VMware Mirage Web Management Guide

Mirage 5.7

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
Contents

About the Mirage Web Management Guide 5

1 About the Mirage Web Management 7
   Access the Web Management 7

2 Managing CVDs 9
   Restart a Device 10
   Enforce Layers on Endpoints 10
   Base Layers and App Layers 11
   Endpoint Disaster Recovery 12
   Working with the File Portal 13
   Assign an Upload Policy 13
   Manage Collections 14
   Move a CVD to a Different Volume 14
   Windows OS Migration 14
   CVD Integrity Report 15

3 Working with Endpoints 17
   Centralizing Endpoints 17
   Migrate a CVD to a Replacement Device 17
   Creating a Reference Machine from an Endpoint 18
   Provisioning a Layer for an Endpoint 19
   Reconnect a Device to a CVD 19
   Delete Pending Device in Mirage Web Management 19

4 Working with Layers 21

5 Working with Upload Policies 23
   Upload Policy Parameters 24
   Add or Edit Upload Policy Rules 25

6 Working with CVD Collections 27
   Add Static Collections 28
   Add CVDs to Static Collections 28
   Add Dynamic Collections 29
   Add Dynamic Collections by Using Active Directory 29
   Edit Collection 29

7 Working with Storage Volumes 31
8 Working with Reports for Mirage Operations  33
   Create a Custom Report  34
   Export Legacy Reports  34
   Import the Mirage Reports Package  35
   Export Grid Data to CSV  35

9 Managing Mirage Tasks  37

10 Managing the Driver Library  39

11 Driver Library Architecture  41

12 Managing Driver Profiles  43

13 Managing Mirage Assignments  45

14 Managing Mirage Event Log Files  47

15 Managing Branch Reflectors  49
   Branch Reflector Matching Process  50
   Select Clients To Be Branch Reflectors  50
   Configure Defaults for Branch Reflectors  51
   Wake on LAN  51
   Configure Wake on LAN  52

16 Managing Mirage Servers, Mirage Management Servers, and Mirage Gateway Servers  53

17 Configuring the Mirage System  55
   Managing Bandwidth Limitation Rules  55
   License Settings  56
   Authenticating the Mirage Gateway Server  56
   Branch Reflector Settings  57
   Configuring User Access to the File Portal  57
   General System Settings  57
   Export Mirage System Settings  58

Index  59
About the Mirage Web Management Guide

The VMware Mirage Web Management Guide provides information about how to use the Mirage Web Management.

Intended Audience

This information is intended for IT help desk users to resolve endpoint issues. It is also intended for the Mirage Image Manager user to manage image-based operations, and the Mirage Protection Manager user to protect the Mirage client endpoints. The administrator user can perform all Mirage operations.
Mirage users can use the Mirage Web Management to perform role-based actions on CVDs, upload policies, volumes, layers, and so on.

The Web Management is used by various Mirage user roles.

Table 1-1. Web Management User Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>Provides information about the Mirage client user device in order to respond to service queries. Access with the Help Desk role displays the Select User and Device page by default.</td>
</tr>
<tr>
<td>Image Manager</td>
<td>Captures and assigns base layers and app layers to CVDs. The Image Manager role provisions new devices with a specified image.</td>
</tr>
<tr>
<td>Protection Manager</td>
<td>Provides detailed information of the Mirage system. Users with the Protection Manager role can update the Mirage system to protect Mirage end-user devices.</td>
</tr>
<tr>
<td>Administrator</td>
<td>A super-set of all Mirage operations.</td>
</tr>
</tbody>
</table>

Mirage Web Management user roles are assigned by the Mirage Management console. For more information about the Mirage users and roles, see the *VMware Mirage Administrator’s Guide*.

**Access the Web Management**

You must log in each time you open the application.

**Prerequisites**

Ensure that you installed the Mirage Web Management.

**Procedure**

   - *WebManagerServer* is the DNS name or IP address of the server where the Mirage Web Management is installed.
2. Type your user name and password.
   - Include the domain in your user name if your company requires it.
3. Click **Login**.
After logging in, the Select User and Device page appears for Help Desk users. Here you perform a search for devices.

The CVD Inventory page appears for Image Manager users and Protection Manager users. Here you can view the current Mirage conditions.
Managing CVDs

You can manage the CVD by performing tasks on the CVD.

You can use the search function to locate the CVD you want to manage. Alternatively, you can locate the CVD you want to manage on the **Collections** tab.

The actions you can perform are available on the action toolbar. For additional tasks, click the double arrow at the end of the action toolbar.

In addition to the tasks for managing CVDs in a collection, you can manage the CVD by performing the following tasks:

- **Restart a Device** on page 10
  You can remotely force a restart of a Mirage client device, for example, when the user does not reboot on a request from the Mirage client.

- **Enforce Layers on Endpoints** on page 10
  Users and applications might make changes to files and registry settings that were provisioned through a base layer or app layer. Sometimes these changes create problems with the desktop operation. In most cases, you can resolve the problem by enforcing the layer originally assigned to the CVD.

- **Base Layers and App Layers** on page 11
  A base layer is a template for common desktop content, cleared of specific identity information and made suitable for mass deployment to endpoints. You can also define app layers, separate from the common base layer, to distribute more specific applications to groups of users.

- **Endpoint Disaster Recovery** on page 12
  You can restore device files to a previous CVD snapshot, or restore a device from a CVD following hard drive replacement, file corruption, or format, or when the device is replaced.

- **Working with the File Portal** on page 13
  End users that have a Mirage client installed can use the Mirage file portal to browse and view files in their CVD.

- **Assign an Upload Policy** on page 13
  An upload policy determines which files and directories to upload from the user endpoint to the CVD in the data center. You can assign an upload policy to all CVDs in the collection or to an individual CVD in a collection.

- **Manage Collections** on page 14
  You can add a collection to the CVD or remove a collection from a CVD.

- **Move a CVD to a Different Volume** on page 14
  You can move a CVD to a different storage volume, according to your disk organization requirements.
Windows OS Migration on page 14
You can migrate existing Windows XP or Windows Vista endpoints to Windows 7, and existing Windows 7 endpoints to Windows 8.1 and Windows 10. The migrations can be either in-place, on the same devices, or to replacement devices.

CVD Integrity Report on page 15
You generate the CVD Integrity report if a system event warns that a CVD might have inconsistencies.

Restart a Device
You can remotely force a restart of a Mirage client device, for example, when the user does not reboot on a request from the Mirage client.

Procedure
1. In the Mirage Web Management, select the device that you want to restart and click Restart.
2. At the confirmation prompt, click OK.

An Audit Event transaction is added to the device information list.

What to do next
After you restart a device, the end-user receives a message to restart the computer. The user can click Restart Now to restart the computer or wait for the computer to automatically restart after 10 minutes.

Enforce Layers on Endpoints
Users and applications might make changes to files and registry settings that were provisioned through a base layer or app layer. Sometimes these changes create problems with the desktop operation. In most cases, you can resolve the problem by enforcing the layer originally assigned to the CVD.

The Mirage client downloads only the relevant files and registry settings required to realign the CVD with the original layer. User profiles, documents, and installed applications that do not conflict with the layer content are preserved.

Enforcing all layers can also be set to remove user-installed applications residing in the machine area of the CVD. This ability is useful, for example, for fixing a problematic CVD in which all layer applications do not function because of overwritten or corrupted system files. Removing user applications deletes Machine Area files and registry keys that are not in the current base layer, with the exception of files defined in the user area policy.

Procedure
1. In the Mirage Web Management, select the device for which you want to enforce layers and click Enforce Layers.
2. Select an option for the user applications, and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preserve user applications</td>
<td>The system is restored to comply with the assigned layer while preserving user data. Use this option to preserve user applications and to retain the user-installed applications on the CVD.</td>
</tr>
<tr>
<td>Remove user applications</td>
<td>The system is restored to comply with the assigned layer while removing user data. Use this option to remove user applications and user-installed applications from the CVD.</td>
</tr>
</tbody>
</table>
3. Use the validation summary to compare the target device with the CVD. This summary alerts you to any potential problems that require additional attention.
   
   You cannot proceed until blocking problems are resolved.

4. At the confirmation prompt, click **Finish**.

   An Audit Event transaction is added to the device information list.

---

**Base Layers and App Layers**

A base layer is a template for common desktop content, cleared of specific identity information and made suitable for mass deployment to endpoints. You can also define app layers, separate from the common base layer, to distribute more specific applications to groups of users.

The base layer includes the operating system, service packs and patches, as well as core enterprise applications and their settings.

An app layer can include a single application, or a suite of applications. You can deploy app layers with other app layers on any compatible endpoint.

App layers require a base layer to be present on an endpoint, but the base layer and any app layers can be updated independently of each other.

The app layer assignment process is wizard driven and similar to base layer assignment. App layer options are listed under separate nodes in CVD views, in parallel with base layer action nodes.

The base layer can still include applications directly. App layers are not needed in organizations where everyone uses the same applications.

---

**Capturing Base Layers**

After you set up the base layer for a reference machine, you can capture a base layer from it so that endpoints can be updated with that content.

The base layer capture process creates a point-in-time snapshot of the data and state of the live reference machine, generalized for mass deployment.

A similar process is employed to capture app layers.

You can use a custom post-base layer script called `post_core_update.bat` to perform certain actions after the base layer update.

For more information, see the *VMware Mirage Administrator's Guide*.

---

**Capturing App Layers**

You can provide sets of more specialized applications to specific users through app layers, independent of the core applications that are generally distributed with the common base layer.

You can capture an app layer that contains a single application, or a suite of applications from the same vendor. You can create app layers to include applications relevant for a specific department or group. You can combine app layers with other app layers and deploy them on any compatible endpoint.

You define and deliver app layers by capturing an app layer and then assigning them to endpoints.

The app layer capture process creates a snapshot of designated applications installed on a live reference machine, which is generalized for mass deployment.

You can use a CVD as the reference CVD for app layer purposes. A base layer does not need to be present on the reference machine.

For more information, see the *VMware Mirage Administrator’s Guide*.
Endpoint Disaster Recovery

You can restore device files to a previous CVD snapshot, or restore a device from a CVD following hard drive replacement, file corruption, or format, or when the device is replaced.

Mirage provides disaster recovery in two key ways:

- Restore files or the entire desktop to a previous CVD snapshot on an existing device. Files and directories are included in CVD snapshots in accordance with the upload policies currently in effect. See Chapter 5, “Working with Upload Policies,” on page 23.

- Restore the hard drive on an existing or a replacement device:
  - Restore a CVD to the same device after a hard-drive replacement, file corruption, or format.
  - Restore the CVD to a replacement device.

When the CVD contains Encrypted File System (EFS) files, the files are recovered in their original encrypted form.

Note: For better deduplication in the revert-to snapshot, the end user must be logged in during the restore Prefetch operation if the CVD contains EFS files.

Restore a Device to a CVD Snapshot

You can use a CVD snapshot to restore a specific file or a complete endpoint on an existing device.

Mirage automatically creates CVD snapshots at regular intervals, and preserves them based on a retention policy, making them available for restoration purposes as needed. For more information, see the VMware Mirage Administrator’s Guide.

You can use a selected CVD snapshot to restore a specific file or a complete endpoint on an existing device. The reversion can be between same operating system, for example, Windows 8.1 to Windows 8.1, or cross-operating systems, for example, Windows 8.1 to Windows 7.

Procedure

1. In the Mirage Web Management, select the CVD that you want to restore to a CVD snapshot and click Revert To Snapshot.
2 Select the revert options.
   a Select the snapshot date to which you want to revert.
   b Select whether you want to only restore the system and click Next.

The Restore System Only check box is selected by default. Select This restores system files only, including the base layer, user-installed applications and user machine settings. The user area content is not affected and any new files in the user area are not erased.

User data in this option pertains to files and directories listed in the upload policies User area.

The option behavior depends if the reversion you are performing is to the same OS or cross-OS.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>If to the same OS, for example,</td>
<td>Clear this check box if you want to restore the entire CVD, including the User area, from the CVD snapshot. If the checkbox is cleared, any application, setting, or document in the current CVD that does not exist in the snapshot is erased from the endpoint.</td>
</tr>
<tr>
<td>Windows 8.1 to Windows 8.1:</td>
<td></td>
</tr>
<tr>
<td>If to a different OS, for example,</td>
<td>This checkbox is not selected so the entire CVD, including the User area, is always restored from the CVD snapshot.</td>
</tr>
<tr>
<td>Windows 8.1 to Windows 7:</td>
<td></td>
</tr>
</tbody>
</table>

3 Use the validation summary to compare the target device with the CVD. This summary alerts you to any potential problems that require additional attention.

You cannot proceed until blocking problems are resolved.

4 Verify the snapshot details and click Finish.

**Working with the File Portal**

End users that have a Mirage client installed can use the Mirage file portal to browse and view files in their CVD.

In some situations, for example in an MSP environment, user devices cannot access the corporate domain.

To enable users to access their files, an administrator maps a CVD that is centralized in the system to specific domain users. Users who are not on the domain can access their files through the file portal by using their domain account.

Users access these files from the data center directly, not from the endpoint, so the endpoint does not need to be accessible for file portal purposes.

To allow or block access to the file portal, select the appropriate CVD and click either Allow File Portal or Block File Portal.

**Assign an Upload Policy**

An upload policy determines which files and directories to upload from the user endpoint to the CVD in the data center. You can assign an upload policy to all CVDs in the collection or to an individual CVD in a collection.

A CVD is assigned only one upload policy at a time.

**Procedure**

1 In the Mirage Web Management, select the device for which you want to assign an upload policy and click Assign Upload Policy.

2 Select a CVD policy to assign and click OK.

An Audit Event transaction is added to the device information list.
The new policy will only take effect after the next synchronization between the devices and the Mirage server. The newly assigned upload policy is displayed in the CVD list.

Manage Collections
You can add a collection to the CVD or remove a collection from a CVD.

Procedure
1. In the Mirage Web Management, select the CVD that you want to manage.
2. On the toolbar, click the double arrow icon to view more options and select Manage Collections.
3. Select one or more available collections from the Available Collections list and click Save.

An Audit Event transaction is added to the device information list.

Move a CVD to a Different Volume
You can move a CVD to a different storage volume, according to your disk organization requirements.

Procedure
1. In the Mirage Web Management, select the CVD that you want to move to a different volume and click Change Volume.
2. Select a volume and click OK.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically select a volume</td>
<td>Use this option if you want the Mirage server to select the volume with the most free space. The Mirage server does not choose blocked volumes.</td>
</tr>
<tr>
<td>Manually select a volume</td>
<td>Use this option if you want to select the volume manually.</td>
</tr>
</tbody>
</table>

Windows OS Migration
You can migrate existing Windows XP or Windows Vista endpoints to Windows 7, and existing Windows 7 endpoints to Windows 8.1 and Windows 10. The migrations can be either in-place, on the same devices, or to replacement devices.

The migration installs a Windows 7, Windows 8.1, or Windows 10 base layer on each target endpoint while preserving user profile data and settings through the Microsoft User State Migration Tool.

- USMT 4.0 or USMT 5.0 for Windows XP to Windows 7 migration
- USMT 6.3 for Windows 7 to Windows 8.1 migration
- USMT 10.0 for Windows 7 to Windows 10 migration

Unlike base layer updates, the migration process installs a complete OS image, including local user profiles as configured on the reference machine when the base layer was captured. You can use this to set up a local administrator and default user account.

The migration moves existing content of a target endpoint to the C:\Windows.0ld directory, which is then processed by USMT. Application settings and data that are not handled by USMT are kept in the C:\Windows.0ld directory. You can manually restore this data, or delete it when you do not need it.

OS migration with Mirage retains the original computer name but requires rejoining the domain to create a Windows 7, Windows 8.1, or Windows 10 machine account. You can define this account in the Mirage system configuration.
Custom boot loaders on the target machine are removed by the migration. If an endpoint includes multiple operating systems, the migration overwrites only the one on the active OS partition and does not provide boot options for the others. You can manually restore other boot options after booting to the new OS.

**NOTE** Mirage requires certain Full Disk Encryption applications to be pre-configured before performing an OS migration. For more information about supported Full Disk Encryption software, contact VMware Support.

**Prerequisites**

- Users with the Administrator role or the Image Manager role can perform Windows OS migrations procedures.
- To reduce bandwidth during OS migration in a small or remote office, use the Mirage branch reflector feature. In particular, a Windows 7, Windows 8.1, or Windows 10 test machine configured as a branch reflector can share its OS files with client endpoints to assist in the migration process.
- USMT does not migrate applications installed on Windows XP or Windows Vista to Windows 7, or applications installed on Windows 7 to Windows 8.1, or Windows 10.
- Make sure to remove any sensitive data from the reference machine. All user data on the reference machine is applied to the target as part of the migration process.

**Windows OS Migration End User Experience**

After the migration base layer download is completed, the system requests a reboot. A swap is made and Windows 7, Windows 8.1, or Windows 10 boots.

Login is disabled until the system completes the migration process. The new OS is loaded and Plug-and-Play hardware is installed and configured. This process might take a few minutes, during which the computer is busy.

You can monitor the progress in the Windows login screen. When the process is completed, the system restarts the PC and you can then log in.

The post-migration script runs the USMT and then rejoins the domain. The PC must be connected to the corporate network to be assigned a network address.

**NOTE** To rejoin the domain, the PC must have network access to the Mirage server and the domain controller. End users can log in using their domain credentials only after the domain join is complete.

**CVD Integrity Report**

You generate the CVD Integrity report if a system event warns that a CVD might have inconsistencies.

The CVD Integrity report verifies that a CVD is consistent and free of corruption, and can continue to reside in the system and be used for restore and other purposes.

**Procedure**

1. In the Mirage Web Manager, click the CVD Inventory tab.
2. Click the double arrow icon in the navigation pane to display more options, and click CVD Integrity.
3. Follow the steps of the report configuration wizard.
After you install the Mirage client, the Mirage Management server, and the Mirage server, you can perform certain actions on endpoints.

This chapter includes the following topics:

- “Centralizing Endpoints,” on page 17
- “Migrate a CVD to a Replacement Device,” on page 17
- “Creating a Reference Machine from an Endpoint,” on page 18
- “Provisioning a Layer for an Endpoint,” on page 19
- “Reconnect a Device to a CVD,” on page 19
- “Delete Pending Device in Mirage Web Management,” on page 19

Centralizing Endpoints

After you install the Mirage client, you centralize the device. Centralization activates the endpoint in the Mirage Management console and synchronizes it with, or assigns it to, a CVD on the Mirage server so that you can centrally manage the device data.

When you first introduce Mirage to your organization, you must back up each device, creating a copy of it on the server, in the form of a Centralized Virtual Desktop (CVD). You can then centrally manage the device.

The endpoint with the client installed appears in the Mirage Management console as Pending Assignment, and is pending activation in the system. You can also reject a device that you do not want to manage in the system.

Migrate a CVD to a Replacement Device

You can migrate a CVD in the Mirage Management server to a replacement device.

You can select one of the following migration options for the selected CVD and device.
### Table 3-1. Options for Migrating a CVD to a Replacement Device

<table>
<thead>
<tr>
<th>Migration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full System Migration, including OS, applications, user data, and settings</td>
<td>The entire CVD is restored to the replacement device, including operating system, applications, and user files. Files that already exist on the replacement device are deleted or overwritten. Use this option for systems with Windows volume licenses or Windows OEM SLP licenses.</td>
</tr>
<tr>
<td>Only Migrate User Data and Settings</td>
<td>The existing operating system and applications on the replacement device are retained. Only user data and settings are migrated to the replacement device. Use this option to migrate users from Windows XP, Windows Vista, or Windows 7 machines to new Windows 7 or Windows 8.1 machines. The OS of the replacement device must be the same as, or newer than, that of the CVD.</td>
</tr>
</tbody>
</table>


If you migrate a CVD from a Windows XP or Windows Vista device to a replacement device running Windows 7, or a Windows 7 device to a replacement device running Windows 8.1, select **Full System Migration** or **Only Migrate User Data and Settings** because Mirage does not transfer user-installed applications from Windows XP or Windows Vista machines to a Windows 7 system.

When you migrate a CVD from Windows XP or Windows Vista to Windows 7, after the CVD has been migrated the system streams to the endpoint so that the end user can resume work without waiting for all of the user data to be downloaded.

If you select a Windows 7 endpoint to be restored to a Windows XP or a Windows Vista CVD, that Windows 7 endpoint becomes a Windows XP or Windows Vista device.

**Procedure**

1. Click the **Pending Devices** tab and select and select the CVD that you want to migrate.
2. Click **Hardware Migration** and follow the steps of the migration wizard to complete the migration wizard.

**Creating a Reference Machine from an Endpoint**

You assign a pending device as a reference CVD and configure it with applications and settings for a base layer that applies to a set of endpoints. After you build and configure the reference machine, you can centralize the device as a reference machine for base layer capture.

A pending device that is assigned as a reference machine is moved from the Pending Devices list to the Reference CVDs view.

For more information, see the *VMware Mirage Administrator’s Guide*.

---

**CAUTION** Files and settings from the reference machine are captured in the base layer, and are then distributed to a large number of endpoint desktops. To avoid unintended consequences, make sure the configuration is appropriate for mass distribution.
Provisioning a Layer for an Endpoint

When Mirage is already implemented, you can prepare new devices to be part of the organization using layer provisioning.

The layer provisioning process first cleans up the device files and applies an existing base layer and app layers, if you selected app layers, as a common template. The device is then freshly imaged, and assigned to and synchronized with a newly created CVD.

After the Mirage client is installed on the new device, the Pending Devices tab shows the device as pending assignment.

The user can use the desktop as usual, performing offline work and network transitions, after the centralization processing associated with the provisioning operation starts. The Mirage client monitors user activities and adjusts its operation to optimize the user experience and performance.

After the server synchronization is completed, the transaction log shows a successful provisioning entry. The desktop is protected and you can centrally manage the desktop at the data center.

Reconnect a Device to a CVD

You can reconnect a device that has lost its synchronization for any reason to its CVD. After the Force Upload operation, you can then continue backing up incremental changes as before.

You can connect an Assignment Pending device to an existing CVD and upload the current device data to the CVD through a Force Upload process.

Procedure

1. In the Mirage Web Management click the Pending Devices tab and select the CVD for which you want to force an upload.
2. Click Force Upload.

The device then synchronizes all its data to the CVD. Local client changes take precedence (“win”) over CVD changes.

Delete Pending Device in Mirage Web Management

You can delete pending devices that are no longer in use from the Mirage Web Management. This helps you keep the list of pending devices short and does not show obsolete devices that have been uninstalled previously. You can delete only those devices which are in Pending Assignment, Pending CVD Creation, or Pending Registration state. You can also delete multiple devices simultaneously.

Prerequisites

To delete pending devices from the Mirage Web Management you must be logged in as an Administrator, a Protection manager, or an Image manager.

Procedure

1. In the Mirage Web Management, select the devices that you want to delete and click Delete.
   The Delete device windows appears.
2. Click OK.

Two audit logs (Reject device and Remove device) are generated that show the names of the deleted devices and the user name of the person who deleted that device.
Working with Layers

Users with the Image Manager role or Administrator role can manage base layers and app layers using the Mirage Web Management.

You can perform various tasks related to Mirage layers.

**Table 4-1. Working with Layers**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Edit base layer or app layer information.</td>
</tr>
<tr>
<td>License Keys</td>
<td>View, update, and edit license key information for Microsoft Office products. You can only update license key information for a single layer at a time.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete a base layer or app layer. You cannot delete a base layer that is assigned to a CVD or an archived CVD.</td>
</tr>
<tr>
<td>Create Reference CVD</td>
<td>Create a reference CVD from a base layer.</td>
</tr>
<tr>
<td>Compare Programs</td>
<td>Generate a comparison report that compares one or more base layers with another base layer. A hypothetical base layer assignment. The comparison report details the differences between the contents of one or more base layers and a selected base layer.</td>
</tr>
</tbody>
</table>
An upload policy determines which files and directories to upload from the user endpoint to the CVD in the data center.

A pre-defined upload policy already exists in the Mirage server in the data center. Ensure that the pre-defined upload policy fits your organizational needs or define an upload policy before you activate endpoints because the activation process selects the existing upload policy for the endpoint.

A CVD is assigned only one upload policy at a time.

You manage upload policies from the Policies tab in the Mirage Web Management. You can perform various operations with upload policies.

**Table 5-1. Working with Upload Policies**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Define which files are to be unprotected, protected, or local to the endpoint. Protected files are uploaded to the Mirage server in the data center. To simplify the task, you identify only files and directory names or patterns that are not uploaded to the CVD. The remaining files are considered part of the CVD and are protected.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit an existing upload policy and distribute the revised policy. You export the policy file, edit it, and import it back to the Mirage Web Management. The new policy takes effect at the next update interval in which the client queries the server. The default is one hour and requires a full disk scan. Before you distribute the revised policy to a group of CVDs, it is good practice to test it on a sample desktop.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete an existing upload policy.</td>
</tr>
<tr>
<td>Upgrade</td>
<td>An upload policy must be updated with new policy information or rules and have a new minor or major version assigned to upgrade the CVDs with the new policy version. The CVDs assigned to the previous version of the upload policy are moved to the new version.</td>
</tr>
</tbody>
</table>

You define two upload policy areas, which the system uses according to the relevant system flow. See “Upload Policy Parameters,” on page 24.

The upload policy that is applied to the CVD is a combination of the following items:

- A selected built-in factory policy that VMware provides to assist the administrator with first time deployment
- Administrator modifications to that policy to address specific backup and data protection needs
The built-in factory policy is a reference for further customization and includes all the mandatory rules that the system needs to function. The administrator cannot modify the mandatory rules.

Before you use a built-in policy, evaluate it to be sure it meets backup policy and data protection needs. The built-in policies, for example, do not upload .MP3 and .AVI files to the CVD.

You can use one of the following customizable built-in upload policies, to help manage mixed Mirage and Horizon View systems:

**Mirage default upload policy**

Use on Mirage servers that manage CVDs on distributed physical devices.

**VMware Horizon View optimized upload policy**

Use on Mirage servers that manage CVDs on virtual machines. This upload policy is provided for convenience. It is identical to the Mirage default upload policy, except that the **Optimize for VMware Horizon View** check box is selected.

- **Upload Policy Parameters** on page 24
  
  Upload policies have various parameters that you can view, configure, and edit.

- **Add or Edit Upload Policy Rules** on page 25
  
  You can add or edit a rule or a rule exception in a policy. A rule defines directories or files that are not protected, and a rule exception defines entities within the scope of the rule that are protected.

## Upload Policy Parameters

Upload policies have various parameters that you can view, configure, and edit.

<table>
<thead>
<tr>
<th>Table 5-2. Upload Policy Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Name and Description</td>
</tr>
<tr>
<td>Upload change interval</td>
</tr>
<tr>
<td>Protected volumes</td>
</tr>
<tr>
<td>Optimize for Horizon View check box</td>
</tr>
<tr>
<td>Unprotected Area tab</td>
</tr>
<tr>
<td>Rules list</td>
</tr>
<tr>
<td>Rule Exceptions list</td>
</tr>
<tr>
<td>User Area tab</td>
</tr>
<tr>
<td>The tab contains Rules and Rule Exception areas, used in the same way as in the Unprotected Area tab.</td>
</tr>
<tr>
<td>Advanced Options tab</td>
</tr>
<tr>
<td>Show Factory Rules check box</td>
</tr>
</tbody>
</table>
Table 5-2. Upload Policy Parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export button</td>
<td>Exports policy rules to an XML file for editing and backup. Mirage factory rules are not exported, even if they appear in the policy window.</td>
</tr>
<tr>
<td>Import button</td>
<td>Imports policy rules from an XML file.</td>
</tr>
</tbody>
</table>

Add or Edit Upload Policy Rules

You can add or edit a rule or a rule exception in a policy. A rule defines directories or files that are not protected, and a rule exception defines entities within the scope of the rule that are protected.

When you formulate policy rules, you can use macros to assist specification of various Mirage directory paths addressed by the rules. For example, macros let Mirage and the administrator handle cases when some endpoints have Windows in c:\windows and some in d:\windows. Using macros and environment variables makes sure Mirage backups important files regardless of their specific location. For information about the macro specifications, see the *VMware Mirage Administrator’s Guide*.

**Procedure**

1. In the Mirage Web Management, click the **Policies** tab and select the required upload policy.
2. Click **Edit**.
3. Click the **User Area** tab.
4. Click **Add** next to the required Rule or Rule Exception area.
5. Type the directory path or select it from the drop-down menu.
   
   **IMPORTANT** Do not type a backslash (\) at the end of the path.
6. Select a filter for this directory or a pattern for matching files under this directory.
   
   For example, to add a rule to not protect Windows search index files for all the users on the desktop, add the following rule:
   
   `%anyuserprofile%\Application Data\Microsoft\Search\*`
7. Click **Save**.
Users with the Image Manager role or Administrator role can work with CVD collections. You can group in a collection folder CVDs that share a logical relation to other CVDs. You can use the collections to update their policies, set drivers, or perform an action on the device such as restarting the device or synchronizing the device with the Mirage server.

For example, you can aggregate all CVDs of users in the marketing department to a folder under a collection called Marketing. Then you can perform updates on the CVDs that all the Marketing CVDs share all at once.

Mirage supports static and dynamic collections. You manually assign CVDs to a static collection, while CVD assignments to dynamic collections are calculated based on predefined filters every time an operation is applied to a collection.

A CVD can be a member of multiple collections. If different base layers or policies are applied to different collections and a CVD belongs to more than one, the last change applied takes effect.

To view additional information for the layers assigned to a collection, click the number in the Number of Layer Assignments column.

You can perform various operations on CVD collections.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Create a dynamic collection or static collection of CVDs.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit a CVD collection.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete a CVD collection.</td>
</tr>
<tr>
<td>Sync</td>
<td>Synchronize all CVDs in a CVD collection.</td>
</tr>
<tr>
<td>Suspend</td>
<td>Suspend the network operation of CVDs in a CVD collection.</td>
</tr>
<tr>
<td>Resume</td>
<td>Resume network operation of CVDs in a CVD collection.</td>
</tr>
<tr>
<td>Restart</td>
<td>Force a restart all devices in a CVD collection.</td>
</tr>
<tr>
<td>Assign Base Layer</td>
<td>Assign a base layer to all devices in a CVD collection.</td>
</tr>
<tr>
<td>Assign App Layer</td>
<td>Assign an app layer to all devices in a CVD collection.</td>
</tr>
<tr>
<td>Enforce Layers</td>
<td>Enforce all layers to resolve any issues with corrupted files and registry settings that were provisioned through a layer. You can preserve user applications, or remove user applications when you enforce layers.</td>
</tr>
<tr>
<td>Migrate Windows OS</td>
<td>An upload policy determines which files and directories to upload from the user endpoint to the CVD in the data center. You can assign an upload policy to all CVDs in a collection or to an individual CVD in a collection.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Apply Driver Library</td>
<td>Apply hardware-specific drivers to a CVD collection.</td>
</tr>
<tr>
<td>Assign Upload Policy</td>
<td>Assign an upload policy to a CVD collection to determine which files and directories are uploaded from the user endpoints to the CVD collection.</td>
</tr>
</tbody>
</table>

- **Add Static Collections** on page 28
  You can add a static collection folder to the **Collections** node, to which you can add CVDs manually.

- **Add CVDs to Static Collections** on page 28
  You can move CVDs to existing collection folders to organize them in logical groupings.

- **Add Dynamic Collections** on page 29
  You can add a dynamic collection. CVD assignments to the dynamic collection are calculated based on predefined filters every time an operation is applied to the collection. You can define an unlimited number of rules for a dynamic collection.

- **Add Dynamic Collections by Using Active Directory** on page 29
  You can use Active Directory (AD) to add a dynamic CVD collection. You can add CVDs to the collection by Active Directory group, organizational unit, or domain. You can create a filter for multiple Active Directory elements, for example, filter CVDs whose users belong to the Human Resources AD group or to the Marketing AD group.

- **Edit Collection** on page 29
  You can use the Edit Collection action to modify the collection properties, add or remove a CVD, or manage the CVDs in the collection.

### Add Static Collections

You can add a static collection folder to the **Collections** node, to which you can add CVDs manually.

**Procedure**

1. In the Mirage Web Management, click the **Collections** tab.
2. Select **Create New > Static Collection**.
3. Type a name and description for the collection.
4. Select the CVDs that you want to manage in the static collection.
5. Click **Save**.

The static collection is added to the **Collections** list.

### Add CVDs to Static Collections

You can move CVDs to existing collection folders to organize them in logical groupings.

**Procedure**

1. In the Mirage Web Management, click the **Collections** tab and select the collection to which you want to add the CVD.
   - Do not click the collection name.
2. Click **Edit**.
3. Select the CVD to add to the current collection and click **Save**.
Add Dynamic Collections

You can add a dynamic collection. CVD assignments to the dynamic collection are calculated based on predefined filters every time an operation is applied to the collection. You can define an unlimited number of rules for a dynamic collection.

Procedure

1. In the Mirage Web Management, click the Collections tab.
2. Select Create New > Dynamic Collection.
3. Type the name and description for this dynamic collection.
4. Select the filters to define the dynamic collection from each of the drop-down menus.
5. Click Apply to preview the CVDs that are filtered into the collection to ensure that your filter is accurate.

   The filtered CVDs are displayed in the list.
6. Click Save.

Add Dynamic Collections by Using Active Directory

You can use Active Directory (AD) to add a dynamic CVD collection. You can add CVDs to the collection by Active Directory group, organizational unit, or domain. You can create a filter for multiple Active Directory elements, for example, filter CVDs whose users belong to the Human Resources AD group or to the Marketing AD group.

The Active Directory is updated whenever a device is authenticated. Active Directory information might change, such as the organizational unit, if the Active Directory is updated for that user or device.

Procedure

1. In the Mirage Web Management, click the Collections tab.
2. Select Create New > Dynamic Collection.
3. Type the name and description for this dynamic collection.
4. Set the filter to define the dynamic collection by Active Directory group, Active Directory organizational unit, or Active Directory domain.
5. Click Apply to view the CVDs filtered to the collection.

   The filtered CVDs that are defined as Active Directory appear in the list.
6. Click Save.

Edit Collection

You can use the Edit Collection action to modify the collection properties, add or remove a CVD, or manage the CVDs in the collection.

Procedure

1. In the Mirage Web Management, click the Collections tab.
2. Select the collection you want to edit and click Edit.

   Do not click on the device name.
3. Click Save after editing the collection.
Mirage provides multiple storage volume support to help manage volume congestion.

Each storage volume can contain base layers, app layers, and CVDs. CVDs are assigned to a storage volume when they are created. The storage volumes must be shared by the servers where network-attached storage (NAS) permissions must be in place.

You can perform various actions with storage volumes in the Mirage Web management.

Table 7-1. Working with Storage Volumes

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a volume to the Mirage system.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit volume parameters.</td>
</tr>
<tr>
<td>Remove</td>
<td>Remove a volume from the Mirage system.</td>
</tr>
<tr>
<td>Block</td>
<td>Block a storage volume to prevent it from being used when new CVDs or base layers are created. Blocking a storage volume is useful when the volume reaches a volume capacity threshold or to stop populating it with new CVDs or base layers. Blocking a volume does not affect access or updates to existing CVDs and base layers on the volume. <strong>IMPORTANT</strong> You cannot move a CVD or base layer to a blocked volume. You can move a CVD or base layer from a blocked volume.</td>
</tr>
<tr>
<td>Unblock</td>
<td>Unblock a volume that is currently blocked. After you unblock a volume, you can add new CVDs and base layers, and you can update existing data.</td>
</tr>
<tr>
<td>Mount</td>
<td>Mount a volume to the Mirage system.</td>
</tr>
<tr>
<td>Unmount</td>
<td>Unmount a volume to the Mirage system.</td>
</tr>
</tbody>
</table>
Working with Reports for Mirage Operations

You can generate and view reports on demand. Reports display the status of various Mirage operations. You access, generate, import, and export reports from the Reports tab in the Mirage Web Management.

You can preview a report as a PDF. The preview displays in a new tab of the Web browser. Ensure that you disable pop-up blocker.

The maximum number of records that you can include in a report by default is 2,000. If the report includes more than 2,000 records, the report fails to generate. When you generate a report that contains more than 200 records, you receive a warning message that the procedure might take some time to generate. You can configure these parameters by editing the configuration files located in C:\Program Files\Wanova\Mirage Web Management\web.config.

- <add key="ReportRecordCriticalThreshold" value="0"/>
- <add key="ReportRecordWarnThreshold" value="0"/>

Centralization Progress

You generate the Centralization Progress report during the first phase of the Mirage deployment to view the progress of CVDs being centralized. The Centralization Progress report displays the centralization status of CVDs and the average time, average CVD size, and average data transfer size of completed CVDs during the specified time frame for the report.

OS Migration Process

The OS Migration Process report displays the number of CVDs that have started, are still pending, and have completed an OS migration procedure.

Endpoint Provisioning Progress Report

You generate the Endpoint Provisioning report to view the CVDs that are being provisioned and the CVDs that have completed provisioning during the specified time frame for the report.

Data Protection Status

You generate the Data Protection Status report to view the percentage of users’ systems that are backed up. The Data Protection Status report displays the data protection status of CVDs and lists the CVDs and users for whom an upload procedure is incomplete.

Custom Report

You can create a custom report based on your organization’s requirements.
This chapter includes the following topics:

- “Create a Custom Report,” on page 34
- “Export Legacy Reports,” on page 34
- “Import the Mirage Reports Package,” on page 35
- “Export Grid Data to CSV,” on page 35

Create a Custom Report

A default report template is deployed when you install the Mirage Management server. You can create a new report template by modifying the ReportTemplate.rdl file and importing it to the Mirage Web management.

Prerequisites

- Install the Mirage Management server.
- Install SSRS for the Mirage Web Management.

Procedure

2. Configure the ReportTemplate.rdl.
4. Import the custom report to the Mirage Web Management.
   a. Access the Mirage Web Management.
   b. On the Reports tab click Import.
   c. Select the custom report you created and click Import.

What to do next

You can now generate the custom report.

Export Legacy Reports

You can export reports that were generated with Mirage 5.2. Reports are exported as a Microsoft Excel files.

The .exe server tool file is created when you install the Mirage Management server. It is located in the

Prerequisites

- Install the Mirage Management server.
- Ensure that you have administrator privileges.

Procedure

Configure the legacy report settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>foldername</td>
<td>Folder where the legacy reports are exported. This parameter is mandatory.</td>
</tr>
<tr>
<td>from</td>
<td>Start date for the time frame of when the legacy reports were created. This parameter is optional.</td>
</tr>
<tr>
<td>to</td>
<td>End date for the time frame of when legacy reports were created. This parameter is optional.</td>
</tr>
<tr>
<td>type</td>
<td>Report type. This parameter is optional. The default report type is All.</td>
</tr>
</tbody>
</table>

**Import the Mirage Reports Package**

The Mirage reports package contains pre-configured reports. You download the reports package and import the reports using the Mirage Web management.

*Note* The reports in the reports package were created by Mirage field engineers for evaluation purposes. Mirage does not officially support the reports in the reports package.

**Prerequisites**

- Install the Mirage Management server.
- Install SSRS for the Mirage Web management.

**Procedure**

1. Access the Mirage Web management and click the **Reports** tab.
2. Click the VMware Mirage Reports Package link.
4. Select **View and Download Products > VMware Mirage Drivers and Tools**. Click the reportspackage file to download the Mirage reports package and select a location to save the reports package.
5. Click **Go to Downloads** and select the **VMwareMirageReportsPackage.zip** file.
6. In the Mirage Web management, click the **Reports** tab and click **Import**.
7. Navigate to the location where you saved the reports package file, and select the file .rdl file to import.
8. Specify a name and description for the reports.

You can now generate the reports package reports.

**Export Grid Data to CSV**

You can use this feature to export all of the data that is presented in the Web console grid to a CSV file. As an administrator, you can export the CSV file to Microsoft Excel for further analysis.

You can export the data from the following grids:

- CVD inventory
- Pending devices
- Tasks
- Assignments
- Logs (all inner event tabs, including transactions and audit events)
Layers

Policies

Collections

**Procedure**

1. Log in to your Web Management Console and navigate to the grid from where you want to export the data.

2. Click the **Export** button on the upper right corner of the grid.

   The CSV file containing all the data from the selected grid is saved on your system.
Managing Mirage Tasks

Users with the Image Manager role or Administrator role can manage all Mirage tasks.

You can click on a hyperlinked task name to view the layer assignments of the selected task.

You can perform actions with Mirage tasks.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Refresh the list of tasks.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete a task with a status of complete, canceled, or finished. You cannot</td>
</tr>
<tr>
<td></td>
<td>delete tasks that have a status of paused or active.</td>
</tr>
<tr>
<td>Pause</td>
<td>Pause an active task.</td>
</tr>
<tr>
<td>Resume</td>
<td>Resume a task that is paused.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancel an active or paused task.</td>
</tr>
<tr>
<td>Start Migration</td>
<td>Starts the Windows OS migration procedure for the device in the selected</td>
</tr>
<tr>
<td></td>
<td>task.</td>
</tr>
<tr>
<td>Apply Layers</td>
<td>Apply layers to the selected device.</td>
</tr>
<tr>
<td>Finalize App Layer Capture</td>
<td>Finalize an app layer capture procedure that was started when you created</td>
</tr>
<tr>
<td></td>
<td>a reference CVD.</td>
</tr>
</tbody>
</table>

Table 9-1. Working with Tasks
Managing the Driver Library

You use the driver library to manage hardware-specific drivers in a separate repository, organized by hardware families.

You add drivers with an import wizard and view them in the driver library’s console.

You can configure the system to add the necessary driver library to the relevant endpoints based on matching profiles between the library and the endpoint configuration.

The driver handling is unconnected to layers. Not having to include drivers in the layer results in smaller and more generic layers.

Mirage does not install the drivers. Mirage delivers the driver to the endpoint and Windows determines whether to install the driver.

You can perform various actions on driver libraries.

Table 10-1. Mirage Driver Library

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a driver to a driver library.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete a driver from a driver library.</td>
</tr>
<tr>
<td>Import</td>
<td>Import a driver library. You can retain the original driver folder hierarchy of the driver library that you import to the Mirage driver library.</td>
</tr>
</tbody>
</table>
The driver library copies drivers from the Mirage system to the endpoint. When Windows scans for hardware changes, these copied drivers are used by the Windows Plug and Play (PnP) mechanism, and the appropriate drivers are installed as required.

This diagram illustrates the driver library architecture and how rules associate drivers to endpoints.

**Figure 11-1. Driver Library Architecture**

- Profile A contains drivers from driver folder 1 and 2. When the profile is analyzed, the drivers from those folders are applied to two endpoints.
- Profile B contains drivers only from driver folder 2, which is also used by profile A. When the profile is analyzed, the drivers from that folder are applied to only one endpoint.

The Mirage system can have multiple driver folders, multiple driver profiles, and many endpoints. A driver profile can contain drivers from multiple driver folders and multiple driver profiles can use a driver folder.

You can apply a driver profile to one, many, or no endpoints. The driver library is used during the following operations:
- Centralization
- Migration
- Hardware migration and restore
- Machine cleanup
- Base layer update
- Set driver library
- Endpoint provisioning
Managing Driver Profiles

The driver library also contains driver profiles. A driver profile is used to select the driver folders to publish to a particular hardware model or set.

A driver profile can select one or more driver folders.

Driver profile rules check if a driver applies to a particular hardware, and can select one or more matching driver profiles for a device.
Managing Mirage Assignments

Users with the Image Manager role or Administrator role can start or cancel migration procedures on CVDs.

The assignments grid view displays by default only active assignments. You can clear the *Show active assignments only* checkbox to view all assignments, including assignments that are no longer applied to CVDs.

You can filter the assignments grid view by assignment status.
Users with the Image Manager role or Administrator role can view and manage Mirage event logs.

You can perform actions on the Mirage event logs.

**Table 14-1. Managing Mirage Event Logs**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Deletes selected event log files.</td>
</tr>
<tr>
<td>Acknowledge</td>
<td>Changes the status of an event log file to Acknowledged in the Acknowledged column, indicated with a green check icon.</td>
</tr>
<tr>
<td>Reinstate</td>
<td>Removes the Acknowledged status of an event log file in the Acknowledged column, indicated with a red X icon.</td>
</tr>
<tr>
<td>Delete All</td>
<td>Deletes all event logs displayed in the Logs grid view. If there is no filter applied to the Logs grid view, all log files in the system are deleted.</td>
</tr>
<tr>
<td>Delete All Acknowledged</td>
<td>Deletes all event log files with a status of Acknowledged.</td>
</tr>
</tbody>
</table>
Managing Branch Reflectors

Using Mirage branch reflectors promotes efficient distribution to branch offices and remote sites where multiple users share the WAN link to the data center. You can enable the branch reflector peering service on endpoint devices that are installed with a Mirage client.

The branch reflector downloads base layer images, app layers, driver files, and USMT files from the Mirage server and makes them available for transfer to other Mirage clients in the site. Only files that reside on the branch reflector machine’s disk are transferred and files are not requested from the Mirage server at all.

In this way, files are downloaded to the branch reflector only once, and common files across base layers become readily available to other clients without duplicate downloads.

Table 15-1. Managing Branch Reflectors

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync</td>
<td>Starts the upload to the CVD.</td>
</tr>
<tr>
<td>Suspend</td>
<td>You can suspend network communications with the server for the branch reflectors and for regular endpoint devices. Suspending network operations for a branch reflector still allows peer clients to download layer files from the branch reflector cache, but the branch reflector cannot download new files from the server.</td>
</tr>
<tr>
<td>Resume</td>
<td>When you resume network operations, the branch reflector or the individual endpoint device can communicate with the Mirage server cluster.</td>
</tr>
<tr>
<td>Restart</td>
<td>Restart the branch reflector device.</td>
</tr>
<tr>
<td>Disable Branch Reflector</td>
<td>When a branch reflector is disabled, the device is deleted from the branch reflectors list. But it continues to be available because an endpoint device remains as a regular Mirage endpoint in the device inventory. When a branch reflector is disabled, its base layer cache is deleted.</td>
</tr>
<tr>
<td>Rebuild Local Cache</td>
<td>Clears the cached files on the branch reflector machine.</td>
</tr>
<tr>
<td>Configure</td>
<td>Use the Configure feature to configure specific branch reflector values.</td>
</tr>
<tr>
<td>Reject Peers</td>
<td>When the branch reflector is operating slowly or is using excessive bandwidth, you can stop providing service to its peer clients. You can resume providing service to the peer clients of a paused branch reflector at any time. When you use the Reject Peers feature, the branch reflector is not deleted from the branch reflectors list. The branch reflector cache is preserved.</td>
</tr>
</tbody>
</table>
Table 15-1. Managing Branch Reflectors ( Continued )

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accept Peers</strong></td>
<td>Use the Accept Peers feature to resume providing service to the peer clients of a paused branch reflector.</td>
</tr>
<tr>
<td><strong>Collect Logs</strong></td>
<td>Collects logs on the branch reflector device.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- “Branch Reflector Matching Process,” on page 50
- “Select Clients To Be Branch Reflectors,” on page 50
- “Configure Defaults for Branch Reflectors,” on page 51
- “Wake on LAN,” on page 51
- “Configure Wake on LAN,” on page 52

**Branch Reflector Matching Process**

You can enable one or more branch reflectors per site. Client endpoints detect enabled branch reflectors on the same or different sites.

The Mirage IP detection and proximity algorithm finds a matching branch reflector using the following process:

1. The algorithm first verifies that a potential branch reflector is in the same subnet as the client.

2. If the branch reflector is in a different subnet, the algorithm checks if the branch reflector is configured to service the client subnet.

   Alternatively, the algorithm can use the client site information to check that the branch reflector is in the same Active Directory site as the client.

3. The algorithm checks that the latency between the branch reflector and the client is within the threshold.

4. If a client and branch reflector match is found that satisfies these conditions, the client connects to the branch reflector to download a base layer. Otherwise, the client repeats the matching process with the next branch reflector.

5. If no match is found or all suitable branch reflectors are currently unavailable, the client connects to the server directly.

   In this case, the client connects to the Mirage server only if no branch reflectors are defined for the specific endpoint.

**Select Clients To Be Branch Reflectors**

You can select any Mirage client endpoint to function as a branch reflector, in addition to serving a user. Alternatively, you can designate a branch reflector to a dedicated host to support larger populations. A branch reflector can run on any operating system compatible with Mirage clients.

**Prerequisites**

Clients that serve as branch reflectors must satisfy the following conditions:

- Connect the device that will serve as a branch reflector to a switched LAN rather than to a wireless network.
- Verify that enough disk space is available to store the base layers of the connected endpoint devices.
Configure Defaults for Branch Reflectors

You can set default values of parameters that govern the behavior of branch reflectors.

The current Maximum Connections and Cache Size values apply to newly defined branch reflectors. You can correct them individually for selected branch reflectors.

Other parameters in this window apply system-wide to all branch reflectors, existing or new.

Prerequisites

Verify that the branch reflector endpoint has enough disk space to support the Default Cache Size value, in addition to its other use as a general purpose desktop.

Procedure

1. Click the gear icon on the top right side of the screen and select General Settings > Branch Reflector.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Maximum Connections</td>
<td>Type the maximum number of endpoint devices that can simultaneously connect to the branch reflector.</td>
</tr>
<tr>
<td>Default Cache Size (GB)</td>
<td>Type the cache size that the branch reflector allocated.</td>
</tr>
<tr>
<td>Required Proximity (msec)</td>
<td>Type the maximum time, for example 50 ms, for a branch reflector to answer a ping before an endpoint considers downloading through the branch reflector. The endpoint downloads from the server if no branch reflectors satisfy the specified proximity.</td>
</tr>
<tr>
<td>Use Active Directory Sites</td>
<td>Mirage uses subnet and physical proximity information to choose branch reflectors. Select this check box to use Active Directory site information to determine to which branch reflector to connect.</td>
</tr>
<tr>
<td>Always Use Branch Reflector</td>
<td>To keep network traffic as low as possible, select this option to force clients to continually repeat the matching process until a suitable branch reflector becomes available. In this case, a client connects to the Mirage server only if no branch reflectors are defined. If the option is not selected, and no match is found or suitable branch reflectors are currently unavailable, the client connects to the Mirage server directly as a last resort.</td>
</tr>
<tr>
<td>Wake-on-LAN</td>
<td>The Wake-On-LAN protocol allows the administrator to start machines from a dormant state (State from which you can resume. Depends on the NIC, and whether it keeps a low power state).</td>
</tr>
</tbody>
</table>

2. Click OK.

Wake on LAN

The Wake-on-LAN protocol allows the administrator to start machines from a dormant state (State from which you can resume. Depends on the NIC, and whether it keeps a low power state). A Wake-on-Lan packet is sent during flows manually run by the customer.

A Wake-on-LAN packet is sent during flows manually run by the customer:

- Enforce Base Layer
- Provisioning
- Migration
- Assign Base Layer/Application Layer
- Restore
- Centralization

Packets are sent only if the endpoint is down when the flow is initiated. The packet is sent to the broadcast address by the management server. Servers will request all the branch reflectors to send wake on lan packets in their own subnet.

**Configure Wake on LAN**

The Wake-on-LAN protocol allows the administrator to start machines from a dormant state (State from which you can resume. Depends on the NIC, and whether it keeps a low power state). A Wake-on-Lan packet is sent during flows manually run by the customer:

**Prerequisites**

Go to **System Configuration** > **Branch Reflectors** > Select **Wake On LAN**.

Make sure the infrastructure supports wake on LAN:

- Networking infrastructure
- Enable Wake On LAN in the BIOS of the endpoint
- Enable Wake On LAN in Windows

**Note**  The following procedure is an example to show the Wake-on-LAN procedure. You can run through any flow to automatically awaken the VM from dormant state.

**Procedure**

1. Log in to your **Web Console**.
2. Go to **Pending Devices** and select the dormant machine that you want to start.
3. Click **Centralize Endpoint**.
4. In the **Select CVD Policy** section of the **Centralize Endpoint** window, select **VMware Mirage default CVD policy**, and click **Next**.
5. In the **Data Layer Selection** section of the **Centralize Endpoint** window, select **Do not use a base layer**, and click **Next**.
6. In the **Target Volume Selection** section of the **Centralize Endpoint** window, ** Automatically chose a volume**, and click **Next**.

The selected machine is awakened from a dormant state.
Managing Mirage Servers, Mirage Management Servers, and Mirage Gateway Servers

You can view information about the Mirage servers, Mirage Management servers, and Mirage Gateway servers in your environment, such as server status, connections, port, and so on.

You can perform various actions for the servers.

Table 16-1. Managing Mirage servers, Mirage Management servers

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure</td>
<td>Configure the maximum connections, port, transport type, and certificate information.</td>
</tr>
<tr>
<td>Remove</td>
<td>Remove the selected servers.</td>
</tr>
<tr>
<td>Start</td>
<td>Start the selected servers.</td>
</tr>
<tr>
<td>Stop</td>
<td>Stop the selected servers.</td>
</tr>
<tr>
<td>Collect Logs</td>
<td>You select the report level, destination, and UNC path.</td>
</tr>
</tbody>
</table>

You can configure and remove Mirage Gateway servers.

You can view the MongoDB path on the Management Servers tab. If a Mirage Management server has less than 5% of available disk space, uploads are suspended for all Mirage Management servers in the Mirage system. Uploads restart after there is sufficient free disk space on the Mirage Management server or after you move the MongoDB database to a drive with sufficient free disk space.

As an administrator, you can move the MongoDB data of a selected Mirage Management Server to a different location. This feature is enabled only after installing more than one Mirage Management Server. In your Web Management, click Servers > Management Servers > Configure. In the Configure Mirage Management Server dialog, enter the name of the location where you move the MongoDB data and click OK.

The Web Management generates events for MongoDB connectivity issues that enables you to take action in time to protect MongoDB from corruptions.

The events are generated in the following cases:

- MongoDB Frequent Crashes: When the system experiences more than a certain number of unexpected MongoDB crashes in the stipulated time period.
- MongoDB Connectivity Issues: When the system experiences 20 incidents of disk latency higher than 1 second during a period of 3 days, for the disk storing the MongoDB data.

In both the cases, the Mirage Management server stops its MongoDB instance immediately.

A critical event is generated and the status of the Management Server changes to “Mongo service is Down” in the Management Servers tab.
To bring Management Server back to its normal state, use the Start command from the Management Servers tab in the Mirage Web Console.

If your configuration has only one Mirage Management Server, the Web Management displays a red banner with the following message:

Your system only has a single active Management Server. Set up multiple Management Servers to prevent data loss in case the Management Server fails.
You can apply settings to your Mirage installation that the administrator can configure, including the retention policy for snapshots. You can also configure the system to use Secure Sockets Layer (SSL) communication between the Mirage client and server.

To configure system settings by using the Mirage Web Management, click the gear icon in the upper-right corner.

This chapter includes the following topics:

- “Managing Bandwidth Limitation Rules,” on page 55
- “License Settings,” on page 56
- “Authenticating the Mirage Gateway Server,” on page 56
- “Branch Reflector Settings,” on page 57
- “Configuring User Access to the File Portal,” on page 57
- “General System Settings,” on page 57
- “Export Mirage System Settings,” on page 58

Managing Bandwidth Limitation Rules

You can set an upper limit on Mirage traffic so that Mirage does not consume all of the bandwidth of a site or subnet. When you use bandwidth limitation, you allocate your network resources more efficiently.

A bandwidth limitation rule contains parameters to set the limitations.

Table 17-1. Bandwidth Limitation Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SubnetMaskV4</td>
<td>Uses the format Ipaddress/bitmask, for example, 100.100.10.100/20.</td>
</tr>
<tr>
<td></td>
<td>For site-based rules, leave this parameter blank.</td>
</tr>
<tr>
<td>Site</td>
<td>Site or domain name of the group of clients for which to limit the bandwidth. The site is the DNS name. Site names cannot contain special characters or non-English characters. For subnet-based rules, leave this parameter blank.</td>
</tr>
<tr>
<td>Download limit</td>
<td>Maximum number of KBps that you can download from the server to the client.</td>
</tr>
<tr>
<td>Upload limit</td>
<td>Maximum number in KBps that you can upload from the client to the server.</td>
</tr>
</tbody>
</table>
Table 17-1. Bandwidth Limitation Parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Time that the rule is applied, for example, 7:00 AM. The time is the local time of the endpoint. It can take up to five minutes after the start time for the rule to be applied.</td>
</tr>
<tr>
<td>End Time</td>
<td>Time that the rule is no longer applicable, for example, 9:00 PM. The time is the local time of the endpoint. It can take up to five minutes after the end time to revoke the rule.</td>
</tr>
<tr>
<td>Days of Week Time</td>
<td>The days of the week that the rule is valid, for example, Monday, Thursday, and Friday. The day is calculated according to the local time of the endpoint.</td>
</tr>
</tbody>
</table>

To add a rule using the Mirage Web management, click Add and edit the bandwidth limiting parameters. To edit a rule that you created, double-click the rule and edit the bandwidth limiting parameters.

You write the rules in a .csv file and import the file using the Mirage Web management. You write the rules in the format \texttt{SubnetMaskV4,Site,Download Limit,Upload Limit, Start Time, End Time, Days of Week}. Click Sample Rules to view a sample rule.

After you write rules, you import the rules by using the Mirage Web management. You can also export existing rules to edit the rules, and import the edited rules to the Mirage Web management. Imported rules replace and overwrite existing rules.

You can add a global limit rule that applies to all clients in the Mirage environment. For example, 0.0.0.0/0,,OutgoingKBps,UploadKBps.

Table 17-2. Rule Constraints and Limitations

<table>
<thead>
<tr>
<th>Constraints</th>
<th>Rule Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>No time constraint specified.</td>
<td>No time limit. Rule is applicable 24 hours on the days specified.</td>
</tr>
<tr>
<td>No day constraint specified.</td>
<td>No day limit. Rule is applicable every day on the time specified.</td>
</tr>
<tr>
<td>No time or day constraint specified.</td>
<td>Always applicable.</td>
</tr>
<tr>
<td>Blank.</td>
<td>Unlimited.</td>
</tr>
<tr>
<td>Zero (0).</td>
<td>Blocked.</td>
</tr>
</tbody>
</table>

License Settings

License settings are used to add a license to Mirage or view existing licenses.

For the relevant procedures, see the \texttt{VMware Mirage Installation Guide}.

Authenticating the Mirage Gateway Server

You can create a custom message that end users receive when they log on to the Mirage system using the Mirage Gateway server.

To create a custom message for end users, click the gear icon in the upper-right corner, click Gateway Authentication, select the Enable Gateway Customization Log-on Message check box, and type the custom message.
Branch Reflector Settings

Branch reflector settings include default values of parameters governing the behavior of branch reflectors. You can update the default values for the branch reflector. See “Configure Defaults for Branch Reflectors,” on page 51.

Configuring User Access to the File Portal

You can create a custom message that is displayed to end users to access the file portal. You can also enable access to the file portal for end users.

To provide users access to the file portal, select the Enable File Portal check box and type the file portal URL in the File Portal URL text box.

To create a custom message that is displayed to end users to access the file portal, type the message in the text box.

General System Settings

You can define the standard configurations for the Mirage system.

Table 17-3. General System Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshots kept</td>
<td>The number of CVD snapshots the system must keep available for restoration, at hour, day, week, and month intervals. For more information about how these values are used in snapshot retention.</td>
</tr>
<tr>
<td>Volumes</td>
<td>This section configures the threshold percentages of data stored on a volume, which when reached, trigger a warning. This section configures the threshold percentages of data stored on a volume, which when reached, trigger a warning or critical events in the Events log.</td>
</tr>
<tr>
<td></td>
<td>Volume capacity - warning threshold (%): Type the threshold percentage of data stored on a volume, which triggers a warning event when reached.</td>
</tr>
<tr>
<td></td>
<td>Volume capacity - critical threshold (%): Type the threshold percentage of data stored on a volume, which triggers a critical event when reached.</td>
</tr>
<tr>
<td></td>
<td>Volume capacity check interval (seconds): Type the elapsed time interval (in seconds) at which the system rechecks the level of data stored on the volume against the thresholds.</td>
</tr>
<tr>
<td></td>
<td>Driver Library and USMT files volume: To select the volume to be addressed by the threshold checks, click Change and select the required volume.</td>
</tr>
<tr>
<td>CVDs</td>
<td>CVD size warning threshold (MB): Type the maximum CVD size. An event is generated in the Event Log when that size is reached.</td>
</tr>
<tr>
<td></td>
<td>Default Upload Policy: To choose the default upload policy used when an end user adds their CVD to the Mirage system, click Change and select the required policy.</td>
</tr>
</tbody>
</table>

Branch Reflector


Report

Specify the report server URL. For more information, see Chapter 8, “Working with Reports for Mirage Operations,” on page 33.

Join Domain Account

User and Password: Account that authorizes joining the domain. The join domain account is used during migration operations. Note: The join domain account must have the following permissions - Reset Password, Write all properties, Delete, Create computer objects, and Delete computer objects. Permissions are set using the Advanced Security Settings for Computers dialog box for this object and all descendant objects.
### Table 17-3. General System Settings (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Bandwidth Limiting | You can set an upper limit on Mirage traffic so that Mirage does not consume all of the bandwidth of a site or subnet. When you use bandwidth limitation, you allocate your network resources more efficiently. A bandwidth limitation rule contains parameters to set the limitations.  
You can import rules, export rules, and view sample rules, and create new rules by specifying several parameters. See “Managing Bandwidth Limitation Rules,” on page 55. |
| License          | You can specify a license key or a license file, and view license information.                                                                                                                                   |

### Export Mirage System Settings

If your current Mirage system deployment exceeds the maximum number of clients, you can migrate all of the systems settings from your current deployment to your new deployment. This helps you to easily install and configure your new Mirage system. You can export the Mirage system configuration and layers to a self-contained archive using a command-line tool that is external to Mirage. You can use the exported items later to import and synchronise items to your new Mirage deployment.

You can export the following items from your current Mirage deployment to a zip file:

- System settings
- Configuration files
- Bandwidth limiting settings
- USMT files
- Driver libraries
- Master and CVD policies
- Base layers
- Application layers

**Procedure**

1. To export the Mirage system configuration and layers to a self-contained archive, run the following command.

   ```
   C:\Program Files\Wanova\Mirage Management Server\Wanova.Server.Tools.exe" ExportSystemSettings –MirageMgmtIp 10.23.220.55 –outputFolder c:\temp\configParams
   ```

   Where,
   - `MirageMgmtIp` is followed by the IP address of the Mirage management server
   - `outputFolder` is followed by the full-path of the folder where you want to save the exported self-contained archive. The path provided should be empty or contain a previously exported settings.

2. To view the progress of the utility, go to the **VMware Mirage Console** on your Mirage System and select **Task Monitoring**.

   **Note** You can only track the progress of the tasks from the **Task Monitoring** option in the VMware Mirage Console. Use the command-line tool to abort exporting the system configurations files.
Index

A
about the Web Manager 7
app layer, capturing 11
app layer capture 11
app layer definition 11
app layers 21
assignments 45
authenticating, Mirage Gateway server 56

B
bandwidth limitation, rules 55
base layer, capturing 11
base layer definition 11
base layers 21
branch reflectors
   configuration 51
default values 51
   IP detection and proximity algorithm 50
   matching process 50
   select clients to be branch reflectors 50
   settings in system configuration 57

C
centralization progress, report 33
centralize endpoints 17
configure the system, See system settings
configuring, file portal 57
CVD
   assign upload policy 13
   manage collections 14
   migration 17
   move to a different volume 14
   settings 57
   view files in CVD with the file portal 13
CVD Integrity report 15, 33
CVD collection
   add dynamic using Active Directory 29
dynamic 29
   static collection management 28
CVD collection, edit collection 29
CVD collection, static collection management 28
CVD management tasks 9
CVDs, collections 27

D
data protection status, report 33
Delete Pending Device 19
device, reboot 10
disaster recovery 12
drivers
   driver library 39
driver library architecture 41
   driver profile management 43
dynamic collections 29
dynamic CVD collection, adding 29

E
end-user operations, view files in CVD with the
   file portal 13
endpoint disaster recovery
   reconnect a device to a CVD 19
   restore a CVD snapshot 12
endpoints
   centralizing 17
   layer provisioning 19
enforce layers on endpoints 10
Export 58
exporting bandwidth limitation rules 55

F
file portal, configuring 57

G
Gateway servers, configuring 53
Grid Data 35

H
hardware drivers, See drivers
help desk login 7

I
importing bandwidth limitation rules 55
IP detection and proximity algorithm 50

J
Join Domain Account settings 57

L
layers, capturing base layers 11
layers provisioning 19

VMware, Inc.
legacy reports, export 34
license keys 21
licenses for Mirage 56
login to the Web Manager 7

M
migrate to Windows OS, See Windows OS migration
migration, Windows OS 45
Mirage Management servers 53
Mirage servers 53
Mirage events, logs 47
Mirage Gateway server, authenticating 56
Mirage logs 47

O
OS migration progress, report 33

P
policy rules
  add 25
  edit 25
  rule exception 25
provisioning, See layers provisioning

R
reference machine 18
replacement devices 17
report template, configuring 34
reports
  centralization progress 33
  configuring 34
  CVD integrity 15, 33
  data protection status 33
  Mirage reports package 35
  OS migration progress 33
  package 35
restore, specific files from a CVD snapshot 12

S
servers, management 53
snapshots kept 57
SSRS, legacy reports 34
storage volumes 31
system settings
  branch reflector settings 57
  general system settings 57
  licenses for Mirage 56

U
upload policies, parameters 24

V
volume settings 57