Deploying XenMobile 10.0 Enterprise Edition (Beta 2)

Hands-on Lab Exercise Guide

November 2014

Contents

Overview

Hands-on Training Module

Objective

This training will provide hands-on experience with the following:

- Initial/Basic configuration of XenMobile Server 10.0
- Integrating XenMobile Server with NetScaler Gateway

Prerequisites

- Basic understanding of Web/SaaS/Mobile apps.
- Familiarity with navigating the NetScaler Configuration Utility.
- Basic understanding of http/https communication.
- Basic understanding of networking concepts (IE: IP addressing and communication)

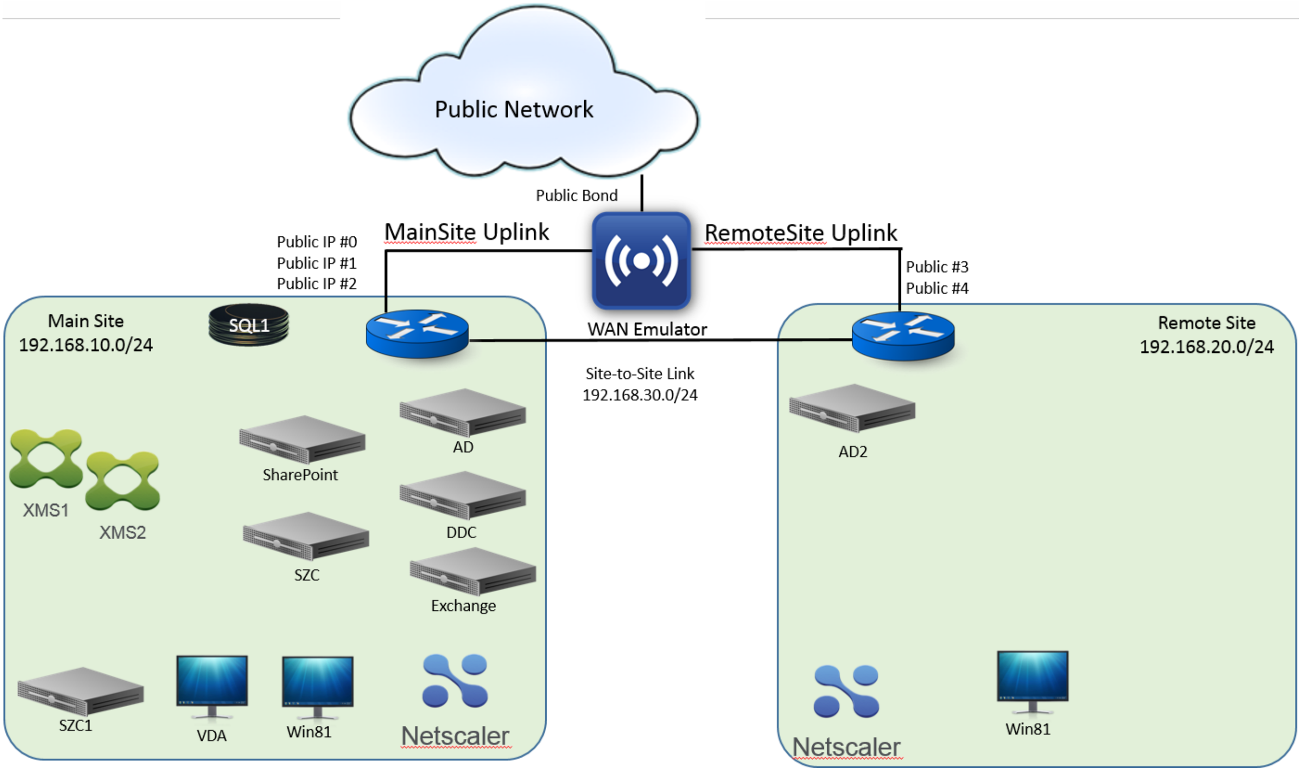
Audience

Citrix Partners, Customers, Sales Engineers, & Consultants.

Lab Environment Details

The lab environment for the exercises to come contains the following:

- External access to common services (HTTP, SSL, SMTP, RDP, SSH, DNS) to simulate a real production environment customized
- 1 Active Directory namespace
- Pre-configured enterprise applications (Exchange & MSSQL)
- XenMobile Enterprise components (App Controller, NetScaler Gateway, W2K12 for MDM)



The Student Desktop is accessed remotely using Citrix Receiver running on your laptop. All windows applications such as XenCenter, (the XenServer GUI management tool), are accessed from the Student Desktop.

Lab Guide Conventions

⚠	This symbol indicates particular attention must be paid to this step
ℹ	Special note to offer advice or background information
`reboot`	Text the student enters or an item they select is printed like this
`VMDemo`	Filename mentioned in text or lines added to files during editing
Start	Bold text indicates reference to a button or object
▭	Focuses attention on a particular part of the screen (R:255 G:20 B:147)
▭	Shows where to click or select an item on a screen shot (R:255 G:102 B:0)

List of Virtual Machines Used

VM Name	IP Address	Description / OS
Site1-AD.training.lab	192.168.10.11	Windows Server 2012 R2 Standard. Domain controller for training.lab, DNS, DHCP services, and license server.
Site1-DDC	192.168.10.40	Windows Server 2012 R2 Std. with XenDesktop 7.6 installed.
Site1-XMS1 Site1-XMS2	192.168.10.20 192.168.10.23	XenMobile Server 10.0. Students will perform the initial/basic XenMobile Server and configure apps, policies, and delivery groups.
Site1-Exchange	192.168.10.15	Windows Server 2008 R2 with Exchange 2010 installed

Site1-NS1	NSIP=192.168.10.50
	VIP=192.168.10.100
	VIP=192.168.10.101
	VIP= 192.168.10.21
		NS/AGEE 10.5. Students will perform steps to integrate NetScaler Gateway with Citrix StoreFront and XenMobile Server.

Site1-SharePoint	192.168.10.14	Windows Server 2008 R2 with SharePoint 2010 installed.
Site1-SQLServer	192.168.10.12	Windows Server 2012 Standard with SQL Server installed.
Site1-SZC	192.168.10.41	Windows Server 2008 R2 Enterprise. Students will install ShareFile Storage Zone Controller on this virtual machine.
Site1-VDA	192.168.10.205	Windows 8.1 Professional with XenDesktop VDA installed.
Site1-Win81Client	192.168.10.201	Windows 8.1 Professional virtual machine
Site2-AD2.remote.lab	192.168.20.11	Windows Server 2012 R2 Standard. Domain controller for remote.lab, DNS, DHCP services, and license server installed.
Site2-NS1	192.168.20.50	NS/AGEE 10.5. Students will perform steps to integrate NetScaler Gateway with Citrix StoreFront and XenMobile Server.
Site2-Win81Client		Windows 8.1 Professional virtual machine

Required Lab Credentials

The credentials required to connect to the environment and complete the lab exercises.

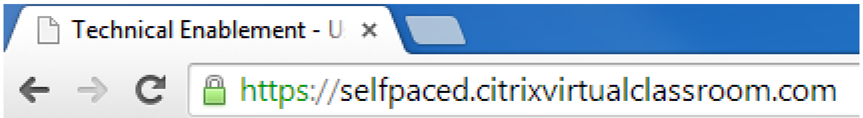
VM Name	Username	Password	Description
Site1-Win81Client & Site2-Win81Client	administrator	Citrix123	Domain admin
Site1-NS1 & Site2-NS1	nsroot	nsroot	NetScaler admin
Site1-AD.training.lab	administrator	Citrix123	Domain admin
Site2-AD.remote.lab	administrator	Citrix123	Domain admin

How to Log into the Lab Environment

Follow the directions below to access the lab environment.

STEP 1

Launch your web browser and go to the training portal URL address provided by your instructor (eg: http://selfpaced.citrixvirtualclassroom.com)

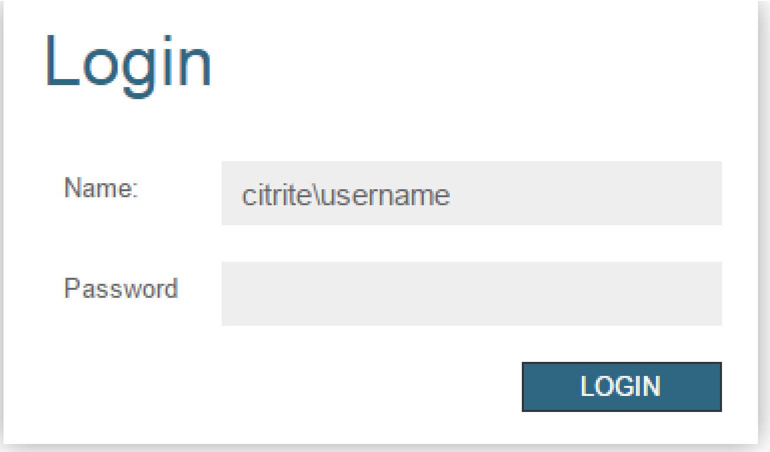


Technical Enablement - U

https://selfpaced.citrixvirtualclassroom.com

STEP 2

On the website, enter your username and password:



Login

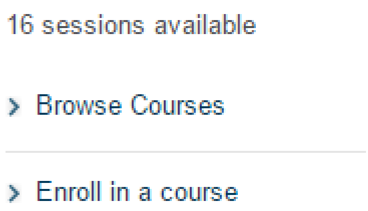
Name: citrite\username

Password

Click **Login**.

STEP 3

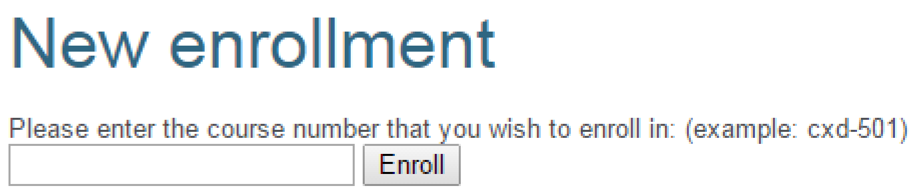
After your are logged in, click **Enroll in a course**.



16 sessions available

STEP 4

Enter your course number and click **Enroll**.

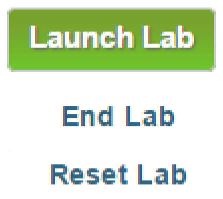


New enrollment

Please enter the course number that you wish to enroll in: (example: cxd-501)

Step 5

Wait for the your environment to be provisioned. Then click on Launch Lab.



Scenario

You have been hired as a consultant to deploy a XenMobile Enterprise Edition for MobileTeX, Inc. in order to provide management of devices along with access to internal applications and data resources from any mobile device. Your task is to use the guidelines outlined below to implement a solution that meets the business needs.

Guidelines:

- **Data**: Company data should be available to employees internally and externally. This data is publicly available and should only be accessed using read-only methods.
- End users should be able to browse internal sites securely.

Exercise 1

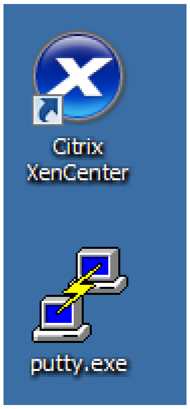
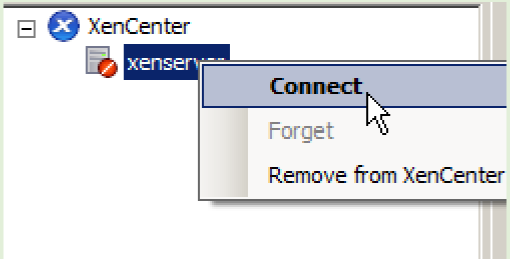
Initial Configuration of the XenMobile Titan Server

Overview

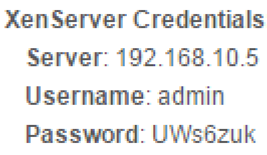
Configuring the XenMobile Server is a two-part process. The initial configuration is done at the console of the server by configuring the new password, network settings (ie: IP address, subnet mask, default gateway), database location, and external fqdn. Once this is done, you connect to the Administration Console from a web browser to configure the basic configuration via the Start-up Wizard. In this lab, you will perform the initial configuration at the console of the XenMobile Titan server.

Step by step guidance

Estimated time to complete this lab: **12** minutes.

Step	Action
1.	On your landing desktop, launch **Citrix XenCenter**. 
2.	If an existing xenserver is displayed, right-click the **xenserver** node and click `Connect`. If it does not exist, select the **XenCenter** node and click `Add New Server`.  XenCenter xenserv... Connect Forget Remove from XenCenter

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>3.</td><td>
Enter the XenServer Credentials from your portal page.

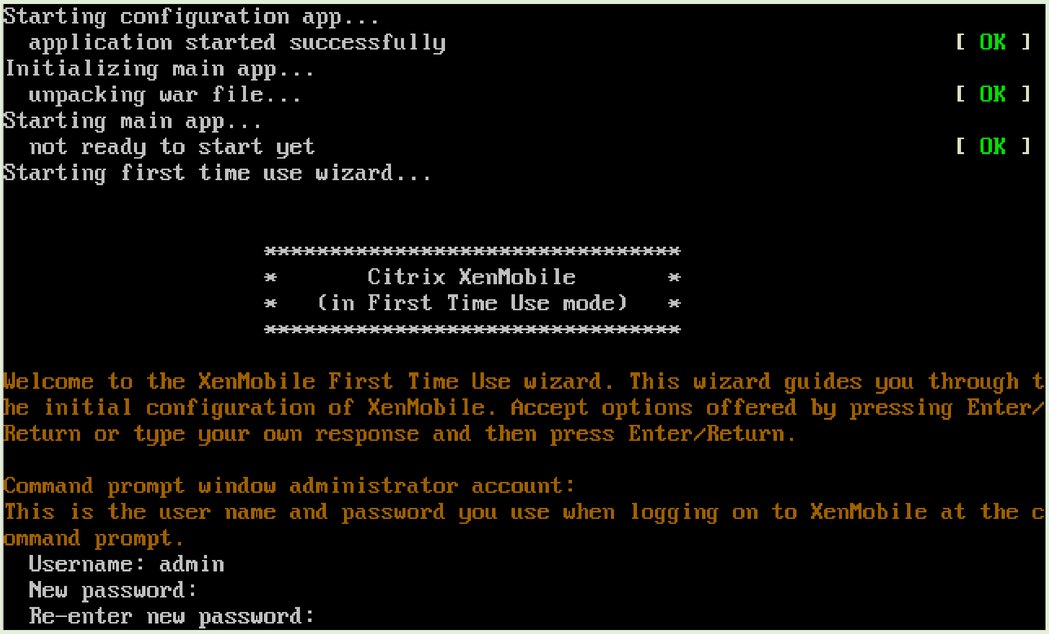


XenServer Credentials:
Server: 192.168.10.5
Username: admin
Password: UWs6zuk

<table>
<tr><td>Server:</td><td>Xenserver or 192.168.10.5</td></tr>
<tr><td>User name:</td><td></td></tr>
<tr><td>Password:</td><td></td></tr>
</table>
</td></tr>
<tr><td>4.</td><td>
Within XenCenter, select the **SITE1-XMS1** virtual machine and click the **Console** tab. You will notice that the XenMobile Server is (**in First Time Use mode**).

Configure the following:

<table>
<tr><td>New Password:</td><td>Citrix123</td></tr>
<tr><td>Re-enter new password:</td><td>Citrix123</td></tr>
</table>



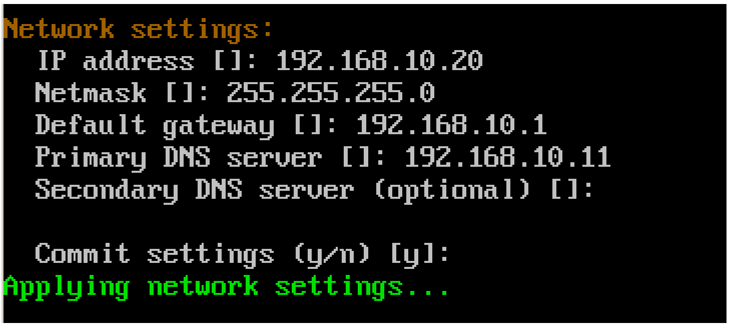
```
Starting configuration app...
  application started successfully                                    [ OK ]
Initializing main app...
  unpacking war file...                                               [ OK ]
Starting main app...
  not ready to start yet                                              [ OK ]
Starting first time use wizard...


                    **********************************
                    *       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:
```
</td></tr>
</table>

Step Action

5. Configure the following settings:

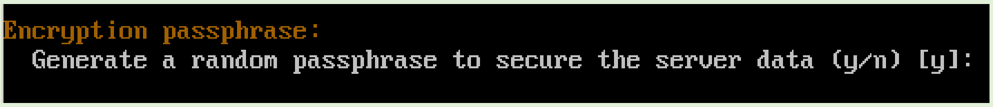
IP Address:	192.168.10.20
Netmask:	255.255.255.0
Default gateway:	192.168.10.1
Primary DNS server:	192.168.10.11
Secondary DNS server [optional]	**Leave blank and hit Enter**

Hit **Enter** to commit the settings.



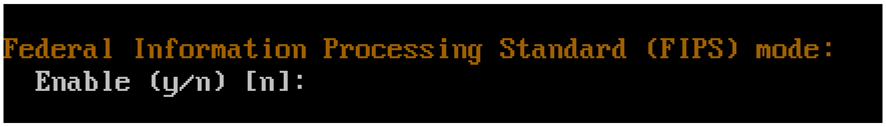
```
Network settings:
  IP address []: 192.168.10.20
  Netmask []: 255.255.255.0
  Default gateway []: 192.168.10.1
  Primary DNS server []: 192.168.10.11
  Secondary DNS server (optional) []:

  Commit settings (y/n) [y]:
Applying network settings...
```

6. The network settings are applied. Hit **Enter** to accept the default **[y]** to generate a random password to secure server data.



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

7. You are given the option to enable FIPS. Hit **Enter** to accept the default **[n]**.



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

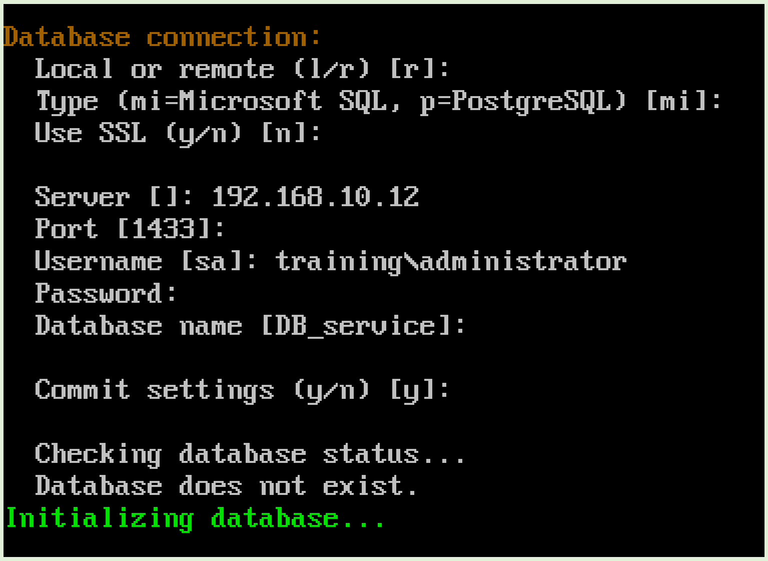
Step | Action

8. Next we will configure a remote database connection.

Configure the following settings:

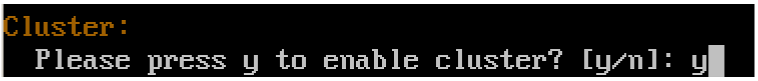
Local or remote [l/r]:	Hit **Enter** to accept the default **[r]**
Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]:	Hit **Enter** to accept the default **[mi]**
Use SSL:	Hit **Enter** to accept the default **[n]**
Server:	`192.168.10.12`
Port:	Hit **Enter** to accept the default **[1433]**
Username:	`training\administrator`
Password:	`Citrix123`
Database name:	Hit **Enter** to accept the default **[DB_service]**

Hit **Enter** to accept the default **y** to commit the settings**.**



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

  Server []: 192.168.10.12
  Port [1433]:
  Username [sa]: training\administrator
  Password:
  Database name [DB_service]:

  Commit settings (y/n) [y]:

  Checking database status...
  Database does not exist.
Initializing database...
```

9. You are prompted to enable clustering. Hit **Enter** to accept the default **[y]**.



```
Cluster:
  Please press y to enable cluster? [y/n]: y
```

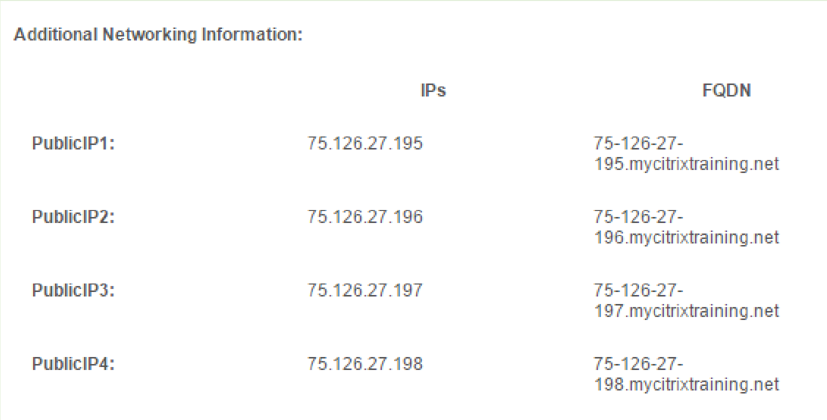
Step | Action

10. You are prompted for the XenMobile hostname.

Enter **<IP2 FQDN>** from your portal page and hit the **Enter** key**.**

Note: Your IP2 FQDN is available on the portal page.

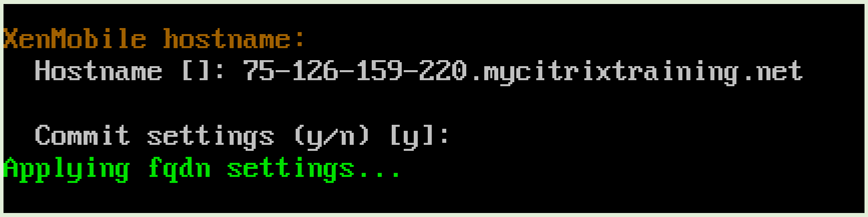
Example Only: 75-126-27-196.mycitrixtraining.net



Additional Networking Information:

	IPs	FQDN
PublicIP1:	75.126.27.195	75-126-27-195.mycitrixtraining.net
PublicIP2:	75.126.27.196	75-126-27-196.mycitrixtraining.net
PublicIP3:	75.126.27.197	75-126-27-197.mycitrixtraining.net
PublicIP4:	75.126.27.198	75-126-27-198.mycitrixtraining.net

Hit **Enter** to accept the default **[y]** to commit the settings.

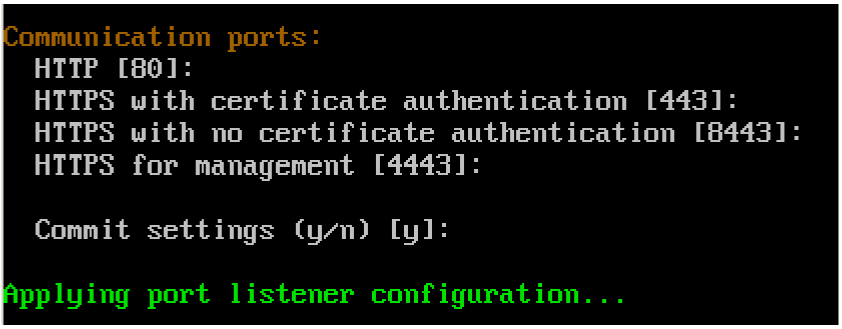


```
XenMobile hostname:
  Hostname []: 75-126-159-220.mycitrixtraining.net

  Commit settings (y/n) [y]:
Applying fqdn settings...
```

11. Configure the following communication ports (Port listeners):

HTTP:	Hit **Enter** to accept the default **[80]**
HTTPS with certificate authentication:	Hit **Enter** to accept the default **[443]**
HTTPS with no certificate authentication:	Hit **Enter** to accept the default **[8443]**
HTTPS for management:	Hit **Enter** to accept the default **[4443]**

Hit **Enter** to accept the default **[y]** to commit the settings.



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

  Commit settings (y/n) [y]:

Applying port listener configuration...
```

Step	Action

12. You are asked to use the same password for all certificates of the PKI.

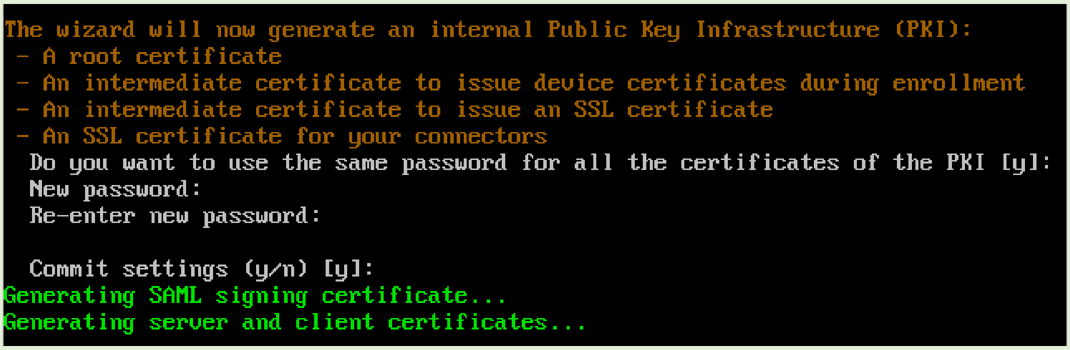
Hit **Enter** to accept the default **[y]**.

Configure the following:

New Password:	**Citrix123**
Re-enter new password:	**Citrix123**

Hit **Enter** to accept the default **[y]** to commit the settings.

Note: This configuration is for all the Public Key Infrastructure (PKI) certificates. This step creates the device manager's certificate authorities. If you intend to cluster XenMobile Server nodes, you will need to provide identical passwords for subsequent nodes.



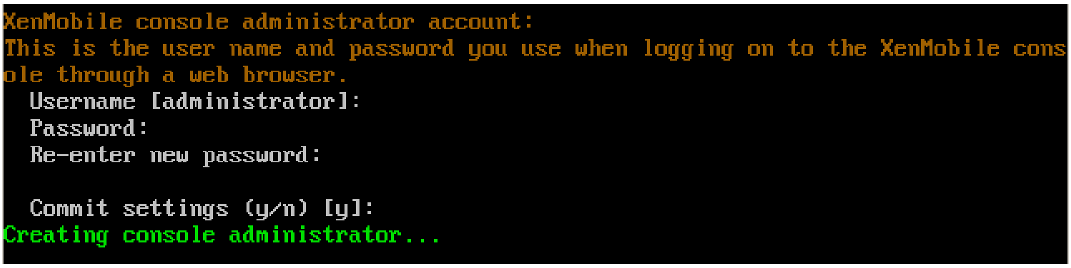
```
The wizard will now generate an internal Public Key Infrastructure (PKI):
 - A root certificate
 - An intermediate certificate to issue device certificates during enrollment
 - An intermediate certificate to issue an SSL certificate
 - An SSL certificate for your connectors
  Do you want to use the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

  Commit settings (y/n) [y]:
Generating SAML signing certificate...
Generating server and client certificates...
```

13. You are prompted to configure the XenMobile console administrator account.

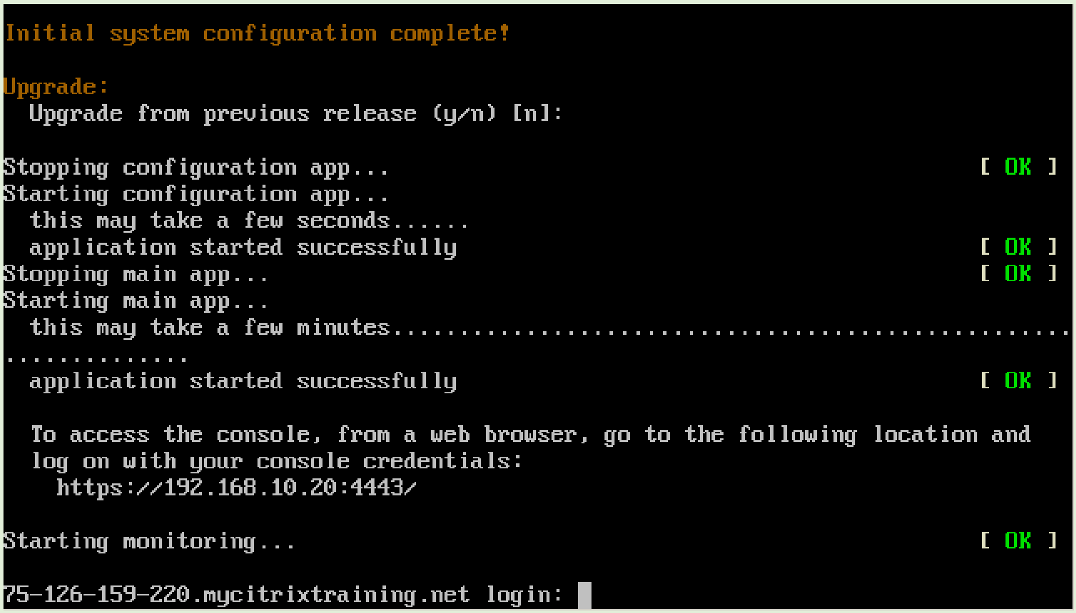
Configure the account as follows:

Username:	Hit **Enter** to accept the default **[administrator]**
Password:	**Citrix123**
Re-enter new password:	**Citrix123**

Hit **Enter** to accept the default **[y]** to commit the settings.



```
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]:
  Password:
  Re-enter new password:

  Commit settings (y/n) [y]:
Creating console administrator...
```

Step	Action
14.	You are asked if this is an upgrade from a previous release. Hit **Enter** to accept the default **[n].** The initial system configuration is complete. Make a note of the url given to complete the setup process. 

```
Initial system configuration complete!

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

Stopping configuration app...                                          [ OK ]
Starting configuration app...
  this may take a few seconds......
  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://192.168.10.20:4443/

Starting monitoring...                                                 [ OK ]

75-126-159-220.mycitrixtraining.net login: 
```

Exercise Summary

In this exercise, the student performed the initial configuration of the XenMobile Server. During the first time use, you configured the XenMobile Server networking information, FQDN, DNS Server, and connection to a remote SQL database.

Exercise 2

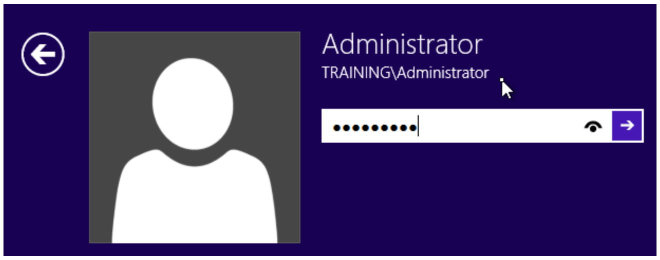
XenMobile Server Getting Started Wizard

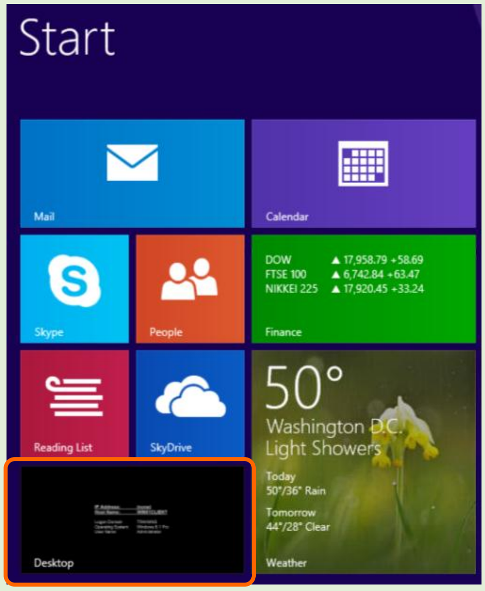
Overview

In this exercise we will go through the XenMobile Server **Getting Started** wizard, in order to configure categories, applications, policies, and delivery groups. The applications and policies will be assigned to the delivery groups.

Step by step guidance

Estimated time to complete this lab: **15** minutes.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1.</td><td>In XenCenter, select the <code>Site1-Win81Client</code> virtual machine and click the <code>Console</code> tab.
Login with the following credentials:
<table>
<tr><td>Username:</td><td><code>training\administrator</code></td></tr>
<tr><td>Password:</td><td><code>Citrix123</code></td></tr>
</table>


</td></tr>
<tr><td>2.</td><td>If needed, click on the <code>Desktop</code> tile.


</td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>3.</td><td>

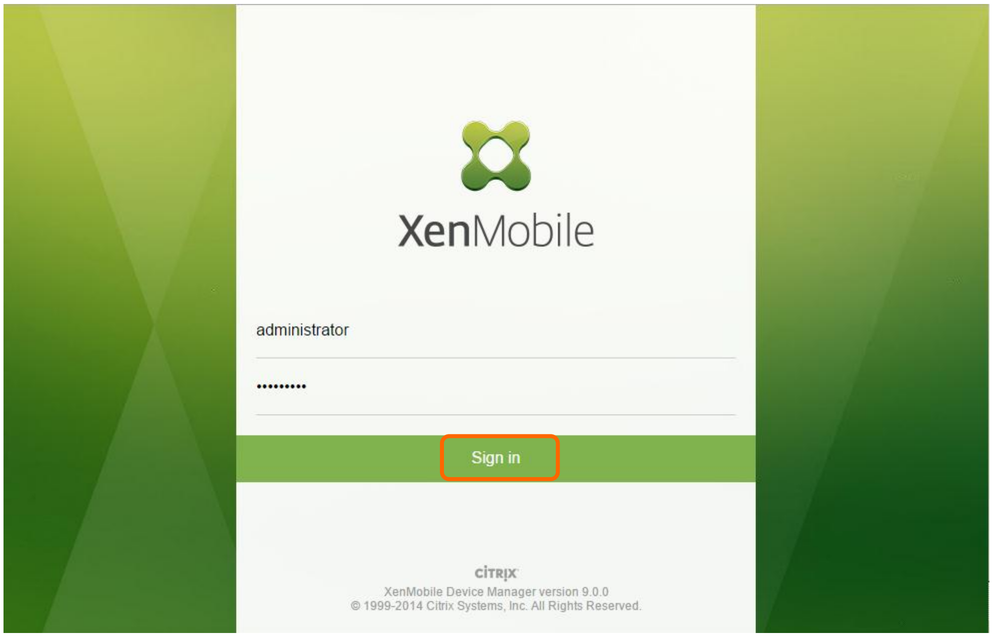
Launch Internet Explorer and browse to **https://192.168.10.20:4443**

Click **Continue to this website** to accept the certificate error.

Login with the following credentials:

<table>
<tr><td>Username</td><td><b>administrator</b></td></tr>
<tr><td>Password</td><td><b>Citrix123</b></td></tr>
</table>

Click **Sign in**.



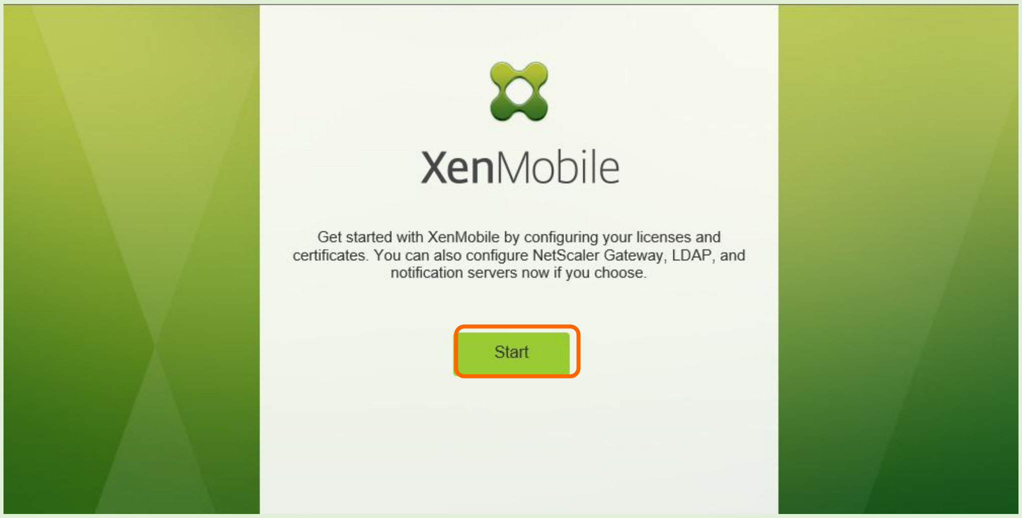
administrator

•••••••••

XenMobile Device Manager version 9.0.0
© 1999-2014 Citrix Systems, Inc. All Rights Reserved.

</td></tr>
<tr><td>4.</td><td>

The **Get Started** page is displayed. Click **Start** to begin the configuration wizard.



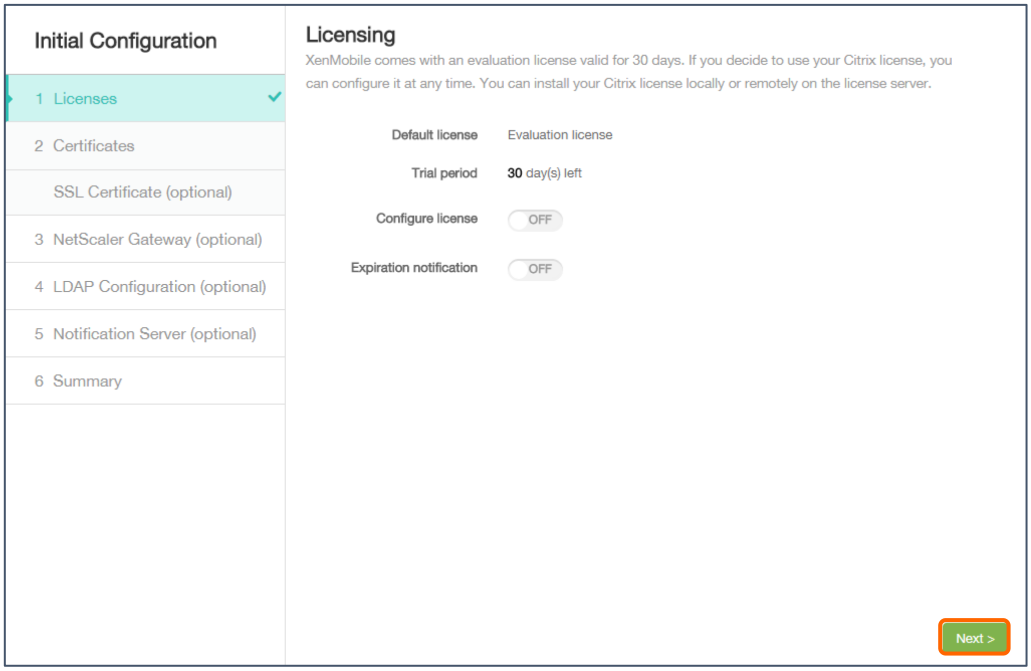
Get started with XenMobile by configuring your licenses and certificates. You can also configure NetScaler Gateway, LDAP, and notification servers now if you choose.

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>5.</td><td>

The Initial Configuration window is displayed.

Click **Next** to accept the use of the evaluation license.



Initial Configuration

1 Licenses ✓
2 Certificates
SSL Certificate (optional)
3 NetScaler Gateway (optional)
4 LDAP Configuration (optional)
5 Notification Server (optional)
6 Summary

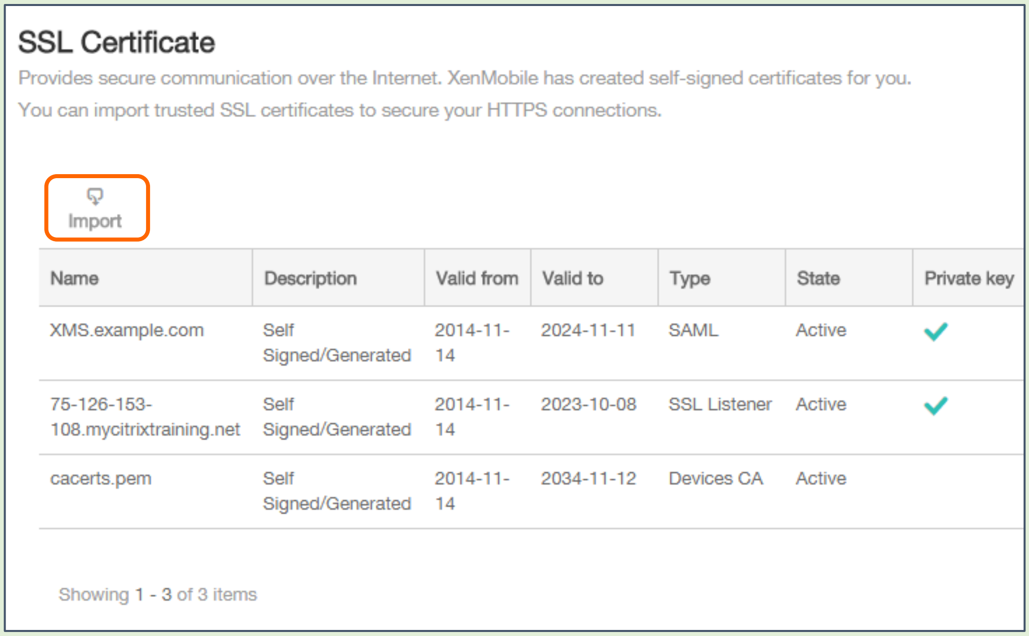
Licensing

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.

<table>
<tr><td>Default license</td><td>Evaluation license</td></tr>
<tr><td>Trial period</td><td>30 day(s) left</td></tr>
<tr><td>Configure license</td><td>OFF</td></tr>
<tr><td>Expiration notification</td><td>OFF</td></tr>
</table>

</td></tr>
<tr><td>6.</td><td>

On the **SSL Certificate** page, click **Import**.



SSL Certificate

Provides secure communication over the Internet. XenMobile has created self-signed certificates for you. You can import trusted SSL certificates to secure your HTTPS connections.

<table>
<tr><th>Name</th><th>Description</th><th>Valid from</th><th>Valid to</th><th>Type</th><th>State</th><th>Private key</th></tr>
<tr><td>XMS.example.com</td><td>Self Signed/Generated</td><td>2014-11-14</td><td>2024-11-11</td><td>SAML</td><td>Active</td><td>✓</td></tr>
<tr><td>75-126-153-108.mycitrixtraining.net</td><td>Self Signed/Generated</td><td>2014-11-14</td><td>2023-10-08</td><td>SSL Listener</td><td>Active</td><td>✓</td></tr>
<tr><td>cacerts.pem</td><td>Self Signed/Generated</td><td>2014-11-14</td><td>2034-11-12</td><td>Devices CA</td><td>Active</td><td></td></tr>
</table>

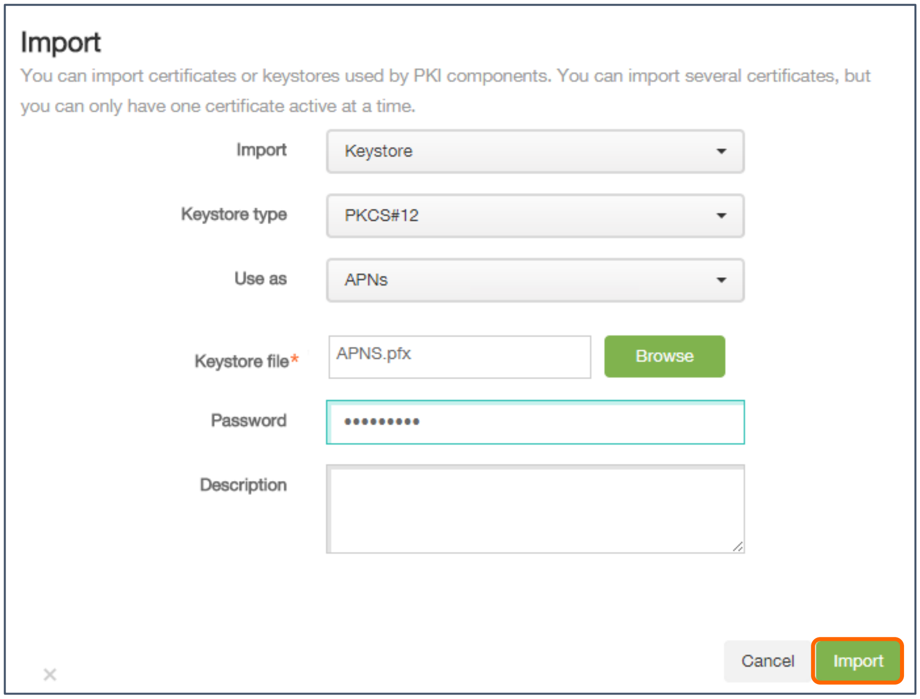
Showing 1 - 3 of 3 items

</td></tr>
</table>

Step	Action
7.	Configure the following settings:

Import	`Keystore`
Keystore type	`PKCS#12`
Use as	`APNs`
Keystore file	`APNS.pfx` (Browse to \\Ad\Software\Certificates)
Password	`Citrix123`

Click `Import`.



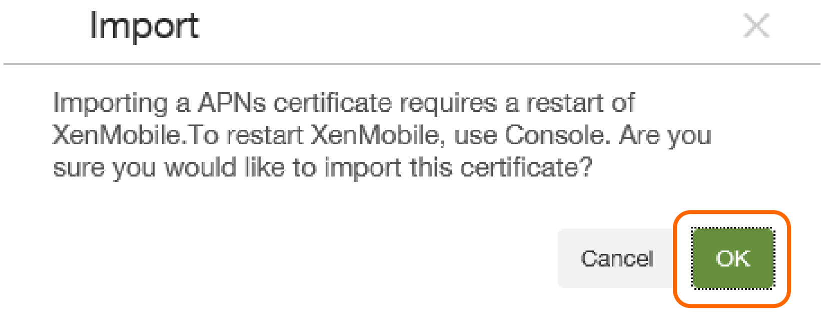
Import

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	APNs
Keystore file*	APNS.pfx
Password	•••••••••
Description	

A confirmation window pops up.

Click `OK`.



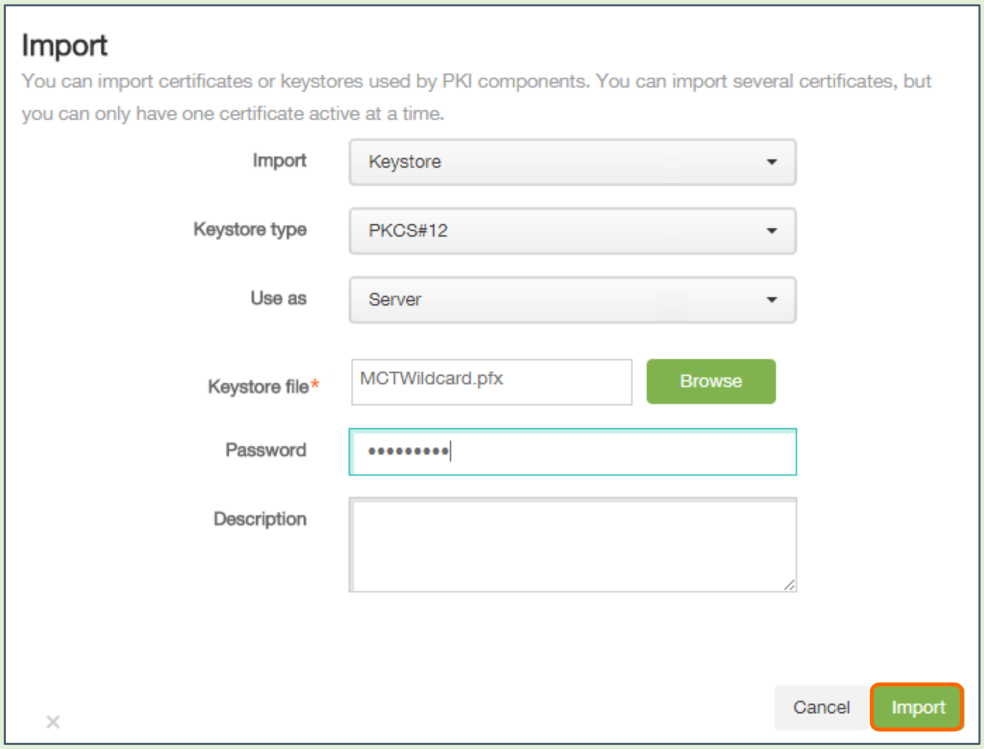
Import

Importing a APNs certificate requires a restart of XenMobile.To restart XenMobile, use Console. Are you sure you would like to import this certificate?

Step	Action
8.	Click **Import** again. Configure the following settings:

Import	**Keystore**
Keystore type	**PKCS#12**
Use as	**Server**
Keystore file	**MCTWildcard.pfx** (Browse to \\Ad\Software\Certificates)
Password	**Citrix123**

Click **Import**.



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*: MCTWildcard.pfx

Password: •••••••••

Description:

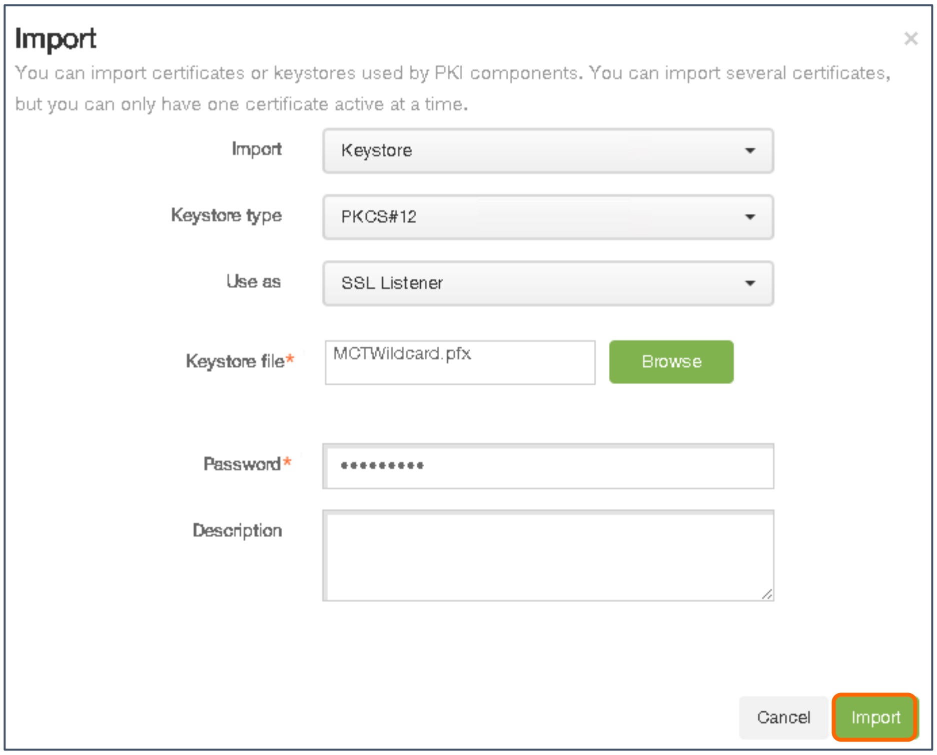
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>9.</td><td>

Click **Import** again.

Configure the following settings:

<table>
<tr><td>Import</td><td><b>Keystore</b></td></tr>
<tr><td>Keystore type</td><td><b>PKCS#12</b></td></tr>
<tr><td>Use as</td><td><b>SSL Listener</b></td></tr>
<tr><td>Keystore file</td><td><b>MCTWildcard.pfx</b> (Browse to \\Ad\Software\Certificates)</td></tr>
<tr><td>Password</td><td><b>Citrix123</b></td></tr>
</table>

Click **Import**.



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: SSL Listener

Keystore file*: MCTWildcard.pfx

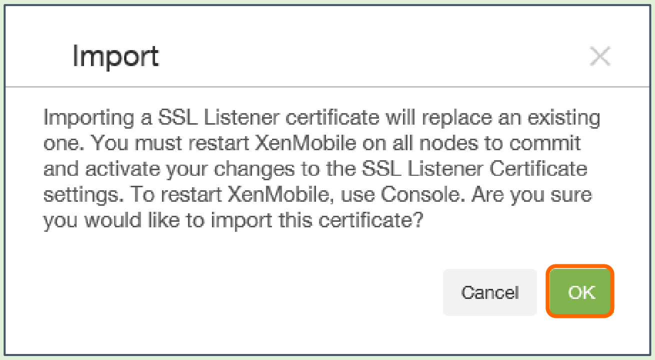
Password*: •••••••••

Description:

</td></tr>
<tr><td>10.</td><td>

You receive a prompt

Click **OK**.



Import

Importing a SSL Listener certificate will replace an existing one. You must restart XenMobile on all nodes to commit and activate your changes to the SSL Listener Certificate settings. To restart XenMobile, use Console. Are you sure you would like to import this certificate?

</td></tr>
</table>

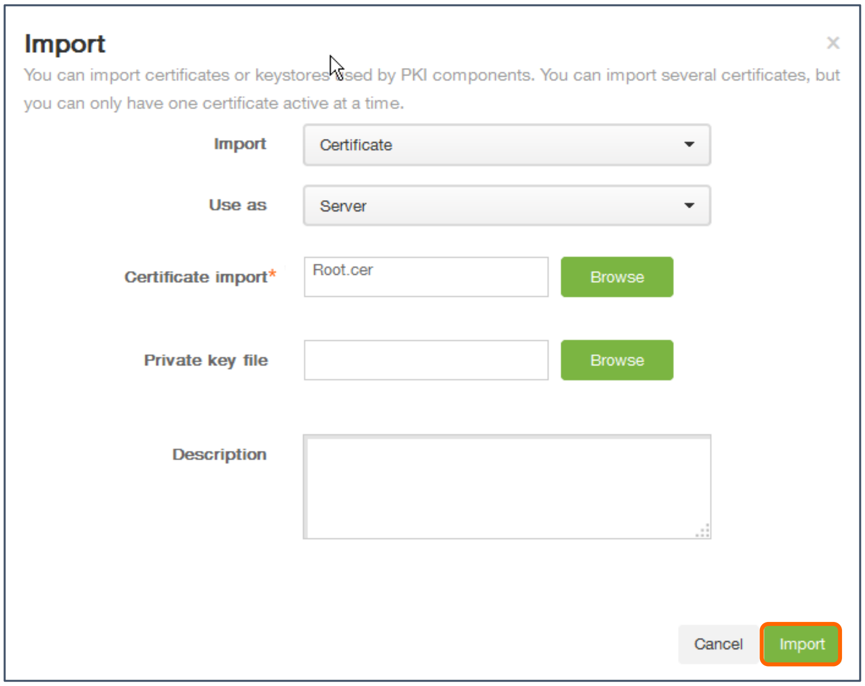
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>11.</td><td>

Click **Import** again.

Configure the following settings:

<table>
<tr><td>Import</td><td><b>Certificate</b></td></tr>
<tr><td>Use as</td><td><b>Server</b></td></tr>
<tr><td>Certificate import*</td><td><b>Root.cer</b> (Browse to \\Ad\Software\Certificates)</td></tr>
</table>

Click **Import**.



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

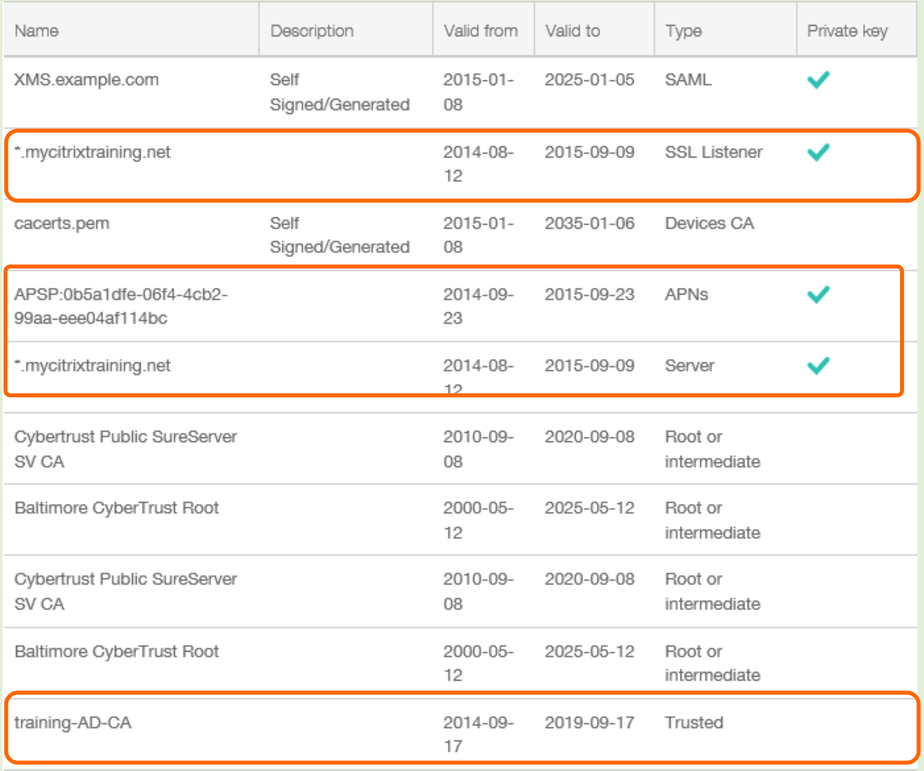
Use as: Server

Certificate import*: Root.cer

Private key file:

Description:

</td></tr>
</table>

Step	Action
12.	The **APNs**, **Server, Root and SSL Listener** certificates are displayed. Click **Next**. 

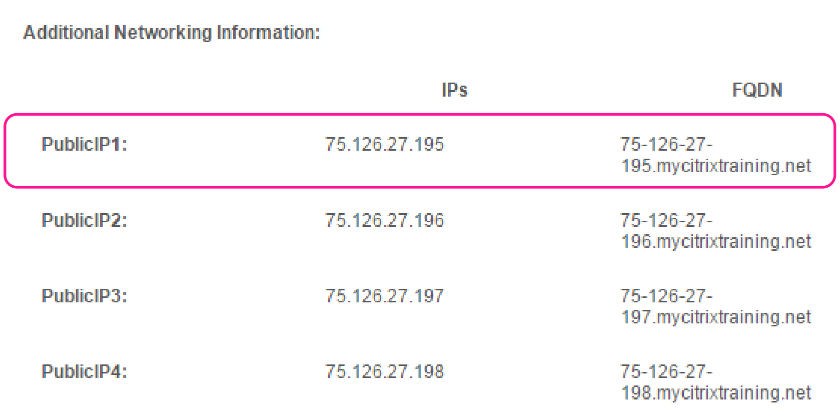
Name	Description	Valid from	Valid to	Type	Private key
XMS.example.com	Self Signed/Generated	2015-01-08	2025-01-05	SAML	✓
*.mycitrixtraining.net		2014-08-12	2015-09-09	SSL Listener	✓
cacerts.pem	Self Signed/Generated	2015-01-08	2035-01-06	Devices CA	
APSP:0b5a1dfe-06f4-4cb2-99aa-eee04af114bc		2014-09-23	2015-09-23	APNs	✓
*.mycitrixtraining.net		2014-08-12	2015-09-09	Server	✓
Cybertrust Public SureServer SV CA		2010-09-08	2020-09-08	Root or intermediate	
Baltimore CyberTrust Root		2000-05-12	2025-05-12	Root or intermediate	
Cybertrust Public SureServer SV CA		2010-09-08	2020-09-08	Root or intermediate	
Baltimore CyberTrust Root		2000-05-12	2025-05-12	Root or intermediate	
training-AD-CA		2014-09-17	2019-09-17	Trusted	

Step	Action
13.	Click **Next**. You are prompted to configure NetScaler Gateway.

Configure the following settings:

Name	**NSG**
Alias	Leave Blank
External URL	**https://<IP1 FQDN>**
Logon Type	**Domain only**
Password Required	**On**

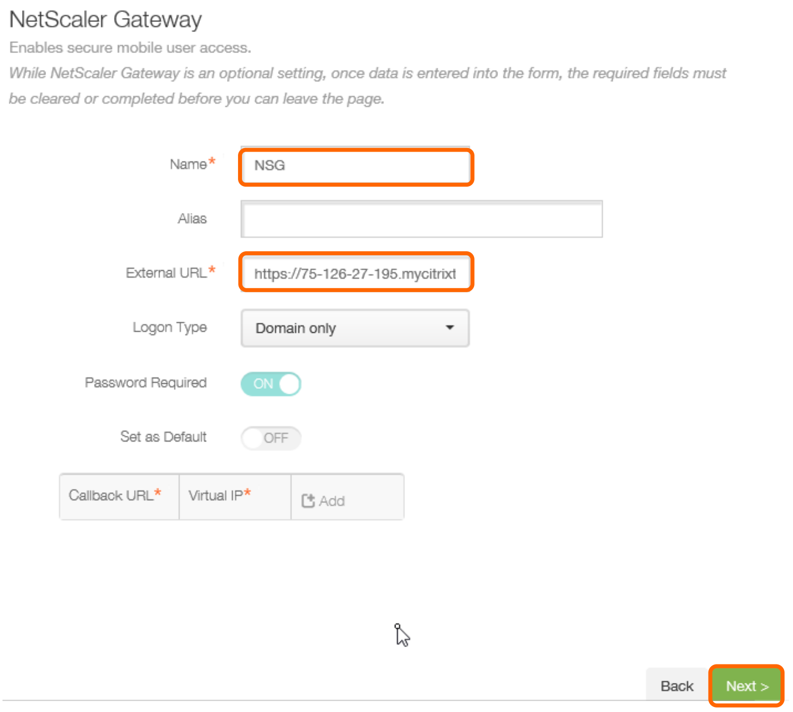
Note: Your IP1 FQDN is available on the portal page.
Example Only: 75-126-27-195.mycitrixtraining.net



Additional Networking Information:

	IPs	FQDN
PublicIP1:	75.126.27.195	75-126-27-195.mycitrixtraining.net
PublicIP2:	75.126.27.196	75-126-27-196.mycitrixtraining.net
PublicIP3:	75.126.27.197	75-126-27-197.mycitrixtraining.net
PublicIP4:	75.126.27.198	75-126-27-198.mycitrixtraining.net

Click **Next.**



NetScaler Gateway

Enables secure mobile user access.

While NetScaler Gateway is an optional setting, once data is entered into the form, the required fields must be cleared or completed before you can leave the page.

Name* NSG

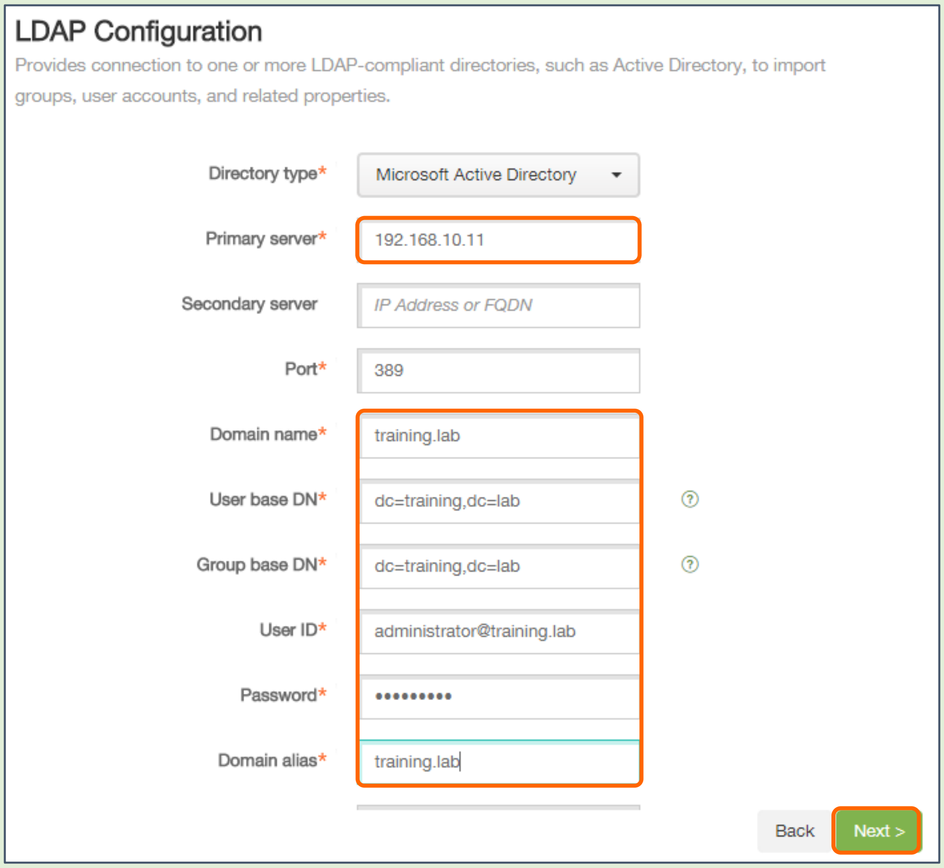
Alias

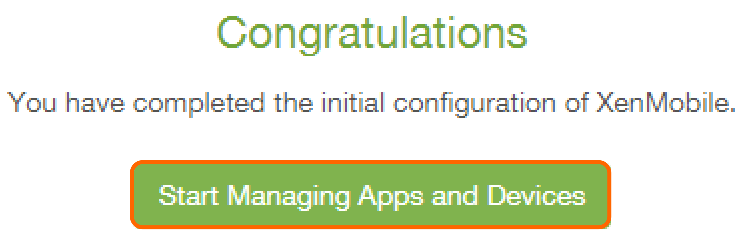
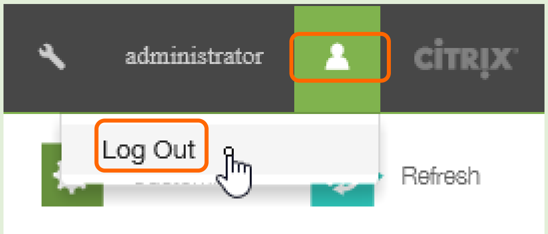
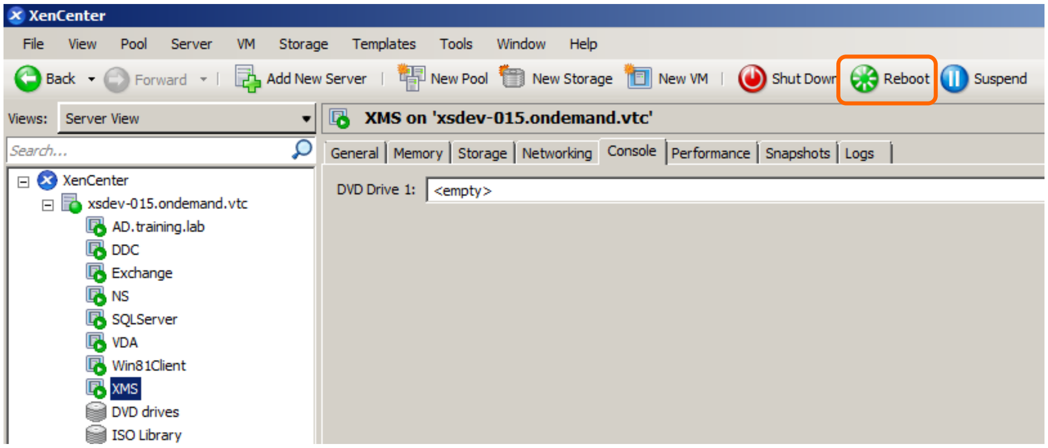
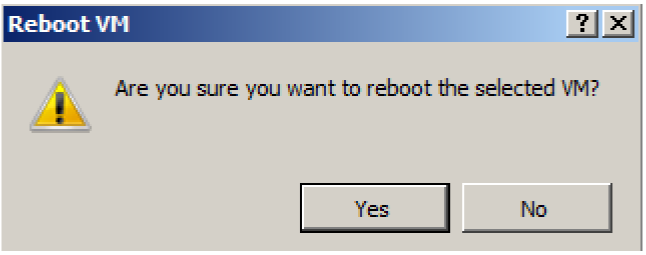
External URL* https://75-126-27-195.mycitrixt

Logon Type Domain only

Password Required ON

Set as Default OFF

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>14.</td><td>The LDAP Configuration page is displayed.
Configure the following settings:
<table>
<tr><td>Primary Server</td><td>192.168.10.11</td></tr>
<tr><td>Port</td><td>389 (Default)</td></tr>
<tr><td>Domain name</td><td>training.lab</td></tr>
<tr><td>User base DN</td><td>dc=training,dc=lab <b>(auto-filled in)</b></td></tr>
<tr><td>Group base DN</td><td>dc=training,dc=lab <b>(auto-filled in)</b></td></tr>
<tr><td>User ID:</td><td>administrator@training.lab</td></tr>
<tr><td>Password</td><td>Citrix123</td></tr>
<tr><td>Domain alias</td><td>training.lab</td></tr>
<tr><td>Use search by</td><td>sAMAccountName</td></tr>
</table>
Click <b>Next</b>.

LDAP Configuration
Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.
Directory type* Microsoft Active Directory
Primary server* 192.168.10.11
Secondary server IP Address or FQDN
Port* 389
Domain name* training.lab
User base DN* dc=training,dc=lab
Group base DN* dc=training,dc=lab
User ID* administrator@training.lab
Password* •••••••••
Domain alias* training.lab
 </td></tr>
<tr><td>15.</td><td>Click <b>Next</b> to skip the <b>Notification Server</b> configuration.</td></tr>
<tr><td>16.</td><td>Click <b>Finish</b> on the <b>Summary</b> page.</td></tr>
</table>

Step	Action
17.	The initial configuration is complete. Click **Start Managing Apps and Devices**.  Congratulations You have completed the initial configuration of XenMobile. Start Managing Apps and Devices
18.	Select the user icon and click **Log Out**. 
19.	In XenCenter, select the **SITE1-XMS1** virtual machine. Click **Reboot** to reboot the server.  XenCenter File View Pool Server VM Storage Templates Tools Window Help Back Forward Add New Server New Pool New Storage New VM Shut Down Reboot Suspend Views: Server View Search... General Memory Storage Networking Console Performance Snapshots Logs XenCenter xsdev-015.ondemand.vtc AD.training.lab DDC Exchange NS SQLServer VDA Win81Client XMS DVD drives ISO Library XMS on 'xsdev-015.ondemand.vtc' DVD Drive 1: <empty> Click **Yes** on the popup window to reboot the vm.  Reboot VM Are you sure you want to reboot the selected VM? Yes No
20.	Wait until the XMS server is back up before continuing with the next exercise.

Exercise Summary

The Getting Started wizard takes you through configuring licensing, certificates, NetScaler Gateway & LDAP settings for the XenMobile Server.

Exercise 3

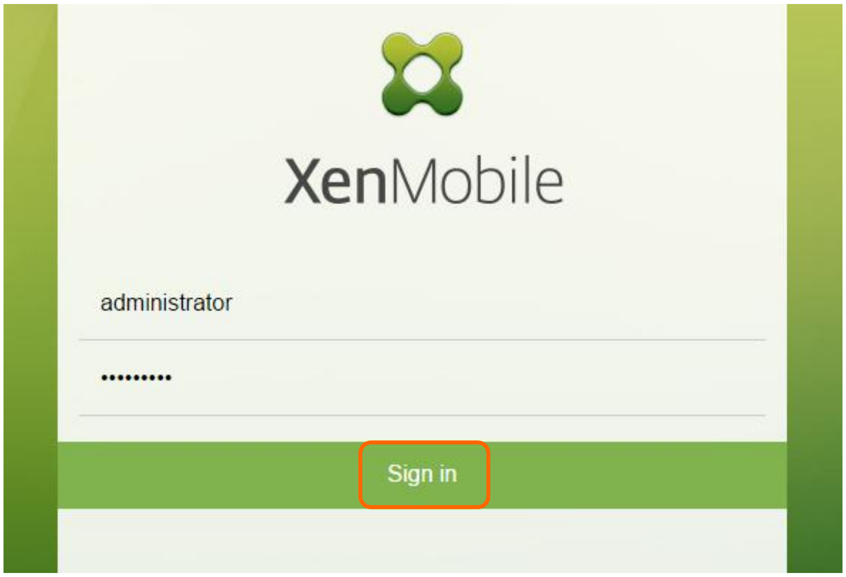
Configure Policies on XenMobile Titan Server

Overview

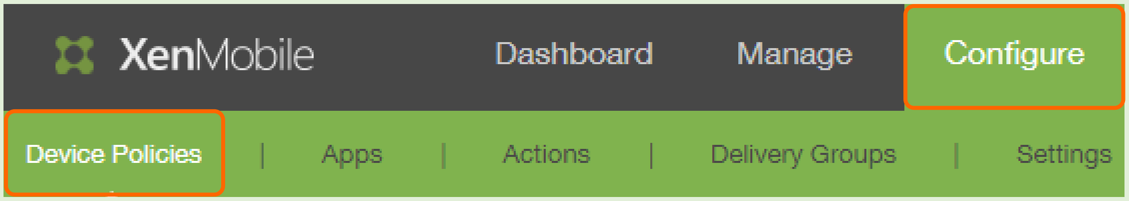
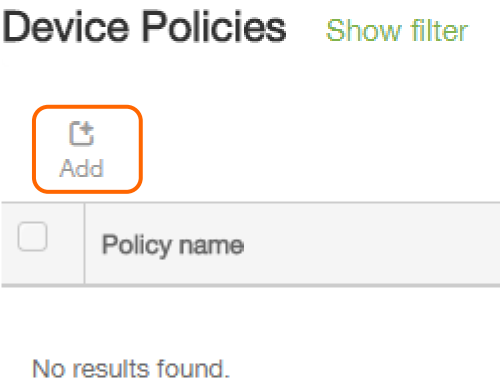
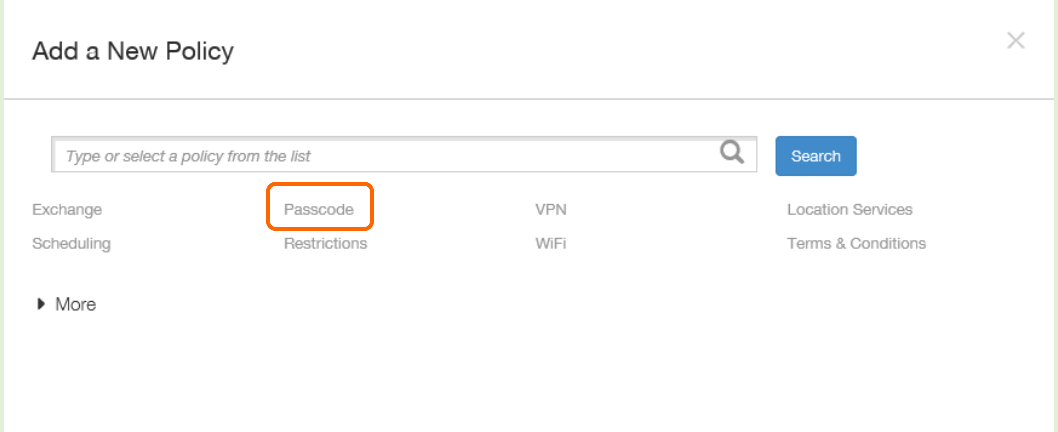
XenMobile Server empowers enterprise organizations to apply device configurations, settings, and security parameters to multiple devices. In this exercise, students will configure policies on XenMobile Server to push to iOS or Android mobile devices.

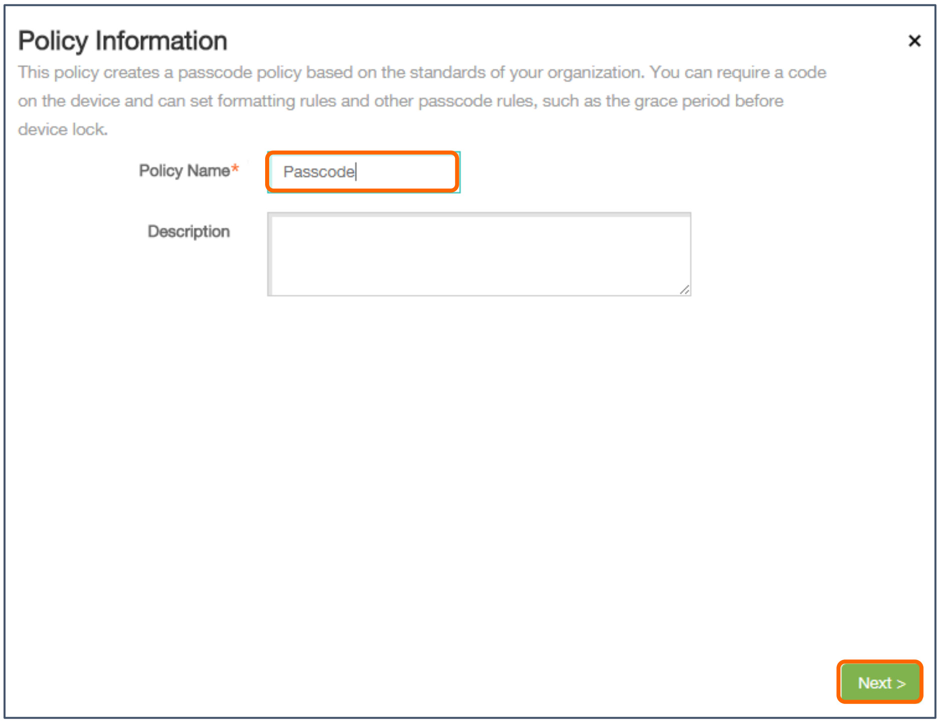
Step by step guidance

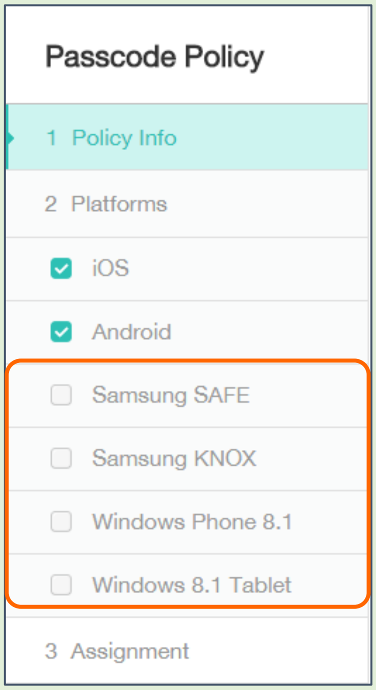
Estimated time to complete this lab: **15** minutes.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1.</td><td>Select the <code>Site1-Win81Client</code> virtual machine.
If the vm screen is locked, login with the following credentials:<table><tr><td>Username:</td><td><code>training\administrator</code></td></tr><tr><td>Password:</td><td><code>Citrix123</code></td></tr></table></td></tr>
<tr><td>2.</td><td>Open a browser and navigate to https://192.168.10.20:4443.</td></tr>
<tr><td>3.</td><td>Login with the following credentials<table><tr><td>Username:</td><td><code>administrator</code></td></tr><tr><td>Password:</td><td><code>Citrix123</code></td></tr></table>Click <code>Sign in</code>.


administrator
•••••••••
 </td></tr>
</table>

Step	Action
4.	In the XenMobile Server management console, select the **Configure** tab and click the **Device Policies** node on the green ribbon.  XenMobile Dashboard Manage Configure Device Policies | Apps | Actions | Delivery Groups | Settings
5.	On the **Device Policies** window, click **Add**.  No results found.
6.	Click **Passcode**  Add a New Policy Type or select a policy from the list Search Exchange Passcode VPN Location Services Scheduling Restrictions WiFi Terms & Conditions More

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>7.</td><td>The Policy Information page is displayed. Configure the following:
<table><tr><td>Policy name</td><td>Passcode</td></tr></table>
Click Next.

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.
Policy Name* Passcode
Description

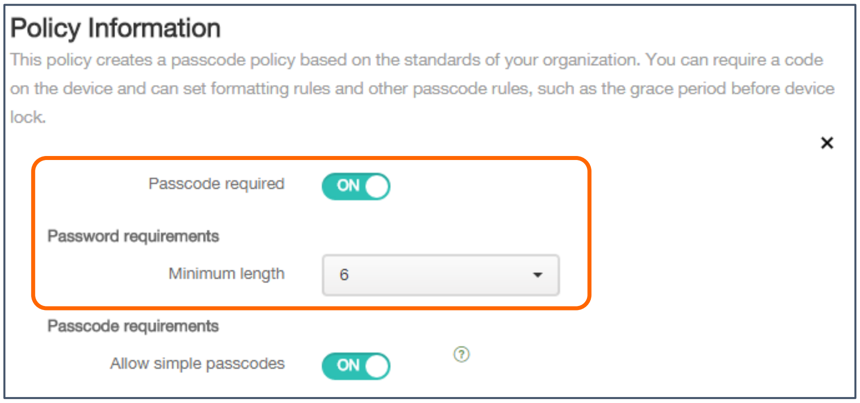
</td></tr>
<tr><td>8.</td><td>Click the checkbox next to the <b>Samsung Safe</b>, <b>Samsung KNOX</b>, <b>Windows Phone 8.1</b>, and <b>Windows 8.1 Tablet</b>, and platforms. These platforms will be disabled.

Passcode Policy
1 Policy Info
2 Platforms
☑ iOS
☑ Android
☐ Samsung SAFE
☐ Samsung KNOX
☐ Windows Phone 8.1
☐ Windows 8.1 Tablet
3 Assignment
</td></tr>
</table>

Step	Action
9.	The **Policy Information** window is displayed for **iOS** devices.

Configure the following settings:

Passcode required	**On**
Minimum length	**6**
Maximum failed sign-on attempts	**4**

Click **Next**.



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.

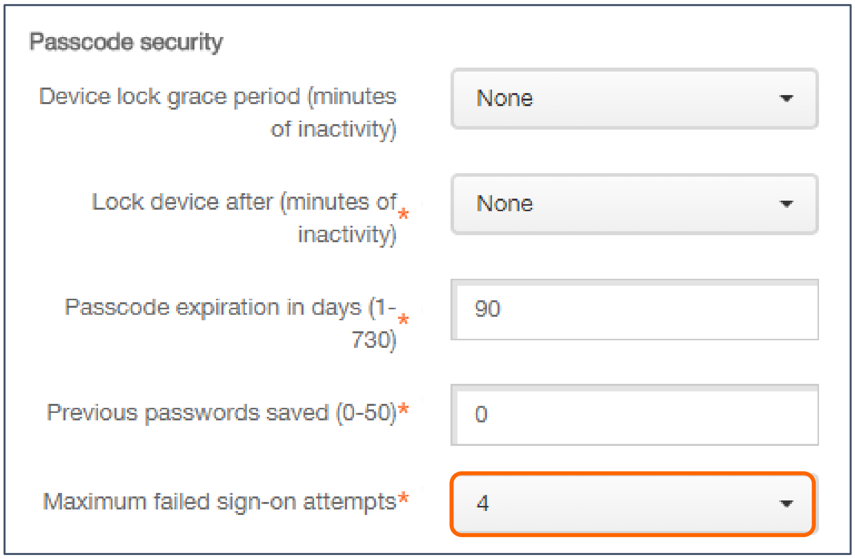
Passcode required: ON

Password requirements

Minimum length: 6

Passcode requirements

Allow simple passcodes: ON



Passcode security

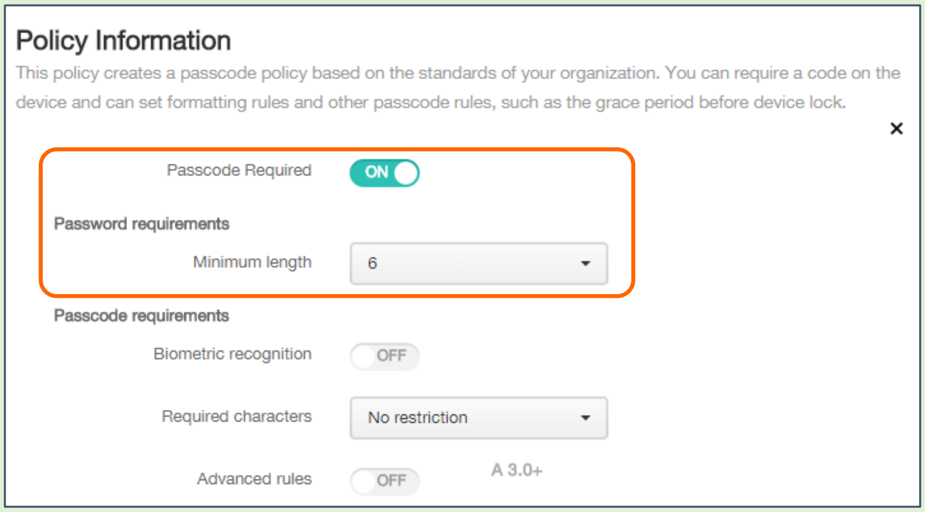
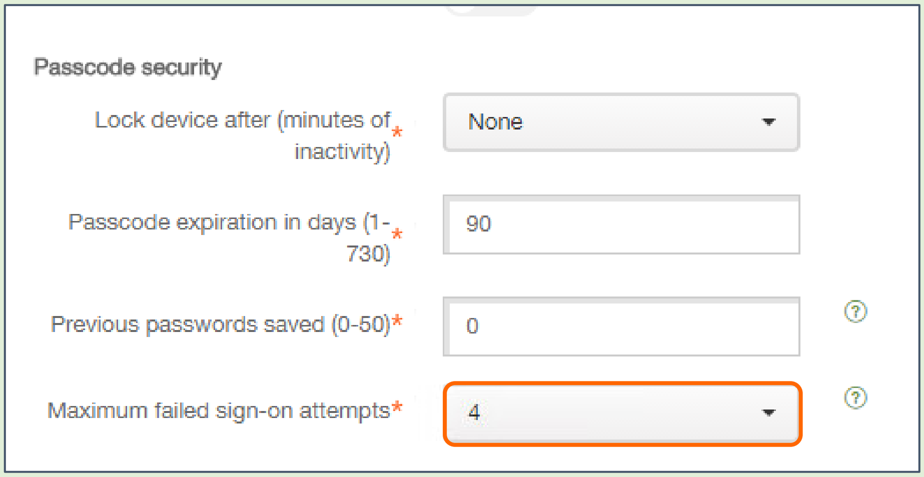
Device lock grace period (minutes of inactivity): None

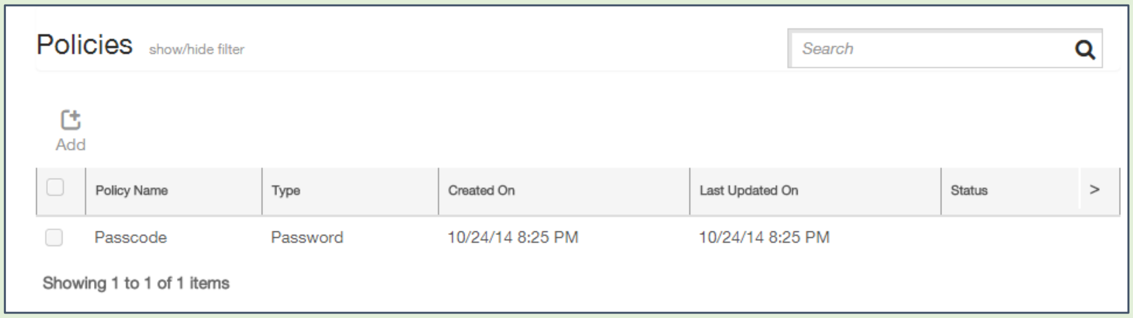
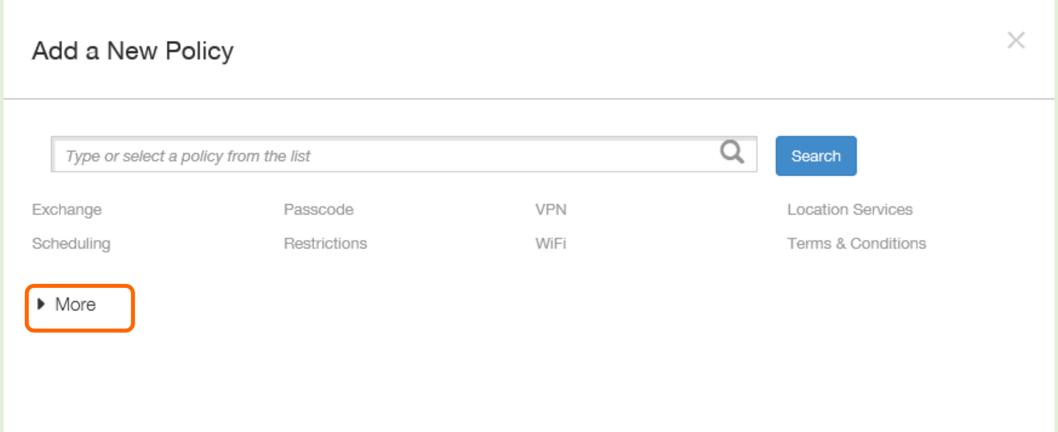
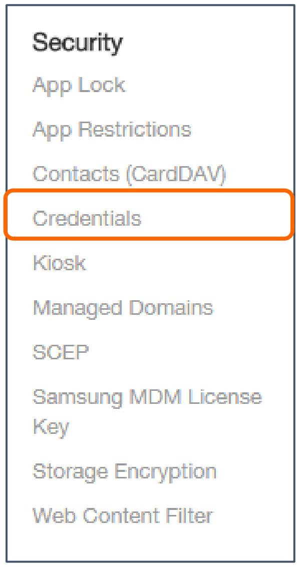
Lock device after (minutes of inactivity)*: None

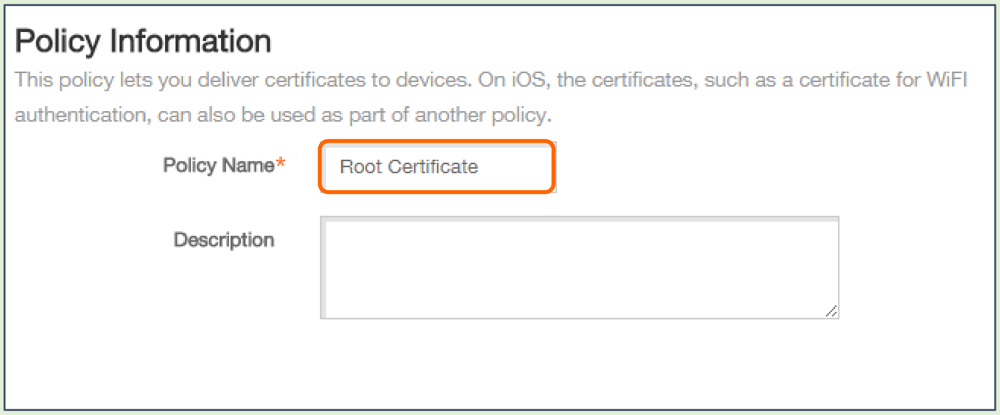
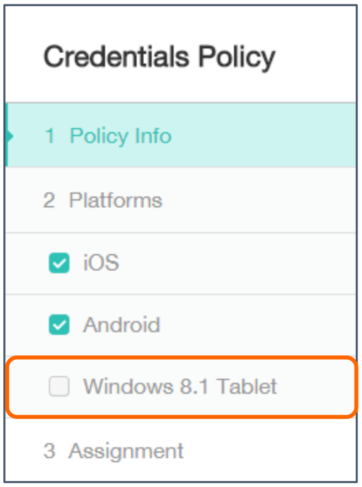
Passcode expiration in days (1-730)*: 90

Previous passwords saved (0-50)*: 0

Maximum failed sign-on attempts*: 4

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>10.</td><td>The **Policy Information** window is displayed for **Android** devices.
Configure the following settings:
<table>
<tr><td>Passcode required</td><td>On</td></tr>
<tr><td>Minimum length</td><td>6</td></tr>
<tr><td>Maximum failed sign-on attempts</td><td>4</td></tr>
</table>
Click Next

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
Password requirements
Minimum length: 6
Passcode requirements
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)*: 90
Previous passwords saved (0-50)*: 0
Maximum failed sign-on attempts*: 4
</td></tr>
<tr><td>11.</td><td>Apply policy to **AllUsers** and click Save.</td></tr>
</table>

Step	Action
12.	The **Passcode** policy is displayed.  Policies show/hide filter Search Add □ Policy Name · Type · Created On · Last Updated On · Status □ Passcode · Password · 10/24/14 8:25 PM · 10/24/14 8:25 PM Showing 1 to 1 of 1 items
13.	Click **Add** again.
14.	The **Add a New Policy** window is displayed. Click **More**.  Add a New Policy Type or select a policy from the list Search Exchange · Passcode · VPN · Location Services Scheduling · Restrictions · WiFi · Terms & Conditions More
15.	Under the **Security** column, select **Credentials**.  Security App Lock App Restrictions Contacts (CardDAV) Credentials Kiosk Managed Domains SCEP Samsung MDM License Key Storage Encryption Web Content Filter

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>16.</td><td>The Credentials Policy configuration is displayed.
Configure the following:<table><tr><td>Policy Name*</td><td>Root Certificate</td></tr></table>
Policy Information
This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFI authentication, can also be used as part of another policy.
Policy Name* Root Certificate
Description</td></tr>
<tr><td>17.</td><td>On the left side of the Window, deselect the <b>Windows 8.1 Tablet</b> platform.
Click <b>Next</b>.
Credentials Policy
1 Policy Info
2 Platforms
☑ iOS
☑ Android
□ Windows 8.1 Tablet
3 Assignment</td></tr>
</table>

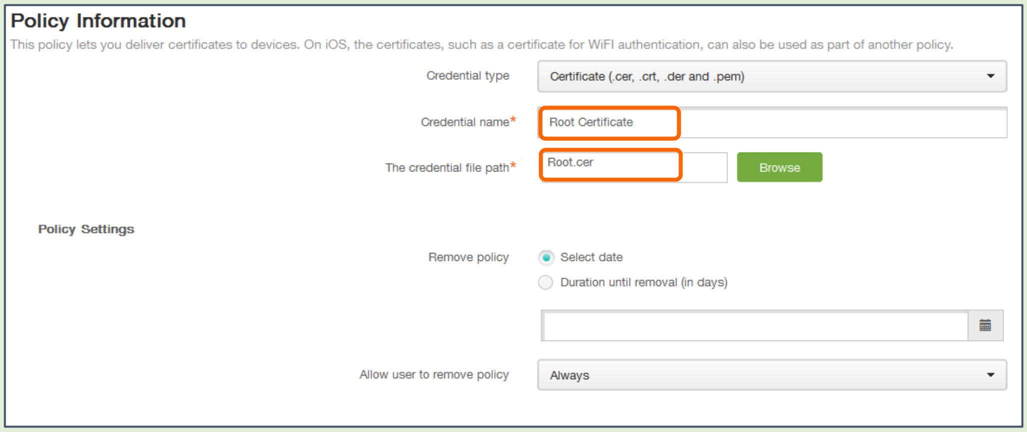
Step | Action

18. The **Policy Information** window for **iOS** devices is displayed.

Configure the following settings:

Credential Name*	`Root Certificate`
The credential file path*	`Root.cer` (Click browse and navigate to **\\AD\Software\Certificates**)

Click **`Next`**.



Policy Information

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFI authentication, can also be used as part of another policy.

Credential type: Certificate (.cer, .crt, .der and .pem)

Credential name*: Root Certificate

The credential file path*: Root.cer

Policy Settings

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

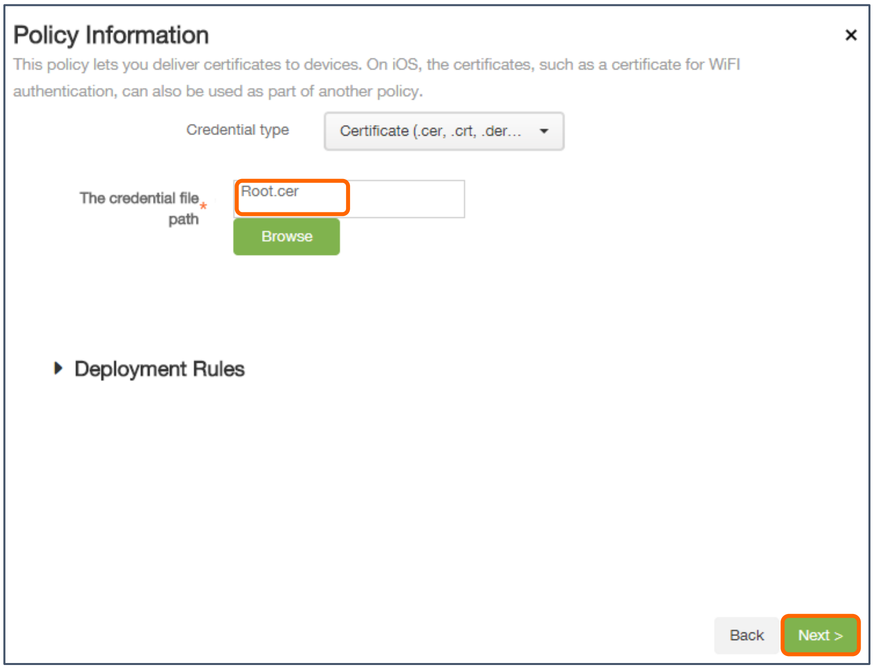
Allow user to remove policy: Always

19. The **Policy Information** window for **Android** devices is displayed.

Configure the following settings:

Credential File Path:	`Root.cer` **(**Click browse and navigate to **\\AD\Software\Certificates)**

Click **`Next`**.

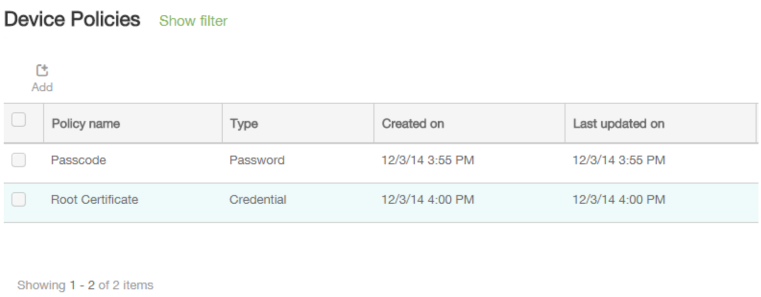
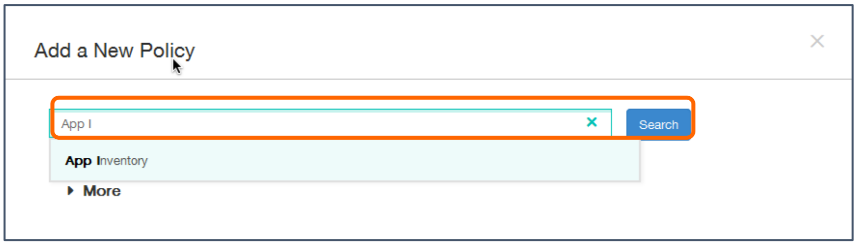
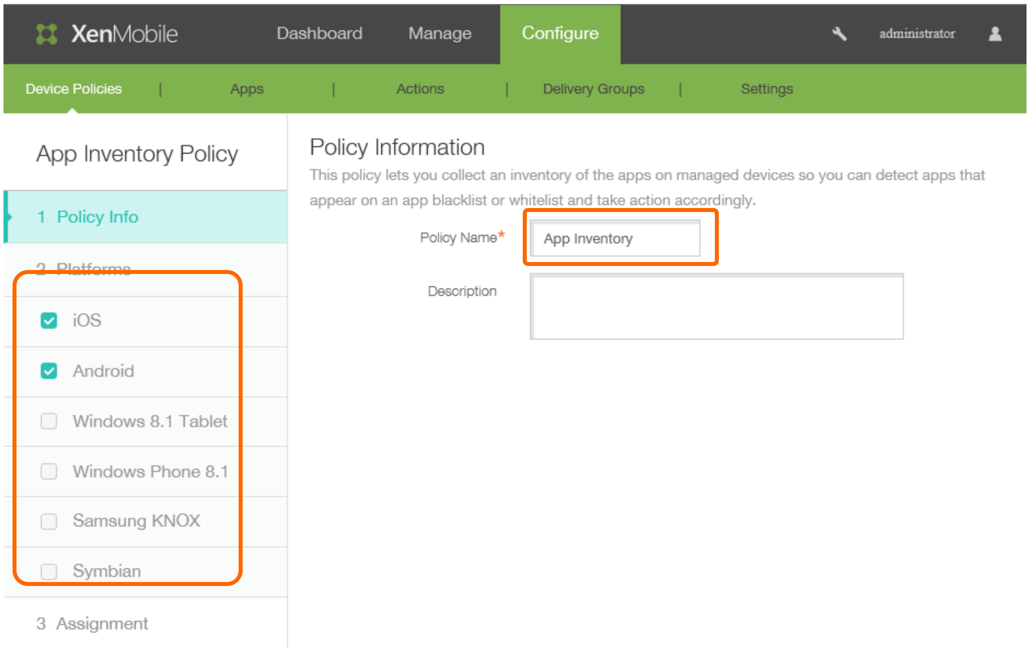


Policy Information

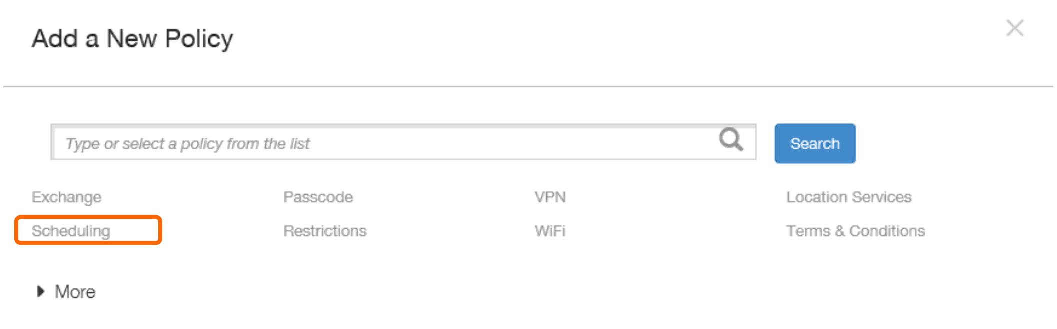
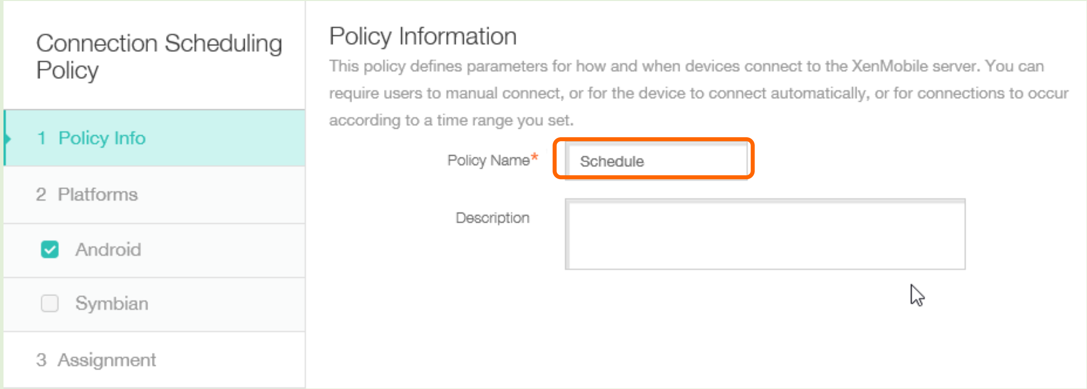
This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFI authentication, can also be used as part of another policy.

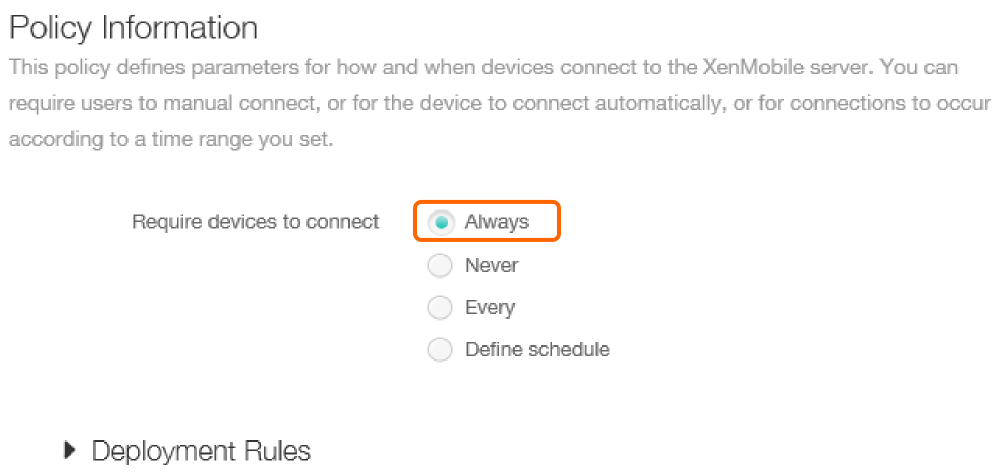
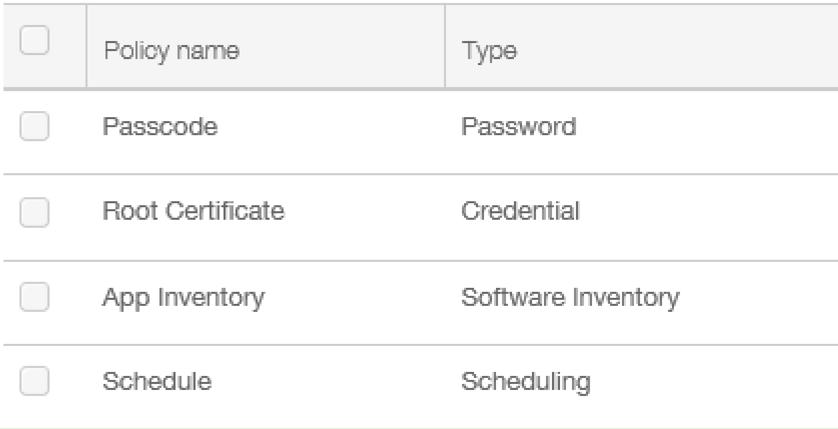
Credential type: Certificate (.cer, .crt, .der…

The credential file path*: Root.cer

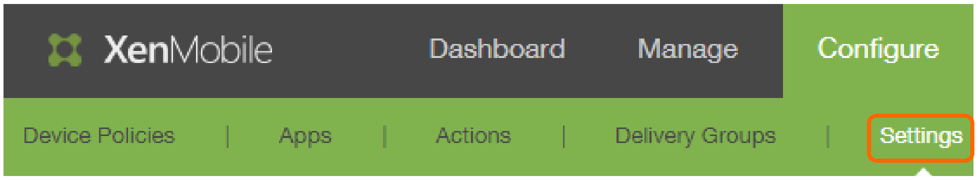
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>20.</td><td>Apply policy to <b>AllUsers</b> and click <code>Save</code>.</td></tr>
<tr><td>21.</td><td>The <b>Root Certificate</b> policy is displayed.

Device Policies Show filter
Add
<table>
<tr><th>□</th><th>Policy name</th><th>Type</th><th>Created on</th><th>Last updated on</th></tr>
<tr><td>□</td><td>Passcode</td><td>Password</td><td>12/3/14 3:55 PM</td><td>12/3/14 3:55 PM</td></tr>
<tr><td>□</td><td>Root Certificate</td><td>Credential</td><td>12/3/14 4:00 PM</td><td>12/3/14 4:00 PM</td></tr>
</table>
Showing 1 - 2 of 2 items</td></tr>
<tr><td>22.</td><td>Click <code>Add</code> again.</td></tr>
<tr><td>23.</td><td>The <b>Add a New Policy</b> window is displayed. Type <code>App Inventory</code> in the search bar and click the <code>Search</code> button. Click <code>More</code>

Add a New Policy
App I ✕ Search
App Inventory
▸ More
Choose <b>App Inventory.</b>
Enter <b>App Inventory i</b>n the policy name and uncheck all but <b>iOS</b> and <b>Android</b> in the platform section. The Policy will be enabled by default for <b>iOS</b> and <b>Android</b>.

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

App Inventory Policy
1 Policy Info
2 Platforms
☑ iOS
☑ Android
□ Windows 8.1 Tablet
□ Windows Phone 8.1
□ Samsung KNOX
□ Symbian
3 Assignment
Policy Information
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.
Policy Name* App Inventory
Description</td></tr>
</table>

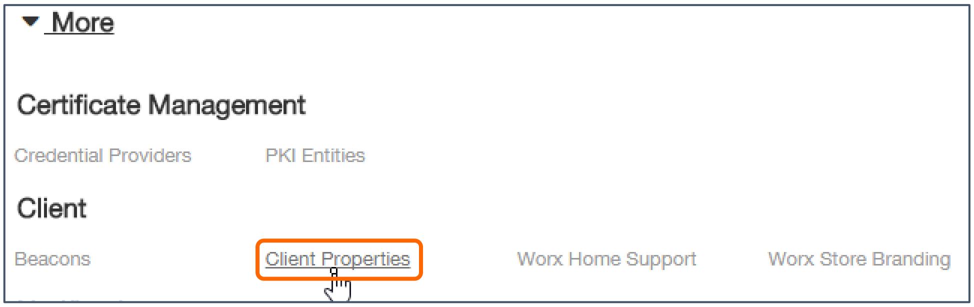
Step	Action
24.	Click **`Next`** three times and assign the policy to the **AllUsers** delivery group. Click **`Save`**
25.	The last policy we're going to setup is to assure Android devices are getting policy updates and new apps without user interaction. On iOS this is being accomplished by APNS, for Android devices we'll setup a scheduler (Interval or always connected). Click **`Add`** again. The **Add a New Policy** window is displayed. Select **`Scheduling`** and enable only the Android platform to keep connected to the XenMobile Server.  Add a New Policy Type or select a policy from the list Search Exchange Passcode VPN Location Services Scheduling Restrictions WiFi Terms & Conditions More
26.	Enter **`Schedule`** as the policy name. Disable the **Symbian** platform and click **`Next`**.  Connection Scheduling Policy 1 Policy Info 2 Platforms ☑ Android □ Symbian 3 Assignment Policy Information This policy defines parameters for how and when devices connect to the XenMobile server. You can require users to manual connect, or for the device to connect automatically, or for connections to occur according to a time range you set. Policy Name* Schedule Description

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>27.</td><td>Accept the default option <code>Always</code> to permanently keep the device connected.

Policy Information
This policy defines parameters for how and when devices connect to the XenMobile server. You can require users to manual connect, or for the device to connect automatically, or for connections to occur according to a time range you set.
Require devices to connect ● Always
○ Never
○ Every
○ Define schedule
▸ Deployment Rules
Click <code>Next</code> and assign the policy to the <b>AllUsers</b> delivery group.</td></tr>
<tr><td>28.</td><td>You should have the following policies defined by now.

<table>
<tr><th>□</th><th>Policy name</th><th>Type</th></tr>
<tr><td>□</td><td>Passcode</td><td>Password</td></tr>
<tr><td>□</td><td>Root Certificate</td><td>Credential</td></tr>
<tr><td>□</td><td>App Inventory</td><td>Software Inventory</td></tr>
<tr><td>□</td><td>Schedule</td><td>Scheduling</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>29.</td><td>
Click the <b>Settings</b> tab on the green ribbon.

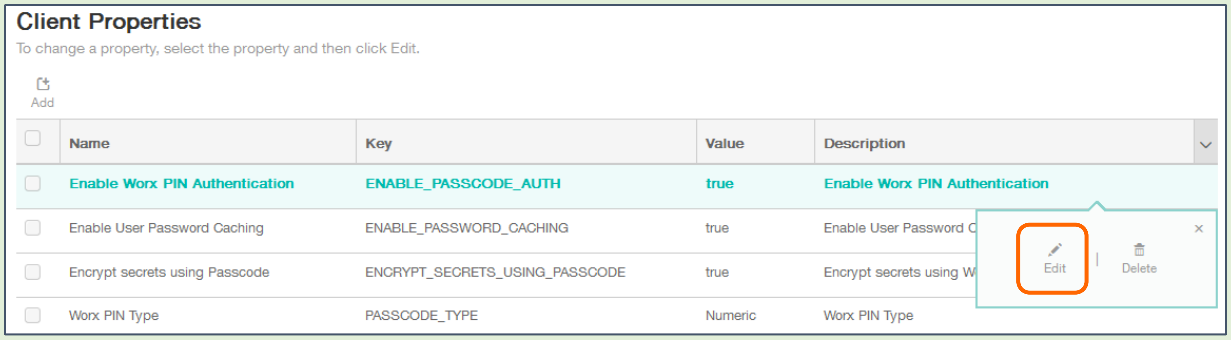


Navigate to <b>More&gt; Client> Client Properties</b>



</td></tr>
<tr><td>30.</td><td>
The <b>Client Properties</b> are displayed.

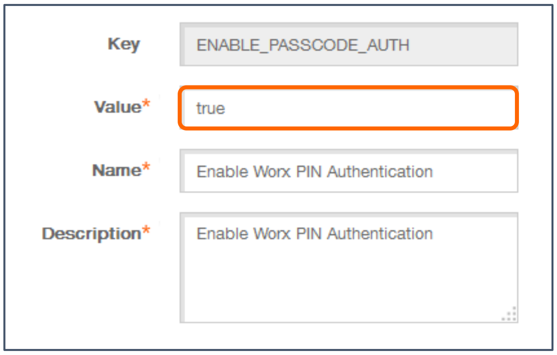
Click <b>Enable Worx PIN Authentication</b> then click <b>Edit</b>.



Client Properties

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

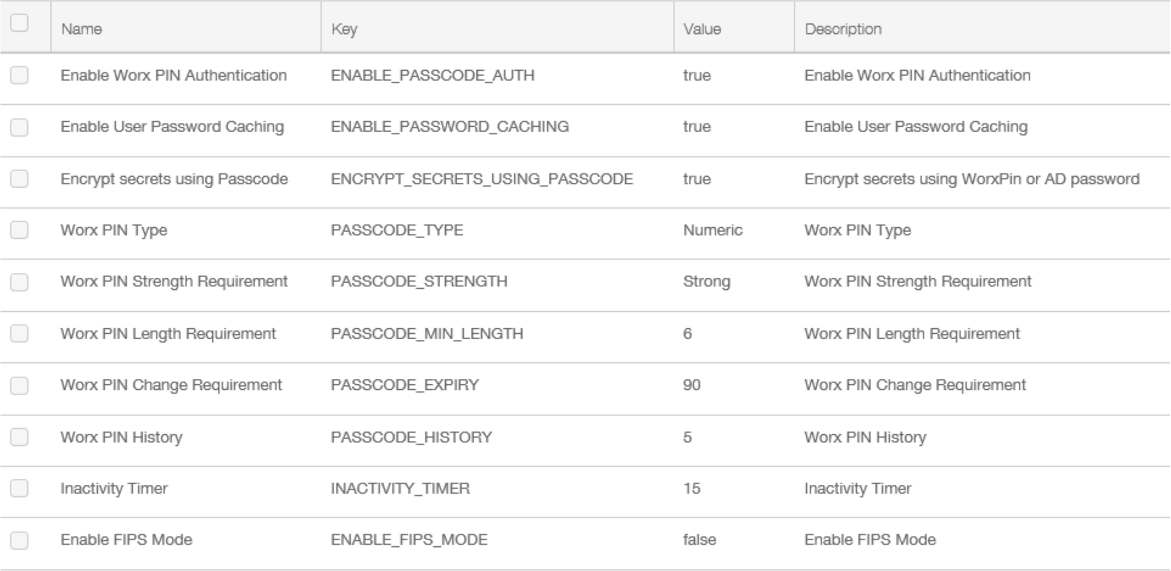
<table>
<tr><th>□</th><th>Name</th><th>Key</th><th>Value</th><th>Description</th></tr>
<tr><td>□</td><td>Enable Worx PIN Authentication</td><td>ENABLE_PASSCODE_AUTH</td><td>true</td><td>Enable Worx PIN Authentication</td></tr>
<tr><td>□</td><td>Enable User Password Caching</td><td>ENABLE_PASSWORD_CACHING</td><td>true</td><td>Enable User Password C</td></tr>
<tr><td>□</td><td>Encrypt secrets using Passcode</td><td>ENCRYPT_SECRETS_USING_PASSCODE</td><td>true</td><td>Encrypt secrets using W</td></tr>
<tr><td>□</td><td>Worx PIN Type</td><td>PASSCODE_TYPE</td><td>Numeric</td><td>Worx PIN Type</td></tr>
</table>
</td></tr>
<tr><td>31.</td><td>
Change the <b>Value</b> parameter to <b>true</b> and click <b>Save</b>.



Key: ENABLE_PASSCODE_AUTH
Value*: true
Name*: Enable Worx PIN Authentication
Description*: Enable Worx PIN Authentication
</td></tr>
<tr><td>32.</td><td>
Configure the remaining <b>Client Properties</b> the with the following settings:

<table>
<tr><td>Enable User Password Caching</td><td>true</td></tr>
<tr><td>Encrypt secrets using Passcode</td><td>true</td></tr>
<tr><td>Worx Pin Strength Requirement</td><td>Strong</td></tr>
</table>
</td></tr>
</table>

Step	Action
33.	After all the changes your **Client Properties** should look like this:



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

Exercise Summary

You have now configured a certificate policy for both iOS and Android devices and enabled WorxPin. The certificate is necessary to enable trust between WorxMail and Exchange. Now you are ready to create add categories and applications to XenMobile Server.

Exercise 4

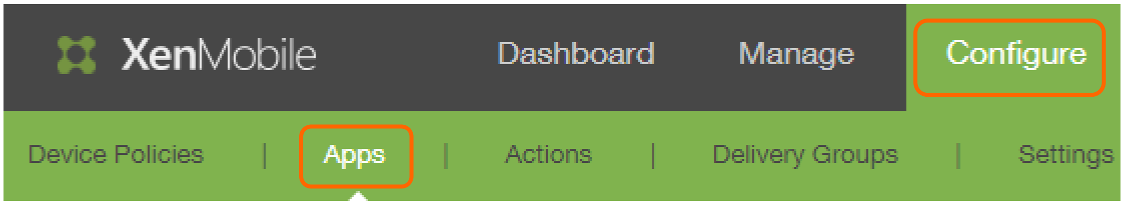
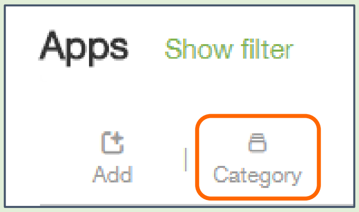
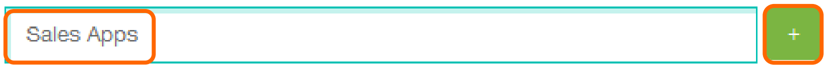
Adding Categories and Applications to XenMobile Server

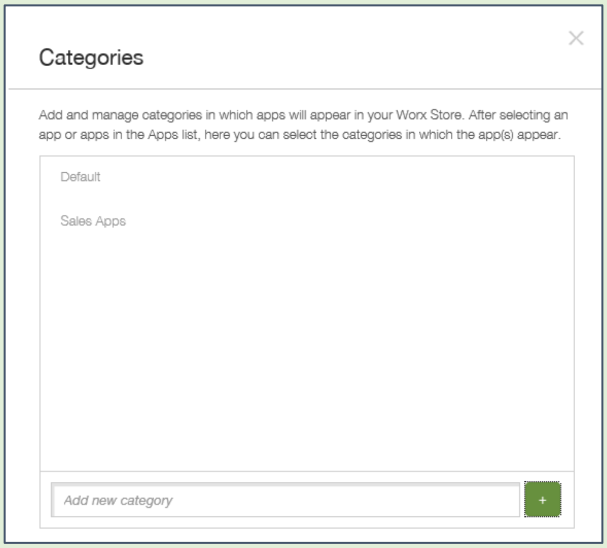
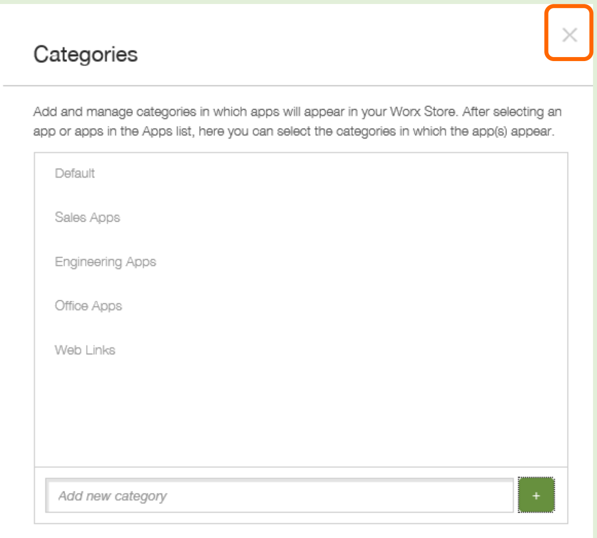
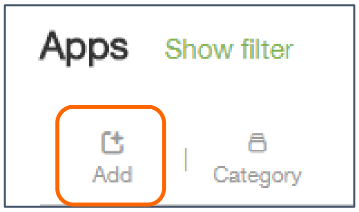
Overview

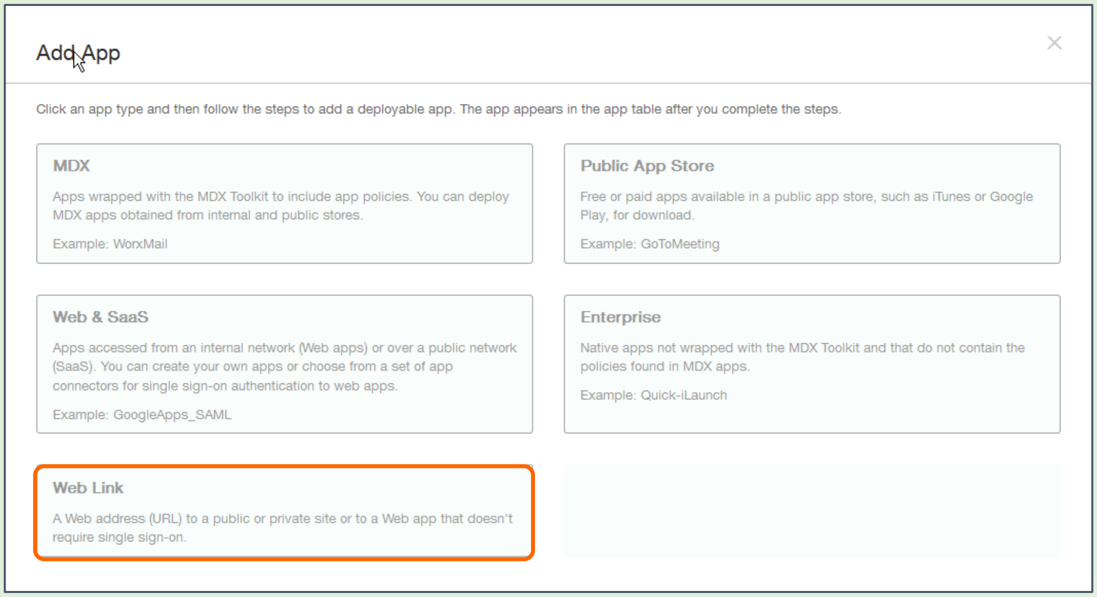
In this exercise students will create **Categories** within the XenMobile Server. Students will then add mobile, web, and SaaS applications and assign them to the appropriate category.

Step by step guidance

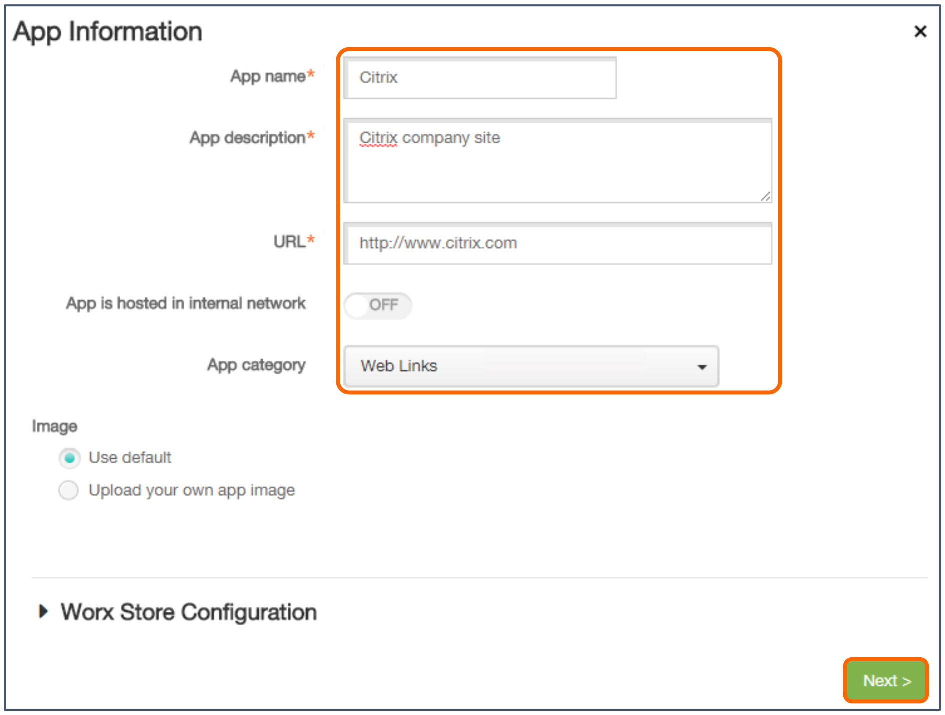
Estimated time to complete this lab: **22** minutes.

Step	Action
1.	On the green ribbon, click on the `Apps` tab.  XenMobile Dashboard Manage Configure Device Policies Apps Actions Delivery Groups Settings
2.	Click `Category`. 
3.	The **Categories** Window pops up. In the **Add new category** text box, enter `Sales Apps` and click the plus sign in the green box.  Sales Apps

Step	Action
4.	The **Sales Apps** category is added.  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 Sales Apps
5.	Repeat **Steps 2-3** to add the following categories: **`Engineering Apps`, `Office Apps`, and `Web Links`.**
6.	The categories have been added. Click the **`X`** on the top right corner to close the window.  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 Sales Apps Engineering Apps Office Apps Web Links
7.	Click **`Add`**. 

Step	Action
8.	In the **Add App** window, click the **`Web Link`** app type.  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.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>9.</td><td>The <b>Add Web App</b> window is displayed. Configure the following settings:
<table>
<tr><td>App Name</td><td>Citrix</td></tr>
<tr><td>App description</td><td>Citrix Company site</td></tr>
<tr><td>URL</td><td>http://www.citrix.com</td></tr>
<tr><td>App is hosted in internal network</td><td>Off</td></tr>
<tr><td>App Category</td><td>Web Links</td></tr>
</table>
Click Next.



App Information

App name* Citrix

App description* Citrix company site

URL* http://www.citrix.com

App is hosted in internal network OFF

App category Web Links

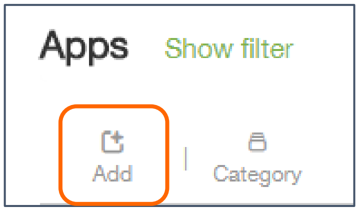
Image

● Use default

○ Upload your own app image

Worx Store Configuration

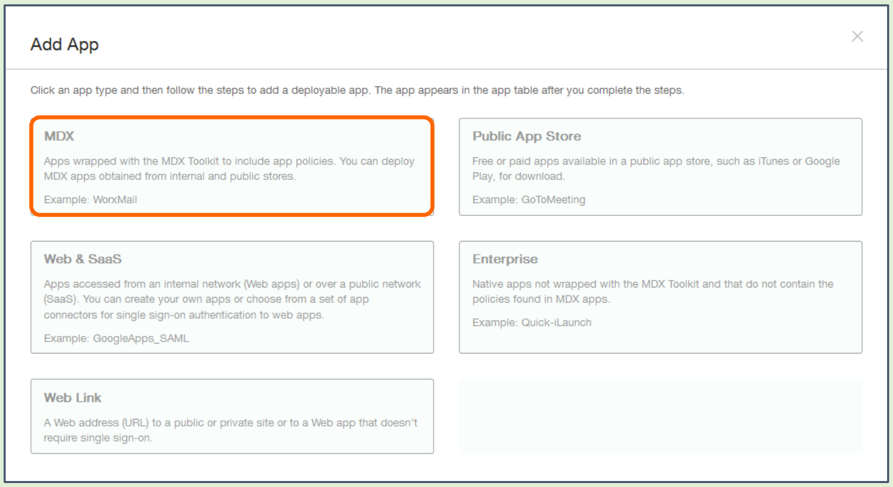
</td></tr>
<tr><td>10.</td><td>Assign to <b>AllUsers</b> and click Save<b>.</b></td></tr>
<tr><td>11.</td><td>Click Add again.



</td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>12.</td><td>

This time select **MDX**.



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

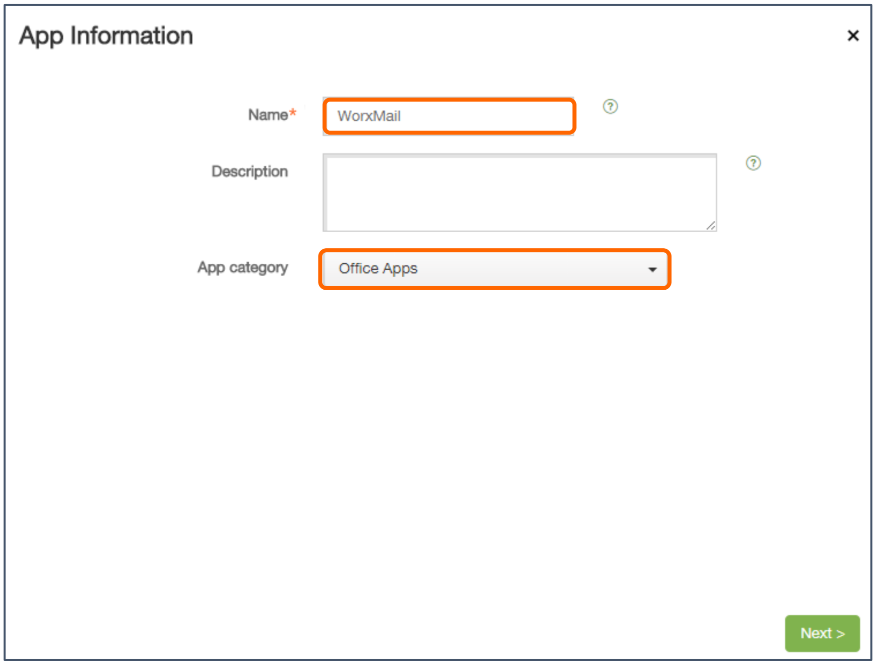
Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

</td></tr>
<tr><td>13.</td><td>

Configure the application as follows:

<table>
<tr><td>Name*</td><td>WorxMail</td></tr>
<tr><td>App category</td><td>Office Apps</td></tr>
</table>



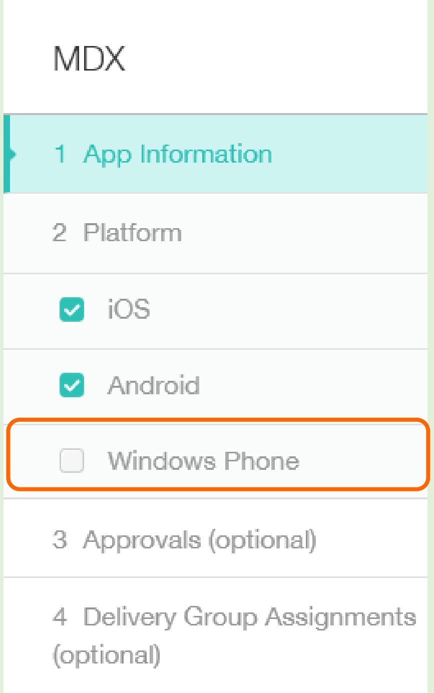
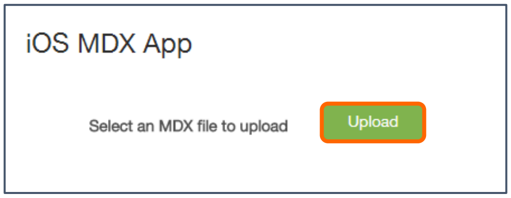
App Information

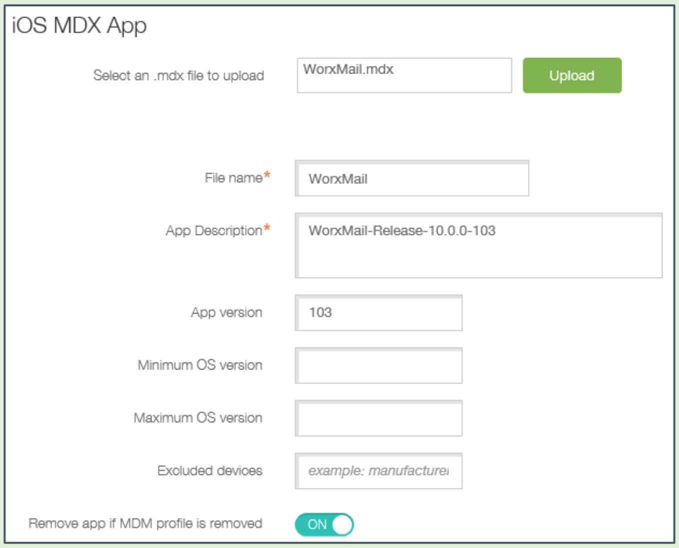
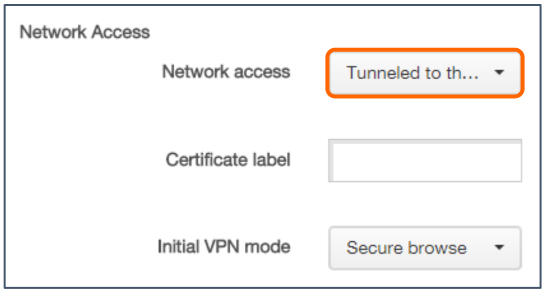
Name* WorxMail

Description

App category Office Apps

</td></tr>
</table>

Step	Action
14.	Deselect the **Windows Phone** platform options on the left. Click **Next**.  MDX 1 App Information 2 Platform ☑ iOS ☑ Android □ Windows Phone 3 Approvals (optional) 4 Delivery Group Assignments (optional)
15.	In the **iOS MDX App** window, click **Upload**. Select **\\AD\Software\XenMobile MDX Apps\iOS\WorxMail.mdx** file.  iOS MDX App Select an MDX file to upload

Step	Action
16.	The **iOS MDX App** details and policy options appear.  iOS MDX App Select an .mdx file to upload: WorxMail.mdx File name*: WorxMail App Description*: WorxMail-Release-10.0.0-103 App version: 103 Minimum OS version: Maximum OS version: Excluded devices: *example: manufacturer* Remove app if MDM profile is removed: ON
17.	Scroll down to the **Network Access** section and configure the following: Network access: `Tunneled to the internal network`  Network Access Network access: Tunneled to th... Certificate label: Initial VPN mode: Secure browse

Step	Action

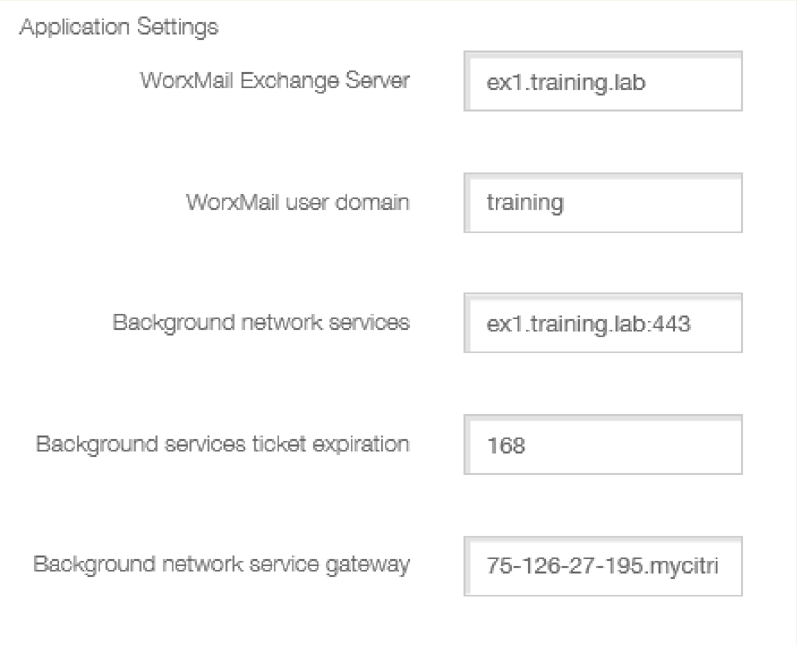
18. Scroll down to the Applications Settings section and configure the following settings:

WorxMail Exchange Server	`ex1.training.lab`
WorxMail user domain	`training`
Background network services	`ex1.training.lab:443`
Background network service gateway	`<IP1>FQDN:443`

Note: Your IP1 FQDN is available on the portal page

Example Only: 75-126-27-195.mycitrixtraining.net

Click **`Next`**.



Application Settings

WorxMail Exchange Server: ex1.training.lab

WorxMail user domain: training

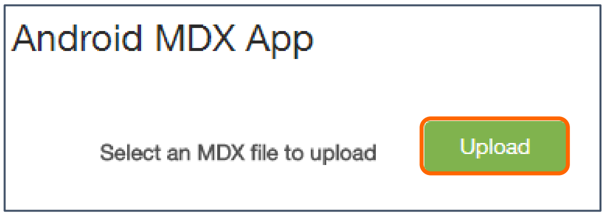
Background network services: ex1.training.lab:443

Background services ticket expiration: 168

Background network service gateway: 75-126-27-195.mycitri

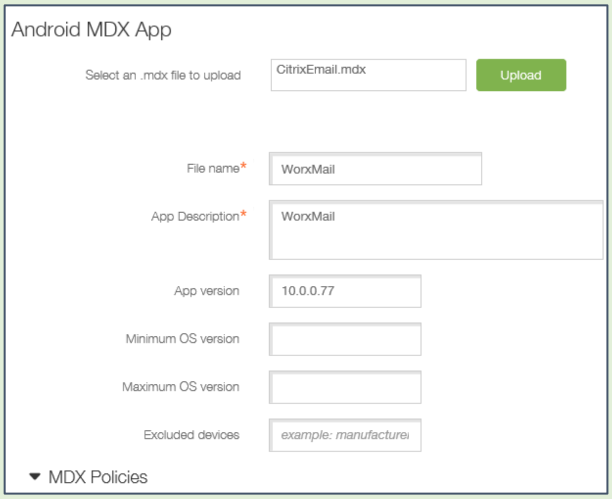
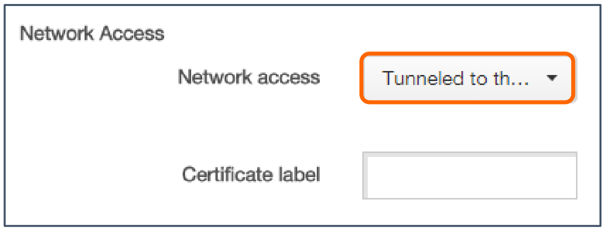
19. In the **Android MDX App** window, click **`Upload`**.

Select **`\\AD\Software\XenMobile MDX Apps\Android\CitrixEmail.mdx`** file.



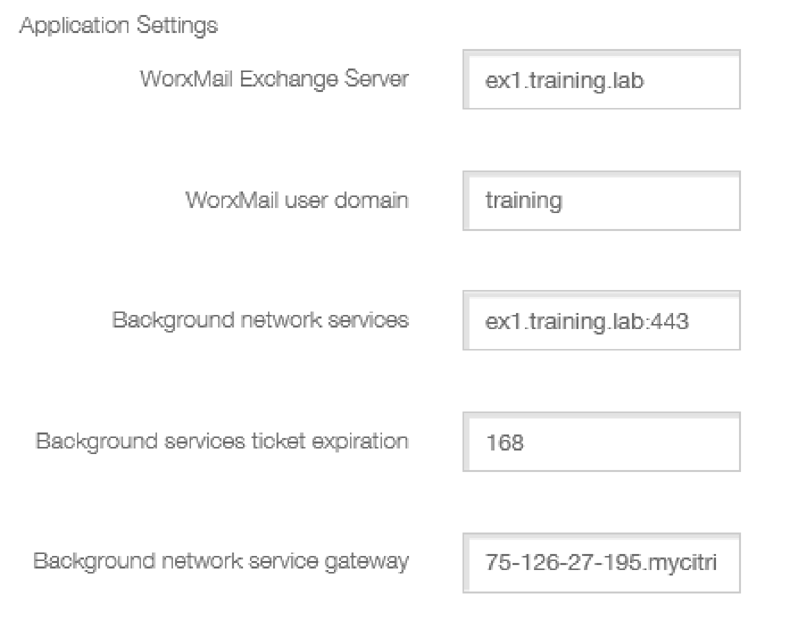
Android MDX App

Select an MDX file to upload

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>20.</td><td>The <b>Android MDX App</b> details and policy options appear.

Android MDX App
Select an .mdx file to upload: CitrixEmail.mdx
Upload
File name*: WorxMail
App Description*: WorxMail
App version: 10.0.0.77
Minimum OS version:
Maximum OS version:
Excluded devices: example: manufacturer
▾ MDX Policies</td></tr>
<tr><td>21.</td><td>Scroll down to the <b>Network Access</b> section and configure the following:<table><tr><td>Network access</td><td>Tunneled to the internal network</td></tr></table>
Network Access
Network access: Tunneled to th… ▾
Certificate label:</td></tr>
</table>

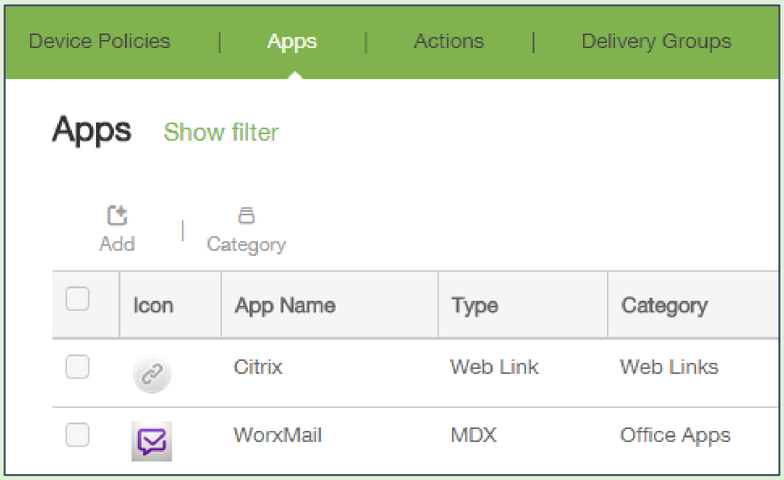
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>22.</td><td>Scroll down to the Applications Settings section and configure the following settings:
<table>
<tr><td>WorxMail Exchange Server</td><td><b>ex1.training.lab</b></td></tr>
<tr><td>WorxMail user domain</td><td><b>training</b></td></tr>
<tr><td>Background network services</td><td><b>ex1.training.lab:443</b></td></tr>
<tr><td>Background network service gateway</td><td><b><IP1>FQDN:443</b></td></tr>
</table>

<b>Note: Your IP1 FQDN is available on the portal page.</b>
<b>Example Only: 75-126-159-219.mycitrixtraining.net</b>

Click <b>Next</b>.

Application Settings
WorxMail Exchange Server: ex1.training.lab
WorxMail user domain: training
Background network services: ex1.training.lab:443
Background services ticket expiration: 168
Background network service gateway: 75-126-27-195.mycitri
</td></tr>
<tr><td>23.</td><td>Click <b>Next</b>. The Approvals window is displayed.</td></tr>
<tr><td>24.</td><td>Click <b>Next</b> to skip the Approvals window.</td></tr>
<tr><td>25.</td><td>Apply to AllUsers and click <b>Save</b> to save the application and its settings.

</td></tr>
</table>

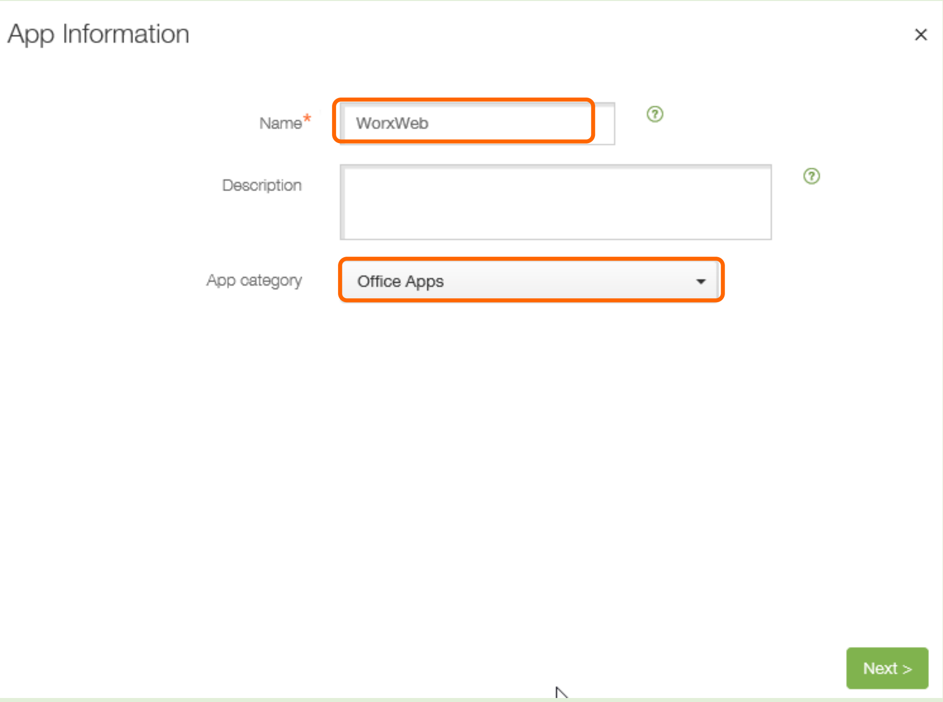
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>26.</td><td>WorxMail has been added to the App Store.



Apps Show filter

<table>
<tr><th>□</th><th>Icon</th><th>App Name</th><th>Type</th><th>Category</th></tr>
<tr><td>□</td><td></td><td>Citrix</td><td>Web Link</td><td>Web Links</td></tr>
<tr><td>□</td><td></td><td>WorxMail</td><td>MDX</td><td>Office Apps</td></tr>
</table>
</td></tr>
<tr><td>27.</td><td>Repeat <b>Steps 11-12</b> of this exercise to add <b>WorxWeb</b>.</td></tr>
<tr><td>28.</td><td>Configure the application as follows:

<table>
<tr><td>Name</td><td><b>WorxWeb</b></td></tr>
<tr><td>App category</td><td><b>Office Apps</b></td></tr>
</table>

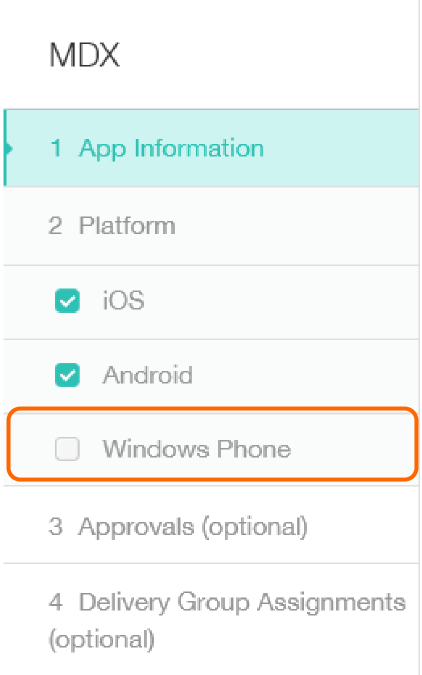
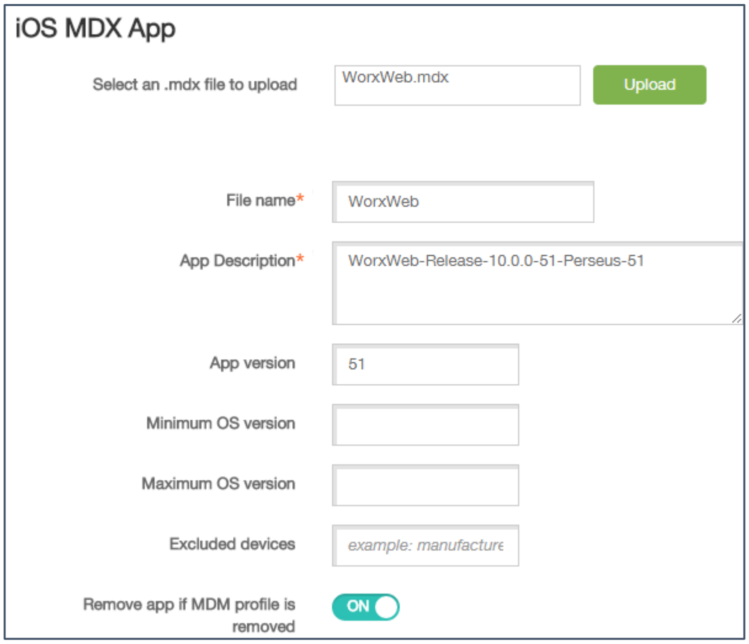


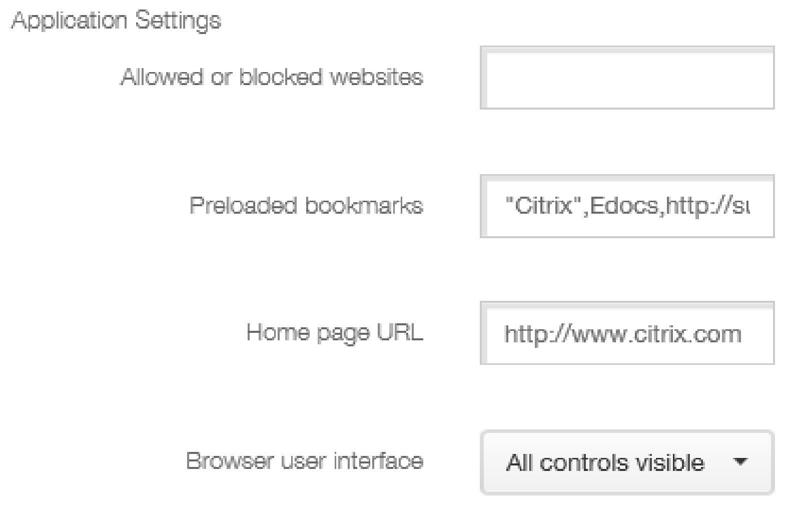
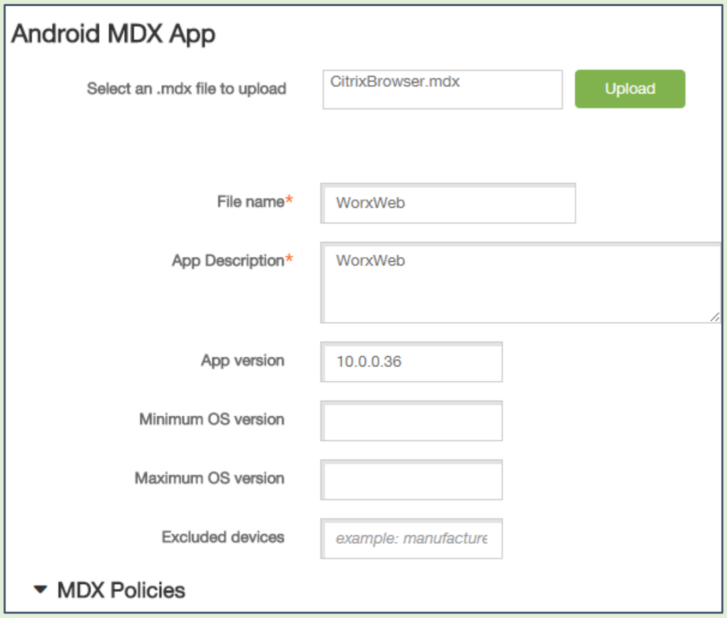
App Information

Name* WorxWeb

Description

App category Office Apps
</td></tr>
</table>

Step	Action
29.	Deselect the **Windows Phone** platform option on the left. Click `Next`.  MDX 1 App Information 2 Platform ☑ iOS ☑ Android □ Windows Phone 3 Approvals (optional) 4 Delivery Group Assignments (optional)
30.	In the **iOS MDX App** window, click `Upload`. Select `\\AD\Software\XenMobile MDX Apps\iOS\WorxWeb.mdx` file.
31.	The **iOS MDX App** details and policy options appear.  iOS MDX App Select an .mdx file to upload: WorxWeb.mdx [Upload] File name*: WorxWeb App Description*: WorxWeb-Release-10.0.0-51-Perseus-51 App version: 51 Minimum OS version: Maximum OS version: Excluded devices: *example: manufacture* Remove app if MDM profile is removed: ON

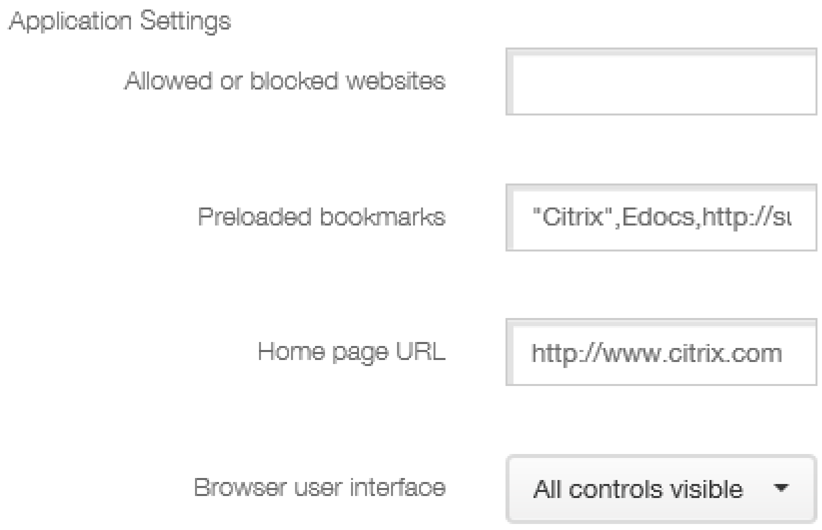
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>32.</td><td>Scroll down to the <b>Application Settings</b> section and configure the following:
<table>
<tr><td>Preloaded bookmarks</td><td>“Citrix”,Edocs,http://support.citrix.com/proddocs</td></tr>
<tr><td>Home page URL</td><td>http://www.citrix.com</td></tr>
</table>
Click Next.

Application Settings
Allowed or blocked websites:
Preloaded bookmarks: "Citrix",Edocs,http://su
Home page URL: http://www.citrix.com
Browser user interface: All controls visible ▾
</td></tr>
<tr><td>33.</td><td>In the <b>Android MDX App</b> window, click Upload.
Select \\AD\Software\XenMobile MDX Apps\Android\CitrixBrowser.mdx file.</td></tr>
<tr><td>34.</td><td>The <b>Android MDX App</b> details and policy options appear.

Android MDX App
Select an .mdx file to upload: CitrixBrowser.mdx [Upload]
File name*: WorxWeb
App Description*: WorxWeb
App version: 10.0.0.36
Minimum OS version:
Maximum OS version:
Excluded devices: example: manufacture
▾ MDX Policies
</td></tr>
</table>

Step | Action

35. Scroll down to the **Application Settings** section and configure the following:

Preloaded bookmarks	`"Citrix",Edocs,http://support.citrix.com/proddocs`
Home page URL	`http://www.citrix.com`

Click **`Next.`**



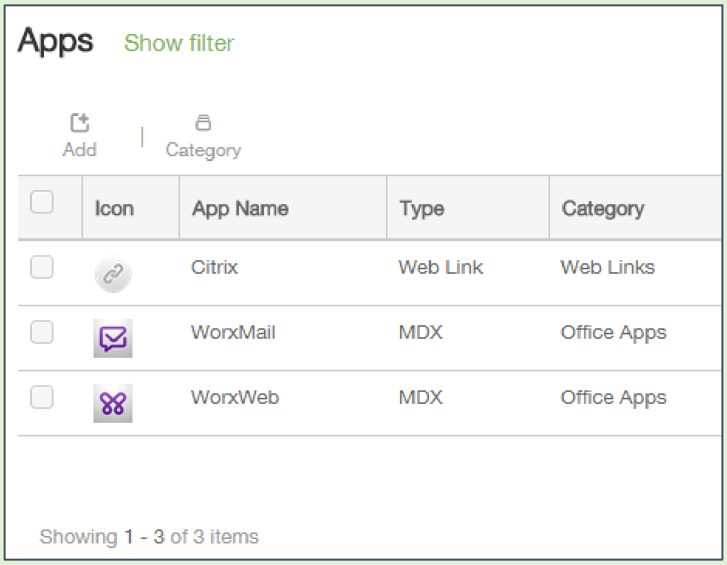
Application Settings

Allowed or blocked websites	
Preloaded bookmarks	"Citrix",Edocs,http://su
Home page URL	http://www.citrix.com
Browser user interface	All controls visible ▾

36. Click **`Next`** to skip the Approvals configuration.

37. Apply to **AllUsers** and click **`Save`**.

38. **WorxWeb** has been added to the App Store.

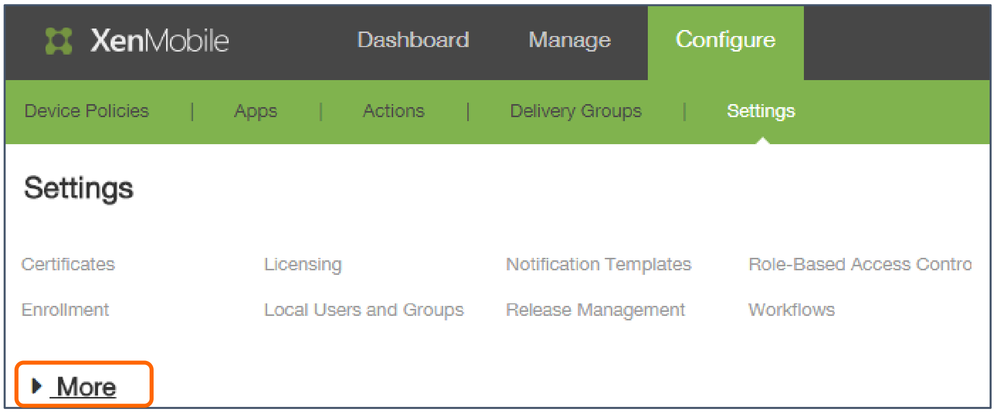
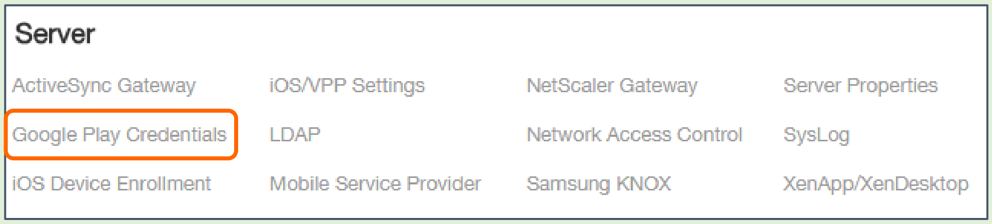
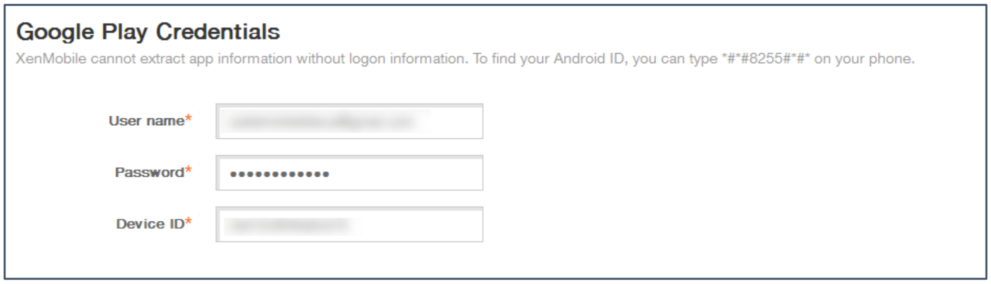


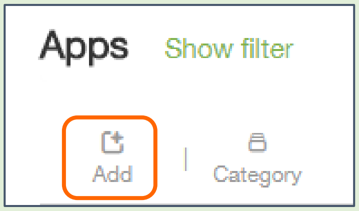
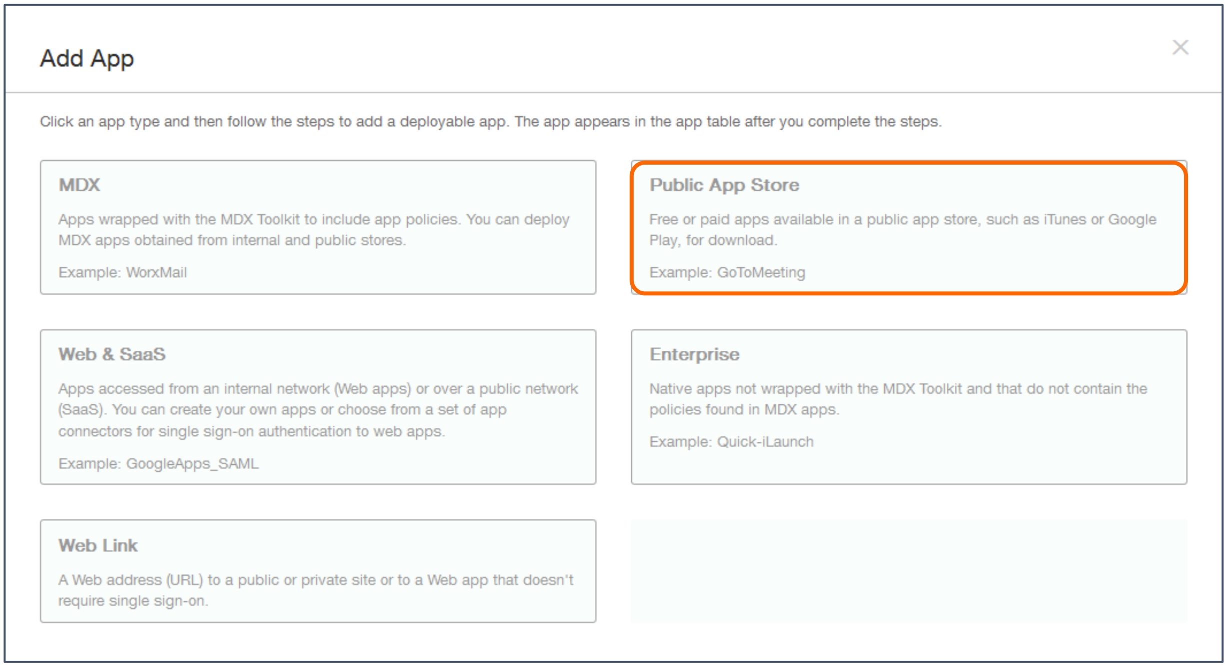
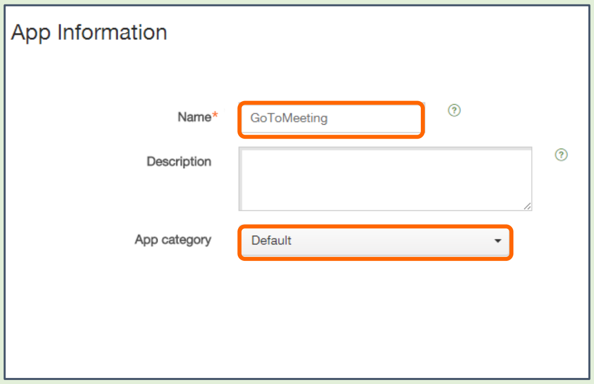
Apps Show filter

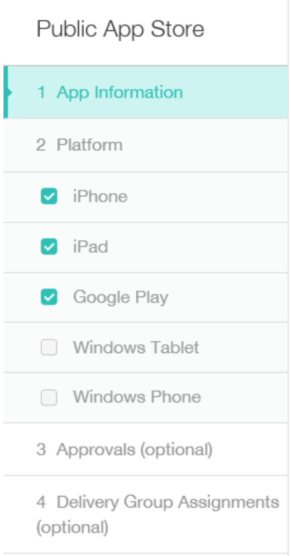
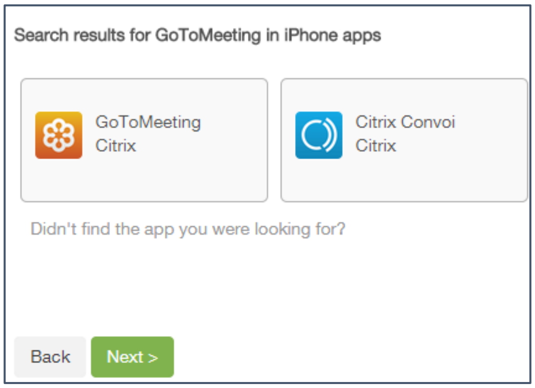
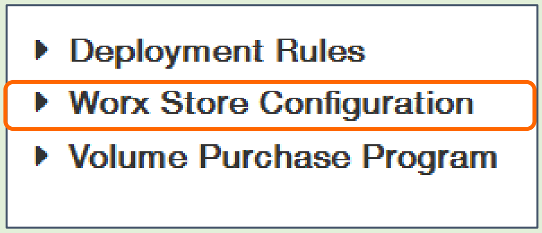
□	Icon	App Name	Type	Category
□		Citrix	Web Link	Web Links
□		WorxMail	MDX	Office Apps
□		WorxWeb	MDX	Office Apps

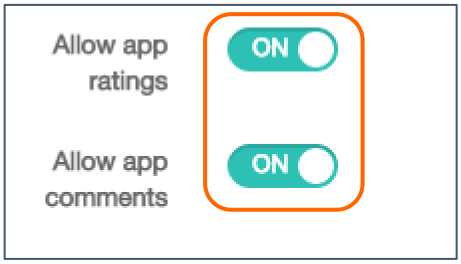
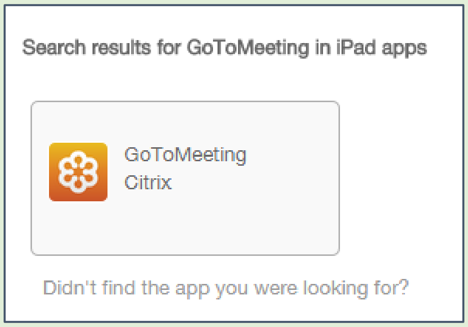
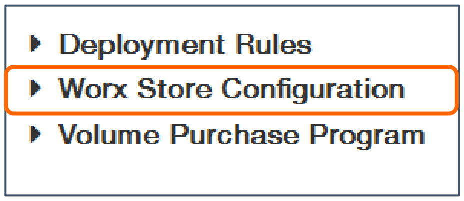
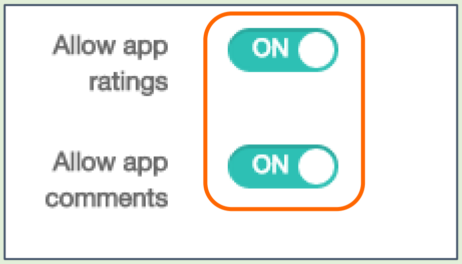
Showing 1 - 3 of 3 items

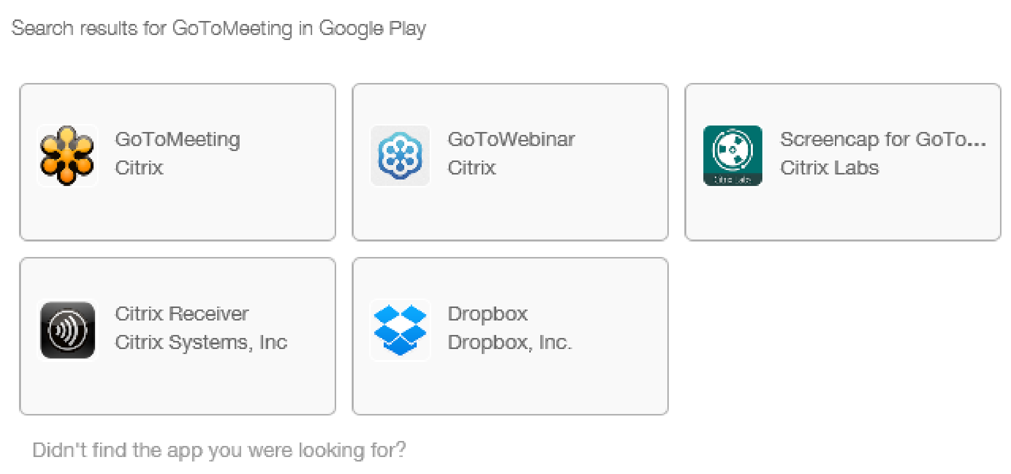
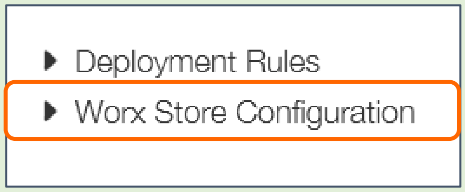
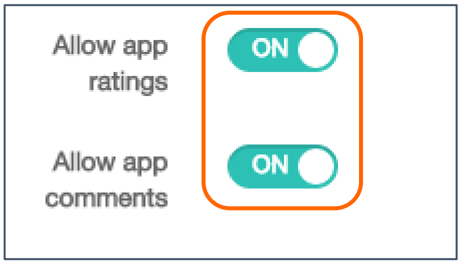
Note: If you are performing this lab with an iOS device, go to Step 42.

Step	Action
39.	Navigate to **Configure > Settings** and expand the **More** node.  XenMobile Dashboard Manage Configure Device Policies | Apps | Actions | Delivery Groups | Settings Settings Certificates Licensing Notification Templates Role-Based Access Contro Enrollment Local Users and Groups Release Management Workflows More
40.	Under the **Server** section, click on `Google Play Credentials`.  Server ActiveSync Gateway iOS/VPP Settings NetScaler Gateway Server Properties Google Play Credentials LDAP Network Access Control SysLog iOS Device Enrollment Mobile Service Provider Samsung KNOX XenApp/XenDesktop
41.	Enter **<u>your</u>** Google credentials and device id below. User name: Password: Device ID: **Note:** To obtain your device id, download the Device ID application from the Google Play store.  Google Play Credentials XenMobile cannot extract app information without logon information. To find your Android ID, you can type "#"#8255#"#" on your phone. User name* [redacted] Password* ••••••••••••• Device ID* [redacted]

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>42.</td><td>Navigate to <b>Configure -> Apps</b> and click <code>Add</code> again.

 </td></tr>
<tr><td>43.</td><td>Select <code>Public App Store</code>.

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 &amp; 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.</td></tr>
<tr><td>44.</td><td>The <b>App Information</b> window is displayed.
Configure the following settings:
<table><tr><td>Name*</td><td><code>GoToMeeting</code></td></tr><tr><td>App category</td><td><code>Default</code></td></tr></table>
App Information
Name* GoToMeeting
Description
App category Default</td></tr>
</table>

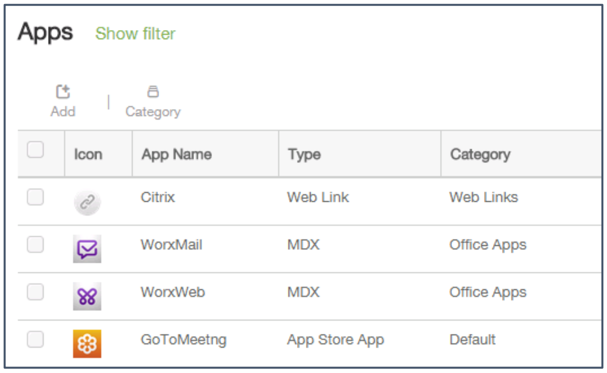
Step	Action
45.	**Windows Tablet** and **Windows Phone** are disabled by default. Click **Next**. **Note:** If you are performing this lab with an iOS device, uncheck the **Google Play** platform.  Public App Store 1 App Information 2 Platform ☑ iPhone ☑ iPad ☑ Google Play ☐ Windows Tablet ☐ Windows Phone 3 Approvals (optional) 4 Delivery Group Assignments (optional)
46.	In the Search text box, enter `GoToMeeting` and click `Search`.
47.	The Search results are displayed. Click on **GoToMeeting**.  Search results for GoToMeeting in iPhone apps GoToMeeting Citrix Citrix Convoi Citrix Didn't find the app you were looking for? Back Next >
48.	Scroll down and expand **Worx Store Configuration.**  Deployment Rules Worx Store Configuration Volume Purchase Program

Step	Action
49.	**App ratings** and **Allow app comments** are enabled by default. Click **Next**.  Allow app ratings: ON Allow app comments: ON
50.	The iPad search results are displayed. Click **GoToMeeting**.  Search results for GoToMeeting in iPad apps GoToMeeting Citrix Didn't find the app you were looking for?
51.	Scroll down and expand **Worx Store Configuration.**  Deployment Rules Worx Store Configuration Volume Purchase Program
52.	**Allow App ratings** and **Allow app comments** are enabled by default. Click **Next**.  Allow app ratings: ON Allow app comments: ON

Step	Action
53.	The Search results for **Google Play** are displayed. Click **GoToMeeting**. **Note:** If you are performing this lab with an iOS device, go to **Step 56**.  Search results for GoToMeeting in Google Play GoToMeeting Citrix GoToWebinar Citrix Screencap for GoTo... Citrix Labs Citrix Receiver Citrix Systems, Inc Dropbox Dropbox, Inc. Didn't find the app you were looking for?
54.	Scroll down and expand Worx Store Configuration. 
55.	**App ratings** and **Allow app comments** are enabled by default. Click **Next**.  Allow app ratings ON Allow app comments ON
56.	Click **Next** to skip the **Approvals** configuration. Apply to the **AllUsers** group and click **Save**.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>57.</td><td>

GoToMeeting has been added from the public app store.



Apps Show filter

Add | Category

<table>
<tr><th>□</th><th>Icon</th><th>App Name</th><th>Type</th><th>Category</th></tr>
<tr><td>□</td><td></td><td>Citrix</td><td>Web Link</td><td>Web Links</td></tr>
<tr><td>□</td><td></td><td>WorxMail</td><td>MDX</td><td>Office Apps</td></tr>
<tr><td>□</td><td></td><td>WorxWeb</td><td>MDX</td><td>Office Apps</td></tr>
<tr><td>□</td><td></td><td>GoToMeetng</td><td>App Store App</td><td>Default</td></tr>
</table>

</td></tr>
<tr><td>58.</td><td>

Click `Add` again and select `Public App Store`.

Configure Citrix Receiver as follows:

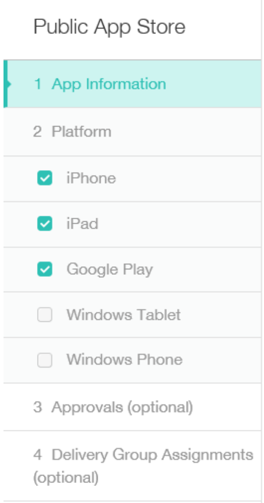
<table>
<tr><td>Name*</td><td><code>Citrix Receiver</code></td></tr>
<tr><td>App category</td><td><code>Default</code></td></tr>
</table>

</td></tr>
<tr><td>59.</td><td>

Windows Tablet and **Windows Phone** are disabled by default.

Click `Next`.

Note: If you are performing this lab with an iOS device, uncheck the **Google Play** platform.



Public App Store

1 App Information

2 Platform

☑ iPhone

☑ iPad

☑ Google Play

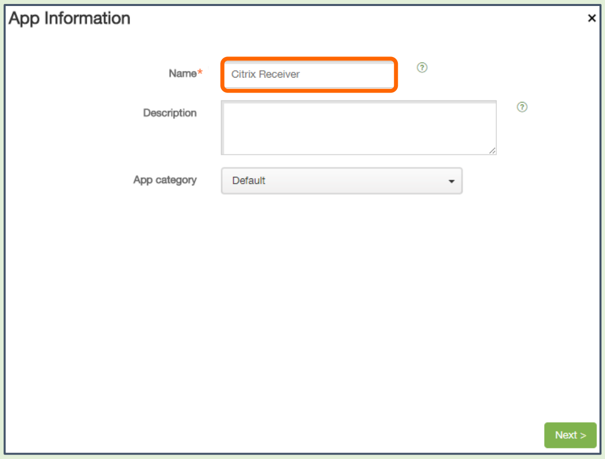
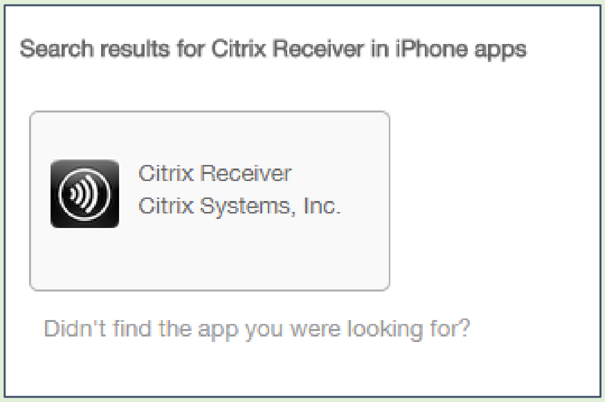
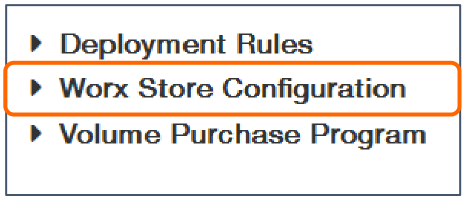
□ Windows Tablet

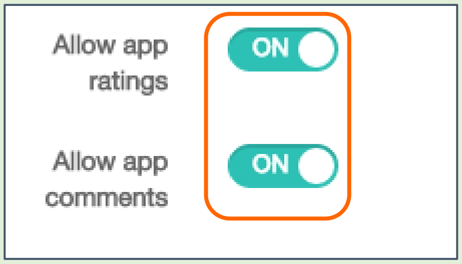
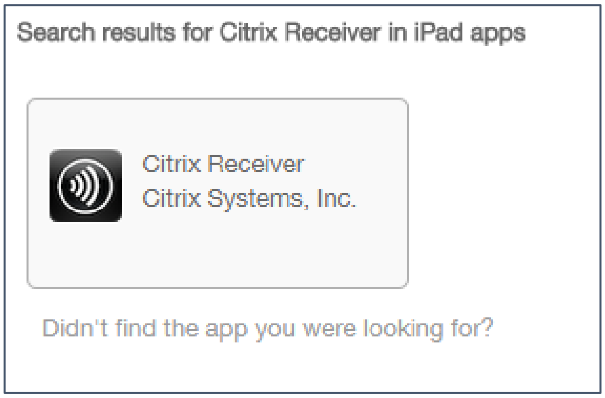
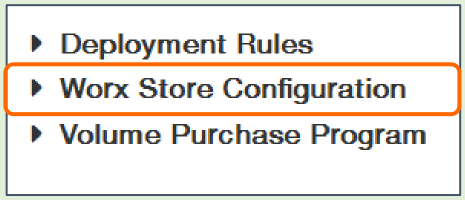
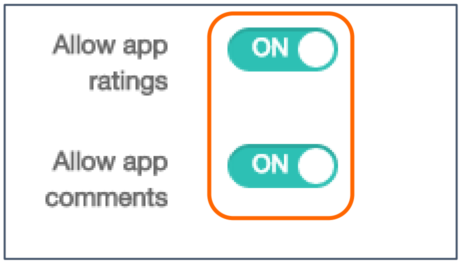
□ Windows Phone

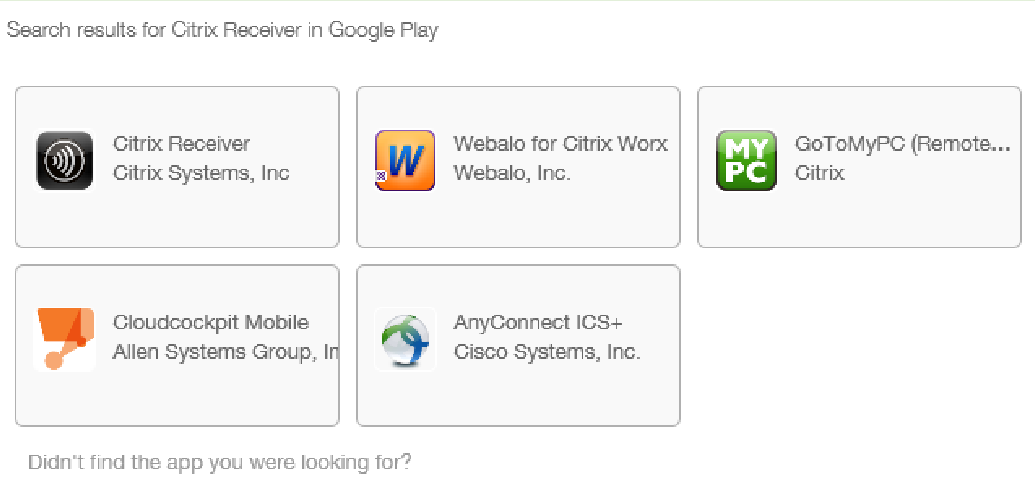
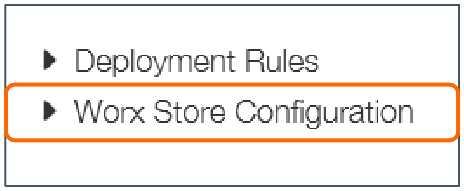
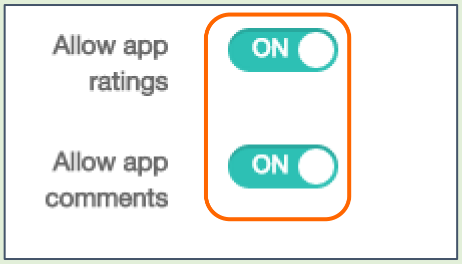
3 Approvals (optional)

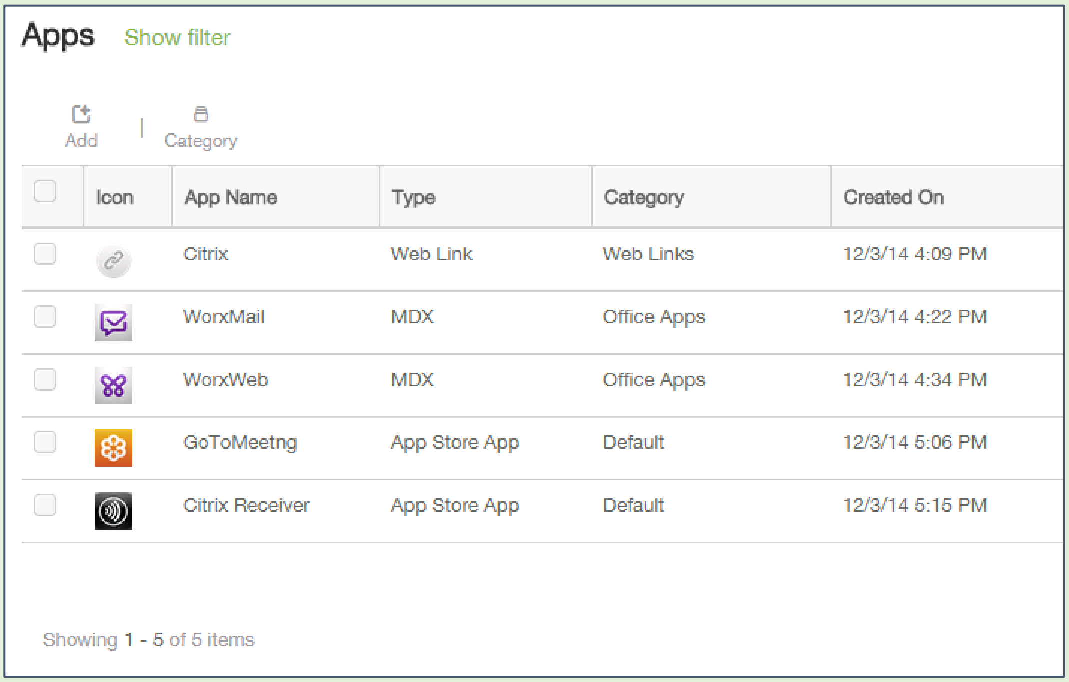
4 Delivery Group Assignments (optional)

</td></tr>
</table>

Step	Action
60.	Name the application Citrix Receiver. Click Next.  App Information Name* Citrix Receiver Description App category Default Next >
61.	In the Search text box, enter Citrix Receiver and click Search.
62.	The search results for **iPhone** are displayed. Click on Citrix Receiver.  Search results for Citrix Receiver in iPhone apps Citrix Receiver Citrix Systems, Inc. Didn't find the app you were looking for?
63.	Scroll down and expand **Worx Store Configuration.**  ▸ Deployment Rules ▸ Worx Store Configuration ▸ Volume Purchase Program

Step	Action
64.	Enable **Allow App ratings** and **Allow app comments** are enabled by default. Click `Next`.  Allow app ratings ON Allow app comments ON
65.	The search results for **iPads** are displayed. Click on `Citrix Receiver`.  Search results for Citrix Receiver in iPad apps Citrix Receiver Citrix Systems, Inc. Didn't find the app you were looking for?
66.	Scroll down and expand **Worx Store Configuration.**  ▸ Deployment Rules ▸ Worx Store Configuration ▸ Volume Purchase Program
67.	**Allow App ratings** and **Allow app comments** are enabled by default. Click `Next`.  Allow app ratings ON Allow app comments ON

Step	Action
68.	The search results for Google Play are displayed. Click on **`Citrix Receiver`**. **Note:** If you are performing this lab with an iOS device, go to **Step 71**.  Search results for Citrix Receiver in Google Play Citrix Receiver Citrix Systems, Inc Webalo for Citrix Worx Webalo, Inc. GoToMyPC (Remote... Citrix Cloudcockpit Mobile Allen Systems Group, In AnyConnect ICS+ Cisco Systems, Inc. Didn't find the app you were looking for?
69.	Scroll down and expand **Worx Store Configuration.**  ▸ Deployment Rules ▸ Worx Store Configuration
70.	**Allow App ratings** and **Allow app comments** are enabled by default. Click **`Next`**.  Allow app ratings: ON Allow app comments: ON
71.	Click **`Next`** to skip the **Approvals** configuration. Apply to the **AllUsers** group and click **`Save`**.

Step	Action
72.	**Citrix Receiver** is added to the **Enterprise App Store**. 

Apps Show filter

□	Icon	App Name	Type	Category	Created On
□		Citrix	Web Link	Web Links	12/3/14 4:09 PM
□		WorxMail	MDX	Office Apps	12/3/14 4:22 PM
□		WorxWeb	MDX	Office Apps	12/3/14 4:34 PM
□		GoToMeetng	App Store App	Default	12/3/14 5:06 PM
□		Citrix Receiver	App Store App	Default	12/3/14 5:15 PM

Showing 1 - 5 of 5 items

Exercise Summary

You have now added web links, mdx apps, and public store applications to XenMobile Server for your iOS or Android devices. Now you are ready to add applications to delivery groups.

Exercise 5

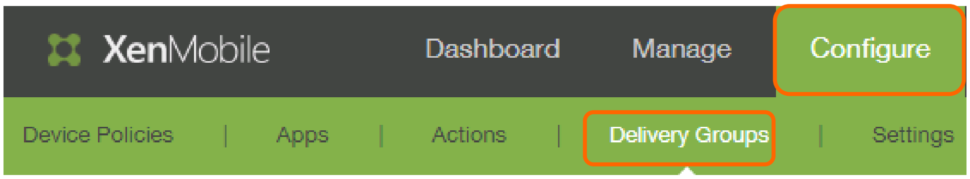
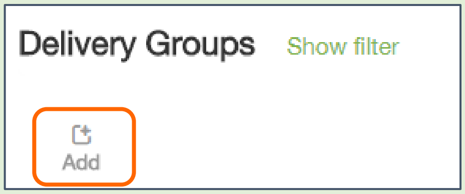
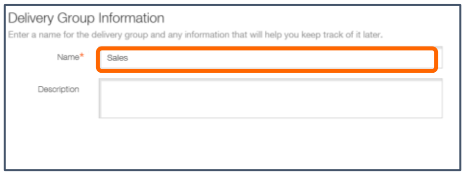
Assigning Applications to a Delivery Group

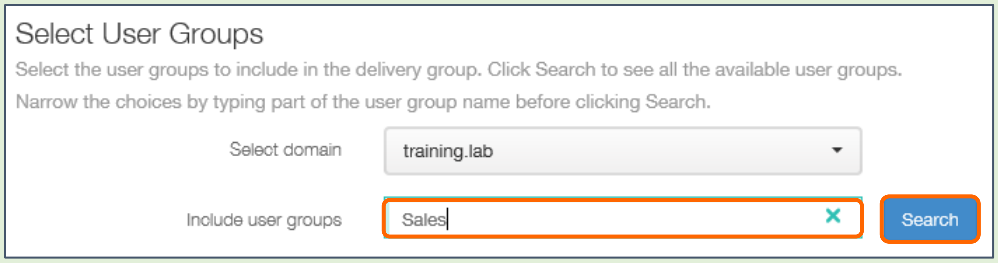
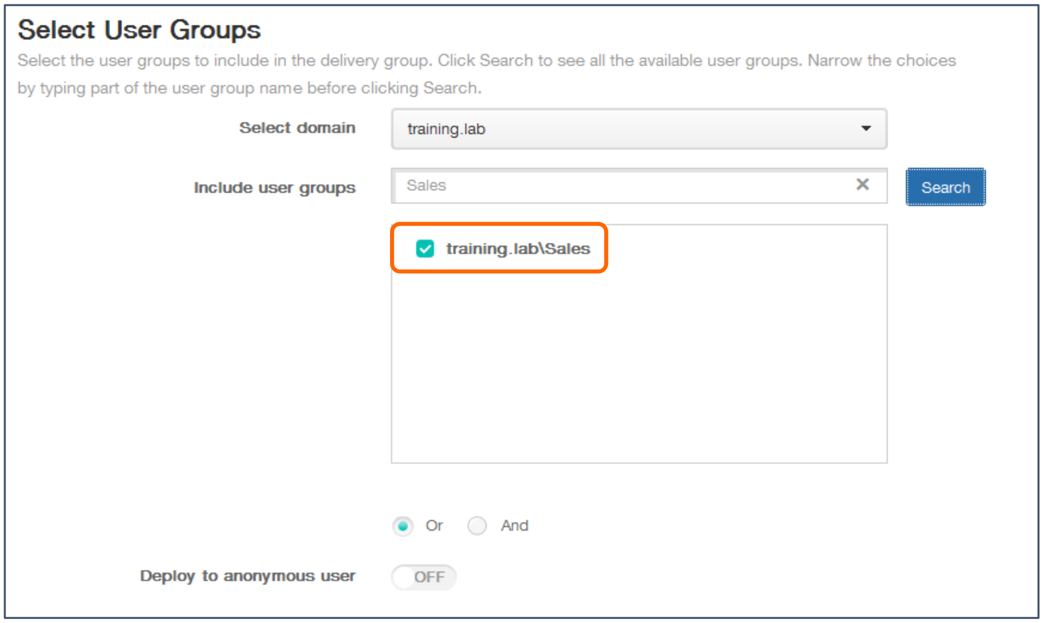
Overview

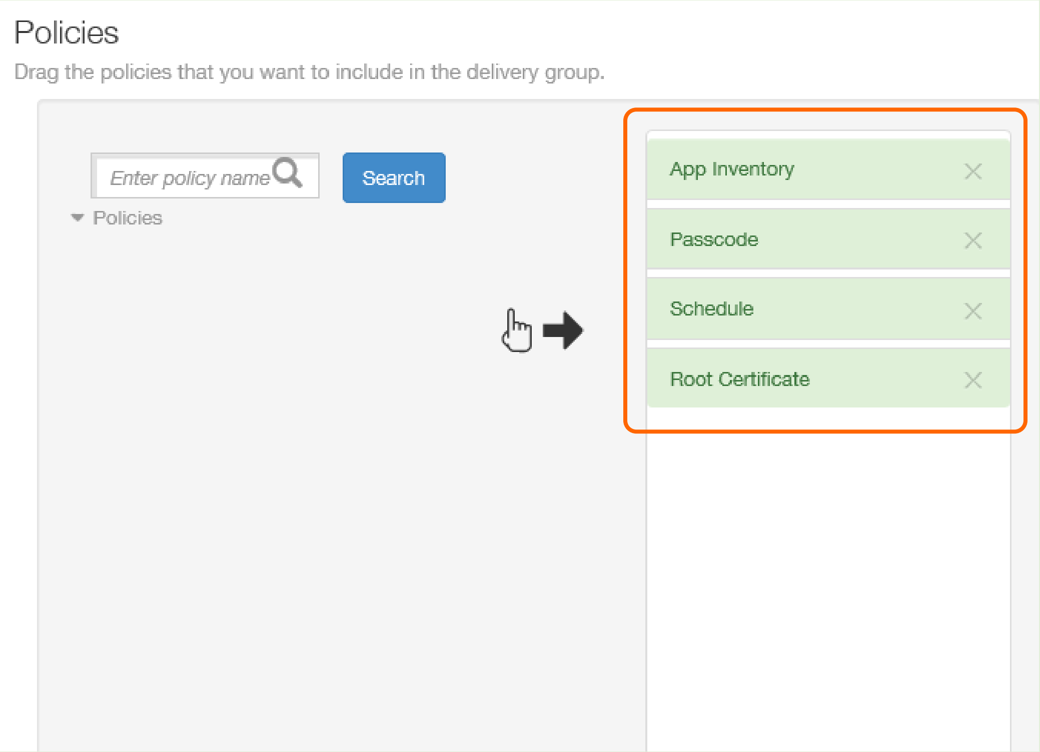
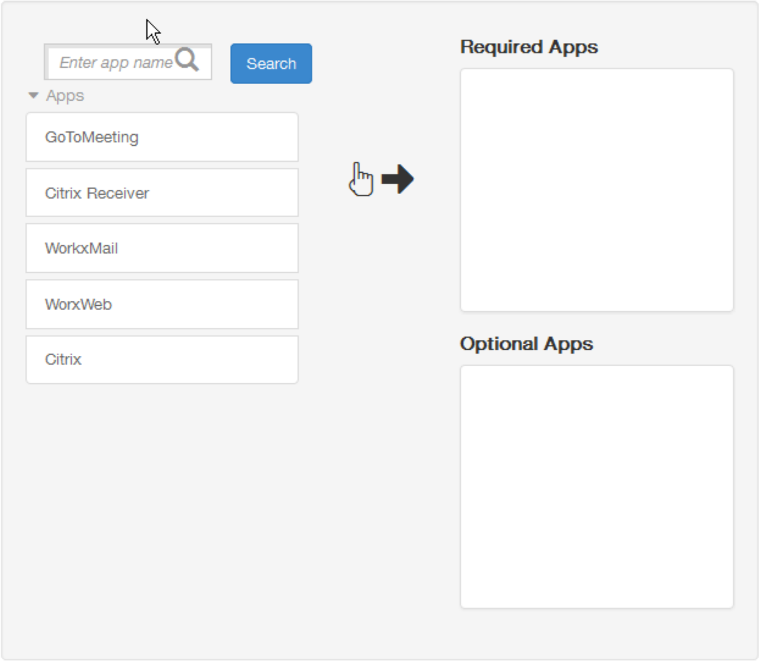
In this exercise students will create Delivery Groups within the XenMobile Server. Students will then map Active Directory groups to those roles and assign applications to the respective delivery groups

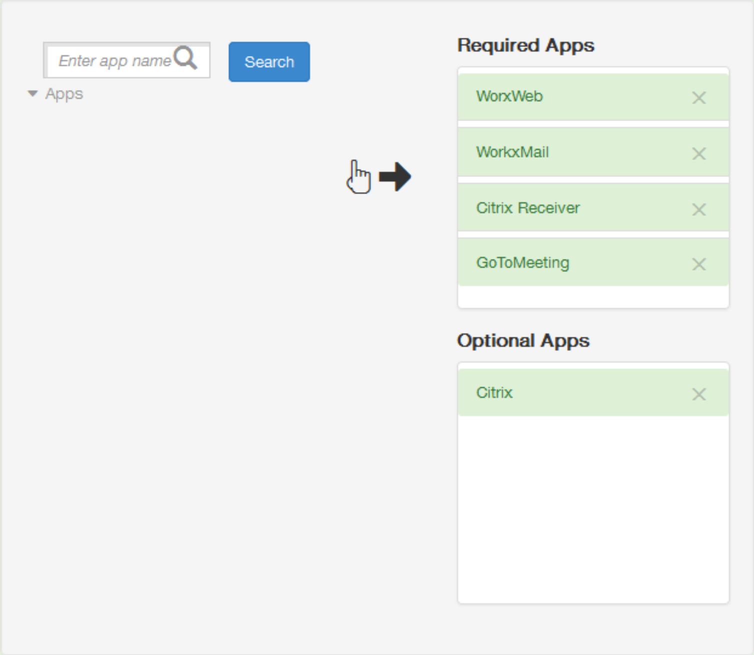
Step by step guidance

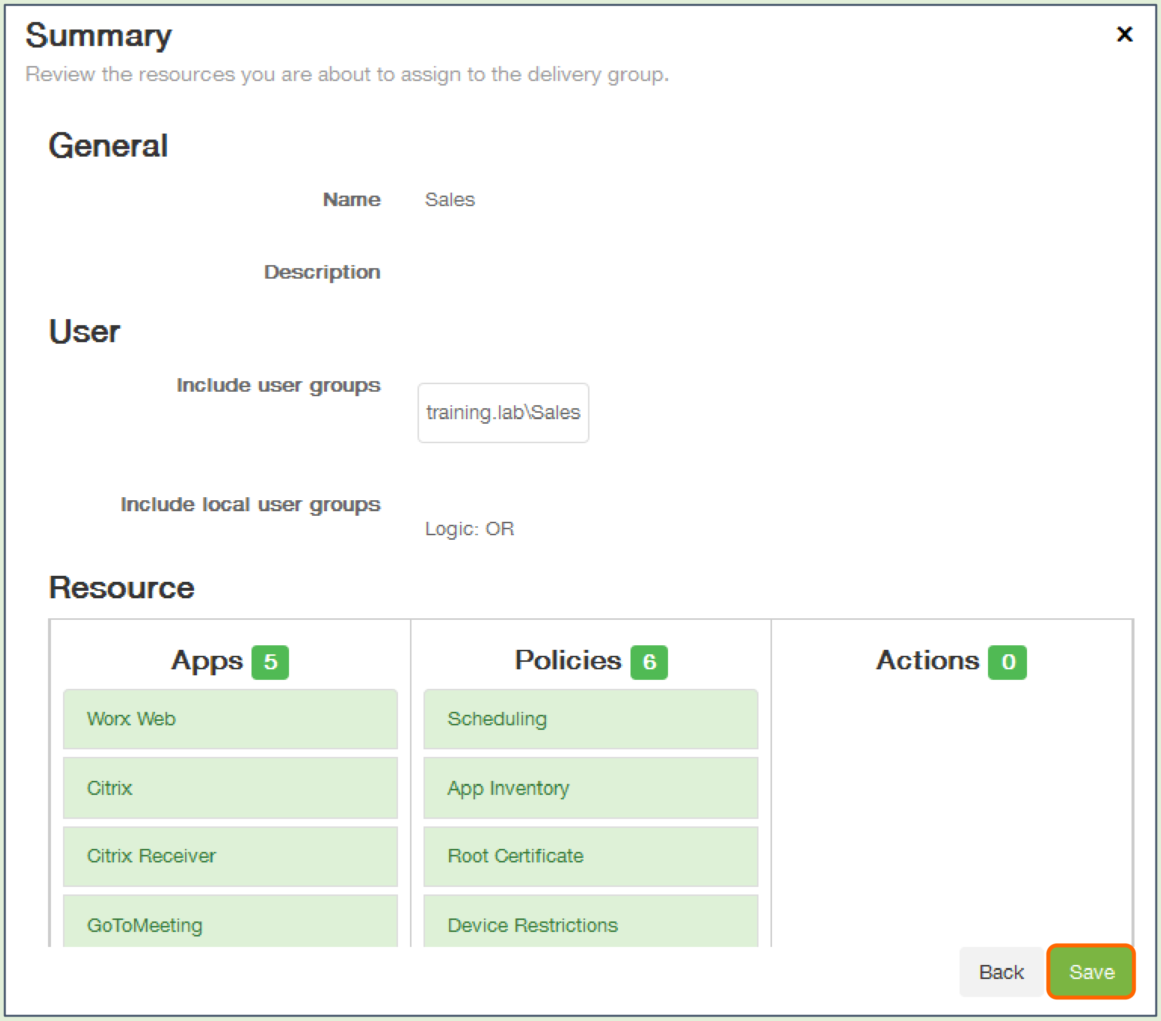
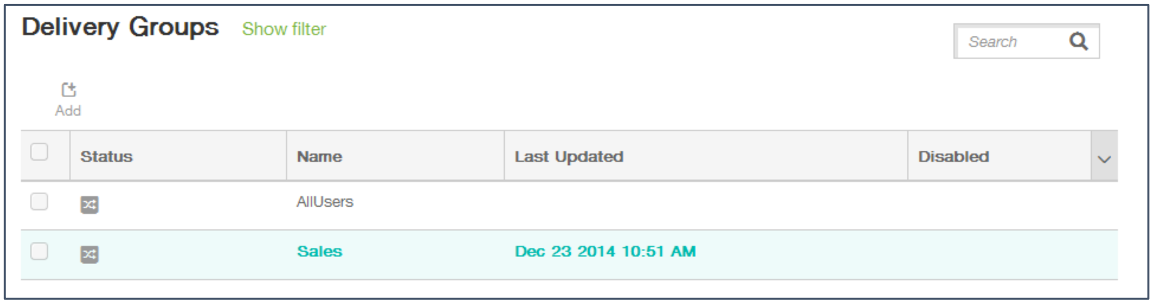
Estimated time to complete this lab: **10** minutes.

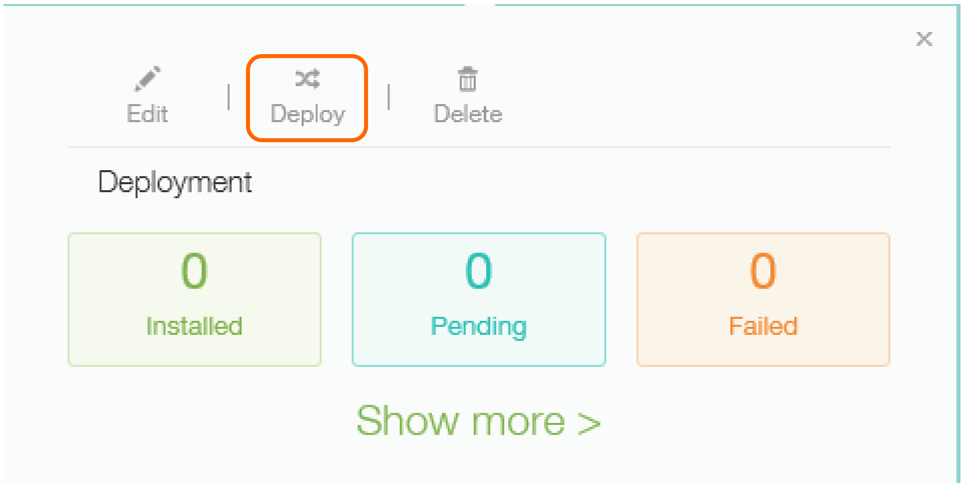
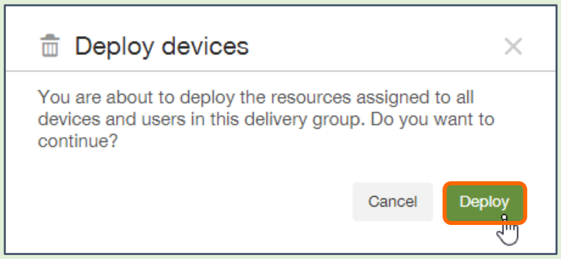
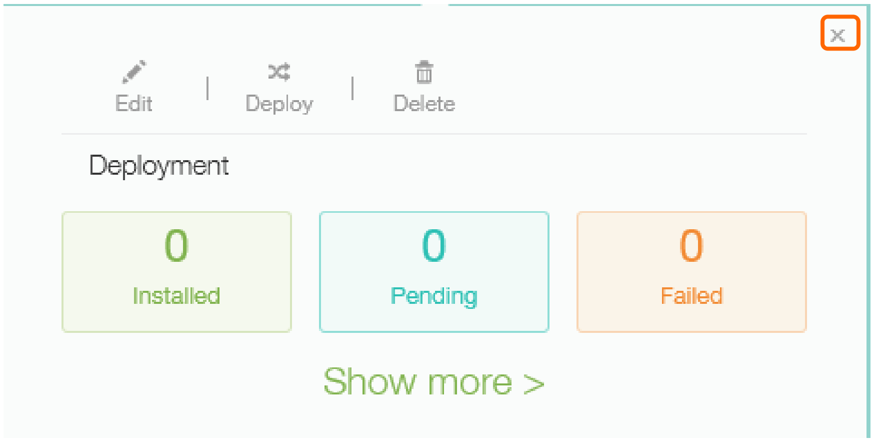
Step	Action
1.	Select the `Configure` tab, and on the green ribbon, click `Delivery Groups`.  XenMobile Dashboard Manage Configure Device Policies Apps Actions Delivery Groups Settings
2.	Click `Add`. 
3.	Name the Delivery Group `Sales`. Click `Next`.  Delivery Group Information Enter a name for the delivery group and any information that will help you keep track of it later. Name* Sales Description

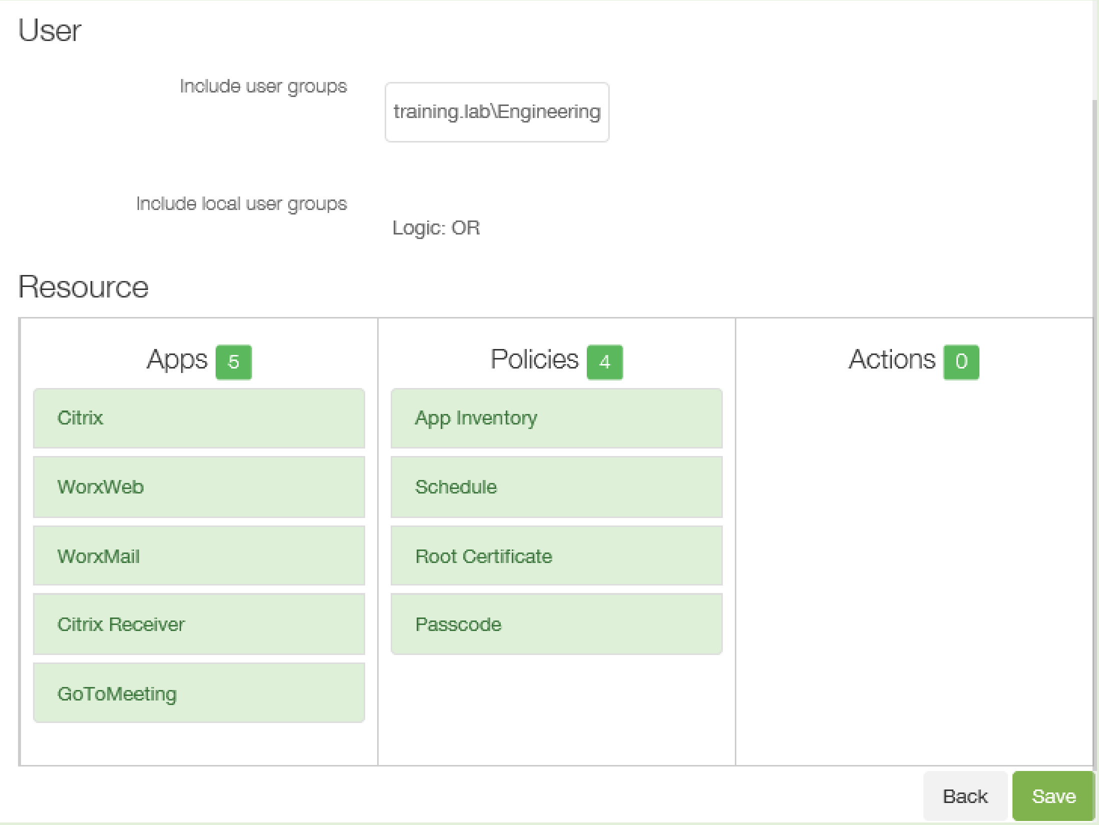
Step	Action
4.	The **Select User Groups** window is displayed. Type `Sales` in the **Include user groups** text box and click the `Search` button. Select User Groups Select the user groups to include in the delivery group. Click Search to see all the available user groups. Narrow the choices by typing part of the user group name before clicking Search. Select domain: training.lab Include user groups: Sales
5.	The **Sales** group is enumerated. Click the checkbox next to the **Sales** group. Click `Next`. 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: training.lab Include user groups: Sales ☑ training.lab\Sales ● Or ○ And Deploy to anonymous user: OFF

Step	Action
6.	The **Policies** window is displayed. Drag the **App Inventory, Schedule, Root Certificate,** and **Passcode** policies to the right to assign to the delivery group.  Policies Drag the policies that you want to include in the delivery group. App Inventory Passcode Schedule Root Certificate Then click **Next**.
7.	The **Applications** window is displayed.  Enter app name Search Apps GoToMeeting Citrix Receiver WorkxMail WorxWeb Citrix Required Apps Optional Apps

Step	Action
8.	Drag **GoToMeeting, Citrix Receiver, WorxMail,** and **WorxWeb** applications over to the **Required Applications** box. Drag the **Citrix** web link over to the **Optional Applications** box. Click **`Next`**.  Enter app name Search Apps Required Apps WorxWeb WorkxMail Citrix Receiver GoToMeeting Optional Apps Citrix
9.	The **Actions** window is displayed. Click **`Next`** to skip.

Step	Action
10.	The **Summary** page is displayed. Click **`Save`**.  Summary Review the resources you are about to assign to the delivery group. General Name Sales Description User Include user groups training.lab\Sales Include local user groups Logic: OR Resource Apps 5: Worx Web, Citrix, Citrix Receiver, GoToMeeting Policies 6: Scheduling, App Inventory, Root Certificate, Device Restrictions Actions 0 Back Save
11.	The **Sales** delivery group is saved.  Delivery Groups Show filter Search Add □ Status · Name · Last Updated · Disabled □ AllUsers □ Sales · Dec 23 2014 10:51 AM
12.	Click on the **`Sales`** delivery group.

Step	Action
13.	The properties of the delivery group are displayed. Click on Deploy.  Edit Deploy Delete Deployment 0 Installed 0 Pending 0 Failed Show more >
14.	Click Deploy again on the **Deploy devices** popup window.  Deploy devices You are about to deploy the resources assigned to all devices and users in this delivery group. Do you want to continue?
15.	Click the X to close the **Sales** delivery group properties window.  Edit Deploy Delete Deployment 0 Installed 0 Pending 0 Failed Show more >

Step	Action
16.	Repeat the above steps to create a new delivery group called **Engineering** with the same policies and apps assigned.  User Include user groups: training.lab\Engineering Include local user groups Logic: OR Resource Apps 5: Citrix, WorxWeb, WorxMail, Citrix Receiver, GoToMeeting Policies 4: App Inventory, Schedule, Root Certificate, Passcode Actions 0

Exercise Summary

In this exercise, you added applications to the XenMobile Server. You have also created delivery groups, mapped an AD group to the delivery group, and assigned applications to the delivery group. This allows an administrator to easily assign applications to users based on their group.

Exercise 6

Configure NetScaler Gateway for Enterprise Store

Overview

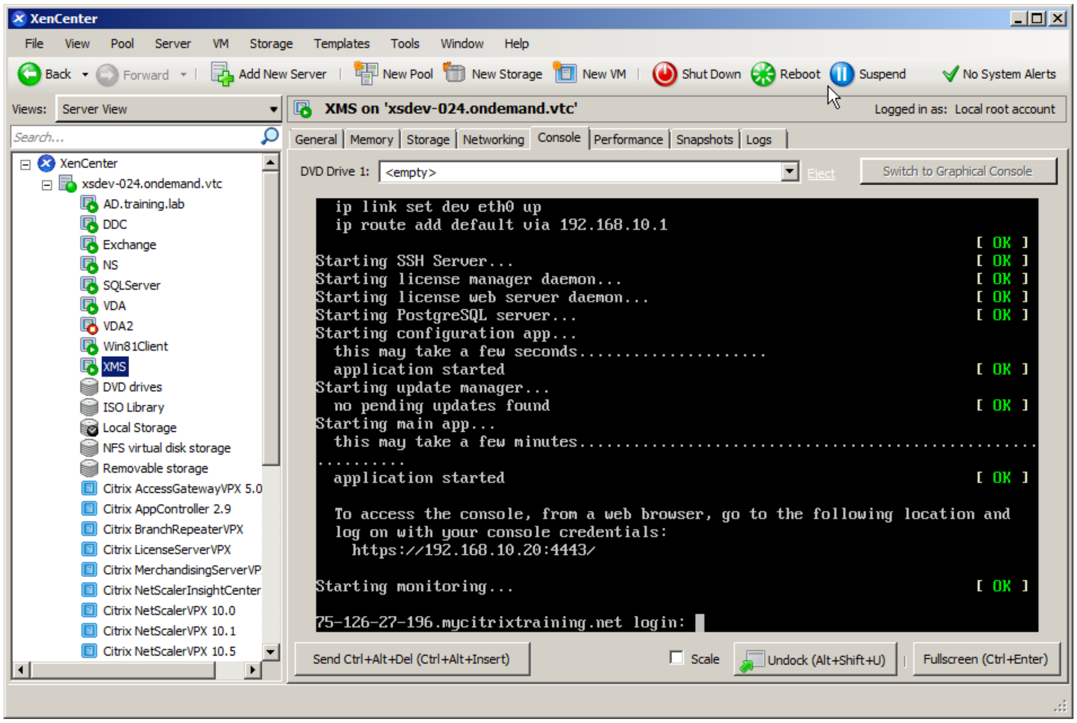
In this exercise you will use the **XenMobile Get Started** wizard within the NetScaler Configuration Utility to configure NetScaler Gateway for an Enterprise Store. The wizard will create the virtual server, load balancing virtual server, policies, and profiles necessary to connect to the enterprise store on the XenMobile Server.

Step by step guidance

Estimated time to complete this lab: **25** minutes.

Step	Action
1.	By using SSL Offload will the SSL session will be terminated on the NetScaler. In order to allow the backend traffic to tcp port 80 (HTTP) we need to re-configure the firewall of the XenMobile Server. Switch to XenCenter and go to the console of the XenMobile Server (SITE1-XMS1) and logon with the following credentials:

Username	`admin`
Password	`Citrix123`

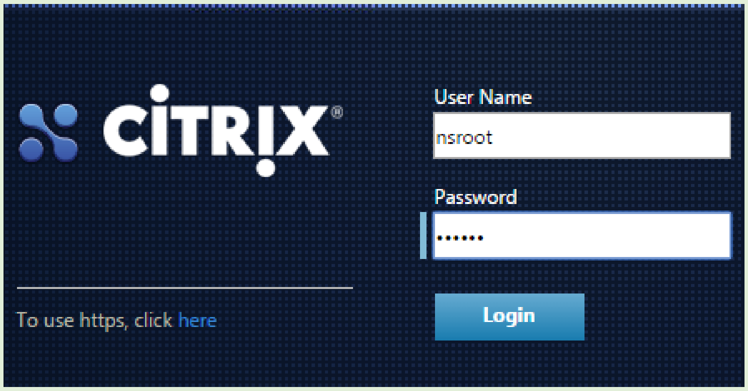
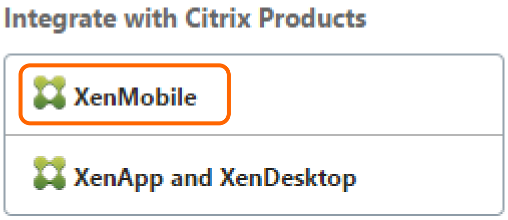
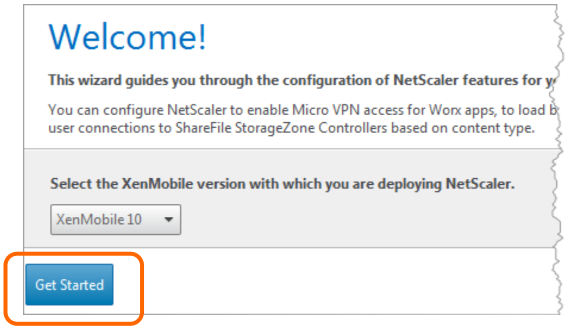


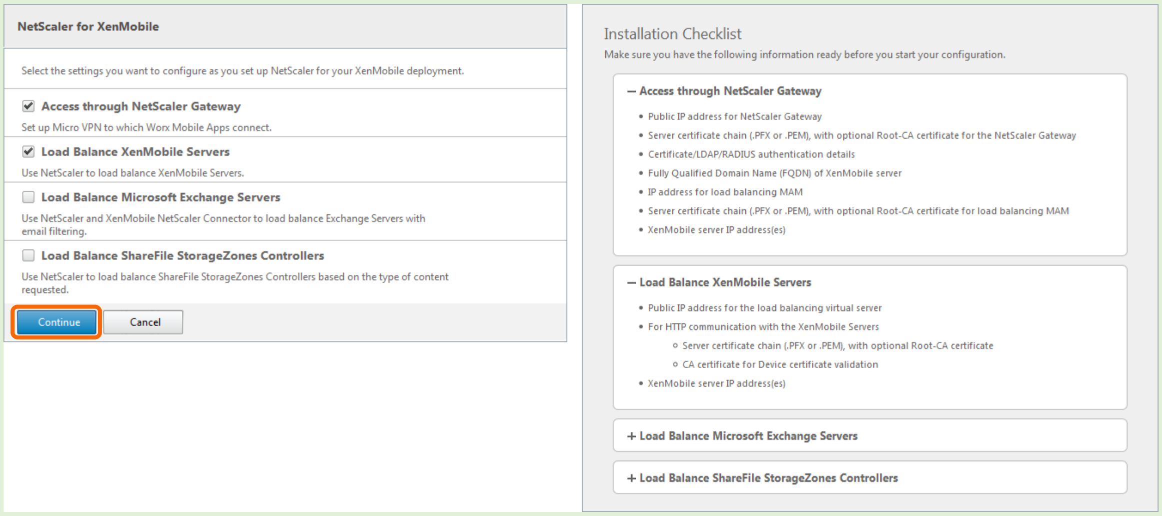
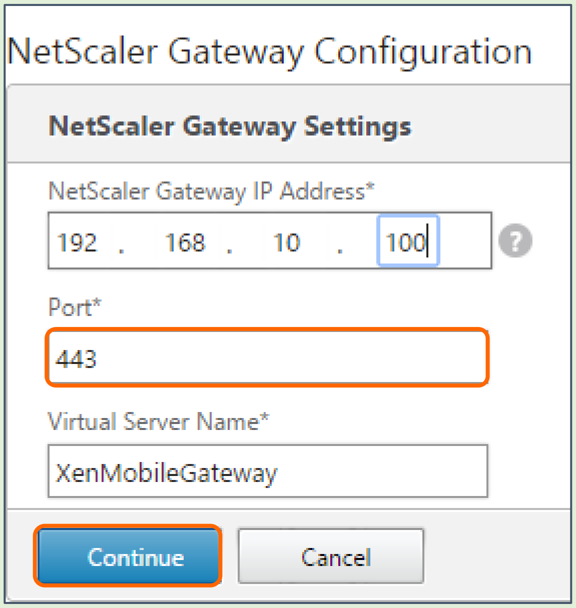
```
  ip link set dev eth0 up
  ip route add default via 192.168.10.1
                                                                        [ OK ]
Starting SSH Server...                                                  [ OK ]
Starting license manager daemon...                                      [ OK ]
Starting license web server daemon...                                   [ OK ]
Starting PostgreSQL server...                                           [ OK ]
Starting configuration app...
  this may take a few seconds.....................
  application started                                                   [ OK ]
Starting update manager...
  no pending updates found                                              [ 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://192.168.10.20:4443/

Starting monitoring...                                                  [ OK ]

75-126-27-196.mycitrixtraining.net login: 
```

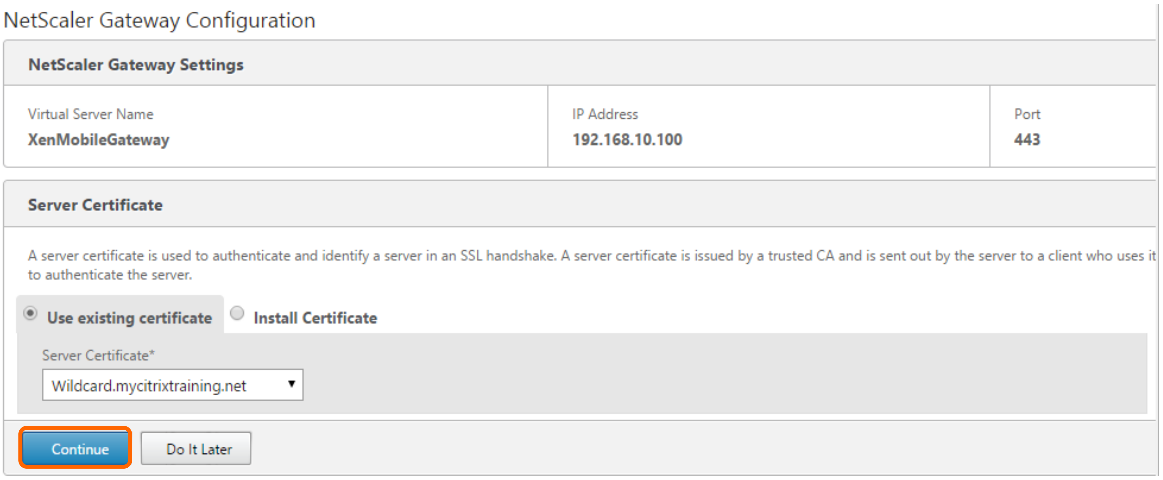
Step	Action
2.	Enable tcp port 80 traffic to the XenMobile Server. Optionally you can add the NetScaler Gateway SNIP in the **Access white list**, to add additional security.

```
-----------------------------------
 Main Menu
 -----------------------------------
 [0] Configuration
 [1] Clustering
 [2] System
 [3] Troubleshooting
 [4] Help
 [5] Log Out
 -----------------------------------
 Choice: [0 - 5] 0

-----------------------------------
 Configuration Menu
 -----------------------------------
 [0] Back to Main Menu
 [1] Network
 [2] Firewall
 [3] Database
 [4] Listener Ports
 -----------------------------------
 Choice: [0 - 4] 2

 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) [n]: y
     Access white list []:

   Management HTTPS service
     Port: 4443
     Enable access (y/n) [y]:
     Access white list []:

   SSH service
     Port [22]: 22
     Enable access (y/n) [n]:

   Management API (for initial staging) HTTPS service
     Port [30001]:
     Enable access (y/n) [y]: n

   Remote support tunnel
     Port [8081]:
     Enable access (y/n) [n]:


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

3.	Select the `Site1-Win81Client` virtual machine in XenCenter.

Step	Action
4.	In IE, open another tab and navigate to `http://192.168.10.50` and log on with the following credentials: Username `nsroot` Password `nsroot`  User Name: nsroot Password: ••••••
5.	In the NetScaler Gateway Configuration Utility, scroll down to the **Integrate with Citrix Products** section and click `XenMobile`. Click `Get Started`.  Integrate with Citrix Products XenMobile XenApp and XenDesktop  Welcome! This wizard guides you through the configuration of NetScaler features for y You can configure NetScaler to enable Micro VPN access for Worx apps, to load b user connections to ShareFile StorageZone Controllers based on content type. Select the XenMobile version with which you are deploying NetScaler. XenMobile 10

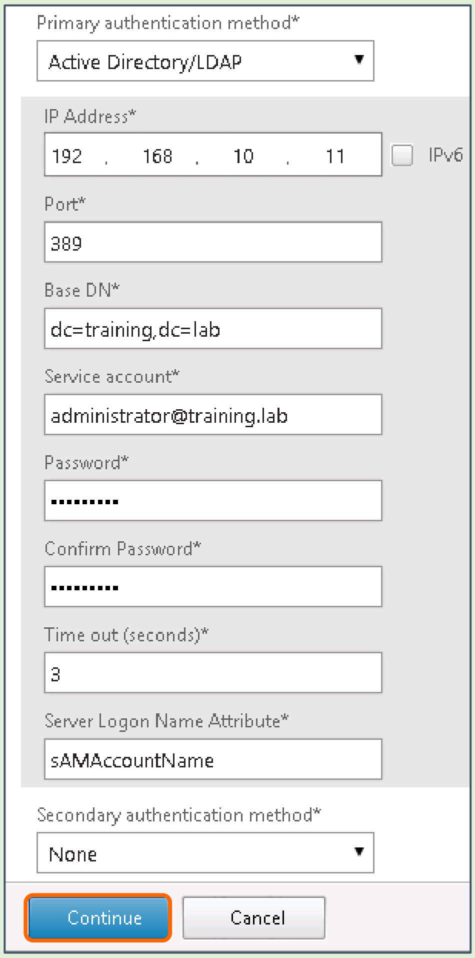
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>6.</td><td>Scroll down to the bottom of the window and click <code>Continue</code>.

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
+ Load Balance ShareFile StorageZones Controllers
 </td></tr>
<tr><td>7.</td><td>Click <code>Continue</code>.</td></tr>
<tr><td>8.</td><td>Configure the following settings:
<table><tr><td>IP Address</td><td><code>192.168.10.100</code></td></tr><tr><td>Port</td><td><code>443</code></td></tr><tr><td>Virtual Server Name</td><td><code>XenMobileGateway</code></td></tr></table>
Click <code>Continue</code>.

NetScaler Gateway Configuration
NetScaler Gateway Settings
NetScaler Gateway IP Address*: 192 . 168 . 10 . 100
Port*: 443
Virtual Server Name*: XenMobileGateway
 </td></tr>
</table>

Step	Action
9.	The **wildcard.mycitrixtraining.net** certificate is selected by default. Click **Continue**.  NetScaler Gateway Configuration **NetScaler Gateway Settings** Virtual Server Name: **XenMobileGateway** IP Address: **192.168.10.100** Port: **443** **Server Certificate** 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*: Wildcard.mycitrixtraining.net ▾ Continue | Do It Later

Step	Action
10.	Configure the following **Authentication Settings**:

IP Address	192.168.10.11
Port	389
Base DN	dc=training,dc=lab
Service account	administrator@training.lab
Password	Citrix123
Confirm Password	Citrix123
Server Logon Name Attribute	sAMAccountName

Click **Continue**.



Primary authentication method*: Active Directory/LDAP

IP Address*: 192 . 168 . 10 . 11 □ IPv6

Port*: 389

Base DN*: dc=training,dc=lab

Service account*: administrator@training.lab

Password*: •••••••••

Confirm Password*: •••••••••

Time out (seconds)*: 3

Server Logon Name Attribute*: sAMAccountName

Secondary authentication method*: None

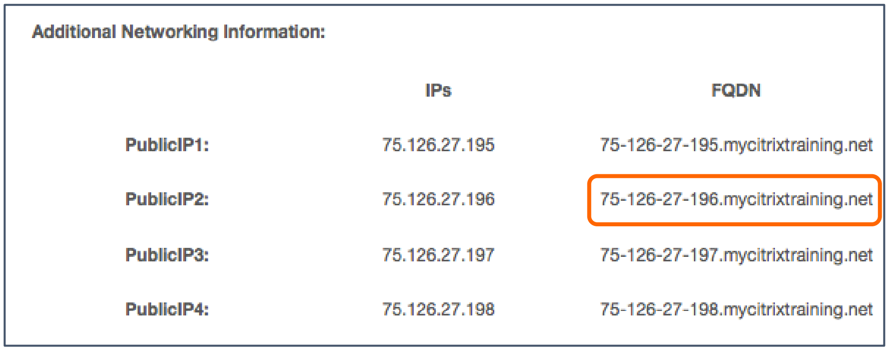
Note: A best practice is to use a service account for the Base DN. However, for this lab environment and exercise, we are using the administrator account.

Step	Action
11.	Configure the following **MAM Controller FQDN, LB IP Address** and **Port No.**

Load Balancing FQDN for MAM	IP2FQDN
Load Balancing IP address for MAM	192.168.10.21
Port	8443
SSL Traffic Configuration	HTTP communication to XenMobile Server

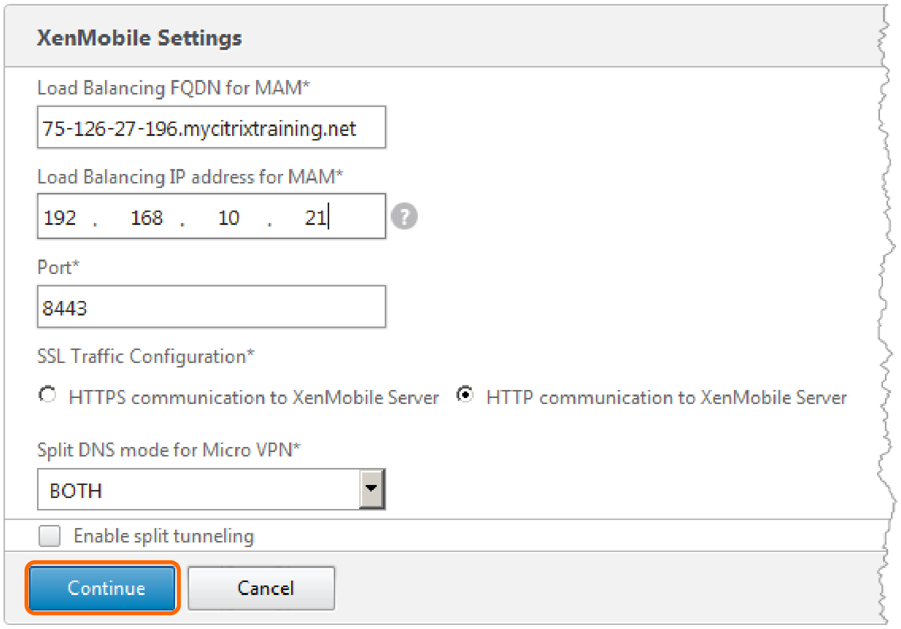
Note: Your IP2 FQDN is available on the portal page.

Example Only: 75-126-27-196.mycitrixtraining.net



Additional Networking Information:

	IPs	FQDN
PublicIP1:	75.126.27.195	75-126-27-195.mycitrixtraining.net
PublicIP2:	75.126.27.196	75-126-27-196.mycitrixtraining.net
PublicIP3:	75.126.27.197	75-126-27-197.mycitrixtraining.net
PublicIP4:	75.126.27.198	75-126-27-198.mycitrixtraining.net



XenMobile Settings

Load Balancing FQDN for MAM*
75-126-27-196.mycitrixtraining.net

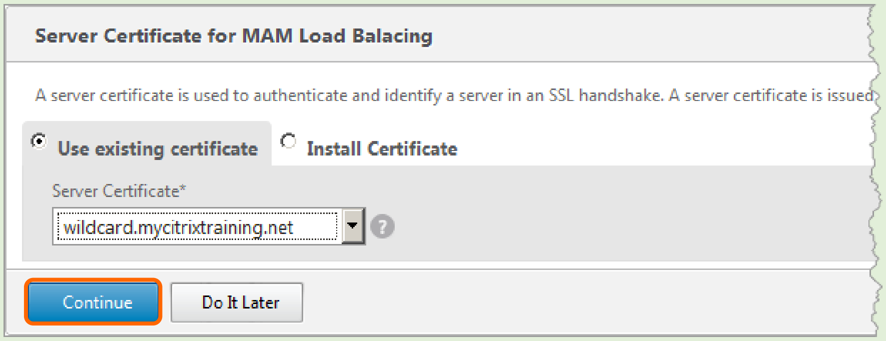
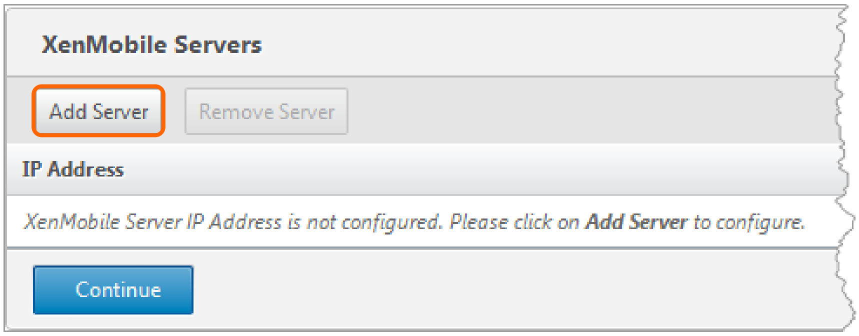
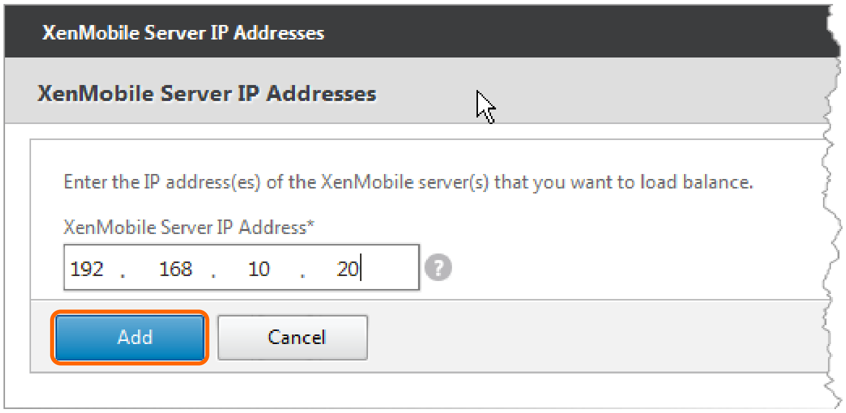
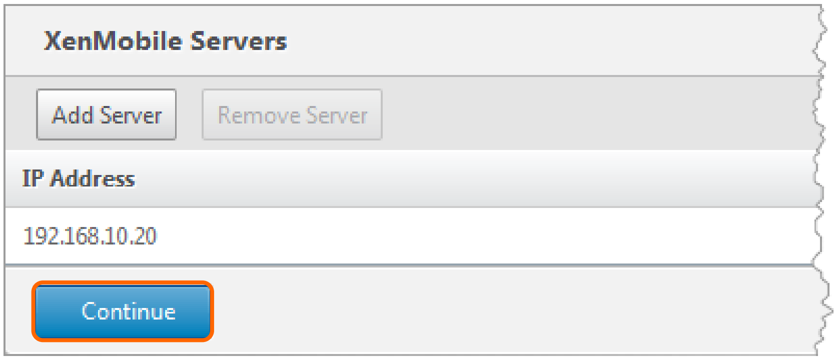
Load Balancing IP address for MAM*
192 . 168 . 10 . 21

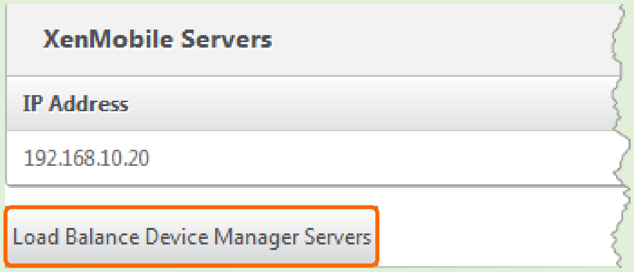
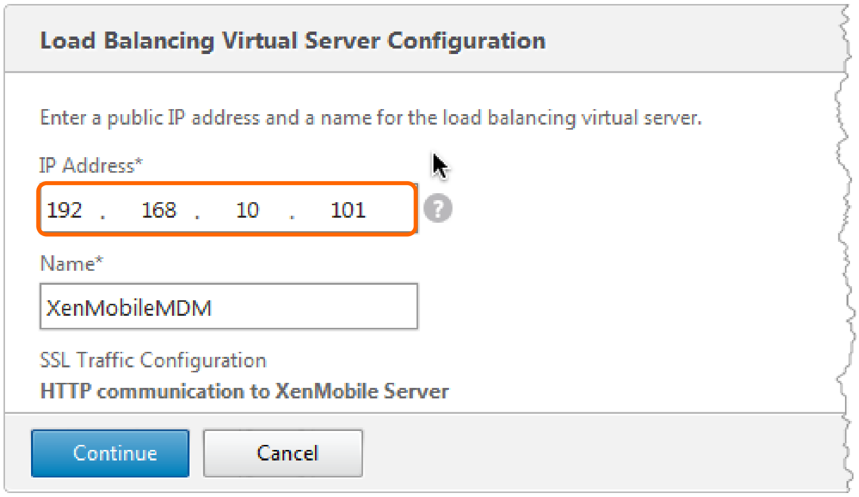
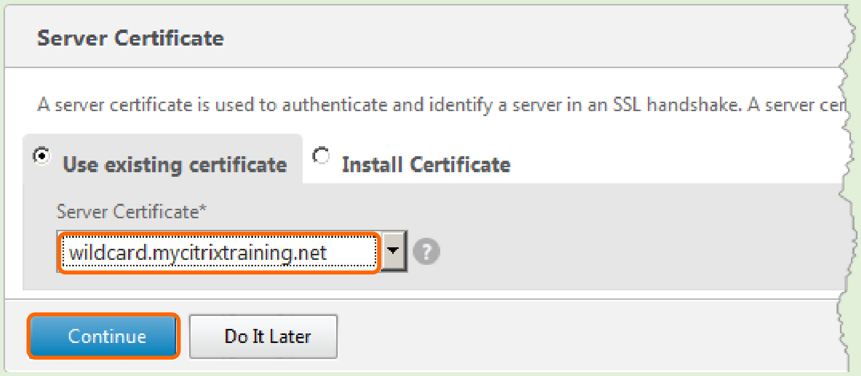
Port*
8443

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

Split DNS mode for Micro VPN*
BOTH

☐ Enable split tunneling

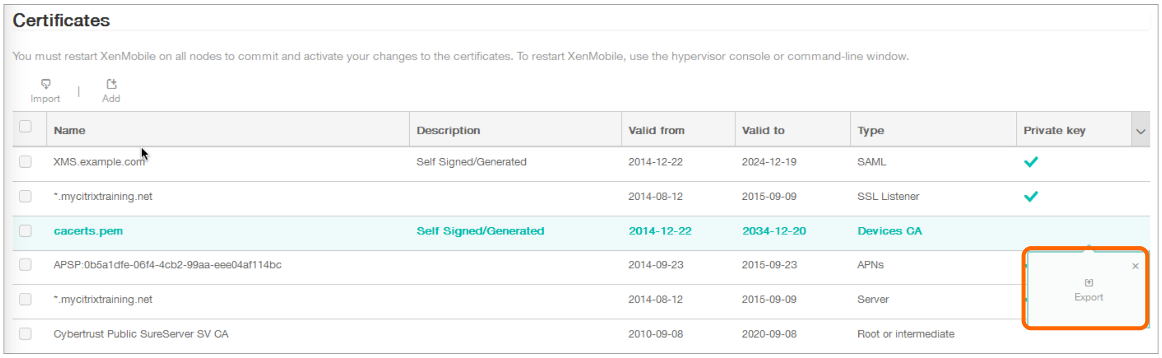
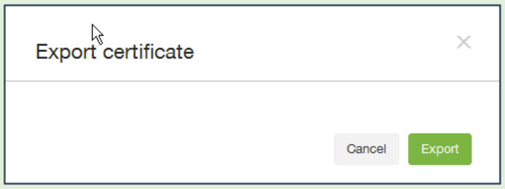
Step	Action
12.	Select the `wildcard.citrixtraining.lab` certificate for the load balancer SSL communication and click `Continue`.  Server Certificate for MAM Load Balacing A server certificate is used to authenticate and identify a server in an SSL handshake. A server certificate is issued ● Use existing certificate ○ Install Certificate Server Certificate* wildcard.mycitrixtraining.net Continue Do It Later
13.	Add the XenMobile Server to the load balancer and click `Continue`.  XenMobile Servers Add Server Remove Server IP Address *XenMobile Server IP Address is not configured. Please click on **Add Server** to configure.* Continue  XenMobile Server IP Addresses XenMobile Server IP Addresses Enter the IP address(es) of the XenMobile server(s) that you want to load balance. XenMobile Server IP Address* 192 . 168 . 10 . 20 Add Cancel  XenMobile Servers Add Server Remove Server IP Address 192.168.10.20 Continue

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>14.</td><td>Click <code>Load Balance Device Manager Servers</code>.

<b>XenMobile Servers</b>
IP Address
192.168.10.20
 </td></tr>
<tr><td>15.</td><td>The Load Balancing Virtual Server Configuration window comes up.
Configure the following settings:
<table><tr><td>IP Address*</td><td><code>192.168.10.101</code></td></tr><tr><td>Name*:</td><td><code>XenMobileMDM</code></td></tr></table>
Click <code>Continue</code>.

<b>Load Balancing Virtual Server Configuration</b>
Enter a public IP address and a name for the load balancing virtual server.
IP Address* 192 . 168 . 10 . 101
Name* XenMobileMDM
SSL Traffic Configuration
HTTP communication to XenMobile Server
 </td></tr>
<tr><td>16.</td><td>Select the existing certificate <code>wildcard.mycitrixtraining.net</code> and click <code>Continue</code>.

<b>Server Certificate</b>
A server certificate is used to authenticate and identify a server in an SSL handshake. A server cer
● Use existing certificate ○ Install Certificate
Server Certificate* wildcard.mycitrixtraining.net
 </td></tr>
</table>

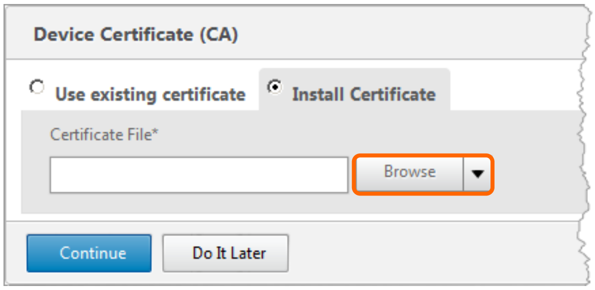
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>17.</td><td>For SSL Offload we need to install the <b>Device Certificate (CA)</b>, which can be exported from the XenMobile Server.

Open a new Tab in your browser; connect to https://192.168.10.20:4443 and login as administrator.

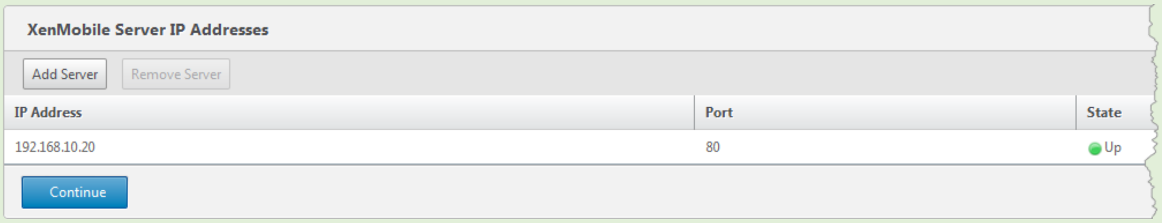
Navigate to <b>Configure -> Settings -> Certificates</b> and export the <code>cacerts.pem</code>.

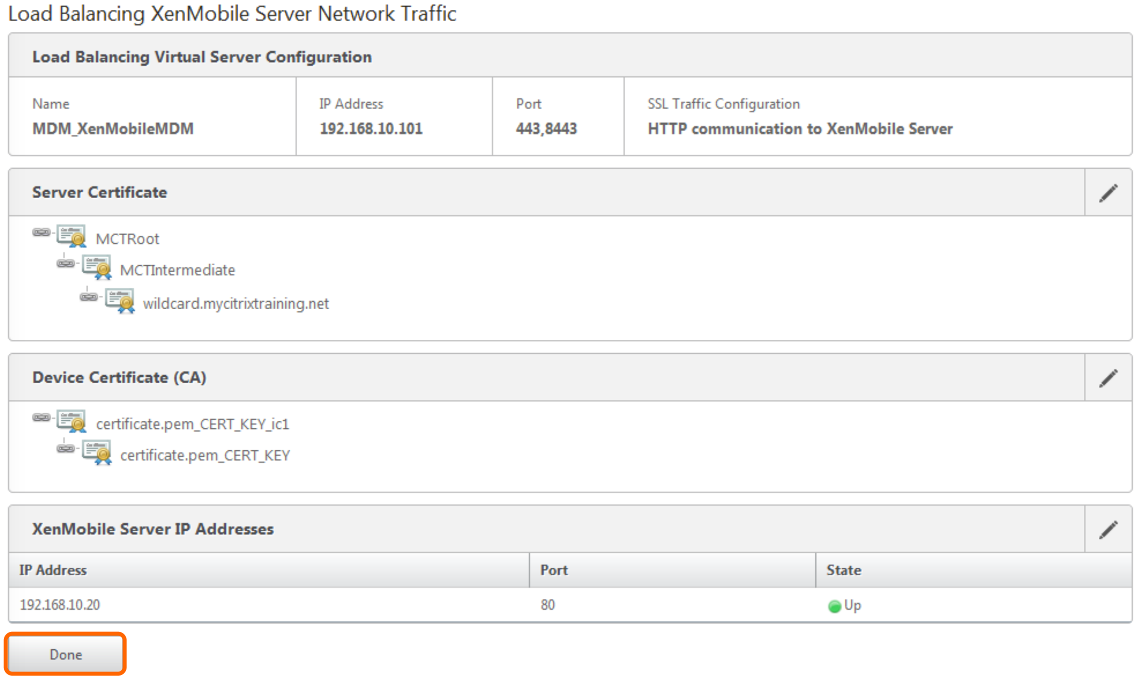

Certificates
You must restart XenMobile on all nodes to commit and activate your changes to the certificates. To restart XenMobile, use the hypervisor console or command-line window.
<table>
<tr><th>□</th><th>Name</th><th>Description</th><th>Valid from</th><th>Valid to</th><th>Type</th><th>Private key</th></tr>
<tr><td>□</td><td>XMS.example.com</td><td>Self Signed/Generated</td><td>2014-12-22</td><td>2024-12-19</td><td>SAML</td><td>✓</td></tr>
<tr><td>□</td><td>*.mycitrixtraining.net</td><td></td><td>2014-08-12</td><td>2015-09-09</td><td>SSL Listener</td><td>✓</td></tr>
<tr><td>□</td><td>cacerts.pem</td><td>Self Signed/Generated</td><td>2014-12-22</td><td>2034-12-20</td><td>Devices CA</td><td></td></tr>
<tr><td>□</td><td>APSP:0b5a1dfe-06f4-4cb2-99aa-eee04af114bc</td><td></td><td>2014-09-23</td><td>2015-09-23</td><td>APNs</td><td></td></tr>
<tr><td>□</td><td>*.mycitrixtraining.net</td><td></td><td>2014-08-12</td><td>2015-09-09</td><td>Server</td><td></td></tr>
<tr><td>□</td><td>Cybertrust Public SureServer SV CA</td><td></td><td>2010-09-08</td><td>2020-09-08</td><td>Root or intermediate</td><td></td></tr>
</table>
</td></tr>
<tr><td>18.</td><td>
Export certificate

Click on <code>Export</code> and save the file.</td></tr>
<tr><td>19.</td><td>Back on the NetScaler GUI Tab, click <code>Browse</code> and install the <code>certificate.pem</code> file you downloaded in the previous step.

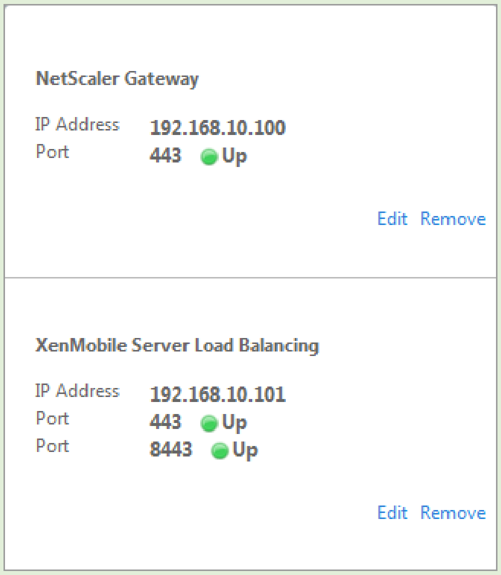
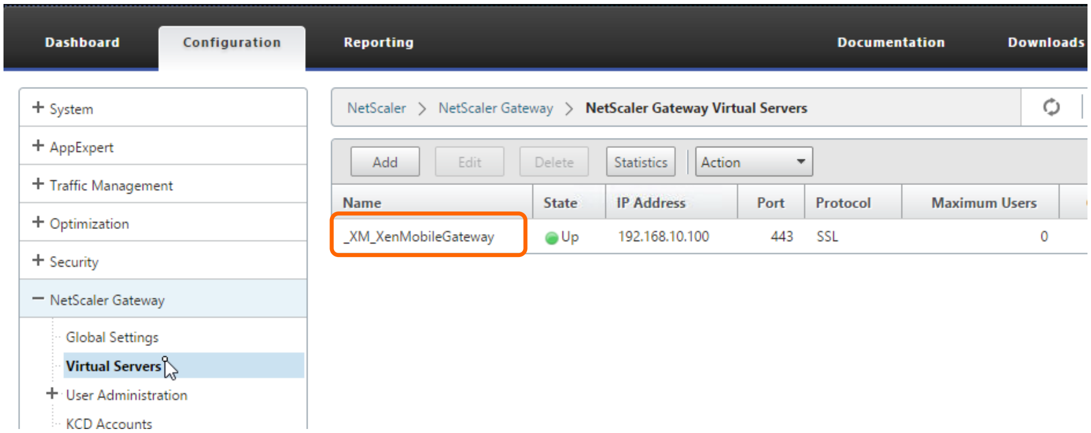
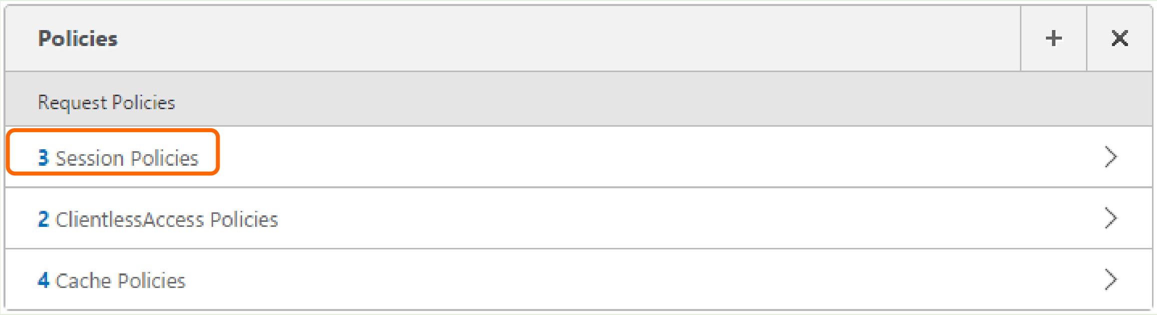

Device Certificate (CA)
○ Use existing certificate ● Install Certificate
Certificate File*

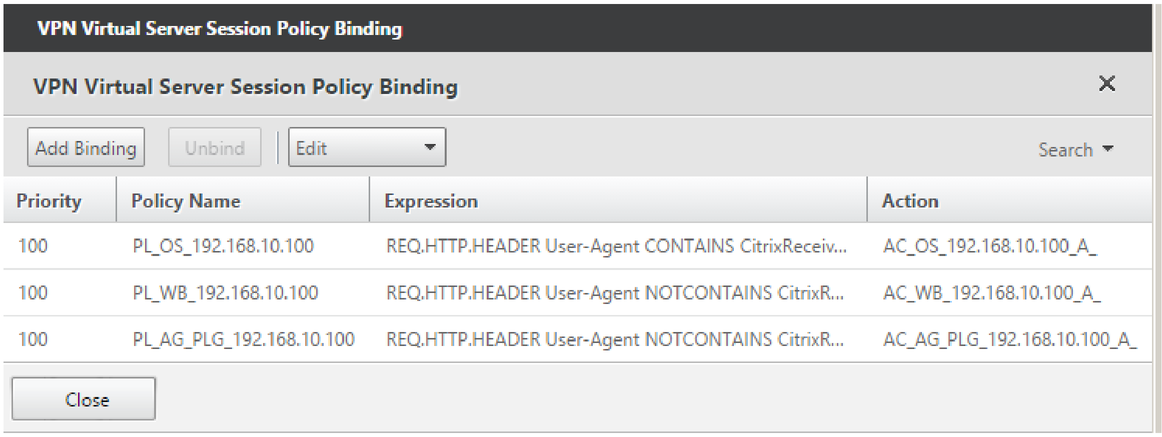
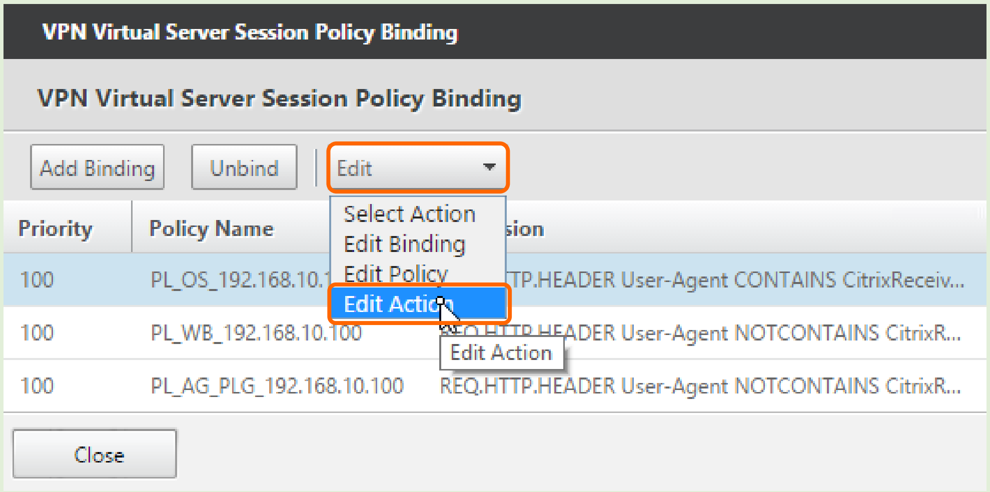
Click <code>Continue</code>.</td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>20.</td><td>The XenMobile Server should be “known” from the first part when configuring the MAM load balancer.


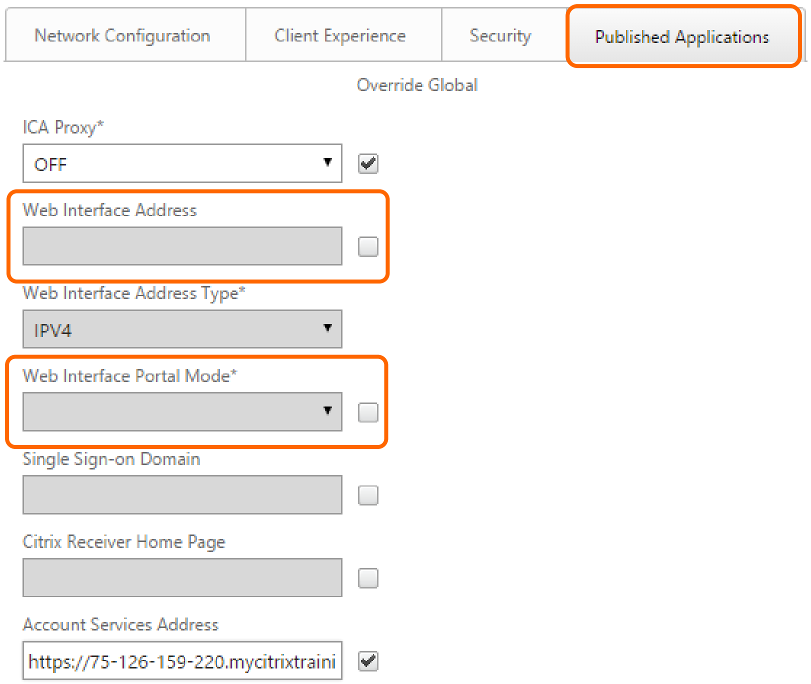
<b>XenMobile Server IP Addresses</b>
<table>
<tr><th>IP Address</th><th>Port</th><th>State</th></tr>
<tr><td>192.168.10.20</td><td>80</td><td>● Up</td></tr>
</table>
If not you may us the <b>Add Server</b> button and add <b>SITE1-XMS1</b> (192.168.10.20).
Click <code>Continue</code>.</td></tr>
<tr><td>21.</td><td>You can review / edit the configuration before exiting the wizard.


Load Balancing XenMobile Server Network Traffic
<b>Load Balancing Virtual Server Configuration</b>
<table>
<tr><th>Name</th><th>IP Address</th><th>Port</th><th>SSL Traffic Configuration</th></tr>
<tr><td>MDM_XenMobileMDM</td><td>192.168.10.101</td><td>443,8443</td><td>HTTP communication to XenMobile Server</td></tr>
</table>
<b>Server Certificate</b>
MCTRoot
MCTIntermediate
wildcard.mycitrixtraining.net
<b>Device Certificate (CA)</b>
certificate.pem_CERT_KEY_ic1
certificate.pem_CERT_KEY
<b>XenMobile Server IP Addresses</b>
<table>
<tr><th>IP Address</th><th>Port</th><th>State</th></tr>
<tr><td>192.168.10.20</td><td>80</td><td>● Up</td></tr>
</table>
Click <code>Done</code>.</td></tr>
</table>

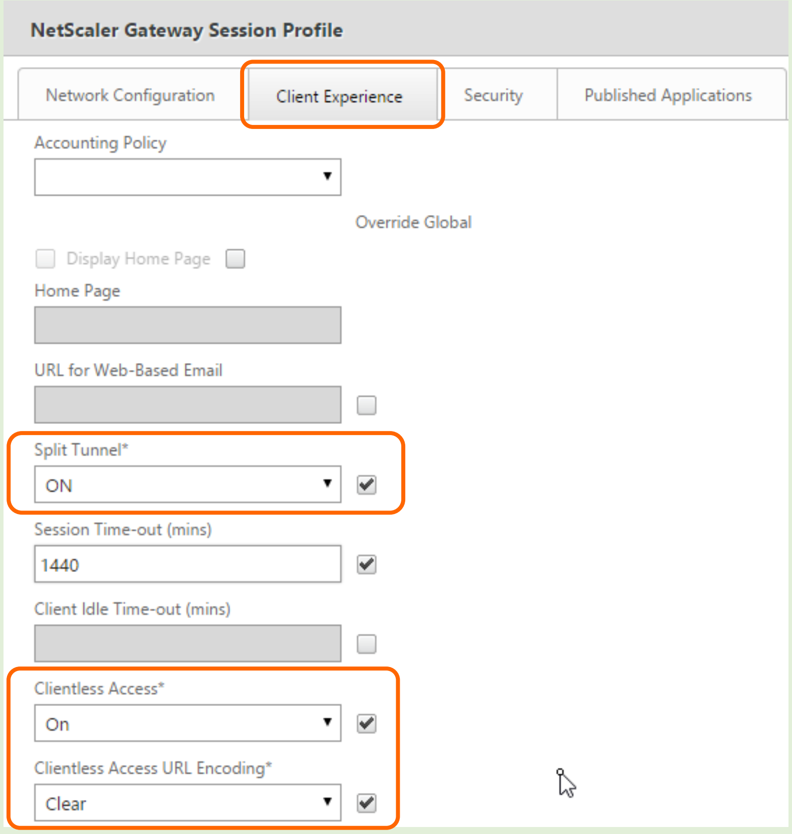
Step	Action
22.	NetScaler Gateway and XenMobile Server Load Balancing should be reported as “up”.  NetScaler Gateway IP Address 192.168.10.100 Port 443 ● Up Edit Remove XenMobile Server Load Balancing IP Address 192.168.10.101 Port 443 ● Up Port 8443 ● Up Edit Remove
23.	Navigate to **NetScaler Gateway > Virtual Servers** and double-click the **`_XM_XenMobileGateway`** virtual server.  Dashboard Configuration Reporting Documentation Downloads + System + AppExpert + Traffic Management + Optimization + Security − NetScaler Gateway Global Settings Virtual Servers + User Administration KCD Accounts NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers Add Edit Delete Statistics Action Name: _XM_XenMobileGateway; State: ● Up; IP Address: 192.168.10.100; Port: 443; Protocol: SSL; Maximum Users: 0
24.	Scroll down to the **Policies** section. Click on **`Session Policies`**.  Policies + ✕ Request Policies 3 Session Policies > 2 ClientlessAccess Policies > 4 Cache Policies >

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>25.</td><td>Notice that the wizard has created all session policies and profiles.

VPN Virtual Server Session Policy Binding
VPN Virtual Server Session Policy Binding
×
Add Binding
Unbind
Edit
Search
Close
<table>
<tr><th>Priority</th><th>Policy Name</th><th>Expression</th><th>Action</th></tr>
<tr><td>100</td><td>PL_OS_192.168.10.100</td><td>REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiv...</td><td>AC_OS_192.168.10.100_A_</td></tr>
<tr><td>100</td><td>PL_WB_192.168.10.100</td><td>REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixR...</td><td>AC_WB_192.168.10.100_A_</td></tr>
<tr><td>100</td><td>PL_AG_PLG_192.168.10.100</td><td>REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixR...</td><td>AC_AG_PLG_192.168.10.100_A_</td></tr>
</table>
</td></tr>
<tr><td>26.</td><td>Select the <code>PL_OS_192.168.10.100</code> policy and click <code>Edit &gt; Edit Action</code>.


<table>
<tr><th>Priority</th><th>Policy Name</th><th>sion</th></tr>
<tr><td>100</td><td>PL_OS_192.168.10.1</td><td>TP.HEADER User-Agent CONTAINS CitrixReceiv...</td></tr>
<tr><td>100</td><td>PL_WB_192.168.10.100</td><td>REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixR...</td></tr>
<tr><td>100</td><td>PL_AG_PLG_192.168.10.100</td><td>REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixR...</td></tr>
</table>
</td></tr>
</table>

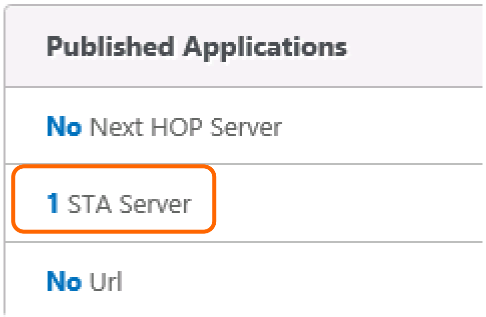
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>27.</td><td>Select the <b>Published Applications</b> tab and configure the following settings:
<table>
<tr><td>Web Interface address</td><td><b>Unchecked</b> (The field should be blank)</td></tr>
<tr><td>Single Sign-on Domain</td><td><b>Unchecked</b> (The field should be blank)</td></tr>
</table>


Override Global
ICA Proxy* OFF ☑
Web Interface Address ☐
Web Interface Address Type* IPV4
Web Interface Portal Mode* ☐
Single Sign-on Domain ☐
Citrix Receiver Home Page ☐
Account Services Address https://75-126-159-220.mycitrixtraini ☑
</td></tr>
</table>

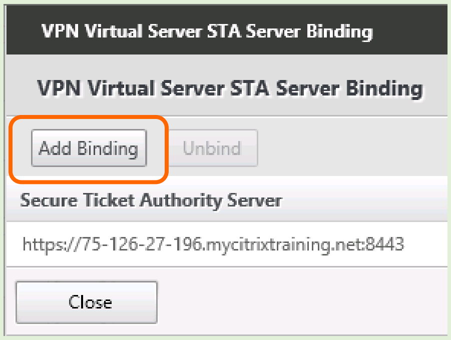
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>28.</td><td>Select the <b>Client Experience</b> tab and configure the following settings:
<table>
<tr><td>Split Tunnel*</td><td><code>On</code></td></tr>
<tr><td>Clientless Access*</td><td><code>On</code></td></tr>
<tr><td>Clientless Access URL Encoding*</td><td><code>Clear</code></td></tr>
<tr><td>Single Sign-on to Web Applications</td><td><code>Checked</code></td></tr>
</table>


Accounting Policy
□ Display Home Page □
Home Page
URL for Web-Based Email □
Split Tunnel* ON ☑
Session Time-out (mins) 1440 ☑
Client Idle Time-out (mins) □
Clientless Access* On ☑
Clientless Access URL Encoding* Clear ☑
</td></tr>
<tr><td>29.</td><td>Scroll down and click <code>OK</code> to close the session profile.</td></tr>
<tr><td>30.</td><td>Click <code>Close.</code>
<b>Note:</b> If you do not intend to integrate with XenDesktop (Optional Exercise 1), then skip to <b>Step 35.</b></td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>31.</td><td>Scroll down to the <b>Published Applications</b> section and click <code>1 STA Server.</code>

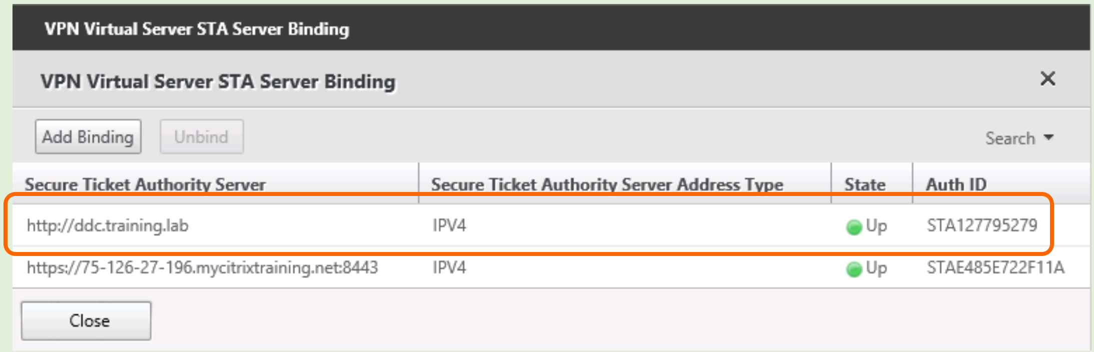


Published Applications
No Next HOP Server
1 STA Server
No Url</td></tr>
<tr><td>32.</td><td>Click <code>Add Binding</code>.



VPN Virtual Server STA Server Binding
VPN Virtual Server STA Server Binding
Add Binding Unbind
Secure Ticket Authority Server
https://75-126-27-196.mycitrixtraining.net:8443
Close</td></tr>
<tr><td>33.</td><td>Configure the STA with the following settings:
<table>
<tr><td>Secure Ticket Authority Server:</td><td><code>http://ddc.training.lab</code></td></tr>
<tr><td>Securit Ticket Authority Server Address Type:</td><td><code>IPV4</code></td></tr>
</table></td></tr>
<tr><td>34.</td><td>Click <code>Bind</code>. The STA server is added and has a status of <b>UP</b>.

Click <code>Close</code>.

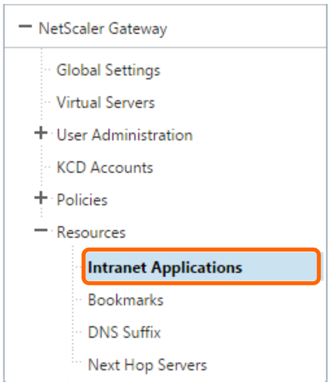


VPN Virtual Server STA Server Binding
VPN Virtual Server STA Server Binding ✕
Add Binding Unbind Search ▾
<table>
<tr><th>Secure Ticket Authority Server</th><th>Secure Ticket Authority Server Address Type</th><th>State</th><th>Auth ID</th></tr>
<tr><td>http://ddc.training.lab</td><td>IPV4</td><td>● Up</td><td>STA127795279</td></tr>
<tr><td>https://75-126-27-196.mycitrixtraining.net:8443</td><td>IPV4</td><td>● Up</td><td>STAE485E722F11A</td></tr>
</table>
Close</td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>35.</td><td>

Click **Back** to close the **Policy Binding** window.

Navigate to **NetScaler Gateway > Resources > Intranet Applications** and click **Add**.

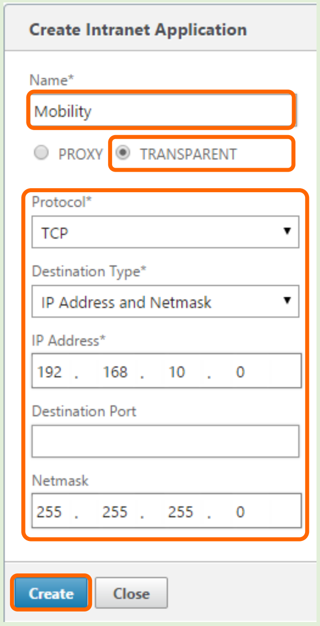


</td></tr>
<tr><td>36.</td><td>

Enter the following Intranet Application settings:

<table>
<tr><td>Name*</td><td><b>Mobility</b></td></tr>
<tr><td>Mode*</td><td><b>Transparent</b></td></tr>
<tr><td>Protocol*</td><td><b>TCP</b> (Accept the default)</td></tr>
<tr><td>Destination Type</td><td><b>IP Address and Netmask</b> (Accept the default)</td></tr>
<tr><td>IP Address*</td><td><b>192.168.10.0</b></td></tr>
<tr><td>Netmask</td><td><b>255.255.255.0</b></td></tr>
</table>

Click **Create**.



Create Intranet Application

Name*: Mobility

○ PROXY ● TRANSPARENT

Protocol*: TCP

Destination Type*: IP Address and Netmask

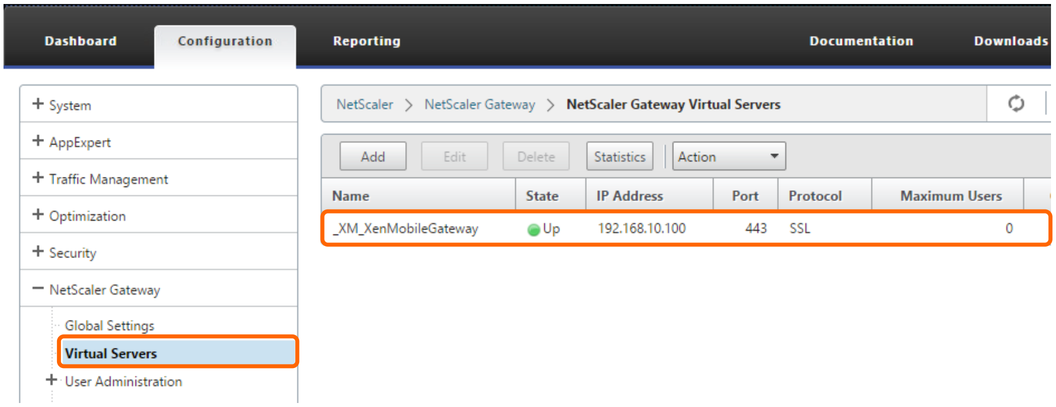
IP Address*: 192 . 168 . 10 . 0

Destination Port:

Netmask: 255 . 255 . 255 . 0

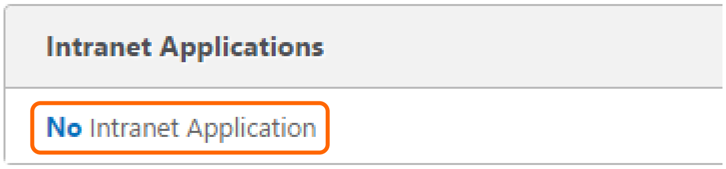
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>37.</td><td>
Navigate to <b>NetScaler Gateway > Virtual Servers</b> and double-click the <code>_XM_XenMobileGateway</code> virtual server.

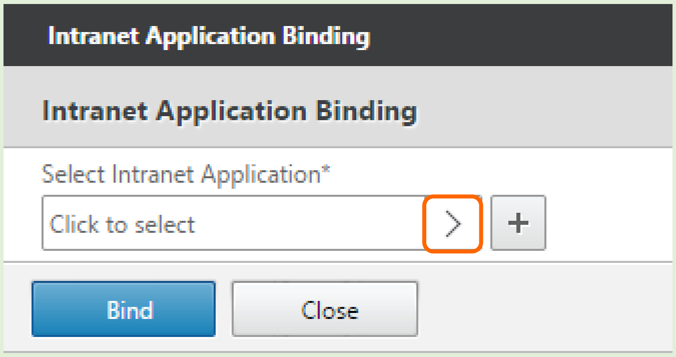


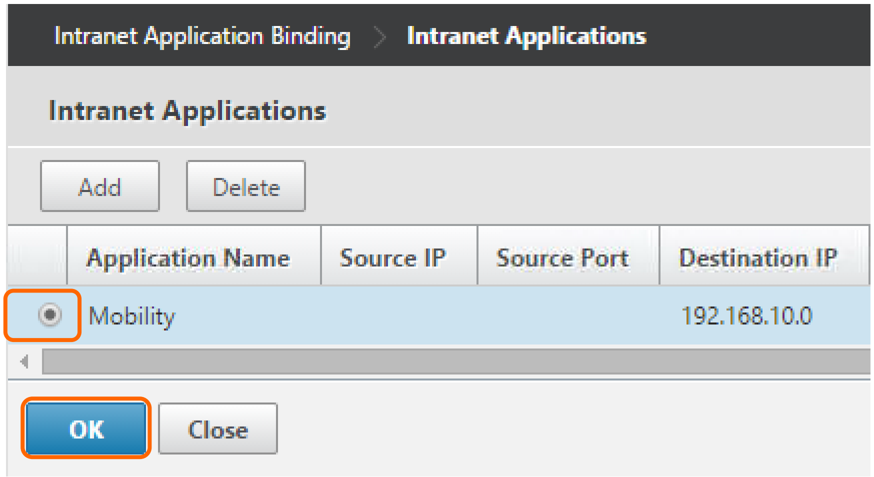
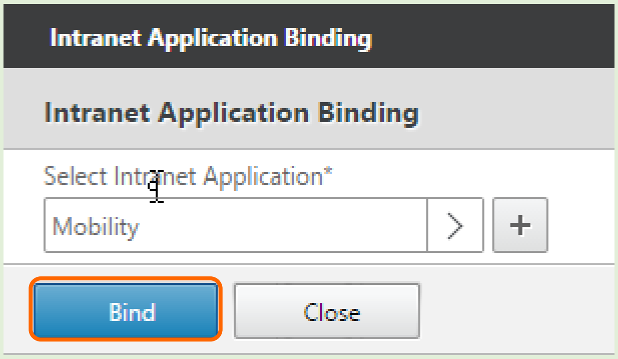
<table>
<tr><th>Name</th><th>State</th><th>IP Address</th><th>Port</th><th>Protocol</th><th>Maximum Users</th></tr>
<tr><td>_XM_XenMobileGateway</td><td>● Up</td><td>192.168.10.100</td><td>443</td><td>SSL</td><td>0</td></tr>
</table>
</td></tr>
<tr><td>38.</td><td>Under the <b>Advanced</b> section on the right, click the <b>“+”</b> next to <b>Intranet Applications</b>.</td></tr>
<tr><td>39.</td><td>
Scroll down to the <b>Intranet Applications</b> section.

Click <code>Intranet Application</code>.



</td></tr>
<tr><td>40.</td><td>
Click the <code>“&gt;”.</code>


Intranet Application Binding
Intranet Application Binding
Select Intranet Application*
Click to select
>
+
Bind
Close
</td></tr>
</table>

Step	Action
41.	Click the radio button next to the **Mobility** intranet application. Click OK.  Intranet Application Binding > Intranet Applications Intranet Applications Add Delete Application Name Source IP Source Port Destination IP ● Mobility 192.168.10.0 OK Close
42.	Click **Bind**.  Intranet Application Binding Intranet Application Binding Select Intranet Application* Mobility
43.	The **Mobility** intranet application is now bound to the **_XM_XenMobileGateway** virtual server. **Note:** A best practice is to save the running configuration after making changes. This prevents loss of configuration in the event the NetScaler is rebooted.

Exercise Summary

In this exercise, you used the wizard to configure NetScaler Gateway to connect to an enterprise store. The wizard created the virtual server as well as the authentication and session policies. The wizard is designed to simplify configuration for the administrator so that manual configuration of the policies is avoided.

Exercise 7

Device Enrollment

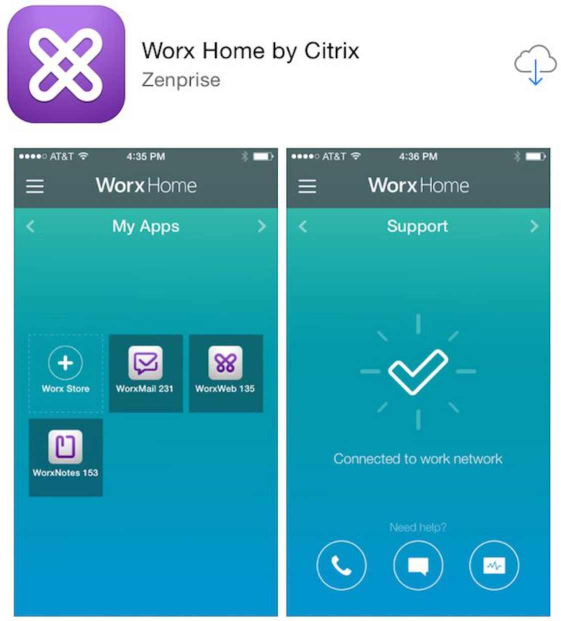
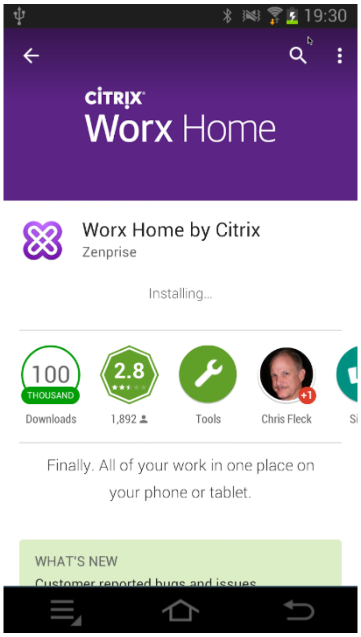
Overview

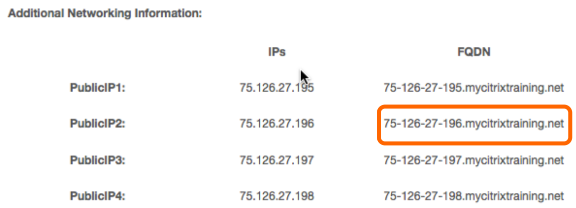
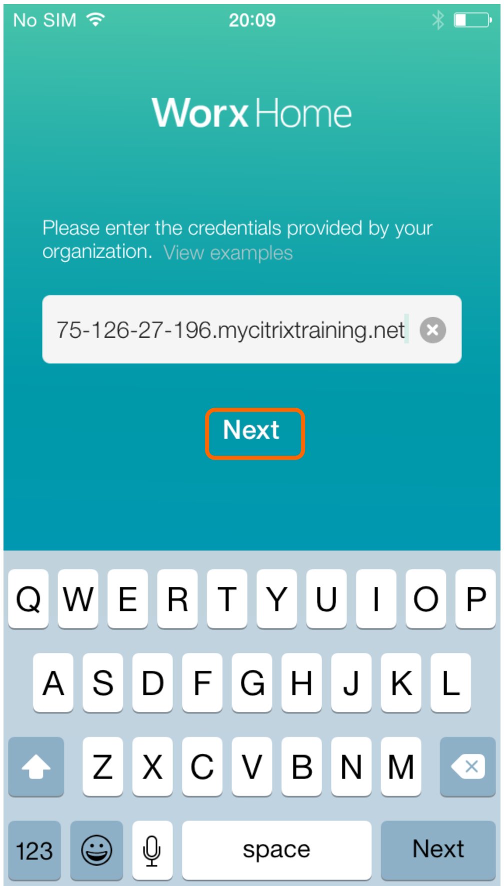
In order for XenMobile Server to manage mobile devices, the WorxHome client must be installed and configured on the endpoint device. In this exercise, you will install WorxHome and configure the XenMobile Server IP address that the device should connect to for enrollment.

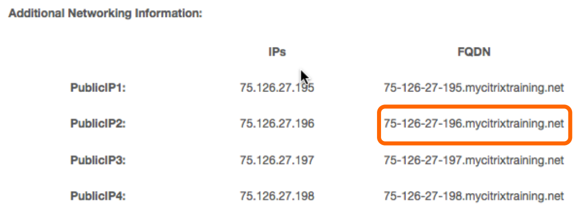
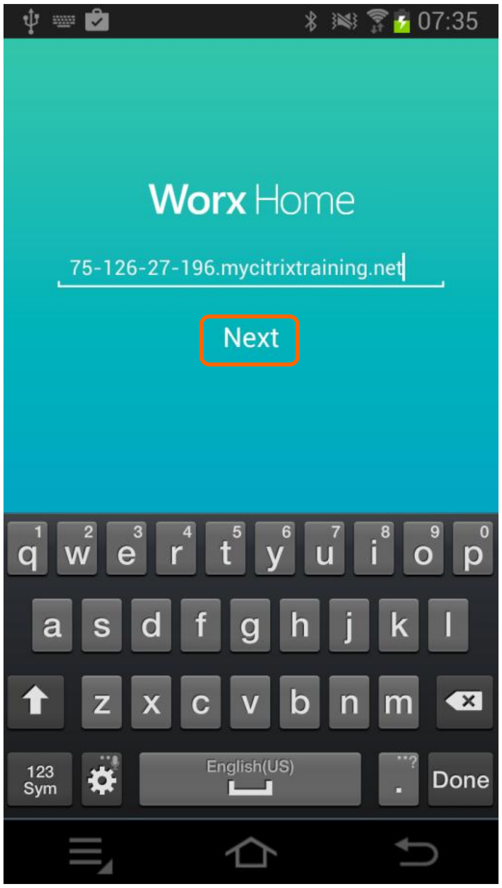
Note: If your device is enrolled with another MDM solution, the enrollment will fail. To continue, you must un-enroll from your existing MDM solution.

Step by step guidance

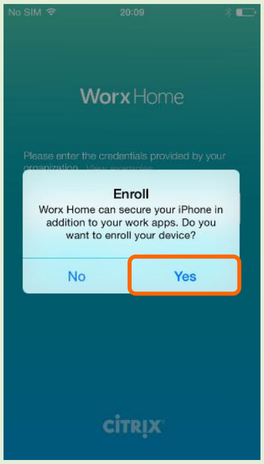
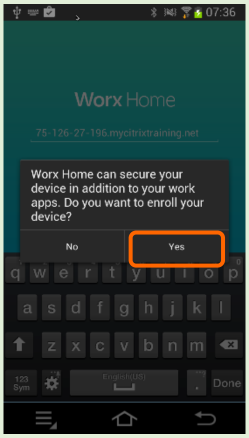
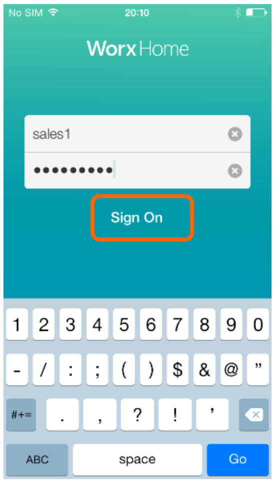
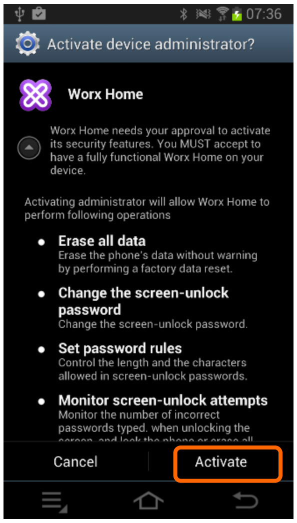
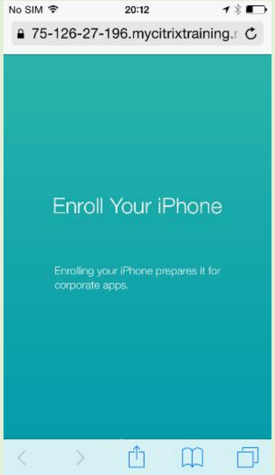
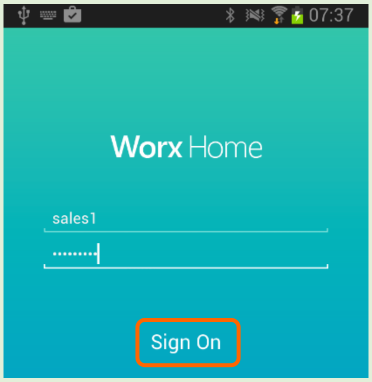
Estimated time to complete this lab: **7** minutes.

Step	iOS	Android
1.	Download and install **WorxHome** from the Apple App Store.  Worx Home by Citrix Zenprise AT&T 4:35 PM Worx Home My Apps Worx Store WorxMail 231 WorxWeb 135 WorxNotes 153 AT&T 4:36 PM Worx Home Support Connected to work network Need help?	Download and install WorxHome from the Google Play Store.  19:30 CiTRiX Worx Home Worx Home by Citrix Zenprise Installing... 100 THOUSAND Downloads 2.8 1,892 Tools Chris Fleck Finally. All of your work in one place on your phone or tablet. WHAT'S NEW Customer reported bugs and issues
2.	After installation is complete, launch the **WorxHome** application.	After installation is complete, launch the **WorxHome** application.

<table>
<tr>
<td>3.</td>
<td>
You are prompted for the server URL, UPN or e-mail address.
Enter the <b>IP2 FQDN</b>
Your IP2 FQDN is available from the portal page.
<b>Example Only</b>:
75-126-27-196.mycitrixtraining.net

Additional Networking Information:
<table>
<tr><th></th><th>IPs</th><th>FQDN</th></tr>
<tr><td>PublicIP1:</td><td>75.126.27.195</td><td>75-126-27-195.mycitrixtraining.net</td></tr>
<tr><td>PublicIP2:</td><td>75.126.27.196</td><td>75-126-27-196.mycitrixtraining.net</td></tr>
<tr><td>PublicIP3:</td><td>75.126.27.197</td><td>75-126-27-197.mycitrixtraining.net</td></tr>
<tr><td>PublicIP4:</td><td>75.126.27.198</td><td>75-126-27-198.mycitrixtraining.net</td></tr>
</table>
Tap <b>Next</b>.

Worx Home
Please enter the credentials provided by your organization. View examples
75-126-27-196.mycitrixtraining.net
Next

</td>
<td>
You are prompted for the server URL, UPN or e-mail address.
Enter the <b>IP2 FQDN</b>
Your IP2 FQDN is available from the portal page.
<b>Example Only</b>:
75-126-27-196.mycitrixtraining.net

Additional Networking Information:
<table>
<tr><th></th><th>IPs</th><th>FQDN</th></tr>
<tr><td>PublicIP1:</td><td>75.126.27.195</td><td>75-126-27-195.mycitrixtraining.net</td></tr>
<tr><td>PublicIP2:</td><td>75.126.27.196</td><td>75-126-27-196.mycitrixtraining.net</td></tr>
<tr><td>PublicIP3:</td><td>75.126.27.197</td><td>75-126-27-197.mycitrixtraining.net</td></tr>
<tr><td>PublicIP4:</td><td>75.126.27.198</td><td>75-126-27-198.mycitrixtraining.net</td></tr>
</table>
Tap <b>Next</b>.

Worx Home
75-126-27-196.mycitrixtraining.net
Next

</td>
</tr>
</table>

4.	Tab **Yes** to enroll your device.  Please enter the credentials provided by your organization. **Enroll** Worx Home can secure your iPhone in addition to your work apps. Do you want to enroll your device? No Yes	Tab **Yes** to enroll your device.  75-126-27-196.mycitrixtraining.net Worx Home can secure your device in addition to your work apps. Do you want to enroll your device? No Yes
5.	Enter the user credentials. Username: **`sales1`** Password: **`Citrix123`** Tap **`Sign On`**.  sales1 ••••••••• Sign On	You are prompted to activate the Device Administrator. Tap **`Activate`**.  Activate device administrator? **Worx Home** Worx Home needs your approval to activate its security features. You MUST accept to have a fully functional Worx Home on your device. Activating administrator will allow Worx Home to perform following operations • **Erase all data** Erase the phone's data without warning by performing a factory data reset. • **Change the screen-unlock password** Change the screen-unlock password. • **Set password rules** Control the length and the characters allowed in screen-unlock passwords. • **Monitor screen-unlock attempts** Monitor the number of incorrect passwords typed. when unlocking the screen, and lock the phone or erase all Cancel Activate
6.	A browser message **"Enroll Your iPhone/iPad"** will appear.  75-126-27-196.mycitrixtraining. Enroll Your iPhone Enrolling your iPhone prepares it for corporate apps.	Enter the user credentials. Username: **`sales1`** Password: **`Citrix123`** Tap **`Sign On`**.  sales1 ••••••••• Sign On

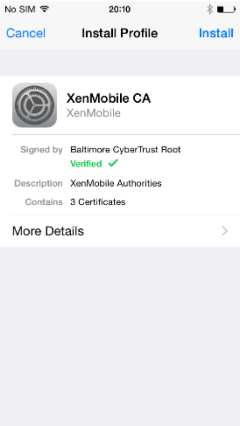
7.

In the following steps the device will be prepared for corporate usage.

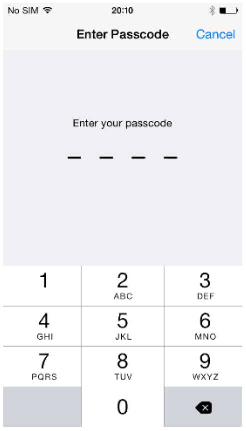
You will go through the tasks to install the following profiles:

- XenMobile CA
- XenMobile Profile Service
- MDM Configuration

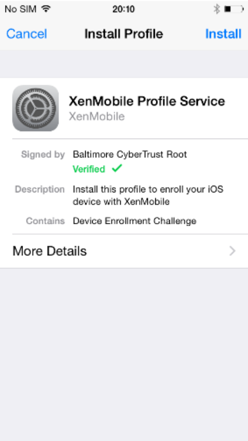
For each of these you need to confirm the installation, enter the device PIN and confirm you trust the management.



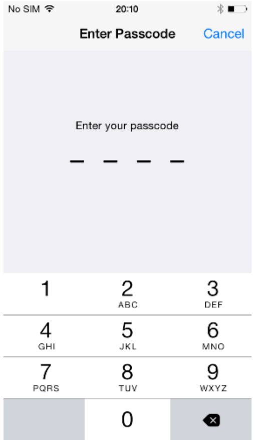
XenMobile CA
XenMobile
Signed by Baltimore CyberTrust Root
Verified ✓
Description XenMobile Authorities
Contains 3 Certificates
More Details



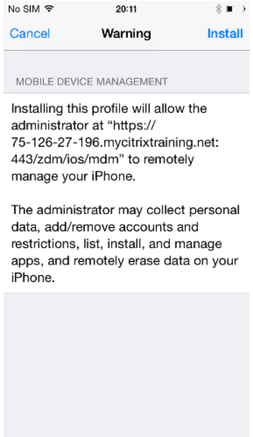
Enter your passcode



XenMobile Profile Service
XenMobile
Signed by Baltimore CyberTrust Root
Verified ✓
Description Install this profile to enroll your iOS device with XenMobile
Contains Device Enrollment Challenge
More Details



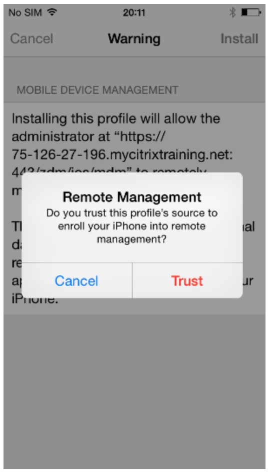
Enter your passcode



MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at "https://75-126-27-196.mycitrixtraining.net:443/zdm/ios/mdm" to remotely manage your iPhone.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPhone.



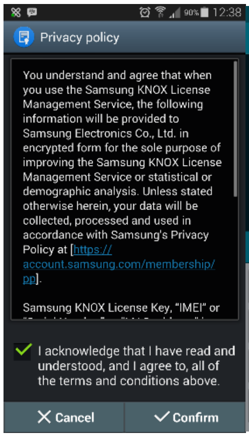
MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at "https://75-126-27-196.mycitrixtraining.net:

Remote Management
Do you trust this profile's source to enroll your iPhone into remote management?
Cancel Trust

WorxHome has enrolled your device against the MDM service and will SSO to the MAM instance (Authenticating).

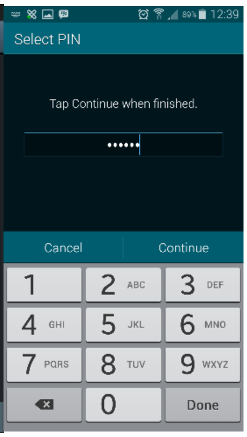
If using a Samsung SAFE capable device you will be asked to accept the terms and conditions and enter your current PIN code to confirm



You understand and agree that when you use the Samsung KNOX License Management Service, the following information will be provided to Samsung Electronics Co., Ltd. in encrypted form for the sole purpose of improving the Samsung KNOX License Management Service or statistical or demographic analysis. Unless stated otherwise herein, your data will be collected, processed and used in accordance with Samsung's Privacy Policy at [https://account.samsung.com/membership/pp].

Samsung KNOX License Key, "IMEI" or

☑ I acknowledge that I have read and understood, and I agree to, all of the terms and conditions above.

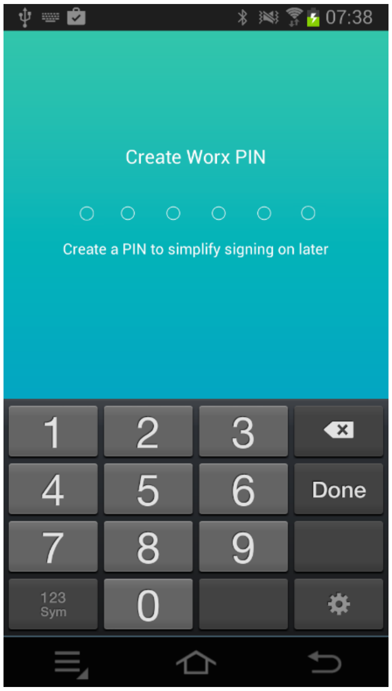


Tap Continue when finished.

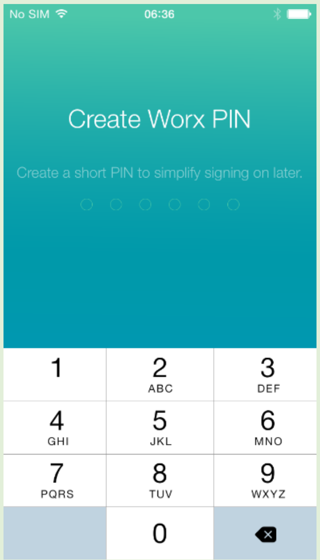
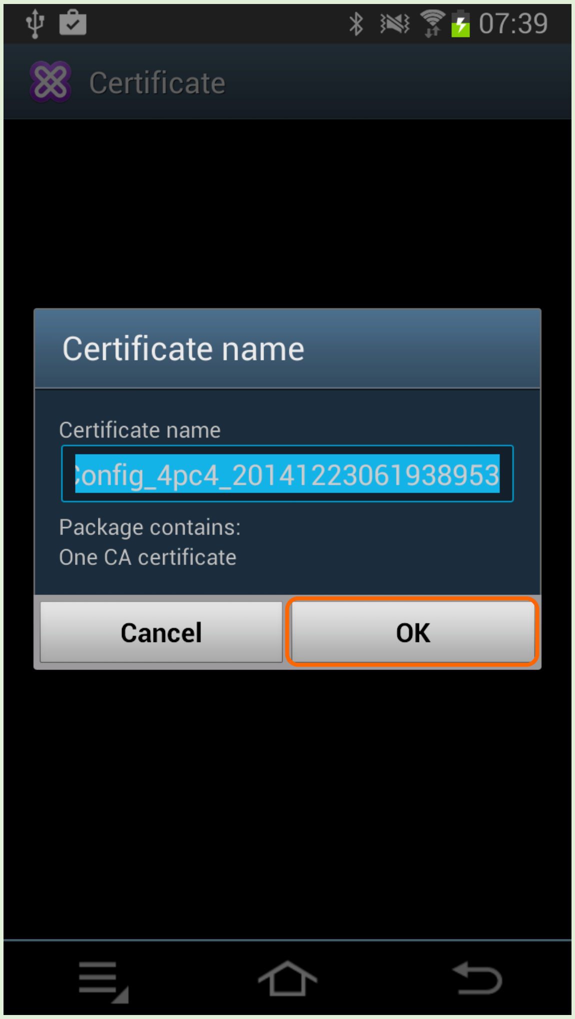
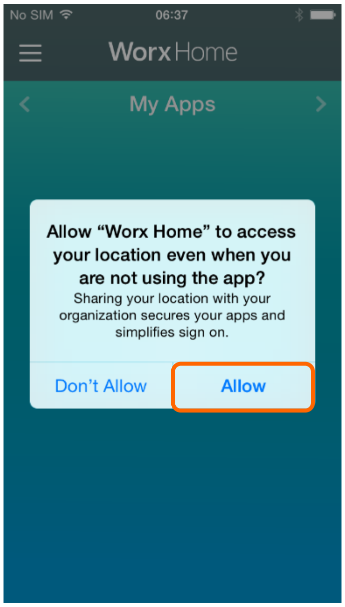
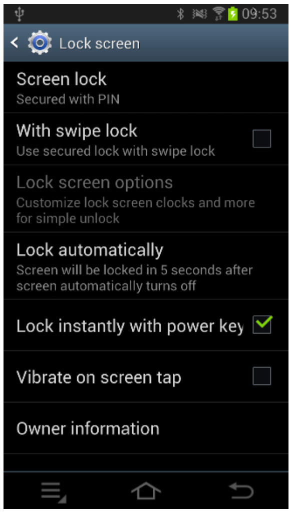
If your PIN code does not meet the new requirements, enter and confirm a 6-digit PIN code.

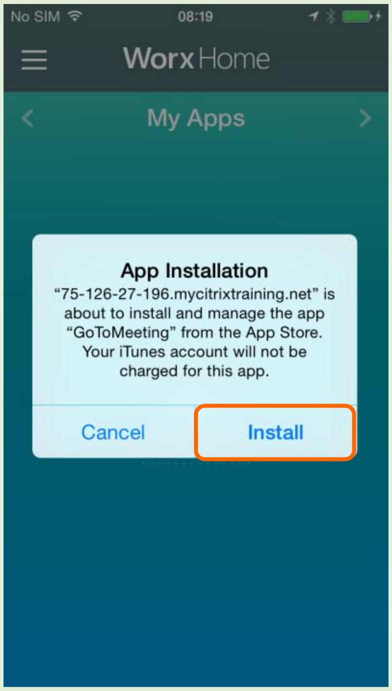
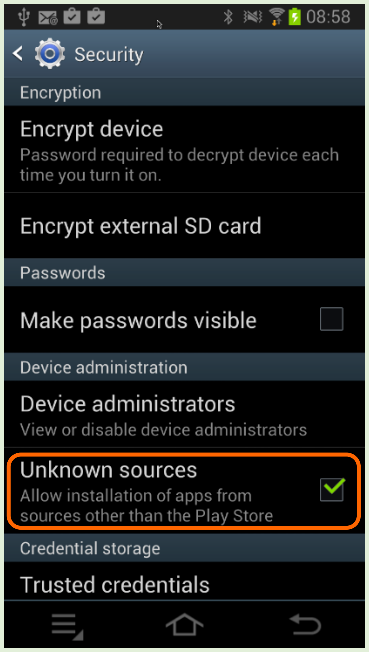
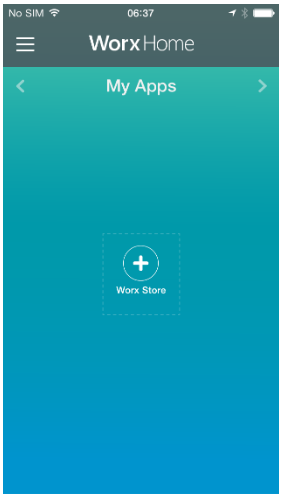
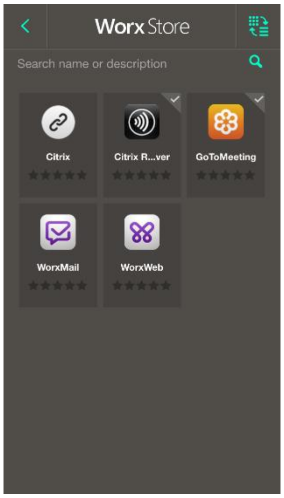
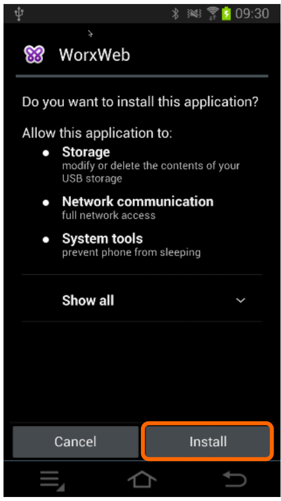
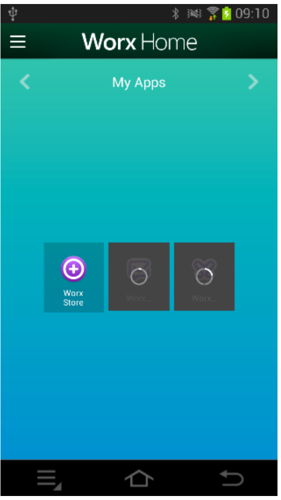
WorxHome will ask for a PIN code, which was defined as **Client Properties** in the XenMobile Server configuration.

Note: Your PIN can not be consecutive numbers. (IE:123456).



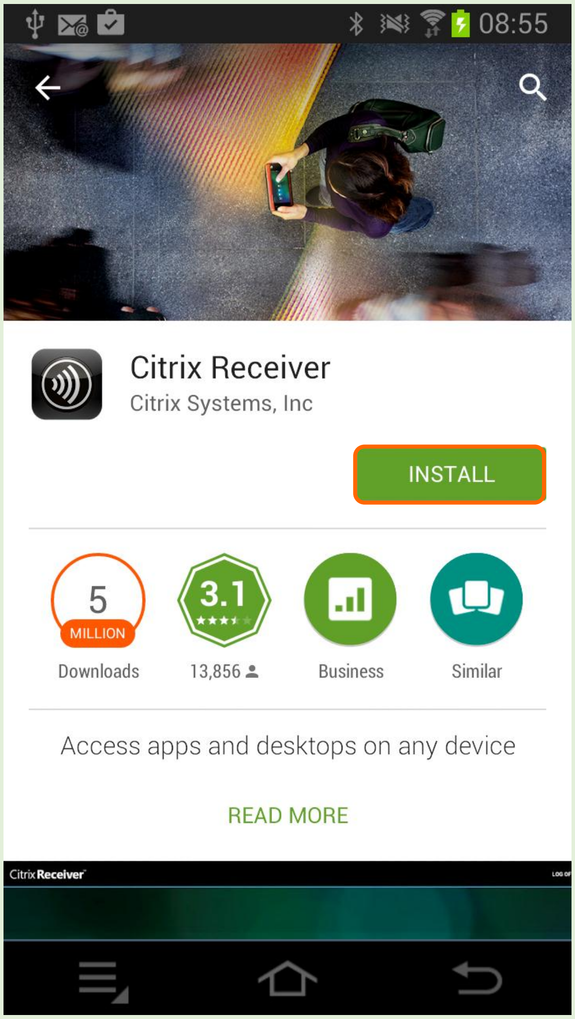
Create a PIN to simplify signing on later

8.	WorxHome has enrolled your device against the MDM service and will SSO to the MAM instance (Authenticating). WorxHome will ask for a PIN code, which was defined as **Client Properties** in the XenMobile Server configuration. **Note:** Your PIN can not be consecutive numbers. (IE:123456).  No SIM 06:36 Create Worx PIN Create a short PIN to simplify signing on later. Enter and confirm your 6-digit PIN code.	Click **OK** to install the CA certificate.  07:39 Certificate Certificate name Certificate name config_4pc4_20141223061938953 Package contains: One CA certificate
9.	You need to confirm, that WorxHome is allowed to use the devices location service.  No SIM 06:37 Allow "Worx Home" to access your location even when you are not using the app? Sharing your location with your organization secures your apps and simplifies sign on. 	If you do not have screen lock configured, you are prompted to configure your screen lock settings. Specify a PIN in the settings.  09:53 Lock screen Screen lock Secured with PIN With swipe lock □ Use secured lock with swipe lock Lock screen options Customize lock screen clocks and more for simple unlock Lock automatically Screen will be locked in 5 seconds after screen automatically turns off Lock instantly with power key ☑ Vibrate on screen tap □ Owner information

10.	Depending on your current settings and installed apps you'll be requested to: • Enter a passcode (passcode policy) • Confirm app install (mandatory apps) • Enter App Store password (public apps)  No SIM 08:19 Worx Home My Apps **App Installation** "75-126-27-196.mycitrixtraining.net" is about to install and manage the app "GoToMeeting" from the App Store. Your iTunes account will not be charged for this app. Cancel Install	**Note:** Some Android devices require you to allow installation of apps from unknown sources before WorxWeb and WorxMail can be installed. This is done in `Settings >Security > Unknown Sources.`  08:58 Security Encryption Encrypt device Password required to decrypt device each time you turn it on. Encrypt external SD card Passwords Make passwords visible ☐ Device administration Device administrators View or disable device administrators Unknown sources ☑ Allow installation of apps from sources other than the Play Store Credential storage Trusted credentials
11.	Tab on the `+ Worx Store` icon to access the enterprise store.  No SIM 06:37 Worx Home My Apps Worx Store  Worx Store Search name or description Citrix Citrix R...ver GoToMeeting WorxMail WorxWeb	Mandatory MDX Apps will be pushed automatically after you confirmed.  09:30 WorxWeb Do you want to install this application? Allow this application to: • **Storage** modify or delete the contents of your USB storage • **Network communication** full network access • **System tools** prevent phone from sleeping Show all Cancel Install  09:10 Worx Home My Apps Worx Store

<table>
<tr><td>12.</td><td></td><td>You are taken to the Google Play store to install “public app store apps” such as <strong>Citrix Receiver</strong>.

Tap <strong>Install > Accept.</strong>



08:55
Citrix Receiver
Citrix Systems, Inc
INSTALL
5
MILLION
Downloads
3.1
13,856
Business
Similar
Access apps and desktops on any device
READ MORE
Citrix Receiver

<strong>Note:</strong> Order of application installs may vary. You may have to logoff/login in order for applications to download.</td></tr>
<tr><td>13.</td><td colspan="2">All installed applications are accessible on your springboard.</td></tr>
</table>

Exercise Summary

In this exercise, you have now enrolled your iOS or Android device. You also successfully pushed mobile applications to your mobile device. Only after the device is successfully enrolled can it be managed by policies on the XenMobile Server.

Optional Exercise 1

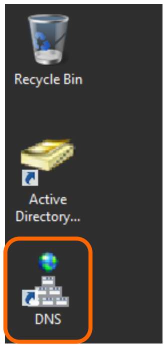
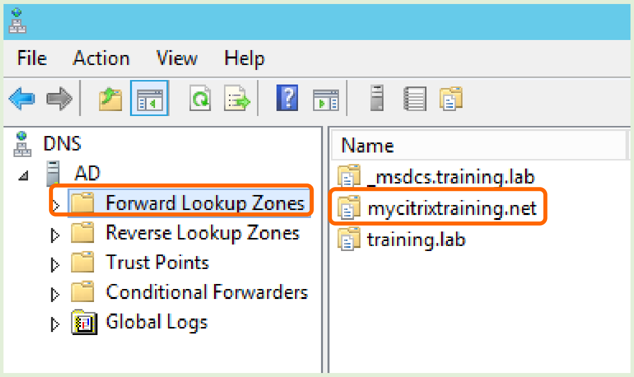
XenMobile Server Integration with XenDesktop

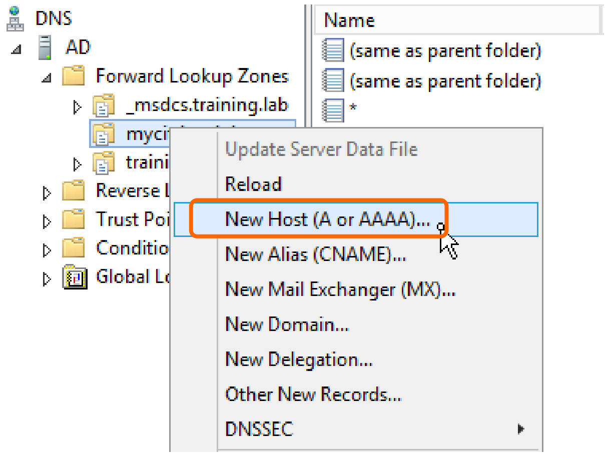
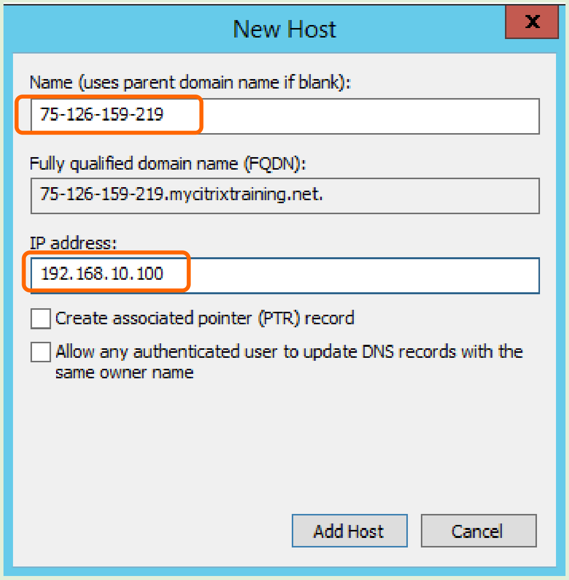
Overview

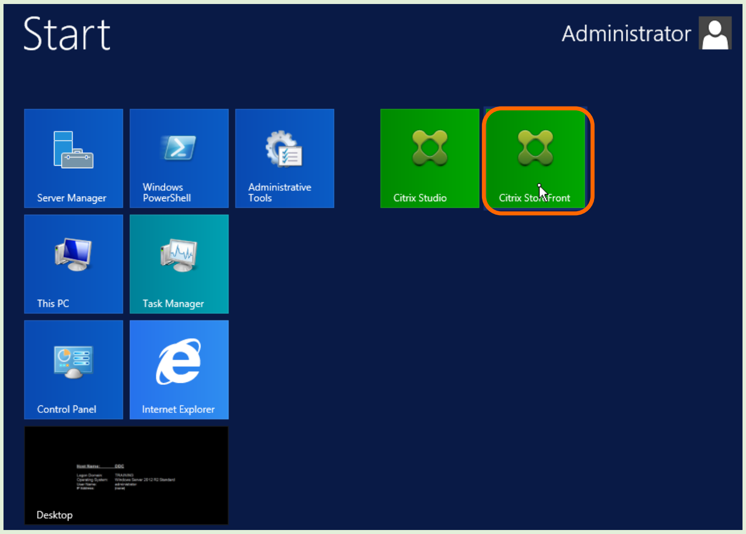
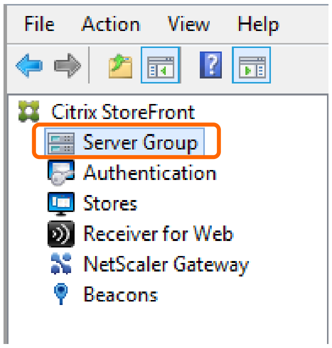
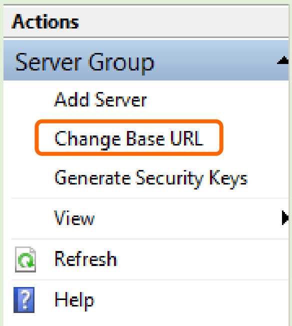
StoreFront provides access to published Windows Applications and Desktops. In this exercise, you will integrate XenMobile Server with XenDesktop 7.6 and configure StoreFront to provide access to published resources in the XenDesktop farm. StoreFront is already installed and only needs to be configured.

Step by step guidance

Estimated time to complete this lab: **15** minutes.

Step	Action
1.	In the XenCenter console, select the `Site1-AD.training.lab` virtual machine.
2.	Login with the following credentials: Username: `training\administrator` Password: `Citrix123`
3.	Double-click the `DNS` icon on your desktop. 
4.	Select `Forward Lookup Zones` and double-click on the `mycitrixtraining.net` zone.  File Action View Help DNS AD Forward Lookup Zones Reverse Lookup Zones Trust Points Conditional Forwarders Global Logs Name _msdcs.training.lab mycitrixtraining.net training.lab

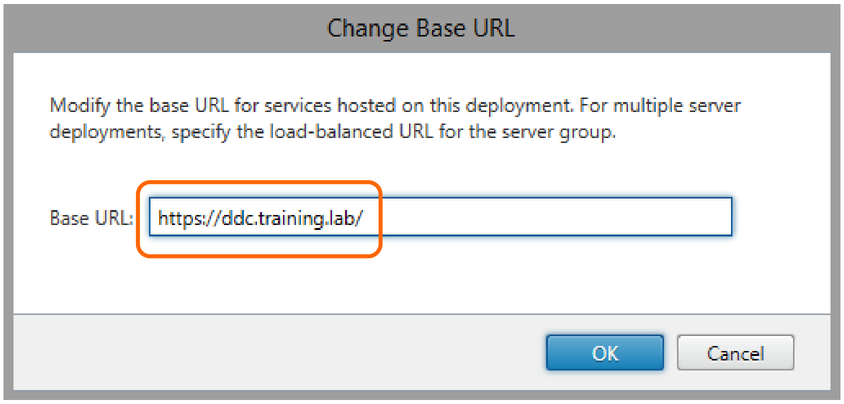
Step	Action
5.	Right-click the **mycitrixtraining.net** zone and click **New Host (A or AAAA)**.  DNS AD Forward Lookup Zones _msdcs.training.lab myci traini Reverse L Trust Poi Conditio Global Lc Name (same as parent folder) (same as parent folder) * Update Server Data File Reload New Host (A or AAAA)... New Alias (CNAME)... New Mail Exchanger (MX)... New Domain... New Delegation... Other New Records... DNSSEC
6.	In the **New Host** window, configure the following: Name: **YourIP1FQDN** **(Enter only the host name, not the domain portion)** IP Address: **192.168.10.100** Click **Add Host**, then click **OK**. **Click Done.**  New Host Name (uses parent domain name if blank): 75-126-159-219 Fully qualified domain name (FQDN): 75-126-159-219.mycitrixtraining.net. IP address: 192.168.10.100 ☐ Create associated pointer (PTR) record ☐ Allow any authenticated user to update DNS records with the same owner name
7.	Select the **Site1-DDC** virtual machine. Login with the following credentials: Username: **training\administrator** Password: **Citrix123**

Step	Action
8.	Launch the **Citrix StoreFront** console from the Start menu.  Start Administrator Server Manager Windows PowerShell Administrative Tools Citrix Studio Citrix StoreFront This PC Task Manager Control Panel Internet Explorer Desktop
9.	When the **Citrix StoreFront** console opens, click the **Server Group** node on the left side of the window.  File Action View Help Citrix StoreFront Server Group Authentication Stores Receiver for Web NetScaler Gateway Beacons
10.	On the right side of the window, select **Change Base URL**.  Actions Server Group Add Server Change Base URL Generate Security Keys View Refresh Help

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>11.</td><td>

Enter **https://ddc.training.lab** in the **Base URL** textbox.

Click OK.



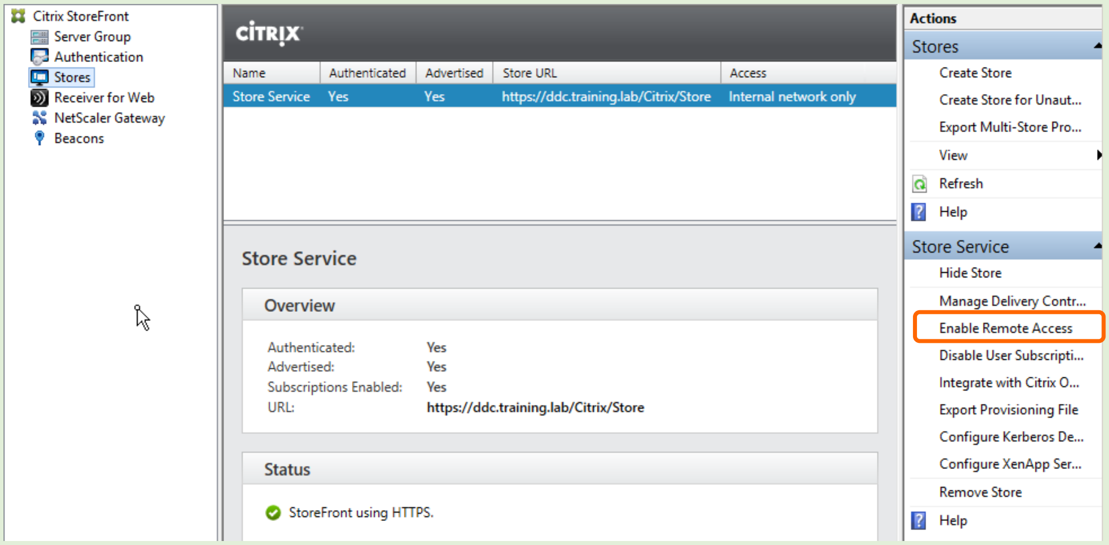
Change Base URL

Modify the base URL for services hosted on this deployment. For multiple server deployments, specify the load-balanced URL for the server group.

Base URL: https://ddc.training.lab/

</td></tr>
<tr><td>12.</td><td>

Select the Stores node. Click Enable Remote Access.



<table>
<tr><th>Name</th><th>Authenticated</th><th>Advertised</th><th>Store URL</th><th>Access</th></tr>
<tr><td>Store Service</td><td>Yes</td><td>Yes</td><td>https://ddc.training.lab/Citrix/Store</td><td>Internal network only</td></tr>
</table>

Store Service

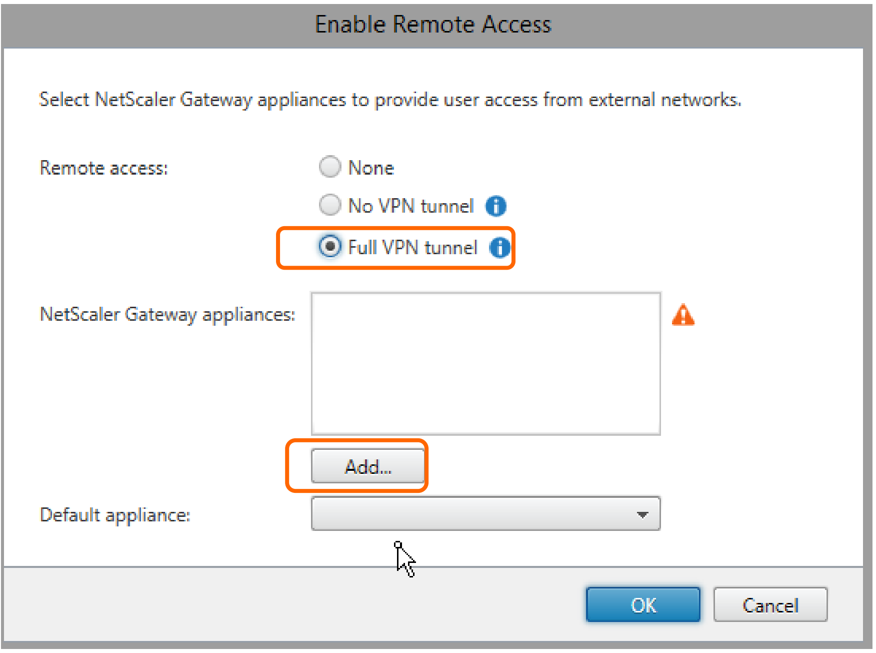
Overview

Authenticated: Yes
Advertised: Yes
Subscriptions Enabled: Yes
URL: https://ddc.training.lab/Citrix/Store

Status

StoreFront using HTTPS.

</td></tr>
</table>

Step	Action
13.	When the **Enable Remote Access** window opens, select the `Full VPN tunnel` radio button in the **Remote access** section. Then click `Add` from just below the **NetScaler Gateway appliances** section.  Enable Remote Access Select NetScaler Gateway appliances to provide user access from external networks. Remote access: ○ None ○ No VPN tunnel ● Full VPN tunnel NetScaler Gateway appliances: Default appliance: -

Step	Action
14.	In the **Add NetScaler Gateway Appliance** window, configure the following settings:

Display name: **NSG**

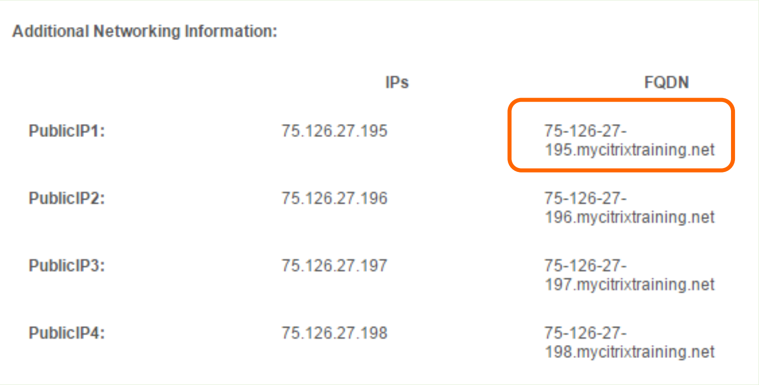
NetScaler Gateway URL: **https://IP1 FQDN**

Version: **10.0 (Build 69.4) or later**

Logon type: **Domain**

Callback URL: **https://IP1 FQDN**

> **Note:** Your IP1 FQDN is available on the portal page.
>
> **Example Only:** 75-126-159-219.mycitrixtraining.net

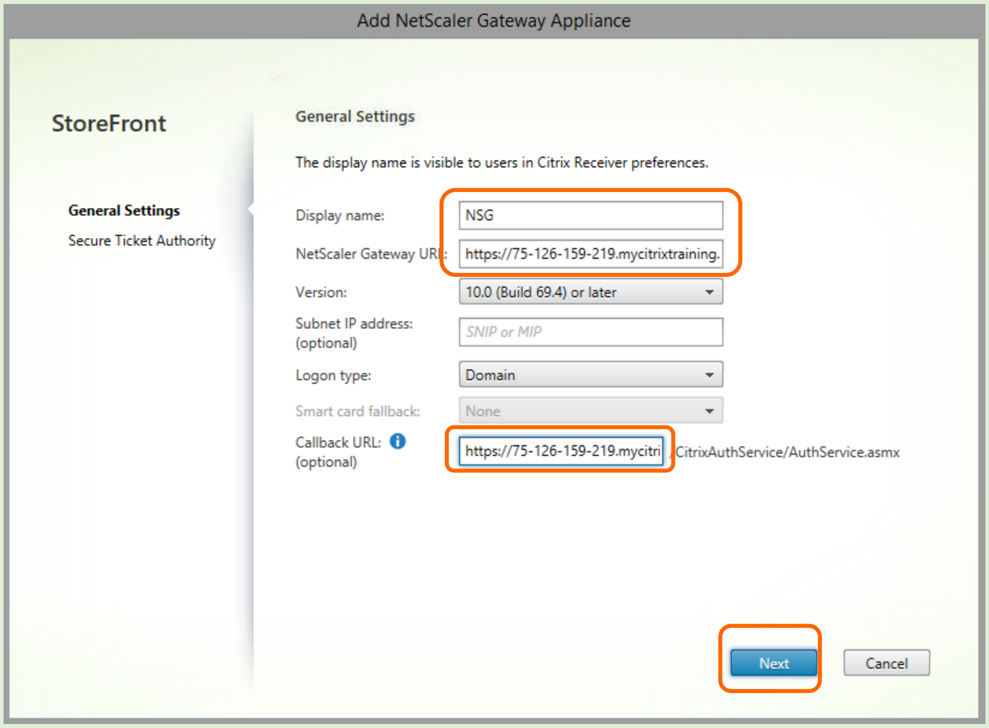


Additional Networking Information:

	IPs	FQDN
PublicIP1:	75.126.27.195	75-126-27-195.mycitrixtraining.net
PublicIP2:	75.126.27.196	75-126-27-196.mycitrixtraining.net
PublicIP3:	75.126.27.197	75-126-27-197.mycitrixtraining.net
PublicIP4:	75.126.27.198	75-126-27-198.mycitrixtraining.net

> **Note:** If you leave the callback URL blank, Smart Access will be disabled.

Click **Next**.



Add NetScaler Gateway Appliance

StoreFront

General Settings

Secure Ticket Authority

General Settings

The display name is visible to users in Citrix Receiver preferences.

Display name: NSG

NetScaler Gateway URL: https://75-126-159-219.mycitrixtraining.

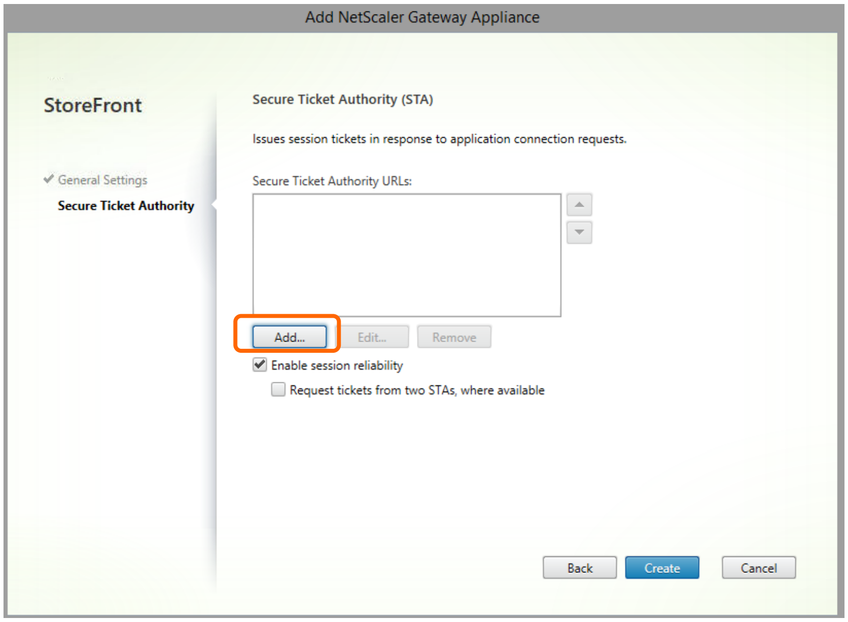
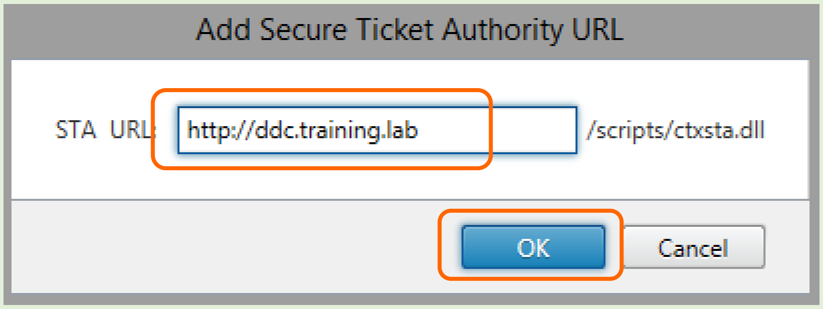
Version: 10.0 (Build 69.4) or later

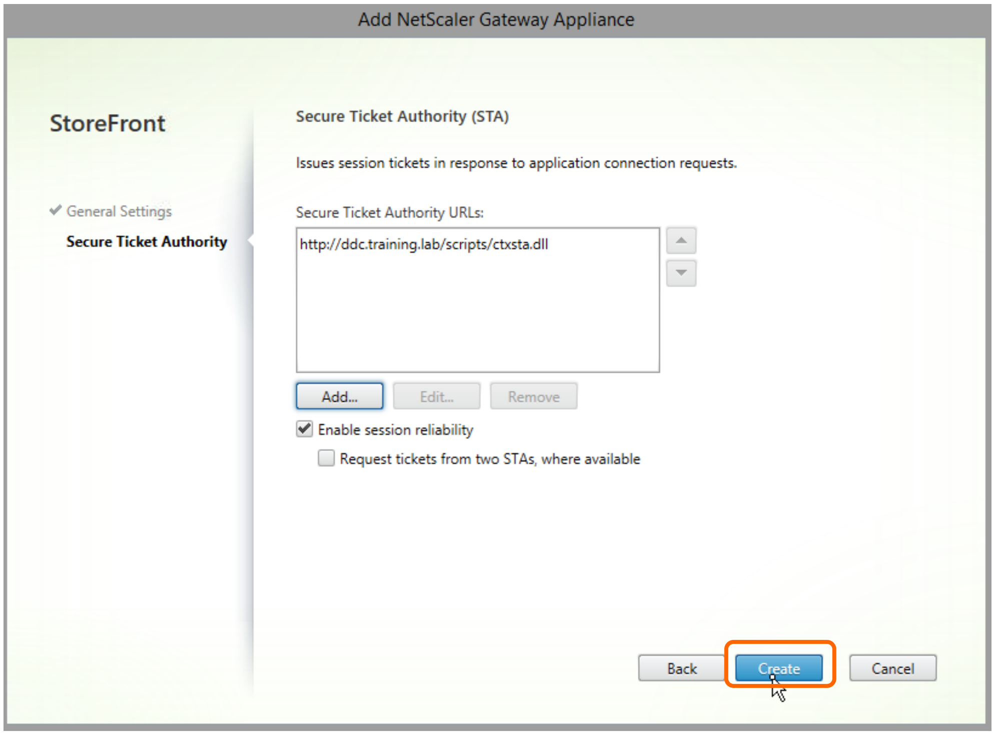
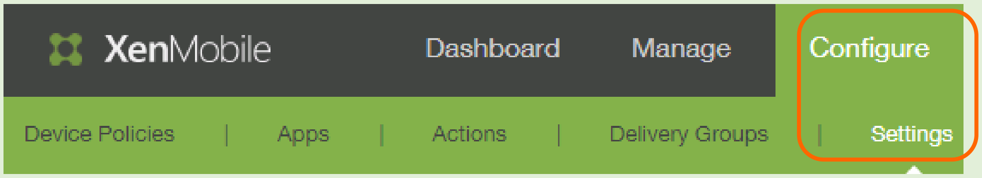
Subnet IP address: (optional) SNIP or MIP

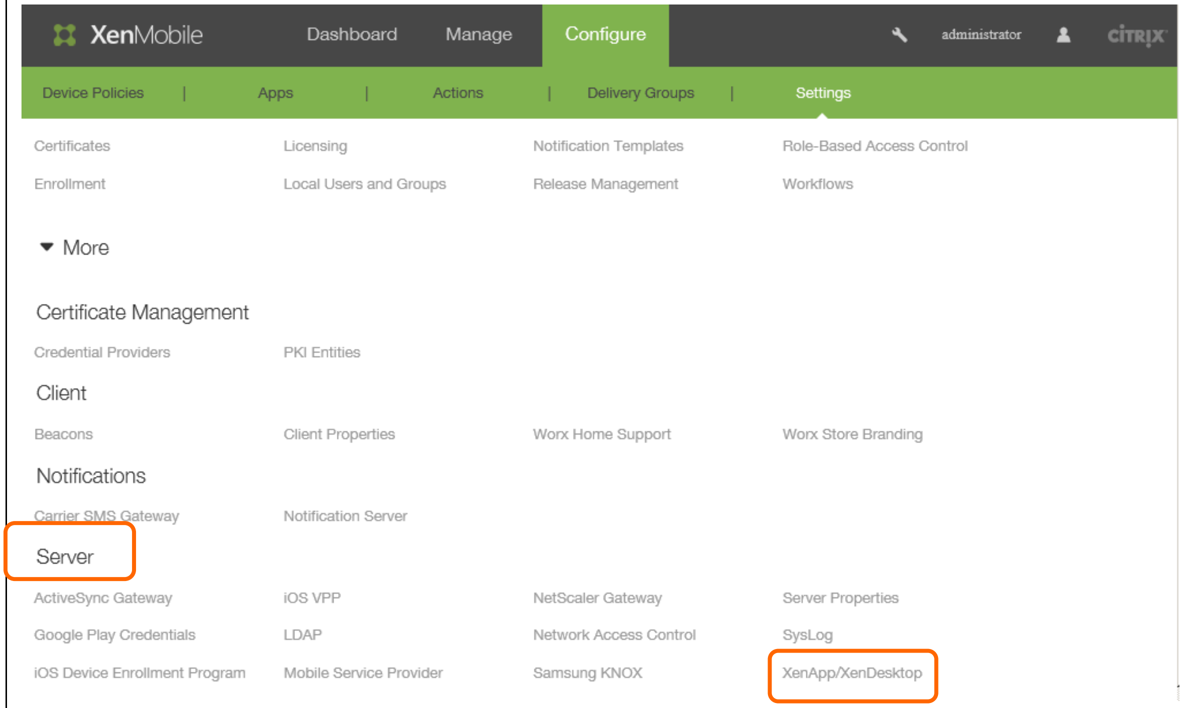
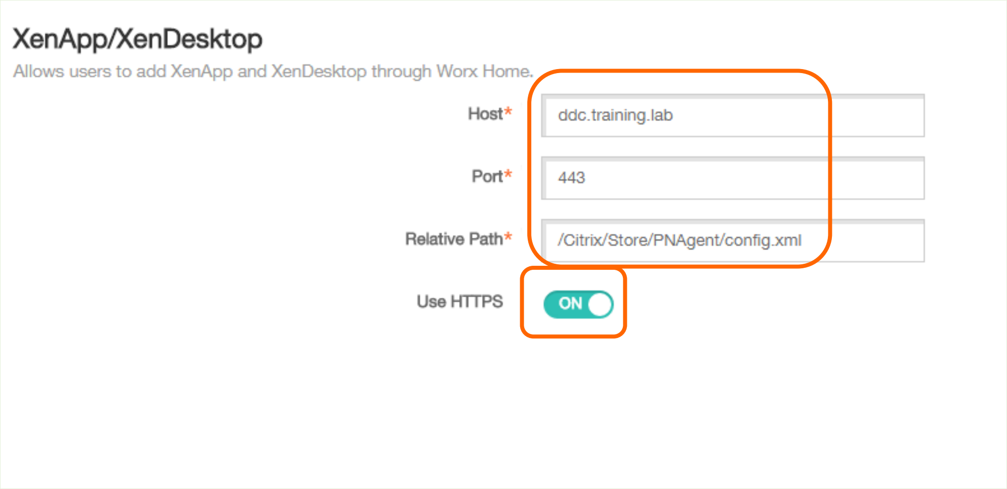
Logon type: Domain

Smart card fallback: None

Callback URL: (optional) https://75-126-159-219.mycitri /CitrixAuthService/AuthService.asmx

Step	Action
15.	In the **Secure Ticket Authority** section, click **Add**.  Add NetScaler Gateway Appliance StoreFront ✓ General Settings Secure Ticket Authority Secure Ticket Authority (STA) Issues session tickets in response to application connection requests. Secure Ticket Authority URLs: Add... Edit... Remove ☑ Enable session reliability □ Request tickets from two STAs, where available Back Create Cancel
16.	Type **`http://ddc.training.lab`** in the **STA URL** field and click **OK**.  Add Secure Ticket Authority URL STA URL: http://ddc.training.lab /scripts/ctxsta.dll OK Cancel

Step	Action
17.	Click **Create** and then **OK**.  Add NetScaler Gateway Appliance StoreFront ✓ General Settings Secure Ticket Authority Secure Ticket Authority (STA) Issues session tickets in response to application connection requests. Secure Ticket Authority URLs: http://ddc.training.lab/scripts/ctxsta.dll Add... Edit... Remove ☑ Enable session reliability ☐ Request tickets from two STAs, where available Back Create Cancel
18.	The NetScaler Gateway configuration has been added.
19.	Select the **Site1-Win81Client** virtual machine in XenCenter. If the virtual machine is locked, login as: Username: **training\administrator** Password: **Citrix123**
20.	Switch to the tab in Internet Explorer containing the XenMobile Server Management Console. **Note:** If you closed IE, open a new instance and browse to `https://192.168.10.20:4443` Navigate to **Configure > Settings**.  XenMobile Dashboard Manage Configure Device Policies | Apps | Actions | Delivery Groups | Settings

Step	Action
21.	Scroll down and expand the **More** node. Then under the **Server** section, click on the **XenApp/XenDesktop** node.  XenMobile Dashboard Manage Configure administrator Device Policies Apps Actions Delivery Groups 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 VPP NetScaler Gateway Server Properties Google Play Credentials LDAP Network Access Control SysLog iOS Device Enrollment Program Mobile Service Provider Samsung KNOX XenApp/XenDesktop
22.	Click **Edit** and enter the following settings: Host: **ddc.training.lab** Port: **443** Relative Path: **/Citrix/Store/PNAgent/config.xml** Use https: **ON** Click **Save**.  XenApp/XenDesktop Allows users to add XenApp and XenDesktop through Worx Home. Host* ddc.training.lab Port* 443 Relative Path* /Citrix/Store/PNAgent/config.xml Use HTTPS ON

Exercise Summary

In this exercise, you configured StoreFront services store on the DDC server. You also configured the XenMobile Server with the StoreFront information so that HDX applications can be enumerated on the end user's device.

Revision:	Change Description	Updated By	Date
1.0	Original version	Curtis Kegler	11/2014
1.1	Updated screenshots & added device enrollment exercise.	Curtis Kegler, Adolfo Montoya, & Karen Sciberras	11/2014
1.2	Updated screenshots, added steps to get to lab environment in Exercise 1, moved XenDesktop Integration to Optional Exercises section.	Curtis Kegler, Adolfo Montoya, & Karen Sciberras	1/2015

About Citrix

Citrix (NASDAQ:CTXS) is a cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, securely accessing apps and data on any of the latest devices, as easily as they would in their own office. Citrix solutions help IT and service providers build clouds, leveraging virtualization and networking technologies to deliver high-performance, elastic and cost-effective cloud services. With market-leading cloud solutions for mobility, desktop virtualization, networking, cloud platforms, collaboration and data sharing, Citrix helps organizations of all sizes achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 330,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at http://www.citrix.com.