# VMware Horizon Mirage Installation Guide

Horizon Mirage 4.4

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

EN-001277-03

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com



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

# Contents

# VMware Horizon Mirage Installation

The *Horizon Mirage Installation Guide* provides information about how to install and deploy the Horizon Mirage components and prepare the system to centralize endpoint devices.

Installing the system involves installing the Horizon Mirage Management server, console, and server components, and associated applications that facilitate, for example, file portal access. For information about how to install Horizon Mirage clients, see the *Horizon Mirage Administrator's Guide*.

## Intended Audience

This information is intended for anyone who wants to install Horizon Mirage. The information is written for experienced Windows system administrators who are familiar with typical Windows Data Center environments such as Active Directory, SQL, and MMC.

# About the Horizon Mirage System Components

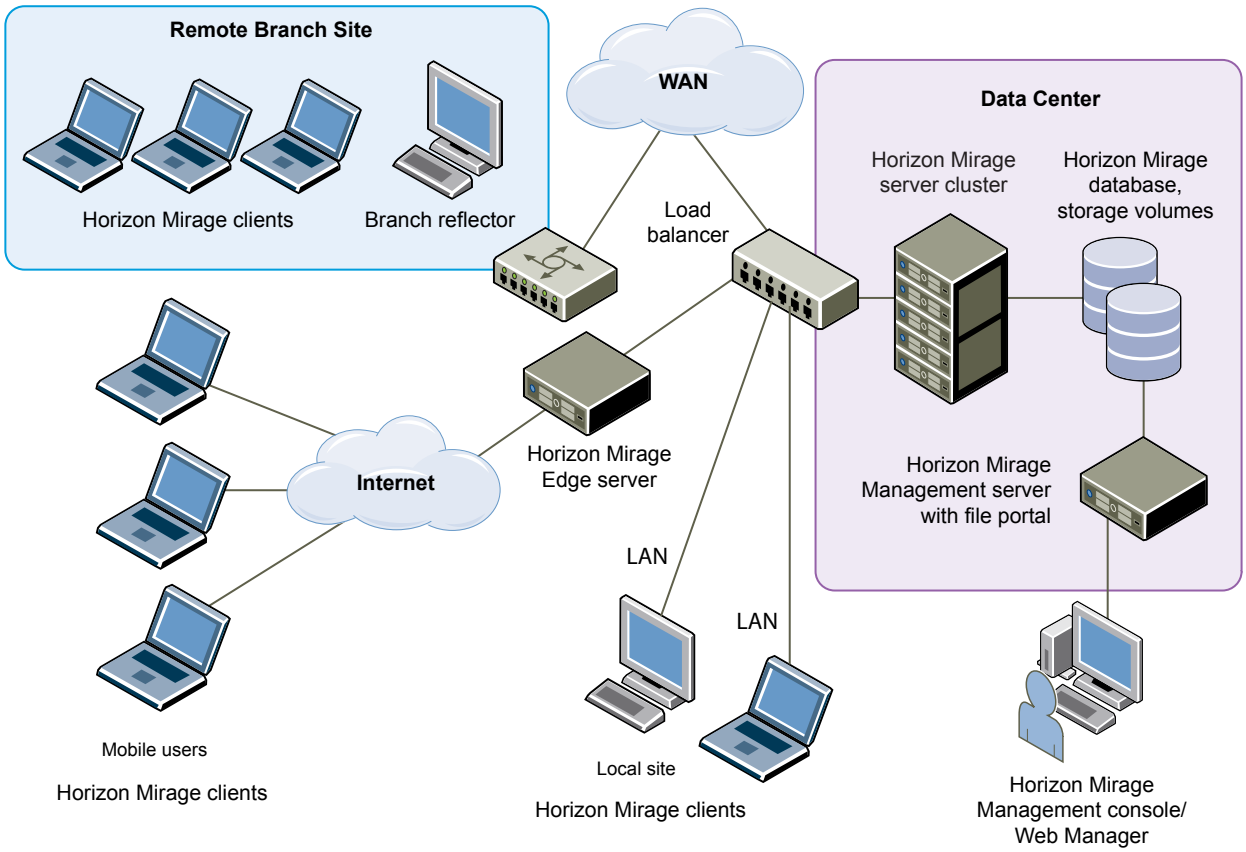
1

VMware® Horizon Mirage™ software centralizes the entire desktop contents in the data center for management and protection purposes, distributes the running of desktop workloads to the endpoints, and optimizes the transfer of data between them.

The Horizon Mirage components integrate into a typical distributed infrastructure, with the following relationships between the system components:

- Horizon Mirage clients connect to a Horizon Mirage server, either directly or through a load balancer.
- The administrator connects to the system through the Horizon Mirage Management server.
- Horizon Mirage servers and the Management server share access to the back-end Horizon Mirage database and storage volumes. Any server can access any volume.

**Figure 1-1.** System Components



## Horizon Mirage clients

Endpoint devices installed with the Horizon Mirage client can run a centralized virtual desktop (CVD) or convert an existing desktop to a CVD. See "Centralized Virtual Desktop (CVD)," on page 8.

The Horizon Mirage client software runs in the base operating system and makes sure the images at the endpoint and the CVD are synchronized. The client does not create or emulate a virtual machine. No virtual machines or hypervisors are required. The Horizon Mirage client software can run on any Type 1 or Type 2 hypervisor.

## Horizon Mirage Management server

The Horizon Mirage Management server, located in the data center, is the main component that controls and manages the Horizon Mirage server cluster.

## Horizon Mirage Management console

The Horizon Mirage Management console is the graphical user interface used to perform scalable maintenance, management, and monitoring of deployed endpoints.

Through the Management console, the administrator configures and manages clients, base and app layers, and reference machines. The administrator uses the Management console to perform operations such as update and restore, and monitors the system operation through the dashboard and event logs.

## Horizon Mirage Web Manager

The Horizon Mirage Web Manager enables help-desk personnel to respond to service queries, and the Dashboard feature assists the Protection manager role to ensure that user devices are protected. The Web Manager mirrors Horizon Mirage Management console functionality. For more information, see the *Horizon Mirage Web Manager Guide*.

## Horizon Mirage Server

The Horizon Mirage servers, located in the data center, manage the storage and delivery of base layers, app layers, and CVDs to clients, and consolidate monitoring and management communications. You can deploy multiple servers as a server cluster to manage endpoint devices for large enterprise organizations. It is good practice to keep the server on a dedicated machine or a virtual machine. However, a server can be co-hosted with the Management server.

---

**NOTE** The server machine must be dedicated for the Horizon Mirage server software to use. It must not be used for any other purposes. For hardware requirements and supported platforms, see "Hardware Requirements," on page 12 the .

---

## Centralized Virtual Desktop (CVD)

CVDs represent the complete contents of each PC. This data is migrated to the Horizon Mirage server and becomes the authoritative copy of the contents of each PC. You use the CVD to centrally manage, update, patch, back up, troubleshoot, restore, and audit the desktop in the data center, regardless of whether the endpoint is connected to the network. A CVD comprises the following components:

- Base layer defined by the administrator, which includes the operating system (OS) image plus core applications such as antivirus, firewall, and Microsoft Office. A base layer is used as a template for desktop content, cleared of specific identity information and made suitable for central deployment to a large group of endpoints.

- App layers defined by the administrator, which include sets of one or more departmental or line-of-business applications, and any updates or patches for already installed applications, suitable for deployment to large numbers of endpoints.
- Driver profile defined by the administrator, which specifies a group of drivers for use with specific hardware platforms. These drivers are applied to devices when the hardware platforms match the criteria that the administrator defines in the driver profile.
- User-installed applications and machine state, including unique identifier, hostname, any configuration changes to the machine registry, DLLs, and configuration files.
- Changes to data, applications, or the machine state made by end-user are propagated to the data center. Conversely, all changes that the administrator makes to the base layer or app layers in the data center are propagated to the endpoints. Administrators can identify data that does not need to be protected, such as MP3s, or other files that are considered local only to the endpoint.

## Horizon Mirage Reference Machine

A Horizon Mirage reference machine is used to create a standard desktop base layer for a set of CVDs. This layer usually includes OS updates, service packs and patches, corporate applications for all target end-users to use, and corporate configurations and policies. A reference machine is also employed to capture app layers, which contain departmental or line-of-business applications and any updates or patches for already installed applications.

You can maintain and update reference machines over time over the LAN or WAN, using a Horizon Mirage reference CVD in the data center. You can use the reference CVD at any time as a source for base and app layer capture.

## Horizon Mirage Branch Reflector

A Horizon Mirage branch reflector is a peering service role that you can enable on any endpoint device. A branch reflector can then serve adjacent clients in the process of downloading and updating base or app layers on the site, instead of the clients downloading directly from the Horizon Mirage server cluster. Using a branch reflector can significantly reduce bandwidth use during mass base or app layer updates or other base or app layer download scenarios. The branch reflector also assists downloading hardware drivers.

## Horizon Mirage File Portal

End users can use appropriate login credentials and the Horizon Mirage file portal to access their data from any Web browser. The file portal front-end component runs on any server machines that have IIS 7.0 or later installed, and the back-end component runs on the Management server.

## Distributed Desktop Optimization

The Distributed Desktop Optimization™ mechanism optimizes transport of data between the Horizon Mirage server and clients, making it feasible to support remote endpoints regardless of network speed or bandwidth. Distributed Desktop Optimization incorporates technologies that include read-write caching, file and block-level deduplication, network optimization, and desktop streaming over the WAN.

## Horizon Mirage Edge Server

The Horizon Mirage Edge server is the secured gateway server that is deployed outside the Mirage data center environment. The Horizon Mirage Edge server meets the enterprise security and firewall requirements and provides a better user experience for Mirage clients that access the Horizon Mirage servers through the Internet. The Edge server seamlessly integrates with the Horizon Mirage system with minor modifications to the Mirage system and protocol.

# Planning the Horizon Mirage Deployment 2

Deploying the Horizon Mirage system involves first ensuring that various requirements of its hardware components, the Horizon Mirage Management server, console, server components, and associated software applications, are satisfied.

The Horizon Mirage components support a range of operating systems. Software, hardware, and database requirements apply to each component. The Horizon Mirage system and clients use default communication ports and protocols.

This chapter includes the following topics:



## Operating System Requirements

Before you deploy Horizon Mirage, verify that the operating system requirements for each Horizon Mirage component that you install are satisfied.

**Table 2-1.** Operating System Requirements for Horizon Mirage Components

| Component | Prerequisites |
|---|---|
| Horizon Mirage client | ■ Windows XP Professional with SP2 or SP3, 32-bit.<br>■ Windows Vista Business or Enterprise, 32-bit and 64-bit.<br>■ Windows 7 Professional or Enterprise, 32-bit and 64-bit.<br>■ Windows 8.0 and 8.1 Professional or Enterprise, 32-bit and 64-bit.<br>NOTE Windows XP Fast User Switching mode must be turned off if the computer is not an AD domain member. Go to http://support.microsoft.com/kb/279765. |
| Horizon Mirage server | ■ Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit.<br>■ Windows Server 2012 Standard Edition, 64-bit.<br>■ Domain membership required. |
| Horizon Mirage Management server | ■ Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit.<br>■ Windows Server 2012 Standard Edition, 64-bit.<br>■ Domain membership required. |
| Horizon Mirage Management console | ■ Same as Horizon Mirage client. |

**Table 2-1.** Operating System Requirements for Horizon Mirage Components (Continued)

| Component | Prerequisites |
|---|---|
| Horizon Mirage reference machine | ■ Windows XP Professional with SP2 or SP3, 32-bit.<br>■ Windows 7 Professional or Enterprise, 32-bit and 64-bit. |
| Horizon Mirage Edge Server | ■ Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit,<br>■ Windows Server 2012 Standard Edition, 64-bit. |

# Hardware Requirements

Before you deploy Horizon Mirage, verify that the hardware requirements for each Horizon Mirage component that you install are satisfied.

**Table 2-2.** Hardware Requirements for Horizon Mirage Components

| Component | Prerequisites |
|---|---|
| Horizon Mirage client | ■ Client systems:<br>  ■ Enterprise-class laptops and desktops<br>  ■ Virtual machines compatible with Windows XP SP2 or later, Windows Vista or Windows 7<br>■ Minimum RAM: 512 MB for Windows XP, 1 GB for Windows Vista. Windows 7, Windows 8 snd 8.1.<br>■ Client installation and normal operation: At least 5 GB of free space |
| Horizon Mirage server node (up to 1500 clients) | ■ Minimum RAM: 16 GB.<br>■ Minimum CPU: 8 vCPU or dual Quad-Core Processor, 2.26 GHz Intel core speed.<br>■ Minimum System Drive capacity: 146 GB, including a 100 GB allocation for the Horizon Mirage network cache.<br>NOTE<br>Horizon Mirage SIS storage is not included. See Horizon Mirage Storage.<br>■ 2 x Gigabit Ethernet Port.<br>NOTE It is a good practice to separate client network and storage network access to dedicated ports. |

**Table 2-2.** Hardware Requirements for Horizon Mirage Components (Continued)

| Component | Prerequisites |
|---|---|
| Horizon Mirage storage | ■ Standalone Horizon Mirage server:<br>  ■ Direct Attached Storage (DAS).<br>  ■ Storage Area Network (SAN) connected through iSCSI or Fiber Channel (FC).<br>  ■ Network Attached Storage (NAS) connected through iSCSI, Fiber Channel (FC), or CIFS network share.<br>■ Horizon Mirage server cluster: Network Attached Storage (NAS) connected using a CIFS network share. A Windows-based NAS (CIFS share or a file server) can be used for up to 3000 endpoints. An enterprise-grade NAS devices is required for more that 3000 endpoints.<br>■ Alternate Data Streams: NAS through CIFS share must support Alternate Data Streams. To verify that the NAS device conforms with the Horizon Mirage requirements, it is recommended to use the `Wanova.Server.Tools.exe NasCompatibilityTest`.<br>■ Storage Capacity: Consumed capacity varies, depending on file duplication level across CVDs, base layers, and the number of snapshots stored, but VMware estimates that on average each user requires 15 GB of data center storage.<br>■ Storage Performance: A minimum of 0.8 IOPS per CVD is required for Mirage steady-state (incremental) uploads. For the centralization phase, higher performance might be needed. Consult with VMware or its partners for the appropriate requirements.<br>■ Enabling Compression: For DAS, SAN (FC, iSCSI) and Windows-based NAS (CIFS shares), you can sometimes realize up to 40% in storage savings by enabling the built-in Windows NTFS compression on your MirageStorage folder. For NAS systems that are not NTFS, you need to leverage their own compression options.<br>  ■ **Note** Apply this change only when Horizon Mirage services are stopped. It is also advisable to do this before the directory is heavily populated. |
| Horizon Mirage Management Server | ■ Minimum RAM: 8 GB.<br>■ Minimum CPU: 1 Quad-Core Processor or 4 vCPUs in virtual configuration, 2.26GHz Intel core speed or equivalent. |
| Horizon Mirage Management console | ■ Minimum RAM: 512 MB.<br>■ Network connectivity to the Horizon Mirage Management Server.<br>■ Minimum screen resolution: 1280 x 1024 |
| Horizon Mirage Edge Server | ■ 4 core CPU, 2.26 GHz Intel core speed or equivalent<br>■ 4 GB RAM<br>■ 40 GB available disk space<br>■ 1 x Gigabit Ethernet port |
| Microsoft SQL Server 2012 | Use the recommended Microsoft Hardware and Software Requirements for Installing SQL Server 2012. Go to http://msdn.microsoft.com/en-us/library/ms143506.aspx. |
| Microsoft SQL Server 2008 R2 | Use the recommended Microsoft Hardware and Software Requirements for Installing SQL Server 2008 R2. Go to http://msdn.microsoft.com/en-us/library/ms143506%28v=sql.105%29.aspx |

# Software Requirements

Before you deploy Horizon Mirage, verify that the software requirements for each Horizon Mirage component that you install are satisfied.

**Table 2-3.** Software Requirements for Horizon Mirage Components

| Component | Requirements |
|---|---|
| Horizon Mirage client | .NET Framework version 3.5 SP1. |
| Horizon Mirage server | ■ Microsoft .NET Framework version 3.5 SP1 64-bit.<br>■ File portal requires an IIS 7.0 or later installation, the IIS 6 Management Compatibility Role, and the ASP.NET feature. Both options are within the IIS installation and are not selected by default. |
| Horizon Mirage Management server | Microsoft .NET Framework version 3.5 SP1 64-bit. |
| Horizon Mirage Management console | ■ Microsoft .NET Framework version 3.5 SP1.<br>■ Microsoft Management Console version 3.0 or later. Go to http://support.microsoft.com/?kbid=907265 |
| Horizon Mirage reference machine | ■ Horizon Mirage client.<br>■ The OS and applications installed on the reference machine must use volume licenses and be designed for multiuser and multimachine deployment.<br>■ Verify that the reference machine does not include the following items:<br>  ■ Applications that install and use hardware-specific licenses.<br>  ■ Applications that install and use local user accounts or local groups, or both.<br>  ■ Software that uses a proprietary update service. Such software must be installed directly on endpoints. |
| File Portal | ■ Microsoft IIS 7 or later.<br>■ Microsoft Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit.<br>■ .NET Framework version 3.5 SP1. |
| Horizon Mirage Web Manager | ■ Microsoft IIS 7.0 or later.<br>■ Microsoft Windows Server 2008 R2 Standard of Enterprise Edition, 64-bit or Microsoft Windows Server 2012 Standard or Enterprise Edition.<br>■ .NET Framework 4.0 |
| Horizon Mirage Edge Server | ■ .NET Framework version 3.5.1 |

# Database Requirements

Before you deploy Horizon Mirage, verify that all database software requirements are satisfied.

**Table 2-4.** Database Software Requirements for Horizon Mirage Components

| Component | Requirements |
|---|---|
| Database software | ■ Windows Installer 4.5 (MS KB942288) or later. Go to http://support.microsoft.com/kb/942288)<br>■ Microsoft SQL Server® 2012 SP1 Express, Standard, and Enterprise editions are supported. Go to http://msdn.microsoft.com/en-us/evalcenter/ff978728.aspx<br>■ Microsoft SQL Server® 2008 64-bit R2. Express, Standard, and Enterprise editions are supported. Go to http://msdn.microsoft.com/en-us/library/ms143506%28v=sql.105%29.aspx<br>NOTE When you install SQL Server 2008 R2 on Windows Server 2012, you must install Service Pack 1 or later. Go to http://support.microsoft.com/kb/2681562.<br>MS SQL Server must be set up with Windows Authentication. The Windows account used for installing Horizon Mirage must have dbcreator privileges, and the user account running the Horizon Mirage server services must be configured with access privileges to the Horizon Mirage database. |

## Database Sizing Requirements

Depending on the size of the Horizon Mirage clusters in your environment, limitations on the size of the database needs careful planning and consideration.

The following guideline can assist you in planning your database sizing requirements for your environment.

**Table 2-5.** Horizon Mirage Database Sizing Guidelines

| Mirage Cluster Size | Minimum System Requirements |
|---|---|
| Mirage cluster with less than 5000 endpoints | Microsoft SQL Server 2008 Express R2 or Microsoft SQL Server 2012 Express |
| | At least one CPU, 2.0 GHz or faster |
| | At least 1 GB RAM |
| Mirage cluster with more than 5000 endpoints | Microsoft SQL Server 2008 Standard R2 or Microsoft SQL Server 2012 Standard |
| | At least two CPUs, 2.0 GHz or faster |
| | At least 4 GB RAM |

The database sizing requirements for Horizon Mirage are based on the Microsoft hardware and software requirements for installing SQL Server 2008 R2. For a detailed explanation, go to http://msdn.microsoft.com/en-us/library/ms143506%28v=sql.105%29.aspx.

# Ports and Protocols Used by Horizon Mirage

The Horizon Mirage system and clients use default communication ports. Make sure that the correct ports and protocols are selected for the system.

The Horizon Mirage Management server and Horizon Mirage servers use external and internal communications, as follows:

- External communications to communicate with the Horizon Mirage clients or Management console
- Internal communications to communicate with each other

**Table 2-6.** Ports and Protocols for Horizon Mirage Components

| Component | Communications | Port | Protocol | Notes |
|---|---|---|---|---|
| Horizon Mirage service | External | 8000 | TCP/IP or SSL/TLS | The only port required for communications between Horizon Mirage clients and servers.<br>**NOTE** SSL/TLS is optional and can be enabled as described in "Install the Server SSL Certificate," on page 21. |
| Horizon Mirage Branch Reflector | External | 8001 | TCP/IP | Used for communication between the branch reflector and the local peers at the remote site. |
| Horizon Mirage Management service | External | 8443 | TCP/IP | Used for communication between the Mirage Management console and the Mirage Management service. SOAP Message-level Security is applied. |
| Horizon Mirage Server service | Internal | 135, 445 | TCP/IP | Used for control communication between the Mirage Management service and the Mirage server.<br>**NOTE** You may limit access to this port to incoming connections from the Mirage Management service host. |
| File Portal | Internal | 8444 | TCP/IP | Used for communication between the IIS server and the Mirage Management Server. |
| Horizon Mirage Edge server | Internal | 8000 | TCP/IP | Used for communication between the Edge Server and the Mirage server.<br>**NOTE** The port must have DNS update access. |
| | Internal | 389, 636 | TCP/IP<br>LDAP or LDAPS | Used for communications between the Mirage Edge server and the LDAP servers. |
| | Internal | 1001 | TCP/IP | Used for communications between the Mirage server and the Mirage MMC console. |
| | External | 8000 | TLS/SSL | Used for communication between the Mirage client and the Mirage Edge server. |

# Install the Horizon Mirage System 3

The Horizon Mirage deployment involves a number of components, which you must install in a specific order.

### Prerequisites

- Verify that all hardware and software prerequisites are fulfilled, that you have a valid license for the system, and that the latest version of the Horizon Mirage software is downloaded from the support site.
- Verify that the SQL server is installed and reachable. The SQL browser service must be started to allow remote connections. Verify that firewall settings allow remote connections on the SQL server host. Go to http://technet.microsoft.com/en-us/library/cc646023.aspx.
- Verify that antivirus software running on the server machine excludes Horizon Mirage server folders and processes from scanning.
  - Server folders, including the Mirage storage directory folder and the local cache directory, for example, `C:\ProgramData\Wanova Mirage\LocalCache`.
  - Server processes, for example, `Wanova.Server.Service.exe`.
  - Prepare the required database information, or install a new database instance to use with Horizon Mirage.

**NOTE** You must have dbcreator privileges to create the Horizon Mirage database in the SQL express database. If you do not have these privileges, ask the database administrator to create the database and then assign you as the database creator.

### Procedure

1 Install the Horizon Mirage Management Server on page 18

The Horizon Mirage Management server is the main component that controls and manages the Horizon Mirage server cluster.

2 Install the Horizon Mirage Management Console on page 19

The Horizon Mirage Management console is the graphical user interface used to perform scalable maintenance, management, and monitoring of deployed endpoints. You install the Management console after you install the Horizon Mirage Management server. The Management console is built as a Microsoft Management Console version 3.0 snap-in.

3 Connect the Console to the Horizon Mirage System on page 20

After you install the Horizon Mirage Management console, you can connect the console to the Horizon Mirage system.

4 Install a Horizon Mirage Server on page 20

The Horizon Mirage server manages the storage and delivery of base and app layers and CVDs to clients, and consolidates monitoring and management communications. After you install and license the Horizon Mirage Management server, you can install Horizon Mirage servers.

5 Install IIS on page 23

You must install Windows Internet Information Services (IIS) 7.0 before installing the Horizon Mirage file portal or the Horizon Mirage Web Manager.

6 Configure IIS for SSL Support on page 24

All Horizon Mirage web applications such as File Portal, Admin File Portal, and Web Management require enabling SSL support for IIS.

7 Install the Horizon Mirage File Portal on page 24

Install the Horizon Mirage file portal so that end-users can view files in their CVD snapshots from a web browser. End-users can access the file portal with the appropriate login credentials.

8 Installing the Horizon Mirage Edge Server on page 26

The Horizon Mirage Edge server is a secured gateway server that is deployed outside the Mirage data center environment.

9 Managing Horizon Mirage Software Licenses on page 29

The Horizon Mirage Management server requires a license. The license file enforces the number of CVDs that you can run on your system and the duration of the license agreement.

10 Configure the Environment for Endpoints on page 30

Before you can attach endpoints to your system, you need to perform a minimum configuration, which includes configuring the file portal web URL, importing USMT settings, and perform domain joining operations.

# Install the Horizon Mirage Management Server

The Horizon Mirage Management server is the main component that controls and manages the Horizon Mirage server cluster.

The installation uses an `msi` file located in the Horizon Mirage installation package.

### Prerequisites

Verify that the relevant software requirements are met. See "Software Requirements," on page 14.

### Procedure

1 Double-click the `Mirage.management.server.x64.`*`buildnumber`*`.msi` file.

2 Type the SQL Server name and the SQL instance name.

SQLEXPRESS is defined as the default SQL instance for the SQL Server Express edition. However, you can just enter the server name without an SQL instance when using a default unnamed instance such as SQL Standard. Alternatively, you can type the SQL instance name that is configured in your environment.

Use the default SQL instance name if your MSSQL edition was installed with Default options, or the custom instance name if a custom name was defined.

| MSSQL Edition | Default SQL Instance Name |
|---|---|
| **Express** | SQLEXPRESS |
| **Standard** | Empty by default, but displayed as MSSQLSERVER in the MS SQL management console. |
| **Enterprise** | MSSQL |

NOTE You must have **db_creator** privileges on the SQL Server to create the Horizon Mirage database. The installation creates a database for the Mirage Management server called MirageDB. You need **dbo** permissions on the MirageDB database and be a local admin on the host with full access (read/write) privileges to the initial volume.

3 Set the remaining installation parameters.

| Option | Action |
|---|---|
| **Create new storage areas checkbox** | Select if this is a new installation of the system or if you do not want to keep the current data.<br>IMPORTANT Do not use the **Create new storage areas** option when upgrading the Mirage management server. If this option is used and the path of the original storage area is entered, your entire Mirage installation (Base Layer, App Layer, CVD data, and so on) will be deleted and permanently lost if a backup is not available. |
| **Name of Horizon Mirage Cluster storage folder** | When you create new storage areas, type the UNC path of the first volume to be created. Sharing privileges must be granted to access the storage.<br>The UNC path to the storage is required whenever Horizon Mirage is installed on more than one host, for example, when the Management server and one or more other servers are each on separate machines. The use of local storage, for example `E:\MirageStorage`, is supported for smaller environments where a single server is co-located on the same machine as the Management server. |

The installation might take a few minutes.

4 Click **Finish** to complete the installation.

The Horizon Mirage Management server is installed.

### What to do next

You can install the Horizon Mirage Management console. See "Install the Horizon Mirage Management Console," on page 19.

## Install the Horizon Mirage Management Console

The Horizon Mirage Management console is the graphical user interface used to perform scalable maintenance, management, and monitoring of deployed endpoints. You install the Management console after you install the Horizon Mirage Management server. The Management console is built as a Microsoft Management Console version 3.0 snap-in.

The installation uses an `.msi` file located in the Horizon Mirage distribution.

### Prerequisites

The End-User License Agreement appears during the installation. You must agree to its terms before you can complete the installation.

### Procedure

- Double-click the `.msi` file for your environment.

| Option | Description |
|---|---|
| **64-bit** | `Mirage.management.console.x64.buildnumber.msi` |
| **32-bit** | `Mirage.management.console.x86.buildnumber.msi` |

A shortcut to the Management console is added to your desktop when the installation is finished.

### What to do next

You can connect the console to the Horizon Mirage Management system. See "Connect the Console to the Horizon Mirage System," on page 20.

## Connect the Console to the Horizon Mirage System

After you install the Horizon Mirage Management console, you can connect the console to the Horizon Mirage system.

### Procedure

1. In the Horizon Mirage Management console tree, right-click **VMware Horizon Mirage** in the root directory and select **Add System**.
2. Type the IP address or host name of the Horizon Mirage Management server in the **Management Server Address** text box.
3. Click **OK**.

The Management console is connected to the system. A Horizon Mirage server node now appears in the console window.

After the console is connected, it shows Server Down status because a Horizon Mirage server is not yet installed. The server status changes to Up when a server is installed.

### What to do next

You can install a Horizon Mirage server. See "Install a Horizon Mirage Server," on page 20.

## Install a Horizon Mirage Server

The Horizon Mirage server manages the storage and delivery of base and app layers and CVDs to clients, and consolidates monitoring and management communications. After you install and license the Horizon Mirage Management server, you can install Horizon Mirage servers.

You can deploy multiple servers as a server cluster to manage endpoint devices for large enterprise organizations. With multiple servers and storage volumes, enterprise organizations can store, manage, and protect end-user device data for large numbers of managed endpoint devices. For more information, see Deploying Additional Horizon Mirage Servers in the *Horizon Mirage Administrator's Guide*.

The Horizon Mirage server uses Local Cache, a storage of popular data blocks, to perform data deduplication over the WAN. When large files are transferred, their blocks are kept in the cache, and the next time similar files need to be transferred, the server obtains the blocks from the cache instead of over the network. It is good practice to keep the cache on fast storage, for example, on a local drive or even on an SSD drive.

The server installation process includes the default option to set up SSL, which requires an SSL Certificate to be installed on the server. See "Install the Server SSL Certificate," on page 21.

If SSL is not implemented at server installation, you can also implement it after the server is installed. See Configuring Secure Socket Layer Communication in the *Horizon Mirage Administrator's Guide*.

**IMPORTANT** Disabling SSL encryption is not recommended as this mode of connection is not secure.

### What to do next

1 Install the server SSL Certificate. See "Install the Server SSL Certificate," on page 21.

2 Install the server. See "Install the Server," on page 21

## Install the Server SSL Certificate

To set up SSL on the Horizon Mirage server, you must obtain SSL certificate values and configure them on the server. SSL Certificates is a Windows feature.

**NOTE** Horizon Mirage does not support wildcard certificates on the Mirage server.

Both the Mirage server and the Mirage Edge server uses the local Computer Store. Ensure that the certificates are installed in the local Computer Trust Store.

### Procedure

1 Open the Windows Management Console, add the Certificates snap-in, and select the local computer account.

2 Select **Certificates > Personal > Certificates** to navigate to your certificate.

3 If you do not have a certificate, create one with tools such as the Microsoft makecert, and import the result into the Certificate Manager.

4 Note the **Certificate Subject** and **Issuer** values.

The certificate values appear in the details of the certificate you imported.

### What to do next

For the Horizon Mirage server, continue to the server installation procedure to enter the SSL certificate values. See "Install the Server," on page 21.

For the Horizon Mirage Edge server, continue to the Edge server installation procedure. See "Install the Horizon Mirage Edge Server," on page 27.

## Install the Server

Allocate a larger number of concurrent CVDs for high-end servers, or a smaller number for low-end servers. For more information about this modification, contact VMware Support.

The installation uses an `msi` file located in the Horizon Mirage installation package.

### Prerequisites

- The server installation process includes the default option to set up SSL, which requires an SSL Certificate to be installed on the server. See "Install the Server SSL Certificate," on page 21.
- Verify that the SQL server is reachable from the server node and the firewall settings on the SQL server allow for remote connections.

### Procedure

1 Double-click the `Mirage.server.x64.buildnumber.msi` file and click **Next** to start the wizard.

2 Accept the End-User License Agreement and click **Next**.

3 Provide the configuration information and click **Next**.

| Option | Action |
|---|---|
| **SQL Server and SQL Instance** | Type the server name and instance. |
| **Create new local cache area check box** | Select this to allocate a new local cache area. If not selected, the installer attempts to use existing cache data. |
| **Name of the Horizon Mirage Server local cache folder** | Type the path to where the local cache is stored, if different from the default.<br>Do not use the **Create new local cache area** option when upgrading the Mirage server. If this option is used and the path of the original storage area is entered, the local cache of the server itself is deleted. This may result in some short-time performance penalties as the cache has to be filled again. |
| **Size of local cache in MB** | Type the size of the cache in megabytes. A cache size of 100GB (102400) is recommended. |

4 Set the server maximum connections and SSL, and click **Next**

| Option | Action |
|---|---|
| **Port** | Change the port used for client-server communication. Either use the default port of 8000 or change the port. Changing the port might require adding firewall rules to open the port. |
| **Encryption Type** | ■ Select **SSL** to set the connection type to SSL to have clients communicate with the server using SSL encryption. This setting applies globally.<br>■ Select **None** for no encryption type. |

5 If you selected **SSL**, enter the Certificate subject and Issuer values.

| Option | Action |
|---|---|
| **Certificate Subject** | Typically the FQDN of the Horizon Mirage server. |
| **Certificate Issuer** | Usually a known entity like VeriSign. Leave this blank if only one certificate is on this server. |

6 Configure the Horizon Mirage services account and click **Next**.

| Option | Action |
|---|---|
| **Use Local System account** | Select if you are using a standalone server with local storage. |
| **Use specific user** | Select if you access CIFS share servers in a Horizon Mirage cluster environment. Type the user name and password (Windows credentials). |
| **User Account and password** | Type the account and password required to manage Horizon Mirage services. |

7 Click **Install** and click **Finish** to complete the server setup.

8 Restart the server when the installation is completed.

### What to do next

You can now install IIS and the Horizon Mirage File Portal.

## Install IIS

You must install Windows Internet Information Services (IIS) 7.0 before installing the Horizon Mirage file portal or the Horizon Mirage Web Manager.

The `msi` file used in the procedure is located in the Horizon Mirage installation package.

### Procedure

1 Install the IIS server role on the Windows Server 2008 R2 or later machine where the Horizon Mirage server software is installed.

In the Server Manager, select **Add Roles > Web Server (IIS)** to install the IIS server role.

2 After the IIS server role installation is finished, in the Server Manager, click **Add Role Services** and select and install the following services:

a Web Server Services:

| Category | Sub Items Required |
|---|---|
| **Common HTTP Features** | Static Content<br>Default Document<br>Directory Browsing<br>HTTP Errors |
| **Application Development** | ASP.NET<br>.NET Extensibility<br>ISAPI Extensions<br>ISAPI Filters |
| **Health And Diagnostics** | Nothing is required |
| **Security** | Request Filtering |
| **Performance** | Nothing is required |

b Management Tools:

| Category | Sub Items Required |
|---|---|
| **IIS Management Console** | All subitems are required |
| **IIS Management Scripts and Tools** | All subitems are required |
| **Management Service** | All subitems are required |
| **IIS 6 Management Compatibility** | All subitems are required |

### What to do next

Verify that the appropriate ports are enabled between IIS and the Horizon Mirage Management server. See "Ports and Protocols Used by Horizon Mirage," on page 15.

Before installing the Horizon Mirage File Portal or Web Management, you must configure IIS for SSL support. See "Configure IIS for SSL Support," on page 24.

# Configure IIS for SSL Support

All Horizon Mirage web applications such as File Portal, Admin File Portal, and Web Management require enabling SSL support for IIS.

### Procedure

1 To open the Internet Information Services (IIS) Manager:

   a Click the Windows **Start** button.

   b Click **Run**.

   c Type **`inetmgr`** and click **OK**.

2 In the Connections tree, click the IIS instance on which the Horizon Mirage web applications are installed.

3 Double-click the **Server Certificates** icon.

4 In the Actions menu, you can either create an SSL certificate (Domain Certificate or Self-Signed Certificate) or import an existing SSL certificate.

   For more information on how to create or import an SSL certificate, go to http://technet.microsoft.com/en-us/library/cc732230%28v=ws.10%29.aspx.

5 Right-click **Default Web Site** and select **Edit Bindings**.

6 Click **Add**.

7 In the Add Site Binding dialog box, enter the following information.

| Option | Description |
|---|---|
| **Type** | Select **https**. |
| **IP Address** | Select **All Unassigned**. |
| **Port** | Type 443. |
| **SSL certificate** | Select the type of SSL certificate that was created or imported. |

8 Click **OK**.

9 Click **Close**.

# Install the Horizon Mirage File Portal

Install the Horizon Mirage file portal so that end-users can view files in their CVD snapshots from a web browser. End-users can access the file portal with the appropriate login credentials.

The `msi` file used in the procedure is located in the Horizon Mirage installation package.

### Prerequisites

- Microsoft IIS 7.0 or later must be installed for the file portal. For more information about installing IIS, see "Install IIS," on page 23
- IIS must be configured for SSL support. For more information, see "Configure IIS for SSL Support," on page 24.

### Procedure

1 Double-click the `msi` file for your environment.

| Option | Description |
|---|---|
| **64-bit** | `mirage.WebAccess.x64.`*`buildnumber`*`.msi` |
| **32-bit** | `mirage.WebAccess.x86.`*`buildnumber`*`.msi` |

2 Click **Next** and provide the final configuration information.

| Option | Action |
|---|---|
| **EULA** | Accept the agreement and click **Next**. |
| **Horizon Mirage Web Access and Admin Web Access** | **Web Access** provides access to only an end-user's user files, as defined by the administrator, across all CVD snapshots.<br>**Admin Web Access** gives the administrator full access to all user CVDs across all CVD snapshots.<br>By default, both the **Web Access** and **Admin Web Access** web applications are configured for the File Portal. You can choose not to configure either of these options by clicking the drop-down menu and selecting **Entire feature will be unavailable**.<br>Click **Next**. |
| **VMware Horizon Mirage Management Server location** | Type the location of the VMware Horizon Mirage Management server and click **Next**. |

3 Click **Install** and click **Finish** when the installation is complete.

### What to do next

The Mirage client user can access the Web Access feature to only download their files at http://Server/Explorer.

The administrator can access the Admin Web Access feature to download all files of any user at http://server/AdminExplorer.

You can now continue to activate endpoints.

## Troubleshooting the File Portal Installation

Specific users might experience difficulty accessing the file portal.

### Problem

After the installation is finished, specific users might experience difficulty accessing the file portal.

### Cause

Difficulty to access the file portal can happen because of a local or domain security policy on IIS servers.

### Solution

1 On the IIS server machine where the file portal is installed, select **Local Security Policy > Local Policies > User Rights Assignments**

2 Add all users who need file portal access to the `Allow logon locally` policy.

# Installing the Horizon Mirage Edge Server

The Horizon Mirage Edge server is a secured gateway server that is deployed outside the Mirage data center environment.

The Horizon Mirage Edge server meets the enterprise security and firewall requirements and provides a better user experience for Mirage clients that access the Horizon Mirage servers through the Internet.

After installing the Horizon Mirage Edge server, you can add and configure an Edge server to your Horizon Mirage system using the Mirage Management console in the **System Configuration** node. For more information on adding and configuring the Horizon Mirage Edge server, see the *VMware Horizon Mirage Administrator's Guide*.

- Generate the Certificate Signing Request for the Horizon Mirage Edge Server on page 26

  When you set up the SSL certificate for the Horizon Mirage Edge server, you must first generate the Certificate Signing Request (CSR).

- Install the Horizon Mirage Edge Server on page 27

  Install the Horizon Mirage Edge server to secure your data center environment for users that communicate with the corporate enterprise data center via Internet.

- Start or Stop the Horizon Mirage Edge Server on page 29

  After installing the Horizon Mirage Edge server, the Horizon Mirage Edge service is running on the Microsoft Computer Management service. The service name is *VMwareHorizon Mirage Edge Server*.

## Generate the Certificate Signing Request for the Horizon Mirage Edge Server

When you set up the SSL certificate for the Horizon Mirage Edge server, you must first generate the Certificate Signing Request (CSR).

You can use the OpenSSL tool or the makecert tool to generate the CSR.

To generate a CSR using the Windows Management Console, perform the following procedure.

### Procedure

1. On the Horizon Mirage Edge server, open the Windows Management Console, add the Certificates snap-in, and select the local computer account.
2. Open the certificate snap-in, right-click the Personal store node and select **All Tasks > Advanced Operations > Create Custom Request**.
3. In the custom request area, select **Proceed without enrollment policy**.

| Option | Description |
|---|---|
| **Custom Request** | Select **Proceed without enrollment policy**. |
| **Template** | Select **Legacy Key**. |
| **Request Format** | Accept the default settings for the PKCS #10 text boxes. |
| **Certificate Information** | Click **Details** for the Custom Request and click **Properties**. |

4. Click the **General** tab and type a certificate-friendly name.

   You can use the same name as the subject name.

5 Click the **Subject** tab, and in the **Subject Name** area, provide the relevant certificate information.

| Option | Description |
|---|---|
| **Common name, value** | Server FQDN. This is the certificate subject name that is used in the Horizon Mirage configuration to find the certificate. The FQDN must point to that server and is validated by the client upon connection. |
| **Organization, value** | Company name, usually required by the CA. |
| **Country, value** | Two-letter standard country name, for example, US or UK. Usually required by the CA. |
| **State, value** | State name. |
| **Locality, value** | City name. |

6 Click the **Extensions** tab and select the key use information from the pull-down menus.

| Option | Description |
|---|---|
| **Key Usage** | Select **Data Encipherment**. |
| **Extended Key Usage** | Select **Server Authentication**. |

7 Click the **Private Key** tab and select key size and export options.

| Option | Description |
|---|---|
| **Key Options** | Select the required key size (usually 1024 or 2048). |
| **make Private Key Exportable** | Select to export the CSR, and later the certificate, with the private key for backup or server movement purposes. |
| **Key Type** | Select **exchange** (the default value is **signature**). |

8 Click **OK** to close the Certificate Properties window, and click **Next** in the Certificate Enrollment wizard.

9 Leave the default file format (Base 64), and click **Browse** to select a file name and location of where to save the CSR. The certificate request is completed.

10 Click the **Certificates Enrollments & Certificates** tab and click **Refresh.**

You can export the CSR with the private key for backup purposes.

### What to do next

After generating the Certificate Signing Request, continue with installing the server SSL certificate for the Edge server. See "Install the Server SSL Certificate," on page 21.

## Install the Horizon Mirage Edge Server

Install the Horizon Mirage Edge server to secure your data center environment for users that communicate with the corporate enterprise data center via Internet.

The installation uses an `.msi` file located in the Horizon Mirage distribution package.

### Prerequisites

Ensure that the Horizon Mirage server, Mirage Management console, and the Mirage Management Server have been installed before installing the Horizon Mirage Edge server.

Additionally, ensure that the Corporate Directory Service Information (LDAP server) is configured to be used for the Horizon Mirage Edge server.

Before installing the Horizon Mirage Edge server, ensure that you have generated the Certificate Signing Request and installed the certificate SSL for the Edge server. See "Generate the Certificate Signing Request for the Horizon Mirage Edge Server," on page 26.

The End-User License Agreement appears during the installation process. You must agree to its terms before you can complete the installation.

### Procedure

1 Double-click the `MirageEdgeServer.buildnumber.msi` file and click **Next** to start the wizard.

2 Accept the End-User License Agreement and click **Next**.

3 Provide the location of the folder to where you want to install the Horizon Mirage Edge Server.

4 Provide the following configuration information for the Horizon Mirage Edge Server and click **Next**.

| Option | Action |
|---|---|
| **IP address or FQDN and port number of the LDAP Server** | Type the IP address or the FQDN and the port number of the LDAP server. |
| **Use LDAPS** | Select this option to use a secured LDAP server using TLS/SSL. |
| **Token expiration time (in hours)** | Type the login token expiration time in hours.<br>The login token determines how frequent the end-users will be requested to log in to the Edge server. |
| **IP address or hostname and port number of the Mirage server** | Type the IP address or the hostname and the port number of the Mirage server that will be connected to the Edge server.<br>NOTE When using a third party load balancer, type the IP address of the load balancer. |
| **Subject of the Mirage Edge Server certificate** | Type a subject name for the Edge server certificate. |

5 Set the user account configuration to run the Horizon Mirage Edge Server and click **Next**.

| Option | Action |
|---|---|
| **User Name** | Type the fully qualified name of the account to run the Horizon Mirage Edge services |
| **Password** | Type the password of the account to run the Horizon Mirage Edge services |

6 Type the Mirage Edge Server activation code that is a random number set by the administrator. Retype the activation code again, and click **Next**.

NOTE You will need to keep this activation code. The activation code is required when you add an Edge server in the Mirage Management console.

7 Click **Install** to install the Horizon Mirage Edge Server.

8 Click **Finish** to exit the setup wizard.

### What to do next

You can now add and configure the Horizon Mirage Edge server to your environment. For more information, see the *Horizon Mirage Administrator's Guide*.

## Start or Stop the Horizon Mirage Edge Server

After installing the Horizon Mirage Edge server, the Horizon Mirage Edge service is running on the Microsoft Computer Management service. The service name is *VMwareHorizon Mirage Edge Server*.

When the service is started, the following processes are running:

- `MirageEdgeService.exe *32`
- `MirageEdgeServer.exe *32`
- `MirageEdgeServer.exe *32`

**NOTE** There can be several `MirageEdgeServer.exe` processes running. The `MirageEdgeService.exe` is the main Edge server process. The other processes are used as working processes for the Mirage server.

### Procedure

- Stop or start the Horizon Mirage Edge server using the `services.msc` command.

# Managing Horizon Mirage Software Licenses

The Horizon Mirage Management server requires a license. The license file enforces the number of CVDs that you can run on your system and the duration of the license agreement.

Individual Horizon Mirage servers do not need licenses.

Software licenses are separate from the server installation package.

You can view the license details at any time. See "Add and View Licenses," on page 29.

When the license expiration date is reached, all management actions are disabled but the administrator can still view the system status and track operation status. Mirage endpoint-related functions, including backup, restore, and image management operations continue, so that clients can still upload changes to the CVD on the server.

When a license expires, or when the system is installed, a dialog box appears when you open the Management console, where you can type the license key. An audit event is created.

When you need a new license, contact VMware.

## Add and View Licenses

The license file enforces the number of CVDs that you can run on your system and the duration of the license agreement. You can view the current license details at any time.

You can add a license or view the number of CVDs currently licensed and the license expiry date through system configuration settings.

If your license expires, or when the system is installed, a dialog box appears when you open the Management console, where you can type the license key.

You do not need to restart the Horizon Mirage Management server to update the license.

### Procedure

1. In the Management console tree, right-click **System Configuration**, select **Settings**, and click the **License** tab.
2. Type or copy and paste the serial key in the **Use license key** text box.
3. Click **OK**.

# Configure the Environment for Endpoints

Before you can attach endpoints to your system, you need to perform a minimum configuration, which includes configuring the file portal web URL, importing USMT settings, and perform domain joining operations.

For information about importing USMT files, see Import USMT Settings in the *Horizon Mirage Administrator's Guide*.

For Join Domain Account information, see General System Settings in the *Horizon Mirage Administrator's Guide*.

### Prerequisites

Verify that a Horizon Mirage server is installed.

### Procedure

1 (Optional) Configure the File Portal Web URL.

2 (Optional) If you need to perform migration operations, import the USMT folder.

3 (Optional) If you need to perform domain joining operations, provide Join Domain Account details.

### What to do next

You can now continue to configure and use your Horizon Mirage system.

# Index