



Guida per l'utente di HP Sure Admin

RIASSUNTO

HP Sure Admin consente agli amministratori IT di gestire in modo sicuro le impostazioni sensibili del firmware del dispositivo mediante certificati e crittografia a chiave pubblica per la gestione remota e locale delle impostazioni invece di una password.

Informazioni legali

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

Apple è un marchio di Apple Computer, Inc., registrato negli Stati Uniti e in altri paesi.

Google Play è un marchio di Google LLC.

Software per computer riservato. Il possesso, l'utilizzo o la copia del software richiedono la concessione da parte di HP di una licenza valida. In conformità con quanto previsto da FAR 12.211 e 12.212, il Software commerciale per computer, la documentazione del Software per computer e i dati tecnici per articoli commerciali vengono concessi in licenza al Governo degli Stati Uniti in base alla licenza commerciale standard del fornitore.

Le informazioni contenute in questo documento sono soggette a modifica senza preavviso. Le uniche garanzie per i prodotti e i servizi HP sono stabilite nelle dichiarazioni di garanzia esplicite che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento può essere interpretato come una garanzia aggiuntiva. HP non risponde di eventuali omissioni o errori tecnici o editoriali contenuti nel presente documento.

Seconda edizione: ottobre 2021

Prima edizione: dicembre 2019

Numero di parte del documento: L83995-062

Sommario

1 Guida introduttiva	1
Utilizzo di HP Sure Admin	1
Disabilitazione di HP Sure Admin	1
2 Creazione e gestione delle chiavi.....	2
Creazione ed esportazione delle chiavi	2
Creazione ed esportazione della chiave con la distribuzione manuale	2
Creazione ed esportazione di una chiave con la revoca di Azure AD	3
Creazione e invio di una chiave alla cartella OneDrive del gruppo Azure AD.....	3
3 Configurazione del telefono	5
Utilizzo dell'app HP Sure Admin per sbloccare il BIOS.....	5
Come ottenere l'accesso alla configurazione del BIOS dopo la registrazione	5
Sblocco del BIOS con la cartella OneDrive del gruppo Azure AD	5
4 Codici di errore di HP Sure Admin	7

1 Guida introduttiva

HP Sure Admin consente agli amministratori IT di gestire in modo sicuro le impostazioni sensibili del firmware del dispositivo mediante certificati e crittografia a chiave pubblica per la gestione remota e locale delle impostazioni invece di una password.

HP Sure Admin è composto dai seguenti elementi:

- **PC target:** le piattaforme da gestire che supportano la modalità di autenticazione BIOS avanzata (Enhanced BIOS Authentication Mode).
- **HP Manageability Integration Kit (MIK):** il plug-in per System Center Configuration Manager (SCCM) o HP BIOS Configuration Utility (BCU) per la gestione remota delle impostazioni del BIOS.
- **HP Sure Admin Local Access Authenticator:** un'app che sostituisce la password per abilitare l'accesso locale alla configurazione del BIOS eseguendo la scansione di un codice QR per ottenere un PIN monouso.

Utilizzo di HP Sure Admin

In questa sezione è descritto il processo per l'utilizzo di HP Sure Admin.

1. Aprire il plug-in HP Sure Admin nel plug-in HP Manageability Integration Kit (MIK) per System Configuration Manager (SCCM) o Enhanced BIOS Configuration Utility (BCU).
2. Scaricare l'app HP Sure Admin dal Google Play™ Store o dall'App Store® di Apple.
3. Creare una coppia di chiavi utilizzata dal dispositivo target e l'app HP Sure Admin per ottenere il PIN monouso per sbloccare il BIOS.

Disabilitazione di HP Sure Admin

In questa sezione sono descritte le opzioni per disabilitare HP Sure Admin.

- Nell'impostazione F10 del BIOS, selezionare **Restore Security settings to Factory Defaults** (Ripristina impostazioni di sicurezza a impostazioni predefinite).



NOTA: È richiesta la presenza fisica dell'utente, che dovrà fornire il PIN di autenticazione tramite l'app HP Sure Admin su smartphone per accedere alle impostazioni F10.

- Utilizzare il comando di BCU per chiamare da remoto il WMI di **Restore Security settings to Factory Defaults** (Ripristina impostazioni di sicurezza a impostazioni predefinite).



NOTA: Per maggiori informazioni, consultare la guida di HP BIOS Configuration Utility (BCU).

- Nella pagina del provisioning di sicurezza in MIK, selezionare **Deprovision** (Deprovisioning).

2 Creazione e gestione delle chiavi

Completare il provisioning di sicurezza in MIK prima di abilitare la modalità di autenticazione BIOS avanzata (Enhanced BIOS Authentication Mode). È necessario abilitare la modalità di autenticazione BIOS avanzata per creare ed esportare chiavi. Per abilitare la modalità di autenticazione BIOS:

- ▲ Aprire il plug-in HP Sure Admin e selezionare **Enhanced BIOS Authentication Mode** (Modalità di autenticazione BIOS avanzata) per creare ed esportare chiavi.

Creazione ed esportazione delle chiavi

Esistono 3 modi per creare coppie di chiavi per l'accesso locale e per consentire all'app HP Sure Admin su smartphone di accedere alla chiave.

- [Creazione ed esportazione della chiave con la distribuzione manuale a pagina 2](#)
- [Creazione ed esportazione di una chiave con la revoca di Azure AD a pagina 3](#)
- [Creazione e invio di una chiave alla cartella OneDrive del gruppo Azure AD a pagina 3](#)

Creazione ed esportazione della chiave con la distribuzione manuale

(Crea ed esporta chiave) Utilizzare questa opzione per esportare la chiave di autorizzazione per l'accesso locale, quindi distribuirla manualmente all'app HP Sure Admin tramite e-mail o altro metodo.



NOTA: Questa opzione non richiede l'accesso alla rete dell'app HP Sure Admin per ottenere un PIN monouso.


1. Assegnare un nome alla chiave nella casella **Key Name** (Nome chiave).
2. Immettere la passphrase nella casella di immissione **Passphrase**.



NOTA: La passphrase consente di proteggere la chiave esportata; per importare la chiave, l'utente dell'app HP Sure Admin deve fornire la passphrase.


3. Selezionare **Browse** (Sfoglia) e scegliere dove esportare il percorso nel sistema.
4. Selezionare **Create Key** (Crea chiave). Se la chiave è stata creata correttamente, accanto al pulsante **Create Key** (Crea chiave) viene visualizzata un'icona di notifica con il messaggio **Key successfully created** (Chiave creata correttamente).
5. Selezionare **Next** (Avanti). La pagina di riepilogo mostra le impostazioni HP Sure Admin immesse.
6. Selezionare **Save Policy** (Salva criteri). Se i criteri sono stati salvati correttamente, viene visualizzato il messaggio **Saved successfully** (Salvataggio riuscito).
7. Andare alla cartella dove è stata salvata la chiave e distribuirla all'utente dell'app HP Sure Admin usando un metodo disponibile sul suo dispositivo, per esempio via e-mail. L'utente necessiterà inoltre della

passphrase per importare la chiave. HP consiglia di utilizzare meccanismi di distribuzione diversi per la chiave e per la passphrase.


 **NOTA:** Quando si invia il codice QR, utilizzare il formato originale. L'app non è in grado di leggere correttamente l'immagine se le sue dimensioni sono inferiori a 800 × 600.

Creazione ed esportazione di una chiave con la revoca di Azure AD


(Crea ed esporta chiave con revoca Azure AD) Utilizzare questa opzione per connettere la chiave per l'accesso locale a un gruppo Azure Active Directory specificato e imporre all'app HP Sure Admin sia di richiedere l'autenticazione utente ad Azure Active Directory sia di verificare che l'utente sia un membro del gruppo specificato prima di fornire un PIN per l'accesso locale. Questo metodo richiede anche la distribuzione manuale della chiave di autorizzazione per l'accesso locale all'app tramite e-mail o altro metodo.

 **NOTA:** Questa opzione richiede l'accesso alla rete dell'app HP Sure Admin per ottenere un PIN monouso.

1. Assegnare un nome alla chiave nella casella **Key Name** (Nome chiave).
2. Immettere la passphrase nella casella di immissione **Passphrase**.

 **NOTA:** La passphrase consente di proteggere la chiave esportata; per importare la chiave, l'utente dell'app HP Sure Admin deve fornire la passphrase.

3. Selezionare **Azure AD Login** (Accesso Azure AD) ed effettuare l'accesso.
4. Selezionare il nome del gruppo dall'elenco a discesa **Azure AD Group Name** (Nome gruppo Azure AD). Per accedere alla chiave occorre essere un membro del gruppo.
5. Selezionare **Browse** (Sfoglia) e scegliere dove esportare il percorso nel sistema.
6. Selezionare **Create Key** (Crea chiave). Se la chiave è stata creata correttamente, accanto al pulsante **Create Key** (Crea chiave) viene visualizzata un'icona di notifica con il messaggio **Key successfully created** (Chiave creata correttamente).
7. Selezionare **Next** (Avanti). La pagina di riepilogo mostra le impostazioni HP Sure Admin immesse.
8. Selezionare **Save Policy** (Salva criteri). Se i criteri sono stati salvati correttamente, viene visualizzato il messaggio **Saved successfully** (Salvataggio riuscito).
9. Andare alla cartella dove è stata salvata la chiave e distribuirla all'utente dell'app HP Sure Admin usando un metodo disponibile sul suo dispositivo, per esempio via e-mail. L'utente necessiterà inoltre della passphrase per importare la chiave. HP consiglia di utilizzare meccanismi di distribuzione diversi per la chiave e per la passphrase.

 **NOTA:** Quando si invia il codice QR, utilizzare il formato originale. L'app non è in grado di leggere correttamente l'immagine se le sue dimensioni sono inferiori a 800 × 600.

Creazione e invio di una chiave alla cartella OneDrive del gruppo Azure AD

(Crea e invia chiave a OneDrive del gruppo Azure AD; consigliata) Utilizzare questa opzione per evitare di archiviare la chiave di autorizzazione per l'accesso locale sul telefono. Se si sceglie questa opzione, MIK memorizzerà la chiave di autorizzazione per l'accesso locale nella cartella OneDrive specificata e accessibile solo al gruppo autorizzato. L'utente dell'app HP Sure Admin dovrà eseguire l'autenticazione su Azure AD ogni volta che occorre un PIN.

1. Assegnare un nome alla chiave nella casella **Key Name** (Nome chiave).

2. Immettere la passphrase nella casella di immissione **Passphrase**.
3. Selezionare **Azure AD Login** (Accesso Azure AD) ed effettuare l'accesso.
4. Selezionare il nome del gruppo dall'elenco a discesa **Azure AD Group Name** (Nome gruppo Azure AD).



NOTA: Per accedere alla chiave occorre essere un membro del gruppo.

5. Immettere il nome della cartella OneDrive dove si desidera salvare la chiave nella casella **OneDrive**.
6. Selezionare **Browse** (Sfoglia) e scegliere dove esportare il percorso nel sistema.
7. Selezionare **Create Key** (Crea chiave).



NOTA: Se la chiave è stata aggiunta correttamente alla cartella OneDrive specificata ed esportata nella cartella locale specificata, accanto al pulsante **Create Key** (Crea chiave) viene visualizzata un'icona di notifica con il messaggio **Key successfully created** (Chiave creata correttamente).

8. Selezionare **Next** (Avanti). La pagina di riepilogo mostra le impostazioni HP Sure Admin immesse.
9. Selezionare **Save Policy** (Salva criteri). Se i criteri sono stati salvati correttamente, viene visualizzato il messaggio **Saved successfully** (Salvataggio riuscito).



NOTA: In questo scenario, non occorre inviare nulla all'app HP Sure Admin per il pre-provisioning. Il provisioning fa in modo che i PC target puntino alla posizione OneDrive inclusa nel codice QR. L'app HP Sure Admin utilizza questo puntatore per accedere alla posizione OneDrive se l'utente appartiene a un gruppo autorizzato ed esegue correttamente l'autenticazione.

3 Configurazione del telefono

Scaricare l'app HP Sure Admin dal Google Play Store o dall'App Store di Apple.

- Scaricare l'app HP Sure Admin dal Google Play Store per i telefoni Android.
- Scaricare l'app HP Sure Admin dall'App Store di Apple per i telefoni iOS.

Utilizzo dell'app HP Sure Admin per sbloccare il BIOS

L'app HP Sure Admin sostituisce l'utilizzo della password del BIOS per l'accesso locale alla configurazione del BIOS fornendo un PIN monouso ottenuto effettuando la scansione del codice QR mostrato dalla macchina target.

Utilizzare questa procedura per salvare la chiave in locale sullo smartphone, in uno scenario in cui la chiave viene inviata all'utente dell'app su smartphone. Nell'esempio seguente la chiave viene inviata tramite e-mail all'utente dell'app HP Sure Admin su smartphone e l'utente apre il messaggio e-mail sullo smartphone.

1. Aprire l'e-mail contenente la chiave.
2. Quando viene visualizzata la pagina **Enrollment** (Registrazione), immettere la passphrase nella casella **Enter passphrase** (Immetti passphrase) e l'indirizzo e-mail nella casella **Enter your email address** (Immetti indirizzo e-mail) per decrittografare la chiave e aggiungerla all'applicazione HP Sure Admin. Il numero del PIN di sblocco è visualizzato nella pagina **Your PIN** (Il tuo PIN).



NOTA: Questo passaggio salva la chiave sul dispositivo mobile e completa la registrazione. A questo punto è possibile utilizzare l'app HP Sure Admin per accedere a qualsiasi dispositivo di cui è stato effettuato il provisioning per renderlo accessibile tramite questa chiave. L'indirizzo e-mail è necessario solo se l'amministratore lo richiede.

3. Immettere il PIN nella casella **BIOS Enter Response Code** (Codice di risposta accesso al BIOS).

Come ottenere l'accesso alla configurazione del BIOS dopo la registrazione

Per ottenere l'accesso alla configurazione del BIOS su una macchina target diversa dopo la registrazione:

1. Accedere alla configurazione del BIOS all'avvio sulla macchina target.
2. Selezionare **Scan QR Code** (Scansione codice QR) nell'app ed effettuare la scansione del codice QR sulla macchina target.
3. Se viene richiesta l'autenticazione dell'utente, fornire le proprie credenziali.
4. Il numero del PIN di sblocco è visualizzato nella pagina **Your PIN** (PIN personale).
5. Immettere il PIN nella casella **BIOS Enter Response Code** (Codice di risposta accesso al BIOS) sulla macchina target.

Sblocco del BIOS con la cartella OneDrive del gruppo Azure AD

Per utilizzare HP Sure Admin per sbloccare il BIOS con la cartella OneDrive del gruppo Azure AD:

1. Selezionare **Scan QR Code** (Scansione codice QR) ed effettuare la scansione del codice QR del BIOS.



NOTA: L'app HP Sure Admin mostra la pagina di accesso di Azure AD.

2. Accedere al proprio account Azure.
3. Immettere il PIN nella casella **BIOS Enter Response Code** (Codice di risposta accesso al BIOS).



NOTA: L'app HP Sure Admin non salva la chiave localmente in questo scenario. L'app HP Sure Admin deve avere un accesso di rete e l'utente deve eseguire l'autenticazione ogni volta che occorre un PIN monouso.

4 Codici di errore di HP Sure Admin

La tabella in questa sezione consente di consultare i codici di errore di HP Sure Admin e KMS Admin Console con le relative tipologie e descrizioni.

Tabella 4-1 Codici di errore dell'app HP Sure Admin con relative tipologie e descrizioni

Codice di errore	Tipo di errore	Descrizione
100	QRCodeUnknownError	Errore generale.
101	QRCodeDeserialization	Impossibile leggere il codice JSON del codice QR. La stringa non è contenuta in un file JSON valido oppure i dati non sono validi.
102	QRCodeInvalidImage	Immagine del codice QR non valida. Impossibile leggere il file immagine del codice QR.
103	QRCodeNoPayload	Immagine del codice QR non valida. Il file di immagine non contiene un payload JSON.
104	QRCodeInvalid	Impossibile leggere il codice JSON del codice QR. La stringa non è un codice JSON valido oppure i dati nell'immagine QR non sono validi.
105	QRCodeInvalidKeyldHash	L'hash a chiave pubblica nel codice JSON del codice QR non corrisponde all'hash a chiave pubblica nel pacchetto di registrazione (dati KeyID).
106	QRCodeTampered	L'immagine del codice QR acquisita è stata manomessa e non è valida.
107	QRCodeTamperedOrInvalidPassPhrase	L'immagine del codice QR acquisita è stata manomessa e non è valida, oppure la passphrase inserita non è corretta.

Tabella 4-2 Errori della chiave di accesso monouso da OneDrive con relative tipologie e descrizioni

Codice di errore	Tipo di errore	Descrizione
200	OneTimeKeyError	Errore generale.
201	OneTimeKeyNoUserGroups	L'utente connesso non appartiene ad alcun gruppo AD nell'organizzazione.
203	OneTimeKeyInvalidUserGroup	L'utente connesso non appartiene al gruppo AD a cui è assegnata questa chiave.
204	OneTimeKeyQRFileDoesNotExist	Il file della chiave monouso non esiste nella cartella OneDrive del gruppo AD.
205	OneTimeKeyInvalidQRFile	Il file della chiave monouso nella cartella OneDrive del gruppo AD non è valido.
206	OneTimeKeyInvalidQRpayload	Il file della chiave monouso esiste ma non è possibile leggere il payload del file.

Tabella 4-3 Errori di autorizzazione di Azure AD

Codice di errore	Tipo di errore	Descrizione
300	AzureADUnknownError	Errore generale.
301	AzureADInvalidDomain	L'indirizzo e-mail inserito non corrisponde al nome di dominio specificato nell'immagine del codice QR.
302	AzureADAccessToken	Errore durante l'acquisizione del token di accesso da Azure AD. L'utente non può effettuare l'accesso ad Azure AD dell'organizzazione oppure l'app non ha le autorizzazioni necessarie per connettersi ad Azure AD dell'organizzazione. È inoltre possibile che l'utente abbia annullato l'autenticazione.
303	AzureADUserProfile	L'app HP Sure Admin è stata abilitata per acquisire le informazioni sul profilo utente da Azure AD dell'organizzazione.
304	AzureADUserPrincipalMismatch	L'indirizzo e-mail inserito non corrisponde al nome principale dell'utente connesso.
305	AzureADUserInvalidUserGroup	L'utente connesso non appartiene al gruppo Azure AD a cui è assegnata questa chiave.

Tabella 4-4 Errori di KMS Admin Console con relative tipologie e descrizioni

Codice di errore	Tipo di errore	Descrizione
401	KmsUnauthorized	L'utente non è autorizzato a utilizzare il servizio KMS.
402	KmsKeyDoesNotExist	Non esiste una chiave privata corrispondente nell'insieme di credenziali delle chiavi KMS. La chiave è attualmente in uno stato eliminato ma ripristinabile e il relativo nome non può essere riutilizzato in questo stato. La chiave può essere solamente recuperata o eliminata.
403	KmsKeyDoesNotExistInTableStorage	La chiave non esiste nell'archivio delle tabelle.
404	KmsUploadKeyErrorInKeyVault	Si è verificato un errore durante l'aggiunta di una chiave all'insieme di credenziali delle chiavi.
405	KmsUploadKeyUnauthorized	L'utente non è autorizzato a caricare le chiavi. L'utente non appartiene al gruppo AD autorizzato a chiamare questa API.
406	KmsInvalidAzureADLogin	L'utente non ha effettuato l'accesso al tenant Azure AD.
407	KmsNoUserGroups	L'utente connesso non appartiene ad alcun gruppo AD nell'organizzazione.
408	KmsInvalidUserGroup	L'utente connesso non appartiene al gruppo AD a cui è assegnata questa chiave.
409	KmsInvalidAccessToken	Il token di accesso fornito nella richiesta non è valido.

Tabella 4-4 Errori di KMS Admin Console con relative tipologie e descrizioni (continuazione)

Codice di errore	Tipo di errore	Descrizione
410	KmsAccessTokenExpired	Il token di accesso fornito è scaduto.
411	KmsAccessTokenInvalidTenantId	Il token di accesso fornito ha un valore ID tenant non valido.
412	KmsAccessTokenTenantIdMismatch	L'ID tenant nel token di accesso fornito non corrisponde all'ID tenant dell'app della funzione.
413	KmsInvalidKeyId	L'ID chiave è nullo o vuoto.
414	KmsDeleteKeyUnauthorized	L'utente non è autorizzato a eliminare le chiavi. L'utente non appartiene al gruppo AD autorizzato a chiamare questa API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Tentativo di recuperare il segreto non riuscito; impossibile effettuare il recupero. L'utente dovrebbe riprovare.
416	KmsInvalidGetKeysRequest	Richiesta di recupero chiavi non valida.
417	KmsGetKeysUnauthorized	L'utente non è autorizzato a recuperare le chiavi. L'utente non appartiene al gruppo AD autorizzato a chiamare questa API.
418	KmsInvalidRequestPayload	La richiesta ricevuta dall'API non è valida.
419	KmsRequestRequired	La richiesta ricevuta non deve essere vuota.
420	KmsKeyNotConcurrent	La chiave nell'archivio delle tabelle è stata aggiornata o modificata dall'ultima volta in cui l'utente ne ha recuperato una copia.