Instrukcja obsługi dla HP Sure Admin

PODSUMOWANIE

HP Sure Admin pozwala administratorom IT bezpiecznie zarządzać poufnymi ustawieniami oprogramowania układowego urządzeń przy użyciu certyfikatów i kryptografii z kluczem publicznym zamiast hasła — zarówno w przypadku zdalnego, jak i lokalnego zarządzania ustawieniami.

Informacje prawne

Wydanie drugie: październik 2021

Wydanie pierwsze: grudzień 2019

Numer katalogowy dokumentu: L83995-242

Spis treści

1 Rozpoczęcie pracy

HP Sure Admin pozwala administratorom IT bezpiecznie zarządzać poufnymi ustawieniami oprogramowania układowego urządzeń przy użyciu certyfikatów i kryptografii z kluczem publicznym zamiast hasła — zarówno w przypadku zdalnego, jak i lokalnego zarządzania ustawieniami.

Rozwiązanie HP Sure Admin składa się z następujących elementów:

- **Komputer docelowy:** platformy do zarządzania, które obsługują rozszerzony tryb uwierzytelniania systemu BIOS.
- **Narzędzie HP Manageability Integration Kit (MIK):** wtyczka do programu System Center Configuration Manager (SCCM) lub HP BIOS Configuration Utility (BCU) przeznaczona do zdalnego zarządzania ustawieniami systemu BIOS.
- **HP Sure Admin Local Access Authenticator:** aplikacja na telefon, która zastępuje hasło, aby umożliwić lokalny dostęp do konfiguracji systemu BIOS poprzez zeskanowanie kodu QR w celu uzyskania jednorazowego kodu PIN.

Korzystanie z narzędzia HP Sure Admin

W tej sekcji opisano proces korzystania z oprogramowania HP Sure Admin.

1. Otwórz wtyczkę HP Sure Admin wbudowaną we wtyczce narzędzia HP Manageability Integration Kit (MIK) do programu System Configuration Manager (SCCM) lub Enhanced BIOS Configuration Utility (BCU).
2. Pobierz aplikację na telefon HP Sure Admin ze sklepu Google Play™ lub App Store® firmy Apple.
3. Utwórz parę kluczy używaną przez urządzenie docelowe oraz aplikację na telefon HP Sure Admin w celu uzyskania jednorazowego kodu PIN do odblokowania systemu BIOS.

Wyłączanie narzędzia HP Sure Admin

W tej sekcji opisano opcje umożliwiające wyłączenie HP Sure Admin.

- W ustawieniu F10 w systemie BIOS wybierz opcję **Restore Security settings to Factory Defaults** (Przywróć fabryczne ustawienia zabezpieczeń).

UWAGA: Wymaga to fizycznej obecności poprzez podanie kodu PIN uwierzytelniania za pomocą aplikacji na telefon HP Sure Admin w celu uzyskania dostępu do ustawień F10.

- Użyj polecenia narzędzia BCU, aby zdalnie wywołać WMI dla opcji **Restore Security settings to Factory Defaults** (Przywróć fabryczne ustawienia zabezpieczeń).

UWAGA: Więcej informacji na ten temat można znaleźć w instrukcji obsługi narzędzia HP BIOS Configuration Utility (BCU).

- Na stronie MIK Security Provisioning wybierz opcję **Deprovision** (Anuluj przydzielanie).

2 Tworzenie kluczy i zarządzanie nimi

Zakończ przydzielanie zabezpieczeń w MIK, zanim włączony zostanie rozszerzony tryb uwierzytelnienia systemu BIOS (Enhanced BIOS Authentication Mode). Aby można było utworzyć i wyeksportować klucze, należy włączyć rozszerzony tryb uwierzytelniania systemu BIOS. Aby go włączyć:

▲ Otwórz wtyczkę HP Sure Admin i wybierz opcję **Enhanced BIOS Authentication Mode** (Rozszerzony tryb uwierzytelniania systemu BIOS), aby utworzyć i wyeksportować klucze.

Tworzenie i eksportowanie kluczy

Istnieją 3 różne sposoby tworzenia par lokalnych kluczy dostępu i umożliwienia aplikacji telefonicznej HP Sure Admin dostępu do klucza.

- Tworzenie i eksportowanie klucza wraz z dystrybucją ręczną na stronie 2
- Tworzenie i eksportowanie klucza za pomocą Azure AD Revocation na stronie 3
- Tworzenie i wysyłanie klucza do grupy Azure AD na dysku OneDrive: na stronie 3

Tworzenie i eksportowanie klucza wraz z dystrybucją ręczną

Ta opcja umożliwia wyeksportowanie klucza autoryzacji dostępu lokalnego, a następnie ręczne rozesłanie go do aplikacji na telefon HP Sure Admin za pośrednictwem poczty e-mail lub innej metody.

UWAGA: Ta opcja nie wymaga, aby aplikacja na telefon HP Sure Admin miała dostęp do sieci w celu uzyskania jednorazowego kodu PIN.

1. Nazwij klucz w polu **Key Name** (Nazwa klucza).
2. Wprowadź hasło w polu **Passphrase** (Hasło).

   UWAGA: Hasło jest używane do ochrony eksportowanego klucza i należy je podać, aby użytkownik aplikacji HP Sure Admin mógł zaimportować ten klucz.

3. Wybierz opcję **Browse** (Przeglądaj) i wybierz miejsce, do którego ma zostać wyeksportowana ścieżka systemu.
4. Wybierz opcję **Create Key** (Utwórz klucz). Twój klucz jest pomyślnie utworzony, gdy obok przycisku **Create Key** (Utwórz klucz) pojawi się ikona z powiadomieniem **Key successfully created** (Pomyślnie utworzono klucz).
5. Wybierz **Dalej**. Na stronie podsumowania zostaną wyświetlone wprowadzone przez użytkownika ustawienia narzędzia HP Sure Admin.
6. Wybierz opcję **Save Policy** (Zapisz zasadę). Zasada jest zapisana, gdy pojawi się komunikat **Saved successfully** (Zapis zakończony powodzeniem).
7. Przejdź do folderu, w którym został zapisany klucz, i przekaż go użytkownikowi aplikacji na telefon HP Sure Admin przy użyciu metody, która jest dostępna dla tego użytkownika na tym urządzeniu, np.

przez wiadomość e-mail. Ten użytkownik będzie również potrzebował hasła w celu zaimportowania tego klucza. Firma HP zaleca korzystanie z różnych mechanizmów dystrybucji klucza i hasła.

UWAGA: Wysyłając kod QR, prześlij go w oryginalnym rozmiarze. Aplikacja nie może prawidłowo odczytać obrazów mniejszych niż 800 × 600.

Tworzenie i eksportowanie klucza za pomocą Azure AD Revocation

Użyj tej opcji, aby połączyć klucz lokalnego dostępu z określoną grupą Azure Active Directory i aby przed udostępnieniem kodu PIN lokalnego dostępu aplikacja na telefon HP Sure Admin wymagała zarówno uwierzytelnienia użytkownika dla Azure Active Directory, jak i potwierdzenia, że użytkownik jest członkiem określonej grupy. Ta metoda wymaga również ręcznej dystrybucji klucza autoryzacji dostępu lokalnego do aplikacji na telefon za pośrednictwem poczty e-mail lub innej metody.

UWAGA: Ta opcja wymaga, aby aplikacja na telefon HP Sure Admin miała dostęp do sieci w celu uzyskania jednorazowego kodu PIN.

1. Nazwij klucz w polu **Key Name** (Nazwa klucza).
2. Wprowadź hasło w polu **Passphrase** (Hasło).

   UWAGA: Hasło jest używane do ochrony eksportowanego klucza i należy je podać, aby użytkownik aplikacji HP Sure Admin mógł zaimportować ten klucz.

3. Wybierz opcję **Azure AD Login** (Logowanie do Azure AD) i zaloguj się.
4. Wybierz nazwę grupy z listy rozwijanej **Azure AD Group Name** (Nazwa grupy Azure AD). Aby uzyskać dostęp do klucza, musisz być członkiem grupy.
5. Wybierz opcję **Browse** (Przeglądaj) i wybierz miejsce, do którego ma zostać wyeksportowana ścieżka systemu.
6. Wybierz opcję **Create Key** (Utwórz klucz). Twój klucz jest pomyślnie utworzony, gdy obok przycisku **Create Key** (Utwórz klucz) pojawi się ikona z powiadomieniem **Key successfully created** (Pomyślnie utworzono klucz).
7. Wybierz **Dalej**. Na stronie podsumowania zostaną wyświetlone wprowadzone przez użytkownika ustawienia narzędzia HP Sure Admin.
8. Wybierz opcję **Save Policy** (Zapisz zasadę). Zasada jest zapisana, gdy pojawi się komunikat **Saved successfully** (Zapis zakończony powodzeniem).
9. Przejdź do folderu, w którym został zapisany klucz, i przekaż go użytkownikowi aplikacji na telefon HP Sure Admin przy użyciu metody, która jest dostępna dla tego użytkownika na tym urządzeniu, np. przez wiadomość e-mail. Ten użytkownik będzie również potrzebował hasła w celu zaimportowania tego klucza. Firma HP zaleca korzystanie z różnych mechanizmów dystrybucji klucza i hasła.

   UWAGA: Wysyłając kod QR, prześlij go w oryginalnym rozmiarze. Aplikacja nie może prawidłowo odczytać obrazów mniejszych niż 800 × 600.

Tworzenie i wysyłanie klucza do grupy Azure AD na dysku OneDrive:

(Zalecane) Ta opcja pozwala uniknąć przechowywania klucza autoryzacji lokalnego dostępu w telefonie. Po wybraniu tej opcji narzędzie MIK będzie przechowywać klucz autoryzacji lokalnego dostępu w określonym folderze na dysku OneDrive, który to folder będzie dostępny tylko dla autoryzowanej grupy. Za każdym

razem, gdy wymagany będzie kod PIN, użytkownik aplikacji na telefon HP Sure Admin będzie musiał uwierzytelnić się w Azure AD.

1. Nazwij klucz w polu **Key Name** (Nazwa klucza).
2. Wprowadź hasło w polu **Passphrase** (Hasło).
3. Wybierz opcję **Azure AD Login** (Logowanie do Azure AD) i zaloguj się.
4. Wybierz nazwę grupy z listy rozwijanej Azure AD Group Name (Nazwa grupy Azure AD).

UWAGA: Aby uzyskać dostęp do klucza, musisz być członkiem grupy.

5. W polu **OneDrive** wprowadź nazwę folderu na dysku OneDrive, w którym to folderze ma być zapisany klucz.
6. Wybierz opcję **Browse** (Przeglądaj) i wybierz miejsce, do którego ma zostać wyeksportowana ścieżka systemu.
7. Wybierz opcję **Create Key** (Utwórz klucz).

UWAGA: Klucz jest pomyślnie dodany do określonego folderu na dysku OneDrive i wyeksportowany do określonego folderu lokalnego, gdy obok przycisku **Create Key** (Utwórz klucz) wyświetlany jest komunikat **Key successfully created** (Tworzenie klucza zakończone powodzeniem).

8. Wybierz **Dalej**. Na stronie podsumowania zostaną wyświetlone wprowadzone przez użytkownika ustawienia narzędzia HP Sure Admin.
9. Wybierz opcję **Save Policy** (Zapisz zasadę). Zasada jest zapisana, gdy pojawi się komunikat **Saved successfully** (Zapis zakończony powodzeniem).

UWAGA: W tym przypadku nie ma potrzeby wysyłania jakichkolwiek danych do aplikacji na telefon HP Sure Admin w celu jej wstępnego przydzielenia. Komputery docelowe uzyskują możliwość wskazania lokalizacji na dysku OneDrive ujętej w kodzie QR. Aplikacja na telefon HP Sure Admin korzysta z tego wskaźnika, aby uzyskać dostęp do lokalizacji na dysku OneDrive, jeśli użytkownik jest członkiem autoryzowanej grupy i pomyślnie się uwierzytelni.

3 Konfiguracja telefonu

Pobierz aplikację na telefon HP Sure Admin ze sklepu Google Play lub App Store.

- W przypadku telefonów z systemem Android pobierz narzędzie HP Sure Admin ze sklepu Google Play.
- W przypadku telefonów z systemem iOS pobierz narzędzie HP Sure Admin ze sklepu App Store.

Korzystanie z aplikacji na telefon HP Sure Admin w celu odblokowania systemu BIOS

Aplikacja mobilna HP Sure Admin zastępuje użycie hasła systemu BIOS do lokalnego dostępu do konfiguracji systemu BIOS poprzez podanie jednorazowego kodu PIN uzyskanego po zeskanowaniu kodu QR wyświetlanego przez urządzenie docelowe.

Wykonaj poniższe czynności, aby zapisać klucz lokalnie w telefonie w scenariuszu, w którym klucz jest wysyłany do użytkownika aplikacji telefonu. W poniższym przykładzie klucz jest wysyłany e-mailem do użytkownika aplikacji telefonu HP Sure Admin, a użytkownik otwiera wiadomość e-mail w telefon.

1. Otwórz wiadomość e-mail zawierającą ten klucz.
2. Gdy zostanie wyświetlona strona **Enrollment** (Rejestracja), wprowadź hasło w polu **Enter passphrase** (Wprowadź hasło) i swój adres e-mail w polu **Enter your email address** (Wprowadź swój adres e-mail), aby odszyfrować klucz i dodać go do aplikacji HP Sure Admin. Odblokowujący kod PIN jest wyświetlany na stronie **Your PIN** (Twój kod PIN).

   UWAGA: Ten krok zapisuje klucz na urządzeniu przenośnym i kończy rejestrację. W tym momencie możesz skorzystać z aplikacji na telefon HP Sure Admin, aby uzyskać dostęp do dowolnego urządzenia, do którego ustanowiono dostęp poprzez ten klucz. Adres e-mail jest wymagany tylko wtedy, gdy wymaga tego administrator.

3. Wprowadź kod PIN w polu **Enter Response Code** (Wprowadź kod odpowiedzi) systemu BIOS.

Uzyskanie dostępu do konfiguracji systemu BIOS po rejestracji

Aby uzyskać dostęp do konfiguracji systemu BIOS na komputerze docelowym po rejestracji:

1. Przejdź do konfiguracji systemu BIOS przy rozruchu na komputerze docelowym.
2. Wybierz opcję **Scan QR Code** (Zeskanuj kod QR) w aplikacji telefonu i zeskanuj kod QR na komputerze docelowym.
3. Jeśli zostanie wyświetlony monit o uwierzytelnienie użytkownika, należy podać dane uwierzytelniające.
4. Odblokowujący numer PIN zostanie wyświetlony na stronie **Your PIN** (Twój kod PIN).
5. Wprowadź kod PIN w polu **Enter Response Code** (Wprowadź kod odpowiedzi) systemu BIOS na komputerze docelowym.

Odblokowywanie systemu BIOS za pomocą usługi OneDrive grupy AD usługi Azure

Aby użyć programu HP Sure Admin w celu odblokowania systemu BIOS za pomocą grupy Azure AD na dysku OneDrive:

1. Wybierz opcję **Scan QR Code** (Zeskanuj kod QR), a następnie zeskanuj kod QR systemu BIOS.

   UWAGA: Aplikacja HP Sure Admin wyświetla stronę logowania Azure AD.

2. Zaloguj się do konta Azure.
3. Wprowadź kod PIN w polu **Enter Response Code** (Wprowadź kod odpowiedzi) systemu BIOS.

   UWAGA: W tym przypadku aplikacja HP Sure Admin nie zapisuje klucza lokalnie. Aplikacja na telefon HP Sure Admin musi mieć dostęp do sieci, a użytkownik musi uwierzytelnić się za każdym razem, gdy potrzebny jest jednorazowy kod PIN.

4 Kody błędów HP Sure Admin

Użyj tabeli w tej sekcji, aby zobaczyć kody błędów, typy i opisy administratora HP Sure Admin oraz KMS Admin Console.

Tabela 4-1 Kody błędów aplikacji HP Sure Admin, typy i opisy aplikacji HP Sure Admin

Kod błędu	Typ błędu	Opis
100	QRCodeUnknownError	Błąd ogólny.
101	QRCodeDeserialization	Nie można odczytać kodu QR JSON. Ciąg nie jest prawidłowym plikiem JSON lub dane są nieprawidłowe.
102	QRCodeInvalidImage	Zeskanowany obraz kodu QR jest nieprawidłowy. Nie można odczytać pliku obrazu kodu QR.
103	QRCodeNoPayload	Zeskanowany obraz kodu QR jest nieprawidłowy. Plik obrazu nie ma ładunku JSON.
104	QRCodeInvalid	Nie można odczytać ciągu JSON kodu QR. Ciąg nie jest prawidłowym ciągiem JSON lub dane w obrazie QR są nieprawidłowe.
105	QRCodeInvalidKeyIdHash	Skrót klucza publicznego ciągu JSON kodu QR nie jest zgodny ze skrótem klucza publicznego pakietu rejestracji (dane KeyID).
106	QRCodeTampered	Zeskanowany obraz kodu QR jest poruszony i nieprawidłowy.
107	QRCodeTamperedOrInvalidPassPhrase	Zeskanowany obraz kodu QR jest poruszony i nieprawidłowy lub wprowadzone hasło jest nieprawidłowe.

Tabela 4-2 Klucz dostępu jednorazowego, pochodzący z błędów, typów i opisów usługi OneDrive

Kod błędu	Typ błędu	Opis
200	OneTimeKeyError	Błąd ogólny.
201	OneTimeKeyNoUserGroups	Zalogowany użytkownik nie należy do żadnej grupy AD, która znajduje się w Twojej organizacji.
203	OneTimeKeyInvalidUserGroup	Zalogowany użytkownik nie należy do grupy AD, do której jest przypisany ten klucz.
204	OneTimeKeyQRFileDoesNotExist	Plik klucza OneTime nie istnieje w folderze grupy AD na dysku OneDrive.
205	OneTimeKeyInvalidQRFile	Plik klucza OneTime w folderze grupy AD na dysku OneDrive jest nieprawidłowy.
206	OneTimeKeyInvalidQRpayload	Plik klucza OneTime istnieje, ale nie można odczytać ładunku pliku.

Tabela 4-3 Błędy uwierzytelnienia usługi Azure AD

Kod błędu	Typ błędu	Opis
300	AzureADUnknownError	Błąd ogólny.
301	AzureADInvalidDomain (Domena)	Wprowadzony adres e-mail nie pasuje do nazwy domeny, która jest określona na obrazie kodu QR.
302	AzureADAccessToken	Wystąpił błąd podczas uzyskiwania tokena dostępu z Azure AD. Użytkownik nie może zalogować się do Azure AD Twojej organizacji lub aplikacja nie ma wymaganych uprawnień do nawiązywania połączeń z usługą AD Azure Twojej organizacji. Może także oznaczać, że użytkownik anulował uwierzytelnianie.
303	AzureADUserProfile	Aplikacja HP Sure Admin została włączona w celu pobrania informacji o profilu użytkownika z Azure AD Twojej organizacji.
304	AzureADUserPrincipalMismatch	Wprowadzony adres e-mail nie pasuje do nazwy głównej zalogowanego użytkownika.
305	AzureADUserInvalidUserGroup	Zalogowany użytkownik nie należy do grupy Azure AD przypisanej dla tego klucza.

Tabela 4-4 Błędy, typy i opisy KMS Admin Console

Kod błędu	Typ błędu	Opis
401	KmsUnauthorized	Użytkownik nie jest uprawniony do korzystania z usługi KMS.
402	KmsKeyDoesNotExist	Dopasowywanie klucza prywatnego nie istnieje w przechowalni kluczy KMS. Klucz jest obecnie w stanie usuniętym, ale możliwym do odzyskania, a jego nazwa nie może być ponownie użyta w tym stanie. Klucz można odzyskać lub oczyścić.
403	KmsKeyDoesNotExistInTableStorage	Klucz nie istnieje w pamięci masowej tabeli.
404	KmsUploadKeyErrorInKeyVault	Podczas dodawania klucza do przechowalni kluczy wystąpił błąd.
405	KmsUploadKeyUnauthorized	Użytkownik nie jest uprawniony do przesyłania kluczy. Użytkownik nie należy do autoryzowanej grupy AD dozwolonej do wywoływania tego interfejsu API.
406	KmsInvalidAzureADLogin	Użytkownik nie jest zalogowany w Azure Tenant AAD.
407	KmsNoUserGroups	Zalogowany użytkownik nie należy do żadnej Grupy AD w Twojej organizacji.
408	KmsInvalidUserGroup	Zalogowany użytkownik nie należy do przypisanej Grupy AD, do której klucz jest przypisany.

Tabela 4-4 **Błędy, typy i opisy KMS Admin Console (ciąg dalszy)**

Kod błędu	Typ błędu	Opis
409	KmsInvalidAccessToken	Nieprawidłowy jest token dostępu, który został podany w żądaniu.
410	KmsAccessTokenExpired	Podany accessToken wygasł.
411	KmsAccessTokenInvalidTenantId	Dostarczony accessToken ma nieprawidlową wartość TenantId.
412	KmsAccessTokenTenantIdMismatch	TenantId w podanym accessToken nie pasuje do TenantId aplikacji funkcyjnej.
413	KmsInvalidKeyId	keyId jest zerowy lub pusty.
414	KmsDeleteKeyUnauthorized	Użytkownik nie jest uprawniony do usuwania kluczy. Użytkownik nie należy do autoryzowanej grupy AD dozwolonej do wywoływania tego interfejsu API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Próba odzyskania utajnionych danych nie powiodła się i nie można ich odzyskać. Użytkownik powinien spróbować ponownie.
416	KmsInvalidGetKeysRequest	Żądanie uzyskania kluczy jest nieważne.
417	KmsGetKeysUnauthorized	Użytkownik nie jest uprawniony do uzyskiwania kluczy. Użytkownik nie należy do autoryzowanej grupy AD dozwolonej do wywoływania tego interfejsu API.
418	KmsInvalidRequestPayload	Żądanie odebrane przez API jest nieważne.
419	KmsRequestRequired	Odebrane żądanie nie może być puste.
420	KmsKeyNotConcurrent	Klucz w pamięci tabeli został zaktualizowany lub zmodyfikowany od czasu ostatniego pobrania kopii przez użytkownika.