VMware Horizon Mirage Web Manager Guide

Horizon Mirage 4.4

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

EN-001278-03

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About the Horizon Mirage Web Manager Guide

The *Horizon Mirage Web Manager Guide* provides information about how to use the Horizon Mirage Web Manager. With the Horizon Mirage Web Manager, IT help-desk personnel and the protection manager user role can assist Mirage client users to resolve endpoint problems and to protect the Mirage user devices from further potential problems.

Intended Audience

This information is intended for IT help desk users to resolve endpoint issues. It is also intended for the Horizon Mirage Protection Manager user to protect the Mirage client endpoints.

About the Horizon Mirage Web Manager

1

IT help-desk users can use the VMware® Horizon Mirage™ Web Manager to respond to service queries, and the Protection Manager user can use the Web Manager to ensure that user devices are protected.

This chapter includes the following topics:

Install the Web Manager

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

The Web Manager can be viewed using Chrome, Firefox, IE 9 and IE 10. Cookies and JavaScript must be enabled.

Prerequisites

- The Horizon Mirage Web Manager must be installed on a Windows server with IIS 7 or later and .NET Framework 4.
- Make sure that your IE 9 browser supports JavaScript and Cookies on an intranet environment.

Procedure

1. Double-click the Web Manager MSI file to start the installation.
2. When prompted, provide the path to the installation location.
3. Complete the installation.

Access the Web Manager

You must log in each time you open the application.

The Web Manager is used by the following Horizon Mirage users:

Table 1-1. Web Manager User Roles

Role	Description
Help Desk role	The Help Desk role provides information about the Mirage client user device to respond to service queries. Access with the Help Desk role displays the Quick Search. See Chapter 2, "Accessing the Web Manager as a Help Desk Role," on page 9. Tabs for searching for device information and users are available in the left-side panel.
Protection Manager role	The Protection Manager role provides detailed information of the Mirage system. The Protection Manager enables the Protection Manager user to update the Mirage system to protect Mirage end-user devices. Access with the Protection Manager displays the Dashboard window. See Chapter 3, "Accessing the Web Manager as a Protection Manager," on page 19. Tabs are available in the left-side panel to allow navigating between the Dashboard and other options such as Policies, Collections, Volumes, and Reports.

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

Procedure

1 Go to `http://WebManagerServer/HorizonMirage` where *WebManagerServer* is the DNS name or IP address of the server where the Horizon 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 (Optional) Select the **Remember Me** check box to display the user name at login.

4 Click **Login**.

After logging in, the Select User and Device window appears for help desk users, where you perform a quick search for devices. The Dashboard window appears for Protection Manager users, where you can view the current Mirage conditions.

What to do next

If you are a help-desk user, continue to search for a device. See "Searching for Devices," on page 9.

If you are a Protection Manager user, continue to analyze device processes in the Dashboard. See "Monitor Device Processes with the Dashboard," on page 24.

Accessing the Web Manager as a Help Desk Role 2

The Horizon Mirage Web Manager Help Desk provides IT help desk personnel with information to assist Mirage client users with service queries.

The Web Manager Help Desk provides a quick search for a device or an advanced search for a refined search for a device. When a device is found, device information is displayed so that the IT help desk personnel can advise the Mirage client user or escalate the problem to the Protection Manager.

- Searching for Devices on page 9

  After logging in, the Select User and Device window appears, where you perform a quick search for devices either by typing the device name or the user name for which you want to view action history. If needed, you can go on to generate an expanded list of candidate devices using an advanced search.

- Working with Device Information on page 11

  After you select a device through a quick search or advanced search, the Device History and Information window appears where you can view information about the device.

Searching for Devices

After logging in, the Select User and Device window appears, where you perform a quick search for devices either by typing the device name or the user name for which you want to view action history. If needed, you can go on to generate an expanded list of candidate devices using an advanced search.

Perform a Quick Search

After logging in, the Select User and Device window appears, where you perform a quick search for devices for which you want to view action history. You can then select a device immediately, or from an expanded list of candidate devices in the advanced search.

Procedure

1 In the **Search** text box of the Select User and Device window, type a character string that the user name or device includes.

  The string must contain at least two characters, which can occur anywhere in the name. If you press **Enter** without typing anything in the **Search** text box, the full list of all the users and devices in the system appears.

  A quick search list of up to four user names and their corresponding devices appears. If a user name is associated with more than one device, all the devices are listed for that user name.

2 If the user and device that you want is in the quick search list, click its device link.

3 If the user and device you want is not in the list and you want to see more results, do the following:

   a Point to the **Search** text box and press Enter.

   A list of all user or device names that match the search string appears in the Advanced Search window search results.

   If you scroll past the fourth result in the list, the focus returns to the **Search** text box.

   b Locate the name that you want in the list and press Enter.

4 To perform a new quick search, click the **Plus** icon in the left-side panel and repeat steps 1 through 3.

What to do next

If you selected to perform an extended search, continue the procedure as described for advanced search. See "Perform an Advanced Search," on page 10.

After you select a device, you can view its action history in the Device History and Information window. See "Working with Device Information," on page 11.

Perform an Advanced Search

If you did not select a device from the quick search results and asked for more results, the Advanced Search window search results window appears showing the full results of the string search, or all users and devices in the system if no string was specified.

You can now select a user and device, or refine the advanced search further.

An advanced search searches simultaneously for Username, Device Name, Device ID and CVD ID instead of only Username and Device Name in the quick search. The results of an advanced search replace existing quick search results.

You can sort search results for any column name by clicking the column header.

- When a sort is by User Name, the default, devices are grouped in the list with their associated users.
- When the list is sorted by Device, user names are grouped with their associated device.

Procedure

1 Type the search string for the advanced search in the text box at the top-right of the window, in the same way as for a quick search.

   The results appear immediately.

   In an advanced search, you can specify a nested search based on two search strings by separating the individual strings in the text box with a space. For example:

   - Typing **`as ti`** searches for "as" or "ti" in usernames or device names.
   - Typing *username*, space, *device name*, identifies a specific username and device name.

2 You can perform another advanced search.

   - Click the **Plus** icon in the left-side panel.
   - In the Select User or Device window (quick search), press Enter without typing anything.
   - In the Advanced Search window, type the new advanced search string.

What to do next

After you select a device, you can view its action history in the Device History and Information window. See "Working with Device Information," on page 11.

Working with Device Information

After you select a device through a quick search or advanced search, the Device History and Information window appears where you can view information about the device.

The Device History and Information window shows the following information about the history of actions on selected devices.

- Left-side panel of **Selected Device** tabs lists the devices you selected in search operations.

  You can search and select any number of devices in a session.

- Right-side panel shows information about a device indicated by a **Selected Device** tab selection.

  The device information is available in two views:

View	Description
Grid View	Lists the device action history in grid form. See "Grid View," on page 12.
Timeline View	Displays the device action history as a timeline. See "Timeline View," on page 15.

View Selected Device Information and Action History

Each time you select a user and device from a search, a **Selected Device** tab is created in the left-side panel, which you can use to view the device information and action history, and navigate between devices selected during the session. The **Selected Device** tabs remain available until they are closed.

You can perform additional actions on any selected devices, including the current device, even while a process is active on it. For more information about actions, see "Perform Actions on a Device in the Grid View," on page 14.

A red triangle in the bottom-right of the tab indicates an active process on a device. You can view more information about tasks currently running on a device. See "View Currently Running Tasks," on page 13.

Procedure

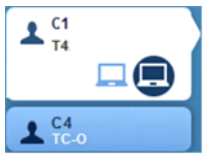
1 Select a device.

Each **Selected Device** tab shows the following information:

- User of the device, for example, **C1**
- Associated device names in a tooltip when pointing to a device icon.

The tab summarizes multiple devices for one user.

The device which is the current focus, or the last focus for an inactive tab, is shown in a blue circle. The name of that device appears under the user name, for example, **T4**.



2 View a device's action history.

Option	Description
Single device in the tab	Click the **Selected Device** tab.
Multiple devices in the tab	Click the device symbol on the tab.

When selected, the tab background becomes white and the device symbol becomes highlighted.

3 Close a tab by pointing in the top-right of the tab and clicking the **X** that appears.

A red triangle in the bottom-right of the tab indicates an active process.

4 Allow the active process to finish or click **OK** at the prompt to cancel it.

What to do next

You see the device information and action history initially in the Grid view.

You can alternate between the Grid view and Timeline view by clicking the **View Selector** icon  . For more information about the two views, see "Grid View," on page 12 and "Timeline View," on page 15.

In both views, all action types are initially filtered into the history. You can display actions selectively by setting the action filters. See "Filter the Grid View by Historical Action Type," on page 12 and "Filter the Timeline View by Action Type," on page 16.

Grid View

The Grid view, selected by default, shows the device action history in tabular form, as well as the device properties.

The Grid view includes a line of information about each action associated with the device, in chronological order. The information includes the action type, or filter, the action is related to, the start and end times, the action description, and the action status, for example, Succeeded.

All the action types are initially filtered into the history. You can display actions selectively by setting the action filters. See "Filter the Grid View by Historical Action Type," on page 12.

For example, the Grid view list includes the snapshot versions currently or formerly associated with the device.

View More Device or Action Information

You can see additional information about the device or an action performed on the device.

The toolbar under the Grid view, which contains the **Device Properties** button, shows you the device status.

Procedure

1 To see additional information about the selected device, click **Device Properties**.

The information appears at the bottom of the window under tab categories.

2 To see additional information about a historical action that was performed on the device, click the action in the list.

The information about that action is shown at the bottom of the window.

Each action type has its own information set.

Filter the Grid View by Historical Action Type

You can filter the historical action lines shown in the Grid view to include only those whose toolbar action icons are enabled.

By default all action types are visible in the view. You can exclude specific action types by clicking their icons to disable them. The same filters are applied in the Timeline view. Filters you set in the Timeline view also apply to the Grid view.

For information about the available action filters, see "Historical Action Type Filters," on page 13.

For more information about the associated actions, see the *Horizon Mirage Administrator's Guide*.

Procedure

- Select or unselect the action type filters according to the actions you want to see or hide in the view.

Historical Action Type Filters

The Grid view or Timeline view action history of a selected device can be filtered to include only specific actions. All actions are initially included in the view.

You can hide actions from the view by unselecting their icons.

Table 2-1. Historical Action Type Filters

Icon	Action Name	Description
	Steady State (incremental upload)	Data transfer from device to server.
	Snapshot	CVD snapshot creation.
	Event	Important system events propagated from the server and clients.
	Audit Event	User-initiated events.
	Task	Operations that deploy, manage, protect, or support Horizon Mirage endpoint devices.
	Download	Data transfer from the server to device.

For more information about the actions, see the *Horizon Mirage Administrator's Guide*.

Filter the Grid View using Free Text

You can further limit the displayed actions to include only those that specifically contain certain text in at least one of the displayed Grid view fields.

This filter can be set in either the Grid view or the Timeline view and is applied in the other view. It is applied as a filter in the Grid view or a search in the Timeline view. See "Filter the Timeline View Using Free Text," on page 17.

Procedure

- Click the **Filter** icon  , and enter the required free text string in the **Filter** text box.

View Currently Running Tasks

A red triangle in the **Device Selection** tab indicates tasks are currently running on the device. You can view information about the currently running tasks.

Procedure

1. Point to the **Currently Running Tasks** icon  to show the number of tasks that are currently running.
2. Click the icon to display a drop-down list of the running tasks.
3. Click an entry in the list.

   In the Grid view, the task line is highlighted and a progress bar appears in its End Time column indicating the task status.

   The Timeline view shows a red action bar (failed) or a blue anchor bar (running). Clicking on a currently running task moves the timeline to display the action.

Perform Actions on a Device in the Grid View

You can perform actions on the selected device, such as Enforce layers, Set Drivers, Reboot, Suspend, Synchronize, Collect Logs, Restore, or Revert to Snapshot.

You can perform the actions on the currently selected device either from the Grid view or the Timeline view. For more information about actions that can be performed on devices, see the *Horizon Mirage Administrator's Guide*.

Certain actions are performed uniquely the Grid view.

- "Update Note in the Grid View," on page 14
- "Revert to Snapshot in the Grid View," on page 14

Procedure

1 Click an action icon in the window toolbar.

2 (Optional) Click the **More** button to see more icons.

Depending on your selection, a confirmation prompt or a wizard appears.

3 Follow the prompts to finish the action.

Update Note in the Grid View

You can maintain a note with descriptive textual information about the selected device.

You can create or update a device's note from either the Grid view or the Timeline view.

Procedure

1 Click the **Note** icon in the window toolbar to open the note page.

It is initially a blank sheet.

2 Type information in the note and click **Submit** to save and close the window.

3 You can edit the note by the same process.

Save incremental changes with **Submit**, or discard them with **Cancel**. If you cancel changes, any previously saved text remains intact.

Revert to Snapshot in the Grid View

You can restore a CVD to a previous snapshot from the Grid view.

When you perform **Revert to Snapshot** from the Grid view, you select the required snapshot through the wizard process. Any snapshots shown in the Grid view list are for information purposes only and are not part of the wizard process. For more information about the procedure, see in Restore a Device to a CVD Snapshot in the *Horizon Mirage Administrator's Guide*.

Revert to Snapshot is performed uniquely when run from the Timeline view. See "Revert to Snapshot in the Timeline View," on page 17.

Procedure

1 In the Grid view, click the **Revert to Snapshot** action icon at the top of the window.

2 Choose the required snapshot.

3 Choose the revert options:

- Select the snapshot date to which you want to revert.
- **Restore System Only check box** (selected by default): 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.

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

Option	Description
If to the same OS, for example, Windows 7 to Windows 7:	Deselect this check box if you want to restore the entire CVD, including the User area, from the CVD snapshot. If the checkbox is deselected, 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 7 to Windows XP/Vista:	This checkbox is deselected and dimmed so the entire CVD, including the User area, is always restored from the CVD snapshot.

- Click **Next** to continue.

4 Complete the domain details. This applies only for Cross-OS reversions.

- Fill in the domain details needed for the device to rejoin the domain.
- Type the Domain and OU or select them from the drop-down menus.

  The drop-down menus are pre-populated with all known domains in the system. The required syntax pattern is shown for each text box.

5 Click **Next** and **Finish**.

Timeline View

The Timeline view shows the device action history as a timeline.

You can display historical actions selectively by setting the action filters. See "Filter the Timeline View by Action Type," on page 16.

Circles represent tasks. The color of the circle represents the task status.

Table 2-2. Task Status Color Coding

Color	Task Status
Blue	Task is in progress
Green	Task completed successfully
Red	Task failed
Orange	Task completed with a warning

When a task or steady state action takes a long time to complete, a bar of the same color replaces the action icon, showing its execution time relative to the timeline.

Other action types such as incremental uploads, steady state, snapshots, events, or audit events, are represented by symbols that resemble the icons used for filtering. See "Historical Action Type Filters," on page 13.

Multiple actions that occurred at or around the same time are grouped as one icon with a circled number indicating the number of actions that the icon summarizes.

Icons of the same action type are lined up at a different heights above the timeline, in their chronological order. For example, events appear at one height, and audit events at another.

Show Action History in the Timeline View

You can present the device's action history in a timeline.

Procedure

1 Select the **Timeline View** icon  .

All action types are initially filtered into the history.

2 Point in the vicinity of icons to open balloons of information about the underlying actions.

The icons are all of the same type, located on the same height above the timeline. Up to three icon or icon group information balloons can appear.

- For an icon representing one action, information about that action appears. Each action type has its own information set.
- For a grouped icon, the balloon lists the actions grouped by that icon. The state of each action is shown. The color of the icon represents the worst case action. For example, if two actions are designated with Warning and one with Failure, the icon is red.

3 Click a grouped icon to limit the timeline zoom range.

The Timeline view shows the date range of the associated actions.

4 Click an individual action listed in a balloon to see its detailed information set.

The parameters differ according to the action type.

5 Click the right-left arrow icons to scroll to the next or previous action in chronological order on the timeline.

Change the Timeline View

The Timeline view initially shows a zoomed-out view with the last 3 to 30 days' events, depending on the number of failed events for the device. You can expand or limit the displayed date range.

Procedure

1 To limit the date range, grab and move the arrows at either end of the timeline in the bottom of the window.

This expands the selected date range to fill the horizontal view.

2 After pointing to a grouped icon to show a list of its component actions, you can expand the date range summarized by the icon to fill the entire horizontal view by clicking the grouped icon or anywhere on the tooltip.

The actions are displayed in chronological order.

3 To zoom in or out on the view contents, point to the **Scroll** icon ⠿ in the timeline bar and roll the mouse wheel forward or back.

Filter the Timeline View by Action Type

You can filter the historical actions that appear in the Timeline view to include only those whose toolbar action icons are enabled.

By default all action types are visible in the view. You can exclude specific action types by clicking their icons to disable them. The same filters are automatically applied in the Grid view. The filters you set in the Grid view also apply to the Timeline view.

For information about the available action filters, see "Historical Action Type Filters," on page 13.

For more information about the associated actions, see the *Horizon Mirage Administrator's Guide*.

Procedure

- Select or unselect the action type filters according to the actions you want to see or hide in the view.

Filter the Timeline View Using Free Text

You can further limit the displayed actions to include only those that specifically contain certain text in at least one of the displayed Grid view fields.

This filter can be set in either the Grid view or the Timeline view and is applied in the other view. It is applied as a filter in the Grid view or a search in the Timeline view. See "Filter the Grid View using Free Text," on page 13.

Procedure

1. Click the **Free Text Search** icon  to open the **Free Text** box, and type a search string.

   The currently defined timeline interval, for example 3 days, shifts so that the earliest action that satisfies the search string appears in the middle of your screen.

2. (Optional) Navigate to the next or previous action.

Option	Description
Next action	Click the right arrow to identify each next action.
Previous action	Click the left arrow to return to an earlier action.

Perform Actions on a Device in the Timeline View

You can perform actions on the selected device, such as Enforce layers, Set Drivers, Reboot, Suspend, Synchronize, Collect Logs, Restore, or Revert to Snapshot.

You can perform the actions on the currently selected device either the Grid view or the Timeline view. For more information about actions that can be performed on devices, see the *Horizon Mirage Administrator's Guide*.

You can maintain a note with descriptive textual information about device. See "Update Note in the Grid View," on page 14.

Certain actions are performed uniquely in the Timeline view. See "Revert to Snapshot in the Timeline View," on page 17.

Procedure

1. Click an action icon in the window toolbar.
2. (Optional) Click the **More** button to see more icons.

   Depending on your selection, a confirmation prompt or a wizard appears.
3. Follow the prompts to finish the action.

Revert to Snapshot in the Timeline View

You can restore a CVD to a previous snapshot from the Timeline view.

When you perform **Revert to Snapshot** from the Timeline view, you can preselect the snapshot that will be used by the wizard. For more information about the procedure, see in Restore a Device to a CVD Snapshot in the *Horizon Mirage Administrator's Guide*.

This action is performed uniquely when run from the Grid view. See "Revert to Snapshot in the Grid View," on page 14.

Procedure

1 Right-click a **Camera** icon, representing a snapshot, in the Timeline space and select **Revert to Snapshot** from the shortcut menu.

The **Revert to Snapshot** wizard opens with the snapshot already selected.

2 Choose the revert options:

- Select the snapshot date to which you want to revert.
- **Restore System Only check box** (selected by default): 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.

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

Option	Description
If to the same OS, for example, Windows 7 to Windows 7:	Deselect this check box if you want to restore the entire CVD, including the User area, from the CVD snapshot. If the checkbox is deselected, 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 7 to Windows XP/Vista:	This checkbox is deselected and dimmed so the entire CVD, including the User area, is always restored from the CVD snapshot.

- Click **Next** to continue.

3 Complete the domain details. This applies only for Cross-OS reversions.

- Fill in the domain details needed for the device to rejoin the domain.
- Type the Domain and OU or select them from the drop-down menus.

  The drop-down menus are pre-populated with all known domains in the system. The required syntax pattern is shown for each text box.

4 Click **Next** and **Finish**.

Accessing the Web Manager as a Protection Manager

3

The Protection Manager enables Horizon Mirage users with the Protection Manager role to support and protect Mirage client end-user devices and run reports. Additionally, the Protection Manager can perform Horizon Mirage management tasks that provide support to the end-user devices.

NOTE The Protection Manager user role is assigned by the Mirage administrator in the Horizon Mirage Mangement console in the Users and Roles window.

After logging on to the Protection Manager, the Dashboard window is displayed. This provides an overview of the current Mirage conditions and statistics to help centralization and backup processes. See "Monitor Device Processes with the Dashboard," on page 24

The Protection Manager can add, update, and delete policies, CVDs, collections, and storage volumes. Additionally, the Protection Manager can generate reports.

- Using the Web Manager General Search Function on page 20

  The Horizon Mirage Web Manager contains a general search function that enables you to search the Mirage management server for the information you need.

- Monitor Device Processes with the Dashboard on page 24

  In addition to help-desk support, the Horizon Mirage Web Manager provides dashboard information that assists the Protection Manager role to ensure that user devices are protected.

- Working with Upload Policies on page 26

  An upload policy determines which files and directories to upload from the user endpoint to the CVD in the data center.

- Working with CVD Collections on page 30

  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.

- Managing Collection Devices on page 48

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

- Working with Storage Volumes on page 49

  Horizon Mirage provides multiple storage volume support to help manage volume congestion.

- Working with Reports on page 50

  You can generate and view a variety of reports on-demand.

Using the Web Manager General Search Function

The Horizon Mirage Web Manager contains a general search function that enables you to search the Mirage management server for the information you need.

The Web Manager general search, displayed on the top right side of the Web Manager window, enables you to search for CVDs, pending devices, upload policies, collections, reports, or all of these elements.

When a search result is displayed, you can perform various Mirage tasks such as centralizing a pending device, performing hardware migration, and other Protection Manager tasks, which is defined by the icons enabled on the Mirage toolbar.

- Search for CVDs on page 20

  You can search the Web Manager for CVDs that are defined in the Horizon Mirage Management server. The search result displays the CVDs with the included text string in the Search text box.

- Search for Pending Devices on page 20

  You can search the Web Manager for devices that are waiting to be centralized or pending hardware migration.

- Search for Policies on page 23

  You can search the Web Manager for upload policies that are defined in the Horizon Mirage Management server.

Search for CVDs

You can search the Web Manager for CVDs that are defined in the Horizon Mirage Management server. The search result displays the CVDs with the included text string in the Search text box.

Procedure

1 Select **CVDs** from the search list.

2 In the **Search** text box, type the text you want to search and press **Enter**.

The search result is displayed underneath the search text box.

3 (Optional) Press **Enter** to display more CVDs from the search result.

4 Select the CVD you want to display device information for that CVD.

The CVD history information is displayed in the Grid view.

What to do next

To understand the device information window, see "Working with Device Information," on page 11.

To perform various tasks on the selected CVD, see "Managing CVDs," on page 33

Search for Pending Devices

You can search the Web Manager for devices that are waiting to be centralized or pending hardware migration.

Procedure

1 Select **Pending** from the search list.

2 In the **Search** text box, type the text you want to search and press **Enter**.

The search result is displayed underneath the search text box.

3 (Optional) Press **Enter** to display a detailed list of pending devices from the search result.

4 Click the device you want to centralize or perform hardware migration.

The device properties are displayed in fhe device window.

What to do next

You can perform the Centralize Endpoint task to activate the device in the Horizon Mirage Management console. See

Additionally, you can perform Hardware Migration to migrate hardware devices. See

Centralizing Endpoints

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

When Horizon Mirage is first introduced to an organization, each device must be backed up, creating a copy of it on the server, in the form of a Centralized Virtual Desktop or CVD. You can then centrally manage the device.

The endpoint with the client installed appears in the Management console, in addition to the Web Manager, as Pending Assignment, and is pending activation in the system.

You activate a pending device by using a centralization procedure, which you can perform with a manual procedure. This provides more control over the process, for example, allowing a choice of upload policies, placement of CVDs on different volumes, and whether to assign a base layer.

- The user can use the desktop as usual while the centralization process runs in the background. This ability includes offline work. The client monitors user activities and network characteristics encountered by the desktop, such as speed, and adjusts its operation to optimize the user experience and performance.
- After the server synchronization is completed, the transaction log includes a successful endpoint centralization or provisioning entry. The desktop is protected and can be managed centrally at the data center.

Centralize an Endpoint

After the Horizon Mirage client is installed, the administrator can centralize the endpoint. Centralization performed by the administrator provides more control over the process, for example, allows a choice of upload policy, placement of CVDs on different volumes, and whether to assign a base layer.

You might want to add devices to a collection. A collection is a folder that aggregates CVDs that share a logical grouping, for example, Marketing CVDs. You can then implement relevant base layer changes with a single action on all CVDs in the collection. See "Working with CVD Collections," on page 30.

Prerequisites

The devices to centralize must be in the Pending Devices queue.

Procedure

1 In the Horizon Mirage Web Manager, use the general search function to search for pending devices.

2 Select the required pending device from the search results list.

3 In the device window, click **Centralize endpoint**.

4 Select the upload policy to be assigned to the device and click **Next**. If you do not make a selection, a default upload policy is applied, as specified in the general system settings.

5 Select a target storage volume option:

Option	Description
Automatically choose volume	Allow the Horizon Mirage Web Manager choose the target storage volume.
Manually choose volume	Manually choose a target storage volume from the storage volume list.

6 Click **Next**.

7 Review your upload policy and storage volume selections and click **Finish**.

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

Migrate a CVD to a Replacement Device

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

In this procedure, you can select one of the following migration options for the selected CVD and device:

Table 3-1. Migrate a CVD to a Replacement Device - Wizard Hardware Migration Options

Migration Option	
Full System Migration, including OS, applications, user data and settings	Use this option for systems with Windows volume licenses or Windows OEM SLP licenses. The entire CVD is restored to the replacement device, including OS, applications, and user files. Any existing files on the replacement device are lost or overwritten.
Only Migrate User Data and Settings	Use this option to migrate users from Windows XP/Vista/Windows 7 machines to new Windows 7 machines. The OS of the replacement device must be the same as or newer than that of the CVD. Only user data and settings are migrated to the replacement device. The existing OS and applications installed on the replacement device are retained.

- User data in these options pertain to files and directories listed in the upload policies User area. See "Working with Upload Policies," on page 26.
- If you migrate a CVD from a Windows XP or Vista device to a replacement device that has Windows 7, you can select **Full System Migration** or **Only Migrate User Data and Settings**. This is because Horizon Mirage does not transfer user-installed applications from a Windows XP/Vista to a Windows 7system (Horizon Mirage cannot guarantee cross-OS compatibility).
- When a CVD is migrated from Windows XP or Vista to Windows 7, the system streams down to the endpoint after the CVD has been migrated so that the end user can resume work without waiting for all of the user data to be downloaded first.
- If a Windows 7 endpoint is selected to be restored to a Windows XP or Vista CVD, that Windows 7 endpoint becomes a Windows XP or Vista device.

Procedure

1 In the Horizon Mirage Web Manager, use the general search function to search for pending devices.

2 Select the required device from the search results list.

3 In the device information window, click **Hardware Migration**.

4 Select the CVD form the CVD Selection list and click **Next**.

5 Select a migration option for the selected CVD and device.

If you selected Full System Migration, you will need to select a base layer in the next step. If you selected Only Migrate User Data and Settings, you will specify a machine name.

6 Select a base layer option:

Option	Description
Do not use a base layer	Proceed without a base layer.
Select a base layer from list	Select a base layer from the list. The next step is to select an app layer for the migration.

7 Click **Next**.

8 If you selected a base layer in the previous step, select the required app layers to be migrated. Select any of the available application layers and move them to the assigned layers list by clicking the left arrow.

9 Click **Next**.

10 Specify CVD naming and domain options.

a Change or define the hostname for a device being restored.

b Select a domain for this endpoint to join after the restore operation. The current domain is shown by default.

Type the OU and Domain or select them from the drop-down menus.

The drop-down menus are populated with all known domains in the system. Each text box shows the required syntax pattern.

Option	Description
OU	Verify that the OU is in standard open LDAP format. For example, OU=Notebooks, OU=Hardware, DC=VMware,DC=com.
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.

c Click **Next**.

11 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.

12 Click **Next** and click **Finish**.

Search for Policies

You can search the Web Manager for upload policies that are defined in the Horizon Mirage Management server.

Procedure

1 Select **Policies** from the search list.

2 In the **Search** text box, type the text you want to search and press **Enter**.

The search result is displayed underneath the search text box.

3 Select the policy you want to display the policy information.

The policy details and general settings are displayed.

What to do next

You can modify the policy, import and export policy rules, and modify or add rules to the unprotected area and the user area. For more information, see "Working with Upload Policies," on page 26.

Monitor Device Processes with the Dashboard

In addition to help-desk support, the Horizon Mirage Web Manager provides dashboard information that assists the Protection Manager role to ensure that user devices are protected.

The installation process creates **Dashboard** and **Search** icons in the left-side panel, used to navigate between the dashboard and device query functionality.

The dashboard provides a variety of statistics to help monitor centralization and backup processes.

Procedure

1 Click the **Dashboard** icon in the left-side panel.

The dashboard opens with four tiles of summary statistics.

The dashboard opens automatically when you access the Web Manager with the dashboard URL.

2 Click in a tile to view detailed statistics.

3 Click the **Restore Down** icon at top-right to return to the tile summary view.

Centralization Status Tile

The Centralization Status tile provides a first level indication of centralization progress.

Summary Statistics

The Centralization Status tile provides a summary of centralization progress:

- How many devices are currently being centralized.
- How many devices completed the centralization process historically. The number of devices includes archived CVDs but not reference CVDs.

Detailed Statistics

Click in the tile to show a line chart with different information about the centralization process based on your selections:

- Cumulative number of centralizations completed over a selected time span since today's date:
  - One week, based on daily data
  - One month, based on daily data
  - Six months, based on weekly data
- Composite chart that includes, for the same time frames as the previous chart:
  - Number of CVDs that completed centralization
  - Number of CVDs that are currently in the centralization process
  - Amount of data transferred in GB.

    The Y-axis is denominated in GB.

Failed to Complete Upload (Protection Status) Tile

The Failed to Complete Upload tile provides a first level indication of protection problems.

Summary statistics

The Failed to Complete Upload tile shows how many devices, centralizing or centralized, have protection problems:

- How many CVDs did not finish backing up the first time during the past week.
- How many CVDs completed centralization but did not back up for more than one week.

NOTE A statistic that is greater than the configured threshold appears with a red warning indicator. The thresholds can be configured in the dashboard's `web.config` file by adjusting the **DashboardKpiCentralizationNotFinishedCount** and **DashboardKpiNotBackedUpCount** values, respectively.

Detailed Statistics

Click in the tile to show a pie chart with details of the top five error types that occurred during the last week, month, or six months:

- The legend shows the top five problem types that stopped uploads from completing during the time frame.
- The pie chart shows the relative proportion of each of these problem types in the time frame. Remaining error types, if any, that are present in the time frame are aggregated as Other.
- CVDs that were suspended or not connected during the indicated time frame are not represented in the pie chart. The number of these CVDs is indicated at the bottom of the chart.

You can view error information in terms of:

- CVDs that did not complete centralization (**Centralization**)
- CVDs that did not finish backup (**Backed up**)
- **Both** (default)

Failed to Complete Layers Download Tile

The Failed to Complete Layers Download tile provides a first level indication of layer download problems.

Summary Statistics

The Failed to Complete Layers Download tile shows the number of devices where the layers download process was problematic and could not be completed during the past week.

NOTE A statistic that is greater than the configured threshold appears with a red warning indicator. The thresholds can be configured in the dashboard's `web.config` file by adjusting the **DashboardKpiDownloadFailureCount** values.

Detailed Statistics

Click in the tile to show a pie chart with details of the top five error types that occurred during the last week, month, or six months:

- The legend shows the top five problem types that stopped downloads from completing during the time frame.

- The pie chart shows the relative proportion of each of these problem types in the time frame. Remaining error types, if any, that were present in the time frame are aggregated as Other.
- CVDs that were suspended or not connected during the indicated time frame are not represented in the pie chart. The number of these CVDs is indicated at the bottom of the chart.

Short Disconnects Tile

The Short Disconnects tile provides a first level indication of network connection problems between servers and clients.

Summary Statistics

The Short Disconnects tile displays the average number of disconnections per device per hour of disconnection in the past 24 hours. Disconnects during idle time are not counted. A "disconnect" is recognized when a network disruption during a Mirage operation is followed by a disconnection within 5 minutes.

NOTE A statistic that is less than the configured threshold appears with a red warning indicator. The threshold can be configured in the dashboard's `web.config` file by adjusting the **DashboardKpiSubnetShortDisconnectsRatio** value.

Detailed Statistics

Click in the tile to display a grid with more information about the failures on each subnet.

Working with Upload Policies

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.

The administrator creates upload policies by defining which files are to be unprotected, protected, or local to the endpoint. Protected files are uploaded to the Horizon 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.

Table 3-2. Upload Policy Areas

Upload Policy Area	Description
Unprotected area	Lists files and directories on the endpoint device that are not protected, but with a subset of exceptions defined as protected. By default, Horizon Mirage protects all other files and directories.
User area	Lists end-user files and directories, such as document files, that are excluded from the restoration and that are kept on the endpoint devices in their current state when the **Restore System Only** option is used to revert a CVD. See "Restore a Device to a CVD Snapshot," on page 41 Additionally, the user area is used to filter out information from the base and app layers. The user area cannot be downloaded or viewed by the end user.

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 Horizon Mirage and Horizon View systems:

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

- View Upload Policies on page 27

  You can view an upload policy to review its content and parameters.
- Add New Upload Policies on page 28

  When you add a new upload policy, the new policy is added to the respective node.
- Edit Upload Policies on page 28

  You can edit an upload policy in the Web manager and distribute the revised policy.
- Add or Edit Upload Policy Rules on page 29

  You can add or edit a policy 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.
- Delete an Upload Policy on page 29

  You can delete an upload policy that is no longer needed.
- Upgrade an Upload Policy on page 30

  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.

View Upload Policies

You can view an upload policy to review its content and parameters.

Table 3-3. 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. See the *VMware Horizon Mirage Administrator's Guide* for more information.
Protected volumes	Denotes which volumes to centralize from the endpoint to the CVD in the server. The system volume is included by default. You can add more volumes by using the assigned drive letters.

Table 3-3. Upload Policy Parameters (Continued)

Parameter	Description	
Protect EFS Files check box, selected by default	Includes all Encrypted File System (EFS) files in the protected upload set. The user encrypts files using the Windows Encrypted File System feature. When the files are download in a CVD restore or file level restore, the files are restored in their original encrypted state.	
Optimize for Horizon View check box	Optimizes performance on servers that use Horizon View to manage virtual machines.	
Unprotected Area tab	Defines the rules to unprotect files and directories.	
	Rules list	Paths that are explicitly unprotected by Horizon Mirage.
	Rule Exceptions list	Paths that are exceptions to unprotect rules in the Rules list. Horizon 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.	
Show Factory Rules check box	Shows the Factory upload policy settings in the rules list, the Horizon 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. Horizon Mirage factory rules are not exported, even if they appear in the policy window.	
Import button	Imports policy rules from an XML file.	

Procedure

1 In the Horizon Mirage Web Manager, click the **Policies** tab.

2 Double-click the policy to view.

Add New Upload Policies

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

Procedure

1 In the Horizon Mirage Web Manager, click the **Policies** tab, and click **Add Policy**.

2 Type the policy name, description, and policy data.

3 Click **Save & Close** to save the policy.

Edit Upload Policies

You can edit an upload policy in the 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 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 Horizon Mirage Web Manager, click the **Policies** tab, and select an upload policy.

2 Click **Edit**.

3 Edit the policy data and click **Save & Close**.

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

Procedure

1 In the Horizon Mirage Web Manager, click the **Policies** tab, and select the required upload policy.

2 Click **Edit**.

3 Click **Add** next to the required Rule or Rule Exception area.

4 Type the directory path or select it from the drop-down menu.

IMPORTANT Do not type a backslash (\) at the end of the path.

5 Specify a filter for this directory or a pattern for matching files under this directory.

For example, to add a rule not to protect Windows search index files for all the users on the desktop, add the following rule:

```
%anyuserprofile%\Application Data\Microsoft\Search\*
```

6 Click **Save & Close**.

Delete an Upload Policy

You can delete an upload policy that is no longer needed.

Procedure

1 In the Horizon Mirage Web Manager, click the **Policies** tab, and select the policy you want to delete.

2 Click **Delete**.

3 At the confirmation prompt, click **Yes**.

The upload policy is deleted from the Policies node.

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 Horizon 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.

Horizon 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 31

  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 31

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

- Add Dynamic Collections on page 31

  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 32

  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 32

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

- Managing CVDs in a Collection on page 33

  In the Collections tab of the Horizon Mirage Web Manager, you can manage the CVDs that are assigned to the collection.

- Managing CVDs on page 33

  You can manage the CVD by performing tasks on the CVD you selected from the CVD in the collection or from the general search function.

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 Horizon Mirage Web Manager, click the **Collections** tab.
2. Click **Add**.
3. Type a name and description for the collection.
4. By default, the **Is static collection** check box is selected. Ensure that the **Is static collection** check box is selected.
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 Horizon Mirage Web Manager, click the **Collections** tab and double-click the collection to where you want to add the CVD.
2. Click **Add CVD**.
3. Select the CVD to add to the current collection.
4. Click **OK**.

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 Horizon Mirage Web Manager, click the **Collections** tab.
2. Click **Add**.
3. Type the name and description for this dynamic collection.
4. Clear the **Is static collection** check box.

   The dynamic collection rules dialog is displayed.
5. Select the filters to define the dynamic collection from each of the drop-down menus.

   You can add more filters to the dynamic collection by clicking the "+" sign at the end of the filter dialog.
6. 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
7. 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 if the Active Directory is updated for that user or device.

Procedure

1 In the Horizon Mirage Web Manager, click the **Collections** tab.

2 Click **Add**.

3 Type the name and description for this dynamic collection.

4 Clear the **Is static collection** check box.

5 Set the filter to define the dynamic collection by Active Directory group, Active Directory organizational unit, or Active Directory domain.

6 Click **Apply** to view the CVDs filtered to the collection. The filtered CVDs that are defined as Active Directory appear in the list.

7 Click **Save**.

Edit Collection

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

Procedure

1 In the Horizon Mirage Web Manager, click the **Collections** tab.

2 Select the collection you want to edit and click **Edit**.

3 Select the required option for editing the collection:

Option	Description
Edit Collection Properties	Expand the Collection Properties area at the bottom of the window and edit the collection name and description. In a dynamic collection, modify the rules to define additional CVDs.
Add CVD	NOTE You can only add a CVD to a static collection. To add CVDs in a dynamic collection, modify the rules in the collection properties. See "Add CVDs to Static Collections," on page 31.
Remove CVD	Select the CVD from the list and click **Remove CVD**.
Manage CVD	You can archive a CVD, delete a CVD, or assign an upload policy to a CVD. For more information, see "Managing CVDs in a Collection," on page 33.
Devices	You can suspend, resume, reboot, or synchronize a device that is connected to the CVD.

Managing CVDs in a Collection

In the Collections tab of the Horizon Mirage Web Manager, you can manage the CVDs that are assigned to the collection.

Managing the CVDs in a collection enable you to:

- Archive a CVD
- Delete a CVD
- Assign an upload policy to a collect of CVDs or to an individual CVD
- Set drivers to a collection or to a CVD
- Move a CVD to a different storage volume

In addition to managing CVDs in the collection, you can also manage the devices for each CVD by double-clicking the CVD in the collection. For more information on managing the devices in the CVD, see "Managing CVDs," on page 33

Managing CVDs

You can manage the CVD by performing tasks on the CVD you selected from the CVD in the collection or from the general search function.

There are several methods to manage a CVD. In the Collections, you select the CVD from the list of CVDs in the collection. From the general search function, you select the CVD from the CVD Search list.

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

- Set the Device Driver Library on page 34

  The device driver library contains hardware specific drivers in a separate repository, organized by hardware families. You can set a device driver library to a CVD or to a collection of CVDs.

- Restarting a Device on page 35

  You can enforce and remotely restart (reboot) a Mirage client device when the user does not reboot on a request from the Mirage client.

- Suspend Network Operations on page 35

  You can suspend network communications with the Horizon Mirage server for endpoint devices.

- Resume Network Operations on page 36

  You can resume network server operations on a device after network server operations have been suspended.

- Synchronize a Device on page 37

  You can synchronize a device with the corresponding CVD on the Mirage server to ensure that the device is properly backed up.

- Generate System Reports on page 37

  You can generate system log reports for the device attached to the Horizon Mirage server.

- Enforce Layers on Endpoints on page 38

  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 38

  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 42

  Mirage client end-users can use the Horizon Mirage file portal to browse and view files in their CVD.

- Update Device Notes on page 43

  You can add and update a note for a specific device. The note is free-form text and you have a maximum of 150 characters to type a note.

- Delete a CVD on page 44

  You can completely delete a CVD from the Horizon Mirage server. This option also deletes the CVD from the collection.

- Archive CVDs on page 44

  You can transfer a CVD that is not immediately required to the CVD archive.

- Assign an Upload Policy on page 45

  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 45

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

- Move a CVD to a Different Volume on page 46

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

- Generate a CVD Integrity Report on page 47

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

Set the Device Driver Library

The device driver library contains hardware specific drivers in a separate repository, organized by hardware families. You can set a device driver library to a CVD or to a collection of CVDs.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 You can set the device driver library for the whole collection by selecting the collection and clicking **Manage CVD > Set Drivers**.

3 From the Collections list:

   a Double-click the required collection.

   b Select the required CVD and device.

   c Click **Manage CVD > Set Drivers**.

4 From the general search function in the device information window:

   a Click **Set Drivers**.

   b At the confirmation prompt, click **OK**.

The device is set to the device driver library.

Restarting a Device

You can enforce and remotely restart (reboot) a Mirage client device when the user does not reboot on a request from the Mirage client.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 You can restart all Mirage client devices in a collection by selecting the collection and clicking **Devices > Reboot**.

3 From the Collections list:

   a Double-click the required collection.

   b Select the required CVD and device.

   c Click **Devices > Reboot**.

4 From the general search function in the device information window, click **Devices > Reboot**.

5 At the confirmation prompt, click **OK**.

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

What to do next

The Mirage client device must be restarted by the end-user. The end-user receives a message to restart the computer. The user can click **Restart Now** to restart the computer or the computer is automatically restarted in 10 minutes.

Suspend Network Operations

You can suspend network communications with the Horizon Mirage server for endpoint devices.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 You can suspend the network communications for the whole collection by selecting the collection and clicking **Devices > Suspend**.

3 From the Collections list:

   a Double-click the required collection.

   b Select the required CVD and device.

   c Click **Devices > Suspend**.

4 From the general search function in the device information window, click **Devices > Suspend**.

5 At the confirmation prompt, click **OK**.

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

What to do next

The network server operations are suspended on the device. You can resume network server operations on the device. See "Resume Network Operations," on page 36

Resume Network Operations

You can resume network server operations on a device after network server operations have been suspended.

Prerequisites

Network server operations on a device must be suspended. The **Resume** option is not available until the device network operations have been suspended.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 You can resume network communications for the whole collection by selecting the collection and clicking **Devices > Resume**.

3 From the collections list:

   a Double-click the required collection.

   b Select the required CVD and device.

   c Click **Devices > Resume**.

4 From the general search functionin the device information window, click **Devices > Resume**.

5 At the confirmation prompt, click **OK**.

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

Synchronize a Device

You can synchronize a device with the corresponding CVD on the Mirage server to ensure that the device is properly backed up.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 You can synchronize all devices in the collection by selecting the collection and clicking**Devices > Synchronize**.

3 From the Collections list:

a Double-click the required collection.

b Select the required CVD and device.

c Click**Devices > Synchronize**.

4 From the general search function in the device information window, click and click **Devices > Synchronize**.

5 At the confirmation prompt, click **OK**.

Generate System Reports

You can generate system log reports for the device attached to the Horizon Mirage server.

The reports can be saved to a UNC path or sent to an FTP site.

IMPORTANT Consider your privacy and regulatory requirements before sending support data to VMware. Log files, system reports and support data generated in order to obtain support from VMware may contain sensitive, confidential or personal information, including file and folder names and information about installed programs and user settings.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Double-click the required collection.

b Select the required CVD and device.

c Click **Collect Logs**.

3 From the general search function in the device information window, click **Collect Logs**.

4 Select one of the following options:

Option	Description
Full	Includes all logs and collectable information from this endpoint.
Medium	Includes the logs and some additional information.
Logs	Generates a report of only the basic logs for this client.

5 Indicate either the UNC path or FTP Server details.

Option	Description
UNC	Select the Remote Share radio button and type the UNC path.
FTP	Select FTP server and type the server name, user name, and password.

6 Click **OK**.

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 Horizon 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 Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Double-click the required CVD and device.

b Click **Enforce Layers**.

3 From the general search function in the device information window, click **Enforce Layers**.

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

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.

Horizon 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 "Working with Upload Policies," on page 26.
- 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 CVD to a Replacement Device

You can restore a CVD to a replacement device.

In this procedure, you select one of the following restore options for the selected CVD and device:

Table 3-4. Restore a CVD to a Replacement Device - Wizard Restore Options

Restore Option	Description
Full System Restore, including OS, Applications, User Data and Settings.	Use this option for systems with Windows volume licenses or Windows OEM SLP licenses. The entire CVD is restored to the replacement device, including OS, applications, and user files. Any existing files on the replacement device are lost or overwritten.
Restore Applications, User Data and Settings	Use this option when replacing a device that has a different Windows OEM license. The OS of the replacement device must be the same as that of the CVD. Only applications and user data are restored to the replacement device. The existing OS and applications installed on the replacement device are retained.
Only Restore User Data and Settings	Use this option to migrate users from Windows XP/Vista/Windows 7 machines to new Windows 7 machines. The OS of the replacement device must be the same as or newer than that of the CVD. Only user data and settings are restored to the replacement device. The existing OS and applications installed on the replacement device are retained.

- User data in these options pertain to files and directories listed in the upload policies User area. See "Working with Upload Policies," on page 26.
- If you migrate a CVD from a Windows XP or Vista device to a replacement device that has Windows 7, you can select only **Full System Restore** or **Only Restore User Data and Settings**. This is because Horizon Mirage does not transfer user-installed applications from a Windows XP/Vista to a Windows 7 system. Horizon Mirage cannot guarantee cross-OS compatibility.

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

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

NOTE You can also migrate users from Windows XP or Windows 7 machines to new Windows 7 machines. In this case, select **Only Restore User Data and Settings** as the restore option. For more information, see the *Horizon Mirage Administrator's Guide*.

Prerequisites

Install the Horizon Mirage client on the client machine. For more information, see the *Horizon Mirage Administrator's Guide*.

The procedure enables you to select a domain for this endpoint to join after the restore operation. If you want to use the same credentials each time, perform the following:

1 In the Horizon Mirage Management console tree, right-click **System Configuration** and select **Settings**.

2 Select the **General** tab and then type the credentials you want to use for domain joining.

The join domain account must meet the appropriate security privilege requirements. See the *Horizon Mirage Administrator's Guide* for detailed information on general system settings.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Double-click the required CVD and device.

b Click **DR > Restore**.

3 From the general search function in the device information window, click **DR > Restore**.

4 Select the device where you want to restore the CVD. Only devices to which the CVD can be restored are listed and click **Next**.

5 Select a restore option.

a Select a restore option for the selected CVD and device.

You can maintain the current layer, if one applies, select a new base layer from the list, or proceed without a base layer.

b If you selected **Full System Restore**, select the base layer.

c Click **Next**.

6 (Optional) Specify CVD naming and domain options.

a Change or define the hostname for a device being restored.

b Select a domain for this endpoint to join after the restore operation. The current domain is shown by default.

Type the OU and Domain or select them from the drop-down menus.

The drop-down menus are populated with all known domains in the system. Each text box shows the required syntax pattern.

Option	Description
OU	Verify that the OU is in standard open LDAP format. For example, OU=Notebooks, OU=Hardware, DC=VMware, DC=com.
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.

c Click **Next**.

7 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.

The migration process proceeds and takes place in two phases. For more information, see the *Horizon Mirage Administrator's Guide*.

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.

Horizon 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 *Horizon 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 7 to Windows 7, or cross-operating systems, for example, Windows 7 to Windows XP/Vista.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Double-click the required CVD and device.

b Click **DR > Revert to Snapshot**.

3 From the general search function in the device information window, click **DR > Revert to Snapshot**.

4 Choose the revert options:

- Select the snapshot date to which you want to revert.
- **Restore System Only check box** (selected by default): 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.

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

Option	Description
If to the same OS, for example, Windows 7 to Windows 7:	Deselect this check box if you want to restore the entire CVD, including the User area, from the CVD snapshot. If the checkbox is deselected, 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 7 to Windows XP/Vista:	This checkbox is deselected and dimmed so the entire CVD, including the User area, is always restored from the CVD snapshot.

- ◆ Click **Next** to continue.

5 Complete the domain details. This applies only for Cross-OS reversions.

- Fill in the domain details needed for the device to rejoin the domain.
- Type the Domain and OU or select them from the drop-down menus.

  The drop-down menus are pre-populated with all known domains in the system. The required syntax pattern is shown for each text box.

6 Click **Next** and **Finish**.

Working with the File Portal

Mirage client end-users can use the Horizon 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.

Allow or Block Access to CVD Files

The Protection Manager user can enable or block end-user access to CVD files in the Horizon Mirage file portal.

The **Show Web Access** icon in the user's notification area indicates that a file portal URL is defined.

Users cannot access the file portal if any of the following conditions are present:

- The file portal feature is disabled
- The CVD is blocked for Web Access
- The device is assigned as reference CVD
- The assigned user is in a workgroup, not in a domain, and a domain user acciunt was not mapped to the workgroup

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Double-click the CVD and device.

b Click **Block File Portal** or **Allow File Portal**.

3 From the general search function in the device information window, click **Block File Portal** or **Allow File Portal**.

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

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

The icon on the toolbar changes when either **Block File Portal** or **Allow File Portal** is performed.

Update Device Notes

You can add and update a note for a specific device. The note is free-form text and you have a maximum of 150 characters to type a note.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Double-click the required CVD and device.

b Click **Note**.

3 From the general search function in the device information window, click **Note**.

4 Type the required text in the Note box.

5 When finished, click **OK**.

Delete a CVD

You can completely delete a CVD from the Horizon Mirage server. This option also deletes the CVD from the collection.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Select the required CVD and device.

b Click **Manage CVD > Delete**.

3 From the general search function in the device information window:

a On the toolbar, click the double arrows to view more options.

b Click **Manage CVD > Delete**.

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

The CVD is deleted.

Archive CVDs

You can transfer a CVD that is not immediately required to the CVD archive.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Select the required CVD and device.

b Click **Manage CVD > Archive**.

3 From the general search function in the device information window:

a On the toolbar, click the double arrows to view more options.

b Click**Manage CVD > Archive**.

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

The CVD is transferred to the CVD Archive.

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 Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 You can assign an upload policy on a whole collection by selecting the collection and clicking **Manage CVD > Assign Upload Policy**.

3 From the Collections list:

   a Select the required CVD and device.

   b Click**Manage CVD > Assign Upload Policy**.

4 From the general search function in the device information window: click **Manage CVD** and click **Assign Upload Policy**.

   a On the toolbar, click the double arrow icon to view more options.

   b Click **Manage CVD > Assign Upload Policy**.

5 From the Assign Upload Policy list, select the required upload policy.

6 Click **OK**.

   The upload policy is assigned to the CVD. An Audit Event transaction is added to the device information list.

The newly assigned upload policy is displayed in the CVD list.

NOTE The new policy will only take effect after the next synchronization between the devices and the Mirage server.

Manage Collections

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

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Double-click the required CVD and device.

b On the toolbar, click the double arrow icon to view more options.

c Click **Manage CVD > Manage Collections**.

3 From the general search function in the device information window: click **Manage CVD** and click **Manage Collections**.

a On the toolbar, click the double arrow icon to view more options.

b Click **Manage CVD > Manage Collections**

4 In the Manage Collections window, you can perform the following actions:

Action	Description
Add a collection to a device	Select the collection from the Collection list and click the left arrow to move the collection to the device.
Remove a collection from the device	Select the collection from the Device collection list and click the right arrow to remove the collection from the device.

5 Click **OK**.

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 Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Select the required CVD and device.

b Click **Manage CVD > Move volume**.

3 From the general search function in the device information window:

a On the toolbar, click the double arrow icon to view more options.

b Click **Manage CVD > Move volume**.

4 In the Move to a different volume window, select the storage volume to where you want to move the CVD.

5 Click **OK**.

Generate a CVD Integrity Report

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

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

IMPORTANT Consider your privacy and regulatory requirements before sending support data to VMware. Log files, system reports and support data generated in order to obtain support from VMware may contain sensitive, confidential or personal information, including file and folder names and information about installed programs and user settings.

Procedure

1 In the Horizon Mirage Web Manager, choose the task from where you want to manage the CVD.

Option	Description
Collections tab	Click the **Collections** tab. Select the collection and click **Edit**.
General search function	Search for the required CVD and select the CVD/device from the search results list.

2 From the Collections list:

a Double-click the required CVD and device.

b On the toolbar, click the double arrow icon to view more options.

c Click **Manage CVD > CVD integrity**.

3 From the general search function in the device information window:

a On the toolbar, click the double arrow icon to view more options.

b Click **Manage CVD > CVD integrity**.

4 In the Report name text box, type the required report name. If none is given, the default name format is applied (CVD_Integrity_{User's environment name}.

5 Select a report option:

Option	Description
Check Only	Generates only the CVD Integrity report, which checks for errors on the selected CVD. No repair actions are performed.
Fix For Upload	Use this report option if you were performing a non-restore process (for example, periodic upload) when you encountered a problem with the CVD. Corrupted files are re-uploaded so that the interrupted process can resume.
Fix For Restore	Use this report option if you were performing a restore process when you encountered a problem with the CVD. Corrupted files are repaired so that the interrupted process can resume.

6 Click **Next** and click **Finish**.

7 To view a report that was generated:

- Double-click the generated report in the report list.

8 Click **OK**.

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

9 To view the CVD Integrity report that was generated:

a Click the **Reports** tab.

b Double-click the generated report in the Reports list.

Managing Collection Devices

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

Managing the collection devices enable you to:

- Suspend network operations
- Resume network operations
- Reboot a device
- Synchronize a device

Suspend or Resume Server Network Operations

You can suspend or resume network communications with the Horizon Mirage server for endpoint devices connected in a collection or in a CVD.

When you resume network operations, the endpoint device can communicate with the Horizon Mirage server cluster.

Procedure

1 In the Horizon Mirage Web Manager, click the **Collections** tab.

2 Select the collection and click **Edit**.

3 Select the CVD and click **Devices**.

4 Click **Suspend**.

5 At the confirmation prompt, click **OK**.

The device or devices are suspended and is displayed in the Status column of the CVD list.

6 To resume network communications, select the CVD and click **Devices > Resume**.

Restarting a Device

You can enforce and remotely restart (reboot) a Mirage client device when the user does not reboot on a request from the Mirage client.

Procedure

1 In the Horizon Mirage Web Manager, click the **Collections** tab.

2 Select the collection and click **Edit**.

3 Select the CVD and click **Devices**.

4 Click **Reboot**.

5 At the confirmation prompt, click **OK**.

The

```
Pending Reboot
```

status is displayed in the Status column of the CVD list until the user has restarted their computer. After the user has restarted the computer, the Status column changes to

`Idle`

.

Synchronizing a Device

You can synchronize a device with the corresponding CVD on the Mirage server to ensure that the device is properly backed up.

Procedure

1 In the Horizon Mirage Web Manager, click the **Collections** tab.

2 Select the collection and click **Edit**.

3 Select the CVD and click **Devices**.

4 Click **Synchronize**.

5 At the confirmation prompt, click **OK**.

Working with Storage Volumes

Horizon 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 the following actions in the Horizon Mirage Web Manager:

- Block a volume
- Unblock a volume
- Block Storage Volumes on page 49

  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 50

  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 Horizon 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 Horizon Mirage Web Manager, click the **Volumes** tab.

2 Select the required volume and click **Unblock**.

3 Click **Yes** to confirm.

Working with Reports

You can generate and view a variety of reports on-demand.

You can request the following reports:

Table 3-5. Reports that can be Requested

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. For more information about this report, see "CVD Integrity Report," on page 50.
Device Hardware Report	Provides a CSV file inventory of all devices, showing information such as chassis type, CPU, printing system, hardware components and associated vendor details. To run the report, select the report in the **Reports** node, click **Generate Report**, select devices, and click **OK**. To view the report, select the report line and click the **View Report** icon on the report list toolbar.

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.

IMPORTANT Consider your privacy and regulatory requirements before sending support data to VMware. Log files, system reports and support data generated in order to obtain support from VMware may contain sensitive, confidential or personal information, including file and folder names and information about installed programs and user settings.

Procedure

1 In the Horizon Mirage Web Manager, click the **Reports** tab and click **Add**.

2 In the Reports Options, select the **CVD Integrity** report.

3 In the Report name text box, type the required report name. If none is given, the default name format is applied (CVD_Integrity_{User's environment name}.

4 Click **Next**.

5 From the CVD Selection list, select the CVD and click **Next**.

6 Select a report option:

Option	Description
Check Only	Generates only the CVD Integrity report, which checks for errors on the selected CVD. No repair actions are performed.
Fix For Upload	Use this report option if you were performing a non-restore process (for example, periodic upload) when you encountered a problem with the CVD. Corrupted files are re-uploaded so that the interrupted process can resume.
Fix For Restore	Use this report option if you were performing a restore process when you encountered a problem with the CVD. Corrupted files are repaired so that the interrupted process can resume.

7 Click **Next** and click **Finish**.

8 To view a report that was generated:

- Double-click the generated report in the report list.

9 To delete a report:

a on the report list, select the report you want to delete.

b Click the **Delete** icon on the report console toolbar.

c At the confirmation prompt, click **OK**.

Device Hardware Report

You can generate a Device Hardware report to provide an inventory of all devices, displaying information such as chassis type, CPU, printing system, hardware components, and associated vendor details.

The report is generated as a CSV file.

Procedure

1 In the Horizon Mirage Web Manager, click the **Reports** tab and click **Add**.

2 In the Reports Options, select the **Device Hardware** report.

3 In the Report name text box, type the required report name. If none is given, the default name format is applied (Device_hardware_{User's environment name}.

4 Click **Next**.

5 From the CVD Selection list, select the CVD and move it to the Selected CVDs list by clicking the right arrow icon.

6 Click **Next**.

7 From the Collection Selection list, select the collection and move it to the Selected Collections list by clicking the right arrow icon.

8 Click **Next** and click **Finish** to generate the report.

9 To view a report that was generated:

- Double-click the generated report in the report list.

10 To delete a report:

a on the report list, select the report you want to delete.

b Click the **Delete** icon on the report console toolbar.

c At the confirmation prompt, click **OK**.

Index