HP Connect User Guide

SUMMARY

HP Connect is a cloud application designed to ease the management of UEFI BIOS on supported HP systems. HP Connect has a framework for developing BIOS management policies that are published to Microsoft Azure device groups.

Legal information

Second Edition: March 2023

First Edition: January 2023

Document Part Number: N39848-002

Table of contents

1 Getting started with HP Connect

HP Connect is a cloud application designed to ease the management of UEFI BIOS on supported HP systems. HP Connect has a framework for developing BIOS management policies that are published to Microsoft Intune device groups.

HP Connect creates the policies and Intune runs them as compliance proactive remediations. No additional software needs to be downloaded to or installed in each device.

HP Connect supports the following types 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

2 Requirements

Before you use HP Connect, make sure you have met the following prerequisites.

- Administrative access to a Microsoft Azure tenant
- An appropriate subscription, including support for Proactive Remediations
- MEM configured as the cloud-based mobile device management (MDM) for device management
- Modern internet browser (Microsoft Edge, Google Chrome, Mozilla Firefox, and so forth)

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

NOTE: To interact with Microsoft Azure AD and Intune, HP Connect requires certain permissions to access the company tenant. HP Connect uses these permissions 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.

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.

NOTE: Policies created by HP Connect are published to and enforced by MEM as proactive remediations. HP Connect interacts with Azure and Intune via the Microsoft Graph API.

3 Onboarding process

The onboarding process includes the integration of HP Connect with the Azure tenant as an Enterprise Application.

To allow this integration, a tenant Global Administrator initially logs in at https://admin.hp.com with Azure credentials and accepts the required permissions through a standard Microsoft dialog box.

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

- 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

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 can log in and use HP Connect at admin.hp.com after accepting permissions. The Global Administrator can, if desired, accept permissions for all other administrators by selecting **Consent on behalf of your organization** in the window.

See Requirements on page 2 for information about the permissions required for HP Connect to interact with Microsoft Intune.

4 Offboarding process

Administrators can end their organization's use of HP Connect on the Settings tab.

1. To end your organization's use of HP Connect, select the **Settings** tab and select **Deactivate Account**.

   The Deactivate Account window displays what comes next when the account is deactivated. You have the following options:

   - **Keep Account** to stop the process
   - **Proceed with Deactivation** to start the clock on full deactivation

   Deactivation starts a 30-day countdown where tenant administrators are able to log in to admin.hp.com in read-only mode (view only). At the end of the 30 days, all policies and secrets created for the organization in HP Connect are permanently deleted. Be sure to review the details in the Deactivation window to understand what to expect. The Microsoft Intune Proactive Remediation scripts published by HP Connect to Azure AD remain in place. If you no longer need these Remediations, you must manually remove them from MEM.

2. At the final confirmation window, select **I read and agree** and select **Confirm Deactivation** to start the process.

   Global Administrators can reactivate the account during the next 30 days by logging back in to HP Connect at admin.hp.com and selecting **Reactivate Account**.

During the 30-day deactivation period, when Intune Administrators log in to admin.hp.com, a banner shows them the action that was taken. To reverse deactivation, a Tenant global administrator is again required to log in and restore access.

5 The HP Connect sidebar menu

When you log in to HP Connect, a dashboard with useful information is displayed. A sidebar menu allows easy access to policies, groups, and authentication secrets stored in an HP vault.

Home tab

After you log in, you see the dashboard, which is also referred to as the Home tab.

You can do the following tasks from the dashboard:

- Select **New Policy** to create policies
- Select **New Secret** to add authentication secrets to the secrets vault

You can use authentication secrets when you define a policy to do the following:

- Implement HP Sure Admin BIOS protection (a secure authentication mechanism using cryptographic certificates)
- Setting or managing BIOS passwords

In addition, the dashboard displays an overview of the policies and 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 dashboard, you can select the link to view a video about HP Connect and other HP endpoint management solutions, such as the HP TechPulse service.

Policies tab

The Policies tab has a list of created policies.

Each policy in the list shows if it is In Use (for example, a policy published to a device group) or is Not In Use.

Create a policy

Use this procedure to create a policy in HP Connect for Microsoft Intune.

- Select **New Policy** to create a policy from this tab.

  After you create a policy, you can publish it to or remove it from device groups by selecting **Add or Remove Groups**. If you add or remove a group, and the policy is reapplied to Intune, all existing policies in that group are affected. In addition, the policy version number shown by MEM increments.

After you apply a policy to a group or multiple groups of devices, the policy entry shows as In Use, and you cannot edit it.

Edit a policy

You can edit a policy if it is not currently published to a device group.

1. To edit a policy that has been published and applied to a device group, select the policy from the list.
2. Select **Add or Remove Groups**.
3. Clear all of the group selections, and then select **Save**.

Certain edits could generate a conflict, in which case you would not be able to publish the policy. For example, if you edit a BIOS Settings policy that applies to a specific platform, you cannot reassign the policy to a different platform because the BIOS settings might not be the same for both platforms. In this case, you must create a new BIOS Settings policy.

Deleting a policy by clicking the trash-can icon immediately removes it from HP Connect.

Add groups to or remove groups from a policy

To enforce a policy on HP-supported devices, the policy must be published to an Azure AD device group. You can also remove a device group from the policy. When adding or removing Connect policies from a device group, any existing published policies for the selected group are recreated with the changes made.

To add or remove device groups, go to the Policy List window and use this procedure.

1. Select the policy to be modified, and then select **Add or Remove Groups**.

   If you add an Azure group and select **Save**, a dialog box opens.
2. To save the policy without publishing, select the following option:

   - **Publish**

   Selecting **Publish** updates the policy to the organization's tenant, where it is enforced through its remediation and compliance task.

Resolve policy conflicts

If a current group device policy exists for a similar type (such as Updates, Settings, or Authentication) on the same platform, it results in a conflict, and the new policy replaces the existing policy when published.

- To prevent the new policy from overwriting the existing policy, clear the Group selection in the conflict dialog box. Then, select one of the following options:

  - **Apply**: Confirms that you want to apply the new policy.
  - **Keep**: Keeps the current policy.
  - **View**: Opens a dialog box that shows the difference between applying a new policy or keeping the current policy.

Apply a policy

After you create a BIOS policy and publish it 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 same device group, the new policy is added to the current policy and the version number is increased.

NOTE: HP Connect policies are published as proactive remediations and can be found on the Microsoft Intune 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.

After you select the appropriate remediation compliance policy, the published HP Connect policies are listed to the right of Properties. Under Settings, you can see whether the Detection and Remediation scripts were applied (marked as Yes), and the schedule for How Often the policy runs in this group.

Groups tab

The Groups tab displays a list of the organization's defined Azure Active Directory groups. Administrators can use the search field to find specific groups by name.

Select a group name from the list on the left to open a panel on the right side with a list of the HP Connect policies that are already assigned to that group.

The side properties card also indicates when the policy was created, modified, or published.

Secrets tab

The Secrets tab is where BIOS authentication secrets are managed in HP Connect. These secrets are stored in a secure cloud vault.

Select **New Secret** to open a dialog box that you can use to add certificates for HP Sure Admin to use or passwords to administer BIOS admin/setup passwords.

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

Adding Sure Admin keys to the Secrets vault

HP Sure Admin requires certain certificates. HP Connect reads the certificates and gets the embedded private/public keys to configure HP Sure Admin. These cryptographic keys are then used when you create BIOS authentication policies and when you authorize BIOS settings changes.

Because you can create and maintain certificates within HP Connect, you do not need externally created certificates. However, you can still use them to implement HP Sure Admin.

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

1. Complete one of the following tasks:
   - From the dashboard, select the **Secrets** tab and select **New Secret**.
   - From the Home tab (dashboard), select **New Secret**.
2. On the Secret Information page, complete the following fields:
   - **Name**: Type a description of the purpose of this secret in this field to identify the purpose of the secret.
   - **Type**: From the dropdown menu, select **Certificate**.
   - **Certificate Type**: Select one of the options that you see next.

- **Secure Platform Management**:

  The Secure Platform Management (SPM) secret helps you set up the trusted firmware environment you need to enable HP Sure Admin. You can also use it for other future HP BIOS security needs.

  The default selection allows HP Connect to create the certificates that contain all the appropriate public/private keys that are required to implement the solution. For SPM, you must have the Endorsement and the Signing keys. Select either **Create Certificate** or **Upload Certificate** for both keys.

  During the process of creating a certificate, HP Connect manages several key defaults, such as expiration date, location information, and organization name and OU. Select the entry below **Create Certificate** to define these settings.

- **Local Access**:

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

  As with the Secure Platform Certificates, choose one of the options for this key, and then edit the required settings for your organization.

- **Description**: Type a description of the secret in this field.
- **Tags**: Type a tag name and select **Add Tag**. Add as many tags as needed.
- **Endorsement Key**: This is a certificate in pfx format.
- **Signing Key**: This is a certificate in pfx format.

3. Select **Save**.

   If HP Connect creates and maintains the certificate keys, they are secured on a Secrets vault and strictly assigned only to policies developed and applied to your tenant.

4. If needed, repeat the previous steps to add a new secret with a **Certificate Type** different from the one you already created (for example, a **Local Access** type).

NOTE: If you save the Secure Platform Management (SPM) key, but not the Local Access key, HP Connect uses the Signing Key (saved as the SPM secret) as the Local Access Key during provisioning.

Adding Passwords to the Secrets vault

HP Connect manages passwords and stores them in a cloud vault. To add a Password secret to HP Connect, follow these steps.

1. Complete one of the following tasks:

   - From the dashboard, select the **Secrets** tab and click **New Secret**.
   - From the home (dashboard) screen, select **New Secret**.

2. On the Secret Information page, complete the following fields:

   - **Name**: Type a description of the purpose of this secret in this field to identify the purpose of the secret.
   - **Type**: From the dropdown menu, select **Password**.

- **Description**: Type a description of the secret in this field.
- **Tags**: Type a tag name and select **Add Tag**. Add as many tags as needed.
- **Complexity Rules**: From the dropdown menu, select the **HP Standard** default or select a different type.
- **Password**: Type a password that meets the requirements of the complexity rule you selected.

3. Select **Save**.

Settings tab

You can select the Settings tab to initiate a deactivation (offboarding) process. Only a global tenant administrator can initiate deactivation.

For more information about offboarding, see Offboarding process on page 4.

6 HP Connect Policies

HP Connect supports BIOS updates policies, BIOS settings policies, and BIOS authentication policies.

BIOS updates policies

HP Connect supports the following types of BIOS updates policies.

NOTE: Set the **HP BIOS Native OS Firmware Update Service** setting to **Enable** (the default) to allow remote BIOS updates. A BIOS Updates policy that you send to the device might fail if an older BIOS for a platform does not have the setting or the setting is set to **Disable**.

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

  When this type of policy is applied to a group of supported platforms, Intune uses 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 applies all new BIOS releases that HP Connect marks as **Critical** to every device in the selected group.

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

  This policy applies a BIOS update to a device group based on a defined criteria or rule. The policy is applied only to a specific platform (HP model), and can be configured to follow one of these rules:

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

NOTE: HP Connect does not support the installation of a BIOS version that is older than the version that is already on the device. You cannot downgrade the BIOS version. If a device has a BIOS version that is newer than or the same as the version defined in the policy, the policy is ignored.

BIOS update policies are grouped under the following categories:

- **Global policy**
- **Platform policy**

When you create a policy, a dialog box opens, prompting you to apply the policy or end its creation.

- Select **Close** to end the policy creation task and return to the Policy list.
- Select **Apply** to open a Publish Policy dialog box where you must choose a Microsoft Azure device group.
- Enter a string in the Search field to find a specific group.

If you try to apply a BIOS update policy that would interfere with an existing published (In-Use) policy, a conflict occurs. You can see a warning that a similar policy already exists.

Your new policy overwrites the existing policy when you select **Publish**, unless you clear the group selection. You do not need to resolve the conflict. You can view the difference by selecting the **View** button.

Steps to create a BIOS Update policy

Use this procedure to create a BIOS Update policy.

To create a BIOS Update policy, perform the following steps:

1. Log in to HP Connect with the Azure administrative account.
2. In the Dashboard page or the Policies side tab, select **New Policy**.
3. In the New Policy window, complete the following fields:
   - **Policy name**: Type a name for this policy. The policy name is shown in Microsoft Intune after you publish the policy. Ensure that the name is descriptive enough to find in the array of future policies. Consider using *Update* in the name to identify policies by type.
   - **Policy type**: From the list, select **Bios Update**.
   - **Tags**: Type a tag name and select **Add Tag**. Add as many tags as you want. You can use tags to distinguish policies from others already created. For example, administrators could add a personal tag, perhaps with a name, to find their policies. Alternatively, you might add a tag to identify the specific platform a policy is applied to.
4. Select **Next**.
5. In the Policy Settings window, select one of the following options:
   - **Keep BIOS of all devices always updated**

     The policy applies to an Azure AD device group. All supported devices in the group receive a new BIOS when released by HP. Compliance policies are scheduled every 60 minutes by default.
   - **Deploy only critical BIOS updates**

     The policy applies to an Azure AD device group. Every device in the selected group is updated when a BIOS release is marked Critical by HP.
   - **Establish a rule for a specific device model**

     Select the policy rule that is most appropriate for your policy:
     - **Keep BIOS always updated to latest version**
     - **Enforce a specific BIOS version**

       Choose a platform from a drop-down box. When applied to an Azure AD device group, the policy applies only to the selected platform, if a platform is part of the device group.
6. Select **Save**.

7. In the next window, select one of these options:
    - **Apply**: Publish the policy to Intune. Select one or more device groups.
    - **Close**: Save the policy to edit or apply later.

How the policy is applied

When you create a BIOS update policy and select a device, the administrator can select **Publish** to send the policy to Microsoft Intune. Microsoft Intune uses 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 whether the Remediation script is run.

By default, Intune checks for policies and applies them every 60 minutes. You can modify the schedule from the Intune console and run the check **Once**, every **Hour**, **Daily**, or every specific number of days. After you send an HP Connect policy to Intune, Intune manages the policy's actions.

In Intune, the proactive remediation compliance policy properties show as Version 1 when the policy is initially published. The version increases when the Policy is updated and republished, or when other policies are added to the group. For example, adding a BIOS Update policy and a BIOS setting policy would increase the proactive remediation version number.

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

NOTE: HP Connect does not support downgrading the BIOS to a version that is older than the installed version. If you must have the older BIOS, you must find a way outside HP Connect.

The HP BIOS update process follows these steps:

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

A BIOS update policy does not automatically restart the device. Therefore, you must restart your device for the BIOS update policy action to occur.

To reiterate, the BIOS update does 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 must be applied, one per platform.

In HP Connect, when you add an AAD device group to a policy, the policy settings changes are displayed in the right pane of the dialog box.

Steps to create a BIOS Settings policy

Use this procedure to create a BIOS Settings modification policy.

1. Log in to HP Connect.
2. In the Dashboard page or the Policies side tab, select **New Policy**.
3. In the New Policy window, complete the following fields:
   - **Policy name**: The policy name is shown in the Microsoft Intune console after you publish the policy. Ensure that the name is descriptive enough to find in the array of future policies. Consider using *Settings* in the name to identify policies by name.
   - **Policy type**: From the list, select **Bios Settings**.
   - **Description**: Type a policy description in this free-format field.
   - **Tags**: Type a tag name and select **Add Tag**. Add as many tags as you want.

     You can use tags to distinguish policies from ones already created. For example, administrators could add a personal tag, perhaps with a name, to find their policies. Alternatively, you might add a tag to identify the specific platform a policy is applied to.
4. Select **Next**.
5. In the Policy Settings window, select the platform to apply the settings to:
   a. Use the dropdown box or search in the search field.
   b. In the right pane, configure the required BIOS settings:
      - Use the Search field to find a setting.
      - Modify as many settings as required.

        NOTE: Certain settings might require you to apply an authentication method (HP Sure Admin or password) to modify the setting. This requirement might not be obvious from the settings selection list.

      - Preview modified settings by selecting **Show Selected**.
6. Select **Save**.
7. In the next window, select one of these options:
   - **Apply**: Publish policy to Intune
   - Select one or more device groups
   - **Close**: Save the policy to edit or apply later

How the policy is applied

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

Microsoft Intune then uses the updated HP Connect Detection policy script to identify the platforms that matched the selection. If a device in the group matched the platform name and ID, the local Intune agent runs a Remediation script.

The Remediation script reviews and acts 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 uses 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.

You can publish a single Global Settings policy to a device group. If you publish a Global Settings policy to a device group and a new policy is published to the same device group, the new policy replaces the existing policy in the group. Settings from the existing policy do not merge with the new policy. The new policy settings apply only to devices checking in on their schedule. If a device applied a setting from the original policy, the setting is not 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 selecting **View** in the Review and Publish dialog box, before publishing the policy.

Global policy vs. platform-specific settings

Although a single Global Policy can be published to a device group, platform-specific policies can coexist with it. Any platform-specific settings policy takes 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 does not apply and does not make an error. A Global Settings policy might contain settings that exist in some platforms and not others and this policy is supported. Each device applies only settings that exist in its BIOS and disregards all others.

NOTE: 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 might have some inconsistent options across platforms might have to be set as platform-specific policies.

Steps to create a Global BIOS settings policy

Use this procedure to create a BIOS Settings modification policy.

1. Log in to HP Connect,
2. In the Dashboard page or the Policies side tab, select **New Policy**.
3. In the dialog box, fill in the following fields:
   - **Policy name**: The policy name is shown in the Microsoft Intune console after the policy is published. The name should be descriptive enough to find in the array of future policies. Consider using **Settings** in the name to identify policies by name.
   - **Policy type** (use list): Select **Bios Settings**
   - **Description**: Type a description in this field
   - **Tags**: Type a tag name and select **Add Tag**. Add as many tags as you want.

Tags can be used to identify policies from ones already created. For example, administrators could add a personal tag, perhaps with a name, to find their policies. Or perhaps a tag to identify a specific platform that it is applied to.

4. Select **Next**.
5. Select **Global Policy**, and select **Next**.
6. In the Policy Settings dialog box, find and set the required settings.
   - In the right pane, configure each BIOS setting.
     - Use the Search field to find a setting.
     - Modify as many settings as required.

       NOTE: Certain settings might require that an authentication method (HP Sure Admin or password) is applied, or the device might not apply the setting. This requirement might not be obvious from the settings selection list.

     - Preview modified settings by enabling **Show Selected Only**.
7. Select **Save**.
8. At the Review Policy page, confirm the settings and select **Save**.
9. In the next dialog box, select one of the following choices:
   - **Apply**: To send policy to Intune
     - Select device groups in the next dialog box.
     - If an existing policy exists, select **View** to analyze the differences.
     - Select **Publish** or **Previous** to change or cancel.
   - **Close**: To save the policy, to edit, or apply later.

Create a Global BIOS settings policy report

Use this procedure to create a BIOS Settings modification policy report on how each setting applies to specific platforms.

1. Log in to HP Connect.
2. In the **Policies** side tab, select the **Global Settings Policy**.
3. Select the **Edit** pencil icon.
4. Select **Next** at the **Policy Information** page.
5. Modify any settings, if required, and select **Next**.
6. At the **Review Policy** page, select **Generate Report**.
7. At the Generate Report dialog, select **platforms**.
   - To select multiple platforms, press Ctrl and select the platforms.
8. Select **Export** to output to a csv format file.

The output file has a list of platforms and how each setting in the policy applies to each platform.

BIOS authentication policies

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 before starting up a Windows Operation System. When the BIOS can be accessed without authentication, a local or remote user might be able to disable basic security features. Doing this configuration can potentially allow malware early into the startup process that Windows might not protect against.

IMPORTANT: HP recommends keeping the device BIOS up to date to implement authentication, because newer BIOS includes security and vulnerability updates. In addition, initial BIOS releases might not always fully implement certain security features or might include authentication issues addressed in future updates.

When enabling administrative security of the BIOS, settings changes are 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 requires using an HP Sure Admin app on an authorized user or 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 security for computer firmware configuration and management by enabling remote administrators to manage BIOS settings securely while allowing field-support personnel to get secure access to BIOS setup in person with a managed Local Access Key. Using digital certificates and public-key cryptography eliminates the risks associated with the legacy password-based approach.

The HP Sure Admin security model relies on public-key cryptography and eliminates requirements to store or transmit the secret (private) key to the managed device. Once the provisioning process is done by an HP Connect policy, firmware management and local access operations are securely authenticated.

NOTE: HP Sure Admin relies on a trusted firmware environment that starts with the HP Secure Platform Management (SPM). HP SPM must be provisioned before enabling Sure Admin. HP Connect Provisions SPM and enables Sure Admin with a BIOS authentication policy.

To secure local access to the BIOS, HP Sure Admin uses a Local Access Key and the authentication policy provisions simultaneously. Use an HP-developed mobile phone app 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. When using a secure channel to communicate with HP Connect over the Internet, a challenge/response protocol provides a one-time pin that the authorized user types on the screen to access the BIOS.

Removing a 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 undoes previous authentication policies applied to devices in the selected group, including HP Sure Admin provisioning and passwords. The BIOS on

these devices is wide open for access. Deprovisioning occurs when the devices next check-in to the MEM console.

Steps to create a BIOS authentication policy

Use this procedure to create a BIOS Update policy.

1. Log in to HP Connect.
2. In the Dashboard page or the Policies sidebar tab, select **New Policy**.
3. In the dialog box, fill in the following fields:
   - **Policy name**: The policy name is shown in Intune console after the policy is published. The name should be descriptive enough to find in the array of future policies. Consider using *Updates*, *Settings*, or *Security* in the name to search and find published policies by name.
   - **Policy type** (use the dropdown box): select **Bios Authentication**.
   - **Description**: Type a description in this field.
   - **Tags**: Type a tag name and select **Add Tag**. Add as many tags as desired.

     Tags can be used to identify policies from ones already created. For example, administrators can add a personal tag, perhaps with a name, to find their policies. They might also add a tag to identify a specific platform that the tab is applied to.
4. Select **Next**.
5. In the new Policy Settings dialog box, choose 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 select **New** to add those keys now.
     - Select a LAK (Local Access Key) previously stored in the secrets vault. If none is stored, HP Connect uses the Signing Key as the LAK.
   - For: Password
     - Select a password from stored secrets.
     - Select **Secure Platform Management** setting if you have made SPM keys and want to preprovision the HP Sure Admin required keys for future use.
6. Select **Save**.
7. In the next dialog box, select either of the following:
   - **Apply**: To send policy to Intune.
   - Select device groups in the next dialog box.
   - **Close**: To save the policy to edit or apply later.

Policy application

When you apply a BIOS authentication policy to a device group, HP Connect sends Intune, via a graph API, the Detection, and Remediation scripts that Intune uses 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 has Security Platform Management (Endorsement and Signing) keys applied. The Sure Admin setting is enabled (BIOS setting is named Enhanced BIOS Authentication Method or EBAM), and if provided, it provisions the Local Access Key/LAK as well to secure local keyboard F10 access to the BIOS. A toaster notification is displayed to restart the system.

Similarly, if BIOS passwords are defined in the policy, the published scripts 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 might fail or give inconsistent results.

NOTE: 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 generates a conflict that needs to be resolved.

7 Freeze Dates

The Freeze Dates feature gives an IT Administrator the ability to pause all policies published to a device group from being acted on by Intune during the set period.

Access the Freeze Dates feature from the Settings menu. On the Settings page, select the **Freeze Dates** menu item.

Create Freeze Date

Use this procedure to create a BIOS Update policy.

1. Log in to HP Connect.
2. On the Dashboard page, select **Settings**.
3. In the dialog box, fill in the following fields:
   - Name: The name is shown in the client log file, when active. The name should be descriptive enough to find in the array of future policies.
   - Description: Type a description in this field.
   - Start Date: Enter or select the starting date for the freeze to be in effect.
   - End Date: Enter or select the ending date for the freeze to be in effect.
4. Select **Save**.
5. In the next dialog box, select either of the following:
   - Apply: To publish the new Freeze date to Intune, then select device groups in the next dialog box.
   - Apply: To publish to the Azure device group.
   - Cancel: To cancel the creation of the Freeze.

The newly created Freeze feature is shown in the HP Connect Settings page. Selecting the Freeze feature provides details, including those shown below:

- A description of the feature
- If the feature is currently in effect
- If the feature is upcoming
- If the feature is in use
- The device groups that the feature is assigned to

NOTE: After a Freeze is applied to one or more device groups, you cannot modify it. To modify or delete the selected feature, select **Add or Remove Groups** to remove it from all published groups. Then, select the **Edit** pencil icon or the **Trash can** icon.

A Freeze applied and published to a device group updates the Intune Proactive Remediation scripts. Each script checks for the specified date range and acts accordingly. If the script runs within the Freeze date range, it returns with no action taken. The HP Connect log in each device group client device shows if the Freeze is active when the Intune agent acts on the Proactive Remediation.

Freeze features are managed separately from HP Connect Policies and you can only create, edit, and remove them from the Settings page. In Intune, the Freeze is scripted into both Proactive Remediation Detection and Remediation scripts and is not listed in the properties otherwise.

A HP Sure Admin/Secure Platform Management

Follow the steps outlined in this section to enable HP Sure Admin and 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 the UEFI BIOS of each device. Once configured, SPM becomes the trusted base for features such as HP Sure Admin, HP Sure Run (technology to help maintain the security of certain Windows services and applications), 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 configures SPM and then enables EBAM, securing remote access to the BIOS. To secure local F10 Setup access, the HP Connect authentication policy needs to provision an additional Local Access Key (LAK).

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. The embedded public/private key pairs are retrieved from the certificates, stored in a secure cloud vault, and used when creating an HP Sure Admin authentication policy. An additional LAK certificate is required to support protection to the F10 Setup.

NOTE: It is critical to safeguard certificates to prevent compromising the security of the BIOS, should they become publicly available but HP Connect does not need them anymore. 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, securing local access to the BIOS F10 Setup menu is required. Instead of passwords, HP Sure Admin uses a Local Access Key/LAK signed with the provisioned signing key.

You can allow Local F10 BIOS from the HP Sure Admin phone app. Enter the 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 task invokes a process to add the supporting HP Sure Admin Enterprise Application on the Azure tenant, where it is used for all local authentication requests.

You can permit Non-Administrators to access the F10 Setup by following these steps in the Azure admin center.

From the Azure portal, select Enterprise Applications, and select HP MEM Connector Services. Notice that the homepage URL column is https://admin.hp.com.

NOTE: Certain Intune Conditional Access policies might prevent HP Connect from being integrated. As an example, **Require approved client app** and **Require app protection policy**, if enabled, might affect activation of the HP Sure Admin application.

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

In the **Edit Assignment** window, go to the **Select a role** section and select the **None Selected** link.

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

You can see the action performed and the permission is displayed for the user. Select **Assign**.

HP Sure Admin local access is now supported for the user.

B Troubleshooting and logs

Follow the steps outlined in this section to troubleshoot policy issues.

To begin troubleshooting, first confirm that 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 published 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.

NOTE: Proactive remediation compliance policies execute on a defined schedule. If the Intune agent on a device checks in prior to the next scheduled run, the policy may not run at that time.

Sync from device

Follow the instructions outlined here to sync a policy from a Windows endpoint.

1. From the Start menu, select **Settings**.
2. Select **Accounts** and then select **Access Work or School.**
3. Select **Connected to <domain> 's Azure AD**.
4. Select **Info**, and then select **Sync**.
5. Restart the device to start an MDM check in.
6. Restart the **Microsoft Intune Management Extension** to initiate a check-in.

Sync from Intune admin center

Follow the instructions outlined here to sync policies from the Intune admin center.

NOTE: By default, Intune devices check in every 8 hours.

1. Select **Devices**.
2. Select the name of the device you want to sync.
3. In the **Overview** pane, select **Sync**. Intune notifies the device to check in the Intune service. Notification time varies from immediate to a few hours

Logs

When an 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 might help troubleshoot certain failures.

HP Connect logs

This sections outlines the HP Connect logs that might be useful in troubleshooting issues.

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.

NOTE: If the `\HPConnect` folder does not exist, Intune has not synced an HP Connect policy with the device

The HP Connect activity log (example, `c814f103-6446-46ab-9885-e4df43d75e93.log`) can be useful for analysis or troubleshooting. You can find the latest actions taken by the policy at the end of the log file. Error conditions are shown here. You can also check the log file update date to confirm when it was last written to.

Intune logs

This sections outlines the Intune MDM Management extension logs that could be useful in troubleshooting issues.

- The Intune MDM Management Extension logs can be found here:

  `%ProgramData%\Microsoft\IntuneManagementExtension\Logs`

- Microsoft Intune agent stores the scripts that run a device here:

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

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

  `C:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown\wu_bios_update.log.`

NOTE: Add `Shutdown` to the name if submitting (example: `wu_bios_update -shutdown.log`).

- `C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup\wu_bios_update.log.`

NOTE: Add `Startup` to the name if submitting (example: `wu_bios_update -startup.log`).

- For Intune MDM troubleshooting purposes, you can run a Diagnostics report from here:

  `Windows Start/Settings/Connected to <AAD tenant>`. Select **Info**, then select **Create Report** and then **Export**. The output is generated to: `C:\Users\Public\Documents\MDMDiagnostics`

Intune Health Evaluation Task

This section describes the Health Evaluation task scheduled by the Intune Management Engine.

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

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

This task creates a log you can find here:

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

How to find the Intune Health Evaluation task in Task Scheduler

Follow the steps outlined here to find the Intune Health Evaluation task in Task Scheduler.

1. Open **Windows Task Scheduler** on the device.
2. Select **Task Scheduler Library/Microsoft/Intune**.
3. Find the **Intune Management Extension Health Evaluation** task.
4. Right-click the entry to select **Properties**.
5. View the execution schedule on the **Triggers** tab.

Note about compliance policies

Cloud management actions do not happen in real time. When a policy is published to Azure, 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 the compliance policy is applied.