



HP Sure Admin User Guide

SUMMARY

HP Sure Admin enables IT administrators to securely manage sensitive device firmware settings using certificates and public key cryptography for both remote and local management of settings instead of a password.

Legal information

© Copyright 2019, 2021, 2022 HP
Development Company, L.P.

Apple is a trademark of Apple Computer, Inc.,
registered in the U.S. and other countries.

Google Play is a trademark of Google LLC.

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

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

Third Edition: July 2022

First Edition: December 2019

Document Part Number: L83995-003

Table of contents

1 Getting started	1
Using HP Sure Admin	1
Disabling HP Sure Admin	1
2 Creating and managing keys	2
Creating and exporting keys.....	2
Create and export Key with manual distribution	2
Creating and exporting key with Azure AD Revocation	3
Create and send a key to Azure AD Group OneDrive	3
3 Phone setup	5
Using HP Sure Admin phone app to unlock BIOS.....	5
Obtaining access to BIOS setup after enrollment	5
Unlocking BIOS with Azure AD Group OneDrive	5
4 HP Sure Admin error codes	7

1 Getting started

HP Sure Admin enables IT administrators to securely manage sensitive device firmware settings using certificates and public key cryptography for both remote and local management of settings instead of a password.

HP Sure Admin consists of the following pieces:

- **Target PC:** The platforms to manage that support Enhanced BIOS Authentication Mode.
- **HP Manageability Integration Kit (MIK):** The plug-in for System Center Configuration Manager (SCCM) or HP BIOS Configuration Utility (BCU) for remote management of the BIOS settings.
- **HP Sure Admin Local Access Authenticator:** A phone app that replaces the password to enable local access to the BIOS setup by scanning a QR code to obtain a one-time PIN.

Using HP Sure Admin

This section describes the process for using HP Sure Admin.

1. Open HP Sure Admin plug-in within the HP Manageability Integration Kit (MIK) plug-in for System Configuration Manager (SCCM) or Enhanced BIOS Configuration Utility (BCU).
2. Download the HP Sure Admin phone app from either Google Play™ store or the Apple App Store®.
3. Create a key pair used by the target device and the HP Sure Admin phone app to obtain the one-time PIN to unlock BIOS.

Disabling HP Sure Admin

This section describes the options to disable HP Sure Admin.

- In BIOS F10 setting, select **Restore Security settings to Factory Defaults**.



NOTE: This requires physical presence by providing authentication PIN via the HP Sure Admin phone app to access the F10 settings.

- Use BCU command to remotely call WMI of **Restore Security settings to Factory Defaults**.



NOTE: For more information, see the HP BIOS Configuration Utility (BCU) User Guide.

- In the MIK Security Provisioning page, select **Deprovision**.

2 Creating and managing keys

Complete Security provisioning within MIK prior to enabling Enhanced BIOS Authentication Mode. Enhanced BIOS Authentication Mode must be enabled to create and export keys. To enable BIOS Authentication Mode:

- Open the HP Sure Admin plug-in and select **Enhanced BIOS Authentication Mode** to create and export keys.

Creating and exporting keys

There are three different ways to create local access key pairs and enable the HP Sure Admin phone app to access the key.

- [Create and export Key with manual distribution on page 2](#)
- [Creating and exporting key with Azure AD Revocation on page 3](#)
- [Create and send a key to Azure AD Group OneDrive on page 3](#)

Create and export Key with manual distribution

Use this option to export the local access authorization key and then manually distribute it to the HP Sure Admin phone app through email or other method.



NOTE: This option does not require HP Sure Admin phone app network access to obtain a one-time PIN.

1. Name your key in the **Key Name** entry box.
2. Enter the passphrase in the **Passphrase** entry box.



NOTE: The passphrase is used to protect the exported key and must be provided so that the HP Sure Admin phone app user is able to import the key.

3. Select **Browse**, and choose where to export the path in the system.
4. Select **Create Key**. Your key is successfully created when a notification icon appears next to the **Create Key** button with the message **Key successfully created**.
5. Select **Next**. The summary page displays the HP Sure Admin settings that you entered.
6. Select **Save Policy**. The policy saves when the message **Saved successfully** appears.
7. Navigate to the folder where you saved the key and distribute it to the HP Sure Admin phone app user using a method that is available to that user on that device such as email. This user will also need the passphrase to import the key. HP recommends to use different distribution mechanisms for the key and the passphrase.



NOTE: When sending the QR code, send it in its original size. The app cannot correctly read the image if it is smaller than 800 × 600 in size.

Creating and exporting key with Azure AD Revocation

Use this option to connect the local access key to a specified Azure Active Directory group and require the HP Sure Admin phone app to require both user authentication to Azure Active Directory and to confirm that the user is a member of the specified group before providing a local access PIN. This method also requires manual distribution of the local access authorization key to the phone app through email or other method.



NOTE: This option requires the HP Sure Admin phone app to have network access in order to obtain a one-time PIN.

1. Name your key in the **Key Name** entry box.
2. Enter the passphrase in the **Passphrase** entry box.



NOTE: The passphrase is used to protect the exported key and must be provided so that the HP Sure Admin phone app user is able to import the key.

3. Select **Azure AD Login** and log in.
4. Select your group name from the **Azure AD Group Name** drop-down box. You must be a member of the group to have access to the key.
5. Select **Browse**, and choose where to export the path in the system.
6. Select **Create Key**. Your key successfully creates when a notification icon appears next to the **Create Key** button with the message **Key successfully created**.
7. Select **Next**. The summary page displays the HP Sure Admin settings that you entered.
8. Select **Save Policy**. The policy saves when the message **Saved successfully** appears.
9. Navigate to the folder where you saved the key and distribute it to the HP Sure Admin phone app user using a method that is available to that user on that device such as email. This user will also need the passphrase to import the key. HP recommends to use different distribution mechanisms for the key and the passphrase.



NOTE: When sending the QR code, send it in its original size. The app cannot correctly read the image if it is smaller than 800 × 600 in size.

Create and send a key to Azure AD Group OneDrive

(Recommended) Use this option to avoid storing the local access authorization key on the phone. When you choose this option, MIK will store the local access authorization key to the specified OneDrive folder that is only accessible to the authorized group. The HP Sure Admin phone app user will be required to authenticate to Azure AD each time a PIN is needed.

1. Name your key in the **Key Name** entry box.
2. Enter the passphrase in the **Passphrase** entry box.
3. Select **Azure AD Login** and log in.
4. Select your group name from the **Azure AD Group Name** drop-down box.



NOTE: You must be a member of the group to have access to the key.

5. Enter the name of the OneDrive folder where you want the key saved to in the **OneDrive** entry box.

6. Select **Browse**, and choose where to export the path in the system.
7. Select **Create Key**.



NOTE: Your key is successfully added to the specified OneDrive folder and exported to the specified local folder when a notification icon appears next to the **Create Key** button with the message **Key successfully created**.

8. Select **Next**. The summary page displays HP Sure Admin settings that you entered.
9. Select **Save Policy**. The policy saves when the message **Saved successfully** appears.



NOTE: In this scenario, there is no need to send anything to the HP Sure Admin phone app to preprovision it. The target PCs are provisioned to point to the OneDrive location that is included in the QR code. The HP Sure Admin phone app uses this pointer to access the OneDrive location if the user is part of the authorized group and successfully authenticates.

3 Phone setup

Download the HP Sure Admin phone app from either Google Play or Apple store.

- Download HP Sure Admin from the Google store for Android phones.
- Download HP Sure Admin from the Apple store for iOS phones.

Using HP Sure Admin phone app to unlock BIOS

The HP Sure Admin mobile app replaces use of the BIOS password for local access to BIOS setup by providing a one-time PIN obtained by scanning the QR code presented by the target machine.

Use these steps to save the key locally on the phone in a scenario where the key is sent to the phone app user. In the following example the key is emailed to the HP Sure Admin phone app user, and the user opens the email on the phone.

1. Open the email that contains the key.
2. When the **Enrollment** page is displayed, enter the passphrase in the **Enter passphrase** entry box and your email address in the **Enter your email address** entry box to decrypt the key and add it to the HP Sure Admin application. The unlock PIN number is displayed on the **Your PIN** page.



NOTE: This step saves the key in the mobile device and completes enrollment. At this point, you can use the HP Sure Admin phone app to access any device that has been provisioned to be accessible via this key. An email address is required only if the administrator requires it.

3. Enter the PIN in the **BIOS Enter Response Code** entry box.

Obtaining access to BIOS setup after enrollment

To obtain access to BIOS setup on a target machine after enrollment:

1. Enter BIOS setup at boot on the target machine.
2. Select **Scan QR Code** in the phone application and scan the QR code on the target machine.
3. If prompted for user authentication, present your credentials.
4. The unlocked PIN number displays on the **Your PIN** page.
5. Enter the PIN in the **BIOS Enter Response Code** entry box on the target machine.

Unlocking BIOS with Azure AD Group OneDrive

To use HP Sure Admin to unlock BIOS with Azure AD Group OneDrive:

1. Select **Scan QR Code** and then scan the BIOS QR code.



NOTE: The HP Sure Admin app displays the Azure AD login page.

2. Log in to your Azure account.

3. Enter the PIN in the **BIOS Enter Response Code** entry box.



NOTE: HP Sure Admin app does not save the key locally in this scenario. The HP Sure Admin phone app must have network access and the user must authenticate each time a one-time PIN is needed.

4 HP Sure Admin error codes

Use the tables in this section to learn about the codes, types, and descriptions of errors you might see when using HP Sure Admin and KMS Admin Console.

Table 4-1 HP Sure Admin app QR Code errors

Error code	Error Type	Description
100	QRCodeUnknownError	General error.
101	QRCodeDeserialization	Unable to read the JSON QR Code. Either the string is not in a valid JSON file or the data is invalid.
102	QRCodeInvalidImage	The scanned QR Code image is invalid. Unable to read the QR Code image file.
103	QRCodeNoPayload	The scanned QR Code image is invalid. The image file does not have a JSON payload.
104	QRCodeInvalid	Unable to read the JSON QR Code. Either the string is not a valid JSON or the data in the QR image is invalid.
105	QRCodeInvalidKeyldHash	The public key hash in the JSON QR Code does not match the enrollment package's public key hash (KeyID data).
106	QRCodeTampered	The scanned QR Code image has been tampered with and is invalid.
107	QRCodeTamperedOrInvalidPassPhrase	The scanned QR Code image has been tampered with and is invalid, or the entered passphrase is incorrect.

Table 4-2 OneTime access key from OneDrive errors

Error code	Error type	Description
200	OneTimeKeyError	General error.
201	OneTimeKeyNoUserGroups	The logged-in user does not belong to any AD group that is in your organization.
203	OneTimeKeyInvalidUserGroup	The logged-in user does not belong to the AD Group that this key is assigned to.
204	OneTimeKeyQRFileDoesNotExist	The OneTime key file does not exist in the AD Group's OneDrive folder.
205	OneTimeKeyInvalidQRFile	The OneTime key file in the AD Group's OneDrive folder is invalid.
206	OneTimeKeyInvalidQRpayload	The OneTime key file exists but is unable to read the file payload.

Table 4-3 Azure AD Authorization errors

Error code	Error type	Description
300	AzureADUnknownError	General error.
301	AzureADInvalidDomain	The entered email address does not match the domain name that is specified in the QR Code image.
302	AzureADAccessToken	An error occurred while acquiring the access token from Azure AD. Either the user cannot log in to your organization's Azure AD, or the app does not have the required permissions to connect with your organization's Azure AD. The error could also mean that the user canceled authentication.
303	AzureADUserProfile	The HP Sure Admin app was enabled to acquire User profile information from your organization's Azure AD.
304	AzureADUserPrincipalMismatch	The entered email address does not match the logged-in user's user principal name.
305	AzureADUserInvalidUserGroup	The logged-in user does not belong to the assigned Azure AD Group that this key is assigned to.

Table 4-4 KMS Admin Console errors

Error code	Error type	Description
401	KmsUnauthorized	The user is not authorized to use the KMS service.
402	KmsKeyDoesNotExist	A matching private key does not exist in the KMS key vault. The key is currently in a deleted but recoverable state, and its name cannot be reused in this state. The key can only be recovered or purged.
403	KmsKeyDoesNotExistInTableStorage	The key does not exist in table storage.
404	KmsUploadKeyErrorInKeyVault	An error occurred while adding a key to the key vault.
405	KmsUploadKeyUnauthorized	The user is not authorized to upload keys. The user does not belong to the authorized AD Group that is permitted to call this API.
406	KmsInvalidAzureADLogin	The user is not logged in to Azure Tenant AAD.
407	KmsNoUserGroups	The logged-in user does not belong to any AD Group in your org.
408	KmsInvalidUserGroup	The logged-in user does not belong to the AD Group that this key is assigned to.
409	KmsInvalidAccessToken	The access token that was provided in the request is invalid.
410	KmsAccessTokenExpired	The accessToken that was provided has expired.

Table 4-4 KMS Admin Console errors (continued)

Error code	Error type	Description
411	KmsAccessTokenInvalidTenantId	The accessToken that was provided has an Invalid TenantId value.
412	KmsAccessTokenTenantIdMismatch	The TenantId in the provided accessToken does not match the TenantId in the function app.
413	KmsInvalidKeyId	The keyId value is null or empty.
414	KmsDeleteKeyUnauthorized	The user is not authorized to delete keys. The user does not belong to the authorized AD Group that is permitted to call this API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	The attempt to recover the secret failed, and it could not be recovered. The user must try again.
416	KmsInvalidGetKeysRequest	The Get Keys request is invalid.
417	KmsGetKeysUnauthorized	The user is not authorized to get keys. User does not belong to AD Group that is permitted to call this API.
418	KmsInvalidRequestPayload	The request received by the API is invalid.
419	KmsRequestRequired	The request received was empty. A request cannot be empty.
420	KmsKeyNotConcurrent	The key in table storage was updated or modified since the user last retrieved a copy.

Table 4-5 KMS Permissions Key Mapping Errors

Error code	Error type	Description
430	KmsAddKeyMappingsUnauthorized	The user is not authorized to add the device Permission. User does not belong to the authorized AD Group permitted to call this API.
431	KmsAddKeyMappingsInvalid	The Permission already exists. Use the PUT HTTP method to update the entity.
432	KmsDeleteKeyMappingsUnauthorized	The user is not authorized to delete the Device Permission. The user does not belong to the authorized AD Group that is permitted to call this API.
433	KmsDeleteKeyMappingsInvalid	The Permission to be deleted is invalid or does not exist.
434	KmsGetKeyMappingsUnauthorized	The user is not authorized to get the Device Permission. The user does not belong to the authorized AD Group that is permitted to call this API.
435	KmsGetKeyMappingsInvalid	This Permission to be returned is invalid or does not exist.

Table 4-5 KMS Permissions Key Mapping Errors (continued)

Error code	Error type	Description
436	KmsUpdateKeyMappingsUnauthorized	The user is not authorized to update the devicekeymappings entry. The user does not belong to the authorized AD Group that is permitted to call this API.
437	KmsUpdateKeyMappingsInvalid	The Permission to be updated is invalid or does not exist. Use the POST http method to insert the entity first.
438	KmsIncorrectContentType	The request payload contains an incorrect content type.
439	KmsUpdateKeyMappingsInvalid	The batch request contains multiple changes with same device ID. An entity can appear only once in a batch request.

Table 4-6 KMS Signing Key Errors

Error code	Error type	Description
501	KmsAddSigningKeyInvalid	The key entity already exists. Use the PUT HTTP method to update the entity.
502	KmsGetSigningKeyInvalid	The key entity to be returned is invalid or does not exist.
503	KmsDeleteSigningKeyInvalid	The key entity to be deleted is invalid or does not exist.
504	KmsUpdateSigningKeyInvalid	The key entity to be updated is invalid or does not exist. Use the POST HTTP method to insert the entity first.
601	KmsGetCommandRequestInvalid	The request to get the command is invalid.
602	KmsGetCommandNoSigningKey	The requested key entity required for signing does not exist.
603	KmsCommandsUnauthorized	The user is not authorized to use the key and no device permissions exist.
604	KmsGetCommandSigningCertInvalid	The key or certificate uploaded is malformed.
605	KmsGetSigningCertExportableInvalid	The key or certificate uploaded requires an exportable key.
606	KmsGetP21SKProvisioningPayloadInvalid	The SK and EK provided are identical. The user may not use the same keys to provision spm.