Citrix Reference Architecture for XenMobile 8.6

Using XenMobile to create a comprehensive solution to manage mobile apps, data and devices
# Table of Contents

Overview .................................................................................................................................................. 1  
Understanding the XenMobile Architecture ............................................................................................ 2  
XenMobile Architectures ............................................................................................................................ 3  
  XenMobile 8.6 MDM Edition ..................................................................................................................... 4  
  XenMobile 8.6 MDM Edition Guidelines ................................................................................................ 4  
  XenMobile 8.6 App Edition ....................................................................................................................... 8  
  XenMobile 8.6 App Edition with XenDesktop Integration ...................................................................... 8  
  XenMobile 8.6 App Edition Guidelines .................................................................................................. 9  
XenMobile 8.6 Enterprise Edition ............................................................................................................... 11  
  XenMobile 8.6 Enterprise Edition with XenDesktop Integration .............................................................. 11  
  XenMobile 8.6 Enterprise Edition Guidelines ....................................................................................... 12  
  XenMobile 8.6 Enterprise Edition with High Availability .................................................................... 16  
  XenMobile 8.6 Enterprise Edition with Global Server Load Balancing (GLSB) .................................... 18  
Reference Environment ............................................................................................................................. 20  
  Network Layout ................................................................................................................................. 20  
  Server Hardware ............................................................................................................................... 20  
  Authentication .................................................................................................................................... 21  
    Step-up Authentication ......................................................................................................................... 22  
  Certificates ......................................................................................................................................... 23  
  Domain Name Service (DNS) .............................................................................................................. 23  
  Microsoft SQL Server ....................................................................................................................... 23  
Conclusion ............................................................................................................................................... 24  
Appendix A – Firewall Port Requirements .............................................................................................. 25  
  XenMobile MDM Edition ...................................................................................................................... 25  
  XenMobile App Edition .......................................................................................................................... 26  
  XenMobile Enterprise Edition ............................................................................................................... 26  
Appendix B – Configuration Guidelines and Recommendations ............................................................. 27  
  Integration of Windows Desktops and Apps with the App Controller ................................................. 27  
  Linking the Device Manager with the App Controller ......................................................................... 27
Overview

Citrix XenMobile is the revolutionary new way to mobilize your business. The product offers security and compliance for IT, while giving users: mobile device, app and data freedom. Users gain single-click access to all of their mobile, SaaS and Windows apps from a unified corporate app store, including seamlessly-integrated email, browser, data sharing and support apps.

IT gains control over mobile devices with full configuration, security, provisioning and support capabilities. In addition, XenMobile securely delivers Worx Mobile Apps, mobile apps built for businesses using the Worx App SDK and found through the Worx App Gallery. With XenMobile, IT can meet their compliance and control needs while users get the freedom to experience work and life their way.

The Citrix® Reference Architecture for XenMobile 8.6 guides architects in designing the next generation of mobile device and application management services. This document is for IT architects looking to implement and manage their mobility infrastructure. Each of these validated architectures has been certified by Citrix to perform and scale to the most demanding enterprise requirements.
Understanding the XenMobile Architecture

Worx Home

Citrix Worx Home is an app that allows IT to enforce mobile settings and security on mobile devices. Employees use this app to access their unified corporate app store and live support services. XenMobile communicates with Worx Home to deliver MDM and Worx-enabled apps and policies. XenMobile App Controller also stocks the unified corporate app store with apps most relevant to the user.

NetScaler

NetScaler is a secure application and data access solution that provides administrators granular application and data-level control while empowering users with remote access from anywhere. It gives IT administrators a single point to manage access control and limit actions within sessions based on both user identity and the endpoint device, providing better application security, data protection and compliance management.

XenMobile Device Manager

Device Manager allows IT 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 the corporate network from mobile threats. With a “one-click” dashboard, simple administrative console, and real-time integration with Microsoft Active Directory and other enterprise infrastructure like PKI and Security Information and Event Management (SIEM) systems, XenMobile Device Manager simplifies the management of mobile devices.

XenMobile App Controller

App Controller manages and enables access to an organization’s mobile, web and SaaS apps and ShareFile data resources.

ShareFile

ShareFile is an enterprise follow-me data solution that enables IT to deliver a robust data sharing and sync service that meets the mobility and collaboration needs of users and the data security requirements of the enterprise. By making follow-me data a seamless and intuitive part of every user’s day, ShareFile enables optimal productivity for today’s highly mobile, anywhere, any-device workforce.
XenMobile Architectures

Determining the correct architecture is based on the device or app management requirements of the enterprise. The components of XenMobile are modular and build upon each other. This section will provide an overview of each edition and its design.

**XenMobile 8.6 MDM Edition**

**XenMobile 8.6 App Edition**

**XenMobile 8.6 Enterprise Edition**

![Diagram](image)

**Figure 2 – Building Blocks to the XenMobile 8.6 Enterprise Edition**

The following sections will further identify and define key guidelines and recommendations for deployment of these respective architectures.

citrix.com
XenMobile 8.6 MDM Edition

XenMobile 8.6 MDM Edition includes the following infrastructure components:

- **XenMobile Device Manager (XDM) 8.6**
- **XenMobile NetScaler Connector (XNC) 8.6**
  
  **Note:** XNC requires a NetScaler.
- **ShareFile StorageZones Controller 2.0**

Citrix recommends using a NetScaler (i.e., NetScaler Gateway 10.1) for a more secure deployment.

There are several reasons to do this:

- Limit exposure to Windows servers in the DMZ
- Easily scale out by adding more servers behind the NetScaler in the future

In order to enable the mobile device management functionality, the device will need to enroll with the Device Manager server using the **Worx Home** application. Worx Home provides the user with the means to access work apps and data.

**ShareFile** enables IT to deliver a robust data sharing and sync service that meets the mobility and collaboration needs of users and the data security requirements of the enterprise. By making follow-me data a seamless and intuitive part of every user’s day, ShareFile enables optimal productivity for today’s highly mobile, anywhere, any-device workforce. The integration between ShareFile and XenMobile provides follow-me data across devices and apps and allows users to view, edit and share data within a secure container on their mobile device.

![Reference Architecture for XenMobile 8.6 MDM Edition](image)

**Figure 3 – Reference Architecture for XenMobile 8.6 MDM Edition**

XenMobile 8.6 MDM Edition Guidelines

In order to facilitate the deployment of XenMobile 8.6 MDM Edition, Citrix recommends that IT administrators review the following minimum guidelines.

1. The following **ports** need to be open to allow XDM to communicate with internal and external resources.
2. The **Apple Push Notification Service (APNS)** is used by XDM to push notifications to iOS devices for configuration and policy updates. This service is provided by Apple and is only required for iOS devices. Non-iOS devices have their own push implementation.

   **Note:** A special APNS certificate that is signed by Citrix and issued by Apple is required before installing XDM. Please see the installation instructions.

3. **NetScaler** is the secure application and data access solution for the infrastructure. NetScaler is available as high-performance network appliances and software-based virtual appliances in a range of editions for maximum deployment flexibility. These editions include:
   - **NetScaler MPX** appliances are hardened network appliances that offer up to 120 Gbps performance.
   - **NetScaler SDX** is a high-density consolidation platform that combines Xen-based virtualization with the advanced architecture of NetScaler MPX to run up to 40 NetScaler instances simultaneously without sacrificing performance or security.
   - **NetScaler VPX** virtual appliances run as virtual machines (VMs) on popular hypervisors, allowing NetScaler to be provisioned on-demand using inexpensive, industry-standard servers (i.e., **NetScaler Gateway 10.1**).

   The following table details the minimum resource requirements of the NetScaler VPX:

<table>
<thead>
<tr>
<th>NetScaler Gateway</th>
<th>vCPU</th>
<th>Memory</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4096 MB</td>
<td>20 GB</td>
<td></td>
</tr>
</tbody>
</table>

4. **XenMobile Device Manager (XDM)** is the central server for MDM that combines policies, devices and users to create deployments to manage the corporate mobile strategy.
   - Endpoint devices may connect to the XDM server over ports 80, 443, and 8443. Port 80 is used by legacy endpoint devices such as older phones and tablets running Windows Mobile, or Symbian. However, newer endpoint devices are more secure and use port 443. Port 8443 is only used during the enrollment process for iOS devices.
   - The XDM server runs on the Microsoft Windows Server operating system (i.e., Windows Server 2008 R2).
   - The XDM server requires connections to core components and common infrastructure services such as Active Directory, DNS, SMTP, Microsoft SQL Server and a certificate authority.
• MDM also requires a PKI service such as Microsoft Certificate Authority or it can use its own PKI service hosted on the XDM server that gets installed with Device Manager. Device Manager will use this service to push client certificates to devices for client certificate authentication to XDM. Client certificates are deployed automatically during device enrollment.

• Citrix recommends the use of Microsoft SQL Server (Express, Standard, or Enterprise) for a production environment.

The MDM components can be installed on physical or virtual machine. The following table describes the resource requirements to support 5,000 devices for each of the components in the XenMobile architecture.

<table>
<thead>
<tr>
<th>Device Manager</th>
<th>vCPU</th>
<th>Memory</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 – 4</td>
<td>4 GB</td>
<td>24 GB</td>
</tr>
<tr>
<td>SQL Server</td>
<td>2</td>
<td>6 GB</td>
<td>24 GB</td>
</tr>
</tbody>
</table>

Table 2 – XenMobile Server Virtual Machine (VM) Specifications

Enterprises requiring scalability greater than 5,000 devices will need to adjust server specifications to match the minimum parameters in the table below.

<table>
<thead>
<tr>
<th>Devices</th>
<th>XenMobile MDM Server</th>
<th>SQL Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000</td>
<td>2 vCPU 4 GB RAM</td>
<td>2 vCPU 6 GB RAM</td>
</tr>
<tr>
<td>10,000</td>
<td>4 vCPU 8 GB RAM</td>
<td>4 vCPU 16 GB RAM</td>
</tr>
<tr>
<td>20,000</td>
<td>8 vCPU 16 GB RAM</td>
<td>16 vCPU 24 GB RAM</td>
</tr>
<tr>
<td>40,000</td>
<td>16 vCPU 32 GB RAM</td>
<td>32 vCPU 64 GB RAM</td>
</tr>
</tbody>
</table>

Table 3 – XenMobile Server Virtual Machine (VM) Specifications for Scalability

The XDM and database servers can be clustered for high availability; please reference the High Availability section for more details on clustering the MDM components. Database backup and recovery should be performed according to the organization’s data center policy.

Tomcat TCP connections also need to be taken into consideration

<table>
<thead>
<tr>
<th>Devices</th>
<th>Port 443</th>
<th>Port 8443</th>
<th>Port 80</th>
<th>Max Threads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 10,000</td>
<td>400</td>
<td>30</td>
<td>20</td>
<td>12</td>
</tr>
<tr>
<td>Over 10,000</td>
<td>750</td>
<td>50</td>
<td>50</td>
<td>20</td>
</tr>
</tbody>
</table>

Table 4 – XenMobile MDM Server and TCP Connections

If the TCP connections are getting close to 750, consider clustering the XDM server.

5. **ShareFile StorageZones Controller** provides instant mobile access to data on existing network file shares through the ShareFile for iPad and ShareFile for iPhone apps. It also provides access to existing ShareFile data.

6. XenMobile MDM Edition provides access to **SharePoint** sites. This requires external access to your SharePoint server. This functionality can be configured in an XDM policy allowing the Worx Home to host the SharePoint data in a secure viewer on the mobile device.

7. **XenMobile NetScaler Connector (XNC)** provides a device level authorization service for ActiveSync clients to NetScaler acting as a reverse proxy for the ActiveSync protocol. Authorization is controlled by a combination of policies defined within the XenMobile Device Manager and by rules defined locally by XenMobile NetScaler Connector. XNC and XDM can be clustered and load balanced by NetScaler.

• The XNC component can be installed on the XDM server or any server running the Microsoft Windows operating system (i.e., Windows Server 2008 R2).

XNC communicates periodically with the XDM server to synchronize policies to ensure that device policies are in sync and can be accurately enforced. The following describes this process flow:
- XenMobile NetScaler Connector Service provides a REST web service interface that can be invoked by NetScaler to determine if an ActiveSync request from a device is authorized.
- XenMobile Configuration Service communicates with XDM to synchronize policy changes with XNC.
- XenMobile Notification Service sends notifications of unauthorized device access to XDM so that XDM can take appropriate measures against the device, such as notifying the user why the device was blocked.
- XenMobile NetScaler Configuration application allows the administrator to configure and monitor XNC.

![Figure 5 – XenMobile NetScaler Connector (XNC) Process Flow](image-url)
XenMobile 8.6 App Edition

XenMobile 8.6 App Edition includes the following infrastructure components:

- **XenMobile App Controller 2.9 – Virtual Appliance**
- **NetScaler** (i.e., NetScaler Gateway 10.1)
- **ShareFile StorageZones Controller 2.0**

In order to connect to the unified corporate app store, the device will need to be installed and configured with **Worx Home**. Worx Home provides the user with the easiest way to access work apps and data.

**WorxMail** is a native iOS and Android email, calendar and contacts app. Citrix WorxMail integrates with other Worx Mobile Apps and leverages the mobile app security features in XenMobile through MDX technologies to offer secure productivity on the go. Users can attach docs to emails and save attachments using ShareFile, open attachments and web links, including internal sites, with WorxWeb, and view the free/busy information of colleagues before sending a meeting invite, all while staying inside the secure container on the mobile device. WorxMail supports ActiveSync and Exchange and offers security features, such as encryption for email, attachments and contacts.

**WorxWeb** is a consumer-like native mobile browser for iOS and Android devices that enables secure access to internal corporate web, external SaaS, and HTML5 web applications. WorxWeb leverages MDX technologies to create a dedicated VPN tunnel for accessing a company’s internal network and the other MDX security features to ensure that users can access all of their websites, including those with sensitive information. WorxWeb offers a seamless user experience in its integration with WorxMail to allow users to click on links, such as ‘mailto’ and have the native apps open inside the secure container on the mobile device.

**ShareFile** enables IT to deliver a robust data sharing and sync service that meets the mobility and collaboration needs of users and the data security requirements of the enterprise. By making follow-me data a seamless and intuitive part of every user’s day, ShareFile enables optimal productivity for today’s highly mobile, anywhere, any-device workforce. The integration between ShareFile and XenMobile provides follow-me data across devices and apps and allows users to view, edit and share data within a secure container on their mobile device.

XenMobile 8.6 App Edition with XenDesktop Integration

**StoreFront** provides access to Windows desktops and apps hosted on the XenDesktop (or XenApp) infrastructure. The App Controller server can be configured to provide access to the Windows desktop and apps. When the user connects to the unified corporate app store, they will be presented with apps from XenDesktop, XenApp, and the App Controller as a consolidated list of resources.

Citrix **Receiver** provides the capability for users to run Windows desktops and apps published on XenApp or XenDesktop from a mobile device. Receiver will run in the background to support the capability of running those Windows desktops and apps.
XenMobile 8.6 App Edition Guidelines

In order to facilitate the deployment of XenMobile 8.6 App Edition, Citrix recommends that IT administrators review the following minimum guidelines.

1. The following **ports** need to be open for the XenMobile 8.6 App Edition reference architecture.

2. **NetScaler** is the secure application and data access solution for the infrastructure. NetScaler is available as high-performance network appliances and software-based virtual appliances in a range of editions for maximum deployment flexibility. These editions include:
   - **NetScaler MPX** appliances are hardened network appliances that offer up to 120 Gbps performance.
   - **NetScaler SDX** is a high-density consolidation platform that combines Xen-based virtualization with the advanced architecture of NetScaler MPX to run up to 40 NetScaler instances simultaneously without sacrificing performance or security.
• **NetScaler VPX** virtual appliances run as virtual machines (VMs) on popular hypervisors, allowing NetScaler to be provisioned on demand using inexpensive, industry-standard servers.

The following table details the minimum resource requirements of the NetScaler VPX (i.e., **NetScaler Gateway** 10.1):

<table>
<thead>
<tr>
<th></th>
<th>vCPU</th>
<th>Memory</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler Gateway</td>
<td>2</td>
<td>4096 MB</td>
<td>20 GB</td>
</tr>
</tbody>
</table>

**Table 5 – NetScaler Gateway Virtual Appliance (VPX) Specifications**

3. The **App Controller** component can be a virtual appliance that is installed on a hypervisor. The following table describes the resource requirements to support 5,000 devices for each of the components in the XenMobile architecture:

<table>
<thead>
<tr>
<th></th>
<th>vCPU</th>
<th>Memory</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Controller</td>
<td>2</td>
<td>4 GB</td>
<td>50 GB</td>
</tr>
</tbody>
</table>

**Table 6 – App Controller Virtual Machine (VM) Specifications**

4. The **ShareFile StorageZones Controller** provides mobile access to data on existing network file shares and SharePoint through the ShareFile for iPad and ShareFile for iPhone apps. It also provides access to existing ShareFile data.
XenMobile 8.6 Enterprise Edition

XenMobile 8.6 Enterprise Edition includes the following infrastructure components:

- XenMobile Device Manager (XDM) 8.6
- XenMobile NetScaler Connector (XNC) 8.6
  
  Note: XNC requires a NetScaler.
- XenMobile App Controller 2.9 – Virtual Appliance
- StoreFront 2.1
- NetScaler (i.e., NetScaler Gateway 10.1)
- ShareFile StorageZones Controller 2.0

In order to enable the mobile device management functionality, the device will need to enroll with the Device Manager server using the Worx Home application. In order to connect to the unified corporate app store, the device will need to be installed and configured with Worx Home. Worx Home provides the user with the easiest way to access work apps and data.

WorxMail is a native iOS and Android email, calendar and contacts app. Citrix WorxMail integrates with other Worx Mobile Apps and leverages the mobile app security features in XenMobile through MDX technologies to offer secure productivity on the go. Users can attach docs to emails and save attachments back using ShareFile, open attachments and web links, including internal sites, with WorxWeb, and view the free/busy information of colleagues before sending a meeting invite, all while staying inside the secure container on the mobile device. WorxMail supports ActiveSync and Exchange and offers security features, such as encryption, for email, attachments and contacts.

WorxWeb is a consumer-like native mobile browser for iOS and Android devices that enables secure access to internal corporate web, external SaaS, and HTML5 web applications. WorxWeb leverages MDX technologies to create a dedicated VPN tunnel for accessing a company's internal network and the other MDX security features to ensure that users can access all of their websites, including those with sensitive information. WorxWeb offers a seamless user experience in its integration with WorxMail to allow users to click on links, such as 'mailto' and have the native apps open inside the secure container on the mobile device.

ShareFile enables IT to deliver a robust data sharing and sync service that meets the mobility and collaboration needs of users and the data security requirements of the enterprise. By making follow-me data a seamless and intuitive part of every user’s day, ShareFile enables optimal productivity for today’s highly mobile, anywhere, any-device workforce. The integration between ShareFile and XenMobile provides follow-me data across devices and apps and allows users to view, edit and share data within a secure container on their mobile device.

XenMobile 8.6 Enterprise Edition with XenDesktop Integration

StoreFront provides access to Windows desktops and apps hosted on the XenDesktop (or XenApp) infrastructure. The App Controller server can be configured to provide access to the Windows desktop and apps. When the user connects to the unified corporate app store, they will be presented with apps from XenDesktop, XenApp, and the App Controller as a consolidated list of resources.

Citrix Receiver provides the capability for users to run Windows desktops and apps published on XenApp or XenDesktop from a mobile device. Receiver will run in the background to support the capability of running those Windows desktops and apps.
Citrix® Reference Architecture for XenMobile 8.6 | Whitepaper

In order to facilitate the deployment of XenMobile 8.6 Enterprise Edition, Citrix recommends that IT administrators review the following minimum guidelines.

1. The following **ports** need to be open to allow XDM to communicate with internal and external resources.

XenMobile 8.6 Enterprise Edition Guidelines

In order to facilitate the deployment of XenMobile 8.6 Enterprise Edition, Citrix recommends that IT administrators review the following minimum guidelines.

1. The following **ports** need to be open to allow XDM to communicate with internal and external resources.
2. The **Apple Push Notification Service (APNS)** is used by XDM to push notifications to iOS devices for configuration and policy updates. This service is provided by Apple and is only required for iOS devices. Non-iOS devices have their own push implementation.

**Note:** A special APNS certificate that is signed by Citrix and issued by Apple is required before installing XDM. Please see the installation instructions.

3. **NetScaler** is the secure application and data access solution for the infrastructure. NetScaler is available as high-performance network appliances and software-based virtual appliances in a range of editions for maximum deployment flexibility. These editions include:

- **NetScaler MPX** appliances are hardened network appliances that offer up to 120 Gbps performance.
- **NetScaler SDX** is a high-density consolidation platform that combines Xen-based virtualization with the advanced architecture of NetScaler MPX to run up to 40 NetScaler instances simultaneously without sacrificing performance or security.
- **NetScaler VPX** virtual appliances run as virtual machines (VMs) on popular hypervisors, allowing NetScaler to be provisioned on demand using inexpensive, industry-standard servers (i.e., **NetScaler Gateway 10.1**).

The following table details the minimum resource requirements of the NetScaler VPX:

<table>
<thead>
<tr>
<th></th>
<th>vCPU</th>
<th>Memory</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler Gateway</td>
<td>2</td>
<td>4096 MB</td>
<td>20 GB</td>
</tr>
</tbody>
</table>

Table 7 – NetScaler Gateway Virtual Appliance (VPX) Specifications

4. **XenMobile Device Manager (XDM)** is the central server for MDM that combines policies, devices, and users to create deployments to manage the corporate mobile strategy.

- Endpoint devices may connect to the XDM server over ports **80, 443, and 8443**. Port **80** is used by legacy endpoint devices such as older phones and tablets running Windows Mobile, or Symbian. However, newer endpoint devices are more secure and use port **443**. Port **8443** is only used during the enrollment process for iOS devices.
- The XDM server runs on the Microsoft Windows Server operating system (i.e., Windows Server 2008 R2).
- The XDM server requires connections to core components and common infrastructure services such as Active Directory, DNS, SMTP, Microsoft SQL Server, and a certificate authority.
- MDM also requires a PKI service like Microsoft Certificate Authority or it can use its own PKI service hosted on the XDM server that gets installed with Device Manager. Device Manager will use this service to push out client certificates to devices for client certificate authentication to XDM. Client certificates are deployed automatically during device enrollment.
- Citrix recommends the use of Microsoft SQL Server (Express, Standard, or Enterprise) for a production environment.

The MDM components can be installed on physical or virtual machine. The following table describes the resource requirements to support 5,000 devices for each of the components in the XenMobile architecture.

<table>
<thead>
<tr>
<th></th>
<th>vCPU</th>
<th>Memory</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Manager</td>
<td>2 – 4</td>
<td>4 GB</td>
<td>24 GB</td>
</tr>
<tr>
<td>SQL Server</td>
<td>2</td>
<td>6 GB</td>
<td>24 GB</td>
</tr>
</tbody>
</table>

Table 8 – XenMobile Server Virtual Machine (VM) Specifications
Enterprises requiring scalability greater than 5,000 devices will need to adjust server specifications to match the minimum parameters in the table below.

<table>
<thead>
<tr>
<th>Devices</th>
<th>XenMobile MDM Server</th>
<th>SQL Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000</td>
<td>2 vCPU 4 GB RAM</td>
<td>2 vCPU 6 GB RAM</td>
</tr>
<tr>
<td>10,000</td>
<td>4 vCPU 8 GB RAM</td>
<td>4 vCPU 16 GB RAM</td>
</tr>
<tr>
<td>20,000</td>
<td>8 vCPU 16 GB RAM</td>
<td>16 vCPU 24 GB RAM</td>
</tr>
<tr>
<td>40,000</td>
<td>16 vCPU 32 GB RAM</td>
<td>32 vCPU 64 GB RAM</td>
</tr>
</tbody>
</table>

Table 9 – XenMobile Server Virtual Machine (VM) Specifications for Scalability

The XDM and database servers can be clustered for high availability; please reference the High Availability section for more details on clustering the MDM components. Database backup and recovery should be performed according to the organization’s data center policy.

Tomcat TCP connections also need to be taken into consideration

<table>
<thead>
<tr>
<th>Devices</th>
<th>Port 443</th>
<th>Port 8443</th>
<th>Port 80</th>
<th>Max Threads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 10,000</td>
<td>400</td>
<td>30</td>
<td>20</td>
<td>12</td>
</tr>
<tr>
<td>Over 10,000</td>
<td>750</td>
<td>50</td>
<td>50</td>
<td>20</td>
</tr>
</tbody>
</table>

Table 10 – XenMobile MDM Server and TCP Connections

If the TCP connections are getting close to 750, consider clustering the XDM server.

5. **App Controller** component can be a virtual appliance that is installed on a hypervisor. The following table describes the resource requirements to support 5,000 devices for each of the components in the XenMobile architecture:

<table>
<thead>
<tr>
<th></th>
<th>vCPU</th>
<th>Memory</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Controller</td>
<td>2</td>
<td>4 GB</td>
<td>50 GB</td>
</tr>
</tbody>
</table>

Table 11 – App Controller Virtual Machine (VM) Specifications

6. **ShareFile StorageZones Controller** provides instant mobile access to data on existing network file shares through the ShareFile for iPad and ShareFile for iPhone apps. It also provides access to existing ShareFile data.

7. XenMobile Enterprise Edition provides access to **SharePoint** sites. This requires external access to your SharePoint server. This functionality can be configured in an XDM policy allowing the Worx Home to host the SharePoint data in a secure viewer on the mobile device.

8. The **XenMobile NetScaler Connector (XNC)** provides a device level authorization service for ActiveSync clients to NetScaler acting as a reverse proxy for the ActiveSync protocol. Authorization is controlled by a combination of policies defined within the XenMobile Device Manager and by rules defined locally by XenMobile NetScaler Connector. XNC and XDM can be clustered and load balanced by NetScaler.

- The XNC component can be installed on the XDM server or any server running the Microsoft Windows operating system (i.e., Windows Server 2008 R2).

XNC communicates periodically with the XDM server to synchronize policies to ensure that device policies are in sync and can be accurately enforced. The following describes this process flow:

- XenMobile NetScaler Connector Service provides a REST web service interface that can be invoked by NetScaler to determine if an ActiveSync request from a device is authorized.
- XenMobile Configuration Service communicates with XDM to synchronize policy changes with XNC.
- XenMobile Notification Service sends notifications of unauthorized device access to XDM so that XDM can take appropriate measures against the device, such as notifying the user why the device was blocked.
- XenMobile NetScaler Configuration application allows the administrator to configure and monitor XNC.

Figure 10 – XenMobile NetScaler Connector (XNC) Process Flow
Citrix recommends using a high availability implementation of XenMobile. Each core component of the XenMobile infrastructure can be configured in high availability mode.

A high availability deployment of two NetScaler Gateway appliances can provide uninterrupted operation in any transaction. With one appliance configured as the primary node and the other as the secondary node, the primary node accepts connections and manages servers while the secondary node monitors the primary node. If for any reason the primary node is unable to accept connections, the secondary node takes over. See Citrix eDocs for information pertaining to “Configuring High Availability on NetScaler Gateway”.

Two XenMobile App Controller virtual machines (VM) can be deployed as a high availability pair. The first XenMobile App Controller on which high availability is configured is called the primary, and the other instance is called the secondary. In this deployment, the primary App Controller listens for requests, serves user requests, and synchronizes its data with the data on the secondary App Controller. The two virtual machines (VM) work as an active-passive pair, in which only one VM is active at a time. If the primary App Controller stops responding for any reason, the secondary App Controller takes over, becoming the active VM and begins to service user requests.

When it becomes the active VM, the secondary App Controller also synchronizes system and database information by using a client-server mechanism. A client on the active App Controller shares the necessary information to a virtual server on the passive App Controller as a series of requests. The virtual server parses the requests and performs the necessary action. A virtual IP is required; this will be the FQDN App Controller address used when configuring StoreFront and NetScaler Gateway in the XenMobile App Edition or XenMobile Enterprise Edition architectures. Review Citrix eDocs for details pertaining to “Configuring High Availability on App Controller”.

Figure 11 – Reference Architecture for XenMobile 8.6 Enterprise Edition with High Availability (HA)
Multiple instances of the App Controller virtual machine can be installed to create a cluster. One App Controller will act as the cluster head and is considered to be the host. As such, the cluster head will host the database for all of the App Controller VMs in the cluster. All other App Controller virtual machines in the cluster are called the service nodes. Each service node has a local database that is used by the service node only. Updating user information from the service node to the cluster head requires writing to the database. A service node connects to the database on the cluster head by using a secure channel.

App Controllers deployed as service nodes obtain their configuration from the App Controller that acts as the cluster head. Citrix recommends deploying two App Controller VMs in a high availability pair. Each VM is a cluster head. If one VM fails, the secondary VM can act as the cluster head.

Search Citrix eDocs for information regarding “Configuring App Controller Clustering”.

---

XenMobile Device Manager (XDM) can be configured with multiple servers load-balanced behind a NetScaler appliance or another hardware load-balancing solution. The Device Managers work in an active-active configuration. In this environment, ports 80, 443, and 8443 are load-balanced. For SSL connections (ports 443 and 8443), make sure to turn on SSL session persistence in the load balancing rules. XDM requires a shared SQL server and NTP configured on each server.

StoreFront is an integral component of any XenDesktop, XenApp, XenMobile, or VDI-in-a-Box implementation. StoreFront provides high availability and multi-site configuration. It includes a number of features that combine to enable load balancing and failover between the deployments providing the resources for stores. StoreFront can be setup with dedicated disaster recovery deployment for increased resiliency. These features enable StoreFront to be distributed over multiple sites to provide high availability for the stores. Additional information can be found in Citrix eDocs regarding “StoreFront high availability and multi-site configuration”.

---
XenMobile 8.6 Enterprise Edition with Global Server Load Balancing (GSLB)

NetScaler appliances configured for global server load balancing (GSLB) provide for disaster recovery and ensure continuous availability of applications by protecting against points of failure in a wide area network (WAN). GSLB can balance the load across sites by directing client requests to the closest or best performing site, or to surviving sites in case of an outage. Global server load balancing is used to manage traffic flow to resources hosted in different geographic locations so that users and devices always access resources via the fastest and most efficient gateway. While XenMobile architecture doesn’t support multisite, GSLB can be used to ensure local access to distributed mailboxes and local resources for multi-region users. The following figure illustrates this configuration.

You can configure GSLB for proximity based on the round trip time (RTT), static proximity, or a combination of the two. When you configure GSLB for proximity, client requests are forwarded to the closest gateway. The main benefit of the proximity-based GSLB method is faster response times resulting from the selection of the closest available gateway. NetScaler appliances at both sites exchange proximity information using the MEP (Metric Exchange Protocol). The GSLB configurations on the two appliances at the two different sites are identical, although each sites load-balancing configuration is specific to that site.

For details on how to configure a basic GSLB setup, see [Configuring Global Server Load Balancing (GSLB)](https://support.citrix.com/article/CTX206240).

Once you have configured a basic GSLB setup, configure static proximity.
For details on how to configure the GSLB virtual server to use static proximity for load balancing, see Configuring Static Proximity.
Reference Environment

In the various reference architectures described in this document, there are many supporting servers and services that are required for operation in an enterprise environment. The following section details the common infrastructure components (storage, virtualization environment, servers, networking equipment, etc.) and how the various architectures integrate with those core components.

Network Layout

Server Hardware

<table>
<thead>
<tr>
<th>XenServer Hosts</th>
<th>Dell PowerEdge C6100</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Dell C6100 contains 4 physical servers enclosed in a 2U form factor with each server having the hardware specifications listed below:</td>
<td></td>
</tr>
<tr>
<td>• 2 – Intel Xeon E5620 Processors</td>
<td></td>
</tr>
<tr>
<td>• 64GB RAM</td>
<td></td>
</tr>
<tr>
<td>• 500GB HDD</td>
<td></td>
</tr>
<tr>
<td>• 2 – physical machines configured in HA (High Availability) mode</td>
<td></td>
</tr>
<tr>
<td>• 2 – 1Gb Ethernet Adapters</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>XenServer Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• 2 – servers configured in a virtualization pool for HA (High Availability)</td>
<td></td>
</tr>
<tr>
<td>• XenServer version 6.1.0-59235p</td>
<td></td>
</tr>
<tr>
<td>• Three separate VLANs configured:</td>
<td></td>
</tr>
<tr>
<td>o VLAN 30 – Storage VLAN configured for 9000 MTU for fast connectivity to backend NFS storage.</td>
<td></td>
</tr>
<tr>
<td>o VLAN 10 – User/Management traffic VLAN configured for standard 1500 MTU. Please note that it is best practice for XenServer to further segregate User and Management traffic by creating additional VLANs in high traffic implementations.</td>
<td></td>
</tr>
<tr>
<td>o VLAN 50 – DMZ VLAN to provide access from outside the enterprise network.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Storage</th>
<th>NetApp 2240-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 7.2TB total configurable storage</td>
<td></td>
</tr>
<tr>
<td>• Active/Active Controller configuration</td>
<td></td>
</tr>
<tr>
<td>• 4.5TB NFS configured storage volume</td>
<td></td>
</tr>
<tr>
<td>• ~250GB used for complete virtualized environment</td>
<td></td>
</tr>
<tr>
<td>• 2 – 10Gb Ethernet (10GbE) Adapters</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>Cisco C3560X</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco ASA 5520</td>
</tr>
</tbody>
</table>

Table 12 – Server Hardware and Specifications for Reference Environment
Authentication

Active Directory running on Windows Server 2008 R2 was used for all reference architecture environments. Active Directory, or LDAP, support is different for each product. App will not authenticate users in nested groups. Please check each product’s documentation for full support requirements.

The reference architecture for XenMobile 8.6 makes use of the new Worx PIN feature, which allows for a more seamless user experience. This feature allows the user to define a PIN and cache their AD Credentials inside of Worx Home, eliminating the pain of entering lengthy credentials when accessing XenMobile applications as well as a simplified offline challenge.

The reference environments also make use of two factor authentication configured on NetScaler Gateway to provide secure access to the internal corporate resources using Client Certificate authentication from Microsoft Certificate Services. Using two-factor authentication will require an extra port to be opened on the firewall (typically TCP/443) from XDM (NetScaler Gateway) to the Certificate server (internal). This also will require the appropriate certificates installed on the NetScaler Gateway to trust the client certificates.

In addition, for HDX applications and App Controller callback URLs to work in a secure client certificate authentication environment, an additional VServer on NetScaler Gateway is required. In the reference architecture, we have utilized port 8081 for this purpose, though this is customizable. This requirement is due to the Mandatory SSL certificate requirement being configured on the primary NetScaler Gateway VServer.

More details and information on client certificate authentication can be found in the XenMobile 8.6 Deployment Guide.

Figure 15 – Reference Architecture for XenMobile 8.6 Enterprise Edition with Client Certificate Authentication
Step-up Authentication

Another authentication feature delivered in XenMobile 8.6 enables administrators to set up a specific NetScaler Gateway through which a user must authenticate to access an application. This allows for higher security apps to use two factor authentication while lower security apps only require single factor authentication. The administrator sets the FQDN of a NetScaler Gateway (different from the default gateway) to which an application should authenticate. When this application is launched, the application recognizes the need for a new NS connection and notifies Worx Home of the need for a login. All traffic will go through this gateway until the step-up authentication period expires and the step-up application is no longer being used. At this time, a re-authentication will be done to the default gateway. The diagram below illustrates the connectivity for Step-up authentication.

Figure 16 – Reference Architecture for XenMobile 8.6 App Edition with Step-up Authentication
Certificates

Wildcard and SAN certificates are supported for all Citrix products. In most deployments, only two wildcard or SAN server certificates are required:

1) External – *.extcompany.com
2) Internal – *.intdomain.net

The following table shows the certificates required and format needed for each component. A simple utility like OpenSSL can be used to convert certificate formats. A separate SAML Certificate will be needed depending on the SAML authentication enabled apps that are published in App Controller.

<table>
<thead>
<tr>
<th>Certificate Format</th>
<th>Certificates Required</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler Gateway</td>
<td>PEM</td>
<td>Server, root CA, intermediates</td>
</tr>
<tr>
<td>App Controller</td>
<td>PEM or PFX (PKCS#12)</td>
<td>Server, SAML, root CA, intermediates</td>
</tr>
<tr>
<td>StoreFront</td>
<td>PFX (PKCS#12)</td>
<td>Server, root CA</td>
</tr>
<tr>
<td>XenMobile XDM</td>
<td>PFX (PKCS#12)</td>
<td>APNS, server. XDM will create its own PKI service or use Microsoft CA for client certificates.</td>
</tr>
</tbody>
</table>

Table 13 – Certificate Requirements

It is recommended to make this a public (3rd party) cert so mobile devices won’t need to download the company’s private root CA first.

Domain Name Service (DNS)

It is recommended to use static IPs for all servers in the environment. As configured in the reference environment the following records were added to the DNS server.

<table>
<thead>
<tr>
<th>Server</th>
<th>Location</th>
<th>Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>XenMobile Device Manager</td>
<td>Internal and External</td>
<td>Host (A)</td>
</tr>
<tr>
<td>NetScaler Gateway (including Vserver IP address)</td>
<td>Internal and External</td>
<td>Host (A)</td>
</tr>
<tr>
<td>App Controller</td>
<td>Internal</td>
<td>Host (A)</td>
</tr>
<tr>
<td>StoreFront</td>
<td>Internal</td>
<td>Host (A)</td>
</tr>
</tbody>
</table>

Table 14 – DNS – Server Records and Locations

Tip: In order to confirm communication between the servers, verify that the FQDN of each server can be resolved and pinged from every other server in the architecture, including the NetScaler.

Microsoft SQL Server

Microsoft SQL Server (Express, Standard, and Enterprise) are supported for all the products in the XenMobile reference architectures. It is important to plan accordingly and size the SQL server based on number of devices, applications and users that will be using the environment. The same SQL server may be used for the different products. It is recommended to size the SQL server based on the XDM requirements.
Conclusion

The Citrix Reference Architecture for XenMobile 8.6 document has outlined the various editions of XenMobile and the respective reference architecture. Each edition offers security and compliance for IT, while giving users; mobile device, app and data freedom. Citrix has well-defined and proven architectures for each of XenMobile editions. Once the IT architects have created their corporate mobile strategy, they can utilize this document to select the appropriate edition and corresponding reference architecture for planning the deployment of their mobility infrastructure.

For additional product information and technical questions or queries, concerning this document or the products mentioned herein, please visit the Citrix corporate web site, search Citrix eDocs for the latest product documentation, or contact your local Citrix representative.
## Appendix A – Firewall Port Requirements

### XenMobile MDM Edition

<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 XDM SMTP configuration of the Notification Service uses port 25. However, if your corporate SMTP server uses a different port, make sure that your corporate firewall does not block that port.</td>
<td>XenMobile XDM</td>
<td>Corporate SMTP Server</td>
</tr>
<tr>
<td>80</td>
<td>Over-the-Air (OTA) Enrollment and Agent Setup (Android and Windows Mobile)</td>
<td>Internet</td>
<td>XenMobile Device Manager Server</td>
</tr>
<tr>
<td>80 or 443</td>
<td>XenMobile Device Manager Nexmo SMS Notification Relay outbound connection</td>
<td>XenMobile XDM</td>
<td>Nexmo SMS Relay server</td>
</tr>
<tr>
<td>443</td>
<td>XenMobile Device Manager CA Requests</td>
<td>XenMobile XDM</td>
<td>MS Certificate Services</td>
</tr>
<tr>
<td>389 or 636</td>
<td>LDAP/LDAPS connection from XDM server to Directory Service Host (Active Directory Global Catalog server or equivalent LDAP directory service host)</td>
<td>XenMobile XDM</td>
<td>LDAP / Active Directory Services</td>
</tr>
<tr>
<td>443</td>
<td>SSL OTA Enrollment/Agent Setup (Android and Windows Mobile), All Device-related traffic and data connections (iOS, Android and Windows Mobile)</td>
<td>Internet</td>
<td>XenMobile XDM</td>
</tr>
<tr>
<td></td>
<td>SSL OTA Enrollment/Agent Setup (Android and Windows Mobile), All Device-related traffic and data connections (iOS, Android and Windows Mobile), XDM Web Console</td>
<td>Corporate LAN and Wi-Fi</td>
<td>XenMobile XDM</td>
</tr>
<tr>
<td>1433</td>
<td>Remote database server connection to separate SQL server (Optional)</td>
<td>XenMobile XDM</td>
<td>SQL Server</td>
</tr>
<tr>
<td>2195</td>
<td>Apple APNS (Push Notification Service) outbound connection to gateway.push.apple.com, used for iOS device notifications and device policy push</td>
<td>XenMobile XDM</td>
<td>Internet (Apple APNS Service Hosts on public IP network17.0.0.0/8)</td>
</tr>
<tr>
<td>2196</td>
<td>Apple APNS (Push Notification Service) outbound connection to feedback.push.apple.com, used for iOS device notifications and device policy push</td>
<td>XenMobile XDM</td>
<td></td>
</tr>
<tr>
<td>5223</td>
<td>Apple APNS (Push Notification Service) outbound connection from iOS devices connected via Wi-Fi network to *.push.apple.com</td>
<td>iOS device on Wi-Fi network service</td>
<td></td>
</tr>
<tr>
<td>8443</td>
<td>Over-the-Air (OTA) Enrollment for iOS Devices only</td>
<td>Internet</td>
<td>XenMobile XDM</td>
</tr>
</tbody>
</table>

**Note:** Corporate LAN traffic outbound to DMZ and the Internet is assumed to be allowed.
### XenMobile App Edition

<table>
<thead>
<tr>
<th>TCP Port</th>
<th>Description</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Connections to StoreFront Services for Enterprise edition access to Web, Mobile, SaaS and Desktop Applications</td>
<td>NetScaler Gateway</td>
<td>StoreFront</td>
</tr>
<tr>
<td></td>
<td>Connections to AppController for Web, Mobile and SaaS application delivery</td>
<td>NetScaler Gateway</td>
<td>App Controller</td>
</tr>
<tr>
<td></td>
<td>Secure Ticket Authority (STA)</td>
<td>NetScaler Gateway</td>
<td>Citrix XenDesktop / XenApp Servers</td>
</tr>
<tr>
<td>389, 636 or 3268</td>
<td>LDAP/LDAPS connection from NetScaler Gateway to Directory Service Host (Active Directory Global Catalog server or equivalent LDAP directory service host)</td>
<td>NetScaler Gateway</td>
<td>LDAP / Active Directory Services</td>
</tr>
<tr>
<td>53</td>
<td>DNS</td>
<td>NetScaler Gateway</td>
<td>DNS Server</td>
</tr>
<tr>
<td>123</td>
<td>NTP Services</td>
<td>NetScaler Gateway</td>
<td>NTP Server</td>
</tr>
<tr>
<td>1494</td>
<td>Citrix ICA Protocol</td>
<td>NetScaler Gateway</td>
<td>Citrix XenDesktop / XenApp Servers</td>
</tr>
<tr>
<td>2598</td>
<td>Citrix ICA/CGP Protocol When Session Reliability is enabled, TCP port 2598 replaces port 1494</td>
<td>NetScaler Gateway</td>
<td>Citrix XenDesktop / XenApp Servers</td>
</tr>
</tbody>
</table>

**Note:** Corporate LAN traffic outbound to DMZ and the Internet is assumed to be allowed.

### XenMobile Enterprise Edition

<table>
<thead>
<tr>
<th>TCP Port</th>
<th>Description</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>XenMobile MDM and App Controller Connectivity</td>
<td>XenMobile MDM</td>
<td>App Controller</td>
</tr>
<tr>
<td></td>
<td>XenMobile App Controller and MDM Connectivity</td>
<td>App Controller</td>
<td>XenMobile MDM</td>
</tr>
<tr>
<td></td>
<td>Sharefile Storage Zones</td>
<td>NetScaler Gateway</td>
<td>Sharefile Storage Zones</td>
</tr>
</tbody>
</table>

**Note:** All ports for XenMobile MDM and App Edition are also required for XenMobile Enterprise Edition.
Appendix B – Configuration Guidelines and Recommendations

Citrix recommends following the installation instructions as presented in the product documentation. However, in order to ensure a successful deployment of XenMobile, the following recommendations have been highlighted to supplement those instructions.

Integration of Windows Desktops and Apps with the App Controller

1. Logon to the App Controller console.
2. Proceed to the Apps & Docs tab.
3. Select the Windows Apps option from the left panel.
4. Input the host FQDN in the Host field.
5. Input the port information in the Port field.
6. Select the Allow secure access option.
7. Save the configuration.

![Figure B-1 – Integration of Windows Desktops and Apps with the App Controller](image)

Linking the Device Manager with the App Controller

1. Logon to the XDM server console.
2. Navigate to the App Controller.
3. Input the App Controller FQDN in the Host Name field.
4. Provide a Shared Key (common password) that will be used by both AppC and the Device Manager.
5. Select the Enable App Controller option, but do not select the Check connection button.
6. Select the Close button.
7. Select the Yes option when prompted to save the configuration.
1. Logon to the App Controller console.
2. Navigate to the **Settings** tab.
3. Select the **XenMobile MDM** option from the left pane.
4. Input the Device Manager FQDN in the **Host** field.
5. Input the port information in the **Port** field.
6. Provide the **Shared Key** (The one that was created on the Device Manager).
7. Verify the instance path is listed as `/zdm`.
8. Select **Require Device Manager enrollment** to force devices to enroll with the Device manager before gaining access to the unified store.
9. Select the **Test Connection** button.
10. Verify the **Test Connection was successful** message is displayed.
11. Close/Save.

---

1. Return to the XDM server console.
2. Navigate to the **App Controller**.
3. Select the **Check connection** button.
4. Verify the Check connection returns as a **Success**.

---

1. Return to the App Controller server console.
2. Select the **Save** button.

**Note:** Synchronization between the Device Manager and App Controller will commence and is expected to complete without issue. Upon completion, the infrastructure will have a fully integrated XDM and MAM environment.

**Figure B-2 – Linking the Device Manager with the App Controller**
About Citrix

Citrix (NASDAQ:CTXS) is the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.

Copyright © 2013 Citrix Systems, Inc. All rights reserved. Citrix, XenMobile, NetScaler, XenDesktop, XenApp ShareFile, Citrix Receiver, WorxMail, WorxWeb, ShareFile and GoToAssist are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.