VMware Horizon FLEX Administration Guide

26 SEP 2017

Horizon FLEX 1.12

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Copyright © 2014–2017 VMware, Inc. All rights reserved. Copyright and trademark information.

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

Contents

VMware Horizon FLEX Administration Guide

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.

1 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

Horizon FLEX is a combination of VMware components, including Mirage, Fusion Pro, and Workstation Player.

VMware Mirage® for Horizon FLEX

The Mirage Server that is used by Horizon FLEX. The server provides Horizon FLEX virtual machine management. You can manage, back up, and patch virtual machines by using the Mirage for Horizon FLEX layering technology. Use of Mirage for Horizon FLEX is optional. You can also use other image management tools to manage Horizon FLEX virtual machines.

Horizon FLEX Policy Server

The standard Mirage server with an extension 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. A Horizon FLEX server can support up to 10,000 users.

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 Manager component. You 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 any 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 Workstation Player™ for Windows computers. Fusion Pro and Workstation Player are included in the Horizon FLEX package. One license key is provided for both Fusion Pro and Workstation Player.

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.

Note You can also use VMware Workstation Pro™ to create source virtual machines. Workstation Pro 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 a subset of the features available in Mirage:

- Mirage Server
  - Mirage Management Server
- Mirage Web Manager
  - Mirage Management Console

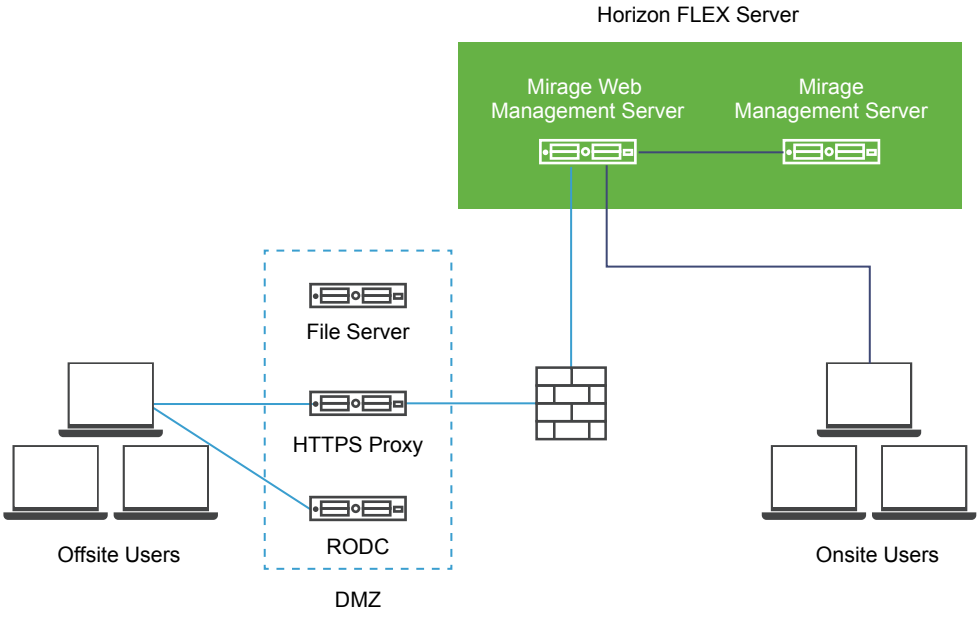
This document does not describe all of the information pertaining to Mirage. For complete information about Mirage, see the Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html.

Horizon FLEX Architecture

A typical Horizon FLEX deployment includes the Horizon FLEX server, a file server, an HTTPS proxy, an optional 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 Without Mirage



Horizon FLEX Server

The Horizon FLEX server is composed of the Horizon FLEX Admin Console and the Horizon FLEX Policy Server. 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
- Provides security certificate management to ensure the secure and trusted communication between the deployed Horizon FLEX virtual machines and the Horizon FLEX server
- Enforces policy settings to the client
- Enables modification of policy settings
- 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.

By default, port 7443 is used by the Horizon FLEX Policy Server for external access, and port 8443 is used by the Mirage Management Server to communicate with the Horizon FLEX Policy Server. You must configure your firewall policies to allow the required ports. For a complete list of ports used by Mirage, see the Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html.

File Server

A file server stores the TAR files that contain the source virtual machine files for Horizon FLEX virtual machines. The file server can be on any server that a client user can access without entering credentials. The file server is located inside the DMZ in this example but that is not required.

HTTPS Proxy

An HTTPS proxy enables offsite end-user systems to reach the Horizon FLEX server and get policy updates.

RODC

An RODC enables office end-user systems to log in to their Horizon FLEX virtual machines and join the Active Directory domain for the first boot up of the virtual machine. An RODC is required only if you are allowing outside users to log in without using a VPN. The RODC is inside the DMZ.

Load Balancing

Horizon FLEX supports load balancing using multiple policy servers. For more information about setting up multiple Mirage servers for load balancing, see the Mirage documentation.

Horizon FLEX System Requirements

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

To determine the appropriate Horizon FLEX Client version for end users, see the Horizon FLEX release notes.

Horizon FLEX Server and Mirage Server Requirements	For more information, see "Horizon FLEX Server System Requirements," on page 10.
Mirage for Horizon FLEX	The system requirements for Horizon FLEX 1.12 are the same as for Mirage 5.9.1. See the Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html.
Horizon FLEX Client for Mac	Fusion Pro is the Horizon FLEX Client for Mac for Horizon FLEX . For Fusion Pro hardware and software requirements, see the *VMware Horizon FLEX Client User Guide*.
Horizon FLEX Client for Windows	Workstation Player is the Horizon FLEX Client for Windows for Horizon FLEX. For more information about Workstation Player, see the Workstation Player for Windows documentation at https://docs.vmware.com/en/VMware-Workstation-Player/index.html . For Workstation Player hardware and software requirements, see the *VMware Horizon FLEX Client User Guide*.
Workstation Pro	You can use Workstation Pro to create and open a source virtual machine, but Workstation Pro cannot download a Horizon FLEX virtual machine. Workstation Pro is not included in the Horizon FLEX installation package. For Workstation Pro hardware and software requirements, see the Workstation Pro documentation at https://docs.vmware.com/en/VMware-Workstation-Pro/index.html.

Horizon FLEX Server System Requirements

The Horizon FLEX environment includes system requirements for both the Horizon FLEX server and the Mirage server.

Horizon FLEX Server System Requirements

- Minimum CPU: 1 Quad-Core Processor or 2 vCPU
- 2.26 GHz Intel core speed or equivalent
- Minimum RAM: 512 MB with 4 GB recommended

- Minimum disk space: 10 GB+, 40 GB+ recommended

  Note Horizon FLEX does not require the MongoDB database, so the additional storage is not required. When installing the Mirage server, disregard the prompt and click **Next**.

- Windows Server 2008 R2, Windows Server 2012 or later
- .NET 4.5.1 and later
- IIS 7.0+ with II6 Management Compatibility, with ASP and ASP.NET
- Active Directory: Administrator account with permissions to add computer objects to the domain (required only if Horizon FLEX virtual machines will join the domain)
- Any of the following Microsoft SQL server versions (required for Mirage installation).
  - Microsoft SQL server 2008 64-bit R2 Express, Standard or Enterprise edition
  - Microsoft SQL server 2012 64-bit SP1 Express, Standard or Enterprise edition
  - Microsoft SQL server 2014 64-bit Express, Standard or Enterprise edition

  Note To optimize the scalability and performance of the Microsoft SQL server, use the Enterprise edition.

- HTTP file share or IIS virtual directory with available space for source virtual machines
- Firewall ports for the Horizon FLEX Admin Console
  - IIS and Horizon FLEX Web App default ports: HTTP - 7080, HTTPS - 7443 (Calls directed to the HTTP port are redirected to the HTTPS port.)
  - Mirage Management Server listens to Windows Communication Foundation (WCF) requests on the following port: HTTP - 8443
- A certificate is required for the Horizon FLEX Server.

Mirage Server Requirements

- Minimum CPU: 4 vCPU with 8 vCPU recommended
- Minimum RAM: 8 GB with 16 GB recommended
- 250 GB free disk space
- Windows 2008 R2, Windows 2012 or later
- .NET 4.5.1 and later

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

Horizon FLEX Client	Supported Operating Systems
Workstation Player for Windows	■ Windows 7 ■ Windows 8.1 Enterprise ■ Windows 8 ■ Windows 8.1 Pro ■ Windows 10 **Note** Workstation Player supports only 64-bit operating systems.
Fusion Pro	■ macOS 10.13 ■ macOS 10.12 ■ Mac OS X 10.11

Supported Guest Operating Systems

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

- Windows 10
- Windows 8.1
- Windows 7
- Windows XP
- Windows Server 2012 R2
- Windows Server 2016
- Ubuntu 15.10
- Ubuntu 16.04

Installing Horizon FLEX 2

The Horizon FLEX installation 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

Horizon FLEX is a combination of VMware components, including Mirage, Fusion Pro, and Workstation Player. The Horizon FLEX installation involves installing each of these components and performing additional Horizon FLEX-specific tasks. For a successful Horizon FLEX deployment, you must understand the sequence of required tasks.

Before you install Horizon FLEX, verify the following:

- All hardware and software requirements are met.
- You have valid licenses for all components.
- You have downloaded the Horizon FLEX component installers from the VMware Horizon FLEX product download page.

You install Horizon FLEX by performing these steps:

1 Install the Mirage system.

  See "Installing and Configuring Mirage Components for the Horizon FLEX Server," on page 14.

2 Set up certificates for the Horizon FLEX Server.

  See Chapter 3, "Setting up Certificates for the Horizon FLEX Server," on page 21.

3 Set up certificates for Horizon FLEX virtual machines.

  See Chapter 4, "Setting Up Certificates for Horizon FLEX Virtual Machines," on page 25.

4 Create a download folder for storing your Horizon FLEX virtual machine packages.

  See "Create a Download Folder for Horizon FLEX Virtual Machine Packages," on page 15.

5 Add a virtual directory in IIS for your Horizon FLEX virtual machine download folder and edit the site bindings.

See "Configure the IIS SSL Server Certificate for the Horizon FLEX Server," on page 21.

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

See "Configure Active Directory Settings," on page 16.

7 Test the connection to the Horizon FLEX Admin Console.

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

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

See "Installing the Horizon FLEX Client for End Users," on page 17.

9 Create and deploy Horizon FLEX virtual machines.

See Chapter 5, "Creating and Deploying Horizon FLEX Virtual Machines," on page 35.

Installing and Configuring Mirage Components for the Horizon FLEX Server

The first Horizon FLEX installation step is to install and configure the Mirage system.

The Horizon FLEX server package includes the following components:

- VMware Mirage for Horizon FLEX (the Mirage Core Software)
- Mirage PowerCLI for Windows
- Mirage Gateway Appliance Software

Note The Mirage Core Software is required for the Horizon FLEX server. The Mirage PowerCLI for Windows and Mirage Gateway Appliance Software are only required if you will use Mirage to manage the Horizon FLEX virtual machines.

Download the installation files from the Horizon FLEX Server product download page.

The Mirage deployment involves the installation of the following components.

1 Mirage Management Server

2 Mirage Server

3 Mirage Management Console

4 Mirage Web manager

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 for the Horizon FLEX server to operate correctly.

- The Mirage Server and Mirage console are only required if you are installing the Mirage client in the source virtual machines.
- If placing the virtual machine images on the same system as the Horizon FLEX Server, place the images in the IIS "Default Web" server.

- The Web Management Server and the Mirage Management Server can be installed on the same server, but installing them on different servers improves scalability. The SQL server can also be installed on a separate server from the Web Management Server and the Mirage Management Server to improve scalability.
- 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 configuring the Mirage Server for SSL, you must install the server SSL certificate.
- Horizon FLEX does not require the MongoDB database, so the additional storage is not required. When installing the Mirage server, disregard the prompt and click **Next**.
- You can deploy the two components of the Horizon FLEX server, the Horizon FLEX Admin Console and the Horizon FLEX Policy Server, on the same port or on separate ports.
- Before you install the Mirage Web Manager, verify that .NET Framework 4.5.1 is installed on the server.
- The Mirage Management Server must run as a user who 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 who has domain join permissions. The user must have permission to add computer objects to the domain.
- FLEX uses the Win32 Logon API to authenticate the end users to the Web Management Server (IIS server). Therefore, client users must be able to perform an interactive login on to the IIS server. If there is a GPO blocking this login, the authentication fails. For added security, you can turn on remote access on the server. Configure the local server security to allow FLEX users to log in to the file portal. This configuration is performed by modifying the Local Security Policy.

  a On the Windows server where IIS and the Mirage Web Access components are installed, log in as Administrator.

  b Under **ADMINISTRATIVE TOOLS**, open the Local Security Policy by selecting **LOCAL SECURITY POLICY**.

  c Under **LOCAL POLICIES | USER RIGHTS ASSIGNMENT**, browse to **ALLOW LOG ON LOCALLY** and double-click to open it.

  d Ensure that ADMINISTRATORS and USERS local security groups are defined here. If not, ensure that the appropriate Domain Security Groups are defined at their place

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 for storing these TAR files.

Procedure

1 Create the download folder on a different server than the Horizon FLEX server.

  The download folder should not be on the Horizon FLEX server, and 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 with an administrative group, such as Horizon FLEX Admins. This can be an administrative group for users to manage Horizon FLEX deployments.

  This step can make it easier to register your source virtual machines with the Horizon FLEX Policy Server.

What to do next

See "Configure the IIS SSL Server Certificate for the Horizon FLEX Server," on page 21.

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 with the Horizon FLEX database. You can optionally configure Horizon FLEX to synchronize only a specific organization unit (OU).

Prerequisites

Install Mirage for Horizon FLEX. See "Installing and Configuring Mirage Components for the Horizon FLEX Server," on page 14.

Procedure

1 Start the Horizon FLEX Admin Console.

   a In a Web browser, enter **`https://WebManagerServer:port/rvm`**.

      - *WebManagerServer* is the DNS name or IP address of the host where the Mirage Web Manager is installed.
      - *port* is the port number with which the Horizon FLEX Admin Console can be accessed. When the Mirage Web Manager is installed, if you deploy the Horizon FLEX Admin Console and the Horizon FLEX Policy Server on different ports, *port* is the port number specified for the **VMware Horizon FLEX Web Management** option. Otherwise, *port* is the port number specified for the **VMware Mirage Web Management** option.

   b Enter 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 verify that 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.

You can configure the policy for client virtual machines so that the power-on password matches the user's Active Directory password after first startup. See "Configure a General Policy for a Horizon FLEX Image," on page 46.

Test the Horizon FLEX Admin Console Connection

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

Prerequisites

- Install Mirage for Horizon FLEX. See "Installing and Configuring Mirage Components for the Horizon FLEX Server," on page 14.

- Configure certificate authentication. See Chapter 4, "Setting Up Certificates for Horizon FLEX Virtual Machines," on page 25.

Procedure

1 Start the Horizon FLEX Admin Console.

   a In a Web browser, enter **`https://WebManagerServer:port/rvm`**.

      - *WebManagerServer* is the DNS name or IP address of the host where the Mirage Web Manager is installed.
      - *port* is the port number with which the Horizon FLEX Admin Console can be accessed. When the Mirage Web Manager is installed, if you deploy the Horizon FLEX Admin Console and the Horizon FLEX Policy Server on different ports, *port* is the port number specified for the **VMware Horizon FLEX Web Management** option. Otherwise, *port* is the port number specified for the **VMware Mirage Web Management** option.

   b Enter 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.

Installing the Horizon FLEX Client for End Users

End users must have the Horizon FLEX Client software installed on their local computers before they can download the Horizon FLEX virtual machines. Supported clients included in the Horizon FLEX package are Fusion Pro for macOS and Mac OS X machines and Workstation Player for Windows machines.

You can create a mass deployment to install the Horizon FLEX Client on many systems at one time, or you can instruct end users to obtain the Horizon FLEX Client from the VMware Web site and install it themselves. You can also run an unattended Workstation Player installation on multiple Windows machines.

Create a Mass Deployment Package to Install Fusion Pro

You can create a Fusion Pro 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 the `[Volume License]` section of the `Deploy.ini` file and place a copy of the Fusion Pro application in the `00Fusion_Deployment_Items` folder.

Note Do not enter the license key if you distributed the Horizon FLEX Client license key. See "Distribute the Horizon FLEX Client License Key," on page 62.

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

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

If no virtual machines are 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 host name and user name that you specified in the `connectAtStartupURL` parameter.

You can use the `vmDownloadDir` parameter in the `[Locations]` section of the `Deploy.ini` file to specify the default folder to which Horizon FLEX virtual machines are downloaded, for example:

```
vmDownloadDir = /Users/Shared/FLEX/Virtual Machines
```

If the end user does not redirect the Horizon FLEX virtual machine to a different folder, the virtual machine is downloaded to the folder you specified in the `vmDownloadDir` parameter.

For step-by-step information about creating a mass deployment package, see the VMware knowledge base article at http://kb.vmware.com/kb/2058680.

Provide a Workstation Player Installation Package to End Users

You can install Workstation Player on end user machines using a command line and specify the Horizon FLEX server connection settings by using a uniform resource identifier (URI). When installation of Workstation Player is complete, the end user is prompted to connect to a server and download a Horizon FLEX virtual machine.

Prerequisites

- Give the end user a password for the server and the Workstation Player license key for use with Horizon FLEX.

  NOTE You don't need to provide end users with the license key if you distributed the Horizon FLEX license key. See "Distribute the Horizon FLEX Client License Key," on page 62.

Procedure

- Construct a URI to create a customized Workstation Player installation and deployment package.

  The command line has the following structure:

  ```
  VMware-player-x.x.x-xxxxxxx.exe /v PLAYER_RVM_URI="vmware-rvm://username@myserver.com:7443"
  ```

  Specify the version and build number of the Workstation Player .exe file. *username* is the user's login name and *myserver.com* is the host name of the server. You must include `vmware-rvm://` and `:7443` in the server address. Do not include http or https in the server address.

Run an Unattended Workstation Player Installation

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

Prerequisites

- Verify that the host system meets the host system requirements.
- Verify that the host computer has version 2.0 or later of the MSI runtime engine. This version of the installer is available from Microsoft. See the Microsoft Web site for more information.

Procedure

1. Log in to the host system as the administrator user or as a user who is a member of the local Administrators group.

   If you log in to the domain, the domain account must also be a local administrator.

2. Extract the administrative installation image from the Workstation Player setup file.

   The setup filename is similar to `VMware-player-xxxx-xxxx.exe`, where *xxxx-xxxx* is the version and build number.

   For example: **`setup.exe /s /e install_temp_path`**

3 Enter the installation command on one line.

These examples show options that you can add to the command.

```
VMware-player-full-x.x.x-xxxxxx.exe /s /pass /v "/qn REBOOT=ReallySuppress EULAS_AGREED=1
INSTALLDIR=path_to_program_directory ADDLOCAL=ALL SERIALNUMBER=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx"
```

```
VMware-player-full-x.x.x-xxxxxx.exe /s /v "/qn REBOOT=ReallySuppress EULAS_AGREED=1
SERIALNUMBER=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx"
```

```
VMware-player-full-x.x.x-xxxxxx.exe /s /v "/qn REBOOT=ReallySuppress EULAS_AGREED=1
SERIALNUMBER=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx PLAYER_RVM_URI="vmware-
rvm://username@myserver.com:7443""
```

```
VMware-player-full-x.x.x-xxxxxx.exe /s /v "/qn REBOOT=ReallySuppress EULAS_AGREED=1
SERIALNUMBER=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx RVMDOWNLOADPATH="c:\VMdownloadFolder""
```

You can use the optional `INSTALLDIR` property to specify a file path for the installation that is different from the default location.

Note The quotation marks around the file path are important. All the MSI arguments are passed with the `/v` option. The outer quotation marks group the MSI arguments and the inner quotation marks put a quotation mark in that argument.

You can use the optional `REMOVE` property to skip the installation of certain features.

Workstation Player Unattended Installation Properties

When you perform an unattended installation of Workstation Player, you can customize the installation by specifying installation properties in the installation command.

To specify an installation property in the installation command, use the format `Property` property= "*value*". A value of 1 means true and a value of 0 means false.

Table 2-1. Installation Properties

Property	Description	Default Value
`AUTOSOFTWAREUPDATE`	Enables automatic upgrades for Workstation Player when a new build becomes available.	1
`DATACOLLECTION`	Sends user experience information to VMware.	1
`DESKTOP SHORTCUT`	Adds a shortcut on the desktop when Workstation Player is installed.	1
`ENABLE_VIRTUAL_PRINTING`	Enables support for ThinPrint virtual printing on the Windows host after installing.	0
`EULAS_AGREED`	Allows you to silently accept the product EULA's. Set to 1 to complete the installation or upgrade.	0
`INSTALL_DIR`	Install Workstation Player in a directory that is different from the default Workstation Player location.	C:\Program Files (86)\VMware\VMware Player
`KEEP_LICENSE`	Specifies whether to keep or remove license keys when Workstation Player is uninstalled.	1
`KEEP_SETTINGFILES`	Specifies whether to keep or remove settings files when Workstation Player is uninstalled.	1

Table 2-1. Installation Properties (Continued)

Property	Description	Default Value
PLAYER_RVM_URI	Specifies the uniform resource identifier (URI) for the Horizon FLEX server.	VMware-player-full-x.x.x-xxxxxx.exe /s /v/qn PLAYER_RVM_URI="vmware-rvm://username@myserver.com:7443"
REBOOT	Prevents host from rebooting after Workstation Player is installed.	VMware-player-full-x.x.x-xxxxxx.exe /s /v /qn REBOOT=ReallySuppress
RVMDOWNLOADPATH	Sets the default folder to which Horizon FLEX virtual machines are downloaded.	VMware-player-full-x.x.x-xxxxxx.exe /s /v "/qn RVMDOWNLOADPATH="c:\VMdownloadFolder""
SERIALNUMBER	Lets you enter the license key when Workstation Player is installed. Enter the license key with hyphens, for example "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx".	
SIMPLIFIEDUI	Turn on or off certain UI features of Workstation Player.	0
SOFTWAREUPDATEURL	Specifies a custom URL for managing software updates (separate from vmware.com).	
STARTMENU_SHORTCUT	Adds a **Start** menu item when Workstation Player is installed.	1
SUPPORTURL	Set a support URL or email alias specifically for your users to contact with product issues through the Workstation Player **Help** menu.	

Setting up Certificates for the Horizon FLEX Server

3

You need to set up certificates for the Horizon FLEX server so the certificates can be used to authenticate the Horizon FLEX virtual machines.

You must configure the IIS SSL server certificate for the Horizon FLEX server to ensure secure communication between the Horizon FLEX client and the Horizon FLEX server. The IIS SSL server certificate ensures that certificate authentication can proceed in the Horizon FLEX virtual machine.

VMware recommends that you use a certificate issued by a certificate authority (CA), such as Entrust or Go Daddy, or a trusted 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 should take steps to ensure that the certificate is trusted on all end-user computers that will download and use Horizon FLEX virtual machines.

This chapter includes the following topics:

Configure the IIS SSL Server Certificate for the Horizon FLEX Server

You must configure the IIS SSL server certificate for the Horizon FLEX server to ensure secure communication between the Horizon FLEX client and the Horizon FLEX server.

Note If setting up certificates for Horizon FLEX virtual machines, make sure the Horizon FLEX server IIS SSL server certificate is included in the certificate list.

Prerequisites

- Install Mirage for Horizon FLEX. See "Installing and Configuring Mirage Components for the Horizon FLEX Server," on page 14.
- Install the Server SSL Certificate on the Mirage server. See the Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html

Procedure

1 Open IIS Manager.

2 Navigate to the root node, the connection node defined for the Mirage server.

3 On the Mirage Home page under IIS, double click **Server Certificates**.

The IIS SSL server certificates window opens.

4 Click **Import** in the right column.

This step imports the created SSL certificate and assigns a key to identify the certificate.

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**.

Set Up a Certificate for the Horizon FLEX Server by Using OpenSSL

You can create a self-signed certificate for the Horizon FLEX server by using OpenSSL.

Note If the certificate is commercially issued by a trusted root certificate authority or intermediate certificate authority, this task is not required.

Prerequisites

The OpenSSL configuration file is created on the Mirage Gateway Server. See the Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html.

Procedure

1 At the OpenSSL command prompt, create a certificate:
$ openssl req –new –days *expiration time* –x509 –newkey rsa:2048 – keyout *key filename* – out*certificate filename* –nodes

expiration time represents the number of days that the certificate should be valid, *key filename* represents the filename for the key, and *certificate filename* represents the new certificate name.

A self-signed certificate and a private key are generated. The certificate uses a 2048-bit RSA key and does not protect the key with a passphrase.

2 When prompted, enter the country name, state name, locality, organization name, and organizational unit name.

3 In the Common Name text box, enter the host name of the Horizon FLEX server to be protected.

This text box must be completed.

4 Enter the email address.

The self-signed certificate and associated private key are generated.

5 If the private key must be in `.pfx` format , enter the following command by using the certificate name and key filename generated in the previous steps:
$ openSSL pkcs12 –export –out*output pfx filename* –inkey *key filename* –in *certificate name*

A new password-protected `.pfx` file is generated that can be deployed on any device that requires `.pfx` certificates instead of PEM certificates.

Configure the System Certificate Store for the Horizon FLEX Server

You must configure the system certificate store for the Horizon FLEX server to store the certificates used for the Horizon FLEX virtual machines.

Note If the certificate is commercially issued by a trusted root certificate authority or intermediate certificate authority, this task is not required.

Prerequisites

- Install Mirage for Horizon FLEX. See "Installing and Configuring Mirage Components for the Horizon FLEX Server," on page 14.

Procedure

1 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.

2 Select **File > Add/Remove Snap-in**.

3 Click the **Certificates** snap-in and click **Add**.

4 On **Certificates snap-in display**, select **Computer account** and click **Next**.

The Horizon FLEX server requires this setting.

5 Select **Local Computer**, click **Finish**, and click **OK**.

6 In the left navigation pane, expand **Certificates (Local Computer)**.

7 Right-click **Trusted Root Certification Authorities** and select **All Tasks > Import**.

8 Click **Next**.

9 Browse for the root certificate file and click **Next**.

10 Select **Place all certificates in the following store: Trusted Root Certification Authorities** , click **Next**, and click **Finish**.

11 Right-click **Intermediate Certification Authorities** and select **All Tasks > Import** .

The **Certificate Import Wizard** opens.

12 Browse for the root certificate file and click **Next**.

13 Select **Place all certificates in the following store: Intermediate Certification Authorities**, click **Next**, and click **Finish**.

14 Repeat steps 12 and 13 for each intermediate certificate to be installed.

What to do next

Test the trusted certificate by manually installing it on the endpoint. If an end user accessing the Horizon FLEX server receives a prompt to allow an untrusted certificate, then the certificate is not trusted. If the end user does not receive the prompt, the certificate is trusted and can be used. Add the trusted certificates in the source virtual machine. See "Create a Source Virtual Machine in Fusion Pro," on page 38 or "Create a Source Virtual Machine in Workstation Pro (Not included in Horizon FLEX)," on page 40.

Updating Trusted Certificates on the Horizon FLEX Server

You need to update trusted certificates before they expire to ensure continued client access to the Horizon FLEX server.

Note Starting with Horizon FLEX 1.10, you cannot change a Horizon FLEX server root CA signed certificate to a self-signed certificate. The Horizon FLEX Client detects that the certificate on the server changed from a root CA signed certificate to a self-signed certificate. The client then terminates the connection attempt to the server.

Horizon FLEX supports a server certificate change of the following types.

From	To
self-signed certificate	self-signed certificate
self-signed certificate	root CA signed certificate
root CA signed certificate	root CA signed certificate

Before a certificate expires, 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 certificate list.

To import, export or delete certificates in the Horizon FLEX Admin Console, click the **General Systems Settings** icon and select **Certificates**.

Caution When updating certificates, verify that the updated certificates are valid before propagating them to the virtual machine instances using a policy update. If you install an invalid certificate on the Horizon FLEX Admin Console, virtual machines with embedded certificates inherit the invalid certificate. As a result, these virtual machines will be unable to connect to the Horizon FLEX server.

When updating certificates, you should follow these guidelines:

- Update certificates before the existing ones expire.
- The certificate imported onto the Horizon FLEX server should be the root certificate, not a leaf certificate. However, if importing self-signed certificates, then you should import the self-signed certificate directly.
- Add the new certificate from the Horizon FLEX Admin Console. Make sure that the trusted certificate list, including the old certificates and the new certificates, can be synchronized to the clients. See "Configure the System Certificate Store for the Horizon FLEX Server," on page 22.

  Both the old and new certificates are now available in the virtual machine policy. If the Horizon FLEX server deploys both certificates, the client should continue to maintain access to the server.
- After the new certificate is added to the virtual machine policy, change the server from IIS Manager to bind the new certificate to the Mirage Management Web Site. For more information, see "Configure the IIS SSL Server Certificate for the Horizon FLEX Server," on page 21.

  After the new certificate binds to the Mirage Management Web site, the client can continue accessing the server .

Setting Up Certificates for Horizon FLEX Virtual Machines

4

Before you create Horizon FLEX virtual machines, make sure certificates are properly configured to ensure that end users can successfully download and use their virtual machines.

The following guidelines apply to ensure security and to enable end user clients to access the Horizon FLEX server:

- VMware recommends that you use a certificate issued by a certificate authority (CA), such as Entrust or Go Daddy, or a trusted third-party certificate, on your Horizon FLEX server. If using a self-signed certificate or a certificate from an internal CA instead of a generally trusted certificate, you should ensure that the certificate is trusted on all end-user computers that will download and use Horizon FLEX virtual machines.
- While not required, creating a trusted certificates list in a source virtual machine enables certificate authorization with increased security on the end client host.
- Using self-signed or internal CA signed certificates might be less secure than using trusted certificates. If the certificate chain that verifies the secure connection to the Horizon FLEX server cannot be processed on the client's host, the client user receives the `Invalid Security Certificate` message. The client user must then select the **Always Trust this host** checkbox and click **Connect Anyway** when first connecting to the Horizon FLEX server. Allowing client users to select this option provides reduced security than other authorization methods.

  However, if you embed a self-signed or internal CA signed certificate into the source virtual machine, then you have total control of certificate flow, ensuring greater security.

For information about setting up certificates in Mirage for the Horizon FLEX Server, see the Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html.

- Creating a Trusted Certificates List in a Source Virtual Machine on page 26

  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.

- Importing Certificates onto the Horizon FLEX Client Host on page 28

  You should import certain types of certificates onto the client host if they are not stored on the Horizon FLEX Policy Server or configured on the source virtual machine.

Creating a Trusted Certificates List in a Source Virtual Machine

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 client host ignores the host's list of certificates and uses the trusted certificates list to verify server connections instead. If the client host 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, Workstation Player 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 on page 26

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

- Creating PEM-Format Certificates on page 27

  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.

- Create and Import the Trusted Certificates List File on page 28

  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.

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-----
MIIDojCCAwugAwIBAgIJAMLM0CJRzPyzMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJUGFsbyBBbHRv
MS8wLQYDVQQKEyZWTXdhcmUsIEluYy4gLSBXb3Jrc3RhdGlvbiBTU0wgVGVzdGlu
ZzEqMCgGA1UEAxMhV29ya3N0YXRpb24gQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTExMDcxNTAyMjY0OFoXDTE1MDcxNDAyMjY0OFowgZMxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYDVQQHEwlQYWxvIEFsdG8xLzAtBgNVBAoT
JlZNd2FyZSwgSW5jLiAtIFdvcmtzdGF0aW9uIFNTTCBUZXN0aW5nMSowKAYDVQQD
EyFXb3Jrc3RhdGlvbiBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAL/tBlngiEkCK7ssCBe8lZ30FlIHmpECmwEm3AaID1C0
lncb+LdRt2AmmQiknXBPxGBGyRNRNnashrzp1XXR/wL2b2AybT7NX+P/XSH2srDb
cGGCTNa/bwh/ArcirTLCjRwY55lAAH9xwzortRYR84IBJQpHzxcopTSI9o4ZVIqx
AgMBAAGjgfswgfgwHQYDVR0OBBYEFMoT527dtvlgR1EzYK4EnQHS6T2ZMIHIBgNV
HSMEgcAwgb2AFMoT527dtvlgR1EzYK4EnQHS6T2ZoYGZpIGWMIGTMQswCQYDVQQG
EwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJUGFsbyBBbHRvMS8w
LQYDVQQKEyZWTXdhcmUsIEluYy4gLSBXb3Jrc3RhdGlvbiBTU0wgVGVzdGluZzEq
MCgGA1UEAxMhV29ya3N0YXRpb24gQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggkAwszQ
```

```
IlHM/LMwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQBcoiwDWGWXzI+j
0gG/7BNzpNHzR1RGAF4nB9JrnCYWvB313kgYDMHogfiAoQchsu/py/OYBYVRjjFJ
YVaTJ7DVl/3Gpk3+tcdJfEmqIz76PVWfWbTnhuJEMYrMM4W06B/K2cs24bkZtcXQ
h8b4FYTVCg/l6TP5SWgei4VWgRfxgA==
-----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-----
<base64 content here>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<base64 content here>
-----END CERTIFICATE-----
```

Creating 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

1 On the Mac, open Keychain Access.

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

1 On the Windows system, open Certificate Manager (`certmgr.exe`).

2 Right-click the certificate to export and select **All Tasks > Export**.

3 Select options in the Certificate Export Wizard.

   a 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.

   b Provide a location to save the certificate and a file name.

   c 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 "Creating PEM-Format Certificates," on page 27.

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 Start the Horizon FLEX Admin Console.

   a In a Web browser, enter **`https://WebManagerServer:port/rvm`**.

   - *WebManagerServer* is the DNS name or IP address of the host where the Mirage Web Manager is installed.
   - *port* is the port number with which the Horizon FLEX Admin Console can be accessed. When the Mirage Web Manager is installed, if you deploy the Horizon FLEX Admin Console and the Horizon FLEX Policy Server on different ports, *port* is the port number specified for the **VMware Horizon FLEX Web Management** option. Otherwise, *port* is the port number specified for the **VMware Mirage Web Management** option.

   b Enter 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.

Importing Certificates onto the Horizon FLEX Client Host

You should import certain types of certificates onto the client host if they are not stored on the Horizon FLEX Policy Server or configured on the source virtual machine.

Note If the certificate is not imported on the Horizon FLEX client host, then the client user must select the **Always Trust this host** checkbox option when first connecting to the Horizon FLEX server. Even if a self-signed root certificate has been imported into the client's certificate store, the security warning might still display when first connecting to the Horizon FLEX server. In this case, the client user must select the **Always Trust this host** checkbox for the Horizon FLEX to work properly.

- Importing Self-Signed Certificates on page 29

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

- Importing Internal CA Certificates on page 31

  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 should import the root CA certificate on each end-user host for Horizon FLEX virtual machines to function correctly.

Importing Self-Signed Certificates

If you do not configure the self-signed certificate into the source virtual machine being prepared, you should import 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, Workstation Player 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 38 or "Create a Source Virtual Machine in Workstation Pro (Not included in Horizon FLEX)," on page 40.

For information about creating a trusted certificates list and importing it to the Horizon FLEX Policy Server, see "Creating a Trusted Certificates List in a Source Virtual Machine," on page 26.

For information about updating certificates, see "Updating Trusted Certificates on the Horizon FLEX Server," on page 24.

Import a Self-Signed Certificate on a Windows Host

To import 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.
- Install Windows IIS.

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 Select **File > Add/Remove Snap-in**.

   c Click the **Certificates** snap-in and click **Add**.

   d On the **Certificates snap-in display**, select **Computer account** and click **Next**.

   This setting is required by the Horizon FLEX server.

   e Select **Local Computer** and click **Finish** and then **OK**.

   f In the left navigation pane, expand **Certificates (Local Computer)**.

g Right-click on **Trusted Root Certification Authorities** and select **All Tasks > Import**.

The Certificate Import Wizard opens.

h Click **Next**.

i Browse for the root certificate file and click **Next**.

j Select **Place all certificates in the following store: Trusted Root Certification Authorities** and click **Next**, then click **Finish**.

k Navigate to **Trusted Root Certification Authorities > Certificates**.

l 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 client Windows computer.

3 Import the self-signed certificate to the client 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.

Import a Self-Signed Certificate on a Mac Host

To import 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.
- Become familiar with how to use Keychain Access on a Mac. For more information, go to the Apple Support Web site at http://support.apple.com.
- Install Windows IIS.

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 Select **File > Add/Remove Snap-in**.

c Click the **Certificates** snap-in and click **Add**.

d On the **Certificates snap-in display**, select **Computer account** and click **Next**.

This setting is required by the Horizon FLEX server.

e Select **Local Computer** and click **Finish** and then **OK**.

f In the left navigation pane, expand **Certificates (Local Computer)**.

g Right-click on **Trusted Root Certification Authorities** and select **All Tasks > Import**.

The Certificate Import Wizard opens.

h Click **Next**.

i Browse for the root certificate file and click **Next**.

j Select **Place all certificates in the following store: Trusted Root Certification Authorities** and click **Next**, then click **Finish**.

k Navigate to **Trusted Root Certification Authorities > Certificates**.

l 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 (vmware-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**.

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

Importing 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 should import 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, Workstation Player 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 38 or "Create a Source Virtual Machine in Workstation Pro (Not included in Horizon FLEX)," on page 40.

For information about creating a trusted certificates list and importing it to the Horizon FLEX Policy Server, see "Creating a Trusted Certificates List in a Source Virtual Machine," on page 26.

For information about updating certificates, see "Updating Trusted Certificates on the Horizon FLEX Server," on page 24.

Import an Internal Root CA Certificate on a Windows Host

To import 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.
- Obtain and install an internal CA certificate. You can use the Windows MMC Certificates snap-in to request a certificate.
- Install Windows IIS.

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 Select **File > Add/Remove Snap-in**.

   c Click the **Certificates** snap-in and click **Add**.

   d On the **Certificates snap-in display**, select **Computer account** and click **Next**.

   This setting is required by the Horizon FLEX server.

   e Select **Local Computer** and click **Finish** and then **OK**.

   f In the left navigation pane, expand **Certificates (Local Computer)**.

   g Right-click on **Trusted Root Certification Authorities** and select **All Tasks > Import**.

   The Certificate Import Wizard opens.

   h Click **Next**.

   i Browse for the root certificate file and click **Next**.

   j Select **Place all certificates in the following store: Trusted Root Certification Authorities** and click **Next**, then click **Finish**.

   k Navigate to **Trusted Root Certification Authorities > Certificates**.

   l 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.

Import an Internal Root CA Certificate on a Mac Host

To import 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.
- Become familiar with how to use Keychain Access on a Mac. For more information, go to the Apple Support Web site at http://support.apple.com.
- Install Windows IIS.

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 Select **File > Add/Remove Snap-in**.

   c Click the **Certificates** snap-in and click **Add**.

   d On the **Certificates snap-in display**, select **Computer account** and click **Next**.

   This setting is required by the Horizon FLEX server.

   e Select **Local Computer** and click **Finish** and then **OK**.

   f In the left navigation pane, expand **Certificates (Local Computer)**.

   g Right-click on **Trusted Root Certification Authorities** and select **All Tasks > Import**.

   The Certificate Import Wizard opens.

   h Click **Next**.

   i Browse for the root certificate file and click **Next**.

   j Select **Place all certificates in the following store: Trusted Root Certification Authorities** and click **Next**, then click **Finish**.

   k Navigate to **Trusted Root Certification Authorities > Certificates**.

   l 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**.

Creating and Deploying Horizon FLEX Virtual Machines

5

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 for the virtual machine to function correctly with Horizon FLEX.

You can use Fusion Pro or Workstation Pro (not included in the Horizon FLEX package) to create a source virtual machine.

This chapter includes the following topics:

Horizon FLEX Virtual Machine Deployment Overview

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

1 Plan the virtual machine deployment.

See "Considerations for Creating Horizon FLEX Virtual Machines," on page 36.

2 Create and configure a source virtual machine.

See "Create a Source Virtual Machine in Fusion Pro," on page 38 or "Create a Source Virtual Machine in Workstation Pro (Not included in Horizon FLEX)," on page 40.

3 (Optional) Prepare the source virtual machine to join an Active Directory domain.

See "Prepare a Source Virtual Machine to Join an Active Directory Domain," on page 43.

4 Compress the source virtual machine package and save it in your download directory.

See "Compress a Source Virtual Machine Package," on page 44.

5 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 44.

6 Create a policy for the Horizon FLEX image and entitle the image to your Active Directory users and groups.

See "Creating Policies and Entitlements," on page 46.

7 (Optional) Create a URI to deploy the Horizon FLEX virtual machine.

See "Create a URI to Deploy a Horizon FLEX Virtual Machine," on page 56.

Considerations for Creating Horizon FLEX Virtual Machines

When you create Horizon FLEX virtual machines, you must consider the requirements of the client end users.

Horizon FLEX virtual machines are restricted virtual machines, meaning that not all functions are available to your client end users. By using policies and entitlements, you can control the features available to client end users. See "Creating Policies and Entitlements," on page 46. Note that client end users can create their own non-Horizon FLEX virtual machines by using the Horizon FLEX client software.

Horizon FLEX Server and Client Compatibility

If you use different versions of the Horizon FLEX server and the Horizon FLEX client, the server and client might become unsynchronized. The following considerations apply to Horizon FLEX server and client compatibility:

- A client with an earlier Horizon FLEX client version cannot download a virtual machine from the current Horizon FLEX server version. The client is also unable to power on an existing virtual machine in online mode. The client user receives an error message that the client version needs to be upgraded.

  For example, a client using a Horizon FLEX 1.6 client version cannot download a virtual machine from a Horizon FLEX 1.7 server.

- The current Horizon FLEX client version can work with an earlier Horizon FLEX server version, but the new features of the current server version are not available .

  For example, a client using Horizon FLEX 1.7 can work with a Horizon FLEX 1.6 server. However, any new features in Horizon FLEX 1.7 are not available to an administrator that uses the Horizon FLEX 1.6 server.

- To prevent compatibility issues, when you upgrade the Horizon FLEX server version, upgrade the client version first. If you upgrade the server before the clients, the clients may not be able to connect to the server until they are upgraded.

Horizon FLEX Virtual Machine Hardware Compatibility

Hardware version incompatibility can prevent client users from opening Horizon FLEX virtual machines. A client running an earlier Horizon FLEX version that does not support later hardware versions cannot open a virtual machine running a higher hardware version.

For example, if a hardware version 12 virtual machine is created by using a Horizon FLEX 1.7 client , a Horizon FLEX 1.5 client cannot open the virtual machine. Because the Horizon FLEX 1.5 client only supports up to hardware version 11, the client cannot open or power on a hardware version 12 virtual machine.

Virtual Processor and Memory Requirements

When you create source virtual machines, Horizon FLEX assumes that the end user host has the same hardware resources as the system you are using. By default, the number of virtual processors and memory size of a Horizon FLEX virtual machine are optimized to fit the end client's host operating system. This setting ensures that the virtual machine is not oversubscribed on the client end user host. For more information, see "Optimizing Virtual Processors and Memory for Horizon FLEX Virtual Machines," on page 37.

If you disable virtual processor and memory size optimization, Horizon FLEX virtual machines must meet the following requirements:

- The number of virtual processor cores cannot exceed the maximum number of logical CPUs supported by the guest operating system.
- The number of sockets cannot exceed the maximum number of sockets that the guest operating system supports. If you create the source virtual machine by using Fusion Pro, you cannot specify the number of sockets.
- The memory size cannot be lower than the minimum memory size that the guest operating system requires.
- When you use Fusion Pro or Workstation Pro software, the total number of virtual processors cannot exceed the maximum number of virtual processors that Fusion Pro or Workstation Pro supports for the specific guest operating system.

  In the Workstation Pro user interface, the virtual processors and sockets of a virtual machine have the following user interface settings:

  - "Number of processors" indicates the number of (virtual) CPUs, which equals the number of (virtual) sockets.
  - "Number of cores per processor" indicates the virtual processor cores per processor.
  - "Total processor cores" indicates the number of sockets times the number of cores per socket.

  In the Fusion Pro user interface, "Processors" indicates the number of sockets times the number of cores per socket.

  On the host operating system the number of logical CPUs or logical processors is the total number of physical CPUs or sockets times the number of physical cores per CPU, times the number of hyper-threading per physical cores.

Optimizing Virtual Processors and Memory for Horizon FLEX Virtual Machines

You can set the policy for a Horizon FLEX image to automatically optimize the virtual machine's virtual processors and memory to fit the client host operating system.

When creating Horizon FLEX virtual machines, you might not know the CPU and memory constraints of the client end user's host operating system. If the number of CPUs and memory size of the Horizon FLEX virtual machine are too large for the user's host operating system, the virtual machine cannot open. In this case, the client end user's host operating system is oversubscribed.

By default, the number of virtual processors and memory size of a Horizon FLEX virtual machine are optimized to fit the end client's host operating system. You can enable or disable the Horizon FLEX virtual machine optimization by using the **Optimize CPU** and **Optimize memory** policy settings. See "Configure a General Policy for a Horizon FLEX Image," on page 46. If you disable virtual machine optimization, the Horizon FLEX virtual machine must meet certain requirements. See "Considerations for Creating Horizon FLEX Virtual Machines," on page 36.

Virtual machine optimization is enabled by default if a current Horizon FLEX client connects to an older Horizon FLEX server version that does not support optimization.

The number of virtual processor cores allocated to a virtual machine is limited to no more than 50 percent of cores on the host. The memory size for a virtual machine is limited by the reserved memory size for all running virtual machines on the host. The limit is approximately 75 percent of the host memory, depending on the platform.

Example: Virtual Processor Optimization

The following examples show how virtual processors for Horizon FLEX virtual machines are optimized by using the **Optimize CPU** policy setting.

Table 5-1. Virtual Processor Optimization Examples

Example	Horizon FLEX Virtual Machine	Client Host	Optimization Result
Example 1	12 sockets with 1 core per socket = 12 cores	8 cores	Virtual machine has 4 cores (4 sockets * 1 core per socket = 4 cores).
Example 2	4 sockets with 2 cores per socket = 8 cores	12 cores	Virtual machine has 4 cores (4 sockets * 1 core per socket = 4 cores). **Note** The number of cores is always reduced to the maximum number that can be divided by the number of sockets.
Example 3	1 socket with 2 cores per socket = 2 cores	8 cores	Virtual machine has 2 cores.

Example: Memory Optimization

The following examples show how memory for Horizon FLEX virtual machines is optimized by using the **Optimize memory** policy setting.

Table 5-2. Memory Optimization Examples

Example	Horizon FLEX Virtual Machine	Client Host	Optimization Result
Example 1	10 GB of memory allocated	12 GB of reserved memory	Horizon FLEX virtual machine is allowed the full 10-GB memory allocation.
Example 2	10 GB of memory allocated	2 GB of reserved memory	Horizon FLEX virtual machine is automatically scaled down to 2 GB of memory.

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.

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

If you enable USB device use, drag and drop, and copy and paste features 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.

Horizon FLEX only supports virtual machine names using English characters. Do not use non-ASCII characters in .vmx or .tar filenames. Fusion Pro cannot create Horizon FLEX virtual machines in Japanese or Simplified Chinese.

Note When preparing a Horizon FLEX virtual machine, make sure that the .vmx policy file is in the same folder as all virtual machine disk (.vmdk) files. If the .vmx file and the virtual machine disk files are in different directories on the client user's machine, then the user will receive an error message when attempting to start the Horizon FLEX virtual machine.

Prerequisites

- Become familiar with how to create a virtual machine in Fusion Pro. See the Fusion documentation at https://docs.vmware.com/en/VMware-Fusion/index.html.
- Become familiar with the supported guest operating systems for Horizon FLEX virtual machines. See "Supported Host and Guest Operating Systems," on page 12.
- Install Fusion Pro with a Horizon FLEX license key .
- If you add certificates to the virtual machine, the trusted certificate must be installed on the Horizon FLEX server or on your local host. See "Configure the System Certificate Store for the Horizon FLEX Server," on page 22.

Procedure

1 Open Fusion Pro and create a virtual machine.

  Select a guest operating system that is supported for Horizon FLEX virtual machines. When the virtual machine is created, Fusion Pro tries to install VMware Tools. VMware Tools is not required, but is recommended. Configure the virtual machine for distribution to your end users.

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

3 Select **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.

  You must retain the encryption password. You cannot access the virtual machine without this password.

4 Check **Enable Restrictions** and set a password for editing the restrictions on the virtual machine.

  This password should be different from the virtual machine encryption password.

  You must 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 Enter 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, choose one of the following:

- To add the trusted root certificate directly from the Horizon FLEX server, click **Get Server Certificate**.

  A dialog box with the full certificate chain retrieved from the Horizon FLEX server appears. Click **OK**.

- To add the certificates from the local host, 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. Do not add the certificate into the virtual machine until you have tested and confirmed that the Horizon FLEX Client can use the certificate to communicate to the server.

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 an Active Directory Domain," on page 43.

To install the Mirage client in the source virtual machine, see "Install the Mirage Client In a Source Virtual Machine," on page 42.

Create a Source Virtual Machine in Workstation Pro (Not included in Horizon FLEX)

You can use Workstation Pro to create a source virtual machine for a Horizon FLEX virtual machine. Workstation Pro is not included in the Horizon FLEX package. A Horizon FLEX license key for Workstation Pro is not required.

Horizon FLEX only supports virtual machine names using English characters. Do not use non-ASCII characters in .vmx or .tar filenames.

Note When preparing a Horizon FLEX virtual machine, make sure that the .vmx policy file is in the same folder as all virtual machine disk (.vmdk) files. If the .vmx file and the virtual machine disk files are in different directories on the client user's machine, then the user will receive an error message when attempting to start the Horizon FLEX virtual machine.

Prerequisites

- Review how to create a virtual machine in Workstation Pro. See the Workstation Pro documentation at https://docs.vmware.com/en/VMware-Workstation-Pro/index.html
- Review the supported guest operating systems for Horizon FLEX virtual machines. See "Supported Host and Guest Operating Systems," on page 12.
- Install Workstation Pro.
- If adding certificates to the virtual machine, the trusted certificate must be installed on the Horizon FLEX server or on your local host. See "Configure the System Certificate Store for the Horizon FLEX Server," on page 22.

Procedure

1 Open Workstation Pro and create a virtual machine.

2 Install the guest OS.

Select a guest operating system that is supported for Horizon FLEX virtual machines. Configure the virtual machine for distribution to your end users.

3 (Optional) Install VMware Tools in the virtual machine.

VMware Tools is not required but is recommended.

4 Encrypt and restrict the virtual machine. Select the virtual machine and select **VM > Settings**.

5 On the **Options** tab, select **Access Control**.

6 Click **Encrypt**, type an encryption password, and click **Encrypt**.

The encryption password is required to gain access to the virtual machine. It does not prevent the user from changing the virtual machine configuration. Turn on restrictions and enter a password to prevent the user from changing the virtual machine configuration.

Important Record the encryption password you use. If you forget the password, Workstation does not provide a way to retrieve it.

Workstation Pro begins encrypting the virtual machine. After the encryption process is complete, you can set a restrictions password.

7 Select the **Enable Restrictions** check box and set a password for editing the restrictions on the virtual machine.

Set a different password from the virtual machine encryption password.

You must retain the restrictions password. You cannot edit the restrictions on the virtual machine without this password.

8 Set the **Restriction Type** to **Managed**.

You must set the restriction type to **Managed** to distribute and use the virtual machine with Horizon FLEX.

9 Enter the URL of the Horizon FLEX server on which you intend to host the virtual machine in the **Restrictions Management Server** text box.

10 Click **Check Server** to verify the Horizon FLEX server URL.

11 (Optional) To add trusted certificates to the virtual machine, click the **Manage Certificates** icon and choose one of the following:

- To add the trusted root certificate directly from the Horizon FLEX server, select **Add > From server**. Select the certificate and click **OK**.

  A dialog box with the full certificate chain retrieved from the Horizon FLEX server appears. Click **OK**.

- To add the certificate from the local host, click **Add > From file** 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. Do not add the certificate into the virtual machine until you have tested and confirmed that the Horizon FLEX Client can use the certificate to communicate to the server.

12 Click **OK**.

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 an Active Directory Domain," on page 43.

To install the Mirage client in the source virtual machine, see "Install the Mirage Client In a Source Virtual Machine," on page 42.

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.

Note When configuring the Mirage server for disaster recovery, make sure the MongoDB ports are configured correctly. For more information, see the *VMware Mirage Installation Guide*.

Prerequisites

- Create the source virtual machine. See "Create a Source Virtual Machine in Fusion Pro," on page 38 or "Create a Source Virtual Machine in Workstation Pro (Not included in Horizon FLEX)," on page 40.
- Obtain the *VMware Mirage Installation Guide* for Mirage client installation instructions.

Procedure

1. In Fusion Pro or Workstation 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 in the source virtual machine.

   See the *VMware Mirage Installation Guide* for more information.
4. In the Mirage Management Console, verify that the endpoint appears as Pending Assignment.

   Note Do not delete this Pending record as long as you are distributing this source virtual machine.
5. In the Mirage Management Console, enable automatic CVD creation.
   a. Right-click **System Configuration** and select **Settings**.
   b. Click the **CVD Auto Creation** tab.

c Select **Enable automatic CVD creation**.

You can change the user message as needed.

d Click **OK**.

6 Power off the source virtual machine in Mirage while it is in Pending Assigning state.

Do not provide the username and password, and do not register the source virtual machine at the Mirage client prompt. If you do register the source virtual machine with Mirage, the Horizon FLEX virtual machine will be duplicated when the end user accesses it.

Once the Mirage client is active, when you create a new Horizon FLEX entitlement for this source virtual machine, Mirage controls for that virtual machine are available. See "Entitle a Horizon FLEX Image," on page 53.

Prepare a Source Virtual Machine to Join an Active Directory 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 38 or "Create a Source Virtual Machine in Workstation Pro (Not included in Horizon FLEX)," on page 40.

  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.
- In the Horizon FLEX Admin Console, edit the entitlement to enable the **Use machine name configuration** option, allowing the virtual machine to join the Active Directory domain. The Horizon FLEX administrator account must have permission to create objects in the Active Directory.
- If using an RODC, it must be installed in the DMZ.
- Configure the Active Directory to support the domain join.

Procedure

1 In Fusion Pro or Workstation 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 that are required to run a virtual machine.

Prerequisites

- Create the source virtual machine. See "Create a Source Virtual Machine in Fusion Pro," on page 38 or "Create a Source Virtual Machine in Workstation Pro (Not included in Horizon FLEX)," on page 40.
- 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 "Configure the IIS SSL Server Certificate for the Horizon FLEX Server," on page 21.

Procedure

1 If the source virtual machine is running, shut it down.

2 In Fusion Pro or Workstation Pro, navigate to the source virtual machine.

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

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 44.

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

- Compress the source virtual machine files in a TAR (`.tar`) archive file. See "Compress a Source Virtual Machine Package," on page 44.
- 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 "Configure the IIS SSL Server Certificate for the Horizon FLEX Server," on page 21.
- Verify that restrictions are already set in the source virtual machine's configuration (`.vmx`) file. If you select a virtual machine that 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 38.

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 Start the Horizon FLEX Admin Console.

   a In a Web browser, enter **`https://`*`WebManagerServer`*`:`*`port`*`/rvm`**.

      - *WebManagerServer* is the DNS name or IP address of the host where the Mirage Web Manager is installed.
      - *port* is the port number with which the Horizon FLEX Admin Console can be accessed. When the Mirage Web Manager is installed, if you deploy the Horizon FLEX Admin Console and the Horizon FLEX Policy Server on different ports, *port* is the port number specified for the **VMware Horizon FLEX Web Management** option. Otherwise, *port* is the port number specified for the **VMware Mirage Web Management** option.

   b Enter 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 `http://`*`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. The URL can start with either http or https.

   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 General Policy for a Horizon FLEX Image," on page 46.

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 so that specific users and groups can 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 that are 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 virtual machine instance is created, the policies associated with entitlements determine the instance's initial restrictions. When you change a policy, the policy change applies to all virtual machine instances assigned to the entitlement. You cannot change the restrictions for a particular virtual machine instance by changing the policy. To change the restrictions for a particular virtual machine instance, you need to create an entitlement for that virtual machine and assign a new policy to that entitlement. You can also change policy for a virtual machine by creating a new policy and assigning it to the virtual machine instance. In this case, creating an entitlement is not required.

Configure a General Policy for a Horizon FLEX Image

You configure general policies to set an expiration date and control the features in virtual machine instances created from a Horizon FLEX image.

Important If the copy-and-paste and drag-and-drop settings 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 Start the Horizon FLEX Admin Console.

   a In a Web browser, enter **`https://WebManagerServer:port/rvm`**.

      - *WebManagerServer* is the DNS name or IP address of the host where the Mirage Web Manager is installed.
      - *port* is the port number with which the Horizon FLEX Admin Console can be accessed. When the Mirage Web Manager is installed, if you deploy the Horizon FLEX Admin Console and the Horizon FLEX Policy Server on different ports, *port* is the port number specified for the **VMware Horizon FLEX Web Management** option. Otherwise, *port* is the port number specified for the **VMware Mirage Web Management** option.

   b Enter 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 create a policy, or select an existing policy and click **Change Policy** to modify it.

4 On the General tab, 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.

Option	Action	
Expiration date	Use the calendar widget to set an expiration date for the virtual machine.	
Copy and Paste operations	This policy controls copy-and-paste operations between the virtual machine guest and host. It does not control copy-and-paste operations in the virtual machine.	
	Allow	Users can perform copy and paste operations from the host to the guest and from the guest to the host.
	Host to Guest	Users can perform copy and paste operations from the host to the guest only.
	Guest to Host	Users can perform copy and paste operations from the guest to the host only.
	Block	Copy and paste operations are disabled. Users cannot perform copy and paste operations from the host to the guest or from the guest to the host.
	Note These policy changes might not occur until users power cycle their virtual machines	

Option	Action	
Drag and Drop operations	This policy controls drag-and-drop operations between the virtual machine guest and host. It does not control drag-and-drop operations in the virtual machine.	
	Allow	Users can perform drag and drop operations from the host to the guest and from the guest to the host.
	Host to Guest	Users can perform drag and drop operations from the host to the guest only.
	Guest to Host	Users can perform drag and drop operations from the guest to the host only.
	Block	Drag and drop operations are disabled. Users cannot perform drag and drop operations from the host to the guest or from the guest to the host.
	NOTE These policy changes might not occur until users power cycle their virtual machines	
Folder Sharing settings	Specify whether to allow or block folder sharing between the host and the virtual machine.	
	Allow	Folder sharing is enabled for the virtual machine. Users can select or edit any of the folder-sharing virtual machine settings.
	Block	Folder sharing is disabled for the virtual machine. Users cannot modify the folder-sharing virtual machine settings.
Change memory settings	Specify whether to allow users to change the memory settings of the virtual machine.	
Change CPU settings	Specify whether to allow users to change CPU settings of the virtual machine.	
Optimize CPU	Specify whether the Horizon FLEX virtual machine's CPU is automatically optimized to fit the client 's host operating system. This option is enabled by default. For more information, see "Optimizing Virtual Processors and Memory for Horizon FLEX Virtual Machines," on page 37.	
Optimize memory	Specify whether the Horizon FLEX virtual machine's memory is automatically optimized to fit the client 's host operating system. This option is enabled by default. For more information, see "Optimizing Virtual Processors and Memory for Horizon FLEX Virtual Machines," on page 37.	
Require the user to change the power on passphrase when moving or copying the virtual machine	Specify whether to require users to change the encryption password if they move or copy the virtual machine.	
Set the power on passphrase to match the user's AD passphrase after first startup	Specify whether the password that users enter when powering on the virtual machine matches the Active Directory password. Leaving this option unselected allows users to change the encryption password at any time.	
Restrict the user from creating multiple copies of the virtual machine	Specify whether to allow users to download multiple instances of the virtual machine or copy already registered virtual machines.	
Network	Specify the network card setting to one of the following options:.	
	Allow	User can select setting.
	Bridged	Always use an IP address separate from the host.
	Shared	Always share the host's IP address.
	Blocked	No network connectivity.

Option	Action
Add New Disk	Specify whether users can add new hard disks to the virtual machine. **Allow** Adding a new virtual disk is enabled for the virtual machine. Users can add a hard disk, specifying details, such as the type of hard disk, disk size, and so on. **Block** Adding a new virtual disk is disabled for the virtual machine. Users cannot add a hard disk to the virtual machine.
Hide the restricted password panel from the user	Specify whether to show or hide the restrictions password panel from the user. Selecting this option prevents certain user interface items from appearing in the Horizon FLEX Client. The result is that users cannot unlock the restrictions of the virtual machine, for example, to access all of the virtual machine setting options. Deselecting this option allows users to unlock the Horizon FLEX virtual machine by entering the restriction password.
Require the user to re-encrypt the virtual machine	Specify whether to re-encrypt the Horizon FLEX virtual machine if it has not been re-encrypted before. The user does not need to take any action. If you select this feature, the re-encryption must occur before the virtual machine can be powered on. The re-encryption provides another layer of security. The result of the re-encryption process is that different users have different encryption credentials.

7 (Optional) In **End User Messages**, configure virtual machine expiration settings.

The default message is `This virtual machine is expired.`

a Type an additional custom message to display to the user when the virtual machine is expired.

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.

Option	Action
FLEX Server URL	Type the URL of the Horizon FLEX server that hosts the virtual machine package. For example: **`https://flexserver.demo.local:7443`** **IMPORTANT** Do not add **`/rvm`** to the end of the URL.
Server Contact Frequency	Select the frequency in minutes, hours, or days with which the virtual machine contacts the server for synchronization.
Offline Time Limit	Set the number of minutes, hours, or 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

Entitle the Horizon FLEX virtual machine. See "Entitle a Horizon FLEX Image," on page 53.

Configure a USB Device Policy for a Horizon FLEX Image

You configure policies to control whether USB devices can be used on virtual machines created from a Horizon FLEX image.

Important If the USB device controller is present in the source virtual machine, you can configure a policy to enable or disable this feature when users download an instance of the virtual machine. If this feature is disabled in the source virtual machine, you cannot override the virtual machine settings by enabling this feature in a policy.

Procedure

1 Start the Horizon FLEX Admin Console.

   a In a Web browser, enter **`https://WebManagerServer:port/rvm`**.

      - *WebManagerServer* is the DNS name or IP address of the host where the Mirage Web Manager is installed.
      - *port* is the port number with which the Horizon FLEX Admin Console can be accessed. When the Mirage Web Manager is installed, if you deploy the Horizon FLEX Admin Console and the Horizon FLEX Policy Server on different ports, *port* is the port number specified for the **VMware Horizon FLEX Web Management** option. Otherwise, *port* is the port number specified for the **VMware Mirage Web Management** option.

   b Enter 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 create a policy, or select an existing policy and click **Change Policy** to modify it.

4 Click the **Device Control** tab to add a new device policy.

5 Select the **Global Use of USB devices** drop-down menu to set whether the policy will allow all USB devices or block all USB devices on the virtual machine.

   All the USB device classes are dimmed and cannot be changed. See "Configure a Custom USB Device Policy for a Horizon FLEX Image," on page 50 to create a custom policy where specific USB device classes are allowed.

6 Click **OK** to save the policy.

   The new or updated policy appears in the policy list.

What to do next

Entitle the Horizon FLEX virtual machine. See "Entitle a Horizon FLEX Image," on page 53.

Configure a Custom USB Device Policy for a Horizon FLEX Image

You can configure custom device policies to control whether specific types of USB devices can be used on virtual machines created from a Horizon FLEX image.

Important If the USB device controller is present in the source virtual machine, you can configure a policy to enable or disable this feature when users download an instance of the virtual machine. If this feature is disabled in the source virtual machine, you cannot override the virtual machine settings by enabling this feature in a policy.

Procedure

1 Start the Horizon FLEX Admin Console.

   a In a Web browser, enter **`https://WebManagerServer:port/rvm`**.

      - *WebManagerServer* is the DNS name or IP address of the host where the Mirage Web Manager is installed.
      - *port* is the port number with which the Horizon FLEX Admin Console can be accessed. When the Mirage Web Manager is installed, if you deploy the Horizon FLEX Admin Console and the Horizon FLEX Policy Server on different ports, *port* is the port number specified for the **VMware Horizon FLEX Web Management** option. Otherwise, *port* is the port number specified for the **VMware Mirage Web Management** option.

   b Enter 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 create a policy, or select an existing policy and click **Change Policy** to modify it.

4 Click the **Device Control** tab to add a new device policy.

5 Set the **Global Use of USB devices** drop-down menu to **Custom** to allow or block specific classes of USB devices on the virtual machine.

   The text boxes for the class of USB devices appear, giving you the opportunity to allow or block specific classes.

6 Select the USB classes to allow or block on the virtual machine.

Table 5-3. USB Device Types

USB Class	Base Class	Examples
Audio	01h	USB sound card
Communication and CDC Device	02h	USB network adapter, RS-232 serial devices
Physical	05h	Joystick
Image	06h	USB camera, USB scanner, webcam
Printer	07h	USB printer
Mass Storage	08h	USB disk
Smart Card	0Bh	USB smart card reader
Content Security	0Dh	Fingerprint reader
Video	0Eh	Webcam
Wireless Controller	E0h	Bluetooth adapter, Microsoft RNDIS
Miscellaneous	EFh	Select the **Miscellaneous** option to allow or block USB devices not covered in the previous classes. See Table 5-4 for USB classes that require the **Miscellaneous** setting.

Table 5-4. Miscellaneous USB Device Classes

USB Class	Base Class	Examples
Human Interface Device (HID)	03h	USB keyboard, USB joystick, USB mouse
Hub	09h	USB hub

Table 5-4. Miscellaneous USB Device Classes (Continued)

USB Class	Base Class	Examples
Personal Healthcare	0Fh	Pulse monitor (watch)
Diagnostic Device	DCh	USB compliance testing device
Application-specific	FEh	IrDA Bridge, Test and Measurement Class (USBTMC), USB Device Firmware Upgrade (DFU)

7 Optionally, you can configure the device policy to allow specific USB devices.

   a Under the **Allow the virtual machine to use the following USB devices** text box, click **Add**.

   b Enter the name of the USB device in the **Name** text box.

   c Enter the vendor ID as a hex value in the **Vendor ID** text box.

   d Enter the product ID as a hex value in the **Product ID** text box.

   e Click **Add** and click **Update**.

   To obtain the USB device information on a Windows machine, click **System Tools** and then select **Device Manager**. To obtain USB device information on a Mac, click the **Apple** icon, select **About the Mac**, select **System Report**, then select **USB** and click the device item.

8 Click **OK** to save the policy.

   The new or updated policy appears in the policy list.

What to do next

Entitle the Horizon FLEX virtual machine. See "Entitle a Horizon FLEX Image," on page 53.

Update a Policy for a Deployed Horizon FLEX Image

After a Horizon FLEX image has been deployed to users, you can update policies that apply to existing virtual machine instances.

Procedure

1 Start the Horizon FLEX Admin Console.

   a In a Web browser, enter **`https://WebManagerServer:port/rvm`**.

   - *WebManagerServer* is the DNS name or IP address of the host where the Mirage Web Manager is installed.
   - *port* is the port number with which the Horizon FLEX Admin Console can be accessed. When the Mirage Web Manager is installed, if you deploy the Horizon FLEX Admin Console and the Horizon FLEX Policy Server on different ports, *port* is the port number specified for the **VMware Horizon FLEX Web Management** option. Otherwise, *port* is the port number specified for the **VMware Mirage Web Management** option.

   b Enter 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.

3 Select the virtual machine.

4 Click **Change Policy**.

5 Update the policy for the Horizon FLEX image and click **OK** when complete.

Note Policy changes related to drag and drop and copy and paste might not take place until users power cycle their virtual machines.

What to do next

See "Configure a General Policy for a Horizon FLEX Image," on page 46 and "Configure a USB Device Policy for a Horizon FLEX Image," on page 50 for more information.

Entitle a Horizon FLEX Image

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

Users can download any Horizon FLEX virtual machine to which they are entitled. Users must enter their Active Directory credentials before they can register and use a Horizon FLEX virtual machine for the first time. Users can log in to the Horizon FLEX server and download the virtual machine. Or they can copy the Horizon FLEX virtual machine from a USB and enter the Active Directory credentials when the virtual machine first boots.

Prerequisites

- Verify that 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 44.
- Configure a policy for the Horizon FLEX image. See "Configure a General Policy for a Horizon FLEX Image," on page 46.

Procedure

1 Start the Horizon FLEX Admin Console.

   a In a Web browser, enter **`https://WebManagerServer:port/rvm`**.

      - *WebManagerServer* is the DNS name or IP address of the host where the Mirage Web Manager is installed.
      - *port* is the port number with which the Horizon FLEX Admin Console can be accessed. When the Mirage Web Manager is installed, if you deploy the Horizon FLEX Admin Console and the Horizon FLEX Policy Server on different ports, *port* is the port number specified for the **VMware Horizon FLEX Web Management** option. Otherwise, *port* is the port number specified for the **VMware Mirage Web Management** option.

   b Enter 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 an entitlement, select an existing entitlement and click **Edit** to modify it, or select an existing entitlement and click **Duplicate** to duplicate it.

4 Create the entitlement name and assign it to a Horizon FLEX image.

   a Enter a name for the entitlement in the **Entitlement Name** text box.

   When users connect to the Horizon FLEX server, the list of entitled virtual machines appears in the Available Desktops window. Each virtual machine displays a virtual machine name and an entitlement name.

   The entitlement name is useful when the same virtual machine is entitled to a user more than once. The user can distinguish such virtual machines by the entitlement name.

   b Select a Horizon FLEX image to add to the entitlement.

   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.

   When you select the Horizon FLEX image, the download URL for the image is automatically populated in the **Download URL** text box.

   c (Optional) In the **Download URL** text box, change the URL that the client uses to download the Horizon FLEX image.

   d Click **Next**.

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.

   New 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 **Use machine name configuration** and configure the naming pattern.

   a Enter 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. You can also create a running number pattern using the {*n*} placeholder to increment virtual machine numbers with user names.

   For more information, see "Create a Virtual Machine Name Pattern," on page 55.

   b Enter a domain name in the **Domain name** text box.

   The name must be for the domain to which the Mirage management server belongs or for one of its child domains.

   c (Optional) Enter an OU in the **Organizational Unit**text box.

   For example: `OU=hr1, OU=hr, OU=flex, DC=ws, DC=test, DC=com`

8 (Optional) To use server assigned MAC address for entitled restricted virtual machines, select **Specify MAC address range** and specify the first and last MAC addresses in the range.

   For more information, see "Specify a MAC Address Range," on page 57.

9 (Optional) Configure Microsoft DirectAccess support for Horizon FLEX virtual machines.

DirectAccess enables remote users to access shared resources, web sites, and applications on an internal network without connecting over a VPN. To support DirectAccess, the Horizon FLEX virtual machine must be running Windows 8.1 or later. The Horizon FLEX server must be deployed on Windows Server 2012 or later. The Active Directory server must be configured to support DirectAccess. For more information, see the Microsoft documentation.

a In the **Policy Names** field, enter the Group Policy object (GPO) names that are used to initiate DirectAccess.

Each policy name is the display name of the GPO in the Active Directory directory service. Separate each policy name using a semicolon.

b (Optional) Select the **Import Root CA Certificates** check box to import the root certificate authority certificates.

c (Optional) Select the **Reuse any existing computer account** check box to overwrite any existing computer accounts of the virtual machine at the domain joining operation.

This setting does not apply when using a serial machine name pattern of {n}.

10 Click **Next**.

11 (Optional) If you installed the Mirage client in the virtual machine, select whether to manage the virtual machine with Mirage.

Option	Description
Use VMware Mirage for disaster recovery and Image management scenarios	Select this option to select a CVD policy, a base layer, an application layer, and other configurations. The Mirage server automatically creates a CVD for virtual machines that the end user downloads. Mirage periodically synchronizes end-user data into the data center 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 application layers to the virtual machine after it has been provisioned for image compliance and remote application delivery.
Use VMware Mirage for disaster recovery scenarios	Select this option to select a CVD policy. The Mirage server creates a CVD for virtual machines that 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.
Do not use VMware Mirage to manage the virtual machines	Select this option to opt out of managing the virtual machine with Mirage.

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

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

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

Create a Virtual Machine Name Pattern

When entitling a Horizon FLEX image, you can create a virtual machine name pattern so that when virtual machines are created for the same user entitlement, Horizon FLEX creates unique virtual machine names.

The virtual machine name pattern must include the {*username*} or {*n*} parameters. The {*n*} parameter enables the creation of a running number pattern to add incremental numbers to virtual machine names. These patterns are valid:

- VM-{*username*}

- VM-{*n*}

The machine name is limited to 15 characters. If a machine name is longer than 15 characters, only the first 15 characters are used. For example, if the pattern is VM-1234567890-*username* and the user name is Jack, the machine name is trimmed to VM-123456789-J. These patterns are not valid, in some cases because the machine name might be too long:

- VM-(*username*}-{*username*}
- VM-{*username*}-{*n*}
- VM-{*n*}-{*n*}

To ensure that each virtual machine receives a different name and can join the domain, it must include the {*username*} or {*n*} placeholders. The {*username*} placeholder is replaced by the individual user's name when the user downloads the virtual machine. For {*n*}, the Active Directory is searched for computers with names that match the pattern. If no names match the pattern, the running number value is 1. Otherwise, the value for the next running number is the successor number of the maximum number between all names that match the pattern.

For example, one virtual machine might be entitled to user1 and the machine name pattern might be set as VM-*username- n*. When user1 downloads the virtual machine, Active Directory is searched to determine whether a machine name matches the name pattern, such as VM-user1-*x*, where *x* is the assigned number. If the maximum mapping number is 25, where the virtual machine name is VM-user1-25, this machine name is set as VM-user1-26. If no virtual machine matches the pattern, Horizon FLEX sets the machine as VM-user1-1.

You can entitle more than one virtual machine to the same user. For example, you can entitle three virtual machines to user1. When user1 downloads the virtual machines, the virtual machine name is changed to vm-*x*-user1. The assigned virtual machine number is not incremented for each user name but is based on when the virtual machine was registered.

For example, user1 might have three virtual machine names vm-10-user1, vm-26-user1 and vm-39-user1, depending on which other virtual machines were entitled to other users and when user1 downloaded each virtual machine. The incremented number is used only for tracking by the Horizon FLEX administrator. The client user does not see the incremented number.

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

- Verify that the Horizon FLEX client is installed on the end user system.
- Give the end 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 consists of one of the following structures:

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

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

username is the user's login name and *myserver.com* is the host name of the server. *username* is optional. If *username* is not included in the URI, the user name text box is not prepopulated in the server connection dialog box. 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.

3 Create an email for the user and enter some link text.

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

4 Select the link text, right-click the selected text, and select **Hyperlink**.

5 Select **Link to: Existing File or Web Page**.

6 Enter the URI in the **Address** text box.

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

The link is now active.

7 Click **OK**.

8 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 that you specified in the URI. The user enters a password and connects to the server to download a virtual machine.

Specify a MAC Address Range

The Horizon FLEX Client creates a random MAC address for each new instance of a virtual machine. However, if you want all virtual machines in an entitlement group to follow a MAC address pattern, you can specify that pattern.

Procedure

1 Specify an initial MAC address.

All MAC addresses assigned from the Horizon FLEX start with OUI: 00:0C:29.

2 Specify the last MAC address in the range.

The range 00:0C:29:00:00:00 to 00:0C:29:FF:FF:FF is an example of a MAC address range.

Note

- The Horizon FLEX server uses each MAC address in order. The server automatically releases the MAC address for reuse when you use the Horizon FLEX Admin Console to delete the virtual machine or the virtual machine instance is in one of the following states.
  - Deleted by User
  - Download Canceled
  - Wiped
  - Invalid Source VM
- When the Horizon FLEX server reaches the end of the range, a message appears telling users to inform their administrator that no MAC addresses are available.
- The new MAC address is only applied to the first NIC, ethernet0.
- The method for specifying a MAC address by manually editing the file on the end point continues to work. If you use the manual method, do not set a range on the Horizon FLEX server. See KB 2130612.

Managing Horizon FLEX Virtual Machines

6

You can manage deployed Horizon FLEX virtual machines by performing operations such as Edit, Lockout, Reactivate, Wipe, Archive, or Delete.

Manage Horizon FLEX Virtual Machines

Once Horizon FLEX virtual machines are deployed, you can manage them by performing different operations. You can view the inventory of deployed Horizon FLEX virtual machines in the Horizon FLEX Admin Console.

You can use the **Search** text box to filter the virtual machine list and the sortable column headings to find a specific virtual machine. Use the column heading drop-down menu 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 Start the Horizon FLEX Admin Console.

   a In a Web browser, enter `https://WebManagerServer:port/rvm`.

      - *WebManagerServer* is the DNS name or IP address of the host where the Mirage Web Manager is installed.
      - *port* is the port number with which the Horizon FLEX Admin Console can be accessed. When the Mirage Web Manager is installed, if you deploy the Horizon FLEX Admin Console and the Horizon FLEX Policy Server on different ports, *port* is the port number specified for the **VMware Horizon FLEX Web Management** option. Otherwise, *port* is the port number specified for the **VMware Mirage Web Management** option.

   b Enter 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.

   If the policy field is blank, the virtual machine was created using Horizon FLEX 1.6 or earlier. The virtual machine may have a policy assigned to it and the policy continues to work. To create a new policy for the virtual machine, see "Creating Policies and Entitlements," on page 46.

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

Option	Action
Change Policy	Select a virtual machine and click **Change Policy** to change the policies assigned to this virtual machine.
Lockout	Select a virtual machine and click **Lockout** to revoke user access to the specific virtual machine.
Reactivate	Select an archived or locked-out virtual machine and click **Reactivate** to reset the virtual machine.
Wipe	Select a virtual machine and click **Wipe** to delete it from the file system.
Archive	Select a virtual machine and click **Archive** to disable the virtual machine for use and keep an offline record of the virtual machine. Select 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.
Delete	Select an archived or wiped virtual machine and click **Delete**. You cannot delete a virtual machine that has any other status than Archived or Wiped.

4 To determine the actions that you can take for a virtual machine, view the virtual machine status in the Status column.

Status	Description
Active	The virtual machine is in use, has contacted the server, and has not expired.
Inactive	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.
Expired	The expiration date has been reached and the virtual machine has been turned off.
Pending Expired	The server is waiting for confirmation from the Horizon FLEX Client that the virtual machine is expired.
Locked Out	An administrator has locked out the user of the virtual machine.
Pending Lockout	A lockout has been initiated. The status remains Pending until the Horizon FLEX Client verifies that the virtual machine has been locked out.
Pending Reactivate	The server is waiting for confirmation from the Horizon FLEX Client that the virtual machine is reactivated.
Downloading	The user is downloading the virtual machine.
Download Cancelled	The user has cancelled the download.
Download Paused	The user has paused the download.
Domain Join Fail	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.
Deleted by User	The user has deleted the VM on the client.
Wiped	The virtual machine has been wiped by the administrator and removed from the user's system.
Pending Wipe	The server is waiting for confirmation from the Horizon FLEX Client that the virtual machine has been removed from the user's system.
Archived	The virtual machine has been archived. **Note** You must select the **Display archived instances** check box to view archived virtual machines.
Invalid Source VM	The downloaded virtual machine is not from the same image entitled to the user.

Maintaining the Horizon FLEX System

7

You can perform maintenance operations on the Horizon FLEX system, including upgrading from previous Horizon FLEX versions.

This chapter includes the following topics:

Upgrade from Previous Horizon FLEX Versions

You can upgrade the Horizon FLEX system from earlier Horizon FLEX versions.

Prerequisites

- All Mirage servers are shut down.
- Perform the appropriate preparation for a Mirage upgrade. See information related to upgrade preparation in the *VMware Mirage Installation Guide*.
- On the Mirage Web Management server, back up the `web.config` file in the `Rvm` directory. The default location of the directory is `C:\Program Files\Wanova\Rvm`.

  When you upgrade the Mirage Web Management server, see Step 3c, the system replaces the `web.config` with a new version, which deletes the customized settings in the file. After the upgrade, update the `web.config` file by applying the customized settings in the backed-up file to the new file.

  Note
  - Except for parameters that affect the customized features mentioned in this prerequisite, do not change the parameters in the `web.config` file, especially the `RvmPolicyVersion` parameter. The supported policy versions are 6, 7, 8, 9, 10, and 11. If you change the policy number to an unsupported version, users might lose access to Horizon FLEX virtual machines.
  - If you deploy the Horizon FLEX Admin Console and Horizon FLEX Policy Server on different ports, back up the `web.config file` in the `RvmAdmin` directory instead of in the `Rvm` directory. The default location of the `RvmAdmin` directory is `C:\Program Files\Wanova\RvmAdmin`.

Procedure

1 Download the Horizon FLEX Server and Horizon FLEX Client installation files for the upgrade version.

2 Upgrade all Horizon FLEX clients to the version that is compatible with the version to which you upgrade the Horizon FLEX Server.

- Provide end users with the installer file for the Fusion Pro or Workstation Player upgrade version. Alternatively, you can instruct them to download the software from the VMware website.
- Upgrade the Horizon FLEX Clients by using a mass deployment.

3 Upgrade the Horizon FLEX Server component.

a To upgrade the Mirage Management Server, double-click the `mirage.management.server.64x.buildnumber.msi` file in the server folder.

By default, the configuration settings you selected during the initial installation are applied. You can change the configuration settings during the upgrade process.

b To upgrade the Mirage server.

- Double-click on `mirage.server.64x.buildnumber.msi` file. Use this option if you are a local administrator and User Account Control (UAC) is enabled.
- Access the command prompt as an administrator and run the `mirage.server.64x.buildnumber.msi` file. Use this option if you are not a local administrator and UAC is enabled.

By default, the configuration settings you selected during the initial installation are applied. You can change the configuration settings during the upgrade process.

c To upgrade the Mirage Web Management.

- Double-click on the `mirage.WebManagement.x64.buildnumber.msi` file. Use this option if you are a local administrator and UAC is enabled.
- Access the command prompt as an administrator and run the `mirage.WebManagement.x64.buildnumber.msi` file. Use this option if you are not a local administrator and UAC is enabled.

Continue with no change.

d If you use Mirage to manage your Windows virtual machines, follow the instructions for upgrading from the previous Mirage version in the *VMware Mirage Administrator's Guide*.

What to do next

For complete Mirage upgrade instructions, see the VMware Mirage documentation at https://www.vmware.com/support/pubs/mirage_pubs.html.

Note Do not select the **Create new storage areas** when upgrading the Mirage Management Server. If you select this option and enter the path to the original storage area, your entire Mirage installation is deleted. For example, the base layer, app layer, and CVD data are deleted and become irretrievable if a backup is unavailable.

See "Installing the Horizon FLEX Client for End Users," on page 17 for information on using a mass deployment to provide the Horizon FLEX Client to end users.

Distribute the Horizon FLEX Client License Key

You can distribute Horizon FLEX license keys from the Horizon FLEX server to automatically activate the Horizon FLEX Client.

End users receive the correct license key when they connect to the Horizon FLEX server. You do not need to update the license key on each end point. You can also set the target Horizon FLEX Client version.

Moreover, if the Horizon FLEX Client version does not meet the version that you configured on the Horizon FLEX server, the warning message you configured appears in the Horizon FLEX Client to provide the user with assistance.

Procedure

1 In the Horizon FLEX Admin Console, click the **General System Settings** icon and select **License Management**.

2 Click **Configure client license**.

3 Fill out the Client License Management form.

Option	Description	
Enable client license distribution	Keep this option selected.	
Version		
	Latest	Select **Latest** if you want users to download the latest version of the client from the VMware Web site. Enforce the use of a minimum client version by entering the version in the **Minimum client version** text box.
	Fixed	Select **Fixed** if you have a version that you would prefer users to use. The version number users use must be the same as the specified version in the **Required client version** text box.
Minimum client version or **Required client version**	The name of this option is **Minimum client version** or **Required client version** depending on the value you select for the preceding option.	
	Minimum client version	The name of this option is **Minimum client version** when you select **Latest** for the preceding option. If you want end users to upgrade the Horizon FLEX Client, for example for a security patch, you do not need to upgrade the Horizon FLEX server. Instead, you can configure this setting to a minimum version that is higher than the minimum the server already enforces.
	Required client version	The name of this option is **Required client version** when you select **Fixed** for the preceding option. If you want end users to keep the specified version, you can configure this setting to a version that is equal to the version the Horizon FLEX server already enforces.
Client license key	Enter the Horizon FLEX Client license key.	
Update server	Enter the URL from which end users can download the Horizon FLEX Client installation package when the current version of their client is not allowed to receive the license.	
Display this message to notify the client user for client software update	Enter a message that tells end users what actions they can take when the current version of their client is not allowed to receive the license.	

4 Click **OK**.

From this point forward, each time an end user uses the Horizon FLEX Client to connect to the Horizon FLEX server, the client sends information to the Horizon FLEX server. The server displays some of the information, such as the Horizon FLEX Client version number, on the Users page in the Horizon FLEX Admin Console. See Step 5

The server does not return the client license key until it verifies that client meets the target version requirement. If the target required version is not met, the server sends the message you created to the end user, prompting the user to upgrade the client. Once the server verifies that the client meets the target version requirement, the server sends the license key to the client and the client applies the key.

5 To monitor user information related to the Horizon FLEX Client, in the future, occasionally, click **Users** in the Horizon FLEX Admin Console.

The Users page displays information about each user who successfully connects to Horizon FLEX server. The information includes the user name, host name, and Horizon FLEX Client version for each user.

Horizon FLEX System Logs

Horizon FLEX log files can be used for troubleshooting system issues.

Horizon FLEX system logs are available in the following locations:

- Web App log file

  `C:\ProgramData\Wanova Mirage\rvm\logs\webapp.log`

- Horizon FLEX server logs

  `C:\Program Files\Wanova\Mirage Management Server\logs`

  The most important log file is the `mgmtservice.log` file.

- Horizon FLEX uses the Microsoft offline domain join feature. The offline domain join log file is at:

  `C:\Windows\debug\NetSetup.LOG`

Index