



User Guide

HP Sure Admin

© Copyright 2019 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.

First Edition: December 2019

Document Part Number: L83995-001

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
3 Phone setup	5
Using HP Sure Admin phone app to unlock BIOS	5

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

The process for using HP Sure Admin is as follows:

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

The following are 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

Select one of the following models to create local access key pairs and enable the HP Sure Admin phone app to access the key:


- **Create and Export Key** — 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.

- **Create and Export 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.

- **Create and Send 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.

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

To create and export a key:

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**.

 **NOTE:** Your key has 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**.



NOTE: The policy saves when a 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 application cannot correctly read the image if it is smaller than 800 × 600 in size.

To create and export a key with Azure AD Revocation:

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.



NOTE: 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**.



NOTE: 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**.



NOTE: The policy saved when the message ” appears.

9. Navigate to the folder where you saved the key and distribute it to the HP Sure Admin phone app user using a mechanism that is available to that user on that device such as email. This user will also need the passphrase to import the key. It is recommended to use different distribution mechanisms for the key and the passphrase.



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

To create and send a key to Azure AD Group OneDrive:

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**.



NOTE: The policy saves when a message **Saved successfully** appears.

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.

To enroll keys on the HP Sure Admin phone app:

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.



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.

The unlock PIN number is displayed on the **Your PIN** page.

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

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.

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.

Table 3-1 Error Codes

Error code	Description
100	General error.
101	Unable to read QR Code json. Either the string is not a valid json or the data is invalid.
102	QR Code image scanned is invalid. Unable to read QR Code image file.
103	QR Code image scanned is invalid. The image file does not have json payload.
104	Unable to read QR Code json. Either the string is not a valid json or the data in the QR image is invalid.
105	Public key hash in QR Code json does not match enrollment package public key hash (KeyID data).
200	General error.
201	The logged-in user does not belong to any AD group in your organization.
203	The logged-in user does not belong to the assigned AD Group for this key.
204	The OneTime key file does not exist in AD Group's OneDrive folder.
205	The OneTime key file in AD Group's OneDrive folder is invalid.
206	The OneTime key file exists but cannot read file payload.
300	General error.
301	Email address does not match the domain name in the QR Code image.
302	Error acquiring 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.
303	The BEAM app cannot acquire user profile information from your organization's Azure AD.
304	Email address does not match the logged-in user's principal name.
305	The logged-in user does not belong to the assigned Azure AD Group for this key.