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
The VMware Horizon FLEX Administration Guide describes how to install and administer VMware Horizon FLEX™.

Intended Audience

This information is intended for anyone who wants to install Horizon FLEX. The information is written for experienced Windows system administrators who are familiar with virtual machine technology.
Introducing Horizon FLEX

Horizon FLEX is a policy-based, containerized desktop solution that enables IT administrators to create, secure, and manage local desktops for end users. End users work within a restricted virtual machine, called a Horizon FLEX virtual machine, on their own computers. Because Horizon FLEX virtual machines are stored locally, on end-user computers, corporate applications are accessible to offline users.

This chapter includes the following topics:
- “Horizon FLEX Components,” on page 7
- “Horizon FLEX Architecture,” on page 8
- “Horizon FLEX System Requirements,” on page 9
- “Horizon FLEX Network Requirements,” on page 10
- “Supported Host and Guest Operating Systems,” on page 10

Horizon FLEX Components

Horizon FLEX is a combination of existing VMware products, including additional Horizon FLEX-specific functionality.

**VMware Mirage® for Horizon FLEX**

The standard Mirage server that provides optional Horizon FLEX virtual machine management. You can manage, back up, and patch virtual machines by using the Mirage for Horizon FLEX layering technology.

**Horizon FLEX Policy Server**

An extension of the Mirage server that includes Horizon FLEX-specific functionality. The Horizon FLEX Policy Server is activated after you apply the Horizon FLEX license to Mirage for Horizon FLEX.

**Horizon FLEX Admin Console**

The Web management user interface for the Horizon FLEX Policy Server. The Horizon FLEX Admin Console is located in the Mirage Web Management component. You can use the Horizon FLEX Admin Console to perform virtual machine management tasks, including the following:
- Manage an inventory of virtual machines
- Browse a list of users and groups in the Active Directory service
- Entitle users and groups to one or more virtual machines
- Specify virtual machine policies for a given entitlement
- Prevent users from accessing virtual machines by using remote lock
- Examine virtual machine details and status at an given point in time
Horizon FLEX Client

The client software that end users use to download the Horizon FLEX virtual machines to their local computers. The clients include VMware Fusion Pro® for Mac computers and VMware Player Pro™ for Windows computers. Fusion Pro and Player Pro are included in the Horizon FLEX package. One license key is provided for both Fusion Pro and Player Pro.

Horizon FLEX Virtual Machine

The virtual machine that end users run on their own computers. You use Fusion Pro to create source virtual machines for Horizon FLEX virtual machines. Fusion Pro is included in the Horizon FLEX package. A Horizon FLEX server can support up to 1000 users.

**Note:** You can also use VMware Workstation™ to create source virtual machines. Workstation is not included in the Horizon FLEX package.

About Mirage

Mirage is integral to the operation and use of Horizon FLEX virtual machines. Horizon FLEX uses only a subset of the features available in Mirage.

This document does not describe all of the information pertaining to Mirage. For complete information about Mirage, see the Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html.

Horizon FLEX Architecture

A typical Horizon FLEX deployment includes the Horizon FLEX server, a file server, an HTTPS proxy, a read-only domain controller (RODC), and offsite and onsite end user systems.

**Figure 1-1** shows the relationships between the major components of a Horizon FLEX deployment.

**Figure 1-1. Sample Horizon FLEX Deployment**
Horizon FLEX Server

The Horizon FLEX server is composed of the Mirage Management Console and Mirage Management Server components of the Mirage system. The Horizon FLEX server provides the following functionality.

- Assigns Horizon FLEX virtual machines to users and groups from a directory service
- Maintains a record of Horizon FLEX virtual machines in use by individual users
- Enforces policy settings to the client
- Enables modification of policy settings for a given user and Horizon FLEX virtual machine combination
- Monitors Horizon FLEX virtual machine status

The Mirage Management Console is the graphical user interface used for scalable maintenance, management, and monitoring of deployed endpoints. The Mirage Web Manager mirrors Mirage Management Console functionality.

The Mirage Web Manager and Mirage Web Management Console communicate by using TCP/IP ports 7080 and 7443. The Mirage Management Console and Mirage Management Service communicate by using TCP/IP port 8443.

File Server

A file server stores the TAR files that contain the source virtual machine files for Horizon FLEX virtual machines. The file server is located inside the DMZ.

HTTPS Proxy

An HTTPS proxy enables offsite end-user systems to reach the Mirage Management Console. The HTTPS proxy is inside the DMZ.

RODC

A RODC enables offsite end-user systems to log in to their Horizon FLEX virtual machines after their virtual machines are joined to an Active Directory domain. A RODC is required only if you want to allow outside users to log in without using a VPN. The RODC is inside the DMZ.

Horizon FLEX System Requirements

Each product in the Horizon FLEX package has certain system requirements.

<table>
<thead>
<tr>
<th>Product</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage for Horizon FLEX</td>
<td>The system requirements are the same as for Mirage 5.3. See the Mirage documentation at <a href="https://www.vmware.com/support/pubs/mirage_pubs.html">https://www.vmware.com/support/pubs/mirage_pubs.html</a>.</td>
</tr>
<tr>
<td>Player Pro</td>
<td>Horizon FLEX 1.1 is compatible with Player Pro 7.1. Player Pro 7.1 is included in the Horizon FLEX 1.1 installation package. For Player Pro hardware and software requirements, see the VMware Horizon FLEX User Guide.</td>
</tr>
<tr>
<td>Fusion Pro</td>
<td>Horizon FLEX 1.1 is compatible with Fusion Pro 7.1.1. Fusion Pro 7.1.1 is included in the Horizon FLEX 1.1 installation package.</td>
</tr>
</tbody>
</table>
For Fusion Pro hardware and software requirements, see “Host System Requirements for Fusion Pro,” on page 17.

Workstation

Horizon FLEX 1.1 is compatible with Workstation 11.1.0. You can use Workstation to create and open a source virtual machine, but Workstation cannot download a Horizon FLEX virtual machine. Workstation 11.1.0 is not included in the Horizon FLEX 1.1 installation package.

For Workstation hardware and software requirements, see the Workstation documentation at https://www.vmware.com/support/pubs/ws_pubs.html.

Horizon FLEX Network Requirements

Horizon FLEX enables end users to run corporate applications even when they are disconnected from the network. Horizon FLEX virtual machines are stored locally for a complete desktop experience that does not require a network connection.

A network connection is required between the Horizon FLEX Policy Server and the Horizon FLEX Client in the following circumstances:

- For the initial download of the Horizon FLEX virtual machine to the user’s local computer.
- To register a Horizon FLEX virtual machine that was provided on a USB device or deployed on the user’s local computer.
- To receive Horizon FLEX virtual machine restriction and policy updates.

When you register a source virtual machine for a Horizon FLEX virtual machine, you specify a download location URL for virtual machine package. The download folder must be accessible to end user computers for end users to download virtual machines.

Supported Host and Guest Operating Systems

The local computer on which end users use the Horizon FLEX Client must have a supported host operating system. A Horizon FLEX virtual machine must use a supported guest operating system.

Supported Host Operating Systems

Your end users can run the Horizon FLEX Client and access their Horizon FLEX virtual machine by using a physical computer that has one of the following operating systems.

**Table 1-1. Supported Host Operating Systems**

<table>
<thead>
<tr>
<th>Horizon FLEX Client</th>
<th>Supported Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Player Pro</td>
<td>Windows 7</td>
</tr>
<tr>
<td></td>
<td>Windows 8.1 Enterprise</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows 8</td>
</tr>
<tr>
<td></td>
<td>Windows 8.1 Pro</td>
</tr>
<tr>
<td><strong>Note</strong> Player Pro supports only 64-bit operating systems.</td>
<td></td>
</tr>
<tr>
<td>Fusion Pro</td>
<td>Mac OS X 10.10</td>
</tr>
<tr>
<td></td>
<td>Mac OS X 10.9</td>
</tr>
</tbody>
</table>

Supported Guest Operating Systems

A Horizon FLEX virtual machine can contain one of the following guest operating systems.

- Windows 7
- Windows 8.1
- Windows XP
- Windows Server 2012 R2
- Windows 2012
- Ubuntu 14.04
Installing Horizon FLEX

Installing Horizon FLEX involves installing the Horizon FLEX server and client components, creating folders to store Horizon FLEX virtual machines, preparing Active Directory, setting up certificates, and creating and deploying Horizon FLEX virtual machines.

This chapter includes the following topics:

- “Horizon FLEX Installation Overview,” on page 13
- “Installing and Configuring Mirage for Horizon FLEX,” on page 14
- “Create a Download Folder for Horizon FLEX Virtual Machine Packages,” on page 15
- “Create a Virtual Directory and Edit Site Bindings in IIS,” on page 15
- “Configure Active Directory Settings,” on page 16
- “Test the Horizon FLEX Admin Console Connection,” on page 16
- “Host System Requirements for Fusion Pro,” on page 17
- “Install Fusion Pro on a Mac,” on page 17
- “Running an Unattended Player Pro Installation,” on page 18
- “Creating a Mass Deployment Package to Deploy Fusion Pro,” on page 18

Horizon FLEX Installation Overview

Horizon FLEX is a combination of existing VMware products, including Mirage, Fusion Pro, and Player Pro. Installing Horizon FLEX involves installing each of these products and performing additional Horizon FLEX-specific steps. To ensure a successful Horizon FLEX deployment, you must understand the sequence of tasks required.

Before you install Horizon FLEX, ensure that all of the hardware and software requirements are met, that you have valid licenses, and that you have downloaded the Horizon FLEX component installers from the VMware Horizon FLEX product download page.

You install Horizon FLEX in this order:

1. Install the Mirage system.

2. Set up certificates for Horizon FLEX virtual machines.

3. Create a download folder to store your Horizon FLEX virtual machine packages.
   See “Create a Download Folder for Horizon FLEX Virtual Machine Packages,” on page 15.
4 Add a virtual directory in IIS for your Horizon FLEX virtual machine download folder and edit site bindings.

See “Create a Virtual Directory and Edit Site Bindings in IIS,” on page 15.

5 (Optional) Configure Horizon FLEX to synchronize entities in only a selected Active Directory organizational unit (OU).

See “Configure Active Directory Settings,” on page 16.

6 Test the connection to the Horizon FLEX Admin Console.

See “Test the Horizon FLEX Admin Console Connection,” on page 16.

7 Install Fusion Pro on a Mac in your network.

You use Fusion Pro to create source virtual machines for Horizon FLEX virtual machines. See “Install Fusion Pro on a Mac,” on page 17.

8 Create and deploy Horizon FLEX virtual machines.

See Chapter 4, “Creating and Deploying Horizon FLEX Virtual Machines,” on page 27.

9 Install a Horizon FLEX Client on each end-user host, or instruct end users to install a Horizon FLEX Client on their own computers.

Horizon FLEX includes Player Pro for Windows hosts and Fusion Pro for Mac hosts. For single-host installation instructions, see the VMware Horizon FLEX User Guide.

For Windows hosts, you can run an unattended installation to install Player Pro on several Windows hosts without having to respond to wizard prompts. See “Running an Unattended Player Pro Installation,” on page 18.

For Mac hosts, you can create a mass deployment package to deploy Fusion Pro to any number of end-user Macs. See “Creating a Mass Deployment Package to Deploy Fusion Pro,” on page 18.

Installing and Configuring Mirage for Horizon FLEX

The first Horizon FLEX installation step is to install and configure the Mirage system. The Horizon FLEX package includes the Mirage Core Software, Mirage Gateway Appliance Software, and Mirage PowerCLI for Windows.

The Mirage deployment involves a number of components, including the Mirage Management Server, Mirage Management Console, Windows Internet Information Services (IIS), and other components, which you must install in a specific order.

To install and configure the Mirage system, follow the installation instructions in the Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html.

When you install the Mirage system, you must select certain options to ensure that the Horizon FLEX server operates correctly.

- During Mirage server installation, choose SSL for the Mirage server transport. SSL is required to use the Mirage Gateway feature for external access and management of Horizon FLEX systems.
- Before you install the Mirage Web Manager, make sure that .NET Framework 4.0 is installed on the server.
- The Mirage Management Server must run as a user that has Active Directory read permissions. If you plan to join Horizon FLEX virtual machines to an Active Directory domain, the Mirage Management Server must run as a user that has domain join permissions.
Create a Download Folder for Horizon FLEX Virtual Machine Packages

During the Horizon FLEX virtual machine deployment process, you compress your source virtual machine packages into TAR (.tar) format so that end users can easily download their Horizon FLEX virtual machines. You must create a download folder to store these TAR files.

Procedure

1. Create the download folder on the Horizon FLEX server or on another server.
   The download folder does not need to reside on the Horizon FLEX server, but the files it contains must be downloadable without any authentication challenge.

2. Assign permissions to the download folder so that users can download the files that it contains.

3. (Optional) Share the download folder to an administrative group, such as Domain Admins.
   This step can make it easier to register your source virtual machines with the Horizon FLEX Policy Server.

What to do next

Create a virtual directory in IIS to allow the Horizon FLEX virtual machines to be downloaded to end-user systems. See “Create a Virtual Directory and Edit Site Bindings in IIS,” on page 15.

Create a Virtual Directory and Edit Site Bindings in IIS

You must create a virtual directory in IIS to allow Horizon FLEX virtual machine packages to be downloaded to end-user computers.

This document does not describe how to set up IIS for the Mirage system. For information about setting up IIS for the Mirage system, see the Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html.

Prerequisites

- Create a download folder for your Horizon FLEX virtual machine packages. See “Create a Download Folder for Horizon FLEX Virtual Machine Packages,” on page 15.

Procedure

1. Open IIS Manager.
2. Navigate to VMware Mirage Management Web Site and select rvm.
3. Right-click rvm and select Add Virtual Directory.
4. Type a name in the Alias text box, browse to the folder that you created to contain the Horizon FLEX virtual machine packages, and click OK.
5. Select VMware Mirage Management Web Site and click Edit Bindings in the right column.
6. Set the HTTPS port to use your Horizon FLEX server certificate and click OK.
Configure Active Directory Settings

When you entitle a Horizon FLEX virtual machine, you add users and groups from your existing Active Directory infrastructure to the entitlement. By default, Horizon FLEX synchronizes your entire Active Directory infrastructure into the Horizon FLEX database. You can optionally configure Horizon FLEX to synchronize only a specific OU.

Prerequisites

Install Mirage for Horizon FLEX. See “Installing and Configuring Mirage for Horizon FLEX,” on page 14.

Procedure

1. Launch the Horizon FLEX Admin Console.
   a. In a Web browser, type https://WebManagerServer:7443/rvm, where WebManagerServer is the DNS name or IP address of the host where the Mirage Web Manager is installed.
   b. Type the user name and password of a domain account that has access to Mirage.
   c. Click Login.

2. In the Horizon FLEX Admin Console, click the General System Settings icon and click Active Directory Settings.

3. Type the OU to synchronize in the Organizational Unit text box.
   As you begin to type in the text box, the available OUs in your Active Directory infrastructure appear in a drop-down menu and you can select the appropriate OU.

4. Click OK to save the OU setting.
   The Horizon FLEX server validates the OU to make sure it exists and is accessible.
   The Horizon FLEX server synchronizes the Active Directory entities that belong only to the OU that you selected, including entities that belong to any child OUs of the selected OU.
   Any time you configure a new OU, the Horizon FLEX server deletes the previously synchronized entities from the database and starts a new full synchronization process.

Test the Horizon FLEX Admin Console Connection

You can verify your Horizon FLEX deployment by testing the Horizon FLEX Admin Console connection.

Prerequisites


Procedure

1. Launch the Horizon FLEX Admin Console.
   a. In a Web browser, type https://WebManagerServer:7443/rvm, where WebManagerServer is the DNS name or IP address of the host where the Mirage Web Manager is installed.
   b. Type the user name and password of a domain account that has access to Mirage.
   c. Click Login.
2 Verify that the Horizon FLEX Admin Console page appears correctly.

   The Images, Policies, Entitlements, and Virtual Machines buttons should be visible in the left navigation panel.

Host System Requirements for Fusion Pro

   The physical computer on which you install Fusion Pro is called the host system and its operating system is called the host operating system. To run Fusion Pro, the host system and the host operating system must meet specific hardware and software requirements.

Processor Requirements for Host Systems

   You can install Fusion Pro on any Mac that has a 64-bit Intel processor.

   Fusion Pro is compatible with Core 2 Duo, Xeon, i3, i5, i7, and newer processors.

Memory Requirements for Host Systems

   The host system must have enough memory to run Mac OS X, the guest operating systems that run inside the virtual machines on the Mac, and the applications that run in the Mac and guest operating systems.

   The minimum memory required on the host system is 4GB. 8GB is recommended.

   The host system must have 750MB of free disk space for Fusion Pro and at least 5GB of free disk space for each virtual machine.

Supported Host Operating Systems

   To install Fusion Pro, your Mac must have a supported Mac OS X operating system.

   - Mac OS X 10.9
   - Mac OS X 10.10

Install Fusion Pro on a Mac

   You install Fusion Pro in the same way you install other Mac OS X applications.

   Prerequisites

   - Verify that your Mac meets the system requirements for Fusion Pro. See “Host System Requirements for Fusion Pro,” on page 17.
   - Verify that you have the administrator password for your Mac.
   - Download the Fusion Pro installer to your Mac. You can obtain the Fusion Pro installer from the VMware website.
   - Verify that you have a Horizon FLEX license key for Fusion Pro. You must provide a Horizon FLEX license key during installation to activate the Horizon FLEX features in Fusion Pro.

   Procedure

   1 Double-click the VMware Fusion .dmg file to open it.
      The contents of the disk image appear in the VMware Fusion Finder window.
   2 In the VMware Fusion Finder window, double-click the VMware Fusion icon or drag it to the Applications folder.
   3 Click the VMware Fusion icon in the Applications folder.
   4 Type the administrator-level user credentials for your Mac to complete the installation.
5 Accept the license agreement and enter your Horizon FLEX license key.

_running an unattended player pro installation_

You can use the unattended installation feature of the Microsoft Windows Installer (MSI) to install Player Pro on several Windows hosts without having to respond to wizard prompts. This feature is convenient in a large enterprise.

Running an unattended installation of Player Pro is similar to running an unattended installation of VMware Workstation. For more information, see the VMware Workstation documentation at https://www.vmware.com/support/pubs/ws_pubs.html.

Creating a mass deployment package to deploy Fusion Pro

You can create a Fusion mass deployment package to install Fusion Pro on any number of end-user Macs. You can use standard package deployment tools, including Apple Remote Desktop Admin, to deploy the mass deployment package.

When you configure the mass deployment package, specify your Horizon FLEX license key in [Volume License] section of the Deploy.ini file and place a copy of the Fusion Pro application to the 00Fusion_Deployment_Items folder.

You can use the optional connectAtStartupURL parameter in the [Locations] section of the Deploy.ini file to specify a user name and the hostname of your Horizon FLEX server, for example:

connectAtStartupURL = vmware-rvm://johndoe@yourflexserver.com:7443

If there are no virtual machines installed on the user’s Mac when the user launches Fusion Pro, the Connect dialog box opens and the Server and Username text boxes are prepopulated with the hostname and user name that you specified in the connectAtStartupURL parameter.

For step-by-step information about creating a mass deployment package, see VMware KB article 2058680: Creating a VMware Fusion mass deployment package.
Before you create and deploy Horizon FLEX virtual machines, you must set up certificates to ensure that end users can successfully download and use their virtual machines.

VMware recommends that you use a certificate that is issued by a certificate authority (CA), such as Entrust or GoDaddy, or a third-party certificate, on your Horizon FLEX server. If you are using a self-signed certificate or a certificate from an internal CA instead of a generally trusted certificate, you must take steps to ensure that the certificate is trusted on all end-user computers that will download and use Horizon FLEX virtual machines.

This document does not describe how to set up certificates in Mirage. For information about setting up certificates in Mirage, see the Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html.

This chapter includes the following topics:

- “Creating a Trusted Certificates List,” on page 19
- “Using Self-Signed Certificates,” on page 22
- “Using Internal CA Certificates,” on page 23

## Creating a Trusted Certificates List

You can create a list of trusted certificates for Horizon FLEX virtual machines and import the list to the Horizon FLEX Policy Server. When you use a trusted certificates list, you do not need to install certificates on end-user hosts.

Using a list of trusted certificates can prevent malicious users from creating their own self-signed certificates for the same hostname and adding those certificates to their host’s list of trusted certificates.

When you configure the Horizon FLEX Policy Server to use a trusted certificates list, the server ignores the host’s list of certificates and uses the trusted certificates list to verify server connections instead. If the Horizon FLEX Policy Server cannot verify a certificate by using the trusted certificates list, the server connection fails.

If the trusted certificates list is empty in the source virtual machine, Player Pro and Fusion Pro authenticate against the host’s list of trusted certificates.

To create the trusted certificates list, you export each certificate to a separate file and then concatenate all of the files into a single file. You use the Horizon FLEX Admin Console to import the concatenated certificates file to the Horizon FLEX Policy Server.

You must export certificates in Privacy Enhanced Mail (PEM) format. On Windows systems, the PEM certificate encoding is called Base-64 encoded X.509 (.CER). Only PEM-encoded certificates are supported. No other certificate format (DER, Serialized Certificate Store/SST, PKCS #12/PFX, PKCS #7/P7B) is accepted.
About the PEM Format

The PEM format is a standard certificate format that is Base64 encoded.

An example of a PEM-format certificate is as follows:

```
-----BEGIN CERTIFICATE-----
MIIDojCCAwugAwIBAgIJAMLM0CJRzPyzMA8GCsqGSIb3DQEBAQUwBQ==
-----END CERTIFICATE-----
```

When you create a trusted certificates list, you concatenate multiple PEM-format certificates into a single file. Line endings are auto-detected. The following example shows the format of a concatenated certificates list that contains two certificates.

```
-----BEGIN CERTIFICATE-----
MIIDojCCAwugAwIBAgIJAMLM0CJRzPyzMA8GCsqGSIb3DQEBAQUwBQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDojCCAwugAwIBAgIJAMLM0CJRzPyzMA8GCsqGSIb3DQEBAQUwBQ==
-----END CERTIFICATE-----
```

Create PEM-Format Certificates

You can create PEM-format certificates by downloading the certificate from the CA's Web site or by exporting the certificates from a host system.

For example, you can download certificates for Verisign from the Symantec Web site at https://www.symantec.com/page.jsp?id=roots.

Export a PEM-Format Certificate From a Mac

You can export a PEM-format certificate from a Mac.

Prerequisites

Become familiar with how to use Keychain Access on a Mac. For more information, see the Apple Support Web site at http://support.apple.com.
Procedure
2. From the sidebar, select System Roots.
3. Locate the certificate to export.
4. Select File > Export Items.
5. Select a location to save the certificate and select the Privacy Enhanced Mail (.pem) file format.

Export a PEM-Format Certificate From a Windows System
You can export a PEM-format certificate from a Windows system. On Windows, the PEM certificate encoding is called Base-64 encoded X.509 (.CER).

Prerequisites
Become familiar with how to use Certificate Manager on a Windows system. For more information, see the Microsoft TechNet Web site at http://technet.microsoft.com.

Procedure
2. Right-click the certificate to export and select All Tasks > Export.
   a. Decide if you will export the private key with the certificate.
   b. Select Base-64 encoded X.509 (.CER) for the file export format.
      For the certificate to work with Horizon FLEX, you must choose this option.
   c. Provide a location to save the certificate and a file name.
   d. Review the settings you selected and click Finish.
      The certificate file is saved to the location you indicated.

Create and Import the Trusted Certificates List File
After you export your PEM-format certificates, you must construct the trusted certificate list and import the certificates list file to the Horizon FLEX Policy Server.

Prerequisites
Export each certificate in PEM format. See “Create PEM-Format Certificates,” on page 20.

Procedure
1. To create the trusted certificates list file, concatenate each PEM-format certificate file into a single file.
   You can use the cat command, or you can copy and paste the contents of the certificate files into a text file. You can safely edit Base64 content in a text editor.
   For example: $ cat mycert1.pem mycert2.pem mycert3.pem > list.pem
2. Launch the Horizon FLEX Admin Console.
   a. In a Web browser, type https://WebManagerServer:7443/rvm, where WebManagerServer is the DNS name or IP address of the host where the Mirage Web Manager is installed.
   b. Type the user name and password of a domain account that has access to Mirage.
   c. Click Login.
3 In the Horizon FLEX Admin Console, click the General System Settings icon and select Certificates.

4 Click Import, browse to the trusted certificates list file, and click Open to import the file.

**Updating Certificates on the Server**

When a certificate expires, and a new certificate has an expiration date that is set far into the future, you can add the new certificate as a second certificate to the trusted certificates list in the Horizon FLEX Policy Server.

Adding the new certificate to the trusted certificates list enables all Horizon FLEX virtual machines to download the new certificate. Then, when the certificate switch occurs, all of the Horizon FLEX virtual machines that received the new list of certificates can connect to the Horizon FLEX server and you can remove the old trusted certificate from the policy file.

**Using Self-Signed Certificates**

If you do not configure the self-signed certificate into the source virtual machine being prepared, you must install the certificate on each end-user host for Horizon FLEX virtual machines to function correctly.

If the list of certificates is empty in the policy file, Player Pro and Fusion Pro will fall back to authenticating against the host’s list of trusted certificates.

If you include the self-signed certificate of a source virtual machine on the Horizon FLEX Policy Server, and you configure or install the self-signed certificate for the Horizon FLEX Client (either in the source virtual machine’s policy file or in the host’s list of trusted certificates), you do not need to install the certificate on end-user hosts when certificate updates are required, for example, when a certificate expires.

For information about configuring certificates into a source virtual machine, see “Create a Source Virtual Machine in Fusion Pro,” on page 28.

For information about creating a trusted certificates list and importing it to the Horizon FLEX Policy Server, see “Creating a Trusted Certificates List,” on page 19.

For information about updating certificates, see “Updating Certificates on the Server,” on page 22.

**Install a Self-Signed Certificate on a Windows Computer**

To install a self-signed certificate on a Windows host, you export the certificate from your Horizon FLEX server and import it to the Windows computer.

**Prerequisites**

Become familiar with how to install and use the MMC Certificates snap-in on a Windows system. For more information, go to the Windows TechNet Web site at http://technet.microsoft.com.

**Procedure**

1 Export the self-signed certificate from your Horizon FLEX server.
   a On the Horizon FLEX server, start MMC (mmc.exe), add the Certificates snap-in for a computer account, and manage certificates for the local computer.
   b Navigate to Trusted Root Certification Authorities > Certificates.
   c Select and export the self-signed certificate.
      Export the certificate in DER-encoded binary X.509 (.CER) format.

2 Copy the self-signed certificate to the Windows computer.
3 Import the self-signed certificate to the Windows computer.
   a On the Windows computer, start MMC (mmc.exe).
   b Add the Certificates snap-in for the computer account and manage certificates for the local computer.
   c Import the self-signed certificate into Trusted Root Certification Authorities > Certificates.

The self-signed certificate is now trusted for all users.

Install a Self-Signed Certificate on a Mac

To install a self-signed certificate on a Mac host, you export the certificate from your Horizon FLEX server and import it to the Mac.

Prerequisites
- Become familiar with how to install and use the MMC Certificates snap-in on a Windows system. For more information, go to the Windows TechNet Web site at http://technet.microsoft.com.

Procedure
1 Export the self-signed certificate from your Horizon FLEX server.
   a On the Horizon FLEX server, start MMC (mmc.exe), add the Certificates snap-in for a computer account, and manage certificates for the local computer.
   b Navigate to Trusted Root Certification Authorities > Certificates.
   c Select and export the self-signed certificate.
      Export the certificate in DER-encoded binary X.509 (.CER) format.
2 Copy the self-signed certificate to the Mac.
3 Import the self-signed certificate on the Mac.
   a Double-click the self-signed certificate to open it in Keychain Access.
      The self-signed certificate appears in login.
   b Copy the self-signed certificate to System.
      You must copy the certificate to System to ensure that it is trusted by all users and local system processes, including the virtual machine (.vmx) processes in Fusion Pro.
   c Open the self-signed certificate in System, expand Trust, select Use System Default, and save your changes.
   d Reopen the self-signed certificate in System, expand Trust, select Always Trust, and save your changes.
   e Delete the self-signed certificate from login.

Using Internal CA Certificates

If you use a certificate from an internal CA instead of from a commercial CA such as Entrust or Go Daddy, and you do not configure the certificate into the source virtual machine being prepared, you must install the root CA certificate on each end-user host for Horizon FLEX virtual machines to function correctly.

**Note** Because the server certificate is signed by the root CA, you do not need to import the server certificate to end-user hosts.
If the list of certificates is empty in the policy file, Player Pro and Fusion Pro will fall back to authenticating against the host's list of trusted certificates.

If you include the internal CA certificate of a source virtual machine on the Horizon FLEX Policy Server, and you configure or install the certificate for the Horizon FLEX Client (either in the source virtual machine’s policy file or in the host’s list of trusted certificates), you do not need to install the root CA certificate on end-user hosts when certificate updates are required, for example, when a certificate expires.

For information about configuring certificates into a source virtual machine, see “Create a Source Virtual Machine in Fusion Pro,” on page 28.

For information about creating a trusted certificates list and importing it to the Horizon FLEX Policy Server, see “Creating a Trusted Certificates List,” on page 19.

For information about updating certificates, see “Updating Certificates on the Server,” on page 22.

### Install an Internal Root CA Certificate on a Windows Computer

To install an internal root CA certificate on a Windows host, you export the certificate from your Horizon FLEX server and import it to the Windows computer.

**Prerequisites**

- Become familiar with how to install and use the MMC Certificates snap-in on a Windows system. For more information, go to the Windows TechNet Web site at [http://technet.microsoft.com](http://technet.microsoft.com).
- Obtain and install an internal CA certificate. You can use the Windows MMC Certificates snap-in to request a certificate.

**Procedure**

1. Export the root CA certificate from your Horizon FLEX server.
   
   a. On the Horizon FLEX server, start MMC (`mmc.exe`), add the Certificates snap-in for a computer account, and manage certificates for the local computer.
   
   b. Navigate to **Trusted Root Certification Authorities > Certificates**.
   
   c. Select and export the root CA certificate.
      
      Export the certificate in DER-encoded binary X.509 (.CER) format.

2. Copy the root CA certificate to the Windows computer.

3. Import the root CA certificate to the Windows computer.
   
   a. On the Windows computer, start MMC (`mmc.exe`).
   
   b. Add the Certificates snap-in for the computer account and manage certificates for the local computer.
   
   c. Import the root CA certificate into **Trusted Root Certification Authorities > Certificates**.

The root CA certificate is now trusted for all users.

### Install an Internal Root CA Certificate on a Mac

To install an internal root CA certificate on a Mac host, you export the certificate from your Horizon FLEX server and import it to the Mac.

**Prerequisites**

- Become familiar with how to install and use the MMC Certificates snap-in on a Windows system. For more information, go to the Windows TechNet Web site at [http://technet.microsoft.com](http://technet.microsoft.com).

Procedure

1. Export the root CA certificate from your Horizon FLEX server.
   a. On the Horizon FLEX server, start MMC (mmc.exe), add the Certificates snap-in for a computer account, and manage certificates for the local computer.
   b. Navigate to **Trusted Root Certification Authorities > Certificates**.
   c. Select and export the root CA certificate.
      Export the certificate in DER-encoded binary X.509 (.CER) format.

2. Copy the root CA certificate to the Mac.

3. Import the root CA certificate on the Mac.
   a. Double-click the root CA certificate to open it in Keychain Access.
      The root CA certificate appears in **login**.
   b. Copy the root CA certificate to **System**.
      You must copy the certificate to **System** to ensure that it is trusted by all users and local system processes, including the virtual machine (.vmx) processes in Fusion.
   c. Open the root CA certificate, expand **Trust**, select **Use System Defaults**, and save your changes.
   d. Reopen the root CA certificate, expand **Trust**, select **Always Trust**, and save your changes.
   e. Delete the root CA certificate from **login**.
You can create multiple Horizon FLEX virtual machines and entitle those virtual machines to a variety of end users, including Mac users. Users can be connected or disconnected from the enterprise network when they use their Horizon FLEX virtual machines. When you create a source virtual machine for a Horizon FLEX virtual machine, you must select certain options to ensure that the virtual machine functions correctly with Horizon FLEX.

This document describes how to use Fusion Pro to create a source virtual machine. For information about using Workstation to create a source virtual machine, see the Workstation documentation at https://www.vmware.com/support/pubs/ws_pubs.html.

This chapter includes the following topics:

- “Horizon FLEX Virtual Machine Deployment Overview,” on page 27
- “Create a Source Virtual Machine in Fusion Pro,” on page 28
- “Prepare a Source Virtual Machine to Join a Domain,” on page 30
- “Compress a Source Virtual Machine Package,” on page 30
- “Register a Source Virtual Machine with the Horizon FLEX Policy Server,” on page 31
- “Creating Policies and Entitlements,” on page 32
- “Create a URI to Deploy a Horizon FLEX Virtual Machine,” on page 36
- “Manage Horizon FLEX Virtual Machines,” on page 37

Horizon FLEX Virtual Machine Deployment Overview

To deploy a Horizon FLEX virtual machine, you perform tasks in a specific order.

1. Create and configure a source virtual machine in Fusion Pro.
2. (Optional) Prepare the source virtual machine to join an Active Directory domain.
   See “Prepare a Source Virtual Machine to Join a Domain,” on page 30.
3. Compress the source virtual machine package and save it in your download directory.
4. Register the source virtual machine with the Horizon FLEX Policy Server.
   See “Register a Source Virtual Machine with the Horizon FLEX Policy Server,” on page 31.
5. Create a policy for the Horizon FLEX image and entitle the image to your Active Directory users and groups.
6 (Optional) Create a URI to deploy the Horizon FLEX virtual machine.

See “Create a URI to Deploy a Horizon FLEX Virtual Machine,” on page 36.

Create a Source Virtual Machine in Fusion Pro

You can use Fusion Pro to create a source virtual machine for a Horizon FLEX virtual machine. When you create a source virtual machine, you must set encryption and restriction information so that the virtual machine functions correctly with Horizon FLEX.

**NOTE** You can also use Workstation 11.0 to create a source virtual machine. Workstation is not included in the Horizon FLEX package.

If you enable USB device use, drag and drop, and copy and paste when you create the virtual machine, you can set policies in the Horizon FLEX Admin Console to enable or disable these features for end users. However, if you disable these features when you create the virtual machine, you cannot override the virtual machine settings to enable the features by setting policies.

**Prerequisites**

- Become familiar with how to create a virtual machine in Fusion Pro. See the Fusion documentation at https://www.vmware.com/support/pubs/fusion_pubs.html.
- Become familiar with the supported guest operating systems for Horizon FLEX virtual machines. See “Supported Host and Guest Operating Systems,” on page 10.
- Install Fusion Pro. See “Install Fusion Pro on a Mac,” on page 17.

**Procedure**

1. Open Fusion Pro and create a virtual machine.
   Select a guest operating system that is supported for Horizon FLEX virtual machines. Configure the virtual machine in the way you want to distribute it to your end users.

2. From the Virtual Machine Library, select the newly created virtual machine and select **Settings > Encryption & Restrictions**.

3. Check **Enable Encryption** and set a password for opening the virtual machine.
   The password must be six characters or longer. You must give this encryption password to your end users to enable them to open the virtual machine.

   **IMPORTANT** Make sure you retain the encryption password. The virtual machine cannot be accessed without this password.

4. Check **Enable Restrictions** and set a password for editing the restrictions on the virtual machine.
   This password should be different than the virtual machine encryption password.

   **IMPORTANT** Make sure you retain the restrictions password. You cannot edit the restrictions on the virtual machine without this password.

5. Click **Configure**.
   The restrictions configuration window opens.

6. Set the **Restriction Type** to **Managed**.
   You must set the restriction type to **Managed** to distribute and use the virtual machine with Horizon FLEX.
7 Type the URL of the Horizon FLEX server on which you intend to host the virtual machine in the Restrictions Management Server text box.

8 Click Check Server to verify the Horizon FLEX server URL.

9 (Optional) To add trusted certificates to the virtual machine, click the + button and navigate to the location of each certificate file.
   If you add certificates to the virtual machine, the Horizon FLEX Client uses the certificates in the virtual machine and does not use the certificates on the host. To control certificates for all virtual machines from the Horizon FLEX Policy Server, leave the certificates box blank.

10 Click Save.

11 Click the Lock icon to prevent further changes to the restrictions of the virtual machine.
   You can edit restrictions for the virtual machine by using the restrictions password.

What to do next
If you intend to join the Horizon FLEX virtual machine to an Active Directory domain, prepare the virtual machine to join the domain. See “Prepare a Source Virtual Machine to Join a Domain,” on page 30.

To install the Mirage client in the source virtual machine, see “Install the Mirage Client In a Source Virtual Machine,” on page 29.

Install the Mirage Client In a Source Virtual Machine
If the source virtual machine has a Windows guest operating system, you can install the Mirage client in the virtual machine. Installing the Mirage client is optional.

If you install the Mirage client in a source virtual machine, you can select disaster recovery scenarios when you entitle the virtual machine. For example, you can select an option to make the Mirage server create a CVD for the Horizon FLEX virtual machines that the end user downloads. Mirage periodically synchronizes end-user data into the datacenter based on the selected Mirage policy. You can use this data to restore the CVD or access files on the virtual machine by using the Mirage File Portal in the main Mirage Management Console.

Prerequisites
- Create the source virtual machine. See “Create a Source Virtual Machine in Fusion Pro,” on page 28.
- Obtain the VMware Mirage Installation Guide for Mirage client installation instructions.

Procedure
1 In Fusion Pro, start the source virtual machine and log in to the guest operating system.
2 Install the latest version of VMware Tools.
   a From the menu bar, select Virtual Machine > Install VMware Tools.
   b Click Next to progress through the installation.
   c Select Complete, unless you need to exclude certain features of VMware Tools, and click Next.
   d Click Install.
   e When the installation finishes, click Yes to restart the virtual machine.
3 Install the Mirage client.
4 In the Mirage Management console, verify that the endpoint appears as Pending Assignment.
5 Power off the source virtual machine.
Prepare a Source Virtual Machine to Join a Domain

If you intend to join a Horizon FLEX virtual machine to a specific Active Directory domain, you must prepare the source virtual machine to join the domain before you register it with the Horizon FLEX Policy Server.

Prerequisites

- Create a source virtual machine. See “Create a Source Virtual Machine in Fusion Pro,” on page 28.

**Note**: Do not install Windows 7 Home edition or a non-Windows guest operating system in the source virtual machine. You cannot join a Windows 7 Home edition operating system or a non-Windows guest operating system to a domain.

- Verify that you have the administrator password for the source virtual machine.

Procedure

1. In Fusion Pro, start the source virtual machine and log in to the guest operating system.
2. (Optional) Turn off Windows update.
3. Install the latest version of VMware Tools.
   a. From the menu bar, select **Virtual Machine > Install VMware Tools**.
   b. Click **Next** to progress through the installation.
   c. Select **Complete**, unless you need to exclude certain features of VMware Tools, and click **Next**.
   d. Click **Install**.
   e. When the installation finishes, click **Yes** to restart the virtual machine.
4. Run `install-rvmsetup.cmd` as an administrator to install the VMware RVM Setup Service in the source virtual machine.
   The VMware RVM Setup Service performs the domain join operation. `install-rvmsetup.cmd` is included with VMware Tools.
5. Open the Windows Services snap-in (`services.msc`) and verify that the VMware RVM Setup Service startup type is set to Automatic.
6. Shut down the source virtual machine.
   The VMware RVM Setup Service starts the next time you boot up the source virtual machine.

Compress a Source Virtual Machine Package

You must compress the source virtual machine package in TAR (.tar) format so that end users can easily download the virtual machine. A virtual machine package (sometimes called a bundle) includes all of the virtual machine files required to run a virtual machine.

Prerequisites

- Create the source virtual machine. See “Create a Source Virtual Machine in Fusion Pro,” on page 28.
- Create and configure a download folder for your Horizon FLEX virtual machine packages. See “Create a Download Folder for Horizon FLEX Virtual Machine Packages,” on page 15 and “Create a Virtual Directory and Edit Site Bindings in IIS,” on page 15.

Procedure

1. If the source virtual machine is running, shut it down.
2 In Fusion Pro, navigate to the source virtual machine.

3 Select File > Export to TAR and export the source virtual machine package to a TAR file.

   **Note** Remove any spaces from the TAR file name. Removing spaces from the file name can make it easier to connect to the download URL for the virtual machine.

4 Export the TAR file to your Horizon FLEX virtual machine packages download folder.

**What to do next**

Register the source virtual machine with the Horizon FLEX Policy Server. See “Register a Source Virtual Machine with the Horizon FLEX Policy Server,” on page 31.

**Register a Source Virtual Machine with the Horizon FLEX Policy Server**

You must register a source virtual machine with the Horizon FLEX Policy Server as a Horizon FLEX image before you can distribute the virtual machine to end users.

**Prerequisites**

- Verify that your Horizon FLEX virtual machine packages download directory is set up properly. See “Create a Download Folder for Horizon FLEX Virtual Machine Packages,” on page 15 and “Create a Virtual Directory and Edit Site Bindings in IIS,” on page 15.
- Verify that restrictions are already set in the source virtual machine's configuration (.vmx) file. If you select a virtual machine does not have restrictions set, the Horizon FLEX Policy Server rejects the .vmx file as invalid. For information about setting restrictions in a virtual machine, see “Create a Source Virtual Machine in Fusion Pro,” on page 28.

**Procedure**

1 If the source virtual machine is on a Mac, perform these steps.
   
   a Find the virtual machine package (.vmwarevm) file for the virtual machine, right-click the file name, and select **Show Package Content**.
   
   b Copy the virtual machine configuration (.vmx) file to a location that is accessible to the Horizon FLEX server.

2 Launch the Horizon FLEX Admin Console.
   
   a In a Web browser, type `https://WebManagerServer:7443/rvm`, where `WebManagerServer` is the DNS name or IP address of the host where the Mirage Web Manager is installed.
   
   b Type the user name and password of a domain account that has access to Mirage.
   
   c Click **Login**.

3 Click **Images** in the left navigation panel.

4 Click the **New ( +)** button.

5 Click **Select** next to the **Select Image File** text box and browse to the virtual machine configuration (.vmx) file for the source virtual machine.

6 Type a user-friendly name for the Horizon FLEX virtual machine file in the **Image Name** text box.

   For example: **Windows 7 VM**

7 (Optional) Type a description of the Horizon FLEX virtual machine in the **Description** text box.
8 (Optional) Click the **Change** button next to **Icon** and upload an icon for the Horizon FLEX virtual machine.

Uploaded icons must be PNG (.png) files.

9 (Optional) In the **Image URL** text box type the fully qualified path of the TAR file that contains the source virtual machine package.

End users will download the Horizon FLEX virtual machine from this URL. The URL format is `https://server:port/download_directory/filename.tar`, where `server` is the hostname or IP address of the server where you stored the TAR file, `port` is the port number on the server, `download_folder` is the name of the Horizon FLEX virtual machine download folder that contains the TAR file, and `filename.tar` is the name of the TAR file that contains the source virtual machine package.

For example: `https://flexserver.demo.local:7443/flexdownloads/windows7vm.tar`

10 (Optional) Type text in the **Disclaimer (Optional)** text box.

If you do not specify any text, the Horizon FLEX Client does not display disclaimer text when a user downloads the Horizon FLEX virtual machine.

11 Click **OK** to register the source virtual machine as a Horizon FLEX image.

12 (Optional) Type the image URL in a Web browser to verify the URL.

For example: `https://flexserver.demo.local:7443/flexdownloads/windows7vm.tar`

You should be prompted to save the file. If you receive a permissions error, you might need to adjust the NTFS permissions for the download folder.

**What to do next**

Add policies to the Horizon FLEX image. See “Configure a Policy for a Horizon FLEX Image,” on page 33.

### Creating Policies and Entitlements

You use policies to set an expiration date and control the features in virtual machine instances created from a Horizon FLEX image. You use entitlements to allow specific users and groups to create virtual machine instances from a particular Horizon FLEX image.

You associate a policy with each entitlement that you create. This policy defines the default restriction settings for the virtual machine instances created from the Horizon FLEX image in the entitlement.

You can include the same Horizon FLEX image in multiple entitlements, and you can associate each entitlement with a different policy. The same user can be a member of multiple entitlements. When a user creates a virtual machine instance from an entitlement, the instance inherits the most restrictive policy settings of all the entitlements of which the user is a member.

When a virtual machine instance is created, the policies associated with entitlements determine the instance’s initial restrictions. As an administrator, you can change the restriction settings for a particular virtual machine instance. Instance-specific restrictions act as the de facto restrictions for a specific user and virtual machine combination. For information about editing restrictions for virtual machines, see “Manage Horizon FLEX Virtual Machines,” on page 37.
Configure a Policy for a Horizon FLEX Image

You configure policies to set an expiration date and control the features in virtual machine instances created from a Horizon FLEX image, including USB device use and copy and paste operations.

IMPORTANT If the USB device use, drag and drop, and copy and paste features are enabled in the source virtual machine, you can configure a policy to enable or disable these features when users download an instance of the virtual machine. If these features are disabled in the source virtual machine, you cannot override the virtual machine settings by enabling the features in a policy.

You select the policy to assign to a Horizon FLEX image when you entitle the image to users. You can use the same policy in multiple entitlements.

Procedure

1. Launch the Horizon FLEX Admin Console.
   a. In a Web browser, type https://WebManagerServer:7443/rvm, where WebManagerServer is the DNS name or IP address of the host where the Mirage Web Manager is installed.
   b. Type the user name and password of a domain account that has access to Mirage.
   c. Click Login.
2. Click Policies in the left navigation pane.
3. Click the New (+) button to add a new policy, or select an existing policy and click Edit to modify it.
4. Type a name for the policy in the Policy Name text box.
5. (Optional) Type a description for the policy in the Description text box.
6. In General Restrictions, configure virtual machine restrictions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expiration date</td>
<td>Use the calendar widget to set an expiration date for the virtual machine.</td>
</tr>
<tr>
<td>Use of USB devices</td>
<td>Specify whether to allow the use of USB devices in the virtual machine.</td>
</tr>
<tr>
<td>Copy and Paste operations</td>
<td>Specify whether to allow copy and paste operations in the virtual machine.</td>
</tr>
<tr>
<td>Drag and Drop operations</td>
<td>Specify whether to allow drag and drop operations in the virtual machine.</td>
</tr>
<tr>
<td>Require the user to change the power on passphrase when moving or copying the virtual machine</td>
<td>Specify whether to require users to change the encryption password if they move or copy the virtual machine.</td>
</tr>
</tbody>
</table>
7. (Optional) In End User Messages, configure virtual machine expiration settings.
   a. Type a message to display to the user when the virtual machine expires.
   b. Select the Display this message check box, select the number of days before the virtual machine expires to display a custom message, and type the custom message text.
8 In **Server Settings**, configure Horizon FLEX server settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| FLEX Server URL | Type the URL of the Horizon FLEX server that hosts the virtual machine package. For example:  
**https://localhost:7443**  
**IMPORTANT** Do not add `/rvm` to the end of the URL. |
| Server Contact Frequency | Select the frequency with which the virtual machine contacts the server for synchronization. |
| Offline Time Limit | Set the number of days that users can use the virtual machine before the virtual machine must connect to the Horizon FLEX server. When the offline time limit is exceeded, the virtual machine must connect to the Horizon FLEX server before it can power on. |

9 Click **OK** to save the policy.  
The new policy appears in the policy list.

**What to do next**  
Enter it the Horizon FLEX virtual machine. See “**Entitle a Horizon FLEX Image,**” on page 34.

**Entitle a Horizon FLEX Image**

You use entitlements to allow specific users and groups to create virtual machine instances from a particular Horizon FLEX image.

Users can download any Horizon FLEX virtual machine to which they are entitled. Users are not required to enter a password before they download a Horizon FLEX virtual machine. All source virtual machines must be created with an encryption password. Users cannot use a Horizon FLEX virtual machine without providing the encryption password. You can share the encryption password with users at your discretion.

**Prerequisites**

- Make sure the appropriate Active Directory users and groups are synchronized in the Horizon FLEX database. See “**Configure Active Directory Settings,**” on page 16.
- Register the source virtual machine with the Horizon FLEX Policy Server. See “**Register a Source Virtual Machine with the Horizon FLEX Policy Server,**” on page 31.
- Configure a policy for the Horizon FLEX image. See “**Configure a Policy for a Horizon FLEX Image,**” on page 33.

**Procedure**

1 Launch the Horizon FLEX Admin Console.
   a In a Web browser, type **https://WebManagerServer:7443/rvm**, where `WebManagerServer` is the DNS name or IP address of the host where the Mirage Web Manager is installed.
   b Type the user name and password of a domain account that has access to Mirage.
   c Click **Login**.
2 Click **Entitlements** in the left pane.
3 Click the **New (++)** button to create a new entitlement, select an existing entitlement and click **Edit** to modify it, or select an existing entitlement and click **Duplicate** to duplicate it.
4 Type a name for the entitlement in the Entitlement Name text box, select a Horizon FLEX image to add to the entitlement, and click Next.

You can use the search field to filter the list of Horizon FLEX images.

If you duplicate an existing entitlement, you must rename the duplicate entitlement before saving it.

5 Select the Active Directory users and groups to include in the entitlement.
   a Use the search field to find and select users and groups to add to the entitlement.
      Newly created Active Directory users and groups can take up to 15 minutes to appear in search results.
   b Click Add to add a user or group to the Entitlement Members list.
      You can use the Remove or Clear All buttons to manage the list of members.
   c Click Next.

6 Select a policy for the entitlement and click Next.

You can use the search field to filter the list of policies and the Clear Filter and Show Filter buttons to manage your searches.

7 (Optional) To use a virtual machine naming pattern, select the Use machine name configuration check box and configure the naming pattern.
   a Type the machine name pattern to use in the Machine Name Pattern text box.
      To ensure that each virtual machine receives a different name and can join the domain, include the {username} placeholder. This placeholder is replaced by the individual user’s name when the user downloads the virtual machine.
      For example, if the name pattern is vm-{username}, and user1 downloads the virtual machine, the virtual machine name is changed to vm-user1.
      The machine name is limited to 15 characters.
   b Select a domain name from the Domain Name drop-down menu.
   c (Optional) Type an OU in the Organizational Unit text box, or leave the text box blank to use the default OU.
      For example: OU=hr1, OU=hr, OU=flex, DC=ws, DC=test, DC=com
8 (Optional) If you installed the Mirage client in the virtual machine, select whether to manage the virtual machine with Mirage.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use VMware Mirage for disaster recovery and Image management scenarios</td>
<td>Select this option to select a CVD policy, a base layer, an apps layer, and other configurations. The Mirage server automatically creates a CVD for virtual machines the end user downloads. Mirage periodically synchronizes end-user data into the datacenter based on the selected Mirage policy. In the main Mirage Management Console, you can use this data to restore the CVD or access files on the virtual machine by using the Mirage File Portal. The Mirage server also automatically deploys base and app layers to the virtual machine after it has been provisioned to ensure image compliance and remote app delivery.</td>
</tr>
<tr>
<td>Use VMware Mirage for disaster recovery scenarios</td>
<td>Select this option to select a CVD policy. The Mirage server automatically creates a CVD for virtual machines the end user downloads. You can use this data to restore the CVD or access files on the virtual machine by using the Mirage File Portal in the main Mirage Management Console.</td>
</tr>
<tr>
<td>Do not use VMware Mirage to manage the virtual machines</td>
<td>Select this option to opt out of managing the virtual machine with Mirage.</td>
</tr>
</tbody>
</table>

**Note**: If you delete a virtual machine in which the Mirage client is installed, the Mirage server automatically archives the CVD of the deleted virtual machine.

9 Click **Next** and review the settings of the entitlement.

10 Click **Finish** to save the entitlement, or click **Back** to return to the previous page and edit the entitlement.

### Create a URI to Deploy a Horizon FLEX Virtual Machine

You can deploy a Horizon FLEX virtual machine by creating a uniform resource identifier (URI). Using a URI, you can create an email that contains a link that the end user can click to connect to a server and download a Horizon FLEX virtual machine.

**Prerequisites**

Give the user a password for the server and the encryption password for the virtual machine.

**Procedure**

1 Construct a URI for the end user.

   A URI has the following structure:

   ```
   vmware-rvm://username@myserver.com:7443
   ```

   * `username` is the user’s login name and `myserver.com` is the hostname of the server. You must include `vmware-rvm://` and `:7443` in the server address. Do not include `http` or `https` in the server address.

2 Type link text in an email and enter hyperlink information for the URI.

   You can use any email system to send the link. However, because the format of the URI is not recognized as a standard URL, you must manually enter the hyperlink information.

   For example, to include the link in an email in Microsoft Outlook, perform these steps.

   a Create an email for the user and type some link text.

   For example: **Your Horizon FLEX virtual machine**

   b Highlight the link text, right-click the highlighted text, and select **Hyperlink**.
c Select Link to: Existing File or Web Page.

d Type the URI in the Address field.

For example: `vmware-rm://johndoe@yourserver.com:7443`

The link is now active.

e Click OK.

f Send the email to the user.

When the user clicks the link in the email, the user's Horizon FLEX Client starts and the server connection dialog box opens. The server and user name text boxes are prepopulated with the values you specified in the URI. The user enters a password and connects to the server to download a virtual machine.

**Manage Horizon FLEX Virtual Machines**

You can view the inventory of deployed Horizon FLEX virtual machines in the Horizon FLEX Admin Console.

You can use the Search field to filter the virtual machine list and the sortable column headings to find a specific virtual machine. The column heading drop-down menu enables you to select the columns to view or hide.

When you select a virtual machine in the list, you can expand the Properties window at the bottom of the page to view general settings for the virtual machine and policies applied to the virtual machine.

**Procedure**

1. Launch the Horizon FLEX Admin Console.

   a In a Web browser, type `https://WebManagerServer:7443/rvm`, where `WebManagerServer` is the DNS name or IP address of the host where the Mirage Web Manager is installed.

   b Type the user name and password of a domain account that has access to Mirage.

   c Click Login.

2. Click Virtual Machines in the left navigation pane.

   The inventory of deployed Horizon FLEX virtual machines appears on the Virtual Machines page.

3. To manage a specific virtual machine, select the virtual machine in the list.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Select a virtual machine and click Edit to change the policies assigned to this virtual machine.</td>
</tr>
<tr>
<td>Lockout</td>
<td>Select a virtual machine and click Lockout to revoke user access to the specific virtual machine.</td>
</tr>
<tr>
<td>Reactivate</td>
<td>Select an expired or locked-out virtual machine and click Reactivate to reset the virtual machine.</td>
</tr>
<tr>
<td>Archive</td>
<td>Select a virtual machine and click Archive to disable the virtual machine for use and keep an offline record of the virtual machine. Check the Display archived instances box at the bottom of the Virtual Machines page to view virtual machines that have been archived. You can click Reactivate to enable an archived virtual machine.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select an archived virtual machine and click Delete. You cannot delete a virtual machine that has any other status than Archived.</td>
</tr>
</tbody>
</table>
To determine the actions you can take for a virtual machine, view the virtual machine status in the Status column.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>The virtual machine is use, has contacted the server, and has not expired.</td>
</tr>
<tr>
<td>Inactive</td>
<td>The Horizon FLEX Client that the user used to open the virtual machine has failed to contact the server for longer than the offline working policy period.</td>
</tr>
<tr>
<td>Expired</td>
<td>The expiration date has been reached and the virtual machine has been turned off.</td>
</tr>
<tr>
<td>Pending Expired</td>
<td>The server is waiting for confirmation from the Horizon FLEX Client that the virtual machine is expired.</td>
</tr>
<tr>
<td>Locked Out</td>
<td>An administrator has locked out the user of the virtual machine.</td>
</tr>
<tr>
<td>Pending Lockout</td>
<td>A lock out has been initiated. The status remains Pending until the Horizon FLEX Client confirms the virtual machine has been locked out.</td>
</tr>
<tr>
<td>Pending Reactivate</td>
<td>The server is waiting for confirmation from the Horizon FLEX Client that the virtual machine is reactivated.</td>
</tr>
<tr>
<td>Downloading</td>
<td>The user is downloading the virtual machine.</td>
</tr>
<tr>
<td>Requires Download</td>
<td>The user deleted the virtual machine after downloading it. Because the user's Horizon FLEX Client will never reuse this instance of the virtual machine, you should archive or delete the virtual machine. If the user downloads a new version of the virtual machine, the Horizon FLEX Client will download a new virtual machine that has a different name.</td>
</tr>
<tr>
<td>Archived</td>
<td>The virtual machine has been archived.</td>
</tr>
<tr>
<td></td>
<td>Note: You must select the <strong>Display archived instances</strong> check box to view archived virtual machines.</td>
</tr>
<tr>
<td>Domain Join Fail</td>
<td>The virtual machine failed to join a domain. The most common reason why a virtual machine might fail to join a domain is that the object already exists in Active Directory. In this case, check the offline domain join log, which is maintained by the operating system, to determine how to solve the failure.</td>
</tr>
</tbody>
</table>
URI format 36
USB settings 33

V
virtual machine package 30
VMware RVM Setup Service 30
VMware Tools 30

W
Windows certificates 21–24