VMware Mirage 5.0 Reviewer's Guide

WHITE PAPER

vmware®

Table of Contents

Introduction

VMware Mirage™ is a unified image management solution for physical desktops, virtual desktops, and mobile devices. Mirage is available as a standalone product and as an integral part of VMware Horizon® 6.

This reviewer's guide enables you to evaluate VMware Mirage.

Audience

The *VMware Mirage Reviewer's Guide* is intended for prospective IT administrators of Mirage and media reviewers of the product.

What You Will Learn

The *VMware Mirage Reviewer's Guide* introduces you to Mirage and its features and gives you hands-on exercises to evaluate the product. Topics addressed include:

- What is VMware Mirage?
- Key features
- Packaging and licensing
- Components and architecture
- Installation and configuration
- Hands-on evaluation exercises

Navigating This Document for Mirage Use Cases

You can navigate directly to descriptions of key Mirage use cases and the hands-on exercises.

- Backing up a desktop with Mirage
- Operating system migration
- Using Mirage for desktop recovery
- Using Mirage to work with base and application layers

Note: The term *desktop* is used in this guide to refer to a desktop computer, laptop computer, virtual machine as in a bring your own device (BYOD) with VMware Fusion® Pro, and virtual desktop through VMware Horizon with View.

What Is VMware Mirage?

Mirage takes a new dynamic-layering approach to managing end users' Windows PCs, Fusion Pro and VMware Player Plus™ virtual machines, and persistent virtual desktops (full clones) in View.

IT manages layers that update the operating system and applications, while end users control their files, profile, and other unmanaged applications.

IT can update their layers without affecting the user layers, and all layers are kept synchronized within the data center when the user is online. In the PC use case, because Mirage leverages local computing, end users can work online or offline and always enjoy full native performance.

This unique layered solution to desktop management and low-footprint architecture empowers IT to strengthen how they perform key initiatives, such as Windows 7 or Windows 8.1 migrations, Windows image and application management, PC management at remote branch offices, and desktop support and recovery.

Mirage has the following primary features:

- Backups of user desktops – Mirage synchronizes the data center backup with changes to the endpoint. Centrally stored desktop images and periodic endpoint snapshots enable IT to recover partial or full desktops when needed.
- Data recovery – You can recover an endpoint at different levels, from applications and data up to a full system restore.
- Layered desktop images – Mirage offers IT a layered desktop-image approach. Layering enables IT to control parts of everyone's desktop and to update or migrate desktops without overwriting user-installed applications or data.

With Mirage, IT can reduce the time and money required to standardize particular layers of the desktop, back up desktops, and handle planned migrations and unplanned desktop recovery.

Backups of User Desktops
Mirage desktop images are stored centrally in the data center. Users work on their local personal computers with full use of native PC hardware capabilities. Execution is local to the PC, and end users can work online or offline. They are not tied to any network. User data and settings and user-installed applications are persistent.

The Mirage client installed on each endpoint enables Mirage to synchronize the data center backup image with changes to the endpoint. Mirage uploads snapshots of endpoints to the data center while users work without interruption. When a user is disconnected from the network, user changes to the endpoint are flagged for upload when the user reconnects.

Data Recovery
The layering technology in Mirage provides the following desktop recovery options:

- Entire device (OS, applications, user data, and profile)
- Only applications, user data, and profile
- Only user data and profile

Layered Desktop Images
Layers are logical divisions of Mirage desktop images and are useful for creating standardized desktop configurations. IT can choose to create desktop layers. Each desktop receives a base layer, a driver library, and one or more application layers (with the operating system, system software, and standard applications). You can create different base layers for specific sets of users. You can also create multiple application layers to distribute to different sets of users. Users can receive multiple application layers.

IT assigns base layers and application layers to endpoints and updates these layers with patches and new content as needed. Endpoints do not receive layer updates continually. Instead, IT initiates and schedules layer updates. IT has total control over the content, assignment, and deployment of base and application layers.

Depending on IT policies, users can control their own data and settings and install their own applications on their endpoints. This personalization exists side by side with IT-controlled base and application layers.

Layers are used in the migration of endpoints from one Windows version to another, such as from Windows XP to Windows 7 or Windows 7 to Windows 8.1, and in the migration of desktop images to new hardware.

For more information, see Layered Desktop Images.

Interaction Between Endpoints and Data Center Desktop Images
IT can choose when to download layer updates—changes that IT makes to base and application layers—to endpoints.

Changes to endpoints are automatically uploaded to the data center to keep desktop images synchronized with endpoints. These changes include user changes to endpoints and layer updates initiated by IT.

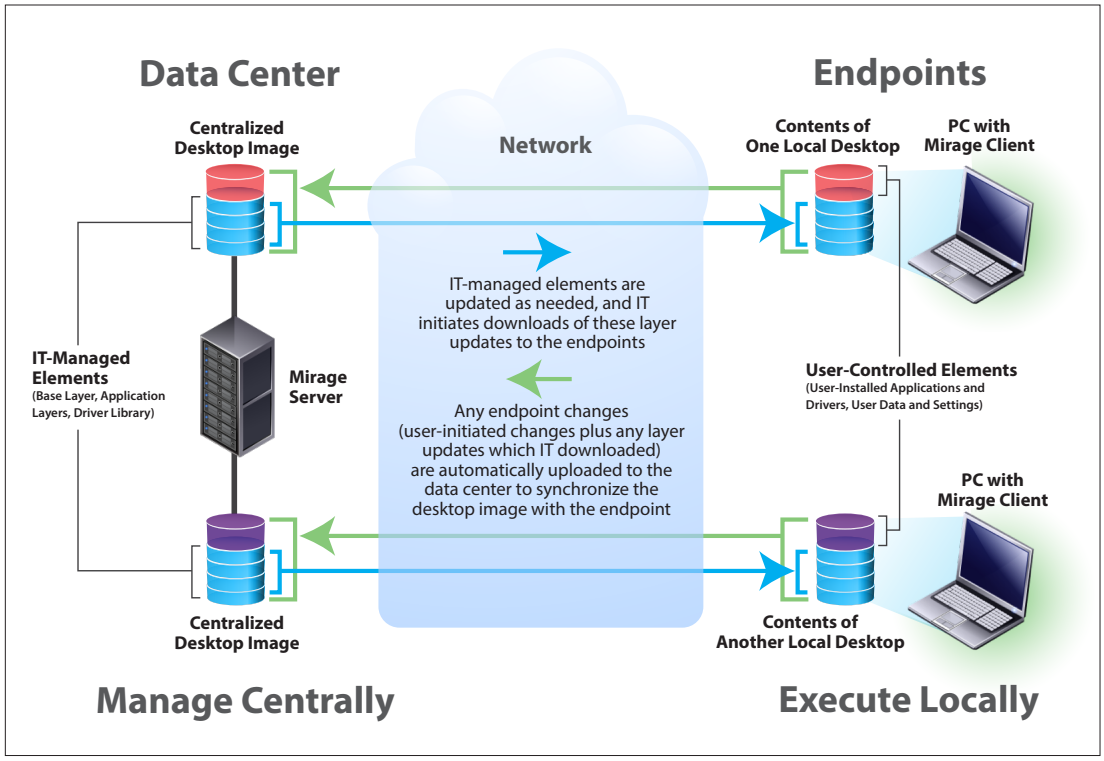


Figure 1: Mirage Uploads and Downloads Updates Between Endpoints and Data Center Desktop Images

Mirage efficiently manages uploads and downloads between endpoints and data center desktop images. Mirage is designed for WANs. It compresses all transferred data and deduplicates data in storage and during network transfers. Data is stored once, and Mirage only transfers data that is not present at the destination.

How Is Mirage Different from a PC Lifecycle Management Tool?

Personal computer lifecycle management (PCLM) is a process for managing a computer desktop from the time of its initial procurement to the later stages of imaging, software application deployment, updates, patching, monitoring, security compliance, and eventually to retirement. Many software tools exist on the market today to automate these processes, including Microsoft SCCM, LANDESK, Symantec CMS, BMC BladeLogic, HP Client Automation, and CA.

Mirage complements and extends your existing PCLM investment and processes. PCLM tools manage the content of the PC image while Mirage manages the building and deployment of the image. The dynamic-layering technology of Mirage enables IT to easily migrate user data and profiles, greatly reducing help desk support costs and end-user downtime.

You can perform an in-place OS migration for end users by deploying a new OS base layer with compatible applications built in. The base layer upgrades each local OS to the new OS, but does not delete or overwrite users' personal files or profiles.

Mirage offers other time and cost savings with its hardware refresh and application layering functionality. With a hardware refresh, you can move the user experience (OS, personal files, profiles, and applications) from one device to another. You determine whether to update the OS and applications during the refresh.

Additionally, you can smoothly update end-user applications by applying application layers whenever needed. The automated snapshot feature that Mirage provides facilitates a quick full-system recovery in case of a failure.

VMware Horizon 6 Components

Mirage is a component of Horizon 6 and an essential element of the VMware end-user computing vision. The Horizon 6 components enable IT to deliver virtualized and remote desktops and applications through a single platform to end users. These desktop and application services, including Remote Desktop Session (RDS)-hosted apps, packaged apps with VMware ThinApp®, software-as-a-service (SaaS) apps, and virtualized apps from Citrix, can all be accessed from one unified workspace across devices, locations, media, and connections.

VMware Workspace™ Portal gives end users a central portal to access all their business apps on any device, meeting the needs of an increasingly mobile workforce. Workspace provides secure, policy-based single sign-on for data, applications, and View virtual desktops. Any endpoint managed by Mirage can access Workspace.

ThinApp creates virtual application packages for placement on Mirage-managed desktops, on View virtual desktops, in the Workspace application catalog, or directly on physical and virtual machines.

View manages virtual machines in the data center and remotely displays virtual desktops on endpoint devices. Execution is on the virtual machines stored in the data center. View is ideal for managing highly standardized, stateless virtual desktops in a call center or "follow-me desktop" implementation. Hospitals, public kiosks, and military outposts are all excellent use cases for View. In these implementations, users tend not to have personal computers and access their desktops from thin or zero clients, tablets, or smartphones. On these devices, VMware Horizon Client™ provides access to the View desktop. Users can also access View virtual desktops through an HTML5 browser without Horizon Client installed on the endpoint.

Mirage fits into the Horizon 6 vision by providing centralized image management for physical, virtual, and BYO devices. Mirage complements the View solution. You can use Mirage for customizing and managing physical desktops and keeping endpoint changes synchronized with backup desktop images in the data center. Execution of operations is local to the endpoint, so users can take the PC offline. User personalization is integral to the desktop image. Mirage is ideal for handling persistent, personalized physical desktops and virtual machines.

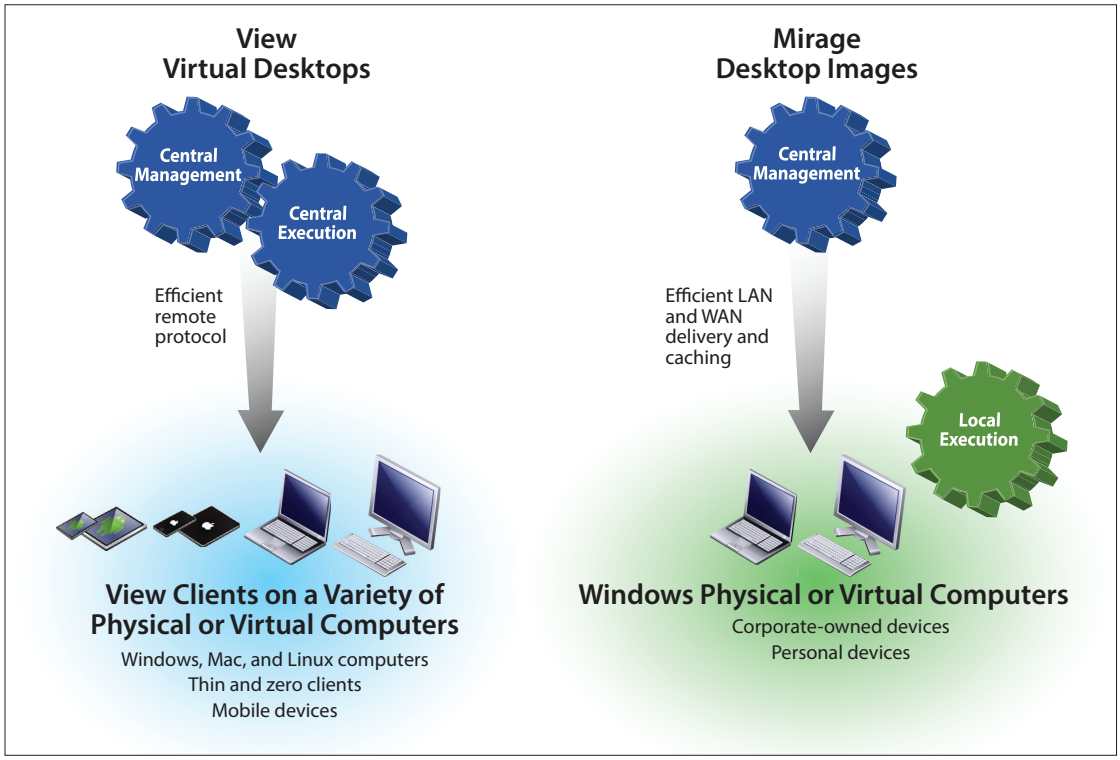


Figure 2: Comparing Central and Local Operations for View and Mirage

Mirage fits these use cases:

- Mobile and laptop users – Users can be offline, but their desktop images are stored in the data center. When the user reconnects to the network, endpoint changes are uploaded to the desktop image in the data center.
- Remote and branch office users – Mirage branch reflectors efficiently download layer updates from the data center to remote endpoints.
- Power users with their own preferred applications – User-installed applications are backed up as part of the desktop image. IT can customize and centrally manage different application layers for subsets of users who use the same applications.

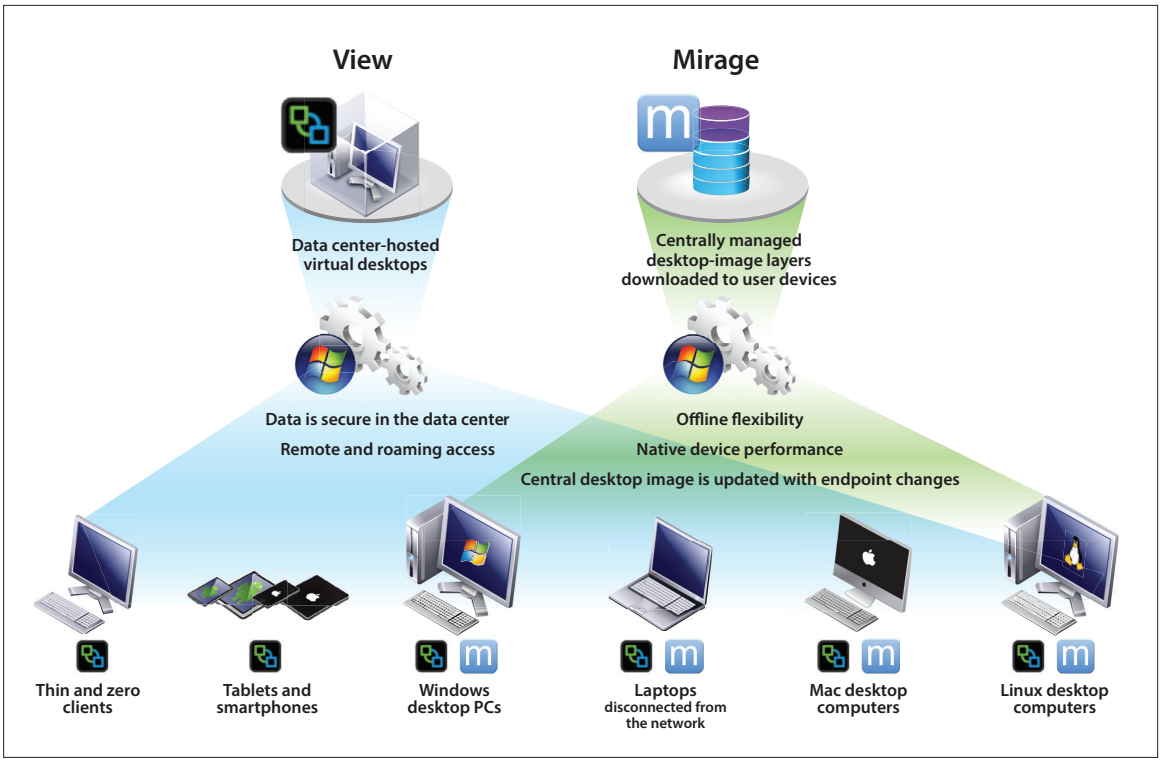


Figure 3: Mirage and View in the VMware End-User Computing Vision

As shown in the figure, View is for remote viewing of centralized virtual desktops from a variety of endpoints. Mirage is for backing up and managing IT-customized layers on the endpoints. On non-Windows physical computers, such as Mac OS and Linux, Mirage can manage Windows virtual machines created with Fusion Pro. Mirage can also manage Windows virtual machines created by VMware Workstation™ or VMware vSphere®. Additionally, Mirage can manage full-clone, persistent virtual desktops in View by updating images to those virtual desktops without losing personalization settings and data.

Key Mirage 5.0 Features

Mirage specializes in the following features:

- Centralized desktop backup
- Recovery of user endpoints
- Operating system migration
- Hardware-refresh migration
- Layered desktop images
- Application layering
- Branch-office desktop management
- Reduced help desk burden for desktop management

Click a feature above for details, or you can proceed to the next section, VMware Mirage Packages and Licensing.

VMware Mirage Packages and Licensing

You can obtain Mirage by purchasing the Mirage bundle, VMware Horizon Advanced Edition, Horizon Enterprise Edition, or the Mirage Windows Migration package.

Mirage Bundle
The Mirage bundle includes the following components:

- Mirage
- Fusion Pro (VMware Fusion® + Player Plus)
- Workstation

> **Note:** The Workstation license included in the Mirage bundle is for administrative use only. It is not for creating virtual machines for end users. Workstation is a recommended platform for IT to capture and build ThinApp virtual applications.

With Fusion Pro installed on a Mac, you can create Windows virtual machine endpoints for use on Mac, Windows, and Linux computers. You can then use Mirage to manage backups of these virtual machine endpoints. You can also create virtual machines to use as Mirage reference machines.

The Mirage bundle offers the following license options:

- Per named user
- Per device

Each product included in the Mirage bundle is also licensed with both the per named user and per device options.

A six-month subscription license exclusively for OS migration is also available. See Mirage Windows Migration Package.

You can obtain a 10-license trial or evaluation version of Mirage. The Mirage software license is separate from the software installers and is installed only on the Mirage Management server. You do not need to install a license for each Mirage server.

Note: Reference machines—where you create base layers and application layers—do not consume licenses. An archived desktop image with no synchronized endpoint also does not consume a license.

Horizon 6

Horizon 6 is available in the following editions, all of which include the components required for an end-to-end virtual desktop deployment. Mirage is included in the Advanced and Enterprise editions.

- Horizon View Standard Edition – Simple, powerful virtual desktop infrastructure (VDI) with great user experience.
- Horizon Advanced Edition – Cost-effective delivery of desktops and applications through a unified workspace.
- Horizon Enterprise Edition – Desktop and application delivery with closed-loop management and automation.

	FEATURE	VIEW STANDARD	ADVANCED	ENTERPRISE
MANAGEMENT	Cloud Automation			
	Design and automate workflows (VMware vCenter™Orchestrator™ + Desktop Plug-In)			✔
	Operations Management			
	Operations dashboard – Health monitoring and performance analytics (VMware vRealize™ Operations Manager™ for Horizon)			✔
	Capacity management – Planning and optimization (vRealize Operations Manager for Horizon)			✔
INFRASTRUCTURE	Storage			
	Virtual storage (VMware Virtual SAN™ for Desktop)		✔	✔
	Applications			
	Application catalog (XA, RDSH, SaaS, ThinApp)		✔	✔
	Application virtualization (hosted apps)		✔	✔
	Application packaging (ThinApp)	✔	✔	✔
	Desktop Infrastructure			
	Image management for physical desktops (Mirage + Fusion Pro)		✔	✔
	Image management for virtual desktops (Mirage for View)		✔	✔
	Virtual desktop infrastructure (View)	✔	✔	✔
	Cloud infrastructure (vSphere Desktop and VMware vCenter™ Desktop)	✔	✔	✔

Table 1: Horizon Components per Edition

Mirage Windows Migration Package
You can purchase a Mirage Windows Migration package for a six-month term per device. You can perform the following with this package:

- Migrate a PC from Windows XP or Windows Vista to Windows 7
- Migrate a PC from Windows 7 to Windows 8.1 or 8.1 Update 1
- Migrate a Windows 7 user to Windows 7, 8.1, or 8.1 Update 1 from an old PC to a new PC (hardware migration)

You can complete migrations across the network, as you can with the full Mirage product. The package includes assessment reports. Licensing for the Mirage Windows Migration package is per named device for a six-month period. The minimum purchase is for 10 devices.

For more information, contact your VMware sales representative or partner representative.

Architecture and Components

This section provides a general overview of how Mirage works and its components and architecture.

How Mirage Works

Mirage is not only a backup tool but also a mechanism to maintain IT-controlled desktop elements. IT can create and manage standardized desktop layers, yet preserve user data and settings on the endpoints. IT can create one or more *base layers*, which consist of the operating system, system software, and core applications. IT can also create supplementary *application layers* for distribution to various groups of users. End users perform daily activities on their own PCs and maintain personal settings and data. Mirage incorporates both the IT-managed and the user-controlled elements into one desktop image, or backup, stored in the data center.

IT also can provision a driver library with the base layer, which detects and fixes broken or missing drivers on endpoints.

You capture a base layer from an IT-configured *reference machine* in the data center. You can have as many reference machines and base layers as needed, and you can capture as many application layers as needed. You capture application layers from devices in a pending state. You assign these base and application layers to endpoints.

If IT does not choose to standardize a base layer and supplementary application layers, the Mirage-managed endpoint is backed up. The desktop image is stored in the data center for desktop recovery operations. IT-managed layers are optional.

If you update your reference machine and want to deploy the changes to the endpoints, you can capture a new base layer from the updated reference machine and assign it.

If you need new applications, you capture new application layers from pending devices and then perform an update to the application layers.

After you assign a new base layer or update the application layers, Mirage replaces the image with minimal downtime for the user and no travel to remote sites for IT. Update operations accommodate user activity on the endpoint. Users remain productive and unaware of the update process. After a layer update, users are prompted to reboot at a convenient time.

To activate an endpoint within Mirage, you install the Mirage client and *centralize* the endpoint (back it up) to the data center.

Mirage takes periodic *snapshots* of the endpoint and stores them in the data center with the original backup image. These snapshots capture incremental changes to the full desktop image and provide time-stamped rollback points for restoring the desktop to a previous system state. The IT administrator has the option of restoring user settings and files along with the IT-controlled elements of the desktop.

Mirage can coexist with your existing IT infrastructure. You can continue to use your electronic software distribution tools, such as SCCM, to deploy individual applications to PCs, an application virtualization program to encapsulate application packages, and application presentation tools such as XenApp. Mirage deploys desktop images, not individual applications, and these desktop images can contain IT-controlled base and application layers. Any changes to user-installed applications are backed up to the desktop image.

Mirage Architecture

The Mirage server (or a cluster of Mirage servers) manages the desktop images in the data center and orchestrates uploads and downloads between data center desktop images and Mirage-managed endpoints.

Storage in the data center contains the desktop images and the base and application layers. The Mirage database contains pointers to the base and application layers and desktop images in storage and an inventory of what is on the endpoints. The database catalogs the information while the storage contains the actual information.

Each Mirage-managed physical or virtual computer has the Mirage client installed. The Mirage client communicates closely with the Mirage server to synchronize the data center desktop image with changes to the endpoint.

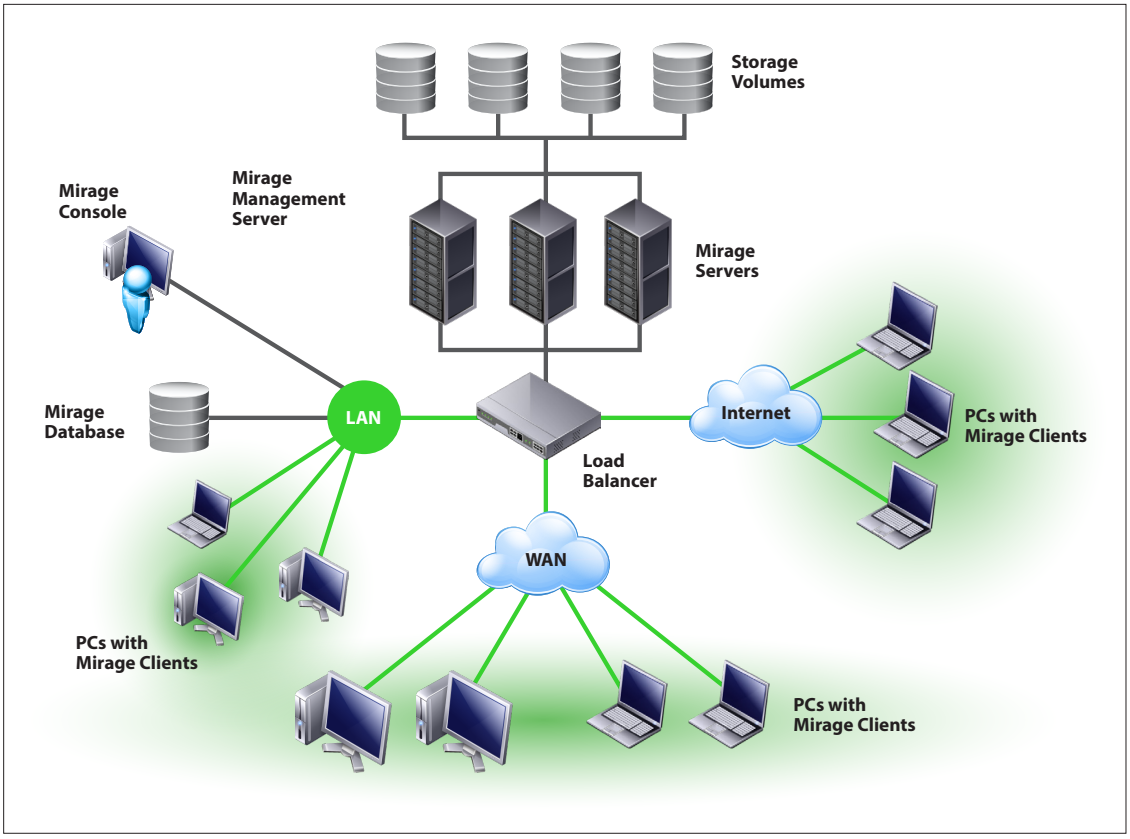


Figure 4: Mirage Clustered Deployment

Storage Setup

Storage that is assigned to Mirage contains the centralized virtual desktops (CVDs, also referred to as desktop backups), base layers, and app layers.

Mirage supports SAN, NAS, or local storage. The chosen storage must support alternate data streams where appropriate.

On average, plan for 20–30 GB of space per user. Deduplication through Mirage usually saves 30–50 percent in storage space. For storage savings of up to 25 percent, enable compression on the selected Mirage storage volume.

If you have a large user base or want storage fault tolerance, set up multiple CIFS storage volumes. For more information, see *Deploying Multiple Storage Volumes* in the VMware Mirage Administrator's Guide.

Storage is optimized with global data deduplication at the file and block level. Mirage has additional optimizations for Microsoft Outlook PST files.

Network Setup

WAN operations are optimized with Mirage. Only distinct bits of data are passed along the network, and all transfers are compressed.

Network utilization with Mirage averages 15 Kbps of sustained communication from the endpoint, or about 50 Mb per user per day. You can throttle bandwidth on any router in your environment to ensure top performance. Mirage supports quality of service (QoS) software.

The Mirage client dynamically adjusts bandwidth on the client side to ensure the best user experience. In addition, end users can "snooze" any Mirage network operations, such as uploads of endpoint changes to the data center.

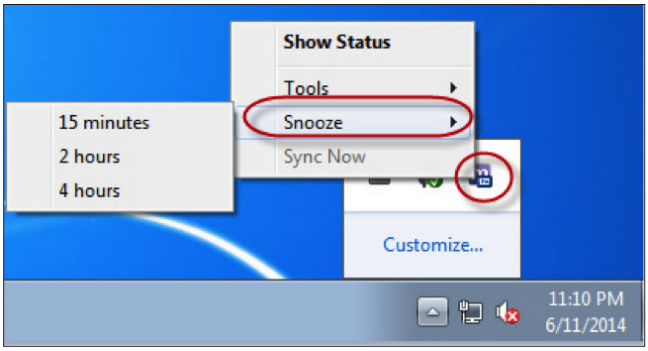


Figure 5: Choosing Snooze from the Mirage Client System Tray Icon

Security Setup

You can globally enable SSL for all Mirage client-server communication. For details, see *Setting Up the SSL Certificate in Windows Server* in the VMware Mirage Administrator's Guide.

To protect user data, Mirage uses NTFS on the server side so that regular Windows Security applies through access-control-list object permissions. If you choose NAS instead, you can leverage vendor data security tools and use them in conjunction with Mirage. For example, to configure NetApp NAS security to mimic pure Microsoft NTFS permissions, see the VMware Knowledge Base article Configuring Mirage Storage security.

During backup and restore operations, Mirage uses the MD5 algorithm to ensure data integrity.

Mirage is compatible with

- Microsoft Encrypting File System (EFS)
- Microsoft BitLocker drive encryption
- Sophos SafeGuard hard drive encryption
- Other encryption technologies

This versatility enables you to decrypt on backup and re-encrypt on restore. If you are performing a Mirage operation that modifies the master boot record (MBR), you must decrypt the data on the endpoint before starting the operation. If you are performing an OS migration and your endpoint is encrypted with Sophos SafeGuard Enterprise 5.5, you do not need to encrypt the endpoint. If you are using other third-party, full-disk-encryption tools, you need to decrypt the endpoint before OS migration.

Server Clustering and Scalability

You can have up to 1,500 Mirage-enabled endpoints per Mirage server. The following table lists the suggested configurations for virtual and physical Mirage servers.

	VIRTUAL MIRAGE SERVER	PHYSICAL MIRAGE SERVER
Maximum Supported Endpoints with CVDs (backups)	1,500	1,500
Required CPUs on Mirage server for CVDs	8 vCPUs	Dual Quad
Required memory on Mirage server for CVDs	16 GB	16 GB
Required local storage attached to the Mirage server for the OS, Mirage installation, and local cache	150 GB	150 GB

Table 2: Suggested Configurations for Virtual and Physical Mirage Server Instances

You can have as many Mirage servers in a cluster as you want, as long as the number of endpoints or CVDs supported by that cluster does not exceed 20,000. This number can be a combination of physical and virtual Mirage servers. All Mirage servers are managed by one Mirage Management server. A load balancer, or round-robin DNS entry, is required to direct endpoint traffic to the Mirage servers.

Mirage Components and Terminology

See Figure 4 for an architectural diagram of a Mirage deployment. Mirage has components in the data center for controlling and managing all Mirage operations and objects:

- Mirage server
- Mirage Management server
- Mirage Console
- Database for Mirage

The file portal and driver library can reside on the Mirage server or on another server in the domain.

A Mirage client is installed on each endpoint.

To more efficiently manage Mirage updates to endpoints in remote offices, you can designate a PC Mirage client in the branch office as a branch reflector.

The following subsections provide details about Mirage components and other terminology.

Mirage Server

The Mirage server controls all Mirage operations and objects. It manages desktop images (CVDs), base layers, and application layers in the data center.

The local cache on the Mirage server stores commonly used data blocks. The server uses the local cache to perform data deduplication over the WAN. When large files are transferred over the WAN, blocks are put into the cache. The next time similar files are transferred, the Mirage server obtains the blocks from the cache instead of transferring them over the network. The cache is best kept on fast storage: a local drive or SSD drive.

You can have a cluster of Mirage servers, which are managed by the Mirage Management server.

Mirage Management Server

If you have more than one Mirage server, the Mirage Management server controls and manages the Mirage server cluster. The Mirage Management server is also the interface with the database and updates the database.

Mirage Console

The Mirage Console, previously named the Mirage Management console, is the UI for the Mirage Management server. Through the Mirage Console, the administrator manages the Mirage server deployment functions. The Mirage Console is installed as a Microsoft Management Console Snap-In.

The Mirage Console provides wizards for easy administration of the following common Mirage functions:

- Centralizing endpoints
- Disaster recovery
- Assigning a base layer
- Capturing a base layer
- Windows OS migration
- Base layer provisioning
- Hardware migration
- Updating app layers
- Capturing app layers

You can access these wizards by selecting VMware Mirage > Mirage System > Common Wizards from the left pane of the Mirage Console.

Mirage Gateway

The Mirage Gateway provides end users secure communication to Mirage servers without using VPN configurations. You deploy the Mirage Gateway outside the Mirage data center environment.

Mirage Web Manager

Mirage Web Manager is a Web-based tool that provides some of the same administrative capabilities available in the Mirage Console. Administrators with either the Help Desk role or the Protection Manager role use Mirage Web Manager to resolve endpoint issues.

Database for Mirage

The Mirage server components require a connection to a Microsoft SQL database. The database contains pointers to the base and application layers and desktop images in storage, an inventory of what is on each endpoint, and driver library information. The database catalogs information for the Mirage system. The actual files of information are in storage.

Mirage File Portal

End users can view their folders and files within historical *snapshots* of their data center desktop image in the optional Mirage file portal. Users can access their files through a Web browser from any device. Because these files are stored in the data center, users can view their files even if the Mirage-managed endpoint is damaged or lost. The files are read-only.

The file portal resides on a server within the domain. It can co-reside with the Mirage server.

For information on installing and accessing the file portal, see the VMware Mirage Installation Guide.

Driver Library

The optional Mirage driver library decouples the Mirage base layer from the hardware and enables IT to build base layers that are agnostic to the hardware on the endpoints. The driver library detects missing or broken drivers on endpoints and then fixes them. The driver library does not upgrade or take other action on existing healthy drivers on endpoints.

The driver library is independent of the base layer and is applied to endpoints after you create the following items:

- Folders containing device drivers
- Profiles for matching endpoints to device drivers

You import hardware-specific device drivers into the Mirage system and set up folders to organize the drivers. You then create driver profiles.

The driver library must be on a server within the domain. It can reside on the Mirage server.

For more information, see *Managing the Driver Library* in the VMware Mirage Administrator's Guide.

Driver Profiles

You create driver profiles when you set up a Mirage driver library. To configure the library, choose a set of drivers and create rules that specify which hardware to apply the profile to by vendor and operating system version.

During Mirage operations such as migrations, base layer updates, and centralization, the drivers are applied to the endpoints according to the rules you set up for matching drivers to endpoints.

Mirage Client
The Mirage client has a role in managing uploads and downloads between the data center desktop image and the endpoint. The Mirage client helps in the following activities:

• Uploading endpoint changes to the data center desktop image

• Downloading IT layer updates to the endpoint

You install the Mirage client on all endpoints that you want to manage with Mirage. The client installs directly on Windows systems. The Windows systems can be physical machines, such as desktops and laptops, and virtual machines, such as Fusion Pro, Workstation, and vSphere virtual machines.

The Mirage client is less than 10 MB in size.

Branch Reflector
An optional branch reflector serves as a local Mirage update service for peer PCs in a branch office deployment. Branch reflectors are more efficient at downloading IT layer updates and reduce bandwidth usage on the WAN. If a branch contains a large number of endpoints, you could dedicate an endpoint as a branch reflector to provide more resources to the upload and download processes.

Any Mirage-enabled endpoint can act as a branch reflector for peer-to-peer downloads at the remote office. You can designate one or more endpoint devices as branch reflectors. No special setup, installation, or infrastructure is required.

For more information, see Branch-Office Desktop Management.

Other Important Mirage Terminology
The following terms and concepts are useful to understanding Mirage:

• Alarms

• App layers

• Assigned devices

• Base layer

• CVDs

• CVD collection

• CVD polices

• Endpoints

• Pending devices

• Reference machine

• Rejected devices

• Roles

• Snapshots

Alarms
An open alarm icon in the Mirage Console or Web Manager indicates that a potential issue exists with a desktop image. For example, the alarm could pertain to an endpoint that does not have enough disk space. Mirage provides information about the alarm to help you determine which actions to take to resolve the issue.

App Layers
An app layer is a template for deploying one or more applications to specific Mirage endpoints. Creating an app layer with a single application is often the best approach because you can update the application without affecting other applications.

To deploy specific applications to specific endpoints or groups of endpoints, you can capture and assign app layers. However, if you want to provide all members of your organization access to the same applications, you can include those applications in the base layer, and not create an app layer.

App layers require a base layer, but you can update the base layer and app layers on an endpoint independently.

You can use the provided wizard to assign an app layer.

Assigned Devices
A pending device becomes an assigned device when an administrator or the end user activates it. Activating a device centralizes it, and it appears in the Mirage Console as an assigned device.

By logging in for the first time, the end user activates the device automatically. In contrast, an administrator activates the device manually. Administrators have control over the details of device activation that end users do not have. For example, an administrator can select the CVD policy, determine on which volumes to place CVDs, and decide whether to assign a base layer to the device.

Base Layer
A base layer is a template for deploying common desktop content to Mirage endpoints. The base layer includes the operating system, service packs and patches, and core enterprise applications and their settings.

CVDs
The centralized virtual desktop (CVD) is the image backup of an endpoint. The end user performs daily functions locally on the endpoint. All changes to the endpoint are backed up to the CVD. A Mirage-enabled endpoint is not a remote display of the centralized desktop image in the data center.

The Mirage user interface uses the term CVD frequently. This guide echoes the usage of CVD for procedures involving the user interface, but often substitutes the terms desktop image or backup in the description.

CVD Collection
You can group CVDs that share a logical relationship in a collection folder. For example, you can place all CVDs of users in the Sales department in a collection folder named Sales. You can then perform an action, such as updating a base layer or CVD policy, on all the CVDs in the collection at once.

CVD Policies
A CVD policy, or upload policy, consists of rules that determine which files and directories are uploaded from the endpoint to the CVD. You can define your own CVD policies or use the policy provided with Mirage. You need to specify the default CVD policy if you allow end users to activate their endpoints.

Endpoints
An endpoint is a physical or virtual machine on which the Mirage client is installed, enabling it to communicate with a Mirage server. This is sometimes referred to as a *Mirage-enabled endpoint*.

Pending Devices
A pending device is a Mirage endpoint that has not yet been activated or centralized. This endpoint appears in the Mirage Console as a pending device.

Reference Machines
A reference machine is an endpoint managed by an administrator and used to capture base layers. You need to create a reference CVD for the reference machine before capturing a base layer from it. To capture a new base layer or a new version of an existing base layer, you update the reference machine and upload the changes to the reference CVD.

Rejected Devices
A pending device becomes a rejected device when you specifically reject it from the Mirage Console. The Mirage server does not honor communication requests from rejected devices. You can view and reinstate rejected devices at anytime.

Roles
Roles are mapped to operations that users can perform with the Mirage Console or Web Manager. Typical operations are managing CVDs, base layers, users, groups, and events, and viewing the dashboard and other system information. You can use the Mirage Console to grant a role to one or more Active Directory (AD) groups.

The Mirage server identifies users by AD group membership and assigns their matching user roles in the system. Mirage provides predefined roles. You can also define roles to meet the specific needs of your organization.

Mirage provides the following predefined roles:

- Mirage Console roles
  - Administrator
  - Desktop Engineer
  - Helpdesk
- Web Manager roles
  - Web Help Desk
  - Web Protection Manager

For more information about managing user roles, see the VMware Mirage Administrator's Guide.

Snapshots
Mirage snapshots are distinct from Mirage desktop images and virtual machine snapshots.

A Mirage desktop image (CVD) is a backup of the endpoint taken when the Mirage-managed endpoint is first activated. Only one desktop image for each endpoint is stored in the data center. Mirage incremental snapshots build on this foundational desktop image.

A Mirage snapshot contains only the incremental changes to the original desktop image since the previous snapshot. The purpose of the snapshot is for rolling back the endpoint to a previous state, if needed. Multiple endpoint snapshots are stored in the data center. Snapshots occur automatically and are taken at a configurable interval. The default is every 24 hours, but you can configure whether snapshots are taken daily or hourly.

By default, the number of snapshots retained are

- Zero hourly
- Seven daily
- Three weekly
- Eleven monthly

This means that you have

- A daily snapshot to roll back to for the previous week
- A weekly snapshot to roll back to for the previous month
- A monthly snapshot to roll back to for the previous year

You can configure the number of snapshots to take for the various intervals.

- Hourly snapshots kept per day
- Daily snapshots kept per week
- Weekly snapshots kept per month
- Monthly snapshots per year

By configuring the number of snapshots to retain at one-hour intervals, you are adding hourly snapshots to the default daily snapshots.

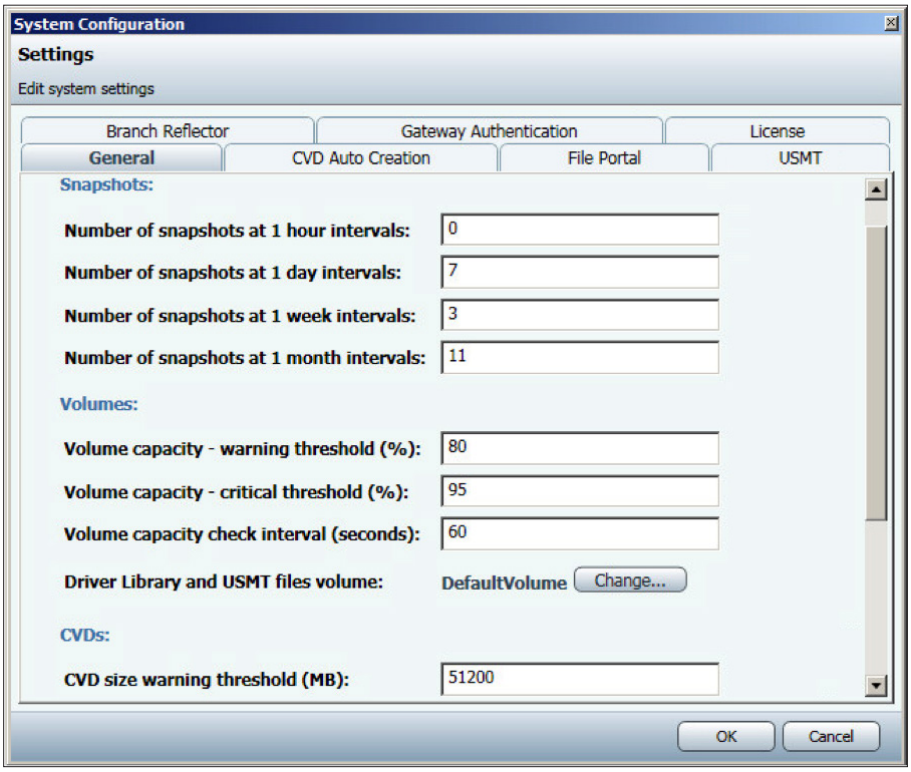


Figure 6: Default Configuration of Frequency and Retention of Snapshots

For more information, see *CVD Snapshot Generation and Retention* in the VMware Mirage Administrator's Guide.

Additional snapshots are taken

- Before a base or application layer update
- Before reverting to a snapshot
- Before a migration
- When an administrator manually invokes a backup using the Force Upload option for an endpoint available in the Pending Devices pane

These extra snapshots ensure the ability to roll back to a critical desktop state. These snapshots are counted as part of the number of daily snapshots retained.

When you monitor the endpoint, reference machine, and various Mirage Console panes, you might notice upload events during a process that you have started. These processes are often the automatic snapshots taken before major changes to the endpoint, such as a migration or a layer update.

You might also notice automatic hourly incremental snapshots that Mirage takes for its own internal system use, aside from your configured hourly or daily snapshots. Evidence of this upload of data from the endpoint to the data center appears in various Mirage Console panes and in the detail window of the Mirage system tray icon for an endpoint. You can see a record of these hourly incremental snapshots in Logs > Transaction Log.

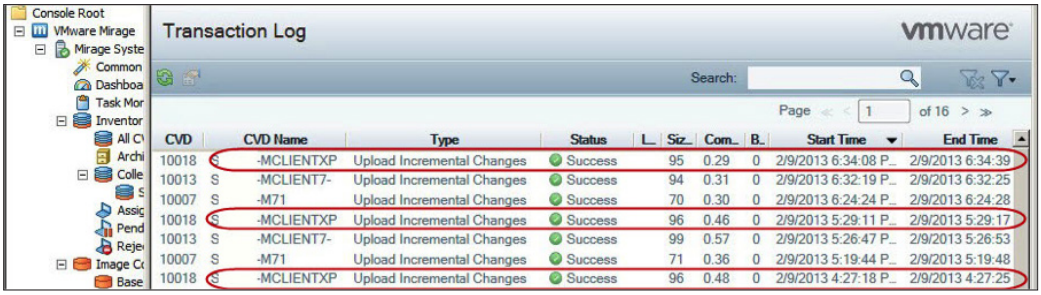


Figure 7: Transaction Log Showing Automatic, Internally Used System Snapshots of the Endpoint

You might also be using virtual machine snapshots, which are different from Mirage snapshots. A virtual machine snapshot is taken in Fusion Pro, Player Plus, or vSphere for the purpose of rolling back the virtual machine to a prior state, if needed. It is used outside of Mirage to manipulate virtual machines. Multiple virtual machine snapshots are stored in the virtual machine files.

Mirage Feature Details

The following list provides more information about Mirage features.

Centralized Desktop Backup

Mirage gives you centralized storage of desktop images, with execution of all desktop operations on the local machine. Mirage manages the desktop image using a layered approach. Mirage can manage either physical computers or virtual machines within physical computers.

For a hands-on exercise in backing up a desktop, see Working with Base and Application Layers.

Recovery of User Endpoints

Mirage takes snapshots of the user desktop, which enables quick recovery or rollback to a previous desktop state. Changes to the endpoint are captured and periodically uploaded to the desktop image in the data center.

Other products require an all-or-nothing desktop restoration. Mirage offers the option of restoring specific layers while preserving others. You can restore an endpoint to a previous snapshot without overwriting user data. If a computer is stolen, damaged, or lost, you can restore the entire computer to a replacement device or restore only selected layers. You can temporarily migrate a physical computer to a virtual machine until a replacement device arrives. If the information on a computer hard disk is corrupted, you can overwrite the prior information and restore the desktop image to the same device.

For a hands-on exercise in restoring a PC, see Data Recovery and Backup.

OS Migration

Mirage facilitates the migration process from one version of Windows to another. You do not need to use a diverse set of incompatible tools to manually manage the deployment of new Windows OS images. Instead, with Mirage, you use a migration wizard to automate in-place upgrades from one Windows OS to another, such as Windows XP to Windows 7, or Windows 7 to Windows 8.1.

Note: References in this guide to Windows 8.1 also apply to Windows 8.1 Update 1.

You can even migrate users between physical and virtual machines during the Mirage Windows migration process. IT orchestrates the migration from the data center. The procedure operates on many PCs at once, so IT staff time is greatly reduced.

PCLM tools typically require the endpoint to be out of operation during a migration from one OS version to another. With Mirage, downloading the new version takes place in the background while users continue working. When the download is complete, users reboot their endpoints, and the exchange of the OS versions occurs. User downtime during a Mirage Windows migration is minimized and is typically only 30–60 minutes.

The migration can be "zero touch" for IT. IT usually does not need to boot individual endpoints, either locally or remotely. Users can choose when to reboot to the new OS, or IT can have everyone reboot at once, such as at the beginning of a work day.

During a migration, Mirage preserves user data and profile information, and IT can move this data to the new OS. Users do not need to re-personalize their computers after the upgrade.

Note: When migrating from different Windows operating systems, such as from Windows XP to Windows 7, data and profiles are migrated while user-installed applications are not. The reason is because applications that are compatible with one Windows OS might not be compatible with another.

Mirage takes a snapshot of each system being migrated before replacing the contents of the desktop. You can use the snapshot to roll back the computer to the previous Windows OS, if needed.

For a hands-on exercise, see Migrating to Windows 7 or 8.1.

Hardware Refresh

With Mirage, you can conveniently migrate all user settings and data to new devices during hardware refresh cycles. If the OS version is the same on the old and new devices, all user-controlled elements can be migrated in full to new hardware. You can even restore a complete user desktop to a new make and model of computer.

The first step is to install the Mirage client on the new Windows computer. Then you use the Hardware Migration wizard to download IT layers and user personalizations. This entire hardware migration process can be zero touch—IT usually does not need to manually touch the endpoint to configure it.

Layered Desktop Images

Mirage divides the desktop image into logical layers. IT has the option of creating and managing standardized layers that are stored in the data center and applied to user endpoints. Depending on IT policies, users can install their own applications and add user data and settings to their endpoint PCs. Both IT-managed elements and user-controlled elements are rolled into one Mirage desktop image in the data center.

IT can create base layers and application layers. A base layer includes the OS, system-level infrastructure software (security products such as antivirus software, connectivity software such as VPN, and firewalls), service packs and patches, and core applications and their settings. Core applications must have enterprise volume licenses. Base layers are hardware-independent.

An application layer contains applications that IT wants to distribute to specific groups of users, such as to different departments.

The desktop image contains both the IT-managed layers and the user-controlled elements. IT downloads layer updates to the endpoint. These layer updates and any user-initiated changes on the endpoint are uploaded to the data center to fully back up the endpoint.

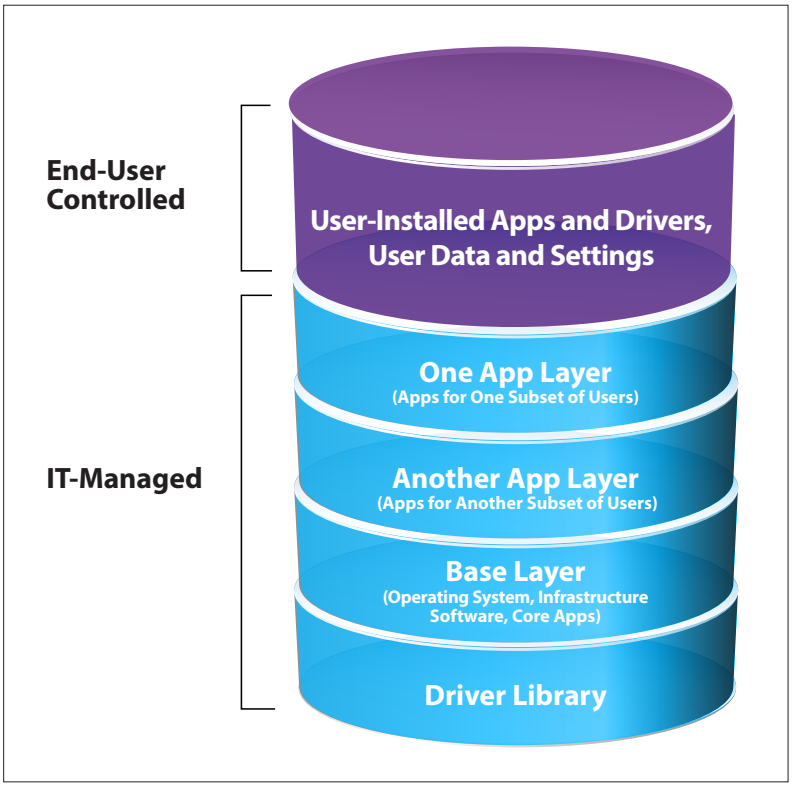


Figure 8: Logical Layers of a Mirage Desktop Image

If IT wants to standardize a base layer and application layers, IT generates these layers, and the user PC is updated with the layers. If IT does *not* generate these layers, users are in control of their own Windows OS environment and applications, and the entire user-generated PC is imaged.

IT can use the desktop image layering approach for modular migration, restoration, and updating. You can migrate, update, or restore each layer independently. For example, you can update the OS base layer but not the application layers. Mirage preserves end-user files, personalization, and user-installed applications during layer updates.

You can deliver patches by updating a base layer in the data center and deploying the updated base layer to the endpoints.

For a hands-on exercise in working with base layers, see Working with Base and Application Layers.

Application Layers

Application layering extends the base layer image management capabilities of Mirage. You can define and capture layers containing only applications and deliver the application layers to Mirage-managed devices independently of the base layer. One endpoint can receive multiple IT-defined application layers, and multiple endpoints can receive the same application layer. Application layering reduces "gold image sprawl" by isolating group-specific applications from the base layer. Using different application layers enables IT to maintain desktop compliance across multiple lines of business.

Mirage application layering is a unique solution for packaging Windows applications and distributing them to user endpoints. It does not require that applications be installed on the endpoints. Other deployment mechanisms require that the applications are installed on each endpoint. This approach can result in complications due to network connection issues, variable endpoint configurations, and users interrupting the installation.

Application layers are deployed in the background at the file system and registry level. Users can continue working with their existing applications while a new application layer is being deployed. A restart might be required at the end of the application layer deployment.

Distribution of application layers uses the same technology as Mirage base layers. The download is WAN-optimized to enable the following behaviors:

- Only new blocks of data are transferred to endpoints, and existing blocks of data are reused.
- Network disruptions and low bandwidth are automatically handled.

An application layer can contain the following kinds of applications:

- A single application, a suite of applications from the same vendor, or a set of line of business (LOB) applications, such as for a specific department or group
- OEM applications (see the VMware Mirage Administrator's Guide)
- Natively installed applications or ThinApp virtual application packages
- ThinApp packages can be either locally deployed in the application layer or streamed from a network share using a user shortcut in the application layer. A shortcut in the application layer points to the virtual application on a file share. For more information, see Table 3.

The following types of applications are not yet supported or not fully supported in application layers:

- Disk encryption software
- Kaspersky Internet Security
- Microsoft SQL Server
- Applications that make changes to the MBR or disk blocks
- Applications that deploy a system driver

It is a best practice to install the following applications in the base layer, not in an application layer:

- Windows security applications, such as antivirus, antimalware, and firewall
- Windows components and frameworks, such as .NET and Java
- Global Windows configurations and setting changes

The following table describes the differences between natively installed applications and ThinApp virtual applications in application layers.

NATIVELY INSTALLED APPLICATIONS	THINAPP VIRTUAL APPLICATIONS
Behave the same as applications installed directly on the user endpoint.	Behave the same as ThinApp packages or shortcuts placed on the user endpoint. ThinApp packages run without interaction with other native or virtual applications on the desktop image.
Execute locally on the endpoint.	Execute in virtual memory space, whether deployed locally on the endpoint or streamed from a network share.
Do not require network access for execution.	Require network access to the file share if streamed using a shortcut in the application layer.

Table 3: Differences Between Mirage Application Layers for Natively Installed Applications and ThinApp Virtual Applications

The following table lists application components that can and cannot be included in Mirage application layers.

CAN BE INCLUDED IN MIRAGE APPLICATION LAYERS	CANNOT BE INCLUDED IN MIRAGE APPLICATION LAYERS
Updates and patches related to the installed application	Network components, such as personal firewalls and VPN virtual adapters*
Application customizations	Windows licenses*
Global application configurations and settings	User-specific changes and user accounts and groups (for both local and domain users)
File and registry changes created by the installed application, or a custom set of files and registry entries	OS components or OS-bundled applications, such as the .NET framework, Windows updates, Internet Explorer, Windows Media Player, and language packs*
Kernel drivers	Drivers installed in the Windows driver store**
COM objects	
Global .NET assemblies	
Windows services	
Shell extensions	
Browser plug-ins	

Table 4. Application Components That Can and Cannot Be Included in Application Layers

*You can, however, deliver these components in a base layer.

**You can include drivers with the Mirage driver library or by adding driver packages to the Windows driver search path (DevicePath). You can also deliver drivers as part of the base layer.

If conflicts occur between an application in the application layer and an application in the base layer, the base layer application takes precedence over the application layer. For example, if Microsoft Word is in both an application layer and the base layer, the Word settings in the base layer supersede the settings of Word in the application layer.

For a hands-on exercise in working with application layers, see Using Mirage to Work with Base and Application Layers.

Branch and Remote Office Desktop Management

Other products require that remote users connect to the data center to update their computers, but Mirage permits local updates for remote users. In a branch or remote office, you can designate a local Mirage-managed endpoint as a branch reflector to handle layer updates for local PCs. Peer Mirage-enabled endpoints can then download layer updates from the branch reflector instead of from the Mirage server in the data center.

The branch reflector reduces bandwidth usage for the following downloads of IT-managed elements from the data center:

- Base layer
- Driver library
- Application layers
- Microsoft User State Migration Tools (USMT) files

Instead of multiple endpoints downloading updated layers from a distant Mirage server over the WAN, the branch reflector communicates with the Mirage server, downloads the differences between the data center layers and the endpoint layers, and stores the data locally. The endpoints on the subnetwork that matches the configuration of the branch reflector try to download IT-managed elements from the branch reflectors.

Branch reflectors can provide different sets of layer updates for different endpoints in the branch office, including its own required layer updates. Branch reflectors are not used for uploads of endpoint changes to the data center. This action is performed over the WAN, with optimizations to accommodate user activity.

Mirage branch office implementations are efficient for software delivery (application layer updates) and for Windows OS base layer migrations. The WAN handles only a single image, instead of multiple images.

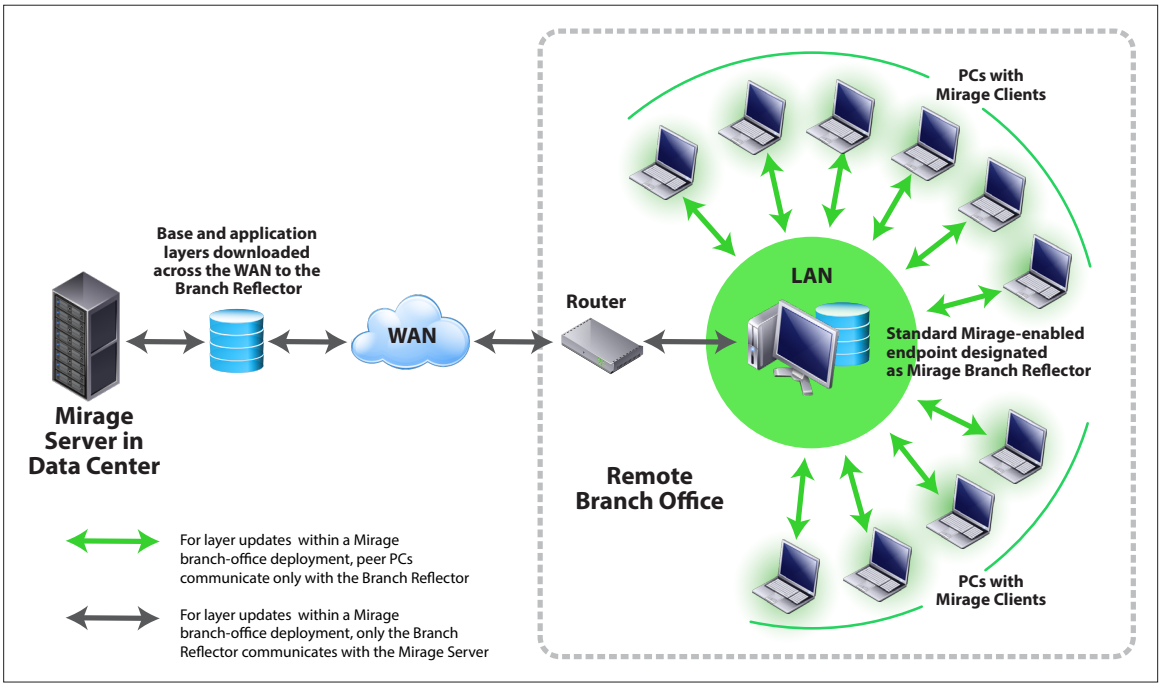


Figure 9: Layer Updates in a Branch Office Deployment

You use the Mirage Console to designate, enable, and configure a branch reflector. You can assign specific values to individual branch reflectors. The default parameters are

- Default Maximum Connections – Maximum number of simultaneous endpoint connections to the branch reflector.
- Default Cache Size in GB – Cache size allocated for the Mirage image cache in the branch reflector.
- Required Proximity in msec – If a ping from an endpoint to the branch reflector is not answered within this time, the endpoint downloads from the Mirage server instead.
- Use Active Directory Sites – Whether to use Active Directory site information to determine which of several available branch reflectors an endpoint should connect to. Mirage uses subnet and physical proximity information from Active Directory to determine optimal connections.
- Always Prefer Branch Reflector – If a branch reflector is not close enough as determined by the Required Proximity setting, this configuration requires Mirage-enabled endpoints to repeat the matching process until a suitable branch reflector becomes available. If the Use Active Directory Sites setting is enabled, the Always Prefer Branch Reflector setting makes use of Active Directory to find suitable branch reflectors. The endpoint keeps pinging the branch reflectors until one is within the required proximity. Connection to the Mirage server in the data center occurs only if no branch reflectors are defined. If the Always Prefer Branch Reflector setting is not selected, and no branch reflector is available within the required proximity, the Mirage-enabled endpoint connects to the Mirage server directly.

The parameters for individual branch reflectors are

- Maximum Connections
- Cache Size in GB
- Additional Networks – Networks other than its own local subnets on which the branch reflector can service Mirage clients

Connect the branch reflector to a switched LAN, not to a wireless network. The branch reflector needs enough space to store the IT-managed layers for the various endpoint devices at the branch office.

For other branch reflector system requirements, see the VMware Mirage Administrator's Guide.

Reduced Help Desk Burden for Desktop Management
Mirage enables Tier-1 IT staff to solve desktop problems with a few simple clicks on the Mirage Console without the need for diagnosis or escalation. This is accomplished through the disaster recovery options, such as reverting to a previous snapshot.

Hands-On Evaluation Exercises for Mirage

This section walks you through

- The upgrade or installation of Mirage
- The preparation of the reference machine and test machines
- Implementing some key features so that you can experience and evaluate Mirage key features in a test environment

If an exercise builds on another, information at the beginning of the exercise explains the connection.

To perform the hands-on evaluation exercises, you must first upgrade to or install Mirage 5.0. Also confirm that you meet the system requirements.

- Preparation
  - Operating System and Software Requirements
  - Data to Gather Prior to Evaluation Exercises
  - Download VMware Mirage Software
- Upgrading or installing
  - Upgrading from Prior Versions of VMware Mirage
  - New Installation and Configuration

After you perform the upgrade or installation, ensure that the following tasks are performed and requirements met:

- Requirements for the Mirage Evaluation Exercises
- Preparing the Reference Machine and Test Machines

After you ensure that the requirements for the evaluation exercises are met and the appropriate machines are prepared, your Mirage 5.0 evaluation environment is ready.

Performing the following exercises introduces you to the basic Mirage procedures:

1. Create a Reference CVD and Capture a Base Layer
2. Capture an App Layer (Optional)
3. Configure the Driver Library and Profile (Optional)
4. Centralize Endpoints
5. Migrate to Windows 7 or 8.1
6. Work with Base and Application Layers
7. Recover Data
8. Use the Mirage File Portal to Enable Users to View Files and Folders
9. Create a CVD Policy for Layer Management
10. Manage Images with View Desktops
11. Work with the Mirage Gateway

For more information on these tasks, see the VMware Mirage Documentation.

For testing purposes, such as in this evaluation, you can install the Mirage components on one Windows server. In a production environment, you must use several Windows servers to install the Mirage components.

Operating System and Software Requirements

The following table lists the current operating system and software requirements. For the most current information, check the VMware Mirage Release Notes and the VMware Mirage Administrator's Guide.

Note: References in this guide to Windows 8.1 also apply to Windows 8.1 Update 1.

MIRAGE COMPONENT	PRIMARY REQUIREMENTS	INSTALLED COMPONENTS
Mirage server	• Windows Server 2008 R2 (Standard Edition), 64-bit or Windows Server 2012 (Standard Edition), 64-bit • Domain membership	• .NET Framework 3.5 SP1, 64-bit • SQL database management system (MS SQL Server 2008 R2; Standard, Express, or Enterprise; 64-bit)
Mirage Management server	• Windows Server 2008 R2 Standard Edition, 64-bit or Windows Server 2012 (Standard Edition), 64-bit • Domain membership	.NET Framework 3.5 SP1, 64-bit
Mirage Console	• Windows XP Professional with SP2 or SP3, 32-bit or • Windows 7 Professional or Enterprise, 32- or 64-bit*	• .NET Framework 3.5 SP1 • MMC 3.0 (see MMC 3.0 update is available for Windows Server 2003 and for Windows XP)
Mirage client**	• Windows XP Professional with SP2 or SP3, 32-bit or • Windows 7 Professional or Enterprise, 32- or 64-bit or • Windows 8.1	.NET Framework 3.5 SP1
Reference machine	• Windows XP Professional with SP2 or SP3, 32-bit or • Windows 7 Professional or Enterprise, 32- or 64-bit or • Windows 8.1	• Mirage client • OS and applications must use volume licenses and be designed for multiuser, multimachine deployment • No applications that install and use - Hardware-specific licenses - Local user accounts or groups • No software that uses a proprietary update service; install such software directly on endpoints
File portal	IIS 7.0 or later	• ASP .NET feature • IIS 7.0 or later, with the IIS 6 Management Compatibility Role

MIRAGE COMPONENT	PRIMARY REQUIREMENTS	INSTALLED COMPONENTS
*The Mirage Console can also be on a Windows Server machine. The minimum configuration is Windows XP or Windows 7. **Turn off XP Fast User Switching mode if the computer is not an AD domain member. See How to Use the Fast User Switching Feature in Windows XP.		

Table 5: Mirage Operating System and Software Requirements

See the VMware Mirage Administrator's Guide for details on

- Hardware requirements
- Storage requirements
- Database requirements
- Communication ports and protocols

Data to Gather Prior to Evaluation Exercises

As you work through the installation, note the following information so that you can reuse it later during the hands-on exercises.

SQL SERVER INFORMATION
Name given to your SQL Server:
SQL instance name (if not using the default):
MIRAGE CLUSTER STORAGE FOLDER
Storage folder (if remote storage, use UNC path):
MIRAGE SERVICES ACCOUNT INFORMATION*
Fully qualified name of account:
Password:
MIRAGE ADMINISTRATOR'S GROUP
Fully qualified name of administrator's group (<domain>\<groupname>):
MIRAGE MANAGEMENT SERVER ADDRESS
IP address or host name:
MIRAGE LICENSE KEY (SERIAL KEY)
License key number (supplied separately from the software):
MIRAGE SERVER LOCAL CACHE FOLDER
Path and folder to local cache if different from the default:
Size of local cache:
*If you are using a standalone server with local storage, you do not need a dedicated Mirage services user account. However, if you are mounting an NFS or CIFS share over a network, or you are installing the optional file portal feature, you must set up a dedicated Mirage services account to access storage and the database. The account must have • Local administrator permissions on Mirage servers • Read and write permissions to the database, with database creation permission • Read and write permissions to relevant storage areas

Table 6: Information Needed During a Mirage Installation

Download VMware Mirage Software

Download the licensed VMware Mirage software or the trial evaluation. Place each installer on the server where you will create the Mirage component.

Upgrading from Prior Versions of VMware Mirage

If you are upgrading Mirage from version 4.0 or later to version 5.0, follow the instructions in this section. To perform a new installation, see New Installation and Configuration. For more information about upgrading, see the VMware Mirage Administrator's Guide.

Upgrading to Mirage 5.0 involves upgrading the MSI file for each Mirage component. SSL and port configurations are preserved through the upgrade.

1. Obtain the following information from the `config` file:
   - Database server name
   - Mirage server cache directory location
   - Cache size
2. Stop the Mirage services.
   a. In the left pane of the Mirage Console, under System Configuration, click **Servers**.
   b. Right-click each active Mirage server and select **Stop Server Service**.
3. Back up the Mirage database:
   a. Run a full sysreport in Mirage by double-clicking the file: `C:\Program Files\Wanova\Mirage Management Server\sysreport_full.cmd`
   b. Back up the Mirage database using SQL Server Management Studio.

   Note: This step assumes knowledge of SQL Server.
4. Take snapshots of all VMware Mirage storage volumes using an image-based block backup, not a file-based backup.

   If you cannot take a snapshot of a volume, use an appropriate backup program to back up each volume directory. The backup software must support Alternate Data Streams (ADS). For best results, use block-based backup programs rather than a file-level backup.

   The backup process can take a significant amount of time to complete.
5. Run the MSI files of the Mirage data center components in the following order.
   a. Mirage Management server
   b. All Mirage servers
   c. Mirage Console
   d. File portal server
   e. Web Manager

After the upgrade of the data center components is complete, Mirage upgrades the Mirage client and prompts for a reboot when an endpoint connects to the network.

New Installation and Configuration

In a production environment, you would consider these factors to determine the number of servers needed:

- Number of endpoints
- Number of concurrently connected endpoints
- System fault tolerance requirements
- Support requirements of multiple servers

For this evaluation, install only one Mirage server and skip the optional steps. In addition, scan the VMware Mirage Administrator's Guide for procedures pertinent to your environment.

Installing Mirage involves the following steps.

1. Install Windows Server 2008 R2 or Windows 2012 on your server.
2. Install a supported Microsoft SQL Server, such as Microsoft SQL Server 2008 R2 or Microsoft SQL Server 2012.
3. Create a Mirage database instance in the SQL database management system, or collect the database information.
4. Install the Mirage Management server.
5. Install the Mirage Console.
6. Connect the Mirage Console to the Mirage Management server.
7. Add the Mirage software license to the Mirage Management server.
8. Configure SSL.
9. Install a Mirage server.
10. (Optional) Configure Mirage server options.
11. (Optional) Install IIS and the file portal, and configure the file portal Web URL.
12. Import the USMT folder to the Mirage server.
13. (Optional but required for domain-joining operations) Configure domain account details.
14. (Optional) Make other system configurations in the Mirage Management server through the Mirage Console.

The following table details each installation step. For more information, see the VMware Mirage Administrator's Guide.

STEP	INSTRUCTIONS
1. Install Windows Server 2008 R2 or Windows Server 2012 on your server.	a. Install .NET Framework 3.5 SP1. b. Turn off UAC. c. Join the server to the existing Active Directory. d. Create an AD group for the Mirage administrator. e. Add an existing administrator account to the Mirage AD group you created, or create a new Mirage administrator and add that administrator to the group. The administrator must be a local administrator on the Mirage server hosts. See Defining administrators for VMware Mirage.
2. Install a supported Microsoft SQL Server, such as Microsoft SQL Server 2008 R2 or Microsoft SQL Server 2012. Create a Mirage database instance in the SQL database management system, or use the default instance.	Set up Microsoft SQL Server with Windows Authentication. This is required for a Mirage file portal implementation, or you might need it to satisfy your own security requirements. Note the SQL Server name and SQL instance name. A best practice for a production system: Install and run the database on a different server from the Mirage server.
3. Install the Mirage Management server. **Note:** The account that installs the Mirage Management server and the Mirage server must have database creator rights, and the account that runs the Mirage service must have rights to the database and storage.	Double-click the `mirage.management.server.x64.<build_number>.msi` file. The VMware Mirage Management Server Setup wizard begins. In the wizard, do the following: • Enter the names of the SQL Server and SQL instance. The default instance names for each SQL Server type are - `SQLEXPRESS` for SQL Express - `MSSQL` for SQL Enterprise **Note:** The default for SQL Standard is no name. • Specify the storage area for Mirage data. • Enter the credentials for the Mirage services account that will access the storage and database. If you did not set up a dedicated Mirage services account, enter **Local System account**. • Specify the administrative group that has access to the Mirage Console.

STEP	INSTRUCTIONS
4. Install the Mirage Console.	The Mirage Console must have network connectivity to the Mirage Management server. For this evaluation, you can install the Mirage Console with all other Mirage components on a single Windows server. For a production environment, the best practice is to use a Windows server solely for the Mirage Console or together with Web Manager. Double-click `mirage.management.console.x64.<build_number>.msi` for 64-bit environments or `mirage.management.console.x86.<build_number>.msi` for 32-bit environments. The VMware Mirage Console Setup wizard starts. A shortcut to the Mirage Console is added to the desktop.
5. Connect the Mirage Console to the Mirage Management server.	Double-click the Mirage Console icon on the desktop. In the Mirage Console window, right-click **VMware Mirage** in the root directory and select **Add System**. Enter the IP address or host name of the Mirage Management server. If the Mirage Console and the Mirage Management server are on the same computer, use `localhost`. In the Mirage Console, the status of the Mirage Management server is Down until you install the server. The status then changes to Up.
6. Add the Mirage software license to the Mirage Management server.	a. In the Mirage Console, right-click **System Configuration** and select **Settings**. b. Select the **General** tab and scroll down to the License section. c. Click **Set License**. d. In the File window, navigate to your license file and click **Open**. e. Click **OK**.
7. Configure SSL on each server.	a. Install the server certificate and private key in the Windows Certificate Store. b. Restart each VMware Mirage server service. c. Configure the transport settings in the Mirage server options. d. Enable SSL on the Mirage clients. See the VMware Mirage Administrator's Guide.
8. Install a Mirage server. **Note:** The account that installs the Mirage Management server and the Mirage server must have database creator rights, and the account that runs the Mirage service must have rights to the database and storage.	Ensure that SQL Server is reachable from the server node and that the firewall settings on SQL Server allow for remote connections. Double-click the `mirage.server.x64.<build_number>.msi` file. The VMware Mirage Server Setup wizard starts. a. Type the SQL Server and SQL instance names. b. Specify the local cache location and size. c. Enter the credentials for the Mirage services account that will access the storage and database. If you did not set up a dedicated Mirage services account, enter **Local System account**. d. Reboot after installing the Mirage server.

STEP	INSTRUCTIONS
9. (Optional) Configure Mirage server options.	a. In the left pane of the Mirage Console, under System Configuration, click **Servers**. b. Right-click the server and select **Configure**. c. Configure the maximum number of concurrent desktop image connections and the transport settings (port and SSL connection). For more information, see *Configuring a Mirage Server* in the VMware Mirage Administrator's Guide.
10. (Optional) Install IIS and the file portal, and configure the file portal Web URL.	a. Install the IIS Server role on the Mirage server machine. b. Install the Mirage file portal files by double-clicking the `mirage.WebAccess.x64.<build_number>.msi` file, or the 32-bit equivalent. The Mirage Web Access Applications Setup wizard starts. c. Select one or both of the following: • Web Access – Gives end users access to their files stored in historical endpoint snapshots. IT determines which files are uploaded to the data center. • Admin Web Access – Gives administrative access to all end-user endpoint snapshots. d. Enter the Mirage Management server location. e. Enable the ports between IIS and the Mirage Management server. f. Enable Windows Authentication on Microsoft SQL Server for the file portal.
11. Import the USMT folder to the Mirage server.	The USMT files are required for various base layer migrations and restorations, such as a Windows XP to Windows 7 migration. See Importing USMT for a Window 7 Migration for more information.
12. (Optional, but required for domain-joining operations) Configure domain account details.	a. In the left pane of the Mirage Console, right-click **System Configuration** and select **Settings**. b. Select the **General** tab. c. Enter the credentials of the account being used to join domains during migrations.
13. (Optional) Make other system configurations in the Mirage Management server through the Mirage Console.	In the left pane of the Mirage Console, right-click **System Configuration** and select **Settings**. You can configure • Snapshot frequency and retention period • Warning threshold for volume capacity • Warning threshold for desktop image size • Upload policy to use when an end user adds their desktop image to the Mirage system • License number • Enablement of automatic desktop image creation, initiated by the end user • Enablement of and specifications for the file portal For more information, see *Configuring the Mirage System* in the VMware Mirage Administrator's Guide.

Table 7: Mirage Installation and Configuration Steps

Requirements for the Mirage Evaluation Exercises

For these Mirage evaluation exercises, you need:

- A product to create virtual machines. The end-user endpoints can be physical PCs, but for the evaluation exercises it is recommended to use virtual machines. To create the virtual machines, you can use vSphere, Fusion Pro, or Workstation. The Mirage bundle includes both Workstation and Fusion Pro. Although vSphere is not required to run Mirage, you can use your current vSphere installation to create virtual machines for these evaluation exercises.
- You need to know how to create virtual machines, manage virtual machine snapshots, and power virtual machines on and off. See the vSphere, Fusion Pro, or Workstation documentation.
- If you are not using vSphere, one computer with enough space for two Fusion Pro or Workstation virtual machines, about 74 GB.
- Installers for some application software, such as Firefox, 7Zip, Skype, and Adobe Reader.

These evaluation exercises assume that you have already installed and configured the Mirage data center components. If not, see New Installation and Configuration.

In these exercises, you receive periodic instructions to take a virtual machine snapshot with vSphere, Fusion, or Workstation. These snapshots provide a safety net in case you make a mistake in the exercises. Mirage adjusts assignments to match the snapshot state.

Note: Rolling back to a previous virtual machine snapshot does not necessarily roll back the state in the Mirage Console. For example, rolling back to a prior virtual machine snapshot might put the virtual machine into a state without an applied layer, yet in App Layer Assignments, you might still see the layer as applied. You might need to manually roll back the Mirage CVD state in the Mirage Console to accommodate the rollback to a prior virtual machine snapshot. Delete the CVD and then recentralize the endpoint.

Preparing the Reference Machine and Test Machines

You need to create your test environment, which consists of a Mirage reference machine and an endpoint. You Mirage-enable the reference machine and endpoint, and then back up each machine to the data center.

Create Your Test Virtual Machines

For these exercises, you need several computers—either physical computers or virtual machines. Virtual machines are suitable for capturing most applications. We will proceed as if you are using virtual machines for your test machines.

These evaluation exercises demonstrate a migration from Windows XP to Windows 7. You can also migrate Windows 7 to Windows 8.1 or Windows 8.1 Update 1. The process is the same. If you choose to perform a Windows 7 to Windows 8.1 migration, adjust the instructions as needed.

Create at least three Windows 7 virtual machines and one Windows XP virtual machine for the following purposes:

- Administrator virtual machines
  - Windows 7 virtual machine for the reference machine to create and maintain base layers
  - Windows 7 virtual machine for capturing application layers
- End-user virtual machines
  - Windows XP virtual machine for the Windows 7 migration
  - Windows 7 virtual machine for layer management

Assign the Windows 7 virtual machines 40 GB of space, thin-provisioned and lazy-zeroed for best performance. Assign the Windows XP virtual machine with 50 GB of space, thin-provisioned, to allow for the Windows 7 OS alongside 10 GB of Windows XP during migration. Make sure that these virtual machines comply with requirements for Mirage clients, as specified in Mirage Operating System and Software Requirements.

In addition, Mirage requires that the Volume Shadow Copy service be enabled. If you have optimized your Windows 7 or Windows XP virtual machine and have disabled the Volume Shadow Copy service, be sure to enable it as either Manual or Automatic.

Before you proceed with these exercises, take a virtual machine snapshot of each test machine so that you can revert to this initial state at any time. Do this in Workstation, Fusion Pro, or vSphere, according to instructions for these products.

Note: This virtual machine snapshot is different from a Mirage snapshot or a Mirage desktop image in the data center.

Mirage takes a snapshot of the endpoint at critical junctures, so you also have a Mirage snapshot to roll back to.

Create a Reference Machine

A reference machine is an endpoint that you use to create and maintain base layers. The reference machine is where you patch the operating system and add core applications to the base layer.

The administrator captures a base layer from the reference machine through the Mirage Console. The administrator provides names and versions for the layers. You can use the same reference machine for multiple layer captures.

After creating the reference machine, you centralize it to create a reference desktop image to distribute to a set of endpoints. The reference machine does not consume any of your Mirage licenses.

The virtual machine you use for the reference machine must be a clean reference machine, such as the following profile:

- Simple OS installation of Windows XP or Windows 7, either 32- or 64-bit
- Same OS profile of Windows service pack and .NET framework versions as the target endpoints that receive the copied base layer
- No auto-updating software

If it is not possible to remove auto-updating software, disable the software's auto-updating feature. For example, turn off automatic Windows Update installations and antivirus definition updates.

Use a Windows 7 virtual machine as your reference machine in these exercises.

After you ensure that the reference machine is clean, you can install the Mirage client on the two virtual machines that you are using for these exercises.

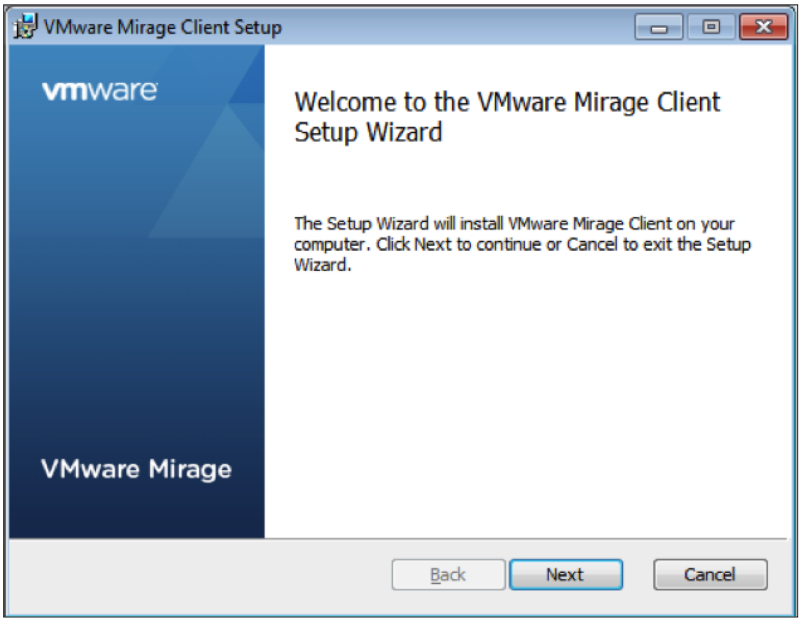
Install the Mirage Client on the Test Machines
Prior to installation, you must

- Install .NET Framework 3.5 on the Windows XP virtual machine. The Windows 7 operating system includes it.
- Verify that an SSL certificate is already configured on the Mirage server. See Overview of Installation and Configuration for instructions about configuring SSL. If the SSL certificate configured on the Mirage server is signed by an internal CA or is self-signed, make sure that the certificate is imported into the Personal and Trusted Root Certification Authorities certificate stores in the Certificates snap-in for the test machine. See Import a Certificate for more information.

Install the Mirage client on each test virtual machine. In a production environment, you can silently install the Mirage client on endpoints from the command line. For this evaluation exercise, run the installer on each endpoint.

1. Place the Mirage client installer on the endpoint. Install either the 64-bit version (.x64) or the 32-bit version (.x86) according to the types of virtual machines you have created.
2. Double-click the Mirage client installer to run it.

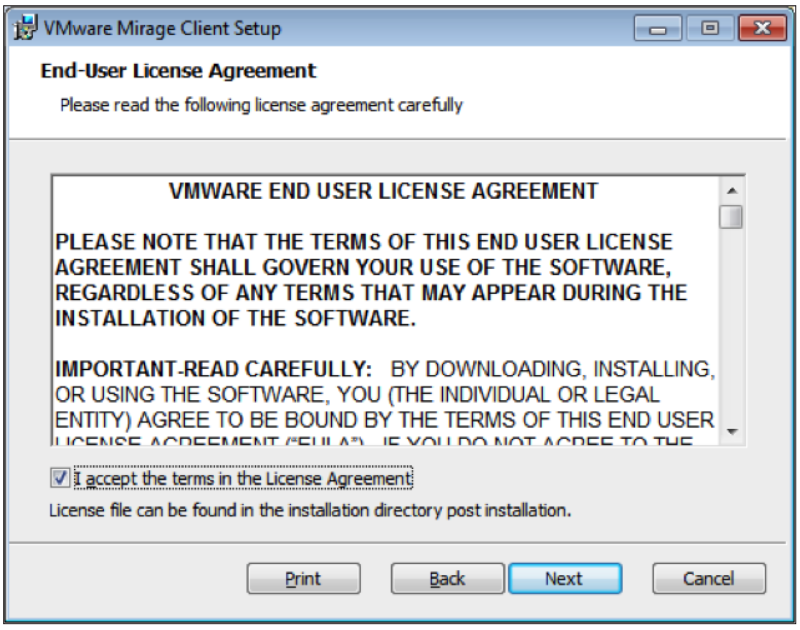
   The Welcome page appears.



3. Click **Next**.

   The End-User License Agreement page appears.

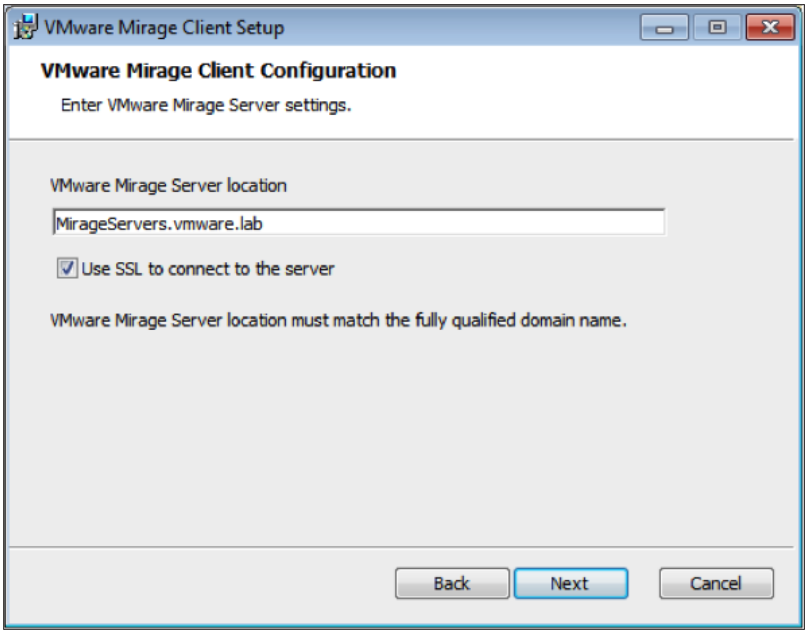
4. Accept the terms and conditions and click **Next**.



The Mirage Client Configuration page appears.

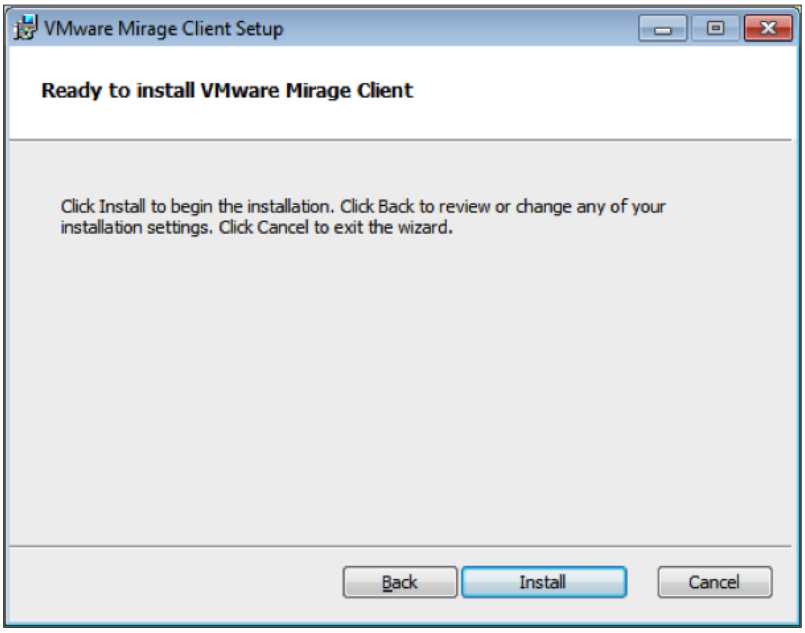
5. In the VMware Mirage Server location, enter the fully qualified domain name of the Mirage server you want this client to communicate with and select the **Use SSL to connect to server** option.

   Note: If the Mirage server uses a port number other than the default of 8000, append the port number to the Mirage server name. Enter a colon (:) and then the port number.



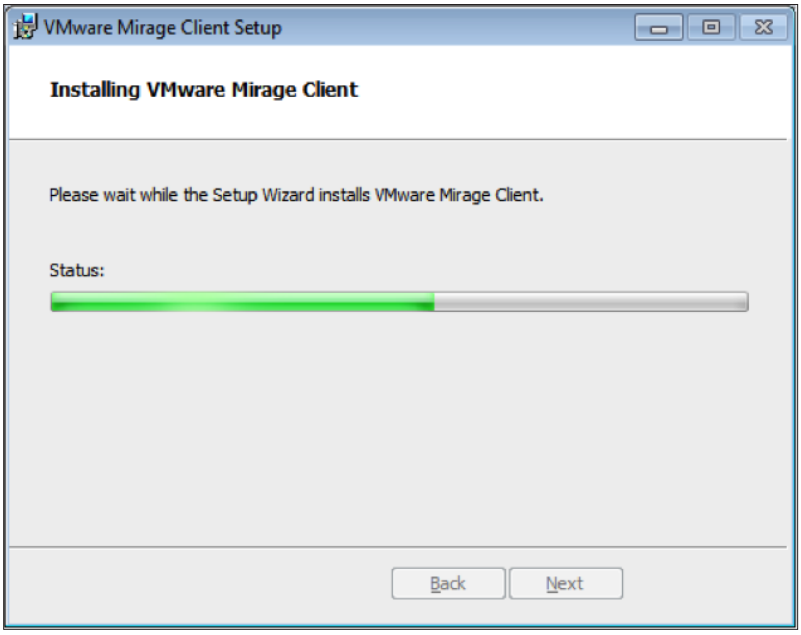
6. Click **Next**.

   The Ready to Install page appears.



7. Click **Install**.

   Installation begins, and a progress page appears.



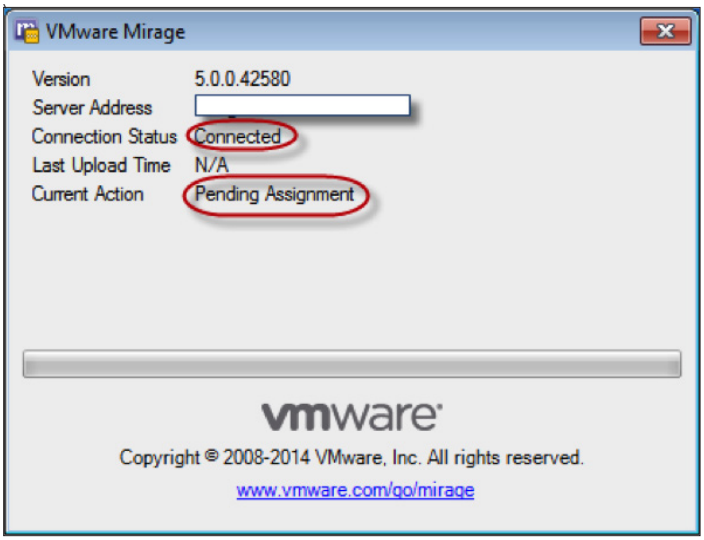
After the installation progress completes, the Completed Setup wizard page appears.

8. Click **Finish**.

9. Validate that the Mirage client is correctly installed on the test machines.

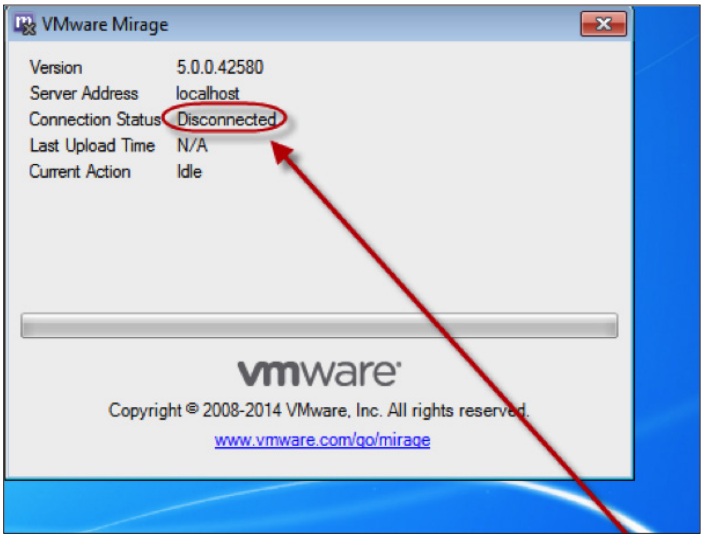
   a. Examine the Mirage system tray icon.

   The Mirage client installation is successful if the system tray icon displays a yellow marking. When you double-click the icon, the details show that the client is connected to the Mirage server and is Pending Assignment. If you are connecting to a Mirage Gateway server, the Current Action setting is Pending Logon. See Working with the Mirage Gateway for more information.

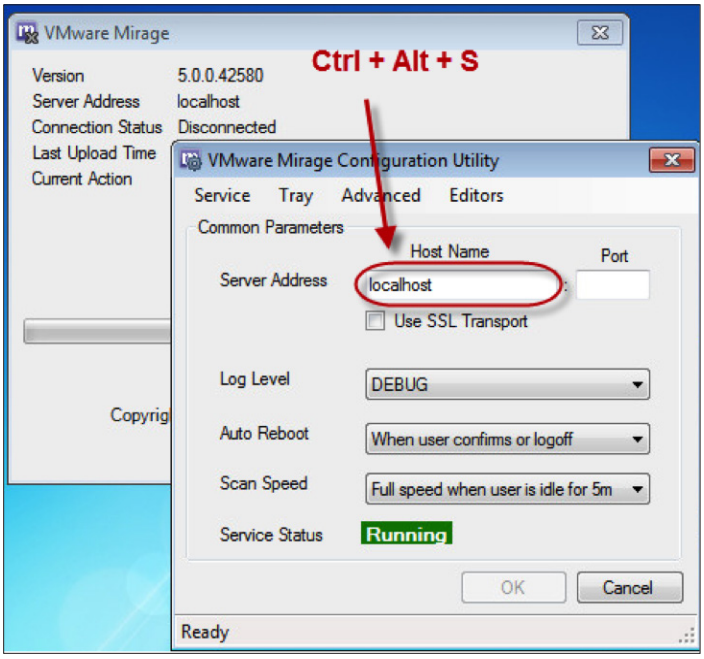


   Pending Assignment means that the endpoint is ready for backup. You activate the endpoint in the Mirage Console by centralizing it (creating the initial desktop image, or CVD, in the data center).

   Troubleshooting Tip: If you see an X on the Mirage system tray icon, double-click the icon. The details show that the client is disconnected.



A possible cause is that you entered an incorrect server address, such as localhost, during the Mirage client installation. You can use the configuration utility to change the server address. In the Mirage client window, press Ctrl+Alt+S to open the VMware Mirage Configuration Utility dialog box and change the settings.

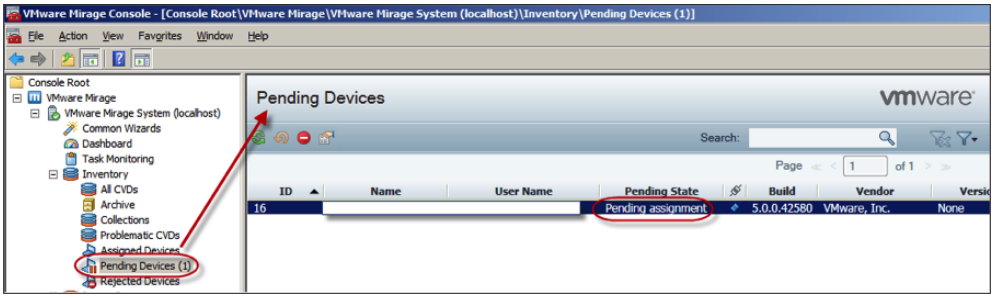


Other reasons for the Disconnected status are discussed in the VMware Knowledge Base article Mirage Client is Disconnected.

b. In the Mirage Console, check the status of each test machine.

When the Mirage client is properly installed on a device and communicating with a Mirage server, the Mirage server recognizes the device as a Mirage-enabled endpoint. The Mirage Console then displays the state of the device.

In the left pane of the Mirage Console, select **VMware Mirage** > **Mirage System** > **Inventory** > **Pending Devices**. Verify that each test machine has a value of Pending assignment under Pending State.



Take Virtual Machine Snapshots of the Test Machines

Take a snapshot of the reference virtual machine in its clean, Mirage-enabled state. Also take a snapshot of the endpoint in Workstation, Fusion Pro, or vSphere, according to the instructions for these products. You can use the snapshot to roll back the reference machine or endpoint to this current state, if needed.

Note: This virtual machine snapshot is different from the Mirage snapshot or a Mirage desktop image in the data center.

Creating a Reference CVD and Capturing a Base Layer

Now that you have a Windows 7 reference machine ready and available as a pending device, you can create a reference CVD from the reference machine and capture a base layer from the reference CVD. A later exercise explains how to apply the Windows 7 base layer to migrate a Windows XP endpoint to Windows 7.

Create a Reference CVD

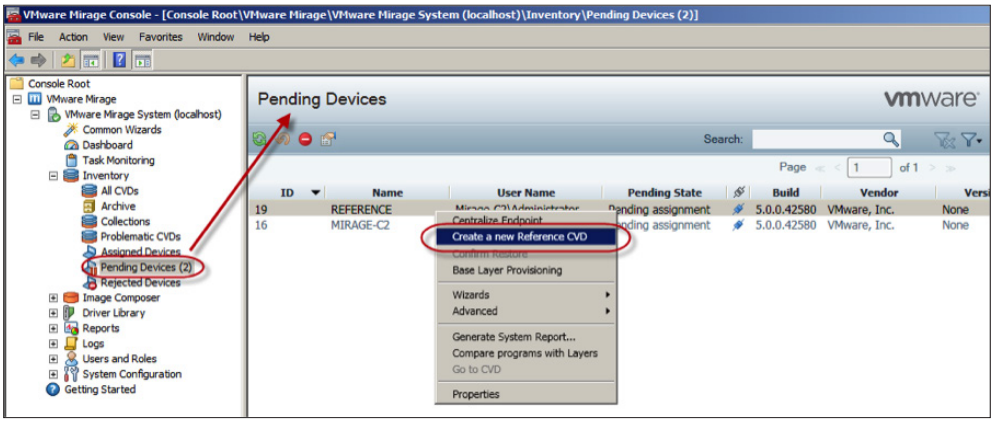
The reference machine serves as a backup in the data center.

1. In the left pane of the Mirage Console, expand **Inventory** and then select **Pending Devices**.

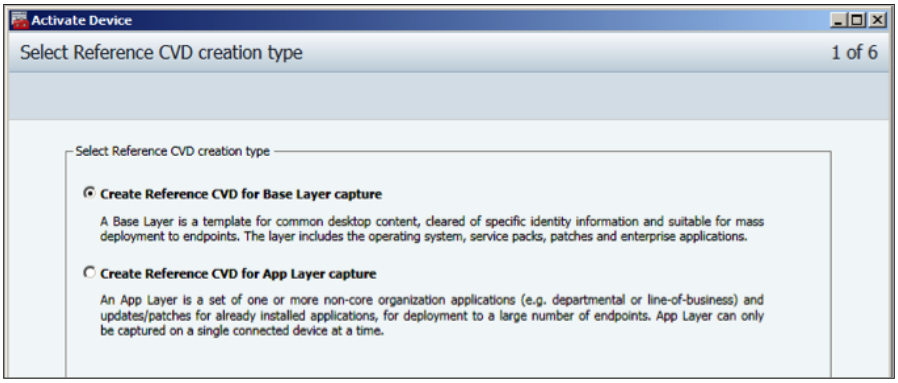
   The right pane displays the pending devices, which are the endpoints you enabled by installing the Mirage client on them. Each endpoint shows pending assignment as the current action in the Mirage system tray icon details. Pending devices are ready to be backed up to the data center.

2. Right-click the clean Windows 7 reference machine that you created and select **Create a new Reference CVD**.

   Note: A CVD is the desktop image in the data center.

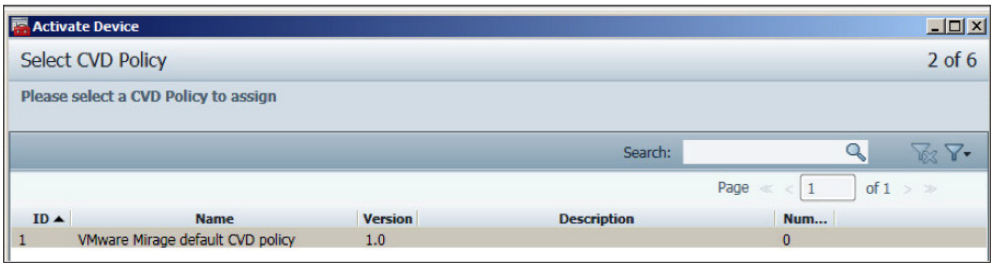


The Select Reference CVD creation type page appears.



3. Select **Create Reference CVD for Base Layer capture** and click **Next**.

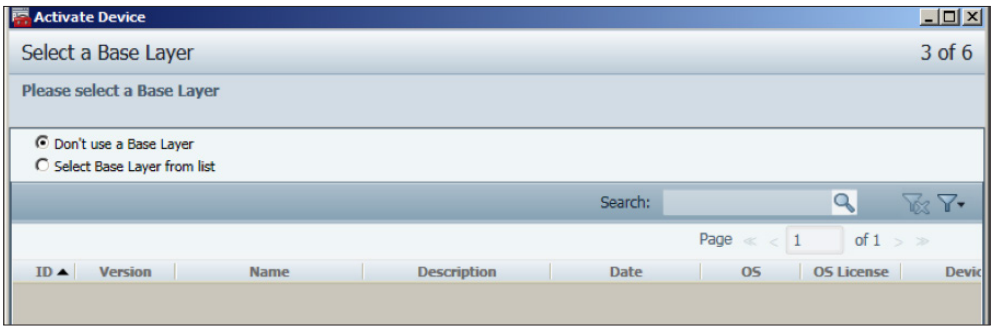
   The Select CVD Policy page appears.



   A CVD policy is a set of rules specifying which files Mirage backs up to the data center in a CVD. For example, the default upload policy ignores MP3 files and movies. Mirage numbers new upload policy versions for you, but you can configure the version numbers. For more information, see the VMware Mirage Administrator's Guide.

4. Select **Mirage default CVD policy** and click **Next**.

   The Select a Base Layer page appears.



5. Select **Don't use a Base Layer** and click **Next**.

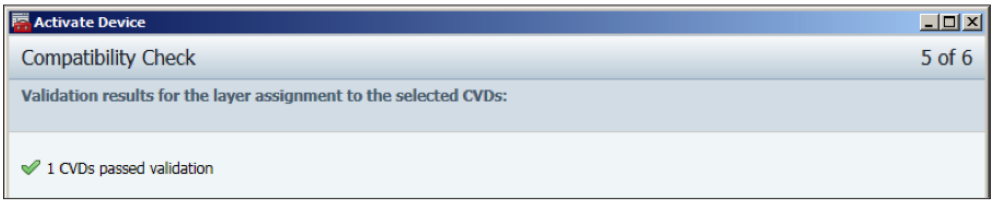
   You choose this option because you have not yet captured a base layer. You would choose **Select Base Layer** from list to apply updates to the base layer.

   The Select Target Volume page appears.

6. Select **Automatically choose a volume** and click **Next**.

   This is the storage volume where the CVD will be located. Mirage finds a storage volume that you have configured and places CVDs on it.

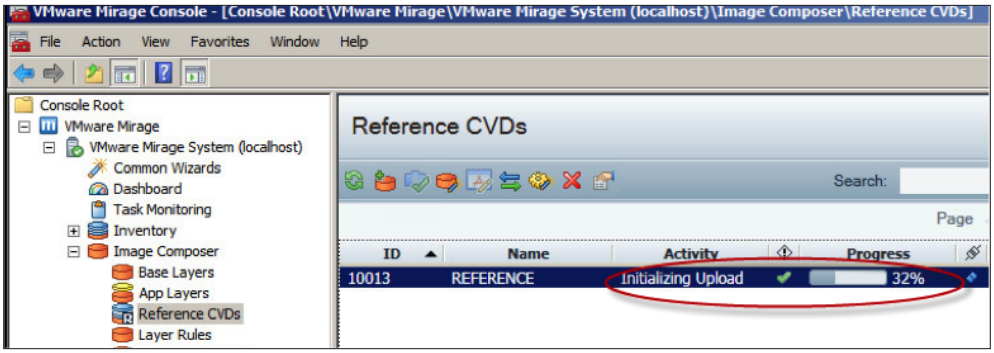
   The Compatibility Check page appears.



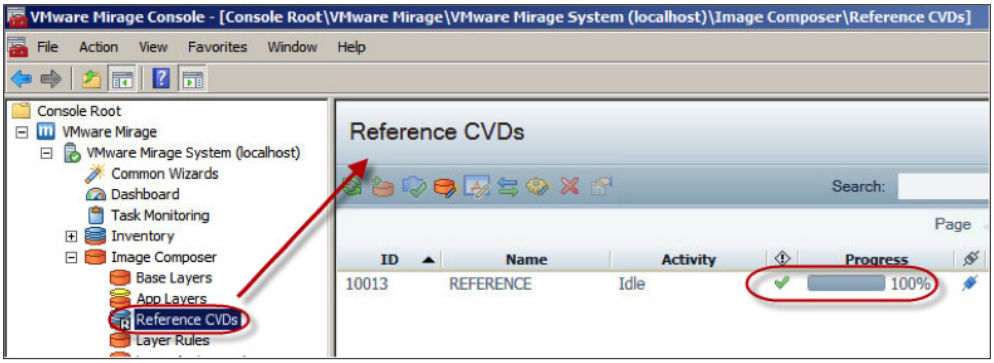
7. Click **Next**.

   The Summary page appears.

8. Click **Finish**.
9. Validate that the reference machine CVD has been created.
   a. In the Mirage Console, check that the reference machine is no longer in the Inventory > Pending Devices list and is now in the Image Composer > Reference CVDs list.



   At first, the Activity value is Initializing Upload. As the backup progresses, it changes to Upload.



When the reference machine backup finishes, the Activity value changes to Idle, and the Progress value changes to 100%.

b. Open the reference machine and double-click the Mirage system tray icon to check that the endpoint is linked to a CVD in the data center. The Current Action value is now Idle.

You have created the desktop image in the data center for the reference machine. You will later use the reference machine for capturing a base layer.

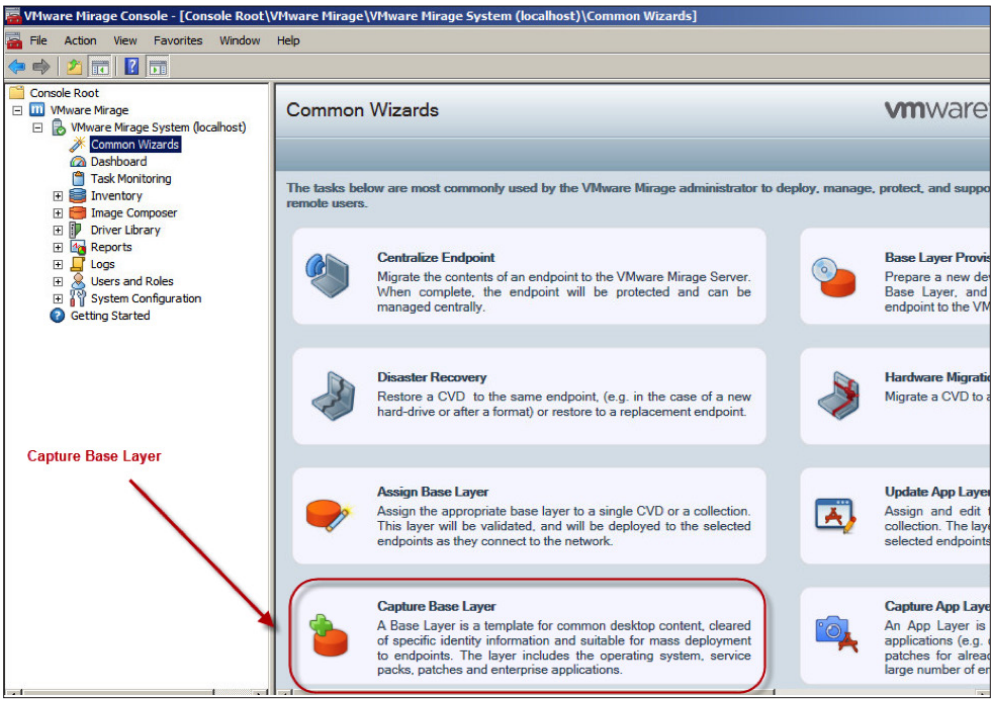
Capture the Base Layer from the Reference CVD

After you create a Windows 7 reference CVD, you can capture the base layer from it. You can have multiple base layers for different sets of users. Base layers are hardware independent. If you want to manage the hardware drivers, you can manage them using the driver library and the driver profiles.

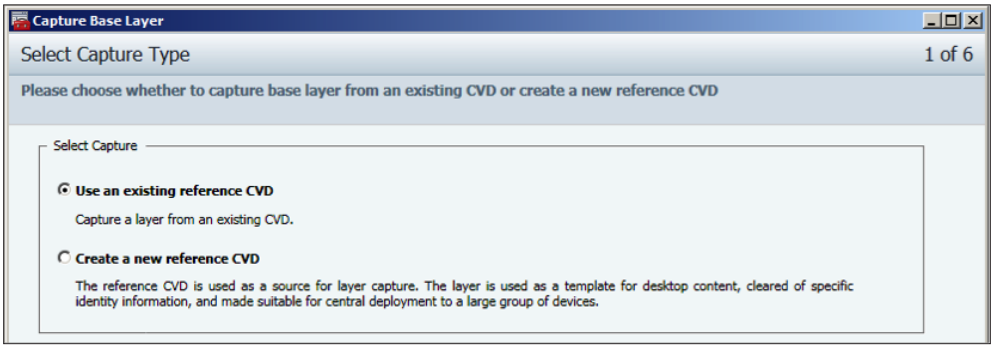
If you are using Mirage to manage virtual machines, a best practice is to use a separate base layer for the virtual machines so that virtual machine integration components are included in the base layer. For example, in a Fusion Pro installation, the base layer needs to include VMware Tools™.

In a production environment, before you capture the base layer, you might want to create base layer rules and add scripts for operations to be carried out after the base layer update. You should also test the base layer prior to deployment.

1. In the left pane of the Mirage Console, click **Common Wizards**, and in the right pane, click **Capture Base Layer**.



The Select Capture Type page appears.

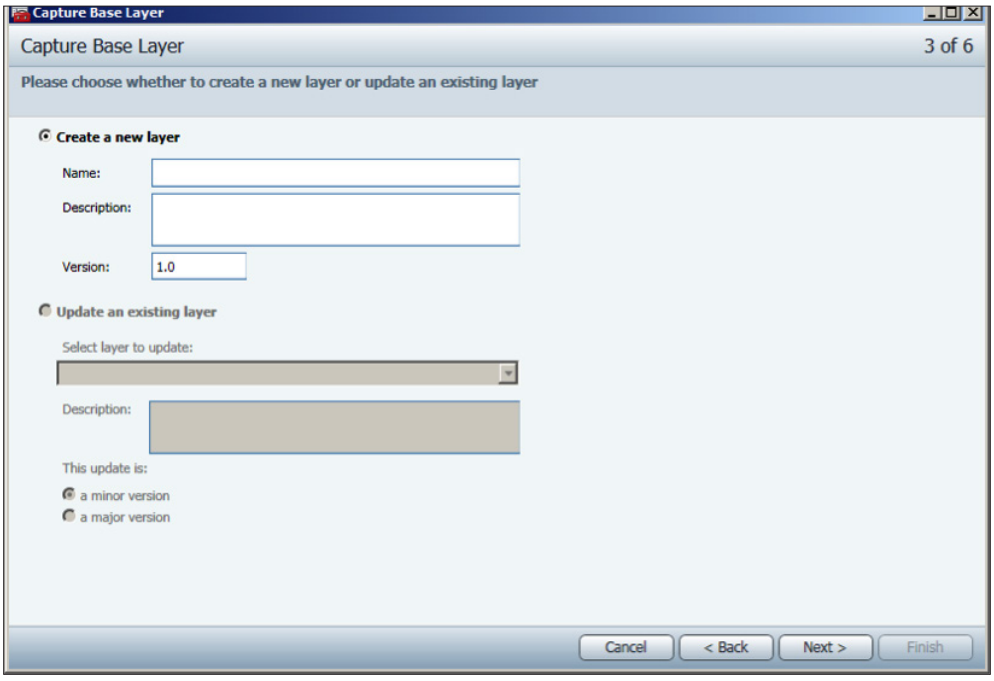


2. Select **Use an existing reference CVD**.

   The Select a Reference CVD page appears

3. Select the reference CVD you created previously and click **Next**.

   The Capture Base Layer page appears.

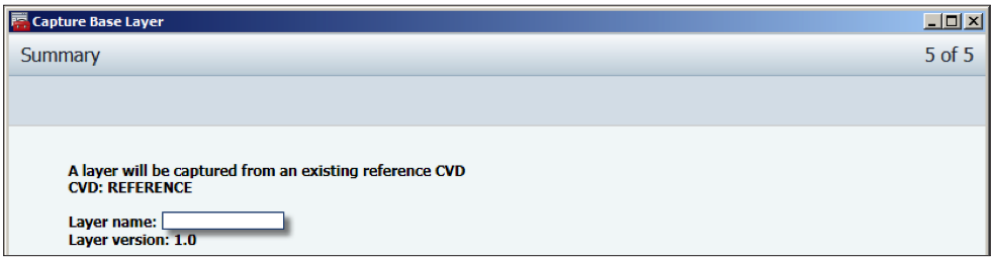


4. Select **Create a new layer**, provide a name and description, and click **Next**.

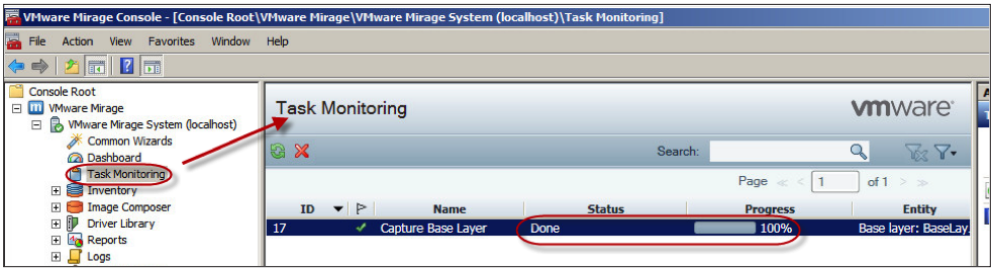
   The Check Compatibility page appears.

5. Click **Next**.

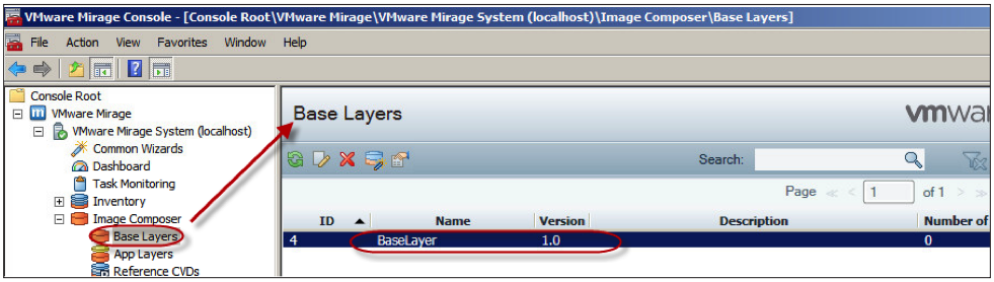
   The Summary page appears.



6. Click **Finish**.
7. To monitor the progress of the task, in the left pane, click **Task Monitoring**.



8. After the capture finishes, select **Image Composer** > **Base Layers** to confirm that the base layer is listed in the Base Layers pane.



You now have a captured base layer that you can use when you want to assign a base layer or migrate to Windows 7 (or 8.1).

Importing USMT for a Windows 7 Migration

To perform an OS migration, you must import Microsoft User State Migration Tools (USMT) to the Mirage server.

For a Windows 7 migration, import USMT 4.0 with hotfix to the Mirage server.

Note: Mirage supports USMT 4 and USMT 5 for Windows XP and Windows 7, and USMT 6.3 for Windows 8 and 8.1.

Prerequisites

- Download the Microsoft Windows Automated Installation Kit (AIK), and copy the USMT folder and all subdirectories to your Mirage server.
- For this evaluation exercise, download the hotfix for USMT 4.0 to a location that the Mirage server can access. Follow the instructions on the Web site to install the hotfix.

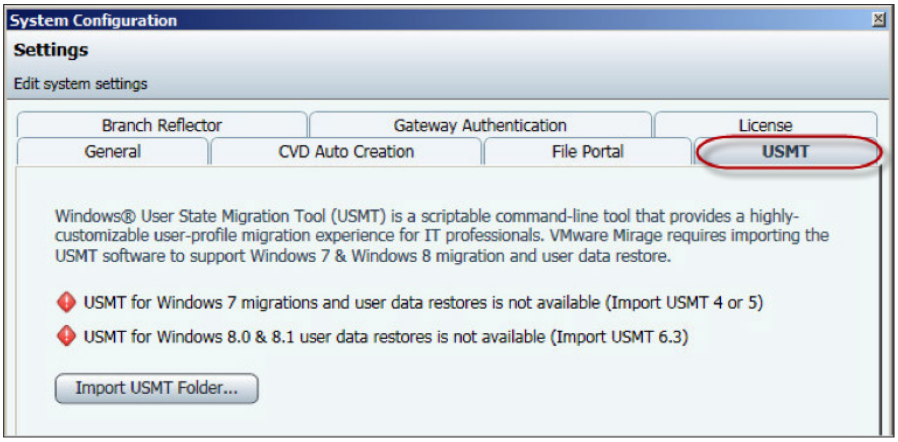
Import USMT

This procedure uses USMT 4.0, but the steps for importing USMT 6.3 are similar.

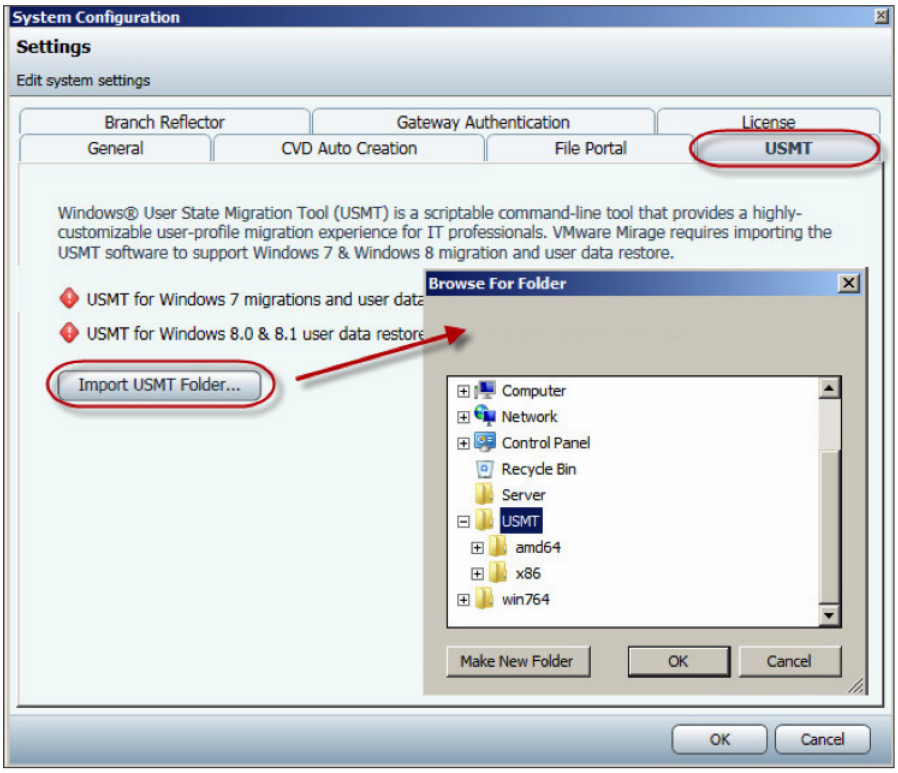
1. In the left pane of the Mirage Console, right-click **System Configuration** and click **Settings**.

   The System Configuration window appears.

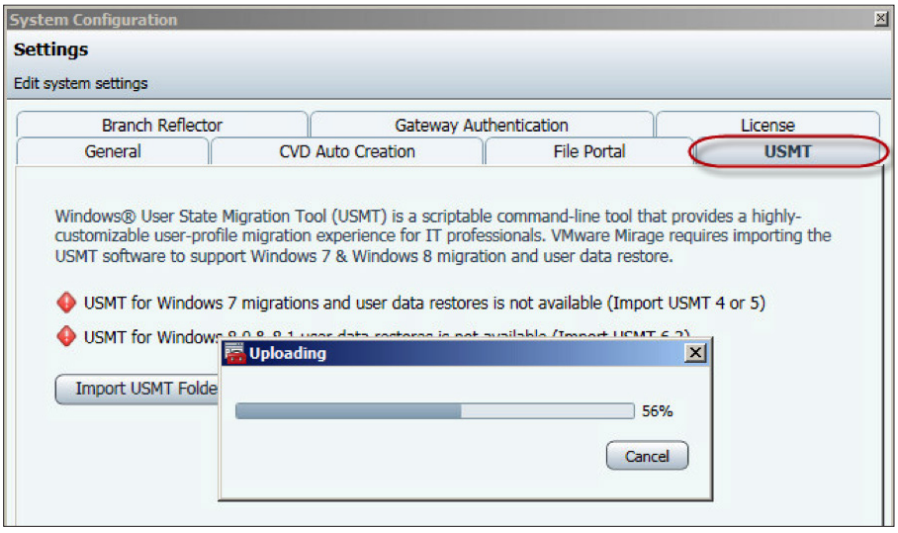
2. Click the **USMT** tab.



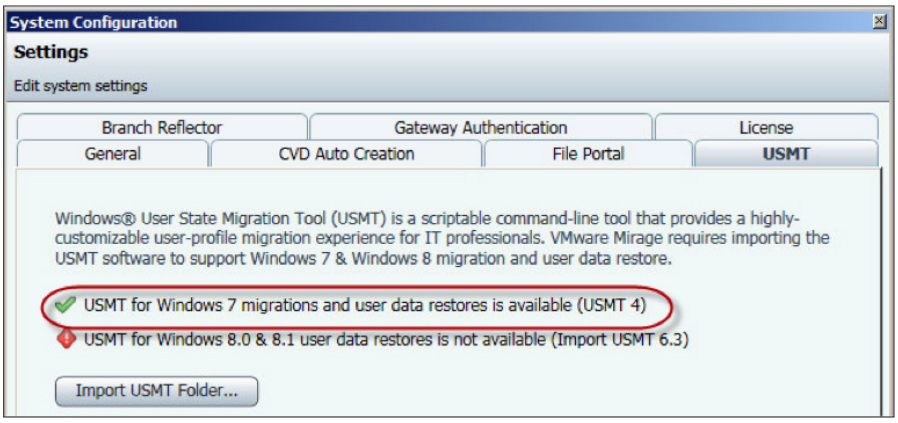
3. Click **Import USMT Folder** and navigate to the USMT folder.



After you select the USMT folder, Mirage imports the tool. The Uploading window shows the progress.



After the USMT successfully uploads, the status message indicates that the tool is available.



Capturing an App Layer (Optional)

The recommended practice in both evaluation and production environments is to use a virtual machine to capture app layers.

Prerequisites

Use a test machine that meets the following requirements:

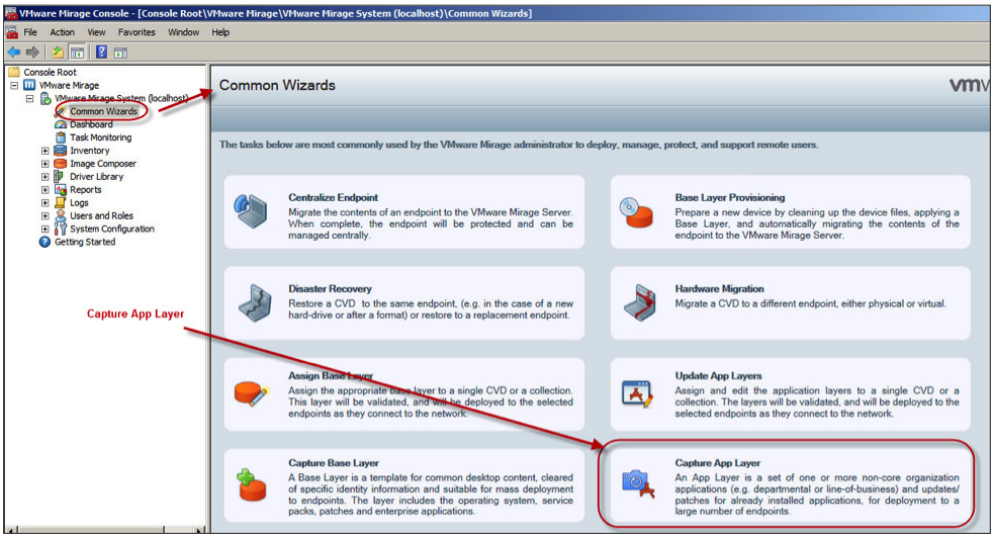
- Standard installation of the required OS, for example, Windows XP, Windows 7 32-bit, or Windows 7 64-bit.
- App layers deployed to compatible OS versions. You must capture app layers separately for Windows XP, Windows 7 32-bit, and Windows 7 64-bit. An app layer captured on Windows XP cannot be deployed on a Windows 7 (32-bit or 64-bit) machine, and the reverse. An app layer captured on Windows 7 32-bit cannot be deployed to Windows 7 64-bit, and the reverse.
- Avoid software in the standard state of the machine that has the following characteristics:
  - Can cause changes to the machine while you are installing the applications
  - Auto-updates
  - If you cannot avoid auto-updating software, try to disable its auto-update feature. For example, turn off automatic Windows Update installation and automatic antivirus definition updates.
- If you are capturing a .NET-based application that uses a version of .NET not included in the standard Windows OS that you installed, install the required .NET framework in the clean machine before you start the capture and install your application. Deliver the .NET framework through the base layer, if possible.
- The standard machine is similar in content to the base layers used throughout the organization, for example, has the same Windows service pack version and .NET framework version as the base layer.

Install the Mirage client on the test machine. For instructions, see Installing the Mirage Client on the Test Machines.

Capture an App Layer

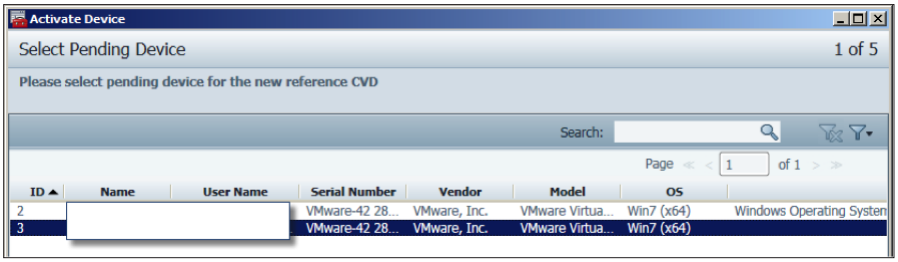
After you complete the prerequisite steps of preparing a virtual machine, capture an app layer from it.

1. In the left pane of the Mirage Console, click **Common Wizards**, and in the right pane, click **Capture App Layer**.



The Select Pending Device page appears.

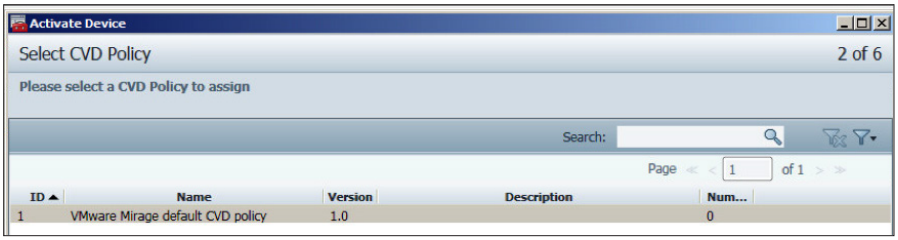
2. Select the pending device from which you want to capture the app layer and click **Next**.



The Select CVD Policy page appears.

3. Select a policy and click **Next**.

   For information about CVD policies, see CVD Policies.



The Select Target Volume page appears.

4. Select **Automatically choose a volume** and click **Next**.

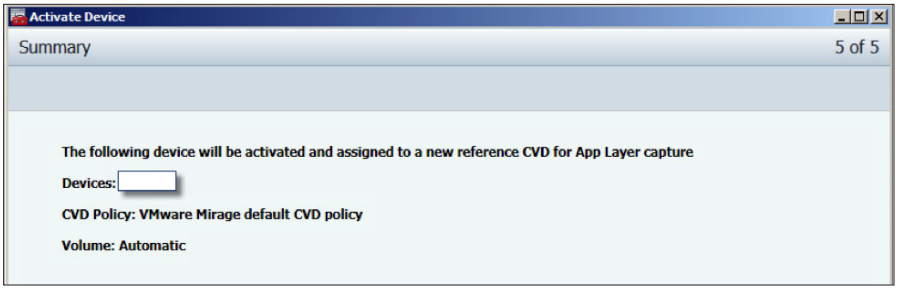
   The Manually choose a volume option enables you to specify the volume to use rather than using the volume selected by Mirage.

   See Storage Setup for more information.

   The Check Compatibility page appears.

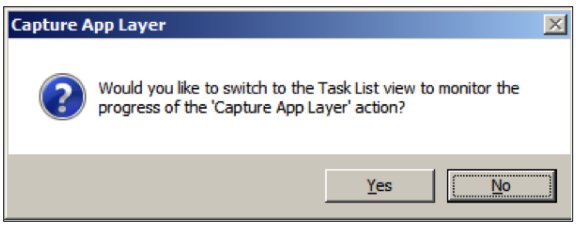
5. Click **Next**.

   The Summary page appears.



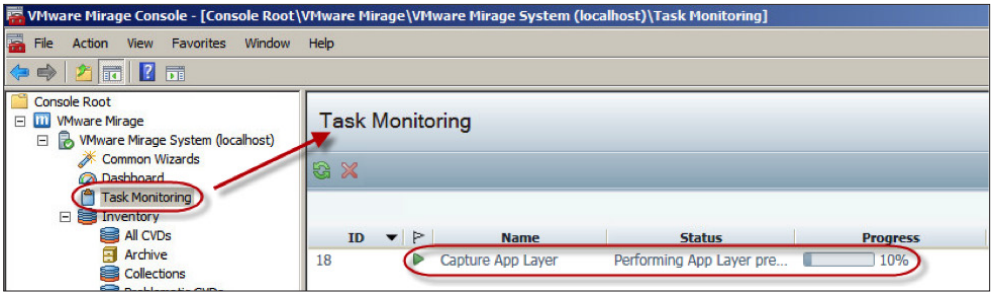
6. Click **Next**.

   A window appears asking if you would like to switch to the Task List view.



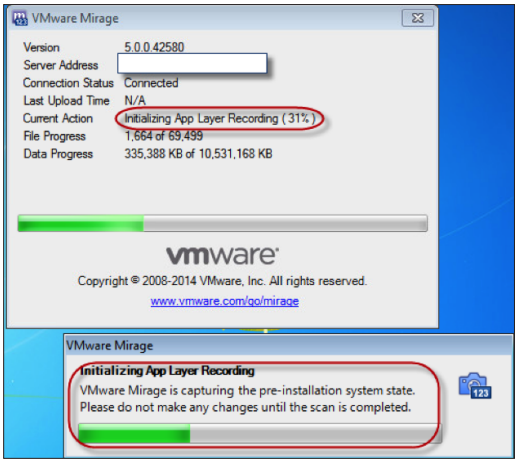
7. Click **Yes**.

   The task is listed in the Task Monitoring pane.



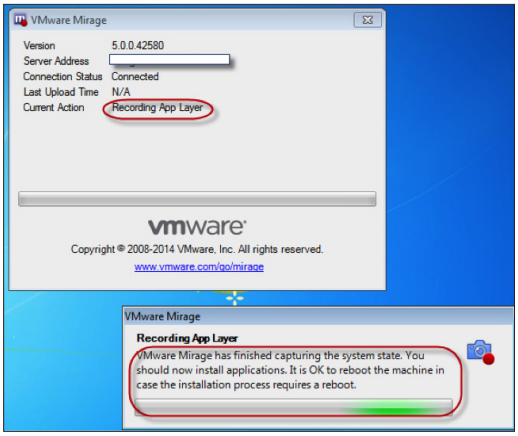
8. Access the virtual machine.

   A dialog box on the desktop of the virtual machine indicates that Mirage is capturing the pre-installation system state.



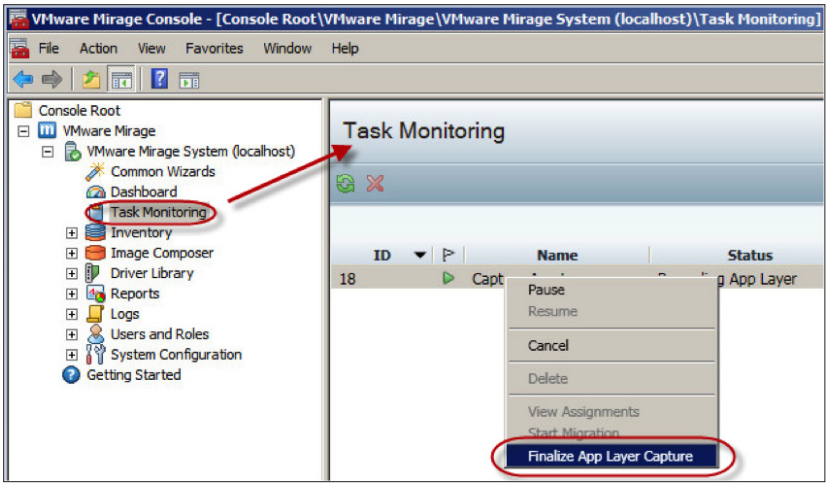
9. Wait until Mirage completes the scan.

   The dialog box indicates when you can install applications and reboot the machine, if needed.

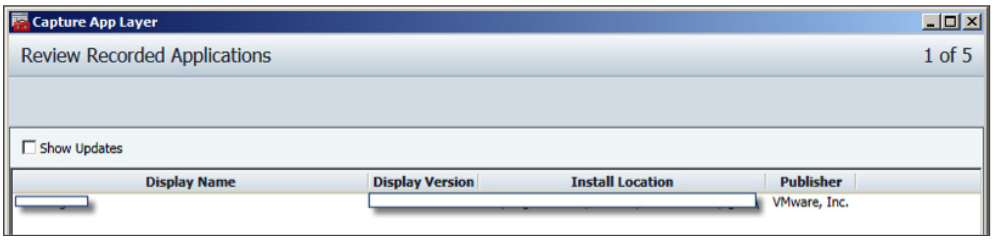


10. In the left pane of the Mirage Console, click **Task Monitoring**.

11. In the Task Monitoring pane, right-click **Capture App Layer** and select **Finalize App Layer Capture**.

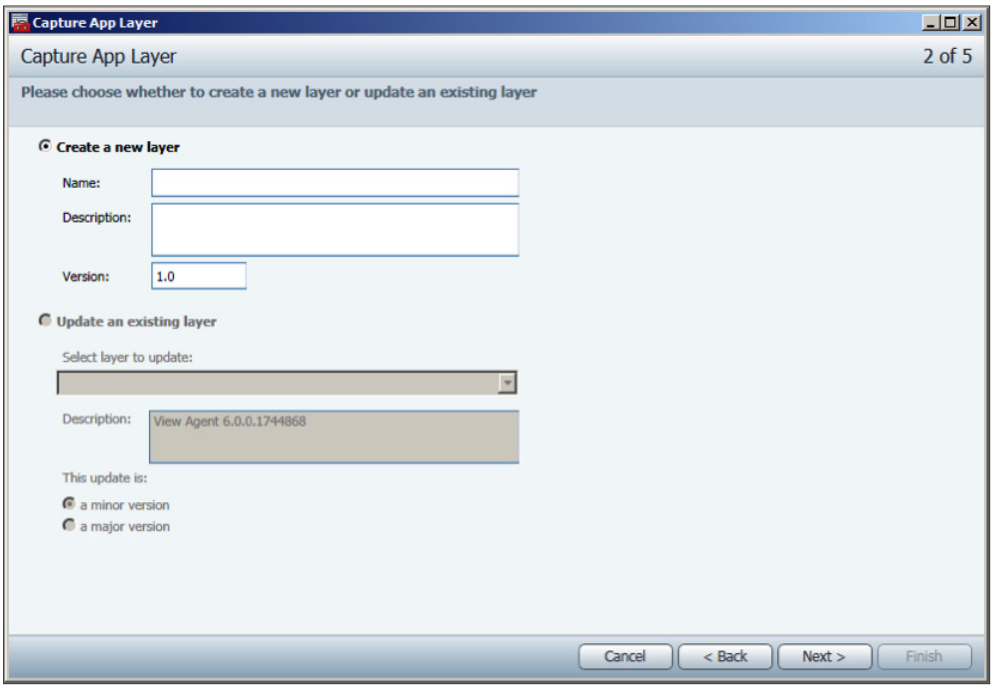


The Capture App Layer page appears and the installed applications are listed.



12. Click **Next**.

13. Enter a name and description for the app layer and click **Next**.



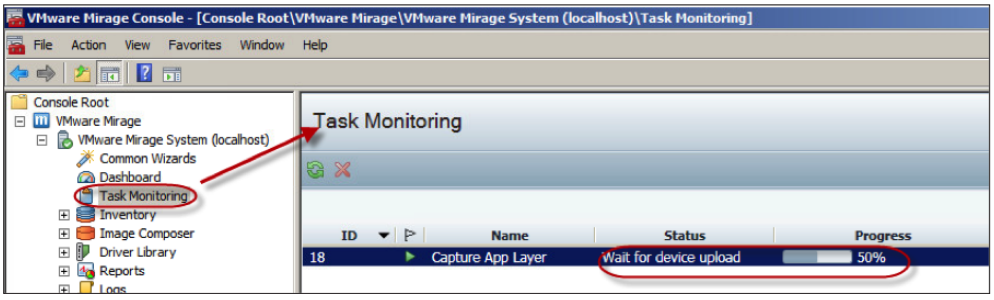
The Check Compatibility page appears.

14. Click **Next**.

The Summary page appears.

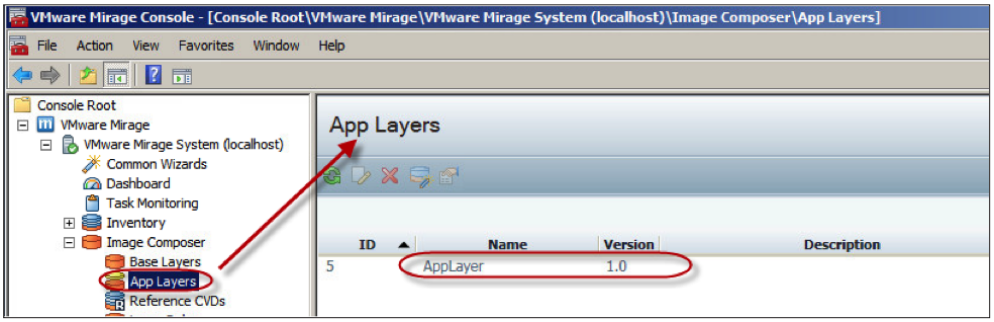
15. Click **Finish**.

The process takes some time to finalize. You can check the progress on the Task Monitoring page.



16. When the process completes, in the left pane, expand **Image Composer** and click **App Layers**.

The captured app layer is listed in the right pane.



Configuring the Mirage Driver Library and Profile (Optional)

With the Mirage driver library, you can centrally manage the drivers for the Mirage endpoints. This practice saves time and provides consistency across endpoints.

The following figure shows the relationship between the driver library, driver profile, and endpoints in Mirage. A driver profile can link to multiple driver folders. The driver profile uses rules to match endpoints.

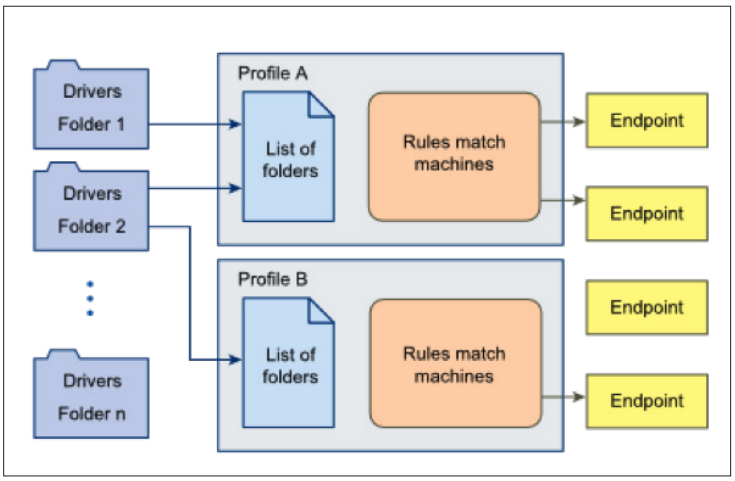


Figure 10: Driver Library Architecture

The driver library is used during the following operations:

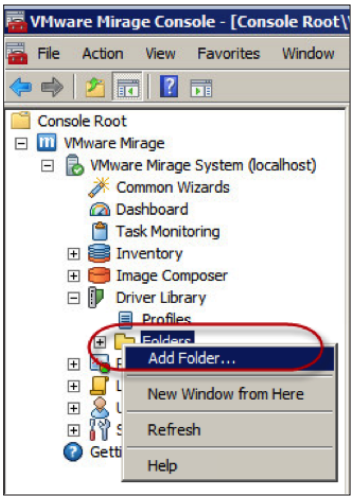
- Centralization
- Migration
- Hardware migration and restore
- Machine cleanup
- Base layer update
- Set driver library

After you decide which drivers should be part of the Mirage driver library, perform the driver-related tasks that follow.

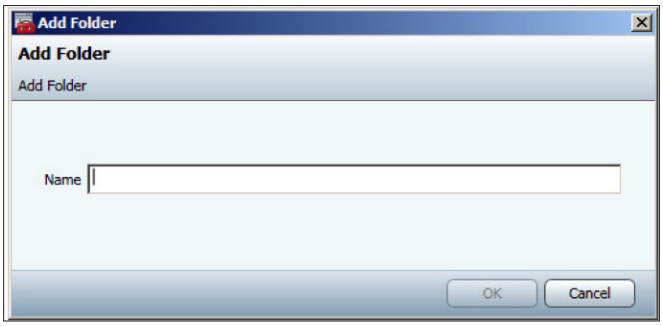
Add Driver Folders

Before you begin, you need to create a driver library structure on a Windows system, obtain the drivers, and extract them. For more information, see Building a driver library in VMware Mirage.

1. In the left pane of the Mirage Console, expand **Driver Library**, right-click **Folders**, and select **Add Folder**.

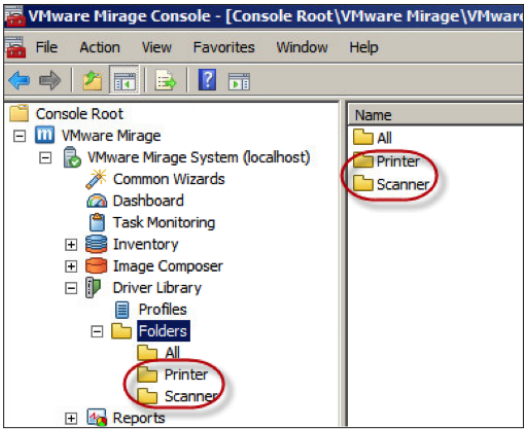


The Add Folder window appears.



2. Enter a folder name and click **OK**.

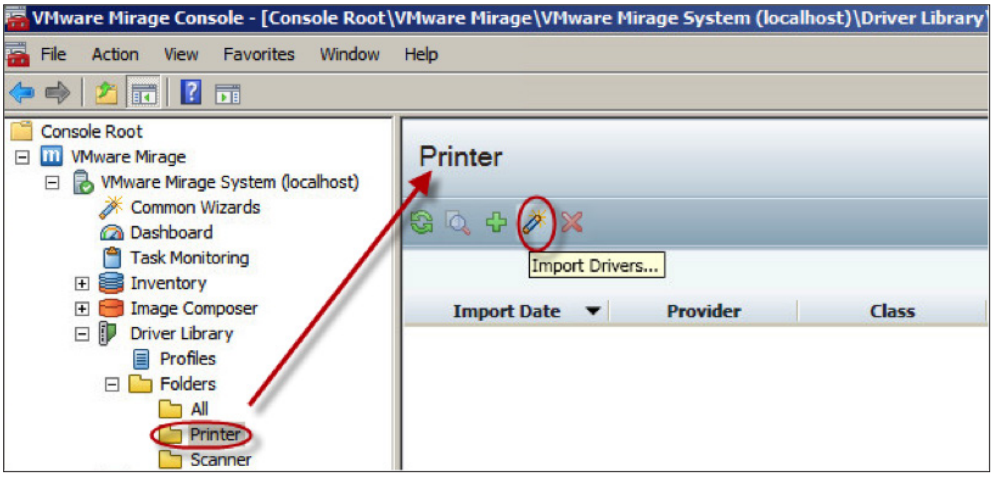
The newly created folder appears.



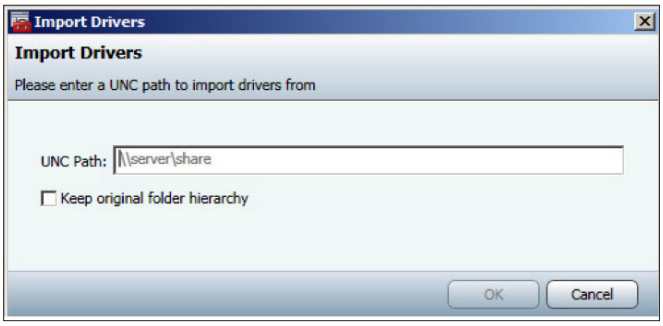
Note: The All folder contains all the drivers and is created by default.

Import Drivers

1. In the left pane of the Mirage Console, click the created driver folder, and in the Printer pane, click the **Import Drivers** icon.

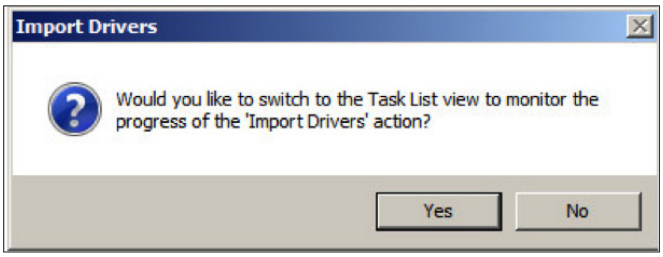


The Import Drivers window appears.

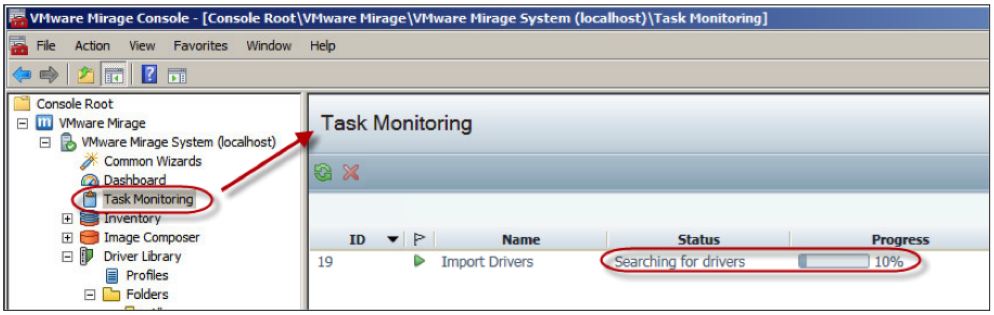


2. Enter the UNC path of the driver.
3. (Optional) To maintain the folder organization of the driver path in the Mirage driver library, select **Keep original folder hierarchy**.
4. Click **OK**.

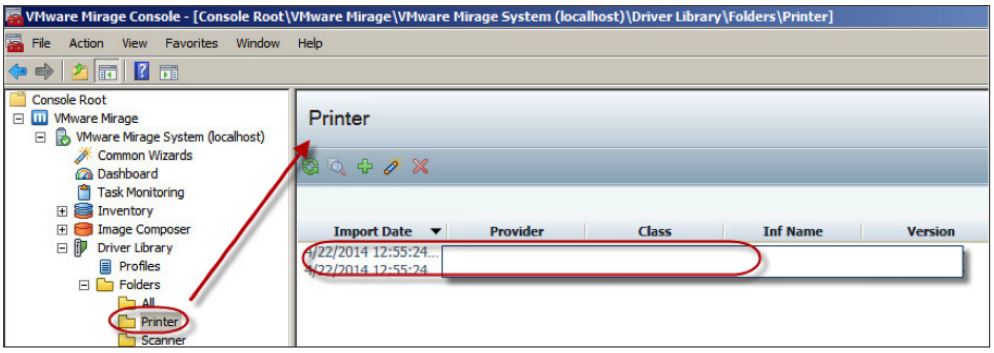
   A prompt asks whether you want to monitor the task progress.



5. Click **Yes** to monitor the task.

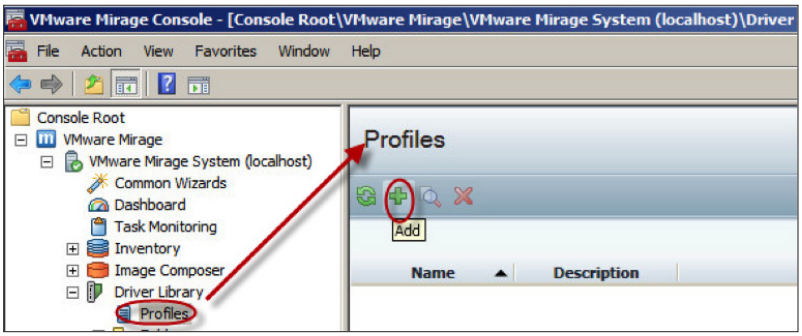


6. When the task finishes, return to the driver folder to verify the imported drivers are listed in the driver folder.

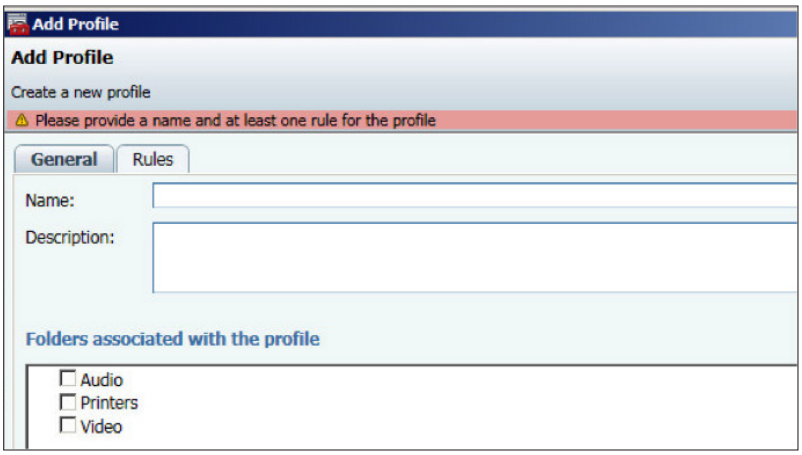


Create a Driver Profile

1. In the left pane of the Mirage Console, expand **Driver Library** and click **Profiles**.
2. In the Profiles pane, click the **Add** icon.

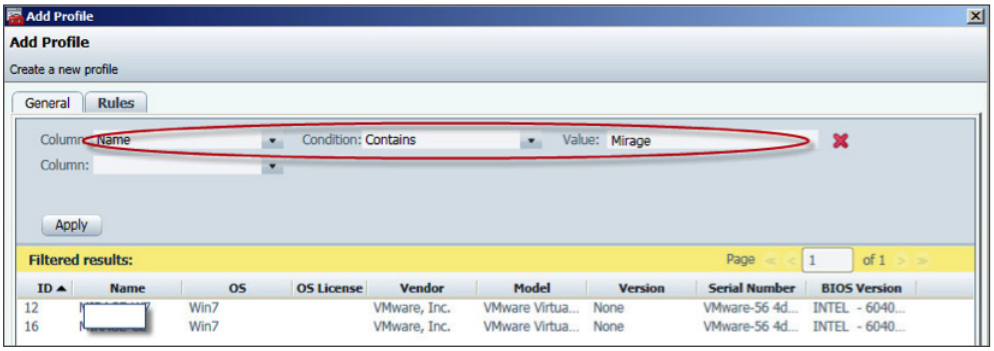


The Add Profile window appears.



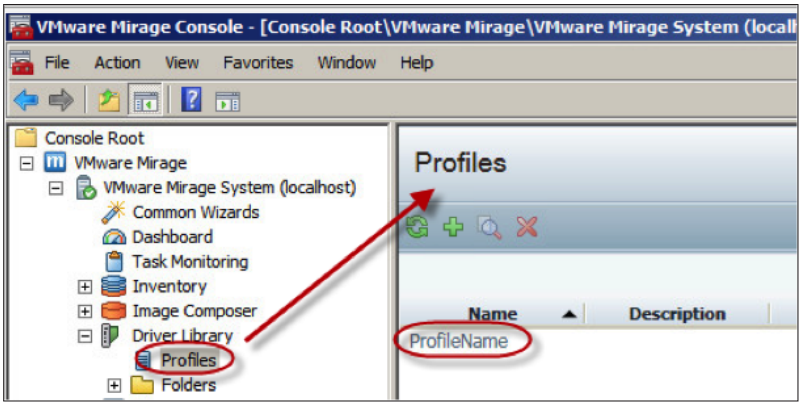
3. In the General tab, provide a name for the profile and select the driver folders.
4. In the Rules tab, define rules for the profile.

   The rules match the profile to the endpoints.



5. Click **OK** to finish.

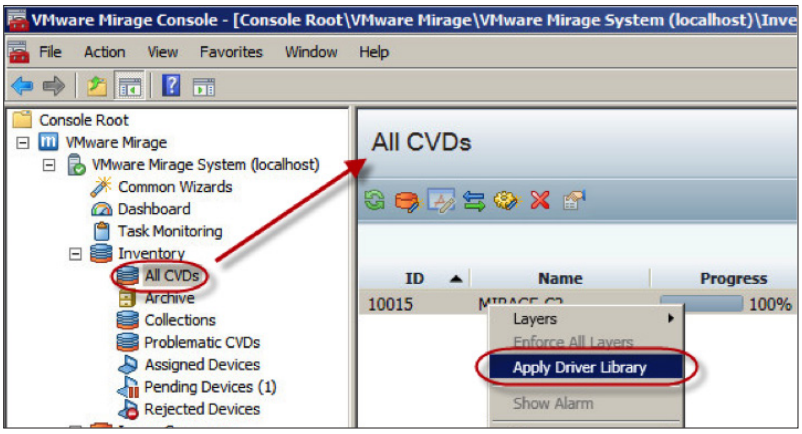
   The created driver profile is listed in the right pane.



Assign a Driver Profile

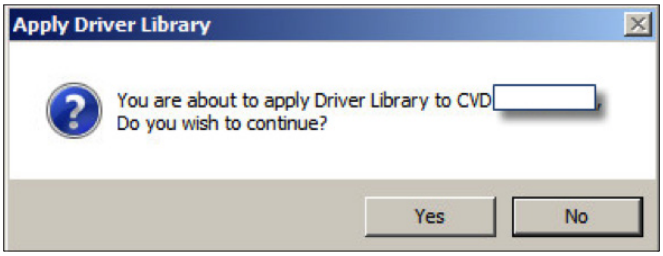
Now that you have drivers imported into the Mirage server and created driver profiles, you can apply the driver profiles to endpoints as follows.

1. In the left pane of the Mirage Console, expand **Inventory** and click **All CVDs**.



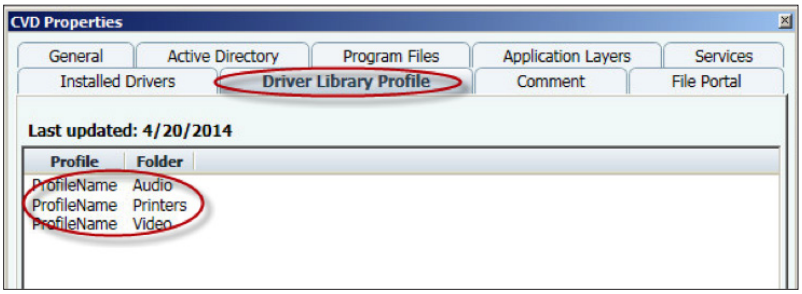
2. In the All CVDs pane, right-click the CVD to which you want to apply a driver profile and select **Apply Driver Library**.

   A confirmation dialog appears.

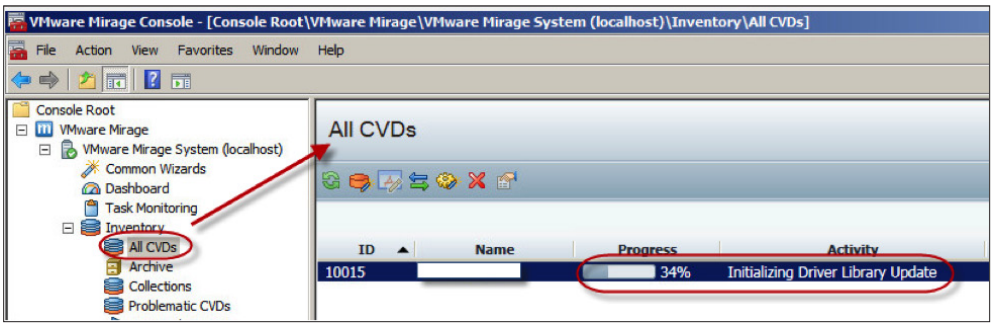


3. Click **Yes**.
4. Double-click a CVD to open its Properties window.
5. Click the **Driver Library Profile** tab.

   A list of the applied driver profiles and folders appears.

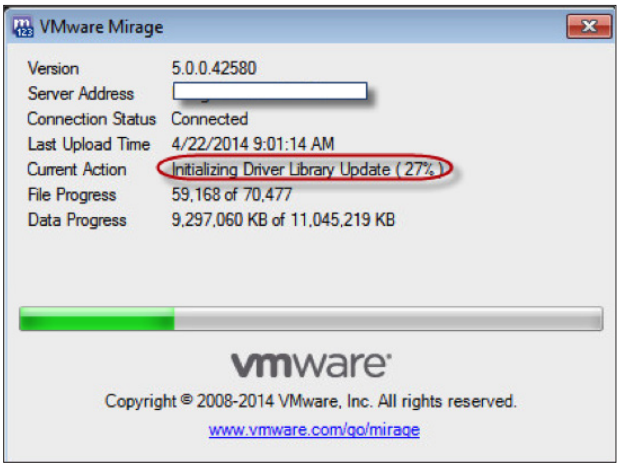


The status of the CVD shows that the drivers are being updated to the endpoint.



6. Access the endpoint to check the driver library download progress.

   Double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.



Centralizing Endpoints

At this point, you have created your test machines, the base layer, app layers, and driver profiles. Now you can centralize the end-user endpoints (the Windows XP virtual machine for the Windows 7 migration and the Windows 7 virtual machine for layer management).

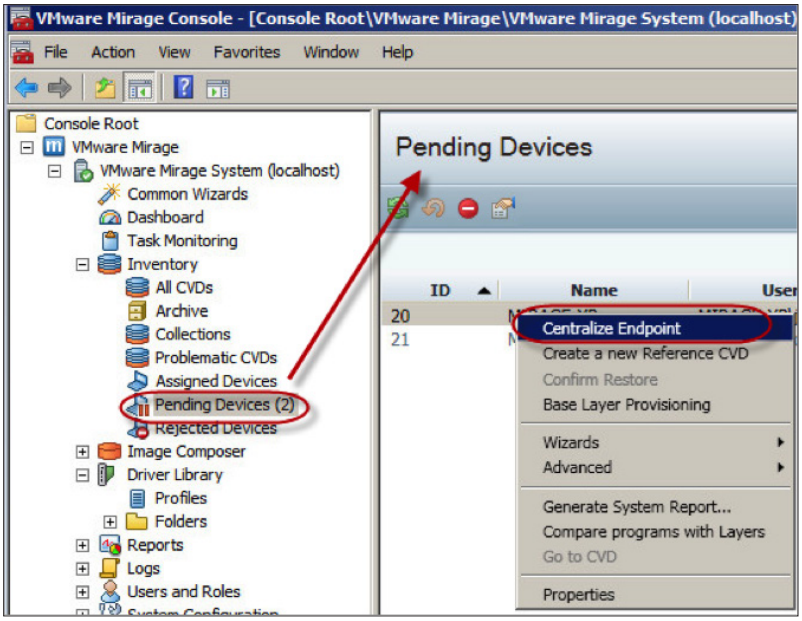
You can centralize the test machines in two ways: using the centralize endpoint method or the base layer provisioning method. Both methods are described in this section. Implement the method that best suits your requirements:

- Centralize endpoint – Backs up your test machine according to the CVD policy. You can select the base layer and app layers during this process.
- Base layer provisioning – First cleans up the device and 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.

Use the Centralize Endpoint Method

Use this method to centralize your test machines if you want to only back up and assign layers to the test machines. This method does not clean up the machines.

1. In the left pane of the Mirage Console, expand **Inventory** and click **Pending Devices**.
2. In the Pending Devices pane, right-click a device and select **Centralize Endpoint**.

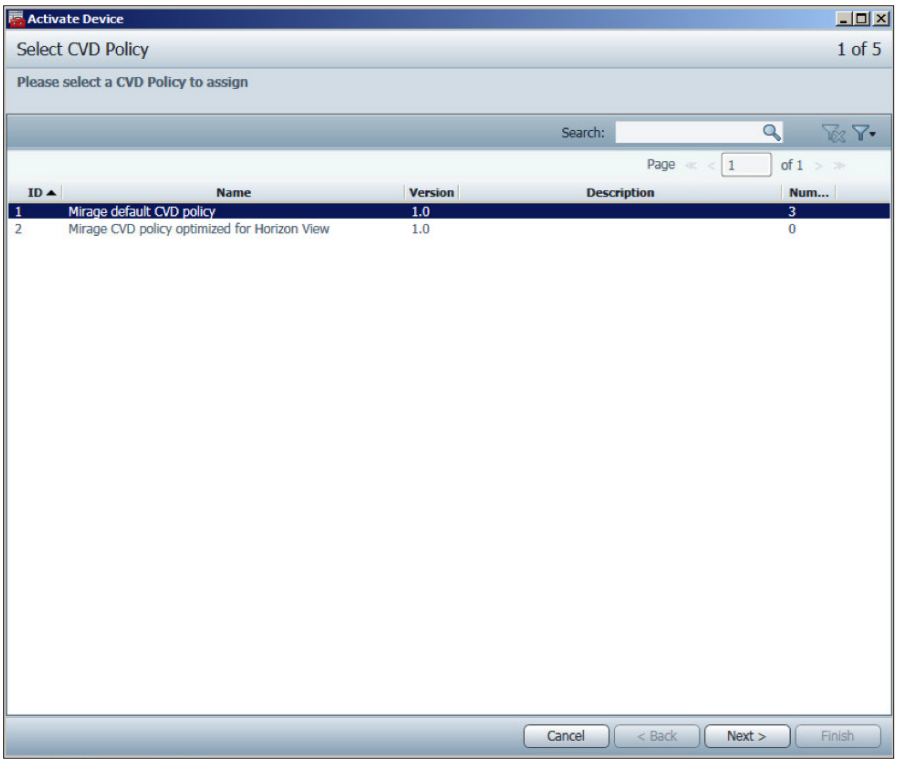


The Activate Device page appears. Two default policies are available:

- Mirage default CVD policy
- Mirage CVD policy optimized for View

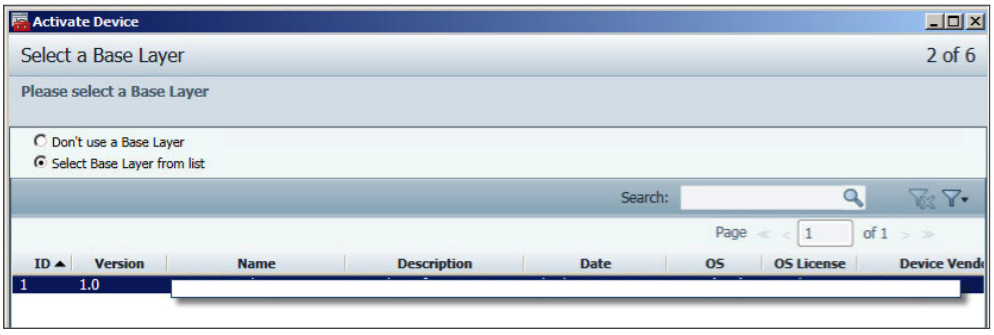
If you select the Mirage default CVD policy, the endpoint's content is backed up according to the rules in the policy. You can revert the devices to a Mirage snapshot, restore user files to previous versions, or perform disaster recovery after centralizing. If you perform Windows 7 migration against a Windows XP endpoint that uses this policy, you can roll back in case of any issues.

If you select the Mirage CVD policy optimized for View, the corresponding devices do not upload files to the data center. Mirage periodically uploads only metadata about these devices, such as the list of installed applications. You *cannot* revert the devices to a Mirage snapshot, restore user files to previous versions, or perform disaster recovery after centralizing the devices. If you perform a Windows 7 migration against a Windows XP endpoint that uses this policy, you *cannot* roll back the endpoint if you encounter an issue. However, you can still assign a base layer and update app layers to the endpoints. For more information, see Using a CVD Policy for Layer Management.



3. Select a policy according to your requirements and click **Next**.

   The Select a Base Layer page appears.



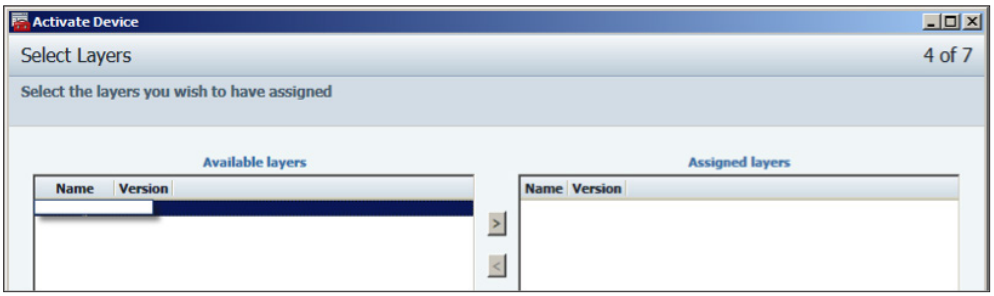
You are presented with two options:

- **Don't use a Base Layer** – This option does not enable you to select app layers.
- **Select Base Layer from list** – This option requires you to select a base layer from the list and then enables you to select app layers.

4. For this evaluation exercise, choose **Select Base Layer from list**, click the base layer to apply to this test machine, and then click **Next**.

   In addition to selecting a base layer, this option enables you to select app layers, but you do not need to select any app layers for this exercise.

   Note: If you select the Don't use a Base Layer option, you also cannot select app layers.

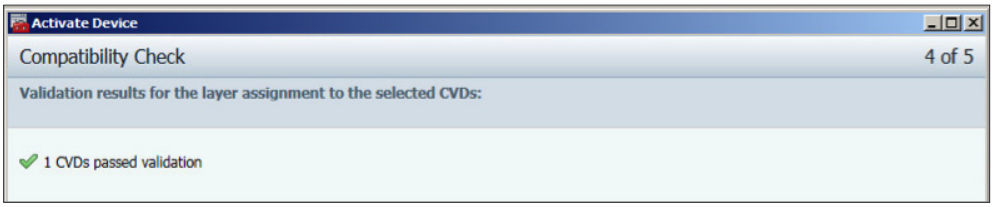


5. Click **Next**.

   The Select Target Volume page appears.

6. Select a volume and click **Next**.

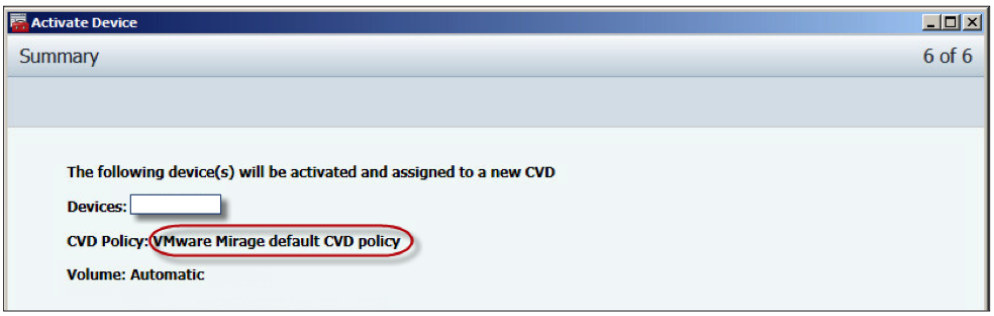
   The Compatibility Check page appears.



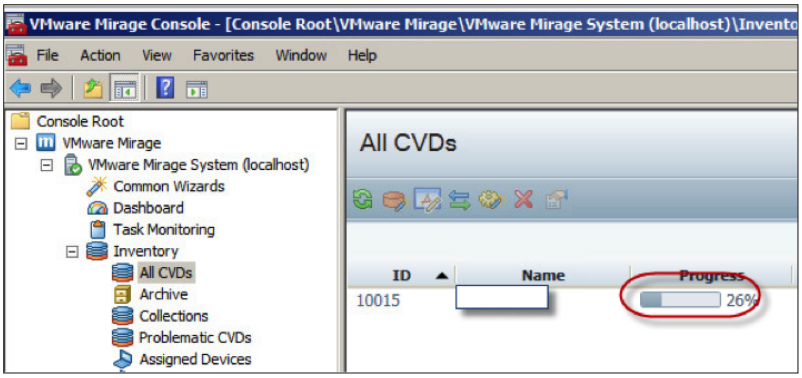
   If the page lists errors, you must fix them before proceeding. If the page lists warnings, you can ignore them and continue.

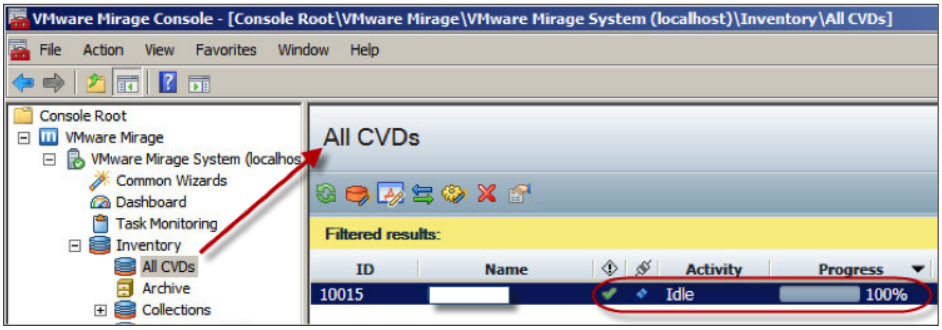
7. Click **Next**.

   The Summary page appears.



8. Click **Finish**.
9. In the left pane, expand **Inventory** and click **All CVDs**.
10. In the All CVDs pane, monitor the progress. When the progress is 100%, the Activity value changes to Idle.

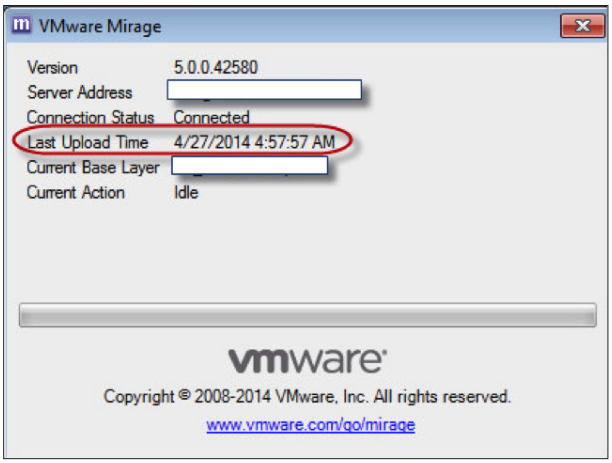




11. (Optional) Verify that the endpoint is centralized by double-clicking the Mirage icon in the system tray to check the status.

    The dialog box lists the selected layers and the last upload time.

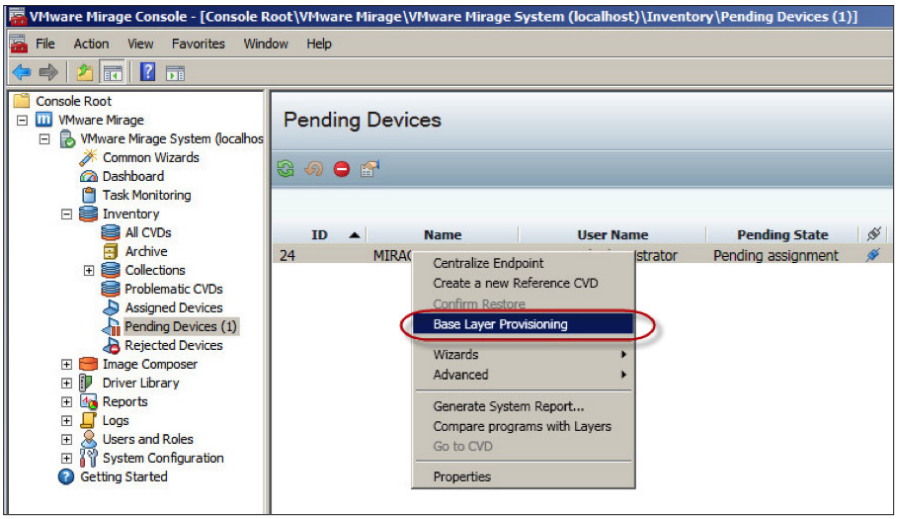
Your endpoints are centralized.



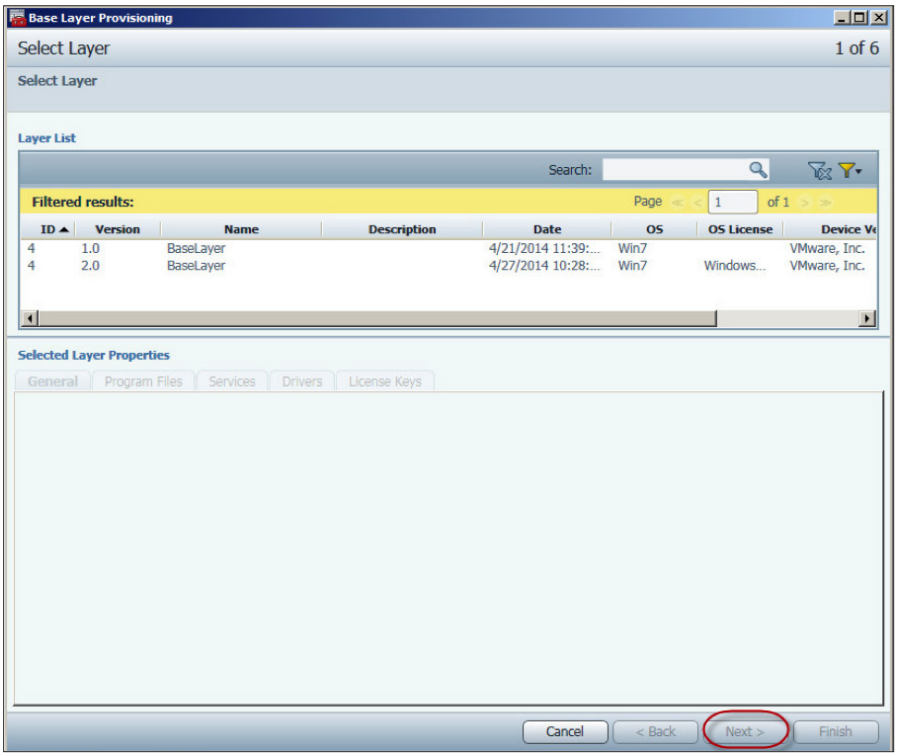
Use the Base Layer Provisioning Method

Use this method to centralize a test machine if you want to first clean up the machine. Base layer provisioning replaces the content on the endpoint with the content in the base layer. All previous content is permanently removed.

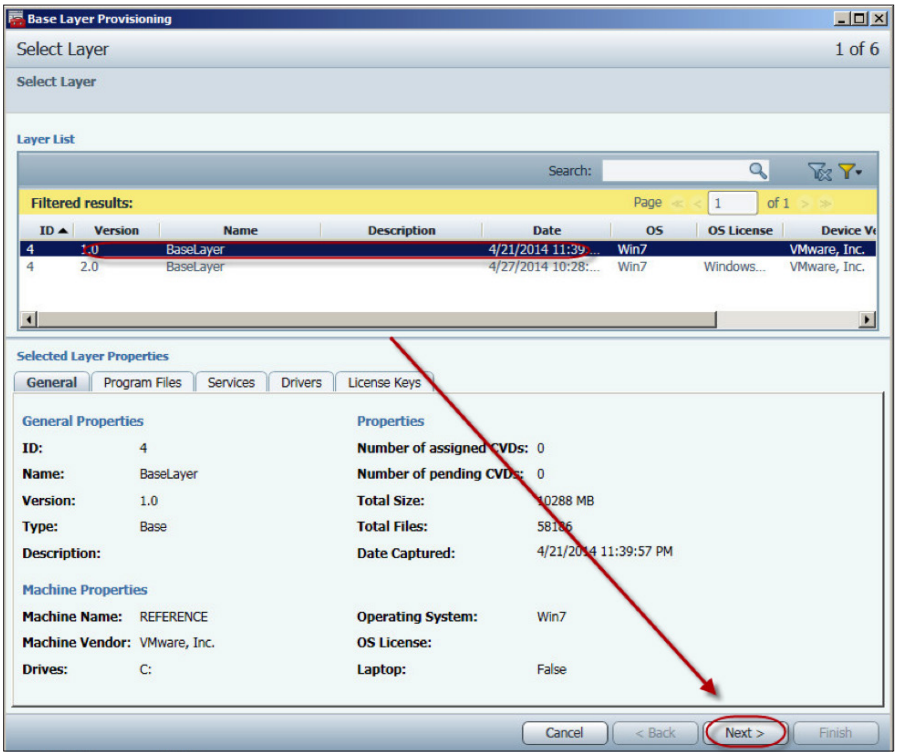
1. In the left pane of the Mirage Console, expand **Inventory** and click **Pending Devices**.
2. In the Pending Devices pane, right-click a device and select **Base Layer Provisioning**.



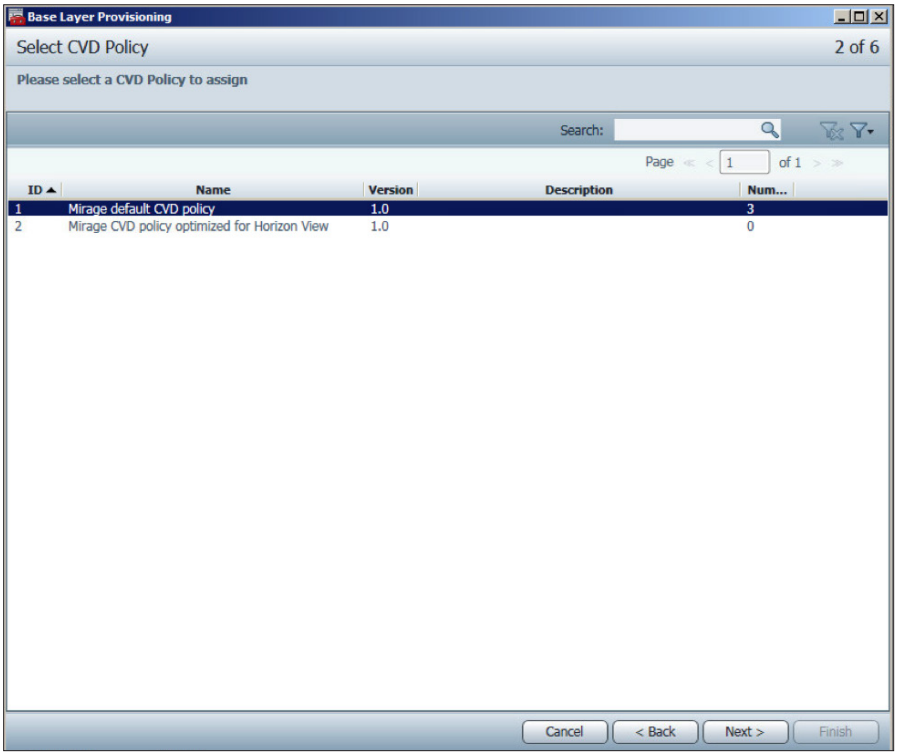
The Select Layer page appears. The **Next** button is grayed out until you select a base layer.



3. Click a base layer to select it and click **Next**.



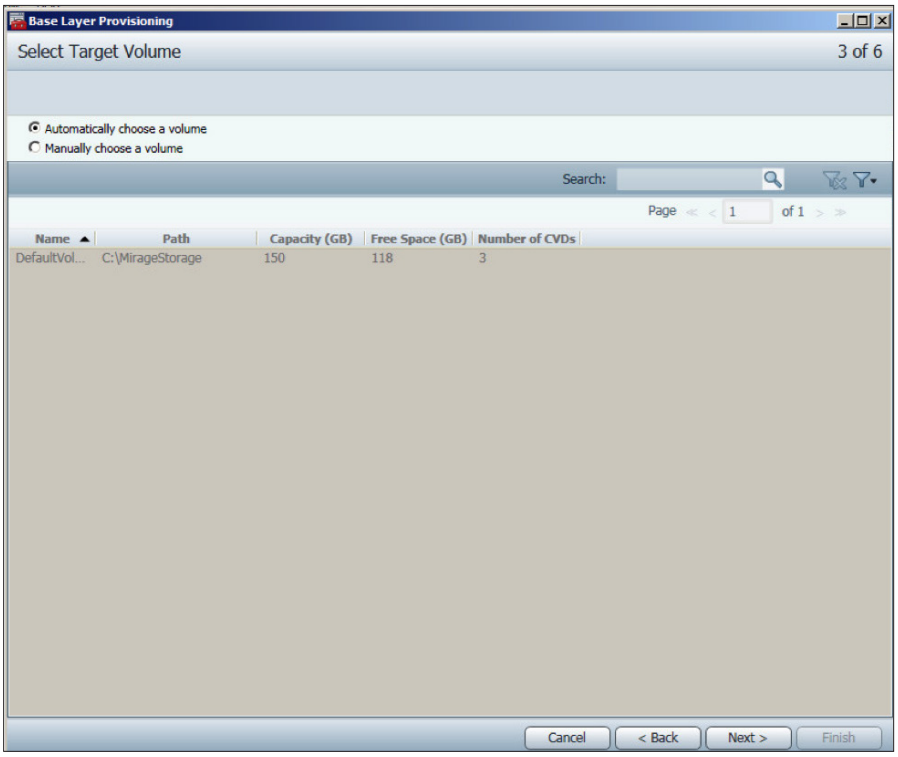
The Select CVD Policy page appears.



4. Select a policy according to your requirements and click **Next**.

   See Centralize an Endpoint Method for an explanation of the default policies.

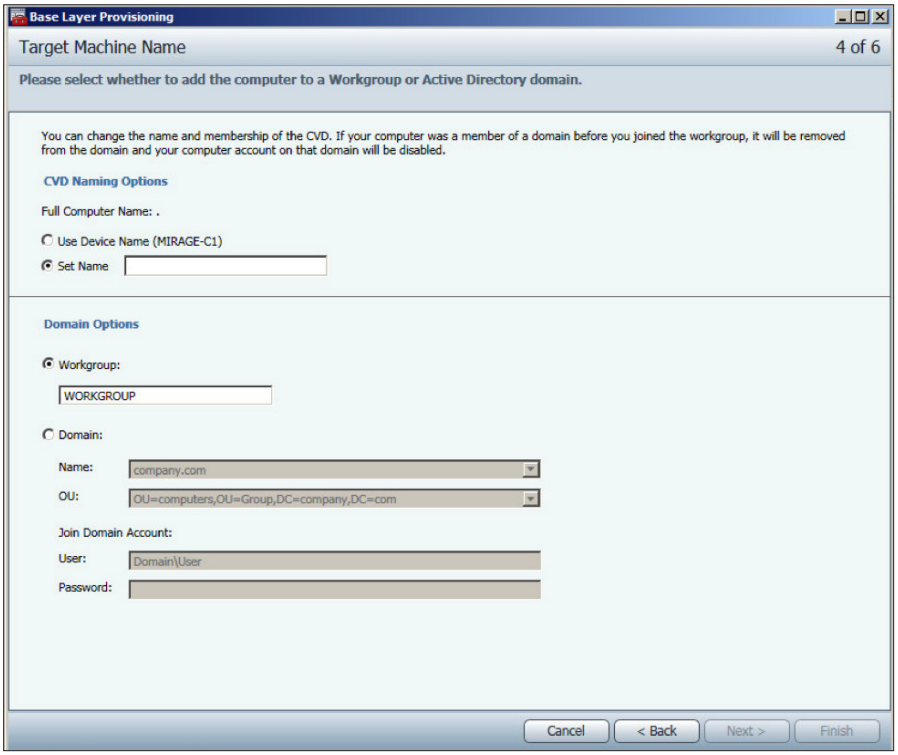
   The Select Target Volume page appears.



5. Select **Automatically choose a volume** and click **Next**.

   The Manually choose a volume option enables you to specify the volume to use rather than using the volume selected by Mirage.

   The Target Machine Name page appears.



6. For this evaluation exercise, select **Use Device Name** and **Workgroup**, and then click **Next**.

   The following table provides useful information about this page when you deploy Mirage in a production environment.

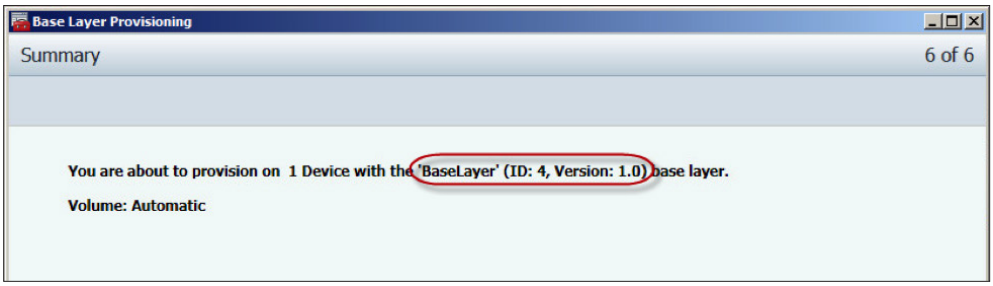
ITEM	DESCRIPTION
CVD Naming Options	Two CVD naming options exist: • Use Device Name • Set Name
Domain Options	Two domain options exist: • Workgroup • Domain If you choose to join the target device to a domain, you must specify the domain that the migrated endpoint joins after the migration process is complete. The Name and Join Domain Account information is automatically specified if you previously entered the Join Domain Account credentials as follows: In the left pane of the Mirage Console, right-click **System Configuration**, select **Settings**, and fill in the fields in the Join Domain Account section of the General tab. If the join domain account is not configured in the system configuration, you must provide the credentials for the endpoints to join the domain. Mirage cannot automatically join the endpoints to the domain. You can change the Name, OU, and Join Domain Account credentials. Select the **Name** and **OU** values from the drop-down menus or enter the values. All used domains in the system prepopulate the drop-down menus. The required syntax pattern is indicated in each field. The OU value must be in standard open LDAP format. For example: `OU=Notebooks`, `OU=Hardware`, `DC=VMware`, `DC=com`

7. Click **Next**.

   The Image Validation page appears.

8. Click **Next**.

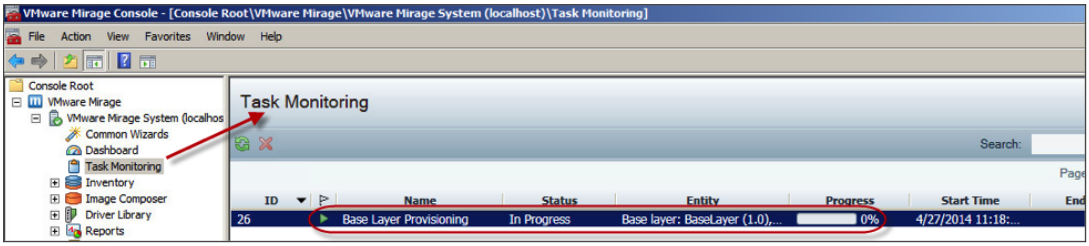
   The Summary page appears. The selected base layer name is listed.



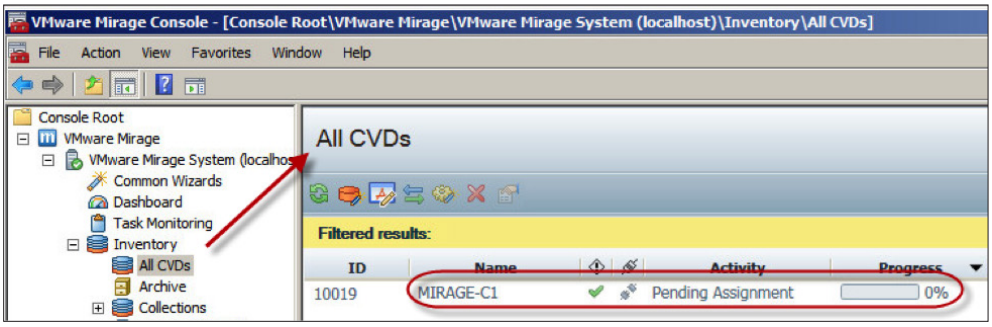
9. Click **Finish**.

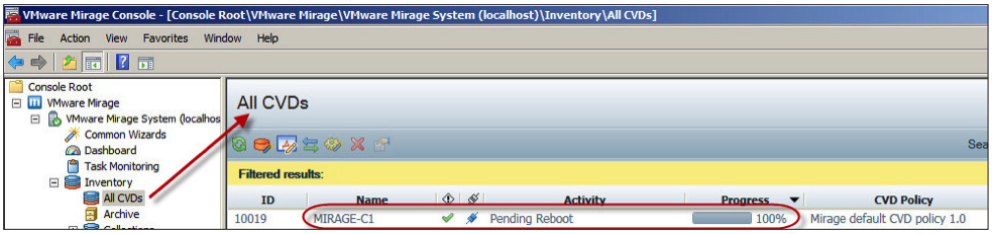
10. In the left pane, click **Task Monitoring** and then verify in the Task Monitoring pane that the task has started.

    A Status value of In Progress indicates that the task has started.

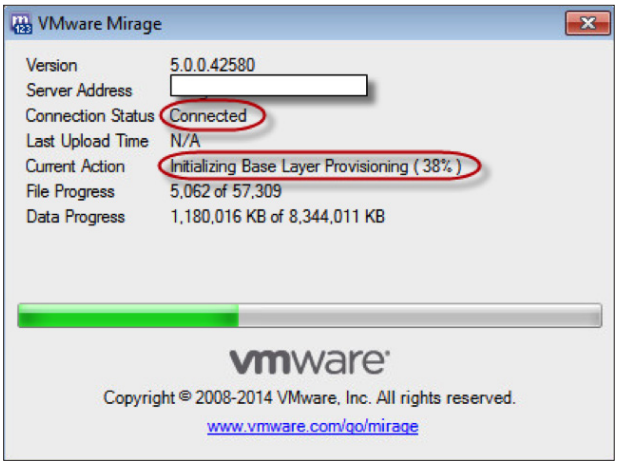


11. Monitor the progress of the task by selecting **Inventory** > **All CVDs**. Initially, the Activity value is Pending Assignment, changes to Initializing Base Layer Provisioning, then Base Layer Provisioning, and finally to Pending Reboot.

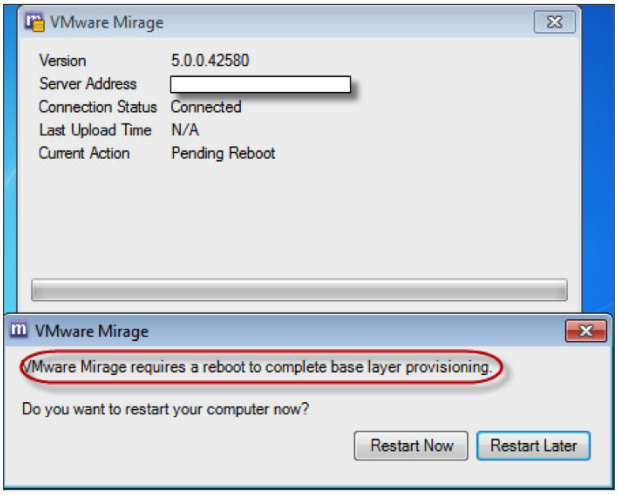




You can also access the endpoint and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box to monitor the task.

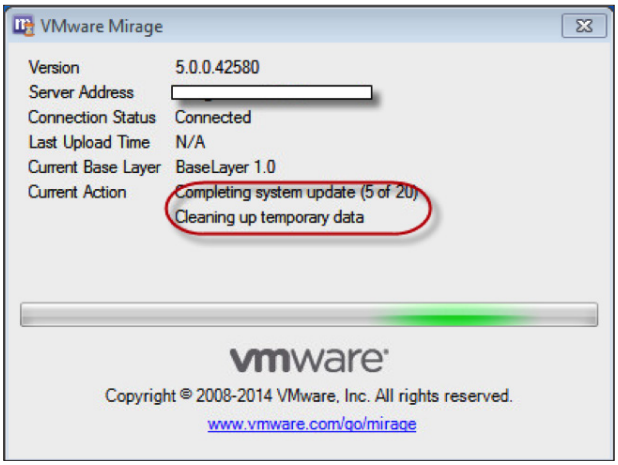


After finalizing, Mirage displays a dialog box asking you to restart the endpoint.

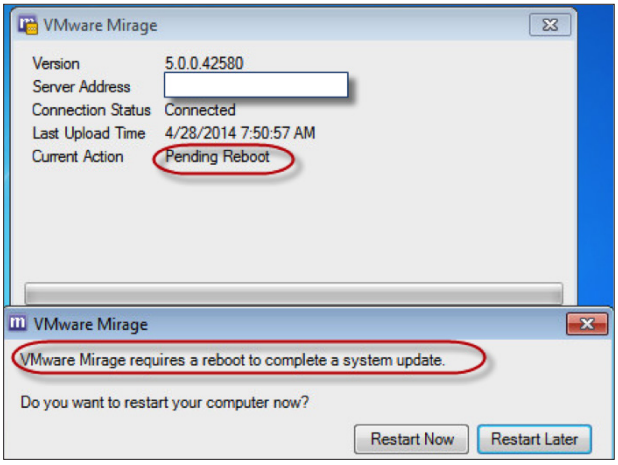


12. Click **Restart Now** in the VMware Mirage dialog box of the endpoint.

13. Log in to the endpoint again.



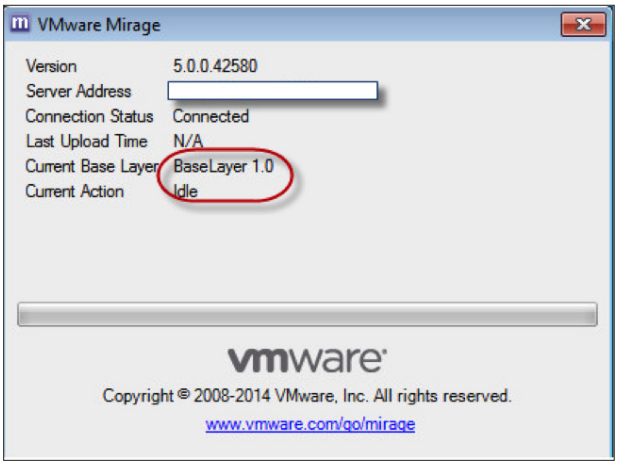
Mirage finishes the update.



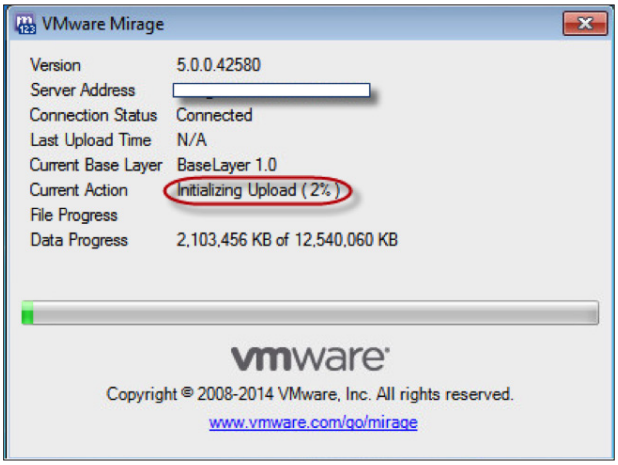
14. Click **Restart Now** again.

15. Log in to the endpoint again and monitor the status of the Mirage client.

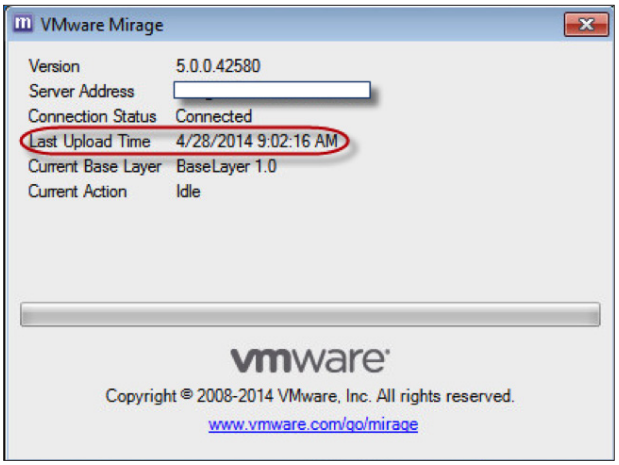
    The Current Action value changes to Idle. The value of Current Base Layer is the name of the base layer you assigned previously in this task.



    In a few seconds, the Current Action value changes to Initializing, which indicates that Mirage is starting the endpoint again.

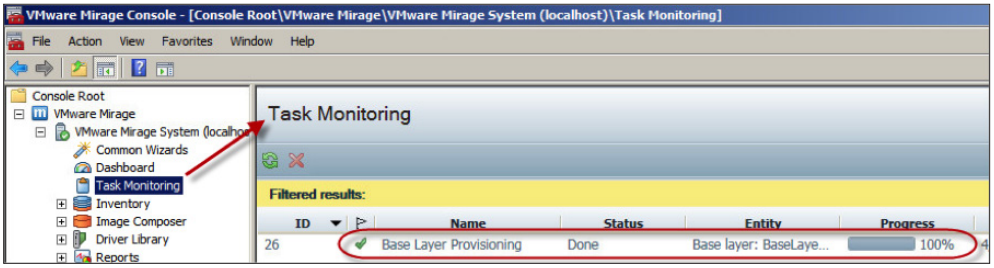


The upload is complete when Last Upload Time has an assigned value and the Current Action value has changed back to Idle.



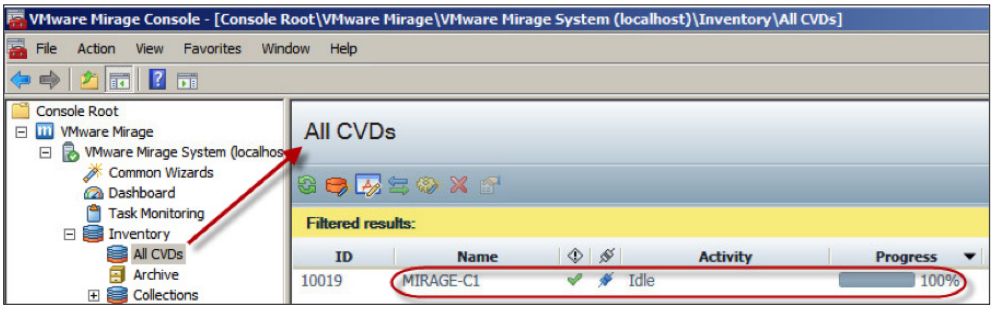
16. In the left pane of the Mirage Console, click **Task Monitoring**.

17. In the Task Monitoring pane, verify that the task has reached 100%.

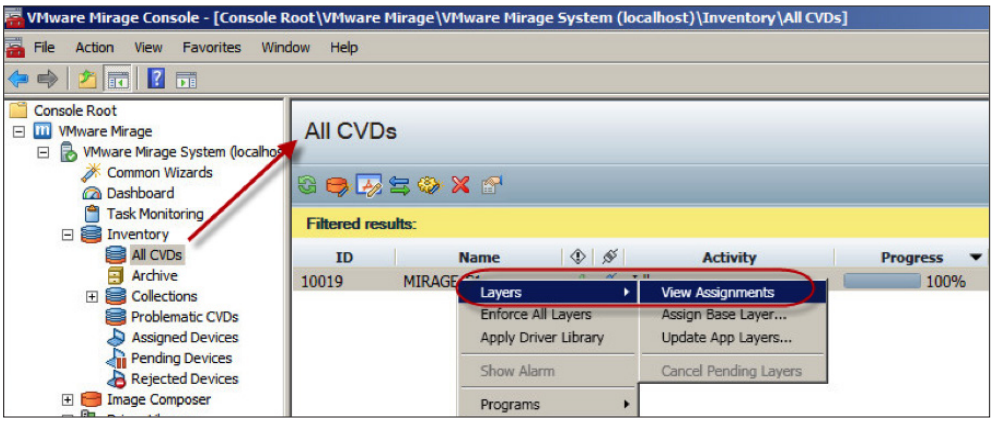


18. Expand **Inventory** and click **All CVDs**.

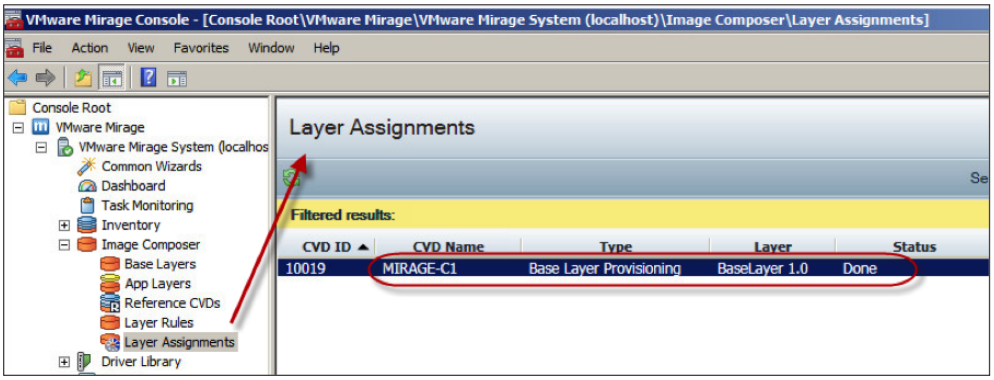
    The Activity value of the CVD changes to Idle.



19. Right-click the CVD and select **Layers** > **View Assignments**.



The Type value for the new layer is Base Layer Provisioning, the Layer value is the layer you selected, and the Status value is Done.



Your test machine is now provisioned with the selected base layer.

Migrating to Windows 7 or 8.1

With Mirage, you can migrate an endpoint from one Windows OS version to another. This guide describes a migration from Windows XP to Windows 7, but you can perform other migrations using the same process.

You can perform a real-time, in-place migration, upgrading the OS of an endpoint from one version to another and migrating user profiles to the new OS without interrupting the user's work.

Mirage supports the following migrations:

• Windows XP endpoint to Windows 7

• Windows Vista endpoint to Windows 7

• Windows 7 endpoint to Windows 8.1 or 8.1 Update 1

For this evaluation exercise, you need USMT 4.0 with hotfix, which you import into the Mirage server before beginning the migration. See Importing USMT for a Windows 7 Migration.

Migration Process
For this migration, you capture a base layer and one or more app layers. You run the Windows OS Migration wizard in the Mirage Console. After you enter your selections, the wizard starts the migration.

Prior to downloading the base layer to the target endpoint, the Mirage server takes a snapshot of the endpoint so that you can roll it back to the pre-migration state, if necessary.

Mirage then compares the base layer in the data center to the endpoint CVD in the data center. Only differences between the two are downloaded to the endpoint.

During migration, the differences between the assigned layers—the base layer and app layers—and the endpoint are downloaded from the data center to the endpoint. This process occurs in the background while the user works.

When the download is complete, the user is prompted to reboot. During the reboot, the following occurs:

1. The necessary drivers for the new Windows 7 endpoint are downloaded from the Mirage driver library, and the drivers are installed on the target endpoint.
2. The OS data is moved in the following manner.
    a. The existing Windows XP files are moved to the `C:\Windows.Old` directory on the endpoint.
    b. The new bits of the Window 7 base layer that were downloaded are moved to the `C:\Windows` directory.
    c. Bits that can be reused from Windows XP to complete the Windows 7 OS are moved from the `C:\Windows.Old` directory back to the `C:\Windows` directory.

An update screen appears. The following tasks are performed during this process:

1. USMT accesses the original user files in the C`:\Windows.Old` directory and migrates the user data and profiles from Windows XP to Windows 7.
2. Mirage rejoins the endpoint into the domain with the credentials you supplied.
3. Mirage runs the post-migration script.
4. The user is prompted to reboot the endpoint.

The login screen appears when the update is finished. The migration to Windows 7 is complete.

Application settings and data that are not handled by USMT remain in the `C:\Windows.Old` directory. You can manually restore or delete them later. See Removing the Windows.Old directory after User Profile or Windows 7 Migration with VMware Horizon Mirage (2050882).

Applications on the Windows XP target endpoint are not retained because they might not work in Windows 7. Instead, the applications in the assigned app layers are downloaded to the Windows 7 endpoint.

The Windows 7 migration process retains the original endpoint computer name. You can choose to leave the endpoint in a workgroup or join it to a domain. If you join it to a domain, you must provide the domain information and credentials.

You can perform the Windows 7 migration over a LAN or WAN. For a migration in a remote office over a WAN, it is recommended that you use the Mirage branch reflector feature to reduce WAN bandwidth usage. A Windows 7 machine configured as a branch reflector can download the new Windows 7 base layer once over the WAN and then have the image ready on the local LAN for the other remote office endpoints.

The Windows 7 Migration wizard is for migrating existing endpoints to a new version of the OS. For a migration involving different hardware, see the VMware Mirage Administrator's Guide.

Prepare Your Migration Environment
In this guide, you have already performed the following tasks:

- Importing USMT for a Windows 7 Migration
- Capturing the Base Layer from the Reference CVD
- Capturing an App Layer (Optional)
- Configuring the Mirage Driver Library and Profile (Optional)
- Centralizing Endpoints

Before you begin the migration, take a virtual snapshot of the endpoint as insurance using a product such as Workstation, Fusion Pro, or vSphere. Mirage also takes a snapshot of the endpoint before you migrate the endpoint.

Note: The virtual machine snapshot is different from a Mirage snapshot or a Mirage desktop image in the data center.

You might also need to decrypt the endpoints. If you are migrating endpoints using a third-party, full-disk-encryption tool other than Sophos SafeGuard Enterprise 5.5, decrypt the endpoints before proceeding with the Windows 7 migration. The encryption software might cause the migration to fail.

If your endpoint devices are decrypted before migration, the device for the base layer capture does not need to be encrypted before capturing the base layer. For more information, see Windows 7 Migration with Sophos SafeGuard Enterprise 5.5.

Windows 7 migration for endpoints encrypted with another full-disk encryption tool might work with the methodology described here, but VMware has not explicitly tested other tools. Therefore, you should decrypt endpoints using a third-party, full-disk encryption tool other than Sophos SafeGuard Enterprise 5.5 before proceeding with the migration, because the encryption software might interfere and cause the migration to fail.

You are now ready to perform the migration.

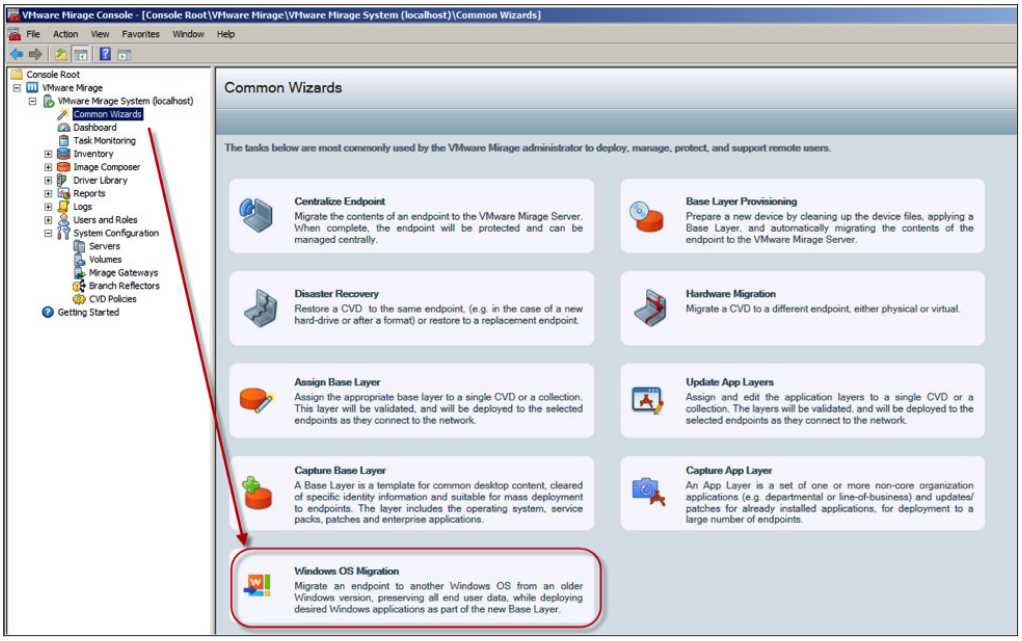
Performing an In-Place Windows 7 Migration

After you have finished preparing your migration environment, you are ready to migrate your Windows OS using the following tasks.

Configure the Migration Parameters

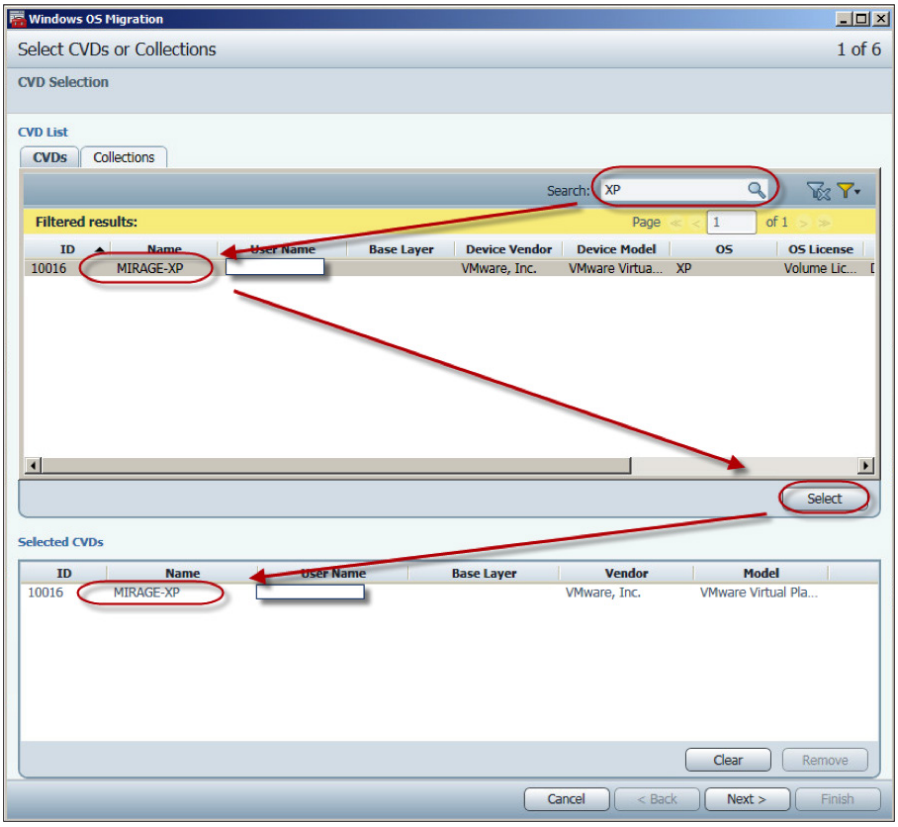
The Windows OS Migration wizard leads you through this task.

1. In the left pane of the Mirage Console, click **Common Wizards**, and in the right pane, click **Windows OS Migration**.

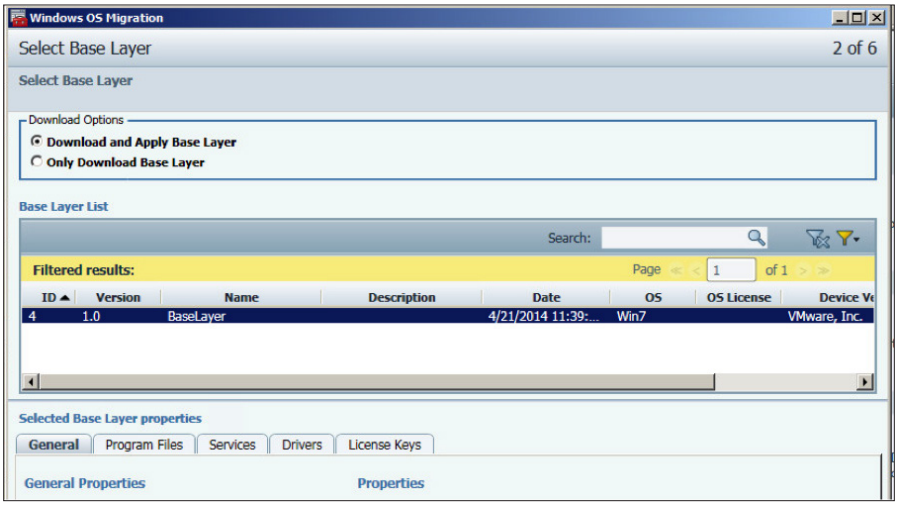


The Select CVDs or Collections page appears.

2. Search for the Windows XP test machine you created and centralized for this exercise, and then click **Next**.



The Select Base Layer page appears.

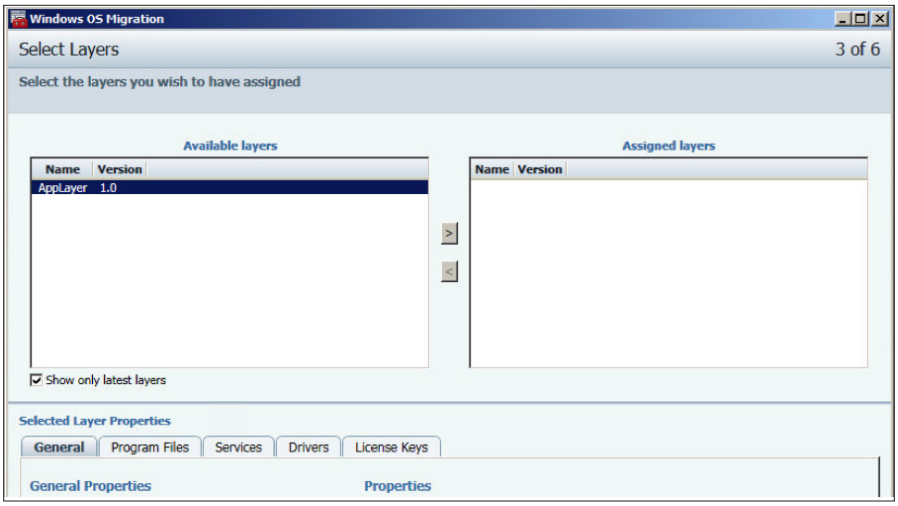


3. For this evaluation exercise, select **Download and Apply Base Layer** to download the image to all endpoints and immediately apply the new OS to all endpoints.

   Note: The Only Download Base Layer option downloads the image to all designated endpoints, but waits to apply the image. You would select this option if you want to apply the base layer at a later time.

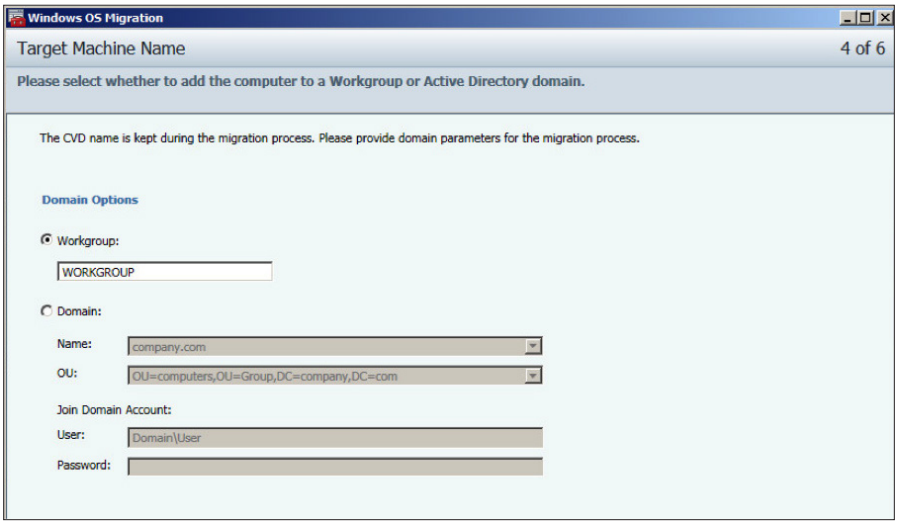
4. Select the base layer you captured from the reference CVD as a prerequisite to this task and click **Next**.

   The Select Layers page appears.



5. Move the layers you want from the Available layers section to the Assigned layers section and click **Next**.

   The Target Machine Name page appears.



6. Select **Workgroup** for this evaluation exercise and then click **Next**.

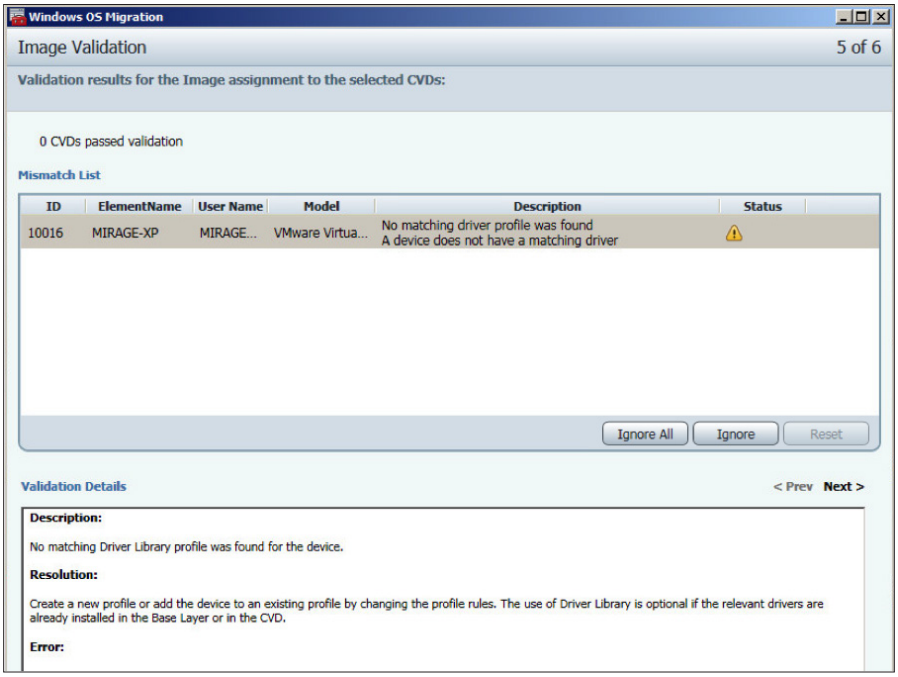
   In a production environment, if you choose to join the target device to a domain, you need to set the domain that the migrated endpoint joins after the migration process is complete. The Domain Name and Join Domain Account credentials are automatically entered if you have already set the credentials in the Mirage Console settings.

7. Click **Next**.

   The Image Validation page appears.

   A warning informs you that no matching profile was found for the device. You can ignore the warning because you are migrating a virtual machine, so a driver profile is not necessary.

   Note: If an error is listed on this page, you must fix it before proceeding.



8. Click **Ignore**, and then click **Next**.

   The Summary page appears.

9. Click **Finish**.

   The migration starts.

What to Do Next

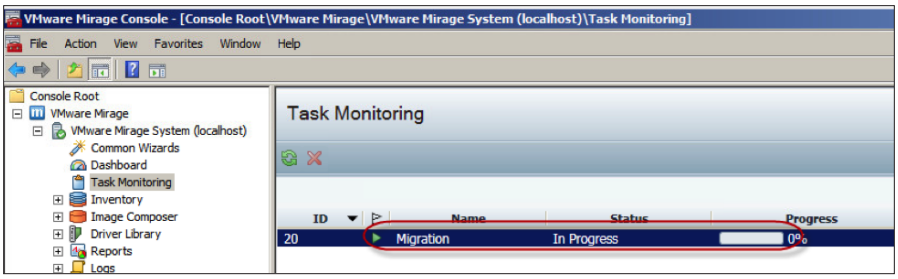
Monitor the progress of the migration using either of the following methods:

- Mirage Console
- Endpoint

Use the Mirage Console to Monitor the Migration Process
The Mirage Console shows you the progress of the migration.

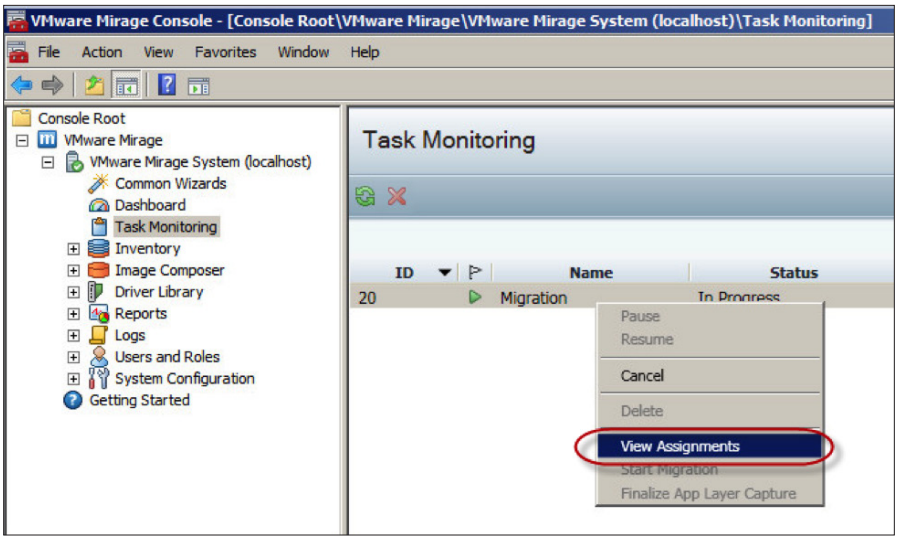
1. In the left pane of the Mirage Console, expand **VMware Mirage**, expand **VMware Mirage System**, and click **Task Monitoring**.

   The Task Monitoring page appears in the right pane with the new Migration task listed. The Status is In Progress, and the Progress bar starts at 0%.

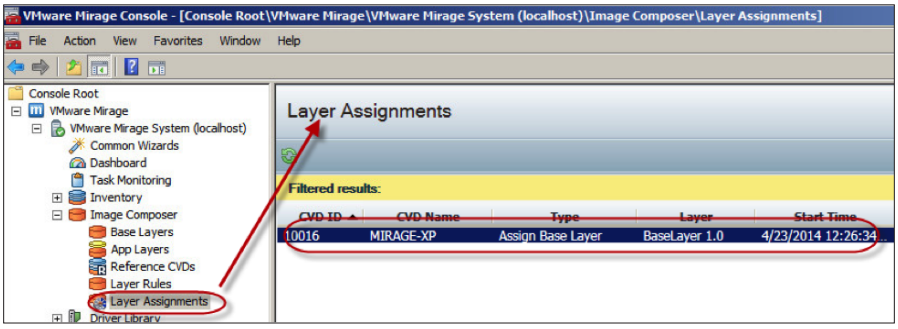


   As you monitor the Task Monitoring page, the percent value of the Progress item increases.

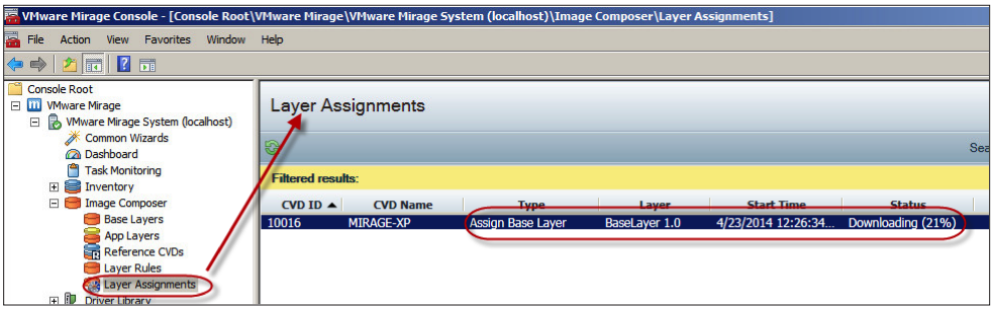
2. Right-click the Migration task and select **View Assignments**.



   The Layer Assignments page appears in the right pane.

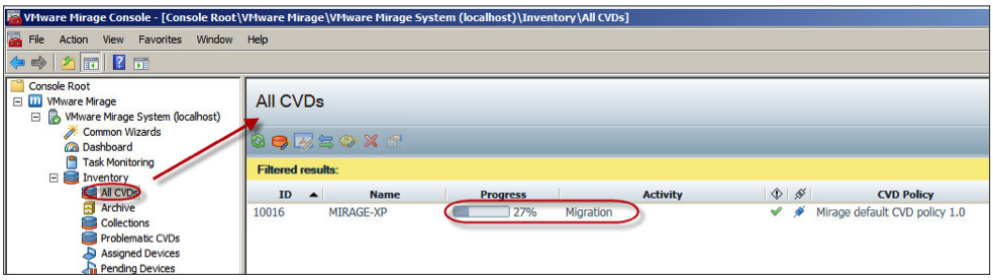


The Windows XP CVD is assigned to the base layer that you selected in the Windows Migration wizard. Mirage compares the base layer from the reference CVD to the Windows XP CVD in the data center to determine which bits are required from the base layer. Only the differences are downloaded to the Windows XP endpoint.

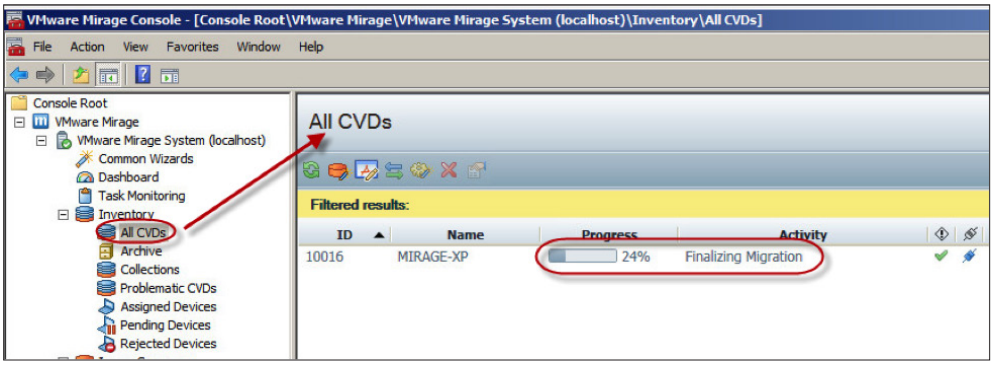


3. In the left pane of the Mirage Console, expand **Inventory** and click **All CVDs**.

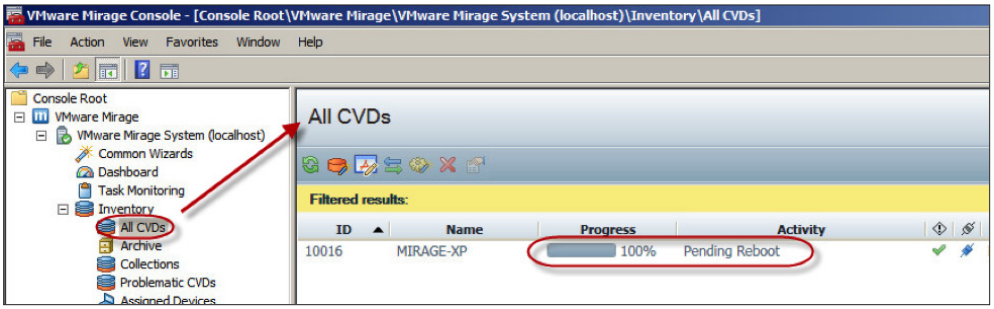
   The All CVDs window appears. The Activity value is Migration, and the Progress value is the percentage completed.



As the migration proceeds, the Activity value changes to Finalizing Migration.



During the reboot of the migrated Windows XP endpoint, the All CVDs list has an Activity value of Pending Reboot and a Progress value that stops when it reaches 100%.



4. Access the Windows XP endpoint, and double-click the Mirage icon in the system tray of the endpoint to open the VMware Mirage dialog box.

What to Do Next

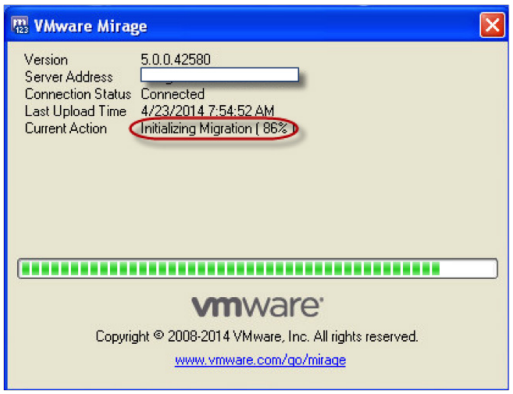
See Restart the XP Endpoint to Complete the Windows 7 Migration.

Use the Endpoint to Monitor the Migration Progress

You can monitor the migration on the endpoint.

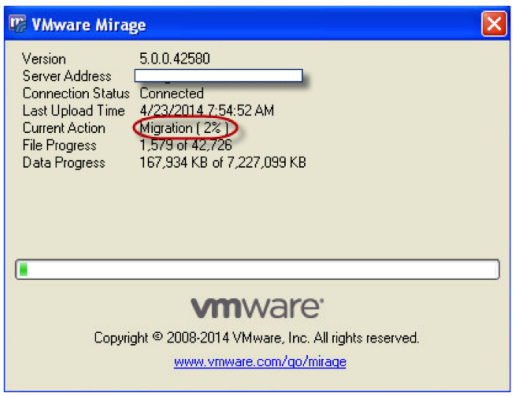
1. Open the Windows XP endpoint and double-click the VMware Mirage system tray icon.

   Current Action displays the preliminary stages of the migration.

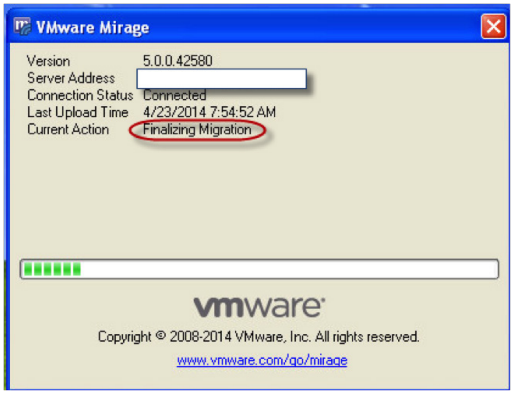


2. Continue to monitor the status by examining the Current Action value.

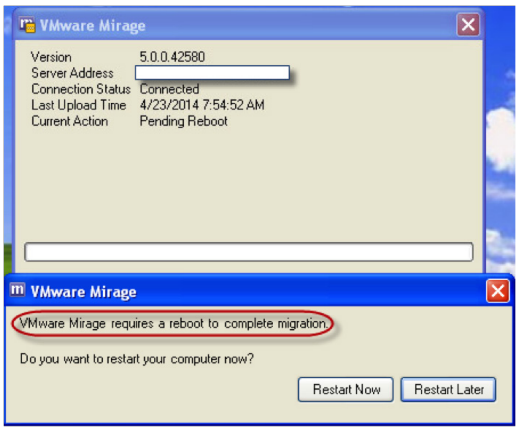
After the initialization finishes, Mirage starts downloading the assigned layers to the endpoint. The Current Action value changes to Migration.



The Windows XP endpoint proceeds, and the Current Action value changes to Finalizing Migration.



When the endpoint has completed this stage of its migration, a dialog box prompting the user to reboot appears on the desktop of the endpoint.



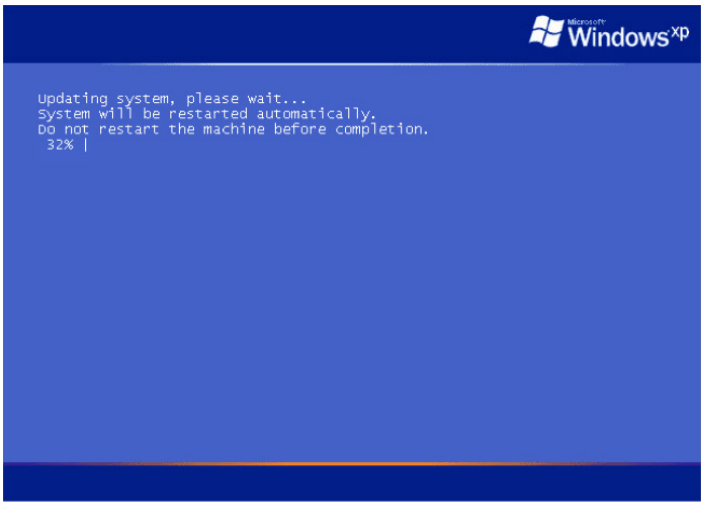
What to Do Next

See Restart the XP Endpoint to Complete the Windows 7 Migration.

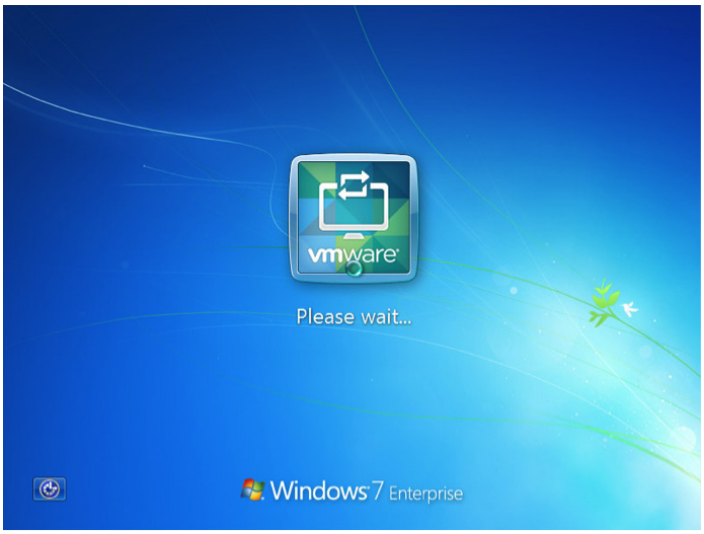
Restart the XP Endpoint to Complete the Windows 7 Migration
When you are finished monitoring the task, you must go to the endpoint and restart it.

Click **Restart Now**.

The converted Windows XP endpoint restarts, which updates the system.



The system stage switches to a pivot stage.

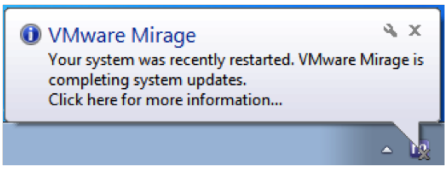


During the pivot stage, Mirage completes the system update.

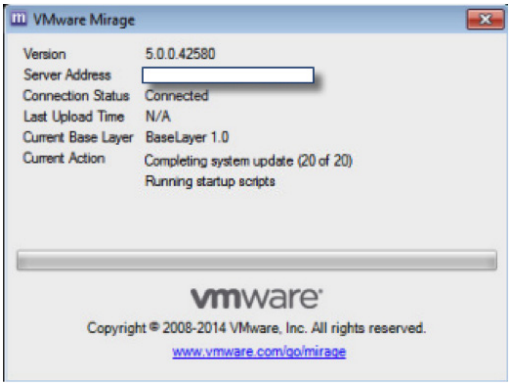
The endpoint restarts after completing the system update.

Note: The login credentials for the new Windows 7 system are the same as for the Windows XP system.

A message appears indicating that Mirage is completing the migration.



The Current Action value changes to Completing system update.



When the system update finishes, the new Windows 7 system is available for use.

Validating the Migration

Before continuing, validate the completion of the Windows 7 migration. You can perform this task using the endpoint or the Mirage Console.

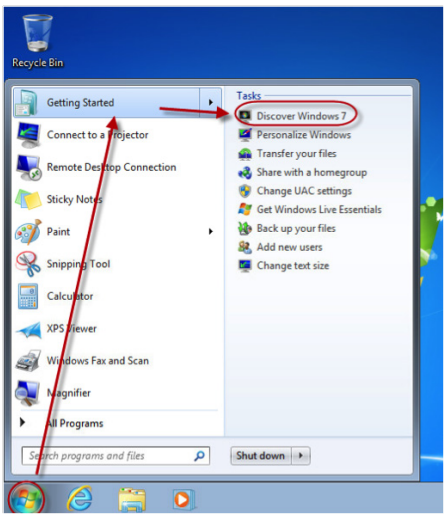
Use the Endpoint to Validate the Migration

This task validates the migration from the perspective of the previous Windows XP endpoint.

1. Log in to the former Windows XP endpoint as the same user, and check that all the user data has been migrated.

   The desktop should look the same as it did before the migration. The desktop should have the same documents, if any, before you migrated to Windows 7.

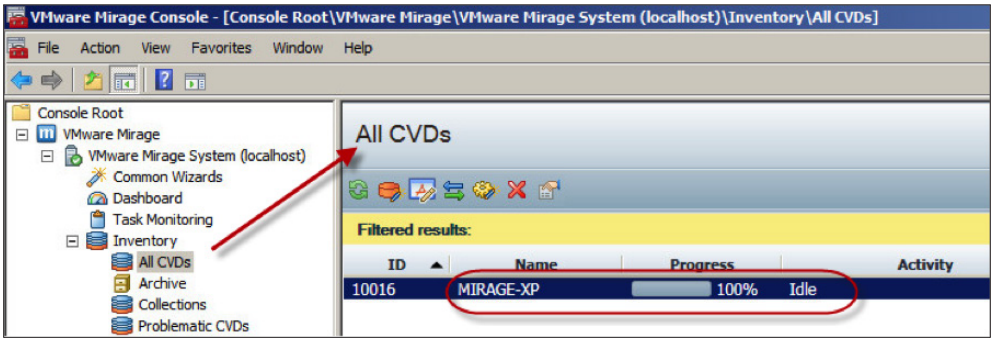
2. Verify that the new OS is Windows 7 by clicking the **Start** menu.



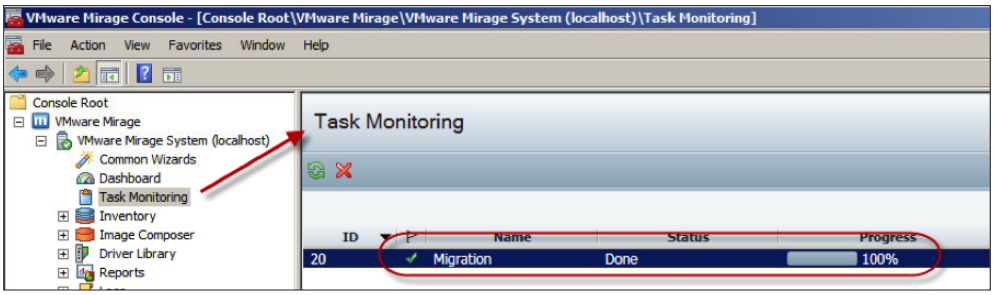
Troubleshooting tip: If you originally installed Microsoft Office on the Windows 7 reference machine and you did not use a volume license, Office requests activation on this new computer. You can ignore this problem for these exercises, but you must resolve the issue in a production system. A best practice is to use an internal KMS server to manage licenses.

Use the Mirage Console to Validate the Migration
This task validates the completion of the Windows 7 migration using the Mirage Console.

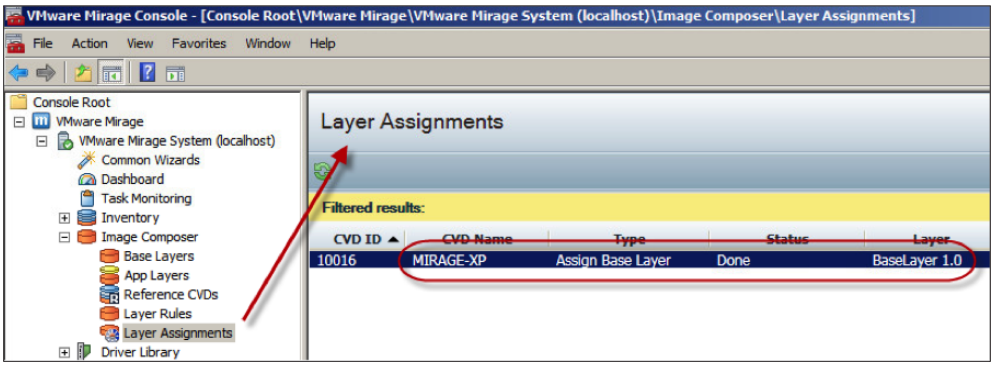
1. In the left pane, expand **Inventory** and click **All CVDs**.
2. In the All CVDs pane, confirm that the Windows XP CVD has an Activity value of Idle and a Progress value of 100%.



3. In the left pane, click **Task Monitoring**, and in the right pane, verify that the Progress value is 100%.



4. In the left pane, expand **Image Composer** and click **Layer Assignments**.
5. In the Layer Assignments pane, verify that the Status value is Done.



You have successfully migrated an endpoint from Windows XP to Windows 7.

Troubleshoot a Failed Migration to Windows 7

The following situations describe potential Mirage migration failures and respective solutions.

Migration Doesn't Start

The migration of the Windows XP desktop does not start, and the Progress value for the Migration task stays at 0%.

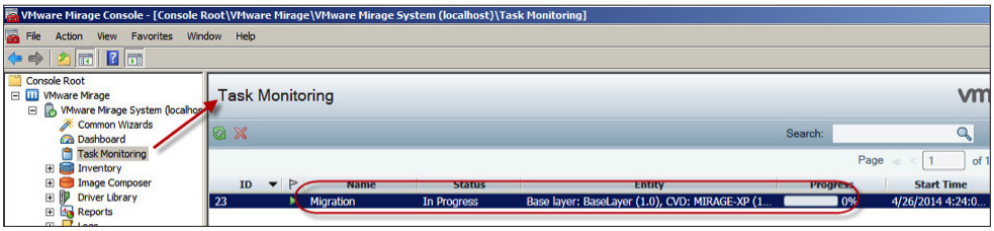


Figure 11: Task Monitoring Showing Migration Stays at 0%

On the Windows XP endpoint, the status only shows Connected.

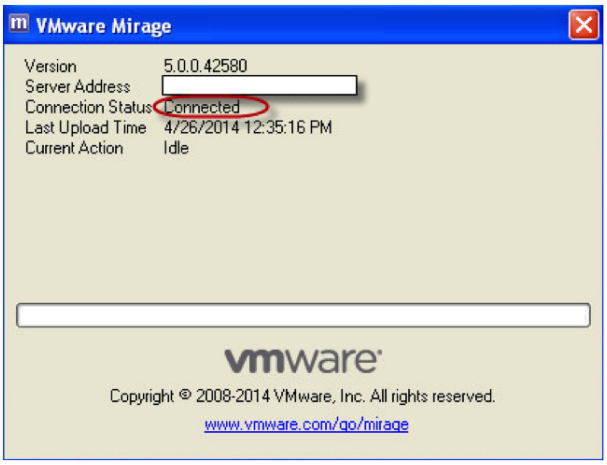


Figure 12: Migration Doesn't Start on Client

Cause

The space on the Windows XP endpoint is insufficient to store the old Windows XP desktop, the new Windows 7 base layer, the old Windows XP personalization, and the new Windows 7 user data and settings. An error message flashes on the Windows XP endpoint, but it is not persistent.

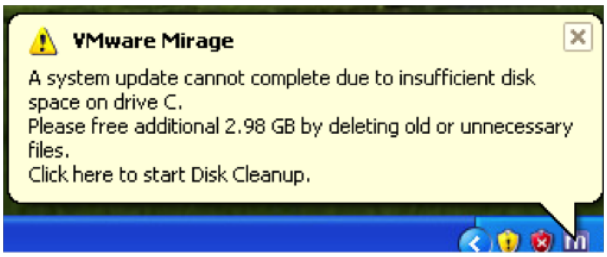
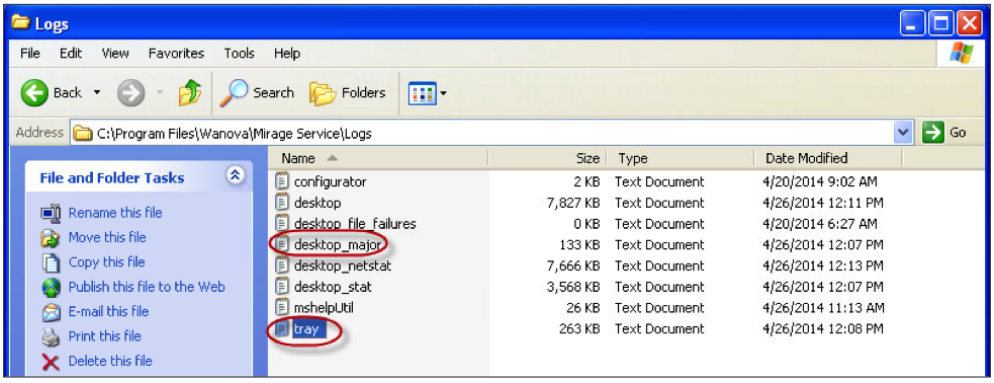


Figure 13: Error Message for Insufficient Disk Space

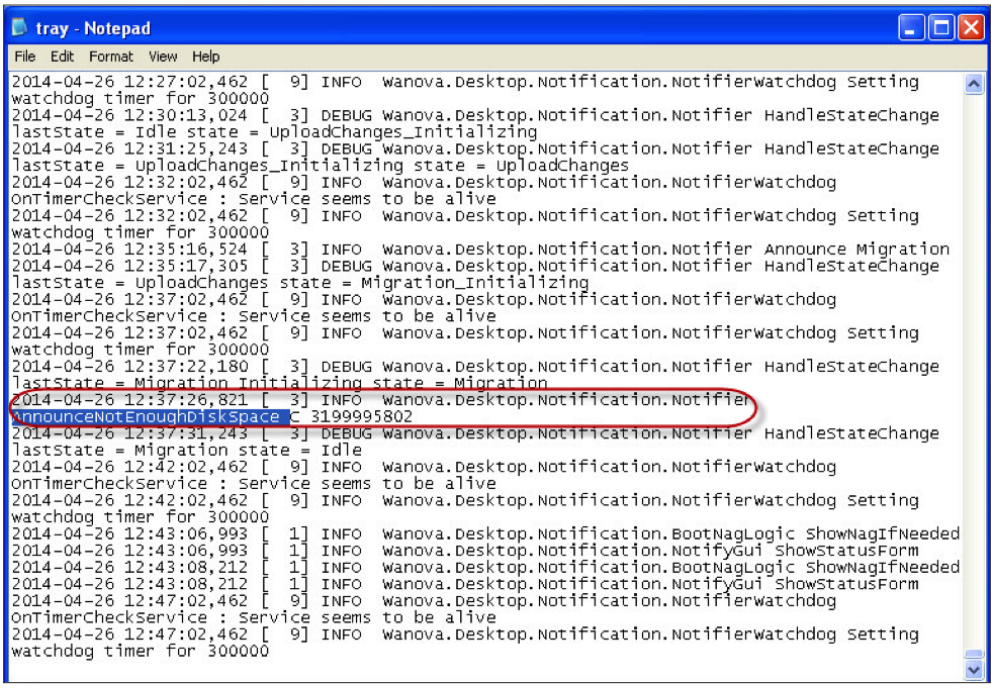
You can confirm that the Windows XP endpoint does not have enough space by examining the Mirage logs.

1. On the Windows XP endpoint, navigate to `C:\Program Files\Wanova\Mirage Service\Logs`.



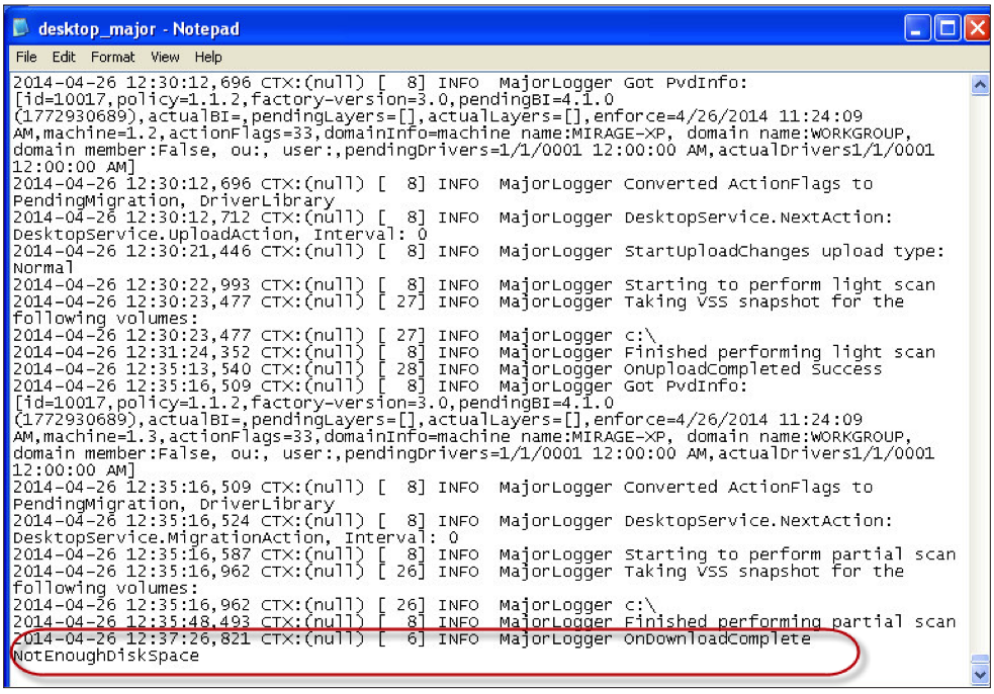
2. Double-click **tray**.

   In the tray log, the notification indicates that not enough disk space was available on the Windows XP endpoint.



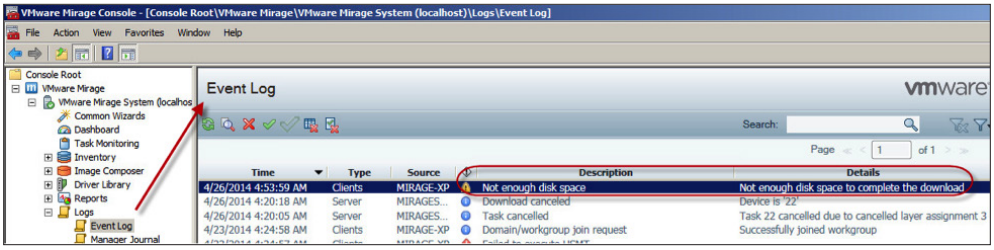
3. Double-click **desktop_major**.

   The desktop major log issues a similar message.



4. In the left pane of the Mirage Console, expand **Logs** and click **Event Log**.

   Under Description, Not enough disk space is listed. The Source value indicates that the endpoint did not migrate to Windows 7.



Resolution

Increase the size of the Windows XP endpoint and try the migration again, including all setup steps.

New Windows 7 Endpoint Disconnected After Migration

The Mirage system tray icon has an *X* flag. When you double-click the system tray icon, the Connection Status value in the detail window is Disconnected.

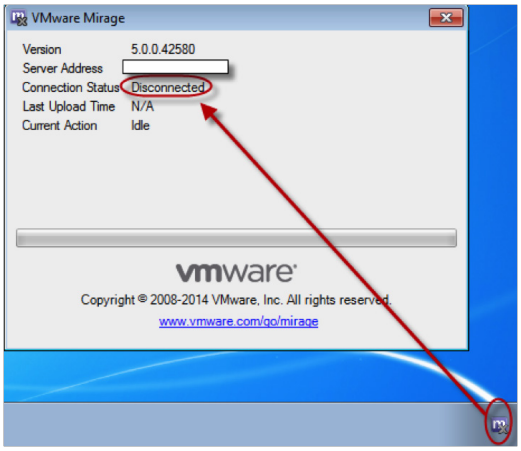


Figure 14: Endpoint Is Disconnected and Cannot Proceed with Migration

The network system tray icon echoes the disconnected state.

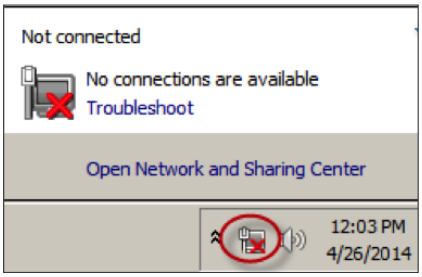


Figure 15: Network System Tray Icon Showing Disconnected Network

In addition, various panes of the Mirage Console do not indicate that the migration completed. For example:

- Expand **Inventory** and click **All CVDs**. For the prior Windows XP CVD, the Activity value persists as Pending Reboot after the second reboot finishes, although the Progress value is 100%.

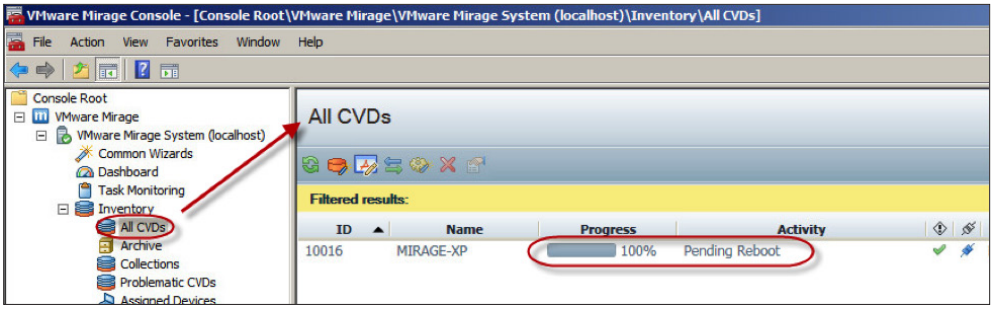


Figure 16: All CVDs Shows 100% Complete in the Migration but Pending Reboot

• On the Task Monitoring page, the Migration task has a Status value of In Progress and a Progress value of 0%.

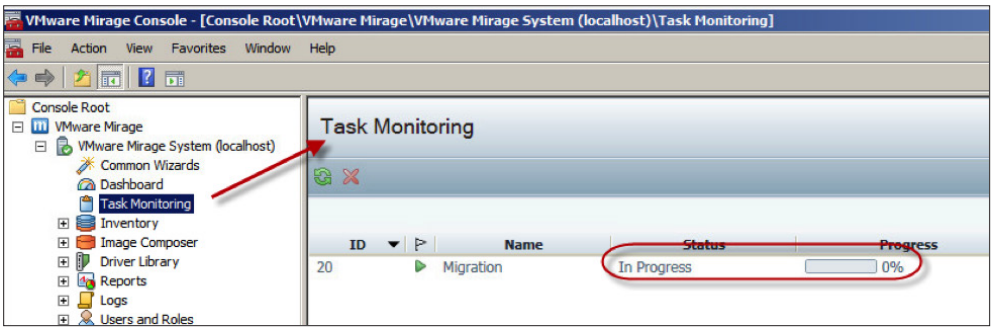


Figure 17: Task Monitoring Showing Migration Not Complete

• On the Layer Assignments page, Assign Base Layer assignment has a Status value of Downloading (0%).

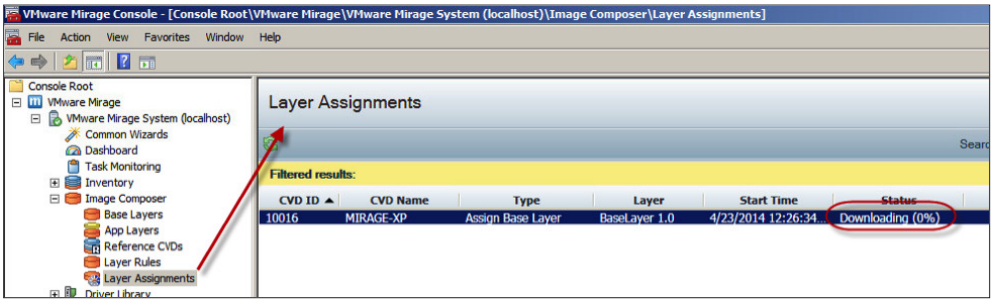


Figure 18: Layer Assignments Showing Migration Not Complete

Mirage cannot complete the migration to Windows 7 if the endpoint is disconnected from the network after the migration.

Cause

This problem occurs when you are migrating from a Windows XP virtual machine to a Windows 7 virtual machine. Windows XP virtual machines and Windows 7 virtual machines have different network adapters, causing the migrating endpoint to lose network connectivity.

Resolution

You need to manually change the network adapter.

1. Power off the former Windows XP virtual machine.
2. In the virtual machine settings in vSphere, Fusion, or Workstation, remove the network adapter from the Windows XP virtual machine and add an Ethernet Adapter with Type of E1000.
3. Power on the former Windows XP virtual machine.

The former Windows XP endpoint now has a network Connection Status value of Connected in the details of the system tray icon. Mirage can complete its migration cycle. When fully migrated, the Mirage system tray icon is unflagged, and the Mirage Console panes show completion of the migration.

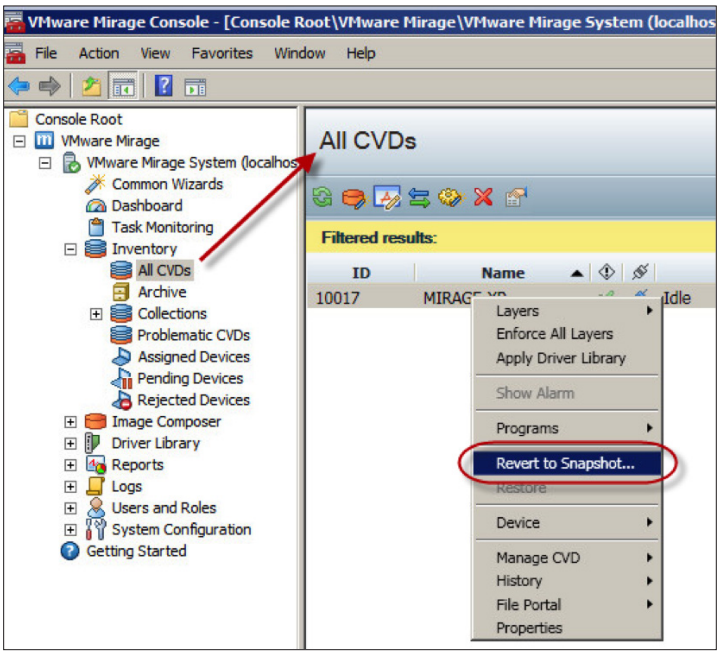
Roll Back a Windows 7 Migration

If you encounter a problem that you cannot resolve during a Windows 7 migration, you can roll back to the previous Windows XP system.

Note: A rollback is possible only when you choose the Mirage Default CVD Policy rather than the Mirage CVD Policy Optimized for View when centralizing the endpoints.

The Mirage Default CVD Policy backs up the endpoint's content to the Mirage server. The Mirage CVD Policy Optimized for View only synchronizes the metadata of your endpoint.

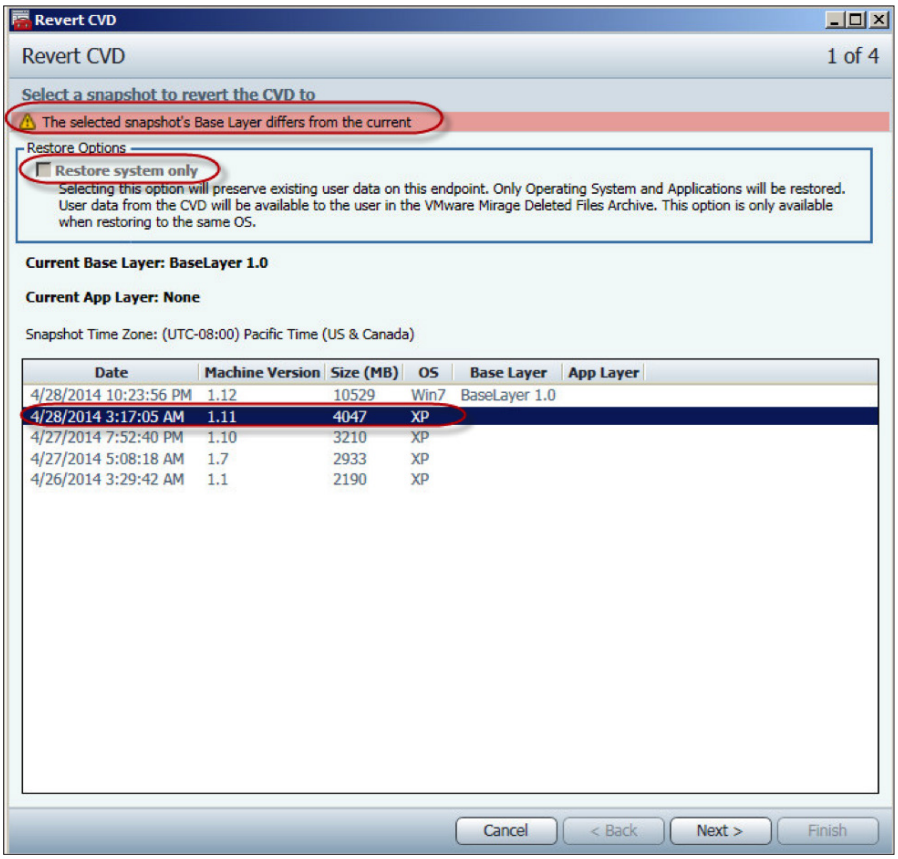
1. In the left pane of the Mirage Console, expand **Inventory** and click **All CVDs**.
2. In the All CVDs pane, right-click the CVD and select **Revert to Snapshot**.



The Revert CVD window appears

3. Deselect the **Restore system only** option.

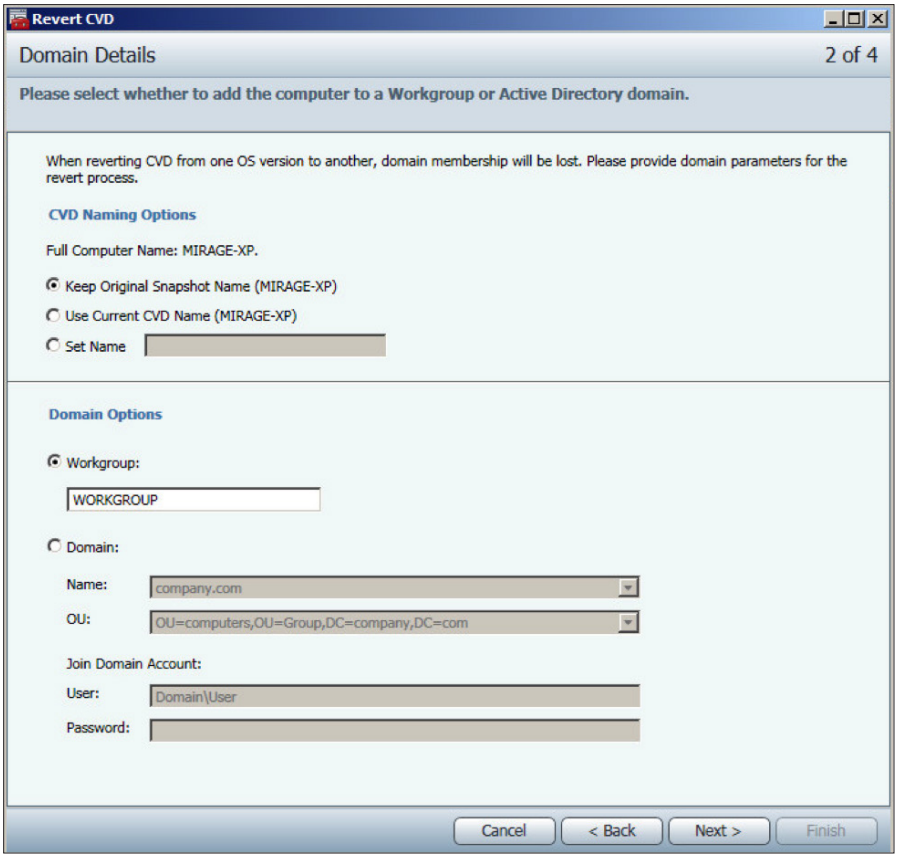
   This option is available only when restoring to the same OS.



4. In the snapshot list, click the snapshot that was taken prior to the migration and click **Next**.

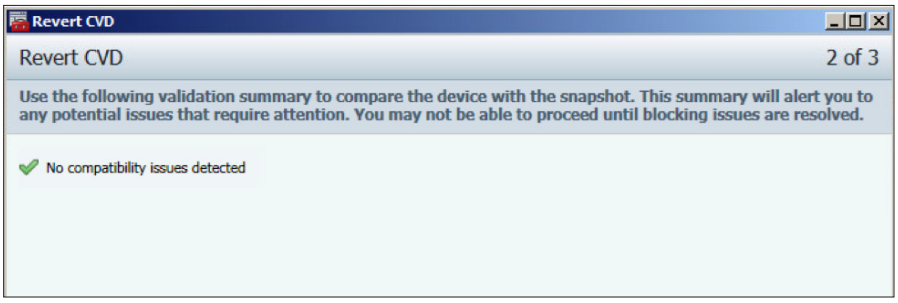
   Ignore the warning message displayed at the top of the page stating that the selected snapshot's base layer differs from the current.

   The Domain Details page appears.



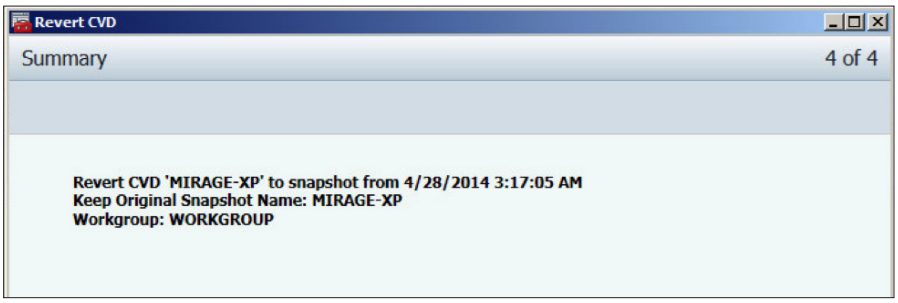
5. Change the settings according to your requirements and click **Next**.

   The page for validation appears.



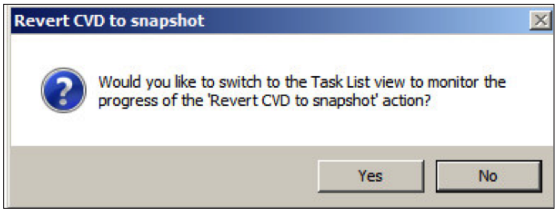
6. Click **Next**.

   The Summary page appears.



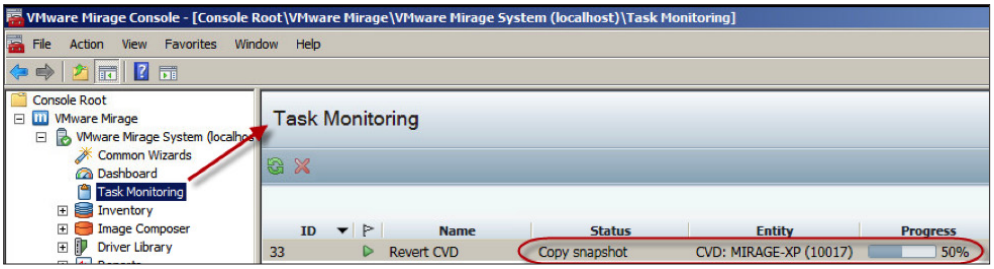
7. Click **Finish**.

   The Revert CVD to snapshot dialog box appears.



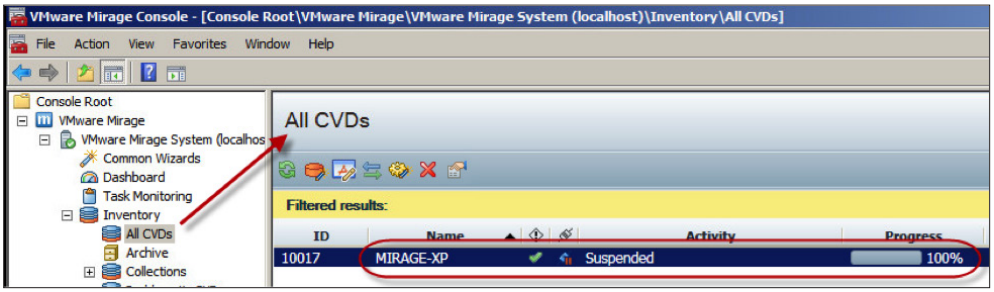
8. Click **Yes**.

   The Mirage Console switches to the Task Monitoring page. The Revert CVD task is listed. The Status value is Copy snapshot.

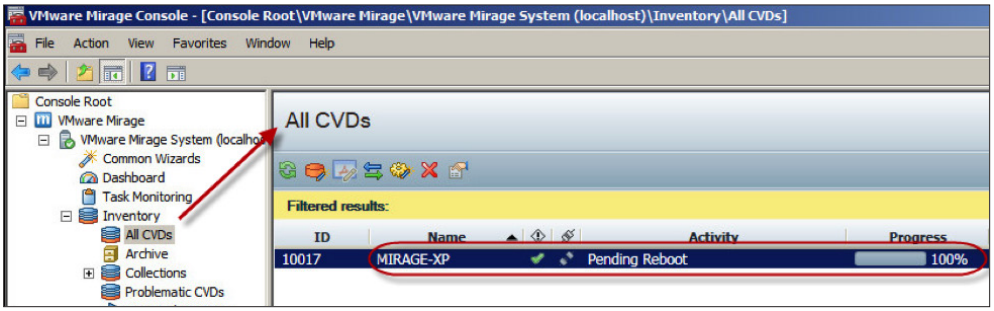


9. Expand **Inventory**, and click **All CVDs**.

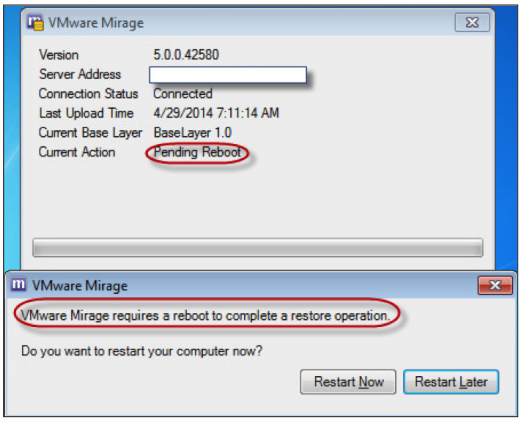
10. In the All CVDs pane, monitor the Activity and Progress values.



As you monitor progress, the Progress value increases until it reaches 100%. The Activity value changes from Suspended to Pending Reboot.

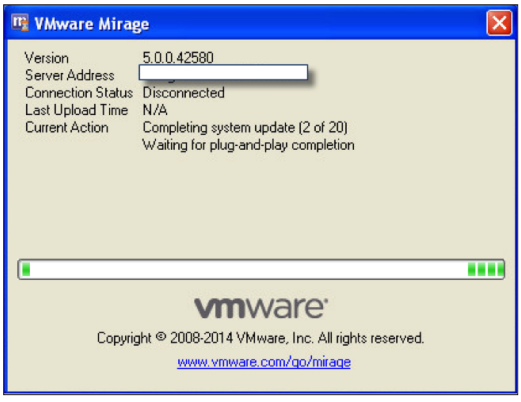


11. Access the endpoint and double-click the Mirage icon to verify that the Current Action value in the VMware Mirage dialog box is Pending Reboot.

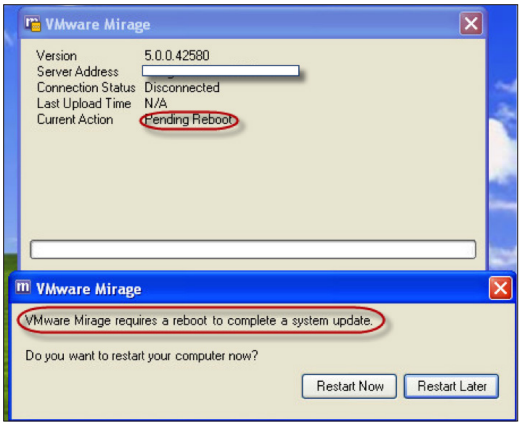


12. Click **Restart Now**.

13. After the endpoint restarts, log in to it again and verify that the Current Action value is Completing system update and the Last Upload Time value is N/A.

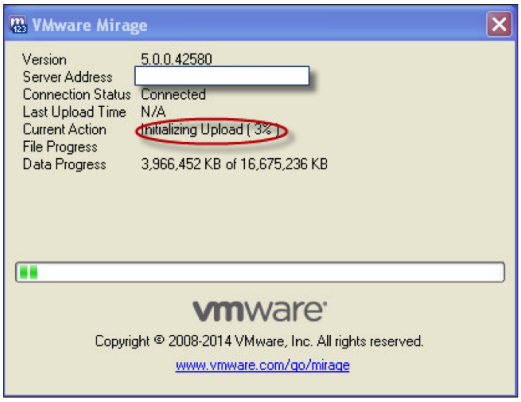


14. After the action finishes, verify that the Current Action value changes to Pending Reboot.

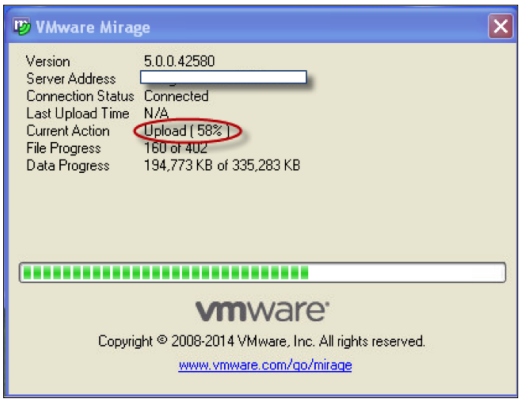


15. Click **Restart Now**.

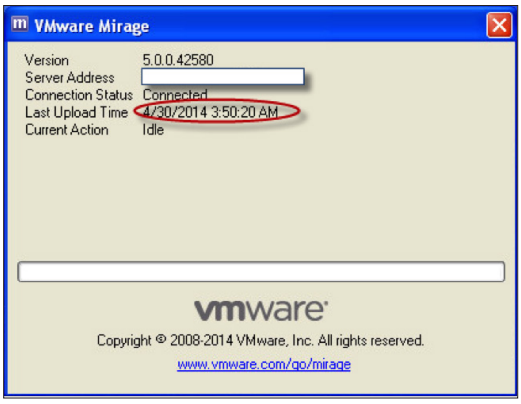
16. After the endpoint restarts, log in to the endpoint again and verify that the Current Action value is Initializing Upload.



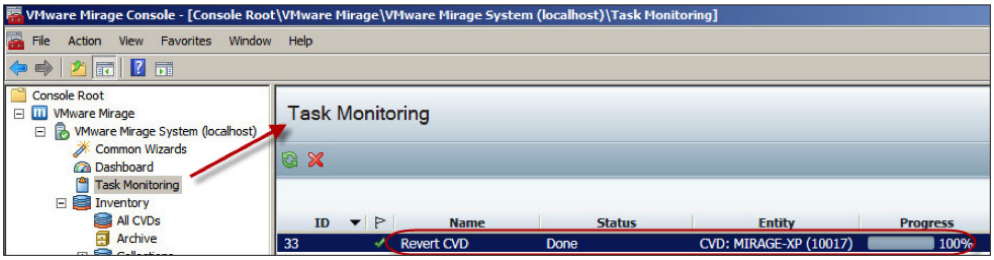
After the initialization finishes, the Current Action value changes to Upload.



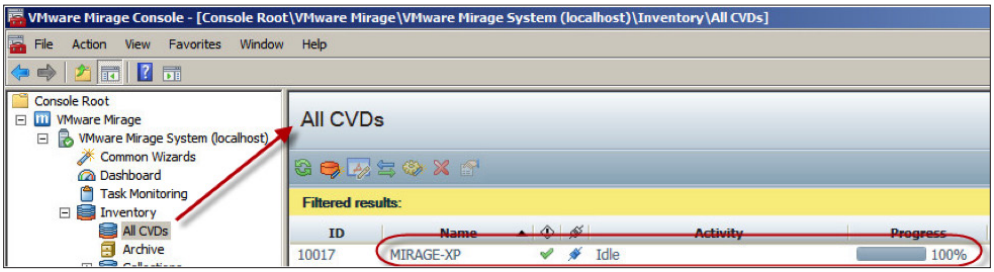
After the upload completes, the Current Action value changes to Idle, and a Last Upload Time value appears.



17. In the left pane of the Mirage Console, click **Task Monitoring**, and in the right pane, verify that the Revert CVD task has a Status value of Done.



18. Go to the All CVDs page and verify that the Activity value for the CVD is Idle.



You have successfully rolled back the system to Windows XP.

Working with Base and Application Layers

After centralizing the endpoints, you can manage your endpoints by assigning a base layer and updating the application layers.

Assigning a Base Layer

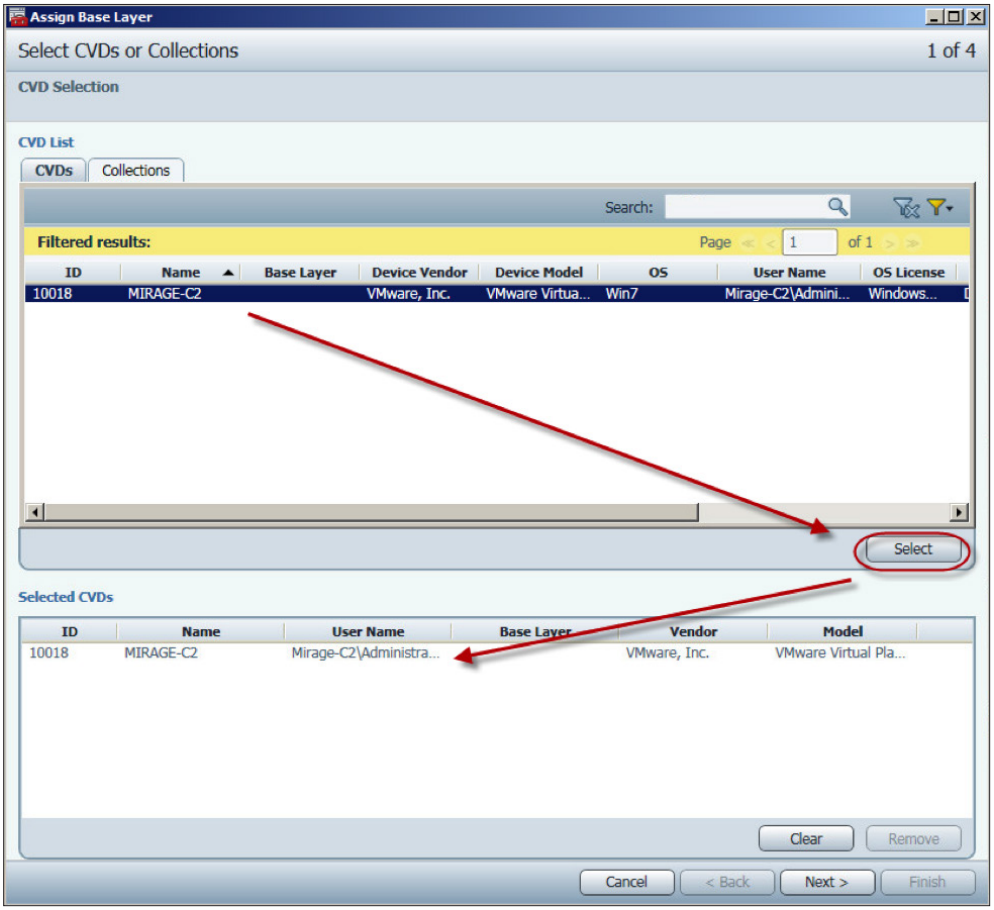
To manage your endpoints, one of the tasks is to assign a base layer. For example, you might need to send an updated base layer to your endpoints if you have applied a patch. Perform the following tasks to assign a base layer.

Assign a Base Layer

You assign a base layer using the Assign Base Layer wizard.

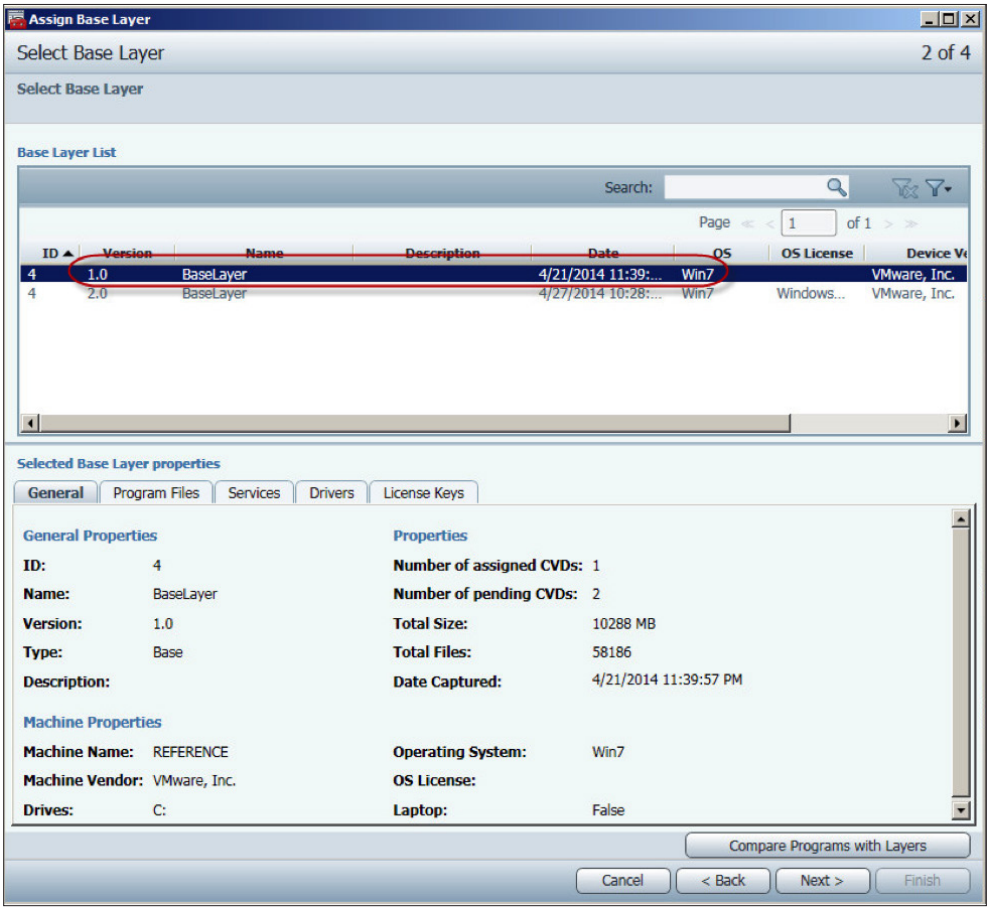
1. In the left pane of the Mirage Console, click **Common Wizards**, and in the right pane, click **Assign Base Layer**.

The Select CVDs or Collections page appears.



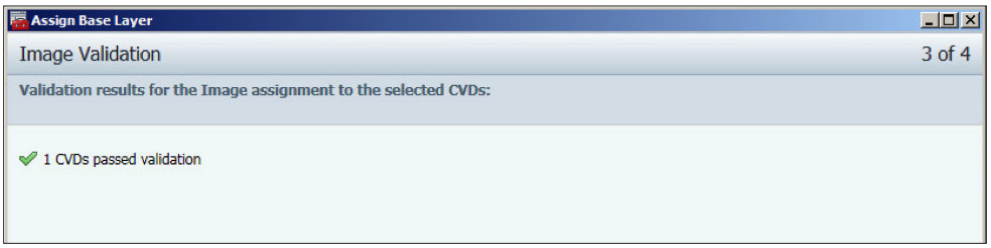
2. Select the endpoints and click **Next**.

The Select Base Layer page appears.



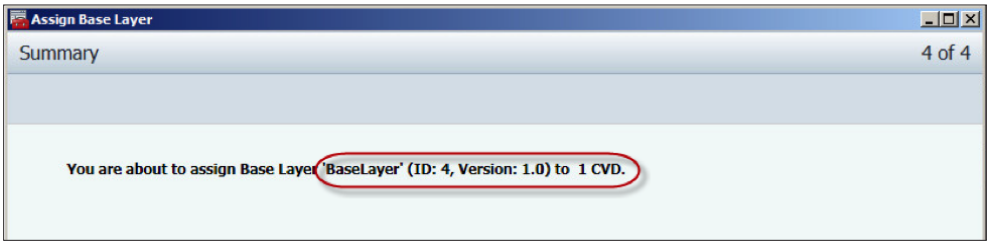
3. Select a base layer and click **Next**.

The Image Validation page appears.



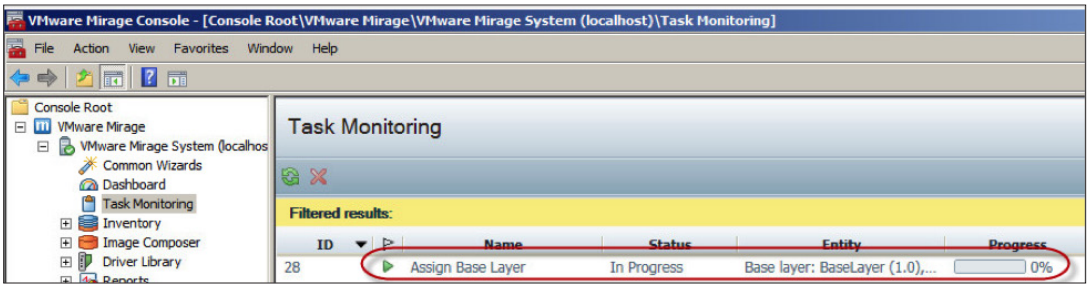
4. Click **Next**.

   The Summary page appears with the selected base layer listed.



5. Click **Finish**.
6. In the left pane, click **Task Monitoring**, and in the right pane, verify that the task has started.

   A Status value of In Progress indicates that the task has started.



What to Do Next

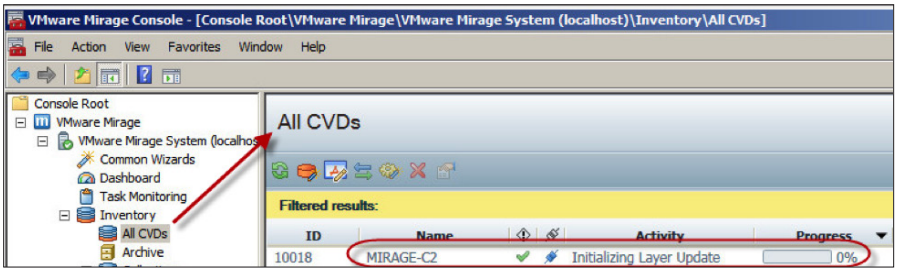
Monitor the progress of the task using either of the following methods:

- Mirage Console
- Endpoint

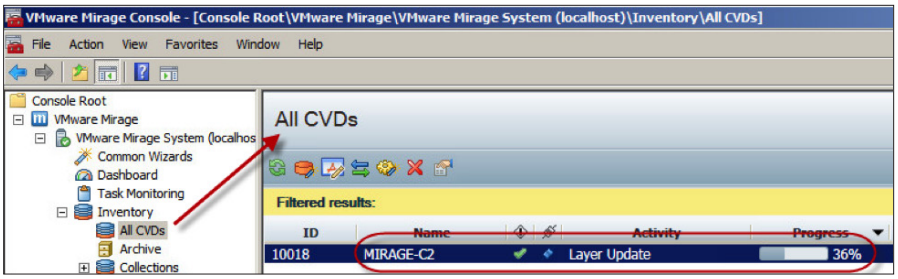
Use the Mirage Console to Monitor the Base Layer Assignment
The Mirage Console shows you the progress of the Assign Base Layer task.

1. In the left pane, expand **Inventory** and click **All CVDs**.
2. Monitor the progress in the All CVDs pane.

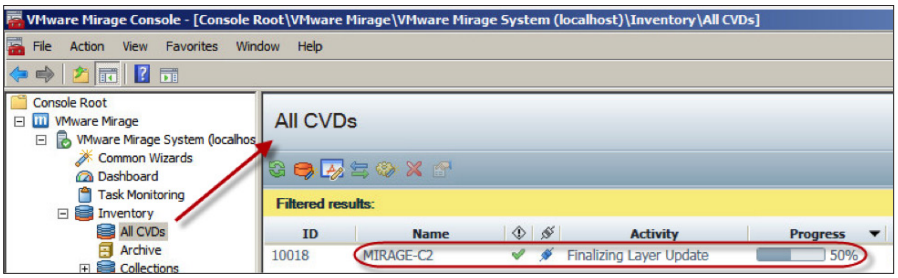
   Initially, the Activity value is Initializing Layer Update.



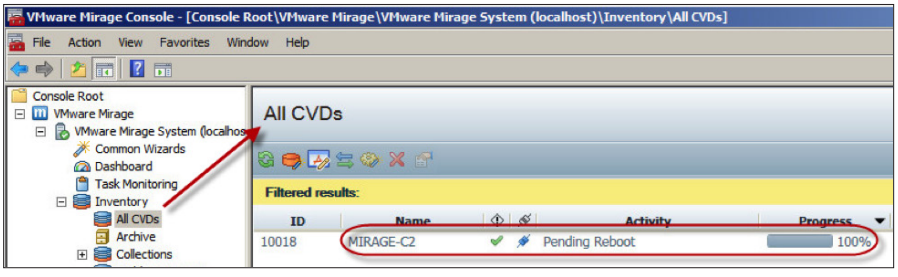
   When the initialization finishes, the Activity value changes to Layer Update.



   After the update finishes, the Activity value changes to Finalizing Layer Update.



   As the progress continues, the Activity value changes to Pending Reboot.

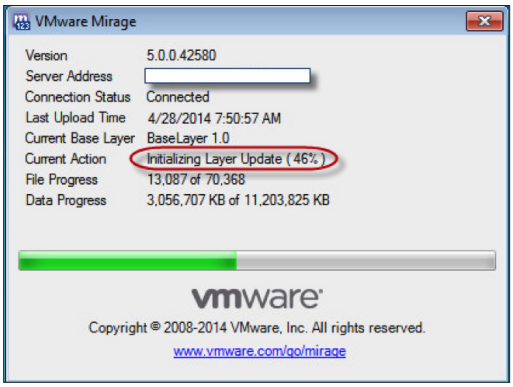


3. Access the endpoint, and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.

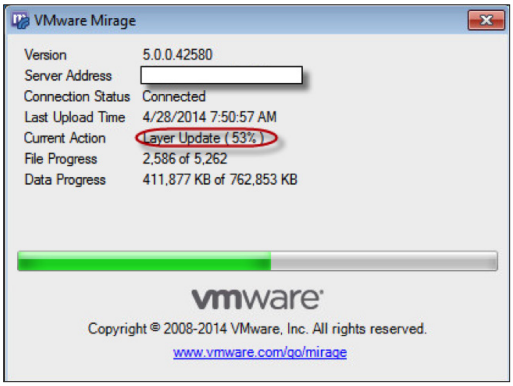
To complete the base layer assignment, restart the endpoint.

Use the Endpoint to Monitor the Base Layer Assignment
You can monitor the Assign Base Layer task on the endpoint.

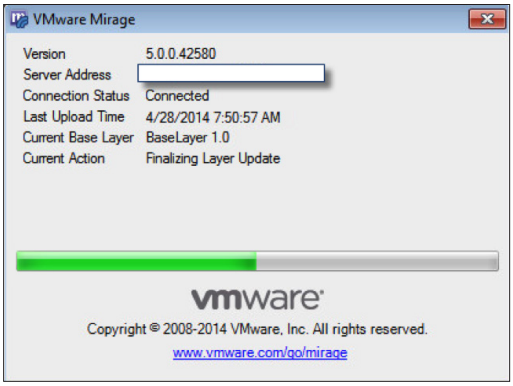
1. Access the endpoint, and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.
2. Monitor the progress.



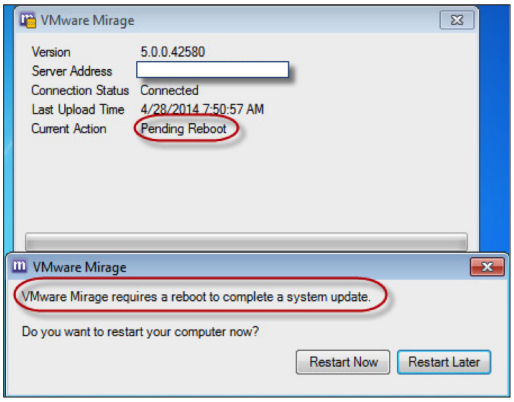
After the initialization, the Current Action value changes to Layer Update.



After the update completes, the Current Action value changes to Finalizing Layer Update.



After the finalization, you are prompted to reboot the endpoint.

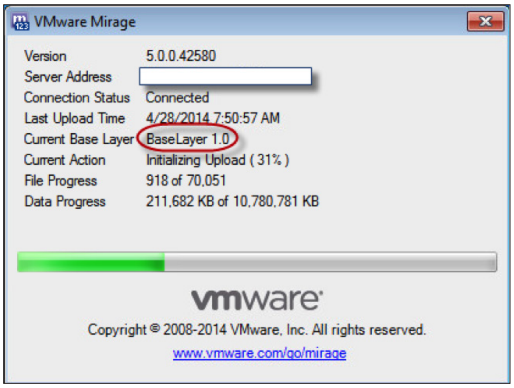


Restart the Endpoint to Complete the Base Layer Assignment

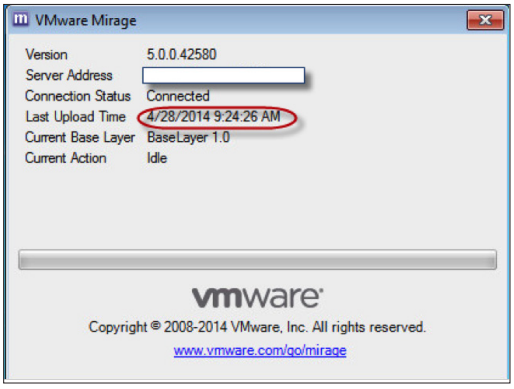
When you are finished monitoring the Assign Base Layer task, you must restart the endpoint.

1. In the VMware Mirage dialog box of the endpoint, click **Restart Now**.
2. Log in to the endpoint again.

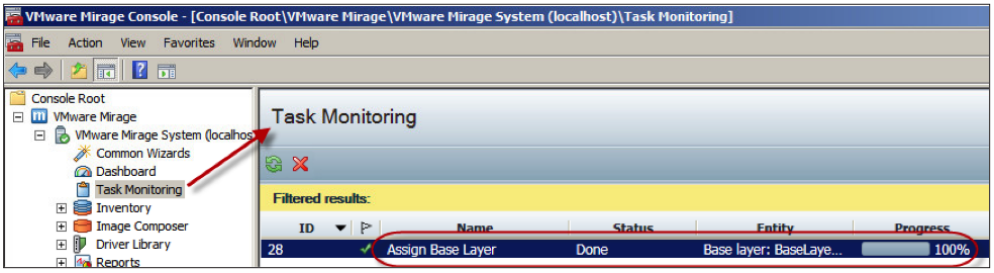
   The Current Base Layer value is the base layer you selected.



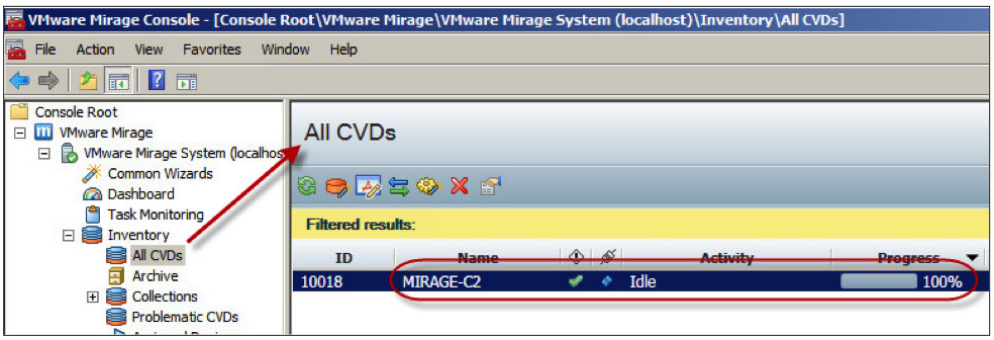
After the upload finishes, the Current Action value changes back to Idle, and the Last Upload Time value is updated.



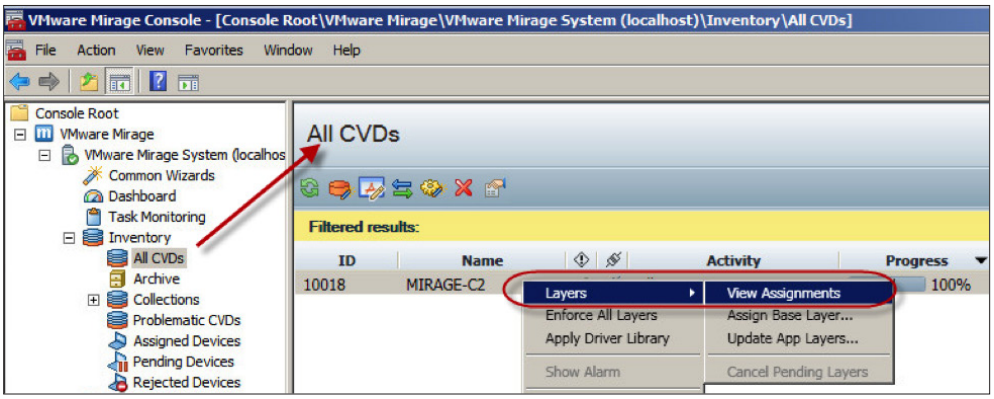
3. In the left pane of the Mirage Console click **Task Monitoring**.
4. In the Task Monitoring page, verify that the Progress value for Assign Base Layer task is 100%, and the Status value changes to Done.



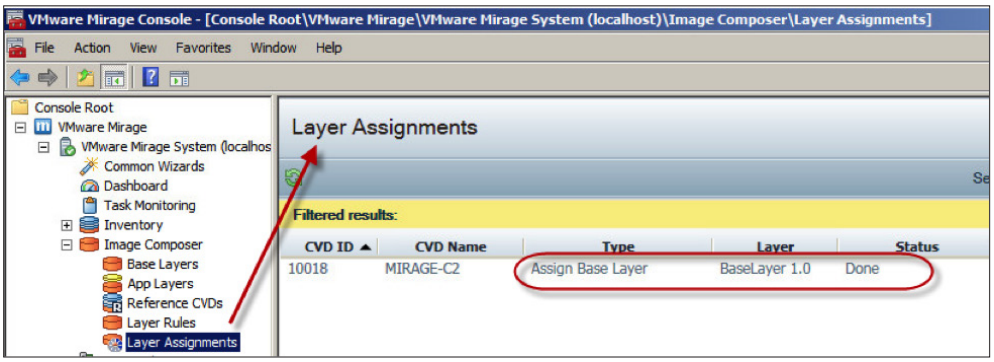
5. In the left pane, expand **Inventory** and click **All CVDs**.
6. In the All CVDs pane, verify that the Progress value is 100%, and the Activity value is Idle.



7. Right-click the CVD and select **Layers** > **View Assignments**.



The Mirage Console switches to the Layer Assignment page and lists the assignments. The Type value is Assign Base Layer, the Layer value is the layer you selected, and the Status value is Done.



You now have assigned the base layer to the CVD.

Updating Application Layers

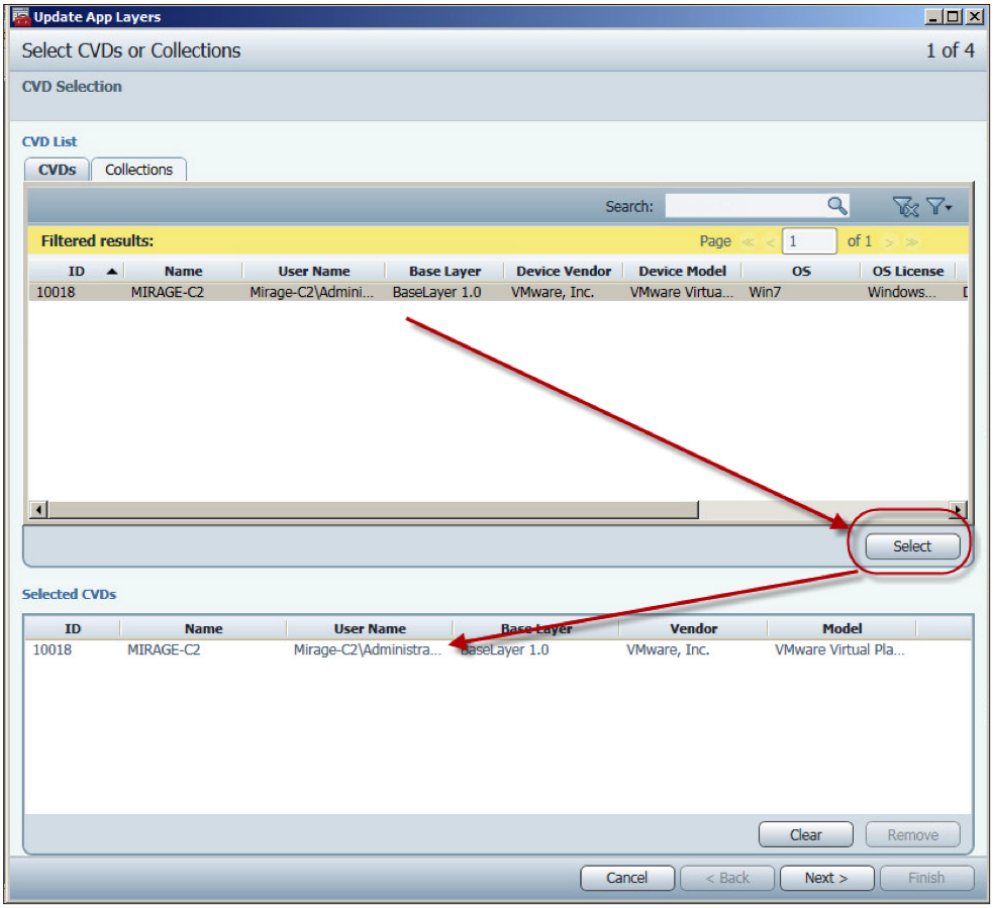
You can deploy updates or add applications to the endpoints by updating the application layer.

Update App Layers

You update an application layer using the Update App Layers wizard.

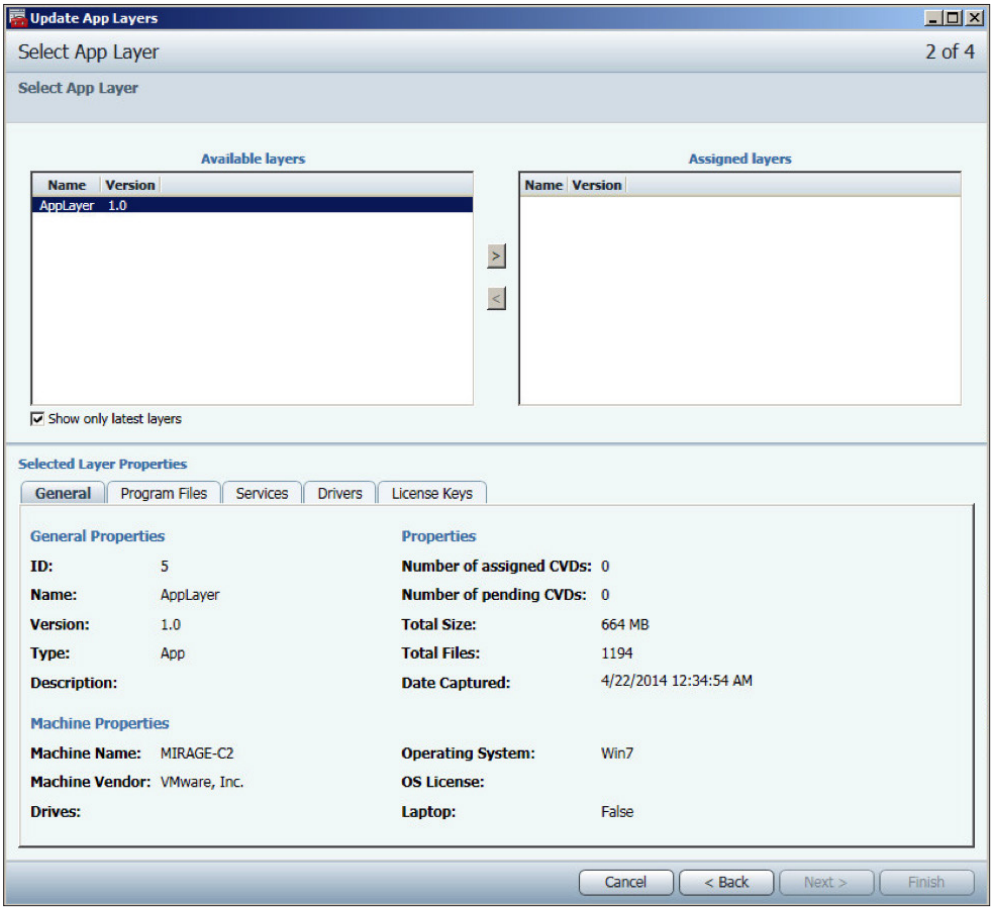
1. In the left pane of the Mirage Console, click **Common Wizards**, and in the right pane, click **Update App Layers**.

The Select CVDs or Collections page appears.

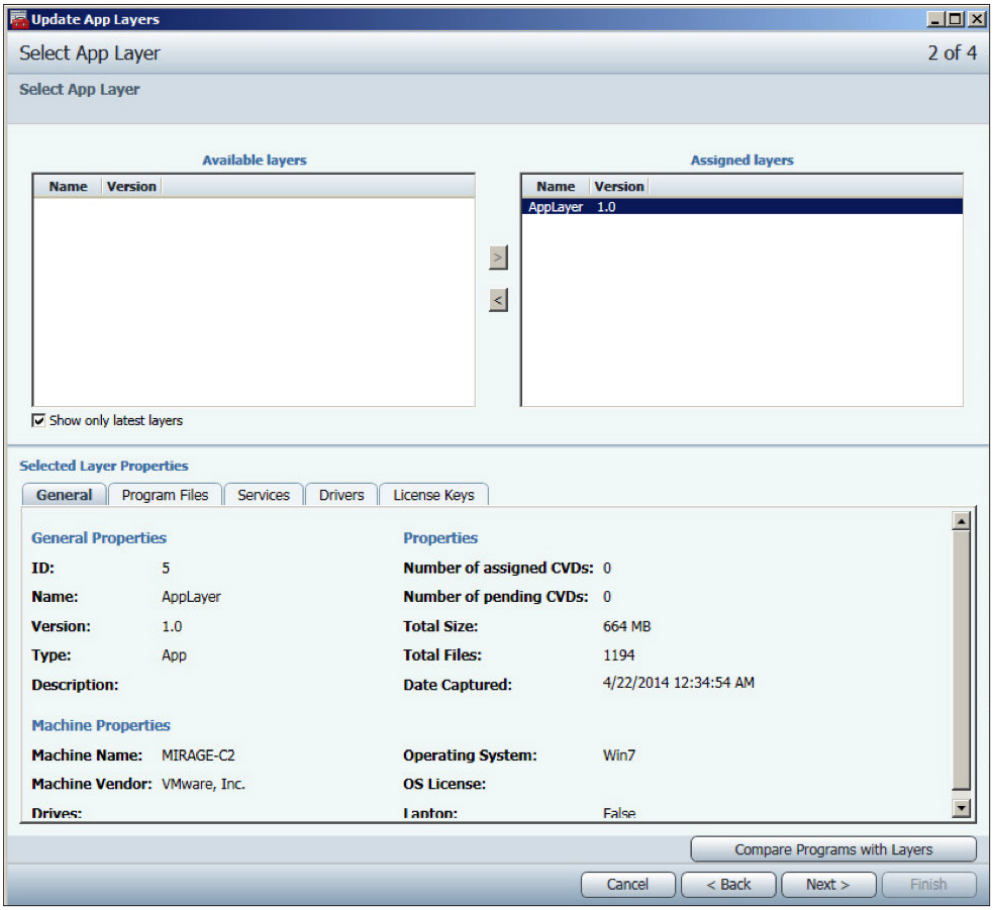


2. Select the CVD and click **Next**.

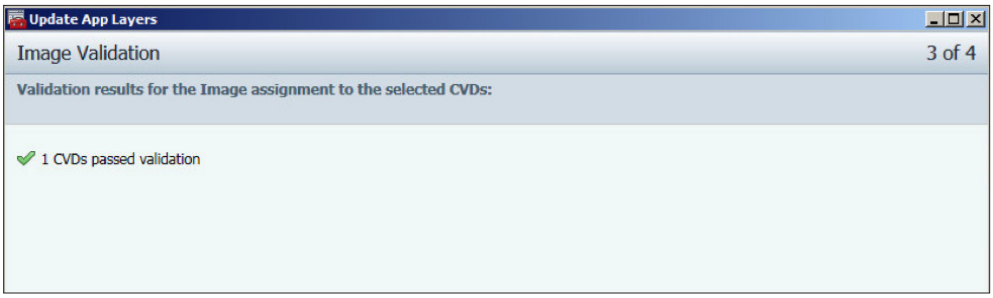
The Select App Layer page appears.



3. Select the app layers you want to update and click **Next**.

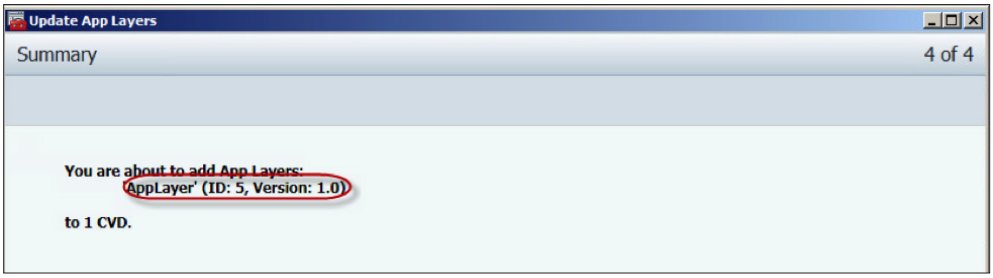


The Image Validation page appears.



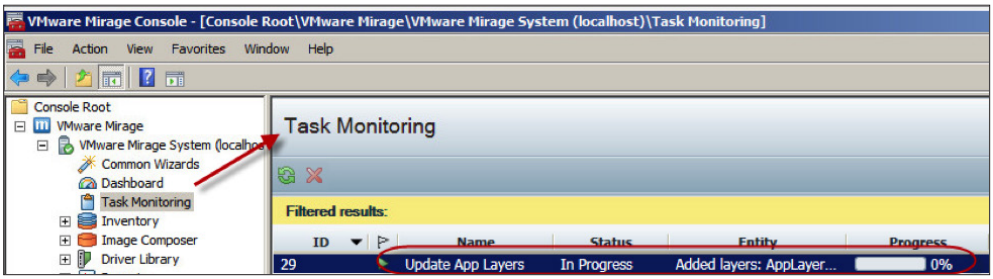
4. Click **Next**.

   The Summary page appears and lists the selected app layer in the summary.



5. Click **Finish**.
6. In the left pane, click **Task Monitoring**, and in the right pane, verify that the task has started.

   A Status value of In Progress indicates that the task has started.



What to Do Next

Monitor the progress of the task using either of the following methods:

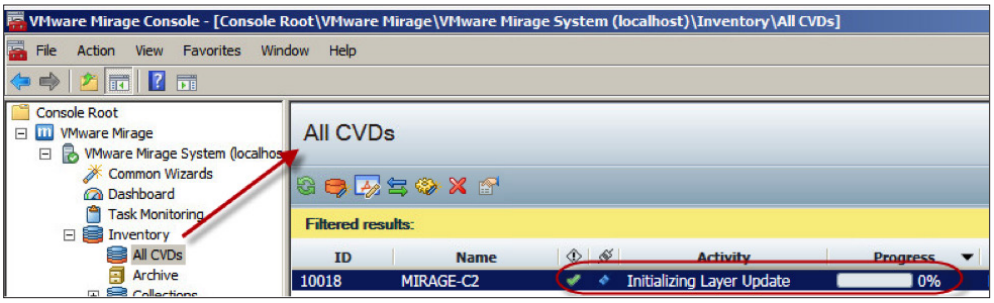
- Mirage Console
- Endpoint

Use the Mirage Console to Monitor the App Layer Update

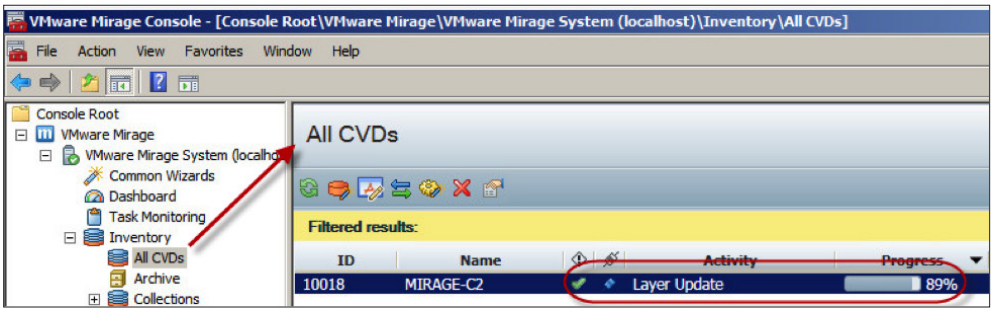
The Mirage Console shows you the progress of the Update App Layers task.

1. In the left pane, expand **Inventory** and click **All CVDs**.
2. Monitor the progress in the All CVDs pane.

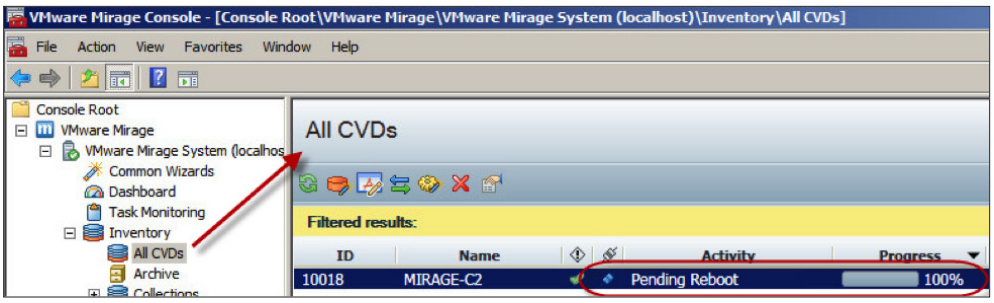
   At first, the Activity value is Initializing Layer Update.



   As the progress continues, the Activity value changes to Layer Update.



   As you monitor the progress, the Progress value reaches 100%, and the Activity value changes to Pending Reboot.



3. Access the endpoint, and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.

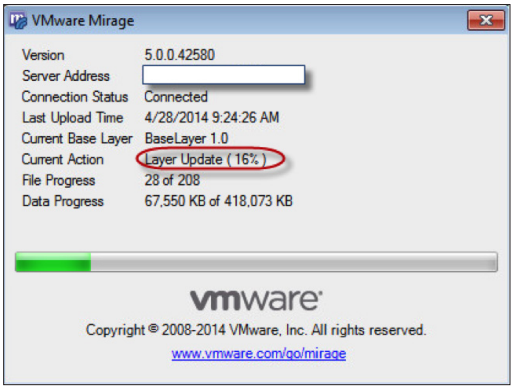
To complete the app layer update, restart the endpoint.

Use the Endpoint to Monitor the App Layer Update

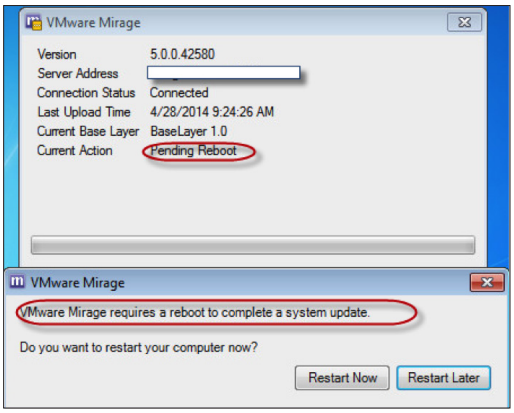
You can monitor the Update App Layers task on the endpoint.

1. Access the endpoint, and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.
2. Monitor the progress.

   At first, the Current Action value is Layer Update.



After the update finishes, the Current Action value changes to Pending Reboot. You are prompted to reboot the endpoint.

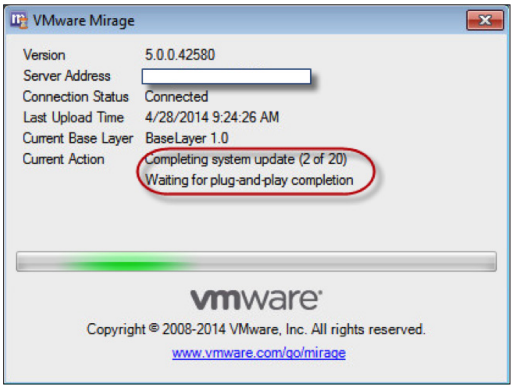


Restart the Endpoint to Complete the App Layer Update

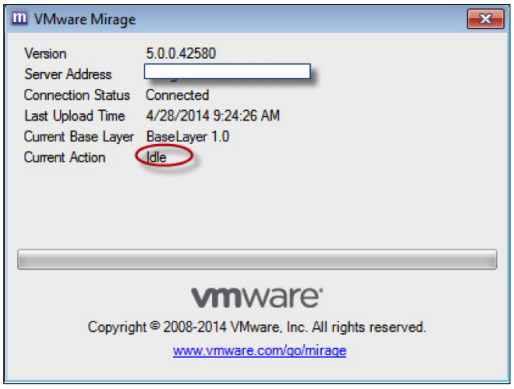
When you are finished monitoring the Update App Layers task, you must restart the endpoint.

1. In the VMware Mirage dialog box of the endpoint, click **Restart Now**.
2. Log in to the endpoint again.

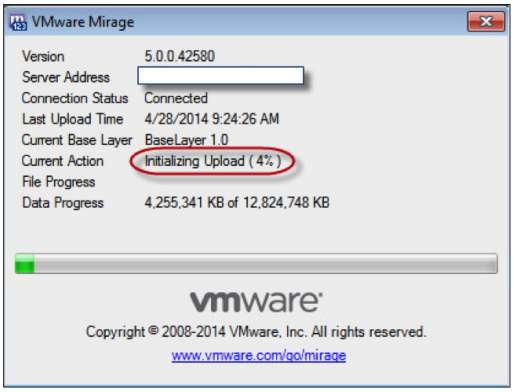
   The Current Action value changes to Completing system update.



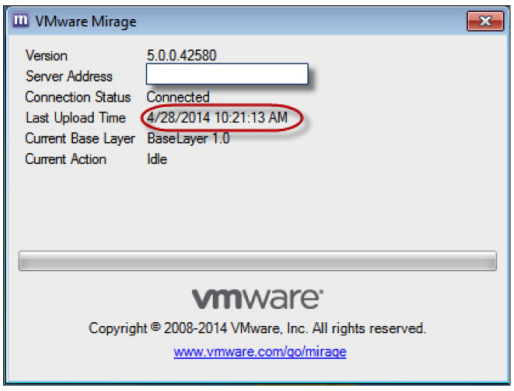
After the system update finishes, the Current Action value changes to Idle.



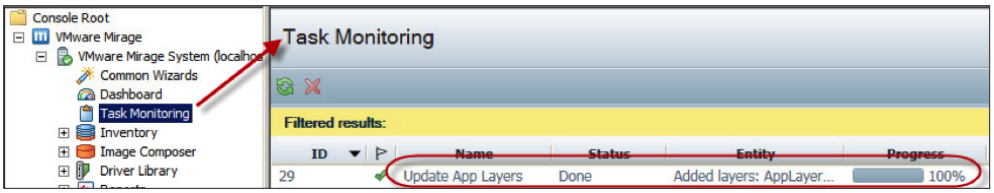
In a few minutes, the client starts to initialize an upload. The Current Action value changes to Initializing Upload.



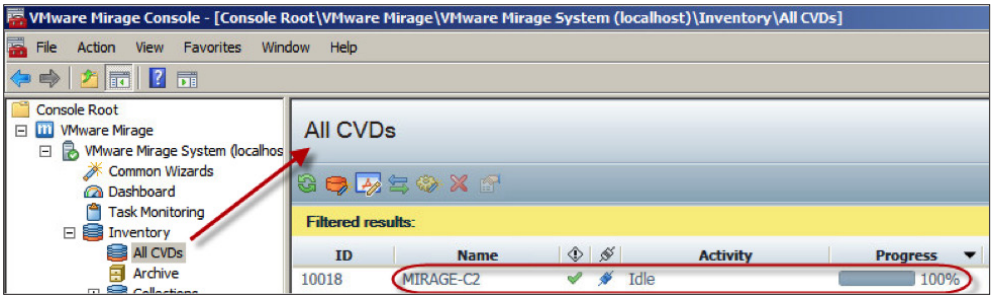
When the upload completes, the Last Upload Time value changes, and the Current Action value changes to Idle.



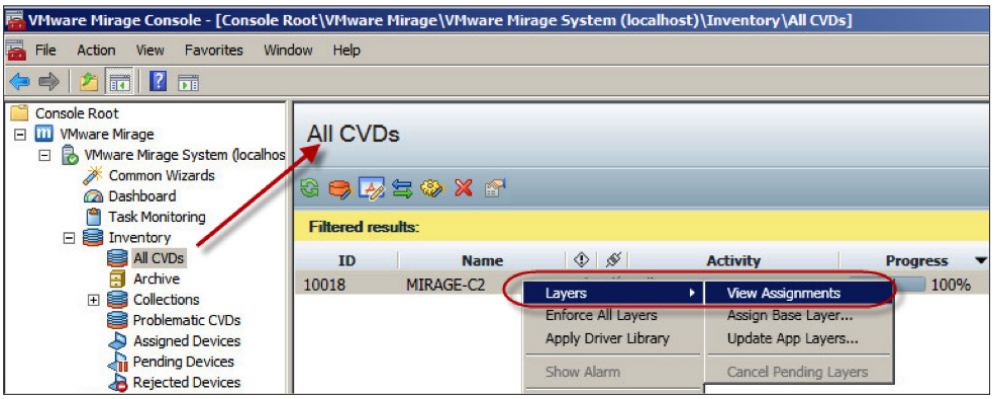
3. In the left pane of the Mirage Console, click **Task Monitoring**.
4. In the Task Monitoring page, verify that the Progress value for the updating app layer reaches 100%, and the Status value changes to Done.



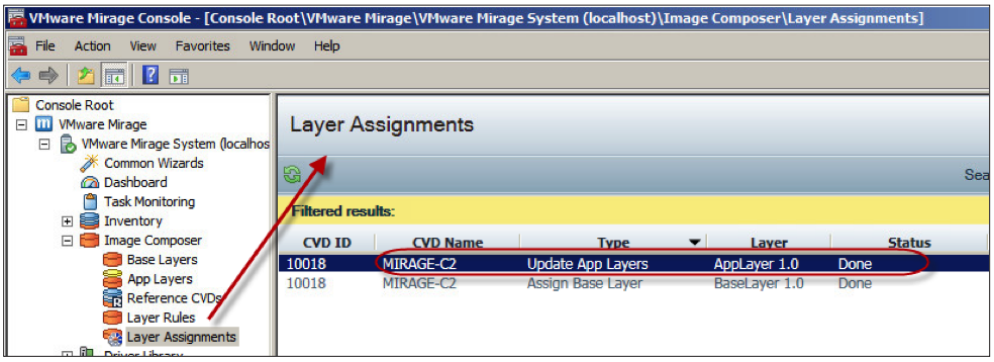
5. In the left pane, expand **Inventory** and click **All CVDs**.
6. In the All CVDs pane, verify that the Progress value of the updating CVD is 100%, and the Activity value is Idle.



7. Right-click the CVD and select **Layers** > **View Assignments**.



The Mirage Console switches to the Layer Assignment page and lists the assignments of the updated CVD. The Type value is Update App Layer, the Layer value is the layer you selected, and the Status value is Done.



You have updated the CVD with a new app layer.

Data Recovery and Backup

If a user's computer fails or is missing, you can use Mirage to restore the desktop image to a new or reformatted hard disk or to a replacement endpoint with minimal user downtime.

For more frequent desktop repair scenarios, you can perform a restoration from a previous snapshot of the desktop image. You can restore only the system files or both the system files and the user data. For this kind of desktop repair, you use the Mirage Revert to Snapshot option.

The following table lists supported OS scenarios for restoring a full-system desktop image to a device.

	TO A WINDOWS DEVICE				
FROM A WINDOWS CVD	XP	Vista	7	8.0	8.1 or 8.1 U1
XP	✔	✘	✔	✘	✘
Vista	✘	✔	✔	✘	✘
7	✘	✘	✔	✔	✔
8.0	✘	✘	✘	✔	✘
8.1 or 8.1 U1	✘	✘	✘	✘	✔

Table 8: Supported Operating Systems in Full-System Restore Scenarios

This section contains the following exercises for data recovery:

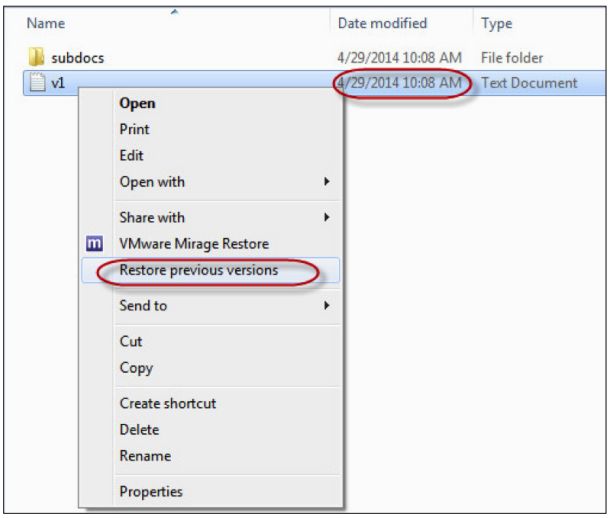
- Restoring a file to a previous version
- Restoring a file or folder from an archive
- Restoring a deleted file or folder
- Enforcing layers
- Reverting a CVD to a Mirage snapshot
- Recovering a failed or missing endpoint

Restore a File to a Previous Version

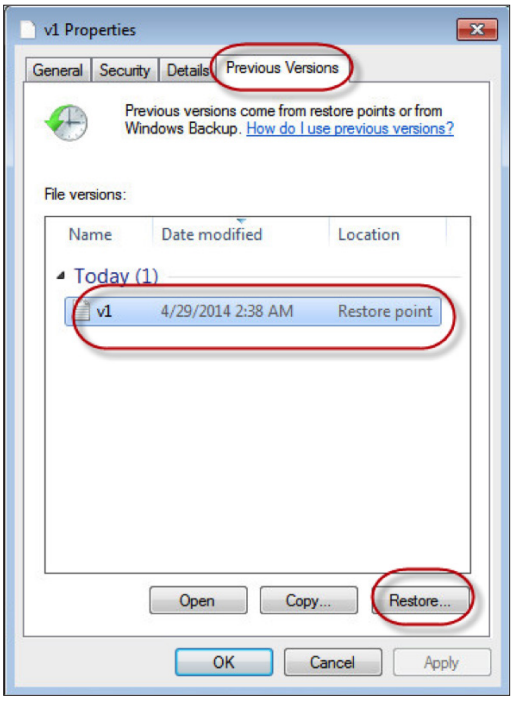
You can restore a file to a previous version.

1. On the endpoint, right-click the file you want to restore and select **Restore previous versions**.

   Note that the most recent date of the file in this example is 4/29/2014 10:08 AM.

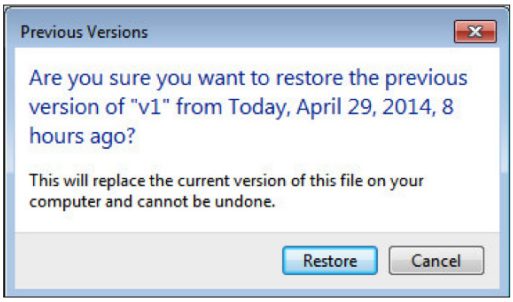


   The Properties dialog box appears. Previous versions are listed with their corresponding modified date and time.



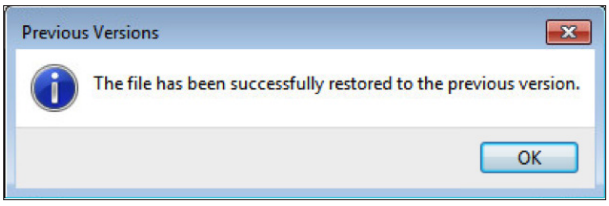
2. Select a version and click **Restore**.

A confirmation dialog box appears.



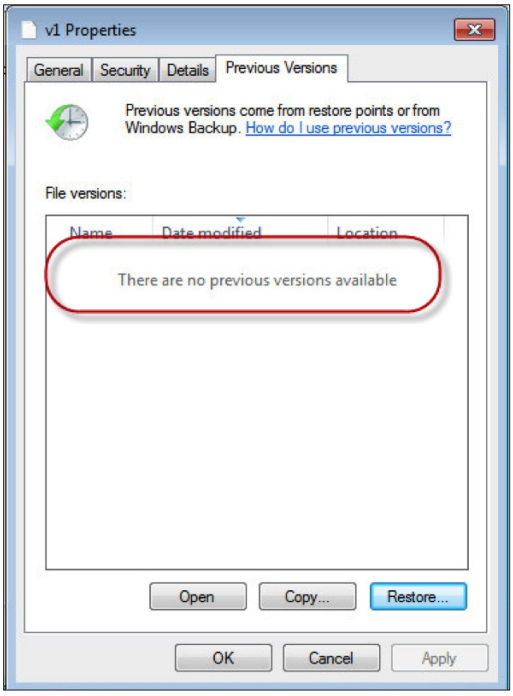
3. Click **Restore**.

   A result dialog box appears.



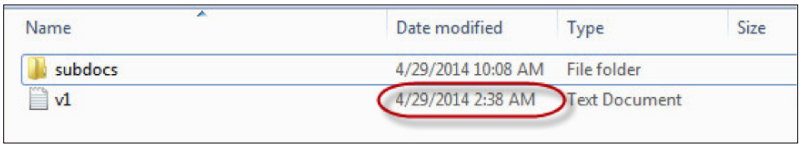
4. Click **OK**.

   The restored version is deleted from the list of file versions.



5. Click **OK**.

The modification time of the file has been reverted to that of the restored version.

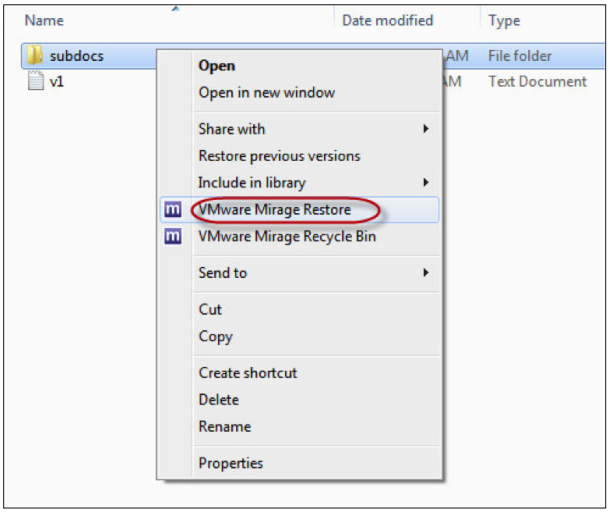


6. Open the file to check the contents.

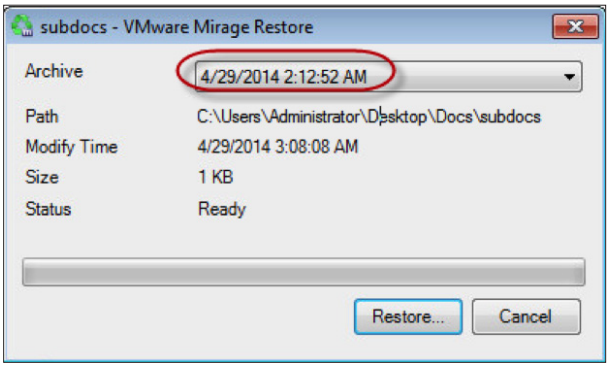
Restore a File or Folder from the Archive

If you want a previous version of a file or folder, you can restore it from an archive of the CVD.

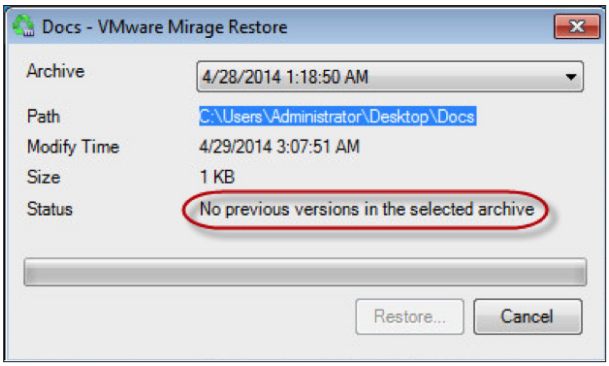
1. On the endpoint, right-click the file you want to restore and select **VMware Mirage Restore**.



The VMware Mirage Restore dialog box appears. The available archives are listed in the drop-down menu.



Note: If you select an archive that does not include the file or folder that you want to restore, the Restore button is dimmed, and the Status value indicates that no previous versions exist in the selected archive.

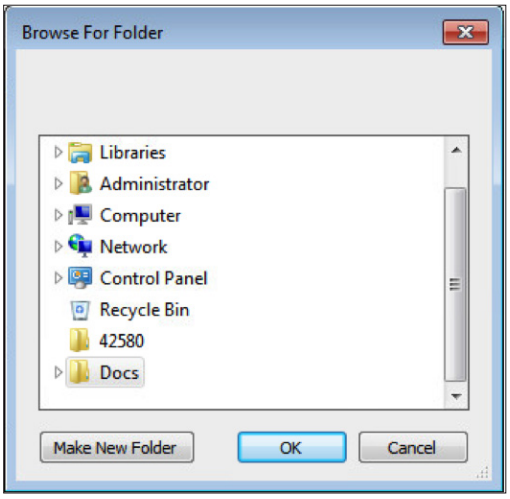


2. Select an archive from the drop-down menu and click **Restore**.

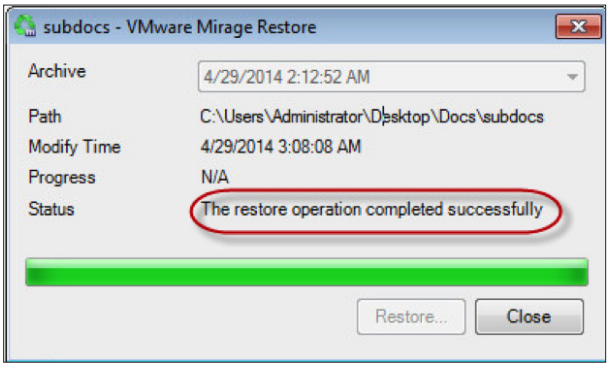
   The Browse For Folder dialog box appears prompting you to select a target folder. The original is selected by default.

   Note: If you choose the original folder, Windows presents a dialog asking whether you want to copy and replace the file or folder.

3. Select a folder and click **OK**.



4. Click **Close**.

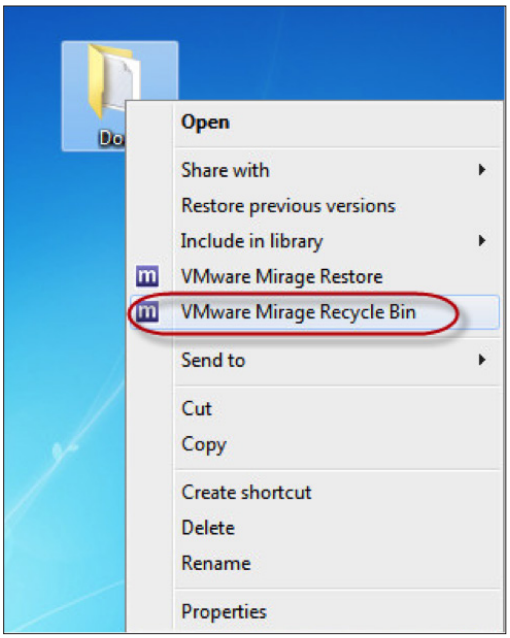


Your file or folder is restored. You can open it to check the contents.

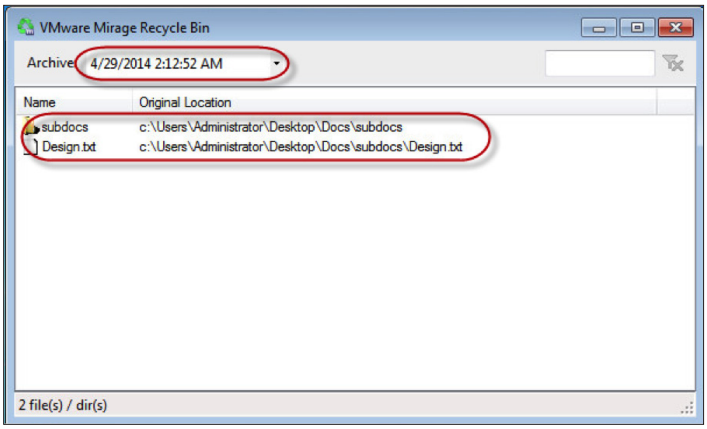
Restore a Deleted File or Folder

If you delete a file or folder, you can get it back from the Mirage Recycle Bin.

1. On the endpoint, right-click the parent folder of the deleted file or folder and select **VMware Mirage Recycle Bin**.



The VMware Mirage Recycle Bin dialog box appears. The available archives are listed in the drop-down menu.

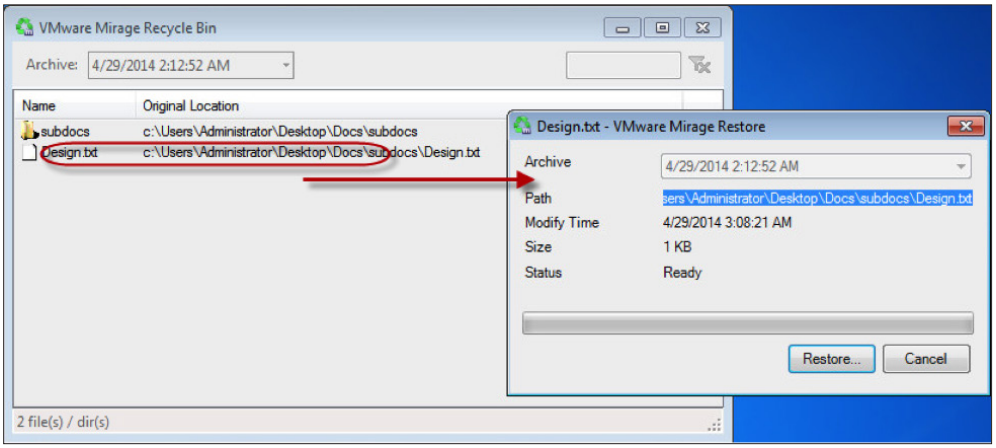


2. Select an archive from the drop-down menu.

   The deleted files and folders in the parent folder are listed.

3. Double-click the file or folder.

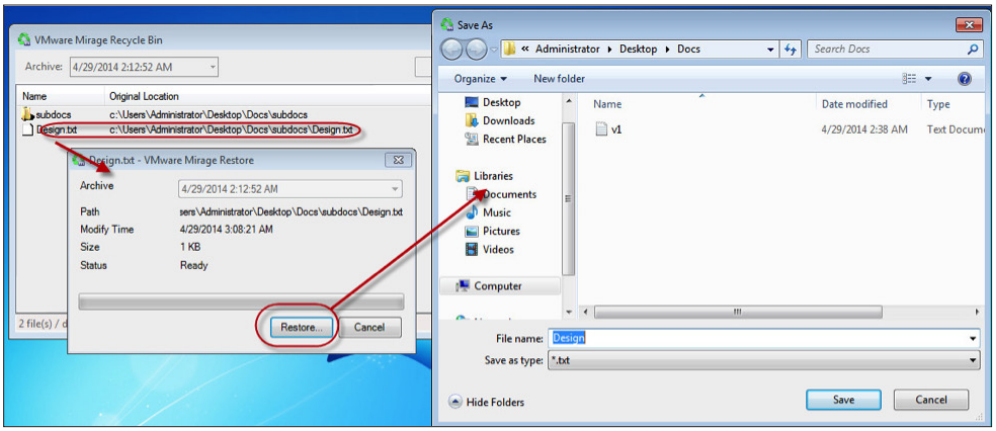
   The VMware Mirage Restore dialog box appears.



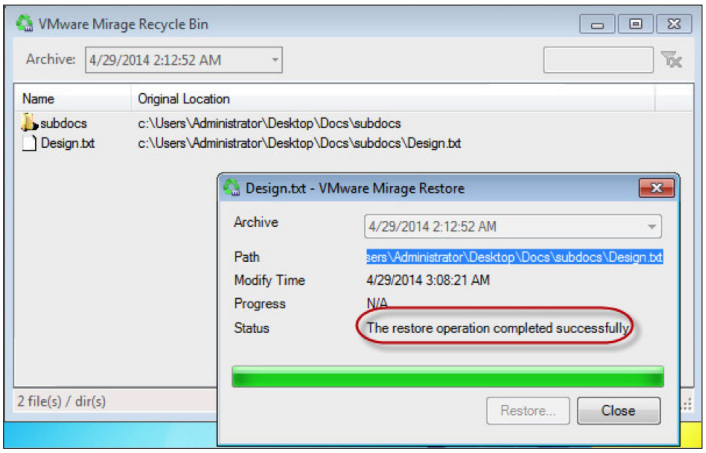
4. Click **Restore**.

The Save As dialog box appears.

5. Navigate to the destination where you want to put the restored file.



6. Click **Save**.



7. Click **Close**.

The deleted file is now restored.

Enforcing Layers

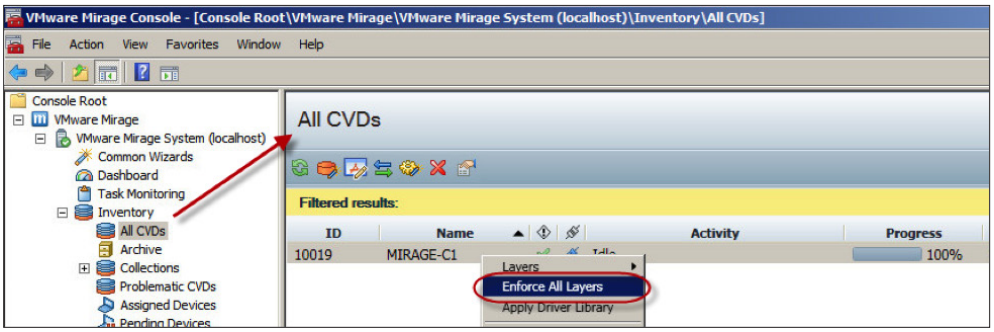
You can make changes to the files and registry settings on an endpoint. These changes might cause problems for applications or the operating system. If problems occur, you can use one of the options of the Enforce All Layers feature to restore the system.

- **Preserve user applications** – This method 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.
- **Remove user applications** – This method removes user-installed applications residing in the machine area of the CVD. Use this method to fix a problematic CVD in which all layer applications do not function because of overwritten or corrupted system files. Removing the user applications deletes machine area files and registry keys that are not in the current base layer, with the exception of the files defined in the user area policy.

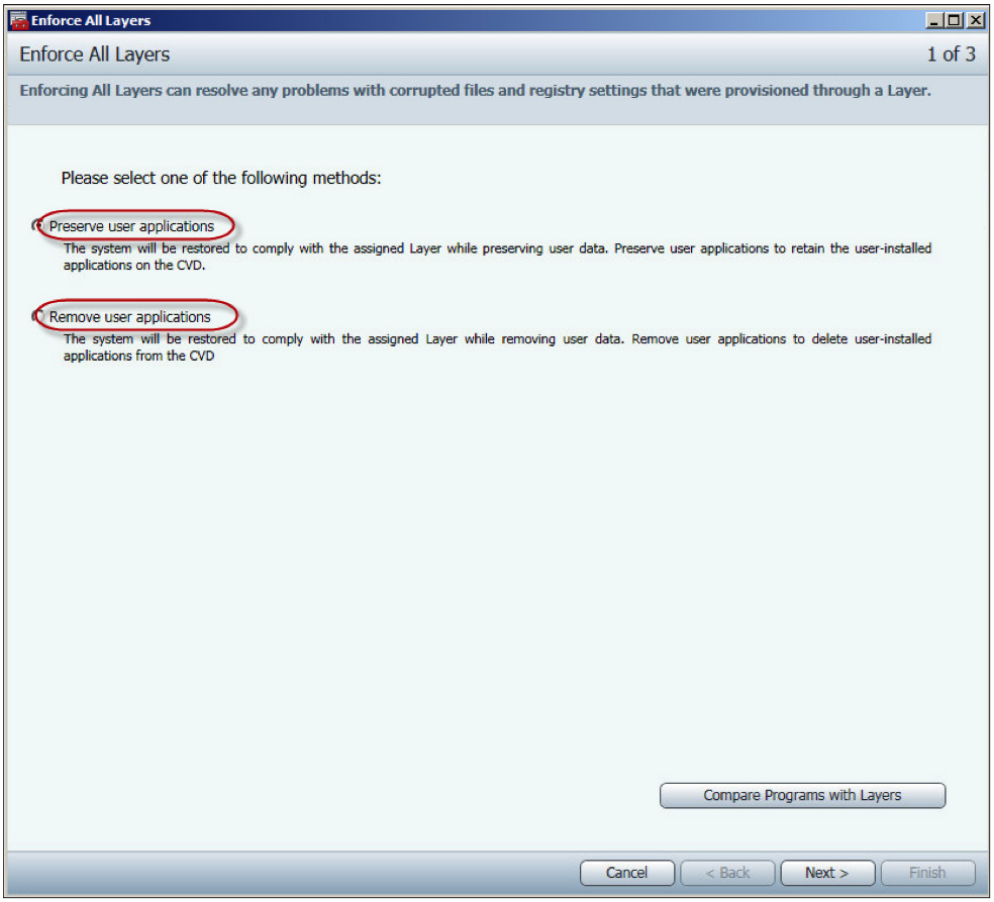
Enforce All Layers

You enforce layers from the CVD that is causing problems.

1. In the left pane of the Mirage Console, expand **Inventory** and click **All CVDs**.
2. In the All CVDs pane, right-click the problematic CVD and select **Enforce All Layers**.



The Enforce All Layers page appears.



3. Select the appropriate method according to your requirements and click **Next**.

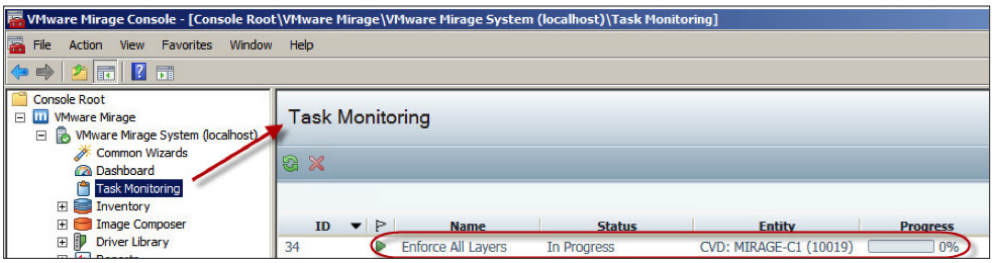
The Compatibility Check page appears.

4. Click **Next**.

   The Summary page appears.

5. Click **Finish**.
6. In the left pane, click **Task Monitoring**, and in the right pane, verify that the task has started.

   A Status value of In Progress indicates that the task has started.



What to Do Next

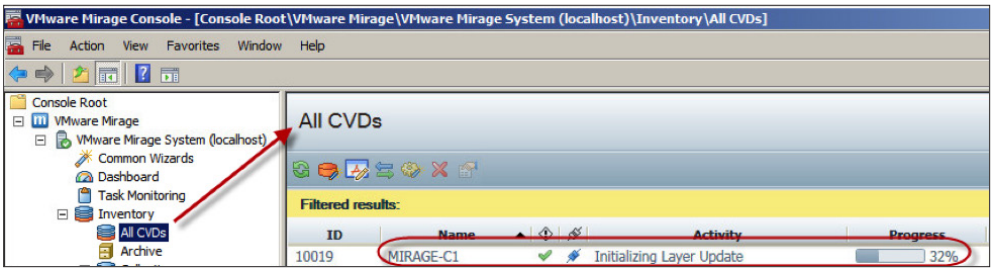
Monitor the progress of the task using either of the following methods:

- Mirage Console
- Endpoint

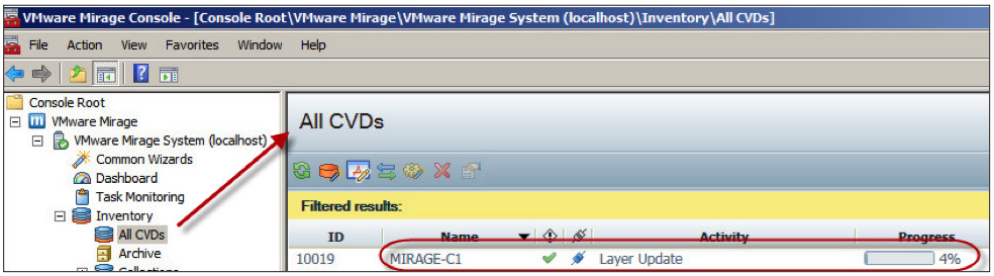
Use the Mirage Console to Monitor Enforce All Layers
The Mirage Console shows you the progress of the Enforce All Layers task.

1. In the left pane, expand **Inventory** and click **All CVDs**.
2. Monitor the progress in the All CVDs pane.

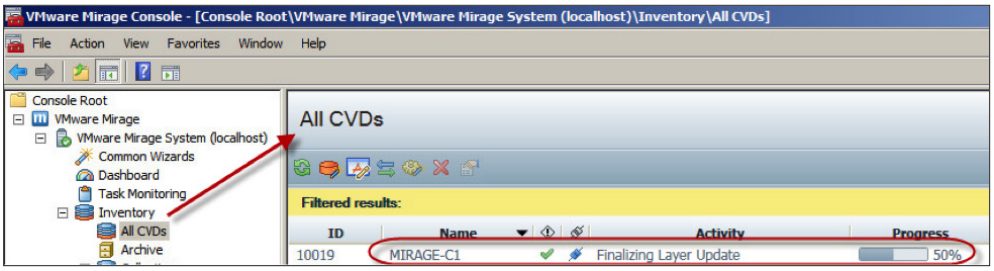
   At first, the Activity value is Initializing Layer Update.



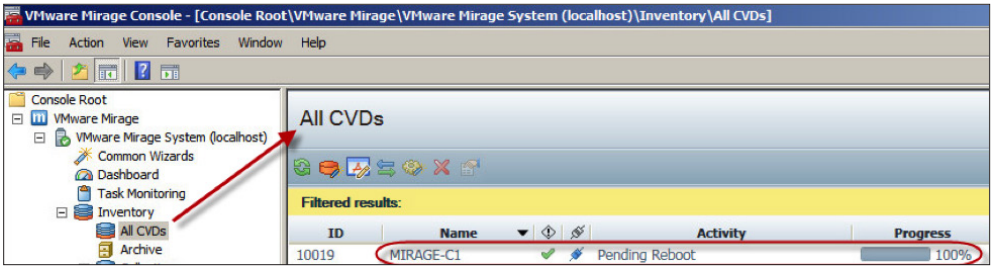
When the initialization finishes, the Activity value changes to Layer Update.



The Activity value then changes to Finalizing Layer Update.



Finally, the Activity value changes to Pending Reboot.



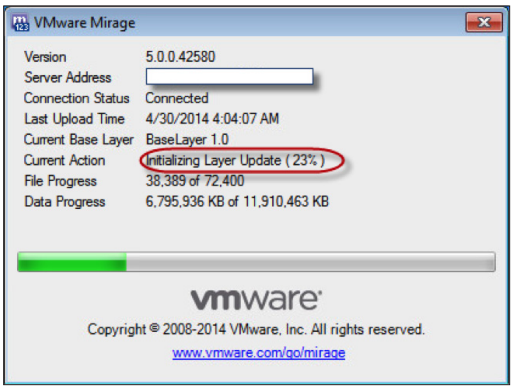
3. Access the endpoint, and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.

To complete enforcing the layers, restart the endpoint.

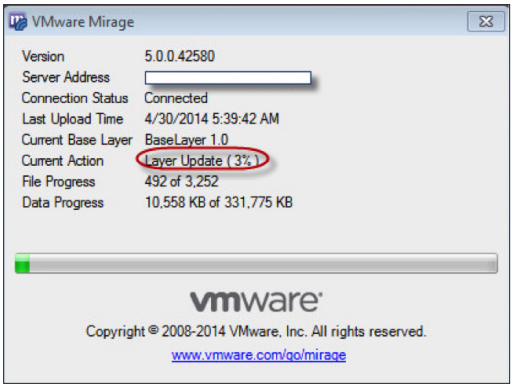
Use the Endpoint to Monitor Enforce All Layers
You monitor the Enforce All Layers task on the endpoint.

1. Access the endpoint, and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.
2. Monitor the progress.

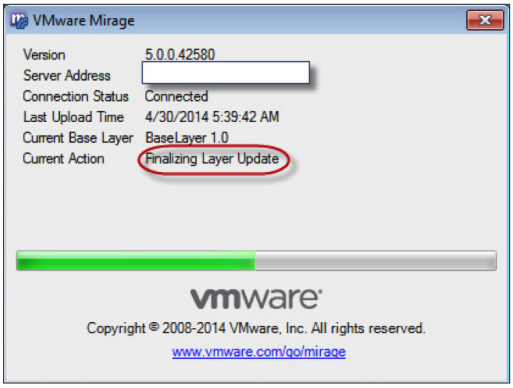
   At first, the Current Action value is Initializing Layer Update.



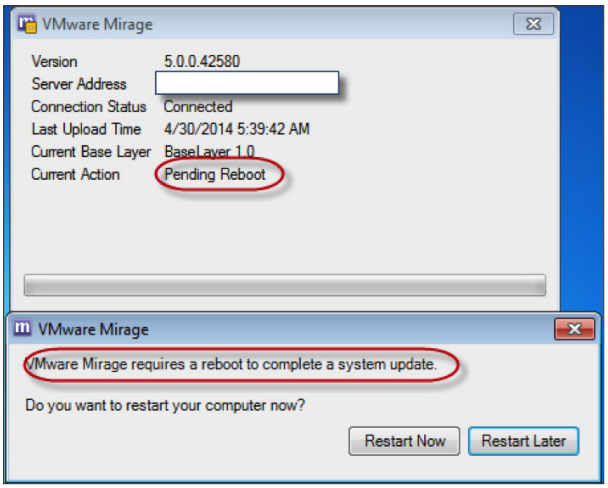
When the initialization is complete, the Current Action value changes to Layer Update.



The Current Action value then changes to Finalizing Layer Update.



After the update is finalized, you are prompted to reboot the endpoint.

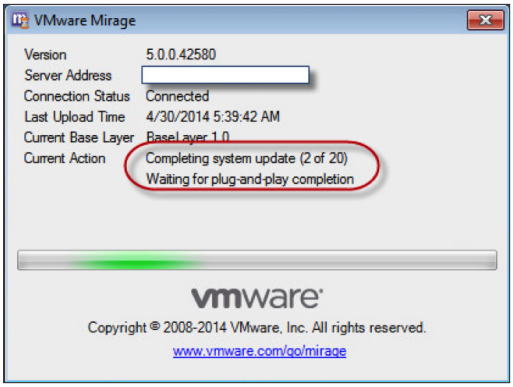


Restart the Endpoint to Complete Enforcing Layers

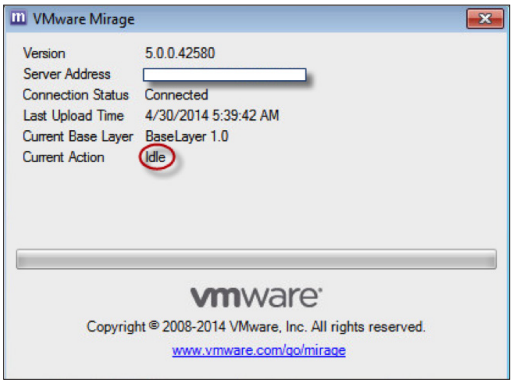
When you are finished monitoring the Enforce All Layers task, you must restart the endpoint.

1. In the VMware Mirage dialog box of the endpoint, click **Restart Now**.
2. After the endpoint restarts, log in to it and wait for the Mirage client to upload.

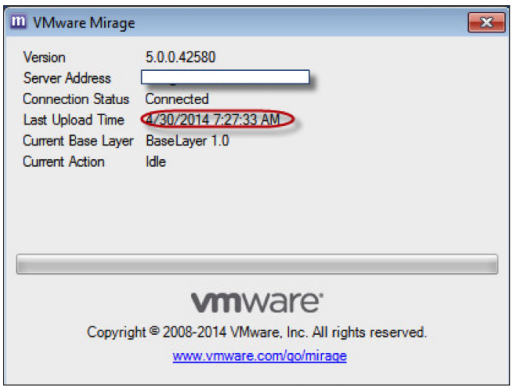
   The Current Action value changes to Completing system update, and the Last Upload Time value has not changed.



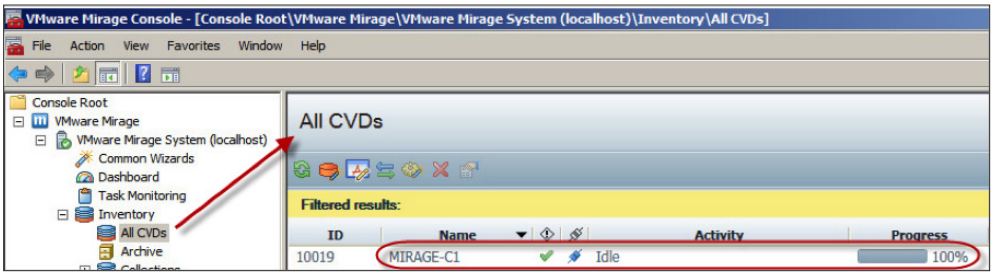
After the update finishes, the Current Action value changes to Idle.



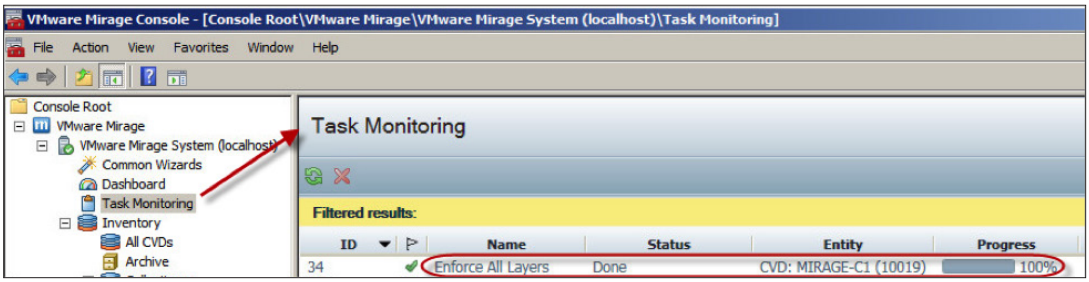
In a few minutes, Mirage starts to upload the Mirage client, and the Last Upload Time value changes to the new time.



3. In the left pane of the Mirage Console, expand **Inventory** and click **All CVDs**.
4. In the All CVDs pane, verify that the Activity value of the CVD is Idle.



5. In the left pane, click **Task Monitoring**, and in the right pane, verify that the Status value of the Enforce All Layers task is Done.



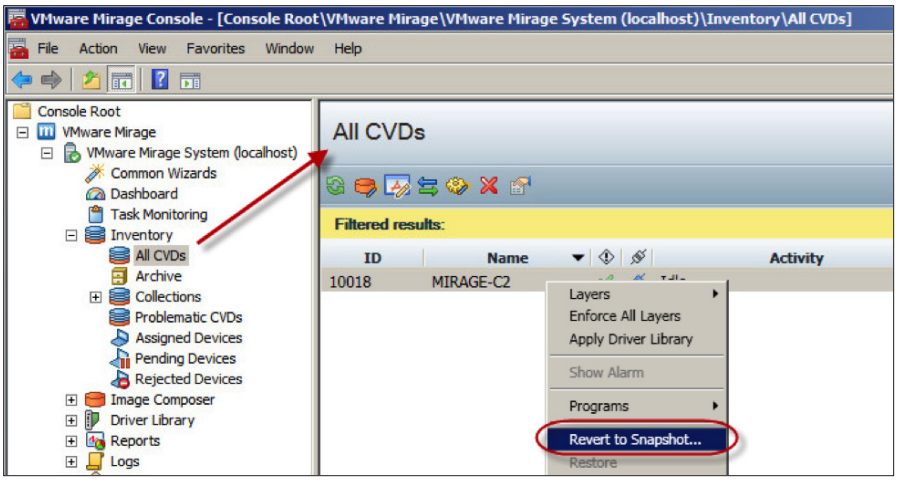
Reverting a CVD to a Mirage Snapshot

If you want to revert an entire endpoint to a previous point in time from a backup on the Mirage server, you can use the Revert to Snapshot option. This option downloads all the content of the selected snapshot and overwrites the endpoint.

Revert a CVD to a Mirage Snapshot

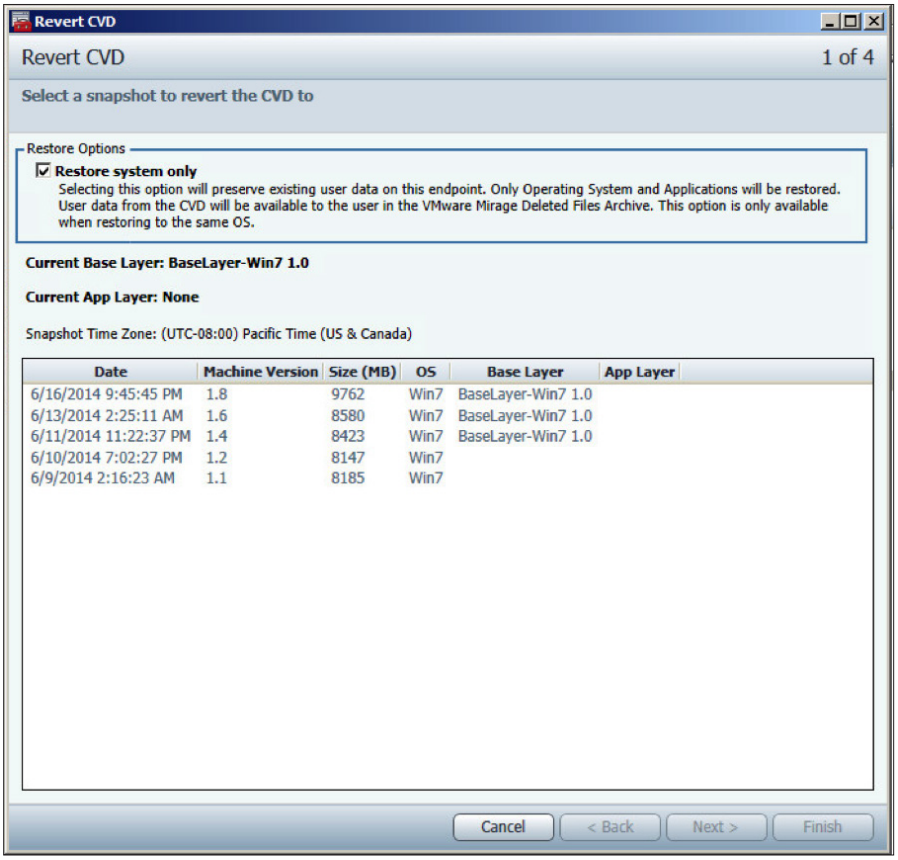
You implement the Revert to Snapshot feature from the CVD that you want to restore to a previous snapshot.

1. In the left pane of the Mirage Console, expand **Inventory** and click **All CVDs**.



2. In the All CVDs pane, right-click the CVD you want to revert and select **Revert to Snapshot**.

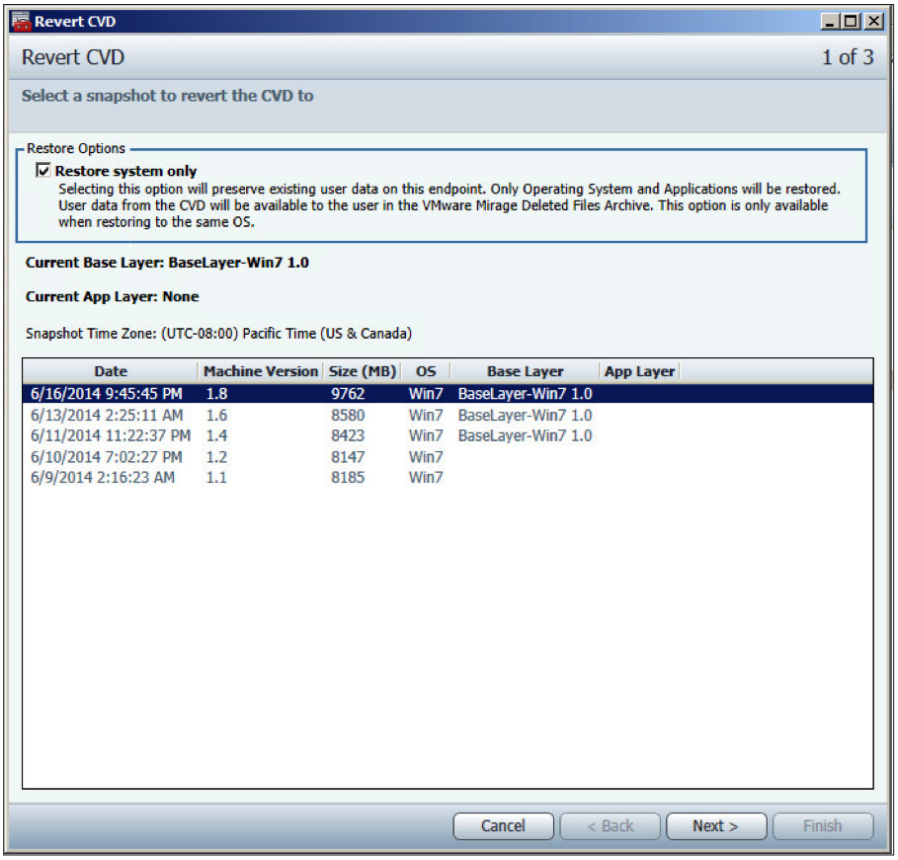
The Revert CVD page appears with the available snapshots listed.



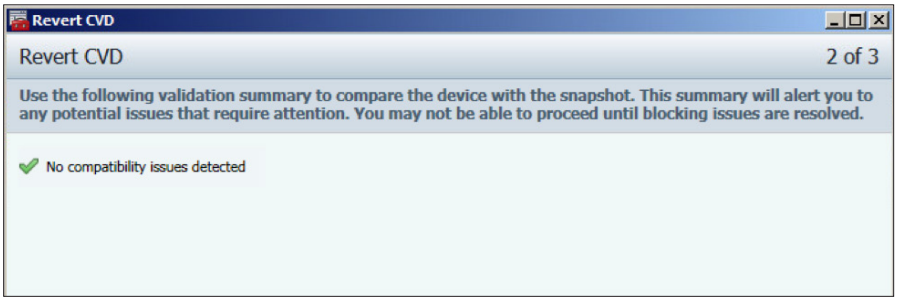
3. If applicable, select the **Restore system only** option.

   Determine if the option applies to your requirements based on the explanation accompanying the option.

4. Select a snapshot and click **Next**.

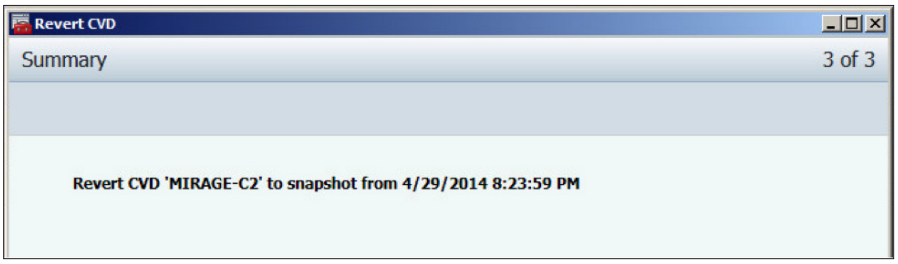


The page for validation appears.



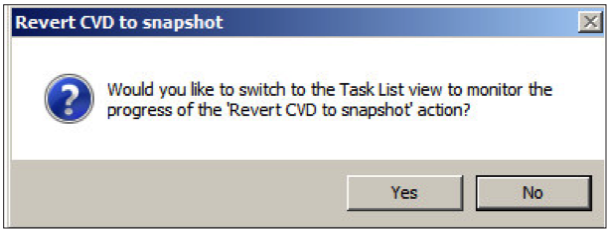
5. Click **Next**.

   The Summary page appears.



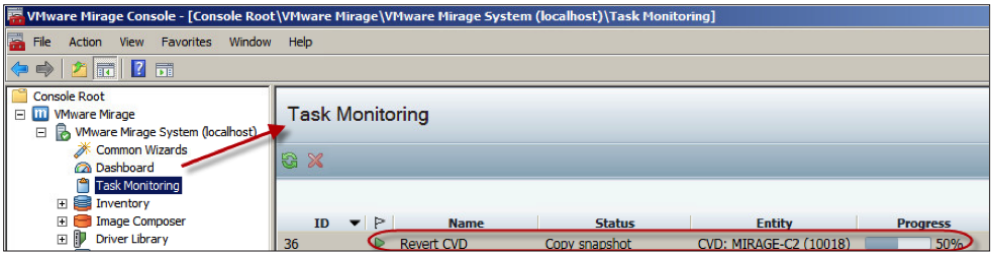
6. Click **Finish**.

   The Revert CVD to snapshot confirmation box appears.



7. Click **Yes**.

   The right pane in the Mirage Console switches to the Task Monitoring page. The Revert CVD task is listed, and the Status value is Copy snapshot.



What to Do Next

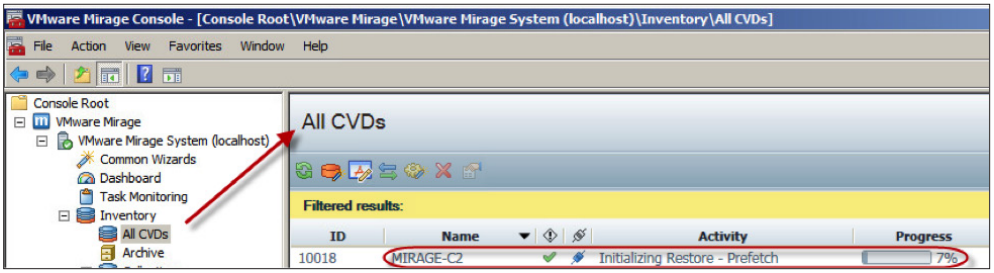
Monitor the progress of the task using either of the following methods:

- Mirage Console
- Endpoint

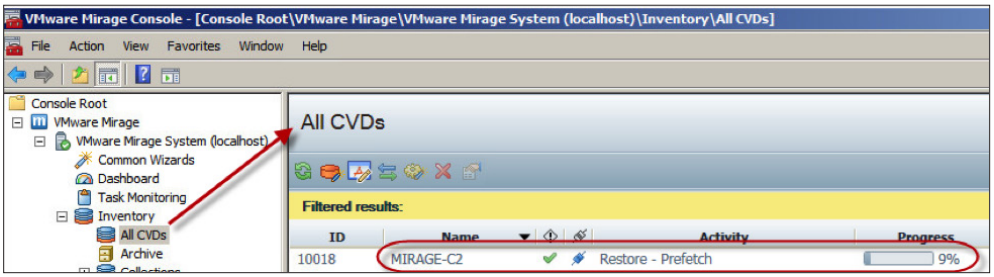
Use the Mirage Console to Monitor Reverting to a Snapshot
The Mirage Console shows the progress of the Revert to Snapshot task.

1. In the left pane, expand **Inventory** and click **All CVDs**.
2. Monitor the progress in the All CVDs pane.

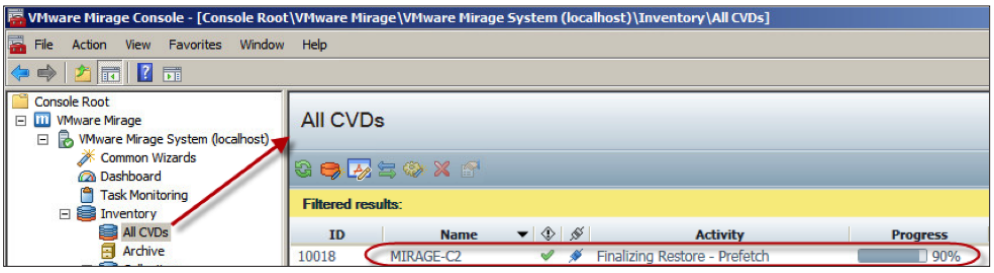
   At first, the Activity value is Initializing Restore – Prefetch.



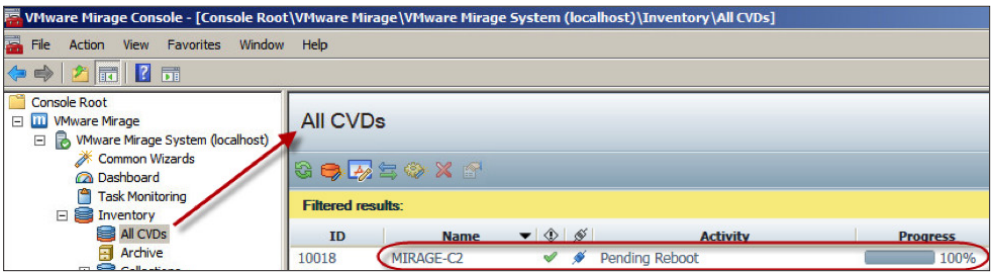
   When the initialization finishes, the Activity value changes to Restore – Prefetch.



   The Activity value then changes to Finalizing Restore – Prefetch.



   As you monitor the progress, the Progress value reaches 100%, and the Activity value changes to Pending Reboot.



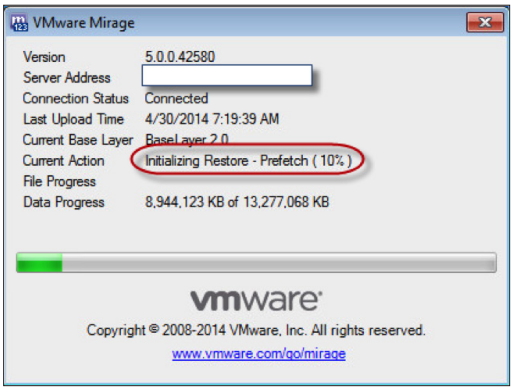
3. Access the endpoint, and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.

To complete reverting the snapshot, restart the endpoint.

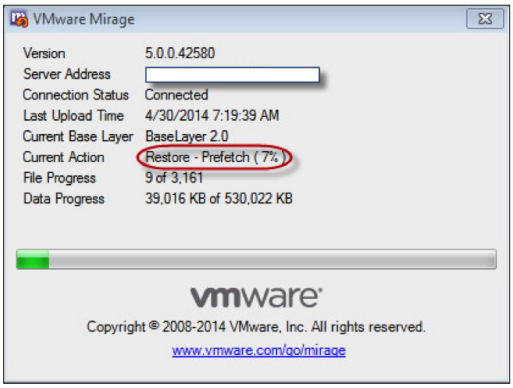
Use the Endpoint to Monitor Reverting to a Snapshot
You can monitor the Revert to Snapshot task on the endpoint.

1. Access the endpoint, and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.
2. Monitor the progress.

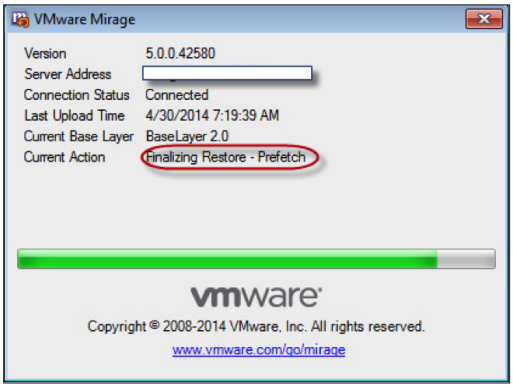
   At first, the Current Action value is Initializing Restore – Prefetch.



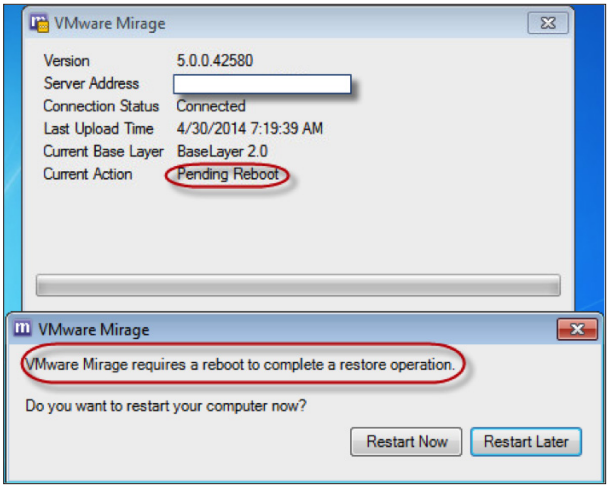
When the initialization is complete, the Current Action value changes to Restore – Prefetch.



The Current Action value then changes to Finalizing Restore – Prefetch.



After it is finalized, you are prompted to reboot the endpoint.

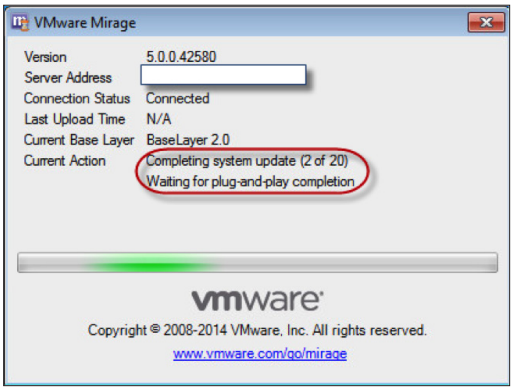


Restart the Endpoint to Revert the Snapshot

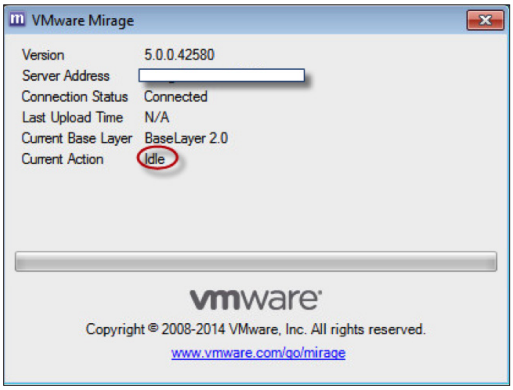
When you are finished monitoring the Revert to Snapshot task, you must restart the endpoint.

1. In the VMware Mirage dialog box of the endpoint, click **Restart Now**.
2. After the endpoint restarts, log in to it and wait for the Mirage client to upload.

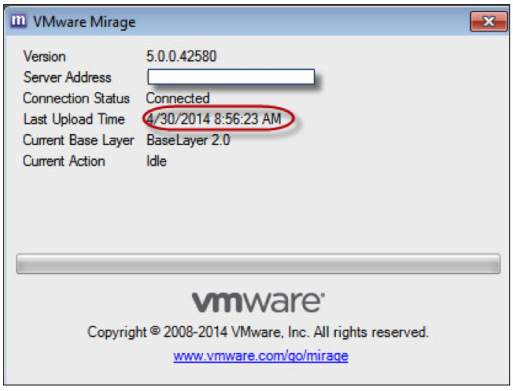
   The Current Action value changes to Completing system update, and the Last Upload Time value is N/A.



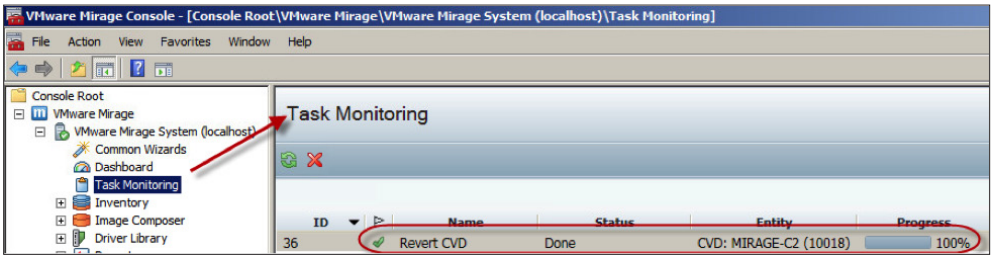
The Current Action value changes to Idle, and the Last Upload Time value remains N/A.



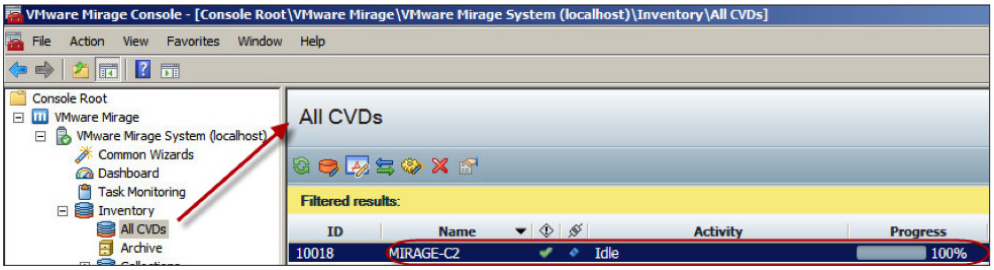
In a few minutes, the Mirage client starts to upload the endpoint. After the upload finishes, the Last Upload Time value changes to the time the upload completes.



3. In the left pane of the Mirage Console, click **Task Monitoring**, and in the right pane, verify that the Revert CVD task has completed.



4. In the left pane, expand **Inventory** and click **All CVDs**.
5. In the All CVDs pane, verify that the Activity value of the CVD is Idle.



You have reverted your endpoint to a Mirage snapshot.

Recovering a Failed or Missing Endpoint

If your endpoint fails or is missing, you can recover the corresponding CVD. You can either restore the entire CVD to the device after replacing or reformatting its hard drive, or you can restore the CVD to a new device.

This exercise uses the Replace the User Machine option, which involves preparing a new machine and installing the Mirage client on it. The new machine can be a physical machine or a virtual machine. Before you begin, install the Mirage client on the new machine.

Recover a Failed or Missing Endpoint

The Disaster Recovery wizard requires you to select one of the following:

• Replace Hard Disk – Restores the entire CVD to the device after its hard drive is replaced or formatted.

• Replace the User Machine – Restores the CVD to a new device.

The steps for these options are similar.

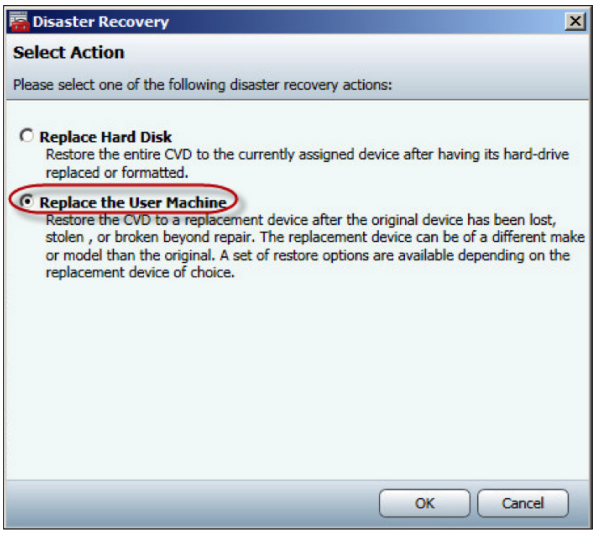
Prerequisite

Prepare a new machine and perform the Installing the Mirage Client on the Test Machines task on the new machine.

Procedure

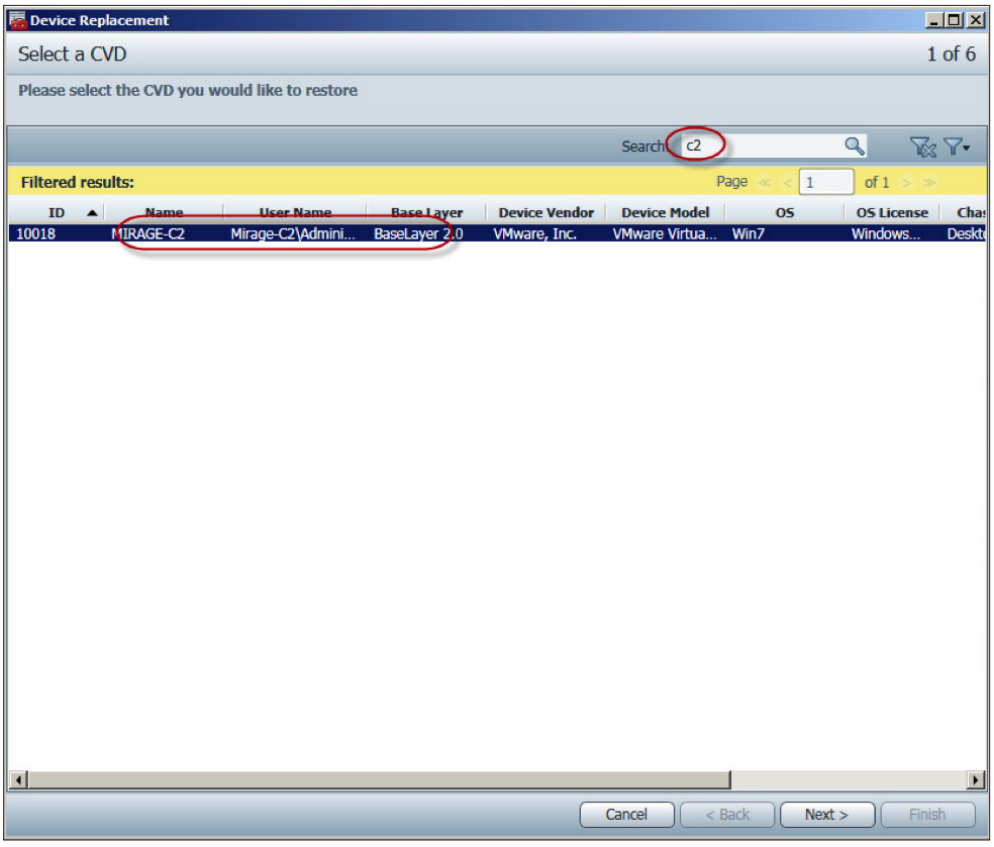
1. In the left pane of the Mirage Console, click **Common Wizards**, and in the right pane, click **Disaster Recovery**.

The Disaster Recovery dialog box appears.



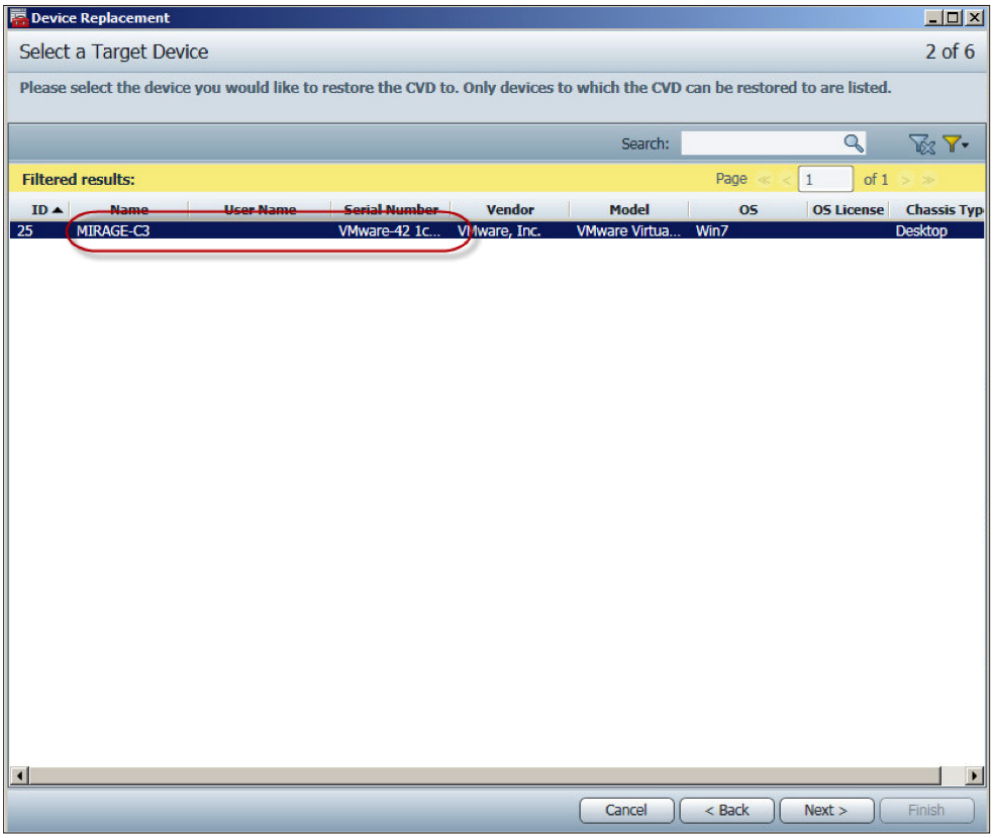
2. For this evaluation exercise, select **Replace the User Machine** and click **OK**.

   The Select a CVD page appears.



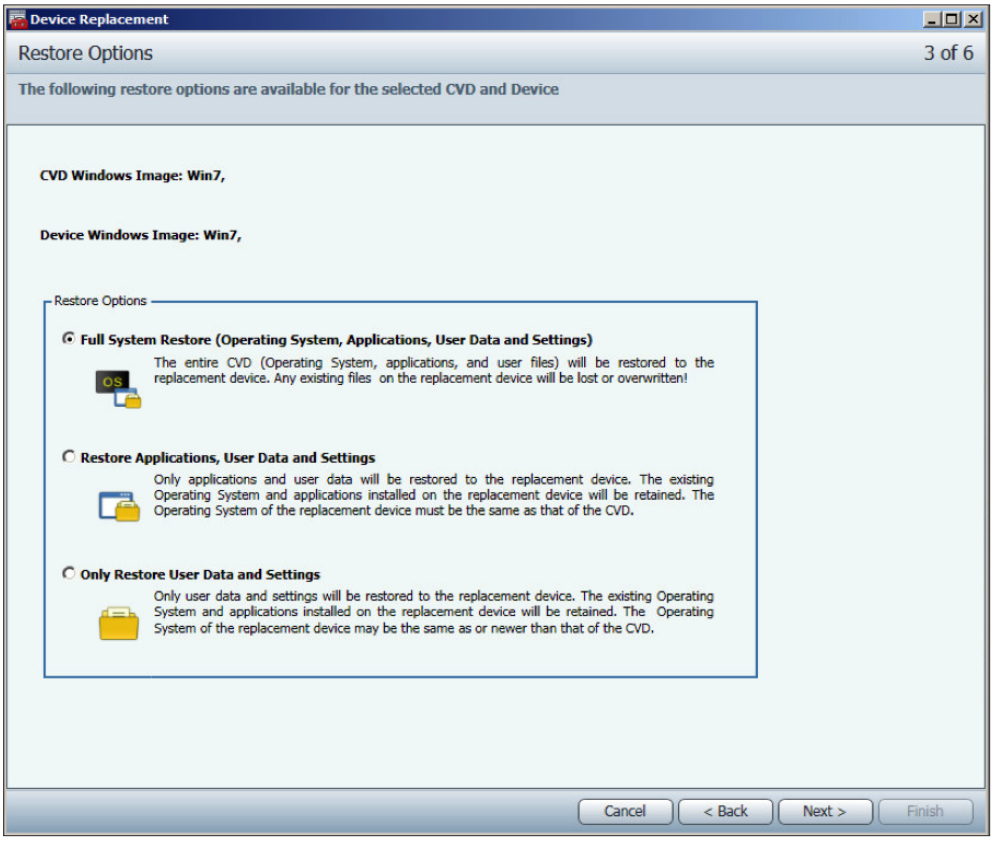
3. Search for the CVD that you want to recover and click **Next**.

The Select a Target Device page appears.

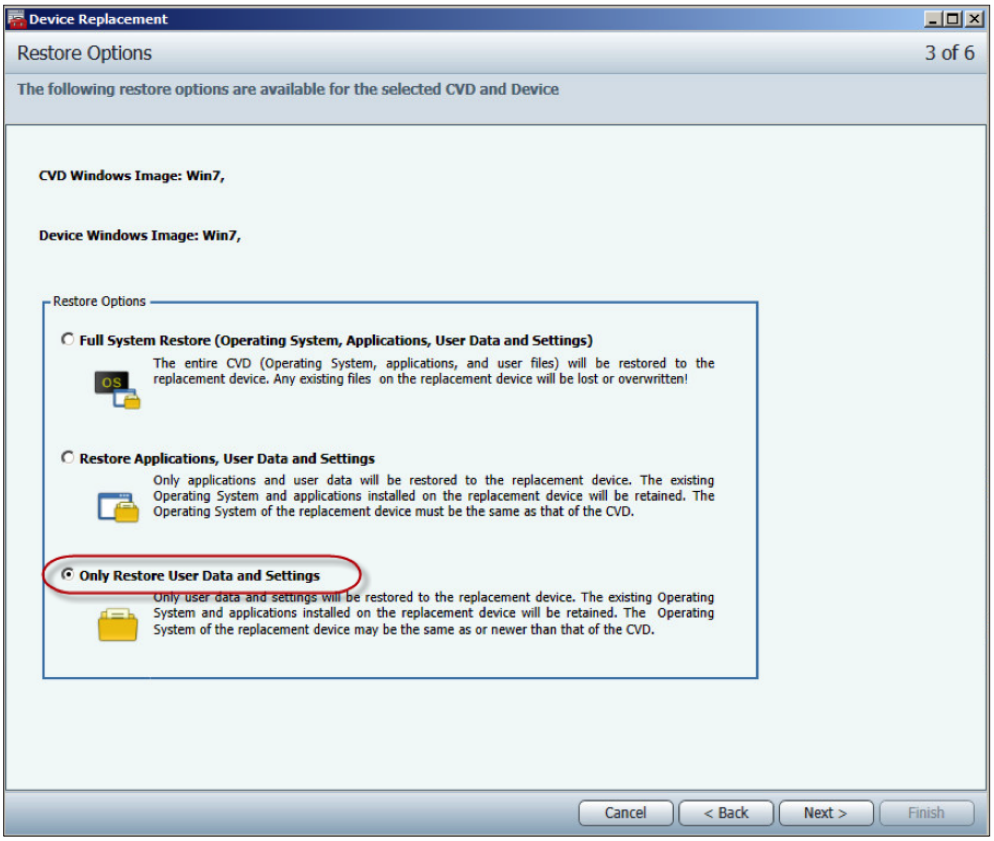


4. Select a pending device and click **Next**.

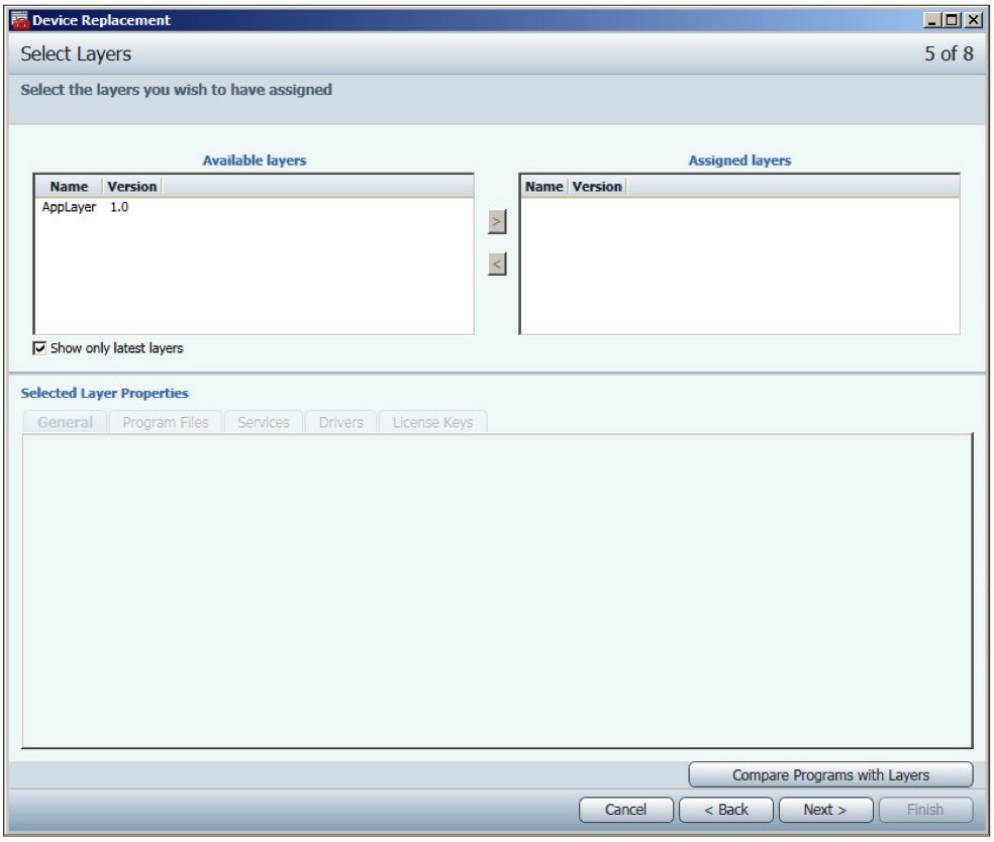
The Restore Options page appears.



5. For this evaluation, select **Only Restore User Data and Settings** and click **Next**.

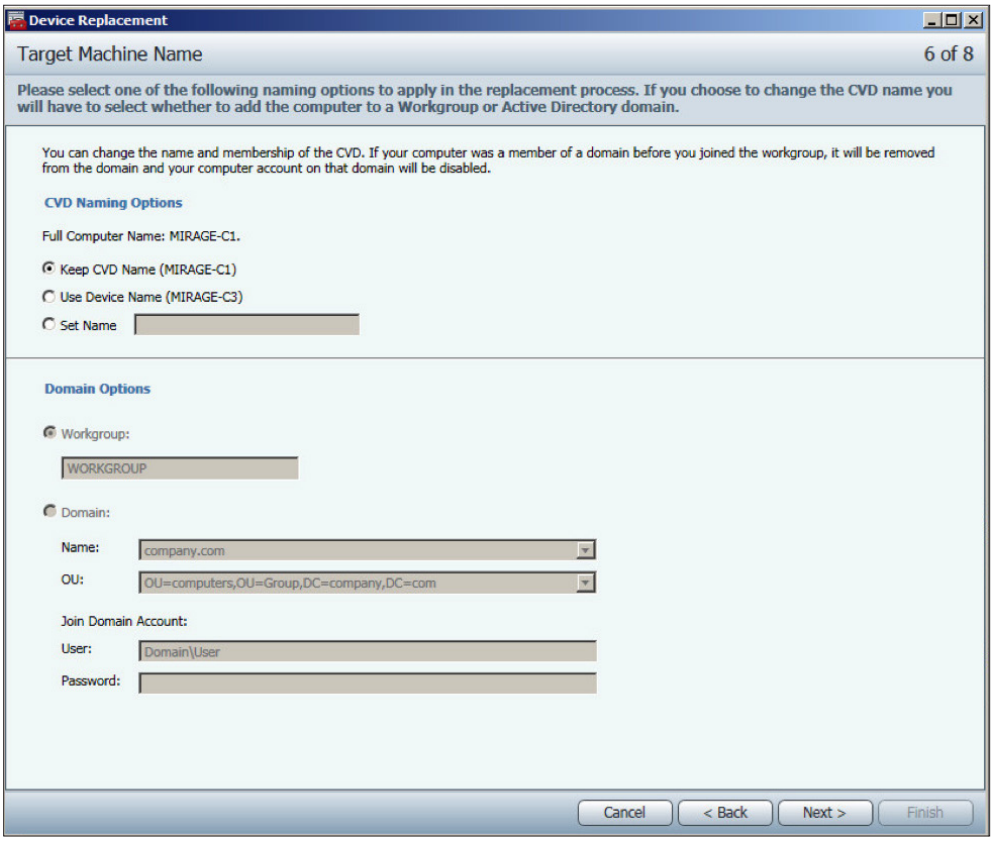


The Select Layers page appears.



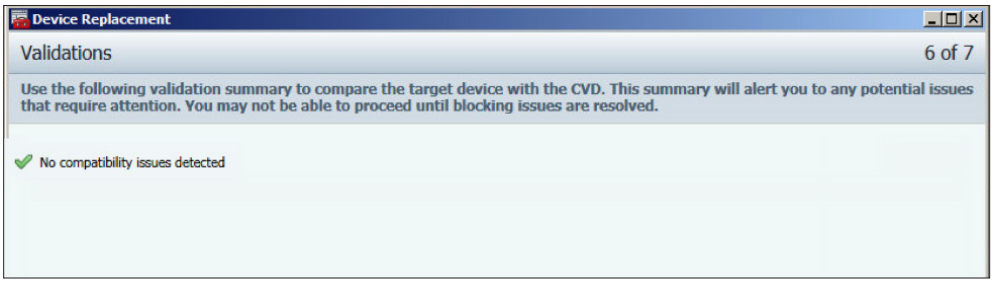
6. Move the layer that best meets your requirements from the Available layers section to the Assigned layers section, and then click **Next**.

The Target Machine Name page appears.



7. Complete the page with the options that best meet your requirements and then click **Next**.

   The Validations page appears.

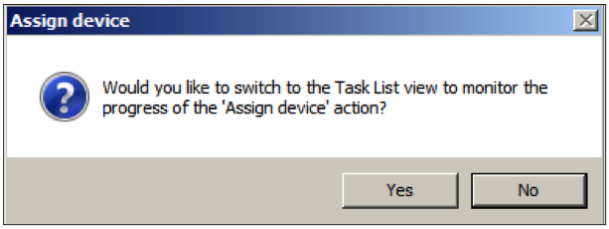


8. Click **Next**.

The Summary page appears.

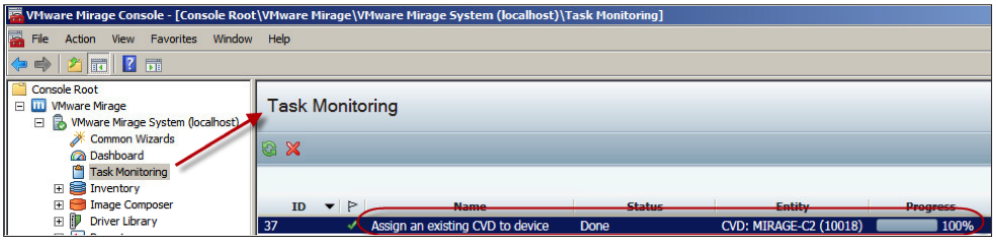
9. Click **Finish**.

   The Assign device confirmation box appears.



10. Click **Yes**.

    The Mirage Console switches to the Task Monitoring page, and the task is listed.



What to Do Next

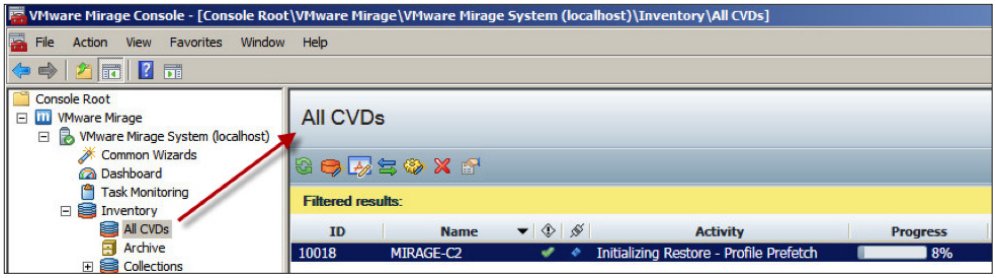
Monitor the progress of the task using either of the following methods:

- Mirage Console
- Endpoint

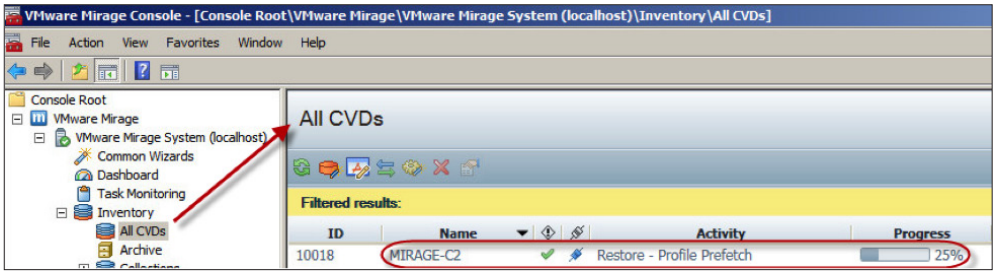
Use the Mirage Console to Monitor Assigning an Existing CVD to a Device
The Mirage Console shows the progress of the task.

1. In the left pane, expand **Inventory** and click **All CVDs**.
2. Monitor the progress in the All CVDs pane.

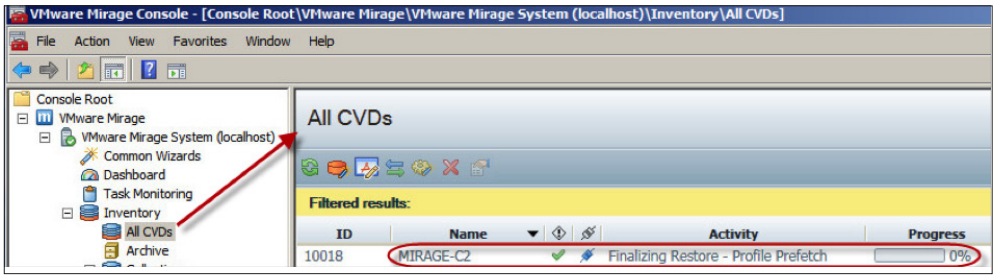
   At first, the Activity value is Initializing Restore – Profile Prefetch.



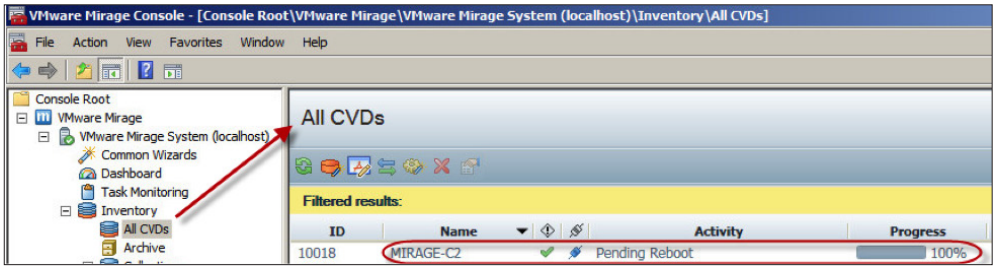
When the initialization finishes, the Activity value changes to Restore – Profile Prefetch.



The Activity value then changes from Restore – Profile Prefetch to Finalizing Restore – Profile Prefetch.



The Activity value then changes to Pending Reboot.



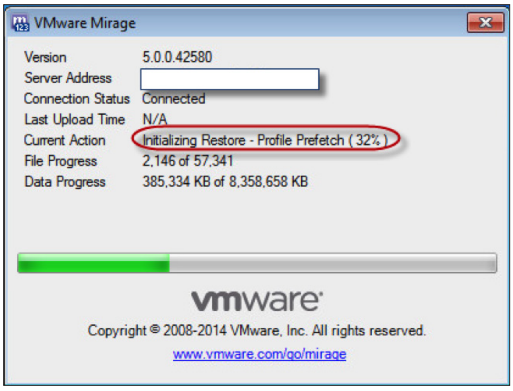
3. Access the endpoint, and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.

To complete assigning an existing CVD to a device, restart the new endpoint.

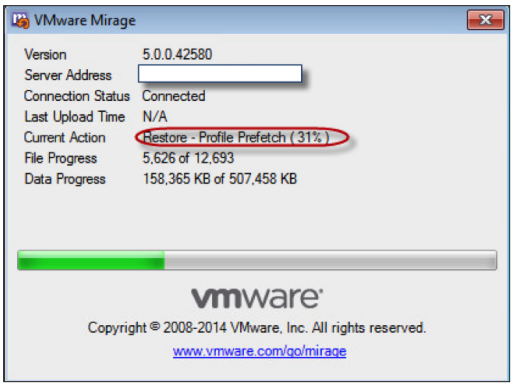
Use the Endpoint to Monitor Assigning an Existing CVD to a Device
You can use the endpoint to monitor the task.

1. Access the endpoint, and double-click the Mirage icon in the system tray to open the VMware Mirage dialog box.
2. Monitor the progress.

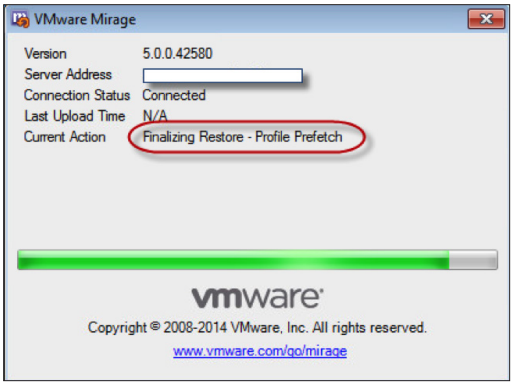
   At first, the Current Action value is Initializing Restore – Profile Prefetch.



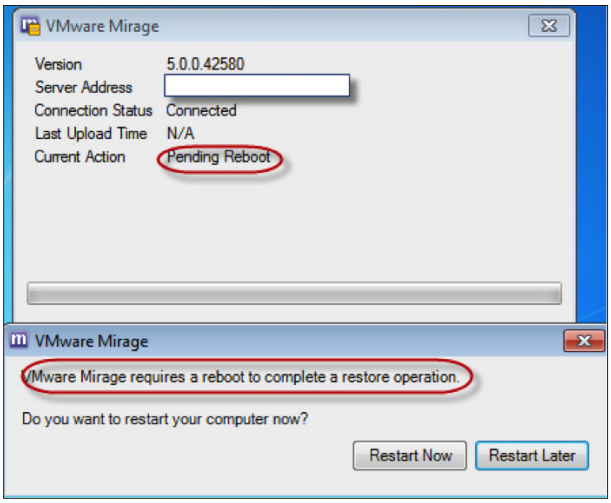
When the initialization is complete, the Current Action value changes to Restore – Profile Prefetch.



The Current Action value then changes to Finalizing Restore – Profile Prefetch.



After the action is finalized, you are prompted to reboot the endpoint.



Restart the Endpoint to Recover the CVD

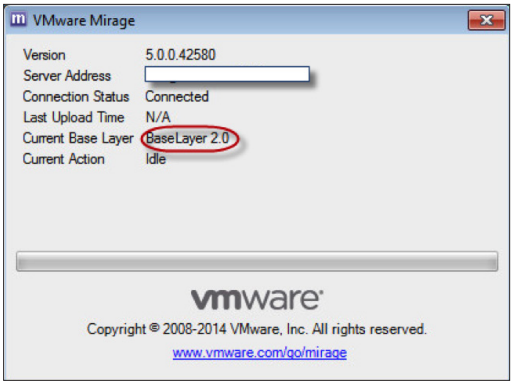
When you are finished monitoring the task, you must restart the endpoint.

1. In the VMware Mirage dialog box of the endpoint, click **Restart Now**.

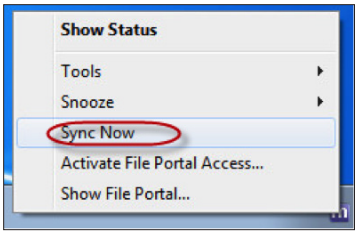
   Mirage completes a system update during the restart.

2. After the endpoint restarts, log in to it.

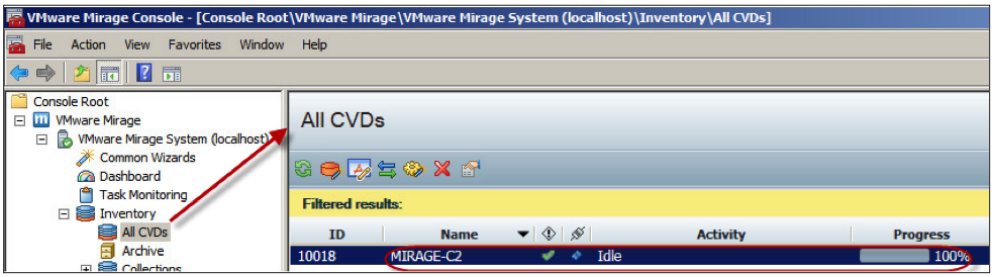
   The VMware Mirage window displays the status and the selected layers. The Last Upload Time value is N/A. In a few minutes, the Mirage client starts a backup and updates the Last Upload Time value.



3. (Optional) If you want to start a backup immediately, right-click the Mirage icon in the system tray, and select **Sync Now**.



4. In the left pane of the Mirage Console, expand **Inventory** and click **All CVDs**.
5. In the All CVDs pane, verify that the Activity value is Idle.



You have recovered the CVD to the target device.

Configuring the Mirage File Portal to Enable Users to View Files and Folders

The Mirage file portal enables users to browse and view files in the CVDs through any browser from any location that can connect to the file portal server.

This section covers the following topics:

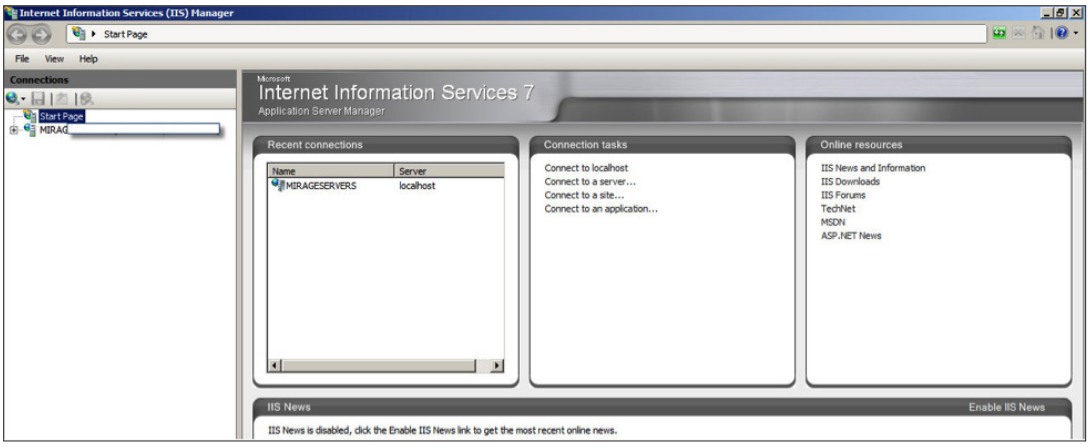
- Configuring IIS on the Mirage file portal
- Configuring the file portal in the Mirage Console
- Accessing the file portal

Configure IIS on the Mirage File Portal

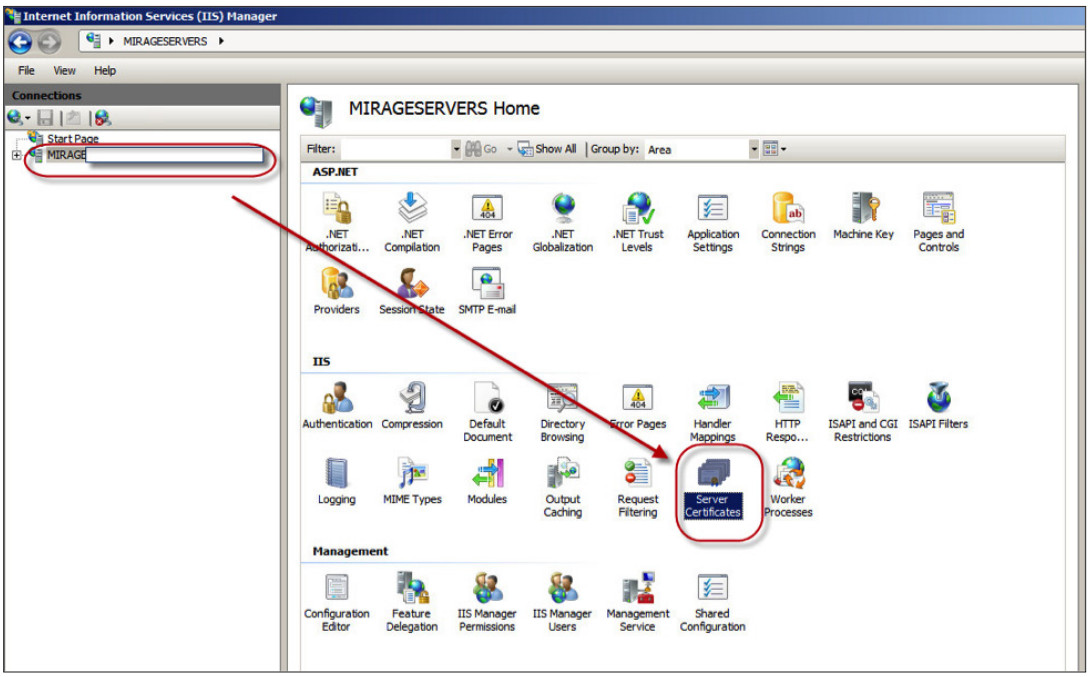
Before beginning, you must install Windows Internet Information Services (IIS) 7.0 and the Mirage file portal. See New Installation and Configuration.

1. In the operating system where the Mirage file portal is installed, select **Start** > **Run**.
2. Type `inetmgr`, and click **OK**.

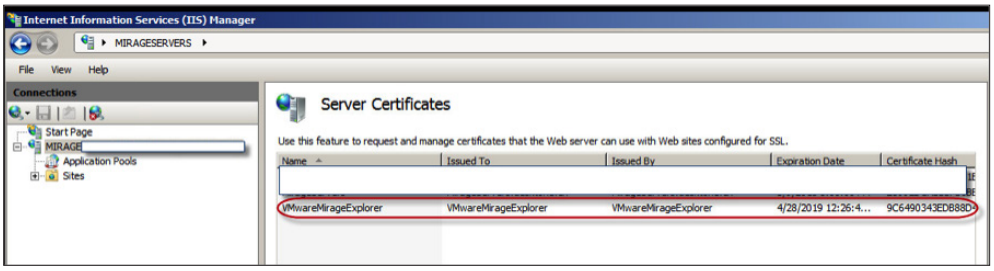
   The IIS Manager appears.



3. In the Connections tree, click the IIS instance on which the Mirage Web applications are installed and click **Server Certificates**.



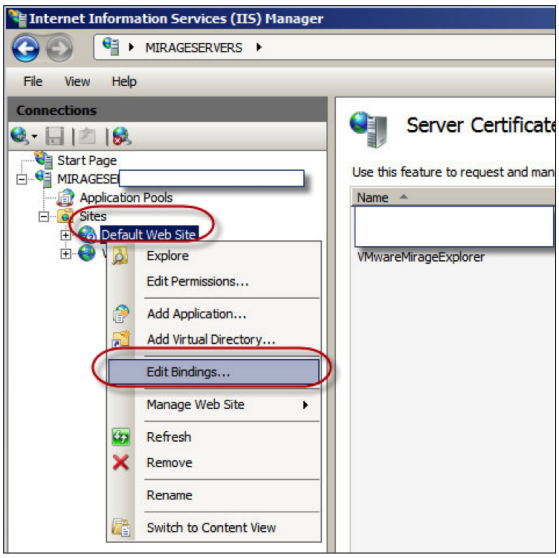
The Server Certificates pane appears.



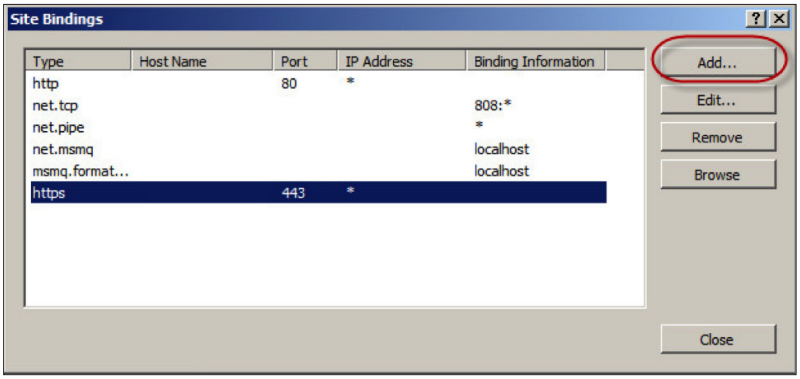
4. Locate the SSL certificate for the Mirage file portal.

   In this evaluation exercise, the SSL certificate is the one created during installation of the Mirage file portal. The name is VMwareMirageExplorer. You can create or import a new SSL certificate for the Mirage file portal.

5. In the left pane, expand **Sites**, right-click **Default Web Site** and select **Edit Bindings**.

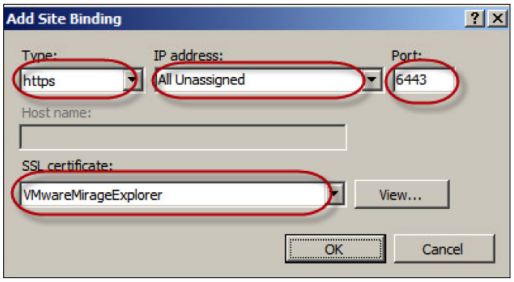


The Site Bindings dialog box appears.



6. Click **Add**.

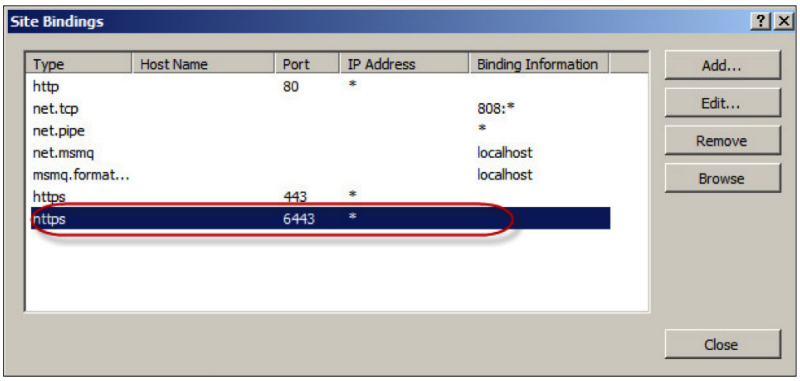
The Add Site Binding dialog box appears.



7. Enter the appropriate information, such as the following, and then click **OK**.

ITEM	VALUE
Type	https
IP address	All Unassigned
Port	The default is 6443.
SSL certificate	The SSL certificate for the Mirage file portal. The default is `VMwareMirageExplorer`.

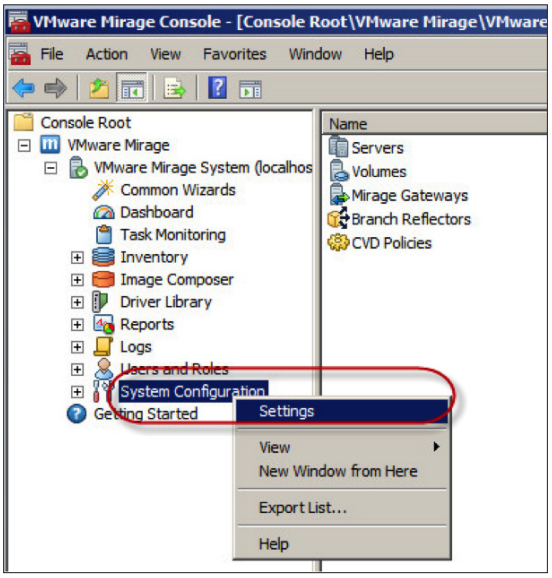
The newly added site binding is listed in the dialog box.



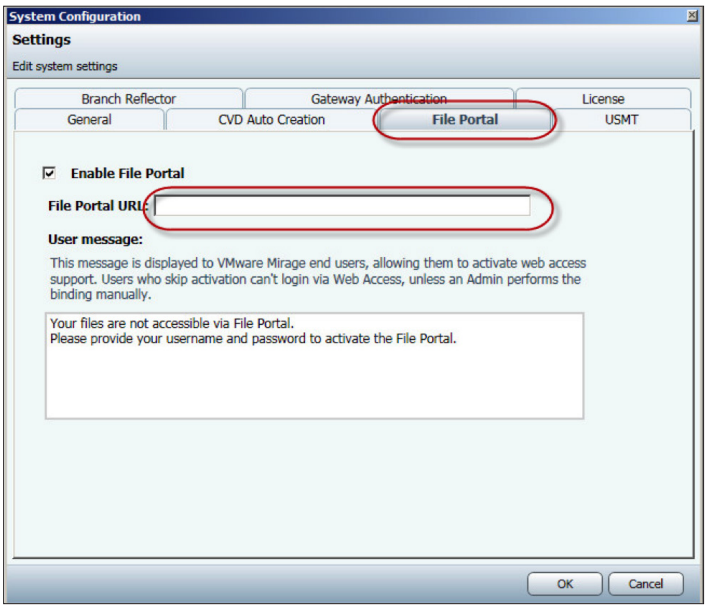
8. Click **Close**.

Configure the File Portal in the Mirage Console

1. In the left pane of the Mirage Console, right-click **System Configuration** and select **Settings**.

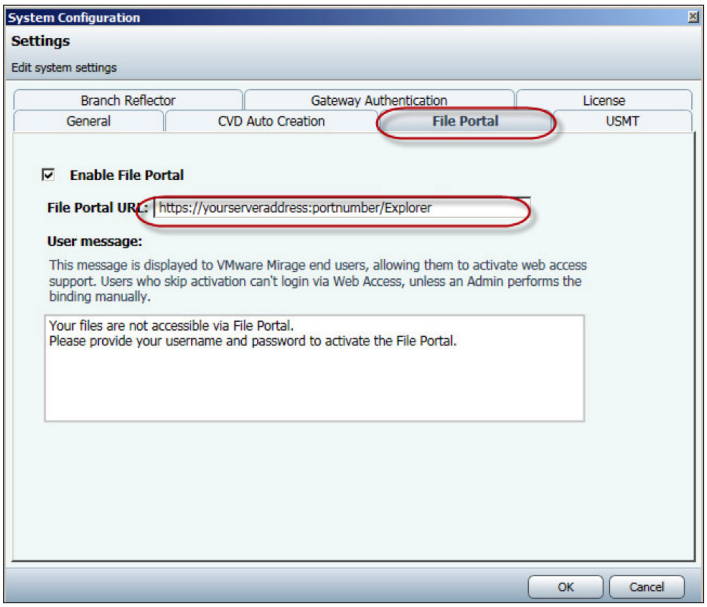


The System Configuration dialog box appears.



2. In the File Portal tab, enter the file portal URL and then click **OK**.

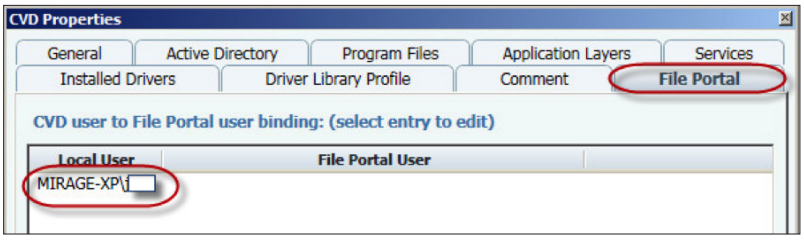
The format of the URL is `https://yourserveraddress:portnumber/Explorer`, where *yourserveraddress* is the address of your Mirage file portal, and *portnumber* is the port assigned to the Mirage file portal. The default is 6443.



3. In the left pane of the Mirage Console, expand **Inventory** and click **All CVDs**.
4. In the All CVDs pane, double-click the CVD for which you want to configure the file portal.

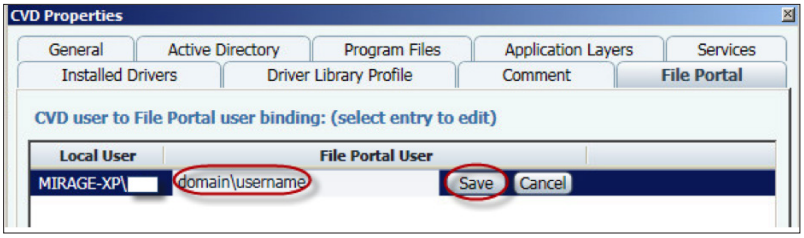
   The CVD Properties dialog box appears.
5. Click the **File Portal** tab.

   The tab lists all the local users who have logged in to the endpoint.



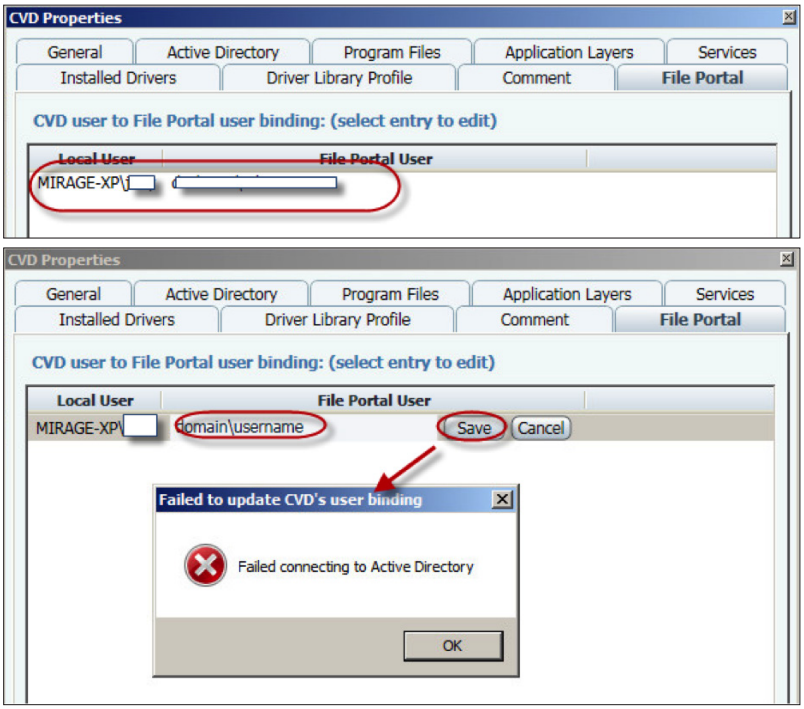
6. Click a local user in the list.
7. Enter the mapped user for the local user in the File Portal User column.

   The mapped user should be a domain user. The format is *domain\username*. This mapped user has access to the user data of the corresponding local user of the CVD.



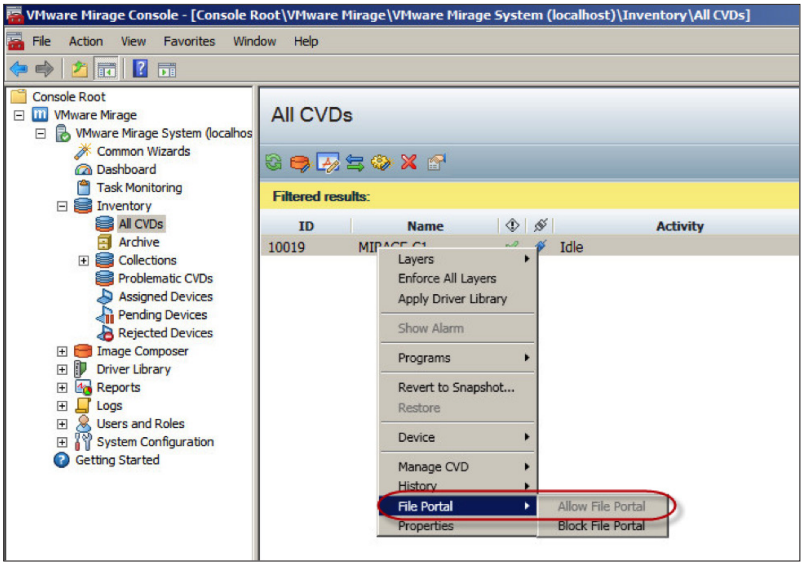
8. Click **Save**.

If the domain and user name are correct, mapping succeeds. If they are incorrect, an error message appears.



9. Right-click the CVD and select **File Portal**, and verify that **Allow File Portal** is selected.

   If the Allow File Portal option is dimmed, it has been selected.



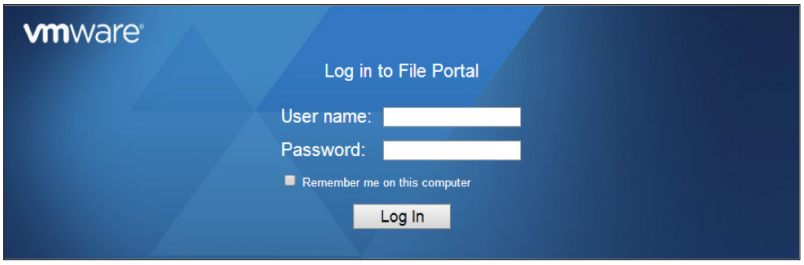
The file portal configuration is complete.

Access the File Portal

You can use a browser to access the file portal.

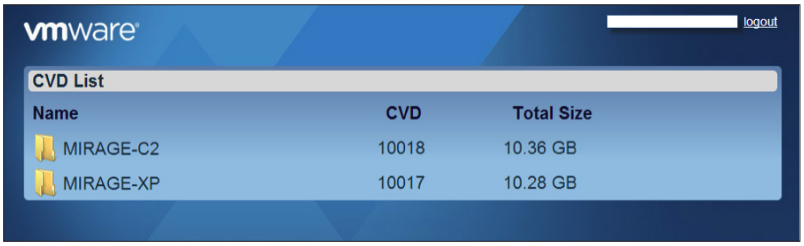
1. Open a browser and enter `https://yourserveraddress:portnumber/Explorer`, where *yourserveraddress:portnumber* is your file portal server address and port number.

   The File Portal login screen appears.



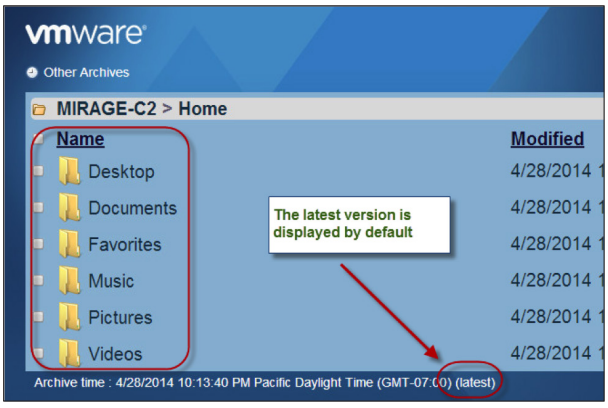
2. Enter the domain user name that you specified in Configure the File Portal in the Mirage Console.

   The CVD list appears.



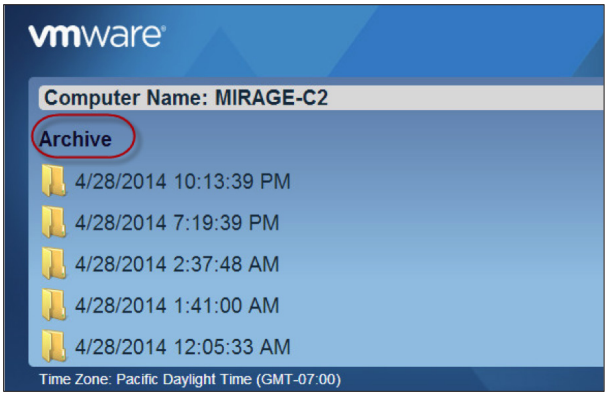
3. Select a CVD to explore.

   If you mapped the user to a local user of a CVD, as described in Configure the File Portal in the Mirage Console, the files of the CVD are listed directly. By default, the latest version of the files and folders are listed.



4. To view other versions, click **Other Archives**.

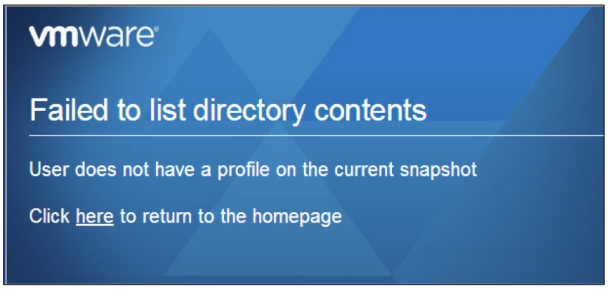
A list of the archives appears.



5. Select an archive.

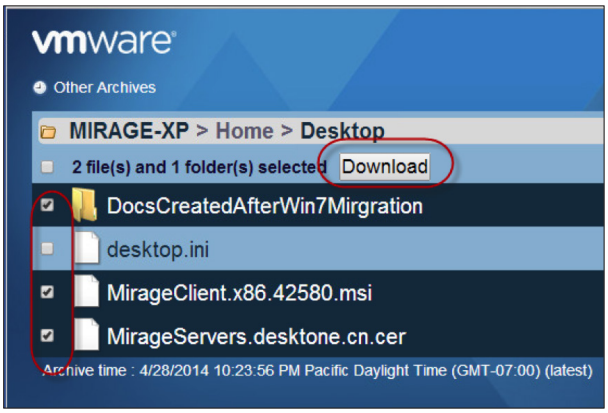
The contents of the selected archive appears, along with the archive time.

Troubleshooting Tip: If you encounter the following error while choosing an archive, the mapped local user does not have a profile in this particular archive. For example, the user was created after the archive was created. Try selecting another archive.



6. Select the check box for each file or folder you want to download.

   The Download button appears.



7. Click **Download**.

   The selected files and folders, including subfolders, are downloaded. You can now view them locally.

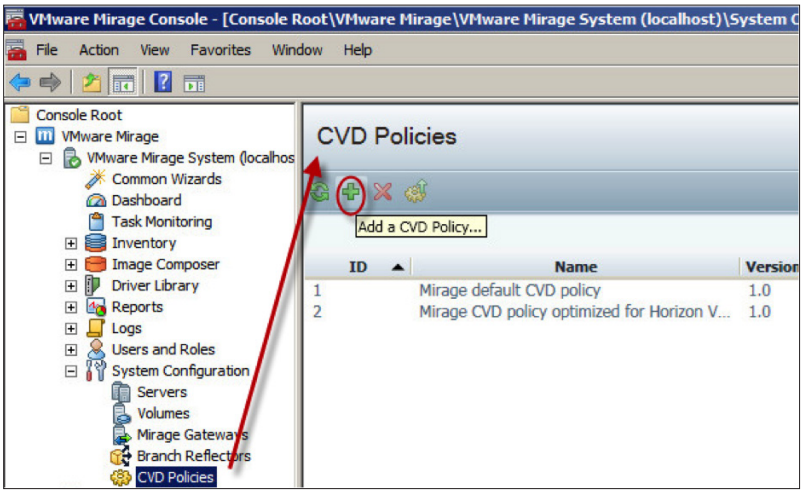
Using a CVD Policy for Layer Management

The Centralizing Endpoints section of this guide provides instructions for using the Mirage default CVD policy for endpoints. That default policy backs up the endpoints to the data center.

If you are not uploading content, except metadata from endpoints to the data center, use the Mirage CVD policy optimized for View. With this policy, you can perform layer management against the devices without backing up the devices.

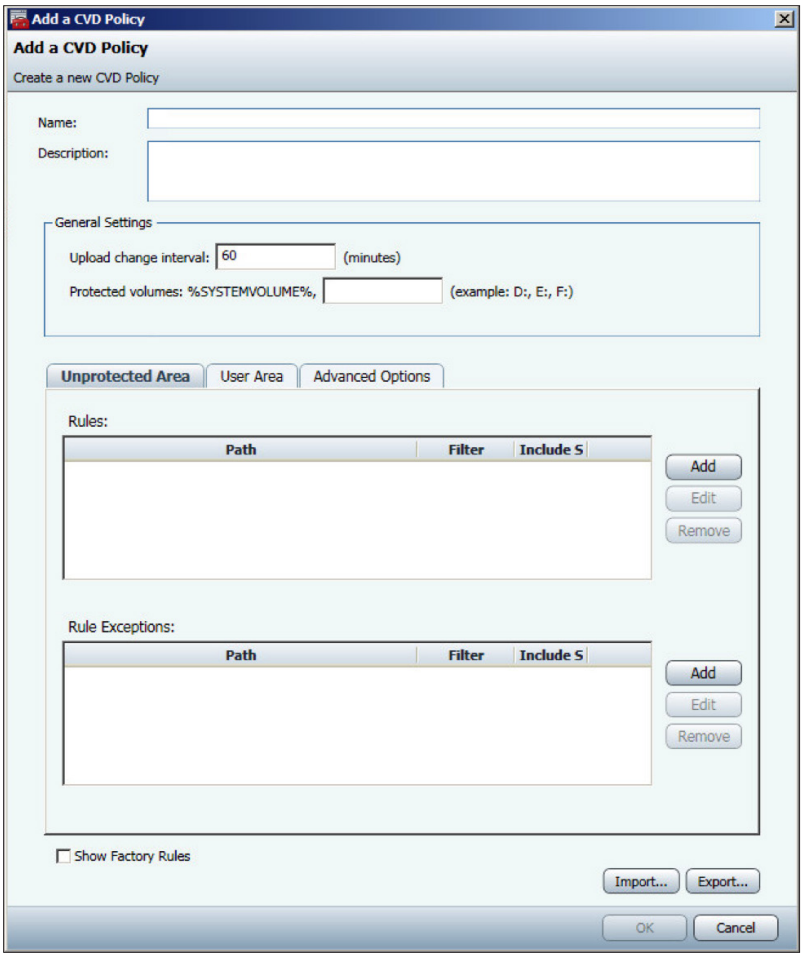
Create a CVD Policy for Layer Management

1. In the left pane of the Mirage Console, expand **System Configuration** and click **CVD Policies**.



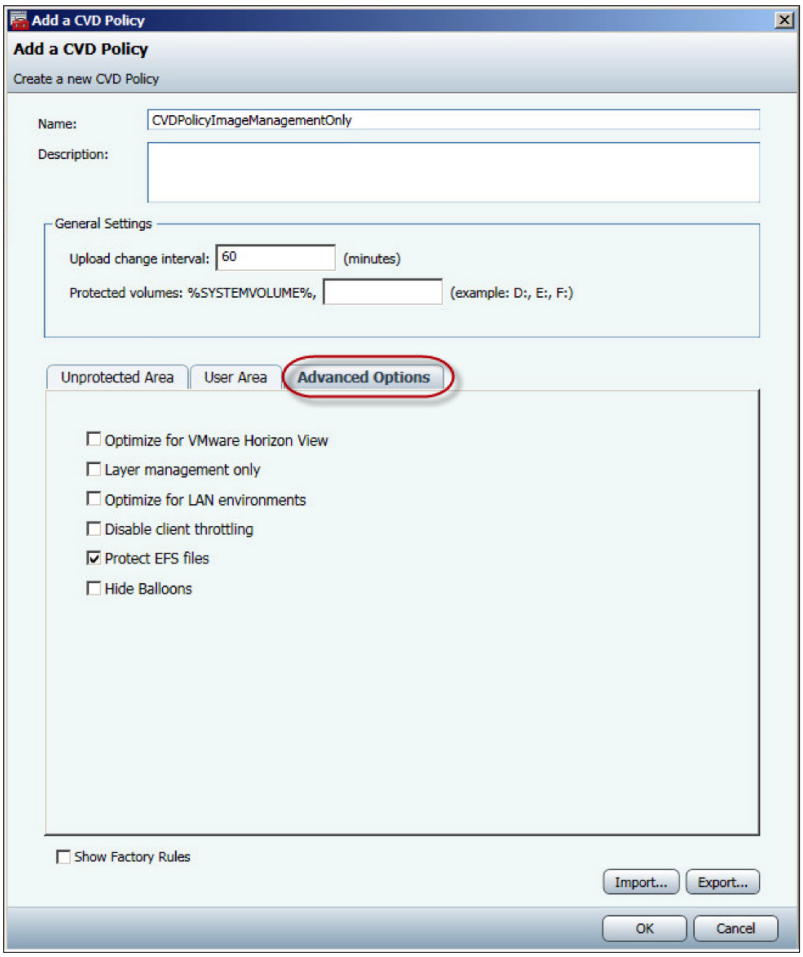
2. In the CVD Policies pane, click the **Add** icon.

The Add a CVD Policy page appears.



3. Name the policy.

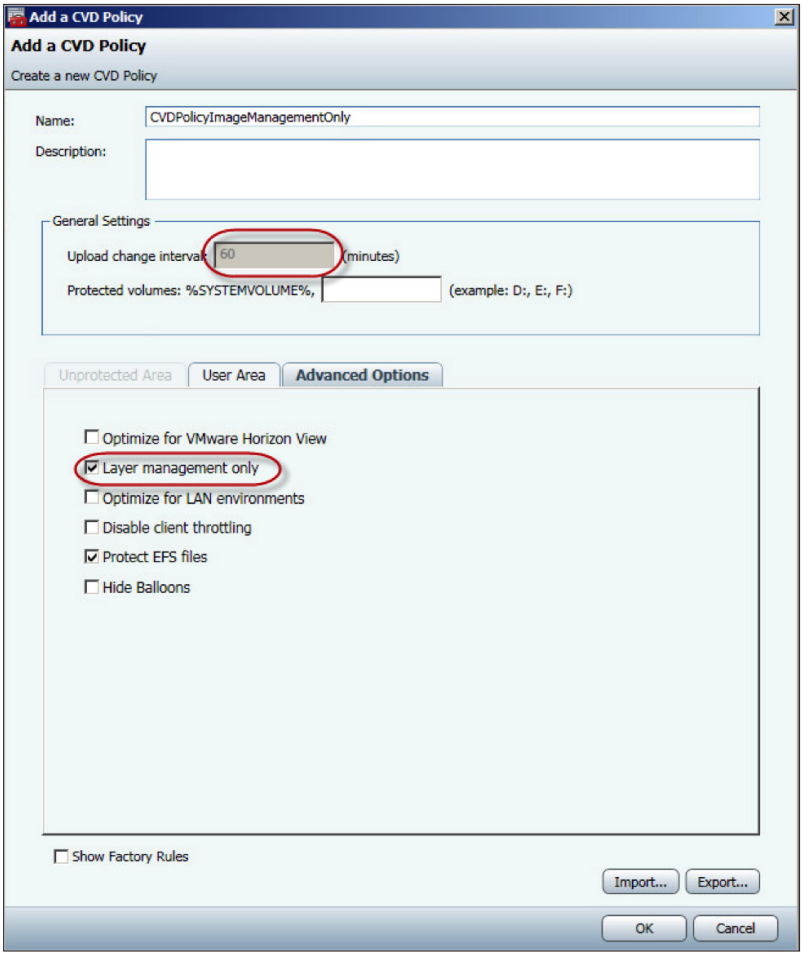
4. Click the **Advanced Options** tab.



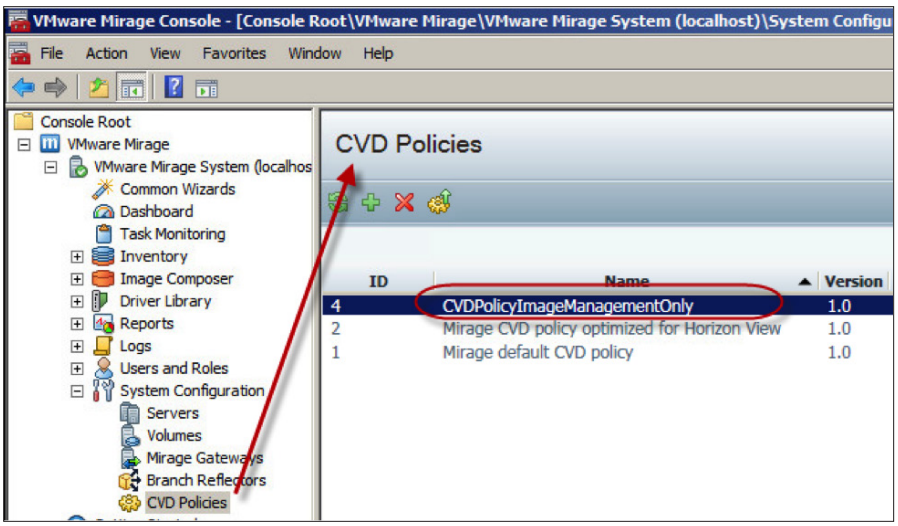
5. Select the **Layer management only** and **Optimize for VMware Horizon View** check boxes. Keep the **Protect EFS files** check box selected.

   Note that the value in the **Upload change interval** text box is dimmed, which means that the devices using this policy are not backed up.

   Click **OK**.



The policy is listed in the right pane.



Now that you have a policy for layer management, you can choose this policy when centralizing endpoints. After you centralize your endpoints with the policy, follow the instructions for assigning a base layer and capturing an app layer.

Integrating Mirage with VMware View Desktops

You can integrate Mirage 5.0 with View as demonstrated in the following tasks. You can use Mirage to manage persistent, full-clone pools, one of the pool types that you can create with View. Full-clone pools use a template to create the virtual desktops.

Prerequisites

The following tasks must be completed before integrating Mirage with View.

1. Create a Mirage environment.

   Mirage server, Mirage Management server, and the Mirage Console must be installed and configured properly. See Overview of Installation and Configuration.

2. Install View.

   View Connection Server must be properly installed.

3. Create a template virtual machine with the Mirage client, VMware View Agent®, and VMware Tools installed.

   Use vSphere to create this template virtual machine. Mirage manages the template virtual machine, and you use the template virtual machine to create a full-clone pool. After you create the template virtual machine, no connection exists between the template and the virtual desktops. As a result, you cannot use View to upgrade the system or applications on the virtual desktops, except by deleting and recreating them. Mirage enables you to upgrade the system and applications using layer management.

4. Centralize the template virtual machine to the Mirage server (see Centralizing Endpoints) and convert into a template. For converting the template virtual machine into a template, see Image Management for View Desktops using VMware Mirage.

5. Capture a base layer. See Capture the Base Layer from the Reference CVD.

6. Capture the app layers. See Capturing an App Layer.

   Best practice is to capture View Agent in a separate app layer. Capture other app layers according to your requirements.

Integrate View and Mirage

1. Create a dedicated full-clone pool, which is an automated pool that contains full virtual machines. See Setting Up Desktop and Application Pools in View.

2. Disable the full-clone pool. See Setting Up Desktop and Application Pools in View.

3. Centralize the View desktops.

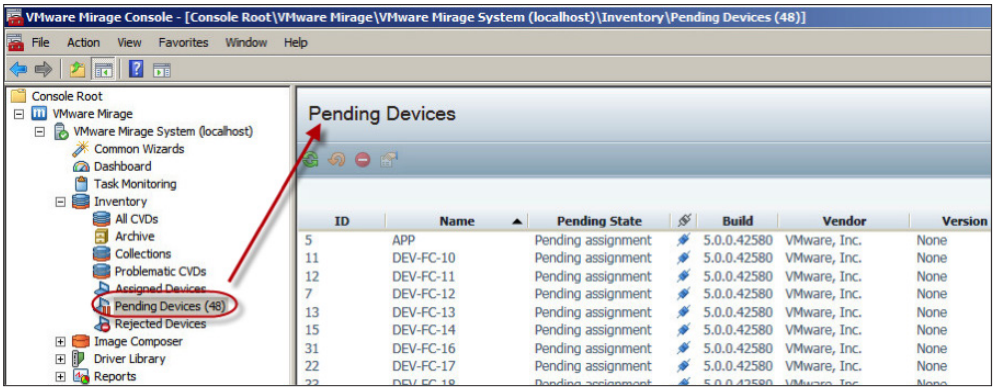
4. Enable a desktop pool and add entitlements. See the Setting Up Desktop and Application Pools in View.

5. Manage CVDs of View desktops. See Working with Base and Application Layers.

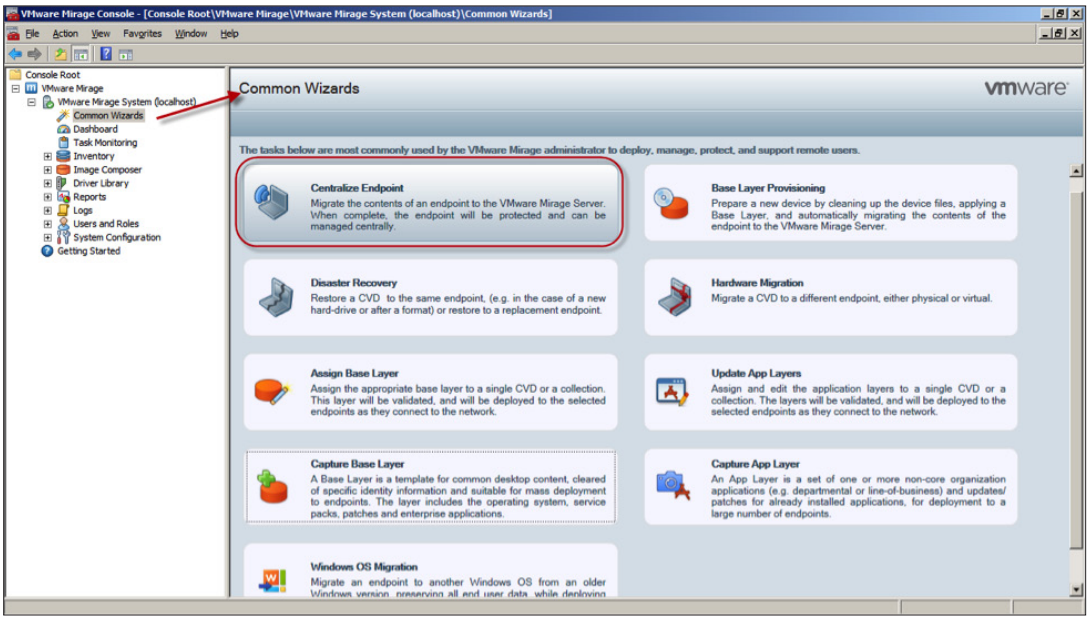
Centralize View Desktops

When the View desktops are created and available, go to the Mirage Console to check the pending devices.

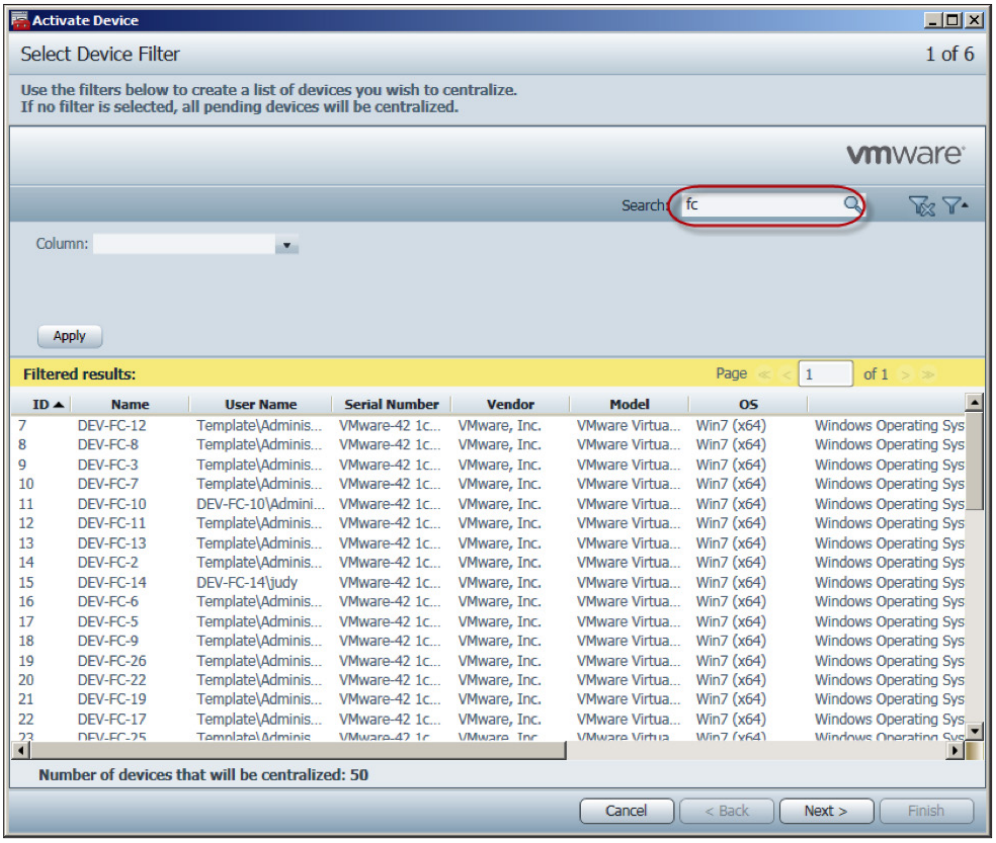
You can centralize these View desktops.



1. In the left pane of the Mirage Console, click **Common Wizards**, and in the right pane, select **Centralize Endpoint**.



The Select Device Filter page appears.

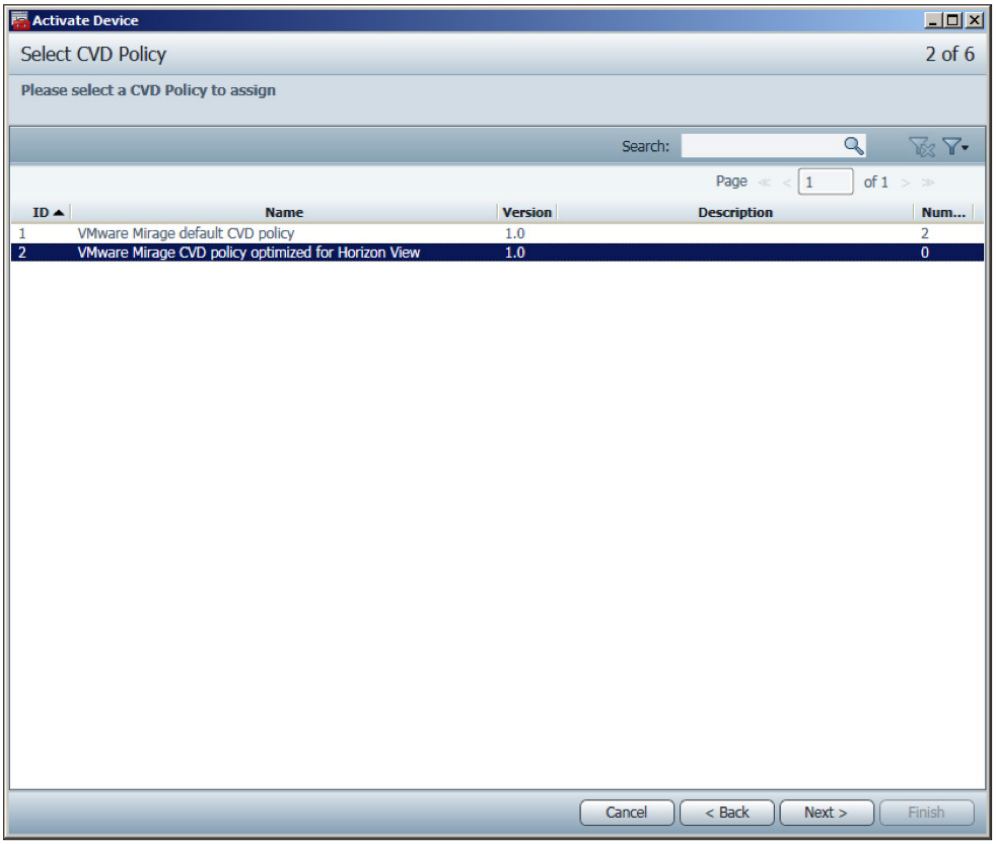


2. Use the search filter to locate the View desktops.

   For example, the names of the View desktops in this case all contain the string "fc," which you can use to filter them.

3. Click **Next**.

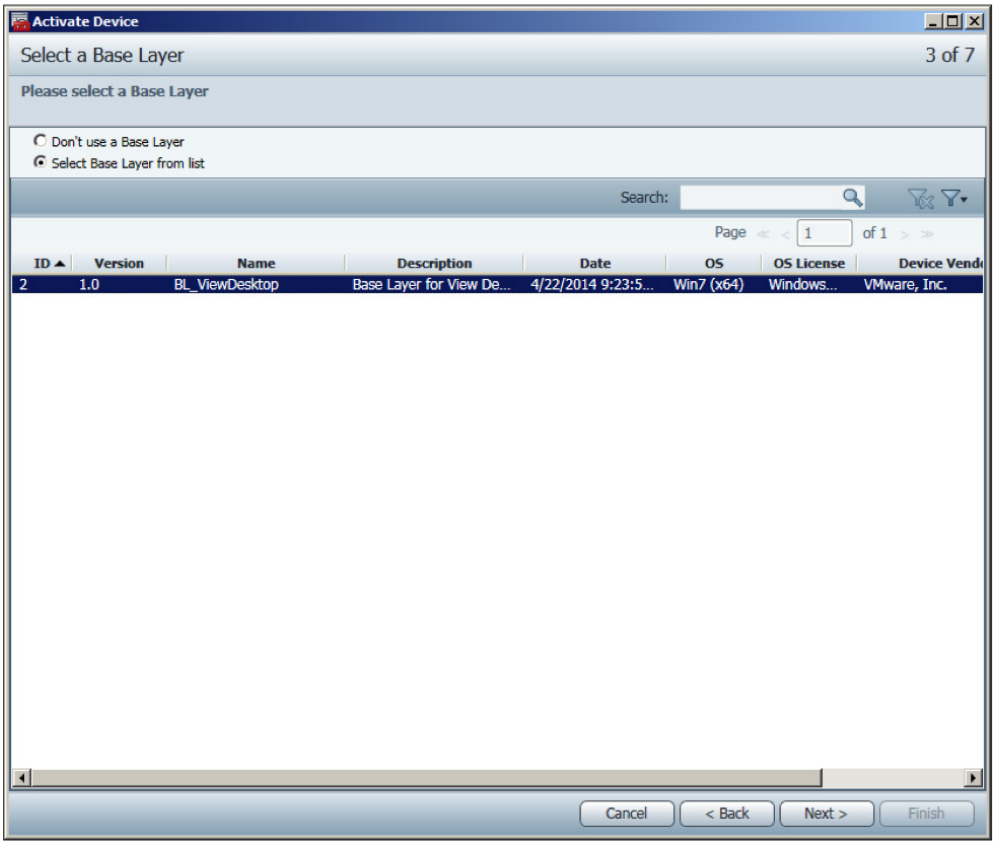
The Select CVD Policy page appears.



4. Select VMware Mirage CVD policy optimized for Horizon View and click **Next**.

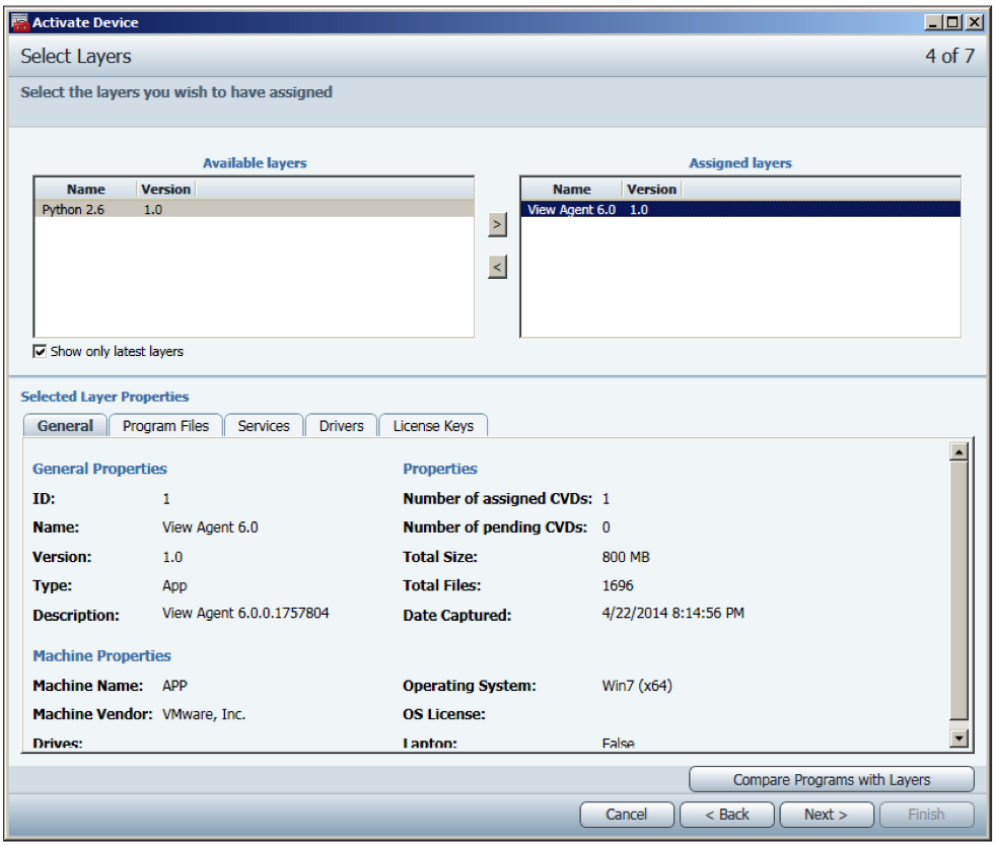
   This policy indicates that the desktops you apply this policy to are not backed up. You can still apply a base layer and app layers to the desktops. You can select the VMware Mirage default CVD policy, but performance will be adversely affected in most View implementations.

The Select a Base Layer page appears.



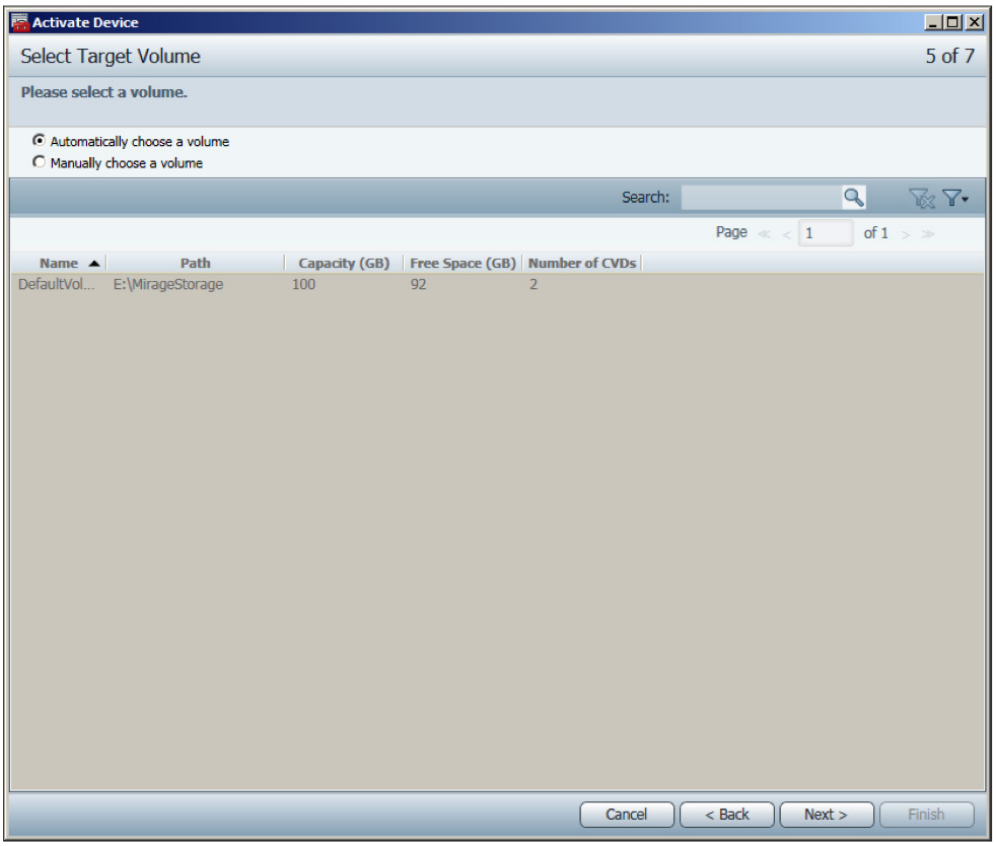
5. Select the base layer you captured previously and click **Next**.

The Select Layers page appears.



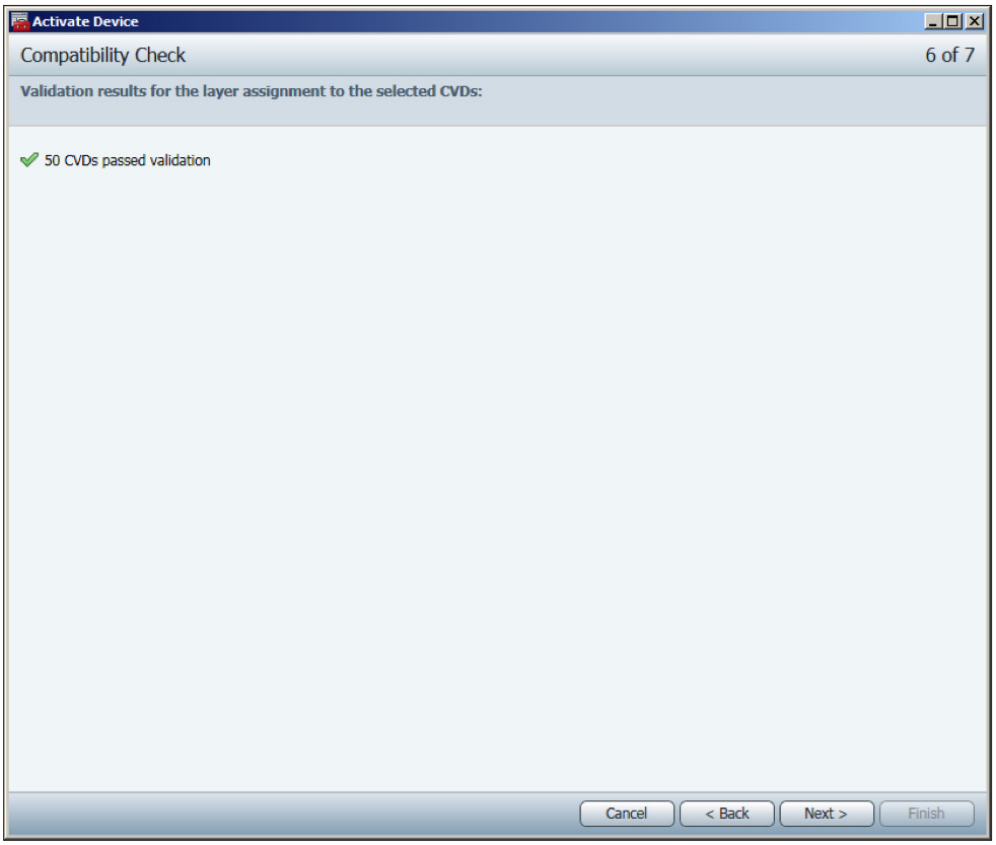
6. Select the app layer with the View Agent and click **Next**.

The Select Target Volume page appears.



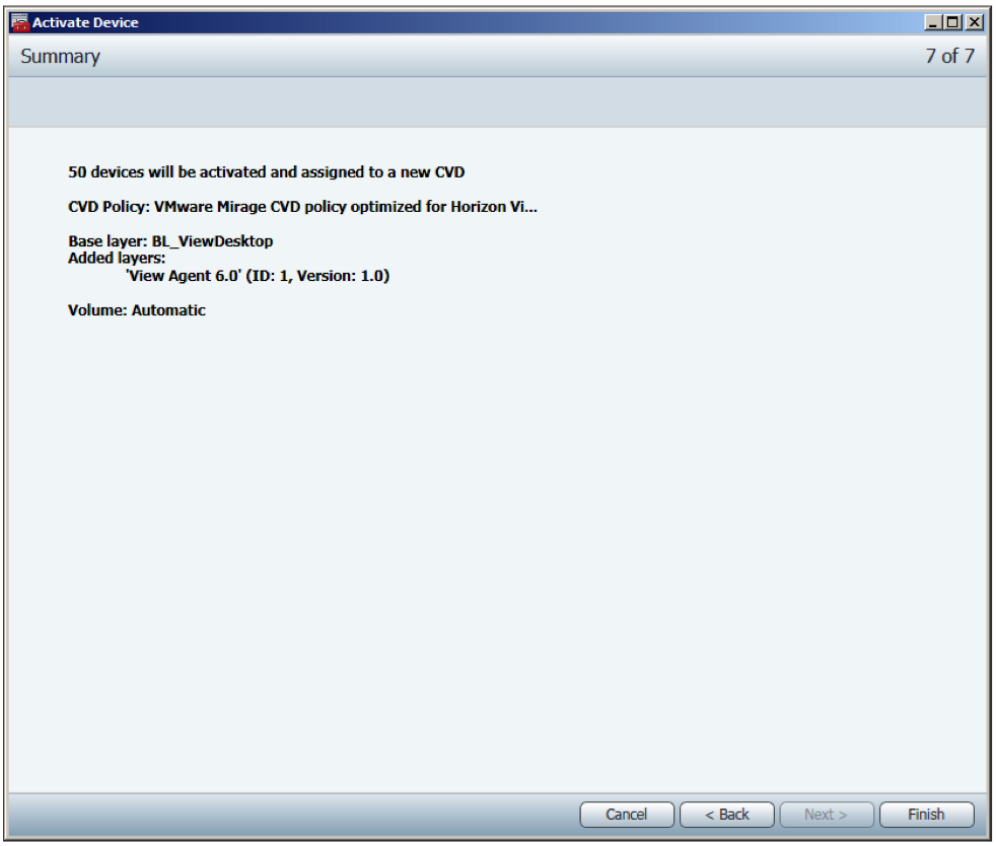
7. Choose how to select the volume and click **Next**. If you select **Manually choose a volume**, specify a volume.

The Compatibility Check page appears.



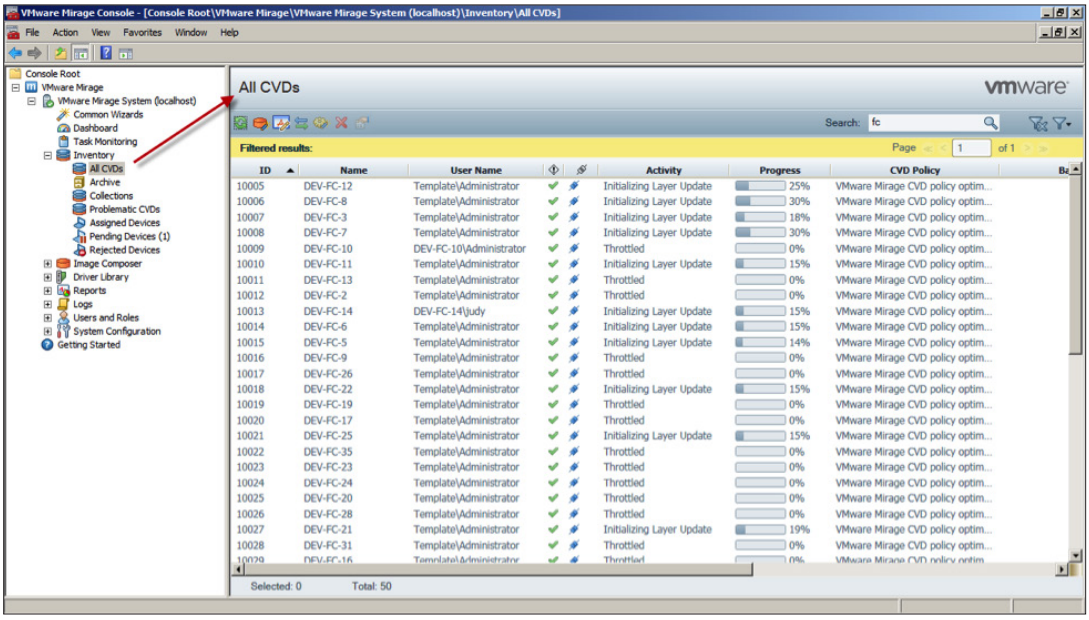
8. Click **Next**.

The Summary page appears.



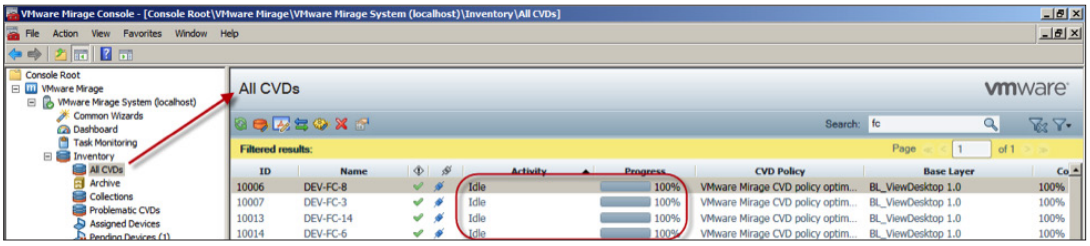
9. Click **Finish**.

10. In the left pane, expand **Inventory** and click **All CVDs**, and in the right pane, monitor the progress on the All CVDs page.

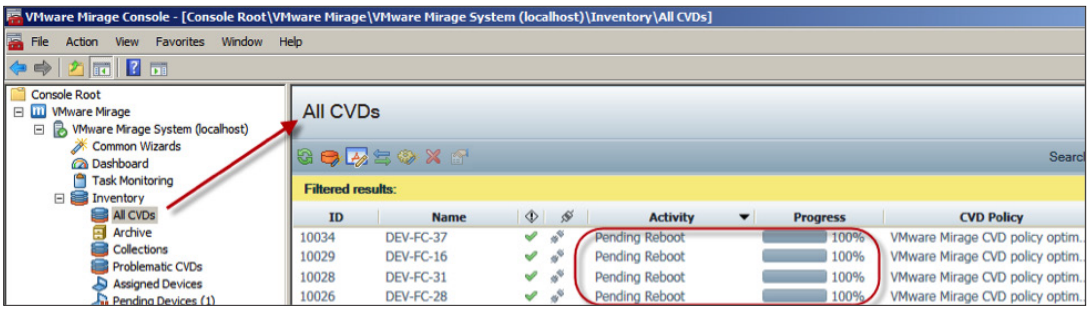


Mirage often starts centralization against some devices while leaving others with an Activity value of Throttled. This behavior saves resources and speeds the progress.

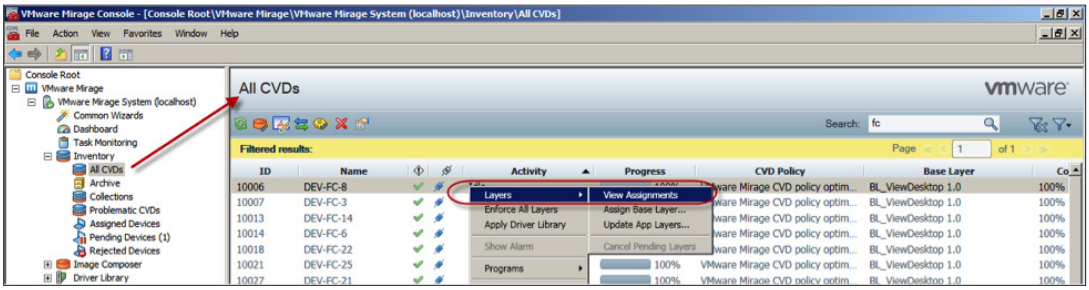
The centralization process ends when the activity of the CVD changes to Idle.



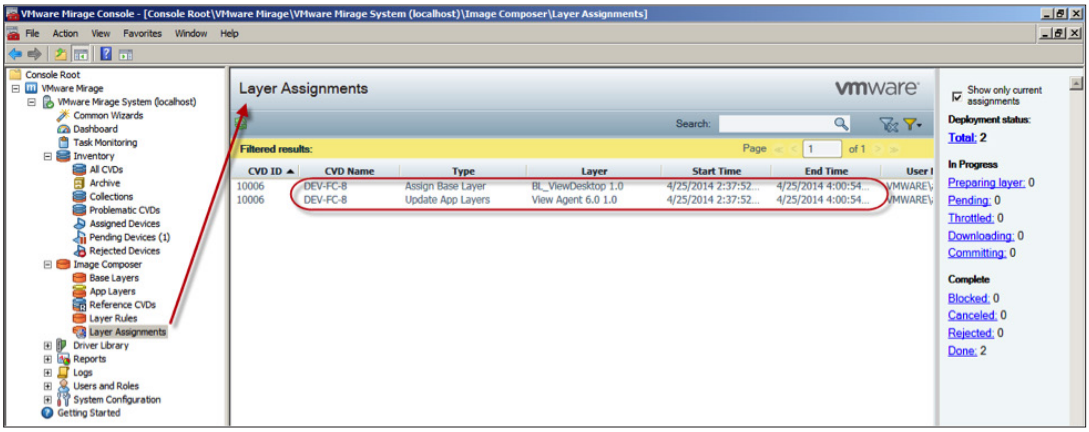
11. If the endpoint device must be rebooted, access the endpoint device and restart it.



12. (Optional) To view the CVD assignment, wait for the Activity value to change to Idle, right-click the CVD, and select **Layers** > **View Assignments**.



The Mirage Console switches to the Layer Assignments page, where the assigned base layer and app layer are listed.



The View desktops are centralized and ready for end users to access.

Working with the Mirage Gateway

The Mirage Gateway, previously called Mirage Edge Server, is a component of Mirage 5.0. With the Mirage Gateway, remote end users can securely connect their devices back to the corporate network where Mirage is centrally located, without going through a VPN.

Prerequisites

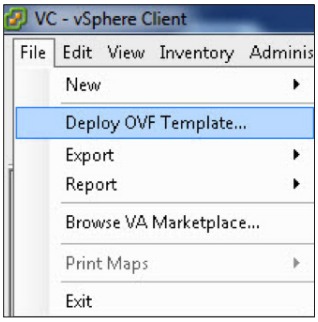
To configure the Mirage Gateway, the Mirage server must be installed, and the LDAP server that the Mirage server belongs to must be accessible. You need a signed SSL server certificate with a private key. The format of the certificate can be PEM or PFX.

Deploy the Mirage Gateway Virtual Appliance

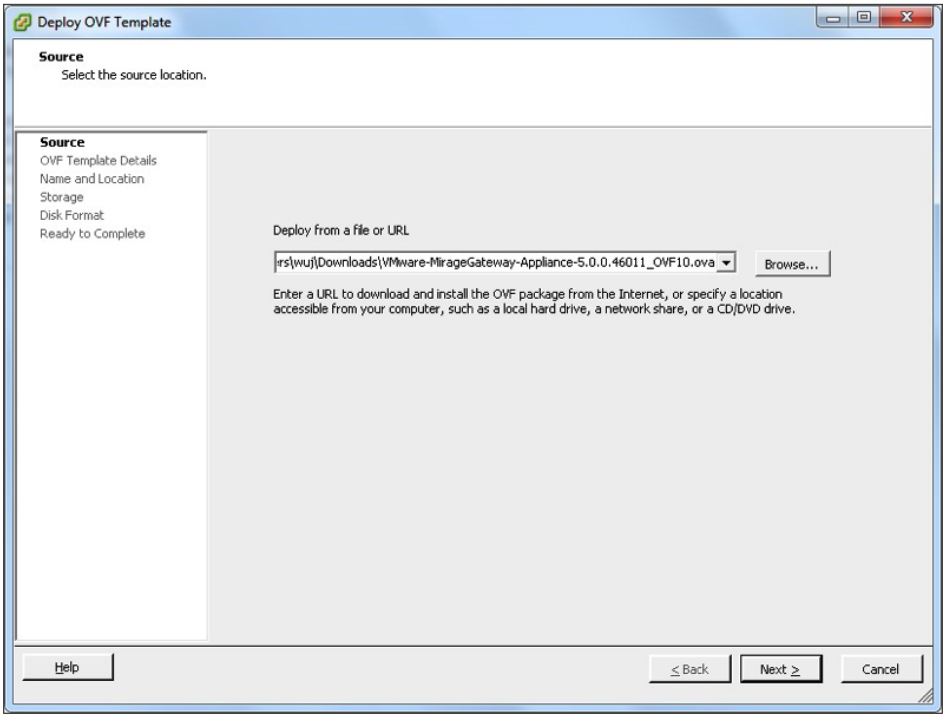
1. Download Mirage Gateway.

   See Download VMware Horizon Mirage. The filename pattern is `VMware-MirageGateway-Appliance-x.y.z.nnnnn_OVF10.ova`, where *x.y.z* is the Mirage version number, and *nnnnn* is the Mirage build number.

2. Use VMware vSphere Client™ to access your VMware ESXi™ server or VMware vCenter Server™ and select **File** > **Deploy OVF Template**.

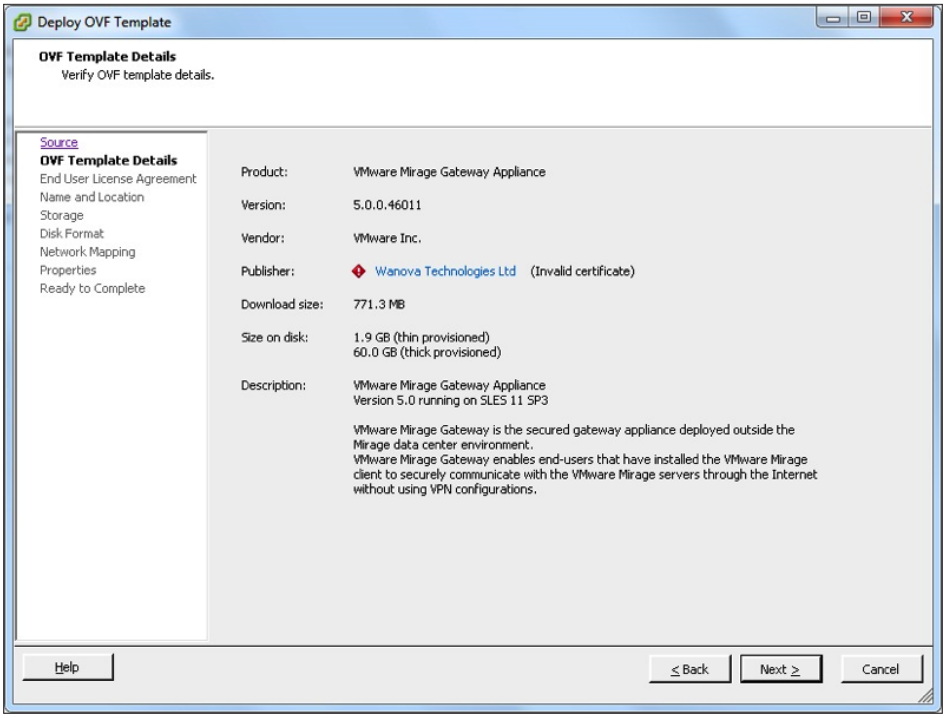


   The Deploy OVF Template window appears.



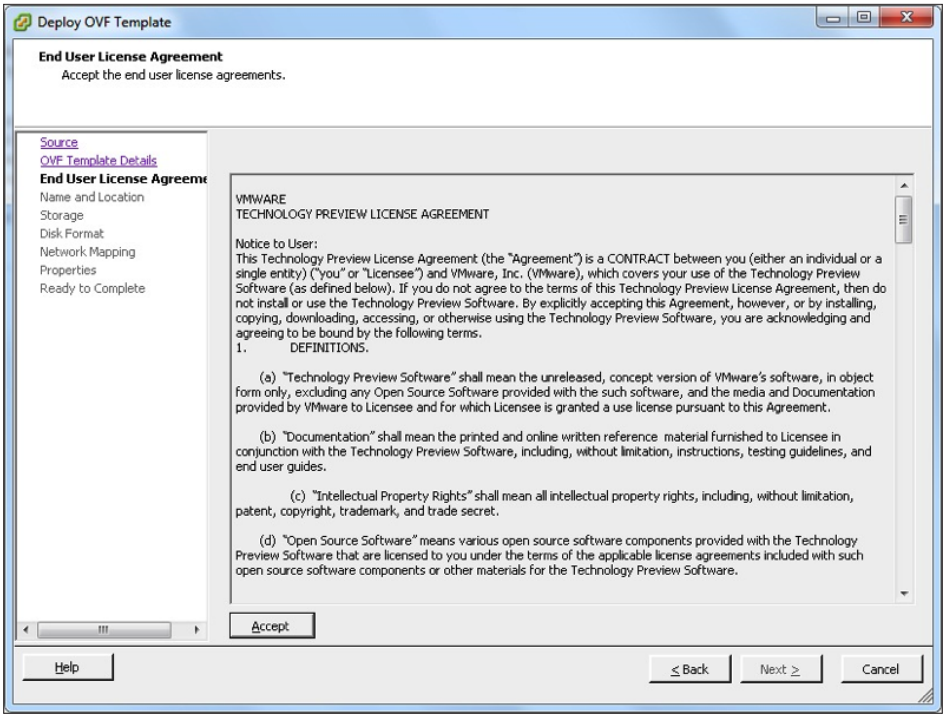
3. Enter the URL or file location of the Mirage Gateway OVA file and click **Next**.

   The OVF Template Details page appears.



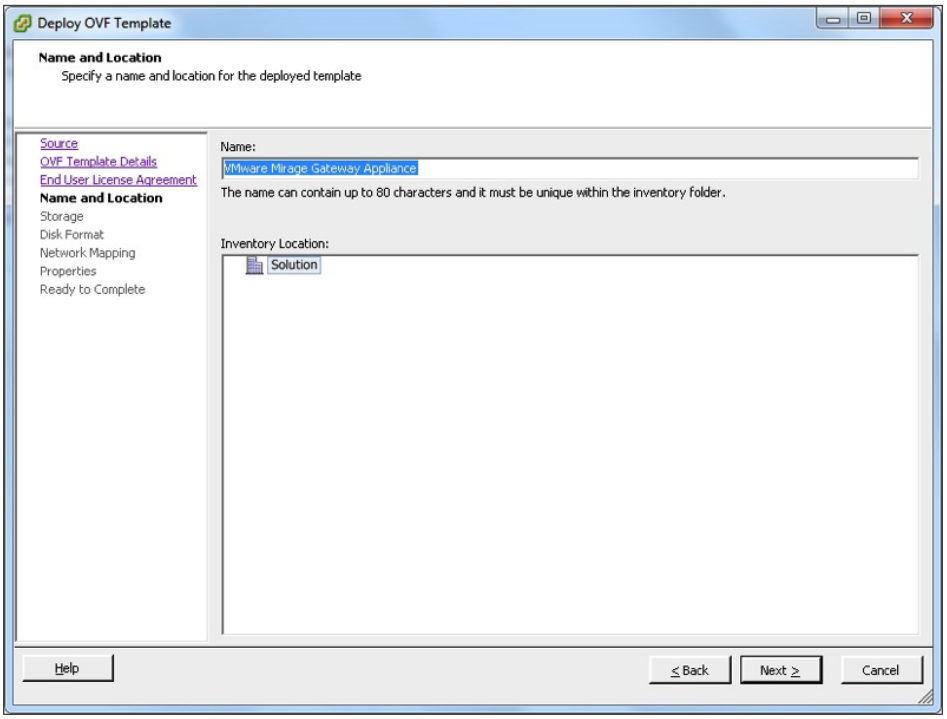
4. Click **Next**.

   The End User License Agreement page appears.



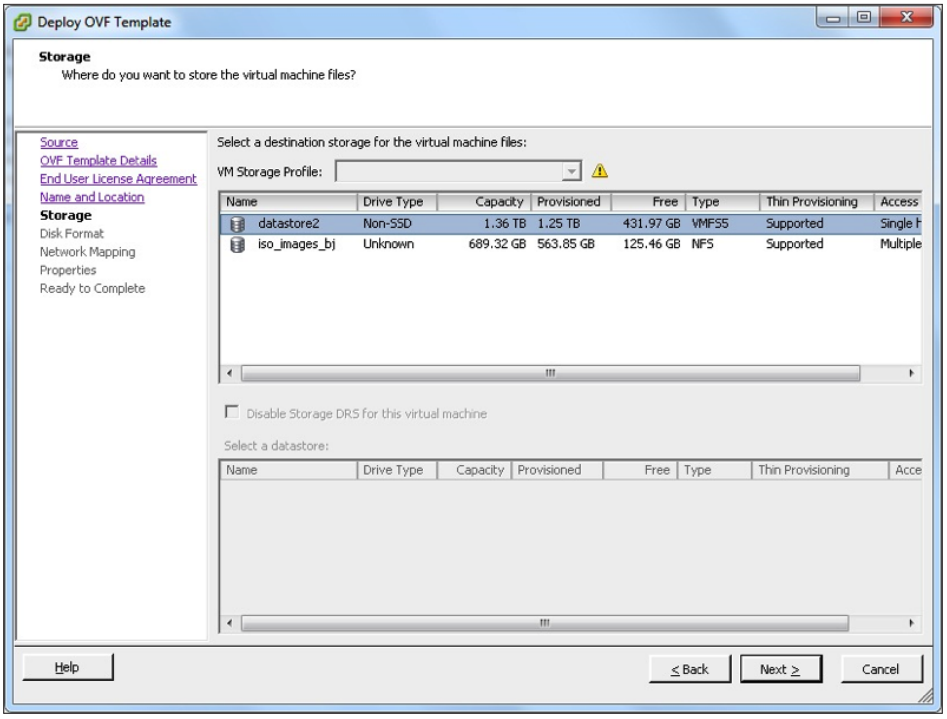
5. Click **Accept** and click **Next**.

   The Name and Location page appears.



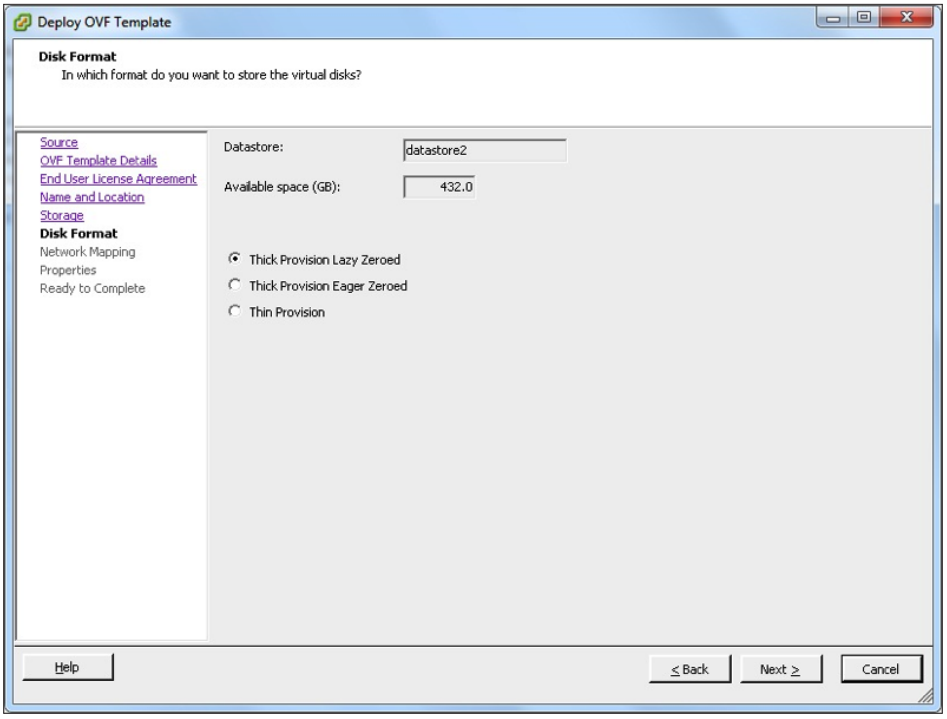
6. Enter a name for the Mirage Gateway, select a location, and click **Next**.

   The Storage page appears.



7. Select storage for the virtual machine and click **Next**.

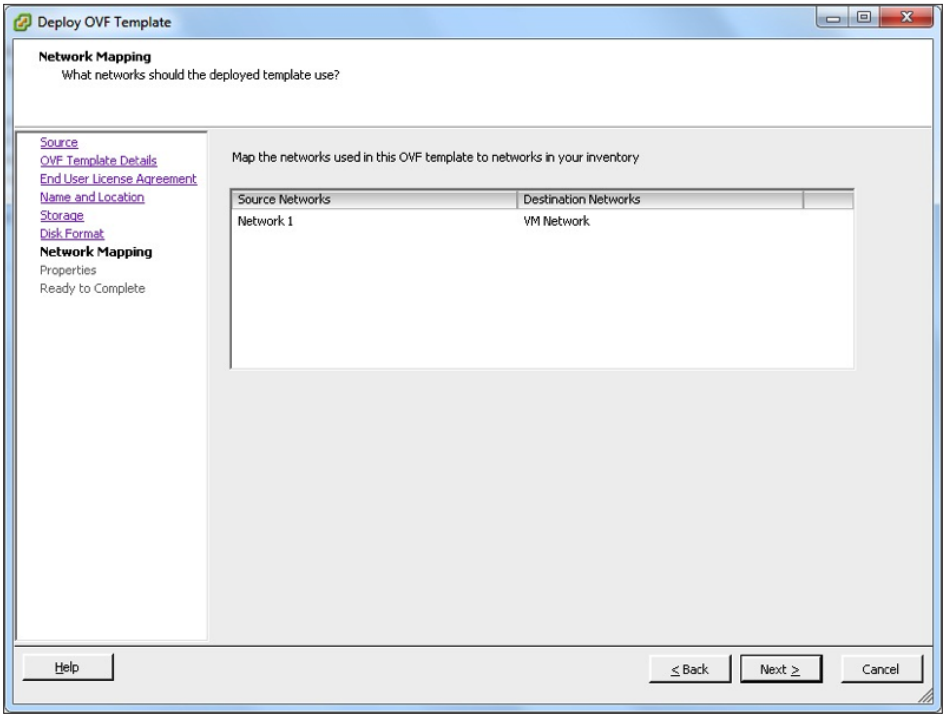
   The Disk Format page appears.



8. For this exercise, use the default selection for the disk format and click **Next**.

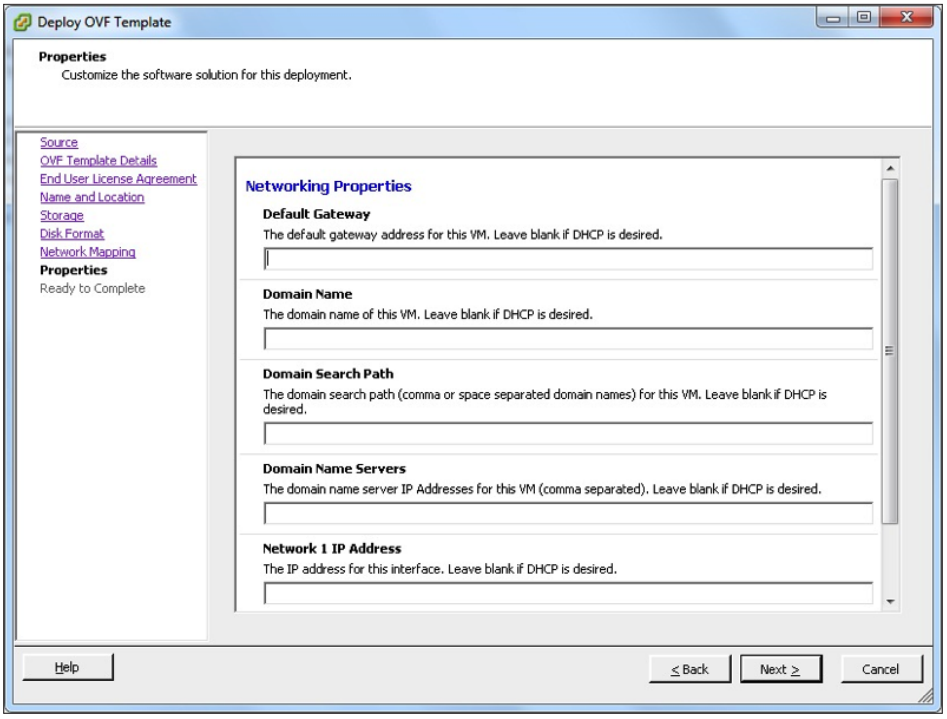
   In a production environment, select the disk format that meets your requirements.

   The Networking Mapping page appears.



9. Select the network adapter that meets your requirements and click **Next**.

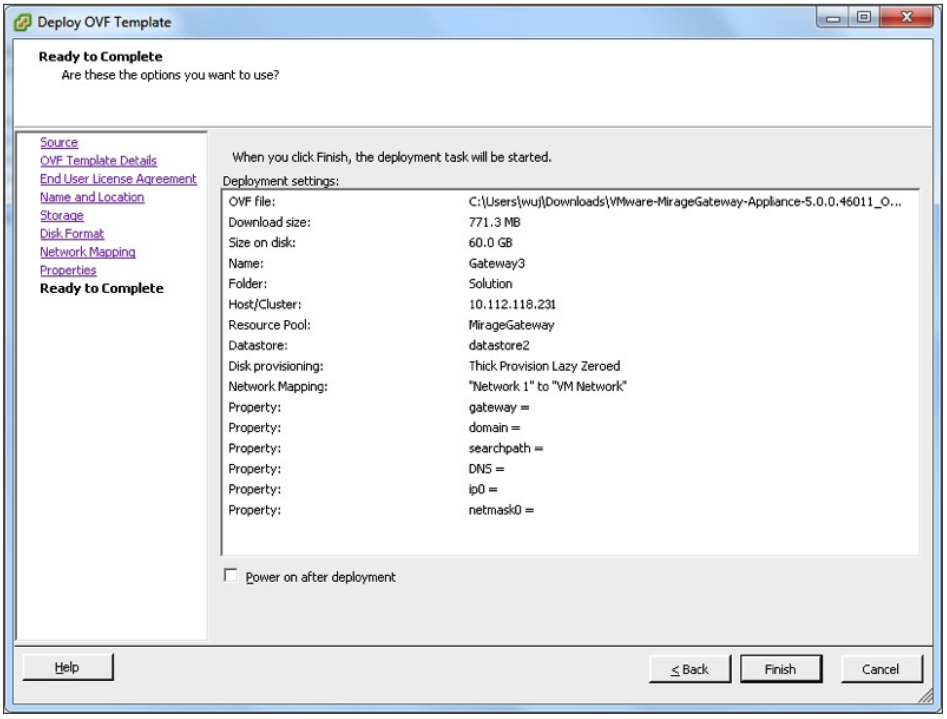
   The Properties page appears.



10. For this exercise, use the blank default settings and click **Next**.

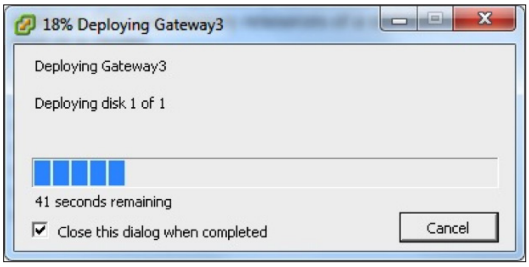
    In a network environment, configure the properties to meet your requirements.

    The Ready to Complete page appears.



11. Click **Finish**.

    The Deploying window appears.



You have deployed the Mirage Gateway virtual appliance and are ready to install Mirage Gateway.

Install the Mirage Gateway

Perform this task on the virtual machine that you just deployed.

1. Log in to the virtual machine that you deployed.

   The default password for the root user is **vmware**.

2. Copy the SSL server certificate to the virtual machine.

3. Install and configure the Mirage Gateway with the following script.
   `/opt/MirageGateway/bin/install.sh`

4. Specify the LDAP or LDAPs to use to connect to the LDAP server.

```
Welcome to Mirage Gateway configuration tool.
Use the wizard to configure Mirage Gateway. Press "Enter" to accept the default
settings.
    To exit the configuration tool at any time and discard changes, press CTRL+C
.
    It is recommended to review the Installation Guide before configuring the Mi
rage Gateway.
Step 1 of 14: Type the LDAP type (1 for LDAP, 2 for LDAPS): (default: ldap)
```

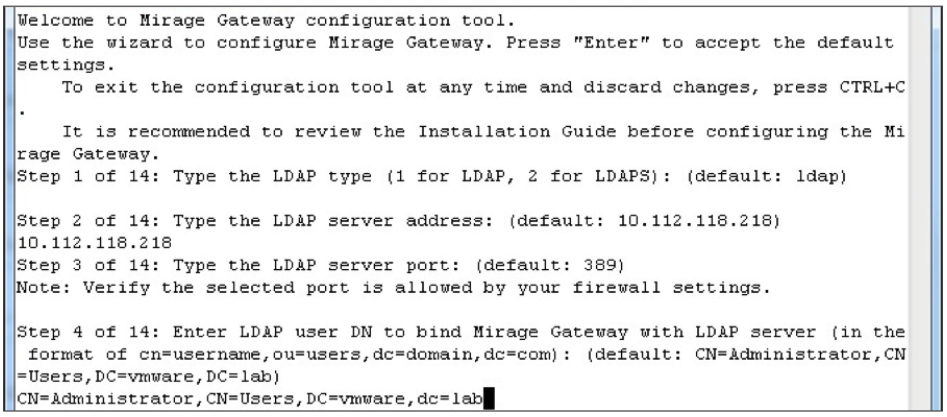
5. Type the LDAP server address, and press Enter.

```
Welcome to Mirage Gateway configuration tool.
Use the wizard to configure Mirage Gateway. Press "Enter" to accept the default
settings.
    To exit the configuration tool at any time and discard changes, press CTRL+C
.
    It is recommended to review the Installation Guide before configuring the Mi
rage Gateway.
Step 1 of 14: Type the LDAP type (1 for LDAP, 2 for LDAPS): (default: ldap)

Step 2 of 14: Type the LDAP server address: (default: 10.112.118.218)
10.112.118.218
```

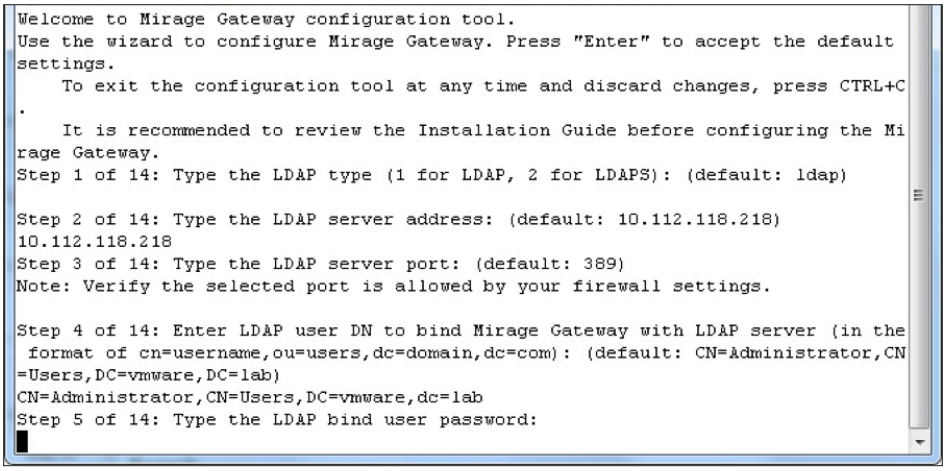
6. Type the LDAP server port, and press Enter.

```
Welcome to Mirage Gateway configuration tool.
Use the wizard to configure Mirage Gateway. Press "Enter" to accept the default
settings.
    To exit the configuration tool at any time and discard changes, press CTRL+C
.
    It is recommended to review the Installation Guide before configuring the Mi
rage Gateway.
Step 1 of 14: Type the LDAP type (1 for LDAP, 2 for LDAPS): (default: ldap)

Step 2 of 14: Type the LDAP server address: (default: 10.112.118.218)
10.112.118.218
Step 3 of 14: Type the LDAP server port: (default: 389)
Note: Verify the selected port is allowed by your firewall settings.
```

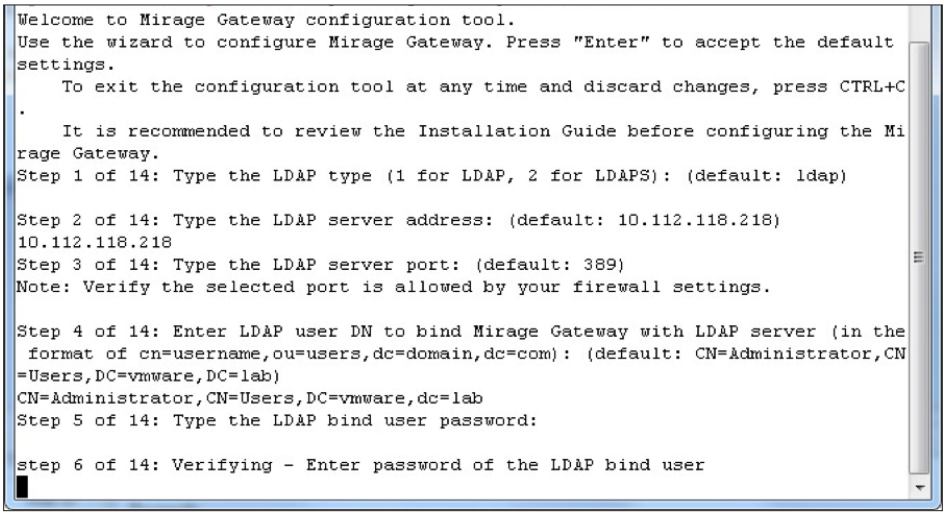
7. Type the LDAP user domain name, and press Enter.



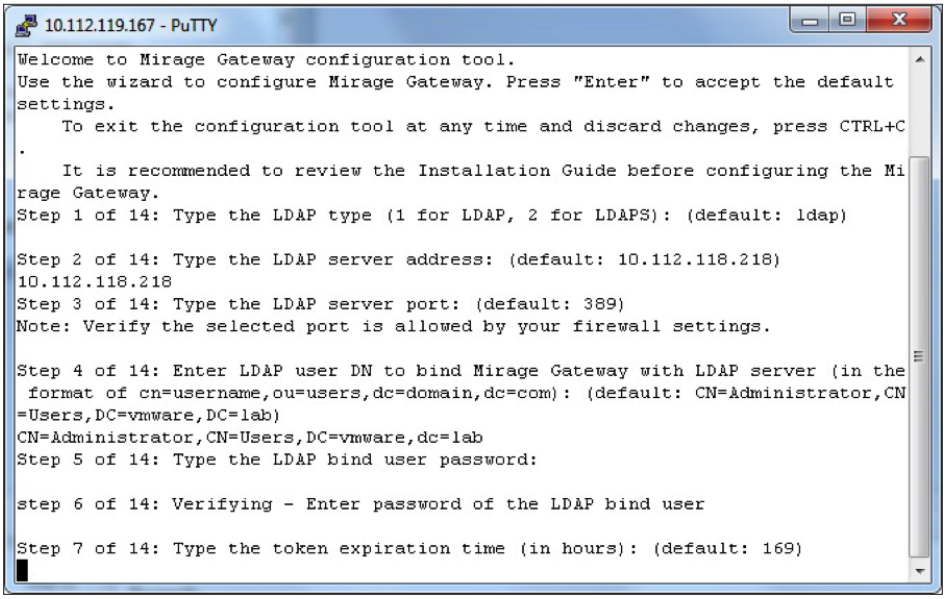
8. Type the password of the LDAP bind user, and press Enter.



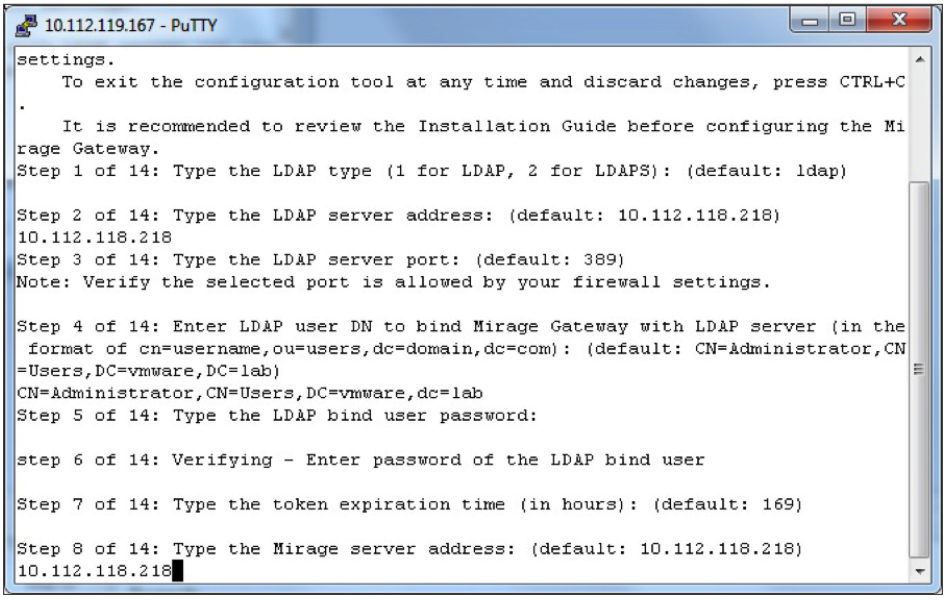
9. Retype the password of the LDAP bind user, and press Enter.



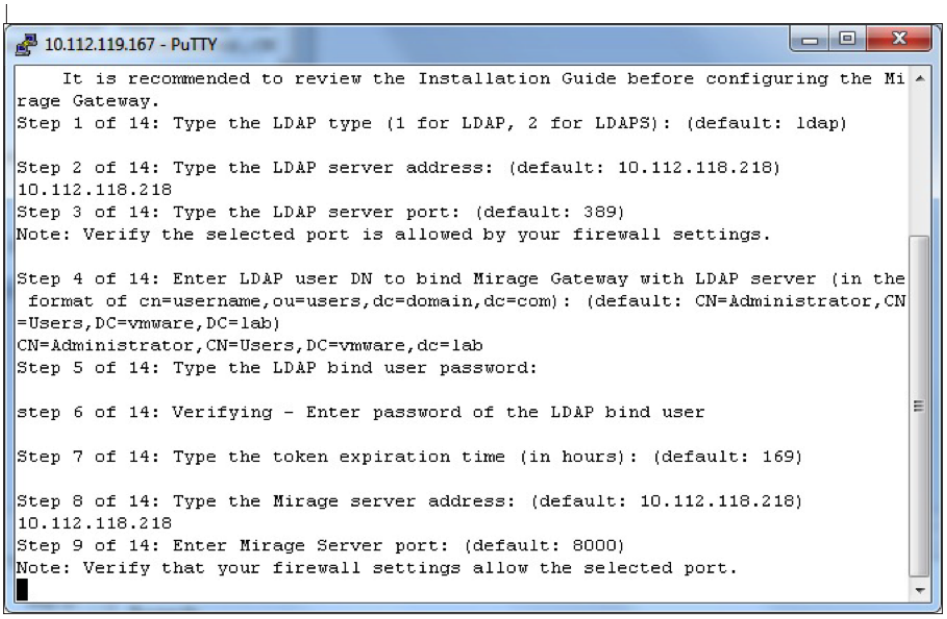
10. Specify the token expiration time in hours, and press Enter. This is the time period after which remote end users are requested to log in to the Mirage Gateway again.



11. Type the Mirage server address, and press Enter.

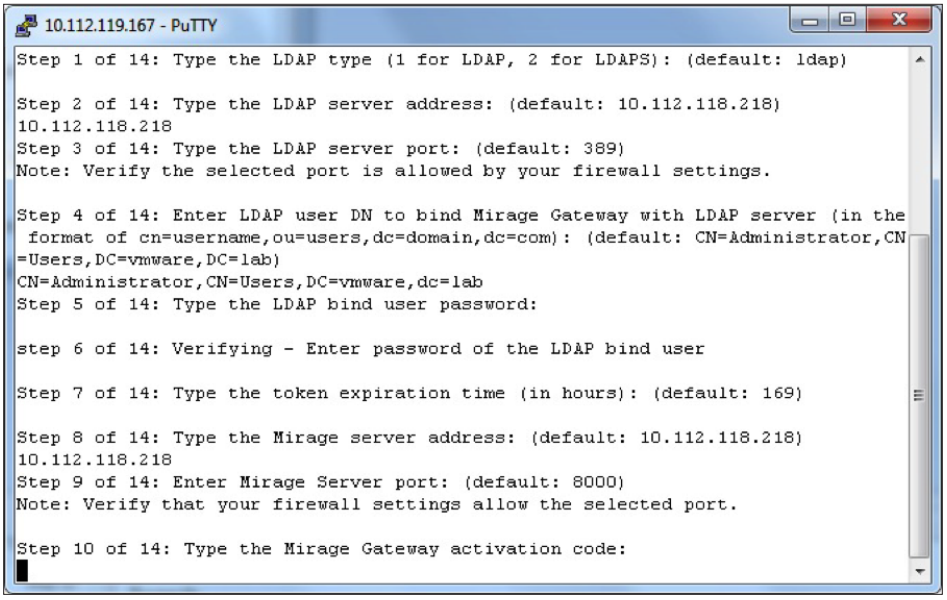


12. Specify the Mirage server port, and press Enter. Make sure that the port is allowed on your Mirage server.

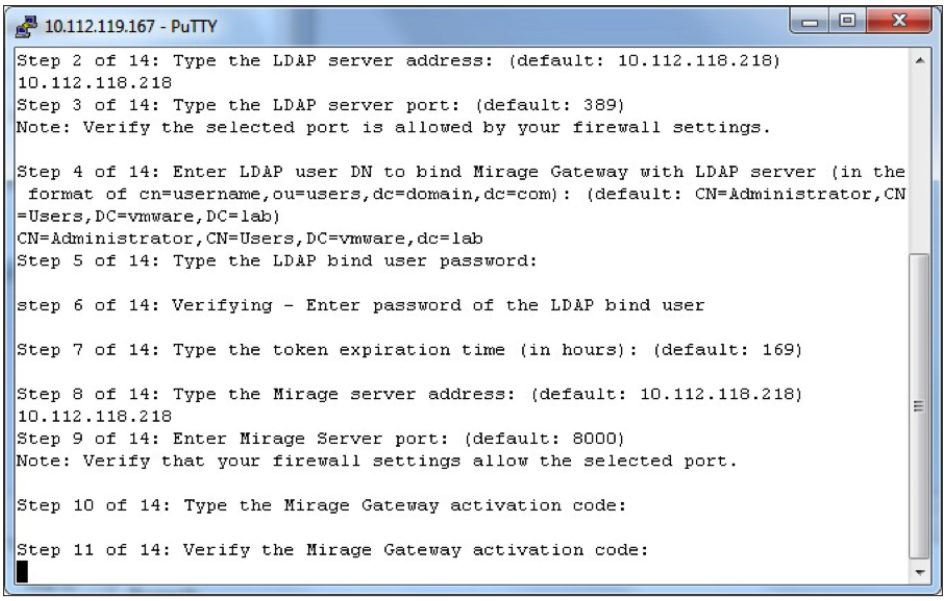


13. Enter the Mirage Gateway Activation Code, and press Enter.

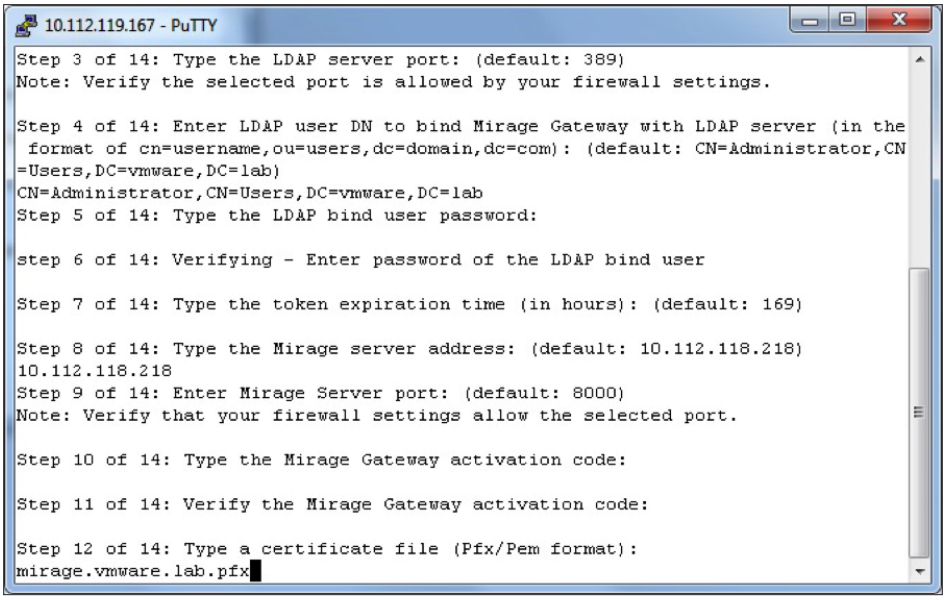
    The Mirage Gateway uses this activation code to authenticate itself against the Mirage server, which enables the Mirage Management server to add the configurations of the Mirage Gateway to the Mirage Console.



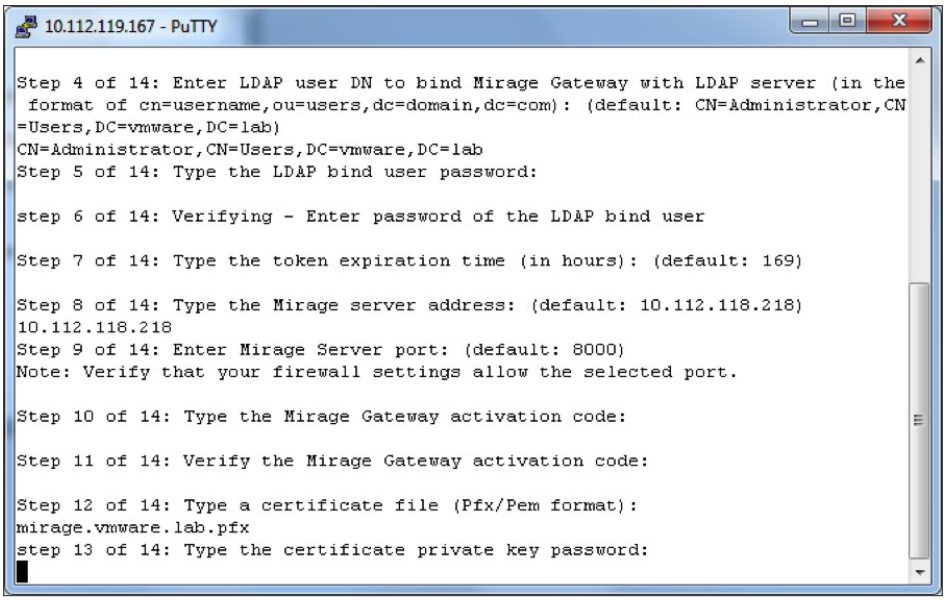
14. Retype the Mirage Gateway Activation Code, and press Enter.



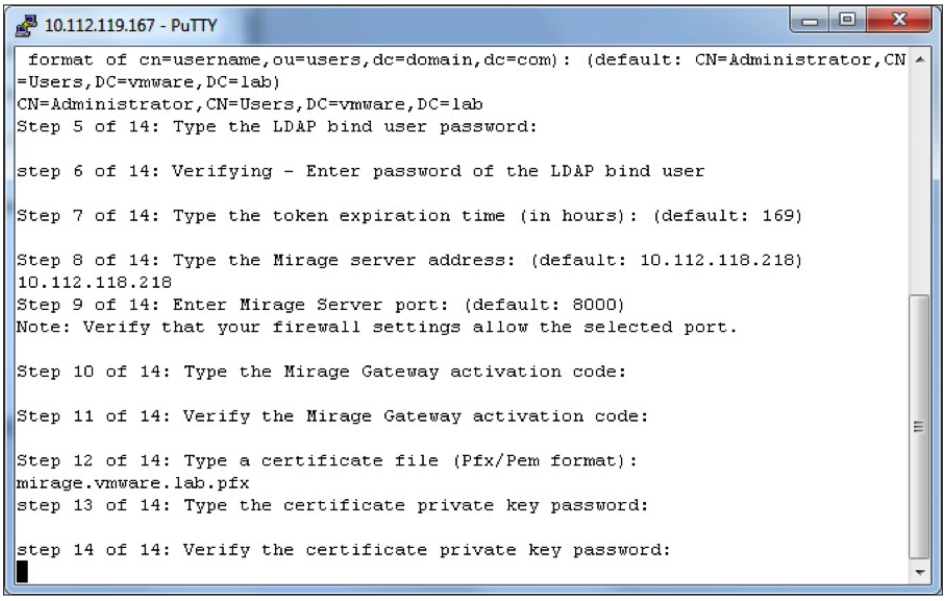
15. Enter the file name of the prepared SSL certificate, and press Enter.



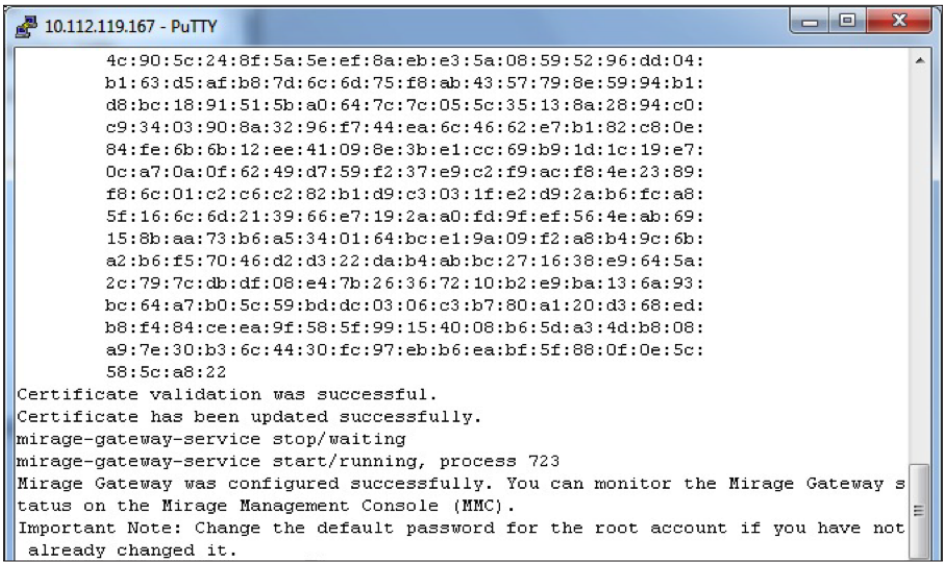
16. Enter the password for the certificate private key, and press Enter.



17. Retype the password, and press Enter.



The wizard displays the results.



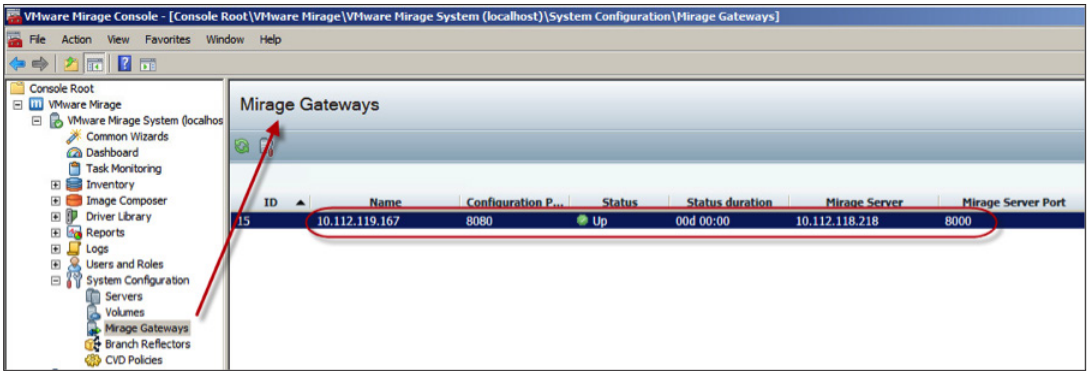
18. (Optional) To check the status of the Mirage Gateway service, use the following command.

```
~ # service mirage-gateway-service status
```

An example result is:

```
mirage-gateway-service start/running, process 1156
```

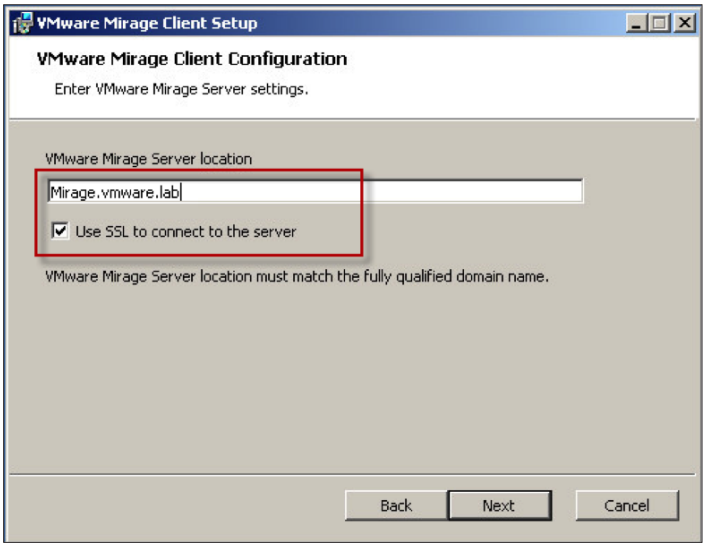
19. In the Mirage Console, check that the status of the installed Mirage Gateway is Up.



The Mirage Gateway is installed and ready to be connected.

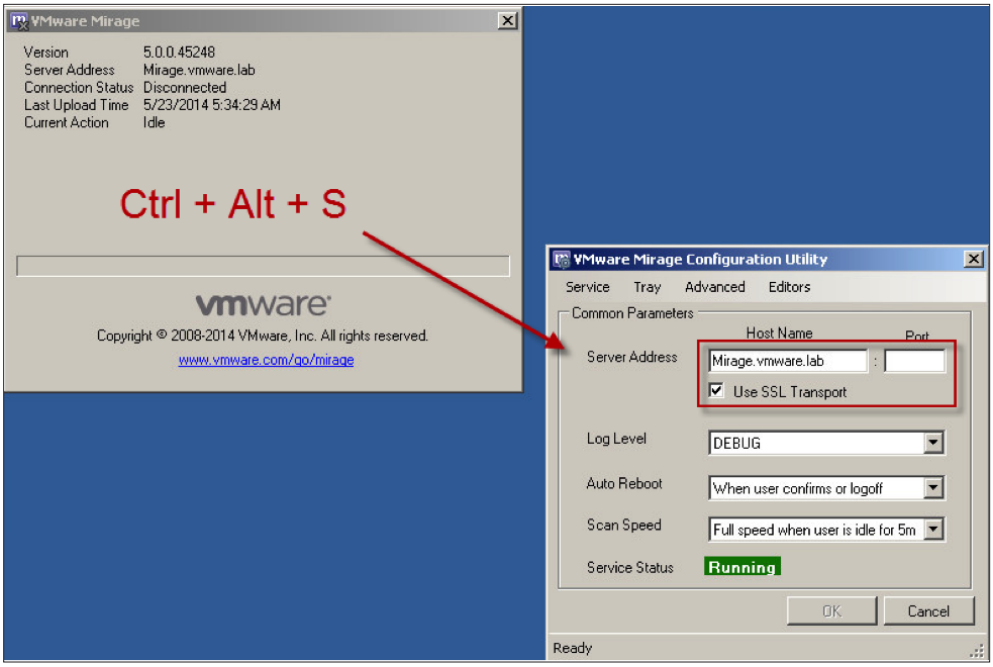
Connect the Mirage Client to the Mirage Gateway

If the Mirage client is not installed on your test machine, see Install the Mirage Client on the Test Machines. Select **Use SSL to connect to the server** option during installation to connect your client to the Mirage Gateway.

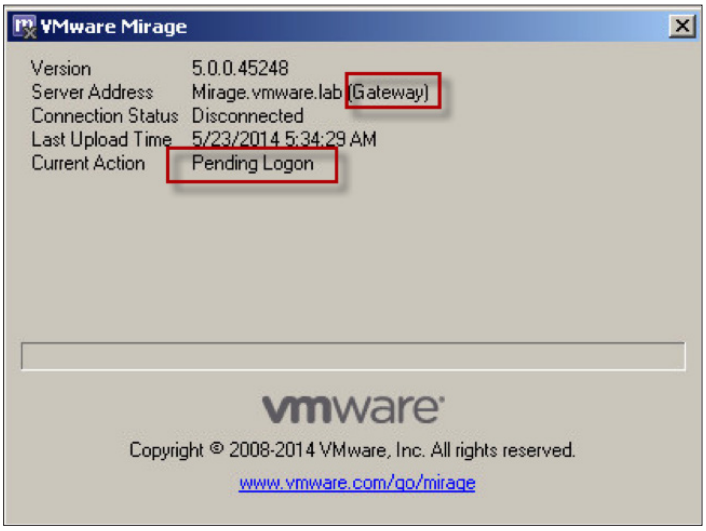


If the Mirage client is installed on the test machine, but you did not select this option during installation, use the configuration utility to change it.

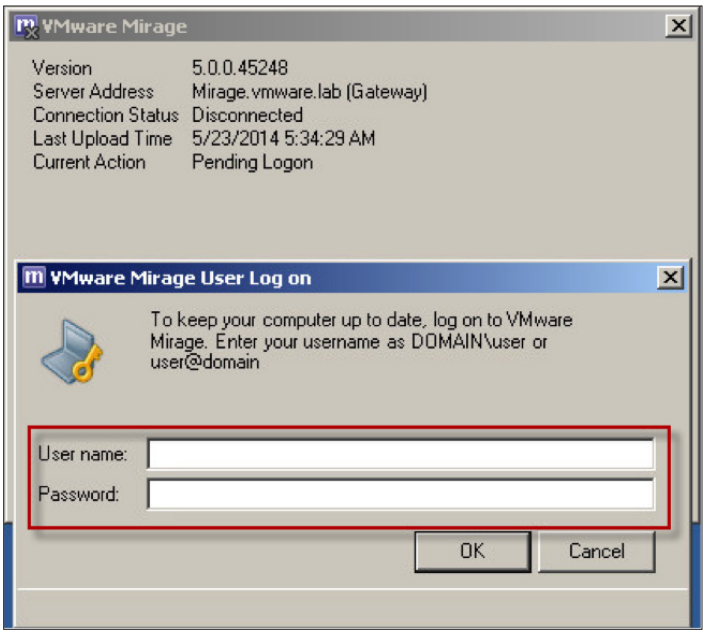
1. From the Mirage client window, press Ctrl+Alt+S to open the VMware Mirage Configuration Utility.
2. Make your changes and click **OK**.



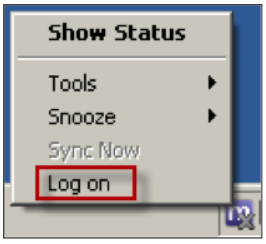
When the client connects to the Mirage Gateway successfully, the status on the Mirage client window is Pending Logon.



3. Provide your login credentials when prompted.



If you accidentally close the login dialog box, right-click the Mirage icon on the system tool bar and select **Log on**.



Note: Because the endpoint connects to the Mirage Gateway rather than to the Mirage server, the Mirage server is not aware of the existence of the endpoint. In addition, the administrator cannot see the endpoint in the Mirage Console Pending Devices list. As a result, the centralization process is started only after the user logs in to the Mirage Gateway.

After providing the correct login information, the Current Action setting of the Mirage client changes to Pending Assignment, and the Mirage Console displays the endpoint in the Pending Devices list. If the Enable automatic CVD Creation option is enabled in the Mirage Console, the device is assigned, and centralization starts accordingly. If the option is disabled, make sure that you are logged in as the administrator to complete the assignment. Until then, the endpoint stays in Pending Assignment state.

Additional Resources

VMware Mirage product Web page

VMware Mirage evaluation Web page

VMware Mirage Community Forum

VMware End-User Computing Blog

VMware Mirage product documentation

About the Author and Contributors

John Domenichini, Senior Technical Writer, and Judy Wu, Solution Engineer in End-User Computing at VMware, wrote this document.

The following individuals contributed content to this guide:

• Stephane Asselin, Architect, End-User Computing, VMware

•Tina de Benedictis, Group Manager, Technical Marketing Content, End-User Computing, VMware

• Sachin Sharma, Product Marketing Manager, End-User Computing, VMware

• Hanan Stein, Senior Product Line Manager, End-User Computing, VMware

To comment on this paper, contact the VMware End-User Computing Solutions Management and Technical Marketing team at twitter.com/vmwareeucsmtm.

vmware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com