HP Manageability Integration Kit

SUMMARY

This user guide explains how to download, install, and use HP Manageability Integration Kit (HP MIK) with Microsoft Configuration Manager. It is intended for IT administrators who manage HP commercial devices in an enterprise environment.

Legal information

© Copyright 2026 HP Development Company, L.P.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

First Edition: April 2026

Document Part Number: Q20605-001

Table of contents

1 Overview

HP computers are Designed for Manageability (DfM).

DfM has the following capabilities:

- Provides a means that will assist an IT administrator in managing HP BIOS, hardware, and preinstalled software that comes with the computer.
- Provides a solution that works with the client management console of an administrator's choice.

The solution created to address these two tenets is called HP Manageability Integration Kit (MIK).

HP MIK is a Microsoft Configuration Manager solution that enables you to manage HP hardware, BIOS, and software capabilities.

The purpose of HP MIK is to provide a user experience that simplifies routine enterprise process and tasks by integrating into existing tools and workflows.

The following are key benefits of HP MIK:

- Speed up the basics of management: Reduce the number of steps needed to create, deploy, and manage images, BIOS, and system security so you can focus on business.
- Protect data: Secure BIOS settings and set authentication and credentials requirements.
- Manage software: Enable IT administrators to remotely manage features supported by the software, such as HP Programmable Key.

HP MIK is optimized to work with Microsoft® Configuration Manager, although it does work with other client management consoles via scripting. This document includes examples and screenshots only of the HP Manageability Integration Kit plugin within Configuration Manager. For the full user guide, go to the HP Manageability website at http://www.hp.com/go/clientmanagement.

For all your client manageability needs, go to the HP Client Management Solutions website at http://www.hp.com/go/clientmanagement. For all HP client tools and driver packs, select HP Download Library on the HP Client Management Solutions home page.

2 System requirements

You can install HP Manageability Integration Kit on servers running supported versions of Microsoft Configuration Manager and clients running supported Windows® operating systems.

Supported Microsoft Configuration Manager versions

You can install HP Manageability Integration Kit on servers running the following versions of the Microsoft Configuration Manager. To determine server operating system requirements, see the Microsoft Configuration Manager documentation.

- Microsoft Configuration Manager 2403 or later

Supported client operating systems

The HP Manageability Integration Kit client components are supported on the following client operating systems:

- Windows 11
- Windows 10

3 Downloading HP Manageability Integration Kit

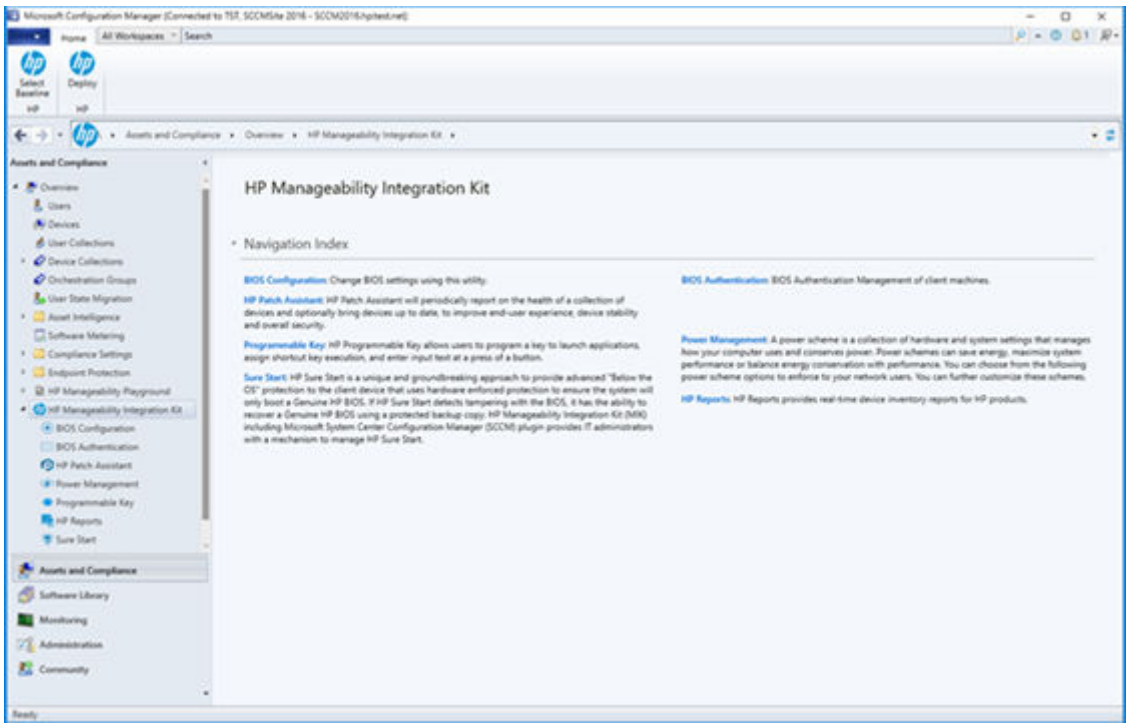
Use this procedure to download the HP Manageability Integration Kit.

1. Go to http://www.hp.com/go/clientmanagement.
2. Under **Resources**, select **HP Download Library**.
3. Download HP Manageability Integration Kit (MIK) for Microsoft Configuration Manager.
4. Under **MIK Client requirements**, download the corresponding SoftPaqs for the features that you want HP MIK to manage.

4 Installing HP Manageability Integration Kit into Configuration Manager

Use this procedure to install HP Manageability Integration Kit into Configuration Manager.

1. Verify that any instances of the Configuration Manager console are closed.
2. If HP Client Integration Kit (CIK) is installed on the system, uninstall it.
3. Run the downloaded HP Manageability Integration Kit (MIK) for Microsoft Configuration Manager SoftPaq and follow the on-screen instructions to complete the installation.
4. Open the Configuration Manager console and verify that HP Manageability Integration Kit is displayed under **Assets and Compliance**.



Distributing HP Client Support Packages

After the installation is complete, HP Client Support Packages must be pushed out to the local distribution points.

1. In Configuration Manager, select **Software Library** > **Overview** > **Application Management** > **Packages** > **HP Client Support Packages**.
2. Do one of the following:
   - If this is a first-time installation, right-click **HP Client BIOS Configuration Utility**, select **Distribute Content**, and then follow the on-screen instructions to complete the distribution.

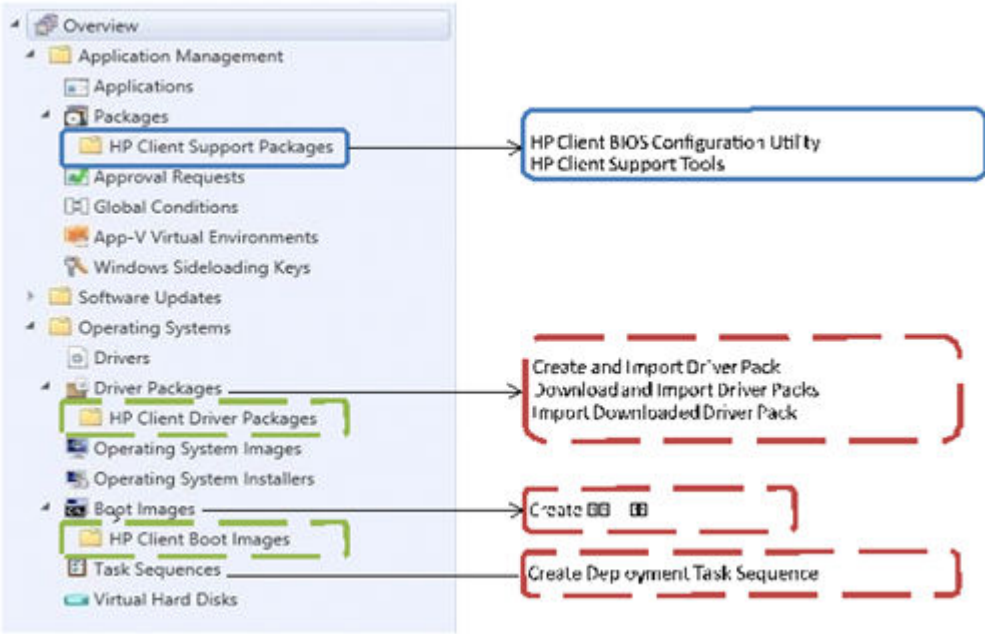
- If this is an upgrade, right-click **HP Client BIOS Configuration Utility**, select **Update Distribution Points**, and then follow the on-screen instructions to complete the distribution.

3. Do one of the following:

   - If this is a first-time installation, right-click **HP Client Support Tools**, select **Distribute Content**, and then follow the on-screen instructions to complete the distribution.
   - If this is an upgrade, right-click **HP Client Support Tools**, select **Update Distribution Points**, and follow the onscreen instructions to complete the distribution.

In the Software Library of Configuration Manager, the following menu items (indicated by dashed lines), folders (indicated by dotted-and-dashed lines), and packages (indicated by solid lines) are created after a driver pack or boot image is created via HP Manageability Integration Kit.

To open a menu item, either select in the ribbon menu or use the right-click context menu.



5 HP MIK plugins

By default, the installer extends the functions of Configuration Manager by adding various plugins under the HP Manageability Integration Kit node.

For more information about managing these plugins with HP MIK, refer to the plugin's respective section within this document.

Current plugins include:

- HP BIOS Configuration
- HP BIOS Authentication (replacing legacy HP BIOS Password Manager)
- HP Patch Assistant
- Power Management
- HP Programmable Key
- HP Reports
- HP Sure Start

HP MIK also includes features to help with operating system and software deployment. These features are detailed in the following sections within this document:

- HP Client Driver Packs
- HP Client Boot Images
- HP Client Task Sequences

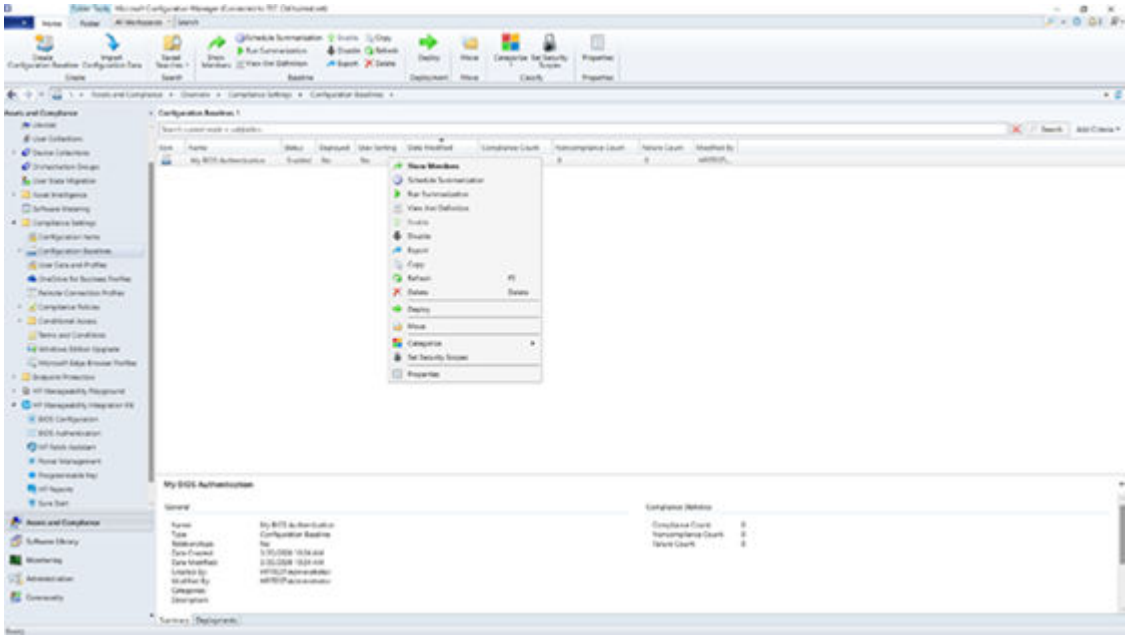
Compliance settings

Policies created or edited using HP MIK plugins are saved as Configuration Manager compliance settings.

To locate a policy:

1. In **Configuration Manager**, select **Assets and Compliance**.
2. Select **Overview** > **Compliance Settings** > **Configuration Items**.

On this page, you can perform Configuration Manager functions, such as opening the **Properties** dialog box and setting the supported operating systems and hardware.



If you create a configuration item with a plugin, the default name is composed of both the baseline name and the plugin name. For example, a configuration item created with a baseline named My BIOS Configuration Baseline and the HP BIOS Configuration plugin is named My BIOS Configuration Baseline – BIOS Configuration by default.

Configuration baselines

IT administrators can select multiple configuration items for one configuration baseline. Baselines can also be deployed to different collections.

Right-click **Configuration Baselines** to select one of the following options:

- Copy: Clone the baseline
- Delete: Delete the baseline
- Deploy: Deploy to different collections
- Properties: View the deployed collection, edit the evaluation conditions, and filter the categories or users

6 HP BIOS Authentication

The HP BIOS Authentication interface allows the IT administrator to manage the BIOS admin password and HP Sure Admin settings on client systems.

- Supported client platforms: HP commercial computers (2015 or later) for BIOS Admin Password
- Supported client operating systems: Windows 11 and Windows 10
- Prerequisites
  - Microsoft .NET Framework 4.8 or higher
  - HP Manageability Integration Kit

User interface

HP BIOS Authentication interface is divided into two sections.

- Manage BIOS Password: The BIOS Password UI is very simple with two sections, current BIOS password and modification password (Change/Set or Remove password).

NOTE: The current password must be provided to change or remove BIOS Password.

- Manage HP Sure Admin:

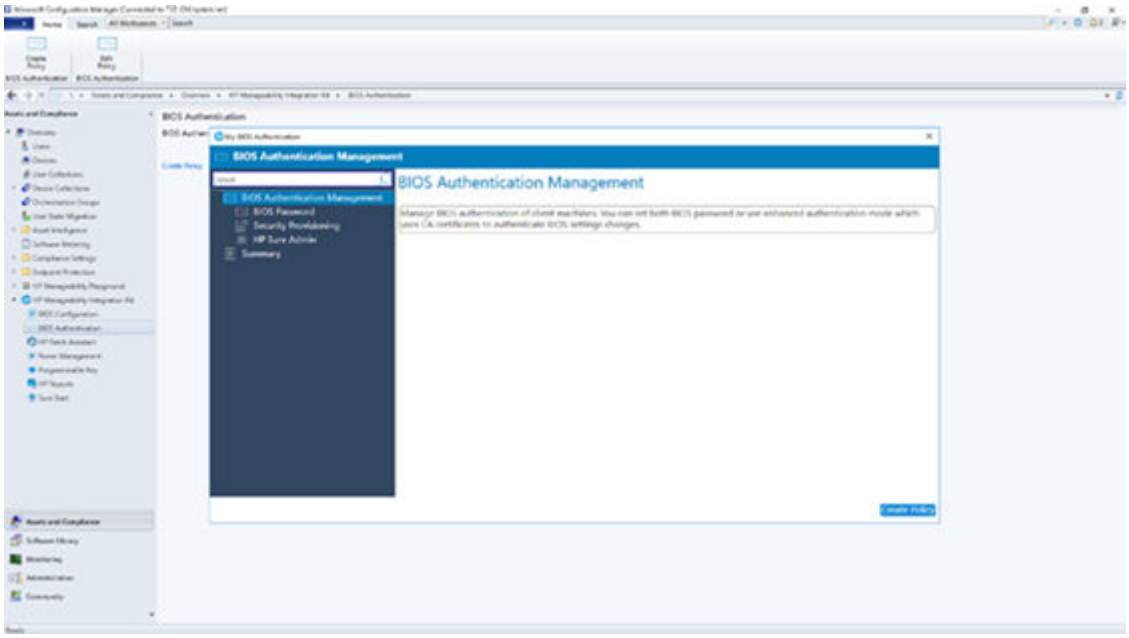
  Security provisioning UI for Management of keys to enable remote configuration of platform features and settings. HP Sure Admin interface allows enabling Enhanced BIOS Authentication Method on the client system and management of the local access key.

Creating a policy

Use this procedure to create a policy in HP BIOS Authentication.

1. In Configuration Manager, select **Assets and Compliance** > **Overview**.
2. Select **HP Manageability Integration Kit**, right-click **BIOS Authentication**, and then select **Create Policy**.
3. Enter a baseline name and start the creating policy wizard.
4. Select **Create**.
5. Select the newly created baseline and select **OK**.

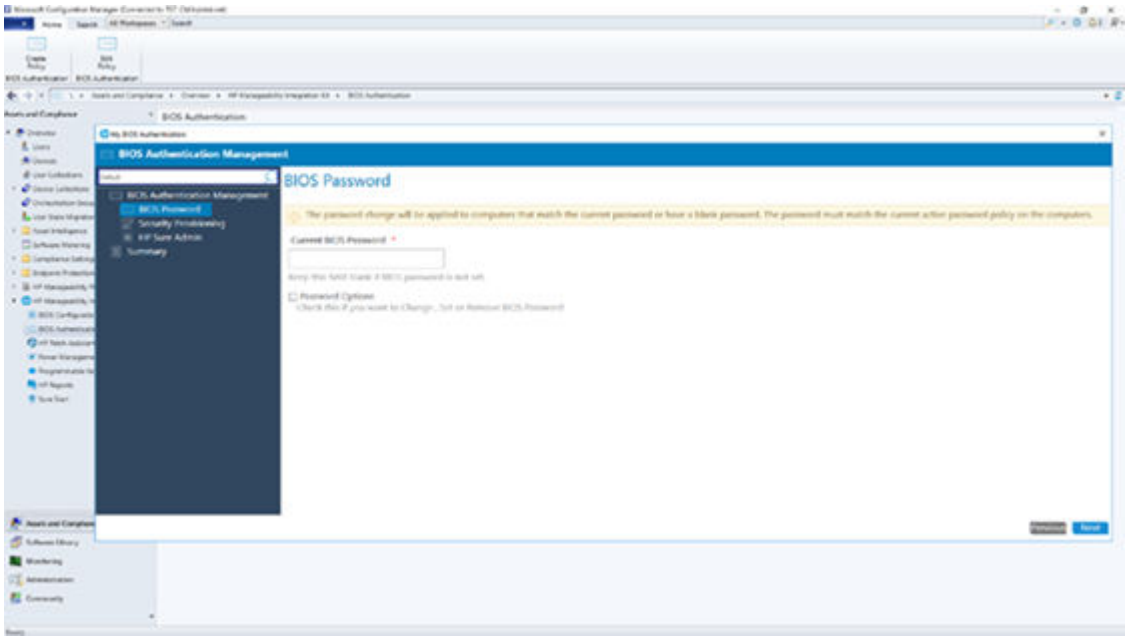
6. In BIOS Authentication Management, select **Create Policy**.



7 BIOS Password

BIOS Password allows you to manage BIOS Admin Password on legacy platforms that do not support HP Sure Admin.

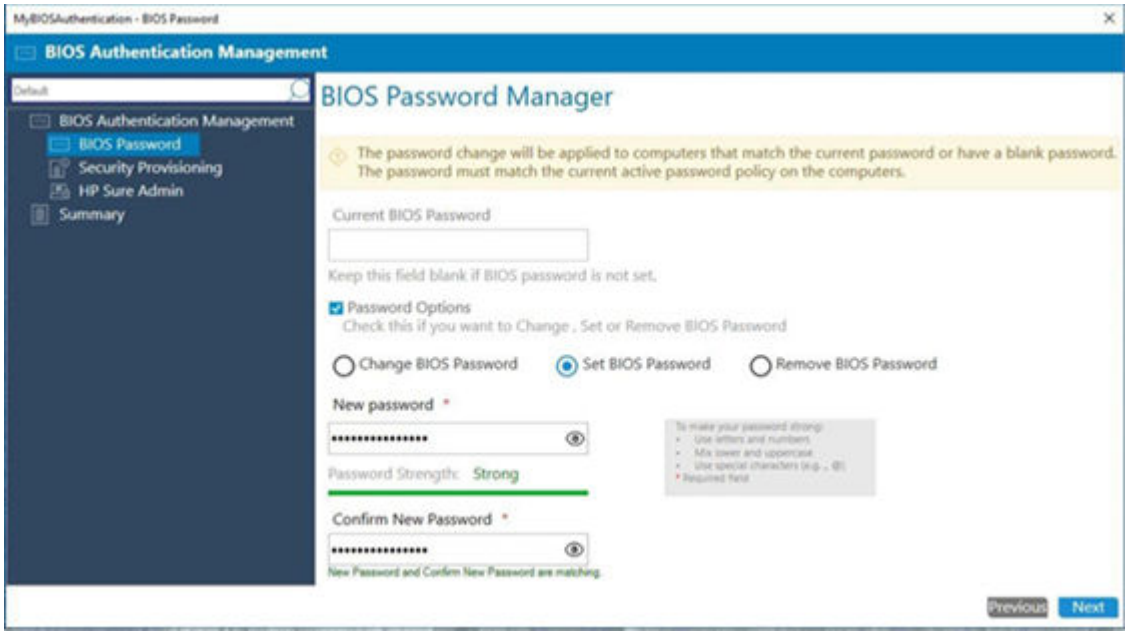
NOTE: If you decide not to set any BIOS password, you can navigate to the next screen. A blank password is considered as no BIOS password to be set on a managed platform.



Setting a BIOS Password

Use this procedure to set a brand-new BIOS Password on client system where there is no current BIOS Password set.

1. Select **Set BIOS Password**, and then type the password in the **New Password** and **Confirm New Password** fields.
2. Select **Next**.



Changing the BIOS password

Use this procedure to change the current password set on the client system to a new password. If your collection includes a mix of devices where some have the BIOS password set and some devices do not, this policy applies the new password to all devices.

1. Type the current password in the **Current Password** field.
2. Select **Password Options**.
3. Select **Change BIOS Password**.
4. Type the new password in the **New Password** and **Confirm New Password** fields.
5. Select **Next**.

Removing the BIOS Password

Use this procedure to remove or clear the current BIOS password set on client systems. If your collection includes a mix of devices where some devices have the BIOS Password set and some devices do not, the policy will apply to all and return as compliant.

If client systems have a different BIOS password set from the one being removed, the policy will fail and return an error.

1. Type the current password in the **Current Password** field.
2. Select **Remove BIOS Password**.
3. Select **Next**.

8 Security Provisioning

The following steps set up two separate key pairs.

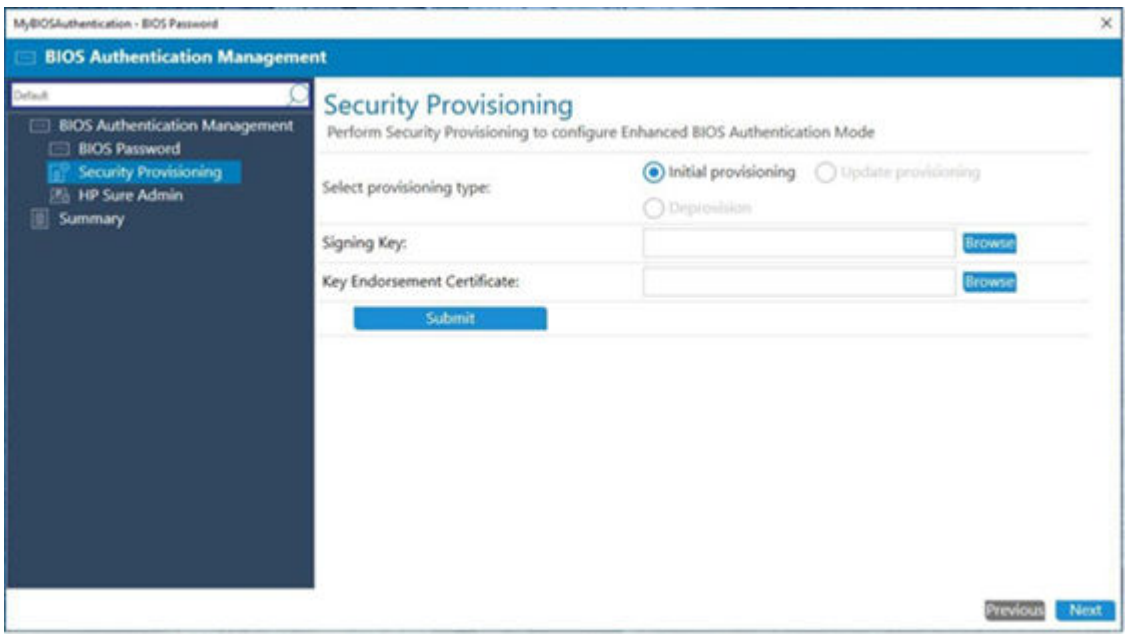
- The signing key, which is the key pair whose private key is used to sign the settings being sent.
- The key pair embedded within the key endorsement certificate whose private key is used only to sign updates to the signing key. The client systems also display the organization string specified in this certificate on the first boot following provisioning.

This provisioning typically happens only once, and the public keys are sent to the client systems as the keys to use for signature validation of future HP Sure Admin, HP Sure Run, and HP Sure Recover commands.

Initial Provisioning or Update Provisioning

The IT Administrator needs to provide both a Signing Key and a Key Endorsement Certificate for initial provisioning.

1. Select **Browse** to select the key/certificate saved on local disks.
2. After the key or certificate has been selected, select **Submit** and then select **Next**.



NOTE: The key format supported is Personal Information Exchange (PFX). See Key generation for HP MIK on page 70 for details about key creation.

Update Provisioning

For collections of systems that have been initially provisioned, the IT Administrator can re-provision with an updated signing key.

1. Navigate to **Security Provisioning** and select **Update Provisioning**.

NOTE: The IT Administrator must provide the signing key to update provisioning.

2. Select **Browse** to select the key saved on local disks.
3. Select **Submit**, and then select **Next**.

Deprovision

For collections of systems that have been provisioned, the IT Administrator can deprovision the systems.

Navigate to **Security Provisioning**, select **Deprovision**, and then select **Next**.

Deprovisioning results in HP Sure Admin being disabled. The system will now switch to legacy mode that will need BIOS Admin password.

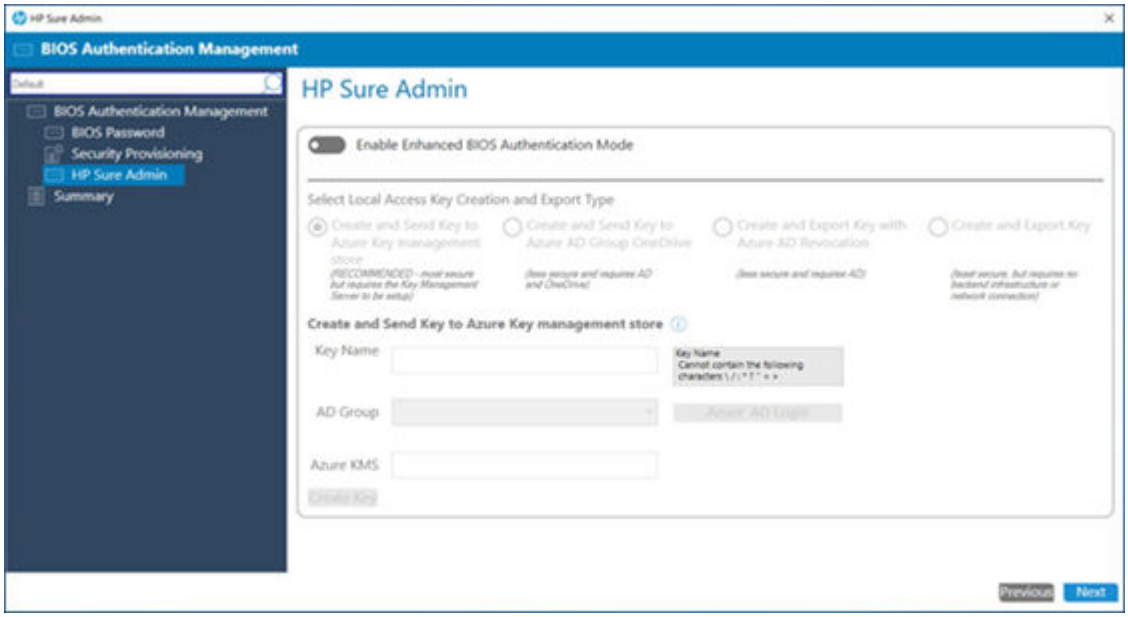
NOTE: Oother dependent features such as HP Sure Run and HP Sure Recover are also automatically disabled as part of the policy push.

9 HP Sure Admin

HP Sure Admin manages BIOS settings using cryptographically verified commands that use public/private key pairs.

- HP Sure Admin is disabled by default.
- Select **Enable Enhanced BIOS Authentication Mode** to enable the HP Sure Admin feature.

NOTE: As a pre-condition user, you need to first perform the step of provisioning using the Security Provisioning UI.



Activating Enhanced BIOS Authentication Mode

Select **Enable Enhanced BIOS Authentication Mode** to activate HP Sure Admin.

Selecting Creation and Export Type

HP MIK provides the following options to create and manage a public/private key pair that can authorize a local administrator user to access the system.

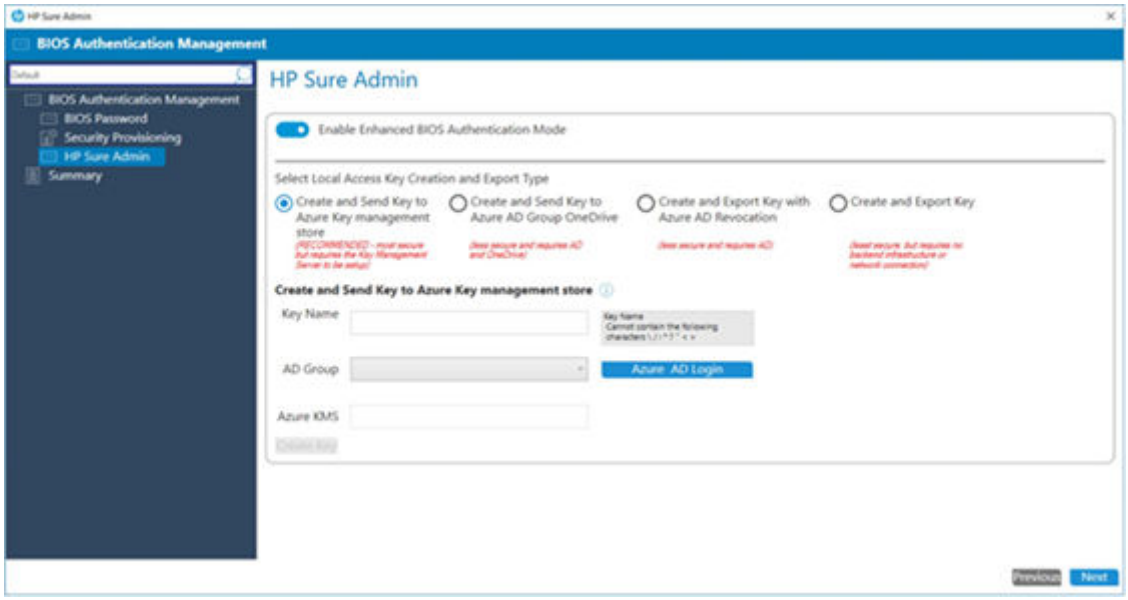
- Create and Send Key to Azure Key to management store
- Create and Send Key to Azure AD Group OneDrive
- Create and Export Key with Azure AD Revocation
- Create and Export Key

NOTE: The selection of options is dependent on infrastructure available within enterprise.

Creating and sending a key to Azure Key Management store – HP recommended

Use this procedure to create and send a key to the Azure Key Management store. HP recommends this procedure.

1. Type the key name in the **Key Name** field.
2. Select **Azure AD Login** to connect to your enterprise Azure AD. You will be prompted to provide the login credentials.
3. After the login is successful, the Azure AD Group Name is listed. Select the appropriate group.
4. Enter the URL path for your enterprise Key Management Store.
5. Select **Create Key**.

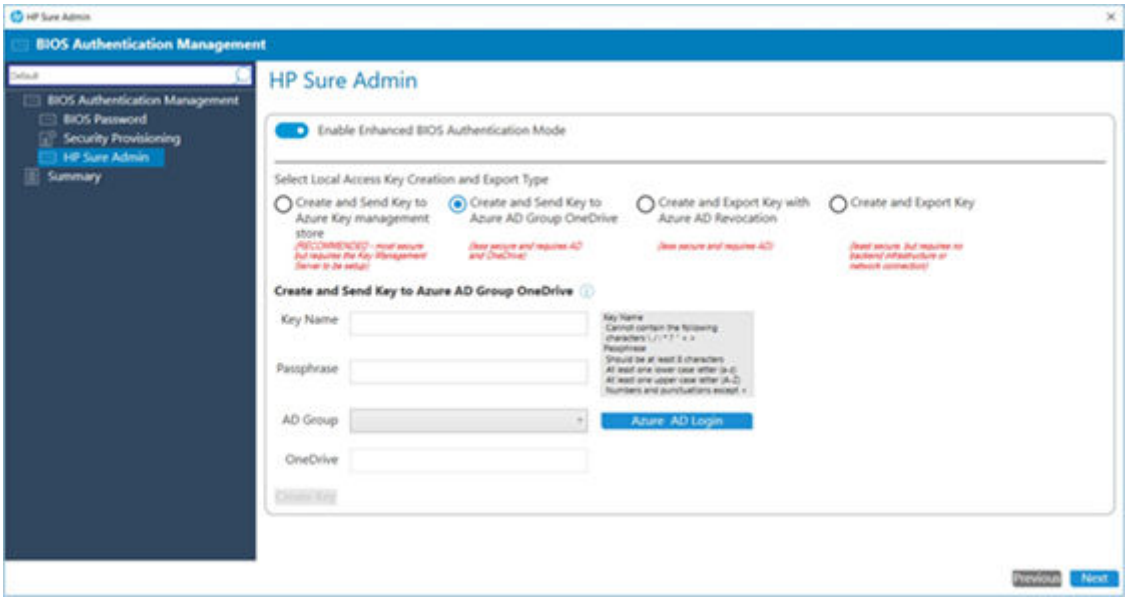


Creating and sending a Local Access key to the Azure Ad Group OneDrive

Use this procedure to create and send a local access key to the Azure Ad Group OneDrive.

1. Type the key name in the **Key Name** field.
2. Optional: type a passphrase in the **Passphrase** field.
3. Select **Azure AD Login** to connect to your enterprise Azure AD. You will be prompted to provide the login credentials.
4. After the login is successful, the Azure AD Group Name is listed. Select the appropriate group.
5. Enter the folder name on your enterprise OneDrive where you want to store the key.

6. Select **Create Key**.

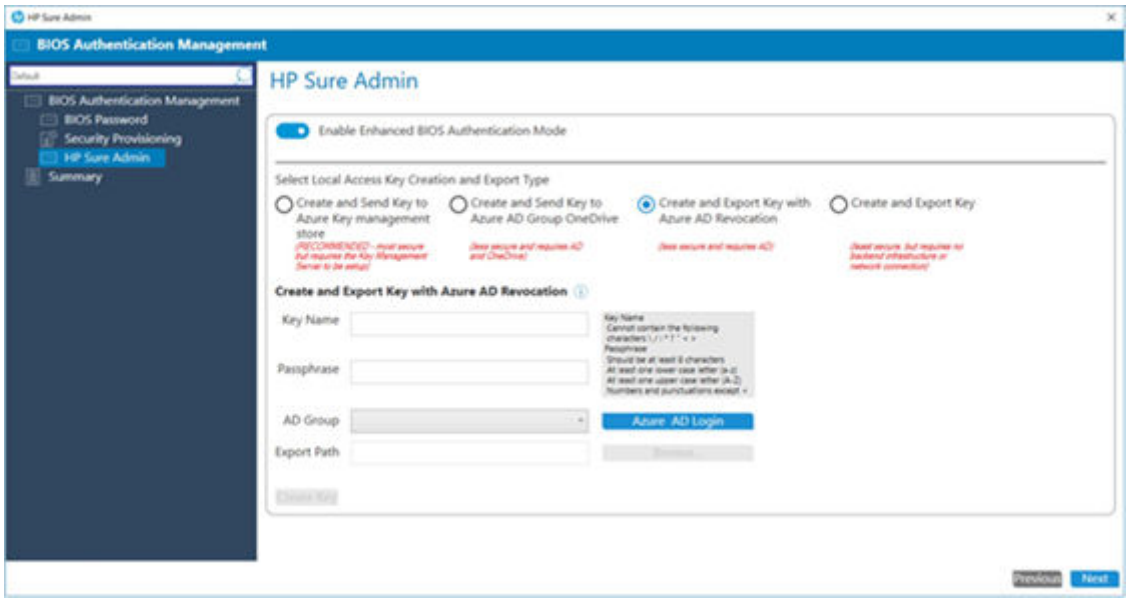


Creating and exporting a key with Azure AD Revocation

Use this procedure to create and export a key with Azure AD Revocation.

1. Type the key name in the **Key Name** field.
2. Optional: type a passphrase in the **Passphrase** field.
3. Select **Azure AD Login** to connect to your enterprise Azure AD. You will be prompted to provide the login credentials.
4. After the login is successful, the Azure AD Group Names are listed. Select the appropriate group.
5. Select **Browse** to select the path where you want to store the key.

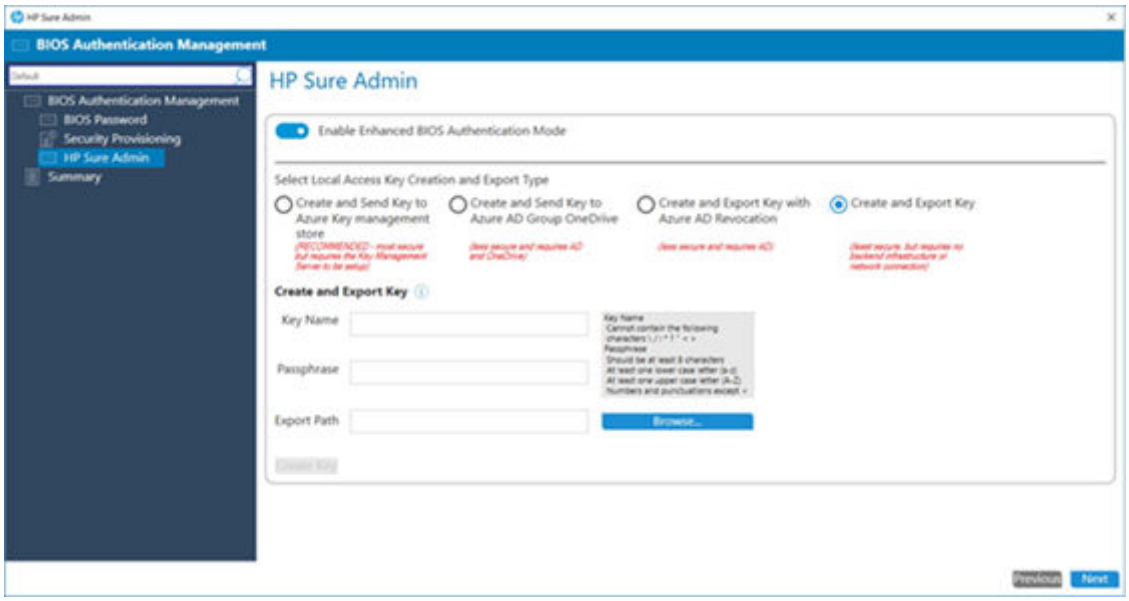
6. Select **Create Key**.



Creating and exporting a key

Use this procedure to create and export a key.

1. Type the key name in the **Key Name** field.
2. Optional: type a passphrase in the **Passphrase** field.
3. Select **Browse** to select the path where you want to store the key.
4. Select **Create Key**.



Enabling HP Sure Admin

To enable HP Sure Admin, a security provisioning policy must be applied first. In a Configuration Manager environment, it is difficult to control which configuration items are applied first or their sequence, so multiple iterations may be needed for HP Sure Admin to be enabled on managed device.

10 HP BIOS Configuration

The HP BIOS Configuration interface enables the IT administrator to define and deploy BIOS settings policies to client computers.

- Supported client platforms: HP commercial computers (2015 or later)
- Supported client operating systems: Windows 11 and Windows 10
- Prerequisites
  - Microsoft .NET Framework 4.8 or higher
  - HP Manageability Integration Kit

User interface

The **HP BIOS Configuration** screen features the following columns.

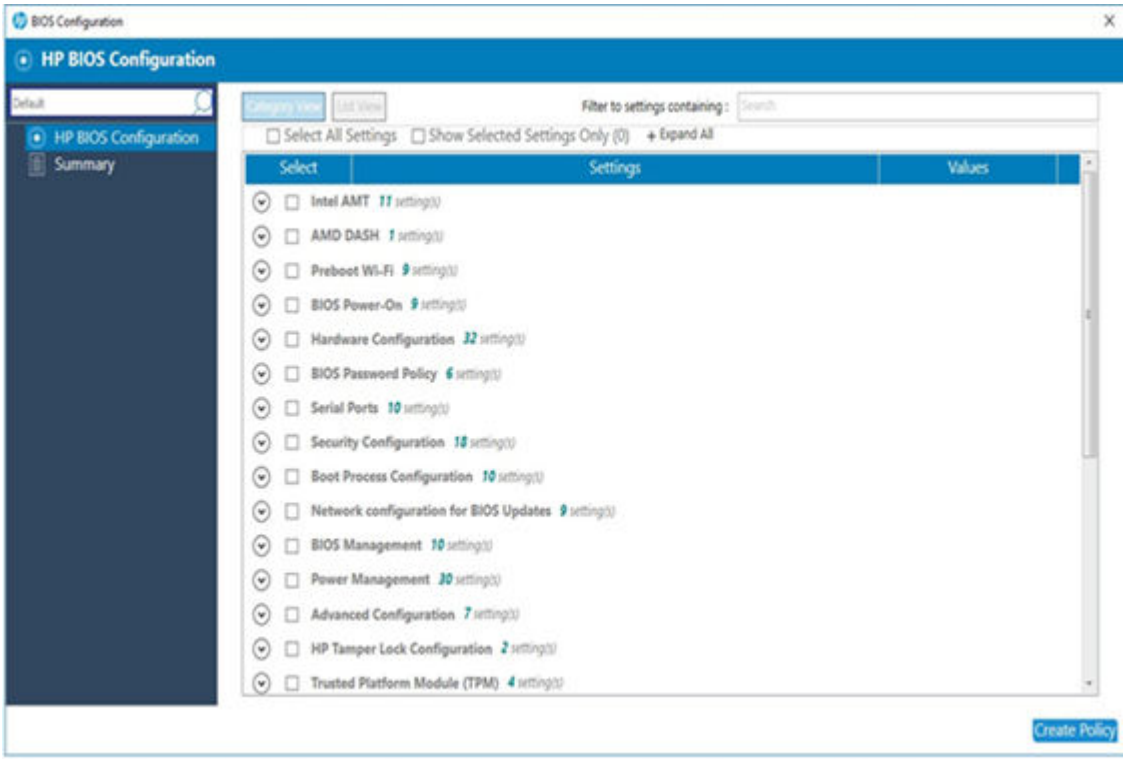


Table 10-1 Column descriptions

Column title	Description
Select	The **Select** column specifies whether or not a setting is enforced by a policy. If a setting is selected, it is set to the specified value. If a setting is cleared, it is not modified.
Settings	The **Settings** column displays the setting name. The icons shown next to some settings indicate the following behaviors: •  Indicates that a setting is only effective for one restart, and then it resets to the default value. •  Indicates that a setting requires confirmation on the next restart, and that the restart cannot be completed until confirmation is given.
Values	The **Values** column can be used to either enter a value or select a value from a drop-down menu, depending on the setting. If a specific syntax is required for an entered value, the box background turns green if the syntax is correct and turns red if the syntax needs to be corrected.

Table 10-2 Options and their descriptions

Option	Description
Category View	Select **Category View** to display BIOS Settings as grouped categories. **NOTE:** In **Category View**, a category must be expanded to display all three columns.
List View	Select **List View** to display the BIOS settings as a list.
Select All Settings	Select **Select All Settings** to select all settings while in **Category View** or in **List View**.
Show Selected Settings Only	Select **Show Selected Settings Only** to show only settings that have been selected.
Expand All/Collapse All	Select **Expand All/ Collapse All** to expand or collapse the details of each setting.
Filter to settings containing	Enter a term in the **Filter to settings containing** field to quickly locate a setting in the list of settings, based on a partial string match.

Creating a policy

Use this procedure to create a policy using HP Configuration Manager.

1. Select **Assets and Compliance** > **Overview**.
2. Expand HP Manageability Integration Kit, right-click **BIOS Configuration**, and then select **Create Policy**.
3. Enter a name in the **Baseline** field, and then start the creating policy wizard.
4. Modify settings by selecting the setting and then selecting the new value.
5. After selecting and modifying BIOS settings, select **Next**.
6. Review the **Summary** page. If changes are necessary, select **Previous**; otherwise, select **Save Policy**.

7. After the policy has been saved successfully, select **Deploy**, and then select the target collections to which to apply the policy.
8. Restart the client computers to ensure that the BIOS settings take effect.

Editing a policy

Use this procedure to edit a policy using HP Configuration Manager.

For client computers, the HP MIK BIOS Configuration logs are stored in `%PROGRAMDATA%\HP\HP MIK\Logs`.

1. Select **Assets and Compliance** > **Overview**.
2. Expand HP Manageability Integration Kit, right-click **BIOS Configuration**, and then select **Edit Policy**.
3. Select an existing baseline policy to edit, and then select **OK** to continue the wizard.
4. After selecting and modifying BIOS settings, select **Next**.
5. Review the **Summary** page. If changes are necessary, select **Previous**; otherwise, select **Save Policy**.
6. After the policy has been saved successfully, select **Deploy**, and then select the target collections to which to apply the policy.
7. Restart the client computers to ensure that the BIOS settings take effect.

11 HP Sure Start

HP Sure Start protects the HP BIOS from any malware or virus threat by verifying the integrity of the BIOS when the computer starts or restarts, by default. Additional policies can increase the frequency with which the BIOS is verified, and the BIOS event log policy can capture any event.

HP Sure Start policy management in HP MIK allows you to manage policies remotely and ensures the appropriate logging and notification of malicious attacks and security breaches in BIOS and the subsequent repairs.

NOTE: Not all features are supported on all systems. Certain systems might require a manual action to restart after a configuration change.

- Supported client platforms: HP 700 series and higher commercial computers (2014 or later)
- Supported client operating systems: Windows 11 and Windows 10
- Prerequisites
  - Microsoft .NET Framework 4.0 or higher
  - HP MIK

BIOS Security Settings tab

The following settings are available on the BIOS Security Settings tab.

Table 11-1 BIOS Security Settings tab settings

Setting	Description
Verify Boot Block on every boot	Verifies that authorized modifications to the system boot image are stored in the non-volatile memory. When enabled, HP Sure Start verifies the integrity of the HP firmware boot image when the computer starts or restarts or exits Hibernation or Sleep mode. This setting provides higher security but can increase start time. When disabled, HP Sure Start verifies the integrity of the HP firmware boot image when the computer starts or exits Hibernation or Sleep mode.
Dynamic Runtime Scanning of Boot Block	Verifies the integrity of the HP boot image periodically while the computer is on and the operating system is running. When enabled, HP Sure Start verifies the integrity of the HP boot image every 15 minutes.
Lock BIOS Version	Disables BIOS updates.
Sure Start BIOS Setting Protection	Disables changes to all critical BIOS settings and provides enhanced protection for these settings via the HP Sure Start non-volatile memory. The BIOS administrator password is required to enable this setting.
Enhanced HP Firmware Runtime Intrusion Prevention and Detection	Monitors HP system firmware executing out of main memory while the operating system is running.

Events and Recovery Settings tab

The following settings are available on the **Events and Recovery Settings** tab. These settings control HP Sure Start behavior after a critical security event, such as the BIOS being attacked or corrupted.

Table 11-2 Events and Recovery Settings tab settings

Setting	Description
Sure Start Security Event Policy	Select Log Event Only to log all critical security events in the HP Sure Start Audit Log within the HP Sure Start non-volatile memory. Select Log Event and Power Off System to power off the system after detecting and logging a HP Sure Start Security Event. Because data might be lost, HP recommends using this setting only in situations where security integrity of the system is a higher priority than the risk of potential data loss.
BIOS Data Recovery Policy	Select Automatic to automatically repair any firmware integrity issues in the non-volatile (flash) memory. Select Manual to repair firmware integrity issues when you press the Esc+Windows+Up Arrow+Down Arrow key combination. HP recommends this setting for IT administrators only.
Prompt on Network Controller Configuration Change	Monitors the network controller configuration and prompts the local user if any changes are detected compared to the factory configuration.
Save/Restore Hard Drive Partition Table	Saves the Master Boot Record (MBR) or the GUID Partition Table (GPT) of the system hard drive.

Audit Log tab

If you select **Gather Sure Start event logs**, HP MIK retrieves HP Sure Start event logs from client computers and stores them in the Configuration Manager hardware inventory.

Creating a policy

Use this procedure to create a policy using HP Sure Start.

1. In Configuration Manager, select **Assets and Compliance**, and then select **Overview**.
2. Select **HP Manageability Integration Kit**, right-click **Sure Start**, and then select **Create Policy**.
3. Enter a name in the **Baseline** field, and then select **Start Policy**.
4. Modify the settings, and then select **Next**.
5. Review the **Summary** page. If changes are necessary, select **Previous**; otherwise, select **Save Policy**.
6. After the policy has been saved successfully, select **Deploy**, and then select the target collections to which to apply the policy.

Editing a policy

Use this procedure to edit a policy using HP Sure Start.

1. In Configuration Manager, select **Assets and Compliance**, and then select **Overview**.
2. Select **HP Manageability Integration Kit**, right-click **Sure Start**, and then select **Edit Policy**.
3. Select an existing baseline policy for edit, and then select **OK**.
4. Modify the settings, and then select **Next**.
5. Review the **Summary** page. If changes are necessary, select **Previous**; otherwise, select **Save Policy**.
6. After the policy has been saved successfully, select **Deploy**, and then select the target collections to which to apply the policy.

Viewing an audit log

For client computers, the HP MIK Sure Start policy log is created in %PROGRAMDATA%\HP\HP MIK\Logs. If enabled, HP MIK retrieves HP Sure Start logs as part of the Configuration Manager hardware inventory.

To view the audit log entries:

1. In Configuration Manager, select **Assets and Compliance** > **Overview** > **Devices**.
2. Right-click a device, select **Start**, and then select **Resource Explorer**.
3. Select **Hardware**, and then select **HP Sure Start Audit Logs**.

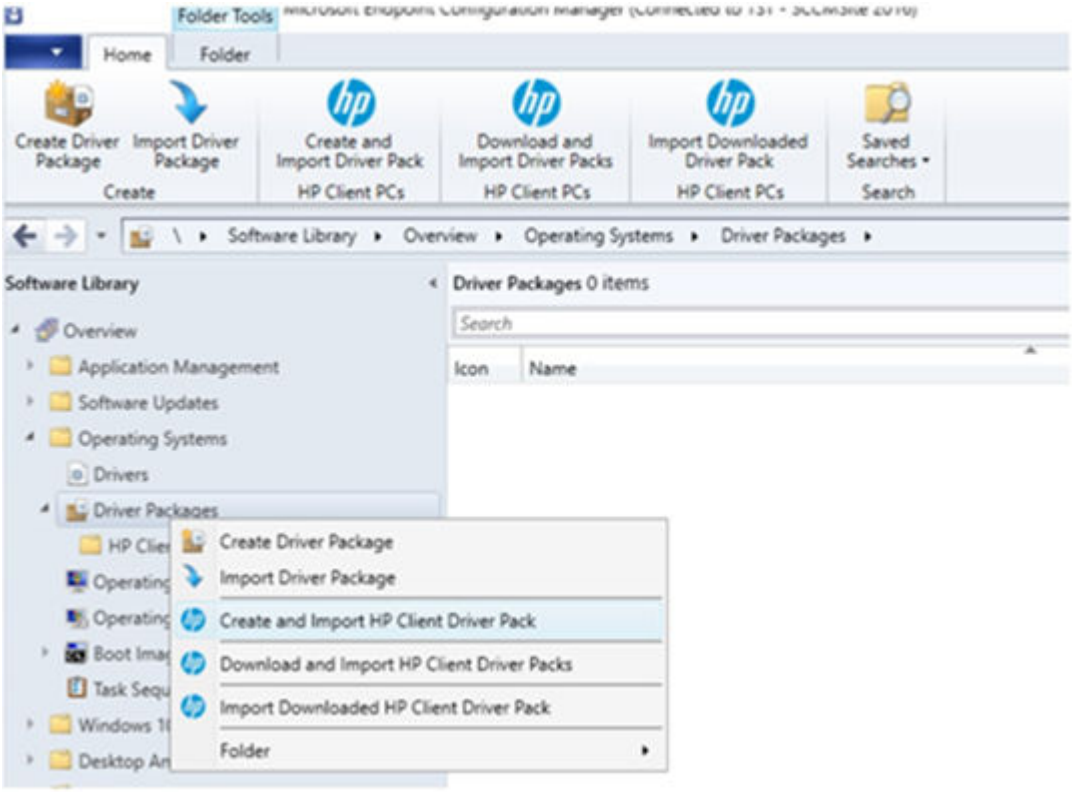
12 Create and import HP Client Driver Pack

The Create and Import HP Client Driver Pack option displays the drivers for supported HP products. This works similarly to the option previously available with HP CIK.

NOTE: OS deployment actions can be found under Software Library > Operating system > Driver Packages.

Use the procedure below to create and import HP Client Driver Packs.

1. In Configuration Manager, select **Software Library** > **Overview** > **Operating Systems** > **Driver Packages**.
2. Select **Create and Import HP Client Driver Pack**. The Create and Import HP Client Driver Pack wizard is displayed.



On the Configuration Manager Console, the new HP Driver Packages folder is displayed. The created driver package is listed under this folder.

In the selected task sequence, you can see **Created driver package** is added under the **HP Driver Packages as Software Packages** folder.

Creating a driver package as a software package

Use this procedure to create a driver package as a software package using HP Client Driver Pack.

NOTE: There is now be an option at the bottom of the page that states **Import Options**. (The box is checked by default.) By checking the box, it creates a driver package as a software package.

1. Select the operating system from the **Operating system** drop-down list.
2. Only the products that support driver-pack creation are displayed in the **Available products** column. Optionally, enter keywords into the HP product name box, and then press **Enter** to filter the list of available products.
3. Select an available product, and then select the right-arrow button to add the product to the **Selected products** column.
4. Repeat the previous step select another product, if necessary. HP recommends selecting products of the same family model to create a driver pack with the optimal relevant drivers. HP also recommends selecting no more than five products per driver pack.
5. Select **Next**.
6. After it completes. select **Next** and the second screen displays. At this point you can name the driver pack and add a version.
7. Select **Next**. On the next screen the wizard prompts you to pick additional software.

NOTE: You can skip the following steps if there you just want to create a driver pack and not a software package. To do this, deselect **Create Software Package**.

8. Select **Next**.
9. If you are creating a driver package, configure the distribution points and network shares as follows:
   a. Select the Distribution point(s) to assign the driver pack to specific destinations. Cloud distribution points are not supported.
   b. Select the location for Configuration Manager to save the Drivers and Driver package(s). Be sure that the specified locations have enough rights to be accessed by all necessary user accounts.

   NOTE: You can also create, add, or choose to not add this to a task sequence.

   Once you have successfully added, do not add, or add to, existing task sequence or they will find them in their task sequence folder. If the **Do not add** option is selected keep in mind it will not show up in the task sequence folder.
10. Select **Import** after the driver pack is created

    In Configuration Manager Console, you can see the new HP Software Packages folder. The created driver package is listed under this folder.

    In the selected task sequence, you can see **Created software package** will be added under **Install HP Softpaq Packages** folder.

Creating a driver package but not as a software package

Use this procedure to create a driver package but not as a software package.

There is now be an option at the bottom of the page that states Import Options. (The box is checked by default.) You must clear the **Create Driver as Software Package** box.

1. Select the operating system from the **Operating system** drop-down list.
2. Select **Operating System** and **HP Products** from drop-down lists.
3. Select **Next**, and then name the driver pack and enter a version.
4. Select **Next** and pick the software to add to the driver pack.

   Skip this section if you do not want to create a software package, but just a driver pack. To do that, deselect **Create Software Package**.
5. Select **Next**, and then select the distribution points, and can also create, add, or choose to not add this to a task sequence.
6. Select **Import** after the driver pack is created

   In Configuration Manager Console, you can see the new HP Software Packages folder. The created driver package is listed under this folder.

   In the Configuration Manager Console, **Created Driver Package** is listed under the **HP Client Driver Packages** folder

   In the selected task sequence, Created Driver Package is listed under the **HP Driver Packs** folder.

Create and Import HP Client Driver Pack – Continue on errors option

On the final step of **Create and Import Drivers Pack**, you have the option to choose to continue on error.

If **Continue on error** is selected, on failure to download/import any softpaqs (either software or driver) for a platform, the package for the impacted platform will be created without the failing softpaqs.

However, if **Continue on error** is not selected, on failure to download/import any softpaqs (either software or driver) for a platform, the package for the platform is not created.

1. Select **Import** to see the the import driver pack status.
2. Select **Summary** to see details and review any failures.

Downloading and importing driver packs as software package

Use this procedure to download and import driver packs as a software package.

1. In **Configuration Manager**, select **Software Library** > **Overview** > **Operating Systems** > **Driver Packages**.
2. Select **Create and Import HP Client Driver Pack**. The Download and Import HP Client Driver Pack wizard displays.

3. Select **Download and Import HP Client Driver Packs**.
4. Select **Operating System** and **Product** from the drop-down lists. Driver packs will be listed that are available for the selected product .
5. Select **Next**.

NOTE: If one or more of the driver packs has been previous imported, it displays a message notifying you that the existing driver pack will be overwritten.

6. Select additional software to import.

NOTE: At this point you can deselect **Create Software Packages** if you do not want to create the software package.

7. Select **Next**.

NOTE: You can select their distribution points, and can also choose to create, add, ornot add this to a task sequence.

8. After you have chosen to add, not add, or add to the existing task sequence, you can find them in the task sequence folder. If you selected **Do not add**, it will not show up in the task sequence folder.
9. Select **Import** to see the import driver pack status.

- For the driver package
  - You can see the new **HP Driver Packages** folder and the created driver package is listed under this folder.
  - In the selected task sequence, you can see **Created driver package** is added under the **HP Driver Packages as Software Packages** folder.
- For the software package
  - In the Configuration Manager Console, you can see the new **HP Software Packages** folder and the created driver package will be listed under this folder.
  - In the selected task sequence, you can see **Created software package** is added under **Install HP Softpaq Packages** folder.

Downloading and importing driver packs not as a software package

Use the following procedure to download and import driver packs but not as a software package.

1. Deselect **Create Driver Package as Software Package** and select **Next**
2. Enter the name and version of the software package you are going to create in the **Name** and **Version** fields.
3. Skip the software package wizard if you do not want to create a software package by deselecting **Create Software Package**, and then select **Next**.
4. Select the distribution point, and then choose a task sequence with three options, for example **Do not Add**, **Add to New**, and **Add to Existing**.

5. Select **Import**. The import driver pack status displays.

In the configuration manager console, **Created Driver Package** is listed in the H**HP Client Driver Packages** folder.

In the selected task sequence, **Created Driver Package** is listed in the **HP Driver Packs** folder.

Download and import driver packs - Continue on errors

Use this procedure to download and import driver packs with **Continue on errors** selected.

- If **Continue on errors** is selected, on failure to download/import any softpaqs (either software or driver) for a platform, the package for the impacted platform will be created without the failing softpaqs.
- If **Continue on errors** is not selected, on failure to download/import any softpaqs (either software or driver) for a platform, the package for the impacted platform will not be created.

When you select **Import**, the import driver pack status displays. Select the summary and detailed log files links for more information and to review any failures.

13 Obtaining HP driver packs

There are several ways to obtain driver packs:

NOTE: Not all driver packs available for download can be used with HP MIK. Driver packs listed under categories such as System > Software Management cannot be imported with HP MIK.

You can obtain HP driver packs from the following locations:

- HP Client Management Solutions website
- HP Support product pages
- HP SoftPaq Download Manager (SDM)

Obtaining HP driver packs using the HP Client Management Solutions website

Use this procedure to obtain HP driver packs using the HP Client Management Solutions website.

1. Go to http://www.hp.com/go/clientmanagement.
2. Under **Resources**, select **HP Driver Packs**.
3. Select 32-bit or 64-bit, depending on the target operating system.
4. Download the appropriate driver pack for the target client computer and operating system.

Obtaining HP driver packs from HP Support product pages

Use this procedure to obtain HP driver packs from HP Support product pages.

1. Go to HP Customer Support.
2. Select **Software and Drivers**.
3. Select the product type.
4. Enter the client computer model number, and then select **Find my product**.
5. Select the client computer.
6. Select your language and operating system.
7. Under **Manageability** > **Tools**, download the appropriate driver pack.

NOTE: WinPE driver packs listed on the download page are used only to create HP client boot images.

Creating driver packs using HP Image Assistant (HPIA)

Use this procedure to create driver packs using HP Image Assistant (HPIA).

1. On the folder where HPIA was extracted and available, select **HPImageAssistant.exe**.
2. Select the **Create Driver Pack** menu on the left.
    a. On the **Choose OS Filter row**, select the required operating system.
    b. Select the model from the **Choose product** list.
    c. Select **Analyze**.
3. Select the SoftPaqs to include in the driver pack from the resulting list.
4. In the **Download** window, confirm the download folder location.
5. Under **Operation**, select **Create driver pack and download driver installation executables**.
6. Confirm the driver pack name.
7. Select **Download**, and then choose Build ZIP or WIM file depending on your needs in the **File type** list.
8. Select **Start**.
9. After a web page displays indicating that the driver pack build is complete, select **OK**.

The driver pack and associated logs are now available in the output directory.

Importing HP driver packs

Use this procedure to import HP driver packs.

1. In Configuration Manager, select **Software Library** > **Overview** > **Operating Systems** > **Driver Packages**.
2. From **HP Client PCs**, select **Import Driver Pack**.
3. Under **Driver package**, select **Browse**, and then select the HP driver pack to be imported.

    As an option, you could select distribution points to assign the imported driver packages to a specific destination; however, cloud distribution points are not supported.
4. Change the default location for Configuration Manager to save the drivers and driver package, if necessary. Be sure that the specified locations have enough rights to be accessed by all necessary user accounts. The location per user is saved automatically after a successful import.

    Any change to this path or other settings enables **Save settings**. Select **Save settings** to save the settings for subsequent driver package download and import procedures.
5. Select **Import**.

During the import process, a dialog box displays the current operation and progress.

After the import process is complete, the imported driver pack is available in Software Library under **HP Client Driver Packages**. Before the imported driver pack can be used in a task sequence, it needs to be pushed out to the distribution points. If no distribution points were selected during the import process or if additional distribution points are needed, select the driver pack and then select **Distribute Content**.

14 HP client boot images

The HP MIK Create Boot Image feature leverages the Configuration Manager and ADK customization support for boot images, so the limitations of HP MIK are dependent on the Configuration Manager version, the ADK version, and the operating system version of the site server.

Before a boot image is made available to a distribution point, Configuration Manager might use Windows Assessment and Deployment Kit (ADK), particularly DISM.exe, to inject drivers to a boot image. DISM might fail to appropriately recognize the signature of some boot-critical drivers added to the boot image because DISM has certain requirements that depend the version of ADK and the operating system. For more information, go to http://technet.microsoft.com/enus/library/hh825070.aspx.

Obtaining a WinPE driver pack

Use this procedure to obtain a WinPE driver pack.

1. Go to http://www.hp.com/go/clientmanagement.
2. Under **Resources**, select **HP Download Library**.
3. Find and download the appropriate HP WinPE Driver Pack. Be sure to select the latest version supporting Windows 11/10.

Because each version of Configuration Manager supports the customization or addition of drivers and components to a specific version of WinPE only, HP MIK Create Boot Image provides limited support. For more information about the specific requirements for WinPE customization, go to http://technet.microsoft.com/en-us/library/dn387582.aspx.

Importing a WinPE driver pack and creating boot images

Use this procedure to import a WinPE driver pack and create boot images.

1. In Configuration Manager, select **Software Library** > **Overview** > **Operating Systems** > **Boot Images**.
2. In the HP Client PCs section of the ribbon menu, select **Create Boot Image**.
3. Under HP client WinPE driver pack, select **Browse**, and then select the HP WinPE driver pack to import. HP MIK shows only the boot images appropriate for the selected WinPE driver pack and supported for customization by Configuration Manager.
4. Select the base boot images to use, and then select **Create** to create boot images with drivers from the selected HP WinPE driver pack.

   Optionally, you can select distribution points to assign the boot images to a specific destination; however, cloud distribution points are not supported.

5. Change the default locations for Configuration Manager to save the drivers, the driver package, and the boot images, if necessary. Be sure that the specified locations have enough rights to be accessed by all necessary user accounts.

   The location per user is saved automatically after a successful importation. Any change to this path or other settings enables **Save settings**. Select **Save settings** to save the settings for subsequent boot image creation and driver or driver pack import procedures.

   After the process is complete, the new boot images are created in **Boot Images** > **HP Client Boot Images**, you need to access the command prompt during the WinPE portion (F8) for debugging purposes.

   a. Right-click the images and select **Properties** > **Customization**.

   b. Select **Enable command support** (testing only).

   Before these boot images can be used in a task sequence, the boot images need to be pushed out to the distribution point. If no distribution points were selected in the import process or if additional distribution points are needed, or if there is a change to the boot image properties, select the boot image and then select **Distribute Content**.

15 HP client task sequences

You can create an HP client task sequence for tasks such as deployment. HP recommends creating task sequences and testing them thoroughly in a test environment prior to any production deployments. HP is not responsible for any data loss caused by the created task sequences.

Creating a deployment task sequence

Use this procedure to create a deployment task sequence.

1. In Configuration Manager, select **Software Library**, and then select **Overview** > **Operating Systems** > **Task Sequences**.
2. From HP Client PCs, select **Create Deployment Task Sequence**.
3. Select a template from the **Task Sequence Template** drop-down list.
4. Enter information as instructed.
5. If you do not plan to use BitLocker Drive Encryption (BDE), clear the Include BitLocker Drive Encryption steps option. For more information on Configuration Manager BDE steps, go to https://technet.microsoft.com/enus/library/hh846237.aspx.
6. Select **Create** to create a basic, bare metal deployment task sequence for HP client systems. A message displays to confirm successful creation of the task sequence.

IMPORTANT: Depending on the selected template, some of the steps in the created task sequence are destructive, including the following:

- Remove Disk Partitions (diskpart clean)
- Format and Partition Disk
- Call Intel RSTCli Utility – Delete All Metadata
- Call Intel RSTCli Utility – Configure RAID Volume

Configuring task sequences

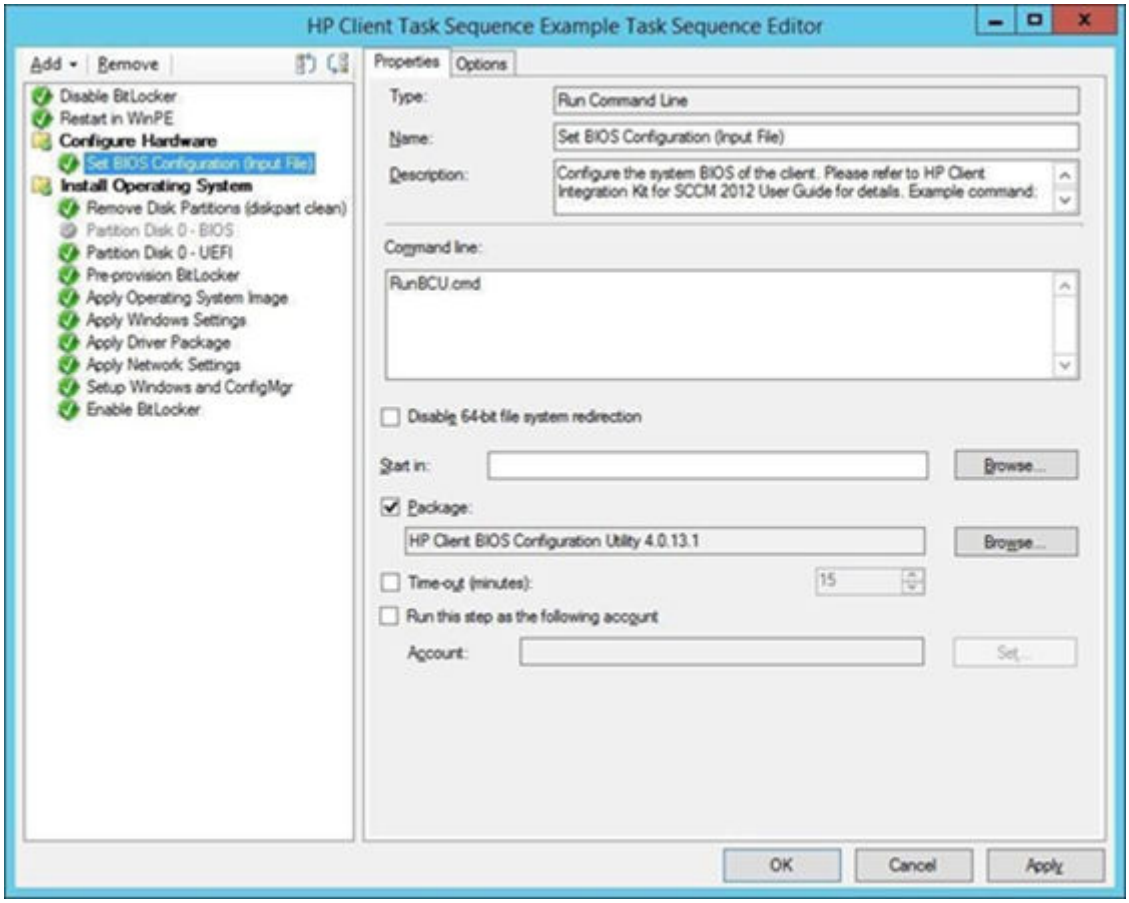
Refresh the list of task sequences to see the created task sequence. Before using the task sequence, additional configuration must be performed for the task sequence to successfully execute.

1. Be sure that the target platform driver pack has been imported. See Importing HP driver packs on page 33.
2. Right-click the task sequence and select **Edit**.

   The figure below shows a task sequence created by the default template.

NOTE: There is also a default template for Windows 10. The default disk partition configuration in the templates is different. For Windows 10, the recommended Windows recovery tool partition is at the end of the drive; in previous versions of Windows, it was at the beginning. The default partition

takes up 1% of the disk space. Change this value to your Windows recovery image size, usually at least 500 megabytes (MB).



3. Depending on the target operating system of the deployment, some or all the following steps need to be configured:

   - Set BIOS Configuration (Input File): Allows the setting of BIOS settings via BCU. The TPM must be turned on and initialized before it can be used. See Configuring task sequence steps on page 40 for more details.
   - Remove Disk Partitions (diskpart clean): This step does not need configuration; however, for the task sequence to run properly on all disk scenarios, the deployment and all packages and content within it need to be configured to allow access to the content directly from the network. See Allowing access to deployment content on page 38 for more information. If this step is not needed, disable the step.
   - Format & Partition Disk: Enables the appropriate step to format and partition the disk to your need. For example, if deploying to a system that is set to UEFI or UEFI Hybrid (with CSM), enable the EFI format step and be sure that the BIOS format step is disabled.
   - Apply Driver Package: Specifies the HP driver package imported for the target platform and operating system.
   - Apply Network Settings: Specifies the workgroup or domain options for your deployment and enter the correct account information for the task sequence to join an Active Directory domain, if necessary. Review each additional task sequence step and set parameters as needed.

4. After all task sequence steps have been configured, select either **OK** or **Apply** to save changes. The task sequence can now be modified, and task sequence steps can be added as needed to perform your operations.

Assigning a boot image

Use this procedure to assign a boot image in the task editor.

1. Right-click the task sequence and select **Properties**.
2. Select the **Advanced** tab and then select **Use a Boot Image**.
3. Select **Browse** and then select the appropriate boot image from the HP Client Boot Images folder.

NOTE: Select the boot image with the same architecture as the operating system being deployed (for example, an x86 image for an x86/32-bit operating system and an x64 image for an x64/64-bit operating system).

Allowing access to deployment content

To run properly, the Remove Disk Partitions (diskpart clean) step in the HP MIK task sequence needs to be run directly from the network. For this to happen, all packages and content in the task sequence (including the boot image) need to be configured as follows:

1. Right-click the content/package and select **Properties**.
2. Select the **Data Access** tab, and select **Copy the content in this package** to a package share on distribution points.
3. Select **OK**.
4. If necessary, select **Access Content Directly** from the distribution point option on the Distribution Points step of the wizard.

   If this step is not needed, or if you wish to use the download content setting, disable this task sequence step. If you still need to be able to run this step when the **Download content locally** option is selected, see the information about removing disk partitions in Configuring task sequence steps on page 40. You cannot use the **Access Content Directly** option for possible workarounds.
5. After the task sequence has been modified and amended as needed, deploy to the target collection and distribute content as needed to use the task sequence. Follow the on-screen instructions to complete this process.

Configuring the Set BIOS Configuration task step

The Set BIOS Configuration (Input File) task step allows the configuration of BIOS settings on platforms managed by HP. This Run Command Line task uses BCU.

This task sequence step is run with the following command line:

```
RunBCU.cmd <parameters to pass to BCU>
```

For a list of parameters and options, see the HP BIOS Configuration Utility User Guide.

This action applies the BIOS settings specified in the selected REPSET file and/or executes specified command line options. The batch file calls the appropriate version of BCU depending on the architecture of the current operating system.

An example REPSET file is included with the package; \ located in the Config folder of the package source folder and named BCUSettingExampleOnly.REPSET. If this REPSET file is used in this task step, the command line is as follows:

```
RunBCU.cmd /setconfig:"Config\BCUSettingExampleOnly.REPSET"
```

HP recommends saving the REPSET file in the source folder or subfolder of the package so that you can easily reference it in the command line.

Adding and editing configuration files

Use this procedure to add and edit configuration files. Be aware of the following when using this task sequence step:

- After making changes or adding a configuration file to the package folder, be sure to update the HP Client BIOS Configuration Utility package to the distribution points to ensure that the new configuration files are available for the task sequence.
- Some BIOS setting changes might not take effect until after a restart of the target client; a restart might be needed to be sure all settings apply.
- Changing certain BIOS settings might cause task sequences to fail to complete. Be sure to test the desired BIOS configuration file before deploying the task sequence widely.
- Certain characters used in BIOS passwords might require special escaping to work properly; see the HP BIOS Configuration Utility User Guide link included with the HP MIK for details.

  For more information, see HP BIOS Configuration Utility (BCU) on page 44.

1. Obtain the configuration file from the target platform and edit the file by setting the new values and removing settings and values from the configuration file that are not required to be applied through this configuration.
2. Go to the package source folder location of BCU. By default, the package is located in the HP Client Support Packages section of the Configuration Manager Software Library.
3. Select the source folder location and copy the REPSET file to the folder.
4. Update the distribution points so that the REPSET file is made available to the task sequence.

Refreshing task sequence references

Task sequence references might need to be refreshed if one of the following conditions applies:

- HP MIK was uninstalled and then reinstalled.
- Some or all of the HP Client Support Packages were deleted and reinstalled using the Repair option in the installer.

1. Right-click the task sequence, and then select **Edit**.
2. Follow the on-screen instructions in the Action column of the following table.

Preparing the boot image used by the task sequence

Use this procedure to prepare the boot image used by the task sequence.

1. Make sure that the boot image has the necessary drivers as shown in Importing a WinPE driver pack and creating boot images.
2. Remove any existing Intel Rapid Storage Technology (Intel RST) RAID drivers to avoid any conflict with the driver added in the following step.
3. Add the version of the Intel Rapid Storage Technology RAID Driver that supports the target client systems to the boot image.

Preparing the packages used by the task sequence

Use this procedure to prepare the packages used by the task sequence.

1. Be sure that the target platform driver pack has been imported as shown in Importing HP driver packs on page 33.
2. Go to https://downloadcenter.intel.com, and then search for the **Smart Response Technology Command Line Interface Deployment Tool**. Locate the tool version that matches the driver version, and follow the on-screen instructions to download it.

NOTE: The major version and minor version values of the driver and the command line tool must match. For example, the command line tool version 12.8.x works with the driver version 12.8.x.

3. Unzip the downloaded file. The file might contain zip files for the 64-bit and 32-bit binaries of the tool. Those also need to be extracted.
4. Copy the extracted files and folders of the command line tool to the location to be the source of the software package for this tool.
5. Create a software package that references the source location.

Configuring task sequence steps

Use this procedure to configure task sequence steps.

1. Right-click the task sequence and select **Edit**.
2. Configure the following steps:
   a. Call Intel RSTCli Command Line Utility - Delete All Metadata: Removes all previously configured disk metadata.
      i. Replace the command: The command line in the step, `rstcliXX.exe`, is a placeholder. Read the utility documentation carefully and replace the placeholder command with the actual command. The package containing the command line utility in the preparation step earlier needs to be selected in this step.

         The following is an example of the command line:

         ```
         IntelRSTCli\12.8\x64\rstcli64.exe --manage --delete-all-metadata
         ```

In this example command, `IntelRSTCli\12.8\x64` is the relative location from the source folder to the actual command line utility in the content of the package.

ii. Select the Intel command line tool package prepared earlier.

b. Set BIOS Configuration (to RAID mode): Allows the setting of BIOS settings via BCU. See Configuring the Set BIOS Configuration task step for more details.

c. Call Intel RSTCli Command Line Utility - Configure RAID Volume: Configures the RAID volume on the target client.

i. Replace the command: Like the step to delete all metadata, the command line in the step, `rstcliXX.exe`, is a placeholder. See the utility documentation and replace the placeholder command with the actual command. The package containing the command line utility needs to be selected. The following is an example of the command line to configure RAID level one (mirror) with hard drives:

```
IntelRSTCli\12.8\x64\rstcli64.exe --create --level 1 -n Volume
0-0-0-0 0-10-0
```

`IntelRSTCli\12.8\x64` is the relative location from the source folder to the actual command line utility in the content of the package.

ii. Select the Intel command line tool package prepared earlier.

d. Remove Disk Partitions (diskpart clean): This step does not need configuration; however, for the task sequence to properly run on all disk scenarios, the deployment and all packages and content within it need to be configured to allow access to the content directly from the network. See Allowing access to deployment content for more information.

e. Format & Partition Disk: By default, the task sequence has the BIOS (legacy/MBR) format step enabled and the EFI (GPT) step disabled. If deploying to a system that is set to UEFI or UEFI Hybrid (with CSM), enable the EFI format step and disable the BIOS format step.

f. Apply Driver Pack–Specifies the HP driver pack imported for the target platform and operating system.

g. Require Reboot to PXE/USB–Because this task sequence requires one or more immediate reboots in the WinPE when the disk has not been defined yet, the RebootStep variable is used to control the flow of the task sequence.

3. Review each task sequence step and set parameters as needed for the rest of the task steps. If these steps do not work, verify that you entered the correct network credentials in the task sequence creation dialog.

4. After all task sequence steps have been configured, select OK or Apply to save changes. The task sequence can now be modified and task sequence steps can be added as needed to perform your desired operations.

Assigning a boot image

Use this procedure to assign a boot image.

1. Right-click the task sequence and select **Properties**.

2. Select the **Advanced** tab and then select **Use a Boot Image**.

3. Select **Browse**, and then select the appropriate boot image that had the Intel RST RAID driver added during the boot image preparation.

NOTE: Select the boot image with the same architecture as the operating system being deployed (for example, an x86 image for an x86/32-bit operating system and an x64 image for an x64/64-bit operating system).

Allowing access to deployment content

To run properly, the Remove Disk Partitions (diskpart clean) step in the HP MIK Configure RAID Example task sequence needs to be run directly from the network. For this to happen, all packages and content in the task sequence (including the boot image) need to be configured as follows:

1. Right-click the content/package and select **Properties**.
2. Select the **Data Access** tab, and select **Copy the content in this package to a package share on distribution points**.
3. Select **OK**.
4. When deploying, the access content directly from the distribution point option can be selected on the **Distribution Points** step.
5. After the task sequence has been modified and amended as needed, deploy to the target collection and distribute content as needed to use the task sequence. Follow the on-screen instructions to complete this process.

Task sequence execution flow

The task sequence is divided into three task groups: Configure Hardware, Configure RAID, and Install Operating System.

Conditions on the three groups and a computer variable are used to control the processing of the task sequence across multiple reboots over PXE/USB. The Set RebootStep Variable task increments the RebootStep variable by one (1) each time it is executed. If the variable is not present, it is created and set to 0 before being incremented.

During the initial execution of the task sequence, the tasks in the Configure Hardware group are executed. After rebooting and re-executing the task sequence, the Set RebootStep Variable task increments RebootStep to two (2). Because the Configure Hardware group has the condition that it only runs when the value of the RebootStep variable is one (1), this group is skipped after the reboot. The next group, Configure RAID Volume, looks for a RebootStep value of two (2), then it is executed. The last group, Install Operating System, looks for a RebootStep value of three (3). If this condition is met, the third group of steps runs.

Towards the end of the task sequence, the Reset RebootStep Variable task resets RebootStep to zero (0). Note the following additional points about deploying a task sequence:

- When deploying a task sequence with reboot to PXE/USB, on the Distribution Points screen, set the deployment options to Access content directly from a distribution point when needed by the running task sequence. For this option to be available for each package referenced by your task sequence, select the Data Access tab of the Properties dialog box, and select **Copy the content in this package to a package share on distribution points**.

- If the task sequence is deployed as Available and not as required, the task sequence must be selected upon reboot for deployment to be continued.
- The target client system must have the appropriate boot order set for reboots for this step to work properly. (That is, if booting via PXE, the PXE NIC should be before any other boot devices in the boot order.) To rerun a required task sequence on a target client system, clear the PXE advertisement:

  1. In Configuration Manager, select **Assets and Compliance** workspace.
  2. Select **Devices**.
  3. Select the target client system.
  4. Select **Clear Required PXE Deployments**.

- If the task sequence failed to run completely, it might be necessary to clear or reset the RebootStep variable as follows:

  1. Right-click the target client system and select **Properties**.
  2. Select the **Variables** tab.
  3. Select the RebootStep variable, and then select the delete button with the X-like icon.

16 HP BIOS Configuration Utility (BCU)

HP BIOS Configuration Utility (BCU) is a free tool that enables you to do the following:

- Read available BIOS settings and their values from a supported desktop, workstation, or notebook computer
- Set or reset Setup Password on a supported desktop, workstation, or notebook computer
- Replicate BIOS settings across multiple client computers For more information, see the HP BIOS Configuration Utility User Guide

NOTE: The version of BCU included with HP MIK includes a batch file (RunBCU.cmd) that automatically detects the current operating system and runs the correct version of BCU (32- or 64-bit).

17 HP Password Utility

HP Password Utility is a tool for creating an encrypted password file that can be used with an HP BCU password file parameter. This tool is included with HP BCU.

For more information, see the HP BIOS Configuration Utility User Guide.

18 HP Reports

Using HP Reports, IT admins have the ability to generate and save different type of reports.

- HW & BIOS inventory reports
- Policy compliance report
- Important security updates reports
- Available HP product releases

Generating HP Reports

Use this procedure to generate HP Reports.

1. Launch the HP MIK Reports Dashboard.
2. Navigate to one of the following sections to generate a report:
   - Hardware Inventory
   - Compliance Reports
   - Bulletins
3. To generate a report:
   a. Select the Device collection in which the client machine is added.
   b. Build a query by selecting different selection options.
   c. Select **Generate Report**.

- Saved Reports lists all reported saved.
- A blank value cannot generate a report.

19 HP Programmable Key

HP Programmable Key allows user to program a key to launch applications, assign shortcut key execution and enter input text at a press of button.

Creating a policy

Use this procedure to create a policy using HP Programmable Key.

1. In Configuration Manager, select **Client Security**, and then select **Overview**.
2. Select **HP Manageability Integration Kit**, right-click **HP Programmable Key**, and then select **Create Policy**.
3. Enter a baseline name, and then start the creating policy wizard.
4. Enter URL for function key + Programmable Key combination.
5. Select **Create Policy**.
6. Select **Save and Deploy Policy**.

20 HP Patch Assistant

HP Patch Assistant periodically reports on the health of a collection of devices and optionally bring devices up to date, to improve end-user experience, device stability and overall security.

Configuring HP Patch Assistant for device collections

You can configure HP Patch Assistant for a device collection or multiple device collections by navigating to HP Patch Assistant Node under HP Manageability Integration Kit node.

To configure HP Patch Assistant for device collections, select **HP Patch Assistant** > **Dashboard Link** > **Configure HP Patch Assistant**.

Configuring HP Patch Assistant for a single device collection

You can configure HP patch Assistant for a specific device collection.

1. Select a device collection under SCCM Device Collection node.
2. Right-click from the menu option for HP Patch Assistant.
3. Select **Configure Settings**.
4. Scroll down to schedule the policy, and then select **Save and Deploy**.

Table 20-1 Configuration settings

Settings Name	Options
Operation	Select the action to perform • Report - Retrieves the list of recommendations. • Report & Remediations - Downloads and Installs all recommendations.

Table 20-1 Configuration settings (continued)

Settings Name	Options
Preferences	Selection • All - All Recommendations • Critical - Only Critical Recommendations Category • All - Selected by default You can select any individual category for BIOS, Drivers, Software, Firmware. **NOTE:** If you select Report & Remediations operation, updates for the selected category will be download and installed.
BIOS Admin Password	• No Password set -If BIOS password not configured on collection. • BIOS Password - Specify the BIOS password set. • BIOS File Password - Specifies the complete path of the encrypted BIOS administrator password file. **NOTE:** The BIOS Password file should be accessible with Local System Account.

Table 20-1 Configuration settings (continued)

Settings Name	Options
Repository	From HP – Choose this option, to select the latest updates available for the selected category from the HP site directly. Configuration of proxy (Optional). • Address: Enter the proxy URL • Port: Enter the proxy port number • Domain: Enter the proxy domain name • User / Password: Enter access credentials **NOTE:** If not specified, the proxy setting on the device will be used. Custom location: For users, to use an onsite repository to recommend and install the updates from the repository. This option requires an offline repository that you can create using the HP Client Management Script Library. For more information, see: • https://developers.hp.com/hp-client-management • https://www.hp.com/us-en/solutions/client-management-solutions/download.html • https://developers.hp.com/hp-client-management/doc/client-management-script-library

Table 20-1 Configuration settings (continued)

Settings Name	Options
Trigger Hardware Inventory Updates	Select the option to trigger the Hardware Inventory cycle run on the SCCM client, immediately after every HP Patch Assistant scheduled task execution.
Schedule	• Option 1 - Users can configure HP Patch Assistant task to run outside of active hours. In case active hour is not configured task will default to run at 8 PM. • Options 2: Specify the exact time.
Reset to default settings	Post installation of MIK with support of HP Patch Assistant, click on this link will load HP default settings. On the successful configuration of HP Patch Assistant for a collection, HP defined defaults will be replaced with the last known configuration. So a reset to default settings will load the last saved configurations.

Dashboard

The dashboard displays the health status for devices that are HP Patch configured and data synched with SCCM.

Table 20-2 Dashboard data settings

Data category	Description
Good	Device does not require any updates.
Fair	Device has at least 1 recommended update and not remediated.

Table 20-2 Dashboard data settings (continued)

Data category	Description
Poor	Device has at least 1 critical update that is pending remediation.
No Data	Data not available for some collection.
Installation Successful	All remediations were successful.
Installation Failure	At least one remediation was unsuccessful.
Actions Required	Device has recommendations that need actions.

Filter Dashboard

To have the dashboard list data only for certain collections, select **Filter Dashboard** on the Dashboard page.

The left list box shows the device collections that have been configured for HP Patch Assistant. Use the arrow buttons to add / remove collections, and then select **Apply**. The dashboard displays only data for the selected collections.

The selection will last for the current SCCM sessions. If HP Patch Assistant is configured for any new collection, you needs to manually add that collection.

Viewing a report from the dashboard

You can click on the hyperlink available on the dashboard to see per device data for that category.

Click the device name to see the report, and then click on the **Installation Successful** hyperlink to see report details.

Viewing a report for a device collection

You can configure HP Patch Assistant for a specific device collection, by selecting a device collection under the Device Collection node, and then selecting the collection from the menu option for HP Patch Assistant.

Select **View Report** to view the report.

Removing HP Patch Assistant configuration

Use this procedure to remove the HP Patch Assistant configuration.

1. Navigate to SCCM **Device Collection** node.
2. Select the device collection for which the HP Patch Assistant policy was configured and deployed.

3. Right-click to select **Configure Settings**.
4. Select **Revoke Policy** and then select **Save and Deploy**. On Policy evaluation HP Patch Assistant configuration is removed.

21 Uninstalling HP MIK

Use this procedure to uninstall HP MIK.

1. In Control Panel, select **Programs and Features**.
2. Select **HP Manageability Integration Kit**, and then select **Uninstall**.

A Device collection query examples

IT administrators can create device collections defined by query rules in Configuration Manager.

For more information on how to create device collection and query rules, go to https://technet.microsoft.com/en-us/library/gg712295.aspx.

NOTE: HP recommends verifying your device collection queries in a test environment to ensure accurate software and policy deployment to supported systems before pushing the queries out to production environments.

The following examples are some basic HP collection queries that can be used as a starting point when working with HP systems and HP MIK features.

All HP systems

NOTE: Older models might have Hewlett-Packard named as the manufacturer. The query might need to have a condition to include those systems. Be sure to check the support platform list for each HP MIK feature to create the appropriate system collections to manage the feature.

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from
SMS_R_System inner join

SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%'
```

All HP Systems including older models

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from
SMS_R_System

inner join SMS_G_System_COMPUTER_SYSTEM on
SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId

where
```

```
(SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'Hewlett-Packard%' and
SMS_G_System_COMPUTER_SYSTEM.Model not like '%Proliant%') or
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%
```

HP systems with a specific model name

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from
SMS_R_System

inner join SMS_G_System_COMPUTER_SYSTEM on
SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId

and SMS_G_System_COMPUTER_SYSTEM.Model = 'HP EliteBook 850 G4'
```

Windows 10 Enterprise systems

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup,

SMS_R_SYSTEM.Client

from SMS_R_System inner join SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%'

inner join SMS_G_System_Operating_System on SMS_R_System.ResourceID =
SMS_G_System_Operating_system.ResourceID

and SMS_G_System_Operating_System.Caption like '%Windows%10%Enterprise%'
```

Determining whether Device Guard can be enabled

To determine which systems can have Device Guard enabled, go to https://techcommunity.microsoft.com/blog/microsoft-security-blog/managing-windows-10-device-guard-with-configur and then follow the steps in the Determine applicable systems section.

B Systems with HP Sure Start support

For all HP client computers with HP Manageability Integration Kit, HP Sure Start support information can be retrieved via the Configuration Manager hardware inventory extension.

To add HP_SureStartPolicy BIOS Sure Start settings and HP Sure Start version information to the Configuration Manager default client settings:

1. In Configuration Manager, select **Administration workspace**, and then select **Client Settings**.
2. Right-click **Default Client Settings**, and then select **Properties**.
3. In the *Default Settings* window, select **Hardware Inventory** and then select **Set Classes**.
4. In then **Hardware Inventory Classes** window, select **Add**.
5. In the *Add Hardware Inventory Class* window, select **Connect**.
6. If Configuration Manager is installed on an HP system that has the HP MIK client installed, then leave the default computer name (which is the system the console is on). Otherwise, specify the name of a system that has the HP MIK client installed.
7. Enter `root\HP\InstrumentedServices\v1` for the WMI namespace.
8. Select **Recursive**, and enter your name and password to connect to the WMI of the specified system.
9. Add the HP_SureStartPolicy class. Select **OK** to add the class to hardware inventory.
10. Select **OK**, and then select **OK** again to close all windows.

After client computers download the updated machine policy and run the hardware inventory cycle, the extended data is reported to Configuration Manager. The data then is available to create collections.

The following is the query to select all HP systems with HP Sure Start support.

```
select SMS_R_SYSTEM.ResourceID, SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client

from SMS_R_System inner join SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%'

inner join SMS_G_System_HP_SureStartPolicy on SMS_R_System.ResourceId =
SMS_G_System_HP_SureStartPolicy.ResourceId

and SMS_G_System_HP_SureStartPolicy.SureStartVersion like 'SS%'
```

TPM queries

These example TPM queries use TPM data from the Win32_TPM class of the ROOT\cimv2\Security\MicrosoftTpm namespace from clients. Be sure that this TPM class is added to hardware inventory. When a client computer applies the latest machine policy and reports its hardware inventory data has been reported to Configuration Manager, the client must be included in the appropriate TPM collection.

Systems with TPM Version 1.2

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from
SMS_R_System inner join

SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and

SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%' inner join

SMS_G_System_TPM on SMS_R_System.ResourceId = SMS_G_System_TPM.ResourceId
and MS_G_System_TPM.SpecVersion like '1.2%'
```

Systems with TPM Version 2.0

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from
SMS_R_System inner join

SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and

SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%' inner join

SMS_G_System_TPM on SMS_R_System.ResourceId = SMS_G_System_TPM.ResourceId
and SMS_G_System_TPM.SpecVersion like '2.0%'
```

Systems with a specified application installed

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,
```

```
SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from
SMS_R_System

inner join SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and

SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%' and
(SMS_R_System.ResourceId in (select ResourceId from

SMS_G_System_ADD_REMOVE_PROGRAMS_64 where ProdID = '' and Version

> = '<Miminum supported application version>')

or (SMS_R_System.ResourceId in (select ResourceId from
SMS_G_System_ADD_REMOVE_PROGRAMS where ProdID = '' and Version >= '')))
```

For example, the following query returns the systems with HP WorkWise version 1.3.1.1 or later installed.

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from
SMS_R_System

inner join SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and

SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%' and

(SMS_R_System.ResourceId in (select ResourceId from

SMS_G_System_ADD_REMOVE_PROGRAMS_64 where ProdID = '{56051A5A-7A04-4CD4-
A5CD-781F1AC10112}' and Version >= '1.3.1.1')

or (SMS_R_System.ResourceId in (select ResourceId from
SMS_G_System_ADD_REMOVE_PROGRAMS where ProdID = '{56051A5A-7A04-4CD4-A5CD-
781F1AC10112}' and Version >= '1.3.1.1') ))
```

C Troubleshooting

See the following sections for troubleshooting information.

HP MIK installation issues

An error occurred while installing a supporting package (HP Client BIOS Configuration Utility or HP Client Support Tools) Verify that you account running the installer has permission to access the Configuration Manager server and modify the data, or log on as a user that has those permissions.

- HP MIK did not completely uninstall: Imported driver packs, created boot images, and task sequences created via HP MIK are not removed when the product is uninstalled. If they are no longer needed, they can be deleted from Configuration Manager.
- A task sequence fails to run after reinstalling and/or repairing the installation: When reinstalling and/or repairing the installation, existing task sequences using packages installed by HP MIK are not automatically updated. To function correctly, task sequence references must be refreshed. See Refreshing task sequence references for details.

Driver pack issues

See the following information for driver pack issues.

Configuration Manager reports that the SoftPaq is not a valid driver pack: Only driver packs under the category Manageability - Tools can be imported with HP MIK. Other driver packs listed under other categories (such as Software - System Management) cannot be used with HP MIK.

HP MIK fails to complete the driver pack import process while processing driver INFs: This might happen if an existing driver is detected but the driver source is missing. Verify that the existing driver's source is present. If not, either delete the driver and reimport the driver pack or restore the missing driver source.

WinPE image creation issues

See the following information for WinPE image creation issues.

Some available boot images are not selectable as base boot images: Because each version of Configuration Manager supports the customization or adding drivers and components to a specific version of WinPE only, the HP MIK Create Boot Image feature can provide only limited support. For more information about the specific requirements for WinPE customization, go to http://technet.microsoft.com/en-us/library/dn387582.aspx.

If ADK and the operating system of your site server fail to appropriately verify the signature of some drivers during the boot image creation, you might get this HP MIK error:

```
Object version mismatch error; a ConfigMgr object has been modified or
updated before changes could have been saved. try the operation again.
```

If a retry attempt fails, manually customize or add the drivers to your boot image.

Troubleshooting a task sequence

See the following information for troubleshooting task sequences.

Before troubleshooting a task sequence

See the following information before troubleshooting a task sequence.

- Verify your task sequence settings. The primary cause of task sequence failures is related to the settings you provided in the task sequence steps. Be sure to check the task sequence steps for the following:
  - Valid environment or task sequence variable references.
  - Valid package references: You must make sure that all packages referenced in the task sequence are available from the distribution points and are up to date.
- Verify that the task sequence was created with the currently installed kit or a previously installed version that was updated. If the kit was uninstalled and then reinstalled, or an HP Client Support Package was removed but reinstalled via setup, the HP packages need to be selected again for the task sequence steps that use them. See this document for more information on updating task sequences with new package references.
- Verify that the downloaded driver packs are removed properly by HP MIK.
  - Driver packs downloaded by HP MIK are stored in `%TEMP%\hpdriverpack`, where `%TEMP%` is the environment variable defining the default application temporary location for the currently logged on user. HP MIK attempts to remove the downloaded driver packs after a successful import.
- Verify and examine log files.
  - Configuration Manager Console log files are located in the AdminUILog folder. This folder is located in the install directory of the Configuration Manager Console.
  - Log files generated by HP MIK are stored in `%TEMP%\hpclient`, where `%TEMP%` is the environment variable defining the default application temporary location for the currently logged on user.

    Extended logging information can be added to the kit log files by adding a debug flag to the registry. In the registry, add a DWORD value named DebugLogging and set the value to 1 for the applicable registry key:

    `HKLM\Software\Wow6432Node\HP\Client\ConfigMgr Integration Kit`
  - Additional applicable log files may be available in the Configuration Manager log folder (typically located at `%ProgramFiles%\Microsoft Configuration Manager\Logs).`

Common task sequence problems

The following are some common problems that might be encountered. If an issue is not listed here, the subsequent troubleshooting sections might provide answers.

Some drivers fail to be injected into the boot image

This might occur when a driver is signed with a newer driver signing method than what DISM and the operating system support. In that case, the driver is treated as an unsigned driver and is not injected into the boot image. For example, when running SCCM 2012 SP1 on Windows Server 2008

R2, some Windows 8/8.1 drivers cannot be injected into a Windows Preinstallation Environment boot image. If the driver in question is not required for your environment, remove the driver from the boot image driver list, and then manually reinject the remaining drivers. For more information, go to https://technet.microsoft.com/en-us/library/hh825070.aspx.

Task sequence fails to start after target platform boots to Windows Preinstallation Environment

There are several possible causes:

- There is no network connection because the network adapter is unsupported.
- There is no network connection because the boot image does not contain the necessary network driver.
- Configuration Manager does not recognize the target HP client platform.
- One or more of the packages referenced by the task sequence are not available.

To resolve this issue:

1. Install a supported network adapter and set it as the PXE NIC.
2. Use an HP Client WinPE image containing the appropriate HP WinPE driver pack.
3. Verify that the target HP client platform was imported into Configuration Manager with the correct identification information.
4. Open the task sequence and fix any errors that might be present.

Updated or new BIOS configuration input files were not used or available during task sequence execution

Verify that the HP Client BIOS Configuration Utility package was pushed to the appropriate distribution points.

Task sequence starts, but fails to continue

There are several possible causes, as follows:

- A BIOS setting or BIOS configuration change prevents the system from correctly starting.
- The incorrect driver package was selected for the target platform.

To resolve this issue:

1. Verify that the correct driver package was selected for the given target platform.
2. Verify that all dependencies of the task sequence were distributed to distribution points or groups that the target clients or collections can access.

Task sequence fails to open for editing, or error messages appear when viewing certain task sequence steps

There are several possible causes:

- The plugin has been uninstalled. (Error messages such as “There may be too many steps in the task sequence object” might appear.)
- The plugin is corrupted.

- HP MIK has not been installed on the primary site server.

To resolve this issue:

1. Reinstall the plugin to verify that all necessary files are present and registered.
2. Install HP MIK on the primary site server.
3. Repair the plugin installation. This can be done either by running the setup again and selecting Repair or by selecting the Repair option in Programs and Features in Control Panel.
4. Recreate the task sequence in a new task sequence.
5. Reselect the packages for some task sequence steps (see Refreshing task sequence references).

Task sequence creation and management issues

See the following for task sequence creation and management issues .

The **There may be too many steps in the task sequence object** error displays when attempting to edit a task sequence created by HP MIK: This error generally appears when HP MIK has been uninstalled from the server. HP MIK must be reinstalled to the server before the task sequence can be viewed or edited.

The Remove Disk Partitions (diskpart clean) step is needed, but you cannot use the Access Content Directly option: There are a number of workarounds that are possible, including the following:

- Use the Connect to Network Folder task sequence step to connect to the network share containing the package files, and use a Run Command Line task to run the step from the network share.
- Add the package files to the boot image and use a Run Command Line task to run the step, referencing the files in the boot image.

See the Configuration Manager documentation for details about how to perform these actions.

Task sequence execution issues

See the following task sequence execution issues.

System fails to boot using PXE

If the client machine is EFI x86 (IA-32), such as the HP ElitePad 900, then Cumulative Update 1 for Configuration Manager 2012 SP1 (KB2817245) must be installed for PXE boot to work successfully. Configuration Manager 2012 R2 does not need this update.

PXE is an extension of DHCP, which uses a broadcast type of communication. Broadcast communication uses standard timeout values that are not readily changeable. As a result, a computer waits for a default timeframe to receive a DHCP or PXE response before timing out and causing a failure condition. Each time a computer is rebooted, it must renegotiate the connection to the switch. Some network switches arrive configured with default settings that might cause connectivity delays. The settings on the switch might cause a DHCP or PXE timeout because they fail to negotiate a connection in time.

The following features might be affected by negotiation timeouts:

- Spanning Tree Protocol (STP)—STP is a protocol that prevents loops and provides redundancy within a network. A networking device using this algorithm might experience some latency as it collects information about other network devices. During this period of information collection, servers might boot to PXE and time out while waiting for a response from Windows Deployment Services. To prevent these issues, disable the STP or enable PortFast on end-node ports for the target server. For further information, see the manufacturer's documentation.

- EtherChannel or Port Aggregation Protocol (PAgP)—EtherChannel enables multiple links between devices to act as one fast link and share the load between the links. Running the EtherChannel Protocol in automatic mode might cause a connectivity delay of up to 15 seconds. To eliminate this delay, switch to a manual mode or turn off this feature.
- Speed and duplex negotiation—If auto-negotiation on the switch is set to off and the server is not configured to that speed and duplex setting, then the switch does not negotiate with that server.

  Verify that PXE is also running properly on the server. The system must be set to boot off PXE before any other bootable devices are present in the system.

Verify that PXE is also running properly on the server. The system must be set to boot off PXE before any other bootable devices are present in the system.

System booted PXE, but timed out waiting for the PXE server to respond

Verify that the WinPE boot images are pushed to the appropriate distribution point. In addition, the distribution points used must have PXE enabled.

To verify this setting:

1. Select Administration, select Site Configuration, and then select Server and Site System Roles.
2. Select the appropriate distribution point.
3. Right-click the Distribution Point role, select Properties, and then select PXE.

WinPE never starts the task sequence

See the SMSTS.LOG file at X:\windows\temp\smstslog\smsts.log. If a package does not download or cannot be accessed, you might not have the appropriate network drivers installed. You might need to update the WinPE image with newer WinPE drivers for the target platform. Verify that all packages referenced in the task sequence are available from the distribution point. WinPE validates all packages to make sure they are available before processing the task sequence.

A task sequence reports "Failed to resolve task sequence dependencies", with the driver pack imported by HP MIK as the dependency at fault, even though the content status says "Distributed".

There is an issue with Configuration Manager where sometimes the hashes for a package are not generated, which results in the device being unable to locate the content since the hashes are used for those purposes.

To resolve this issue:

1. Select the driver pack.
2. Right-click and select **Update Distribution Points**.
3. Select **Yes** on the dialog box that appears.

After the process completes, the driver pack can be located and resolved by the task sequence.

Target system failed to run or use an updated BCU file

You must update the distribution points containing the BCU package when you modify, add, or remove a configuration file.

The default boot order does not enable PXE to boot when a valid drive exists

When an active partition is created on a hard drive, it automatically becomes a bootable device if a valid operating system has been installed. If the PXE NIC is after the hard drive in the boot order, then the hard drive boots to Windows before PXE or causes an "Invalid System Partition" error if Windows is not installed.

To resolve this issue:

1. Verify that PXE is placed before the hard drive in the boot order.
2. If necessary, set the boot order using HP Client BIOS Configuration Utility in a task step.

   or

   Set the boot order in the BIOS on the target platform. See the platform documentation for specific instructions on how to do this.

   For more info on using BCU to set the boot order, see Configuring the Set BIOS Configuration task step.

   If PXE is first in the boot order, the computer does not actually boot to PXE unless Configuration Manager has a mandatory task sequence for it to run.

Task sequence fails with the error "Failed to Download Policy"

This error code (0x80093102 or 0x80004005) refers to a certificate validation issue. The SMSTS.LOG file displays an entry with any of the following text:

```
CryptDecryptMessage ( &DecryptParams, pbEncrypted, nEncryptedSize,0,
&nPlainSize,0 ), HRESULT=80093102 no cert available for policy decoding
```

The following are possible causes:

- A misconfiguration of your domain or site server, such as the DNS not pointing to the site server or the site server not specifying a valid FQDN (which is referred to by the DNS listing), can cause this error. If your site server does not specify a FQDN and only specifies the NETBIOS name, and your DNS server tries to refer to the FQDN, an incorrect lookup might cause this error.
- The certificate being used for PXE and boot media is blocked or missing. Verify whether any of the certificates under the Site Settings node are blocked or missing. Open the certificates to verify that they are actually installed into the certificate store. If not, install them.

  If the task sequence still fails, remove the package from the distribution points and/or groups, and then add it back. This causes the package hash to be regenerated.

A task sequence does not run again even after clearing the PXE advertisement

You must make sure that the deployment is set to allow a rerun so that the advertisement is applied to the computer regardless of whether it previously ran the task sequence.

To resolve this issue:

1. On the properties page of the deployment, select Scheduling.
2. Select Rerun behavior.

Task sequence fails at Apply Operating System step with "Failed to make volume X:\bootable" error message

This issue is indicated by log content similar to the following message:

```
MakeVolumeBootable( pszVolume ), HRESULT=80004005
```

```
(e:\nts_sms_fre\sms\client\osdeployment\applyos\installcommon.cpp,759)

Failed to make volume E:\ bootable. ensure that you have set an active
partition on the boot disk before installing the operating system.

Unspecified error (Error: 80004005; Source: Windows)

ConfigureBootVolume(targetVolume), HRESULT=80004005

(e:\nts_sms_fre\sms\client\osdeployment\applyos\applyos.cpp,326)

Process completed with exit code 2147500037
```

To resolve this issue if you are using a Format & Partition action in your task sequence to partition the hard drives for MBR systems:

Select the **Make this the boot partition** option. If you do not select this option and the computer has a single hard drive, then the task sequence engine automatically makes one of the partitions the boot partition. If there are multiple drives, it cannot automatically determine which boot partition must be bootable.

System environment variables are not carried over to the next action in the task sequence

When a task sequence runs, commands are executed in a command shell. When that task ends, so does that command shell environment, causing the loss of any system variables defined within that task. Verify that variables that pass between tasks are set as Task Sequence variables, Collection variables, or Machine variables.

Task sequence reported an error while executing

Although there can be a wide variety of reasons why a task sequence fails to fully execute, there are a number of common reasons that might need to be resolved to fix the task sequence execution issue:

- Verify that the DNS and WINS servers are working properly and are stable.
- Verify that the supplied credentials in the task sequence steps have the necessary access rights to the SCCM server to clear and set task sequence variables and PXE flags.
- If attempting to apply BIOS settings via the BCU while in WinPE, the disk must already be partitioned and formatted to allow downloading of the package to the system.

Examining the log files as shown in Diagnosing driver pack or task sequence errors on page 66 might also provide insight into the reason for failure.

Diagnosing driver pack or task sequence errors

See the following information about diagnosing driver pack or task sequence errors.

1. Export the task sequence by right-clicking the task sequence and selecting Export.
2. If the issue appears, collect screen captures of the relevant portions.
3. If the issue is related to the installation of the product or occurs soon after installation:
   - Copy the MSI installation log located in the temporary files directory (locate using the `%TEMP%` environment variable). This file is usually located in a "1" directory and has a random name that is formatted as follows:

     `MSI<RandomCharacters>.LOG.`

- Copy the support packages installation log located in the temporary files directory (locate using the %TEMP% environment variable). The file name is `HPClientSCCM2012Kit-setup.log`.

4. If the issue occurred while using the console, copy the HP MIK log files located in %TEMP%\hpclient. In addition, the Configuration Manager console log files located in the AdminUILog folder of the Configuration Manager console should be copied as well.

5. If the issue occurred while running a task sequence, the following files should be copied from the WinPE environment. These files can be accessed during task sequence execution by pressing F8 to open the command prompt. To use the command prompt in WinPE, select the Enable command support option for the boot image. This option can be found by right-clicking the boot image and selecting Properties, and then selecting Windows PE.

   a. Copy the SMSTS.LOG file from where WinPE might be stored:

      - For PXE boot: X:\Windows\Temp\Smstslog
      - On a local (for example, C: or D:) drive under \Smstslog
      - SMSTSLOG<Time-Based-Name>.LOG

   b. Copy the files used as input to the configuration task, such as configuration INI or XML files.

   c. Copy `SetupAPI.APP.LOG and SetupAPI.DEV.LOG` from WinPE stored in `X:\Windows\inf for PXE boot`.

6. If the error relates to baselines and policies, capture the following log files:

   - HP MIK console log files located in `%PROGRAMDATA%\HP\HP MIK\Logs B`. All HP MIK client side log files located in `%PROGRAMDATA%\HP\HP MIK\Logs`
   - `%\SYSTEMROOT%\System32\config\systemprofile\AppData\Roaming\hpqLog\com.hp.si am.log`

7. If examining these log files does not help you resolve the issue and you need to contact HP, prepare a complete, detailed explanation of the issue, including the following:

   - The exact point of failure (for example, the action running when the process failed, a description or screen captures of error messages and error codes)
   - A detailed description of the computers being configured (model, hardware configuration, and NIC details) – A description of other circumstances, such as the following:
     - Has this task sequence or action ever worked?
     - If so, when did it stop working?
     - If it has worked before, what is different now? Is the task sequence being applied to different computer types, is it using different configuration files or different task sequence variables, or has something else been modified?

D Security Provisioning

See the following sections on security provisioning.

Successfully provisioning a client system

The IT Administrator needs to ensure that the keys required for provisioning are saved in a secure location.

The Signing Key is used every time a setting in HP Sure Run or HP Sure Recover is changed. The Key Endorsement Certificate is only used in cases where an update to the Signing Key needs to be made.

A one-time reboot of the client system is required after policy deployment.

After the reboot, the end user will be prompted to type in 4-digit security code as displayed on the screen.

Updating provisioning for provisioned systems

To update both the Signing Key and Key Endorsement Certificate, the IT Administrator will have to first deprovision and then perform Initial Provisioning again.

If the private half of the Signing Key becomes compromised it can be replaced by choosing the “Update Provisioning” option and selecting a new signing key, then clicking Next.

NOTE: Should the private half of the key endorsement certificate become compromised the method used to replace it depends on the state of the private half of the signing key on the client systems.

If the signing key has not been replaced on the client systems perform a deprovision and do the initial provisioning again with a new signing key pair and a new endorsement certificate. It is important to verify that all systems were successfully updated.

If the signing key has been replaced on the client systems, it is necessary to use the “Unprovision SPM” option on the “Secure Platform Management” menu in BIOS F10 Setup (this option is not available remotely).

Unprovisioning a client system

See the following information for unprovisioning a client system.

1. Multiple “Evaluate” attempts (within Configuration Manager) might be required in some cases for deprovisioning to be successful.
2. It is recommended to first send out a policy with HP Sure Run disabled and/or HP Sure Recover disabled followed by a second policy push with Deprovision selected.

System fails to be unprovisioned

Refer to the following information for a system that fails to be unprovisioned.

HP Sure Run / HP Sure Recover can only be managed via the local (HP Client Security Manager) or remote (MIK) approach, on a first come, first served basis. Once enabled and configured using one of these approaches, the other is no longer available until it is unconfigured and disabled. This can be accomplished by using the “Unprovision SPM” option on the “Secure Platform Management” menu in BIOS F10 Setup (this option is not available remotely).

If the signing key or endorsement certificate is lost, it is possible to manually deprovision HP Sure Run and HP Sure Recover by using the “Unprovision SPM” option from the Secure Platform Management menu in BIOS F10 Setup (this option is not available remotely).

BIOS Admin password

While a BIOS Admin Password is not required to use HP Sure Run or HP Sure Recover, it is recommended to use a BIOS administrator password to prevent an attacker with physical access from disabling HP Sure Run or HP Sure Recover via the HP Computer (BIOS) Setup page.

Security Provisioning for HP Sure Admin or Client Security: HP Sure Run and HP Sure Recover

You need Security Provisioning enable HP Sure Admin, HP Sure Run, and HP Sure Recover.

1. Provisioning is needed only once. If ITDM has pushed a provisioning policy for either HP Sure Admin or Client Security successfully, provisioning step can be skipped for subsequent policy for same collection.
2. Deprovisioning policy push as part of HP BIOS Authentication – Security Provisioning or Client Security – Security Provisioning will result in all dependent features disabled.

E Key generation for HP MIK

The Key Endorsement Certificate used by HP Sure Run and HP Sure Recover contains the top level key used to authorize all other operations. As such, the intent is that its corresponding private key is strongly controlled.

In the future, the firmware will enforce the requirement of the certificate being an EV certificate. For now, the firmware supports using self signed certificates to test HP Sure Run and HP Sure Recover.

The following are sample steps to generate a Key Endorsement Certificate and Signing Key Certificate using the open source openssl command. At the end of these steps you will have a key endorsement certificate in the file key_endorsement_cert.pfx and a signing key certificate in the file signing_key_cert.pfx.

⚠ **CAUTION:** These instructions are creating private keys that will be used to securely configure the Sure Run / Sure Recover on platforms. Appropriate care should be taken to protect the files being generated here as well as the temporary files create.

NOTE: On some Windows versions of OpenSSL, it may be necessary to set up an environment variable to point to the openssl configuration file. Without this these openssl command may not generate output.

Creating the Key Endorsement Certificate

Use the following information to create the Key Endorsement Certificate.

del key.pem

del cert.pem

1. Generate a certificate to use for the key endorsement certificate (the command below should be typed as a single line):

```
openssl req -x509 -nodes -newkey rsa:2048
-keyout key.pem -out cert.pem -days 3650
-subj /C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com
```

NOTE: The -subj command line parameter in the first command should be updated to reflect information specific to your organization. If you do not include this parameter openssl will prompt you for the information. This information may be reported to users and admins in future versions of the firmware so it should be correct.

2. Convert the self-signed public certificate to PKCS#12 format (the command below should be typed as a single line):

```
openssl pkcs12 -inkey key.pem -in cert.pem -export
-keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES
-out key_endorsement_cert.pfx
-name "Sure Run / Sure Recover Key Endorsement Certificate"
```

In this step you will be prompted for the export password. You must only press enter without entering a password.

NOTE: The files key.pem and cert.pem are temp files that should be securely discarded.

NOTE: The private key in use here is unprotected in all files.

Creating the Signing Key Certificate

Use the following information to create the Signing Key Certificate.

1. Ensure that the temp files do not exist from the prior operations

   del key.pem

   del cert.pem

2. Generate a certificate to use for the key endorsement certificate (the command below should be typed as a single line):

   openssl req -x509 -nodes -newkey rsa:2048 -keyout

   key.pem -out cert.pem -days 3650

   -subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

NOTE: The -subj command line parameter in the first command should be updated to reflect information specific to your organization. If you do not include this parameter openssl will prompt you for the information.

3. Convert the self-signed public certificate to PKCS#12 format (the command below should be typed as a single line):

NOTE: In this step you will be prompted for the “Export Password” – do not enter the password, just press enter.

NOTE: The files key.pem and cert.pem are temp files that should be securely discarded. The private key in use here is unprotected in all files.

   openssl pkcs12 -inkey key.pem -in cert.pem -export

   -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES

   -out signing_key_cert.pfx

   -name "Sure Run / Sure Recover Signing Key Certificate"

- Once you have selected Submit Certificate, the files are loaded and stored as an embedded property within the site control. At this point the files are no longer needed.
- If MIK has a problem with the certificate or key provided it displays a generic message like “Failed to store signing key certificate” or “Failed to store key endorsement certificate”.
- The keys are required to be 2048 bits in length and use an exponent of 0x10001.

New Custom Category

With Gen 3 HP Sure Run S/W ITDM now can define or specify custom process that they want to be monitored.

- Only 10 custom processes can be added.
- If new custom process is part of Standard Category, it will not be saved.
- ITDM: Need to ensure the path of the process and publisher details are correctly entered, MIK S/W cannot validate the same and will send as is. If any incorrect information is entered with respect to location of the application or the publisher, HP Sure Run S/W will report it as non-compliance will perform the configured remediation action.

Specifying the path to the binary to be monitored

Refer to the following for information about specifying the path to the binary to be monitored.

- Sure Run Gen3 and earlier the full path to the binary being monitored must be specified.
- At this time, environment variables like, %ProgramFiles% and %ProgramFiles(x86)%, cannot be used in the path.

Finding the publisher

The publisher field is generated from the certificate used to sign the image. If you do not have the certificate available you can use the sigcheck tool from SysInternals

Go to https://learn.microsoft.com/en-us/sysinternals/downloads/sigcheck.

For example:

```
C:\>sigcheck64.exe \Windows\system32\mspaint.exe

Sigcheck v2.73 - File version and signature viewer

Copyright (C) 2004-2019 Mark Russinovich

Sysinternals - www.sysinternals.com

C:\windows\system32\mspaint.exe

Verified: Signed

Signing date: 3:22 AM 9/15/2018

Publisher: Microsoft Windows

Company: Microsoft Corporation

Description: Paint

Product: Microsoft Windows Operating System

Prod version: 10.0.17763.1

File version: 10.0.17763.1 (WinBuild.160101.0800)
```

```
MachineType: 64-bit
```

In the output above the value you would specify for the publisher would be “Microsoft Windows”.

Additional requirements

The “Original filename” property found in **Details** tab when viewing the properties of a file needs to match the name of the executable. If not, Sure Run cannot verify that this is the file it is expecting to monitor.

Currently you need to disable sure run from watching the image before you attempt to update it.

HP Sure Admin

Refer to the following for information about HP Sure Admin.

Passphrase rules

ITDM can control access to QR Code with passphrase. Allowable characters are upper/lowercase characters, numbers and special characters other than < or >. Current limitations include:

- Special Character is must in a passphrase.
- Passphrase cannot end with special character.

Security provisioning needed for HP Sure Admin

Refer to the following for information about security provisioning needed for HP Sure Admin.

IMPORTANT: If you skip the provisioning step, HP Sure Admin cannot be activated.

HP Sure Admin Manage Keys

ITDM is responsible to manage the Local Access Keys generated. ITDM based on enterprise policy needs to control the access and back up of Local Access Keys at an alternate secure location.

Also, if keys are created with the same name and at the same location they will be overwritten, no warning message will be displayed.

Create and export keys with Azure Ad

Azure AD Group type needs to be of type security and should have a valid email id associated with it.

Create and Send Key to Azure Ad Group One drive

User need to ensure required permissions are associated for the credentials used for login, so that the QR code file can be created on one drive path specified.

Create and Send Key to Azure Key management store

You must ensure that TLS 1.2 is enabled on server.

Multiple iterations may be needed to enable Sure Admin on managed device

In scenarios where a configuration policy is pushed to set BIOS Admin Password, Security Provisioning, Enable Sure Admin AND/OR set BIOS settings -OR- Configure Client security, the policy will not get successfully applied in the first iteration. Security provisioning and the PPI process need to have been

done first for Sure Admin to be enabled and Local Access Key to be set. Also, the exact sequence of CI execution cannot be predetermined / predicted or controlled on SCCM client.

Analysis indicates that min two or max four iterations may be needed for the policy to be applied successfully in above scenario.

Recommended Best Practice

Before you push Configuration Item or policy to set BIOS or Client Security settings using Sure Admin

- 1st push policy to provision systems on which HP Sure Admin needs to be enabled.
- 2nd push policy to enable Sure Admin on the managed device. System which does not support HP Sure Admin, BIOS admin password will be set.

IDTM can now schedule policies to set BIOS settings or configuration of client security software.

Other information

Existing legacy Baselines created for HP BIOS Password can be accessed using the new BIOS Authentication Plugin.

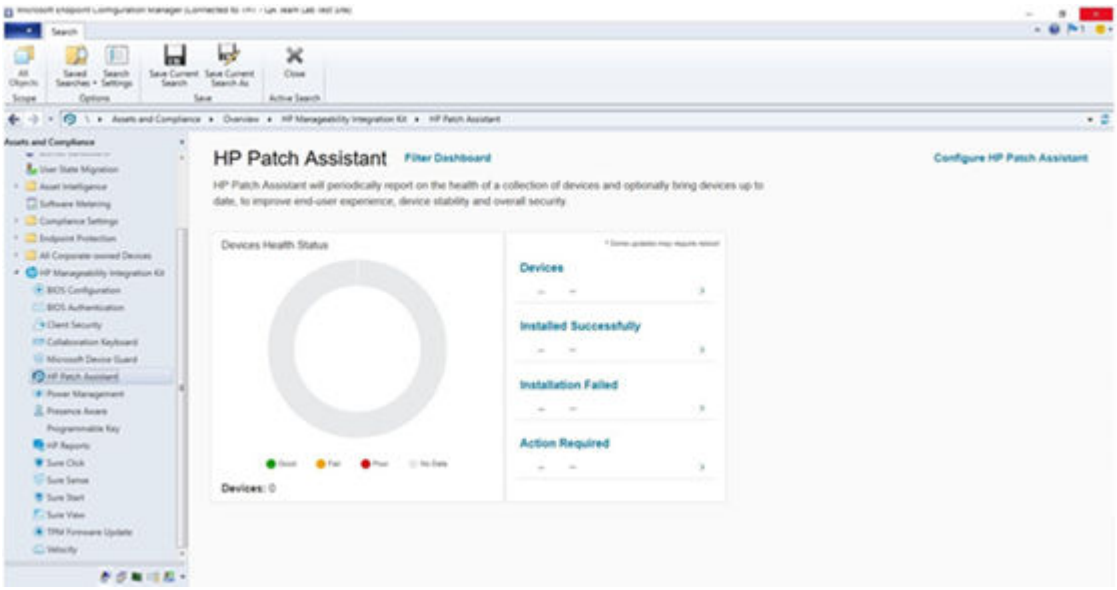
ITDM must take a call to set either BIOS or BEAM or both based on the platforms in the collection.

HP recommends that you use HP Sure Admin for enhanced security.

HP Patch Assistant

Refer to the following for information about HP Patch Assistant.

The image below shows HP Patch Assistant Configured for a device collection. Data is not yet synched with SCCM.



Index