VMware Mirage Web Management Guide

VMware Mirage 5.9.1

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

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.

About the Mirage Web Management 1

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

Role	Description
Help Desk	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..
Image Manager	Captures and assigns base layers and app layers to CVDs. The Image Manager role provisions new devices with a specified image.
Protection Manager	Provides detailed information of the system. Users with the Protection Manager role can update the Mirage system to protect end-user devices.
Administrator	A super-set of all Mirage operations.

Mirage Web Management user roles are assigned by the Mirage Management console. For more information about the VMware 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

1 Go to `https://`*`WebManagerServer`*`:7443/VMwareMirage`.

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 2

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, existing Windows 7 endpoints to Windows 8.1 and Windows 10, and existing Windows 8.1 endpoints to 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**.

Option	Description
Preserve user applications	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.
Remove user applications	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.

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 MirageAdministrator'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.

Option	Action
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 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**.

Option	Description
Automatically select a volume	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.
Manually select a volume	Use this option if you want to select the volume manually.

Windows OS Migration

You can migrate existing Windows XP or Windows Vista endpoints to Windows 7, existing Windows 7 endpoints to Windows 8.1 and Windows 10, and existing Windows 8.1 endpoints to 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
- USMT 10.0 for Windows 8.1 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.Old` directory, which is then processed by USMT. Application settings and data that are not handled by USMT are kept in the `C:\Windows.Old` 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 to Windows 10, or applications installed on Windows 8.1 to 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.

Working with Endpoints 3

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

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

Migration Option	Description
Full System Migration, including OS, applications, user data, and settings	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.
Only Migrate User Data and Settings The existing operating system and applications on the replacement device are retained. Only user data and settings are migrated to the replacement device.	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, or Windows Vista, or from Windows 7 machines to Windows 8.1, or Windows 10 machines. The OS of the replacement device must be the same as, or newer than, that of the CVD.

User data referred to in the options pertain to files and directories listed in the upload policies User area. See Chapter 5, "Working with Upload Policies," on page 23.

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.

Provision a Device

You can provision pending devices using the Mirage Web Management. You can select the layer to be downloaded, which can be assigned at a later stage.

Procedure

1 Go to `https://WebManagerServer:7443/VMwareMirage`.

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**.

4 Click **Pending Devices**.

5 Select the name of the device and click **Endpoint Provision**.

The Endpoint Provisioning wizard opens.

6 On the Select CVD Policy page, select a CVD policy to assign and click **Next**.

7 Select **Only Download Layer** option on the Base Layer Selection page, select the base layer, and click **Next**.

8 Select the layer you want to assign on the Application Selection Layer page, move the selected layer from Available Layers to Assigned Layers, and click **Next**.

9 Select a volume on the Target Volume Selection page and click **Next**.

You can automatically choose a volume or manually choose a volume.

10 Enter the domain information on the Device Name page and click **Next**.

11 Review the validation results for the image assignments to the selected devices on the Validations page and click **Next**.

12 Review the final details on the Summary page and click **Finish**.

The device provisioning download starts. You can review the progress of your device provisioning download from the Tasks tab.

After the device provisioning download is completed, you must apply device provisioning on the selected assignment. To do so, go to the **Assignment** tab, select the downloaded file, and click **Apply Provisioning**

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

4

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

Option	Description
Edit	Edit base layer or app layer information.
License Keys	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.
Delete	Delete a base layer or app layer. You cannot delete a base layer that is assigned to a CVD or an archived CVD.
Create Reference CVD	Create a reference CVD from a base layer.
Compare Programs	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.

Working with Upload Policies 5

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

Option	Description
Add	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.
Edit	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.
Delete	Delete an existing upload policy.
Upgrade	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.

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 5-2. Upload Policy Parameters

Parameter	Description
Name and **Description**	Name and description of the policy.
Upload change interval	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. The Upload change interval affects the frequency of automatic CVD snapshot creation.
Protected volumes	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.
Unprotected Area tab	Defines the rules to unprotect files and directories. **Rules list**: Paths that are explicitly unprotected by Mirage. **Rule Exceptions list**: Paths that are exceptions to unprotect rules in the Rules list. Mirage protects exceptions to unprotect rules.
User Area tab	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.
Advanced Options tab	Provides advanced policy options for optimization of the CVD policy.
Show Factory Rules check box	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.
Export button	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.
Import button	Imports policy rules from an XML file.

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**.

Working with CVD Collections

6

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 6-1. Working with CVD Collections

Option	Description
Create New	Create a dynamic collection or static collection of CVDs.
Edit	Edit a CVD collection.
Delete	Delete a CVD collection.
Sync	Synchronize all CVDs in a CVD collection.
Suspend	Suspend the network operation of CVDs in a CVD collection.
Resume	Resume network operation of CVDs in a CVD collection.
Restart	Force a restart all devices in a CVD collection.
Assign Base Layer	Assign a base layer to all devices in a CVD collection.
Assign App Layer	Assign an app layer to all devices in a CVD collection.
Enforce Layers	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.
Migrate Windows OS	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.

Table 6-1. Working with CVD Collections (Continued)

Option	Description
Apply Driver Library	Apply hardware-specific drivers to a CVD collection.
Assign Upload Policy	Assign an upload policy to a CVD collection to determine which files and directories are uploaded from the user endpoints to the CVD collection.

- 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.

Working with Storage Volumes 7

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

Option	Description
Add	Add a volume to the Mirage system.
Edit	Edit volume parameters.
Remove	Remove a volume from the Mirage system.
Block	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. **Important** You cannot move a CVD or base layer to a blocked volume. You can move a CVD or base layer from a blocked volume.
Unblock	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.
Mount	Mount a volume to the Mirage system.
Unmount	Unmount a volume to the Mirage system.

Working with Reports for Mirage Operations

8

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.

Branch Reflector Cached Layers

The Branch Reflector Cached Layer report displays the cached base and app layers of each branch reflector as well as the branch reflectors that do not have any cached layers.

This chapter includes the following topics:

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

1. Access the Report Manager, and open the `ReportTemplate.rdl` using Report Builder.
2. Configure the `ReportTemplate.rdl`.

   For information about report parameters, see https://technet.microsoft.com/en-au/library/aa337432%28v=sql.105%29.aspx.
3. Save the custom report as an `.rdl` file.
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

1 Access a command prompt and run the `C:\Program Files\Wanova\Mirage Management Server>Wanova.Server.Tools.exe ExportLegacyReport` command.

2 Configure the legacy report settings.

Option	Description
`foldername`	Folder where the legacy reports are exported. This parameter is mandatory.
`from`	Start date for the time frame of when the legacy reports were created. This parameter is optional.
`to`	End date for the time frame of when legacy reports were created. This parameter is optional.
`type`	Report type. This parameter is optional. The default report type is All.

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 Mirage Reports Package link.

3 Enter your log-in credentials for http://my.vmware.com.

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 you 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

9

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 9-1. Working with Tasks

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

Managing the Driver Library 10

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

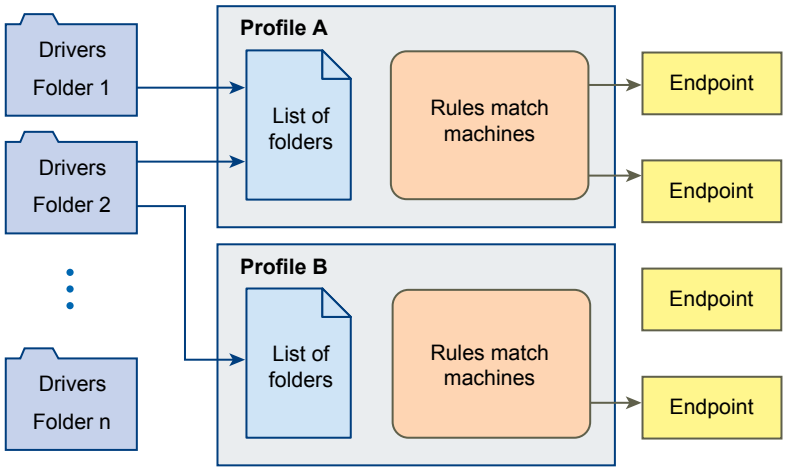
Option	Description
Add	Add a driver to a driver library.
Delete	Delete a driver from a driver library.
Import	Import a driver library. You can retain the original driver folder hierarchy of the driver library that you import to the Mirage driver library.

11 Driver Library Architecture

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

12 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.

13 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.

Managing Mirage Event Log Files 14

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

Option	Description
Delete	Deletes selected event log files.
Acknowledge	Changes the status of an event log file to Acknowledged in the Acknowledged column, indicated with a green check icon.
Reinstate	Removes the Acknowledged status of an event log file in the Acknowledged column, indicated with a red X icon.
Delete All	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.
Delete All Acknowledged	Deletes all event log files with a status of Acknowledged.

Managing Branch Reflectors 15

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

Option	Description
Sync	Starts the upload to the CVD.
Suspend	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.
Resume	When you resume network operations, the branch reflector or the individual endpoint device can communicate with the Mirage server cluster.
Restart	Restart the branch reflector device.
Disable Branch Reflector	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.
Rebuild Local Cache	Clears the cached files on the branch reflector machine.
Configure	Use the Configure feature to configure specific branch reflector values.
Reject Peers	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.

Table 15-1. Managing Branch Reflectors (Continued)

Option	Description
Accept Peers	Use the Accept Peers feature to resume providing service to the peer clients of a paused branch reflector.
Collect Logs	Collects logs on the branch reflector device.

This chapter includes the following topics:

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.

- Verify that port 8001 on the branch reflector host is open to allow incoming connections from peer endpoint devices.
- If the branch reflector endpoint also serves as a general purpose desktop for an interactive user, use a dual-core CPU and 2GB RAM.

To determine if an endpoint has an eligible branch reflector, click the **CVD Inventory** tab, select a CVD, and click **Show Potential Branch Reflectors**.

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**.

Option	Action
Default Maximum Connections	Type the maximum number of endpoint devices that can simultaneously connect to the branch reflector.
Default Cache Size (GB)	Type the cache size that the branch reflector allocated.
Required Proximity (msec)	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.
Use Active Directory Sites	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.
Always Use Branch Reflector	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.
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).

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

16

You can view and manage 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

Option	Description
Configure	Configure the maximum connections, port, transport type, and certificate information.
Remove	Remove the selected servers.
Start	Start the selected servers.
Stop	Stop the selected servers.
Collect Logs	You select the report level, destination, and UNC path.

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:

Event	Description
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.
MongoDB is disabled due to repetitive crashes	When MongoDB is disabled after a certain number of unexpected MongoDB failures in the stipulated time period

Event	Description
MongoDB is disabled due to high latency to the data disk	When the MongoDB is disabled because of high latency on the data disk.
MongoDB is disabled because not enough disk space is available	When the MongoDB is disabled if there is not enough disk space.
MongoDB is replicating or rebuilding index, please wait	When the MongoDB is temporarily disabled when it is replication of rebuilding index.

In these 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 has a single active Management Server. Set up multiple Management Servers to prevent data loss in case the Management Server fails. Important: Do not clone the VM.
```

If your configuration has only one Mirage Management Server, and if any one of the management servers is down or disabled, the Web Management displays a red banner with the following message:

```
Some of the Mongo nodes on your system are down, if all nodes are down Mirage operations will fail. View the Management Servers tab for details. After resolving the issue start the Management Server via Management Servers tab. For more information refer to KB2144975.
```

17 Configuring the Mirage System

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

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

Parameter	Description
`SubnetMaskV4`	Uses the format *IPaddress/bitmask*, for example, 100.100.10.100/20. For site-based rules, leave this parameter blank.
`Site`	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.
`Download limit`	Maximum number of KBps that you can download from the server to the client.
`Upload limit`	Maximum number in KBps that you can upload from the client to the server.

Table 17-1. Bandwidth Limitation Parameters (Continued)

Parameter	Description
`Start Time`	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.
`End Time`	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.
`Days of Week Time`	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.

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 `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

Constraints	Rule LImitations
No time constraint specified.	No time limit. Rule is applicable 24 hours on the days specified.
No day constraint specified.	No day limit. Rule is applicable every day on the time specified.
No time or day constraint specified.	Always applicable.
Blank.	Unlimited.
Zero (0).	Blocked.

License Settings

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

For the relevant procedures, see the *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

Option	Description
Snapshots kept	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.
Volumes	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. ■ Volume capacity - warning threshold (%): Type the threshold percentage of data stored on a volume, which triggers a warning event when reached. ■ Volume capacity - critical threshold (%): Type the threshold percentage of data stored on a volume, which triggers a critical event when reached. ■ 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. ■ Driver Library and USMT files volume: To select the volume to be addressed by the threshold checks, click Change and select the required volume.
CVDs	■ CVD size warning threshold (MB): Type the maximum CVD size. An event is generated in the Event Log when that size is reached. ■ 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.
Branch Reflector	See Chapter 15, "Managing Branch Reflectors," on page 49
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)

Option	Description
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.

Index