Legal Notice

Copyright © 2012 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

The purpose of this document is to guide system administrators through the installation and deployment of VMware Mirage.

This guide includes the following parts:

- **PART 1 - OVERVIEW**, provides a brief overview of VMware Mirage, including features and benefits, key concepts, and components.

- **PART 2 - DEPLOYING THE MIRAGE SERVER**, lists the installation prerequisites. It also describes how to install the Mirage System and connect the Mirage System to the Management Console.

- **PART 3 - DEPLOYING MIRAGE TO YOUR ENDPOINTS**, describes how to install the Mirage Client on endpoint devices, add them to the Mirage system, and have their data centralized to the data center or cloud. It also describes the actions that an end user can perform, such as viewing the Status window, restoring files, and activating the Snooze and Sync Now functions. This part also describes how to configure your File Portal.

- **PART 4 - CONFIGURING THE MIRAGE SYSTEM**, describes how to configure the Mirage System with Secure Sockets Layer (SSL), how to configure a Mirage Server and the Mirage Management System. In addition, it describes how to manage the Driver library. It also describes how to add and manage multiple storage volumes connected to the Mirage Servers, and how to configure a branch reflector for large enterprise organizations with multiple remote sites. This part also describes how to install and manage multiple VMware Mirage Servers for enterprise organizations with a large number of endpoint devices.

- **PART 5 - IMAGE MANAGEMENT**, describes image management, and how to setup a Reference Machine. It also defines Base Layers and describes the Base Layer life cycle, including how a Base Layer is captured and used.

- **PART 6 - DESKTOP OPERATIONS**, describes how to perform various operations such as endpoint disaster recovery, hardware migrations and migrating from Windows XP to Windows 7.

- **PART 7 - MONITORING, REPORTING, AND TROUBLESHOOTING**, describes how to use the Management Console dashboard to monitor desktop deployments, and how to obtain storage statistics from the Server. It also describes the reporting framework that enables the Administrator to generate reports to be saved for future purposes, and how to generate, view, and delete the reports. The troubleshooting chapter describes tools the IT manager can use to troubleshoot the Mirage System, and also describes how to customize the minimal restore set and use the system report utility. This section also describes how to back up and restore the Mirage Server, and how to upgrade the system.
• **APPENDIX**, describes additional functions and details of the VMware Mirage System, such as, setting up the SSL certificate in Windows Server, using Microsoft Office in a Core Image, as well as describing the user role definitions, and how to manage users and roles using AD groups. It also describes macros in policy groups.
Table of Contents

About This Guide .............................................................................................................................................. 3

Part 1 - Overview ........................................................................................................................................... 13

Chapter 1  Introduction ................................................................................................................................ 15
    1.1  Overview .............................................................................................................................................. 15
    1.2  Key Concepts ..................................................................................................................................... 17
    1.3  Solution Components ....................................................................................................................... 18
    1.4  New Features in v3.6 ......................................................................................................................... 20
    1.5  New Features in Major Release (3.x) ................................................................................................ 20

Part 2 - Deploying the Mirage System ........................................................................................................... 25

Chapter 2  Planning Your Deployment ............................................................................................................ 27
    2.1  Supported Operating Systems .......................................................................................................... 27
    2.2  Software Prerequisites ....................................................................................................................... 28
    2.3  Hardware Prerequisites ...................................................................................................................... 28
    2.4  Database Prerequisites ..................................................................................................................... 29
    2.5  Ports Used by the Mirage System .................................................................................................... 30

Chapter 3  Installing the Mirage System ......................................................................................................... 31
    3.1  Installation Overview .......................................................................................................................... 31
    3.2  Configuring Third-Party Antivirus Software ..................................................................................... 32
    3.3  Installing the Mirage Management Server ......................................................................................... 32
    3.4  Installing the Mirage Management Console ....................................................................................... 34
    3.5  Connecting the Console to the Mirage System .................................................................................. 35
    3.6  Managing VMware Mirage Software Licenses .................................................................................. 36
        3.6.1  Adding and Viewing Licenses ...................................................................................................... 36
    3.7  Installing a Mirage Server ................................................................................................................ 37
    3.8  Minimum Configuration Requirements .............................................................................................. 38
    3.9  Installing IIS and the Mirage File Portal ............................................................................................ 39

Part 3 - Deploying Mirage to your Endpoints .................................................................................................. 41

Chapter 4  Activating Endpoints ...................................................................................................................... 43
    4.1  Activation Overview ........................................................................................................................... 43
Part 4 - Configuring the Mirage System ................................................................. 75

Chapter 7  Configuring the Mirage System ............................................................. 77
  7.1 Configuring the Secure Sockets Layer (SSL/TLS) ............................................ 77
  7.2 Configuring a Mirage Server ......................................................................... 78
  7.3 Configuring the Mirage System ...................................................................... 79
    7.3.1 General Tab ............................................................................................. 80
    7.3.2 CVD Auto Creation Tab .......................................................................... 82
    7.3.3 File Portal Tab ........................................................................................ 83
    7.3.4 USMT Settings Tab .................................................................................. 84
    7.3.5 Experimental Features Tab ...................................................................... 84

Chapter 8  Managing the Driver Library ................................................................. 85
  8.1 Overview ........................................................................................................ 85
    8.1.1 Architecture ............................................................................................ 85
    8.1.2 Driver Library Application ...................................................................... 86
  8.2 Managing Driver Folders ................................................................................ 87
    8.2.1 Creating a Drivers Folder ....................................................................... 87
    8.2.2 Performing a Folder Operation ................................................................ 88
    8.2.3 Importing Drivers into a Folder .............................................................. 89
    8.2.4 Adding a Driver to a Specific Folder from the All Folder ....................... 89
  8.3 Managing Driver Profiles .............................................................................. 90
    8.3.1 Creating/Editing Driver Library Profile ................................................... 90
    8.3.2 Setting Driver Library ............................................................................. 92

Chapter 9  Adding Multiple Volumes ....................................................................... 93
  9.1 Multiple Volumes Overview .......................................................................... 93
  9.2 Using the Mirage Volumes Window ............................................................... 94
  9.3 Adding a Volume ............................................................................................ 96
  9.4 Editing the Volume Information ...................................................................... 97
  9.5 Removing a Storage Volume .......................................................................... 97
    9.5.1 Removing a Volume ................................................................................ 97
    9.5.2 Unmounting a Volume ............................................................................. 98
  9.6 Mounting a Volume ....................................................................................... 98
9.7 Blocking a Volume .............................................................. 99
9.8 Unblocking a Volume ............................................................ 99
9.9 Volume Maintenance ............................................................. 100

**Chapter 10  Using Branch Reflectors** .................................................. 101

10.1 Branch Reflector Overview ...................................................... 101
10.2 How Client End Points Use Branch Reflectors ............................ 102
10.2.1 Branch Reflector Selection Process ........................................ 102
10.2.2 Branch Reflector Cache ......................................................... 103
10.2.3 Branch Reflector Local File Sharing ....................................... 103
10.3 Installing a Branch Reflector ..................................................... 104
10.4 Enabling a Branch Reflector .................................................... 104
10.5 Configuring Branch Reflectors .................................................. 105
10.5.1 Setting Defaults for Branch Reflectors .................................... 105
10.5.2 Configuring Specific Branch Reflector Values ........................... 107
10.6 Disabling a Branch Reflector .................................................... 108
10.7 Rejecting Peers ................................................................. 108
10.8 Accepting Peers ................................................................. 108
10.9 Suspending Network Operations .............................................. 109
10.10 Resuming Network Operations ............................................... 109
10.11 Monitoring Branch Reflectors and Peer Clients ......................... 110
10.11.1 Viewing CVD Activity and Branch Reflector Association ........ 110
10.11.2 Viewing Branch Reflector and Peer Client Information ............ 111
10.11.3 Monitoring Branch Reflector and Peer Client Transactions ....... 112

**Chapter 11  Deploying Additional Mirage Servers** .................................. 115

11.1 Multiple Servers Overview .................................................... 115
11.2 Using the Mirage Servers Window .......................................... 117
11.3 Adding a New Server .......................................................... 118
11.4 Stopping and Starting the Server Service ................................... 118
11.5 Removing a Server ............................................................. 119
11.6 Integrating the VMware Mirage System and Load Balancing ....... 119
11.7 Configuring the VMware Watchdog Service ............................... 120
Part 5 - Image Management .................................................................................. 123

Chapter 12  Image Management Overview .......................................................... 125
  12.1   Traditional versus Mirage Image Management Overview.............................. 125
  12.1.1  VMware Mirage: A New Approach to Image-based Deployment and Updates 126
  12.2   Base Layer Management Life Cycle......................................................... 128
  12.3   Different Hardware Platforms with Base Layers...................................... 129
         12.3.1  Virtual Machine Support ............................................................ 129
         12.3.2  Special Case Hardware Drivers .................................................... 130
  12.4   Planning and Preparation for Image Management .................................... 130
         12.4.1  System Level Software ................................................................. 130
         12.4.2  Software Licensing ................................................................. 131
         12.4.3  User-Specific Software ............................................................... 131
         12.4.4  OEM Software ........................................................................ 131
         12.4.5  Endpoint Security Software ...................................................... 132
         12.4.6  BitLocker Support .................................................................. 132

Chapter 13  Preparing a Reference Machine ....................................................... 133
  13.1   Setting Up a Reference Machine.............................................................. 133
  13.2   Software Considerations ...................................................................... 136
  13.3   Settings Captured from Reference Machine ........................................... 136
         13.3.1  Settings Captured from the Reference Machine ............................... 136
         13.3.2  Domain Membership and Login Settings .................................... 137
         13.3.3  Selecting the Captured Data ........................................................ 137

Chapter 14  Capturing Base Layers ..................................................................... 139
  14.1   Editing Base Layer Rules ...................................................................... 139
  14.2   Base Layer Override Policy .................................................................... 142
         14.2.1  Overriding Files ........................................................................ 142
         14.2.2  Overriding Registry Values ........................................................... 143
         14.2.3  Overriding Registry Keys ................................................................. 143
  14.3   Post-Base Layer Scripts ........................................................................ 144
  14.4   Capturing Base Layers ........................................................................ 145
  14.5   Recreating a Reference Machine from a Base Layer .............................. 148
Chapter 15  Assigning Base Layers

15.1  Introduction

15.2  Comparison Report between Base Layer and CVD

15.2.1  Comparison Report Format

15.3  Testing the Base Layer before Rollout

15.4  Assigning Layers

15.5  Base Layer Provisioning

15.6  Monitoring Layer Assignments

15.7  Dealing with Conflicts

15.8  Updating a Base Layer Assigned to a CVD

15.8.1  Monitoring a Base Layer Update

15.9  Enforcing a Base Layer

Part 6 - Desktop Operations

Chapter 16  Endpoint Disaster Recovery

16.1  Recovering from a Disaster

16.2  Restoring CVD Snapshots

16.3  Restoring a CVD Using the Disaster Recovery Wizard

16.4  Mirage Boot USB Keys

16.4.1  Overview

16.4.2  Prerequisites

16.4.3  Creating the VMware Boot USB Key

16.4.4  Using the VMware Boot USB Key

16.4.5  Customizing your Boot USB Key

16.4.6  Adding Drivers to your existing VMware Boot USB Key

16.4.7  Known Limitations

16.5  Advanced Scenarios

16.5.1  Reconnecting a Device to a CVD

16.6  User Experience with Restore Processes

Chapter 17  Hardware Migrations

17.1  Using the Hardware Migration Wizard

17.2  Planning for a Mass Hardware Migration
### Table of Contents

17.3 Performing a Mass Hardware Migration .............................................................. 187  

**Chapter 18**  Windows XP to Windows 7 Migration ................................................. 189  
18.1 Planning for a Windows XP to Windows 7 in-place Migration ......................... 189  
18.2 Setting Up a Windows 7 Base Layer for Migration ............................................ 190  
18.3 XP to Windows 7 Migration ................................................................................. 191  
18.3.1 Using the XP to Windows 7 Migration Wizard .................................................. 191  
18.3.2 Migration Following “Only Download Base Layer” ............................................ 195  
18.3.3 Monitoring the Migration .................................................................................. 198  
18.4 Migration to Windows 7 Replacement Devices ................................................... 199  
18.5 Post-Migration Scripts ........................................................................................ 199  
18.6 End User Experience During a Migration ............................................................ 200  
18.6.1 Known Limitations ........................................................................................... 200  

**Part 7 - Monitoring, Reporting, and Troubleshooting** ............................................. 201  

**Chapter 19**  Monitoring Desktop Deployment ......................................................... 203  
19.1 Using the System Dashboard .............................................................................. 203  
19.1.1 System Status .................................................................................................... 204  
19.1.2 Server ............................................................................................................... 204  
19.1.3 Update Progress ................................................................................................. 204  
19.1.4 Data Protection ................................................................................................... 204  
19.1.5 Compliance Meter ............................................................................................. 204  
19.1.6 Capacity Status .................................................................................................. 205  
19.1.7 Efficiency Benchmarks ....................................................................................... 205  
19.2 Transaction Logs .................................................................................................. 206  
19.2.1 Transaction Entry Properties ............................................................................. 207  
19.2.2 Search and Filter Results Specification ............................................................. 207  
19.2.3 Total Transaction Records Limit ....................................................................... 208  

**Chapter 20**  Mirage Reporting .................................................................................. 209  
20.1 Mirage Reporting Overview ................................................................................ 209  
20.2 Generating a Report .............................................................................................. 210  
20.3 Base Layer Dry-Run Reports ................................................................................ 211  
20.4 CVD Integrity Report ............................................................................................ 212
PART 1 - OVERVIEW

➢ In this Part...

1. Introduction
   1.1 Overview
   1.2 Key Concepts
   1.3 Solution Components
   1.4 New Features in v3.6
   1.5 Features in Major Release (3.x)
Chapter 1

Introduction

In this Chapter...

1.1 Overview
1.2 Key Concepts
1.3 Solution Components
1.4 New Features in v3.6
1.5 Features in Major Release (3.x)

1.1 Overview

VMware Mirage™ software centralizes the entire desktop contents in the data center for management and protection purposes, distributes the execution of desktop workloads to the endpoints for superior user experience, and optimizes the transfer of data between them. This Distributed Desktop Virtualization (DDV) architecture transforms how companies manage, support, and protect end-user desktops and laptops, especially those of remote and mobile workers.

- **Manage: centralized image management and provisioning**
  VMware Mirage enables enterprise IT managers to centrally control the Base Layer and guarantees a consistent view of the image at all endpoints. Administrators update a single image in the data center, and the new version of the image automatically and optimally propagates to the endpoints, retaining user-installed applications and personalization.

- **Support: faster troubleshooting**
  With Mirage, a full desktop instance resides in the data center. Support staff can then troubleshoot an endpoint regardless of the user’s physical location or network connectivity. With a click of a button, Mirage delivers a clean Base Layer to remote and mobile endpoints within minutes, transparently replacing the endpoint image while preserving all user data and customization.
• **Protect: continuous desktop protection**
  All data changes made by users are tracked continuously and then uploaded to the data center, making the endpoint fully disposable and eliminating the need for desktop backup agents. Upon loss or failure of an endpoint, Mirage quickly delivers a complete instance of the desktop – including user-installed applications and user data – to the new endpoint, dynamically adapting the image to the new hardware.

• **Migration: move users or groups of users to new or replacement hardware**
  IT Administrators can easily move users from a broken, lost or stolen device to a replacement device without losing or disrupting any user data or installed applications. In addition, IT Administrators can perform mass hardware migrations that move groups of users from old hardware to new, replacement hardware without affecting any user data.

  Mirage provides these benefits while ensuring an unparalleled user experience through:

  • **Full offline support**, seamless transition from online to offline.
  • **Desktop streaming over the WAN**, for fast availability and recovery.
  • **Flexibility**, with support for user-installed applications and customization with persistent personalization.
  • **Native desktop performance**, independent of network bandwidth, latency, or load.
  • **User mobility**, enabling users to access their desktop from multiple endpoints and locations.
1.2 Key Concepts

VMware Mirage comprises several key components:

- **Mirage Server**: The complete contents of each PC are migrated to the Mirage Server and become the authoritative copy, called a Centralized Virtual Desktop (CVD). A CVD enables an Administrator to centrally manage, update, patch, back up, troubleshoot, restore, and audit the desktop in the data center – regardless of whether the endpoint is connected to the network.

  A CVD comprises four components:

  - **Base Layer** defined by the administrator, which comprises the operating system image plus the core applications.
  
  - **Driver Profile**, defined by the IT Administrator, is a group of drivers that have been designated for use with specific hardware platforms. These drivers are applied to devices automatically when the hardware platforms match the criteria defined by the IT Administrator in the Driver Profile.
  
  - **User-installed applications and machine state** (unique identifier, hostname, any configuration changes to the machine registry, DLLs, and configuration files).
  
  - **User settings and data**.

Changes made by the end user to data, applications, or the machine state are efficiently propagated to the data center. Conversely, all changes made to the Base Layer by administrators in the data center are similarly propagated to the endpoints. Administrators can identify data that should not be protected, such as MP3s, or other files that are considered local-only to the endpoint.

- **Mirage Client**: Installed on the endpoint, this software executes in the base operating system, making sure the image at the endpoint and the CVD are fully synchronized. The Mirage Client is hypervisor-free but hypervisor-friendly: no virtual machines or hypervisors are required, though execution on any Type 1 or Type 2 hypervisor is supported.

- **Distributed Desktop Optimization™ (DDO)**: Optimizes transport of data between the Mirage Server and the Mirage Client – making it feasible to support remote endpoints regardless of network speed or bandwidth. DDO incorporates technologies that include read-write caching, file and block-level de-duplication, network optimization, and desktop streaming over the WAN.
1.3 Solution Components

The following diagram illustrates how the Mirage solution components integrate into a typical distributed infrastructure.

Figure 1-1: VMware Mirage Solution Components

The VMware Mirage components include:

- **Mirage Client** on the desktop. The Mirage Client is installed on endpoint devices to enable them to run a Centralized Virtual Desktop (CVD) or convert an existing desktop into a CVD.

- **Mirage Management Server** in the datacenter. The Mirage Management Server is the main component that controls and manages the Mirage Server cluster.

- **Mirage Management Console**. The Mirage Management Console is the graphical user interface used to perform scalable maintenance, management, and monitoring of deployed endpoints.

  Through the Mirage Management Console, the administrator configures and manages Clients, Base Layers, and reference machines, performs operations such as update and restore, and monitors the system operation through the dashboard and event logs.
• **Mirage Server** in the data center. The Mirage Server efficiently manages the storage and delivery of Base Layers and CVDs to clients, and consolidates monitoring and management communications. A Base Layer is used as a template for desktop content, cleared of specific identity information, and made suitable for central deployment to a large group of endpoints. Multiple Mirage Servers can be deployed as a server cluster to manage endpoint devices for large enterprise organizations.

  **Note:** The server machine must be dedicated for use by the Mirage Server software; it should not be used for any other purposes. For hardware requirements and supported platforms, see 2.3 *Hardware Prerequisites*.

• **Reference Machine.** A reference machine is used to create a standard desktop build for a set of CVDs. This usually includes operating system updates, service packs and patches, corporate applications to be used by all target end users, and corporate configuration and policies.

  Mirage offers unique capabilities to maintain and update reference machines over time, either over the LAN or WAN, using a Mirage Reference CVD entity in the data center. The Reference CVD can be used at any time as a source for Base Layer capture.

• **Branch Reflector.** The Branch Reflector is a peering service role that can be enabled on any endpoint device. When enabled, the Branch Reflector serves adjacent clients when downloading and updating Base Layers in the site, instead of having the clients download directly from the Mirage Server cluster. Using the Branch Reflector can significantly reduce bandwidth usage during mass Base Layer updates or other Base Layer download scenarios.

• **File Portal.** The file portal (which leverages IIS 7.0 or higher) allows end users to view the files that exist in their CVD snapshots from any web browser by using the appropriate login credentials.
1.4 New Features in v3.6

VMware Mirage v3.6 introduces the following features and improvements:

- **Base Layer Provisioning** - Prepares a new device to be part of the organization by cleaning up the device files, applying an existing Base Layer, and then seamlessly migrating the contents of the endpoint to the Mirage Server (as in Centralize Endpoint).

- **Streaming enhancements**
  - During Restore processing, you can view the streaming status of each downloading file. You are notified if a file you try to open is not finished downloading, and advised when that file becomes ready for use.
  - Performance improvements were implement which promote faster response time and enhanced user experience.

- **Scalability improvements** - Faster management response time in larger scale CVD configurations.

- **Reconnecting a device to a CVD (Force Upload)** - A device that has lost its synchronization for any reason can be reconnected to its CVD and can continue backing up incremental changes as before.

- **Default Policy Auto Selection**
  - In endpoint assignment wizard streams, a default Upload Policy (predefined in Security Settings) automatically applies to the endpoint if no other policy is specifically selected.
  - Configuration tabs are more logically organized - Upload Policy selection moved from CVD Auto Creation tab to General tab.

1.5 New Features in Major Release (3.x)

VMware Mirage major release 3.x includes the following key features that enable administrators to better manage, support, and protect endpoints:

- **Encrypted File System (EFS) support**
  - The Protect EFS Files option of Upload policies enables all Encrypted File System (EFS) files to be included in the protected upload set. (Files are encrypted by the user using the Windows Encrypted File System feature.)
  - Upon eventual download (CVD restore or file level restore (FLR)), the EFS files will be restored in their original encrypted form.
  - For File portal viewing, only the EFS files that were encrypted by the recovering user will be visible on the CVD. Non-authorized files will be filtered from the view.
• **Bootless client installer** – Restarting the computer immediately following installation or upgrade is no longer mandatory, but recommended.

• **Branch Reflector improvements**
  - **Driver library caching** - The Branch Reflector now also maintains a dedicated cache for the Driver library file downloads (as well as Base Layer and USMT files) from the server, from which distribution of these files to Client End Points can be optimized.
  - **Local file sharing** - The Branch Reflector can now share any files on its local disk with Client End Points (as well as files that were downloaded from previous Base Image requests). These files can be resident local files, or files copied from a DVD or USB device.
  - **Additional networks** - A Branch Reflector can be configured to service clients outside its own subnet. The Mirage IP detection and proximity algorithm first verifies whether a potential Branch Reflector is in the same subnet as the client. If it is in another subnet, the algorithm checks if the Branch Reflector is configured to service the client’s subnet.
  - **Always Prefer Branch Reflector (No fallback to server)** Ordinarily, if a client does not immediately find an available suitable Branch Reflectors, the client connects to the Mirage Server directly as a last resort. In order to keep network traffic as low as possible clients can be prevented from downloading from the server and forced to repeat the matching process until a suitable Branch Reflector becomes available. (A client will connect to the Mirage server directly only if no Branch Reflectors are defined.)

• **CVD Integrity Report**
  - The CVD Integrity report can now be executed from the management console. This 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.
• **Network Client Throttling**
  - Mirage’s continuous desktop synchronization is never at the expense of performance. A new Network Client Throttle mechanism enables Mirage clients to automatically regulate the data transfer at all times. The synchronization process operates transparently in the background and never impedes other applications.

• **File Portal**
  - Users can quickly and easily access their files from any of their saved snapshots (that reside in the data center) by using any portable device. Since these files are stored in the data center they can access these files even if their endpoint device has been damaged, lost or stolen, and can always access the files from any previous snapshot that exists in the data center.

• **Driver Library**
  - Decouples the core images from the hardware and helps the IT manager build core images that are agnostic to the hardware that those images are applied to.
  - Administrators can store and manage drivers in their Mirage system
  - Correct drivers from the Driver Library are automatically applied to endpoints connected to the Mirage system.

• **Directory Level File Restore**
  - Restore an entire directory from previous endpoint snapshots.

• **Auto create CVD**
  - Administrators can configure their Mirage system to allow end users to add their endpoint to the Mirage system without Administrator assistance.

• **Disaster Recovery Wizard**
  - Navigate through the disaster recovery wizard to quickly and easily restore a user’s previous system to hew (or fixed) hardware.

• **Hardware Migration Wizard**
  - Use the hardware migration wizard to seamlessly move a user (or group of users) from old hardware to new replacement hardware.

• **Support Windows OEM versions**
  - Mirage now supports endpoints that have Windows OEM licenses. Continue to use those devices normally or use core images to apply corporate volume licensing to a device.
New Features in Major Release (3.x)

- **Scalable and Cost-effective System Architecture**
  - Deploy a single server or a multi-node cluster of servers.
  - Easy multi-volume management.
  - Easy integration with third party server load balancers.

- **Peering technology for remote sites**
  - Endpoint devices at remote sites can be used as Branch Reflectors.
  - Minimizes network traffic between datacenter and remote site endpoint clients.

- **Centralize Single-Image Management, Preserving Personalization**
  - Automate Core Image creation and capture.
  - Change Reference CVD once, and automatically propagate changes to all endpoints as they connect to the network.
  - Maintain endpoint identity, user data, profile customizations, and installed applications, even upon re-imaging.

- **Faster Troubleshooting and Support**
  - Quickly restore operation of corporate applications on improperly functioning or broken remote endpoints, and ensure compliance with assigned Base Image, while retaining user data.
  - Enable removal of user-installed applications while ensuring compliance with assigned Base Image and preserving user data.
  - Recover system-only components from CVD snapshots, while preserving current user data at endpoint.
  - Centrally apply patches and updates to one or multiple endpoints, regardless of whether the end user is online.
  - Troubleshoot a problematic desktop centrally, by loading the CVD in the data center.

- **Continuous Desktop Protection**
  - Identify and protect endpoint data in the data center in accordance with IT policies.
  - Ensure secure communication between Server and Clients with SSL/TLS.
  - Store snapshots of CVD data to enable point-in-time recovery. Snapshots are kept on a daily, weekly, and monthly basis.
  - Archive CVDs for long term data retention and regulatory policies. Archived CVDs can be reinstated and assigned to another endpoint on-demand.
• Restore a CVD to an endpoint, preserving user customization, data, and installed applications.

• Leverage desktop streaming to quickly download components required for endpoint boot, and then synchronize remaining components in the background.

• Migrate a CVD across different endpoint hardware (re-base).

• Supports endpoint devices that have multiple volumes.

• Provide self-service operations for end users:
  • Restore a prior version of a file or a deleted file.
  • Sync Now: initiate synchronization to protect the latest changes to data.

• **Mirage Reporting**
  • Provides a reporting framework to generate and save reports for future use.
  • Reports on utilization of storage volumes.
  • Reports on Base Image dry-run results to allow creating customized conflict resolution rules. These reports list the expected impact of a Base Image download on applications and software modules in selected CVDs or CVD collections.

• **Deployment and Maintenance**
  • Simplify desktop management by leveraging the VMware Mirage Console, a Microsoft Management Console (MMC) snap-in:
    • Gain operational visibility with a consolidated dashboard.
    • Manage CVDs by collections.
    • Provide Active Directory (AD) Single-Sign-On (SSO) for console users.
    • Enable administrator role authorization with role-based access control (RBAC) by AD group membership.
  • Provide an excellent end-user experience over the WAN and optimize server storage capacity:
    • Leverage data de-duplication and compression to optimize network transfer over the WAN.
    • Optimize server storage capacity with global single-instance storage.
    • Enable rapid installation and deployment: convert existing endpoints to Mirage CVDs, regardless of endpoint location.
PART 2 - DEPLOYING THE MIRAGE SYSTEM

In this Part...

2. Planning Your Deployment
   2.1 Supported Operating Systems
   2.2 Software Prerequisites
   2.3 Hardware Prerequisites
   2.4 Database Prerequisites
   2.5 Ports Used by the Mirage System

3. Installing the Mirage System
   3.1 Installation Overview
   3.2 Configuring Third-Party Antivirus Software
   3.3 Installing the Mirage Management Server
   3.4 Installing the Mirage Management Console
   3.5 Connecting the Console to the Mirage Server
   3.6 Managing Winova Mirage Software Licenses
   3.7 Installing a Mirage Server
   3.8 Minimum Configuration Requirements
   3.9 Installing IIS and the Mirage File Portal


Chapter 2

Planning Your Deployment

In this Chapter...

2.1 Supported Operating Systems
2.2 Software Prerequisites
2.3 Hardware Prerequisites
2.4 Database Prerequisites
2.5 Ports Used by the Mirage System

2.1 Supported Operating Systems

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage Client</td>
<td>▪ Windows XP Professional with SP2 or SP3, 32-bit.</td>
</tr>
<tr>
<td></td>
<td>▪ Windows 7 Professional or Enterprise, 32-bit and 64-bit.</td>
</tr>
<tr>
<td></td>
<td>▪ XP “Fast User Switching” mode must be turned off if the computer is not an AD domain member. For further information, see <a href="http://support.microsoft.com/kb/279765">http://support.microsoft.com/kb/279765</a>.</td>
</tr>
<tr>
<td></td>
<td>▪ Domain membership required.</td>
</tr>
<tr>
<td></td>
<td>▪ Domain membership required.</td>
</tr>
<tr>
<td>Management Console</td>
<td>Same as Mirage Client.</td>
</tr>
<tr>
<td>Reference Machine</td>
<td>▪ Windows XP Professional with SP2 or SP3, 32-bit.</td>
</tr>
<tr>
<td></td>
<td>▪ Windows 7 Professional or Enterprise, 32-bit and 64-bit.</td>
</tr>
</tbody>
</table>
2.2 Software Prerequisites

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage Client</td>
<td>.NET Framework version 3.5 SP1.</td>
</tr>
<tr>
<td>Mirage Server</td>
<td>• Microsoft .NET Framework version 3.5 SP1 64-bit.</td>
</tr>
<tr>
<td></td>
<td>• File Portal requires an IIS 7.0 (or later) installation as well as the</td>
</tr>
<tr>
<td></td>
<td>IIS 6 Management Compatibility Role and ASP.NET feature (both options</td>
</tr>
<tr>
<td></td>
<td>within the IIS installation that are not selected by default).</td>
</tr>
<tr>
<td>Mirage Management Server</td>
<td>• Microsoft .NET Framework version 3.5 SP1 64-bit.</td>
</tr>
<tr>
<td>Management Console</td>
<td>• Microsoft .NET Framework version 3.5 SP1.</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Management Console (MMC) version 3.0.</td>
</tr>
<tr>
<td></td>
<td>(See <a href="http://support.microsoft.com/?kbid=907265">http://support.microsoft.com/?kbid=907265</a>)</td>
</tr>
<tr>
<td>Reference Machine</td>
<td>• Mirage v3.0 Client.</td>
</tr>
<tr>
<td></td>
<td>• Operating system and applications installed on the reference machine must</td>
</tr>
<tr>
<td></td>
<td>use volume licenses and be designed for multi-user, multi-machine</td>
</tr>
<tr>
<td></td>
<td>deployment.</td>
</tr>
<tr>
<td></td>
<td>• The Reference Machine should not include:</td>
</tr>
<tr>
<td></td>
<td>• Applications that install and use hardware-specific licenses.</td>
</tr>
<tr>
<td></td>
<td>• Applications that install and use local user accounts and/or local</td>
</tr>
<tr>
<td></td>
<td>groups.</td>
</tr>
<tr>
<td></td>
<td>• Software that uses a proprietary update service. Such software must be</td>
</tr>
<tr>
<td></td>
<td>installed directly on endpoints.</td>
</tr>
</tbody>
</table>

2.3 Hardware Prerequisites

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage Client</td>
<td>• Client systems:</td>
</tr>
<tr>
<td></td>
<td>• Enterprise-class laptops and desktops.</td>
</tr>
<tr>
<td></td>
<td>• Virtual machines compatible with Windows XP SP2 or higher or Windows 7.</td>
</tr>
<tr>
<td></td>
<td>• Minimum RAM: 512 MB for Windows XP, 1 GB for Windows 7.</td>
</tr>
<tr>
<td></td>
<td>• Client install and normal operation: At least 5 GB of free space.</td>
</tr>
<tr>
<td>Mirage Server Node</td>
<td>• Minimum RAM: 16 GB.</td>
</tr>
<tr>
<td>(up to 1500 clients)</td>
<td>• Minimum CPU: 2 x Quad-Core Processor, 2.26 GHz Intel core speed or</td>
</tr>
<tr>
<td></td>
<td>equivalent.</td>
</tr>
<tr>
<td></td>
<td>• Minimum System Drive capacity: 146 GHz.</td>
</tr>
<tr>
<td></td>
<td>This includes a 100 GB allocation for the Mirage network cache.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This does not include Mirage SIS storage. See Mirage Storage</td>
</tr>
<tr>
<td></td>
<td>prerequisites below.</td>
</tr>
<tr>
<td></td>
<td>• 2 x Gigabit Ethernet Port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> It is recommended to separate Client network and Storage-network access to dedicated ports.</td>
</tr>
</tbody>
</table>
**Component** | **Description**
--- | ---
Mirage Storage | ▪ Standalone Mirage Server:
▪ Direct Attached Storage (DAS).
▪ Storage Area Network (SAN) connected through iSCSI or Fiber Channel (FC).
▪ Network Attached Storage (NAS) connected through iSCSI, Fiber Channel (FC), or CIFS network share.
▪ Mirage Server Cluster:
▪ Network Attached Storage (NAS) connected using a CIFS network share.
▪ Alternate Data Streams:
▪ NAS via CIFS share must support Alternate Data Streams.
▪ Storage Capacity:
▪ Consumed capacity varies, depending on file duplication level across CVDs, Base Layers, and the number of snapshots stored, but VMware estimates on average each user requires 10 GB worth of data center storage.
▪ Enabling Compression:
▪ For DAS, SAN (FC, iSCSI) and Windows-based NAS (CIFS shares), you can sometimes realize up to 40% in storage savings by enabling the built-in Windows NTFS compression on your MirageStorage folder. For NAS systems that are not NTFS you need to leverage their own compression options.
**Note:** It is important only to apply this change when the Mirage services are stopped. It is also highly advisable to do this before this directory is heavily populated.

Management Console | ▪ Minimum RAM: 512 MB.
▪ Network connectivity to the Mirage Management Server.
▪ Minimum screen resolution: 1280 x 1024

### 2.4 Database Prerequisites

It is recommended to install and run the database on a separate server (not on the same machine as the Mirage Server).

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database software</td>
<td>Windows Installer 4.5 (MS KB942288) (<a href="http://support.microsoft.com/kb/942288">http://support.microsoft.com/kb/942288</a>)</td>
</tr>
<tr>
<td>File Portal</td>
<td>MS SQL Server must be setup with Windows Authentication. In addition, the Windows account used for installing Mirage must have <strong>dbcreator</strong> privileges, and the user account running the Mirage Server services must be configured with access privileges to the Mirage database.</td>
</tr>
</tbody>
</table>
2.5 Ports Used by the Mirage System

The following table summarizes the default communication ports and protocols used by Mirage System and Clients:

<table>
<thead>
<tr>
<th>Component</th>
<th>Communication</th>
<th>Port</th>
<th>Protocol</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirage Server Service</td>
<td>External</td>
<td>8000</td>
<td>TCP/IP or SSL/TLS</td>
<td>The only port required for communications between Mirage Clients and Mirage Servers. <strong>Note:</strong> SSL/TLS is optional and can be enabled as described in Configuring the Secure Sockets Layer (SSL/TLS).</td>
</tr>
<tr>
<td>Branch Reflector</td>
<td>External</td>
<td>8001</td>
<td>TCP/IP</td>
<td>Used for communication between the Branch Reflector and the local peers at the remote site.</td>
</tr>
<tr>
<td>Mirage Management Service</td>
<td>External</td>
<td>8443</td>
<td>TCP/IP</td>
<td>Used for communication between Mirage Management Console and Mirage Management service. SOAP Message-level Security applied.</td>
</tr>
<tr>
<td>Mirage Server Service</td>
<td>Internal</td>
<td>135, 445</td>
<td>TCP/IP</td>
<td>Used for control communication between the Mirage Management Service and the Mirage server. <strong>Note:</strong> You may limit access to this port to incoming connections from the Mirage Management Service host.</td>
</tr>
<tr>
<td>File Portal</td>
<td>Internal</td>
<td>8444</td>
<td>TCP/IP</td>
<td>Used for communication between the IIS server and the Mirage Management Server.</td>
</tr>
</tbody>
</table>

External communications is used for communications between the Mirage Management Server and Mirage Servers with the Mirage Clients or Management Console.

Internal communications is used for communications between Mirage Management Server and the Mirage Servers.

**Note:** You can configure different ports to be used as part of the SSL configuration CLI command as described in the previous section, or by modifying the Mirage Server and Management services configuration files if SSL is not used. Consult with VMware Support for further instructions.
Chapter 3
Installing the Mirage System

In this Chapter...

3.1 Installation Overview
3.2 Configuring Third-Party Antivirus Software
3.3 Installing the Mirage Management Server
3.4 Installing the Mirage Management Console
3.5 Connecting the Console to the Mirage Server
3.6 Managing VMware Mirage Software Licenses
3.7 Installing a Mirage Server
3.8 Minimum Configuration Requirements
3.9 Installing IIS and the Mirage File Portal

3.1 Installation Overview

Before installing the VMware Mirage System, ensure that all of the hardware and software prerequisites have been fulfilled and that you have a valid license for the Mirage System and that you’ve downloaded the latest version of the VMware Mirage software from the support site.

Additionally, ensure that the SQL server is installed and reachable before installing the Mirage System. The SQL browser service must be started to allow remote connections. Ensure that the firewall settings allow remote connections on the SQL server host. For more details, see http://technet.microsoft.com/en-us/library/cc646023.aspx.

The VMware Mirage System is installed in the following order:

1. Collect the required database information, or, install a new database instance to be used with Mirage.
   Note: You must have db creator privileges to create the Mirage database in the SQL express database. If you do not have these privileges, ask the database administrator to create the Mirage database and then assign you as the database creator.

2. Installing Mirage Management Server

3. Installing Mirage Management Console

4. Connecting the console to the Mirage System
5. Installing a Mirage Server

6. Installing the VMware File Portal
   **Note:** This requires IIS 7.0 or higher be installed on the Mirage server.

### 3.2 Configuring Third-Party Antivirus Software

When using antivirus software on the Mirage Server machine, exclude the Mirage Server folders, including the local cache directory (for example, `C:\ProgramData\Wanova Mirage\LocalCache`) and process from scanning (`Wanova.Server.Service.exe`).

### 3.3 Installing the Mirage Management Server

Before installing the Mirage Management Server, ensure that all the relevant software prerequisites listed in 2.2 *Software Prerequisites* have been met.

➢ To install the Mirage Management Server:

1. Double-click the `Mirage.management.server.x64.[BUILDNUMBER].msi` file. The *Welcome to Mirage Management Server Setup Wizard* window appears.
2. Click **Next**. The *End-User License Agreement* window appears.
   **Note:** A copy of the End-User License Agreement is located in the installation directory for future reference.
3. Select I accept the terms in the License Agreement.
4. Click **Next**. The *Mirage Management Server configuration* window appears.

5. Type the **SQL Server** name and the **SQL Instance**.
6. Select the **Create new storage areas** check box if this is a new installation of the Mirage System or if you do not want to keep the current data.

7. When creating new storage areas, type the UNC path of the first volume to be created. Sharing privileges must be granted to access the storage.

8. Click **Next**. The **Mirage services account configuration** window appears.

9. Select the **Use Local System account** option when using a standalone server with local storage or select **Use specific user** and enter the user name and password (Windows credentials) when accessing CIFS share servers in a cluster environment. The credentials used must be sufficient to access the storage and database.

10. Click **Next**. The **Ready to install VMware Mirage Management Server** window appears.

11. Click **Install**. The VMware Mirage Management Server is installed on the server. This may take a few minutes. When the installation is completed, the **Completed the VMware Mirage Management Server Setup Wizard** window appears.

12. Click **Finish** to complete the installation.
3.4 Installing the Mirage Management Console

This section describes how to install the Mirage Management Console. The Mirage Management Console is built as an MMC version 3.0 snap-in.

➢ To install the Management Console:

- Double-click the `Mirage.management.console.x64.[BUILDNUMBER].msi` file (for 32-bit environments, use the `Mirage.management.console.x86.[BUILDNUMBER].msi` file).

The installation starts and the `Mirage Management Console Setup` window appears which shows the installation progress. The window closes upon completion of the installation and a shortcut is automatically added to your desktop for the Management Console.

**Note:** During the installation, the *End-User License Agreement* is displayed and you are asked to agree to its terms before you can complete the installation.
3.5 Connecting the Console to the Mirage System

➢ To connect the Mirage Management Console to the Mirage System:

1. Double click the Mirage Management Console icon on your desktop.

2. In the Mirage Management Console window, right-click VMware Mirage in the root directory, and select Add System.

   ![Add System window]

   The Add System window appears.

3. Enter the IP address of the Management Server or the Management Server host name in the Management System Address field, and then click OK. The Mirage Server node appears in the MMC window.

   ![Add System configuration window]

Note: After connecting the console to the Mirage Management System, a server down status is displayed in the Server console. A Mirage Server has not yet been installed. When a Mirage Server is installed, the server status changes to Up.
3.6 Managing VMware Mirage Software Licenses

VMware Mirage Software licenses are provided separately from the Server installation package.

The Mirage software licenses are to be installed for the Mirage Management Server only. There is no need to install Mirage software licenses for each Mirage Server.

The license file enforces the number of CVDs you can run on your system and the duration of the license agreement. You can access the license details at any time to view this information (see below for more details).

**Note:** Reference CVDs do not take up a license and do not reduce the number of CVDs you are entitled to run on your system.

When the license capacity is reached, IT managers can no longer create new CVDs. Assigning replacement devices to existing CVDs is still permissible, and the system continues to work as usual.

When the license expiration date is reached, all management functions are disabled. No new Clients can be added to the system, nor can CVDs be restored to Client devices or Base Layers deployed. Nevertheless, system functions continue, so Clients continue uploading changes to the CVD on the Server.

A license error message appears when a license expires. Contact VMware for a new license and add it to the system as described below. An audit event is also created when a license expires.

3.6.1 Adding and Viewing Licenses

This section describes how to add a license to VMware Mirage or view existing licenses.

**Note:** You do not need to restart the Mirage Server to update the license.

➢ To add a license to VMware Mirage:

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

2. In the **General** tab, scroll down to the **License** section. The number of CVDs currently licensed and the license expiry date are shown.

![License Information](image)

3. Click **Set License**.

4. In the *File* window, navigate to your license file and click **Open**.

5. Click **OK** to continue.
3.7 Installing a Mirage Server

This section describes how to install a Mirage Server.

Multiple servers and storage volumes can be installed to provide enterprise organizations with large amounts of managed endpoint devices to store, manage, and protect the end-user device data. For more information about multiple servers, see 11.1 Multiple Servers Overview.

**Note**: Before installing the Mirage server, ensure that the SQL server is reachable from the server node and that the firewall settings on the SQL server allow for remote connections.

To install a Mirage Server:

2. Click **Next** to begin the Mirage Server Setup Wizard. The End-User License Agreement window appears.
3. Select the **I accept the terms in the License Agreement** check box.
4. Click **Next**. The Mirage Server configuration window appears.

![VMware Mirage Server Setup](image)

5. Type the **SQL Server** name and the **SQL Instance**.
6. Select the **Create new local cache area** check box to allocate new local cache area. If not selected, the installer attempts to use existing cache data.
7. Type a path and folder to where the local cache is stored, if different from the default.
8. Type the size of the cache in megabytes. The recommended cache size is 100 GB (102400).
9. Click **Next**. The *Mirage service account configuration* window appears.

10. Select **Use Local System account** when using a standalone server with local storage, or select **Use specific user** and enter the user name and password (Windows credentials) when accessing CIFS share servers in a Mirage cluster environment.

11. Type the password of the account to manage the Mirage services.

12. Click **Next**. The *Ready to Install the VMware Mirage Server* window appears.

13. Click **Install**. When the VMware Mirage server is successfully installed, the *VMware Mirage Server Setup Completed* window appears.

14. Click **Finish** to complete the server setup.

15. When the installation is complete, you must reboot the Server.

### 3.8 Minimum Configuration Requirements

Before using your Mirage system with endpoints, there a number of configurations you’ll want to perform that are outlined throughout this guide (sometimes in varying sections). Before attaching endpoints to your system, consider performing the following configurations first:

- Install a license file (required).  
  See *Chapter 3 Installing the Mirage System, 3.6.1 Adding and Viewing Licenses*).

- Configure the File Portal Web URL (optional).  
  See *Chapter 7, Configuring the Mirage System, 7.3.3 File Portal Tab*.

- Import the USMT folder (optional, but required for migration operations).  
  See *Chapter 7, Configuring the Mirage System, 7.3.4 USMT Settings Tab*.

- Domain Account details (optional, but required for domain joining operations).  
  See *Chapter 7, Configuring the Mirage System, 7.3.1 General Tab*.
3.9 Installing IIS and the Mirage File Portal

This section describes how to install IIS 7.0 and the Mirage File Portal on your Mirage Server.

➢ To install IIS and the Mirage File Portal:

1. Install the IIS Server role on the Windows Server 2008 R2 machine that has the Mirage Server software installed.
2. Open up the Server Manager and click the Add Roles option.
3. Select the Web Server (IIS) option and install it.
4. When installation is complete, still from Server Manager, click the Add Role Services option, and make sure that in addition to the default installation, that the following services are also installed:
   - Web Server
     - Common HTTP Features
       - Static Content
       - Default Document
       - Directory Browsing
       - HTTP Errors
     - Application Development
       - ASP.NET
       - .NET Extensibility
       - ISAPI Extensions
       - ISAPI Filters
     - Health And Diagnostics
       - [nothing is required]
   - Management Tools
     - IIS Management Console
     - IIS Management Scripts and Tools
     - Management Service
     - IIS 6 Management Compatibility
       - [all subitems are required]
5. Once the options are selected properly complete the installation.
7. Click Next to begin the Mirage Web Applications Setup Wizard. The End-User License Agreement window appears.
8. Select I accept the terms in the License Agreement.
9. Click **Next**. The *Mirage Web Access back end configuration* window appears. Select the components you wish to install. You’ll have two options:

- **Web Access**: This provides access only to an end user’s user files (as defined by the IT Administrator) across all CVD snapshots. Access to this feature is located here:  
  http://Server/Explorer

- **Admin Web Access**: This feature gives the Administrator full access to all the users CVDs across all CVD snapshots. Access to this feature is located here:  
  http://Server/AdminExplorer

10. Click **Next**. A Management Server entry window appears.

11. Input the location of the VMware Management Server, and then click **Next**. The *Ready to Install VMware Mirage Web Applications* window appears.

12. Click **Install**.

13. Click **Finish** when the installation completes.

**Note:** Be sure that the appropriate ports are enabled between IIS and the Mirage Management Server. See 2.5 *Ports Used by the Mirage System*. 
PART 3 - DEPLOYING MIRAGE TO YOUR ENDPOINTS

In this Part...

4. Activating Endpoints
   4.1 Activation Overview
   4.2 Installing the Mirage Client
   4.3 Common Wizards
   4.4 Activating Endpoints
   4.5 Working with Upload Policies
   4.6 Working with CVD Collections
   4.7 Archiving a CVD

5. End-User Operations
   5.1 Client Status Window
   5.2 File Level Restore
   5.3 Directory Level Restore
   5.4 Snooze
   5.5 Sync Now

6. Mirage File Portal
   6.1 Configuring your File Portal
   6.2 Configuring User CVD Mapping
   6.3 Accessing your File using File Portal
Chapter 4
Activating Endpoints

➤ In this Chapter...

4.1 Activation Overview
4.2 Installing the Mirage Client
4.3 Common Wizards
4.4 Activating Endpoints
4.5 Working with Upload Policies
4.6 Working with CVD Collections
4.7 Archiving a CVD

4.1 Activation Overview

Endpoint activation first requires installing the Mirage Client on the device. The device can then be activated in the Mirage Management Console - assigned to and synchronized with a CVD on the Mirage Server to enable centralized management of the device data.

This chapter also describes how to define upload policies and how to work with CVD collections and archives. Upload policies, which determine which files will be synchronized, should be defined before endpoints are activated since the activation wizards will select an existing upload policy for the endpoint.

4.2 Installing the Mirage Client

The Mirage Client installer can be installed using the Graphical User Interface (GUI). Administrators can also push out the Mirage Client installer silently, without disturbing user operations, by using manual command line arguments. The installation procedures apply to both first time installation of the Mirage Client and upgrade to a new version of the Client.

**Note:** Administrative permissions are required to install the Mirage client and the Client can only be installed on supported platforms (conforming to the prerequisites listed in 2.2 Software Prerequisites and 2.3 Hardware Prerequisites).
To install the Mirage Client using the Graphical User Interface (GUI)

1. Find the Mirage Client MSI Installer file and double click it. The *Welcome* window appears. Click **Next**.

2. The *Terms and Services* window appears. Accept the terms and conditions and click **Next**.

3. The *Mirage Client Configuration* window appears.
1. Enter the IP address or FQDN of the Mirage Server you want this client to communicate with.

   **Note:** You can also append a port to the Mirage Server location if you do not want to use the Mirage default (port 8000).

2. Check the **Use SSL to connect to the server** option to enable SSL if your Mirage server is configured for SSL usage, and enter the proper SSL port (these options must already be configured on the Mirage Server).

3. Click **Next**.

4. The **Ready to Install** window appears. Click **Install**.

   The installation begins.

5. When it is completed the **Finished Installing** window appears.

   Click **Finish**.

   - The **Mirage Client** icon appears in the system tray indicating that Mirage Client is pending assignment.

   ![Mirage (pending assignment)](image)

   - The Mirage Client appears in the Mirage Management Console in the pending devices list.

6. You are prompted to restart your computer. This is not mandatory, but highly recommended. For first-time installation, restarting will assure better backup protection and enables streaming which promotes faster restore. For an Upgrade, restarting will promote better performance.
Silent Mirage Client Installation

1. On the Start menu, click Run, type cmd, and then click OK. The Windows Command window appears.

2. Type the following command:

   `<Mirage MSI path>\MirageClient.x86.[BUILDNUMBER].msi SERVERIP=MirageServer /quiet` and press <Enter>.

   **Note:** For the SERVERIP parameter, you can use a DNS FQDN or hostname instead of the Server IP address.

   For 64-bit clients, use `MirageClient.x64.[BUILDNUMBER].msi`.

3. Add the following parameters if SSL has to be enabled (make sure to enable SSL on the Mirage Server):

   Type `<Mirage MSI path>\MirageClient.x86.[BUILDNUMBER].msi SERVERIP=MirageServer:port USESSLTRANSPORT=true /quiet` and press <Enter>.

   The installation starts. When it is completed:

   - The **Mirage Client** icon appears in the system tray indicating that Mirage Client is pending assignment.
   - The Mirage Client appears in the Mirage Management Console in the pending devices list.

4. You are prompted to restart your computer. This is not mandatory, but highly recommended. For first-time installation, this will assure better backup protection and enables streaming which promotes faster restore. For an Upgrade, restarting will promote better performance.
4.3 Common Wizards

Before we begin assigning endpoints we’ll briefly discuss the Common Wizards that VMware provides. The Common Wizards give the Mirage administrator an easy way to perform the most commonly used Mirage tasks to deploy, manage, protect, and support Mirage endpoint devices. One of these tasks is centralizing an endpoint, which we’ll discuss next.

➢ To access the Common Wizards:

1. Click the Common Wizards tab in the Mirage Management Console.

The Common Wizards menu appears.

Common Wizards

- Centralize Endpoint
  Migrate the contents of an endpoint to the Mirage Server. When complete, the endpoint will be protected and can be managed centrally.

- Capture Layer
  A layer is a template for common desktop content, cleaned of specific identity information and suitable for mass deployment to endpoints. The layer includes the operating system, service packs, patches and enterprise applications.

- Disaster Recovery
  Restore a CVO to the same endpoint, (e.g. in case of a new drive or after a format) or restore to a replacement endpoint.

- Hardware Migration
  Migrate a CVO to a different endpoint, either physical or virtual.

- Assign Layer
  Assign the appropriate layer to a single CVO or a collection. This layer will be validated, and will be deployed to the selected endpoints as they connect to the network.

- Windows 7 Migration
  Migrate an endpoint to Windows 7 from an older Windows XP/Vista), preserving all end user data, while deploying desired Windows 7 applications as part of the new Core Image.

- Base Layer Provisioning
  Prepare a new device to be part of the organization by cleaning up the device files, applying a Base Layer, and automatically migrating the contents of the endpoint to the Mirage Server.
2. From the *Common Wizards* window you can begin any of the following common tasks:

- **Centralize Endpoint**: Migrates the contents of an endpoint to the Mirage Server. When complete, the endpoint will be protected and can be managed centrally. See 4.4.1 Centralizing an Endpoint.

- **Capture Layer**: A layer is a template for common desktop content, cleared of specific identity information and suitable for mass deployment to endpoints. The layer includes the operating system, service packs, patches and enterprise applications. See 14.4 Capturing Base Layers.

- **Disaster Recovery**: Restore a CVD to the same endpoint (e.g. in case of a new hard drive or after a format) or restore to a replacement endpoint. See 16.3 Restoring a CVD Using the Disaster Recovery Wizard.

- **Hardware Migration**: Migrate a CVD to a different endpoint, either physical or virtual. See 17.1 Using the Hardware Migration Wizard.

- **Assign Layer**: Assign the appropriate layer to a single CVD or a collection. This layer will be validated, and will be deployed to the selected endpoints as they connect to the network.

- **XP to Win7 Migration**: Migrate an endpoint from XP to Windows 7, preserving all end user data, while deploying desired Windows 7 applications as part of the new Core image. See 18.3.1 Using the XP to Windows 7 Migration Wizard.

- **Base Layer Provisioning**: Prepare a new device to be part of the organization by cleaning up the device files, applying an existing Base Layer, and then seamlessly migrating the contents of the endpoint to the Mirage Server (as in Centralize Endpoint). See 15.5 Base Layer Provisioning.
4.4 Activating Endpoints

After the Mirage Client is installed, the endpoint appears in the Mirage Management Console as Pending Assignment, that is, pending activation in the system. The device should then be activated in the Mirage Management Console, assigned to (synchronized with) a CVD on the Mirage Server, thereby enabling centralized management of the device data.

Device activation is performed by Wizard-driven Centralization process, as described below.

Besides activating a device that is Pending Assignment, you can also reject a device, that you do not want to manage in the Mirage System – see 4.4.2 Rejecting Pending Devices.

4.4.1 Centralizing an Endpoint

When Mirage is first introduced to an organization, each device requires to be centralized (backed up), creating a copy of it (a Centralized Virtual Device, or CVD) on the server. The devices can then be centrally managed.

The Centralization procedure can be performed either:

- By the end user (an automatic procedure), or
- By the IT Administrator (a manual procedure).

The Administrator option provides additional control over the process, for example, enables a choice of upload policy, placement of CVDs on different volumes, and whether to assign a Base Layer. The two procedures are described below.

Tips:

- The end user is free to use the desktop as usual while the Centralization process is progressing in the background. This includes offline work and network transitions. The Mirage Client monitors user activities and adjusts its operation to optimize the user experience and performance.
- After the Server synchronization is completed, the Transaction log shows a successful endpoint centralization or provisioning entry. The desktop is protected and can be managed centrally at the data center.
To centralize an endpoint (end-user procedure):

1. CVD auto-creation is disabled by default and must be enabled by the IT Administrator via System Settings - see 7.3.2 CVD Auto Creation Tab.

   **Note:** If the prompt is closed, an end user can re-initiate this process by right-clicking the Mirage client in their system tray and selecting **Create New CVD**.

2. After the Mirage client has been installed, the end-user can centralize his own endpoint by just logging in.

3. Log in. The following login prompt appears.

4. Log in using one of the following formats: **DOMAIN\user** or **user@DOMAIN**. CVD auto-creation starts automatically.
To assign a pending device using the Common Wizards (Administrator procedure):

This procedure describes centralization initiated from the Common Wizards node Centralize Endpoint option. You can also initiate centralization from the Pending Devices or Layer Assignments windows, by selecting a device, right-clicking and selecting Centralize Endpoint from the shortcut menu. The Centralize Endpoint wizard will open at the Select Upload Policy step (see below).

1. In the Mirage Management Console, select the Common Wizards node.

2. Then select Centralize Endpoint.

3. The Select Pending Device window appears. Select the device or devices you want to assign.

Note: The device must be in the Pending Devices queue before you can select it.
4. The *Select Upload Policy* window appears. Select the upload policy you want to use and click **Next**. If you do not make a selection, a default policy will apply, as specified in the security settings - see Default Upload Policy in 7.3.1 General Tab.

![Select Upload Policy Window](image1)

5. The *Change Collections* window appears. If you wish to add the device(s) to a collection, select the required static collection.

![Change Collections Window](image2)

6. Click **Finish**. The Client starts the scanning phase according to the policy defined during the installation.

![Finish Window](image3)
Activating Endpoints

Monitoring the Centralization Progress

The system tray icon changes to show that the initialization process has started.

Mirage (initializing upload - 5%) 7:36 PM

The console displays that the Client has started an upload.

When the initialization process is complete and Server synchronization starts, the system tray icon on the Client shows the progress of the upload.

Mirage (upload - 28%) 7:45 PM

The console also shows the upload progress in the Upload field of the CVD inventory list.

The end user can also click the Mirage icon in the system tray to view the detailed status of the upload operation.

After the wizard operation completes, the device appears in All CVDs panel.
4.4.2 Rejecting Pending Devices

You can reject a device that is Pending Assignment which do not want the Mirage System to manage. If a device is rejected, the Server does not honor any of its communication requests. The rejected device is moved to the Rejected list.

You can remove a device from the Rejected list at any time. If a device is removed from the Rejected list and is still configured to connect to this Server, it reappears in the Pending list the next time the Client connects.

➢ To reject a pending device:

1. In the Mirage Management Console, select the Inventory node, and click Pending Devices. The Mirage Clients awaiting activation (pending) are listed in the console’s right pane.
2. Right-click the device to be removed, and then select Reject. A message appears requesting confirmation that you want to reject the selected device.
3. Click Yes. The device is moved from the Pending Devices list to the Rejected Devices list.
4. To remove the device from the Rejected Devices list, right-click it and select Remove. The device is removed from the Rejected Devices list. The next time the Client connects to the Server, the device appears in the Pending list.
4.5 Working with Upload Policies

An upload policy determines which files and directories should be uploaded from the user endpoint to the CVD in the data center. A CVD is assigned only one upload policy at a time.

Upload policies should be defined before endpoints are activated since the activation wizards will select an existing upload policy for the endpoint.

An authorized Mirage management user creates upload policies by defining which files are considered unprotected or local to the endpoint, and which files should be protected (uploaded) to the Mirage Server in the data center. The list of files is defined by a set of rules and exceptions.

To ease the task, the management user is required to identify files and directory names or patterns which are not uploaded or protected, at the CVD. The remaining files are considered part of the CVD.

Two areas of upload policy should be defined, which will be used by the system according to the system flow that is relevant:

- **Unprotected area**: In this area, the administrator lists files and directories on the endpoint device which should *not* be protected. By default, Mirage will protect *all other* files and directories.

- **User area**: In this area, the administrator lists the subset of Protected files and directories belonging to endpoint users, such as document files.

These are the files that the user will see in the Mirage File Portal (see 6.3 Accessing your Files using File Portal).

When the **Restore System Only** option is used to revert a CVD, these files and directories are excluded from the restore and are kept on the endpoint devices in their current state (see option in 16.2 Restoring CVD Snapshots).

The User area files and directories are also referred to in various **Restore** options described in 16.3 Restoring a CVD Using the Disaster Recovery Wizard.

**IMPORTANT**: A default, customizable upload policy is installed to assist the management user with first time deployment. It also serves as a reference for further customization. The default policy, for example, does not upload .MP3 and .AVI files to the CVD. **Make sure to evaluate the default policy against backup policies and data protection needs before using it as-is.**

The effective upload policy applied to the CVD is a combination of the upload policy created by the management user and a built-in factory policy provided by VMware. The built-in factory policy includes all the mandatory rules needed for the system to function and it cannot be modified by management users.
4.5.1 Viewing a Policy

You can view a policy to review its content.

➢ To view an upload policy:

1. In the Mirage Management Console, select Upload Policies. The upload policies are listed in the right pane under the System Configuration tab.
2. Double-click the policy you want to view. The *Upload Policy Details* window appears.

The *Policy Details* window displays the following information:

- **Upload change interval**: How frequently the Client synchronizes with the Server (in seconds). The default value is 1 hour.
- **Volumes to load**: Which volumes to centralize from the endpoint to the CVD in the Server. The system volume is included by default. Additional volumes can be added by using the assigned drive letters.
• **Protect EFS Files checkbox**: (Selected by default). Includes all Encrypted File System (EFS) files in the protected upload set. Files are encrypted by the user using the Windows Encrypted File System feature. Upon eventual download (CVD restore or file level restore (FLR), as described in later sections), the files will be restored in their original encrypted state.

• **Show Factory Rules checkbox**: Shows Factory upload policy settings in the rules list - Mirage’s mandatory settings that cannot be changed by the IT manager. The factory rules are grayed out in the rules list.

• **Unprotected Area tab**: Defines the rules to unprotect files and directories.
  - **Rules list**: Paths that are explicitly unprotected by Mirage.
  - **Rule Exceptions list**: Paths that are exceptions to unprotect rules in the Rules list. Exceptions to unprotect rules are protected by Mirage.

• **User Area tab**: Defines the rules to unprotect files and directories defined as user files – see description of User Area in 4.5.1 Working with Upload Policies. These rules are used instead of Unprotected Area rules when certain system flows specifically refer to user files. (Tab contains Rules and Rule Exception areas, used in the same way as in the Unprotected Area tab.)

• **Export**: Export policy rules to an XML file for easy editing and backup. Mirage factory rules are not exported (even if they are displayed in the policy window).

• **Import**: Import policy rules from an XML file.

## 4.5.2 Adding New Upload Policies

You can add a new upload policy by following these steps.

➢ **To add an upload policy:**

1. In the *Mirage Management Console*, right-click the **Upload Policies** node under the **System Configuration** tab and select **Add an Upload Policy**.

The *Add Upload Policy* window appears (similar to the **Upload Policy Details** window in 4.5.1 Working a Policy).
2. Enter the policy name, description, and policy data in the Policy Name, Policy Description, and Policy Data fields.

3. Click OK to save the policy. The new policy is added to the respective node.

4.5.3 Editing an Upload Policy

You can edit an upload policy by following these steps.

➢ To edit an upload policy:

1. In the Mirage Management Console, select the Upload Policies node under the System Configuration tab.

2. Double-click the upload policy you want to edit. The Edit Policy Info window appears (similar to the Upload Policy Details window in Viewing a Policy).

3. Edit the policy data (see 4.5.4 Adding and Editing Rules).

   Note: You can also edit the policy using an external editor by exporting the policy file, editing it, and then importing it back into the MMC.

4. When you finish editing the policy, click OK. The system prompts you with a version window.

5. Indicate the scope of the update by selecting a minor version or a major version, and then click OK. The new policy is added to the MMC with the new version number. If you want to distribute the changed policy, right-click the policy, then select Update CVDs with this Policy Version.

   Note: It is highly recommended to test the revised policy on a sample desktop before distributing it to a group of CVDs.

   The new policy takes effect at the next update interval in which the Client queries the Server. The default is 1 hour and requires a full disk scan.
### 4.5.4 Adding and Editing Rules

You can add or edit policy rules by following these steps.

➢ **To add or edit a rule in a policy:**

1. Double-click the upload policy, and then select **Add** or **Edit** next to the rule you want to modify. The *Edit Rule* window appears.

2. Type the path of the directory you want to add or select a path from the dropdown list (see *A.7 Macros in Policy Rules* for macro definitions).

   **Important:** Do not type a back-slash (\) at the end of the path.

3. Enter the filter for this directory or a pattern for matching files under this directory.

   For example, if you want 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\*`
4.6 Working with CVD Collections

The Collections node in the console enables you to create folders in which you can aggregate CVDs that share logical grouping. For example, you can aggregate all CVDs of users in the Marketing Department to a folder under Collections called Marketing. Then, when you have to implement changes to the Base Layer shared by all the Marketing CVDs, you can do so with a single action as all the CVDs are in one collection.

Mirage supports both static and dynamic collections.

A static collection is a collection to which you manually assign CVDs, while a dynamic collection is a collection to which CVD assignment is dynamically computed based on filter criteria.

Note: 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.

4.6.1 Adding a Static Collection

➢ To add a static collection:

1. In the Mirage Management Console, select the CVDs node and right-click Collections > Add a Collection. The Add a Collection window appears.

![Add Collection Window]

2. Enter a name and description for the collection in the Collection Name and Collection Description fields.

3. Click OK. The new folder appears in the Collections node.
4.6.2 Adding CVDs to a Static Collection

You can copy CVDs into existing Collection folders.

➢ To move CVDs to a collection:

1. In the Mirage Management Console, select the CVDs node and select CVD Inventory. The Mirage Clients are listed in the right pane.

2. Select the Clients that you want to move to the collection, then right-click and select Manage CVD > Add to Collections.

3. Select the collection to which you want to move the CVDs and click OK. The selected CVDs appear in the required collection.

4.6.3 Adding a Dynamic Collection

➢ To add a dynamic collection:

1. In the Mirage Management Console, right-click the CVDs node and select Collections > Add a Collection. The Add a Collection window appears.

2. Select the Dynamic collection option.

3. Set the filter to define the dynamic collection, like any other filter in the Mirage Management Console.

4. Click the Apply button to see the result of your filter. The result is listed in the lower pane, and displays the current result of your filter.

5. You can define as many rules as you want to define the dynamic collection.

6. Fill the name and the description for this dynamic collection.

7. Click OK. The dynamic collection content is calculated based on these filters every time an operation is applied to the collection.

4.6.4 Adding a Dynamic Collection using Active Directory

Mirage provides the ability to add a CVD collection dynamically using the Active Directory. You can add CVDs to the collection by Active Directory group, organizational unit, or domain.

Note: The Active Directory is updated whenever a device is authenticated. AD information may change if the active directory was updated for that user or device.

➢ To add a dynamic collection using Active Directory:

1. In the CVD Collections window, click the Add a Collection icon.

2. Alternatively, right-click the Collections node in the Mirage Management Console tree and click Add a Collection.

3. Type the name and description for this dynamic collection.

4. Select the Dynamic collection option.
5. Set the filter to define the dynamic collection by Active Directory group, AD organizational unit (OU), or AD domain in the filter columns field.

6. Click **Apply** to view the results of the filter. The results are listed in the lower pane and display the filtered CVDs in the collection.

7. Click **OK**.

### 4.7 Archiving a CVD

Mirage offers the option to archive a CVD to preserve its data, snapshots and operational history for long term retention, for example, when an employee leaves the company or is on leave. Archived CVDs can be reinstated and assigned to another endpoint.

**Note:** Once a CVD is archived that CVD no longer consumes a Mirage license.

➢ **To archive a CVD:**

1. From the **Inventory > All CVDs** tab, right-click the CVD you want to archive.
2. Click **Manage CVD**.
3. Click **Archive CVD**. The CVD is transferred to the CVD Archive console.

➢ **To view archived CVDs:**

- In the **Mirage Management Console** tree, click **CVD Archive**. The **CVD Archive** window appears.

### 4.7.1 Deleting an Archived CVD

➢ **To delete an archived CVD:**

1. From the **CVD Archive** window, select the CVD archive you want to delete.
2. Click the **Delete from Inventory** icon on the CVD Archive toolbar.
4.7.2 Moving an Archived CVD to Another Volume

➢ To move the archived CVD to another volume:

1. From the CVD Archive console, right-click the CVD archive you want to move and select *Move to a different volume*. The *Move to a different volume* window appears.

2. Select *Automatically choose a volume* to allow Mirage to choose the volume.
   Or,
   Select *Manually choose a volume* to enable you to choose the volume to where you want to move the archived CVD. Then select the volume to where you want to move the archived CVD.

3. Click OK.

4.7.3 Assigning an Archived CVD to a Device

You can assign an archived CVD to an endpoint device. The device can be the original endpoint device or a new device that is a replacement for the original device.

➢ To assign an archived CVD to a device:

- Right-click the archived CVD and select *Assign to a Device*. 
5.1 Client Status Window

Users can view information about the Mirage Client by double-clicking the Mirage icon in the Windows system tray.

The table lists the settings that appear in the client status window.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The version of Mirage.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The IP or FQDN of the Mirage Server.</td>
</tr>
<tr>
<td>Connection Status</td>
<td>Whether or not the Mirage is in a Connected or Disconnected state.</td>
</tr>
<tr>
<td>Last Upload Time</td>
<td>This is the last time that Mirage successfully completed an upload of data to the data center.</td>
</tr>
<tr>
<td>Current Base Layer</td>
<td>The Base Layer that is currently applied to this endpoint.</td>
</tr>
<tr>
<td>Current Action</td>
<td>The operation that is currently being performed on this endpoint.</td>
</tr>
<tr>
<td>File Progress</td>
<td>The file-level progress of the current transfer operation.</td>
</tr>
<tr>
<td>Data Progress</td>
<td>The data-level progress of the current transfer operation.</td>
</tr>
</tbody>
</table>
5.2 File Level Restore

Mirage offers end users self-service file restore. Users can restore a previous version of an existing file or a deleted file using available snapshots stored at the Mirage Server. The file restore operation generates an audit event at the Mirage Server for management and support purposes.

The restore is based on files and directories included in CVD snapshots, in accordance with the Upload policies currently in effect – see 4.5 Working with Upload Policies. When the CVD contains Encrypted File System (EFS) files, the files are recovered in their original encrypted form. (Only the EFS files that were encrypted by the recovering user will be restored from the CVD. Non-authorized files will be filtered from the restore.)

**Note:** Files are restored with their original Access Control Lists (ACLs).

Users can restore files in the following ways:

- Restore a previous file version of an existing file using the *Mirage Restore* option in Windows Explorer.
- Restore a deleted file using the *Mirage Deleted Files Archive* option in Windows Explorer on its parent directory. For example, if you want to restore a file that was deleted from the *My Documents* folder, select the *My documents* folder to restore the file.

➢ To restore a previous file version of an existing file:
1. Right-click a file in Windows Explorer, and then select *Mirage Restore*.

The *File Restore* window appears.
2. Select the archive file version you want to restore. The **File size** and **Modify time** are updated with the files archive information. If the file does not exist in the archive, an error message appears.

![File Level Restore](image)

3. Click **Restore**. The **Save As** window appears.

4. Browse to the location where you want to save the file (the default path is the original file location).

When the file download is complete, the file is moved to the selected location and the status message is updated to indicate a successful restore.

**Note:** If you try to write to a location for which you do not have access permissions, you are redirected to *My Documents*.

➤ **To restore a deleted file using the Mirage Deleted Files Archive:**

1. Right-click the parent directory from where the file was deleted, and then select **Mirage Deleted Files Archive**.

![Mirage Recycle Bin](image)

The **Mirage Recycle Bin** window appears.
2. Select the archive date from which you want to restore the file. Mirage downloads the archive information and searches for the available deleted files.

3. Double-click the archive file you want to restore. The *File Restore* window appears.

4. Click **Restore**. The *Save As* window appears.

5. Browse to the location where you want to save the file (the default path is the original file location).

   When the file download is complete, the file is moved to the selected location and the status message is updated to indicate a successful restore.

   **Note**: If you try to write to a location for which you do not have access permissions, you are redirected to My Documents.

### 5.3 Directory Level Restore

The Directory Level Restore allows users to recover entire directories (that is, a directory and all the files in that directory, including sub-folders and their files) back to their endpoint from their data center (assuming those directories exist in one of their snapshots saved in the data center). When a file exists, the user is prompted to overwrite a file or keep the previous version.

➢ **To restore a directory level restore:**

1. Right-click the parent directory from where the folder was deleted, and then select **Mirage Restore**.
The VMware Mirage Restore window appears.

2. Select the archive date from which you want to restore the file. Mirage downloads the archive information and searches for the available deleted files.

3. Double-click the archive file you want to restore. The File Restore window appears.

4. Click Restore. The Save As window appears.

5. Browse to the location where you want to save the file (the default path is the original file location).

   When the file download is complete, the file is moved to the selected location and the status message is updated to indicate a successful restore.

   **Note:** If you try to write to a location for which you do not have access permissions, you are redirected to My Documents.
5.4 Snooze

Mirage uses some of the endpoint processing power to synchronize the endpoint with the Mirage Server and keep it up to date. Mirage features a Network Client Throttle mechanism, by which Mirage clients automatically regulate the data transfer so as to optimize end-user experience. The Mirage Client senses end-user activity and reduces or suspends its synchronization process until the endpoint is idle.

If the end user is operating over a limited or metered network link, they may choose to temporarily suspend activities of the Mirage Client using the “Snooze” option.

➢ To activate Snooze:

• Right-click the **Mirage** icon in the system tray, and then select **Snooze**. The end user has the option to snooze the client for **15 minutes**, **2 hours**, or **4 hours**.

To deactivate Snooze:

• Click **Sync Now** to exit the snooze state before its scheduled expiration.

5.5 Sync Now

Mirage synchronizes the CVD at the Server with the end-user endpoint at policy-configured intervals. “Sync Now” enables user-initiated synchronization outside the defined intervals, for example, when important changes are made to documents and the user wants to ensure they are backed up to the CVD.

➢ To activate Sync Now:

• Right-click the Mirage icon in the system tray, and then select **Sync Now**.
Chapter 6

Mirage File Portal

In this Chapter...

6.1 Configuring your File Portal
6.2 Configuring User CVD Mapping
6.3 Accessing your File using File Portal

6.1 Configuring your File Portal

The IT Administrator can use the Mirage Management Console to configure the Mirage File Portal. End users do not have File Portal access if any one of the following is true:

- The File Portal feature is disabled.
- The CVD is blocked for Web Access (right-click on the required CVD, select File Portal > Block File Portal).
- The device is assigned as a Reference CVD.
- The assigned user is in a workgroup (not in a domain) and has not had a domain user account mapped to it (see section below).

If a File Portal URL is defined, a Show Web Access item appears in the user’s tray menu.
6.2 Configuring User CVD Mapping

There are some situations where a corporate domain is not available to the end user’s devices. This may be common in an MSP environment. To facilitate this, an Administrator can manually map a CVD that has centralized with the Mirage System to specific domain users. This way, end users who are not on the domain can still access their files via the File Portal. An Administrator can perform this by following these steps.

➢ To configure the file portal user CVD mapping:

1. In the Mirage Management Console tree, expand the Inventory node and select the All CVDs node.
2. Right-click the required CVD, and select Properties.
4. Select the text box to the right of the Local User column and input the desired user domain account.

5. Click Save. This user can now access their files using the domain account provided.
6.3 Accessing your Files using File Portal

If enabled, File Portal allows end users to browse and view any of the files contained within their CVD (as defined in the upload policies User area – see 4.5 Working with Upload Policies). These files are accessed from the data center directly, not from the endpoint, so the endpoint does not need to be accessible for the File Portal to function properly. This assumes that an Administrator has configured File Portal properly.

Note: When the CVD contains Encrypted File System (EFS) files, only the EFS files that were encrypted by the accessing user will be visible on the CVD. Non-authorized files will be filtered from the view.

➢ To use File Portal

1. Do one of the following:

   • In the Web browser on any device navigate to http://mirage-server-address/Explorer/
     Note: This URL can be changed by Administrators.

   OR,

   • Using the system tray icon application of an endpoint that has the Mirage client installed, right-click and select Show File Portal.

Note: A File Portal URL must be configured in the Management Server for this option to be available.
2. Users login to the File Portal in one of three ways (depending on what kind of environment is deployed):

- **Enterprise**: The end user uses their corporate Active Directory logon.
- **Hosted MSP (with domain)**: The end user’s corporate Active Directory profile is automatically mapped to their MSP logon as part of File Portal activation (this happens the first time they logon to a computer with an active Mirage client).
- **Hosted MSP (without domain)**: If the end user is not a member of a domain, the local profile on the client is manually mapped to the MSP logon (similar to the previous option in this list only the IT Administrator performed the mapping manually using the Mirage Management Console).

3. Browse through your files and open them as needed. This provides read-only access. Files may not be modified or uploaded.

**Note**: A user can select files from any available CVD snapshot, which means, they have access to files that were previously deleted or previous version of their files, from their snapshots.
PART 4 - CONFIGURING THE MIRAGE SYSTEM

In this Part...

7. Configuring the Mirage System
   7.1 Configuring the Secure Sockets Layer (SSL/TLS)
   7.2 Configuring a Mirage Server
   7.3 Configuring the Mirage System

8. Managing the Driver Library
   8.1 Overview
   8.2 Managing Driver Folders
   8.3 Managing Driver Profiles

9. Adding Multiple Volumes
   9.1 Multiple Volumes Overview
   9.2 Using the Mirage Volumes Window
   9.3 Adding a Volume
   9.4 Editing the Volume Information
   9.5 Removing a Storage Volume
   9.6 Mounting a Volume
   9.7 Blocking a Volume
   9.8 Unblocking a Volume
   9.9 Volume Maintenance

10. Using Branch Reflectors
   10.1 Branch Reflector Overview
   10.2 How Client End Points Use Branch Reflectors
   10.3 Installing a Branch Reflector
   10.4 Enabling a Branch Reflector
   10.5 Configuring Branch Reflector
   10.6 Disabling a Branch Reflector
   10.7 Rejecting Peers
   10.8 Accepting Peers
   10.9 Suspending Network Operations
   10.10 Resuming Network Operations
   10.11 Monitoring Branch Reflectors and Peer Clients

11. Deploying Additional Mirage Servers
   11.1 Multiple Servers Overview
   11.2 Using the Mirage Servers Window
   11.3 Adding a New Server
   11.4 Stopping and Starting the Server Service
   11.5 Removing a Server
   11.6 Integrating the VMware Mirage System and Load Balancing
   11.7 Configuring the VMware Watchdog Service
Chapter 7

Configuring the Mirage System

➣ In this Chapter...

7.1 Configuring the Secure Sockets Layer (SSL/TLS)
7.2 Configuring a Mirage Server
7.3 Configuring the Mirage System

7.1 Configuring the Secure Sockets Layer (SSL/TLS)

Mirage supports SSL communication between the Client and Server. By default, the Mirage Server does not install with SSL enabled. If you enable SSL on the Server, you must also enable SSL on Clients.

The Mirage Server uses an SSL certificate and private key pair stored in the Windows certificate store of the Local Machine account.

Notes:

- For environments with multiple Mirage Servers, you must enable SSL and install the SSL certificate for each server. For more information, see A.2 Setting Up the SSL Certificate in Windows Server.
- For this, as well as many other advanced management procedures, use the Mirage command line interface (CLI).

➢ To set up SSL on the Server:

1. Install the Server certificate and private key in the Windows certificate store. For more information, see A.2 Setting Up the SSL Certificate in Windows Server.
2. Restart each VMware Mirage Server service.
3. Perform the steps in the To configure the transport settings procedure in 7.2 Configuring a Mirage Server.
7.2 Configuring a Mirage Server

You can configure a number of options for each Mirage Server.

➢ To configure a Mirage Server:
   1. In the Mirage Management Console tree, expand the System Configuration node.
   2. Click Servers. The Servers window appears.
   3. Right-click the required server and select Configure.

➢ To configure the server for maximum CVD connections:
   - In the Maximum Connections field, type the maximum number of concurrent CVD connections. The maximum connections range is from 1 to 2500.

   Tip: For high-end servers, you can allocate a higher number of concurrent CVDs. For low-end servers, allocate a lower number of concurrent CVDs. Consult with the VMware Mirage Support team on this modification.
To configure the transport settings

1. In the Port field, change the port that is used for client-server communication here. You can use the default port of 8000 or you can change the port. Changing the port may require you to add additional firewall rules to open the port.

2. Mirage also allows you to have clients communicate with the server using SSL encryption. Note, that this is a global change. To do this, you must change the connection type to SSL and configure the appropriate certificate values on this Mirage Server.
   - The Certificate Subject can be found in the details of the certificate you installed and is typically the FQDN of the Mirage Server.
   - The Certificate Issuer can also be found in the details of the certificate you installed but this field can be left blank if there is only one certificate on this server.

   Note: SSL only works if the proper certificates have been installed on the Mirage server.

7.3 Configuring the Mirage System

The Mirage System has a number of configuration options that an Administrator can define.

To configure the Mirage Management System:

1. In the Mirage Management Console tree, right-click System Configuration and select Settings. The System Configuration window appears.

2. Make the required changes.

3. Click OK. The system configuration takes effect instantly.

The configurable options are illustrated in the following windows.
General Tab

In the **System Configuration** window **General** tab, the Administrator defines the standard options for the Mirage System, including the frequency that snapshots occur, the warning thresholds for volumes and CVD size, the account used to join domains, and the license file. You can also specify which upload policy to use when an end-user adds their CVD to the Mirage System.

![System Configuration window](image)

**Snapshots:**
- Number of snapshots at 1 hour intervals: 6
- Number of snapshots at 1 day intervals: 5
- Number of snapshots at 1 week intervals: 4
- Number of snapshots at 1 month intervals: 0

**Volumes:**
- Volume capacity - warning threshold (%): 85
- Volume capacity - critical threshold (%): 95
- Volume capacity check interval (seconds): 60

**Driver Library and USMT files volume:**

**CVDs:**
- CVD size warning threshold (MB): 51200

**Default Upload Policy:**

**Join Domain Account:**
- User: METISTECqa1
- Password: ********

**License:**
- Capacity: 10000 CVDs
- Expires: 9/11/2012 11:11:53 AM
• **Snapshots**: Configures the number of CVD snapshots retained by the system and available for restoration, at hourly, daily, weekly, and monthly intervals. For example, 7 days means 7 daily generations of CVD snapshot are retained and older generations are discarded. For more information about snapshots, see 16.2 Restoring CVD Snapshots.

• **Volumes**: Configures the percentage of volumes threshold warnings to display. For more information about using multiple volumes, see 9.2 Using the Mirage Volumes Window.
  • **Volume capacity - warning threshold (%)**: Issues a warning event in the Event Log when the volume reaches the percentage of data stored on the volume.
  • **Volume capacity - critical threshold (%)**: Issues a critical event when the volume reaches the maximum percentage of data stored on the volume.
  • **Volume capacity check interval (seconds)**: The interval (in seconds) when the system checks the volumes capacities.

• **CVDs**:
  • **CVD size warning threshold (MB)**: The maximum CVD size. When the CVD size is reached, an event is issued in the Event Log.
  • **Default Upload Policy**: Default upload policy that will be used when an end-user adds their CVD to the Mirage System. To change the default policy, click **Change**. The Assign Upload Policy window appears.

    ![Assign Upload Policy](image)

Select an upload policy to apply, and click **OK**.

• **Join Domain Account user and password**: The account must have access to join the domain and will be used during migration operations.
  **Note**: For the join domain account, the account must have the following permissions - Reset Password, Write all properties, Delete, Create computer objects, and Delete computer objects. Permissions are set using the Advanced Security Settings for Computers dialog for this object and all descendant objects.

• **License**: Capacity and License Expiry information are provided. The **Set License** button lets you add a license – see 3.6.1 Adding and Viewing Licenses.
7.3.2 CVD Auto Creation Tab

Automatic CVD creation enables an end user to manually create a new CVD for their machine, and avoid the need for IT manager intervention in the critical first phase of adding the machine to Mirage System. The Administrator can define whether the feature is enabled or disabled and what message is displayed to the end user when this operation takes place.

Once this is configured, any system that connects to the Mirage system prompts the end user to add their CVD. Additionally, a user can also initiate the CVD creation by right-clicking their Mirage icon in their system tray.

This allows an end user to manually create a new CVD for their machine, and avoid the need for IT manager intervention in the critical first phase of adding the machine to Mirage.

➢ To enable automatic CVD creation:

1. In the Mirage Management Console tree, right-click System Configuration and select Settings. The System Configuration window appears.

2. Select the CVD Auto Creation tab.

3. Select Enable automatic CVD creation. Click OK.
7.3.3 File Portal Tab

In the *File Portal* tab, an Administrator can enable the VMware File Portal, redefine the URL, and modify the message that the end user’s sees when the end user is prompted for access.
7.3.4  USMT Settings Tab

An Administrator must import the Microsoft User State Migration Tools (USMT) files that are required for the following Base Layer operations:

- Windows XP to Windows 7 Migration.
- Cross-hardware Windows 7 Migration (using hardware migration wizard)
- User Profile and Data-only restores (using the restore wizard)

The USMT folder can be found in the directories that are installed with the Windows Automated Installation Kit (AIK) software. You can download this software for free from Microsoft. Once downloaded, copy the USMT folder and all subdirectories to your Mirage Server and use this menu to import it.

Note: USMT 4 is the only version that is supported with this feature.

7.3.5  Experimental Features Tab

The experimental features are features that are not officially supported by VMware at this time but which an Administrator can enable on an experimental basis. VMware does not recommend using these features in a production environment.
Chapter 8

Managing the Driver Library

➢ In this Chapter...

8.1 Overview
8.2 Managing Driver Folders
8.3 Managing Driver Profiles

8.1 Overview

The Driver library allows an administrator to manage hardware specific drivers outside the core images in a separate repository and organize them by hardware families. Using a simple import wizard, drivers can be added and then viewed in the driver library’s console.

More importantly, the system can be configured to inject the necessary driver library to the relevant endpoints based on matching rules between the library and the endpoint configuration. This results in smaller core images and helps administrators to build more generic core images.

The Driver Library copies drivers from the Mirage system to the endpoint. When Windows scans for hardware changes, these copied drivers are used by the Windows Plug and Play (PnP) mechanism, and the appropriate drivers are installed as required.

8.1.1 Architecture

The diagram below explains how the Driver Library works with endpoints:

- A Mirage System can have multiple Driver Folders, multiple Driver Profiles, and many endpoints.
- A Driver Profile can contain drivers from multiple Driver Folders and a Driver Folder can be used by multiple Driver Profiles.
- A Driver Profile can be applied to one, many, or no endpoints.
For example, Profile A contains drivers from Driver Folder 1 and 2, and when the Profile is analyzed, the drivers from folders 1 and 2 are applied to 2 endpoints.

As another example, Profile B contains drivers only from Driver Folder 2 (which is also used by Profile A), and when the Profile is analyzed, the drivers from folder 2 are applied only to one endpoint.

8.1.2 Driver Library Application

The Driver Library is automatically used during the following operations:

- Centralization
- Migration
- Hardware migration / Restore
- Machine Cleanup
- Base Layer update
- SET driver library
8.2 Managing Driver Folders

The purpose of driver folders is to manage drivers that you have imported into the Mirage system. You can add these folders to the root (the All folder), or you can create your own sub-folders, or you can have Mirage mirror your current Driver Store folder structure by selecting the Keep original folder hierarchy check box.

The driver folders are used to import and store drivers into the Mirage system. You then use these folders.

Some important notes about the Driver Library:

- IT is able to group drivers by folders (for example, common model). A single driver may be associated with several folders.
- A folder may contain other folders (recursive hierarchy).
- Drivers can be enabled/disabled within the folder (without deleting it).
- Right-click on any of the device drivers and select Properties to view their details.

Note: VMware recommends obtaining drivers directly from vendor websites or restore media.

8.2.1 Creating a Drivers Folder

To create a drivers folder:

1. In the Mirage Management Console tree, expand the Driver Library node.
2. Right-click on Folders or any of the driver folders.
3. Select Add folder. The Add Folder window appears.
4. Enter a folder name and click OK.
8.2.2 Performing a Folder Operation

➢ To perform a folder operation:

1. In the Mirage Management Console tree, expand the Driver Library node.
2. Right-click on any of the driver folders.
3. To rename the folder, click Rename Folder, enter the new name and click OK.
4. To remove the folder, click Remove Folder, and then click Yes to continue or No to cancel.

When this operation is performed the drivers remain intact. The folder is merely a logical grouping of drivers that are stored on the system. Therefore, when you delete a folder, the drivers themselves persist.
5. To add drivers to the folder, click Add drivers. The Add drivers window appears.

6. Select a driver and then click OK.
8.2.3 Importing Drivers into a Folder

➢ To import drivers into a folder:

1. In the Mirage Management Console tree, expand the Driver Library node.
2. Right-click on any of the driver folders.
3. Click Import drivers. The Import Drivers window appears.

![Import Drivers window]

4. Input the UNC path where the drivers are stored (this is scanned recursively).
   Note: The Mirage Management Server must have access to this UNC path.
5. Select Keep original folder hierarchy to re-create the folder structure on your driver store within the Mirage System.
6. Click OK.
   Note: This UNC path must be reachable by the Mirage Server.

8.2.4 Adding a Driver to a Specific Folder from the All Folder

➢ To add a driver to a specific folder from the All folder:

1. In the Mirage Management Console tree, expand the Driver Library node.
2. In the All folder, right-click one or more drivers and select Add drivers to folder.
   The Add drivers to folders window appears.
3. Select the folders in the tree.
4. Click OK.

8.3 Managing Driver Profiles

A profile is used to select the driver folders to publish to a particular hardware model/set of hardware models. Some important things to know about driver profiles:

- A profile may select one or more driver folders.
- A profile contains rules to check if it applies to a particular hardware.
- The above rules are used to automatically select one or more matching profiles for a device.
- A warning is shown if no matching profile is found.

8.3.1 Creating/Editing Driver Library Profile

➢ To create/edit driver library profile:

1. In the Mirage Management Console tree, expand the Driver Library node.
2. Right-click on Profiles, and click Add or right-click on an existing profile and select Properties.
This window is used to define the Driver Folders that are applied to this profile and what rules apply to this profile. The rules are used to validate the endpoints that use these profiles during Mirage operations.

3. Enter a profile name and then select the checkboxes of the drivers that you want applied in this profile. For example, if you were building a profile for a Dell Latitude E6410, select all the driver folders that apply to that hardware family.

4. Click the Rules tab.
5. Create the criteria for this hardware family. Use the drop down menus to create specific rules for hardware families. For example, set the Vendor to Dell, and select the appropriate OS type.

6. Click **Apply** to test the result set that is returned by these rules.

7. Continue to fine-tune the rules until the result set is accurate.

8. Click **OK**.

   **Note:** These rules are automatically used to check which Driver Profiles should be applied to hardware during certain Mirage operations. Once these rules are defined no additional work is required for them to function, however, if devices that meet this criteria already exist in the Mirage system, you must initiate a Driver Profile update on those systems.

### 8.3.2 Setting Driver Library

An Administrator may want to apply the rules and profiles they have created to endpoints that have already been centralized within the Mirage system. The IT Administrator does not need to perform this SET operation for any clients that are added to the Mirage system after you have configured your driver library. Anytime an operation is performed that can leverage the Driver Library (Image updates, CVD restores, and so on), it does so automatically, without the IT Administrator needing to perform the Set Driver Library operation (below).

**➢ To set driver library:**

1. In the **Mirage Management Console** tree, expand the **Inventory** node and click on **All CVDs**.

2. Right-click on one or more CVDs (or a collection) and select **Apply Driver Library**. The following happens:
   - A profile is automatically selected for each device according to the rules.
   - Devices that match more than one profile receive a driver-store that contains a merged view of all the matching profiles.
   - A warning/and or event is issued for devices that have no matching driver-store.

The progress of a driver library download is visible in the desktop status window and in the task list of the Management Console and in the transaction logs. The drivers are stored in one of the Mirage volumes in the **MirageStorage** directory (and deduplication is applied). If you have multiple volumes you can change what volume the Driver Library is stored on by modifying the System Configuration options.

3. You can view the assigned Driver Profiles of any CVD by right-clicking a CVD and selecting **Properties**.
Chapter 9

Adding Multiple Volumes

In this Chapter...

9.1 Multiple Volumes Overview
9.2 Using the Mirage Volumes Window
9.3 Adding a Volume
9.4 Editing the Volume Information
9.5 Removing a Storage Volume
9.6 Mounting a Volume
9.7 Blocking a Volume
9.8 Unblocking a Volume
9.9 Volume Maintenance

9.1 Multiple Volumes Overview

VMware Mirage provides multiple storage volume support. As storage volumes become congested, more storage volumes are needed to keep up with the ever-increasing data storage. With multiple storage volumes, Mirage provides ample storage of CVDs and Base Layers for large enterprise organizations.

Each storage volume can contain Base Layers and CVDs. CVDs are assigned a storage volume when they are created.
9.2 Using the Mirage Volumes Window

The Mirage Volumes window displays all storage volumes connected to the Mirage Management System.

➢ To display the Mirage Volumes window:

1. In the Mirage Management Console tree, expand the System Configuration node.
2. Click Volumes. The Mirage Volumes window appears.

The Mirage Volumes window displays the following volume information:

- **ID**: A unique volume identification number set by the Mirage Management System.
- **Name**: The volume name assigned when the volume was added.
- **Volume State**: The current status of the storage volume. Volumes can have the following volume states:
  - **Mounted**: The volume is reachable and accessible.
  - **Malfunctioned**: The volume is currently unreachable and inaccessible. CVDs and Base Layers on this volume cannot be accessed or used until the volume status is restored to “Mounted”. A manual action is needed to rectify the problem.
  - **Unmounted**: The volume was temporarily disconnected by the Administrator using the Unmount Volume function. For more information about unmounting a volume, see 9.5.2 Unmounting a Volume.
  - **Removing**: The volume is being removed from the Mirage System.
- **Path**: The UNC or local path where the volume resides.

Note: It is recommended to run a SIS volume integrity check before returning the volume to the active state. For more information, see 9.9 Volume Maintenance.
• **Description**: A description of the storage volume assigned when the volume was added. You can edit the volume description using the *Edit Volume Information* window. For information about editing volume information, see 9.4 *Editing the Volume Information*.

• **Capacity (GB)**: The storage volume capacity in gigabytes.

• **Free Space (GB)**: the amount of free space in gigabytes available on the storage volume.

• **Number of CVDs**: The number of CVDs stored on the storage volume.

• **Number of Base Layers**: The number of Base Layers and Base Layer versions stored on the storage volume.

• **Status**: The status of the storage volume. Volumes can have the following statuses:
  - (blank) – The storage volume is available.
  - **Blocked** – The storage volume is not used when creating new CVDs and Base Layers, but continues to serve existing stored entities. For more information on blocked storage volumes, see 9.7 *Blocking a Volume*. 
9.3 Adding a Volume

This section describes how to add a storage volume to the Mirage System.

To add a volume to the Mirage System, the user account that manages the Mirage System must have access permissions to the new volume. The server service accesses the volume using the user credentials. In a CIFS (clustered) environment, the volume must be shared.

➢ To add a storage volume:

1. In the Mirage Management Console tree, right-click Volumes and select Add a Volume. Alternatively, click the Add Volume icon on the Volumes console toolbar. The Add a Volume window appears.

2. Type a name of the storage volume.

3. Type the server UNC path of the volume where the volume resides. Ensure that the volume has sufficient privileges for the Management server and the Mirage Server cluster to access this volume.

4. Type a description of the storage volume.

5. Click OK.

Note: Mirage performs the following validations when adding a new volume:
- If the path exists
- If the volume is empty
- If the volume supports alternative data streams
9.4 Editing the Volume Information

You can edit the volume name, description, and the UNC path in the storage volume information.

➢ To edit the volume information:

1. From the Volumes window, right-click the volume you want to edit the information and select Edit Volume Info from the popup menu. Alternatively, click the Edit Volume Info icon on the Volumes window toolbar. The Edit Volume Info window appears.

2. Edit the volume name and the UNC path as desired.

3. Type a description of the volume, if desired.

4. Click OK.

9.5 Removing a Storage Volume

There are several methods of removing a storage volume from the Mirage System:

- Remove
- Unmount

9.5.1 Removing a Volume

You can remove a storage volume from the Mirage System using the Remove volume function. The Remove volume function deletes the volume from the Mirage System.

Note: Before removing a volume from the Mirage System, ensure that the volume is empty and does not contain any CVDs or Base Layers. The remove operation fails if CVDs or Base Layers reside on the selected volume.
➢ To remove a storage volume from the Mirage System:

1. From the Volumes window, right-click the volume you want to remove and select **Remove** from the popup menu. Alternatively, click the **Remove Volume** icon on the Volumes window toolbar. The **Remove volume** confirmation message appears.

2. Click **Yes**.

### 9.5.2 Unmounting a Volume

Unmounting a volume places the volume in a non-operational status but retains the CVD and Base Layer data on the volume. A volume should be unmounted before performing any maintenance operations such as integrity checks.

➢ To unmount a volume:

1. From the Volumes window, right-click the volume you want to unmount and select **Unmount Volume** from the popup menu. Alternatively, click the **Unmount Volume** icon on the Volumes window toolbar. The **Unmount volume** confirmation message appears.

2. Click **Yes**. When the volume has been unmounted, the **Volume State** column on the Volumes window displays **Unmounted**.

### 9.6 Mounting a Volume

You can activate an unmounted volume when the storage volume is ready to be reactivated. The activate function is unavailable when the **Volume State** is **Mounted**.

**Note:** You should run the SIS integrity check before mounting a volume if the volume was in the **Malfunctioned** state. For more information, see 9.9 Volume Maintenance.

➢ To mount a volume:

1. From the Volumes window, right-click the volume you want to mount and select **Mount** from the popup menu. A confirmation message appears.

2. Click **Yes**. The volume state is modified to **Mounted**.
9.7 Blocking a Volume

You can block a storage volume to prevent it from being used when creating a new CVDs or Base Layers. This is useful when the storage volume has reached a volume capacity threshold or if you want to stop populating it with new CVDs or Base Layers. Blocking a volume does not impact access or updates to existing CVD and Base Layer objects on the volume.

**Note**: Moving a CVD or a Base Layer from the blocked volume to another volume or to a blocked volume is not allowed.

➢ **To block a volume:**

1. From the *Volumes* window, right-click the volume you want to block and select *Block* from the popup menu. The *Block volume* confirmation message appears.
2. Click *Yes*. The *Volume Status* column on the *Volumes* window is modified to *Blocked*.

9.8 Unblocking a Volume

You can unblock a volume that has been previously blocked. This enables the volume to accept new CVDs and Base Layers in addition to updating existing data.

➢ **To unblock a volume:**

1. From the *Volumes* window, right-click the volume you want to unblock and select *Unblock* from the popup menu. The *Unblock volume* confirmation message appears.
2. Click *Yes*. The *Blocked* status in the *Volume Status* column is removed.
9.9 Volume Maintenance

When a volume state has changed to malfunctioned, such as following a network disconnect or a storage access error, it is recommended to schedule a Single-Instance Storage (SIS) integrity procedure before mounting the volume on the Mirage System. The SIS integrity script is located in the `Wanova.Server.Tools.zip` file.

**Note:** This procedure may take a few hours to complete depending on the number of files on the volume. During this time, CVDs residing on this volume are suspended, and Base Layers stored on the volume are not accessible.

➢ **To run the SIS Integrity script:**

1. Unmount the volume using the `Unmount` option. For more information, see 9.5.2 Unmounting a Volume.
2. Run the SIS Integrity script from a Mirage Server.
3. Open the command window.
4. Type the commands:

   ```
   C:\Program Files\Wanova\Mirage Server> Wanova.Server.Tools.exe SisIntegrity -full <volume path>
   For example:
   SisIntegrity -full \apollo\vol100\MirageStorage
   ```

When the SIS Integrity script is completed, the following message appears.

```csharp
C:\Program Files\Wanova\Mirage Server> Wanova.Server.Tools.exe SisIntegrity -full -online \apollo\vol100\MirageStorage
SIS Integrity version 2.0.0.27151
Scanning SIS structure (online scan)... SIS integrity check summary:
Total files scanned: 26,550
Total SIS entries scanned: 26,550
Total run time: 00:13:50.1070702
Total files with invalid header: 0
Total files with invalid data: 0
Total data loss errors: 0
Total possible storage leaks: 0 (0 KB)
Total actual storage leaks: 0 (0 KB)
No corrupted CVDs found
No corrupted BIs found
```
Chapter 10
Using Branch Reflectors

In this Chapter...

10.1 Branch Reflector Overview
10.2 How Client End Points Use Branch Reflectors
10.3 Installing a Branch Reflector
10.4 Enabling a Branch Reflector
10.5 Configuring Branch Reflector
10.6 Disabling a Branch Reflector
10.7 Rejecting Peers
10.8 Accepting Peers
10.9 Suspending Network Operations
10.10 Resuming Network Operations
10.11 Monitoring Branch Reflectors and Peer Clients

10.1 Branch Reflector Overview

The Mirage Branch Reflector feature promotes efficient Base Layer, Driver, and USMT distribution to Branch offices and remote sites where multiple users are sharing the WAN link to the Datacenter.

The Branch Reflector peering service can be enabled on any endpoint device installed with a Mirage Client. The Branch Reflector downloads Base Layer images, Driver files and USMT files from the Mirage Server, and optimizes their transfer to other Mirage Clients in the site. Files that already reside on the Branch Reflector machine’s disk will be used and will not be asked from the Mirage server at all.

The files are downloaded only once to the Branch Reflector, and common files across Base Layers become readily available without duplicate downloads.
The following diagram illustrates an example of a site with Branch Reflector enabled:

10.2 How Client End Points Use Branch Reflectors

10.2.1 Branch Reflector Selection Process

One or more Branch Reflectors can be enabled in each site. Branch reflectors that are enabled are automatically detected by Client End Points on the same or different sites.

The Mirage IP detection and proximity algorithm finds a matching Branch Reflector, as follows:

1. The algorithm first verifies whether a potential Branch Reflector is in the same subnet as the client.

2. If the Branch Reflector is in another subnet, the algorithm checks if the Branch Reflector is configured to service the clients subnet (see Additional Networks in 10.5.2 Configuring Specific Branch Reflector Values).

3. Alternatively, the algorithm can use the client site information to check whether the Branch Reflector is in the same Active Directory site as the client (see Use Active Directory Sites in 10.5.1 Setting Defaults for Branch Reflectors).
4. Additionally, the algorithm checks the latency between the Branch Reflector and the Mirage Client is within the threshold (see **Required Proximity** in **10.5.1 Setting Defaults for Branch Reflectors**).

5. If a match is found between the client and the Branch Reflector that satisfies the above conditions, the client connects to the Branch Reflector to download a Base Layer. Otherwise, the client repeats the matching process with the next Branch Reflector.

6. If no match is found or all suitable Branch Reflectors are currently unavailable, the client connects to the Mirage Server directly as a last resort. Alternatively, in order to keep network traffic as low as possible, setting **Always Prefer Branch Reflector** (see **10.5.1 Setting Defaults for Branch Reflectors**), forces clients to continually repeat the matching process until a suitable Branch Reflector becomes available. (In this case, the client will connect to the Mirage server only if no Branch Reflectors are defined.)

### 10.2.2 Branch Reflector Cache

A Branch Reflector maintains a dedicated cache which holds Base Layer, Driver library and USMT file downloads from the server, from which distribution of these files to Client End Points can be optimized.

**Note:** The Branch Reflector should have enough disk space to enable cache storage of these files.

### 10.2.3 Branch Reflector Local File Sharing

Files available for sharing from a Branch Reflector are not limited to server downloads from the Branch Reflector cache. The Branch Reflector can share any files on its local disk with Client End Points. These files can be resident local files, or files copied from a DVD or USB device.

For example, a test machine with a Windows 7 operating system can be configured as a Branch Reflector to assist in the migration of other clients from Windows XP to Windows 7. In this case the Branch Reflector will use the local Windows 7 operating system files and will download from the Mirage server only specific files that are missing, and not the complete Windows 7 operating system.

The local file sharing capability is available from any Branch Reflector, regardless of its operating system type.
10.3 Installing a Branch Reflector

Any Mirage Client endpoint can function as a Branch Reflector, in addition to serving an end-user. Alternatively, a dedicated Branch Reflector host can be installed to support larger populations. The Branch Reflector is installed as any typical Mirage Client, on a supported edition of Windows XP or Windows 7.

It is recommended to have the Branch Reflector connected to a switched LAN and not to a wireless network. There should be enough disk space available to store the Base Layers of the connected endpoint devices.

**Note:** Port 8001 on the Branch Reflector host must be opened to allow incoming connections from peer endpoint devices.

**Note:** A dual-core CPU and 2GB RAM is recommended if the Branch Reflector endpoint is also serving as a general purpose desktop for an interactive user.

10.4 Enabling a Branch Reflector

A branch reflector is enabled using the Mirage Management Console.

➢ **To enable a branch reflector:**

- Navigate to the **Inventory > Assigned Devices** tab and right-click an endpoint device. Then select **Branch Reflector > Enable Branch Reflector**.
The device is listed in the Branch Reflectors window (as well as remaining on the Device Inventory list). You can view which devices are enabled as Branch Reflectors by navigating to the System Configuration > Branch Reflectors tab.

10.5 Configuring Branch Reflectors

This section describes how to set default values of parameters governing the behavior of Branch Reflectors, as well as how to set parameters for individual Branch Reflectors if needed.

10.5.1 Setting Defaults for Branch Reflectors

The IT Administrator sets default values for parameters associated with Branch Reflectors using the System Configuration window.

The Maximum Connections and Cache Size apply to newly defined Branch Reflectors, and can then be individually corrected as needed for selected Branch Reflectors – see 10.5.2 Configuring Specific Branch Reflector Values.

The other parameters in this window automatically apply system-wide with respect to all Branch Reflectors, existing or new.

➢ To configure default values for new Branch Reflectors:

1. In the Mirage Management Console tree, right-click System Configuration and select Settings. The System Configuration window appears.
2. Select the *Branch Reflector* tab and configure the required default values.

- **Default Maximum Connections**: Maximum number of endpoint devices that can simultaneously connect to the Branch Reflector at the same time.

- **Default Cache Size (GB)**: Cache size that the Branch Reflector has allocated. 
  **Note**: Ensure that the Branch Reflector endpoint has enough disk space for the cache, in addition to its other usage as a general purpose desktop.

- **Required Proximity (msec)**: Maximal time (for example, 50 ms) that it should take a Branch Reflector to answer ping from an endpoint for that endpoint to consider downloading through the Branch Reflector. If no Branch Reflectors satisfy the specified proximity, the endpoint is set to download from the server.

- **Use Active Directory Sites**: Mirage uses subnet and physical proximity information to choose Branch Reflectors. Select this checkbox to use Active Directory site information to determine which of several Branch Reflectors in the system to connect to.

- **Always Prefer Branch Reflector**: In order to keep network traffic as low as possible, selecting this option forces clients to continually repeat the matching process until a suitable Branch Reflector becomes available. (In this case, a client will connect to the Mirage server only if no Branch Reflectors are defined.) If the option is not selected, and no match is found or suitable Branch Reflectors are currently unavailable, the client connects to the Mirage Server directly as a last resort.
10.5.2 Configuring Specific Branch Reflector Values

Default values apply to newly created Branch Reflectors – see 10.5.1 Setting Defaults for Branch Reflectors.

The following parameters can be adjusted for individual Branch Reflectors as needed:

- **Maximum Connections**: The maximum number of endpoint devices that can connect to the Branch Reflector at the same time.
- **Cache Size (GB)**: The cache size in gigabytes that the Branch Reflector has allocated.
  **Note**: Ensure that the Branch Reflector endpoint has enough disk space for the cache, in addition to its other usage as a general purpose desktop.
- **Additional Networks**: Networks where the Branch Reflector is authorized to service Client End Points in addition to its own local subnets.

➢ To configure the Branch Reflector:

1. From the Branch Reflectors list, right-click the Branch Reflector device and select **Branch Reflector > Configure**. The **Branch Reflector Configuration** window appears.

2. Enter the parameters values that should apply to the current Branch Reflector.

3. Click **OK**. The Branch Reflector configuration settings take effect immediately. There is no need to restart the Branch Reflector client.
10.6 Disabling a Branch Reflector

You can disable the Branch Reflector peering service at any time. The endpoint device is retained in the Device Inventory window and continues to be available as a regular Mirage endpoint.

**Note:** Disabling a Branch Reflector causes its Base Layer cache to be deleted.

➢ To disable a Branch Reflector:

- From the System Configuration > Branch Reflectors node, right-click the Branch Reflector device and select Branch Reflector > Disable Branch Reflector from the popup menu. The device is deleted from the Branch Reflectors list. It is not deleted as a device or from your device inventory.

10.7 Rejecting Peers

When the Branch Reflector is operating slowly or is using excessive bandwidth, you can stop providing service to its peer clients. When using the Reject Peers function, the Branch Reflector service is only paused and is not deleted from the Branch Reflectors list. Also, the Branch Reflector cache is preserved.

➢ To reject the Branch Reflector peers:

- From the System Configuration > Branch Reflectors node, right-click the Branch Reflector device and select Branch Reflector > Reject Peers. The Branch Reflector Status is set to Paused.

10.8 Accepting Peers

When the branch reflector status is **Paused**, you can resume providing service to the its peer clients using the Accept Peers function.

➢ To resume providing service to the Branch Reflector peers:

- From the System Configuration > Branch Reflectors node, right-click the Branch Reflector device and select Branch Reflector > Accept Peers. The Branch Reflector Status is set to Enabled.
10.9 Suspending Network Operations

You can suspend network communications with the Mirage Server for both the Branch Reflectors and regular endpoint devices. Suspending network operations for Branch Reflectors still allows its peers to download Base Layer files from the Branch Reflector cache, but the Branch Reflector is not able to download new files from the Mirage Server.

➢ To suspend network operations:

- From the Branch Reflector list, right-click the Branch Reflector device and select **Suspend Network Operations** from the popup menu. The network operations are suspended. You can view which branch reflectors are suspended in the **Branch Reflectors** window by selecting the **Connection State** on the column headings drop-down menu.

10.10 Resuming Network Operations

Resuming network operations enables the branch reflector or the individual endpoint device to communicate with the Mirage Server cluster.

➢ To resume network connections:

- From the **Branch Reflectors** node, right-click a suspended Branch Reflector device and select **Resume Network Operations** from the popup menu. The network operations are resumed. At any time, you may inspect which Branch Reflectors are connected by selecting the **Connection State** on the column headings drop-down menu.
10.11 Monitoring Branch Reflectors and Peer Clients

You can monitor Branch Reflector and associated peer client Base Layer download activity in various ways.

10.11.1 Viewing CVD Activity and Branch Reflector Association

The All CVDs window shows CVDs’ current Activity and associated upload/download Progress (% completed) and Rate (transfer speed in kB/s). The Branch Reflector column shows the Branch Reflector to which CVDs are currently connected, if any.

➢ To open the All CVDs window:

- Navigate to the Inventory > All CVDs node. The All CVDs window appears.
10.11.2 Viewing Branch Reflector and Peer Client Information

The Branch Reflector window shows information about Branch Reflectors and their currently connected peer clients.

➢ To view information about Branch Reflectors:
- Navigate to the System Configuration > Branch Reflectors node. The Branch Reflectors window appears.

The Branch Reflector window Downloading Peers and Waiting Peers columns show how many peer clients connected to a Branch Reflector are currently either downloading the Base Layer from this Branch Reflector, or waiting to download.

Endpoints in excess of the Maximum Connections (maximum allowed simultaneously downloading client peers) defined for this Branch Reflector will be rejected and will receive their download from another Branch Reflector or directly from the server.

**Note:** If you observe that the number of Downloading Peers is constantly close to the Maximum Connections, consider either increasing the Maximum Connections value or configuring another client in the site as a Branch Reflector.
To view information about connected peer clients:

- Right-click a Branch Reflector in the Branch Refectors window and select Branch Reflector > Show Connected Peers. The Connected Peers window appears.

This window shows each connected peer client’s identifiers, current Activity (for example, waiting/downloading), and the Progress of that activity.

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>User Name</th>
<th>Activity</th>
<th>Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>AKOP-SP2-IM1</td>
<td>AKOP-SP2-IM1|Administrator</td>
<td>pending reboot</td>
<td>100%</td>
</tr>
</tbody>
</table>

10.11.3 Monitoring Branch Reflector and Peer Client Transactions

The Transaction Log window lets you track Branch Reflector and peer client activity related to Base Layer download. The Transaction Properties window shows how much data was acquired from a Branch Reflector by a peer client.

To view transactions:

- Navigate to the Logs > Transaction Log node. The Transaction Log appears.

The following example shows the Branch Reflector activities in the Transaction Log.

Transaction 1 shows a Branch Reflector is downloading the Base Layer.
Transaction 2 shows an endpoint in which a peer client has updated its image. The properties of the Update Base Layer transaction shows how much data was downloaded from the Branch Reflector and how much data was downloaded directly from the Mirage Server.
To view the transaction properties:

- From the Transaction Log, right-click a transaction line and select **Update Base Layer transaction > Properties**. The Transaction Properties window appears.

In this example, the endpoint transaction (in previous example) downloaded 173 MB of data from the Branch Reflector and 0 MB from the server.
Chapter 11

Deploying Additional Mirage Servers

In this Chapter...

11.1 Multiple Servers Overview
11.2 Using the Mirage Servers Window
11.3 Adding a New Server
11.4 Stopping and Starting the Server Service
11.5 Removing a Server
11.6 Integrating the VMware Mirage System and Load Balancing
11.7 Configuring the VMware Watchdog Service

11.1 Multiple Servers Overview

VMware Mirage offers enterprise organizations with large amounts of endpoint devices to add multiple servers to the Mirage System, providing optimal access and efficiency where a single server is not sufficient. The Mirage Management Server and the Management Console control and manage all the multiple servers.

Additionally, Mirage provides multiple storage volume support. As storage volumes become congested, more storage volumes are needed to keep up with the ever-increasing data storage. With multiple storage volumes, Mirage provides ample storage of CVDs and Base Layers for large enterprise organizations.

Each storage volume can contain Base Layers and CVDs. CVDs are assigned a storage volume when they are created.

Any Mirage Server that uses the Mirage File Portal requires an IIS 7.0 installation.
The following diagram illustrates a possible scenario of multiple servers and storage volumes:

Each Mirage Server (cluster node) supports up to 1500 CVDs, depending on its actual system specifications. The **Maximum Connections** option, set in the server configuration function, enables the Mirage administrator to control the number of CVDs permitted on each server. For more information, see 7.2 *Configuring a Mirage Server*.

An enterprise datacenter can have multiple servers configured in a cluster. Load balancers are used in conjunction with the Mirage System to direct client connections to available servers. For a detailed discussion on load balancing in the Mirage System, see 11.6 *Integrating the VMware Mirage System and Load Balancing*. 

* VMware File Portal requires IIS 7.0 installed on the Mirage Servers.
11.2 Using the Mirage Servers Window

The Mirage Servers window displays all servers connected to the Mirage Management system.

➢ To display the Mirage Servers window:

1. In the Mirage Management Console tree, expand the System Configuration node.
2. Click Servers. The Servers window appears.

The Servers window displays the following server information:

- **ID**: A unique server identification number configured by the Mirage Management System.
- **Status**: The status of the server. Servers can have the following statuses:
  - **Up**: the server is available and running
  - **Down**: the server is not available
- **Name**: The name of the server machine.
- **Status duration**: Amount of time that the server has been in the same status.
- **Connections**: The number of CVDs currently connected to the server.
- **Max Connections**: The maximum number of concurrent CVD connections allowed on the server. This setting can be configured using the server configuration. For more information, see 7.2 Configuring a Mirage Server.

**Note**: It is recommended to use the default setting. Different server specifications may allow changing this setting. For best results, consult with VMware support before making modifications.

- **Use SSL**: Is this server configured to have clients connect using SSL or not. This is a global configuration.
- **Port**: Port that the Mirage server is configured to communicate with clients over.
• CPU: The average percentage of CPU currently running for this server over a 15 minute period.

• Used memory (committed): The average amount of memory in megabytes that is currently being used for the server over a 15 minute period.

• Physical Memory: The amount of physical memory allocated for the server.

11.3 Adding a New Server

This section describes how to install multiple Mirage Servers in the Mirage Management System.

➢ To install a Mirage Server:

1. Double-click the Mirage.server.x64.[BUILDNUMBER].msi file. The Mirage Server installation commences and the Mirage Server Setup Wizard window appears showing the installation process. For instructions on installing a Mirage Server, see 3.7 Installing a Mirage Server. When the server is installed, it automatically registers itself with the Mirage Management Server and appears in the servers list.

2. Repeat the server installation process for each server you want to install on the Mirage Management System.

11.4 Stopping and Starting the Server Service

When maintenance is to be performed on the servers or when backing up the servers, you can stop and start a server service in the Mirage Management System.

➢ To stop the Mirage Server service:

1. In the Servers window, right-click the server you want to stop and select Stop Server Service. The Stop server service confirmation message appears.

2. Click Yes.

➢ To start the Mirage Server service:

• In the Servers window, right-click the server you want to start and select Start Server Service. The server service is started and the server status displays Up.
11.5 Removing a Server

A Mirage Server can be removed from the Mirage Management System. Removing a server does not uninstall the server, but only removes the server from the Mirage System and does not remove any CVD data from the shared Mirage storage volumes.

➢ To remove a server from the Mirage System:

1. In the Servers window, right-click the server you want to remove and select Remove. The Remove server service confirmation message appears.

2. Click Yes. The server is removed from the Mirage Management system.

   Note: Removing the server does not uninstall the server from the server machine. The server should be uninstalled manually.

11.6 Integrating the VMware Mirage System and Load Balancing

As there are many load balancers in the market today, VMware Mirage provides a load balancing framework, called VMware Watchdog, in which Administrators can use to integrate with the existing load balancer servers.

VMware Watchdog is a service that periodically checks if a specific server is running and whether it can receive new connections.

When the server state changes, the VMware Watchdog calls an external command to communicate the state change to the load balancer. The commands can be customized and configured to match the particular type of load balancer deployed in the datacenter.

The following are the Mirage Server states:

- **Alive**: Signals that a server is running and is available to receive new client connections.
- **Full**: Signals that a server has reached the maximum number of concurrent connections. The service is still running but new client connections are not accepted.
- **Dead**: Signals that a Mirage Server service is not responding or is not operational.

By default, the Watchdog service is initially disabled. You must start the service for it to function.

The Mirage Watchdog log file is located in C:\ProgramData\Wanova Mirage\Watchdog\Watchdog.txt
11.7 Configuring the VMware Watchdog Service

The Watchdog configuration file (Wanova Watchdog.exe.xml) is an XML file located in the C:\Program Files\Wanova\Mirage Server directory. You can configure which service and port to monitor, the interval time (in milliseconds), and which load balancing command to run when switching to any state.

**Note**: After modifying the settings in the XML file, you must restart the VMware Watchdog service.

The following options can be configured in the Watchdog service:

- **PollTimeMs**: Polling frequency (in milliseconds)
- **ServiceName**: VMware server service name
- **ListenPort**: Listening port
- **OnAliveProcess**: The commands to run when the Mirage Server is open to receive new connections
- **OnAliveArgs**: The arguments used for the OnAliveProcess commands
- **OnDeadProcess**: The commands to run when the Mirage Server is down
- **OnDeadArgs**: The arguments used for the OnDeadProcess commands
- **OnFullProcess**: The commands to run when the Mirage Server cannot receive new connections
- **OnFullArgs**: The arguments used for the OnFullProcess commands

For reference purposes, VMware Mirage provides a default script to work with the Microsoft Network Load Balancer (NLB).

**Note**: When configuring an NLB port rule, make sure to configure the port rule to listen on all the Cluster Virtual IP (VIP) addresses and not just on a specific VIP address. This is required for the default script provided by Mirage to work.
The following are the specific NLB parameters that are configured in the XML file. The **PollTimeMs**, **ServiceName**, and **ListenPort** commands are relevant for all load balancing scripts.

For each Mirage Server, replace the IP address with the dedicated IP address of the server node as registered with the cluster manager.

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>PollTimeMs</td>
<td><code>&lt;setting name=&quot;PollTimeMs&quot; serializeAs=&quot;String&quot;&gt;5000&lt;/value&gt;</code></td>
</tr>
<tr>
<td>ServiceName</td>
<td><code>&lt;setting name=&quot;ServiceName&quot; serializeAs=&quot;String&quot;&gt;Wanova Mirage Server Service&lt;/value&gt;</code></td>
</tr>
<tr>
<td>ListenPort</td>
<td><code>&lt;setting name=&quot;ListenPort&quot; serializeAs=&quot;String&quot;&gt;8000&lt;/value&gt;</code></td>
</tr>
<tr>
<td>OnAliveProcess</td>
<td><code>&lt;setting name=&quot;OnAliveProcess&quot; serializeAs=&quot;String&quot;&gt;cscript.exe&lt;/value&gt;</code></td>
</tr>
<tr>
<td>OnAliveArgs</td>
<td><code>&lt;setting name=&quot;OnAliveArgs&quot; serializeAs=&quot;String&quot;&gt;nlbcontrol.vbs 10.10.10.10 enable -1&lt;/value&gt;</code></td>
</tr>
<tr>
<td>OnDeadProcess</td>
<td><code>&lt;setting name=&quot;OnDeadProcess&quot; serializeAs=&quot;String&quot;&gt;cscript.exe&lt;/value&gt;</code></td>
</tr>
<tr>
<td>OnDeadArgs</td>
<td><code>&lt;setting name=&quot;OnDeadArgs&quot; serializeAs=&quot;String&quot;&gt;NlbControl.vbs 10.10.10.10 disable -1&lt;/value&gt;</code></td>
</tr>
<tr>
<td>OnFullProcess</td>
<td><code>&lt;setting name=&quot;OnFullProcess&quot; serializeAs=&quot;String&quot;&gt;cscript.exe&lt;/value&gt;</code></td>
</tr>
<tr>
<td>OnFullArgs</td>
<td><code>&lt;setting name=&quot;OnFullArgs&quot; serializeAs=&quot;String&quot;&gt;NlbControl.vbs 10.10.10.10 drain -1&lt;/value&gt;</code></td>
</tr>
</tbody>
</table>

**Note:** VMware recommends using the default NLB load balancing settings:

- Affinity= single
- Timeout=infinity
PART 5 - IMAGE MANAGEMENT

➢ In this Part...

12. Image Management Overview
   12.1 Traditional versus Mirage Image Management Overview
   12.2 Base Layer Management Life Cycle
   12.3 Different Hardware Platforms with Base Layers
   12.4 Planning and Preparation for Image Management

13. Preparing a Reference Machine
   13.1 Setting Up a Reference Machine
   13.2 Software Considerations
   13.3 Settings Captured from Reference Machine

14. Capturing Base Layers
   14.1 Editing Base Layer Rules
   14.2 Base Layer Override Policy
   14.3 Post-Base Layer Scripts
   14.4 Capturing Base Layers
   14.5 Recreating a Reference Machine from a Base Layer

15. Assigning Base Layers
   15.1 Introduction
   15.2 Comparison Report between Base Layer and CVD
   15.3 Testing the Base Layer before Rollout
   15.4 Assigning Layers
   15.5 Base Layer Provisioning
   15.6 Monitoring Layer Assignments
   15.7 Dealing with Conflicts
   15.8 Updating a Base Layer Assigned to a CVD
   15.9 Enforcing a Base Layer
Chapter 12

Image Management Overview

In this Chapter...

12.1 Traditional versus Mirage Image Management Overview
12.2 Base Layer Management Life Cycle
12.3 Different Hardware Platforms with Base Layers
12.4 Planning and Preparation for Image Management

12.1 Traditional versus Mirage Image Management Overview

Operating system (OS) and core application images are commonly deployed in one of the following ways:

- **Individual installation** and configuration of the OS on each physical endpoint.
- **Image-based deployment:** Installation and configuration of the OS and core applications on a reference machine. This is followed by the capture of reference machine disk content into a generalized Base Layer, and the distribution of the Base Layer to endpoints for installation over the network using, for example, a PXE boot, or a distribution media such as a USB flash disk, or a DVD and a setup procedure that instantiates the image to the specific machine’s hardware profile, assigned identity, and user settings.

The two main advantages of image-based deployment are that Administrators do not need to manually install the OS and application components on each and every physical endpoint, and the fact that the functional end result is the same. For an organization with more than a few dozen endpoints, this is a critical consideration and, therefore, image-based deployment is the main method of deployment. Once a Base Layer is deployed and set up, subsequent changes to it or new applications added to the endpoints by IT are delivered to the endpoints incrementally as individual packages.
Furthermore, each endpoint’s image further diverges from the original Base Layer resulting from user-installed applications, plug-ins, and other customizations, which often overwrite elements of the Base Layer. Over time, there remains little resemblance between the Base Layer and the endpoint contents, leading to the so-called image sprawl problem. This poses problems not only in maintaining the health and compliance of the endpoints, but also in supporting and troubleshooting endpoints since each one contains a potentially very different image compared to the Base Layer or even the result of malicious tampering.

One way to potentially mitigate the image sprawl problem is periodically to redeploy an updated Base Layer to all endpoints, ensuring a common baseline. However, there are several challenges with this simplistic approach:

- The new Base Layer would remove all personalization that users have attached to it. User data would have to be backed up and restored, which is a very costly and tedious procedure. Moreover, all user-installed applications and customizations would need to be reinstalled by the user since they are wiped out by the new image, a major issue for most customers.

- Base Layers tend to contain several GB of data. Frequently, sending such images to all endpoints over the network is impractical, especially when users are distributed and remote over the WAN.

Redeploying a new image implies reformatting and reinstalling the OS, resulting in a long, tedious, and disruptive process for end users.

12.1.1 VMware Mirage: A New Approach to Image-based Deployment and Updates

Mirage offers a new approach to the current limitations of image-based updates. By using Mirage, the concept of a Base Layer is used in a broader context. Instead of using the Base Layer only once during deployment, Mirage uses the Base Layer for any image update. This means that when an Administrator wants to update the endpoints, all they need do is update the reference machine. Once performed, the administrator captures the Base Layer, essentially a snapshot in time of the contents of the reference machine devoid of any user-specific or machine-specific content. The Base Layer is then transferred to all of the endpoints.

Using a proprietary technology, the Mirage client automatically swaps the old image with the new image without affecting user personalization. Since the effect of the update is equivalent to reimaging the endpoint with the entire Base Layer, this method ensures that all endpoints always contain the correct and most up-to-date working Base Layer that complies with corporate policy. For example, if the endpoint has been tampered with (either inadvertently or intentionally), the next Base Layer update realigns the endpoint with the content of the IT-managed Base Layer.
The key advantage of Mirage image-based deployment is the way it addresses the main limitations of current image-based update solutions:

- **Personalization Preservation**: Mirage decouples the desktop into four distinct layers:
  
a. **Base Layer**: Operating system, service packs, core applications

b. **Driver Library**: System drivers as defined by the IT Administrator by importing drivers and using Driver Profiles.

c. **Machine State and User Applications**: Machine ID, user-installed applications, general application settings

d. **User Data and Settings**: User data files, preferences and settings

Mirage’s layering and image-swapping technology enables administrators to update endpoints with new versions of the Base Layer without compromising user personalization or user-installed applications.

- **Network Efficiency**: Mirage employs advanced transport optimization technologies to ensure that image updates are transferred quickly and with minimal use of bandwidth. Specifically, multi-GB images are typically transferred in minutes over the WAN. Furthermore, during the transfer of the updated Base Layer, there is no disruption or impact on the user experience at the endpoint.

- **No Reformatting**: Mirage Base Layer updates do not require reformatting of the endpoint or any other manual intervention in setting up the desktop. At most, users are asked to reboot their desktop. After reboot, the revised Base Layer appears seamlessly, with prior personalization and user data intact.
### 12.2 Base Layer Management Life Cycle

A **Base Layer** is a template for common desktop content, cleared of specific identity information and made suitable for mass deployment to a large group of endpoints. The Base Layer includes the operating system, service packs and patches, as well as core enterprise applications and their settings.

The basic Base Layer lifecycle is illustrated in the following figure. It begins with a reference machine, used by Administrators to create and maintain Base Layers.

While working on the **Reference Machine**, administrators manage and update the content planned for inclusion in the Base Layer by performing various operations, such as adding applications or patching the operating system.

Using the Mirage Management Console, an administrator performs the **Base Layer Capture** operation on the reference machine. The capture creates a point-in-time snapshot of the data and state of the live reference machine, which is generalized for mass deployment. The Base Layer is given a name and version, and stored in the Base Layer repository of the Mirage Server.

Next is the **Base Layer Update**. This step is initiated from the Mirage Management Console. During this phase, the revised Base Layer is distributed to the relevant endpoint desktops. At the end of this process, the new Base Layer is stored at each desktop, ready to be applied. The user is advised to reboot the endpoint. After the reboot, the endpoint automatically performs the **Apply Base Layer** operation, which swaps the old Base Layer with the new one, and instantiates the endpoint.
Any changes in an endpoint resulting from the Base Layer update automatically propagate back to the CVD. When the CVD is synchronized with the latest changes, the Base Layer update operation for that endpoint is completed. Because each endpoint operates at its own pace, depending on network connectivity and whether the desktop is online or offline, this phase ends at different times for different desktops.

When an administrator next updates the Base Layer, the process begins again by generating a new version of the Base Layer.

The Base Layer management lifecycle is policy-driven. For example, Upload Policy that belongs to the Reference CVD contains system rules that determine which elements of the reference machine are not included in the Base Layer. Similarly, the Base Layer Rules policy determines which elements of the Base Layer are not downloaded to endpoints.

Both policies contain system-defined defaults, which are typically sufficient for standard deployments. Additionally, the system allows the administrator to add custom rules to the policy. More details on the policy rules are provided in later sections.

12.3 Different Hardware Platforms with Base Layers

Administrators can now create generic Base Layers that can be used on a number of different hardware families by leveraging the Mirage Driver Library feature. By using the Driver Library, an administrator can have a minimum number of generic base layers and then have the appropriate hardware drivers applied automatically by using Driver Profiles.

12.3.1 Virtual Machine Support

A common use case with Mirage includes the re-assignment of a CVD from a physical machine to a virtual machine and vice versa. This enables the administrator to download a CVD to a workbench device at the data center for troubleshooting purposes.

In addition, most virtualization platforms include integration components to enhance the experience of working on a virtual machine (for example, VMware tools). These too should be included as part of a virtual machine Base Layer.

The use of a separate Base Layer for a virtual machine is recommended, especially if the integration features are to be a part of the Base Layer (for example, VMware tools).
12.3.2 Special Case Hardware Drivers

Certain hardware drivers include installation programs that make them incompatible with pre-installation in a Base Layer (for example, Bluetooth Driver installation and Wireless-over-USB). These drivers can be installed using a special script which is launched by Mirage after a Base Layer is applied. Mirage then reports any failure to the management service at the center.

12.4 Planning and Preparation for Image Management

When building a reference machine, it is important to select the software to include in the Base Layer carefully, since this software is distributed to end users with the Base Layer.

The following categories of software require special instructions:

- System level software
- Software licensing
- User-specific software
- OEM (and hardware-specific) software
- Endpoint Security software

12.4.1 System Level Software

It is highly recommended to include the following applications in the Base Layer:

- Anti-virus/security products
- VPN or other connectivity software (such as iPass)
- Firewalls

System level software is very sensitive to conflicting software. It is therefore important that endpoints do not receive conflicting software via other distribution methods. If a certain type of system level software (for example, anti-virus) is distributed via a Base Layer, do not distribute different versions of the same software or conflicting software via other software distribution mechanisms, and vice versa.

Note: It is recommended to ensure that minimal restore set includes the organization VPN, antivirus, firewall applications as well as the driver store.
12.4.2 Software Licensing

Base Layers are usually included in most core applications used by an organization. It is important to ensure that the software is suitable for mass distribution and leverages a volume license that does not require any machine-specific identification or individual manual activation.

Certain applications are protected by hardware-based identification methods or a unique license key that resides on the endpoint (for example, in a license file). Such software should not be distributed with the Base Layer or installed on the reference machine. It may still be installed on the endpoint by the end user or via software distribution solutions that target individual endpoints.

Most enterprise software is protected by a floating (volume) license, which eliminates this problem.

12.4.3 User-Specific Software

On the reference machine, install software as an Administrator, and if the option exists, install for “All Users”. User profiles on the reference machine are excluded from the Base Layer and are not distributed. Software installed exclusively for a specific user is not distributed or may not function properly.

Example: Google Chrome’s default installation is to the current user profile. Make sure to install it for “All Users” if it is to be included in the Base Layer.

To ensure that an application shortcut appears on the end user’s desktop or Programs menu, ensure that the shortcut is created after installing the application. If not, manually create a shortcut within the “All Users profile.”

Applications that set up and use local user accounts and/or local groups might not function well on endpoints when the Base Layer is applied to them. Consequently, definitions of local user accounts and local groups are excluded from the Base Layer.

12.4.4 OEM Software

Many hardware vendors include special software to enhance the user experience of their platforms. These applications can support specific hardware buttons, connection management and power management capabilities, and so on.

To include special software as part of the Base Layer, it is important that the Base Layer is only used for compatible hardware. In order to use a single Base Layer for multiple incompatible hardware platforms, do not pre-install hardware-specific software in it. Instead, allow users to install special software manually or use the Post-Base Layer script to implement more complex selection rules.
12.4.5 Endpoint Security Software

Mirage does not distribute software that changes the Master Boot Record (MBR). Full Disk Encryption software usually modifies the MBR; hence this type of software cannot be delivered via a Base Layer. Such software can still be installed on individual endpoints through an external delivery mechanism or during first-time provisioning.

Examples of Disk Encryption software that uses preboot authentication are Checkpoint Full Disk Encryption, PGPDisk, Sophos SafeGuard and McAfee Endpoint Encryption.

Certain security software products take measures to protect their software and do not allow any other processes to modify their files. Software of this type cannot be updated via Mirage. Instead, use the security vendor recommended update process to allow central control and management of that software. Mirage does not interfere or manipulate the operation of these security products, and does not override the security measures they provide.

12.4.6 BitLocker Support

Microsoft BitLocker (in Windows 7) performs full disk encryption and is fully compatible with VMware Mirage. The state of BitLocker is kept and managed on each endpoint and doesn’t not propagate to the Mirage CVD in the datacenter.

The following BitLocker scenarios apply:

- If BitLocker is enabled on the target endpoint, it remains enabled after Mirage restore/Base Layer update/rebase operations, regardless of the BitLocker configuration in original endpoint on which the CVD was running, or on the reference machine from which the Base Layer was captured.

- In a similar manner, if BitLocker is disabled on the target endpoint it remains disabled after Mirage restore/Base Layer update/rebase operations.

IMPORTANT: When building a Windows 7 Base Layer for migration purposes, BitLocker must be disabled on the reference machine or migration operations fail.
Chapter 13

Preparing a Reference Machine

In this Chapter...

13.1 Setting Up a Reference Machine
13.2 Software Considerations
13.3 Settings Captured from Reference Machine

13.1 Setting Up a Reference Machine

A reference machine is used to create a Base Layer for a set of endpoints.

While the reference machine is built and configured, the installed Mirage Client efficiently uploads its content to an assigned Reference CVD. The Reference CVD is then used to capture a Base Layer.

Note: Files and settings from the reference machine are captured in the Base Layer, which is then distributed to a large number of endpoint desktops, therefore extra care should be taken when constructing and modifying the reference machine.

Note: The license file enforces the number of CVDs you can run on your system. Reference CVDs do not take up a license and do not reduce the number of CVDs you are entitled to run.
➢ To assign a pending reference machine:

1. In the Mirage Management Console, select the **Inventory** node, and then select **Pending Devices**. The Mirage Clients awaiting activation (pending) are listed on the right side of the MMC window.

2. Right-click the reference machine to be assigned, and then select **Create a new reference CVD**.

The **Activate Device – Select Upload Policy** window appears.
3. Select the required upload policy, and then click **Next**. The *Activate Device – Select a Base Layer* window appears.

![Base Layer Selection Screen]

4. Select **Don't use a Core Image**. As this is a first-time use, there is no existing Base Layer. In the future, you can select an existing Base Layer to apply updates and modify content.

5. Click **Next**. The *Select Target Volume* window appears. Select to automatically choose a volume or select one manually.

6. Click **Next**. The *Activate Device – Summary* window appears.

7. Click **Finish**. The device is moved from the Pending to the CVDs list.
13.2 Software Considerations

When you capture a Base Layer, the software that is installed on the Reference Machine becomes part of that Base Layer. When you deploy the Base Layer to other endpoints, this software is delivered to the endpoints as well (as part of that Base Layer).

Consider the following before deciding what software to include in your Base Layers:

- Do not include software that is licensed specifically to individual pieces of hardware, or whose licenses are tied to the hardware.
- If there is OEM software on a laptop you will only be able to deploy that Base Layer to endpoints of the same hardware family going forward. This is because OEM software is tied to specific hardware vendors, makes and models.
- Core corporate software is typically the most commonly included software in a Base Layer, which includes (but is not necessarily limited to):
  - Anti-Virus
  - VPN client
  - Microsoft Office
  - Departmental Applications
- Disk encryption software may be installed on the reference machine but it should not be part of the Base Layer. Disk encryption software should always be deployed to the endpoints after the fact.

13.3 Settings Captured from Reference Machine

13.3.1 Settings Captured from the Reference Machine

Various system-wide settings are transferred from the reference machine to all machines that receive the Base Layer. It is therefore important to check which settings are required and configure them accordingly. In special cases, specific exclusion rules can be added to the Base Layer Rules policy (for more information, see 14.2 Editing Base Layer Rules).

Alternatively, many of these settings can be configured using Active Directory Group Policy Objects (GPOs) to ensure more granular control outside of the Base Layer configuration.

The following are examples of various settings included in the reference machine:

- Power Management
- Remote Desktop Settings
- Service Startup Options
13.3.2 Domain Membership and Login Settings

If the target endpoints assigned to the Base Layer are members of a domain, the reference machine used for this Base Layer must also be a member of the same domain. Failing this, users of the target endpoints are prevented from logging on to the domain (only local users are able to log on). In addition, ensure that the Net Logon service is set to start automatically.

13.3.3 Selecting the Captured Data

A Base Layer consists of all of the files in the Reference CVD, excluding a list of files and registry entries specified in the Base Layer Rules policy (constructed by combining the factory policy with user-customized Base Layer Rules).

All data placed on the reference machine is downloaded as part of a Base Layer, and therefore:

- Directories residing directly under the root (C:\) are by default included in the Base Layer. Do not leave directories in the root directory that should not be part of the Base Layer.

- It is not recommended to store unnecessary data that consumes disk space on the endpoints on the reference machine.

- It is important to verify whether the Documents and Settings directory contains abandoned user profile directories. If an old user directory exists under the Documents and Settings directory and no user profile is registered for it in the system, Mirage considers it a regular directory and treats it as part of the Base Layer.

To exclude specific areas of the reference machine from the Base Layer, modify the Base Layer Rules. (For more information, see 14.2 Editing Base Layer Rules.)
Chapter 14

Capturing Base Layers

➢ In this Chapter...

14.1 Editing Base Layer Rules
14.2 Base Layer Override Policy
14.3 Post-Base Layer Scripts
14.4 Capturing Base Layers
14.5 Recreating a Reference Machine from a Base Layer

14.1 Editing Base Layer Rules

Base Layer Rules determine which part of the Base Layer does not get applied to the CVD.

At all times, there is only one set of applicable Base Layer rules. This rule set is defined as the default Base Layer rule set.

➢ To view the Base Layer rules:

1. In the Mirage Management Console, expand the Image Composer node.
2. Click Base Layer Rules. The Base Layer rules are listed in the right pane.
3. Right-click the Base Layer rule you want to view, and then select Properties. The Base Layer rule details are displayed.
4. The Base Layer Rules policy defines which Base Layer files and directories are not applied to the CVD:
   • Include paths: List the Base Layer files and directories that are not applied to the CVD.
   • Exclude paths: List the files and directories that are exceptions to the include list above, that is, are applied to the CVD.

All other files not matching a Base Layer Rule will be applied to the CVD.
5. Click the Show factory rules to view the Mirage mandatory settings that cannot be changed by the IT manager. The factory rules appear grayed out in the rules list.
To edit Base Layer rules:

1. Right-click the default Base Layer rules, then select **Clone**. The **Base Layer Rules** window appears.

2. To add an include path rule, click the **Add** button under the **Include path** section.

3. To add an exclude path rule, click the **Add** button under the **Exclude path** section.

4. Click **OK**. The new Base Layer rules object is now marked as “draft.”

You should test the edited rules on several Base Layers. When you are satisfied with the changes, you can set the new Base Layer rule object as the default rule set.
To test a Base Layer rule object:

1. Right-click the draft Base Layer rule object and select Test Rules Draft.

2. Select the CVD on which you want to test the new Base Layer rules.

3. Click Next.

4. Select the Base Layer you want to use for the test.

5. Click Finish.

To set a draft of Base Layer rules as the default Base Layer rule set:

- Right-click the draft Base Layer rule object and select Set As Default.
14.2 Base Layer Override Policy

14.2.1 Overriding Files

The Mirage policy includes an option to override Base Layer content to persist certain CVD files across Base Layer Updates. This option allows the Base Layer to distribute a file only if it does not exist in the CVD.

Base Layer Override Example 1: Shared Component between CVD and Base Layer applications

1. Microsoft Office and Microsoft Visual Studio have a common shared component. Office is part of the Base Layer but Microsoft Visual Studio is user installed and part of the layer that maintains user-installed applications and machine information.

Microsoft Visual Studio includes a newer version of the shared component that is backwards compatible with Microsoft Office, but the Microsoft Office component version is too outdated for Microsoft Visual Studio.

Without a special override policy, every Base Layer update that occurs after Visual Studio is installed might corrupt the Visual Studio installation.

2. Adding the path of this component to the Do Not Override By Base Layer policy section enforces the following behavior:

   a. If the user first installs Microsoft Visual Studio and then receives Microsoft Office via a Base Layer Update, Mirage recognizes that the file already exists and does not override it, leaving the newer version.

   b. If the user first receives the Base Layer Update, the file does not exist and is downloaded as part of Microsoft Office. If the user installs Microsoft Visual Studio, the newer version of the shared file is installed, and both Microsoft Office and Microsoft Visual Studio function properly.

Base Layer Override Example 2: Initial Provisioning of a Global Configuration File

Lotus Notes has a configuration file that is placed under “Program Files” directory and is shared across all users. The file has to be initially provisioned by the Base Layer to have Lotus Notes function properly. However, it is then modified locally to maintain user configuration.

Without a Base Layer Override policy, each Base Layer Update or Enforce Core Image causes user customizations to be lost. Adding the configuration file path to the Base Layer Override Policy resolves the situation. The Base Layer version of the file is provisioned to users who are receiving Lotus Notes for the first time, but is not delivered to existing Lotus Notes users.
14.2.2 Overriding Registry Values

Similarly, Mirage offers a Base Layer Override policy for Registry Keys and Values. Registry values behave exactly like files in the sense that if a value exists, it is not overwritten, but if it does not exist its content is distributed via the Base Layer.

14.2.3 Overriding Registry Keys

Registry keys have a slightly different behavior. If a registry key path is included in the Do Not Override By Base Layer policy section, and the key exists both in the CVD and in the Base Layer, the key (including its sub-keys and values) is skipped entirely in the Base Layer update.

If the key does not exist in the CVD, it is handled normally and delivered with all its sub-keys and values via the Base Layer.

➤ To add a Do Not Override by Base Layer rule:

1. In the Add Base Layer Rule window scroll to the Do Not Override By Base Layer section.

2. The Do Not Override by Base Layer rules syntax is the same as the Base Layer rules.
14.3 Post-Base Layer Scripts

A Base Layer can include a custom Post-Base Layer script, which allows administrators to automatically perform certain actions after the Base Layer update. Examples of actions that require Post-Base Layer update processing include:

- Installation of software requiring execution on the individual endpoint. This may include hardware-specific software that is only compatible with certain endpoints.
- Update or removal of hardware drivers that may already exist on the endpoint.

This file and any auxiliary files used or called by the script will be captured as part of the Base Layer and distributed to the various endpoints. It is important to ensure that the auxiliary files are placed in the same directory as the script or another directory that is captured in the Base Layer.

In order to create a Post-Base Layer script, create a file named post_core_update.bat under the %ProgramData%\Wanova\Mirage Service directory. The file must be edited on the reference machine.

**IMPORTANT:** The client continues to execute the Post-Base Layer script upon every boot until the first Mirage upload following the Base Layer update is complete. This is done to ensure that the state of the CVD on the server includes the result of the Post-Base Layer script, and also occurs for every enforced Base Layer operation. The script must include the relevant checks and conditional clauses to ensure that the parts that require one-time execution are not run again.

**Note:** The Mirage Client installation includes a default sample script that does not perform any Post-Base Layer script actions.

To monitor the execution of the Post-Base Layer script, Mirage Client reports events to the Mirage central management service if the script returns an error value other than 0.
14.4 Capturing Base Layers

After the reference machine has been centralized into a Reference CVD on the Mirage Server, you can capture a new Base Layer from that Reference CVD.

➢ To capture a Base Layer:

1. In the Mirage Management Console, select **Common Wizards**, then **Capture Layer**.

2. Select whether you want to capture a Base Layer from an existing Reference CVD or from a new one.

➢ To capture a Base Layer using an existing Reference CVD:

1. Select the Reference CVD from which you want to capture the Base Layer.
2. Specify the new Base Layer details, or select the Base Layer to update and click **Next**.
3. A validation window appears which checks the Reference Machine for possible problems. If there are problems reported, you can fix them and then click the Refresh button to see if they are resolved. The following parameters are checked during the validation (below):

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Mirage checks to make sure that the CVD and the new Base Layer have the same operating system (XP or Windows 7) and type (32- or 64-bit). If they are different, Mirage blocks those CVDs from receiving the Base Layer.</td>
</tr>
<tr>
<td>Computer Type</td>
<td>Mirage checks if the CVDs and the Base Layer share the same computer type (for example, laptop vs. desktop). If they are different, the administrator is warned. If the Base Layer was prepared to support both desktops and laptops, the administrator can approve and continue.</td>
</tr>
<tr>
<td>Vendor and Model Name</td>
<td>Mirage checks to see whether the Base Layer and the CVDs are from the same computer vendor. If they are different, the administrator is warned. If the Base Layer was prepared to support the different vendor types, the administrator can approve and continue.</td>
</tr>
<tr>
<td>Drive Letters</td>
<td>Mirage checks whether the CVDs have the required drive letter included in the Base Layer. If the CVDs do not have the appropriate drive letters, Mirage blocks these CVDs from receiving the Base Layer.</td>
</tr>
</tbody>
</table>

4. Once they are resolved, click Next.

5. If Microsoft Office 2010 is installed, a window prompts you to specify the Office license files. Define your licenses and click Next.

6. Click Finish to start the capture process.

   A message is displayed asking if you want to switch to the task list view.

7. Click Yes. The console view changes to the Task list, where you can monitor the progress of the capture task.

   When the task is complete, the Base Layer is moved to the Base Layers list under the Image Composer node.
To capture a Base Layer using a New Reference CVD:

1. Choose Create a new reference CVD.
2. Select the pending device you want to use.
   The wizard displays the properties of the selected pending device.
3. Select the upload policy you want to use for this Reference CVD.
4. Select whether you want to use a Base Layer for the new Reference CVD or not.
5. Specify the new Layer details, or select an existing Layer you wish to update.

6. A validation window appears which checks the Reference Machine for possible problems. If there are problems reported, you can fix them and then click the Refresh button to see if they are resolved. The following parameters are checked during the validation (below):

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Mirage checks to make sure that the CVD and the new Base Layer have the same operating system (XP or Windows 7) and type (32- or 64-bit). If they are different, Mirage blocks those CVDs from receiving the Base Layer.</td>
</tr>
<tr>
<td>Computer Type</td>
<td>Mirage checks if the CVDs and the Base Layer share the same computer type (for example, laptop vs. desktop). If they are different, the administrator is warned. If the Base Layer was prepared to support both desktops and laptops, the administrator can approve and continue.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Details</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vendor and Model Name</td>
<td>Mirage checks to see whether the Base Layer and the CVDs are from the same computer vendor. If they are different, the administrator is warned. If the Base Layer was prepared to support the different vendor types, the administrator can approve and continue.</td>
</tr>
<tr>
<td>Drive Letters</td>
<td>Mirage checks whether the CVDs have the required drive letter included in the Base Layer. If the CVDs do not have the appropriate drive letters, Mirage blocks these CVDs from receiving the Base Layer.</td>
</tr>
</tbody>
</table>

7. Once they are resolved, click **Next**.

8. If Microsoft Office 2010 is installed, a window prompts you to specify the Office license files. Define your licenses and click **Next**.

9. A message is displayed asking if you want to switch to the task list view. If you want to follow the capture task, click **Yes**. The console view changes to the Task list, where you can monitor the progress of the capture task.

10. When the task is complete, the Base Layer is moved to the **Base Layers** list under the **Image Composer** node.

### 14.5 Recreating a Reference Machine from a Base Layer

When you want to update an existing Base Layer but the Reference Machine that was used to create the original Base Layer is not available, you can recreate the original Reference Machine from the existing Base Layer.

The image of the previous Reference Machine is downloaded and applied to the selected device.

On the new reference machine, you can update or install applications and apply security updates before capturing a new Base Layer using the existing Reference CVD. For more information about capturing a Base Layer, see **14.4 Capturing Base Layers**.

➢ **To recreate a Reference Machine from an existing Base Layer:**

1. From the **Image Composer > Base Layers tab**, right-click the Base Layer and select **Create Reference CVD from layer** from the popup menu.

2. Select the Pending device.

3. Select the desired Upload policy.

4. Click **Finish**. This starts a Mirage Restore operation. At the end of the restore, the device is updated with the contents of the previous Reference Machine.
Chapter 15
 Assigning Base Layers

In this Chapter...

15.1 Introduction
15.2 Comparison Report between Base Layer and CVD
15.3 Testing the Base Layer before Rollout
15.4 Assigning Layers
15.5 Base Layer Provisioning
15.6 Monitoring Layer Assignments
15.7 Dealing with Conflicts
15.8 Updating a Base Layer Assigned to a CVD
15.9 Enforcing a Base Layer

15.1 Introduction

Assigning a Base Layer to an endpoint (or collection of endpoints) takes the contents of the Base Layer and applies it to the designated endpoint(s). This means that any applications or updates/patches built into the Base Layer will, after assignment, also reside on the endpoint device.

Important Note: If you upgraded a 2.0 Mirage system to 3.1 or later and had existing Base Layers (formerly referred to as ‘Base Images’), it is highly recommended that you capture new Base Layers (from the same Reference Machine, if preferred) to apply to your endpoints.

15.2 Comparison Report between Base Layer and CVD

Before applying a new Base Layer version to a CVD or collection of CVDs, you can run a report to compare the content of the Base Layer and the CVD.

This report can help you plan the Base Layer update process, and resolve in advance conflicts that might result from any mismatch between the CVD and the Base Layer content.

The report is in HTML format and you can use Excel to easily view it and filter data. See 15.2.1 Comparison Report Format for details about the report.
To run a comparison report between a collection of CVDs and a Base Layer:

1. In the Mirage Management Console, right-click a collection and select Programs > Compare Programs with Layer.

The Compare program files with layer window appears.

2. Select the Layer to compare with the collection, and then click OK. The HTML report is generated and opened in your default web browser.

To run a comparison report between a specific CVD and a Base Layer:

1. Right-click the desired CVD, and then select Programs > Compare Programs with Layer.

2. Select the Base Layer to compare with the collection, and then click OK. The HTML report is generated and opened in your default web browser.

To run a comparison report between two Base Layers:

1. Right-click the first Base Layer, and then select Programs > Compare Programs with Layer. The Compare program files with layer window appears.

2. Select the second Base Layer to compare, and then click OK.

The HTML report is generated and opened in your default web browser.

15.2.1 Comparison Report Format

The comparison report includes all the programs that are installed either on the Base Layer or on the CVDs, in the following format:

- **Remove Programs table**: Lists all programs that will be removed from the endpoint device when the Base Layer is deployed.

- **Update Programs table**: Lists all programs that will be either installed or upgraded on the endpoint device when the Base Layer is deployed.
The following headings are listed in the reports:

- **Product**: The name of the product installed.
- **CVD**: the number of CVDs affected by this operation - removed, installed, or upgraded.
- **Action**: The type of action taken when the Base Layer is applied.
  - **Remove**: The product is removed from the endpoint device.
  - **Install**: The product is installed on the endpoint device.
  - **Upgrade**: The product is upgraded to a new version.
  - **Major Upgrade**: The product is upgraded to a new version that is different than the current version (a difference in the Major revision number).
  - **Downgrade**: The product is downgraded to a new version.
  - **Major Downgrade**: The product is downgraded to a new version that is different than the current version (a difference in the Major revision number).
- **Version**: The version of the product.
- **Current Base Layer**: The current Base Layer assigned to the CVD.
- **Publisher**: The program publisher.
- **Install Location**: The product installation path.

### 15.3 Testing the Base Layer before Rollout

Since Base Layer updates include OS and other critical component updates, it is important to test a new Base Layer before distributing it to endpoints. After capturing a Base Layer, select a sample group of endpoints and distribute the Base Layer to them to ensure that there are no issues.

If the Base Layer is used with multiple hardware platforms, test one sample per platform. It is also recommended to have typical user-installed applications available in the selected samples to test the overall update results.

### 15.4 Assigning Layers

The Base Layer Rules policy is used during first-time deployment to identify the parts of the endpoint to be managed by the Base Layer, and the parts to be left unmanaged at the endpoint. In an initial rollout, there is no previous Base Layer to compare against; therefore Mirage does not remove any existing software from the endpoints prior to applying the Base Layer.
15.5 Base Layer Provisioning

Base Layer Provisioning can be initiated for a device that is Pending Assignment is a new device in an organization in which VMware Mirage is already implemented.

After the Mirage Client is installed, the Pending Devices panel shows the new device as pending assignment, in the same way as when Centralize Endpoint applies (see 4.4.1 Centralizing an Endpoint).

To prepare the new device to be part of the organization, the Base Layer Provisioning process first cleans up the device files and applies an existing Base Layer as a common template. The device is then freshly-imaged, assigned to and synchronized with a newly created CVD.

Tips:

- The end user is free to use the desktop as usual once the Centralization processing associated with the Provisioning operation starts. This includes offline work and network transitions. The Mirage Client monitors user activities and adjusts its operation to optimize the user experience and performance.

- After the Server synchronization is completed, the Transaction log shows a successful endpoint centralization or provisioning entry. The desktop is protected and can be managed centrally at the data center.

➢ To assign a pending device using Base Layer Provisioning:

This procedure describes Base Layer Provisioning initiated from the Common Wizards node Base Layer Provisioning option. You can also initiate Base Layer Provisioning from the Pending Devices or Layer Assignments windows, by selecting a device, right-clicking and selecting Base Layer Provisioning from the shortcut menu. The Base Layer Provisioning wizard will open at the Select Layer step (see below).

1. In the Mirage Management Console, select the Common Wizards node.

   - Console Root
   - VMware Mirage
     - Mirage System (localhost)
       - Common Wizards
       - Dashboard
       - Task Monitoring

2. Then select Base Layer Provisioning.
3. The **Select Layer** window appears. Select the layer that you want to provision with.

![Select Layer window](image)

4. The **Select Pending Device** window appears. Select the device or devices you want to assign.

![Select Pending Device window](image)
5. The **Select Upload Policy** window appears. Select the upload policy you want to use and click **Next**. If you do not make a selection, a default policy will apply, as specified in the security settings - see Default Upload Policy in 7.3.1 General Tab.

6. The **Target Machine Name** window appears. Select the device name and set the domain.
7. The *Image Validation* window appears. Click **Next**.

8. The *Summary* window appears.

9. Click **Finish**.

The Base Layer Provisioning process starts, including device file cleanup, downloading the Base Layer, and subsequent centralization upload processes.

**Monitoring the Provisioning Progress**

Since Base Layer Provisioning includes assigning a Base Layer, the Base Layer Provisioning progress can be monitored as described in 15.6 Monitoring Layer Assignments.

When the initialization process is complete, the device starts Base Layer download and then performs a boot operation and applies the Base Layer image.

After the boot operation and image application are completed, Server synchronization starts. The system tray icon on the Client shows the progress of the upload.

The console also shows the upload progress in the **Upload** field of the CVD inventory list.

The end user can also click the **Mirage** icon in the system tray to view the detailed status of the upload operation.

After the wizard operation completes, the device appears in the *All CVDs* panel.
15.6 Monitoring Layer Assignments

An administrator can always see what endpoints have certain layers assigned to them. The following use cases show several ways to review and monitor currently running assignments.

➢ To monitor layer assignments in the Layer Assignments window:

- Progress of a Base Layer Provisioning download to a specific device:
  - Right-click on a CVD, and select Core Image > View assignments.

- Progress or status of a specific layer:
  - Go to a specific layer, right-click the layer, and select View assignments.

- All your current Layer Assignments:
  - Expand the Image Composer > Layer Assignments node.

- Progress of a layer assignment task, for example, you sent a layer to 100 CVDs:
  - Right-click the task in Task Monitoring and select View assignments.

The Layer Assignments window, referred to in the above use cases, shows the status of Base Layer propagation to devices.

![Layer Assignments Window](image1)

You can also monitor Layer Assignment progress through the Task Monitoring window, which shows overall status as well as the task progress.

![Task Monitoring Window](image2)
15.7 Dealing with Conflicts

Before applying a Base Layer, ensure that software to be deployed by the Base Layer does not conflict with locally installed software (for example, the Base Layer contains an anti-virus product that is different from that on an endpoint).

Conflicting software can either be removed locally on the endpoint or coordinated remotely through GPOs, login scripts, or other software distribution tools.

Alternatively, an ad-hoc cleanup procedure can be performed using a transition Base Layer concept. A problematic endpoint can be used as a reference machine to capture a Base Layer with the conflicting software. This Base Layer is then applied to the endpoint and others alike and acts as a temporary Base Layer for the purpose of a clean transition. The transition Base Layer is then replaced by applying the Base Layer of choice, resulting in replacement of conflicting software.

The initial rollout flow with a transition Base Layer is as follows:

a. Any application that is included in the transition Base Layer becomes a managed application when the transition Base Layer is assigned.

b. Managed applications undergo an update or removal process upon subsequent Base Layer update operations.

c. New Base Layers are constructed and endpoints are updated with the new Base Layer.

15.8 Updating a Base Layer Assigned to a CVD

After a Base Layer is updated at the Server and tested on at least one CVD, you can assign it to multiple CVDs. If Collections are defined (see 4.6 Working with CVD Collections), you can assign the new Base Layer to all the CVDs in a collection in one step. Alternatively, you can assign it to individual CVDs.

When the updated Base Layer is downloaded to the endpoint, only new files and relative changes to existing files of the target endpoint are transferred. This speeds up the download process considerably. When the download is completed, a reboot message is displayed on an endpoint machine. After the reboot, the updated Base Layer takes effect.

Before a new or updated Base Layer is applied, the Mirage Server automatically takes a CVD snapshot to allow roll-back in case of post-update issues.

Note: Before and during Base Layer download, Mirage ensures that enough disk space is available to proceed with the operation.
To assign or update a Base Layer to a CVD:

1. In the Mirage Management Console, select **Common Wizards**, and then click **Assign Base Layer**.

The **Assign Base Layer Wizard** appears.

2. Choose the Base Layer with which you want to update the CVDs. You can see the Base Layer details in the bottom pane.

3. Choose the CVDs you want to update. You can either choose individual CVDs, or choose a collection by clicking the Collections tab.

4. Select the CVDs you want to update, and then click **Select**.

The validation page appears. The characteristics below are checked, and warnings may be presented in case of a possible mismatch between the Base Layer and the selected CVDs. You may choose to ignore warnings if not applicable, and continue with the Base Layer update.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Mirage checks to make sure that the CVD and the new Base Layer have the same operating system (XP or Windows 7) and type (32- or 64-bit). If they are different, Mirage blocks those CVDs from receiving the Base Layer.</td>
</tr>
<tr>
<td>Computer Type</td>
<td>Mirage checks if the CVDs and the Base Layer share the same computer type (for example, laptop vs. desktop). If they are different, the administrator is warned. If the Base Layer was prepared to support both desktops and laptops, the administrator can approve and continue.</td>
</tr>
<tr>
<td>Vendor and Model Name</td>
<td>Mirage checks to see whether the Base Layer and the CVDs are from the same computer vendor. If they are different, the administrator is warned. If the Base Layer was prepared to support the different vendor types, the administrator can approve and continue.</td>
</tr>
<tr>
<td>Drive Letters</td>
<td>Mirage checks whether the CVDs have the required drive letter included in the Base Layer. If the CVDs do not have the appropriate drive letters, Mirage blocks these CVDs from receiving the Base Layer.</td>
</tr>
</tbody>
</table>

5. **Click Finish**. An update task is created. The Mirage Client, as part of its regular processing, periodically checks the Server for updates to download.
To cancel a Base Layer update in progress:

- Right-click the CVD or collection for which you want to cancel the Base Layer update. Under the Base Layer menu item, select Cancel Pending Base Layer.

**Note:** It is recommended that you assign a Base Layer to a CVD only after endpoint centralization is complete for that CVD, and its content is protected in the Server. This enables you to revert back to the prior CVD state in case of a problem.

### 15.8.1 Monitoring a Base Layer Update

After a Base Layer has been assigned to a number of CVDs, the IT manager can monitor the update process through the Base Layer deployment view.

The Base Layer deployment view displays the current status of the Base Layer deployment progress. Progress states include:

- **Pending:** The Base Layer was assigned to the CVD, but has not begun downloading to the endpoint.
- **Throttled:** The endpoint tried to download the Base Layer from the Mirage Server and was rejected due to server resource throttling.
- **Downloading:** The endpoint is downloading the Base Layer.
- **Committing:** The Base Layer was downloaded and installed successfully by the endpoint; the Client is now updating the CVD with the new content.
- **Blocked:** The Base Layer was blocked, and wasn’t downloaded to the endpoint.
- **Canceled:** The Base Layer download process was canceled by the administrator.
- **Rejected:** The Base Layer was downloaded to the endpoint and failed the validation check on the endpoint.
- **Done:** The Base Layer update operation was completed.

To view Base Layer update progress:

1. In the *Mirage Management Console*, select the Tasks node, right-click the specific Assign Base Layer task, and select View assignments.
2. The specific Base Layer update assignment delivery view is opened.

To view a Base Layer update progress:

- In the *Mirage Management Console*, choose the Image Composer node, then right-click the Base Layer you want to view and select View assignments.
15.9 Enforcing a Base Layer

End users and applications may make changes to files and registry settings that were provisioned through a Base Layer. At times, these changes create problems with the desktop operation.

In most cases, it is easy to resolve the issue by enforcing the Base Layer originally assigned to the CVD. The Mirage Client downloads only the relevant files and registry settings required to realign the CVD with the original Base Layer. User profiles, documents, and installed applications that do not conflict with the Base Layer content are preserved.

Additionally, enforcing a Base Layer can remove any user-installed applications residing on the machine area of the CVD. This can be useful, for example, for fixing a problematic CVD in which Base Layer applications no longer function because of overwritten or corrupted system files. Removing user applications deletes any machine area files and registry keys that are not in the current Base Layer, excluding files that are defined in the user area policy.

➢ To enforce a Base Layer on an endpoint:

1. From the Inventory > All CVDs tab, right-click the relevant CVD and select Enforce Core Image. The Enforce Core Image window appears.

   ![Enforce Core Image](image)

   Please select one of the following methods:
   - Preserve user applications
   - Remove user applications

2. Select Preserve user applications to keep the user-installed applications on the CVD or select Remove user applications to delete user-installed applications from the CVD.

3. Click OK.
PART 6 - DESKTOP OPERATIONS

➣ In this Part...

16. Endpoint Disaster Recovery
   16.1 Recovering from a Disaster
   16.2 Restoring CVD Snapshots
   16.3 Restoring a CVD Using the Disaster Recovery Wizard
   16.4 Mirage Boot USB Keys
   16.6 User Experience with Restore Processes

17. Hardware Migrations
   17.1 Using the Hardware Migration Wizard
   17.2 Planning for a Mass Hardware Migration
   17.3 Performing a Mass Hardware Migration

18. Windows XP to Windows 7 Migration
   18.1 Planning for a Windows XP to Windows 7 in-place Migration
   18.2 Setting Up a Windows 7 Base Layer for Migration
   18.3 XP to Windows 7 Migration
   18.4 Migration to Windows 7 Replacement Devices
   18.6 End User Experience During a Migration
Chapter 16

Endpoint Disaster Recovery

In this Chapter...

16.1 Recovering from a Disaster
16.2 Restoring CVD Snapshots
16.3 Restoring a CVD Using the Disaster Recovery Wizard
16.4 Mirage Boot USB Keys
16.6 User Experience with Restore Processes

16.1 Recovering from a Disaster

Mirage has two key ways to provide disaster recovery:

- Restore a device to a previous CVD Snapshot.
- Using the Disaster Recovery Wizard
  - Restore the CVD after a hard-drive replacement, file corruption, or format, that is, restore a CVD to the same device.
  - Restore the CVD to a replacement device.

The restore is based on files and directories included in CVD snapshots, in accordance with the Upload policies currently in effect – see 4.5 Working with Upload Policies. When the CVD contains Encrypted File System (EFS) files, the files are recovered in their original encrypted form.

Note: If the CVD contains EFS files, it is highly recommended that the user be logged in during the restore Prefetch operation for better de-duplication in the revert to snapshot.
16.2 Restoring CVD Snapshots

A snapshot is a centrally retained point-in-time image of CVD content, including OS, applications and user data. The CVD snapshot is a read-only view that enables complete restore of a specific endpoint as well as for a specific file.

A new CVD snapshot is automatically created by the Mirage Server every 24 hours following at least one successful CVD upload. In addition, the Mirage Server automatically creates a snapshot in the following cases:

- **Before a Base Layer update.** If the update fails or the update is problematic, or after any migration, an authorized Mirage management user can revert to the CVD state prior to the update.
- **Before reverting to a snapshot.** This ensures that the current endpoint state is kept in case a roll-back is required.

Mirage preserves CVD snapshots based on a retention policy. By default, snapshot retention is set to provide 7 daily snapshots then keep 3 weekly snapshots, and 11 monthly snapshots. The retention of Hourly snapshots can also be defined. You can modify the retention policy in the System Configuration options of the Mirage server – see Snapshots parameters in 7.3.1 General Tab.

**Note:** Automatic snapshots taken before a Base Layer update and before reverting to a snapshot, or force uploads are counted against the daily snapshot capacity. This signifies that the automatic snapshot causes the number of regular daily snapshots to decrease.

Different procedures apply if the reversion is between same or different operating systems:

- For Win7 to Win7 or XP to XP reversions, see the procedure below.
- For Win7 to XP or XP to Win7 reversions, see To restore a CVD to a previous snapshot of a different OS on page 166.

➢ To restore a CVD to a previous snapshot of the same OS:

1. In the Mirage Management Console tree, expand the Inventory node and select the All CVDs node. Right-click the CVD to which you want to restore and click Revert to Snapshot.
2. The *Revert CVD* window appears.

![Revert CVD Window]

- Select the snapshot date to which you want to revert.
- The *Restore System Only* check box (selected by default) restores system files only, including the Base Layer, user-installed applications and machine settings. This option does not affect current User area content and does not erase any new files in the user area. (See User area description in 4.5 Working with Upload Policies.)
  Clear the *Restore System Only* check box if you want to restore the entire CVD, including the User area, from the CVD snapshot. Any application, setting, or document in the current CVD that does not exist in the snapshot will be erased from the endpoint.
- Click *Next*. 
3. The Revert CVD window appears. This makes sure that there are no conflicts with your CVD Snapshot Restore. Click Next.

4. The Summary window appears. Click Next.

➢ To restore a CVD to a previous snapshot of a different OS:

1. In the Mirage Management Console tree, expand the Inventory node and select the All CVDs node. Right-click the CVD to which you want to restore and click Revert to Snapshot.

2. The Revert CVD window appears.

   a. Select the snapshot date to which you want to revert.

   b. Ensure that the Restore System Only check box is cleared, so that the entire CVD will be restored, including the User area, from the CVD snapshot. (See User area description in 4.5 Working with Upload Policies.) Any application, setting, or document in the current CVD that does not exist in the snapshot will be erased from the endpoint.

   c. Click Next.
3. The *Target Machine Name* wizard page appears showing Domain Options. Fill in the domain details in order for the device to rejoin the domain. Click **Next**.

![Domain Details](image1)

**Tip:** Choose the Domain and OU by either selecting from the dropdown lists or typing. The dropdown lists are pre-populated with all known domains in the system. The required syntax pattern is shown for each entry field.

4. The *Validation Summary* window appears. This makes sure that there are no conflicts with your CVD Snapshot Restore. Click **Next**.

![Validation Summary](image2)

5. The *Summary* window appears. Click **Finish**.

![Summary](image3)
16.3 Restoring a CVD Using the Disaster Recovery Wizard

If the hard drive on an endpoint is replaced or the user machine was lost and a new machine was supplied, you will need to restore the CVD to the device. The device must be set up with at least a basic operating system image and must comply with the Mirage software prerequisites listed in 2.2 Software Prerequisites.

It is not necessary to specifically identify the endpoint and locate the CVD in the console. The Server automatically recognizes the endpoint’s GUID in the device BIOS and finds the associated CVD.

**Note:** The IT manger can also use the To restoring a CVD to a replacement device procedure to migrate users from Windows XP or Windows 7 machines to new Windows 7 machines. For this purpose, in the Restore Options selection in the procedure, select Only Restore User Data and Settings. See 18.4 Migration to Windows 7 Replacement for more information.

There are two procedures:

- **To restore a CVD after hard-drive replacement**, file corruption or format, below.
- **To restoring a CVD to a replacement device**, on page 170.

➢ To restore a CVD after hard-drive replacement, file corruption or format:

1. Install the Mirage Client on the Client machine as described in 4.1 Activation Overview.

2. In the Mirage Management Console, select Common Wizards, and select Disaster Recovery.

3. The Select Action window appears. Select Restore CVD after hard-drive replacement, file corruption, or format and click OK.
Restoring a CVD Using the Disaster Recovery Wizard

4. The Device Selection window appears. Select the device you would like to proceed with for the restore operation. Only devices that are recognized as connected to CVDs and are pending restore are listed.

![Device Selection Window]

5. The Restore Options and Validation window appears. This makes sure that there are no conflicts with your CVD Snapshot Restore.

![Restore Options and Validation Window]

   a. The Restore System Only check box (selected by default) restores system files only, including the Base Layer, user-installed applications and machine settings. This option does not affect current user area content and does not erase any new files in the user area. (See User area description in 4.5 Working with Upload Policies.)

   Clear the Restore System Only check box if you want to restore the entire CVD, including the user area, from the CVD snapshot. Any application, setting, or document in the current CVD that does not exist in the snapshot will be erased from the endpoint.

   b. Click Next.

6. The Summary window appears. Click Finish.

![Summary Window]
To restoring a CVD to a replacement device:

1. Install the Mirage Client on the Client machine as described in 4.1 Activation Overview.

2. In the Mirage Management Console, select Common Wizards, and select Disaster Recovery.

3. In the Select Action window, select Restore CVD to a replacement device and click OK.

4. The Select a Target Drive window appears. Select the device you would like to restore the CVD to. Only devices to which the CVD can be restored to are listed.
5. The *Restore Options* area appears.

Select one of the following restore options for the selected CVD and Device:

- **Full System Restore (Operating System, Applications, User Data and Settings)**. The entire CVD (Operating System, applications, and user files) is restored to the replacement device. Any existing files on the replacement device will be lost or overwritten!

  **Note**: This option is recommended for systems with Windows volume licenses or Windows OEM SLP licenses.

- **Restore Applications, User Data and Settings**. Only applications and user data are restored to the replacement device. The existing Operating System and applications installed on the replacement device are retained. The Operating System of the replacement device must be the same as that of the CVD.

  **Note**: This option should be used when replacing a device that has a different Windows OEM license.

- **Only Restore User Data and Settings**. Only user data and settings are restored to the replacement device. The existing Operating System and applications installed on the replacement device are retained. The Operating System of the replacement device may be the same as or newer than that of the CVD.

  **Note**: This option should be used if you want to migrate users from Windows XP or Windows 7 machines to new Windows 7 machines.
Additional Notes:

- User Data in these options pertains to files and directories listed in the upload policies User area. See the User area description in 4.5 Working with Upload Policies.

- If you migrate a CVD from a Windows XP device to a replacement device that has Windows 7, you are only allowed to select the Full System Migration option or the Only Restore User Data and Settings option. This is because Mirage does not transfer user-installed applications from a Windows XP to a Windows 7 system (because Mirage cannot guarantee cross-Operating System compatibility).

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

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

6. If you selected the Full System Restore option, the Select a Base Layer window appears. (Not relevant for other options.)

Select the Base Layer (optional).
You can maintain the current Base Layer (if one applies), or select a new Base Layer from the list, or proceed without a Base Layer.
7. The Target Machine Name window appears. You can change (or define) the hostname for a device that is undergoing the restore operation.

You can also select a domain for this endpoint to join after the restore operation. The current domain is shown by default.

Tip: Choose the Domain and OU by either selecting from the dropdown lists or typing. The dropdown lists are pre-populated with all known domains in the system. The required syntax pattern is shown for each entry field.

a. Any OU defined here should be in standard open LDAP format (For example, OU=Notebooks, OU=Hardware, DC=VMware, DC=com).

b. The join domain account must meet the appropriate security privilege details (as detailed in 7.3.1 General Tab).

Note: The account must have access to join the domain. This is not validated. To use the same credentials each time, perform the following:

a. In the Mirage Management Console tree, right-click System Configuration and select Settings. The System Configuration window appears.

b. Select the General tab and then enter the credentials you want to use for domain joining.

c. Click Next.
8. The Validations window appears. Use the Validation Details to compare the target device with the CVD. This summary alerts you to any potential issues that require additional attention. You may not be able to proceed until blocking issues are resolved. Click Next.


10. The migration process proceeds and takes place in two phases (as described in 16.6 User Experience with Restore Processes).
16.4 Mirage Boot USB Keys

16.4.1 Overview

To help assist customers with recovery operations and system imaging VMware has developed a way to create bootable USB media. Once created, VMware’s Boot USB contains a clean install of Windows 7 (Professional or Enterprise Edition). The VMware Mirage client is installed and is pre-configured to connect to your VMware Mirage Server when the machine boots. The VMware Boot USB Key can be customized to accommodate a variety of different hardware platforms and additional pre- and post-Windows installation actions (which may include joining the new system to the desired domain, renaming the system, and so on). The most common usage scenarios are as follows:

- Restoring a device which can no longer boot into Windows.
- Restoring or reimagining a remote device out in the field.
- Provisioning/Imaging a fresh Windows installation on an existing machine quickly.

Deploying the Windows image with the VMware Boot USB Key takes between 15 to 30 minutes (on average).

16.4.2 Prerequisites

The following prerequisites are required:

- A Windows 7 (Professional or Enterprise Edition) machine.
  \textbf{Note:} This is represented as Drive C throughout this guide.
- The VMware Boot USB Scripts (provided by VMware).
- A Windows 7 (Professional or Enterprise Edition) DVD or ISO file.
  \textbf{Note:} This is represented as Drive D throughout this guide.
- An 8 Gigabyte USB Drive
  \textbf{Note:} This is represented as Drive U throughout this guide.
- A Mirage Client MSI installer file (x86 or x64 version).
  \textbf{Note:} This file is renamed later in this guide.
16.4.3 Creating the VMware Boot USB Key

IMPORTANT NOTES:

- To create the bootable USB disk, drive letter "U" must be available (the creation scripts currently do not warn you if it is already in use).
- **The entire USB drive that you use is formatted during this process!**

To create the VMware Boot USB key:

1. Create the following folder on your workstation: C:\BootUSB.
2. Extract the VMware Boot USB Scripts from the BootUSB.zip file (obtained from VMware) into the root of the C:\BootUSB folder. Do not modify the file structure or add sub-directories.
3. Open the C:\BootUSB\MirageClient folder. There are two Mirage clients in the folder, a 32-bit client and a 64-bit client.
   - If you are building this key for a 64-bit installation of Windows 7, rename the MirageClient.x64.34651.msi file to MirageClient.msi.
   - If you are building this key for a 32-bit installation of Windows 7, rename the MirageClient.x86.34651.msi file to MirageClient.msi.
4. Find any hardware drivers you need for the new hardware and copy them into the C:\BootUSB\Drivers folder.
5. Insert the Windows 7 Pro DVD into your DVD Drive. Alternatively, you can mount your Windows 7 ISO file (this speeds up boot USB key creation).
6. Insert the USB Key and wait until Plug and Play detection completes.
7. Run a Command Prompt window as an administrator and type `cd C:\BootUSB` and press <Enter>.
8. Type `win7usb.cmd` and press <Enter>. A list of the available disks and their disk number are displayed. Look for the disk number of your USB drive (which you can identify by the size value):

![Command Prompt window showing USB disks and their sizes](image-url)
9. Run the complete command as follows:
   \texttt{win7usb.cmd [win7 dvd path] [msi path] [server ip] [usb disk number]}
   
a. [\texttt{win7 dvd path}] is the path to the Windows 7 DVD or ISO file.

b. [\texttt{msi path}] is the path of a Mirage client msi path.

c. [\texttt{server ip}] is the IP address for your Mirage server which any client devices connect to.

d. [\texttt{SSL}] is whether or not this client connects using SSL (Use true or false).
   
   \textbf{Note:} the Mirage Server must already be configured for SSL for this to be turned on!

e. [\texttt{usb disk number}] is the number of the USB disk to format a list of connected disk numbers will be displayed upon invocation.

Each customer’s exact string is different. For example, this is a typical string assuming that the Windows 7 DVD is in the D: drive, the Mirage client has been renamed (step 3), the IP of the Mirage server is 192.168.11.203, SSL is turned off, and the USB Key is listed as disk #2:
\begin{verbatim}
C:\BootUSB>win7usb.cmd D:\
C:\BootUSB\MirageClient\MirageClient.msi 192.168.11.203 false 2
\end{verbatim}

10. The USB disk is prepared. When the USB key creation is complete you can customize it in additional ways (for example, have it automatically install additional software, or embed hardware drivers, and so on). For more information about customizing your USB Key, see the appendices at the end of this guide.
16.4.4 Using the VMware Boot USB Key

Note: Do not unplug the USB disk until this process is fully completed and you have Windows and Mirage installed on your Windows 7 system.

➢ To use the VMware Boot USB Key

1. Perform a one-time boot from the USB disk by choosing the correct option in the startup menu. For example, most Dell laptops use the F12 key. Windows 7 begins loading (the process is very similar to a clean install of Windows 7).

2. Select the version of Windows that you wish to install (must select a Professional or better edition).

3. Install Windows (prompts may vary based on which version of Windows you are installing and what Windows installations (if any) currently exist on the endpoint).
   a. If you are prompted to select a version of Windows, you must select a Professional edition (Mirage does not support Home editions).
   b. If you are prompted with an option to choose between an upgrade and custom (advanced), select the Custom (advanced) option.
   c. When you select a partition to install the new copy of Windows onto, it is up to you if you want to format that partition or not.

   Note: VMware software does not modify any existing partition tables.

   d. As Windows installs, the target machine reboots several times to complete the Windows install. This is normal.

4. Once the installation is complete you are prompted to login. Use the following login information:
   - The default user is TEST and the password is: password
   - The default administrator password is: passwd1!

   Note: You can change these passwords by editing the account values in the autounattend.xml file found on the USB Key.

5. Once you login for the first time, the target machine may install the PnP (Plug and Play) Drivers. It may require an additional reboot after this process completes and this reboot should happen automatically.
16.4.5 Customizing your Boot USB Key

Once the Boot USB has been created you can customize and configure it to suit your site or location. There are a number of files on the Boot USB Key that you can use to modify without having to rebuild your Boot USB Key in the process. These files are all found on the root of the built USB Key (unless specified otherwise).

1. **InstallClient.cmd**. This file controls the command that runs the Mirage installer. You can modify the commands here, including the server Mirage connects to, using SSL or not, and any MSI switches you wish to use during installation.

2. **SetupComplete.cmd**. This batch file is invoked automatically when Windows 7 deployment is completed. You can add additional commands to this file as needed (install VPN client, for example). The file is located in:
   ```plaintext
   USB_ROOT\sources\$oem$\$\setup\scripts\SetupComplete.cmd
   ```

3. **MirageClient.msi**. The Mirage client that is installed on the new Windows 7 machine. You can change which Mirage Client is on your Boot USB Key. Remember to rename it to **MirageClient.msi** when you copy it to the root of the created Boot USB Key.

4. **Autounattend.xml**. An answer file for the unattended Windows 7 installation that you can edit to customize the deployed Windows 7 installation.

16.4.6 Adding Drivers to your existing VMware Boot USB Key

It may be necessary to add additional drivers to the VMware Boot USB Key depending on what hardware you’ll be using. To do this, you do not need to rebuild your entire VMware Boot USB Key. You only need to locate the Drivers folder on the USB Key and copy any new drivers into that directory. The next time you use the USB Key on a replacement system all the drivers in this folder are copied over to the device and used for potential plug and play driver installations.

16.4.7 Known Limitations

- The Windows 7 installation is not activated and does not include a product key. Windows 7 allows working with a non-activated machine for a few days. This limitation can be worked around by editing the **autounattend.xml** file.

- It is known that some antivirus products (for example, Trend Micro) prevent the copying of "autorun.inf" to removable disks. As the process of creating a bootable USB disk requires the copying of such a file, it is necessary to disable Trend Micro while creating the USB disk using this utility.

- If trying to install Mirage with a SSL Mirage server, the newly deployed machine may not be able to connect to the server (as it would not be a member of the domain yet). In this case, one should add a custom action on the USB disk to add the machine to the domain.
16.5 Advanced Scenarios

16.5.1 Reconnecting a Device to a CVD

A device that has lost its synchronization for any reason can be reconnected to its CVD and can continue backing up incremental changes as before. The **Force Upload** command can be invoked for an Assignment Pending device and will:

(a) Connect device to an existing CVD
(b) Upload the current device data to the CVD

You can initiate Force Upload from the *Pending Devices* window by selecting the device, right-clicking and selecting **Force Upload** from the shortcut menu. The device will then synchronize all its data to the CVD, while local client changes win over CVD changes.
16.6 User Experience with Restore Processes

Restore processes take place in two phases:

**Restore Prefetch**

The Server downloads the minimal set of files and configuration required for the endpoint to boot into the CVD and connect to the network. This is called the **Minimal Restore Set** and enables the end user to start working as soon as this subset of data is resident on their endpoint.

**Restore Streaming**

After the Minimal Restore Set has downloaded and reboot is complete, the Server begins streaming the remainder of the CVD content to the endpoint in the background while the end user works. If the user or application requests a file that has not yet been downloaded, this request takes priority over background transfers.

The user can view the download request by right-clicking the **Mirage** icon on the system tray and clicking **Show Streaming Status**. The **Streaming Status** window appears, which shows the streaming status of each downloading file.
When the user opens a file which has not yet fully downloaded, Mirage will notify the user that the file is currently downloading.

![Image of Mirage notification for file downloading](image)

When that file finishes downloading, Mirage will notify the user that the file is available.

![Image of Mirage notification for file availability](image)

In some cases the user is advised to wait until the connection is reestablished.

![Image of Mirage notification for connection reestablishment](image)

CVD files which have yet to be streamed to the endpoint appear in Windows Explorer with the Offline icon overlay (see images below). This indicates that the files exist on a remote storage medium and that accessing them involves network download delay.

![Windows XP Offline Files and Windows 7 Offline Files](image)
Chapter 17

Hardware Migrations

In this Chapter...

17.1 Using the Hardware Migration Wizard
17.2 Planning for a Mass Hardware Migration
17.3 Performing a Mass Hardware Migration

17.1 Using the Hardware Migration Wizard

Sometimes it is necessary to move a user from one device to another (for example, when new hardware is purchased).

**Note:** When reassigning a CVD to a new device, Mirage checks for drive letter compatibility between the endpoint and the CVD in the data center. If the CVD and the new endpoint have the same drive letters, Mirage displays a confirmation message that includes the drive letters and the disk numbers. If the CVD has different drive letters than the new endpoint, Mirage does not allow the restore operation to proceed.

**Note:** It is important to do a “Sync Now” option on the endpoint before migrating it to a new machine. This ensures that all data is saved to the data center before the migration takes place.

➢ To reassign a CVD to a new device:

1. Install the Mirage Client on the Client machine as described in 4.1 Activation Overview.

2. In the *Mirage Management Console*, select **Common Wizards**, and select **Hardware Migration**.
3. From the first menu, select the CVD you wish to migrate and click **Next**. On the next menu, select the device you would like to migrate the CVD to and click **Next**. Only devices compatible with the selected CVD are listed.

4. On the next menu, select one of the following restore options for the selected CVD and Device and click **Next**.

   - **Full System Migration (Operating System, Applications, User Data and Settings)**
     - The entire CVD (Operating System, applications, and user files) will be migrated to the replacement device. Any existing files on the replacement device will be lost or overwritten.

   - **Migrate Applications, User Data and Settings**
     - Only applications and user data will be migrated to the replacement device. The existing Operating System and applications installed on the replacement device will be retained. The Operating System of the replacement device must be the same as that of the CVD.

   - **Only Migrate User Data and Settings**
     - Only user data and settings will be migrated to the replacement device. The existing Operating System and applications installed on the replacement device will be retained. The Operating System of the replacement device may be the same as or newer than that of the CVD.

**Additional Notes:**

- If you migrate a CVD from a Windows XP device to a replacement device that has Windows 7, you are only allowed to select the **Full System Migration** option or the **Only Migrate User Data and Settings** option. This is because Mirage does not transfer user-installed applications from a Windows XP to a Windows 7 system (because Mirage cannot guarantee cross-Operating System compatibility).

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

- If a Windows 7 endpoint is selected to be restored to a Windows XP CVD, that Windows 7 endpoint becomes a Windows XP device.
5. Select the Base Layer (optional). This window only appears if you selected the **Full System Restore** option in the previous window. You can maintain the current Base Layer (if one applies), select a new Base Layer from the list, or proceed without a Base Layer.

![Hardware Migration Window](image)

6. Click **Next** when ready to proceed.

7. The **Target Machine Name** window appears. Select one of the naming options to apply in the replacement process. If you choose to change the CVD name you have to select whether to add the computer to a Workgroup or Active Directory domain. Click **Next** when done.

![Device Replacement Window](image)
Tip: Choose the Domain and OU by either selecting from the dropdown lists or typing. The dropdown lists are pre-populated with all known domains in the system. The required syntax pattern is shown for each entry field.

a. Any OU defined here should be in standard open LDAP format (For example, OU=Notebooks, OU=Hardware, DC=VMware, DC=com).

b. The join domain account must meet the appropriate security privilege details (as detailed in 7.3.1 General Tab).

8. Use the Validation Summary to compare the target device with the CVD. This summary alerts you to any potential issues that require additional attention. You may not be able to proceed until blocking issues are resolved. Click Next when ready to proceed.

9. Click Finish.

10. The migration process proceeds and takes place in two phases (as described in 16.3 Restoring a CVD Using the Disaster Recovery Wizard).

17.2 Planning for a Mass Hardware Migration

The mass migration feature is required for scenarios in which the customer needs to migrate a mass of old machines (for example, thousands of machines) to new hardware models (without changing the OS version in the process) with a simple, stream-lined process. The solution is based on CSV based input file that defines the set of needed transitions (source machine, destination machine, parameters) and is performed using the VMware Mirage command line tools.

This CSV file contains the following columns:

- Source CVD name (the Windows name of the CVD)
- New CVD name following the rebase (machine name + OU)
- Target device name (the Windows name of the device)
- Optional: note per machine (appears in the Management Console)
- The identifier of the target Base Layer (rebase) or no target Base Layer (universal restore).
- The credentials for the domain join account (username, password, and domain).
- The server address.
- Should warnings/validations be ignored? (“force“)
- Optional: provide name for the created collection.
17.3 Performing a Mass Hardware Migration

The general procedure of a mass hardware migration is as follows (specific steps for these procedures can be found within this guide):

- Centralize the source machines into the Mirage server.
- Assign these CVDs to a specific collection.
- Connect the new machines to the network with an initial Windows system and deploy the Mirage client to them. You can use mass deployment tools to deploy the Mirage client. There are several methods to achieve this, including the following:
  - Using the VMware boot over USB / LAN to deploy the initial image.
  - Deploying an image using 3rd party solutions (for example, PXE / MDT).
  - Asking the hardware vendor to integrate the Mirage client in the Windows image it deploys on the machines.
- Once the Mirage client is deployed, the new machines now appear in the Inventory > Pending Devices queue.
  - The administrator creates a CSV file mapping of source machine names to target machine names. The target machine names are the desired names of the machines after the migration – not the existing names of the target devices (these are probably randomly generated names by the HW vendor). Optionally, it is possible to import this mapping from XML.
  - The administrator also provides the MMC with a domain join account (username/password). This account is used to rejoin the machines into the domain.
  - The administrator selects the pending devices to be used as target machines (should be the same amount of machines as source machines). The Administrator also has the following Base Layer options:
    - The administrator can maintain the Base Layer from the source machines, which removes extraneous applications (OEM applications, for example) from the target machines.
    - The administrator can apply a new Base Layer to the target machines to apply additional applications to the target devices.
The migration process is started automatically and the following processes take place:

- For each source CVD, an available pending device is selected (any of these devices work).
- The source CVD is assigned to the selected pending target device, along with the Base Layer for the target model (if any).
- The migration operation takes place, including automatic boots whenever necessary.
- The migration task is marked as done only when an upload was completed.
- Once complete, the previous CVDs are migrated to the new machines.
Chapter 18

Windows XP to Windows 7 Migration

➢  In this Chapter...

18.1 Planning for a Windows XP to Windows 7 in-place Migration
18.2 Setting Up a Windows 7 Base Layer for Migration
18.3 XP to Windows 7 Migration
18.4 Migration to Windows 7 Replacement Devices
18.6 End User Experience During a Migration

18.1 Planning for a Windows XP to Windows 7 in-place Migration

VMware Mirage offers a unique capability that enables the in-place migration of existing Windows XP endpoints to Windows 7.

The migration includes installation of a Windows 7 Base Layer on each target endpoint, while preserving user profile data and settings via the Microsoft User State Migration Tool (USMT v4.0).

**Note:** This section is for the advanced administrator. VMware recommends that you get acquainted with system operations and functional behavior of Mirage before proceeding with this section.

The migration moves existing content of a target endpoint to the C:\Windows.Old directory, which then gets automatically processed by USMT. Application settings and data that are not handled by USMT are kept in the C:\Windows.Old directory and can be restored manually, or deleted when not needed anymore.

Windows 7 migration with VMware Mirage also retains the original computer name but requires rejoining the domain to create a Windows 7 machine account. This account can be defined in the Mirage System Configuration menu.

Unlike Base Layer updates, the migration process installs a complete OS image, including local user profiles as configured on the reference machine at time of Base Layer capture. This can be used to set up a local Administrator and default user account.
If you are performing a migration in a small or remote office it is often recommended to leverage the VMware Branch Reflector feature (built-in to the Mirage system) to help mitigate the bandwidth used during a migration. See Chapter 10, Using Branch Reflectors for more information. In particular, a Windows 7 test machine configured as a Branch Reflector can share its OS files with Client End Points to assist in the migration process.

18.2 Setting Up a Windows 7 Base Layer for Migration

Important Note: If you upgraded a Version 2.0 Mirage system to Version 3.1 or later and had existing Base Layers (formerly referred to as ‘Base Images’) prepared for use with Windows 7 Migration, you must re-capture a new Base Layer using your 3.x Server and clients. Windows 7 Base Images from 2.0 are not compatible with endpoints running the Mirage 3.x client.

Setting up a Base Layer for use in migration is very similar to setting up a Base Layer for standard Mirage operation.

A Windows 7 Base Layer that is to be used for Windows 7 migration must have the Boot Configuration Data (BCD) and boot-loader files present on the OS Partition and not on a separate boot partition. To do this, right-click the Mirage client in the system tray of the Reference Machine and select Tools > Windows 7 Migration Setup.

Once you have run this setup, right-click the Mirage client in the system tray of the same Reference machine and select Tools > Check Reference Machine. This ensures that the Reference Machine is properly prepped and ready to have a Windows 7 Base Layer captured for use in a migration.

The USMT 4 package also has to be configured in the System Configuration tab of your Mirage Server. See 7.3.4 USMT Settings Tab.

It is also important to make sure that all endpoint devices are decrypted before proceeding with an in-place Windows 7 migration. Disk encryption software may interfere with migrations if endpoints are not decrypted first.
18.3 XP to Windows 7 Migration

The Windows 7 Migration wizard downloads and migrates existing Windows XP endpoints to Windows 7. The process involves first downloading the Win7 image to the endpoints and then applying (migrating) the image. The **Download and Apply Base Layer** option does this in one step, migrating the Win7 image to the endpoints after all the CVDs in the task have finished downloading.

Since the time required for the download stage may vary by endpoint, the IT Administrator may find it convenient to selectively migrate endpoints that have finished the downloading, in advance of the others, thereby having control over when the new Win7 is applied to specific endpoints. The **Only Download Base Layer** option performs only the Download stage, enabling the Administrator to selectively migrate CVDs that have completed downloading as a separate operation. In this case, after the Wizard procedure is concluded, and while the associated download processing is still ongoing, you can selectively start to migrate endpoints that finished downloading – see 18.3.2 Migration Following “Only Download Base Layer”.

**Note:** The Windows 7 Migration wizard performs an in-place migration of existing Windows XP endpoints to Windows 7, within the same equipment. To perform a migration involving different hardware, see 18.4 Migration to Windows 7 Replacement.

### 18.3.1 Using the XP to Windows 7 Migration Wizard

The **Download and Apply Base Layer** option migrates the Win7 image to endpoints only after download has been completed on all the CVDs included in the task. The **Only Download Base Layer** option only downloads the Win7 image to the endpoints. The migration process requires a separate step - see 18.3.2 Migration Following “Only Download Base Layer”.

➢ **To use the XP to Windows 7 Migration wizard:**

1. Open the *Mirage Management Console* and click **Common Wizards**.
2. Click **XP to Win7 Migration**.
3. The **Select Base Layer** wizard page appears.

   ![Select Base Layer Wizard](image)

   - a. Decide if the Windows 7 image should be downloaded and applied, or just downloaded (and then the IT Administrator can choose when the update is applied afterwards).
   - b. Select the Windows 7 Base Layer image that you want to use for migration.
   - c. Click **Next**.
4. Select the XP CVDs or collections of CVDs you want to migrate to Windows 7 by selecting and clicking Select to copy the entity to the Selected CVDs area. The window shows all the CVDs that are eligible for download/migration. Click Next.
5. The **Target Machine Name** window appears. You can change (or define) the hostname for a device that is undergoing the restore operation. You can also select a domain for this endpoint to join after the restore operation.

![Target Machine Name window](image)

**Tip:** Choose the Domain and OU by either selecting from the dropdown lists or typing. The dropdown lists are pre-populated with all known domains in the system. The required syntax pattern is shown for each entry field.

a. Any OU defined here should be in standard open LDAP format (For example, `OU=Notebooks, OU=Hardware, DC=VMware, DC=com`).

b. The join domain account must meet the appropriate security privilege details (as detailed in 7.3.1 General Tab).

**Note:** The account must have access to join the domain. This is not validated. To use the same credentials each time perform the following:

a. In the **Mirage Management Console** tree, right-click **System Configuration** and select **Settings**. The **System Configuration** window appears.

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

c. Click **Next**.
6. A validation dialog appears. Use this dialog to resolve any compatibility issues between the Base Layer and selected CVDs. Click **Next**.

7. A summary dialog appears. Review the summary and click **Finish**.

8. After the Wizard is completed, one task is created which contains all the CVDs that you selected.

   - If you selected **Download and Apply Base Layer**, a **Migration** task will be created and the migration will be performed automatically as part of the wizard process. You can monitor the progress of the migration task – see 18.3.3 *Monitoring the Migration*.

   - If you selected **Only Download Base Layer**, the migration must be performed manually on the task as a separate step – see 18.3.2 *Migration Following “Only Download Base Layer”*.

**18.3.2 Migration Following “Only Download Base Layer”**

If you selected the XP to Win7 Migration wizard **Only Download Base Layer** option, a **Migration Download** task is created containing the CVDs selected for the operation. At the conclusion of the wizard operation, Win7 image downloading to individual endpoints will either be in progress or completed. User action is now needed to apply the image to the endpoints (start the migration). This can be done before the download is completed on all the CVDs in the task, either selectively or for the task as a whole. In either case, migration will be performed on the CVDs that finished downloading, while other CVDs will continue to download and can be migrated in another cycle.

The Start Migration operation can be applied to all eligible CVDs in the task, or on selected CVDs.
To migrate all eligible CVDs in the task:

1. Navigate to the VMware System > Task Monitoring node. In the Task Monitoring window, right-click the Migration Download task and select Start Migration.

2. If downloads were not completed on at least one of the CVDs in the task, a warning appears.

   ![Start Migration Window]

   You are about to start migration on 1 Task.

   WARNING: Not all CVDs have completed the image download. Do you wish to start migration only on CVDs which have completed image download?

   Choose Yes to migrate CVDs which have completed image download.
   Choose No to migrate all CVDs.

3. Select:
   - **Yes** - Apply migration to the CVDs that have finished downloading so far. The not-yet-downloaded CVDs will not be migrated. They will continue to download and be left in the Migration Download task. You can migrate them later in a separate operation.
   - **No** - Wait for the downloading to finish on all CVDs in the task and apply migration automatically to all the CVDs at that time.

   The migration operation will start on the eligible CVDs, according to the option you selected.

4. You can monitor the progress of the migration – see 18.3.3 Monitoring the Migration.

5. You can repeat the procedure as more CVDs complete downloading.
To migrate selected CVDs in the task:

1. Navigate to the **VMware System > Task Monitoring** node. In the **Task Monitoring** window, right-click the **Migration Download** task and select **View Assignments**.

2. The Image **Composer > Layer Assignments** node shows the CVDs in the task. Select the CVDs that you want to migrate, right-click, and select **Start Migration**.

   ![Task Monitoring Screenshot](image)

   ![Layer Assignments Screenshot](image)

   **Note:** The Status panel shows how many CVDs were downloaded. Multiple statuses are shown while downloading is in progress.

3. If downloads were not completed on at least one of the selected CVDs, a warning appears, like the warning described in **To migrate all eligible CVDs in the task**, above, but in terms of the selected assignments.

4. Select:
   - **Yes** - Apply migration to the selected CVDs that have finished downloading so far. The not-yet-downloaded CVDs will not be migrated. They will continue to download and be left in the **Migration Download** task. You can migrate them later in a separate operation.
   - **No** - Wait for the downloading to finish on all the selected CVDs and apply migration automatically on all the CVDs at that time. The migration will start on the eligible CVDs according to **the selected** option.
5. You can monitor the progress of the migration – see 18.3.3 Monitoring the Migration.

6. You can repeat the procedure as more CVDs complete downloading.

18.3.3 Monitoring the Migration

You can monitor the detailed progress of all the CVDs in the migration by viewing the task progress.

➢ To monitor the migration task progress:

1. Navigate to VMware System > Task Monitoring, right-click the required task and select View Assignments.

2. The Image Composer > Layer Assignments node shows the CVDs in the task. The Status panel shows how many CVDs were downloaded. Multiple statuses are shown while downloading is in progress.
18.4 Migration to Windows 7 Replacement Devices

The IT manager can migrate users from a Windows XP or Windows 7 machines to new Windows 7 machines. This is relevant for smaller customers that use Windows OEM SLP licenses, and supports both disaster recovery and hardware refresh scenarios.

Migration to a different device requires restoring only user data and settings. For this purpose, use the To restoring a CVD to a replacement device procedure in 16.3 Restoring a CVD Using the Disaster Recovery Wizard. For the Restore Options selection in that procedure, select Only Restore User Data and Settings.

This operation can be used for:

- Windows XP 32-bit to Windows 7 32-bit or 64-bit
- Windows 7 32-bit to Windows 7 32-bit or 64-bit
- Windows 7 64-bit to Windows 7 64-bit

(The 18.3 XP to Windows 7 Migration section describes “in-place” migration” for Win7 and is not suitable for migration to replacement devices.)

18.5 Post-Migration Scripts

A migration can include a custom Post-migration script, which allows administrators to automatically perform certain actions after the migration update.

Examples of actions that require Post-migration update processing include:

- Installation of software requiring execution on the individual endpoint. This may include hardware-specific software that is only compatible with certain endpoints.
- Update or removal of hardware drivers that may already exist on the endpoint.

This file and any auxiliary files used or called by the script will be captured as part of the Base Layer and distributed to the various endpoints. It is important to ensure that the auxiliary files are placed in the same directory as the script or another directory that is captured in the Base Layer.

In order to create a Post-migration script, create a file named post_migration.bat under the %ProgramData%\Wanova\Mirage Service directory. The file must be edited on the reference machine.

Note: The Mirage Client installation includes a default sample script that does not perform any Post-migration script actions.

To monitor the execution of the Post-migration script, Mirage Client reports events to the Mirage central management service if the script returns an error value other than 0.
18.6 End User Experience During a Migration

After the Migration Base Layer download is complete, Mirage requests a reboot. A swap is made and Windows 7 boots.

The machine loads Windows 7 and automatically logs in to an automated user that Mirage created. During this time, Windows 7 installs and configures all hardware discovered using Plug-and-Play. This process may take a few minutes, during which the computer is fairly busy.

When Plug and Play discovery is complete, the post-migration script runs. The script executes USMT and then rejoins the domain. To rejoin the domain, the PC must be connected to the corporate network and automatically assigned a network address.

The user can monitor the progress of this process in Mirage status window.

Note: In order to re-join the domain, the computer must have network access to the domain controller. End users are not able to login using their domain credentials until the domain join is complete.

18.6.1 Known Limitations

- A Windows 7 migration using VMware Mirage only works if the Base Layer includes the Boot Configuration Data (BCD) and the required Boot Loader files as described in this document.

- If an endpoint includes multiple operating systems, the migration only overwrites the one on the active OS Partition and does not provide boot options for the others. Other boot options may be manually restored after booting into Windows 7.

- USMT does not migrate any applications that were installed on XP to Windows 7. To provide applications upon migration, they must be installed in the Base Layer.

- All custom boot loaders on the target machine are removed. In addition, if the target machine uses third-party Full-Disk-Encryption, you must decrypt the target machine disk before starting the migration process.

- All user data on the reference machine is applied to the target as part of the migration process. Make sure to remove any sensitive data from the reference machine.
PART 7 - MONITORING, REPORTING, AND TROUBLESHOOTING

In this Part...

19. Monitoring Desktop Deployment
   19.1 Using the System Dashboard
   19.2 Transaction Logs

20. Mirage Reporting
   20.1 Mirage Reporting Overview
   20.2 Generating a Report
   20.3 Base Layer Dry-Run Reports
   20.4 CVD Integrity Report

21. Maintaining the Mirage System
   21.1 Server Backup and Restore
   21.2 Upgrading from Previous Mirage Versions

22. Troubleshooting
   22.1 Using the CVD History View
   22.2 Using the Event Log
   22.3 Customizing the Minimal Restore Set
   22.4 Using the System Report Utility
   22.5 Remote SysReport Collection
Chapter 19

Monitoring Desktop Deployment

In this Chapter...

19.1 Using the System Dashboard
19.2 Transaction Logs

19.1 Using the System Dashboard

The System Dashboard provides at-a-glance monitoring of system status and operations. The Dashboard displays statistics about system activities as well as other information, such as, alerts and indications about actions the system administrator must carry out. Some titles are links to relevant areas in the Dashboard, enabling you to access and view related information.

Most Dashboard information is refreshed automatically every three minutes. By pressing F5, users can also refresh key information indicators, such as system status, Server status, and capacity usage.
19.1.1 System Status

The System Status area shows the number of unacknowledged events according to severity (Critical, Warning, Info) and source (Server or Clients).

System events have been propagated from Clients, from the Server, and from the management service on the Server. Warning and Info events provide advice or instructions and do not require urgent attention. Clicking an event button opens the event log view filtered according to the selected severity and source.

19.1.2 Server

The Server area shows the current status of the Mirage Servers, Up or Down. The icon also reflects the Server status.

19.1.3 Update Progress

The Update Progress area shows a vertical histogram of the number of Clients currently downloading updates or restoring operations, and their download progress.

A device count appears alongside each bar to show the number of devices that are downloading in each percentage range. This graph enables you to view a scalable download progress summary after Base Layer assignment, enforcement, or update, and during CVD restore.

- **Total Ready**: The number of desktops that have finished downloading (reached 100%) and desktops that have no pending download.
- **Total in Progress**: The total number of desktops that are currently downloading or have an incomplete download pending network reconnection.

19.1.4 Data Protection

The Data Protection area enables you to view the total protection level of the desktop deployment.

The gauge shows the ratio of total desktop content stored and protected at the Server versus total desktop data at the endpoint that is in the process of synchronization. The gauge reflects only information provided by online devices. Offline devices report the next time they connect.

19.1.5 Compliance Meter

The Compliance meter area enables you to view the total compliance level of your endpoints.

The gauge represents, as a percentage, the deviation of all managed endpoints from their IT-approved Base Layer. Based on this information, administrators can easily and quickly enforce the Base Layer for one or many endpoints to bring them back into compliance and decrease the likelihood of end user problems.
19.1.6 Capacity Status

The Capacity Status area shows the number of devices according to the following status options:

- **Pending**: The number of devices pending restore or activation (irrespective of their connection status).
- **Online**: The number of activated and online devices (excluding online devices that are pending restore).
- **Offline**: The number of activated and offline devices (excluding offline devices that are pending restore).

The Pending label and counter links to the pending devices window in the console, where you can view the pending devices and apply relevant actions.

An exclamation mark icon indicates license depletion. This occurs if the total number of pending plus online devices is greater than the licensed capacity.

19.1.7 Efficiency Benchmarks

The Efficiency Benchmarks area shows the actual traffic between the desktops and the Server.

The Network Usage (In) graph shows the upload traffic (from the desktops to the Server), and the Network Usage (Out) graph shows the download traffic (from the Server to the desktops).

The bar chart shows the traffic over the last 24 hours. Each bar shows the total data for one hour.

**Note**: The bar representing the current hour shows total traffic from the start of the hour to the last dashboard refresh time.

The following information is shown on each graph:

- **Y axis**: Data size in bytes, KB, MB, or GB, according to the maximum data transferred in the 24-hour span.
- **X axis**: Time in hours, where each bar represents one hour.
- **Total**: Total traffic in the last 24 hours.
- **Average**: Hourly traffic average in the last 24 hours.
- **Peak**: Hourly traffic peak in the last 24 hours.
19.2 Transaction Logs

A transaction is a logical operation between the Mirage Server and the Client. The transaction log can be used to monitor the progress of updates coming from and to the Mirage Server.

The following are the types of transactions:

- **Centralize Endpoint**: First upload of the end-user machine to the Mirage Server.
- **Upload Incremental Changes**: Synchronizing ongoing changes from the end-user machine to the Mirage Server.
- **Update Base Layer**: End-user machine is updated with the assigned Base Layer.
- **Base Layer Caching**: The Branch Reflector downloads a Base Layer.
- **Base Layer Verification**: Base Layer download is verified prior to being applied.
- **Restore Prefetch**: Client downloads the minimum file set required from the CVD in order to allow the endpoint to boot the restored CVD and allow network access to complete restore through background streaming.
- **Restore Streaming**: Client streams the remainder of the restored CVD to the endpoint while the user works normally online.

Each transaction is built from a collection of sub-transactions, each representing a network session between the Client and Server. Sub-transactions are reported only when a session is either complete (succeeded) or terminated (failed due to a network disconnect or other specified reason).

**Note**: More than one sub-transaction appears when one or more attempts to complete the parent transaction have failed. The sub-transaction status reported is final and does not change.
19.2.1 **Transaction Entry Properties**

Each transaction entry contains the following properties:

- CVD
- Type: The operation being performed (Centralize Endpoint, Upload Incremental Changes, and so on)
- Base Layer ID and version (if applicable)
- Start/End time and duration
- Total number of changed files
- Total number of files to be transferred (after duplicate files are eliminated)
- Total Data size of the files to be transferred (after duplicate files are eliminated)
- Data Size After Dedup: Total size of file and metadata to be transferred after it is reduced by intra-file and inter-file block level deduplication but before LZ compression
- Before Compression: Total network transfer as seen over WAN, before applying LZ compression
- Data transferred: Total network transfer that actually took place.
- Transfer Savings: Ratio between total size of the changed files and actual transfer size
- Branch Reflector Transfer Size: The amount of data that was sent from the Branch Reflector to the endpoint (instead of from the Mirage Server directly to clients).

19.2.2 **Search and Filter Results Specification**

Whenever a Search or Filter query is initiated in any list window, the first page of results is displayed in the view area. The number of pages of qualifying records appears under the **Search** field and you can scroll to the next or previous page by clicking the arrow icons. For improved query response time, when the number of records retrieved is very large, the associated page count is not calculated and is replaced by three dots (...).
19.2.3 Total Transaction Records Limit

Mirage implements the following transaction records limits to prevent log files from becoming too large:

<table>
<thead>
<tr>
<th>Transaction Record Type</th>
<th>Cleaned up after:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steady State (SS) transactions</td>
<td>30 days</td>
</tr>
<tr>
<td>Core Image transactions</td>
<td>180 days</td>
</tr>
<tr>
<td>All other transactions</td>
<td>365 days</td>
</tr>
</tbody>
</table>
Chapter 20
Mirage Reporting

➢ In this Chapter…
20.1 Migration Reporting Overview
20.2 Generating a Report
20.3 Base Layer Dry-Run Reports
20.4 CVD Integrity Report

20.1 Mirage Reporting Overview

VMware Mirage provides Mirage System reporting. Reports are generated on-demand. The Mirage reports include:

- **Storage Usage Report**: Describes storage utilization on the selected volume or volumes.
- **Base Layer Dry-Run Reports**: Compare the content of the Base Layer and the CVD.
  - **Application-level report**: Describes projected applications that are added to, updated in, or deleted from an endpoint device when the selected Base Layer is downloaded.
  - **Program Executable (PE) level report**: Analyzes the outcome of removing or updating a PE file.

For more information about these reports, see 20.3 Base Layer Dry-Run Reports.

- **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.

- **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 20.4 CVD Integrity Report.
20.2 Generating a Report

This procedure applies to all reports except the wizard driven CVD Integrity report. To generate that report, see 20.4 CVD Integrity Report.

➢ To generate the Mirage reports:

1. In the Mirage Management Console tree, under the Reports tree, click the report that you want to generate.
2. Click the Generate Report icon on the report toolbar. The Generate Report window appears.
3. In the Report Name field, type a report name.
4. Select the volumes on which you want to report.
5. Click OK. The report is generated. You can view the report when the status is Done.

➢ To view the report:

- Click the View Report icon on the report list toolbar. The report is displayed as an HTML page.

➢ To delete the report:

1. On the report list, select the report you want to delete.
2. Click the Delete icon on the report console toolbar.
20.3 Base Layer Dry-Run Reports

Before applying a new Base Layer version to a CVD or collection of CVDs, you can run a report to compare the content of the Base Layer and the CVD. This report helps you plan the Base Layer update process, and resolve in advance conflicts that might result from any mismatch between the CVD and the Base Layer content.

This report can be generated in two ways:

- **Application-level report**: This report describes projected applications that are added to, updated in, or deleted from an endpoint device when the selected Base Layer is downloaded. It compares the installed applications of the Base Layer and the CVD and provides a general view of the result for the Base Layer update.

- **Program Executable (PE) level report**: This report analyzes the outcome of removing or updating a PE file. It projects affected software modules, such as .DLL files, when a Base Layer is downloaded to an endpoint device client, and details whether each affected module is downgraded.

**Note**: Depending on the number of CVDs selected, running the report may take a while.

The table below can be used to identify what different conflicts mean when they appear in a module report:

<table>
<thead>
<tr>
<th>Conflict Type</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Layer Application Downgrades a user installed application</td>
<td>An application installed in the Base Layer uses and older version of shared component/s than another user installed application uses.</td>
</tr>
<tr>
<td>Base Layer Application Downgrades OS component</td>
<td>An application installed in the Base Layer downgrades OS component/s.</td>
</tr>
<tr>
<td>Base Layer OS Component/s downgrades user installed application</td>
<td>OS component/s in the Base Layer downgrades shared components that are used by a user installed application.</td>
</tr>
</tbody>
</table>
20.4 CVD Integrity Report

This 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.

The report generation process is Wizard-driven.

You should generate the CVD Integrity report if a system event warns that a CVD might have inconsistencies and suggests that you run the report.

To run the CVD Integrity report:

1. In the Mirage Management Console tree, under the Reports tree, select the CVD Integrity report.
2. Click the **Generate Report** icon on the report toolbar. The **Select CVD** window appears.

![Select CVD window](image)

**a.** In the **Report Name** field, enter the desired report name. If none is given, the default name format will be applied (CVD_Integrity_{User's environment name}_{Short date}).

**b.** In the CVD List area, select the required CVD.

**c.** Click **Next** to continue.
3. The **CVD Integrity Options** window opens.

![Image of CVD Integrity Options window]

**a. Select the required report option:**

- **Check Only**: Only generates 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 (e.g., periodic upload) when you encountered a problem with the CVD. Corrupted files are re-uploaded to allow the interrupted process to resume.

**b. 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 to allow the interrupted process to resume. Click **Next** to continue.

4. The **Summary** window opens. Click **Finish**.

![Image of Summary window]

You are about to run “Check Only” CVD integrity on CVD device100 [ID 10040]. The CVD will be suspended during the integrity check.
Report Name: CVD_Inventory_qa1_4/19/2012.
Chapter 21

Maintaining the Mirage System

➢ In this Chapter...

21.1 Server Backup and Restore
21.2 Upgrading from Previous Mirage Versions

21.1 Server Backup and Restore

➢ Backup procedure:

Server state backup involves the backup of all the Mirage storage volumes and database. The Mirage storage volumes should be copied (preferably via a snapshot mechanism) to the backup location. Additionally, the database should be backed up.

In order to make sure that backup is consistent across all the volumes and the database, it is imperative that the SIS and the database be backed up using a point-in-time representation. Make sure to configure your server backup software to stop the Mirage Server cluster and the Management server during the snapshot and database backup time.

Note: If storage snapshots are not used, the Mirage Servers and the Management server should be stopped for the full duration of the backup.

➢ Restore procedure – Mirage Management Server only

Important Note: Even if only a single Mirage volume or only the Mirage database needs to be restored, restore all Mirage volumes and the database at the same time.

Note: You must use the same fully-qualified name of the original Mirage Management server to enable existing Mirage Servers to locate the Management server and connect to it.

When the Mirage Management Server needs to be restored, you only need to re-install the Mirage Management server. For detailed instructions on installing a Mirage Management Server, see 3.3 Installing the Mirage Management Server.
> **Restore procedure - Mirage Server only**

When only a single server needs to be restored and there is no Mirage storage or database installed on this machine, you only need to re-install the Mirage Server and point it to the Mirage Management Server. For detailed instructions on installing a Mirage Server, see 3.7 *Installing a Mirage Server*.

If the Mirage Management Server was installed on the same machine, you need to re-install the Management Server before re-installing the Mirage Server. For more information on installing the Mirage Management Server, see 3.3 *Installing the Mirage Management Server*.

> **Restore procedure - Mirage Storage Volumes and Database:**

The following procedure restores the Mirage volumes and database in a standalone or clustered environment, where the Mirage storage volumes and database are not co-hosted on the same server as the Mirage Management Server.

**Note:** The restore procedure requires the **ServerTools.zip** package, prior to installing the Mirage Server. You may download the package from the downloads section of the VMware support web page at [http://www.vmware.com](http://www.vmware.com) or contact VMware Support through email or phone to receive a copy of the package.

1. Ensure that all Mirage Servers and the Mirage Management server are stopped.
2. Restore all the Mirage storage volumes and the database from backup. Make sure to restore into original UNC paths.
3. Copy the **ServerTools.zip** to the server machine, extract the zip, and run the following command from any Mirage Server machine:
   ```
   Wanova.Server.Tools.exe  ResetPendingBT
   ```
4. Start the Mirage Management server and all Mirage Servers.
5. If the UNC path was changed on any of the volumes, you must change the UNC path in the *Edit Volume* window and mount the volume. For more information, see 9.4 *Editing the Volume Information*.
21.2 Upgrading from Previous Mirage Versions

This section describes how to upgrade the Mirage System to Version 3.6 from earlier Mirage versions.

21.2.1 Upgrade Notes

- Uninstalling the Mirage Servers does not remove any data from the storage volumes that were connected to the Mirage System.

- When upgrading to a new version of Mirage, the SSL and port configurations from the previous versions are not be migrated over. The IT Administrator needs to reconfigure the SSL and port configurations after the new versions of Mirage are installed.

- When the upgrade is complete, your Mirage clients automatically prompt their end users to perform a client upgrade and reboot. The IT Administrator does not have to perform any operations for this to occur.

- Upgrade from Version 2.0 - If you had Base Images from your 2.0 system, it is highly recommended that you recapture new Base Layers using your 3.6 system and clients. However, it is required that you recapture any Base Image/ Base Layer that was used for Windows 7 migrations. Base Images from 2.0 that were used for Windows 7 migrations are not compatible with later system versions.
21.2.2 Upgrade Procedure

The Mirage System must be uninstalled in the following order (from the Control Panel – Add/Remove Programs):

1. Uninstall all Mirage Servers.
2. Uninstall the Mirage Management Console.
3. Uninstall the Mirage Management Server.

The Mirage 3.6 Software must then be installed using the new MSIs in the following order:

1. Install Mirage Management Console.
2. Install Mirage Management Server.
3. Install Mirage Servers.
22.1 Using the CVD History View

To help the administrator troubleshoot problems in a CVD, the Mirage Management Console provides a single view that consolidates all related events during the CVD’s life in the system into a common timeline.

The following events are displayed in the CVD history view:

- Transaction log events.
- Audit events.
- Client system events.

You can copy/paste information from the CVD History view for use elsewhere by using standard Windows key combinations (Ctrl+C to copy, Ctrl+V to paste).
To open the CVD history view:

1. In the CVD Inventory, right-click the CVD name and select **History**.
2. Click **Timeline**. The **CVD History** window appears.

### 22.2 Using the Event Log

The Mirage Management Console event logs include:

- **Event Log**: Important system events as propagated from the Server and Clients.
- **Manager Journal**: Audit events to collect and track the history of management user operations resulting in system configuration changes.

#### 22.2.1 Audit Events

An audit event is created for any management user action resulting in a system setting or configuration change. This includes actions performed using the Mirage Management Console or through a CLI. Read-only actions do not create audit events. The following information is recorded for audit events:

- Time of the operation
- Operation name
- Operation details
- User name
22.3 Customizing the Minimal Restore Set

The system administrator can customize the Minimal Restore Set. This is the minimal set of files that must be restored to an endpoint to enable rebooting into the CVD and working online; it should include the organization VPN, antivirus, firewall applications, and driver store.

The restore set consists of two elements:

- **Static Minimal Restore Set**: A static list of files created by the system administrator and placed in an XML file that is fetched during the restore operation. The files restored provide the endpoint with the minimum environment required to boot into a CVD. The static list is used for all endpoint devices in the system.

- **Dynamic Minimal Restore Set**: This is a CVD-specific list of files that is acquired during normal CVD usage. The list is built on each boot and captures the system, applications, and user files over a short time period after booting. A separate dynamic restore set is created for each CVD in the system and is used in conjunction with the static minimal restore set when a restore is performed.

**Important Note**: The following procedure describes how to modify critical Mirage configurations using the CLI. Follow these steps carefully, as serious problems can occur if you use the CLI incorrectly.

➢ **To customize the minimal restore set:**

1. On the Start menu, click Run, type cmd, and then click OK.

2. In the Command window, type:
   ```
   cd <Mirage Server program files path>
   ```
   For example, C:\Program Files\Wanova\Mirage Server and then press <Enter>.

3. Type:
   ```
   ```
   The VMware Server Management Console starts running.

   **Note**: To access the VMware Management Console, you must be authenticated as a member of a group with access to the console (see A.5 Managing Users and Roles Using AD Groups).

4. To export the minimal restore set, type:
   ```
   getminimalset <path to output file>
   ```

5. Modify the file using an XML editor.

6. Add the modified file to the minimal set, using the following command:
   ```
   addMinimalSet <path to XML file>
7. Press <Enter>.

**Note:** Executing this command overrides any existing static minimal set.

```
C:\Program Files\Wanova\Mirage Server\MinimalSet.xml
```

A message is displayed confirming that the Static Minimal Set has been added successfully.

8. To view the minimal set type `printMinimalSet` and press <Enter>.

9. Type **Exit** and press <Enter> to exit the Command window.

You can also remove the minimal set using this procedure with the command `removeMinimalSet`. If this command is run, the entire CVD content is downloaded prior to the restore and online streaming is not used.

If you want to revert to the original (default) VMware minimal set, the file is located at:`C:\Program Files\Wanova\Mirage Server\MinimalSet.xml`.

You may also use that file as basis for further customizations, such as adding the corporate antivirus and VPN files, and so on.

### 22.4 Using the System Report Utility

The System Report Utility collects internal Mirage log files, relevant registry entries, event logs, and system information and configuration, to help VMware support and IT with troubleshooting.

The report utility offers the following report types:

- **Full report:** Collects the most comprehensive set of Mirage logs, registry and system information. While helpful in troubleshooting confirmed issues, this report can be very large (containing several hundreds of MB of data), and is only used by special request from VMware Support.
  
  Run: `sysreport_full.cmd`

- **Medium report:** Used most frequently, this report type collects a limited set of Mirage logs and system information. It is faster to generate and more resource efficient than the full report.
  
  Run: `sysreport_medium.cmd`

- **Logs only report:** Returns a minimal set of log entries. Usually used in early troubleshooting stages to determine next steps.
  
  Run: `sysreport_logs_only.cmd`
Remote SysReport Collection

➢ To generate a system report:

- As an administrator, run the sysreport batch file from the Mirage install directory, for example: C:\Program Files\Wanova\Mirage Server

A CAB file containing all the logs is created and can be found at: c:\sysreport-MMDDYYYY-HHMM-ComputerName.cab

Note: This command can be CPU-intensive, especially on the Server, hence intermediate impact should be expected.

Or,

- Alternatively, you can generate a system report by right-clicking the Mirage icon in the system tray, and selecting Tools.

22.5 Remote SysReport Collection

An Administrator can save system remotes from any device attached to the Mirage server.

➢ To save system remotes:

1. In the Mirage Management Console tree, expand the Inventory node and select the All CVDs node.

2. Find the CVD that you would like to generate a report for. Right-click the CVD and select Device > Generate System Report.
3. Select one of the following options:

- **Logs**: this only generates a report of the basic logs for this client.
- **Medium**: this includes the logs and some additional information.
- **Full**: this includes all logs and collectable information from this endpoint.
In the appendix...

A.1 Mirage and SCCM
A.2 Setting Up the SSL Certificate in Windows Server
A.3 Using Microsoft Office 2010 in a Core Image
A.4 User Role Definitions
A.5 Managing Users and Roles Using AD Groups
A.6 Working with Roles and Active Directory Groups
A.7 Macros in Policy Rules

A.1 Mirage and SCCM

This topic specifies the steps that must be taken before capturing a Base Layer that contains an SCCM client for Migration to Windows 7. This procedure must be performed before each capture Base Layer (that is going to be used for migration). The reference machine must not be rebooted, and the ccmexec service must not be restarted in the time period between performing the procedure and capturing the Base Layer.

There is no need to follow these steps for regular Base Layer updates, as this is already handled automatically by Mirage.


2. Stop the SMS Agent Host service (net stop ccmexec).

3. Use ccmdelcert.exe to delete the SMS certificates (ccmdelcert.exe is available as part of the Systems Management Server 2003 Toolkit, and also attached to this wiki page).

4. Delete c:\windows\smscfg.ini if it exists.

5. Capture a Base Layer (do not reboot or start the ccmexec service, otherwise you will have to repeat this procedure).
A.2 Setting Up the SSL Certificate in Windows Server

Set up the SSL certificate in Windows server by following these steps. In a multi-server setup, repeat this procedure for each installed Mirage Server.

➢ To generate the Certificate Signing Request (CSR):

1. On the Server, open the MMC, add the Certificates snap-in, and then select the Local Computer account.
2. Open the snap-in, right-click the Personal store node, and then select All Tasks > Advanced Operations > Create Custom Request. A wizard opens.
3. Click Next.
4. In the Custom Request area, select Proceed without enrollment policy, and then click Next.
5. Click Next to accept the default settings in the Template and Request Format fields (CNG Key, PKCS #10).
6. In the Certificate Information area, click Details for the Custom Request.
8. In the General tab, enter a certificate-friendly name. (You can use the same name as the subject name.)
9. In the Subject tab, in the Subject Name area, fill in the relevant certificate fields as follows:
   - **Common name, value**: Server FQDN. Note that this is the certificate subject name that is used in the Mirage config to find the certificate. The FQDN must point to that Server and are validated by the Client upon connection.
   - **Organization, value**: company name. (Usually required by CA.)
   - **Country, value**: two-letter standard country name (for example, US or UK). (Usually required by CA.)
   - **State, value**: state name (optional).
   - **Locality, value**: city name (optional).
10. In the Extensions tab, do the following:
    - **Key Usage**: Select Data Encipherment.
    - **Extended Key Usage**: Select Server Authentication.
11. In the **Private Key** tab, do the following:
   - **Key Options**: Select the required key size (usually 1024 or 2048).
   - Select **Make Private Key Exportable** if you want to be able to export the CSR (and later on the certificate) with the private key for backup or Server movement purposes.

12. Click **OK** to close the *Certificate Properties* window.

13. Click **Next** in the Certificate Enrollment wizard.

14. Leave the default file format (Base 64) as it appears, and click **Browse** to select a file name and location where to save the CSR. The certificate request is completed.

15. To see the CSR, go to *Certificate Enrollment Requests & Certificates*, and click **Refresh**. You can export the CSR with the private key for backup purposes.

➢ **To use the CSR:**
   1. Open the CSR .req file with notepad.
   2. Copy the text inside.
   3. Go to the external CA Web site, and paste the CSR text in the provided form.

➢ **To install the signed certificate:**
   When the CA sends you the signed certificate file (.CER or .CRT), go back to the certificates snap-in and do the following:
   1. In the **Personal** area, select **All Tasks Import**, and then click **Next**.
   2. Browse to select the signed certificate file, and then click **Next**.
   3. Accept system auto selection or select the **Personal Store** for the certificate. Complete the wizard to complete the import.
   4. Go to **Personal Certificates**, and then click **Refresh**. Alternatively, use **Find Certificates** to find the certificate location.
   5. Open the certificate and verify that it states that you have the private key. Go to the **Certification Path** tab and check that you have all the certificates in the chain and that they are usable (no validity warnings or missing certificates).
A.3 Using Microsoft Office 2010 in a Core Image

When building a Core Image using the Core Image Capture Wizard, Mirage prompts you for the Microsoft Office 2010 license key, as well as for licenses for every other activated Office component on the Reference Machine. For example, Office, Visio, OneNote, and so on. When you deploy the core image to an endpoint these Office keys are used when installing Office. This is done to preserve the licensing for an existing version of Office. This helps prevent issues with Office and Visio licensing.

It is highly recommended to build in the Office licenses into your Core Images to prevent interfering with existing licenses on user’s endpoints.

**Note:** If you are upgrading from Office 2007 to Office 2010 and end users have specific components installed on their endpoint (Visio, for example), make sure that those components are also installed in your new Base Layers for those applications to remain on your endpoints.
## A.4 User Role Definitions

Dynamic role-based access control (RBAC) is the part of the Mirage System that determines which actions each user in the system can perform based on assigned roles.

The following is a list of actions in the system:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View dashboard</td>
<td>User can view the dashboard.</td>
</tr>
<tr>
<td>View server status</td>
<td>To view the server status node; if you do not have it appears as an empty list.</td>
</tr>
<tr>
<td>View tasks</td>
<td>User can view the tasks list in the Task Monitoring node.</td>
</tr>
<tr>
<td>Manage tasks</td>
<td>User can delete running tasks.</td>
</tr>
<tr>
<td>View CVDs</td>
<td>User can view the CVD inventory.</td>
</tr>
<tr>
<td>Manage CVDs</td>
<td>User can delete a CVD, assign a Base Layer to a CVD, enforce a Base Layer, assign a policy to a CVD, and revert to snapshot.</td>
</tr>
<tr>
<td>Manage collections</td>
<td>User can create and remove collections.</td>
</tr>
<tr>
<td>Manage collections CVDs</td>
<td>User can add and remove CVDs from a collection.</td>
</tr>
<tr>
<td>View upload policies</td>
<td>User can view policies.</td>
</tr>
<tr>
<td>Manage upload policies</td>
<td>User can edit, create, and delete policies.</td>
</tr>
<tr>
<td>View devices</td>
<td>User can see the devices in the device inventory and the pending list.</td>
</tr>
<tr>
<td>Manage devices</td>
<td>User can assign a device to a CVD, reject a device, restore a device, remove a device, suspend a device, and synchronize the device with the CVD.</td>
</tr>
<tr>
<td>View Layers</td>
<td>View the layers that are assigned to different devices.</td>
</tr>
<tr>
<td>Manage Layers</td>
<td>Create layers, delete layers, cancel layer assignment (this is a bug), update layer data (name, details).</td>
</tr>
<tr>
<td>View ref CVDs</td>
<td>User can view the Reference CVD inventory.</td>
</tr>
<tr>
<td>Manage ref CVDs</td>
<td>User can assign a reference device to a Reference CVD, assign a Base Layer to a Reference CVD, assign a policy to a Reference CVD, and delete a Reference CVD.</td>
</tr>
<tr>
<td>View Base Layer rules</td>
<td>User can view the image rules.</td>
</tr>
<tr>
<td>Manage Base Layer rules</td>
<td>User can add new rules, remove rules, test Base Layer draft rules, and set new default Base Layer rules.</td>
</tr>
<tr>
<td>View Driver Library</td>
<td>See the driver profiles and driver folders and their details in the driver library</td>
</tr>
</tbody>
</table>
### A.5 Managing Users and Roles Using AD Groups

Mirage supports dynamic role-based access control (RBAC) to allow the system administrator to define which users can perform which operations in the system.

A role can be granted to one or more Active Directory (AD) groups. The Mirage Server identifies users by AD group membership and automatically assigns their matching user roles in Mirage.

A user can only have one active role at a time. If the user’s group is assigned to more than one role, the user inherits the superset privileges of all assigned roles.

Each role is mapped to a set of actions the user can perform in the system, such as managing CVDs, Base Layers, users, groups, and events, as well as viewing the dashboard and other system information. For a complete list of actions available in the Mirage System, see A.4 User Role Definitions.

Mirage comes with three predefined user roles: Administrator, Desktop Engineer, and Helpdesk:

- The Administrator role has access to all Mirage functions, including Base Layer management functions and the management of users and roles. The Administrator role cannot be edited or deleted.

- The Desktop Engineer role provides, by default, privileges for all system operations except Base Layer management, user management, and role management. This default privilege set can be customized.

- The Helpdesk role is only authorized by default to perform view operations on the system in order to troubleshoot a CVD problem. This default privilege set can also be customized.

Additional custom roles can be defined by the Administrator to fit various company processes.
A.6 Working with Roles and Active Directory Groups

An Administrator in the Mirage System can create new user roles and define which actions role members can perform. The Administrator can also edit or modify existing roles.

➢ To add a new user role:

1. In the Mirage Management Console tree, right-click Users and Roles and select Add a Role.

2. In the Add Role window, enter the role name and description. By default, the new role does not have any privileges until they are assigned by the Administrator.

➢ To edit an existing role:

1. In the Mirage Management Console tree, click Users and Roles. Edit the role in the right pane as required.

2. Click Save.
To assign an Active Directory group to a role:

- Expand the **Users and Roles** node, right-click the required user role, and select **Add a Group**.

3. Enter the group name in the **Group Name** field, using the following syntax: `domain\group`.

**Note:**
- A group cannot be added to two different roles.
- The role view is not auto-refreshed.

A.7 **Macros in Policy Rules**

The supported macros for the directory path are:

- **System directories:**
  - `%systemvolume%`: The system drive letter followed by a "\:" (for example, c:\).
  - `%systemtemp%`: The Windows system temp directory (usually c:\windows\temp).
  - `%windows%`: The Windows directory (usually c:\windows).
  - `%Anyvolume%`: Expands to multiple rules, one per drive letter (for example: c:, d:, e:)
  - `%documentsandsettings%`: Expands to one rule of the path that contains the user profiles (usually c:\documents and settings).
  - `%programfiles%`: The program files directory (including support for localized Windows versions) and the Program Files (x86) in 64-bit.
  - `%systemdir%`: The Windows system directory.
Remote SysReport Collection

- Profile directories:
  - `%anyuserprofile%`: Expands to multiple rules, one per any user profile, including both local user profiles and domain user profiles (for example, C:\Documents and settings\myuser, and so on). This macro does not include the `%defaultuserprofile%` content.
  - `%domainuserprofile%`: Expands to multiple rules, one per any domain user profile.
  - `%localuserprofile%`: Expands to multiple rules, one per any local user profile.
  - `%anyuserlocalappdata%`: All the users local app data directories.
  - `%anyusertemp%`: All the user’s TEMP directories.

- Special profile directories (not included in the Profile directories):
  - `%ProgramData%`: The special Application data directory under the All Users directory. For example, C:\Documents and Settings\All Users\Application data.
  - `%defaultuserprofile%`: The special Default User directory.
  - `%builtinuserprofile%`: Expands to multiple rules, one for each built-in user profile (not including local or domain users). For example, “NetworkService?” and “LocalService?”. In Windows XP, this also includes “All Users”.
  - `%localserviceprofile%`: The special “local service” directory.
  - `%Anyuserroamingappdata%`:
  - `%Anyusertempinternetfiles%`: All the users temp internet directories on the machine
  - `%anyshellpaths%`: All the directories below.
  - `%desktop%`: All the user’s desktop directories in the machine
  - `%favorites%`: All the users favorites directories in the machine
  - `%videos%`: All the users Video directories in the machine
  - `%pictures%`: All the users pictures directories in the machine
  - `%documents%`: All the users documents directories in the machine
  - `%music%`: All the users music directories in the machine
no fallback to server ........................................ 21, 106
overview ......................................................... 101
rejecting peers .................................................. 108
waiting peers ..................................................... 111

C

cache size .......................................................... 106, 107
capacity status .................................................. 205
Centralizing an endpoint .................................... 49
collection
add CVDs .......................................................... 62
Collections node ............................................... 61
compliance meter ................................................. 204
CVD ................................................................. 17
collections .......................................................... 61
snapshots .......................................................... 161, 163, 164
viewing history ................................................... 219
CVD Integrity report ............................................ 21, 212
CVDs
add to collection .................................................. 62
restore ............................................................... 168

D

Dashboard
capacity status .................................................. 205
collection compliance meter .................................. 204
Data Protection view ........................................... 204
efficiency benchmarks ........................................ 205
server status ...................................................... 204
system status ..................................................... 204
Update Progress view ......................................... 204
data protection ................................................... 23
desktop
monitor deployment ........................................... 203
operations ........................................................ 61
desktop management ........................................ 24
desktop policies .................................................. 55
rule macros ........................................................ 232
devices
reject pending ..................................................... 54
downloading peers .............................................. 111
Driver library caching ......................................... 21, 103
### N
- Network Client Throttling ........................................... 70
  - network operations
    - resuming .................................................... 109
    - suspending ................................................. 109
- NLB
  - default settings ............................................... 121

### P
- pending devices
  - reject ......................................................... 54
- policies
  - view ............................................................ 56
- prerequisites
  - hardware ...................................................... 28
  - software ....................................................... 28
- Provisioning
  - see Base layer provisioning ................................ 152
  - proximity, required .......................................... 106

### R
- Reference CVD ................................................... 19
- reference machine ................................................. 19
  - assign pending ............................................... 134
  - configuring .................................................... 133
  - recreating from Base Layer ................................ 148
  - software prerequisites ....................................... 28
  - supported operating systems ................................ 27
- rule macros ....................................................... 232

### S
- server storage capacity .......................................... 24
- Single-Instance Storage (SIS) ................................. 100
  - single-sign-on ................................................. 24
  - SIS integrity procedure ....................................... 100
  - Snooze .......................................................... 70
  - software prerequisites ........................................ 28
  - SSL .............................................................. 28
    - See Mirage Server system report
      - create ....................................................... 223
      - system status .............................................. 204

### T
- transaction log .................................................... 206
- transactions
  - types ........................................................... 206

### U
- upgrading from version 2.0 ..................................... 217

### V
- VMware Watchdog .................................................. 119
  - configuring ..................................................... 120
  - volume maintenance ......................................... 100

### W
- waiting peers ..................................................... 111
- WAN emulator ..................................................... 18
- Wizards ............................................................. 47