How VMware Mirage Complements and Extends Microsoft System Center Configuration Manager
Table of Contents

Introduction ................................................................. 3
  Intended Audience .................................................... 3
  What Is VMware Mirage? .............................................. 3
  What Is System Center Configuration Manager? ............... 6

Deployment Scenarios for Mirage with SCCM ......................... 8
  Deploy Mirage into an Existing SCCM Environment .......... 10
  Use Cases for Combining Mirage and SCCM ..................... 11

Determining When to Use Mirage or SCCM .......................... 12
  Image Management and Software Deployment .................. 12
    How Mirage Manages Images and Applications ............... 12
    How SCCM Manages Images and Applications ................. 13
    How Mirage Can Complement and Extend SCCM ............... 13
  Disaster Recovery .................................................... 14
    Mirage Backups of Endpoints .................................. 14
    Lost or Stolen Laptops .......................................... 15
    Desktop Repairs .................................................. 15
    Using Mirage to Restore Failed SCCM-Enabled Endpoints .. 15
  Hardware Refresh .................................................... 22
  Windows Operating System Migration ............................ 23
    Advantages of Using Mirage for a Windows Migration ...... 24
    How Mirage Can Complement and Extend SCCM ............... 24
  Migrating a Windows Operating System with Mirage .......... 25
  Installing SCCM Application Packages on Mirage Application Layers 26

Summary ................................................................. 27

Additional Resources .................................................. 27

About the Author and Contributors ................................... 28
Introduction

This white paper describes how VMware Mirage™ can extend and complement PC-life-cycle-management (PCLM) tools, such as Microsoft System Center Configuration Manager (SCCM) 2007 or 2012.

Mirage is not a replacement for SCCM, which you can use for managing PCs from inception to retirement. Rather, Mirage extends and complements certain SCCM functions. You can use either Mirage or SCCM for building and deploying PC images and applications, migrating Windows operating systems (OSes), and migrating users to different hardware. For example, you can use Mirage to build, deploy, and back up PC images, and use SCCM to manage inventory and client settings and to protect endpoints from viruses and malware.

Mirage provides disaster recovery for endpoints, but SCCM does not.

Intended Audience

This white paper is intended for Windows IT administrators who want to learn how to use Mirage to complement and extend SCCM.

The first section provides an overview of Mirage and SCCM. If you are familiar with Mirage and SCCM, you can jump to the following sections:

• Deploy Mirage into an Existing SCCM Environment
• Use Cases for Combining Mirage and SCCM
• Determining When to Use Mirage or SCCM

What Is VMware Mirage?

Mirage is a unified image management solution for Windows physical and virtual machines. Mirage is available as a standalone product or as part of VMware Horizon®.

Mirage provides the following benefits:

• Manages images for Windows PCs
• Deploys software applications to endpoints
• Automates backup and recovery on endpoints
• Repairs broken, lost, or stolen PCs
• Manages remote and branch office PCs without added infrastructure
• Accelerates Windows 7 and Windows 8.1 migrations
• Simplifies PC hardware refreshes

Mirage provides layered image management for physical PCs (desktops and laptops), tablets that run Windows 8, virtual machines, and VMware Horizon with View virtual desktops. You can deliver the OS and core applications via a Mirage base layer, and customized sets of applications via application layers. Mirage layering permits the preservation of user customizations.

Mirage optimizes downloads of layers for WAN transfers so that only new blocks of data are transferred to the endpoints, and Mirage automatically handles network disruptions. Mirage optimizes storage by deduplicating the data that is stored in the data center.
Mirage also provides disaster recovery through backups and incremental snapshots for both physical and virtual machines. If a user endpoint is corrupted or damaged, Mirage can restore all or part of the endpoint. In addition, IT can use Mirage to migrate endpoints to newer Windows operating system versions.

You can use several Mirage server clusters to back up and recover endpoints or to migrate endpoints in a large organization. Each Mirage server supports a maximum of 1,500 endpoints. The formula is:

\[(\text{Number of endpoints in the organization}/1,500) + 1 = X\]

where \(X\) is the number of Mirage servers needed to manage all the physical and virtual endpoints.

**Note:** Mirage can back up and recover virtual machines created by VMware Fusion® Pro or VMware Player Plus™.

Figure 1 shows the Mirage system components. The Mirage Management server manages Mirage server clusters. The Mirage server cluster in the data center communicates with Mirage clients installed on endpoints. Mirage can manage endpoints for users in local and remote offices, for home workers, and for traveling employees. Mirage also can manage disconnected laptops.

The Mirage Gateway server for managing the mobile endpoints is also located in the data center, but is part of the DMZ. The Gateway server allows mobile endpoints to connect to the Mirage server without using VPN. The Gateway server can be part of a cluster, depending on the number of users that connect to it. If the Gateway server is a cluster, it needs a load balancer, as depicted in Figure 1. The Gateway server can connect to either the Mirage server cluster or to the load balancer for the WAN clients.
The Mirage branch reflector makes the distribution of downloads more efficient in branch and remote offices. The branch reflector downloads base layers, application layers, drivers, and user state migration tool (USMT) files to its local cache. The branch reflector receives downloads over the WAN, and the other endpoints in the branch office receive downloads over the LAN from the branch reflector. Each branch office can have its own branch reflector. Mobile laptops receive downloads directly from the Mirage server.

For more information about Mirage, see the following references:

- VMware Mirage Installation Guide
- VMware Mirage product page
- VMware Mirage Reviewer’s Guide
What Is System Center Configuration Manager?

Microsoft SCCM is systems management software for managing large groups of client devices. SCCM supports Windows, Mac OS X, UNIX, and Linux operating systems; and mobile operating systems such as Windows Phone, Windows RT, iOS, and Android.

SCCM enables secure and scalable deployment of operating systems and applications, compliance-settings management, and asset management of servers, desktops, laptops, virtual machines, tablets, and mobile phones.

SCCM provides the following benefits:

- Manages both Windows and non-Windows devices
- Deploys applications to all of a user’s devices
- Deploys Windows operating systems to endpoints
- Delivers updates of Microsoft products and operating system patches, third-party applications, hardware drivers, and system BIOS updates
- Uses Microsoft Endpoint Protection to protect endpoints from viruses and malware
- Manages policies, such as user roles, email alerts, and client settings
- Creates asset and compliance reports for PCs and mobile devices
- Takes inventory of software and hardware at a site
- Monitors client operations and health of the SCCM agent
- Provides client power-management tools for administrators

Figure 2 is an overview of the SCCM configuration. You can use SCCM to manage local, remote, and mobile clients. Central Administration Server (not shown) is used for managing multiple SCCM servers.

You can connect the local clients through the LAN, and connect remote and mobile clients by using distribution points that run as a cloud service in Microsoft Windows Azure. Windows Azure manages Web applications over the Internet. Distribution points reduce the load on the SCCM server.

There are two types of distribution points:

- Distribution points on server workstations.
- Branch distribution points, usually on PC workstations. These receive content from standard distribution points at the primary or secondary sites.

SCCM distribution points contain source files for clients to download, such as software packages, software updates, operating system images, and boot images. You copy the packages to the distribution point over the WAN once, and the clients download the packages from the local distribution point over the LAN. For more information, see Fundamentals of Configuration Manager.
You can use SCCM to manage WAN clients. A public key infrastructure (PKI) server with Windows Server Active Directory Certificate Services is required for SCCM to manage WAN clients. An Active Directory domain controller can act as a PKI server.

SCCM can manage up to 100,000 endpoints, 10 management points, and 250 distribution points per primary site. Management points provide policy and service location information to clients and receive configuration data from clients. Distribution and management points might be in the data center or at other sites.

For more information about configuring and using SCCM, see the Documentation Library for System Center 2012 Configuration Manager and System Center 2012 Configuration Manager Step by Step Guides.

The next section looks at deployment scenarios for Mirage with SCCM.
Deployment Scenarios for Mirage with SCCM

As Figure 3 shows, the IT administrator installs the Mirage and SCCM server components in a side-by-side configuration in the data center. The two systems can coexist independently without any problems. The IT administrator first deploys the SCCM clients on all endpoints and then deploys the Mirage clients. You have a choice of deployment scenarios to combine Mirage and SCCM.

The Mirage and SCCM server systems in the data center do not interact with each other, exchange information, or share back-end database information. The endpoints are the only place where you see evidence that Mirage and SCCM are working in parallel. You can optionally configure these systems to interact on the endpoints with the Mirage and SCCM clients installed. For example, SCCM can manage the PC that is designated as the Mirage branch reflector.

Mirage manages endpoints over the LAN and WAN. SCCM manages endpoints over the LAN, WAN, and cloud. However, SCCM is less efficient than Mirage at managing operating system deployment and application deployment over the WAN.

You can optionally use a Mirage branch reflector to enable endpoints in branch and remote offices to download layer updates more efficiently. The Mirage Gateway server enables mobile end users to securely connect their devices to the corporate network, where the Mirage server is located, without using VPN connections. If branch offices are connected to the corporate network, they do not need to use the Gateway server. However, if the remote branch office is connected through the wireless network, it needs to use the Gateway server.
How VMware Mirage Complements and Extends Microsoft System Center Configuration Manager

Mirage Server Components
- Mirage Console
- Database, Storage Volumes

SCCM Primary Site Server
- Database, Storage Volumes

DMZ
- Mirage Gateway Server

Mirage Branch Reflector
- Optional

SCCM Cloud Distribution Point

No VPN

LAN

WAN

Cloud (WAN)

Remote and Branch Office Endpoints
- Mirage and SCCM Clients

Figure 3: Mirage and SCCM Servers Side by Side with Mirage and SCCM Clients on Endpoints

The most likely deployment scenario is installing Mirage into an existing SCCM environment. You also can deploy SCCM into an existing Mirage environment if you need to do PCLM tasks. For more information, see the System Center 2012 Configuration Manager Survival Guide. No special customization is needed for Mirage.
Deploy Mirage into an Existing SCCM Environment

The following steps assume that the SCCM client is already installed on each endpoint, which enables the SCCM server to communicate with each endpoint. Deploying Mirage enables you to manage these same endpoints with Mirage.

1. Install the Mirage server system in the data center. For more information, see the VMware Mirage Installation Guide.

2. Configure the Mirage server system. For more information, see the VMware Mirage Administrator’s Guide.

3. Use SCCM tools to package the Mirage client and deploy it to all endpoints. Both the Mirage client and the SCCM client must be installed on each endpoint. For more information, see How to Install Clients on Windows-Based Computers in Configuration Manager.

If you want to use secure SSL connections in your Mirage and SCCM environment, you must configure SSL on both the Mirage client and the Mirage server. To install the Mirage client and enable SSL at the same time, type the following command and press Enter:

```
<Mirage MSI path>\MirageClient.x86.<buildnumber>.msi
SERVERIP=<MirageServer>:<port> USESSLTRANSPORT=true /quiet
```

where MirageServer is the name, IP address, or FQDN of the Mirage server, and port is the port number. The default port number is 8000.

4. Validate that the Mirage clients are correctly installed on the endpoints by examining the Mirage system tray icon on each endpoint.

The Mirage client installation is successful if the system tray icon displays a yellow marking. The details show that the client is connected to the Mirage server and is Pending Assignment, which means the endpoint is ready for backup. If the endpoint is connecting to a Mirage Gateway server, the Current Action setting is Pending Logon.

![Figure 4: Verifying That the Mirage Client Is Communicating with the Mirage Server](image-url)
5. In the left pane of the Mirage Console, expand **VMware Mirage > VMware Mirage System > Inventory** and click **Pending Devices**.

A pending device is a virtual or physical machine with the Mirage client installed and configured to communicate with a Mirage server. A pending device becomes an assigned device when an administrator or the end user activates it. Activating a device centralizes it (backs it up).

6. Centralize endpoints into CVDs and perform periodic snapshots. For more information, see the VMware Mirage Administrator’s Guide.

7. If something goes wrong, you can roll back to an earlier state. In the left pane of the Mirage Console, select **Inventory > All CVDs**. Right-click the CVD that you want to revert and click **Revert to Snapshot**. For more information, see the VMware Mirage Administrator’s Guide.

8. Define and implement the desired use cases for your system environment, and decide which server (Mirage or SCCM) performs those tasks. For more details, see Use Cases for Combining Mirage and SCCM.

### Use Cases for Combining Mirage and SCCM

Table 1 lists use cases for combining Mirage and SCCM in your organization. For example, if an endpoint crashes, you can use Mirage to restore the endpoint to its last snapshot. You can use either Mirage or SCCM for migrations and application deployments.

To decide which use case fits your organization, see Determining When to Use Mirage or SCCM.

<table>
<thead>
<tr>
<th>USE CASE</th>
<th>MIRAGE FUNCTIONS</th>
<th>SCCM FUNCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• Perform all tasks for Windows PCs</td>
<td>• Perform all tasks for non-Windows PCs and mobile phones</td>
</tr>
</tbody>
</table>
| 2        | • Back up and restore  
• Replace lost or stolen laptops  
• Repair malfunctioning desktops | • Migrate Windows OS  
• Migrate users to new hardware  
• Deploy applications  
• Perform PCLM tasks |
| 3        | • Back up and restore  
• Replace lost or stolen laptops  
• Repair malfunctioning desktops  
• Migrate Windows OS  
• Migrate users to new hardware | • Deploy applications  
• Perform PCLM tasks |
| 4        | • Back up and restore  
• Replace lost or stolen laptops  
• Repair malfunctioning desktops  
• Migrate Windows OS  
• Migrate users to new hardware  
• Deploy departmental applications  
• Deploy service packs | • Deploy user-specific applications  
• Deploy device drivers  
• Deploy third-party applications  
• Perform PCLM tasks |
| 5        | • Back up and restore  
• Replace lost or stolen laptops  
• Repair malfunctioning desktops  
• Deploy applications | • Migrate Windows OS  
• Migrate users to new hardware  
• Perform PCLM tasks |

Table 1: Use Cases for Mirage and SCCM Working Together
Determining When to Use Mirage or SCCM

The following sections can help you determine when to use Mirage or SCCM for particular functions in your deployment:

- Image Management and Software Deployment
- Disaster Recovery
- Hardware Refresh
- Windows Operating System Migration

Image Management and Software Deployment

Mirage and SCCM use different methods for managing images of operating systems and applications and for deploying applications on endpoints. If properly configured, Mirage and SCCM can work side by side in a complementary fashion without interrupting each other.

How Mirage Manages Images and Applications

Mirage divides the desktop image into logical layers: the base layer, one or more application layers, the user layer, and the driver library. A base layer contains the operating system, system-level software, service packs and patches, and core applications. An application layer contains applications that IT wants to distribute to specific users or groups of users. The user layer contains the content that a specific user creates. Mirage backs up a logical user layer for each managed endpoint.

IT can deliver operating system patches and add new applications by updating the base and application layers on a reference machine and then deploying those layers to endpoints. The Mirage server synchronizes the assigned layers with the endpoints when they connect to the network. Mirage preserves end-user files and settings and user-installed applications during these updates. Figure 5 shows the Mirage Console where you can work with layers.

Figure 5: Wizards for Assigning the Base Layer and Application Layers to Endpoints
Users can install and configure their own applications on their computers. Users also can update or uninstall applications. Both IT-managed elements and user-controlled elements are rolled into one Mirage desktop backup in the data center.

If a user uninstalls an application in an application layer, Mirage does not have a record that the application was uninstalled. However, when the IT administrator updates the application layer, the application is reinstalled on the endpoint.

Mirage provides the benefit of install-free application delivery. It performs the application layer deployment in the background, so end users are not interrupted during work. End users can continue working until prompted to reboot their systems. If something goes wrong while deploying an application layer, you can roll back to the previous version of the desktop without losing user data.

For more information about working with base and application layers, see the VMware Mirage Administrator’s Guide and the VMware Mirage Reviewer’s Guide.

**How SCCM Manages Images and Applications**
SCCM manages operating system and application images on endpoints that have the SCCM client installed. SCCM uses the ImageX tool to create and apply these images to the endpoints. The ImageX tool is included with the Microsoft Windows Assessment and Deployment Kit (ADK), which you need to install separately from SCCM. However, you cannot use ImageX to update Windows operating systems or applications. For more information, see Windows ADK Overview.

You can choose whether to install updates on a specific date and time or make updates available to users immediately. You can also configure applications to be uninstalled.

The Configuration Manager Software Center, which lets users manage their own software, is installed on client endpoints. Users can access the Configuration Manager Application Catalog from the Software Center to request and install software for their Windows-based computers and schedule when SCCM can install software on their computers.

SCCM installs the applications and packages being deployed. The average deployment time depends on the number of applications that are being deployed after the operating system image is applied on the endpoint. End users cannot work during that time, and also need to reboot after each application is installed.

**How Mirage Can Complement and Extend SCCM**
The following examples illustrate how Mirage and SCCM can complement each other in the area of image management and application deployment:

- Use Mirage and VMware ThinApp® for distributing some applications in application layers, and use SCCM to distribute the rest of your applications. ThinApp is bundled with Mirage. ThinApp enables you to virtualize and run multiple versions of the same application on one device, and frees your applications from interfering with each other.

- Use Mirage for re-imaging endpoint systems and deploying large service packs and departmental applications, and use SCCM to deliver individual packages through the application catalog. Operating system patches can be delivered through Mirage or SCCM.

- Use SCCM to deploy all applications and Microsoft updates to the endpoints, and use Mirage to perform backups, periodic snapshots, and restores. If something goes wrong while deploying or updating an application, you can use Mirage to roll back to the previous version of the desktop.

- Use Mirage to manage images and deploy all applications, and use SCCM for PCLM tasks that Mirage cannot perform.
Important: You must decide whether to use Mirage or SCCM for specific software deployment tasks. If you are managing an endpoint, you want to track the actions that are performed on it. This is particularly important for the application deployment task. If one system deploys an application and another system uninstalls that application, it is difficult to track this action. Mirage manages via application layers. SCCM has a different mechanism for deploying applications, and the two products do not collaborate on any one application. SCCM can install, upgrade, or uninstall a specific application that was previously deployed in a Mirage application layer. However, SCCM cannot update Mirage application layers. If SCCM uninstalls an application, Mirage has no record that the application was uninstalled. If Mirage redeploys the application layer, the uninstalled application is reinstalled.

Disaster Recovery

Mirage provides built-in backup and recovery capabilities for user endpoints. If something goes wrong during deployment or migration, you can use Mirage to roll back endpoints to a previous version. SCCM is not designed for disaster recovery.

If your organization has a significant investment in SCCM, your best method is to continue using SCCM for deploying and updating applications and operating system patches, and to use Mirage for backups and restores. Mirage does not overwrite SCCM components or user data during a restore.

Mirage Backups of Endpoints

To activate an endpoint with Mirage, you install the Mirage client and back up (centralize) the endpoint to the data center. This backup image of the endpoint is called a centralized virtual desktop (CVD). Mirage uses incremental snapshots to keep the desktop image synchronized with changes to the endpoints. Changes to the endpoint are uploaded to the desktop image stored in the data center.

Mirage takes periodic incremental snapshots of the endpoint, which enables quick recovery or rollback to a previous desktop state. By default, a snapshot is taken every 24 hours. You can configure the frequency. You can also configure the number of retained snapshots per interval. Each snapshot contains incremental changes since the previous snapshot.
Mirage takes additional snapshots in the following situations:
- Before a base or application layer update
- Before reverting to a snapshot
- Before a migration

For more information about centralizing endpoints, restoring a device to a CVD snapshot, or restoring to a CVD after hard-drive replacement or device loss, see the VMware Mirage Administrator’s Guide.

**Lost or Stolen Laptops**
If a laptop is lost, stolen, or damaged, you can use the Disaster Recovery wizard in the Mirage Console to restore the entire laptop to a replacement computer or restore only selected layers. You can also temporarily migrate a physical computer to a virtual machine until a replacement computer arrives.

After the new computer is completely restored, you can use Mirage to re-centralize the endpoint so that the computer is backed up. You also can resume SCCM operations on that endpoint.

**Desktop Repairs**
Mirage can repair malfunctioning desktops caused by broken applications or viruses. For example, if a user installs an application that later crashes with a blue screen or that corrupts another application or data, you can use a Mirage snapshot to restore a specific file, directory, or application, or the entire system on an endpoint.

To revert to an earlier snapshot:
1. In the left pane of the Mirage Console, select **Inventory > All CVDs**.
2. Right-click the CVD that you want to restore to an earlier snapshot and select **Revert to Snapshot**.
3. Select the date of the snapshot to which you want to revert.

If the hard drive is corrupted and needs to be replaced, you can overwrite the prior information and restore the desktop image to the same computer or a different computer. In this case, use the Disaster Recovery wizard in the Mirage Console.

After the malfunctioning desktop is restored, you can use Mirage to centralize the endpoint so that it can be backed up again. You also can resume SCCM operations on that endpoint.

**Using Mirage to Restore Failed SCCM-Enabled Endpoints**
The following example shows how to use Mirage to restore an SCCM-enabled endpoint to its original state and then use SCCM to redeploy the applications.

In this example, Adobe Reader XI has become corrupted on endpoint **demo-vdi-02**. The endpoint is connected to the Mirage server **demo-mss-01**.
1. In the left pane of the Mirage Console, select **Inventory > All CVDs**.

2. Right-click the CVD that you want to revert and select **Revert to Snapshot**.
3. In the Revert CVD window, select the snapshot version to restore.
   
   In this example, the CVD is being reverted to a snapshot before Acrobat Reader was installed, so this particular application will not be among those restored.

4. To restore the operating system and applications while preserving the existing user data on the endpoint, select **Restore system only**.

5. In the left pane of the Mirage Console, click **Task Monitoring** to monitor the progress of the restore operation.

   ![Image of Task Monitoring](image)

   You also can view the progress on the endpoint, as shown in the next step.
6. To view the restore operation on the endpoint, click the Mirage icon in the system tray.

7. When prompted, reboot the endpoint to complete the restore operation.

Now that Mirage has restored the system to a clean state, you can use either Mirage or SCCM to redeploy recently installed applications to the endpoints. This example uses SCCM.

On this desktop, both Google Chrome and Adobe Reader were installed after the point of the snapshot, so both of these applications must be reinstalled.
8. In SCCM, expand Application Management > Packages and select Adobe Reader from the list of packages.

This action schedules Adobe Reader for deployment on the endpoint.

9. In SCCM, expand Application Management > Applications and select Google Chrome in the software library.

10. Right-click Google Chrome and select Deploy.

The Deploy Software wizard displays.
11. On the General page, browse to the Mirage Desktops collection. This desktop belongs to an SCCM collection of desktops called Mirage Desktops, and you will use the wizard to deploy Google Chrome to this collection.

12. On the Content page, select the distribution point that contains the Google Chrome installer. The applications to be installed are stored on SCCM distribution points.
13. Complete the SCCM Deploy Software wizard to specify the installation settings, and then click **Close** on the Completion page.

The SCCM Software Center shows that Google Chrome is being installed on the endpoint.
After the applications are installed on the endpoint, Mirage takes a snapshot at the next regular interval.

**Hardware Refresh**

Both Mirage and SCCM can refresh PCs to new hardware and migrate end users to new hardware. You can migrate users one at a time or many users at the same time. Both Mirage and SCCM support migration to hardware of a different make and model, and automated mass migrations.

You must decide whether you want to use Mirage or SCCM to perform hardware migrations, depending on your organization’s goals.

The following are some advantages of using Mirage for hardware migrations:

- Laptops do not need to be connected to the corporate network for the hardware migration operation. Laptop users can be on the Internet.
- Mirage is optimized for WAN connections.
- The deployment time is shorter.

An example is using Mirage to reinstall an endpoint on new hardware. To prepare for the hardware migration, you use the **Sync Now** operation to save the data on the old computer. Install the Mirage client on the new computer and join it to the domain. Then, you use the Hardware Migration wizard from the Mirage Console to migrate the CVD to the new computer. This CVD image includes the operating system, all applications, and user data and settings. When the migration is complete, the end user is ready to work and does not need to reinstall personal applications and reconfigure the computer settings.

For more information about migrating users to different hardware, see the [VMware Mirage Administrator’s Guide](#).
Windows Operating System Migration

You must decide whether you want to use Mirage or SCCM to perform Windows operating system (OS) migrations, depending on your organization’s goals.

Both Mirage and SCCM can migrate endpoints from Windows XP to Windows 7, or from Windows 7 to Windows 8.1. Table 2 compares the migration capabilities for Mirage and SCCM.

The Windows OS migration can be in place (on the same devices) or to replacement devices. Migrate only the applications that work on the new Windows OS version.

<table>
<thead>
<tr>
<th>MIGRATION CAPABILITY</th>
<th>MIRAGE</th>
<th>SCCM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application migration</td>
<td>Yes, with base and application layers, if the applications work on the new OS version</td>
<td>Yes, if the applications work on the new OS version</td>
</tr>
<tr>
<td>Automated mass migration</td>
<td>Yes, optimized for mass migration</td>
<td>Yes, scheduled via PowerShell and internal tasks</td>
</tr>
<tr>
<td>Back up and restore to previous Windows OS</td>
<td>Yes, using CVD snapshots</td>
<td>No. Requires other disaster recovery solution or reinstallation of everything.</td>
</tr>
<tr>
<td>Revert Windows OS to previous version if migration fails</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>In-place migration on existing endpoints</td>
<td>Yes</td>
<td>Yes, by assigning a task sequence to an endpoint</td>
</tr>
<tr>
<td>Remote and distributed users</td>
<td>Yes, using branch reflectors at remote sites</td>
<td>Yes, using distribution points</td>
</tr>
<tr>
<td>Minimize downtime for users</td>
<td>30–60 minutes</td>
<td>30–60 minutes</td>
</tr>
<tr>
<td>User data, file permissions, and settings</td>
<td>Yes, via USMT</td>
<td>Yes, via USMT</td>
</tr>
<tr>
<td>Zero touch (IT does not need to touch the endpoint to configure it)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual machines</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Migrate to new hardware</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 2: Mirage and SCCM Windows OS Migration Capabilities

Both Mirage and SCCM can manage migrations for a distributed organization with remote branch offices and mobile workers with laptops.
Advantages of Using Mirage for a Windows Migration

Using Mirage for Windows OS migrations has several advantages:

• If something goes wrong during the Windows migration, Mirage can roll back the endpoints to the pre-migration state. Mirage takes snapshots at key stages. SCCM does not have an easy way to roll back the endpoints to the previous Windows state.

• For distributed organizations, it is easier to set up a Mirage migration. Administrators can perform the migration over the WAN using branch reflectors to minimize bandwidth usage and the time to complete. For information about the speed of remote Windows OS migrations, see the VMware Horizon Mirage Branch Office Reference Architecture white paper.

• Mirage makes migrations and deployments simpler and more cost-effective with reduced downtime. Downloading the new OS version takes place in the background while users continue working. When the download is complete, users reboot their endpoints, and the exchange of OS versions occurs.

• User downtime during a Mirage migration is typically 30–60 minutes. Downtime during an SCCM migration is about 45–90 minutes.

• You can deploy new Windows 7 or 8.1 applications with the migration base layer or in an application layer, which saves time.

• The Mirage server deduplicates and compresses files. For example, if 5,000 users have a copy of the same PowerPoint presentation, the Mirage server backs up only one copy of that presentation to the migration CVD. SCCM does not support deduplication.

The fastest migration method is to use Mirage for Windows OS migrations and application deployments. You migrate the Windows OS in the Mirage base layer and deploy the applications in the Mirage application layer. This migration method can take less than one hour because Mirage downloads the required files ahead of time, uses deduplication and other WAN optimization techniques, and then installs everything in a single reboot. In comparison, SCCM downloads and installs the applications one by one, which results in multiple reboots.

How Mirage Can Complement and Extend SCCM

Mirage and SCCM can complement each other, such as in these use cases:

• You can use Mirage for Windows OS migrations and disaster recovery. When Mirage completes the migration, you can resume using SCCM for other tasks, such as application deployment, asset management, and software inventory. Consider this use case if your organization is looking for a simpler Windows migration solution, and you have SCCM application packages available for post-migration deployment. Many organizations have SCCM packages ready for their applications, and they might not want to newly capture applications on Mirage application layers. Post-migration, you have the choice of standard SCCM application deployment, or of SCCM application deployment to Mirage application layers. For more information about installing SCCM packages on Mirage application layers, see Installing SCCM Application Packages on Mirage Application Layers.

• You can use SCCM for Windows migrations and Mirage for disaster recovery. If something goes wrong during the migration, you can roll back endpoints to the previous Windows OS state. Consider this use case if your organization already has used SCCM to perform Windows OS migrations. For information about capturing the base layer when using SCCM to migrate Windows, see the Mirage and SCCM section in the VMware Mirage Administrator’s Guide.

• You can use SCCM to migrate LAN users and Mirage to migrate WAN and mobile users, because you do not need to set up a special infrastructure. Using both systems makes the Windows migration process more efficient. However, you need to coordinate application deployment.
Migrating a Windows Operating System with Mirage

You can migrate endpoints from Windows XP or Windows Vista to Windows 7 using the Windows OS Migration wizard from the Mirage Console. Beginning with Mirage 5.0, you can also migrate endpoints from Windows 7 to Windows 8.1 or 8.1 Update 1.

Mirage automatically detects the Windows version from which you are migrating. When using the Windows OS Migration wizard, you select the source device and target device, and Mirage detects whether the migration is from Windows XP to Windows 7, or from Windows 7 to Windows 8.1.

For more information about performing Windows migrations, see the VMware Mirage Administrator’s Guide or the VMware Mirage Reviewer’s Guide.
Installing SCCM Application Packages on Mirage Application Layers

After you complete the Windows OS migration, you can use either Mirage or SCCM to deploy the new applications. If you are accustomed to using SCCM to deploy applications, you can deploy the applications to endpoints with SCCM in a standard way, or you can deploy the SCCM applications to Mirage application layers. However, SCCM cannot reach into Mirage application layers on endpoints and manage the SCCM applications. For example, to update an SCCM application on a Mirage application layer, you need to update the SCCM application on the reference machine and then update the Mirage application layer to endpoints via Mirage.

Use the following steps to deploy SCCM application packages to Mirage application layers on the reference machine. For more information, see Capturing App Layers in the VMware Mirage Administrator’s Guide or the VMware Mirage Reviewer’s Guide.

1. Install the Mirage and SCCM clients on a reference machine.

   A reference machine is an endpoint where you capture base and application layers.

2. Centralize the reference machine to a reference CVD.

   In the Mirage Console, expand Inventory > Pending Devices, right-click the name of the reference machine, and select Create a New Reference CVD.

3. In the Mirage Console, click Common Wizards > Capture App Layer to start the Mirage application layer recording and the prescan process.

   After the prescan process completes, you can install the applications on the reference machine.

4. Use SCCM to install the SCCM application packages on the reference machine.

5. In the Mirage Console, click Task Monitoring.

6. In the Task Monitoring pane, right-click the reference CVD and select Finalize App Layer Capture to complete the creation of the application layer.

To verify the captured applications, expand Image Composer and click App Layers in the Mirage Console. You can now use Mirage application layers to deploy SCCM application packages to endpoints.

**Important:** Remember that SCCM cannot manage applications on Mirage application layers on endpoints.
Summary

Mirage extends and complements PCLM tools, such as SCCM. Mirage offers disaster recovery for SCCM-managed endpoints, and SCCM application deployments are not overwritten with a Mirage restore.

You can use either Mirage or SCCM to perform hardware and Windows operating system migrations, and application deployments. Consider using Mirage instead of SCCM for migrations if you are looking for a simpler migration solution with less user downtime. Mirage branch reflectors optimize the deployment of application and base layers, and migrations for branch offices and remote users.

To get started, deploy Mirage in your SCCM environment. Then determine whether to use Mirage or SCCM to perform various tasks, according to your organization’s goals and use cases.

Additional Resources

VMware Mirage product Web page
VMware Mirage documentation
- VMware Mirage Installation Guide
- VMware Mirage Administrator’s Guide
- VMware Mirage Reviewer’s Guide
VMware Horizon Mirage Branch Office Reference Architecture
SCCM documentation
- Documentation Library for System Center 2012 Configuration Manager
- How to Install Clients on Windows-Based Computers in Configuration Manager
- System Center 2012 Configuration Manager Survival Guide
About the Author and Contributors

Karen Smith, formerly a Technical Writer in End-User-Computing Technical Marketing at VMware, wrote this paper.

The following people contributed to the content and review of this paper:

• Stephane Asselin, Architect, Technical Enablement, End-User Computing, VMware
• Manrat Chobchuen, former Technical-Solutions Architect, End-User Computing, VMware
• Tina de Benedictis, Group Manager, Technical Marketing Content, End-User Computing, VMware
• Maor Kuriel, Product Specialist, Mirage Engineering, End-User Computing, VMware
• Sachin Sharma, Senior Product Marketing Manager, End-User Computing, VMware
• Shlomo Wygodny, Senior Manager, Mirage Engineering, VMware

To comment on this paper, contact the VMware End-User-Computing Technical Marketing team at euc_tech_content_feedback@vmware.com.