Guia do usuário do HP Sure Admin

RESUMO

O HP Sure Admin permite que os administradores de TI gerenciem com segurança as configurações importantes de firmware do dispositivo usando certificados e criptografia de chave pública para o gerenciamento remoto e local de configurações em vez de uma senha.

Informações legais

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

Apple é marca comercial da Apple Computer, Inc. registrada nos EUA e em outros países.

Google Play é uma marca comercial da Google LLC.

Software de computador confidencial. Licença válida da HP necessária para posse, utilização ou cópia. Consistente com o FAR 12.211 e 12.212, o Software de Computador Comercial, a Documentação de Software de Computador e os Dados Técnicos para Itens Comerciais estão licenciados para o Governo dos EUA sob a licença comercial do vendedor.

As informações contidas neste documento estão sujeitas a alterações sem aviso. As únicas garantias para produtos e serviços da HP são as estabelecidas nas declarações de garantia expressa que acompanham tais produtos e serviços. Nenhuma informação contida neste documento deve ser interpretada como uma garantia adicional. A HP não será responsável por omissões, erros técnicos ou erros editoriais contidos neste documento.

Segunda edição: outubro de 2021

Primeira edição: dezembro de 2019

Número de peça do documento: L83995-202

Conteúdo

1 Passos iniciais

O HP Sure Admin permite que os administradores de TI gerenciem com segurança as configurações importantes de firmware do dispositivo usando certificados e criptografia de chave pública para o gerenciamento remoto e local de configurações em vez de uma senha.

O HP Sure Admin consiste nos seguintes itens:

- **Computador de destino:** As plataformas para gerenciar suportam o Modo de autenticação aprimorada de BIOS.
- **HP Manageability Integration Kit (MIK):** O plug-in do System Center Configuration Manager (SCCM) ou do HP BIOS Configuration Utility (BCU) para o gerenciamento remoto das configurações do BIOS.
- **HP Sure Admin Local Access Authenticator:** Um aplicativo para celular que substitui a senha para permitir o acesso local à configuração do BIOS fazendo a leitura de um código QR para obter um PIN de uso único.

Utilização do HP Sure Admin

Esta seção 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 Enhanced BIOS Configuration Utility (BCU).
2. Baixe o aplicativo para celular HP Sure Admin da loja Google Play™ ou da Apple App Store®.
3. Crie um par de chaves usado pelo dispositivo de destino e pelo aplicativo para celular HP Sure Admin para obter o PIN de uso único para desbloquear o BIOS.

Desativação do HP Sure Admin

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

- Na configuração F10 do BIOS, selecione **Restaurar as configurações de segurança para os padrões de fábrica**.

NOTA: Isso requer presença física ao fornecer o PIN de autenticação através do aplicativo para celular HP Sure Admin para acessar as configurações F10.

- Use o comando BCU para chamar remotamente o WMI da opção **Restaurar as configurações de segurança para os padrões de fábrica**.

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

- Na página MIK Security Provisioning, selecione **Desprovisionar**.

2 Criação e gerenciamento de chaves

Conclua o provisionamento de segurança dentro do MIK antes de ativar o Modo de autenticação aprimorada de BIOS. O Modo de autenticação aprimorada de BIOS deve ser ativado para criar e exportar chaves. Para ativar o Modo de autenticação de BIOS:

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

Criação e exportação de chaves

Existem 3 maneiras diferentes de criar pares de chaves de acesso local e habilitar o aplicativo para celular HP Sure Admin para acessar a chave.

Criação e exportação da Chave com distribuição manual

Use esta opção para exportar a chave de autorização de acesso local e, em seguida, distribuí-la manualmente ao aplicativo para celular HP Sure Admin por e-mail ou outro método.

NOTA: Esta opção não exige o acesso à rede pelo aplicativo para celular HP Sure Admin para obter um PIN de uso único.

1. Dê um nome para sua chave na caixa de entrada **Nome da chave**.
2. Insira a senha na caixa de entrada **Senha**.

   NOTA: A senha é usada para proteger a chave exportada e deve ser fornecida para que o usuário do aplicativo para celular HP Sure Admin seja capaz de importar a chave.

3. Selecione **Procurar** e escolha para onde exportar o caminho no sistema.
4. Selecione **Criar chave**. Sua chave terá sido criada com êxito quando um ícone de notificação for exibido ao lado do botão **Criar chave** com a mensagem **Chave criada com êxito**.
5. Selecione **Avançar**. A página de resumo exibe as configurações do HP Sure Admin que você inseriu.
6. Selecione **Salvar política**. A política estará salva quando uma mensagem **Salva com êxito** for exibida.
7. Navegue até a pasta na qual você salvou a chave e distribua-a ao usuário do aplicativo para celular HP Sure Admin usando um método que esteja disponível para esse usuário no dispositivo, como e-mail. Esse usuário também precisará da senha para importar a chave. A HP recomenda usar diferentes mecanismos de distribuição para a chave e a senha.

   NOTA: Ao enviar o código QR, envie-o em seu tamanho original. O aplicativo não conseguirá ler corretamente a imagem se ela for menor que 800 × 600.

Criação e exportação de uma chave com Revogação de Azure AD

Use esta opção para conectar a chave de acesso local a um grupo Azure Active Directory especificado e exigir que o aplicativo para celular HP Sure Admin exija a autenticação do usuário no Azure Active Directory e para confirmar que o usuário 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 ao aplicativo para celular por meio de e-mail ou outro método.

NOTA: Esta opção exige que o aplicativo para celular HP Sure Admin tenha acesso à rede para obter um PIN de uso único.

1. Dê um nome para sua chave na caixa de entrada **Nome da chave**.
2. Insira a senha na caixa de entrada **Senha**.

   NOTA: A senha é usada para proteger a chave exportada e deve ser fornecida para que o usuário do aplicativo para celular HP Sure Admin seja capaz de importar a chave.

3. Selecione **Login Azure AD** e efetue login.
4. Selecione o nome do seu grupo na caixa suspensa **Nome do grupo Azure AD**. Você 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**. Sua chave terá sido criada com êxito quando um ícone de notificação for exibido ao lado do botão **Criar chave** com a mensagem **Chave criada com êxito**.
7. Selecione **Avançar**. A página de resumo exibe as configurações do HP Sure Admin que você inseriu.
8. Selecione **Salvar política**. A política estará salva quando uma mensagem **Salva com êxito** for exibida.
9. Navegue até a pasta na qual você salvou a chave e distribua-a ao usuário do aplicativo para celular HP Sure Admin usando um método que esteja disponível para esse usuário no dispositivo, como e-mail. Esse usuário também precisará da senha para importar a chave. A HP recomenda usar diferentes mecanismos de distribuição para a chave e a senha.

   NOTA: Ao enviar o código QR, envie-o em seu tamanho original. O aplicativo não conseguirá ler corretamente a imagem se ela for menor que 800 × 600.

Criação e envio de uma chave para o OneDrive do Grupo Azure AD

(Recomendado) Use esta opção para evitar armazenar a chave de autorização de acesso local no celular. Quando você escolher esta opção, o MIK armazenará a chave de autorização de acesso local na pasta OneDrive especificada que só é acessível ao grupo autorizado. Será necessário que o usuário do aplicativo para celular HP Sure Admin autentique o Azure AD sempre que um PIN for necessário.

1. Dê um nome para sua chave na caixa de entrada **Nome da chave**.
2. Insira a senha na caixa de entrada **Senha**.
3. Selecione **Login Azure AD** e efetue login.
4. Selecione o nome do seu grupo na caixa suspensa Nome do grupo Azure AD.

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

5. Insira o nome da pasta OneDrive na qual deseja que a chave seja salva na caixa de entrada do **OneDrive**.

6. Selecione **Procurar** e escolha para onde exportar o caminho no sistema.
7. Selecione **Criar chave**.

NOTA: Sua chave terá sido adicionada com êxito à pasta OneDrive especificada e exportada para a pasta local especificada quando um ícone de notificação for exibido ao lado do botão **Criar Chave** com a mensagem **Chave criada com êxito.**

8. Selecione **Avançar**. A página de resumo exibe as configurações do HP Sure Admin que você inseriu.
9. Selecione **Salvar política**. A política estará salva quando a mensagem **Salva com êxito** for exibida.

NOTA: Neste cenário, não é necessário enviar nada ao aplicativo para celular HP Sure Admin para preprovisioná-lo. Os computadores de destino são provisionados para apontar para o local do OneDrive incluído no código QR. O aplicativo para celular HP Sure Admin usa esse indicador para acessar o local do OneDrive se o usuário fizer parte do grupo autorizado e for autenticado com êxito.

3 Configuração do celular

Baixe o aplicativo para celular HP Sure Admin da Google Play ou Apple store.

- Baixe o HP Sure Admin da loja da Google para celulares Android.
- Baixe o HP Sure Admin da loja da Apple para celulares iOS.

Utilização do aplicativo para celular HP Sure Admin para desbloquear o BIOS

O aplicativo para celular HP Sure Admin substitui o uso da senha do BIOS para o acesso local à configuração do BIOS fornecendo um PIN de uso único obtido por meio da leitura do código QR apresentado pela máquina de destino.

Siga essas etapas para salvar a chave localmente no celular em um cenário em que a chave seja enviada ao usuário do aplicativo para celular. No exemplo a seguir, a chave é enviada por e-mail para o usuário do aplicativo para celular HP Sure Admin e o usuário abre o e-mail pelo celular.

1. Abra o e-mail que contém a chave.
2. Quando a página de **Registro** for exibida, insira a senha na caixa de entrada **Insira a senha** e seu endereço de e-mail na caixa de entrada **Insira o seu endereço de e-mail** para descriptografar a chave e adicioná-la ao aplicativo HP Sure Admin. O número PIN de desbloqueio é exibido na página **Seu PIN**.

> **NOTA:** Esta etapa salva a chave no dispositivo móvel e conclui o registro. Neste ponto, você pode usar o aplicativo para celular HP Sure Admin para acessar qualquer dispositivo que tenha sido provisionado para ser acessível através dessa chave. Um endereço de e-mail é necessário somente se o administrador assim exigir.

3. Insira o PIN na caixa de entrada **Insira o código de resposta do BIOS**.

Obtenção de acesso à configuração do BIOS após o registro

Para obter acesso à configuração do BIOS em uma máquina de destino após o registro:

1. Insira a configuração do BIOS durante inicialização na máquina de destino.
2. Selecione **Leitura de código QR** no aplicativo para celular e faça a leitura do código QR na máquina de destino.
3. Se solicitada a autenticação de usuário, apresente suas credenciais.
4. O número PIN desbloqueado é exibido na página **Seu PIN**.
5. Insira o PIN na caixa de entrada **Insira o código de resposta do BIOS** na máquina de destino.

Desbloqueio do BIOS com o OneDrive do Grupo Azure AD

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

1. Selecione **Leitura de código QR** e, em seguida, faça a leitura do código QR do BIOS.

NOTA: O aplicativo HP Sure Admin exibe a página de login do Azure AD.

2. Faça login em sua conta do Azure.
3. Insira o PIN na caixa de entrada **Insira o código de resposta do BIOS**.

NOTA: O aplicativo HP Sure Admin não salva a chave localmente neste cenário. O aplicativo para celular HP Sure Admin deve ter acesso à rede e o usuário deve autenticar sempre que for necessário um PIN de uso único.

4 Códigos de erro do HP Sure Admin

Use a tabela nesta seção para ver os códigos, tipos e descrições dos erros do HP Sure Admin e KMS Admin Console.

Tabela 4-1 Códigos, tipos e descrições dos erros do aplicativo HP Sure Admin

Código de erro	Tipo de erro	Descrição
100	QRCodeUnknownError	Erro geral.
101	QRCodeDeserialization	Não é possível ler o código QR JSON. A string não é um arquivo JSON válido ou os dados são inválidos.
102	QRCodeInvalidImage	A imagem de código QR digitalizada é inválida. Não é possível ler o arquivo de imagem do código QR.
103	QRCodeNoPayload	A imagem de código QR digitalizada é inválida. O arquivo de imagem não tem conteúdo JSON.
104	QRCodeInvalid	Não é possível ler o código QR JSON. A string não é uma JSON válida ou os dados na imagem QR são inválidos.
105	QRCodeInvalidKeyIdHash	O hash de chave pública no JSON do código QR não é compatível com o hash da chave pública do pacote de registro (dados KeyID).
106	QRCodeTampered	A imagem de código QR digitalizada está adulterada e é inválida.
107	QRCodeTamperedOrInvalidPassPhrase	A imagem de código QR digitalizada está adulterada e é inválida, ou a senha inserida está incorreta.

Tabela 4-2 Tecla de acesso OneTime de tipos e descrições dos erros do OneDrive

Código de erro	Tipo de erro	Descrição
200	OneTimeKeyError	Erro geral.
201	OneTimeKeyNoUserGroups	O usuário logado não pertence a nenhum grupo AD que esteja na sua organização.
203	OneTimeKeyInvalidUserGroup	O usuário logado não pertence ao grupo AD ao qual essa chave foi atribuída.
204	OneTimeKeyQRFileDoesNotExist	O arquivo de chave OneTime não existe na pasta OneDrive do Grupo AD.
205	OneTimeKeyInvalidQRFile	O arquivo de chave OneTime na pasta OneDrive do Grupo AD é inválido.
206	OneTimeKeyInvalidQRpayload	O arquivo de chave OneTime existe, mas não consegue ler o conteúdo do arquivo.

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 inserido não corresponde ao nome de domínio que está especificado na imagem do código QR.
302	AzureADAccessToken	Erro ao adquirir o token de acesso do Azure AD. O usuário não pode efetuar login no Azure AD da sua organização, ou o aplicativo não tem as permissões necessárias para se conectar ao Azure AD da sua organização. Também pode ser que o usuário tenha cancelado a autenticação.
303	AzureADUserProfile	O aplicativo HP Sure Admin não consegue adquirir informações de perfil de usuário do Azure AD da sua organização.
304	AzureADUserPrincipalMismatch	O endereço de e-mail inserido não corresponde ao nome principal do usuário logado.
305	AzureADUserInvalidUserGroup	O usuário logado não pertence ao Grupo Azure AD atribuído ao qual essa chave foi atribuída.

Tabela 4-4 Tipos e descrições dos erros do KMS Admin Console

Código de erro	Tipo de erro	Descrição
401	KmsUnauthorized	O usuário não está autorizado a usar o serviço KMS.
402	KmsKeyDoesNotExist	Uma chave privada compatível não existe no cofre de chave KMS. A chave está atualmente em um estado excluído, mas recuperável, e seu nome não pode ser reutilizado neste estado. A chave só pode ser recuperada ou purgada.
403	KmsKeyDoesNotExistInTableStorage	A chave não existe no armazenamento de tabela.
404	KmsUploadKeyErrorInKeyVault	Ocorreu um erro ao adicionar uma chave ao cofre de chave.
405	KmsUploadKeyUnauthorized	O usuário não está autorizado a carregar chaves. O usuário não pertence ao Grupo AD autorizado com permissão para chamar esta API.
406	KmsInvalidAzureADLogin	O usuário não está logado ao Azure Tenant AAD.
407	KmsNoUserGroups	O usuário logado não pertence a nenhum Grupo AD na sua organização.
408	KmsInvalidUserGroup	O usuário logado não pertence ao grupo AD ao qual essa chave foi atribuída.
409	KmsInvalidAccessToken	O token de acesso que foi fornecido na solicitação é inválido.

Tabela 4-4 Tipos e descrições dos erros do KMS Admin Console (continuação)

Código de erro	Tipo de erro	Descrição
410	KmsAccessTokenExpired	O accessToken fornecido expirou.
411	KmsAccessTokenInvalidTenantId	O accessToken fornecido tem valor inválido de TenantId.
412	KmsAccessTokenTenantIdMismatch	O TenantId no accessToken fornecido não corresponde ao aplicativo de função TenantId.
413	KmsInvalidKeyId	O keyId é nulo ou está vazio.
414	KmsDeleteKeyUnauthorized	O usuário não está autorizado a excluir chaves. O usuário não pertence ao Grupo AD autorizado com permissão para chamar esta API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	A tentativa de recuperar o segredo falhou, e não foi possível recuperá-lo. O usuário deve tentar novamente.
416	KmsInvalidGetKeysRequest	A solicitação de Obter Chaves é inválida.
417	KmsGetKeysUnauthorized	O usuário não está autorizado a obter as chaves. O usuário não pertence ao Grupo AD autorizado com permissão para chamar esta API.
418	KmsInvalidRequestPayload	A solicitação recebida pela API é inválida.
419	KmsRequestRequired	A solicitação recebida não pode estar vazia.
420	KmsKeyNotConcurrent	A chave no armazenamento de tabela foi atualizada ou modificada desde que o usuário recuperou uma cópia pela última vez.