



HP Sure Admin 사용 설명서

요약

HP Sure Admin을 통해 IT 관리자는 설정의 원격 및 로컬 관리를 위한 인증서와 공개 키 암호화를 암호 대신 사용하여 중요한 장치 펌웨어 설정을 안전하게 관리할 수 있습니다.

법적 정보

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

Apple은 미국 및 기타 국가/지역에서 Apple Computer, Inc.의 등록 상표입니다.

Google Play는 Google LLC의 상표입니다.

기밀 컴퓨터 소프트웨어. 소유, 사용 또는 복사에 필요한 유효한 라이선스를 HP로부터 취득했습니다. FAR 12.211 및 12.212, 상업용 컴퓨터 소프트웨어, 컴퓨터 소프트웨어 설명서 및 상용 품목에 대한 기술 데이터는 공급업체의 표준 상업 라이선스에 따라 미국 정부에 사용이 허가되었습니다.

본 설명서의 내용은 사전 통지 없이 변경될 수 있습니다. HP 제품 및 서비스에 대한 유일한 보증은 제품 및 서비스와 함께 동봉된 보증서에 명시되어 있습니다. 본 설명서에는 어떠한 추가 보증 내용도 들어 있지 않습니다. HP는 본 설명서의 기술상 또는 편집상 오류나 누락에 대해 책임지지 않습니다.

제2판: 2021년 10월

초판: 2019년 12월

문서 일련 번호: L83995-AD2

목차

1 시작하기	1
HP Sure Admin 사용	1
HP Sure Admin 비활성화	1
2 키 만들기 및 관리	2
키 만들기 및 내보내기	2
수동 배포로 키 만들기 및 내보내기.....	2
Azure AD 해지로 키를 만들고 내보내는 방법	3
키를 만들고 Azure AD 그룹 OneDrive에 전송	3
3 휴대폰 설정	5
HP Sure Admin 휴대폰 앱을 사용하여 BIOS 잠금 해제	5
등록 후 BIOS 설정에 대한 액세스 권한 가져오기	5
Azure AD 그룹 OneDrive로 BIOS 잠금 해제	5
4 HP Sure Admin 오류 코드	7

1 시작하기

HP Sure Admin을 통해 IT 관리자는 설정의 원격 및 로컬 관리를 위한 인증서와 공개 키 암호화를 암호 대신 사용하여 중요한 장치 펌웨어 설정을 안전하게 관리할 수 있습니다.

HP Sure Admin은 다음과 같이 구성됩니다.

- **대상 PC:** 향상된 BIOS 인증 모드를 지원하는 관리 대상 플랫폼입니다.
- **HP Manageability Integration Kit(MIK):** BIOS 설정의 원격 관리를 위한 System Center Configuration Manager(SCCM) 또는 HP BIOS Configuration Utility(BCU)용 플러그인입니다.
- **HP Sure Admin Local Access Authenticator:** 암호를 대체하는 휴대폰 앱으로, QR 코드를 스캔하여 일회성 PIN을 얻어 BIOS 설정에 로컬로 액세스하는 데 사용합니다.

HP Sure Admin 사용

다음 섹션에서는 HP Sure Admin을 사용하는 프로세스를 설명합니다.

1. System Configuration Manager(SCCM) 또는 향상된 BIOS Configuration Utility(BCU)용 HP Manageability Integration Kit(MIK) 플러그인에서 HP Sure Admin 플러그인을 엽니다.
2. Google Play™ 스토어 또는 Apple App Store®에서 HP Sure Admin 휴대폰 앱을 다운로드합니다.
3. 대상 장치와 HP Sure Admin 휴대폰 앱에서 BIOS 잠금을 해제하는 일회성 PIN을 얻는 데 사용할 키 쌍을 만듭니다.

HP Sure Admin 비활성화

다음 섹션에서는 HP Sure Admin을 비활성화하는 옵션을 설명합니다.

- BIOS F10 설정에서 **출하 시 기본값으로 보안 설정 복원**을 선택합니다.

 **참고:** F10 설정에 액세스하려면 HP Sure Admin 휴대폰 앱을 통해 인증 PIN을 제공하여 물리적 실체를 증명해야 합니다.

- BCU 명령을 사용하여 **출하 시 기본값으로 보안 설정 복원**의 WMI를 원격으로 호출합니다.

 **참고:** 자세한 내용은 HP BIOS Configuration Utility(BCU) 사용 설명서를 참조하십시오.

- MIK 보안 프로비저닝 페이지에서 **프로비전 해제**를 선택합니다.

2 키 만들기 및 관리

항상된 BIOS 인증 모드를 사용하도록 설정하기 전에 MII에서 보안 프로비저닝을 완료합니다. 키를 만들고 내보내려면 항상된 BIOS 인증 모드를 사용하도록 설정해야 합니다. BIOS 인증 모드를 사용하도록 설정하는 방법은 다음과 같습니다.

▲ 키를 만들고 내보내려면 HP Sure Admin 플러그인을 열고 **항상된 BIOS 인증 모드**를 선택합니다.

키 만들기 및 내보내기

로컬 액세스 키 쌍을 만들고 HP Sure Admin 휴대폰 앱에서 키에 액세스하도록 설정하려면 세 가지 방법 중에서 하나를 사용할 수 있습니다.

- [2페이지의수동 배포로 키 만들기 및 내보내기](#)
- [3페이지의Azure AD 해지로 키를 만들고 내보내는 방법](#)
- [3페이지의키를 만들고 Azure AD 그룹 OneDrive에 전송](#)

수동 배포로 키 만들기 및 내보내기

로컬 액세스 인증 키를 내보내고 이메일이나 다른 방법을 통해 HP Sure Admin 휴대폰 앱에 수동으로 배포하려면 이 옵션을 사용합니다.

 **참고:** 이 옵션을 선택할 경우 일회성 PIN을 얻는 데 HP Sure Admin 휴대폰 앱 네트워크 액세스 권한이 필요하지 않습니다.

1. **키 이름** 입력란에 키의 이름을 지정합니다.
2. **암호** 입력란에 암호를 입력합니다.

 **참고:** 암호는 내보낸 키를 보호하는 데 사용되며 암호를 제공해야만 HP Sure Admin 휴대폰 앱 사용자가 키를 가져올 수 있습니다.

3. **찾아보기**를 선택하고 시스템에서 경로를 내보낼 위치를 선택합니다.
4. **키 만들기**를 선택합니다. **키 만들기** 버튼 옆의 알림 아이콘에 **키를 만들었습니다** 메시지가 표시되면 키가 만들어진 것입니다.
5. **다음**을 선택합니다. 요약 페이지에 입력한 HP Sure Admin 설정이 표시됩니다.
6. **정책 저장**을 선택합니다. **저장 완료** 메시지가 표시되면 정책이 저장된 것입니다.
7. 키를 저장한 폴더로 이동하고 해당 장치에서 사용자가 사용할 수 있는 이메일 등의 방법을 사용하여 HP Sure Admin 휴대폰 앱 사용자에게 키를 배포합니다. 키를 가져오려면 이 사용자도 암호가 필요합니다. 키와 암호에 서로 다른 배포 메커니즘을 사용하는 것이 좋습니다.

 **참고:** QR 코드를 전송할 때는 원래 크기로 전송합니다. 이미지 크기가 800 × 600보다 작으면 앱에서 이미지를 올바르게 읽을 수 없습니다.

Azure AD 해지로 키를 만들고 내보내는 방법

로컬 액세스 키를 지정된 Azure Active Directory 그룹에 연결하고 HP Sure Admin 휴대폰 앱에서 Azure Active Directory에 대한 사용자 인증과 로컬 액세스 PIN을 제공하기 전에 사용자가 지정된 그룹의 구성원인지 확인하도록 요구하려면 이 옵션을 사용합니다. 이 방법을 사용하려면 이메일이나 다른 방법을 통해 휴대폰 앱에 로컬 액세스 인증 키를 수동으로 배포해야 합니다.

 **참고:** 이 옵션을 선택할 경우 일회성 PIN을 얻기 위해 HP Sure Admin 휴대폰 앱 네트워크 액세스 권한이 필요합니다.

1. 키 이름 입력란에 키의 이름을 지정합니다.
2. 암호 입력란에 암호를 입력합니다.

 **참고:** 암호는 내보낸 키를 보호하는 데 사용되며 암호를 제공해야만 HP Sure Admin 휴대폰 앱 사용자가 키를 가져올 수 있습니다.

3. Azure AD 로그인을 선택하고 로그인합니다.
4. Azure AD 그룹 이름 드롭다운 상자에서 그룹 이름을 선택합니다. 키에 액세스하려면 그룹의 구성원이어야 합니다.
5. 찾아보기를 선택하고 시스템에서 경로를 내보낼 위치를 선택합니다.
6. 키 만들기를 선택합니다. 키 만들기 버튼 옆의 알림 아이콘에 키를 만들었습니다 메시지가 표시되면 키가 만들어진 것입니다.
7. 다음을 선택합니다. 요약 페이지에 입력한 HP Sure Admin 설정이 표시됩니다.
8. 정책 저장을 선택합니다. 저장 완료 메시지가 표시되면 정책이 저장된 것입니다.
9. 키를 저장한 폴더로 이동하고 해당 장치에서 사용자가 사용할 수 있는 이메일 등의 방법을 사용하여 HP Sure Admin 휴대폰 앱 사용자에게 키를 배포합니다. 키를 가져오려면 이 사용자도 암호가 필요합니다. 키와 암호에 서로 다른 배포 메커니즘을 사용하는 것이 좋습니다.

 **참고:** QR 코드를 전송할 때는 원래 크기로 전송합니다. 이미지 크기가 800 × 600보다 작으면 앱에서 이미지를 올바르게 읽을 수 없습니다.

키를 만들고 Azure AD 그룹 OneDrive에 전송

(권장) 휴대폰에 로컬 액세스 인증 키를 저장하지 않으려면 이 옵션을 사용합니다. 이 옵션을 선택하는 경우 MİK에서는 권한이 있는 그룹만 액세스할 수 있는 지정된 OneDrive 폴더에 로컬 액세스 인증 키를 저장합니다. PIN이 필요할 때마다 HP Sure Admin 사용자가 Azure AD에 인증해야 합니다.

1. 키 이름 입력란에 키의 이름을 지정합니다.
2. 암호 입력란에 암호를 입력합니다.
3. Azure AD 로그인을 선택하고 로그인합니다.
4. AZURE AD 그룹 이름 드롭다운 상자에서 그룹 이름을 선택합니다.

 **참고:** 키에 액세스하려면 그룹의 구성원이어야 합니다.

5. OneDrive 입력란에서 키를 저장한 OneDrive 폴더의 이름을 입력합니다.

6. **찾아보기**를 선택하고 시스템에서 경로를 내보낼 위치를 선택합니다.

7. **키 만들기**를 선택합니다.

 **참고:** 키가 지정된 OneDrive 폴더에 추가되고 지정된 로컬 폴더로 내보내지면 **키 만들기** 버튼 옆의 알림 아이콘에 **키를 만들었습니다** 메시지가 표시됩니다.

8. **다음**을 선택합니다. 요약 페이지에 입력한 HP Sure Admin 설정이 표시됩니다.

9. **정책 저장**을 선택합니다. **저장 완료** 메시지가 표시되면 정책이 저장된 것입니다.

 **참고:** 이 시나리오에서는 사전 프로비저닝하기 위해 HP Sure Admin 휴대폰 앱에 아무것도 보내지 않아도 됩니다. 대상 PC는 QR 코드에 포함된 OneDrive 위치를 가리키도록 프로비저닝되어 있습니다. 사용자가 권한이 있는 그룹에 속해 있고 성공적으로 인증되는 경우 HP Sure Admin 휴대폰 앱에서는 이 포인터를 사용하여 OneDrive 위치에 액세스합니다.

3 휴대폰 설정

Google Play 스토어 또는 Apple 스토어에서 HP Sure Admin 휴대폰 앱을 다운로드합니다.

- Android 휴대폰은 Google 스토어에서 HP Sure Admin을 다운로드합니다.
- iOS 휴대폰은 Apple 스토어에서 HP Sure Admin을 다운로드합니다.

HP Sure Admin 휴대폰 앱을 사용하여 BIOS 잠금 해제

HP Sure Admin 모바일 앱에서는 BIOS 암호를 사용하는 대신 대상 시스템에서 제시한 QR 코드를 스캔하여 얻은 일회성 PIN을 제공하여 BIOS 설정에 로컬로 액세스할 수 있습니다.

다음 단계에 따라 휴대폰 앱 사용자에게 키가 전송되는 시나리오에서 키를 휴대폰에 로컬로 저장하는 방법을 확인하십시오. 다음 예시에서 키는 HP Sure Admin 휴대폰 앱 사용자에게 이메일로 전송되며, 사용자는 휴대폰에서 이메일을 열게 됩니다.

1. 키가 포함된 이메일을 엽니다.
2. 등록 페이지가 표시되면 **암호 입력** 입력란에 암호를 입력하고 **이메일 주소 입력** 입력란에 이메일 주소를 입력하여 키의 암호를 해독한 다음 HP Sure Admin 응용프로그램에 추가합니다. 잠금 해제 PIN 번호는 PIN 페이지에 표시되어 있습니다.

 **참고:** 이 단계에서는 키를 모바일 장치에 저장하고 등록을 완료합니다. 이제 이 키를 통해 액세스할 수 있도록 프로비저닝된 모든 장치에 HP Sure Admin 휴대폰 앱을 사용하여 액세스할 수 있습니다. 이메일 주소는 관리자가 요구하는 경우에만 필요합니다.

3. **BIOS 응답 코드 입력** 입력란에 PIN을 입력합니다.

등록 후 BIOS 설정에 대한 액세스 권한 가져오기

등록 후 대상 컴퓨터에서 BIOS 설정에 액세스하는 방법은 다음과 같습니다.

1. 대상 컴퓨터에서 부팅 시 BIOS 설정을 시작합니다.
2. 휴대폰 응용 프로그램에서 **QR 코드 스캔**을 선택하고 대상 컴퓨터에서 QR 코드를 스캔합니다.
3. 사용자 인증을 묻는 메시지가 표시되면 자격 증명을 제공합니다.
4. 잠금 해제된 PIN 번호는 PIN 페이지에 표시되어 있습니다.
5. 대상 컴퓨터의 **BIOS 응답 코드 입력** 입력란에 PIN을 입력합니다.

Azure AD 그룹 OneDrive로 BIOS 잠금 해제

Azure AD 그룹 OneDrive에서 HP Sure Admin을 사용하여 BIOS 잠금을 해제하는 방법은 다음과 같습니다.

1. **QR 코드 스캔**을 선택한 다음 BIOS QR 코드를 스캔합니다.

 **참고:** HP Sure Admin 앱에 Azure AD 로그인 페이지가 표시됩니다.

2. Azure 계정에 로그인합니다.
3. BIOS 응답 코드 입력 입력란에 PIN을 입력합니다.

 **참고:** 이 시나리오에서는 HP Sure Admin 앱에서 키를 로컬로 저장하지 않습니다. HP Sure Admin 휴대폰 앱에는 네트워크 액세스 권한이 있어야 하며, 사용자는 일회성 PIN이 필요할 때마다 인증해야 합니다.

4 HP Sure Admin 오류 코드

이 섹션의 표를 사용하여 HP Sure Admin 및 KMS Admin Console 오류 코드, 유형 및 설명을 확인하십시오.

표 4-1 HP Sure Admin 앱 오류 코드, 유형 및 설명

오류 코드	오류 유형	설명
100	QRCodeUnknownError	일반 오류입니다.
101	QRCodeDeserialization	QR 코드 JSON을 읽을 수 없습니다. 문자열이 올바른 JSON 파일에 포함되지 않았거나 데이터가 잘못되었습니다.
102	QRCodeInvalidImage	스캔한 QR 코드 이미지가 잘못되었습니다. QR 코드 이미지 파일을 읽을 수 없습니다.
103	QRCodeNoPayload	스캔한 QR 코드 이미지가 잘못되었습니다. 이미지 파일에 JSON 페이로드가 없습니다.
104	QRCodeInvalid	QR 코드 JSON을 읽을 수 없습니다. 문자열이 올바른 JSON이 아니거나 QR 이미지의 데이터가 잘못되었습니다.
105	QRCodeInvalidKeyIdHash	QR 코드 JSON의 공개 키 해시가 등록 패키지 공개 키 해시(KeyID 데이터)와 일치하지 않습니다.
106	QRCodeTampered	스캔한 QR 코드 이미지가 변조 및 잘못되었습니다.
107	QRCodeTamperedOrInvalidPassPhrase	스캔된 QR 코드 이미지가 변조 및 잘못되었거나 입력한 암호가 올바르지 않습니다.

표 4-2 OneDrive 오류, 유형 및 설명의 일회성 액세스 키

오류 코드	오류 유형	설명
200	OneTimeKeyError	일반 오류입니다.
201	OneTimeKeyNoUserGroups	로그인한 사용자가 조직의 AD 그룹에 속하지 않습니다.
203	OneTimeKeyInvalidUserGroup	로그인한 사용자가 이 키가 할당된 AD 그룹에 속하지 않습니다.
204	OneTimeKeyQRFileDoesNotExist	일회성 키 파일이 AD 그룹의 OneDrive 폴더에 없습니다.
205	OneTimeKeyInvalidQRFile	AD 그룹의 OneDrive 폴더에 있는 일회성 키 파일이 잘못되었습니다.
206	OneTimeKeyInvalidQRpayload	일회성 키 파일이 있지만 파일 페이로드를 읽을 수 없습니다.

표 4-3 Azure AD 인증 오류

오류 코드	오류 유형	설명
300	AzureADUnknownError	일반 오류입니다.
301	AzureADInvalidDomain	입력한 이메일 주소가 QR 코드 이미지에서 지정하는 도메인 이름과 일치하지 않습니다.
302	AzureADAccessToken	Azure AD에서 액세스 토큰을 가져오는 동안 오류가 발생했습니다. 사용자가 조직의 Azure AD에 로그인할 수 없거나, 앱에 조직의 Azure AD와 연결하는 데 필요한 권한이 없습니다. 또한 사용자가 인증을 취소한 것일 수도 있습니다.
303	AzureADUserProfile	조직의 Azure AD에서 사용자 프로필 정보를 가져오기 위해 HP Sure Admin 앱이 활성화되었습니다.
304	AzureADUserPrincipalMismatch	입력한 이메일 주소가 로그인한 사용자의 사용자 계정 이름과 일치하지 않습니다.
305	AzureADUserInvalidUserGroup	로그인한 사용자가 이 키가 할당된 할당 AD 그룹에 속하지 않습니다.

표 4-4 KMS Admin Console 오류, 유형 및 설명

오류 코드	오류 유형	설명
401	KmsUnauthorized	사용자에게 KMS 서비스를 사용할 권한이 없습니다.
402	KmsKeyDoesNotExist	일치하는 개인 키가 KMS 키 자격 증명에 존재하지 않습니다. 키가 현재 삭제되었으나 복구 가능한 상태이며 키의 이름은 이 상태에서 다시 사용할 수 없습니다. 키를 복구하거나 제거할 수만 있습니다.
403	KmsKeyDoesNotExistInTableStorage	키가 테이블 저장소에 존재하지 않습니다.
404	KmsUploadKeyErrorInKeyVault	키 자격 증명에 키를 추가하는 동안 오류가 발생했습니다.
405	KmsUploadKeyUnauthorized	사용자에게 키를 업로드할 권한이 없습니다. 사용자가 이 API를 호출할 수 있도록 허용된 권한이 있는 AD 그룹에 속하지 않습니다.
406	KmsInvalidAzureADLogin	사용자가 Azure Tenant AAD에 로그인하지 않았습니다.
407	KmsNoUserGroups	로그인한 사용자가 조직의 AD 그룹에 속하지 않습니다.
408	KmsInvalidUserGroup	로그인한 사용자가 이 키가 할당된 AD 그룹에 속하지 않습니다.
409	KmsInvalidAccessToken	요청에 따라 제공된 액세스 토큰이 잘못되었습니다.
410	KmsAccessTokenExpired	제공된 accessToken이 만료되었습니다.

표 4-4 KMS Admin Console 오류, 유형 및 설명 (계속)

오류 코드	오류 유형	설명
411	KmsAccessTokenInvalidTenantId	제공되는 accessToken에 잘못된 TenantId 값이 있습니다.
412	KmsAccessTokenTenantIdMismatch	제공된 accessToken의 TenantId가 함수 앱의 TenantId와 일치하지 않습니다.
413	KmsInvalidKeyId	keyId가 null이거나 비어 있습니다.
414	KmsDeleteKeyUnauthorized	사용자에게 키를 삭제할 권한이 없습니다. 사용자가 이 API를 호출할 수 있도록 허용된 권한이 있는 AD 그룹에 속하지 않습니다.
415	KmsKeyVaultSoftDeleteUnrecoverableState	비밀을 복구하려는 시도가 실패했으며, 복구할 수 없습니다. 사용자가 다시 시도해야 합니다.
416	KmsInvalidGetKeysRequest	Get Keys(키 가져오기) 요청이 잘못되었습니다.
417	KmsGetKeysUnauthorized	사용자에게 키를 가져올 권한이 없습니다. 사용자가 이 API를 호출할 수 있도록 허용된 권한이 있는 AD 그룹에 속하지 않습니다.
418	KmsInvalidRequestPayload	API에서 받은 요청이 잘못되었습니다.
419	KmsRequestRequired	받은 요청이 비어 있으면 안 됩니다.
420	KmsKeyNotConcurrent	사용자가 마지막으로 사본을 검색한 이후 테이블 저장소의 키가 업데이트되거나 수정되었습니다.