HP Connect for Microsoft Endpoint Manager - User Guide

DISCLAIMER: Content may be changed at any time

Table of Contents

HP Connect for Microsoft Endpoint Manager

HP Connect for Microsoft Endpoint Manager (https://admin.hp.com) is a cloud application designed to ease the management of UEFI BIOS on supported HP systems. HP Connect has a framework to develop BIOS management policies that are published to Microsoft Endpoint Manager device groups.

While HP Connect creates the policies, Endpoint Manager (Intune) executes them as compliance proactive remediations. No additional software is required to be downloaded or installed in each device.

HP Connect for Microsoft Endpoint Manager supports the following type of policies:

- BIOS Updates
  - Always up to date
  - Critical versions only
  - specific version for a platform
- BIOS Settings
  - Supported on a per platform basis
  - Global Settings policy applies across platforms
- BIOS Authentication
  - HP Sure Admin (HP Sure Admin Info sheet)
  - Passwords

Requirements

The following is necessary to use HP Connect for Microsoft Endpoint Manager (HP Connect):

- Administrative access to a Microsoft Azure tenant
- An appropriate Microsoft Endpoint Manager (MEM) subscription
  - Including support for Proactive Remediations
- MEM configured as the MDM for device management
- Modern Internet browser (Microsoft Edge, Google Chrome, Mozilla Firefox, etc.)

HP Connect requires an appropriate subscription level to Microsoft Azure (example, E3/A3 and E5/A5, Virtual Desktop/user)[1]. The license must allow the use of Proactive Remediations.

As a cloud application, HP Connect interacts directly with an Azure Active Directory (AAD) tenant to access device groups and to publish BIOS policies to these groups.

[1] Licensing section at Tutorial - Proactive remediations - Microsoft Endpoint Manager | Microsoft Docs discusses the requirements to allow the use of proactive remediations

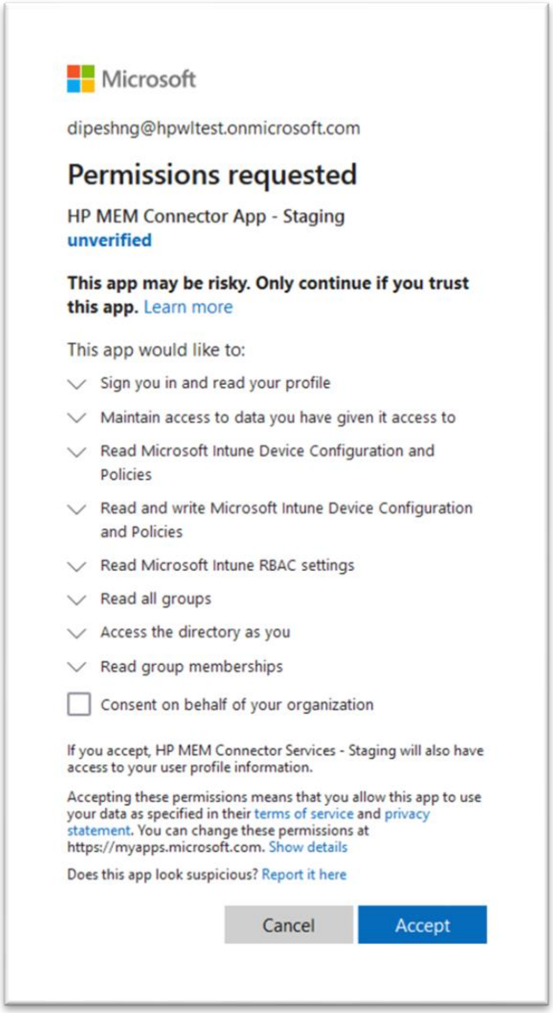
Policies created by HP Connect are published to and enforced by MEM as proactive remediations. HP Connect interacts with Endpoint Manager via Microsoft Graph API.

No additional storage is currently required in an organization' Azure tenant.

To interact with Microsoft Azure Active Directory and Endpoint Manager, HP Connect requires certain permissions to access the company tenant. Permissions are used to search for and obtain device group information, and to publish policies. A tenant Global Administrator can accept these permissions on behalf of the entire organization. See **Appendix C** for additional details on required permissions.

Onboarding Process

To allow HP Connect for MEM to integrate with the Azure tenant as an Enterprise Application, a Global tenant Administrator must initially login at https://admin.hp.com with Azure credentials and accept the required permissions. The permissions are accepted via a standard Microsoft dialog.



Microsoft

dipeshng@hpwltest.onmicrosoft.com

Permissions requested

HP MEM Connector App - Staging
unverified

This app may be risky. Only continue if you trust this app. Learn more

This app would like to:

- Sign you in and read your profile
- Maintain access to data you have given it access to
- Read Microsoft Intune Device Configuration and Policies
- Read and write Microsoft Intune Device Configuration and Policies
- Read Microsoft Intune RBAC settings
- Read all groups
- Access the directory as you
- Read group memberships

□ Consent on behalf of your organization

If you accept, HP MEM Connector Services - Staging will also have access to your user profile information.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

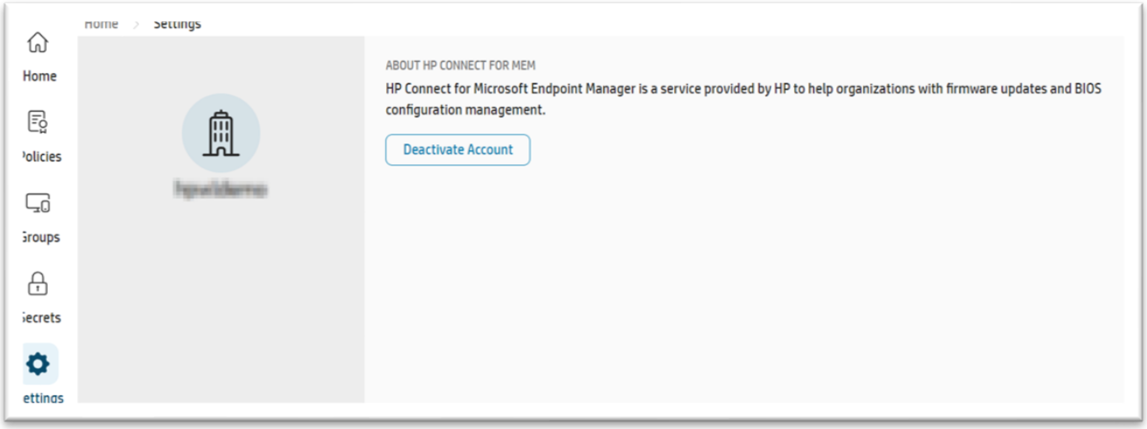
As shown in the Microsoft permissions dialog, most of the permissions are Read-Only, except for one. HP Connect requires write access to device configuration and policies.

After the initial access, an Intune Administrator will be able to login and use HP Connect at admin.hp.com after accepting permissions. The Global Administrator can, if desired, accept permissions for all other administrators by setting the 'Consent on behalf of your organization' checkmark in the dialog.

Appendix C describes the Permissions required for HP Connect to interact with Microsoft Endpoint Manager

Offboarding Process

Organizations can terminate use of HP Connect by selecting *Deactivate Account* from the **Settings** menu



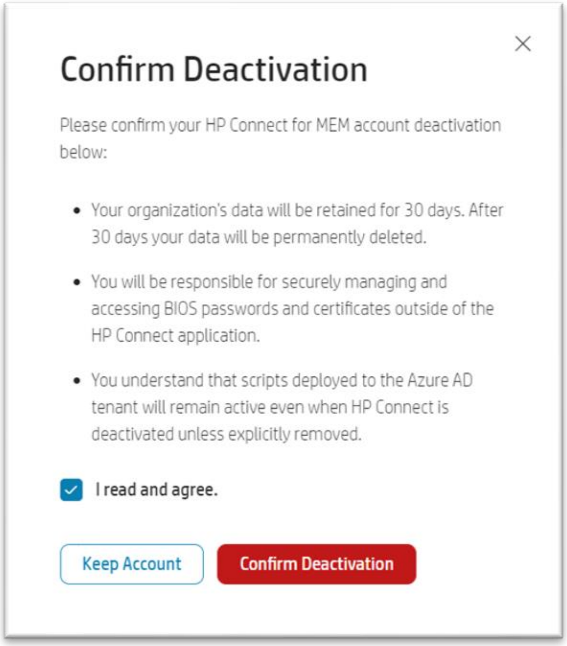
ABOUT HP CONNECT FOR MEM

HP Connect for Microsoft Endpoint Manager is a service provided by HP to help organizations with firmware updates and BIOS configuration management.

The Deactivate Account screen will display what happens next when the account is deactivated. At this point, you can press *Keep Account* to stop the process or start the clock on full deactivation by selecting *Proceed with Deactivation*.

Deactivation starts a 30-day countdown where tenant administrators will be able to login to admin.hp.com in read only mode (view only). At the end of the 30 days, all policies and secrets created by the organization in HP Connect will be permanently deleted. Please, review the details in the Deactivation screen to understand what will be set in motion. Also, the Microsoft Endpoint Manager Proactive Remediation scripts published by HP Connect to AAD will remain in place. If these Remediations are no longer required, they need to be manually removed from MEM.

At the final confirmation dialog check '*I read and agree*' and then *Confirm Deactivation* to start the process.



Confirm Deactivation

Please confirm your HP Connect for MEM account deactivation below:

- Your organization's data will be retained for 30 days. After 30 days your data will be permanently deleted.
- You will be responsible for securely managing and accessing BIOS passwords and certificates outside of the HP Connect application.
- You understand that scripts deployed to the Azure AD tenant will remain active even when HP Connect is deactivated unless explicitly removed.

☑ I read and agree.

The account can be reactivated during the next 30 days by logging back into HP Connect at admin.hp.com and selecting *Reactivate Account*. A Global Administrator is required to reactivate the account.

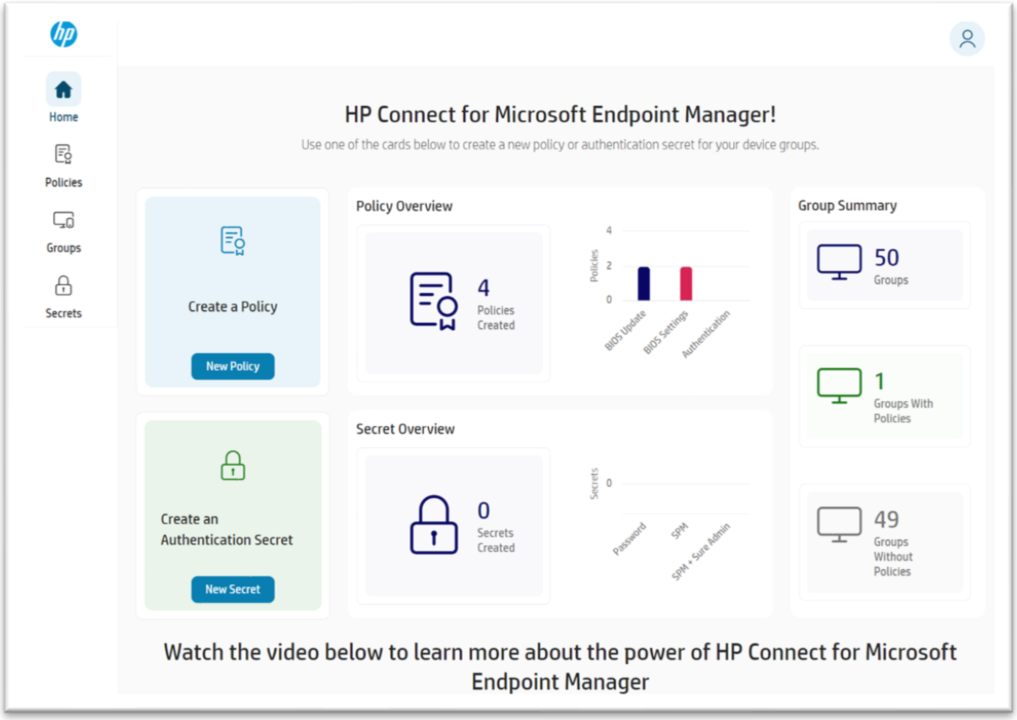
During (30 day) deactivation period, an Intune Administrator can login to admin.hp.com where a banner will inform of the action being taken. Again, to reverse deactivation, a Tenant global administrator will be required to login and restore access.

The HP Connect Sidebar Menu

When logging into HP Connect, a dashboard with useful information will be displayed. A sidebar menu allows easy access to policies, groups, and (authentication) secrets stored in an HP vault.

The Home Tab

On login, the home dashboard page is displayed.



HP Connect for Microsoft Endpoint Manager!

Use one of the cards below to create a new policy or authentication secret for your device groups.

Watch the video below to learn more about the power of HP Connect for Microsoft Endpoint Manager

From the dashboard, policies can be created by selecting *New Policy*, and authentication secrets can be added to the secrets vault with the *New Secret* button. Authentication secrets can be used when defining a policy to implement HP Sure Admin BIOS protection (a secure authentication mechanism utilizing cryptographic certificates), as well as for setting, or managing, BIOS passwords.

In addition, the home page dashboard displays an Overview of the Policies, Secrets created, and their status.

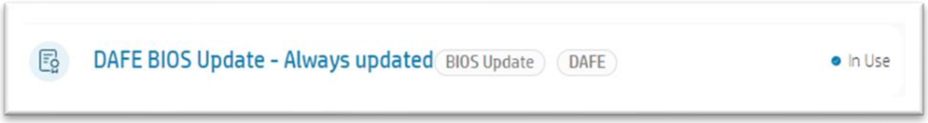
A Group Summary card displays the Azure Directory Groups read from Azure and groups with HP Connect policies applied to them.

At the bottom of the home screen, discovery information can be found about HP Connect and other HP endpoint management solutions, such as the HP TechPulse service.

The Policies Tab

Selecting the Policies menu tab lists created policies. Each policy in the list shows if it is ' In Use' (e.g., policy published to a device group) or is 'Not In Use'.

Example of policy shown as In Use

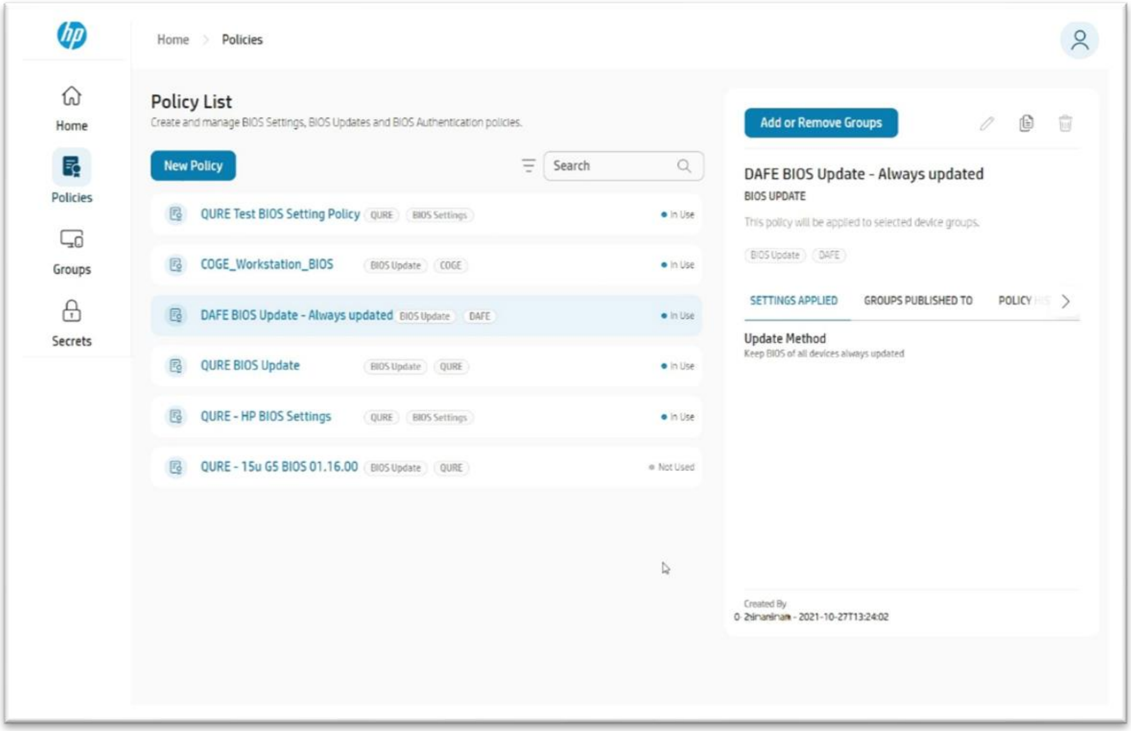


DAFE BIOS Update - Always updated BIOS Update DAFE ● In Use

Creating a Policy

A *New Policy* can be created from this menu.

Once a policy is created, it can be published to, or removed, from device groups by clicking on *Add or Remove Groups*. If a group is added or removed and the policy is re-applied to Endpoint Manager, it will affect all existing policies in that group. In addition, the policy version number shown by MEM will increment.



Policy List

Create and manage BIOS Settings, BIOS Updates and BIOS Authentication policies.

QURE Test BIOS Setting Policy	QURE	BIOS Settings	● In Use
COGE_Workstation_BIOS	BIOS Update	COGE	● In Use
DAFE BIOS Update - Always updated	BIOS Update	DAFE	● In Use
QURE BIOS Update	BIOS Update	QURE	● In Use
QURE - HP BIOS Settings	QURE	BIOS Settings	● In Use
QURE - 15u G5 BIOS 01.16.00	BIOS Update	QURE	● Not Used

DAFE BIOS Update - Always updated

BIOS UPDATE

This policy will be applied to selected device groups.

BIOS Update DAFE

SETTINGS APPLIED | GROUPS PUBLISHED TO | POLICY

Update Method

Keep BIOS of all devices always updated

Created By

[illegible] - 2021-10-27T13:24:02

Once applied to a Group (or multiple groups) of devices, the Policy entry will show as In Use, and cannot be edited.

Editing a Policy

A policy can be edited if it is not currently published to a device group. To edit a Policy that has been published and applied to a device group, select it from the list, then click on *Add or Remove Groups*, unselect all groups and *save*.

Certain edits may generate a conflict and might not be possible to publish. For example, editing a BIOS Settings policy that applies to a particular platform cannot be reassigned to a different platform, as BIOS settings may or may not be the same for both platforms. In this case, a new BIOS Settings policy needs to be created.

Deleting a Policy by clicking on the trash-icon removes it immediately from HP Connect.

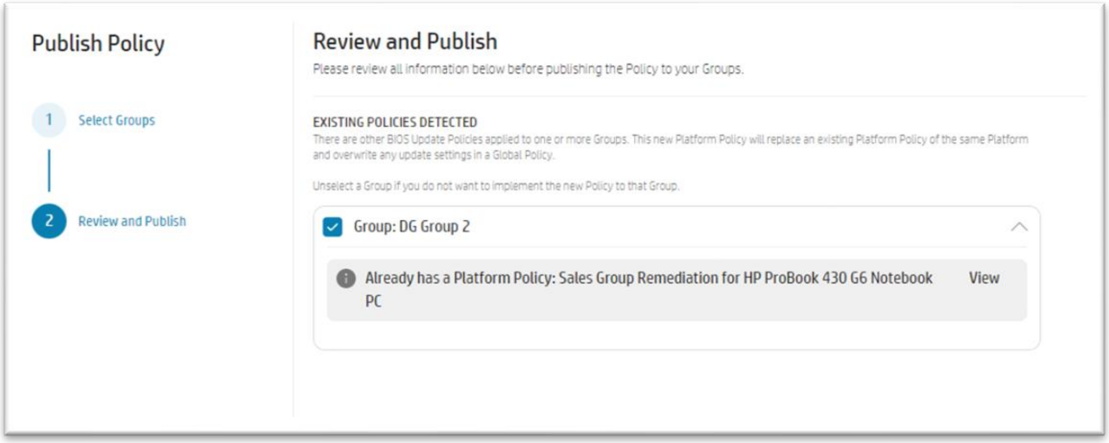
Adding/Removing Groups to a Policy

For a policy to be enforced on HP supported devices, it must be published to an Azure AD device group. A device group can also be removed from the policy. When adding or removing Connect policies from a device group, any existing published policies (for the selected group) will be recreated with the changes made.

To add or remove device groups, in the Policy List window, select the Policy to be modified, and click on '*Add or Remove Groups'*. When adding an Endpoint Manager group and clicking on *Save*, a dialog asks to '*Publish'* or just '*Close'* to save the Policy without publishing. If selecting '*Publish'*, the policy is updated to the organization's tenant, where will then be enforced via its remediation and compliance task.

Policy Conflict Resolution – Feature Change!

If an existing group device Policy exists for a similar type (Updates, Settings, Authentication) for the same platform, it will result in a conflict, and the new policy will replace existing policy when published.



Review and Publish

Please review all information below before publishing the Policy to your Groups.

EXISTING POLICIES DETECTED

There are other BIOS Update Policies applied to one or more Groups. This new Platform Policy will replace an existing Platform Policy of the same Platform and overwrite any update settings in a Global Policy.

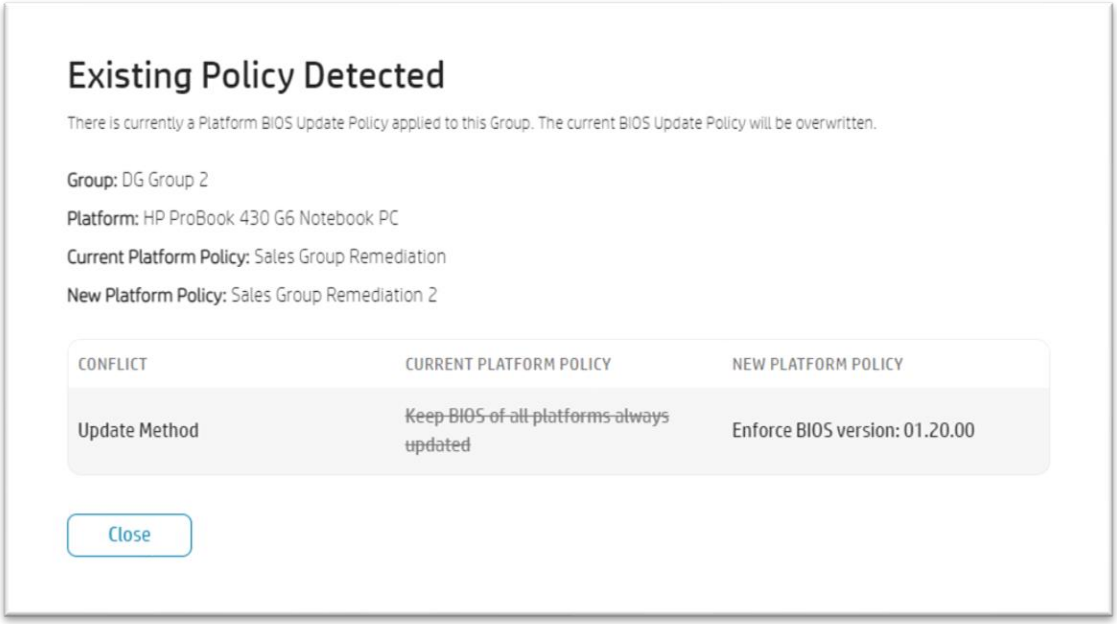
Unselect a Group if you do not want to implement the new Policy to that Group.

☑ Group: DG Group 2

Already has a Platform Policy: Sales Group Remediation for HP ProBook 430 G6 Notebook PC

User can prevent the new policy from overwriting the existing policy by unchecking the Group selection in the conflict dialog. User will no longer need to resolve the conflict by confirming to Apply new policy or keep current policy. User can View the difference by clicking on the View button.

The View dialog will display the current policy and the effects of publishing the new policy.



Existing Policy Detected

There is currently a Platform BIOS Update Policy applied to this Group. The current BIOS Update Policy will be overwritten.

Group: DG Group 2

Platform: HP ProBook 430 G6 Notebook PC

Current Platform Policy: Sales Group Remediation

New Platform Policy: Sales Group Remediation 2

CONFLICT	CURRENT PLATFORM POLICY	NEW PLATFORM POLICY
Update Method	~~Keep BIOS of all platforms always updated~~	Enforce BIOS version: 01.20.00

How is a Policy Applied

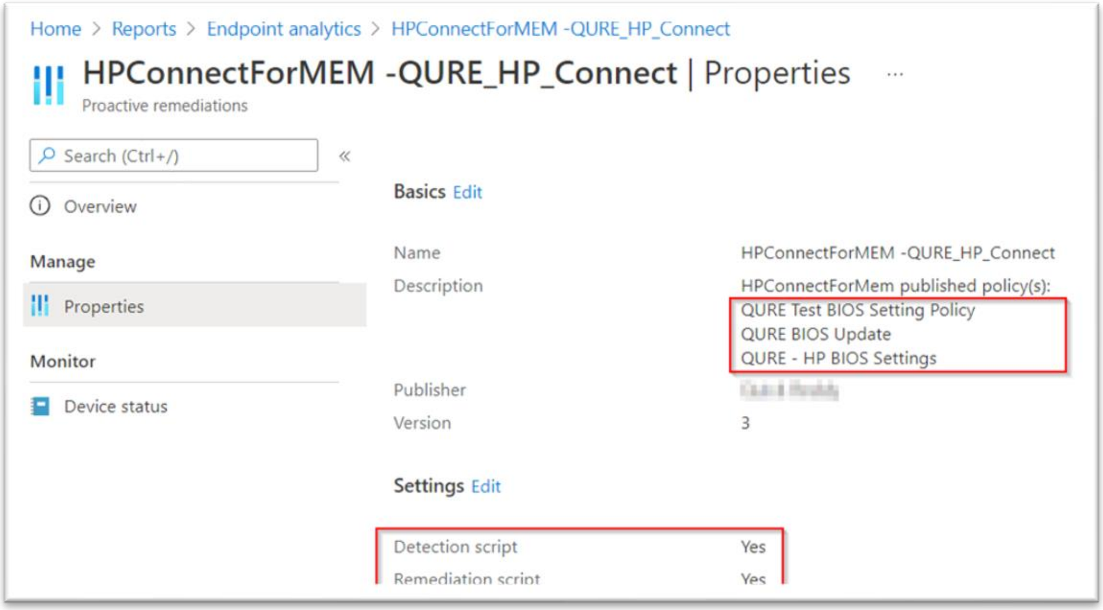
Once a BIOS policy is created and published to one or more Azure AD device groups, a compliance policy is created in MEM. If an HP Connect policy was already applied to the device group, the new policy will be added to the current policy (e.g., scripts recreated) and the version number increased.

HP Connect policies are published as proactive remediations and can be found on the Microsoft Endpoint Manager Admin Center under Reports, Endpoint Analytics, Proactive Remediations.

The proactive remediation compliance policy is named 'HPConnectforMEM - *device_group_name*'. Select the policy from the list to review its Properties and Device status.

Once selected, the published HP Connect policies will be listed under the Properties, *Description* field. In the Properties pane, you will see the HP Connect applied policies as well as the indicator that both Detection and Remediation scripts were applied (marked as 'Yes'), and the schedule (how often) the policy executes in this group.

Example of a compliance policy Properties pane displaying published HP Connect policies (3 Connect policies have been applied to this group):



Home > Reports > Endpoint analytics > HPConnectForMEM -QURE_HP_Connect

HPConnectForMEM -QURE_HP_Connect | Properties ...

Proactive remediations

Search (Ctrl+/) «

Overview

Manage

Properties

Monitor

Device status

Basics Edit

Name	HPConnectForMEM -QURE_HP_Connect
Description	HPConnectForMem published policy(s): QURE Test BIOS Setting Policy QURE BIOS Update QURE - HP BIOS Settings
Publisher	[redacted]
Version	3

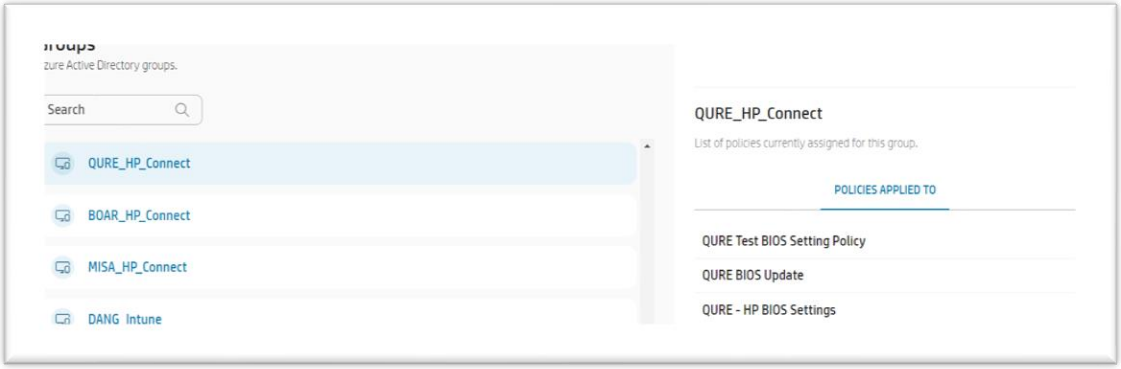
Settings Edit

Detection script	Yes
Remediation script	Yes

The Groups tab

The Groups sidebar menu displays a list of the organization's Azure Active defined Directory Groups. A search field allows the Administrator to quickly find specific groups by name.

Selecting a group name from the list will bring up a sidebar with a list of HP Connect policies already assigned to that group.



roups

zure Active Directory groups.

Search

QURE_HP_Connect

BOAR_HP_Connect

MISA_HP_Connect

DANG_Intune

QURE_HP_Connect

List of policies currently assigned for this group.

POLICIES APPLIED TO

QURE Test BIOS Setting Policy

QURE BIOS Update

QURE - HP BIOS Settings

The side properties card will also indicate when the policy was created, modified, and/or published.

The Secrets tab

The Secrets menu tab is where BIOS authentication secrets are managed in HP Connect. These secrets are stored in a secure cloud vault. Selecting *New Secret* will display a dialog where you can add certificates for use by HP Sure Admin or passwords to administer BIOS admin/setup passwords.

Both HP Sure Admin cryptography-based access control and passwords can be used by HP Connect to secure BIOS access by policy. Both types of authentication can not coexist on a device at the same time.

Adding Sure Admin secrets to the Vault

HP Sure Admin required certificates which must be provided. HP Connect will read the certificates and obtain the embedded private/public keys to configure HP Sure Admin. These cryptographic keys are then used when creating BIOS authentication policies, and to authorize (sign) BIOS settings changes.

Appendix A provides additional details on HP Sure Admin, and illustrates a step-step process for creating the required certificates (examples provided using OpenSSL).

To add a HP Sure Admin secret that will later be provisioned by policy to HP devices, follow these steps:

From the dashboard, select the *Secrets* sidebar tab and then select *New Secret*, or click on *New Secret* on the home page.

- In the Secret Information page fill in the following fields
  - *Name*

    It is useful to identify the purpose of the secret as part of the name

  - *Type* - select 'Certificate' from dropdown
  - *Certificate Type* – select either
    - Select '*Secure Platform Management* '

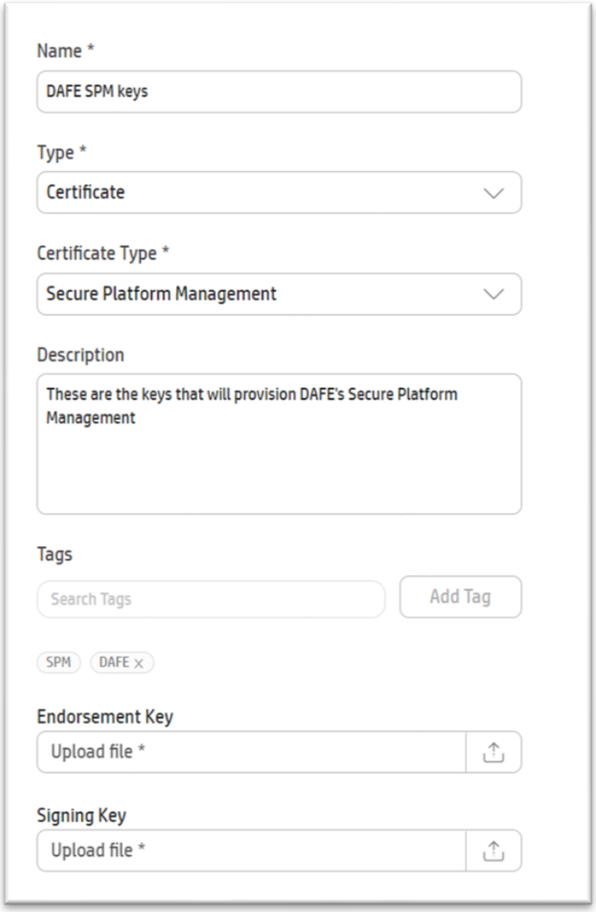
      The Secure Platform Management secret will help set up the trusted firmware environment required to enable HP Sure Admin, and for other future HP BIOS security needs

    or

    - '*Local Access'*

      An Individual secret will be used to allow secure access to the F10 BIOS Setup on a device. This is the LAK (Local Access Key)

  - *Description* – free format field
  - *Tags* – type a tag name and click *Add Tag.* Add as many tags as desired
  - *Endorsement Key* – the certificate in pfx format described in Appendix A
  - *Signing Key* – the certificate in pfx format described in Appendix A
- Click *Save*



Name *

DAFE SPM keys

Type *

Certificate

Certificate Type *

Secure Platform Management

Description

These are the keys that will provision DAFE's Secure Platform Management

Tags

Endorsement Key

Signing Key

- Repeat previous steps to add a new Local Access secret

If only the Secure Platform Management (SPM) keys are saved but not the Local Access key, HP Connect will use the Signing Key (saved as the SPM secret) as the Local Access Key.

Adding Password secrets to the Vault

Passwords are managed by HP Connect and stored in a cloud vault.

From the dashboard, select the *Secrets* sidebar tab and then select *New Secret*, or click on *New Secret* on the home page.

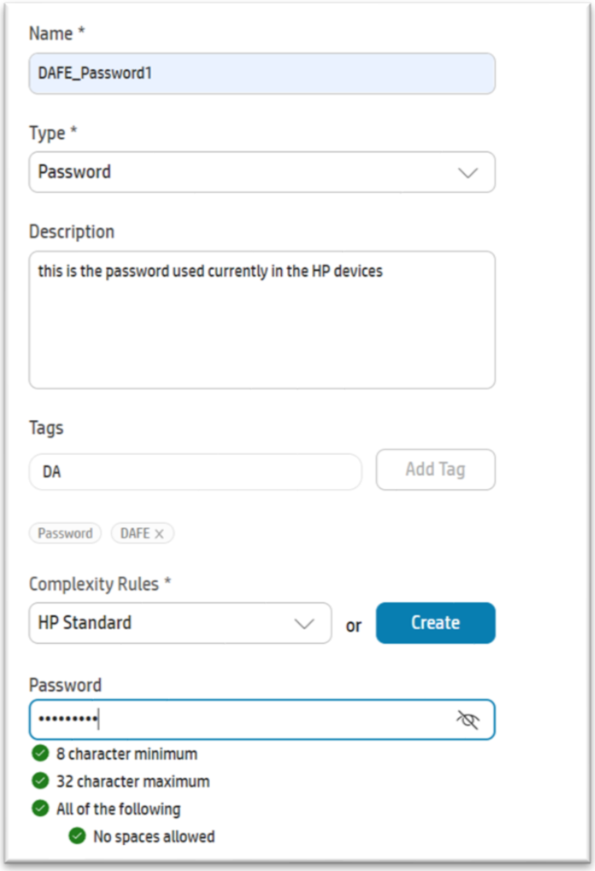
To add a Password secret to HP Connect,

- In the Secret Information page fill in the following fields
  - *Name*

    It is useful to identify the purpose of the secret as part of the name

  - *Type* - select 'Password' from the dropdown
  - *Description* – free format field

    - *Tags* – type a tag name and click *Add Tag.* Add as many tags as desired
    - *Complexity Rules* – select the default ‘HP Standard’ from the dropdown or create a new complexity rule
    - *Password* – type the password string meeting the selected complexity rule
- Click *Save*



Name *
DAFE_Password1

Type *
Password

Description
this is the password used currently in the HP devices

Tags
DA

Password
DAFE ×

Complexity Rules *
HP Standard

Password
•••••••••

✓ 8 character minimum
✓ 32 character maximum
✓ All of the following
  ✓ No spaces allowed

HP Connect Policies

BIOS Updates Policies

> *The HP BIOS setting 'Native OS Firmware Update Service' must be set to Enable (the default) to allow remote BIOS updates. A BIOS Updates policy sent to the device may fail if an older BIOS for a platform does not have the setting or the setting is set to Disable*

To analyze why a policy fails to apply to a device, use the guidelines in **Appendix B** to review the appropriate logs.

Following types of BIOS update policies supported by HP Connect:

- **Keep BIOS of all devices always updated**

  When applied to a group of supported platforms, Endpoint Manager will use the policy as a compliance item to monitor for and update every device in the selected group every time a BIOS is released that matches a device.

- **Deploy only critical BIOS updates**

  This policy will apply a new BIOS release if it is marked 'Critical' by HP to every device in the selected group.

- **Establish a rule for a specific device model**

  This policy will apply a BIOS update to a device group based on a defined criteria/rule. The policy is applied to a specific platform (HP model) only, and can be configured to, either

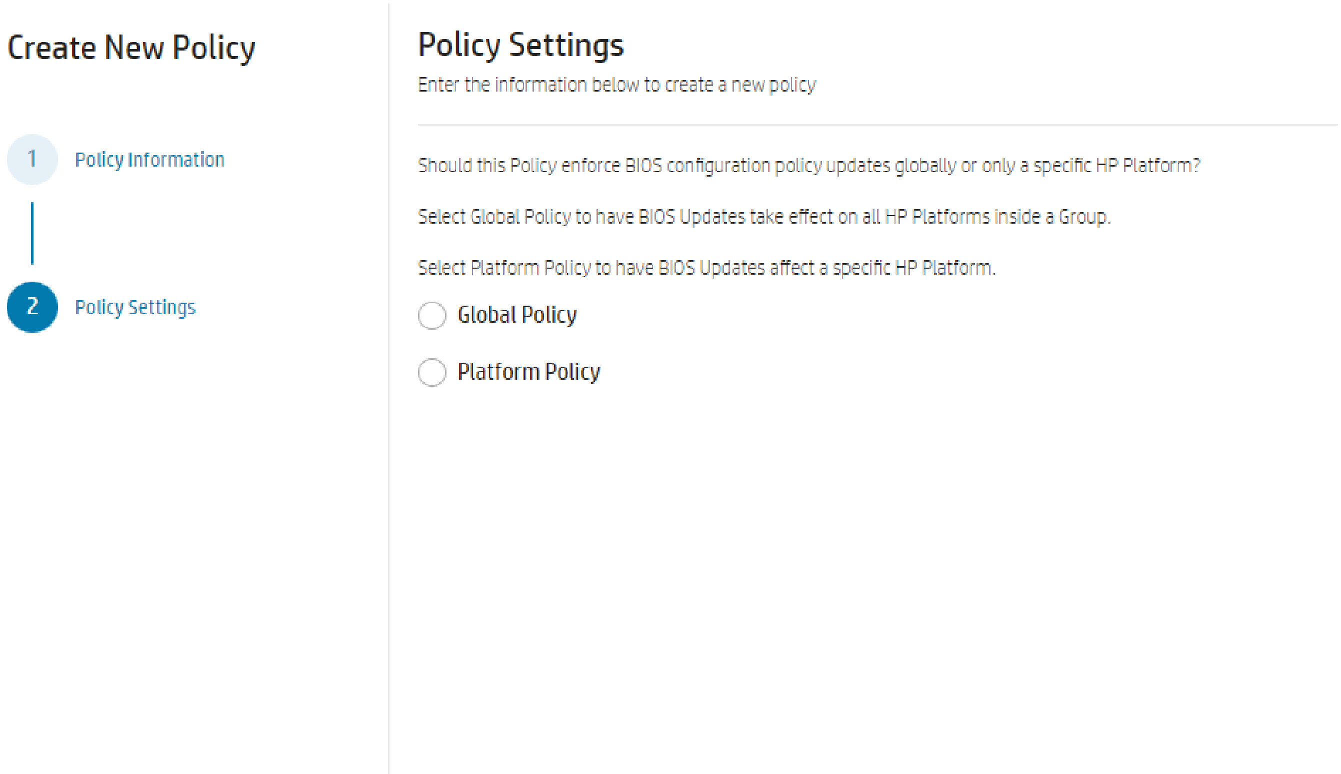
  - **Keep BIOS updated to the latest version**
  - **Enforce a specific BIOS version**

    NOTE: HP Connect does not support the installation of an older BIOS than the version already on the device (e.g., downgrading the BIOS version). If a device has a BIOS version that is newer (or same) than the version defined in the policy, the policy will be ignored.

Note – New Feature updates

BIOS Update Policy will be grouped under the following 2 categories

- Global Policy
- Platform Policy



Create New Policy

Policy Settings

Enter the information below to create a new policy

Should this Policy enforce BIOS configuration policy updates globally or only a specific HP Platform?

Select Global Policy to have BIOS Updates take effect on all HP Platforms inside a Group.

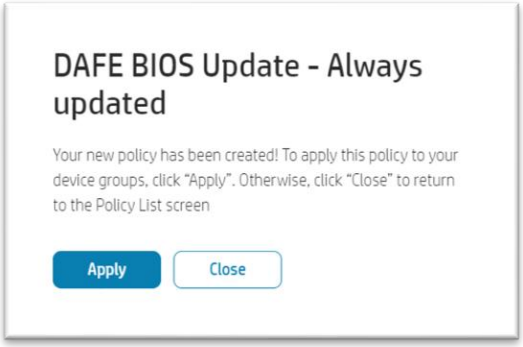
Select Platform Policy to have BIOS Updates affect a specific HP Platform.

○ Global Policy

○ Platform Policy

When a policy is created, a dialog will prompt to Apply or Close. Selecting *Close* ends, the policy creation task and returns to the Policy list, while clicking on *Apply* displays a 'Publish Policy' dialog where a selection is made for a Microsoft Azure device group. Enter a string in the Search field to find specific groups.

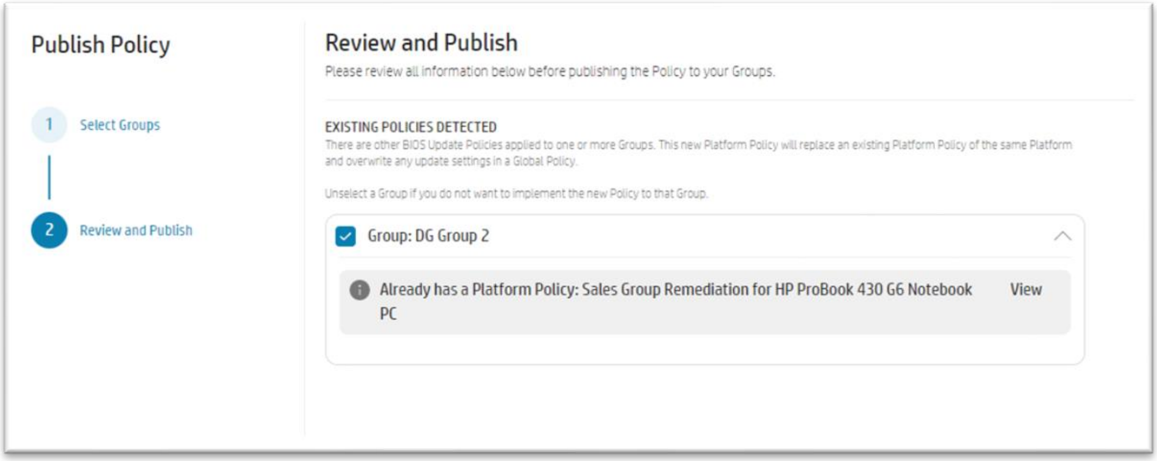
Example of an Apply/Close dialog



DAFE BIOS Update - Always updated

Your new policy has been created! To apply this policy to your device groups, click "Apply". Otherwise, click "Close" to return to the Policy List screen

If applying a BIOS Update policy that may conflict with an existing published (In-Use) policy, it will result in a conflict, and the new policy will replace the existing policy on Publish.



Publish Policy

1 Select Groups

2 Review and Publish

Review and Publish

Please review all information below before publishing the Policy to your Groups.

EXISTING POLICIES DETECTED

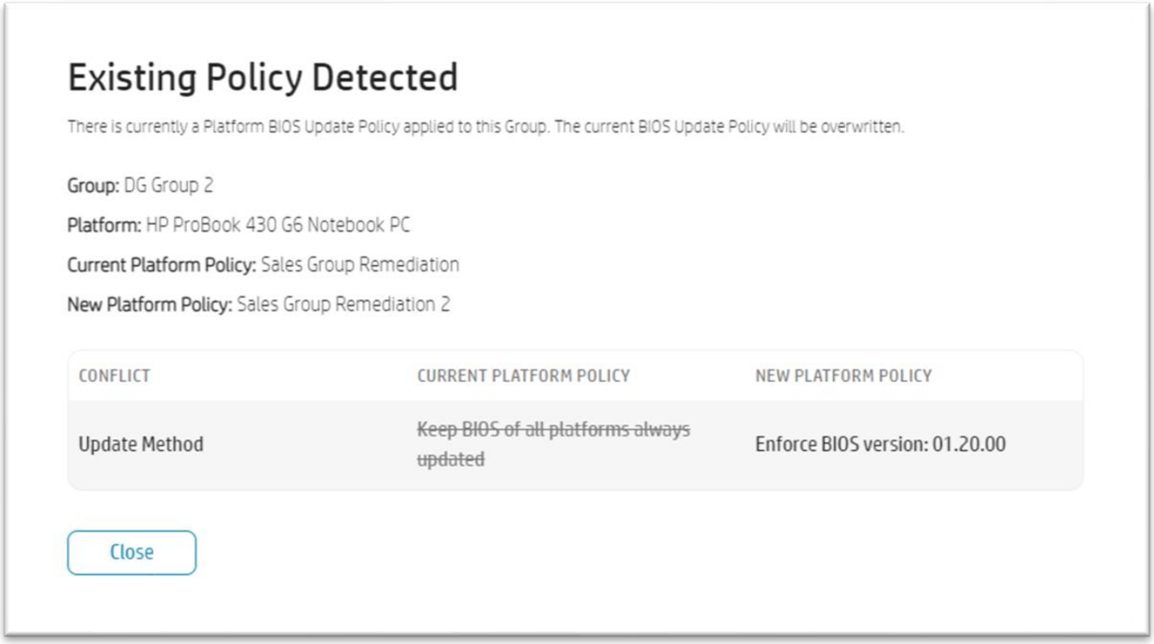
There are other BIOS Update Policies applied to one or more Groups. This new Platform Policy will replace an existing Platform Policy of the same Platform and overwrite any update settings in a Global Policy.

Unselect a Group if you do not want to implement the new Policy to that Group.

☑ Group: DG Group 2

Already has a Platform Policy: Sales Group Remediation for HP ProBook 430 G6 Notebook PC View

User can still prevent new policy from overwriting existing policy, by unchecking the Group selection. User will no longer need to resolve the conflict by confirming to Apply new policy or keep current policy. User can View the difference by clicking on the View button.



Existing Policy Detected

There is currently a Platform BIOS Update Policy applied to this Group. The current BIOS Update Policy will be overwritten.

Group: DG Group 2

Platform: HP ProBook 430 G6 Notebook PC

Current Platform Policy: Sales Group Remediation

New Platform Policy: Sales Group Remediation 2

CONFLICT	CURRENT PLATFORM POLICY	NEW PLATFORM POLICY
Update Method	~~Keep BIOS of all platforms always updated~~	Enforce BIOS version: 01.20.00

Steps to create a BIOS Update Policy

To create a BIOS Update policy, perform the following steps

- Login to HP Connect with the Azure administrative account
- In the Dashboard page or the Policies side tab select *New Policy*
- In the dialog, fill in the following fields
    - *Policy name*

The policy name will be shown in Microsoft Endpoint Manager once the policy is published. The name should be descriptive enough to quickly find in the array of policies that will eventually be created. Consider using 'Update' in the name to quickly identify policies by type.

  - *Policy type* - select 'Bios Update' from dropdown
  - *Description* – free format field
  - *Tags* – type a tag name and click *Add Tag.* Add as many tags as desired

    Tags can be used to identify policies from those already created. For example, an administrator could add a personal tag, perhaps with a name, to quickly find his/her policies. Or perhaps a tag to identify a specific platform it is applied to.

- Select *Next*
- In the Policy Settings dialog, select one of the following
  - *Keep BIOS of all devices always updated*

    The policy will apply to an Azure AD device group. All supported devices in the group will receive new BIOS when released by HP. Note that compliance policies are scheduled every 60 minutes by default (this may change in the future to every 24 hours).

  - *Deploy only critical BIOS updates*

    The policy will apply to an Azure AD device group. Every device in the selected group will be updated whenever a BIOS release is marked Critical by HP.

  - *Establish a rule for a specific device model*

    Select the appropriate policy rule to either:

    - *Keep BIOS always updated to latest version*, or
    - *Enforce a specific BIOS version*

      A platform is chosen from a drop-down list. When applied to an Azure AD device group, the policy will apply only to the selected platform, if a platform is part of the device group.

- Select *Save*
- on the next dialog, chose either
  - *Apply* – to publish policy to Endpoint Manager
    - Select device group(s) in dialog
  - *Close* – to save the policy to edit and/or apply later

How is the Policy Applied

When a BIOS update policy is created and a device selection made, the administrator can select '*Publish'* to send the policy to Microsoft Endpoint Manager. Microsoft Intune will then use its native Windows 10 (or 11) agent to send the policy action to all devices in the collection at the scheduled times. The policy's Detection script runs and helps decide if the Remediation script is executed.

By default, policies are checked for and applied every 60 minutes by Endpoint Manager. The schedule can be modified from the Intune console. It can be edited to run Once, every Hour, or Daily (or every number of days). Once a HP Connect policy is sent to Endpoint Manager, it is up to Intune to manage its actions.

In Endpoint Manager, the proactive remediation compliance policy properties will show Version 1 when it is initially published. The version is increased whenever the Policy is updated and re-published, or other policies are added to the group (for example, a BIOS Update policy + a BIOS setting policy would change the proactive remediation version number).

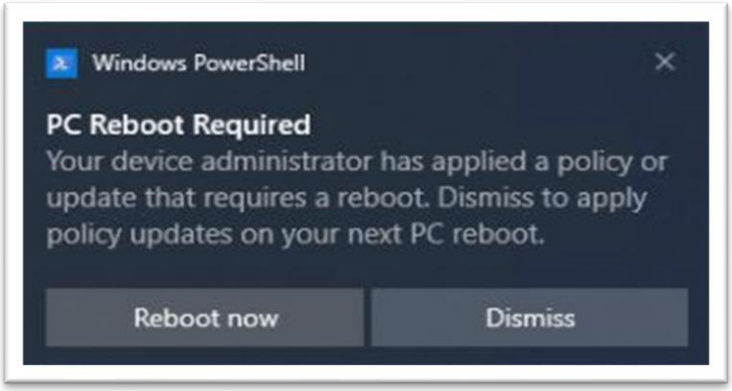
Because this is an HP policy, the Windows 10 (or 11) Intune agent sends a task to each device in the group as an action to be performed by an HP CSP (Configuration Service Provider). The HP action, in this case, for a BIOS update, proceeds to query an HP Cloud. If a required version that is newer than installed exists, it downloads the (signed) firmware capsule file and applies it to the device.

HP Connect does not support downgrading of the BIOS to an older version than installed. If this is required, it must be done by other methods outside HP Connect.

The HP BIOS update process follows these steps:

- BIOS UEFI capsule bin file is downloaded
- The capsule file components are hosted on the UEFI System partition
- UEFI BIOS in device is made aware of the pending update
- On next reboot, UEFI BIOS performs the update

A BIOS update policy will not automatically restart the device: therefore, the update will not occur until such action is taken. Once a BIOS update policy is applied, the device will display a toaster notification message like the following:



PC Reboot Required

Your device administrator has applied a policy or update that requires a reboot. Dismiss to apply policy updates on your next PC reboot.

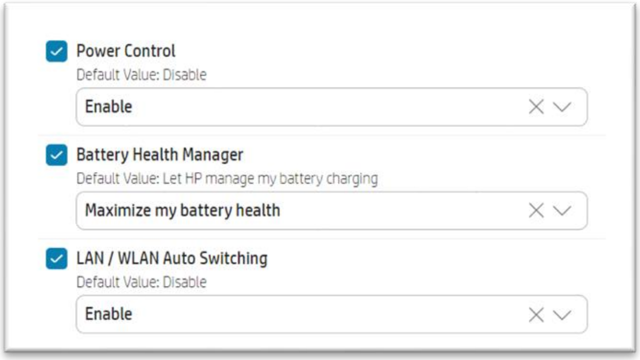
Again, the BIOS update will not occur until the device is rebooted.

BIOS Settings Policies – Platform Specific

An HP Connect BIOS setting policy is designed for a specific HP platform. Therefore, to apply the same policy to different platforms, or models, multiple policies need to be applied, one per platform.

In HP Connect, when adding an AAD device group to a policy, the policy settings changes are displayed on the right pane of the dialog.

Example of Settings being modified



☑ Power Control
Default Value: Disable
Enable

☑ Battery Health Manager
Default Value: Let HP manage my battery charging
Maximize my battery health

☑ LAN / WLAN Auto Switching
Default Value: Disable
Enable

Steps to create a BIOS Settings Policy

To create a BIOS Settings modification policy, perform the following steps

- Login to HP Connect
- In the Dashboard page or the Policies side tab select '*New Policy*'
- In the dialog, fill in the following fields
    - Policy name

      The policy name will be shown in Microsoft Endpoint Manager once the policy is published. The name should be descriptive enough to quickly find in the array of policies that will eventually be created. Consider using 'Settings' in the name to quickly identify policies by name.

    - Policy type (use dropdown): select Bios Settings
    - Description – free format field
    - Tags – type a tag name and click *Add Tag.* Add as many tags as desired

      Tags can be used to identify policies from those already created. For example, an administrator could add a personal tag, perhaps with a name, to quickly find his/her policies. Or perhaps a tag to identify a specific platform it is applied to.

- Select '*Next'*
- In the new Policy Settings dialog, chose the platform to apply the settings to
    - Use drop-down list or search in search field
    - On the right pane, configure the required BIOS settings
        - Use the Search field to find a setting
        - Modify as many settings as required

        Note that certain settings may require that an authentication method (Hp Sure Admin or password) be applied, or the setting may not be modified. This may not be obvious from the settings selection list.

        - Preview modified settings by selecting Show Selected

- Select '*Save*'
- on the next dialog, select either
    - *Apply* – to send policy to Endpoint Manager
        - Select device groups in next dialog
    - *Close* – to save the policy to edit and/or apply later

How is the Policy Applied

The HP Connect BIOS Settings policy will be added to the selected device group.

Microsoft Endpoint Manager will then use the updated HP Connect Detection policy script to identify any platform that matched the selection. If a device in the group matched the platform name and ID, a Remediation script will be run by the local Intune agent.

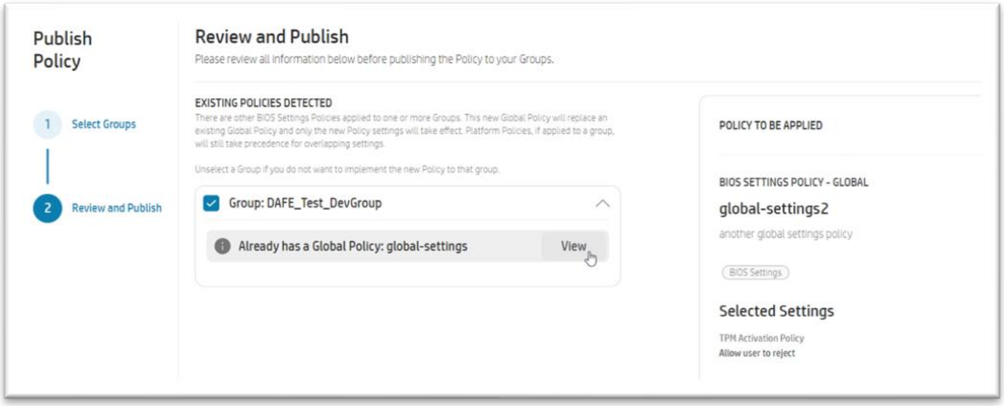
The Remediation script will then review and act on the BIOS settings modifications requested in the HP Connect policy. If an authentication policy has been applied (either HP Sure Admin or password) to the device group, the Settings script will use the appropriate authentication method to manage the BIOS settings.

BIOS Settings Policies – Global Settings

The Global Settings policy is designed to apply to all supported platform models in a device group.

A single Global Settings policy can be published to a device group. If a Global Settings policy has been published to a device group and a new policy is published to the same device group, the new policy will replace the existing policy in the group. Settings from the existing policy will not be merged with the new policy. Only the new policy settings will apply to devices checking in on their schedule, and if a device had applied a setting from the original policy, the setting will not be checked for compliance unless the setting also exists in the new policy.

If a global policy is applied to a device group with an existing global policy, the administrator can view the policies' settings and the resulting list by pressing 'View' in the Review and Publish dialog, prior to publishing the policy



Publish Policy

1 Select Groups

2 Review and Publish

Review and Publish

Please review all information below before publishing the Policy to your Groups.

EXISTING POLICIES DETECTED

There are other BIOS Settings Policies applied to one or more Groups. This new Global Policy will replace an existing Global Policy and only the new Policy settings will take effect. Platform Policies, if applied to a group, will still take precedence for overlapping settings.

Unselect a Group if you do not want to implement the new Policy to that group.

☑ Group: DAFE_Test_DevGroup

Already has a Global Policy: global-settings View

POLICY TO BE APPLIED

BIOS SETTINGS POLICY - GLOBAL

global-settings2

another global settings policy

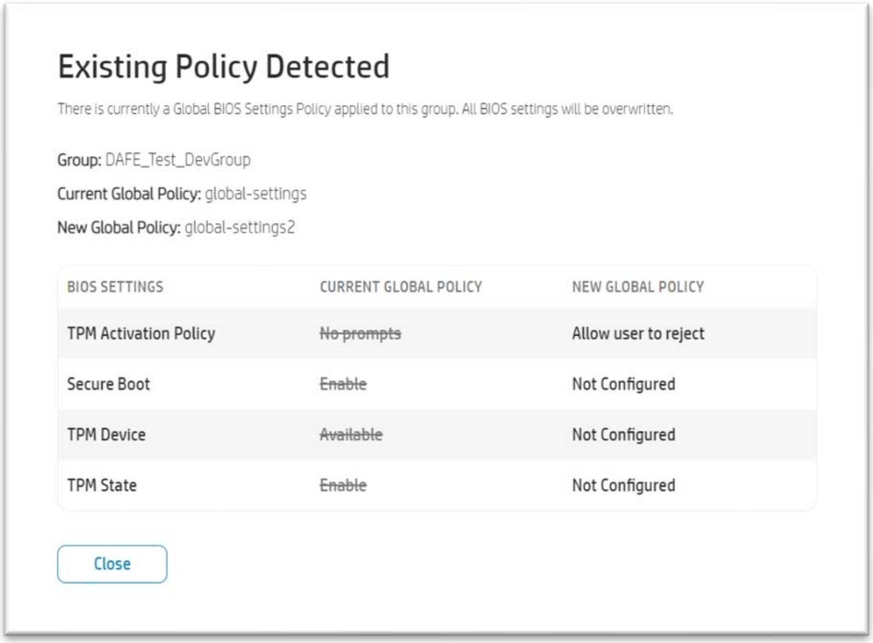
BIOS Settings

Selected Settings

TPM Activation Policy

Allow user to reject

The following dialog shows how pressing the View button displays the settings from both policies, and the right column indicates which settings will be used for compliance from the moment the new policy is published.



Existing Policy Detected

There is currently a Global BIOS Settings Policy applied to this group. All BIOS settings will be overwritten.

Group: DAFE_Test_DevGroup

Current Global Policy: global-settings

New Global Policy: global-settings2

BIOS SETTINGS	CURRENT GLOBAL POLICY	NEW GLOBAL POLICY
TPM Activation Policy	~~No prompts~~	Allow user to reject
Secure Boot	~~Enable~~	Not Configured
TPM Device	~~Available~~	Not Configured
TPM State	~~Enable~~	Not Configured

Global Policy vs. Platform-Specific settings

Note that although a single Global Policy can be published to a device group, platform-specific policies can coexist with it. Any platform-specific settings policy will take precedence over a similar setting from a published Global Policy. Conflict resolution is maintained when applying a Global Policy with existing policies in each device group

Global Policy settings that don't apply

Any selected setting in a Global Policy that does not exist or applies to a particular platform when applied to a device group will not be applied and will not generate an error. A Global Settings policy may contain settings that exist in some platforms and not others and this is supported. Each device will only apply settings that exists in its BIOS and will disregard all others.

> *The list of available settings in the Global Policy includes a majority but not ALL possible settings exposed by every supported platform. Therefore, some unique platform settings or settings that may have some inconsistent options across platforms may have to be set as platform-specific policies.*

Steps to create a Global BIOS Settings Policy

To create a BIOS Settings modification policy, perform the following steps

- Login to HP Connect

- In the Dashboard page or the Policies side tab select '*New Policy*'
- In the dialog, fill in the following fields
    - Policy name

      The policy name will be shown in Microsoft Endpoint Manager once the policy is published. The name should be descriptive enough to quickly find in the array of policies that will eventually be created. Consider using 'Settings' in the name to quickly identify policies by name.

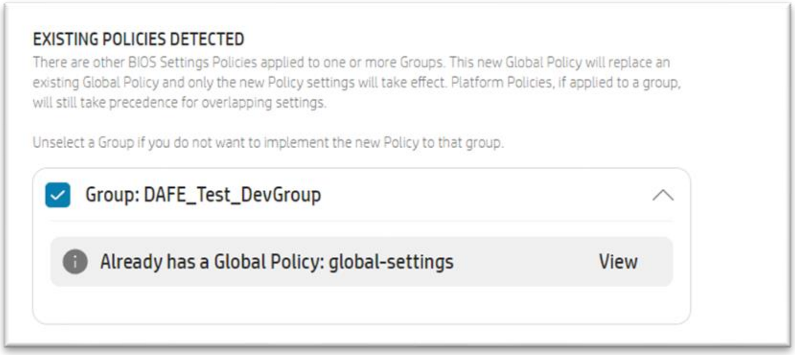
    - Policy type (use dropdown): select Bios Settings
    - Description – free format field
    - Tags – type a tag name and click *Add Tag.* Add as many tags as desired

      Tags can be used to identify policies from those already created. For example, an administrator could add a personal tag, perhaps with a name, to quickly find his/her policies. Or perhaps a tag to identify a specific platform it is applied to.

- Select '*Next'*
- Check *'Global Policy'*
- Select '*Next'*
- In the Policy Settings dialog find and set the required settings
    - On the right pane, configure each BIOS setting
        - Use the Search field to find a setting
        - Modify as many settings as required

          Note that certain settings may require that an authentication method (HP Sure Admin or password) be applied, or the setting may not be applied by the device. This may not be obvious from the settings selection list.

        - Preview modified settings by enabling Show Selected Only
- Select '*Save'*
- At the Review Policy page, confirm the settings and select '*Save'*
- On the next dialog, select either
    - *Apply* – to send policy to Endpoint Manager
        - Select device groups in next dialog
        - If an existing policy exists, press *View* to analyze the differences



EXISTING POLICIES DETECTED

There are other BIOS Settings Policies applied to one or more Groups. This new Global Policy will replace an existing Global Policy and only the new Policy settings will take effect. Platform Policies, if applied to a group, will still take precedence for overlapping settings.

Unselect a Group if you do not want to implement the new Policy to that group.

☑ Group: DAFE_Test_DevGroup

ⓘ Already has a Global Policy: global-settings

        - Press *'Publish'* or *'Previous'* to change or cancel
    - *Close* – to save the policy to edit and/or apply later

BIOS Authentication Policies

IMPORTANT: It is recommended that the device BIOS be up to date to implement authentication, as is often the case that newer BIOS include security and vulnerability updates. In addition, initial BIOS releases may not always fully implement certain security features or might include authentication issues addressed in future updates.

BIOS Authentication is an important aspect of managing, controlling, and securing Windows devices. An UEFI BIOS contains the hardware start-up code and many settings that should be secured prior to booting into a Windows Operation System. When the BIOS can be accessed without authentication, a local or remote user may be able to disable basic security features, potentially allowing malware early into the startup process that Windows may not protect against.

When enabling administrative security of the BIOS, settings changes will be accessible only to users or administrators with knowledge of the authentication mechanism. Both remote and local F10 setup access can be configured during BIOS authentication policies. Local F10 access authentication with HP Sure Admin will require the use of an HP Sure Admin app on an authorized user/administrator's phone.

HP Connect supports two types of BIOS authentication policies:

- HP Sure Admin
- Passwords

Authenticating with HP Sure Admin

HP Sure Admin provides modern security for PC firmware configuration-management by enabling remote administrators to securely manage BIOS settings while also allowing field support personnel to obtain secure in-person access to BIOS setup with a managed Local Access Key. Use of digital certificates and public-key cryptography eliminates risks associated with the legacy password-based approach.

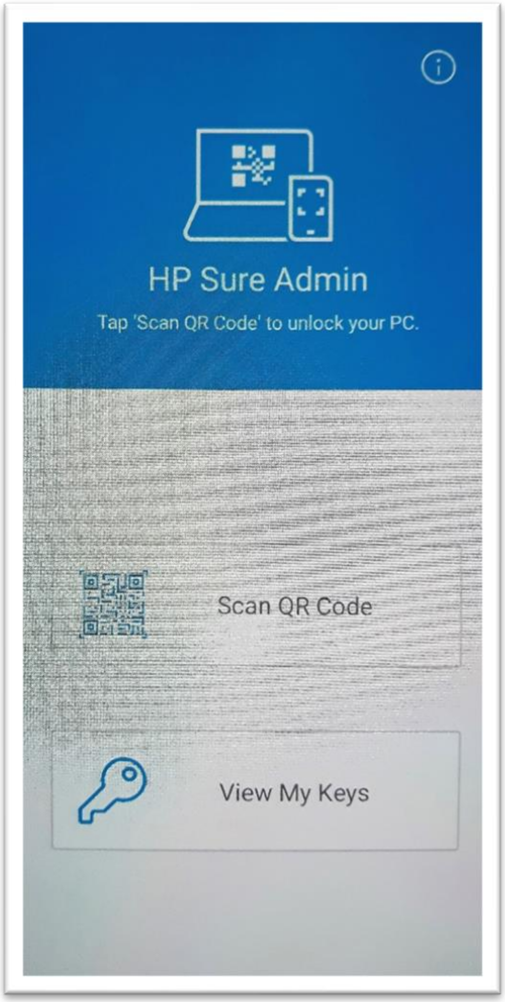
The HP Sure Admin security model relies on public-key cryptography and the strength of the approach is based on the elimination of any requirements to store or transmit the secret (private) key to the device being managed. Once the provisioning process is done by an HP Connect policy, firmware management and local access operations that require authentication are done securely.

> *HP Sure Admin relies on a trusted firmware environment that starts with the HP Secure Platform Management (SPM). HP SPM must be provisioned prior to enabling Sure Admin. Provisioning of SPM and enabling Sure Admin are performed by HP Connect with a BIOS Authentication policy.*

To secure local access to the BIOS, HP Sure Admin uses a Local Access Key, which is concurrently provisioned by the authentication policy. An HP developed mobile phone app is required when there is a need to access the BIOS setup at the device.

To authenticate to the BIOS after pressing F10, the user opens the HP Sure Admin mobile app, selects *Scan QR Code*, and scans the QR code displayed on the screen. Using a secure channel to communicate with HP Connect over the Internet, a challenge/response protocol will provide a one-time pin that the authorized user will type on the screen to access the BIOS.

HP Sure Admin mobile phone app



An overview of HP Sure Admin is presented in **Appendix A,** including using OpenSSL for creating the required cryptographic certificates. It also discusses how to allow non-Intune administrators to access the BIOS locally. AAD administrators are automatically enabled for local access via the Sure Admin app.

Authenticating with BIOS Passwords

When configuring BIOS passwords as the authentication type, HP Connect will use the applied password when publishing BIOS Settings configuration policies to devices in a device group. Adding a BIOS password requires matching complexity rules. Once a complexity rule is defined and selected, a password secret can be added and saved. A default BIOS password complexity rule is predefined, *HP Standard*.

HP Connect maintains password hints on each device managed by policy. The hint resides in the BIOS and point back to information stored in HP Connect. If a BIOS password is then modified via new policy, HP Connect will determine which password has been used before and use it to allow access and to change the password defined in the new policy. Then, a new BIOS password hint is set for future use.

Publishing a BIOS (password) authentication policy to a device group that currently has a similar policy in place will replace the existing policy with the new one.

NOTE: if a BIOS password authentication policy is published to a device group and the devices currently have a BIOS password not matching the password in the policy, dependent on the device BIOS policy for lockout , a device may get a BIOS lockout should the authentication policy is attempted by the MEM remediation script and fail to match or set the password a number of times.

> *A BIOS password authentication policy can pre-provision SPM cryptographic keys on all devices in the group by enabling the 'Enable Secure Platform management' check in the policy. HP Sure Admin can then be enabled easily.*

While BIOS passwords can help secure access, there are some drawbacks to using this protection mechanism:

- Having a common password across the organization makes it vulnerable to being published and accessible outside the secure environment.
- As passwords can change over time, it may leave some devices with inconsistent passwords and will be hard to keep track of what devices have which passwords.
- Passwords are used in clear text on the device which, in some cases, may pose a security threat.

Removing BIOS authentication Policy

When a BIOS authentication policy is removed from a device group, HP Connect publishes a 'no-authentication' policy to the same group. This policy will undo previous authentication policies applied to devices in the selected group, including Sure Admin provisioning and passwords. The BIOS on these devices will then be wide open for access. Note that deprovisioning occurs when devices next check-in to the MEM console.

Steps to create a BIOS Authentication Policy

To create a BIOS Update policy, perform the following steps

- Login to HP Connect
- In the Dashboard page or the Policies sidebar tab select '*New Policy*'
- In the dialog, fill in the following fields
  - Policy name

    The policy name will be shown in Microsoft Endpoint Manager once the policy is published. The name should be descriptive enough to quickly find in the array of policies that will eventually be created and applied. Consider using 'Updates', 'Settings', or 'Security' in the name to quickly search and find published polices by name.

  - Policy type (use dropdown): select Bios Authentication
  - Description – free format field

    - Tags – type a tag name and click *Add Tag.* Add as many tags as desired

      Tags can be used to identify policies from those already created. For example, an administrator could add a personal tag, perhaps with a name, to quickly find his/her policies. Or perhaps a tag to identify a specific platform it is applied to.

- Select '*Next'*
- In the new Policy Settings dialog, chose the authentication type, HP Sure Admin or Password
    - For: HP Sure Admin (recommended by HP)
        - Select the SPM keys previously stored in the HP Connect secrets vault or click on '*New'* to add those keys now
        - Select a LAK (Local Access Key) previously stored in the secrets vault. If none stored, HP Connect will use the Signing Key as the LAK
    - For: Password
        - Select a password from stored secrets
        - check 'Secure Platform Management' setting if you have made SPM keys and want to pre-provision the HP Sure Admin required keys for future use
- Select '*Save'*
- on the next dialog, select either
    - *Apply* – to send policy to Endpoint Manager
        - Select device group(s) in the next dialog
    - *Close* – to save the policy to edit and/or apply later

How is the Policy Applied

When a BIOS Authentication policy is applied (published) to a device group, HP Connect will send Microsoft Endpoint Manager, via graph API, the Detection and Remediation scripts that Intune will use as Proactive Remediation compliance for BIOS security.

If the authentication policy relies on HP Sure Admin certificates and key-pairs, each device in the device group will have the Security Platform Management (Endorsement and Signing) keys applied, Sure Admin setting enabled (BIOS setting is named *Enhanced BIOS Authentication Method*/EBAM), and if provided, provisions the *Local Access Key/*LAK as well to secure local keyboard F10 access to the BIOS. A toaster notification will be displayed to reboot the system.

Similarly, if BIOS passwords are defined in the policy, the published scripts will set up the password as the authentication mechanism on each device in the group. If a previous password has been applied outside an HP Connect policy, this step may fail or give inconsistent results.

Either BIOS password or HP Sure Admin authentication can be used on an HP device. Attempting to publish a BIOS password policy on a device group that uses HP Sure Admin will generate a conflict that will need resolved.

Appendix A: HP Sure Admin/Secure Platform Management

HP Sure Admin

HP Sure Admin is a Public-key cryptography technology developed to secure access to the HP BIOS on commercial systems. Public Key Cryptography is known for its security and is well understood. HP Sure Admin relies on Public/Private key pairs to enforce secure access, and the implementation works for both remote and local F10 Setup access management.

The basis for HP Sure Admin is called HP Secure Platform Management (SPM), a trusted environment present in each device' UEFI BIOS. Once configured, SPM becomes the trusted base for features such as HP Sure admin, HP Sure Run (technology to help maintain security of certain Windows services and application), and HP Sure Recover (a secure Windows OS recovery method).

After the SPM is configured on the HP BIOS, HP Sure Admin can be enabled or disabled by enabling the 'Enhanced BIOS Authentication Mode' (EBAM) setting. The HP Connect policy will configure SPM and then enable EBAM, therefore securing remote access to the BIOS. To secure local F10 Setup access an additional Local Access Key (LAK) needs provisioned and will be done by the same HP Connect authentication policy.

Secure Platform Management

The Secure Platform Management technology relies on two cryptographic keys. An Endorsement key and a Signing key. The Endorsement key (obtained from an Endorsement certificate) becomes the rooted trust for security features in the BIOS. This key is used to authorize the Signing key.

The Signing key is used for signing packages during management of the BIOS (Settings compliance policies).

At introduction, the two certificates need to be provided. The certificates are not stored in the HP cloud, but the embedded public/private key pairs are retrieved from the certificates, stored in a secure cloud vault, and used when creating a HP Sure Admin authentication policy. An additional (Local Access Key) certificate is required to support protection to the F10 Setup.

NOTE: it is critical that the certificates be safeguarded to prevent the security of the BIOS from being compromised should they become publicly available but will no longer be needed by HP Connect. The resulting key-pairs themselves are safely stored in the HP cloud by HP Connect.

Protection for Local F10 Access

While provisioning HP Sure Admin secures remote access to the BIOS settings, there is a need to also secure local access to the BIOS F10 Setup menu. In lieu of passwords, HP Sure Admin utilizes a Local Access Key/LAK (signed with the provisioned Signing Key).

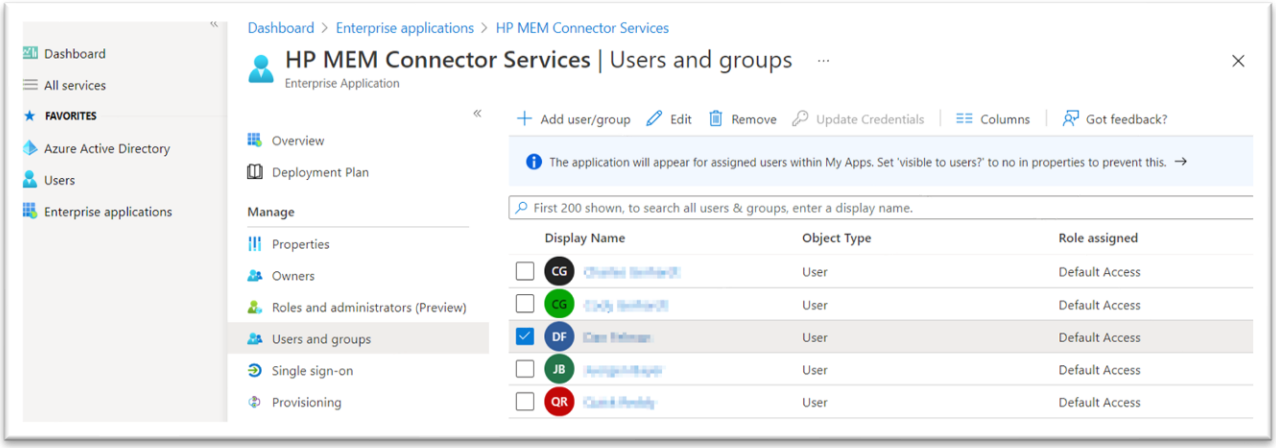
Local F10 BIOS access can be allowed from the HP Sure Admin phone app by entering appropriate credentials in the app. An administrator must use a phone app the first time on a provisioned device to scan the visible QR code and provide AAD credentials. This will invoke a process to add the supporting HP Sure Admin Enterprise Application on the Azure tenant, where it will be used for all local authentication requests.

Non-Administrators can be permitted to access the F10 setup following these steps in Azure admin center.

From the Azure portal, select Enterprise Applications, and click on HP MEM Connector Services. You should notice the homepage URL column is https://admin.hp.com

Certain Intune Conditional Access policies may prevent HP Connect for MEM from being integrated. As example, 'Require approved client app' and 'Require app protection policy', if enabled, may affect activation of the HP Sure Admin application.

In the HP MEM Connector Services window, select Users and Groups, and click on the user requiring local Sure Admin BIOS access, and click on Edit. Notice that the default roles assigned to users is *Default Access*. Next steps will modify the Role to support local BIOS access

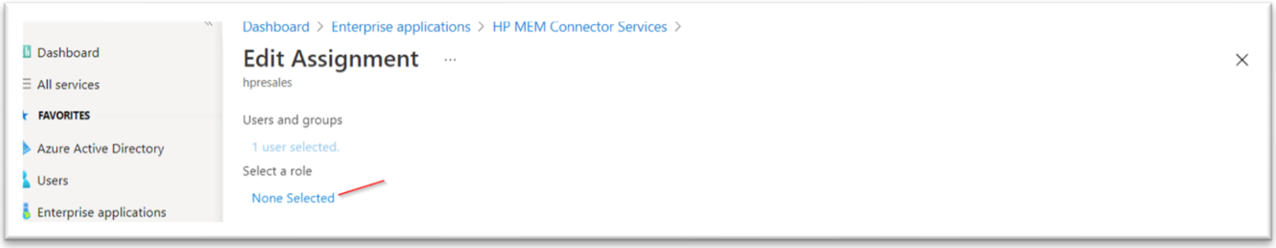


The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

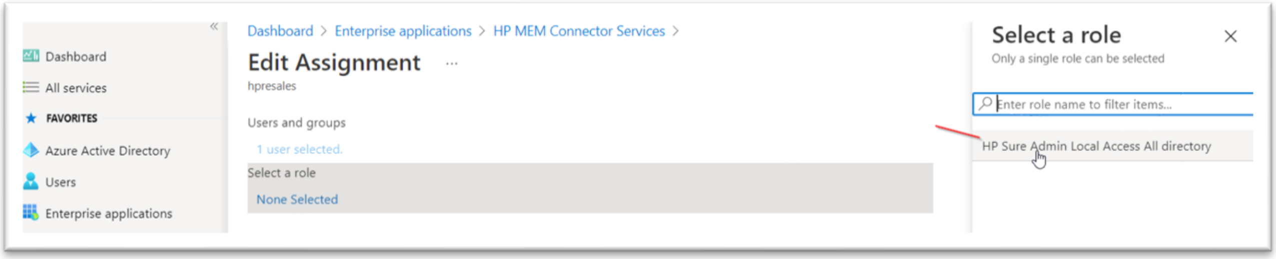
	Display Name	Object Type	Role assigned
□	CG [redacted]	User	Default Access
□	CG [redacted]	User	Default Access
☑	DF [redacted]	User	Default Access
□	JB [redacted]	User	Default Access
□	QR [redacted]	User	Default Access

In the Edit Assignment window, click on 'select a role' link None Selected (see below)



Users and groups
1 user selected.
Select a role
None Selected

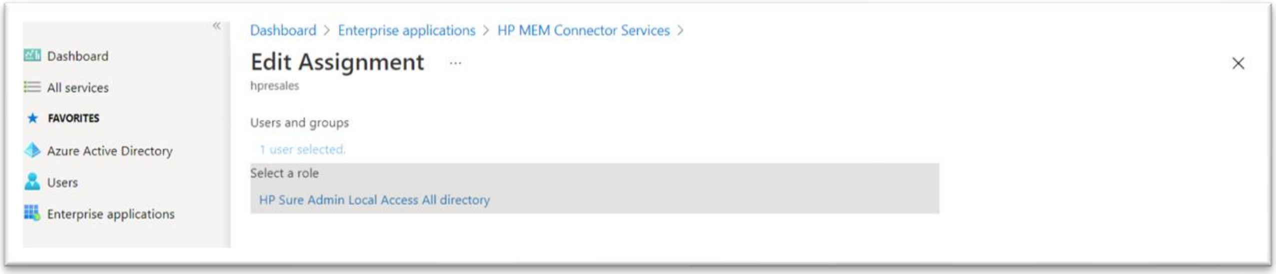
Then, on the Select a role pane, click on HP Sure Admin Local Access All directory. End by clicking *Select*


Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > Enterprise applications > HP MEM Connector Services >
Edit Assignment
hpresales
Select a role
Only a single role can be selected
Enter role name to filter items...

Users and groups
1 user selected.
Select a role
None Selected

HP Sure Admin Local Access All directory

You will then see the action performed and the user will have the permission displayed. Click on *Assign*



Dashboard > Enterprise applications > HP MEM Connector Services >

Edit Assignment

hpresales

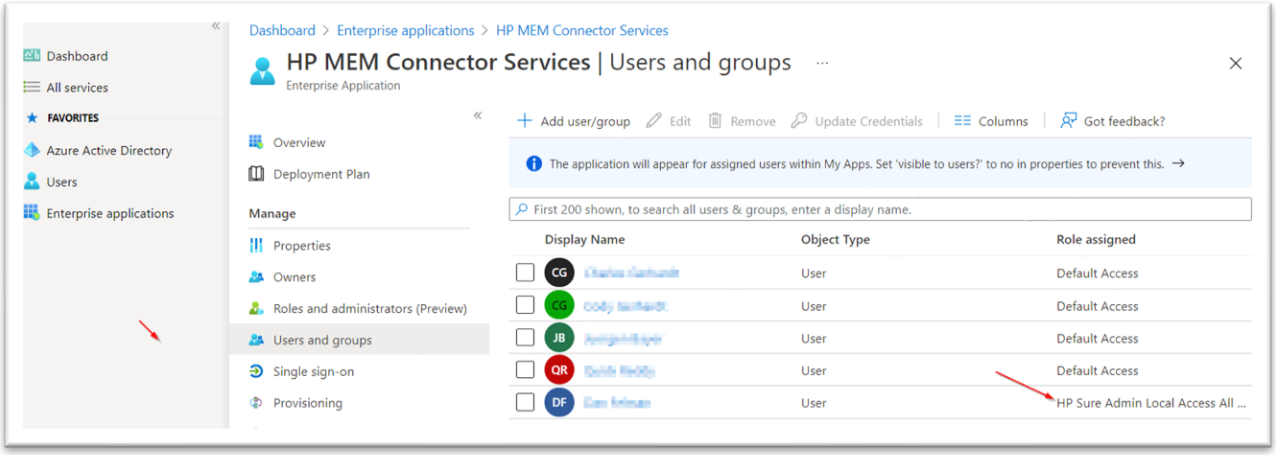
Users and groups

1 user selected.

Select a role

HP Sure Admin Local Access All directory

HP Sure Admin local access is now supported for the user



Dashboard > Enterprise applications > HP MEM Connector Services

HP MEM Connector Services | Users and groups

Enterprise Application

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

	Display Name	Object Type	Role assigned
□	CG [redacted]	User	Default Access
□	CG [redacted]	User	Default Access
□	JB [redacted]	User	Default Access
□	QR [redacted]	User	Default Access
□	DF [redacted]	User	HP Sure Admin Local Access All ...

Devices with currently provisioned HP Sure Admin

For HP Connect to manage devices already provisioned and enabled with Sure Admin, care must be taken.

A security mechanism to prevent the replay of authenticated BIOS setting packages is the use of a Nonce value that changes (increases) based on use. HP Connect implements a Nonce service that is used when it signs a BIOS package delivered to HP supported devices. The produced nonce value might conflict with the nonce value used by existing provisioning. Therefore, to properly support HP Sure Admin for devices managed by HP Connect policies, the following steps are suggested:

1. Deprovision HP Sure Admin
   a. Deprovision Secure Platform Management (SPM)
   b. Disable Sure Admin setting
   c. Clear the LAK (Local Access Key)
2. Re-Provision HP Sure Admin
   a. Add certificates keys as secrets to HP Connect
      i. SPM, Signing Key, LAK
   b. Create HP Connect Sure Admin authentication policy
   c. Publish policy to HP Device group(s)

OpenSSL and certificates

As described, HP Connect will provision HP Sure Admin, an extremely secure BIOS access technique, to supported HP endpoints with cryptographic keys. HP will read the contents of an organization supplied certificates and will use the public/private key pairs for this purpose. HP Connect keeps track of the keys to ensure BIOS settings changes are only possible with their use.

It is extremely important that the organization created and provided certificates be safely stored as their release can impair the security of the managed devices. HP Connect does not keep the certificates in the HP cloud but will store the embedded key pairs to use during device authentication required policies.

As an example, OpenSSL will be used here to create the certificates. OpenSSL, the open-source software, supports creation of correctly formatted certificates. It does not matter how the certificates are created if the embedded private/public key pairs meet the requirements. Any certificate creation method can be used, including an organizations' Certificate Authority.

The following OpenSSL commands can be used to create the Endorsement, Signing, and Local Access Key certificates. The certificates include the private and public key pairs HP Connect will use to provision Secure Platform Management and enable HP Sure Admin (EBAM). The certificates should be secured and protected. HP will store the keys from the certificate in HP's secure cloud.

The following steps can be used to create the required certificates. The examples are described by using the Open-Source OpenSSL application, but the certificates can be created within the organization with any available technique.

How to Create the Endorsement Key Certificate

If OpenSSL asks for a password, press Enter to terminate execution of the command if a certificate password is not wanted or type the password string of choice. HP Connect now supports certificate passwords.

1. Create a X.509 self-signed certificate

   The `EKPriv.pem` and `EK.crt` output files are used to create the actual endorsement certificate next and can be renamed as desired

   In the OpenSSL command below, the `–subj` command line parameter should be updated to reflect information specific to the organization. OpenSSL will prompt If not included. This information may be reported to users and admins in future versions of the firmware so it should be correct.

   ```
   OpenSSL> req -x509 -nodes -newkey rsa:2048 -keyout EKpriv.pem -out EK.crt
   -days 3650 -subj
   '/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com'
   ```

2. Convert self-signed certificate to the PKCS#12 pfx format

   A certificate password is not required. It is used in the example below in case additional certificate protection is desired. If not required, leave the option out of the run string, and hit ENTER if requested by OpenSSL

```
OpenSSL> pkcs12 -inkey EKpriv.pem -in EK.crt -export -keypbe PBE-SHA1-
3DES -certpbe PBE-SHA1-3DES -out EK.pfx -name ‘SPM Endorsement Key
Certificate’
```

If OpenSSL asks for a password, press Enter to terminate execution of the command or type a desired certificate password.

How to Create the Signing Key Certificate

3. Create a X.509 self-signed certificate

   The `SKPriv.pem` and `SK.crt` output files are used to create the actual endorsement certificate next and can be renamed as desired

   ```
   OpenSSL> req -x509 -nodes -newkey rsa:2048 -keyout SKpriv.pem -out SK.crt
   -days 3650 -subj
   ‘/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com’
   ```

4. Convert self-signed certificate to the PKCS#12 pfx format

   ```
   OpenSSL> pkcs12 -inkey SKpriv.pem -in SK.crt -export -keypbe PBE-SHA1-
   3DES -certpbe PBE-SHA1-3DES -out SK.pfx -name ‘SPM Signing Key
   Certificate’
   ```

   If OpenSSL asks for a password, press Enter to terminate execution of the command or type a desired certificate password.

How to Create the Local Access Key (LAK) Certificate

5. Create a X.509 self-signed certificate

   The `LAK.pem` and `LAK.crt` output files are used to create the actual endorsement certificate next and can be renamed as desired

   ```
   OpenSSL> req -x509 -nodes -newkey rsa:2048 -keyout LAK.pem -out LAK.crt -
   days 3650 -subj
   ‘/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com’
   ```

6. Convert self-signed certificate to the PKCS#12 pfx format

   ```
   OpenSSL> pkcs12 -inkey LAK.pem -in LAK.crt -export -keypbe PBE-SHA1-3DES
   -certpbe PBE-SHA1-3DES -out LAK.pfx -name ‘EBAM Local Access Key
   Certificate’
   ```

   If OpenSSL asks for a password, press Enter to terminate execution of the command or type a desired certificate password.

NOTE: After the .pfx certificates are created, all other temporary files (.pem and .crt) are no longer required and should be safely deleted.

Appendix B: Troubleshooting and Logs

The first troubleshooting step should be a confirmation of the policy created. Confirm the policy meets the requirements by selecting it from the Policy tab and reviewing its contents.

HP Connect defined policies involve the development of Detection and Remediation scripts. The scripts are then published to MEM as proactive remediations and executed by the Intune MDM agent on a device. When the Intune MDM agent runs a HP Connect-generated Proactive Remediation, a log is generated on the device.

> *Microsoft Endpoint Manager proactive remediation compliance policies (for example, as published by HP Connect) execute on a defined schedule. If the Intune agent on a device checks in prior to the next scheduled run, the policy may not execute.*

To gather information about the execution of a HP Connect policy, an IT administrator should make sure devices sync to Endpoint Manager and review HP Connect and Microsoft Intune MDM logs of activities.

Sync a Policy

For testing purposes and to see the effects of applied policies without waiting for Endpoint Manager MDM agent to check in, Sync to the console as follows:

Sync from Device

On a Windows endpoint, Sync by

1. Selecting Windows Start\Settings, then
   - Chose Accounts
   - Select 'Access Work or School'
   - Click on '*Connected to <domain>'s Azure* AD '
   - Click on *Info*
   - Scroll and click on *Sync*
2. Rebooting the device to start an MDM check in, if the schedule is appropriate.
3. Restarting the 'Microsoft Intune Management Extension' service, to initiate a check-in

Sync from Intune admin center

By default, Intune devices check in every 8 hours (Troubleshoot policies and configuration profiles in Microsoft Intune - Intune | Microsoft Docs).

Sync Policies from the Endpoint Manager admin center

- Select 'Devices'
- Select the <device> to Sync
- In the Overview pane, click on *Sync*

  Intune notifies the device to check in with the Intune Service. The notification times vary, from *immediate* to a *few hours* (Troubleshoot device profiles in Microsoft Intune | Microsoft Docs).

Logs

When a HP Connect policy fails in some way when executed by the Intune agent, access to the logs will be useful. Next is a review of logs that may help troubleshoot certain failures.

Managed device

HP Connect logs

HP Connect maintains a log of operation at `~\AppData\Local\HPConnect`. Since Intune scripts on a device execute in the System context, the logs will be created at `C:\WINDOWS\system32\config\systemprofile\AppData\Local\HPConnect` (Note that at introduction, the log was written to `%ProgramData%\HP\Endpoint\Logs`). Policies created and published from late March 2022 will move existing logs (if exist) to the new location and update as needed.

– This logs folder contains logs of HP Connect policy being applied to the device. **NOTE**: If the ..`\HPConnect` folder does not exist, Intune has not synced an HP Connect policy with the device.

  The HP Connect activity log (*Ex.* *`c814f103-6446-46ab-9885-e4df43d75e93.log`*), can be useful for analysis or troubleshooting.

  Find the latest actions taken by the policy at the end of the log file. Error conditions would be shown here. Also, check the log file update date to confirm when it was last written to.

Impact to the log location change

New policy deployed on client device for 1st time after log location changes

- Policy enforcement files and the CMSL version downloaded will be maintained in the new folder `C:\WINDOWS\system32\config\systemprofile\AppData\Local\HPConnect`.

Existing Policy on client device before changes

- In order to implement new location for the log and CMSL files, user has to edit existing policy and redeploy or deploy a new policy.
- Folder `C:\WINDOWS\system32\config\systemprofile\AppData\Local\HPConnect` will be created.
- Existing log file will be copied from previous location to new folder.
- New version of CMSL will be downloaded fresh under folder `C:\WINDOWS\system32\config\systemprofile\AppData\Local\HPConnect`
- Previous folder at `C:\ProgramData\HP\Endpoint` will be deleted.

Intune logs

– The Intune MDM Management Extension logs can be found at

  `%ProgramData%\Microsoft\IntuneManagementExtension\Logs`

  and a useful log to explore is `IntuneManagementExtension.log`

– Microsoft Intune agent stores scripts run on a device at

  `C:\Windows\IMECache\HealthScripts\Endpoint Manager Diagnostics logs`

- For a 'BIOS Update' policy, the following logs can be useful (*Note: `GroupPolicy` subfolder is hidden*):

  `C:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown\wu_bios_update.log.` **NOTE***: Add '`Shutdown`' to name if submitting (ex. wu_bios_update -shutdown.log)*

  `C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup\wu_bios_update.log.` **NOTE***: Add '`Startup`' to name if submitting (ex. wu_bios_update -startup.log)*

- For Intune MDM troubleshooting purposes, you can run a Diagnostics report at

  `Windows Start/Settings/Connected to <AAD tenant>`

  click *Info* – then *Create_Report* and *Export* (output defaults to `C:\Users\Public\Documents\MDMDiagnostics`)

Intune Health Evaluation Task

Intune Management Engine runs a Health Evaluation as a scheduled task every day

```
C:\Program Files (x86)\Microsoft Intune Management
Extension\ClientHealthEval.exe
```

with a log created at

`%ProgramData%\Microsoft\IntuneMNagementExtension\Logs\ClientHealth.log`.

Find the Intune Health Evaluation task in Task Scheduler:

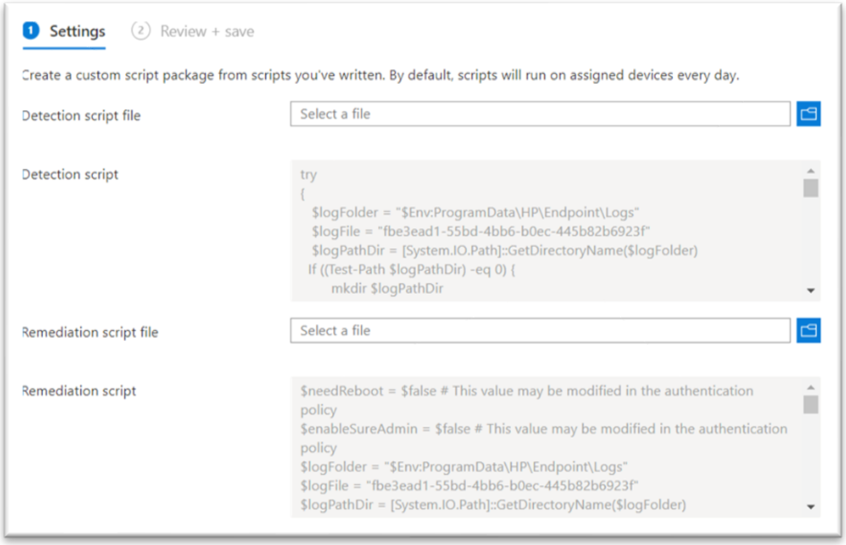
- Open Windows Task Scheduler on the device, and
- Select 'Task Scheduler Library/Microsoft/Intune'.
- Look for the 'Intune Management Extension Health Evaluation' task.
- Select Properties by right-clinking on the entry, and
- The execution schedule is listed in the 'Triggers' tab.

Information from Endpoint Manager Console

Published HP Connect policies

Policies published by HP Connect can be found on the Endpoint Manager Intune console at Reports/Endpoint Analytics/Proactive Remediation (*MDM Policies are listed here*)

- Select the corresponding HPConnectForMEM-<device group name> script package name from the list, and then chose
  - Properties to list the device groups the policy was applied to, and the schedule
    - To view the HP, Connect Detection and Remediation scripts, select Settings *Edit* and capture both Detection and Remediation scripts (click inside each script and copy/paste) into files



Create a custom script package from scripts you've written. By default, scripts will run on assigned devices every day.

Detection script file: Select a file

Detection script

```
try
{
  $logFolder = "$Env:ProgramData\HP\Endpoint\Logs"
  $logFile = "fbe3ead1-55bd-4bb6-b0ec-445b82b6923f"
  $logPathDir = [System.IO.Path]::GetDirectoryName($logFolder)
 If ((Test-Path $logPathDir) -eq 0) {
     mkdir $logPathDir
```

Remediation script file: Select a file

Remediation script

```
$needReboot = $false # This value may be modified in the authentication
policy
$enableSureAdmin = $false # This value may be modified in the authentication
policy
$logFolder = "$Env:ProgramData\HP\Endpoint\Logs"
$logFile = "fbe3ead1-55bd-4bb6-b0ec-445b82b6923f"
$logPathDir = [System.IO.Path]::GetDirectoryName($logFolder)
```

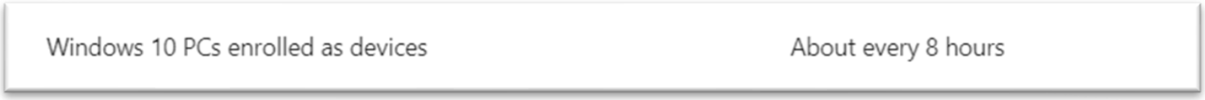
- ○ Device Status to show which systems (if any) received the policy from Intune, and their compliance status. Status reporting can take hours, even days to apply and show up in this list.

Notes about MEM compliance policies

Cloud management actions do not happen in real-time. When a policy is applied by Microsoft Endpoint Manager, the policy cannot take effect until each device's Intune agent checks in. It may take hours, or longer, depending on the check in schedule or how often is the compliance policy applied.

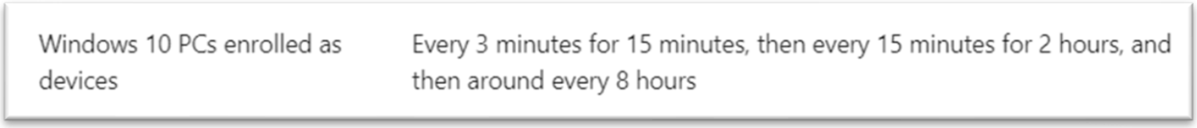
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot?WT.mc_id=EM-MVP-5003177

Intune Refresh cycle



Windows 10 PCs enrolled as devices	About every 8 hours

If devices recently enroll, then the compliance, non-compliance, and configuration check-in runs more frequently. The check-ins are **estimated** at:



Windows 10 PCs enrolled as devices	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Additional reading on MDM policy refresh: https://www.petervanderwoude.nl/post/windows-10-mdm-policy-refresh/

Appendix C: Azure Active Access

Required permissions

For access and use of HP Connect at *https://admin.hp.com* an organization's Global Administrator can accept required permissions to allow interaction with Microsoft Azure and Endpoint Manager and also accept those on behalf of the whole organization. So,

- An AAD Global Administrator must login first to enable HP Connect as an Enterprise Application, and accept permissions on the EULA dialog.
- An Intune administrator will need to accept permission to log into HP Connect to use the application unless the global administrator accepted on behalf of the organization.

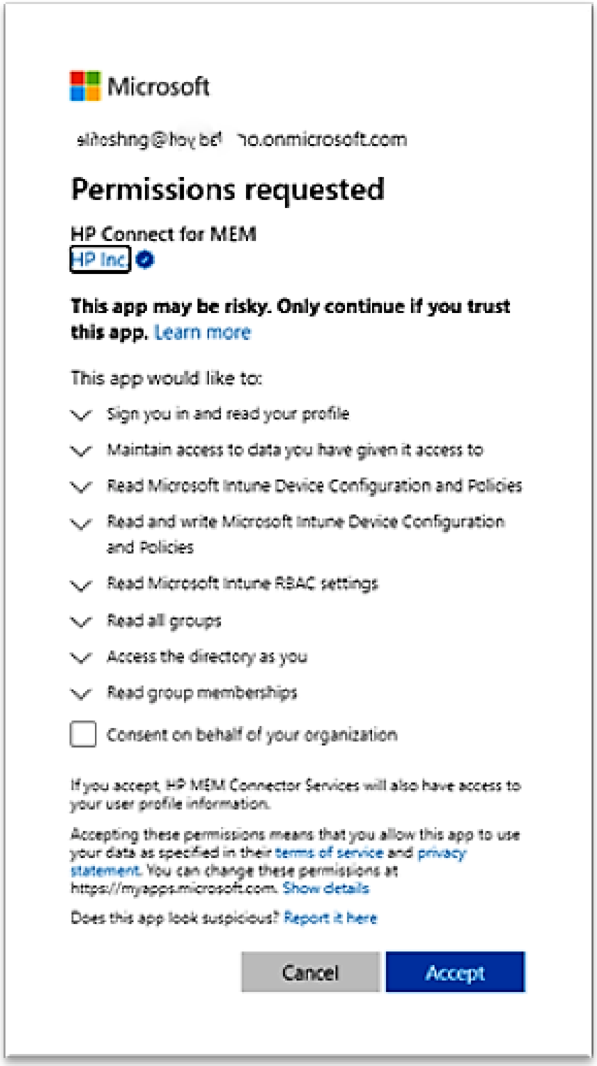
As an update to improve performance of Azure groups listing,

- Intune Administrators need to accept permissions for the User Interface application itself (seen below)

The HP Connect connector app for Microsoft Endpoint Manager utilizes Azure Graph API to access read users and groups and read and write compliance policies. Microsoft Graph API permissions are referenced at https://docs.microsoft.com/en-us/graph/permissions-reference

The following permissions are required for HP Connect in the Microsoft EULA acceptance dialog:

- ✓ Sign you in and read your profile
- ✓ Maintain access to data you have given it access to
- ✓ Read Microsoft Intune Device Configuration and Policies
- ✓ Read and write Microsoft Intune Device Configuration and Policies
- ✓ Read Microsoft Intune RBAC settings
- ✓ Read all groups
- ✓ Access the directory as you
- ✓ Read group memberships



Microsoft

sliteshng@hoy be ho.onmicrosoft.com

Permissions requested

HP Connect for MEM

HP Inc

This app may be risky. Only continue if you trust this app. Learn more

This app would like to:

- Sign you in and read your profile
- Maintain access to data you have given it access to
- Read Microsoft Intune Device Configuration and Policies
- Read and write Microsoft Intune Device Configuration and Policies
- Read Microsoft Intune RBAC settings
- Read all groups
- Access the directory as you
- Read group memberships

□ Consent on behalf of your organization

If you accept, HP MEM Connector Services will also have access to your user profile information.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

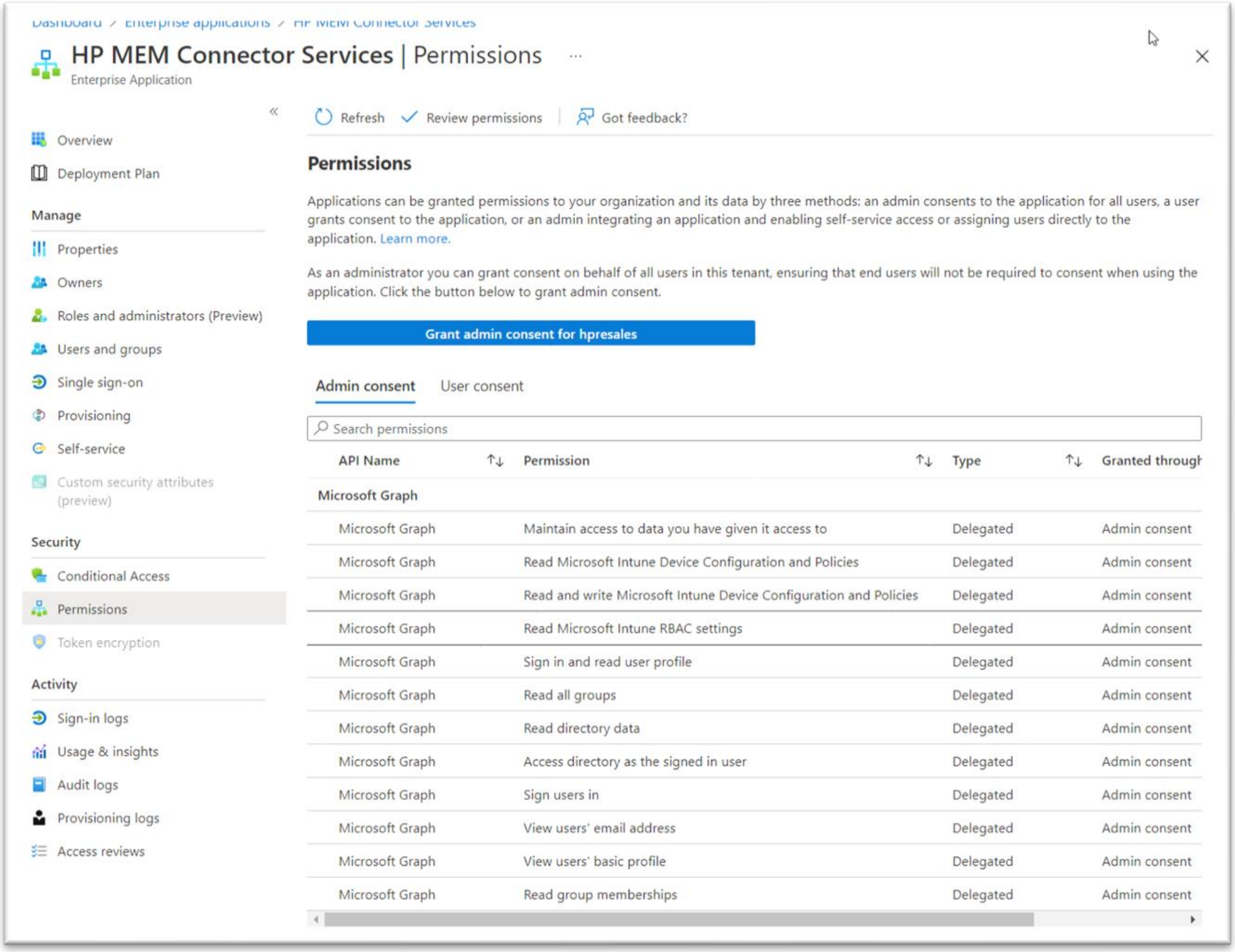
As mentioned, Intune Administrators will be asked to accept the following additional permissions, unless also accepted by a global administrator

- ✓ Sign you in and read your profile
- ✓ Read all groups
- ✓ Maintain access to data you have given access to

Note: If the browser has a popup blocker in place, it may have to be disable for the dialog to appear.

Permissions in Azure

Permissions granted can be seen in the organization’s Azure tenant selecting Enterprise Applications. To review the permissions accepted for HP Connect for MEM, select HP MEM Connector Services, and then Permissions.



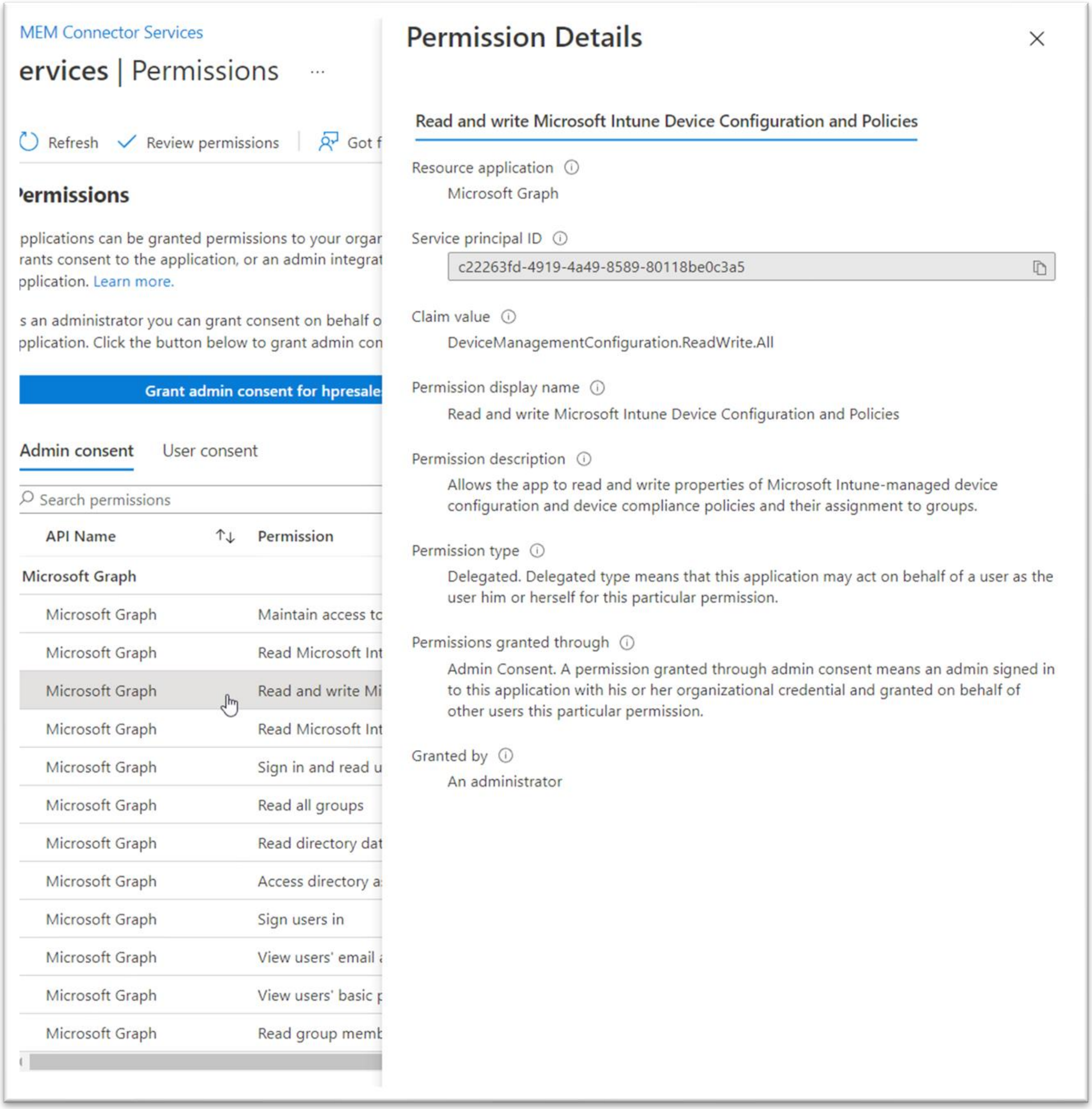
Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application. Learn more.

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

API Name	Permission	Type	Granted through
Microsoft Graph			
Microsoft Graph	Maintain access to data you have given it access to	Delegated	Admin consent
Microsoft Graph	Read Microsoft Intune Device Configuration and Policies	Delegated	Admin consent
Microsoft Graph	Read and write Microsoft Intune Device Configuration and Policies	Delegated	Admin consent
Microsoft Graph	Read Microsoft Intune RBAC settings	Delegated	Admin consent
Microsoft Graph	Sign in and read user profile	Delegated	Admin consent
Microsoft Graph	Read all groups	Delegated	Admin consent
Microsoft Graph	Read directory data	Delegated	Admin consent
Microsoft Graph	Access directory as the signed in user	Delegated	Admin consent
Microsoft Graph	Sign users in	Delegated	Admin consent
Microsoft Graph	View users' email address	Delegated	Admin consent
Microsoft Graph	View users' basic profile	Delegated	Admin consent
Microsoft Graph	Read group memberships	Delegated	Admin consent

Clicking on a permission will display a card with details on what that permission allows.



MEM Connector Services

ervices | Permissions ···

Refresh ✓ Review permissions | Got f

'ermissions

pplications can be granted permissions to your orgar
rants consent to the application, or an admin integrat
pplication. Learn more.

s an administrator you can grant consent on behalf o
pplication. Click the button below to grant admin con

Grant admin consent for hpresale

Admin consent   User consent

Search permissions

API Name	Permission
Microsoft Graph	
Microsoft Graph	Maintain access tc
Microsoft Graph	Read Microsoft Int
Microsoft Graph	Read and write Mi
Microsoft Graph	Read Microsoft Int
Microsoft Graph	Sign in and read u
Microsoft Graph	Read all groups
Microsoft Graph	Read directory dat
Microsoft Graph	Access directory a
Microsoft Graph	Sign users in
Microsoft Graph	View users' email
Microsoft Graph	View users' basic p
Microsoft Graph	Read group memb

Permission Details ×

Read and write Microsoft Intune Device Configuration and Policies

Resource application ⓘ
Microsoft Graph

Service principal ID ⓘ
c22263fd-4919-4a49-8589-80118be0c3a5

Claim value ⓘ
DeviceManagementConfiguration.ReadWrite.All

Permission display name ⓘ
Read and write Microsoft Intune Device Configuration and Policies

Permission description ⓘ
Allows the app to read and write properties of Microsoft Intune-managed device configuration and device compliance policies and their assignment to groups.

Permission type ⓘ
Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Permissions granted through ⓘ
Admin Consent. A permission granted through admin consent means an admin signed in to this application with his or her organizational credential and granted on behalf of other users this particular permission.

Granted by ⓘ
An administrator

Permissions Descriptions

Maintain access to data you have given it access to

Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.

Read Microsoft Intune Device Configuration and Policies

Allows the app to read properties of Microsoft Intune-managed device configuration and device compliance policies and their assignment to groups.

Read and write Microsoft Intune Device Configuration and Policies

Allows the app to read and write properties of Microsoft Intune-managed device configuration and device compliance policies and their assignment to groups.

Read Microsoft Intune RBAC settings

Allows the app to read the properties relating to the Microsoft Intune Role-Based Access Control (RBAC) settings.

Sign in and read user profile

Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.

Read all groups

Allows the app to list groups, and to read their properties and all group memberships on behalf of the signed-in user. Also allows the app to read calendar, conversations, files, and other group content for all groups the signed-in user can access.

Access directory as the signed in user

Allows the app to have the same access to information in the directory as the signed-in user.

Sign users in

Allows users to sign in to the app with their work or school accounts and allows the app to see basic user profile information.

View users' email address

Allows the app to read your users' primary email address

View users' basic profile

Allows the app to see your users' basic profile (name, picture, user name)

Read group memberships

Allows the app to list groups, read basic group properties and read membership of all groups the signed-in user has access to.

Removing Access to HP Connect

If a AAD user needs to have access revoked from HP Connect policy creation, you can follow instructions from Microsoft documentation at

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/methods-for-removing-user-access

Appendix D: HP Connect Supported HP Models

HP Connect for Microsoft Endpoint Manager supports HP commercial platforms released since 2018 with a UEFI HP BIOS. An example of a platform released in 2018 is the HP EliteBook 840 G5 Notebook PC. If a device previously supported both Legacy and UEFI methods, it must be set to UEFI mode to be supported by the solution.

NOTE: An administrator can find out if a platform is supported by attempting to create a custom policy and searching for the platform. If not listed, then it is not currently supported.

As of release, these are the currently supported platforms:

Product name	System id
HP Collaboration G6 24 All-in-One with Zoom Rooms	874d
HP Collaboration G6 24 All-in-One with Zoom Rooms	874e
HP Collaboration G6 27 All-in-One with Zoom Rooms	874d
HP Collaboration G6 27 All-in-One with Zoom Rooms	874e
HP Elite Dragonfly G2 Notebook PC	8716
HP Elite Dragonfly Max Notebook PC	8890
HP Elite Dragonfly Notebook PC	861f
HP Elite x2 G8 Tablet	870D
HP EliteBook 735 G5 Notebook PC	83da
HP EliteBook 735 G6 Notebook PC	8589
HP EliteBook 745 G5 Notebook PC	83d5
HP EliteBook 745 G6 Notebook PC	8584
HP EliteBook 755 G5 Notebook PC	83d5
HP EliteBook 830 G5 Notebook PC	83b3
HP EliteBook 830 G6 Notebook PC	854a
HP EliteBook 830 G7 Notebook PC	8723
HP EliteBook 830 G8 Notebook PC	880D
HP EliteBook 835 G7 Notebook PC	8760
HP EliteBook 835 G8 Notebook PC	8895
HP EliteBook 836 G5 Notebook PC	83b3
HP EliteBook 836 G6 Notebook PC	854a
HP EliteBook 840 Aero G8 Notebook PC	880D
HP EliteBook 840 G5 Healthcare Edition Notebook PC	845d
HP EliteBook 840 G5 Notebook PC	83b2
HP EliteBook 840 G6 Healthcare Edition Notebook PC	8549
HP EliteBook 840 G6 Notebook PC	8549
HP EliteBook 840 G7 Notebook PC	8723
HP EliteBook 840 G8 Notebook PC	880D
HP EliteBook 845 G7 Notebook PC	8760
HP EliteBook 845 G8 Notebook PC	8895
HP EliteBook 846 G5 Notebook PC	83b2
HP EliteBook 850 G5 Notebook PC	83b2
HP EliteBook 850 G6 Notebook PC	8549
HP EliteBook 850 G7 Notebook PC	8724
HP EliteBook 850 G8 Notebook PC	8846
HP EliteBook 855 G7 Notebook PC	8760
HP EliteBook 855 G8 Notebook PC	8895
HP EliteBook x360 1030 G7 Notebook PC	876d
HP EliteBook x360 1030 G8 Notebook PC	8720

HP EliteBook x360 1040 G6 Notebook PC	857f
HP EliteBook x360 1040 G7 Notebook PC	876d
HP EliteBook x360 1040 G8 Notebook PC	8720
HP EliteBook x360 830 G5 Notebook PC	853d
HP EliteBook x360 830 G6 Notebook PC	8548
HP EliteBook x360 830 G7 Notebook PC	8725
HP EliteBook x360 830 G8 Notebook PC	8847
HP EliteDesk 705 G5 Desktop Mini PC	8619
HP EliteDesk 705 G5 Small Form Factor PC	8617
HP EliteDesk 705 G5 Small Form Factor PC	8618
HP EliteDesk 800 G5 Desktop Mini PC	8593
HP EliteDesk 800 G5 Desktop Mini PC	8594
HP EliteDesk 800 G5 Desktop Mini PC	8595
HP EliteDesk 800 G5 Small Form Factor PC	8592
HP EliteDesk 800 G5 Tower PC	8591
HP EliteDesk 800 G6 Desktop Mini PC	870f
HP EliteDesk 800 G6 Desktop Mini PC	8710
HP EliteDesk 800 G6 Desktop Mini PC	8711
HP EliteDesk 800 G6 Small Form Factor PC	870B
HP EliteDesk 800 G6 Small Form Factor PC	870C
HP EliteDesk 800 G6 Tower PC	870B
HP EliteDesk 800 G6 Tower PC	870C
HP EliteDesk 800 G8 Desktop Mini PC	889F
HP EliteDesk 800 G8 Desktop Mini PC	88A0
HP EliteDesk 800 G8 Small Form Factor PC	889C
HP EliteDesk 800 G8 Tower PC	889C
HP EliteDesk 805 G6 Desktop Mini PC	872B
HP EliteDesk 805 G6 Desktop Mini PC	872C
HP EliteDesk 805 G6 Small Form Factor PC	872B
HP EliteDesk 805 G8 Desktop Mini PC	8881
HP EliteDesk 805 G8 Small Form Factor PC	8883
HP EliteDesk 880 G5 Tower PC	8591
HP EliteDesk 880 G6 Tower PC	870B
HP EliteDesk 880 G6 Tower PC	870C
HP EliteDesk 880 G8 Tower PC	889C
HP EliteOne 800 G5 23.8-in Healthcare Edition All-in-One	859f
HP EliteOne 800 G5 23.8-in Healthcare Edition All-in-One	85a0
HP EliteOne 800 G5 23.8-in Healthcare Edition All-in-One	85eb
HP EliteOne 800 G5 23.8-inch All-in-One	859f
HP EliteOne 800 G5 23.8-inch All-in-One	85a0

HP EliteOne 800 G5 23.8-inch All-in-One	85eb
HP EliteOne 800 G6 24 All-in-One PC	874d
HP EliteOne 800 G6 24 All-in-One PC	874e
HP EliteOne 800 G6 27 All-in-One PC	874D
HP EliteOne 800 G6 27 All-in-One PC	874d
HP EliteOne 800 G6 27 All-in-One PC	874D
HP EliteOne 800 G6 27 All-in-One PC	874E
HP EliteOne 800 G6 27 All-in-One PC	874E
HP EliteOne 800 G6 27 All-in-One PC	874e
HP EliteOne 800 G8 24 All-in-One PC	88AA
HP EliteOne 800 G8 27 All-in-One PC	88AA
HP Engage Flex Mini Retail System	8715
HP ProBook 430 G5 Notebook PC	8377
HP ProBook 430 G6 Notebook PC	8536
HP ProBook 430 G7 Notebook PC	869b
HP ProBook 430 G8 Notebook PC	87DF
HP ProBook 430 G8 Notebook PC	8806
HP ProBook 440 G5 Notebook PC	837b
HP ProBook 440 G6 Notebook PC	8537
HP ProBook 440 G7 Notebook PC	869d
HP ProBook 440 G8 Notebook PC	87E0
HP ProBook 440 G8 Notebook PC	8807
HP ProBook 445 G6 Notebook PC	85d9
HP ProBook 445 G7 Notebook PC	8730
HP ProBook 445 G8 Notebook PC	8861
HP ProBook 445R G6 Notebook PC	85ad
HP ProBook 450 G5 Notebook PC	837d
HP ProBook 450 G6 Notebook PC	8538
HP ProBook 450 G7 Notebook PC	86a0
HP ProBook 450 G8 Notebook PC	87E1
HP ProBook 450 G8 Notebook PC	8808
HP ProBook 455 G5 Notebook PC	836e
HP ProBook 455 G5 Notebook PC	8370
HP ProBook 455 G6 Notebook PC	85d9
HP ProBook 455 G7 Notebook PC	8730
HP ProBook 455 G8 Notebook PC	8864
HP ProBook 455R G6 Notebook PC	85ad
HP ProBook 470 G5 Notebook PC	837f
HP ProBook 630 G8 Notebook PC	87EA
HP ProBook 630 G8 Notebook PC	87ED

HP ProBook 635 Aero G7 Notebook PC	8830
HP ProBook 635 Aero G8 Notebook PC	8892
HP ProBook 640 G5 Notebook PC	856d
HP ProBook 640 G7 Notebook PC	882c
HP ProBook 640 G8 Notebook PC	87EA
HP ProBook 640 G8 Notebook PC	87ED
HP ProBook 650 G5 Notebook PC	856e
HP ProBook 650 G7 Notebook PC	882d
HP ProBook 650 G8 Notebook PC	87EA
HP ProBook 650 G8 Notebook PC	87ED
HP ProBook x360 11 G5 EE Notebook PC	86cf
HP ProBook x360 11 G7 Education Edition Notebook PC	887D
HP ProBook x360 11 G7 EE	887D
HP ProBook x360 11 G7 EE	887D
HP ProBook x360 435 G7 Notebook PC	8735
HP ProBook x360 435 G8 Notebook PC	8886
HP ProDesk 400 G5 Desktop Mini PC	859c
HP ProDesk 400 G5 Microtower PC	83f0
HP ProDesk 400 G5 Microtower PC	83f1
HP ProDesk 400 G5 Small Form Factor PC	83f2
HP ProDesk 400 G6 Desktop Mini PC	871a
HP ProDesk 400 G6 Microtower PC	8599
HP ProDesk 400 G6 Microtower PC	859a
HP ProDesk 400 G6 Small Form Factor PC	859b
HP ProDesk 400 G7 Microtower PC	8717
HP ProDesk 400 G7 Small Form Factor PC	8719
HP ProDesk 405 G6 Desktop Mini PC	872E
HP ProDesk 405 G6 Desktop Mini PC	8836
HP ProDesk 405 G8 Desktop Mini PC	8882
HP ProDesk 405 G8 Desktop Mini PC	8968
HP ProDesk 405 G8 Small Form Factor PC	8884
HP ProDesk 480 G5 Microtower PC	83f0
HP ProDesk 480 G5 Microtower PC	83f1
HP ProDesk 480 G6 Microtower PC	8599
HP ProDesk 480 G6 Microtower PC	859a
HP ProDesk 480 G7 PCI Microtower PC	8718
HP ProDesk 600 G5 Desktop Mini PC	8598
HP ProDesk 600 G5 Microtower PC	8596
HP ProDesk 600 G5 Microtower PC	861a
HP ProDesk 600 G5 Microtower PC (with PCI slot)	8596

HP ProDesk 600 G5 Microtower PC (with PCI slot)	861a
HP ProDesk 600 G5 Small Form Factor PC	8597
HP ProDesk 600 G6 Desktop Mini PC	8715
HP ProDesk 600 G6 Microtower PC	8712
HP ProDesk 600 G6 PCI Microtower PC	8713
HP ProDesk 600 G6 Small Form Factor PC	8714
HP ProDesk 680 G6 PCI Microtower PC	8713
HP ProOne 400 G5 20-inch All-in-One Business PC	85a1
HP ProOne 400 G5 20-inch All-in-One Business PC	85a2
HP ProOne 400 G5 23.8-inch All-in-One Business PC	85a1
HP ProOne 400 G5 23.8-inch All-in-One Business PC	85a2
HP ProOne 400 G6 20 All-in-One PC	871b
HP ProOne 400 G6 20 All-in-One PC	871c
HP ProOne 400 G6 20 All-in-One PC	880f
HP ProOne 400 G6 20 All-in-One PC	8810
HP ProOne 400 G6 24 All-in-One PC	871B
HP ProOne 400 G6 24 All-in-One PC	871C
HP ProOne 400 G6 24 All-in-One PC	880F
HP ProOne 400 G6 24 All-in-One PC	8810
HP ProOne 440 G5 23.8-in All-in-One Business PC	85a1
HP ProOne 440 G5 23.8-in All-in-One Business PC	85a2
HP ProOne 440 G6 24 All-in-One PC	871b
HP ProOne 440 G6 24 All-in-One PC	871c
HP ProOne 440 G6 24 All-in-One PC	880f
HP ProOne 440 G6 24 All-in-One PC	8810
HP ProOne 600 G5 21.5-in All-in-One Business PC	85a1
HP ProOne 600 G5 21.5-in All-in-One Business PC	85a2
HP ProOne 600 G6 22 All-in-One PC	871b
HP ProOne 600 G6 22 All-in-One PC	871c
HP Z1 Entry Tower G5	8591
HP Z1 Entry Tower G6	870b
HP Z1 Entry Tower G6	870c
HP Z1 Entry Tower G8	889c
HP Z2 G8 Tower Workstation Desktop PC	88BE
HP Z2 Mini G4 Workstation	8457
HP Z2 Mini G4 Workstation	8458
HP Z2 Mini G5 Workstation	8754
HP Z2 Mini G5 Workstation	8755
HP Z2 Small Form Factor G4 Workstation	8456
HP Z2 Small Form Factor G8 Workstation	88BF

HP Z2 Tower G4 Workstation	8455
HP Z2 Tower G5 Workstation	8750
HP Z2 Tower G5 Workstation	8751
HP Z4 G4 Workstation	81c5
HP Z6 G4 Workstation	81c6
HP Z8 G4 Workstation	81c7
HP ZBook 14u G5 Mobile Workstation	83b2
HP ZBook 14u G6 Mobile Workstation	8549
HP ZBook 15 G5 Mobile Workstation	842a
HP ZBook 15 G6 Mobile Workstation	860f
HP ZBook 15u G5 Mobile Workstation	83b2
HP ZBook 15u G6 Mobile Workstation	8549
HP ZBook 17 G6 Mobile Workstation	860c
HP ZBook Create G7 Notebook PC	8736
HP ZBook Firefly 14 G7 Mobile Workstation	8723
HP ZBook Firefly 14 G7 Mobile Workstation	8724
HP ZBook Firefly 14 inch G8 Mobile Workstation PC	880D
HP ZBook Firefly 15 G7 Mobile Workstation	8724
HP ZBook Firefly 15.6 inch G8 Mobile Workstation PC	8846
HP ZBook Fury 15 G7 Mobile Workstation	8783
HP ZBook Fury 15.6 Inch G8 Mobile Workstation PC	8870
HP ZBook Fury 15.6 Inch G8 Mobile Workstation PC	8870
HP ZBook Fury 17 G7 Mobile Workstation	8780
HP ZBook Fury 17.3 Inch G8 Mobile Workstation PC	886d
HP ZBook Fury 17.3 Inch G8 Mobile Workstation PC	886d
HP ZBook Power 15.6 inch G8 Mobile Workstation PC	888d
HP ZBook Power G7 Mobile Workstation	87EC
HP ZBook Studio 15.6 inch G8 Mobile Workstation PC	8873
HP ZBook Studio G5 Mobile Workstation	8427
HP ZBook Studio G5 Mobile Workstation	844f
HP ZBook Studio G7 Mobile Workstation	8736
HP ZBook Studio x360 G5 Convertible Workstation	8427
HP ZBook Studio x360 G5 Convertible Workstation	844f
HP ZCentral 4R Workstation	873E

Appendix E: Usage FAQ

HP Connect for MEM

How do I add HP Connect to my existing Azure tenant?

HP Connect is added to an organization's Azure tenant as an Enterprise Application. This requires that a tenant administrator be the 1st login to admin.hp.com. When onboarded correctly, 2 applications will be added to the tenant, HP Connect for MEM, and HP MEM Connector Service – both pointing to https://admin.hp.com

Will HP Connect support other consoles?

At introduction, HP Connect for MEM supports Microsoft's cloud management tool, Endpoint Manager/Intune with a dedicated connector. HP will investigate how to potentially support other management systems, like VMWare's Workspace ONE, Ivanti, etc.

Who is authorized to access HP Connect and create policies?

Based on the permissions required to allow an Enterprise Application access to device groups, tenant and Intune administrators have rights (assuming permissions are accepted) to use HP Connect at admin.hp.com. There is ongoing investigation to determine if/how to enable access to non-Intune-Administrator users.

Is there a cost for using HP Connect?

HP Connect for MEM is available at no cost to HP customers for BIOS management operations.

Permissions granted during Early Access/Pilot

If your tenant was enabled during the Early Access period the accepted permissions include one that is no longer required for HP Connect. This is the 'Read Directory Data' permission. If the 'HP MEM Connector Service' Enterprise Application in your tenant include this permission, you can remove it. One option is to remove all permissions, and have a Global Administrator login again, which will be prompted to accept the required permissions.

Do I have to install anything on a device to support HP Connect?

NO. HP Connect relies on the Microsoft Endpoint Manager Intune MDM agent on each device to apply the published compliance policies as proactive remediations. The Intune MDM agent will execute Detection (and possibly) Remediation scripts (as defined by the Connect policy). The policy will install and manage a copy of the HP Client management Script Library (CMSL) on each managed device.

Do I have to install CMSL on each managed HP system?

NO. HP Connect policies will maintain a separate copy of HP CMSL to be use by its scripts doing BIOS management tasks. This version will not conflict with any other already installed and used on a device.

What systems are supported by HP Connect?

HP Connect supports HP devices with a commercial HP BIOS released since 2018. These systems support HP Sure Admin authentication as a more secure method for authenticating to the BIOS.

The supported product list is available on the HP Connect for MEM User Guide as an Appendix. An administrator can also find out if a model is supported by searching for the model at policy creation time.

What Windows versions are supported by HP Connect?

HP Connect support endpoint devices running Windows 10 or Windows 11.

Does HP Connect maintain separate logs?

Yes. When the Intune MDM agent executes an HP policy as a proactive remediation compliance, HP Connect will write to a log at `%ProgramData%\HP\Endpoint\Logs.` Additional logs that are described in the User Guide. However, if a device in the device group does not meet the compliance policy requirements, nothing is done, and no information is written to the log.

HP Connect fails to retrieve device groups

When HP Connect attempts to retrieve a very large number of device groups from Azure using graph API there may be instances when the connection will not allow this to happen. HP is working on a solution to likely release by end of February. Until then, HP Connect may not work with that tenant correctly.

About Policies

What devices are targeted when a HP Connect policy is published to a device group?

HP Connect policies apply ONLY to supported HP commercial devices when applied to a device group. HP Connect policies apply as follows:

BIOS Authentication	applies to ALL devices in the device group
BIOS Settings	applies to a selected model in the device group
BIOS Update	applies to ALL devices in the device group, or as a rule, to a selected model (based on the update method chosen)

What is the outcome of publishing an HP Connect policy to MEM?

When a policy is created in HP Connect and published to a device group, Microsoft's graph API is used to interact with Azure, find the selected device group, and publish the policy as a Proactive Remediation.

The Proactive Remediation will consist of Detection and Remediation scripts, and a schedule for the compliance to take effect will be set. The default schedule is every 24 hours. The Proactive Remediation will be updated as policies are added or removed from the device group.

Can multiple policies be applied to the same device group?

Yes. HP Connect will consolidate all applied/published policies into a single proactive remediation. Any policies that generate a conflict (ex. 2 policies of same type for same platform) may need to be resolved before being published.

Can I modify the check-in schedule of a proactive remediation?

Yes. The default compliance schedule can be modified by selecting the Proactive Remediation (at: MEM admin center, Reports, Endpoint Analytics, Proactive Remediations), selecting Properties, Assignments Edit, and clicking on the selected group list. The default schedule is set to once every 24 hours (was every 60 minutes in initial versions).

I published a policy, and nothing happens on the devices

An HP Connect policy published to an Azure device group becomes a proactive remediation managed by MEM/Intune. These remediations are executed on each device by the built-in Intune MDM agent which checks in on its own schedule. Therefore, an HP Connect policy will only be enforced when a device agent checks in with the management console. To speed up the process during testing, you can sync from the device manually. The HP Connect user guide describes the process.

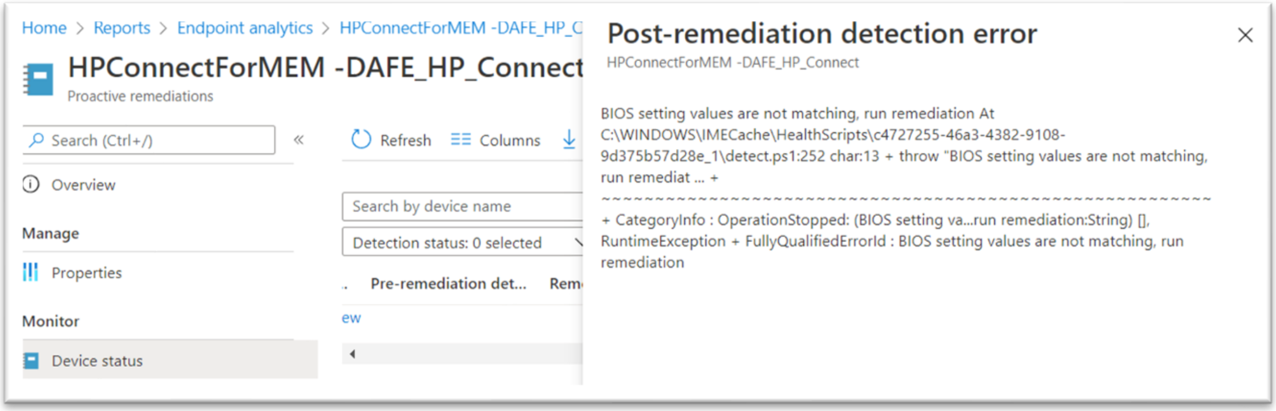
Device does not get policy even after I Sync manually

If the device does not appear to sync the HP created proactive remediation, confirm the schedule of the remediation. In MEM console, select the proactive remediation and verify the schedule. If it is longer than the last remediation sync, doing another sync will not cause it to be run. You may need to modify the schedule for a shorter time period, sync again as needed, and then reset the schedule, if needed.

In MEM, how do I check the status of a Proactive Remediation for a device?

Microsoft Endpoint Manager does not seem to provide significant information on pre and post-remediations, but to find whatever is available, in the MEM console, find and select the proactive remediation, click on ‘Device status’, and select the ‘Columns’ menu item to enable all non-selected fields.

Select a device you need information on, scroll and then click on the ‘Review’ link in the post-remediation error column. Here is an example


Home > Reports > Endpoint analytics > HPConnectForMEM -DAFE_HP_C
HPConnectForMEM -DAFE_HP_Connect
Proactive remediations
Search (Ctrl+/)
«
Overview
Manage
Properties
Monitor
Device status
Refresh
Columns
Search by device name
Detection status: 0 selected
Pre-remediation det...
Rem
ew
Post-remediation detection error
HPConnectForMEM -DAFE_HP_Connect

```
BIOS setting values are not matching, run remediation At
C:\WINDOWS\IMECache\HealthScripts\c4727255-46a3-4382-9108-
9d375b57d28e_1\detect.ps1:252 char:13 + throw "BIOS setting values are not matching,
run remediat ... +
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : OperationStopped: (BIOS setting va...run remediation:String) [],
RuntimeException + FullyQualifiedErrorId : BIOS setting values are not matching, run
remediation
```

BIOS Update Policies

Missing BIOS Updates

HP Connect installs Microsoft-signed BIOS packages found in Windows Update (WU) servers. Note that after a BIOS is released by HP (as Softpaq) and uploaded to WU servers, it may take up to 4 weeks to make it to wide distribution, due to standard Microsoft release flighting and telemetry observations.

Note that not all HP BIOS releases are available in WU, so it is possible that some BIOS (release as HP Softpaqs) may not be available in HP Connect. You may contact HP to confirm for specific BIOS version needs.

What if a user dismisses the restart toaster notification?

When a user dismisses a BIOS Update (for example) restart notification, it will reappear at next Intune MDM check-in, and will continue to reappear until the system is restarted. HP Connect will have the ability (soon) to configure the behavior for the user dismissing the notification. The ability to customize this behavior when a policy is being created is in development.

What happens if a device is not plugged-in when doing a BIOS update?

HP Connect does not check if the device is on A/C or working off battery. The BIOS update will continue when on battery but will not occur unless the battery is at least at 50% of charge capacity. This is a requirement native to the HP BIOS. The BIOS flash will be done on next reboot, if the device is plugged-in, or battery charge is at proper level.

Note that HP Sure Start technology is designed to manage BIOS corruption with its self-healing technology.

I cannot downgrade the BIOS with an HP Connect policy

HP Connect is designed to not downgrade a BIOS by policy. If a device sports a version newer (or similar) to the version defined in the policy, the policy will not take effect. To downgrade a BIOS to a previous version, use an alternative method, like HP CMSL commands, or executing an BIOS Softpaq.

As example, the following HP CMSL command will install a particular version to a system (CMSL must be available on the device, and version is not locked in the BIOS):

```
Get-HPBiosUpdates -Flash -Version 1.04.01 -Bitlocker Suspend -Force -Yes
```

I get a missing BIOS setting error and the BIOS update fails

A BIOS Update policy fails and the HP Connect log shows this: Setting not found: '*Native OS Firmware Update Service*'. With some platforms, earlier generation of the BIOS did not include this setting which allows remote update of the (Windows Update packaged) BIOS. In this case, the BIOS must be manually updated to a more recent version for remote BIOS updates to be possible. In addition, the setting must be set to 'Enable'

Find the error in the HP Connect log on a device at `%ProgramData%\HP\Endpoint\Logs`

The setting value can be checked on a device with HP CMSL or a WMI call. This is an example WMI script (if HP CMSL is not installed on the device):

```
(gwmi -Class 'HP_BIOSSetting' -Namespace 'root/hp/instrumentedBIOS' |
Where-Object {$_.Name -match "native os"}).Value
```

How Is Microsoft Bitlocker handled?

Whenever an HP policy requires the device to be restarted, HP Connect will detect when the device restarts or the user does a shutdown. Bitlocker is suspended just prior to that event.

BIOS Authentication Policies

Managing BIOS passwords

Devices with no BIOS passwords

When an authentication policy with password is applied, each device not currently having a BIOS password gets the password set and a hint of the password is stored in the BIOS (as a UEFI variable). Thereafter, if a different authentication policy with password is applied, HP Connect uses the hint to know what the existing password is and uses it to allow the change to the new password. Then, the password hint is updated.

Devices with 'known' BIOS passwords

For HP Connect to manage these devices, the initial authentication policy must match the existing password in the devices. The policy will update the password (since it is the same) and store a password hint in the BIOS for future use.

> *Recommended process: assume known BIOS passwords 'password1' and 'password2' are known and exist in a device group (group A) along with devices with no BIOS passwords*
>
> *Attempt to get as many devices to the first password ('password1') as possible, then move to the next password ('password2'), etc. These steps will take time to accomplish, as all devices need to check in and get the BIOS authentication remediation done*

1. Setup BIOS authentication policy with 'password1', named, say, PWD1
   a. add (known) 'password1' secret to HP Connect secrets vault
   b. create BIOS Authentication policy using secret PWD1
   c. apply policy to device group A
   d. wait until all devices check-in (could take days) and either succeed in applying password or fail due to existing BIOS different from 'password1'
2. Setup BIOS authentication policy with 'password2', name PWD2
   a. Follow steps a..d from 1. above but using secret PWD2
   b. All devices (with no passwords, or with 'password1' or 'password2') will now have 'password2' in the BIOS and HP Connect will know about it and able to manage those passwords
3. Repeat step 2 for additional 'known' passwords, if necessary

Devices with 'unknown' BIOS passwords

HP Connect is not able to manage devices with existing passwords that are not known. In such cases, contact HP for options that might be considered. In some cases, an out-of-warranty motherboard replacement may be the only option.

Managing HP Sure Admin BIOS authentication

How do I provision HP Sure Admin?

To provision HP Sure Admin, at least 2 certificates must be available. These are Endorsement and Signing certificates. HP Connect will obtain the cryptographic key pairs from each. Then a BIOS Authentication policy needs to be created linking to both named secrets (keys). An additional certificate is required to protect the BIOS from unauthorized local F10 access, the Local Access Key (LAK) certificate. If not provided, HP Connect will use the Signing Key as the LAK and provision it to secure the BIOS.

A reboot is required for the provisioning policy to take effect.

How do I protect local F10 access with Sure Admin?

Once HP Sure Admin is provisioned on devices via HP Connect authentication policy, an ‘approved’ user that presses F10 at power on to access the BIOS will need to use a phone app (HP Sure Admin, installed from the Apple or Android store) to scan a QR code displayed on the screen and enter AAD credentials. With a challenge/response mechanism, a pin will be presented on the app to be entered on the device, which will then allow access to the BIOS.

Note that an administrator must use a phone app the first time on a provisioned device to scan the visible QR code and provide AAD credentials – on any device where HP Sure Admin is enabled. This will invoke a process to add a supporting HP Sure Admin Enterprise Application to the Azure tenant, where it will be used for all local authentication requests.

What happens if I remove an authentication policy from a device group?

When an authentication policy is removed from a device group, HP Connect will create a no-auth policy and apply it back to the group. This means any authentication, including Sure Admin keys or passwords, will be removed from each device when they check in.

If there is a need to maintain existing authentication implemented in each device, then the MEM proactive remediation should be deleted, or perhaps the schedule changed to not run again.

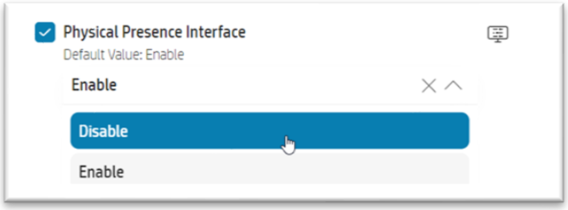
BIOS Setting Policies

Can I apply a Settings policy to multiple platforms?

NO. Initially, HP Connect requires that a BIOS Settings policy be applied to a particular platform (model). There is ongoing development to enhance the feature to allow for a BIOS settings policy to apply to multiple platforms. The enhancement will be released once development of the feature is complete.

What is the meaning of the icon shown next to some settings?

The icon, resembling a display, indicates that certain setting modifications will require physical presence at the device being applied to accept the change (typing a 4-digit pin), unless the Physical Presence Interface setting was disabled in the first place



☑ Physical Presence Interface

Default Value: Enable

Enable

Why didn’t a BIOS setting get set?

Certain BIOS settings may require BIOS authentication enabled, either password or HP Sure Admin. If BIOS security is not set, the setting in question may not be settable. The F10 BIOS settings show if a particular setting requires BIOS administrator credentials to be set.

Revisions

Version 1.1.4

Added HP notice to document pages

Added support for Sure Admin certificate passwords

Version 1.2.0

Added section on new Global Setting policies

Added FAQ as Appendix E