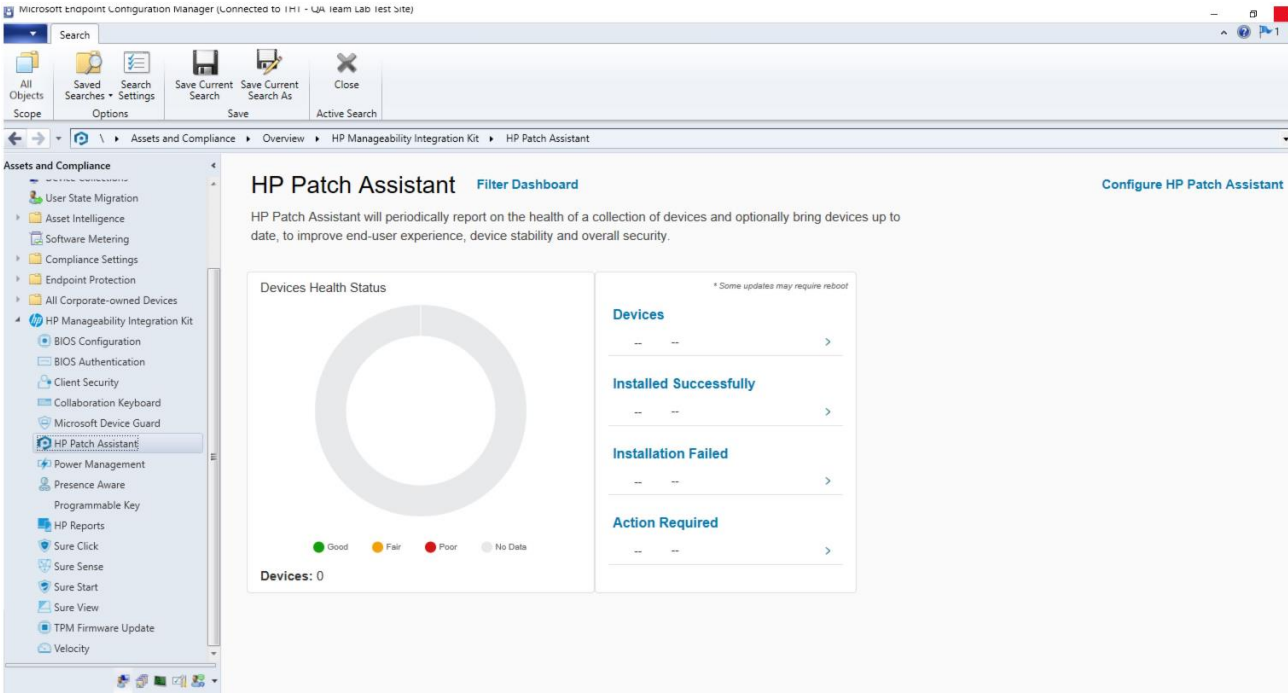
HP Manageability Integration Kit
HP Client Management Solutions

October 2022

Table of contents

Contents


Search
All Objects
Saved Searches
Search Settings
Save Current Search
Save Current Search As
Close
Scope
Options
Save
Active Search
Assets and Compliance
Overview
HP Manageability Integration Kit
HP Patch Assistant
Assets and Compliance
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
All Corporate-owned Devices
HP Manageability Integration Kit
BIOS Configuration
BIOS Authentication
Client Security
Collaboration Keyboard
Microsoft Device Guard
HP Patch Assistant
Power Management
Presence Aware
Programmable Key
HP Reports
Sure Click
Sure Sense
Sure Start
Sure View
TPM Firmware Update
Velocity
HP Patch Assistant
Filter Dashboard
Configure HP Patch Assistant
HP Patch Assistant will periodically report 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.
Devices Health Status
Good
Fair
Poor
No Data
Devices: 0
* Some updates may require reboot
Devices
Installed Successfully
Installation Failed
Action Required

1 Overview

HP computers are Designed for Manageability (DfM), DfM is centered on two tenets:

- Provide a means that will assist an IT administrator in managing HP BIOS, hardware, and preinstalled software that comes with the computer.
- Provide 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 client-management-console-agnostic solution that extends management aspects to HP hardware, BIOS, and software capabilities.

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

Deploy HP MIK to begin enjoying these key benefits:

- 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, set authentication and credentials requirements, enable Device Guard, and manage Trusted Platform Module (TPM) firmware updates.
- Manage software—Enable IT administrators to remotely manage features supported by the software, such as HP Client Security.

HP MIK is optimized to work with Microsoft® System Center 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.

2 System requirements

HP Manageability Integration Kit can be installed on servers running supported versions of Microsoft System Center Configuration Manager 2012 and clients running supported Windows® operating systems.

2.1 Supported Microsoft System Center Configuration Manager versions

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

- Microsoft System Center 2012 R2 Configuration Manager service pack 1 (SP1) with or without cumulative update 1 (CU1) or later
- Microsoft System Center 2012 R2 Configuration Manager
- Microsoft System Center 2012 Configuration Manager SP2 with or without CU1 or later and
- Microsoft System Center 2012 Configuration Manager SP1 and
- Microsoft System Center Configuration Manager 1511 or later

2.2 Supported client operating systems

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

NOTE
Some HP Manageability Kit features have additional requirements.

- Windows 10

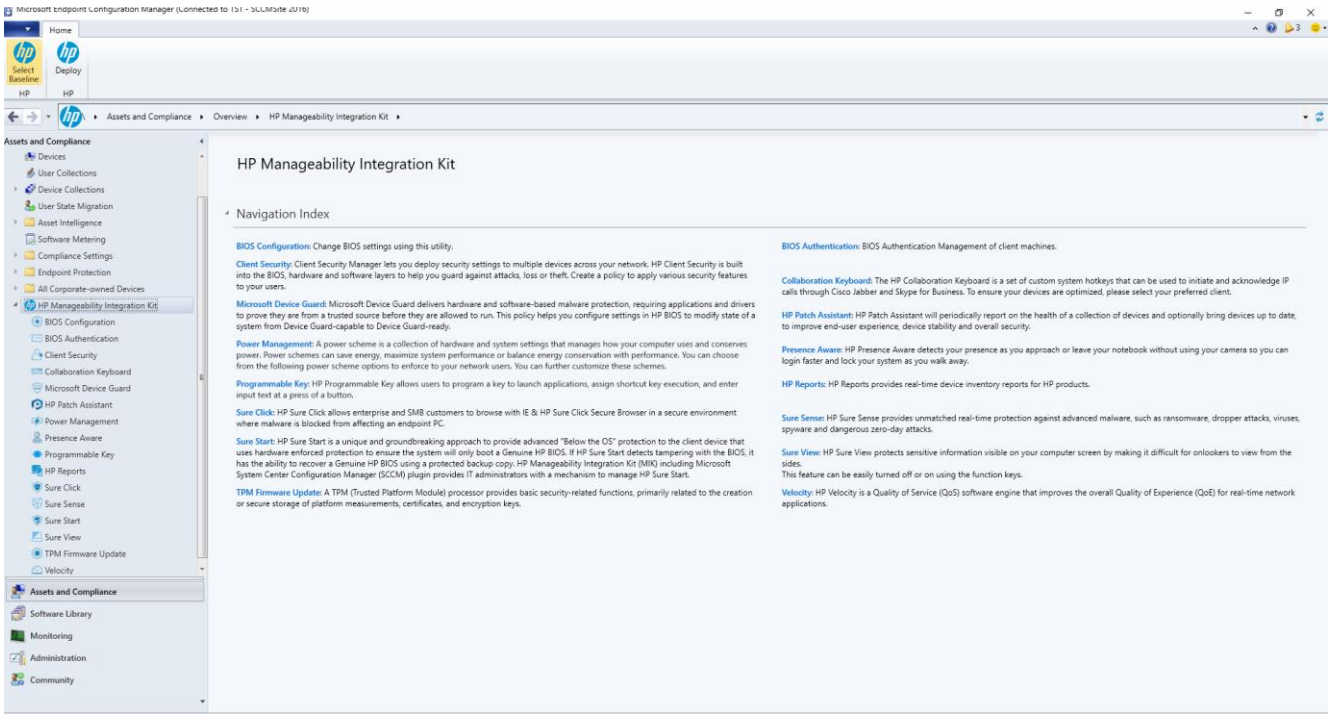
3 Downloading HP Manageability Integration Kit

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 System Center Configuration Manager.
4. Under MIK Client requirements, download the corresponding SoftPaqs for the features MIK will be used to manage

4 Installing 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 System Center 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.



4.1 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, select Overview, select Application Management, select Packages, and then select HP Client Support Packages.

NOTE
Do not delete or rename the packages in this folder to prevent failure of dependent task sequences.
If a package is deleted, reinstall HP Manageability Integration Kit and select Repair in the installation wizard. Then, refresh the task sequences using the package. For more information, see Refreshing task sequences.

2. f this is a first-time installation, right-click HP Client BIOS Configuration Utility and select Distribute Content, and

then follow the on-screen instructions to complete the wizard.

– or –

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

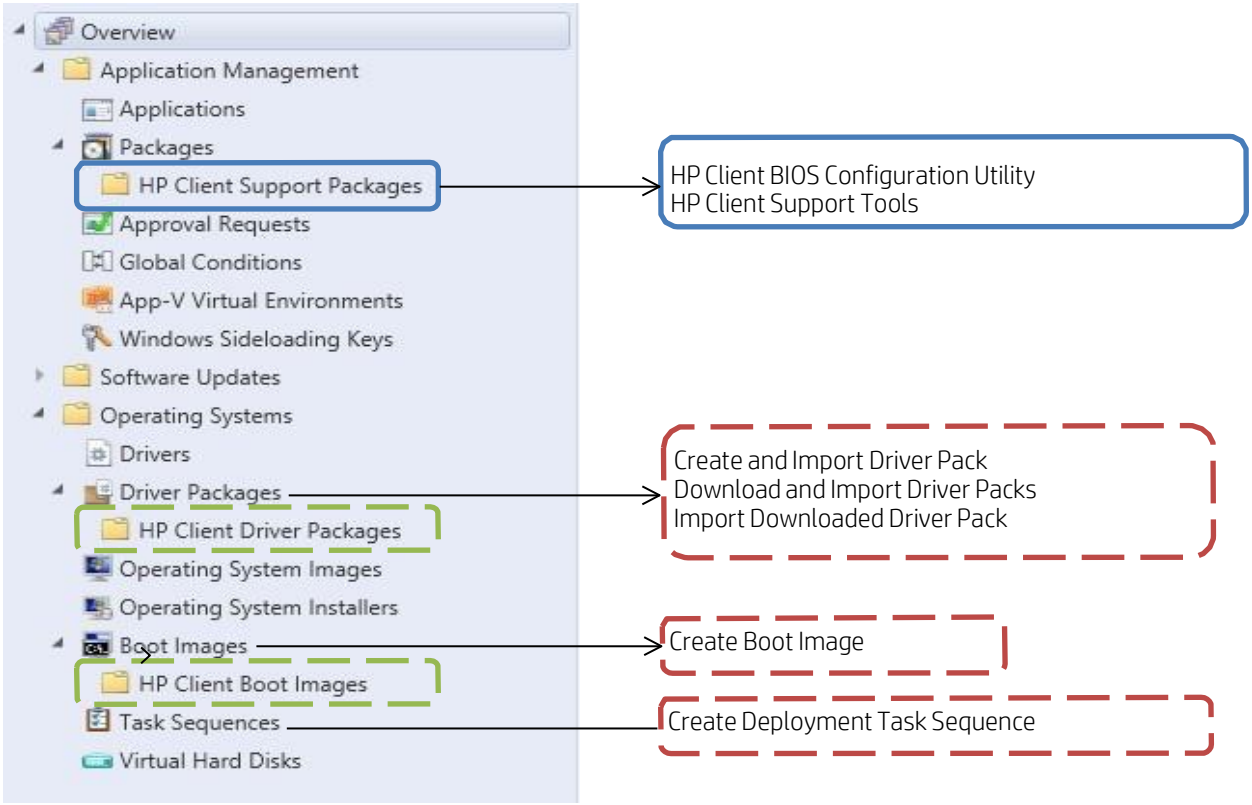
3. If this is a first-time installation, right-click HP Client Support Tools and select Distribute Content, and then follow the on-screen instructions to complete the wizard.

   – or –

   If this is an upgrade, right-click HP Client Support Tools and select Update Distribution Points and follow the onscreen instructions to complete the wizard.

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:

- HP BIOS Configuration
- HP BIOS Authentication (replacing legacy HP BIOS Password Manager)
- HP Client Security – (Includes sub-plugins for HP Sure Run , HP Sure Recover)
- HP Collaboration Keyboard
- Microsoft Device Guard
- New – HP Patch Assistant
- Power Management
- Programmable Key
- HP Reports
- Sure Click
- Sure Sense
- HP Sure Start
- HP Sure View
- TPM Firmware Update

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

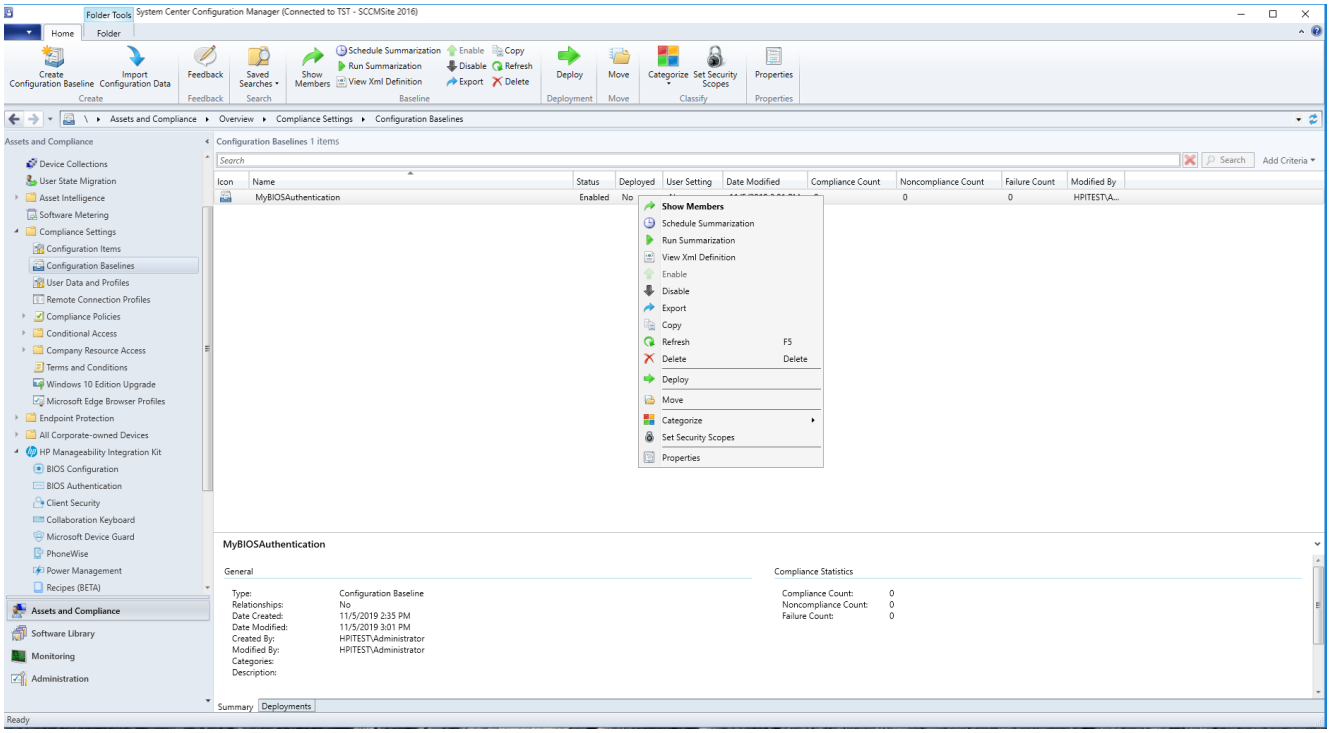
5.1 Compliance settings

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, select Compliance Settings, and then select 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.

5.2 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 BIOS Admin Password and HP Sure Admin settings on client systems.

6.1 Supported client platforms

- HP commercial computers (2015 or later) for BIOS Admin Password.

6.2 Supported client operating systems

- Windows 10

6.3 Prerequisites

- Microsoft .NET Framework 4.8 or higher.
- HP Manageability Integration Kit

6.4 User interface

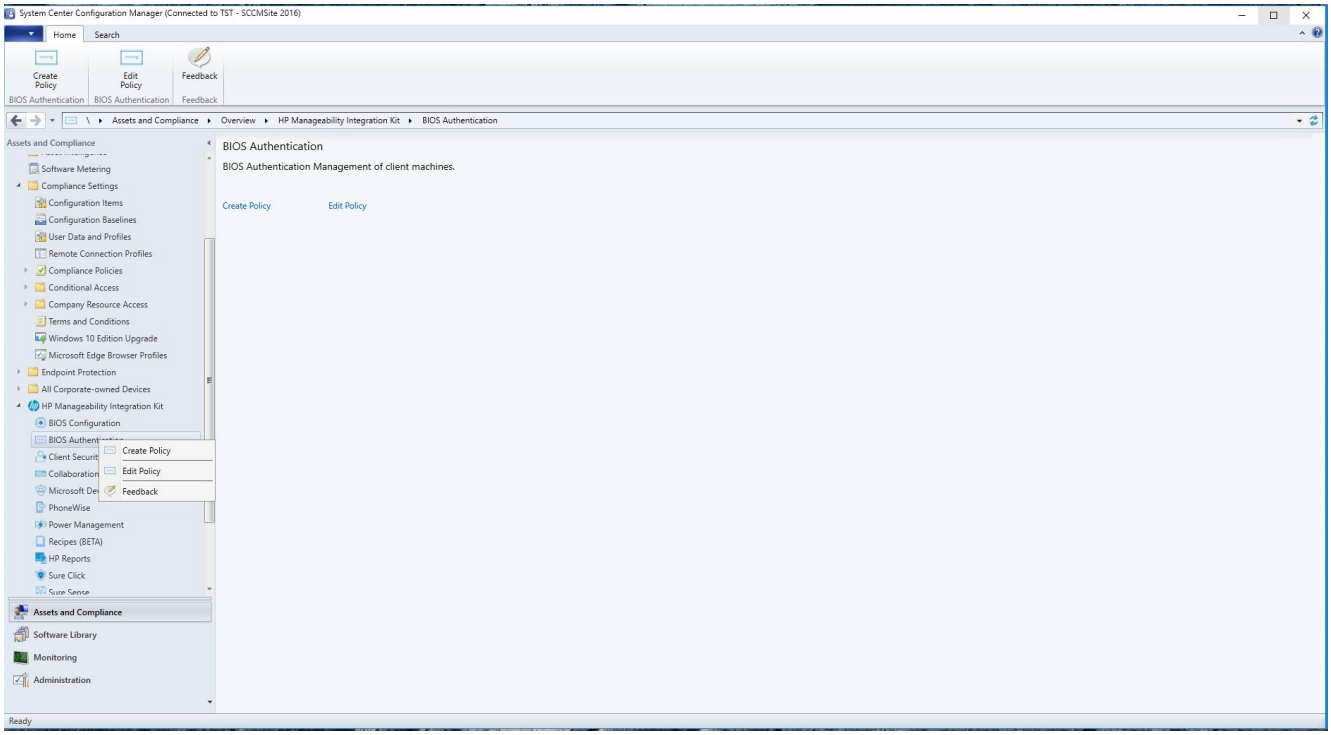
HP BIOS Authentication interface is divided into 2 section

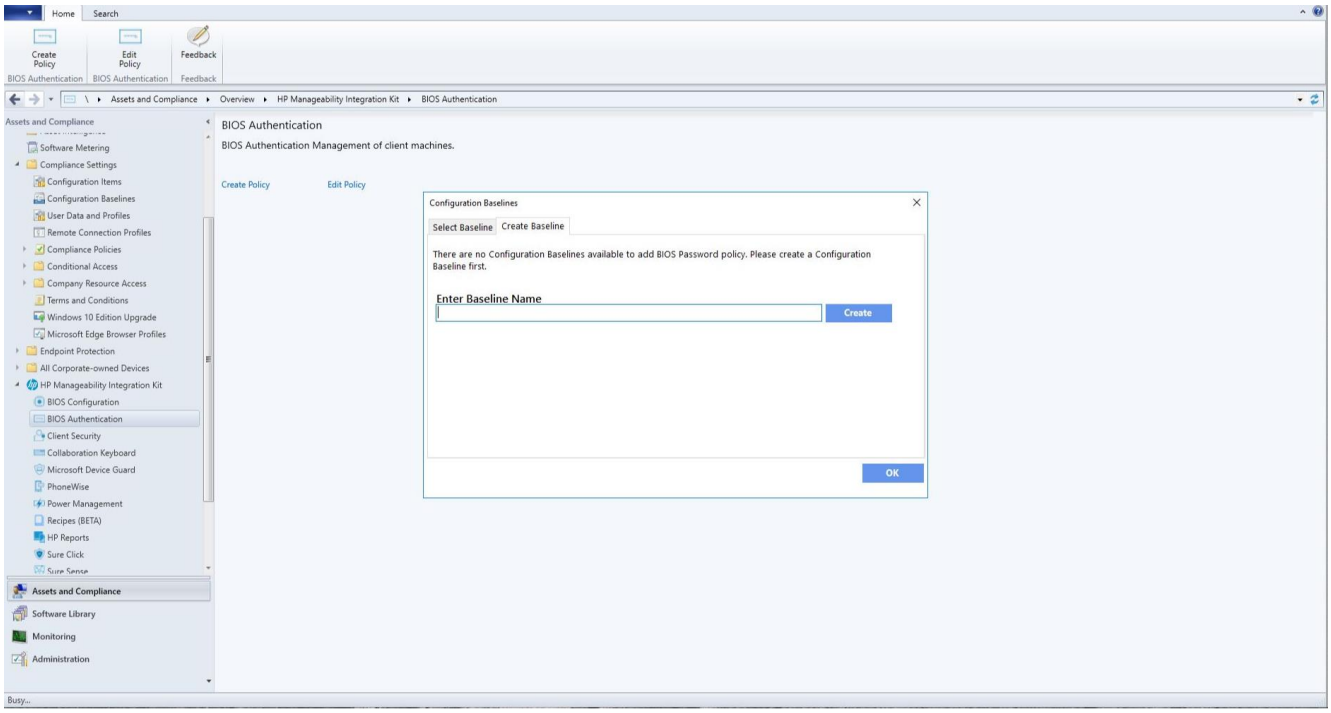
Manage BIOS Password
The BIOS Password UI is very simple with two sections, current BIOS password and modification password (Change/Set or Remove password). Note - The current password must be provided to change or remove BIOS Password.

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.

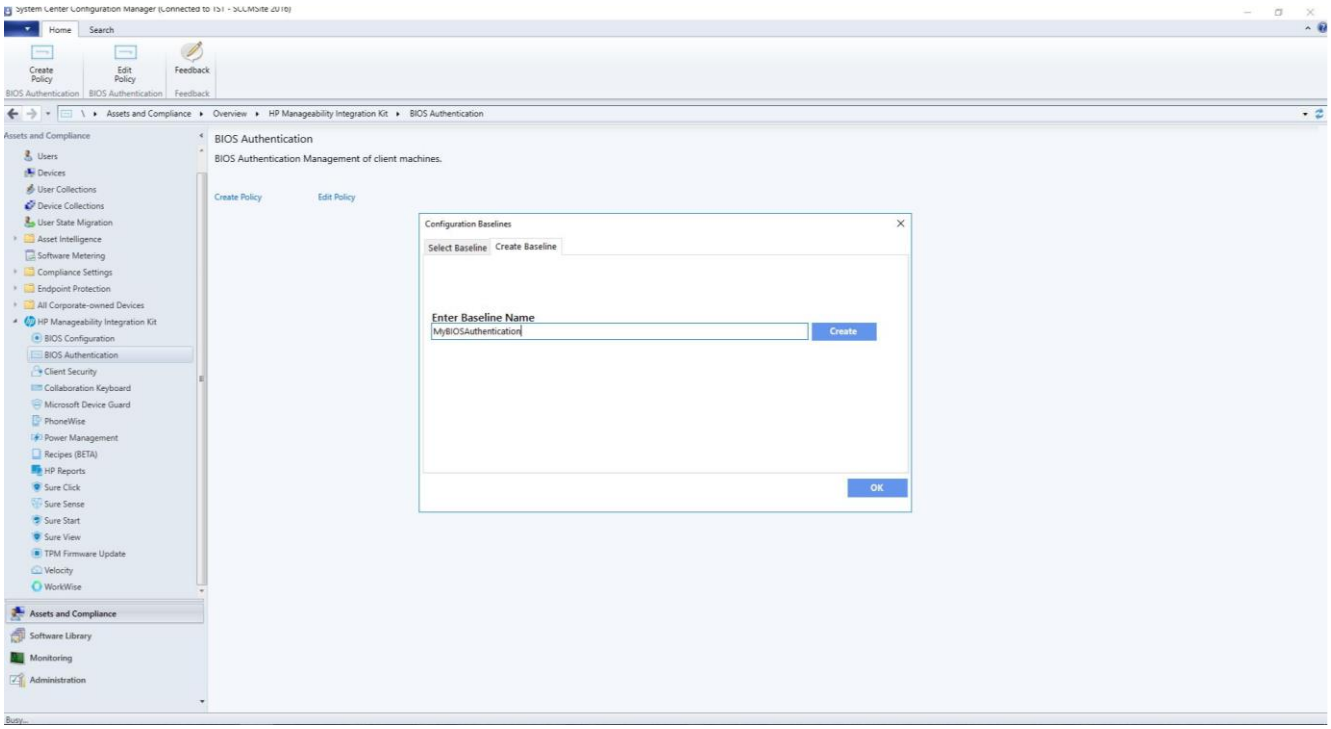
6.5 Creating a policy

1. In Configuration Manager, select Assets and Compliance, and then select Overview.
2. Select HP Manageability Integration Kit, right-click **BIOS Authentication**, and then select Create Policy.

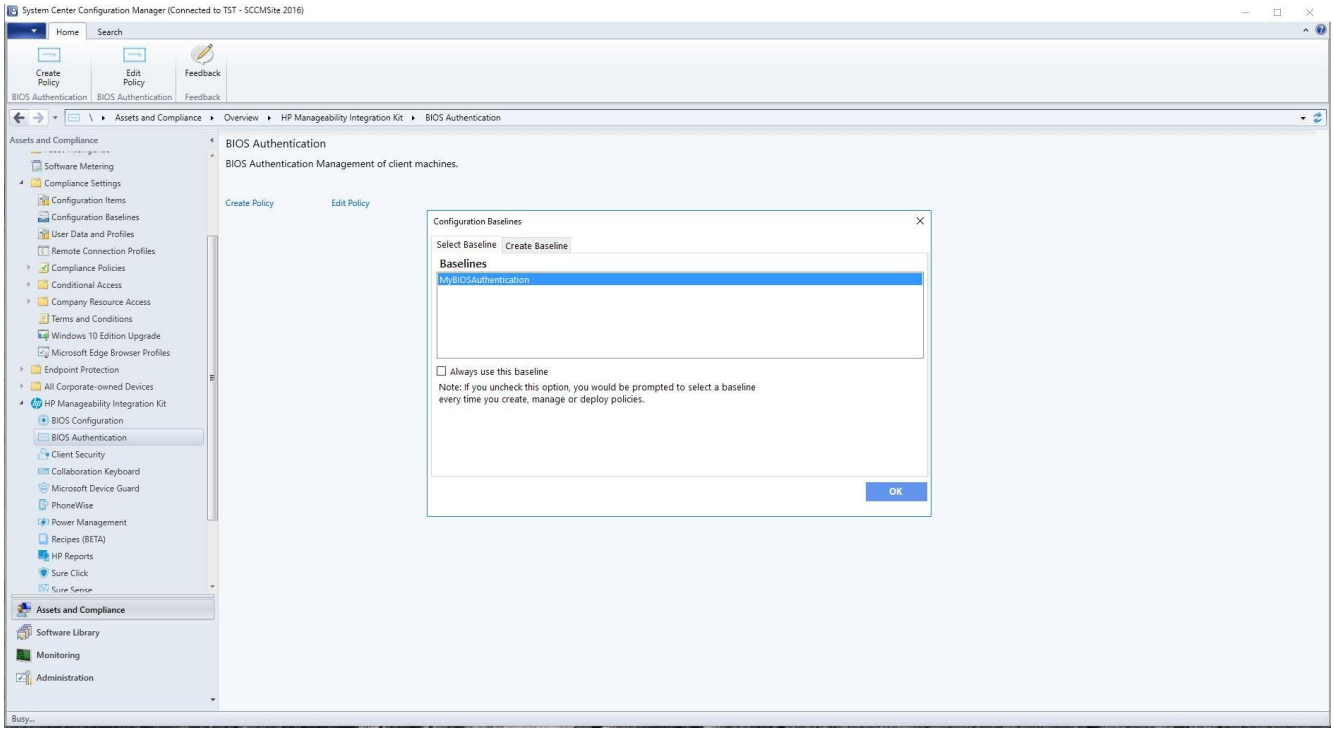




3. Enter a Baseline name and start the creating policy wizard.

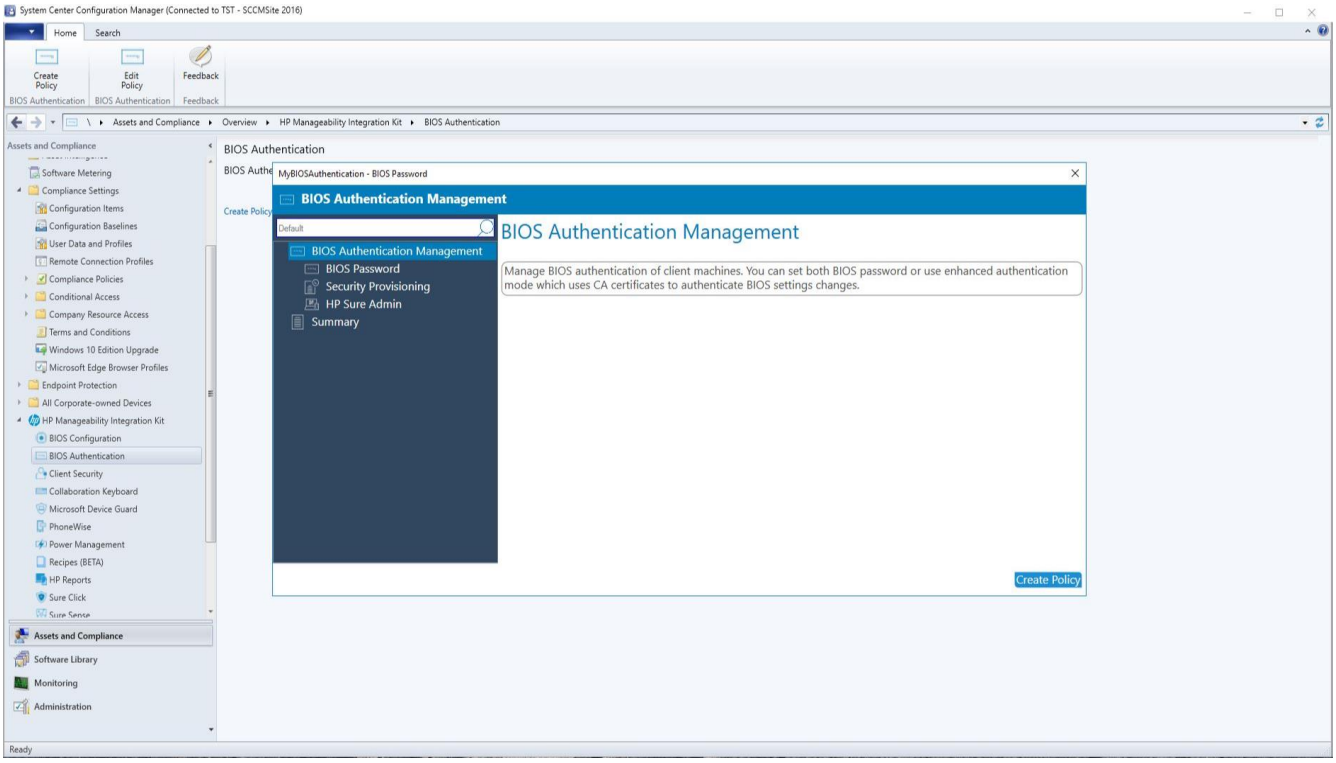


4. Click Create



5. Select the newly created baseline and click OK

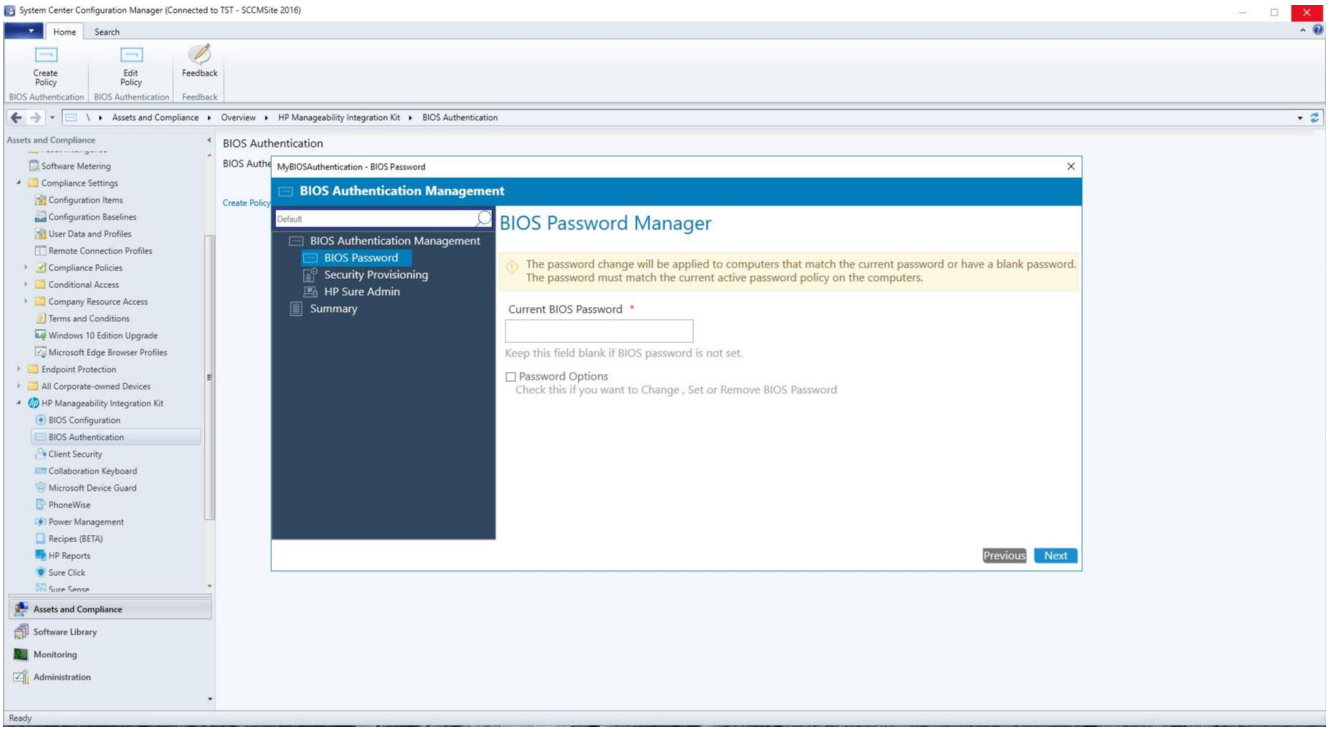
6. In BIOS Authentication Management UI click on Create Policy.



6.6 BIOS Password

Allows managing BIOS Admin Password on legacy platforms that don't support HP Sure Admin.

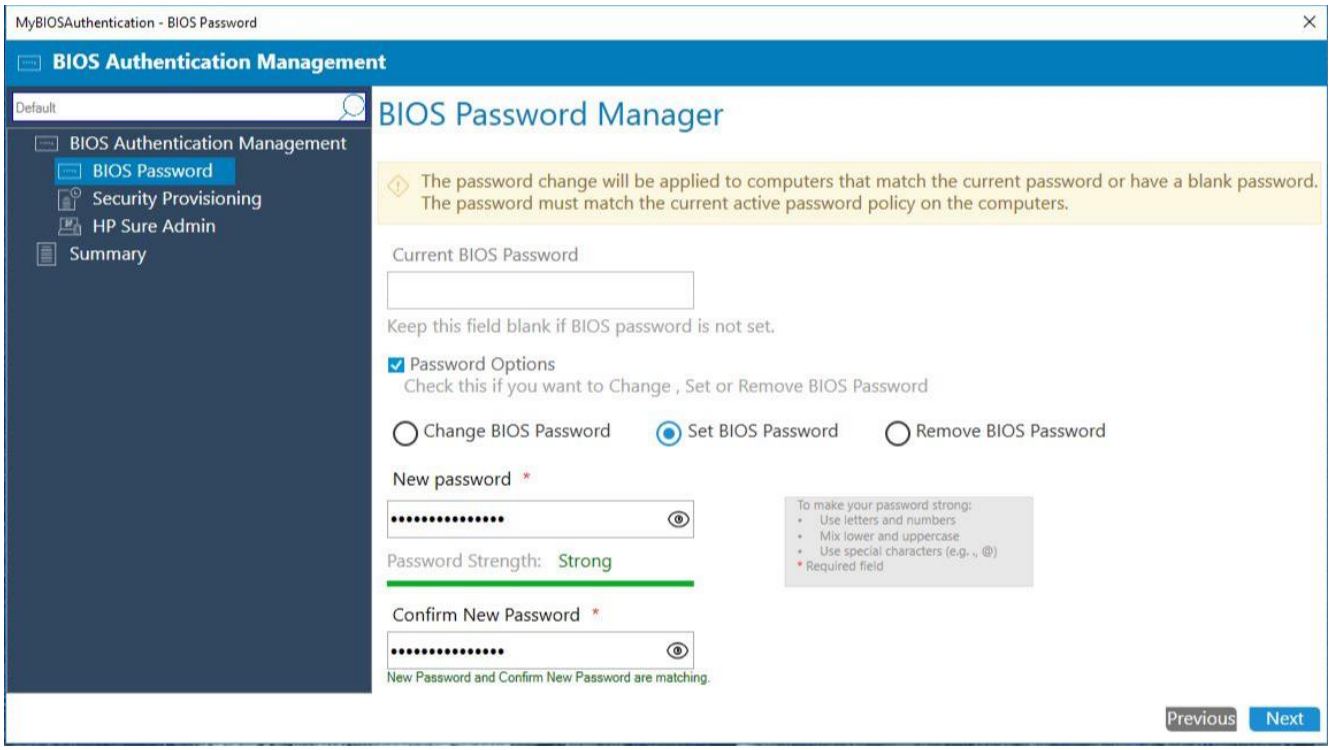
Note – If the user decided not to set any BIOS password, they can navigate to the next screen. A blank password is considered as no BIOS password to be set on a managed platform.



6.6.1 Set BIOS Password

To set a brand-new BIOS Password on client system where there is no current BIOS Password set.

1. Select the radio button Set Password and provide the password in both New Password and Confirm New Password fields

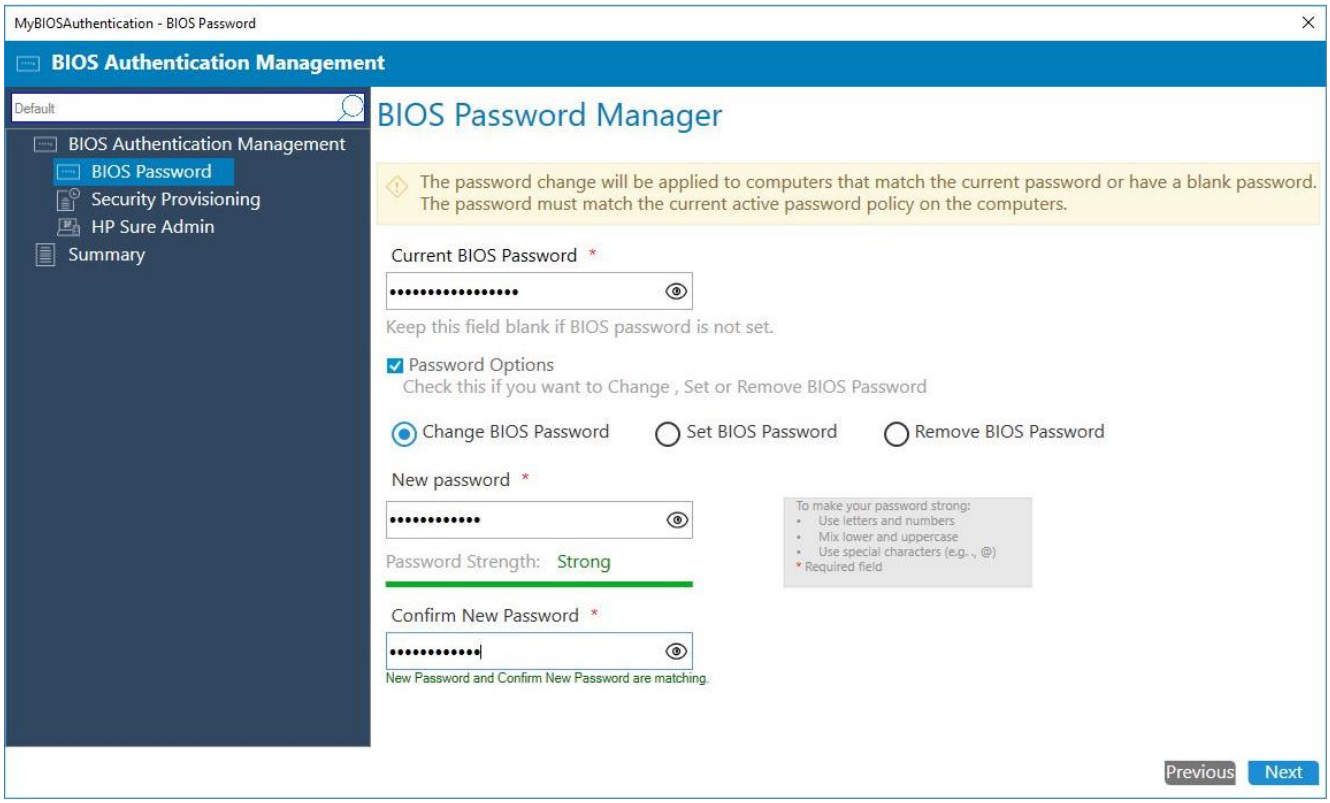


2. Click Next

6.6.2 Change BIOS Password

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 will apply the new password to all devices.

7. Provide the current password.
8. Mark the checkbox Password Options.
9. Select Change BIOS Password
10. Provide new password string in both New Password and Confirm New Password fields



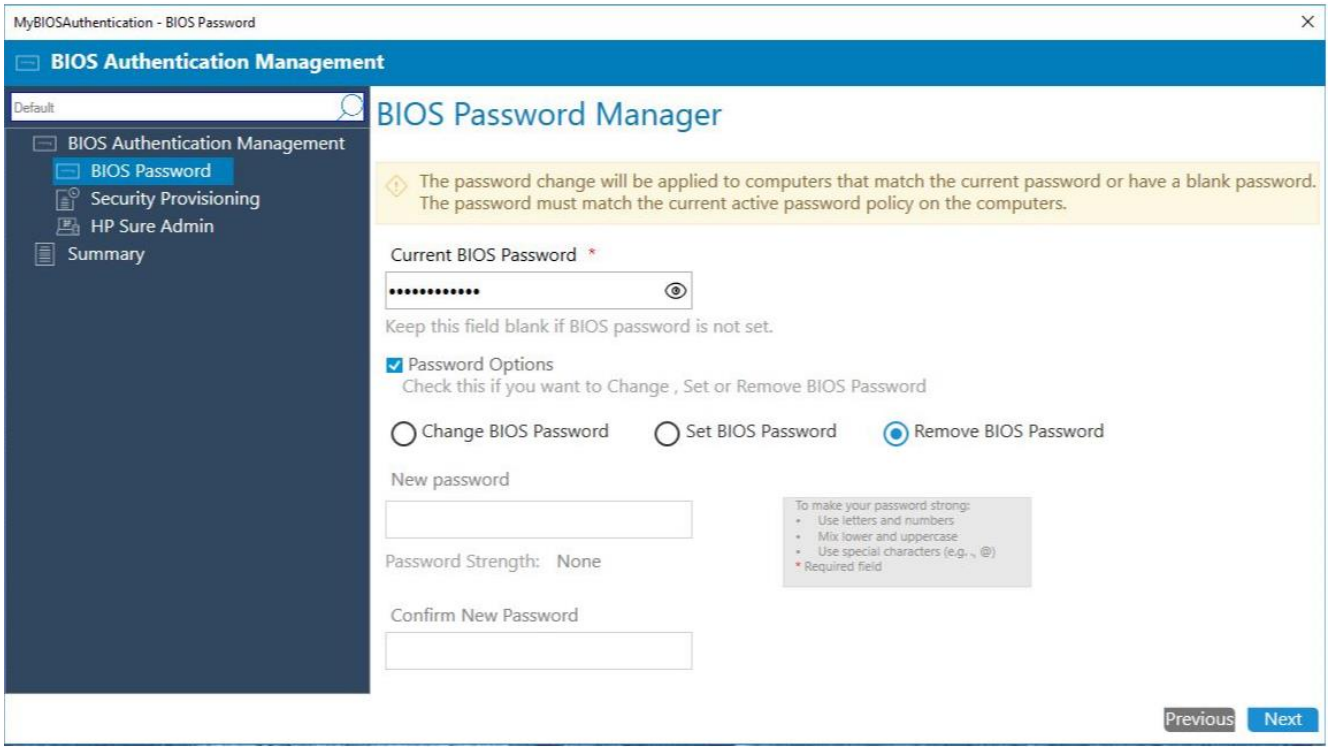
11. Click Next

6.6.3 Remove the BIOS Password

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. Provide the current password.
2. Select Remove BIOS Password


MyBIOSAuthentication - BIOS Password
BIOS Authentication Management
Default
BIOS Authentication Management
BIOS Password
Security Provisioning
HP Sure Admin
Summary
BIOS Password Manager
The password change will be applied to computers that match the current password or have a blank password.
The password must match the current active password policy on the computers.
Current BIOS Password *
Keep this field blank if BIOS password is not set.
Password Options
Check this if you want to Change , Set or Remove BIOS Password
Change BIOS Password
Set BIOS Password
Remove BIOS Password
New password
Password Strength: None
To make your password strong:
Use letters and numbers
Mix lower and uppercase
Use special characters (e.g., @)
* Required field
Confirm New Password
Previous
Next

3. Click Next

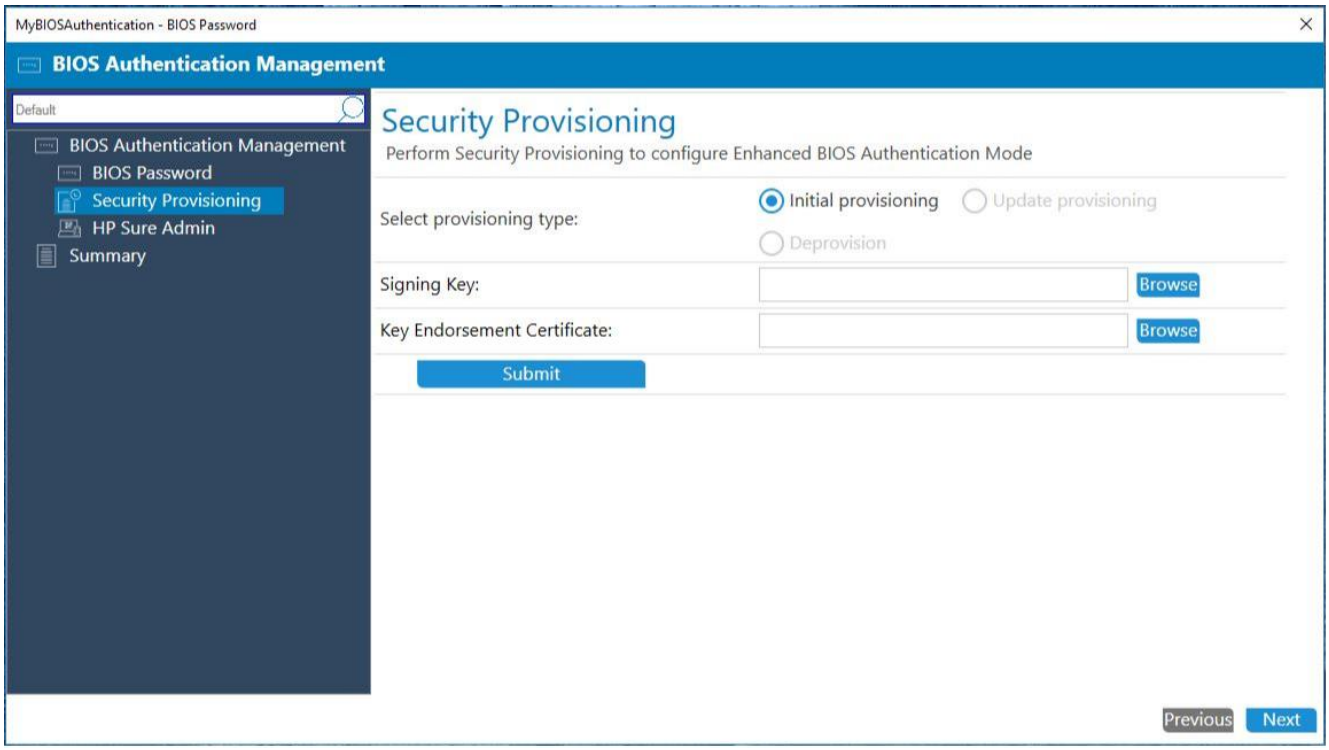
6.7 Security Provisioning

In the steps below two separate key pairs are set up:

- 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 will 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.

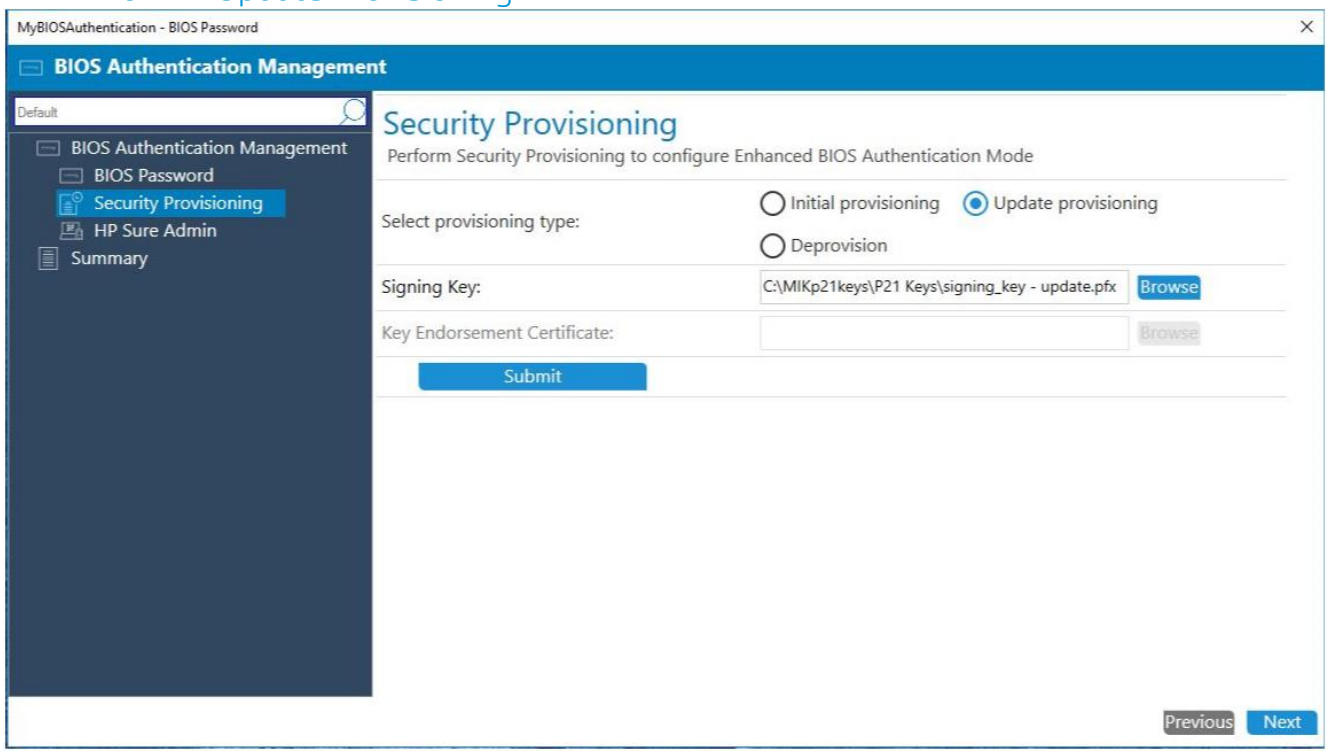
6.7.1 Initial Provisioning or Update Provisioning



The IT Administrator needs to provide both a Signing Key and a Key Endorsement Certificate for initial provisioning. Click on the Browse button next to the text field to select the key/certificate saved on local disks.

Once the key or certificate has been selected, click Submit and then hit Next. Note - The key format supported is Personal Information Exchange (PFX). Please refer to Section 26 for details on key creation.

6.7.2 Update Provisioning



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

Navigate to Security Provisioning and select option Update Provisioning.

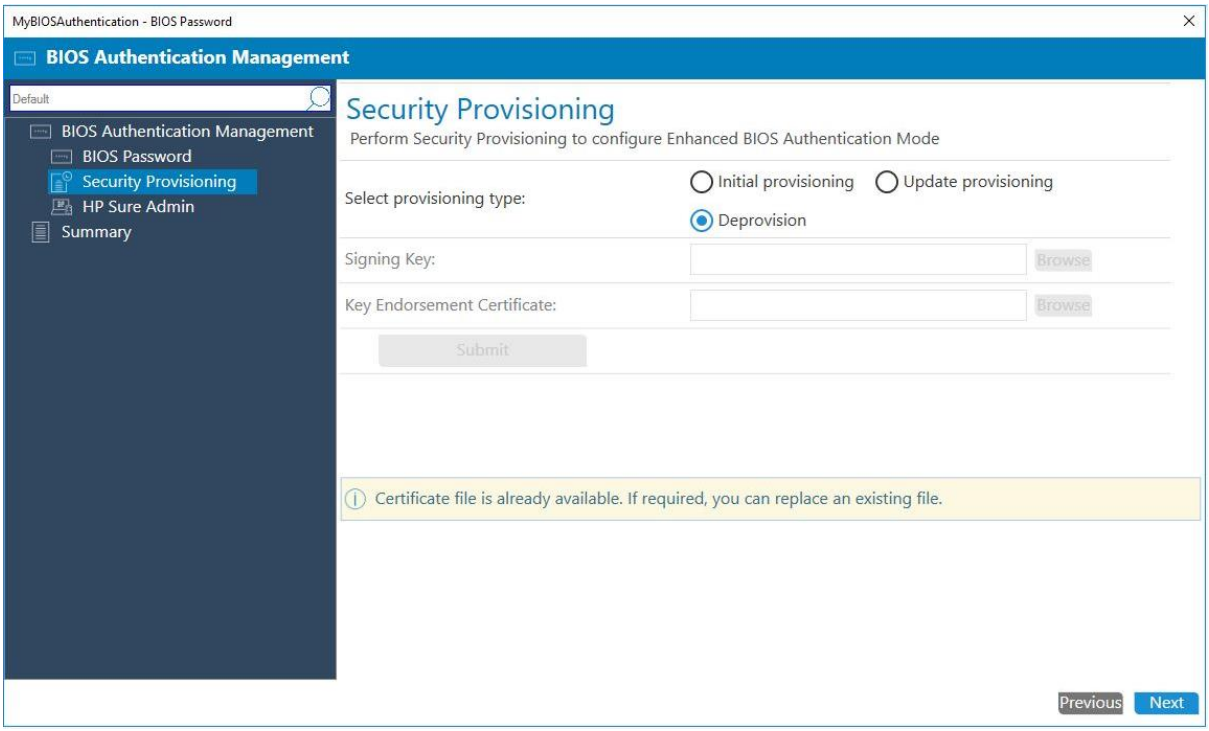
The IT Administrator needs to provide the signing key to update provisioning. Click on the Browse button next to the text field to select the key saved on local disks.

Once selected, click Submit and then hit Next

6.7.3 Deprovision

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

Navigate to Security Provisioning and select the option to Deprovision, then click Next.



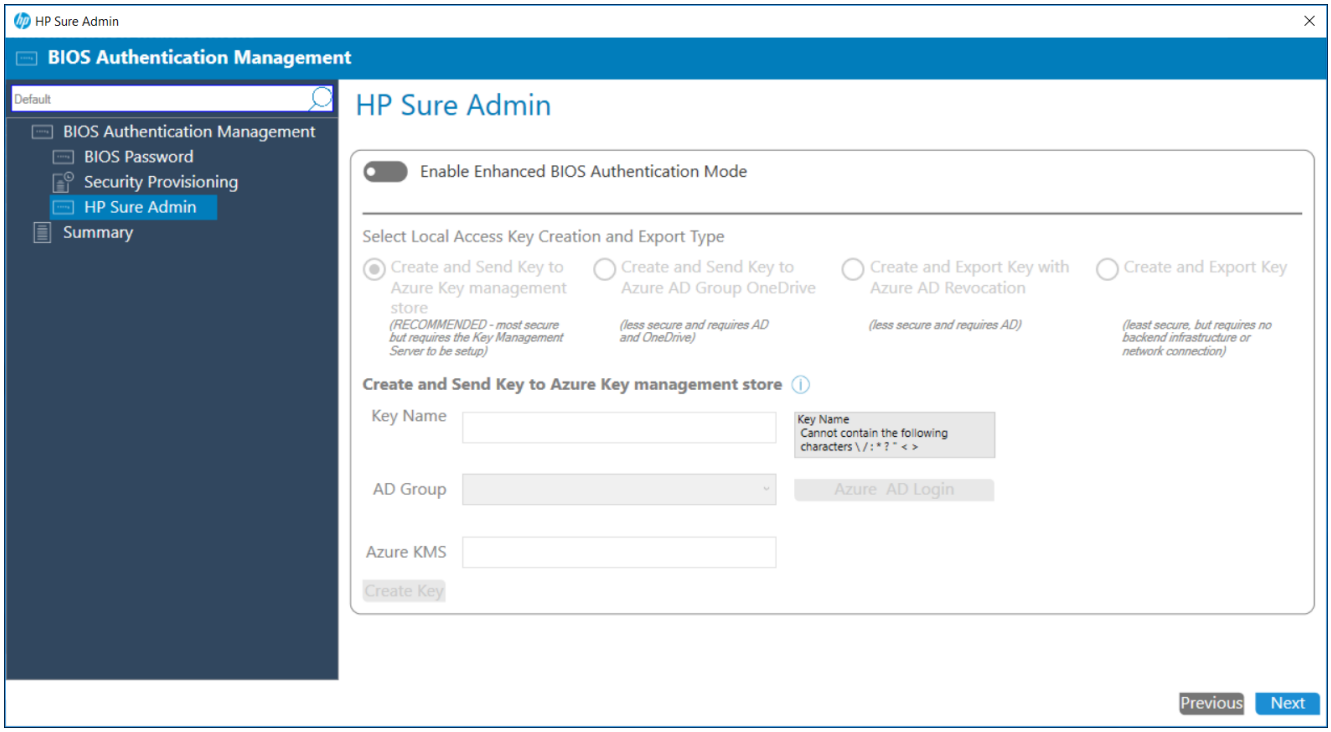
Deprovisioning, will result in HP Sure Admin being disabled. The system will now switch to legacy mode that will need BIOS Admin password.

Note other dependent features HP Sure Run and HP Sure Recover will also be automatically disabled as part of the policy push.

6.8 HP Sure Admin

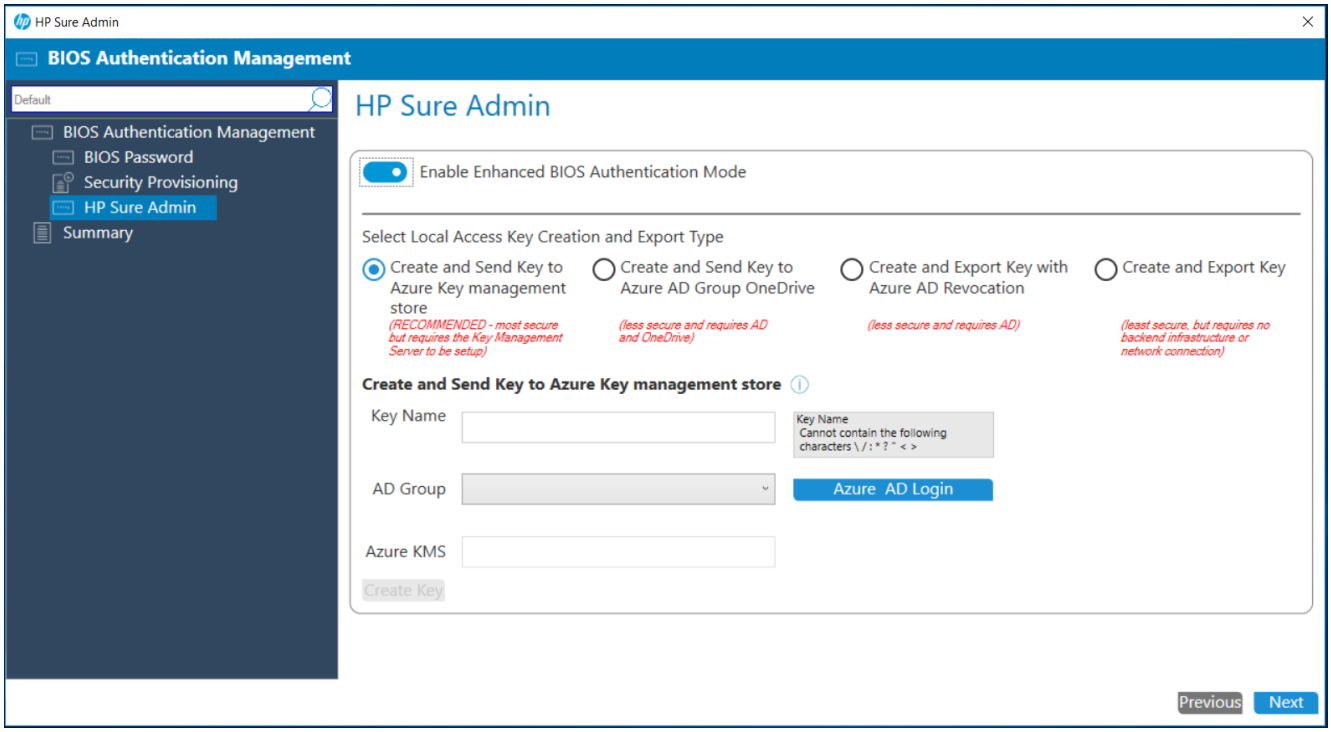
HP Sure Admin manages BIOS settings using cryptographically verified commands that use public/private key pairs.

- By Default, HP Sure Admin is disabled.
- Click on Enable Enhanced BIOS Authentication Mode to enable the HP Sure Admin feature.
- Note - As a pre-condition user, first need to perform the step of provisioning using the Security Provisioning UI.



6.8.1 Activate Enhanced BIOS Authentication Mode

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



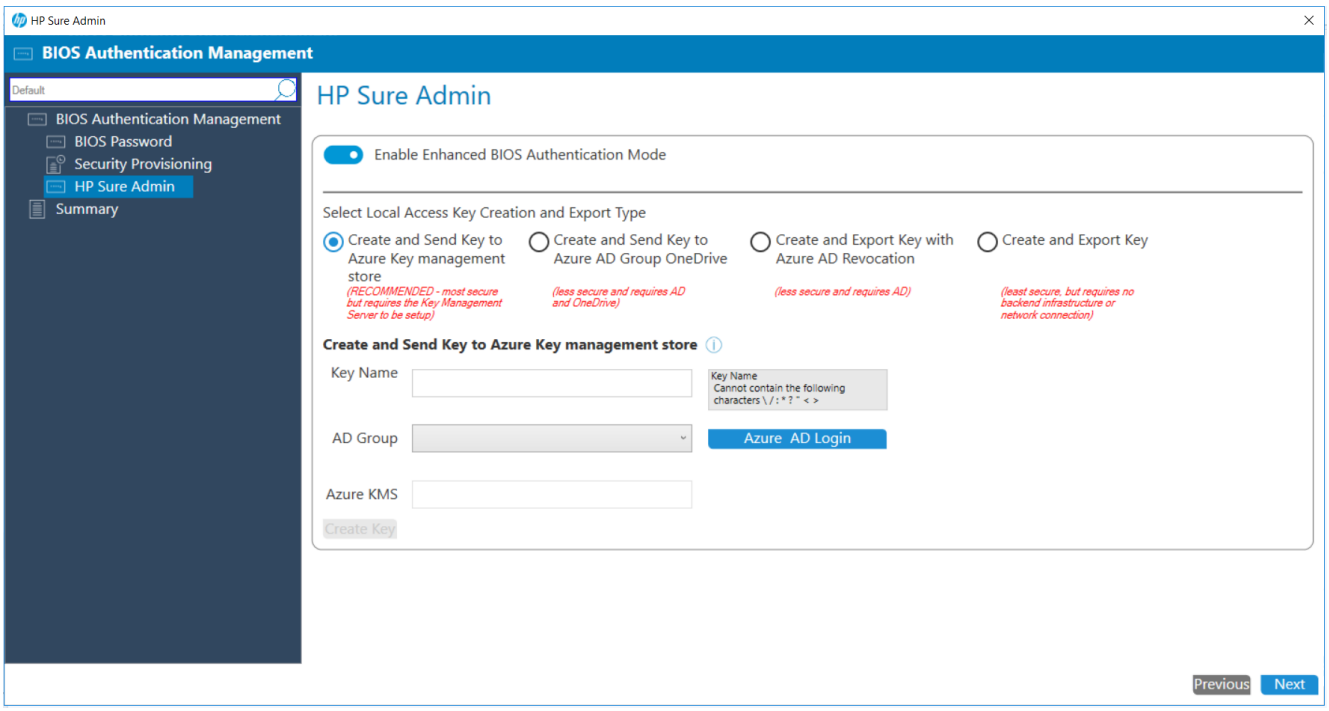
6.8.2 Select Creation and Export Type

HP MIK provides 4 options to create and manage a public/private key pair that will authorize a local administrator user to access the system.

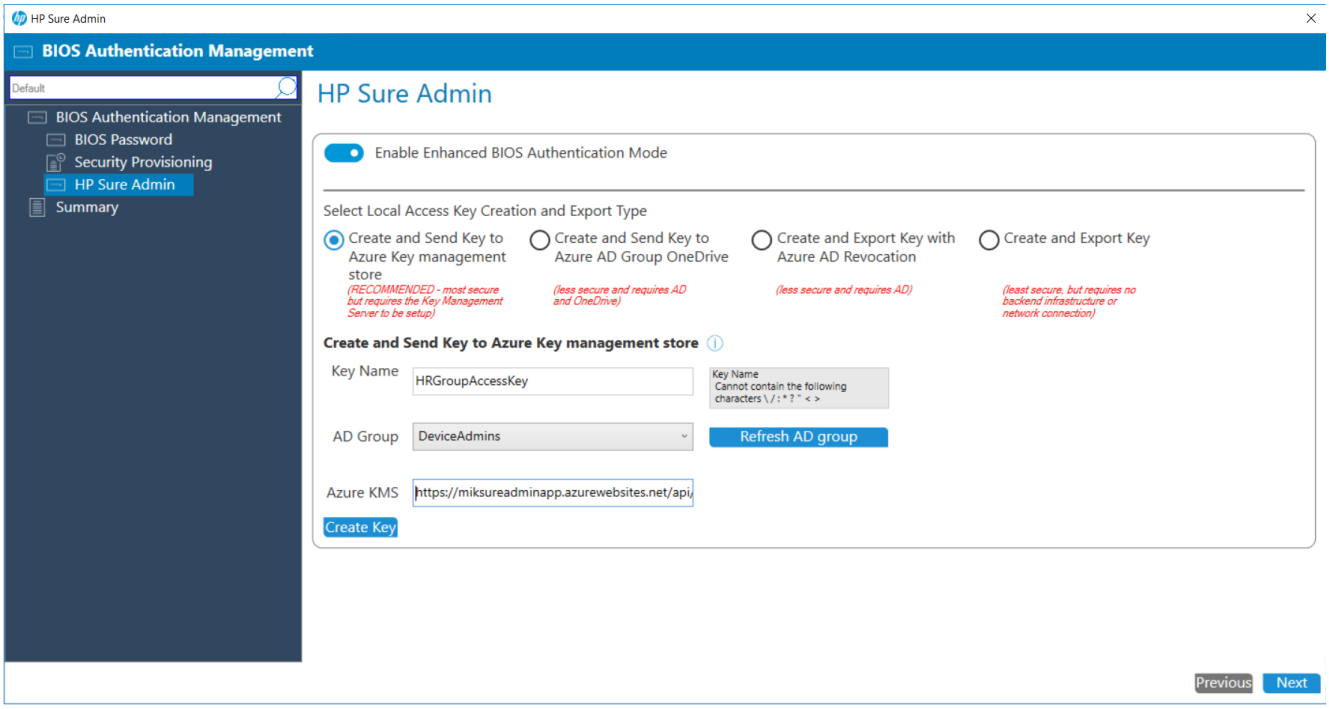
- ✓ Create and Send Key to Azure Key to management store
- ✓ Create and Send Key to Azure AD Group OneDrive
- ✓ Create and Export Key with Azure AD Revocation
- ✓ Create and Export Key

Note the selection of option is dependent on infrastructure available within enterprise.

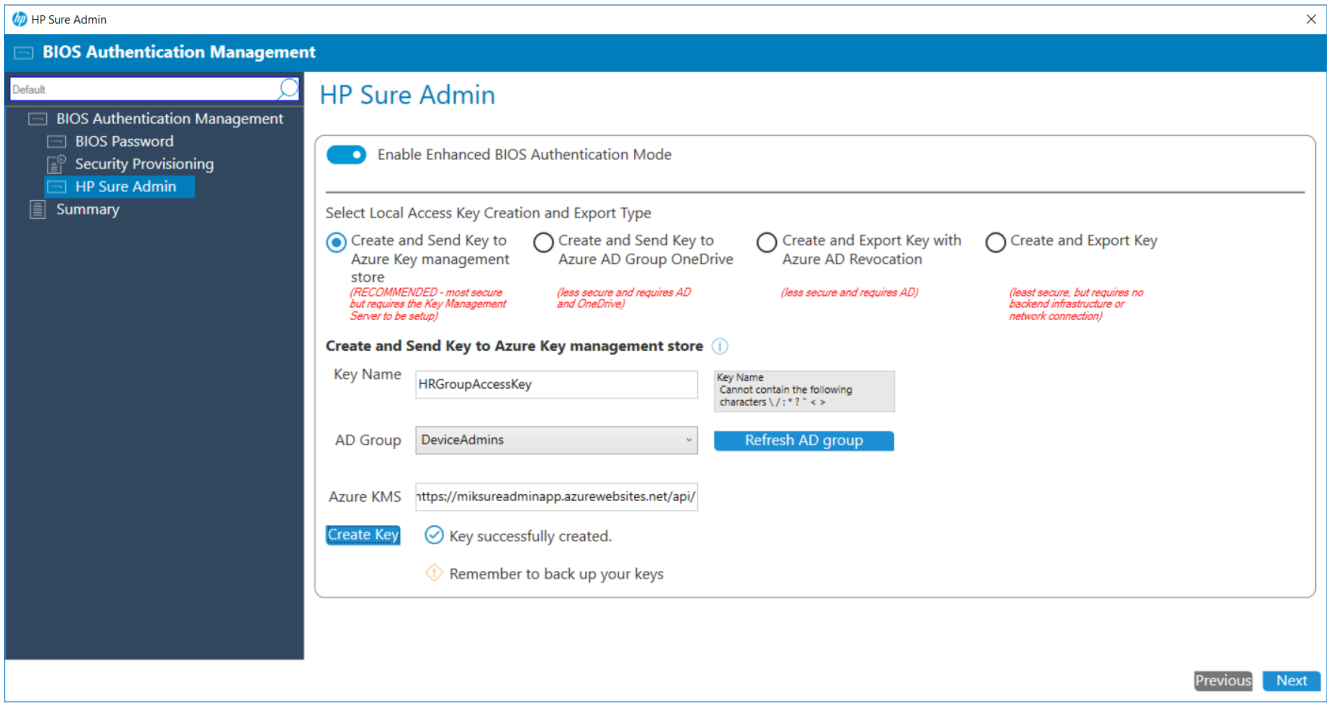
6.8.2.1.1 Create and Send Key to Azure Key Management store – HP Recommended



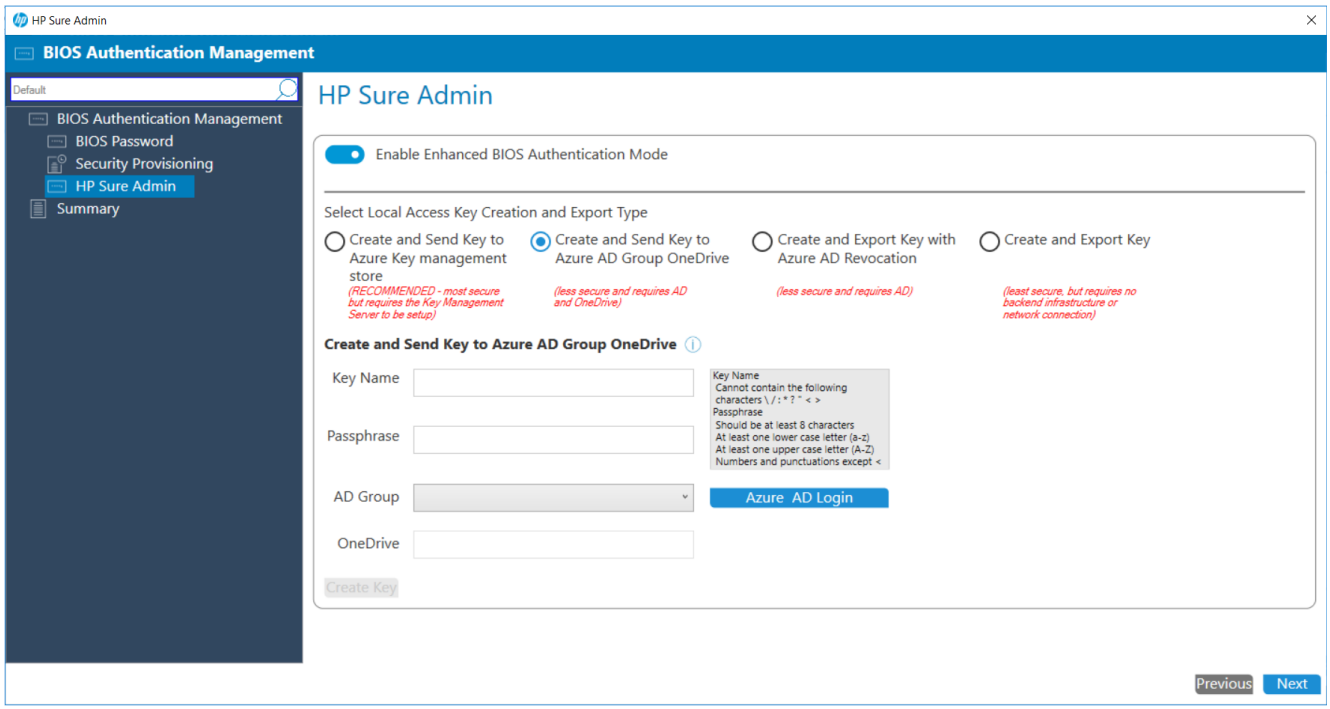
1. Enter Key Name.
2. Click on Azure AD login to connect to your enterprise Azure AD. You will be prompted to provide the login credentials.
3. On Successful login the Azure AD Group Name will be listed. Please select the appropriate group.
4. Enter the URL path for your enterprise Key Management Sore - KMS.



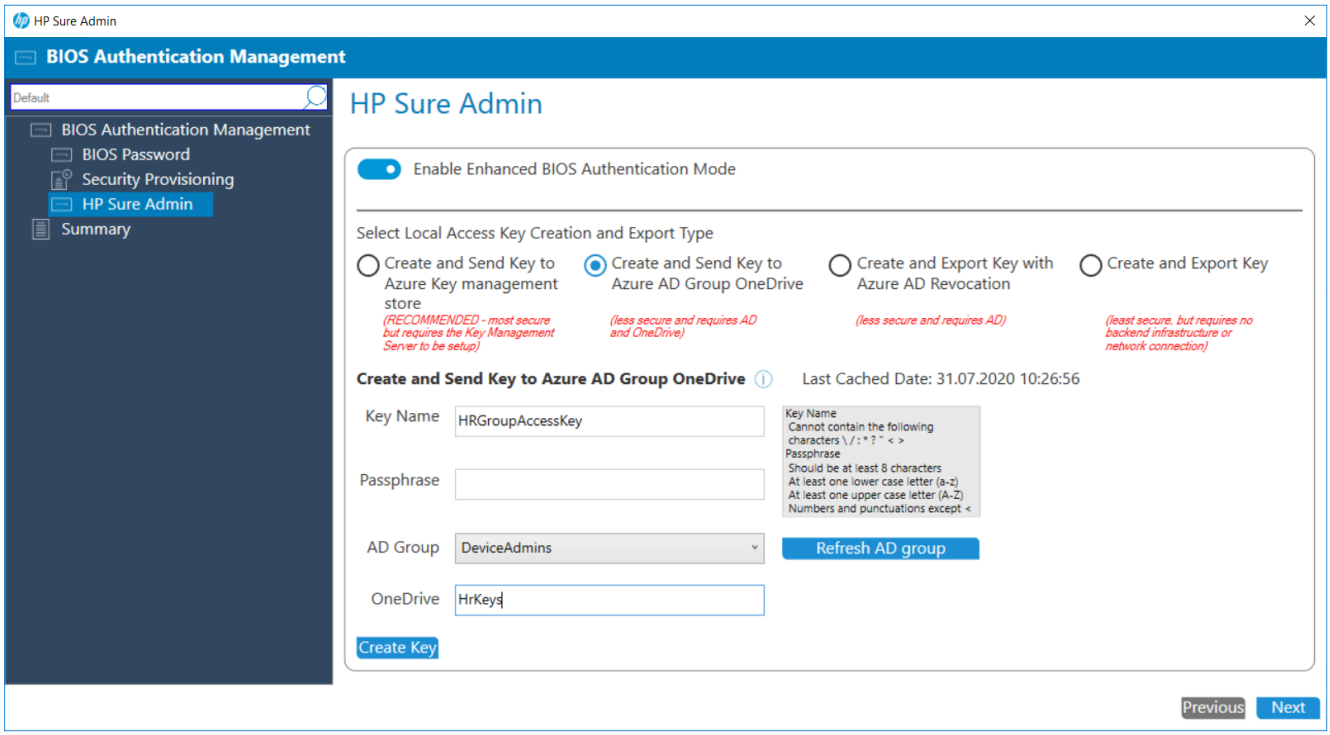
5. Click on Create Key.



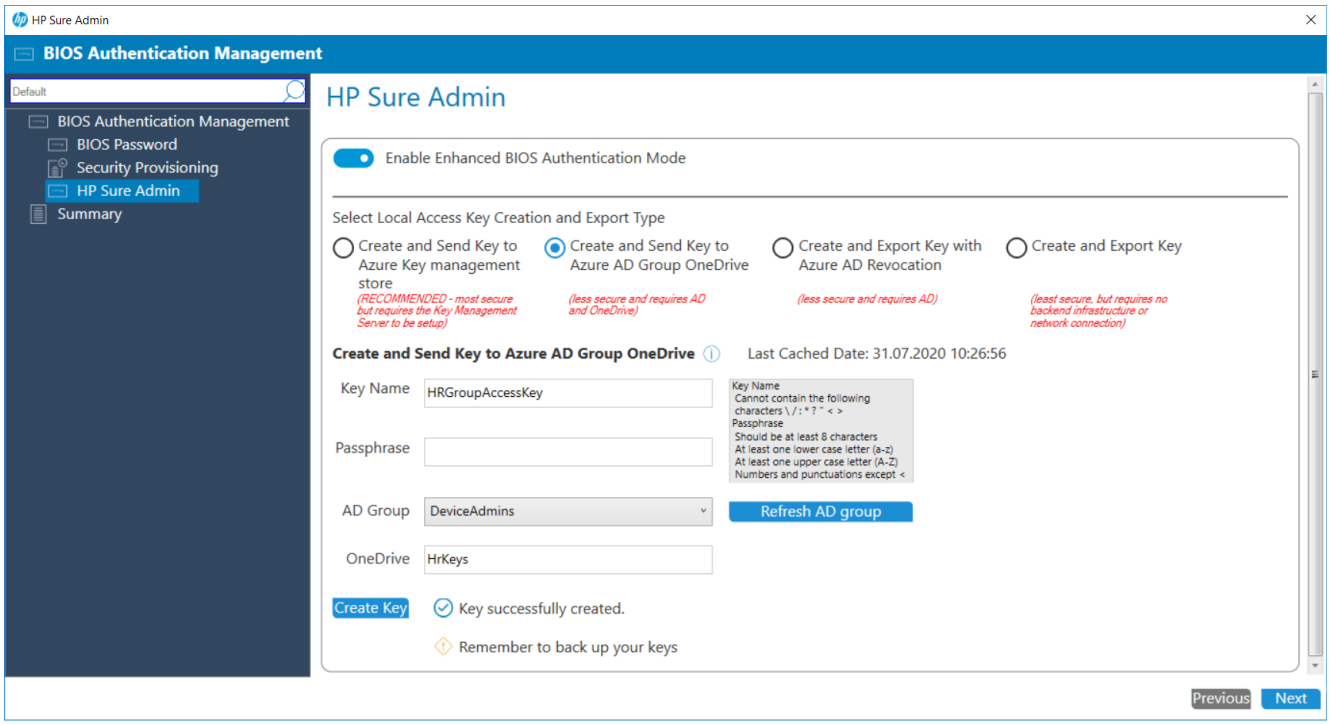
6.8.2.1.2 Create Local Access key to Azure Ad Group OneDrive.



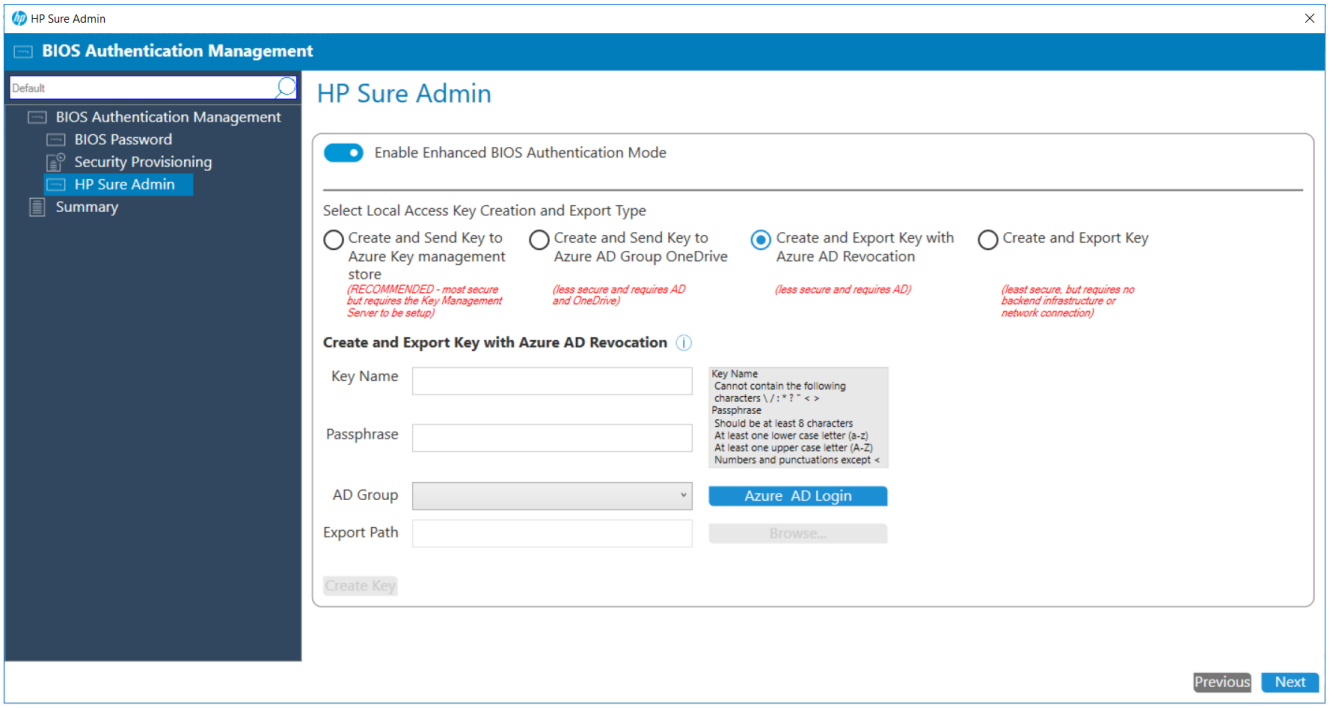
1. Enter Key Name.
2. Enter a Passphrase, note - Passphrase is optional. Please refer to section #27 for details.
3. Click on Azure AD login to connect to your enterprise Azure AD. You will be prompted to provide the login credentials.
4. On Successful login the Azure AD Group Name will be listed. Please select the appropriate group.



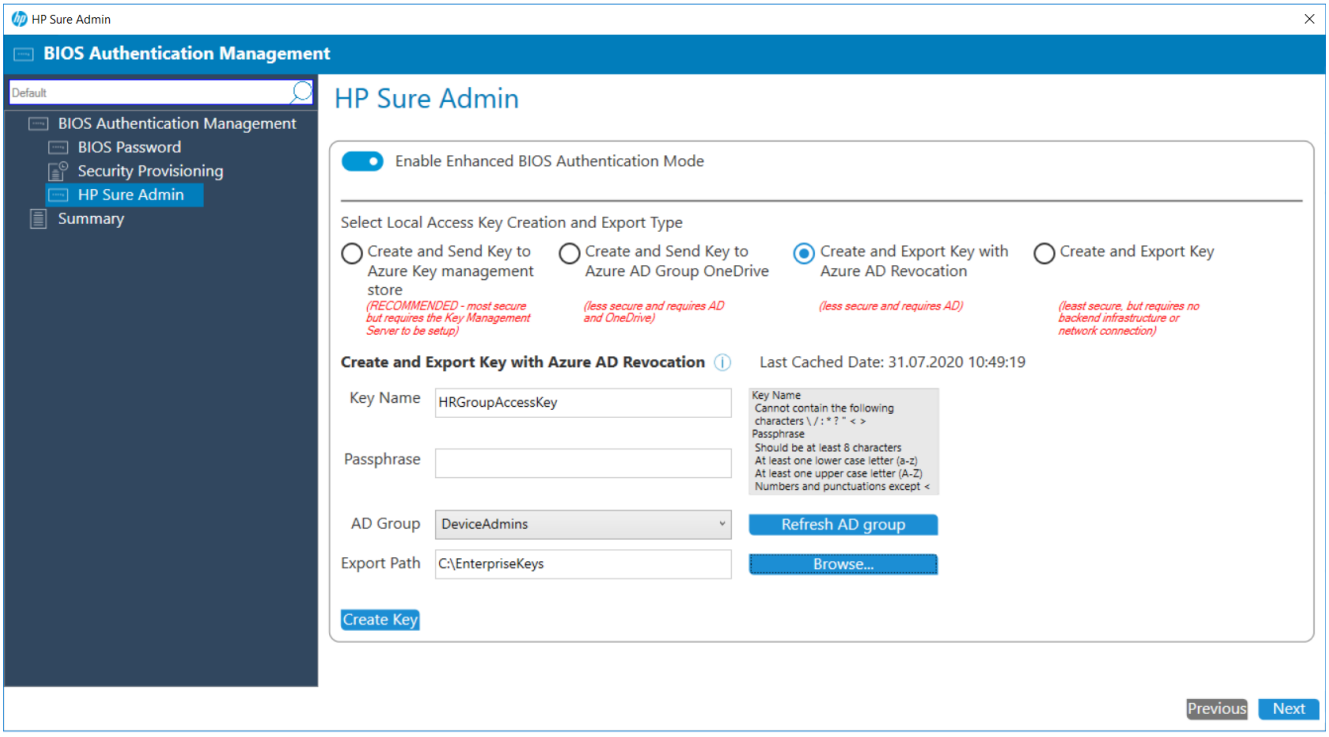
5. Enter the folder name on your enterprise one drive to store the key.
6. Click on Create Key.



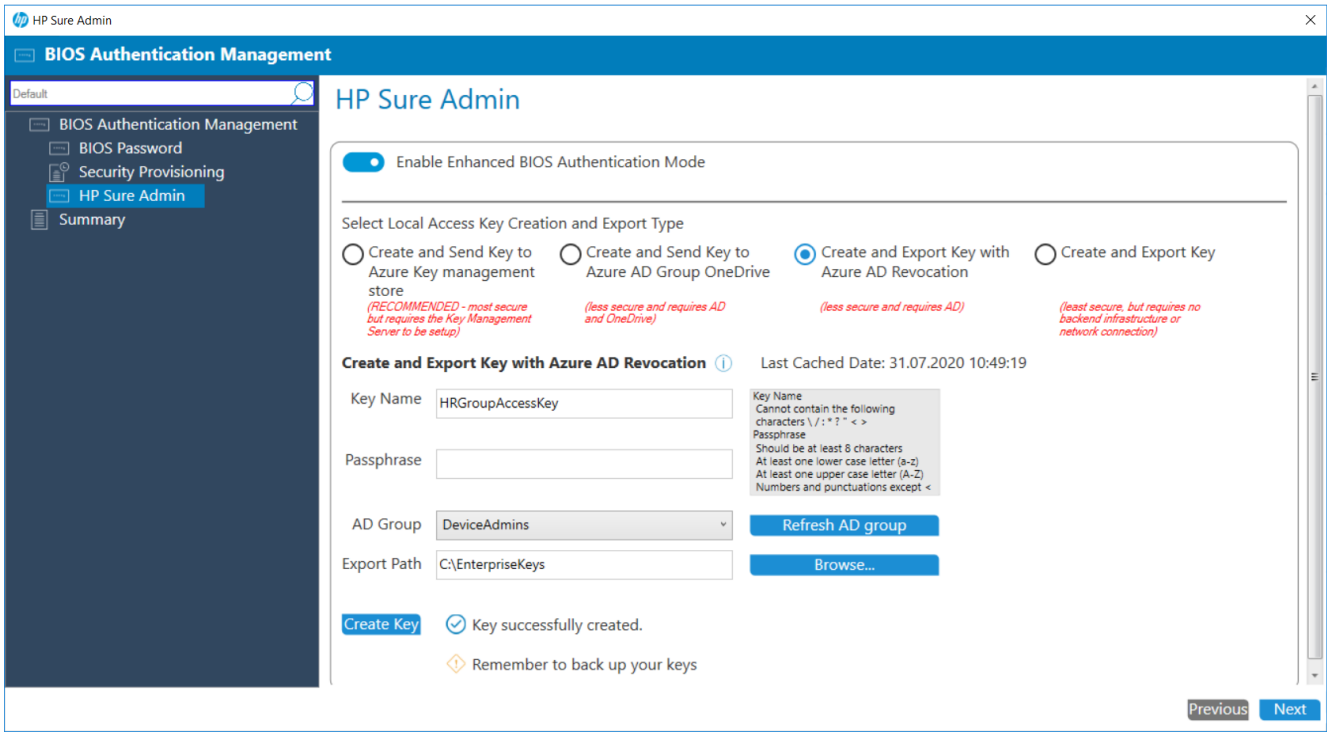
6.8.2.1.3 Create and Export key with Azure AD Revocation



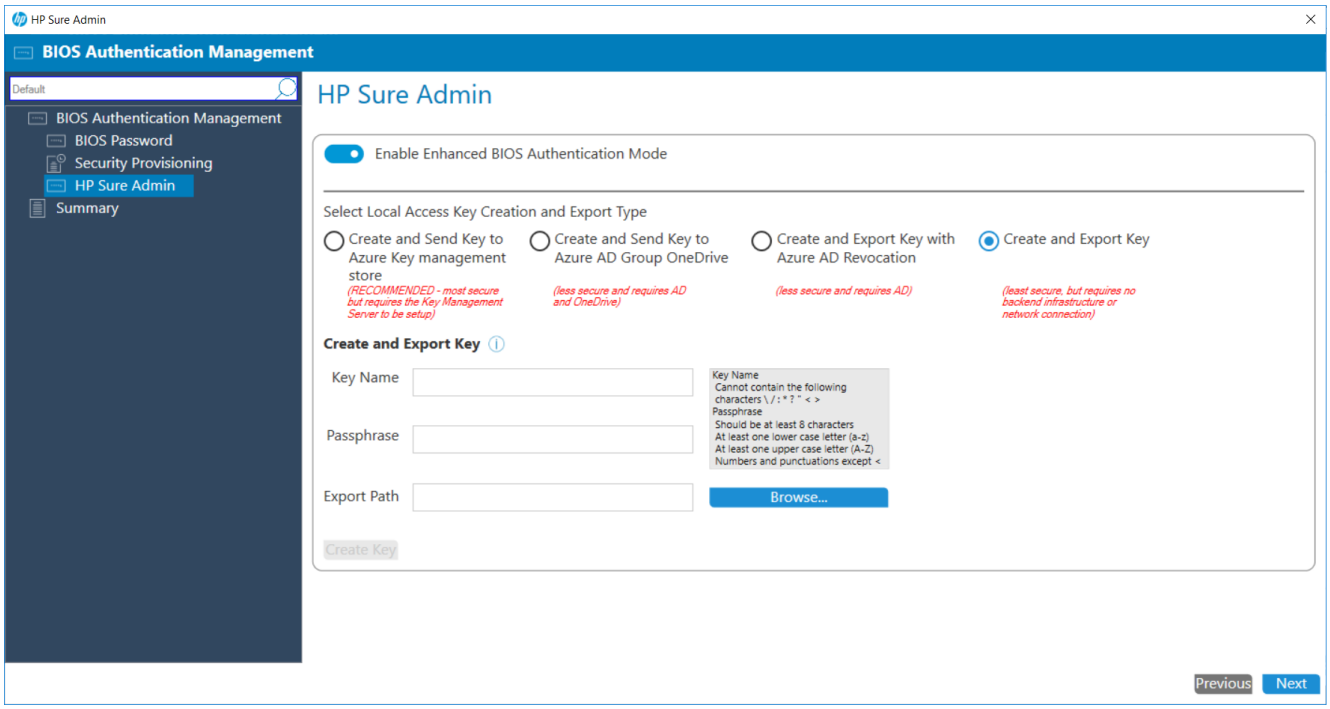
1. Enter Key Name.
2. Enter a Passphrase, note - Passphrase is optional. Please refer to section #27 for details.
3. Click on Azure AD login to connect to your enterprise Azure AD. You will be prompted to provide the login credentials.
4. On Successful login the Azure AD Group Names will be listed. Please select the appropriate group.



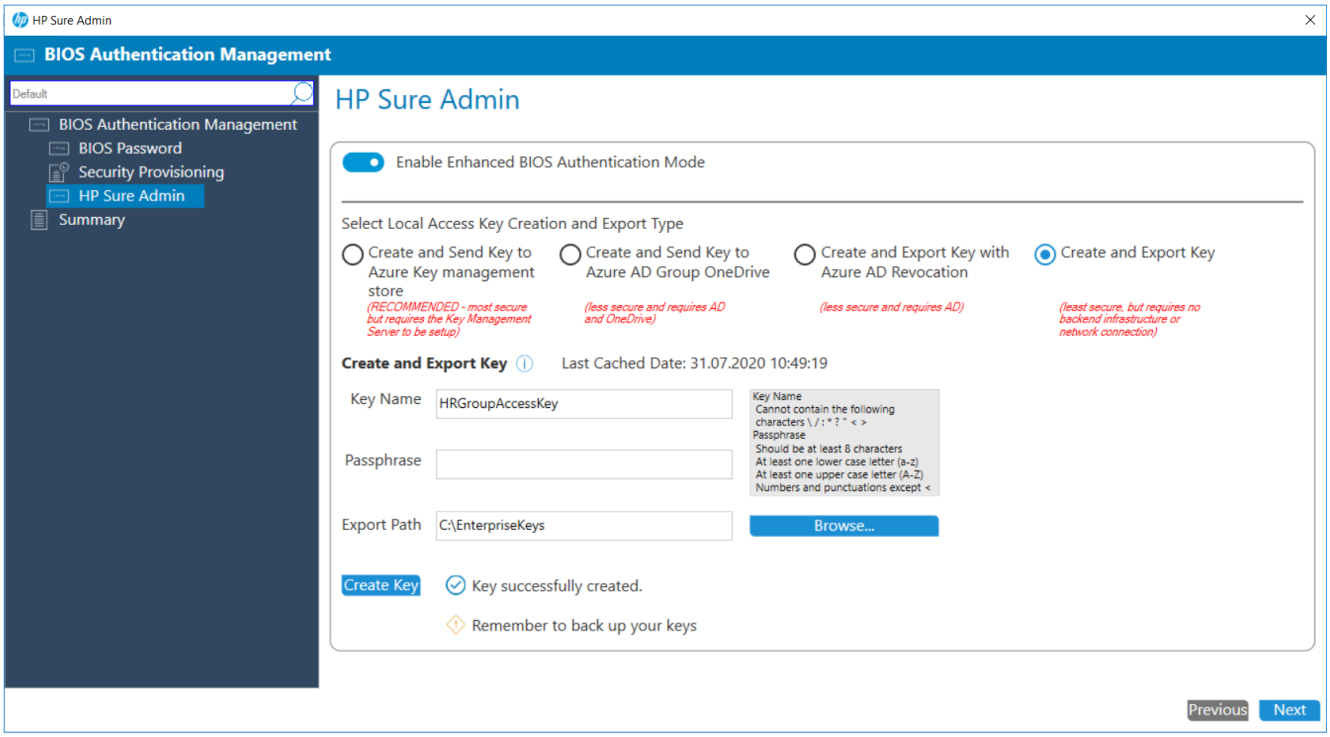
5. Click on Browse to select the path to store the key.
6. Click on Create Key.



6.8.2.1.4 Create and Export key



1. Enter Key Name.
2. Enter a Passphrase, note - Passphrase is optional. Please refer to section #27 for details.
3. Click on Browse to select the path to store the key.
4. Click on Create Key.



6.8.3 Note

For Sure Admin to be enabled, a security provisioning policy needs to have been applied first. In an SCCM environment it is difficult to control which configuration items will get applied first or their sequence, so multiple iterations may be needed for Sure Admin to be enabled on managed device.

For details refer Appendix section for Sure Admin.

7 HP BIOS Configuration

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

7.1 Supported client platforms

- HP commercial computers (2015 or later)

7.2 Supported client operating systems

- Windows 10
- Windows 8.1
- Windows 7

7.3 Prerequisites

- Microsoft .NET Framework 4.0 or higher.
- HP Manageability Integration Kit

7.4 User interface

There are three columns in the HP BIOS Configuration window.

The Select column is used to specify whether a setting is enforced by a polity. If a setting is selected, it is set to the specified value. If a setting is cleared, it is not modified.

The Settings column displays the setting name.

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.

NOTE:
In Category View, a category must be expanded to display all three columns.

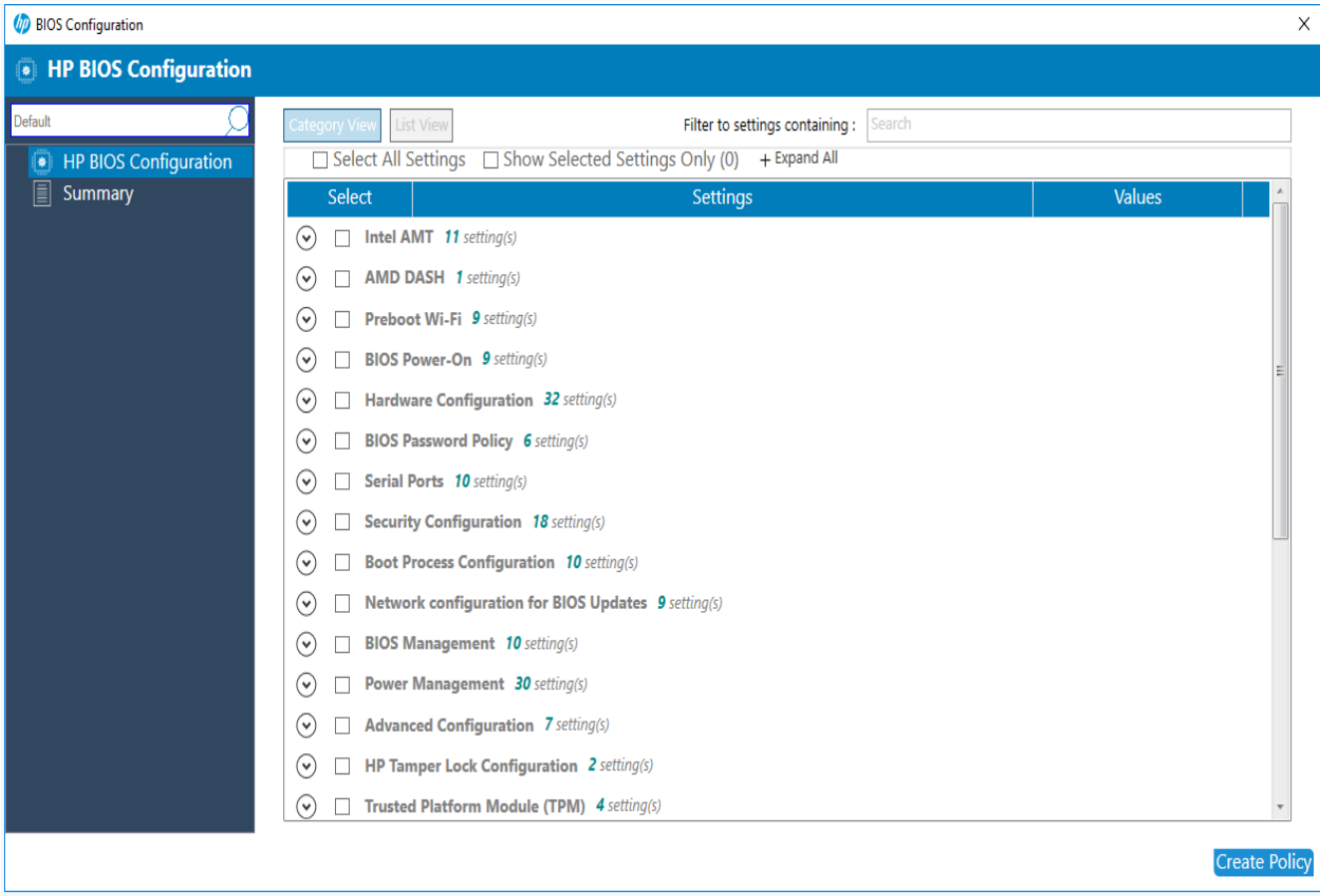
The icons next to some settings indicate the following behaviors:

- 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.

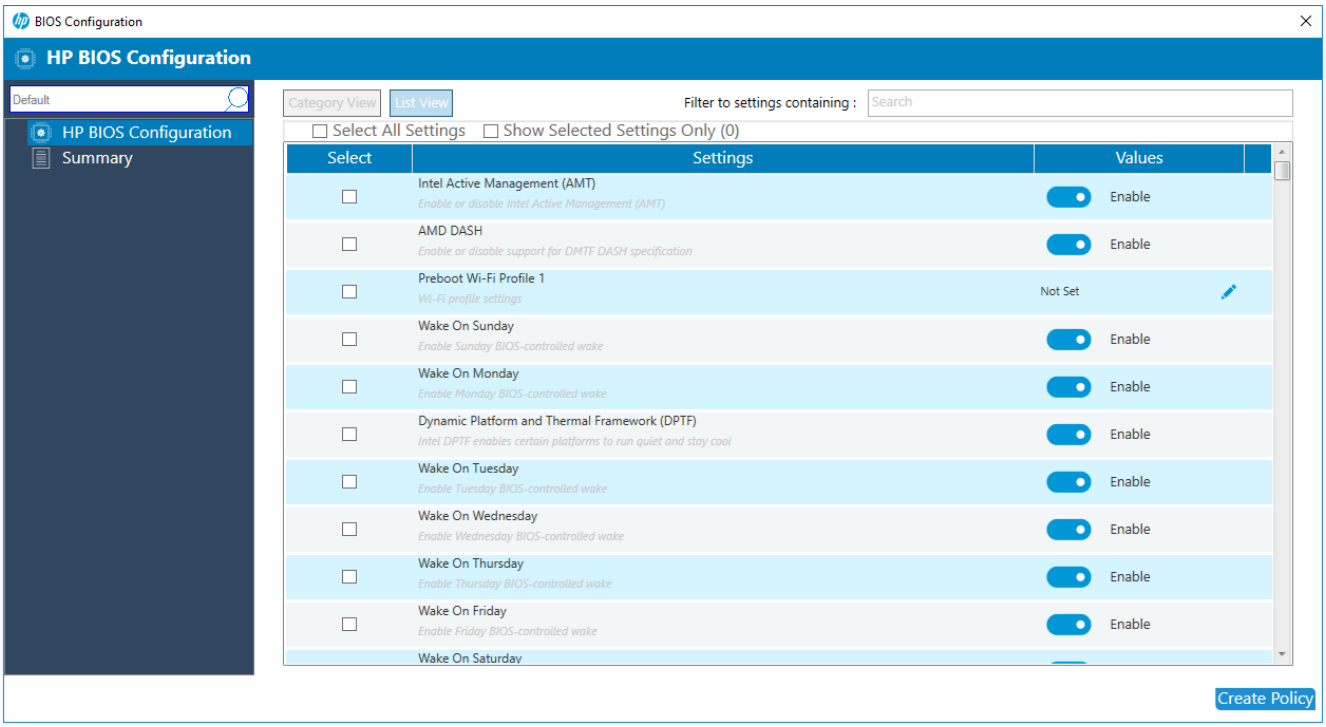
7.5 Category View button

Select this button to display BIOS Settings as grouped categories


BIOS Configuration
HP BIOS Configuration
Default
HP BIOS Configuration
Summary
Category View
List View
Filter to settings containing :
Search
Select All Settings
Show Selected Settings Only (0)
Expand All
Select
Settings
Values
Intel AMT 11 setting(s)
AMD DASH 1 setting(s)
Preboot Wi-Fi 9 setting(s)
BIOS Power-On 9 setting(s)
Hardware Configuration 32 setting(s)
BIOS Password Policy 6 setting(s)
Serial Ports 10 setting(s)
Security Configuration 18 setting(s)
Boot Process Configuration 10 setting(s)
Network configuration for BIOS Updates 9 setting(s)
BIOS Management 10 setting(s)
Power Management 30 setting(s)
Advanced Configuration 7 setting(s)
HP Tamper Lock Configuration 2 setting(s)
Trusted Platform Module (TPM) 4 setting(s)
Create Policy

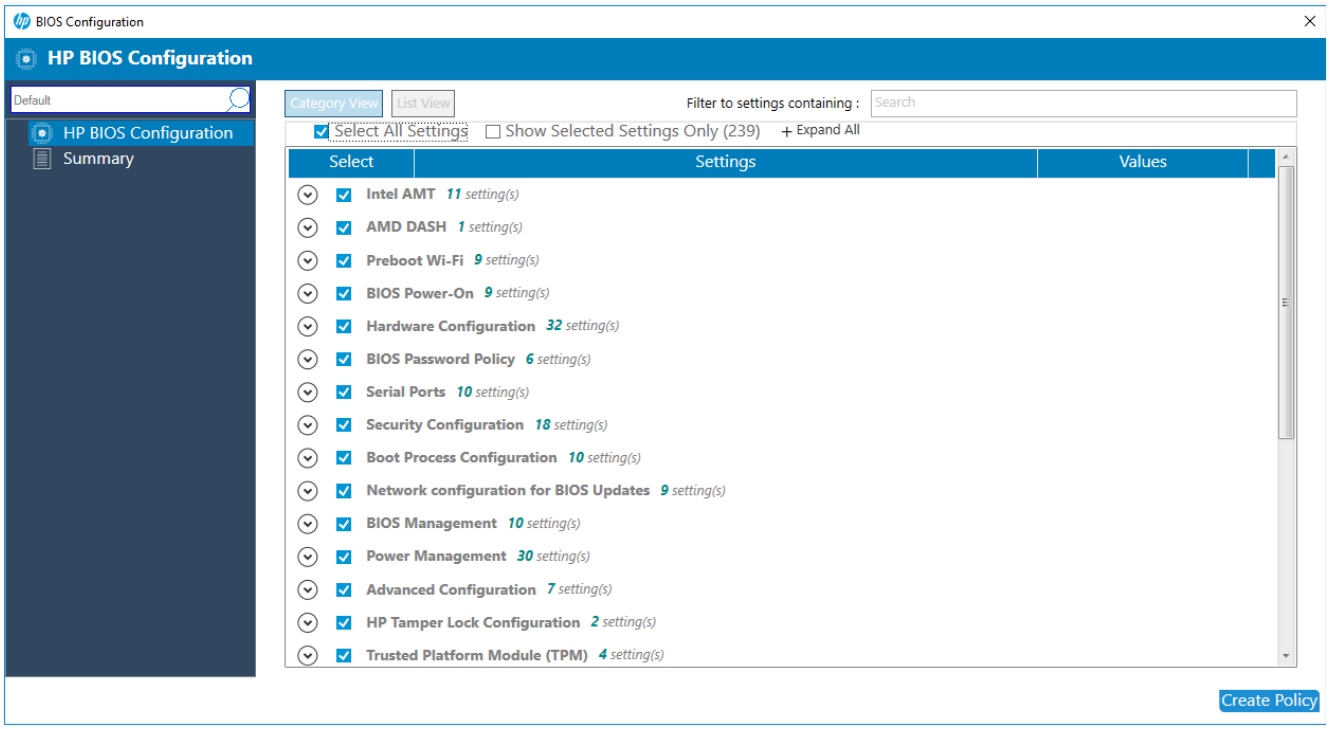
7.6 List View button

Select this button to display the BIOS settings as a list.



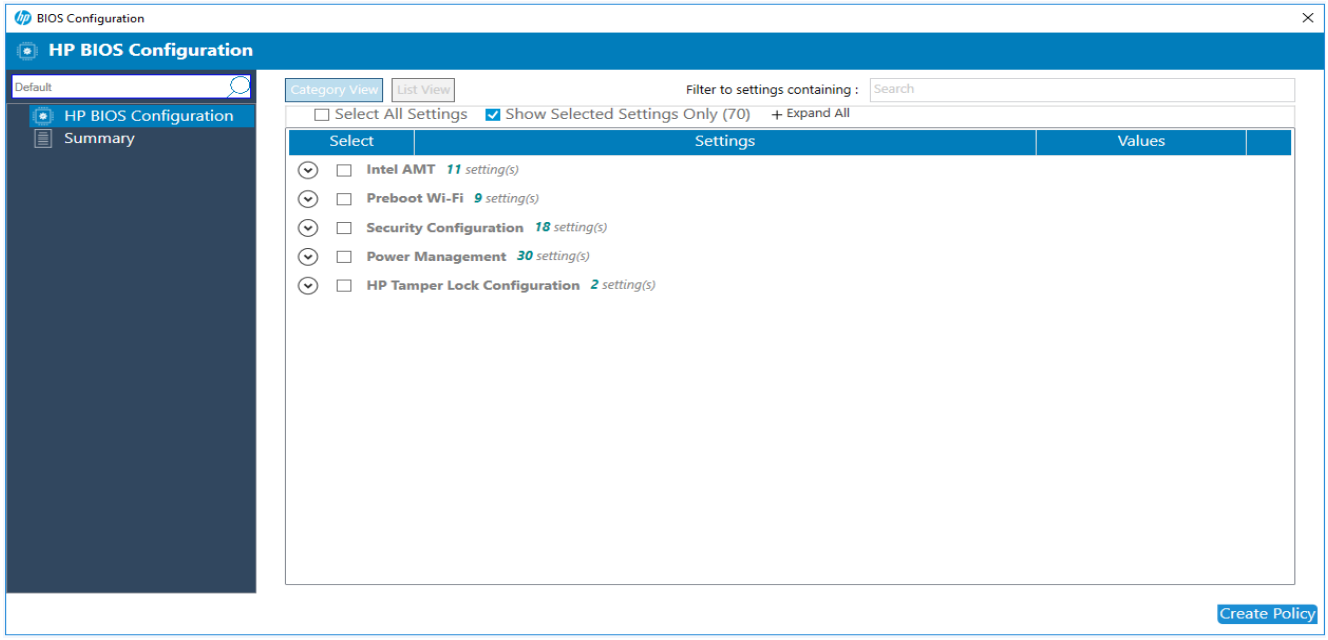
7.7 Select All Settings

Select this checkbox option to select all settings while in Category view or in List view



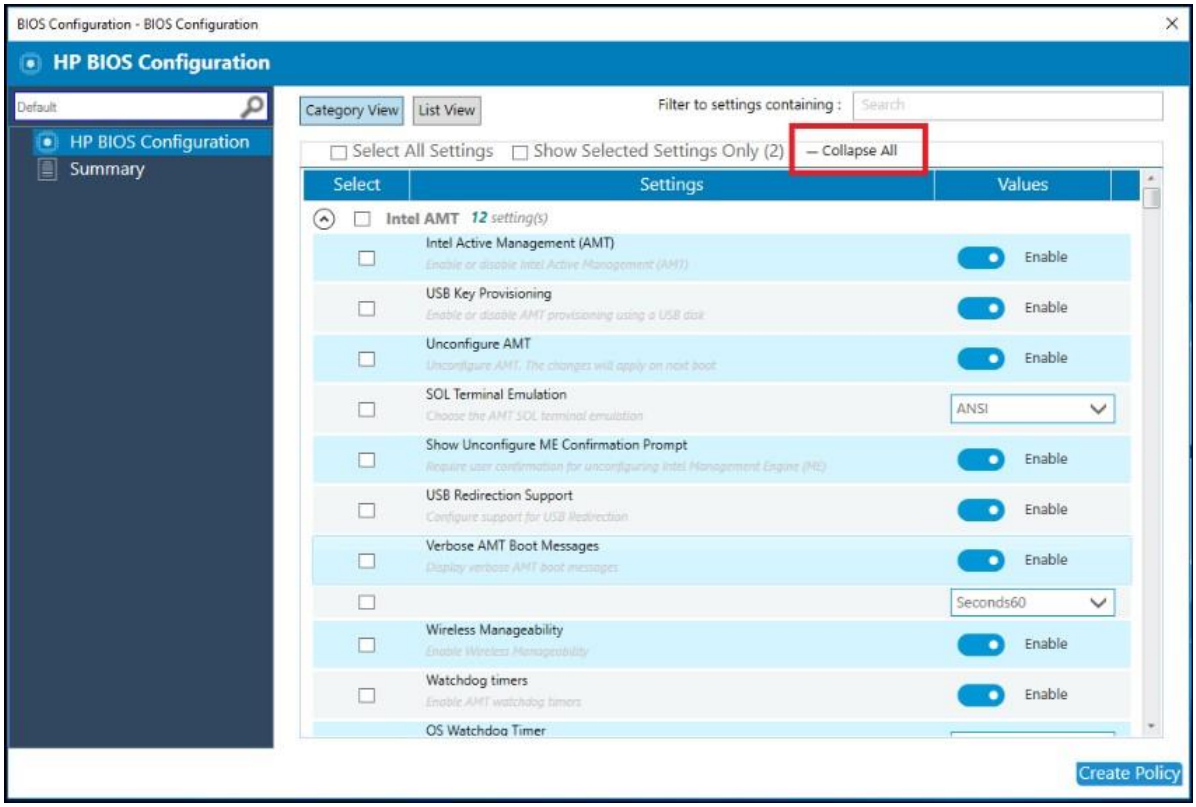
7.8 Show Selected Settings Only

Select this checkbox option to show only settings that have been selected.



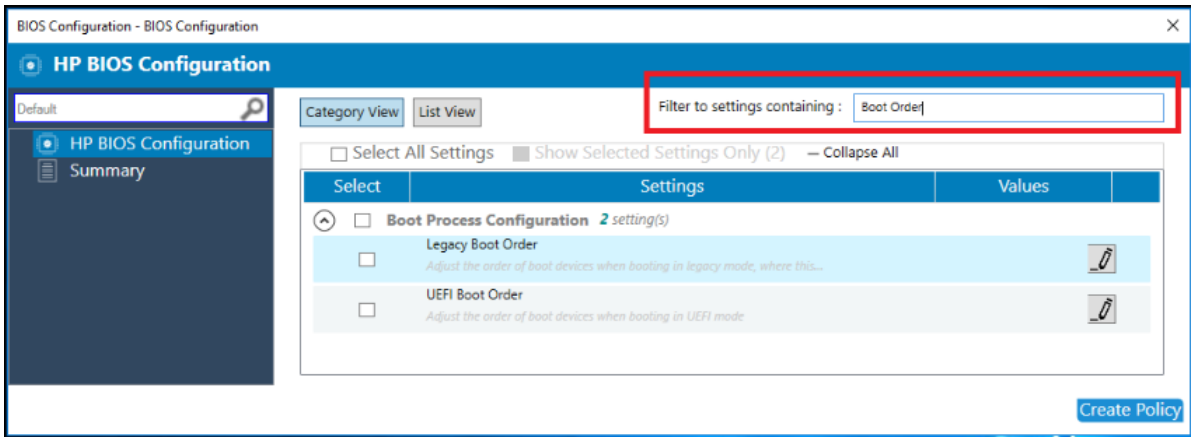
7.9 Expand All/Collapse All button

Select this button to expand or collapse the details of each setting.



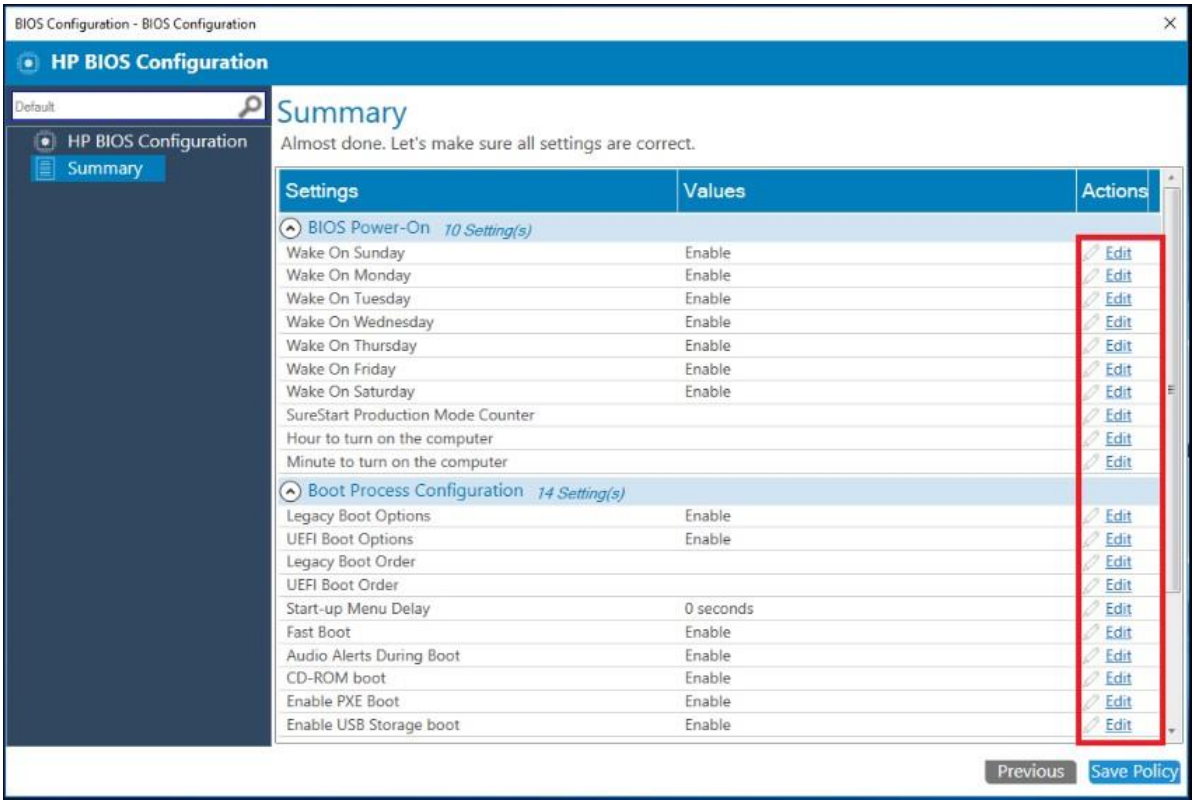
7.10 Filter to settings containing

Enter a term to quickly locate a setting in the list of settings, based on a partial string match.



7.11 Creating a policy

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



9. After the policy has been saved successfully, select Deploy, and then select the target collections to which to apply the policy.

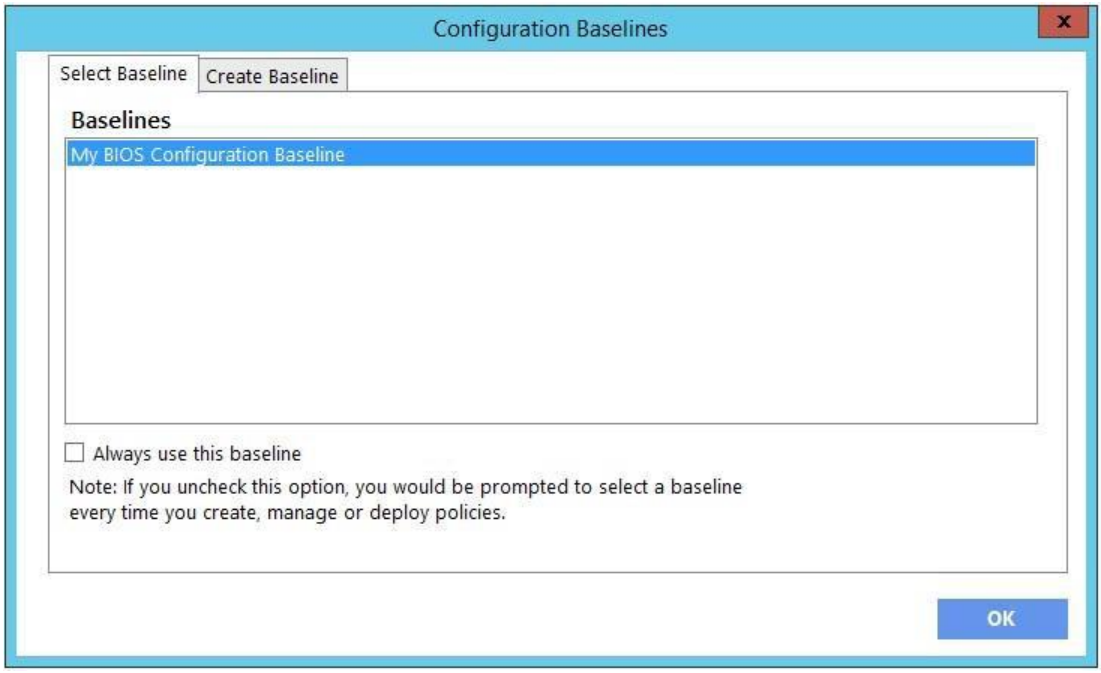
10. Restart the client computers to ensure that the BIOS settings take effect.

7.12 Editing a policy

11. In Configuration Manager, select Assets and Compliances and then select Overview.

12. Expand HP Manageability Integration Kit, right-click BIOS Configuration, and then select Edit Policy.

13. Select an existing baseline policy to edit and click OK to continue the wizard.



14. Follow steps 4 through 8 of Creating a policy.

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

8 HP Client Security with Intel Authenticate Support

HP Client Security with Intel® Authenticate™ Support enables the management of HP Client Security software through Configuration Manager. HP Client Security uses features built into the BIOS, hardware, and software layers to help protect against attacks, loss, or theft. It can also take advantage of Intel® Authenticate™ capabilities to further enhance security.

8.1 Supported client platforms

- HP commercial computers using KBL processor (2015 or later)
- Intel Authenticate requires commercial level ME firmware 11.8.50.3399.
- If three factor authentication is desired, computers must be vPro enabled.
- Modern Standby – At this time Intel Authenticate does not fully support Modern Standby. Please disable this feature in the OS if using Intel Authenticate.

8.2 Supported client operating systems

- Windows 10 (Intel® Authenticate™ only supports Windows 10)
- Windows 8.1
- Windows 7

8.3 Other client system prerequisites

- Microsoft .NET Framework 4.6.1 or higher
- HP Client Security Manager 9.3.10.2571 or higher
- The HP Device Access Manager 8.4.12.0 or higher
- Intel Authenticate Engine 3.0.0.78 (optional)

NOTE:
Intel® Authenticate™ Engine is required to make use of Intel® Authenticate™ enhanced security features and requires the following additional drivers:

— Intel Management Engine Driver 11.6.0.1019 or higher

— Intel Bluetooth® Driver 19.00.1626.3453 or higher

— Intel Graphics Driver 21.20.16.4481or higher - Intel Authenticate requires use of the Intel graphics card. If the PC has more than one graphic solution, Intel graphics must be used for Intel Authenticate PTD PIN authentication.

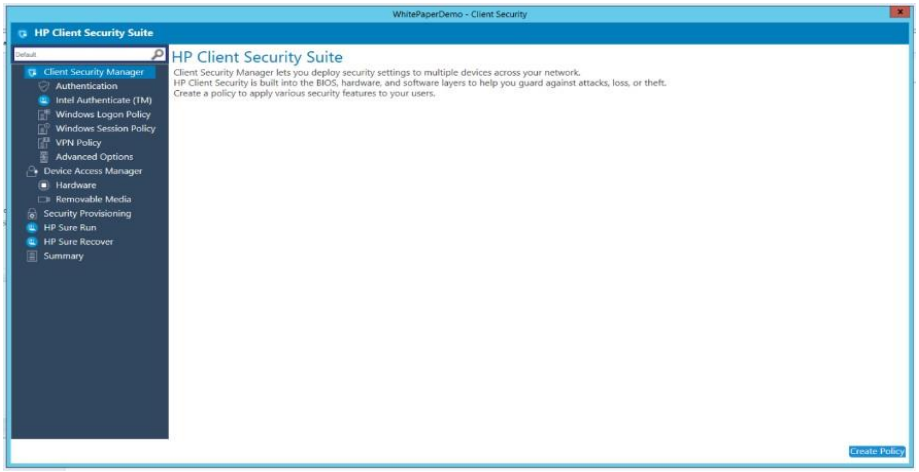
— Synaptics Touch Fingerprint Driver 5.5.6.1099 or higher (Swipe sensors are not supported.)

8.4 User interface

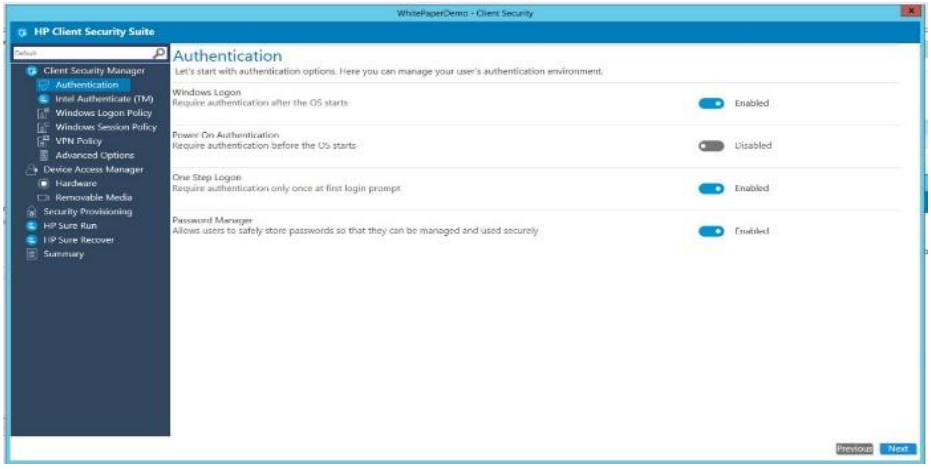
HP Client Security includes Client Security Manager, Device Access Manager, Sure Run, and Sure Recover

When you open HP Client Security, an introduction with a high-level description of the plugin is displayed. Select Create Policy. You will then be prompted to name your new policy baseline, select the new baseline, and enter any BIOS passwords needed (See HP BIOS Password Manager.)

8.5 Client Security Manager



8.5.1 Authentication



The following options are available:

- Windows Logon—Requires authentication at Windows logon (after the operating system starts)
- Power On Authentication—Requires authentication at computer start before the operating system starts.
- One Step Logon—Requires authentication only once at first logon prompt. Power-On Authentication must be enabled. (Please note that if using Intel® Authenticate™, One Step Logon is not supported due to the heightened security level.)
- Password Manager—Allows secure logon using security questions in case of a forgotten password or lost authentication device.

8.5.2 Intel Authenticate

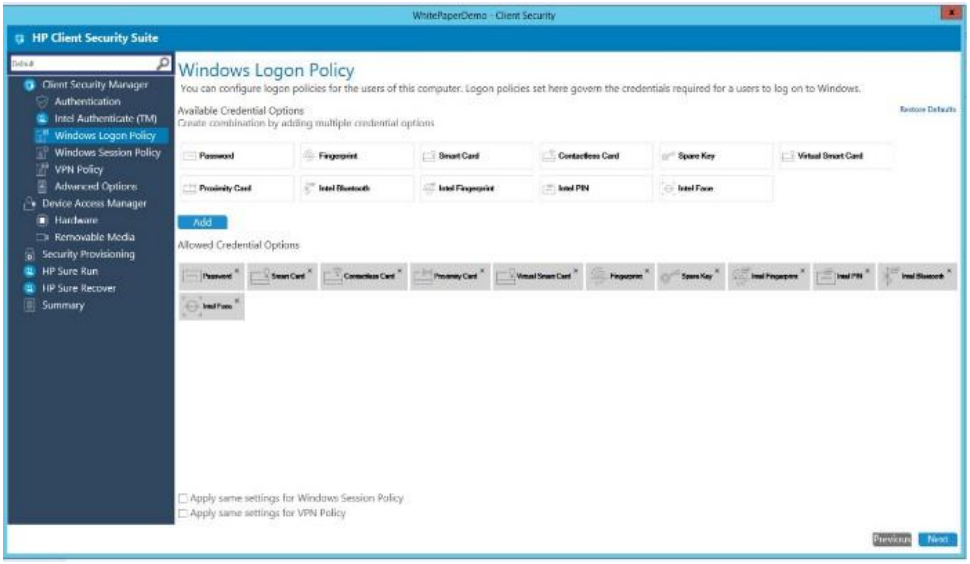
This page allows you to configure Intel Authenticate, if Intel Authenticate Engine is installed.

The following options are available:

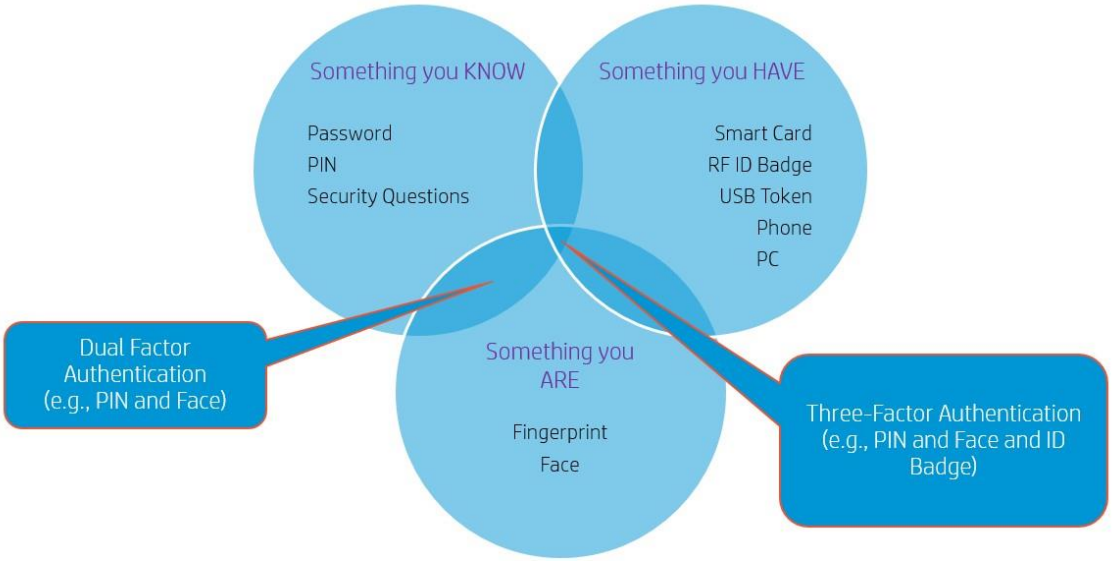
- Enable Intel Authenticate—Enables Intel Authenticate support. Please note that Intel Authenticate requires that certain hardware and software prerequisites be met in all computers in the collection the policy is being applied to. It also cannot be used with AMD processors so a separate collection of devices that meet the minimum requirements will need to be made. You can use the Authenticate_Check.exe file to determine if your computers meet the minimum requirements. Information on the minimum requirements and how to use the Authenticate_Check.exe can be obtained in the "Intel(R) Authenticate OEM Bring Up Guide" included with the Intel Authenticate engine on the HP Manageability website.
  If this option is enabled, you can select the certificate used to provision or communicate with the Intel Authenticate engine on client computers.
- Type the location of the security certificate—Browse to and select an X.509 certificate file, in Personal Information Exchange (PFX) format.
- Enter the password to unlock your certificate—Select this option and enter a password, if the certificated is protected by a password.
- My certificate does not have a password—Select this option and enter a password, if the certificated is protected by a password.

8.5.3 Windows Logon Policy

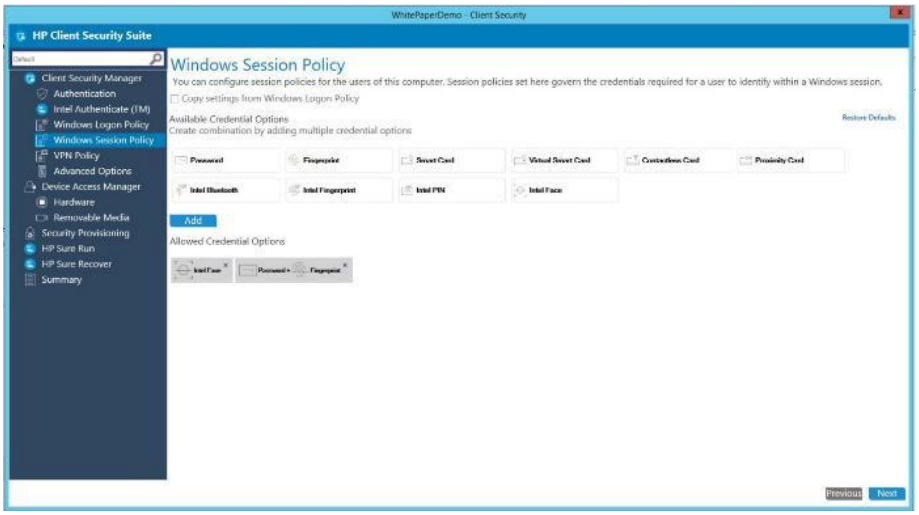
This page allows you to configure Windows Logon authentication.



- Add Credential— Select a credential or a combination of two or three credentials (three factor authentication requires vPro be enabled on the client computers) required for Windows Logon. To remove a configured credential, select the X icon in the upper-right corner of the credential. Each credential can only be used in one combination.
  - Please note: If allowing both Intel Authenticate fingerprint as well as classic Fingerprint, both policies must match. For example, if combining Intel Fingerprint with password you should do the same for classic Fingerprint.
  - If allowing Intel Authenticate Bluetooth, please note the following. The Intel Authenticate application must be downloaded from the appropriate store for Android or iOS. In order to force pairing of the phone via BLE the application must be open while pairing the phone to the computer. (Please see the document Intel Authenticate Bluetooth Pairing Steps) Also note that as of the writing of this guide some issues have been reported with IPhones receiving error31 or error35 when attempting to authenticate. Until this is corrected or tested in your environment it is suggested that if Intel Authenticate Bluetooth is allowed, another credential be allowed as well in case of Bluetooth failure.
  - If allowing use of Intel Authenticate Fingerprint for authentication, it has been reported that some sensors are timing out and not authenticating if no internet connection is available. To resolve this, please ensure the touch area fingerprint sensor reader has the latest driver available. Please see pre-requisites section.
  - At the time of this writing, Intel Authenticate supports only one user per device. This is expected to be enhanced in future releases late 2018. If more than one user is going to log into the computer, it is suggested that Intel Authenticate not be enabled in the managed scenario.
- Restore Default—Restores default settings, providing a way to start configuration from a known state.
- Apply Same Settings for Session and VPN policies – Applies the settings from this page to the Session and VPN policy pages automatically.
- Policy Creation Suggestions: When creating a policy keep in mind three types of authentication methods. These factors can include something you know (Password / PIN), something you are (Fingerprint / Face), and something you have (Phone / Contactless card). When allowing these items to be used for authentication it is recommended you combine one from each type of factor for best security. Keep in mind that when creating a policy with something you have, such as a Bluetooth phone, it is recommended that you allow an alternate method of authentication in case the authenticating item is inaccessible.


Something you KNOW
Password
PIN
Security Questions
Something you HAVE
Smart Card
RF ID Badge
USB Token
Phone
PC
Something you ARE
Fingerprint
Face
Dual Factor Authentication (e.g., PIN and Face)
Three-Factor Authentication (e.g., PIN and Face and ID Badge)

8.5.4 Windows Session and VPN Policy

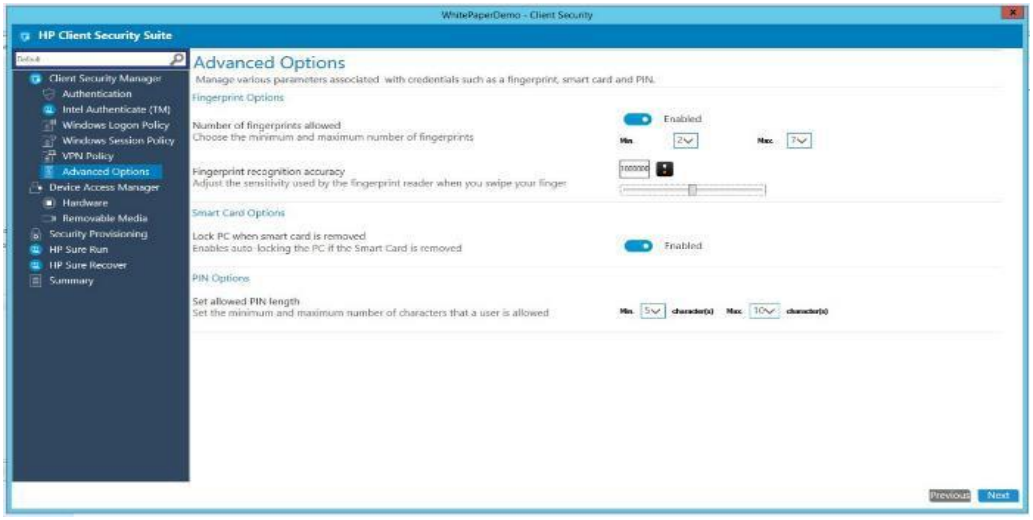


This page allows you to configure the policy and credentials used for a Windows session. This is for authenticating with applications such as Password Manager and Device Access Manager. The following page allows you to set the policy used for VPN authentication. Please see the document entitled VPN_Setup_Instructions for information on how to set up the VPN environment to authenticate with Intel Authenticate.

- Copy Settings from Logon Policy—Automatically copies the policy from Logon Policies
- Allowed Credential Options—Select a credential or a combination of two or three credentials (three factor authentication requires vPro be enabled on the client computers) allowed for Session Logon.

8.5.5 Advanced Options

This page allows you to further configure various credentials managed by HP Client Security.



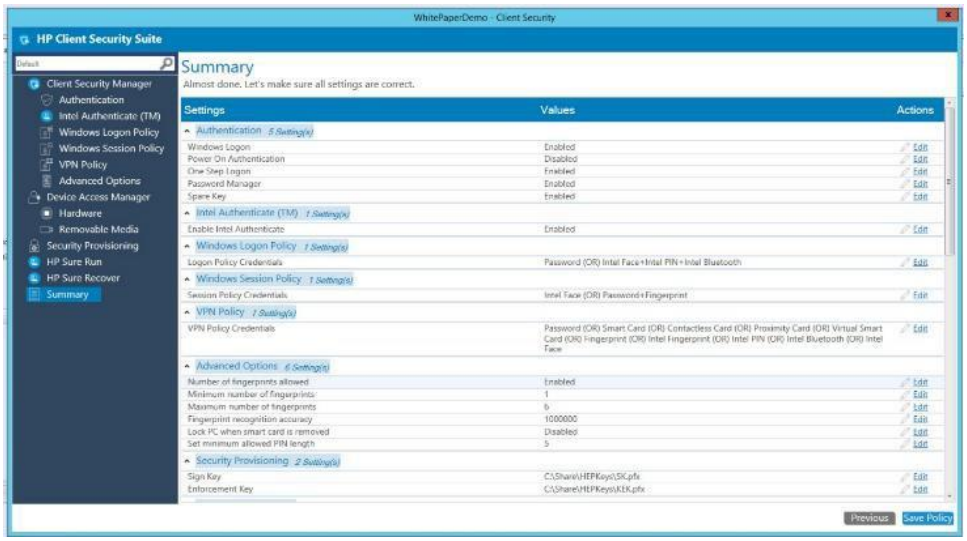
- Fingerprint Options

- Minimum number of fingerprints and Maximum number of fingerprints—Specify the minimum and maximum number of fingerprints a user can enroll. Force number of fingerprints to enroll must be selected.
- Fingerprint recognition accuracy—Configure the required fingerprint reader accuracy. (Not supported with Intel Authenticate fingerprint)

- • Smart Card Options
  - – Lock PC when smart card is removed—Automatically locks the computer when a smart card used as a credential is ejected.
- • PIN Options
  - – Set allowed PIN length—Specify the minimum number of characters for a user PIN. (Not supported with Intel Authenticate PIN)

8.6 Creating a Client Security policy

15. In Configuration Manager, select Assets and Compliance, and then select Overview.
16. Select HP Manageability Integration Kit, right-click Client Security Manager, and then select Create Policy.
17. Enter a Baseline name and start the creating policy wizard.
18. Modify settings. After configuring the settings, select Next.
19. Review the Summary page. If changes are necessary, select the Previous button; otherwise, select Save Policy.



20. After the policy has been saved successfully, select Deploy, and then select the target collections to which to apply the policy.

8.6.1 Editing a policy

21. In Configuration Manager, select Assets and Compliance, and then select Overview.
22. Select HP Manageability Integration Kit, right-click Client Security Manager, and then select Edit Policy.
23. Select an existing baseline policy to edit, and the select OK.
24. Follow the on-screen instructions to complete the wizard.

8.6.2 Additional information

Policies created with HP Client Security create configuration items for both Client Security Manager, Provisioning, HP Sure Run and HP Sure Recover.

Be sure to configure Intel Authenticate before creating policies. See the Intel Authenticate documentation for more information on whether your computer is supported and how to set up Intel Authenticate.

8.7 Security Provisioning

Remotely managed systems need to be configured to activate HP Sure Run and HP Sure Recover.

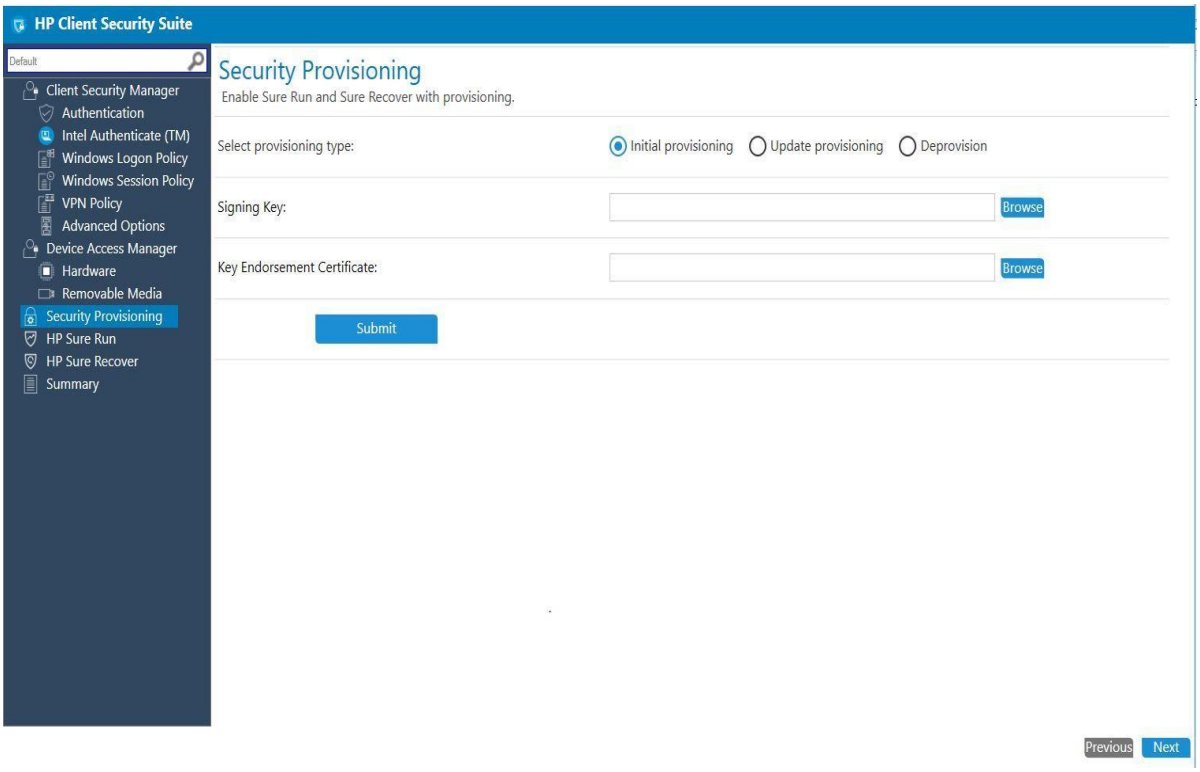
HP Sure Run and HP Sure Recover are managed using cryptographically verified commands that use public/private key pairs. In the steps below two separate key pairs are set up:

- 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 will 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 Run and HP Sure Recover commands.

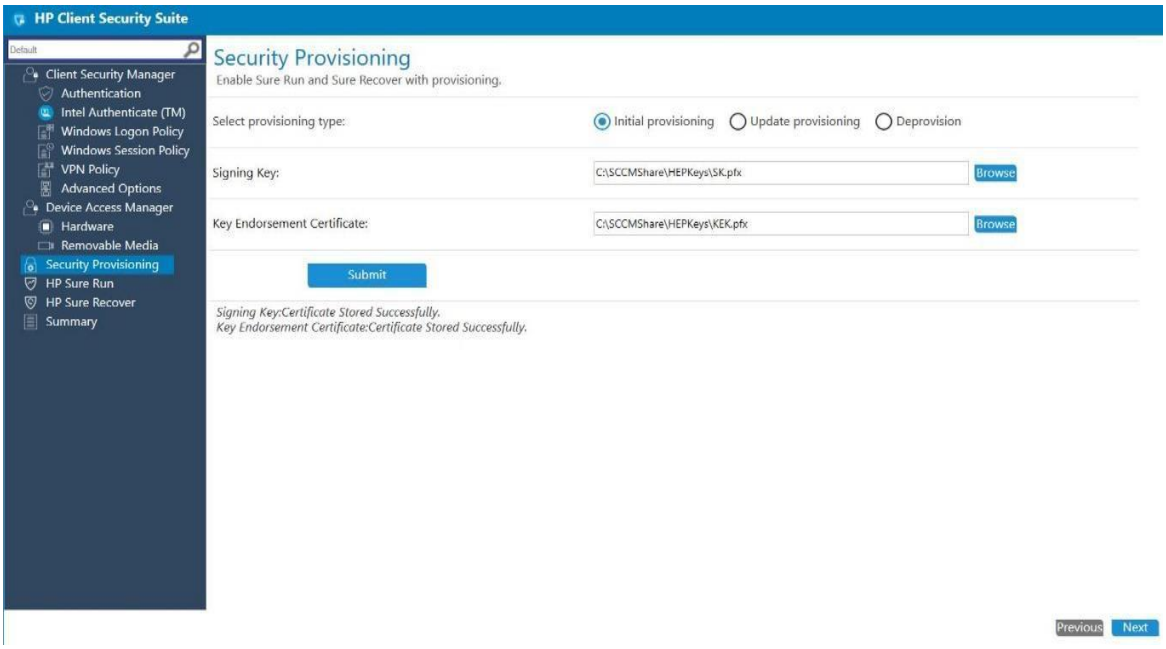
8.7.1 Initial Provisioning or Update Provisioning

8.7.1.1 Initial Provisioning – Provision the system for 1st time setup.



The IT Administrator needs to provide both a Signing Key and a Key Endorsement Certificate for initial provisioning. Click on the Browse button next to the text field to select the key/certificate saved on local disks.

Once the key or certificate has been selected, click Submit and then hit Next. Note - The key format supported is Personal Information Exchange (PFX).



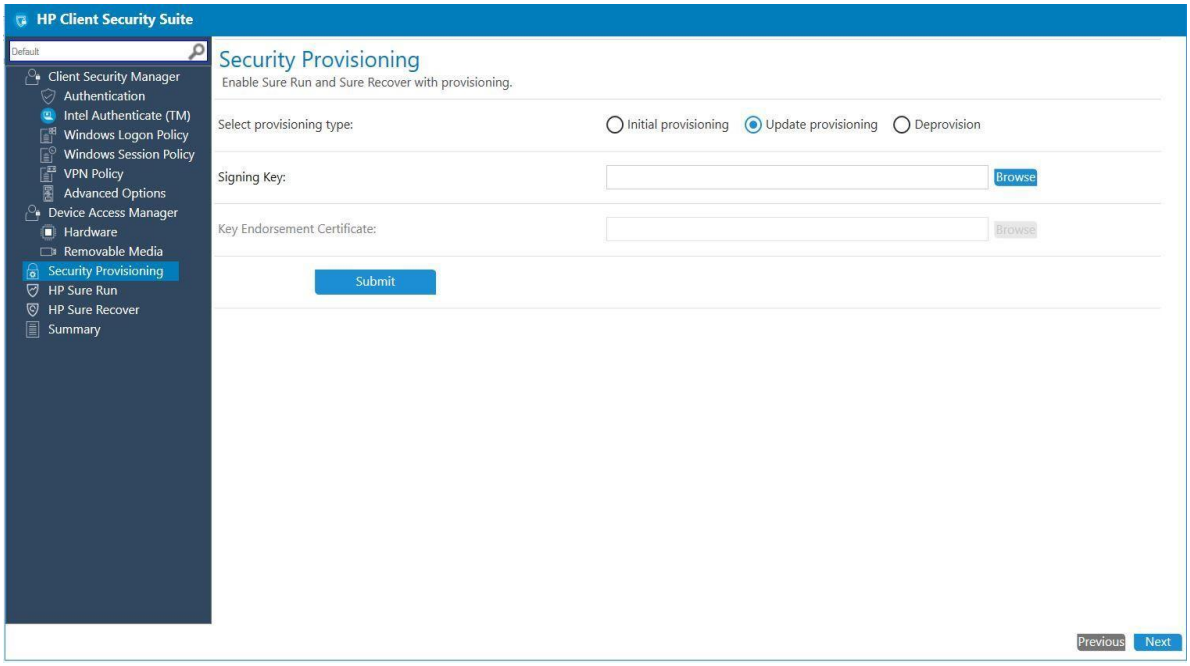
8.7.1.2 Update Provisioning

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

Navigate to Security Provisioning and select option Update Provisioning.

The IT Administrator needs to provide the signing key to update provisioning. Click on the Browse button next to the text field to select the key saved on local disks.

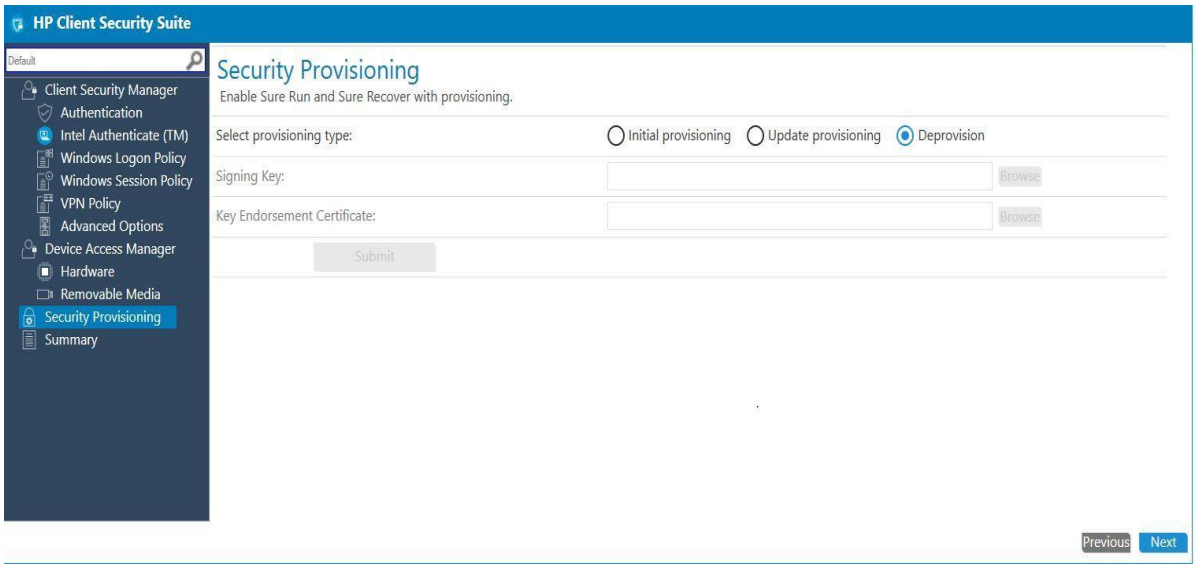
Once selected, click Submit and then hit Next



8.7.1.3 Deprovision

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

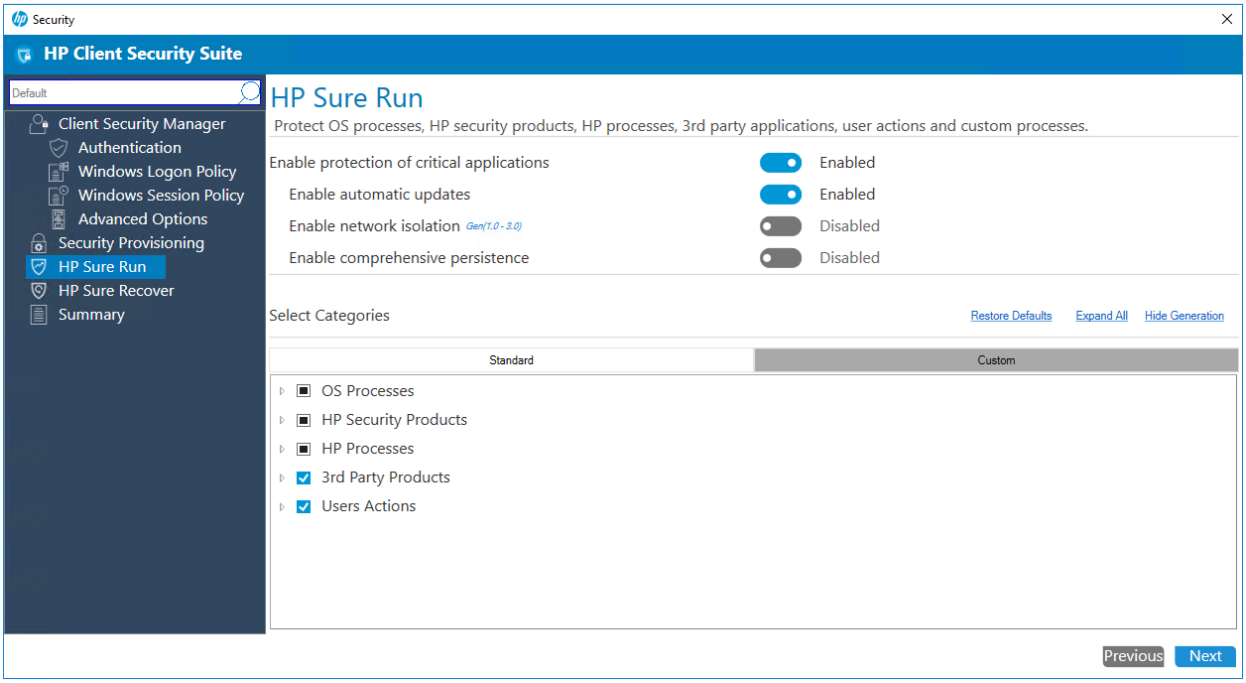
Navigate to Security Provisioning and select the option to Deprovision, then click Next.



8.8 HP Sure Run

8.8.1.1 Overview

- HP Sure Run can help you monitor critical applications and alert you in case of external threat.
- HP Sure Run allows the selection of individual applications or application categories to be monitored.



8.8.1.2 Configuration

Enable protection of critical applications

- Navigate to HP Sure Run Page. To enable HP Sure Run, select “Enable”.

Network Isolation

- Ability to enable / disable network isolation on managed system. When enabled it will disconnect managed PC from network for repeated non-compliance of watched items.
- Note! - this feature is only supported up to generation 3.0 of HP Sure Run S/W

Automatic Updates

- Enable this feature to update to the latest HP Sure Run version release available on HP FTP.
- Default for performing automatic updates for Sure Run S/W on remote managed device is now **enabled**.

Comprehensive Persistence – New!

- Enable this feature to automatically restore HP Security S/W product and any Custom apps in case of non-compliance.
- Note – Please refer to HP Sure Run Documentation for HP Security S/W products that can be persisted by the current generation of HP Sure Run S/W app.

Hide / Show Generation – New!

- Generation tag displayed to help identify feature support available across different generations of HP Sure Run S/W app.
- Generation tag will be shown by default across different features.

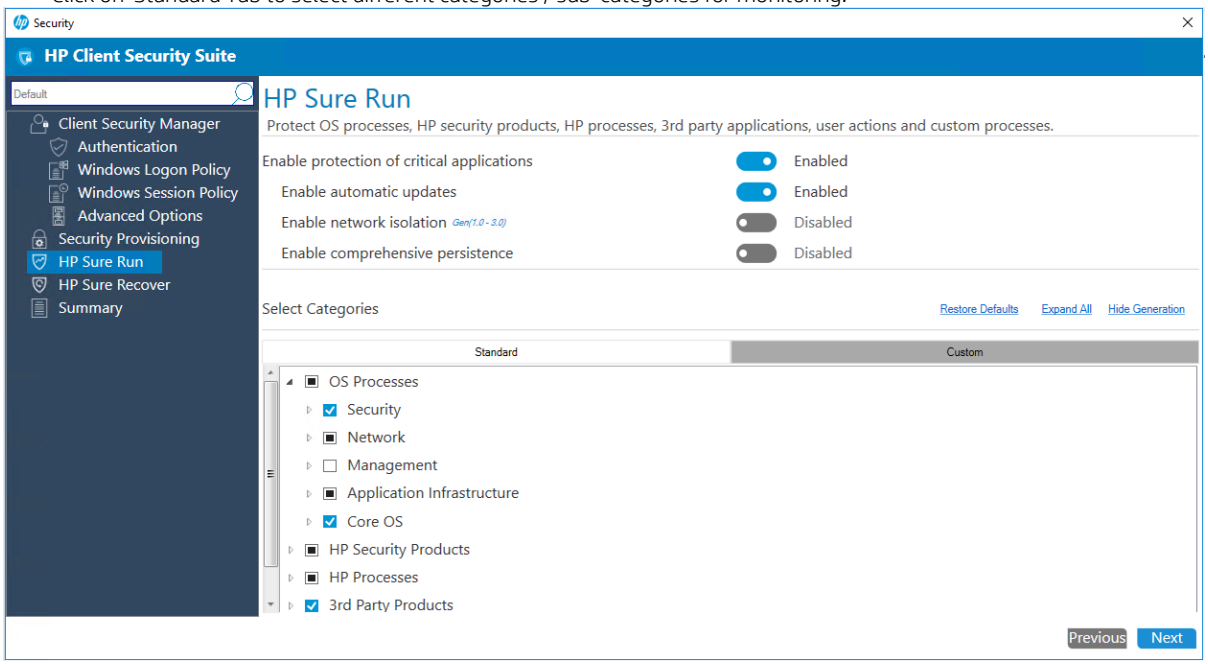
Categories

- IT Administrator have 2 options available to configure different watched item by HP Sure Run S/W.
  - **Standard** - HP-recommended policy pre-selected, with ability to modify as needed.

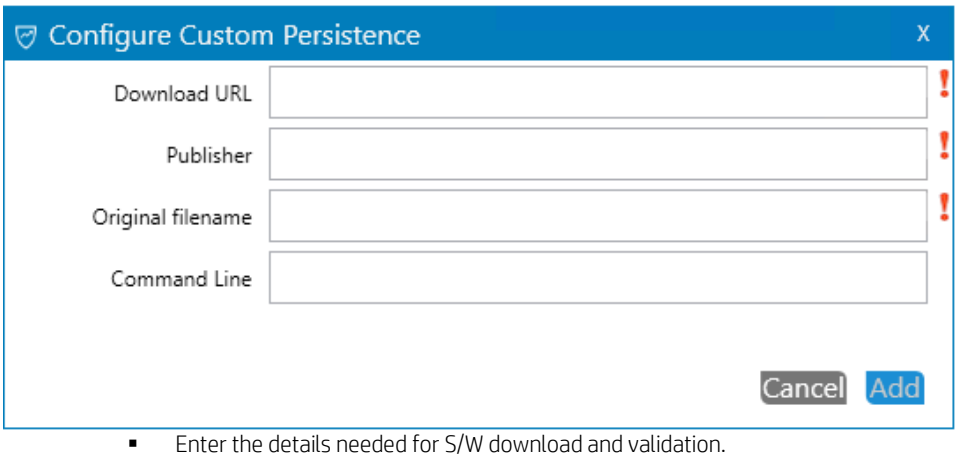
➢ **Custom** - ITDM can now add up to 10 custom processes that they wish to monitor

Standard Categories

- Click on Standard Tab to select different categories / sub-categories for monitoring.



- To configure Persistence for HP Standard Watched item expand category "HP Security Products"
  - Sub-category that supports persistence will have a edit link next to it.
  - Click on Edit Link

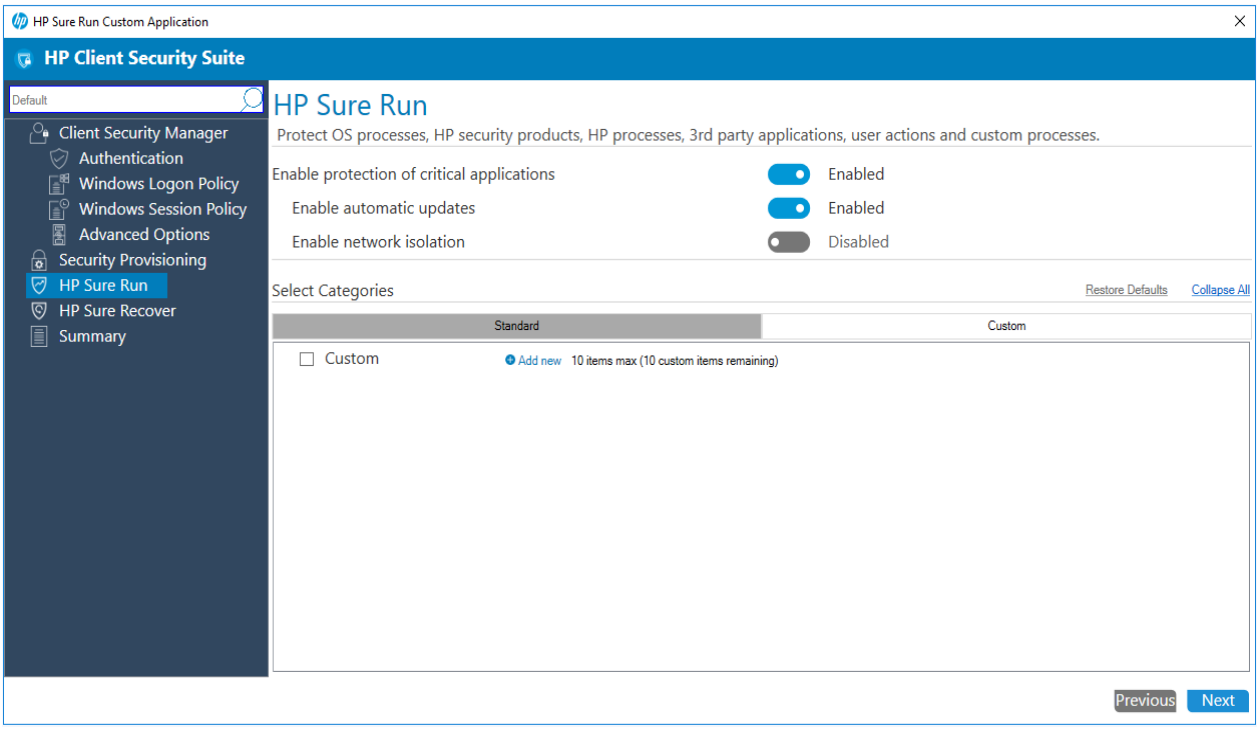


  - Enter the details needed for S/W download and validation.

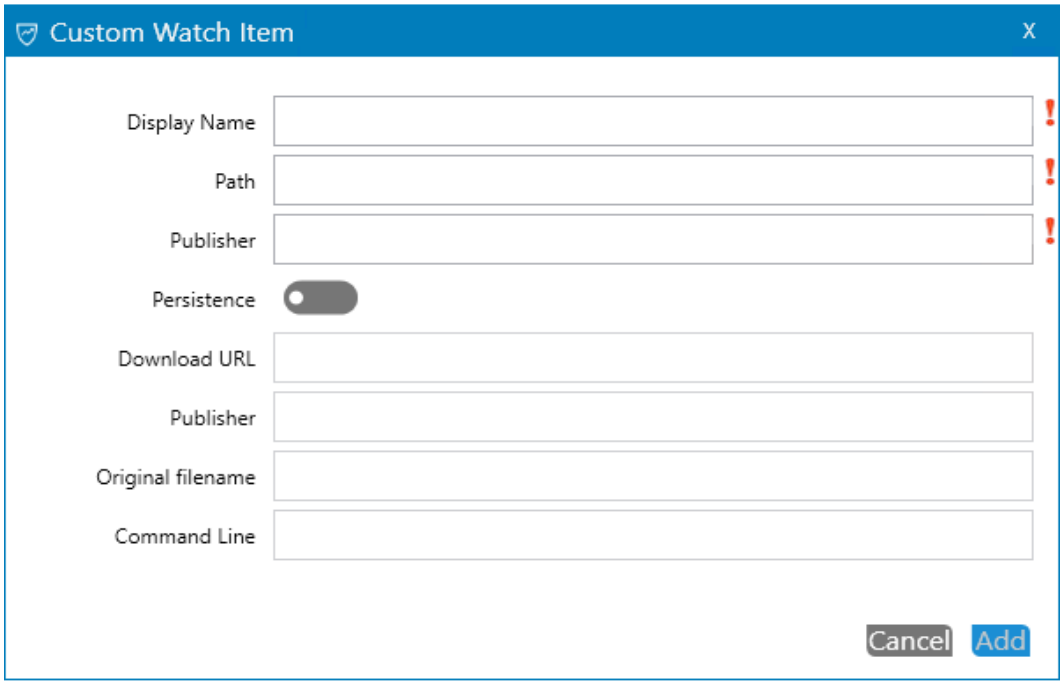
(!) Note fields are mandatory.

Custom Category

- To add a Custom watch entry, select Custom Tab



- Click on Add new link.
- Following dialog box will be displayed to add custom application details.



- To configure Persistence select enable “Persistence”
  - Enter the details needed for S/W download and validation.

(!) Note fields are mandatory. Please refer to appendix section for additional information.

8.8.1.3 Supported client platforms

- HP Elite products equipped with 8th generation Intel or AMD processors.

8.8.1.4 Supported client operating systems

- Windows 10 RS3 and above.

8.8.1.5 Other client system prerequisites

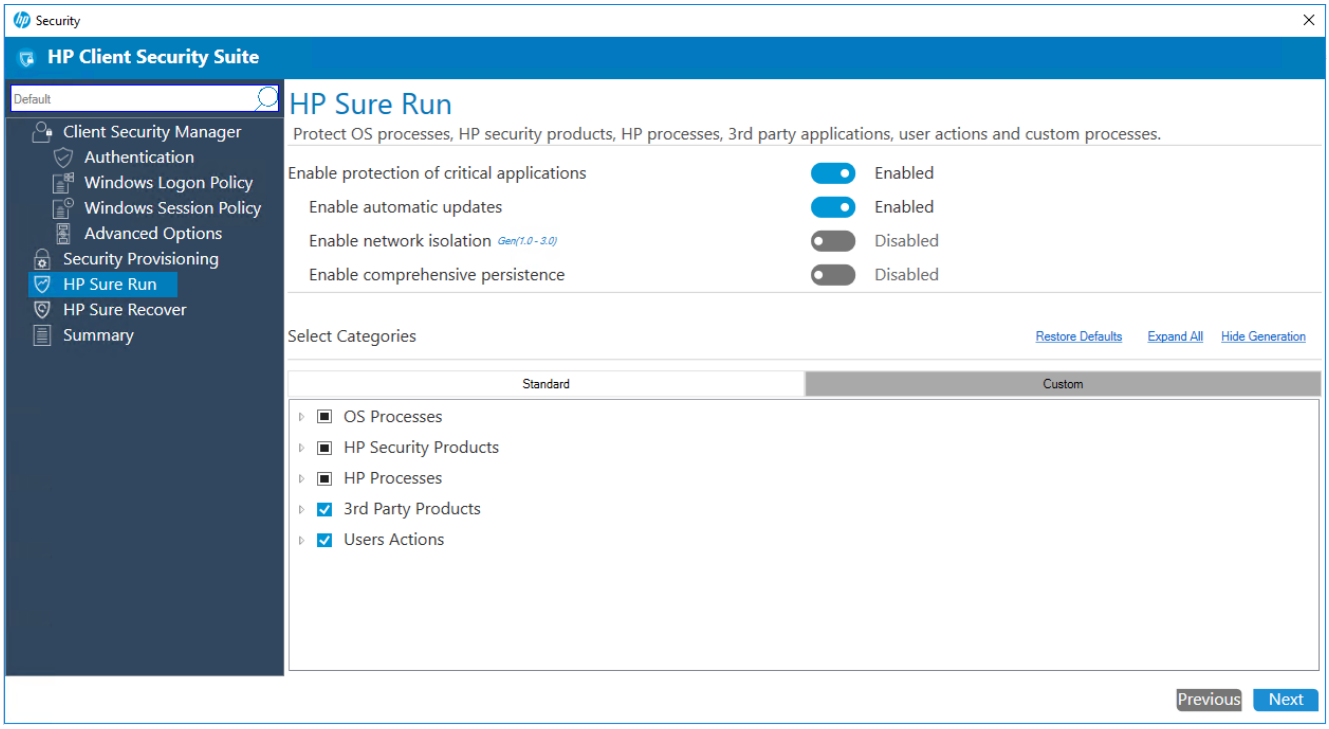
- Microsoft .NET Framework 4.6.1 or higher
- HP Client Security Manager 9.3.11.* or above
- HP MIK Client v2.0.18.1 or higher.

8.8.1.6 Pre-Requisite

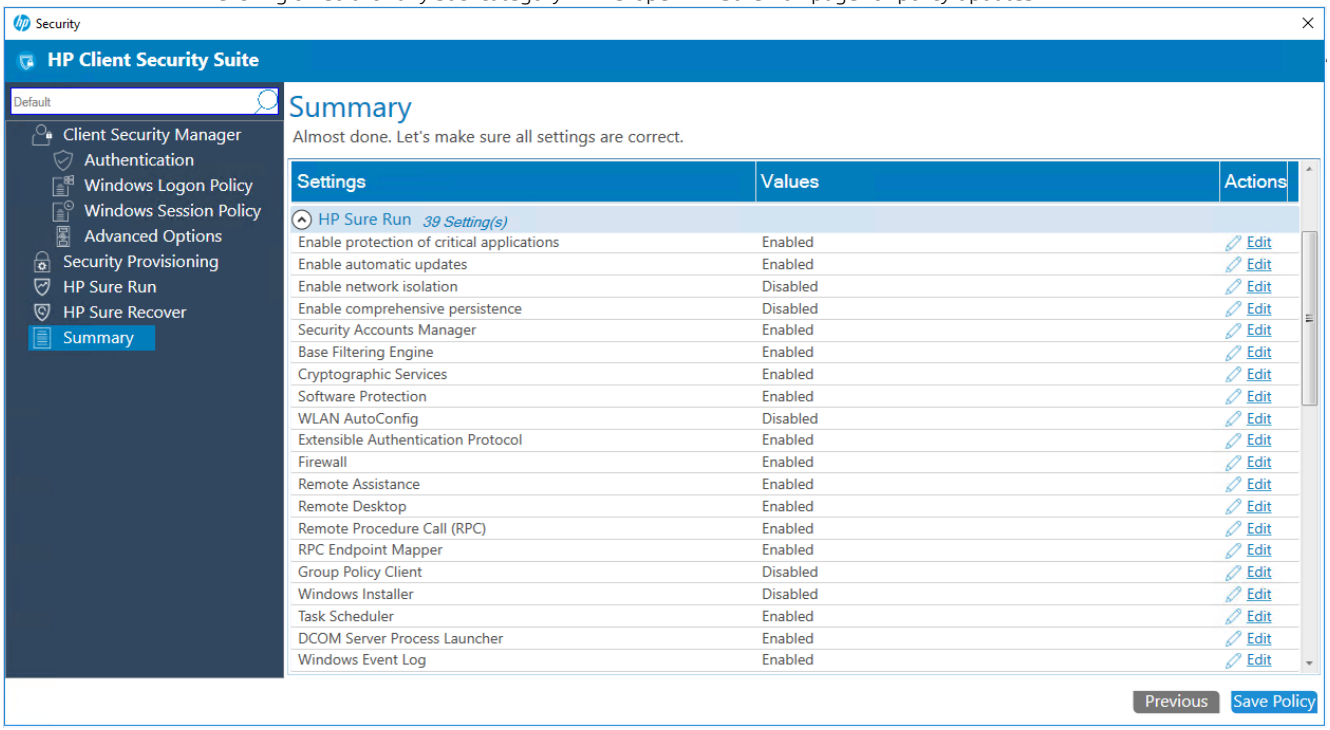
All client systems are provisioned for HP Sure Run Policy to be applied. Please review section on Security Provisioning for details.

8.8.1.7 Creating a policy

1. In Configuration Manager, select Client Security, and then select Overview.
2. Select HP Manageability Integration Kit, right-click Client Security Manager, and then select Create Policy.
3. Enter a Baseline name and start the creating policy wizard.



4. Navigate to HP Sure Run page. Confirm default standard selections and modify as needed. Add custom application if any that need to be monitored. Click on Next.
5. On Summary Page under section HP Sure Run selected sub-categories are available for final review and changes. Clicking on edit for any sub-category will re-open HP Sure Run page for policy updates.



6. Select Save Policy.
7. After the policy has been saved successfully, select Deploy, and then select the target collection{s} to apply the policy.

8.8.1.8 Additional information

1. Client system must be rebooted for policy to be applied successfully. In case a policy fails to deploy, an additional reboot may be required.

2. IT Administrator need to ensure selected application{s} installed on client systems. Otherwise end user will see continuous toaster notifications for applications not installed.

3. Any potential malicious activity on client system will result in:

   - Toaster pop-up displayed to end user.
   - Equivalent HP Sure Run messages logged in Windows Event Viewer.
   - Gen 2 supports network isolation when repeated noncompliance detected for watched item.

8.8.1.9 Uninstalling protected applications

If protected applications are no longer needed, the HP Sure Run configuration must be modified to remove the application from the watch list before uninstalling.

8.8.1.10 Interaction between HP Sure Run and HP Sure Recover

If an OS recovery is performed using HP Sure Recover, HP Sure Run is automatically disabled following the recovery process and must be reenabled.

8.8.1.11 Resetting or clearing of the TPM will result in HP Sure Run failures

HP Sure Run requires the use of TPM 2.0 to perform signing and decryption operations. When the TPM is reset or cleared any keys that HP Sure Run created will be invalidated and cannot be used. The only way to resolve this is to disable HP Sure Run and then reenable it.

8.9 HP Sure Recover

8.9.1 Overview

HP Sure Recover helps you to securely install the operating system from the network with minimal user interaction. Systems with HP Sure Recover with Embedded Reimaging also support installation from a dedicated local storage device. Note that the imaging process reformats the drive so data should be backed up if possible, beforehand or data loss will occur.

Recovery images provided by HP include the basic Windows 10 installer and install optimized drivers for HP devices. HP recovery images do not include data recovery agents that are not included with the Microsoft Windows 10 media, for example, OneDrive. Corporations can create their own custom images to add corporate settings, applications, drivers, and data recovery agents.

An OS recovery agent performs the steps necessary to install the recovery image. The recovery agent provided by HP performs common steps like partitioning, formatting, and extracting the recovery image to the target device. Systems that don't support Embedded Reimaging download the HP recovery agent from hp.com, so Internet access is required to retrieve it. Corporations can also host the HP recovery agent within their firewall or create custom recovery agents for more complicated recovery environments.

8.9.2 Configuration

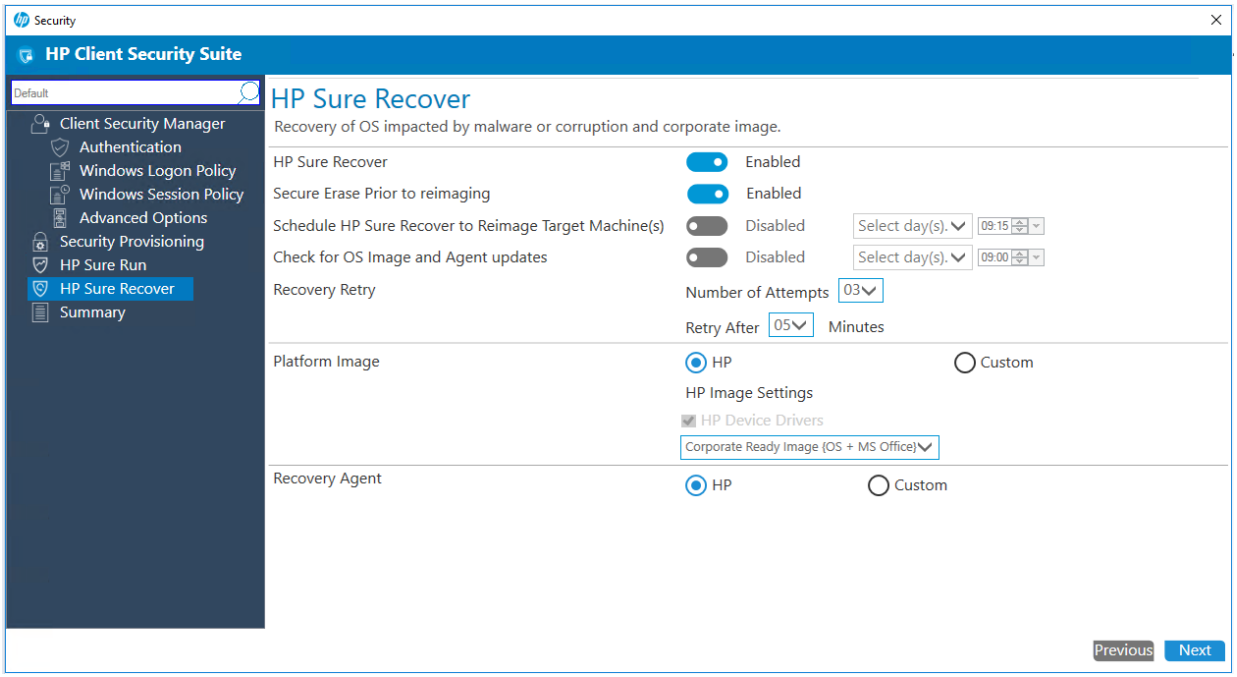
Navigate to the HP Sure Recover Page. To enable HP Sure Recover, select "Enable".

The location to download the recovery agent or recovery image from can also be configured, either from HP or corporate locations. Reimaging can also be performed on a schedule to ensure that the system is in a pre-determined state after the event. Another schedule can be established to check for recovery agent and recovery image updates on systems that support Embedded Reimaging. When newer content is available on the network than what's currently in the Embedded Reimaging device it will be downloaded to a cache on the drive, then copied to the Embedded Reimaging device on the next reboot after validation.

8.9.3 Recovery from HP

The IT Administrator will have the HP-recommended policy pre-selected, with the ability to modify as needed.

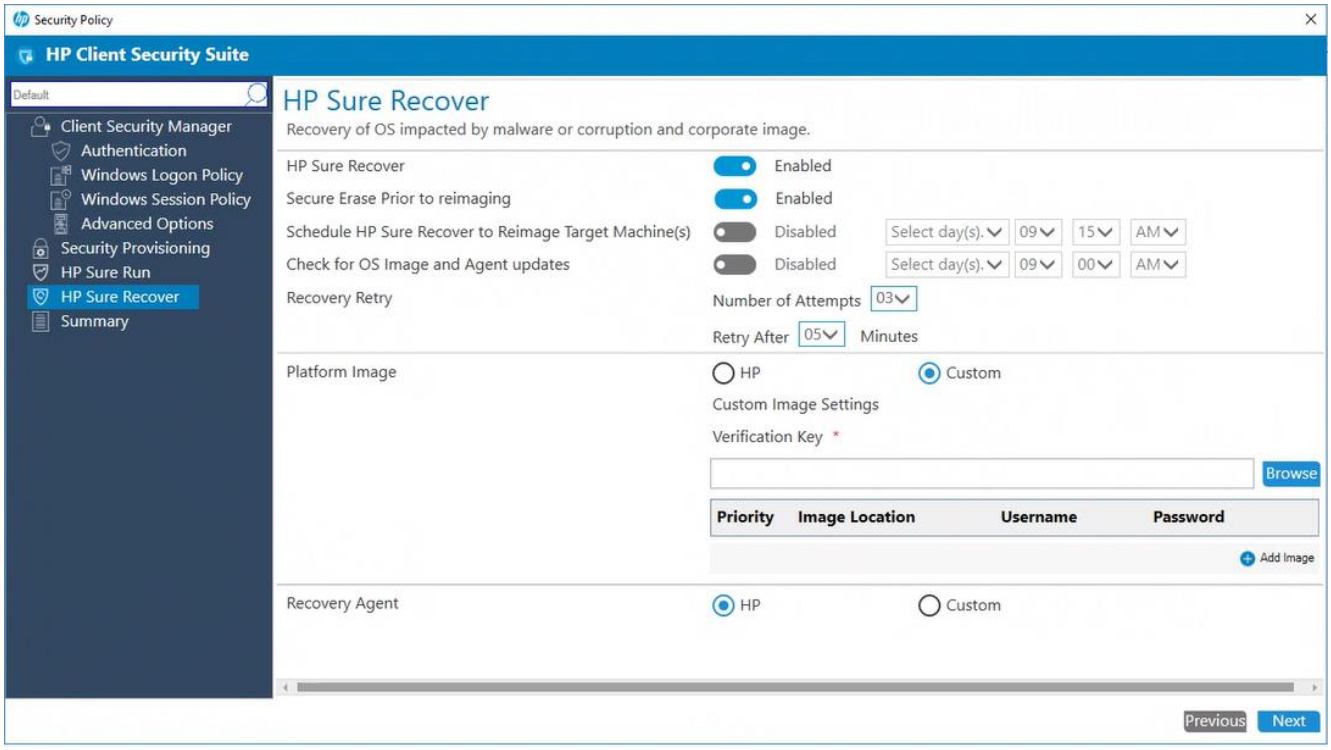
- New ! - The default configuration uses the HP recovery agent to install a HP Corporate Ready image with Microsoft Office and the drivers that are included with the Windows 10 installation media and the HP Device Drivers.
- No default schedule is established to perform Sure Recover or update the Embedded Reimaging device contents.



8.9.4 Custom Recovery

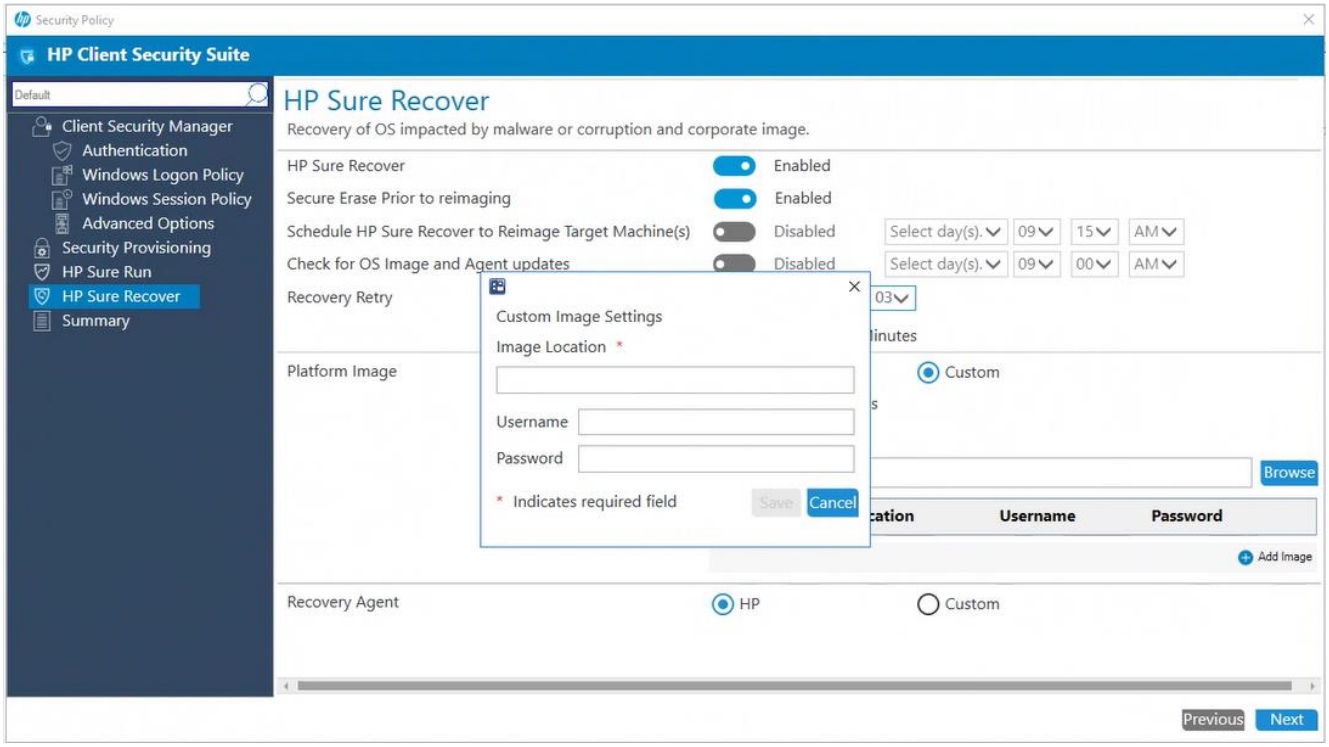
8.9.4.1 Platform Image - Custom

Select the Custom option to restore a customized OS image from a corporate distribution point. The IT Administrator needs to provide the URL to download the image from and the public key to use for image validation.



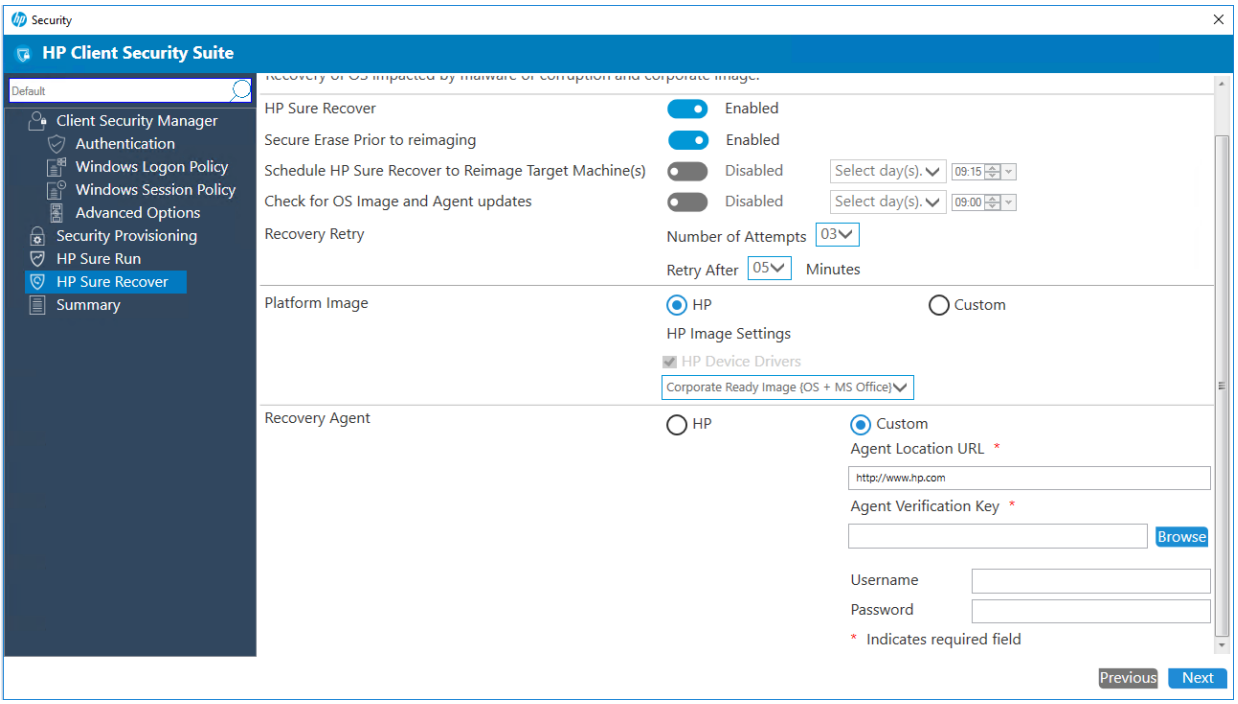
Click on Add Image. Enter the username and password to access the distribution point if required.

Note - ITAdmin can add maximum 2 custom image location. First 1 entered is considered the primary location to download , the 2nd one will be configured as failover URL site.



8.9.4.2 Recovery Agent - Custom

Select the Custom option to use a custom recovery agent or the HP recovery agent from a corporate distribution point. The IT Administrator needs to provide the URL to download the agent from and the public key to use for agent validation.

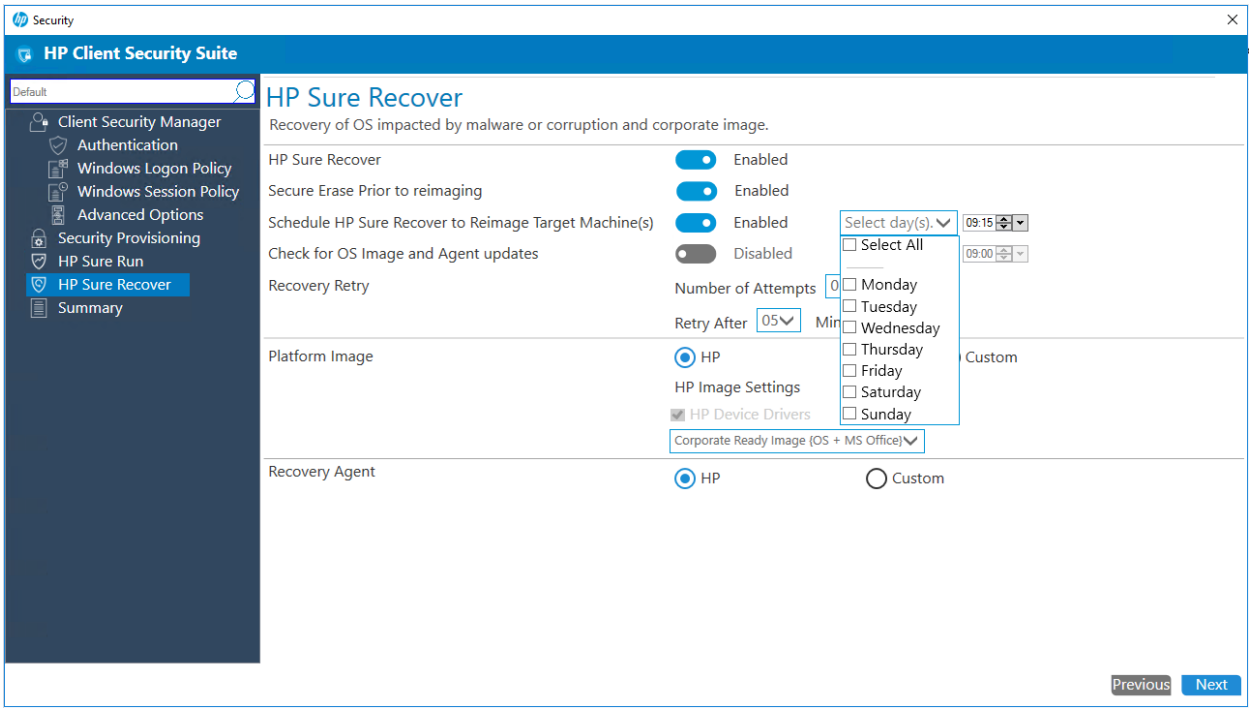


Note:

- FTP & HTTP are supported for downloading the recovery agent and recovery image.
- Username and password are optional and depend on the way server accounts are configured.
- The Image Verification Key must be provided in ".pem" format.
- The Image Location URL must be provided in the following example format:
  http://server.com/<folder>/<name>.mft
  Refer to section # Additional Information for details on how to create manifest file.
    - The Agent Location URL must be provided in the following example format:
      http://server.com/<folder>/
      Refer to section # Additional Information for details on how to create manifest file.
    - The manifest and its signature must be in the same directory on the server, and the signature file must have the same name as the manifest but with a .sig extension.
    - The agent manifest signature must be in little-endian format. Signature files created by openssl must be converted from big-endian to little-endian.

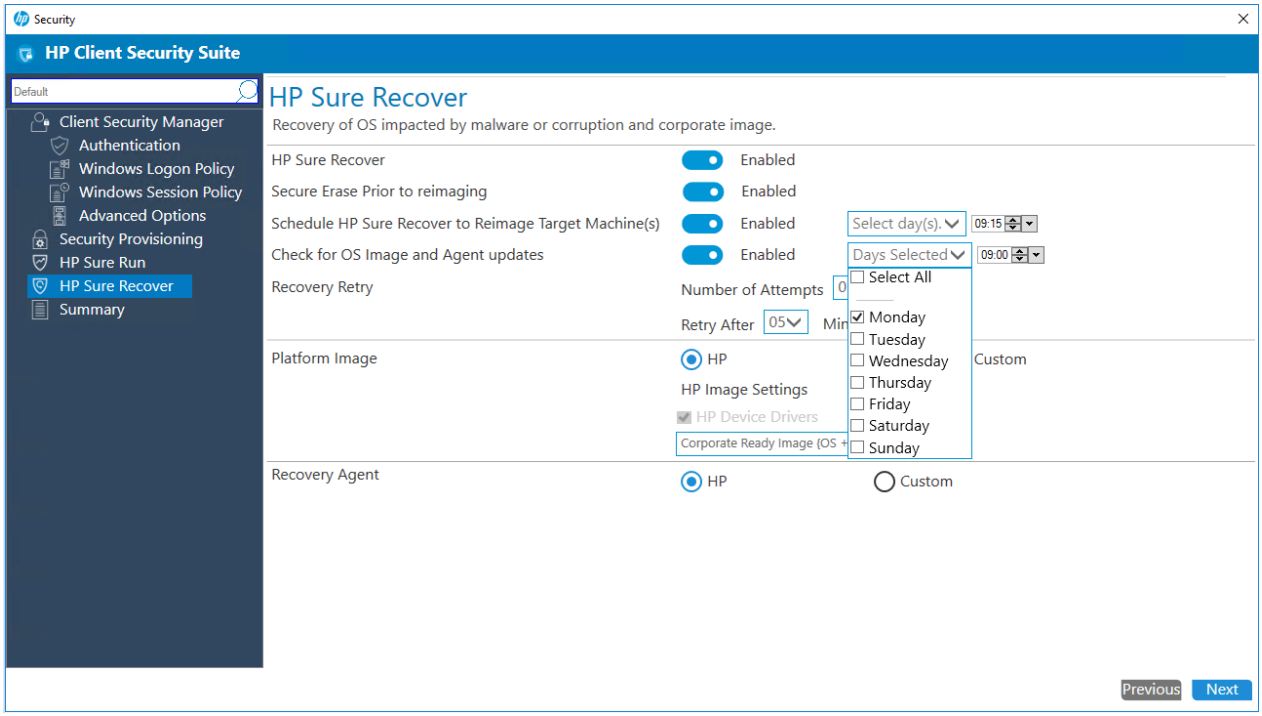
8.9.5 Schedule Recovery on client systems

Recovery can be scheduled on managed devices by enabling the **Schedule HP Sure Recover to Reimage Target Machine(s)**. Recovery can be scheduled for multiple days each week at a specific time.

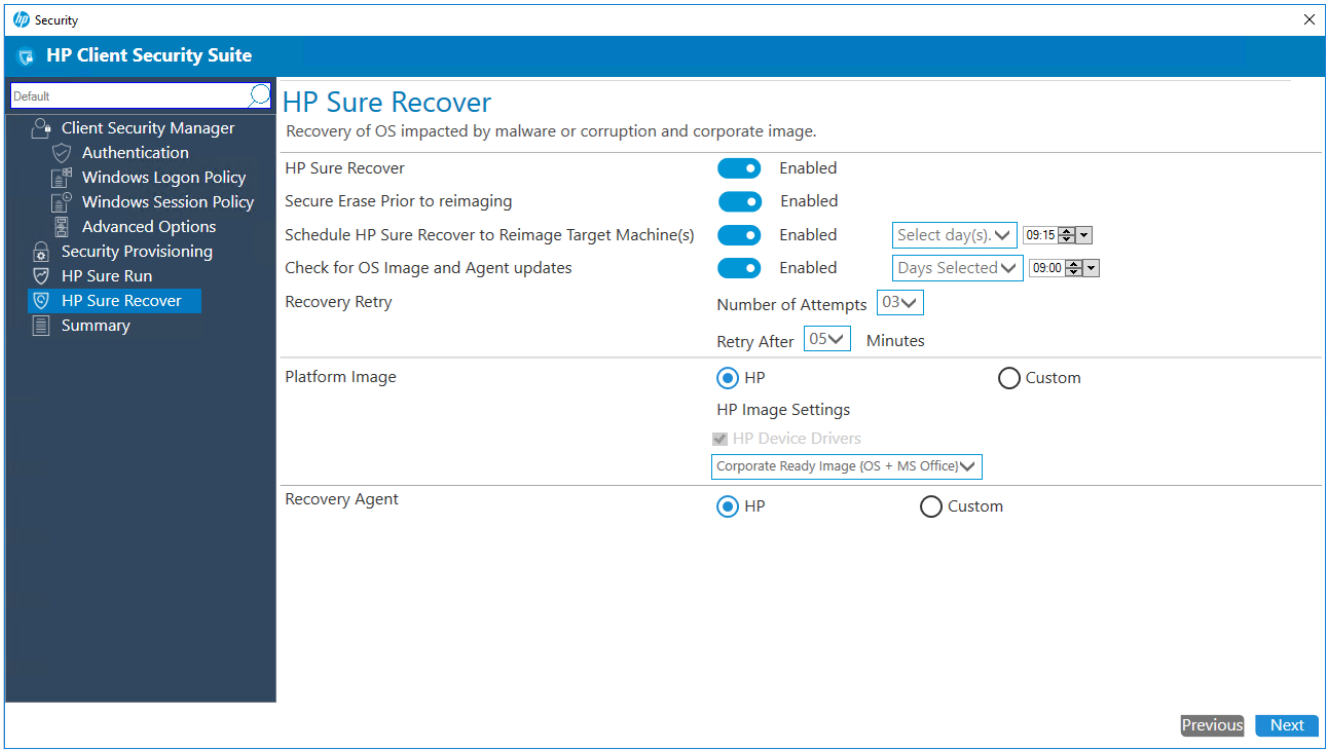


8.9.6 Schedule Embedded Reimaging device content updates

The contents of the Embedded Reimaging device need to be updated when the recovery agent or recovery image on the network is updated. Since the Embedded Reimaging storage device is only available during recovery events that occur in the pre-boot environment a Windows task can be created to download updates to a cache and trigger the pre-boot environment to copy from the cache to the Embedded Reimaging device on the next reboot. The schedule for the task can be established on managed devices by enabling the **Check for OS Image and Agent updates** option and can be scheduled for multiple days each week at a specific time.



8.9.7 Support for OS Recovery Retry attempts and Wait period between retry attempts



In environments where many systems need to be recovered simultaneously but the network is experiencing errors it may be desirable to establish policies that prioritize systems and restrict downloads. Systems that support Embedded Reimaging can be configured to automatically recover from the onboard storage with no user intervention or by requiring a Physical Presence Indicator (PPI). Please refer to the system BIOS documentation for PPI configuration information.

Systems that don't support Embedded Reimaging can be configured to keep attempting recovery until successful, or the number of retry attempts and wait period between attempts can be configured to minimize network utilization. By default, the BIOS will make 3 recovery attempts and wait 5 minutes before retrying. The recovery agent adheres to the same policy.

8.9.8 Supported client platforms

- Most commercial systems support recovery from the network. Select configurations also support Sure Recover with Embedded Reimaging. Refer to the product specifications for more details.

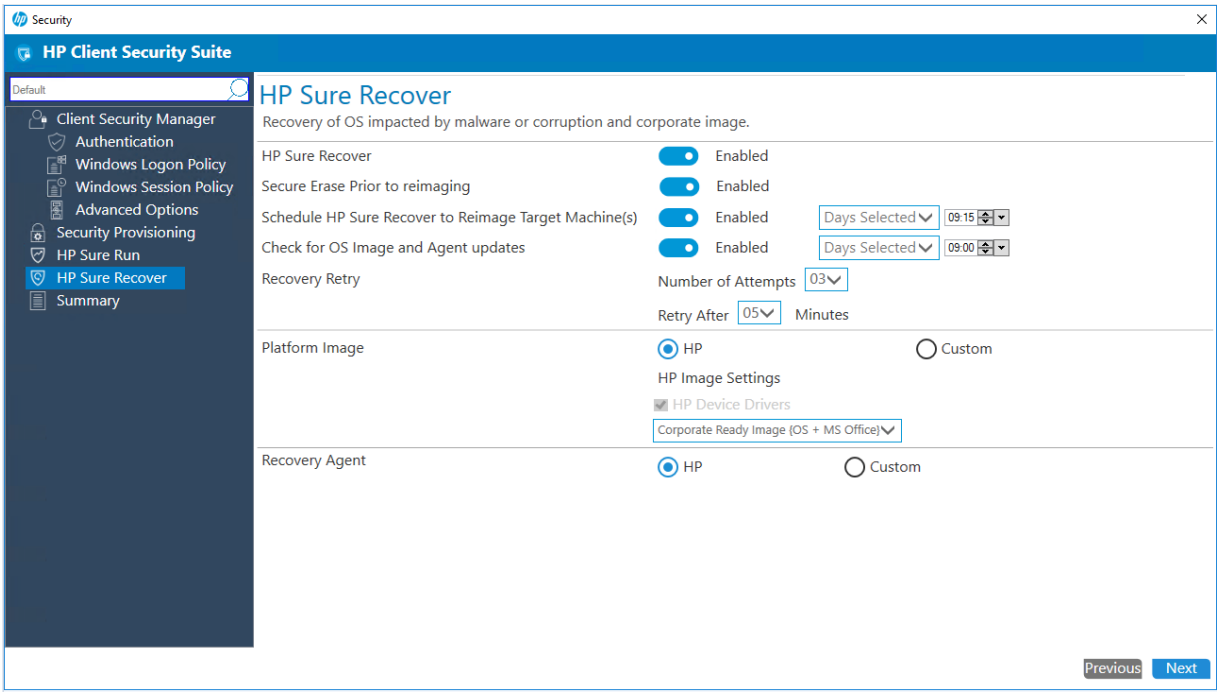
8.9.9 Supported client operating systems and system prerequisites

- The default Sure Recover policies require no additional configuration, but client systems must be provisioned before changing policies. Please review the section on Security Provisioning for details.
- Windows 10 RS3 and above.
- Microsoft .NET Framework 4.6.1 or higher
- HP Client Security Manager 9.3.11.XXXX or above
- HP MIK client v2.0.8.1 for only Gen 1 supported platform
- HP MIK client v3.0.X.X and above for Gen 1 & Gen 2 supported platforms.

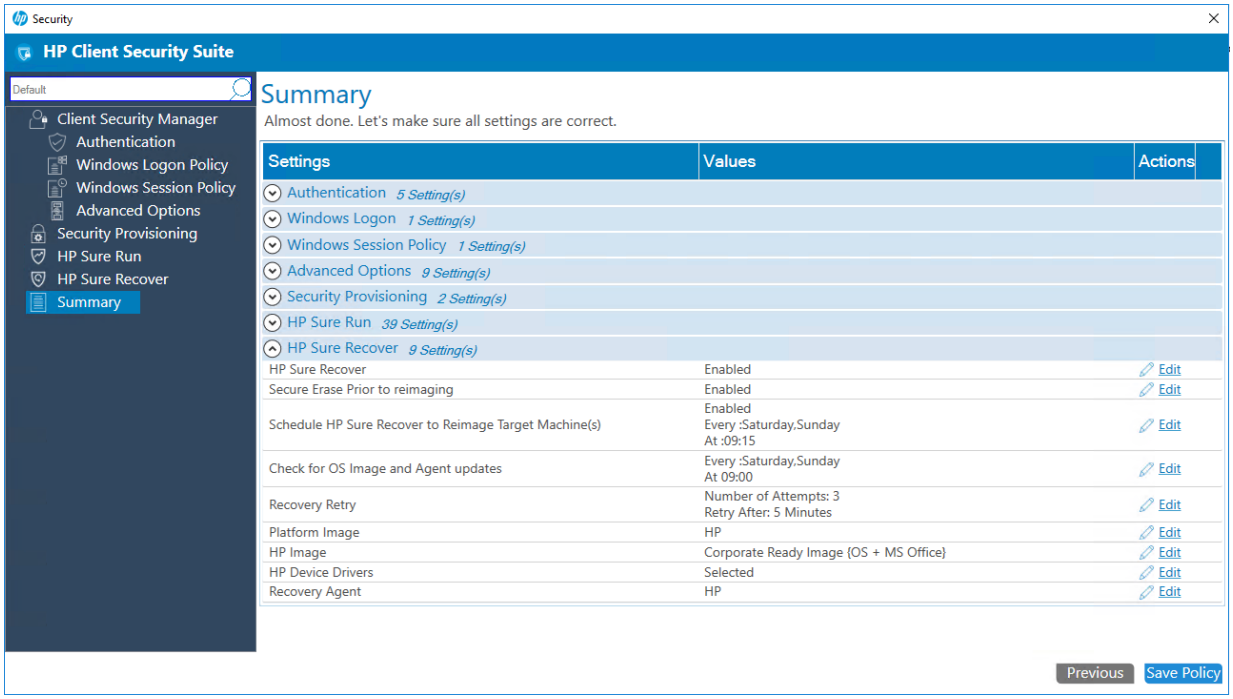
8.9.10Creating a policy

1. In System Center Configuration Manager, select HP Manageability Integration Kit, right-click Client Security Manager, and then select Create Policy.

2. Navigate to the HP Sure Recover Page. Confirm default selections and modify as needed, then click Next.



3. On the Summary Page under the HP Sure Recover section, selections are available for final review and changes. Clicking edit for any of the item listed will re-open the HP Sure Recover page for policy updates.



4. Select Save Policy.

The client system must be rebooted for the policy to be applied successfully. If the policy fails to deploy, an additional reboot may be required.

8.9.11Steps to create and sign an image manifest

Pre-requisites: a tool to generate sha256 hashes and a tool to create a private/public key pair and sign the manifest file, e.g., PowerShell or OpenSSL.

To create an RSA 2048 bit key pair with OpenSSL:
openssl genrsa -out private_key.pem 2048
openssl rsa -in private_key.pem –pubout -out public_key.pem

1. Create the image manifest file

   The manifest filename should follow Windows naming conventions without spaces and must have a .mft extension. The manifest format for corporate images includes a header as the first line, followed by a list of files that make up the image, one per line. The manifest header consists of the manifest format version and image version. The remaining lines in the file must consist of the sha256 hash of the file, its filename and path relative to the URL provisioned for the manifest, and its filesize in bytes.

   For example:

   mft_version=1, image_version=1

   8f161eac8d9197088ad8892e5d529b0287b5a9b8604c546e5a66d8737531c1ab os-drivers.wim 535769370
   The following methods can be used to create sha256 hashes in Windows:

   - certutil -hashfile os-drivers.wim sha256
   - Powershell: ps> get-filehash os-drivers.wim -algorithm sha256

2. Sign the manifest

   The signature file must have the same filename as the manifest but with a .sig extension.

openssl.exe dgst -sha256 -sign private_key.pem -out image.sig image.mft

Verify that the manifest is signed correctly:
openssl dgst -sha256 -verify public_key.pem -signature image.sig image.mft

3. Place the image files, manifest, and signature file on the distribution point.

   - IIS servers require creating mime types of application/octet-stream for .wim, .swm, .mft, .sig , .efi and .sig files for pcbios folder or default web.
   - IIS servers also require creating mime types of application/octet-stream for **"."** (dot) files that have no filename extension

Note:

A public/private keypair must be used to sign/validate the manifest file. Keep the private key in a safe location. The Image Verification Key used must be the public key corresponding to the private key used when signing the manifest, otherwise a validation failure will occur when running the recovery process.

8.9.12Steps to create and sign a recovery agent manifest

Pre-requisites: a tool to generate sha256 hashes and a tool to create a private/public key pair and sign the manifest file, e.g., powershell or OpenSSL.

To create an RSA 2048 bit key pair with OpenSSL:
openssl genrsa -out private_key.pem 2048
openssl rsa -in private_key.pem –pubout -out public_key.pem

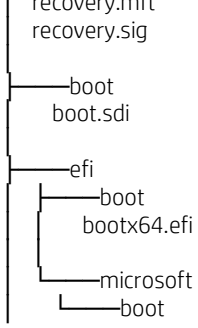
1. Create the recovery agent manifest file

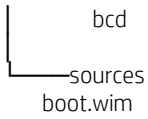
   The recovery agent manifest file must be named recovery.mft. The manifest format for corporate recovery agents includes a header as the first line, followed by a list of files that make up the recovery agent, one per line. The manifest header consists of the manifest format version, which currently must be 1, and recovery agent version, which must increment each time a new recovery agent is released. The rest of the manifest must include the sha256 hashes of each file included in the recovery agent, the filename and path relative to the URL provisioned for the manifest, and filesize in bytes, one line per file.

   For example:

   version=1, agent_version=1
   77bcf4fe47f8383f6e7324a46d8aba37c218836a6233843f9a046b1320bd5710 \sources\boot.wim 592969344
   cd2c00ce027687ce4a8bdc967f26a8ab82f651c9becd703658ba282ec49702bd \boot\boot.sdi 3170304
   e8e52ac8de68a034481f7a43f5c7db5883f2a5934b0892a158356c554681a4d1 \efi\boot\bootx64.efi 1469240
   f198ad15597940db4fb3a660b5a26828834176ba70222c83249a9d77e24ecc7e \efi\microsoft\boot\bcd 262144

   In this example, the agent location URL should specify the full path to the manifest starting at the document root, but should not include the manifest filename, e.g., http://server.com/agents, where the manifest is in a directory called "agents" within in the document root and the remaining files are located in the directory tree shown below:





The following methods can be used to create sha256 hashes in Windows:

- certutil -hashfile os-drivers.wim sha256
- Powershell: ps> get-filehash os-drivers.wim -algorithm sha256

4. Sign the manifest

   The signature file must be named recovery.sig. For example, to sign the manifest with OpenSSL:

   openssl.exe dgst -sha256 -sign private_key.pem -out recovery.sig recovery.mft

   Verify that the manifest is signed correctly:
   openssl dgst -sha256 -verify public_key.pem -signature recovery.sig recovery.mft

   Note:

   Openssl signatures are generated in big-endian format and must be converted to little-endian format for the BIOS to properly validate the manifest.

5. Place the agent files, manifest, and signature file on the distribution point.

   - IIS servers require creating mime types of application/octet-stream for .wim, .swm, .mft, .sig , .efi and .sig files for pcbios folder or default web.
   - IIS servers also require creating mime types of application/octet-stream for **"."** (dot) files that have no filename extension

Note:

A public/private keypair must be used to sign/validate the manifest file. Keep the private key in a safe location. The Image Verification Key used must be the public key corresponding to the private key used when signing the manifest, otherwise a validation failure will occur when running the recovery process.

8.9.13Interaction between HP Sure Run and HP Sure Recover

If an OS recovery is performed using HP Sure Recover, HP Sure Run is automatically disabled following the recovery process and must be reenabled.

9 Device Guard (Windows 10 only)

Device Guard is included with Windows 10 and provides hardware- and software-based malware protection, by verifying that applications and drivers are from a trusted source before they are allowed to run. In HP MIK, Device Guard polices provide an easy option for an IT administrator to enable Device Guard.

9.1 Supported client platforms

- • HP commercial computers (2015 or later)

9.2 Supported client operating systems

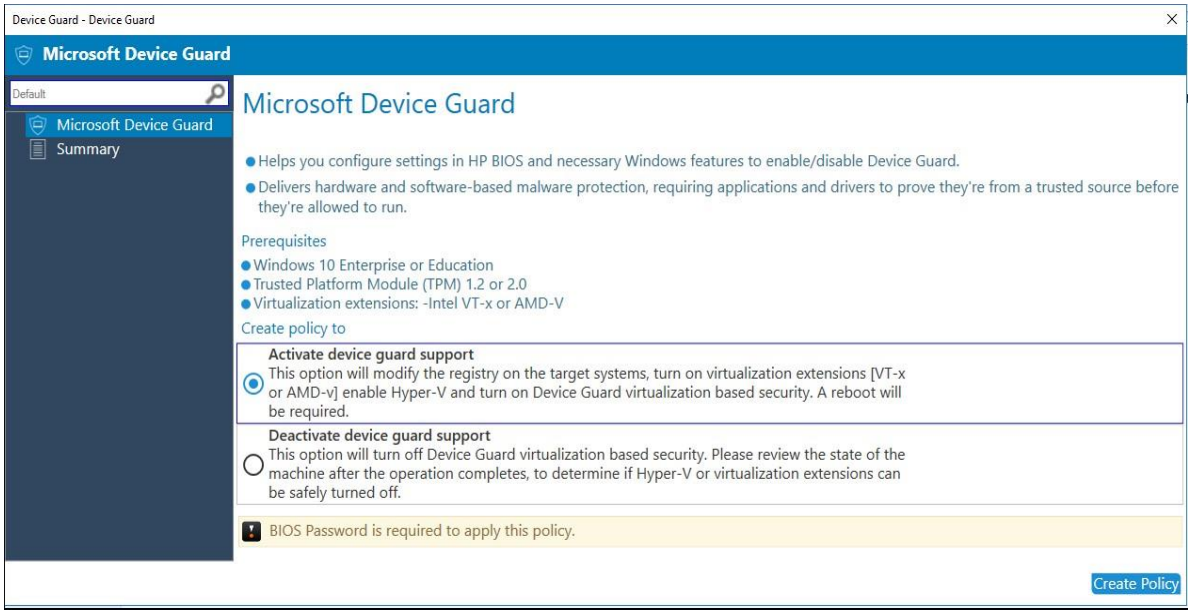
- • Windows 10

9.3 Other client system prerequisites

- Microsoft .NET Framework 4.0 or higher
- HP MIK

9.4 Creating a policy

1. In Configuration Manager, select Assets and Compliance, and then select Overview.
2. Select HP Manageability Integration Kit, right-click Device Guard, and then select Create Policy.
3. Enter a Baseline name and then follow the on-screen instructions to complete the wizard.
4. Select one of the following options:



a. Create a policy to activate device guard support—Modifies the registry on target systems, enables the virtualization extension, enables Hyper-V, and enables Device Guard virtualization-based security.

   The following registry settings are modified:

   i. [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceGuard]

      1. "EnableVirtualizationBasedSecurity"=dword:00000001

      2. "HypervisorEnforcedCodeIntegrity"=dword:00000001

      3. "RequirePlatformSecurityFeatures"=dword:00000002

   ii. [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]

      1. "LsaCfgFlags"=dword:00000001

   The following Windows features are modified:

   i. Microsoft Hyper-V and Isolated User Mode are enabled.

   The following BIOS settings are modified (if they are available on the client computer)

   i. SVM CPU Virtualization is enabled on AMD Platforms

   ii. Virtualization Technology (VTx) is enabled on Intel platforms

   iii. Virtualization Technology for Directed I/O (VTd) is enabled on Intel Platforms

   iv. TPM Device is set to available

   v. TPM State are set to available

   vi. CD-ROM Boot is disabled

   vii. PXE Boot is disabled

   viii. USB Storage Boot is disabled

   ix. Legacy Boot is disabled

   x. UEFI Boot is enabled

   xi. Configure Legacy Boot Support is set to Legacy Support Disable and Secure Boot Enable

b. Create policy to deactivate device guard support—Disables Device Guard virtualization-based security.

   Deactivating Device Guard reverts registry settings to their default settings.

   i. Hyper-V is disabled.

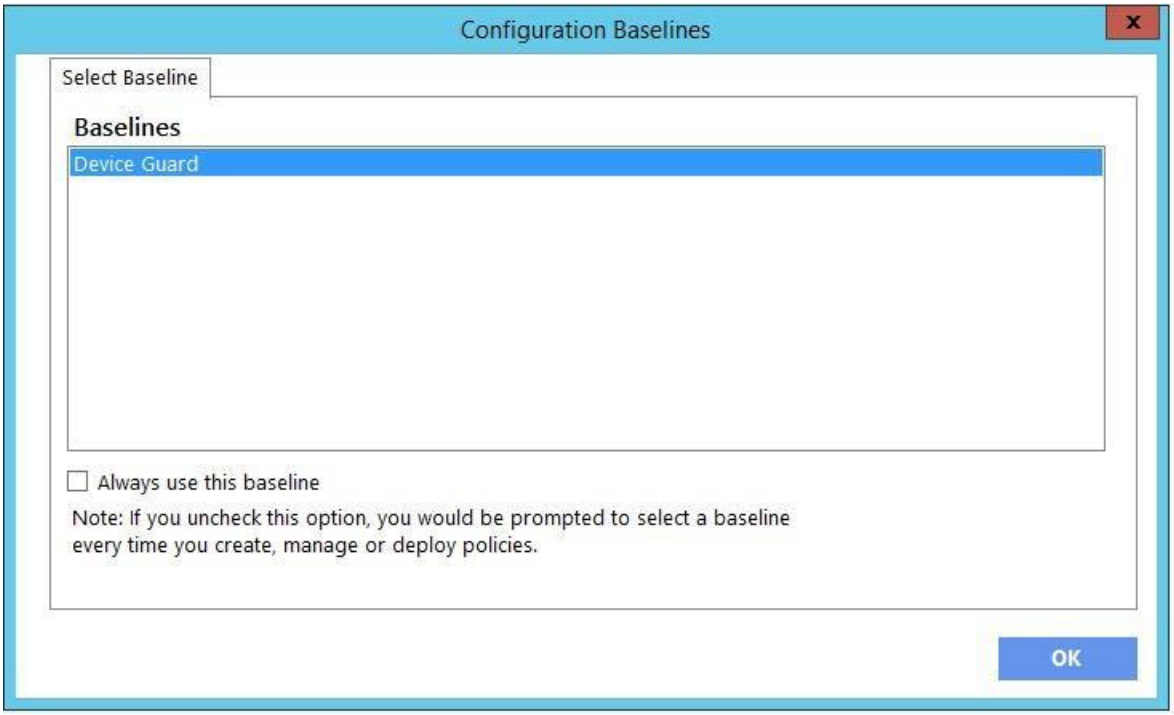
   ii. BIOS Virtualization is disabled.

5. Review the Summary page. If changes are necessary, select the Previous button; 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.

9.5 Editing policy

1. In Configuration Manager, select Assets and Compliance, and then select Overview.
2. Select HP Manageability Integration Kit, right-click Device Guard, and then select Edit Policy.
3. Select an existing baseline policy to edit, and then select OK.



4. Complete the procedure for steps 4 through 6 in Creating a policy.

9.6 Additional information

For client computers, the HP MIK Device Guard policy log is created in `%PROGRAMDATA%\HP\HP MIK\Logs`.

The following error codes might be encountered:

Table 1 Device Guard error code table

Error code	Description
0	OK
1	Item is not known. There might be an installation error.
2	Operating system not supported. See the operating system requirements.
3	CPU/Chipset not supported. See the platform requirements.
4	Outdated Graphics Driver. Update the graphics driver before attempting the operation again.

Error code	Description
5	Failed to enable BIOS CPU Virtualization
6	Failed to set BIOS TPM Device as Available
7	Failed to disable BIOS USB device boot
8	Failed to disable BIOS PXE boot
9	Failed to disable BIOS Floppy boot
10	Failed to disable BIOS CD-ROM boot
11	Failed to change BIOS Boot Mode to UEFI Native (Without CSM)
12	Failed to enable BIOS Secure Boot
13	Failed to set Hyper-V
14	Failed to set Isolated User Mode
15	Error in setting Registry value(s)
16	Failed to modify Windows features

10 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.

10.1 Supported client platforms

- HP 700 series and higher commercial computers (2014 or later)

10.2 Supported client operating systems

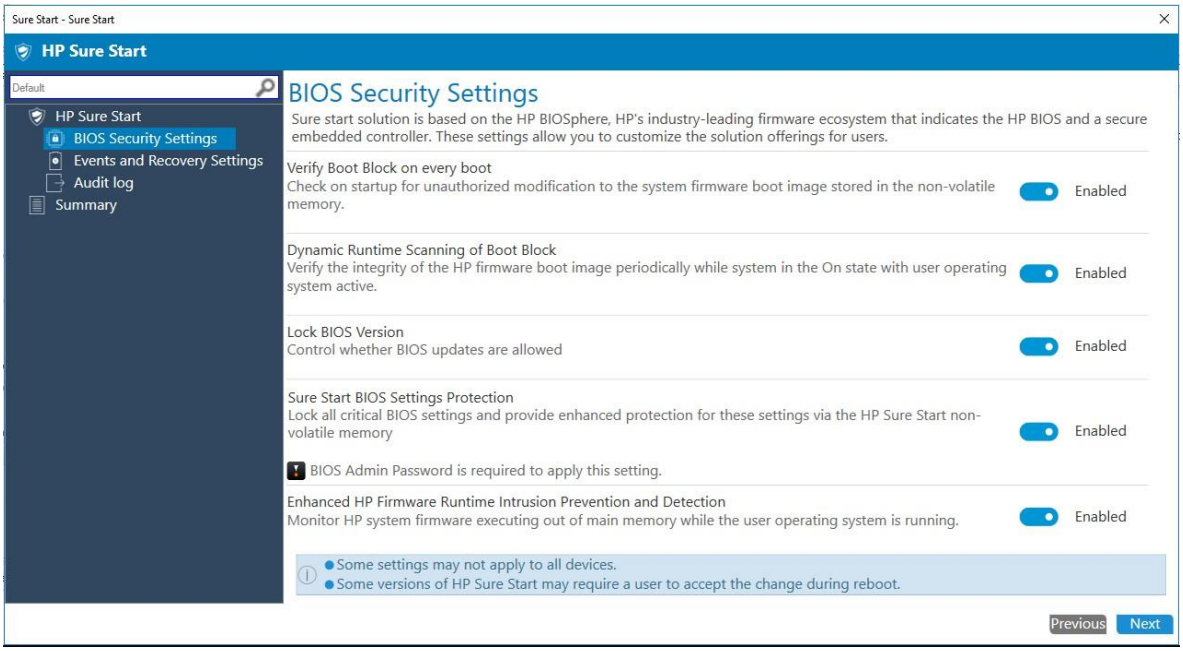
- Windows 10
- Windows 8.1
- Windows 7

10.3 Other client system prerequisites

- Microsoft .NET Framework 4.0 or higher
- HP MIK

10.4 User interface

10.4.1 BIOS Security Settings tab



- 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.

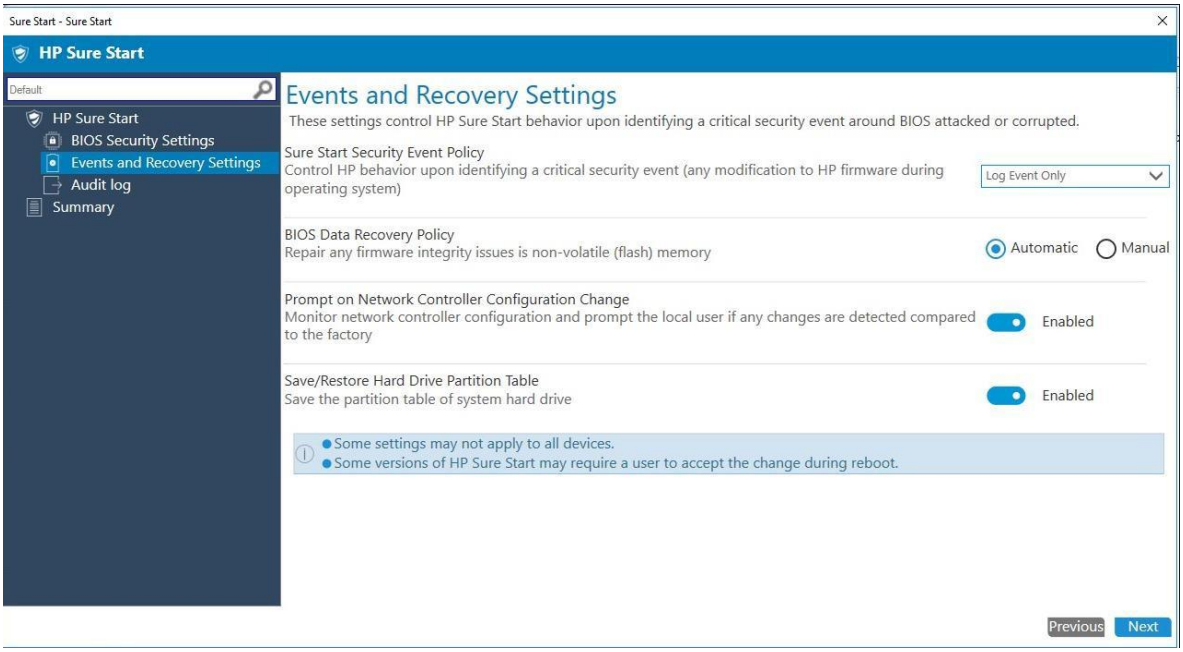
  The BIOS administrator password is required to enable this setting.

- Enhanced HP Firmware Runtime Intrusion Prevention and Detection—Monitors HP system firmware executing out of main memory while the operating system is running.

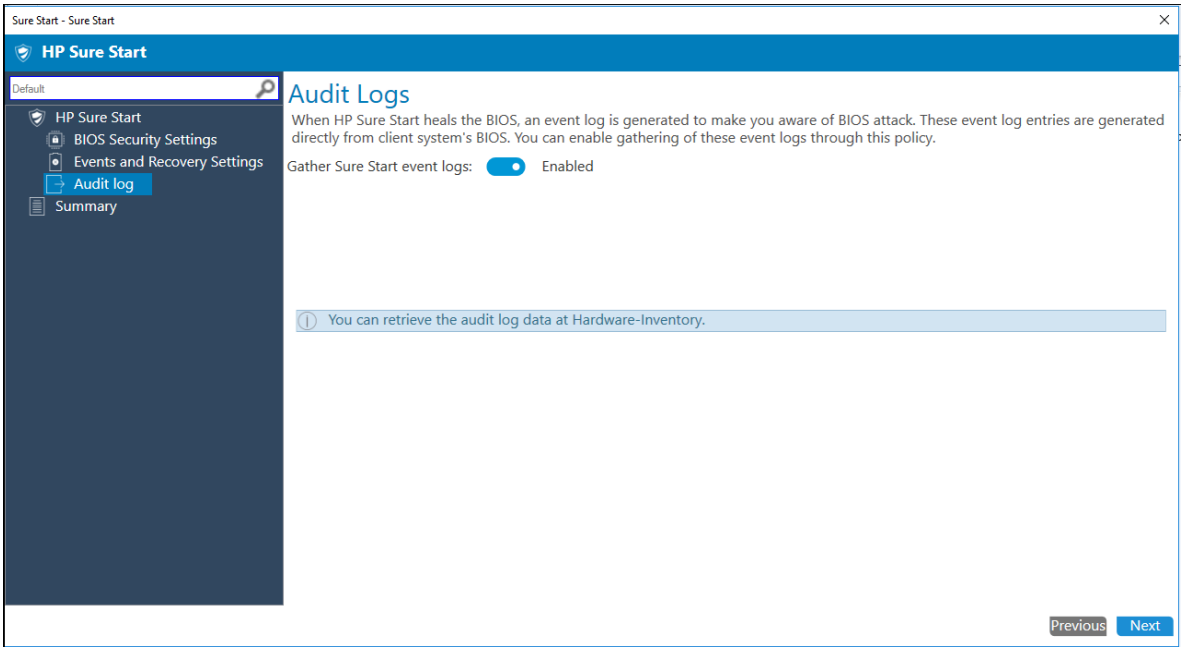
10.4.2 Events and Recovery Settings tab

These setting control HP Sure Start behavior after a critical security event, such as the BIOS being attacked or corrupted, is identified.

- 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 the Esc+Windows+Up Arrow+Down Arrow key combination is pressed. 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.



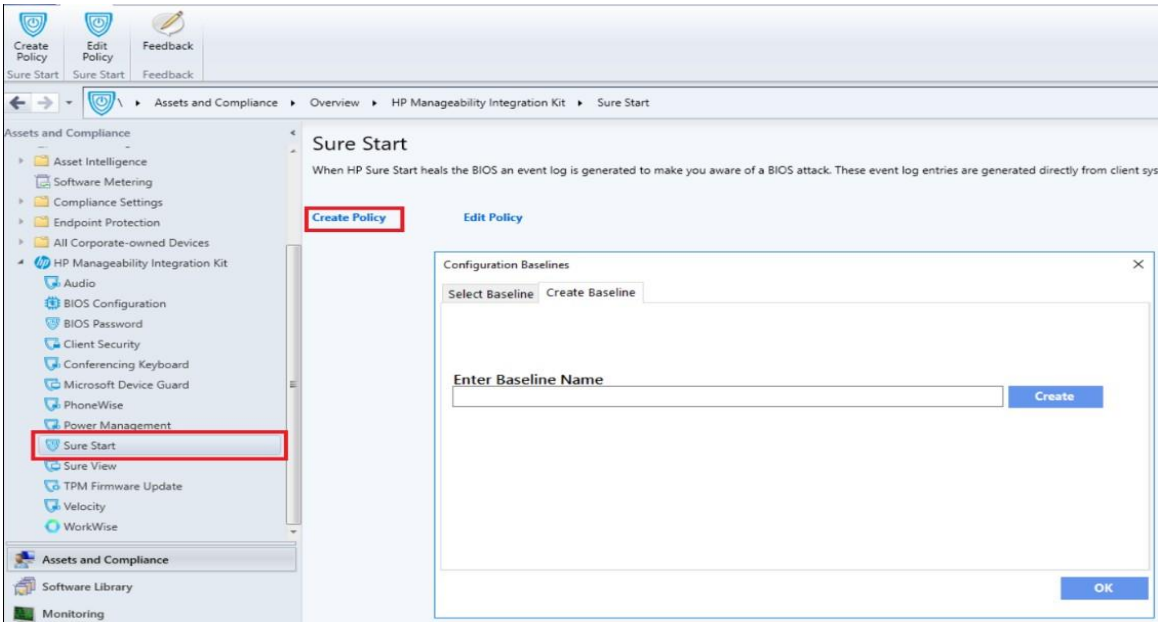
10.4.3 Audit Log tab



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

10.5 Creating a policy

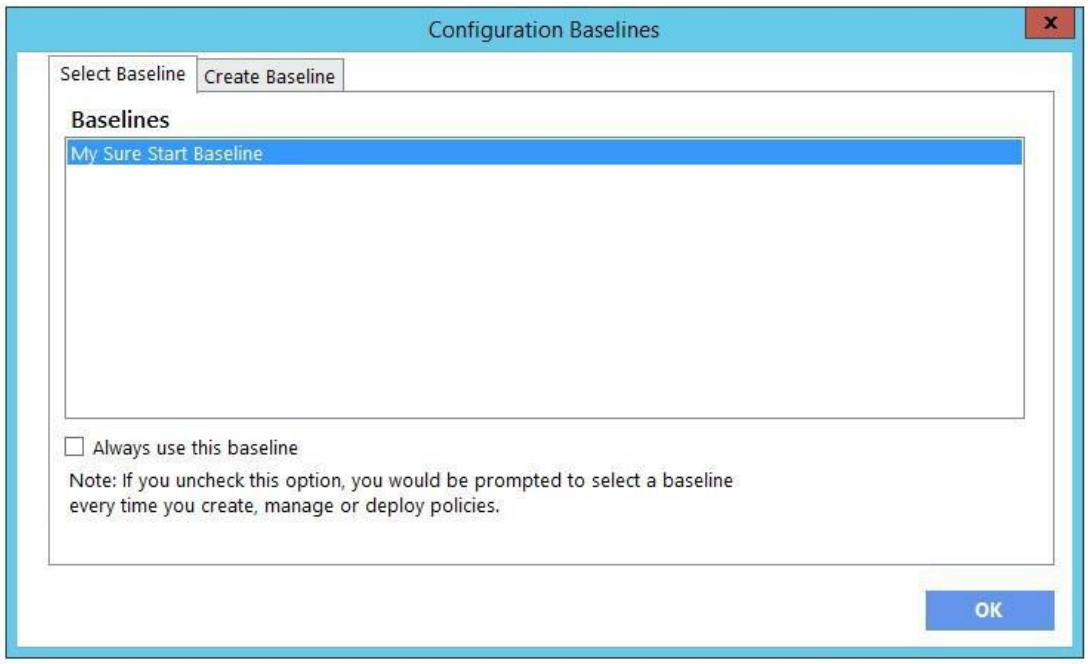
1. In Configuration Manager, select Assets and Compliance, and then select Overview.
2. Select HP Manageability Integration Kit, right-click Sure Start, and then select Create Policy.
3. Enter a Baseline name, and then select Start Policy.



4. Modify the settings, and then click Next.
5. Review the Summary page. If changes are necessary, select the Previous button; 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.

10.6 Editing a policy

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 to edit and select OK to continue the wizard.
4. Complete the procedure for steps 4 through 6 in Creating a policy.

10.7 Additional information

Not all features are supported on all systems.

Certain systems might require a manual action to restart after a configuration change.

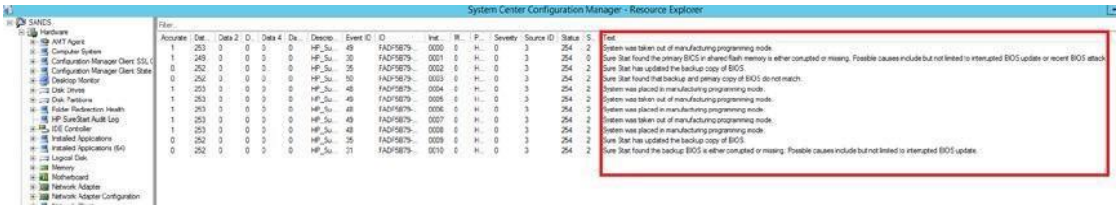
10.7.1 Audit logs

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, select Overview, and then select Devices.
2. Right-click a device, select Start, and then select Resource Explorer.
3. Select Hardware, and then select HP Sure Start Audit Logs.



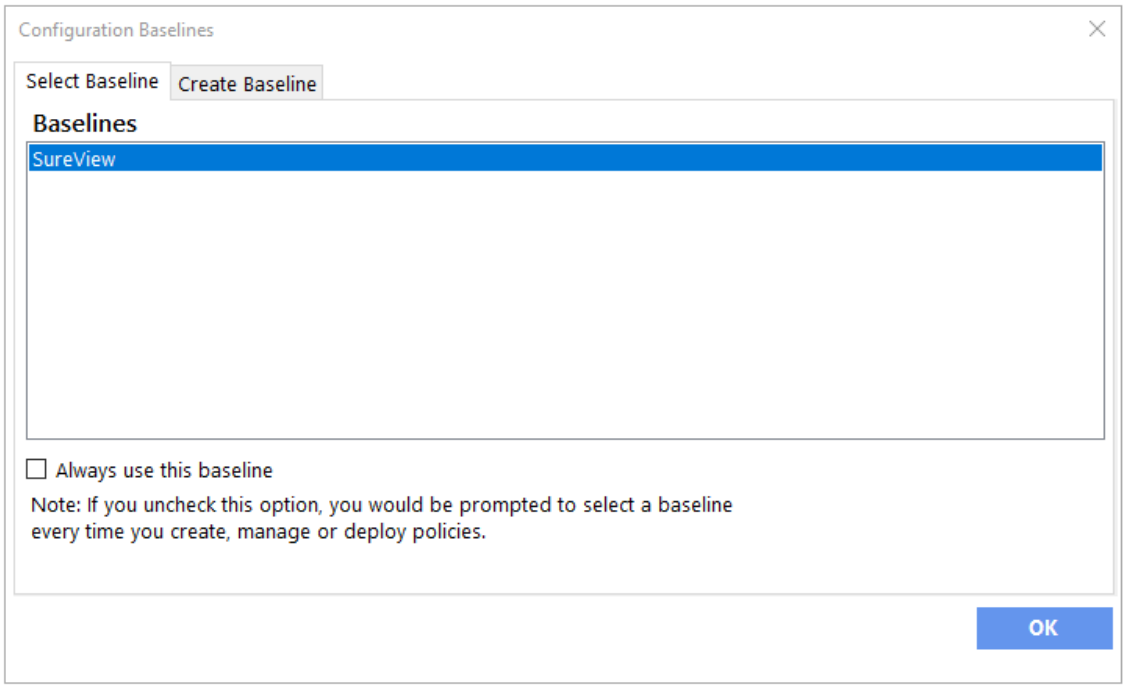
11 HP Sure View

11.1 Overview

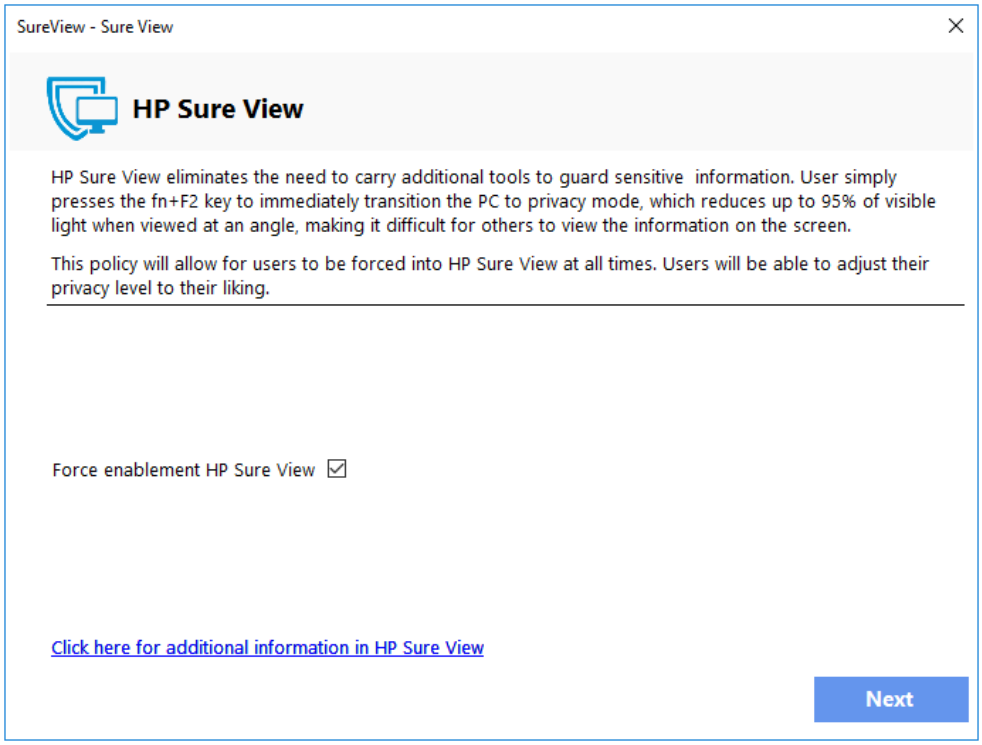
HP Sure View eliminates the need to carry additional tools to guard sensitive information. Users simply press the fn+F2 key to immediately transition the PC to privacy mode, which reduces up to 95 percent of visible light when viewed at an angle, making it difficult for others to view information on the screen.

11.2 Creating a policy

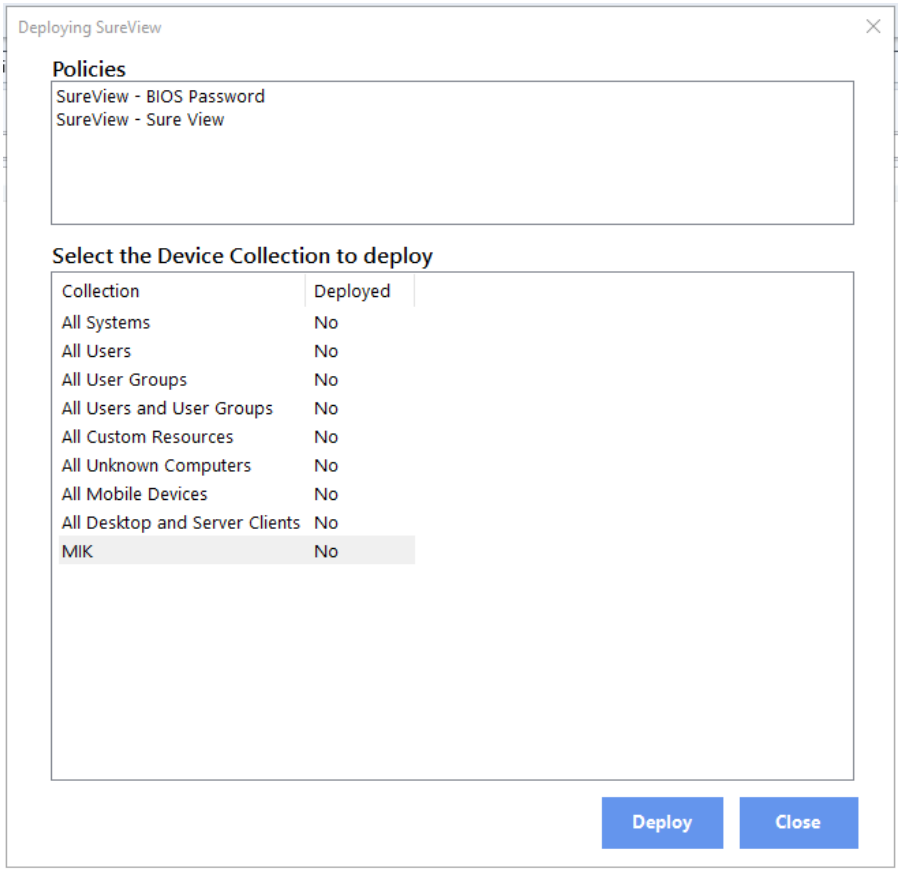
1. In Configuration Manager, select Assets and Compliance, and then select Overview.



2. Select HP Manageability Integration Kit, right-click SureView, and then select Create Baseline.
3. Enter a Baseline name, and then click 'OK' to save the Baseline with that name.
4. HP Sure View will be enabled by default.



5. Click ‘Next’ and save the policy. Then select the collection the policy should be applied to.



6. Click ‘Deploy’ to apply the policy to the client systems within the collection.

11.3 Editing a policy

1. In Configuration Manager, select the policy you want to edit.

2. Select HP Manageability Integration Kit, right-click SureView, and then select Edit Policy.
3. Make any necessary changes, and then click 'OK' to save the policy with that name.

12 TPM Firmware Update

The TPM firmware update policy helps perform the following actions:

- Upgrading to TPM 2.0

12.1 Supported client platforms

12.1.1 Desktop computers:

- HP EliteDesk 705 G2 Desktop Mini PC
- HP EliteDesk 800 35W G2 Desktop Mini PC
- HP EliteDesk 800 65W G2 Desktop Mini PC
- HP EliteDesk 800 G2 Small Form Factor PC
- HP EliteDesk 800 G2 Tower PC
- HP EliteOne 800 G2 23-inch Non-Touch All-in-One PC
- HP EliteOne 800 G2 23-inch Touch All-in-One PC
- HP ProDesk 400 G2 Desktop Mini PC
- HP ProDesk 400 G3 Microtower PC
- HP ProDesk 400 G3 Small Form Factor PC
- HP ProDesk 480 G3 Microtower PC
- HP ProDesk 490 G3 Microtower PC
- HP ProDesk 498 G3 Microtower PC
- HP ProDesk 600 G2 Desktop Mini PC
- HP ProDesk 600 G2 Microtower PC
- HP ProDesk 600 G2 Small Form Factor PC
- HP ProOne 400 G2 20-inch Non-Touch All-in-One PC
- HP ProOne 400 G2 20-inch Touch All-in-One PC
- HP ProOne 600 G1 All-in-One PC
- HP ProOne 600 G2 21.5-inch Non-Touch All-in-One PC
- HP RP9 G1 Retail System Model 9015
- HP RP9 G1 Retail System Model 9018

12.1.2 Notebook computers:

- HP EliteBook 1030 G1 Notebook PC
- HP EliteBook 1040 G3 Notebook PC

- HP EliteBook 725 G3 Notebook PC
- HP EliteBook 745 G3 Notebook PC
- HP EliteBook 755 G3 Notebook PC
- HP EliteBook 820 G3 Notebook PC
- HP EliteBook 840 G3 Notebook PC
- HP EliteBook 850 G3 Notebook PC
- HP EliteBook Folio G1 Notebook PC
- HP Elite x2 1012 G1
- HP ProBook 430 G3 Notebook PC
- HP ProBook 440 G3 Notebook PC
- HP ProBook 450 G3 Notebook PC
- HP ProBook 455 G3 Notebook PC
- HP ProBook 470 G3 Notebook PC
- HP ProBook 640 G2 Notebook PC
- HP ProBook 645 G2 Notebook PC
- HP ProBook 650 G2 Notebook PC
- HP ProBook 655 G2 Notebook PC
- HP ZBook 15 G3 Mobile Workstation
- HP ZBook 17 G3 Mobile Workstation
- HP ZBook Studio G3 Mobile Workstation

12.2 Supported client operating systems

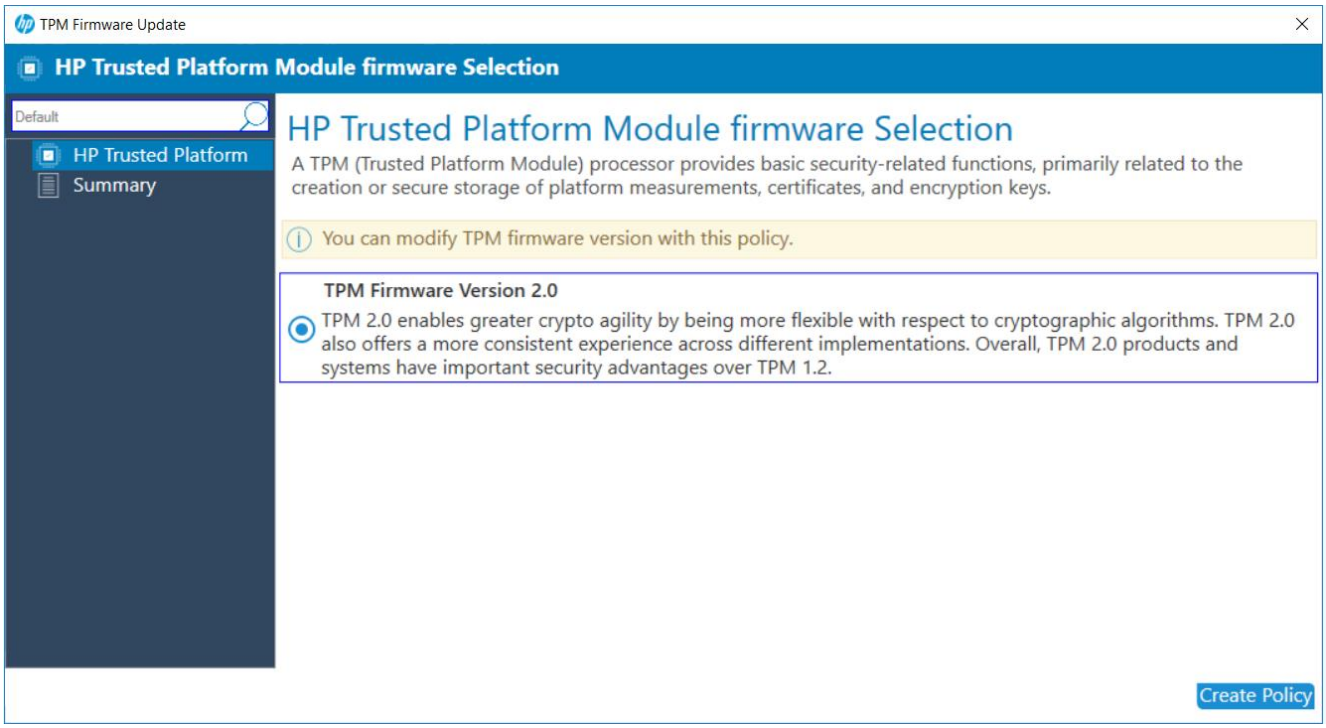
- Windows 10
- Windows 8.1
- Windows 7 (TPM 1.2 only)

12.3 Other client system prerequisites

- Infineon SLB9670 TPM chip
- Latest commercial BIOS
- Microsoft .NET Framework 4.0 or higher.
- HP MIK

12.4 Creating a policy

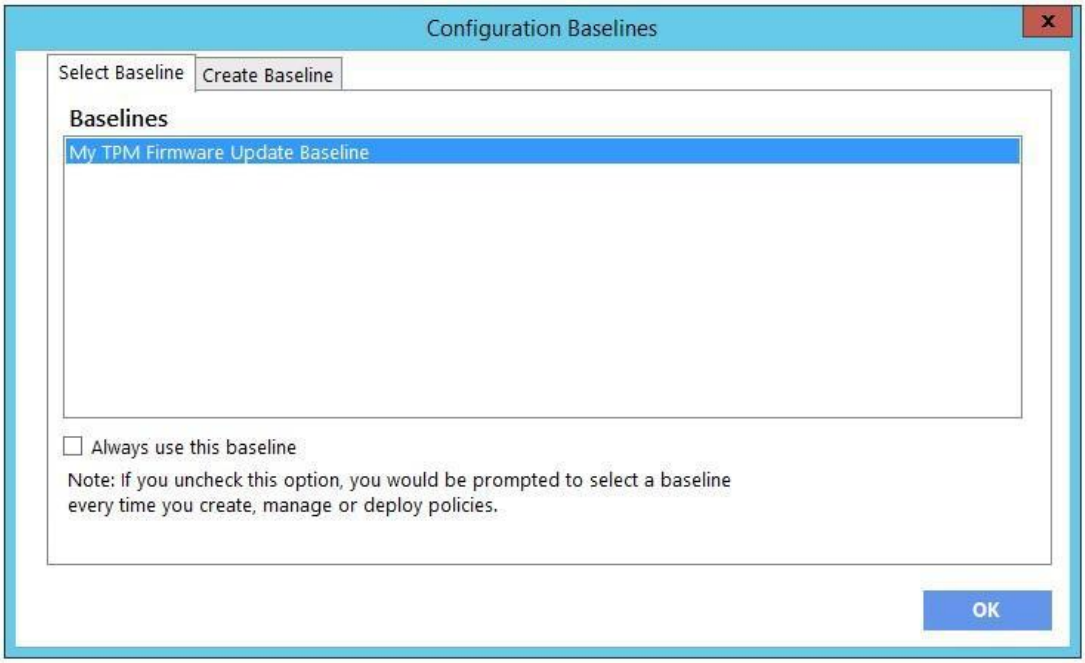
1. In Configuration Manager, select Assets and Compliance, and then select Overview.
2. Select HP Manageability Integration Kit, right-click TPM Firmware Update, and then select Create Policy.
3. Enter a Baseline name, and then follow the on-screen instructions to complete the wizard.
4. Select the target TPM version, and then select Create Policy. See Additional information for warnings and limitations.



5. Review the Summary page. If changes are necessary, select the Previous button; 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.

12.5 Editing a policy

1. In Configuration Manager, select Assets and Compliance, and then select Overview.
2. Select 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. Complete the procedure for steps 4 through 6 in Creating a policy.

12.6 Additional information

WARNING!
To avoid a complete loss of data, the primary drive must be in a decrypted state before pushing this policy. The policy has a built-in check for BitLocker and WinMagic disk encryption solutions only. If BitLocker or WinMagic drive encryption is used, the policy exits with an appropriate error code logged. The policy does not detect other disk encryption solutions.

TPM can be updated to TPM 2.0 up to a maximum of 64 times.

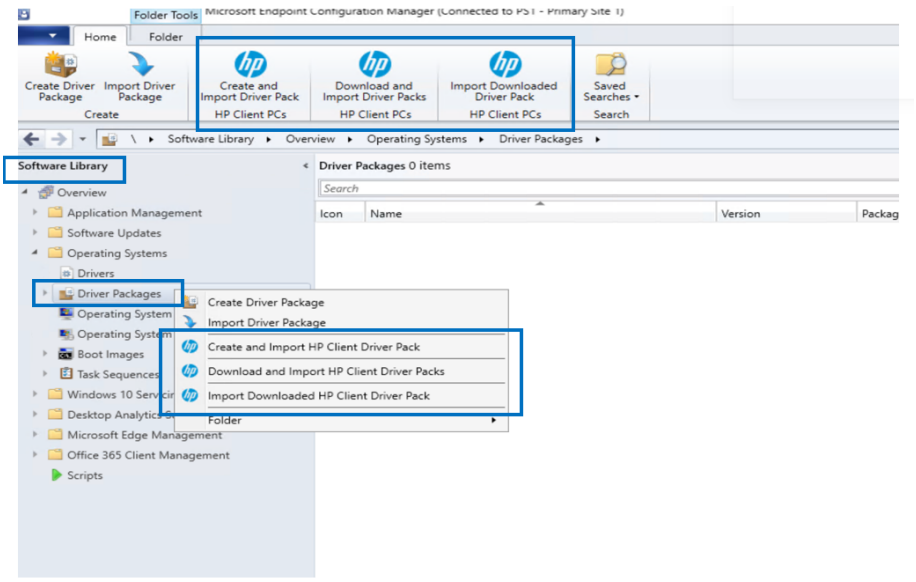
Converting TPM involves potentially upgrading to a newer TPM firmware. The following rules govern this operation:

- If the system has TPM 1.2 and the target is TMP 2.0, TPM 2.0 is enabled and upgraded with the latest firmware version.
- If the system has TPM 2.0 and the target is TPM 2.0, TPM 2.0 is upgraded to the latest firmware version.
- This procedure requires a manual action to complete the reboot.

13 HP Client Driver Packs

13.1 Operating System (OS) Deployment Overview.

OS Deployment actions will be under Software Library > Operating system > Driver Packages

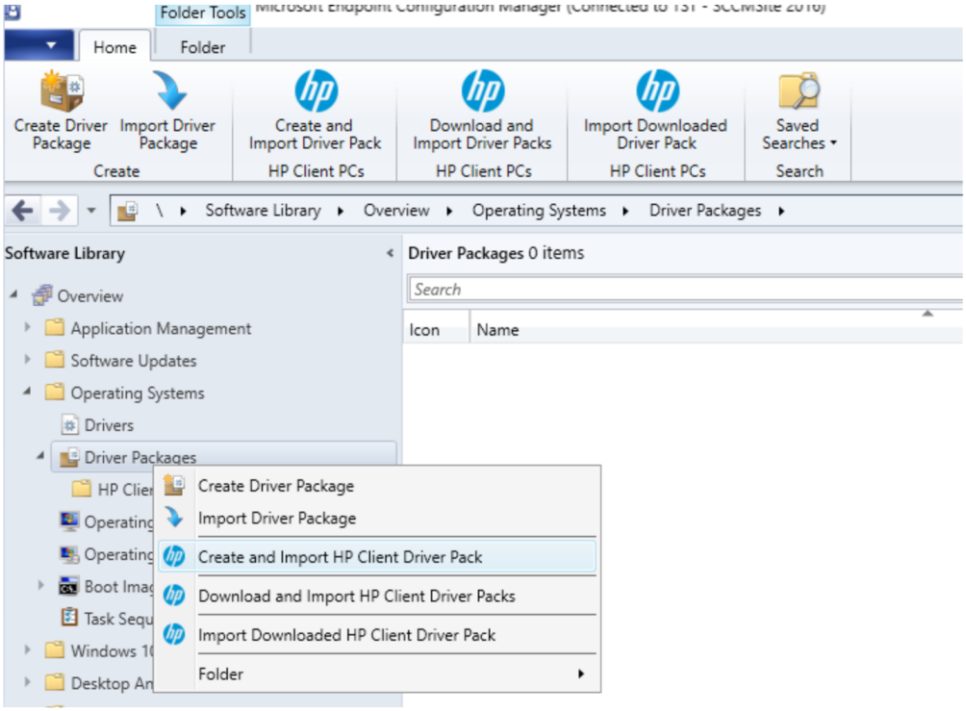


13.2 Create and Import HP Client Driver Pack

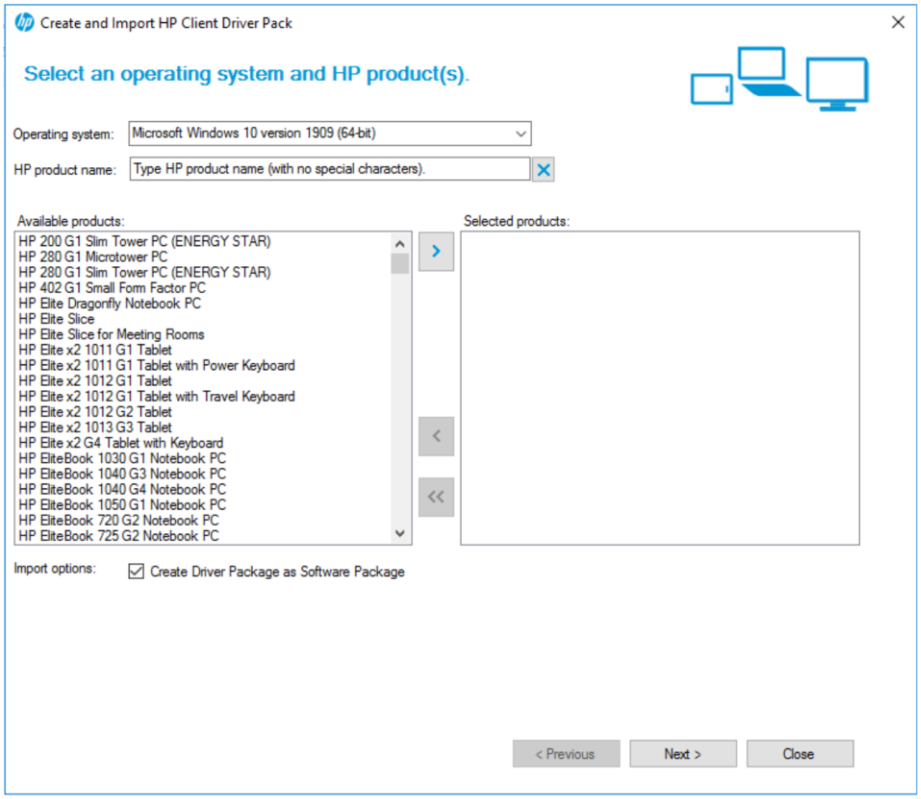
The Create and Import HP Client Driver Pack option displays the drivers for supported HP products. This works similarly to the option previously available with HP CIK.

1. In Configuration Manager, select Software Library, select Overview, select Operating Systems, and then select Driver Packages.

2. Select Create and Import HP Client Driver Pack. The Create and Import HP Client Driver Pack wizard is displayed.



13.2.1 Creating a driver package as a software package.



New–There will now be an option at the bottom of the page that states Import Options. (The box will be checked by default.) By checking the box, it will create driver package as a software package.

3. Select the Operating system.

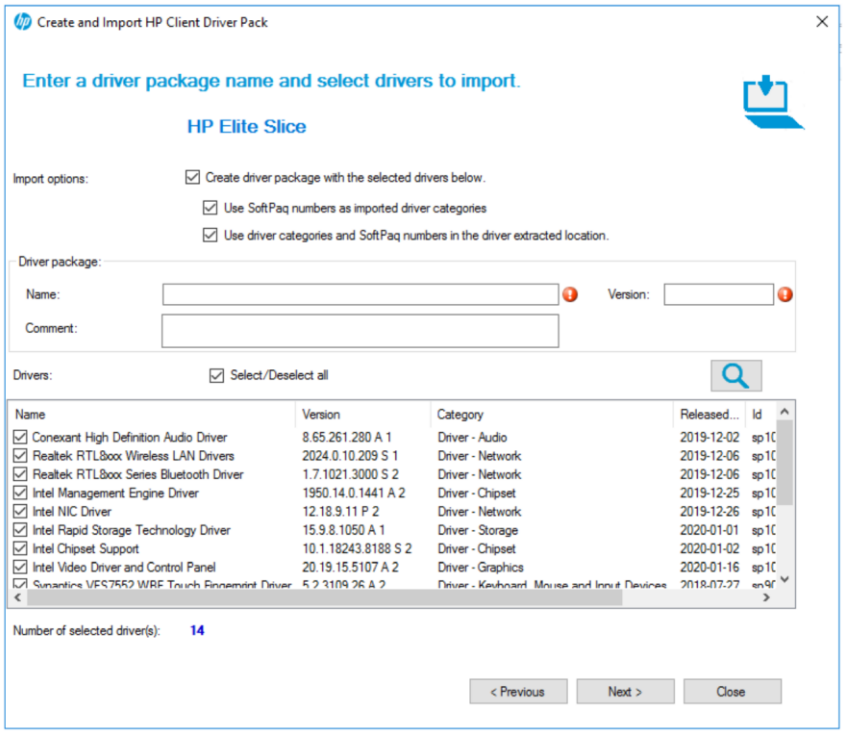
4. Only the products that support driver-pack creation are displayed in the Available products column. Optionally, enter keywords into the HP product name box, and then press Enter to filter the list of available products.

5. Select an available product, and then select the right-arrow button to add the product to the Selected products column.

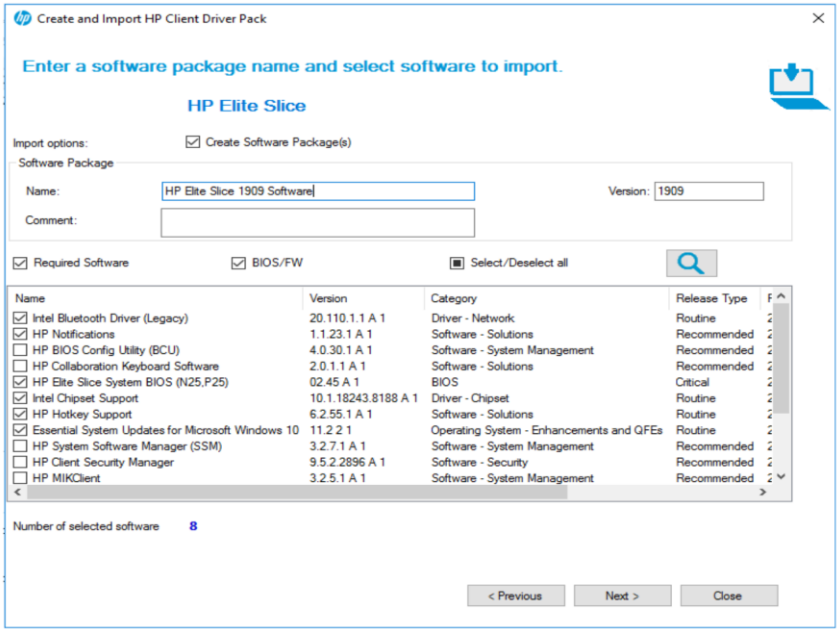
6. Repeat step 5 to select another product, as necessary. HP recommends selecting products of the same family model to create a driver pack with the optimal relevant drivers. Also, HP recommends selecting no more than five products per driver pack.

7. Click Next.

8. Once complete hit next and the second screen of the wizard will appear. At this point there is an ability to name and insert a version to that driver pack.

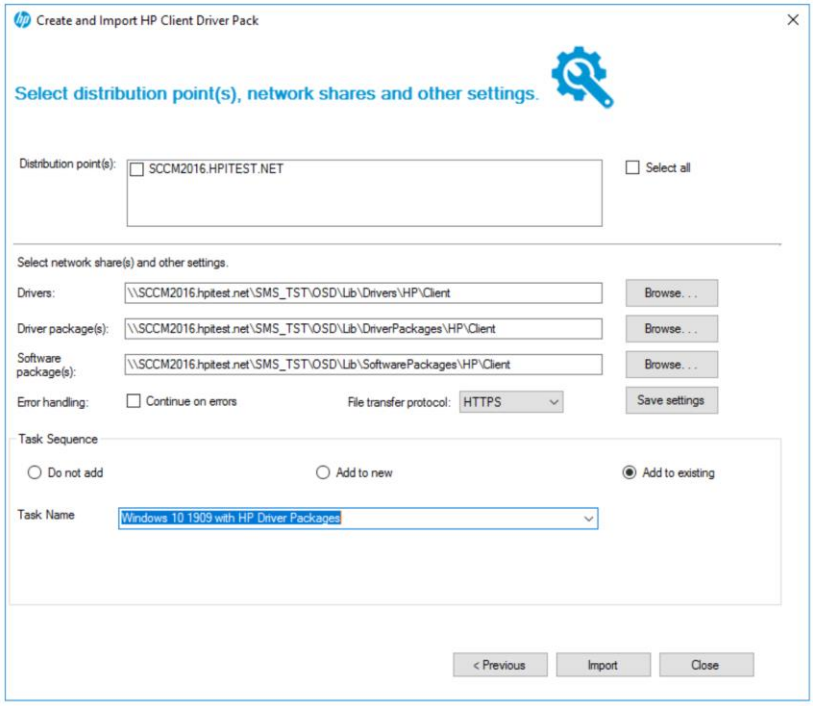


9. Click Next. On the next screen the wizard will prompt the user to pick the additional software they would like.



Notice! This section can be skipped. Skip this section if there is no desire to create a Software package, but just a driver pack. To accomplish this please just unselect the "Create Software Package" box.

10. Select Next.

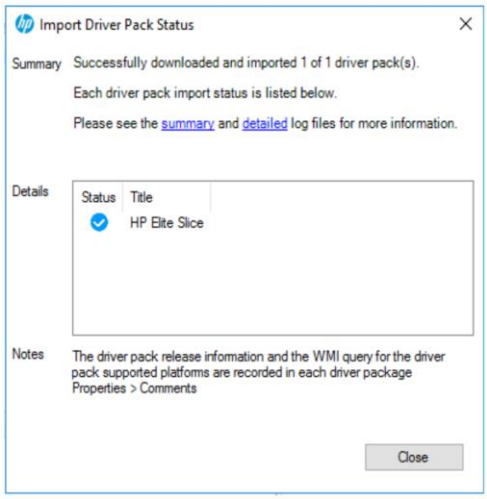


11. If you are creating a driver package, configure the distribution points and network shares as follows:

    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! The user can also create, add, or choose to not add this to a task sequence.
Once the user has successfully added, do not add, or add to existing task sequence 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.

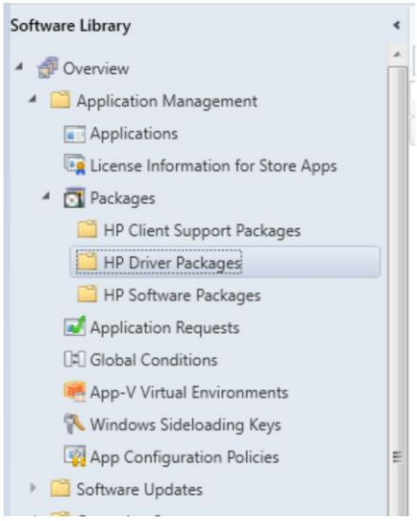
12. Click on ‘Import’, once the Driver Pack is created, following pop-up will be displayed.



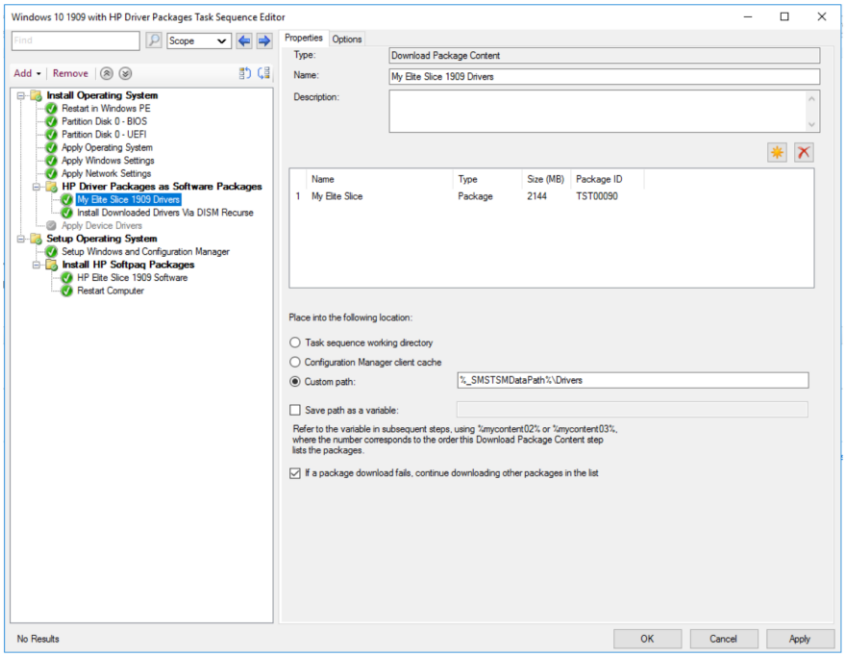
Once completed:

For the Driver Packages:

In Configuration Manager Console, the user can see the new folder ‘HP Driver Packages’ and the created driver package will be listed under this folder.

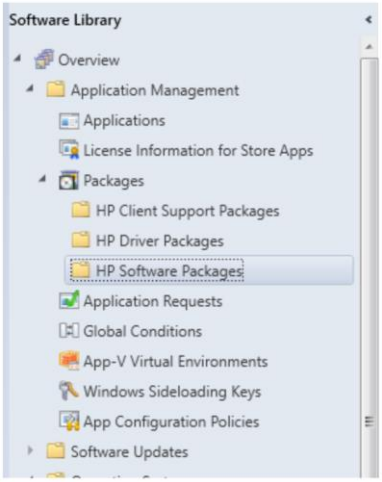


In the selected task sequence, the user can see Created driver package will be added under ‘HP Driver Packages as Software Packages’ folder.

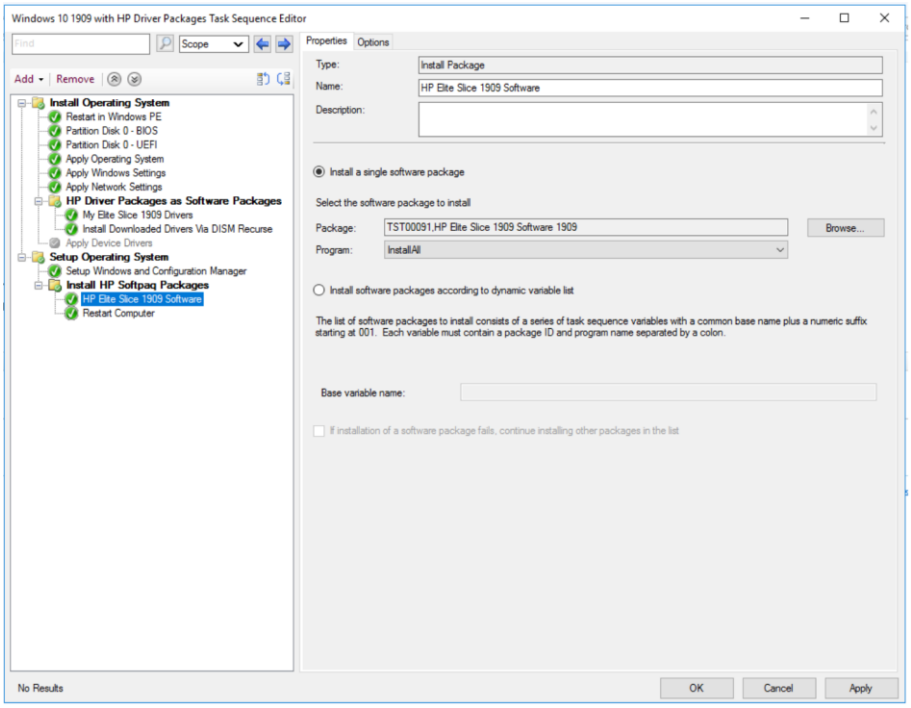


For the software package:

In Configuration Manager Console, the user can see the new folder 'HP Software Packages' and the created driver package will be listed under this folder.

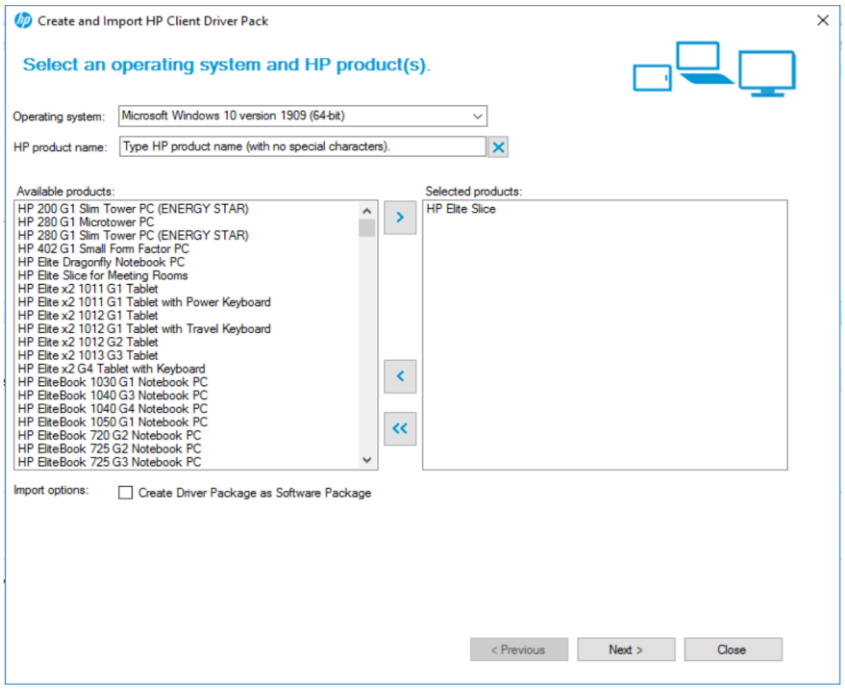


In the selected task sequence, the user can see Created software package will be added under 'Install HP Softpaq Packages' folder.



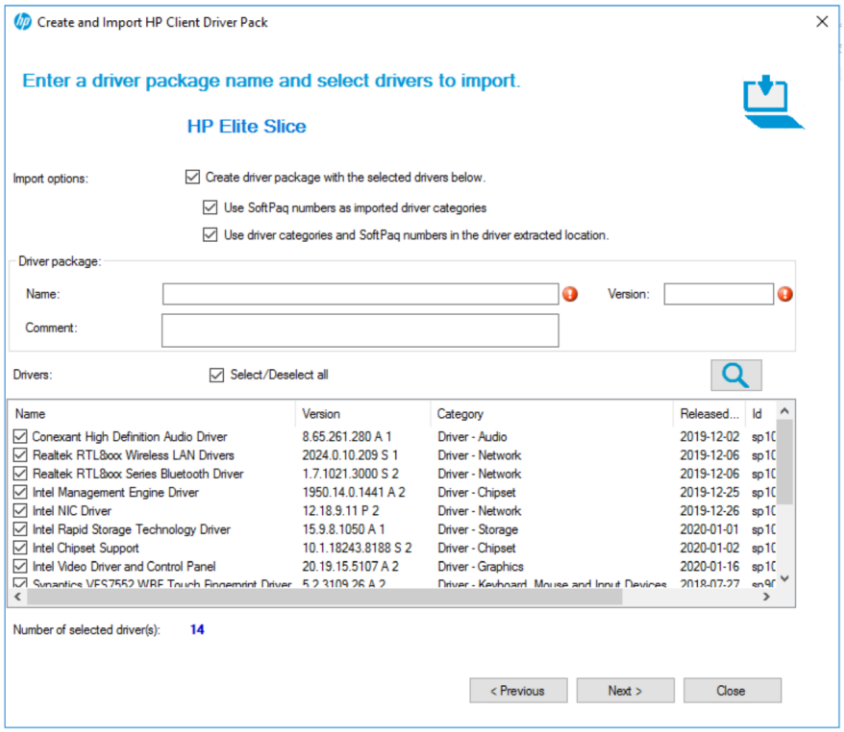
13.2.2Creating a driver package not as a software package.

Select Operating System and HP Products from available list.
New-There will now be an option at the bottom of the page that states Import Options. (The box will be checked by default.) user needs to uncheck the box “Create Driver Package as Software Package.”



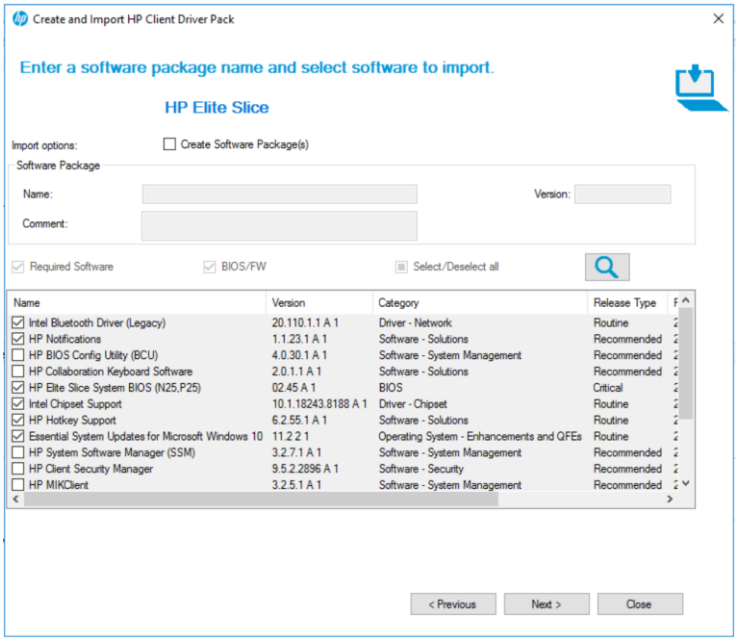
Select Operating System and HP Products from available list.

Once complete hit next and the second screen of the wizard will appear. At this point there is an ability to name and insert a version to that driver pack.



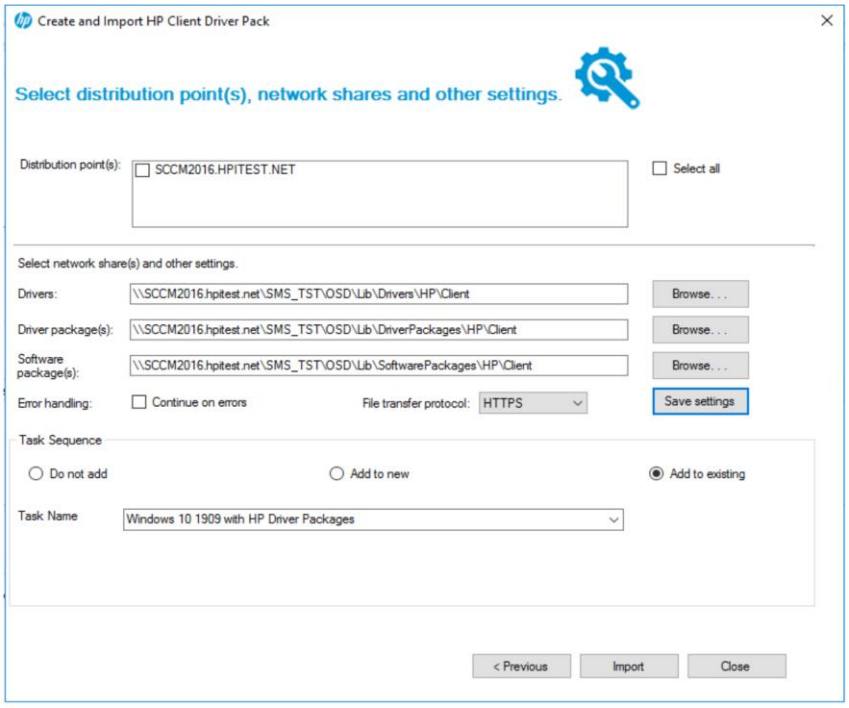
Once the user hits next, the user will be promoted to pick the software they'd like to add.

Notice! This is where the user can skip this section if they are not wanting to create a software package, but just a driver pack. To accomplish this please just unselect the "Create Software Package" box.



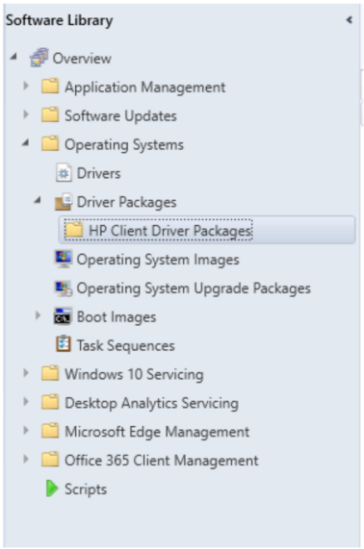
Once the user clicks on Next, the last page of the wizard will appear.

Notice! On this page the user will select the distribution points, and can also create, add, or choose to not add this to a task sequence.

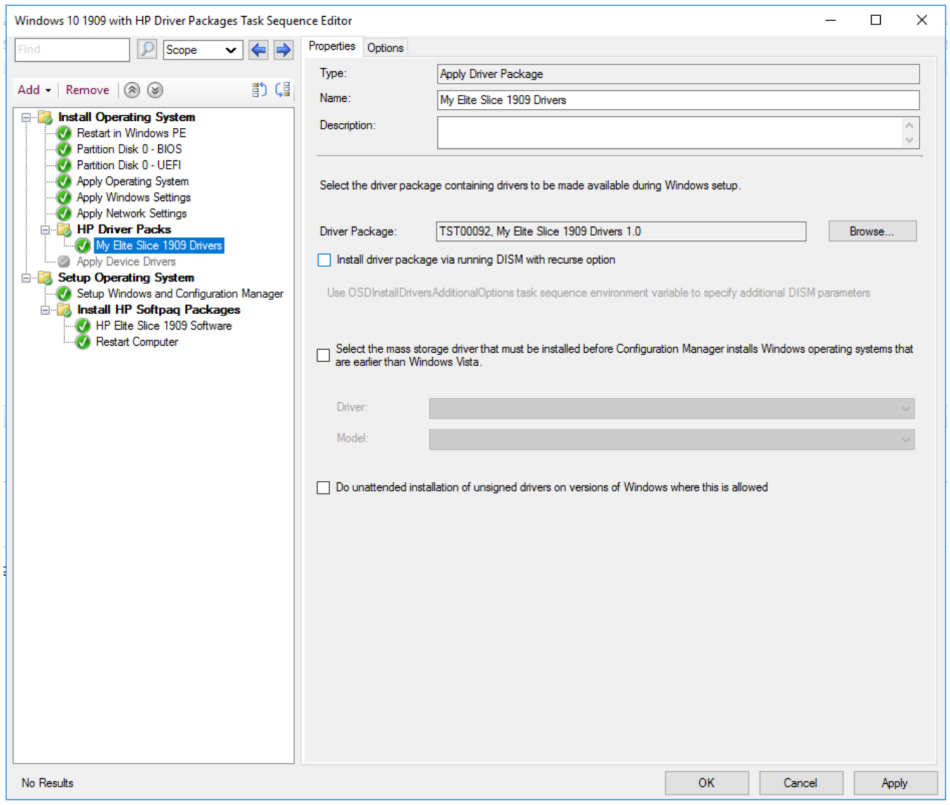


Select Import.

Once completed:
In the configuration manager console, Created Driver Package will be listed under 'HP Client Driver Packages' folder

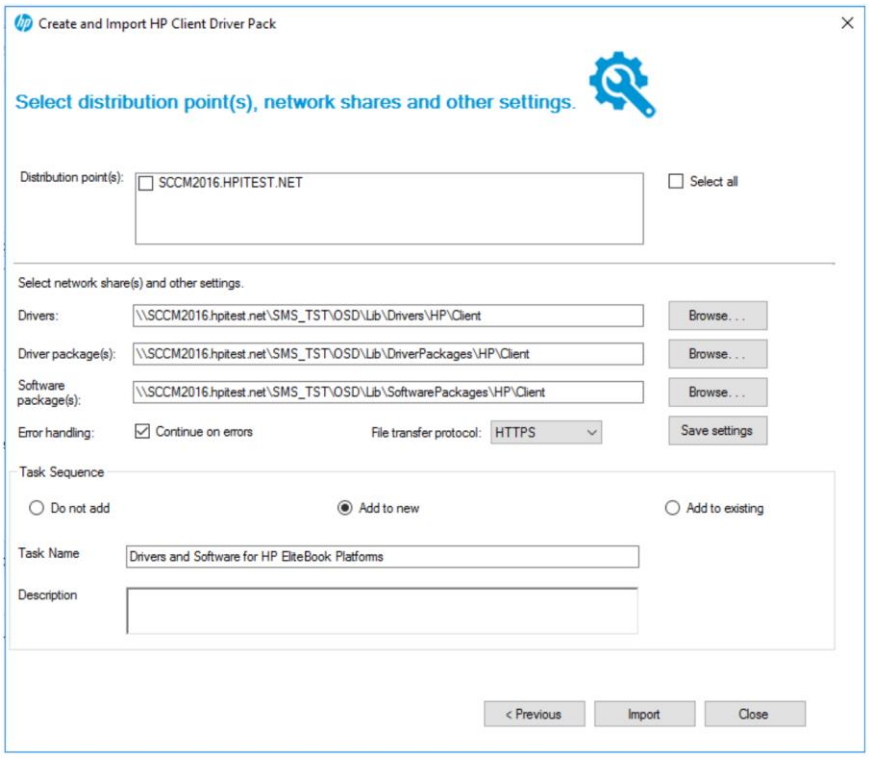


In the selected task sequence, Created Driver Package will be listed under 'HP Driver Packs' folder.


Windows 10 1909 with HP Driver Packages Task Sequence Editor
Find
Scope
Add
Remove
Install Operating System
Restart in Windows PE
Partition Disk 0 - BIOS
Partition Disk 0 - UEFI
Apply Operating System
Apply Windows Settings
Apply Network Settings
HP Driver Packs
My Elite Slice 1909 Drivers
Apply Device Drivers
Setup Operating System
Setup Windows and Configuration Manager
Install HP Softpaq Packages
HP Elite Slice 1909 Software
Restart Computer
Properties
Options
Type:
Apply Driver Package
Name:
My Elite Slice 1909 Drivers
Description:
Select the driver package containing drivers to be made available during Windows setup.
Driver Package:
TST00092, My Elite Slice 1909 Drivers 1.0
Browse...
Install driver package via running DISM with recurse option
Use OSDInstallDriversAdditionalOptions task sequence environment variable to specify additional DISM parameters
Select the mass storage driver that must be installed before Configuration Manager installs Windows operating systems that are earlier than Windows Vista.
Driver:
Model:
Do unattended installation of unsigned drivers on versions of Windows where this is allowed
No Results
OK
Cancel
Apply

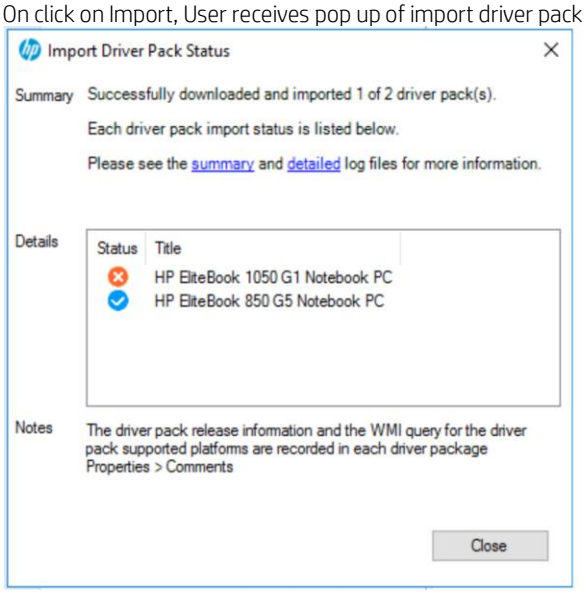
13.2.3 Create and Import HP Client Driver Pack – Option – Continue on errors

Note in the Final step of Create and Import Drivers Pack user has the option to select “continue on error”.



If **“Continue on error”** checkbox 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 will not be created.

On click on Import, User receives pop up of import driver pack status.

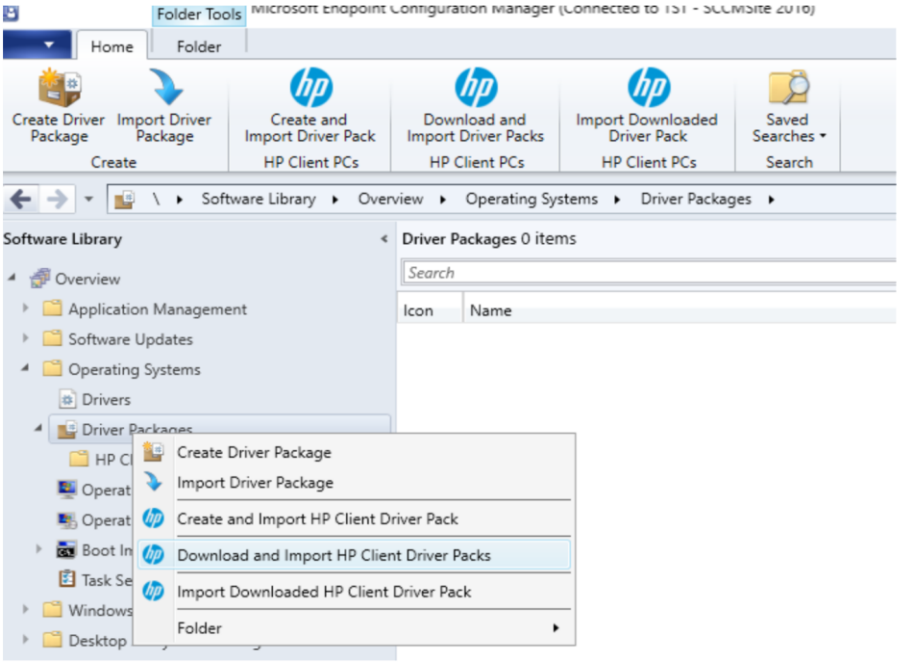


User can click on Summary and details logs to review any failures.

13.3 Download and Import Driver Packs

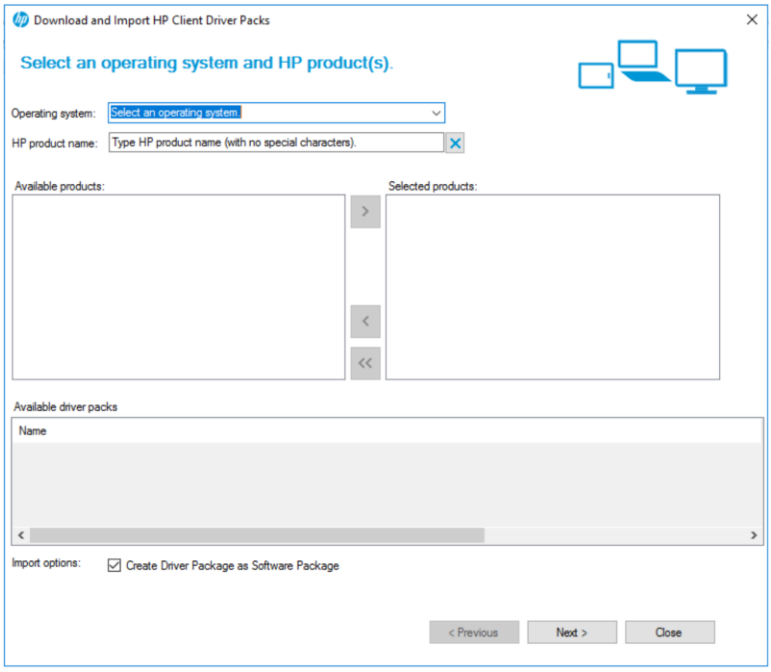
1. In Configuration Manager, select Software Library, select Overview, select Operating Systems, and then select Driver Packages.

2. Select Create and Import HP Client Driver Pack. The Download and Import HP Client Driver Pack wizard is displayed.



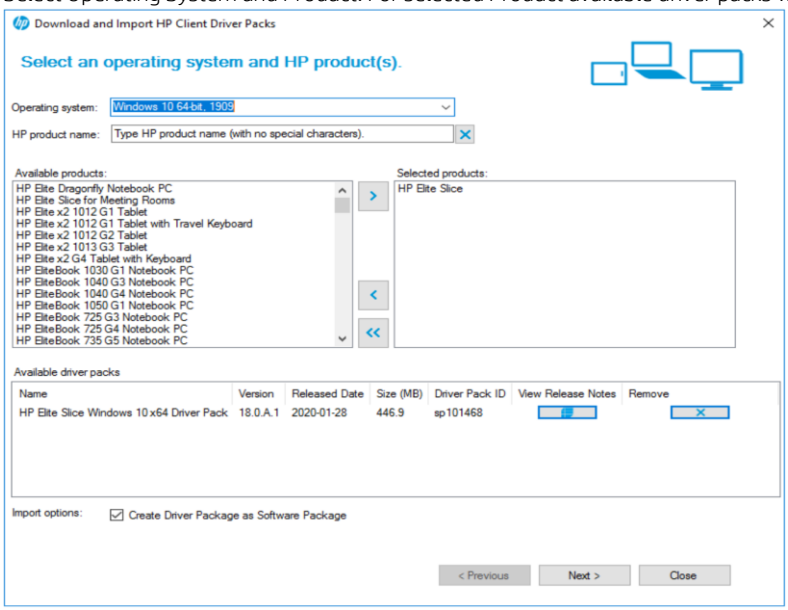
3. Select Download and Import HP Client Driver Packs.

13.3.1Download and Import Driver Packs as a software package.



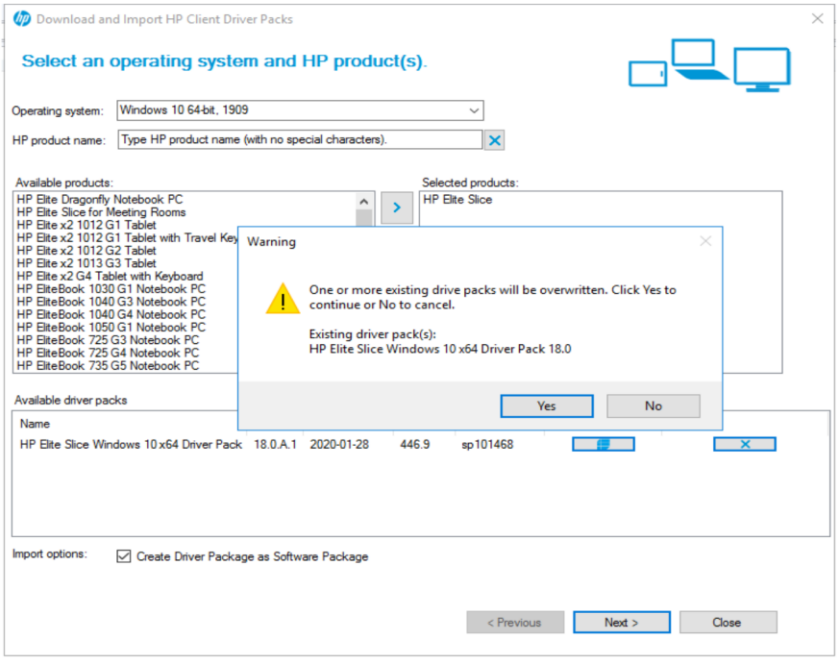
Notice! Create Driver Package as Software Package is now an option at the bottom. Default setting will be checked as shown in the screenshot below.

Select Operating System and Product. For selected Product available driver packs will be listed. Example below.

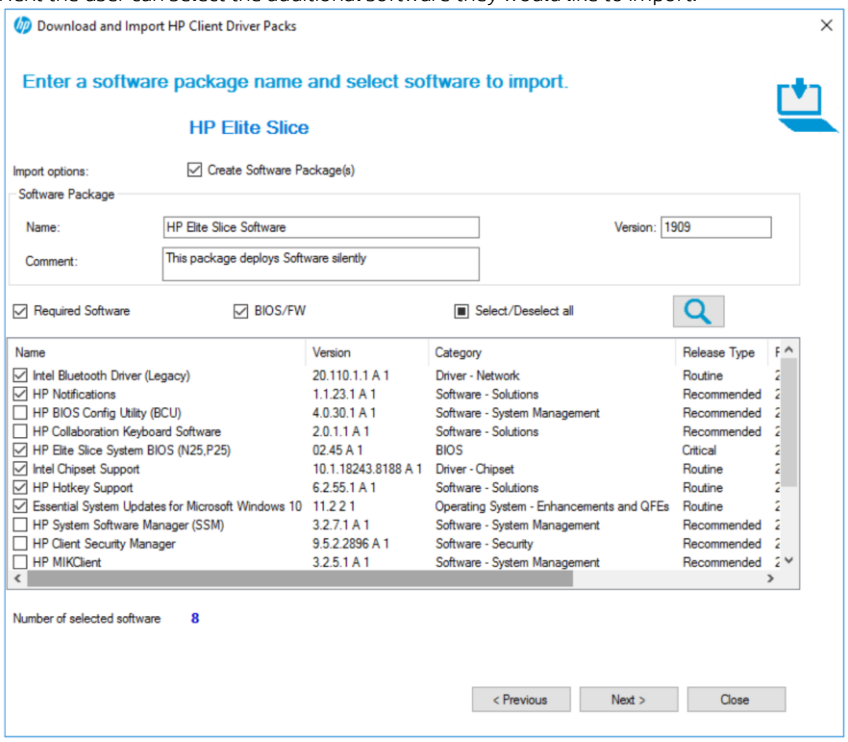


Once the user clicks on Next, they will be prompted to the next screen.

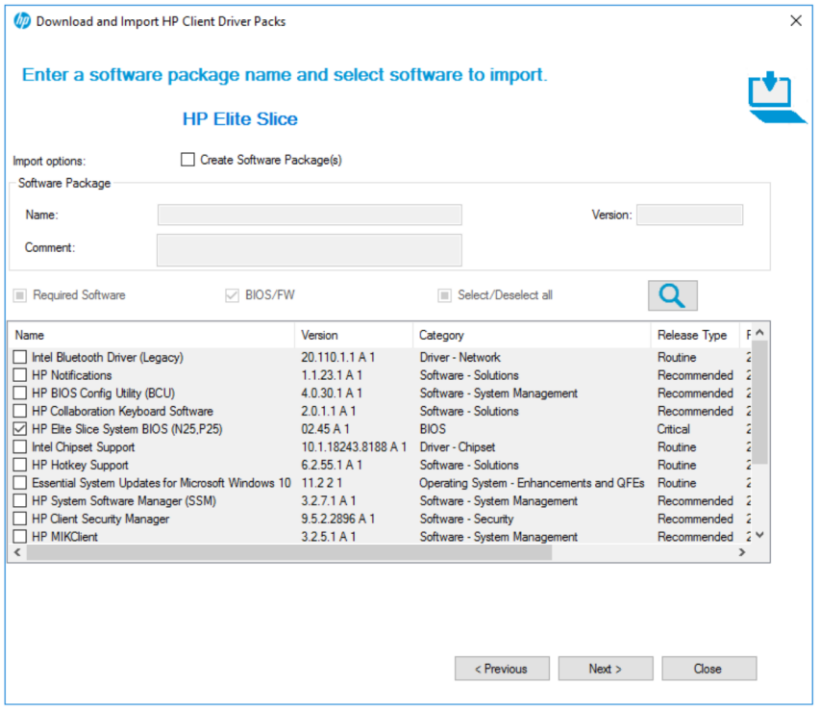
Notice! If one or more of the driver pack(s) has been previous imported it will prompt a message identifying the existing driver pack will be overwritten. See screenshot below.



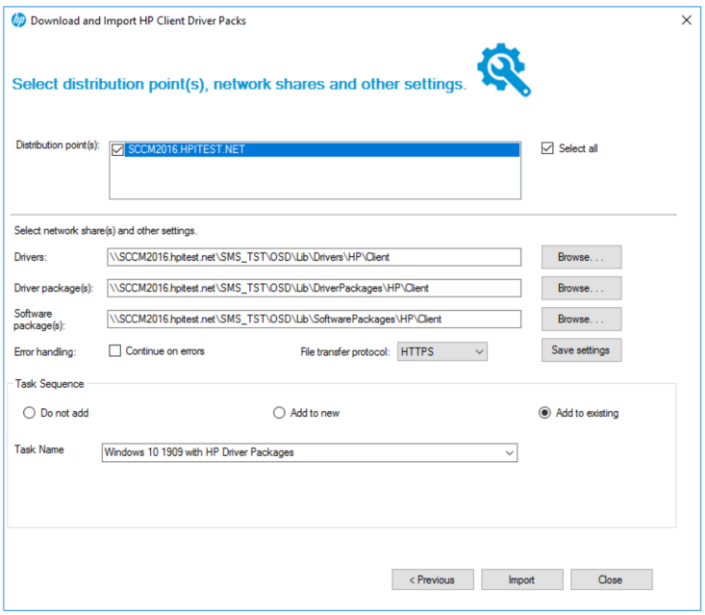
Next the user can select the additional software they would like to import.



Notice! This is the same screen. At this point the user can uncheck the box below if the user does not want to create the software package.

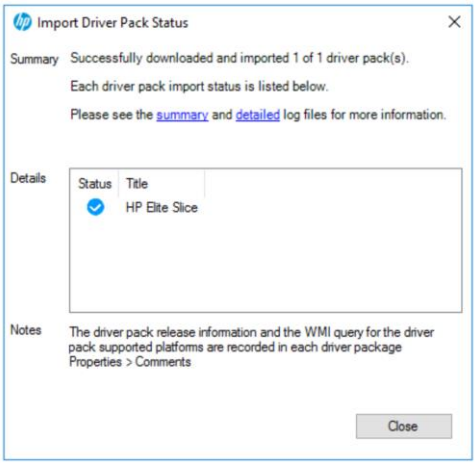


Once the user hits Next, they will be promoted to the last page of the wizard.
Notice! The user will select their distribution points, and can also create, add, or choose to not add this to a task sequence.



Note! The user can also create, add, or choose to not add this to a task sequence.
Once the user has successfully added, do not add, or add to existing task sequence 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.

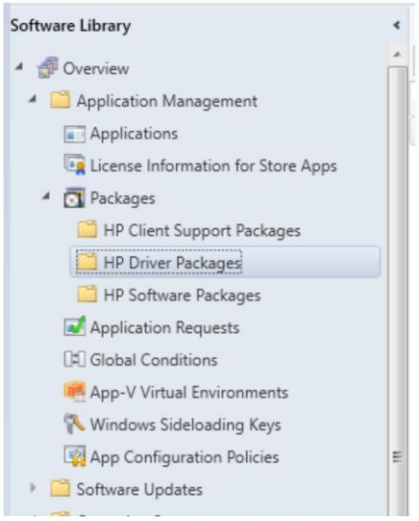
On click on Import, User receives pop up of import driver pack status.



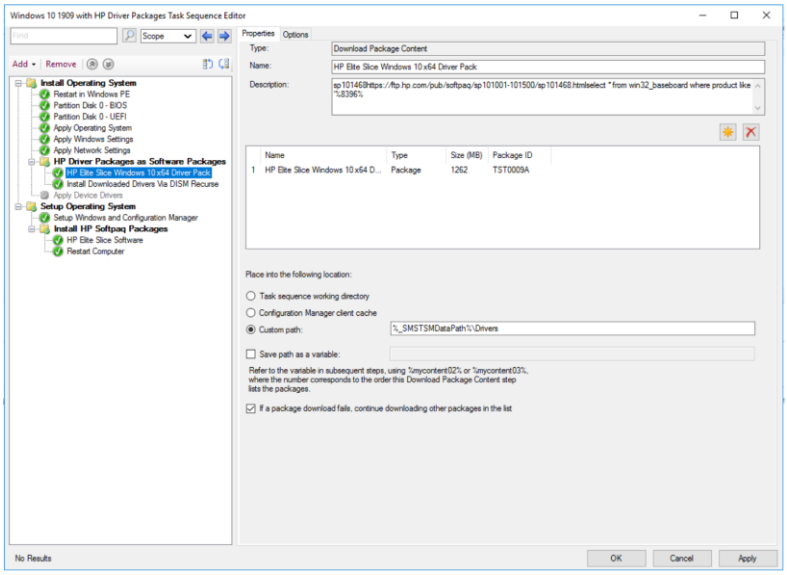
Once completed:

For the Driver Package:

In Configuration Manager Console, the user can see the new folder 'HP Driver Packages' and the created driver package will be listed under this folder.

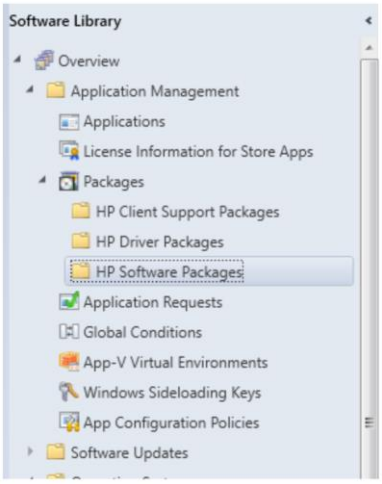


In the selected task sequence, the user can see Created driver package will be added under 'HP Driver Packages as Software Packages' folder.

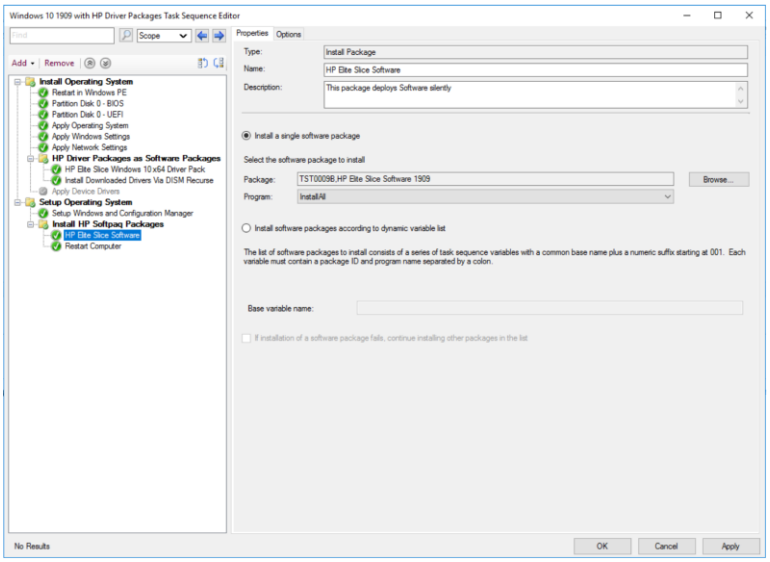


For the software package:

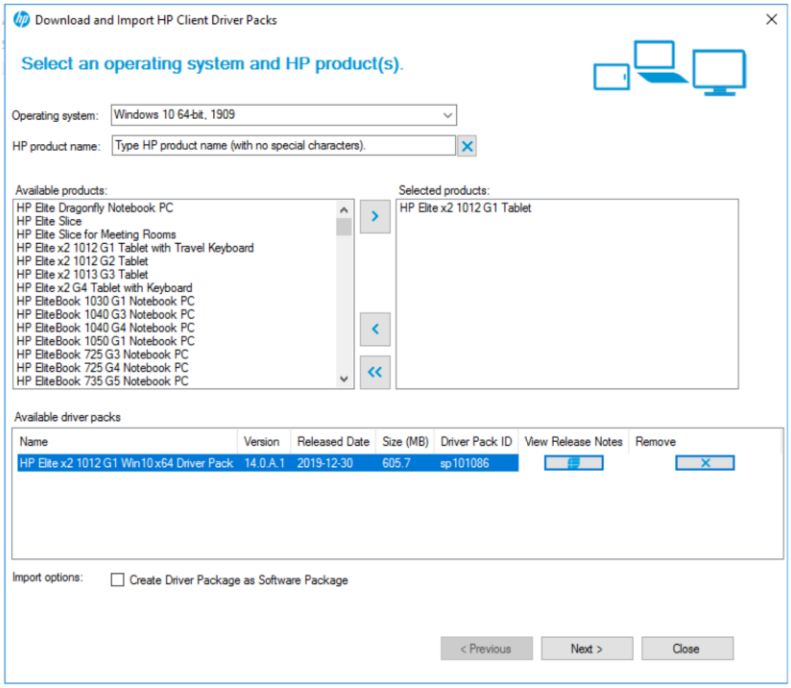
In Configuration Manager Console, the user can see the new folder 'HP Software Packages' and the created driver package will be listed under this folder.



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

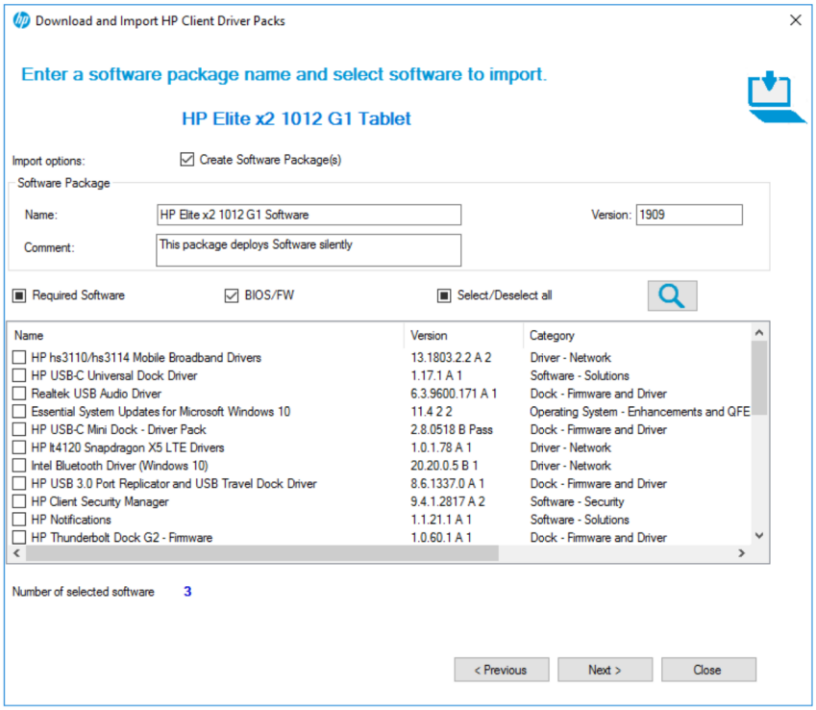


13.3.2Download and Import Driver Packs not as a software package.

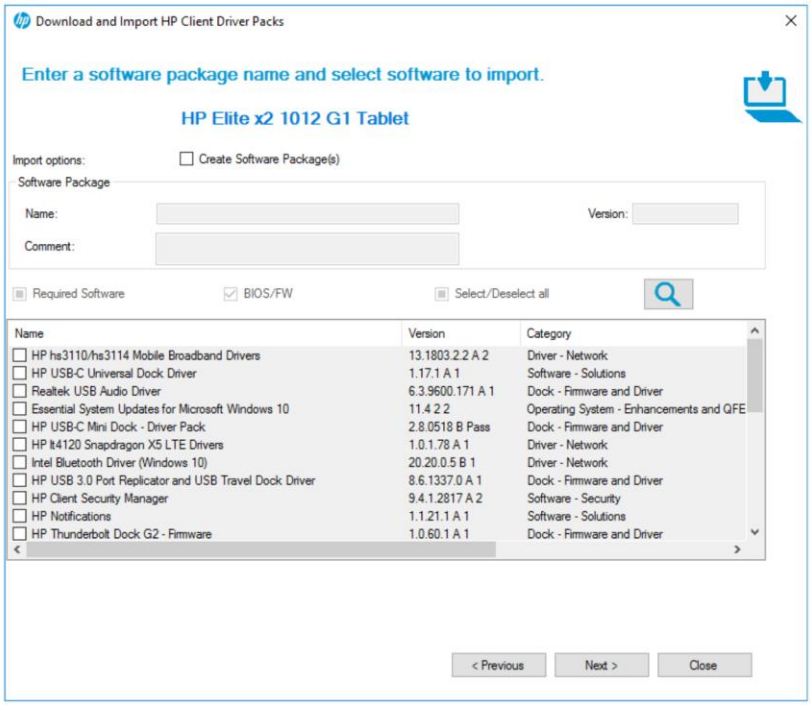


Unselect “Create Driver Package as Software Package” checkbox and click Next

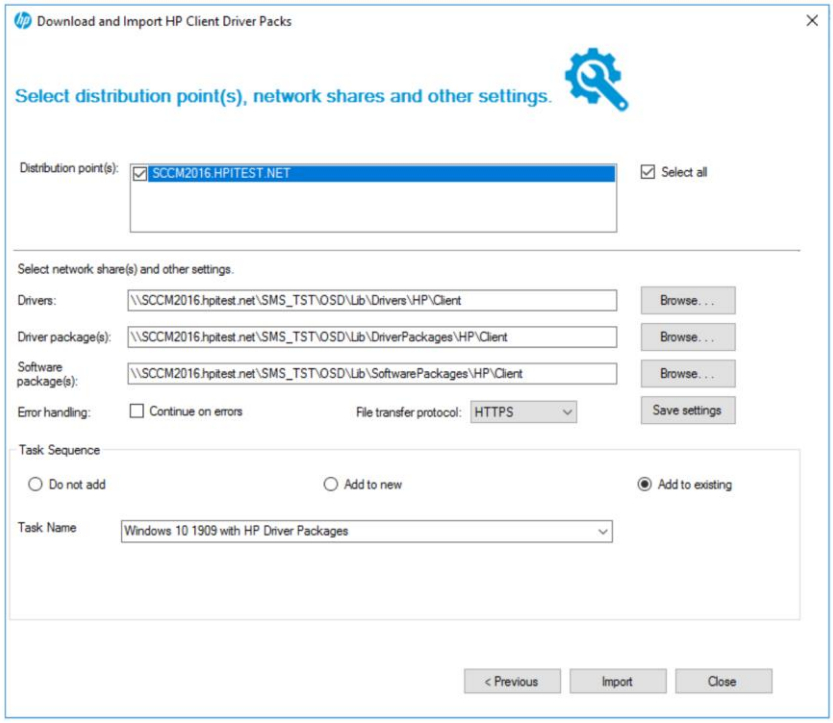
User can select the software to create software package by providing the name and version of the software package the user will create.



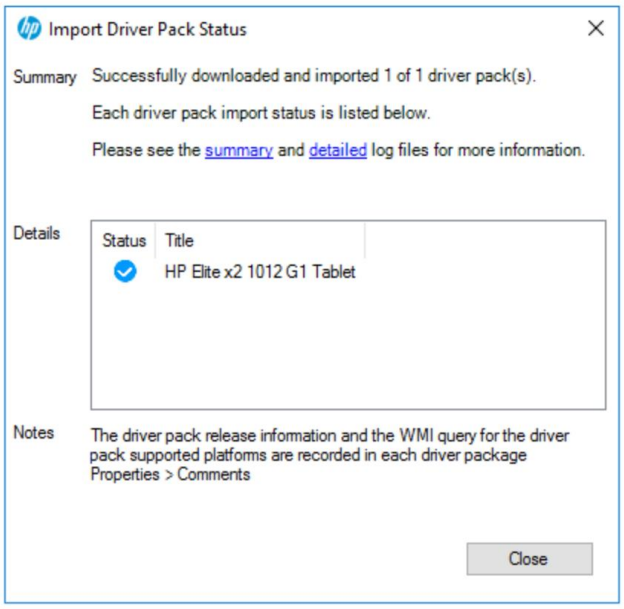
Skip the software package wizard if the user does not want to create Software Package(s) by unselect “Create Software Package” checkbox and click Next



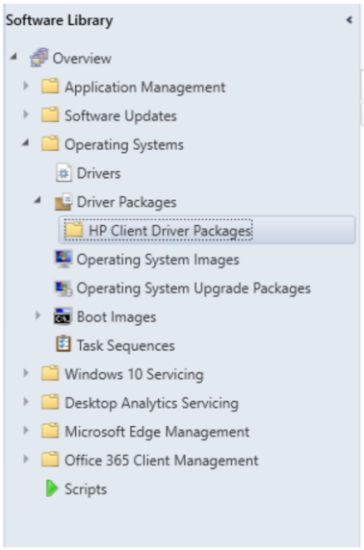
Select the distribution point and user has the privilege to choose the task sequence with 3 option i.e.; Do not Add, Add to New and Add to Existing and Click Import



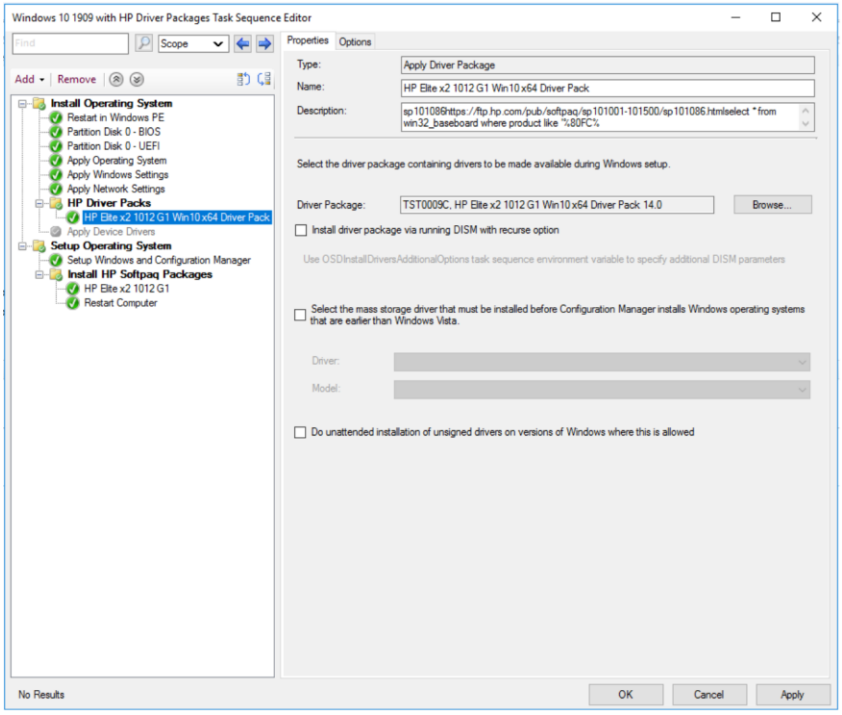
User receives pop up with the import driver pack status



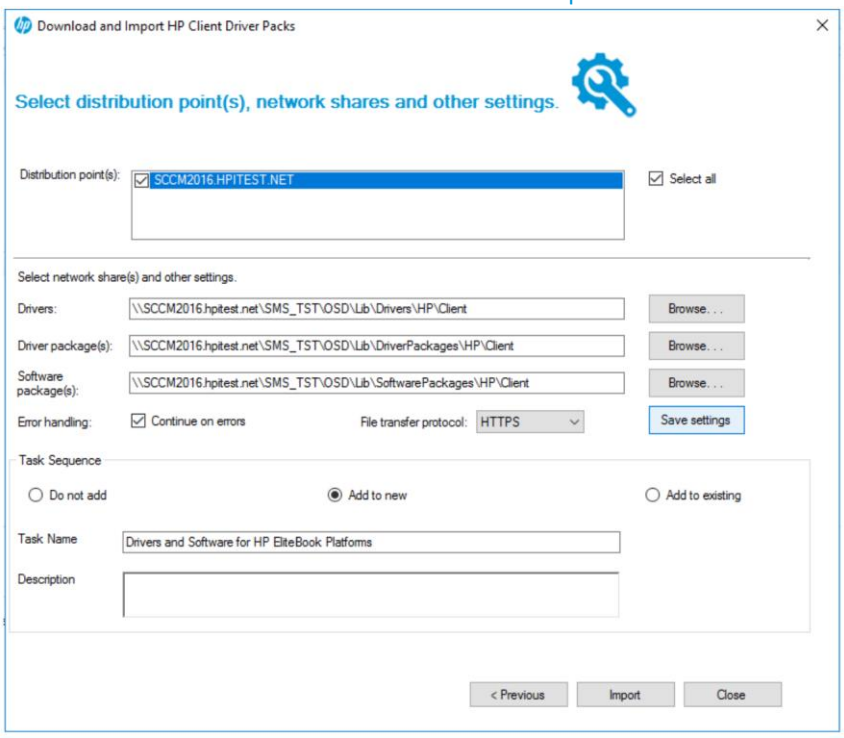
Once completed:
In the configuration manager console, Created Driver Package will be listed under 'HP Client Driver Packages' folder



In the selected task sequence, Created Driver Package will be listed under 'HP Driver Packs' folder.

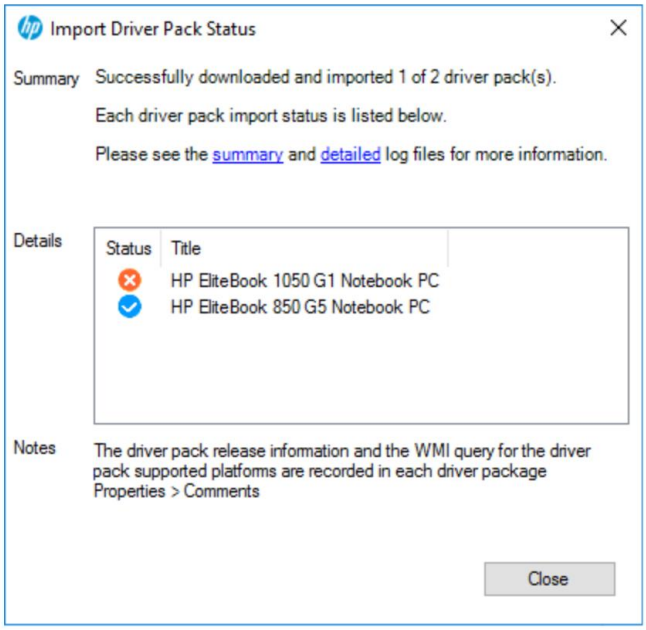


13.3.3Download and Import Driver Packs - Continue on errors



If **"Continue on error"** checkbox 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 impacted platform will not be created.

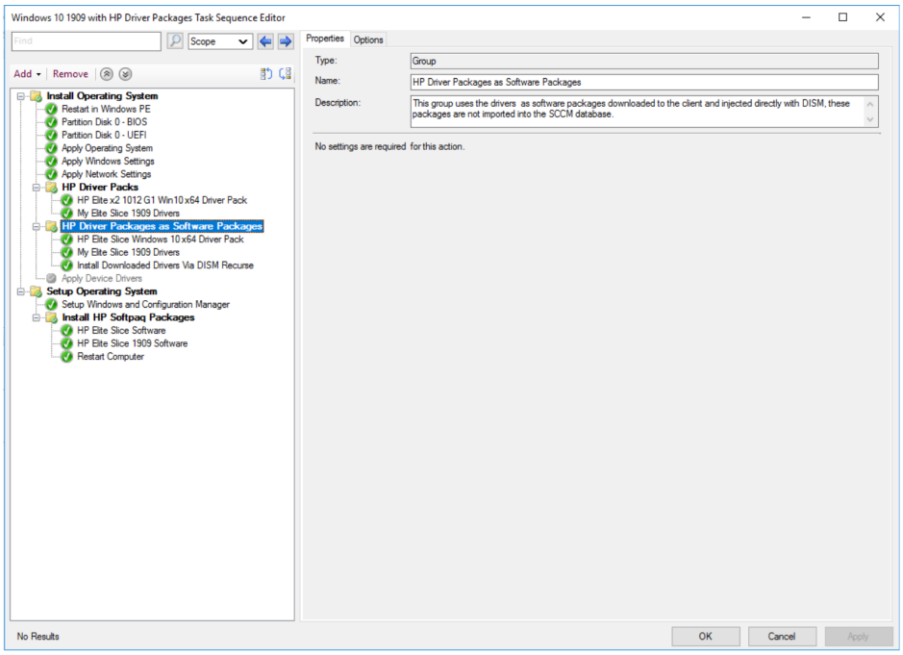
On click on Import, User receives pop up of import driver pack status.



User can click on Summary and details logs to review any failures.

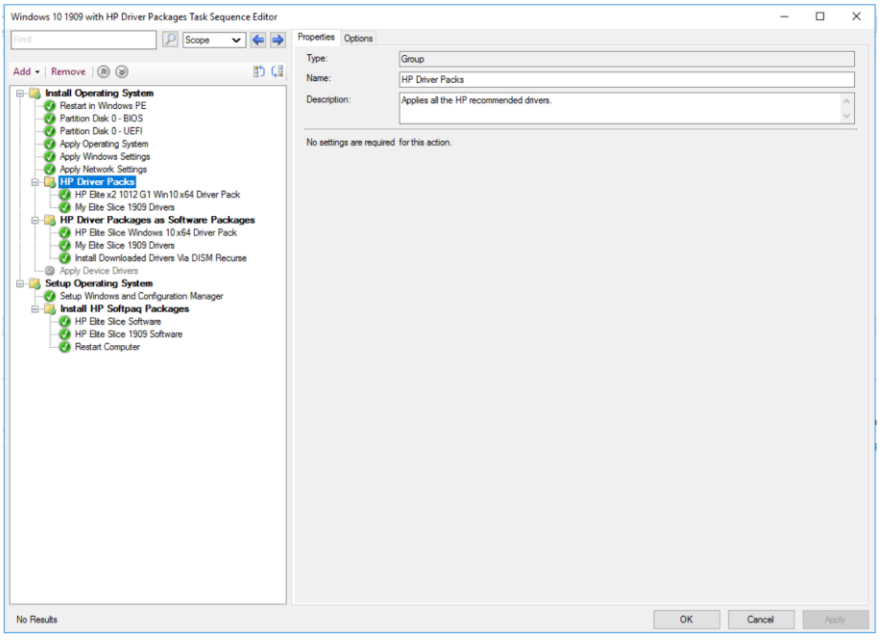
13.4 Examples

13.4.1 Task Sequence format when user check ”Create Driver Package as Software Package” checkbox.



The Driver Pack will be created under “HP Driver Packages as Software Packages”.

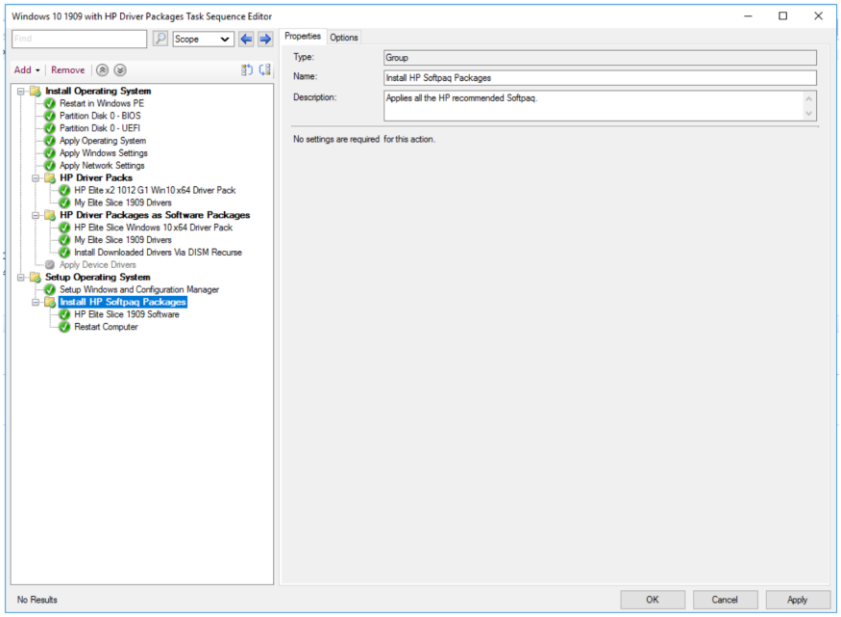
13.4.2 Task Sequence format when user Uncheck ”Create Driver Package as Software Package” checkbox.



The Driver Pack will be created under “HP Driver Packs”

13.4.3 Task Sequence format when user check ”Create Software

Package(s)” checkbox.



The Software Package will be created under “Install HP Softpaq Packages”

13.5 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.

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

To obtain 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.

To obtain driver packs using HP Support product pages:

1. Go to http://www.hp.com/support.
2. Select Get software and drivers.
3. Enter the client computer model number, and then select Find my product.
4. Select the client computer.
5. Select your language and operating system.
6. 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.

To obtain driver packs using HP SDM:

1. Go to http://www.hp.com/go/clientmanagement.
2. Under Resources, select HP Download Library.
3. Download SoftPaq Download Manager.
4. Select Start, select All Programs, select HP, and then select HP SoftPaq Download Manager.
5. Select Show software for all supported models.
6. Select English – International as the target language.
7. Under Product Catalog, select the target platform and operating system, and then select Find Available SoftPaqs.
8. Download the driver packs in the category Manageability – Driver Pack.

13.6 Creating driver packs using HP SDM

To create driver packs using HP SDM (version 3.5.2.0 or higher):

1. Select Start, select All Programs, select HP, and then select HP SoftPaq Download Manager.
2. Select Tools, and then select Configuration Options.

a. On the OS Filter tab, select the Win7, Win 8, or Win 8.1 operating system.

b. On the Language Filter tab, select English – International as the target language.

c. Select OK.

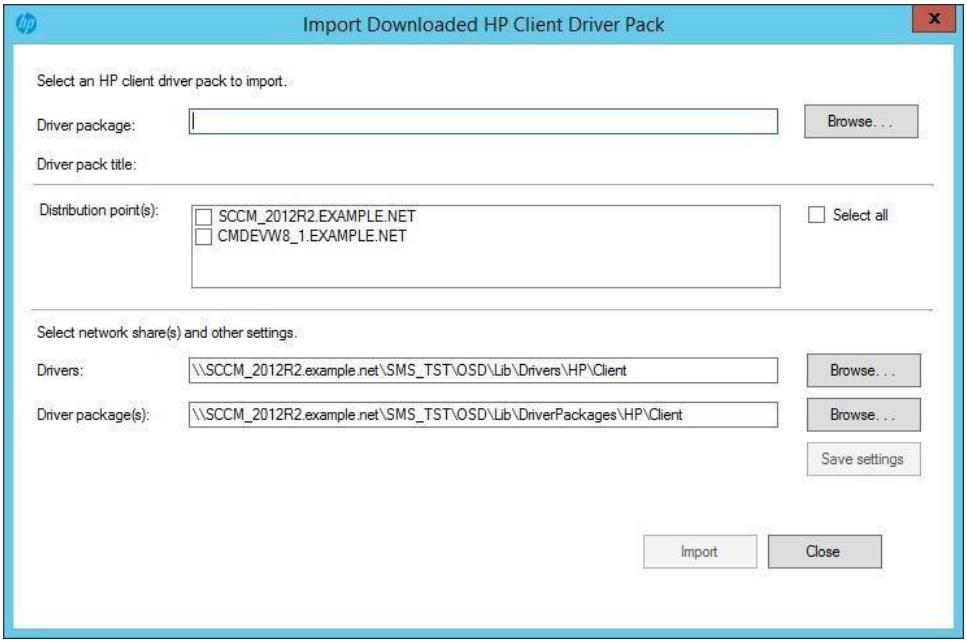
3. On the Build Driver Pack tab, select the plus sign (+) next to a product category to display all products in the category. Select products to add to the driver pack.
4. Select the platforms and operating systems, and then select Find Available SoftPaqs.
5. Select the SoftPaqs to include in the driver pack.
6. In the Download SoftPaqs window, select an action from the drop-down menu next to the Download button:
   - Build CAB File—Select this option to use Microsoft Deployment Toolkit or HP MIK in conjunction with Configuration Manager to deploy the driver pack.
   - Build ZIP File—Select this option to use HP MIK with Configuration Manager or to manually deploy the driver pack through another application.
7. Select Download.
8. If the EULA appears, accept the license and continue.
9. The Driver Pack Builder screen displays boxes for the Driver Pack Name, OS-Bitness, and Output directory. Enter any necessary information, and then select Build.
10. A message is displayed indicating that the driver pack build is complete. Select OK.

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

13.7 Importing HP driver packs

1. In Configuration Manager, select Software Library, select Overview, select Operating Systems, and then select Driver Packages.
2. In the HP Client PCs section of the ribbon menu, select Import Driver Pack.
3. Under Driver package, select Browse, and then select the HP driver pack to be imported.
4. Optionally, select distribution points to assign the imported driver packages to a specific destination; however, cloud distribution points are not supported.
5. 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 importation.

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



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

After the importation 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

14.1 Obtaining a WinPE driver pack

1. Go to http://www.hp.com/go/clientmanagement
2. Under Resources, select HP Download Library.
3. Download either HP WinPE Driver Pack 32-bit or HP WinPE Driver Pack 64-bit.

Not all platforms or configurations require the WinPE 4.0 driver pack, as WinPE 4.0 already contains many of the necessary hardware drivers needed to support operating system deployment. HP recommends creating and using the WinPE 4.0 driver pack, because the added drivers do not impact systems or configurations that do not need them.

WinPE 5.0 natively supports HP commercial desktops, notebooks, and workstations shipping from 2011 to 2013. Platforms shipping in 2014 or later might require the WinPE 5.0 driver pack. The WinPE 5.0 driver pack cannot be used with WinPE 4.0, nor can the WinPE 4.0 driver pack be used with WinPE 5.0.

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.

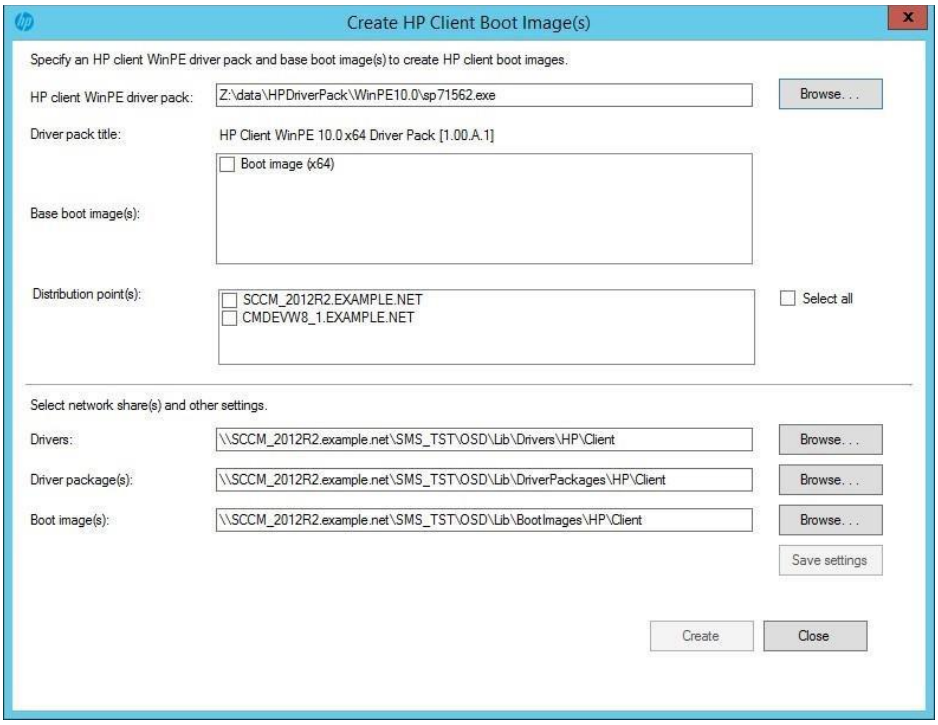
Before a boot image is made available to a distribution point, Configuration Manager might use Windows Assessment and Deployment Kit (ADK), particularly DISM.exe, to inject drivers to a boot image. DISM might fail to appropriately recognize the signature of some boot-critical drivers added to the boot 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.

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.

14.2 Importing a WinPE driver pack and creating boot images

1. In Configuration Manager, select Software Library, select Overview, select Operating Systems, and then select 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. 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.
5. Optionally, select distribution points to assign the boot images to a specific destination; however, cloud distribution points are not supported.
6. 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 the Save settings button. Select this button to save the settings for subsequent boot image creation and driver or driver pack import procedures.



Depending on the architecture of the base image and the architecture supported by the Windows Preinstallation

Environment boot image, x86 and/or x64 images are created. HP Windows Preinstallation Environment driver packs for Windows 10 contain drivers for 64-bit boot images. Windows Preinstallation Environment driver packs for previous versions of Windows contain drivers for both 32- and 64-bit boot images.

After the process is complete, the new boot images are created in Boot Images > HP Client Boot Images.

To access the command prompt during the WinPE portion (F8) for debugging purposes:

1. Right-click the image and select Properties, and then select Customization.
2. Select Enable command support (testing only).

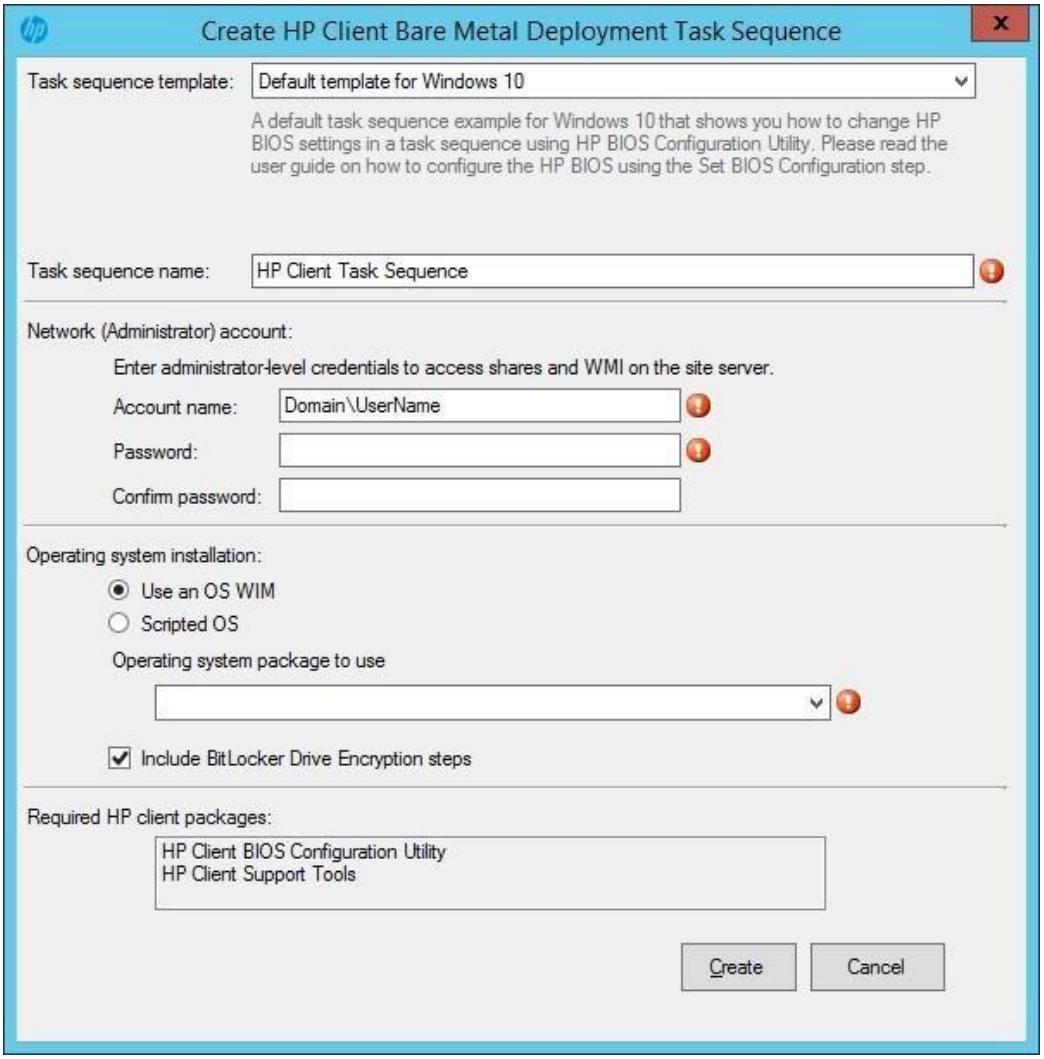
Before these boot images can be used in a task sequence, the boot images need to be pushed out to the distribution point. If no distribution points were selected in the import process or if additional distribution points are needed, or if there is a change to the boot image properties, select the boot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

15 HP Client Task Sequences

15.1 Creating a deployment task sequence

1. In Configuration Manager, select Software Library, select Overview, select Operating Systems, and then select Task Sequences.
2. In the HP Client PCs section of the ribbon menu, select Create Deployment Task Sequence.
3. Select a template from the Task Sequence Template drop-down menu.

   The following examples show how to reference HP tools to aid with the deployment process.
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 box displays confirmation of the 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

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.

15.2 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.

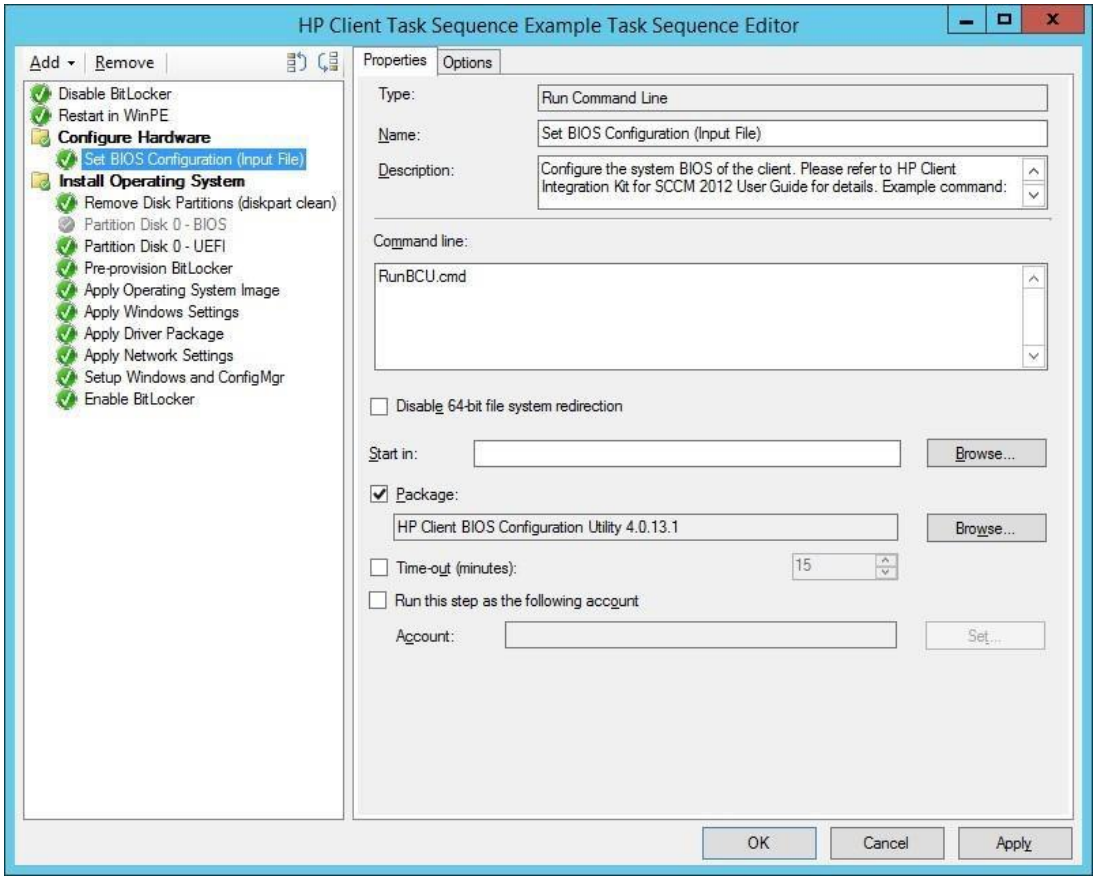
The template Configure RAID Example contains specific steps that are discussed in Using the Configure RAID Example template.

1. Be sure that the target platform driver pack has been imported. See Importing HP driver packs.

2. Right-click the task sequence and select Edit.

   The following figure is a task sequence created by the Default Template for Windows 7 or Windows 8. This task sequence can be used with either Windows 7 or Windows 8.

   There is also the 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 of 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 the section Configuring the Set BIOS Configuration task step 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 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.

16.2.1 Assigning 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 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).

16.2.2 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:

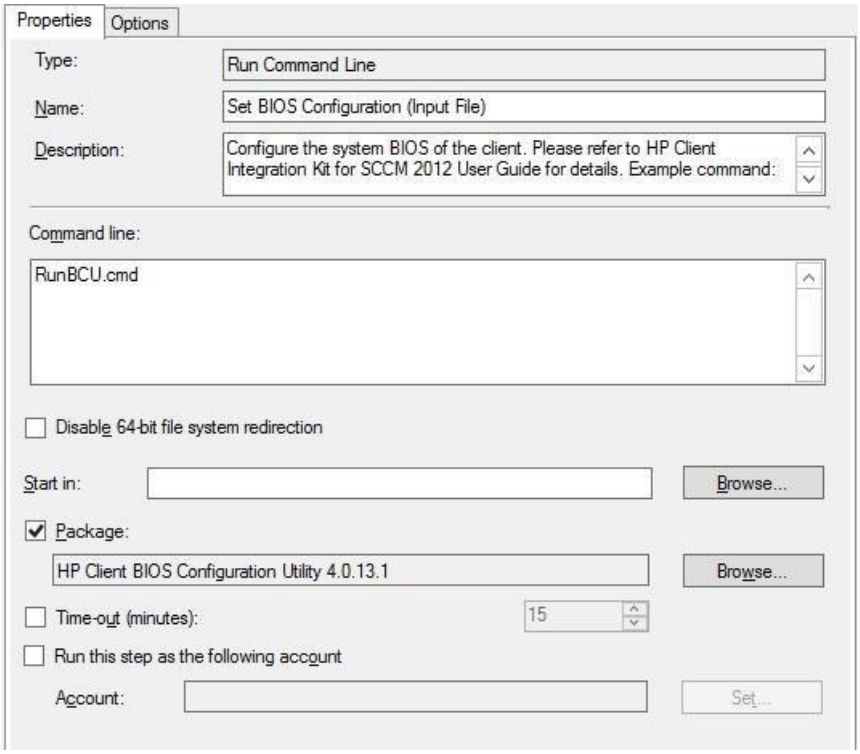
1. Right-click the content/package and select Properties.
2. Select the Data Access tab, and select Copy the content in this package to a package share on distribution points.
3. Select OK.
4. If necessary, select the Access content directly from the distribution point option on the Distribution Points 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 Remove Disk Partitions (diskpart clean) step is needed, but I 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.

16.3 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.

16.3.1 Adding and editing configuration files

NOTE:
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).

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.

16.4 Refreshing task sequence references

Task sequence references might need to be refreshed if one of the following 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. To refresh the references:
  1. Right-click the task sequence and select Edit.
  2. Follow the on-screen instructions in the Action column of the following table.

Table 2 Refreshing task sequence references

Task sequence step	Action
Set BIOS Configuration (Input File)	Select the package HP Client BIOS Configuration Utility in the folder HP Client Support Packages.
Remove Disk Partitions (diskpart clean)	Select the package HP Client Support Tools in the folder HP Client Support Packages.

16.5 Using the Configure RAID Example template

16.5.1 Preparing 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.

16.5.2 Preparing 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.

2. Go to https://downloadcenter.intel.com, and then search for 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.

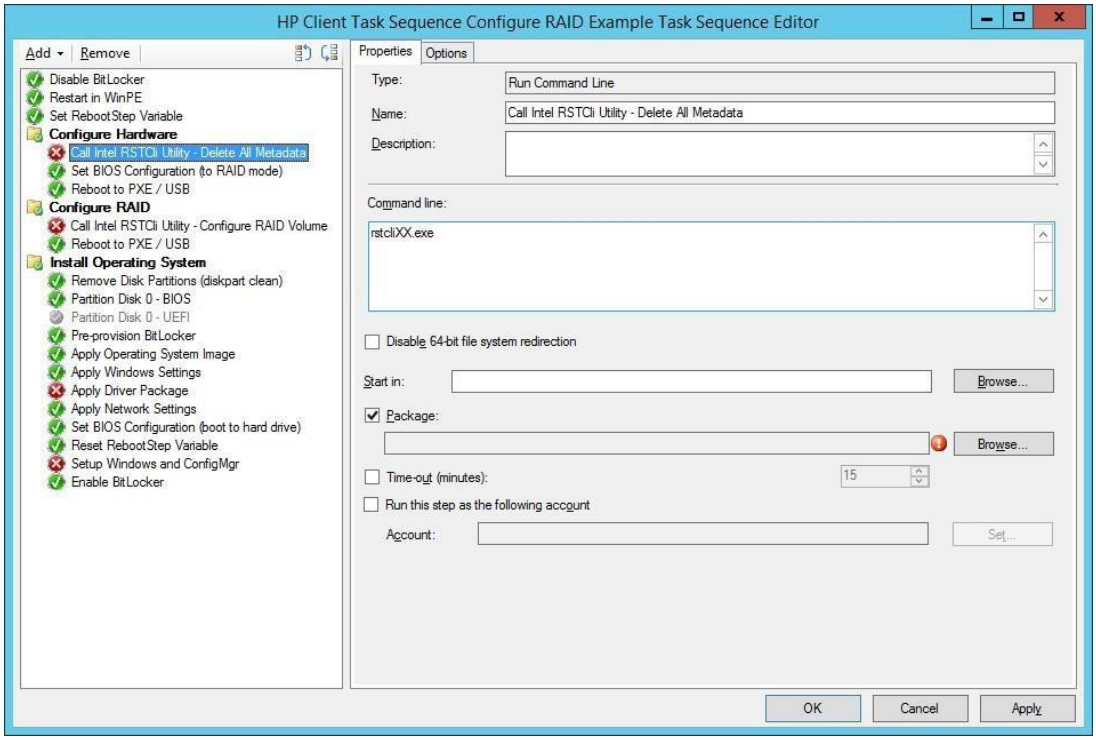
3. Unzip the downloaded file. The file might contain zip files for the 64-bit and 32-bit binaries of the tool. Those also need to be extracted.

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.

16.5.3 Configuring task sequence steps

1. To begin configuration, right-click the task sequence and select Edit.



2. The following steps need to be configured:

   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 just 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 just 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
```

Again, `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.

16.5.4 Assigning 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).

16.5.5 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 of the wizard.

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.

16.5.6 Understanding the 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:

    a. In Configuration Manager, select Assets and Compliance workspace.

b. Select Devices.

c. Select the target client system.

d. Select Clear Required PXE Deployments on the ribbon.

- If the task sequence failed to run completely, it might be necessary to clear or reset the RebootStep variable as follows:
    a. Right-click the target client system and select Properties.

    b. Select the Variables tab.

    c. Select the RebootStep variable, and then select the delete button with the X-like icon.

17 HP BIOS Configuration Utility (BCU)

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.

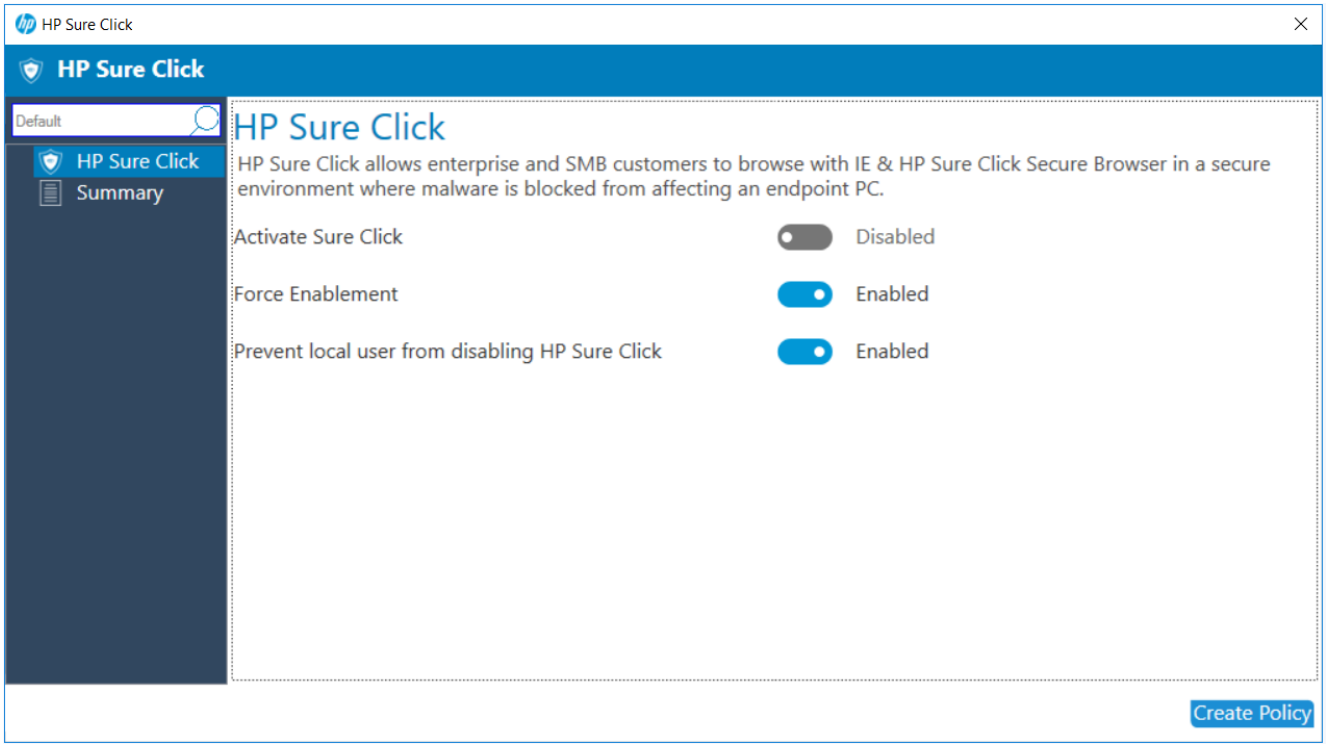
NOTE:
The version of BCU included with HP MIK includes a batch file (RunBCU.cmd) that automatically detects the current operating system and runs the correct version of BCU (32- or 64-bit).

18 HP Sure Click

HP Sure Click secures your computer when you browse the internet. When Sure Click is installed, websites are opened in a micro-VM that acts as a container that prevents malware from infecting your computer, since any malicious code executed by the website will be restricted within the micro-VM.

The following HP Sure Click features can be managed with MIK:

- Activate Sure Click
- Force Enablement of Sure Click
- Prevent Sure Click from being disabled

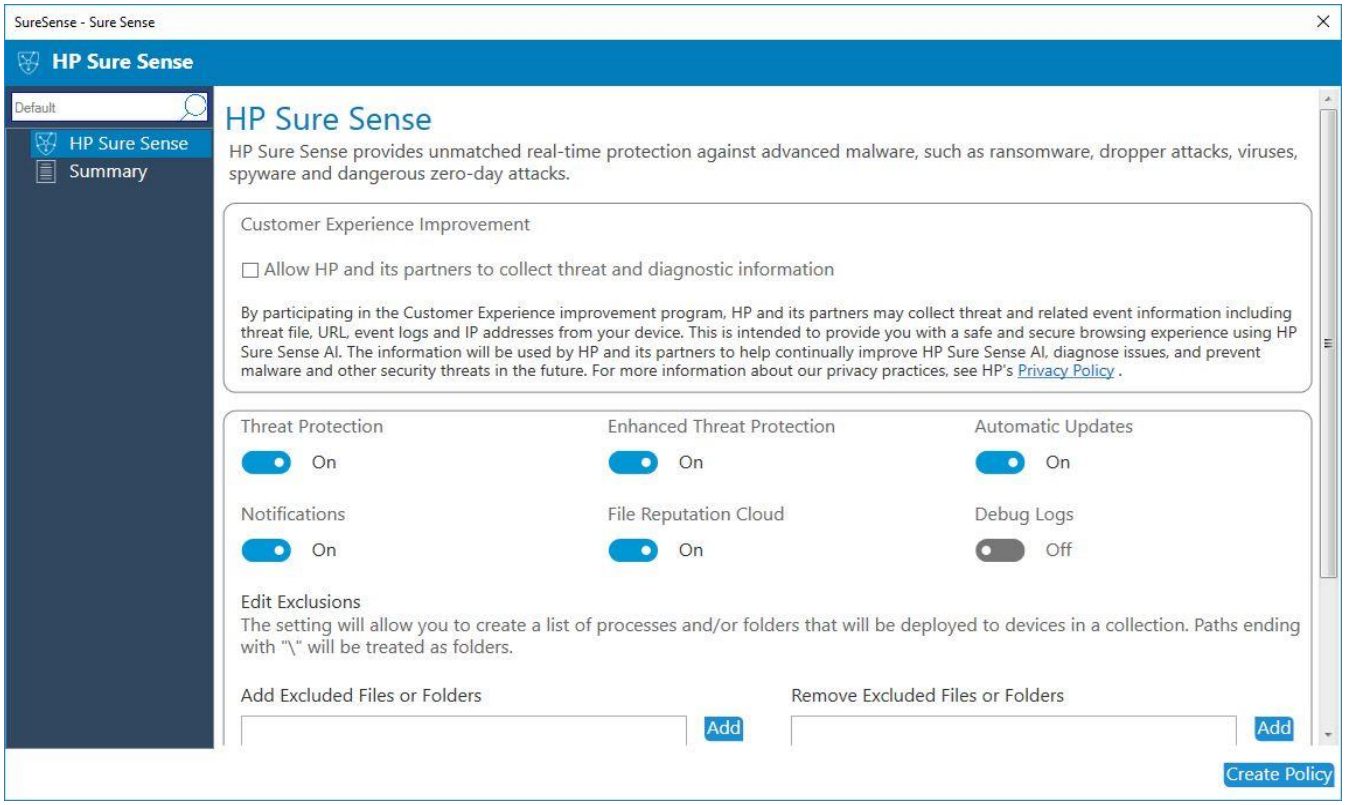


19 HP Sure Sense

HP Sure Sense uses deep learning models to detect malicious files and prevent malware, zero-day, ransomware, and Advanced Persistent Threat (APT) attacks from harming your computer.

The following HP Sure Sense features can be managed with MIK:

1. Threat Protection
2. Enhanced Threat Protection
3. File Reputation Cloud
4. Trusted Files / Folders.

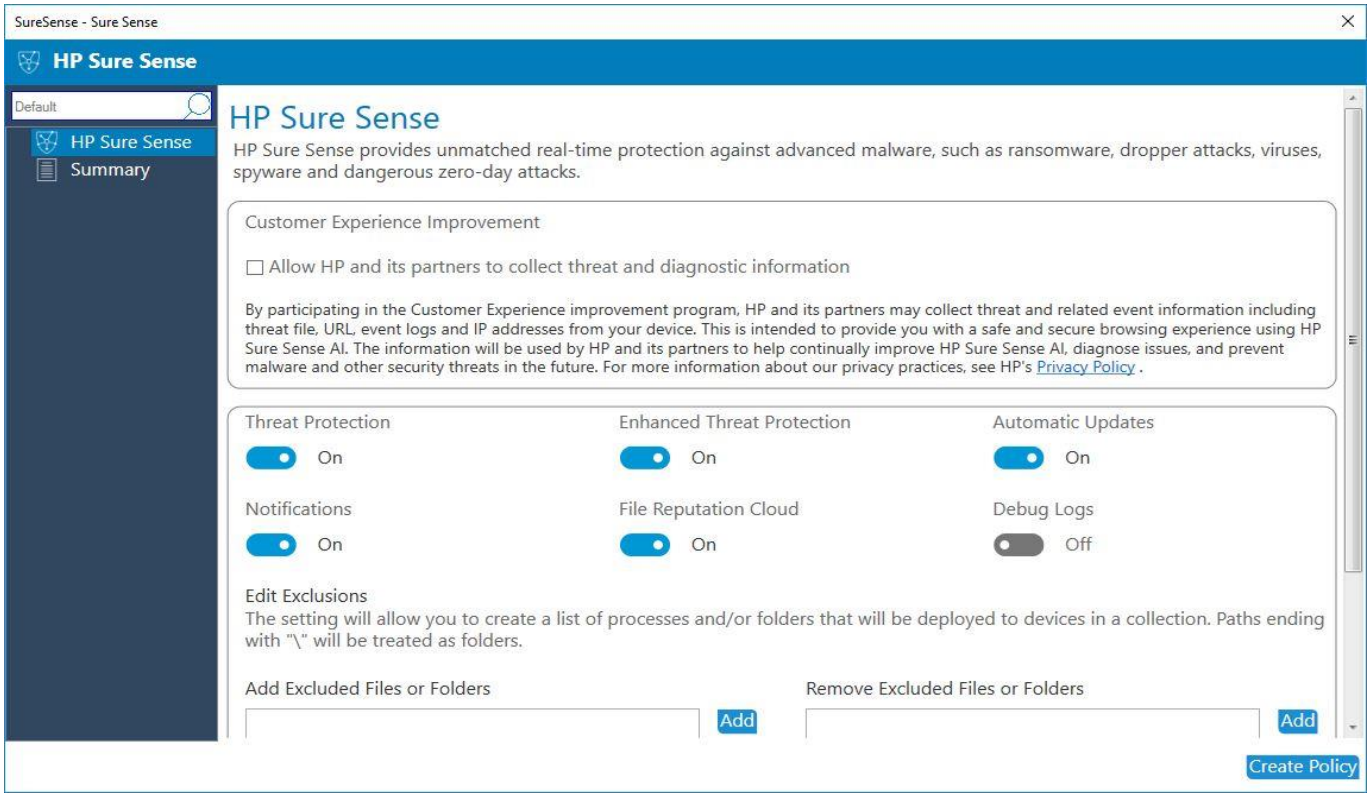


Creating a policy

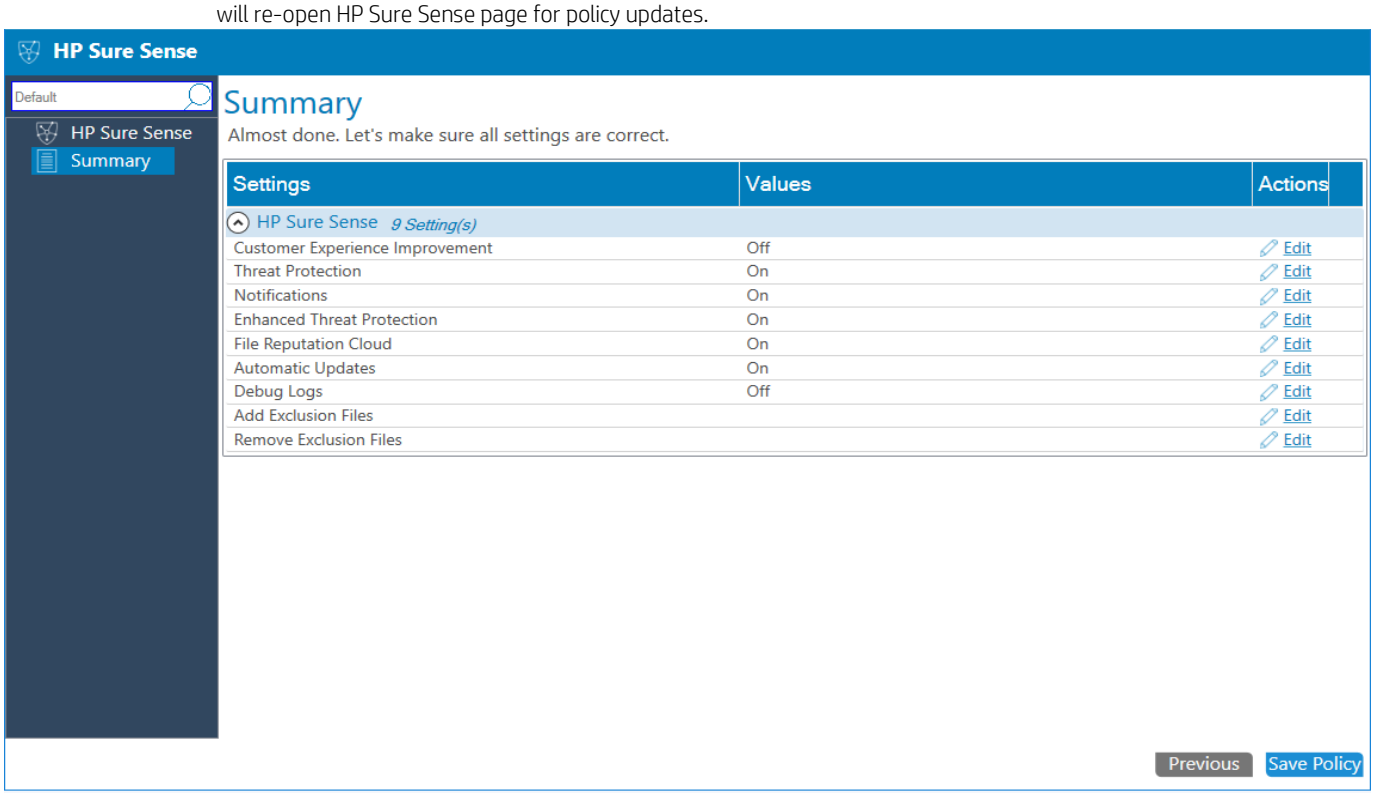
a. In Configuration Manager, select Client Security, and then select Overview.

b. Select HP Manageability Integration Kit, right-click Sure Sense, and then select Create Policy.

c. Enter a Baseline name and start the creating policy wizard.



8. Confirm default selections and modify as needed. You can Add / Remove trusted Files or Folders.
9. Click on Next.
10. On Summary Page policy details are available for final review and changes. Clicking on edit for any sub-category will re-open HP Sure Sense page for policy updates.



11. Select Save Policy.
12. After the policy has been saved successfully, select Deploy, and then select the target collection{s} to apply the policy.

20 HP Password Utility

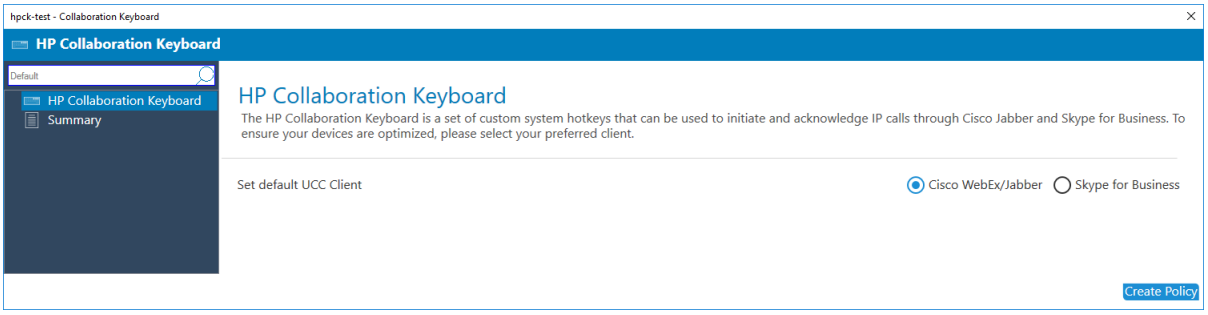
HP Password Utility is a tool for creating an encrypted password file that can be used with a BCU password file parameter. This tool is included with BCU. For more information, see the *HP BIOS Configuration Utility User Guide*.

21 HP Collaboration Keyboard

The HP Collaboration Keyboard software is used to manage conference calls with the built-in controls of certain HP keyboards.

HP MIK can be used to manage the following features of the software:

- Set the default communication client



22 HP Reports

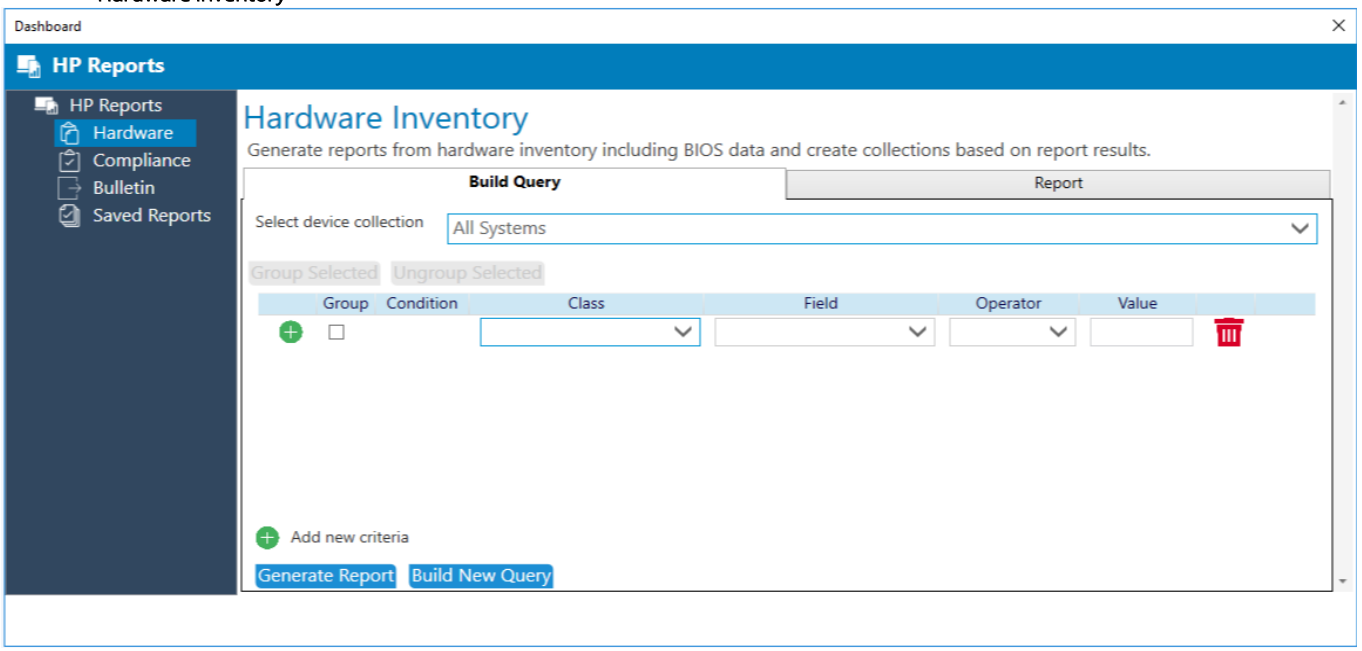
With HP Reports IT Admin will have ability to generate and save different type of reports,

- HW & BIOS inventory reports.
- Policy compliance report
- Pull reports for important security updates , HP product releases available.

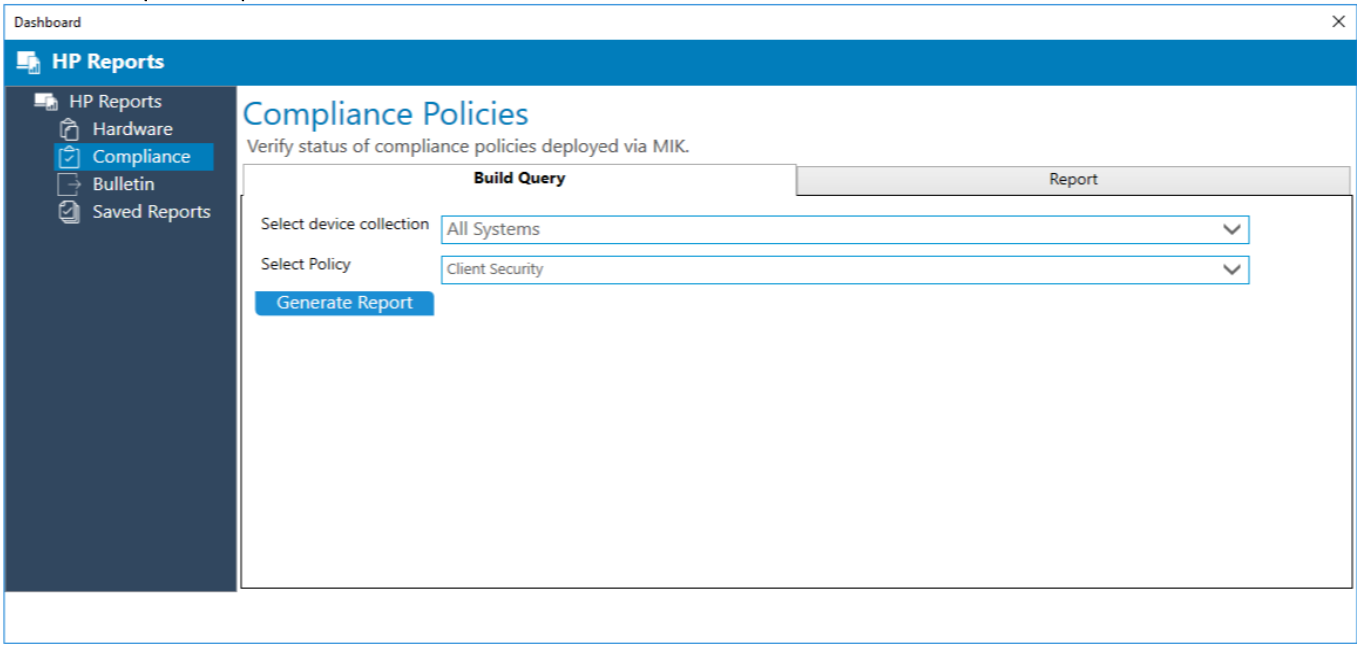
Generate Report:

1. Launch MIK Reports Dashboard.
2. You can Navigate to following sections to generate report

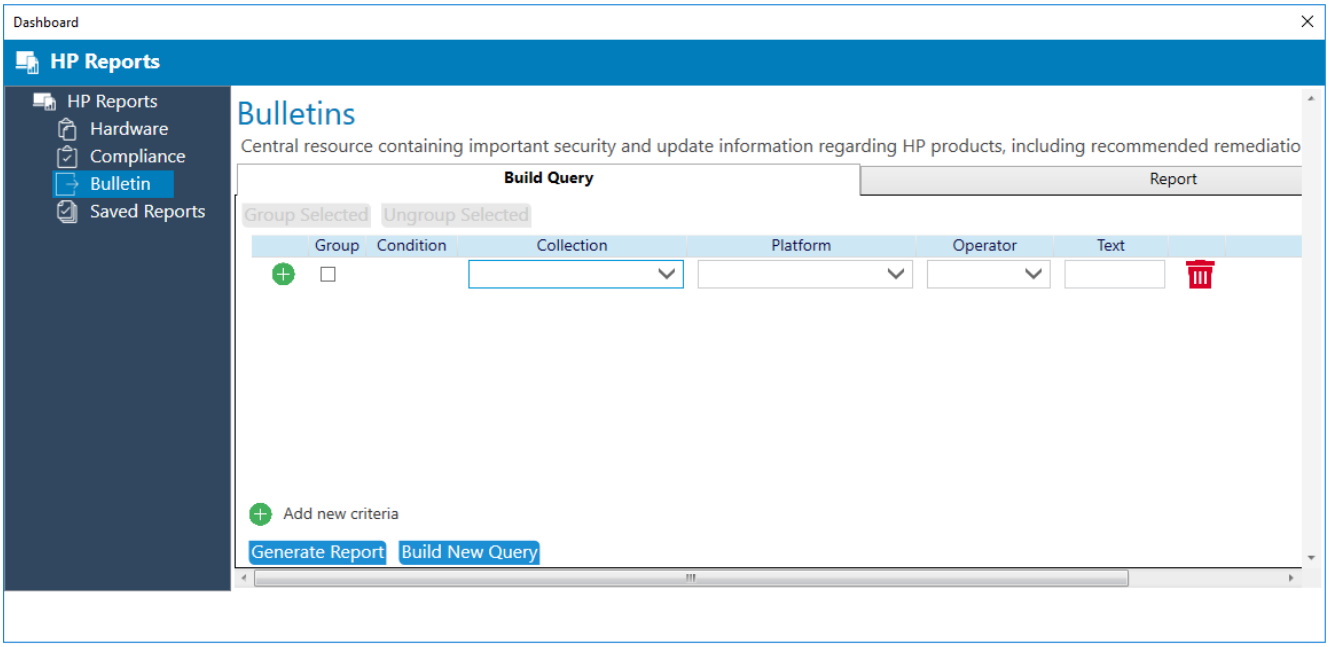
Hardware Inventory



Compliance Reports



Bulletins



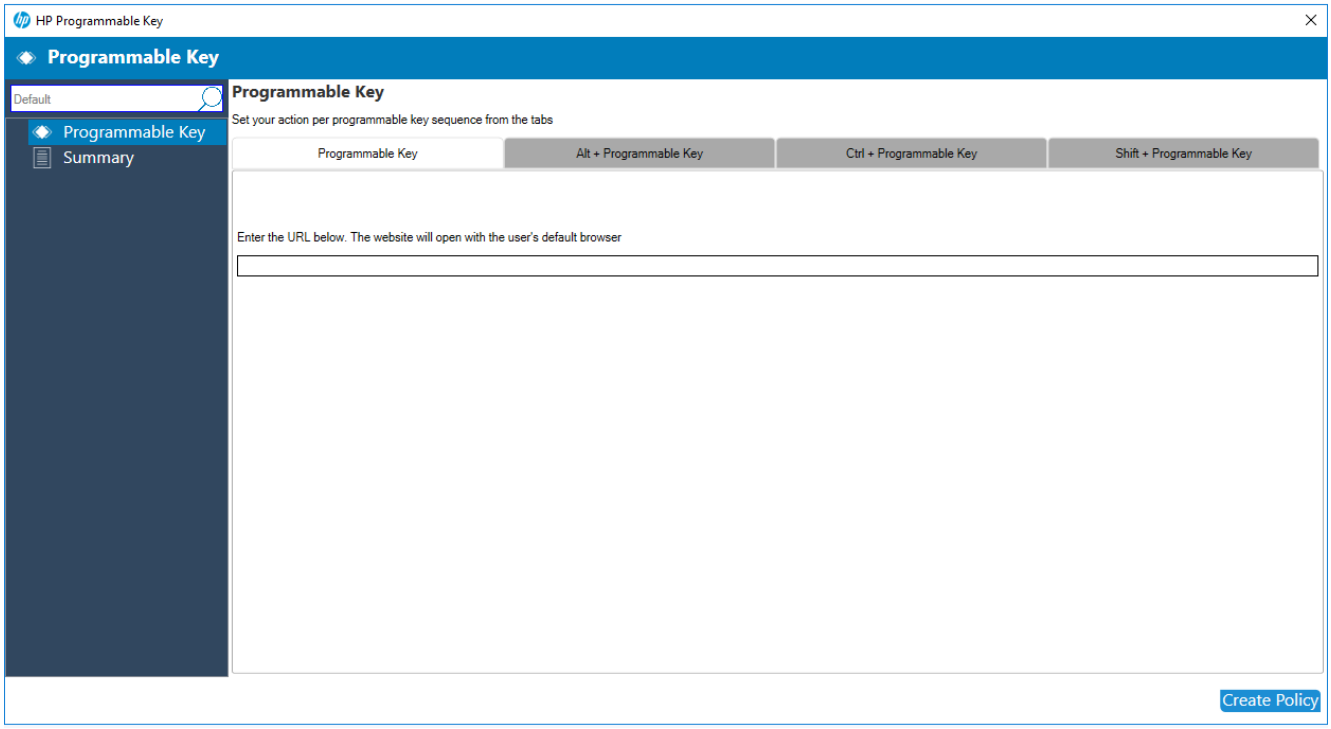
3. To generate report
   - Select the Device collection in which the client machine is added.
   - Build a query by selecting different selection options.
   - Click on Generate Report.

Note

- Saved Reports Will list all reported saved.
- Blank value cannot generate a report.

23 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.



ITDM can deploy policy through MIK to configure URL's only.

Creating a policy

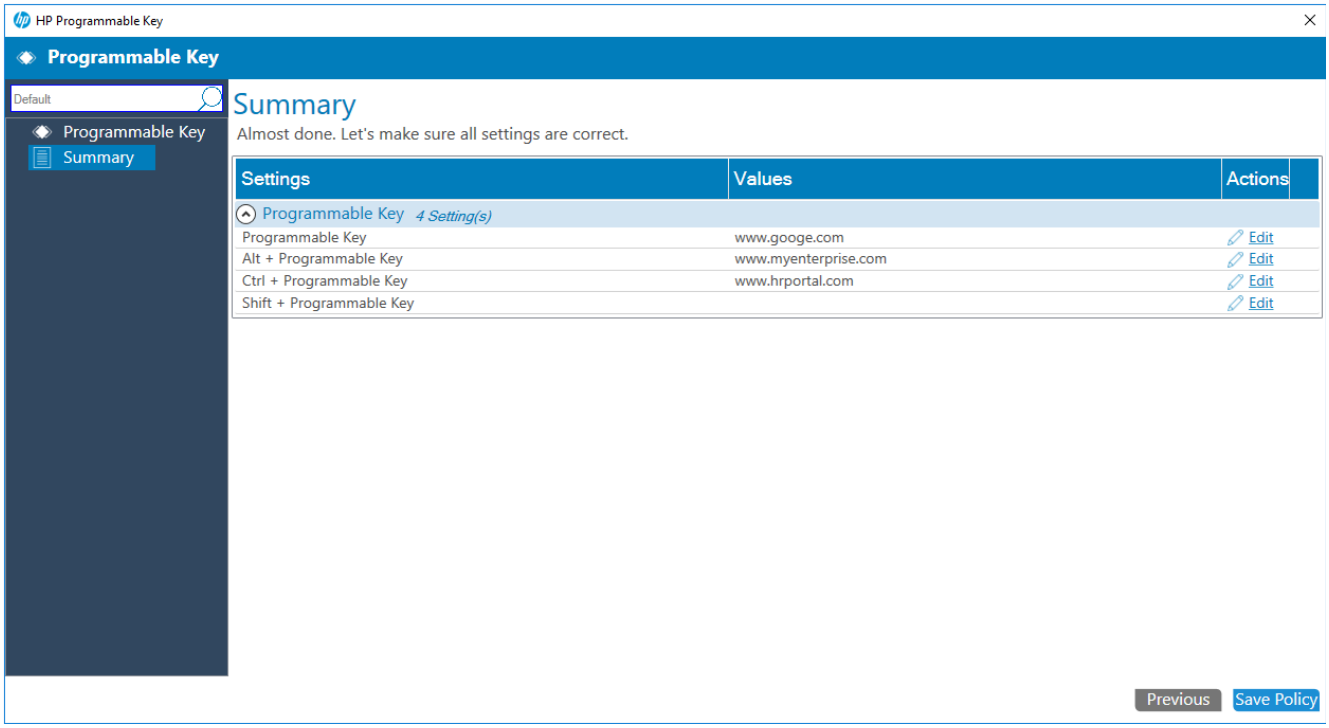
a. In Configuration Manager, select Client Security, and then select Overview.

b. Select HP Manageability Integration Kit, right-click HP Programmable Key, and then select Create Policy.

c. Enter a Baseline name and start the creating policy wizard.

d. Enter URL for function key + Programmable Key combination.

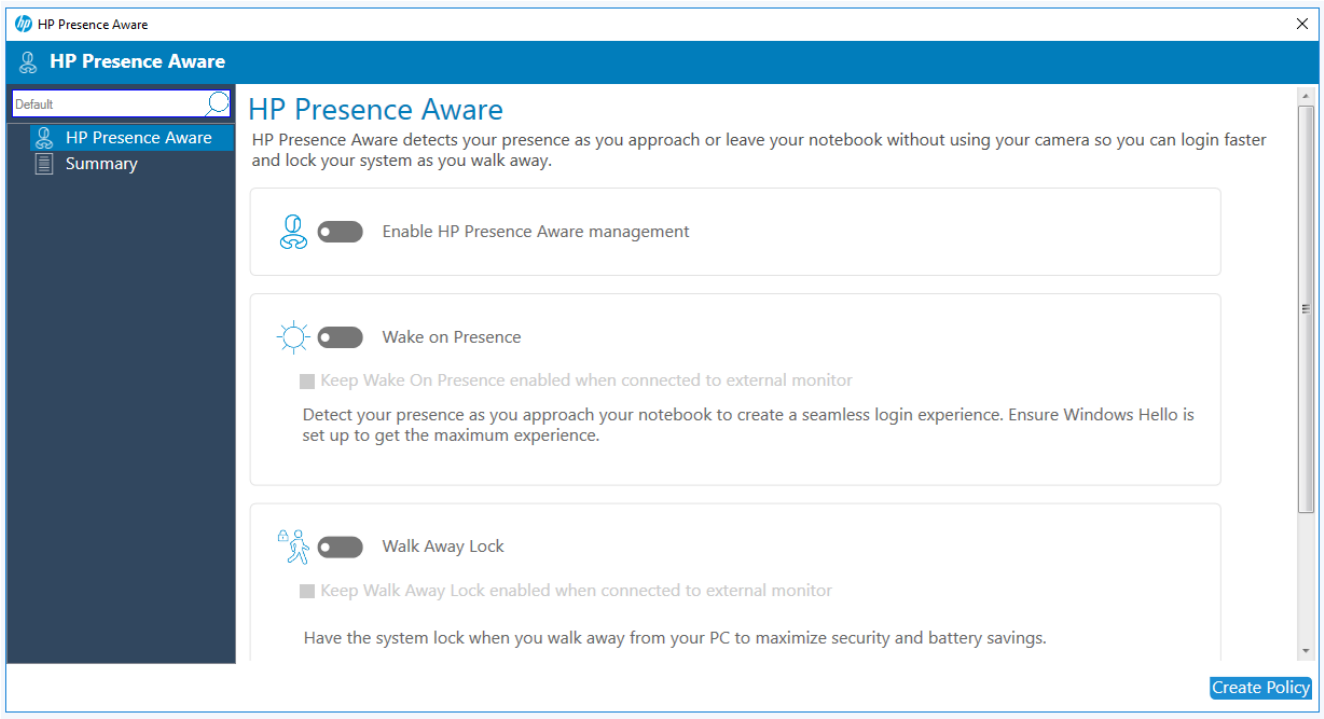
e. Click on Create Policy



f. Click on Save and Deploy Policy

24 HP Presence Aware

HP Presence Aware detects your presence as you approach or leave your notebook without using your camera so you can login faster and lock your system as you walk away.



Creating a policy

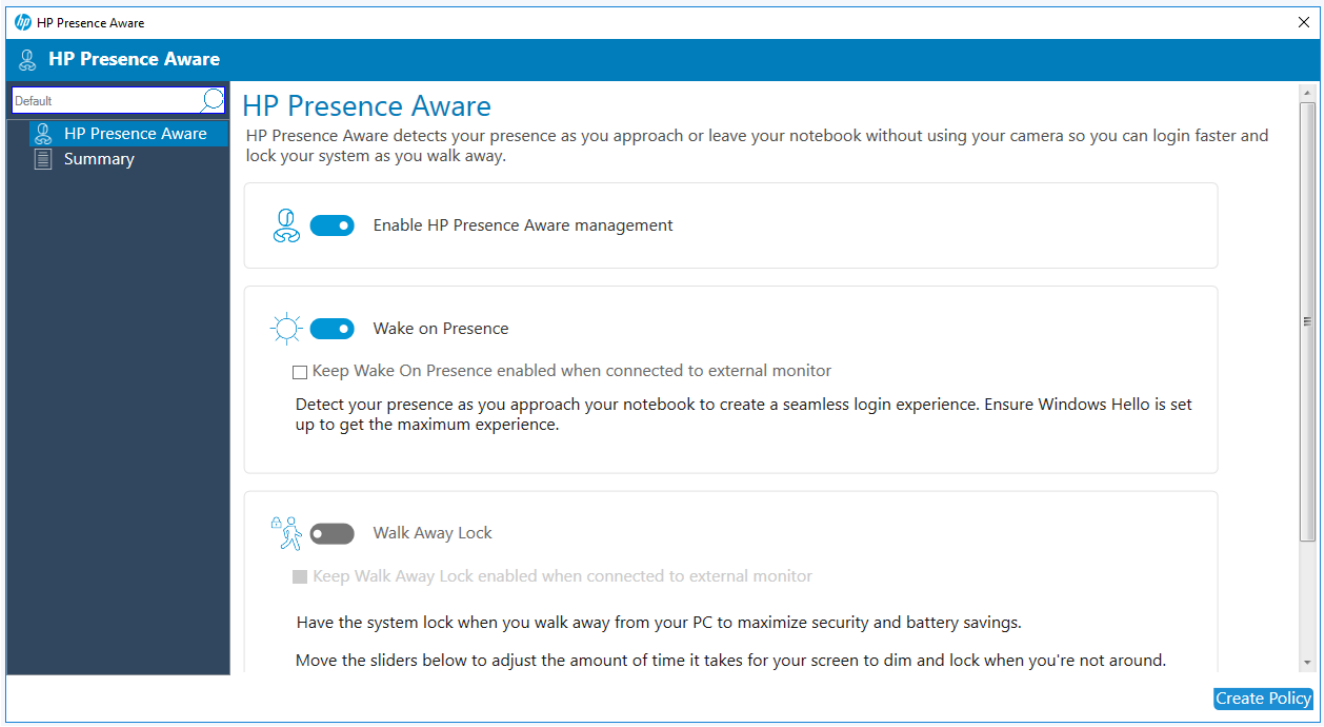
a. In Configuration Manager, select Client Security, and then select Overview.

b. Select HP Manageability Integration Kit, right-click Presence Aware, and then select Create Policy.

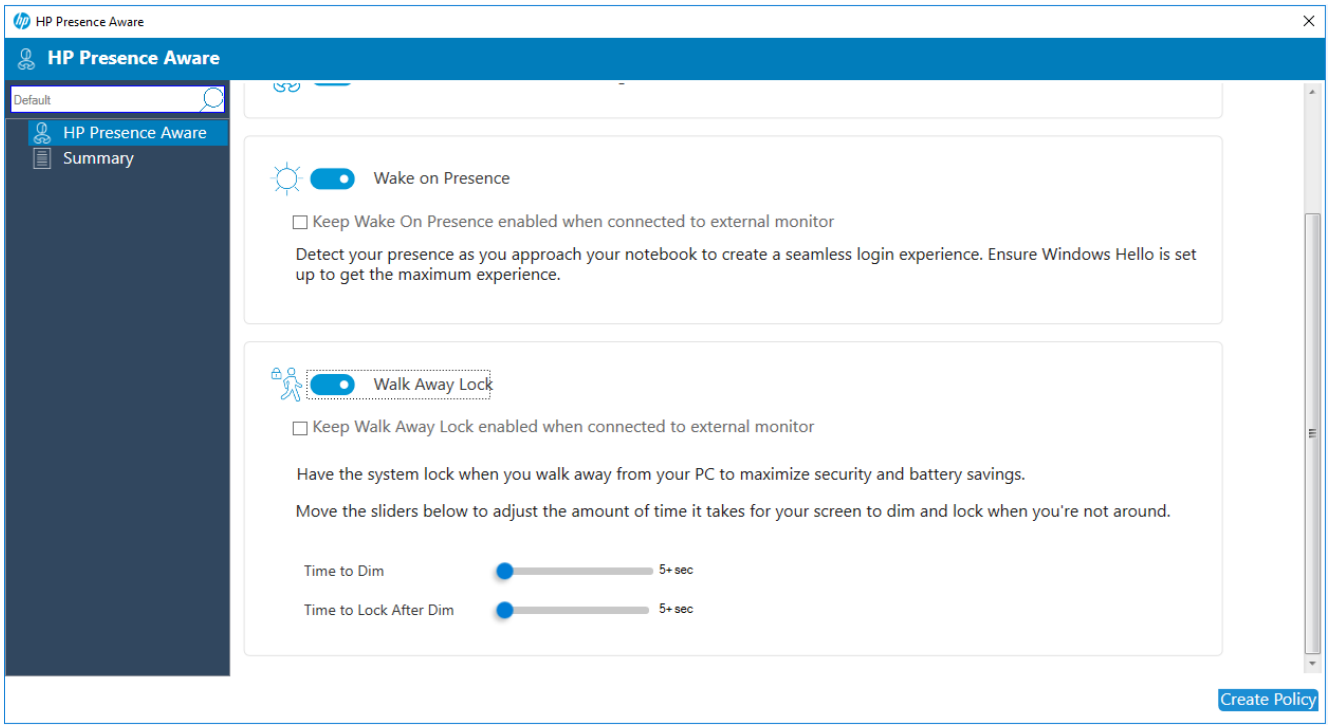
c. Enter a Baseline name and start the creating policy wizard.

d. Select Enable HP Presence Aware Management to enable feature.

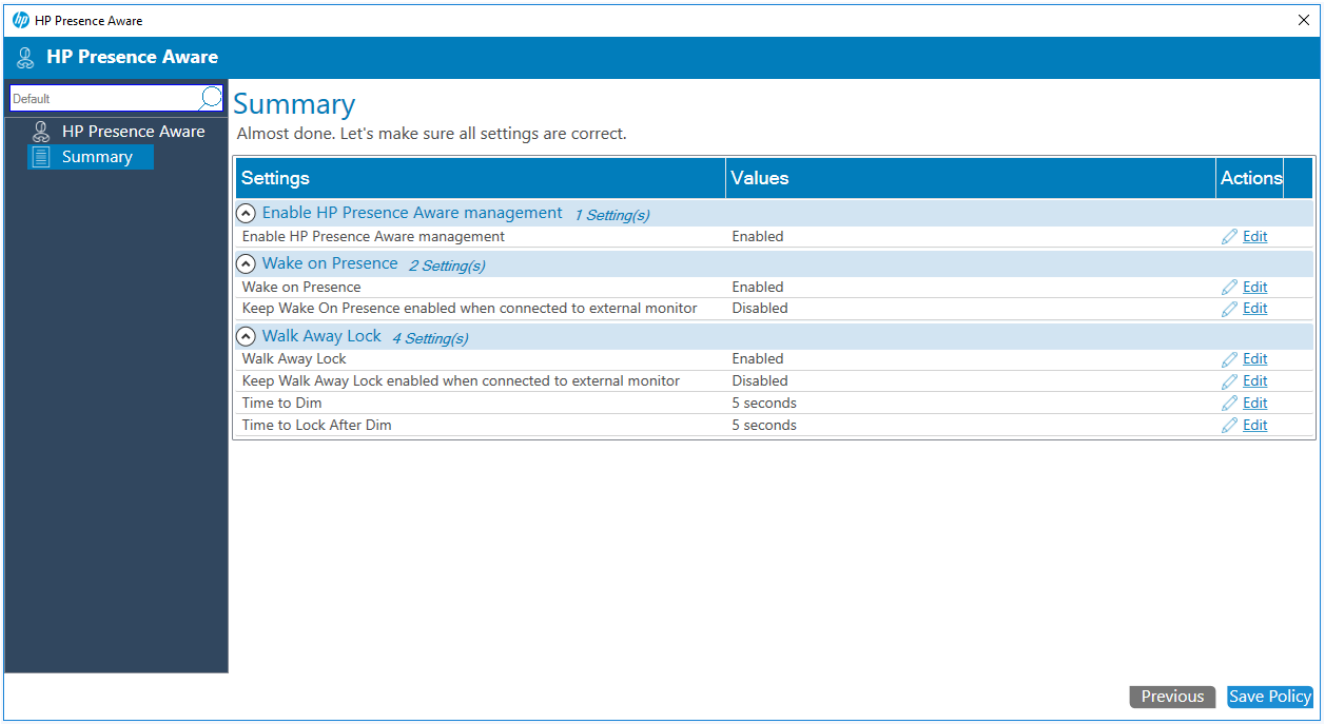
e. Select Wake on Presence to configure the feature settings.



f. Select Walk Away Lock to configure feature settings



g. Click on Create Policy



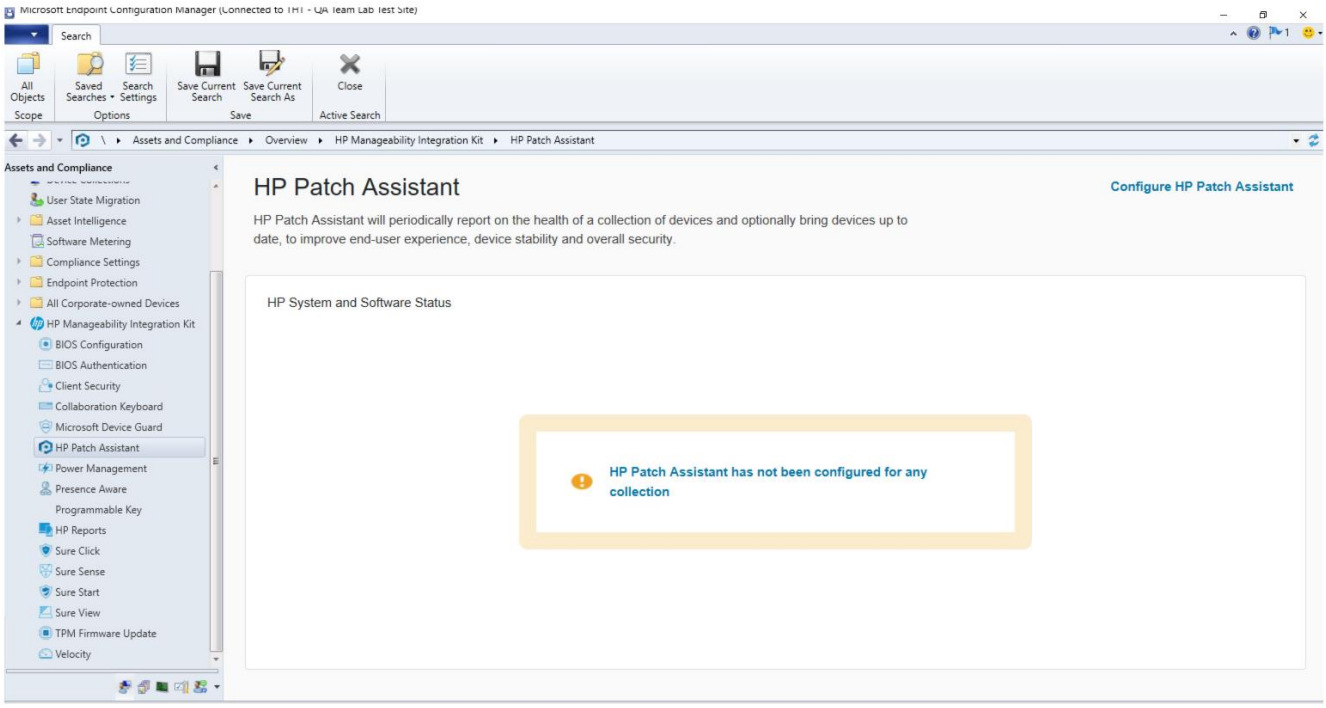
h. Click on Save and Deploy Policy

25 HP Patch Assistant

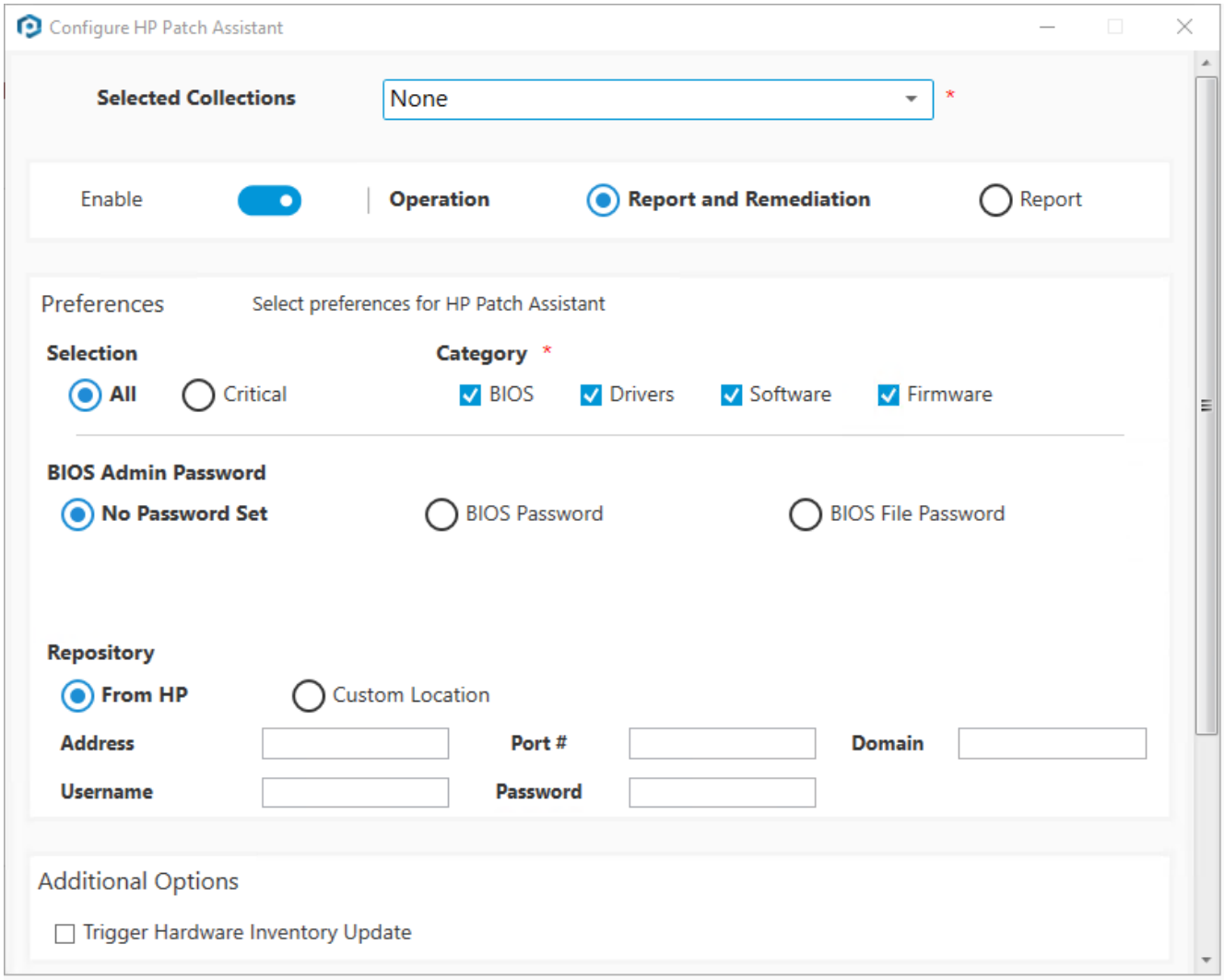
HP Patch Assistant will periodically report on the health of a collection of devices and optionally bring devices up to date, to improve end-user experience, device stability and overall security.

Configuring HP Patch Assistant for device collections.

Users 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.

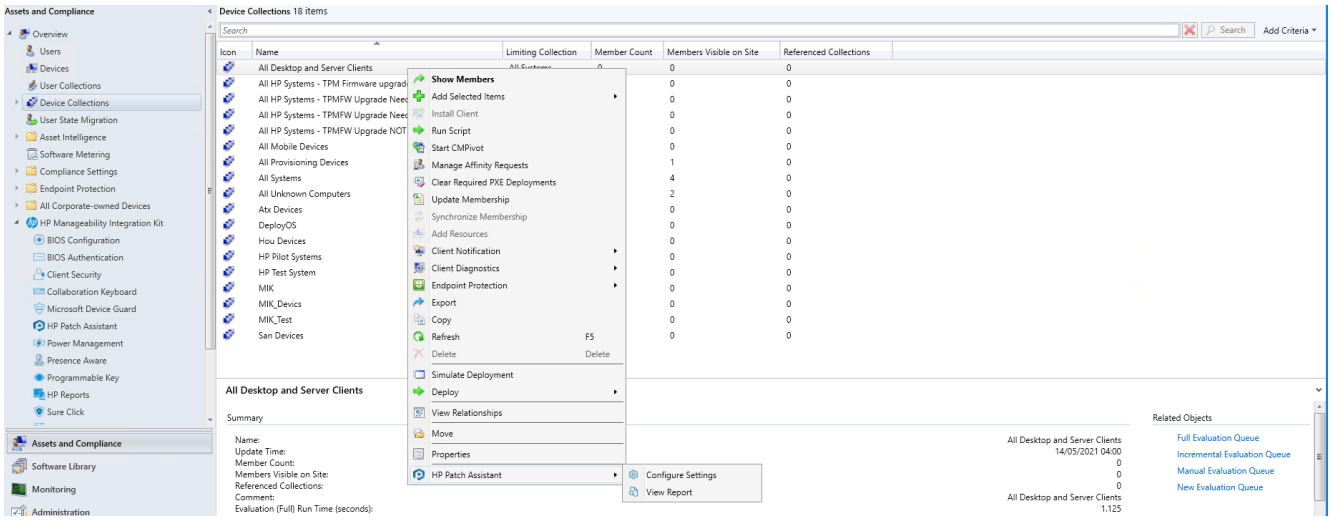


Click on HP Patch Assistant – Dashboard Link **"Configure HP Patch Assistant"**

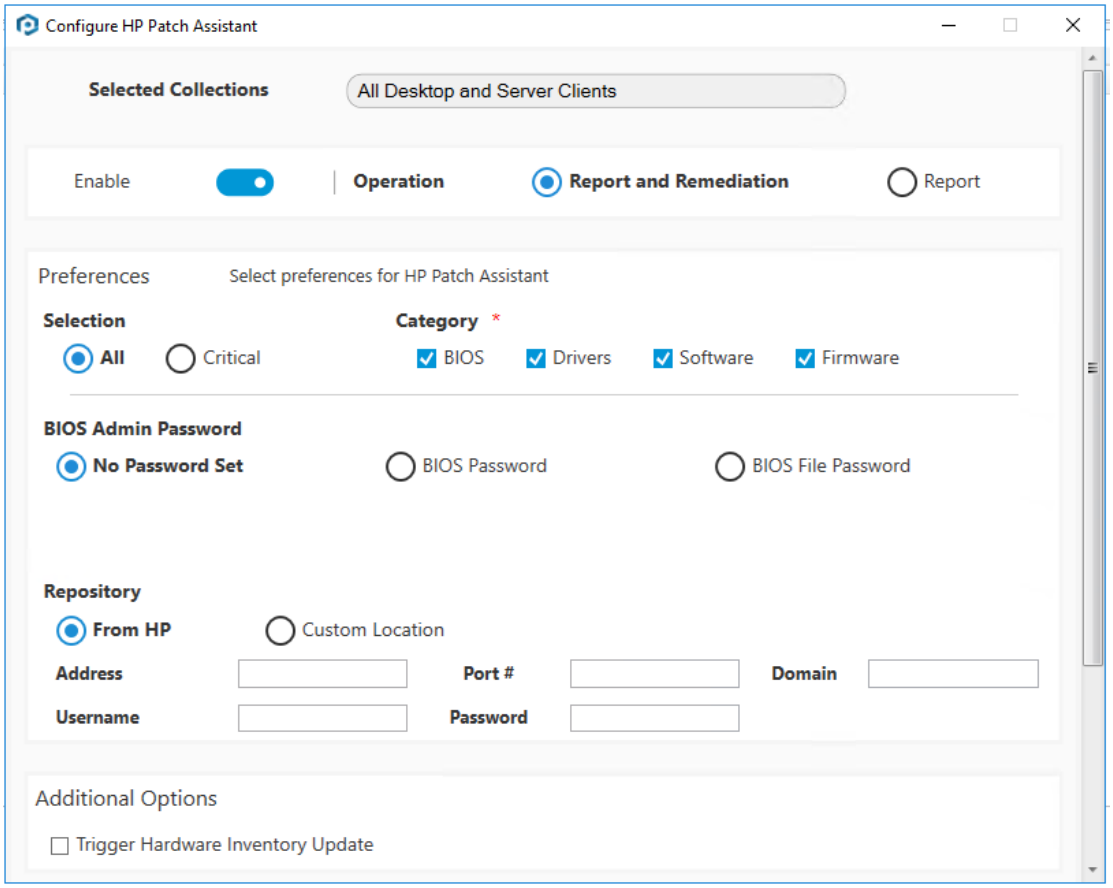


Configuring HP Patch Assistant for a single device collection.

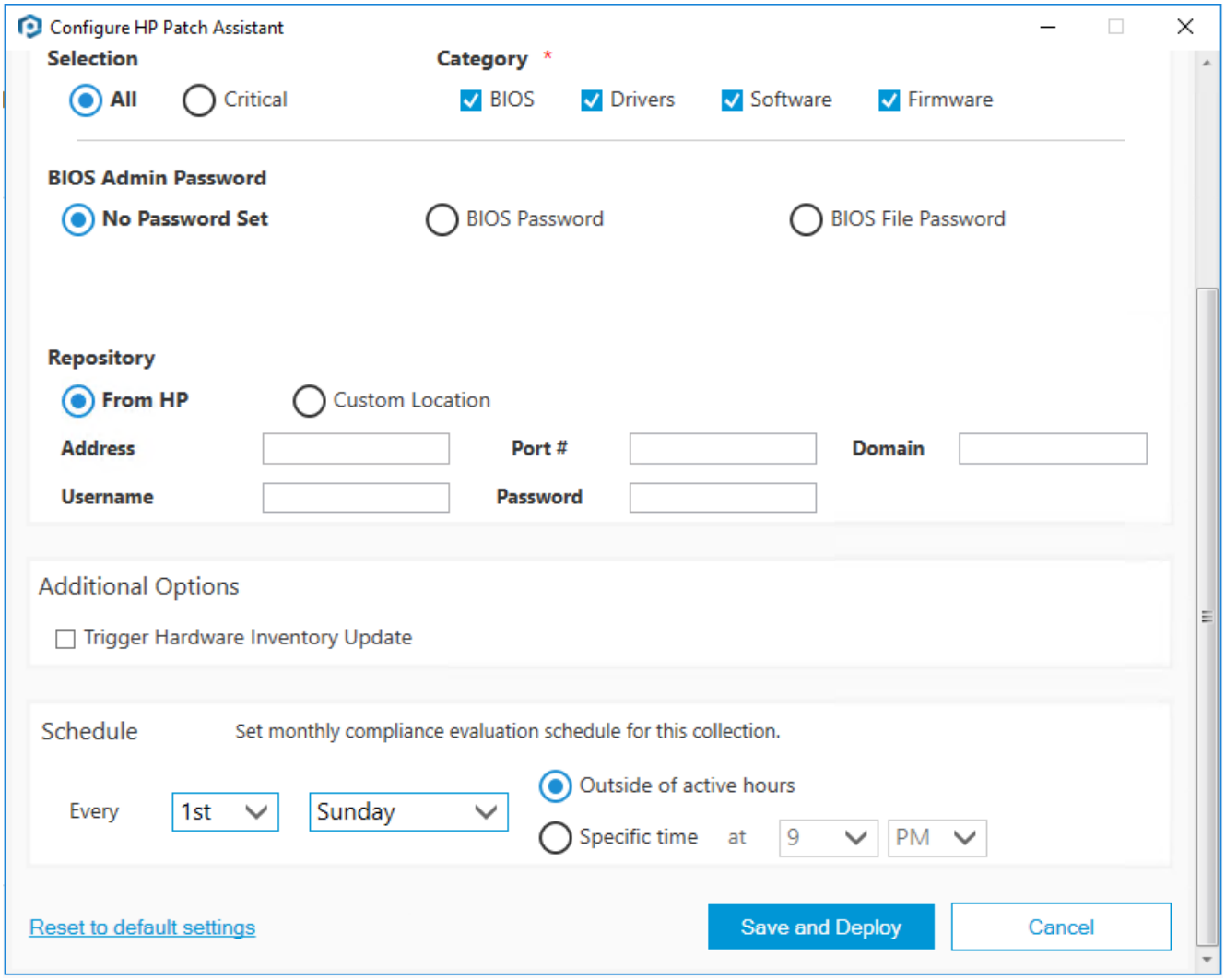
Users can configure HP patch Assistant for a specific device collection, by selecting a device collection under SCCM "**Device Collection**" node and right-click, from the menu option for HP Patch Assistant.



Select sub menu "**Configure Settings**"



Scroll down to Schedule and Save and Deploy Policy.

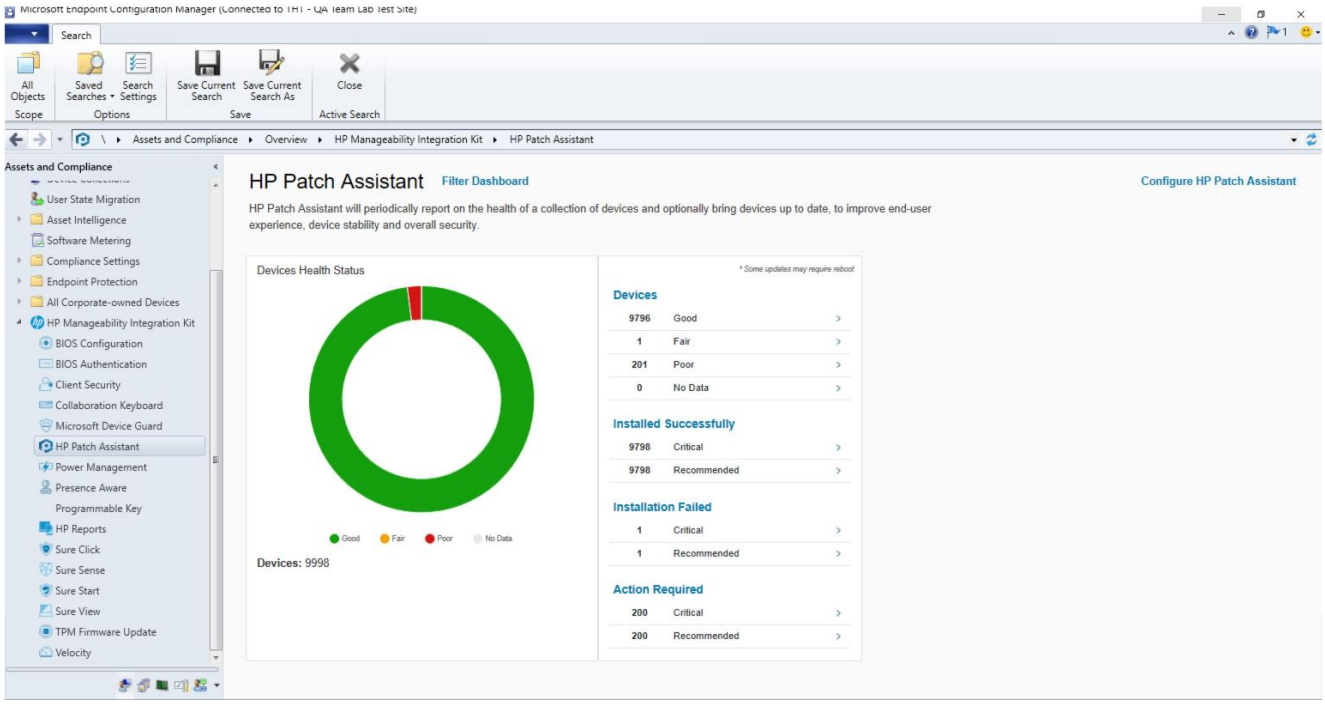


Configuration Settings

Settings Name	Options
Operation	Select the action to perform Report – Retrieves the list of recommendations. Report & Remediations – Downloads and Installs all recommendations.
Preferences	**Selection** **All** – All Recommendations – OR- **Critical** – Only Critical Recommendations. **Category** All – selected by default User can select any individual category for BIOS, Drivers, Software, Firmware. Note if you select Report & Remediations operation

	- Updates for 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.**
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 documentation https://developers.hp.com/hp-client-management/doc/client-management-script-library
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

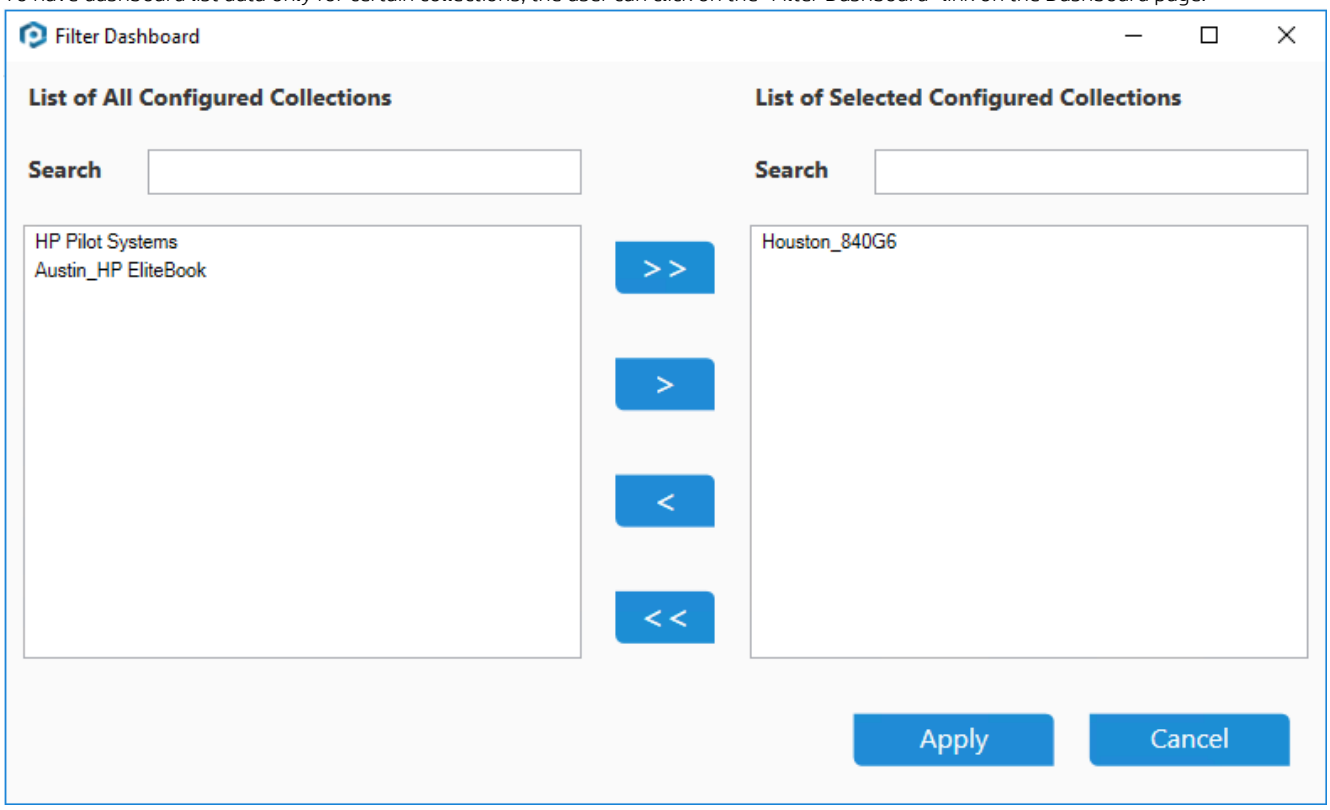


Dashboard will display device health status for devices which has HP Patch configured and data synched with SCCM.

Data Category	Description
Good	Device does not require any updates.
Fair	Device has at least 1 recommended update and not remediated.
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 dashboard list data only for certain collections, the user can click on the “Filter Dashboard” link on the Dashboard page.

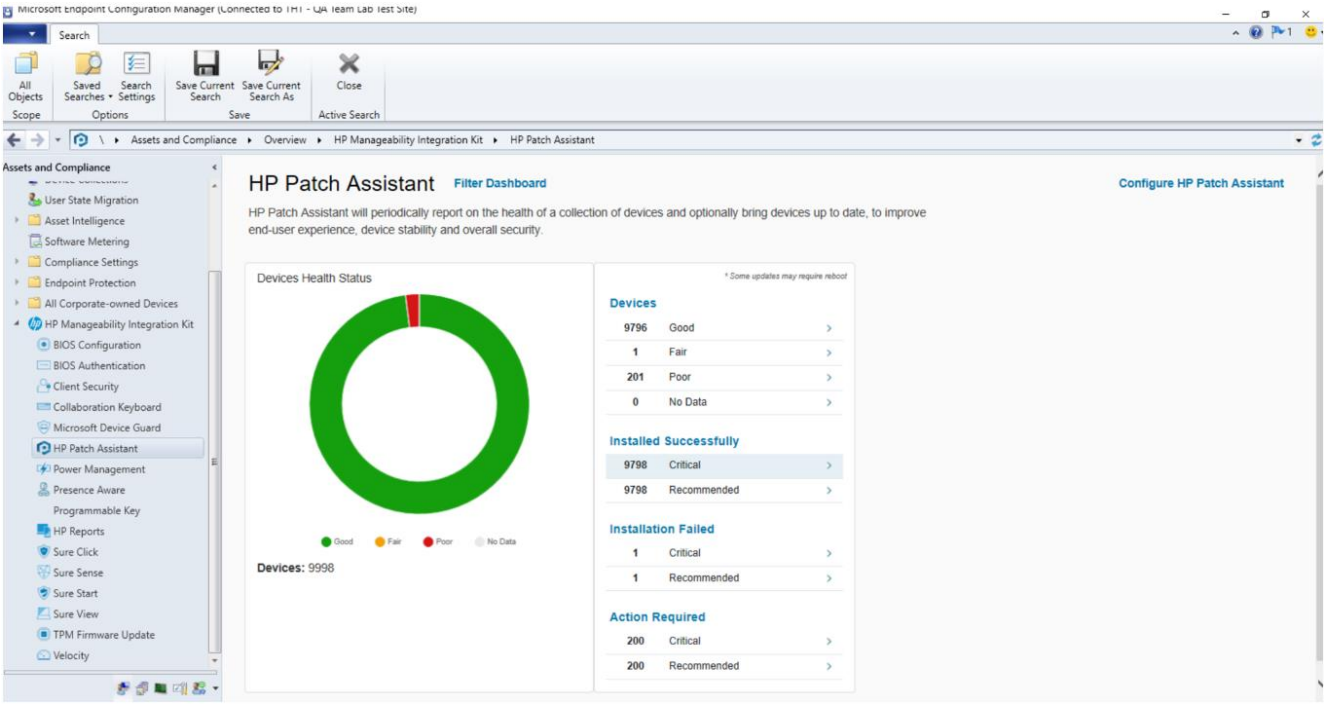


The left list box shows the device collections that have been configured for HP Patch Assistant.
Use the arrow buttons to add / remove collections. Click Apply. The dashboard will now display only data for the selected collections.

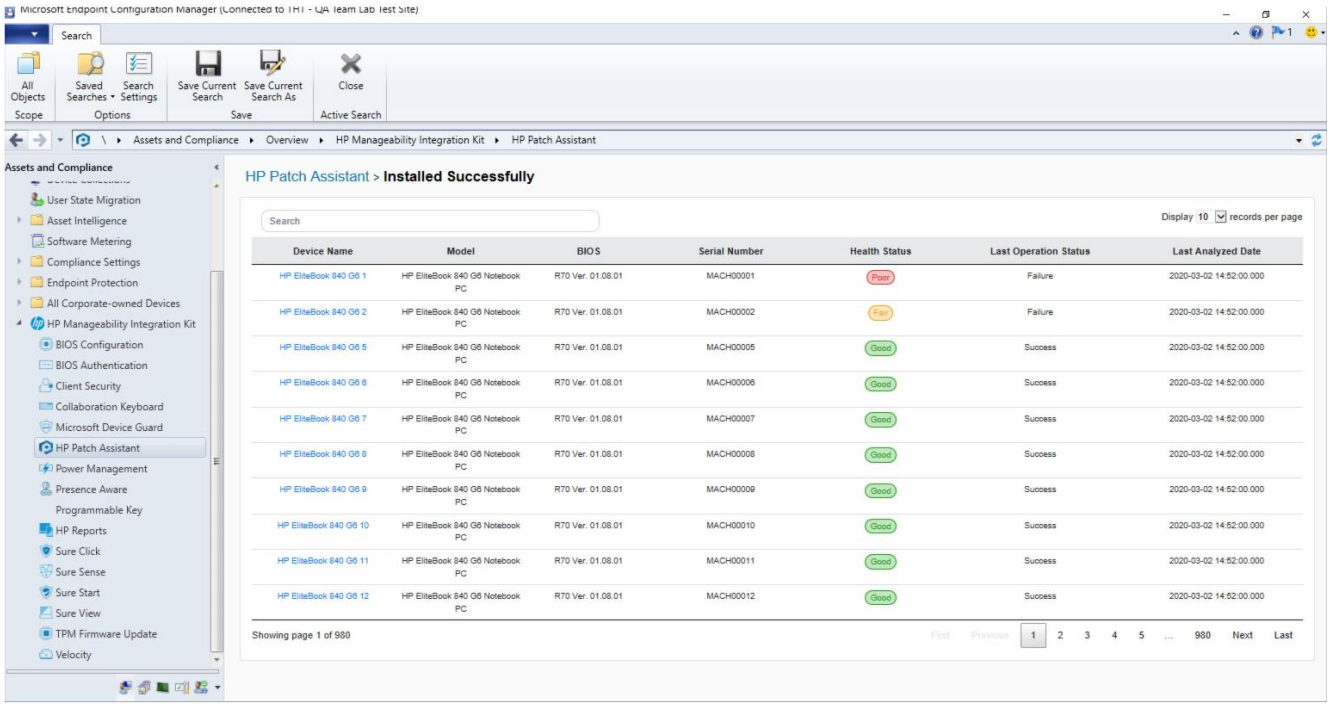
Note - The selection will last for the current SCCM sessions. If HP Patch Assistant is configured for any new collection, the user needs to manually add that collection.

View Report from Dashboard

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

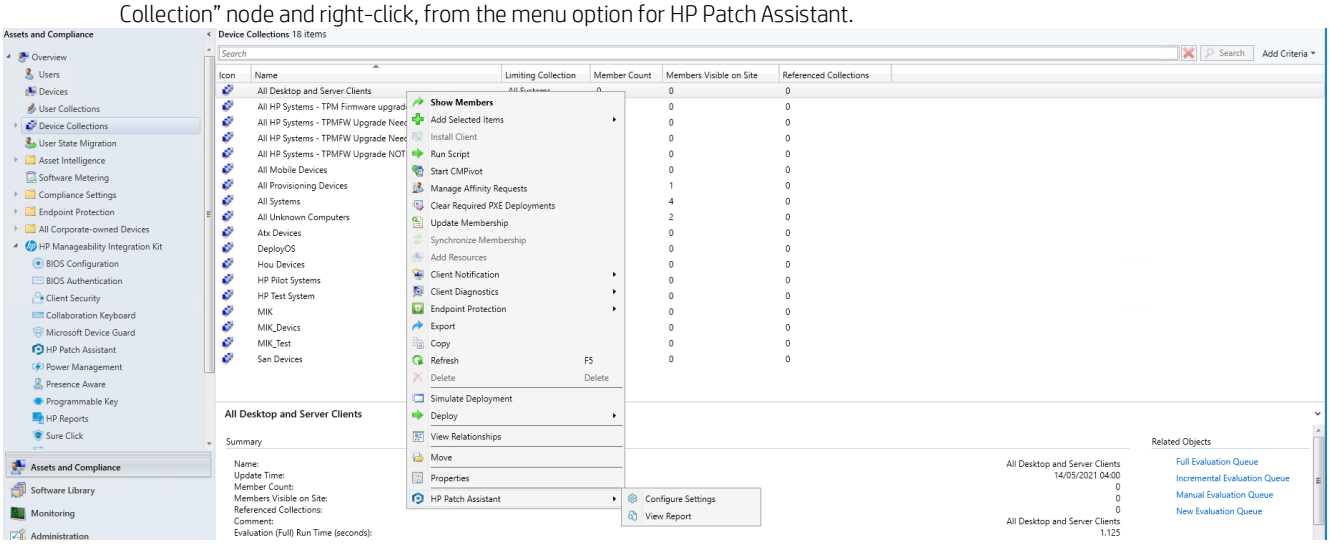


For example click on Installation Successful link.

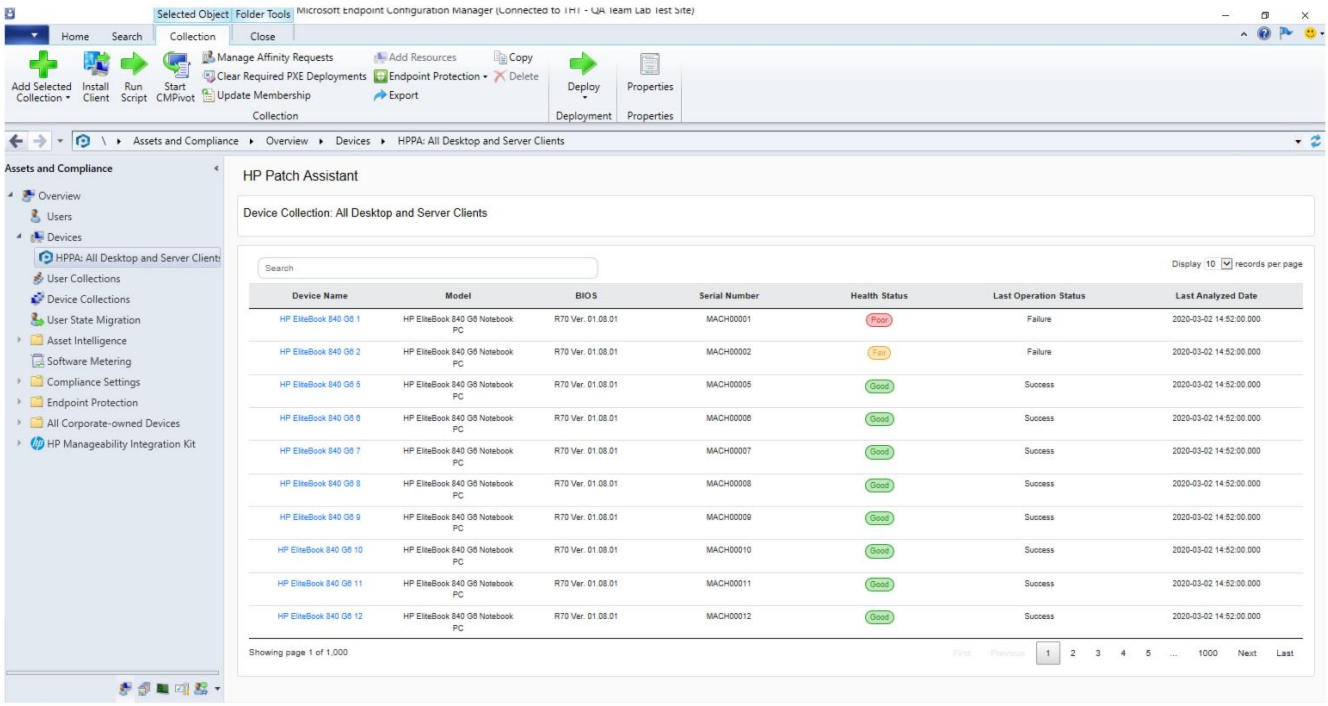


View Report for a device collection

Users can configure HP Patch Assistant for a specific device collection, by selecting a device collection under SCCM “Device Collection” node and right-click, from the menu option for HP Patch Assistant.

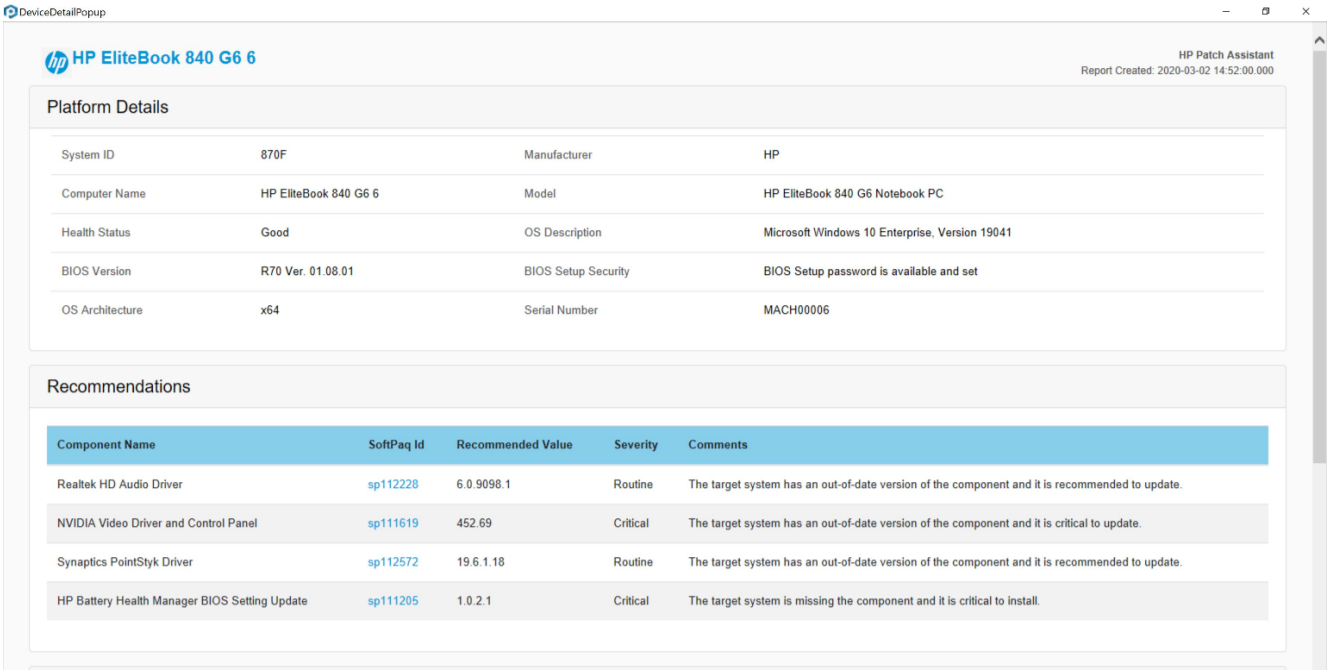


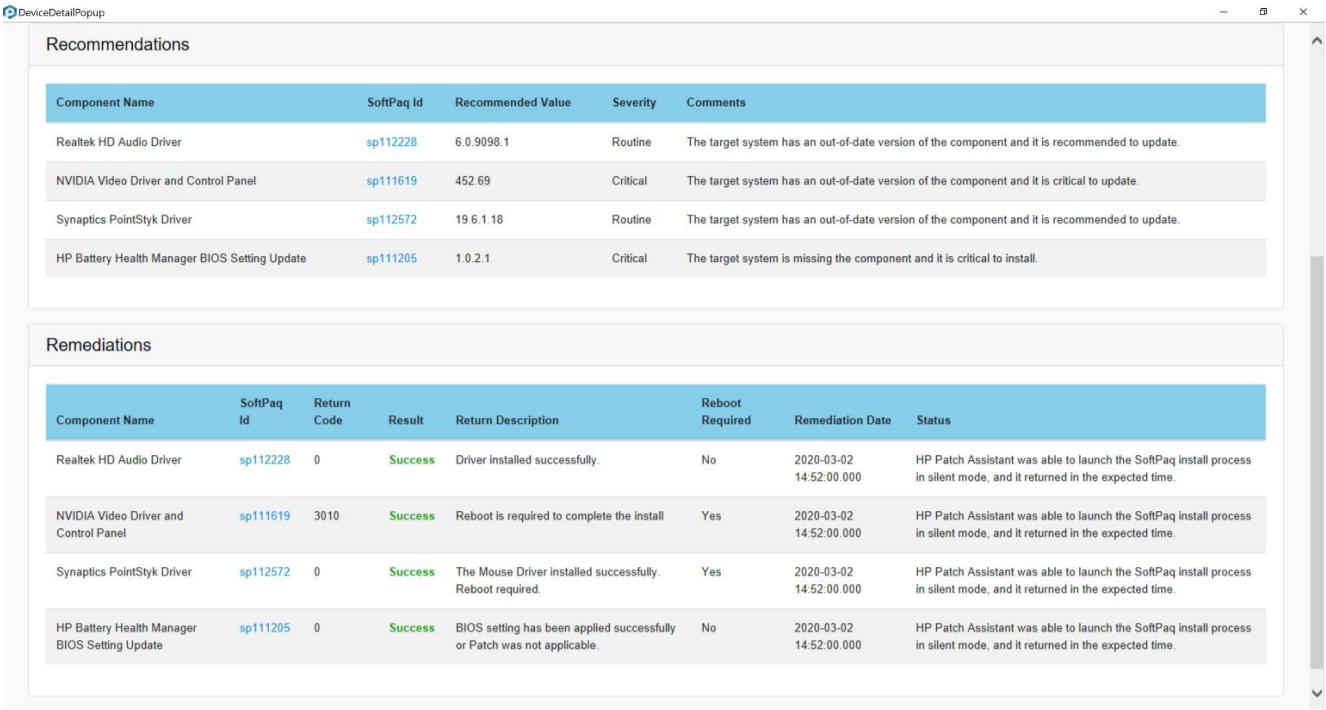
Select “View Report” from sub-menu.



Device Report

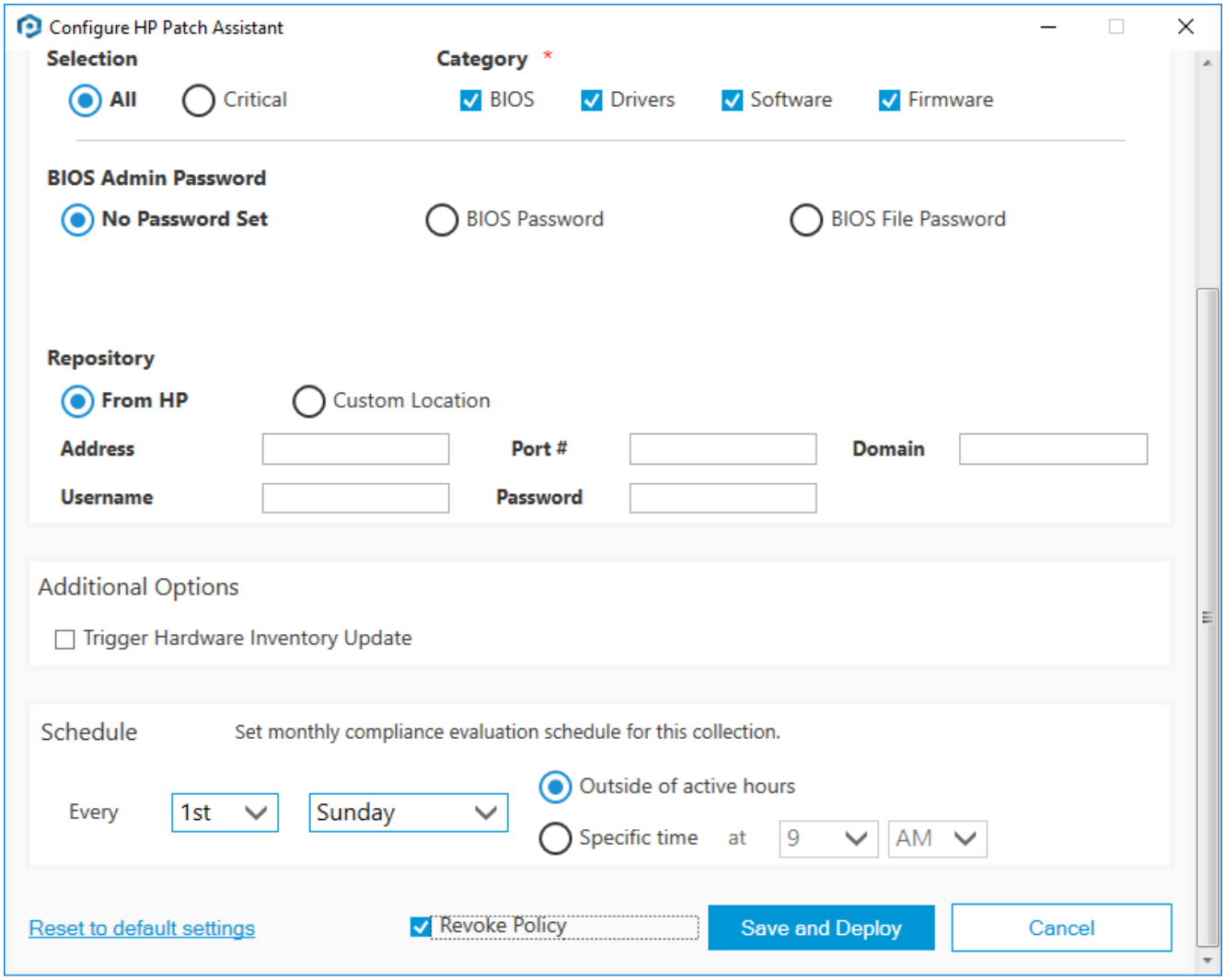
For a detailed report on a device, please click on the device name.





Remove HP Patch Assistant configuration

Navigate to SCCM “Device Collection” node. Select the device collection for which HP Patch Assistant policy was configured and deployed. Right-click and from the menu option for HP Patch Assistant, select option “**Configure Settings**”.



Check Revoke Policy and Save and Deploy. On Policy evaluation HP Patch Assistant configuration will be removed.

26 Uninstalling HP MIK

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

Any imported driver packages and boot images, and task sequences created by HP MIK remain on the server. The supporting client packages and source files are deleted; however, to preserve the BIOS configuration files, the source folder for BCU is not deleted.

27 Appendix 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 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://blogs.technet.microsoft.com/enterprisemobility/2015/10/30/managing-windows-10-device-guard-withconfiguration-manager/ and follow the steps in the *Determine applicable systems* section.

28 Appendix 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 Sure Start version information to the Configuration Manager default client settings:

1. In Configuration Manager, select Administration workspace. 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 the user 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 = '<Application product
ID>' and Version

>= '<Miminum supported application version>')

or (SMS_R_System.ResourceId in (select ResourceId from
SMS_G_System_ADD_REMOVE_PROGRAMS where ProdID = '<Application product ID>'
and Version >= '<Miminum supported application 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') ))
```

Systems with Intel Authenticate or a valid Intel Authenticate policy enforced for HP Client Security

For all HP systems that have HP Client Security (with HP MIK support) installed, the WMI class CM_IntelAuthenticatePolicies with the properties State and IsValidPolicyInstalled can be retrieved via the Configuration Manager hardware inventory extension.

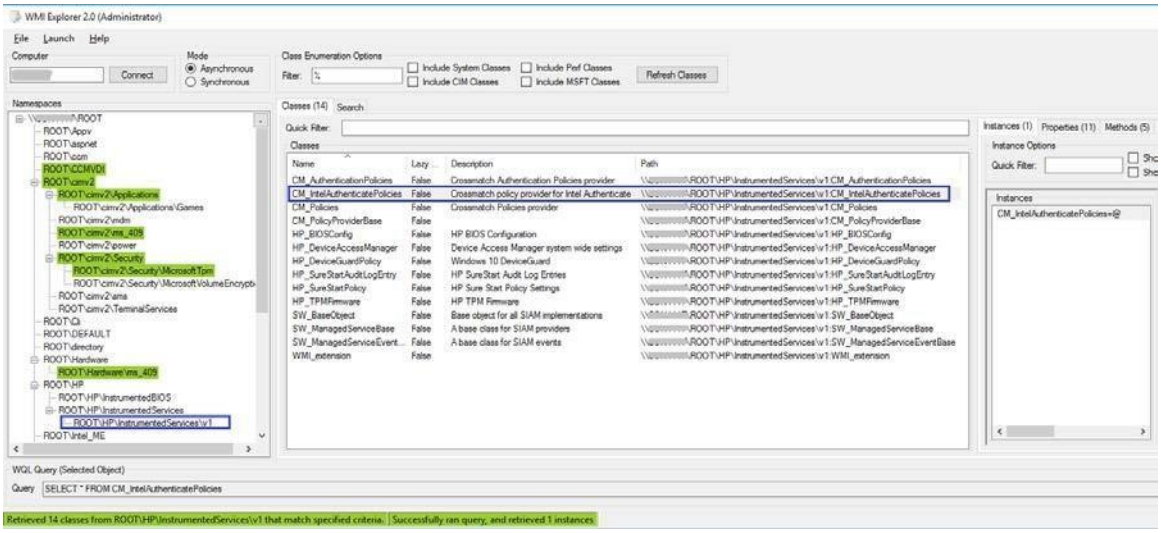
To add CM_IntelAuthenticatePolicies to the Configuration Manager default client settings:

1. In Configuration Manager, select Administration workspace. 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 and HP Client Security 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 and HP Client Security installed.
7. Enter `root\HP\InstrumentedServices\v1` for the WMI namespace.
8. Select Recursive, and enter the user name and password to connect to the WMI of the specified system.
9. Add the CM_IntelAuthenticatePolicies class. Select OK to add the class to hardware inventory.
10. Select OK, and then select OK again to close all windows.

After a client computer downloads the updated machine policy and runs the hardware inventory cycle, the extended data is reported to Configuration Manager. The data then is available to create collections.

The following image shows the CM_IntelAuthenticatePolicies WMI Class on a client computer.



The following query selects all HP systems that are ready to receive a valid Intel Authenticate policy for HP Client Security.

```
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_CM_IntelAuthenticatePolicies on
SMS_R_System.ResourceId =
SMS_G_System_CM_IntelAuthenticatePolicies.ResourceId  and
SMS_G_System_CM_IntelAuthenticatePolicies.State = 'Active'
```

If a system does not have Intel Authenticate installed, its `State` returns `NotInstalled`, meaning that Intel Authenticate has either not been installed or failed to install. Install Intel Authenticate and restart the client computer to enable HP Client Security to detect the status change.

Similarly, the query to select all HP systems that have a valid Intel Authenticate policy for HP Client Security enabled is as follows:

```
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_CM_IntelAuthenticatePolicies on
SMS_R_System.ResourceId =
SMS_G_System_CM_IntelAuthenticatePolicies.ResourceId

and SMS_G_System_CM_IntelAuthenticatePolicies.IsValidPolicyInstalled
='True'
```

If a system does not have a valid Intel Authenticate policy for HP Client Security, the `IsValidPolicyInstalled` property returns False.

29 Appendix C - Troubleshooting

HP MIK installation issues

An error occurred while installing a supporting package (HP Client BIOS Configuration Utility or HP Client Support Tools) Verify that the user 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

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

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. Please try the operation
again.
```

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

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, as follows:

- 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

The error "There may be too many steps in the task sequence object" appears 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 I 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

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.

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:

- Select Administration, select Site Configuration, and then select Server and Site System Roles.
- Select the appropriate distribution point.
- 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:

5. Select the driver pack.
6. Right-click and select Update Distribution Points.
7. 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:

8. Verify that PXE is placed before the hard drive in the boot order.

9. 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. Please 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 step 5 of Diagnosing driver pack or task sequence errors might also provide insight into the reason for failure.

Diagnosing driver pack or task sequence errors

10. Export the task sequence by right-clicking the task sequence and selecting Export.
11. If the issue appears, collect screen captures of the relevant portions.
12. If the issue is related to the installation of the product or occurs soon after installation:
    a. 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.`

    b. 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`.

13. 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.

14. 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.

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

    a. 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` and

    `%\SYSTEMROOT%\System32\config\systemprofile\AppData\Roaming\hpqLog\com.hp.si am.log`

16. 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:

    a. 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)

    b. A detailed description of the computers being configured (model, hardware configuration, and NIC details) – A description of other circumstances, such as the following:

        i. Has this task sequence or action ever worked? When did it stop working?

        ii. If it had 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?

30 Appendix D - Security Provisioning

For the client system to be successfully provisioned

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.

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.

Update 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).

For client system to be successfully un-provisioned.

1. Multiple "Evaluate" attempts (within SCCM Configuration Manager) may 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.

Systems which fail 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).

What to do if the signing key or endorsement certificate are lost

It is possible to manually deprovision HP Sure Run and HP Sure Recover by using the "Unprovision SPM" option on 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 / Sure Recover

Security Provisioning is needed to enable HP Sure Admin / HP Sure Run / HP Sure Recover.

For collection of system:

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.

31 Appendix E - Sure Run / Sure Recover / Sure Admin Key Generation for 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 addition, the hope is that in the future the firmware will enforce the requirement of the certificate being an EV certificate. In the meantime, 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.

WARNING: 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:

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. This information may be reported to users and admins in future versions of the firmware so it should be correct.

3. 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" – it is **REQUIRED** that you just press ENTER (i.e., no 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.

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):

```
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"
```

In this step you will be prompted for the "Export Password" – it is **REQUIRED** that you just press ENTER (i.e., no 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.

A few notes:

- Once the user has pressed the 'Submit Certificate' button 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. Key Points to be noted –

1. Only 10 custom processes can be added.
2. If new custom process is part of Standard Category, it will not be saved.
3. 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.

When 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.
- Note- At this time environment variables like, %ProgramFiles% and %ProgramFiles(x86)%, can NOT be used in the path.

How to find 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 and available on the Microsoft website (https://docs.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.

Updating the item being watched

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

32 Appendix F - HP Sure Admin

Passphrase for additional security

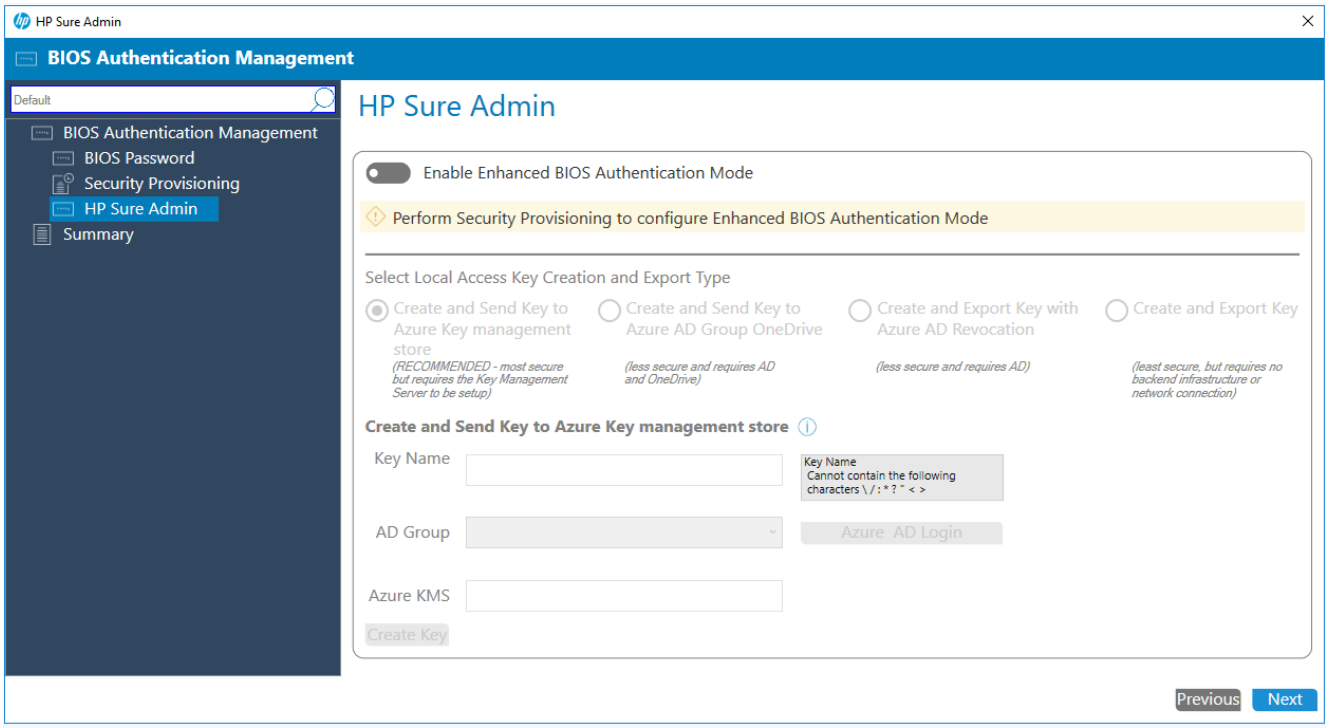
ITDM can control access to QR Code with passphrase.

Passphrase Rules

Allowable characters are upper/lowercase characters, numbers and special characters other than < or >.
Note – Current limitations.

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

Security Provisioning needed for HP Sure Admin



Note - If provisioning step is skipped, 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

User need to ensure 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.

Our analysis indicates that min 2 or max 4 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.
- Now IDTM can schedule policies to set BIOS settings or configuration of Client security S/W.

Other Information

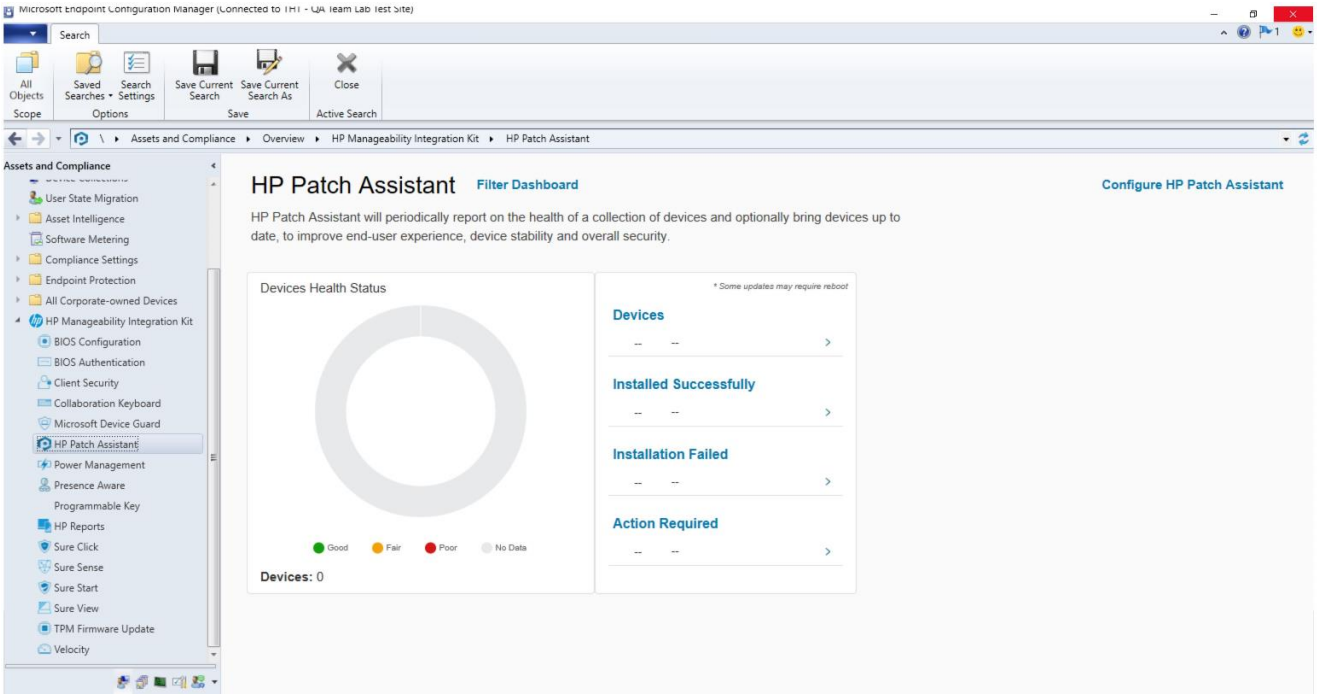
Existing legacy Baselines created for HP BIOS Password can be accessed using the new BIOS Authentication Plugin.

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

HP's recommendation to use HP Sure Admin for enhanced security.

33 Appendix - HP Patch Assistant

HP Patch Assistant Configured for a device collection – Data not yet synched with SCCM



34 For more information

For all your client manageability needs, go to the HP Client Management Solutions website: 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.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

May 2021