Legal Notice

Copyright © 2013 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® Horizon Mirage™.

This guide includes the following parts:

- **PART 1 - OVERVIEW**, provides a brief overview of Horizon 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 Horizon 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 App Layers and describes the Layer life cycle, including how Base Layers and App Layers are captured and deployed to endpoints.

- **PART 6 - DESKTOP OPERATIONS**, describes how to perform various operations such as endpoint disaster recovery, hardware migrations and migrating to Windows 7 from other Windows versions.
• **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 Horizon Mirage System, such as, setting up the SSL certificate in Windows Server, using Microsoft Office in a Layer, 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.

**Note:** Screen examples are sometimes cropped for better presentation on the page. Actual screen proportions in the Mirage Management Console may differ slightly.
# 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 Improvements in This Version ....................................................................................... 20
  1.5 Major Features in Previous Mirage Versions ............................................................... 21

Part 2 - Deploying the Mirage System ...................................................................................... 27

Chapter 2  Planning Your Deployment .................................................................................... 29
  2.1 Supported Operating Systems ....................................................................................... 29
  2.2 Software Prerequisites .................................................................................................. 30
  2.3 Hardware Prerequisites ............................................................................................... 31
  2.4 Database Prerequisites ............................................................................................... 32
  2.5 Ports Used by the Mirage System .............................................................................. 33

Chapter 3  Installing the Mirage System .................................................................................. 35
  3.1 Installation Overview ..................................................................................................... 35
  3.2 Configuring Third-Party Antivirus Software .................................................................. 36
  3.3 Installing the Mirage Management Server .................................................................... 36
  3.4 Installing the Mirage Management Console ............................................................... 38
  3.5 Connecting the Console to the Mirage System ............................................................ 39
  3.6 Managing Horizon Mirage Software Licenses .............................................................. 40
    3.6.1 Adding and Viewing Licenses .............................................................................. 41
  3.7 Installing a Mirage Server ............................................................................................ 42
  3.8 Minimum Configuration Requirements ....................................................................... 44
  3.9 Installing IIS and the Mirage File Portal ....................................................................... 44

Part 3 - Deploying Mirage to your Endpoints ......................................................................... 47

Chapter 4  Activating Endpoints .............................................................................................. 49
  4.1 Activation Overview ...................................................................................................... 49
  4.2 Installing the Mirage Client .......................................................................................... 49
  4.3 Common Wizards ......................................................................................................... 53
  4.4 Activating Endpoints ..................................................................................................... 55
### Table of Contents

7.3.4 USMT Settings Tab ................................................................. 90
7.3.5 Branch Reflectors Tab ............................................................. 91
7.3.6 License Tab ............................................................................. 92

#### Chapter 8 Managing the Driver Library ............................................. 93
8.1 Overview ....................................................................................... 93
8.1.1 Architecture .............................................................................. 93
8.1.2 Driver Library Application .......................................................... 94
8.2 Managing Driver Folders .................................................................... 95
8.2.1 Creating a Drivers Folder .............................................................. 95
8.2.2 Performing a Folder Operation ...................................................... 96
8.2.3 Importing Drivers into a Folder .................................................... 97
8.2.4 Adding a Driver to a Specific Folder from the All Folder ................. 98
8.3 Managing Driver Profiles ................................................................... 99
8.3.1 Creating/Editing Driver Library Profile .......................................... 99
8.3.2 Setting Driver Library ................................................................... 101

#### Chapter 9 Adding Multiple Volumes ................................................... 103
9.1 Multiple Volumes Overview ............................................................. 103
9.2 Using the Mirage Volumes Window ................................................ 104
9.3 Adding a Volume ............................................................................ 106
9.4 Editing the Volume Information ....................................................... 107
9.5 Removing a Storage Volume ............................................................. 107
9.5.1 Removing a Volume .................................................................... 107
9.5.2 Unmounting a Volume ................................................................. 108
9.6 Mounting a Volume ........................................................................ 108
9.7 Blocking a Volume .......................................................................... 108
9.8 Unblocking a Volume ...................................................................... 109
9.9 Volume Maintenance ........................................................................ 109

#### Chapter 10 Using Branch Reflectors ................................................... 111
10.1 Branch Reflector Overview ............................................................. 111
10.2 How Client Endpoints Use Branch Reflectors .................................... 112
10.2.1 Branch Reflector Selection Process ............................................. 112
10.2.2 Branch Reflector Cache .............................................................. 113
10.2.3 Branch Reflector Local File Sharing ............................................ 113
10.3 Installing a Branch Reflector ............................................................ 114
## 10.4 Enabling a Branch Reflector .......................................................... 114
## 10.5 Configuring Branch Reflectors ......................................................... 115
## 10.5.1 Setting Defaults for Branch Reflectors .......................... 115
## 10.5.2 Configuring Specific Branch Reflector Values ....................... 117
## 10.6 Disabling a Branch Reflector .......................................................... 118
## 10.7 Rejecting Peers .................................................................. 118
## 10.8 Accepting Peers .................................................................. 118
## 10.9 Suspending Network Operations ...................................................... 119
## 10.10 Resuming Network Operations ....................................................... 119
## 10.11 Monitoring Branch Reflectors and Peer Clients ....................... 120
## 10.11.1 Viewing CVD Activity and Branch Reflector Association .... 120
## 10.11.2 Viewing Branch Reflector and Peer Client Information .......... 121
## 10.11.3 Monitoring Branch Reflector and Peer Client Transactions .... 122

### Chapter 11 Deploying Additional Mirage Servers ......................... 125
## 11.1 Multiple Servers Overview ............................................................ 125
## 11.2 Using the Mirage Servers Window .............................................. 127
## 11.3 Adding a New Server ................................................................. 128
## 11.4 Stopping and Starting the Server Service ..................................... 128
## 11.5 Removing a Server .................................................................. 129
## 11.6 Integrating the Horizon Mirage System and Load Balancing .. 129
## 11.7 Configuring the VMware Watchdog Service ............................... 130

### Part 5 - Image Management .............................................................. 133

### Chapter 12 Image Management Overview ..................................... 135
## 12.1 Overview ........................................................................ 135
## 12.2 Traditional versus Mirage Image Management ....................... 135
## 12.2.1 Mirage Image-based Deployment and Update ..................... 137
## 12.3 Base Layers and App Layers ...................................................... 138
## 12.4 Layer Management Life Cycle ................................................. 139
## 12.5 Hardware Considerations with Base Layers ............................... 141
## 12.5.1 Virtual Machine Support ........................................................ 141
## 12.5.2 Special Case Hardware Drivers ............................................. 141
## 12.6 Planning and Preparation for Image Management .................... 141
## 12.6.1 Software Requiring Special Instructions ............................... 142
## 12.6.2 System Level Software .......................................................... 142
12.6.3 Software Licensing 142
12.6.4 User-Specific Software 143
12.6.5 OEM Software 143
12.6.6 Endpoint Security Software 144
12.6.7 BitLocker Support 144

Chapter 13 Preparing a Reference Machine ................................................................. 145
13.1 Setting Up a Reference Machine ........................................................................ 145
13.2 Software Considerations ...................................................................................... 147
13.3 Settings and Data Captured from Reference Machine ....................................... 148
13.3.1 System-wide Settings ..................................................................................... 148
13.3.2 Domain Membership and Login Settings ......................................................... 148
13.3.3 Selecting the Data for the Capture .................................................................. 149

Chapter 14 Capturing Base Layers .............................................................................. 151
14.1 Overview .............................................................................................................. 151
14.2 Working with Base Layer Rules ......................................................................... 152
14.3 Base Layer Override Policy ................................................................................ 155
14.3.1 Overriding Files ............................................................................................. 155
14.3.2 Overriding Registry Values ........................................................................... 156
14.3.3 Overriding Registry Keys .............................................................................. 156
14.4 Post-Base Layer Scripts ..................................................................................... 157
14.5 Capturing Base Layers ....................................................................................... 158
14.6 Recreating a Reference Machine from a Base Layer ........................................ 162

Chapter 15 Capturing Application Layers ................................................................. 163
15.1 Overview .............................................................................................................. 163
15.2 App Layer Capture Summary ............................................................................. 164
15.3 How to Prepare a Clean Reference Machine ...................................................... 165
15.4 How to Install Applications for Layer Capture ............................................... 166
15.4.1 Part 1 – Start App Layer Capture ................................................................ 166
15.4.2 Part 2 – Application Installation ................................................................ 169
15.4.3 Part 3 – Post-scan and Layer Creation .......................................................... 170
15.5 What can be Captured as Part of an App Layer ............................................... 173
15.6 Capturing OEM App Layers .............................................................................. 174
15.7 Capturing Multiple Layers on a Virtual Machine ............................................. 174
15.8 Configuring Post App Layer Deployment Scripts ............................................. 175
Chapter 16  Assigning Base Layers ................................................................. 177
  16.1 Overview ......................................................................................... 177
  16.2 Comparison Report between Layers and CVDs .................................. 178
    16.2.1 Comparing Base Layers to Each Other ...................................... 180
    16.2.2 Comparison Report Format ..................................................... 180
  16.3 Testing the Base Layer before Rollout .............................................. 183
  16.4 Updating (Assigning) a Base Layer to a CVD ................................... 183
    16.4.1 Monitoring the Update Progress ............................................. 188
  16.5 Updating Layers for All CVDs with Previous Version of those Layers .... 189
  16.6 Monitoring Layer Assignments ...................................................... 189
  16.7 Dealing with Conflicts .................................................................. 190
  16.8 Enforcing All Layers .................................................................. 191
  16.9 Base Layer Provisioning ............................................................... 192

Chapter 17 Assigning Application Layers .................................................... 197
  17.1 Overview ......................................................................................... 197
  17.2 Comparison Report between App Layers and CVDs .......................... 198
  17.3 Testing the App Layer before Rollout .............................................. 198
  17.4 Updating (Assigning) an App Layer to a CVD ................................. 198
    17.4.1 Monitoring the Update Progress ............................................. 203
  17.5 Monitoring Layer Assignments ...................................................... 203

Part 6 - Desktop Operations ................................................................. 205

Chapter 18 Endpoint Disaster Recovery ...................................................... 207
  18.1 Recovering from a Disaster ............................................................ 207
  18.2 Restoring CVD Snapshots ............................................................. 208
  18.3 Restoring a CVD Using the Disaster Recovery Wizard ....................... 212
  18.4 Mirage Boot USB Keys ................................................................. 220
    18.4.1 Prerequisites ........................................................................... 220
    18.4.2 Creating the Mirage Boot USB Key ........................................ 221
    18.4.3 Using the Mirage Boot USB Key ............................................. 223
    18.4.4 Customizing your Boot USB Key ............................................. 224
    18.4.5 Known Limitations ................................................................. 224
    18.4.6 Windows XP Boot USB Keys .................................................. 225
  18.5 Advanced Scenarios ..................................................................... 225
    18.5.1 Reconnecting a Device to a CVD ............................................ 225
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.6 User Experience with Restore Processes</td>
<td>226</td>
</tr>
<tr>
<td><strong>Chapter 19 Hardware Migrations</strong></td>
<td>229</td>
</tr>
<tr>
<td>19.1 Using the Hardware Migration Wizard</td>
<td>229</td>
</tr>
<tr>
<td>19.2 Planning for a Mass Hardware Migration</td>
<td>232</td>
</tr>
<tr>
<td>19.3 Performing a Mass Hardware Migration</td>
<td>232</td>
</tr>
<tr>
<td><strong>Chapter 20 Windows7 Migration</strong></td>
<td>235</td>
</tr>
<tr>
<td>20.1 Planning for a Windows 7 in-place Migration</td>
<td>235</td>
</tr>
<tr>
<td>20.2 Setting Up a Windows 7 Base Layer for Migration</td>
<td>236</td>
</tr>
<tr>
<td>20.3 Windows 7 Migration</td>
<td>237</td>
</tr>
<tr>
<td>20.3.1 Using the Windows 7 Migration Wizard</td>
<td>237</td>
</tr>
<tr>
<td>20.3.2 Migration Following “Only Download Base Layer”</td>
<td>242</td>
</tr>
<tr>
<td>20.3.3 Monitoring the Migration</td>
<td>245</td>
</tr>
<tr>
<td>20.4 Migration to Windows 7 Replacement Devices</td>
<td>246</td>
</tr>
<tr>
<td>20.5 Post-Migration Scripts</td>
<td>246</td>
</tr>
<tr>
<td>20.6 End User Experience During a Migration</td>
<td>247</td>
</tr>
<tr>
<td>20.6.1 Known Limitations</td>
<td>248</td>
</tr>
<tr>
<td><strong>Part 7 - Monitoring, Reporting, and Troubleshooting</strong></td>
<td>249</td>
</tr>
<tr>
<td><strong>Chapter 21 Monitoring Desktop Deployment</strong></td>
<td>251</td>
</tr>
<tr>
<td>21.1 Using the System Dashboard</td>
<td>251</td>
</tr>
<tr>
<td>21.1.1 System Status</td>
<td>252</td>
</tr>
<tr>
<td>21.1.2 Server</td>
<td>252</td>
</tr>
<tr>
<td>21.1.3 Update Progress</td>
<td>252</td>
</tr>
<tr>
<td>21.1.4 Data Protection</td>
<td>252</td>
</tr>
<tr>
<td>21.1.5 Compliance Meter</td>
<td>252</td>
</tr>
<tr>
<td>21.1.6 Capacity Status</td>
<td>253</td>
</tr>
<tr>
<td>21.1.7 Efficiency Benchmarks</td>
<td>253</td>
</tr>
<tr>
<td>21.2 Transaction Logs</td>
<td>254</td>
</tr>
<tr>
<td>21.2.1 Transaction Entry Properties</td>
<td>255</td>
</tr>
<tr>
<td>21.2.2 Search and Filter Results Specification</td>
<td>256</td>
</tr>
<tr>
<td>21.2.3 Total Transaction Records Limit</td>
<td>256</td>
</tr>
<tr>
<td><strong>Chapter 22 Mirage Reporting</strong></td>
<td>257</td>
</tr>
<tr>
<td>22.1 Mirage Reporting Overview</td>
<td>257</td>
</tr>
<tr>
<td>22.2 Generating a Report</td>
<td>258</td>
</tr>
<tr>
<td>22.3 Layer Dry-Run Reports</td>
<td>259</td>
</tr>
</tbody>
</table>
22.4 CVD Integrity Report ................................................................. 260

Chapter 23 Maintaining the Mirage System ............................................. 263
  23.1 Server Backup and Restore ....................................................... 263
  23.2 Upgrading from Previous Mirage Versions .................................. 265
    23.2.1 Before You Start ......................................................... 265
    23.2.2 Upgrade Procedure ..................................................... 266

Chapter 24 Troubleshooting ................................................................. 267
  24.1 Using the CVD History View .................................................... 267
  24.2 Using the Event Log .............................................................. 268
    24.2.1 Audit Events ............................................................... 268
  24.3 Customizing the Minimal Restore Set ........................................ 269
  24.4 Using the System Report Utility ............................................... 270
  24.5 Remote SysReport Collection .................................................. 271

Appendix .................................................................................................. 273
  A.1 Mirage and SCCM ...................................................................... 273
  A.2 Setting Up the SSL Certificate in Windows Server ...................... 274
  A.3 Using Microsoft Office 2010 in a Layer ..................................... 276
  A.4 User Role Definitions ............................................................... 277
  A.5 Managing Users and Roles Using AD Groups ............................ 278
  A.6 Working with Roles and Active Directory Groups ..................... 279
  A.7 Macros in Policy Rules ............................................................. 280

Index ........................................................................................................ 285
PART 1 - OVERVIEW

➢ In this Part...

1. Introduction
   1.1 Overview
   1.2 Key Concepts
   1.3 Solution Components
   1.4 Improvements in This Version
   1.5 Major Features in Previous Mirage Versions
Chapter 1
Introduction

In this Chapter...

1.1 Overview
1.2 Key Concepts
1.3 Solution Components
1.4 Improvements in This Version
1.5 Major Features in Previous Mirage Versions

1.1 Overview

Horizon 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**
  Horizon Mirage enables enterprise IT managers to centrally control the Base Layer and App Layers and guarantees a consistent view of the image at all endpoints. Administrators update a single Layer in the data center, and the new version of the Layer 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 and/or App Layers 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.

- **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 refresh that moves 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**

Horizon 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 five components:

- **Base Layer** defined by the Administrator, which comprises the operating system image plus core applications such as Anti-virus, Firewall, Microsoft Office.

- **App Layers** defined by the Administrator, which comprise sets of one or more departmental or line-of-business applications, and any updates or patches for already installed applications, suitable for deployment to a large number of endpoints.

- **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 or App Layers 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: Horizon Mirage Solution Components

The Horizon 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 and App 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 and App 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 Base Layer 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. A reference machine is also employed to capture App Layers, which contain departmental or line of business applications and any updates or patches for already installed applications.

  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 and App 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 or App 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 or App Layer updates or other Base or App 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 Improvements in This Version

This version includes the following improvements:

- **Endpoint centralization** - Performance improvement when a large number of endpoint centralizations are performed, by reducing the number of IO operations required from the storage.

- **License implementation** - Integration with VMware licensing. New licenses are provided as a serial-key instead of the former license-file.

- **Server 2012 support** – Mirage servers can now run on Windows Server 2012.

- **App Layering OEM support** - Mirage App Layering now also supports capture of OEM software, including drivers.

- **App Layering conflict report** - Reporting and usability improvements. Reports now take App Layers into account.

- **App Layering capture process improvements**.

- **App Layering update** – The administrator can easily send a new App Layer update to all CVDs that were previously assigned the former App Layer version.

- **Windows 7 migration usability improvements** – Operation progress can be monitored in the Windows login screen.

- **Active-Directory filtering** - You can create a filter for multiple Active-Directory elements (for example, filter CVDs whose users belong to the HR AD group or to the Marketing AD group).

- **Hardware Migration** - App Layers can be changed during hardware migration, for example OEM layer.
1.5 Major Features in Previous Mirage Versions

Earlier Horizon Mirage versions introduced the following key features that enable Administrators to better manage, support, and protect endpoints:

- **App Layers** – App Layers enable you to package departmental or line-of-business applications, and any updates or patches for already installed applications, in App Layers, for distribution only to specific groups/departments. The Base Layer can then include only core applications for general distribution.

  Layering granularity enables the packaging of core applications in the Base Layer, and departmental applications in any number of separate App Layers. App Layers can then be assigned to many desktops in any combination. If an application needs to be updated, the App Layer is patched once and all desktops are updated. The Base Layer “gold image” is kept clean, enabling the same Base Layer to be used for all desktops.

- **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 performed by the Centralize Endpoint function).

- **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.
- **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 endpoints can be optimized.
  - **Local file sharing** - The Branch Reflector can now share any files on its local disk with Client endpoints (as well as files that were downloaded from previous Base Layer 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 Layers from the hardware and helps the IT manager build Layers 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 Layers to apply corporate volume licensing to a device.

• **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 Layer 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 Layer, while retaining user data.
  • Enable removal of user-installed applications while ensuring compliance with assigned Base Layer 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 (rebase).
  • 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 Layer dry-run results to allow creating customized conflict resolution rules. These reports list the expected impact of a Base Layer download on applications and software modules in selected CVDs or CVD collections.

• **Deployment and Maintenance**
  - Simplify desktop management by leveraging the Horizon 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 System
   3.6 Managing Horizon 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 Vista Business or Enterprise, 32-bit and 64-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</td>
</tr>
<tr>
<td></td>
<td>an AD domain member. For further information, see</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. File Portal requires an IIS 7.0 (or later) installation as well as the IIS 6 Management Compatibility Role and ASP.NET feature (both options 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. Microsoft Management Console (MMC) version 3.0. (See <a href="http://support.microsoft.com/?kbid=907265">http://support.microsoft.com/?kbid=907265</a>)</td>
</tr>
<tr>
<td>Reference Machine</td>
<td>Horizon Mirage v4.0 Client. Operating system and applications installed on the reference machine must use volume licenses and be designed for multi-user, multi-machine deployment. The reference machine should not include: Applications that install and use hardware-specific licenses. Applications that install and use local user accounts and/or local groups. Software that uses a proprietary update service. Such software must be 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, Windows Vista or 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 equivalent.</td>
</tr>
<tr>
<td></td>
<td>▪ Minimum System Drive capacity: 146 GB.</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 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>
<tr>
<td>Mirage Storage</td>
<td>▪ Standalone Mirage Server:</td>
</tr>
<tr>
<td></td>
<td>• Direct Attached Storage (DAS).</td>
</tr>
<tr>
<td></td>
<td>• Storage Area Network (SAN) connected through iSCSI or Fiber Channel (FC).</td>
</tr>
<tr>
<td></td>
<td>• Network Attached Storage (NAS) connected through iSCSI, Fiber Channel (FC), or CIFS network share.</td>
</tr>
<tr>
<td></td>
<td>▪ Mirage Server Cluster:</td>
</tr>
<tr>
<td></td>
<td>• Network Attached Storage (NAS) connected using a CIFS network share.</td>
</tr>
<tr>
<td></td>
<td>▪ Alternate Data Streams:</td>
</tr>
<tr>
<td></td>
<td>• NAS via CIFS share <strong>must</strong> support Alternate Data Streams.</td>
</tr>
<tr>
<td></td>
<td>▪ Storage Capacity:</td>
</tr>
<tr>
<td></td>
<td>• Consumed capacity varies, depending on file duplication level across CVDs, Base Layers, and the number of snapshots stored, but VMware estimates <strong>on average</strong> each user requires 15 GB worth of data center storage.</td>
</tr>
<tr>
<td></td>
<td>▪ Enabling Compression:</td>
</tr>
<tr>
<td></td>
<td>• 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 <strong>MirageStorage</strong> folder. For NAS systems that are not NTFS you need to leverage their own compression options.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Management Console</td>
<td>▪ Minimum RAM: 512 MB.</td>
</tr>
<tr>
<td></td>
<td>▪ Network connectivity to the Mirage Management Server.</td>
</tr>
<tr>
<td></td>
<td>▪ Minimum screen resolution: 1280 x 1024</td>
</tr>
</tbody>
</table>
## 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></td>
<td><strong>Note:</strong> When installing SQL Server 2008R2 on Windows Server 2012 - Service Pack 1 or later must be installed, as described here: <a href="http://support.microsoft.com/kb/2681562">http://support.microsoft.com/kb/2681562</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. Note: 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. Note: 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 7.1 Configuring the Secure Sockets Layer (SSL/TLS), 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 System
3.6 Managing Horizon 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 Horizon 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 Horizon 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 Horizon 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
   \textbf{Note:} This requires IIS 7.0 or higher be installed on the Mirage server.

\section*{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).

\section*{3.3 Installing the Mirage Management Server}

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

\textbf{Note:} The procedure requires entry of the SQL Server name and the SQL Instance. MSSQL is available in one of three editions: Express, Standard and Enterprise. When installed with DEFAULT options, MS SQL editions use the following instance names:

- Express - SQLEXPRESS
- Standard - empty by default
- Enterprise - MSSQL

For the Standard edition, the instance name is empty by default, but displayed as MSSQLSERVER in the MS SQL management console.

In the entry field below, you must either:

- Enter the default instance name, as described above (if SQL was installed with default parameters)
- OR
- Enter the configured SQL instance name (if a custom instance name was configured during SQL installation)

\textbf{To install the Mirage Management Server:}

1. Double-click the \texttt{Mirage.management.server.x64.[BUILDNUMBER].msi} file. The \textit{Welcome to Mirage Management Server Setup Wizard} window appears. Click \textbf{Next}.

2. The \textit{End-User License Agreement} window appears.

Select I accept the terms in the License Agreement. Click \textbf{Next}.

\textbf{Note:} A copy of the End-User License Agreement is located in the installation directory for future reference.
3. The *Mirage Management Server configuration* window appears.

![Mirage Management Server configuration window](image)

4. Type the **SQL Server** name and the **SQL Instance**.

5. 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.

6. 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. Click **Next**.

7. The *Mirage services account configuration* window appears.

![Mirage services account configuration window](image)
8. 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. Click **Next**.

9. The *Ready to install VMware Mirage Management Server* window appears. 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.

10. 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.

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 Horizon Mirage Software Licenses

Horizon 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

If your license has expired, or in the case of a new Horizon Mirage installation, a license popup appears when you open the management console, which allows you to type the license-key directly.

Alternatively, this section describes how to add a license to Horizon Mirage or view existing licenses through the System Configuration settings.

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

➢ To add a license to Horizon Mirage:

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

2. Open the *License* tab. The number of CVDs currently licensed and the license expiry date are shown.

3. Select *Use license key* and type or paste the serial key.

4. 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.

Local Cache, referred to in the procedure below, is a storage of popular data blocks used by the Mirage Server to perform data deduplication over the WAN. When large files are transferred, their blocks are put into the cache and the next time similar files need to be transferred, the Mirage Server uses the cache to get the blocks instead of transferring them over the network. It is good practice to keep the cache on fast storage (e.g. local drive or even SSD drive).

**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:

1. Double-click the `Mirage.server.x64.[BUILDNUMBER].msi` file. The *Mirage Server Setup Wizard* window appears.
2. Click Next to begin the Mirage Server Setup Wizard.
3. The *End-User License Agreement* window appears. Select the I accept the terms in the License Agreement check box. Click Next.
4. The *Mirage Server configuration* window appears.

- Type the **SQL Server** name and the **SQL Instance**.
Installing a Mirage Server

- 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.
- Type a path and folder to where the local cache is stored, if different from the default.
- Type the size of the cache in megabytes. The recommended cache size is 100 GB (102400)

5. Click **Next**. The **Mirage service account configuration** window appears.

![Mirage service account configuration](image)

6. 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.

7. Type the password of the account to manage the Mirage services. Click **Next**.

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

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

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

10. 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.

**Note:** After the installation is completed, specific users may experience difficulty to access the file portal due to a local or domain security policy on IIS server(s). To allow those users to access the file portal, on the IIS server machine where the file portal is installed, add all users who need file portal access to the Allow logon locally policy under Local Security Policy - Local Policies - User Rights Assignments.

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]
- Security
  - Request Filtering
- Performance
  - [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.

6. Once IIS is installed properly, install the Mirage File Portal files. Double-click the **Mirage.WebAccess.x64.[BUILDNUMBER].msi** file (use the 32-bit installer file for 32-bit systems). The **Mirage Web Access Applications Setup Wizard** window appears.

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 Files using File Portal
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).

Note: Because you cannot place Horizon Mirage servers in the customer's DMZ premises, use a VPN to connect clients that will be used outside the network.
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.
**Installing the Mirage Client**

a. 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).

b. 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).

c. 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 icon](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:

```cmd
<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):

```cmd
<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.
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.

- **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. See 16.9 Base Layer Provisioning.

- **Disaster Recovery**: Restore a CVD to the same endpoint (e.g. in the case of a new hard drive or after a format) or restore to a replacement endpoint. See 18.3 Restoring a CVD Using the Disaster Recovery Wizard.

- **Hardware Migration**: Migrate a CVD to a different endpoint, either physical or virtual. See 19.1 Using the Hardware Migration Wizard.

- **Assign Base Layer**: Assign the appropriate Base 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. See 16.4 Updating (Assigning) a Base Layer to a CVD.

- **Update App Layer**: Assign and edit the application layers to a single CVD or a collection. The layers will be validated, and will be deployed to the selected endpoints as they connect to the network. See 16.4 Updating (Assigning) an App Layer to a CVD.

- **Capture Base Layer**: A Base 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 14.5 Capturing Base Layers.

- **Capture App Layer**: An App Layer is a set of one or more non-core organization applications (e.g. departmental or line-of-business) and updates/patches for already installed applications, for deployment to a large number of endpoints. See Chapter 15 Capturing Application Layers.

- **Windows 7 Migration**: Migrate an endpoint to Windows 7 from another Windows version (XP/Vista), preserving all end user data, while deploying desired Windows 7 applications as part of the new Base Layer. See 20.3.1 Using the Windows 7 Migration Wizard.
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 a 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**.
5. The Change Collections window appears. If you wish to add the device(s) to a collection, select the required static collection.

**Note:** A Collection is a folder that aggregates CVDs that share a logical grouping, for example, Marketing CVDs. This enables relevant Base Layer changes to be implemented with a single action on all CVDs in the collection. For more information, see 4.6 Working with CVD Collections.

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

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

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.

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.
4.4.2 Rejecting Pending Devices

You can reject a device that is Pending Assignment which you 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 18.2 Restoring CVD Snapshots).

The User area files and directories are also referred to in various Restore options described in 18.3 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 minutes). The default value is 60 minutes.
- **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 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 Viewing 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 4.5.1 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.

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 > Manage 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.

You can create a filter for multiple Active-Directory elements (for example, filter CVDs whose users belong to the HR AD group or to the Marketing AD group).

**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.
- Continue the procedure as described in 19.1 Using the Hardware Migration Wizard.
Chapter 5

End-User Operations

In this Chapter...

5.1 Client Status Window
5.2 File Level Restore
5.3 Directory Level Restore
5.4 Snooze
5.5 Sync Now

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 Recycle Bin 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.

![VMware Mirage 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 Recycle Bin:**

   1. Right-click the parent directory from where the file was deleted, and then select **Mirage Recycle Bin**.

      The *Mirage Recycle Bin* window appears.

      ![VMware Mirage Recycle Bin](image)

   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.

   ![VMware Mirage Restore Window](image)

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

3. Double-click the archive folder you want to restore. The *File Restore* window appears.
4. Click **Restore**. The *Browse to Folder* window appears.

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

   When the folder download is complete, the folder 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**.

![Snooze screenshot]

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 Files 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 Endpoints 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 Horizon 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 Horizon 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 Horizon 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.
   a. The Certificate Subject can be found in the details of the certificate you installed and is typically the FQDN of the Mirage Server.
   b. 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.
7.3.1 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, and the account used to join domains. You can also specify which upload policy to use when an end-user adds their CVD to the Mirage System.

![System Configuration window with General tab settings](image)
• **Snapshots**: Type the number of CVD snapshots the system will retain to be available for restoration - at hour, day, week, and month intervals. For example, “Number of snapshots at 1 day intervals” = 7 means 7 daily generations of CVD snapshot are retained and older generations are discarded. For more information about snapshots, see 18.2 Restoring CVD Snapshots.

• **Volumes**: This section configures the threshold percentages of data stored on a volume that will generate warning or critical events in the Events log. For more information about using multiple volumes, see 9.2 Using the Mirage Volumes Window.

  • **Volume capacity - warning threshold (%)**: Type the threshold percentages of data stored on a volume that will generate a warning event when the data stored on the volume reaches that threshold.

  • **Volume capacity - critical threshold (%)**: Type the threshold percent that will generate a critical event when the data stored on the volume reaches that threshold.

  • **Volume capacity check interval (seconds)**: Type the interval (in seconds) when the system checks the level of data stored on the volume.

  • **Driver Library and USMT files volume**: Choose the volume that will be addresses by the threshold checks by clicking **Change** and selecting the required volume.

• **CVDs**:

  • **CVD size warning threshold (MB)**: Type 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.

    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*.

### 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 sees when the end user is prompted for access.

![File Portal Tab Image]

The image shows the System Configuration window with tabs for General, CVD Auto Creation, File Portal, USMT, Branch Reflector, and License. The File Portal tab is in focus, showing the enable option, File Portal URL, and User message fields.
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:

- Migration to Windows 7 from another Windows version.
- 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 Branch Reflectors Tab

The System Configuration window Branch Reflector tab is used 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.

For the relevant procedures, see Chapter 10 Using Branch Reflectors.
7.3.6 License Tab

The *System Configuration* window License tab is used to add a license to Horizon Mirage or view existing licenses.

For more information, see Chapter 10 Adding and Viewing Licenses.
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 Layers 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 Layers and helps Administrators to build more generic Layers.

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 can 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

**Note:** Drivers must be extracted from the archive before importing them into the Mirage Management Console.

➢ **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](image)

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.
Managing Driver Profiles

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

Horizon 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.
    - **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.
  - **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.
- **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 two ways to remove a storage volume from the Mirage System: Remove and 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.
Chapter 10

Using Branch Reflectors

In this Chapter...

10.1 Branch Reflector Overview
10.2 How Client Endpoints 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 Endpoints 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 endpoints 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 for the specific endpoint.)

### 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 endpoints 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 endpoints. 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 to Windows 7 from another Windows version. 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 like a typical Mirage Client on any OS on which Mirage runs.

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 endpoints 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 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 cannot 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 Reflectors 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 Reflectors 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.
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 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 Horizon Mirage System and Load Balancing
11.7 Configuring the VMware Watchdog Service

11.1 Multiple Servers Overview

Horizon 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:

* VMware Horizon Mirage File Portal requires IIS 7.0 installed on the Mirage Servers.

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 Horizon Mirage System and Load Balancing.
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. It 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 Horizon Mirage System and Load Balancing

As there are many load balancers in the market today, Horizon 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, Horizon 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;VMware Horizon 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 Overview
   12.2 Traditional versus Mirage Image Management
   12.3 Base Layers and App Layers
   12.4 Layer Management Life Cycle
   12.5 Hardware Considerations with Base Layers
   12.6 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 and Data Captured from Reference Machine

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

15. Capturing Application Layers
   15.1 Overview
   15.2 App Layer Capture Summary
   15.3 How to Prepare a Clean Reference Machine
   15.4 How to Install Applications for Layer Capture
   15.5 What can be Captured as Part of an App Layer
   15.6 Capturing OEM App Layers
   15.7 Capturing Multiple Layers on a Virtual Machine
   15.8 Configuring Post App Layer Deployment Scripts
16. Assigning Base Layers
   16.1 Overview
   16.2 Comparison Report between Layers and CVDs
   16.3 Testing the Base Layer before Rollout
   16.4 Updating (Assigning) a Base Layer to a CVD
   16.5 Updating Layers for All CVDs with Previous Version of those Layers
   16.6 Monitoring Layer Assignments
   16.7 Dealing with Conflicts
   16.8 Enforcing All Layers
   16.9 Base Layer Provisioning

17. Assigning Application Layers
   17.1 Overview
   17.2 Comparison Report between App Layers and CVDs
   17.3 Testing the App Layer before Rollout
   17.4 Updating (Assigning) an App Layer to a CVD
   17.5 Monitoring Layer Assignments
Chapter 12

Image Management Overview

➣ In this Chapter...

12.1 Overview
12.2 Traditional versus Mirage Image Management
12.3 Base Layers and App Layers
12.4 Layer Management Life Cycle
12.5 Hardware Considerations with Base Layers
12.6 Planning and Preparation for Image Management

12.1 Overview

Horizon Mirage overcomes the limitations of traditional image-based update by extending the Image Layer concept for any image update - not just once during deployment, and by using separate application layer packages (App Layers) to distribute more specialized applications to specific groups of users.

This chapter describes the advantages of the Mirage approach and details the associated Base Layer lifecycle, introducing the Base Layer preparation, capture, update, and assignment processes used to synchronize endpoints described in detail in later chapters.

12.2 Traditional versus Mirage Image Management

Operating system (OS) and core application images are commonly deployed either by Individual installation and configuration of the OS on each physical endpoint, or Image-based deployment. The 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.
Image-based deployment involves the following steps:

1. Installing and configuring the OS and core applications on a reference machine.
2. Capturing the reference machine disk content into a generalized Base Layer.
3. Distributing the Base Layer to endpoints for installation over the network using, for example, a PXE boot, or distribution media such as a USB flash disk, or a DVD.
4. A setup procedure that instantiates the image to the specific machine’s hardware profile, assigned identity, and user settings.

Then, once a Base Layer is deployed and set up, subsequent changes to it or new applications can be delivered to the endpoints incrementally as individual packages.

However, over time, each endpoint’s image tends to diverge from the Base Layer on the reference machine. User-installed applications, plug-ins, and other customizations often overwrite elements of the Base Layer, leaving little resemblance between the endpoint contents and the Base Layer, and 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.

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, this simplistic approach has several challenges:

- The new Base Layer would remove all local personalization. User data needs to be backed up and restored - a costly and tedious procedure. User-installed applications and customizations then 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.
12.2.1 Mirage Image-based Deployment and Update

Horizon Mirage offers a new approach to current image-based update limitations, by extending the Base Layer concept. Mirage uses the Base Layer for any image update - not just once during deployment.

Whenever endpoints need to be updated, the Administrator just updates the reference machine, then 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 on the endpoints with the new Base Layer 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.

Mirage image-based deployment includes the following advantages over traditional image-based deployment:

- **Personalization Preservation**: Mirage decouples the desktop into distinct layers:
  
  a. **Base Layer**: Operating system, service packs, and 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.
12.3 Base Layers and App Layers

Horizon Mirage extends the Image Layer concept even further by introducing Application Layers (App Layers).

Traditional application organization typically comprises two “layers”:

- Core image layer with the handful of core apps used by everyone.
- PC layer with “one-off” individual user-installed applications

But low user-count departmental applications can make up most of a customer’s environment - too many to build into separate Base Layers. Multiple Base Layers (“gold image sprawl”) are hard to maintain and patch.

As well, installing applications one at a time in each user machine doesn’t scale.

Mirage provides layering granularity that enables packaging core applications in the Base Layer, and departmental applications in any number of separate App Layers. App Layers can then be assigned to many desktops in any combination. If an application needs to be updated, the App Layer is patched once and all desktops are updated. The Base Layer “gold image” is kept clean, enabling the same Base Layer to be used for all desktops.

Moreover:

- Delivering applications only to users who need them saves on installation and patching complexity and licensing costs.
- Departmental applications are no longer the responsibility of individual users to install and maintain.

An App Layer can be captured with a single application, or a suite of applications. App Layers can be deployed with other App Layers on any compatible endpoint.

App Layers are distributed in addition to and separate from the common Base Layer.

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

The Base Layer can still include applications directly. App Layers are not needed in organizations where everyone uses all the same applications.
12.4 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 OS, service packs and patches, as well as core enterprise applications and their settings. App Layers may also be defined to include more specific applications to groups of users. App Layers require a Base Layer to be present on an endpoint, but the Base Layer and any App Layers can otherwise be updated independently of each other.

The Base Layer or App Layer lifecycle is illustrated in the following figure. It begins with a reference machine, where Administrators create and maintain the Layer content.

1. The Administrator manages and revises the content that the Base Layer and App Layers should include through various operations on a reference machine, such as adding core or specific applications or patching the OS. For more information, see Chapter 13 Preparing a Reference Machine.

2. The Administrator performs a Base Layer or App Layer Capture from the reference machine using the Mirage Management Console. Mirage collects the data from the reference machine to create the Layer, which is generalized for mass deployment. The Layer is given a name and version. (Multiple captures can be made from the same reference machine, stored in the Mirage Server’s Layer repositories.) For more information, see Chapter 14 Capturing Base Layers, and Chapter 15 Capturing Application Layers.
3. The Administrator then initiates Base Layer or App Layer assignment (update) from the *Mirage Management Console*.
   
a. This operation first distributes and stores the revised Layer at each endpoint, ready to be applied.
   
b. Following a reboot of the endpoint, the Base Layer or App Layer assignment (update) automatically swaps the old Base or App Layer on the endpoint with the new one, thereby assigning the Layer to that endpoint. The Base Layer, or specific applications in the App Layer, are instantiated on the endpoint.

   For more information, see 16.4 *Updating (Assigning) a Base Layer to a CVD* and 17.4 *Updating (Assigning) an App Layer to a CVD*.

4. The changes in an endpoint resulting from the Layer update process are automatically propagated back to the endpoint’s CVD on the server. After the CVD is synchronized with the latest changes, the 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 or an App Layer, the process begins again by generating a new version of the Layer.

The management lifecycle for Base Layers 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.
12.5 **Hardware Considerations with Base Layers**

Administrators can 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.

**12.5.1 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 virtual machine 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).

**12.5.2 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.

**12.6 Planning and Preparation for Image Management**

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

This section describes various software considerations for image management. For additional software aspects, see **13.2 Software Considerations**.
12.6.1 Software Requiring Special Instructions

The following categories of software require special instructions:

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

12.6.2 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 the minimal restore set includes the organization VPN, antivirus, firewall applications, as well as the driver store.

12.6.3 Software Licensing

The Base Layer should include core applications used by an organization, while more specialized applications can be distributed via App Layers. 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 or App 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.
12.6.4 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 should be excluded from the Base Layer and should not be distributed. Software installed exclusively for a specific user should not be distributed as it 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 should be excluded from the Base Layer.

12.6.5 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.

Use App Layering for OEM software.
12.6.6 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 use 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 with or manipulate the operation of these security products, and does not override the security measures they provide.

12.6.7 BitLocker Support

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

**Note:** After using BootUSB to do bare metal restore, the BitLocker state is not preserved (the machine will not be encrypted).

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 will fail.
Chapter 13

Preparing a Reference Machine

➤ In this Chapter...

13.1 Setting Up a Reference Machine
13.2 Software Considerations
13.3 Settings and Data 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. For more about the Image Layer deployment process, see 12.4 Layer Management Life Cycle.

After 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.

This chapter describes the preparation of a reference machine that will be used to capture a Base Layer.

The reference machine used for App Layer capture does not generally require advance preparation. Certain guidelines apply for special circumstances. A Base Layer does not have to be present on the machine.

Note: Files and settings from the reference machine are captured in the Base Layer, which are 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 device as a reference CVD:

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.

3. The Select Upload Policy window appears. Select the required upload policy and click Next.
4. The Select a Base Layer window appears. Select Don’t use a Base Layer. As this is a first-time use, there is no existing Base Layer. In future, you can select an existing Base Layer to apply updates and modify content. Click Next.

5. The Select Target Volume window appears. Specify whether you want to automatically choose a volume or to select one manually. Click Next.


7. The device is moved from the Pending Devices list to the Reference CVDs view.

13.2 Software Considerations

When you capture a Base Layer, the software that is installed on the reference machine becomes part of that Layer. When you deploy the Layer to other endpoints, this software is delivered to the endpoints as well (as part of that 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 the reference machine you can only 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
• 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.

For additional software aspects, see 12.6 Planning and Preparation for Image Management.

13.3 Settings and Data Captured from Reference Machine

This section applies to Base Layer capture only.

13.3.1 System-wide Settings

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 14.3 Base Layer Override Policy.

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

Examples of settings included in the reference machine: Power Management, Remote Desktop Settings, and 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 can log on). In addition, ensure that the Net Logon service is set to start automatically.
13.3.3 Selecting the Data for the Capture

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 14.3 Base Layer Override Policy.
Chapter 14
Capturing Base Layers

➢ In this Chapter...

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

14.1 Overview

After a reference machine is set up with what the Base Layer should contain, the Administrator can prepare to capture the Base Layer from the reference machine to enable updating endpoints with that Base Layer. For more about the Base Layer deployment process, see 12.4 Layer Management Life Cycle.

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

A similar process is employed to capture Application Layers. For details, see Chapter 15 Capturing Application Layers.
14.2 Working with Base Layer Rules

By default, the entire reference machine content is applied to the Base Layer.

Rules can be defined to exclude specific content on the reference machine from being captured for the Base Layer (and include specified subsets of the excluded content). As well, Override policies can be defined to prevent specific endpoint content from being overwritten by the Base Layer.

The system comes with a built-in default rule set for production use. You can define a draft rule set, or edit any rule set. You can test a draft rule set, and when you are satisfied, define it as the default. Only the rule set currently defined as the default applies for Base Layer Capture purposes.

When a draft rule set is being tested, only the selected CVD is affected. Other CVDs still use the default rule set, hence the production environment is not affected.

➢ To view existing Layer rule set details:

1. In the Mirage Management Console, expand the Image Composer node.
2. Click Layer Rules. The Layer rule sets are listed in the right pane.
3. Right-click the Layer rule set you want to view, and then select Properties.

A read-only Layer Rules Details window appears which shows the rule details.
To create a new Layer rule set based on an existing rule set:

1. Open the list of Layer rules, as described in To view the Layer rules.
2. In the Mirage Management Console, expand the Image Composer node.
3. Right-click any Layer rule set, then select **Clone**.

The Add Layer Rules window opens a copy of the selected rule set with its original details, and a new name, which you can modify.

The Add Layer Rules window is displayed, with details of the current rule set.

- The **Do Not Download** section **Rules** list defines the files and directories on the reference machine that should **not be applied** to the CVD.

- The **Rule Exceptions** list shows specific files and directories within directories in the Do Not Download Rules list which should be applied. For example, suppose you want to apply only certain system DLLs within C:\Windows.
  - First exclude all C:\Windows\* by entering this in the **Rules** list.
  - Then enter specific files (e.g. at c:\Windows\system32\myapp.dll) in the **Rule Exceptions** list.

  All other files not matching a rule in the Rules list will be applied to the CVD.

- Click **Show factory rules** to view the Mirage mandatory settings that cannot be changed by the IT manager. Factory rules appear grayed out in the rules list.
4. To edit an existing rule or rule exception in the rule set:
   a. To add a new rule or a rule exception to the rule set, click the Add button
      next to the relevant list. The Edit Rule window appears with empty input
      fields.
   
   ![Edit Rule Window]
   
   b. Enter the rule or exception details and click OK.

5. To edit an existing rule or rule exception in the rule set:
   a. Select the rule or rule exception line, and click the Edit button next to the
      relevant list. The Edit Rule window appears as in the previous step, with
      details of the selected rule.
   b. Correct the rule or exception details and click OK.

6. To remove a rule or an exception, select the rule or exception line and click the
   Remove button next to the relevant list.

7. When you are finished working with this rule set, click OK to close the Add Layer
   Rules window.

8. The new Layer rule set marked as Draft is listed in the Layer Rules list.

You should test the edited rule set as a draft on several Base Layers (see procedure
below). When you are satisfied with the changes, you can define the new Layer rule
set as the Default rule set (see procedure below).

➢ To test a draft Layer rule set on a test machine:

1. Open the list of Layer rules, as described in To view the Layer rules.
2. Right-click the Layer rule set you want to test and select Test Rules Draft.

   **Note:** Only rule sets with Draft status can be tested with this option. To test
   changes to the Default rule set, it is recommended to first create a clone of that
   rule set (see To create a new Layer rule set.) with the desired changes for
   testing, then define that new rule set as the Default if the testing is satisfactory.

3. Select the CVD on which you want to test the selected Layer rules and click Next.
4. Select the Base Layer you want to use for the test.
5. Click Finish.

➢ To define a Draft rule set as the Default rule set:
   1. Open the list of Layer rules, as described in To view the Layer rules.
   2. Right-click a Draft rule set and select Set As Default.

14.3 Base Layer Override Policy

The Mirage policy includes an option to override Base Layer content in order 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. The rule can also be applied for setting registry values and registry keys. See the sections below for examples.

➢ To add a Do Not Override by Base Layer rule:
   1. Open the list of Layer rules, as described in To view the Layer rules.
   2. Scroll to the Do Not Override By Base Layer section.

The Do Not Override by Base Layer rules syntax is the same as for Layer rules.

14.3.1 Overriding Files

➢ 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 the “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 the user configuration.

Without a Base Layer Override policy, each Base Layer Update or Enforce All Layers operation 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.

14.3.2 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.

14.3.3 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.
14.4 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 zero.
14.5 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.

You can capture the Base Layer from an existing reference CVD, or a new reference CVD as a new source of layer capture.

**Note:** When creating a Base Layer to be used in a Windows 7 migration, refer to requirements described in 20.2 Setting Up a Windows 7 Base Layer for Migration.

➢ To capture a Base Layer:

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

   ![Capture Base Layer](image)

   **Tip:** You can also start the process by right-clicking the required CVD in any CVD view and selecting **Capture Base Layer**. Then skip forward to Step 4 below.

2. The **Select Capture Type** window opens. Select:
   - **Use an existing reference CVD** if you want to capture a Base Layer from an existing CVD. In this case, please skip forward to Step 4.
     OR
   - **Create a new reference CVD** if you want to create a new source of layer capture. In this case, perform step 3, then continue to Step 5.
3. If you selected **Create a new reference CVD**:

   a. Select the pending device you want to use. Click **Next**.

   b. The wizard displays the properties of the selected pending device. Select the upload policy you want to use for this reference CVD. Click **Next**.
4. If you selected **Use an existing reference CVD:**
   The *Select a Reference CVD* window opens. Select the reference CVD from which you want to capture the Base Layer. Click **Next.**

5. The *Capture Base Layer* window opens. Select:
   - Create a new layer and specify the new Base Layer details.
   - OR
   - Update an existing layer and select the Base Layer to update. Click **Next.**
6. A validation window appears which checks the reference machine for possible problems. If problems are reported, you can fix them and then click the Refresh button to see if they are resolved. After the problems are resolved, click Next.

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

8. A Summary window opens. Click Finish to start the capture process.
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.

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

You can now apply the capture to endpoints. See Chapter 16 Assigning Base Layers.

14.6 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 core 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 14.5 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

Capturing Application Layers

➣ In this Chapter...

15.1 Overview
15.2 App Layer Capture Summary
15.3 How to Prepare a Clean Reference Machine
15.4 How to Install Applications for Layer Capture
15.5 What can be Captured as Part of an App Layer
15.6 Capturing OEM App Layers
15.7 Capturing Multiple Layers on a Virtual Machine
15.8 Configuring Post App Layer Deployment Scripts

15.1 Overview

This chapter describes the VMware Horizon Mirage application layer concept and provides guidelines to ensure successful application layer creation.

Sets of more specialized applications can be provided to specific users through App Layers, independent of the core applications that are generally distributed with the common Base Layer.

An App Layer can be captured with a single application, or a suite of applications from the same vendor. App Layers can be flexibly created to include applications relevant for a specific department or group. App Layers can be combined with other App Layers and deployed on any compatible endpoint.

App Layers are defined and delivered by a two-step process of App Layer capture, as described in this chapter, and update to endpoints, described in Chapter 17 Assigning Application Layers.

The App Layer Capture process creates a point-in-time snapshot of designated applications installed on a live reference machine, which is generalized for mass deployment. It is Wizard driven and similar to the Base Layer Capture process.

Any CVD can be used as the reference CVD for App Layer purposes. A Base Layer does not need to be present on the reference machine.

For more about Application Layers, see 12.3 Base Layers and App Layers.

For more about Layer deployment, see 12.4 Layer Management Life Cycle.
15.2 App Layer Capture Summary

The steps below describe how to capture a single App Layer. For information about capturing multiple App Layers, see 15.7 Capturing Multiple Layers on a Virtual Machine.

1. **Prepare the reference machine:** A clean reference machine is required for capturing an App Layer. A virtual machine is suitable for capturing most applications. For more information, see 15.3 How to Prepare a Clean Reference Machine.

2. **Capture the pre-install state:** Once the reference machine is ready, invoke the Start App Layer Capture wizard to capture the pre-installation state of the machine. For more information, see 15.4 How to Install Applications for Layer Capture - Part 1 – Start App Layer Capture.

3. **Install the applications:** You then install the applications to be captured, apply any application updates and patches, and customize global settings or configurations. For more information, see the following sections:
   - 15.4 How to Install Applications for Layer Capture - Part 2 – Application Installation.
   - 15.5 What can be Captured as Part of an App Layer.
   - 15.6 Capturing OEM App Layers.
   - Note about application upgrades, below.

4. **Capture the post-install state:** Once applications are installed, updated and configured as desired, use the Finalize App Layer Capture wizard to complete the capture. This will upload the App Layer to the Mirage server and add it to the list of available App Layers in the Mirage Management Console (MMC). For more information, see 15.4 How to Install Applications for Layer Capture - Part 3 – Post-scan and Layer Creation.

5. **Test the App Layer deployment:** Before deploying App Layers to many endpoints, it is good practice to test each captured App Layer by deploying it to a selected sample of target endpoints to verify that the applications work as expected on these endpoints after deployment. In upcoming versions of Mirage, conflict reports will help to identify conflicts between App Layers and user-installed applications on the target endpoints.

6. **Deploy the App Layer:** Once testing is completed, the App Layer is ready for deployment to any selected collection of target endpoints. To deploy App Layers, use the Update App Layers wizard for a selected CVD or CVD collection in the MMC.
Note about application upgrades: When a new version of an application is available, you can replace the existing App Layer with a new layer. To do this, you capture the upgraded application in an App Layer (together with any other applications or updates required at that time) by the same process as described above (starting with a clean reference machine and capturing the installed new application). Once you have a new App Layer, use Update App Layers to replace the old App Layer with the new App Layer.

15.3 How to Prepare a Clean Reference Machine

The reference machine used for App Layer capture does not generally require advance preparation. Certain guidelines apply for special circumstances, as described in this section.

- A virtual machine is suitable and good practice for capturing most App Layers (except for hardware-specific App Layers).

- The first step in capturing an App Layer is to prepare a reference machine with a clean (“vanilla”) installation of the required OS (e.g. Windows XP, Windows 7 32-bit or Windows 7 64-bit).

- App Layers can only be deployed to compatible OS versions. Thus, App Layers need to be captured separately for Windows XP, Windows 7 32-bit and Windows 7 64-bit. An App Layer captured on Windows XP cannot be deployed on a Windows 7 (32-bit or 64-bit) machine, and vice versa. Similarly, an App Layer captured on Windows 7 32-bit can’t be deployed to Windows 7 64-bit, and vice versa.

- Avoid software in the clean state of the reference machine:
  - That can cause changes to be made to the machine while you are installing the applications.
  - That is auto-updating. If this is not possible, try to disable the auto-update feature of any pre-existing software. For example, turn off automatic Windows Update installation and automatic anti-virus definition updates.

- If you plan to capture a .NET-based application which uses a version of .NET not included in the vanilla Windows OS you installed, it is good practice to install the required .NET framework in the clean reference machine before starting the capture and installing your application. Deliver the .NET framework itself via the Base Layer, if possible.

- It is generally good practice for the clean reference machine to be similar in content to the Base Layers used throughout the organization (e.g. with the same Windows service pack version and .NET framework version as the Base Layer).
Once the clean reference machine has been set up,

1. Install the Mirage client on the reference machine. The VM device will be “Pending Assignment” in the MMC.
2. Restart the reference machine. (Restarting assures best scan performance when capturing App Layers.)
3. Continue to capture the pre-install state of the machine - see 15.4 How to Install Applications for Layer Capture - Part 1 – Start App Layer Capture.

15.4 How to Install Applications for Layer Capture

The App Layer Capture process involves three stages:

- **Part 1 – Start App Layer Capture.** This part performs a “Pre-scan” that creates a “Before” image of the reference machine before the required applications are installed.
- **Part 2 – Application Installation.** The required applications are then installed by the Administrator on the reference machine that was selected in Part 1.
- **Part 3 – Post-scan and Layer Creation.** This part creates a “After” image of the reference machine, after the required applications are installed. It then detects all changes following the installation and starts the Capture process.

15.4.1 Part 1 – Start App Layer Capture

Once a clean reference machine is ready with the Mirage client, use the Start App Layer Capture wizard to capture the pre-installation system state. The wizard runs a series of validations to check that the machine is ready for capture. Follow the on-screen instructions to remove any validation warnings or errors.

Any CVD can be used as the reference CVD for App Layer purposes. A Base Layer does not need to be present on the reference machine.

➢ To start the App Layer Capture:

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

   ![Capture App Layer](image)

   **Tip:** You can also start the process by right-clicking a pending device in the Pending Devices view, selecting **Create a new Reference CVD** and choosing **Create Reference CVD for App Layer capture**. Then continue from Step 3.
2. The Select a Pending Device window opens. Select the pending device from which you want to capture an App Layer and click **Next**.

3. 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.

4. A validation window appears which checks the reference machine for possible problems. Follow the on-screen instructions to remove any validation warnings or errors. Click **Next** to continue.

5. A Summary window opens. Click **Finish** to start the Pre-scan capture process.

6. 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.
When the task is complete, the App Layer is moved to the App Layers list under the Image Composer node.

7. The Pre-scan processing starts. A progress window shows the Pre-Install State Capture progress. Balloon popups advise the process stage.

The Task Monitoring window shows a Capture App Layer task, which enables you to monitor the operation progress and status.

During the pre-scan process, the Mirage client will display the following window, indicating that the pre-scan is in progress:

When the “finished capturing pre-installation system state” balloon popup appears, you can continue to Part 2.

Note: If you miss the balloon, ensure that the “red recording” icon appears on the Mirage icon before you start installing applications.
15.4.2 Part 2 – Application Installation

The Mirage client notifies that the system is ready for application installation.

You now install all the applications required to be captured for the App Layer on the reference machine that was selected in Part 1. This includes applying application updates and patches to the installed applications, and customizing global settings and configurations as needed.

➢ To install applications for the capture:

The CVD remains in a “recording” mode until Part 3 processing is started, which signals that application installations were completed.

If the reference machine is rebooted for any reason, the console will remind you that recording is still in progress and that you should complete application installation.

After all the required applications are installed and tested on the reference machine, you can proceed to Part 3.

Guidelines for the application installation process:

- Mirage does not capture application installations or configuration changes made for specific user profiles for an App Layer. Whenever applications (such as Google Chrome) give options to install (or set shortcuts), for either a specific user or globally for all users, always choose the “all users” option so that these installations/ configurations will be captured as part of the App Layer.

- When installing applications, do not make any changes that are not wanted in the capture. For example:
  - Avoid installing software updates or applications that you don’t want to capture.
  - Avoid hardware changes, domain membership changes and any other configurations which are not required.
  - Avoid launching other applications/Windows components which are not required by the installation process of the application you want to capture.
  - Avoid GPO scripts running on the machine during the recording phase.
  - To reduce intra-vendor conflicts, it is good practice to install applications of the same vendor in the same single App Layer.
Whenever possible, install software which can be volume-licensed and doesn’t require hardware-bound licensing/activation. Delivering hardware-bound licensed applications via App Layers will usually trigger re-activation of the software on the endpoints.

**Important:** Any file/registry change that you make inside the captured area (this area can be configured by the Mirage policy), will be part of the App Layer and applied to endpoints when you deliver the App Layer. Avoid putting sensitive information in the reference machine used for capturing App Layers.

### 15.4.3 Part 3 – Post-scan and Layer Creation

This part performs a “Post-scan” of the reference machine, creating an “After” image after the required applications are installed. The process then detects all changes following the installation and starts the final capture process.

Invoke the capture finalization wizard only after you complete installation of your application(s), updates and configuration changes, including any machine restarts required by the application installer. Do not start the finalization process before all installations have been successfully completed. Follow the on-screen instructions in the finalization wizard to handle any validation warnings or errors.

During the post-scan process, the Mirage client indicates the progress of the post-scan.

To finalize the capture:

1. In a **Reference CVD** view, select the same reference CVD as in Part 1, right-click and select **Finalize App Layer capture**. (This can also be done from the Task view.)
2. The Review Recorded Applications list opens, where you will review the applications to be captured. Click Next.

```
<table>
<thead>
<tr>
<th>Display Name</th>
<th>Display Version</th>
<th>Install Location</th>
<th>Publisher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skype™ 5.10</td>
<td>5.10.114</td>
<td>C:\Program Files\Skype</td>
<td>Skype Technologies S.A.</td>
</tr>
</tbody>
</table>
```

Selecting the Show Updates checkbox displays any hot fixes for Windows that were installed in the recording phase.

3. The Capture App Layer window opens. Select:

- **Create a new layer** and specify the new App Layer details.
  OR
- **Update an existing layer** and select the App Layer you want to update.

Mirage automatically detects if a new App Layer will be an update of existing App Layer based on installed application upgrade codes. In this case the Update an existing layer option is selected by default. You can change the selection if needed.

Click Next.
4. A **Validation** screen opens. Follow the on-screen instructions to remove any validation warnings or errors. Click **Next** to continue.

![Capture App Layer]

Check Compatibility

**Validations**

- No compatibility issues detected

![Capture Layer]

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

![Capture App Layer]

6. A **Summary** screen opens. Click **Finish** to start the capture conclusion processing.

The **Task** list shows the task is completed.

The new App Layer appears in the **App Layers** list.

You can now apply the capture to endpoints. See *Chapter 17 Assigning Application Layers*. 
15.5 What can be Captured as Part of an App Layer

An App Layer can contain:

- A single application or a set of applications.
- Any updates or patches related to the installed applications.
- Global application configurations and settings.
- Any custom set of files and registry entries.

For example, an App Layer can contain Adobe Reader, Microsoft Visio 2010 or the entire Microsoft Office 2010 suite. An App Layer can also be used to capture OEM software (e.g. the Dell software suite, including any drivers and utilities).

Unlike some application virtualization solutions, Mirage App Layers can also contain any of the following elements:

- Windows services
- Kernel drivers
- Shell integration components (e.g. shell extensions)
- Browser plug-ins
- COM objects
- Global .NET assemblies

The following components cannot yet be delivered as part of Mirage App Layers:

- User accounts and groups (both local and domain users) and any user-specific changes
- OS components or OS-bundled applications (e.g. the .NET framework, Windows updates, Internet Explorer, Windows Media Player, language packs)
- Windows license

**Note:** The components mentioned in the last two bullets can be delivered as part of a Base Layer instead.

The following applications are currently not or partially supported for delivery as App Layers:

- Disk encryption software
- Any application which makes changes to the Master Boot Record or to disk blocks
- Kaspersky Internet Security
- Microsoft SQL Server
It is good practice to install the following applications in the Base Layer and not in App Layers:

- Windows security applications (e.g. anti-virus, anti-malware, firewall)
- Windows components/frameworks (e.g. .NET, Java)
- Global Windows configuration/settings changes

## 15.6 Capturing OEM App Layers

To successfully capture hardware-specific software (e.g. Dell/HP application and driver suite), please follow these guidelines:

- Some vendors provide a single OEM application suite which is compatible with many or most of their hardware models. It is good practice to use this suite for the OEM layer capture.
- If the vendor only provides an OEM suite which is relevant for a specific hardware model or model line, make sure you install the OEM software on the hardware model for which it is intended or on a compatible model.
- Unlike OEM applications, which can only be delivered via app or Base Layers, Mirage provides several ways to deliver OEM device drivers to target endpoints:
  - **Via the Mirage driver library:** See the *VMware Horizon Mirage Administrator’s Guide* for detailed instructions on how to deliver device drivers to specific hardware models in a rule-based manner.
  - **Via Base or App Layers:** In this method, you either install or place all relevant device driver packages in the reference machine, in a path which is also defined in the Windows DevicePath registry value. You can also install the corresponding OEM applications in the same reference machine. A base or App Layer is then captured from the reference machine in the usual way. This layer can be used to deploy OEM applications and drivers to any endpoint of the matching hardware models.

## 15.7 Capturing Multiple Layers on a Virtual Machine

When you need to capture multiple App Layers, it is useful to use a single virtual machine (VM). The following steps describe this process:

1. Create a clean reference machine on a VM, install the Mirage Client and centralize the device to a reference CVD. For more information, see 15.3 How to Prepare a Clean Reference Machine.
2. Take a snapshot of the VM in this state (e.g. “Clean State”).
3. In the MMC, use the Start App Layer Capture option to capture the pre-install state. For more information, see 15.4 How to Install Applications for Layer Capture Part 1 – Start App Layer Capture.

4. Install the desired applications. For more information, see:
   - 15.4 How to Install Applications for Layer Capture - Part 2 – Application Installation.
   - 15.5 What can be Captured as Part of an App Layer.
   - 15.6 Capturing OEM App Layers.

5. In the MMC, use the Finalize App Layer Capture option to complete the creation of the App Layer. For more information, see 15.4 How to Install Applications for Layer Capture - Part 3 – Post-scan and Layer Creation.

6. Wait until the App Layer appears in the “App Layers” view of the MMC.

7. Revert to the VM to the “Clean State” snapshot.

8. Wait for the device to become “Pending Assignment” and go back to Step 3 to capture the next App Layer.

15.8 Configuring Post App Layer Deployment Scripts

In rare cases, you might need to execute a custom script after the App Layer is deployed, for example, to apply a specific application license after it is installed via an App Layer.

➢ To have the Mirage client execute a custom script:

1. Invoke the App Layer Capture wizard in the usual way to complete a pre-scan of the reference machine.

2. Install the application to be captured in the usual way.

3. Give your script a unique name with this pattern: post_layer_update_* .bat
   (for example: “post_layer_update_myappv2_license.bat”)

4. Copy this script into “%programdata%\Wanova\Mirage Service”.
   This path usually translates into:
   - “c:\ProgramData\Wanova\Mirage Service” (Windows 7)
   - “c:\Documents and Settings\All Users\Application Data\Wanova\Mirage Service” (Windows XP)

5. Run the Finalize App Layer Capture wizard in the usual way to complete the post-scan and the creation of the App Layer.

6. After the App Layer is deployed to an endpoint, Mirage automatically launches your script.
Chapter 16
Assigning Base Layers

> In this Chapter...

16.1 Overview
16.2 Comparison Report between Layers and CVDs
16.3 Testing the Base Layer before Rollout
16.4 Updating (Assigning) a Base Layer to a CVD
16.5 Updating Layers for All CVDs with Previous Version of those Layers
16.6 Monitoring Layer Assignments
16.7 Dealing with Conflicts
16.8 Enforcing All Layers
16.8 Base Layer Provisioning

16.1 Overview

After Base Layer Capture is completed, the revised Base Layer is distributed and stored at each endpoint desktop, then applied (assigned) at each endpoint.

Assigning a Base Layer to an endpoint (or collection of endpoints) applies the contents of the Base Layer to the designated endpoint(s). This means that after assignment any applications or updates/patches built into the Base Layer will also reside on the endpoint device. For more information, see 16.4 Updating (Assigning) a Base Layer to a CVD.

Similar processes are employed to assign applications associated with App Layers to endpoints. For details, see 17.4 Updating (Assigning) an App Layer to a CVD.

For more about the Base Layer deployment process, see 12.4 Layer Management Life Cycle.
16.2 Comparison Report between Layers and CVDs

Before applying a new Base Layer and/or replacing App Layers for a CVD or collection of CVDs, you can run a report that describes the potential effects of applying the Base and/or replacing the App Layers on the CVD. This report can help you plan the Layer update process, and resolve in advance conflicts that might result from any mismatches in the Layer contents on the selected CVDs.

The report is in HTML format and you can use Excel to easily view it and filter data. See 16.2.2 Comparison Report Format for more information about the report.

➢ To describe the potential effects of Layer Changes on selected CVDs:

1. In the Mirage Management Console, right-click a single CVD or a collection, or select multiple CVDs (by pressing Ctrl and selecting CVDs with the pointer) and right-click one of them.

2. From the shortcut menu, select Programs > Compare Programs with Layer.

3. The Select a Base Layer page appears showing all the available Base Layers. Decide on the Base Layer that will apply to the analysis:
   - Select **No change to the target Base Layer** if you want the current analysis to analyze only App Layer changes, and click Next. OR
   - Select **Select Base Layer from list** to apply a new Base Layer to all the selected CVDs. Then select the required Base Layer and click Next. (The selected CVDs might currently have different Base Layers and this option will have the effect of standardizing the Base Layer over all the CVDs.)
4. The **Select App Layers to be included in the report** page appears.

   The **Available Layers** panel lists the available App Layers that are not currently used by any of the selected CVDs. (When **Show only latest layers** is selected, older versions of any software are suppressed from the view.)

   The **Assigned layers** panel lists the App Layers currently used by some or all the selected CVDs. (Black lines denote App Layers used by all the CVDs, gray lines denote App Layers that are used by only some of the CVDs.)

   ![Comparison Report between Layers and CVDs](image)

   - If you only want to analyze a Base Layer change without App Layer changes, click **Finish** without making any changes in this page.
   - To add App Layers to all the selected CVDs, select lines in the Available Layers panel and click the Right-arrow.
   - To remove App Layers from all the selected CVDs where they are used, select lines in the Available Layers panel and click the Right-arrow.

   Click **Finish** to continue.

5. The HTML report is generated and opened in your default web browser.
16.2.1 Comparing Base Layers to Each Other

You can also produce a comparison report that describes the differences between the contents of one or more Base Layers and a selected Base Layer. The same format of report is generated, but showing Base Layers instead of CVDs.

➢ To compare one or more Base Layers with another Base Layer:

1. Select one or more Base Layers in the Base Layers view, right-click, and select Compare Programs with Layer. The Select a Base Layer page appears.

2. Continue as described in the previous procedure, from Step 3.

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

16.2.2 Comparison Report Format

This report summarizes the changes in the programs installed on the selected endpoints resulting from planned changes in their assigned layers. It lists the layering operations to be performed and simulates how the user program list will change as a result.

The layering operations can include the following, in any combination:

- Base Layer change or assignment
- App Layer (single or multiple) assignments or removals
- Enforcement (reinstallation) of the current layers
- Enforcement with removal of user installed applications

The changes listed in the report tables should be reviewed and relevant adjustments made in the reference machine to avoid any unintended consequences. In the case of downgrades, upgrading the relevant software should be considered to avoid software being downgraded on endpoints, or CVDs excluded from the assignment.

This report can be run for a selection of CVDs, pending devices, or a collection, as described in 16.2 Comparison Report between Layers and CVDs.

This report is one of the several Layer Dry-Run reports available from the Management Console Reports feature. For more information about these reports, see 22.3 Layer Dry-Run Reports.
The report is organized in the following sections:

**General Information Section**

The report provides the following general information:

- **Generated By**: Username of the administrator who generated the report.
- **New Base Layer**: Base layer which is requested to be assigned, if any.
- **Added App Layers**: App Layers which are requested to be assigned, if any.
- **Removed App Layers**: App Layers which are requested to be removed, if any.
- **Enforced**: Indicates whether the administrator asked to enforce the content of the layers.

**User Installed Application Conflicts Section**

This section summarizes any conflict that the layer operation would involve (upgrade/downgrade) on programs installed/changed by end-users. The administrator should especially note this, as these conflicts cannot be anticipated from previous layering operations.

**Managed Application Changes Section**

This section summarizes the changes resulting from the layer operation on programs managed with Horizon Mirage layers.

**Tables Included in Application Conflicts and Changes Sections**

The above two sections contain the following tables (according to the scope of the changes), which show the effects of the operation on the endpoint device when the Layer update is executed:

- **Installed**: Lists programs that will be installed (Managed Application Changes section only).
- **Removed**: Lists programs that will be removed.
- **Downgraded**: Lists programs that will be downgraded.
- **Upgraded**: Lists programs that will be upgraded to a new version.
Headings in Each Table

Each table lists the programs and CVDs that will be affected by the operation, under the following headings:

- **Name**: The program name.
- **Publisher**: The program publisher.
- **New Version**: The version of the program after this operation, if any.
- **CVD Affected**: A CVD ID and name, if only one CVD was affected, or the number of CVDs affected with a link to a list of those CVDs, which shows:
  - **CVD**: CVD ID and name.
  - **Operation**: The effect that the operation will have on the program.
    - **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 build version (a difference in the build number only).
    - **Major Upgrade**: The product is upgraded to a new version (a difference in the Major or the Minor revision number).
    - **Downgrade**: The product is downgraded to a new build version (a difference in the build number only).
    - **Major Downgrade**: The product is downgraded to a new version (a difference in the Major or the Minor revision number).
  - **Old Version**: The current version of the program on the endpoint device, if any.
- **Reason**: The layer which caused the change, as well as other information.
  - If any layer brings a new/upgraded/downgraded version of the app, its name will appear.
  - If any layer is removed, and therefore the application is removed, its name will appear.
16.3 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 good practice to test-distribute a Base Layer to a typical user machine with user-installed applications to ensure that the overall update results are satisfactory before distributing to multiple endpoints.

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.

16.4 Updating (Assigning) a Base Layer to a CVD

After a Base Layer is updated at the Server and tested on at least one CVD, you can assign it to individual or 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.

When the updated Base Layer is downloaded to the endpoint, only new files and incremental 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. The old Base Layer is automatically swapped with the new one, thereby assigning the Base Layer to the endpoint and instantiating the endpoint.

The changes in an endpoint resulting from the Base Layer update process are automatically propagated back to the endpoint’s CVD on the server.

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.

The same interfaces are used to apply or modify a Base Layer for multiple CVDs, or a collection.

**Note:** Before and during Base Layer download, Mirage ensures that enough disk space is available to proceed with the operation.

**Tip:** You can upgrade an existing Base Layer or App Layers to all CVDs that are already assigned with previous versions of those Layers – see 16.5 Updating Layers for All CVDs with Previous Version of those Layers.
To assign (update) a Base Layer to a CVD:

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

   **Tip:** You can also start the process by selecting CVDs in any CVD view, right-clicking, and selecting **Layers – Assign Base Layer**.

In this case, you will skip forward to Step 3 to select a Base layer.
2. In the *Select CVDs or Collections* window, choose the CVDs you want to update and click **Select**.

You can either choose individual or multiple CVDs, or choose a collection from the *Collections* tab.

You can see the Base Layer details in the bottom pane. Click **Next** to continue.
3. In the *Select Base Layer* window, choose the Base Layer with which you want to update the CVDs. You can see the Base Layer details in the bottom pane.
4. The validation page appears.

The characteristics below are checked, and warnings may be presented if a mismatch between the Base Layer and the selected CVDs is suspected. You may ignore any warnings that are not applicable. Click **Next** to continue with the operation.

<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 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. In the **Summary** window, click **Finish**. An update task is created. The Mirage Client, as part of its regular processing, periodically checks the Server for updates to download.

This completes the Administrator procedure.

When the Client next connects, download and swap operation will automatically take place, during which the user is asked to reboot. Please allow some time for the changes 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 Layers menu item, select **Cancel Pending Layers**.

**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.

### 16.4.1 Monitoring the Update Progress

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

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

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

To view Layer update progress:

- In the **Mirage Management Console**, select the **Tasks** node, right-click the specific Layer task, and select **View assignments**. The specific Layer update or assignment view opens.

  OR

- In the **Mirage Management Console**, choose the **Image Composer** node, then right-click the Layer you want to view and select **View assignments**.
16.5 Updating Layers for All CVDs with Previous Version of those Layers

You can upgrade an existing Base Layer or App Layers to all CVDs that are already assigned with previous versions of those Layers.

Any program in App Layers or a Base Layer that already exists in a CVD at the same version is not reinstalled (not enforced).

The status of this operation will be Update Layer, in the same way as the regular Update Layers operation.

➢ To update all CVDs to specified layers:

1. In the Base Layers or App Layers view, select the Base Layer or the App Layers with which you want all CVDs with previous versions of those layers to be updated.

2. Right-click and select Update CVDs to this layer version.

16.6 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 Layers > 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 Layer propagation to devices.

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

### 16.7 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.

16.8 Enforcing All Layers

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

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

Additionally, enforcing all layers 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 all 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 Layers on an endpoint:

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

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.
16.9 Base Layer Provisioning

Base Layer Provisioning can be initiated for a device that is Pending Assignment as a new device in an organization in which Horizon 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.

**Note:** Base Layer provisioning is supported for only Windows 7 Base Layers.

**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.

   **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.
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**.

![Select Upload Policy Window]

6. The Target Machine Name window appears. Select the device name and set the domain.

![Target Machine Name Window]
7. The *Image Validation* window appears. Click **Next**.

![Image Validation Window]

8. The *Summary* window appears.

![Summary Window]

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 16.5 Updating Layers for All CVDs with Previous Version of those Layers.

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.
Chapter 17
Assigning Application Layers

In this Chapter...

17.1 Overview
17.2 Comparison Report between App Layers and CVDs
17.3 Testing the App Layer before Rollout
17.4 Updating (Assigning) an App Layer to a CVD
17.5 Monitoring Layer Assignments

17.1 Overview

After App Layer Capture is completed, the revised App Layer can be distributed to each endpoint desktop, then applied (assigned) at each endpoint.

Assigning App Layers to an endpoint (or collection of endpoints) applies the contents of the App Layers to the designated endpoint(s). This means that after assignment all the changes or modifications to the applications will also reside on the endpoint device. For more information, see 17.4 Updating (Assigning) an App Layer to a CVD.

For more about Application Layers, see 12.3 Base Layers and App Layers.

For more about the Layer deployment process, see 12.4 Layer Management Life Cycle.

Note: Before applying an App Layer, ensure that software to be deployed by the App Layer does not conflict with locally installed applications. See 16.7 Dealing with Conflicts.

Note: App Layer assignment requires that a Base Layer to be present on the endpoints.
17.2 Comparison Report between App Layers and CVDs

Before applying a new Base Layer and/or App Layers to a CVD or collection of CVDs, you can run a report that describes the potential effects of the Base and/or App Layer changes on the CVD contents. This report can help you plan the Layer update process, and resolve in advance conflicts that might result from any mismatches in the Layer contents on the selected CVDs.

For more information, see 16.2 Comparison Report between Layers and CVDs and 16.2.2 Comparison Report Format.

17.3 Testing the App Layer before Rollout

The IT manager should check the App Layer to ensure that it was captured properly and all the intended settings are in place. After capturing an App Layer, select a sample group of endpoints and distribute the App Layer to them to ensure that there are no problems.

It is good practice to test-distribute an App Layer to a typical user machine with user-installed applications to ensure that the overall update results are satisfactory before distributing to multiple endpoints.

17.4 Updating (Assigning) an App Layer to a CVD

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

When the updated App Layer is downloaded to the endpoint, only new files and incremental 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 App Layer takes effect and the applications are instantiated to the endpoint.

The changes in an endpoint resulting from the App Layer update process are automatically propagated back to the endpoint’s CVD on the server.

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

The same interfaces are used to apply or modify App Layers for multiple CVDs, or a collection.

Note: Before and during App Layer download, Mirage ensures that enough disk space is available to proceed with the operation.
Tip: You can also upgrade an existing Base Layer or App Layers to all CVDs that are already assigned with previous versions of those Layers – see 16.5 Updating Layers for All CVDs with Previous Version of those Layers.

➢ To update (assign) an App Layer to a CVD:

1. In the Mirage Management Console, select Common Wizards, and then click Update App Layer.

Tip: You can also start the process by selecting CVDs in any CVD view, right-clicking, and select Layers - Update App Layers. Then continue from Step 3.
2. In the *Select CVDs or Collections* window, choose the CVDs you want to update and click **Select**.

   You can either choose individual or multiple CVDs, or choose a collection from the *Collections* tab.

   You can see the CVD details in the bottom pane. Click **Next** to continue.
3. In the *Select App Layer* window, choose the App Layers with which you want to update the CVDs. You can see the App Layer details in the bottom pane.

You choose a layer in the *Available Layers* pane and click the Right arrow to move it to the *Assigned Layers* pane. (To remove a layer, select it in the Assigned Layers pane and click the Left arrow.)

Layers shown in gray indicate that they are assigned already to some CVDs.
4. The validation page appears.

The characteristics below are checked, and warnings may be presented if a mismatch between the Base Layer and the selected CVDs is suspected. You may ignore any warnings that are not applicable. Click **Next** to continue with the operation.

<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 App Layer have the same operating system and type (32- or 64-bit). If they are different, Mirage blocks those CVDs from receiving the App Layer.</td>
</tr>
<tr>
<td>Drive Letters</td>
<td>Mirage checks whether the CVDs have the required drive letter included in the App Layer. If the CVDs do not have the appropriate drive letters, Mirage blocks these CVDs from receiving the App Layer.</td>
</tr>
</tbody>
</table>

5. In the **Summary** window, click **Finish**. An update task is created. The Mirage Client, as part of its regular processing, periodically checks the Server for updates to download.

This completes the Administrator procedure.

When the Client next connects, download and swap operation will automatically take place, during which the user is asked to reboot. Please allow some time for the changes to download.
To cancel an App Layer update in progress:

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>User Name</th>
<th>Activity</th>
<th>Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>16138</td>
<td>domino8000</td>
<td>METISTECIL</td>
<td>idle</td>
<td>100%</td>
</tr>
<tr>
<td>16151</td>
<td>device8001</td>
<td>METISTECIL</td>
<td>idle</td>
<td>0%</td>
</tr>
<tr>
<td>16127</td>
<td>E14-V7SP2-64B-2</td>
<td>idle</td>
<td>0%</td>
<td>App Layer</td>
</tr>
</tbody>
</table>
| 16116| E70-V7-64B-4  | QA
dev1 | idle     | 0%       | App Layer|
| 16147| PC-DEMO         | METISTECIL| idle     | 0%       | Mirage d |
| 16146| PC-DEMO         | METISTECIL| idle     | 0%       | Mirage d |

**Note:** It is recommended that you assign an App 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.

17.4.1 Monitoring the Update Progress

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

For more information, see 16.4.1 Monitoring the Update Progress.

17.5 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.

For more information, see 16.5 Updating Layers for All CVDs with Previous Version of those Layers.
PART 6 - DESKTOP OPERATIONS

In this Part...

18. Endpoint Disaster Recovery
   18.1 Recovering from a Disaster
   18.2 Restoring CVD Snapshots
   18.3 Restoring a CVD Using the Disaster Recovery Wizard
   18.4 Mirage Boot USB Keys
   18.5 Advanced Scenarios
   18.6 User Experience with Restore Processes

19. Hardware Migrations
   19.1 Using the Hardware Migration Wizard
   19.2 Planning for a Mass Hardware Migration
   19.3 Performing a Mass Hardware Migration

20. Windows7 Migration
   20.1 Planning for a Windows 7 in-place Migration
   20.2 Setting Up a Windows 7 Base Layer for Migration
   20.3 Windows 7 Migration
   20.4 Migration to Windows 7 Replacement Devices
   20.5 Post-Migration Scripts
   20.6 End User Experience During a Migration
18.1 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.
18.2 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 same OS reversions (for example, Windows 7 to Windows 7), see the procedure below.

- For cross-OS reversions (for example, Windows 7 to XP or Windows 7 to Vista), see To restore a CVD to a previous snapshot of a different OS on page 210.

➢ **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]

   **Revert Options**
   - **Restore system only**
     - Selecting this option will preserve existing user data on this endpoint. Only Operating System and Applications will be restored. User data from the CVD will be available to the user in the Mirage Deleted Files Archive. This option is only available when restoring to the same OS.

   **Current Base Layer: None**
   - **Snapshot Time Zone:** UTC+02:00 Jerusalem

   ![Snapshot table]

   **Date** | **Machine Version** | **Size (MB)** | **Base Layer** | **OS**
   --- | --- | --- | --- | ---
   1/30/2012 9:33:35 AM | 1.1 | 0 | | XP

   - **a.** Select the snapshot date to which you want to revert.
   - **b.** 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.)
   - **c.** 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.

   - **c.** Click **Next**.

3. The Revert CVD window appears. This makes sure that there are no conflicts with your CVD Snapshot Restore. Click **Next**.

   ![Revert CVD window2]

   **Use the following validation summary to compare the device with the snapshot. This summary will alert you to any potential issues that require attention. You may not be able to proceed until blocking issues are resolved.**

   - **No compatibility issues detected**
4. The Summary window appears. Click Finish.

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 that you want to restore to a previous snapshot 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 *Domain Details* wizard page appears showing Domain Options. Fill in the domain details in order for the device to rejoin the domain. Click **Next**.

![Domain Details page](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.

4. A validation window appears. This makes sure that there are no conflicts with your CVD Snapshot Restore. Click **Next**.

![Validation window](image)

5. The *Summary* window appears. Click **Finish**.

![Summary window](image)
18.3 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.

There are two restore procedures:

- To restore a CVD after hard-drive replacement, file corruption or format, below.
- To restore a CVD to a replacement device, on page 215.

**Note:** The IT manager can also migrate users from Windows XP or Windows 7 machines to new Windows 7 machines by performing the To restore a CVD to a replacement device procedure - see 20.4 Migration to Windows 7 Replacement for more information. In that case, select Only Restore User Data and Settings as the Restore Options selection.

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.

**Disaster Recovery**

Restore a CVD to the same endpoint, (e.g., in the case of a new hard-drive or after a format) or restore to a replacement endpoint.
3. The *Select Action* window appears. Select *Replace Hard Disk* and click *OK*.

4. The *Device Selection* window appears. Select the device you want to use for the restore operation. Only devices that are recognized as connected to CVDs and are pending restore are listed.
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](image)

- **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](image)
To restore 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, **Replace the user machine** 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) will be 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 will be restored 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.

  *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 will be restored 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.

  *Note:* This option should be used if you want to migrate users from Windows XP/Vista 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/Vista 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/Vista to a Windows 7 system (because Mirage cannot guarantee cross-Operating System compatibility).

- When a CVD is migrated from a Windows XP/Vista 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/Vista CVD, that Windows 7 endpoint becomes a Windows XP/Vista 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.

![Target Machine Name window]

**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:

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

ii) 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 cannot proceed until blocking issues are resolved. Click **Next**.

![Validation Details](image)

9. The **Summary** window appears. Click **Finish**.

![Summary](image)

10. The migration process proceeds and takes place in two phases (as described in 18.6 User Experience with Restore Processes).
18.4 Mirage Boot USB Keys

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 Horizon Mirage client is also installed and is pre-configured to connect to your Horizon Mirage Server when the machine boots. The Mirage 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 reimaging a remote device out in the field.
- Provisioning/Imaging a fresh Windows installation on an existing machine quickly.

Deploying the Windows image with the Mirage Boot USB Key takes between 15 to 30 minutes (on average).

18.4.1 Prerequisites

The following prerequisites are required:

- A Windows 7 (Professional or Enterprise Edition) machine.
  **Note:** This is represented as Drive C throughout this guide.
- The Mirage Boot USB Scripts (provided by VMware).
- A Windows 7 (Professional or Enterprise Edition) DVD or ISO file.
  **Note:** This is represented as Drive D throughout this guide.
- An 8 Gigabyte USB Drive
  **Note:** This is represented as Drive U throughout this guide.
- A Mirage Client MSI installer file (x86 or x64 version).
  **Note:** Current clients can be found on the Horizon Mirage support downloads page.
- Drivers for the end point hardware (Optional)
- Network drivers are highly recommended.
- All other drivers can be delivered via the Driver Library feature within the Mirage Server.
18.4.2 Creating the Mirage Boot USB Key

Important Notes before you begin:

- 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!**
- When using an ISO file for Windows 7 installation, extract the content of the ISO file by one of the following methods:
  - Use .ISO image file software to download and save the .ISO image file to a CD-R or a DVD-R. OR
  - Virtually mount and access ISO files as a virtual device.
  - Extract the .ISO files to your hard drive. OR

The results will be a folder/drive/virtual-drive containing the Windows 7 installation folders.

To create the Mirage Boot USB key:

1. On your workstation, create the folder `C:\BootUSB`.
2. Create two subdirectories in `C:\BootUSB`. One named `Drivers` and one named `MirageClient`.
3. 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.
4. Open the `C:\BootUSB\MirageClient` folder and copy the appropriate Mirage client install MSI into this folder.
5. Find any hardware drivers you need for the new hardware and copy them into the `C:\BootUSB\Drivers` folder.
6. 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).
7. Insert the USB Key and wait until Plug and Play detection completes.
8. Run a Command Prompt window as an administrator and type `cd C:\BootUSB` and press `<Enter>`.
9. 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).

10. Run the complete command (syntax as follows):

```
win7usb.cmd [win7 dvd path] [msi path] [server address] [use ssl transport (true/false)] [usb disk number] [Drivers folder (optional)]
```

   a. `[win7 dvd path]` is the path to the Windows 7 DVD or folder containing Windows 7 installation files (folder containing the contents of the Windows 7 DVD).

   b. `[msi path]` is the path of a Mirage client msi.

   c. `[server address]` is the IP address for your Mirage server which any client devices connect to.

   d. `[Use SSL transport]` is whether or not this client will connect using SSL (Use true or false).

   Note: the Mirage Server must already be configured for SSL for this to be turned on!

   e. `[usb disk number]` is the number of the USB disk to format a list of connected disk numbers will be displayed upon invocation.

   f. `[Drivers folder]` is where any hardware drivers you need on your new device or stored so that they can be added to the Boot USB Key. This parameter is optional.

Each customer’s exact string will be different. This is an example of how a typical string may look assuming that the Windows 7 DVD is in the D: drive, the Mirage client’s exact path and filename, the IP or FQDN of the Mirage server is 192.168.11.203, SSL is turned off, the USB Key is listed as disk #2, and the end point drivers are in C:\BootUSB\Drivers.

```
C:\BootUSB>win7usb.cmd D:\ C:\BootUSB\MirageClient\MirageClient.x86.45071.msi 192.168.11.203 false 2 C:\BootUSB\Drivers
```
11. 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.

18.4.3 Using the Mirage 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 Mirage 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. 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 or Enterprise 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. Windows now installs. No further user intervention is required. In the process, the target machine reboots several times to complete the Windows install. This is normal.

3. 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. You can use the System Image Manager (SIM) tool that comes with the Windows Automated Installation Kit (AIK) to do this.

4. Once you login for the first time, the target machine should be ready to use but may also perform additional Windows operations in the background.
18.4.4 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. Unless specified otherwise, these files are located in: USB_ROOT\sources\$oem$\$$\setup\Wanova\n
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).

3. **MirageClient.msi**. The Mirage client that is installed on the new Windows 7 machine. Make sure the client version matches the Mirage server version.

4. **Autounattend.xml**. An answer file for the unattended Windows 7 installation that you can edit to customize the deployed Windows 7 installation. This file is found in the root of the USB drive.

**Note:**

1. Boot-critical drivers can be added to the Boot USB by putting them in `<USB DRIVE>:\$WinPEDrivers$` . Use this option only if the Windows 7 installation cannot proceed due to missing a critical driver (for example, missing disk controller, preventing the installation from detecting the hard drive).

2. The contents of `<USB DRIVE>:\sources\$oem$\$1\MirageDrivers` is copied into the local folder `C:\MirageDrivers`. The Windows 7 installation will search and use drivers located in the folder “MirageDrivers” on the root of any drive.

3. The Windows 7 installation can be further customized as follows:
   a. The contents of `<USB DRIVE>:\sources\$oem$\$$` is copied into Windows folder on the installation drive, e.g. `C:\Windows`.
   b. The contents of `<USB DRIVE>:\sources\$oem$\$1` is copied into the installation drive, e.g. `C:\`.

18.4.5 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 you try to install Mirage with a SSL Mirage server, the newly deployed machine may not be able to connect to the server (as it is not yet a member of the domain). In such a case, add a custom action on the USB disk to add the machine to the domain.

18.4.6 Windows XP Boot USB Keys

• Wanova does not officially support a Boot USB Key for Windows XP. To restore a bare metal Windows XP device, use your Windows 7 Boot USB Key, and then use Mirage to restore the device to a previous Windows XP snapshot.

18.5 Advanced Scenarios

18.5.1 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.
18.6 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.

When that file finishes downloading, Mirage will notify the user that the file is available.

In some cases the user is advised to wait until the connection is reestablished.

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.
Chapter 19

Hardware Migrations

▷ In this Chapter...

19.1 Using the Hardware Migration Wizard
19.2 Planning for a Mass Hardware Migration
19.3 Performing a Mass Hardware Migration

19.1 Using the Hardware Migration Wizard

This chapter describes how to move a user from one device to another, for example, when new hardware is purchased.

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.

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 or newer than that of the CVD.

**Additional Notes:**

- If you migrate a CVD from a Windows XP/Vista 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/Vista to a Windows 7 system (because Mirage cannot guarantee cross-Operating System compatibility).

- When a CVD is migrated from a Windows XP/Vista 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/Vista CVD, that Windows 7 endpoint becomes a Windows XP/Vista 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. Click **Next** when ready to proceed.
6. 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.

![](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**).

7. 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 cannot proceed until blocking issues are resolved. Click **Next** when you are ready to proceed.

8. Click **Finish**.

9. The migration process proceeds and takes place in two phases (as described in **18.3 Restoring a CVD Using the Disaster Recovery Wizard**).
19.2 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 Horizon 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.

19.3 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 Mirage 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.
Performing a Mass Hardware Migration

- 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 20

Windows 7 Migration

➢ In this Chapter...

20.1 Planning for a Windows 7 in-place Migration
20.2 Setting Up a Windows 7 Base Layer for Migration
20.3 Windows 7 Migration
20.4 Migration to Windows 7 Replacement Devices
20.5 Post-Migration Scripts
20.6 End User Experience During a Migration

20.1 Planning for a Windows 7 in-place Migration

Horizon Mirage offers a unique capability that enables the in-place migration of existing Windows XP/Vista 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 Horizon 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 endpoints to assist in the migration process.

20.2 Setting Up a Windows 7 Base Layer for Migration

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 Image Setup.

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.
20.3 Windows 7 Migration

The Windows 7 Migration wizard downloads and migrates existing Windows XP/Vista endpoints to Windows 7. The process involves first downloading the Windows 7 image to the endpoints and then applying (migrating) the image.

Note: The Windows 7 Migration wizard performs an in-place migration of existing Windows XP/Vista endpoints to Windows 7, within the same equipment. To perform a migration involving different hardware, see 20.4 Migration to Windows 7 Replacement.

20.3.1 Using the Windows 7 Migration Wizard

The Windows 7 migration can be done in two ways:

- **Download and Apply Base Layer**: This performs the migration in one step, migrating the Windows 7 image to the endpoints after all the CVDs in the task have finished downloading.

- **Only Download Base Layer** option: This performs only the Download stage, enabling the Administrator to selectively migrate CVDs that have completed downloading as a separate operation. 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 Windows 7 is applied to specific endpoints.

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 20.3.2 Migration Following “Only Download Base Layer”.

To migrate an endpoint to Windows 7:

1. Open the Mirage Management Console and click Common Wizards.
2. Click Windows 7 Migration.

3. The Select CVDs or Collections window appears. Choose the CVDs you want to update and click Select.

You can either choose individual or multiple CVDs, or choose a collection from the Collections tab.

You can see the CVD details in the bottom pane. Click Next to continue.
4. The Select Base Layer wizard page appears.

   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**.
5. Select the XP or Vista 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**.
6. 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.

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:

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

ii) Select the General tab and then enter the credentials you want to use for domain joining.

c. Click Next.
7. A validation dialog appears. Use this dialog to resolve any compatibility issues between the Base Layer and selected CVDs. Click Next.


9. 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 20.3.3 Monitoring the Migration.
   - If you selected Only Download Base Layer, the migration must be performed manually on the task as a separate step – see 20.3.2 Migration Following “Only Download Base Layer”.

20.3.2 Migration Following “Only Download Base Layer”

If you selected the Windows 7 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, Windows 7 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 of 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. In the Mirage Management Console, select Task Monitoring. 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](image)

   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 **20.3.3 Monitoring the Migration**.

5. You can repeat the procedure as more CVDs complete downloading.
To migrate selected CVDs in the task:

1. In the Mirage Management Console, select 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.

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 20.3.3 Monitoring the Migration.

6. You can repeat the procedure as more CVDs complete downloading.

20.3.3 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.
20.4 Migration to Windows 7 Replacement Devices

The IT manager can migrate users from a Windows XP/Vista 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 restore a CVD to a replacement device procedure in 18.3 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
- Windows Vista 32-bit to Windows 7 32-bit or 64-bit
- Windows Vista 64-bit to Windows 7 64-bit

(The 20.3 Windows 7 Migration section describes “in-place” migration” for Windows 7 and is not suitable for migration to replacement devices.)

20.5 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 zero.

### 20.6 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 login is disabled until Mirage completes the migration process. 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 the Windows logon screen. When the process is completed, Mirage automatically restarts the machine and login will then be possible.

![VMware Mirage migrating user state](image)

**Note:** In order to re-join the domain, the computer must have network access to the domain controller. End users cannot login using their domain credentials until the domain join is complete.
20.6.1 Known Limitations

- A Windows 7 migration using Horizon 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/Vista 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...

21. Monitoring Desktop Deployment
   21.1 Using the System Dashboard
   21.2 Transaction Logs
22. Mirage Reporting
   22.1 Mirage Reporting Overview
   22.2 Generating a Report
   22.3 Layer Dry-Run Reports
   22.4 CVD Integrity Report
23. Maintaining the Mirage System
   23.1 Server Backup and Restore
   23.2 Upgrading from Previous Mirage Versions
24. Troubleshooting
   24.1 Using the CVD History View
   24.2 Using the Event Log
   24.3 Customizing the Minimal Restore Set
   24.4 Using the System Report Utility
   24.5 Remote SysReport Collection
Chapter 21

Monitoring Desktop Deployment

In this Chapter...

21.1 Using the System Dashboard
21.2 Transaction Logs

21.1 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.
21.1.1 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.

21.1.2 Server

The Server area shows the current status of the Mirage Servers, Up or Down. The icon also reflects the Server status.

21.1.3 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.

21.1.4 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.

21.1.5 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.
21.1.6 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.

21.1.7 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.
21.2 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.
- **Update App Layer**: End-user machine is updated with the assigned App 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.
21.2.1 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).
21.2.2 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 (...).

21.2.3 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>Layer transactions</td>
<td>180 days</td>
</tr>
<tr>
<td>All other transactions</td>
<td>365 days</td>
</tr>
</tbody>
</table>
Chapter 22
Mirage Reporting

In this Chapter...

22.1 Mirage Reporting Overview
22.2 Generating a Report
22.3 Layer Dry-Run Reports
22.4 CVD Integrity Report

22.1 Mirage Reporting Overview

Horizon 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 22.3 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 22.4 CVD Integrity Report.
22.2 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.
22.3 Layer Dry-Run Reports

Before applying a layer update to a CVD or collection of CVDs, you can run a report to compare the content of the layers and the CVD. This report helps you plan the layer update process, and resolve in advance conflicts that might result from any mismatch between the CVD and the layers content.

There are two kinds of Layer Dry-Run reports:

- **Application-level report**: This report describes projected applications that are added to, updated in, or deleted from to an endpoint device when the selected layer changes are applied. It compares the applications installed on the layers and the CVD and provides a general view of the result for the change in layers. For more information, see 16.2 Comparison Report between Layers and CVDs.

- **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><strong>Base Layer Application Downgrades a user installed application</strong></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><strong>Base Layer Application Downgrades OS component</strong></td>
<td>An application installed in the Base Layer downgrades OS component/s.</td>
</tr>
<tr>
<td><strong>Base Layer OS Component/s downgrades user installed application</strong></td>
<td>OS component/s in the Base Layer downgrades shared components that are used by a user installed application.</td>
</tr>
</tbody>
</table>
22.4 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.

**Note:** Systems Reports or log files generated using the System Report Utility may contain sensitive, confidential or personal information. Consider obfuscating the logs before sending them to VMware.

---

**Event Properties**

<table>
<thead>
<tr>
<th>Event Properties</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>712</td>
</tr>
<tr>
<td>Time</td>
<td>4/22/2012 7:37:51 PM</td>
</tr>
<tr>
<td>First Seen</td>
<td>4/22/2012 7:37:51 PM</td>
</tr>
<tr>
<td>Device</td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>SRV-SERVERS5[Server]</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Type</td>
<td>Server</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>False</td>
</tr>
<tr>
<td>Count</td>
<td>1</td>
</tr>
</tbody>
</table>

**Description:**
Possible CVD inconsistency detected

**Details:**
CVD VM-SERVER-N11 (16090) might have data inconsistencies. Please run CVD Integrity tool to detect and try to resolve CVD area structural issues.
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.

   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.

![CVD Integrity Options window](image)

**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**.

![Summary window](image)

You are about to run "Check Only" CVD integrity on CVD device 100 [ID 10040]. The CVD will be suspended during the integrity check.
Report Name: CVD_Integrity_qa1_4/19/2012.
Chapter 23
Maintaining the Mirage System

▷ In this Chapter...

23.1 Server Backup and Restore
23.2 Upgrading from Previous Mirage Versions

23.1 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 **Server.Tools.zip** package, prior to installing the Mirage Server. For information about obtaining the package, contact VMware support.

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 **Server.Tools.zip** to the server machine, extract the zip, and run the following command from any Mirage Server machine:

   `Wanova.Server.Tools.exe ResetPendingBI`

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*.

➤ **Restore procedure – Standalone Server only:**

**Note:** This procedure is applicable only to a small-scale, standalone server setup where the database, storage and Mirage services are all co-hosted on the same server. This procedure assumes that the Administrator restores a complete Mirage Server system from backup, including OS image, Mirage Server software, Mirage Storage and Database.

1. Restore the complete Server System (that is, from full disk image).
2. Boot the server into **Windows Safe Mode**.
3. Set the VMware Server Service and VMware Management service start type to **disabled**.
4. Boot the server normally.
5. Run the following commands:
   `Wanova.Server.Tools.exe ResetPendingBI`

6. Set the VMware Server service and VMware Management service start type to *Automatic*.

7. Start the VMware Server service and VMware Management service.

### 23.2 Upgrading from Previous Mirage Versions

This section describes how to upgrade the Mirage System from earlier Mirage versions.

**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 current 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.

#### 23.2.1 Before You Start

Before beginning the Upgrade process, ensure that the following steps are performed.

**Pre-upgrade steps:**

1. Have the following information available for use during installation. Locate this information either in the server config file or via other methods.
   
   - **a.** Database server name
   - **b.** Credentials for the database server
   - **c.** Mirage server cache directory location
   - **d.** Cache size
2. Stop Mirage Services.

3. Back up the Mirage database using one of these methods:
   - Run a full sysreport in Mirage by double-clicking this file:
     
     C:\Program Files\Wanova\Mirage Management Server\sysreport_full.cmd
   - Use SQL Server Management Studio.

   **Notes:**
   For more information on backing up the MS SQL database, see Using SQL Server Management Studio in the MSDN article Create a Full Database Backup (SQL Server) - see [http://msdn.microsoft.com/en-us/library/ms187510.aspx#SSMSProcedure](http://msdn.microsoft.com/en-us/library/ms187510.aspx#SSMSProcedure).
   Ensure you select the database named MirageDB, and that you use the Full backup type.
   Make a note of the location of the backup file.

4. Take snapshots of all Mirage volumes. Ensure that you use image-based block backup, and not file-based.

   **Note:** If snapshot functionality is not available, create and run a backup job for the each volume's directory using any available backup program. This will take a significant amount of time to complete. The backup software must support Alternate Data Streams (ADS). VMware recommends using block-based backup programs rather than file-level backup using ADS.

### 23.2.2 Upgrade Procedure

It is important to perform the upgrade steps and sub steps in the specified order.

➤ **To upgrade Mirage:**

1. Uninstall the Mirage system using Control Panel > Add or Remove Programs, in this order:
   - Uninstall all Mirage Servers.
   - Uninstall Mirage Management Console.
   - Uninstall Mirage Management Server.
   - Uninstall Mirage WebAccess.

2. The Install the latest version of Mirage using the new MSIs, in this order:
   - Install Mirage Management Server.
   - Install Mirage Management Console.
   - Install Mirage Servers.
   - Install Mirage WebAccess.
Chapter 24

Troubleshooting

In this Chapter...

24.1 Using the CVD History View
24.2 Using the Event Log
24.3 Customizing the Minimal Restore Set
24.4 Using the System Report Utility
24.5 Remote SysReport Collection

24.1 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.

24.2 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.

24.2.1 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
24.3 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.

   A message is displayed confirming that the Static Minimal Set has been added successfully.

   ```
   C:\Program Files\Metis\Mirage Server\Metis.Server.Cli.exe localhost
   Metis Server Management Console
   Static Minimal Set 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.

### 24.4 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:syssreport-MMDDYYYY-HHMM-ComputerName.cab

This command can be CPU-intensive, especially on the Server, hence intermediate impact should be expected.

- Alternatively, you can generate a system report by right-clicking the Mirage icon in the system tray, and selecting Tools.

24.5 Remote SysReport Collection

An Administrator can save system reports from any device attached to the Mirage server.

➢ To save system reports:

1. In the Mirage Management Console tree, expand the Inventory node and select the All CVDs node.

2. Find the CVD for which you would like to generate a report. 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.
Appendix

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
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.

1. If SCCM client is not yet installed, follow the instructions at http://technet.microsoft.com/en-us/library/bb693546.aspx to manually install the client.

   DO NOT specify a SCCM site code for the client in the CCMSetup.exe command-line properties (SMSSITECODE parameter).

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 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 Layer

When building a Layer using the Layer 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 Layer 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.

![Capture Layer Screenshot]

It is highly recommended to build in the Office licenses into your Layers 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.
# Appendix 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), and 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>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Manage Driver Library</td>
<td>User can add drivers to the driver folders and create new driver profiles, and modify existing driver folders and libraries.</td>
</tr>
<tr>
<td>View Reports</td>
<td>The user can see the generated reports.</td>
</tr>
<tr>
<td>Manage Reports</td>
<td>Create reports and delete reports.</td>
</tr>
<tr>
<td>View events</td>
<td>User can view the events under the event log and manager journal.</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.

![Image of Users and Roles node with Add a Group option highlighted]

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.
• 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
A

Activating endpoints .................................................. 55
  Base Layer provisioning .................................. 192
centralizing ................................................. 55
Active Directory groups ................................. 278
  managing users and roles ......................... 278
Active user sites
  to select branch reflector .......................... 116
Always prefer branch reflector (no fallback to server) .................. 116
Antivirus
  configuring 3rd party software ....................... 36
App Layers ..................................................... 138
  assigning ................................................. 197
Assigning ..................................................... 198
  monitoring assignments .............................. 203
testing before rollout .................................. 198
Assigning
  App Layers .............................................. 197, 198
  Base Layers ............................................. 177, 183
Audit events .................................................. 268

B

Base Layers
  assigning .............................................. 177, 183
capturing ................................................ 151, 158
  comparison report ..................................... 178
conflicts .................................................. 190
Dry-Run report ........................................... 259
  enforcing all layers ................................ 191
  hardware considerations ............................ 141
lifecycle .................................................. 139
  monitoring assignments ............................. 189
Override policy ........................................... 155
  Post-base payer scripts ............................... 157
provisioning ................................................. 192
  recreating reference machine ....................... 162
  rules ................................................... 152
software considerations ................................ 141
testing before rollout .................................. 183

Index

BitLocker support ........................................... 144
Bootless client installer ......................... 22, 50
Branch reflector
  accepting peers ........................................ 118
  additional networks ................................. 22, 117
  cache size ............................................. 116, 117
  configuring ........................................... 115
  default values ....................................... 115
  disabling .............................................. 118
  downloading peers ................................. 121
driver library cache .................................. 22, 113
  enabling .............................................. 114
local file distribution ................................. 22, 113
  maximum connections .............................. 116, 117
  monitoring .......................................... 120
no fallback to server .................................. 22, 116
  overview ............................................. 111
rejecting peers ......................................... 118
waiting peers .......................................... 121

C

Cache size .................................................. 116, 117
Capacity status ............................................. 253
Capturing
  Base Layers ............................................. 151, 158
Centralizing an endpoint ............................. 55
Collections
  add CVDs ............................................. 68
node ................................................... 67
Compliance meter .......................................... 252
Conflicts
  Base Layer ............................................. 190
CVD ....................................................... 17
CVD Integrity report ..................................... 22
CVDs
  add to collection ................................... 68
collections ............................................. 67
  Integrity report ...................................... 260
restore ............................................... 212
snapshots .............................................. 205, 207, 208
viewing history ......................................... 267

BI See Base Layers
Dashboard
  capacity status ........................................ 253
  compliance meter ........................................ 252
  Data Protection view .................................... 252
  efficiency benchmarks ................................... 253
  server status ............................................. 252
  system status ............................................. 252
  Update Progress view .................................... 252
  Data protection ........................................... 24
  Desktop
    management ............................................. 25
    monitor deployment .................................... 251
    operations .............................................. 67
    policies ................................................ 61
    policies - rule macros .................................. 280
  Downloading peers ....................................... 121
  Driver library caching ................................... 22, 113

  E
  Efficiency benchmarks ................................... 253
  Encrypted File System (EFS) ................................
  Enforcing all layers ..................................... 191
  Event log .................................................. 268
  Events, audit .............................................. 268

  F
  Factory Policy ........................................... 61
  Fast user switching ..................................... 29

  H
  Hardware prerequisites .................................. 31

  I
  Image management ....................................... 135
    traditional vs. Mirage ................................ 135
  Installation
    Mirage management console ........................... 38
    Mirage management server .............................. 36
    Mirage Server ........................................... 42, 128

  L
  Layer management life cycle ............................ 139
  Licenses .................................................. 40
    add ....................................................... 41
    and reference CVDs ..................................... 40
    Load balancing ......................................... 129

  M
  Management Server ....................................... 18
  Manager Journal ......................................... 268
  Maximum connections
    branch reflector ........................................ 116, 117
    Mirage server .......................................... 84
  Microsoft Management Console ......................... 30
  Microsoft NLB ............................................ 130
  Minimal Restore Set ..................................... 226
    dynamic ................................................ 269
    static .................................................. 269
  Mirage Client ............................................ 18
    deploy to endpoint ..................................... 49
    install .................................................. 49
  supported operating systems ................................ 29
  Mirage Management Console ............................. 18
    install .................................................. 38
  Mirage Management Server
    install .................................................... 36
    software prerequisites .................................. 30
  supported operating systems ............................. 29
  Mirage reports
    Base Layer Dry-Run ..................................... 259
    CVD Integrity report ................................... 22, 260
    generating ............................................. 258
  Mirage Server ............................................ 19
    configuring ............................................ 84
    configuring SSL ......................................... 83
    install .................................................. 42, 128
    maximum connections ................................... 84, 126, 127
    removing ............................................... 129
    starting service ....................................... 128
    stopping service ...................................... 128
  supported operating systems ................................ 29
  Mirage System
    audit events ............................................ 268
    configuring ............................................. 81, 85
    ports used .............................................. 33
    solution components ................................... 18
    upgrading from v2.0 .................................... 265
  Monitor
    capacity status ......................................... 253
    Dashboard ............................................... 251
    Monitoring ............................................. 251
App Layer assignments ........................................ 203
Base Layer assignments ....................................... 189
compliance meter ................................................ 252
network usage .................................................... 253
server status ...................................................... 252
system status .................................................... 252
update progress ................................................ 252
Multiple servers ............................................... 125
Multiple volumes ............................................... 103
adding ............................................................. 106
blocking ........................................................... 107
editing volume info ............................................ 107
maintenance ...... See volume maintenance mounting ................................................ 108
removing .......................................................... 107
unblocking ........................................................ 109
unmounting ....................................................... 108
Network Client Throttling ..................................... 76
Network operations
resuming .......................................................... 119
suspending ........................................................ 119
NLB
default settings .............................................. 131
Override policy ................................................. 155
Pending devices
reject .............................................................. 60
Policies ............................................................ 62
Post-base payer scripts ....................................... 157
Provisioning
see Base Layer provisioning ................................ 192
Proximity, required ............................................. 116
Reference CVD .................................................. 19
Reference machine ............................................ 19
assign pending .................................................. 146
configuring ...................................................... 145
recreation ....................................................... 162
settings ........................................................... 148
software considerations ..................................... 147
software prerequisites ....................................... 30
supported operating systems ................................ 29
Rule macros ..................................................... 280
Server storage capacity ...................................... 25
Single-Instance Storage (SIS) ................................ 109
Single-sign-on ................................................... 25
SIS integrity procedure ....................................... 109
Snooze ............................................................ 76
Software prerequisites ....................................... 30
Mirage Management Server ................................ 30
SSL .............................................................. See Mirage Server
System status ................................................... 252
Testing
App Layers before rollout ................................... 198
Base Layers before rollout ................................... 183
Transaction log .................................................. 254
Transaction types .............................................. 254
Upgrading from v.2.0 .......................................... 265
VMware Watchdog ............................................. 129
configuring ....................................................... 130
Volume maintenance ......................................... 109
Waiting peers ................................................... 121
WAN emulator ................................................... 18
Wizards .......................................................... 53