Deploying the XenMobile Solution
Contents

Copyright and Trademarks ........................................................................................................ ii

1 Deploying the XenMobile 8.6 Solution ................................................................................. 7
   About the XenMobile Solution ......................................................................................... 9

2 Building Your XenMobile Solution ...................................................................................... 11
   Deploying XenMobile Components .................................................................................. 12
   Deploying NetScaler Gateway with App Controller and StoreFront ............................ 13
      Allowing Access to MDX Apps Through NetScaler Gateway ..................................... 14
   Deploying Device Manager .............................................................................................. 15
   Deploying the MDX Toolkit ............................................................................................... 16
   Deploying the Entire XenMobile Solution ........................................................................ 16

3 XenMobile Deployment Prerequisites .................................................................................. 19
   Gathering Information Before You Deploy XenMobile Components ............................ 20
   Opening Ports for the XenMobile Solution ...................................................................... 21
      Opening Ports for NetScaler Gateway and App Controller ....................................... 21
      Opening XenMobile MDM Ports .................................................................................. 23
   Gathering Network Information ....................................................................................... 25
   Obtaining and Installing Certificates ............................................................................... 25
      Configuring Client Certificates for Authentication ....................................................... 26
   Determining Your Hardware, Hypervisor, and Sizing Requirements ......................... 27
      NetScaler Gateway Requirements .............................................................................. 27
      Device Manager System Requirements ...................................................................... 28
         Windows Server ....................................................................................................... 28
         Java Requirements .................................................................................................... 28
         Server Hardware Requirements ............................................................................... 28
         Device Manager Database Requirements .................................................................. 29
      Windows Service Account Requirements .................................................................. 29
      Installation Requirements ............................................................................................. 29
Chapter 1

Deploying the XenMobile 8.6 Solution

Topics:

- **About the XenMobile Solution**

XenMobile Enterprise Edition includes the following Citrix products:

- NetScaler or NetScaler Gateway (user licenses for NetScaler Gateway included, but hardware or virtual appliance(s) must be purchased separately)
- XenMobile MDM Edition (with XenMobile Device Manager)
- XenMobile App Edition (with App Controller)
- MDX Toolkit
- Worx Home

You can deploy other Citrix products, such as Receiver, StoreFront, and the Web Interface to work with XenMobile.

XenMobile allows you to manage the following:

- Android, iOS, Windows 8 phones, tablets and Symbian mobile devices with Device Manager
- Access to web, Software as a Service (SaaS), and mobile apps through App Controller
- Provisioning access to ShareFile data and documents through App Controller
- Access to Windows-based apps and virtual desktops through StoreFront or the Web Interface

Users connect from mobile devices by using Worx Home. When users install Worx Home on their mobile device, they can use WorxMail to access their email and use WorxWeb to access web sites.

To allow access to email, calendar, and contacts from mobile devices through NetScaler, you can deploy the XenMobile NetScaler Connector (XNC). The connector allows you to send a list of compliant devices from Device Manager to NetScaler, which in turn controls which mobile devices are allowed to synchronize with the Exchange Server.

This section contains details about the features in each component, and information about integrating the XenMobile
Enterprise Edition products to deploy a complete solution to meet your users' needs.
About the XenMobile Solution

Citrix XenMobile is a comprehensive solution that allows you to manage mobile devices, apps, and data. Users can access all of their mobile, SaaS, Web, and Windows-based apps from a unified app store, including seamlessly integrated email, browser, data sharing, and support apps. XenMobile allows you to control mobile devices with full configuration, security, provisioning and support capabilities. In addition, XenMobile securely delivers Worx mobile apps that are built for businesses by using the Worx App SDK and found through the Worx App Gallery. With XenMobile, you can meet your compliance and control needs while giving users the freedom to experience work and life their way.

The XenMobile solution consists of the following components:

- **NetScaler Gateway.** NetScaler Gateway allows remote users to securely access internal network resources. Users can connect with any device to access their applications, email, and file shares in the internal network.

- **XenMobile MDM Edition.** XenMobile MDM includes Device Manager that allows you to manage mobile devices, set mobile policies and compliance rules, gain visibility to the mobile network, provide control over mobile apps and data, and shield your network from mobile threats. Device Manager simplifies the management of mobile devices.

- **XenMobile App Edition.** XenMobile App Edition includes App Controller 2.9, the industry's first unified service broker that aggregates, controls, and securely delivers Windows, web, and SaaS applications, iOS and Android apps, integrated ShareFile-based data, and virtual desktops to any device, anywhere. XenMobile App Edition gives users an intuitive single point of access and self-service for all of their business applications on any device anywhere.

- **MDX Toolkit.** The MDX Toolkit is a software application that you can install on Mac OS X computers and use to convert unsigned iOS or Android mobile apps (.ipa or .apk) into signed MDX files. In the process of this conversion, Citrix embeds a policy framework and default set of policies that enable you to configure, securely distribute, and manage each prepared application by using App Controller.

- **Worx apps.** Mobile users can connect with Worx Home to access their mobile apps from App Controller. Users can enroll their device in Device Manager by using Worx Enroll. Users can connect to the Worx Store and download Worx Home, WorxMail, and WorxWeb.

- **ShareFile.** ShareFile is a cloud-based file sharing service that enables users to easily and securely exchange documents. ShareFile enables users to send large documents by email, securely handle document transfers to third parties, and access a collaboration space from desktops or mobile devices. ShareFile provides users with a variety of ways to work, including a web-based interface, desktop tools, and integration with Microsoft Outlook.
Chapter 2

Building Your XenMobile Solution

Topics:

- Deploying XenMobile Components
- Deploying NetScaler Gateway with App Controller and StoreFront
- Deploying Device Manager
- Deploying the MDX Toolkit
- Deploying the Entire XenMobile Solution

The XenMobile components you deploy are based on the device or app management requirements of your organization. The components of XenMobile are modular and build on each other. For example, you want to give users in your organization remote access to mobile apps and you need to track the device types with which users connect. In this scenario, you would deploy NetScaler Gateway, XenMobile Device Manager, and App Controller.

This section discusses this and additional scenarios for deploying the XenMobile components in your network, as well as for the NetScaler appliance. The topics include architectural diagrams, information about the Citrix products you can integrate into your deployment, a recommended order in which to deploy the components, and the ways users connect depending on the deployment scenario you implement.
Deploying XenMobile Components

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

- **Connections to the internal network.** If your users are remote, they can connect by using a VPN or Micro VPN connection through NetScaler Gateway to access apps and desktops in the internal network.

- **Device enrollment in Device Manager.** Users can enroll mobile devices in Device Manager so you can manage the devices that connect to network resources.

- **Web, SaaS, and mobile apps from App Controller.** Users can access their web, SaaS, and mobile apps from AppController by using Worx Home or Receiver.

- **Windows-based apps and virtual desktops.** Users can connect with Citrix Receiver or a web browser to access Windows-based apps and virtual desktops from StoreFront or the Web Interface.

To achieve some or all of these capabilities, Citrix recommends deploying XenMobile components in the following order:

- **NetScaler Gateway.** You can configure settings in NetScaler Gateway to enable communication with App Controller, StoreFront, or the Web Interface by using the Quick Configuration wizard. You must install App Controller, StoreFront, or the Web Interface before using the Quick Configuration wizard in NetScaler Gateway.

- **Device Manager.** After you install Device Manager, you can configure policies and settings that allow users to enroll their mobile devices.

- **App Controller.** After you install App Controller, you can configure mobile, web, and SaaS apps. Mobile apps can include apps from the Apple App Store or Google Play. Users can also connect to mobile apps you wrap with the MDX Toolkit and upload to App Controller.

- **MDX Toolkit.** You can wrap .ipa or .apk apps and Worx apps with the MDX Toolkit. After you wrap the apps, you can upload the apps to App Controller.

- **StoreFront (optional).** You can provide access to Windows-based apps and virtual desktops from StoreFront through connections with Receiver.

- **ShareFile Enterprise (optional).** If you deploy ShareFile, you enable enterprise directory integration through App Controller or Security Assertion Markup Language (SAML). For more information about ShareFile, see *ShareFile Enterprise* in Citrix eDocs.

If you install all of the XenMobile components in your network, the deployment may look like the following figure:
The topics in this section detail the possible deployment scenarios in your network for the XenMobile components, as well as for the NetScaler appliance. The topics include architectural diagrams, information about the Citrix products you can integrate into your deployment, and the ways users connect depending on the deployment scenario you implement.

**Deploying NetScaler Gateway with App Controller and StoreFront**

You can deploy NetScaler Gateway at the perimeter of your organization's internal network (or intranet) to provide a secure single point of access to the servers, applications, and other network resources that reside in the internal network. In this deployment, all remote users must connect to NetScaler Gateway before they can access any resources in the internal network.

You can deploy NetScaler Gateway with the following Citrix products:

- XenMobile App Edition
- StoreFront
- XenApp
- XenDesktop
- Web Interface

Users can connect to resources in your internal network by using the following methods:
- Worx Home for users who connect with mobile devices and need access to MDX mobile apps. Users must connect with Worx Home on the mobile device to access MDX apps.

- Receiver so users can access Windows-based applications and desktops hosted by XenApp or XenDesktop. To allow users access to their Windows-based apps, you must deploy StoreFront or the Web Interface. If users connect with Receiver on a Windows or Mac computer, MDX apps are not available to users.

- Optionally, users can also connect with the NetScaler Gateway Plug-in for full VPN access to the internal network. Users can access email servers, files shares, and web servers with the NetScaler Gateway Plug-in for Windows or the NetScaler Gateway Plug-in for Mac.

The way you deploy App Controller in your internal network depends on how users connect: with Worx Home or with Receiver. In either scenario, you install NetScaler Gateway in the DMZ.

You can deploy the App Controller virtual machine (VM) on XenServer, VMware ESXi, or Microsoft Hyper-V located in your internal network. Users can connect to App Controller from an external connection (the Internet) or from the internal network. If users connect from the Internet or a remote location, the connection must route through NetScaler Gateway. App Controller resides in the internal network behind the firewall.

### Allowing Access to MDX Apps Through NetScaler Gateway

If users connect with Worx Home and you have MDX mobile apps installed on App Controller, you place StoreFront behind App Controller in your internal network. Users can connect to App Controller through NetScaler Gateway in the DMZ to obtain their web, SaaS, Android and iOS mobile apps, along with documents from ShareFile. StoreFront resides behind App Controller to deliver Windows-based apps and virtual desktops as shown in the following figure:

**Figure 2-2. Deploying NetScaler Gateway with MDX Apps**
Deploying Device Manager

In order to get your users' devices under management, users need to enroll their devices into Device Manager. To get started, you install Device Manager in your network. Next, you connect to Active Directory to import users by using the LDAP wizard. Then, you configure the following settings in Device Manager:

- Enrollment
- Policies
- Apps

When you finish configuring Device Manager, you can send enrollment invitations to your users. The invitation contains a link that allows users to download Worx Enroll, which then allows users to enroll their devices in Device Manager. When users log on, Device Manager authenticates the user's identity and enrolls the device.

Citrix recommends that you deploy NetScaler or NetScaler Gateway for security. You deploy NetScaler or NetScaler Gateway in the DMZ with Device Manager, as shown in the following figure. When you deploy NetScaler or NetScaler Gateway, you can use the XenMobile NetScaler Connector (XNC) to control access to email, calendar, and contacts from mobile devices. In this deployment, after enrollment, user devices connect to NetScaler or NetScaler Gateway to access resources.

If users enroll their iOS devices, the devices and Device Manager must communicate with the Apple Push Notification Service (APNS).

Figure 2-3. Deploying NetScaler or NetScaler Gateway and Device Manager

The preceding figure also shows the ports you need to open to enable the connections. You must open all of the ports behind the firewall for each identified service. For details about the ports, see Opening Ports for the XenMobile Solution on page 21. For
details about the APNS server, also shown in the preceding figure, see Requesting an APNS Certificate in the Device Manager documentation in Citrix eDocs.

Deploying the MDX Toolkit

Mobile app management allows you to securely manage and deliver mobile apps to users. With the Citrix MDX Toolkit, you can wrap iOS and Android apps to secure access and enforce policies. After you wrap the app, you can upload the app to XenMobile App Edition and configure MDX policies. Users can then download and install the app from Citrix Receiver. They can subsequently open and work with the app from an icon on the home screen, on the mobile device, or from the Receiver home page.

For more information about MDX policies for Android and iOS mobile apps in App Controller 2.8, see the following topics in Citrix eDocs:

- Configuring MDX Policies for Android Apps in App Controller
- Configuring MDX Policies for iOS Apps in App Controller

Deploying the Entire XenMobile Solution

If you deploy all of the components of the XenMobile solution, you have successfully completed the following tasks:

- Opened the required ports for communication between each component.
- Installed each component in your network.
- Successfully tested connections from user devices.

The next section discusses the deployment prerequisites and includes a checklist for you to use to get ready for your deployment. The subsequent sections contain component installation steps, and configuration tests you can carry out.

The following figure shows the complete solution:
Figure 2-4. The XenMobile Solution
Chapter 3
XenMobile Deployment Prerequisites

Topics:

• Gathering Information Before You Deploy XenMobile Components
• Opening Ports for the XenMobile Solution
• Gathering Network Information
• Obtaining and Installing Certificates
• Determining Your Hardware, Hypervisor, and Sizing Requirements
• Obtaining and Installing Licenses
• System Requirements for Wrapping Mobile Apps
• Choosing Your Authentication Method
• XenMobile Solution Pre-Installation Checklist

Before you deploy the XenMobile solution and install the components, make sure you have the right prerequisites and system requirements. This effort will prepare you to configure the network settings, open ports in your firewall, install certificates and licenses, and configure authentication.

This section details the deployment information you need to gather and includes the XenMobile Solution Pre-Installation Checklist to guide you through the recommended settings.
Gathering Information Before You Deploy XenMobile Components

Before you install XenMobile components in your network, you need the right prerequisites. These prerequisites include:

- **Network settings.** These settings include IP addresses, ports, DNS, Network Time Protocol (NTP) and SMTP servers, and the IP address or fully qualified domain name (FQDN) of a load balancer.

- **Hardware and sizing requirements.** These include Windows Servers, hypervisors, and NetScaler Gateway requirements. The NetScaler Gateway appliance you select (VPX, MDX, or SDX) determines the maximum number of user connections to your XenMobile deployment.

- **Certificates.** These include server, root, intermediate, Apple Push Notification Service (APNS), and certificates for wrapping mobile apps with the MDX Toolkit.

- **Licenses.** Licenses are required for XenMobile MDM Edition and NetScaler Gateway.

- **Active Directory settings.** These settings are required for XenMobile MDM Edition and for XenMobile App Edition.

- **Authentication method** Before deploying XenMobile components, it’s important to decide on an authentication method. For example, you should decide if you are implementing the Worx PIN that you configure in App Controller. The Worx PIN caches Active Directory credentials and works with client certificate authentication. Authentication settings can enable LDAP, RADIUS, one-time passwords, client certificate authentication, and two-factor authentication. If users connect to internal web sites, you need to configure authentication for NetScaler Gateway and SharePoint to allow single sign-on (SSO) to work.

  **Note:** If you implement an authentication method for users and then change the method after users enroll, users will need to enroll again.

- **Load balancers.** Load balancers manage connections to your XenMobile deployment. You might also need to plan for packet inspection appliances to monitor network traffic entering your internal network.

- **Email server and data synchronization settings** These settings include Exchange Server and ActiveSync configurations for XenMobile MDM Edition and WorxMail.

- **Databases.** These databases include either Microsoft SQL Server or Postgres for XenMobile MDM Edition. The Postgres database comes with XenMobile MDM Edition and installs when you install Device Manager.

  **Note:** Citrix recommends that you use Microsoft SQL Server. You should only use PostgreSQL in test deployments.
Opening Ports for the XenMobile Solution

To allow devices and apps to communicate with each XenMobile component, you need to open ports in your firewall. The following tables define the ports you need to open.

Opening Ports for NetScaler Gateway and App Controller

You need to open the following ports to allow user connections from Worx Home, Receiver, or the NetScaler Gateway Plug-in through NetScaler Gateway to App Controller, StoreFront, XenDesktop and to other internal network resources, such as intranet web pages.

**Note:**

- If NetScaler Gateway can reach the authentication server through a system IP (NSIP) subnet, the appliance uses the NSIP as the source IP. If the authentication server is not on a local subnet to the NSIP, the source IP is the subnet IP (SNIP). You should configure the firewall rules accordingly.

- For the sake of this guide, the listed ports are the default settings for the associated protocols. You may need to adjust the port configuration if your environment uses custom ports for any of the associated services. The list is also not exhaustive; advanced features not covered in this guide may use additional ports.

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Open this port to send support bundles to an FTP server.</td>
<td>App Controller</td>
<td>FTP server</td>
</tr>
<tr>
<td>53</td>
<td>DNS.</td>
<td>NetScaler Gateway (subnet IP address [SNIP])</td>
<td>DNS server</td>
</tr>
<tr>
<td>80</td>
<td>NetScaler Gateway passes the VPN connection to the internal network resource through the second firewall. Typically occurs if users log on with the NetScaler Gateway Plug-in.</td>
<td>NetScaler Gateway SNIP</td>
<td>Intranet web sites</td>
</tr>
<tr>
<td>80 or 8080</td>
<td>The XML and STA port that does enumeration, ticketing, and authentication. Citrix recommends using port 443.</td>
<td>XML network traffic - StoreFront or Web Interface STA - NetScaler Gateway SNIP</td>
<td>XenDesktop or XenApp</td>
</tr>
<tr>
<td>TCP port</td>
<td>Description</td>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>123</td>
<td>Network Time Protocol (NTP) services.</td>
<td>NetScaler Gateway SNIP</td>
<td>NTP server</td>
</tr>
<tr>
<td>389</td>
<td>Unsecure LDAP connections.</td>
<td>NetScaler Gateway SNIP or system IP (NSIP)</td>
<td>LDAP authentication server or Active Directory</td>
</tr>
<tr>
<td>443</td>
<td>Connections to StoreFront from Receiver or Receiver for Web that provides access to Windows-based applications and virtual desktops hosted in XenApp and XenDesktop.</td>
<td>Internet</td>
<td>NetScaler Gateway (virtual IP address [VIP] )</td>
</tr>
<tr>
<td></td>
<td>Connections to App Controller for web, mobile, and SaaS application delivery.</td>
<td>Internet</td>
<td>NetScaler Gateway VIP</td>
</tr>
<tr>
<td></td>
<td>Communication required for Callback URL.</td>
<td>App Controller</td>
<td>NetScaler Gateway VIP</td>
</tr>
<tr>
<td></td>
<td>The XML and STA port that does enumeration, ticketing, and authentication.</td>
<td>XML network traffic - StoreFront or Web Interface STA - NetScaler Gateway SNIP</td>
<td>XenDesktop or XenApp</td>
</tr>
<tr>
<td>636</td>
<td>Secure LDAP connections.</td>
<td>NetScaler Gateway SNIP or NSIP</td>
<td>LDAP authentication server or Active Directory</td>
</tr>
<tr>
<td>1494</td>
<td>Connections to Windows-based applications in the internal network by using the ICA protocol. Citrix recommends keeping this port open.</td>
<td>NetScaler Gateway SNIP</td>
<td>XenApp or XenDesktop</td>
</tr>
<tr>
<td>1812</td>
<td>RADIUS connection.</td>
<td>NetScaler Gateway SNIP</td>
<td>RADIUS authentication server</td>
</tr>
<tr>
<td>2598</td>
<td>Connections to Windows-based applications in the internal network by using session</td>
<td>NetScaler Gateway SNIP</td>
<td>XenApp or XenDesktop</td>
</tr>
</tbody>
</table>
### Opening XenMobile MDM Ports

You need to open the following ports to allow XenMobile MDM to communicate in your network.

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>By default, the Device Manager SMTP configuration of the notification service uses this port. If your SMTP server uses a different port, make sure your firewall does not block that port.</td>
<td>XenMobile MDM</td>
<td>SMTP server</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>3268</td>
<td>Microsoft Global Catalog unsecure LDAP connections.</td>
<td>NetScaler Gateway SNIP or NSIP</td>
<td>LDAP authentication server or Active Directory</td>
</tr>
<tr>
<td>3269</td>
<td>Microsoft Global Catalog secure LDAP connections.</td>
<td>NetScaler Gateway SNIP or NSIP</td>
<td>LDAP authentication server or Active Directory</td>
</tr>
<tr>
<td>8081</td>
<td>Passthrough for ICA Traffic using STA. (Optional: Required for certificate-based deployments that use StoreFront.)</td>
<td>Internet</td>
<td>NetScaler Gateway VIP</td>
</tr>
<tr>
<td>9080</td>
<td>NetScaler communicates with the XNC. This port is for HTTP traffic.</td>
<td>NetScaler SNIP</td>
<td>XNC</td>
</tr>
<tr>
<td>9443</td>
<td>NetScaler communicates with the XNC. This port is for HTTPS traffic.</td>
<td>NetScaler SNIP</td>
<td>XNC</td>
</tr>
<tr>
<td>9736</td>
<td>Communication between two App Controller virtual machines deployed as a high availability pair.</td>
<td>App Controller</td>
<td>App Controller</td>
</tr>
<tr>
<td>TCP port</td>
<td>Description</td>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>80 or 443</td>
<td>MDM server Enterprise App Store connection to Apple iTunes App Store (ax.itunes.apple.com) or to Google Play. Used for publishing iTunes App Store or Google Play apps from the available app store from within the Device Manager web console and Citrix Mobile Self-Serve on the iOS device or Worx Home for Android. Citrix Mobile Self-Serve is available when iOS devices enroll in Device Manager.</td>
<td>XenMobile MDM</td>
<td>Apple iTunes App Store (ax.itunes.apple.com)</td>
</tr>
<tr>
<td>80 or 443</td>
<td>XenMobile Device Manager Nexmo SMS Notification Relay outbound connection.</td>
<td>XenMobile MDM</td>
<td>Nexmo SMS Relay Server</td>
</tr>
<tr>
<td>389</td>
<td>Unsecure LDAP connections.</td>
<td>XenMobile MDM</td>
<td>LDAP authentication server or Active Directory</td>
</tr>
<tr>
<td>443</td>
<td>Enrollment and agent setup for Android and Windows Mobile.</td>
<td>Internet</td>
<td>XenMobile Device Manager Server</td>
</tr>
<tr>
<td></td>
<td>Enrollment and agent setup for Android and Windows Mobile, the Device Manager web console, and MDM Remote Support Client.</td>
<td>Internal local area network (LAN) and Wi-Fi</td>
<td></td>
</tr>
<tr>
<td>1433</td>
<td>Remote database server connection to a separate SQL server (optional).</td>
<td>XenMobile MDM</td>
<td>SQL Server</td>
</tr>
<tr>
<td>2195</td>
<td>Apple Push Notification Service (APNS) outbound connection to gateway.push.apple.com that is used for iOS device notifications and device policy push.</td>
<td>XenMobile MDM</td>
<td>Internet (Apple APNS Service Hosts using the public IP address 17.0.0.0/8)</td>
</tr>
<tr>
<td>2196</td>
<td>APNS outbound connection to feedback.push.apple.com that is used for iOS device notification and device policy push.</td>
<td>XenMobile MDM</td>
<td></td>
</tr>
</tbody>
</table>
### TCP Port Description

<table>
<thead>
<tr>
<th>TCP Port</th>
<th>Description</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>5223</td>
<td>APNS outbound connection from iOS devices that connect through Wi-Fi networks to *.push.apple.com.</td>
<td>iOS device on Wi-Fi network service</td>
<td>Internet (Apple APNS Service Hosts using the public IP address 17.0.0.0/8)</td>
</tr>
<tr>
<td>8443</td>
<td>Enrollment for iOS devices only.</td>
<td>Internet</td>
<td>XenMobile MDM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LAN and Wi-Fi</td>
<td></td>
</tr>
</tbody>
</table>

### Gathering Network Information

You need to identify the following network settings and configure appropriate server settings before you install the XenMobile components in your network:

- IP addresses for each XenMobile component. For example, for NetScaler Gateway, you need the system IP (NSIP) and the subnet IP (SNIP) addresses.
- Opening the appropriate ports in your firewall to allow network traffic to communicate with each component.
- Domain Name Servers (DNS) for name resolution with users inside your network and users who connect from remote locations. You might need different IP addresses for each DNS server.
- Network Time Protocol (NTP) server. The NTP server synchronizes the time between all of your network components. Citrix recommends that you use an NTP server for your XenMobile deployment.
- SMTP server for email. When you configure an SMTP server, you need the fully qualified domain name (FQDN) of the email server, such as mail.mycompany.com. You also need to identify the port, the email addresses used for the send function, and user email addresses and passwords.

The XenMobile Pre-Installation checklist includes a section where you can write down all of your network settings. You might need to coordinate with other team members to configure the ports and servers you need for the XenMobile deployment. For more information about ports and to print the checklist, see:

- XenMobile Solution Pre-Installation Checklist
- Opening Ports for the XenMobile Solution on page 21

### Obtaining and Installing Certificates

Certificates are used to create secure connections and authenticate users.

XenMobile MDM requires a certificate from the Apple Push Notification Service (APNS). XenMobile MDM also uses its own PKI service or obtains certificates from the Microsoft Certificate Authority (CA) for client certificates.
All Citrix products support wildcard and SAN certificates. For most deployments, you only need two wildcard or SAN certificates. You can use the following formats:

- External - *.mycompany.com
- Internal - *.myinternaldomain.net

The following table shows the certificate format and type for each XenMobile component:

<table>
<thead>
<tr>
<th>XenMobile component</th>
<th>Certificate format</th>
<th>Required certificate type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler Gateway</td>
<td>PEM (BASE64)</td>
<td>Server, root</td>
<td>External</td>
</tr>
<tr>
<td>App Controller</td>
<td>PEM or PFX (PKCS#12)</td>
<td>Server, SAML, root</td>
<td>Internal</td>
</tr>
<tr>
<td>StoreFront</td>
<td>PFX (PKCS#12)</td>
<td>Server, root</td>
<td>Internal</td>
</tr>
<tr>
<td>XenMobile MDM</td>
<td>P12 format (PKCS#12)</td>
<td>APNS, server Device Manager creates its own PKI service or uses the Microsoft CA for client certificates</td>
<td>External</td>
</tr>
</tbody>
</table>

For NetScaler Gateway and App Controller, Citrix recommends obtaining server certificates from a public CA, such as Verisign, DigiCert, or Thawte. You can create a Certificate Signing Request (CSR) from the NetScaler Gateway configuration utility or the App Controller management console. After you create the CSR, submit it to the CA for signing. When the CA returns the signed certificate, you can install the certificate on NetScaler Gateway or App Controller.

For more information about installing certificates, see the following topics in Citrix eDocs:

- NetScaler Gateway: Installing and Managing Certificates
- App Controller: Configuring Certificates in App Controller
- Device Manager: Requesting an APNS Certificate

**Configuring Client Certificates for Authentication**

NetScaler Gateway supports the use of client certificates for authentication. Users logging on to a NetScaler Gateway virtual server can also be authenticated based on the attributes of the client certificate that is presented to the virtual server. Client certificate authentication can also be used with another authentication type, such as LDAP or RADIUS, to provide two-factor authentication.

To authenticate users based on the client-side certificate attributes, client authentication should be enabled on the virtual server and the client certificate should
be requested. You must bind a root certificate to the virtual server on NetScaler Gateway.

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

You can authenticate users based on the client certificate by setting the default authentication type to use the client certificate. You can also create a certificate action that defines what is to be done during the authentication based on a client SSL certificate.

**Determining Your Hardware, Hypervisor, and Sizing Requirements**

Each XenMobile component has specific hardware, hypervisor, or sizing requirements:

- **User devices.** This hardware requirement includes the number and types of devices that enroll when you deploy Device Manager, such as iPads or Android phones.

- **Hardware or hypervisor.** These requirements include the hardware resources to support your number of users and devices. You install App Controller and NetScaler VPX on a hypervisor, such as XenServer. You can also deploy the physical NetScaler or NetScaler Gateway appliance. The number of users who connect determines the NetScaler Gateway appliance model you select, or the number of App Controller instances you install on the hypervisor.

  Your hypervisor, such as XenServer, must contain enough disk space and memory to support multiple instances of App Controller or NetScaler VPX.

- **Sizing.** The number of devices that connect to XenMobile components. For example, if Device Manager supports 5,000 devices, the Device Manager server needs from 2 through 4 CPUs, a minimum of 4 gigabytes (GB) of memory, and 24 GB of disk space.

This section describes detailed hardware or hypervisor requirements for each XenMobile component.

**NetScaler Gateway Requirements**

To determine which of the following NetScaler Gateway models suit the needs of your organization, you need to consider how many users will connect. You can use the following guidelines:

- **NetScaler SDX** - a hardware platform on which virtual instances on NetScaler and NetScaler Gateway can run. NetScaler SDX can handle up to 62,500 user connections. For more information, see the NetScaler documentation in Citrix eDocs.

- **NetScaler Gateway MPX** - a physical appliance that can handle up to 7,500 user connections.
NetScaler Gateway VPX - a virtual machine that can handle up to 875 user connections.

**Device Manager System Requirements**

You can refer to the following system requirements for installing Device Manager.

**Windows Server**

- Microsoft Windows Server 2012 64-bit Standard or Enterprise Edition
- Microsoft Windows Server 2008 R2 Standard or Enterprise Edition

**Note:** If you plan to use device certificate templates with Microsoft Certificate Services, the Windows Server running the Active Directory Certificate Services must be running Microsoft Windows Server 2008 R2 SP1, Standard or Enterprise Edition.

If you plan to use the SharePoint access management feature, you must have Microsoft Windows Server 2008 R2 Standard or Enterprise Edition with Service Pack 1 or with fix KB976217 installed on the server.

**Java Requirements**

- Oracle Java SE 7 JDK (JDK Download Edition) with a minimum of update 11
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7

The Java Cryptography Extension (JCE) is an officially released Standard Extension to the Java Platform. JCE provides a framework and implementation for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms. For more information, see [Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7](#) on the Oracle web site.

**Note:** Oracle Java components all must be downloaded separately from the download web site. The JCE components must be installed in the JDK's Java Runtime Environment in order to properly support enrollment of iOS devices. Please follow the installation Read Me instructions that accompany the Java JCE download package [Java SE Downloads](#) on the Oracle web site.

After you download and extract the JCE package, copy the files local_policy.jar and US_export_policy.jar to the `<java-home>\jre\lib\security` folder and overwrite the existing files.

**Server Hardware Requirements**

- Physical or virtual server host environment
- Intel Xeon 3Ghz or AMD Opteron-1.8Ghz server class
- 4-GB RAM minimum recommended for 64-bit operating system
- 500-MB free disk space minimum
The Windows Server hardware needs to support the number of devices that connect. You can use the following table for guidance:

<table>
<thead>
<tr>
<th>Number of devices</th>
<th>Windows Server</th>
<th>SQL Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000</td>
<td>2 vCPU and 4GB of memory</td>
<td>2 vCPU and 6 GB memory</td>
</tr>
<tr>
<td>10,000</td>
<td>4 vCPU and 8 GB of memory</td>
<td>4 vCPU and 16 GB memory</td>
</tr>
<tr>
<td>20,000</td>
<td>8 vCPU and 16 GB of memory</td>
<td>16 vCPU and 24 GB memory</td>
</tr>
<tr>
<td>40,000</td>
<td>16 vCPU and 32 GB of memory</td>
<td>32 vCPU and 64 GB memory</td>
</tr>
</tbody>
</table>

**Device Manager Database Requirements**

The Device Manager Server repository requires one of the following databases:

- Microsoft SQL Server 2005
- SQL Server 2008
- SQL Server 2008 R2

**User Account Needed:** For the database server, you will need a service account that has administrator rights to SQL server, including the following access rights: Creator, Owner, and Read/Write permissions.

**Windows Service Account Requirements**

The Windows service accounts for the Device Manager Server and the database must be a Local Administrator of the computer on which the Device Manager Server is installed.

**Installation Requirements**

When you install XenMobile, use the following guidelines:

**Note:** Domain membership is not required for the Device Manager server.

- Do not install a new version of IIS, and uninstall IIS if it exists on this server.
- Create an external DNS record for the Device Manager server, such as mobile.yourcompany.com.

**App Controller System Requirements**

You can install App Controller on the following:

- XenServer 6.2
- XenServer 6.0
XenServer 6.1
- XenServer 5.6 with a minimum of Service Pack 1
- Microsoft Server 2012 with Hyper-V enabled
- Microsoft Hyper-V Server 2012
- VMware ESXi 5.0.1
- VMware ESXi 5.1
- VMware ESXi 4.x

XenServer, Hyper-V, and VMware ESXi must provide adequate virtual computing resources to App Controller as listed in the following table.

### XenServer and VMware ESXi Requirements

XenServer and VMware ESXi must provide adequate virtual computing resources to App Controller as listed in the following table.

<table>
<thead>
<tr>
<th>Memory</th>
<th>4 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPU (VCPU)</td>
<td>2 VCPUs</td>
</tr>
<tr>
<td><strong>Note:</strong> If App Controller is acting as the cluster head, Citrix recommends 4 VCPUs.</td>
<td></td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
</tbody>
</table>

### Microsoft Hyper-V Requirements

Microsoft Hyper-V must provide adequate virtual computing resources to App Controller as listed in the following table.

| Disk space (this is maximum disk size to which the App Controller disk can increase) | 50 GB |
| Memory                                                                          | 4 GB  |
| VCPU                                                                            | 2     |
| Virtual Network interfaces (available for each App Controller VM)                | 1     |

### Active Directory

When you add users to Active Directory, you must enter the first name, last name, and email in the user properties. If you do not configure users in Active Directory with this information, App Controller cannot synchronize these individuals. When users attempt to start an app, users receive a message that they are not authorized to use the app.
Obtaining and Installing Licenses

XenMobile MDM Edition and NetScaler Gateway require licenses. When you purchase a Citrix product, you receive an email that contains a link for your licenses. You obtain your licenses by logging on to the Citrix web site and then downloading your licenses.

**Important:** Citrix recommends that you retain a local copy of all license files you receive. When you save a backup copy of the configuration file, all uploaded licenses files are included in the backup. If you need to reinstall XenMobile MDM Edition or NetScaler Gateway appliance software and do not have a backup of the configuration, you will need the original license files.

For more information about NetScaler Gateway and Device Manager licenses, see XenMobile Licensing on the Citrix web site.

System Requirements for Wrapping Mobile Apps

The following are system requirements for wrapping iOS and Android mobile apps.

The MDX Toolkit requires the Java Development Kit (JDK) 1.7. You can download the JDK 1.7 from Java SE Development Kit Downloads on the Oracle web site. The instructions for installing the JDK on Mac OS X are on the Computech Tips web site.

Operating System

You can run the MDX Toolkit for wrapping iOS and Android apps on Mac OS X Versions 10.7 (Lion), 10.8 (Mountain Lion), or 10.9 (Mavericks).

Tools for Wrapping iOS Mobile Apps

You must obtain the iOS Distribution Provisioning Profile from Apple that allows Apple to sign the app. For more information about obtaining provisioning profiles, see the Apple Web site.

Any app that runs on a physical iOS device (other than apps in the Apple App Store) needs to be signed with a provisioning profile and a corresponding certificate. There are two kinds of profiles: Enterprise and Ad Hoc.

- The Enterprise profile allows you to run the app on unlimited devices
- The Ad Hoc profile allows you to run the app on up to about 100 devices

To wrap apps, Citrix recommends using the Enterprise profile. You can purchase the profile from the Apple web site.
**Note**: If you are running Apple Xcode 4.5 or later versions, you also need to install the Xcode command-line tools from the Xcode Apple Developer web site. The Mac OS X Mavericks 10.9, for example, does not install the command line tools automatically. To install the tools, do the following:

1. In Applications > Utilities, click Terminal to use the Mac command-line interface.
2. Type the following command:

   ```
xcode-select -install
   ```

   Be sure to include two hyphens before the word install in the command.

---

**Tools for Wrapping Android Mobile Apps**

To wrap Android mobile apps, you must install the following on your computer before running the MDX Toolkit:

- Android Software Development Kit (SDK).
- Digitally signed certificate whose private key is held by the application’s developer. For more information about the certificate, see Signing Your Applications on the Android Developers web site.

You must sign your applications with a key that meets the following guidelines:

- 1024 bit keysizes
- DSA key algorithm (keyalg)
- SHA1with DSA signing algorithm (sigalg)

You need to add the Android SDK path in the PATH environment variable on your computer. You can also provide the PATH variable in the MDX Toolkit during the wrapping process. You also need to add the APK Tool installation path in the PATH environment variable.

---

**Choosing Your Authentication Method**

Before you install XenMobile components, you need to determine what authentication types you use to authenticate users. XenMobile supports several authentication types. It is important to choose the authentication method you want to configure before you deploy XenMobile; if you implement an authentication method for users and then change the method after users enroll or you implement Worx PIN, they will need to enroll again.

XenMobile supports the following authentication types:

- Active Directory or LDAP
You can configure the following authentication types for two-factor authentication:

- Active Directory and Worx PIN
- Active Directory and client certificate authentication

XenMobile 8.6 introduces support for client certificate authentication. Users can now authenticate their devices seamlessly to XenMobile using client certificates, giving administrators the choice of authenticating their users using Active Directory credentials or client certificates. By using client certificates, users will only need to use their own chosen PIN number to log on with single sign-on (SSO) to any of the Worx-enabled apps.

Worx PIN also simplifies the user authentication experience. Worx PIN is used to secure a client certificate or save Active Directory credentials locally on the device. If you configure Worx PIN settings in App Controller, when users start Worx Home for the first time, they receive a prompt to enter a PIN, which caches the Active Directory credentials. When users subsequently start Worx Home, WorxMail, or WorxWeb, they enter the PIN and log on. This simplifies the logon process on the mobile device. For more information about configure Worx PIN, see Configuring Worx PIN Options.

Citrix recommends using two-factor authentication for the highest security and recommends that you combine Worx PIN with Active Directory and client certificate authentication, which allows for the security of two-factor authentication while maintaining a streamlined user experience. For instructions on how to configure client certificate authentication in XenMobile, see this Knowledge Base article.

The XenMobile architecture supports the following authentication combinations:

- Domain only (Worx PIN supported)
- Security token only
- Domain and security token (Worx PIN supported)
- Client certificate only
- Client certificate and domain (Worx PIN supported)
- Client certificate and security token

**XenMobile Solution Pre-Installation Checklist**

This checklist lists the tasks you should complete and the configuration values you should note before you install the following three XenMobile components: NetScaler Gateway, Device Manager, and App Controller. Each task or note includes a column indicating the component or components for which the requirement applies.
Citrix recommends that you print and complete this checklist. The checklist has an extra column that you can use to check off each task as you complete it and to record information.

For installation instructions of XenMobile components, see the following:

- Installing NetScaler Gateway 10.1 in Your Network
- Installing Device Manager
- Installing App Controller

## Basic Network Connectivity

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

<table>
<thead>
<tr>
<th>Prerequisite description</th>
<th>Configure on component</th>
<th>Note the setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note the fully qualified domain name (FQDN) to which remote users connect.</td>
<td>NetScaler Gateway Device Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note the public and local IP address. You need these IP addresses to configure the firewall to set up network address translation (NAT).</td>
<td>Device Manager NetScaler Gateway App Controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note the subnet mask.</td>
<td>Device Manager NetScaler Gateway App Controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note the DNS IP addresses.</td>
<td>Device Manager NetScaler Gateway App Controller</td>
<td></td>
</tr>
<tr>
<td>Prerequisite description</td>
<td>Configure on component</td>
<td>Note the setting</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Write down the WINS server IP addresses (if applicable).</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>Identify and write down the NetScaler Gateway host name.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> This is not the FQDN. The FQDN is contained in the signed server certificate that is bound to the virtual server and to which users connect. You can configure the host name by using the Setup Wizard in NetScaler Gateway.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note the App Controller FQDN.</td>
<td>App Controller</td>
<td></td>
</tr>
<tr>
<td>Note the IP address of App Controller.</td>
<td>App Controller</td>
<td></td>
</tr>
<tr>
<td>Reserve one IP address if you install one instance of App Controller.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reserve three IP addresses if you configure high availability on App Controller. There is one virtual IP address and an IP address for each node. If you configure a cluster, note all of the IP addresses you need.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note the IP address or FQDN of the Network Time Protocol (NTP) server.</td>
<td>NetScaler Gateway</td>
<td>App Controller</td>
</tr>
<tr>
<td>• One public IP address configured on NetScaler Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• One external DNS entry for NetScaler Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note the web proxy server IP address, port, proxy host list, and the administrator user name and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prerequisite description</td>
<td>Configure on component</td>
<td>Note the setting</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>password. These settings are optional if you deploy a proxy server in your network (if applicable).</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> You can user either the sAMAccountName or the User Principal Name (UPN) when configuring the user name for the web proxy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write down the default gateway IP address.</td>
<td>App Controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device Manager</td>
<td></td>
</tr>
<tr>
<td>Write down the system IP (NSIP) address and subnet mask.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>Write down the subnet IP (SNIP) address and subnet mask.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>Write down the NetScaler Gateway virtual server IP address and FQDN from the certificate.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>If you need to configure multiple virtual servers, write down all of the virtual IP addresses and FQDNs from the certificates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write down the internal networks that users can access through NetScaler Gateway.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>Example: 10.10.0.0/24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enter all internal networks and network segments that users need access to when they connect with Worx Home or the NetScaler Gateway Plug-in when split tunneling is set to <strong>On</strong>.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Licensing

XenMobile requires you to purchase licensing options for NetScaler Gateway and Device Manager. For more information about obtaining your license files, see The Citrix Licensing System.

<table>
<thead>
<tr>
<th>Prerequisite description</th>
<th>Configure on component</th>
<th>Note the setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain Universal licenses from the <a href="https://citrix.com">Citrix web site</a>. For details about NetScaler Gateway licensing, see Installing Licenses on NetScaler Gateway in Citrix eDocs.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>Obtain perpetual, annual, or hosted cloud-based server licensing from the <a href="https://citrix.com">Citrix web site</a>. For details about Device Manager licensing, see Licensing in Citrix eDocs.</td>
<td>Device Manager</td>
<td></td>
</tr>
</tbody>
</table>

Certificates

Device Manager, App Controller, and Device Manager require certificates to enable connections with other Citrix products and applications and from user devices. For more information about requesting certificates for XenMobile components, see the following in Citrix eDocs.

- [Requesting an APNS Certificate for Device Manager](https://citrix.com/support)
- [Configuring Certificates in App Controller](https://citrix.com/support)
- [Installing and Managing Certificates for NetScaler Gateway](https://citrix.com/support)

**Note:** For Device Manager, you need to install the required Java components, as noted later in this checklist, before you install the APNS certificate.

<table>
<thead>
<tr>
<th>Prerequisite description</th>
<th>Configure on component</th>
<th>Note the setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain and install required certificates. You can create Certificate Signing Requests (CSRs) by using Windows Server and Internet Information Services (IIS). You can also create CSRs in NetScaler Gateway and App Controller.</td>
<td>App Controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device Manager</td>
<td></td>
</tr>
</tbody>
</table>
Prerequisite description | Configure on component | Note the setting  
--- | --- | ---  
NetScaler Gateway  

### Ports

You need to open ports to allow communication with the XenMobile components. For a complete list of all ports you need to open for the XenMobile Solution, see Opening Ports for the XenMobile Solution on page 21.

| Prerequisite description | Configure on component | Note the setting  
--- | --- | ---  
Open ports for the XenMobile Solution | App Controller  
Device Manager  
NetScaler Gateway |   

### Active Directory Settings

**Important**: When you add users in Active Directory for App Controller, you must enter the first name, last name, and email in the user properties. If you do not configure users in Active Directory with this information, App Controller cannot synchronize these individuals. When users attempt to start an app, users receive a message that they are not authorized to use the app.

| Prerequisite description | Configure on component | Note the setting  
--- | --- | ---  
Note the Active Directory IP address and port.  
If you use port 636, install a root certificate from a CA on Device Manager.  
If you use port 636, install a root certificate from a CA on App Controller. | App Controller  
Device Manager  
NetScaler Gateway |   
Note the Active Directory domain name. | App Controller |
<table>
<thead>
<tr>
<th>Prerequisite description</th>
<th>Configure on component</th>
<th>Note the setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note the Active Directory service account.</strong></td>
<td>App Controller, Device Manager, NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>The Active Directory service account is the account that App Controller and Device Manager uses to query Active Directory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note the Base DN.</strong></td>
<td>App Controller, Device Manager, NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>This is the directory level under which users are located; for example, cn=users,dc=ace,dc=com. NetScaler Gateway, App Controller, and Device Manager use this to query Active Directory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> If your Active Directory database is large, you can configure multiple Base DNs to which App Controller or Device Manager binds and in which the server searches to find user objects. For example, you can use the following: ou=Finance,dc=ace,dc=com; ou=Sales,dc=ace,dc=com</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note the Group Base DN.</strong></td>
<td>App Controller, Device Manager, NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>This is the directory level under which users are located. You can use the same value that you used for Base DN. NetScaler Gateway, App Controller, and Device Manager use this to query Active Directory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note a user account for testing.</strong></td>
<td>App Controller, Device Manager</td>
<td></td>
</tr>
<tr>
<td>This is an Active Directory account that you can use to log on and test single sign-on (SSO).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Database Requirements for Device Manager

<table>
<thead>
<tr>
<th>Prerequisite description</th>
<th>Configure on component</th>
<th>Note the setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note the SQL Server user accounts.</td>
<td>Device Manager</td>
<td></td>
</tr>
<tr>
<td>Configure a service account with administrator rights to SQL Server, including the following access rights: Creator, Owner, and Read/Write permissions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note the Windows Service Account.</td>
<td>Device Manager</td>
<td></td>
</tr>
<tr>
<td>This account is for the Device Manager Server and the database. The account must be a Local Administrator of the computer on which you install Device Manager Server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note the SQL Server FQDN or IP address.</td>
<td>Device Manager</td>
<td></td>
</tr>
</tbody>
</table>

Connections Between App Controller, Device Manager, and NetScaler Gateway

You can configure Device Manager and App Controller to connect. Complete the following tasks that are indicated for Device Manager if you deploy App Controller in your internal network. If users connect to App Controller from an external network, such as the Internet, users must connect to NetScaler Gateway before accessing mobile, web, and SaaS apps. If that is the case, complete the following tasks that are indicated for NetScaler Gateway.

Note: Configure App Controller settings on Device Manager first. Then, you can configure Device Manager settings in App Controller.
### Prerequisite description

<table>
<thead>
<tr>
<th>Prerequisite description</th>
<th>Configure on component</th>
<th>Note the setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note the Device Manager host name.</td>
<td>App Controller</td>
<td></td>
</tr>
<tr>
<td>Note the Device Manager port (80 or 443).</td>
<td>App Controller</td>
<td></td>
</tr>
<tr>
<td>Note the shared key from Device Manager. Enter the same shared key in Device Manager and App Controller.</td>
<td>App Controller Device Manager</td>
<td></td>
</tr>
<tr>
<td>Note if you want mobile devices to enroll in Device Manager as a requirement before connecting to App Controller.</td>
<td>App Controller</td>
<td></td>
</tr>
<tr>
<td>Note the App Controller host name.</td>
<td>Device Manager</td>
<td></td>
</tr>
<tr>
<td>Write down the FQDN or IP address of App Controller.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>Identify web, SaaS, and mobile iOS or Android applications users can access.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>Note the Callback URL to allow communication between App Controller and NetScaler Gateway</td>
<td>App Controller</td>
<td></td>
</tr>
</tbody>
</table>

### User Connections: Access to XenDesktop, XenApp, the Web Interface, or StoreFront

In NetScaler Gateway, you need to create two virtual servers. One virtual server allows user connections to App Controller from Worx Home. Citrix recommends that you use the Quick Configuration wizard in NetScaler Gateway to configure these settings.

You create a second virtual server to enable user connections from Receiver and web browsers to connect to Windows-based applications and virtual desktops in XenApp and XenDesktop. Citrix recommends configuring the virtual server, session and clientless access policies by using the NetScaler Gateway Policy Manager. For more information, see Configuring Access To StoreFront Through NetScaler Gateway in Citrix eDocs.
### Prerequisite description

<table>
<thead>
<tr>
<th>Prerequisite description</th>
<th>Configure on component</th>
<th>Note the setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note the NetScaler Gateway host name and external URL.</td>
<td>App Controller</td>
<td></td>
</tr>
<tr>
<td>The external URL is the web address with which users connect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note the NetScaler Gateway callback URL.</td>
<td>App Controller</td>
<td></td>
</tr>
<tr>
<td>Note the IP addresses and subnets masks for the virtual servers.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>Note the path for Program Neighborhood Agent or a XenApp Services site.</td>
<td>NetScaler Gateway</td>
<td>App Controller</td>
</tr>
<tr>
<td>Note the FQDN or IP address of the XenApp or XenDesktop server running the Secure Ticket Authority (STA) (for ICA connections only).</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>Note the public FQDN for Device Manager.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
<tr>
<td>Note the public FQDN for Worx Home.</td>
<td>NetScaler Gateway</td>
<td></td>
</tr>
</tbody>
</table>

### Devices

XenMobile MDM supports the following device platforms: iOS, Android, Windows Phone 8 and Windows Tablet, Windows Mobile, and Symbian. For a list of platforms versions and the Device Manager features supported for each platform, see Feature Support by Device Platform in Citrix eDocs.

<table>
<thead>
<tr>
<th>Prerequisite description</th>
<th>Configure on component</th>
<th>Note the setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note the mobile device platforms in your organization.</td>
<td>Device Manager</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4

XenMobile Component Installation Steps

Topics:
- Downloading XenMobile Product Software
- Installing NetScaler Gateway 10.1 in Your Network
- Installing Device Manager
- Installing App Controller
- Enabling Connections Between Device Manager and App Controller
- Downloading and Installing the MDX Toolkit

Citrix recommends that you install XenMobile components in the following order:
- NetScaler or NetScaler Gateway
- Device Manager
- XenMobile NetScaler Connector (XNC)
- App Controller
- StoreFront (optional)
- ShareFile (optional)

In addition to installing these components, you also need to configure each component to communicate with other components.

After you install the XenMobile components, you can use the MDX Toolkit to wrap .ipa and .apk files. Then, you can upload the MDX files to App Controller for users to download and install.

This section includes installation and configuration steps for each XenMobile component, as well as the MDX Toolkit.
Downloading XenMobile Product Software

You can download product software from the Citrix web site. You need to log on to the site and then click the Downloads link on the Citrix web page. You can then select the product and type you want to download. For example, the following figure shows XenMobile product software drop-down list:

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

XenMobile

Product Software

You can select your software from the available list of options. For example, if you select XenMobile 8.6 Enterprise Edition, you can download the software for Device Manager, App Controller, NetScaler Gateway, and other XenMobile components as shown in the following figure:
To download the software for NetScaler Gateway

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

1. Go to the Citrix web site.
2. Click My Account and log on.
3. Click Downloads.
4. Under Find Downloads, select NetScaler Gateway.
5. In Select Download Type, select Product Software and then click Find.
   You can also select Virtual Appliances to download NetScaler VPX. When you select this option, you receive a list of software for the virtual machine for each hypervisor.
7. Click the appliance software version you want to download.
8. On the appliance software page for the version you want to download, select the virtual appliance and then click Download.
9. Follow the instructions on your screen to download the software.

To download the software for Device Manager

1. Go to the Citrix web site.
2. Click My Account and log on.
3. Click Downloads.
4. Under Find Downloads, select XenMobile.
5. In Select Download Type, select Product Software and then click Find.
8. Follow the instructions on your screen to download the software.

To download the software for App Controller

1. Go to the Citrix web site.
2. Click My Account and log on.
3. Click Downloads.
4. Under Find Downloads, select XenMobile.
5. In Select Download Type, select Product Software and then click Find.
7. On the XenMobile 8.6 App Edition page, click the appropriate App Controller virtual image in order to install App Controller on XenServer, VMware, or Hyper-V.
8. Follow the instructions on your screen to download the software.

To download the MDX Toolkit

You can run the MDX Toolkit for wrapping iOS and Android apps on Mac OS X Versions 10.7 (Lion), 10.8 (Mountain Lion), or 10.9 (Mavericks).

1. Go to the Citrix web site.
2. Click My Account and log on.
3. Click Downloads.
4. Under Find Downloads, select XenMobile.
5. In Select Download Type, select Product Software and then click Find.
8. Locate MDX Toolkit & SDK for iOS and Android Build <number> where <number> is the toolkit build number, such as 324.
9. Click Download.
10. Follow the instructions on your screen to download the software.
Installing NetScaler Gateway 10.1 in Your Network

This section discusses the installation of the NetScaler Gateway MDX physical appliance and NetScaler VPX in your network. Before you install either the physical appliance or the virtual appliance, complete the NetScaler information in the XenMobile Solution Pre-Installation Checklist. After you install the physical appliance by following the instructions in Installing the Model MPX Appliance in Citrix eDocs, you turn on the appliance and perform the initial configuration. This includes configuring:

- NetScaler Gateway IP address (NSIP)
- Subnet IP address (SNIP)
- Default gateway
- DNS servers
- Host name
- Licenses
- Certificates that include the fully qualified domain name (FQDN)

Configuring IP Addresses on NetScaler Gateway

You can configure IP addresses to log on to the configuration utility and for user connections. NetScaler Gateway is configured with a default IP address of 192.168.100.1 and subnet mask of 255.255.0.0 for management access. The default IP address is used whenever a user-configured value for the NetScaler Gateway system IP (NSIP) address is absent.

- **NSIP address.** The management IP address for NetScaler Gateway that is used for all management-related access to the appliance. NetScaler Gateway also uses the NSIP address for authentication.
- **Default gateway.** The router that forwards traffic from outside the secure network to NetScaler Gateway.
- **Subnet IP (SNIP) address.** The IP address that represents the user device by communicating with a server on a secondary network.

The SNIP address use ports 1024 through 64000.

Configuring the Host Name and FQDN on NetScaler Gateway

The host name is the name of the NetScaler Gateway appliance that is associated with the license file. The host name is unique to the appliance and is used when you download the Universal license. You define the host name when you run the Setup Wizard to configure NetScaler Gateway for the first time.
The fully qualified domain name (FQDN) is included in the signed certificate that is bound to a virtual server. You do not configure the FQDN on NetScaler Gateway. One appliance can have a unique FQDN assigned to each virtual server that is configured on NetScaler Gateway by using certificates.

You can find the FQDN of a certificate by viewing the details of the certificate. The FQDN is located in the subject field of the certificate.

**To view the FQDN of a certificate**

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, click **SSL**.
2. In the details pane, select a certificate, click **Actions** and then click **Details**.
3. In the **Certificate Details** dialog box, click **Subject**.
   The FQDN of the certificate appears in the list.

**Configuring the Initial Settings on the NetScaler Gateway Appliance**

The way you configure the initial settings on NetScaler Gateway depends on if you install the physical appliance or the virtual image.

To perform the initial configuration on the physical appliance, you can use the LCD keypad on the front panel of the appliance, the serial console, or the Setup Wizard. You can access the Setup Wizard from any computer that is on the same network as the new NetScaler Gateway appliance. However, because this method uses the default IP address for NetScaler Gateway, you must install and configure one appliance at a time. To configure the virtual appliance, see Configuring the Initial Settings on the NetScaler VPX on page 49.

If you want to configure a new NetScaler Gateway appliance from a remote network, or if you want to install multiple appliances and then configure them without using the console port, you can use Dynamic Host Configuration Protocol (DHCP) to assign each new appliance an IP address at which you can access the appliance for remote configuration.

Citrix recommends configuring the appliance by using the serial console.

**To configure the NetScaler Gateway by using the serial console**

**Note:** To locate the serial console port on your appliance, see Configuring the MPX Appliance by Using the LCD Keyboard in the NetScaler Gateway Appliances section in Citrix eDocs.

1. Connect the Ethernet cable into your appliance.

   For more information, see Connecting the Cables to the MPX Appliance in the NetScaler Gateway Appliances section in Citrix eDocs.
2. In a Secure Shell (SSH) application, such as PuTTY, log on to the appliance by using
   the administrator credentials.
   The default user name and password is nsroot.

3. At the command prompt, type `config ns` to run the configuration script.

4. To complete the initial configuration of your appliance, follow the prompts.

Instead of step 2 and 3, you can directly enter the commands for the initial
configuration. Log on to the appliance with an SSH application and at the command
prompt, type:

```
set ns config -ipAddress <IPAddress> -netmask <Netmask>
add ns ip <IPAddress> <Netmask> -type <Type>
add route <Network> <Netmask> <Gateway>
set system user nsroot <Password>
save ns config
reboot
```

**Example**

```
set ns config -ipAddress 10.102.29.60 -netmask 255.255.255.0
add ns ip 10.102.29.61 255.255.255.0 -type nsip
add route 0.0.0.0 0.0.0.0 10.102.29.1
set system user nsroot administrator
save ns config
reboot
```

The initial configuration of your physical NetScaler Gateway appliance is complete. You
can now log on to the configuration utility to configure additional settings and run the
Quick Configuration wizard to set up connections between NetScaler Gateway and App
Controller.

**Configuring the Initial Settings on the NetScaler VPX**

When you install NetScaler VPX on your hypervisor, you configure the initial settings by
using the command line. For example, if you install NetScaler VPX on XenServer, you
use the **Console** tab to configure the initial settings.

You are prompted to configure the following:

- IPv4 address
- Subnet mask
- Default gateway

The following figure shows the settings configured on the **Console** tab in XenCenter.
When you press 4 to save the settings, the appliance restarts. When the appliance is in an UP state, you then log on to the command-line console by using a Secure Shell (SSH) application, such as PuTTY. Configure the subnet IP (SNIP) address by using the following commands:

```
set ns config -ipAddress <IPAddress> -netmask <Netmask>
add ns ip <IPAddress> <Netmask> -type <Type>
save ns config
reboot
```

Example

```
set ns config -ipAddress 10.102.29.60 -netmask 255.255.255.0
add ns ip 10.102.29.61 255.255.255.0 -type snip

save ns config
reboot
```

You must set the SNIP address. When you set this address, you can then log on to the configuration utility by using the IP address you configured on the Console tab. For example, as shown in the preceding figure, you can use the format http://10.199.242.67 in a web browser to log on to the configuration utility.

**Creating a Certificate Signing Request on NetScaler Gateway**

On NetScaler Gateway, you use certificates to create secure connections and to authenticate users. To establish a secure connection, a server certificate is required at
one end of the connection. A root certificate of the Certificate Authority (CA) that issued the server certificate is required at the other end of the connection. Typically, you install the server certificate on NetScaler Gateway and the root certificate is installed on the user device.

Citrix recommends creating a Certificate Signing Request (CSR) to create the server certificate and private key. You can send the certificate to a public Certificate Authority (CA) such as VeriSign, Digi-Cert, or Thawte for signing. The private key remains on the NetScaler Gateway appliance and is password protected. When you receive the certificate from the CA, you install the certificate on NetScaler Gateway and pair the certificate with the private key.

You use the Create Certificate Request included in the NetScaler Gateway wizard to create the CSR.

**Important:** When you use the NetScaler Gateway wizard to create the CSR, you must exit the wizard and wait for the CA to send you the signed certificate. When you receive the certificate, you can run the NetScaler Gateway wizard again to create the settings and install the certificate. For more information about the NetScaler Gateway wizard, see *Configuring Settings by Using the NetScaler Gateway Wizard* in the NetScaler Gateway 10.1 documentation in Citrix eDocs.

On the **Specify a server certificate** page in the wizard, you click **Create a Certificate Signing Request** as shown in the following figure:

![Certificate Signing Request dialog box](image)

The **Certificate Signing Request** dialog box appears. You complete the fields as described in the following procedure.
To configure a CSR by using the NetScaler Gateway Wizard

1. In the configuration utility, click the Configuration tab and then in the navigation pane, click NetScaler Gateway.

2. In the details pane, under Getting Started, click NetScaler Gateway wizard.

3. Follow the directions in the wizard until you come to the Specify a server certificate page.

4. Click Create a Certificate Signing Request and then complete the fields.

   **Note:** The Common Name is the fully qualified domain name (FQDN), which does not need to be the same as the NetScaler Gateway host name. The FQDN is used for user logon.

5. Click Create to save the certificate on your computer and then click Close.

6. Exit the NetScaler Gateway wizard without saving your settings.

After you create the certificate and private key, email the CSR to the CA, such as Thawte, Digi-Cert, or VeriSign.

**Installing the Signed Certificate on NetScaler Gateway**

When you receive the signed certificate from the Certificate Authority (CA), you install the certificate on NetScaler Gateway and then you pair it with the private key.

**To pair the signed certificate with a private key**

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand SSL and then click Certificates.
2. In the details pane, click **Install**.
   The **Install Certificate** dialog box opens.

3. In **Certificate-Key Pair Name**, type the name of the certificate.

4. In **Certificate File Name**, select the drop-down box in **Browse** and then click **Local**.

5. Navigate to the certificate, select the certificate and then click **Open**.

6. In **Key File Name**, select the drop-down box in **Browse** and then click **Appliance**.
   The name of the private key is the same name as the Certificate Signing Request (CSR). The private key is located on NetScaler Gateway in the directory \nsconfig\ssl.

7. Choose the private key and then click **Open**.

8. If the certificate is PEM format, in **Password**, type the password for the private key.

9. If you want to configure notification for when the certificate expires, in **Notifies When Expires**, click **ENABLED**.

10. In **Notification Period**, type the number of days, click **Create** and then click **Close**.

---

**To install a license on NetScaler Gateway**

After you successfully download the license file to your computer, you can then install the license on NetScaler Gateway. The license is installed in the /nsconfig/license directory.

If you used the Setup Wizard to configure the initial settings on NetScaler Gateway, the license file is installed when you run the wizard. If you allocate part of your licenses and then at a later date, you allocate an additional number of licenses, you can install the licenses without using the Setup Wizard.

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **System** and then click **Licenses**.

2. In the details pane, click **Manage Licenses**.
3. Under **Update Licenses**, click **Browse**, navigate to the license file and then click **OK**. A message appears in the configuration utility stating that you need to restart NetScaler Gateway. Click **Restart**.

### Configuring NetScaler Gateway by Using Wizards and Utilities

To deploy NetScaler Gateway as part of the XenMobile solution, you use the First-time Setup Wizard, the new ShareFile wizard, and the Quick Configuration wizard.

#### How the First-time Setup Wizard Works

When you finish installing and configuring the initial settings on the NetScaler Gateway appliance, when you log on to the configuration utility for the first time, the First-time Setup wizard appears if you still need to configure the following settings:

- Install a license on the appliance.
- Configure a subnet IP (SNIP) address.
- Change the default IP address of the appliance from 192.168.100.1.

#### How the NetScaler ShareFile Wizard Works

The NetScaler appliance supports load balancing of multiple ShareFile StorageZone Controllers. You can configure the load balancing virtual server by using either the integrated XenMobile configuration utility or by using the ShareFile wizard in NetScaler. This wizard prompts you for basic information about your StorageZones Controller environment and then generates a configuration that does the following:

- Load balances traffic across StorageZones Controllers.
- Provides user authentication for StorageZones Connectors.
- Validates URI signatures for ShareFile uploads and downloads.
- Terminates SSL connections at the NetScaler appliance.

To start the ShareFile wizard, in the configuration utility, in the navigation pane, expand **Traffic Management** and then click **Load Balancing**. In the details pane, under **Citrix ShareFile**, click **Setup NetScaler for ShareFile**.
You can run the ShareFile wizard by using the ShareFile link or as part of the new integrated XenMobile configuration in NetScaler. For more information about the XenMobile configuration, see Configuring the NetScaler Gateway by Using Wizards in the NetScaler Gateway documentation in eDocs.

How the Quick Configuration Wizard Works

The Quick Configuration wizard allows you to configure multiple virtual servers on NetScaler Gateway. With the wizard, you can add, edit, and remove virtual servers. How you start this wizard depends on how you log on to the configuration utility:

- **NetScaler Gateway only.** When you log on to the configuration utility, in Deployment Type, select NetScaler Gateway. When logon is successful, the Home tab appears. On this tab, you can click Create NetScaler Gateway to configure the virtual server.

- **NetScaler and NetScaler Gateway.** When you log on to the configuration utility, in Deployment Type, select NetScaler ADC. If you install a NetScaler license to enable NetScaler features along with the NetScaler Gateway license, you start the Quick Configuration wizard by clicking the link Configure NetScaler Gateway for Enterprise Store on the NetScaler Gateway landing page on the Configuration tab.

The Quick Configuration wizard allows for seamless configuration to App Controller. The Quick Configuration wizard allows you to configure the following settings on the appliance:

- Virtual server name, IP address, and port
- Redirection from an unsecure to a secure port
- LDAP server
- RADIUS server
- Certificates
When you run the Quick Configuration wizard, the following policies are created based on your App Controller, StoreFront, and Web Interface settings:

- Session policies, including policies and profiles for Receiver, Receiver for Web, NetScaler Gateway Plug-in, and Program Neighborhood Agent
- Clientless access
- LDAP and RADIUS authentication

**Configuring NetScaler Gateway with the First-time Setup Wizard**

To configure the NetScaler Gateway (the physical appliance or the VPX virtual appliance) for the first time, you need an administrative computer configured on the same network as the appliance.

You must assign a NetScaler Gateway IP (NSIP) address as the management IP address of your appliance and a subnet IP (SNIP) address to which your servers can connect. You assign a subnet mask that applies to both NetScaler Gateway and SNIP addresses. You must also configure a time zone. If you assign a host name, you can access the appliance by specifying its name instead of the NSIP address.

There are two sections in the First-time Setup Wizard. In the first section, you configure the basic system settings for the NetScaler Gateway appliance including:

- NSIP address, SNIP address, and subnet mask
- Appliance host name
- DNS servers
- Time zone
- Administrator password

In the second section, you install licenses. If you specify the address of a DNS server, you can use the hardware serial number (HSN) or license activation code (LAC) to allocate your licenses, instead of uploading your licenses from a local computer to the appliance.

**Note:** Citrix recommends saving your licenses to your local computer.

When you finish configuring these settings, NetScaler Gateway prompts you to restart the appliance. When you log on to the appliance again, you can use other wizards and the configuration utility to configure additional settings.

**Configuring Settings with the Quick Configuration Wizard**

You can configure settings in NetScaler Gateway to enable communication with App Controller, StoreFront, or Web Interface by using the Quick Configuration wizard. When you complete the configuration, the wizard creates the correct policies for communication between NetScaler Gateway, App Controller, StoreFront, or the Web Interface. These policies include authentication, session, and clientless access policies. When the wizard completes, the policies are bound to the virtual server.
During the wizard, you configure the following settings:

- Virtual server name, IP address, and port
- Redirection from an unsecure to a secure port
- Certificates
- LDAP server
- RADIUS server
- Client certificate for authentication (only for double-source authentication)
- App Controller, StoreFront, or Web Interface

The Quick Configuration wizard supports LDAP and RADIUS authentication. You can configure two-factor authentication in the wizard by following these guidelines:

- If you select LDAP as your primary authentication type, you can configure RADIUS as the secondary authentication type.
- If you select RADIUS as your primary authentication type, you can configure LDAP as the secondary authentication type.

**Important:** You can only configure one LDAP authentication policy by using the Quick Configuration wizard. The wizard does not allow you to configure multiple LDAP authentication policies. If you run the wizard more than one time and want to use a different LDAP policy, you must configure the additional policies manually by using the NetScaler Gateway Policy Manager. For more information about configuring NetScaler Gateway to authenticate user access with one or more LDAP servers, see Configuring LDAP Authentication.

After you initially run the wizard, you can run the wizard again to create additional virtual servers and settings. Each additional virtual server must have a unique IP address and port number.

This procedure assumes you have already obtained and installed a secure server certificate on NetScaler Gateway. For more information, see the following topics: and

- Creating a Certificate Signing Request on NetScaler Gateway on page 50
- To pair the signed certificate with a private key on page 52

How you start the Quick Configuration wizard depends what you select when you log on.
If you select NetScaler Gateway, the Home tab appears from which you can configure settings to App Controller.

If you select NetScaler ADC, the Home tab does not appear. You configure the settings to App Controller by using the link Configure NetScaler Gateway for Enterprise Store on the NetScaler Gateway logon page.

To configure settings with the Quick Configuration wizard

1. In the configuration utility, do one of the following:
   a. If you select NetScaler Gateway when you log on, click the Home tab and then click Create New NetScaler Gateway.
   b. If you select NetScaler ADC when you log on, on the Configuration tab, in the navigation pane, click NetScaler Gateway and then in the details pane, under Getting Started, click Configure NetScaler Gateway for Enterprise Store.

2. In NetScaler Gateway Settings, configure the following:
   a. In Name, type a name for the virtual server.
   b. In IP address, type the IP address for the virtual server.
   c. In Port, type the port number. The default port number is 443.
   d. Select Redirect requests from port 80 to secure port to allow user connections from port 80 to go to port 443.
   e. If you select Redirect requests from port 80 to secure port, Gateway FQDN appears. Enter the fully qualified domain name (FQDN) that is contained in the certificate you bind to this virtual server.

3. Click Continue.

4. On the Certificate page, do one of the following:
   a. Click Choose Certificate and then in Certificate, select the certificate.
   b. Click Install Certificate and then in Choose Certificate and in Choose Key, click Browse to navigate to the certificate and private key.
   c. Click Use Test Certificate and then in Certificate FQDN enter the FQDN contained in the test certificate.

5. Click Continue.

6. In Authentication Settings, do the following:
   a. In Primary Authentication, select LDAP or RADIUS.
   b. Select an authentication server or configure the settings for the authentication type you selected in the previous step.
   c. If you are using two-factor authentication, in Secondary Authentication, select the authentication type and then configure the authentication server settings.
Configure the RADIUS policy as the primary authentication type and LDAP as the secondary. When users log on, they receive a prompt for their LDAP credentials and then their RADIUS credentials.

7. Click Continue.

When you finish configuring the network and authentication settings, you can then configure XenMobile (App Controller) or XenApp / XenDesktop (StoreFront or Web Interface) settings.

To configure LDAP authentication settings in the Quick Configuration wizard

1. In **Primary Authentication**, select **LDAP** and then click **Configure New**.
2. In **IP Address** and **Port**, type the IP address and port number of the LDAP server.
3. In **Base DN (location of users)**, type the base DN under which users are located.
   The base DN is usually derived from the Bind DN by removing the user name and specifying the group where users are located. Examples of syntax for base DN are:
   
   ```
   ou=users,dc=ace,dc=com
   cn=Users,dc=ace,dc=com
   ```

4. In **Administrator Bind DN**, type the administrator bind DN for queries to the LDAP directory.
   Examples for syntax of bind DN are:
   
   ```
   domain/user name
   ou=administrator,dc=ace,dc=com
   user@domain.name (for Active Directory)
   cn=Administrator,cn=Users,dc=ace,dc=com
   ```

   For Active Directory, the group name specified as `cn=groupname` is required. The group name that you define in NetScaler Gateway and the group name on the LDAP server must be identical.

   For other LDAP directories, the group name either is not required or, if required, is specified as `ou=groupname`.

   NetScaler Gateway binds to the LDAP server using the administrator credentials and then searches for the user. After locating the user, NetScaler Gateway unbinds the administrator credentials and rebinds with the user credentials.

5. In **Server Logon Name Attribute**, type the attribute under which NetScaler Gateway should look for user logon names for the LDAP server that you are configuring. You can use either `samAccountName` or `userPrincipalName`.

6. In **Password** and **Confirm Password**, type the administrator password for the LDAP server and then click **Continue**.
To configure RADIUS authentication settings in the Quick Configuration wizard

You can configure NetScaler Gateway to authenticate user access with one or more RADIUS servers. If you are using RSA SecurID, SafeWord, or Gemalto Protiva products, each of these is configured by using a RADIUS server.

Your configuration might require using a network access server IP address (NAS IP) or a network access server identifier (NAS ID). When configuring NetScaler Gateway to use a RADIUS authentication server, use the following guidelines:

- If you enable use of the NAS IP, the appliance sends its configured IP address to the RADIUS server, rather than the source IP address used in establishing the RADIUS connection.
- If you configure the NAS ID, the appliance sends the identifier to the RADIUS server. If you do not configure the NAS ID, the appliance sends its host name to the RADIUS server.
- When you enable the NAS IP, the appliance ignores any NAS ID that is configured using the NAS IP to communicate with the RADIUS server.

1. In Primary Authentication, select RADIUS and then click Configure New.
2. In IP Address and Port, type the IP address and port number of the RADIUS server. The default port is 1812.
3. In Secret Key and Confirm Secret Key, type the RADIUS server secret and then click Continue.

Configuring Enterprise Store Settings

After you configure authentication settings, you can configure the connection to App Controller. NetScaler Gateway supports user access to web, SaaS, and mobile apps and ShareFile only through App Controller.

When you click Continue from the preceding procedure, you can then configure the App Controller FQDN.

After you create the virtual server, editing the virtual server in the Quick Configuration wizard does not allow you to change XenMobile or XenApp/XenDesktop settings.

For example, if you cancel the configuration of a virtual server at any stage before configuring the Citrix Enterprise Store settings, the wizard automatically selects the Web interface without configuring any settings. When this situation occurs, you can edit the virtual server details for configuring the Web Interface, but you cannot switch to XenMobile. To switch, you must create a new virtual server and must not cancel the wizard at any time during the configuration. If you do not need the Web Interface virtual server, you can delete it by using the Quick Configuration wizard.

To configure settings for App Controller only

1. Click XenMobile.
2. In **App Controller FQDN**, enter the FQDN for App Controller.
3. Click **Done**.

**To configure Web Interface settings**

1. In the Quick Configuration wizard, click **XenApp / XenDesktop**.
2. In **Deployment Type**, select **Web Interface** and then configure the following:
   a. In **XenApp Site URL**, type the complete IP address or FQDN of the Web Interface.
   b. In **XenApp Services Site URL**, type the complete IP address or FQDN of the Web Interface with the PNAgent Path. You can enter the default path or enter your own path.
   c. In **Single Sign-on Domain**, enter the domain to use.
   d. In **STA URL**, type the complete IP address or FQDN of the server running the STA.
3. Click **Done**.

After you run the Quick Configuration Wizard, you need to do the following:

- If you configure a RADIUS authentication policy, you need to set the **Credential Index** to **SECONDARY** on the **Client Experience** tab in the operation system profile. For more information, see **To set the credential index** on page 61.
- Configure an intranet application and set it to transparent. For more information, see **Configuring Intranet Applications** on page 62.
- Configure DNS suffixes. For more information, see **Configuring a DNS Suffix** on page 65.
- Configure split DNS settings for Android devices. For more information, see **Supporting DNS Queries by Using DNS Suffixes for Android Devices** on page 64.

**To set the credential index**

If you configure two-factor authentication with LDAP and RADIUS authentication policies, you need to set the credential index in the operating system session profile to make the RADIUS authentication policy secondary.

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click **Session**.
2. In the details pane, on the **Profiles** tab, select the operation system profile and then click **Open**.
   For example, in the following figure, select **ACT_OS_10.199.242.65**.
3. In the session profile, click the **Client Experience** tab.

4. In **Credential Index**, click **Override Global**, select **SECONDARY** and then click **OK** as shown in the following figure.

![Configuring Intranet Applications](image)

**Configuring Intranet Applications**

You create intranet applications for user access to resources by defining the following:

- Access to one IP address and subnet mask
- Access to a range of IP addresses

When you define an intranet application on NetScaler Gateway, the NetScaler Gateway Plug-in for Windows intercepts user traffic that is destined to the resource and sends the traffic through NetScaler Gateway.

Intranet applications do not need to be defined if the following conditions are met:
- Interception mode is set to transparent
- Users are connecting to NetScaler Gateway with the NetScaler Gateway Plug-in for Windows
- Split tunneling is disabled

When configuring an intranet application, you must select an interception mode that corresponds to the type of plug-in software used to make connections.

**Note:** You cannot configure an intranet application for both proxy and transparent interception. To configure a network resource to be used by both the NetScaler Gateway Plug-in for Windows and NetScaler Gateway Plug-in for Java, configure two intranet application policies and bind the policies to the user, group, virtual server, or NetScaler Gateway global.

### To create an intranet application for one IP address

1. In the configuration utility, click the **Configuration** tab and then in the navigation pane, click **NetScaler Gateway**.
2. In the details pane, under **Policy Manager**, click **Change group settings and user permissions**.
3. In the NetScaler Policy Manager, under **Available Policies / Resources**, click **Intranet Applications**.
4. Under **Related Tasks**, click **Create new intranet application**.
5. In **Name**, type a name for the profile.
6. Under **Options**, next to **Interception Mode**, select **Transparent**.
7. In **Protocol**, select the protocol that applies to the network resource.
8. Under **Destination**, click **Specify an IP Address and Netmask**.
9. In **IP Address**, type the IP address and in **Netmask**, type the subnet mask, click **Create** and then click **Close**.

### To configure an IP address range

If you have multiple servers in your network, such as web, email, and file shares, you can configure a network resource that includes the IP range for network resources. This setting allows users access to the network resources contained in the IP address range.

1. In the configuration utility, click the **Configuration** tab and then in the navigation pane, click **NetScaler Gateway**.
2. In the details pane, under **Policy Manager**, click **Change group settings and user permissions**.
3. In the NetScaler Policy Manager, under **Available Policies / Resources**, click **Intranet Applications**.
4. Under **Related Tasks**, click **Create new intranet application**.
5. In **Name**, type a name for the profile.

6. Under **Options**, next to **Interception Mode**, select **Transparent**.

7. In **Protocol**, select the protocol that applies to the network resource.

8. Under **Destination**, click **Specify an IP Address Range**.

9. In **IP Start**, type the starting IP address and in **IP End**, type the ending IP address, click **Create** and then click **Close**.

### Supporting DNS Queries by Using DNS Suffixes for Android Devices

When users establish a Micro VPN connection from an Android device, NetScaler Gateway sends split DNS settings to the user device. NetScaler Gateway supports split DNS queries based on the split DNS settings you configure. NetScaler Gateway can also support split DNS queries based on DNS suffixes you configure on the appliance. If users connect from an Android device, you must configure DNS settings on NetScaler Gateway.

Split DNS works in the following manner:

- If you set split DNS to **Local**, the Android device sends all DNS requests to the local DNS server.

- If you set split DNS to either **Remote** or **Both**, the Android device sends the DNS request based on the DNS suffixes. The setting **Both** is the default setting. If the DNS request ends with one of the configured DNS suffixes, the request is sent to NetScaler Gateway for resolution; otherwise, the request is sent to the local DNS server. For this reason, you must configure the DNS suffix when you set split DNS to **Remote** or **Both**.

- If a **DNS A record** query matches the NetScaler Gateway fully qualified domain name (FQDN) to which users connect with a VPN connection, the user device replies with a cached local DNS server response. For example, if users establish a VPN connection to mycompany.ng.com and if the user device makes a DNS request for mycompany.ng.com, the DNS response comes from the cached DNS response. This is true even if the NetScaler Gateway FQDN matches the configured DNS suffix. If the DNS query does not contain a domain name, DNS requests are sent to NetScaler Gateway for resolution. For example, a user is connecting to an internal web site, such as mycompany and the DNS query is sent to NetScaler Gateway for resolution. If you configure split DNS to either **Both** or **Remote**, if users enter the full FQDN, mycompany.nginternal.com, the DNS resolution occurs based on the DNS suffix.

- If the DNS query is not a DNS A record, the DNS query strictly follows the NetScaler Gateway split DNS setting.

For more information about configure DNS suffixes, see **Configuring a DNS Suffix** on page 65.

### To configure split DNS globally on NetScaler Gateway

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under Settings, click Change global settings.

3. On the Client Experience tab, click Advanced Settings.

4. On the General tab, in Split DNS, select Both, Remote, or Local and then click OK.

To configure split DNS in a session policy on NetScaler Gateway

1. In the configuration utility, click the Configuration tab and then in the navigation pane, click NetScaler Gateway.

2. In the details pane, under Policy Manager, click Change group settings and user permissions.


4. Under Related Tasks, click Create new session policy.

5. In Name, type a name for the policy.

6. Next to Request Profile, click New.

7. In Name, type a name for the profile.

8. On the Client Experience tab, click Advanced.

9. On the General tab, next to Split DNS, click Override Global, select Both, Remote, or Local and then click OK.

10. In the Create Session Policy dialog box, next to Named Expressions, select General, select True value, click Add Expression, click Create and then click Close.

Configuring a DNS Suffix

When a user logs on to NetScaler Gateway and is assigned an IP address, a DNS record for the user name and IP address combination is added to the NetScaler Gateway DNS cache. You can configure a DNS suffix to append to the user name when the DNS record is added to the cache. This allows users to be referenced by the DNS name, which can be easier to remember than an IP address. When the user logs off from NetScaler Gateway, the record is removed from the DNS cache.

To configure a DNS suffix

1. In the configuration utility, click the Configuration tab and then in the navigation pane, click NetScaler Gateway.

2. In the details pane, under Policy Manager, click Change group settings and user permissions.


4. Under Related Tasks, click Modify session policy.

5. Next to Request Profile, click Modify.
6. On the **Network Configuration** tab, click **Advanced**.
7. Next to **Intranet IP DNS Suffix**, click **Override Global**, type the **DNS suffix** and then click **OK** three times.

### Creating a Load Balancing Server for ShareFile

The NetScaler appliance supports load balancing of multiple ShareFile StorageZone Controllers. You can configure the load balancing virtual server by using either the integrated XenMobile configuration utility or by using the ShareFile wizard in NetScaler.

When you configure the settings in NetScaler, you need the following information:

- Name of the content switching server.
- Public IP address or an IP address in the DMZ that uses network address translation (NAT) from the external firewall.
- StorageZone Connectors that support NetScaler authenticating users.
- Trusted SSL server certificate. This certificate cannot be self-signed.
- Internal IP addresses of one or more ShareFile StorageZone Controller servers.
- Protocol and ports used for communication between NetScaler and StorageZone Controllers.
- LDAP authentication settings.

You can configure LDAP authentication during the wizard. To do so, you need the following information:

- Unused internal IP address for the AAA virtual server
- IP address and port number of the LDAP server
- Domain name for single sign-on
- Base DN where users are stored in Active Directory
- Administrator Bind DN that is the email address of the service account
- Service account password

When users connect to ShareFile, the connection routes to the Content Switching virtual server and then to the load balancing servers. These servers pass the connection to the StorageZone controllers as shown in the following figure:

**Figure 4-1. Deploying NetScaler and ShareFile**
Configuring ShareFile StorageZone Connector Settings in NetScaler

You can configure ShareFile settings in NetScaler in the following ways:

- Select **XenMobile** when you log on to NetScaler. With this option, the **Home** tab appears and the XenMobile configuration links appear on the right side of the details pane.

- Select **NetScaler ADC** when you log on to NetScaler. With this option, the **Home** tab does not appear. You use the **Traffic Management** node to configure ShareFile settings.

**To configure ShareFile settings on the Home tab**

1. On the NetScaler logon page, in **Deployment Type**, select XenMobile and then log on.

2. On the **Home** tab, under **ShareFile LB**, click **Configure**.

3. On the **Setup Load Balancing for ShareFile** page, do the following:
   a. Under **ShareFile Configuration**, in **Name**, enter the name of the content switching server.
   b. In **IP Address**, enter the public IP address or an IP address in the DMZ that uses network address translation (NAT) from the external firewall.
   c. Click **StorageZone Connector for Network File Shares/SharePoint** and then click **Continue**.

4. Under **Certificate**, do one of the following:
   a. On the **Choose Certificate** tab, select the secure server certificate and then click **Continue**.
   b. On the **Install Certificate** tab, in **Certificate** and **Key**, click **Browse** and navigate to the certificate and private key. Click **Continue**.

   **Note:** Citrix recommends that you use a certificate from a trusted Certificate Authority and not a self-signed certificate.

5. On the **ShareFile StorageZone Controller Configuration** page, do the following:
   a. In **StorageZone Controller IP Address**, enter the IP address.

   **Note:** To add more StorageZone Controller IP addresses, click the plus (+) sign next to **StorageZone Controller IP Address**.

   b. In **Port**, enter the port number. The default is 443.
   c. In **Protocol**, select between secure (HTTPS) and unsecure (HTTP) web browsing, click **Create** and then click **Done**.

6. Under **LDAP Authentication Settings**, do the following:
a. In **AAAVServer IP Address**, enter a unique IP address for the AAA virtual server.

b. In **LDAP Server IP Address** and **Port**, type the IP address and port number of the LDAP server. The default port number is 389.

c. In **Single Sign-on Domain**, enter the domain to which users log on, such as mydomain.net.

d. In **Base DN (location of users)** type the base DN under which users are located.

   The base DN is usually derived from the Bind DN by removing the user name and specifying the group where users are located. Examples of syntax for base DN are:

   ```
   ou=users,dc=ace,dc=com
   cn=Users,dc=ace,dc=com
   ```

e. In **Administrator Bind DN**, type the administrator bind DN for queries to the LDAP directory. Examples for syntax of bind DN are:

   ```
   domain/user name
   ou=administrator,dc=ace,dc=com
   user@domain.name (for Active Directory)
   cn=Administrator,cn=Users,dc=ace,dc=com
   ```

   For Active Directory, the group name specified as `cn=groupname` is required. The group name that you define in NetScaler Gateway and the group name on the LDAP server must be identical.

   For other LDAP directories, the group name either is not required or, if required, is specified as `ou=groupname`.

   NetScaler Gateway binds to the LDAP server using the administrator credentials and then searches for the user. After locating the user, NetScaler Gateway unbinds the administrator credentials and rebinds with the user credentials.

   f. In **Password** and **Confirm Password**, type the administrator password for the LDAP server, click **Continue** and then click **Done**.

   After you configure all of the settings, the **Home** tab appears and shows the ShareFile configuration.

**To configure ShareFile settings in the configuration utility**

1. On the NetScaler logon page, in **Deployment Type**, select **NetScaler ADC** and then log on.

2. On the **Configuration** tab, in the navigation pane, expand **Traffic Management** and then click **Load Balancing**.

3. In the details pane, under **Citrix ShareFile**, click **Setup NetScaler for ShareFile**.

4. Follow Steps 3 through 6 in the preceding procedure.
Installing Device Manager

Before you install Device Manager, make sure you do the following:

- Disable TCP/IP6 on the network adapter and in the registry. For more information, see How to disable IP version 6 or its specific components in Windows on the Microsoft web site.
- Disable the User Account Control setting in Control Panel.

**Caution:** Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

The setup wizard includes several discrete tasks. You need to complete the all of the tasks in this topic in consecutive order to complete the entire wizard. The installation tasks include:

- Device Manager components
- Installation location
- PostgreSQL database installation
- Database cluster settings
- Licenses
- Device Manager and database communication
- Crystal Reports keycode
- HTTP and HTTPS connectors
- Root and server certificates
- Apple Push Notification Service (APNS) certificates
- Remote support settings
- Active Directory service account for managing users

**To select Device Manager components**

After you download the software package to your computer, navigate to the folder and then double-click the Device Manager executable installation file to start the Setup Wizard.

When the wizard starts, you set the language and then read and accept the End User License Agreement. After these two steps, on the **Choose Components** page, click to clear **Database server** to disable installation of the PostgreSQL database.
Important: Citrix recommends that you use Microsoft SQL Server instead of the PostgreSQL database that comes with Device Manager. The PostgreSQL database should be used for demonstration purposes only.

After you select your components, on the Choose Install Location page, leave the default install location and then click Install. Citrix recommends that you use the default location to install Device Manager.

To install the license on Device Manager

Device Manager requires a license. For more information about licenses for Device Manager, see Obtaining and Installing Licenses on page 31. You upload the .crt license from your computer. When the upload is complete, the license details appear in the XenMobile Device Manager License dialog box.
To test the connection to the database from Device Manager

You need to configure the Device Manager settings to connect to your database. In the Configure database connection dialog box, you select the SQL Server database. You provide the database name or use the default value. You need to complete the following information, as shown in the following figure:

- In Host name or IP address, enter the fully qualified domain name (FQDN) or IP address of SQL Server.
- In Port, enter the port number. The default port number for SQL Server is 1433.
- In User name, enter a user name for the database.
- In Password, enter the password to connect to the SQL Server database.
- In Database name, enter the database name or leave the default value.

After you configure the database connection, you then enter the keycode for Crystal Reports.

To configure and register Crystal Reports

With Crystal Reports, you can process the mobile device connection and session logs to generate activity reports online by using the Device Manager web console, or offline from the Device Manager repository database. The reports include a watermark with registration information. To remove the watermark, you need a Crystal Reports Developer Edition license and a keycode for the product. If you did not enter a license serial number during installation, you can define it later by following these steps:

1. Open the crconfig.xml configuration file located at in the Device Manager setup folder, which is typically %systemroot%\Program Files\Xenmobile\tomcat\webapps \Device Manager\WEBINF\classes\crconfig.xml on a Windows Server.
2. Add your serial number by editing the `<keycode></keycode>` element. For example, if your serial number is XXXX-YYYY-ZZZZ, modify the line as follows:

`<keycode>XXXX-YYYY-ZZZZ</keycode>`

On the Crystal Report Java Reporting Components configuration page, to leave a watermark on the reports, leave the `keycode` blank. Or, to remove the watermark, enter your keycode for the product.

**To configure the server connectors**

When you configure the connection between the Device Manager agent and the Device Manager server, you can configure the following connectors, which require the same information but serve different purposes:

- If you manage IOS devices, select Enable iOS. When you select the checkbox, the authentication code appears automatically. In **Authentication code for applications/tunnels**, enter a prefix that Device Manager uses to create authentication keys used by the software. Use a simple alphanumeric word or passphrase. Use mixed case, numbers, and letters only. Then, record this value for use later when you configure the system.

  **Important:** You can only select **Enable iOS** during installation. If you do not select this option and you want to enable the mode in the future, you must reinstall the application server.

- HTTP connector that allows unsecure connections over port 80. You can configure this connector if NetScaler Gateway is installed between the Device Manager server and mobile devices.

- HTTPS connector for secure connections over port 443 with a certificate.
HTTPS connector that allows secure connections over port 8443 for device enrollment.

When you configure connectors, you set the following parameters:

- Protocol for secure and unsecure connections (HTTP or HTTPS).
- IP addresses.
- Port settings for the connector. To allow connections over HTTPS and that use certificates for authentication, you use port 443. For secure connections without certificates, use port 8443. For unsecure connections use port 80.
Maximum concurrent connections defines the total amount of user connections that are allowed for each connector.

**To configure root and server certificates in Device Manager**

Device Manager supports root, server, and APNS certificates. Root certificates enable Device Manager to communicate with other XenMobile components. Server certificates enable secure communication between Device Manager and devices.

The installation wizard prompts you to install a root certificate from a Certificate Authority (CA) first and then the server certificate. For each certificate, you provide the following information:

- **Keystore file path** is the certificate location on your computer. Do not change the default path. The server configuration provides the file path automatically.

- **Keystore password** and **Confirm keystore password** is for the private key. Enter the private password used for each component of the local CA. Although you can use the same password for each CA keystore component, Citrix recommends using separate passwords for the root, server, device, and Web Service certificates. Passwords must have at least eight characters, and can consist of alphanumeric and ASCII symbol values. Passwords are case sensitive.

- **Organizational unit** is an optional parameter. Enter a value typically given to the entity or group that has management authority over the certificate.

- **Organization** is an optional parameter. Enter a value typically given to the entity or organization that is the parent that owns the certificate and its rights.

For root certificates, you need to provide the common name for the CA that issued the root certificate. Leave the default name to associate it with the creation of the CA component and certificate. If you change this field, your devices may not receive the proper chain of certificates and will not be able to enroll.

**Note:** The root certificate is used to issue and sign certificates for intermediate server and client-device certificates. The root certificate is also used to regenerate intermediate certificates in the event of compromise. You can install root certificates in the operating system as a trusted CA root certificate.
For secure server certificates, you need to include the IP address or FQDN that is in the certificate. Users connect by using the IP address or FQDN contained within the certificate.

To install an APNS certificate in Device Manager

To allow users to connect from iOS devices, you must install an APNS certificate from Apple. When you install the certificate on Device Manager, you enter the associated private key password used to generate the original Certificate Signing Request (CSR) in the field in **Private key password**.
In **Certificate file** path, specify the file system location of a pre-authenticated APNS certificate file that you download and convert to PKCS#12 format from the Apple iOS Developer for Enterprise portal.

**Note:** APNS certificates are provisioned by Apple, Inc. To obtain an APNS certificate, sign in to the Apple Push Certificates Portal. When you log on, you can compare the information on the Apple web site with the values shown in the following figure:

---

**Allowing Remote Support to Connect to Mobile Devices**

On the **Configure tunnel port(s) used by remote support** page, define the port range used by remote support for Android and Windows Mobile devices. The default is port 8081.
To designate the Device Manager administrator

To connect to the Device Manager web console, you need to configure an account with the administrator role.

On the Extended management of the users page, you enter the administrator’s name and password. After you enter the values, you can check the user name in Active Directory.

After you configure the administrator user and password, you can finish the installation wizard.
After you finish the wizard, you should do the following:

- Log on to the administration console at https://serverfqdn/zdm to configure Device Manager.
- On the console, use the first-time use wizard to configure LDAP and your first deployment package.

**Note:** If you want to add your own server certificate instead of the self-signed server certificate that is issued during the installation, follow the steps in this topic, Configuring an External Certificate Authority by Using SSL.

### Configuring Active Directory on Device Manager

You use Active Directory with Device Manager to manage groups of users, not individual user accounts. Device Manager supports the following sources of user account information:

- **LDAP directory.** You can configure Device Manager to read an LDAP-compliant directory, such as Active Directory to import groups, user accounts, and related properties.

- **Manual entry.** You can use group maintenance forms in Device Manager to quickly create user accounts.

- **Provisioning file.** You can develop a file outside of Device Manager containing user accounts and properties and then import the file. Device Manager automatically creates objects and sets properties values.

You can perform the following actions in Device Manager for LDAP connections:

- Create a new LDAP connection.
- Edit an existing connection.
- Set the default LDAP connection.
- Activate or deactivate an LDAP connection.

When you create a new LDAP connection, you configure the LDAP directory settings and then you import a signed secure certificate. When you define the connection parameters, you need to grant the following rights to the Search User service account:

```
READALLUSERINFORMATION
READALLNETWORKPERSON
```

**Note:** In the Lockout Limit field, the default is set to zero. However, Citrix recommends using a higher value, as well as a value that is slightly lower than the lockout limit set on your LDAP server. For example, if your LDAP server is configured to a limit of five attempts before lockout, Citrix suggests that you enter a 3 or 4 in this field.

You can also map the LDAP directory attributes to the Device Manager Repository database. If you do not modify the default settings, Device Manager binds
automatically to the LDAP directory. You can specify the base DN that defines the LDAP directory groups that are imported to Device Manager.

### Installing App Controller

The App Controller virtual machine (VM) runs on Citrix XenServer, Microsoft Hyper-V, or VMware ESXi. You can use XenCenter or vSphere management consoles to install App Controller 2.8.

You install App Controller on the hypervisor and then configure initial settings by using the command line. Then, you log on to the App Controller management console and configure settings with the Configure wizard.

For information about installing App Controller on your hypervisor, see the following topics in the App Controller documentation in Citrix eDocs:

- *Installing App Controller on XenServer*
- *Installing App Controller by Using VMware ESXi*
- *Installing App Controller on Microsoft Hyper-V*

This section discusses configuring App Controller for the first time by using the command-line console and the management console.

### Setting the App Controller IP Address for the First Time

After you import the App Controller software to your hypervisor, you use the Express Setup command line to configure the App Controller initial settings as shown in the following figure:
The initial settings include:

- IP address and subnet mask, which is the management address to connect to the management console
- Default gateway IP addresses
- DNS servers
- Network Time Protocol (NTP) server

The default IP address for App Controller is 10.20.30.40.
To change the IP address for App Controller in XenCenter

1. In XenCenter, select the App Controller virtual machine and then click the Console tab.

2. At the console logon prompt, enter the administrator credentials.
   The default user name for the console is admin and the default password is password.

3. At a command prompt, type 0 to select Express Setup.

4. Select the appropriate number to change the IP address, subnet mask, default gateway, DNS servers, and NTP server.
   
   **Note:** Citrix recommends using an NTP server to set the date and time on App Controller.

5. Press 5 to commit the changes.

When you commit the changes, you are prompted to restart App Controller. Review your settings and then type y to commit the changes. After App Controller restarts, you can then access the management console by using the new IP address in a web browser. To open the management console, type https://App ControllerIPaddress:4443/ControlPoint in the address bar of the web browser. For example, type https://10.20.30.40:4443/ControlPoint. The user name is administrator and the password is password.

When you connect to App Controller, you must use HTTPS. If you attempt to connect with HTTP, the connection fails.

Configuring App Controller for the First Time in the Management Console

After you install the App Controller virtual machine (VM) and configure the initial settings by using the command-line console, you can configure additional App Controller network settings in the App Controller management console. When you log on to the management console for the first time, the Configure wizard appears.
The wizard prompts you to configure settings that include the following:

- Administrator password
- App Controller host name, IP address, subnet mask, and default gateway

**Note:** You can also configure an IP address for App Controller if you want a different IP address than what you configured by using the command-line console.

- Active Directory settings
- Certificates

**Note:** In the **Configure** wizard, you can add, create, or remove certificates on the Active Directory page. The option to configure certificates from the Active Directory page appears only when you configure App Controller for the first time in the management console. After you run the **Configure** wizard for the first time, you can then manage certificates from the **Settings** tab in the management console.

- Network Time Protocol (NTP) server and time zone
- DNS server settings
- Workflow email settings

**Important:** For workflows to work correctly, when you add users to Active Directory, you must enter the first name, last name, and email in the user properties. If you do not configure users in Active Directory with this information, App Controller cannot synchronize these individuals. When users attempt to start an app, users receive a message that they are not authorized to use the app.
After you configure and save the remaining network settings in the management console, App Controller retrieves users from Active Directory and then logs off. If you changed the password, log on again with the new password.

**Important:** If you have a large number of users or groups, it might take a few hours for App Controller to retrieve users. You cannot make any changes to App Controller until this process is complete. If you close the browser, interrupt the synchronization and then restart the Configure wizard in another web browser, your settings are not saved. Citrix recommends that you allow the Active Directory synchronization to complete. When you configure the App Controller settings for the first time, you can enter a group domain name (DN) that speeds the synchronization of Active Directory membership with App Controller.

### Installing Certificates

App Controller requires root and server certificates to communicate in the following ways:

- Between App Controller and the App Controller management console
- Between applications and App Controller
- Between App Controller and StoreFront

**Note:** You can only install Privacy Enhanced Mail (PEM) and Personal Information Exchange (.pfx) certificate files on App Controller.

You need to install multiple certificates on App Controller to facilitate secure communication. Each certificate serves a specific communication purpose.

App Controller requires the following three certificates:

- Secure SSL server certificate that is used for secure connections to the management console and for communicating with StoreFront
- Secure SSL server certificate for communicating between App Controller and applications that require an SSL certificate for user account management
- Secure SSL certificate for communication between App Controller and SAML applications that require an SSL certificate

If you configure a SAML application in App Controller, such as Google Apps, you might need to upload a SAML certificate to App Controller. For more information about SAML certificates, see the application documentation.

### Installing a Signed Server Certificate and Private Key on App Controller

App Controller includes a server certificate that is not signed by a trusted Certificate Authority (CA). You need to install on App Controller a digital X.509 server certificate that belongs to your company and is signed by a CA. Your company can operate as its own CA, or you can obtain a digital signed server certificate from a commercial CA, such as VeriSign or Thawte.
App Controller accepts a Privacy Enhanced Mail (PEM) format certificate file. PEM is a text format that is the Base-64 encoding of the Distinguished Encoding Rules (DER) binary format. The PEM format specifies the use of text `BEGIN` and `END` lines that indicate the type of content that is being encoded.

You can install a secure digital certificate and private key on App Controller in the following two ways:

- **Generate a Certificate Signing Request (CSR) by using the App Controller management console.** When App Controller generates the CSR, App Controller creates a certificate and private key. The private key remains on App Controller and the certificate contents are copied and submitted to a CA web site for signing. When the signed certificate is returned, you install the certificate on App Controller. During installation, the signed certificate is paired with the password-protected private key. Citrix recommends that you use this method to create and install secure certificates.

- **Install a PEM certificate and private key from a Windows-based computer.** By using this method, you upload a signed certificate and private key together. The certificate is signed by a CA and is paired with the private key.

**To create a CSR**

To provide secure communication by using SSL or TLS, a server certificate is required on App Controller. Before you can upload a certificate to App Controller, you need to generate a CSR and private key. You configure settings as shown in the following figure.
1. In the App Controller management console, click the Settings tab.

2. In the left panel, under System Configuration, click Certificates.

3. In the Certificates panel, click New and in Certificate Signing Request, type the required information:
   - In Key Length (required), select the encryption strength.
   - In Common name (required), type the host name or the fully qualified domain name (FQDN) of App Controller as it appears on the Network Connectivity panel.
   - In Email, type the email address for the contact person at your company.
   - In Description, type a description for the CSR.
   - In Company name, type the name of your company or organization.
   - In Department name, type the name of the department that will use the certificate.
• In City, type the name of the city in which your company or organization is located.
• In State, type the full name of the state where your company is located.
• In Country Code (required), select the code for your country, such as United States.

4. Click Save.

App Controller creates the CSR. A dialog box that contains the contents of the CSR opens.

5. Copy the certificate contents from the dialog box and then paste the content into the appropriate area on the Certificate Authority web site.

The certificate provider returns a signed certificate to you by e-mail. When you receive the signed certificate, install it on App Controller.

You can create up to three CSRs. You can view or delete existing CSRs, and you can also choose to sign a CSR so that you can use the certificate immediately.

**To import a signed server certificate to App Controller**

When you receive the signed certificate from the Certificate Authority (CA), you can upload the certificate to App Controller. The file can be a Privacy Enhanced Mail (PEM) or Personal Information Exchange (PKCS#12) file, which includes both a server certificate and its password-protected private key.

1. In the App Controller management console, click the Settings tab.
2. In the left pane, under System Configuration, click Certificates.
3. Click Import and then select Server (.pem) to import a CA signed root certificate.
4. In the Upload dialog box, click Browse, navigate to the certificate and then click Open.

**Installing Root Certificates on App Controller**

After the Certificate Authority (CA) signs your server certificate, the CA returns it to you. If the CA provides the server certificate in PEM format, the CA might also send the root certificate. You need to install the root certificate on App Controller along with the server certificate.

You might also need to install root certificates for applications you configure on App Controller. Each root certificate must match the fully qualified domain name (FQDN) of the server running the application.

**To install a root certificate**

1. In the App Controller management console, click the Settings tab.
2. In the left pane, under System Configuration, click Certificates.
3. Click Import and then select Trusted (.pem) to import a CA-signed root certificate.
4. In the **Upload** dialog box, click **Browse**, navigate to the certificate and then click **Open**.

**To link server and root certificates**

After you import server and root certificates to App Controller, link the certificates together.

1. In the App Controller management console, click the **Settings** tab and then click **Certificates**.
2. Select the server certificate and then click **Add to Chain**.
3. Select the root certificate and then click **OK**.
   
The server certificate is linked to the root certificate.
4. Click on the server certificate again and click **Make Active**.

When you activate the server certificate, App Controller logs off from the management console. When you log on again, check to make sure the correct certificate appears in your web browser. You must log on by using the fully qualified domain name (FQDN) to the management console. For directions on how to check the certificate in your browser, see the manufacturer's documentation.

### Configuring Applications and Trust Settings for NetScaler Gateway

If you have an application that runs on a server in your internal network and users who connect from the Internet, you can configure trust settings in App Controller to route the connection through NetScaler Gateway. You also configure the application connector to indicate that the application is hosted in your internal network. When users connect to the application, NetScaler Gateway routes the request to App Controller. The application then starts on the user device. For more information about configuring application connectors in App Controller, see *[Configuring Applications for Single Sign-On]*.

**To configure connections to NetScaler Gateway**

1. In the App Controller management console, click the **Settings** tab.
2. Under **System Configuration**, click **Deployment**.
3. In the details pane, under **NetScaler Gateway**, click **Edit**.
4. In **Enable**, click **Yes**.
5. In **Display name**, type the NetScaler Gateway name.
6. In **Callback URL** and **External URL**, enter the NetScaler Gateway Web address. For example, enter https://mynetscalergateway.com.
   
   You can specify the port number in the web address, such as https://mynetscalergateway.com:443.
   
   When you add the web address to **Callback URL**, App Controller appends the URL automatically with the NetScaler Gateway authentication service URL. For
example, the URL appears as https://NetScalerGatewayFQDN/CitrixAuthService/AuthService.asmx.

7. Optionally, in Logon type, select one of the following:
   - **Domain only.** This setting requires users to enter their Active Directory credentials.
   - **Security token only.** This setting requires users to enter the code from a security token, such as an RSA token.
   - **Domain and security token.** This setting requires user to enter domain credentials and the code from a security token.

8. Optionally, select the **Do not require passwords** check box if you do not want to require users to enter a password.

9. Click **Save**.

**To configure an application to allow NetScaler Gateway connections**

1. In the management console, click the **Apps & Docs** tab.

2. Do one of the following:
   a. To edit an app, in the right pane, click an application from the list of **All Apps** and then click the pencil icon to edit the application.
   b. To add an app, in the left pane, under **Applications**, click **Web & SaaS**, click the Plus sign and then click an application from the catalog.

3. On the **Details** page, select **App is hosted in internal network**.

4. Click **Next**, configure settings on each subsequent page and then click **Save**.

**Configuring App Controller to Provide STA Tickets for WorxMail**

App Controller provides a ticketing service that is similar to the Secure Ticket Authority (STA) in XenApp and XenDesktop. WorxMail uses the ticketing service to allow users to stay connected for long periods of time without requiring them to authenticate multiple times.

App Controller and NetScaler Gateway work together to provide the ticketing service for users’ connections. You configure settings on NetScaler Gateway and then configure policy settings for WorxMail on App Controller.

To allow connections through NetScaler Gateway, you must configure the following on the appliance:

- Virtual server that uses the SOCKS protocol for ICA connections
- STA

When you configure the STA on NetScaler Gateway, you add the App Controller IP address or fully qualified domain name (FQDN) as the STA to the URL. For example,
https://myApp_Controller/ where myApp_Controller is the IP address or FQDN of App Controller. You also need to define ports 80 and 443 to allow connections. For more information about configuring the STA in NetScaler Gateway, see Configuring the Secure Ticket Authority on NetScaler Gateway.

You configure the following settings in App Controller:

- **WorxMail Exchange Server** that is the FQDN of the Exchange server in the internal network.
- **WorxMail user domain** that is your domain name.
- **Background network services** that is a list of servers and ports. An empty list implies that users do not have access to background services.
- **Background services ticket expiration** that is the amount of time before the ticket expires. Enter the number of days that the ticket is valid.
- **Background network service gateway** is the alternate virtual server address and port on NetScaler Gateway that is used to connect by using the SOCKS protocol.

Tickets issued by App Controller are not intended for one time use. The setting **Background services ticket** defines how long the ticket is valid. When WorxMail sends the ticket to NetScaler Gateway for SOCKS connectivity, WorxMail might append a #fqdn:port parameter to the end of the ticket to identify to which server and port App Controller prefers to connect.

**To configure WorxMail ticketing in App Controller**

This procedure assumes that you have already installed WorxMail in App Controller.

1. In the App Controller management console, click the **Apps & Docs** tab.
2. Do one of the following:
   - To open WorxMail for iOS, in the navigation pane, click iOS MDX.
   - To open WorxMail for Android, in the navigation pane, click Android MDX.
3. In the details pane, click **WorxMail** and then click the pencil icon in the dialog box.
4. Click **Next** until you come to the **Policies** page.
5. Under **Application Settings**, do the following:
   a. In **Worx Exchange Server**, type the path to your Exchange server in the secure network.
   b. In **Worx user domain**, type the domain name.
   c. In **Background network services**, enter the servers and ports. You can use the format serverFQDN:port or serverIPAddress:port. Use a comma as a separator between servers and ports.
   d. In **Background services ticket expiration** enter the number of days the ticket is valid. The default is 168 hours (7 days).
   e. In **Background network service gateway** enter the FQDN or IP address of the NetScaler virtual IP address and the port number.
6. Click Save.

**Enabling Access to Windows-Based Apps from Worx Home or Receiver**

You can configure trust settings in App Controller 2.8 to allow users to access their mobile, web, SaaS and Windows-based apps through Receiver or Worx Home. For more information about configuring the trust settings, see To configure App Controller to connect to StoreFront.

**To configure Windows App settings in App Controller**

1. In the management console, click the Apps & Docs tab.
2. In the left pane, under XenApp/XenDesktop, click Windows Apps.
3. Next to Win Apps Configuration, click Edit.
4. In Host, type the PNA site of the Web Interface or the fully qualified domain name (FQDN) or IP address of StoreFront.
   For example, enter storefront.johndoe.local.
5. In Port, enter the port of the Web Interface or for the server running StoreFront.
   The default port number is 443.
6. In Relative Path, enter the path to the Web Interface or StoreFront. For example, for the Web Interface, enter /Citrix/PNAgent/config.xml. For StoreFront, enter /Citrix/Store/PNagent/config.xml.
7. Select Allow secure access to specify an HTTPS connection.

Keep in the mind the following scenarios that occur when you configure the preceding settings and deploy StoreFront on the Settings tab in the management console:

- If you enable StoreFront, disable authentication in App Controller and then provide the StoreFront web address in App Controller, users can connect to their Windows-based apps. On the Apps & Docs tab, you configure Windows App settings by following the procedure in this topic. In this scenario, users can connect to App Controller with Worx Home and access mobile, web, SaaS, and Windows-based apps. If users connect with Receiver for Windows or Receiver for Mac, they can access apps in either StoreFront or App Controller.

**Note:** If you have users who connect from a remote location and you disable StoreFront authentication as in the first scenario, NetScaler Gateway authenticates users. To allow NetScaler Gateway to authenticate users, you need to configure authentication settings on NetScaler Gateway and configure App Controller to connect to NetScaler Gateway. For details, see Configuring Authentication on NetScaler Gateway and Configuring Connections to Enterprise Web Applications Through NetScaler Gateway.

- If you enable StoreFront and enable authentication in App Controller, you cannot configure Windows-based apps on the Apps & Docs tab. In this scenario, users...
cannot access Windows-based apps. When users connect, StoreFront authenticates
users. If users connect with Worx Home to App Controller, they have access to
mobile, web, and SaaS apps only. Users who connect with Worx Home do not have
access to Windows-based apps in StoreFront. Users who connect with Receiver must
connect to StoreFront directly to access Windows-based apps.

- If you disable StoreFront and disable authentication in App Controller, and you
  configure Windows App settings, users can access HDX apps when they connect with
  Worx Home and Receiver.

**Configuring Worx PIN Options**

When users install Worx Home, you can required them to log on by using a personal
identification number (PIN). You can configure the settings for the Worx PIN
requirement in App Controller. This feature simplifies the user authentication
experience when logging on.

When you enable this feature, it works as follows: When users log on to Worx Home for
the first time, they enter their user name and password. In addition, when they log on,
the Active Directory credentials or client certificate is saved on the user device. Then,
Worx Home prompts the user to enter a PIN. When users log on again, instead of
requiring a user name and password or a token, they type in the PIN and can access
their Worx apps. The following figure shows the screen where users enter their Worx
PIN on an iPad.

![Figure 4-2. Entering the Worx PIN on an iPad](image)

You configure Worx PIN settings on the **Settings > Support Options** page in App
Controller. You can configure the following settings:

- Enabling Worx PIN. The default is false.
- Enabling password caching. The default is false.
- Configuring the PIN complexity to require alphanumeric or numeric characters. The
default is numeric.
- Configuring the length of the PIN. The default is 6 characters.
- Configuring the length of time before users need to change their PIN. The default is
  0.

You can configure the following combinations for the PIN:
If users change their Active Directory password, the next time they log on to Worx Home, they receive an error message. Users can log on with their Active Directory credentials and then Worx Home caches the updated credentials. After that, users can log on with their PIN.

After you configure a Worx PIN, each of these settings appears on the Support Options page as shown in the following figure. You can click the pencil icon for each item to edit the settings to match your requirements.

**Figure 4-3. Configuring Worx PIN Options**

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Key</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Worx PIN Authentication</td>
<td>ENABLE_WORX_PAS_MAC</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Enable User Password Caching</td>
<td>ENABLE_PASSWORD_CACHING</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Worx PIN Complexity Requirement</td>
<td>MINPASSWORD_COMPLEXITY</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Worx PIN Length Requirement</td>
<td>MINPASSWORD_LENGTH</td>
<td>8</td>
<td>N/A</td>
</tr>
<tr>
<td>Worx PIN Change Requirement</td>
<td>MINPASSWORD_CHANGE</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

To edit Worx PIN settings

1. In the App Controller management console, click **Settings**.
2. In the navigation pane, under **System Configuration**, click **Support options**.
3. In the details pane, select an item and then click the pencil icon.
4. In the **Add Property** dialog box, do the following:
   a. In **Value**, type the value for the item.
   b. In **Name**, type a name for the item.
   c. In **Description**, type a description for the item.
5. Click **Save**.

**Enabling Connections Between Device Manager and App Controller**

If you are using Device Manager with App Controller to provide apps to your Worx Home users, you will need to configure the Device Manager server and App Controller to communicate.

For secure communication between Device Manager and App Controller, install secure signed certificates. App Controller needs to initiate communication with Device
Manager and App Controller must validate the server certificate from Device Manager. When Device Manager initiates communication with App Controller, it needs to validate the server certificate from App Controller. This handshake fails if the issuer of the certificate is not trusted on both systems.

If you select **Allow Secure Communication** in the App Controller management console, Device Manager communicates with App Controller on a secure port (for example: 443). This secure communication requires public certificates on both servers, and requires that the ports are open in both directions.

The communication between Device Manager and App Controller are RESTful API calls if the traffic occurs over port 80. The typical communication is App Controller communicating with Device Manager that the user needs an application from Worx Home. Device Manager could also contact App Controller to find out if App Controller exists and if the user is part of an Active Directory group that synchronized with App Controller.

**Note:** To allow users to connect to Windows-based apps or virtual desktops, users must have Citrix Receiver installed on their devices.

After you configure Device Manager and App Controller to communicate, you can then test the connection.

**To configure Device Manager to connect to App Controller**

**Important:** You must configure settings in Device Manager before configuring settings in App Controller.

1. Log in to the XenMobile Device Manager web console.
2. Click **Options**.
3. In the **Options** dialog box, in select **Modules Configuration > AppC Webservice API**, enter the App Controller fully qualified domain name (FQDN) and a shared key. You will enter the same shared key in App Controller.
4. Select **Enable App Controller**.
   **Note:** Do not click **Test Connectivity** until you have configure Device Manager settings in the App Controller management console.
5. Click **Save**.

**To configure App Controller to connect to Device Manager**

1. In the App Controller management console, click the **Settings** tab.
2. In the navigation pane, click **XenMobile MDM**.
3. In the details pane, next to **XenMobile Device Manager Configuration**, click **Edit**.

4. In **Host**, enter the Device Manager IP address or FQDN.

5. In **Port**, leave the default of 80 or enter your own.

6. In **Shared Key**, enter the key you configured on Device Manager.

7. Select **Allow secure access** to secure the connection between App Controller and Device Manager.

8. Select **Require Device Manager enrollment** to require that all user devices are enrolled and managed by Device Manager.

9. Click **Test Connection** to test the connection to Device Manager.
   
   If the test fails, make sure your settings in App Controller and Device Manager match.

10. Click **Save**.

### To test the connection between Device Manager and App Controller

When you finish configuring the connection in App Controller, you need to test the connection from Device Manager.

1. In the Device Manager web console, in the **Options** dialog box, select **Modules Configuration > AppC Webservice API**, and then click **Check connection** to test communication between Device Manager and App Controller.

2. When Device Manager establishes the connection, click **Close**.

### Downloading and Installing the MDX Toolkit

The Citrix MDX Toolkit is available from the [Citrix web site](https://www.citrix.com). The MDX Toolkit runs on a computer running Mac OS X Versions 10.7 (Lion), 10.8 (Mountain Lion), and 10.9 (Mavericks). The tool is not supported on a Windows-based computer.

**Important:** You must update to the latest version of Worx Home 8.6 on Android and iOS devices before you wrap apps with the 2.2.321 version of the MDX Toolkit. If not, when you try to open the apps in earlier versions of Worx Home, an incompatibility error message appears.

After you download the tool from the Citrix web site, you install the tool on your computer. When you install the tool, you are prompted for licensing, the location where you want to install the tool, and installation information.

The installation package includes a small utility for removing the MDX Toolkit. You can find the utility at the following location on your computer: `/Applications/Citrix/CGAppPrepTool/Uninstaller.app/Contents`. Double-click the utility to start the uninstaller app and then follow the prompts. When you remove the tool, you receive a message prompting you for your user name and password.
To install the MDX Toolkit

1. Click the installation package that you downloaded to your computer to start the installation and then click Continue.
2. Read and accept the End User License Agreement and then click Continue.
3. Follow the prompts to install the MDX Toolkit.

Upgrading the MDX Toolkit

To upgrade the MDX Toolkit, you must first remove earlier versions of the tool from your computer. Then, you can install the latest version.

To remove the App Preparation Tool

1. On your Mac OS X computer, navigate to the directory Go > Application > Citrix > CGAppPrepTool > Uninstaller.app.
2. Double-click the Uninstaller icon.
   A message prompts you to confirm the removal of the MDX Toolkit.
3. Click Continue.
4. Enter your user name and password, click OK and then click Done.

After you remove the earlier version of the tool, you can then install the new version of the tool.

Wrapping Android and iOS Mobile Apps

Citrix provides the MDX Toolkit so that you can wrap a mobile app for iOS or Android with Citrix logic and policies. The tool can securely wrap an app that was created within your organization or a mobile app made outside the company. When you install the MDX Toolkit, the Worx SDK libraries also install and appear in the MDX SDK folders on your computer in the tool and data directories. The MDX SDK folders are required for the integration of wrapped iOS mobile apps with Citrix Worx. When you wrap iOS apps that include the Worx SDK libraries, you can publish the apps in the Apple App Store and the Citrix Worx Store. After the app is wrapped, you can upload then the app to XenMobile App Edition. For more information about the Worx App SDK, such as an overview for ISVs, and to download the SDK, see Worx App SDK on the Citrix web site.

Prerequisites

Before you wrap an iOS app, download and install the iOS Distribution Provisioning Profile and Distribution Certificate to your computer. The provisioning profile signs the app for distribution.

Wrapping Android Mobile Apps

For Android apps, you need to follow these basic steps:
Specify an Android mobile app APK file. When you click Next, the MDX Toolkit validates the Android SDK path. If the tool cannot validate the path, you can browse to the SDK on your computer.

Choose the Java Development Kit (JDK) on your computer for wrapping Android mobile apps. If the JDK is not installed on your computer, the tool prompts you to install the tool. When you click Install, the tool locates the tool on the Web and then installs the JDK on your computer.

Choose the Android Software Development Kit (SDK) on your computer for wrapping Android mobile apps and choose the Android APK tool.

Choose the keystore for signing Android mobile apps. When you wrap the app, you must provide the keystore that was created when the app was developed. The Android operating system requires that all installed mobile apps be digitally signed with a certificate with a private key that is held by the developer. The certificate does not need to be signed by a Certificate Authority. Android mobile apps can use self-signed certificates. For more information about signing Android mobile apps, see the Android developers web site.

When you wrap the mobile app with the MDX Toolkit, you can select the option Use debug keystore. This option allows you to sign the mobile app if the release keystore is not available during development. To create an Android app that users install on their devices, you must create a retail build of the app and disable Use debug keystore so you can sign the package with a real key. A keystore can contain multiple private keys, in most cases it will be only one key. If the keystore contains multiple private keys, when you wrap the app, you can select the key alias.

When the MDX Toolkit finishes wrapping the app, the app file name includes _andr. The file type is .mdx.

Wrapping iOS Mobile Apps
For iOS apps, you need to following these basic steps:

Specify an iOS mobile app IPA file.

In the MDX Toolkit wizard, choose the option to deploy the app from XenMobile or to deploy the app from the Apple App Store.

Choose the iOS Distribution Provisioning Profile and Distribution Certificate to sign the app for distribution.

When the MDX Toolkit finishes wrapping the app, the app file name includes _iOS. The file type is .mdx.

When you run the MDX Toolkit, the app determines the application type and version. You can select the minimum and maximum operating system versions.

Uploading the Wrapped App and Configuring Policies
After you complete wrapping the app, you then upload the MDX file to App Controller. You use the App Controller management console to configure specific app details and policy settings that Citrix Receiver or the Worx Store enforces. When users log on, the app appears in the store. Users can then subscribe, download, and install the app on
their device. For more information about configuring the app details and policy settings in App Controller, see Adding Apps.
Chapter 5

XenMobile Configuration Tests and Troubleshooting

Topics:

- Testing Your NetScaler Gateway Configuration
- Configuring GoToAssist Settings for Worx Apps

After you install and configure each component in your XenMobile deployment, you can test your configuration:

- You can test your NetScaler Gateway settings by connecting to the appliance.
- You can install applications that connect to each XenMobile component. For example, you can deploy Worx Enroll to register user devices with Device Manager.
- You can configure Device Manager and AppController to communicate with each other and then test the connection.
- You can also test to make sure users can use Worx Home to connect from their mobile devices through NetScaler Gateway by using Micro VPN, and then open and install mobile apps from App Controller.

This section describes the configuration tests you can carry out, and what to do if you experience problems.
Testing Your NetScaler Gateway Configuration

After you configure the initial settings on NetScaler Gateway, you can test your settings by connecting to the appliance.

To test the NetScaler Gateway settings, open a Web browser and type the web address. For example, in the address bar, type https://my.company.com or https://192.168.96.183.

At the logon screen, enter the test user name and password from Active Directory. At the logon screen, enter the test user name and password from Active Directory. When you log on, Receiver for Web appears and displays your applications and virtual desktops. NetScaler Gateway passes the user name and password on to Receiver for Web with single sign-on.

Note: To allow this test to work, you must only configure LDAP authentication on NetScaler Gateway.

Configuring GoToAssist Settings for Worx Apps

App Controller and Citrix GoToAssist integrate to provide continuous technical support for mobile device users who are using WorxMail or WorxWeb. When you configure settings, you can add an email address, phone number, chat information, and ticket information. If the user needs assistance, they can tap a chat button on their mobile device and the GoToAssist web page opens.

To get started, you need to do the following:

1. After you purchase XenMobile, you receive a promotion code for GoToAssist.

   Note: The promotion enables a one-year subscription to GoToAssist that allows one Help desk support personnel to log on to the management console and support an organization's users. You must renew the subscription each year.

2. Log on to the GoToAssist web site.

3. Create a new service for integrating GoToAssist with XenMobile.

When you do these steps, GoToAssist generates the email address that users can use to create a support ticket. This also creates an integration key that you enter in the App Controller management console.

When users start GoToAssist from their mobile device, the Worx app provisions XenMobile App Edition and GoToAssist accounts. GoToAssist sends an account key (token) to XenMobile App Edition which is then sent to the Worx app. Users can use GoToAssist to receive technical support in the following ways:

- Enter a valid email address to allow support personnel to contact them.
- Use chat to contact support personnel.
Note: When users log on to chat from their device, the XenMobile App Edition and Worx app logs are bundled together and sent to support personnel.

- Create an incident form by clicking Create Incident. If support personnel are not available through chat, GoToAssist redirects users to the incident form automatically.

When you configure GoToAssist in App Controller, the settings appear on the Support Options page in Settings. On this page you can view the settings for phone, chat, and ticket options. In Support Options, you can do the following:

- Edit existing GoToAssist settings for phone, chat, or the ticket.
- Add email or key support options.
- Delete an option.

On the Support Options page, you can add the following support information, however Citrix recommends using the GoToAssist page in Settings to configure support settings.

- Phone numbers
- Email addresses
- Chat settings
- Ticket settings
- Custom key settings

To configure GoToAssist settings in App Controller

1. In the App Controller management console, click the Settings tab.
2. In the navigation pane, under System Configuration, click GoToAssist.
3. In the details pane, next to GoToAssist Configuration, click Edit.
4. In Support email, enter the email address for support personnel. Users can choose to use the email address to contact support personnel instead of GoToAssist.
5. In Support phone, enter the phone number for users to use to contact support personnel.
6. In GoToAssist chat leave the default token number or enter one of your own. When users request a chat session, this token is sent to the Worx app.
7. In GoToAssist ticket, enter the email address that you can use to differentiate GoToAssist support requests and then click Save.

To edit support settings

1. In the App Controller management console, click the Settings tab.
2. In the navigation pane, click Support Options.
3. In the details pane, next to an item, under Actions, click the pencil icon.

4. In the Add Property dialog box, do the following:
   a. In Value, change the value for the support option type.
      For example, if you are editing the chat option, enter the new key in this field.
   b. In Name, change the name of the value.
   c. In Description, add a description for the option.
5. Click Save
   The changes appear in the Support Options details pane.

To add support information by using Support Options
You can add a support email address or a custom key.

1. In the App Controller management console, click the Settings tab.
2. In the navigation pane, click Support Options.
3. In the details pane, click Add.
4. In the Add Property dialog box, do the following:
   a. In Key, select either SUPPORT_EMAIL or Custom Key.
   b. If you select Custom Key, enter a name of the custom key you want to add in the blank field that appears. Keys have two parts: key name and the value, such as GTA_PHONE=5551212.
   c. In Value, add the value for the support option type.
      For example, if you are editing the chat option, enter the new chat key in this field.
   d. In Name, add a name of the value.
   e. In Description, add a description for the option and then click Save.

To remove a support option
1. In the App Controller management console, click the Settings tab.
2. In the navigation pane, click Support Options.
3. In the details pane, click an option and then under Actions click the X icon.
4. To confirm, click Yes.