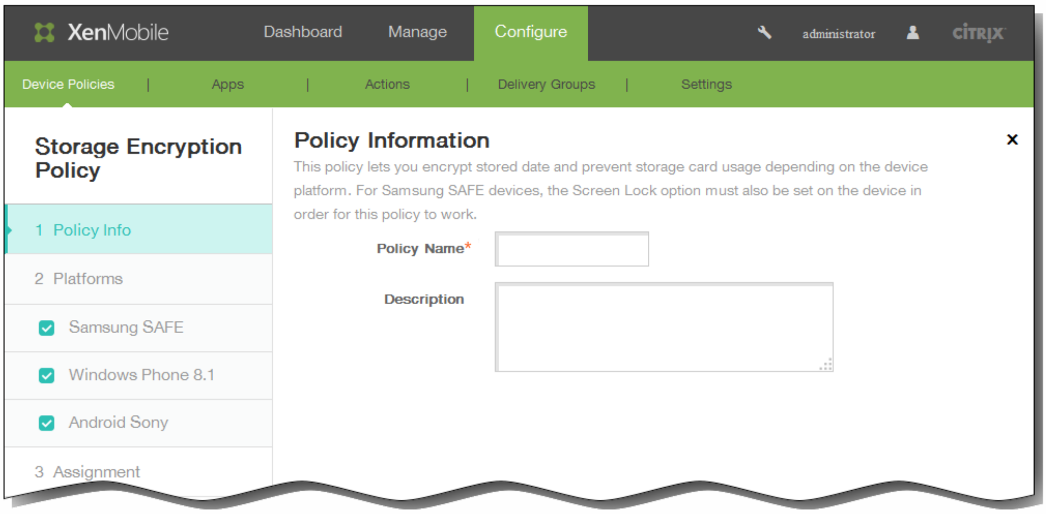
Deploy for always-on connections: OFF



□	Policy name	Type	Created on	Last updated on	Status

No results found.





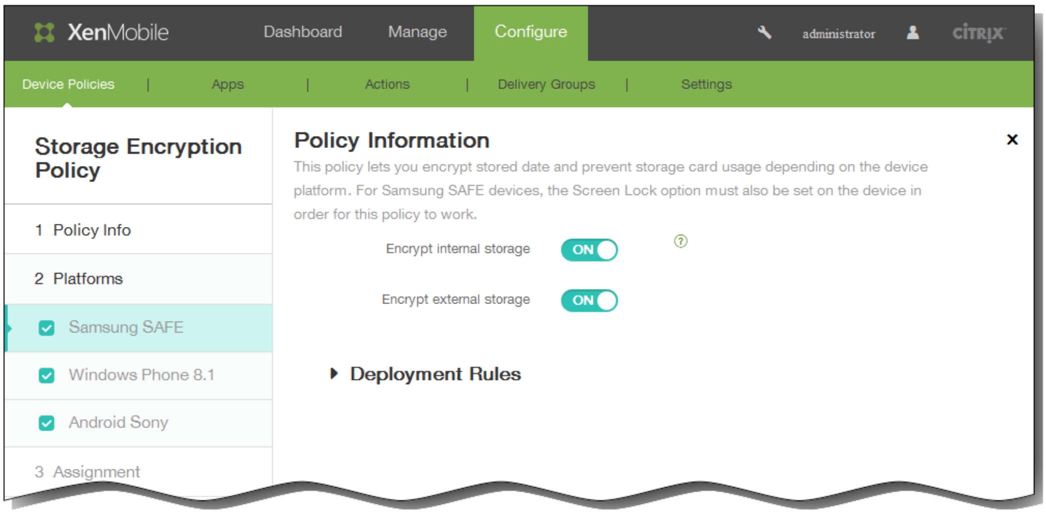
Policy Information

This policy lets you encrypt stored date and prevent storage card usage depending on the device platform. For Samsung SAFE devices, the Screen Lock option must also be set on the device in order for this policy to work.

Policy Name*

Description

-
    -
    -



XenMobile | Dashboard | Manage | Configure | administrator | Citrix

Device Policies | Apps | Actions | Delivery Groups | Settings

Storage Encryption Policy

1 Policy Info

2 Platforms

☑ Samsung SAFE

☑ Windows Phone 8.1

☑ Android Sony

3 Assignment

Policy Information

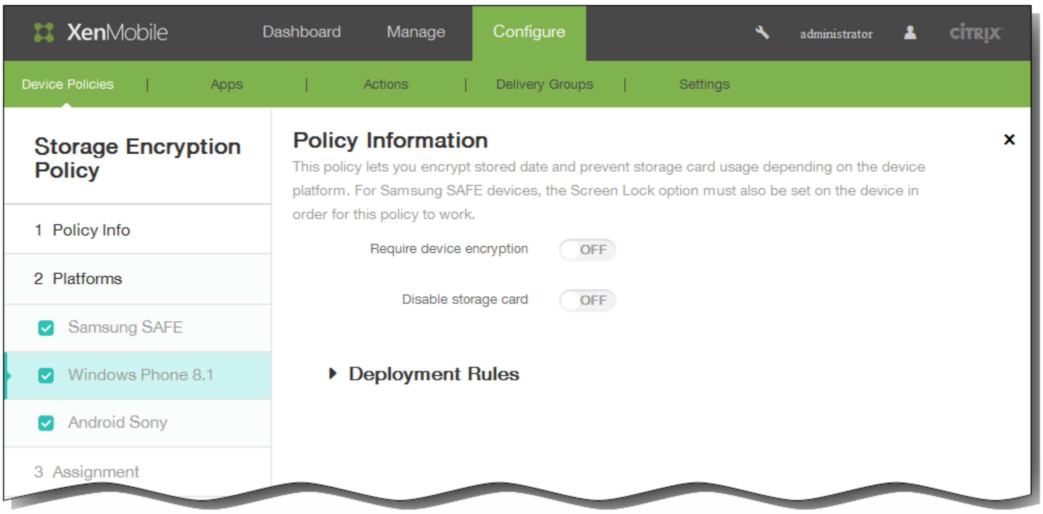
This policy lets you encrypt stored date and prevent storage card usage depending on the device platform. For Samsung SAFE devices, the Screen Lock option must also be set on the device in order for this policy to work.

Encrypt internal storage: ON

Encrypt external storage: ON

▸ Deployment Rules

-
    -
    -



XenMobile | Dashboard | Manage | Configure | administrator | Citrix

Device Policies | Apps | Actions | Delivery Groups | Settings

Storage Encryption Policy

1 Policy Info

2 Platforms

☑ Samsung SAFE

☑ Windows Phone 8.1

☑ Android Sony

3 Assignment

Policy Information

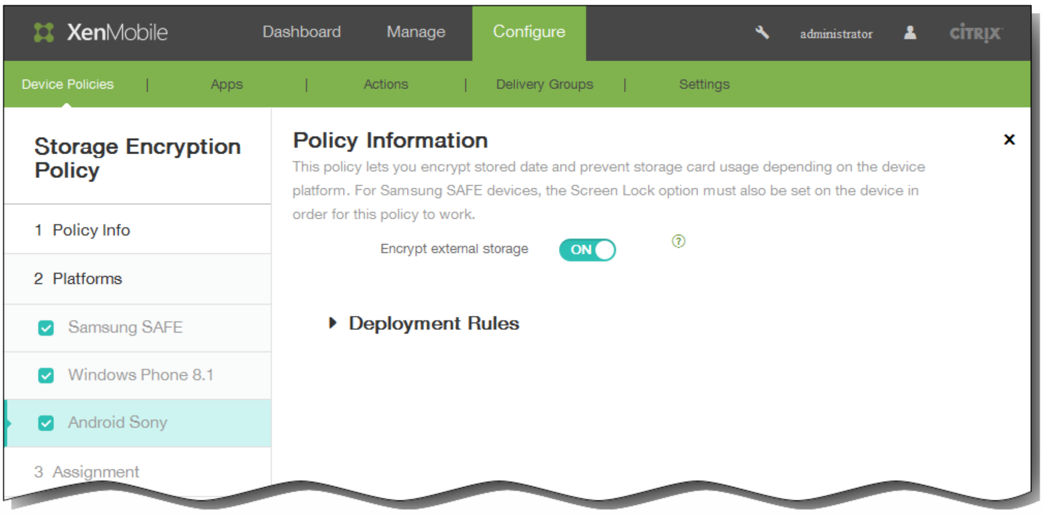
This policy lets you encrypt stored date and prevent storage card usage depending on the device platform. For Samsung SAFE devices, the Screen Lock option must also be set on the device in order for this policy to work.

Require device encryption: OFF

Disable storage card: OFF

▸ Deployment Rules

-



Storage Encryption Policy

1 Policy Info

2 Platforms

☑ Samsung SAFE

☑ Windows Phone 8.1

☑ Android Sony

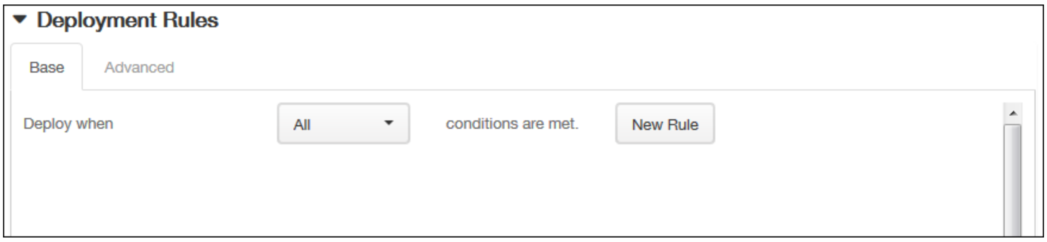
3 Assignment

Policy Information

This policy lets you encrypt stored date and prevent storage card usage depending on the device platform. For Samsung SAFE devices, the Screen Lock option must also be set on the device in order for this policy to work.

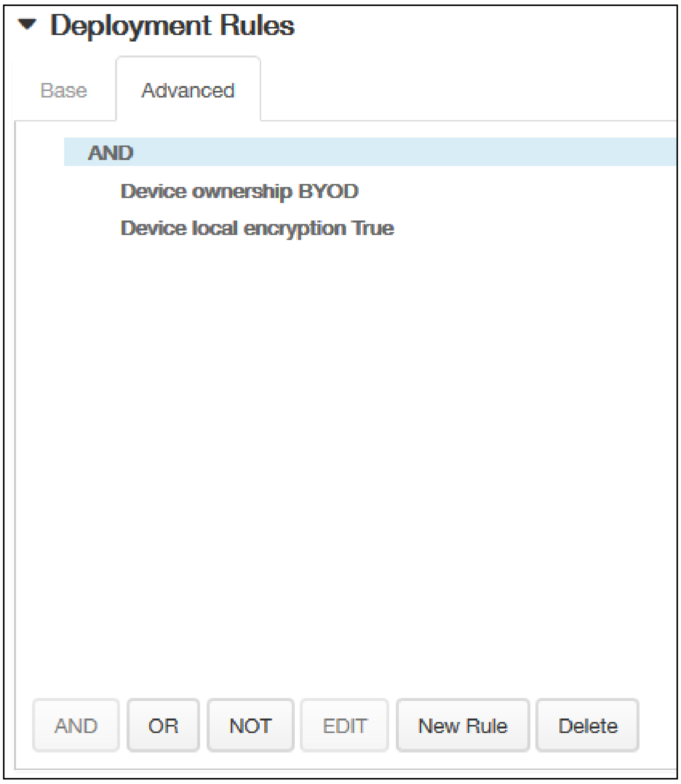
Encrypt external storage: ON

▸ Deployment Rules



▾ Deployment Rules

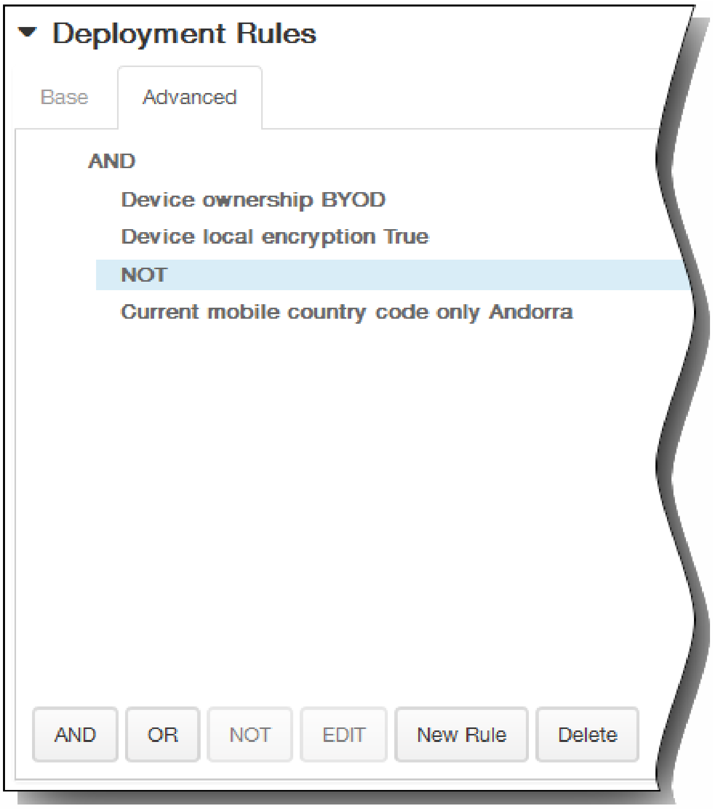
Deploy when All conditions are met.



AND

Device ownership BYOD

Device local encryption True



Deployment Rules

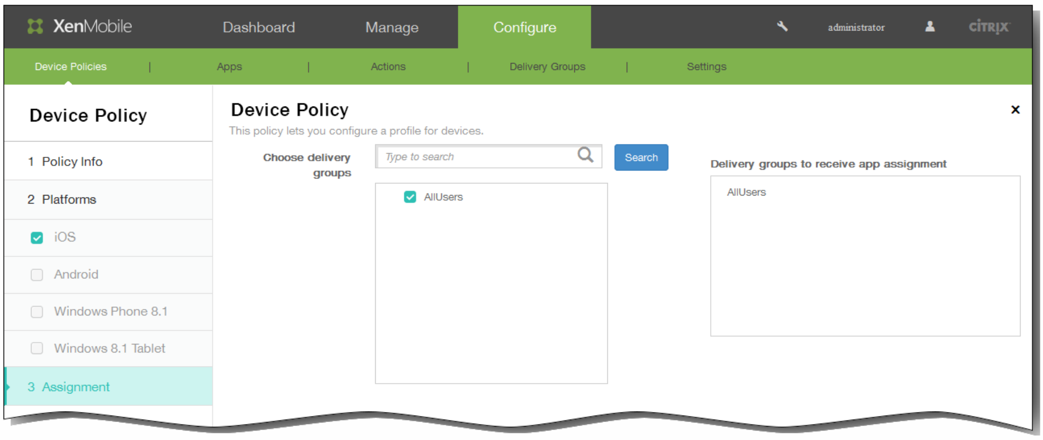
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

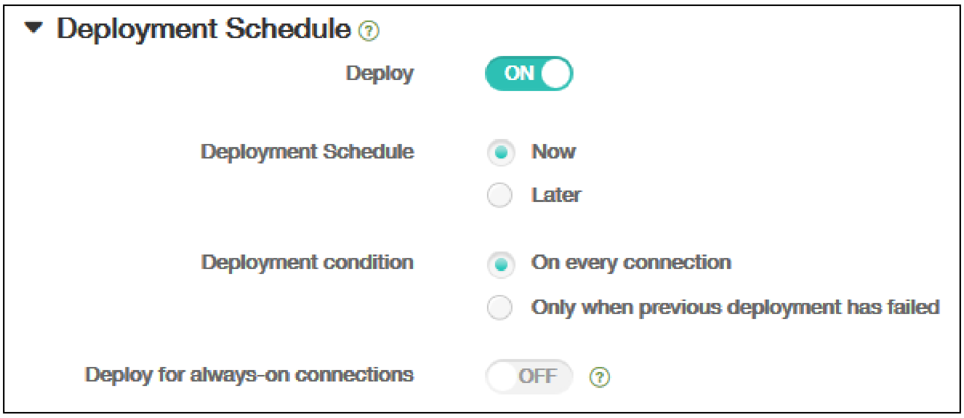
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



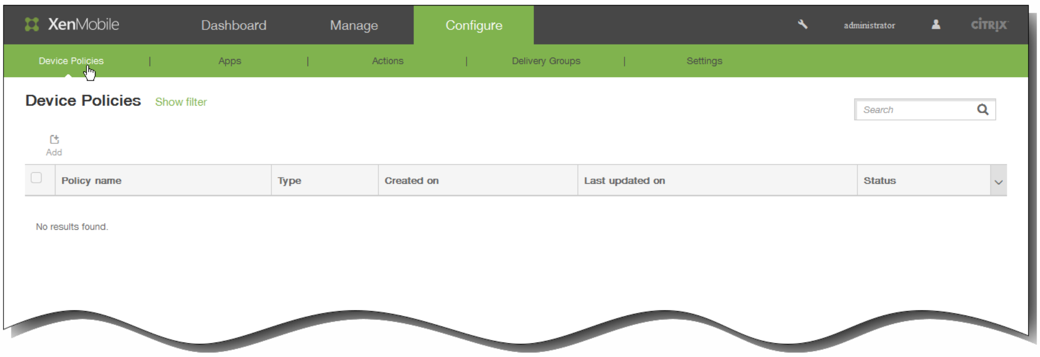
Deployment Schedule

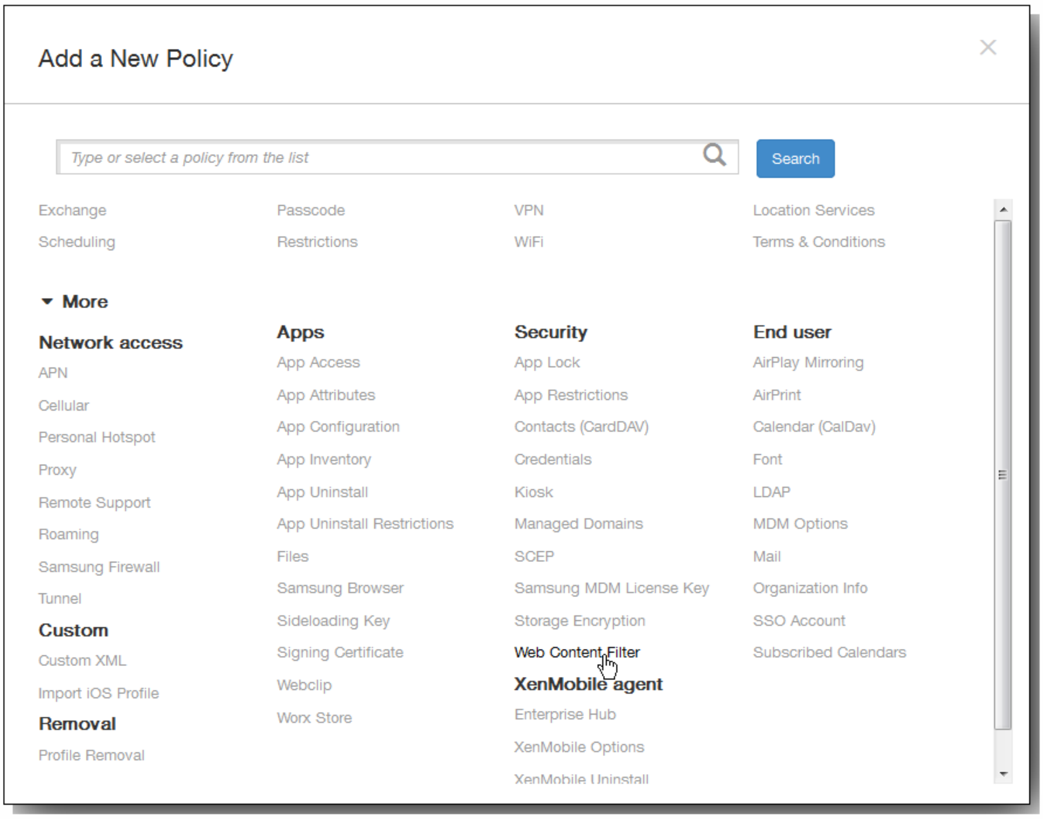
Deploy: ON

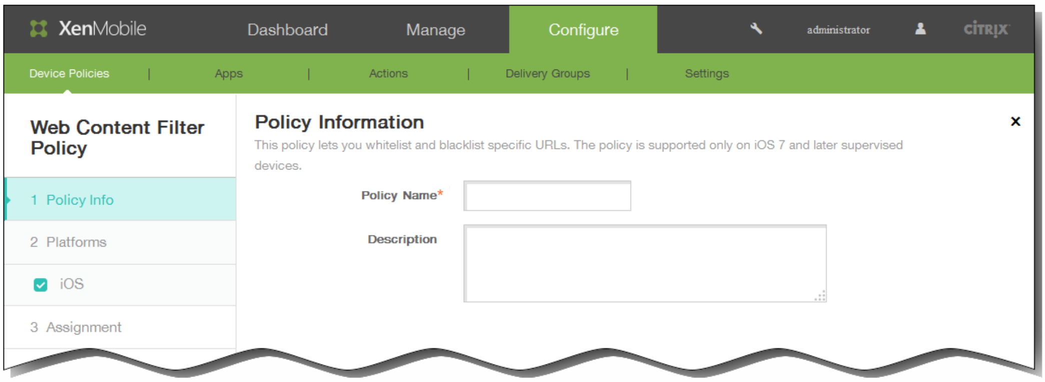
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies
Apps
Actions
Delivery Groups
Settings
Device Policies
Show filter
Search
Add
Policy name
Type
Created on
Last updated on
Status
No results found.


Add a New Policy
Type or select a policy from the list
Search
Exchange
Scheduling
Passcode
Restrictions
VPN
WiFi
Location Services
Terms & Conditions
More
Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel
Custom
Custom XML
Import iOS Profile
Removal
Profile Removal
Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store
Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter
XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall
End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars



Web Content Filter Policy

1 Policy Info

2 Platforms

☑ iOS

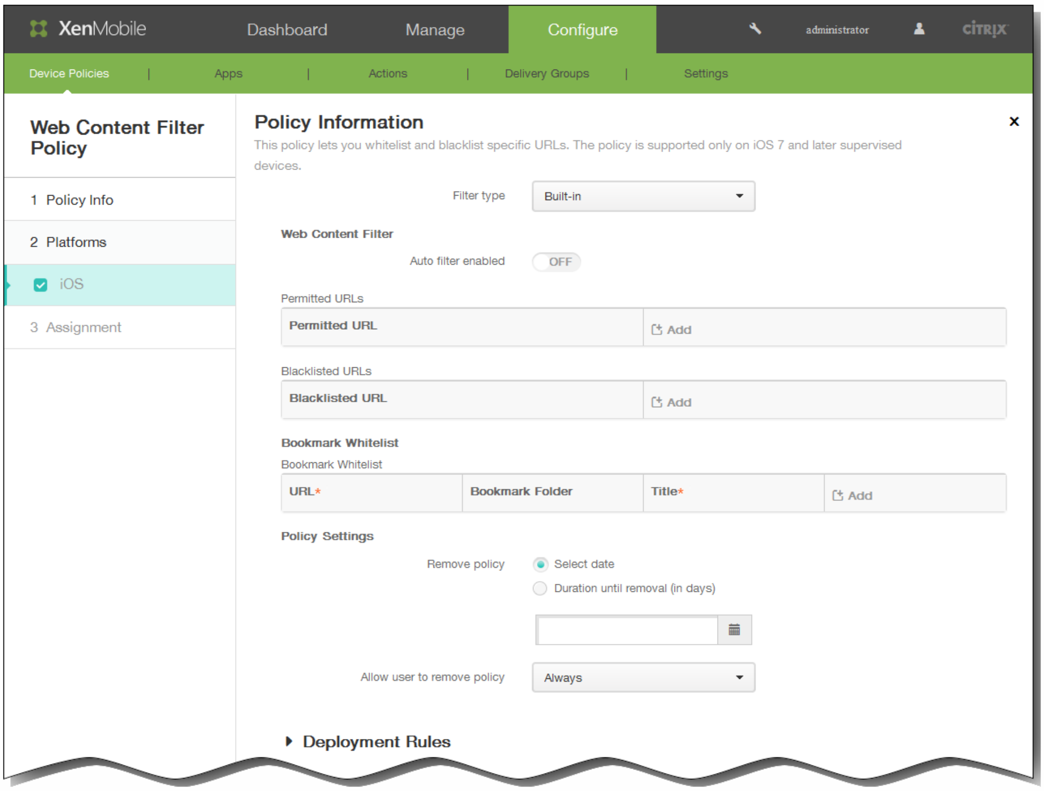
3 Assignment

Policy Information

This policy lets you whitelist and blacklist specific URLs. The policy is supported only on iOS 7 and later supervised devices.

Policy Name*

Description



Web Content Filter Policy

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

Policy Information

This policy lets you whitelist and blacklist specific URLs. The policy is supported only on iOS 7 and later supervised devices.

Filter type: Built-in

Web Content Filter

Auto filter enabled: OFF

Permitted URLs

Permitted URL	Add

Blacklisted URLs

Blacklisted URL	Add

Bookmark Whitelist

Bookmark Whitelist

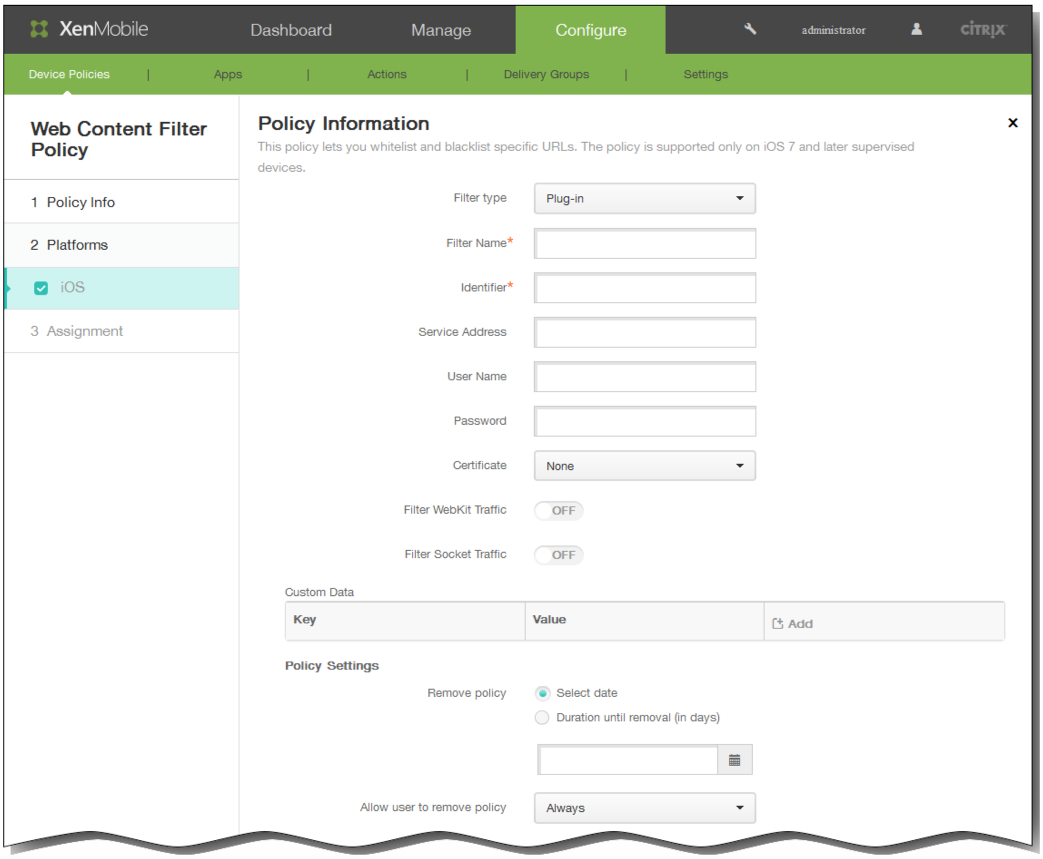
URL*	Bookmark Folder	Title*	Add

Policy Settings

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

Allow user to remove policy: Always

▸ Deployment Rules



Web Content Filter Policy

1 Policy Info

2 Platforms

☑ iOS

3 Assignment

Policy Information

This policy lets you whitelist and blacklist specific URLs. The policy is supported only on iOS 7 and later supervised devices.

Filter type	Plug-in
Filter Name*	
Identifier*	
Service Address	
User Name	
Password	
Certificate	None
Filter WebKit Traffic	OFF
Filter Socket Traffic	OFF

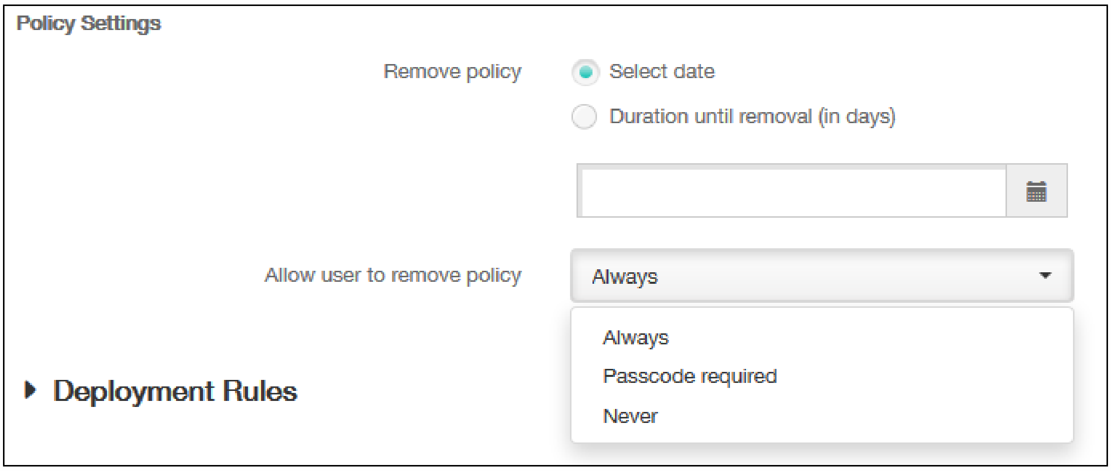
Custom Data

Key	Value	Add

Policy Settings

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

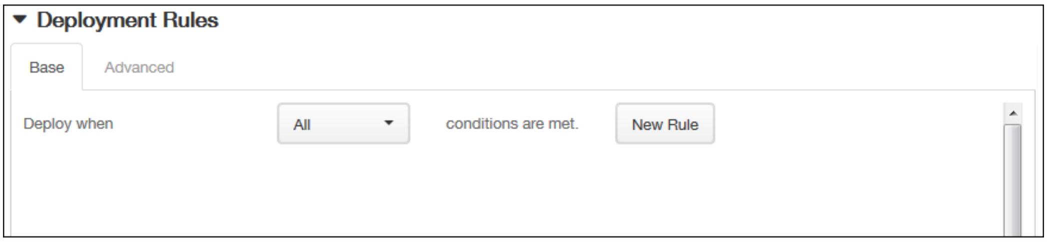
Allow user to remove policy: Always



Policy Settings

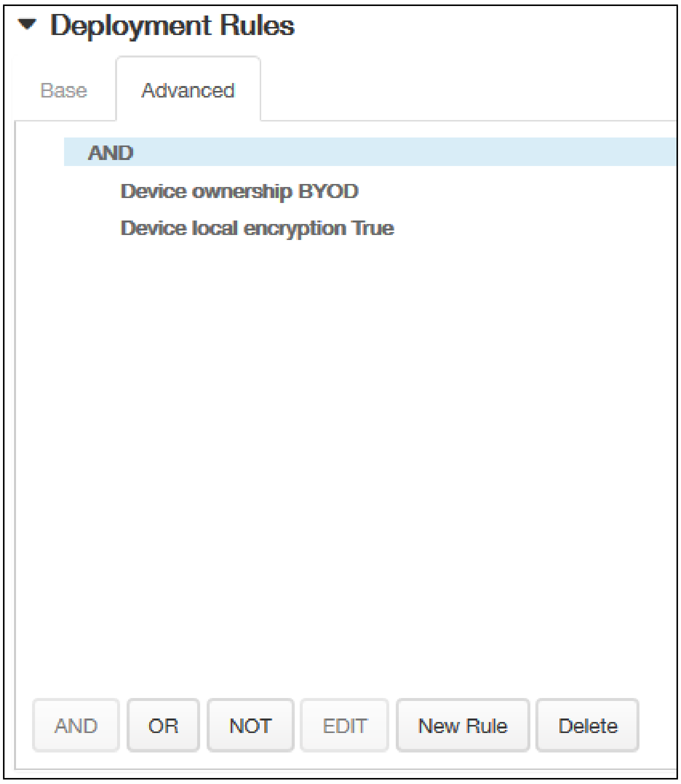
Remove policy ● Select date ○ Duration until removal (in days)

Allow user to remove policy: Always



▾ Deployment Rules

Deploy when All conditions are met.

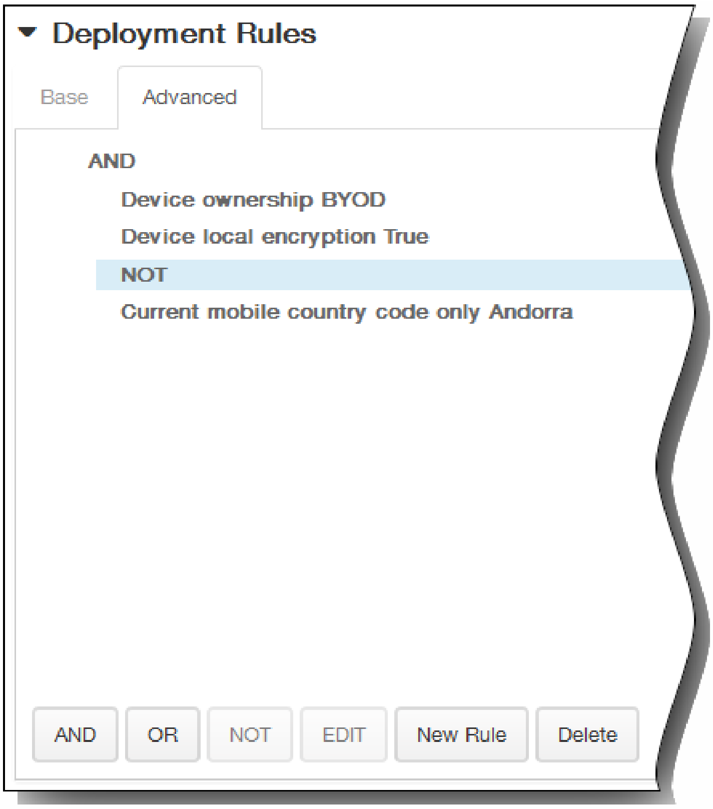


Deployment Rules

AND

Device ownership BYOD

Device local encryption True



Deployment Rules

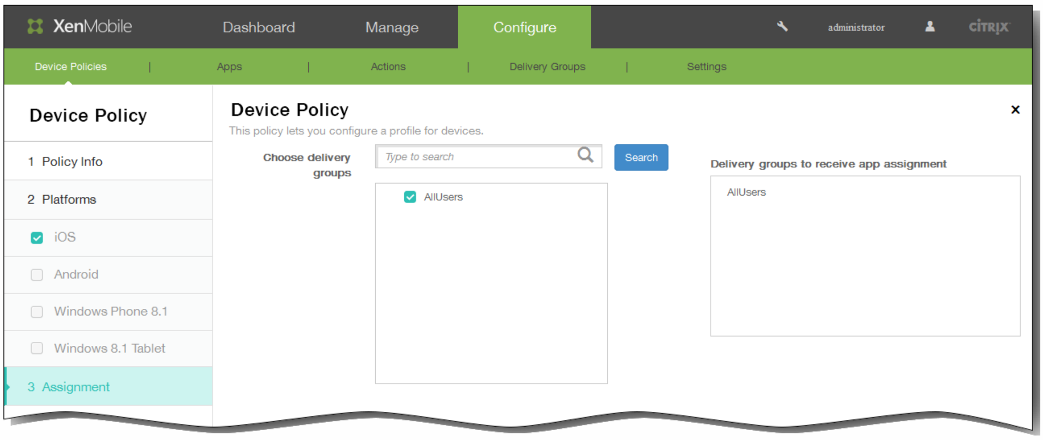
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

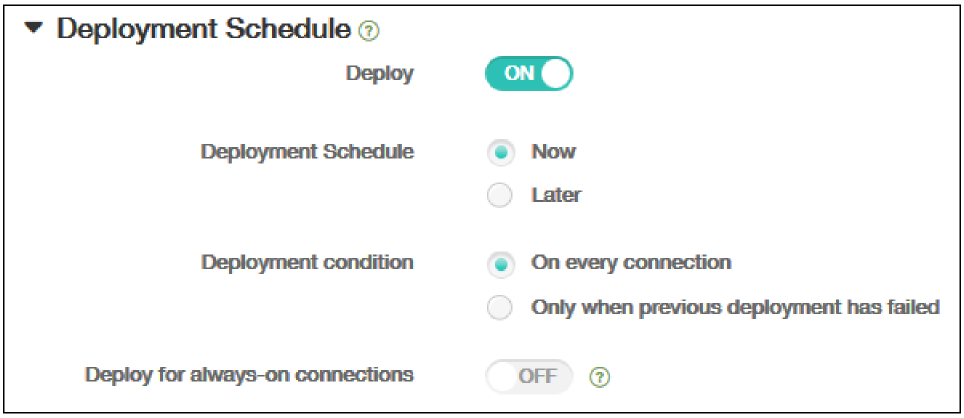
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



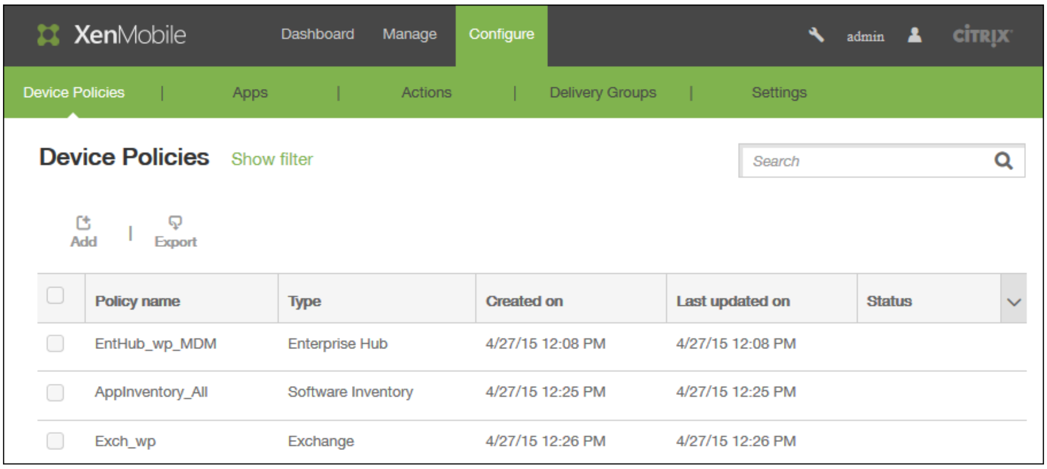
▼ Deployment Schedule ?

Deploy: ON

Deployment Schedule: ● Now ○ Later

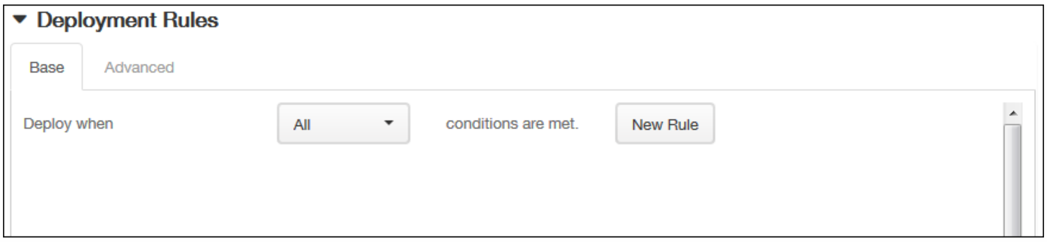
Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF ?



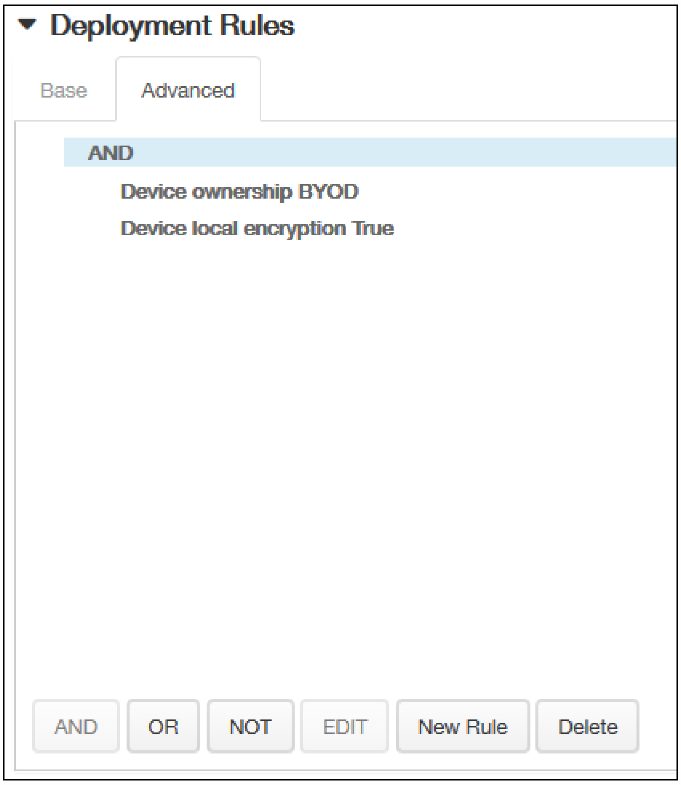
Device Policies

□	Policy name	Type	Created on	Last updated on	Status
□	EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
□	AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
□	Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	



Deployment Rules

Deploy when All conditions are met.

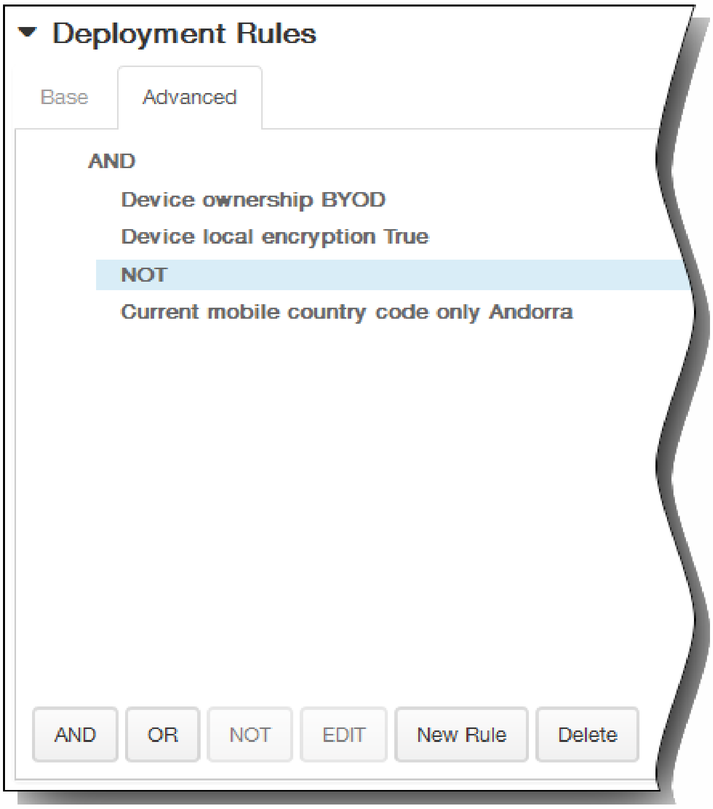


Deployment Rules

AND

Device ownership BYOD

Device local encryption True



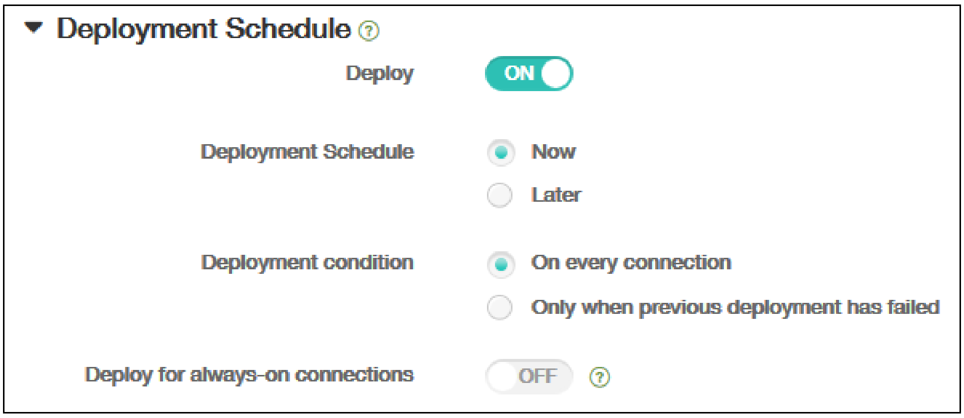
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



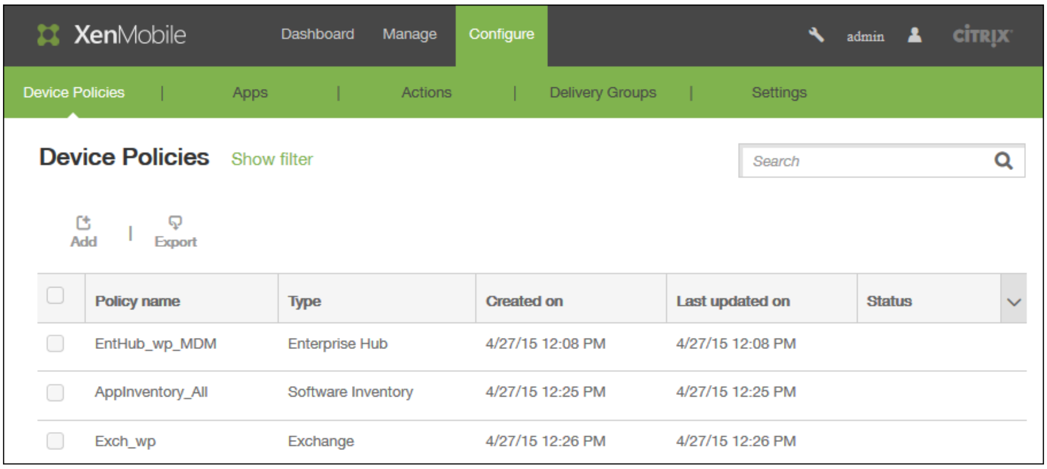
Deployment Schedule

Deploy: ON

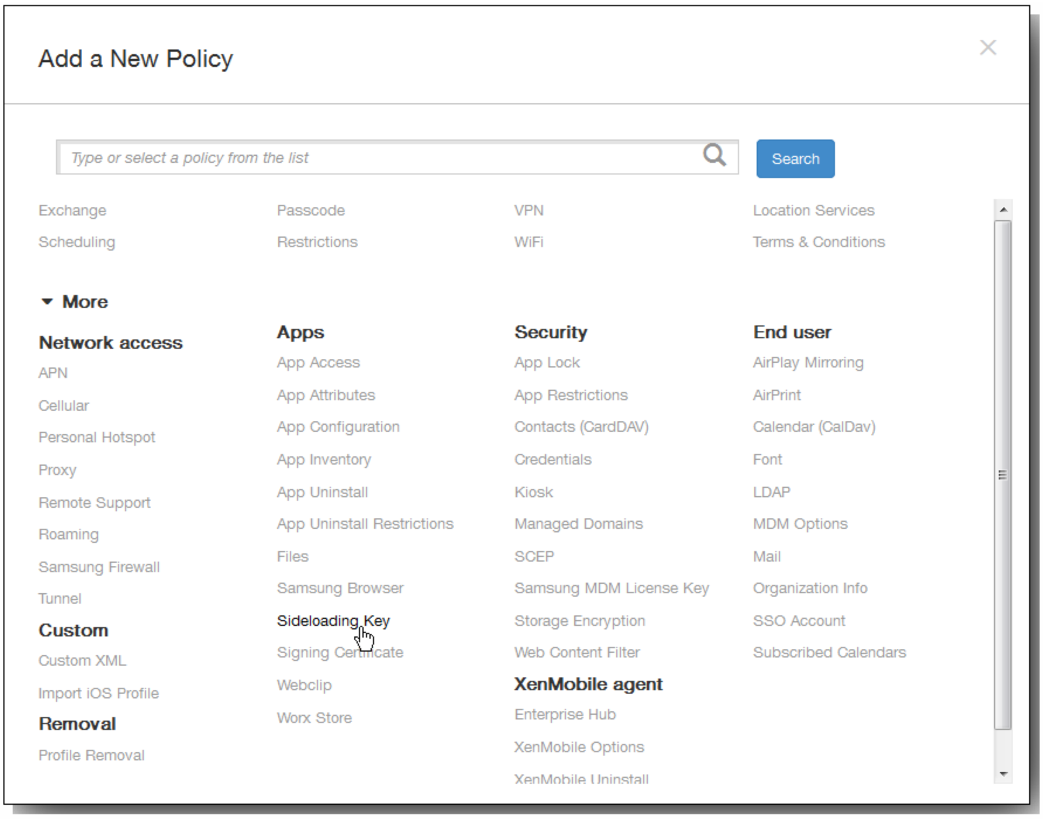
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF



	Policy name	Type	Created on	Last updated on	Status
□	EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
□	AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
□	Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	



Add a New Policy

Type or select a policy from the list

Search

Exchange
Scheduling

Passcode
Restrictions

VPN
WiFi

Location Services
Terms & Conditions

More

Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel

Custom
Custom XML
Import iOS Profile

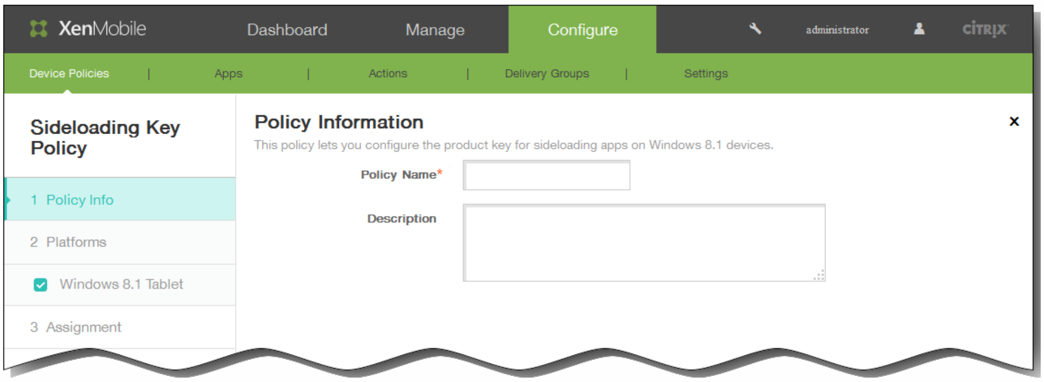
Removal
Profile Removal

Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store

Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter

XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall

End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars



Sideloading Key Policy

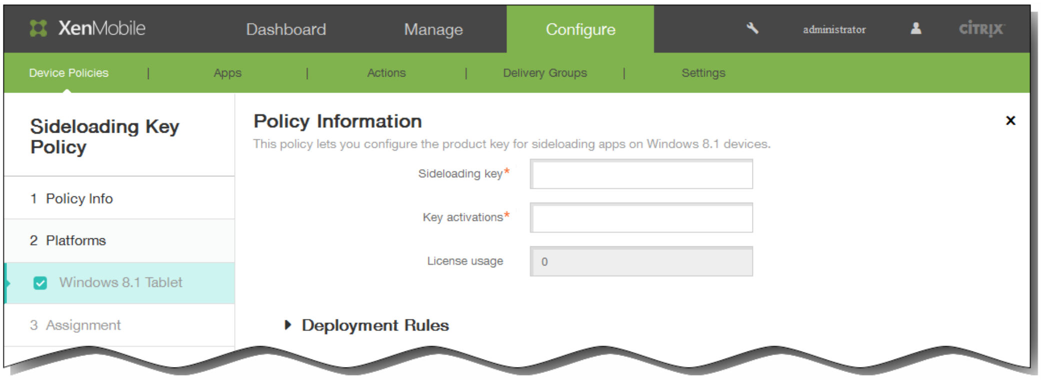
1 Policy Info
2 Platforms
☑ Windows 8.1 Tablet
3 Assignment

Policy Information

This policy lets you configure the product key for sideloading apps on Windows 8.1 devices.

Policy Name*

Description



Sideloading Key Policy

1 Policy Info

2 Platforms

☑ Windows 8.1 Tablet

3 Assignment

Policy Information

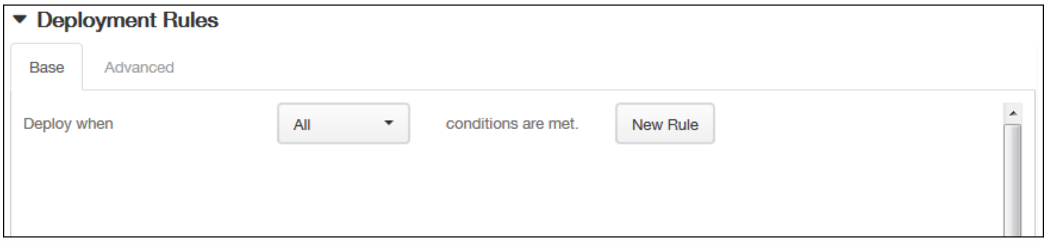
This policy lets you configure the product key for sideloading apps on Windows 8.1 devices.

Sideloading key*

Key activations*

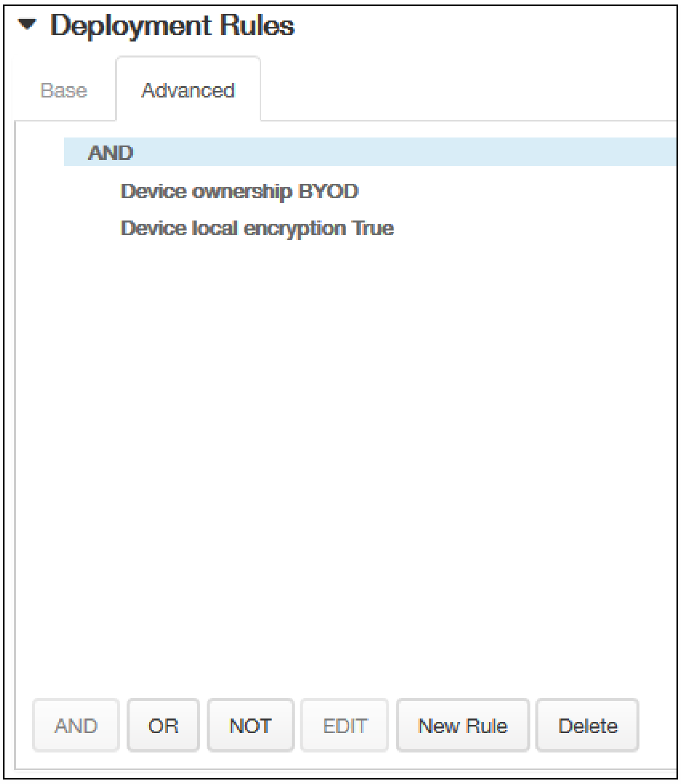
License usage: 0

Deployment Rules



Deployment Rules

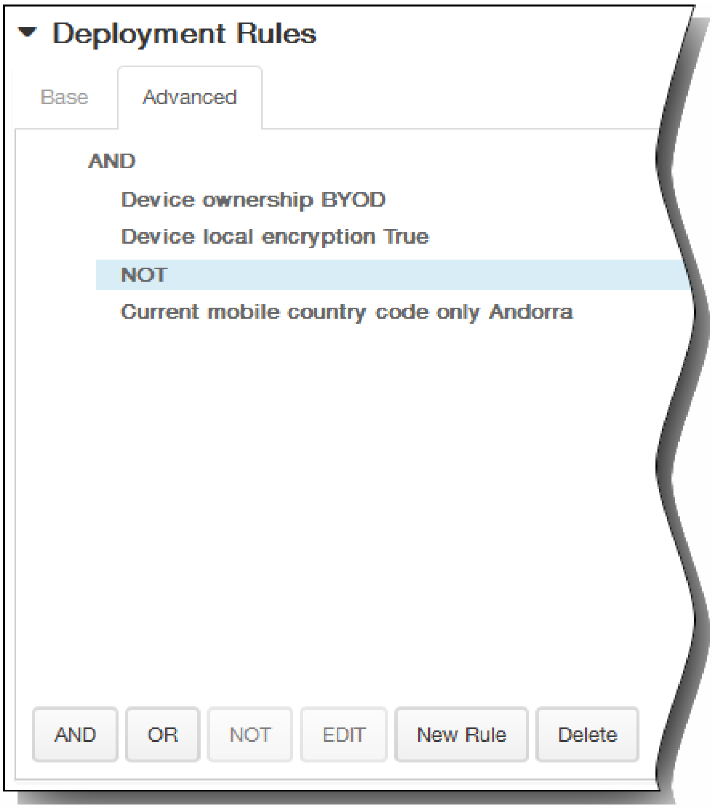
Deploy when All conditions are met.



AND

Device ownership BYOD

Device local encryption True



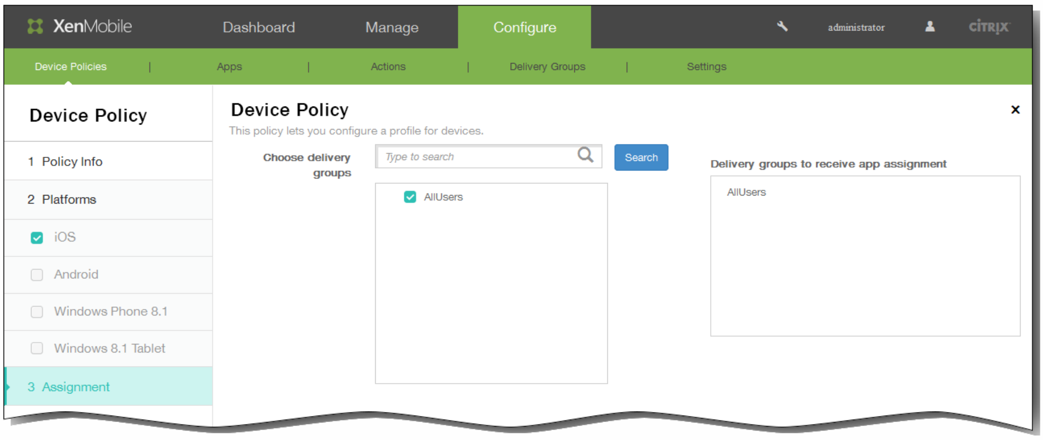
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra

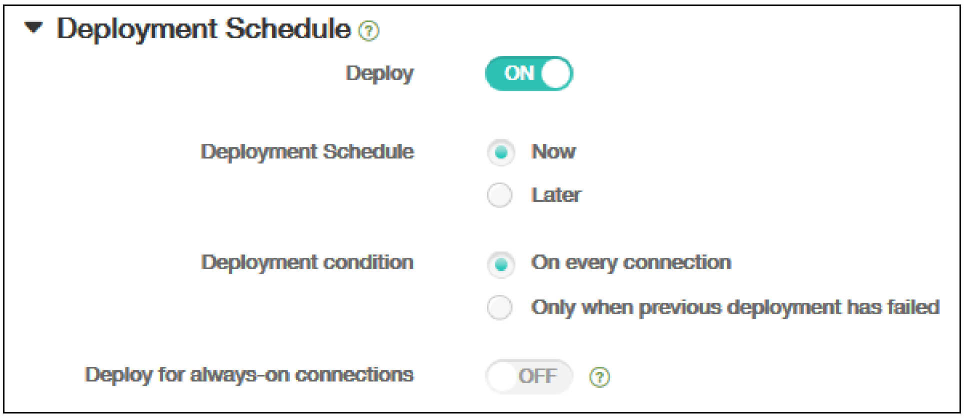


This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment: AllUsers



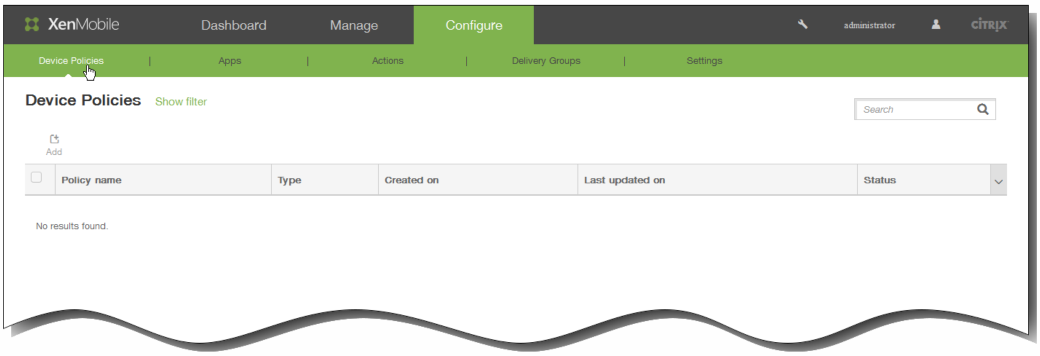
Deployment Schedule

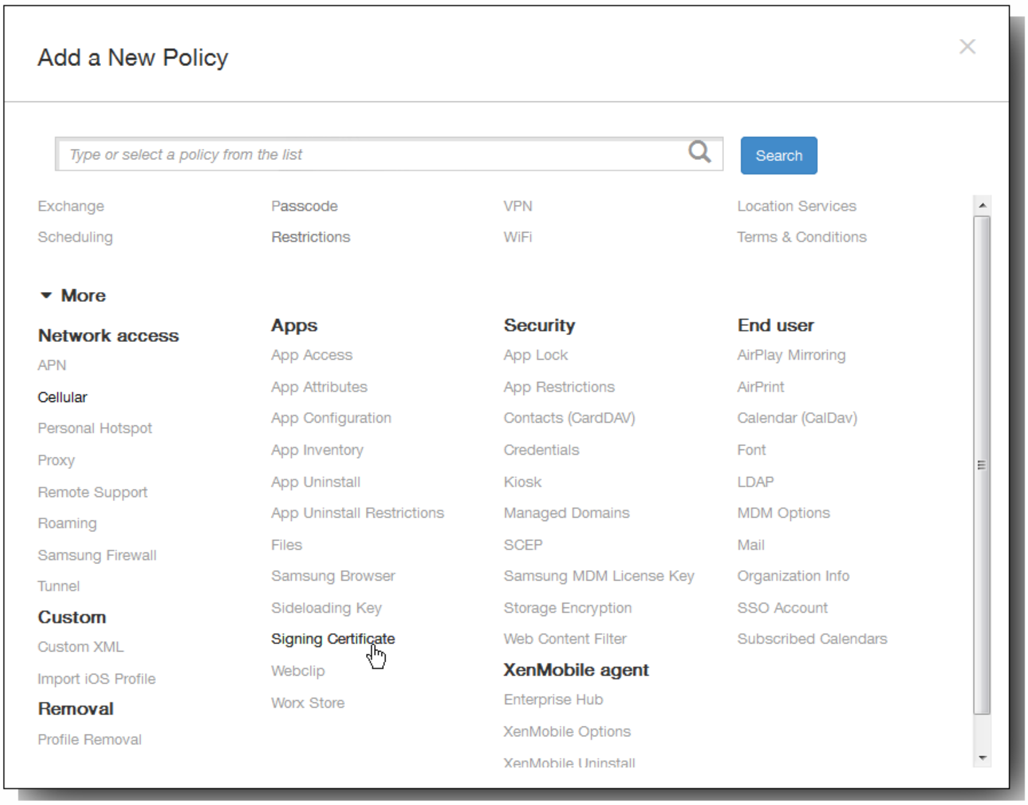
Deploy: ON

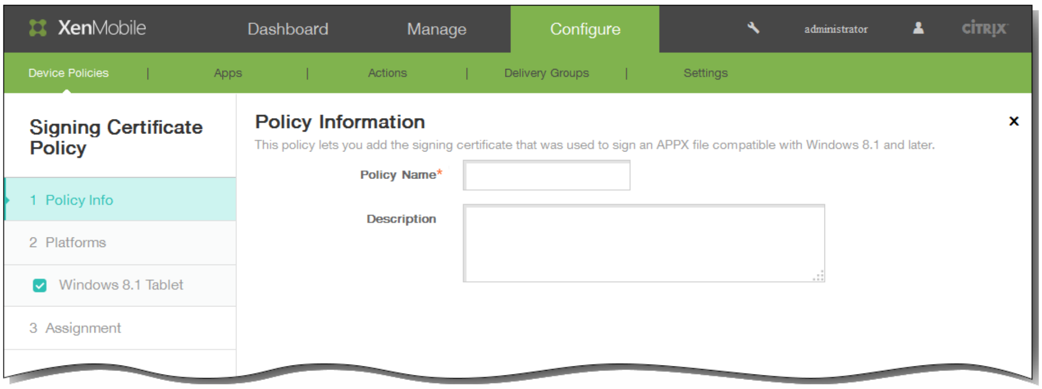
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies
Apps
Actions
Delivery Groups
Settings
Device Policies
Show filter
Search
Add
Policy name
Type
Created on
Last updated on
Status
No results found.


Add a New Policy
Type or select a policy from the list
Search
Exchange
Scheduling
Passcode
Restrictions
VPN
WiFi
Location Services
Terms & Conditions
More
Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel
Custom
Custom XML
Import iOS Profile
Removal
Profile Removal
Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store
Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter
XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall
End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars



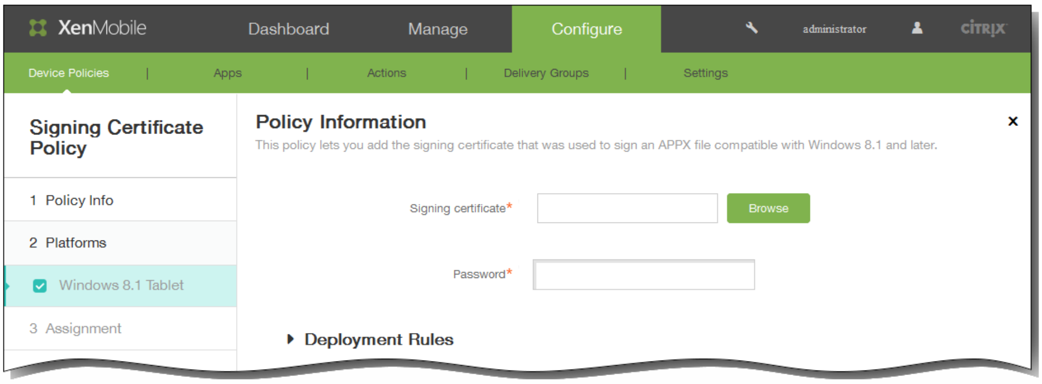
Signing Certificate Policy

Policy Information

This policy lets you add the signing certificate that was used to sign an APPX file compatible with Windows 8.1 and later.

Policy Name*

Description



Signing Certificate Policy

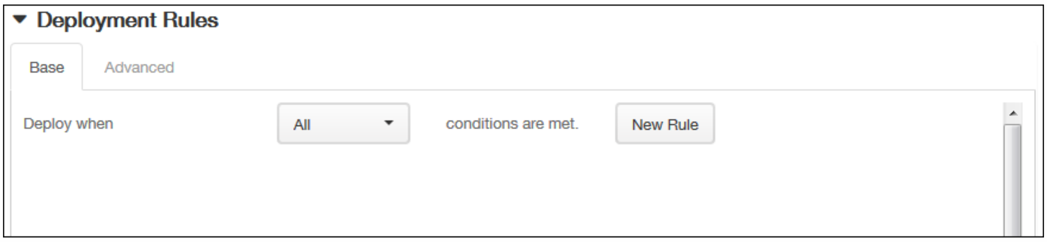
Policy Information

This policy lets you add the signing certificate that was used to sign an APPX file compatible with Windows 8.1 and later.

Signing certificate*

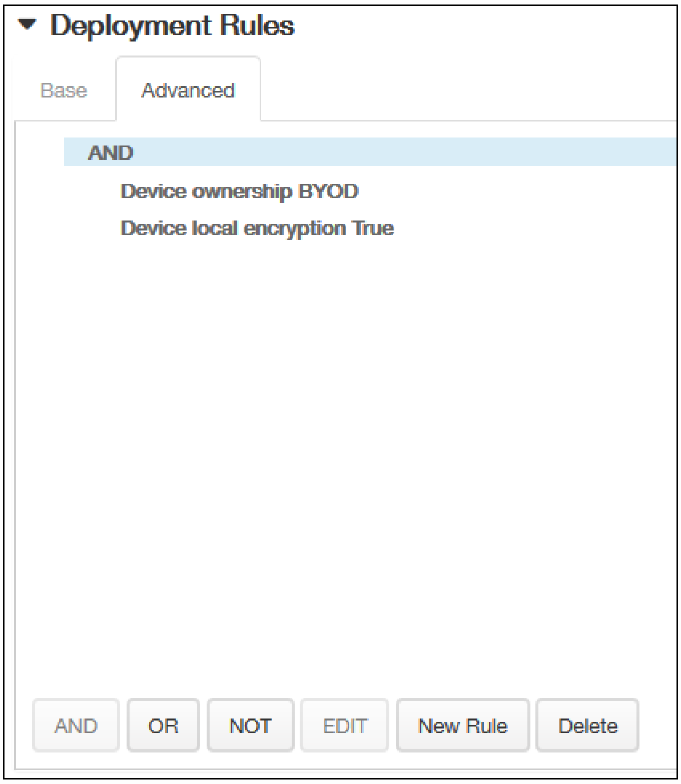
Password*

▸ Deployment Rules



▾ Deployment Rules

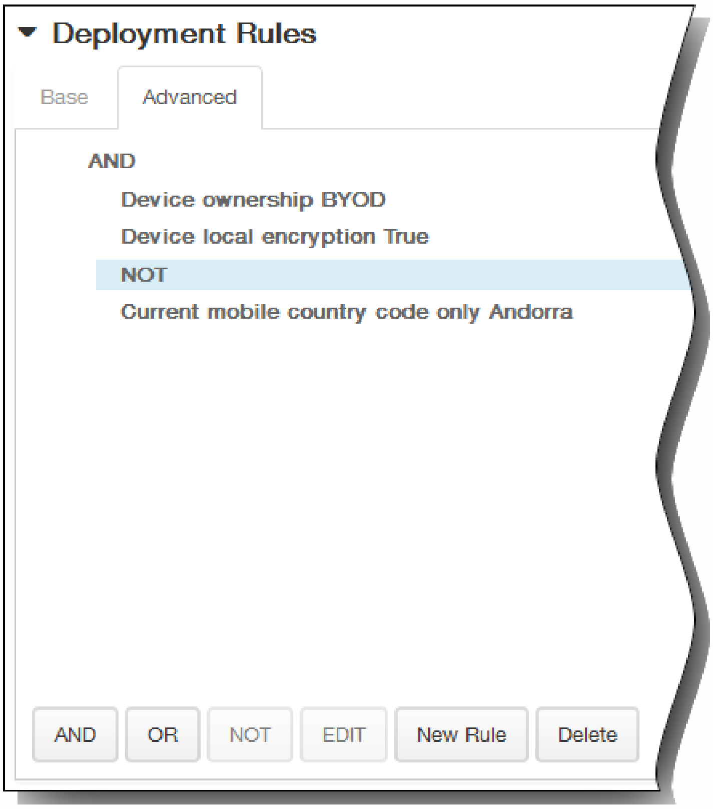
Deploy when All ▾ conditions are met.



AND

Device ownership BYOD

Device local encryption True



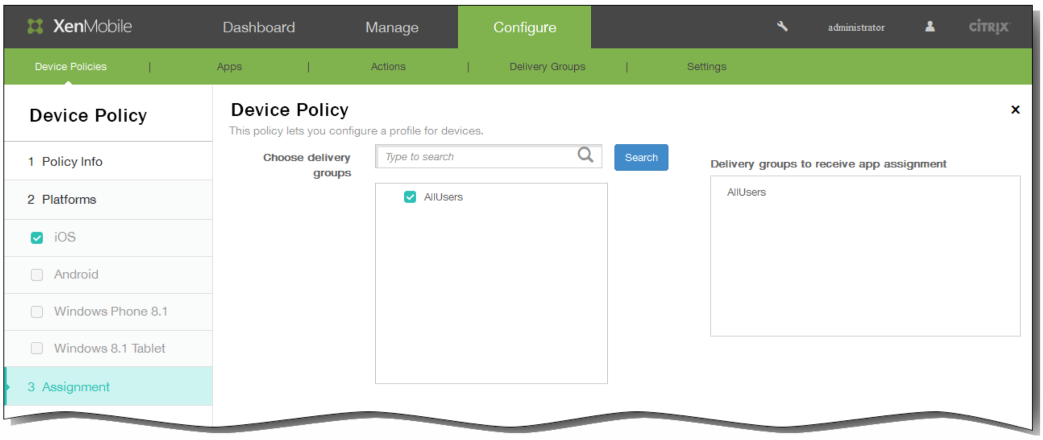
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



☑ iOS
☐ Android
☐ Windows Phone 8.1
☐ Windows 8.1 Tablet

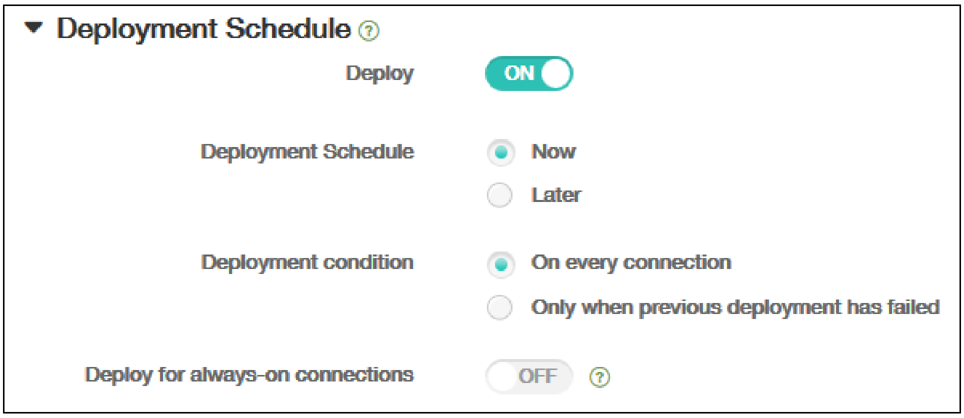
Device Policy

This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment: AllUsers



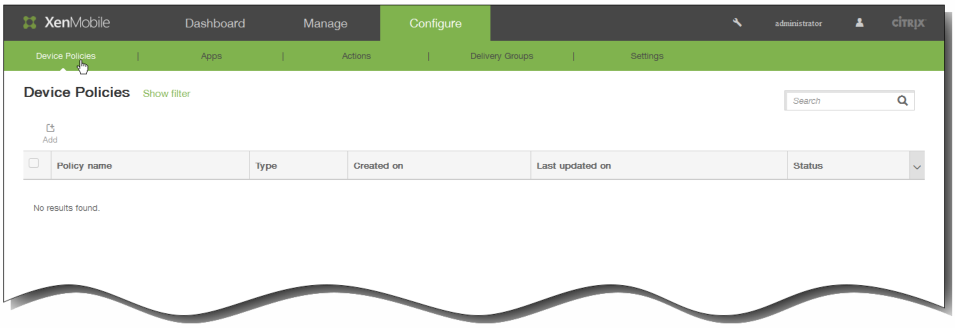
Deployment Schedule

Deploy: ON

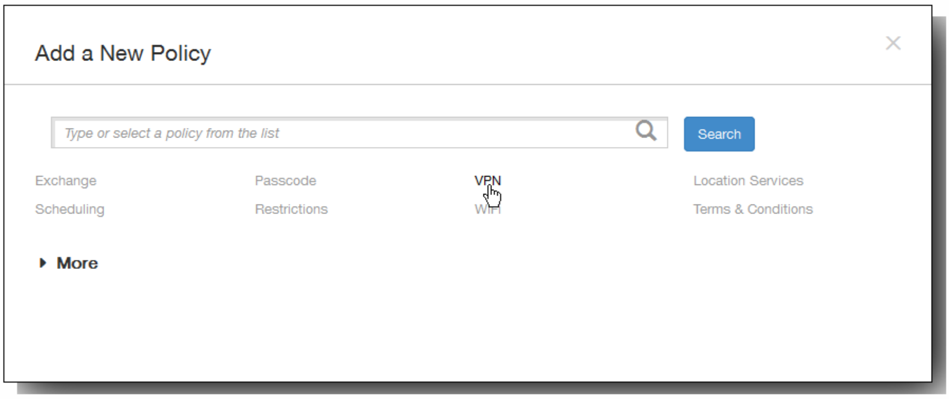
Deployment Schedule: ● Now ○ Later

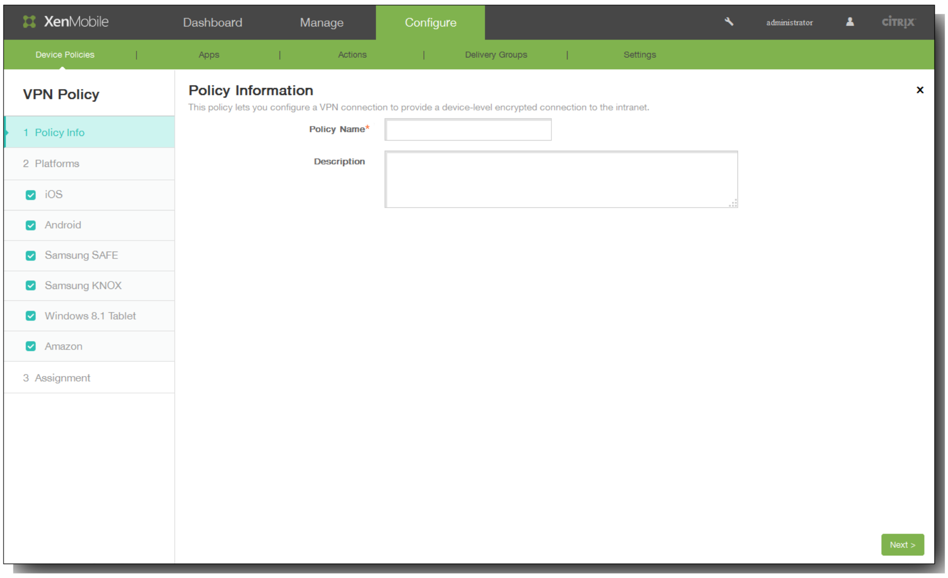
Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF



No results found.



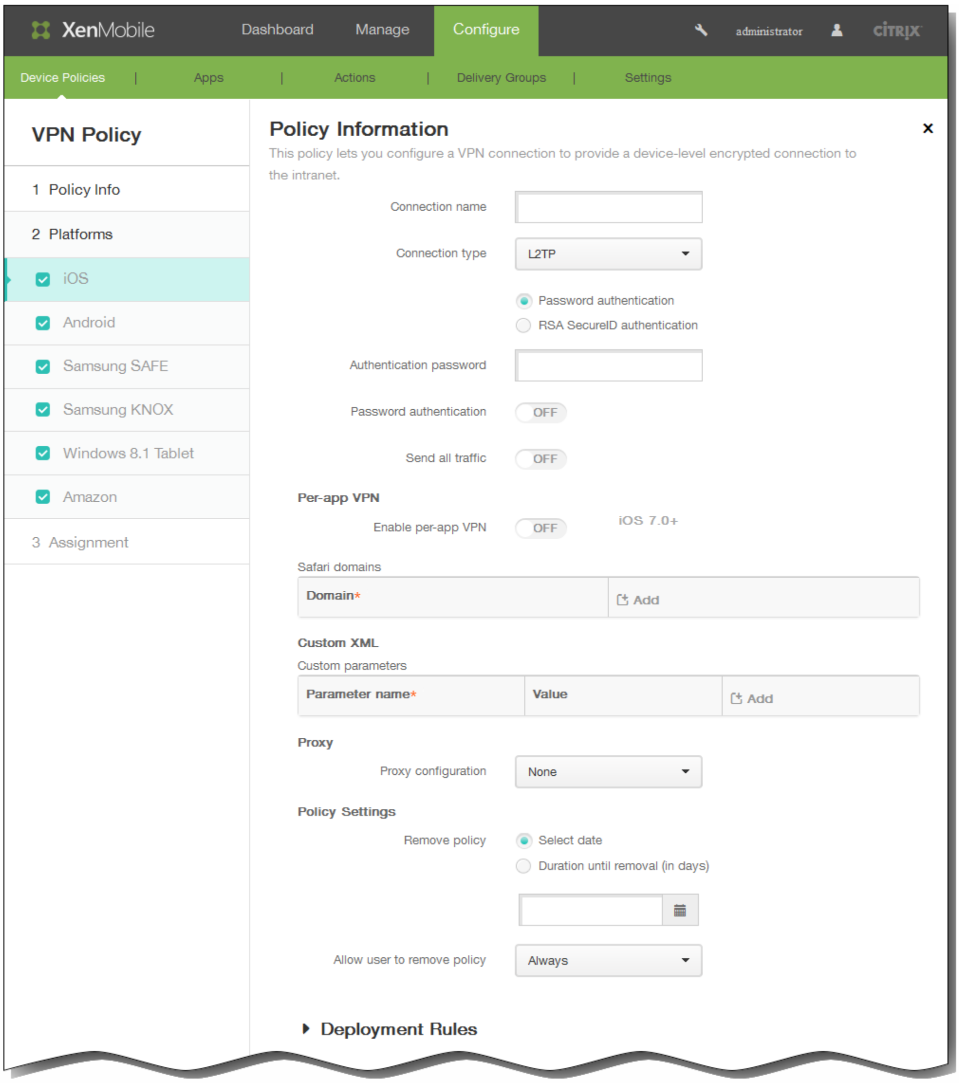


Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet.

Policy Name*

Description


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings

VPN Policy

1 Policy Info

2 Platforms

- ☑ iOS
- ☑ Android
- ☑ Samsung SAFE
- ☑ Samsung KNOX
- ☑ Windows 8.1 Tablet
- ☑ Amazon

3 Assignment

Policy Information ×

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet.

Connection name

Connection type: L2TP

● Password authentication
○ RSA SecureID authentication

Authentication password

Password authentication: OFF

Send all traffic: OFF

Per-app VPN

Enable per-app VPN: OFF iOS 7.0+

Safari domains

Domain*	Add

Custom XML

Custom parameters

Parameter name*	Value	Add

Proxy

Proxy configuration: None

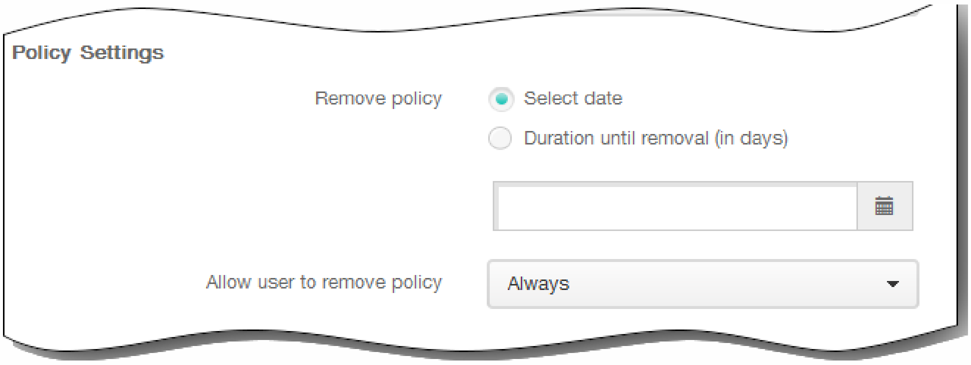
Policy Settings

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

Allow user to remove policy: Always

▸ Deployment Rules

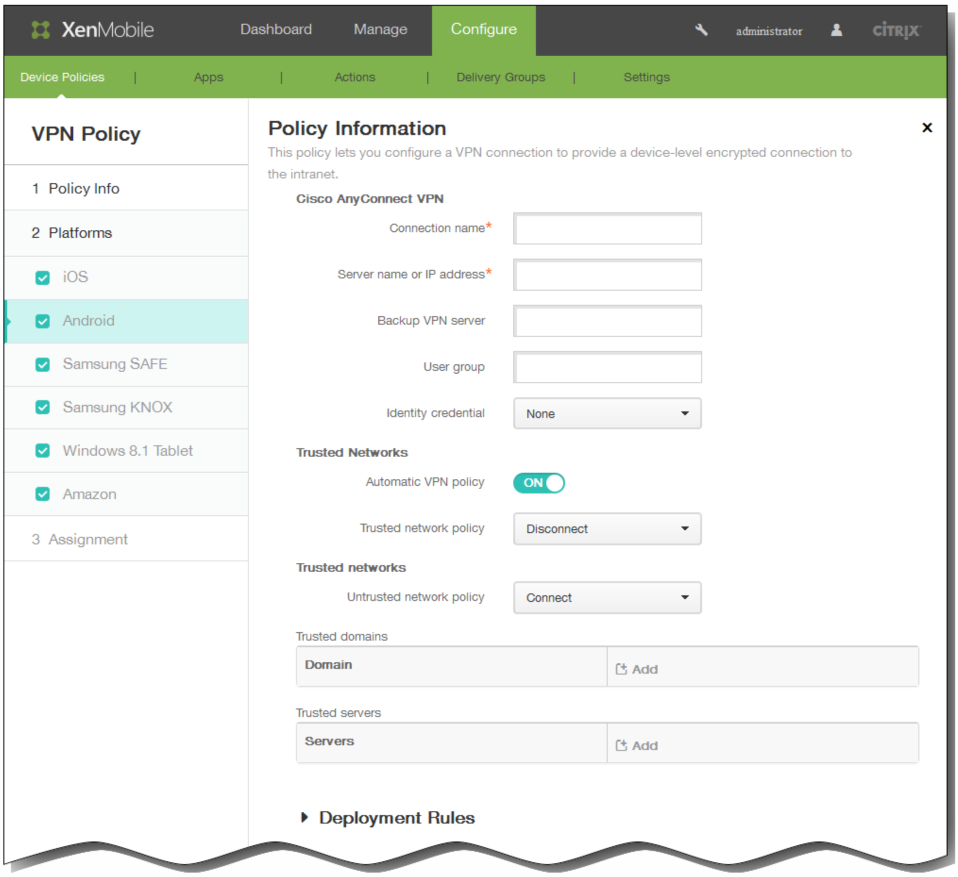
-
-
-
-
-
-
-
-
-
-



Policy Settings

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

Allow user to remove policy: Always



VPN Policy

1 Policy Info

2 Platforms

☑ iOS

☑ Android

☑ Samsung SAFE

☑ Samsung KNOX

☑ Windows 8.1 Tablet

☑ Amazon

3 Assignment

Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet.

Cisco AnyConnect VPN

Connection name*	
Server name or IP address*	
Backup VPN server	
User group	
Identity credential	None

Trusted Networks

Automatic VPN policy	ON
Trusted network policy	Disconnect

Trusted networks

Untrusted network policy	Connect

Trusted domains

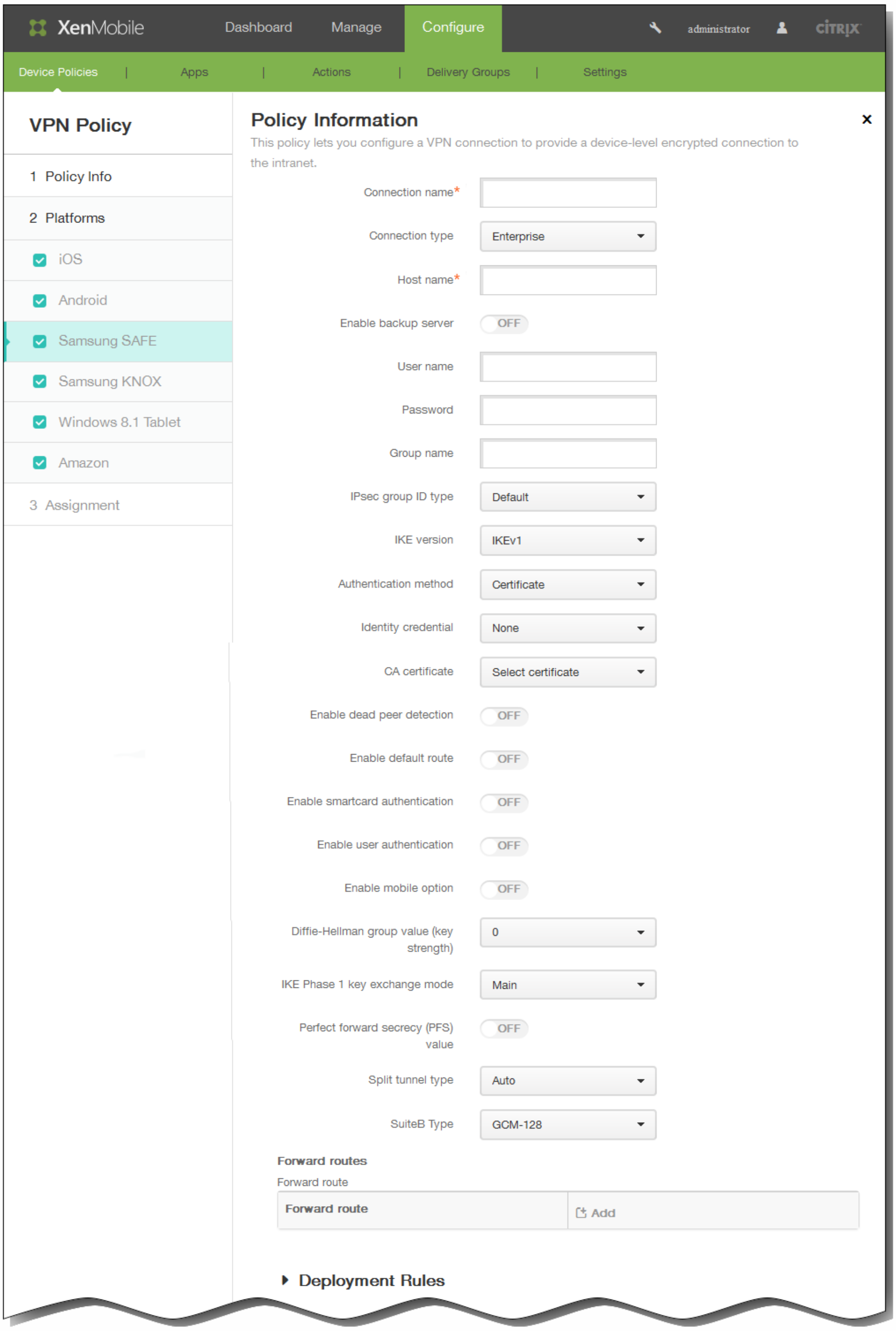
Domain	Add

Trusted servers

Servers	Add

Deployment Rules

-
-



XenMobile
Dashboard
Manage
Configure
administrator
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings

VPN Policy

1 Policy Info

2 Platforms

- ☑ iOS
- ☑ Android
- ☑ Samsung SAFE
- ☑ Samsung KNOX
- ☑ Windows 8.1 Tablet
- ☑ Amazon

3 Assignment

Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet.

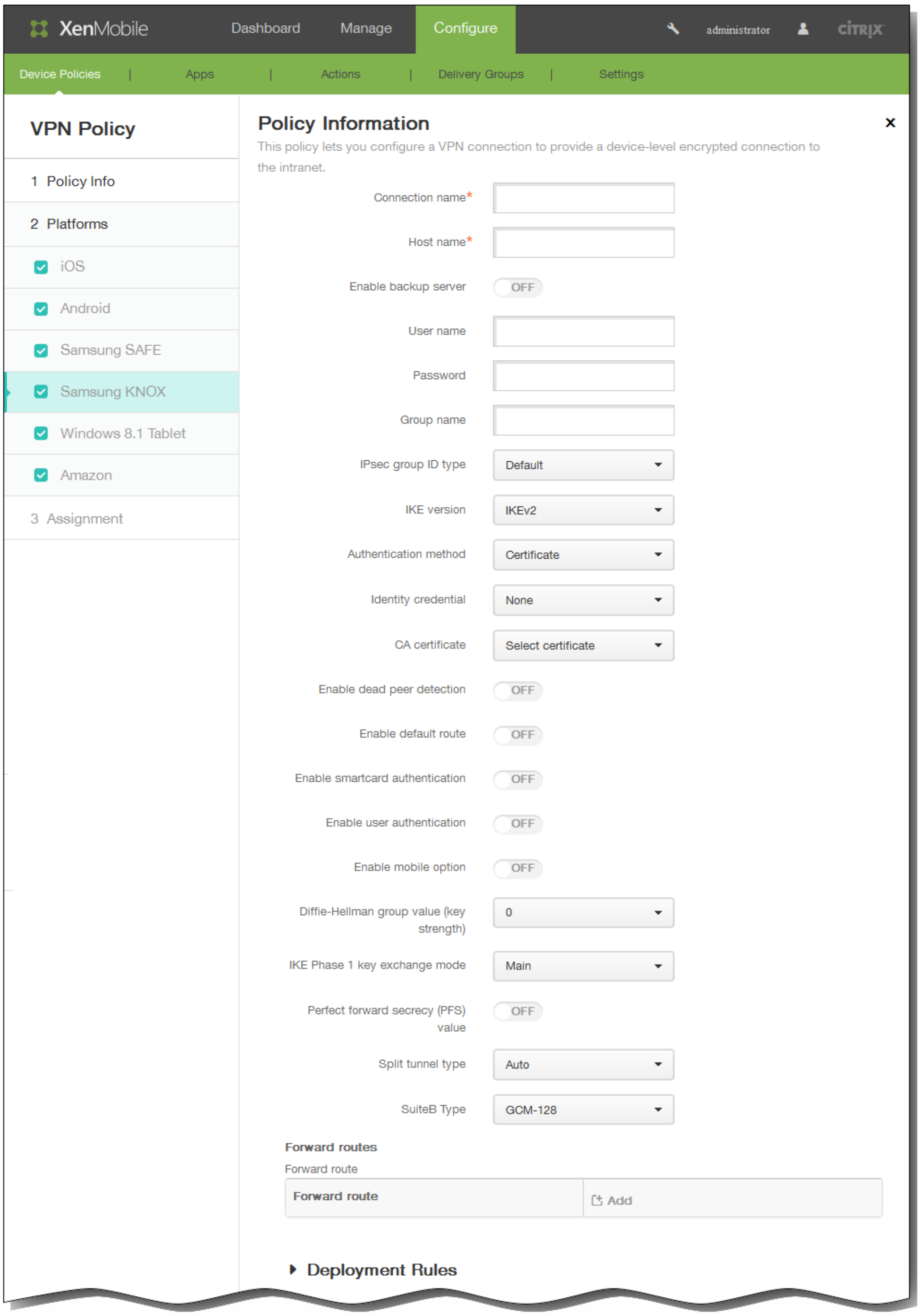
Connection name*	
Connection type	Enterprise
Host name*	
Enable backup server	OFF
User name	
Password	
Group name	
IPsec group ID type	Default
IKE version	IKEv1
Authentication method	Certificate
Identity credential	None
CA certificate	Select certificate
Enable dead peer detection	OFF
Enable default route	OFF
Enable smartcard authentication	OFF
Enable user authentication	OFF
Enable mobile option	OFF
Diffie-Hellman group value (key strength)	0
IKE Phase 1 key exchange mode	Main
Perfect forward secrecy (PFS) value	OFF
Split tunnel type	Auto
SuiteB Type	GCM-128

Forward routes

Forward route

Forward route	Add

Deployment Rules



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	Default
IKE version	IKEv2
Authentication method	Certificate
Identity credential	None
CA certificate	Select 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)	0
IKE Phase 1 key exchange mode	Main
Perfect forward secrecy (PFS) value	OFF
Split tunnel type	Auto
SuiteB Type	GCM-128

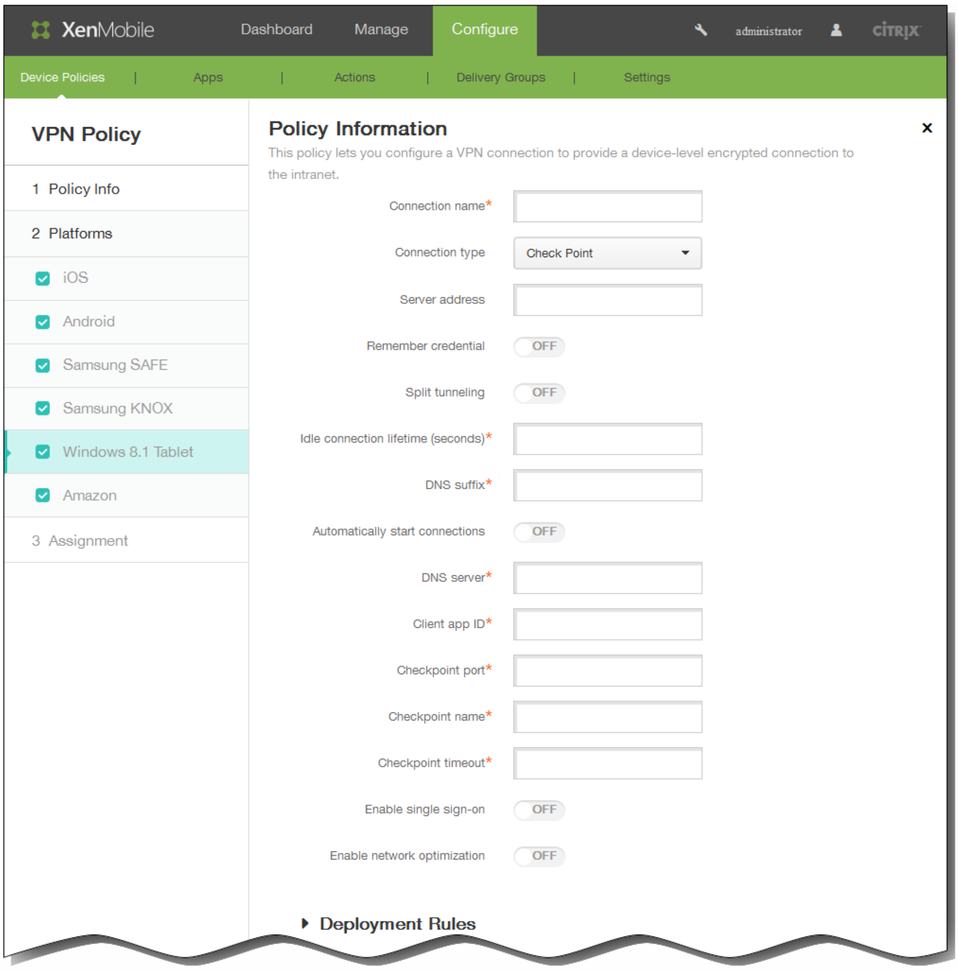
Forward routes

Forward route

Forward route	Add

Deployment Rules

-
-



XenMobile Dashboard Manage Configure administrator

Device Policies | Apps | Actions | Delivery Groups | Settings

VPN Policy

1 Policy Info

2 Platforms

☑ iOS

☑ Android

☑ Samsung SAFE

☑ Samsung KNOX

☑ Windows 8.1 Tablet

☑ Amazon

3 Assignment

Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet.

Connection name*

Connection type: Check Point

Server address

Remember credential: OFF

Split tunneling: OFF

Idle connection lifetime (seconds)*

DNS suffix*

Automatically start connections: OFF

DNS server*

Client app ID*

Checkpoint port*

Checkpoint name*

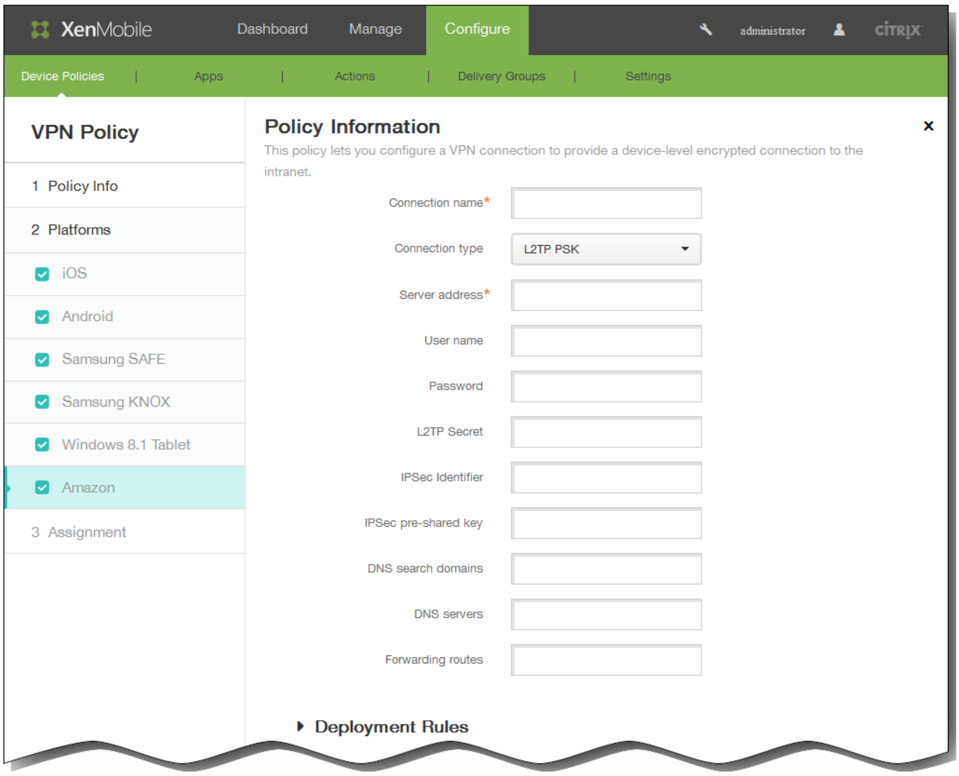
Checkpoint timeout*

Enable single sign-on: OFF

Enable network optimization: OFF

Deployment Rules

-
-
-
-
-



VPN Policy

1 Policy Info

2 Platforms

☑ iOS

☑ Android

☑ Samsung SAFE

☑ Samsung KNOX

☑ Windows 8.1 Tablet

☑ Amazon

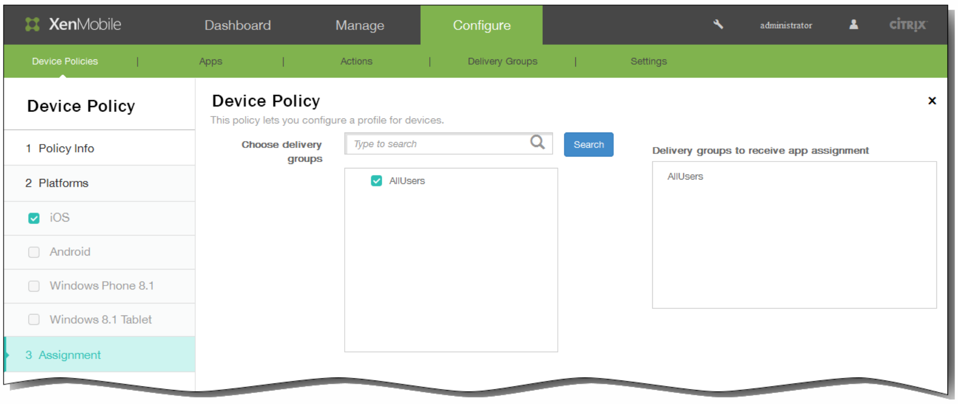
3 Assignment

Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet.

Connection name*	
Connection type	L2TP PSK
Server address*	
User name	
Password	
L2TP Secret	
IPSec Identifier	
IPSec pre-shared key	
DNS search domains	
DNS servers	
Forwarding routes	

▸ Deployment Rules



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

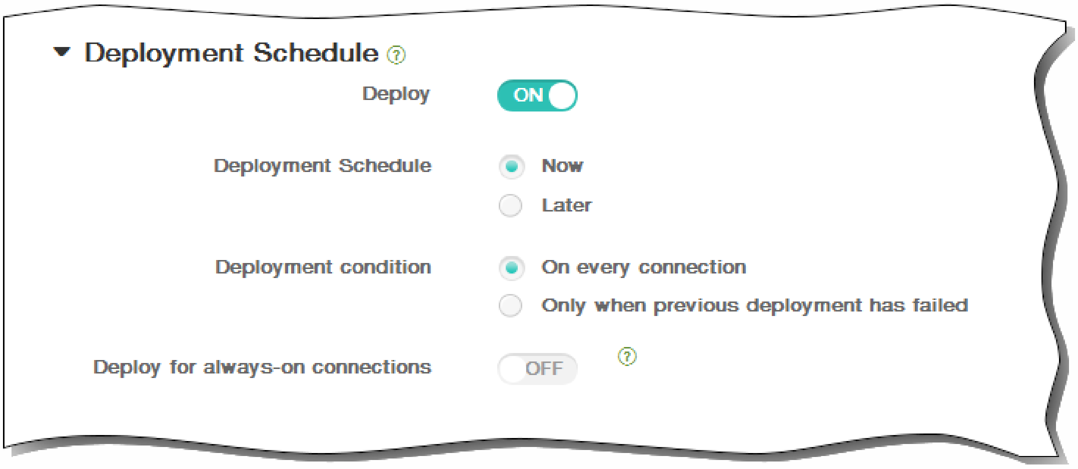
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search [Search]

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



Deployment Schedule

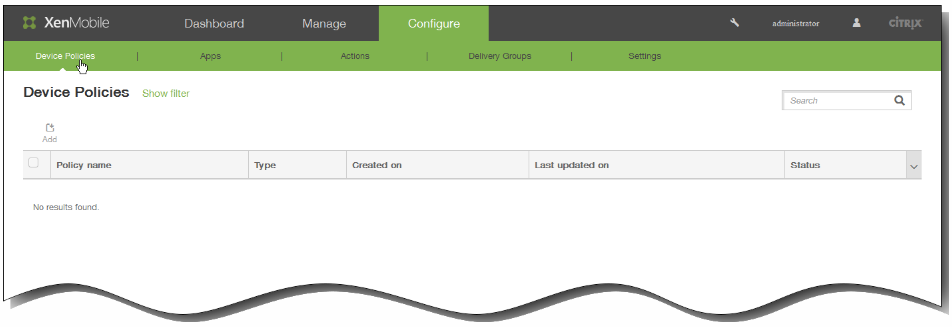
Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF

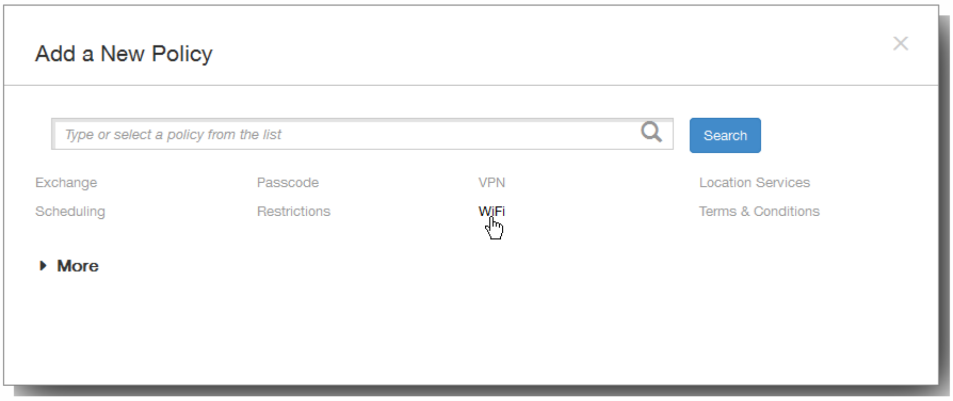
-
-
-
-
-
-



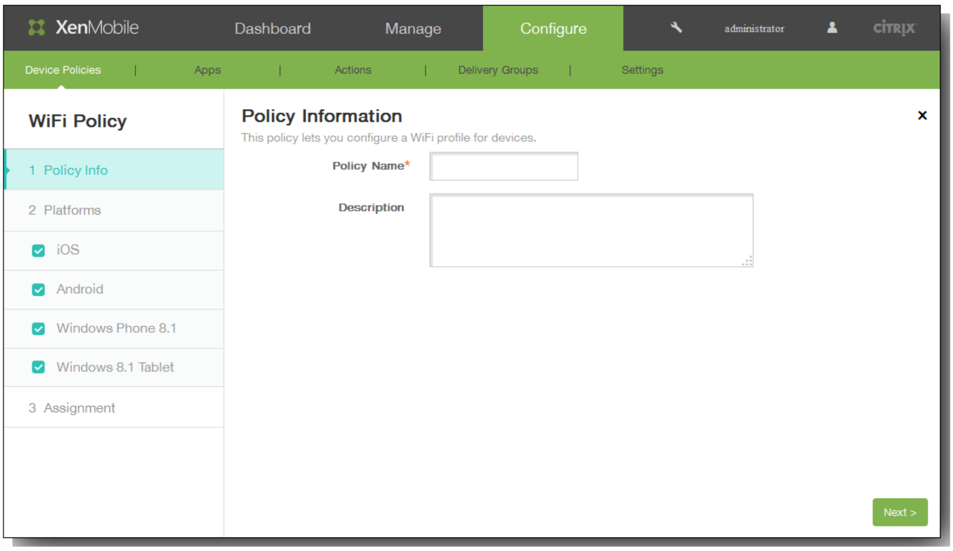
Device Policies Show filter

□	Policy name	Type	Created on	Last updated on	Status

No results found.



Add a New Policy

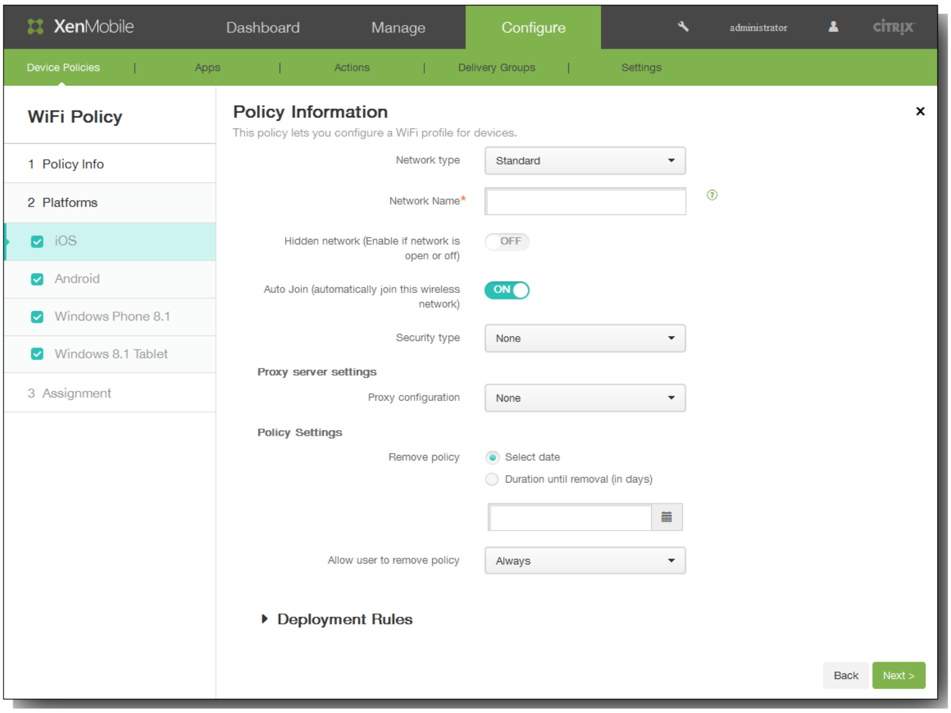


Policy Information

This policy lets you configure a WiFi profile for devices.

Policy Name*

Description



Policy Information

This policy lets you configure a WiFi profile for devices.

Network type: Standard

Network Name*

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

Auto Join (automatically join this wireless network): ON

Security type: None

Proxy server settings

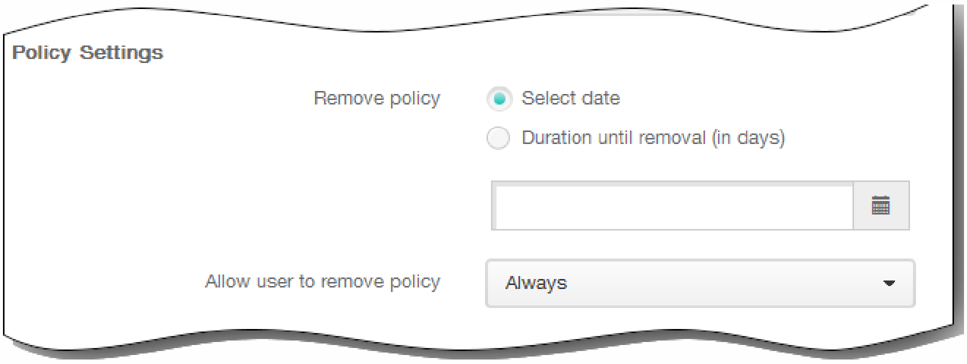
Proxy configuration: None

Policy Settings

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

Allow user to remove policy: Always

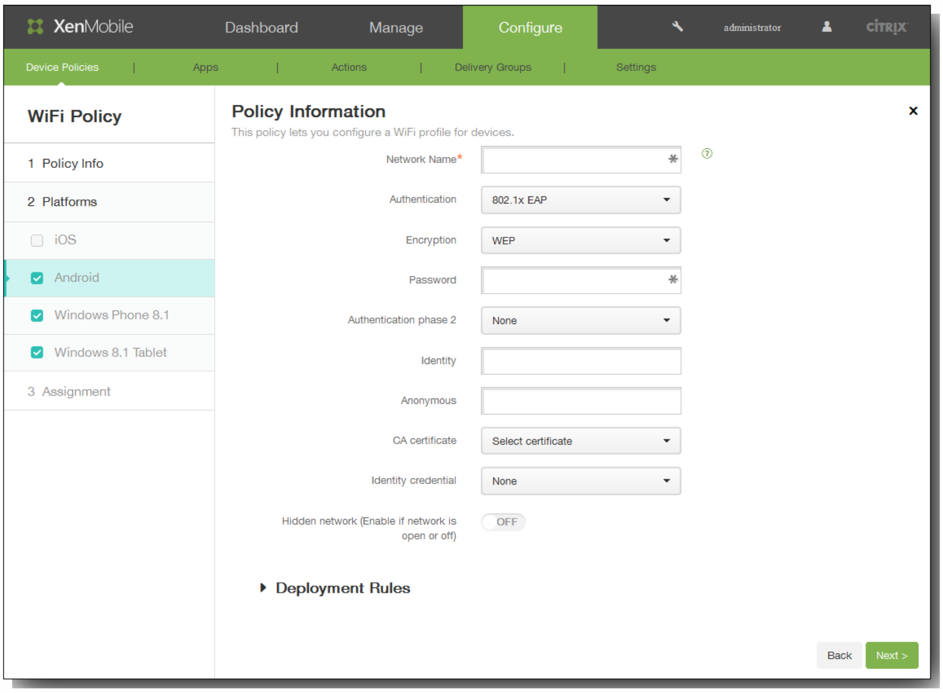
Deployment Rules



Policy Settings

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

Allow user to remove policy: Always



Policy Information

This policy lets you configure a WiFi profile for devices.

Network Name*

Authentication: 802.1x EAP

Encryption: WEP

Password

Authentication phase 2: None

Identity

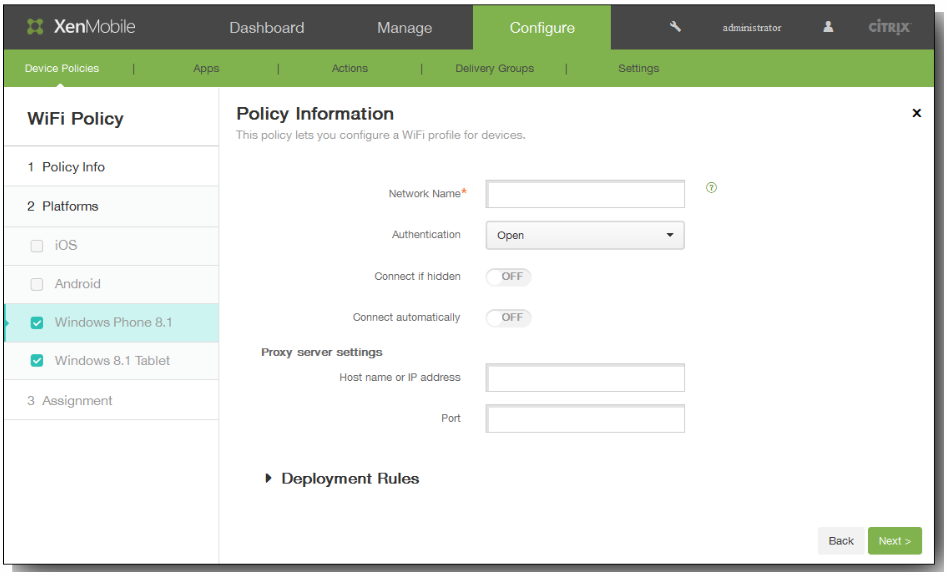
Anonymous

CA certificate: Select certificate

Identity credential: None

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

-
-
-
-
-
-
-



WiFi Policy

1 Policy Info

2 Platforms

□ iOS

□ Android

☑ Windows Phone 8.1

☑ Windows 8.1 Tablet

3 Assignment

Policy Information

This policy lets you configure a WiFi profile for devices.

Network Name*

Authentication: Open

Connect if hidden: OFF

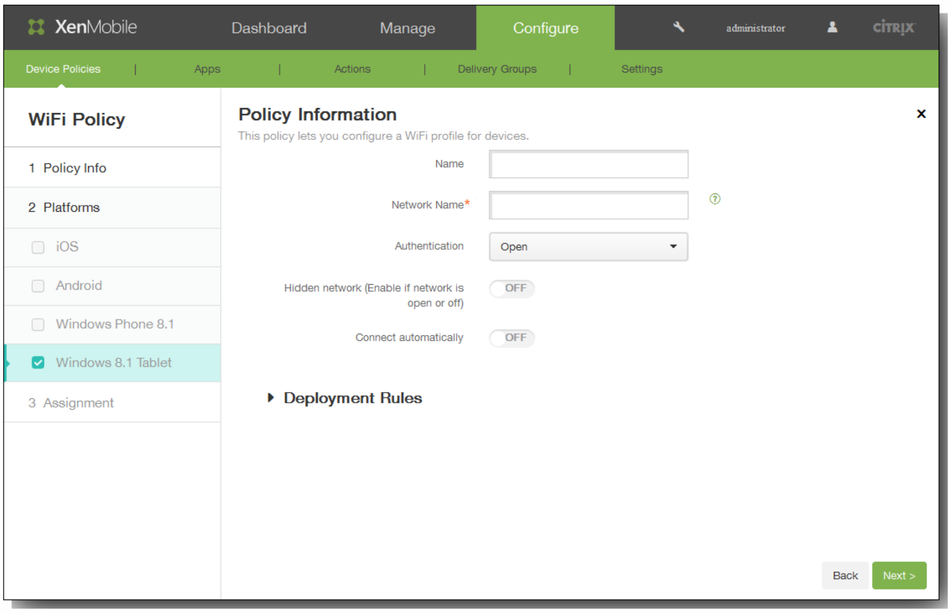
Connect automatically: OFF

Proxy server settings

Host name or IP address

Port

Deployment Rules



Policy Information

This policy lets you configure a WiFi profile for devices.

Name

Network Name*

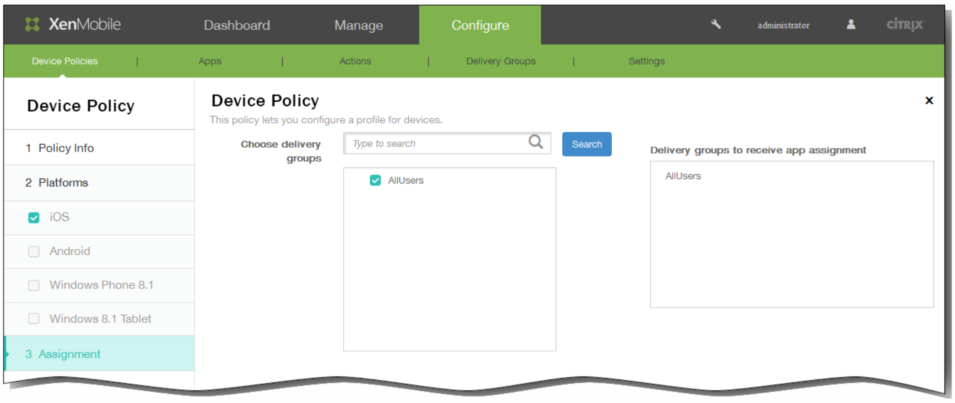
Authentication: Open

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

Connect automatically: OFF

Deployment Rules

-
-
-
-
-



Device Policy

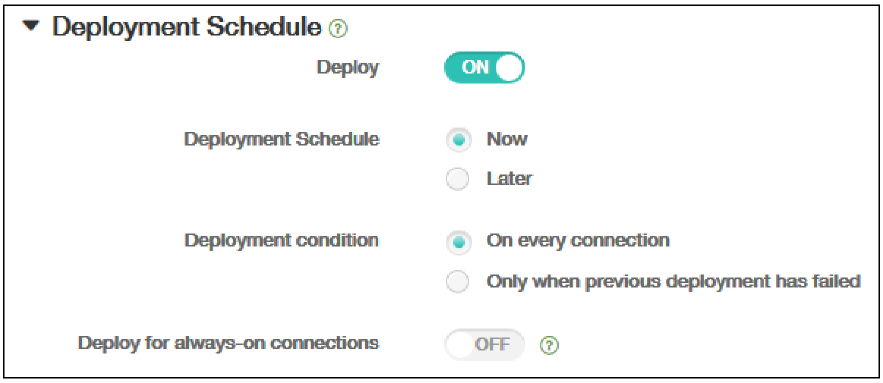
This policy lets you configure a profile for devices.

Choose delivery groups

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



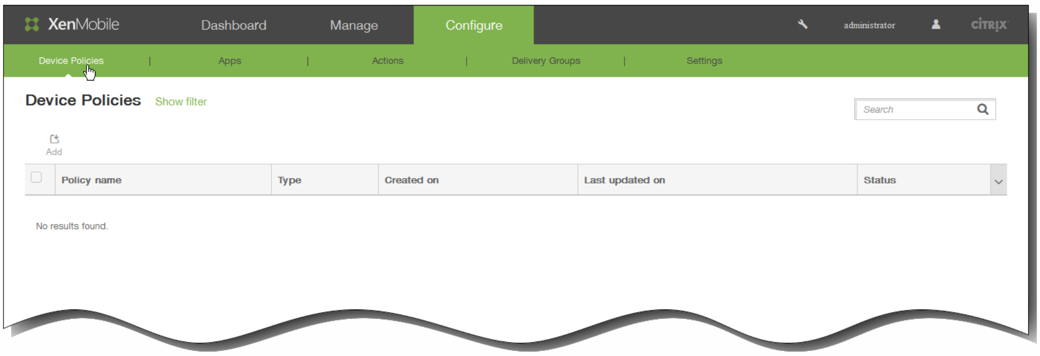
Deployment Schedule

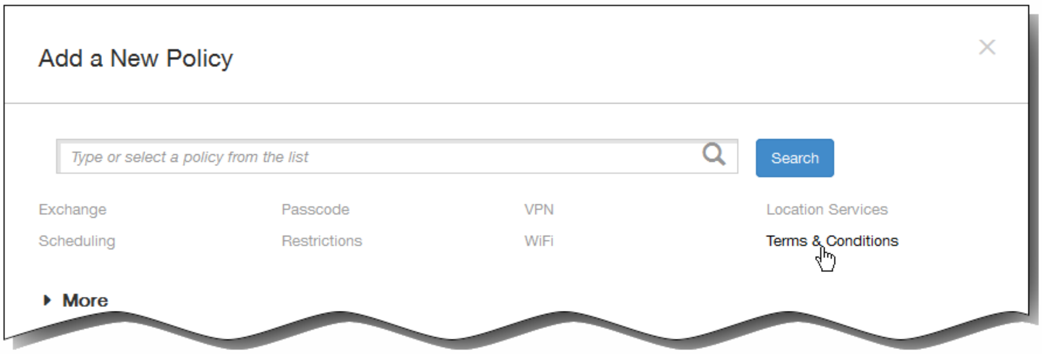
Deploy: ON

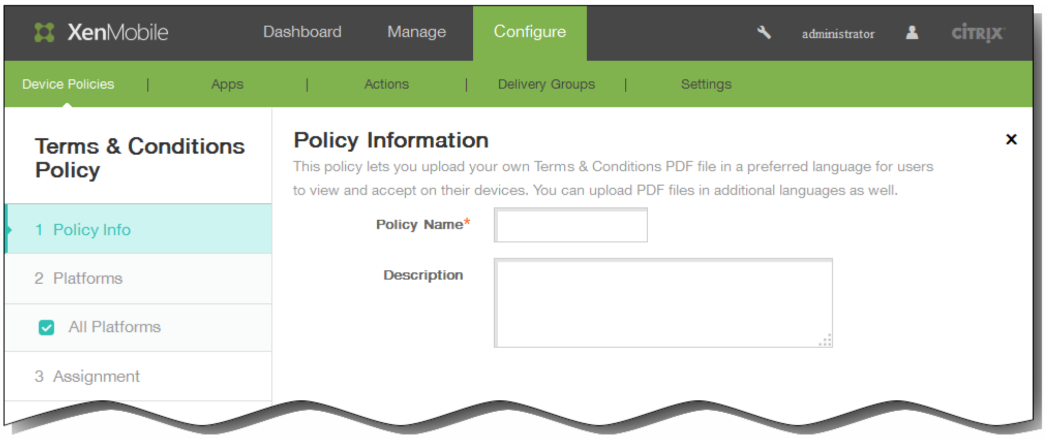
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

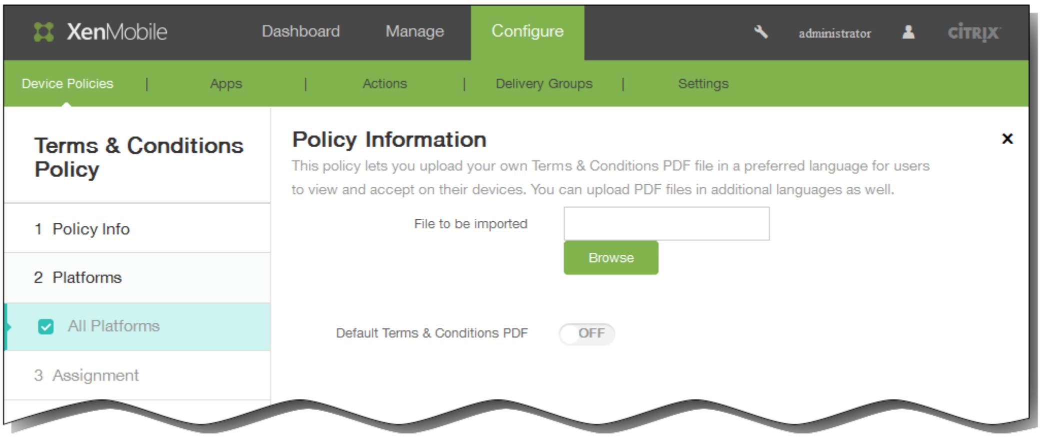
Deploy for always-on connections: OFF


XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies
Apps
Actions
Delivery Groups
Settings
Device Policies
Show filter
Search
Add
Policy name
Type
Created on
Last updated on
Status
No results found.

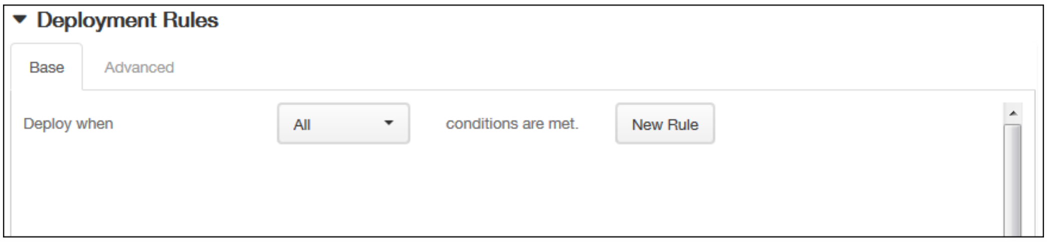

Add a New Policy
Type or select a policy from the list
Search
Exchange
Passcode
VPN
Location Services
Scheduling
Restrictions
WiFi
Terms & Conditions
More

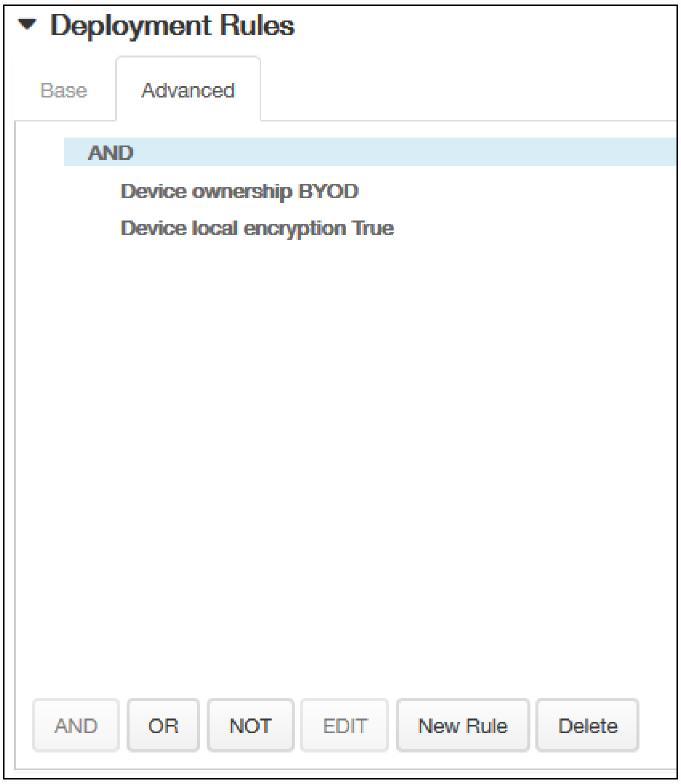


This policy lets you upload your own Terms & Conditions PDF file in a preferred language for users to view and accept on their devices. You can upload PDF files in additional languages as well.



This policy lets you upload your own Terms & Conditions PDF file in a preferred language for users to view and accept on their devices. You can upload PDF files in additional languages as well.

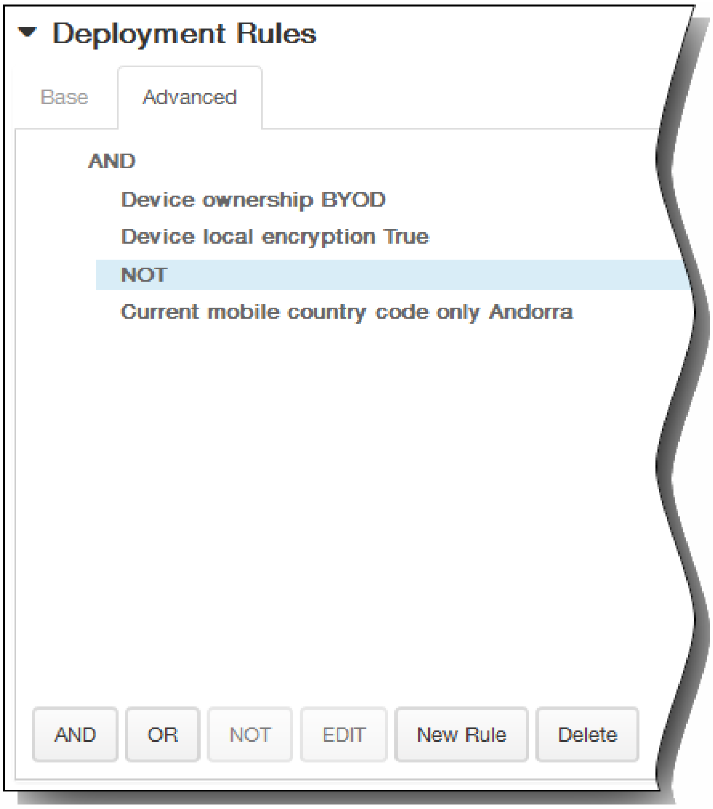




AND

Device ownership BYOD

Device local encryption True



▼ Deployment Rules

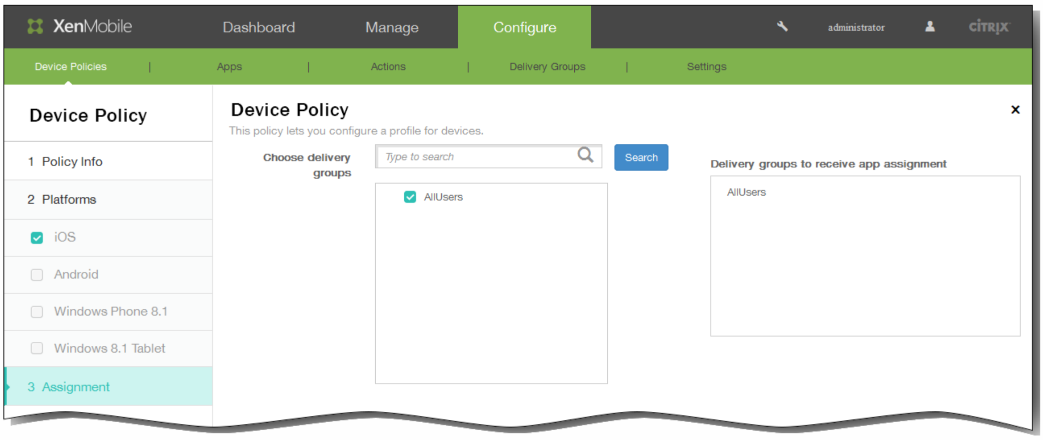
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

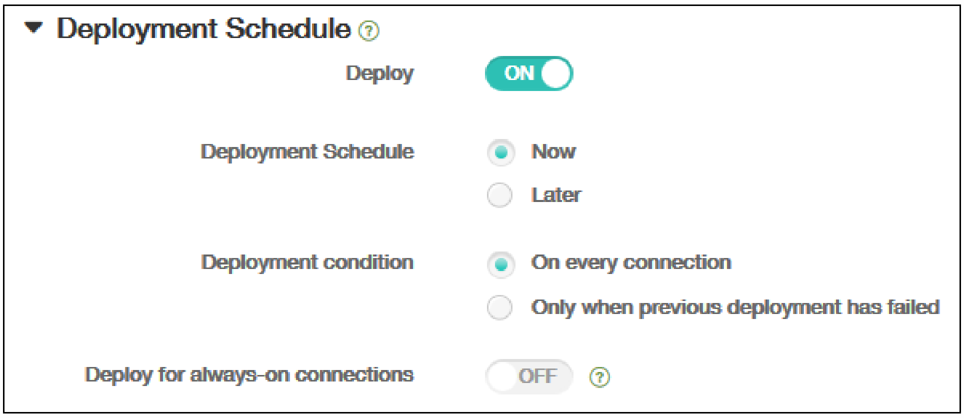
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



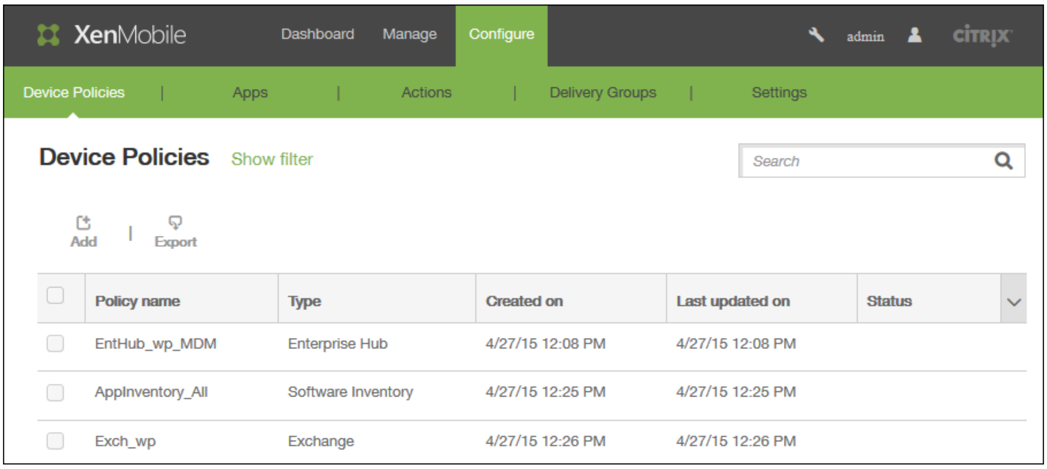
Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

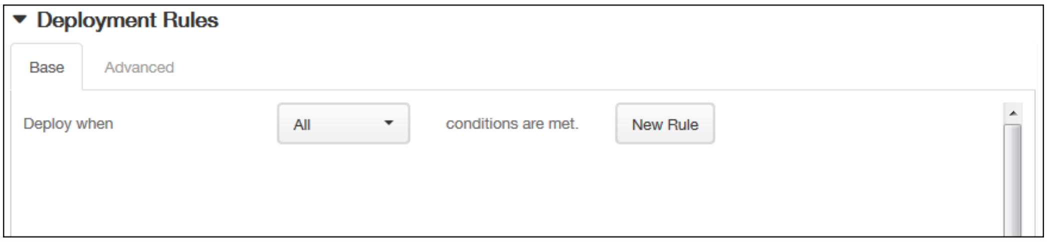
Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF



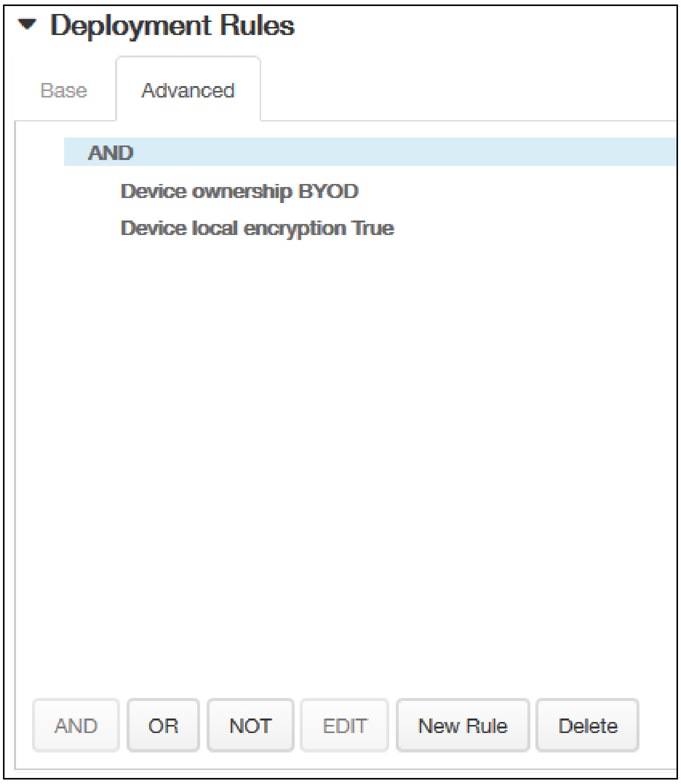
Device Policies

Policy name	Type	Created on	Last updated on	Status
EntHub_wp_MDM	Enterprise Hub	4/27/15 12:08 PM	4/27/15 12:08 PM	
AppInventory_All	Software Inventory	4/27/15 12:25 PM	4/27/15 12:25 PM	
Exch_wp	Exchange	4/27/15 12:26 PM	4/27/15 12:26 PM	



Deployment Rules

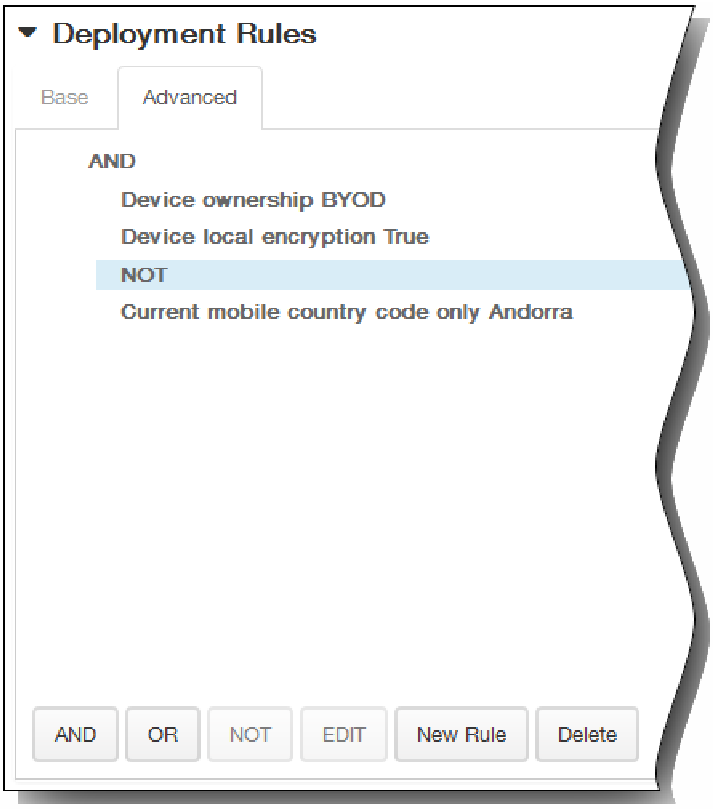
Deploy when All conditions are met.



AND

Device ownership BYOD

Device local encryption True



Deployment Rules

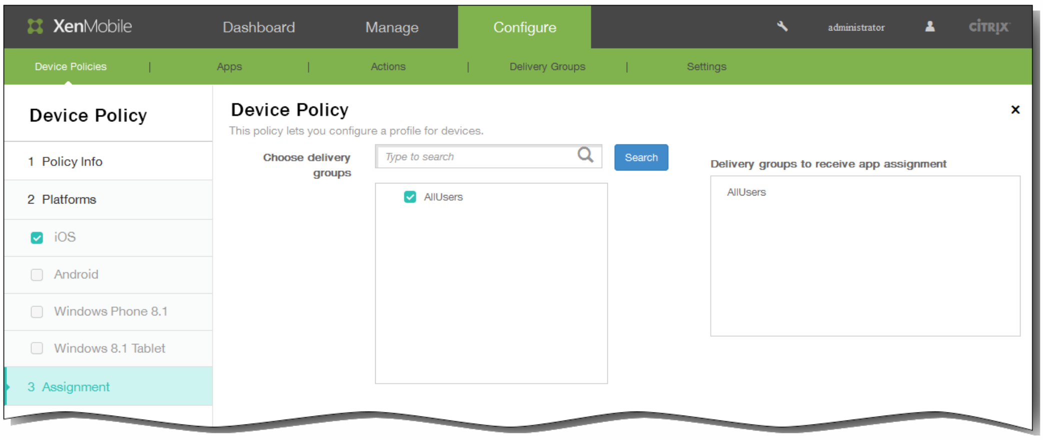
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

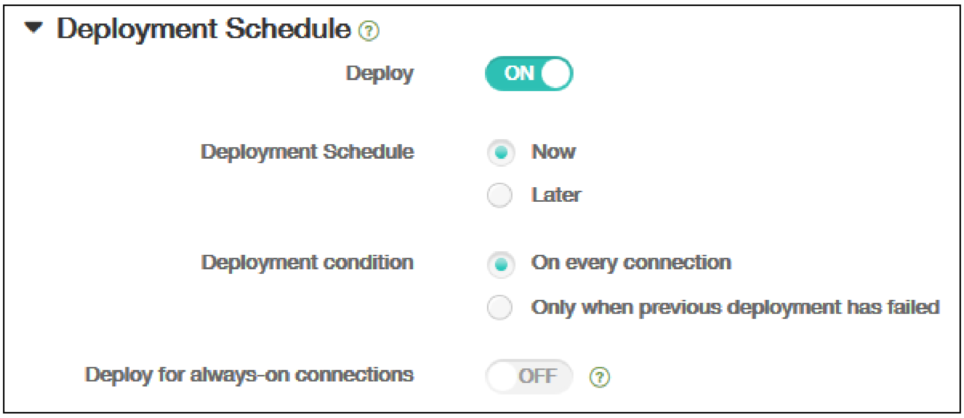
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



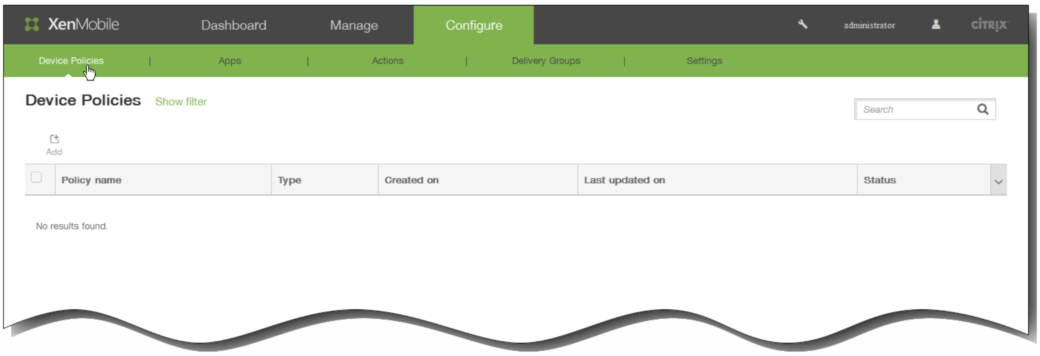
Deployment Schedule

Deploy: ON

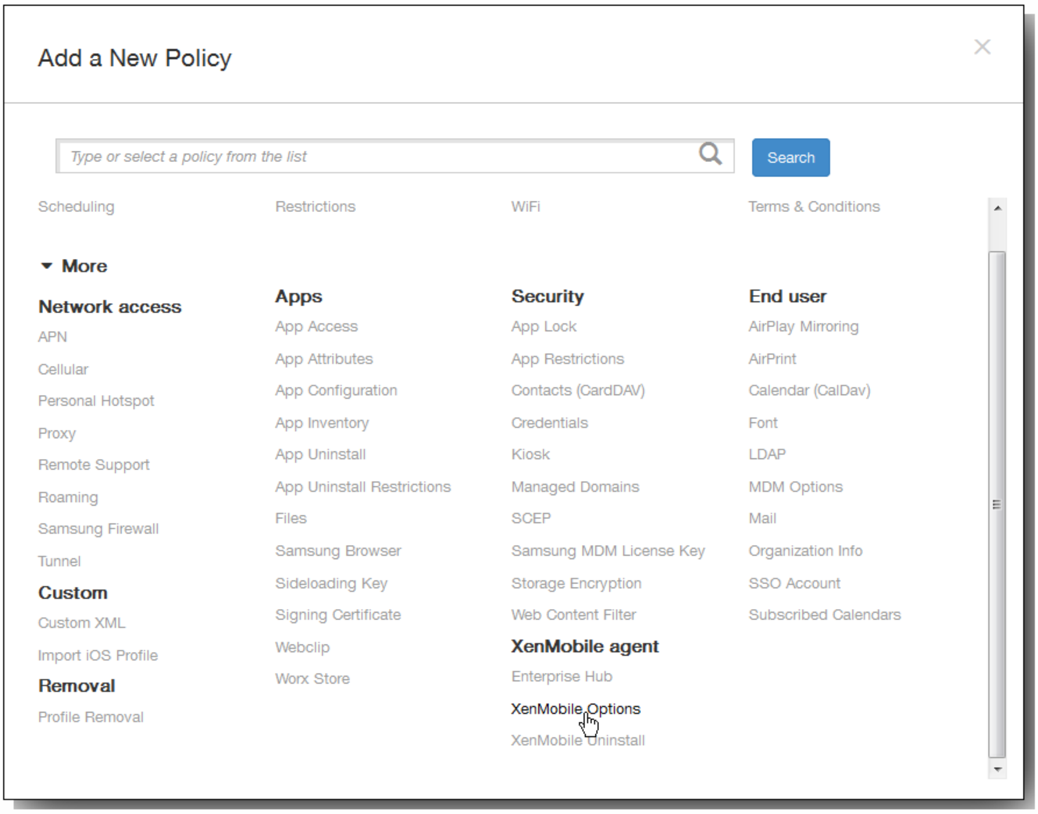
Deployment Schedule: ● Now ○ Later

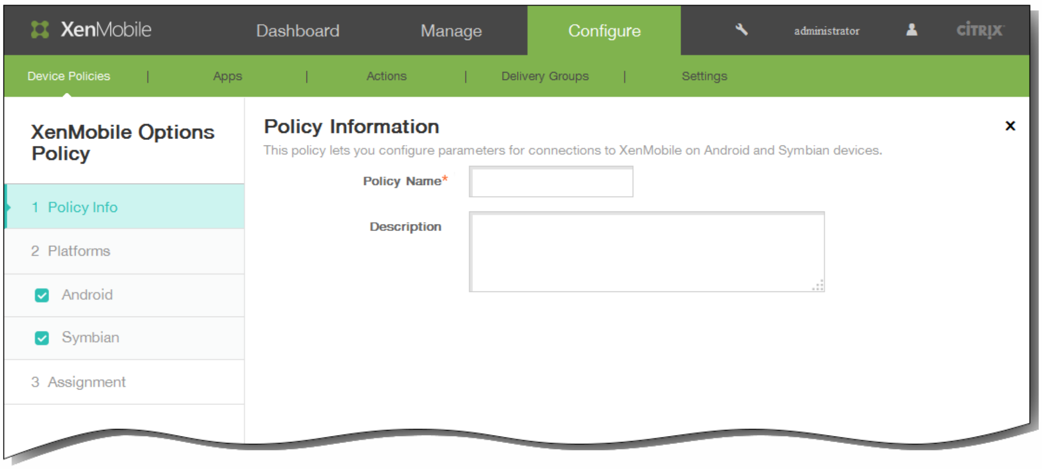
Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF



No results found.





XenMobile Dashboard Manage Configure administrator

Device Policies | Apps | Actions | Delivery Groups | Settings

XenMobile Options Policy

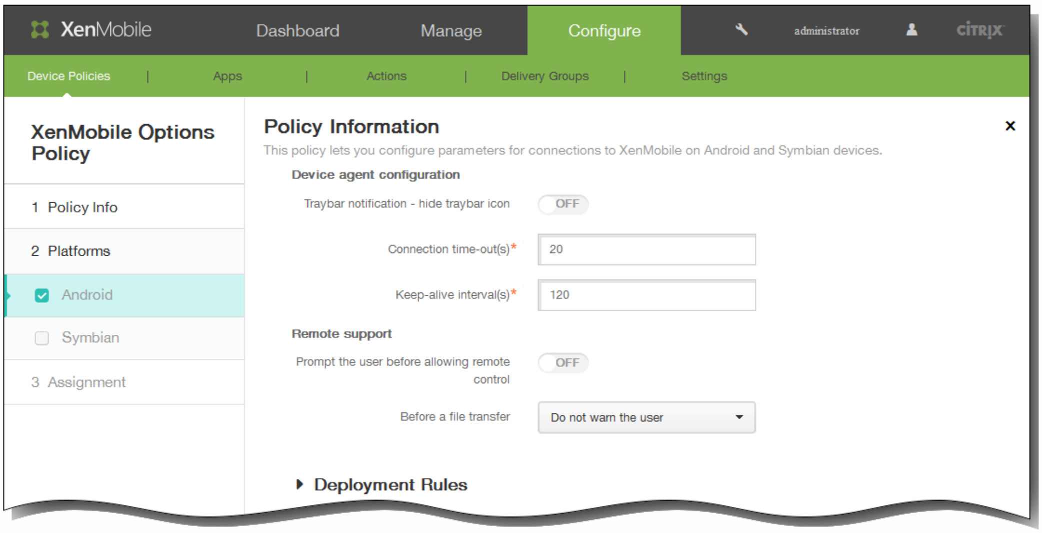
1 Policy Info
2 Platforms
☑ Android
☑ Symbian
3 Assignment

Policy Information

This policy lets you configure parameters for connections to XenMobile on Android and Symbian devices.

Policy Name*

Description



XenMobile Dashboard Manage Configure administrator

Device Policies | Apps | Actions | Delivery Groups | Settings

XenMobile Options Policy

1 Policy Info
2 Platforms
☑ Android
□ Symbian
3 Assignment

Policy Information

This policy lets you configure parameters for connections to XenMobile on Android and Symbian devices.

Device agent configuration

Traybar notification - hide traybar icon: OFF

Connection time-out(s)*: 20

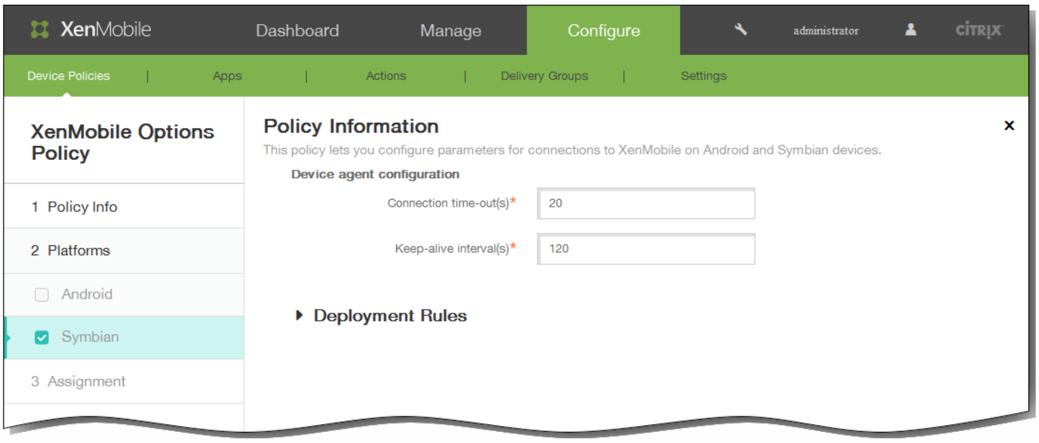
Keep-alive interval(s)*: 120

Remote support

Prompt the user before allowing remote control: OFF

Before a file transfer: Do not warn the user

▸ Deployment Rules



XenMobile
Dashboard
Manage
Configure
administrator
Device Policies | Apps | Actions | Delivery Groups | Settings

XenMobile Options Policy

1 Policy Info
2 Platforms
□ Android
☑ Symbian
3 Assignment

Policy Information

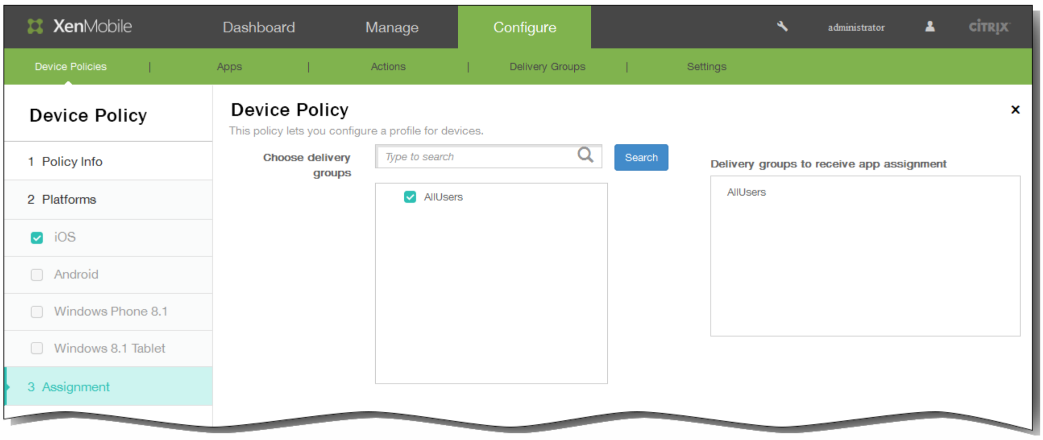
This policy lets you configure parameters for connections to XenMobile on Android and Symbian devices.

Device agent configuration

Connection time-out(s)* 20

Keep-alive interval(s)* 120

Deployment Rules



Device Policy

1 Policy Info
2 Platforms
☑ iOS
□ Android
□ Windows Phone 8.1
□ Windows 8.1 Tablet
3 Assignment

Device Policy

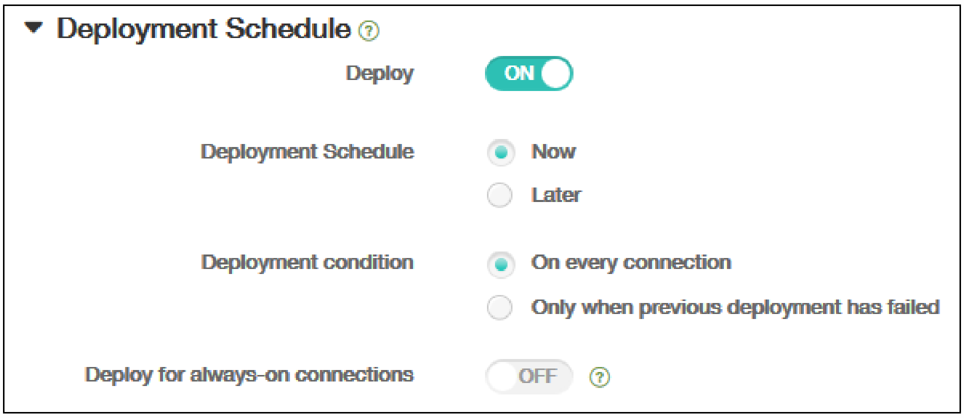
This policy lets you configure a profile for devices.

Choose delivery groups

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



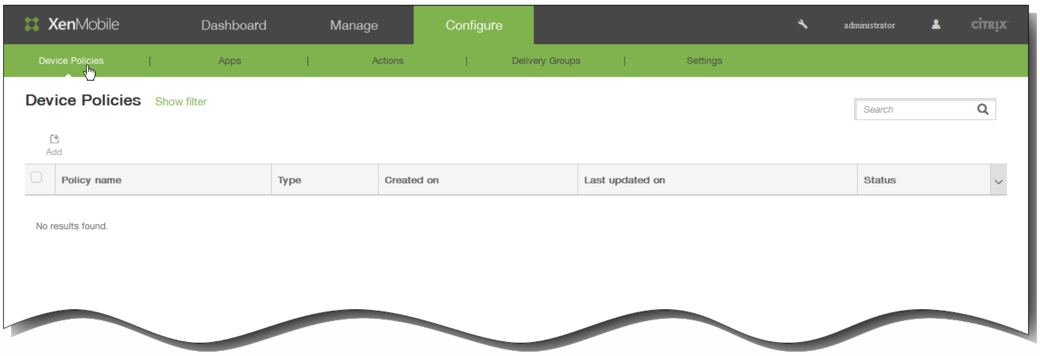
Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF



XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings

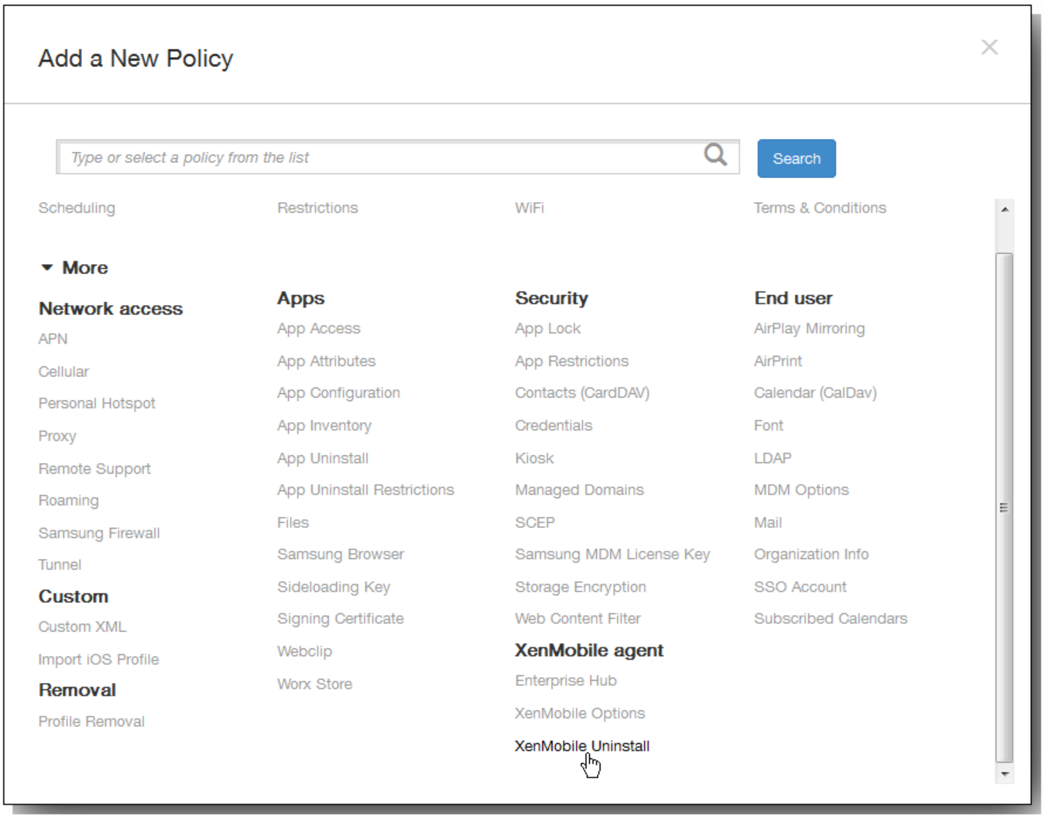
Device Policies Show filter

Search

Add

□	Policy name	Type	Created on	Last updated on	Status

No results found.



Add a New Policy

Type or select a policy from the list

Scheduling | Restrictions | WiFi | Terms & Conditions

▼ More

Network access
APN
Cellular
Personal Hotspot
Proxy
Remote Support
Roaming
Samsung Firewall
Tunnel

Custom
Custom XML
Import iOS Profile

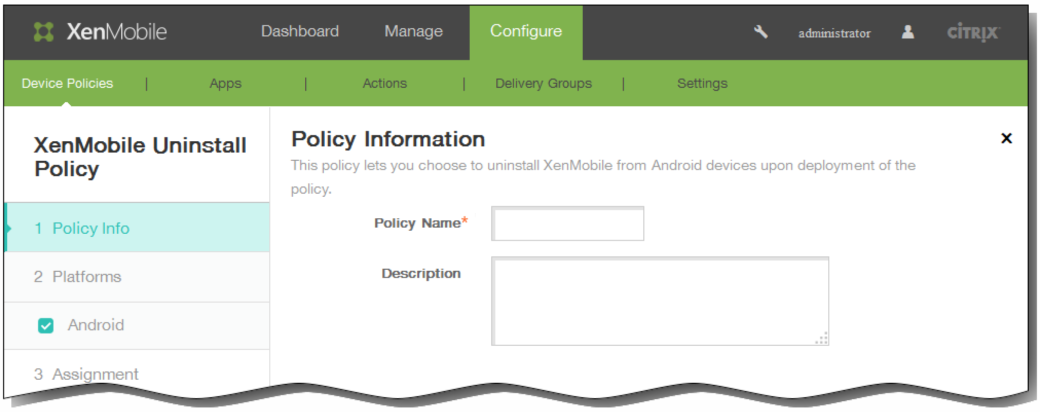
Removal
Profile Removal

Apps
App Access
App Attributes
App Configuration
App Inventory
App Uninstall
App Uninstall Restrictions
Files
Samsung Browser
Sideloading Key
Signing Certificate
Webclip
Worx Store

Security
App Lock
App Restrictions
Contacts (CardDAV)
Credentials
Kiosk
Managed Domains
SCEP
Samsung MDM License Key
Storage Encryption
Web Content Filter

XenMobile agent
Enterprise Hub
XenMobile Options
XenMobile Uninstall

End user
AirPlay Mirroring
AirPrint
Calendar (CalDav)
Font
LDAP
MDM Options
Mail
Organization Info
SSO Account
Subscribed Calendars


XenMobile
Dashboard
Manage
Configure
administrator
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings
×

XenMobile Uninstall Policy

1 Policy Info

2 Platforms

☑ Android

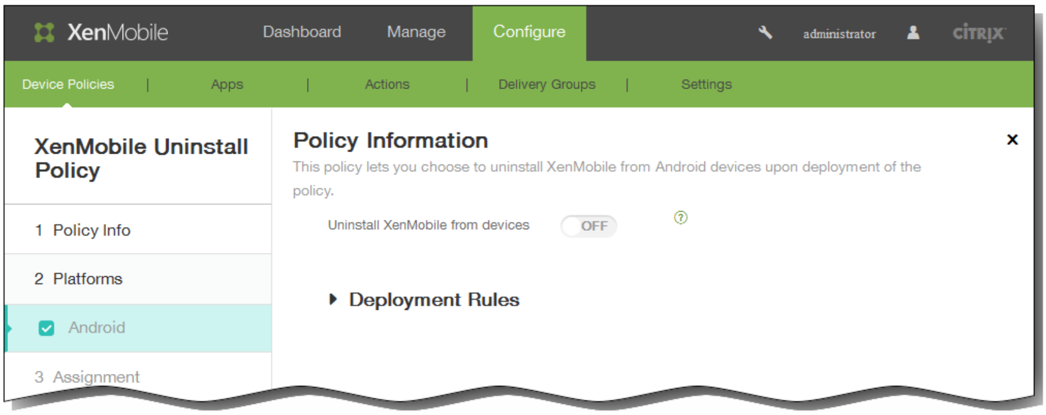
3 Assignment

Policy Information

This policy lets you choose to uninstall XenMobile from Android devices upon deployment of the policy.

Policy Name*

Description


XenMobile
Dashboard
Manage
Configure
administrator
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings
×

XenMobile Uninstall Policy

1 Policy Info

2 Platforms

☑ Android

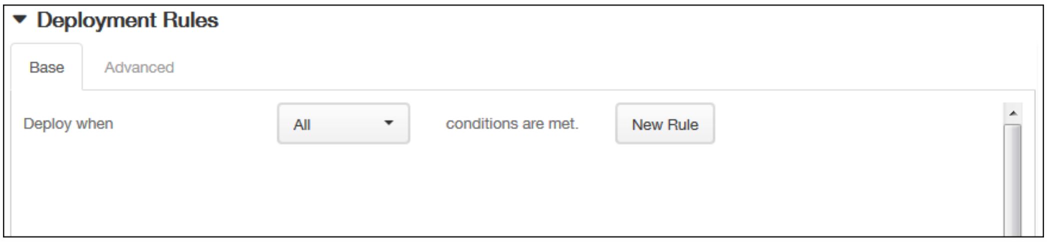
3 Assignment

Policy Information

This policy lets you choose to uninstall XenMobile from Android devices upon deployment of the policy.

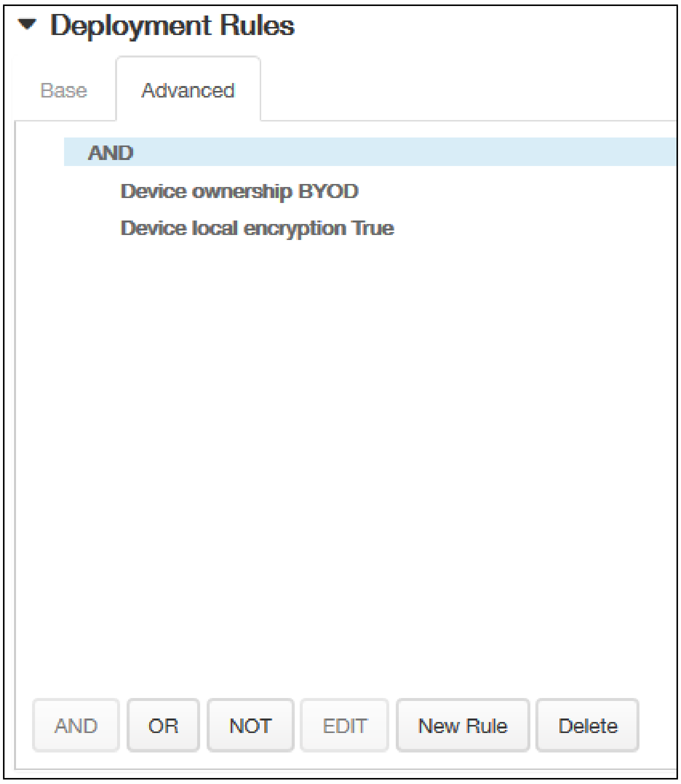
Uninstall XenMobile from devices OFF

▸ Deployment Rules



▾ Deployment Rules

Deploy when All conditions are met.

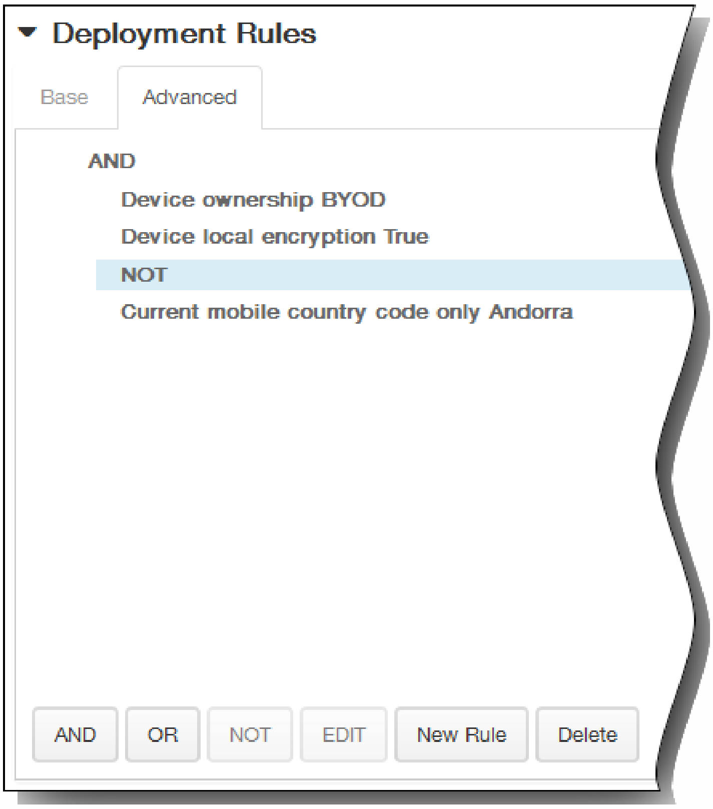


Deployment Rules

AND

Device ownership BYOD

Device local encryption True



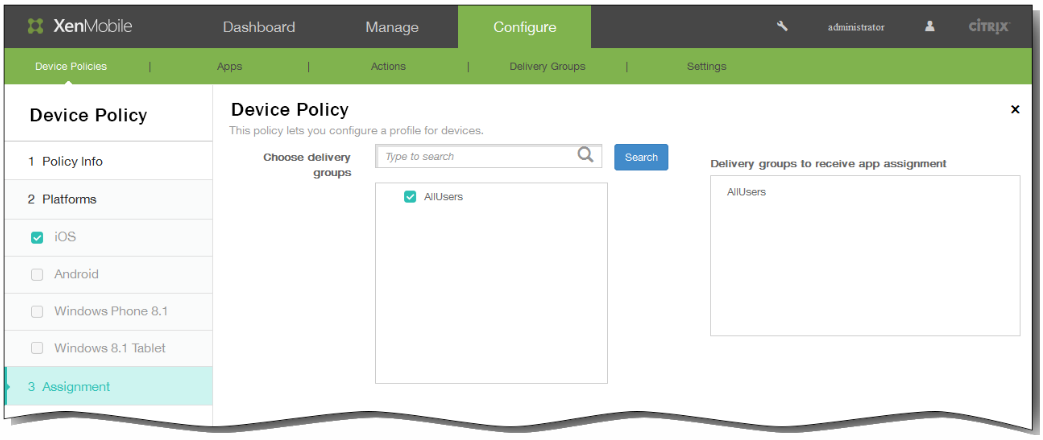
AND

Device ownership BYOD

Device local encryption True

NOT

Current mobile country code only Andorra



Device Policy

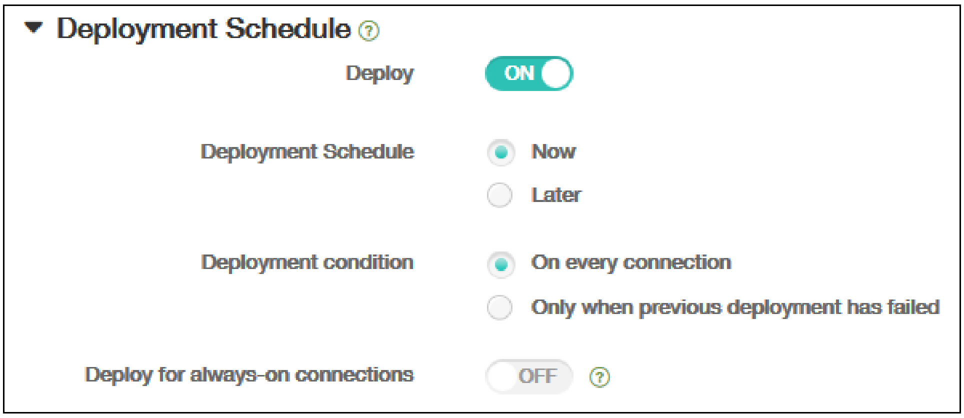
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



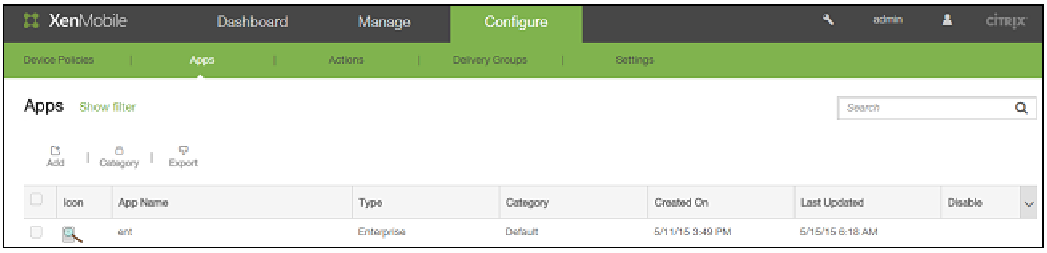
Deployment Schedule

Deploy: ON

Deployment Schedule: ● Now ○ Later

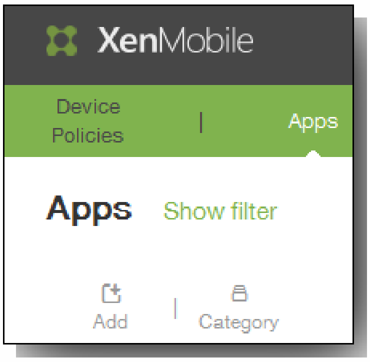
Deployment condition: ● On every connection ○ Only when previous deployment has failed

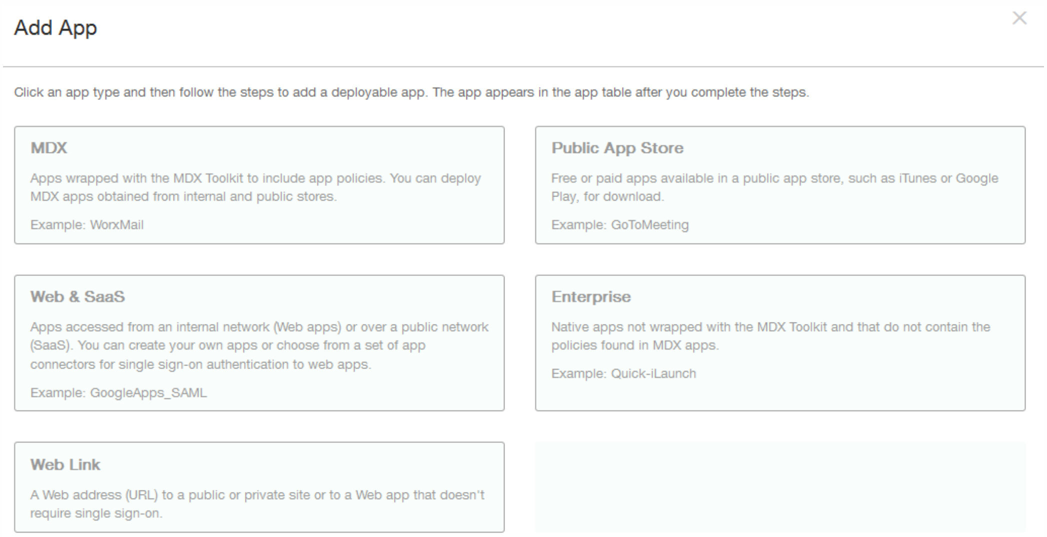
Deploy for always-on connections: OFF



Apps

	Icon	App Name	Type	Category	Created On	Last Updated	Disable
□		ant	Enterprise	Default	5/11/15 3:49 PM	5/15/15 6:18 AM	




Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

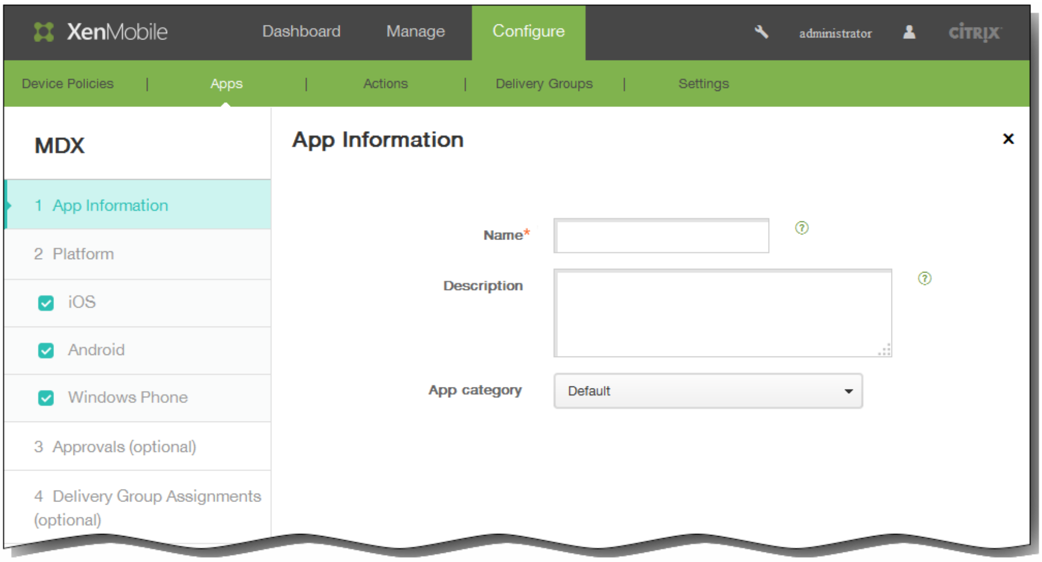
Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

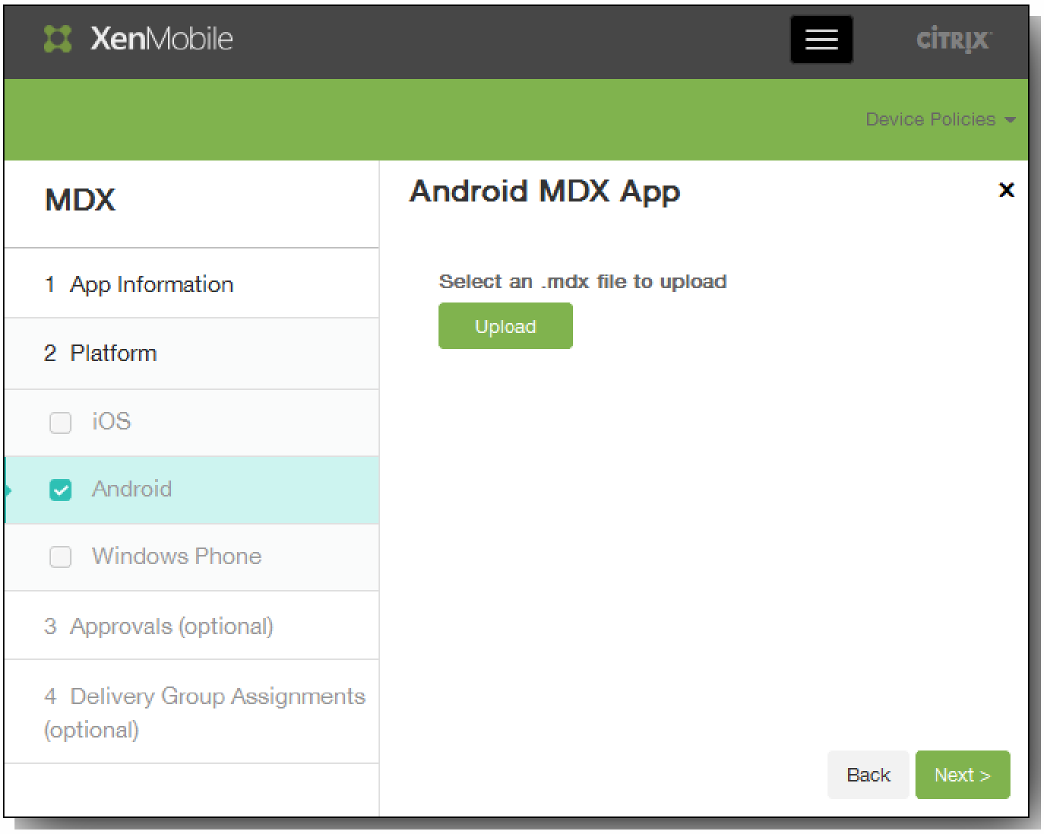
Example: Quick-iLaunch

Web Link

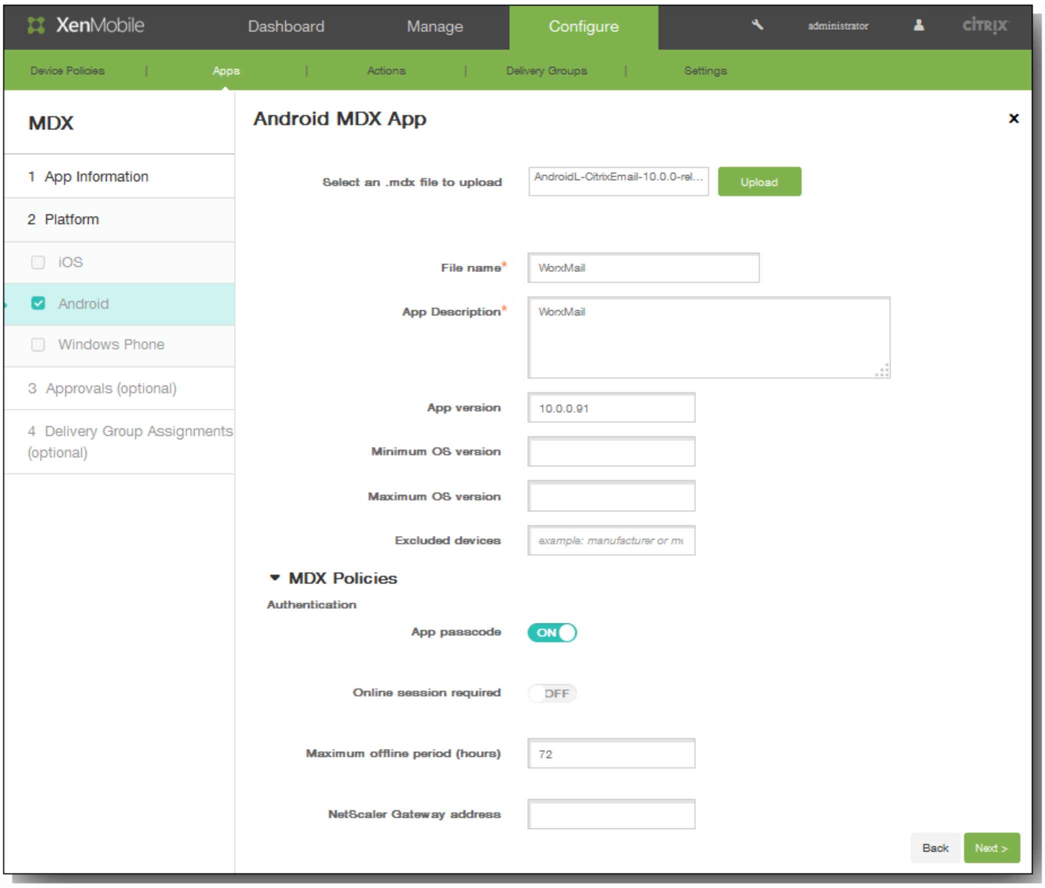
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.



XenMobile
Dashboard
Manage
Configure
administrator
Device Policies | Apps | Actions | Delivery Groups | Settings
MDX
1 App Information
2 Platform
☑ iOS
☑ Android
☑ Windows Phone
3 Approvals (optional)
4 Delivery Group Assignments (optional)
App Information
×
Name*
Description
App category
Default



XenMobile
Device Policies
MDX
1 App Information
2 Platform
□ iOS
☑ Android
□ Windows Phone
3 Approvals (optional)
4 Delivery Group Assignments (optional)
Android MDX App
×
Select an .mdx file to upload
Upload
Back
Next >



Android MDX App

Select an .mdx file to upload: AndroidL-CitrixEmail-10.0.0-rel...

File name*: WorxMail

App Description*: WorxMail

App version: 10.0.0.91

Minimum OS version:

Maximum OS version:

Excluded devices: example: manufacturer or m

MDX Policies

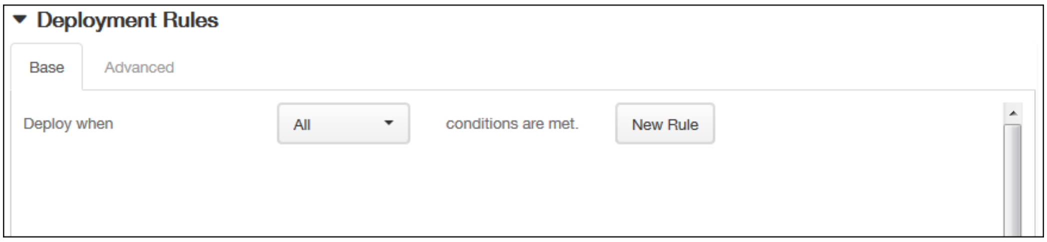
Authentication

App passcode: ON

Online session required: OFF

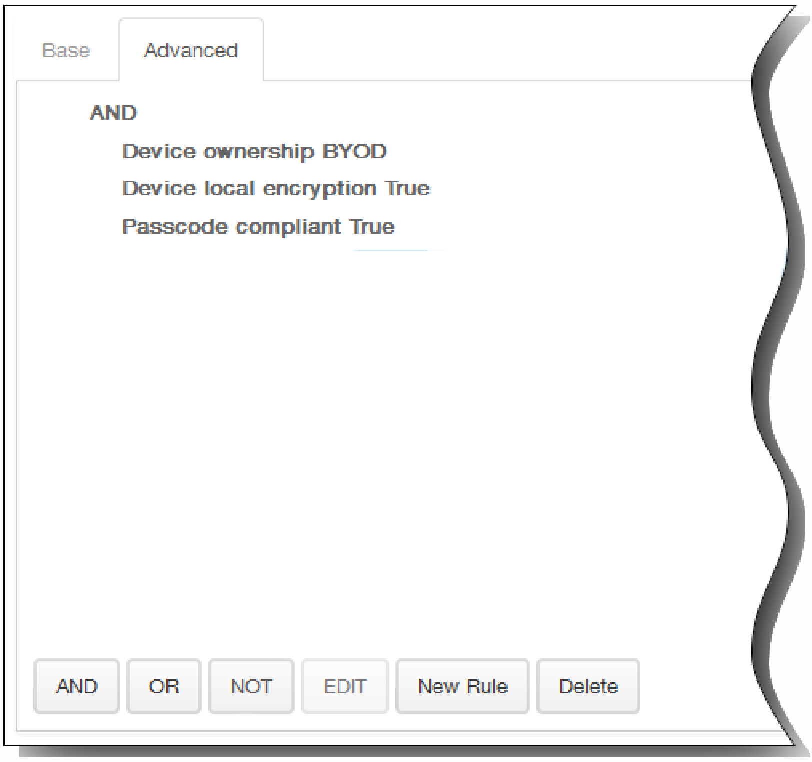
Maximum offline period (hours): 72

NetScaler Gateway address:



Deployment Rules

Deploy when All conditions are met.

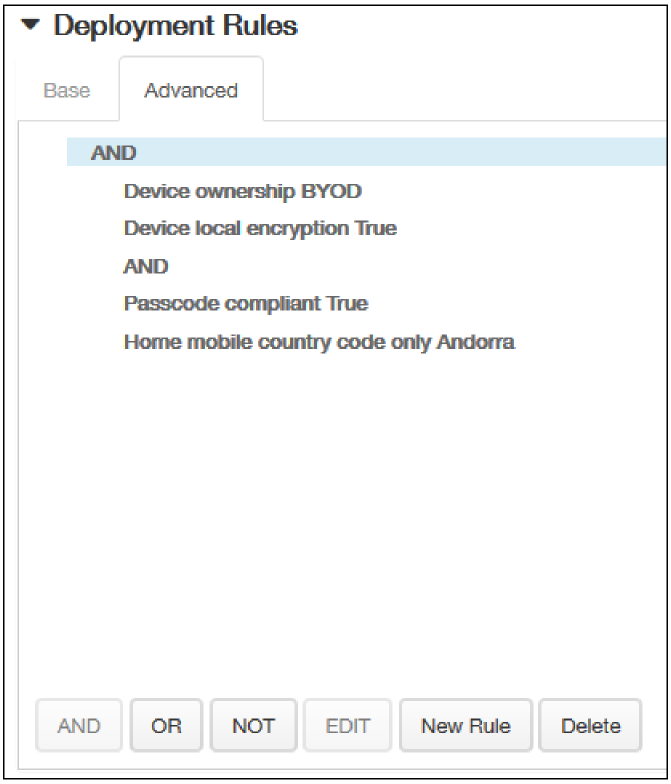


AND

Device ownership BYOD

Device local encryption True

Passcode compliant True


Deployment Rules

Base | Advanced

AND

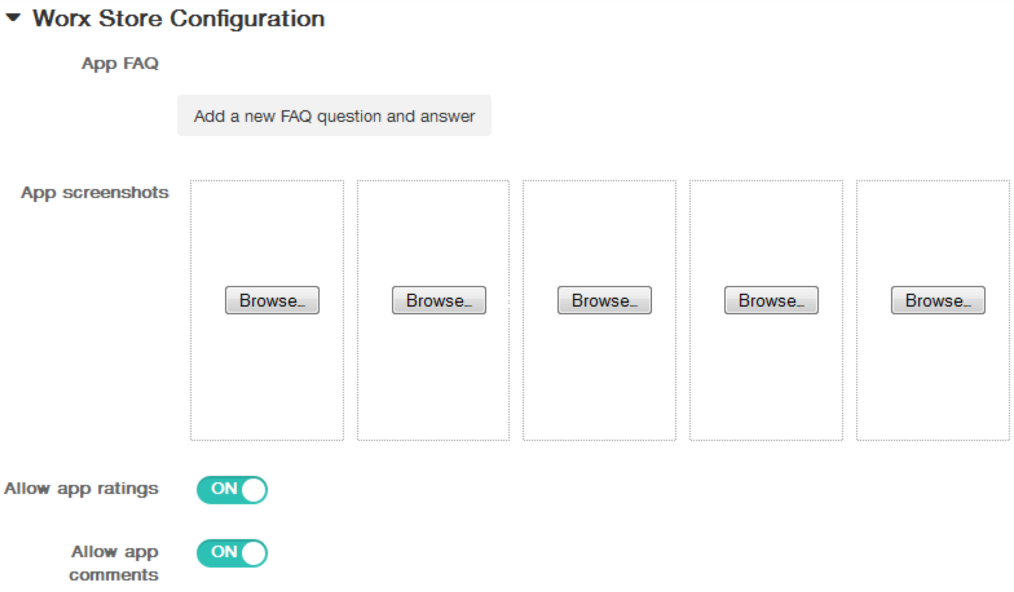
Device ownership BYOD

Device local encryption True

AND

Passcode compliant True

Home mobile country code only Andorra

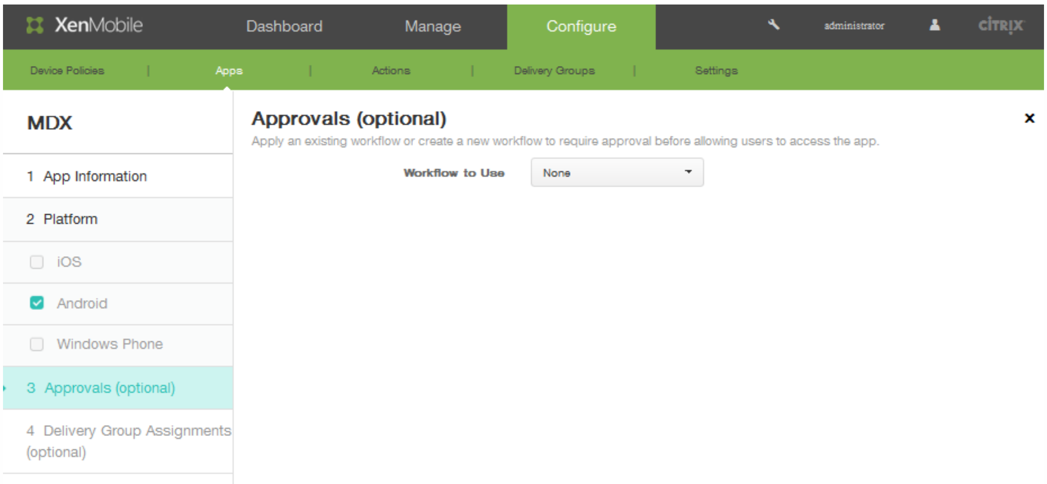

Worx Store Configuration

App FAQ

App screenshots

Allow app ratings: ON

Allow app comments: ON



MDX

1 App Information

2 Platform

□ iOS

☑ Android

□ Windows Phone

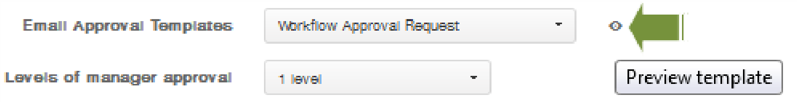
3 Approvals (optional)

4 Delivery Group Assignments (optional)

Approvals (optional)

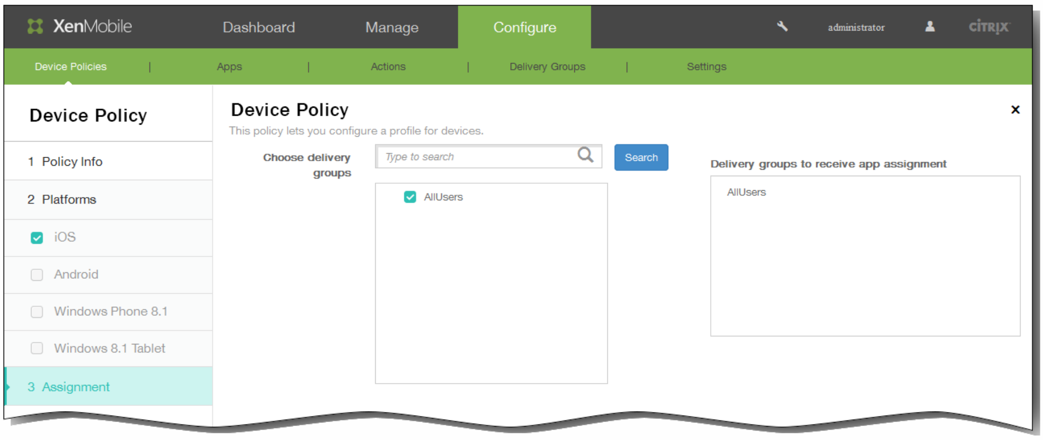
Apply an existing workflow or create a new workflow to require approval before allowing users to access the app.

Workflow to Use: None



Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level



Device Policy

1 Policy Info

2 Platforms

☑ iOS

□ Android

□ Windows Phone 8.1

□ Windows 8.1 Tablet

3 Assignment

Device Policy

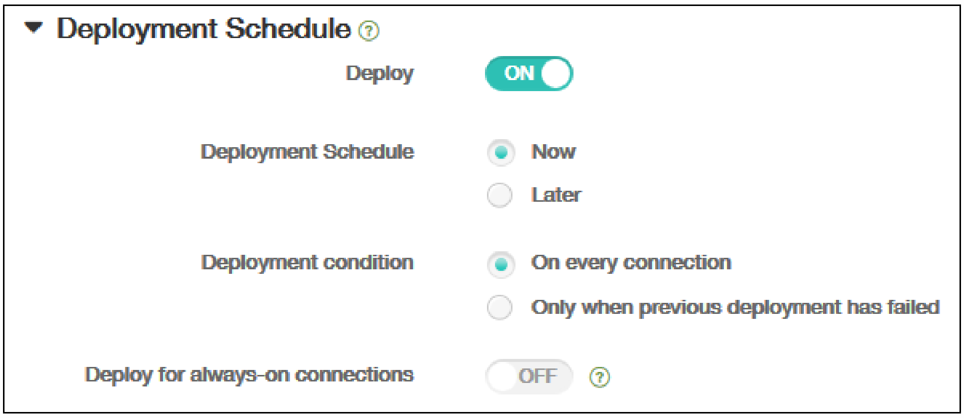
This policy lets you configure a profile for devices.

Choose delivery groups: Type to search

☑ AllUsers

Delivery groups to receive app assignment

AllUsers



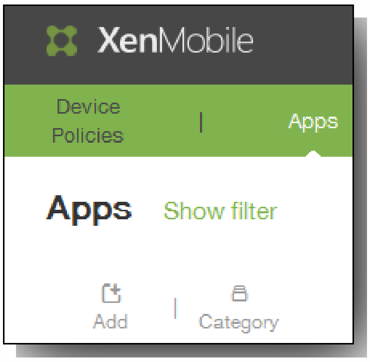
Deployment Schedule

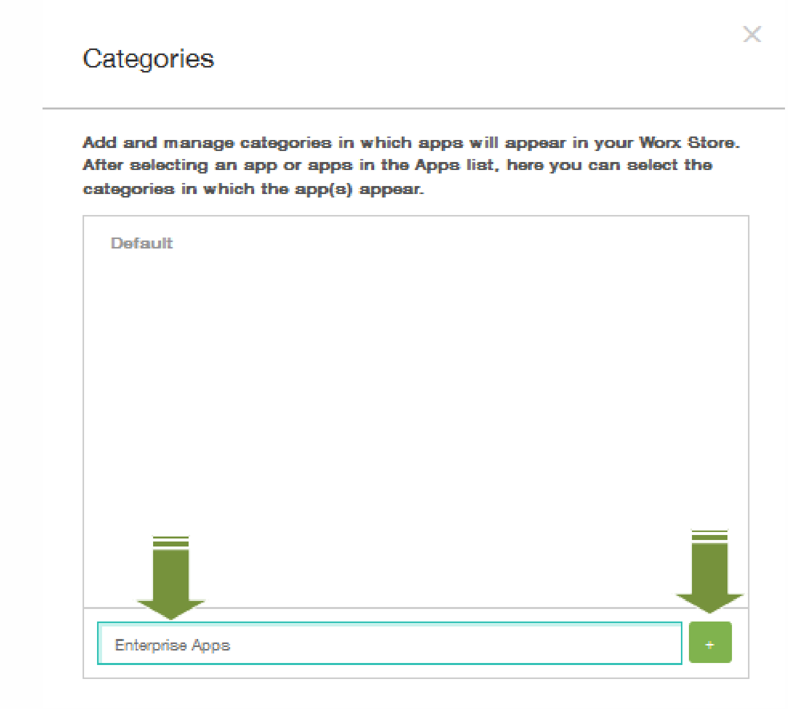
Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF


XenMobile
Device Policies
Apps
Apps
Show filter
Add
Category

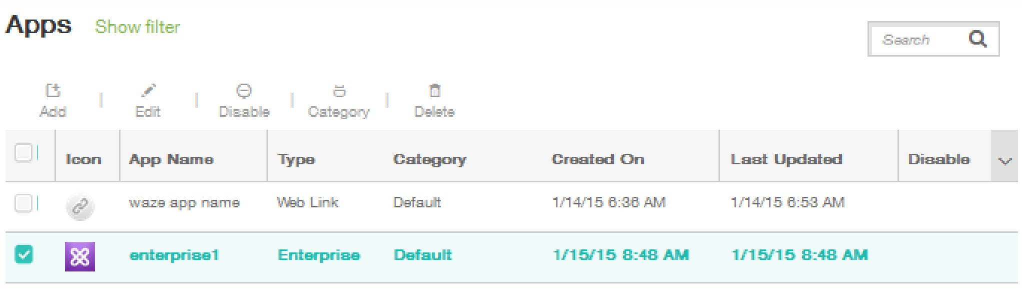


Categories

Add and manage categories in which apps will appear in your Worx Store. After selecting an app or apps in the Apps list, here you can select the categories in which the app(s) appear.

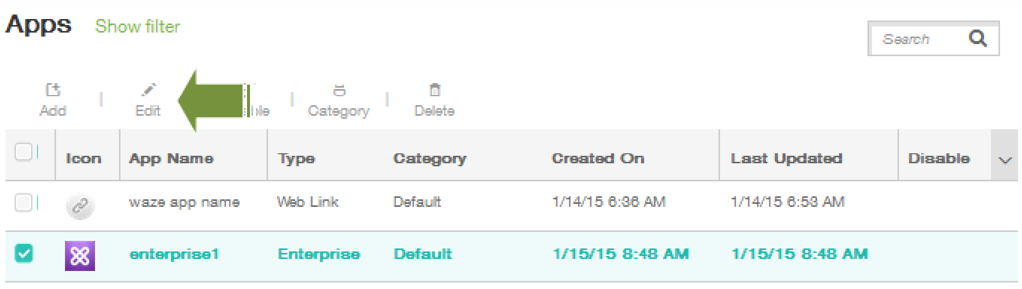
Default

Enterprise Apps



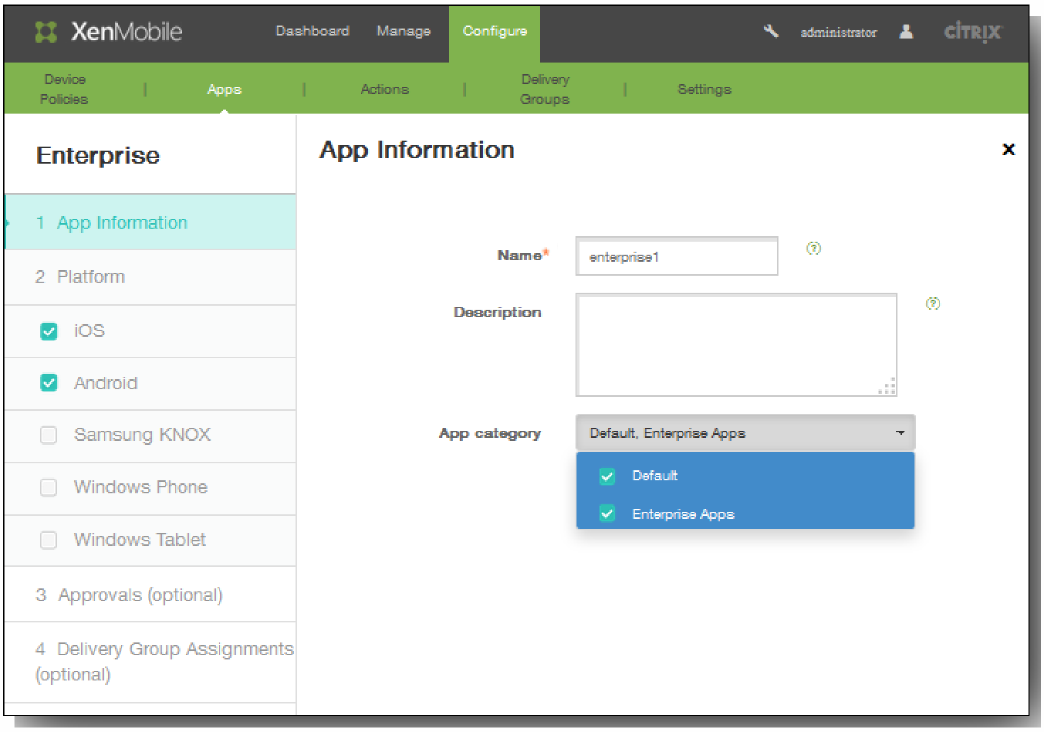
Apps Show filter

☐	Icon	App Name	Type	Category	Created On	Last Updated	Disable
☐		waze app name	Web Link	Default	1/14/15 6:36 AM	1/14/15 6:53 AM	
☑		enterprise1	Enterprise	Default	1/15/15 8:48 AM	1/15/15 8:48 AM	



Apps Show filter

☐	Icon	App Name	Type	Category	Created On	Last Updated	Disable
☐		waze app name	Web Link	Default	1/14/15 6:36 AM	1/14/15 6:53 AM	
☑		enterprise1	Enterprise	Default	1/15/15 8:48 AM	1/15/15 8:48 AM	



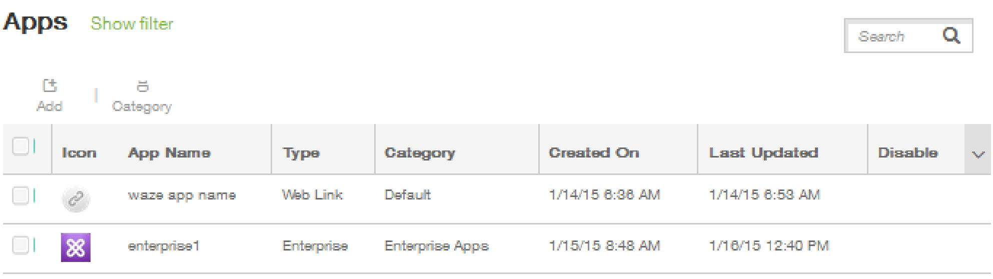
App Information

Name*: enterprise1

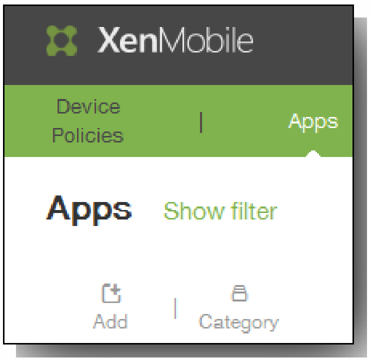
Description:

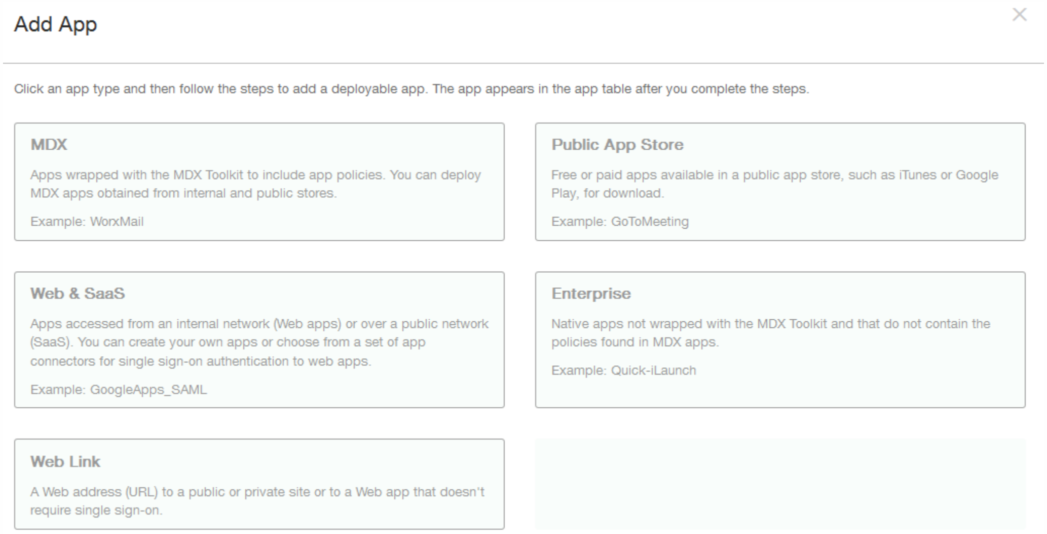
App category: Default, Enterprise Apps

- ☑ Default
- ☑ Enterprise Apps



□	Icon	App Name	Type	Category	Created On	Last Updated	Disable
□		waze app name	Web Link	Default	1/14/15 6:36 AM	1/14/15 6:53 AM	
□		enterprise1	Enterprise	Enterprise Apps	1/15/15 8:48 AM	1/16/15 12:40 PM	




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

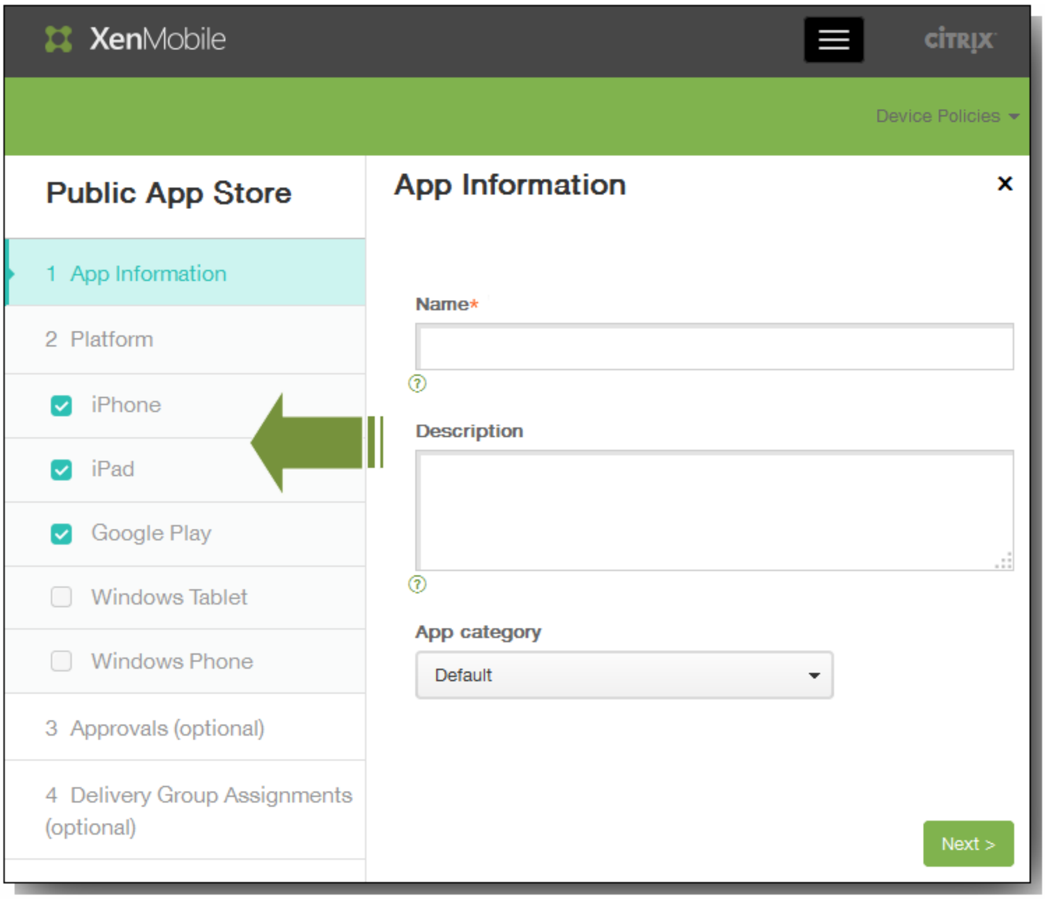
Enterprise

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.



Public App Store

1 App Information

2 Platform

- ☑ iPhone
- ☑ iPad
- ☑ Google Play
- □ Windows Tablet
- □ Windows Phone

3 Approvals (optional)

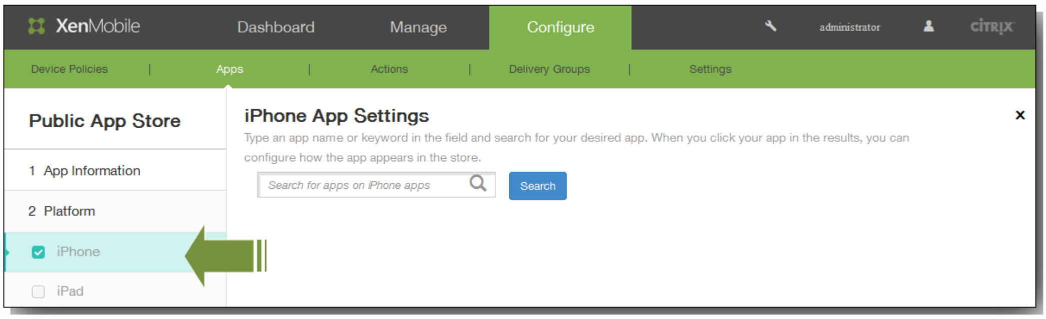
4 Delivery Group Assignments (optional)

App Information

Name*

Description

App category: Default



Public App Store

1 App Information

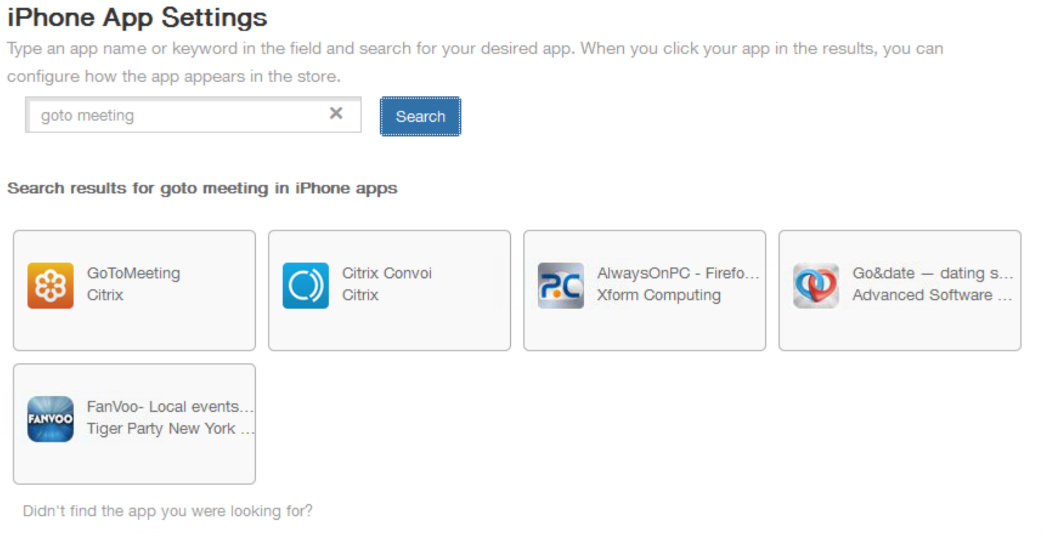
2 Platform

- ☑ iPhone
- □ iPad

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 for apps on iPhone apps



iPhone App Settings

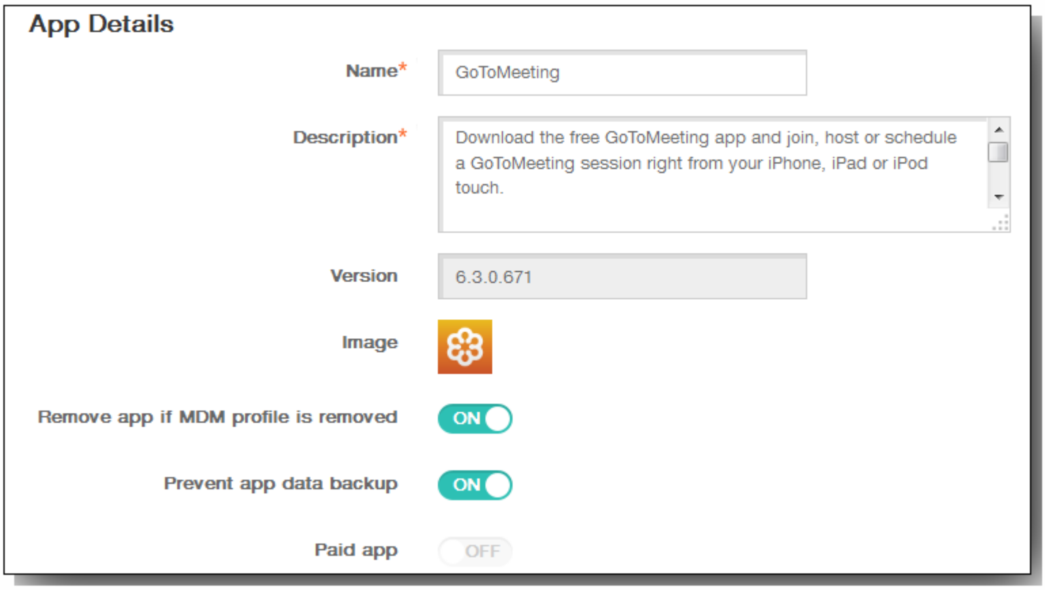
Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

goto meeting ✕ Search

Search results for goto meeting in iPhone apps

GoToMeeting	Citrix
Citrix Convoi	Citrix
AlwaysOnPC - Firefo…	Xform Computing
Go&date – dating s…	Advanced Software …
FanVoo- Local events…	Tiger Party New York …

Didn't find the app you were looking for?



App Details

Name* GoToMeeting

Description* Download the free GoToMeeting app and join, host or schedule a GoToMeeting session right from your iPhone, iPad or iPod touch.

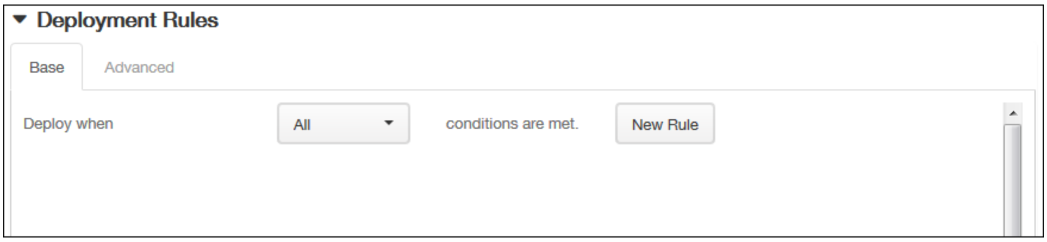
Version 6.3.0.671

Image

Remove app if MDM profile is removed ON

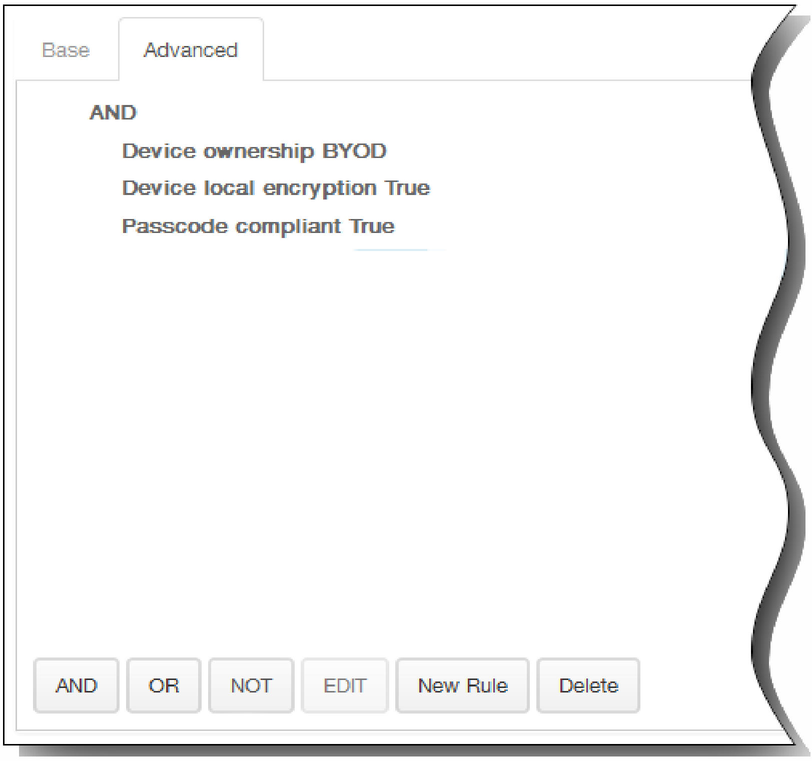
Prevent app data backup ON

Paid app OFF



Deployment Rules

Deploy when All conditions are met. New Rule

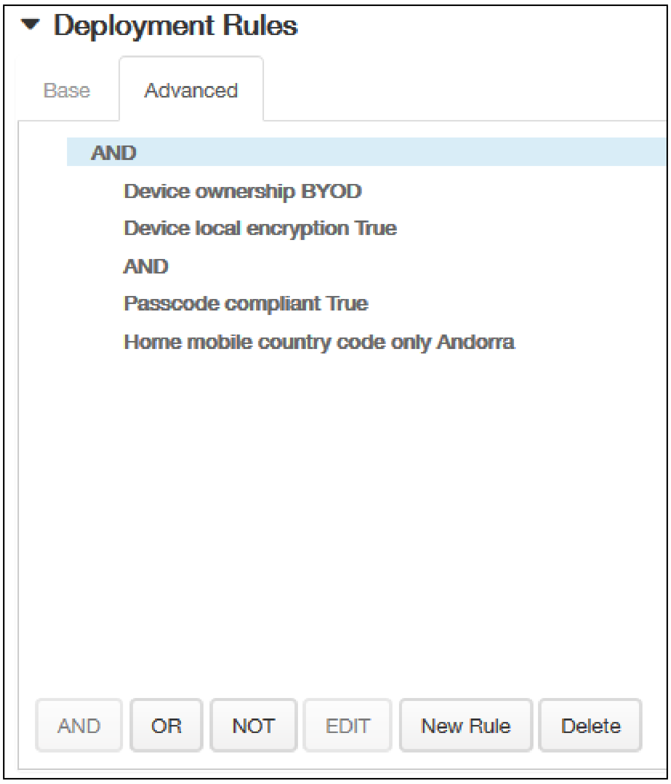


AND

Device ownership BYOD

Device local encryption True

Passcode compliant True



AND

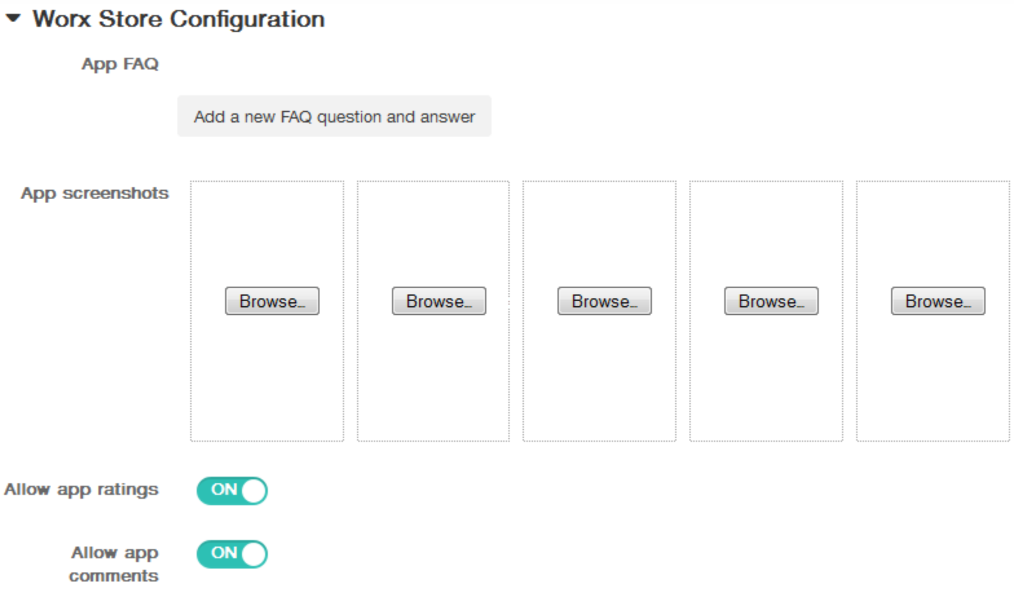
Device ownership BYOD

Device local encryption True

AND

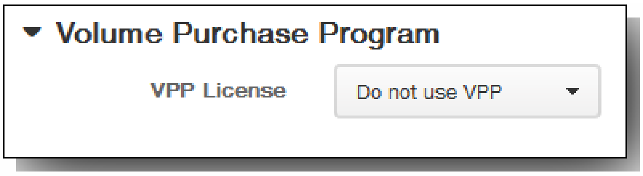
Passcode compliant True

Home mobile country code only Andorra



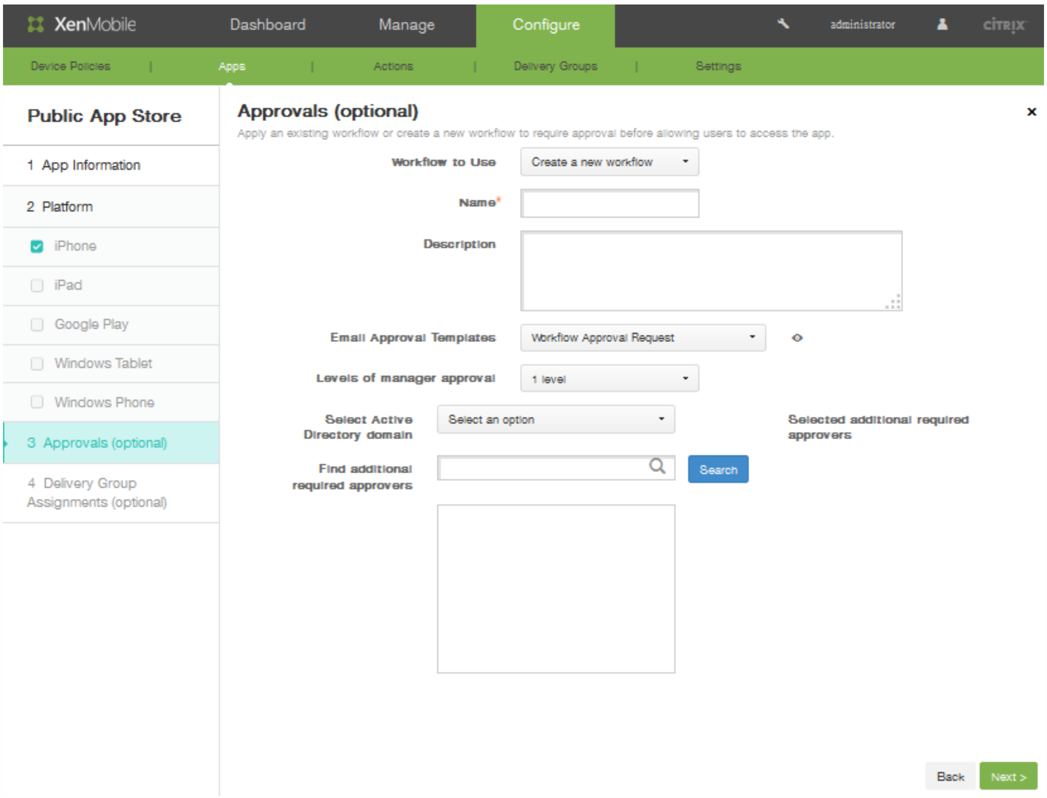
Allow app ratings ON

Allow app comments ON



Volume Purchase Program

VPP License: Do not use VPP



XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings

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:

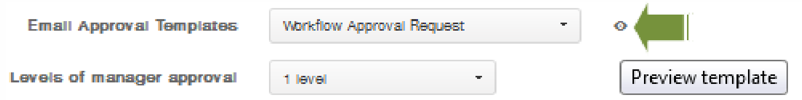
Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level

Select Active Directory domain: Select an option

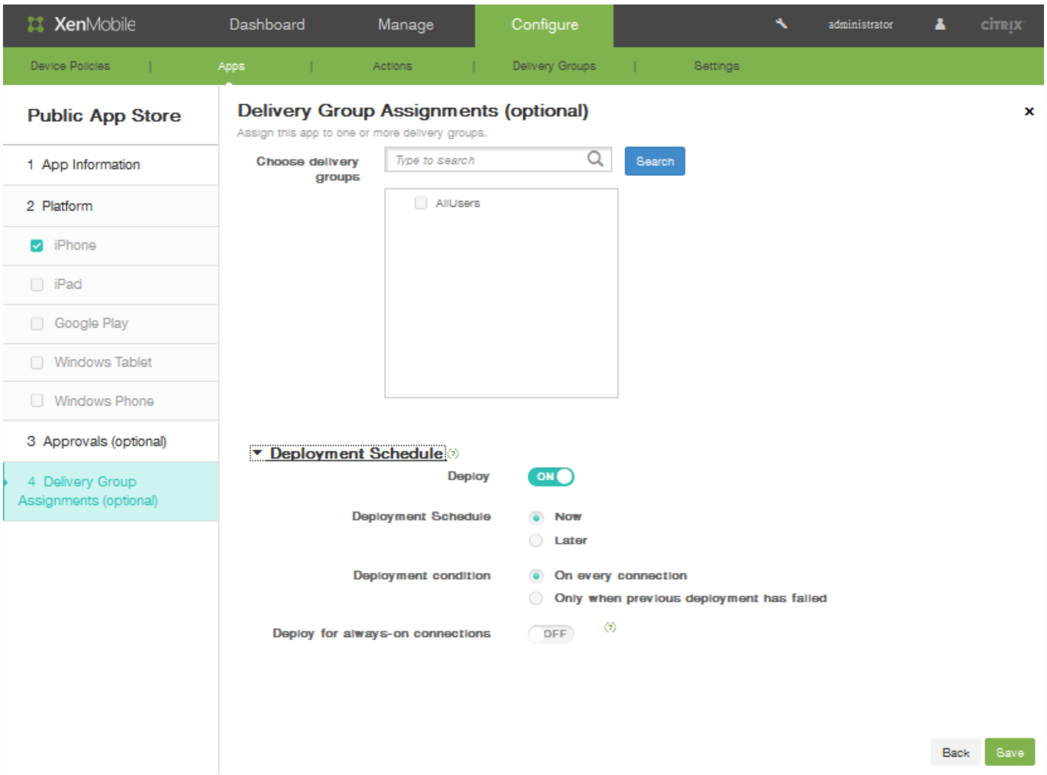
Selected additional required approvers

Find additional required approvers:



Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level



Delivery Group Assignments (optional)

Assign this app to one or more delivery groups.

Choose delivery groups: Type to search

□ AllUsers

Deployment Schedule

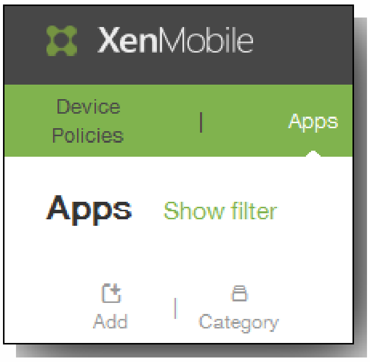
Deploy: ON

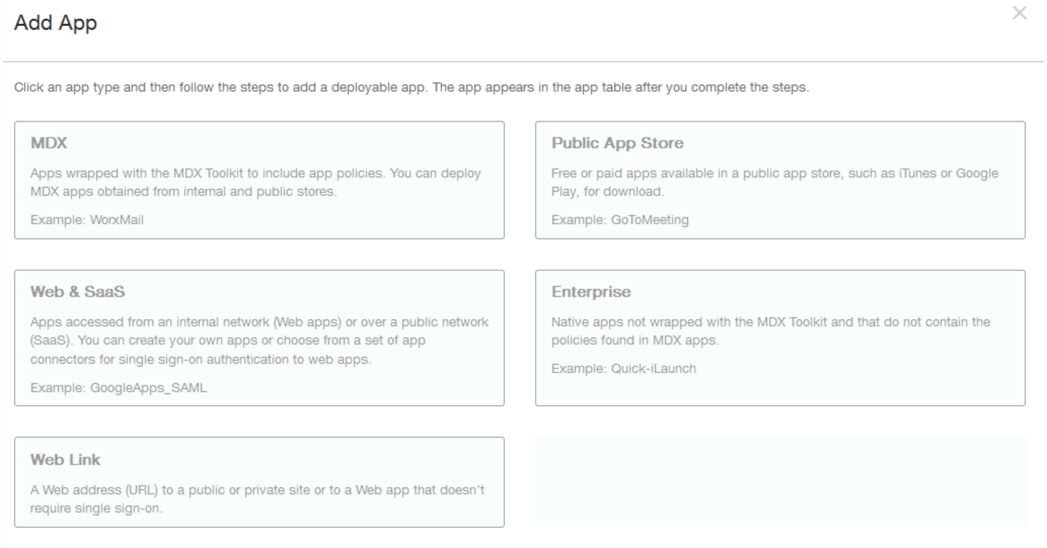
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF

To add an app connector in XenMobile





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

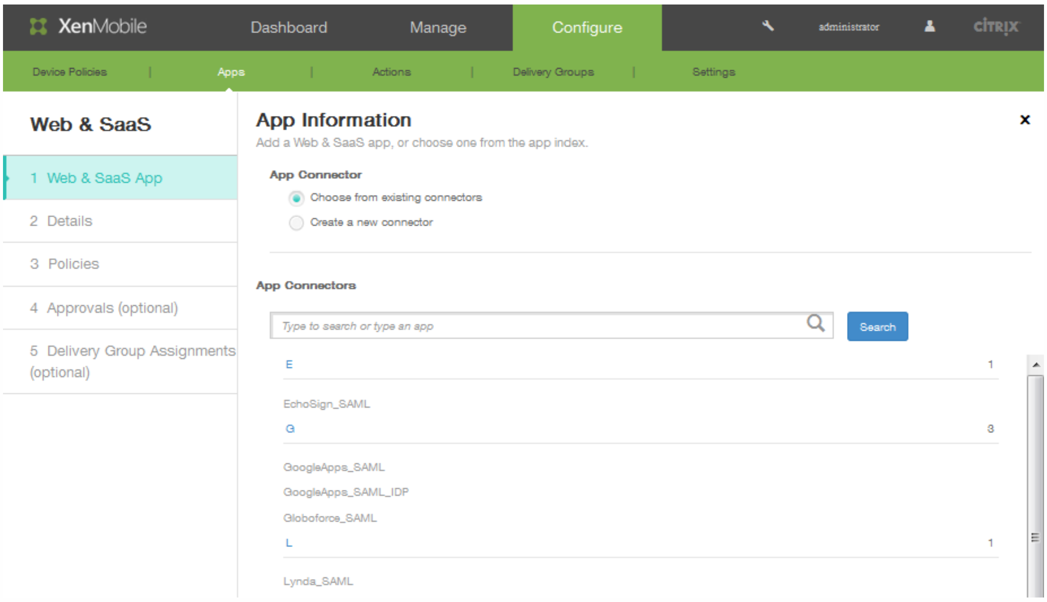
Enterprise

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.



Web & SaaS

1 Web & SaaS App

2 Details

3 Policies

4 Approvals (optional)

5 Delivery Group Assignments (optional)

App Information

Add a Web & SaaS app, or choose one from the app index.

App Connector

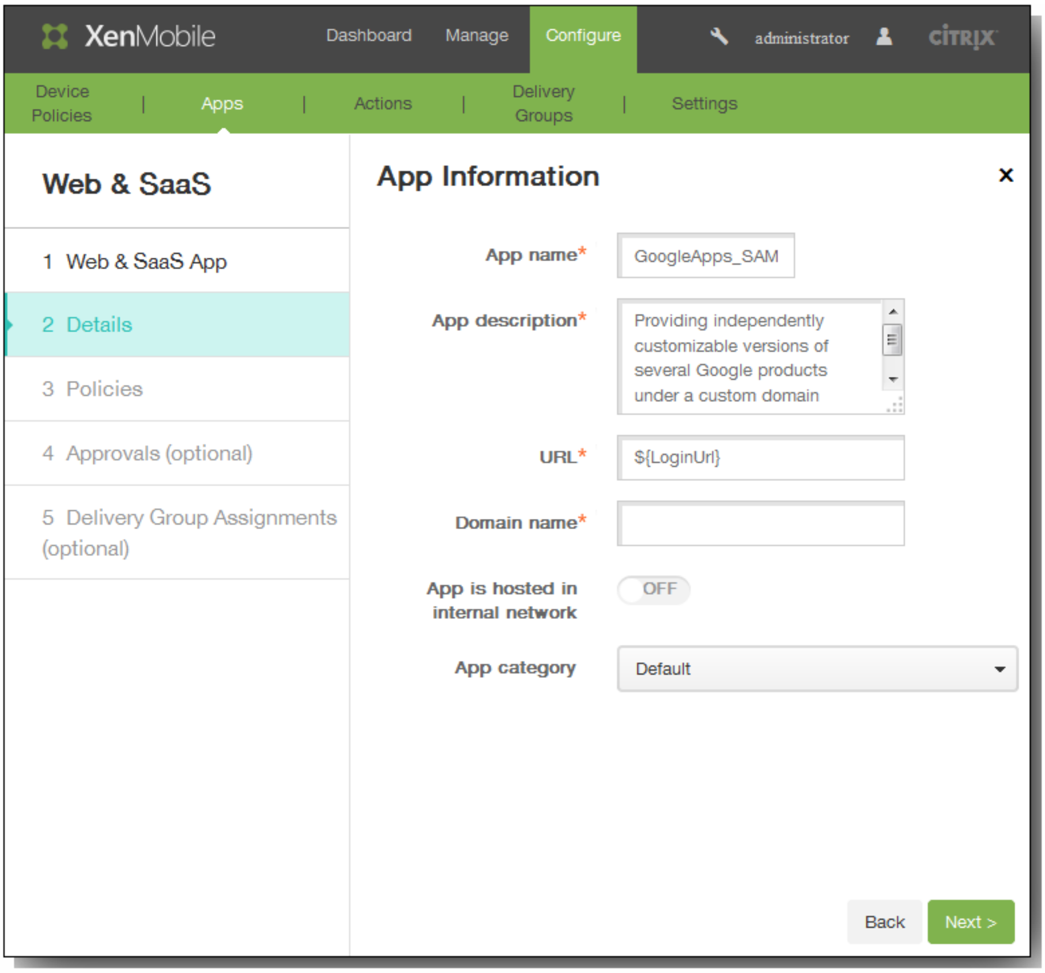
● Choose from existing connectors

○ Create a new connector

App Connectors

Type to search or type an app

E	1
EchoSign_SAML	
G	3
GoogleApps_SAML	
GoogleApps_SAML_IDP	
Globoforce_SAML	
L	1
Lynda_SAML	



Web & SaaS

1 Web & SaaS App

2 Details

3 Policies

4 Approvals (optional)

5 Delivery Group Assignments (optional)

App Information

App name*: GoogleApps_SAM

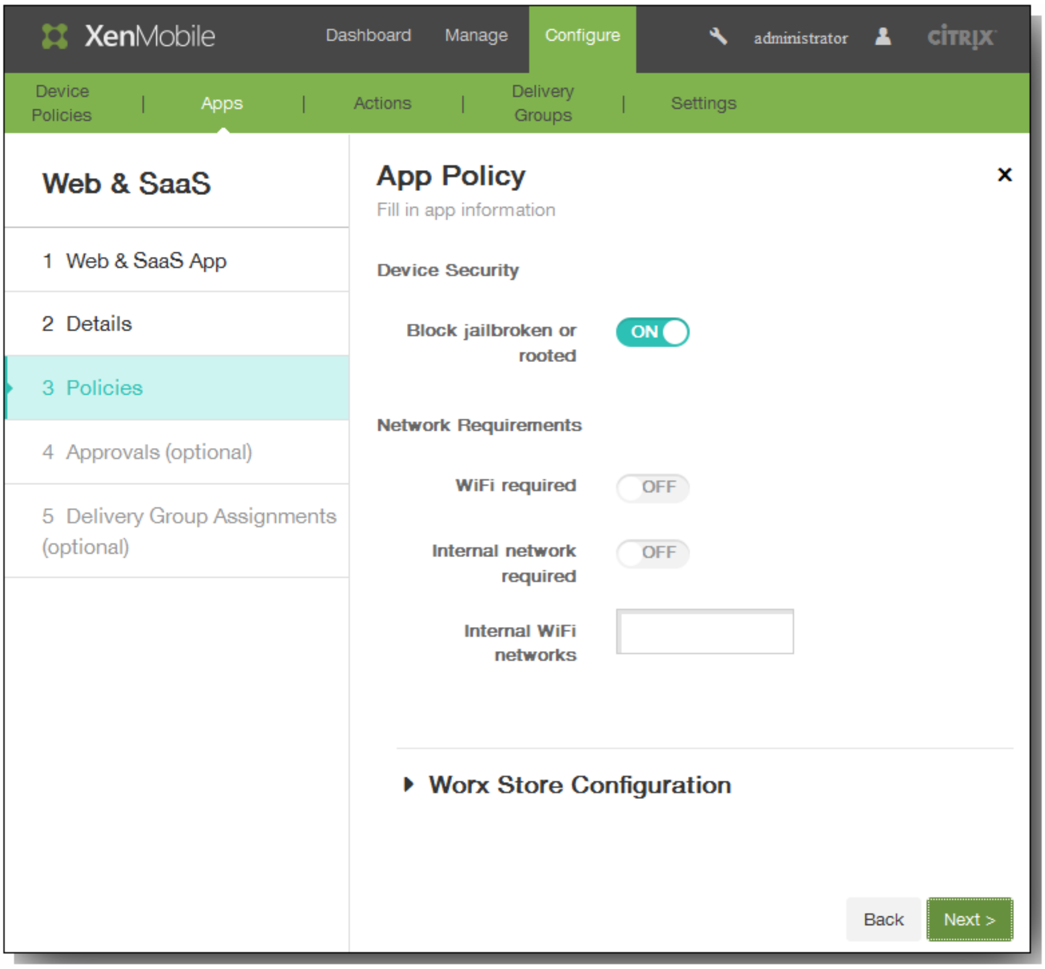
App description*: Providing independently customizable versions of several Google products under a custom domain

URL*: ${LoginUrl}

Domain name*:

App is hosted in internal network: OFF

App category: Default



Web & SaaS

1 Web & SaaS App

2 Details

3 Policies

4 Approvals (optional)

5 Delivery Group Assignments (optional)

App Policy

Fill in app information

Device Security

Block jailbroken or rooted ON

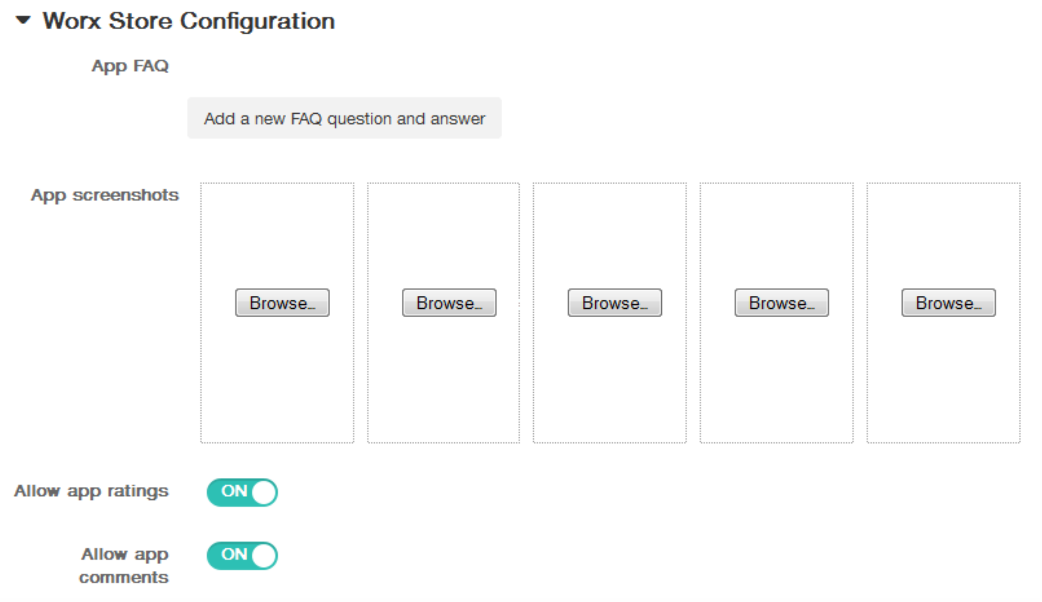
Network Requirements

WiFi required: OFF

Internal network required: OFF

Internal WiFi networks

▸ Worx Store Configuration



Worx Store Configuration

App FAQ

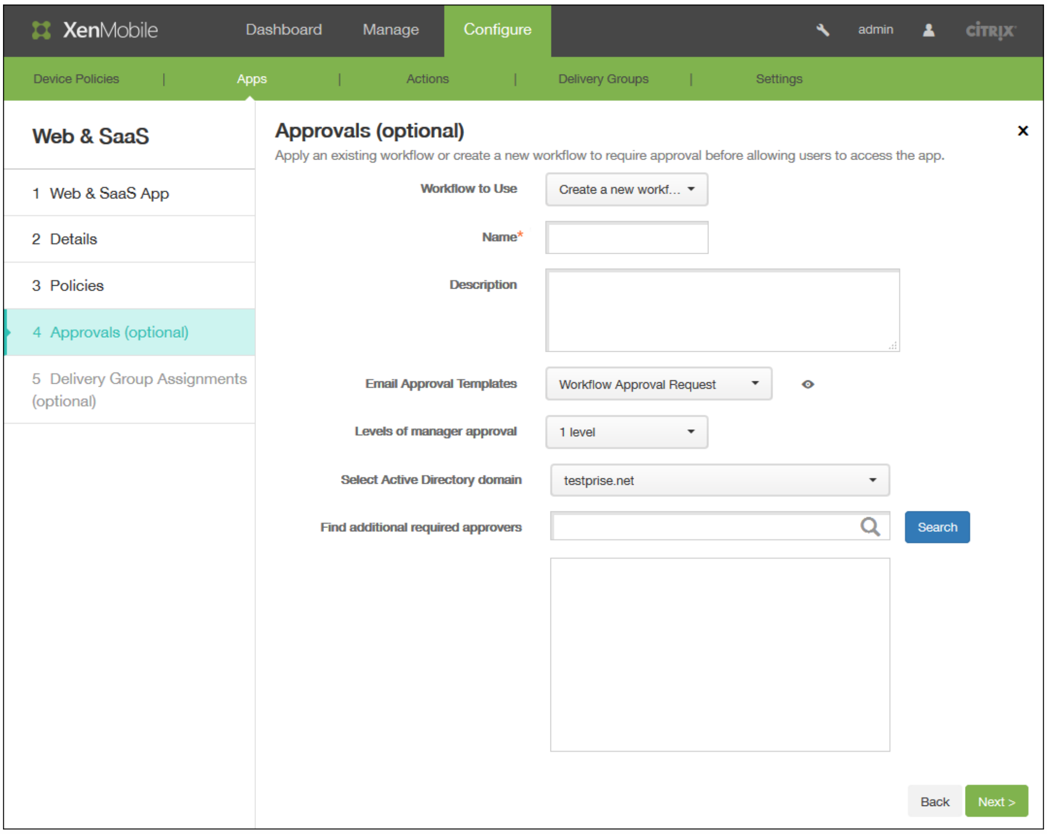
Add a new FAQ question and answer

App screenshots

Browse... Browse... Browse... Browse... Browse...

Allow app ratings: ON

Allow app comments: ON



XenMobile
Dashboard
Manage
Configure
admin
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings

Web & SaaS

1 Web & SaaS App

2 Details

3 Policies

4 Approvals (optional)

5 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 workf...

Name*

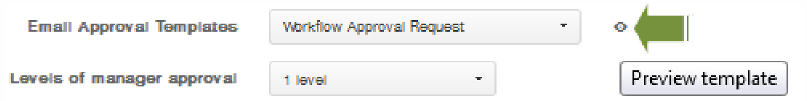
Description

Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level

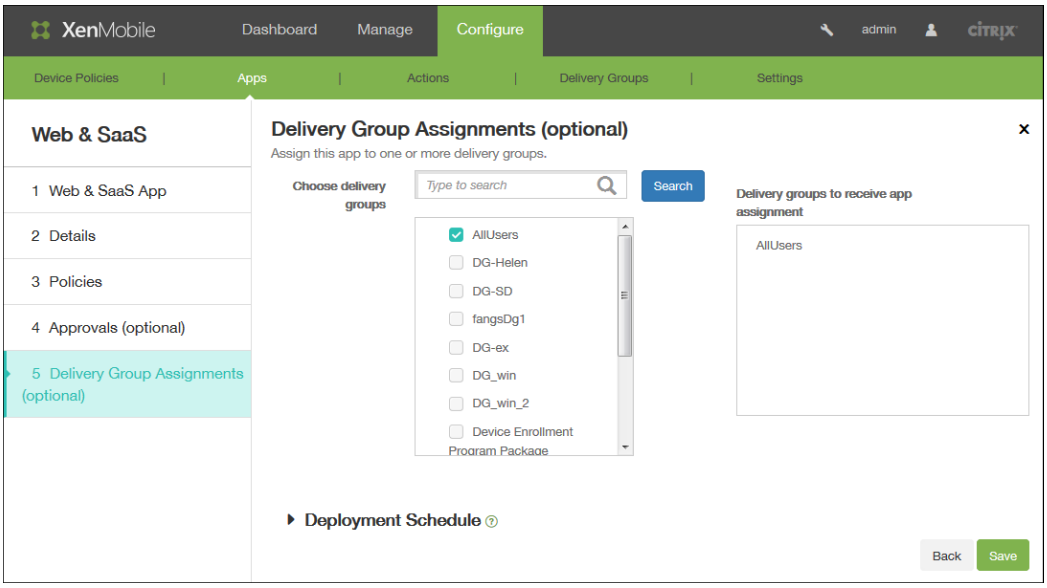
Select Active Directory domain: testprise.net

Find additional required approvers



Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level



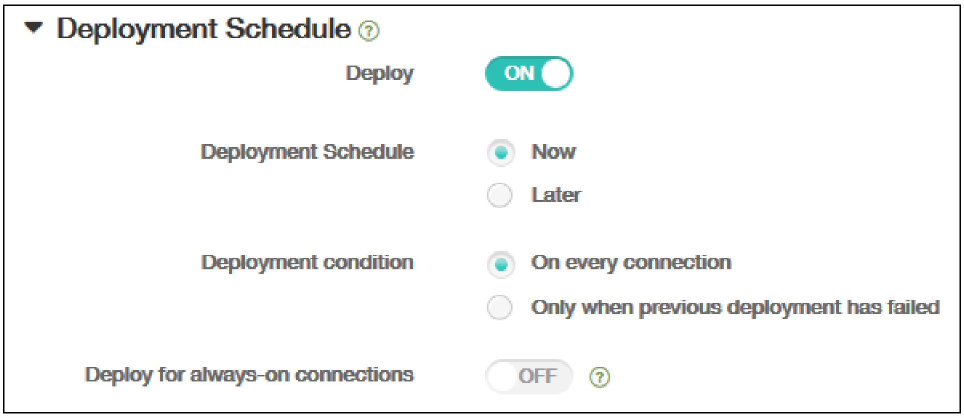
Delivery Group Assignments (optional)

Assign this app to one or more delivery groups.

Choose delivery groups

- ☑ AllUsers
- □ DG-Helen
- □ DG-SD
- □ fangsDg1
- □ DG-ex
- □ DG_win
- □ DG_win_2
- □ Device Enrollment Program Package

Delivery groups to receive app assignment: AllUsers



▾ Deployment Schedule ?

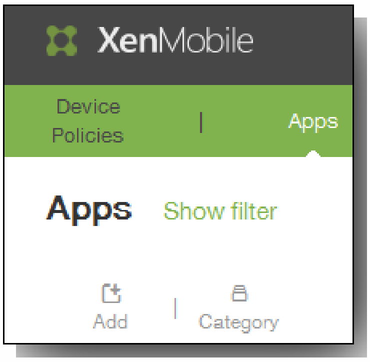
Deploy: ON

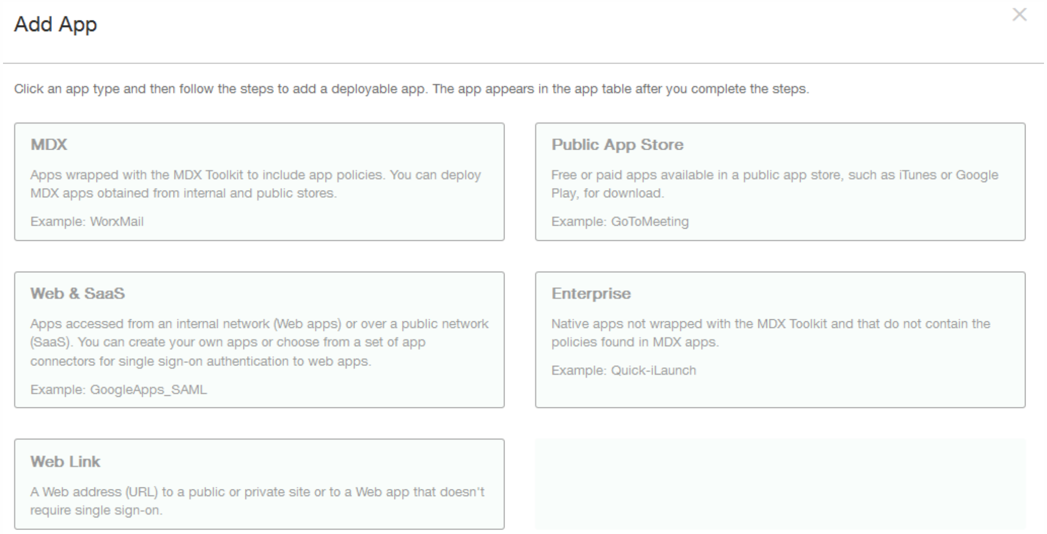
Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF ?

To create an enterprise application




Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

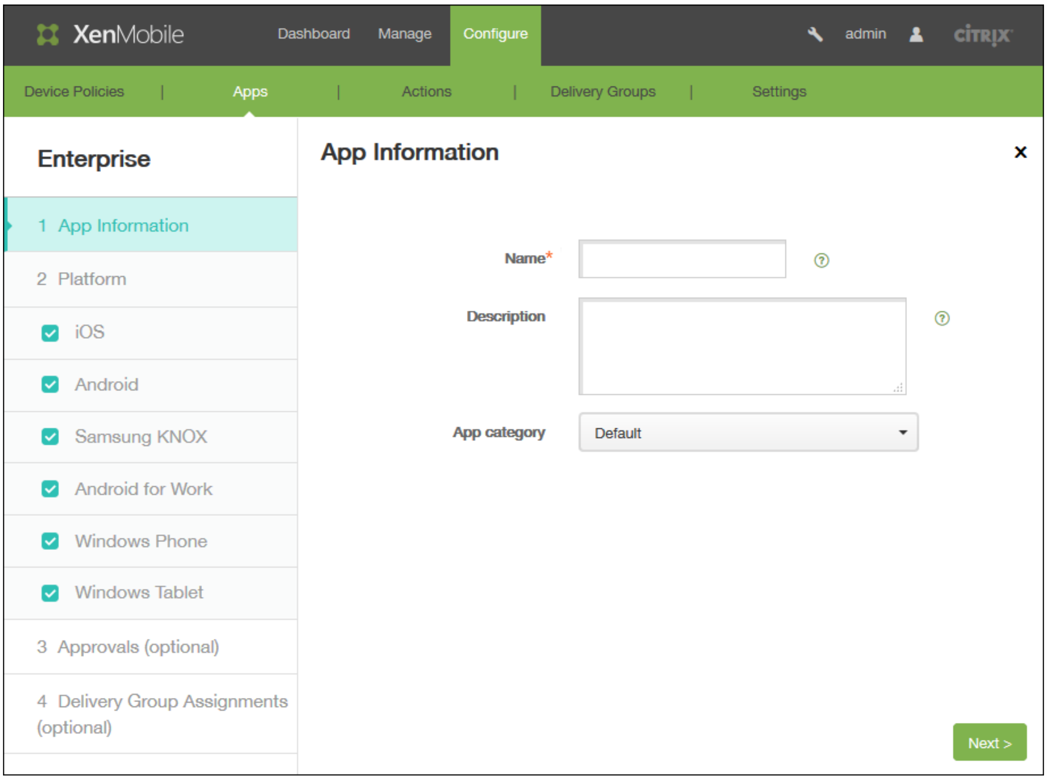
MDX
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

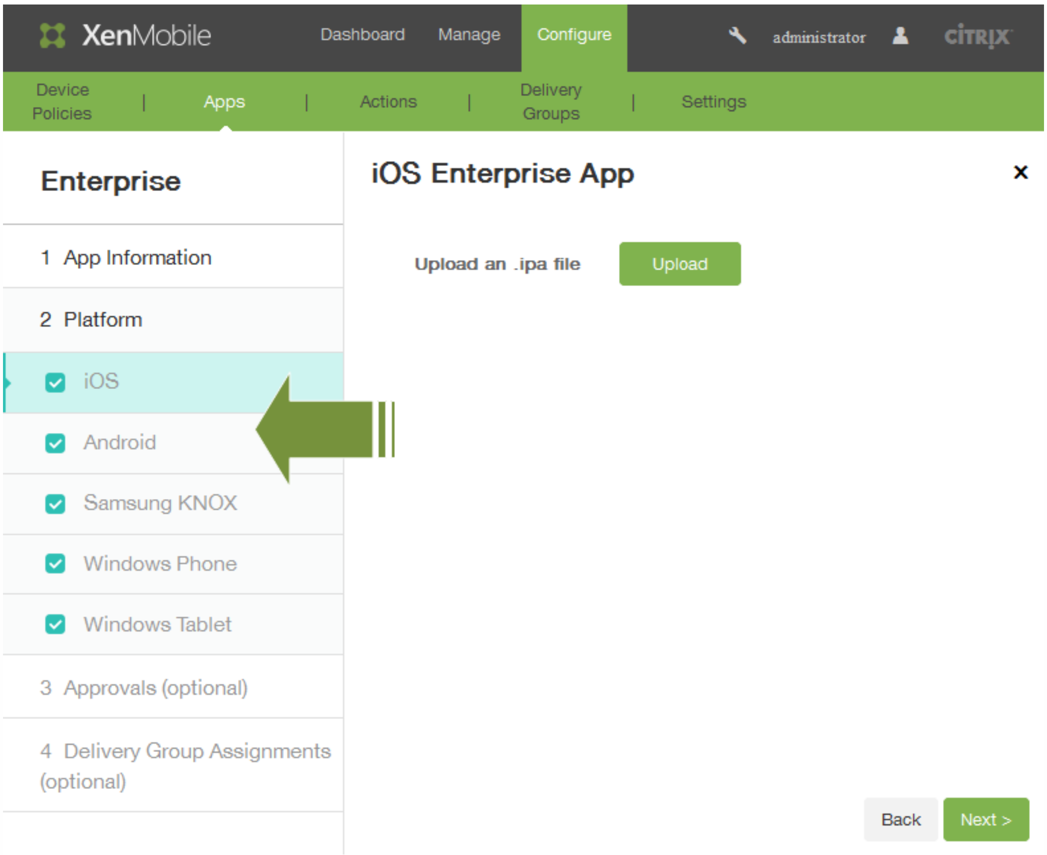
Web & SaaS
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

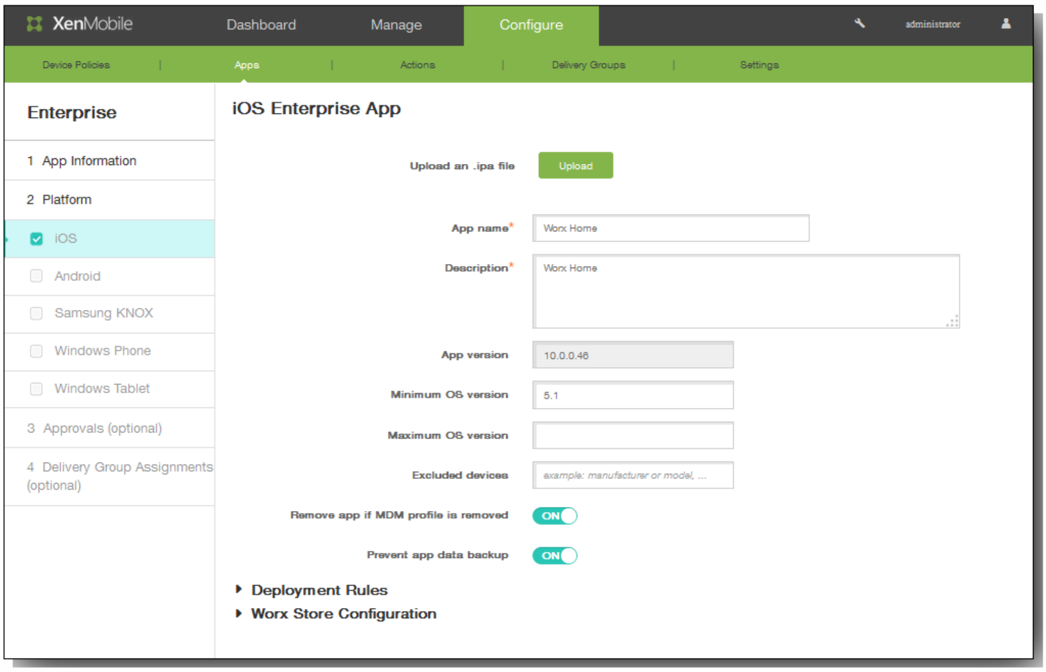
Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.



XenMobile
Dashboard
Manage
Configure
admin
citrix
Device Policies
Apps
Actions
Delivery Groups
Settings
Enterprise
1 App Information
2 Platform
iOS
Android
Samsung KNOX
Android for Work
Windows Phone
Windows Tablet
3 Approvals (optional)
4 Delivery Group Assignments (optional)
App Information
Name*
Description
App category
Default
Next >





App name*: Worx Home

Description*: Worx Home

App version: 10.0.0.46

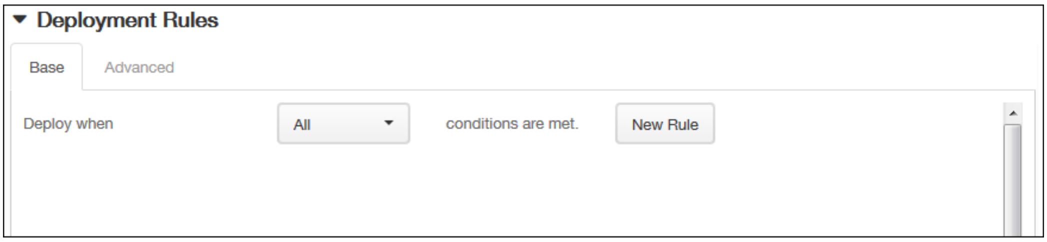
Minimum OS version: 5.1

Maximum OS version:

Excluded devices: example: manufacturer or model, ...

Remove app if MDM profile is removed: ON

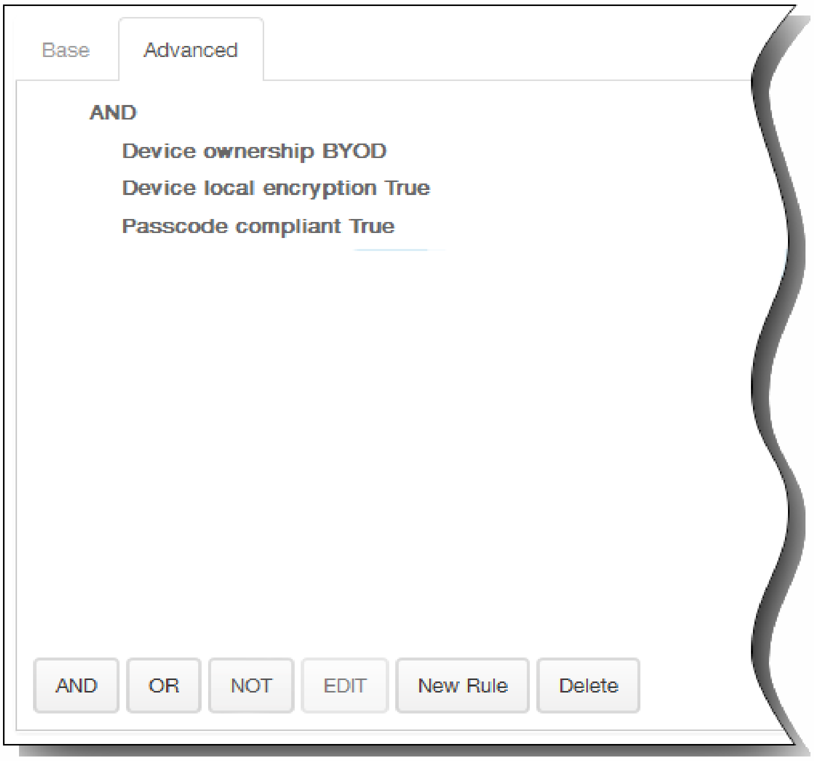
Prevent app data backup: ON



Deployment Rules

Base | Advanced

Deploy when All conditions are met. New Rule

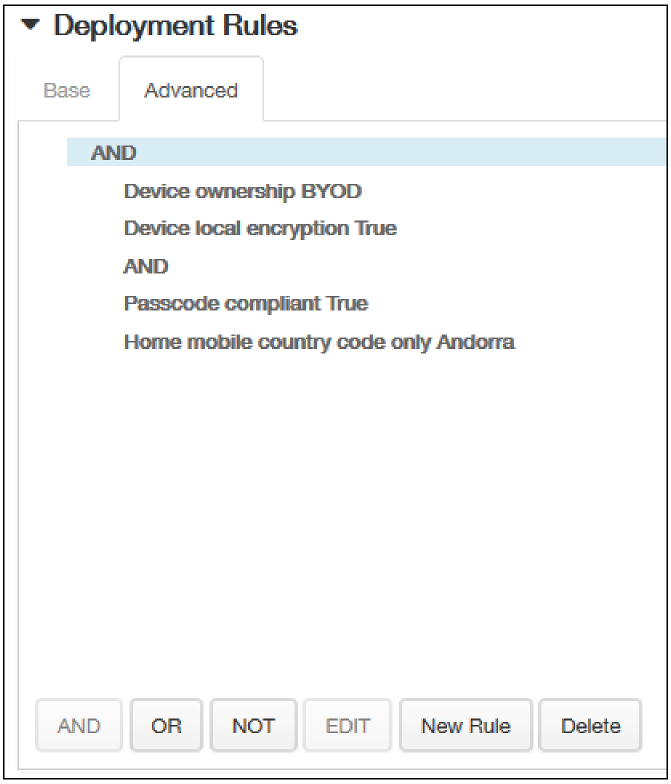


AND

Device ownership BYOD

Device local encryption True

Passcode compliant True



AND

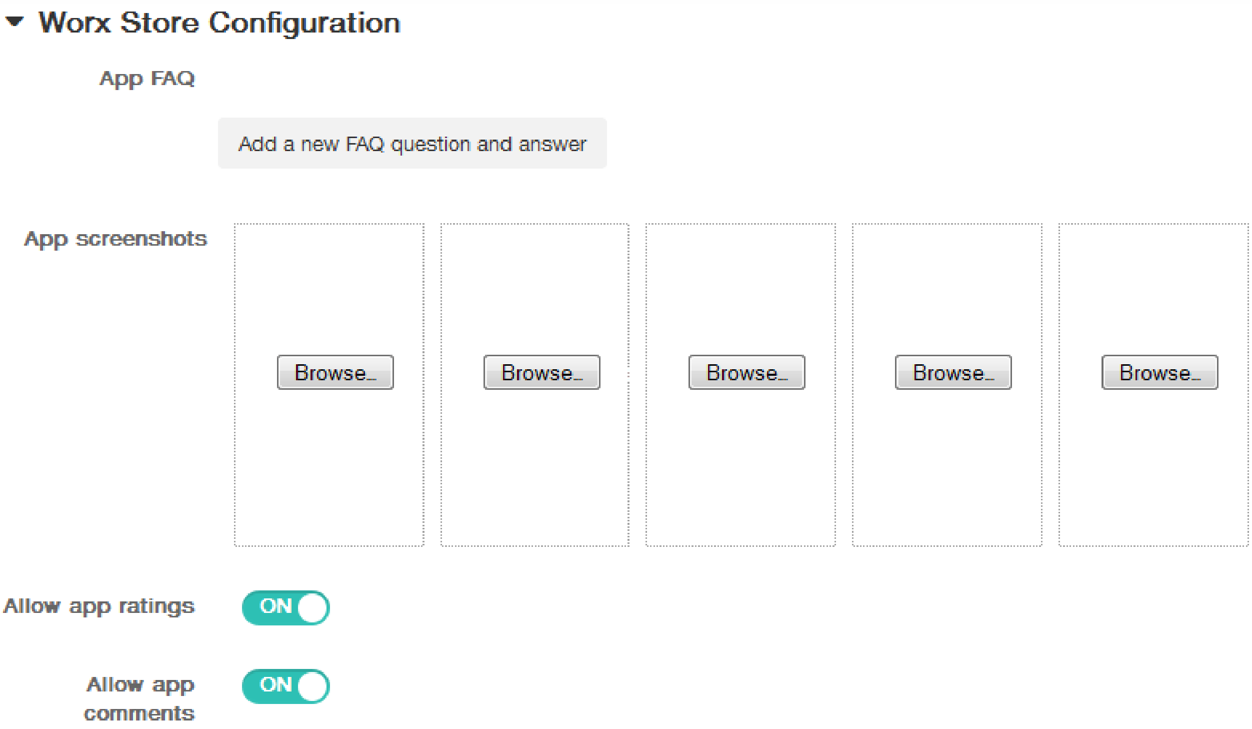
Device ownership BYOD

Device local encryption True

AND

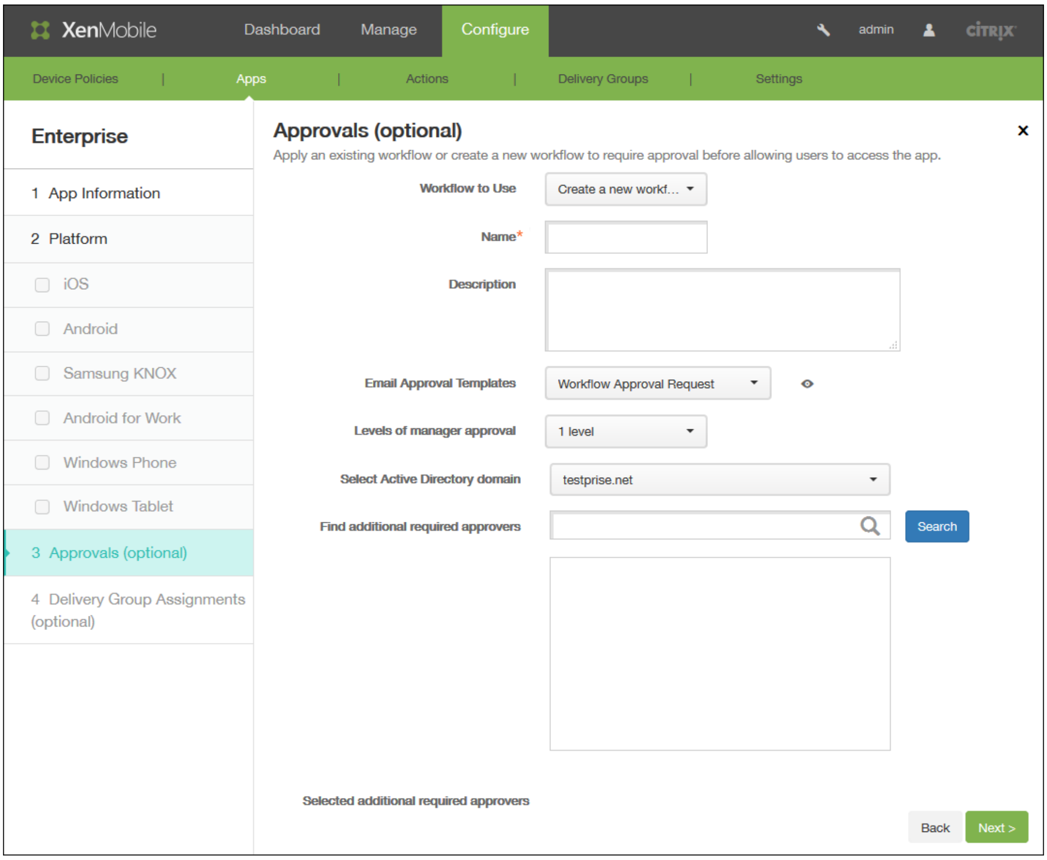
Passcode compliant True

Home mobile country code only Andorra



Allow app ratings: ON

Allow app comments: ON



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 workf...

Name*:

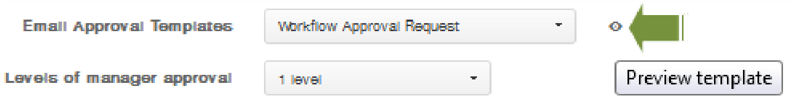
Description:

Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level

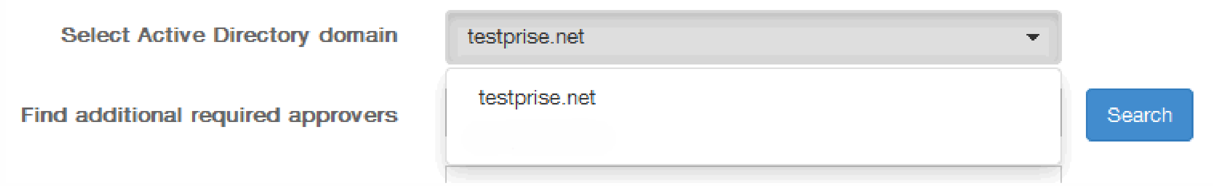
Select Active Directory domain: testprise.net

Find additional required approvers:



Email Approval Templates: Workflow Approval Request

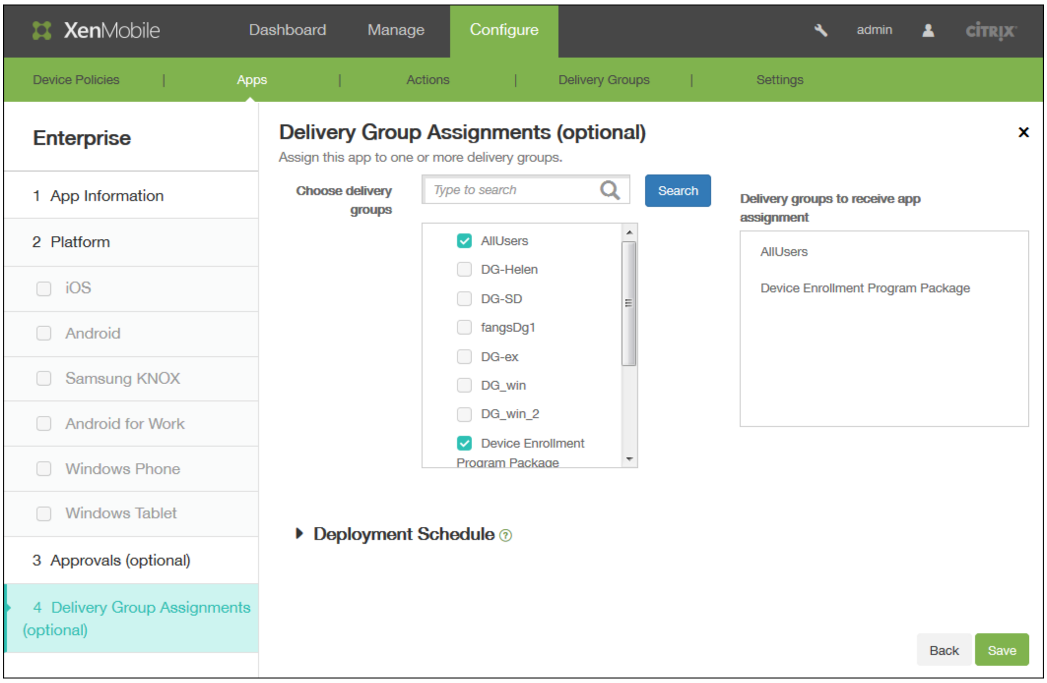
Levels of manager approval: 1 level



Select Active Directory domain: testprise.net

Find additional required approvers

testprise.net



XenMobile
Dashboard
Manage
Configure
admin
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings

Enterprise

1 App Information

2 Platform

- □ iOS
- □ Android
- □ Samsung KNOX
- □ Android for Work
- □ Windows Phone
- □ Windows Tablet

3 Approvals (optional)

4 Delivery Group Assignments (optional)

Delivery Group Assignments (optional)

Assign this app to one or more delivery groups.

Choose delivery groups

- ☑ AllUsers
- □ DG-Helen
- □ DG-SD
- □ fangsDg1
- □ DG-ex
- □ DG_win
- □ DG_win_2
- ☑ Device Enrollment Program Package

Delivery groups to receive app assignment

AllUsers

Device Enrollment Program Package

Deployment Schedule

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).

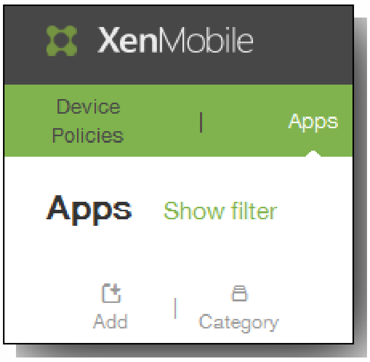
You can configure web links from the Apps tab in the XenMobile console. When you finish configuring the web link, the link appears as an link icon in the list in the Apps table. When users log on with Worx Home, the link appears with the list of available apps and desktops.

To add the link, you provide the following information:

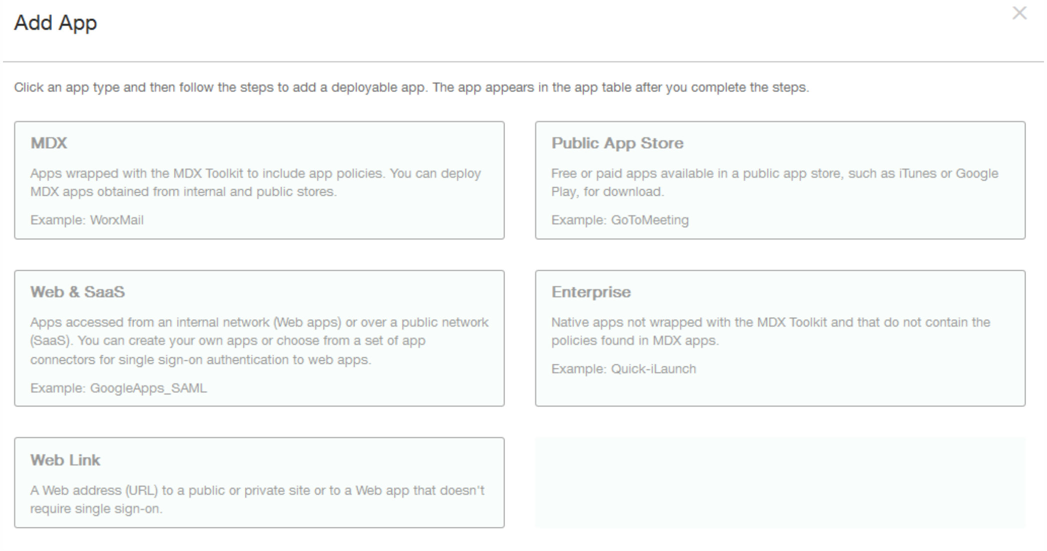
- Name for the link
- Description of the link
- Web address (URL)
- Category
- Role
- Image in .png format (optional)

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.

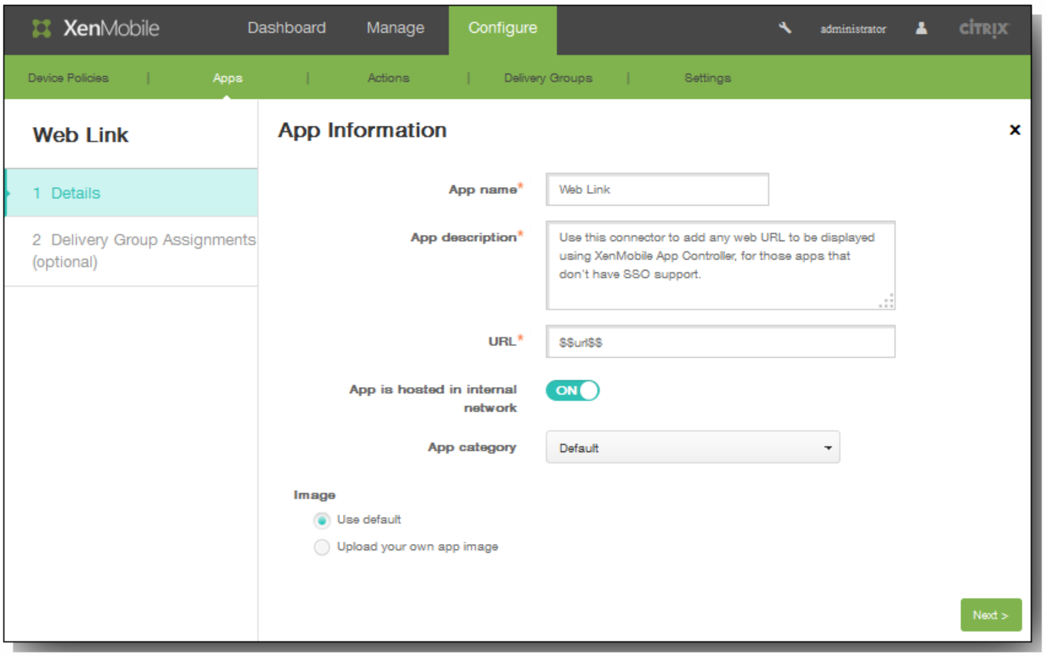
Example: Quick-iLaunch

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.

4. The App name, Description, and URL are pre-populated.



App Information

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

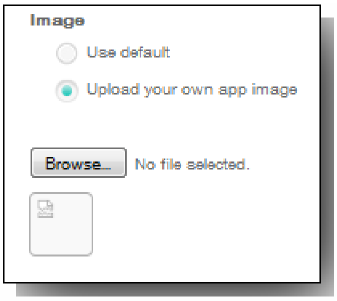
App category Default

Image

● Use default

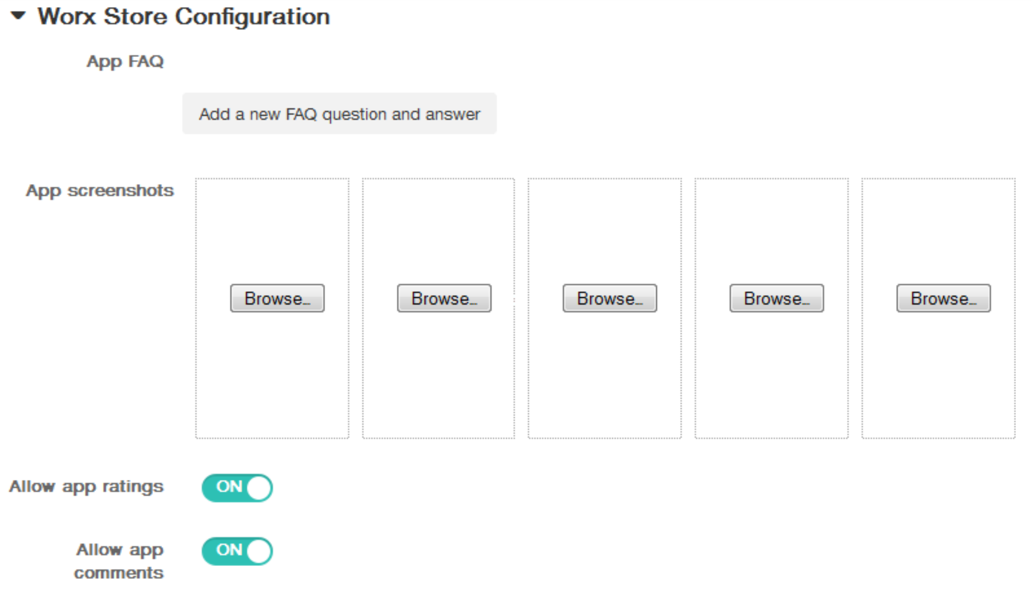
○ Upload your own app image

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. 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:



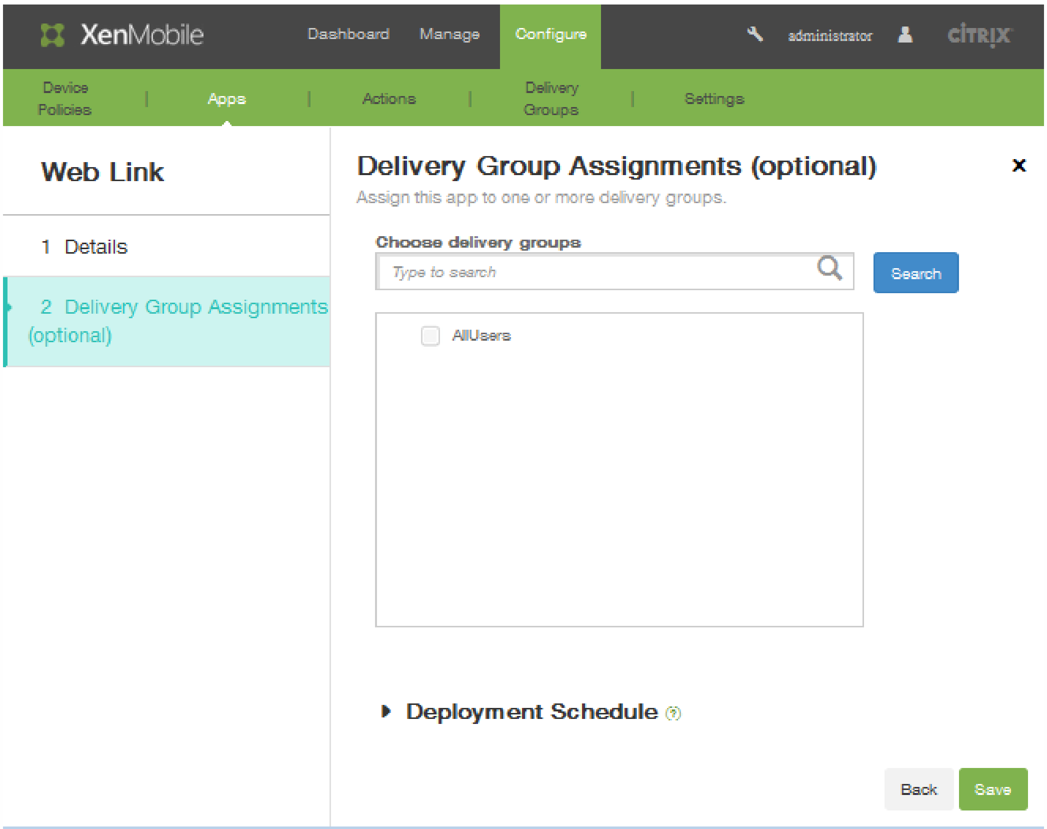
Images must be of the type PNG.

5. 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.



In Allow app ratings, click ON to permit a user to rate the app.

6. In Allow app comments, click ON to permit users to comment about the selected app.
7. Click Next.
8. On the **Delivery Groups Assignment** page, optionally assign the app to one or more delivery groups.



Web Link

1 Details

2 Delivery Group Assignments (optional)

Delivery Group Assignments (optional)

Assign this app to one or more delivery groups.

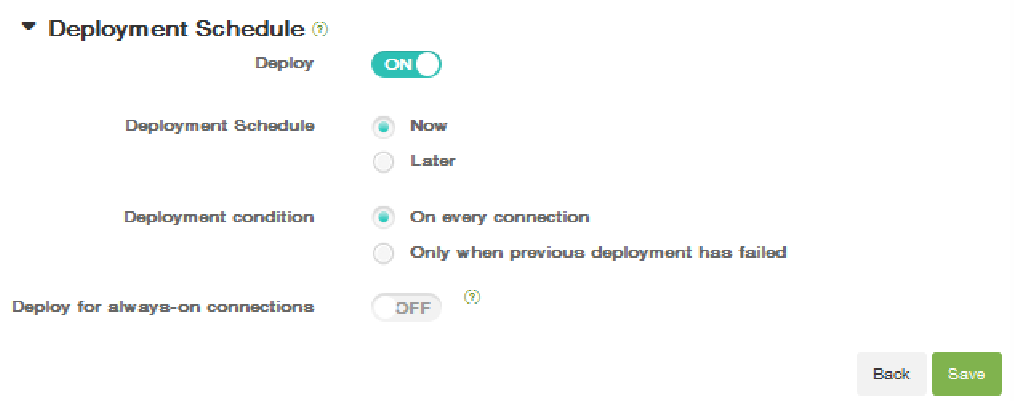
Choose delivery groups

Type to search

□ AllUsers

▸ Deployment Schedule

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.



▾ 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

   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.

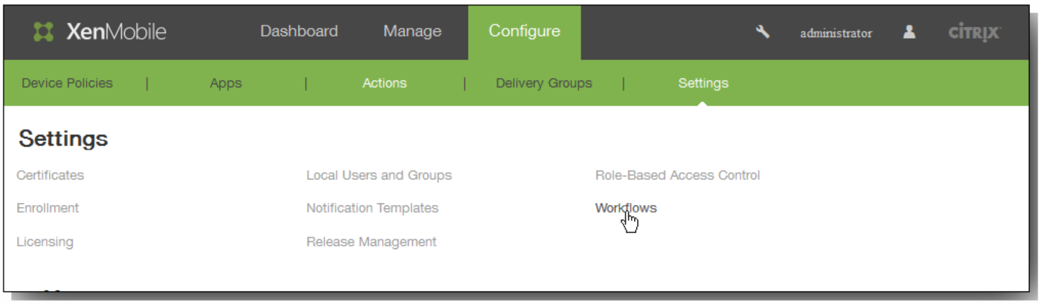
When you configure XenMobile for the first time, you configure workflow email settings. You must configure workflow email settings to use workflows. You can change workflow email settings at any time. These settings include the email server, port, email address, and whether the request to create the user account requires approval or not.

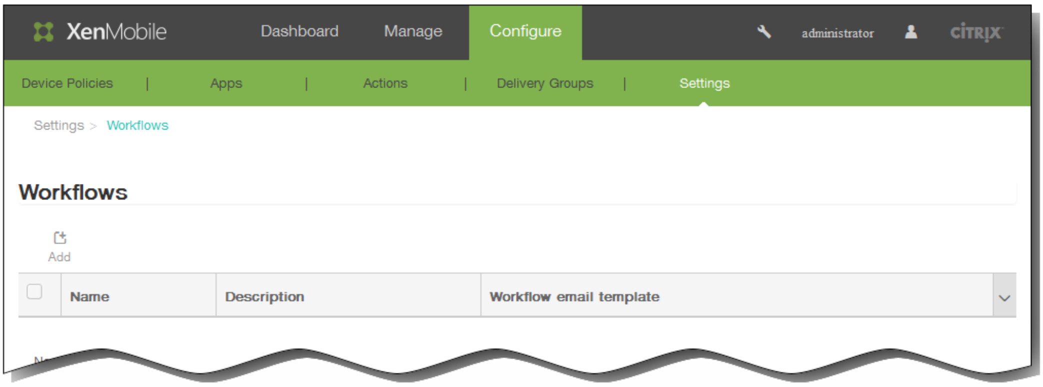
You can configure workflows in two places in XenMobile:

- 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.

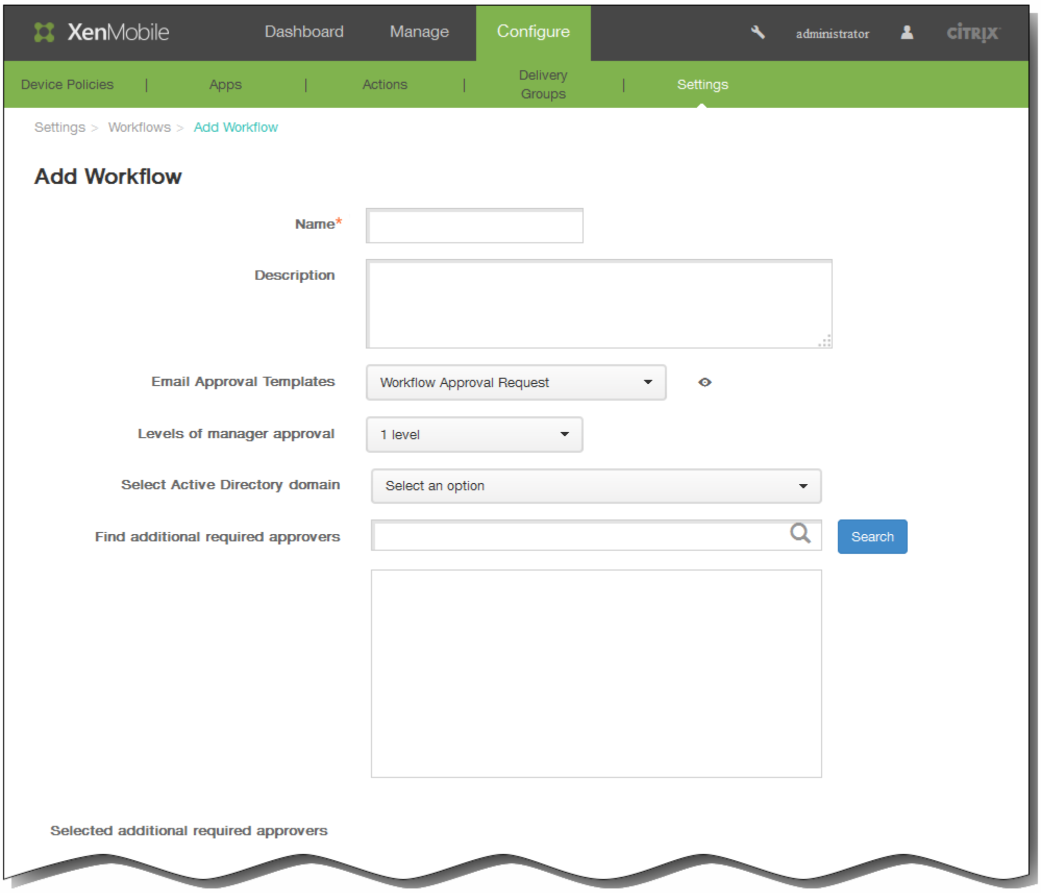
1. In the XenMobile console, click Configure > Settings > Workflows.





The Workflows page appears.

2. On the Workflows page, click Add. The Add Workflow page appears.



Add Workflow

Name*

Description

Email Approval Templates: Workflow Approval Request

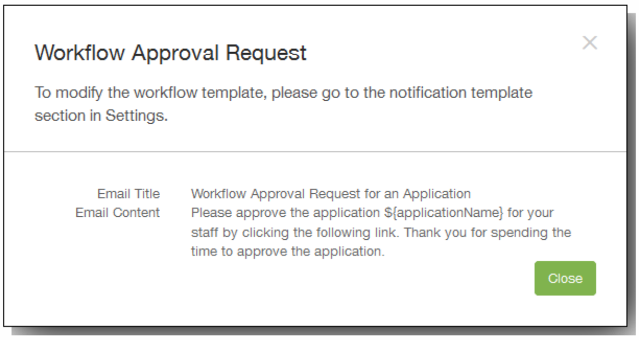
Levels of manager approval: 1 level

Select Active Directory domain: Select an option

Find additional required approvers

Selected additional required approvers

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.



Workflow Approval Request

To modify the workflow template, please go to the notification template section in Settings.

Email Title: Workflow Approval Request for an Application

Email Content: Please approve the application ${applicationName} for your staff by clicking the following link. Thank you for spending the time to approve the application.

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

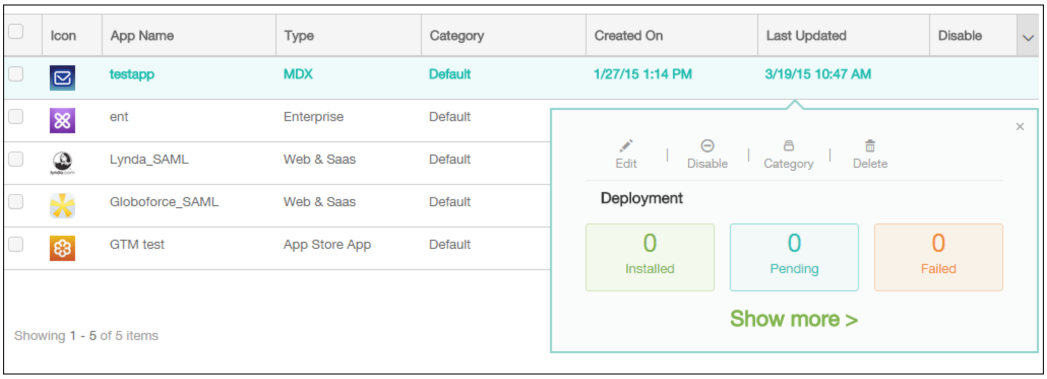
1. On the Workflows page, in the list of existing workflows, select a specific workflow by clicking the row in the table or by checking the check box next to workflow.
2. To delete a workflow, click Delete. A confirmation dialog box appears. Click Delete again.
   Important: You cannot undo this operation.

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.

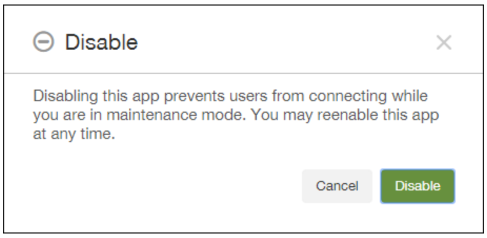
1. In the XenMobile console, click Configure > Apps.
2. For managed devices (devices enrolled in XenMobile for mobile device management), skip to step 3. For unmanaged devices (devices enrolled in XenMobile for enterprise app management purposes only), do the following:
   1. In the Apps table, click to select the app you want to update and then in the menu that appears, click Disable.



□	Icon	App Name	Type	Category	Created On	Last Updated	Disable
□		testapp	MDX	Default	1/27/15 1:14 PM	3/19/15 10:47 AM	
□		ent	Enterprise	Default			
□		Lynda_SAML	Web & Saas	Default			
□		Globoforce_SAML	Web & Saas	Default			
□		GTM test	App Store App	Default			

Showing 1 - 5 of 5 items

   2. On the confirmation dialog box, click Disable.

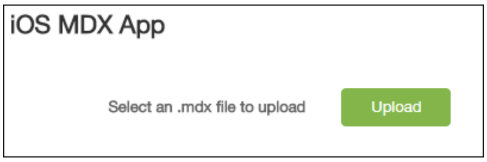


Disable

Disabling this app prevents users from connecting while you are in maintenance mode. You may reenable this app at any time.

   The app shows the status of Disabled in the Apps table.

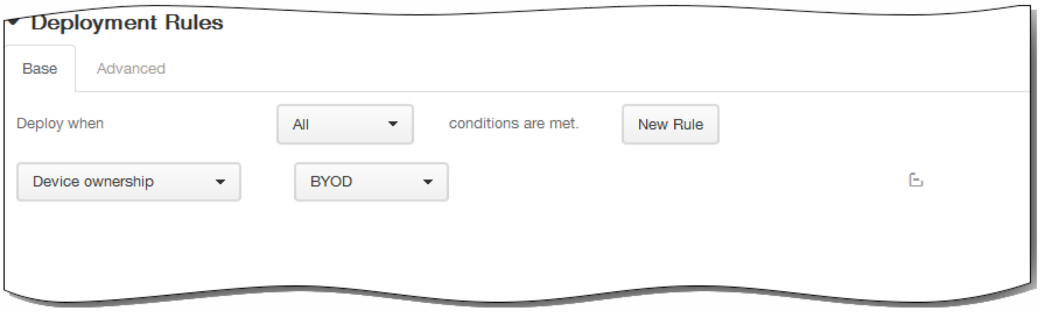
   Note: Disabling an app puts the app in maintenance mode. Users cannot connect to the app again after they log off, while an app is disabled. Disabling an app is an optional setting, but Citrix recommends disabling the app to avoid issues with app functionality. Issue may arise due to policy updates, 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.



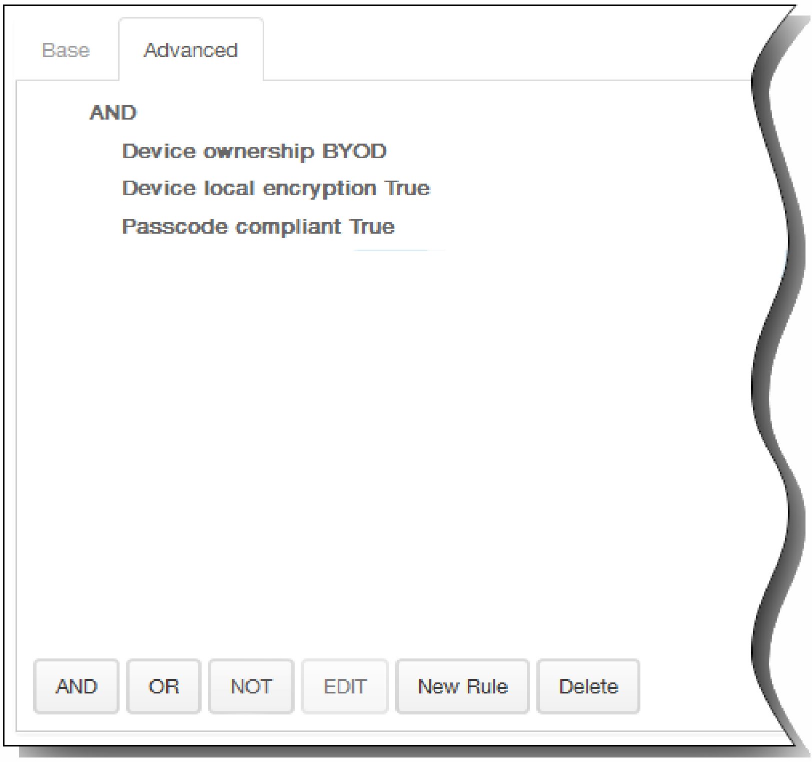
iOS MDX App

Select an .mdx file to upload

   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.



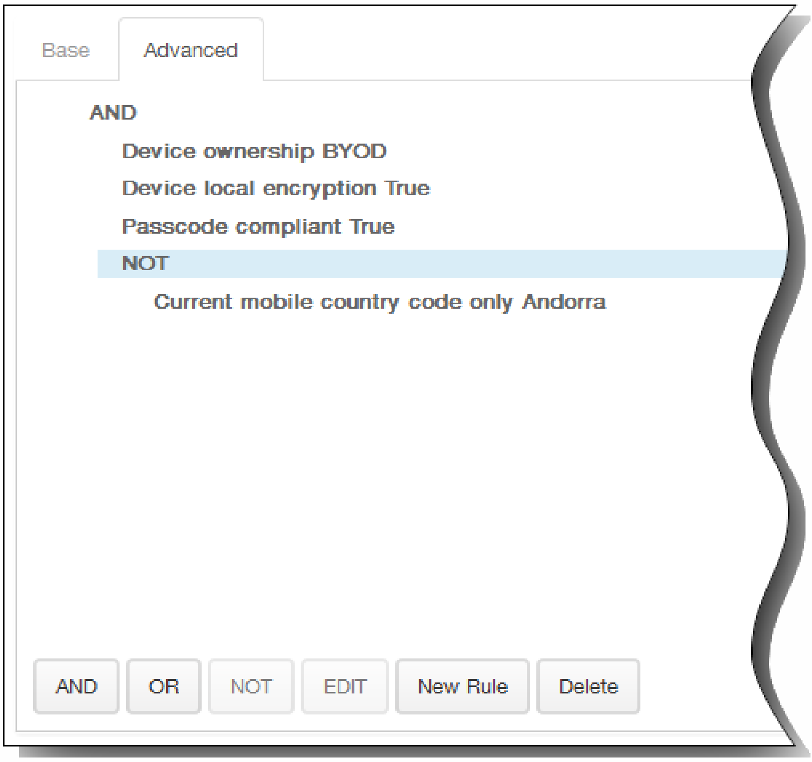
1. In the lists, click options to determine when the app should be deployed.
   1. You can choose to deploy the app when all conditions are met or when any conditions are met. The default option is All.
   2. Click New Rule to define the conditions.
   3. In the lists, click the conditions, such as Device 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

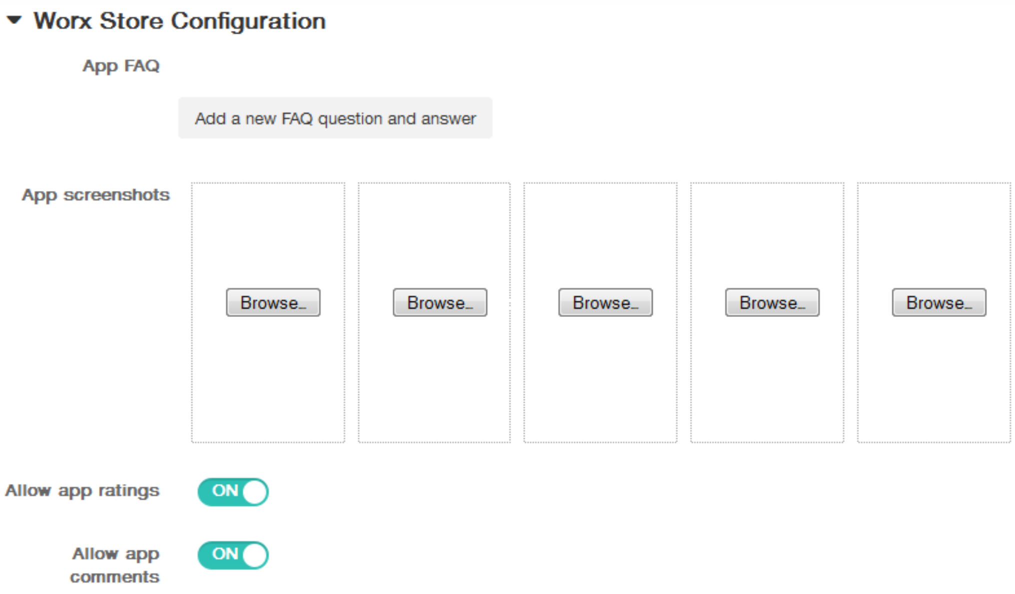
the condition.

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.



AND
- Device ownership BYOD
- Device local encryption True
- Passcode compliant True
- NOT
  - Current mobile country code 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.



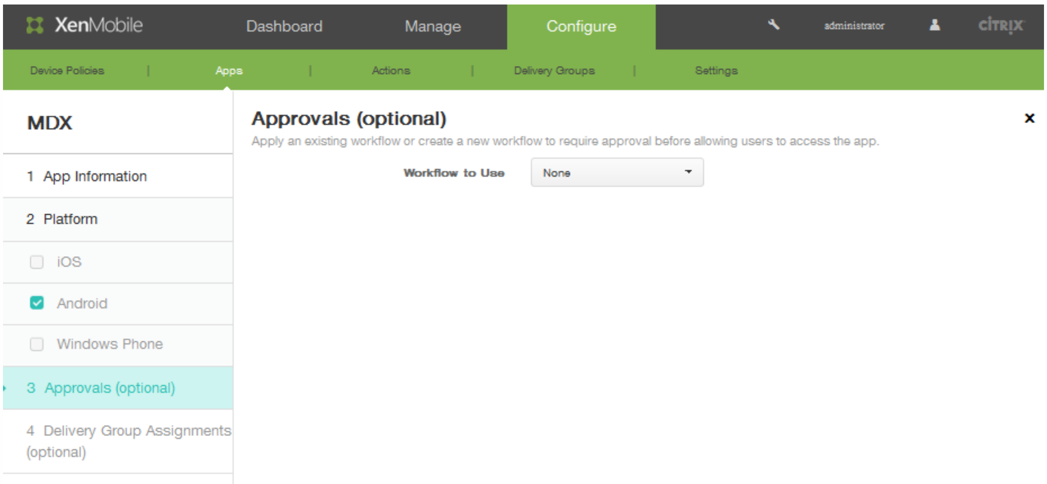
Allow app ratings: ON

Allow app comments: ON

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.

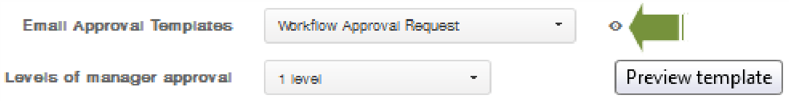


Approvals (optional)

Apply an existing workflow or create a new workflow to require approval before allowing users to access the app.

Workflow to Use: None

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.

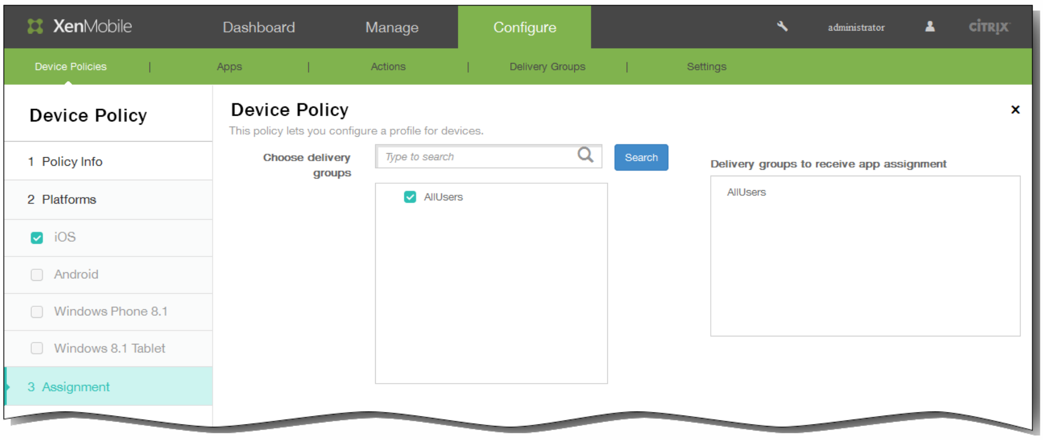


Email Approval Templates: Workflow Approval Request

Levels of manager approval: 1 level

    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.



Device Policy

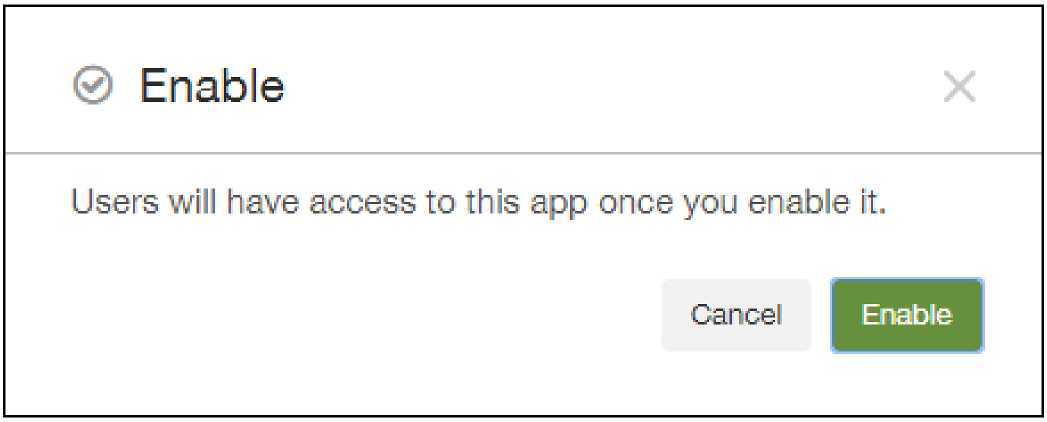
This policy lets you configure a profile for devices.

Choose delivery groups: ☑ AllUsers

Delivery groups to receive app assignment: AllUsers

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.



Enable

Users will have access to this app once you enable it.

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 Worx Home.

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

Aug 15, 2016

You can configure XenMobile and ShareFile to use Security Assertion Markup Language (SAML) to provide single sign-on (SSO) access to ShareFile mobile apps that are wrapped with the MDX toolkit, as well as to non-wrapped ShareFile clients, such as the web site, Outlook plugin, or sync clients.

- **For wrapped ShareFile apps**. Users who log on to ShareFile through the ShareFile mobile app are redirected to Worx Home for user authentication and to acquire a SAML token. After successful authentication, the ShareFile mobile app sends the SAML token to ShareFile. After the initial log on, users can access the ShareFile mobile app through SSO and can attach documents from ShareFile to WorxMail emails without logging on each time.
- **For non-wrapped ShareFile clients**. Users who log on to ShareFile using a web browser or other ShareFile client are redirected to XenMobile for user authentication and to acquire a SAML token. After successful authentication, the SAML token is sent to ShareFile. After the initial log on, users can access ShareFile clients through SSO without logging on each time.

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

Prerequisites

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

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

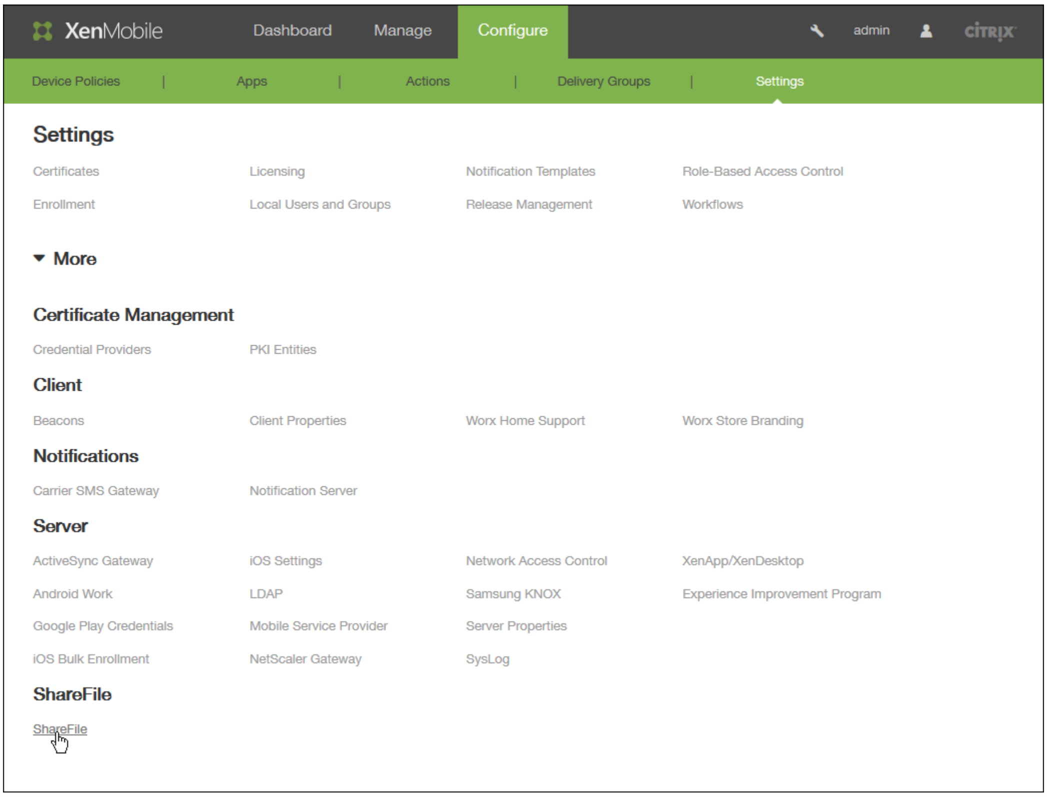
- ShareFile administrator account

Ensure that XenMobile and ShareFile are able to connect. For information about checking connectivity, see Conducting Connectivity Checks.

Configure ShareFile Access

Before configuring SAML for ShareFile, provide ShareFile access information as follows:

1. In the XenMobile web console, click Configure > Settings. The Settings page appears.


XenMobile
Dashboard
Manage
Configure
admin
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings

Settings

Certificates | Licensing | Notification Templates | Role-Based Access Control
Enrollment | Local Users and Groups | Release Management | Workflows

▾ More

Certificate Management

Credential Providers | PKI Entities

Client

Beacons | Client Properties | Worx Home Support | Worx Store Branding

Notifications

Carrier SMS Gateway | Notification Server

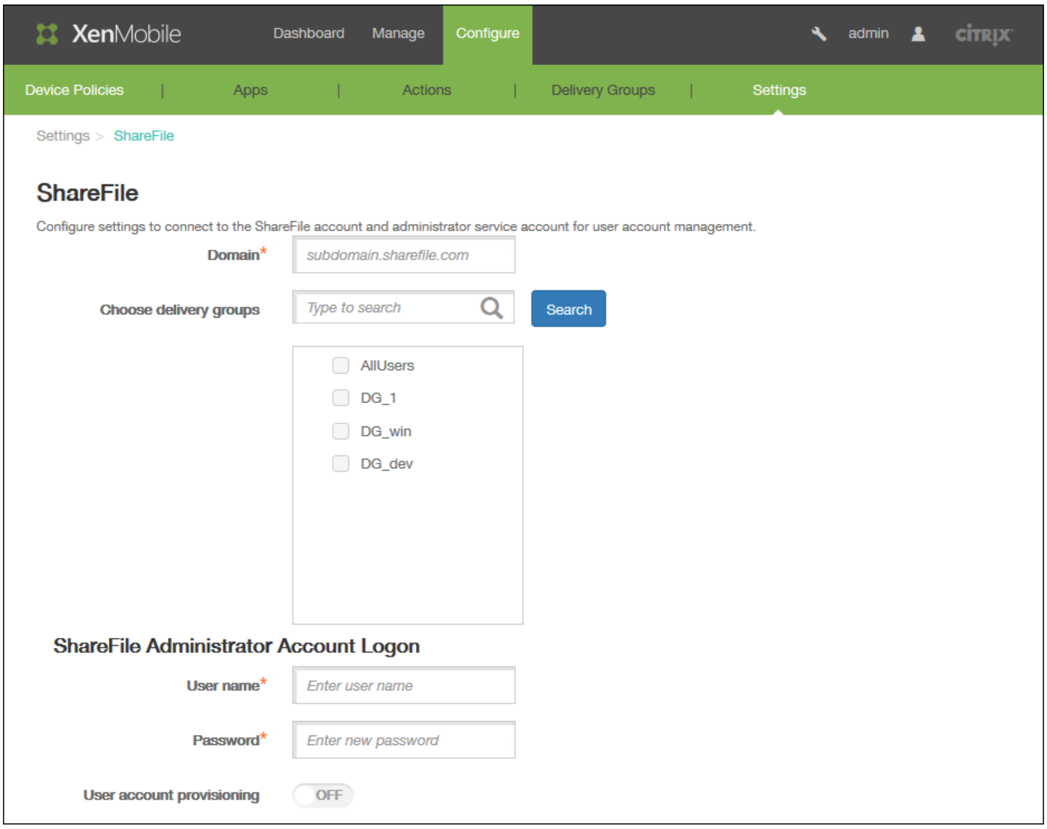
Server

ActiveSync Gateway | iOS Settings | Network Access Control | XenApp/XenDesktop
Android Work | LDAP | Samsung KNOX | Experience Improvement Program
Google Play Credentials | Mobile Service Provider | Server Properties
iOS Bulk Enrollment | NetScaler Gateway | SysLog

ShareFile

ShareFile

2. Click More and then under ShareFile, click ShareFile. The ShareFile configuration page appears.



ShareFile

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

Domain* subdomain.sharefile.com

Choose delivery groups Type to search

□ AllUsers
□ DG_1
□ DG_win
□ DG_dev

ShareFile Administrator Account Logon

User name* Enter user name

Password* Enter new password

User account provisioning OFF

3. Configure the following settings:
   - Domain: Type your ShareFile subdomain name; for example example.sharefile.com.
   - Choose delivery groups: Select or search for the delivery groups that you want to be able to use SSO with ShareFile.
   - User name: Type the ShareFile administrator user name. This user must have administrator privileges.
   - Password: Type the ShareFile administrator password.
   - User account provisioning: Turn on this option if you want to enable user provisioning in XenMobile; leave it disabled if you plan to use the ShareFile User Management Tool for user provisioning.
     Note: If a user without a ShareFile account is included in the selected roles, XenMobile automatically provisions a ShareFile account for that user if you enable User account provisioning. Citrix recommends that you use a role with a small membership for testing the configuration. Doing so avoids the potential of a large number of users without ShareFile accounts.
4. Click Save.

Configure SAML for Wrapped ShareFile MDX Apps

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

1. With the MDX Toolkit, wrap the ShareFile mobile app. For more information about wrapping apps with the MDX Toolkit, see Wrapping Apps with the MDX Toolkit.
2. In XenMobile, upload the wrapped ShareFile mobile app. For information about uploading MDX apps, see To add an MDX app to XenMobile.
3. Verify the SAML settings by logging on to ShareFile with the administrator user name and password you configured in Configure ShareFile Access.
4. Ensure that ShareFile and XenMobile are configured for the same time zone.
   Note: Different time zones can result in mismatched time stamps, leading to SSO failure.

Validate the ShareFile mobile app

1. On the user device, if it has not already been done, install and configure Worx Home.
2. From the Worx Store, download and install the ShareFile mobile app.
3. Start the ShareFile mobile app.
   ShareFile starts without prompting for user name or password.

Validate with WorxMail

1. On the user device, if it has not already been done, install and configure Worx Home.
2. From the Worx Store, download, install, and configure WorxMail.
3. Open a new email form and then tap Attach from ShareFile.
   Files available to attach to the email are shown without asking for user name or password.

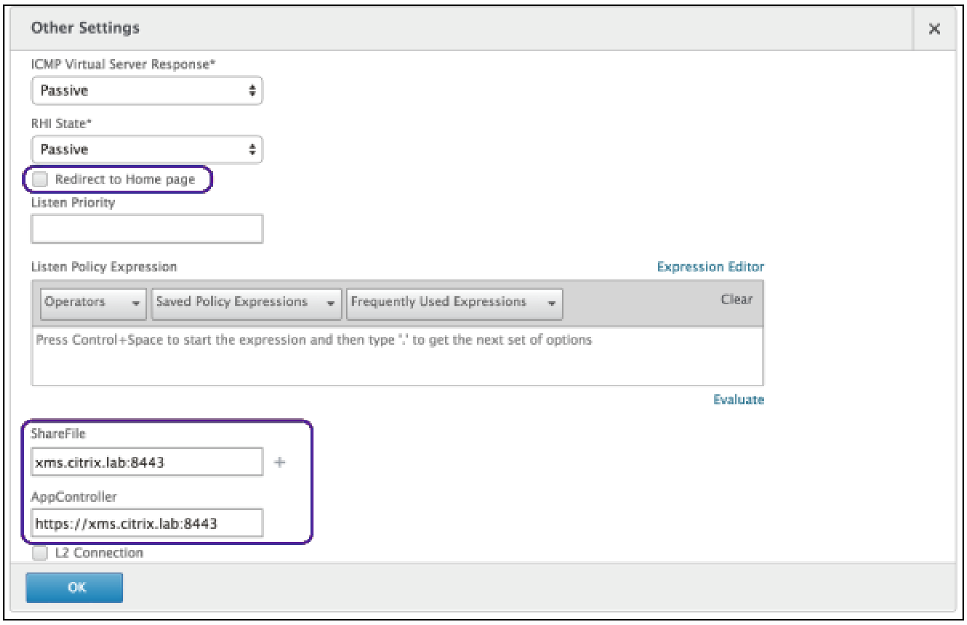
Configure NetScaler Gateway for Other ShareFile Clients

If you want to configure access for non-wrapped ShareFile clients, such as the web site, Outlook plugin, or the sync clients, you must configure NetScaler Gateway to support the use of XenMobile as a SAML identity provider as follows:
- Disable home page redirection.
- Create a ShareFile session policy and profile.
- Configure policies on the NetScaler Gateway virtual server.

Disable home page redirection

You must disable the default behavior for requests that come through the /cginfra path so that the user sees the original requested internal URL instead of the configured home page.

1. Edit the settings for the NetScaler Gateway virtual server that is used for XenMobile logons. In NetScaler 10.5, go to Other Settings and then clear the check box labeled Redirect to Home Page.



ICMP Virtual Server Response*: Passive

RHI State*: Passive

□ Redirect to Home page

Listen Priority

Listen Policy Expression

Press Control+Space to start the expression and then type '.' to get the next set of options

ShareFile: xms.citrix.lab:8443 +

AppController: https://xms.citrix.lab:8443

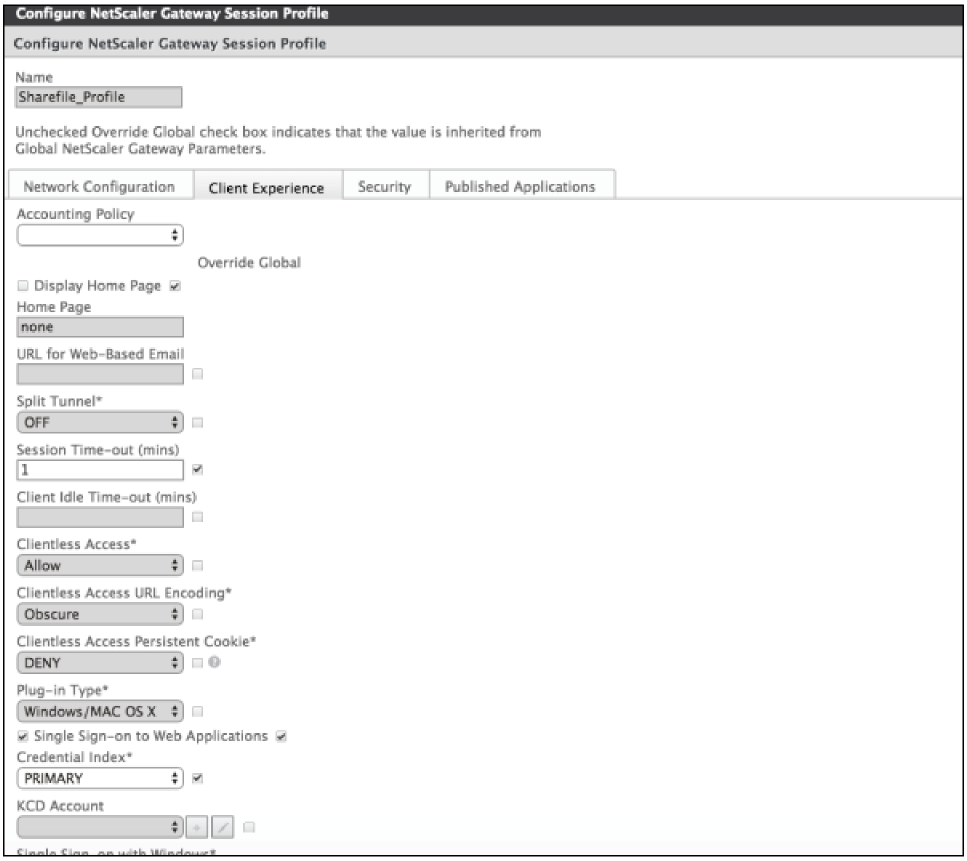
□ L2 Connection

2. Under ShareFile, type your XenMobile internal server name and port number.
3. Under AppController, type your XenMobile URL.
   This configuration authorizes requests to the URL you entered through the /cginfra path.

Create a ShareFile session policy and request profile

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

1. In the NetScaler Gateway configuration utility, in the left-hand navigation pane, click NetScaler Gateway > Policies > Session.
2. Create a new session policy. On the Policies tab, click Add .
3. In the Name field, type ShareFile_Policy.
4. Create a new action by clicking the + button.
   The Create NetScaler Gateway Session Profile screen appears. Configure the following settings:



Configure NetScaler Gateway Session Profile

Configure NetScaler Gateway Session Profile

Name

Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from
Global NetScaler Gateway Parameters.

Accounting Policy

Override Global

□ Display Home Page ☑

Home Page: none □

URL for Web-Based Email □

Split Tunnel*: OFF □

Session Time-out (mins): 1 ☑

Client Idle Time-out (mins) □

Clientless Access*: Allow □

Clientless Access URL Encoding*: Obscure □

Clientless Access Persistent Cookie*: DENY □

Plug-in Type*: Windows/MAC OS X □

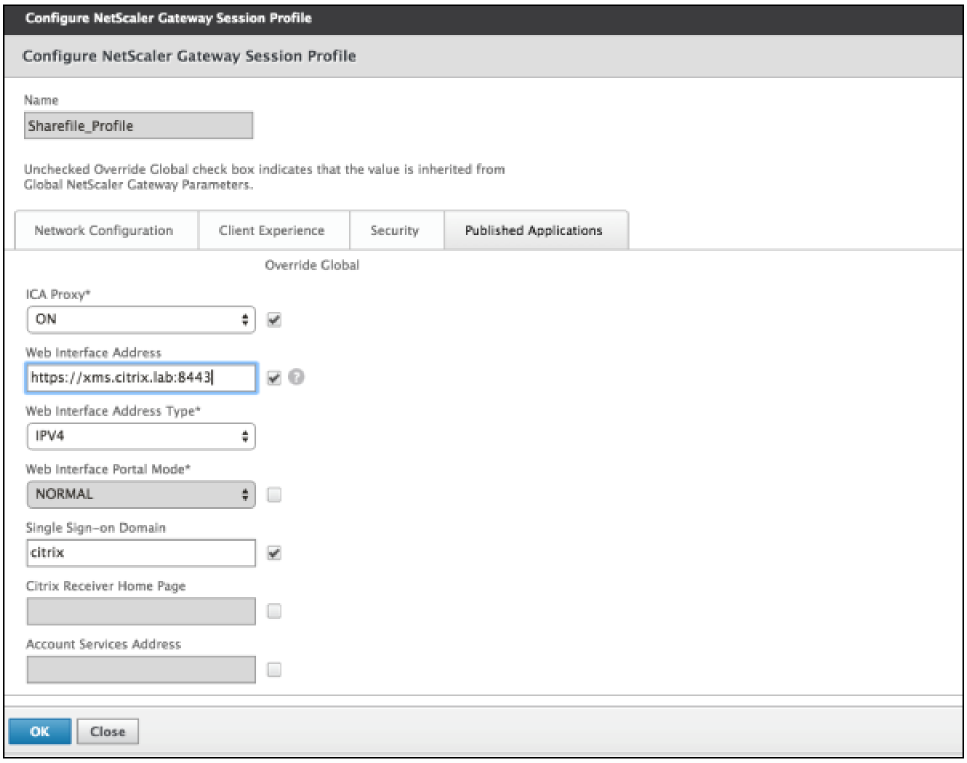
☑ Single Sign-on to Web Applications ☑

Credential Index*: PRIMARY ☑

KCD Account □

Single Sign-on with Windows*

1. Name: Type ShareFile_Profile.
2. Click the Client Experience tab and then configure the following settings:
   1. Home Page: Type none.
   2. Session Time-out (mins): Type 1.
   3. Single Sign-on to Web Applications: Select this setting.
   4. Credential Index: In the list, click PRIMARY.
3. Click the Published Applications tab and then configure the following settings:



Configure NetScaler Gateway Session Profile

Configure NetScaler Gateway Session Profile

Name

Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

ICA Proxy*: ON ☑

Web Interface Address: https://xms.citrix.lab:8443 ☑

Web Interface Address Type*: IPV4

Web Interface Portal Mode*: NORMAL □

Single Sign-on Domain: citrix ☑

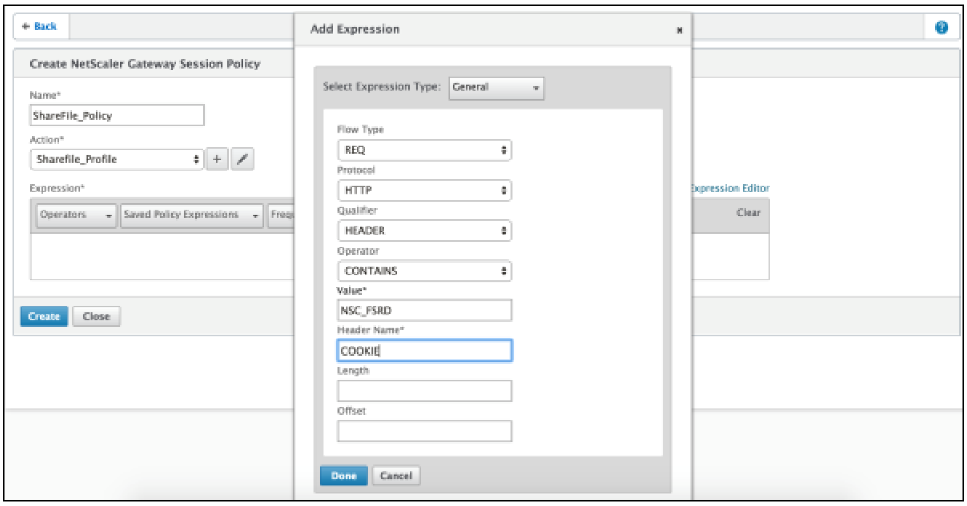
Citrix Receiver Home Page: □

Account Services Address: □

1. ICA Proxy: In the list, select ON.
2. Web Interface Address: Type your XenMobile server URL.
3. Single Sign-on Domain: Type your Active Directory domain name.

   Note: When configuring the NetScaler Gateway Session Profile, the domain suffix for Single Sign-on Domain must match the XenMobile domain alias defined in LDAP.

5. Click Create to define the session profile.
6. Click Expression Editor and then configure the following settings:



Name*: ShareFile_Policy

Action*: Sharefile_Profile

Select Expression Type: General

Flow Type: REQ

Protocol: HTTP

Qualifier: HEADER

Operator: CONTAINS

Value*: NSC_FSRD

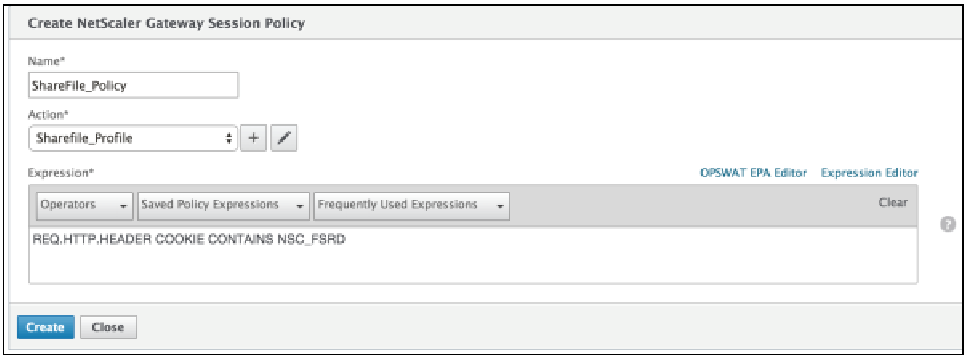
Header Name*: COOKIE

Length:

Offset:

1. Value: Type NSC_FSRD.
2. Header Name: Type COOKIE.
3. Click Done.

7. Click Create and then click Close.



Create NetScaler Gateway Session Policy

Name*: ShareFile_Policy

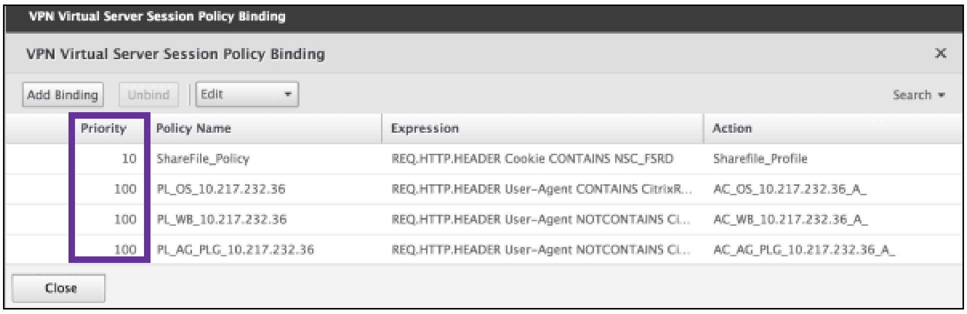
Action*: Sharefile_Profile

Expression*: REQ.HTTP.HEADER COOKIE CONTAINS NSC_FSRD

Configure policies on the NetScaler Gateway virtual server

Configure the following settings on the NetScaler Gateway virtual server.

1. In the NetScaler Gateway configuration utility, in the left-hand navigation pane, click NetScaler Gateway > Virtual Servers.
2. In the Details pane, click your NetScaler Gateway virtual server.
3. Click Edit.
4. Click Configured policies > Session policies and then click Add binding.
5. Select ShareFile_Policy.
6. Edit the auto-generated Priority number for the selected policy so that it has the highest priority (the smallest number) in relation to any other policies listed, as shown in the following figure.



VPN Virtual Server Session Policy Binding

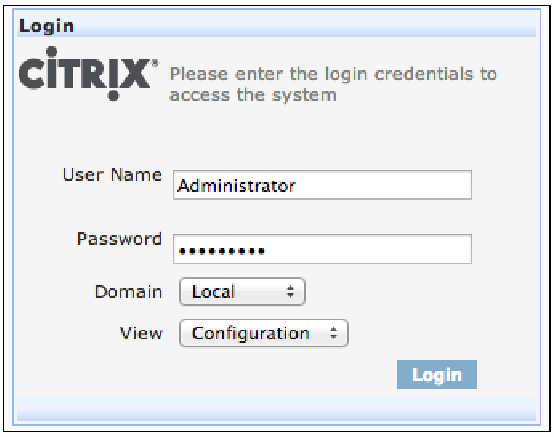
Priority	Policy Name	Expression	Action
10	ShareFile_Policy	REQ.HTTP.HEADER Cookie CONTAINS NSC_FSRD	Sharefile_Profile
100	PL_OS_10.217.232.36	REQ.HTTP.HEADER User-Agent CONTAINS CitrixR...	AC_OS_10.217.232.36_A_
100	PL_WB_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Ci...	AC_WB_10.217.232.36_A_
100	PL_AG_PLG_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Ci...	AC_AG_PLG_10.217.232.36_A_

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

Configure SAML for non-MDX ShareFile apps

Use the following steps to find the internal app name for your ShareFile configuration.

1. Log on to the XenMobile admin tool using the URL https://<XenMobile server>:4443/OCA/admin/. Be sure to enter "OCA" in uppercase letters.
2. In the View list, click Configuration.



Login

Please enter the login credentials to access the system

User Name: Administrator

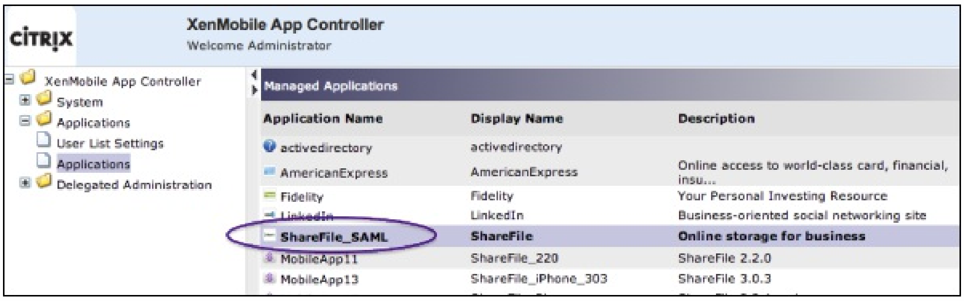
Password: •••••••••

Domain: Local

View: Configuration

Login

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



XenMobile App Controller
Welcome Administrator

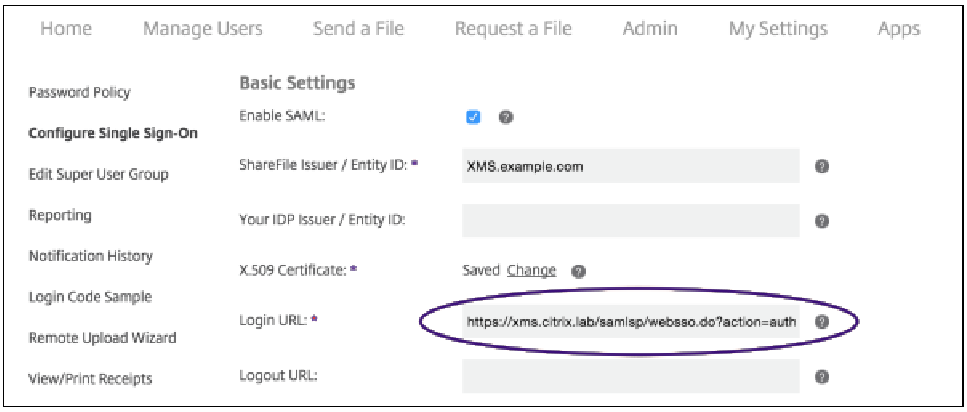
- XenMobile App Controller
  - System
  - Applications
    - User List Settings
    - Applications
  - Delegated Administration

Managed Applications

Application Name	Display Name	Description
activedirectory	activedirectory	
AmericanExpress	AmericanExpress	Online access to world-class card, financial, insu...
Fidelity	Fidelity	Your Personal Investing Resource
LinkedIn	LinkedIn	Business-oriented social networking site
ShareFile_SAML	**ShareFile**	**Online storage for business**
MobileApp11	ShareFile_220	ShareFile 2.2.0
MobileApp13	ShareFile_iPhone_303	ShareFile 3.0.3

Modify the ShareFile.com SSO settings

1. Log on to your ShareFIle account (https://<subdomain>.sharefile.com) as a ShareFile administrator.
2. In the ShareFile web interface, click Admin and then select Configure Single Sign-on.
3. Edit the Login URL as follows:
   The Login URL should look similar to: https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.



Home | Manage Users | Send a File | Request a File | Admin | My Settings | Apps

- Password Policy
- **Configure Single Sign-On**
- Edit Super User Group
- Reporting
- Notification History
- Login Code Sample
- Remote Upload Wizard
- View/Print Receipts

Basic Settings

Enable SAML: ☑

ShareFile Issuer / Entity ID: * XMS.example.com

Your IDP Issuer / Entity ID:

X.509 Certificate: * Saved Change

Login URL: * https://xms.citrix.lab/samlsp/websso.do?action=auth

Logout URL:

1. Insert the NetScaler Gateway virtual server external FQDN plus "/cginfra/https/" in front of the XenMobile server FQDN and then add "8443" after the XenMobile FQDN.

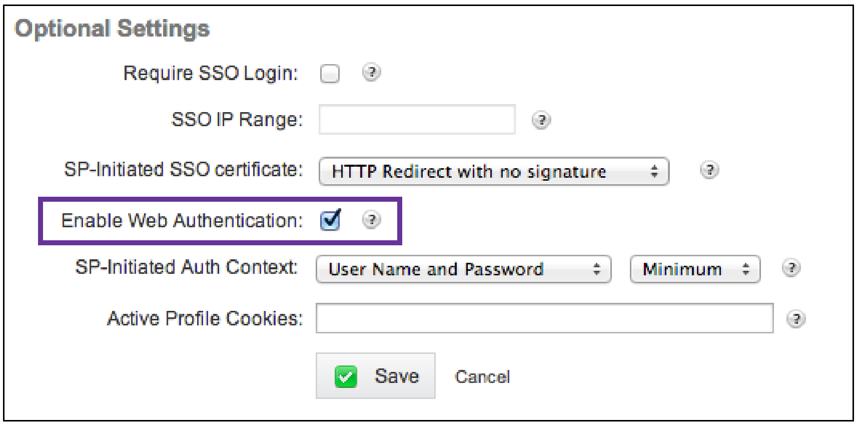
The URL should now look similar to this:
https://**nsgateway.acme.com/cginfra/https**/xms.citrix.lab:**8443**/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1

2. Change the parameter **&app=ShareFile_SAML_SP** to the internal ShareFile application name from step 3 in Configure SAML for non-MDX ShareFile apps. The internal name is **ShareFile_SAML** by default; however, every time you change your configuration, a number is appended to the internal name (ShareFile_SAML_2, ShareFile_SAML_3, and so on).
   The URL should now look similar to this:
   https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**&app=ShareFile_SAML**&reqtype=1

3. Add "&nssso=true" to the end of the URL.
   The modified URL should now look similar to:
   https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**.

   Important: Each time you edit or recreate the ShareFIle app or change the ShareFile settings in the XenMobile console, a new number is appended the internal application name, which means you must also update the Login URL in the ShareFile web site to reflect the updated app name.

4. Under Optional Settings, select the Enable Web Authentication check box.



Optional Settings

Require SSO Login: □

SSO IP Range:

SP-Initiated SSO certificate: HTTP Redirect with no signature

Enable Web Authentication: ☑

SP-Initiated Auth Context: User Name and Password | Minimum

Active Profile Cookies:

5. Click Save.

Validate the configuration

Do the following to validate the configuration.

1. Point your browser to https://<subdomain>sharefile.com/saml/login.
   You are redirected to the NetScaler Gateway log on form. If you are not redirected, verify the preceding configuration settings.

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

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.

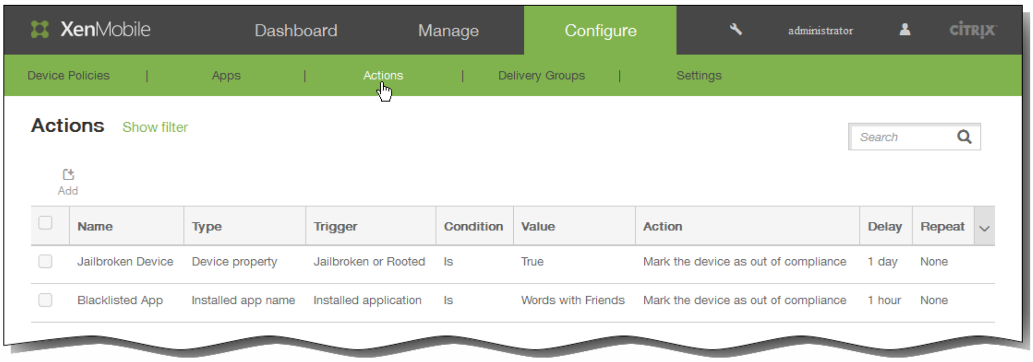
The effects that you set to happen automatically range from the following:

- 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.

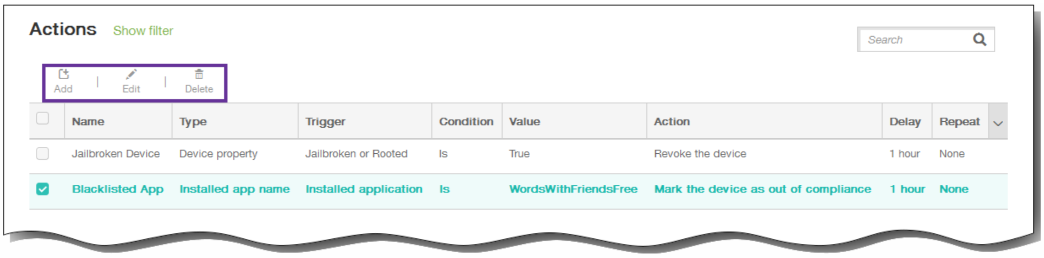
This topic explains how to add, edit, and filter automated actions in XenMobile.

1. From the XenMobile console, click Configure > Actions. The Actions page appears.



	Name	Type	Trigger	Condition	Value	Action	Delay	Repeat
□	Jailbroken Device	Device property	Jailbroken or Rooted	Is	True	Mark the device as out of compliance	1 day	None
□	Blacklisted App	Installed app name	Installed application	Is	Words with Friends	Mark the device as out of compliance	1 hour	None

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.

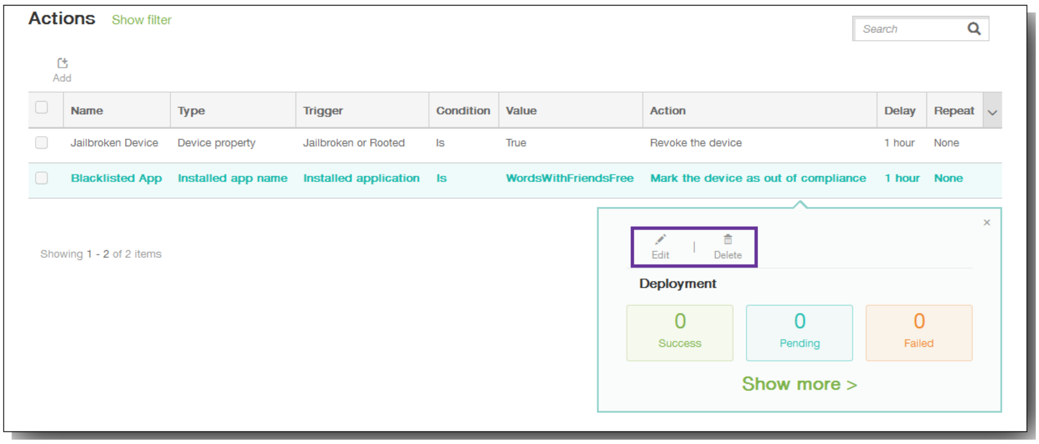


Actions Show filter

Search

Add | Edit | Delete

☐	Name	Type	Trigger	Condition	Value	Action	Delay	Repeat
☐	Jailbroken Device	Device property	Jailbroken or Rooted	Is	True	Revoke the device	1 hour	None
☑	Blacklisted App	Installed app name	Installed application	Is	WordsWithFriendsFree	Mark the device as out of compliance	1 hour	None



Actions Show filter

Search

Add

☐	Name	Type	Trigger	Condition	Value	Action	Delay	Repeat
☐	Jailbroken Device	Device property	Jailbroken or Rooted	Is	True	Revoke the device	1 hour	None
☐	Blacklisted App	Installed app name	Installed application	Is	WordsWithFriendsFree	Mark the device as out of compliance	1 hour	None

Showing 1 - 2 of 2 items

Edit | Delete

Deployment

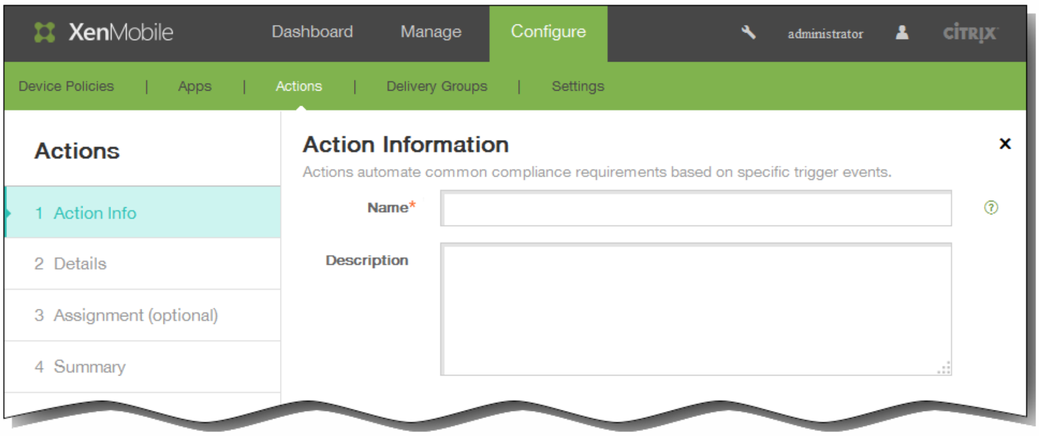
0 Success

0 Pending

0 Failed

Show more >

The Action Information page appears.



XenMobile Dashboard Manage Configure administrator CITRIX

Device Policies | Apps | Actions | Delivery Groups | Settings

Actions

1 Action Info

2 Details

3 Assignment (optional)

4 Summary

Action Information

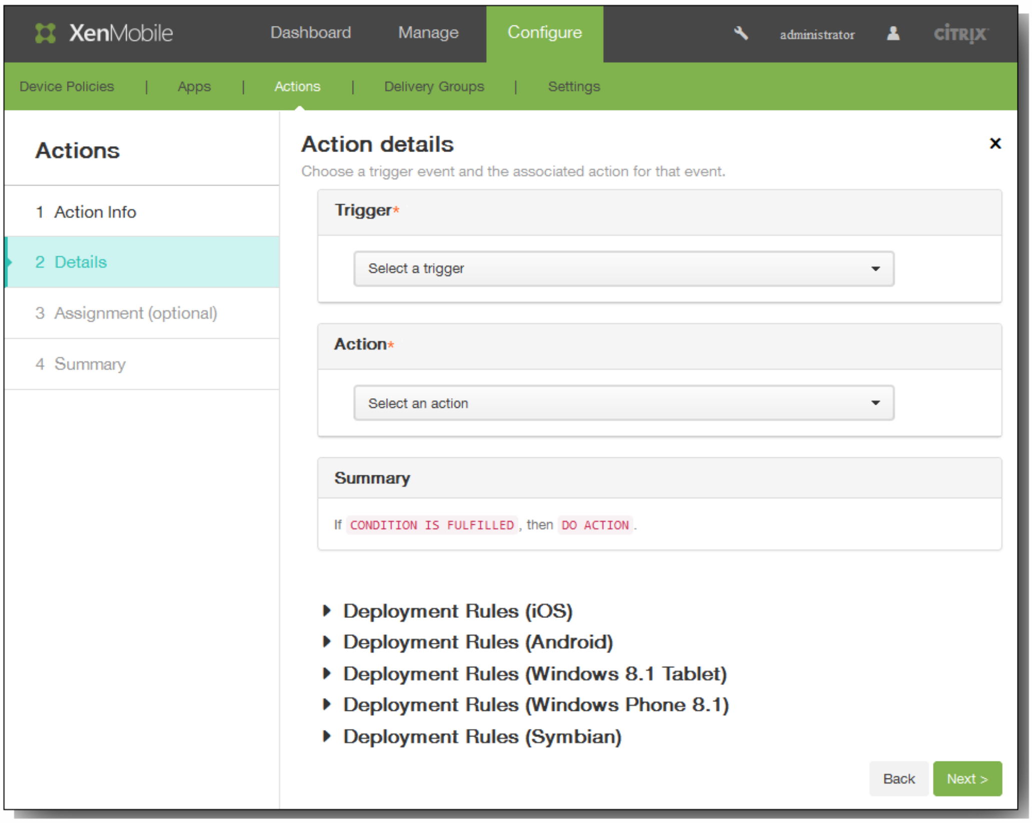
Actions automate common compliance requirements based on specific trigger events.

Name*

Description

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.



Action details

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

Trigger*

Select a trigger

Action*

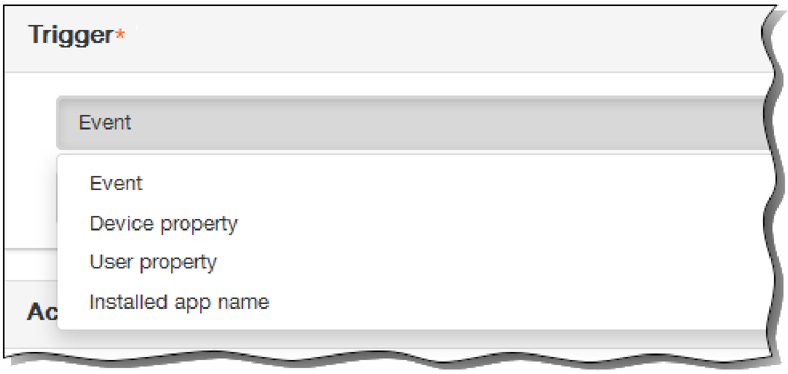
Select an action

Summary

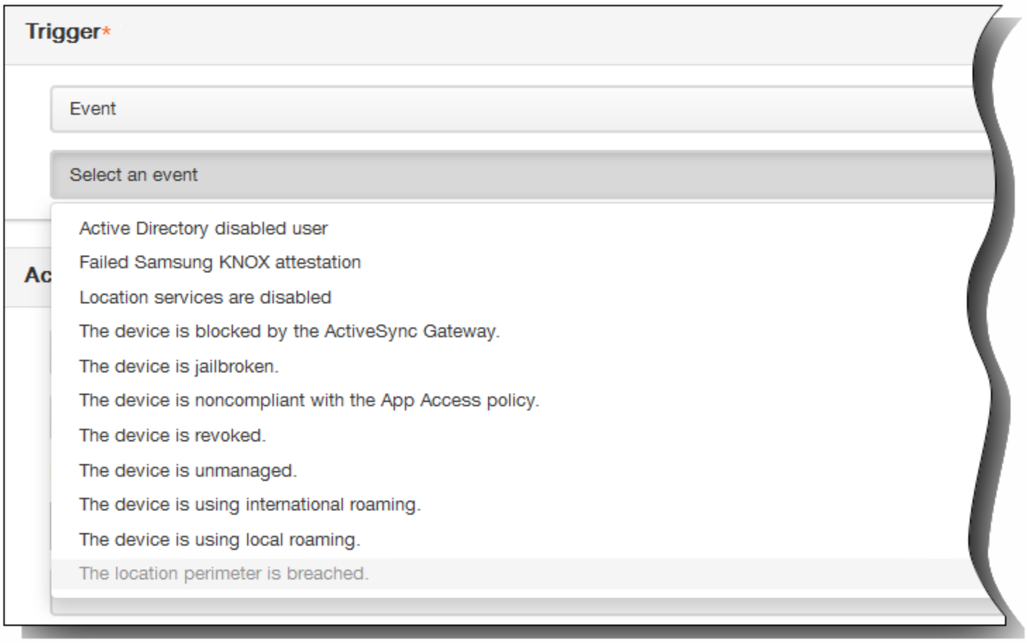
If CONDITION IS FULFILLED, then DO ACTION.

- Deployment Rules (iOS)
- Deployment Rules (Android)
- Deployment Rules (Windows 8.1 Tablet)
- Deployment Rules (Windows Phone 8.1)
- Deployment Rules (Symbian)

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.



Trigger*

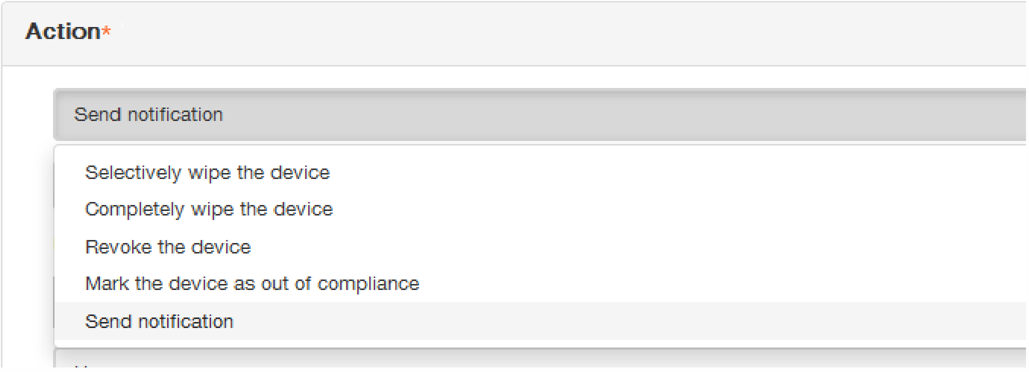
Event

Select an event

Ac

Active Directory disabled user
Failed Samsung KNOX attestation
Location services are disabled
The device is blocked by the ActiveSync Gateway.
The device is jailbroken.
The device is noncompliant with the App Access policy.
The device is revoked.
The device is unmanaged.
The device is using international roaming.
The device is using local roaming.
The location perimeter is breached.

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.



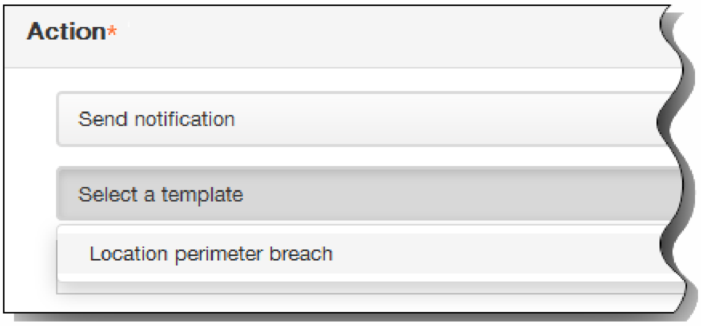
Action*

Send notification

Selectively wipe the device
Completely wipe the device
Revoke the device
Mark the device as out of compliance
Send notification

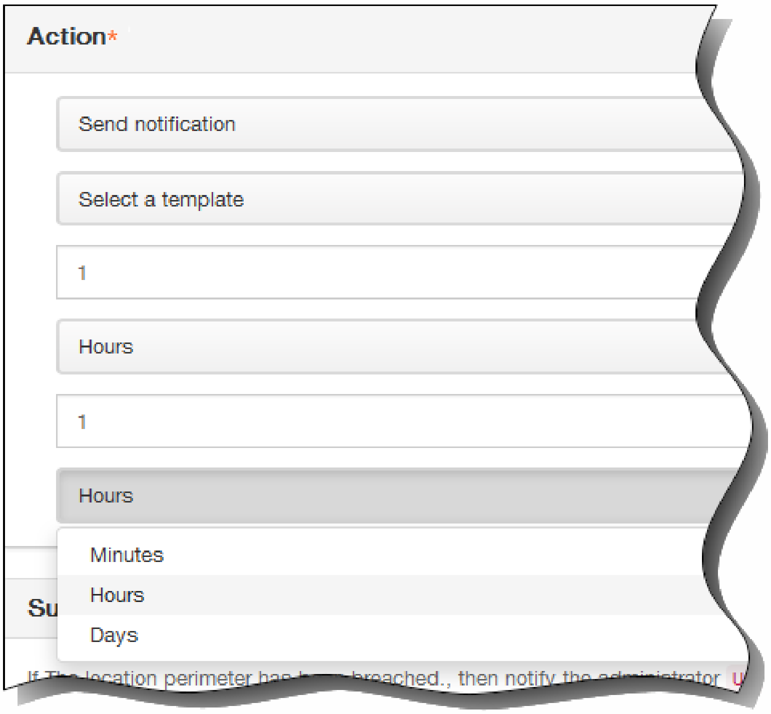
The remainder of this procedure explains how to send a notification action.

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.



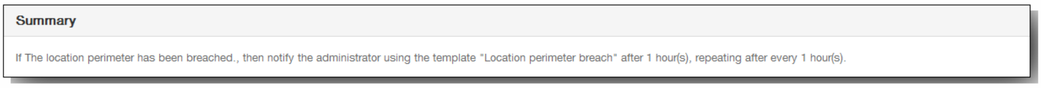
Note: After you select the template, you can preview the notification by clicking Preview notification message.

5. 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.



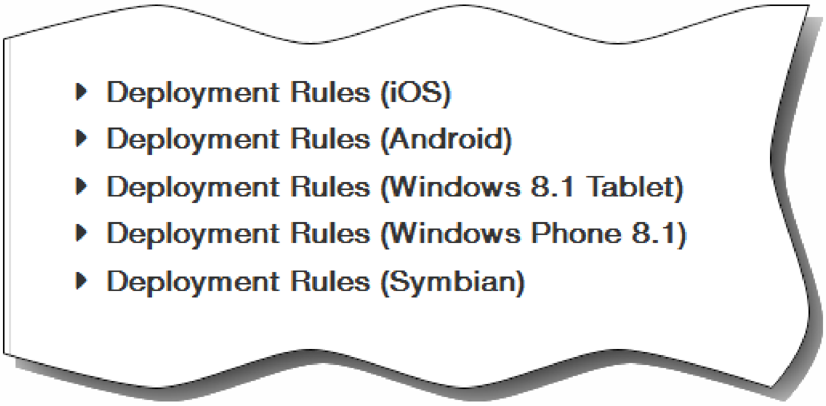
If The location perimeter has been breached., then notify the administrator u

6. In Summary verify that you created the automated action as you intended.



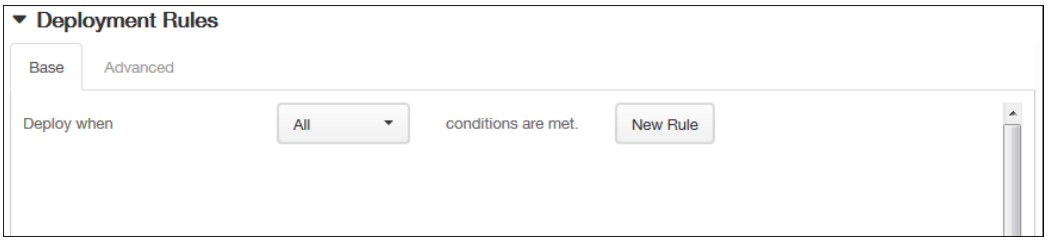
If The location perimeter has been breached., then notify the administrator using the template "Location perimeter breach" after 1 hour(s), repeating after every 1 hour(s).

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.

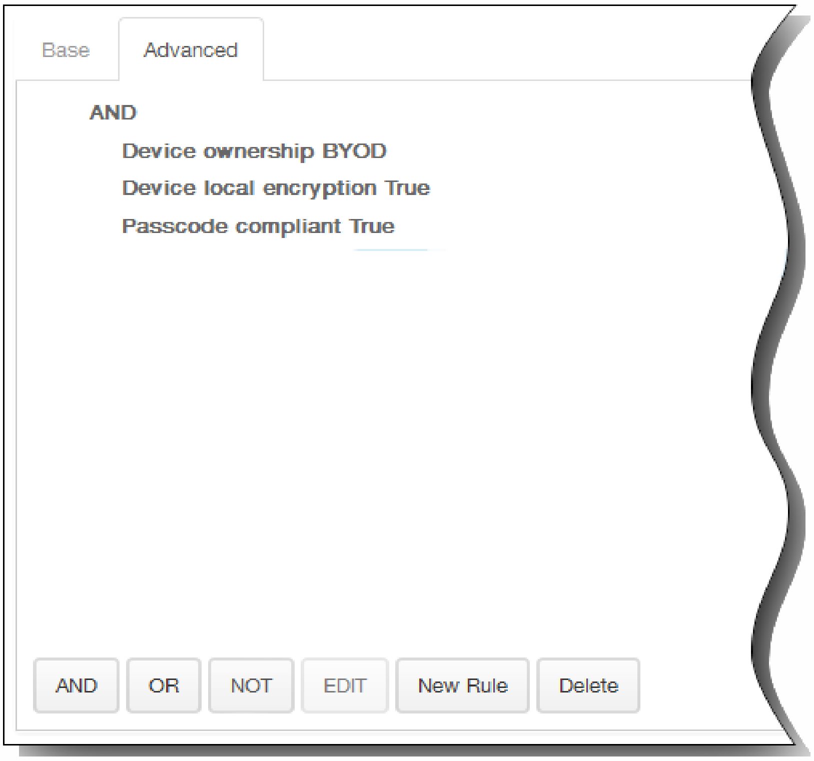


- Deployment Rules (iOS)
- Deployment Rules (Android)
- Deployment Rules (Windows 8.1 Tablet)
- Deployment Rules (Windows Phone 8.1)
- Deployment Rules (Symbian)

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.



AND

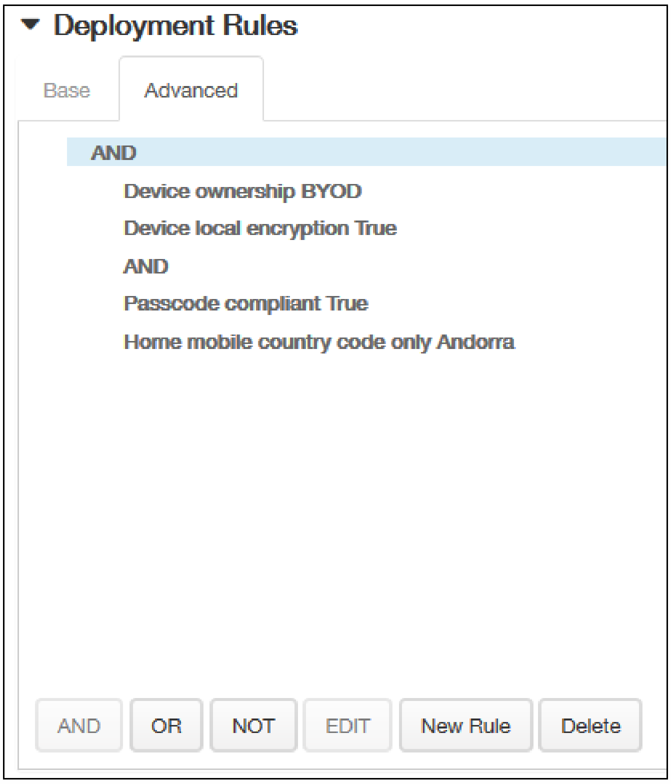
Device ownership BYOD

Device local encryption True

Passcode compliant True

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.



AND

Device ownership BYOD

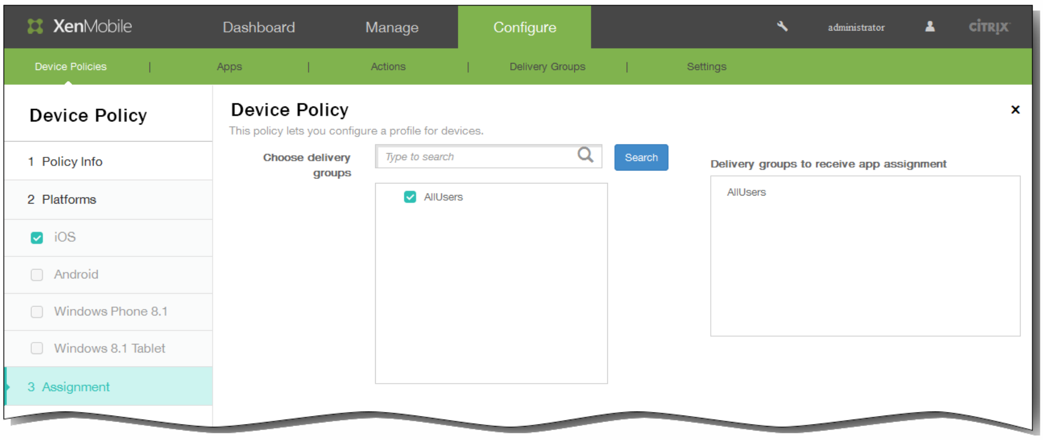
Device local encryption True

AND

Passcode compliant True

Home mobile country code 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.



Device Policy

This policy lets you configure a profile for devices.

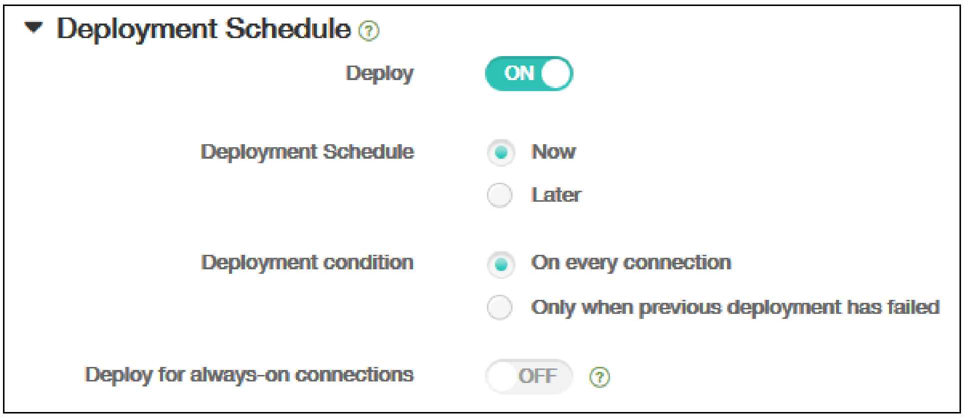
Choose delivery groups: ☑ AllUsers

Delivery groups to receive app assignment: AllUsers

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.



Deployment Schedule

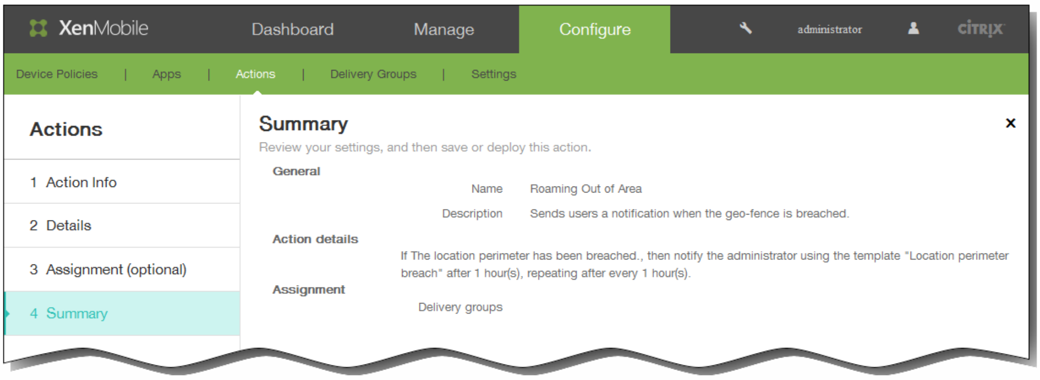
Deploy: ON

Deployment Schedule: ● Now ○ Later

Deployment condition: ● On every connection ○ Only when previous deployment has failed

Deploy for always-on connections: OFF

10. Click Next. The Summary page appears, where you can verify the action configuration.



XenMobile
Dashboard
Manage
Configure
administrator
citrix
Device Policies | Apps | Actions | Delivery Groups | Settings

Actions

1 Action Info

2 Details

3 Assignment (optional)

4 Summary

Summary

Review your settings, and then save or deploy this action.

General

Name: Roaming Out of Area

Description: Sends users a notification when the geo-fence is breached.

Action details

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).

Assignment

Delivery groups

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.

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)

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.

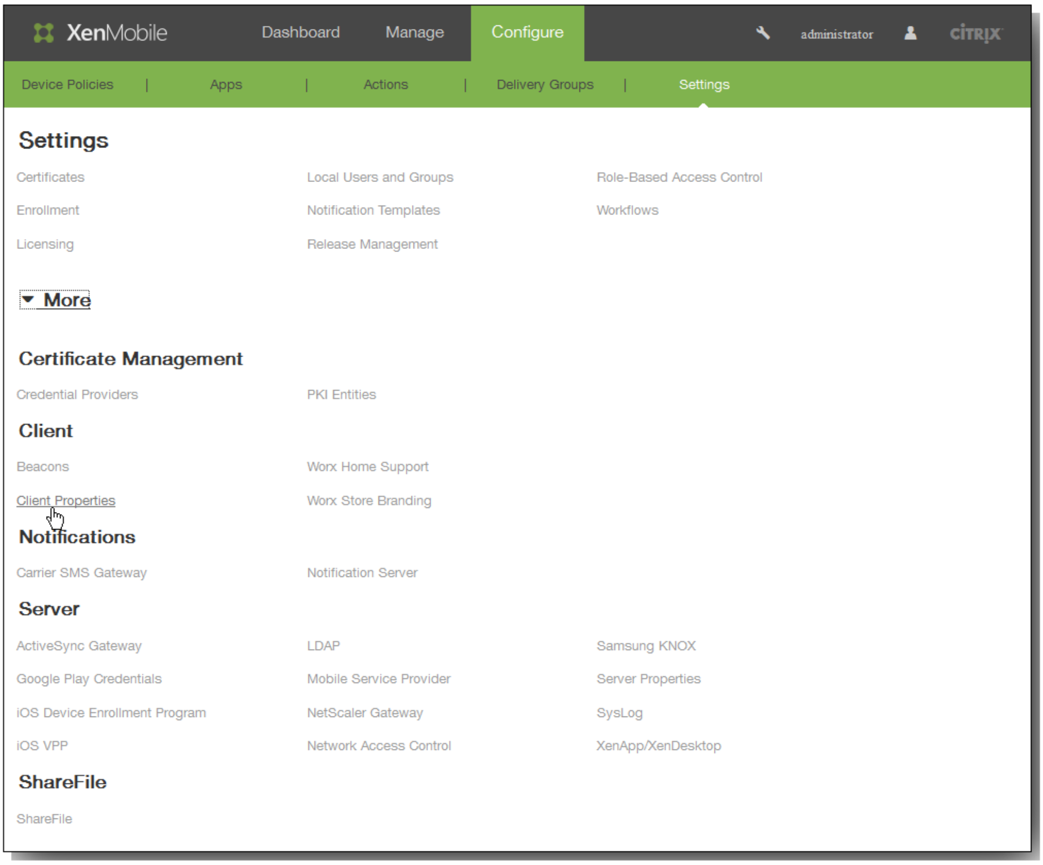
To add, edit, or delete client properties

Jun 19, 2015

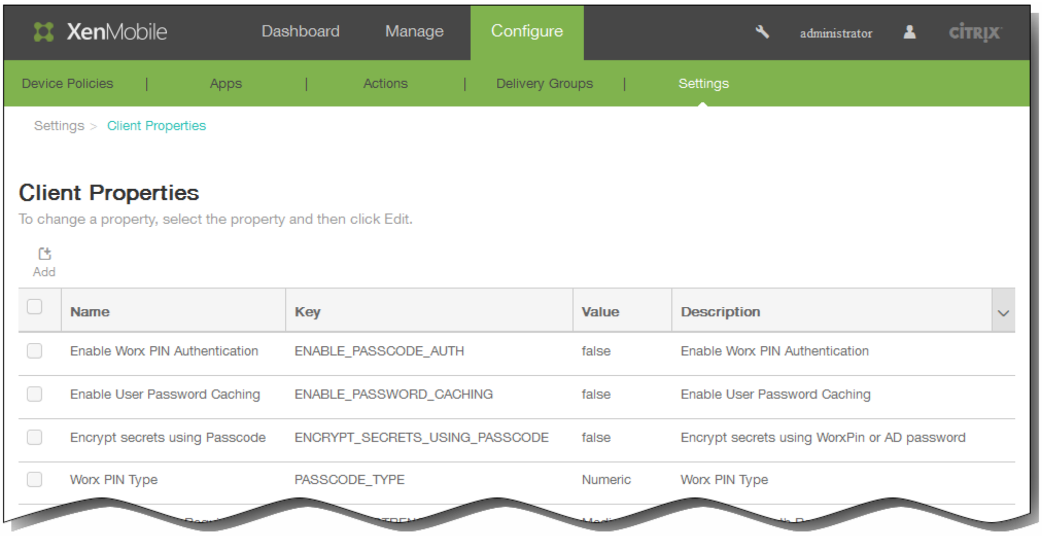
Client properties contain information that is provided directly to Worx Home on users' devices. These properties are used to configure advanced settings, such as the Worx PIN. You obtain client properties from Citrix support.

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.



Settings > Client Properties

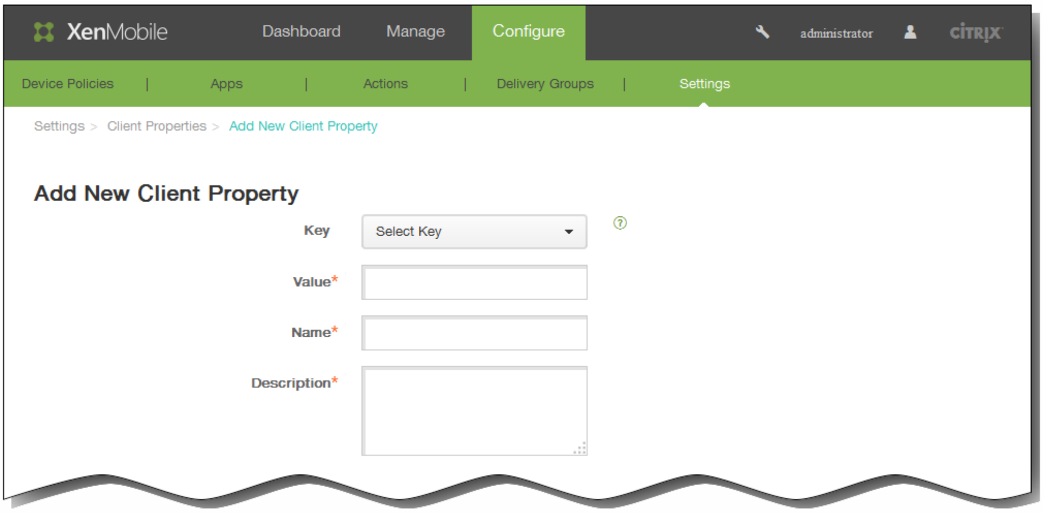
Client Properties

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

☐	Name	Key	Value	Description
☐	Enable Worx PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Worx PIN Authentication
☐	Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
☐	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using WorxPin or AD password
☐	Worx PIN Type	PASSCODE_TYPE	Numeric	Worx PIN Type

To add a client property

1. In the Client Properties page, click Add. The Add New Client Property page appears.



Settings > Client Properties > Add New Client Property

Add New Client Property

Key: Select Key

Value*

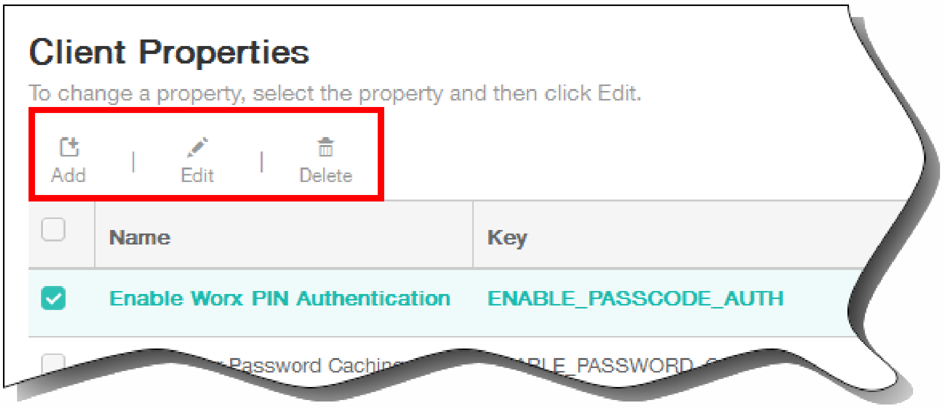
Name*

Description*

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

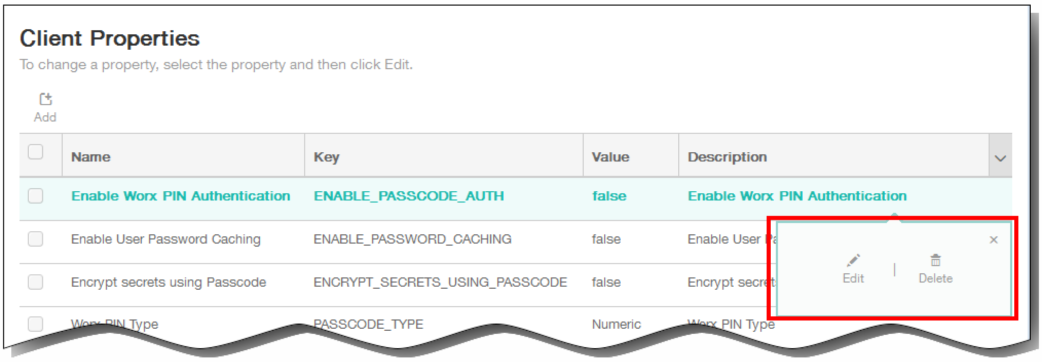
1. In the Client Properties table, select the client property you want to edit.
   Note: When you select the check box next to a client property, the options menu appears above the client property list; when you click anywhere else in the list, the options menu appears on the right side of the listing.



Client Properties

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

☐	Name	Key
☑	Enable Worx PIN Authentication	ENABLE_PASSCODE_AUTH
☐	Password Cachin	BLE_PASSWORD_C

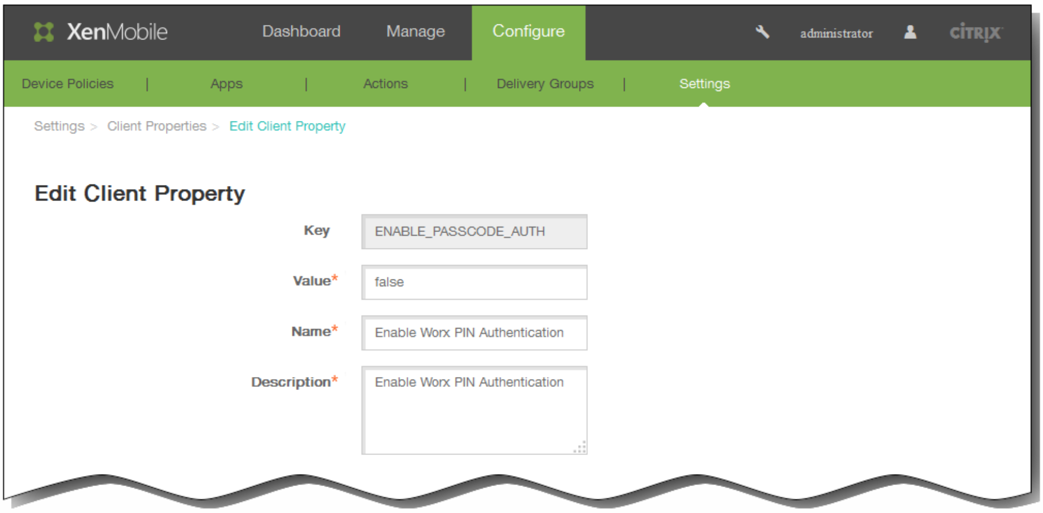


Client Properties

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

☐	Name	Key	Value	Description
☐	Enable Worx PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Worx PIN Authentication
☐	Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Pa
☐	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secret
☐	Worx PIN Type	PASSCODE_TYPE	Numeric	Worx PIN Type

2. Click Edit. The Edit Client Property page appears.



XenMobile
Dashboard
Manage
Configure
administrator
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings

Settings > Client Properties > Edit Client Property

Edit Client Property

Key	ENABLE_PASSCODE_AUTH
Value*	false
Name*	Enable Worx PIN Authentication
Description*	Enable Worx PIN Authentication

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.

XenMobile Server Settings

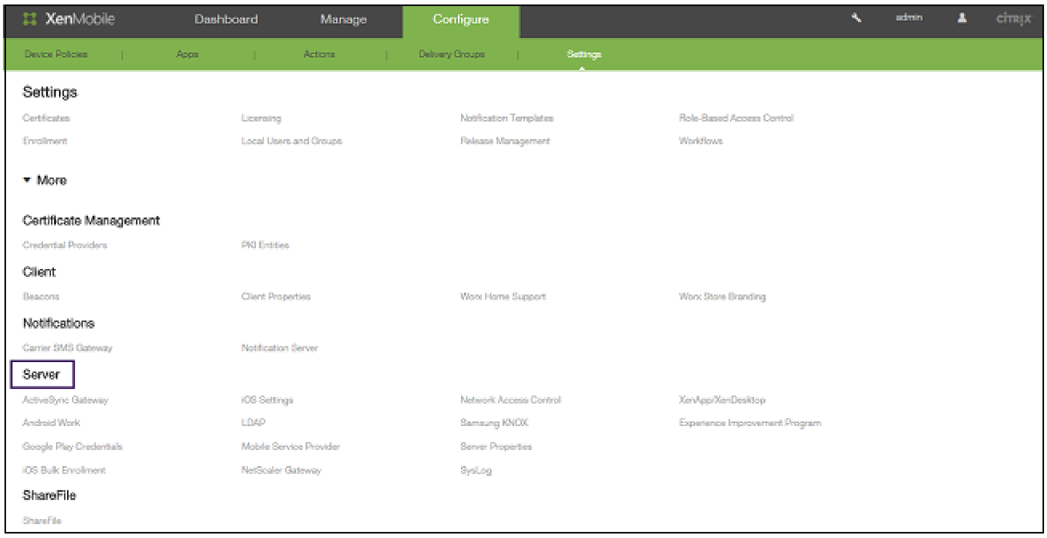
May 29, 2015

The XenMobile server settings that you configure in the XenMobile web console include:

- ActiveSync Gateway
- Android for Work
- Google Play Credentials
- iOS Bulk Enrollment
- iOS Settings
- LDAP
- Mobile Service Provider
- NetScaler Gateway
- Network Access Control
- Samsung KNOX
- Server Properties
- SysLog
- XenApp/XenDesktop
- Experience Improvement Program

1. In the XenMobile console, click Configure and then click Settings.

   The Settings page appears.



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.

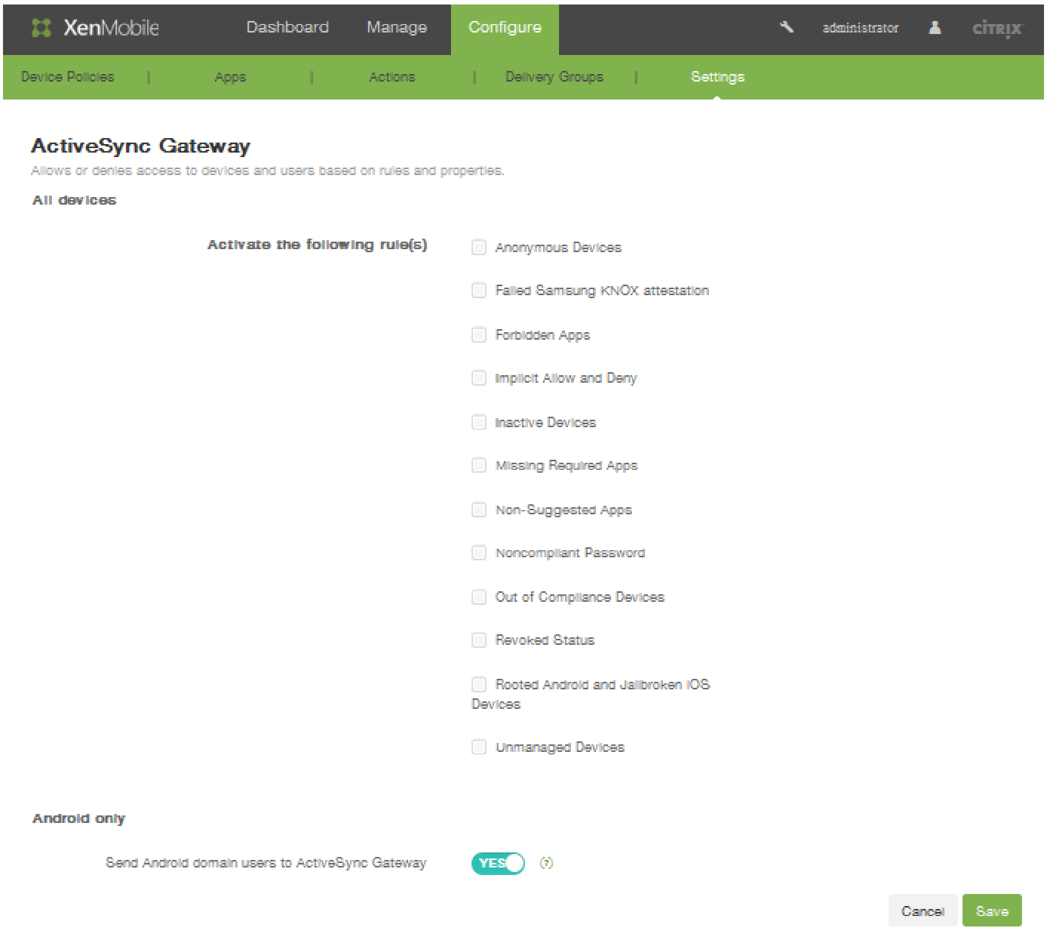
Rooted Android and Jailbroken iOS Devices: Checks whether an Android or iOS device is jailbroken.

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.



ActiveSync Gateway

Allows or denies access to devices and users based on rules and properties.

All devices

Activate the following rule(s)

- □ Anonymous Devices
- □ Failed Samsung KNOX attestation
- □ Forbidden Apps
- □ Implicit Allow and Deny
- □ Inactive Devices
- □ Missing Required Apps
- □ Non-Suggested Apps
- □ Noncompliant Password
- □ Out of Compliance Devices
- □ Revoked Status
- □ Rooted Android and Jailbroken iOS Devices
- □ Unmanaged Devices

Android only

Send Android domain users to ActiveSync Gateway: YES

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.

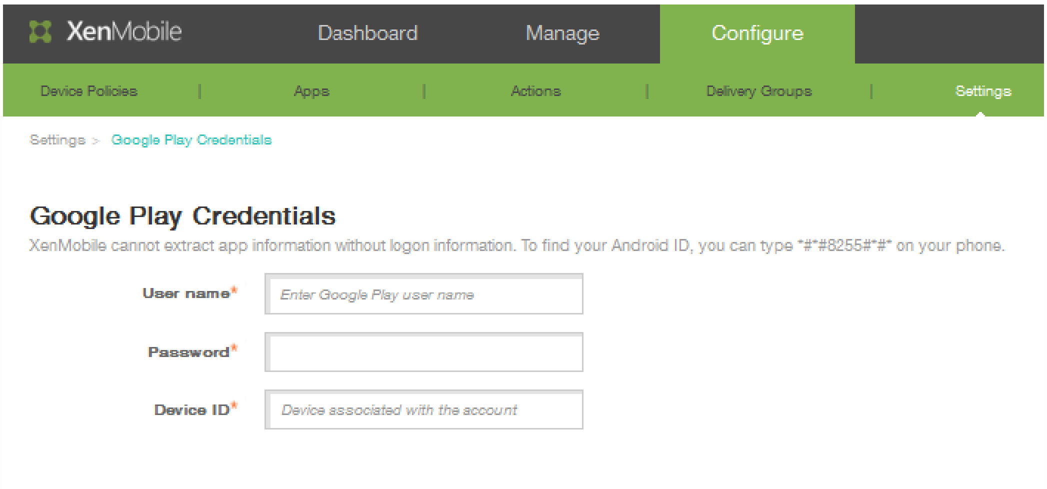
Note: To locate your Android ID, enter *#*#8255#*#* on your phone.

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.



Google Play Credentials

XenMobile cannot extract app information without logon information. To find your Android ID, you can type *#*#8255#*#* on your phone.

User name* Enter Google Play user name

Password*

Device ID* 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 can be assigned to specific devices.

To configure the iOS Device Enrollment Program in XenMobile

1. In the XenMobile web console, click Configure > Settings > More > iOS Bulk Enrollment Program > DEP Configuration. The DEP (Device Enrollment Program) Configuration page appears.

2. In Details, configure the following settings:
   - 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.
3. Click Test Connection to verify connectivity.
4. 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.
5. 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.
6. 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.
7. Click Save.

Deploying iOS Devices Through Apple DEP

Nov 10, 2015

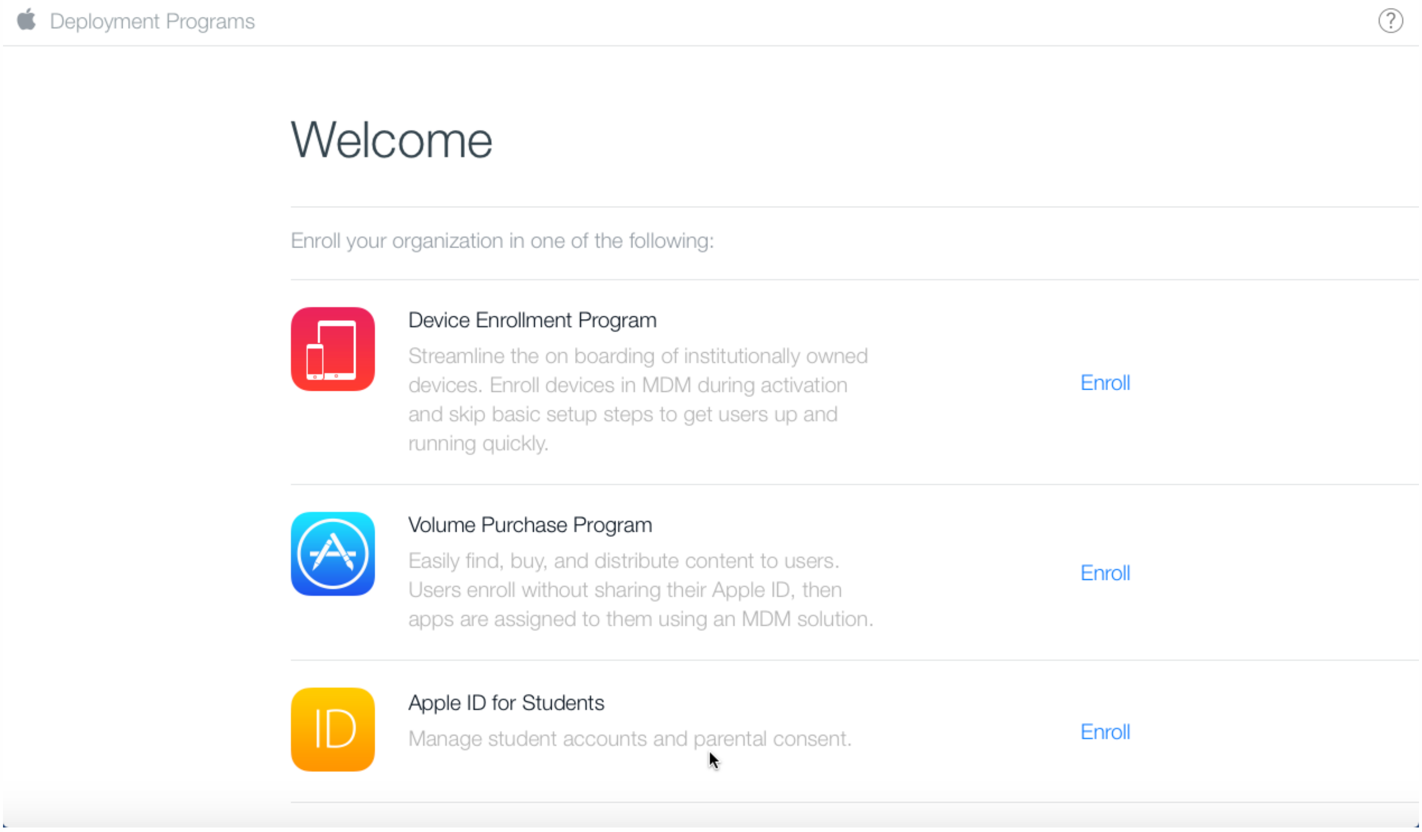
You need an Apple Developer Enterprise Program (DEP) account to be able to take advantage of the Apple DEP for IOS device enrollment and management in XenMobile. The main requirements for organizations to sign up for the Apple DEP are as follows.

- Business or institution phone number and email address
- Verification contact
- Business or institution information (D-U-N-S / tax ID)
- Apple Customer number

For more information about Apple DEP details, see this PDF from Apple. It is important to highlight that Apple DEP is available for organizations and not individuals. It is also important to be aware that a fair amount of corporate details and information needs to be provided to create an Apple DEP account, which means it could take time for customers to request and receive approval for their accounts.

Applying for the Apple DEP account

When applying for a DEP account, the best practice is to use an email address that is tied to the organization, such as dep@company.com.



Deployment Programs

Welcome

Enroll your organization in one of the following:

Device Enrollment Program

Streamline the on boarding of institutionally owned devices. Enroll devices in MDM during activation and skip basic setup steps to get users up and running quickly.

Enroll

Volume Purchase Program

Easily find, buy, and distribute content to users. Users enroll without sharing their Apple ID, then apps are assigned to them using an MDM solution.

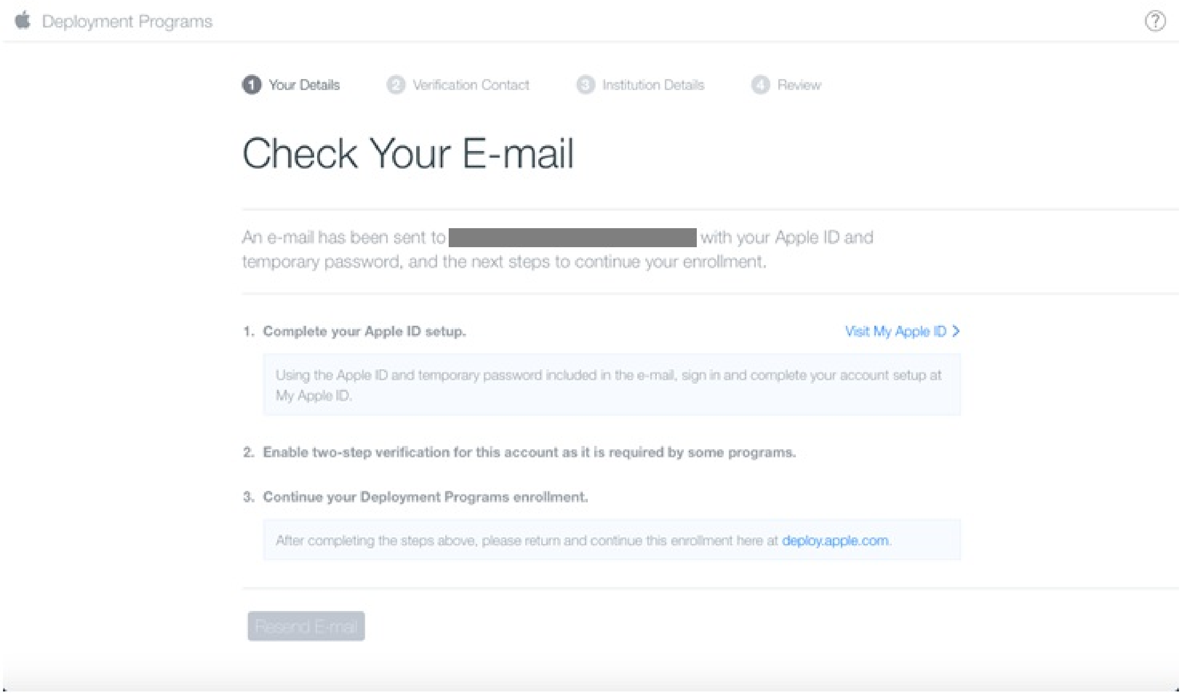
Enroll

Apple ID for Students

Manage student accounts and parental consent.

Enroll

1. After you enter your organization information, you should receive a temporary password for the new Apple ID through email.



Check Your E-mail

An e-mail has been sent to [redacted] with your Apple ID and temporary password, and the next steps to continue your enrollment.

1. Complete your Apple ID setup. Visit My Apple ID >

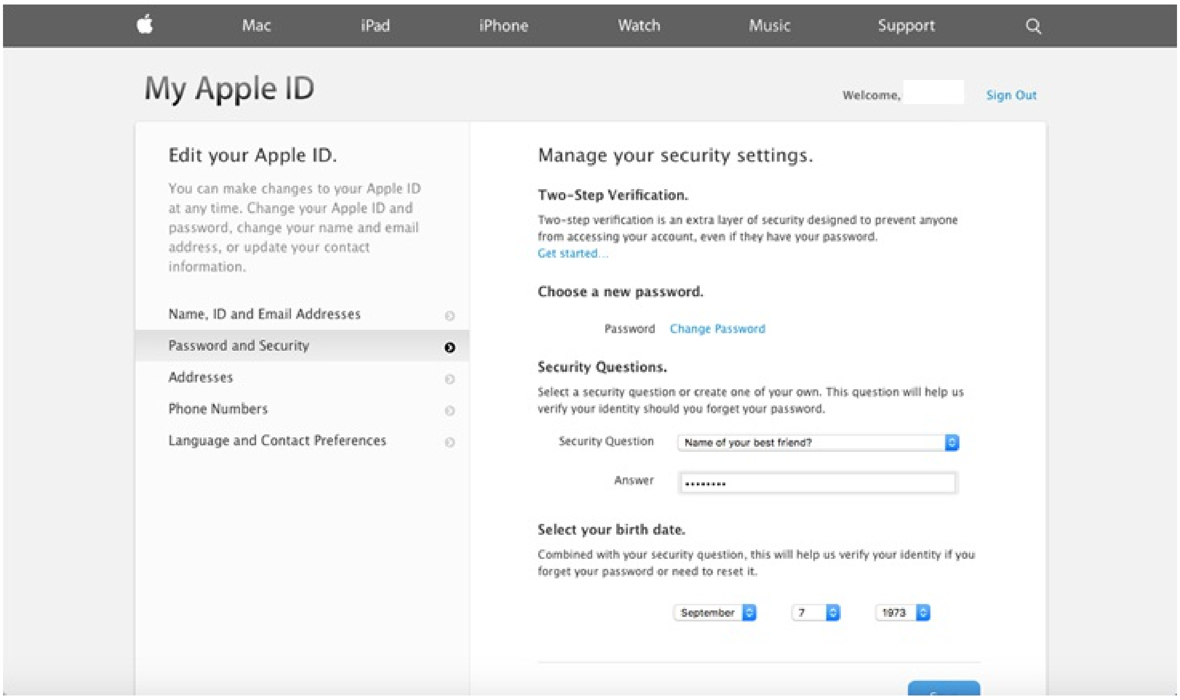
Using the Apple ID and temporary password included in the e-mail, sign in and complete your account setup at My Apple ID.

2. Enable two-step verification for this account as it is required by some programs.

3. Continue your Deployment Programs enrollment.

After completing the steps above, please return and continue this enrollment here at deploy.apple.com.

2. You then sign in with the Apple ID and complete the security settings for the account.



My Apple ID

Welcome, Sign Out

Edit your Apple ID.

You can make changes to your Apple ID at any time. Change your Apple ID and password, change your name and email address, or update your contact information.

Name, ID and Email Addresses
Password and Security
Addresses
Phone Numbers
Language and Contact Preferences

Manage your security settings.

Two-Step Verification.

Two-step verification is an extra layer of security designed to prevent anyone from accessing your account, even if they have your password.
Get started...

Choose a new password.

Password Change Password

Security Questions.

Select a security question or create one of your own. This question will help us verify your identity should you forget your password.

Security Question: Name of your best friend?

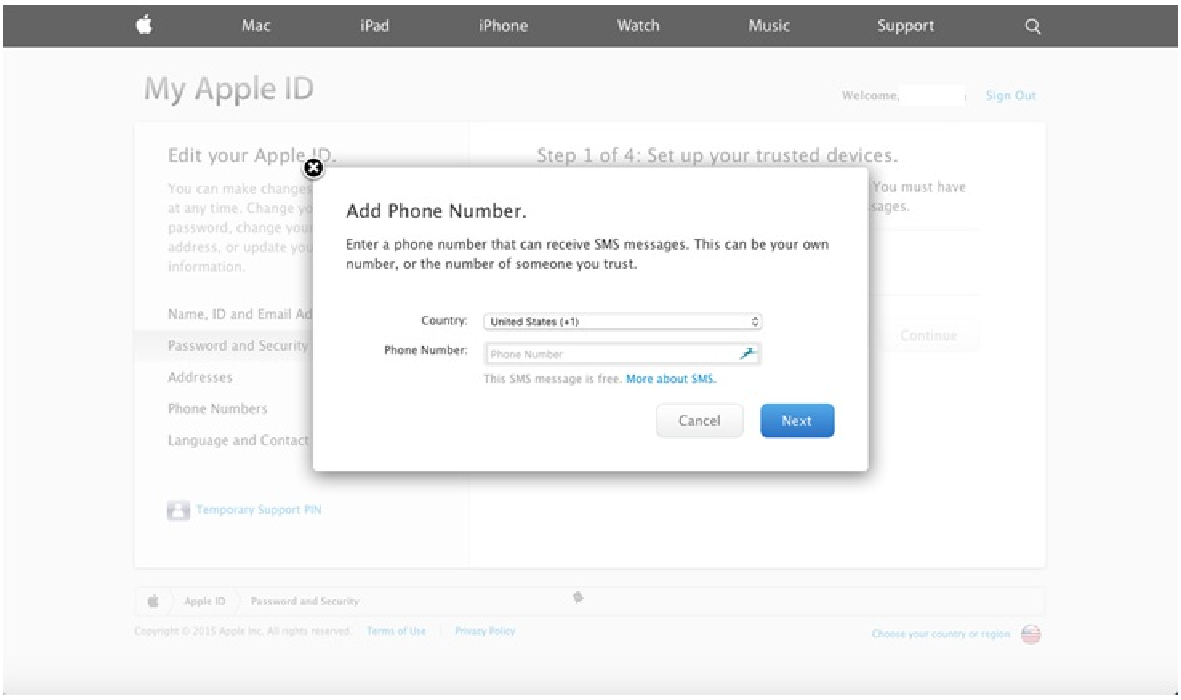
Answer: ••••••••

Select your birth date.

Combined with your security question, this will help us verify your identity if you forget your password or need to reset it.

September 7 1973

3. Configure and enable two-step verification, which is required for use with the DEP Portal. During these steps, you add a phone number where you will receive the 4-digit PIN for the two-step verification.



My Apple ID

Add Phone Number.

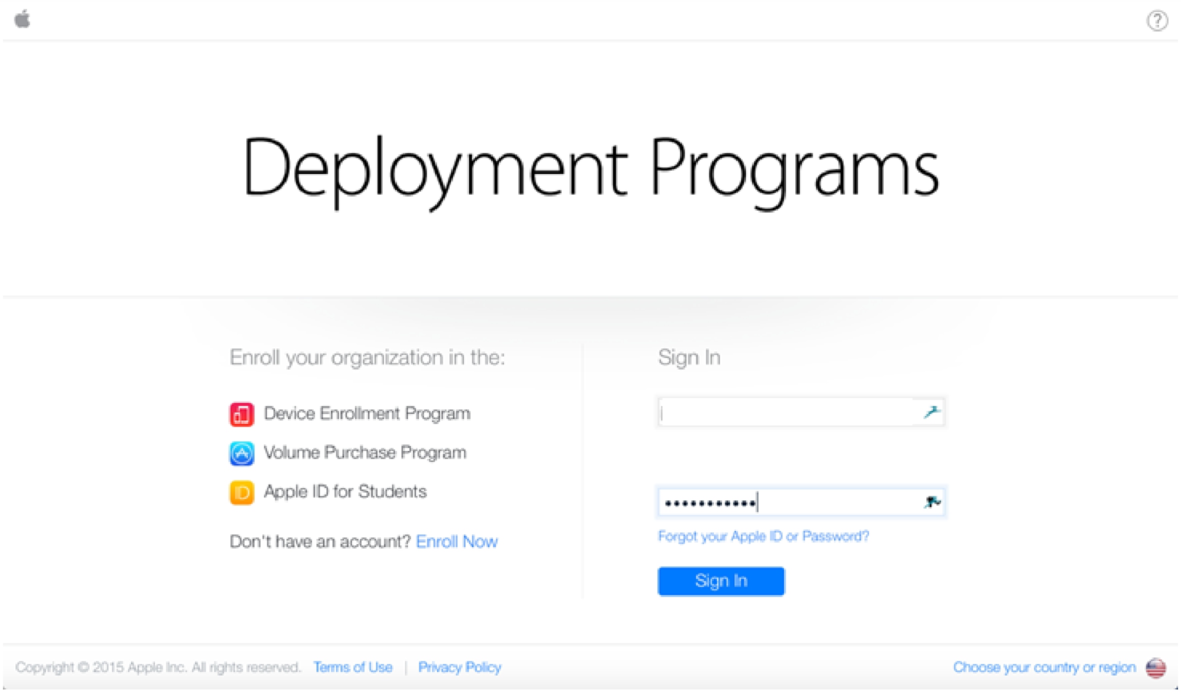
Enter a phone number that can receive SMS messages. This can be your own number, or the number of someone you trust.

Country: United States (+1)

Phone Number: Phone Number

This SMS message is free. More about SMS.

4. Log in to the DEP Portal to complete the account configuration using the two-step verification that you just set up.



Deployment Programs

Enroll your organization in the:

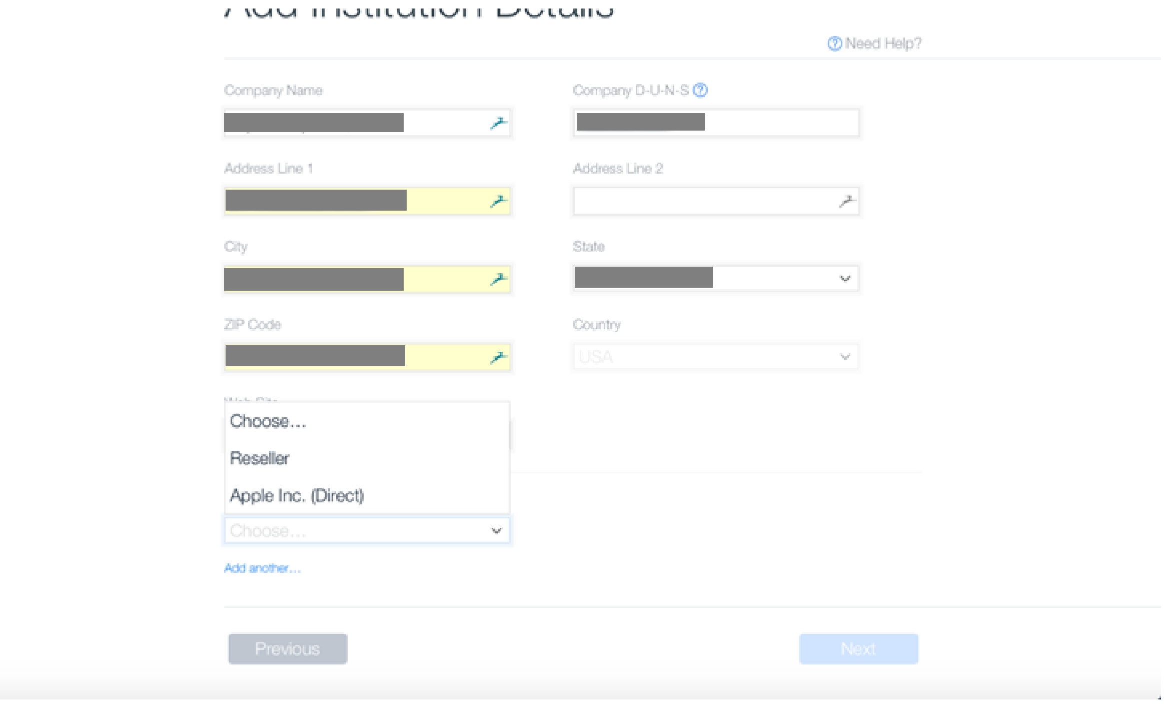
- Device Enrollment Program
- Volume Purchase Program
- Apple ID for Students

Don't have an account? Enroll Now

Sign In

Forgot your Apple ID or Password?
Sign In
Copyright © 2015 Apple Inc. All rights reserved.
Terms of Use
Privacy Policy
Choose your country or region

5. Add your company details and then select from where you purchase devices. For details on purchasing options, see the next section, Ordering DEP-enabled devices.



Add Institution Details

Company Name: [redacted]

Company D-U-N-S: [redacted]

Address Line 1: [redacted]

Address Line 2:

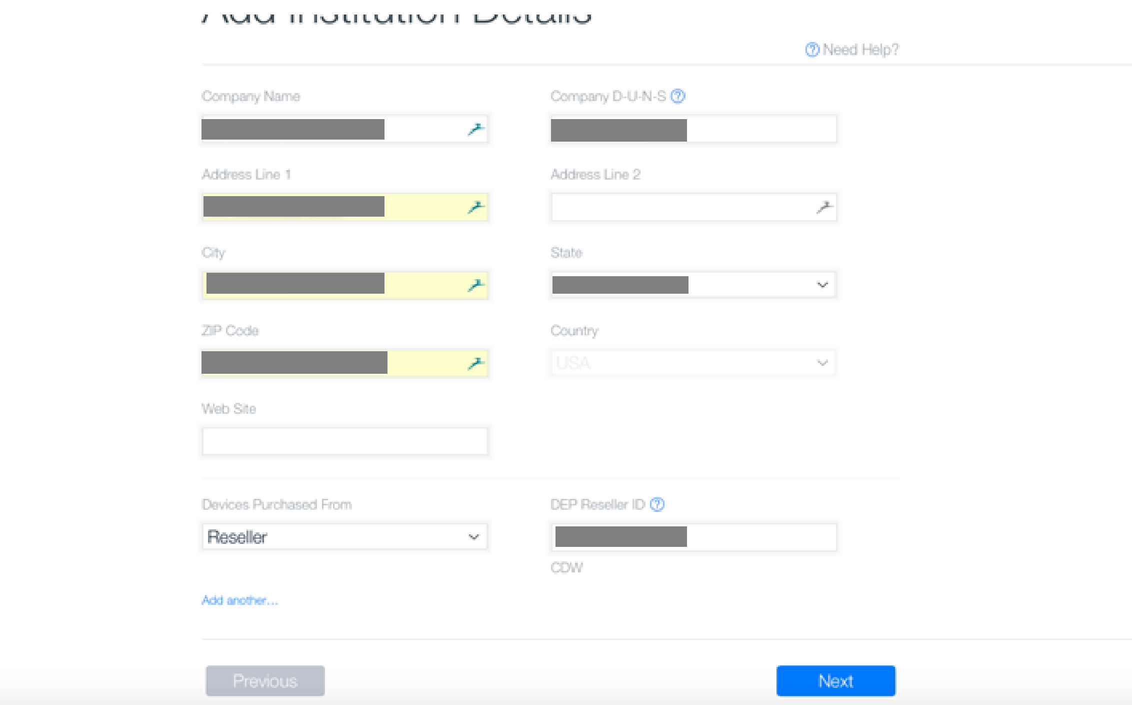
City: [redacted]

State: [redacted]

ZIP Code: [redacted]

Country: USA

6. Add the Apple Customer Number or the DEP Reseller ID and then verify your enrollment details and wait for Apple to approve your account.



Add Institution Details

Company Name: [redacted]

Company D-U-N-S: [redacted]

Address Line 1: [redacted]

Address Line 2:

City: [redacted]

State: [redacted]

ZIP Code: [redacted]

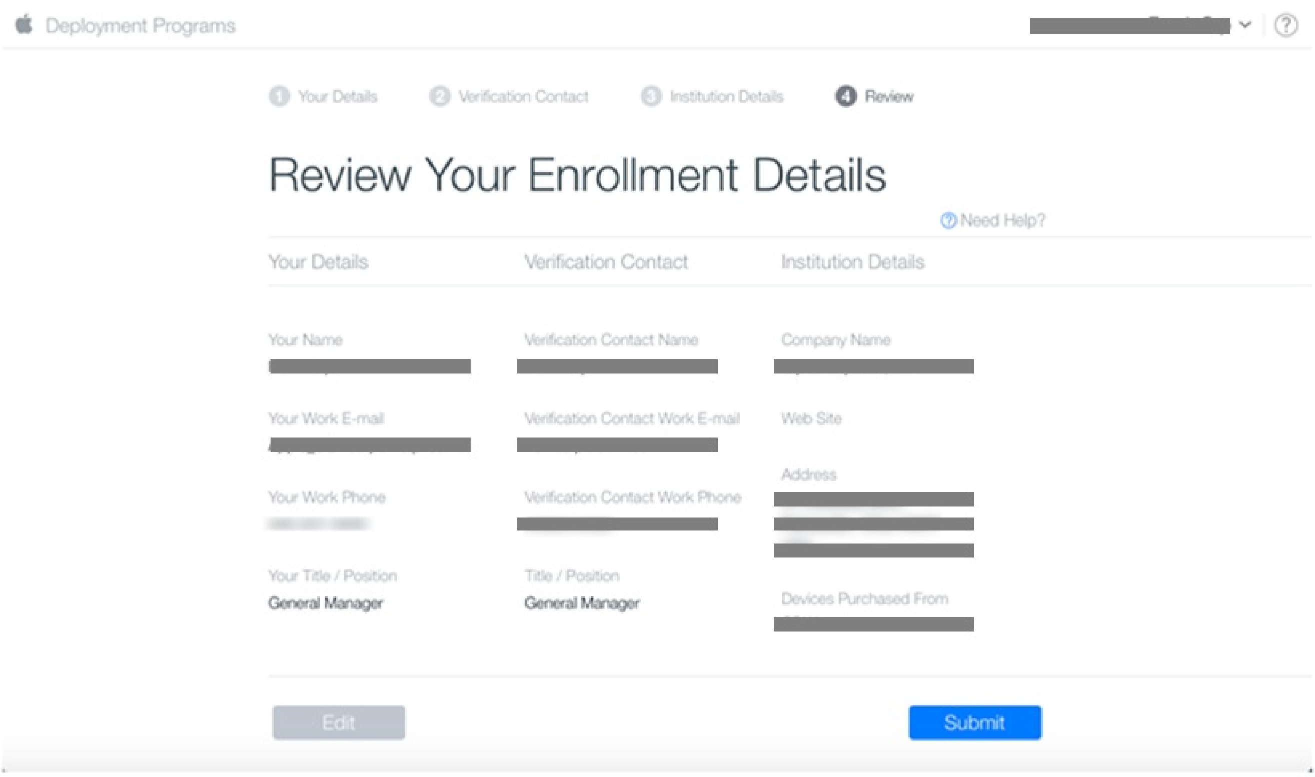
Country: USA

Web Site:

Devices Purchased From: Reseller

DEP Reseller ID: [redacted]

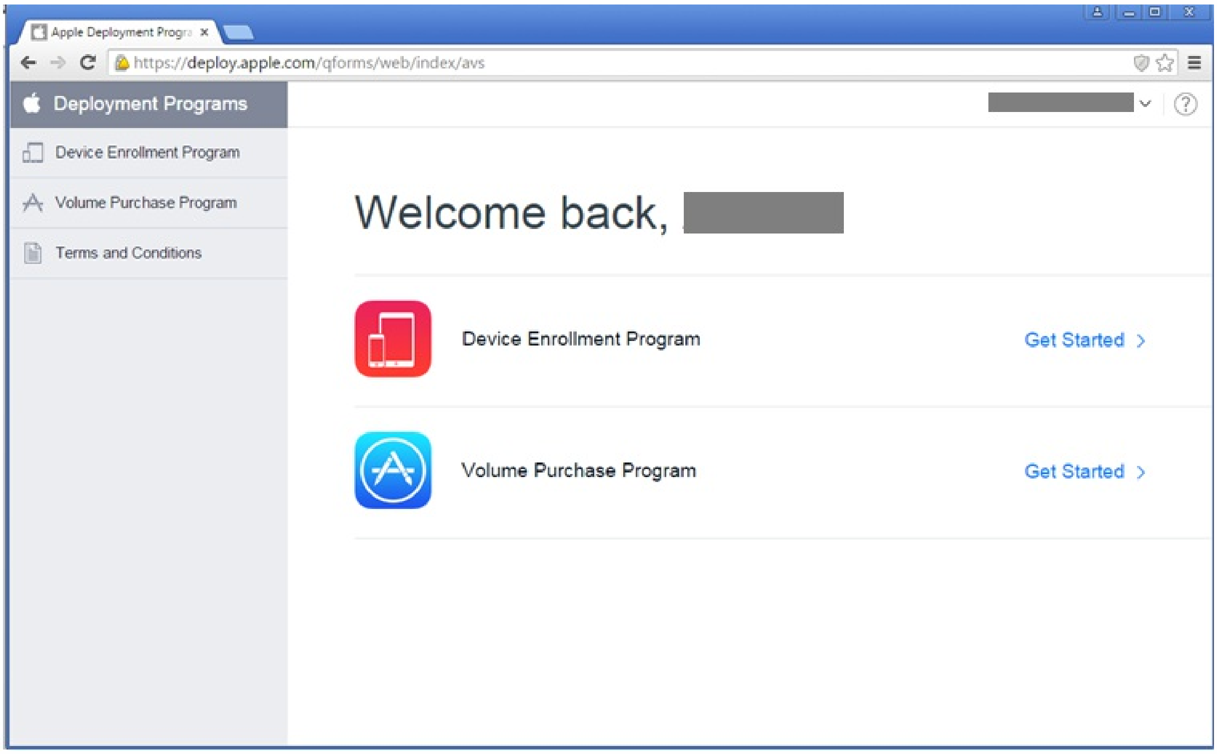
CDW



Review Your Enrollment Details

Your Details	Verification Contact	Institution Details
Your Name [redacted]	Verification Contact Name [redacted]	Company Name [redacted]
Your Work E-mail [redacted]	Verification Contact Work E-mail [redacted]	Web Site
Your Work Phone [redacted]	Verification Contact Work Phone [redacted]	Address [redacted]
Your Title / Position General Manager	Title / Position General Manager	Devices Purchased From [redacted]

7. After you receive your logon credentials from Apple, log into the Apple DEP Portal. Then, follow the steps in the next section to connect your account with XenMobile.

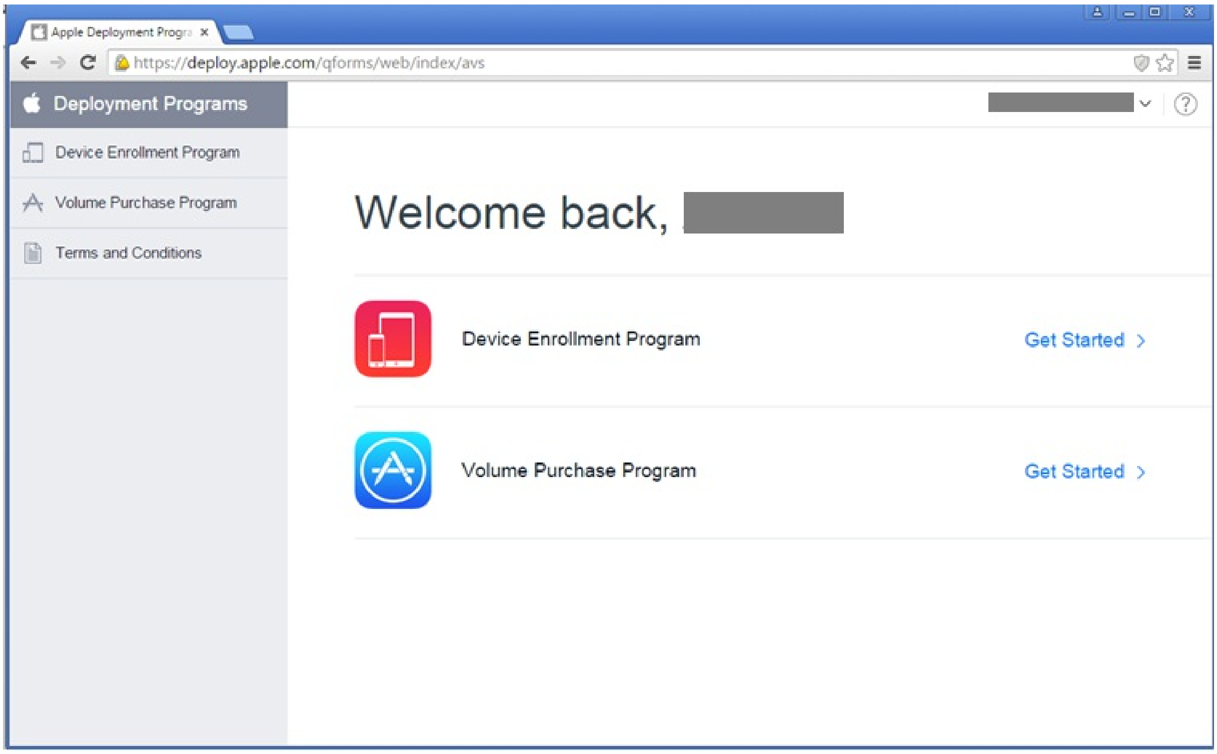


Welcome back, [redacted]

Integrating your Apple DEP account with XenMobile

Follow the steps in this section to connect your Apple DEP account with your XenMobile server deployment.

1. On the left-hand side of the Apple DEP Portal, click **Device Enrollment Program**.

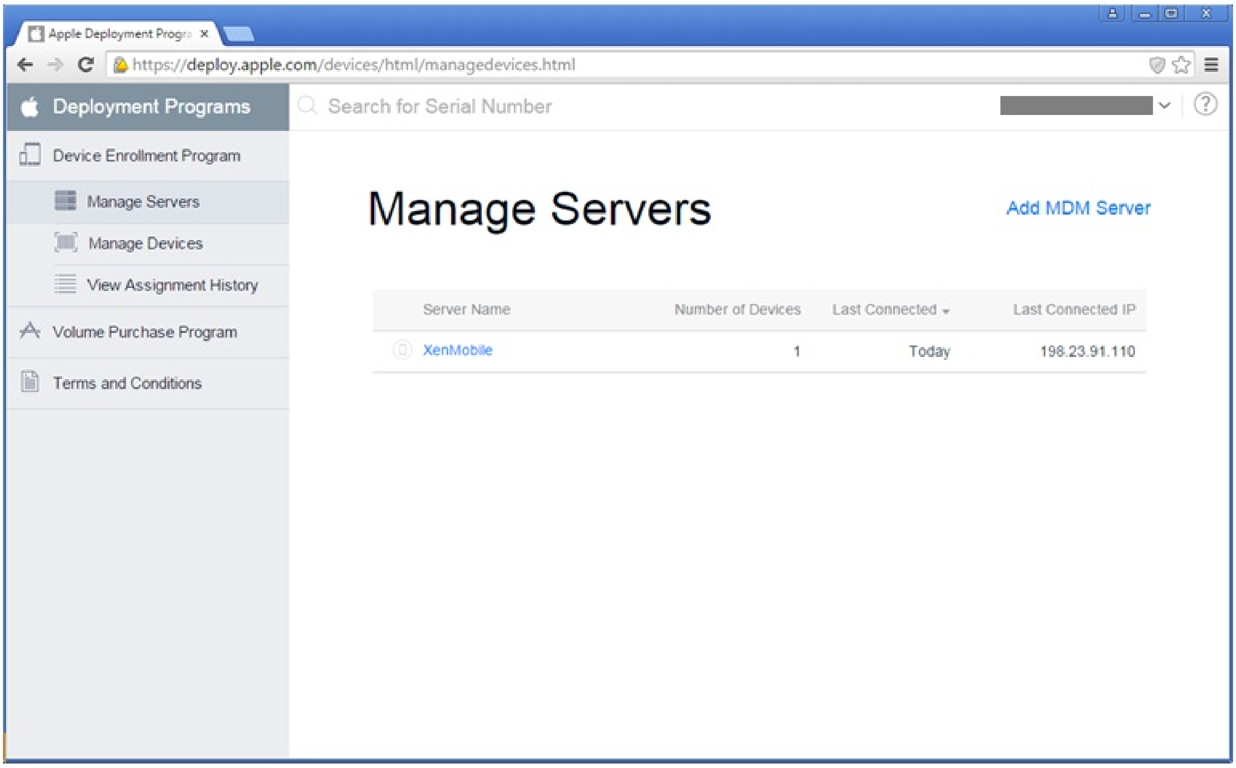


https://deploy.apple.com/qforms/web/index/avs

[redacted]

Welcome back, [redacted]

2. Click **Manage Servers** and then on the right-hand side, click **Add MDM Server**.

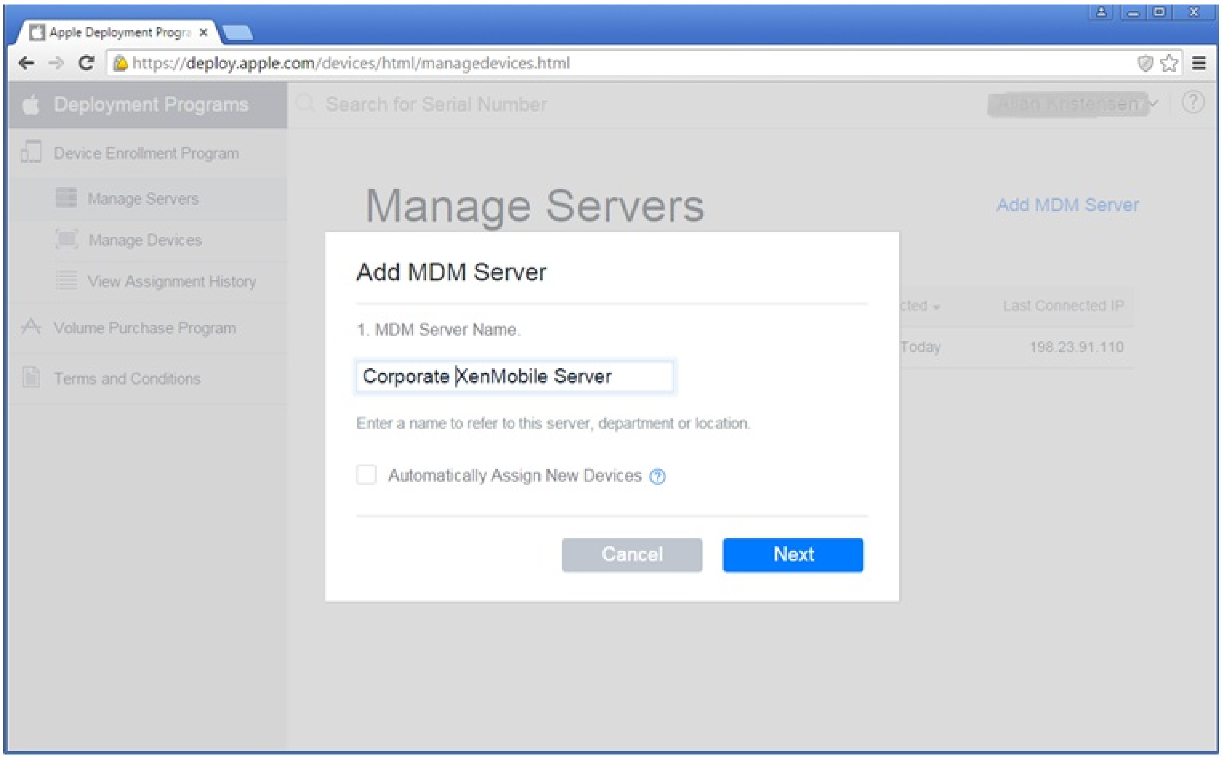


https://deploy.apple.com/devices/html/managedevices.html

[redacted]

Server Name	Number of Devices	Last Connected	Last Connected IP
XenMobile	1	Today	198.23.91.110

3. In **Add MDM Server**, enter a name for your XenMobile server and then click **Next**.



Add MDM Server

1. MDM Server Name.

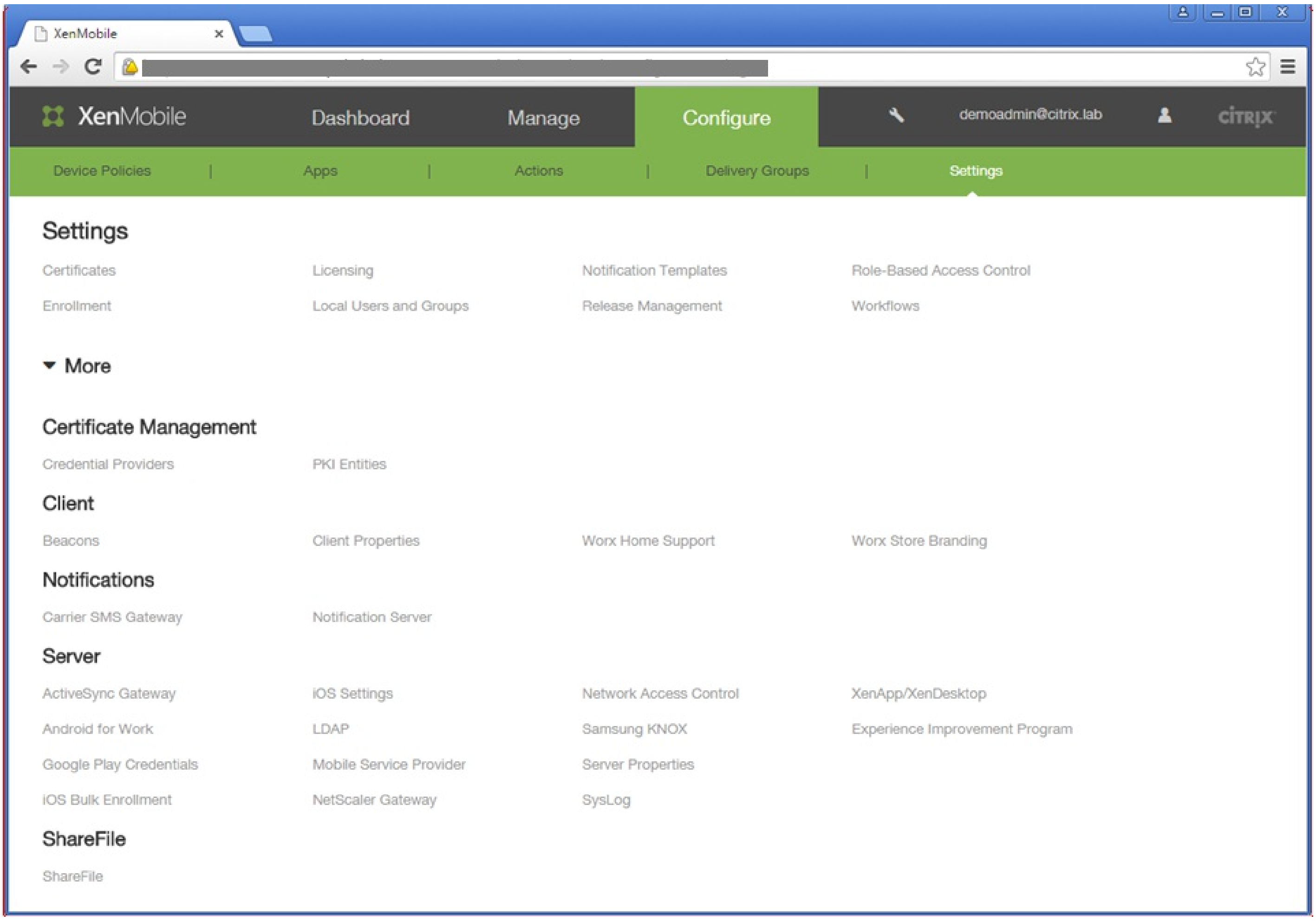
Corporate XenMobile Server

Enter a name to refer to this server, department or location.

□ Automatically Assign New Devices

4. Upload a public key from your XenMobile server. To generate the key from XenMobile, do the following:

   a. Log on to the XenMobile console, click **Configure**, click **Settings** and then under **More**, click **iOS Bulk Enrollment**.



Settings

Certificates | Licensing | Notification Templates | Role-Based Access Control
Enrollment | Local Users and Groups | Release Management | Workflows

▼ More

Certificate Management

Credential Providers | PKI Entities

Client

Beacons | Client Properties | Worx Home Support | Worx Store Branding

Notifications

Carrier SMS Gateway | Notification Server

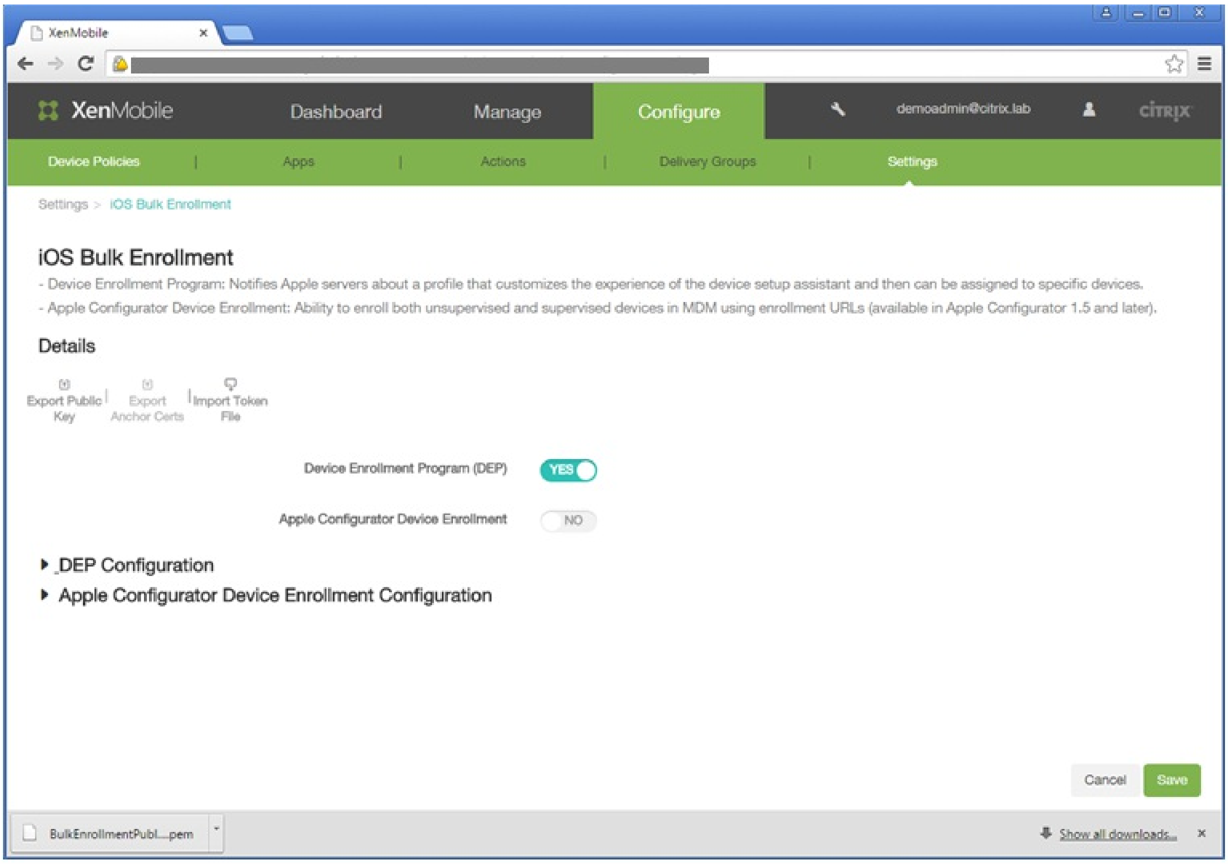
Server

ActiveSync Gateway | iOS Settings | Network Access Control | XenApp/XenDesktop
Android for Work | LDAP | Samsung KNOX | Experience Improvement Program
Google Play Credentials | Mobile Service Provider | Server Properties
iOS Bulk Enrollment | NetScaler Gateway | SysLog

ShareFile

ShareFile

b. On the **iOS Bulk Enrollment** page, click **Export Public Key**. The public key is downloaded.



XenMobile
[redacted]
XenMobile
Dashboard
Manage
Configure
demoadmin@citrix.lab
CITRIX
Device Policies | Apps | Actions | Delivery Groups | Settings
Settings > iOS Bulk Enrollment

iOS Bulk Enrollment

- Device Enrollment Program: Notifies Apple servers about a profile that customizes the experience of the device setup assistant and then can be assigned to specific devices.
- Apple Configurator Device Enrollment: Ability to enroll both unsupervised and supervised devices in MDM using enrollment URLs (available in Apple Configurator 1.5 and later).

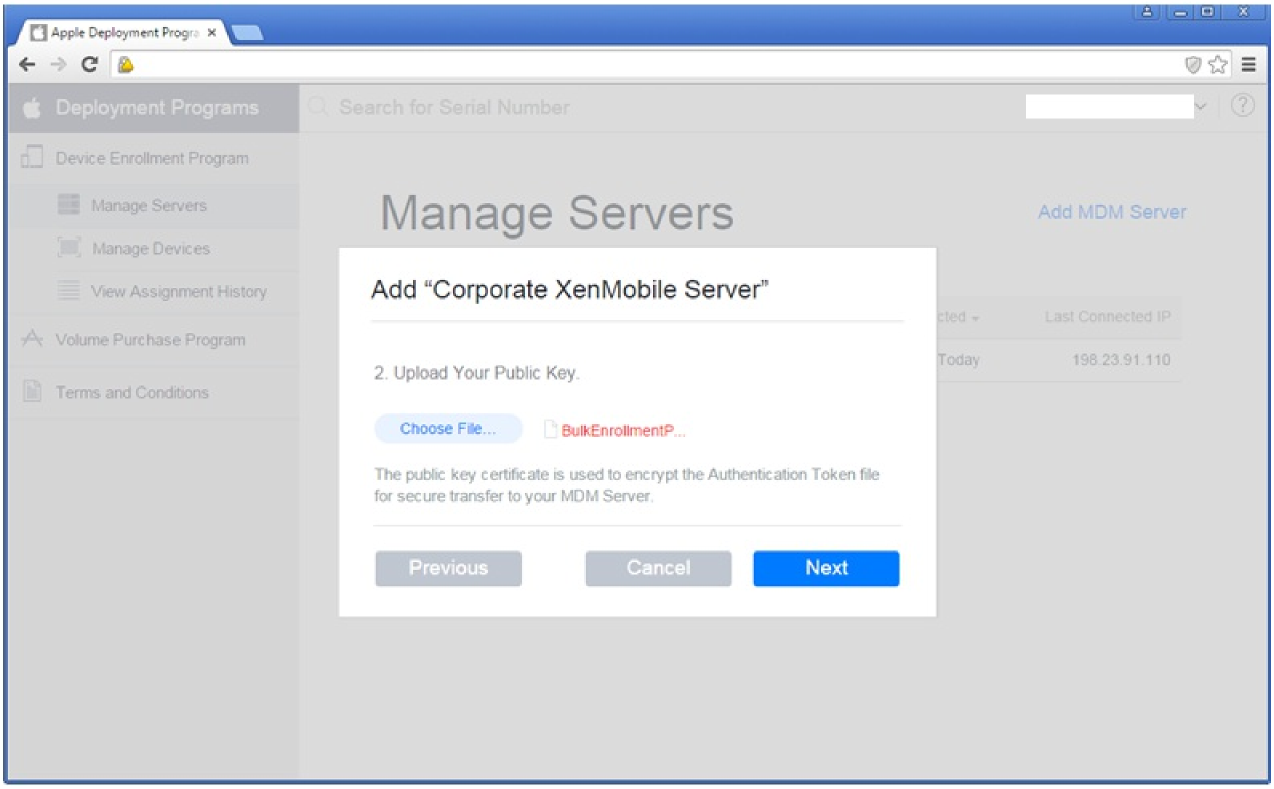
Details

Device Enrollment Program (DEP): YES

Apple Configurator Device Enrollment: NO

▸ DEP Configuration
▸ Apple Configurator Device Enrollment Configuration
Cancel
Save
BulkEnrollmentPubl....pem
Show all downloads...

5. On the Apple DEP Portal, click **Choose file**, select the public key you just downloaded and then click **Next**.



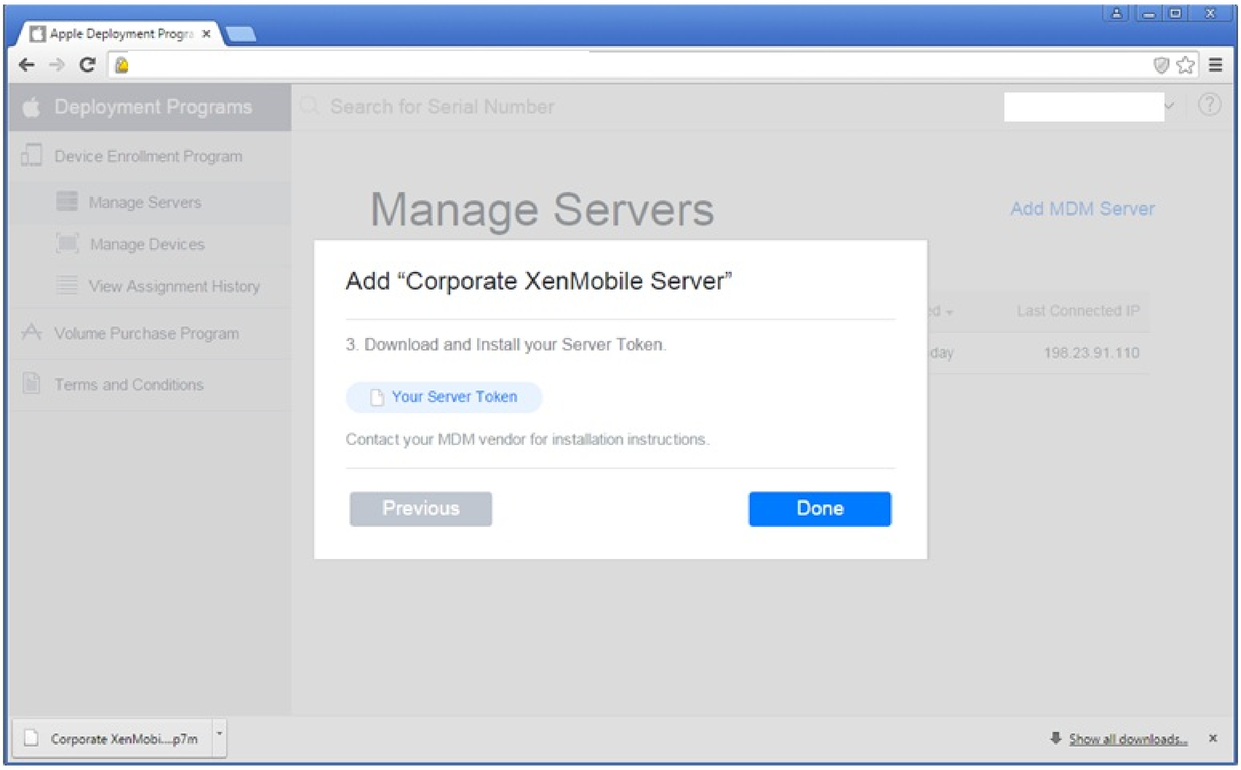
Add “Corporate XenMobile Server”

2. Upload Your Public Key.

Choose File... BulkEnrollmentP...

The public key certificate is used to encrypt the Authentication Token file for secure transfer to your MDM Server.

6. Click **Your Server Token** to generate a server token, which is downloaded from the browser, and then click **Done**.

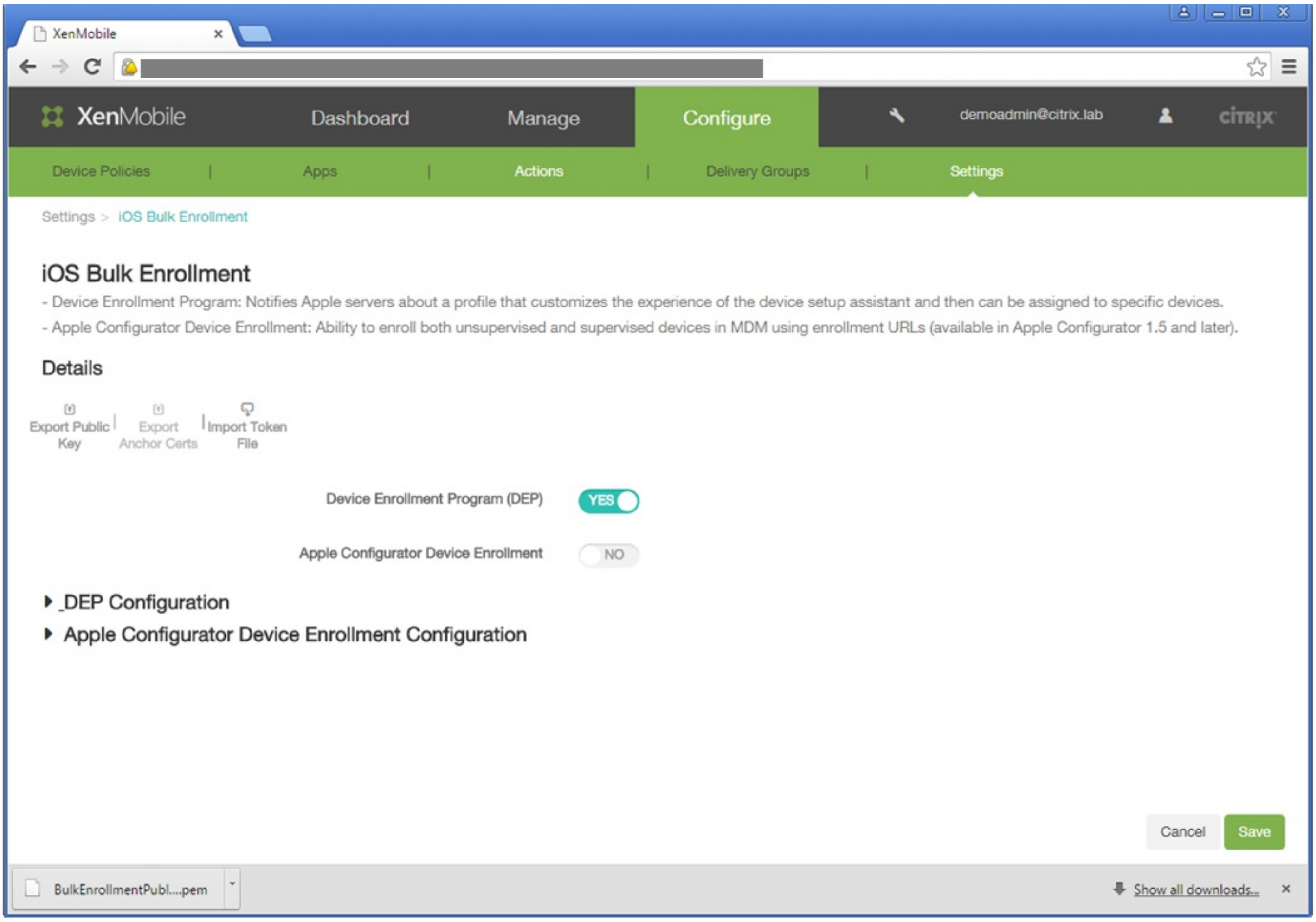


Add “Corporate XenMobile Server”

3. Download and Install your Server Token.

Contact your MDM vendor for installation instructions.

7. On the XenMobile console **iOS Bulk Enrollment** page, click **Import Token File** and then upload the token file you downloaded in the preceding step.



iOS Bulk Enrollment

- Device Enrollment Program: Notifies Apple servers about a profile that customizes the experience of the device setup assistant and then can be assigned to specific devices.

- Apple Configurator Device Enrollment: Ability to enroll both unsupervised and supervised devices in MDM using enrollment URLs (available in Apple Configurator 1.5 and later).

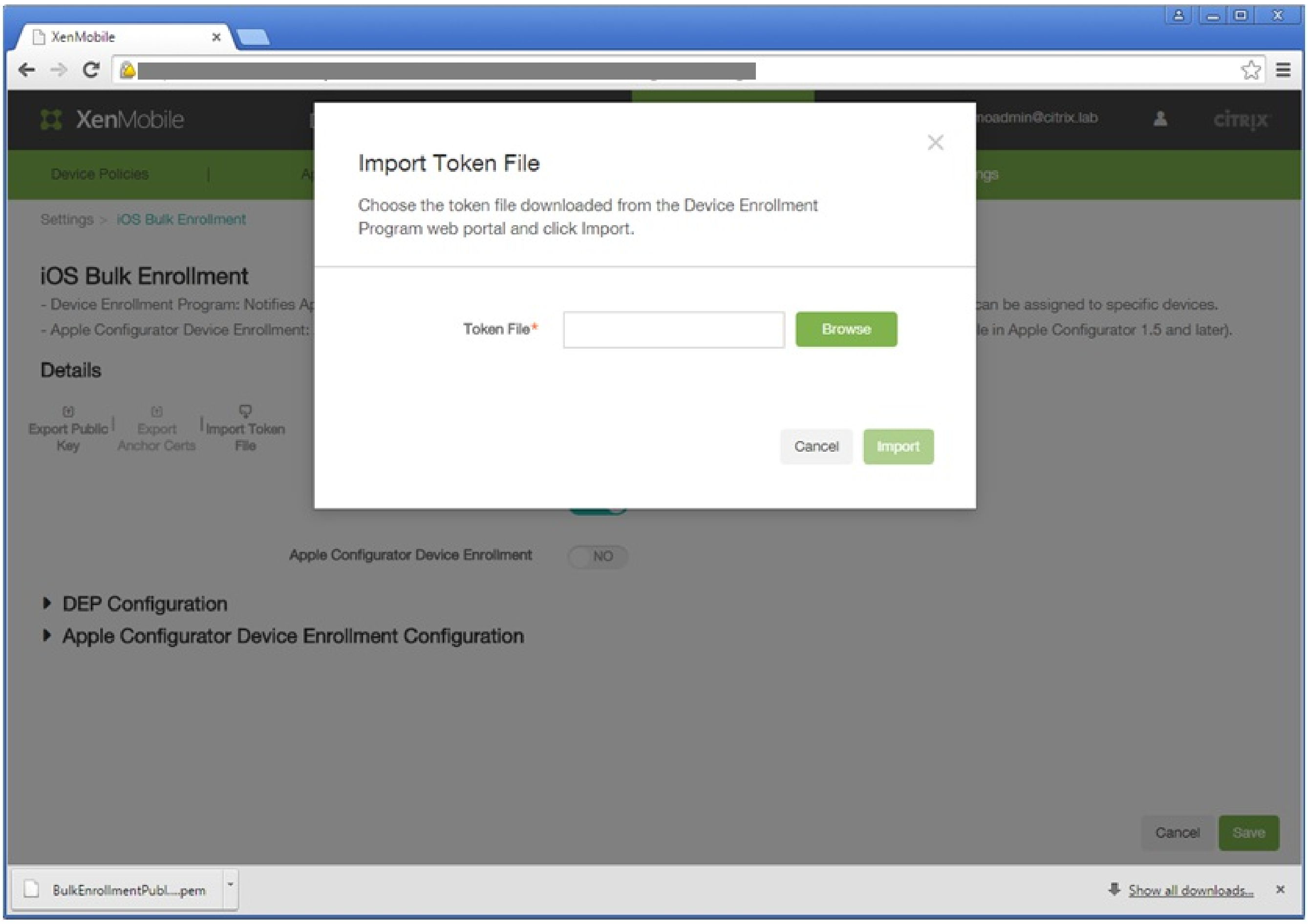
Details

Device Enrollment Program (DEP): YES

Apple Configurator Device Enrollment: NO

▸ DEP Configuration

▸ Apple Configurator Device Enrollment Configuration



iOS Bulk Enrollment

- Device Enrollment Program: Notifies A… …can be assigned to specific devices.

- Apple Configurator Device Enrollment: … …le in Apple Configurator 1.5 and later).

Details

DEP Configuration

Apple Configurator Device Enrollment Configuration

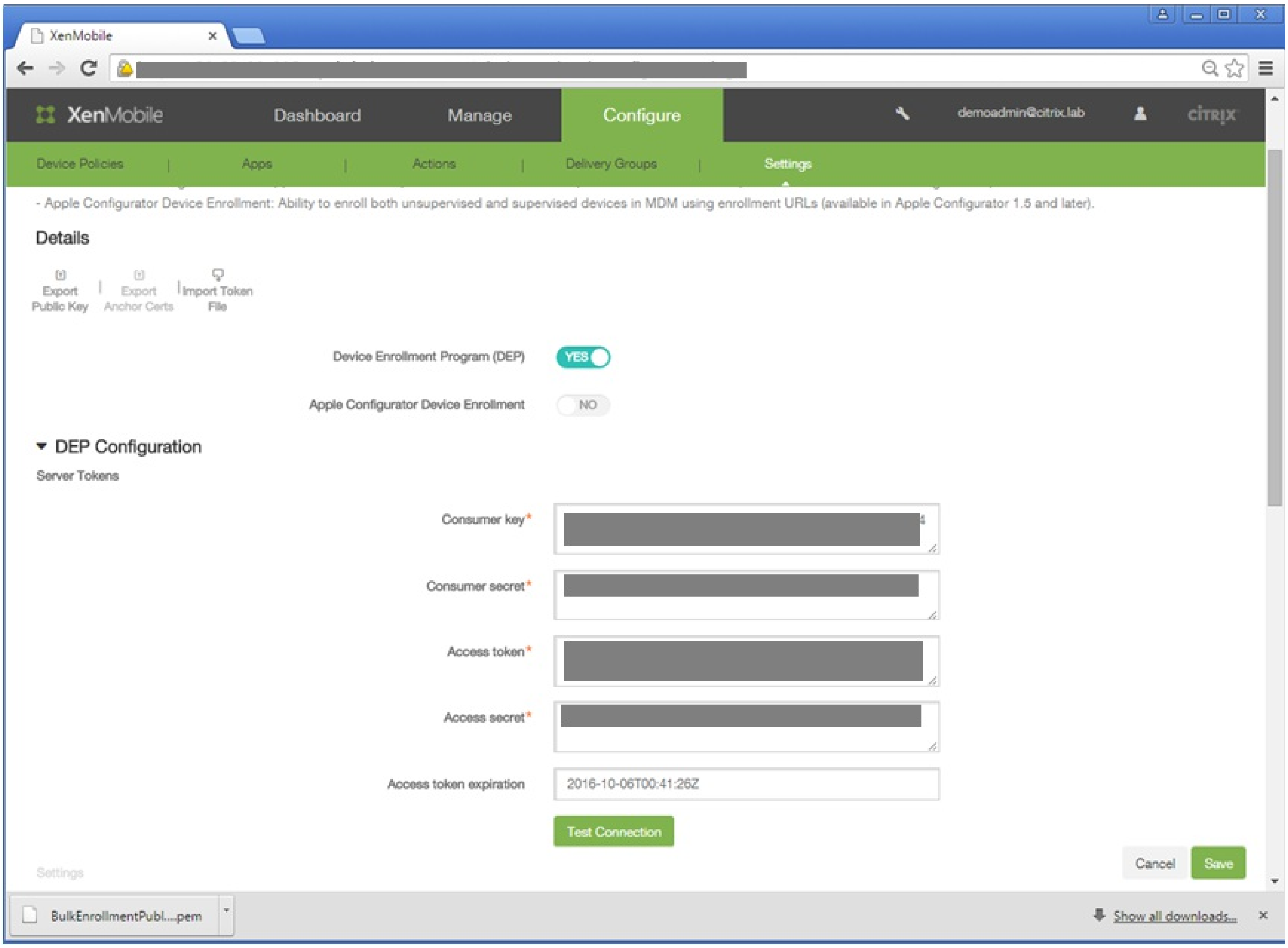
Import Token File

Choose the token file downloaded from the Device Enrollment Program web portal and click Import.

Token File*

Your Apple DEP token information appears in the XenMobile console after you import the token file.

8. Click **Test Connection** to verify the Apple DEP connection with XenMobile.



- Apple Configurator Device Enrollment: Ability to enroll both unsupervised and supervised devices in MDM using enrollment URLs (available in Apple Configurator 1.5 and later).

Details

Device Enrollment Program (DEP): YES

Apple Configurator Device Enrollment: NO

▾ DEP Configuration

Server Tokens

Consumer key*: [redacted]

Consumer secret*: [redacted]

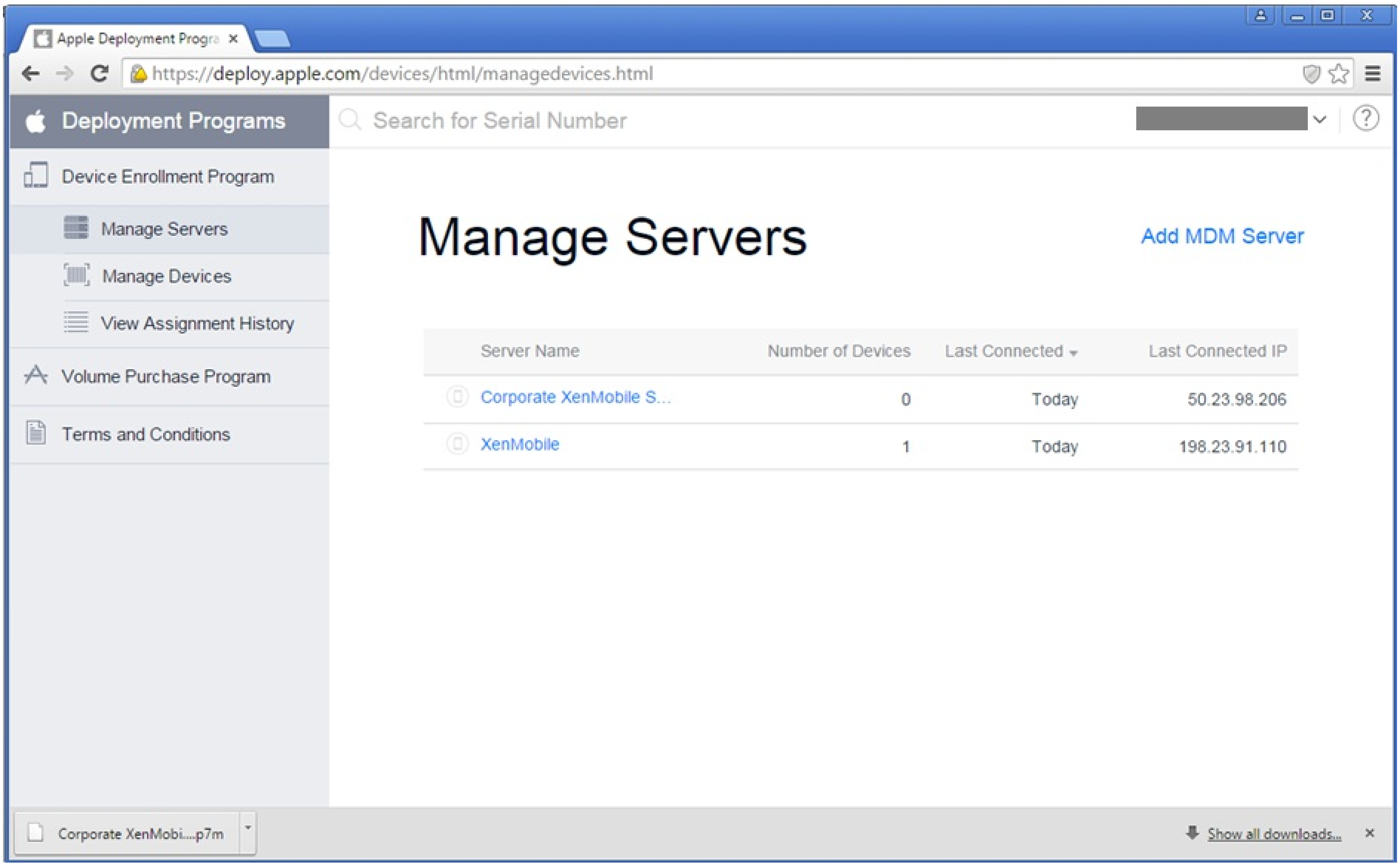
Access token*: [redacted]

Access secret*: [redacted]

Access token expiration: 2016-10-06T00:41:26Z

9. On the **iOS Bulk Enrollment** page, complete the additional settings, select the Apple DEP controls and policies you want to implement for your Apple DEP devices and then click **Save**.

The XenMobile server appears in the Apple DEP Portal.



Manage Servers

Server Name	Number of Devices	Last Connected	Last Connected IP
Corporate XenMobile S...	0	Today	50.23.98.206
XenMobile	1	Today	198.23.91.110

Ordering DEP-enabled devices

You can order DEP-enabled devices directly from Apple or DEP-enabled authorized resellers or carriers. To order from Apple, you need to provide your Apple Customer ID within the Apple DEP Portal to enable Apple to associate your device purchased with your Apple DEP account.

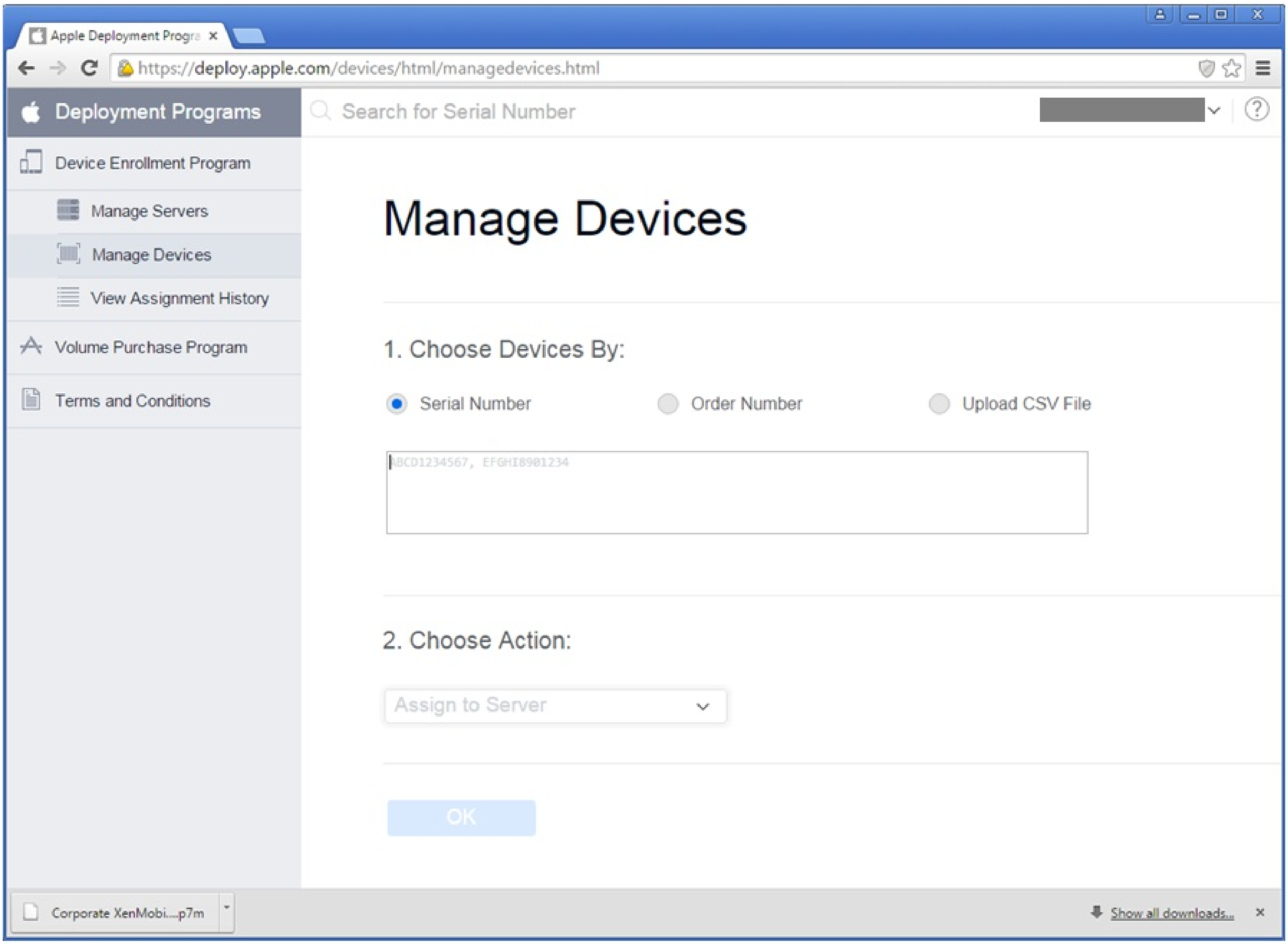
To order from your reseller or carrier, contact your Apple reseller or carrier to check if they participate in the Apple DEP. Ask for the resellers' Apple DEP ID when purchasing devices. You will need this information to add your Apple DEP reseller to your Apple DEP account. You will receive a DEP customer ID after adding the resellers' Apple DEP ID, when approved. Provide the DEP customer ID to the reseller, who will use the ID to submit information about your device purchases to Apple. For more information, see this Apple website.

Managing DEP-enabled devices

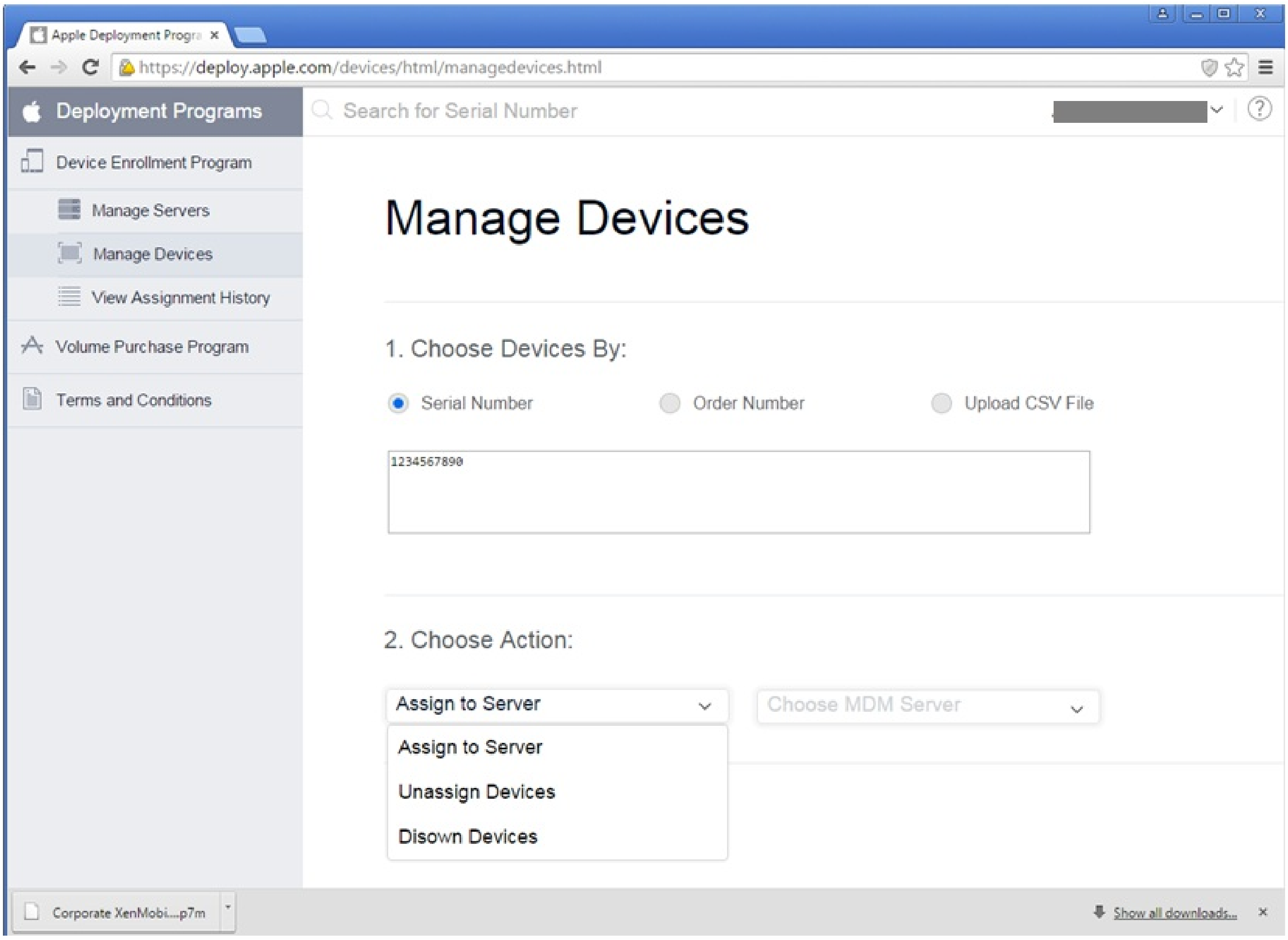
Follow these steps to associate devices with your XenMobile server within your Apple DEP account through the DEP Portal.

1. Log on to the Apple DEP Portal.

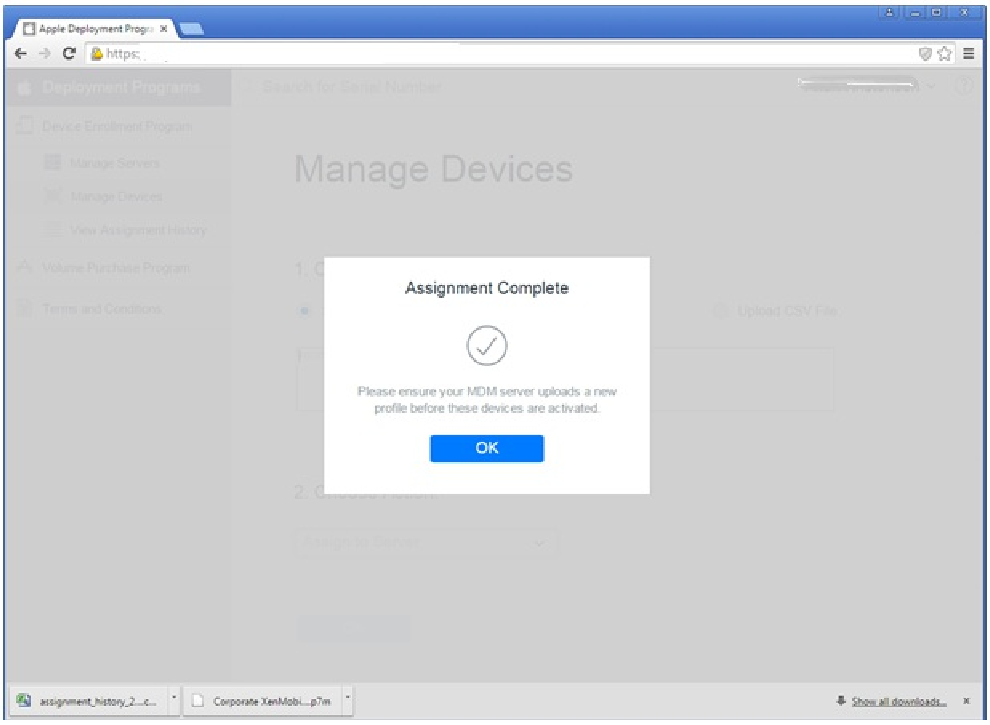
2. Click **Device Enrollment Program**, click **Manage Devices** and then in **Choose Devices By**, select the option for which you want to upload and define your Apple DEP-enabled devices - **Serial Number**, **Order Number**, or **Upload CSV File**.



3. Under **Choose Action**, to assign your devices to a XenMobile server, click **Assign to Server** and then in the list, click the name of your XenMobile server and then click **OK**.



Your Apple DEP devices are now associated with the selected XenMobile server.


Apple Deployment Progr
https:
Manage Devices
Assignment Complete
Please ensure your MDM server uploads a new profile before these devices are activated.
OK
assignment_history_2....c...
Corporate XenMobi....p7m
Show all downloads...

User experience enrolling an Apple DEP-enabled device

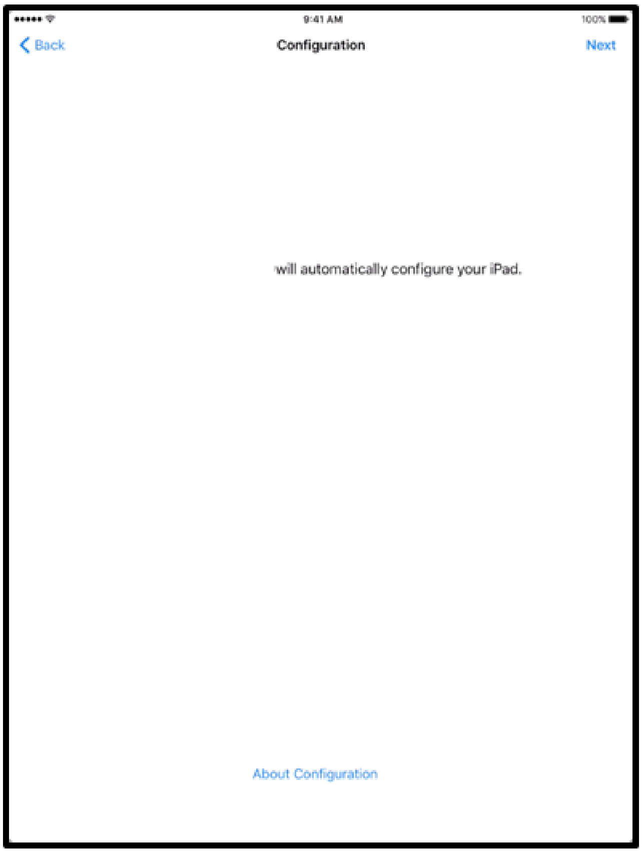
When users enroll an Apple DEP-enabled device, their experience is as follows.

1. Users start their Apple DEP-enabled device.

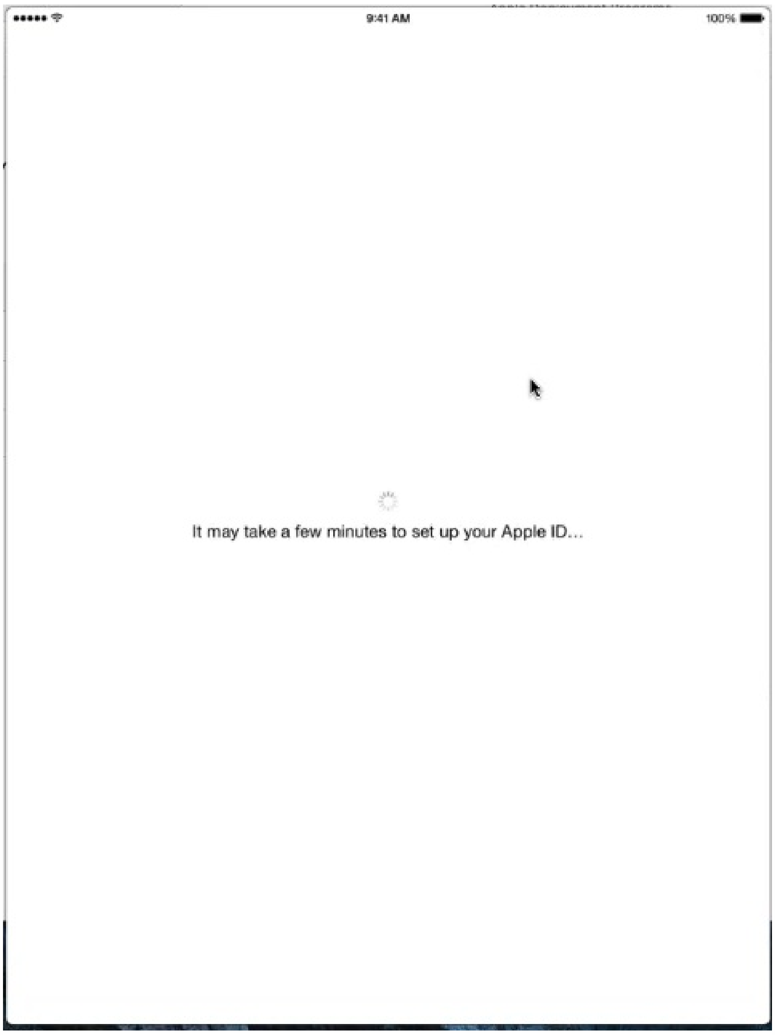
2. Users the configuration wizard to configure the initial settings on their iOS device.

3. The device automatically starts the XenMobile device enrollment process. Users follow the wizard to enroll the device into the XenMobile server associated with the Apple DEP-enabled device.

The Apple DEP enrollment process starts automatically as part of the initial IOS configuration flow for Apple DEP enabled devices.

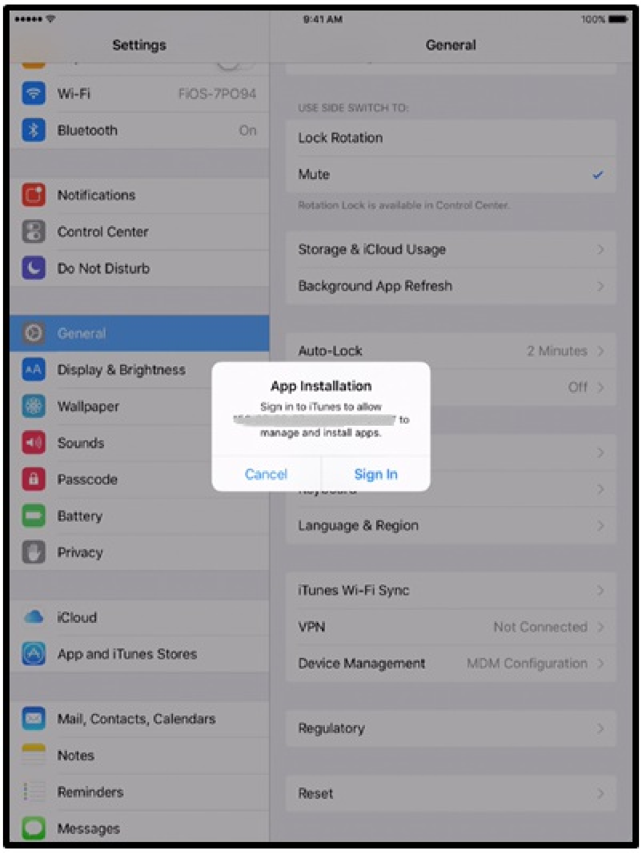


4. The Apple DEP configuration that you configured in the XenMobile console is delivered to the Apple DEP-enabled device. Users follow the wizard to configure the device.



It may take a few minutes to set up your Apple ID...

5. Users may be prompted to sign into iTunes so that Worx Home can be downloaded.



Wi-Fi FiOS-7PO94

Bluetooth On

Mute ✓

Auto-Lock 2 Minutes

Off

VPN Not Connected

Device Management MDM Configuration

App Installation

Sign in to iTunes to allow [redacted] to manage and install apps.

6. Users open Worx Home and enter their credentials. If required by the policy, users may be prompted to create and verify a Worx PIN.

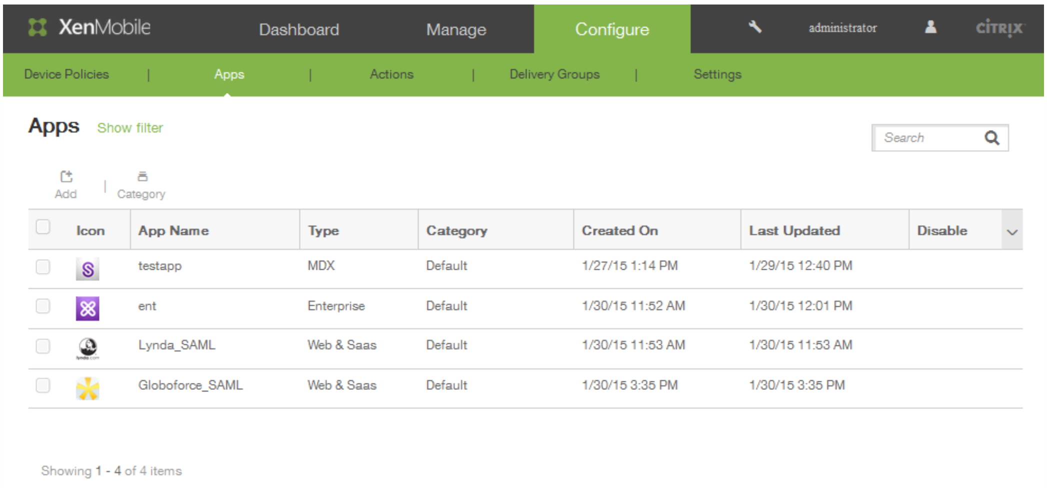
The remainder of the required apps are pushed down to the device.

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.



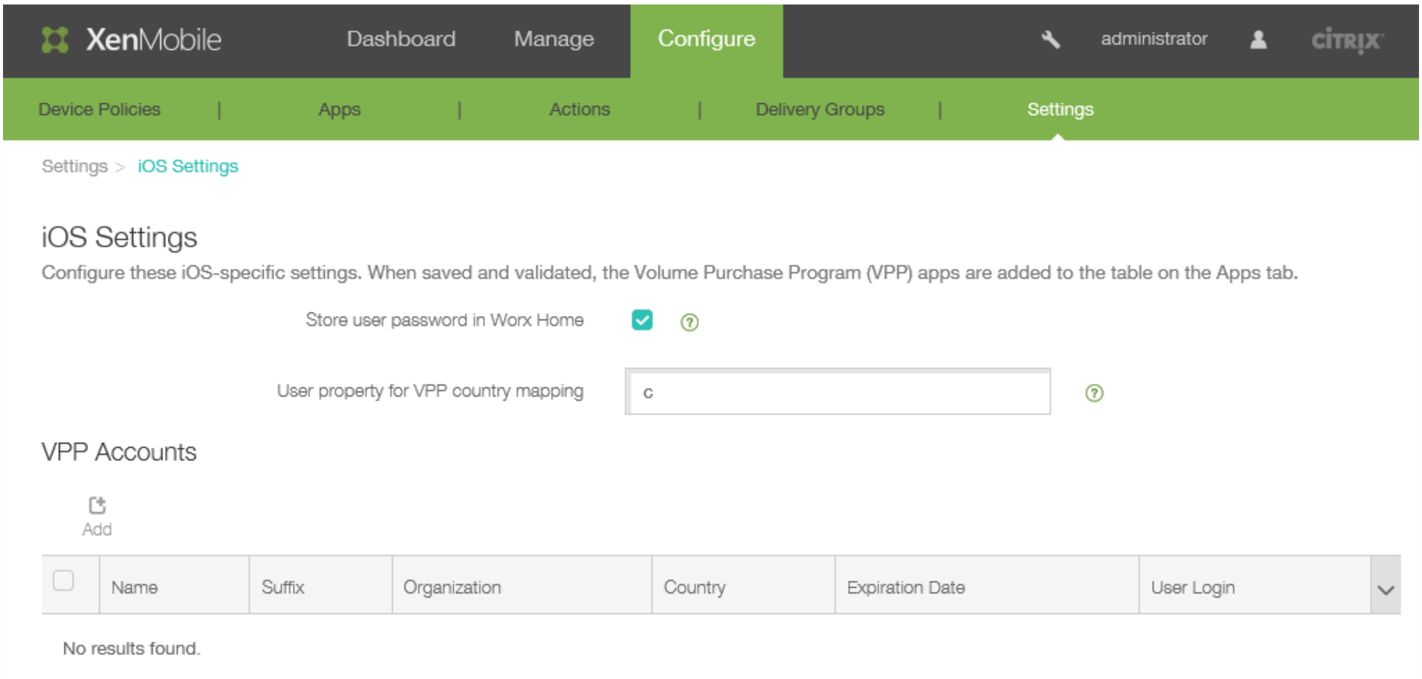
	Icon	App Name	Type	Category	Created On	Last Updated	Disable
□		testapp	MDX	Default	1/27/15 1:14 PM	1/29/15 12:40 PM	
□		ent	Enterprise	Default	1/30/15 11:52 AM	1/30/15 12:01 PM	
□		Lynda_SAML	Web & Saas	Default	1/30/15 11:53 AM	1/30/15 11:53 AM	
□		Globoforce_SAML	Web & Saas	Default	1/30/15 3:35 PM	1/30/15 3:35 PM	

Showing 1 - 4 of 4 items

To configure iOS VPP in XenMobile

In the XenMobile web console, click **Configure** > **Settings** > **More** > **iOS Settings**.

The iOS VPP configuration screen appears.



iOS Settings

Configure these iOS-specific settings. When saved and validated, the Volume Purchase Program (VPP) apps are added to the table on the Apps tab.

Store user password in Worx Home ☑

User property for VPP country mapping: c

VPP Accounts

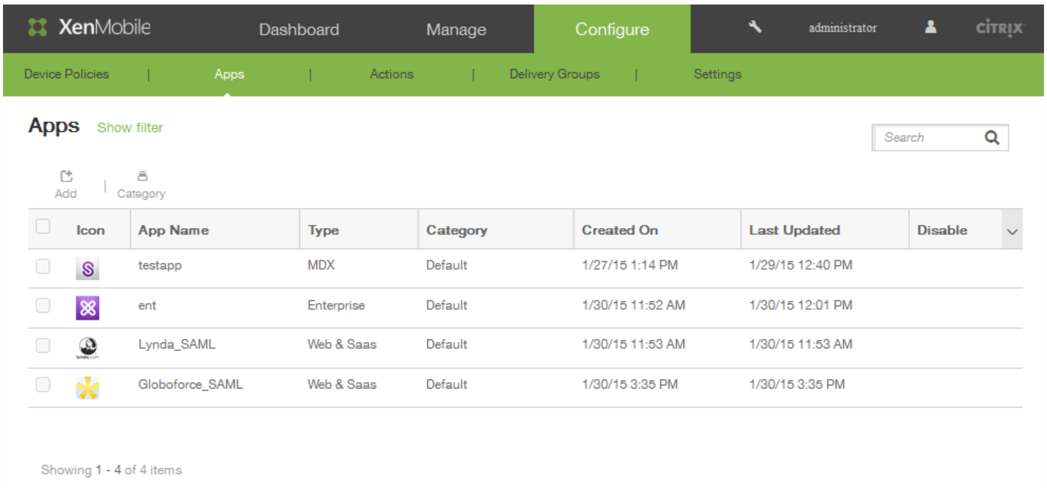
□	Name	Suffix	Organization	Country	Expiration Date	User Login

No results found.

1. 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.
2. 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.

3. Click **Add** under **VPP Accounts**.
4. Add a Name and Suffix.
5. In 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.
6. Click Save. The information is then displayed in the Apps table:



Apps

□	Icon	App Name	Type	Category	Created On	Last Updated	Disable
□		testapp	MDX	Default	1/27/15 1:14 PM	1/29/15 12:40 PM	
□		ent	Enterprise	Default	1/30/15 11:52 AM	1/30/15 12:01 PM	
□		Lynda_SAML	Web & Saas	Default	1/30/15 11:53 AM	1/30/15 11:53 AM	
□		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

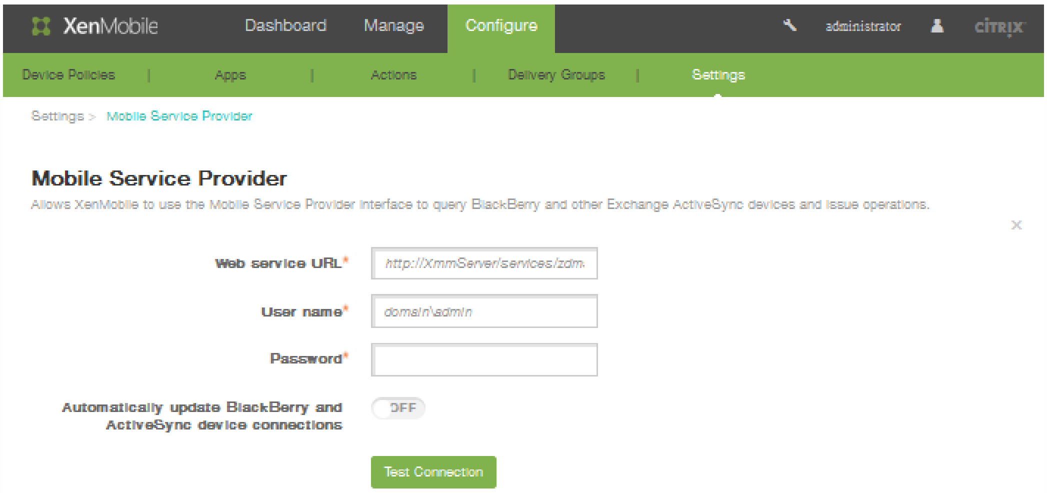
You can enable XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.

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.



Mobile Service Provider

Allows XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.

Web service URL* http://XmmServer/services/zdm

User name* domain\admin

Password*

Automatically update BlackBerry and ActiveSync device connections OFF

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.

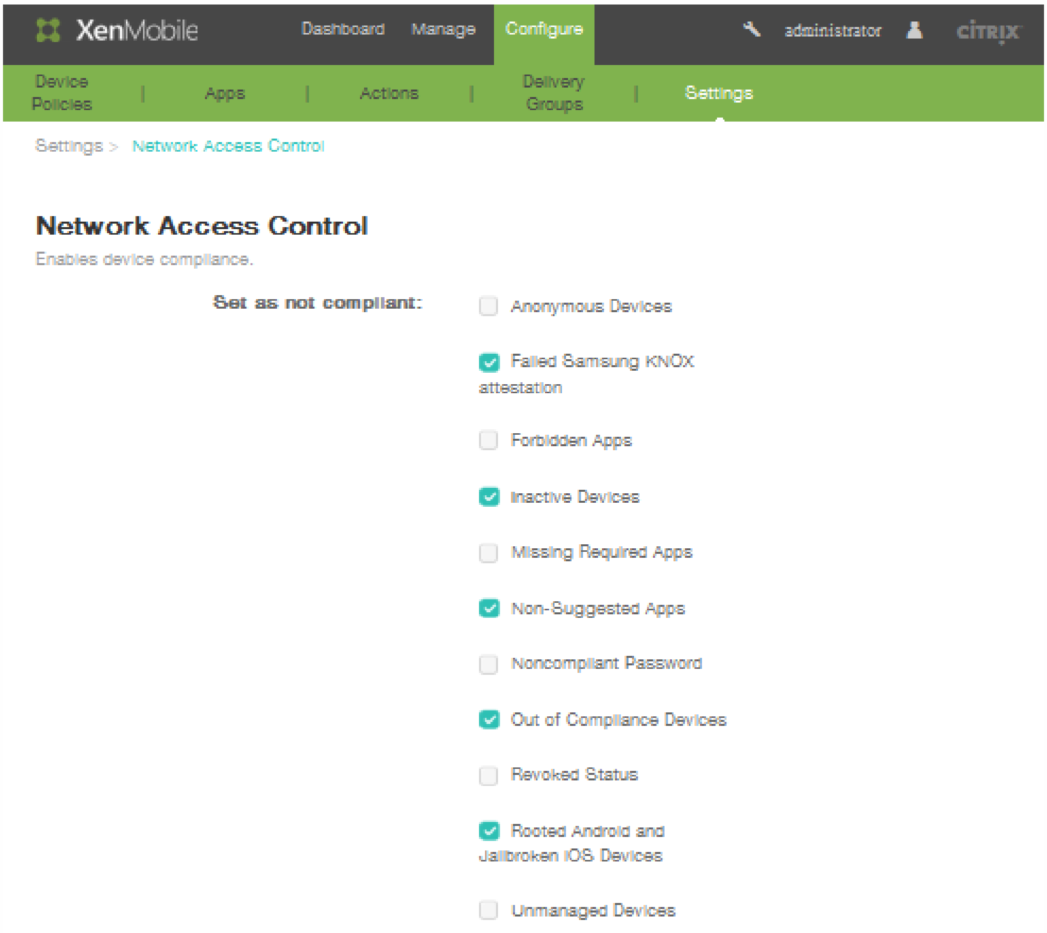
Send Android domain users to ActiveSync Gateway: Click **YES** to ensure that XenMobile sends Android device information to the ActiveSync Gateway. When this option is enabled, it ensures that XenMobile sends Android device information to the ActiveSync Gateway in the event that XenMobile does not have 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.



Network Access Control

Enables device compliance.

Set as not compliant:

- □ Anonymous Devices
- ☑ Failed Samsung KNOX attestation
- □ Forbidden Apps
- ☑ Inactive Devices
- □ Missing Required Apps
- ☑ Non-Suggested Apps
- □ Noncompliant Password
- ☑ Out of Compliance Devices
- □ Revoked Status
- ☑ Rooted Android and Jailbroken iOS Devices
- □ Unmanaged Devices

2. Select the checkboxes for the **Set as not compliant** filters you want to enable.
3. Click **Save**.

Samsung KNOX

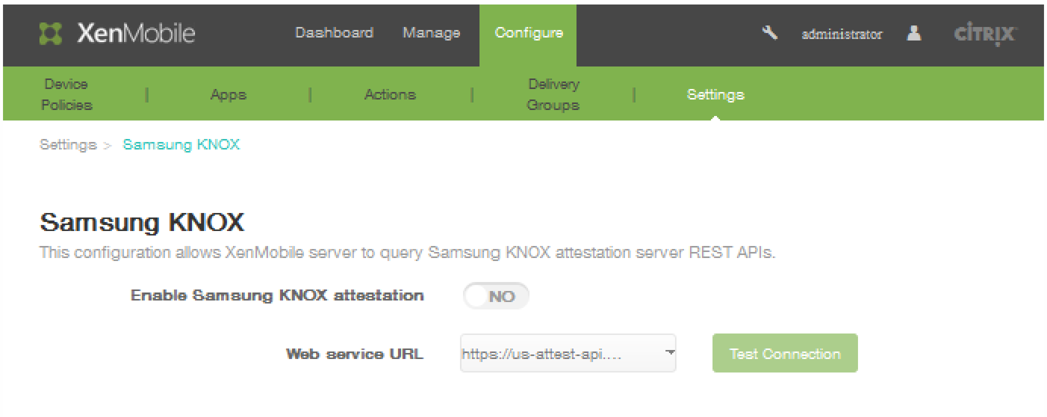
Feb 13, 2015

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.



Samsung KNOX

This configuration allows XenMobile server to query Samsung KNOX attestation server REST APIs.

Enable Samsung KNOX attestation: NO

Web service URL: https://us-attest-api....

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 Connectiion** to verify the connection.
5. Click **Save**.

Server Properties

May 04, 2016

XenMobile has over 100 properties that apply to server-wide operations. This article describes some of the more important server properties and also details how to add, edit, or delete server properties.

Server Property Definitions

Audit Log Cleanup Execution Time

The time to start the audit log cleanup, formatted as HH:MM AM/PM. Example: 04:00 AM. Defaults to **02:00 AM**.

Audit Log Cleanup Interval (in Days)

The number of days that the XenMobile server should retain the audit log. Defaults to **1**.

Audit Logger

If **False**, does not log user interface (UI) events. Defaults to **False**.

Audit Log Retention (in Days)

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

Deploy Log Cleanup (in Days)

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

Disable SSL Server Verification

If **True**, disables SSL server certificate validation when all of the following conditions are met: You have enabled certificate-based authentication on your XenMobile server, the Microsoft CA server is the certificate issuer, and your certificate has been signed by an internal CA whose root is not trusted by Xenmobile server. Defaults to **True**.

Inactivity Timeout in Minutes

The number of minutes after which an inactive administrator who used the XenMobile server Public API to access the XenMobile console or any third-party app, is logged out. A timeout of **0** means an inactive user remains logged in. Defaults to **5**.

NetScaler Single Sign-On

If **False**, disables the XenMobile callback feature during single signon from NetScaler to the XenMobile server. The callback feature is used to verify the NetScaler Gateway session ID, if the NetScaler Gateway configuration includes a callback URL. Defaults to **False**.

Session Log Cleanup (in Days)

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

Unauthenticated App Download for Android Devices

If **True**, you can download self-hosted apps to Android devices running Android for Work. This property is needed if the Android for Work option to provide a download URL in the Google Play Store statically is enabled. In that case, download URLs can't include a one-time ticket (defined by the **XAM One-Time Ticket** server property) which has the authentication token. Defaults to **False**.

Unauthenticated App Download for Windows Devices

Used only for older Worx Home versions which don't validate one-time tickets. If **False**, you can download unauthenticated apps from XenMobile to Windows devices. Defaults to **False**.

XAM One-Time Ticket

The number of milliseconds that a one-time authentication token (OTT) is valid for downloading an app. This property works in conjunction with the properties **Unauthenticated App download for Android** and **Unauthenticated App download for Windows**, which specify whether to allow un-authenticated app downloads. Defaults to **3600000**.

XenMobile MDM Self Help Portal console max inactive interval (minutes)

The number of minutes after which an inactive user is logged out of the XenMobile Self Help Portal. A timeout of **0** means an inactive user remains logged in. Defaults to **30**.

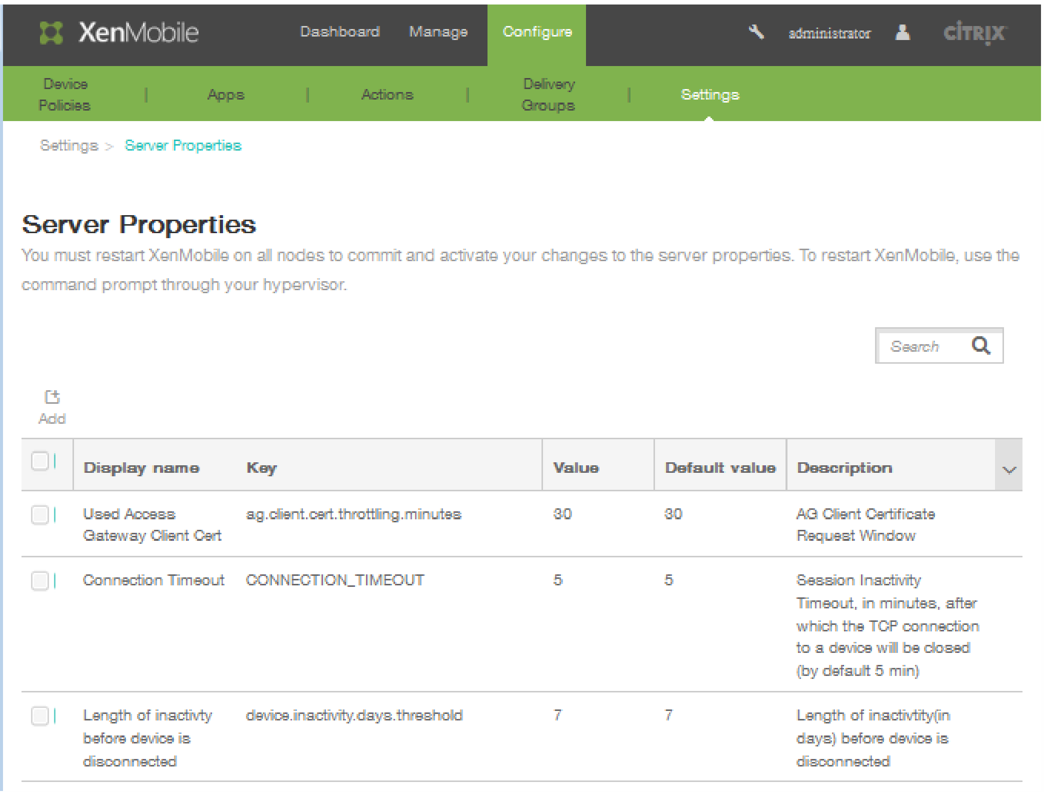
Adding, Editing, or Deleting Server Properties

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

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

To configure server properties in XenMobile

1. In the XenMobile web console, click Configure > Settings > More > Server Properties.
   The Server Properties configuration page appears.



Server Properties

You must restart XenMobile on all nodes to commit and activate your changes to the server properties. To restart XenMobile, use the command prompt through your hypervisor.

□	Display name	Key	Value	Default value	Description
□	Used Access Gateway Client Cert	ag.client.cert.throttling.minutes	30	30	AG Client Certificate Request Window
□	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)
□	Length of inactivty before device is disconnected	device.inactivity.days.threshold	7	7	Length of inactivtity(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.

Configuring XenMobile Server Mode

Mar 09, 2016

The XenMobile server mode is the value set in Server Properties. You can set the value to MAM, MDM, or ENT corresponding to app management, device management, or app and device management. Set the Server Mode property according to how you want devices to register, as noted in the table below. Server Mode defaults to ENT, regardless of license type.

For information about setting the server mode, see Server Properties.

If you have a XenMobile MDM Edition license, the effective server mode is always MDM regardless of how you set the server mode in Server Properties. If you have an MDM Edition license, you cannot enable app management by setting the server mode to either MAM or ENT.

Your licenses are this Edition	You want devices to register in this mode	Set Server Mode property to
Enterprise / Advanced	MDM mode	MDM
Enterprise / Advanced	MDM+MAM mode	ENT
MDM	MDM mode	MDM

The *effective server mode* is a combination of the license type and server mode. For an MDM license, the effective server mode is always MDM, regardless of the server mode setting. For Enterprise and Advanced licenses, the effective server mode matches the server mode, if the server mode is ENT or MDM. If the server mode is MAM, the effective server mode is ENT.

The effective server mode is added to the server log every time a license is activated or deleted and when the server mode is changed in Server Properties. For information about creating and viewing log files, see XenMobile Support and Maintenance.

SysLog

Apr 11, 2016

You can configure XenMobile to send log files to a systems log (syslog) server. You need the server host name or IP address.

Syslog is a standard logging protocol with two components: an auditing module (which runs on the appliance) and a server, which can run on a remote system. The Syslog protocol uses the user data protocol (UDP) for data transfer. Admin events and User events will be recorded.

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:

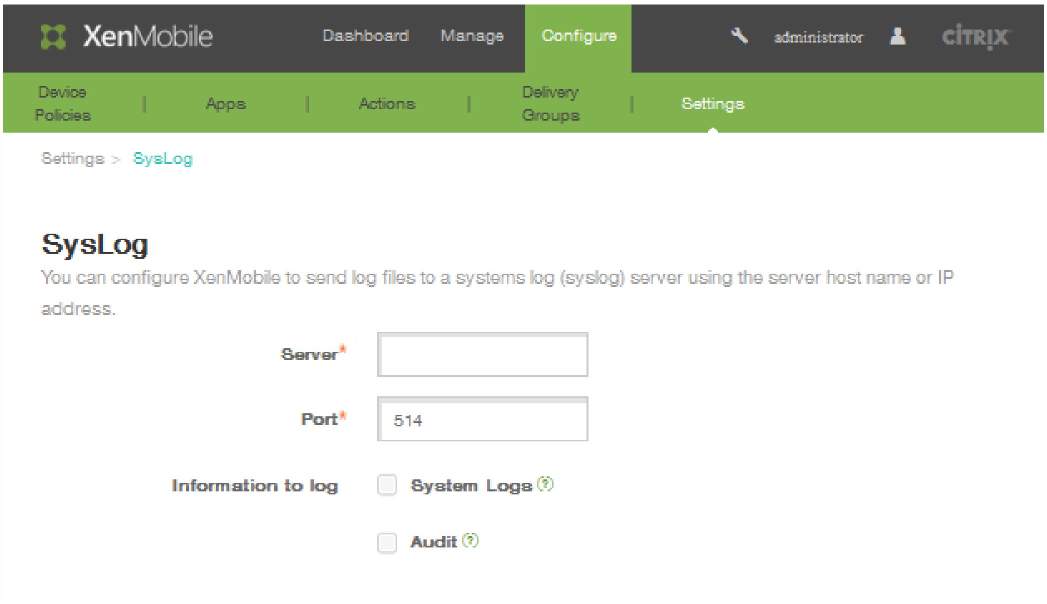
- The IP address of the appliance that generated the log message
- A time stamp
- The message type
- The log level associated with an event (Critical, Error, Notice, Warning, Informational, Debug, Alert, or Emergency)
- The message information

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 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.



SysLog

You can configure XenMobile to send log files to a systems log (syslog) server using the server host name or IP address.

Server*

Port* 514

Information to log □ System Logs

□ Audit

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**.

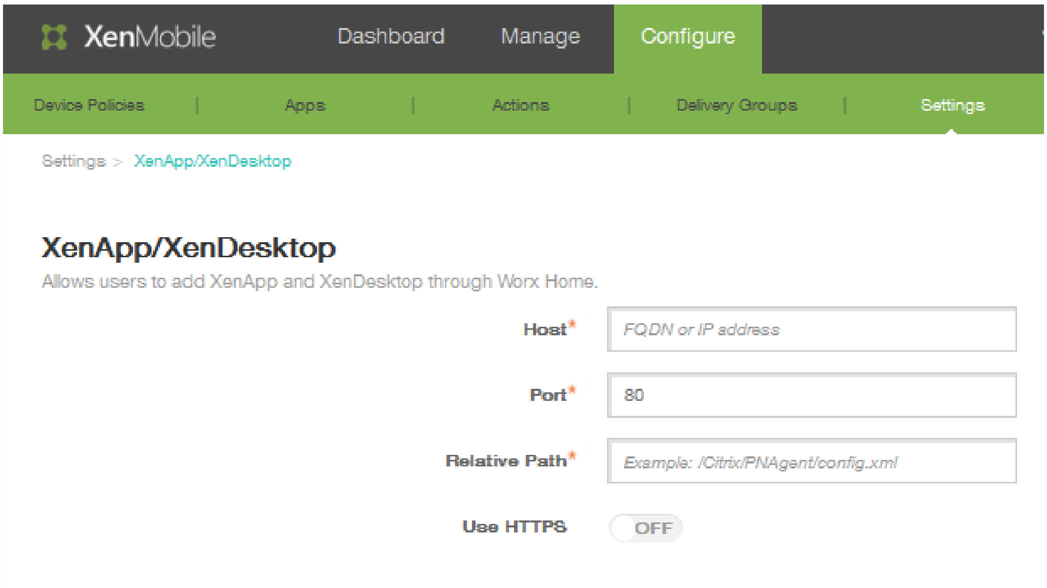
To configure XenApp and XenDesktop

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.



XenApp/XenDesktop

Allows users to add XenApp and XenDesktop through Worx Home.

Host* FQDN or IP address

Port* 80

Relative Path* Example: /Citrix/PNAgent/config.xml

Use HTTPS 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**.

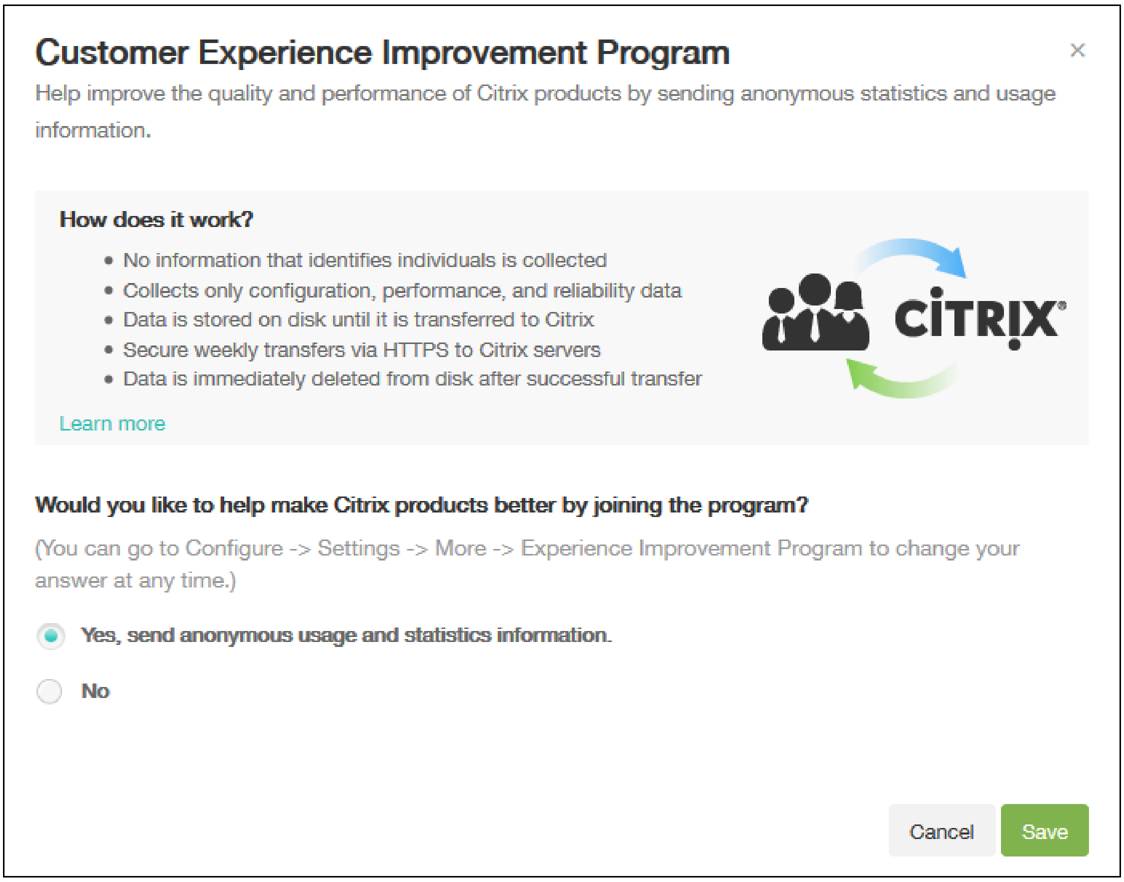
Customer Experience Improvement Program

Jul 16, 2015

The Citrix Customer Experience Improvement Program (CEIP) gathers anonymous configuration and usage data from XenMobile and automatically sends the data to Citrix. This data helps Citrix improve the quality, reliability, and performance of XenMobile. Participation in the CEIP is completely voluntary. When you first install XenMobile, or when you install an update, you have the option to participate in the CEIP. When you opt-in, data is typically collected on a weekly basis, and performance and usage data is collected hourly. The data is stored on disk and transferred securely via HTTPS to Citrix weekly. You can change whether you participate in the CEIP in the XenMobile console. For more information on the CEIP, see About the Citrix Customer Experience Improvement Program (CEIP).

CEIP when installing or updating XenMobile

The first time you install XenMobile or when you do an update, you see the following dialog box, in which you select whether to participate and then click **Save**.



Customer Experience Improvement Program

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer

Learn more

Would you like to help make Citrix products better by joining the program?

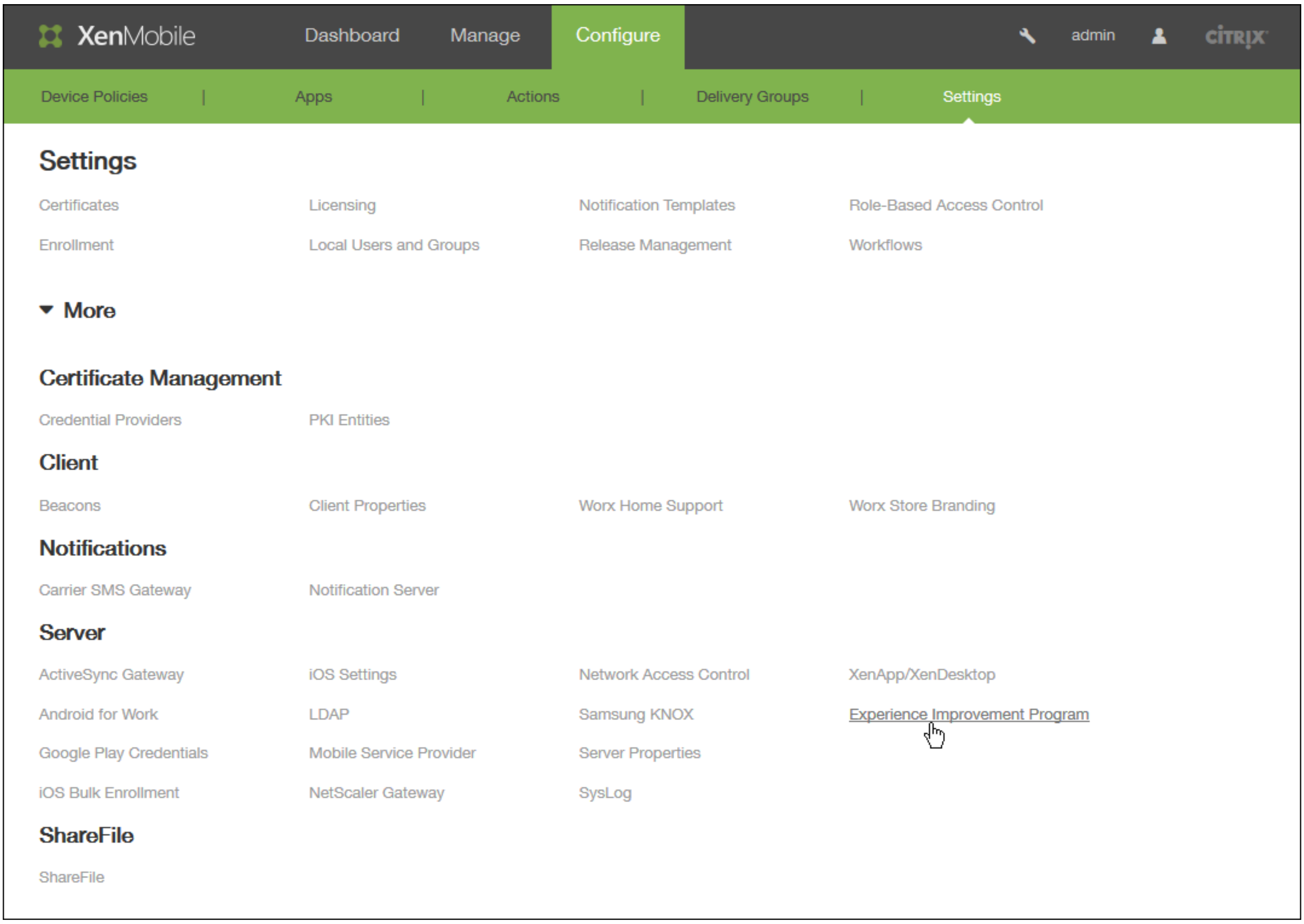
(You can go to Configure -> Settings -> More -> Experience Improvement Program to change your answer at any time.)

● Yes, send anonymous usage and statistics information.

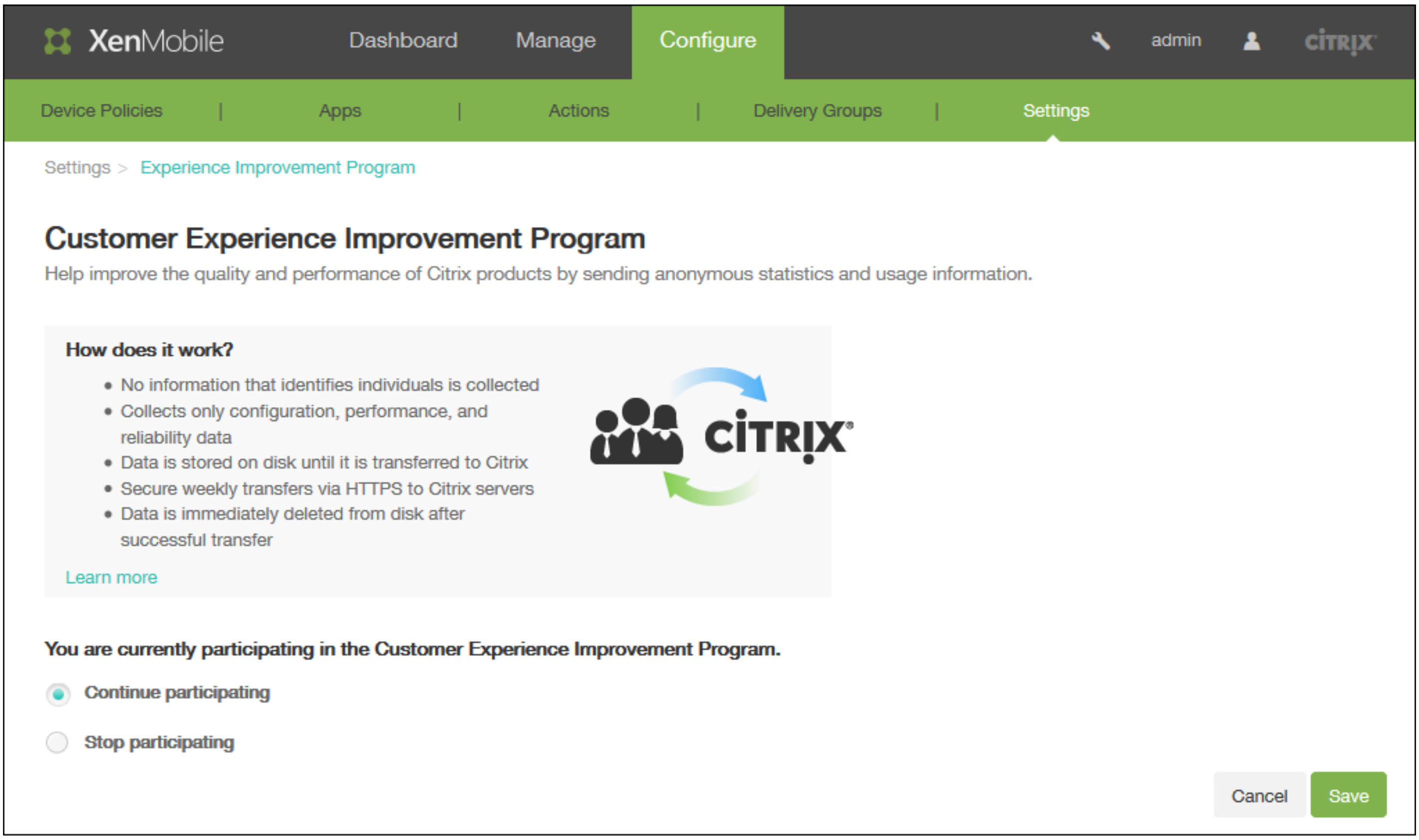
○ No

Changing your CEIP participation setting

1. To change your CEIP participation setting, in the XenMobile console, click **Configure -> Settings**. The **Settings** page appears.



2. Under **Server**, click **Experience Improvement Program**. The **Customer Experience Improvement Program** page appears. The exact page you see depends on whether you are currently participating in the CEIP. The following figure shows the page of a participating user.



Customer Experience Improvement Program

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer

Learn more

You are currently participating in the Customer Experience Improvement Program.

● Continue participating

○ Stop participating

2. If you are currently participating in the CEIP and want to stop, click **Stop participating**.

3. If you are not currently participating in the CEIP and want to start, click **Start participating**.

4. Click **Save**.

Bulk enrollment of iOS devices

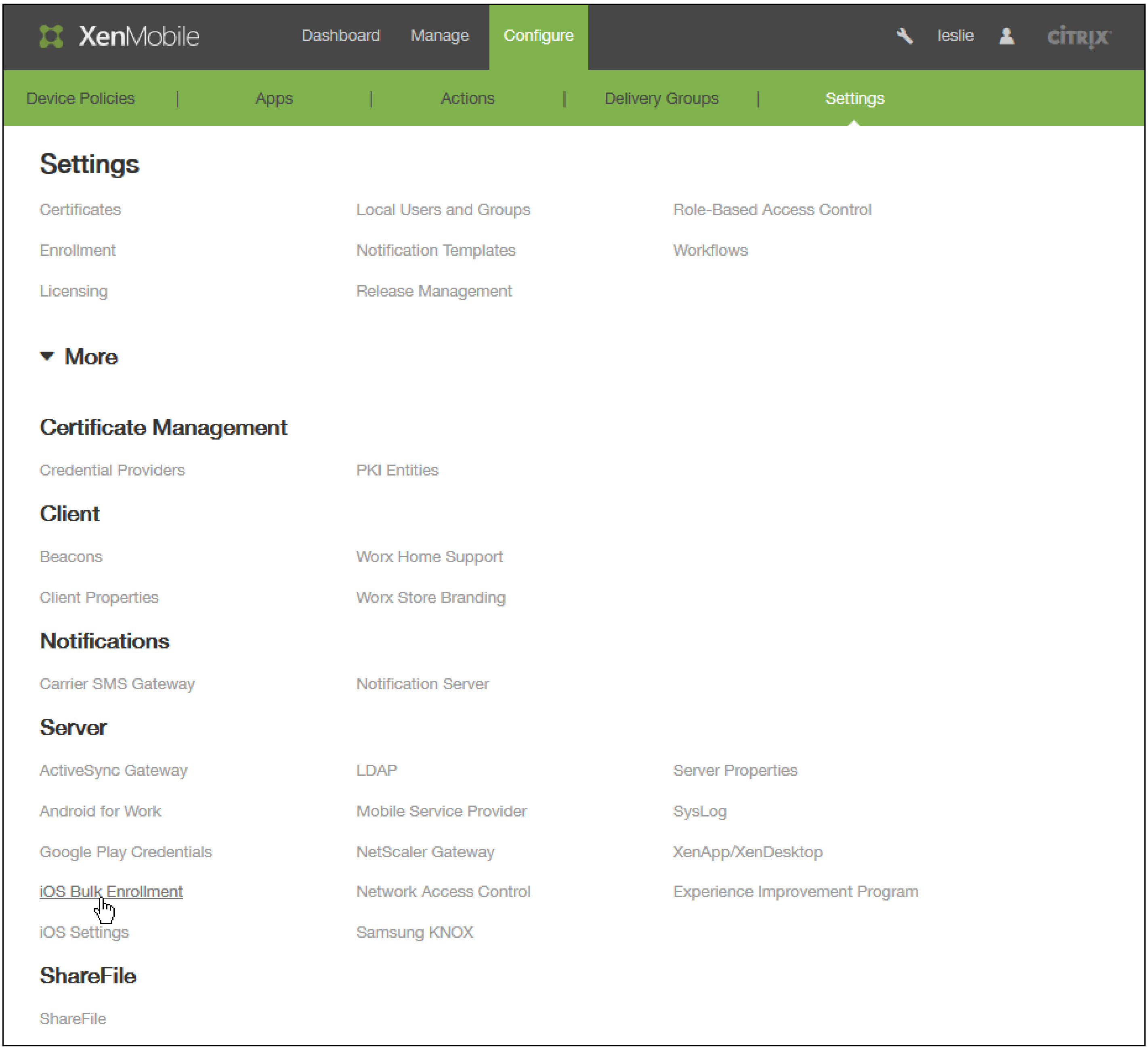
Jul 14, 2015

You can enroll large numbers of iOS devices in XenMobile in two ways. You can use Apple's Device Enrollment Program (DEP) to enroll devices that you buy directly from Apple or from a participating Apple Authorized Reseller or carrier; or you can use the Apple Configurator to enroll devices regardless of whether they were purchased directly from Apple.

With DEP, you do not have to touch or prepare the devices; you submit device serial numbers or purchase order numbers through DEP and the devices are configured and enrolled in XenMobile. After the devices are enrolled, you can give them to users who can start using them right out of the box. In addition, when you set up devices with DEP, you can eliminate some of the Setup Assistant steps that users would otherwise have to complete when they first start their devices. For more information on setting up DEP, see Apple's Device Enrollment Program page.

With the Apple Configurator, you attach devices to an Apple computer running OS X 10.7.2 or later and the Apple Configurator app. You prepare the devices and configure policies through the Apple Configurator. After you provision the devices with the required policies, the first time the devices connect to XenMobile, the policies are applied and you can start managing the devices. For more information on using the Apple Configurator, see Apple's Apple Configurator page.

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



XenMobile Dashboard Manage Configure leslie

Device Policies | Apps | Actions | Delivery Groups | Settings

Settings

Certificates
Enrollment
Licensing
Local Users and Groups
Notification Templates
Release Management
Role-Based Access Control
Workflows

▼ More

Certificate Management

Credential Providers
PKI Entities

Client

Beacons
Client Properties
Worx Home Support
Worx Store Branding

Notifications

Carrier SMS Gateway
Notification Server

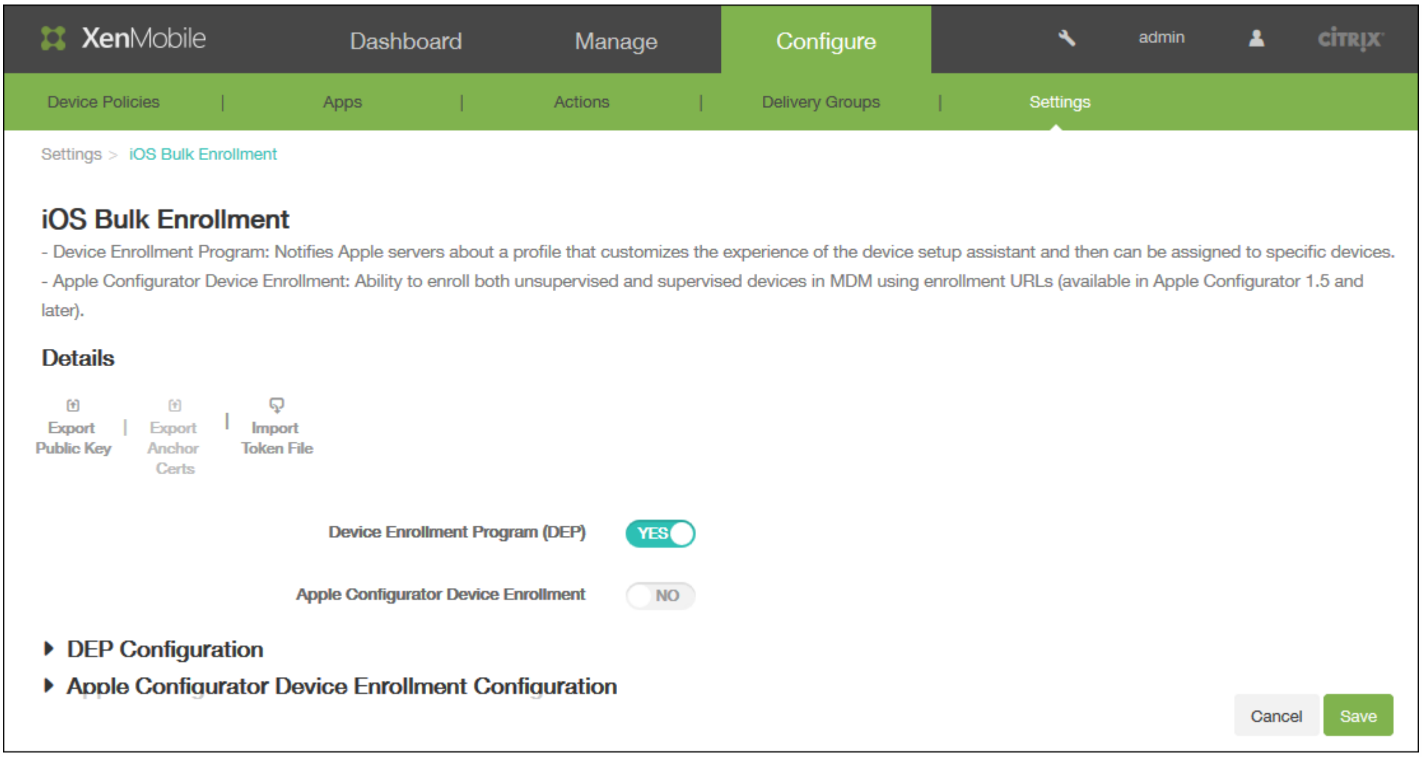
Server

ActiveSync Gateway
Android for Work
Google Play Credentials
iOS Bulk Enrollment
iOS Settings
LDAP
Mobile Service Provider
NetScaler Gateway
Network Access Control
Samsung KNOX
Server Properties
SysLog
XenApp/XenDesktop
Experience Improvement Program

ShareFile

ShareFile

2. Under **Server**, click **iOS Bulk Enrollment**. The **iOS Bulk Enrollment** page appears.



iOS Bulk Enrollment

- Device Enrollment Program: Notifies Apple servers about a profile that customizes the experience of the device setup assistant and then can be assigned to specific devices.
- Apple Configurator Device Enrollment: Ability to enroll both unsupervised and supervised devices in MDM using enrollment URLs (available in Apple Configurator 1.5 and later).

Details

Device Enrollment Program (DEP) YES

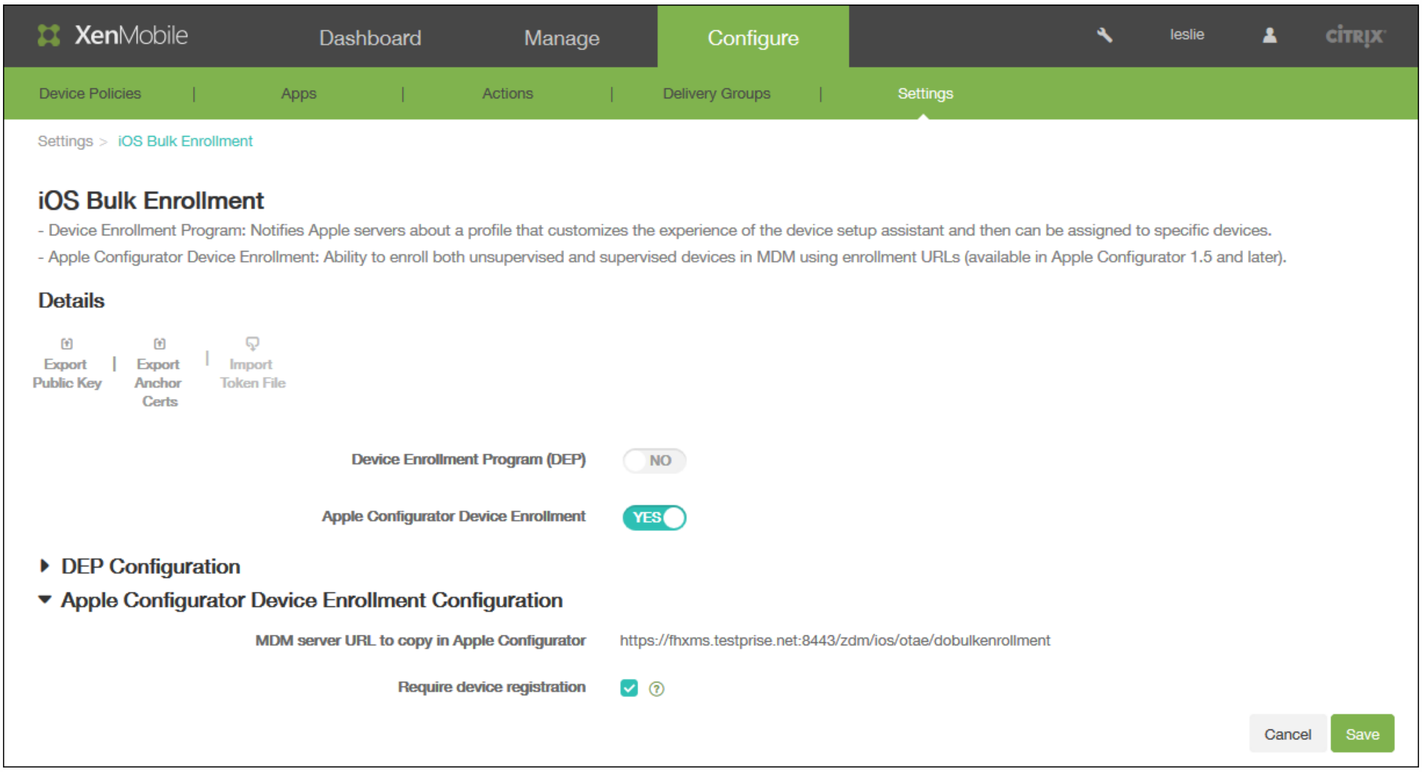
Apple Configurator Device Enrollment NO

▸ DEP Configuration

▸ Apple Configurator Device Enrollment Configuration

If you are configuring DEP settings, see Configuring DEP settings; if you are configuring Apple Configurator settings, see Configuring Apple Configurator settings.

Configuring Apple Configurator settings



iOS Bulk Enrollment

- Device Enrollment Program: Notifies Apple servers about a profile that customizes the experience of the device setup assistant and then can be assigned to specific devices.
- Apple Configurator Device Enrollment: Ability to enroll both unsupervised and supervised devices in MDM using enrollment URLs (available in Apple Configurator 1.5 and later).

Details

Device Enrollment Program (DEP) NO

Apple Configurator Device Enrollment YES

▸ DEP Configuration

▾ Apple Configurator Device Enrollment Configuration

MDM server URL to copy in Apple Configurator https://fhxms.testprise.net:8443/zdm/ios/otae/dobulkenrollment

Require device registration ☑

1. Set **Device Enrollment Program** to **No**.

2. Set **Apple Configurator Device Enrollment** to **Yes**.

3. Expand **Apple Configurator Device Enrollment Configuration** and note and configure these settings:

- **MDM server URL to copy in Apple Configurator**: This read-only field is the URL for the XenMobile server that communicates with Apple, and which you copy and paste into the Apple Configurator in a later step.
- **Require device registration**: Selecting this setting requires you to add the configured devices to the **Devices** tab in XenMobile manually or through a CSV file before they can be enrolled. This ensures that no unknown devices can enroll. The default is to require adding devices.

> ### Note
>
> If the XenMobile server is using a trusted SSL certificate, skip the next step.

4. Click **Export Anchor Certs** and save the certchain.pem file to the OS X keychain (login or System).

5. Start the Apple Configurator and go to **Prepare -> Setup -> Configure Settings ...**

6. In the **Device Enrollment** setting, paste the MDM server URL from step 5 into the **MDM server URL** field in the Configurator.

7. In the **Device Enrollment** setting, copy the Root Certificate Authority and SSL Servers Certificate Authority to the **Anchor** certificates, if XenMobile is not using a trusted SSL certificate.

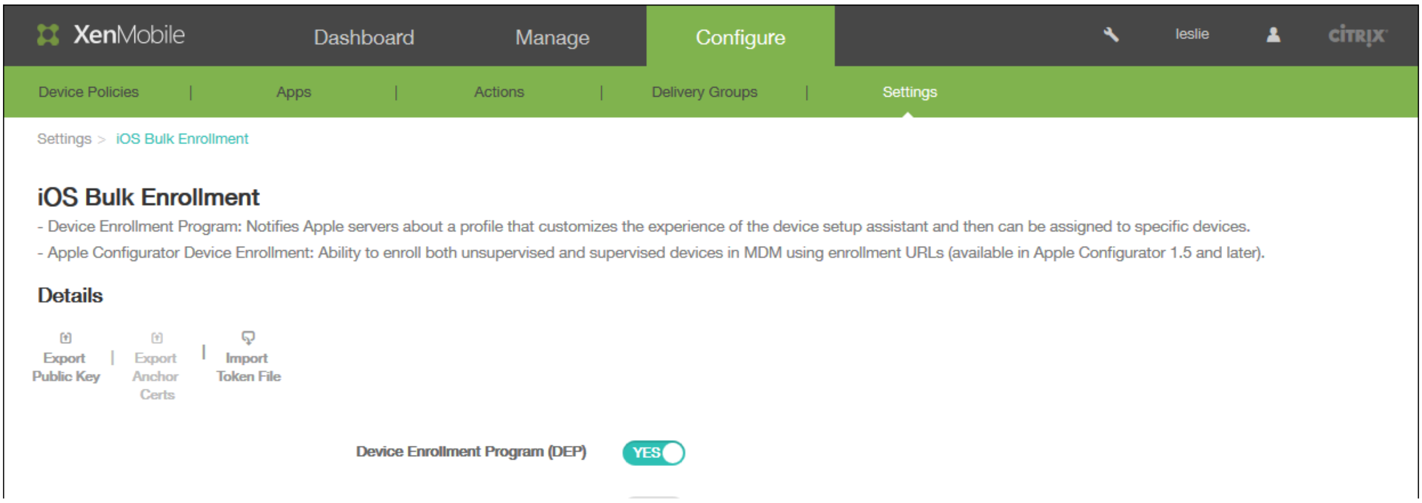
8. Use a Dock Connector to USB cable to connect devices to the Mac running the Apple Configurator to simultaneously configure up to 30 connected devices. If you do not have a Dock Connector, use one or more powered USB 2.0 high-speed hubs to connect the devices.

9. Click **Prepare**. For more information on preparing devices with the Apple Configurator, see the Apple Configurator help page Prepare devices.

10. In the Apple Configurator, configure the device policies you require.

11. As each device is prepared, turn it on to start the iOS Setup Assistant, which prepares the device for first-time use.

Configuring DEP settings

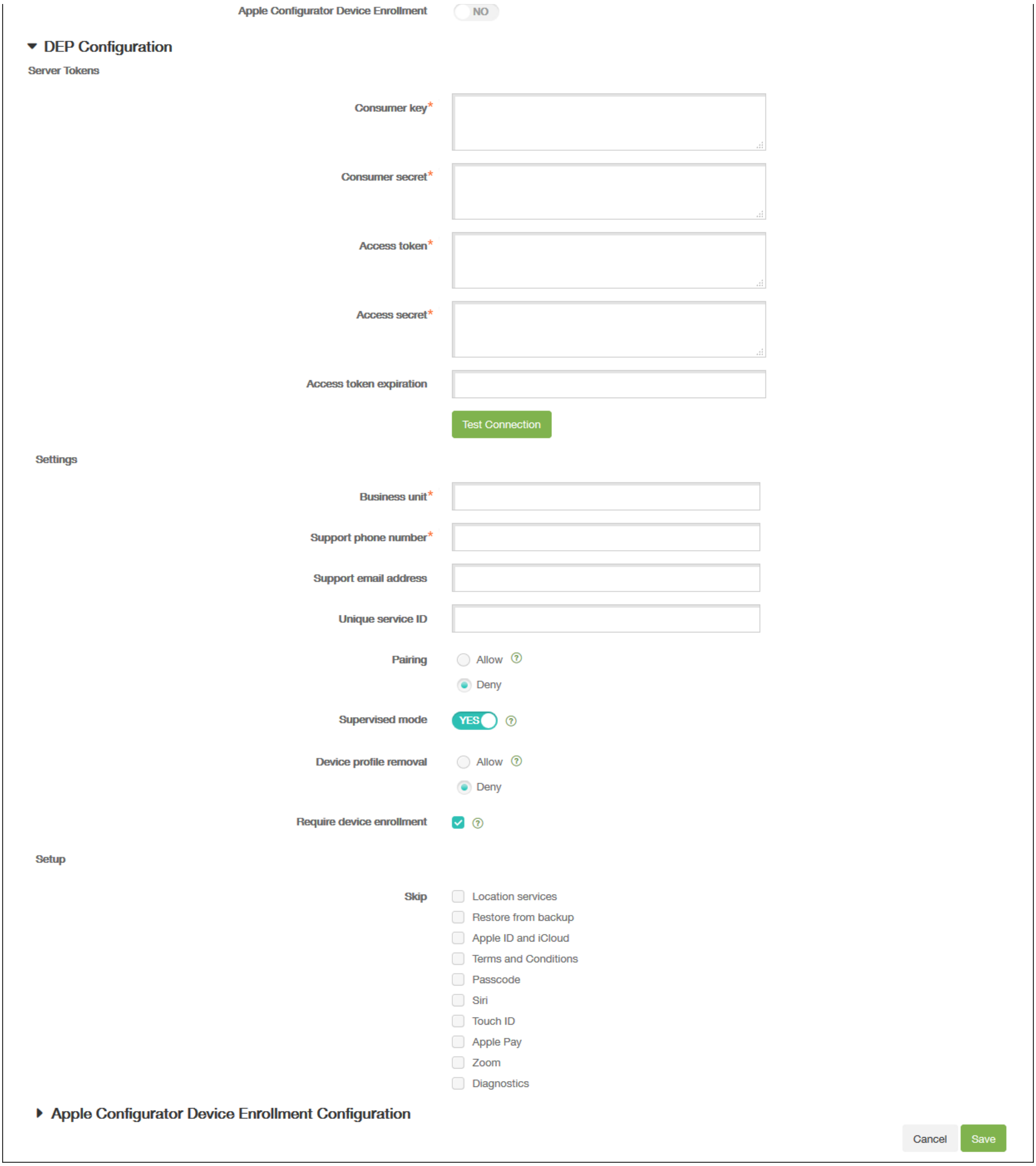


iOS Bulk Enrollment

- Device Enrollment Program: Notifies Apple servers about a profile that customizes the experience of the device setup assistant and then can be assigned to specific devices.
- Apple Configurator Device Enrollment: Ability to enroll both unsupervised and supervised devices in MDM using enrollment URLs (available in Apple Configurator 1.5 and later).

Details

Device Enrollment Program (DEP) YES



Apple Configurator Device Enrollment NO

▾ DEP Configuration

Server Tokens

Consumer key*

Consumer secret*

Access token*

Access secret*

Access token expiration

Test Connection

Settings

Business unit*

Support phone number*

Support email address

Unique service ID

Pairing ○ Allow ● Deny

Supervised mode YES

Device profile removal ○ Allow ● Deny

Require device enrollment ☑

Setup

Skip
- □ Location services
- □ Restore from backup
- □ Apple ID and iCloud
- □ Terms and Conditions
- □ Passcode
- □ Siri
- □ Touch ID
- □ Apple Pay
- □ Zoom
- □ Diagnostics

▸ Apple Configurator Device Enrollment Configuration

Cancel Save

1. Set **Device Enrollment Program** to **Yes**.

2. Set **Apple Configurator Device Enrollment** to **No**.

3. Expand **DEP Configuration** and configure these settings:

Server Tokens

- **Consumer key**:
- **Consumer secret**:
- **Access token**:
- **Access secret**:
- **Access token expiration**:

Settings

- **Business unit**:
- **Support phone number**:
- **Support email address**:
- **Unique service ID**:
- **Pairing**: Select whether to allow devices enrolled through DEP to be managed through iTunes and the Apple Configurator. The default is **Allow**.
- **Supervised mode**: Must be set to **Yes** if you are using the Apple Configurator to manage DEP enrolled devices. The default is **Yes**.
- **Device profile removal**: Select whether to allow devices to use a profile that can be removed remotely. The default is **Allow**.
- **Require device enrollment**: Select whether to require users to enroll their devices. The default is to not require enrollment.

Setup

Select the iOS Setup Assistant steps that your users will *not* have to use when they start their devices for first time use.

- **Skip**
  - **Location**: Set up the location service on the device.
  - **Restore from backup**: Set up the device as new or from an iCloud or iTunes backup.
  - **Apple ID and iCloud**: Set up an Apple ID and iCloud account for the device.
  - **Terms and Conditions**: Require user to accept terms and conditions for use of the device.
  - **Passcode**: Create a passcode for the device.
  - **Siri**: Use or not use Siri on the device.
  - **Touch ID**: Set up Touch ID on the device.
  - **Apple Play**: Set up access to Apple Play on the device.
  - **Zoom**: Set up the display resolution (either standard or zoomed).
  - **Diagnostics**: Set up whether to share crash data and usage statistics with Apple.

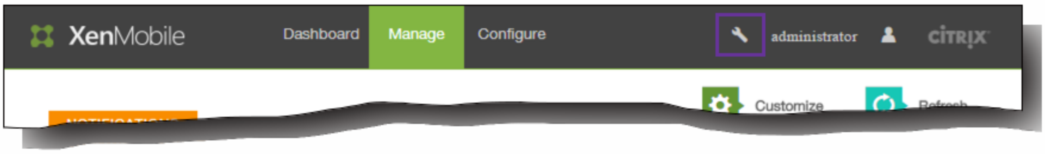
XenMobile Support and Maintenance

Jun 01, 2016

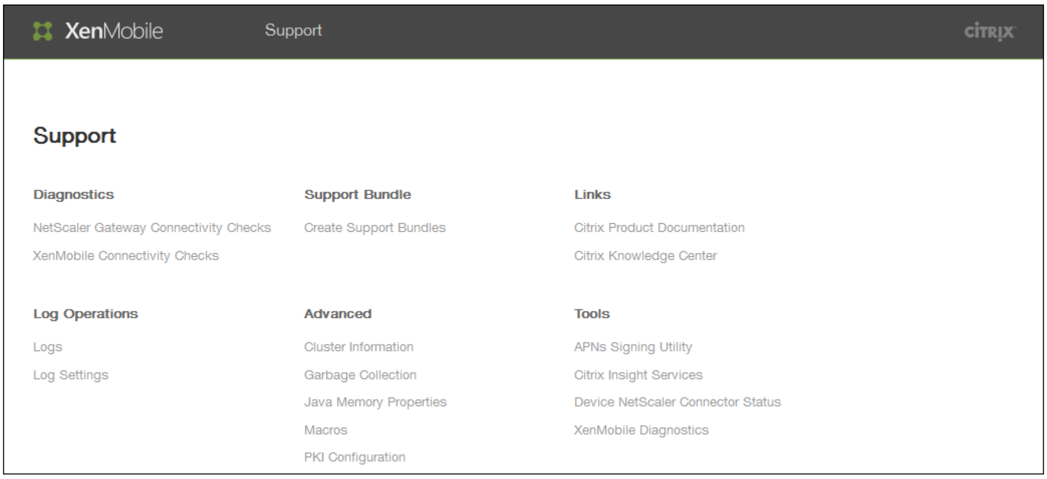
Use the XenMobile Support page to access a number of support-related information and tools. You can also carry out actions from the command-line interface. For details, see XenMobile Command-Line Interface Options.

To access the Support page

In the XenMobile console, click the wrench icon 🔧 in the upper-right corner of the console:



The Support page page appears in a separate browser tab:


XenMobile Support CITRIX

Support

Diagnostics

NetScaler Gateway Connectivity Checks

XenMobile Connectivity Checks

Support Bundle

Create Support Bundles

Links

Citrix Product Documentation

Citrix Knowledge Center

Log Operations

Logs

Log Settings

Advanced

Cluster Information

Garbage Collection

Java Memory Properties

Macros

PKI Configuration

Tools

APNs Signing Utility

Citrix Insight Services

Device NetScaler Connector Status

XenMobile Diagnostics

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.

XenMobile REST API reference

Sep 23, 2015

You can call REST services by using any REST client and the XenMobile REST API to call services that are exposed through the XenMobile console. The API does not require you to sign on to the XenMobile console to call any service described in this article.

You need one of the following permissions to access the REST API:

- Public API access permission set as part of role-based access configuration (for more information on setting role-based access, see Configuring roles with RBAC)
- Super user permission

You can invoke REST API services by using REST client.

To invoke REST API services

The following are examples of how to invoke the REST API using each of the preceding methods.

> ## Note
>
> In the following examples, change the host name and port number to match your environment.

Using a REST client

This example uses the Advanced REST client for Chrome.

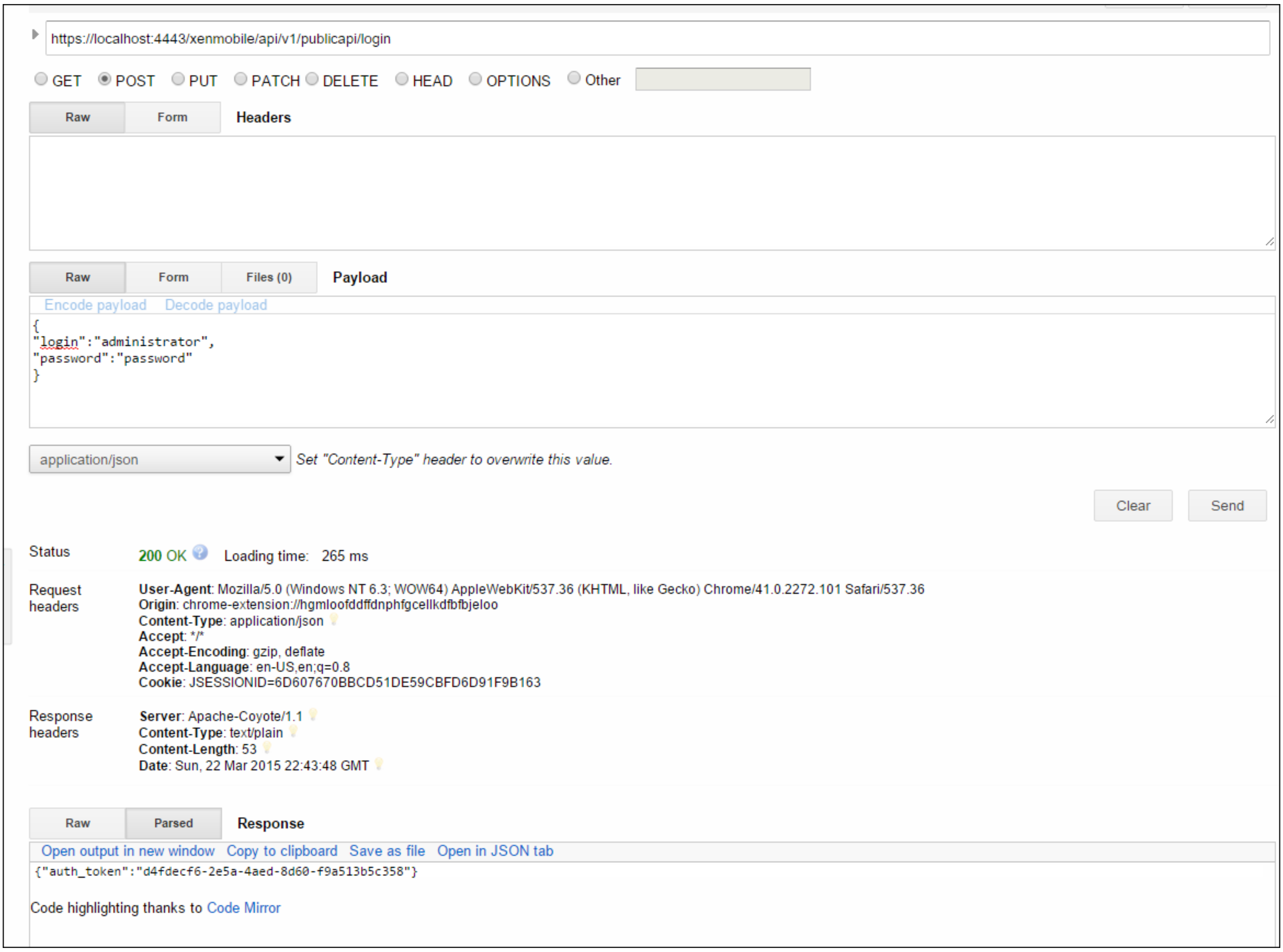
Login

URL: https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login

Request: { "login":"administrator", "password":"password" }

Method type: POST

Content type: application/json



https://localhost:4443/xenmobile/api/v1/publicapi/login
○ GET ● POST ○ PUT ○ PATCH ○ DELETE ○ HEAD ○ OPTIONS ○ Other
Raw
Form
Headers
Raw
Form
Files (0)
Payload
Encode payload
Decode payload

```
{
"login":"administrator",
"password":"password"
}
```

application/json
Set "Content-Type" header to overwrite this value.
Clear
Send

Status 200 OK Loading time: 265 ms

Request headers
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.101 Safari/537.36
Origin: chrome-extension://hgmloofddffdnphfgcellkdfbfbjeloo
Content-Type: application/json
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=6D607670BBCD51DE59CBFD6D91F9B163

Response headers
Server: Apache-Coyote/1.1
Content-Type: text/plain
Content-Length: 53
Date: Sun, 22 Mar 2015 22:43:48 GMT

```
{"auth_token":"d4fdecf6-2e5a-4aed-8d60-f9a513b5c358"}
```

Code highlighting thanks to Code Mirror

Get Delivery Groups by filter

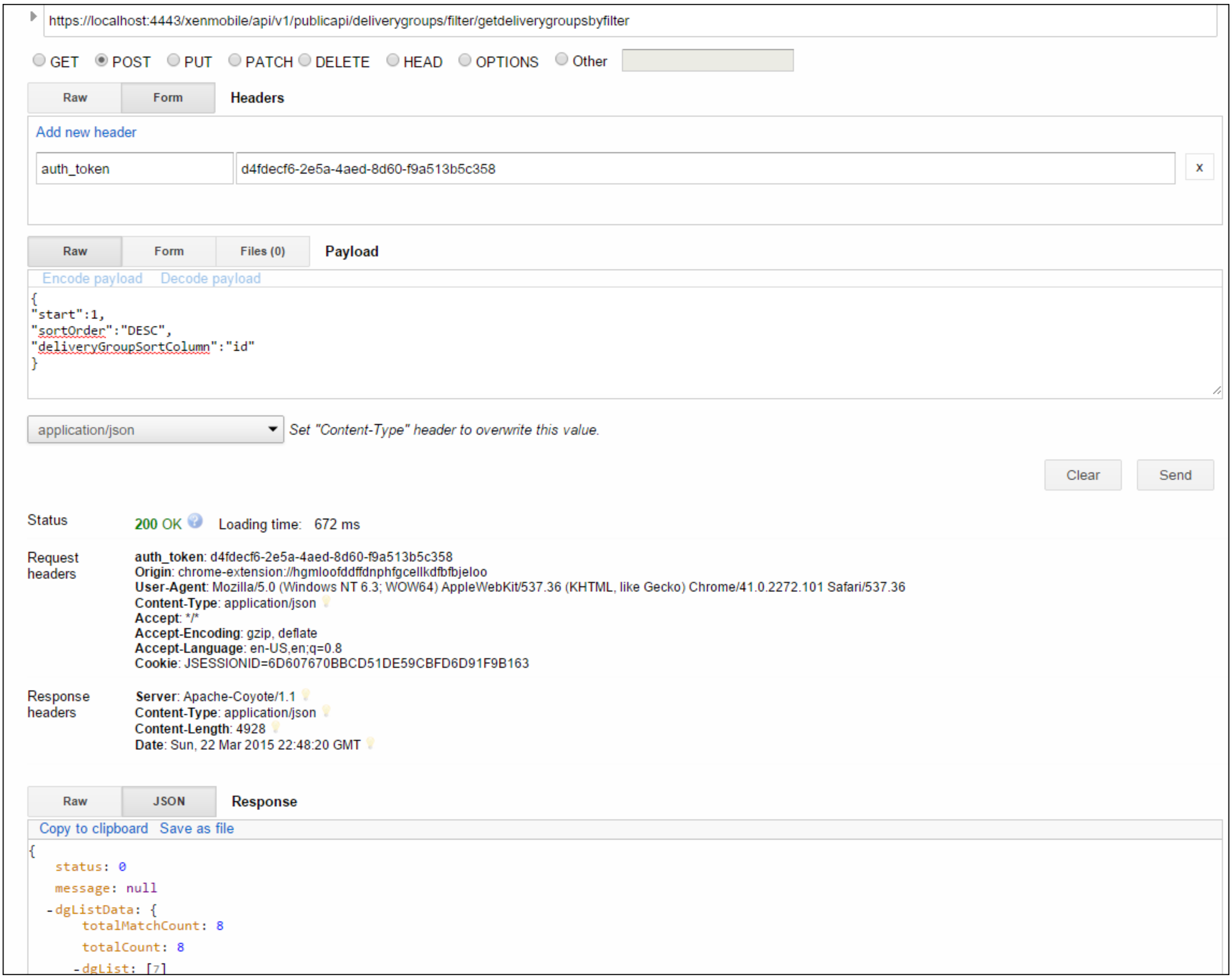
URL: /xenmobile/api/v1/deliverygroups/filter

Request COPY

```
{

    "start": 1,

    "sortOrder": "DESC",

    "deliveryGroupSortColumn":"id",

    "search":"add"

}
```

Method type: POST

Content type: application/json



https://localhost:4443/xenmobile/api/v1/publicapi/deliverygroups/filter/getdeliverygroupsbyfilter

○ GET ● POST ○ PUT ○ PATCH ○ DELETE ○ HEAD ○ OPTIONS ○ Other

auth_token: d4fdecf6-2e5a-4aed-8d60-f9a513b5c358

```
{
"start":1,
"sortOrder":"DESC",
"deliveryGroupSortColumn":"id"
}
```

application/json — *Set "Content-Type" header to overwrite this value.*

Status: 200 OK Loading time: 672 ms

Request headers:

```
auth_token: d4fdecf6-2e5a-4aed-8d60-f9a513b5c358
Origin: chrome-extension://hgmloofddffdnphfgcellkdfbfbjeloo
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.101 Safari/537.36
Content-Type: application/json
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=6D607670BBCD51DE59CBFD6D91F9B163
```

Response headers:

```
Server: Apache-Coyote/1.1
Content-Type: application/json
Content-Length: 4928
Date: Sun, 22 Mar 2015 22:48:20 GMT
```

```
{
   status: 0
   message: null
  -dgListData: {
       totalMatchCount: 8
       totalCount: 8
     -dgList: [7]
```

Public API REST services

The following table lists the available REST services.

Function	REST service	URL
Login	Login	/xenmobile/api/v1/authentication/login
	Logout	/xenmobile/api/v1/authentication/logout
Certificates	Get all certificates	xenmobile/api/v1/certificates
	Delete certificates	xenmobile/api/v1/certificates/

	Import certificate as SAML	xenmobile/api/v1/certificates/import/certificate/saml
	Import certificate as server	xenmobile/api/v1/certificates/import/certificate/server
	Import certificate as listener	xenmobile/api/v1/certificates/import/certificate/listener
	Create certificate	xenmobile/api/v1/certificates/csr
	Export certificate	xenmobile/api/v1/certificates/export
Keystore	Import keystore as server	xenmobile/api/v1/certificates /import/keystore/server
	Import keystore as SAML	xenmobile/api/v1/certificates /import/ keystore/saml
	Import keystore as APNS	xenmobile/api/v1/certificates /import/ keystore/apns
	Import keystore as listener	xenmobile/api/v1/certificates /import/ keystore/listener
Licenses	Get License Info	xenmobile/api/v1/licenses
	Save License Info	xenmobile/api/v1/licenses
	Upload License	xenmobile/api/v1/licenses/upload
	Delete Licenses	xenmobile/api/v1/licenses/remove
	Activate License	xenmobile/api/v1/licenses/activate/{licenseType}
	Test Server	xenmobile/api/v1/licenses/testserver
	Get Expiration Date	xenmobile/api/v1/licenses/getexpirationdate
LDAP	Get LDAP configuration list	xenmobile/api/v1/ldap
	Add a new LDAP	xenmobile/api/v1/ldap/msactivedirectory
	Edit a new LDAP	xenmobile/api/v1/ldap/msactivedirectory/{name}

	Set default LDAP	xenmobile/api/v1/ldap/default/{name}
	Delete LDAP	configxenmobile/api/v1/ldap/{name}
NetScaler	Get NetScaler Gateway	xenmobile/api/v1/netscaler
	Add NetScaler Gateway	xenmobile/api/v1/netscaler
	Update NetScaler Gateway	xenmobile/api/v1/netscaler/{id}
	Set Default NetScaler Gateway	xenmobile/api/v1/netscaler/default/{id}
	Delete NetScaler Gateways	xenmobile/api/v1/netscaler
Notification	Get Notification Servers	xenmobile/api/v1/notificationserver
	Get Notification Server by Id	xenmobile/api/v1/notificationserver/{id}
	Add/Edit SMTP Server	xenmobile/api/v1/notificationserver/smtp
	Add/Edit SMS Gateway	xenmobile/api/v1/notificationserver/sms
	Set SMTP server as default (activate)	xenmobile/api/v1/notificationserver/activate/smtp/{id}
	Delete notification server	xenmobile/api/v1/notificationserver/{id}
	Set SMS Gateway as default (activate)	xenmobile/api/v1/notificationserver/activate/sms/{id}
Local Users and Groups	Get Local Users	xenmobile/api/v1/localusersgroups
	Get Specific User	xenmobile/api/v1/localusersgroups/{name}
	Add User	xenmobile/api/v1/localusersgroups

	Import Provisioning File	xenmobile/api/v1/localusersgroups/importprovisioningfile
	Update User	xenmobile/api/v1/localusersgroups
	Delete Users	xenmobile/api/v1/localusersgroups/deletelocalusers
	Delete User	xenmobile/api/v1/localusersgroups/{name}
	Get Local Users By Filter	xenmobile/api/v1/localusersgroups/filter
	Reset User Password	xenmobile/api/v1/localusersgroups/password
App Management	Delete Application Container	xenmobile/api/v1/application/{container id}
	Delete Application Containers	xenmobile/api/v1/application
	Get App Containers by Filter	xenmobile/api/v1/application/filter
	Get Weblink Apps Container by Container ID	xenmobile/api/v1/application/weblink/{container id}
	Get Web and SAAS Apps Container by Container ID	xenmobile/api/v1/application/saas/{container id}
	Get Appstore Apps Container by Container ID	xenmobile/api/v1/application/appstore/{container id}
	Get Mobile Apps Container by Container ID	xenmobile/api/v1/application/mobile/{container id}
Delivery Groups	Add Delivery Groups	xenmobile/api/v1/deliverygroups
	Edit Delivery Groups	xenmobile/api/v1/deliverygroups
	Get Delivery Group Specific	xenmobile/api/v1/deliverygroups/{role name}
	Get Delivery Groups by	xenmobile/api/v1/deliverygroups/filter

	Filter	
	Get Delivery Groups All	xenmobile/api/v1/deliverygroups
	Delete Delivery Groups	xenmobile/api/v1/deliverygroups
	Get Deployment Status	xenmobile/api/v1/deliverygroups/getdeploymentstatus/{name}
Server Properties	Get Server Properties	xenmobile/api/v1/serverproperties/
	Get Server Properties by Filter	xenmobile/api/v1/serverproperties/filter/
	Add Server Properties	xenmobile/api/v1/serverproperties/
	Edit Server Properties	xenmobile/api/v1/serverproperties/
	Reset Server Properties	xenmobile/api/v1/serverproperties/reset
	Delete Server Properties	xenmobile/api/v1/serverproperties/

REST API definitions

The following sections describe the APIs listed in the preceding table.

Remember: In the following examples, change the host name and port number to match your environment.

To log on to the public API

Accepts user credentials and uses the existing AuthenticationManager to authenticate the user. The first time the AuthenticationManager authenticates a user, it generates an authentication token that is placed in the request header.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login

Request type: POST

Request Parameters COPY

```
{ "login":"administrator", "password":"password" }
```

Example Response

```
{

    "auth-token":"q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"

}
```

To log out of the public API

Removes the authentication token issued when the user logged on and logs out the current user. Requires the user name and the authentication token.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/authentication/logout

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Request Parameters

```
{"login":"administrator"}
```

Example Response

```
{"Status":"user administrator logged out successfully."}
```

To manage certificates

With certificate management operations, you can view, delete, import, and add certificates through the public API.

Get all certificates

Returns all certificates in the database.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Request Parameters: None

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": null,
    "certificate": [
         {
              "name": "ent-root-ca",
              "description": "test description server 1",
              "validFrom": "2012-02-22",
              "validTo": "2017-02-21",
              "type": "chain",
              "isActive": false,
              "privateKey": "false",
              "ca": null,
              "id": 4656,
            "certDetails": {
                "signatureAlgo": "SHA1WithRSAEncryption",
                "version": null,
                "serialNum": "34823788180011841845726834648368716413",
                "issuerName": {
                    "certString": "DC=com,DC=example,CN=ent-root-ca",
                    "emailAddress": null,
                    "commonName": "ent-root-ca",
                    "orgUnit": null,
                    "org": null,
                    "locality": null,
                    "state": null,
                    "country": null,
                    "description": null
                },
                "subjectName": {
                    "certString": "DC=com,DC=example,CN=ent-root-ca",
                    "emailAddress": null,
                    "commonName": "ent-root-ca",
                    "orgUnit": null,
                    "org": null,
                    "locality": null,
                    "state": null,
                    "country": null,
                    "description": null
                }
            }
        }
    ],
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```

Delete certificates

Deletes the specified certificates. Requires the certificate ID for each certificate to be deleted.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/publicapi/certificates

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Request Parameters COPY

```
{“certificateIds”:[“<certificate_id_1>”,”<certificate_id_2>”, ..., "<certificate_id_n>"]}
```

Import certificate as SAML certificate

Imports the specified certificate as a SAML certificate.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/certificate/saml

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters COPY

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'saml',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
          "topicNameMismatch": false,

          "certExpired": false,

          "certNotYetValid": false,

          "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

          "topicNameMismatch": false,

          "certExpired": false,

          "certNotYetValid": false,

          "malformed": false

    }

}
```

Import certificate as server certificate

Imports the specified certificate as a server certificate.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/certificate/server

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters COPY

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```

Import certificate as listener certificate

Imports the specified certificate as an SSL listener certificate.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/certificate/listener

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters COPY

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'listener',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

Example Response

COPY

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
  }
```

Create certificate

Creates a self-signed certificate or a CSR request that requires a CA signature.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/csr

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Application/form_url_encoded

Request Parameters

COPY

```
{
    "isSelfSign":true,
    "csrRequest":{
    "commonName":"your certificate name",
    "description":"certificate description",
    "org":"organization",
    "orgUnit":"organization unit",
    "locality":"location",
    "state":"CA",
    "country":"US",
    "isSelfSign":true
    },
"validDays":"60",
"keyLength":"1024",
"useAs":"none"
}
```

Example Response

COPY

```
{

    status: 0

    message: "Success"

    csrRequest: ""

    apnsCheck: null

    certificate: null

    apnsCheckObj:

    {

    topicNameMismatch: false

    certExpired: false

    certNotYetValid: false

    malformed: false

    }

}
```

Export certificate

Downloads the specified certificate. The following table lists the parameters for this operation.

Parameter	Required	Description
id	Yes	The numeric certificate ID

password	Password associated with the certificate being exported.
exportPrivateKey	Flag indicating whether to export the private key.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/export

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "id": "300",

    "password": "1111",

    "exportPrivateKey": true

}
```

Example response: Displays the certificate string on successful request.

To manage keystores

You can import keystores through the public API.

Import a server keystore

Imports a server keystore.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/keystore/server

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters

COPY

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Example Response

COPY

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```

Import SAML keystore

Imports a SAML keystore.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/keystore/saml

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Paramaters

COPY

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
 }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Example Response

COPY

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```

Import APNs keystore

Imports an APNS keystore.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/keystore/apns

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':apns,

    'keystoreType':'PKCS12',

    'uploadType':'keystore',

    'description':'test description'

    }

uploadFile = <certificate file>

uploadFile = <private key file>
```

Example Response

```
{

    "status": 0,
    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```

Import SSL listener keystore

Imports an SSL listener keystore.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/certificates/import/keystore/listener

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters COPY

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':”listener”,

    'keystoreType':'PKCS12',

    'uploadType':'keystore',

    'description':'test description'

    }

 uploadFile = <certificate file>

 uploadFile = <private key file>
```

Example Response COPY

```
{

    "status": 0,
    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

"certificate": null,

"apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```

To manage licenses

Lets you manage licenses through the public API.

Get license information

Lists information about all licenses.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
    status: 0
    message: "Success"
    cpLicenseServer: {
        serverAddress: "192.0.2.20"
        localPort: 0
        remotePort: 27000
        serverType: "remote"
        licenseType: "none"
        isServerConfigured: true
        gracePeriodLeft: 0
        isRestartLpeNeeded: null
        isScheduleNotificationNeeded: null
            licenseList: []
```

```
{
    sadate: "2015.1210"
    notice: "Example Systems Inc."
    vendorString: ";LT=Retail;GP=720;UDM=U;LP=90;CL=STD,ADV,ENT;SA=1;ODP=0"
    licensesInUse: 0
    licensesAvailable: 102
    overdraftLicenseCount: 2
    p_E_M: "CXM_ENTU_UD"
    serialNumber: "cxmretailent1000user"
    licenseType: "Retail"
    expirationDate: "01-DEC-2015"
}
licenseNotification:
{
    id: 1
    notificationEnabled: false
    notifyFrequency: 7
    notifyNumberDaysBeforeExpire: 60
    recepientList: ""
    emailContent: "License expiry notice"
```

```
        }

    }

}
```

Save license information

Saves all license information.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "serverAddress": "192.0.2.20",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": "remote",

    "licenseType": "none",

    "isServerConfigured": true,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": true,

    "isScheduleNotificationNeeded": true,
    "isScheduledNotificationNeeded": true,

    "licenseList": [],

    "licenseNotification": {

        "id": 1,

        "notificationEnabled": true,

        "notifyFrequency": 20,

        "notifyNumberDaysBeforeExpire": 60,

        "recepientList": "justa.name123@example.com",

        "emailContent": "Licenseexpirynotice"

    }

}
```

Example Response COPY

```
{

    "status": 0,

    "message": "Success"

}
```

Upload license file

Uploads the specified license file.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses/upload

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – Multipart/form-data

Request Parameters: uploadFile = <license file to be uploaded>

Example Response COPY

```
{

    "status": 0,

    "message": "Success"

}
```

Activate license

Activates the specified license.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses/activate/{license type}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters: Append the license type to the activate license URL.

Example Response COPY

```
{
    "status": 0,
    "message": "Success"
    "cpLicenseServer": null
}
```

Remove all licenses

Removes all licenses.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses/remove

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "isConnected": null
}
```

Test license server

Performs a connectivity check on the license server.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses/testserver/

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "serverAddress": "192.0.2.7",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": null,

    "licenseType": null,

    "isServerConfigured": null,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": null,

    "isScheduleNotificationNeeded": null,

    "licenseList": [],

    "licenseNotification": null

}
```

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "isConnected": true

}
```

Get earliest expiration date

Finds the license with the earliest expiration date.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/licenses/getexpirationdate

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "expiredDate": 1448956800000,
    "daysBeforeExpire": 229,
    "daysInPOC": 0
}
```

To manage LDAP configurations

The following table lists the parameters used in LDAP configuration operations.

Parameter	Required	Description
primaryHost	Yes	Primary LDAP server IP address or host name. Input as IP address or FQDN.
secondaryHost	No	Secondary LDAP server IP address or host name. Input as IP address or FQDN.
port	Yes	LDAP server port number
username	Yes	Valid LDAP server user name
password	Yes	Password for username
userBaseDN	Yes	
lockoutLimit	No	
lockoutTime	No	

useSecure	No	
userSearchBy	Yes	Search for users by upn or samaccount
domain	Yes	Unique LDAP server domain name
domainAlias	Yes	Alias for the LDAP domain
globalCatalogPort	No	
gcRootContext	No	
groupBaseDN	Yes	
isDefault	No	Part of the GET response that indicates whether the LDAP configuration is the default.
name	No	Part of the GET response that is a unique identifier used to update or delete the LDAP configuration.

List LDAP configuration

Lists the entire LDAP configuration in XenMobile.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/ldap

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response

COPY

```
{

    “result”: [

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"aaa@example.com","password":"1.pwd","userB

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"test@xmexample.com","password":"1.pwd","us

    ]

}
```

Add new LDAP configuration

Adds a new LDAP configuration. The domain name must be unique and cannot be the same as any other LDAP configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/ldap/msactivedirectory

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```

Example Response COPY

```
{

    “status”: 0,

    “message”: “LDAP configuration created”

}
```

Edit LDAP configuration

Edits an existing LDAP configuration with the exception that you cannot change the domain with the edit operation.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/ldap/msactivedirectory/{name}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "primaryHost":"192.0.2.7",
    "secondaryHost":"",
    "port":"389",
    "username":"aaa@example.com",
    "password":"1.pwd",
    "userBaseDN":"dc=example,dc=com",
    "groupBaseDN":"dc=example,dc=com",
    "lockoutLimit":"0",
    "lockoutTime":"1",
    "useSecure":"false",
    "userSearchBy":"upn",
    "domain":"example.com",
    "domainAlias":"exampleAlias",
    "globalCatalogPort":"0",
    "gcRootContext":""
}
```

Set default LDAP configuration

Sets the specified LDAP configuration as the default.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/ldap/default/{name}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Delete LDAP configuration

Deletes the specified LDAP configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/ldap/{name}

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

To manage NetScaler Gateway configurations

Lets you manage NetScaler Gateway configurations. The following table lists the parameters used in NetScaler Gateway operations.

Parameter	Required	Description
name	Yes	Unique NetScaler Gateway name
alias	No	
url	Yes	Publicly accessible URL for NetScaler Gateway
passwordRequired	Yes	
logonType	Yes	Valid values: domain-only, domain-token, domain-certificate, certificate-only, certificate-token, and token-only
callback	No	
default	Yes	Set to true or false when adding or editing a NetScaler Gateway configuration. If this parameter is not passed, the default is set to false.

id	No	Part of the GET response that is a unique identifier used to update or delete the NetScaler Gateway configuration.

List all NetScaler Gateway configurations

Lists the entire NetScaler Gateway configuration in XenMobile.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/netscaler

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{

    “result”: [

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false","id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        },

        { "name":"displayName",

        "alias":"",
        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false",

        "id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        }

    ]

}
```

Add new NetScaler Gateway configuration

Adds a new NetScaler Gateway configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/netscaler

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "name":"displayName",
    "alias":"",
    “default”:true, "url":"https://externalURl.com",
    "passwordRequired":"false",
    "logonType":"domain”,
    “callback”: [{“callbackUrl”:http://example.com,
    “ip”:”192.0.2.8”}]
}
```

Edit NetScaler Gateway configuration

Edit the specified NetScaler Gateway configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/netscaler/{id}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "name":"displayName",

    "alias":"",

    "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “default”: true,

    “callback”: [{“callbackUrl”:http://ag.com,

    “ip”:”192.0.2.8”}]

}
```

Delete NetScaler Gateway configuration

Delete the specified NetScaler Gateway configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/netscaler/{id}

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Set default NetScaler Gateway configuration

Set the specified NetScaler Gateway configuration as the default.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/netscaler/default/{id}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

To manage SMS and SMTP notification server configurations

You can add, edit, activate (set as default), and delete the SMS server and SMTP server configurations. The following table lists the parameters used with SMS server and SMTP server configuration operations.

Parameter	**Required**	**Description**
name	Yes	Unique SMS/SMTP configuration name.
serverType	No	Notification server type (SMS or SMTP) sent by the server in the GET request.
active	No	Indicates whether server is being used for notifications. Only one server can be active for each type.
id	No	Unique identifier used to update, delete, or activate the server.
description	No	Description of the server.
SMS parameters		
key	Yes	
secret	Yes	
virtualPhoneNumber	Yes	Must be in phone number format.
https	Yes	Default is false.
country	Yes	
carrierGateway	Yes	Default is false.
SMTP parameters		
secureChannelProtocol	Yes	The type of security protocol to use. Valid values are: None, SSL, and TLS. Default is none.

port	Yes	
authentication	Yes	Whether to use authentication. Valid values are true and false.
username	Yes, if authentication is true.	
password	Yes, if authentication is true.	
msSecurePasswordAuth	Yes	Default is false.
fromName	Yes	
fromEmail	Yes	
numOfRetries	No	An integer. Default is 5.
timeout	No	An integer. Default is 30.
maxRecipients	No	An integer. Default is 100.

List all SMS and SMTP servers

Lists all SMS and SMTP servers in XenMobile.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Accept – application/json

Example Response

COPY

```
{

    “result”: [

          { "name":"serverName","serverType":"SMS,"active":"true","id":"10"},

          { "name":"serverName2","serverType":"SMTP,"active":"true","id":"10"},

          { "name":"serverName3","serverType":"SMS,"active":"false","id":"10"}

    ]

}
```

Get server details

Get details about the server by server ID.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/{id}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Accept – application/json

Example SMS Response COPY

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Example SMTP Response COPY

```
{
    name":"displayName",
    "description":"",
    "server":"192.0.2.12",
    "secureChannelProtocol":"true",
    "port":"345",
    "authentication":"false”,
    “username”: “test”,
    “password”: “testPassword”,
    "msSecurePasswordAuth":"true",
    "fromName":"Email name",
    "fromEmail":test@example.com,
    "numOfRetries":5,
    "timeout":30,
    "maxRecipients":100
}
```

Add SMS server configuration

Add an SMS server configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/sms

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Edit SMS server configuration

Edit the specified SMS server configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/sms/{id}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Add SMTP server configuration

Adds an SMTP server configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/smtp

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Edit SMTP configuration

Edit the specified SMTP configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/smtp/{id}

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    name":"displayName",
    "description":"Edited description",
    "server":"192.0.2.9"
    "secureChannelProtocol":"true",
    "port":"345",
    "authentication":"false”,
    “username”: “test”,
    “password”: “testPassword”,
    "msSecurePasswordAuth":"true",
    "fromName":"Email name",
    "fromEmail":test@example.com,
    "numOfRetries":5,
    "timeout":30,
    "maxRecipients":100
}
```

Delete server configuration

Delete the specified SMS or SMTP server configuration.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/{id}

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Set default SMS configuration

Set the specified SMS server configuration as the default.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/activate/sms/{id}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Set default SMTP configuration

Set the specified SMTP server configuration as the default.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/notificationserver/activate/smtp/{id}

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

To manage local users and groups

You can manage local users and groups by using the following services.

Get all users

Get all local users.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response

COPY

```
{
    "status": 0,
    "message": "Success",
    "result": [
        {
            "userid": 8,
            "username": "admin",
            "password": null,
            "confirmPassword": null,
            "groups": [],
            "attributes": {
                "company": "example"
            },
            "role": "ADMIN",
            "roles": null,
            "createdOn": "1/10/15 11:42 AM",
            "lastAuthenticated": "1/10/15 11:42 AM",
            "domainName": null,
            "adUser": false,
            "vppUser": false
        }
    ]

  }
```

Get one user

Get the specified local user.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups/{name}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
  {

    "status": 0,

    "message": "Success",

    "result": {

         "userid": 8,

         "username": "admin",

         "password": null,

         "confirmPassword": null,

         "groups": [],

         "attributes": {

              "company": "example"
```

```
                "company": "example"

            },

            "role": "ADMIN",

            "roles": null,

            "createdOn": "1/10/15 11:42 AM",

            "lastAuthenticated": "1/10/15 11:42 AM",

            "domainName": null,

            "adUser": false,

            "vppUser": false

        }

    }
```

Add user

Add a user with the specified attributes.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "attributes": {
         "badpwdcount": "4",
         "asuseremail": "justa.name@example.com",
         "company": "example",
         "mobile": "4695557854"
         },
    "groups": [
         "MSP"
         ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",

    "user": {

        "userid": 0,

        "username": "justaname_XX",

        "password": "password",

        "confirmPassword": null,

        "groups": [

            "MSP"

        ],

        "attributes": {

            "badpwdcount": "4",

            "asuseremail": "justa.name@example.com",

            "company": "example",

            "mobile": "4695557854"

        },

        "role": "USER",

        "roles": null,

        "createdOn": null,

        "lastAuthenticated": null,

        "domainName": null,
        "adUser": false,

        "vppUser": false

    }

}
```

Update user

Update user attributes.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "attributes": {
         "badpwdcount": "4",
         "asuseremail": "justa.name@example.com",
         "company": "example",
         "mobile": "4695557854"
         },
    "groups": [
         "MSP"
         ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

Example Response COPY

```
{
    "status": 0,
    "message": "Success",
    "user": {
        "userid": 108,
        "username": "justaname_XX",
        "password": null,
        "confirmPassword": null,
        "groups": [
            "MSP"
        ],
        "attributes": {
            "badpwdcount": "4",
            "asuseremail": "justa.name@example.com",
            "company": "example",
            "mobile": "4695557854"
        },
        "role": "USER",
        "roles": null,
        "createdOn": "3/27/15 1:10 PM",
        "lastAuthenticated": "3/27/15 1:10 PM",
        "domainName": null,
        "adUser": false,

        "vppUser": false

    }

}
```

Change user password

Reset a user's password; you can also change a user's password in the update local user call.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups/resetpassword

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
    {

        "username": “administrator”,

        “password”: “newPassword”

    }
```

Example Response COPY

```
Response Errors:

1250 – User id not found

1252 – Failed to reset the password

Password can also be changed in the update local user call.
```

Delete users

Delete the specified users.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups/resetpassword

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{ justaname XX }
```

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

Delete one user

Delete the specified user.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups/

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response

COPY

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

Import provisioning file

Upload a file containing local user data. The file to be uploaded must be in .csv format. For more information on provisioning files, see Provisioning File Formats.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/localusersgroups/importprovisioningfile

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters

COPY

```
importdata={"fileType:"user"}

uploadfile=<file to be uploaded.csv>
```

Example Response

COPY

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

To manage apps

You can manage apps with the following services.

Get all apps by filter

Get apps based on the specified filter parameters.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/application/filter

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "start": 0,

    "limit": 10,

    "orderBy": "name",

    "sortOrder": "desc",

    "searchStr": "justaserver1"

}
```

Get mobile apps by container

Get mobile apps in the specified container.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/application/mobile/{containerId}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example response COPY

```
{
    "status": 0,
    "message": "Success",
    "result": {
        "id": 14,
        "name": "testApp",
        "description": "",
        "createdOn": null,
        "lastUpdated": null,
        "disabled": false,
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0,
        "schedule": {
            "enableDeployment": true,
            "deploySchedule": "NOW",
            "deployScheduleCondition": "EVERYTIME",
            "deployDate": null,
            "deployTime": null,
            "deployInBackground": false
        },
        "iconData": "",

        "appType": "MDX",

        "categories": [

            "Default"

        ],

        "roles": [],

        "workflow": null,

        "ios": {

            "displayName": "GoToMeeting",

            "description": "G2MW_IOS_5.3.3_075_01",

            "paid": false,

            "removeWithMdm": true,

            "preventBackup": true,

            "appVersion": "5.3.3.075",

            "minOsVersion": "",

            "maxOsVersion": "",

            "excludedDevices": "",

            "avppParams": null,

            "avppTokenParams": null,

            "rules": null,
        "rules": null,

        "appType": "mobile_ios",

        "uuid": "8e69d397-48bb-4f29-a95c-dd7b16665c1c",

       "id": 0,

        "store": {

            "rating": {

                "rating": 0,

                "reviewerCount": 0

            },

            "screenshots": [],

            "faqs": [],

            "storeSettings": {

                "rate": true,

                "review": true

            }

        },

        "policies": [

            {

                "policyName": "ReauthenticationPeriod",

                "policyValue": "480",
        "policyType": "integer",
        "policyCategory": "Authentication",
        "title": "Reauthentication period (minutes)",
        "description": "\nDefines the period before a user is challenged to authenticate again. ",
        "units": "minutes",
        "explanation": null
    },
    {
        "policyName": "BlockJailbrokenDevices",
        "policyValue": "true",
        "policyType": "boolean",
        "policyCategory": "Device Security",
        "title": "Block jailbroken or rooted",
        "description": "\nIf On, the application is locked when the device is jailbroken or rooted.",
        "units": null,
        "explanation": null
    },
    {
        "policyName": "CertificateLabel",
        "policyValue": "",
                "policyType": "string",

                "policyCategory": "Network Access",

                "title": "Certificate label",

                "description": "\nThe label for the certificate.\n                    Default value is e

                "units": null,

                "explanation": null

              }

            ]

        },

        "android": null,

        "android_knox": null,

        "android_work": null,

        "windows": null,

        "windows_tab": null

    }

}
```

Get SaaS apps by container

Get SaaS apps from the specified container.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/application/mobile/saas/{containerId}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Get public store apps by container

Get public store apps from the specified container.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/application/mobile/appstore/{containerId}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Get Web link apps by container

Get Web link apps from the specified container.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/application/mobile/weblink/{containerId}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Delete app container

Delete the specified app container.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/application/{containerId}

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

To manage delivery group configurations

You can manage delivery group configurations with the following services.

Get delivery groups by filter

Use the specified filter parameters to get delivery groups.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups/filter

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{
    "start": 1,
    "sortOrder": "DESC",
    "deliveryGroupSortColumn": "id",
    “limit”:10,
    "search": "add"
}
```

Example Response COPY

```
{
     "status": 0,
     "message": "Success",
     "dgListData": {
          "totalMatchCount": 7,
          "totalCount": 10,
          "dgList": [
    {
        "id": null,
        "name": "add delivery group 6.0",
        "description": "testing add delivery group 6.0",
        "groups": [
            {
                "id": 1,
                "userListId": 1,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
                "domainName": "local",
                "primaryToken": 0
            }
        ],
        "zoneId": null,
        "zoneDomain": null,
        "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\"
        "disabled": false,
        "lastUpdated": 1427144713353,
        "anonymousUser": true,
        "roledefLangVersionId": 1,
        "applications": [
            {
                "name": "Web Link",
                "required": false
            },
            {
                "name": "GoogleApps_SAML",
                "required": true
            }
        ],
        "devicePolicies": [
            "test terms conditions"
        ],
        "smartActions": [
            "shankar ganesh"
        ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    },
    {
        "id": null,
        "name": "add delivery group 5.0",
        "description": "testing add delivery group 5.0",
        "groups": [
            {
                "id": 1,
                "userListId": 1,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
                "domainName": "local",
                "primaryToken": 0
            }
        ],
        "zoneId": null,
        "zoneDomain": null,
        "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\"

        "disabled": false,

        "lastUpdated": 1426891345698,

        "anonymousUser": true,

        "roledefLangVersionId": 1,

        "applications": [

            {

                "name": "GoogleApps_SAML",

                "required": true

            },

            {

                "name": "Web Link",

                "required": false

             }

        ],

        "devicePolicies": [

            "test terms conditions"

        ],

        "smartActions": [

            "shankar ganesh"
```

```
                ],
                "nbSuccess": 0,
                "nbFailure": 0,
                "nbPending": 0
            }
        ]
    }
}
```

Get delivery group by name

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups/{name}

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response

COPY

```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": null,
        "name": "AllUsers",
        "description": "default role",
        "groups": [],
        "zoneId": null,
        "zoneDomain": null,
        "rules": null,
        "disabled": false,
        "lastUpdated": null,
        "anonymousUser": false,
        "roledefLangVersionId": 1,
        "applications": [
            {
                "name": "test mdx",
                "required": false
            },
            {
                "name": "test all",
                "required": false
            },
            {
            {
                "name": "justa test",
                "required": false
            },
            {
                "name": "test enterprise",
                "required": false
            },
            {
                "name": "name test",
                "required": false
            }
        ],
        "devicePolicies": [
            "test terms conditions"
        ],
        "smartActions": [
            "justa name"
        ],
        "nbSuccess": 0,
        "nbFailure": 0,

        "nbPending": 0

    }

}
```

Edit delivery group

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
    {

        "name": "add delivery group 2",

        "description": "Changing the description of the delivery group xxx",

        "groups": [

            {

                "name": "MSP",

                "uniqueName": "MSP",

                "uniqueId": "MSP",

                "domainName": "local"
            },
            {
                "name":"CN=Users,CN=Builtin,DC=example,DC=com",
                "uniqueName": "Users",
                "uniqueId":"a4169204-45f6-48fb-8a0d-847a3200d47e",
                "domainName": "example.com"
            }
            ],
        "disabled": false,
        "anonymousUser": false,
        "applications": [
            {
                "name": "GoogleApps_SAML",
                "required": true
            },
            {
                "name": "test mdx",
                "required": false
            }
            ],
        "devicePolicies": [

            {

                "name":"test terms conditions",

                "priority":-1

            }

            ],

        "smartActions": [

            {

                "name":"Smart Action Name 1",

                "priority":-1

            }

            ],

        "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"justa.name@example.com\"},\"ruleId\":\"001-restrictU

     }
```

Example Response COPY

```
 {

    "status": 0,

    "message": "Success",
"role": {
    "id": null,
    "name": "add delivery group 2",
    "description": "Changing the description of the delivery group xxx",
    "groups": [
        {
            "id": null,
            "userListId": null,
            "name": "MSP",
            "uniqueName": "MSP",
            "uniqueId": "MSP",
            "domainName": "local",
            "primaryToken": null
        },
        {
            "id": null,
            "userListId": null,
            "name": "CN=Users,CN=Builtin,DC=example,DC=com",
            "uniqueName": "Users",
            "uniqueId": "a4169204-45f6-48fb-8a0d-847a3200d47e"
```

```
          "uniqueId": "a4169204-45f6-48fb-8a0d-847a5200d47e",

         "domainName": "example.com",

         "primaryToken": null

     }

    ],

"zoneId": null,

"zoneDomain": null,

"rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"justa.name@example.com\"},\"ruleId\":\"001-rest

"disabled": false,

"lastUpdated": null,

"anonymousUser": false,

"roledefLangVersionId": null,

"applications": [

    {

     "name": "GoogleApps_SAML",

         "required": true

    },

    {

         "name": "test mdx",

         "required": false
```

```
            }

            ],

        "devicePolicies": [

            "test terms conditions"

             ],

        "smartActions": [

            "justa name"

            ],

        "nbSuccess": 0,

        "nbFailure": 0,

        "nbPending": 0

    }

}
```

Add delivery group

Adds a delivery group.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "name": "add delivery group 4.0",

    "description": "testing add delivery group 4.0",

    "anonymousUser": true,

    "devicePolicies": [

        {

            "name":"test terms conditions",

            "priority":-1

        }

        ],

        "applications": [

            {

                "name": "GoogleApps_SAML",

                "required": true

            },

            {

                "name": "Web Link",

                "required": false

            }
        ],
    "devicePolicies": [
        {
            "name":"test terms conditions",
            "priority":-1
        }
        ],
     "smartActions": [
        {
            "name":"Smart Action Name 1",
            "priority":-1
        }
        ],
    "groups": [
        {
            "uniqueName": "MSP",
            "domainName": "local",
            "name": "MSP",
            "uniqueId": "MSP"
        }
        ],

    "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"ju

}
```

Example Response

COPY

```
{

    "status": 0,

    "message": "Success",

    "role": {

        "id": 16,

        "name": "add delivery group 11.0",

        "description": "testing add delivery group 4.0",

        "groups": [

            {

                "id": null,

                "userListId": null,

                "name": "MSP",

                "uniqueName": "MSP",

                "uniqueId": "MSP",
                "domainName": "local",

                "primaryToken": null

            }

        ],

        "zoneId": null,

        "zoneDomain": null,

        "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\"

        "disabled": false,

        "lastUpdated": null,

        "anonymousUser": true,

        "roledefLangVersionId": null,

        "applications": [

            {

                "name": "GoogleApps_SAML",

                "required": true

            },

            {

                "name": "Web Link",

                "required": false
            }
            ],
        "devicePolicies": [
            "test terms conditions"
            ],
        "smartActions": [
            "just a name"
            ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    }
}
```

Delete delivery group

Delete specified delivery groups.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/deliverygroups

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
[ "add delivery group 11.0" ]
```

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "roleNames": [

          "add delivery group 11.0"

    ]

}
```

To manage server properties

You can manage XenMobile server properties by using the following services.

Get all server properties

Get all current XenMobile server properties.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties

Request type: GET

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Example Response COPY

```
{
```

```
"status": 0,

"message": "Success",

"allEwProperties": [

    {

        "id": 1,

        "name": "ios.mdm.pki.ca-root.certificatefile",

        "value": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayName": "ios.mdm.pki.ca-root.certificatefile",

        "description": "",

        "defaultValue": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayFlag": false,

        "editFlag": true,

        "deleteFlag": false,

        "markDeleted": false

    } ,

    {

        "id": 2,

        "name": "ios.mdm.https.host",

        "value": "192.0.2.4",
        "displayName": "ios.mdm.https.host",
        "description": "",
        "defaultValue": "192.0.2.4",
        "displayFlag": false,
        "editFlag": false,
        "deleteFlag": false,
        "markDeleted": false
    },
    {
        "id": 3,
        "name": "ios.mdm.enrolment.checkRemoteAddress",
        "value": "false",
        "displayName": "iOS Device Management Enrollment - Check Remote Address",
        "description": "",
        "defaultValue": "false",
        "displayFlag": true,
        "editFlag": true,
        "deleteFlag": false,
        "markDeleted": false
    },
]

}
```

Get server properties by filter

Get server properties using the specified filter parameters.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties/filter

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "start": 0,

    "limit": 1000,

    "orderBy": "name",

    "sortOrder": "desc",

    "searchStr": "justaserver1"

}
```

Example Response COPY

```
{
    "status": 0,

    "message": "Success",

    "allEwProperties": [

        {

            "id": 154,

            "name": "justaserver123",

            "value": "justaserver1",

            "displayName": "justarserver display name",

            "description": "justaserver description",

            "defaultValue": "justaserver1",

            "displayFlag": true,

            "editFlag": true,

            "deleteFlag": true,

            "markDeleted": false

        }

    ]

}
```

Add server property

Add the specified server property.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "name": "Key 2",

    "value": "Value 1",

    "displayName": "Display Name 1",

    "description": "Description 1"

}
```

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

Edit server properties

Edit the specified server property.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties

Request type: PUT

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters COPY

```
{

    "name": "Key 2",

    "value": "Value 1",

    "displayName": "Display Name 2",

    "description": "Description 2"

}
```

Example Response COPY

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

Reset server properties

Reset the specified server properties.

URL: https://<host-name>:<port-number>/xenmobile/api/v1/serverproperties/reset

Request type: POST

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters

COPY

```
{

    "names": [,

        "justaname7"

        ]

}
```

Example Response

COPY

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

Delete server properties

URL: https://hostname:4443 /xenmobile/api/v1/serverproperties

Request type: DELETE

Request header: auth_token – the authentication token obtained when the user logged on

Content type – application/json

Request Parameters

COPY

```
{
    "justaname3",
    "justaname4"
}
```

Example Response

COPY

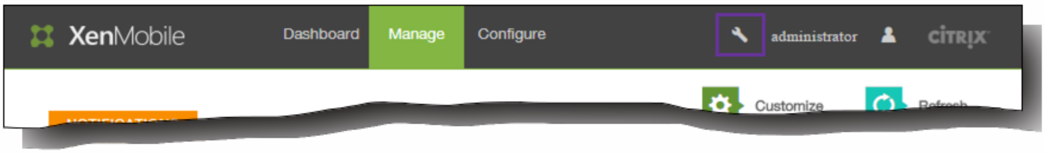
```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Conducting Connectivity Checks

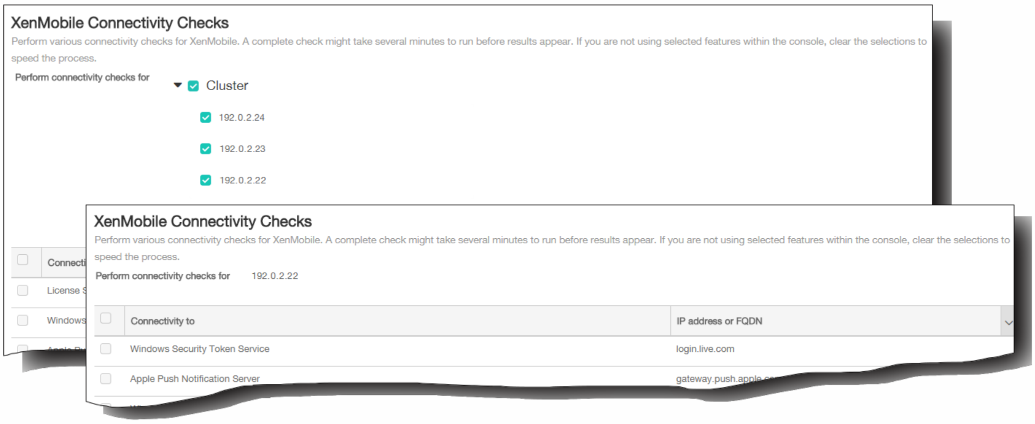
Aug 12, 2015

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 and they are not all shown, click the check box next to **Perform connectivity checks for** to expand the list of nodes. If your environment contains only a single server, it is listed next to **Perform connectivity checks for**.



XenMobile Connectivity Checks

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

Perform connectivity checks for ☑ Cluster
☑ 192.0.2.24
☑ 192.0.2.23
☑ 192.0.2.22

XenMobile Connectivity Checks

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

Perform connectivity checks for 192.0.2.22

□	Connectivity to	IP address or FQDN
□	Windows Security Token Service	login.live.com
□	Apple Push Notification Server	gateway.push.apple.c

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. Click the listing for a server (not the check box next to the server) in the Test Results table to see detailed results for that server.
4. When you are done, click **Clear Results** to return to the server table.

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.

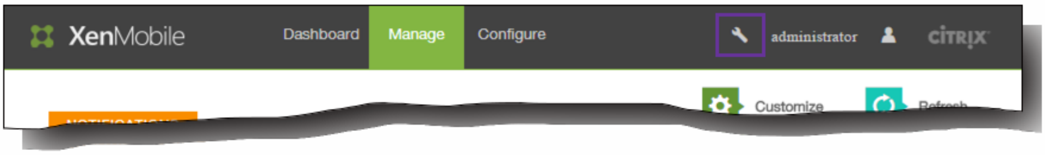
5. Click Add. The NetScaler Gateway is added to the table on the NetScaler Gateway Connectivity Checks page.
6. Click Test Connectivity. The results appear in a Test Results table.
7. Select a server in the Test Results table to see detailed results for that server.

Creating Support Bundles in XenMobile

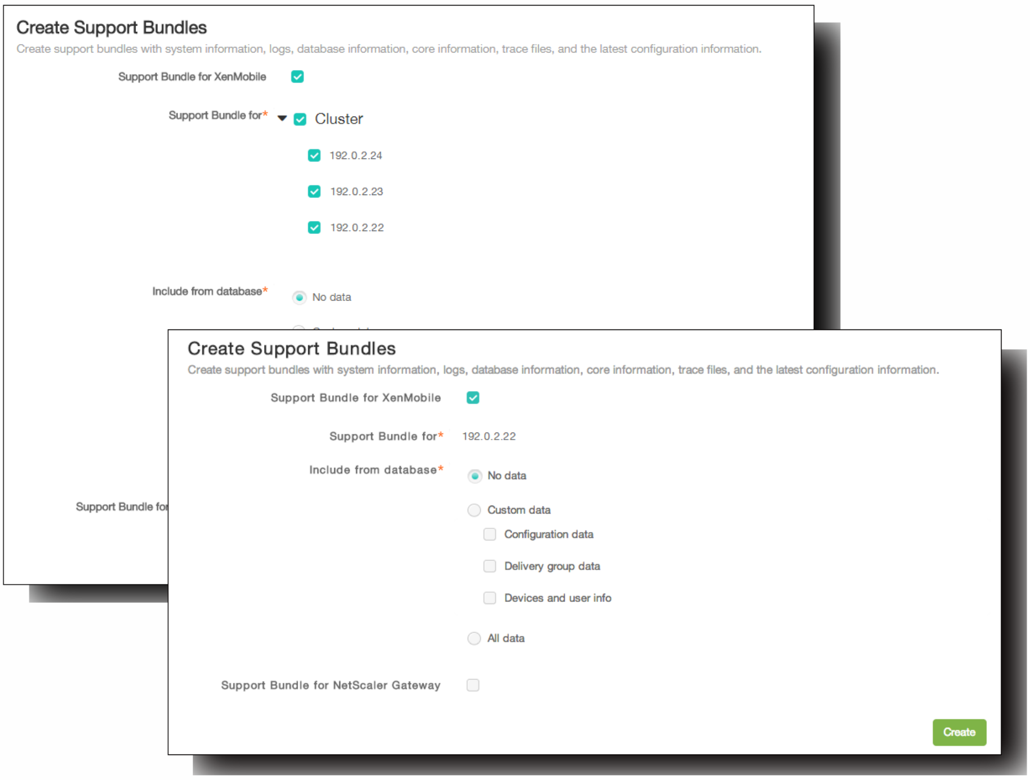
Feb 16, 2015

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.



Create Support Bundles

Create support bundles with system information, logs, database information, core information, trace files, and the latest configuration information.

Support Bundle for XenMobile ☑

Support Bundle for* ☑ Cluster
☑ 192.0.2.24
☑ 192.0.2.23
☑ 192.0.2.22

Include from database* ● No data

Create Support Bundles

Create support bundles with system information, logs, database information, core information, trace files, and the latest configuration information.

Support Bundle for XenMobile ☑

Support Bundle for* 192.0.2.22

Include from database* ● No data
○ Custom data
□ Configuration data
□ Delivery group data
□ Devices and user info
○ All data

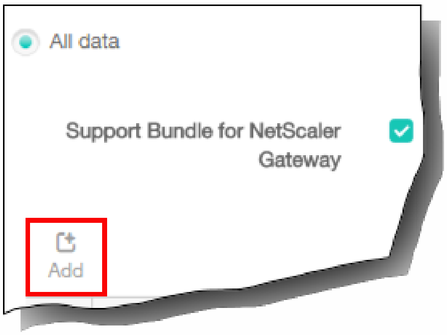
Support Bundle for NetScaler Gateway □

Create

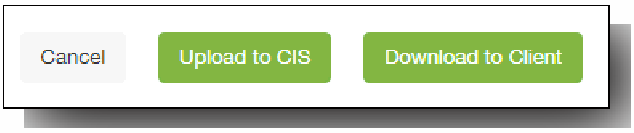
3. Ensure that the Support Bundle for XenMobile check box is selected.
4. If your XenMobile environment contains clustered nodes, in Support Bundle for, you can select all the nodes or any combination of nodes to draw data from.
5. In Include from Database, do one of the following:
   - Click No data.

- 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.

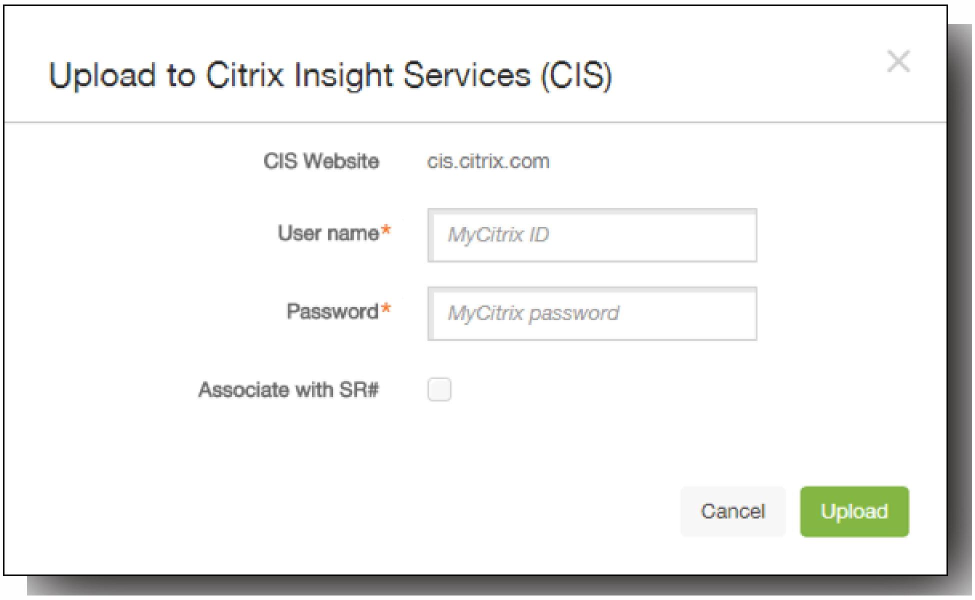


Continue to the procedures for **Uploading Support Bundles to Citrix Insight Services** or **Downloading Support Bundles to a Client**.

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# □

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

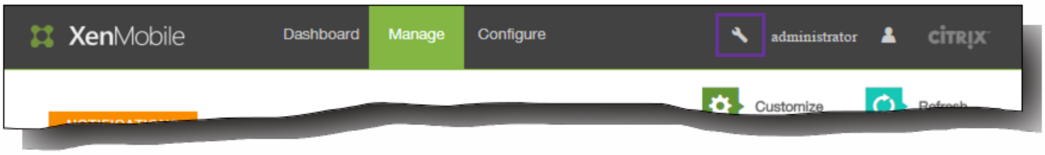
After you create a support bundle, you can upload the bundle to CIS or download the bundle to your computer. If you would like to troubleshoot the problem on your own, download the support bundle to your computer.
On the Create Support Bundles page, click Download to Client. The bundle is downloaded to your computer.

To view the debug log file

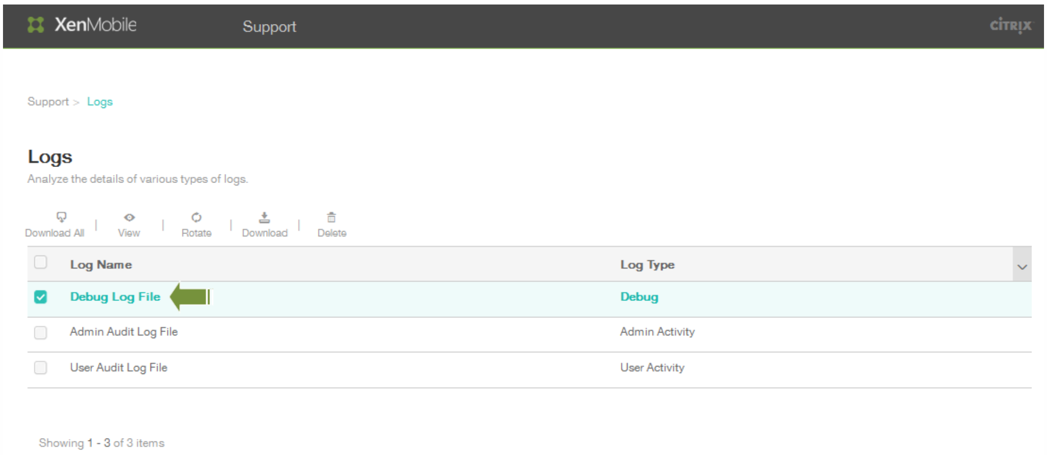
Aug 12, 2015

Follow these steps to view and download the Debug Log File:

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.



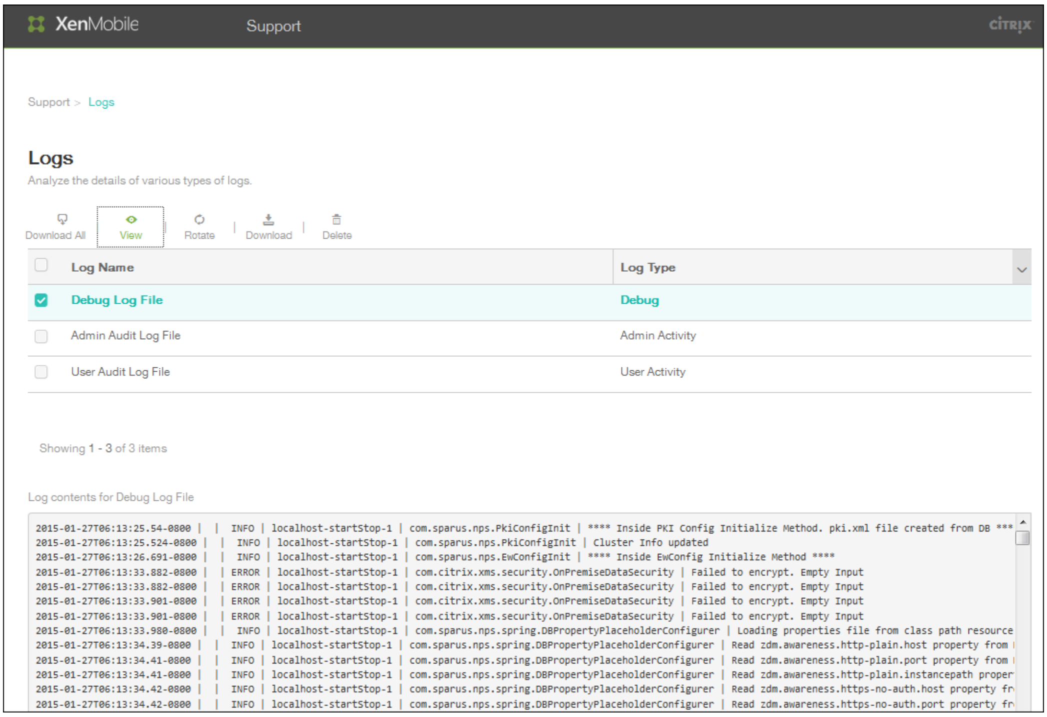
Logs

Analyze the details of various types of logs.

□	Log Name	Log Type
☑	Debug Log File	Debug
□	Admin Audit Log File	Admin Activity
□	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

3. Select Debug Log File and then click View to display the contents of the log.



Logs

Analyze the details of various types of logs.

	Log Name	Log Type
☑	Debug Log File	Debug
□	Admin Audit Log File	Admin Activity
□	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Debug Log File

```
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
```

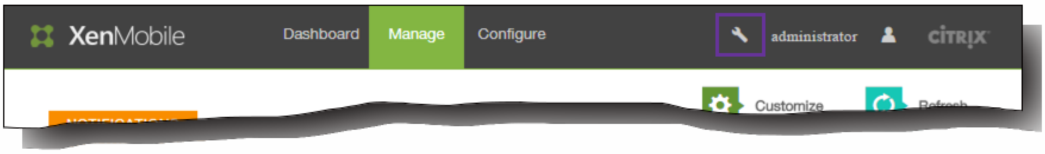
After analyzing the log file, use the Download File option to save the data, or click Delete to remove the contents of the log from the database.

To configure log settings

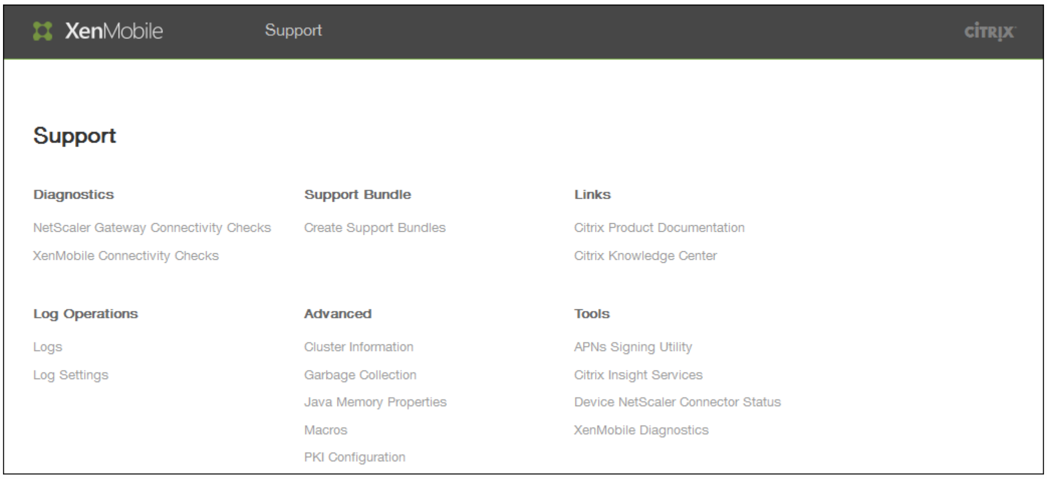
Jun 12, 2015

You can configure log settings to customize the output of logs that XenMobile generates. If you have clustered XenMobile servers, when you configure log settings in the XenMobile console, those settings are shared with all other servers in the cluster.

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.



Support

Diagnostics

NetScaler Gateway Connectivity Checks

XenMobile Connectivity Checks

Support Bundle

Create Support Bundles

Links

Citrix Product Documentation

Citrix Knowledge Center

Log Operations

Logs

Log Settings

Advanced

Cluster Information

Garbage Collection

Java Memory Properties

Macros

PKI Configuration

Tools

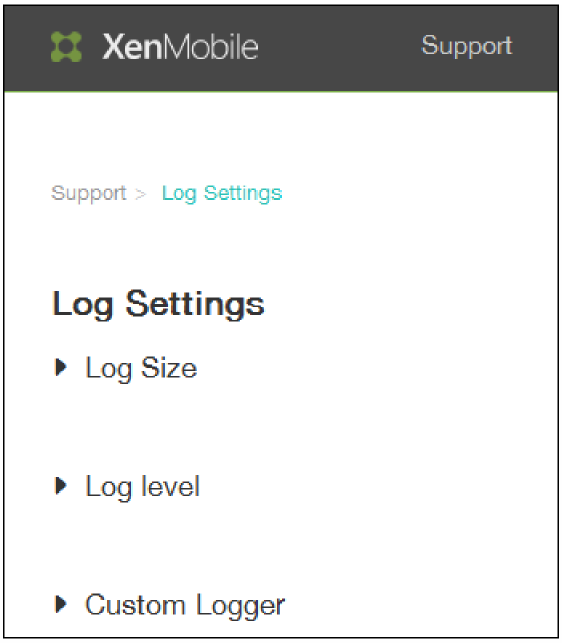
APNs Signing Utility

Citrix Insight Services

Device NetScaler Connector Status

XenMobile Diagnostics

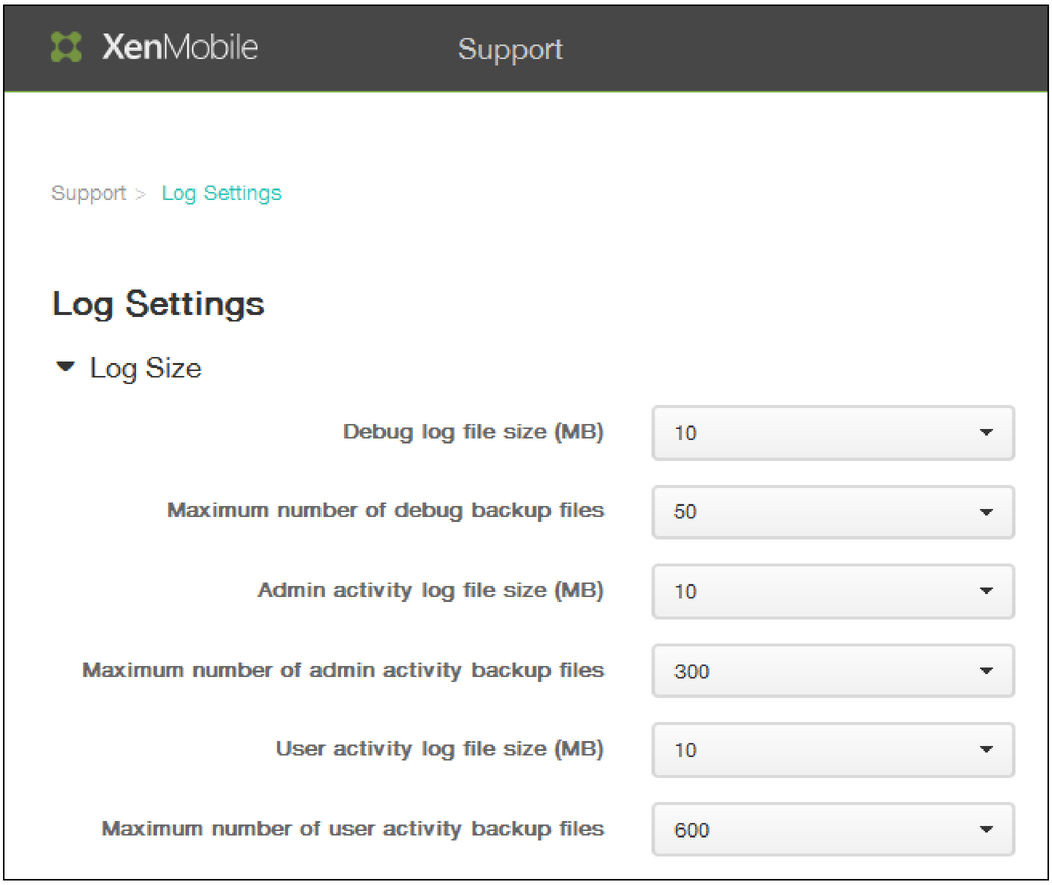
Under Log Operations, click Log Settings to access the following options:



- 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 user activity log).
- Log level. Use this option to change the log level or to persist settings.
- Custom Logger. Use this option to create a custom logger; custom logs require a class name and the log level.

To configure the Log Size options

1. On the Log Settings page, expand Log Size and configure the following settings:



Log Settings

Log Size

Debug log file size (MB): 10

Maximum number of debug backup files: 50

Admin activity log file size (MB): 10

Maximum number of admin activity backup files: 300

User activity log file size (MB): 10

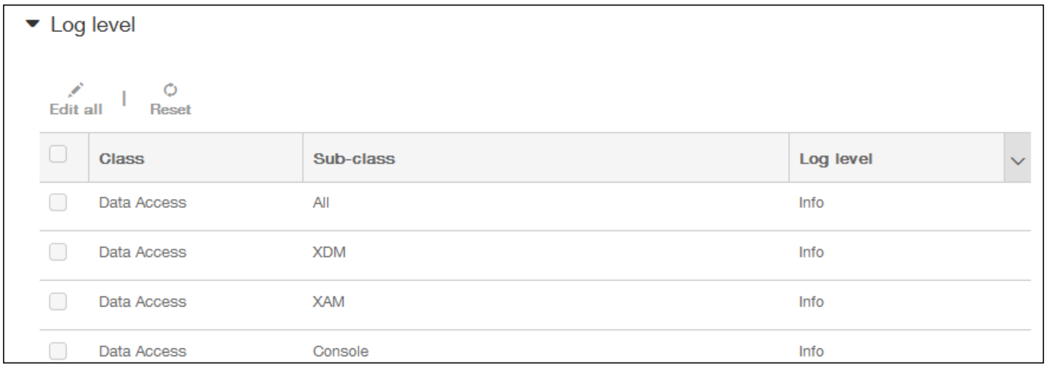
Maximum number of user activity backup files: 600

1. Debug log file size (MB): In the list, click a size between 5 MB and 20 MB to change the maximum size of the debug file. By default, the size of the file is set to 10 MB.
2. Maximum number of debug backup files: In the list, click the maximum number of debug files retained by the server. By default, XenMobile retains 50 backup files on the server.
3. Admin activity log file size (MB): in the list, click a size between 5 MB and 20 MB to change the maximum size of the admin activity file. By default, the size of the file is set to 10 MB.
4. Maximum number of admin activity backup files: In the list, click the maximum number of admin activity files retained by the server. By default, XenMobile retains 300 backup files on the server.
5. User activity log file size (MB): In the list, click a size between 5 MB and 20 MB to change the maximum size of the user activity file. By default, the size of the file is set to 10 MB.
6. Maximum number of user activity backup files: In the list, click the maximum number of user activity files retained by the server. By default, XenMobile retains 300 backup files on the server.

To configure Log Level options

Log Level lets you specify what type of information XenMobile collects in the log. You can set the same level for all classes or you can set individual classes to specific levels.

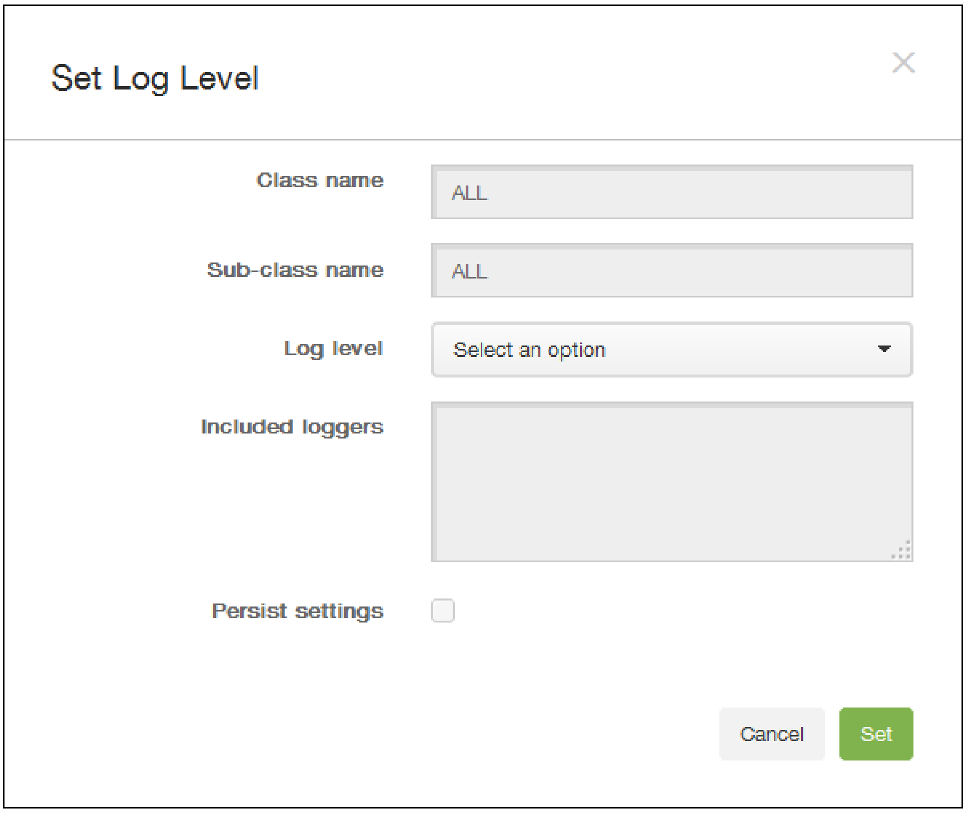
1. On the Log Settings page, expand Log level. The table of all log classes appears.



□	Class	Sub-class	Log level
□	Data Access	All	Info
□	Data Access	XDM	Info
□	Data Access	XAM	Info
□	Data Access	Console	Info

2. Do one of the following:
   - Click the check box next to one Class and then, click Set Level to change just this class's log level.
   - Click Edit all to apply the log level change to all classes in the table.

   The Set Log Level screen appears.



Class name: ALL

Sub-class name: ALL

Log level: Select an option

Included loggers:

Persist settings: □

1. Class Name: This field displays All when you are changing the log level for all classes or it displays the individual class name; it is not editable.
2. Sub-class name.This field displays All when you are changing the log level for all classes or it displays the individual class sub-class name; it is not editable.
3. Log level: In the list, click a log level. The supported log levels include:
   - Fatal
   - Error
   - Warning

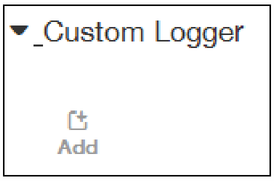
- Info
- Debug
- Trace
- Off

4. Included Loggers: This field is blank when you are changing the log level for all classes or it displays the currently configured loggers for an individual class; it is not editable.
5. Persist settings: If you want the log level settings to persist when you reboot the server, select this check box. Not selecting this check box means that the log level settings revert to their defaults when you reboot the server.

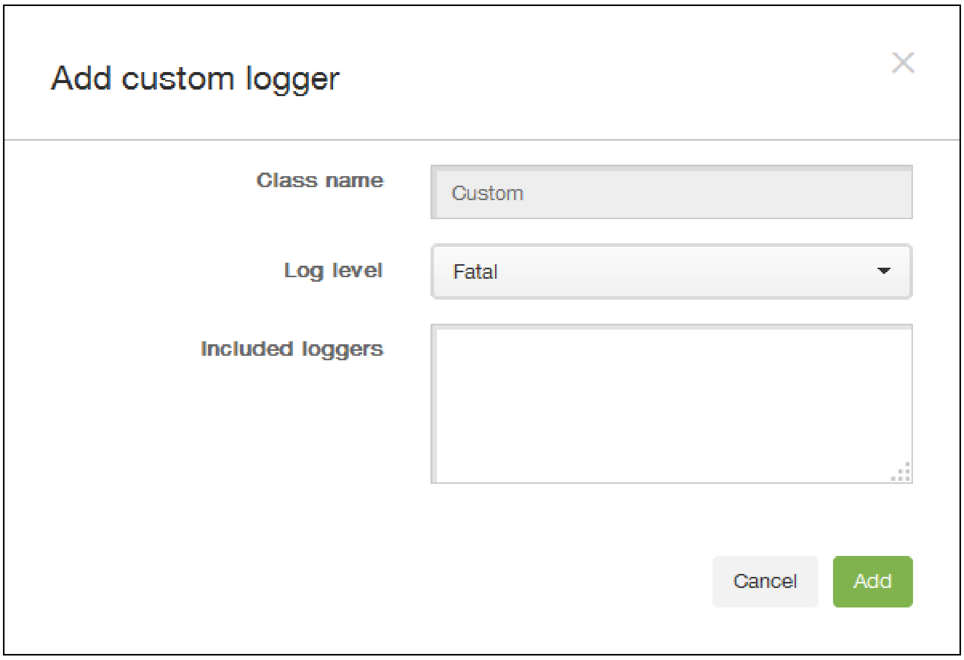
3. Click Set to commit your changes.

To add a Custom Logger

1. On the Log Settings page, expand Custom Logger and click Add.



The Add custom logger screen appears.


Add custom logger

Class name: Custom

Log level: Fatal

Included loggers

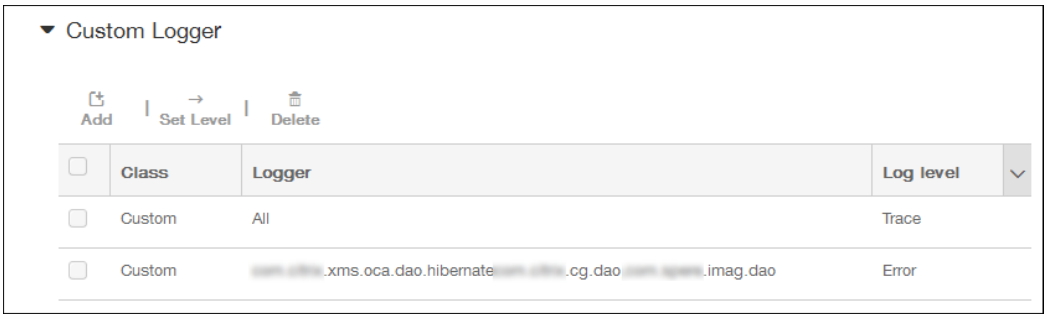
Configure the following settings:

1. Class Name: This field displays Custom; it is not editable.
2. Log level: In the list, click a log level. The supported log levels include:
   - Fatal
   - Error

- Warning
- Info
- Debug
- Trace
- Off

3. Included loggers: Add the loggers to be included in this custom log. You must add at least one logger.

2. Click Add. The custom logger is added to the Custom Logger table.



☐	Class	Logger	Log level
☐	Custom	All	Trace
☐	Custom	[redacted].xms.oca.dao.hibernate[redacted].cg.dao[redacted].imag.dao	Error

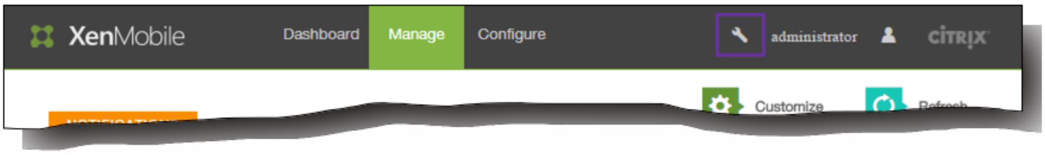
To delete a Custom Logger

1. On the Log Settings page, expand Custom Logger and select the custom logger you want to delete.
2. Click Delete. A dialog box appears asking whether you want to delete the custom logger. Click OK.
   Important: You cannot undo this operation.

Viewing and Analyzing Log Files in XenMobile

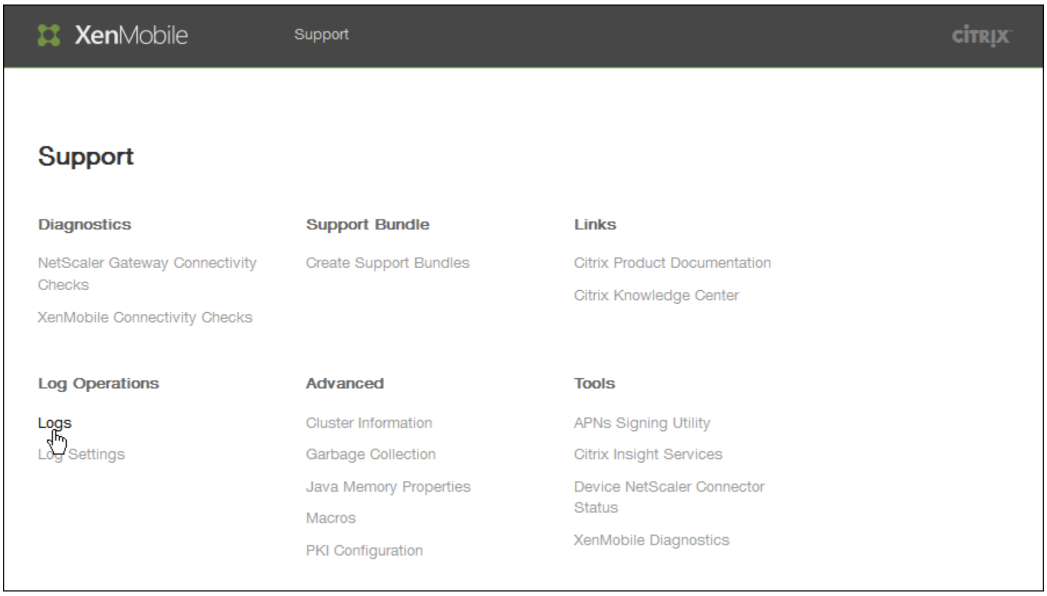
May 05, 2015

1. In the XenMobile console, click the wrench icon 🔧 in the upper-right corner of the console.



   The Support page opens in a new browser window.

2. Under Log Operations, click **Logs**.



Support

Diagnostics
NetScaler Gateway Connectivity Checks
XenMobile Connectivity Checks

Support Bundle
Create Support Bundles

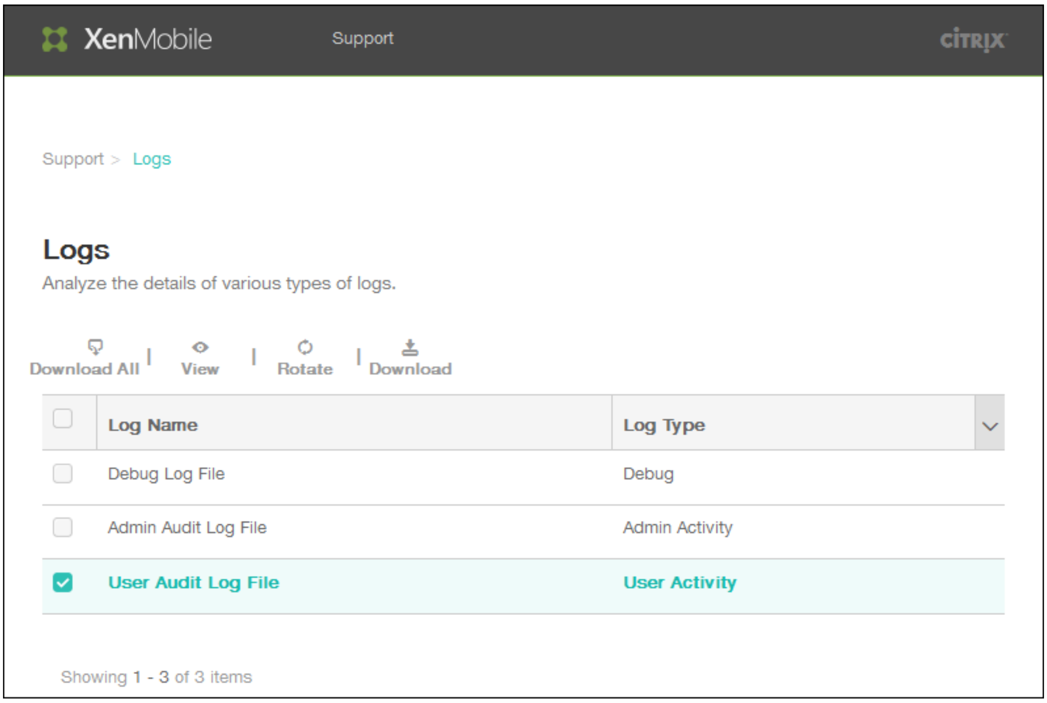
Links
Citrix Product Documentation
Citrix Knowledge Center

Log Operations
Logs
Log Settings

Advanced
Cluster Information
Garbage Collection
Java Memory Properties
Macros
PKI Configuration

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

   The **Logs** screen appears. Individual logs appear in a table.



Logs

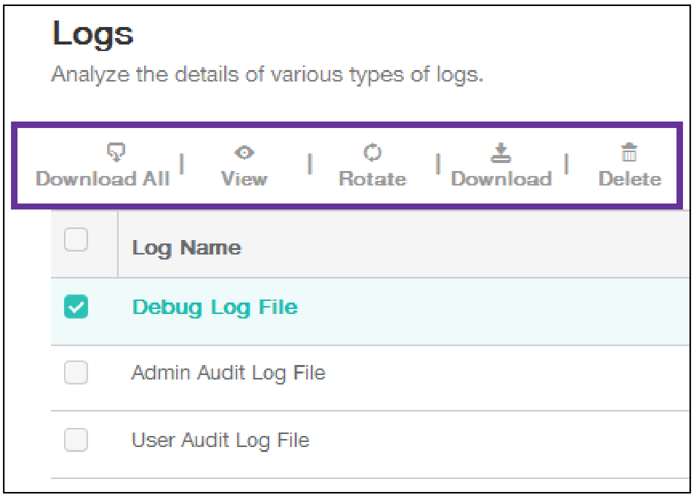
Analyze the details of various types of logs.

□	Log Name	Log Type
□	Debug Log File	Debug
□	Admin Audit Log File	Admin Activity
☑	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

3. Select the log you want to view:
   - Debug Log Files contain information useful for Citrix Support, such as error messages and server-related actions.
   - Admin Audit Log Files contain audit information about activity on the XenMobile console.
   - User Audit Log Files contain information related to configured users.
4. Use the actions at the top of the table to do the following:

   Note:
   - If you select more than one log file, only Download All and Delete are available.
   - If you have clustered XenMobile servers, you can only view the logs for the server to which you are connected. To see logs for other servers, use one of the download options.

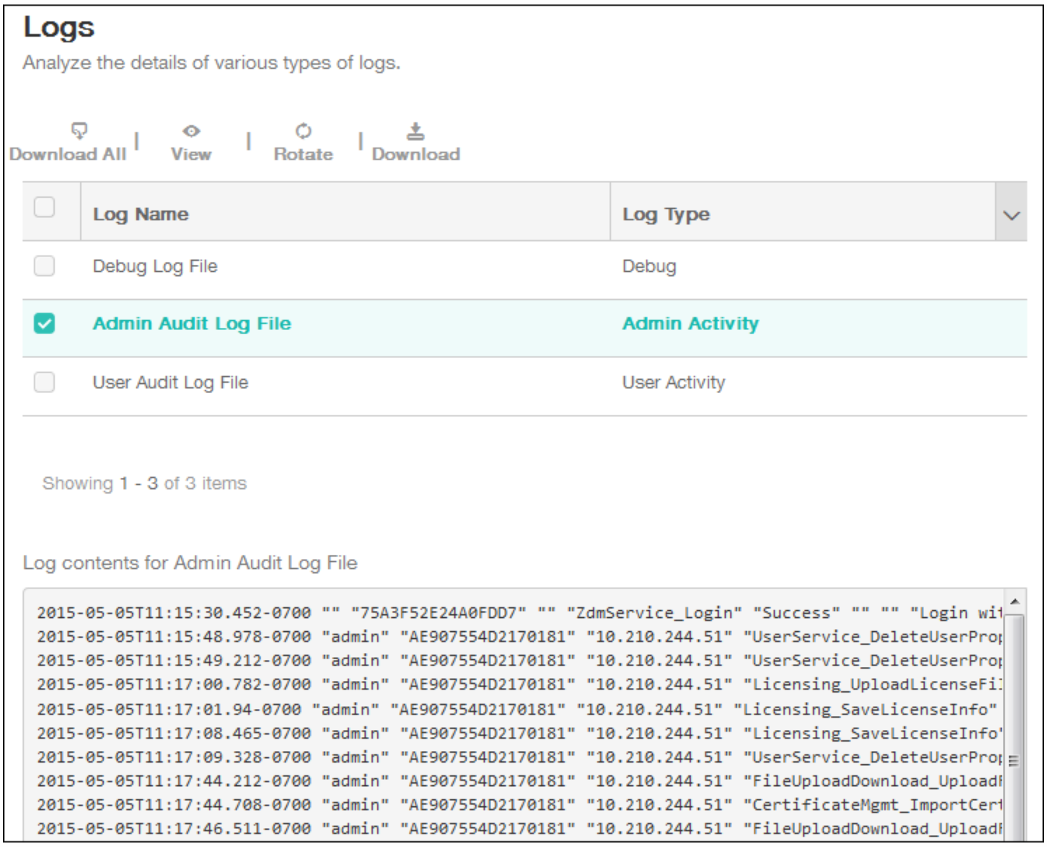


Logs

Analyze the details of various types of logs.

□	Log Name
☑	Debug Log File
□	Admin Audit Log File
□	User Audit Log File

- Download All: The console downloads all the logs present on the system (including debug, admin audit, user audit, server logs, and so on).
- View: Shows the contents of the selected log below the table.



Logs

Analyze the details of various types of logs.

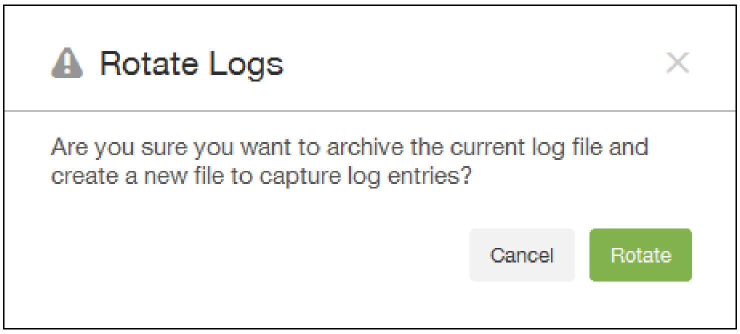
	Log Name	Log Type
□	Debug Log File	Debug
☑	Admin Audit Log File	Admin Activity
□	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Admin Audit Log File

```
2015-05-05T11:15:30.452-0700 "" "75A3F52E24A0FDD7" "" "ZdmService_Login" "Success" "" "" "Login wi
2015-05-05T11:15:48.978-0700 "admin" "AE907554D2170181" "10.210.244.51" "UserService_DeleteUserPro
2015-05-05T11:15:49.212-0700 "admin" "AE907554D2170181" "10.210.244.51" "UserService_DeleteUserPro
2015-05-05T11:17:00.782-0700 "admin" "AE907554D2170181" "10.210.244.51" "Licensing_UploadLicenseFi
2015-05-05T11:17:01.94-0700 "admin" "AE907554D2170181" "10.210.244.51" "Licensing_SaveLicenseInfo"
2015-05-05T11:17:08.465-0700 "admin" "AE907554D2170181" "10.210.244.51" "Licensing_SaveLicenseInfo'
2015-05-05T11:17:09.328-0700 "admin" "AE907554D2170181" "10.210.244.51" "UserService_DeleteUserPro
2015-05-05T11:17:44.212-0700 "admin" "AE907554D2170181" "10.210.244.51" "FileUploadDownload_Upload
2015-05-05T11:17:44.708-0700 "admin" "AE907554D2170181" "10.210.244.51" "CertificateMgmt_ImportCer
2015-05-05T11:17:46.511-0700 "admin" "AE907554D2170181" "10.210.244.51" "FileUploadDownload_Upload
```

- 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?

- Download: The console downloads only the single log file type selected; it also downloads any archived logs for that same type.
- Delete: Permanently removes the selected log files.

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 cluseter, please reboot that node.

System Menu Options

From the main menu, when you select the System option, the following menus appear:

```
------------------------------

[0] Back to Main Menu

[1] Display System Date

[2] Set Time Zone

[3] Display System Disk Usage

[4] Update Hosts File

[5] Proxy Server

[6] Admin (CLI) Password

[7] Restart Server

[8] Shutdown Server

[9] Advanced Settings

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

Choice: [0 - 9]
```

Troubleshooting Menu Options

From the main menu, when you select the Troubleshooting option, the following menus appear:

```
------------------------------

[0] Back to Main Menu

[1] Network Utilities

[2] Logs

[3] Support Bundle

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

Choice: [0 - 3]
```

When you choose the Network Utilities option, the following menu appears:

```
------------------------------

[0] Back to Troubleshooting Menu

[1] Network Information
```

```
[2] Show Routing Table

[3] Show Address Resolution Protocol (ARP) Table

[4] PING

[5] Traceroute

[6] DNS Lookup

[7] Network Trace

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

Choice: [0 - 7]

When you choose the Logs option, the following menu appears:

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

Logs Menu

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

[0] Back to Troubleshooting Menu

[1] Display Log File

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

Choice: [0 - 1]
```

/

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

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content

d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

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.

Known Issues

- The installed XenMobile Mail Manager version always displays as 8.5 during upgrade to XenMobile Mail Manager 10; however, the upgrade to XenMobile Mail Manager occurs. [#539520]
- Reporting of “devices found” in the minor snapshot may be confusing. The same device or devices may be reported as “new” in the successive minor snapshot summaries when the minor snapshots are run subsequent to the start of a major snapshot.

Fixed Issues

Power Shell/Exchange Management

In certain Microsoft Exchange environments (primarily Office 365), a restriction is placed on XenMobile Mail Manager that effectively limits bandwidth, preventing an app from issuing any PowerShell requests or commands. You can now use an alternate PowerShell cmdlet pathway in the Exchange configuration tab, which puts XenMobile Mail Manager into an alternate snapshot mode; this mode bypasses the original data path.

A new flag enables you to expose the **AllowRedirection** flag for non-Microsoft Office 365 environments. Use the Microsoft Exchange configuration tab to enable this flag.

Rules Management

LDAP local rules now support an indiscriminate number of groups for large Active Directory environments.

XenMobile duplicates device information for WorxMail clients. Resolving this issue requires that you enable regular expression support in the Managed Service Provider (MSP) portion of XenMobile Mail Manager; doing so filters the record sets returned to XenMobile. Devices matching the filter are not returned to XenMobile.

MSP

Users who are removed from the Blackberry Enterprise Server (BES) database are now removed from the local database.

UI

You can now use a progress dialog class for scenarios in which a persistent process takes place. In such a process, XenMobile Mail Manager sends users feedback and provides them with an opportunity to cancel where applicable.

The default value for new Microsoft Exchange instances is now set to *Shallow*.

Installer

Components referring to Zenprise have been changed to reflect XenMobile Mail Manager.

The installer hangs when it fails to find the installation path.

Support binaries and scripts now reside in the Support folder after installation.

In the Windows Start menu, XenMobile Mail Manager shortcuts now reside in the \Citrix\XenMobile Mail Manager folder.

Support

The Support model provides the ability to enable troubleshooting functionality through the addition of a config.xml file. You can use this file to help Citrix troubleshoot problems. At this release of XenMobile Mail Manager, this functionality only applies to the Microsoft Exchange configuration Add and Edit screens.
Note: You can also enable this troubleshooting functionality by holding the Shift key when opening the Configure utility.

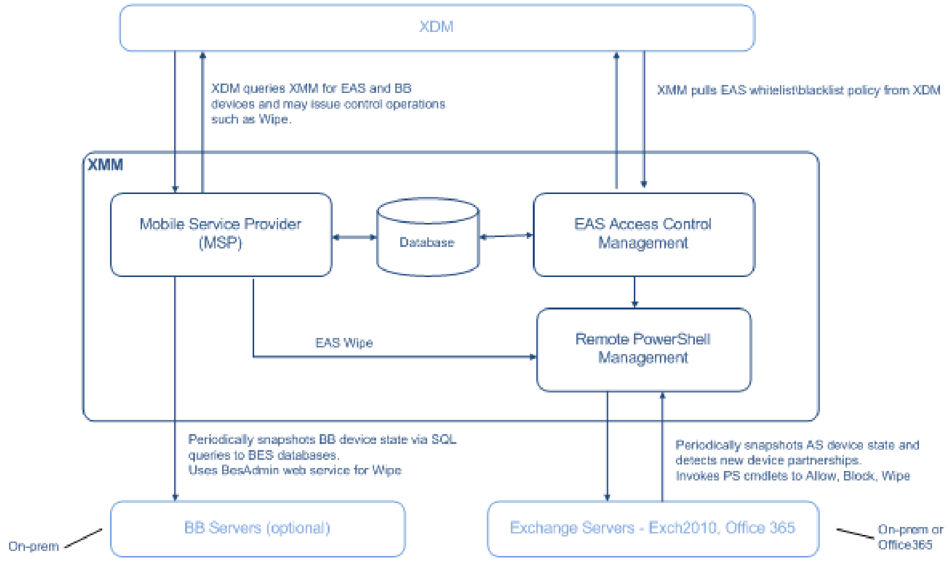
Logging

Error messages returned from PowerShell now have a GUID associated with them. Use this value to control what appears in the Snapshot History detail tab.

Architecture

Aug 12, 2016

The following diagram shows the main components of XenMobile Mail Manager. For a detailed reference architecture diagram, see the XenMobile Deployment Handbook article Reference Architecture for On-Premises Deployments.


XDM
XDM queries XMM for EAS and BB devices and may issue control operations such as Wipe.
XMM pulls EAS whitelist\blacklist policy from XDM
XMM
Mobile Service Provider (MSP)
Database
EAS Access Control Management
EAS Wipe
Remote PowerShell Management
Periodically snapshots BB device state via SQL queries to BES databases.
Uses BesAdmin web service for Wipe
Periodically snapshots AS device state and detects new device partnerships.
Invokes PS cmdlets to Allow, Block, Wipe
On-prem
BB Servers (optional)
Exchange Servers - Exch2010, Office 365
On-prem or Office365

The three main components are:

- **Exchange ActiveSync Access Control Management**. Communicates with XenMobile to retrieve an Exchange ActiveSync policy from XenMobile, and merges this policy with any locally defined policy to determine the Exchange ActiveSync devices that should be allowed or denied access to Exchange. Local policy allows extending the policy rules to allow access control by Active Directory Group, User, Device Type, or Device User Agent (generally the mobile platform version).

- **Remote PowerShell Management**. Responsible for scheduling and invoking remote PowerShell commands to enact the policy compiled by Exchange ActiveSync Access Control Management. Periodically takes a snapshot of the Exchange ActiveSync database to detect new or changed Exchange ActiveSync devices.
- Mobile Service Provider. Provides a web service interface so that XenMobile can query Exchange ActiveSync and/or Blackberry devices, as well as issue control operations such as Wipe against them.

System Requirements and Prerequisites

Dec 23, 2016

The following minimum system requirements are required to use XenMobile Mail Manager:

- Windows Server 2008 R2 (must be an English-based server)
- Microsoft SQL Server 2008, SQL Server 2012, SQL Server Express 2008, SQL Server 2012, or Microsoft SQL Server 2012 Express LocalDB
- Microsoft .NET Framework 4.5
- Blackberry Enterprise Service, version 5 (optional)

Minimum supported versions of Microsoft Exchange Server

- Microsoft Office 365
- Exchanger Server 2013
- Exchange Server 2010 SP2

Device email clients

Not all email clients consistently return the same ActiveSync ID for a device. Because XenMobile Mail Manager expects a unique ActiveSync ID for each device, only email clients that consistently generate the same, unique ActiveSync ID for each device are supported. These email clients have been tested by Citrix and performed without errors:

- HTC native email client
- Samsung native email client
- iOS native email client
- Touchdown for Smartphones

XenMobile Mail Manager Prerequisites

- Windows Management Framework must be installed.
  - PowerShell 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

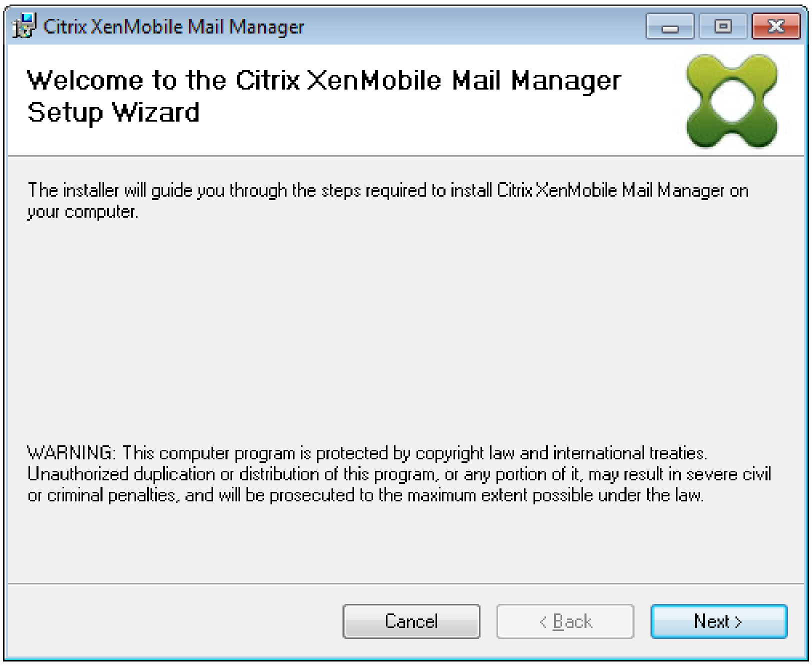
- **Permissions**. Exchange Role-Based Access Control (RBAC) is beyond the scope of this documentation. That being said, at a minimum, the credentials specified in the Exchange Configuration UI must be able to connect to Office 365 and be given full access to execute the following Exchange-specific PowerShell 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.



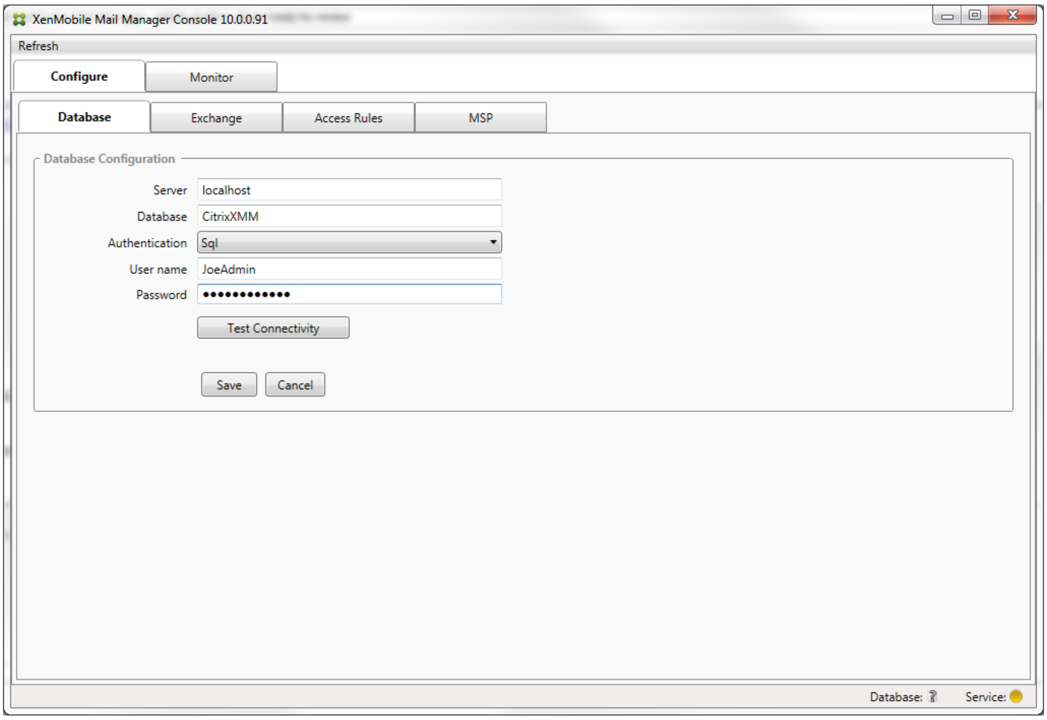
Citrix XenMobile Mail Manager

Welcome to the Citrix XenMobile Mail Manager Setup Wizard

The installer will guide you through the steps required to install Citrix XenMobile Mail Manager on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

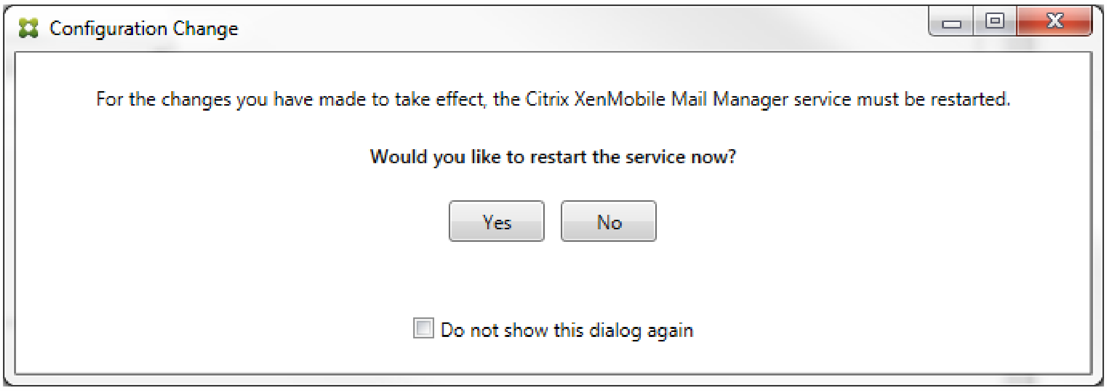
2. From the Start menu, open XenMobile Mail Manager.
3. Configure the following database properties:
   1. Select the Configure > Database tab.
   2. Enter the name of the SQL Server (defaults to localhost).
   3. Keep the database as the default CitrixXmm.
   4. Select one of the following Authentication 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.



Server: localhost
Database: CitrixXMM
Authentication: Sql
User name: JoeAdmin
Password: ••••••••••••

5. Click Test Connectivity to check that a connection can be made to the SQL Server and then click Save.

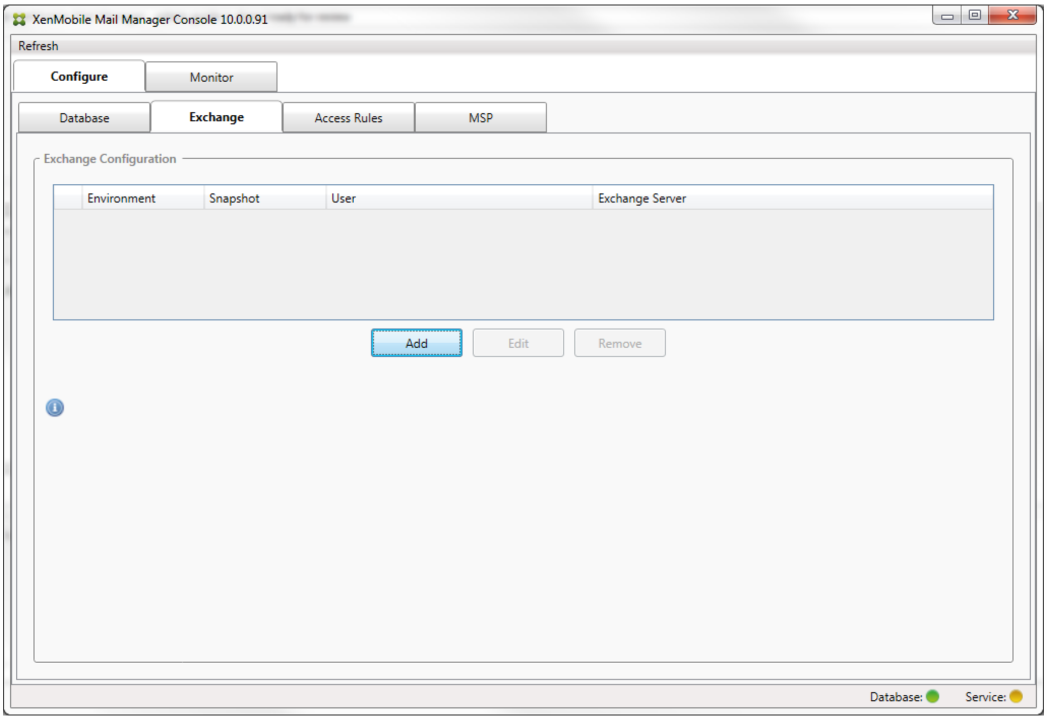
4. A message prompts you to restart the service. Click Yes.



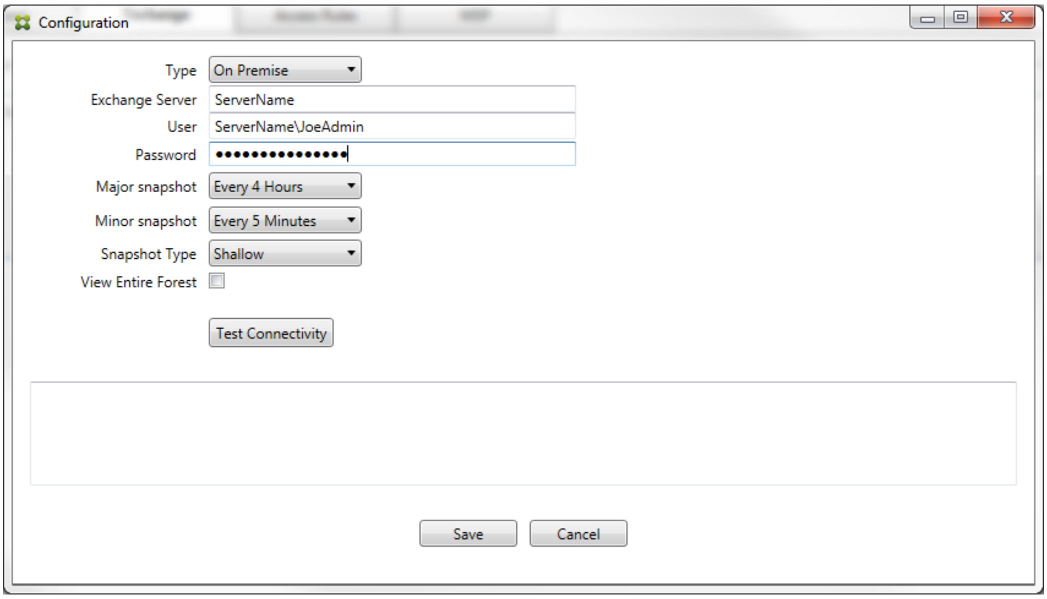
For the changes you have made to take effect, the Citrix XenMobile Mail Manager service must be restarted.

Would you like to restart the service now?

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.

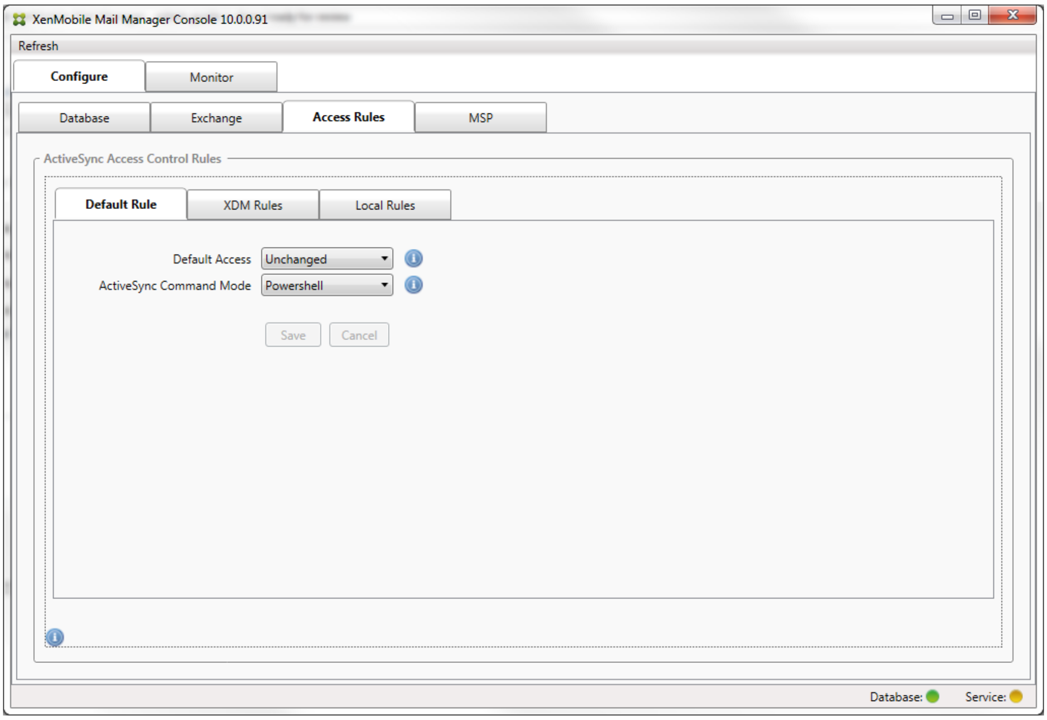


Type: On Premise
Exchange Server: ServerName
User: ServerName\JoeAdmin
Password: •••••••••••••••
Major snapshot: Every 4 Hours
Minor snapshot: Every 5 Minutes
Snapshot Type: Shallow
View Entire Forest: □

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.

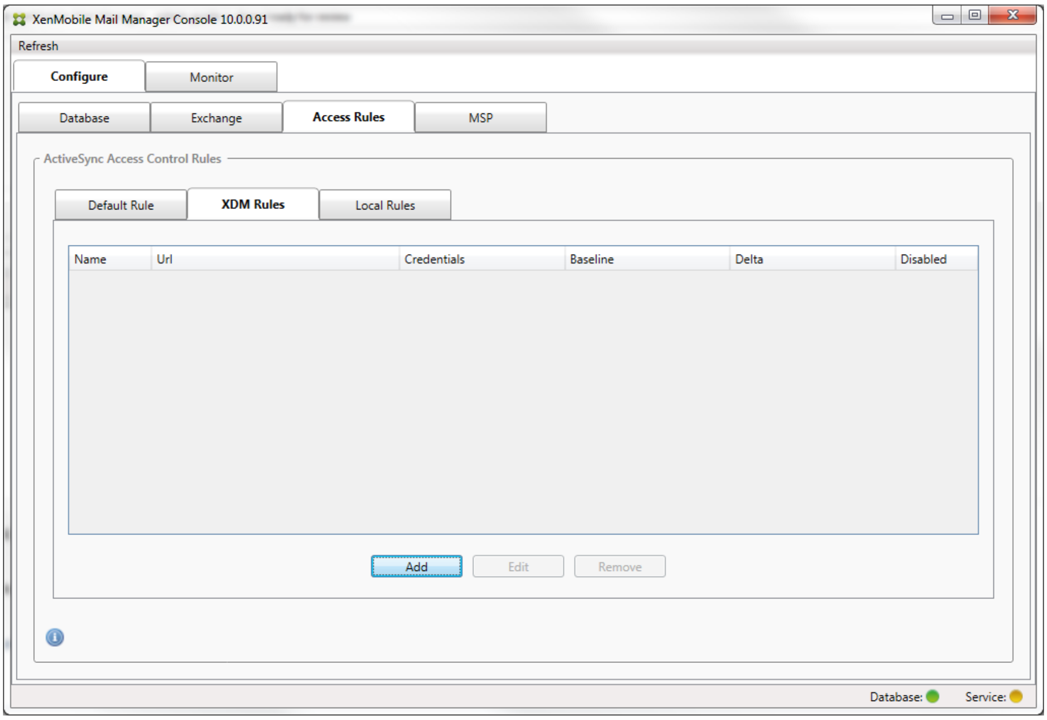
6. Configure the access rules:
    1. Select the Configure > Access Rules tab.



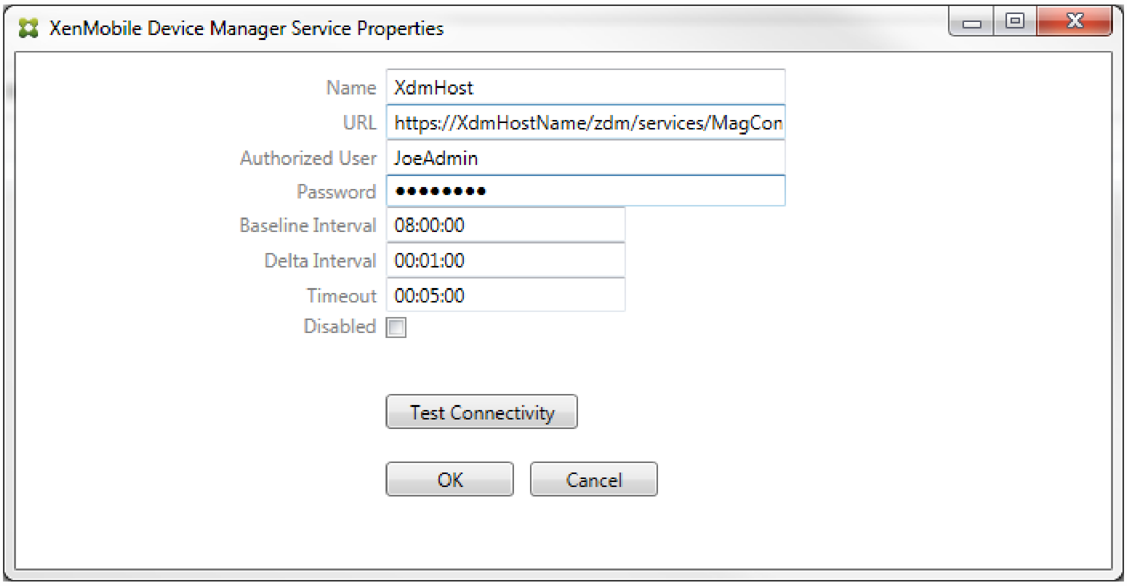
Default Access: Unchanged

ActiveSync Command Mode: Powershell

    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.

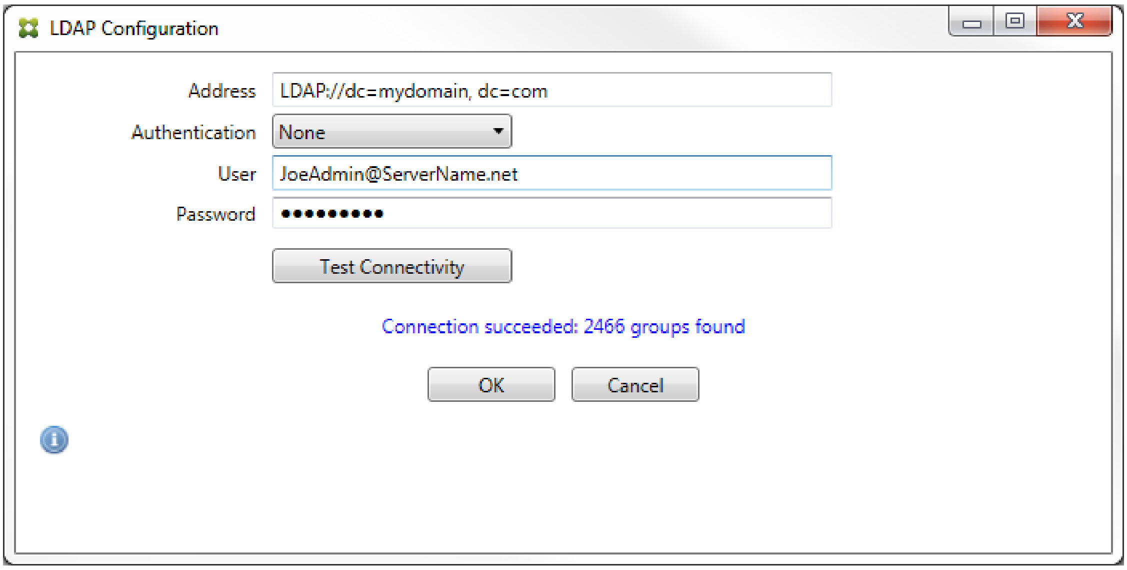


Name	XdmHost
URL	https://XdmHostName/zdm/services/MagCon
Authorized User	JoeAdmin
Password	●●●●●●●●
Baseline Interval	08:00:00
Delta Interval	00:01:00
Timeout	00:05:00
Disabled	□

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.

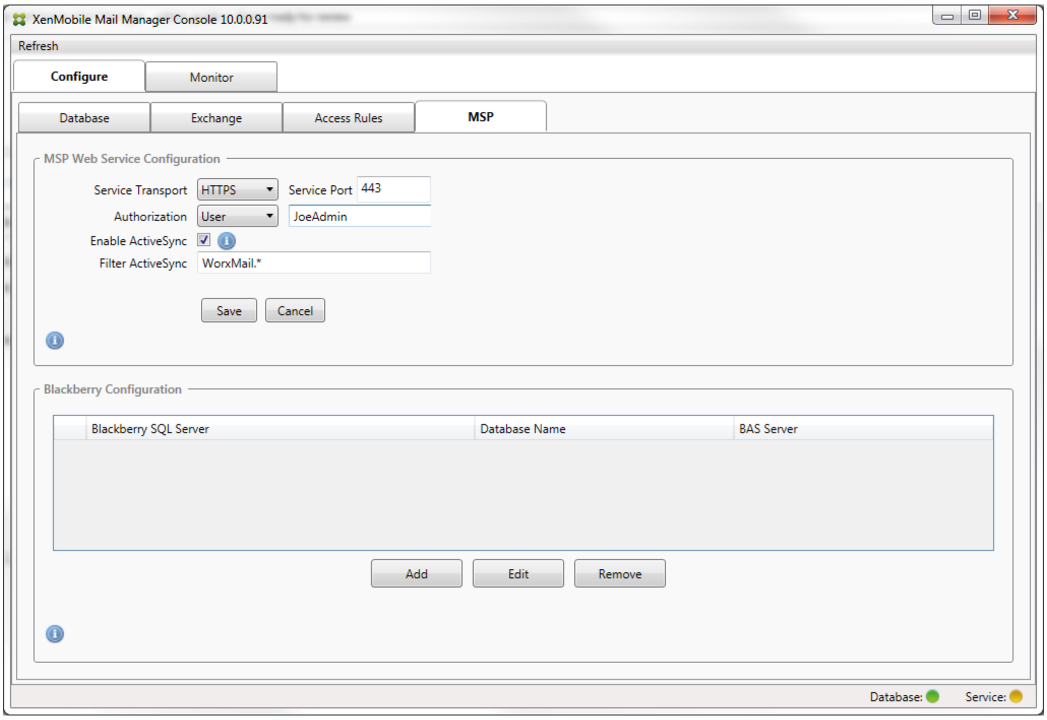


Address: LDAP://dc=mydomain, dc=com
Authentication: None
User: JoeAdmin@ServerName.net
Password: ●●●●●●●●●

Connection succeeded: 2466 groups found

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.



XenMobile Mail Manager Console 10.0.0.91

Service Transport: HTTPS

Service Port: 443

Authorization: User — JoeAdmin

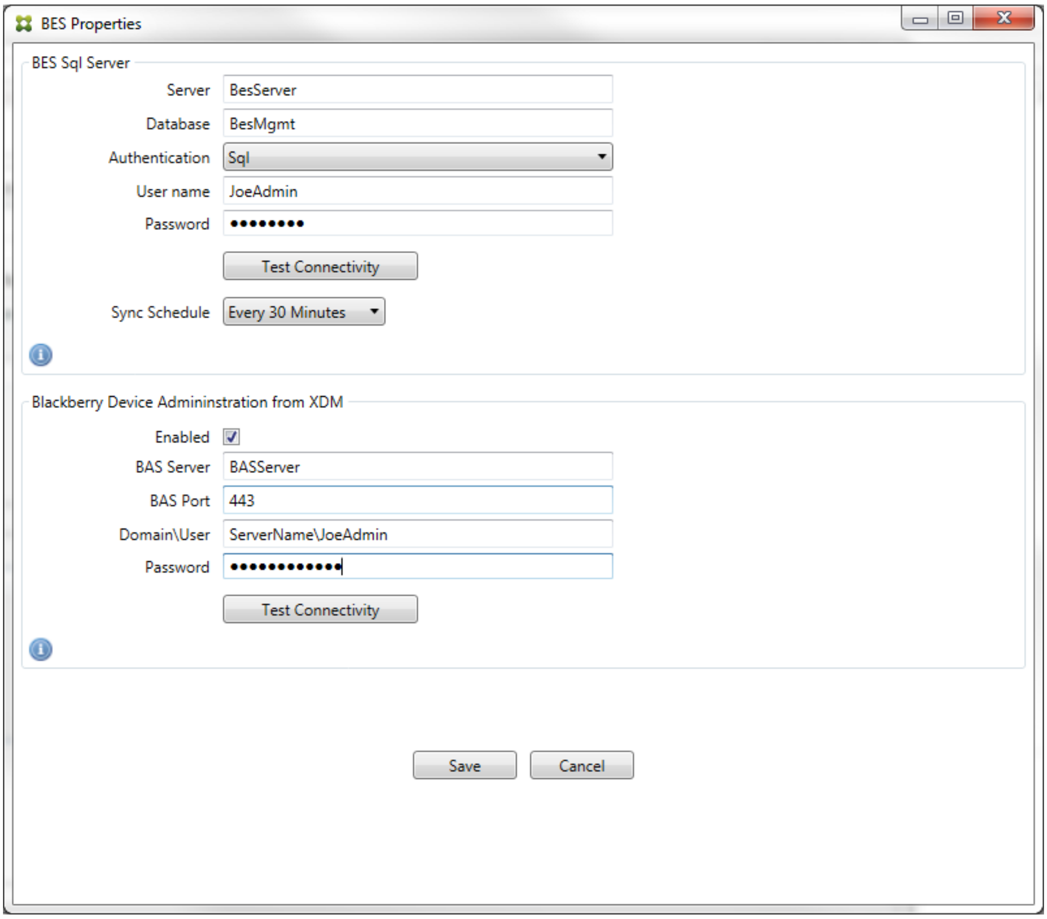
Enable ActiveSync: ☑

Filter ActiveSync: WorxMail.*

Blackberry SQL Server	Database Name	BAS Server

  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.



BES Properties

BES Sql Server

Server: BesServer

Database: BesMgmt

Authentication: Sql

User name: JoeAdmin

Password: ••••••••

Sync Schedule: Every 30 Minutes

Blackberry Device Admininstration from XDM

Enabled: ☑

BAS Server: BASServer

BAS Port: 443

Domain\User: ServerName\JoeAdmin

Password: •••••••••••••

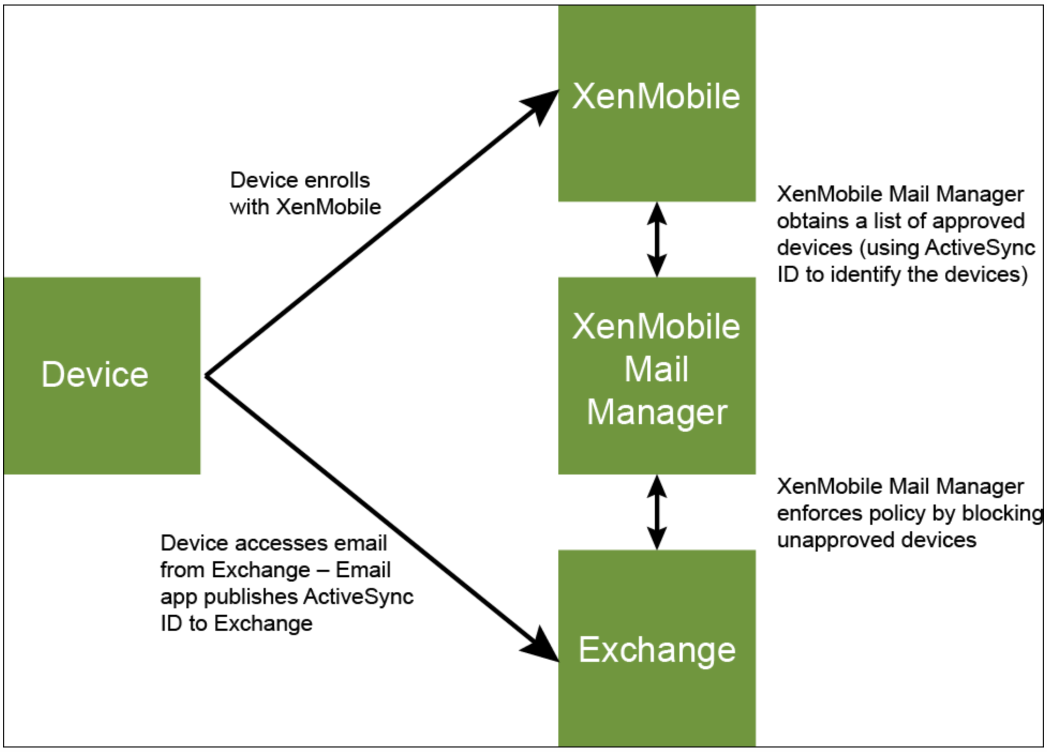
3. Enter the database name of the BES management database.
4. Select the Authentication mode. If you select Windows Integrated authentication, the user account of the XenMobile Mail Manager service is the account that is used to connect to the BES SQL Server.
   Note: If you also choose Windows Integrated 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. Worx 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:


XenMobile
Device enrolls with XenMobile
XenMobile Mail Manager obtains a list of approved devices (using ActiveSync ID to identify the devices)
Device
XenMobile Mail Manager
XenMobile Mail Manager enforces policy by blocking unapproved devices
Device accesses email from Exchange – Email app publishes ActiveSync ID to Exchange
Exchange

If XenMobile sends XenMobile Mail Manager an ActiveSync ID that is different from the ID the device publishes to Exchange, XenMobile Mail Manager cannot indicate to Exchange what to do with the device.

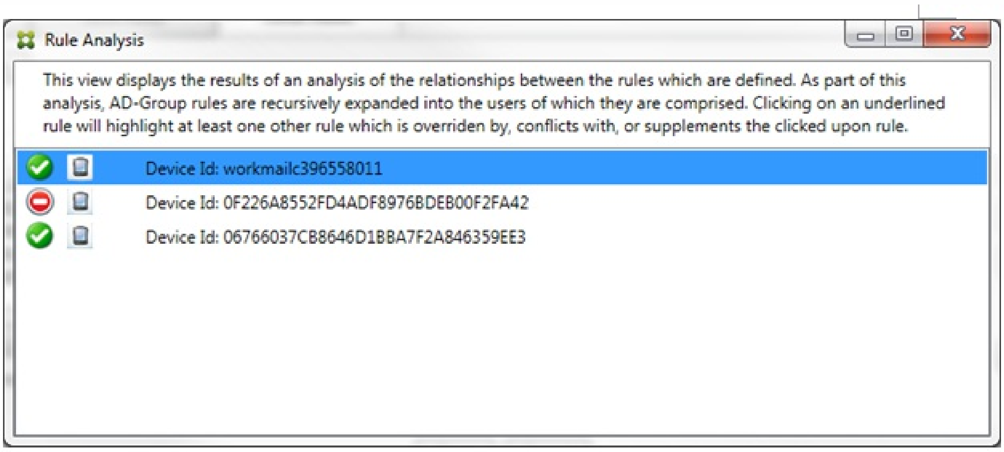
Matching ActiveSync IDs works reliably on most platforms; however, Citrix has found that on some Android implementations, the ActiveSync ID from the device is different from the ID that the mail client advertises to Exchange. To mitigate this problem, you can do the following:

- On the Samsung SAFE platform, push the device ActiveSync configuration from XenMobile.
- On all other Android platforms, push both the Touchdown app and the Touchdown ActiveSync configuration from XenMobile.

This does not, however, prevent an employee from installing an email client other than Touchdown on an Android device. To guarantee that your corporate email access policy is enforced properly, you can adopt a defensive security stance and configure XenMobile Mail Manager to block emails by setting the static policy to Deny by default. This means that if an employee does configure an email client on an Android device other than Touchdown, and if ActiveSync ID detection does not work properly, the employee is denied corporate email access.

-
-
-
-

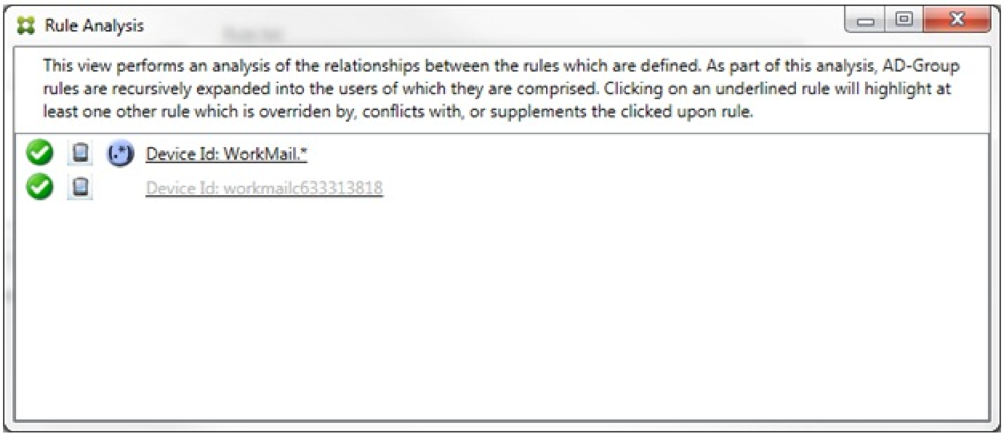
-
-
-



Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

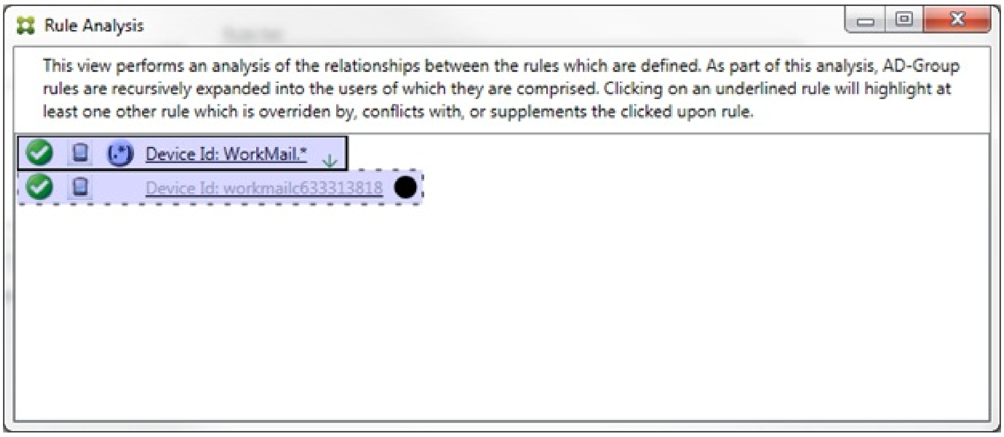
- ✓ Device Id: workmailc396558011
- ⊖ Device Id: 0F226A8552FD4ADF8976BDEB00F2FA42
- ✓ Device Id: 06766037CB8646D1BBA7F2A846359EE3



Rule Analysis

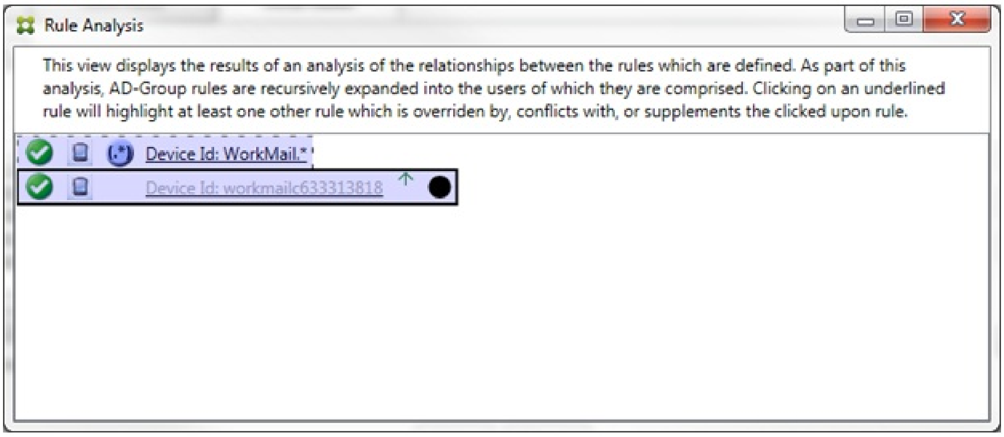
This view performs an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

- ✓ (.*) Device Id: WorkMail.*
- ✓ Device Id: workmailc633313818



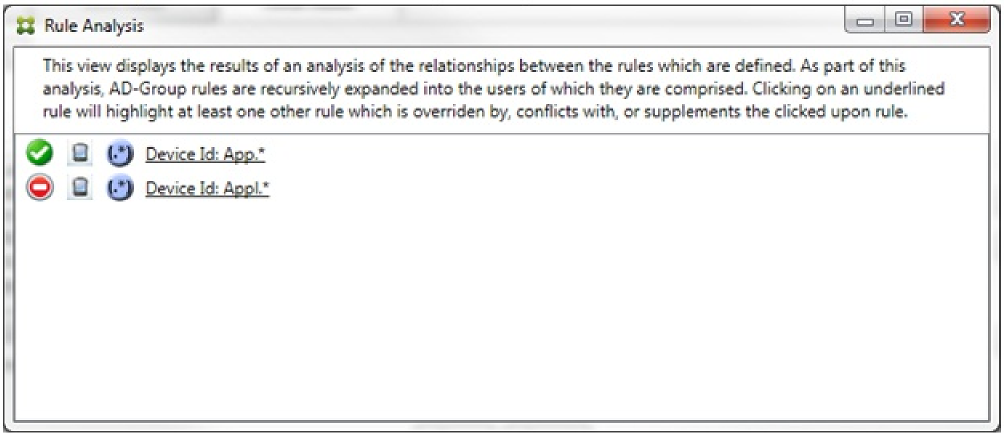
Rule Analysis

This view performs an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.



Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

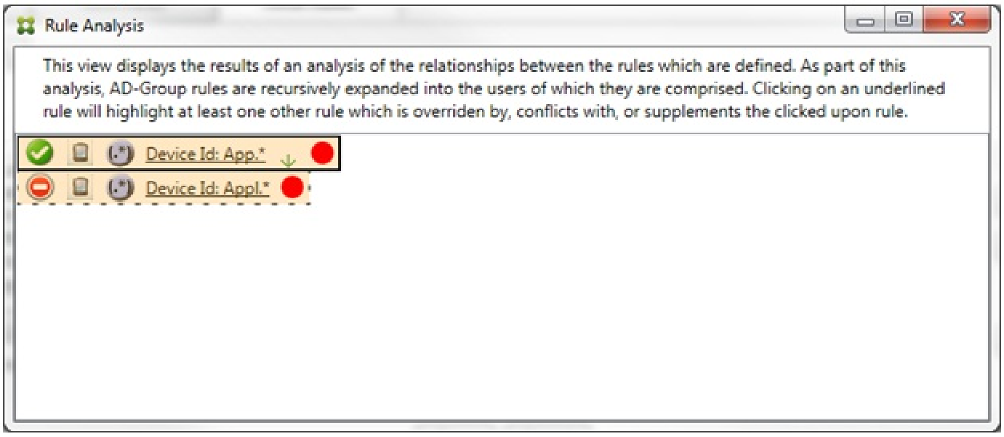


Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

✓ Device Id: App.*

⊖ Device Id: Appl.*

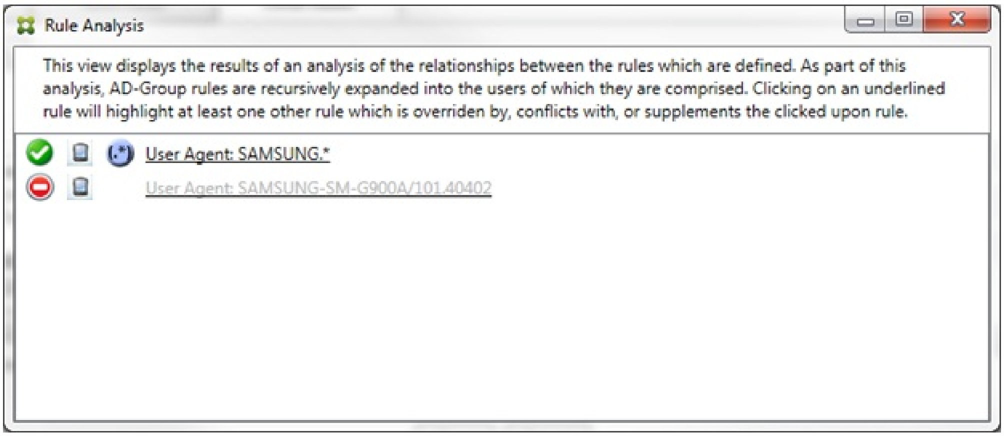


Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

✓ Device Id: App.* ●

⊖ Device Id: Appl.* ●

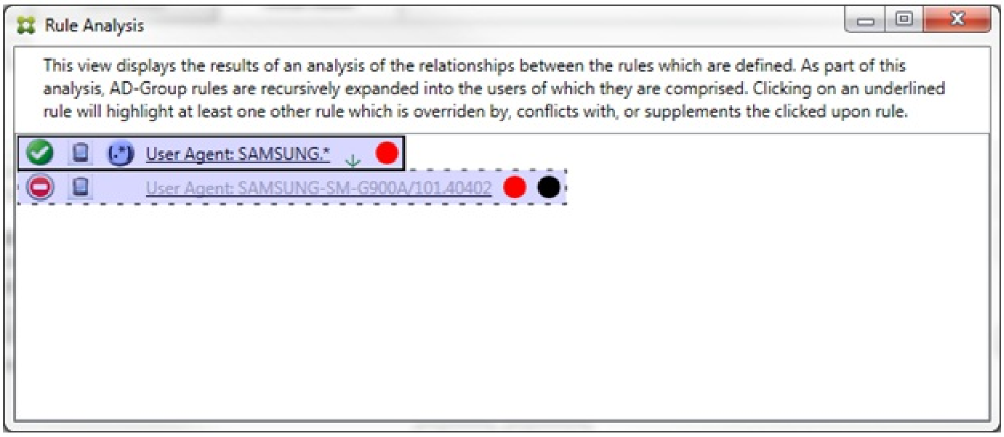


Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

User Agent: SAMSUNG.*

User Agent: SAMSUNG-SM-G900A/101.40402

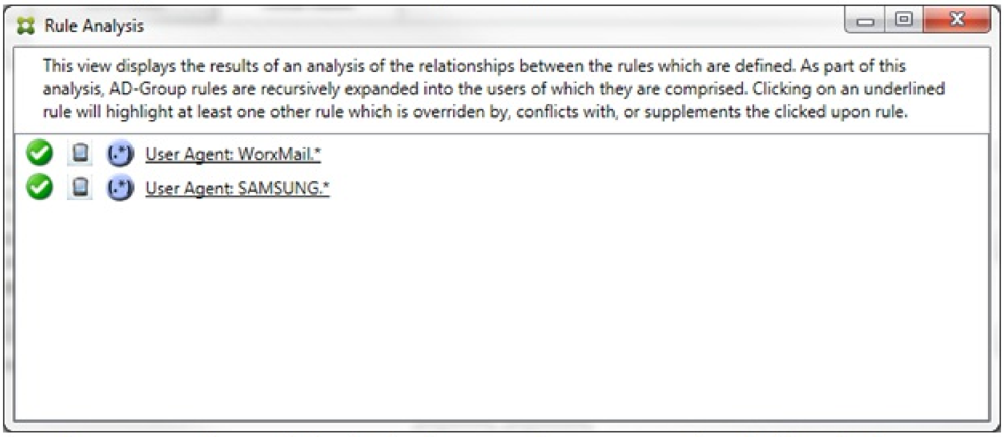


Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

User Agent: SAMSUNG.*

User Agent: SAMSUNG-SM-G900A/101.40402

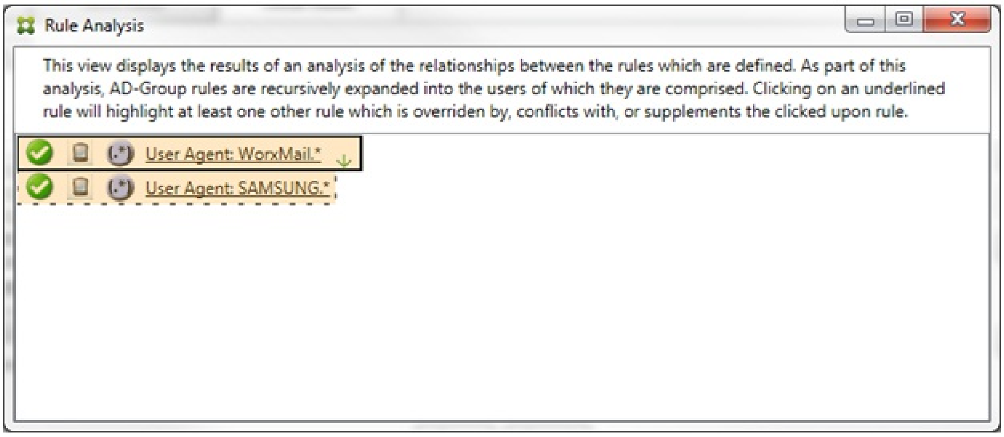


Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

✓ User Agent: WorxMail.*

✓ User Agent: SAMSUNG.*



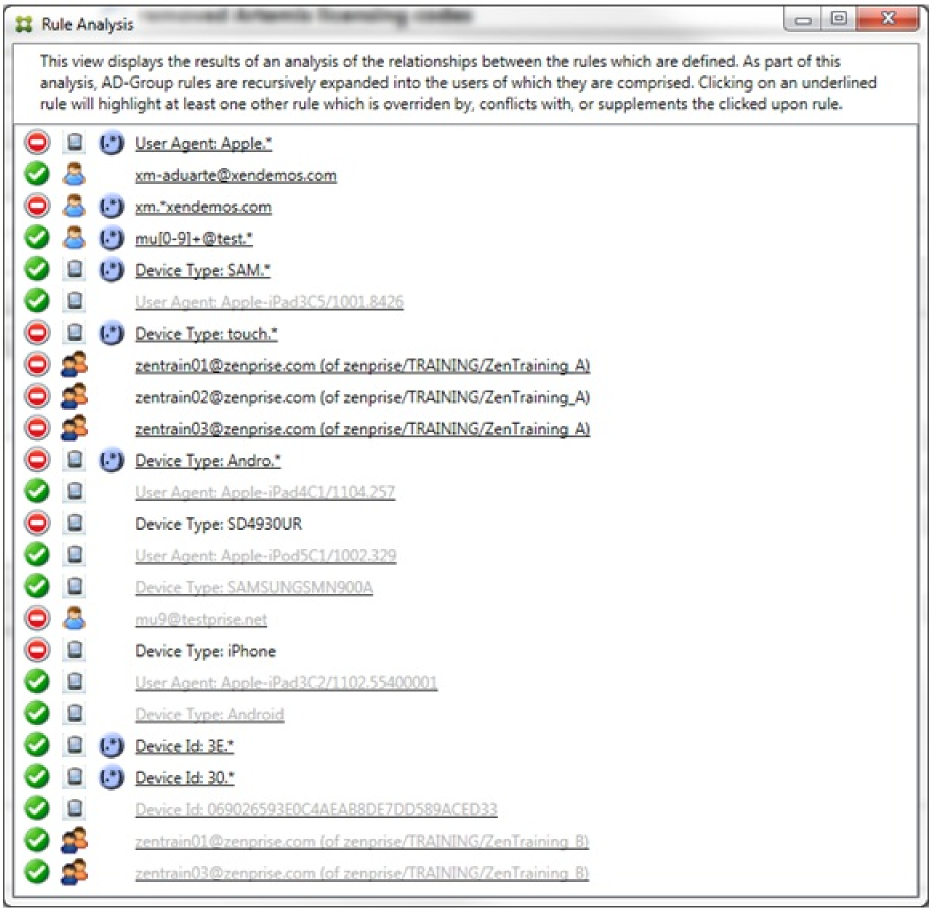
Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

✓ User Agent: WorxMail.*

✓ User Agent: SAMSUNG.*

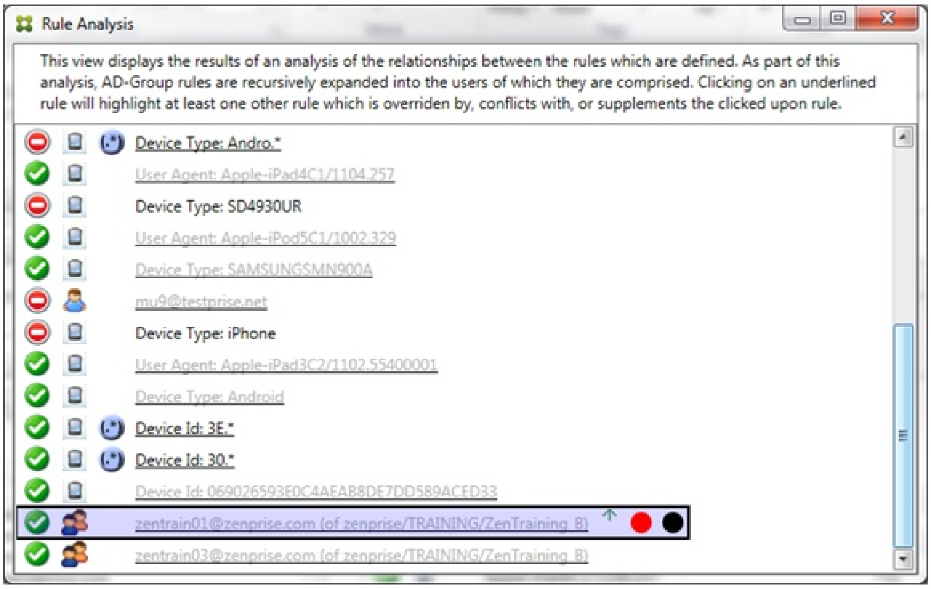
(.*)



Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

- ⛔ (.*) User Agent: Apple.*
- ✓ xm-aduarte@xendemos.com
- ⛔ (.*) xm.*xendemos.com
- ✓ (.*) mu[0-9]+@test.*
- ✓ (.*) Device Type: SAM.*
- ✓ User Agent: Apple-iPad3C5/1001.8426
- ⛔ (.*) Device Type: touch.*
- ⛔ zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
- ⛔ zentrain02@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
- ⛔ zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
- ⛔ (.*) Device Type: Andro.*
- ✓ User Agent: Apple-iPad4C1/1104.257
- ⛔ Device Type: SD4930UR
- ✓ User Agent: Apple-iPod5C1/1002.329
- ✓ Device Type: SAMSUNGSMN900A
- ⛔ mu9@testprise.net
- ⛔ Device Type: iPhone
- ✓ User Agent: Apple-iPad3C2/1102.55400001
- ✓ Device Type: Android
- ✓ (.*) Device Id: 3E.*
- ✓ (.*) Device Id: 30.*
- ✓ Device Id: 069026593E0C4AEAB8DE7DD589ACED33
- ✓ zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining_B)
- ✓ zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining_B)

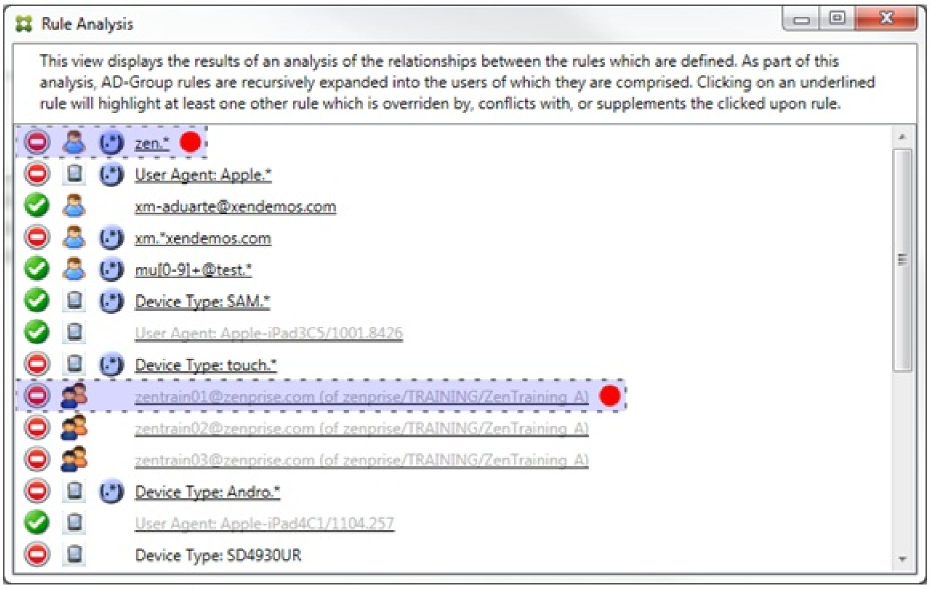


Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

Device Type: Andro.*
User Agent: Apple-iPad4C1/1104.257
Device Type: SD4930UR
User Agent: Apple-iPod5C1/1002.329
Device Type: SAMSUNGSMN900A
mu9@testprise.net
Device Type: iPhone
User Agent: Apple-iPad3C2/1102.55400001
Device Type: Android
Device Id: 3E.*
Device Id: 30.*
Device Id: 069026593E0C4AEAB8DE7DD589ACED33
zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining_B)
zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining_B)

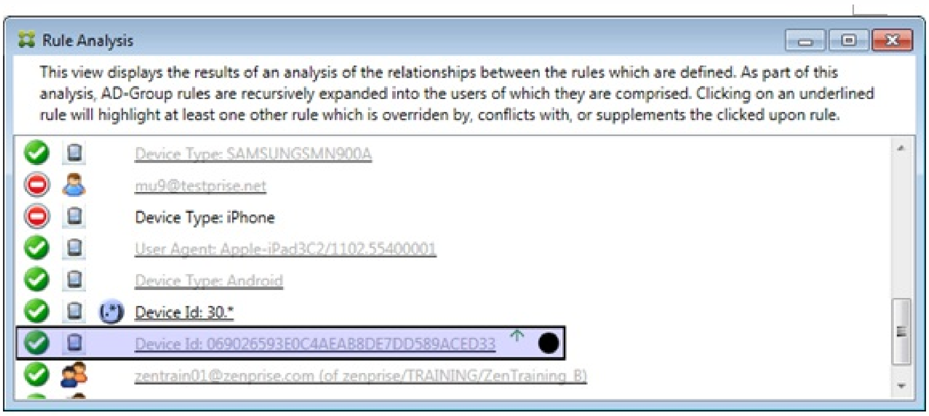
-
-
-



Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

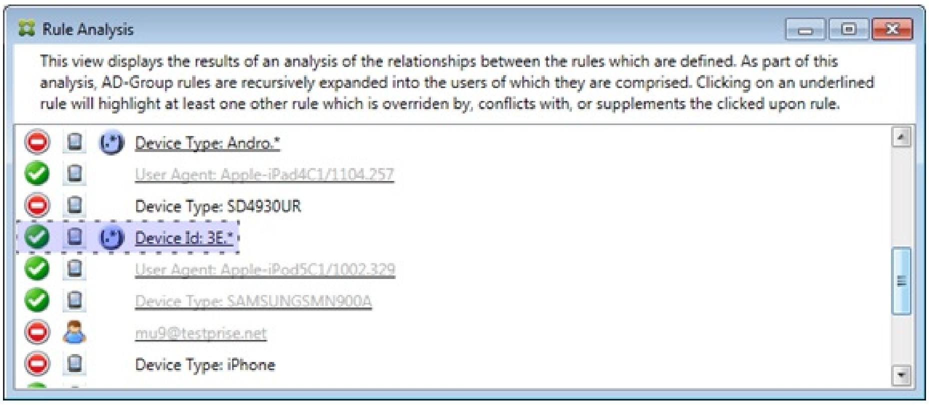
zen.*
User Agent: Apple.*
xm-aduarte@xendemos.com
xm.*xendemos.com
mu[0-9]+@test.*
Device Type: SAM.*
User Agent: Apple-iPad3C5/1001.8426
Device Type: touch.*
zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
zentrain02@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
Device Type: Andro.*
User Agent: Apple-iPad4C1/1104.257
Device Type: SD4930UR



This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

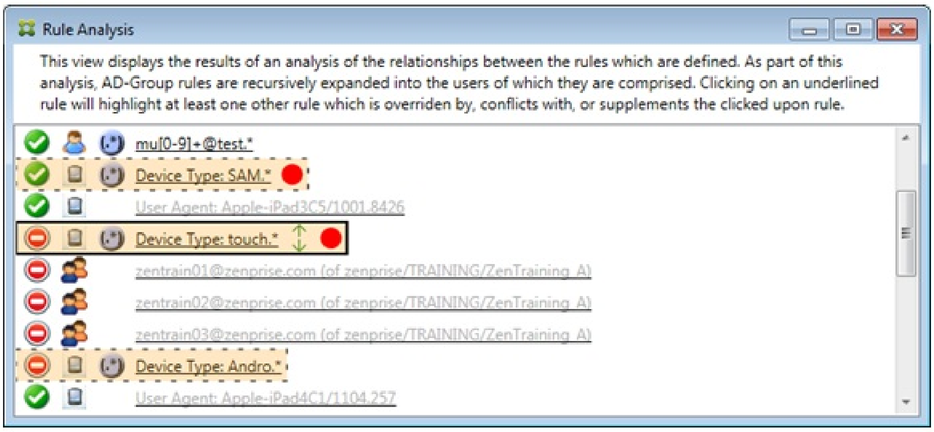
Device Type: SAMSUNGSMN900A
mu9@testprise.net
Device Type: iPhone
User Agent: Apple-iPad3C2/1102.55400001
Device Type: Android
Device Id: 30.*
Device Id: 069026593E0C4AEAB8DE7DD589ACED33
zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining_B)

-
-
-



This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

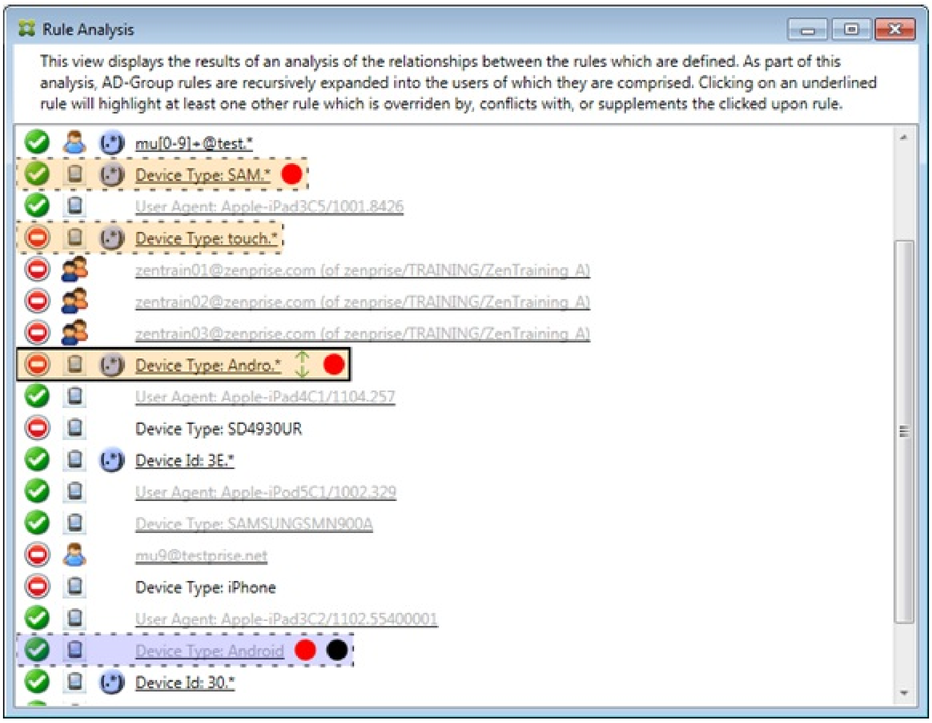
Device Type: Andro.*
User Agent: Apple-iPad4C1/1104.257
Device Type: SD4930UR
Device Id: 3E.*
User Agent: Apple-iPod5C1/1002.329
Device Type: SAMSUNGSMN900A
mu9@testprise.net
Device Type: iPhone



Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

✓ mu[0-9]+@test.*
✓ Device Type: SAM.* ●
✓ User Agent: Apple-iPad3C5/1001.8426
⊖ Device Type: touch.* ↕ ●
⊖ zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
⊖ zentrain02@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
⊖ zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
⊖ Device Type: Andro.*
✓ User Agent: Apple-iPad4C1/1104.257

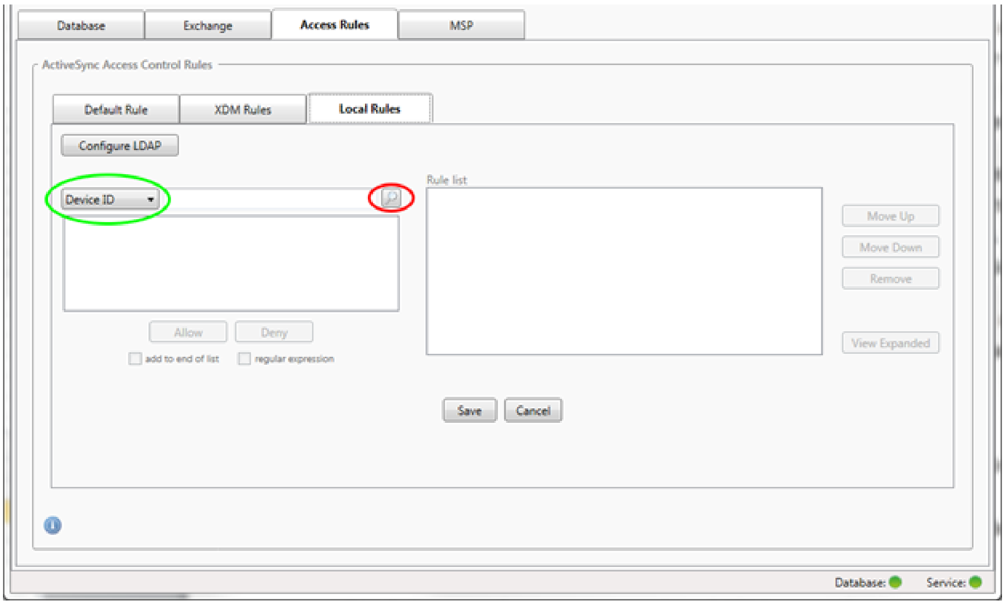


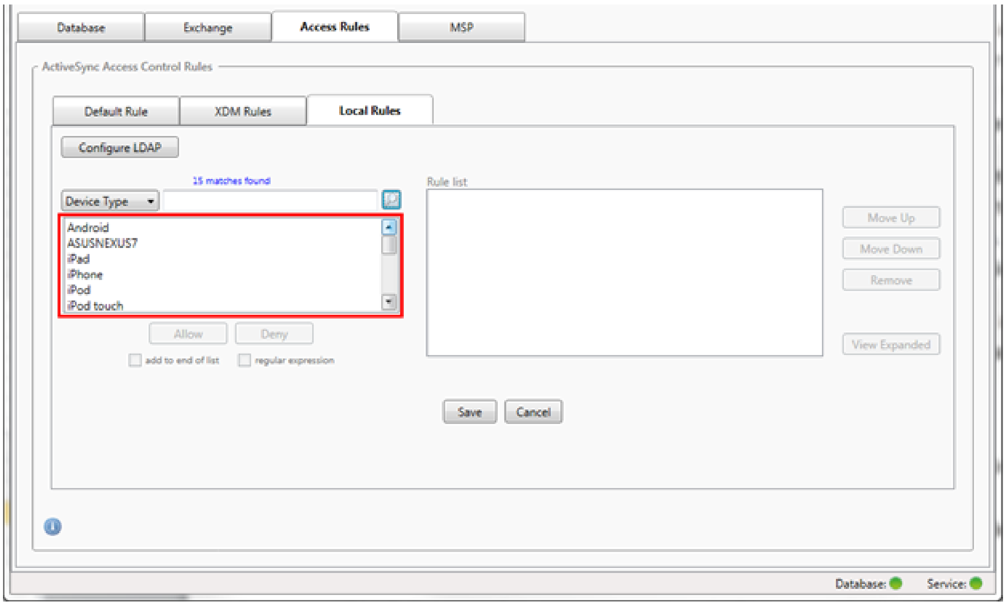
Rule Analysis

This view displays the results of an analysis of the relationships between the rules which are defined. As part of this analysis, AD-Group rules are recursively expanded into the users of which they are comprised. Clicking on an underlined rule will highlight at least one other rule which is overriden by, conflicts with, or supplements the clicked upon rule.

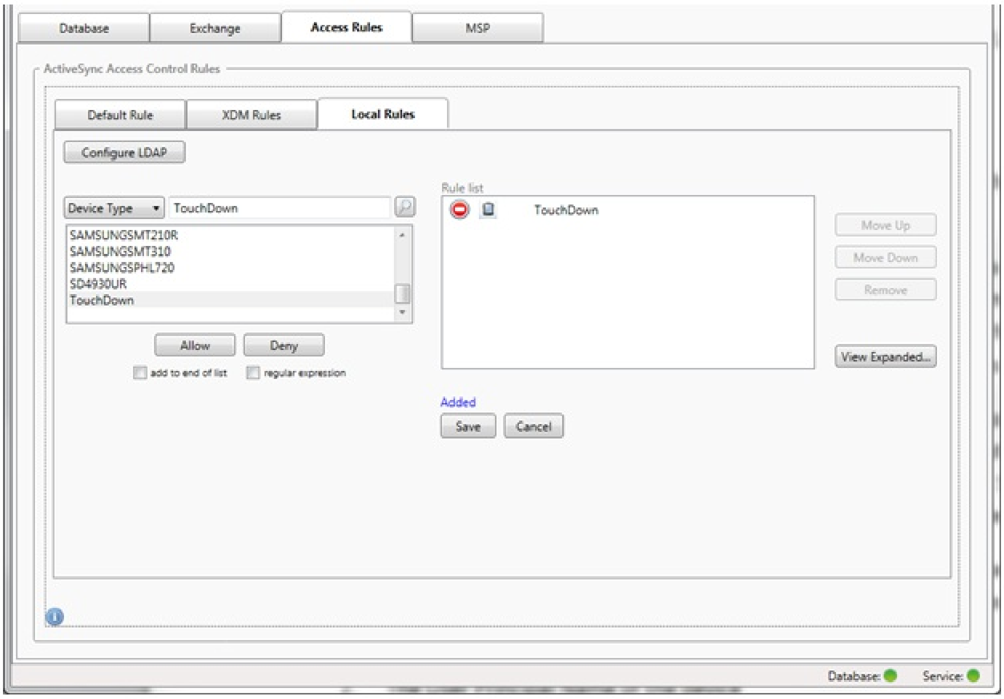
mu[0-9]+@test.*
Device Type: SAM.*
User Agent: Apple-iPad3C5/1001.8426
Device Type: touch.*
zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
zentrain02@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
zentrain03@zenprise.com (of zenprise/TRAINING/ZenTraining_A)
Device Type: Andro.*
User Agent: Apple-iPad4C1/1104.257
Device Type: SD4930UR
Device Id: 3E.*
User Agent: Apple-iPod5C1/1002.329
Device Type: SAMSUNGSMN900A
mu9@testprise.net
Device Type: iPhone
User Agent: Apple-iPad3C2/1102.55400001
Device Type: Android
Device Id: 30.*

To configure a normal expression local rule



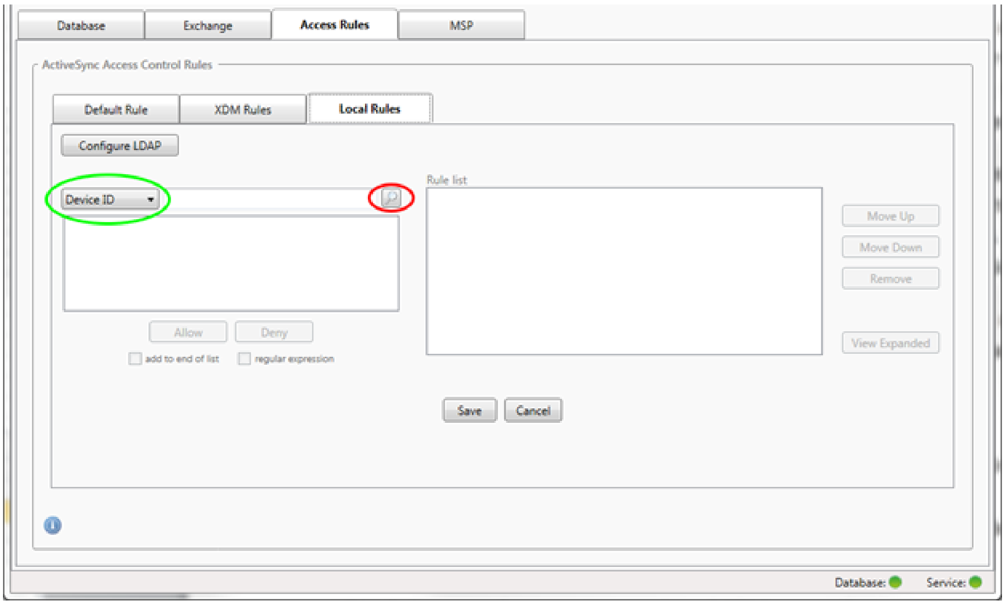


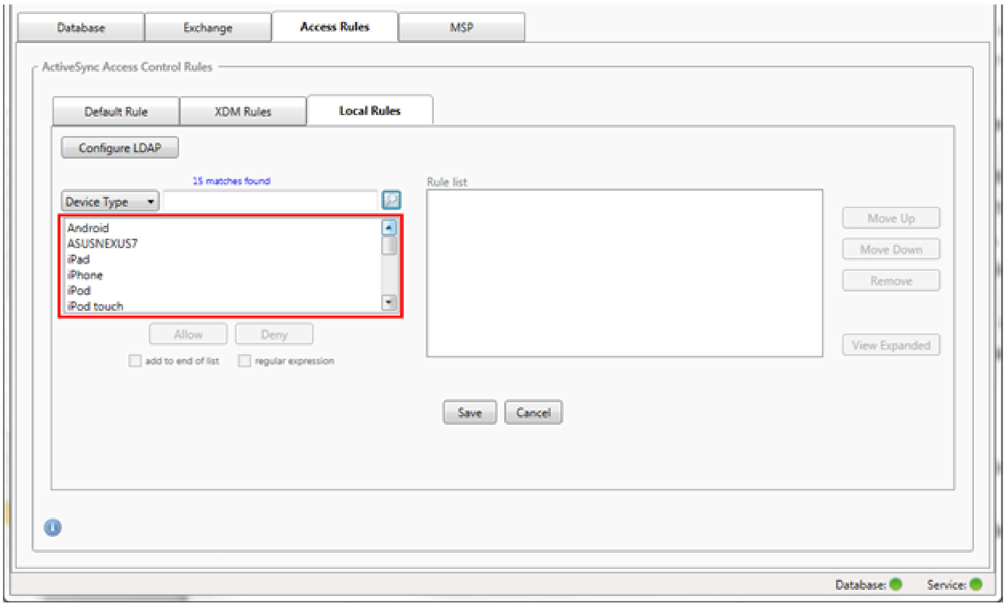
-
-



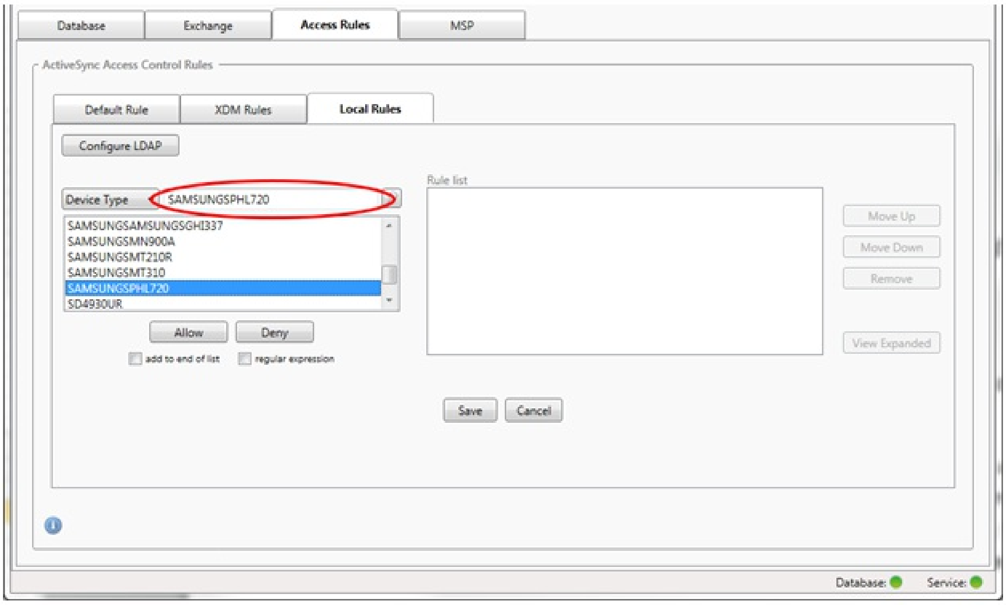
To add a regular expression

(.*)





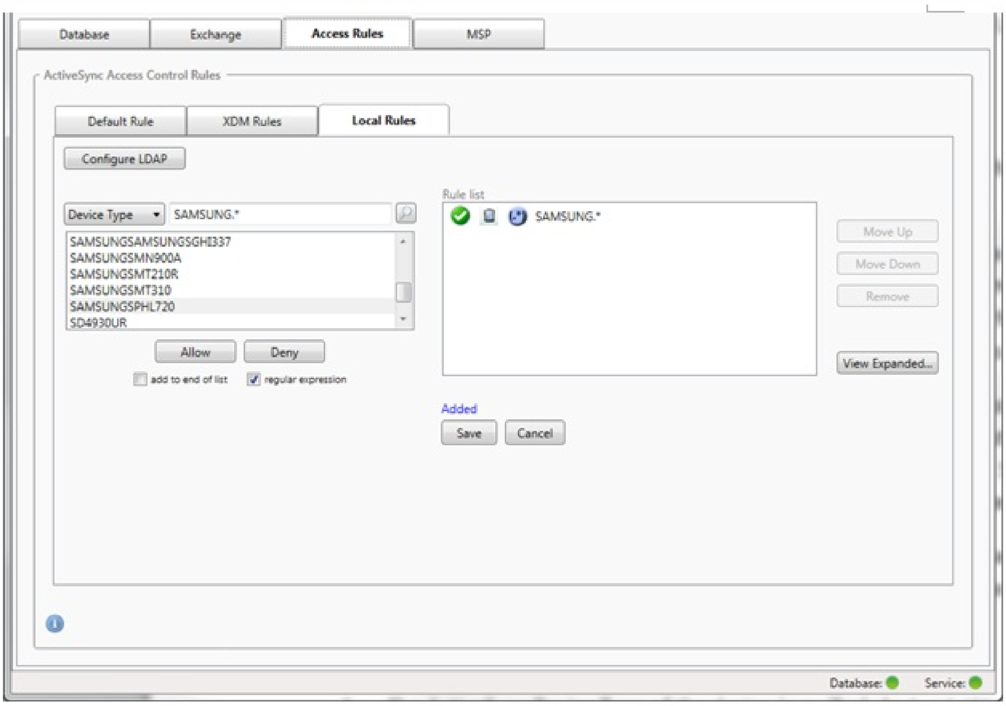
Android
ASUSNEXUS7
iPad
iPhone
iPod
iPod touch



Device Type: SAMSUNGSPHL720

SAMSUNGSAMSUNGSGHI337
SAMSUNGSMN900A
SAMSUNGSMT210R
SAMSUNGSMT310
SAMSUNGSPHL720
SD4930UR

□ add to end of list □ regular expression



Device Type: SAMSUNG.*

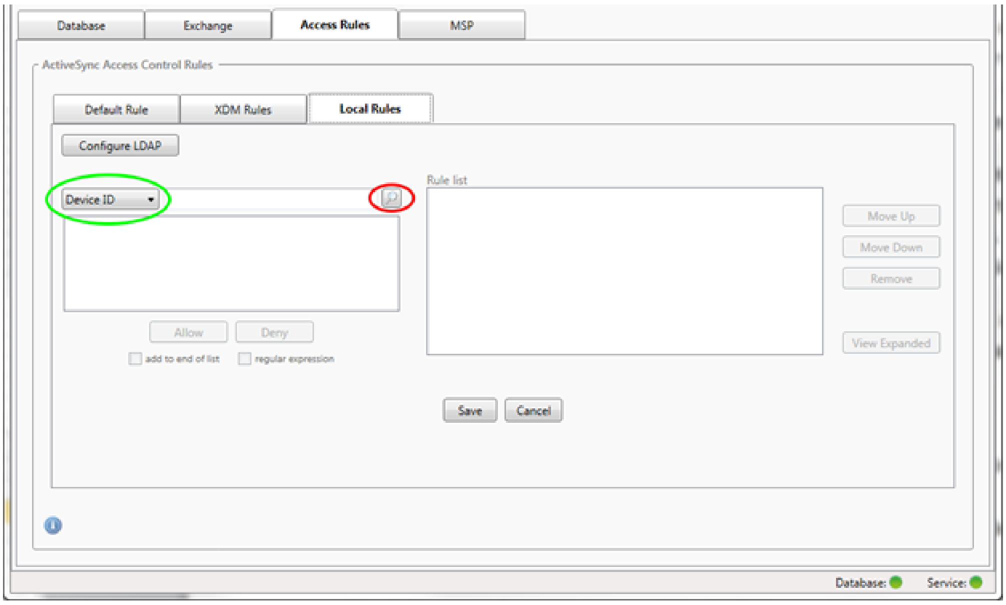
SAMSUNGSAMSUNGSGHI337
SAMSUNGSMN900A
SAMSUNGSMT210R
SAMSUNGSMT310
SAMSUNGSPHL720
SD4930UR

□ add to end of list ☑ regular expression

Rule list: ✓ SAMSUNG.*

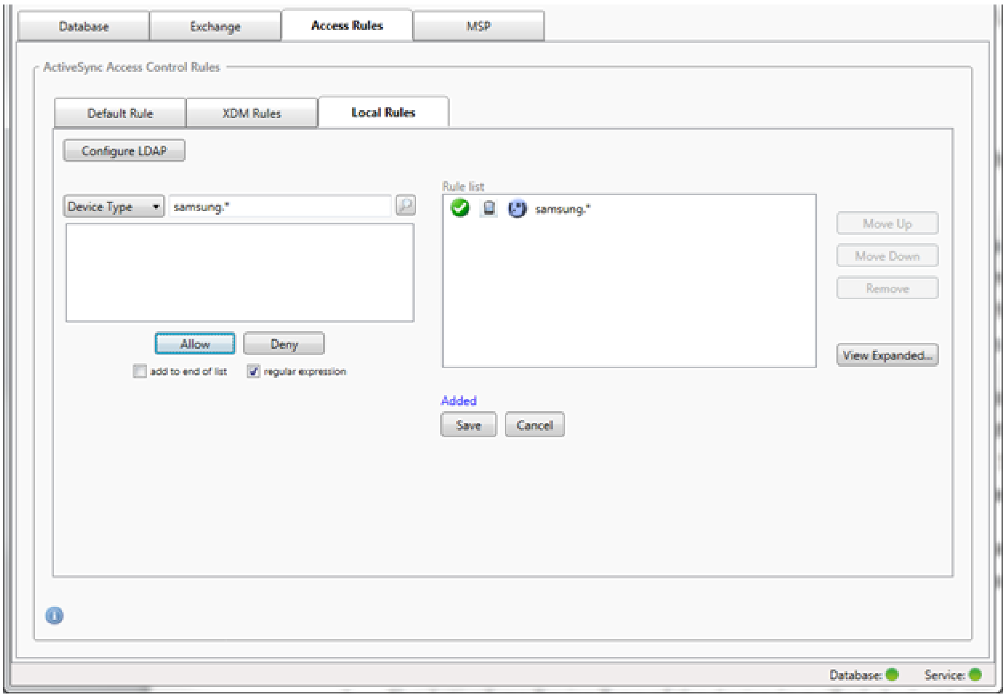
Added

To build an access rule



Device ID

□ add to end of list □ regular expression



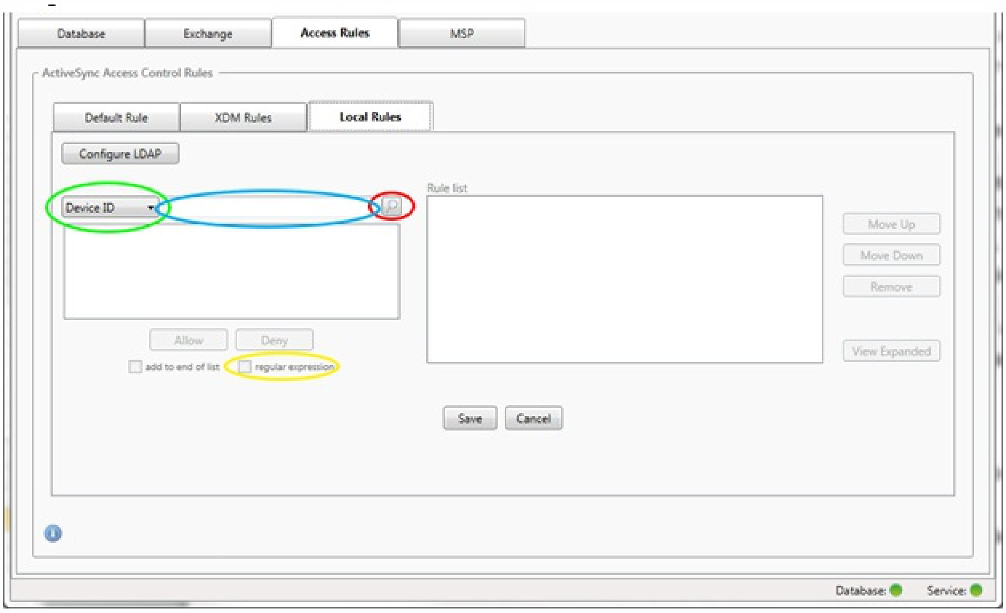
Device Type samsung.*

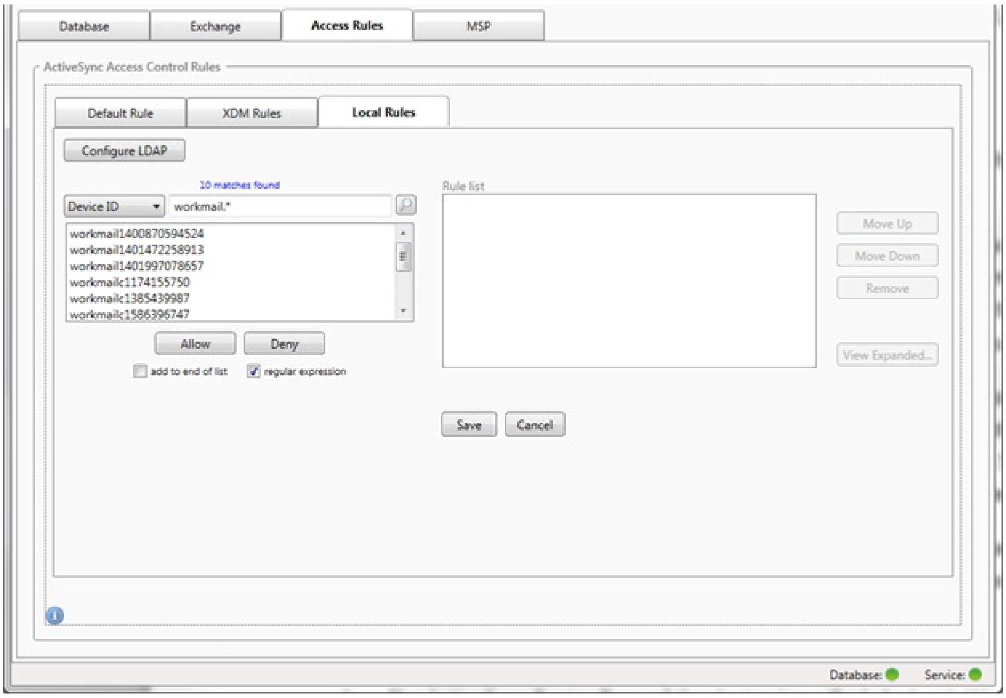
Rule list: ✓ samsung.*

□ add to end of list ☑ regular expression

Added

To find devices





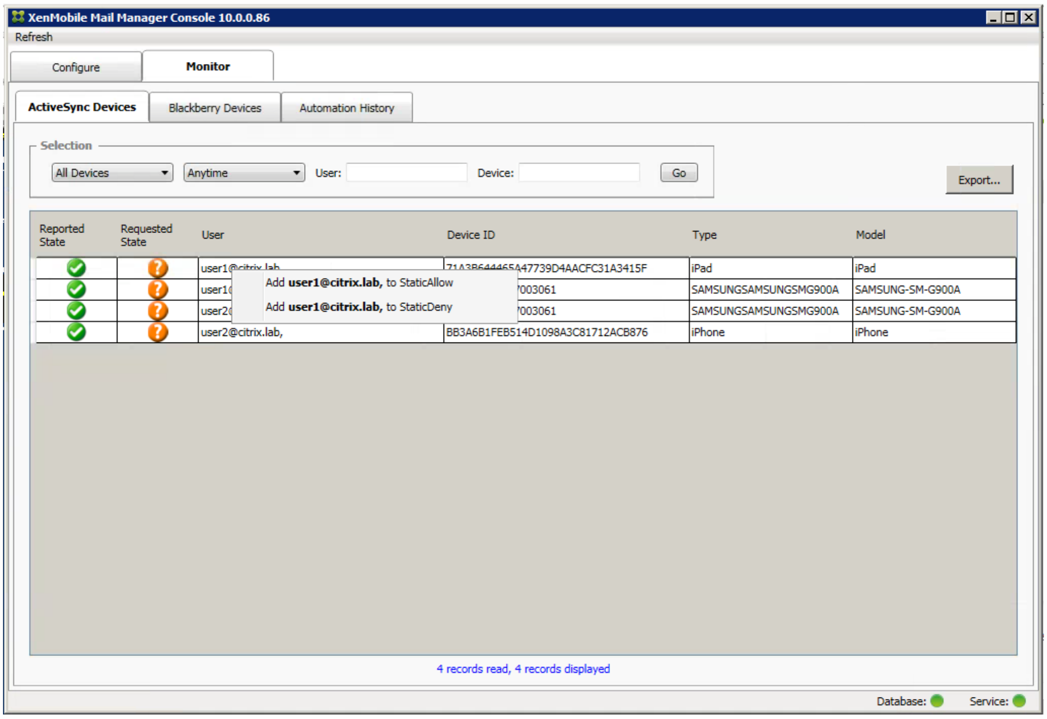
10 matches found

Device ID: workmail.*

workmail1400870594524
workmail1401472258913
workmail1401997078657
workmailc1174155750
workmailc1385439987
workmailc1586396747

□ add to end of list ☑ regular expression

To add an individual user, device, or device type to a static rule



Reported State	Requested State	User	Device ID	Type	Model
✓	?	user1@citrix.lab	71A3B644465A47739D4AACFC31A3415F	iPad	iPad
✓	?	user1	003061	SAMSUNGSAMSUNGSMG900A	SAMSUNG-SM-G900A
✓	?	user2	003061	SAMSUNGSAMSUNGSMG900A	SAMSUNG-SM-G900A
✓	?	user2@citrix.lab,	BB3A6B1FEB514D1098A3C81712ACB876	iPhone	iPhone

Add **user1@citrix.lab,** to StaticAllow
Add **user1@citrix.lab,** to StaticDeny

4 records read, 4 records displayed

Database: ● Service: ●