



Guía del usuario de HP Sure Admin

RESUMEN

HP Sure Admin permite que los administradores de TI manejen de forma segura la delicada configuración del firmware de dispositivos utilizando certificados y criptografía de claves públicas para la administración remota y local de las configuraciones, en lugar de una contraseña.

Información legal

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

Apple es una marca comercial de Apple Computer, Inc., registrada en los Estados Unidos y otros países.

Google Play es una marca comercial de Google LLC.

Software confidencial para equipos. Se requiere una licencia válida de HP para su posesión, uso o copia. Según lo dispuesto en las disposiciones FAR 12.211 y 12.212, el software de computación comercial, la documentación del software de computación y los datos técnicos para elementos comerciales se otorgan bajo la licencia comercial estándar del fabricante al gobierno de EE. UU.

La información contenida en el presente documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de HP están estipuladas en las declaraciones expresas de garantía que acompañan a dichos productos y servicios. La información contenida en este documento no se debe interpretar como una garantía adicional. HP no se hará responsable de los errores técnicos o de edición ni de las omisiones contenidas en el presente documento.

Segunda edición: octubre de 2021

Primera edición: diciembre de 2019

Número de referencia del documento: L83995-E52

Tabla de contenido

1 Pasos iniciales	1
Uso de HP Sure Admin	1
Desactivación de HP Sure Admin	1
2 Creación y administración de claves.....	2
Creación y exportación de claves	2
Crear y exportar clave con distribución manual.....	2
Crear y exportar una clave con la revocación de Azure AD	3
Crear y enviar una clave a OneDrive del grupo de Azure AD	3
3 Configuración del teléfono.....	5
Uso de la aplicación de teléfono de HP Sure Admin para desbloquear el BIOS	5
Obtener acceso a la configuración del BIOS después del registro	5
Desbloqueo del BIOS con el grupo de Azure AD en OneDrive	5
4 Códigos de error de HP Sure Admin	7

1 Pasos iniciales

HP Sure Admin permite que los administradores de TI manejen de forma segura la delicada configuración del firmware de dispositivos utilizando certificados y criptografía de claves públicas para la administración remota y local de las configuraciones, en lugar de una contraseña.

HP Sure Admin consta de las siguientes partes:

- **PC de destino:** Las plataformas para administración que admiten el modo de autenticación del BIOS mejorado.
- **HP Manageability Integration Kit (MIK):** El complemento para System Center Configuration Manager (SCCM) o la HP BIOS Configuration Utility (BCU) para la administración remota de la configuración del BIOS.
- **Local Access Authenticator de HP Sure Admin:** Una aplicación de teléfono que sustituye la contraseña para permitir el acceso local a la configuración del BIOS escaneando un código QR para obtener un PIN utilizable solo una vez.

Uso de HP Sure Admin

Esta sección describe el proceso de uso de HP Sure Admin.

1. Abra el complemento de HP Sure Admin dentro del complemento HP Manageability Integration Kit (MIK) para System Configuration Manager (SCCM) o la BIOS Configuration Utility (BCU) mejorada.
2. Descargue la aplicación de teléfono de HP Sure Admin desde la tienda Google Play™ o la Apple App Store®.
3. Cree un par de claves utilizadas por el dispositivo de destino y la aplicación telefónica de HP Sure Admin para obtener el PIN utilizable solo una vez y desbloquear el BIOS.

Desactivación de HP Sure Admin

Esta sección describe las opciones para desactivar HP Sure Admin.

- En la configuración del BIOS F10, seleccione **Restaurar configuración de Seguridad a los valores predeterminados de fábrica**.



NOTA: Esto requiere presencia física proporcionando un PIN de autenticación a través de la aplicación de teléfono de HP Sure Admin para acceder a la configuración de F10.

- Use el comando BCU para llamar de forma remota a WMI de **Restaurar configuración de Seguridad a los valores predeterminados de fábrica**.



NOTA: Para obtener más información, consulte la Guía del usuario de BIOS Configuration Utility (BCU) de HP.

- En la página de Provisión de seguridad de MIK, seleccione **Desprovisión**.

2 Creación y administración de claves

Provisión de seguridad completa dentro de MIK antes de habilitar el modo de autenticación del BIOS mejorado. Se debe activar el modo de autenticación del BIOS mejorado para crear y exportar claves. Para activar el modo de autenticación del BIOS:

- ▲ Abra el complemento de HP Sure Admin y seleccione el **Modo de autenticación del BIOS mejorado** para crear y exportar claves.

Creación y exportación de claves

Existen tres maneras diferente de crear pares de claves de acceso local y habilite la aplicación de teléfono de HP Sure Admin para acceder a la clave.


- [Crear y exportar clave con distribución manual en la página 2](#)
- [Crear y exportar una clave con la revocación de Azure AD en la página 3](#)
- [Crear y enviar una clave a OneDrive del grupo de Azure AD en la página 3](#)

Crear y exportar clave con distribución manual


Use esta opción para exportar la clave de autorización de acceso local y luego distribuirla manualmente a la aplicación de teléfono de HP Sure Admin a través de correo electrónico u otro método.

 **NOTA:** Esta opción no necesita el acceso a la red de la aplicación de teléfono de HP Sure Admin para obtener un PIN utilizable una sola vez.

1. Dele un nombre su clave en el cuadro de entrada **Nombre de clave**.
2. Escriba la frase de contraseña en el cuadro de entrada **Frase de contraseña**.

 **NOTA:** La frase de contraseña se utiliza para proteger la clave exportada y debe ser proporcionada para que el usuario de la aplicación de teléfono de HP Sure Admin pueda importar la clave.

3. Seleccione **Examinar** y elija dónde exportar la ruta en el sistema.
4. Seleccione **Crear clave**. Su clave se habrá creado con éxito cuando aparezca un icono de notificación junto al botón **Crear clave** con el mensaje **Clave creada correctamente**.
5. Seleccione **Siguiente**. La página de resumen muestra la configuración de HP Sure Admin que introdujo.
6. Seleccione **Guardar política**. La política estará guardada cuando aparezca el mensaje **Guardado correctamente**.
7. Desplácese hasta la carpeta donde guardó la clave y désela al usuario de la aplicación de teléfono de HP Sure Admin usando un método disponible para ese usuario en ese dispositivo, como el correo electrónico. Este usuario también necesitará la frase de contraseña para importar la clave. HP recomienda utilizar diferentes mecanismos de distribución para la clave y la frase de contraseña.

 **NOTA:** Al enviar el código QR, envíelo en su tamaño original. La aplicación no podrá leer correctamente la imagen si es más pequeña que 800 × 600.

Crear y exportar una clave con la revocación de Azure AD

Use esta opción para conectar la clave de acceso local a un grupo Azure Active Directory especificado y requerir que la aplicación de teléfono de HP Sure Admin solicite la autenticación de usuario a Azure Active Directory y confirme que el usuario es un miembro del grupo especificado antes de proporcionar un PIN de acceso local. Este método también requiere la distribución manual de la clave de autorización de acceso local a la aplicación de teléfono mediante correo electrónico u otro método.



NOTA: Esta opción requiere que la aplicación de teléfono de HP Sure Admin tenga acceso a la red a fin de obtener un PIN utilizable una sola vez.

1. Dele un nombre su clave en el cuadro de entrada **Nombre de clave**.
2. Escriba la frase de contraseña en el cuadro de entrada **Frase de contraseña**.



NOTA: La frase de contraseña se utiliza para proteger la clave exportada y debe ser proporcionada para que el usuario de la aplicación de teléfono de HP Sure Admin pueda importar la clave.

3. Seleccione **inicio de sesión con Azure AD** y conéctese.
4. Seleccione su nombre de grupo en el cuadro desplegable **Nombre del grupo de Azure AD**. Debe ser miembro del grupo para tener acceso a la clave.
5. Seleccione **Examinar** y elija dónde exportar la ruta en el sistema.
6. Seleccione **Crear clave**. Su clave se habrá creado con éxito cuando aparezca un icono de notificación junto al botón **Crear clave** con el mensaje **Clave creada correctamente**.
7. Seleccione **Siguiente**. La página de resumen muestra la configuración de HP Sure Admin que introdujo.
8. Seleccione **Guardar política**. La política estará guardada cuando aparezca el mensaje **Guardado correctamente**.
9. Desplácese hasta la carpeta donde guardó la clave y désela al usuario de la aplicación de teléfono de HP Sure Admin usando un método disponible para ese usuario en ese dispositivo, como el correo electrónico. Este usuario también necesitará la frase de contraseña para importar la clave. HP recomienda utilizar diferentes mecanismos de distribución para la clave y la frase de contraseña.



NOTA: Al enviar el código QR, envíelo en su tamaño original. La aplicación no podrá leer correctamente la imagen si es más pequeña que 800 × 600.

Crear y enviar una clave a OneDrive del grupo de Azure AD

(Recomendado) Use esta opción para evitar almacenar la clave de autorización de acceso local en el teléfono. Cuando elija esta opción, MIK almacenará la clave de autorización de acceso local en la carpeta OneDrive especificada, a la cual tiene acceso solo el grupo autorizado. Se le solicitará al usuario de la aplicación de teléfono de HP Sure Admin la autenticación con Azure AD cada vez que se necesite un PIN.

1. Dele un nombre su clave en el cuadro de entrada **Nombre de clave**.
2. Escriba la frase de contraseña en el cuadro de entrada **Frase de contraseña**.
3. Seleccione **inicio de sesión con Azure AD** y conéctese.
4. Seleccione su nombre de grupo en el cuadro desplegable **Nombre del grupo de Azure AD**.



NOTA: Debe ser miembro del grupo para tener acceso a la clave.

5. Escriba el nombre de la carpeta OneDrive donde desea que se guarde la clave en el cuadro de entrada **OneDrive**.
6. Seleccione **Examinar** y elija dónde exportar la ruta en el sistema.
7. Seleccione **Crear clave**.



NOTA: Su clave se agrega correctamente a la carpeta OneDrive especificada y se exporta a la carpeta local especificada cuando aparece un icono de notificación junto al botón **Crear clave** con el mensaje **Clave creada correctamente**.

8. Seleccione **Siguiente**. La página de resumen muestra la configuración de HP Sure Admin que introdujo.
9. Seleccione **Guardar política**. La política estará guardada cuando aparezca el mensaje **Guardado correctamente**.



NOTA: En este escenario, no es necesario enviar nada a la aplicación de teléfono de HP Sure Admin para preprovisión. Los PC de destino se provisionan para señalar la ubicación de OneDrive que se incluye en el código QR. La aplicación de teléfono de HP Sure Admin utiliza este indicador para acceder a la ubicación de OneDrive si el usuario forma parte del grupo autorizado y se autentica correctamente.

3 Configuración del teléfono

Descargue la aplicación de teléfono de HP Sure Admin desde Google Play o Apple Store.

- Descargue HP Sure Admin en la tienda Google Play para teléfonos con Android.
- Descargue HP Sure Admin en la tienda Apple Store para teléfonos con iOS.

Uso de la aplicación de teléfono de HP Sure Admin para desbloquear el BIOS

La aplicación móvil HP Sure Admin sustituye el uso de la contraseña del BIOS para el acceso local a la configuración del BIOS al proporcionar un PIN utilizable una sola vez, obtenido al escanear el código QR presentado por el equipo de destino.

Use estos pasos para guardar la clave localmente en el teléfono en un escenario en que se envía la clave al usuario de la aplicación del teléfono. En el siguiente ejemplo, la clave se envía por correo electrónico al usuario de la aplicación de teléfono de HP Sure Admin y el usuario abre el correo electrónico en el teléfono.

1. Abra el correo electrónico que contiene la clave.
2. Cuando aparezca la página de **Registro**, escriba la frase de contraseña en el cuadro de entrada **Introducir frase de contraseña** y su dirección de correo electrónico en la casilla **Introducir su dirección de correo electrónico** para descifrar la clave y agregarla a la aplicación HP Sure Admin. El número de PIN de desbloqueo aparece en la página **Su PIN**.



NOTA: Este paso guarda la clave en el dispositivo móvil y completa el registro. En este punto, puede utilizar la aplicación de teléfono de HP Sure Admin para acceder a cualquier dispositivo que se haya provisionado para ser accesible mediante esta clave. Solo se requiere una dirección de correo electrónico si el administrador lo exige.

3. Introduzca el PIN en el cuadro de entrada **Introducir código de respuesta del BIOS**.

Obtener acceso a la configuración del BIOS después del registro

Para obtener acceso a la configuración del BIOS en un equipo de destino después del registro:

1. Entre en la configuración del BIOS durante el arranque del equipo de destino.
2. Seleccione **Escanear código QR** en la aplicación del teléfono y escanee el código QR en el equipo de destino.
3. Si se le solicita autenticación de usuario, presente sus credenciales.
4. El número de PIN desbloqueado aparece en la página **Su PIN**.
5. Introduzca el PIN en el cuadro de entrada **Introducir código de respuesta del BIOS** en el equipo de destino.

Desbloqueo del BIOS con el grupo de Azure AD en OneDrive

Para usar HP Sure Admin para desbloquear el BIOS con el grupo de Azure AD en OneDrive:

1. Seleccione **Escanear código QR** y luego escanee el código QR del BIOS.



NOTA: La aplicación HP Sure Admin muestra la página de inicio de sesión de Azure AD.

2. Inicie sesión en su cuenta de Azure.
3. Introduzca el PIN en el cuadro de entrada **Introducir código de respuesta del BIOS**.



NOTA: La aplicación HP Sure Admin no guarda la clave localmente en esta situación. La aplicación de teléfono de HP Sure Admin debe tener acceso a la red y el usuario debe autenticarse cada vez que se necesite un PIN utilizable una sola vez.

4 Códigos de error de HP Sure Admin

Use la tabla de esta sección para ver los códigos de error de HP Sure Admin y KMS Admin Console, los tipos y sus descripciones.

Tabla 4-1 Códigos, tipos y descripciones de errores de la aplicación HP Sure Admin

Código de error	Tipo de error	Descripción
100	QRCodeUnknownError	Error general.
101	QRCodeDeserialization	No se puede leer el código QR JSON. La cadena no es un archivo JSON válido o los datos no son válidos.
102	QRCodeInvalidImage	Esta imagen de código de QR no es válida. No se puede leer el archivo de imagen del código QR.
103	QRCodeNoPayload	Esta imagen de código de QR no es válida. El archivo de imagen no tiene carga JSON.
104	QRCodeInvalid	No es posible leer el JSON del código QR. La cadena no es un JSON válido o los datos de la imagen QR no son válidos.
105	QRCodeInvalidKeyIdHash	El hash de clave pública en el JSON del código QR no coincide con el hash de clave pública del paquete de inscripción (datos KeyID).
106	QRCodeTampered	La imagen de código de QR escaneada fue alterada y no es válida.
107	QRCodeTamperedOrInvalidPassPhrase	La imagen de código de QR escaneada fue alterada y no es válida, o la frase de contraseña introducida es incorrecta.

Tabla 4-2 Errores de clave de acceso de un solo uso de OneDrive, sus tipos y descripciones

Código de error	Tipo de error	Descripción
200	OneTimeKeyError	Error general.
201	OneTimeKeyNoUserGroups	El usuario que ha iniciado sesión no pertenece a ningún grupo de AD de su organización.
203	OneTimeKeyInvalidUserGroup	El usuario que ha iniciado la sesión no pertenece al grupo de AD al que se asignó esta clave.
204	OneTimeKeyQRFileDoesNotExist	El archivo de claves de un solo uso no existe en la carpeta OneDrive del grupo AD.
205	OneTimeKeyInvalidQRFile	El archivo de claves de un solo uso en la carpeta OneDrive del grupo AD no es válido.
206	OneTimeKeyInvalidQRpayload	El archivo de claves de un solo uso existe pero no puede leer la carga del archivo.

Tabla 4-3 Errores de autorización de Azure AD

Código de error	Tipo de error	Descripción
300	AzureADUnknownError	Error general.
301	AzureADInvalidDomain	La dirección de correo electrónico introducido no coincide con el nombre de dominio especificado en la imagen del código QR.
302	AzureADAccessToken	Error al adquirir token de acceso de Azure AD. El usuario no puede iniciar sesión en Azure AD de su organización, o la aplicación no tiene los permisos necesarios para conectarse con Azure AD de su organización. También podría ser que el usuario canceló la autenticación.
303	AzureADUserProfile	La aplicación HP Sure Admin fue habilitada para adquirir información de perfil de usuario de Azure AD de su organización.
304	AzureADUserPrincipalMismatch	La dirección de correo electrónico introducido no coincide con el nombre principal del usuario que ha iniciado la sesión.
305	AzureADUserInvalidUserGroup	El usuario que ha iniciado la sesión no pertenece al grupo asignado de Azure AD al que se asignó esta clave.

Tabla 4-4 Errores de KMS Admin Console, tipos y sus descripciones

Código de error	Tipo de error	Descripción
401	KmsUnauthorized	El usuario no está autorizado a usar el servicio KMS.
402	KmsKeyDoesNotExist	No existe una clave privada que coincida en el almacén de claves de KMS. El estado actual de la clave es eliminada pero recuperable, y su nombre no se puede volver a utilizar en este estado. La clave solo puede recuperarse o desecharse.
403	KmsKeyDoesNotExistInTableStorage	La clave no existe en el almacenamiento de tablas.
404	KmsUploadKeyErrorInKeyVault	Se produjo un error al agregar una clave al almacén de claves.
405	KmsUploadKeyUnauthorized	El usuario no está autorizado a cargar claves. El usuario no pertenece al Grupo de AD autorizado que puede llamar esta API.
406	KmsInvalidAzureADLogin	El usuario no ha iniciado la sesión en Azure Tenant AAD.
407	KmsNoUserGroups	El usuario que ha iniciado sesión no pertenece a ningún grupo de AD en su organización.
408	KmsInvalidUserGroup	El usuario que ha iniciado la sesión no pertenece al grupo de AD al que se asignó esta clave.

Tabla 4-4 Errores de KMS Admin Console, tipos y sus descripciones (continúa)

Código de error	Tipo de error	Descripción
409	KmsInvalidAccessToken	El token de acceso que se proporcionó en la solicitud no es válido.
410	KmsAccessTokenExpired	El token de acceso proporcionado ha caducado.
411	KmsAccessTokenInvalidTenantId	El token de acceso proporcionado tiene un valor de TenantId no válido.
412	KmsAccessTokenTenantIdMismatch	El TenantId en el token de acceso proporcionado no coincide con la aplicación de función TenantId.
413	KmsInvalidKeyId	El valor keyId es nulo o está vacío.
414	KmsDeleteKeyUnauthorized	El usuario no está autorizado a eliminar claves. El usuario no pertenece al Grupo de AD autorizado que puede llamar esta API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	El intento de recuperar el secreto ha fallado y no se pudo recuperar. El usuario debe intentar de nuevo.
416	KmsInvalidGetKeysRequest	La solicitud Obtener claves no es válida.
417	KmsGetKeysUnauthorized	El usuario no está autorizado a obtener claves. El usuario no pertenece al Grupo de AD autorizado que puede llamar esta API.
418	KmsInvalidRequestPayload	La solicitud recibida por la API no es válida.
419	KmsRequestRequired	La solicitud recibida no debe estar vacía.
420	KmsKeyNotConcurrent	La clave de almacenamiento de tablas se actualizó o se modificó desde la última vez que el usuario recuperó una copia.