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 Manager Guide 5

1 About the Mirage Web Manager 7
   Access the Web Manager 7

2 Managing CVDs 9
   Restart a Device 10
   Enforce Layers on Endpoints 10
   Endpoint Disaster Recovery 11
   Working with the File Portal 12
   Assign an Upload Policy 12
   Manage Collections 13
   Move a CVD to a Different Volume 13

3 Base Layers and App Layers 15
   Capturing Base Layers 15
   Capturing App Layers 16

4 Managing Collection Devices 17

5 Working with Endpoints 19
   Creating a Reference Machine from an Endpoint 19
   Centralizing Endpoints 19
   Migrate a CVD to a Replacement Device 19

6 Working with Upload Policies 23
   Upload Policy Parameters 24
   Add New Upload Policies 25
   Edit Upload Policies 25
   Add or Edit Upload Policy Rules 25
   Upgrade an Upload Policy 26

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

8 Working with Storage Volumes 31
   Block Storage Volumes 31
Unblock Storage Volumes 32

9 Working with Layers 33

10 Managing Mirage Tasks 35

11 Working with Reports for Mirage Operations 37
   Export Legacy Reports 38

Index 39
About the Mirage Web Manager Guide

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

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.
About the Mirage Web Manager

Mirage users can use the Mirage Web Manager to perform role-based actions on CVDs, upload policies, volumes, layers, and so on.

The Web Manager is used by various Mirage user roles.

<table>
<thead>
<tr>
<th>Table 1-1. Web Manager User Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
</tr>
<tr>
<td>Help Desk</td>
</tr>
<tr>
<td>Image Manager</td>
</tr>
<tr>
<td>Protection Manager</td>
</tr>
</tbody>
</table>

Mirage Web Manager 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 Manager

You must log in each time you open the application.

**Prerequisites**

Ensure that you installed the Mirage Web Manager.

**Procedure**


   *WebManagerServer* is the DNS name or IP address of the server where the Mirage Web Manager 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.

- **Endpoint Disaster Recovery** on page 11
  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 12
  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 12
  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 13
  You can add a collection to the CVD or remove a collection from a CVD.

- **Move a CVD to a Different Volume** on page 13
  You can move a CVD to a different storage volume, according to your disk organization requirements.
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 Manager, 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 Manager, 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.
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 6, “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 Manager, 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. See **Working with Upload Policies**.

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>
</table>
| If to the same OS, for example, Windows 8.1 to Windows 8.1: | 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. |
| If to a different OS, for example, Windows 8.1 to Windows 7: | This checkbox is not selected so the entire CVD, including the User area, is always restored from the CVD snapshot. |

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 Manager, 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 Manager, 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 Manager, 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>
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.

This chapter includes the following topics:

- “Capturing Base Layers,” on page 15
- “Capturing App Layers,” on page 16

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.

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. See Assigning App Layers.

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.

See Base Layers and App Layers and Layer Management Life Cycle.

For more information, see the VMware Mirage Administrator’s Guide.
Managing Collection Devices

On the **Collections** tab of the Mirage Web Manager, you can manage the devices that are assigned to the collection or to a CVD in a collection.

You can perform actions such as suspend network operations, resume network operations, enforce layers, and assign an upload policy.
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:

- “Creating a Reference Machine from an Endpoint,” on page 19
- “Centralizing Endpoints,” on page 19
- “Migrate a CVD to a Replacement Device,” on page 19

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. See Layer Management Life Cycle.

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.

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 5-1. 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 **Pending Devices** on the left panel.
2. Select the required device from the search results list.
3. In the device information window, click **Hardware Migration**.
4. Select the CVD from the CVD Selection list and click **Next**.
5. Select a migration option for the selected CVD and device and click **Next**.
   - If you select **Full System Migration**, you must specify whether to assign a base layer in the next step.
   - If you select **Only Migrate User Data and Settings**, you must specify a machine name.
6. Select a base layer option.
   a. (Optional) Select **Do not use a base layer** to select a base layer later, and click **Next**.
   b. (Optional) Select **Select a base layer from list** to apply to the CVD.
      - Select one or more app layers to migrate from the Available Layers pane and click **Add Layers**.
      - Click **Next**.
7 Select the option that determines how the device is named.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep CVD Name</td>
<td>Uses the name of the CVD you selected.</td>
</tr>
<tr>
<td>Use Device Name</td>
<td>Uses the name of the device you selected.</td>
</tr>
<tr>
<td>Set New Name</td>
<td>Enables you to specify a new name.</td>
</tr>
</tbody>
</table>

8 Select a workgroup or a domain for the endpoint to be included in following the restore operation.

a (Optional) Type the name of the workgroup for this endpoint to join.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workgroup</td>
<td>Type the name of the workgroup for this endpoint to join.</td>
</tr>
<tr>
<td>Domain</td>
<td>▪ Type the domain name or select from the drop-down menu.</td>
</tr>
<tr>
<td></td>
<td>▪ Verify that the OU is in standard open LDAP format. For example, OU=Notebooks, OU=Hardware, DC=VMware, DC=com.</td>
</tr>
<tr>
<td></td>
<td>▪ Specify the username and password for the join domain account. The join domain account must meet the appropriate security privilege requirements as defined in the system general settings. The account must have access to join the domain. This is not validated.</td>
</tr>
</tbody>
</table>

The current domain is shown by default.

9 Click Next.

10 Use the Validation Summary to compare the target device with the CVD.

You cannot proceed until you resolve the blocking issues.

11 Click Next and click Finish.
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 Manager. You can create a new upload policy, and edit, delete, and upgrade existing upload policies.

You create upload policies by defining 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.

The list of files that are not protected is defined by a set of rules and exceptions.

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:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mirage default upload policy</strong></td>
<td>Use on Mirage servers that manage CVDs on distributed physical devices.</td>
</tr>
<tr>
<td><strong>VMware Horizon View optimized upload policy</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
- **Upload Policy Parameters** on page 24
  Upload policies have various parameters that you can view, configure, and edit.

- **Add New Upload Policies** on page 25
  When you add a new upload policy, the new policy is added to the respective node.

- **Edit Upload Policies** on page 25
  You can edit an upload policy in the Mirage Web Manager and distribute the revised policy.

- **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.

- **Upgrade an Upload Policy** on page 26
  When upgrading a policy with a new minor or major version, you can upgrade the CVDs that are assigned to the previous upload policy version.

### Upload Policy Parameters

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

#### Table 6-1. Upload Policy Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Description</td>
<td>Name and description of the policy.</td>
</tr>
<tr>
<td>Upload change interval</td>
<td>Denotes how frequently the client attempts to synchronize with the server. The default is every 60 minutes. End users can override the policy in effect at an endpoint. See Suspend and Reactivate Synchronization. The Upload change interval affects the frequency of automatic CVD snapshot creation. See CVD Snapshot Generation and Retention.</td>
</tr>
<tr>
<td>Protected volumes</td>
<td>Denotes which volumes to centralize from the endpoint to the CVD in the server. All fixed volumes are protected by default. You can select to protect only the system volumes and add more volumes by using the assigned drive letters.</td>
</tr>
<tr>
<td>Optimize for Horizon View check box</td>
<td>Optimizes performance on servers that use Horizon View to manage virtual machines.</td>
</tr>
<tr>
<td>Unprotected Area tab</td>
<td>Defines the rules to unprotect files and directories.</td>
</tr>
<tr>
<td>Rules list</td>
<td>Paths that are explicitly unprotected by Mirage.</td>
</tr>
<tr>
<td>Rule Exceptions list</td>
<td>Paths that are exceptions to unprotect rules in the Rules list. Mirage protects exceptions to unprotect rules.</td>
</tr>
<tr>
<td>User Area tab</td>
<td>Defines the rules to unprotect files and directories defined as user files. These rules are used instead of Unprotected Area rules when certain system flows specifically refer to user files. 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>
<td>Provides advanced policy options for optimization of the CVD policy.</td>
</tr>
<tr>
<td>Show Factory Rules check box</td>
<td>Shows the Factory upload policy settings in the rules list, the Mirage mandatory settings that the administrator cannot change. The factory rules are dimmed in the rules list.</td>
</tr>
<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 New Upload Policies

When you add a new upload policy, the new policy is added to the respective node.

Procedure
1. In the Mirage Web Manager, click the Policies tab, and click Add.
2. Type the policy name, description, and policy data.
3. Click Save to save the policy.

Edit Upload Policies

You can edit an upload policy in the Mirage Web Manager and distribute the revised policy. You can also use an external editor to edit the policy. You export the policy file, edit it, and import it back to the Mirage Web Manager.

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.

Procedure
1. In the Mirage Web Manager, click the Policies tab, and select an upload policy.
2. Click Edit.
3. Edit the policy data and click Save.
4. Indicate the scope of the update.
   - Select a minor version, for example, 1.1, or a major version, for example, 2.0, and click OK.
   - The new policy is added with the new version number.

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 Manager, 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.

Upgrade an Upload Policy

When upgrading a policy with a new minor or major version, you can upgrade the CVDs that are assigned to the previous upload policy version.

Prerequisites

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.

Procedure

1 In the Mirage Web Manager, click the Policies tab and select the policy to be upgraded
2 Click Upgrade.
3 At the confirmation prompt, click OK.

The CVDs assigned to the previous version of the upload policy are moved to the new version.
Working 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.

- **Add Static Collections on page 27**
  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 28**
  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 28**
  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 Manager, 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 Manager, 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 Manager, 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 Manager, 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 Manager, 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 Manager.

- **Block Storage Volumes** on page 31
  You can block a storage volume to prevent it from being used when new CVDs or base layers are being created.

- **Unblock Storage Volumes** on page 32
  You can unblock a volume that is currently blocked. The volume can then accept new CVDs and base layers and existing data can be updated.

### Block Storage Volumes

You can block a storage volume to prevent it from being used when new CVDs or base layers are being 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.

**IMPORTANT** You cannot move a CVD or a base layer to a blocked volume. You can move a CVD or a base layer from a blocked volume.

#### Procedure

1. In the Mirage Web Manager, click the **Volumes** tab.
2. Select the required volume and click **Block**.
3. Click **OK** to confirm.

The Volume Status column in the Volumes window shows Blocked.
Unblock Storage Volumes

You can unblock a volume that is currently blocked. The volume can then accept new CVDs and base layers and existing data can be updated.

Procedure

1. In the Mirage Web Manager, click the **Volumes** tab.
2. Select the required volume and click **Unblock**.
3. Click **Yes** to confirm.
Users with the Image Manager role can manage base layers and app layers using the Mirage Web Manager. You can perform various tasks related to Mirage layers.

Table 9-1. 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>
Managing Mirage Tasks

Users with the Image Manager role can delete tasks that have a status of complete, canceled, or finished.

You cannot delete tasks that have a status of paused or active.
You can generate and view reports on demand. Reports display the status of various Mirage operations. You access, generate, and export reports from the Reports tab in the Mirage Web Manager.

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.
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


2. Configure the legacy report settings.

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

A
about the Web Manager 7
app layer, capturing 16
app layer capture 16
app layer definition 15
app layers 33

B
base layer, capturing 15
base layer definition 15
base layers 33

C
centralization progress, report 37
centralize endpoints 19
CVD
assign upload policy 12
manage collections 13
migration 19
move to a different volume 13
view files in CVD with the file portal 12
CVD Integrity report 37
CVD collection
add dynamic using Active Directory 28
dynamic 28
static collection management 28
CVD collection, edit collection 29
CVD collection, static collection management 27
CVD management tasks 9
CVDs, collections 27

D
data protection status, report 37
device, reboot 10
disaster recovery 11
dynamic collections 28
dynamic CVD collection, adding 28

E
dend-user operations, view files in CVD with the file portal 12
disaster recovery, restore a CVD snapshot 11
endpoints, centralizing 19
enforce layers on endpoints 10

F
file portal 12

H
help desk login 7

L
layers, capturing base layers 15
legacy reports, export 38
license keys 33
login to the Web Manager 7

O
OS migration progress, report 37

P
policy rules
add 25
edit 25
rule exception 25

R
reference machine 19
replacement devices 19
reports
centralization progress 37
CVD integrity 37
data protection status 37
OS migration progress 37
restore, specific files from a CVD snapshot 11

S
SSRS, legacy reports 38

U
upload policies
edit 25
parameters 24
upgrade policy version 26
upload policy management 25

V
volume support
block volume 31
unblock volume 32
W
web manager
  help desk role 7
  protection manager 7
Web Manager
  logging in to the Web Manager 7
  tasks 35