VMware Horizon Mobile Manager Installation and Configuration Guide

Horizon Mobile Manager 1.3

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-001072-00

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, and how to verify operations of your installation.

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 replacing 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

The Horizon Mobile Manager virtual appliance is designed to control, customize, and manage a corporate workspace on your users' mobile devices. The appliance uses an embedded Apache 2.2 server to provide the server-side management capabilities, and sends communications over Secure Sockets Layer (SSL) protocol connections. You should deploy the virtual appliance so that it can manage workspaces on the devices whether those devices are communicating over a corporate network or over the Internet.

The typical deployment configurations for Horizon Mobile Manager are described in the following table.

Table 1-1. Horizon Mobile Manager Deployment Configurations

Configuration	Description	Advantages	Disadvantages
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 is 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. ■ Prevents connections between Horizon Mobile Manager and enterprise internal services such as Active Directory, LDAP, or corporate database services, unless ports to those services are accessible through the enterprise's firewall.
Horizon Mobile Manager in the enterprise's internal network, using network address translation (NAT) to translate its internal IP address to an externally available IP address.	In this configuration, Horizon Mobile Manager has a private IP address. The devices communicate with SSL requests to an externally available IP address, and those SSL requests are 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 to receive the requests from NAT. ■ 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, using 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 handles the SSL communications with 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 the specific URLs used by Horizon Mobile Manager.	■ 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. ■ More easily leverages existing corporate infrastructure. 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 to communicate with Horizon Mobile Manager. ■ Requires configuring the reverse proxy server for SSL communications using your own SSL certificate. ■ 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	Advantages	Disadvantages
		existing proxy servers can be extended to work with Horizon Mobile Manager.	

Of the three configurations, installing Horizon Mobile Manager in the DMZ is the fastest way to get started to see how the VMware® 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 VMware vSphere®.

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

Prerequisites

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

Procedure

1 Log in to the 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 the 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 the 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 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 VMware® vFabric™ Postgres 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	Determine what directory service to use to provide user account information to Horizon Mobile Manager. By default, the virtual appliance includes a preconfigured, embedded OpenLDAP service. This embedded OpenLDAP service is suitable for experimental use in proof-of-concept demonstrations or test environments. In production environments, you should use your organization's LDAP or single-domain Active Directory naming service. Use of multiple Active Directory domains is not supported.
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. Use of multiple Active Directory domains is not supported.

   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 in to 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.

Configure NDES Settings For Use with Horizon Mobile Manager

6

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

Digital Certificates and Horizon Mobile Manager

7

Horizon Mobile Manager encrypts session information using standard digital certificates, and communications between Horizon Mobile Manager and the mobile devices are sent over SSL protocol connections. The deployment environment must support the ability for Horizon Mobile Manager to present valid certificates to the devices, and also to 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 server URLs that you enter in the configuration user interface (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.

In its default configuration, Horizon Mobile Manager uses these automatically generated, self-signed certificates. To decide between using the default certificates or replacing them with your own, you must consider:

- Which approach is more appropriate for your chosen deployment configuration.
- What requirements you can impose on the device owners. Using self-signed SSL certificates requires your device owners to update authentication settings on their devices to ensure the devices can communicate with the server (see "Mobile Device Requirements When Using Self-Signed SSL Certificates," on page 25).

CAUTION Any changes you make by replacing the default certificates in the embedded Apache server will be lost if you change the leasing server URL used by Horizon Mobile Manager. The leasing server URL is set in the Horizon Mobile Manager configuration interface (as described in Chapter 5, "Configure Horizon Mobile Manager Settings," on page 17). When you click the **Save & Restart** button in the configuration interface, the system automatically generates new default certificates using that leasing server URL as the domain and signed by the internal MVP root CA. The new generated certificates replace the previously used ones. Therefore, if you replace the default certificates with your own, and then subsequently change the leasing server URL, you must repeat the certificate replacement process.

Certificate Approaches By Deployment Configuration

The following table outlines the appropriate options for each deployment configuration.

Table 7-1. Horizon Mobile Manager Deployment Configurations and Appropriate Certificate Approaches

Configuration	Certificate Choices
Horizon Mobile Manager in your network DMZ	■ Use the default self-signed certificates in the embedded Apache server. ■ Replace the default self-signed certificates in the embedded Apache server with your own certificates. Your certificates can be self-signed or signed by a trusted CA. When you replace a default certificate, you must upload the root CA certificate and any intermediate CA certificates that are in that certificate's trust chain. See "Replacing the Default Certificates With Trusted Signed Certificates," on page 25 and "Replace the Default SSL Certificate In a DMZ or NAT Deployment Configuration," on page 26.
Horizon Mobile Manager in the enterprise's internal network, and using NAT	■ Use the default self-signed certificates in the embedded Apache server. ■ Replace the default self-signed certificates in the embedded Apache server with your own certificates. Your certificates can be self-signed or signed by a trusted CA. When you replace a default certificate, you must upload the root CA certificate and any intermediate CA certificates that are in that certificate's trust chain. See "Replacing the Default Certificates With Trusted Signed Certificates," on page 25 and "Replace the Default SSL Certificate In a DMZ or NAT Deployment Configuration," on page 26.
Horizon Mobile Manager in the enterprise's internal network, and using a reverse proxy server in the DMZ	Because using a reverse proxy server requires that server to be configured for SSL communications, you use your own SSL certificate in your reverse proxy server. This certificate can be self-signed or signed by a trusted CA. In this configuration, you must upload the root CA certificate and any intermediate CA certificates that are in that SSL certificate's trust chain. See "Replacing the Default Certificates With Trusted Signed Certificates," on page 25 and "Use Your Own Trusted Signed SSL Certificate In a Reverse Proxy Server Deployment Configuration," on page 28.

This chapter includes the following topics:

Mobile Device Requirements When Using Self-Signed SSL Certificates

Although the automatically generated 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. As a result, before your device owners start the VMware® Switch application to install their corporate workspace for the first time, they must update the Switch application's default authentication setting.

When Horizon Mobile Manager uses self-signed SSL certificates, device owners must deselect the **Authenticate Server** check box in the Switch application settings. That check box is selected by default when the Switch application is installed. When the **Authenticate Server** check box is selected 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.

If your Horizon Mobile Manager deployment is using a self-signed SSL certificate (either the one automatically generated by default or your own self-signed certificate), notify your device owners to ensure that they deselect the **Authenticate Server** check box before they start the Switch application for the initial installation of the workspace. When that check box is deselected, the device ignores the fact that the SSL certificate is self-signed and allows the connection to Horizon Mobile Manager. To display the **Authenticate Server** setting for the Switch application on the device, open the device's **Application Settings** display, touch **VMware Switch**, and touch **Manage Space**.

NOTE When the **Authenticate Server** check box is deselected and the device owner begins the initial installation, a message is displayed warning the user about this condition, even though the communication is secured with the SSL protocol.

Replacing the Default Certificates With Trusted Signed Certificates

Replacing the default self-signed SSL certificate with a certificate that is signed by a trusted Certificate Authority (CA) avoids requiring device owners to alter the Switch application settings.

NOTE While there are benefits to replacing the default SSL certificate with one that is signed by a trusted CA, there is usually no strong reason to replace the default signing certificate unless you suspect the automatically generated internal-ca-root certificate has been compromised.

For a DMZ or NAT deployment, you replace the automatically generated SSL certificate in the embedded Apache server with your own trusted signed SSL certificate. In the reverse proxy server configuration, you use your own trusted signed SSL certificate in your reverse proxy server. In all deployment configurations, if you use your own certificate (SSL or signing) you must upload to Horizon Mobile Manager the root CA certificate and any intermediate CA certificates that are in the replacement certificate's trust chain.

The general procedure to replace either the default SSL certificate or signing certificate with your own trusted signed certificate:

1 Generate a private key and a Certificate Signing Request (CSR).

2 Send the CSR to the certificate authority (CA) that you are having sign your certificate.

The CA sends your signed certificate to you, along with the CA's trusted certificate chain of root and intermediate certificates used by your certificate.

3 Load your signed certificate and the CA certificates that signed your certificate so they can be used by Horizon Mobile Manager:

In the DMZ or NAT configuration	Load your trusted SSL certificate into the embedded Apache server from the virtual appliance's console. Load a replacement signing certificate using the administration interface.
In the reverse proxy server configuration	Load your trusted SSL certificate into your reverse proxy server. Load a replacement signing certificate using the administration interface.
For all configurations	Load the root and intermediate CA certificates for any replacement certificates (SSL or signing) using the administration interface.

Replace the Default SSL Certificate In a DMZ or NAT Deployment Configuration

To use your own trusted signed SSL certificate when using Horizon Mobile Manager in your DMZ or in the NAT deployment configuration, you replace the automatically generated one with your own certificate.

Prerequisites

Install and configure the Horizon Mobile Manager virtual appliance.

In the vSphere Client, power on the virtual appliance, click the **Console** tab, and log in to the virtual appliance's Linux operating system as the **`root`** user. Use the password that you set when you configured the virtual appliance. If you did not change the default password, enter **`vmware`** as the password.

Procedure

1 In the virtual appliance's console, run the following command to generate a private key and a CSR.

```
openssl req –out CSR.csr –new –newkey rsa:2048 –nodes –keyout privateKey.key
```

The command prompts you for the information required for the CSR.

2 At the prompts, enter the information that is appropriate for your enterprise.

For the **`Common Name`**, enter the fully qualified domain name that the device owners need to enter in the Switch application to log into the server and initially set up their workspaces. This domain name should be:

- The fully qualified domain name that is externally resolvable to the public IP address used in this Horizon Mobile Manager deployment.
- The same externally facing URL that was entered for the **Login Server URL** (without the https:// portion of that URL) when the virtual appliance was configured.

For example, the following code block shows entries for a login server URL of *our.domainname.com*.

```
Generating a 2048 bit RSA private key
.............................................+
++...........+++
writing new private key to 'privateKey.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Massachusetts
Locality Name (eg, city) [ ]:Cambridge
```

```
Organization Name (eg, company) [Internet Widgets Pty Ltd]:OurCompany
Organizational Unit Name (eg, section) [ ]:OurUnit
Common Name (eg, YOUR name) [ ]:our.domainname.com
Email Address [ ]:ourwebmaster@ourcompany.com
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password [ ]:
An optional company name [ ]:
```

The command generates two files: `CSR.csr` and `privateKey.key`.

3 Send the `CSR.csr` file to your certificate authority. The certificate authority sends you the signed certificate (such as `cert.pem`), the root and intermediate CA certificates used by your certificate, and the certificate chain file (such as `chain.pem`) to use with it.

4 Log in to the Horizon Mobile Manager administration interface as an administrator. In your browser go to the Horizon Mobile Manager administration URL, in the format **`https://`*`ip_address`***, where *ip_address* is Horizon Mobile Manager's private IP address. Log in using a Horizon Mobile Manager user account that has been assigned the Administrator role. If your deployment is configured to use the embedded naming service and you did not modify the default value for the system administrator name, you can log in to the administration interface with the **`admin`** user name and **`vmware`** password.

5 Click **Security** to display the Security page.

6 In the **Server Trust Certificate Chain** section, upload the root CA certificate and intermediate CA certificates that signed your SSL certificate. Upload each certificate by clicking the **Upload New Certificate** button.

This step ensures that when mobile devices are provisioned, the root CA certificate and intermediate CA certificates needed to trust the SSL communications are included in the keystore of the workspace on the device.

CAUTION Do not remove any of the certificates listed in the **Server Trust Certificate Chain** list, especially a root CA certificate (including the default MVP Internal CA certificate), except under very controlled circumstances. Removing a root CA certificate from the **Server Trust Certificate Chain** list will remove it from all provisioned devices at the next lease renewal operation. Unless you have provided a replacement root certificate, those provisioned devices must be wiped and reprovisioned. It is extremely rare to have to remove a certificate from the list. The only reason to remove a certificate from this list is if you suspect the certificate has been compromised. In that situation, you must follow a specific sequence of steps to ensure that workspaces already installed on user devices remain operational (as described in "Change Root CA and Intermediate CA Certificates For Provisioned Workspaces," on page 30).

7 If devices have already been provisioned by this Horizon Mobile Manager instance, wait for the lease renewal time to elapse so that all devices make a leasing call. When the lease is renewed, the root CA certificates and intermediate CA certificates are sent to the workspaces. Waiting for the lease renewal time to elapse ensures that the certificate trust chain is installed in the keystores of the workspaces before the new SSL certificate is used in the embedded Apache server.

CAUTION Any devices that are disconnected and go without network access for longer than the leasing interval are not able to obtain the new certificates in this step. Workspaces on devices that are disconnected for a time period that extends past that leasing interval such that they do not obtain the new certificates will not trust the SSL communication with the server when those devices regain network access. Those workspaces will have to be wiped and reprovisioned to enable communications.

8 Use the `scp` command to secure copy the signed SSL certificate to the virtual appliance's file system.

9 In the virtual appliance's file system, edit the `/etc/apache2/vhosts.d/mmp.conf` file, and verify the lines related to the SSL certificate files are present in the file, and ensure the paths point to the certificates and your generated private key.

For example:

```
SSLCertificateFile /path/to/the/signed/cert.pem
SSLCertificateKeyFile /path/to/your/generated/privateKey.key
SSLCertificateChainFile /path/to/the/cert/chain.pem
```

10 Restart the Apache server using this command: `/etc/init.d/apache2 graceful`

After restarting, the embedded Apache server uses the new SSL certificate.

Use Your Own Trusted Signed SSL Certificate In a Reverse Proxy Server Deployment Configuration

Because using a reverse proxy server requires that server to be configured for SSL communications, you use your own SSL certificate in your reverse proxy server. While this certificate can be self-signed or signed by a trusted CA, one of the benefits of replacing the default self-signed SSL certificate with a certificate that is signed by a trusted CA is to avoid requiring the device owners to clear the **Authenticate Server** check box in the Switch application.

For this deployment configuration, you must upload to Horizon Mobile Manager the root CA certificate and any intermediate CA certificates that are in your SSL certificate's trust chain. It is recommended that you perform the trust chain upload before provisioning any devices, so that they will have the correct trust chain when their workspaces are first installed on the devices.

Prerequisites

Power on the Horizon Mobile Manager virtual appliance.

Procedure

1 Log in to the Horizon Mobile Manager administration interface. In your browser, go to the Horizon Mobile Manager administration URL, in the format **`https://ip_address`**, where *ip_address* is Horizon Mobile Manager's private IP address. Log in using a Horizon Mobile Manager user that has been assigned the Administrator role. If your deployment is configured to use the embedded naming service and you did not modify the default value for the system administrator name, you can log in to the administration interface with the **`admin`** user name and **`vmware`** password.

2 Click **Security** to display the Security page.

3 In the **Server Trust Certificate Chain** section, upload the root CA certificate and intermediate CA certificates that signed your SSL certificate. Upload each certificate by clicking the **Upload New Certificate** button.

This step ensures that when mobile devices are provisioned, the root CA certificate and intermediate CA certificates needed to trust the SSL communications are included in the keystore of the workspace on the device.

CAUTION Do not remove any of the certificates listed in the **Server Trust Certificate Chain** list, especially a root CA certificate (including the default MVP Internal CA certificate), except under very controlled circumstances. Removing a root CA certificate from the **Server Trust Certificate Chain** list will remove it from all provisioned devices at the next lease renewal operation. Unless you have provided a replacement root certificate, those provisioned devices must be wiped and reprovisioned. It is extremely rare to have to remove a certificate from the list. The only reason to remove a certificate from this list is if you suspect the certificate has been compromised. In that situation, you must follow a specific sequence of steps to ensure that workspaces already installed on user devices remain operational (as described in "Change Root CA and Intermediate CA Certificates For Provisioned Workspaces," on page 30).

At this point, devices can be provisioned using the reverse proxy server.

Replace the Default Signing Certificate

There is usually no strong reason to replace the default signing certificate unless you suspect the automatically generated internal-ca-root certificate has been compromised.

Prerequisites

Power on the Horizon Mobile Manager virtual appliance.

Procedure

1 Log in to the administration interface as an administrator, and click **Security** to display the Security page.

2 Generate the CSR to send to your CA by clicking the **Generate Certificate Signing Request** button in the **Server Signing Certificate** section.

3 Email the CSR to your CA.

4 When your CA sends back the new signing certificate and the root CA and intermediate CA certificates that signed it, expand the **Server Trust Certificate Chain** section on the Security page, and upload each root CA and intermediate CA certificate by clicking **Upload New Certificate**.

CAUTION Do not remove any of the certificates listed in the **Server Trust Certificate Chain** list, especially a root CA certificate (including the default MVP Internal CA certificate) until after Step 5, and the lease renewal time has passed.

5 Wait for the lease renewal time to elapse so that all devices make a leasing call. When the lease is renewed, the root CA certificates and intermediate CA certificates are sent to the workspaces. Waiting for the lease renewal time to elapse ensures that the certificate trust chain for the replacement signing certificate is installed in the keystores of the workspaces before you make the new signing certificate the active one.

CAUTION Any devices that are disconnected and go without network access for longer than the leasing interval are not able to obtain the new certificates in this step. Workspaces on devices that are disconnected for a time period that extends past that leasing interval such that they do not obtain the new certificates will not function properly when those devices regain network access. Those workspaces will have to be wiped and reprovisioned.

6 On the Security page, expand the **Server Signing Certificates** section and upload the new signing certificate sent by your CA by clicking **Upload New Certificate**.

7 Use the **Signing Certificate** drop-down list to select the new signing certificate and make it the active one.

CAUTION Do not remove the previously used signing certificate from the **Server Signing Certificate** list until after Step 8, and a second lease renewal time has passed.

8 Wait for the lease renewal time to elapse so that all devices make another leasing call. When the lease is renewed, the new signing certificate is sent to the workspaces as the active signing certificate. Waiting for the lease renewal time to elapse ensures that the workspaces are using the new certificate to sign messages before you remove the old signing certificate from the list.

CAUTION Any devices that are disconnected and go without network access for longer than the leasing interval are unable to use the new active signing certificate in this step. Workspaces on devices that are disconnected for a time period that extends past that leasing interval will not function properly when those devices regain network access. Those workspaces will have to be wiped and reprovisioned.

9 On the Security page, expand the **Server Signing Certificates** list and remove the older signing certificate. At this point, you can also remove the root CA and intermediate CA certificates that are associated with the older signing certificate, unless they are also used for the new signing certificate.

At this point, the replacement signing certificate is the active one used by the devices.

Change Root CA and Intermediate CA Certificates For Provisioned Workspaces

The provisioned workspaces use the certificate trust chain specified in the administration interface to verify the identities of the server-side SSL certificate and signing certificate used by Horizon Mobile Manager. This certificate trust chain is deployed to the workspace when the workspace is provisioned to the device. If you suspect that a certificate in that certificate trust chain is compromised, this sequence of steps must be followed to replace the compromised certificate.

Following this sequence of steps ensures the new certificate trust chain is deployed to the provisioned workspaces before you remove individual certificates from the trust chain. If these steps are not followed and the deployed certificate chain of trust becomes broken (for example, by removal of a root CA certificate before the workspaces are able to obtain the replacement root CA certificate), the workspaces on the devices will cease to work properly, and the workspaces must be wiped and reprovisioned.

Prerequisites

Power on the Horizon Mobile Manager virtual appliance.

Procedure

1. Log in to the Horizon Mobile Manager administration interface as an administrator, and click **Security** to display the Security page.
2. Add the new root CA certificate and any intermediate CA certificates to the **Server Trust Certificate Chain** section by clicking **Upload New Certificate** to add each certificate.
3. Wait for a lease renewal time period to pass so that all devices make a leasing call to the server. When the lease is renewed, the specified set of root CA certificates and intermediate CA certificates (including both the old and the new ones) are deployed to the workspaces.
4. After the lease renewal time has passed, you can click the **Remove** button next to the compromised certificate in the **Server Trust Certificate Chain** section.

At the next lease renewal, the certificate trust chain is again deployed to the provisioned workspaces, not including the removed compromised certificate. From that point on, the workspaces use the updated certificate trust chain.

CAUTION Any devices that are disconnected and go without network access for longer than the leasing interval cannot obtain the new certificates. Workspaces on devices that are disconnected for a time period that extends past that leasing interval such that they do not obtain the new certificates will not function properly when those devices regain network access. Those workspaces will have to be wiped and reprovisioned.

Recover a Root CA Certificate Accidentally Removed from the Certificate Trust Chain

If a Horizon Mobile Manager administrator accidentally clicks **Remove** next to a root CA certificate in the **Server Trust Certificate Chain** list, the system displays a warning that deleting the root CA certificate could result in a catastrophic failure. Already provisioned workspaces could lose the ability to trust communications with the server when the root CA certificate is deleted. If the administrator selects to proceed with deleting the root CA certificate without following the replacement procedure and then needs to restore the earlier configuration, you can use the following procedure to restore the removed root CA certificate to the certificate trust chain.

Prerequisites

In the vSphere Client, power on the virtual appliance, click the **Console** tab, and log in to the virtual appliance's Linux operating system as the **`root`** user. Use the password that you set when you configured the virtual appliance. If you did not change the default password, enter **`vmware`** as the password.

Procedure

1 Run the following commands.

```
su tcserver
mkdir /opt/vmware-mmp/repo/security/certs-for-devices/internal-ca-root
cp /opt/vmware-mmp/repo/security/root/cert.pem /opt/vmware-mmp/repo/security/certs-for-
devices/internal-ca-root/
```

2 In the administrative interface, refresh the Security page. The root CA certificate is restored to the **Server Trust Certificate Chain** list.

What to do next

After the deleted root CA certificate is restored, you must wipe and reprovision the workspaces so that the restored certificate trust chain is deployed to the devices.

Manual Verification Tests

8

Use these manual tests to verify that your Horizon Mobile Manager installation can provision and manage workspaces on VMware® Ready™ smartphones.

Before starting these tests, verify that you have the following items:

- An installed, configured, and powered-on Horizon Mobile Manager instance.
- A VMware Ready smartphone with:
  - Data access (Wi-Fi, 3G, LTE) to that Horizon Mobile Manager instance.
  - An active Wi-Fi connection.
  - An installed SIM card.
  - The VMware Switch application installed. The VMware Switch application is available from Google Play.

    If you have not configured this Horizon Mobile Manager instance to use a trusted signed SSL certificate, verify that the **Authenticate Server** check box is deselected in the Switch settings. See "Mobile Device Requirements When Using Self-Signed SSL Certificates," on page 25.
- Name and password for the Horizon Mobile Manager default system administrator (see Chapter 5, "Configure Horizon Mobile Manager Settings," on page 17).
- Three test users (their names and passwords). These users must exist in the naming service that is used by your Horizon Mobile Manager instance. The naming service is specified during the installation and configuration of the Horizon Mobile Manager virtual appliance. If your instance is using the preconfigured embedded OpenLDAP service, use the three preconfigured users such as **`user20`**, **`user21`**, and **`user22`**. The password for the three preconfigured users is **`vmware`**.
- Five image files (in JPG or PNG formats) for the branding and wallpaper test procedures. The images should have the following sizes:
  - Horizon Mobile Manager site logo image: 80 pixels by 50 pixels.
  - Login screen image: 600 pixels by 400 pixels.
  - On-device company logo image: 200 pixels by 200 pixels.
  - Workspace wallpaper images (two files): 960 pixels by 640 pixels.
- The login server URL for this Horizon Mobile Manager instance.
- A URL to use in a shortcut on the workspace (such as your company's Web site URL).

Tests that involve the VMware Email client application require an email client account (that will be used by the device user) and Wi-Fi access to the email server (either Microsoft Exchange or VMware Zimbra).

The following terms are used in the verification tests:

administrator	Refers to a user that is assigned the Administrator role in Horizon Mobile Manager.
fleet manager	Refers to a user that is assigned the Fleet Manager role in Horizon Mobile Manager.
personal phone	Refers to the personal side of the phone. After a workspace is installed, the phone has two sides: the personal phone and the workspace. When the phone has an installed workspace, you can switch between the two sides by touching the **Switch** icon.

This chapter includes the following topics:

Create Administrators and Fleet Managers by Assigning Roles to Users

In production environments, you assign roles to individuals in your organization according to their responsibilities for performing administrative and management operations. This test verifies that you can assign roles to such users.

During initial configuration of the Horizon Mobile Manager virtual appliance, a user account is specified as the default system administrator. That default system administrator can log into the administration interface and perform all operations. However, after the initial setup, to maintain a consistent audit trail, ongoing operations should be carried out by users who are assigned a specific role as an administrator or a fleet manager. The system displays to a logged-in user only those features that correspond to the types of operations their assigned role has the rights to perform. For a description of the operations associated with the standard roles, see the Horizon Mobile Manager Administration online help.

NOTE If your instance uses the embedded OpenLDAP service, you can use **`user20`** and **`user21`** for this test. Assign the administrator role to **`user20`** and the fleet manager role to **`user21`**. The password for both users is **`vmware`**.

Prerequisites

Verify that you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Procedure

1 Log in to Horizon Mobile Manager as the default system administrator (the one that was specified during the configuration of this instance of Horizon Mobile Manager). If your organization retained the default values during the configuration process, use the name **`admin`** and the password **`vmware`**.

2 Click **Roles & Jobs** in the left navigation, and click **Edit.**

3 Assign the administrator or fleet manager role to those users in your organization to whom you want to give those responsibilities:

   a In the Add Roles column, search for the user. When the system displays the user's name, click **Add Roles**. Select the appropriate role for that user. For example, if you are using the preconfigured users for this test, assign the administrator role to **`user20`**.

   b Repeat Step 3a to assign roles to additional users. For example, if you are using the preconfigured users for this test, assign the fleet manager role to **`user21`**.

4 Click **Save**.

What to do next

Verify that the assigned roles are in effect:

1 Log in to the administration interface as a user that has been assigned only the fleet manager role (for example, **`user21`**). Verify that the left navigation displays the following names: **Dashboard**, **Users**, **Groups**, **Policy Sets**, **Templates**, **Workspace Images**, and **Applications**. The **Roles & Jobs**, **Branding**, and **Security** choices are not displayed in the left navigation, because the rights to perform their associated operations belong to the administrator role.

2 Log in to the administration interface as a user that has been assigned only the administrator role (for example, **`user20`**). Verify that the left navigation displays the following page names: **Dashboard**, **Roles & Jobs**, **Branding**, and **Security**. No other choices are displayed, because the administrator role only has rights to perform operations associated with the displayed choices.

Create a Template

In this test, you create a template. A template defines a corporate workspace that can be deployed to users' mobile devices. A template determines the software that is included in the workspace, and the wallpaper background and shortcuts for the workspace home display.

Prerequisites

Verify you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Complete the steps in "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34.

Procedure

1 Log in to the administrative interface as a fleet manager (such as **`user21`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 Click **Templates** in the left navigation, and click **Create New Template**.

3 Type a name and description, for example:

- **Name:** **`Sales Template`**
- **Description:** **`Template for employees in the Sales organization`**

4 In the **All applications** section, include the VMware View application in the workspace by clicking its green **+** icon. Verify that two applications are displayed in the **Deployed applications** section: VMware Email and VMware View.

5 In the **Customization** section:

   a Change the wallpaper by clicking **Upload New**. Enter a name for the wallpaper (such as **`Our Wallpaper`**), and browse to one of your 960 pixels by 640 pixels image files. Click **Save**, and use the drop-down menu to select your wallpaper.

   b Click **Add Shortcut** and enter a name and a URL (such as your company's main Web site).

6 Click **Save**.

What to do next

Verify that the template is created:

1 In the left navigation, verify that the name of your template is displayed under **Template**.

2 Click your template, and verify that it displays the two applications (VMware Email and VMware View) and the shortcut that you specified.

Create a Policy Set

In this test, you create a policy set. A policy set controls the actions that device users can perform in the corporate workspace, as well as security settings such as password strength and expiration.

Prerequisites

Verify you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Complete the steps in "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34.

Procedure

1 Log in to the administrative interface as a fleet manager (such as **`user21`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 Click **Policy Set** in the left navigation, and click **Create New Policy Set**.

3 Type a name and description, for example:

- **Name:** **`Sales Group Policies`**
- **Description:** **`Policy settings for employees in the Sales organization`**

4 In the **Lease Renewal** section, select an interval of 20 minutes. Do not change the automatic disable or automatic wipe settings.

5 Expand the **Password** section. Verify that **Require Password** is selected, and the **Password Strength** is set to **PIN**.

6 Click **Save**.

What to do next

Verify that the policy set is created:

1 In the left navigation, verify that the name of your policy set is displayed under **Policy Sets**.

2 Click your policy set, and verify that it displays the description and lease renewal interval that you specified.

Create a Group and Add a User to the Group

In this test, you create a group that is used to associate the device user with the corporate workspace. A mobile device user must belong to a group before that user's device can be provisioned with a corporate workspace. A user's group determines what software is installed in, and what policies apply to the corporate workspace that is deployed to the device.

Prerequisites

Verify you have the users as described in Chapter 8, "Manual Verification Tests," on page 33.

Complete the steps in "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34, "Create a Template," on page 35, and "Create a Policy Set," on page 36.

Procedure

1 Log in to the administrative interface as a fleet manager (such as **`user21`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 Click **Groups** in the left navigation, and click **Create New Group**.

3 Type a name and description, for example:

- **Name:** **`Sales Group`**
- **Description:** **`Employees in the Sales organization`**

4 Select the template and policy set created in "Create a Template," on page 35 and "Create a Policy Set," on page 36.

5 In the search field in the **Add Users** column, type the name of the device user that you identified for use in these verification tests. The available users are those in the naming service that was specified in the configuration of your Horizon Mobile Manager instance. If this instance is using the embedded OpenLDAP service, type **`user23`**.

6 When the system displays the name of the user in the list, click **Add** in that user's row. The user name is displayed in the Group Users column, indicating that the user is assigned to this group.

7 Click **Save**.

What to do next

Verify that the group is created and the selected user is assigned to it:

1 In the left navigation, verify that the name of your group is displayed under **Groups**.

2 Click your group, and verify that your selected user is listed and has **Pending Install** displayed for the workspace status. The status is **Pending Install** because the workspace has not yet been provisioned to the user's device.

Configure Workspace and Horizon Mobile Manager Branding Elements

In this test, you configure the branding elements that display on the mobile device and in the administration interface.

Prerequisites

Verify you have the image files described in Chapter 8, "Manual Verification Tests," on page 33.

Complete the steps in "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34.

Procedure

1 Log in to the administrative interface as an administrator (such as **`user20`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 Click **Branding** in the left navigation, and click **Edit**.

3 In the **Site Branding** section, update the following items:

   a Change the site title to **`Our Site`** and the login screen title to **`Our Horizon Mobile Manager`**.

   b Change the site logo by clicking the corresponding **Browse** button and selecting your 600 pixels by 400 pixels image file.

   c Change the login screen image by clicking the corresponding **Browse** button and selecting your 80 pixels by 50 pixels image file.

4 In the **Workspace Branding** section, update the following items:

   a Change the company name (for example **`Our Company`**). This name is displayed on the device when the user first provisions the workspace.

   b Change the text for the usage terms for using the corporate workspace. This text is displayed on the device when the user first provisions the workspace. For example, you might type:
   `Your use of Our Company's corporate workspace is governed by the terms of this agreement.`

   c Change the company logo image by clicking the corresponding **Browse** button and selecting your 200 pixels by 200 pixels image file. This image is displayed on the device when the user touches the Switch icon to enter the workspace.

5 Click **Save**.

What to do next

Verify the site branding elements:

1 Verify that the title displayed in the top banner is the title you specified in the **Site Title** field.

2 Log out and refresh your browser. Verify that the login screen displays your site logo and login screen images.

The workspace branding elements are verified in "Install the Workspace on a Mobile Device," on page 38.

Install the Workspace on a Mobile Device

In this test, you provision a device with a workspace.

Prerequisites

Verify you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Complete the steps in "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34, "Create a Template," on page 35, "Create a Policy Set," on page 36, "Create a Group and Add a User to the Group," on page 37, and "Configure Workspace and Horizon Mobile Manager Branding Elements," on page 37.

Procedure

1 On the mobile device, touch the **Switch** icon.

   The Set Up VMware Switch form displays.

2 Type the user name and password for the user account that corresponds to the user you added to the group in "Create a Group and Add a User to the Group," on page 37.

If the specified user does not belong to any group defined in Horizon Mobile Manager, the user cannot log in and the workspace cannot be provisioned to the device.

3 Type the fully qualified domain address used for the login server for your Horizon Mobile Manager instance.

This address is specified in the **Login Server URL** field when the virtual appliance is configured. You do not have to type the **`https://`** portion of the address.

4 Touch **Go**. When the connection is made, verify that the company branding elements that you specified in "Configure Workspace and Horizon Mobile Manager Branding Elements," on page 37 are displayed on the device.

5 Touch **Next**.

The process of downloading and installing the workspace begins. You can see the progress by viewing the notifications on the device. When the installation is complete, a notification that says `VMware Switch is ready. Touch for your workspace` is sent to the device.

6 Open the workspace by touching the notification, and follow the on-screen instructions, including creating a password.

The password requirements are specified in "Create a Policy Set," on page 36.

7 (Optional) Enter email credentials to set up access for testing the email application. Use the email account you identified to use in these tests.

You can defer the email setup process by touching **Manual setup** and then **Discard**.

The device displays the workspace home.

What to do next

Verify that the wallpaper and shortcut specified in "Configure Workspace and Horizon Mobile Manager Branding Elements," on page 37 are displayed. Touch the application display icon, and verify the presence of the application you added to the template in "Create a Template," on page 35.

Switch to the personal phone by touching the **Switch** icon in the workspace.

View Details About Interactions with a Managed Device

In this test, as a fleet manager, you view details about Horizon Mobile Manager interactions with a managed device.

Prerequisites

Verify that you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Verify that the workspace is successfully provisioned on the smartphone.

Procedure

1 Log in to the administrative interface as a fleet manager (such as **`user21`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 In the left navigation, click **Users**.

3 Click the user that corresponds to the provisioned mobile device.

For example, if you used **`user23`** in "Install the Workspace on a Mobile Device," on page 38, select that user.

The system displays detailed information about the interactions between the mobile device and Horizon Mobile Manager, such as the history of updates made to the device, the provisioning status, and the associated group, policy set, and template.

NOTE The graphic image of the device displays information from when the workspace was initially provisioned. That information is not updated with data from subsequent changes to the device.

What to do next

Verify that the history of interactions displays the provisioning interaction performed in "Install the Workspace on a Mobile Device," on page 38.

Disable and Re-Enable a User's Workspace

In this test, as a fleet manager, you disable the user's workspace, and then re-enable it. When the workspace is disabled, the device user cannot access the workspace. When it is re-enabled, the user can access the workspace.

Prerequisites

Verify that you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Verify that the workspace is successfully provisioned on the smartphone.

Procedure

1 Log in to the administrative interface as a fleet manager (such as **`user21`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 In the left navigation, click **Users** and select the user that corresponds to the provisioned device.

The system displays the details page for that user.

3 On the details page, click **Disable** to disable the user, and click **OK** in the confirmation message.

4 In the personal phone, touch **Settings** > **Account & sync**, and touch the user associated with the Switch application (the user account with the **`Switch`** icon).

5 Touch **Settings** > **Sync now** to initiate a sync with Horizon Mobile Manager.

The device communicates with the Horizon Mobile Manager server and receives the command to disable the workspace.

6 Open the notifications on the mobile device to view the notification that Switch has been disabled.

7 In the applications list on the personal phone, touch the **Switch** icon. A message is displayed that states Switch was disabled.

8 In the Horizon Mobile Manager administration interface, use the refresh icon in the top banner to refresh the user details page. The page displays a disabled status for that user.

9 Click **Enable** to re-enable the user's workspace access.

10 In the personal phone, repeat Step 4 and Step 5 to sync the mobile device with the server. When you see the notification that access is restored, touch the **Switch** icon to confirm that you can open the workspace on the device.

What to do next

Switch to the personal phone by touching the **Switch** icon in the workspace.

Update Applications in the Provisioned Workspace

In this test, you add and remove applications in the provisioned workspace and update the managed device.

Prerequisites

Verify that you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Verify that the workspace is successfully provisioned on the smartphone.

Procedure

1 Log in to the administrative interface as a fleet manager (such as **user21** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 In the left navigation, click the template that defines the provisioned workspace, and click **Edit.**

3 In the **Deployed applications** section, remove the application that you added in "Create a Template," on page 35 (the VMware View application) by clicking the red **X** on the application's icon.

4 Add another application to the **Deployed applications** section by dragging the application's icon from the **All applications** section into the **Deployed applications** section. Add a different application than the one you removed in Step 3.

5 Click **Deploy**. A message displays to alert you that the changes will affect the users associated with the template. Click **OK**.

6 In the personal phone, sync the phone with Horizon Mobile Manager:

   a Touch **Settings** > **Account & sync**.

   b Touch the user associated with the Switch application.

   c Touch **Settings** > **Sync now**.

   The device communicates with the Horizon Mobile Manager server and updates the workspace according to the updated template.

7 Switch to the workspace and verify that the set of applications reflects the choices you made in Step 3 and Step 4.

What to do next

Switch to the personal phone by touching the **Switch** icon in the workspace.

Update the Wallpaper and Shortcuts for the Provisioned Workspace

In this test, you update the wallpaper and shortcuts used in the workspace home screen and update the managed device.

Prerequisites

Verify that you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Verify that the workspace is successfully provisioned on the smartphone.

Procedure

1 Log in to the administrative interface as a fleet manager (such as **user21** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 In the left navigation, click the template that defines the provisioned workspace, and click **Edit**.

3 In the **Customization** section, click **Upload New** to upload the other 960 pixels by 640 pixels wallpaper image (as described in Chapter 8, "Manual Verification Tests," on page 33), and use the drop-down control to select it as the current wallpaper.

4 Click **Add Shortcut**, and add another shortcut to the list (for example, **`communities.vmware.com`**).

5 Click **Deploy.**

6 In the personal phone, sync the device with the server as described in "Update Applications in the Provisioned Workspace," on page 41.

7 Switch to the workspace and verify that the wallpaper and shortcuts on the home display reflect your choices.

What to do next

Switch to the personal phone by touching the **Switch** icon in the workspace.

Update the Workspace Password Policy

In this test, you update the password policy for the provisioned workspace and deploy the new policies to the managed device.

Prerequisites

Verify that you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Verify that the workspace is successfully provisioned on the smartphone.

Procedure

1 Log in to the administrative interface as a fleet manager (such as **`user21`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 In the left navigation, click the policy set that is used for the provisioned workspace (the policy set created in "Create a Policy Set," on page 36), and click **Edit**.

3 Click **Password Strength** to expand the section, and select **Manual** for the password strength. Set the password length to **6**, minimum digits to **1**, and minimum special characters to **1**.

4 Click **Deploy**, and in the message alert, click **OK**.

5 In the personal phone, sync the device with the server as described in "Update Applications in the Provisioned Workspace," on page 41.

6 Touch the **Switch** icon to switch to the workspace. In the validate password form, type the password you set when the workspace was initially provisioned (in "Install the Workspace on a Mobile Device," on page 38).

7 In the create password form, create a new password. As a test, type **`1234`**. A message displays that describes the new policy.

8 Type a password that matches the policy set in Step 3, and confirm the new password.

What to do next

Verify that the workspace is displayed.

Switch to the personal phone by touching the **Switch** icon in the workspace.

Update the Location Services Policy

In this test, you change the workspace's policy settings for location services and deploy the new settings to the managed device.

Prerequisites

Verify that you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Verify that the workspace is successfully provisioned on the smartphone.

Procedure

1 In the personal phone, disable the location services.

Touch **Settings** > **Location services**, and clear the appropriate check boxes.

2 Log in to the administrative interface as a fleet manager (such as **`user21`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

3 Click the policy set that is used by the provisioned workspace, and click **Edit**.

4 In the **Features** section, select the **Location Services Required** select box if it is not already selected. Verify that the location accuracy is set to **High Accuracy**.

5 Click **Deploy**, and in the alert message, click **OK**.

6 In the personal phone, sync the device with the server as described in "Update Applications in the Provisioned Workspace," on page 41. Verify that when you touch the **Switch** icon to enter the workspace, an alert is displayed that states there is a policy violation.

If the fleet manager specifies that location services are required, and the device user disables location services in the device, it is a policy violation and Horizon Mobile Manager disables the workspace.

7 Re-enable location services on the device, and switch to the workspace. Verify that you can enter the workspace.

8 Switch to the personal phone, and modify the Switch application settings to turn off its access to the location services:

a Touch **Settings** > **Accounts & sync**, and touch the Switch user account.

b Touch **Manage Switch Settings**. In the Manage VMware Switch Settings display, touch **Location**.

c Select **Hidden**, to hide location services from the Switch application.

9 Sync the device with the server. Verify that when you touch the **Switch** icon to enter the workspace, an alert is displayed that states there is a policy violation.

If the fleet manager specifies that location services are required, and the device user disables location services in the Switch settings, it is a policy violation and Horizon Mobile Manager disables the workspace.

10 Repeat Step 8a and Step 8b to open the location setting for the Switch application. Touch the **Fine** setting to match the **High Accuracy** setting in Horizon Mobile Manager (described in Step 4).

11 Touch the **Switch** icon to switch to the workspace, and verify that you can switch to the workspace.

What to do next

Switch to the personal phone by touching the **Switch** icon in the workspace.

Update Policy Settings for the Cut/Copy/Paste and Camera Features

In this test, you change the policy settings for use of the cut/copy/paste features and the camera in the workspace, and deploy the new policies to the managed device.

When the cut/copy/paste feature is not enabled in the policy set, the user is unable to copy text from the workspace to the personal side of the device. When the camera feature is not enabled in the policy set, the user is prevented from using the camera in the workspace.

Prerequisites

Verify that you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Verify that the workspace is successfully provisioned on the smartphone.

Procedure

1 In the personal phone, switch to the workspace and verify that you can use the camera: display the applications, touch the **Camera** icon, and take a picture.

2 Copy some text in an application in the workspace, switch to the personal phone, and verify that you can paste the text into an application.

3 Log in to the administrative interface as a fleet manager (such as **`user21`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

4 Click the policy set that is used by the provisioned workspace, and click **Edit**.

5 In the **Features** section, disable the cut/paste/copy and camera features by clearing the appropriate check boxes. Click **Deploy**, and then click **OK** in the message alert.

6 In the personal phone, sync the device with the server (as described in "Update Applications in the Provisioned Workspace," on page 41). Repeat Step 1 and Step 2 to verify that you are prevented from using the camera in the workspace, and from copying and pasting text from the workspace to the personal phone.

What to do next

Switch to the personal phone by touching the **Switch** icon in the workspace.

Initiate a Password Reset to the Provisioned Workspace

In this test, you force a password reset to the provisioned workspace. This action is typically used when the device user has forgotten his or her workspace password. After a password reset, the user is prompted to configure a new password without having to validate the previous one.

Prerequisites

Verify that you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Verify that the workspace is successfully provisioned on the smartphone.

Procedure

1 Log in to the administrative interface as a fleet manager (such as **`user21`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 Open the user details page for the user that corresponds to the provisioned workspace (as described in "Disable and Re-Enable a User's Workspace," on page 40).

3 Click **Reset Password**. In the confirmation message, click **OK**.

4 In the personal phone, sync the device with the server as described in "Update Applications in the Provisioned Workspace," on page 41.

5 Switch to the workspace. Verify that you are prompted to configure a new password without having to validate the previous one.

6 Create a new password.

What to do next

Verify that the device displays the workspace after you create the new password.

Switch to the personal phone by touching the **Switch** icon in the workspace.

Wipe the Provisioned Workspace from the Device

In this test, you wipe the provisioned workspace from the device. This action is typically done when the user reports the device is lost or stolen. When the provisioned workspace is wiped, all of the workspace data on the device is removed and cannot be recovered from the device.

Prerequisites

Verify that you have the items described in Chapter 8, "Manual Verification Tests," on page 33.

Verify that the workspace is successfully provisioned on the smartphone.

Procedure

1 Log in to the administrative interface as a fleet manager (such as **`user21`** from "Create Administrators and Fleet Managers by Assigning Roles to Users," on page 34).

2 Open the user details page for the user that corresponds to the provisioned workspace (as described in "Disable and Re-Enable a User's Workspace," on page 40).

3 Click **Wipe**. In the confirmation message, click **OK**.

4 In the personal phone, sync the device with the server (as described in "Update Applications in the Provisioned Workspace," on page 41). A notification is sent to the device that states the workspace is wiped by your administrator.

5 Touch the **Switch** icon to switch to the workspace.

6 Verify that the Set Up VMware Switch form is displayed.

Because the workspace has been removed, the Set Up VMware Switch form is displayed to begin the provisioning process.

What to do next

At this point, you can re-provision the workspace by repeating the steps "Install the Workspace on a Mobile Device," on page 38, or you can cancel the provisioning process.

Using the Embedded OpenLDAP Service

9

The embedded OpenLDAP service is typically used for demonstration or test configurations. When using the embedded OpenLDAP service, you might want to perform common LDAP operations such as adding new users, deleting existing users, and changing user passwords.

This information is intended for experienced system administrators who are familiar with standard LDAP operations and commands.

The embedded OpenLDAP server runs on TCP port 389. The OpenLDAP server is only accessible locally from the Linux console for the Horizon Mobile Manager virtual appliance. You can use standard LDAP commands to perform operations in the embedded OpenLDAP server. The required binaries (`ldapadd`, `ldapsearch`, `ldapdelete`, and `ldapmodify`) are installed in the virtual appliance.

By default, when the virtual appliance is installed and configured, the embedded OpenLDAP service is preconfigured with entries that have common names (`cn`) that follow the pattern **`Enterprise User 1`**, **`Enterprise User 2`**, and so on. The users are preconfigured with the following attributes:

- `userPassword:` **`vmware`**
- `sn:` **`User`**
- `uid`: Follows the pattern of **`user1`**, **`user2`**, and so on.
- `ou:` **`people`**

For example, the preconfigured entry for **`Enterprise User 1`** has the following attribute values.

```
cn: Enterprise User 1
sn: User
mail: user1@mvp.org
uid: user1
```

During configuration of the virtual appliance, you specify the user account to use as the default system administrator. This account can log into the Horizon Mobile Manager administration interface and perform all operations. If you used the default value during configuration of the virtual appliance, this user account is the preconfigured entry in the embedded LDAP service that has its `cn` attribute set to **`Admin User`**, its `uid` attribute set to **`admin`**, and its `userPassword` attribute set to **`vmware`**.

Base Distinguished Name (DN), Bind DN, and Bind PW

The base Distinguished Name (`DN`) for the embedded OpenLDAP server is **`dc=mvp, dc=org`**.

The `bind DN` is **`admin`**, and the `bind PW` is **`vmware.`**

Changing the Password for the Default System Administrator Entry

To change the password for the preconfigured administrator entry (`uid: admin`), create an LDAP Data Interchange Format (LDIF) file with the appropriate attribute settings and run the `ldapmodify` command to change the existing values to those in the LDIF file.

1 Log into the virtual appliance from its console.

2 Use a text editor to create a new LDIF file within the file system. For example,
`vi /home/tcserver/changepass.ldif`

3 Type the appropriate lines in the LDIF file and save the file. In this example, the password for the **`admin`** `uid` is changed to **`classic*CD`**.

```
dn: uid=admin,ou=people,dc=mvp,dc=org
changetype: modify
replace: userPassword
userPassword: classic*CD
```

4 Run the `ldapmodify` command.

```
/usr/bin/ldapmodify –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware –
f /home/tcserver/changepass.ldif
```

If your Horizon Mobile Manager instance uses the preconfigured user account as the default system administrator, the next time you log into the Horizon Mobile Manager administration interface, log in with username **`admin`** and the new password.

Adding a User to the Embedded OpenLDAP

In demonstration environments, you might want to have user accounts that correspond to people in your organization or team, or use names other than the preconfigured ones. You can use an LDIF file and the standard `ldapadd` operation to add new entries to the OpenLDAP service. In this example, an LDIF file named addentry.ldif defines an entry for individual Stacy Barr, with `uid:`**`sbarr`** and `userPassword:`**`stacy*b`**.

```
dn: uid=sbarr,ou=people,dc=mvp,dc=org
objectclass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Stacy Barr
sn: Barr
uid:sbarr
mail: s.barr@mvp.org
userPassword: stacy*b
```

To add the entry to the embedded OpenLDAP, run the `ldapadd` command in the virtual appliance console.

```
/usr/bin/ldapadd –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware –
f /home/tcserver/addentry.ldif
```

Removing a User from the Embedded OpenLDAP

Use the `ldapdelete` command in the virtual appliance console to remove an entry from the embedded OpenLDAP service.

For example, to remove the preconfigured **`user50`** entry, run:

```
/usr/bin/ldapdelete –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware
"uid=user50,ou=people,dc=mvp,dc=org"
```

Changing User Passwords

Like the steps for changing the password of the default admin account, to change passwords for users, you can use an LDIF file and the standard `ldapmodify` operation. To change more than one user's password using a single LDIF file in one `ldapmodify` operation, create a four-line block in the file for each user, with each block separated by a blank line.

For example, to change the passwords for preconfigured **`user21`**, **`user22`**, **`user23`**, and **`user24`**, create an LDIF file named **`changeuserpwd.ldif`** with the following lines.

```
dn: uid=user21,ou=people,dc=mvp,dc=org
changetype: modify
replace: userPassword
userPassword: user*21

dn: uid=user22,ou=people,dc=mvp,dc=org
changetype: modify
replace: userPassword
userPassword: user*22

dn: uid=user23,ou=people,dc=mvp,dc=org
changetype: modify
replace: userPassword
userPassword: user*23

dn: uid=user24,ou=people,dc=mvp,dc=org
changetype: modify
replace: userPassword
userPassword: user*24
```

Running the `ldapmodify` command with the LDIF file changes the passwords in one operation.

```
/usr/bin/ldapmodify –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware –
f /home/tcserver/changeuserpwds.ldif
```

Using Other OpenLDAP Commands

You can use standard OpenLDAP commands with the embedded OpenLDAP service.

Determining Your Versions of the Horizon Mobile Components 10

When opening a support request, the version, build, or model numbers of the key components in your Horizon Mobile environment are useful aids to help diagnose the source of an issue.

The key components in a Horizon Mobile environment are:

- VMware Ready mobile device
- VMware Ready component
- VMware Switch application
- Base workspace image
- VMware Horizon Mobile Manager virtual appliance

Each component has a relevant identifier.

Table 10-1. Identifiers for the Horizon Mobile Components

Component	Identifier
Mobile device	Model number (on the mobile device)
VMware Ready component	Software version number (on the mobile device)
Vmware Switch component	Software version number (on the mobile device)
Base workspace image	■ Software version number (on the mobile device) ■ Build ID and image name (in the administration interface)
Horizon Mobile Manager	Software version and build number (in the virtual appliance's console and in the configuration interface)

Version Information on the Mobile Device

NOTE The steps to obtain version information might be different depending on your specific mobile device.

On the mobile device, you can obtain the device's model number, and the software version information for the VMware Ready, VMware Switch, and base workspace image components.

Device model number

Obtain the model number on the device. The model number is usually found in the device's **About phone** information.

VMware Ready, VMware Switch, and base workspace image software versions

Obtain the version numbers for these components by viewing the list of all applications, finding VMware Switch in that list, and opening its settings. For example:

1 Open **Settings** > **Apps** > **All**.

2 In the list of all applications, touch **VMware Switch**.

3 Touch **Manage space**. The Manage VMware Switch Settings is displayed.

4 Touch **Diagnostics**. The software version numbers for the VMware Ready, VMware Switch, and the provisioned workspace are displayed. If a workspace is not provisioned on the device, no workspace information is displayed.

Information You Can Obtain in the Horizon Mobile Manager Virtual Appliance

In addition to the information available on the mobile device itself, you can obtain additional information about the workspace that is provisioned on a user's mobile device by using Horizon Mobile Manager's administration interface.

1 Log in to the administrative interface as a fleet manager.

2 Open the user details page for the user by clicking **Users** and then clicking the user's name in the displayed list of users.

3 Expand the **Workspace Container** section if it is not already expanded. The Name row displays the name of the base workspace image. Make a note of the name.

4 To associate the name with a build ID, view the list of workspace images available to this instance of Horizon Mobile Manager by clicking **Workspace Images**.

5 Click the list entry that displays the name of the base workspace image. In the Workspace Image Details window, the Build ID row displays the build number for that workspace image.

Information About the Horizon Mobile Manager Virtual Appliance

You can view the identification information for your Horizon Mobile Manager installation in the following locations:

Using the vSphere Client Select the Horizon Mobile Manager virtual appliance and view its console by clicking **Console**. The version and build number for the Horizon Mobile Manager virtual appliance are displayed.

Using the configuration interface Log in to the configuration interface as described in Chapter 4, "Add License Keys," on page 15. The version and build information is displayed on the **System** tab.

Using the administration interface Log in to the administration interface as fleet manager or administrator. Click **About** to view the identifying hash and branch information.

11 Collect Diagnostic Logs

When you open a support request, VMware Technical Support might request the logs from the virtual appliance's embedded components. You can collect these logs and provide them in a zip file along with your support request.

You can collect logs for these embedded components:

- Apache server
- vFabric Postgres database
- Linux operating system

Prerequisites

In the vSphere Client, power on the virtual appliance, click the **Console** tab, and log in to the virtual appliance's Linux operating system as the **root** user. Use the password that you set when you configured the virtual appliance. If you did not change the default password, enter **vmware** as the password.

Procedure

1. Zip up the Apache server log files:
   a. Run the command: `tar czf apachelog1.tgz /home/tcserver/tcserver-current/mmp/logs/`
   b. Run the command: `tar czf apachelog2.tgz /home/tcserver/tcserver-current/mmp-config/logs/`
2. Zip up the vFabric Postgres database log files by running the command: `tar czf postgreslog.tgz /opt/vmware/vpostgres/1.0/data/pg_log/`
3. Zip up the Linux operating system log files by running the command: `tar czf suselog.tgz /var/log/`

What to do next

Copy the resulting zip (.tgz) files to a location from which you can provide them to VMware Technical Support.

Index