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.
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
Updated Information

This VMware Mirage Installation Guide is updated with each release of the product or when necessary. This table provides the update history of the VMware Mirage Installation Guide.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Updated the command for installing the Mirage Gateway server. See “Install the Mirage Gateway Server,” on page 35.</td>
</tr>
<tr>
<td>00</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
Mirage Installation

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

Installing the system involves installing the Mirage Management server, console, and server components, and associated applications that facilitate, for example, file portal access.

Intended Audience

This information is intended for anyone who wants to install 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.
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 Mirage components integrate into a typical distributed infrastructure, with the following relationships between the system components:

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

**Figure 1-1. System Components**
Mirage Client
The Mirage client software runs on 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 Mirage client software can run on any Type 1 or Type 2 hypervisor.

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

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

The administrator can use the Mirage Management console to configure and manage Mirage clients, base layers, app layers, and reference machines. The administrator uses the Mirage Management console to update and restore CVDs.

Mirage Web Manager
The Mirage Web Manager lets help desk personnel respond to service queries, and lets the Protection Manager role ensure that user devices are protected. The Web Manager mirrors Mirage Management console functionality. For more information, see the VMware Mirage Web Manager Guide.

Mirage Server
The Mirage servers, located in the data center, synchronize data between the Mirage client and the datacenter. The Mirage servers also 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 run on the same machine as the Mirage Management server.

The server machine must be dedicated for the Mirage server software to use. The server machine must not be used for other purposes.

Centralized Virtual Desktop
CVDs represent the complete contents of each PC. This data is migrated to the Mirage server and becomes the 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 several components.
Table 1-1. CVD Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Defined By (Role)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base layer</td>
<td>Administrator</td>
<td>The base layer includes the operating system (OS) image and 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.</td>
</tr>
<tr>
<td>App layers</td>
<td>Administrator</td>
<td>App layers include sets of one or more departmental or line-of-business applications, and any updates or patches for already installed applications. App layers are suitable for deployment to a large number of endpoints.</td>
</tr>
<tr>
<td>Driver profile</td>
<td>Administrator</td>
<td>The driver profile 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.</td>
</tr>
<tr>
<td>User-installed applications and machine state</td>
<td>End users</td>
<td>User-installed applications and machine state can include a unique identifier, host name, any configuration changes to the machine registry, DLLs, and configuration files.</td>
</tr>
</tbody>
</table>

**Mirage Reference Machine**

A 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, patches, corporate applications for all target end users to use, corporate configurations, and policies. A reference machine is also used 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 regularly over the LAN or WAN, using a 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.

**Mirage Branch Reflector**

A 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 Mirage server cluster. A branch reflector can significantly reduce bandwidth use in several situations, such as during mass base or app layer updates. The branch reflector also assists in downloading hardware drivers.

**Mirage File Portal**

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

The Distributed Desktop Optimization mechanism optimizes transport of data between the Mirage server and clients, making the ability to support remote endpoints feasible 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.

Mirage Gateway Server

The Mirage Gateway server is the secure gateway server that is deployed outside the Mirage data center environment, but should be within the datacenter. The Mirage Gateway server meets the enterprise security and firewall requirements and provides a better user experience for Mirage clients that access the Mirage servers through the Internet. The Mirage Gateway server seamlessly integrates with the Mirage system with minor modifications to the Mirage system and protocol.
Deploying the Mirage system involves ensuring that various requirements of its hardware components, the Mirage Management server, Mirage Management console, Mirage server components, and associated software applications, are satisfied.

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

This chapter includes the following topics:

- “Operating System Requirements,” on page 13
- “Hardware Requirements,” on page 14
- “Software Requirements,” on page 16
- “Database Requirements,” on page 16
- “Ports and Protocols Used by Mirage,” on page 17

### Operating System Requirements

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

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage client</td>
<td>- Windows XP Professional with SP3, 32-bit</td>
</tr>
<tr>
<td></td>
<td>- Windows Vista Business or Enterprise, 32-bit and 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Windows 7 Professional or Enterprise, 32-bit and 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Windows 8.0 and 8.1 Professional or Enterprise, 32-bit and 64-bit</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Windows XP Fast User Switching mode must be disabled if the computer is not an AD domain member.</td>
</tr>
<tr>
<td>Mirage server</td>
<td>- Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>- Domain membership required.</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>- Domain membership required.</td>
</tr>
</tbody>
</table>
Table 2-1. Operating System Requirements for Mirage Components (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage Management console</td>
<td>- Windows XP Professional with SP3, 32-bit</td>
</tr>
<tr>
<td></td>
<td>- Windows Vista Business or Enterprise, 32-bit and 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Windows 7 Professional or Enterprise, 32-bit and 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Windows 8.0 and 8.1 Professional or Enterprise, 32-bit and 64-bit</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Windows XP Fast User Switching mode must be disabled if the computer is not an AD domain member.</td>
</tr>
<tr>
<td>Mirage reference machine</td>
<td>- Windows XP Professional with SP3, 32-bit</td>
</tr>
<tr>
<td></td>
<td>- Windows 7 Professional or Enterprise, 32-bit and 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2012 R2</td>
</tr>
</tbody>
</table>

Hardware Requirements

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

Table 2-2. Hardware Requirements for Mirage Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage client</td>
<td>- Client systems:</td>
</tr>
<tr>
<td></td>
<td>- Enterprise-class laptops and desktops</td>
</tr>
<tr>
<td></td>
<td>- Virtual machines compatible with Windows XP SP2 or later, Windows Vista or Windows 7</td>
</tr>
<tr>
<td></td>
<td>- Minimum RAM: 512 MB for Windows XP, 1 GB for Windows Vista, Windows 7, Windows 8, and Windows 8.1</td>
</tr>
<tr>
<td></td>
<td>- Client installation and normal operation: At least 5 GB of free space</td>
</tr>
<tr>
<td>Mirage server node (up to 1000 clients)</td>
<td>- Minimum RAM: 8 GB</td>
</tr>
<tr>
<td></td>
<td>- Minimum CPU: 4 vCPU</td>
</tr>
<tr>
<td></td>
<td>- Minimum System Drive capacity: 146 GB, including 100 GB for the Mirage network cache</td>
</tr>
<tr>
<td></td>
<td>Mirage SIS storage is not included.</td>
</tr>
<tr>
<td></td>
<td>- 2 x Gigabit Ethernet Port</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: It is good practice to separate client network and storage network access to dedicated ports.</td>
</tr>
<tr>
<td>Mirage server node (up to 1500 clients)</td>
<td>- Minimum RAM: 16 GB</td>
</tr>
<tr>
<td></td>
<td>- Minimum CPU: 8 vCPU or dual Quad-Core Processor, 2.26 GHz Intel core speed</td>
</tr>
<tr>
<td></td>
<td>- Minimum System Drive capacity: 146 GB, including 100 GB for the Mirage network cache</td>
</tr>
<tr>
<td></td>
<td>Mirage SIS storage is not included.</td>
</tr>
<tr>
<td></td>
<td>- 2 x Gigabit Ethernet Port</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: It is good practice to separate client network and storage network access to dedicated ports.</td>
</tr>
</tbody>
</table>
### Table 2-2. Hardware Requirements for Mirage Components (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Mirage storage          | - Standalone Mirage server:  
  - Direct Attached Storage (DAS)  
  - Storage Area Network (SAN) connected through iSCSI or Fiber Channel (FC)  
  - Network Attached Storage (NAS) connected through iSCSI, Fiber Channel (FC), or CIFS network share  
  - 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.  
  - Alternate Data Streams: NAS through CIFS share must support Alternate Data Streams. To verify that the NAS device conforms with the Mirage requirements, use the `Wanova.Server.Tools.exe NasCompatibilityTest`. See the VMware knowledge base article at [http://kb.vmware.com/kb/2070000](http://kb.vmware.com/kb/2070000)  |
|                         | - Storage Capacity: Consumed capacity varies, depending on file duplication level across CVDs, base layers, and the number of snapshots stored, but on average, each user requires 15 GB of data center storage.  
  - 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 .  
  - Enabling Compression: For DAS, SAN (FC, iSCSI), and Windows-based NAS (CIFS shares), you can 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 the systems' compression options.  
  - **Note**: Apply this change only when Mirage services are stopped. Also consider making this change before the directory is heavily populated . |
| Mirage Management Server| - Minimum RAM: 8 GB.  
  - Minimum CPU: 1 Quad-Core Processor or 4 vCPUs in virtual configuration, 2.26GHz Intel core speed or equivalent |
| Mirage Management console| - Minimum RAM: 512 MB.  
  - Network connectivity to the Mirage Management server  
  - Minimum screen resolution: 1280 x 1024 |
| Mirage File Portal      | - Minimum RAM: 512 MB.  
  - Network connectivity to the Mirage Management server  
  - Minimum screen resolution: 1280 x 1024 |
| Mirage Web Management Console| - Minimum RAM: 512 MB.  
  - Network connectivity to the Mirage Management server  
  - Minimum screen resolution: 1280 x 1024 |
| Mirage Gateway server   | - 4 core CPU, 2.26 GHz Intel core speed or equivalent  
  - 4 GB RAM  
  - 40 GB available disk space  
  - 1 x Gigabit Ethernet port |
| Microsoft SQL Server 2012| Use the recommended Microsoft Hardware and Software Requirements for Installing SQL Server 2012. |
| Microsoft SQL Server 2008 R2 | Use the recommended Microsoft Hardware and Software Requirements for Installing SQL Server 2008 R2. |
Software Requirements

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

Table 2-3. Software Requirements for Mirage Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage client</td>
<td>Microsoft .NET Framework version 3.5 SP1</td>
</tr>
<tr>
<td>Mirage server</td>
<td>- Microsoft .NET Framework version 3.5 SP1 64-bit</td>
</tr>
<tr>
<td></td>
<td>- For the file portal, 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.</td>
</tr>
<tr>
<td>Mirage Management server</td>
<td>Microsoft .NET Framework version 3.5 SP1 64-bit.</td>
</tr>
<tr>
<td>Mirage Management console</td>
<td>- Microsoft .NET Framework version 3.5 SP1</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Management Console version 3.0 or later</td>
</tr>
<tr>
<td>Mirage reference machine</td>
<td>- Mirage client.</td>
</tr>
<tr>
<td></td>
<td>- The OS and applications installed on the reference machine must use volume licenses and be designed for multiuser and multimachine deployment.</td>
</tr>
<tr>
<td></td>
<td>- Verify that the reference machine does not include the following items:</td>
</tr>
<tr>
<td></td>
<td>- Applications that install and use hardware-specific licenses.</td>
</tr>
<tr>
<td></td>
<td>- Applications that install and use local user accounts, local groups, or both.</td>
</tr>
<tr>
<td></td>
<td>- Software that uses a proprietary update service. Such software must be installed directly on endpoints.</td>
</tr>
<tr>
<td>Mirage file portal</td>
<td>- Microsoft IIS 7 or later</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Microsoft .NET Framework version 3.5 SP1</td>
</tr>
<tr>
<td>Mirage Web Manager</td>
<td>- Microsoft IIS 7.0 or later</td>
</tr>
<tr>
<td></td>
<td>- Microsoft .NET Framework 4.0</td>
</tr>
<tr>
<td>Mirage Gateway server</td>
<td>- Microsoft .NET Framework version 3.5.1</td>
</tr>
</tbody>
</table>

Database Requirements

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

Table 2-4. Database Software Requirements for Mirage Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database software</td>
<td>- Windows Installer 4.5 (MS KB942288) or later</td>
</tr>
<tr>
<td></td>
<td>- Microsoft SQL Server 2012 SP1 Express, Standard, and Enterprise editions</td>
</tr>
<tr>
<td></td>
<td>- Microsoft SQL Server 2008 64-bit R2 Express, Standard, and Enterprise editions</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you install SQL Server 2008 R2 on Windows Server 2012, you must install Service Pack 1 or later.</td>
</tr>
<tr>
<td></td>
<td>MS SQL Server must be set up with Windows Authentication. The Windows account used for installing Mirage must have <strong>dbcreator</strong> privileges, and the user account running the Mirage server services must be configured with access privileges to the Mirage database.</td>
</tr>
</tbody>
</table>
Database Sizing Requirements

Table 2-5. Mirage Database Sizing Guidelines

<table>
<thead>
<tr>
<th>Mirage Cluster Size</th>
<th>Minimum System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage cluster with fewer than 5000 endpoints</td>
<td>Microsoft SQL Server 2008 Express R2 or Microsoft SQL Server 2012 Express</td>
</tr>
<tr>
<td></td>
<td>At least one CPU, 2.0 GHz or faster</td>
</tr>
<tr>
<td></td>
<td>At least 1 GB RAM</td>
</tr>
<tr>
<td>Mirage cluster with more than 5000 endpoints</td>
<td>Microsoft SQL Server 2008 Standard R2 or Microsoft SQL Server 2012 Standard</td>
</tr>
<tr>
<td></td>
<td>At least two CPUs, 2.0 GHz or faster</td>
</tr>
<tr>
<td></td>
<td>At least 4 GB RAM</td>
</tr>
</tbody>
</table>

The database sizing requirements for Mirage are based on the Microsoft hardware and software requirements for installing SQL Server 2008 R2.

Ports and Protocols Used by Mirage

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

The Mirage Management server and Mirage servers use external communications to communicate with the Mirage clients or the Mirage Management console, and internal communications to communicate with each other.

Table 2-6. Ports and Protocols for Mirage Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Communications</th>
<th>Port</th>
<th>Protocol</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage service</td>
<td>External</td>
<td>8000</td>
<td>TCP/IP or SSL/TLS</td>
<td>The only port required for communications between Mirage clients and servers. Note SSL/TLS is optional and can be enabled. See &quot;Install the Server SSL Certificate,&quot; on page 23.</td>
</tr>
<tr>
<td>Mirage Branch Reflector</td>
<td>External</td>
<td>8001</td>
<td>TCP/IP</td>
<td>Used for communication between the branch reflector and the local peers at the remote site.</td>
</tr>
<tr>
<td>Mirage Management service</td>
<td>External</td>
<td>8443 ,1443</td>
<td>TCP/IP</td>
<td>Used for communication between the Mirage Management console and the Mirage Management service. SOAP Message-level Security is applied.</td>
</tr>
<tr>
<td>Mirage Server service</td>
<td>Internal</td>
<td>135 ,445</td>
<td>TCP/IP</td>
<td>Used for control communication between the Mirage Management service and the Mirage server. Note You can limit access to this port to incoming connections from the Mirage Management service host.</td>
</tr>
<tr>
<td>File Portal</td>
<td>Internal</td>
<td>6080 ,6443</td>
<td>TCP/IP</td>
<td>Used for communication between the IIS server and the Mirage Management server.</td>
</tr>
<tr>
<td>Mirage Gateway server</td>
<td>Internal</td>
<td>8000</td>
<td>TCP/IP</td>
<td>Used for communication between the Mirage Gateway server and the Mirage server. Note The port must have DNS update access.</td>
</tr>
<tr>
<td></td>
<td>Internal</td>
<td>389 ,636</td>
<td>TCP/IP LDAP or LDAPS</td>
<td>Used for communications between the Mirage Edge server and the LDAP servers.</td>
</tr>
</tbody>
</table>
Table 2-6. Ports and Protocols for Mirage Components (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Communications</th>
<th>Port</th>
<th>Protocol</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>1001</td>
<td>TCP/IP</td>
<td>Used for communications between the Mirage server and the Mirage MMC console.</td>
<td></td>
</tr>
<tr>
<td>External</td>
<td>8000</td>
<td>TLS/SSL</td>
<td>Used for communication between the Mirage client and the Mirage Edge server.</td>
<td></td>
</tr>
</tbody>
</table>
Installing the Mirage System

The 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.
- Verify that you have a valid license for the system.
- Verify that the latest version of the 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.
- Prepare the required database information, or install a new database instance to use with Mirage.
- Verify that antivirus software running on the server machine excludes 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.
- You must have **dbcreator** privileges to create the Mirage database in the SQL express database. If you do not have these privileges, ask the database administrator to create the database and then designate you as the database creator.

**Procedure**

1. **Worksheet for Installing the Mirage Management Server** on page 21
   When you install the Mirage Management server, the installation wizard prompts you to configure certain options. You must prepare your configuration options before you install the Management server.

2. **Install the Mirage Management Server** on page 21
   The Mirage Management server is the component that controls and manages the Mirage server cluster.

3. **Install a Mirage Server** on page 22
   The 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 Mirage Management server, you can install Mirage servers.

4. **Install IIS** on page 25
   You must install Windows Internet Information Services (IIS) 7.0 before installing the Mirage file portal or the Mirage Web Manager.
5 Install the Web Manager on page 26
You install the Mirage Web Manager using the Web Manager .msi file provided in the installation package.

6 Install the Mirage File Portal on page 27
Install the 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.

7 Install the Mirage Management Console on page 28
The Mirage Management console is the graphical user interface used to perform scalable maintenance, management, and monitoring of deployed endpoints. The Management console is built as a Microsoft Management Console version 3.0 snap-in.

8 Connect the Console to the Mirage System on page 29
After you install the Mirage Management console, you can connect the console to the Mirage system.

9 Installing the Mirage Gateway Server on page 29
The Mirage Gateway server is a secured gateway server that is deployed outside the Mirage data center environment.

10 Managing Mirage Software Licenses on page 36
The 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.

11 Configure the Environment for Endpoints on page 36
Before you can attach endpoints to your system, you need to perform a minimum configuration, which includes configuring the Web URL for the file portal, importing USMT settings, and performing domain joining operations.
Worksheet for Installing the Mirage Management Server

When you install the Mirage Management server, the installation wizard prompts you to configure certain options. You must prepare your configuration options before you install the Management server.

Table 3-1. Configuration Options for Installing the Mirage Management Server

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL server name and instance</td>
<td>Select the SQL server name and instance.</td>
<td>- SQLEXPRESS is defined as the default SQL instance for the SQL Server Express edition.</td>
</tr>
<tr>
<td></td>
<td>- You can type 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.</td>
<td>- MSSQL is defined as the default SQL instance for the SQL Server Enterprise edition.</td>
</tr>
<tr>
<td></td>
<td>- Use the default SQL instance name if your Microsoft SQL Server edition was installed with default options, or the custom instance name if you defined a custom name.</td>
<td>- Use the default SQL instance name if your Microsoft SQL Server edition was installed with default options, or the custom instance name if you defined a custom name.</td>
</tr>
<tr>
<td>Storage areas</td>
<td>Use the Create new storage areas option if this is a new installation of the system or if you do not want to keep the current data.</td>
<td>Do not select the Create new storage areas check box when upgrading the Mirage Management server. If you select this option and enter the path to the original storage area, your entire Mirage installation, including base layer, app layer, CVD data, and so on, are deleted and become irretrievable if a backup is unavailable.</td>
</tr>
<tr>
<td>Services account configuration</td>
<td>You can use a local system account or a specific user account.</td>
<td>Use of a specific user account requires use of login credentials.</td>
</tr>
</tbody>
</table>

Install the Mirage Management Server

The Mirage Management server is the component that controls and manages the Mirage server cluster. The .msi installation file is located in the Mirage installation package.

Prerequisites

- You must have db_creator privileges on the SQL Server to create the Mirage database.
The installation creates the MirageDB database for the Mirage Management server. You need **dbo** permissions on the MirageDB database, and be a local administrator on the host with **read-write access** privileges to the initial volume.

Verify that the relevant software requirements are met. See “Software Requirements,” on page 16

**Procedure**

1. Double-click the `mirage.management.server.64x.msi` file to start the installation wizard.
2. Follow the prompts in the wizard to install the Mirage Management server.
   
   Use the configuration information that you gathered in the worksheet.

The Mirage Management server is installed.

**What to do next**

The SQL server recovery model must be set to simple.

You can install a Mirage server. See “Install a Mirage Server,” on page 22.

---

**Install a Mirage Server**

The 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 Mirage Management server, you can install Mirage servers.

You can deploy multiple servers as a server cluster to manage endpoint devices for large 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 Mirage Servers in the *VMware Mirage Administrator’s Guide*.

The 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 23.

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

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

**Procedure**

1. **Install the Server SSL Certificate** on page 23
   
   To set up SSL on the Mirage server, you must obtain SSL certificate values and configure them on the server. SSL certificates is a Windows feature.

2. **Worksheet for Installing the Mirage Server** on page 24
   
   When you install the Mirage server, the installation wizard prompts you to configure certain options. Prepare your configuration options before you install the Mirage server.

3. **Install the Mirage Server** on page 25
   
   The Mirage servers manage the storage and delivery of base layers, app layers, and CVDs to clients, and consolidate communications for monitoring and management. You can deploy multiple servers as a server cluster to manage endpoint devices for large enterprise organizations.
Install the Server SSL Certificate

To set up SSL on the Mirage server, you must obtain SSL certificate values and configure them on the server. SSL certificates is a Windows feature. The Mirage server uses the local computer store.

Prerequisites

Ensure that the certificates are installed in the local Computer Trust Store. If you do not have a certificate, you can create one with tools such as the Microsoft MakeCert. You must then import the result into the Certificate Manager.

Procedure

1. Open the Windows Management Console, add the Certificates snap-in, and select the local computer account.
2. To navigate to your certificate, select Certificates > Personal > Certificates.
3. Note the Certificate Subject and Certificate Issuer values.

What to do next

For the Mirage server, continue to the server installation procedure to enter the SSL certificate values. See Install the Mirage Server.
Worksheet for Installing the Mirage Server

When you install the Mirage server, the installation wizard prompts you to configure certain options. Prepare your configuration options before you install the Mirage server.

### Table 3-2. Configuration Options for Installing the Mirage Server

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL server name and instance</td>
<td>Select the SQL server name and instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SQLEXPRESS is defined as the default SQL instance for the SQL Server Express edition.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- You can type 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- MSSQL is defined as the default SQL instance for the SQL Server Enterprise edition.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Use the default SQL instance name if your Microsoft SQL Server edition was installed with default options, or the custom instance name if you defined a custom name.</td>
<td></td>
</tr>
<tr>
<td>Local cache areas</td>
<td>Select the Create new local cache area check box to allocate a new local cache area. If not selected, the installer attempts to use existing cache data. Do not select the Create new storage areas check box when upgrading the Mirage server. If you select this option and the path of the original storage area is entered, the local cache of the server itself is deleted. This might result in short-time performance penalties as the cache has to be refilled.</td>
<td></td>
</tr>
<tr>
<td>Name of the Mirage server local cache folder</td>
<td>The path to where the local cache is stored if different from the default. A default path is provided.</td>
<td></td>
</tr>
<tr>
<td>Size of local cache in MB</td>
<td>A cache size of 100GB (102400MB) is recommended.</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>The default port for client-server communication is 8000. If you change the port, additional firewall rules might be required to open the port.</td>
<td></td>
</tr>
</tbody>
</table>
Table 3-2. Configuration Options for Installing the Mirage Server (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption type</td>
<td>You can select to have an SSL certificate to have clients communicate with the server using SSL encryption. SSL encryption requires the Certificate Subject and Certificate Issuer values. Typically, the Certificate Subject is the FQDN of the Mirage server, and the Certificate Issuer is a known entity like VeriSign. You can leave the Certificate Issuer text box blank if only one certificate is installed on this server.</td>
</tr>
<tr>
<td>Services account configuration</td>
<td>You can use a local system account, or you can use a specific user account for your services account. Select the specific user account if you access CIFS share servers in a Mirage cluster environment. This option requires Windows login credentials.</td>
</tr>
</tbody>
</table>

Install the Mirage Server

The Mirage servers manage the storage and delivery of base layers, app layers, and CVDs to clients, and consolidate communications for monitoring and management. You can deploy multiple servers as a server cluster to manage endpoint devices for large enterprise organizations.

You can allocate a larger number of concurrent CVDs for high-end servers, or a smaller number for low-end servers.

The .msi installation file is located in the Mirage installation package.

**Prerequisites**

- Verify that the SQL server is reachable from the server node, and that the firewall settings on the SQL server allow for remote connections.

**Procedure**

1. Double-click the mirage.server.64x.msi file to start the installation wizard.
2. Follow the prompts in the wizard to install the Mirage server.
   - Use the configuration information that you gathered in the worksheet.
3. Restart the server when the installation is completed.

**What to do next**

You can now install IIS and the Mirage Web Manager.

Install IIS

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

The .msi installation file is located in the Mirage installation package.
Procedure

1. Install the IIS server role on the Windows Server 2008 R2 or later machine where the Mirage server software is installed.
   a. In the Server Manager, right-click the Roles node and select Add Roles.
   b. On the left-panel menu, select Server Roles.
   c. Select the Web Server (IIS) check box.

2. After the IIS server role is installed, install Web Service (IIS) services.
   a. Expand the Roles node and select Web Server (IIS).
   b. On the right panel, click Add Role Services.
   c. Expand the Web Server node and add these services.

<table>
<thead>
<tr>
<th>Role Service</th>
<th>Required Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common HTTP Features</td>
<td>Static Content</td>
</tr>
<tr>
<td></td>
<td>Default Document</td>
</tr>
<tr>
<td></td>
<td>Directory Browsing</td>
</tr>
<tr>
<td></td>
<td>HTTP Errors</td>
</tr>
<tr>
<td></td>
<td>HTTP Redirection</td>
</tr>
<tr>
<td>Application Development</td>
<td>ASP.NET</td>
</tr>
<tr>
<td></td>
<td>.NET Extensibility</td>
</tr>
<tr>
<td></td>
<td>ISAPI Extensions</td>
</tr>
<tr>
<td></td>
<td>ISAPI Filters</td>
</tr>
<tr>
<td>Health And Diagnostics</td>
<td>There are no required items for this role service.</td>
</tr>
<tr>
<td>Security</td>
<td>Request Filtering</td>
</tr>
<tr>
<td>Performance</td>
<td>There are no required items for this role service.</td>
</tr>
</tbody>
</table>

3. Install Management Tools services.
   a. Expand the Roles node and select Web Server (IIS).
   b. On the right panel, click Add Role Services.
   c. Expand the Management Tools node and add these services.

<table>
<thead>
<tr>
<th>Role Service</th>
<th>Required Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIS Management Console</td>
<td>All subitems are required</td>
</tr>
<tr>
<td>IIS Management Scripts and Tools</td>
<td>All subitems are required</td>
</tr>
<tr>
<td>Management Service</td>
<td>All subitems are required</td>
</tr>
<tr>
<td>IIS 6 Management Compatibility</td>
<td>All subitems are required</td>
</tr>
</tbody>
</table>

What to do next

Verify that the appropriate ports are enabled between IIS and the Mirage Management server. See “Ports and Protocols Used by Mirage,” on page 17.

Install the Web Manager

You install the Mirage Web Manager using the Web Manager .msi file provided in the installation package.

The .msi installation file is located in the Mirage installation package.
Prerequisites

- You must enable Cookies and JavaScript.
- The Mirage Web Manager must be installed on a Windows server with IIS 7 or later and .NET Framework 4.
- You can view the Web Manager using Microsoft Internet Explorer 9 and later, Chrome, and Firefox.
- Make sure that your Microsoft Internet Explorer browser supports JavaScript and Cookies on an intranet environment.

Procedure

1. Double-click the .msi file for your environment and click Run to start the installation wizard.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit</td>
<td>mirage.WebManagement.x64.buildnumber.msi</td>
</tr>
<tr>
<td>32-bit</td>
<td>mirage.WebManagement.x86.buildnumber.msi</td>
</tr>
</tbody>
</table>

2. When prompted, provide the path to the Mirage Management server location.
3. Verify the HTTP port and the HTTPS port.
   - The default HTTP port is 7080, and the default HTTPS port is 7443.
4. Follow the prompts to complete the installation.

Install the Mirage File Portal

Install the 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 installation file is located in the Mirage installation package.

Prerequisites

You must install Microsoft IIS 7.0 or later for the file portal. For more information about installing IIS, see "Install IIS," on page 25.

Procedure

1. Double-click the .msi file for your environment and click Run to start the installation wizard.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit</td>
<td>mirage.WebAccess.x64.buildnumber.msi</td>
</tr>
<tr>
<td>32-bit</td>
<td>mirage.WebAccess.x86.buildnumber.msi</td>
</tr>
</tbody>
</table>
2 Follow the prompts until you come to Web Access Configuration page and provide the Web access configuration information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Access</td>
<td>Select <strong>Web Access</strong> to provide access to only an end-user's user files, as defined by the administrator, across all CVD snapshots. The Mirage client user can access the Web Access feature to only download their files at <a href="http://server:6080/Explorer">http://server:6080/Explorer</a>.</td>
</tr>
<tr>
<td>Admin Web Access</td>
<td>Select <strong>Admin Web Access</strong> to give the administrator full access to all user CVDs across all CVD snapshots. The administrator can access the Admin Web Access feature to download all files of any user at <a href="http://server:6080/AdminExplorer">http://server:6080/AdminExplorer</a>.</td>
</tr>
</tbody>
</table>

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**.

3 When prompted, provide the path to the Mirage Management server location.

4 Verify the HTTP port and the HTTPS port.
   - The default HTTP port is 6080, and the default HTTPS port is 6443.

5 Complete the installation.

**What to do next**

You can now install the Mirage Management console.

**Troubleshooting the File Portal Installation**

You might be unable to access the Mirage file portal because of local or domain security policies.

**Problem**

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

**Cause**

You might be unable to access the file portal 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.

**Install the Mirage Management Console**

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

The .msi installation file is located in the Mirage installation package.

**Prerequisites**

Install the Mirage Management server.
Procedure

1. Double-click the .msi file for your environment to start the installation wizard.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit</td>
<td>mirage.management.console.x64.buildnumber.msi</td>
</tr>
<tr>
<td>32-bit</td>
<td>mirage.management.console.x86.buildnumber.msi</td>
</tr>
</tbody>
</table>

2. Follow the prompts to complete the installation wizard.

After you install the Management console, a shortcut to the Management console is added to your desktop.

What to do next

You can connect the console to the Mirage Management system. See “Connect the Console to the Mirage System,” on page 29.

Connect the Console to the Mirage System

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

Procedure

1. In the Mirage Management console tree, click **VMware Mirage** in the root directory, and select **Add System**.

2. Type the IP address or host name of the Mirage Management server in the **Management Server Address** text box, and click **OK**.

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

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

What to do next

You can install the Mirage Gateway server. See “Installing the Mirage Gateway Server,” on page 29.

Installing the Mirage Gateway Server

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

The Mirage server lets end users who have installed the Mirage client to communicate securely with the Mirage servers over the Internet without using VPN configurations.

After installing the Mirage Gateway server, you can add and configure a Gateway server to your Mirage system by using the Mirage Management console.

1. **Generate the Certificate Signing Request for the Mirage Gateway Server** on page 30

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

2. **Submit the Certificate Request** on page 31

   After you generate the certificate signing request, you submit the request.

3. **Convert the Certificate File Extension** on page 32

   After you generate the certificate, you convert the certificate file extension from .p7b to .pfx.
4 Configure the Mirage System to Work with SSL on page 32
   After you convert the certificate file type, you configure the Mirage system to work with SSL.

5 Deploy the OVA Template in ESX on page 33
   You must deploy the OVA template before installing the Mirage Gateway server.

6 Worksheet for Installing the Mirage Gateway Server on page 34
   When you install the Mirage Gateway server, you are prompted to configure certain options. You
   must prepare your configuration options before you install the Mirage Gateway server.

7 Install the Mirage Gateway Server on page 35
   Install the Mirage Gateway server to secure your data center environment for users that communicate
   with the corporate enterprise data center via Internet.

Generate the Certificate Signing Request for the Mirage Gateway Server

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

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

Procedure

1 On the Mirage Management console, select File > Add/Remove Snap-in.
2 On the Add or Remove Snap-ins window, select Certificates and click Add.
3 On the Certificates snap-in window, select Computer account and click Next.
4 Select Local computer and click Finish.
5 Click OK in the Add or Remove Snap-ins window to close the window.
6 Expand the Certificates (Local Computer) node.
7 Expand the Personal node and right-click Certificates.
8 Select All Tasks > Advanced Operations > Create Custom Request.
9 Follow the prompts, and on the Select Certificate Enrollment Policy page, select Proceed without
   enrollment policy and click Next.
10 Verify the relevant information on the Custom Request page.
   a Select Legacy key for the template type.
   b Select PKCS #10 for the request format.
   c Click Next.
11 Expand the Details drop-down menu and click Properties.
12 In the General tab of the Certificate Information page, type a certificate-friendly name.
   You must use this name in the DNS record.
13 On the Subject tab, verify the relevant information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common name, value</td>
<td>The server FQDN. This is the certificate subject name that is used in the</td>
</tr>
<tr>
<td></td>
<td>Mirage configuration to find the certificate. The FQDN must point to that</td>
</tr>
<tr>
<td></td>
<td>server and is validated by the client upon connection.</td>
</tr>
<tr>
<td>Organization, value</td>
<td>The company name. Usually required by the CA.</td>
</tr>
<tr>
<td>Country, value</td>
<td>A two-letter standard country name, for example, US or UK. Usually required by the CA.</td>
</tr>
</tbody>
</table>
14 On the Extensions tab, select the key-use information from the drop-down menus.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Usage</td>
<td>Select <strong>Data Encipherment</strong>, and click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Extended Key Usage</td>
<td>Select <strong>Server Authentication</strong>, and click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>

a Expand the **Key usage** drop-down menu, select **Data encipherment** and click **Add**.
b Expand the **Extended Key usage** drop-down menu, select **Server Authentication** and click **Add**.

15 On the Private Key tab, select the key size and export options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Options</td>
<td>This is the required key size (usually 1024 MB or 2048 MB).</td>
</tr>
<tr>
<td>Make private key exportable</td>
<td>This option exports the CSR, and later the certificate, with the private key for backup or server movement purposes.</td>
</tr>
<tr>
<td>Key Type</td>
<td>Select <strong>Exchange</strong> (the default value is <strong>Signature</strong>).</td>
</tr>
</tbody>
</table>

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

17 On the Certificate Enrollment page, leave the default file format (Base 64), and click **Browse** to select a file name and location for the CSR, and click **Finish**.

The certificate request is complete.

18 On the **Certificates Enrollments & Certificates** tab, click **Refresh**.

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

**What to do next**

After generating the Certificate Signing Request, you submit the CSR. See “Submit the Certificate Request,” on page 31.

**Submit the Certificate Request**

After you generate the certificate signing request, you submit the request.

**Procedure**

1 Go to the external CA Web site and click **Request a certificate**.
2 On the Request a Certificate page, select **advanced certificate request**.
3 On the Advanced Certificate Request page, select **Submit a certificate request using a base-64-encoded CMC or PKCS #10 file or submit a renewal request by using a base-64-encoded PKCS #7 file**.
4 Open the **csr.req** file with notepad and copy the text.
5 Paste the CSR text in the **Base-64-encoded certificate request** text box.
6 Select **Web Server** from the **Certificate Template** drop-down menu and click **Submit**.
7 On the Certificate Issued page, select **Base 64 encoded**, and then click **Download certificate**.
   a When prompted, select **Save As**, type the file name, and save the certificate as a **.p7b** file.
Convert the Certificate File Extension

After you generate the certificate, you convert the certificate file extension from .p7b to .pfx.

**Prerequisites**
- Verify that you installed the Mirage server.
- Verify that you generated a certificate.

**Procedure**
1. Double-click the certificate and right-click **Install Certificate** to start the Certificate Install wizard.
2. Select the **Place all certificates in the following store** check box and then click **Browse**.
3. Select the **Personal** folder on the Select Certificate Store window, and click **OK** to close the window.
4. To continue with the Certificate Install wizard, click **Next**.
5. Verify the information for installing the certificate, and click **Finish**.
6. In the Windows MMC, expand the **Certificates** node, then expand the **Personal** node, and then select **Certificates**.
7. Right-click the **certificate** and select **All Tasks > Export**.
8. Follow the prompts and select **Yes, export the private key**, and click **Next**.
9. Verify the export file format.
   a. Select the **Personal Information Exchange - PKCS #12 (.PFX)** check box.
   b. Select the **Include all certificates in the certification path if possible** check box.
   c. Click **Next**.
10. On the Security page, select the **Password** check box and type a new password in the **Password** text box.
    a. Confirm the password and click **Next**.
11. On the File to Export page, click **Browse**
    a. Locate and select the certificate, and save it as a .pfx file.
    b. Click **Save**.
12. Follow the prompts to complete the export procedure.

The certificate is now installed on the Mirage server and configured for SSL.

Configure the Mirage System to Work with SSL

After you convert the certificate file type, you configure the Mirage system to work with SSL.

**Prerequisites**
Verify that you converted the certificate to the .pfx extension.

**Procedure**
1. In the MMC, expand the **Certificates** node, then expand the **Personal** node, and then select **Certificates**.
2. Double-click the **certificate** and on the **Details** tab, select **Subject**.
   a. Note the CN of the certificate.
3 On the **Details** tab, select **Issuer**.
   a Note the CN of the issuer.

4 In the Mirage Management console, expand the **System and Configuration** node, and select **Servers**.

5 Right-click the **server** and select **Configure**.

6 Configure the server.
   a Select the **SSL** option.
   b Type the CN of the certificate in the **Certificate Subject** text box.
   c Type the CN of the certificate issuer in the **Certificate Issuer** text box.

7 Click **OK**.

### Deploy the OVA Template in ESX

You must deploy the OVA template before installing the Mirage Gateway server.

The `.ova` file is located in the Mirage installation package.

**Prerequisites**

You must have VMware ESX® installed to deploy the OVA template.

**Procedure**

1 Double-click the `.ova` file and click **Run** to start the deployment wizard.

2 Provide login credentials for the ESX, and click **Login**.

3 In the ESX console, select **File > Deploy OVF Template** to start the deployment wizard.

4 Deploy the OVA template and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File</strong></td>
<td>You can specify a location that is accessible from your computer, such as a local hard drive, a network share, or a CD/DCD drive. To select a file location, click <strong>Browse</strong>.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>You can type a URL to download and install the OVA package from the Internet.</td>
</tr>
</tbody>
</table>

After the OVA template is verified, a green check mark icon appears next to the publisher name.

5 Verify the OVA template details, and click **Next**.

6 To accept the End User License Agreement, click **Accept** and then click **Next**.

7 Specify a name and location for the deployed template and click **Next**.

8 Select the host and cluster and click **Next**.

9 Select the resource pool and click **Next**.

10 Select a storage destination for the virtual machine files and click **Next**.
11 Select the disk format and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Thick Provision Lazy Zeroed</strong></td>
<td>Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine. Virtual machines do not read stale data from the physical device.</td>
</tr>
<tr>
<td><strong>Thick Provision Eager Zeroed</strong></td>
<td>A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take longer to create virtual disks in this format than to create other types of disks.</td>
</tr>
<tr>
<td><strong>Thin Provision</strong></td>
<td>Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the virtual disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations. If the thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it. Thin provisioning is the fastest method to create a virtual disk because it creates a disk with just the header information. It does not allocate or zero out storage blocks. Storage blocks are allocated and zeroed out when they are first accessed.</td>
</tr>
</tbody>
</table>

12 Complete the deployment wizard.

The OVA template is deployed.

**Worksheet for Installing the Mirage Gateway Server**

When you install the Mirage Gateway server, you are prompted to configure certain options. You must prepare your configuration options before you install the Mirage Gateway server.

**Table 3-3. Configuration Options for Installing the Mirage Gateway Server**

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP type</td>
<td>You can select either <strong>LDAP</strong> or <strong>LDAPS</strong>. The default value is <strong>LDAP</strong>.</td>
<td></td>
</tr>
<tr>
<td>LDAP server address</td>
<td>You can type either the LDAP server or the IP address, for example, ldap.yourcompany.com, or ldap.IPaddress.com.</td>
<td></td>
</tr>
<tr>
<td>LDAP server port</td>
<td>The default port is 389. Verify that your firewall settings allow the selected port.</td>
<td></td>
</tr>
<tr>
<td>LDAP user DN to bind Mirage Gateway with the LDAP server</td>
<td>This follows the format: cn=username, cn=users, dc=domain, dc=com For example: CN=Administrator, CN=USERS, DC=MIRAGEDOMAIN, DC=COM</td>
<td></td>
</tr>
<tr>
<td>LDAP bind user password</td>
<td>This is your password.</td>
<td></td>
</tr>
<tr>
<td>Token expiration time (in hours)</td>
<td>The default is 168 hours.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-3. Configuration Options for Installing the Mirage Gateway Server (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage server address</td>
<td>You can type either the hostname or the IP address, for example,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mirageserver.yourcompany.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default is 10.117.43.70.</td>
<td></td>
</tr>
<tr>
<td>Mirage server port</td>
<td>The default is 8000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify that your firewall settings allow the selected port.</td>
<td></td>
</tr>
<tr>
<td>Mirage Gateway activation code</td>
<td>You create the activation code during the installation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The activation code must contain at least 8 characters,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>including a number, an upper-case character, a lower-case character,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and a special character.</td>
<td></td>
</tr>
<tr>
<td>Certificate file</td>
<td>This follows the format:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/root/certificatename.pfx</td>
<td></td>
</tr>
<tr>
<td>Certificate private key password</td>
<td>The password you created as part of the certificate export procedure.</td>
<td></td>
</tr>
</tbody>
</table>

### Install the Mirage Gateway Server

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

Linux is case sensitive.

**Prerequisites**

- Ensure that you installed the following Mirage components:
  - Mirage server
  - Mirage Management server
  - Mirage Management console
  - Mirage file portal
- Create a bind user to authenticate the communication request between the client and the Mirage servers.
- Verify that you created a DNS record.
- Verify that you set the DNS server address.

**Procedure**

1. In the ESX console, power on the VM.
2. On the Console tab, press Enter.
3. When prompted, provide the login credentials.
   The default username is **mirage**, and the default password is **vmware**.
4. To start the installation, run the `sudo /opt/MirageGateway/bin/install.sh` command.
Follow the prompts to install the Mirage Gateway server.

Use the configuration information that you gathered in the worksheet.

The Mirage Gateway server is installed and available in the Mirage Management console.

Managing Mirage Software Licenses

The 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 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 36.

When a license expires, all management actions are disabled. However, 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, when you open the Management console a dialog box appears where you can type the license key.

You do not need to restart the 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 Web URL for the file portal, importing USMT settings, and performing domain joining operations.

For information about importing USMT files, see Import USMT Settings.

For Join Domain Account information, see General System Settings.

Prerequisites

Verify that a Mirage server is installed.
Procedure

1. (Optional) Configure the file portal Web URL.
2. (Optional) To perform migration operations, import the USMT folder.
3. (Optional) To perform domain joining operations, provide Join Domain Account details.

What to do next

You can now configure and use your Mirage system.
Index

A
antivirus scanning 19

C
certificate, installing 32
console connection 29

D
database, sizing requirements 16
database software requirements 16
deployment planning 13

E
endpoints, required environment 36

F
file portal
access troubleshooting 28
install 27

G
gateway server, installing 34
Gateway server
certificate signing request 30
installation 33, 35

H
hardware requirements 14

I
IIS configuration 25
install the Web Manager 26
installation, gateway server 34
installing the system
endpoint requirements 36
file portal 27
IIS configuration 25
licenses 36
Management console connection 29
Management console installation 28
server 22

L
licenses, adding and viewing 36

M
management, server installation 21
Management
console installation 28
server installation 21
management server, installing 21
Mirage, installation 7
Mirage Gateway, certificate 32
Mirage system, installation 19
Mirage Gateway server, installation 29

O
operating system requirements 13
OVA, deployment 33

P
planning the deployment 13
ports and protocols 17

S
secure sockets layer, See SSL
servers
install 22, 25
installation 24
software requirements 16
SSL
configuring 32
install the SSL certificate 23
SSL certificate setup 31
system requirements
database software 16
hardware 14
operating system 13
ports and protocols 17
software 16
system components 9

U
updated information 5

W
Web Manager, installing 26
Windows Internet Information Services, See IIS