Manual do usuário do HP Sure Admin

RESUMO

O HP Sure Admin permite que os administradores de TI efetuem a gestão com segurança das definições sensíveis de firmware dos dispositivos, usando certificados e criptografia de chave pública para a gestão remota e local das definições, em vez de uma palavra-passe.

Informação jurídicas

Apple é uma marca comercial da Apple Inc., registada nos EUA e outros países.

Google Play é uma marca comercial da Google LLC.

Software informático confidencial. Licença válida da HP necessária para posse, utilização ou cópia. De acordo com a FAR 12.211 e 12.212, o Software Informático Comercial, a Documentação do Software Informático e os Dados Técnicos de Itens Comerciais são licenciados ao Governo dos EUA segundo a licença comercial padrão do fornecedor.

As informações contidas neste documento estão sujeitas a alteração sem aviso prévio. As únicas garantias para os produtos e serviços da HP são estabelecidas nas declarações de garantia expressa que acompanham esses produtos e serviços. Nenhuma declaração constante neste documento deverá ser interpretada como constituindo uma garantia adicional. Não são da responsabilidade da HP quaisquer erros técnicos ou editoriais ou omissões contidos no presente documento.

Segunda edição: outubro de 2021

Primeira edição: dezembro de 2019

Número de publicação do documento: L83995-132

Índice

1 Introdução

O HP Sure Admin permite que os administradores de TI efetuem a gestão com segurança das definições sensíveis de firmware dos dispositivos, usando certificados e criptografia de chave pública para a gestão remota e local das definições, em vez de uma palavra-passe.

O HP Sure Admin consiste nas seguintes peças:

- **PC de destino:** As plataformas a gerir com suporte para o Modo Melhorado de Autenticação do BIOS.
- **HP Manageability Integration Kit (MIK):** O plug-in do System Center Configuration Manager (SCCM) ou do HP BIOS Configuration Utility (BCU) para a gestão remota das definições do BIOS.
- **HP Sure Admin Local Access Authenticator:** Uma aplicação para telemóvel que substitui a palavra-passe para permitir o acesso local à configuração do BIOS ao digitalizar um código QR para obter um PIN único.

Utilização do HP Sure Admin

Esta secção descreve o processo para a utilização do HP Sure Admin.

1. Abra o plug-in do HP Sure Admin dentro do plug-in HP Manageability Integration Kit (MIK) para o System Configuration Manager (SCCM) ou o BIOS Configuration Utility (BCU) Melhorado.
2. Transfira a aplicação HP Sure Admin para telemóvel a partir da loja Google Play™ ou da Apple App Store®.
3. Crie um par de chaves utilizado pelo dispositivo de destino e pela aplicação HP Sure Admin para telemóvel para obter o PIN único para desbloquear o BIOS.

Desativar o HP Sure Admin

Esta secção descreve as opções para desativar o HP Sure Admin.

- Na configuração F10 do BIOS, selecione **Restaurar as Definições de segurança para as predefinições de fábrica**.

NOTA: Isto requer a presença física, ao fornecer o PIN de autenticação através da aplicação HP Sure Admin para telemóvel para aceder às configurações F10.

- Utilize o comando BCU para ligar remotamente ao WMI de **Restaurar as Definições de segurança para as predefinições de fábrica**.

NOTA: Para obter mais informações, consulte o Manual do usuário do HP BIOS Configuration Utility (BCU).

- Na página de Provisionamento de Segurança do MIK, selecione **Desprovisionar**.

2 Criação e gestão de chaves

Conclua o provisionamento de Segurança dentro do MIK, antes de ativar o Modo de Autenticação Melhorado do BIOS. O Modo de Autenticação Melhorado do BIOS deve estar ativado para criar e exportar as chaves. Para ativar o Modo de Autenticação do BIOS:

▲ Abra o plug-in HP Sure Admin e selecione o **Modo de Autenticação Melhorado do BIOS** para criar e exportar chaves.

Criação e exportação de chaves

Há 3 formas diferentes de criar pares de chaves de acesso local e ativar a aplicação HP Sure Admin para telemóvel para aceder à chave.

- Criar e exportar chave com distribuição manual na página 2
- Criar e exportar uma chave com a Revogação Azure AD na página 3
- Criar e enviar uma chave para o OneDrive do Grupo Azure AD na página 3

Criar e exportar chave com distribuição manual

Utilize esta opção para exportar a chave de autorização de acesso local e, em seguida, distribuí-la manualmente para a aplicação HP Sure Admin para telefone por e-mail ou outro método.

NOTA: Esta opção não necessita do acesso à rede da aplicação HP Sure Admin para telemóvel para obter um PIN único.

1. Dê um nome à sua chave na caixa de entrada **Nome da Chave**.
2. Introduza a frase de acesso na caixa de entrada **Frase de acesso**.

   NOTA: A frase de acesso é utilizada para proteger a chave exportada e deve ser fornecida de modo a que o utilizador da aplicação HP Sure Admin para telemóvel seja capaz de importar a chave.

3. Selecione **Procurar** e escolha para onde exportar o caminho no sistema.
4. Selecione **Criar Chave**. A sua chave é criada com sucesso quando um ícone de notificação for apresentado ao lado do botão **Criar Chave** com a mensagem **Chave criada com sucesso**.
5. Selecione **Seguinte**. A página de resumo mostra as definições do HP Sure Admin que introduziu.
6. Selecione **Guardar Política**. A política é guardada quando é apresentada a mensagem **Guardada com sucesso**.
7. Navegue até à pasta onde guardou a chave e distribua-a para a aplicação HP Sure Admin para telemóvel, utilizando um método que esteja disponível para esse utilizador nesse dispositivo, tal como o e-mail. Este utilizador também precisará da frase de acesso para importar a chave. A HP recomenda que utilize diferentes mecanismos de distribuição para a chave e a frase de acesso.

   NOTA: Ao enviar o código QR, envie-o no respetivo tamanho original. A aplicação não poderá ler corretamente a imagem se esta tiver um tamanho inferior a 800 × 600.

Criar e exportar uma chave com a Revogação Azure AD

Utilize esta opção para ligar a chave de acesso local a um grupo do Azure Active Directory específico e exigir que a aplicação HP Sure Admin para telemóvel exija a autenticação do utilizador no Azure Active Directory e confirme que o utilizador é um membro do grupo especificado, antes de fornecer um PIN de acesso local. Este método também requer a distribuição manual da chave de autorização de acesso local à aplicação para telemóvel através de e-mail ou outro método.

NOTA: Esta opção exige que a aplicação HP Sure Admin para telemóvel tenha acesso à rede para obter um PIN único.

1. Dê um nome à sua chave na caixa de entrada **Nome da Chave**.
2. Introduza a frase de acesso na caixa de entrada **Frase de acesso**.

   NOTA: A frase de acesso é utilizada para proteger a chave exportada e deve ser fornecida de modo a que o utilizador da aplicação HP Sure Admin para telemóvel seja capaz de importar a chave.

3. Selecione **Iniciar sessão no Azure AD** e inicie a sessão.
4. Selecione o nome do seu grupo na caixa pendente **Nome do Grupo Azure AD**. Deve ser um membro do grupo para ter acesso à chave.
5. Selecione **Procurar** e escolha para onde exportar o caminho no sistema.
6. Selecione **Criar Chave**. A sua chave é criada com sucesso quando um ícone de notificação for apresentado ao lado do botão **Criar Chave** com a mensagem **Chave criada com sucesso**.
7. Selecione **Seguinte**. A página de resumo mostra as definições do HP Sure Admin que introduziu.
8. Selecione **Guardar Política**. A política é guardada quando é apresentada a mensagem **Guardada com sucesso**.
9. Navegue até à pasta onde guardou a chave e distribua-a para a aplicação HP Sure Admin para telemóvel, utilizando um método que esteja disponível para esse utilizador nesse dispositivo, tal como o e-mail. Este utilizador também precisará da frase de acesso para importar a chave. A HP recomenda que utilize diferentes mecanismos de distribuição para a chave e a frase de acesso.

   NOTA: Ao enviar o código QR, envie-o no respetivo tamanho original. A aplicação não poderá ler corretamente a imagem se esta tiver um tamanho inferior a 800 × 600.

Criar e enviar uma chave para o OneDrive do Grupo Azure AD

(Recomendado) Utilize esta opção para evitar armazenar a chave de autorização de acesso local no telefone. Quando escolher esta opção, o MIK armazenará a chave de autorização de acesso local na pasta OneDrive especificada, que apenas é acessível ao grupo autorizado. O utilizador da aplicação HP Sure Admin para telemóvel terá de se autenticar no Azure AD sempre que seja necessário um PIN.

1. Dê um nome à sua chave na caixa de entrada **Nome da Chave**.
2. Introduza a frase de acesso na caixa de entrada **Frase de acesso**.
3. Selecione **Iniciar sessão no Azure AD** e inicie a sessão.
4. Selecione o nome do grupo na caixa pendente Nome do Grupo Azure AD.

   NOTA: Deve ser um membro do grupo para ter acesso à chave.

5. Introduza o nome da pasta do OneDrive onde pretende guardar a chave na caixa de entrada **OneDrive**.
6. Selecione **Procurar** e escolha para onde exportar o caminho no sistema.
7. Selecione **Criar Chave**.

NOTA: A sua chave foi adicionada com sucesso à pasta OneDrive especificada e exportada para a pasta local especificada quando um ícone de notificação for apresentado ao lado do botão **Criar Chave** com a mensagem **Chave criada com sucesso**.

8. Selecione **Seguinte**. A página de resumo mostra as definições do HP Sure Admin que introduziu.
9. Selecione **Guardar Política**. A política é guardada quando é apresentada a mensagem **Guardada com sucesso**.

NOTA: Neste cenário, não é necessário enviar nada para a aplicação HP Sure Admin para telemóvel para efetuar o provisionamento prévio. Os PCs de destino são provisionados para apontar para a localização OneDrive que está incluída no código QR. A aplicação HP Sure Admin para telemóvel utiliza este apontador para aceder à localização OneDrive, caso o utilizador faça parte do grupo autorizado e seja autenticado com sucesso.

3 Configuração do telefone

Transfira a aplicação HP Sure Admin para telemóvel a partir da Google Play ou Apple Store.

- Transferir o HP Sure Admin da Google Store para telemóveis Android.
- Transferir o HP Sure Admin da Apple Store para telemóveis iOS.

Utilização da aplicação HP Sure Admin para telemóvel para desbloquear o BIOS

A aplicação HP Sure Admin para telemóvel substitui a utilização da palavra-passe do BIOS para acesso local à configuração do BIOS ao fornecer um PIN único, obtido ao digitalizar o código QR apresentado no computador de destino.

Siga estes passos para guardar a chave localmente no telefone, quando a chave for enviada ao utilizador da aplicação para telemóvel. No exemplo a seguir, a chave é enviada por e-mail para o utilizador da aplicação para telemóvel HP Sure Admin, e o utilizador abre o e-mail no telemóvel.

1. Abra o e-mail que contém a chave.
2. Quando a página de **Registo** for apresentada, introduza a frase de acesso na caixa de entrada **Introduza a frase de acesso** e o seu endereço de e-mail na caixa de entrada **Introduza o seu endereço de e-mail** para desencriptar a chave e adicioná-la à aplicação HP Sure Admin. O número PIN de desbloqueio é apresentado na página **O Seu PIN**.

> **NOTA:** Este passo guarda a chave no dispositivo móvel e completa o registo. Nesta altura, é possível utilizar a aplicação HP Sure Admin para telemóvel para aceder a qualquer dispositivo que tenha sido provisionado para estar acessível através desta chave. Apenas é necessário um endereço de e-mail se o administrador o exigir.

3. Introduza o PIN na caixa de entrada **Introduza o Código de Resposta** do BIOS.

Obter acesso à configuração do BIOS após o registo

Para obter acesso à configuração do BIOS num computador de destino após o registo:

1. Aceda à configuração do BIOS no arranque no computador de destino.
2. Selecione **Digitalizar Código QR** na aplicação para telemóvel e digitalize o código QR no computador de destino.
3. Se for solicitada a autenticação do utilizador, apresente as suas credenciais.
4. O número PIN desbloqueado é apresentado na página **O Seu PIN**.
5. Introduza o PIN na caixa de entrada **Introduza o Código de Resposta** do BIOS no computador de destino.

Desbloquear o BIOS com o OneDrive do Azure AD Group

Para utilizar o HP Sure Admin para desbloquear o BIOS com o OneDrive do Grupo Azure AD:

1. Selecione **Digitalizar Código QR** e, em seguida, digitalize o código QR do BIOS.

NOTA: A aplicação HP Sure Admin apresenta a página de início de sessão do Azure AD.

2. Inicie sessão na sua conta Azure.
3. Introduza o PIN na caixa de entrada **Introduza o Código de Resposta** do BIOS.

NOTA: A aplicação HP Sure Admin não guarda a chave localmente neste cenário. A aplicação HP Sure Admin para telemóvel tem de ter acesso à rede e o utilizador deve fazer a autenticação sempre que seja necessário um PIN único.

4 Códigos de erro de HP Sure Admin

Use a tabela nesta secção para ver os códigos, tipos e descrições de erro do HP Sure Admin e da KMS Admin Console.

Tabela 4-1 Códigos, tipos e descrições de erro da aplicação HP Sure Admin

Código de erro	Tipo de erro	Descrição
100	QRCodeUnknownError	Erro geral.
101	QRCodeDeserialization	Não é possível ler o JSON do código QR. A cadeia não se encontra num ficheiro JSON válido ou os dados são inválidos.
102	QRCodeInvalidImage	A imagem do Código QR digitalizado é inválida. Não é possível ler o ficheiro de imagem do Código QR.
103	QRCodeNoPayload	A imagem do Código QR digitalizado é inválida. O ficheiro de imagem não tem um payload JSON.
104	QRCodeInvalid	Não é possível ler o JSON do código QR. A cadeia não é um JSON válido ou os dados na imagem QR são inválidos.
105	QRCodeInvalidKeyIdHash	O hash de chave pública no JSON do Código QR não corresponde ao hash da chave pública do pacote de registo (Dados KeyID).
106	QRCodeTampered	A imagem do Código QR digitalizado foi alterada e é inválida.
107	QRCodeTamperedOrInvalidPassPhrase	A imagem do Código QR digitalizada foi alterada e é inválida, ou a frase de acesso inserida está incorreta.

Tabela 4-2 Chave de acesso única de erros, tipos e respetivas descrições do OneDrive

Código de erro	Tipo de erro	Descrição
200	OneTimeKeyError	Erro geral.
201	OneTimeKeyNoUserGroups	O utilizador com sessão iniciada não pertence a nenhum grupo AD na sua organização.
203	OneTimeKeyInvalidUserGroup	O utilizador com sessão iniciada não pertence ao grupo AD atribuído por esta chave.
204	OneTimeKeyQRFileDoesNotExist	O ficheiro da chave única não existe na pasta OneDrive do Grupo AD.
205	OneTimeKeyInvalidQRFile	O ficheiro da chave única na pasta OneDrive do Grupo AD é inválido.
206	OneTimeKeyInvalidQRpayload	O ficheiro da chave única existe, mas não foi possível ler o payload do ficheiro.

Tabela 4-3 Erros de autorização do Azure AD

Código de erro	Tipo de erro	Descrição
300	AzureADUnknownError	Erro geral.
301	AzureADInvalidDomain	O endereço de e-mail introduzido não corresponde ao nome de domínio que é especificado na imagem do código QR.
302	AzureADAccessToken	Erro ao adquirir o token de acesso do Azure AD. O utilizador não pode iniciar sessão no Azure AD da sua organização, ou a aplicação não possui as permissões necessárias para se ligar à Azure AD da sua organização. Também é possível que o utilizador tenha cancelado a autenticação.
303	AzureADUserProfile	Foi permitido à aplicação HP Sure Admin obter as informações de perfil de utilizador do Azure AD da sua organização.
304	AzureADUserPrincipalMismatch	O endereço de e-mail introduzido não corresponde ao nome principal do utilizador com sessão iniciada.
305	AzureADUserInvalidUserGroup	O utilizador com sessão iniciada não pertence ao grupo Azure AD ao qual esta chave foi atribuída.

Tabela 4-4 Erros, tipos e respetivas descrições da KMS Admin Console

Código de erro	Tipo de erro	Descrição
401	KmsUnauthorized	O utilizador não está autorizado a usar o serviço KMS.
402	KmsKeyDoesNotExist	Não existe qualquer chave privada compatível no cofre de chaves KMS. A chave está atualmente num estado excluído, mas recuperável, e o respetivo nome não pode ser reutilizado neste estado. A chave apenas pode ser recuperada ou removida.
403	KmsKeyDoesNotExistInTableStorage	A chave não existe no armazenamento de tabelas.
404	KmsUploadKeyErrorInKeyVault	Ocorreu um erro ao adicionar uma chave ao cofre de chaves.
405	KmsUploadKeyUnauthorized	O utilizador não está autorizado a carregar chaves. O utilizador não pertence ao Grupo AD autorizado a chamar esta API.
406	KmsInvalidAzureADLogin	O utilizador não possui sessão iniciada no Azure Tenant AAD.
407	KmsNoUserGroups	O utilizador com sessão iniciada não pertence a nenhum grupo AD na sua organização.
408	KmsInvalidUserGroup	O utilizador com sessão iniciada não pertence ao grupo AD atribuído para esta chave.

Tabela 4-4 Erros, tipos e respetivas descrições da KMS Admin Console (continuação)

Código de erro	Tipo de erro	Descrição
409	KmsInvalidAccessToken	O token de acesso que foi fornecido no pedido é inválido.
410	KmsAccessTokenExpired	O token de acesso fornecido expirou.
411	KmsAccessTokenInvalidTenantId	O token de acesso fornecido tem o valor TenantId inválido.
412	KmsAccessTokenTenantIdMismatch	O TenantId no token de acesso fornecido não corresponde à aplicação de função TenantId.
413	KmsInvalidKeyId	O keyId é nulo ou vazio.
414	KmsDeleteKeyUnauthorized	O utilizador não está autorizado a excluir chaves. O utilizador não pertence ao Grupo AD autorizado a chamar esta API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	A tentativa de recuperação do segredo falhou e não foi possível recuperá-lo. O utilizador deve tentar novamente.
416	KmsInvalidGetKeysRequest	O pedido para obter chaves é inválido.
417	KmsGetKeysUnauthorized	O utilizador não está autorizado a obter chaves. O utilizador não pertence ao Grupo AD autorizado a chamar esta API.
418	KmsInvalidRequestPayload	O pedido recebido pela API é inválido.
419	KmsRequestRequired	O pedido recebido não deve estar vazio.
420	KmsKeyNotConcurrent	A chave no armazenamento de tabelas foi atualizada ou modificada desde a última vez que o utilizador recuperou uma cópia.