VMware Horizon Mobile Manager Installation and Configuration

Horizon Mobile Manager 1.2

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000994-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware Horizon Mobile Manager Installation and Configuration Guide

VMware Horizon Mobile Manager Installation and Configuration Guide provides information about how to install and configure the VMware Horizon Mobile Manager virtual appliance.

The Horizon Mobile Manager virtual appliance provides the server-side components used in the Horizon Mobile solution. The overall installation and configuration process for the server-side components involves:

1 Determining which deployment configuration to use

2 Deploying the virtual appliance

3 Powering on the virtual appliance

4 Configuring settings for the appliance itself

5 Installing and configuring the items required for your chosen deployment configuration

6 Configuring settings for Horizon Mobile Manager, according to your chosen deployment configuration

7 Restarting to apply the selected settings

8 Determining the appropriate digital identity certificate approach to use, and optionally replace the default certificates

Intended Audience

This information is intended for experienced system administrators who are familiar with virtual machine technology and datacenter operations.

1 Deployment Configurations

Horizon Mobile Manager is designed to control, customize, and manage a corporate workspace on the users' mobile devices. The deployment configuration of Horizon Mobile Manager in your enterprise should support management of the workspace on the device without any constraints on whether the device is communicating with Horizon Mobile Manager over the corporate network or over the Internet.

The Horizon Mobile Manager virtual appliance contains an embedded Apache 2.2 server that provides the server-side management capabilities. The typical deployment configurations for Horizon Mobile Manager are described in the following table.

Table 1-1. Horizon Mobile Manager Deployment Configurations

Configuration	Description	Pros	Cons
Horizon Mobile Manager in a network demilitarized zone (DMZ).	In network computing, a network DMZ is a mixed-trust zone between the internal network services and the Internet. In this configuration, Horizon Mobile Manager's IP address is an external public IP address, and directly accessible on the Internet. The devices communicate with SSL requests to Horizon Mobile Manager's public IP address.	■ Easiest way to get Horizon Mobile Manager up and running. ■ No special network configuration needed other than an external IP address.	■ Unsuitable for production environments, because all of Horizon Mobile Manager services are publically exposed to the Internet. ■ Cannot configure Horizon Mobile Manager to connect to enterprise internal services such as Active Directory, LDAP, or corporate database services without opening ports through the enterprise's firewall.
Horizon Mobile Manager in the enterprise's internal network, and translate Horizon Mobile Manager's internal IP address to an externally available IP address using network address translation (NAT).	In this configuration, Horizon Mobile Manager has a private IP address. The devices communicate with SSL requests to an externally available IP address. Those SSL requests must be translated to Horizon Mobile Manager's private IP address using NAT.	■ Horizon Mobile Manager services are protected within the enterprise's firewall. ■ Horizon Mobile Manager can connect with internal services such as Active Directory, LDAP, or corporate database services without opening ports through the firewall. ■ NAT is a common network setup used and understood in enterprises.	■ Requires defining NAT rules that translate public IP requests to TCP/IP port 443 on the Horizon Mobile Manager's private IP address. ■ Horizon Mobile Manager's port 433 must be publically available. ■ Less than ideal architecture for an environment with clustered Horizon Mobile Manager servers that have one or more external reverse proxy Apache servers.
Horizon Mobile Manager in the enterprise's internal network, and use a reverse proxy server in the DMZ to handle the SSL requests from the devices on the Internet.	In this configuration, the reverse proxy server terminates the SSL requests from the devices, and then initiates new requests to Horizon Mobile Manager on the internal-facing side within the core network. The reverse proxy server converts requests for Horizon Mobile Manager's login, leasing, and download services to specific URLs that Horizon Mobile Manager supports.	■ Horizon Mobile Manager services are protected within the enterprise's firewall. ■ Horizon Mobile Manager can connect with internal services such as Active Directory, LDAP, or corporate database services without opening ports through the firewall. ■ Many enterprises typically use reverse proxy servers to isolate internal application servers from the Internet, and these	■ Requires careful planning to set up the reverse proxy server and the rules for its communication with Horizon Mobile Manager. ■ Requires involvement by networking teams to ensure that the reverse proxy server has a route to Horizon Mobile Manager on a secondary interface.

Table 1-1. Horizon Mobile Manager Deployment Configurations (Continued)

Configuration	Description	Pros	Cons
		existing proxy servers can be extended to work with Horizon Mobile Manager. ■ This configuration is the most scalable and secure architecture for deploying Horizon Mobile Manager in a production environment.	

Of the three configurations, installing Horizon Mobile Manager in the DMZ is the fastest way to get started to see how the Horizon Mobile solution works. However, because that configuration has Horizon Mobile Manager's services publically exposed to the Internet, it is the least secure. Use of the DMZ configuration should be used only for proof-of-concept demonstrations and testing purposes. Because of the visibility of Horizon Mobile Manager in the DMZ configuration, avoid connecting Horizon Mobile Manager in that configuration to any Active Directory or database server running in the internal network. For proof-of-concept demonstrations, use the embedded LDAP and database server installed with the Horizon Mobile Manager virtual appliance, and assign test users in that embedded LDAP to particular mobile devices to demonstrate Horizon Mobile Manager's administration capabilities.

While using a reverse proxy server is the most complex configuration to set up, it is the most secure, and is the best one for production deployment.

Install the Horizon Mobile Manager Virtual Appliance

2

Horizon Mobile Manager is distributed as a virtual appliance. The first step in the installation process is to deploy the Horizon Mobile Manager virtual appliance.

You can install the Horizon Mobile Manager virtual appliance on any OVF 1.0 compliant virtualization platform. The steps in the procedure describe deploying on vSphere.

To deploy the virtual appliance on vSphere, you need a Microsoft Windows desktop with vSphere Client installed.

Prerequisites

Download the Horizon Mobile Manager OVA file from the product download page.

Procedure

1 Log in to vSphere Client.

2 Select **File > Deploy OVF Template**.

3 Click **Browse** and browse to and select the Horizon Mobile Manager OVA file location.

4 Click **Next**.

5 Review the Horizon Mobile Manager template details, and click **Next**.

6 Read and accept the end user license agreement, and click **Next**.

7 Type a meaningful name for the Horizon Mobile Manager virtual appliance, and click **Next**.

8 Select **Thin provisioned format**, and click **Next**.

9 Review the options that you have chosen, and click **Finish**.

   A progress message indicates that the Horizon Mobile Manager virtual appliance is being deployed, and a success message indicates when the deployment is complete.

What to do next

Power on and configure the Horizon Mobile Manager virtual appliance. See Chapter 3, "Configure the Horizon Mobile Manager Virtual Appliance," on page 13.

Configure the Horizon Mobile Manager Virtual Appliance

3

Configure the network adapter for the virtual appliance and power it on. After powering on the virtual appliance, configure the appliance itself by changing the default password, setting a static IP address, and configuring the appliance's network settings.

Prerequisites

Install the Horizon Mobile Manager virtual appliance. See Chapter 2, "Install the Horizon Mobile Manager Virtual Appliance," on page 11.

Determine which deployment configuration to use. See Chapter 1, "Deployment Configurations," on page 7.

Procedure

1 In vSphere Client, on the **Getting Started** tab for the virtual appliance, click **Edit virtual machine settings**.

2 On the **Hardware** tab, configure the network adapter for the virtual appliance, according to the options appropriate for your chosen deployment.

Deployment Configuration	Description
Horizon Mobile Manager in your DMZ	Connect to a network interface in your DMZ.
Horizon Mobile Manager in your internal network, using NAT to translate a public IP to the internal IP	Connect to a network interface in your internal network.
Horizon Mobile Manager in your internal network, using a reverse proxy server to proxy external requests to the internal IP	Connect to a network interface in your internal network.

3 Power on the Horizon Mobile Manager virtual appliance in vSphere Client, and click the **Console** tab.

The virtual appliance displays messages while it is powering on. Read and accept the end user licensing agreement.

4 When the virtual appliance is powered on and the main menu is displayed, select **Login**.

5 Log in to the virtual appliance's Linux operating system using the appliance's default values: user name **`root`** and password **`vmware`**.

6 For security reasons, change the default root password.

7 Type **`exit`** to return to the main menu.

8 Select **Configure Network**.

9 Configure network settings according to the appropriate ones for your chosen deployment configuration.

Deployment Configuration	Description
Horizon Mobile Manager in your DMZ	Configure the appliance's network settings to use a static IP address. Respond to the prompts to configure the IP address, netmask, gateway, DNS servers, and hostname.
Horizon Mobile Manager in your internal network, using NAT to translate a public IP to the internal IP	a Configure the appliance's network settings to use a static, internal IP address. Respond to the prompts to configure the IP address, netmask, gateway, DNS servers, and hostname. If your internal network requires use of a forward proxy server, configure the proxy server. b Create NAT rules on your firewall to map TCP/IP port 443 to the appliance's internal IP address.
Horizon Mobile Manager in your internal network, using a reverse proxy server to proxy external requests to the internal IP	a Configure the appliance's network settings to use a static IP address. Respond to the prompts to configure the IP address, netmask, gateway, DNS servers, and hostname. If your internal network requires use of a forward proxy server, configure the proxy server. b Set up your reverse proxy server with two network interfaces: ■ One interface in your DMZ ■ One interface in your internal network c Configure the reverse proxy server to enable HTTPS connections, encrypting traffic between the Internet and the proxy server using Secure Sockets Layer (SSL) protocol connections. d Configure the proxy rules to require SSL connections, and to proxy the following URIs to Horizon Mobile Manager in the internal network: ■ `https://<your_domain_name>/provision` ■ `https://<your_domain_name>/leasing` ■ `https://<your_domain_name>/download` The embedded Apache server in Horizon Mobile Manager is configured to listen on specify TCP/IP ports for certain types of requests. Therefore, if the reverse proxy server uses the `mod_jk` or `mod_proxy_ajp` module, use TCP/IP port 8009 to contact Horizon Mobile Manager. If the reverse proxy server uses the `mod_proxy_http` module, use TCP/IP port 8080 to contact Horizon Mobile Manager.

When you are finished configuring the network settings for the virtual appliance on the **Console** tab, you are returned to the main menu.

Horizon Mobile Manager virtual appliance configuration is now complete.

What to do next

Connect to the Horizon Mobile Manager configuration interface to add license keys and configure settings. See Chapter 4, “Add License Keys,” on page 15 and Chapter 5, “Configure Horizon Mobile Manager Settings,” on page 17.

Add License Keys

4

Use the configuration interface to add license keys that enable the capability to manage work phones using Horizon Mobile Manager. Each license key provides for the license to manage a specific number of work phones with Horizon Mobile Manager.

Prerequisites

- Obtain one or more valid license keys. A license key is also referred to as a serial number in the configuration interface.
- Verify that you are using a recent version of a Chrome, Firefox, Internet Explorer, or Safari browser.

Procedure

1. In your browser, enter the Horizon Mobile Manager configuration interface URL, in the format **`https://`*`ip_address`*`:5480`**, where the *ip_address* is the one you set when you configured the virtual appliance itself.

   The web interface uses a self-signed certificate.

2. Log in as the **`root`** user.

   Use the password that you set when you configured the Horizon Mobile Manager virtual appliance. If you didn't change the default password, enter **`vmware`** as the password.

3. Click the **Horizon** tab, and click **Licenses**.
4. Click **Add Work Phone License**.
5. Enter the license key (serial number) and click **Add**.

After entering a valid license key, the system displays information related to the license, such as when the license expires and the number of work phones you are licensed to manage.

What to do next

If you haven't already done so, configure Horizon Mobile Manager settings. You must click **Save & Restart** on the **Settings** tab at least once to complete the Horizon Mobile Manager installation process. See Chapter 5, “Configure Horizon Mobile Manager Settings,” on page 17.

Configure Horizon Mobile Manager Settings

5

You must customize certain settings, or accept the default values, before Horizon Mobile Manager is ready for its initial use. You must click **Save & Restart** on the **Settings** tab to initialize elements that are needed to set up user workspaces in Horizon Mobile Manager, such as the base workspace image.

Prerequisites

- Verify that you are using a recent version of a Chrome, Firefox, Internet Explorer, or Safari browser.
- Add license keys. See Chapter 4, "Add License Keys," on page 15.
- If you are using either the NAT or the reverse proxy server deployment configuration, obtain the externally facing URL or IP address used in your deployment configuration. See Chapter 3, "Configure the Horizon Mobile Manager Virtual Appliance," on page 13.
- Obtain your organization's email-related information for sending email using an SMTP email server, and an email address that can receive a test configuration email.
- Determine whether to use the default values or specify custom values for the following items:

Database

You can use the embedded vPostgres database (the default) or your own external database. The following external databases are supported:

- Microsoft SQL Server 2008
- Oracle 11g R2

For example, you might want to use an external database in the following situations:

- To meet your company's database standards
- To provide management and backup using your company's standard database management practices
- To improve performance or load balancing when managing a large number of users

Installation of Horizon Mobile Manager in a clustered configuration requires use of an external database.

Naming service

You can use the embedded OpenLDAP naming service (the default) or your own naming service. Except for testing and initial deployments, typically you would use your own LDAP or Active Directory service.

Default system administrator

Determine which user account in your selected naming service is the account you want to use as the default system administrator for Horizon Mobile Manager. The default system administrator can log into the Horizon Mobile Manager administrative interface and perform all operations.

It is a good practice to limit use of this account to the initial setup of Horizon Mobile Manager, which includes assigning roles for ongoing operations to the appropriate users. To maintain a consistent audit trail, ongoing Horizon Mobile Manager operations should be carried out by Horizon Mobile Manager users who are assigned an administrator or fleet manager role. After you have completed the configuration procedure and initialization of base elements, have the default system administrator log into the Horizon Mobile Manager administrative interface to assign the appropriate Horizon Mobile Manager roles to users using the Roles & Jobs page.

Repository

You can use the default location for the Horizon Mobile Manager repository or specify another location. The repository stores Horizon Mobile Manager objects, such as workspace images, applications, and system files. By default, the repository path is `/opt/vmware-mmp/repo` in the file system of the Horizon Mobile Manager virtual appliance.

You might want to use a repository external to the virtual appliance if you are using Horizon Mobile Manager in a clustered configuration or if you plan to deploy many large applications in users' workspaces. Because the virtual appliance has a maximum disk size of 40 GB, if you plan to deploy many large applications that would exceed that capacity, choose a repository location that has suitable storage capacity.

NOTE You can update the settings on the **Settings** tab for an existing Horizon Mobile Manager installation at any time. However, updating some of these settings after the first use of Horizon Mobile Manager might result in additional effort needed to manually apply changes that were made in the system after the initial use. For example, if you initially choose to use the embedded OpenLDAP naming service and provision user devices, and then update the setting to use a different naming service, the existing users will not work unless the same user IDs are added to the new naming service.

Procedure

1 In your browser, enter the Horizon Mobile Manager configuration interface URL, in the format **`https://`*`ip_address`*`:5480`**

2 Log in as the **`root`** user.

Use the password that you set when you configured the Horizon Mobile Manager virtual appliance. If you didn't change the default password, enter **`vmware`** as the password.

3 Click the **Horizon** tab, and click **Settings**.

4 In the **Default administrator name** field, specify the name of a user to be the Horizon Mobile Manager system administrator.

The specified name must exist in the naming service you select to use for Horizon Mobile Manager. The displayed default value (**`admin`**) is a user account in the embedded OpenLDAP naming service. This default **`admin`** account has **`vmware`** as its password.

If you choose to use an external naming service, you must update the value in the **Default administrator name** field to a name that exists in your naming service.

5 Specify the location for the Horizon Mobile Manager file system repository.

You can enter a local or network file system path. By default, the repository path is `/opt/vmware-mmp/repo` in the virtual appliance's file system. When you click **Save & Restart**, the default objects provided by Horizon Mobile Manager (such as the base workspace image) are written into the specified location.

6 Type an externally facing root (entry level) URL for the login server, download server, and leasing server.

NOTE Because the workspaces on the managed mobile devices periodically communicate with Horizon Mobile Manager, the login, leasing, and download server URLs must be accessible from the devices on which the workspaces are or will be installed. If you are using either the NAT or the reverse proxy server deployment configuration, you must enter the externally facing URL used in that configuration.

Include **`https://`** at the beginning of the URLs. Even if you enter **`http://`**, the workspace on the devices uses the secure **`443`** port for communication with the servers.

These three URLs can be the same. For example, in a simple configuration of one Horizon Mobile Manager virtual appliance deployed with a public IP address, that virtual appliance can provide the server for administration, login, download, and leasing purposes. In this scenario, the URL specified for the login, download, and leasing servers is **`https://`*`ip_address`***, where the *ip_address* is the public IP address.

Server	Use
Login server	Used by the workspace user on their mobile device to install and download their workspace.
Download server	Provides software to workspaces.
Leasing server	Manages the workspace leases.

7 (Optional) To use your own Oracle or SQL Server database instead of the embedded database, select **Use external database** and select the database type from the drop-down menu. Then specify information that allows Horizon Mobile Manager to store and access data in the database.

Address (URL)	The address to the database.
User name	The database user for the database connection.
Password	The password for the database connection.
DBA user name	A database user of DBA level with DDL privileges, to create database objects used by Horizon Mobile Manager.
DBA password	The password for the DBA user
Validation query	SQL query to use to validate connections to the database.

For the external database, you can specify additional advanced settings, such as the initial size of the connection pool.

8 (Optional) To use your own naming service instead of the embedded OpenLDAP service, select **Use external service**, and select the type.

If you are using your own Active Directory naming service, you must enter the Active Directory domain.

If you are using your own LDAP naming service, you must enter the LDAP server URL, root DN, and user search query. You can also enter the manager DN user name and password.

9 Configure email settings for Horizon Mobile Manager to connect to your organization's email server:

a Enter your email server's SMTP host address and port information.

b (Optional) To use SSL encryption, select the **Use SSL** check box.

c (Optional) To use authentication, select the **Use authentication** check box and specify the user name and password to perform the SMTP authentication.

d Test the configuration by specifying a recipient email address and clicking **Send Email** to send a confirmation email.

   If the system can successfully send an email using the SMTP information, the confirmation email contains a verification code.

e Obtain the code from the confirmation email and enter the code in the **Code from test email** field.

10 Click **Save & Restart** to save the configuration settings and initialize the base elements needed to set up workspaces and manage employee devices using Horizon Mobile Manager.

   A message indicates that the restart is taking place.

When the restart process is complete, Horizon Mobile Manager is initialized, and you can log in to the administration interface using the user account specified for the default system administrator.

NOTE You must click **Save & Restart** to ensure the base elements are initialized before logging into the administration interface. Otherwise, some necessary elements might not be available for use.

What to do next

You can now configure workspace users in Horizon Mobile Manager. In your browser, enter the Horizon Mobile Manager administrator interface URL, in the format **`https://`*`ip_address`***

If you specify the embedded naming service and did not modify the default value for the system administrator name, you can log into the administrator interface with the **`admin`** user name and **`vmware`** password.

For more information about how to use Horizon Mobile Manager, after logging in, view the online help.

Horizon Mobile Manager Digital Certificate Requirements

6

Horizon Mobile Manager encrypts session information using standard digital certificates. In its default configuration, Horizon Mobile Manager uses automatically generated, self-signed certificates. You should use a certificate approach that is appropriate for your deployment configuration.

Communications between Horizon Mobile Manager and the mobile devices are sent over Secure Sockets Layer (SSL) protocol connections. Horizon Mobile Manager must present valid certificates to the devices, and also propagate signed certificates that are used in the workspaces on those devices. The certificates used in communications between Horizon Mobile Manager and the mobile devices are:

SSL certificate	Encrypts the secure session between the server and the client (the mobile device).
Signing certificate	Digitally signs communications between the server and the client.
Root and intermediate certificate authority (CA) certificates	Provide a certificate trust chain for determining whether to trust a particular SSL or signing certificate.

When you initially install and configure Horizon Mobile Manager, a self-signed SSL certificate and a signing certificate are automatically generated using an automatically generated internal root Certificate Authority (CA) and the URL specified for the leasing server (see Chapter 5, "Configure Horizon Mobile Manager Settings," on page 17). The Security page in the Horizon Mobile Manager's administration interface lists the aliases for the automatically generated certificates.

NOTE Do not remove the `internal-ca-root` entry in the **Server Trust Certificate Chain** list in the Security page in Horizon Mobile Manager. That certificate is the automatically generated internal root CA and should not be removed except under controlled circumstances and following a specific sequence of steps. For more information, see the VMware knowledge base article at http://kb.vmware.com/kb/2035492.

Although these certificates are unique and allow for initial or proof-of-concept use of the server, they are not signed by a trusted well-known CA. Determine whether to replace the automatically generated certificates with your own self-signed certificates, or certificates signed by a commercial certificate authority. For a description of the deployment configurations, and when and how to use your own SSL and signing certificates, see the VMware knowledge base article at http://kb.vmware.com/kb/2035492.

NOTE When the SSL certificate is a self-signed certificate (either your own or the one automatically generated in Horizon Mobile Manager), before the device user starts the VMware® Switch application to install their corporate workspace for the first time, the user must clear the **Authenticate Server** check box in the VMware® Switch application settings. That check box is selected by default. If the **Authenticate Server** check box is not cleared and the SSL certificate is a self-signed certificate, the device attempts to use the Android trust store of well-known CAs to verify the certificate. Because the certificate is not signed by a well-known CA, the session fails to authenticate and the device refuses to connect to Horizon Mobile Manager.

To display the **Authenticate Server** setting for the VMware® Switch application on the device, open the device's **Application Settings** display, touch **VMware Switch**, and touch **Manage Space**. If you are using a self-signed SSL certificate, clear the **Authenticate Server** check box.

After the corporate workspace is installed on the device, the user can select the **Authenticate Server** check box in the VMware® Switch application settings. After the initial install of the workspace, communications use the certificates contained in the workspace. If the workspace is subsequently wiped, the user must clear the **Authenticate Server** check box to re-install their workspace, when the SSL certificate is a self-signed certificate.

Configure NDES Settings For Use with Horizon Mobile Manager

7

Horizon Mobile Manager includes a Simple Certificate Enrollment Protocol (SCEP) connector plug-in for the Microsoft Network Device Enrollment Service (NDES). This SCEP connector plug-in supports a connection between Horizon Mobile Manager and your company's Microsoft NDES server, to automate the process of creating digital certificates for the managed devices.

Prerequisites

- Verify that you are using a recent version of a Chrome, Firefox, Internet Explorer, or Safari browser.
- Add license keys. See Chapter 4, "Add License Keys," on page 15.
- Configure Horizon Mobile Manager settings and click **Save & Restart** to initialize the system. See Chapter 5, "Configure Horizon Mobile Manager Settings," on page 17.

Procedure

1 In your browser, enter the Horizon Mobile Manager configuration interface URL, in the format `https://ip_address:5480`

2 Log in as the `root` user.

Use the password that you set when you configured the Horizon Mobile Manager virtual appliance. If you didn't change the default password, enter `vmware` as the password.

3 Click the **Horizon** tab, and click **SCEP**.

The NDES connector that is provided by Horizon Mobile Manager is listed in the SCEP Connectors list.

4 Click **Add SCEP Server**.

In the Add a SCEP Server window, supply the following information:

Server Name	The name of your company's Microsoft NDES server.
External URL	The URL that NDES clients use to contact your company's Microsoft NDES server.
SCEP Connector	The SCEP connector plug-in used to connect to the NDES server. The provided NDES connector is displayed.
Admin URL	The URL that administrators use to manage your company's Microsoft NDES server.
Admin Username	The user name of your company's NDES administrator.

Admin Password	The password of your company's NDES administrator.
Domain	The name of the Windows domain in which your company's NDES administrator account was created.

5 Click **Add** to add the NDES server information to Horizon Mobile Manager

Index