SOPHOS

Cybersecurity made simple.

Sophos Central Device Encryption

관리자 가이드

목차

1 Sophos Central Device Encryption 정보

Sophos Central Device Encryption을 사용하면 Sophos Central을 통해 Windows 엔드포인트의 BitLocker Drive Encryption 및 Mac 엔드포인트의 FileVault 암호화를 관리할 수 있습니다.

장치를 분실하거나 도난당한 경우에도 하드 디스크 데이터를 안전하게 보호합니다.

이 가이드는 Device Encryption을 설정하고 사용하는 방법을 설명합니다. 또한 Self Service Portal을 사용하여 복구 키를 검색하는 방법도 설명합니다. Sophos Central을 통해 정책 설정, 경고 및 복구에 대한 세부 정보를 보려면, Sophos Central 도움말을 참조하십시오.

관련 정보

Sophos Central 도움말

2 BitLocker Drive Encryption 관리

이 섹션에서는 네트워크의 Windows 엔드포인트에서 BitLocker Drive Encryption을 사용하기 위한 필수 조건, 사용 가능한 다양한 인증 모드, 독점적인 그룹 정책 설정과 상호 작용하는 방식을 설명합니다.

2.1 Sophos Central Device Encryption으로 마이그레이션

BitLocker Drive Encryption 또는 Sophos Full Disk Encryption과 함께 SafeGuard Enterprise를 이미 사용하고 있는 경우, 이 섹션에서는 Sophos Central Device Encryption을 마이그레이션하는 방법에 대해 설명합니다.

다루는 내용은 다음과 같습니다.

- SafeGuard Enterprise 및 BitLocker
- SafeGuard Enterprise 및 Sophos Full Disk Encryption
- Mac 엔드포인트 마이그레이션에 대한 자세한 내용은 Sophos Central Device Encryption(Mac)으로의 마이그레이션을 참조하십시오.

관련 작업

Sophos Central Device Encryption으로 마이그레이션(Mac) (페이지 13)
Sophos Central을 사용하여 이미 FileVault로 암호화된 Mac 엔드포인트를 관리하려면 Sophos Central Device Encryption 정책을 이 엔드포인트에 적용해야 합니다.

2.1.1 SafeGuard Enterprise BitLocker에서 마이그레이션

마이그레이션하려면 다음 단계를 따르십시오.

> 참고
> SafeGuard Enterprise 버전 6.x 또는 7.x와(과) 함께 BitLocker를 사용할 경우 먼저 최신 버전의 SafeGuard Enterprise로 업그레이드하는 것이 좋습니다.
>
> SafeGuard Enterprise 버전 6.x 또는 7.x을(를) 사용할 경우 SafeGuard Enterprise 관리자 도움말의 단계에 따라 시스템 디스크의 암호를 해독해야만 Sophos Central Device Encryption으로 마이그레이션할 수 있습니다.

SafeGuard Enterprise BitLocker 클라이언트(버전 8.0 이상)에서 Sophos Central Device Encryption으로 마이그레이션하려면:

1. 제어판 > 프로그램 제거로 이동하고 Sophos SafeGuard 클라이언트를 마우스 오른쪽 단추로 클릭합니다.
2. 오른쪽 클릭 메뉴에서 변경을 선택합니다.
   Sophos SafeGuard 클라이언트 설치 마법사가 열립니다.
3. BitLocker 구성 요소를 제거합니다.

참고
BitLocker 구성 요소를 제거해도 볼륨이나 파일의 암호가 해독되지 않습니다.

4. Sophos Central Device Encryption 소프트웨어를 설치합니다.
5. Sophos Central Device Encryption 정책이 엔드포인트에 할당되고 활성화되었는지 확인합니다.

이제 Sophos Central을 사용해 BitLocker를 관리할 수 있습니다. 다시 암호화할 필요가 없습니다. 엔드포인트에 Sophos Central Device Encryption 정책을 적용하고 나면 복구 키가 갱신되고 Sophos Central로 전송됩니다. 파일 암호화 기능은 변경되지 않은 상태로 남아 있습니다.

관련 정보
SafeGuard Enterprise 관리자 도움말

2.1.2 SafeGuard Enterprise 전체 디스크 암호화에서 마이그레이션

마이그레이션하려면 다음 단계를 따르십시오.

SafeGuard Enterprise 전체 디스크 암호화에서 마이그레이션하려면 다음과 같이 하십시오.

1. Sophos SafeGuard 클라이언트 소프트웨어를 제거합니다.
   암호화된 볼륨이 자동으로 암호 해독됩니다. 암호화된 파일은 암호화된 상태로 남아 있습니다.
2. Sophos Central Device Encryption 소프트웨어를 설치합니다.
3. Sophos Central Device Encryption 정책이 엔드포인트에 할당되고 사용하도록 설정되었는지 확인합니다.
4. 필요한 SafeGuard Enterprise File Encryption 모듈(Synchronized Encryption 또는 Location Based File Encryption)을 다시 설치합니다.

이제 Sophos Central을 사용해 BitLocker를 관리할 수 있습니다. 엔드포인트에 Sophos Central Device Encryption 정책을 적용하고 나면 배경에서 암호화가 시작되고 복구 키가 갱신되고 Sophos Central로 전송됩니다.

2.2 Device Encryption 준비

기본적으로 BitLocker를 위해 대부분의 시스템 드라이버가 준비되어 있습니다. 그렇지 않을 경우, Sophos Central Device Encryption에서는 필수 Microsoft 명령줄 도구 BdeHdCfg.exe를 자동으로 실행하여 드라이브를 준비합니다.

이는 별도의 BitLocker 파티션이 시스템 드라이브에 생성됨을 의미합니다.

Sophos Central Device Encryption을 설정하는 동안, 시스템 드라이브를 준비하려면 재시작이 필요하다는 메시지가 사용자에게 표시됩니다. 사용자가 컴퓨터를 즉시 다시 시작하거나 작동을 연기하도록 선택할 수 있습니다. Device Encryption은 컴퓨터를 재시작하고 시스템 드라이브 준비가 성공적으로 완료되었을 때만 시작할 수 있습니다.

Device Encryption에서 요구하는 .NET Framework 버전이 자동으로 엔드포인트에 설치됩니다.

2.3 Device Encryption 단계

장치를 암호화하려면 다음 단계를 따르십시오.

시작 전 사용자 참고 사항:

- Sophos Central 에이전트 소프트웨어가 엔드포인트에 설치되어 있어야 합니다.
- Sophos Central에서 Device Encryption 정책을 구성하고 설정해야 합니다.
- 사용자는 대화형으로 엔드포인트에 로그인하고 이를 Sophos Central에 연결하고 동기화해야 합니다. 원격 로그온은 지원되지 않습니다.
- 운영 체제에서 BitLocker 드라이브 암호화를 지원해야 합니다. 자세한 내용은 Device Encryption 준비 및 Device Encryption 시스템 호환성을 참조하십시오.

이러한 지침에는 사용자에게 표시되는 내용 및 사용자가 수행해야 할 작업이 설명되어 있습니다.

1. TPM 보안 하드웨어가 아직 사용 설정되어 있지 않은 경우, 이를 사용 설정하기 위한 BIOS 작업이 시작됩니다. 이 경우 재시작이 필요합니다. 사용자는 즉시 재시작하거나 재시작을 미룰 수 있습니다.
   재시작을 하는 동안 사용자에게는 TPM을 사용 설정하라는 메시지가 표시됩니다. TPM을 사용 설정할 수 없거나 사용자가 반응하지 않을 경우, 메시지가 표시됩니다.
2. TPM이 활성 상태이고 사용 설정되었으나 소유 상태가 아닌 경우, Sophos Central 에이전트 소프트웨어에서는 TPM 소유자 정보를 자동으로 생성하고 설정합니다. 이 작업이 실패할 경우 Sophos Central에 경고가 전송됩니다.
3. TPM 인증 키가 누락된 경우, Sophos Central 에이전트 소프트웨어에서 이를 자동으로 생성합니다. 이 작업이 실패할 경우 Sophos Central에 경고가 전송됩니다.
4. Device Encryption 정책에 시작 인증 필요가 규정되어 있지 않다면 하드 디스크의 암호화가 자동으로 시작됩니다. 여기서 사용자가 수행해야 할 작업은 없습니다. 8단계를 건너뛸 수 있습니다.
5. Device Encryption 정책에 시작 인증 필요가 규정되어 있다면 사용자에게 Sophos Device Encryption 대화 상자가 표시됩니다.
   - Device Encryption 정책에 따라 인증을 위해 PIN 또는 암호가 필요한 경우, 화면의 지시 사항에 따라 PIN 또는 암호를 정의하십시오. TPM+PIN이 사용될 경우 시스템 디스크의 암호화 키는 TPM에 저장됩니다.

     참고
     사용자는 암호를 설정할 때 주의해야 합니다. 사전 부팅 환경에서만 미국-영어 키보드 레이아웃을 지원합니다. 지금 특수 문자와 함께 PIN 또는 암호를 설정할 경우, 나중에 로그온하기 위해 입력할 때 다른 키를 사용해야 할 수 있습니다.

   - Device Encryption 정책에 따라 인증을 위해 USB 키가 필요한 경우, 사용자는 USB 플래시 드라이브를 해당 컴퓨터에 연결해야 합니다. USB 플래시 드라이브는 NTFS, FAT 또는 FAT32로 포맷해야 합니다.
6. 사용자가 다시 시작 및 암호화를 클릭하면 컴퓨터가 다시 시작되고 Device Encryption가 작동하는지 확인됩니다.
   사용자는 나중에 하기를 선택하여 대화 상자를 닫을 수 있습니다. 그러나 사용자가 다음에 로그온하거나 Device Encryption 정책을 변경할 경우 이 대화 상자가 다시 표시됩니다.
7. 사용자가 올바른 PIN/암호를 입력할 수 없는 경우 Esc 키를 누를 수 있습니다. 암호화가 아직 적용되지 않았으므로 시스템이 정상적으로 부팅됩니다. 사용자에게 로그온 후 PIN/암호를 다시 입력하도록 시도할 것인지 묻는 메시지가 표시됩니다.
8. 어떤 사용자가 암호화를 사용 설정하지 않았는지 볼 수 있습니다. 이는 해당 사용자가 아직 컴퓨터를 다시 시작하지 않았거나 화면상 지침을 아직 완료하지 않았음을 의미합니다. Sophos Central에서 보고서를 찾아봅니다.
9. 사전 부팅 테스트가 성공적으로 완료된 경우, Sophos Central 에이전트 소프트웨어는 고정 디스크의 암호화를 시작합니다. 암호화는 백그라운드에서 이루어지므로, 사용자는 평소와 마찬가지로 컴퓨터로 작업을 수행할 수 있습니다.
   하드웨어 테스트가 실패할 경우 시스템이 재부팅되고 암호화가 시행되지 않습니다. 사용자에게 알림을 전달하기 위한 이벤트가 Sophos Central에 전송됩니다.

10. Sophos Central 에이전트가 시스템 볼륨을 암호화하고 나면 데이터 볼륨의 암호화가 시작됩니다(정책에 지정된 경우). 이러한 볼륨에 대한 보호는 시스템 볼륨에 저장되므로, 데이터 볼륨은 시작 후 자동으로 사용 가능합니다. 이는 사용자가 자신의 컴퓨터에 로그온할 경우, 추가 사용자 작업 없이 데이터 볼륨에 액세스할 수 있음을 의미합니다. 예를 들어 USB 플래시 드라이브 같은 이동식 데이터 볼륨은 암호화되지 않습니다.

엔드포인트의 %ProgramData%₩Sophos₩Sophos Data Protection₩Logs에서 2개의 로그 파일, CDE.log와 CDE_trace.xml을 찾을 수 있습니다.

관련 개념

Device Encryption 준비 (페이지 3)
기본적으로 BitLocker를 위해 대부분의 시스템 드라이버가 준비되어 있습니다. 그렇지 않을 경우, Sophos Central Device Encryption에서는 필수 Microsoft 명령줄 도구 BdeHdCfg.exe를 자동으로 실행하여 드라이브를 준비합니다.

Device Encryption 시스템 호환성 (페이지 5)
아래 표에는 해당 플랫폼에서 지원되는 보호 유형의 개요가 나와 있습니다. 적용되는 보호 유형은 사용된 Windows 유형 및 TPM 보안 하드웨어의 사용 가능 여부에 따라 달라집니다.

TPM+ PIN (페이지 7)
TPM+ PIN 모드에서는 컴퓨터의 TPM 보안 하드웨어 및 PIN을 인증으로 사용합니다.

2.4 Device Encryption 시스템 호환성

아래 표에는 해당 플랫폼에서 지원되는 보호 유형의 개요가 나와 있습니다. 적용되는 보호 유형은 사용된 Windows 유형 및 TPM 보안 하드웨어의 사용 가능 여부에 따라 달라집니다.

괄호 안의 숫자는 특정 보호 유형의 우선순위를 나타냅니다.

(*) 시작 인증 필요를 사용 설정한 경우, TPM 전용 보호 설치가 가능하지 않으므로 TPM+ PIN이 첫 번째 우선순위가 됩니다.

	Win 7 TPM 없음	Win 7 TPM 있음	Win 8.1 TPM 없음	Win 8.1 TPM 있음	Win 10 TPM 없음	Win 10 TPM 있음
TPM 전용	-	가능(1*)	-	가능(1*)	-	가능(1*)
TPM+ PIN	-	가능(2*)	-	가능(2*)	-	가능(2*)
암호	-	-	가능(1*)	가능(3*)	가능(1*)	가능(3*)
USB 키	가능(1*)	가능(3*)	-	-	-	-

Central Device Encryption을 사용하는 경우 엔드포인트 컴퓨터에서 TPM을 구성해야 할 수 있습니다.

TPM 2.0 이상을 사용하는 경우 하드 드라이브를 GPT로 포맷해야 하며 BIOS가 UEFI 모드여야 합니다.

TPM 1.2를 사용하는 경우 BIOS/UEFI에서 TPM을 활성화해야 하며 사용할 준비가 되어 있어야 합니다. TPM.MSC를 사용하여 이를 확인할 수 있습니다.

Central Device Encryption을 설치하기 전에 엔드포인트 컴퓨터를 최신 BIOS/UEFI 버전으로 업데이트하는 것이 좋습니다.

Windows FIPS 모드가 사용 설정된 경우, BitLocker 암호화는 Windows 8.1 또는 Windows 10 시스템에서만 지원됩니다. Windows 7에서 FIPS 모드의 BitLocker에 대한 자세한 내용은 FIPS 규격

복구 암호는 Windows 7 또는 Windows Server 2008 R2에서 BitLocker용 AD DS에 저장할 수 없음을 참조하십시오.

Sophos Central Device Encryption으로 하드 드라이브를 암호화할 수 있습니다. 자세한 내용은 암호화된 하드 드라이브를 참조하십시오.

Central Device Encryption은 프로비저닝된 BitLocker를 지원합니다.

관련 정보

FIPS 규격 복구 암호는 Windows 7 또는 Windows Server 2008 R2에서 BitLocker용 AD DS에 저장할 수 없음

암호화된 하드 드라이브

2.5 Device Encryption 인증 모드

Device Encryption 설정에서 시작 인증 필요 스위치를 사용하여 사용자가 컴퓨터에 로그온할 때 인증이 필요한지 여부를 제어할 수 있습니다.

컴퓨터에 설치되는 인증 모드는 시스템, BitLocker 그룹 정책 설정 및 구성된 Device Encryption 정책에 따라 달라집니다. Device Encryption 시스템 호환성에 따라, 엔드포인트에 다음 인증 모드 중 하나가 설치됩니다.

- TPM+ PIN
- 암호
- TPM 전용
- USB 키

BitLocker로 이미 암호화된 엔드포인트에서는 필요한 단계에 대한 메시지가 사용자에게 전달됩니다.

시작 인증 필요를 설정하면 사용자에게 PIN/패스프레이즈/USB 키를 정의하고 적용을 클릭하라는 메시지가 나타납니다. 사용자는 이후에 컴퓨터를 시작할 때마다 이 PIN/패스프레이즈/USB 키를 사용해야 합니다. 시작 인증 필요를 해제하면 TPM 전용 모드가 자동으로 적용되고 추가 인증이 필요하지 않습니다. 사용자가 컴퓨터를 시작하면 해당 컴퓨터가 장치 잠금을 자동으로 해제했다는 알림이 표시됩니다.

Sophos Device Encryption은 해당 설정이 구성되지 않음으로 설정되어 있는 경우 모든 인증 모드가 허용되도록 그룹 정책 개체(GPO)를 자동으로 구성할 수 있습니다. 설정을 수동으로 구성할 경우, 이러한 정의가 덮어쓰기 되지 않습니다. 자세한 내용은 BitLocker 그룹 정책 설정을 참조하십시오.

사용자는 인증 모드의 설치를 연기할지 여부를 결정할 수 있습니다. 이 경우, 암호화가 이루어지지 않습니다. 사용자가 Windows에 다시 로그온할 때마다 또는 관리자가 새 암호화 정책을 배포할 경우, 컴퓨터를 재시작한다는 메시지가 사용자에게 표시됩니다. 재시작 후, 인증 모드가 설치되고 Device Encryption이 시작됩니다. 이후에는 사용자가 장치의 암호화를 해제할 수 없습니다.

관련 개념

Device Encryption 시스템 호환성 (페이지 5)
아래 표에는 해당 플랫폼에서 지원되는 보호 유형의 개요가 나와 있습니다. 적용되는 보호 유형은 사용된 Windows 유형 및 TPM 보안 하드웨어의 사용 가능 여부에 따라 달라집니다.

BitLocker 그룹 정책 설정 (페이지 8)
Sophos Central에서는 일부 그룹 정책 설정을 자동으로 정의하므로, 관리자는 장치 암호화를 위해 컴퓨터를 준비해야 할 필요가 없습니다.

2.5.1 TPM+ PIN

TPM+ PIN 모드에서는 컴퓨터의 TPM 보안 하드웨어 및 PIN을 인증으로 사용합니다.

사용자는 컴퓨터를 시작할 때마다 Windows 사전 부팅 환경에서 이 PIN을 입력해야 합니다.

TPM+ PIN을 사용하려면 준비된 TPM이 있어야 하며 시스템의 GPO 설정에서 TPM+ PIN 모드를 허용해야 합니다.

모든 조건을 충족하면 TPM+ PIN 설정 대화 상자가 표시되고 사용자에게 PIN을 정의하라는 메시지가 표시됩니다. 사용자는 재시작 및 암호화를 클릭하여 컴퓨터를 즉시 재부팅하고 암호화를 시작할 수 있습니다.

GPO 설정 시작 시 고급 PIN 허용이 사용 설정된 경우 PIN에는 숫자, 문자, 특수 문자가 포함될 수 있습니다. 그렇지 않을 경우, 숫자만 허용됩니다.

BitLocker용 PIN의 길이는 4~20자입니다. 그룹 정책을 통해 더 높은 최소 길이를 정의할 수 있습니다. Sophos Central 에이전트 소프트웨어는 강화된 PIN을 허용하도록 그룹 정책을 설정합니다. 대화 상자에는 사용자가 입력할 수 있는 문자의 종류 및 허용되는 최소/최대 길이가 표시됩니다.

참고
특정 Windows 컴퓨터의 모든 사용자는 동일한 PIN을 사용해 시스템 디스크를 잠금 해제해야 합니다. 그 이후에 개별 자격 증명으로 운영 체제에 로그온합니다. Windows 컴퓨터에는 단일 로그온이 지원되지 않습니다.

2.5.2 패스프레이즈

TPM 보안 하드웨어 없이 엔드포인트에서 인증을 수행하려는 경우 패스프레이즈를 사용할 수 있습니다.

사용자는 컴퓨터를 시작할 때마다 Windows 사전 부팅 환경에서 이 패스프레이즈를 입력해야 합니다.

패스프레이즈 보호를 사용하려면 Windows 8.0 이상이 필요하며 시스템의 GPO 설정에서 패스프레이즈 모드를 허용해야 합니다.

모든 조건을 충족하면 암호 설정 대화 상자가 표시되고 사용자에게 8~100자 길이의 암호를 정의하라는 메시지가 표시됩니다. 사용자는 재시작 및 암호화를 클릭하여 컴퓨터를 즉시 재부팅하고 암호화를 시작할 수 있습니다.

2.5.3 TPM 전용

TPM 전용 모드에서는 PIN 인증 없이 컴퓨터의 TPM 보안 하드웨어를 사용합니다.

이는 사용자가 Windows 사전 부팅 환경에서 PIN을 입력하라는 메시지 없이 컴퓨터를 시작할 수 있음을 의미합니다.

TPM 전용 모드를 사용하려면 준비된 TPM이 필요하며 Device Encryption 정책 설정 시작 인증 필요를 사용 해제해야 합니다. 또한, 시스템의 GPO 설정에서 TPM 전용 모드 보호를 허용해야 합니다.

모든 조건이 충족되면 TPM 전용 보호 설치 대화 상자가 표시됩니다. 사용자는 재시작 및 암호화를 클릭하여 컴퓨터를 즉시 재부팅하고 암호화를 시작할 수 있습니다.

2.5.4 USB 키

USB 키 모드에서는 인증을 위해 USB 플래시 드라이브에 저장된 키를 사용합니다.

시작할 때마다 USB 플래시 드라이브를 컴퓨터에 연결해야 합니다.

사용 가능한 TPM이 없거나 GPO를 통해 TPM이 사용 해제된 경우 USB 키 보호 모드는 Windows 7 엔드포인트에서 사용됩니다.

USB 플래시 드라이브는 NTFS, FAT 또는 FAT32로 포맷해야 합니다. exFAT 포맷은 지원되지 않습니다. 또한, USB 플래시 드라이브는 쓰기 가능해야 합니다.

모든 조건을 충복하면 USB 키 보호 설치 대화 상자가 표시되며, 사용자가 키를 저장하는 데 사용할 연결된 USB 플래시 드라이브를 선택해야 합니다.

사용자는 재시작 및 암호화를 클릭하여 컴퓨터를 즉시 재부팅하고 암호화를 시작할 수 있습니다.

2.6 BitLocker 그룹 정책 설정

Sophos Central에서는 일부 그룹 정책 설정을 자동으로 정의하므로, 관리자는 장치 암호화를 위해 컴퓨터를 준비해야 할 필요가 없습니다.

관리자가 설정을 이미 정의한 경우, 구성된 값이 덮어쓰기되지 않습니다.

로컬 그룹 정책 편집기의 컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > BitLocker 드라이브 암호화 > 운영 체제 드라이브 아래에서 다음 정책을 찾을 수 있습니다.

정책	설정	Sophos Central에 의해 설정된 값	주석
시작 시 네트워크 잠금 해제 허용		사용함	미리 구성된 BitLocker 네트워크 잠금 해제를 허용하여 Central Device Encryption을 활성화한 후 작동을 유지할 수 있습니다.
시작 시 추가 인증 요구	호환 TPM이 없는 BitLocker 허용	선택 표시됨	이는 사용 가능한 TPM이 없을 경우 Windows 8에 설정되는 값이며, 시작 시 암호를 사용하여 시스템 디스크의 잠금을 해제할 수 있습니다.
시작 시 추가 인증 요구	TPM 시작 PIN 구성	TPM과 함께 시작 PIN 허용	Device Encryption 정책 설정 시작 인증 필요가 설정되고 시스템에 TPM이 있는 경우, 이 그룹 정책 설정은 TPM에 의한 시스템 드라이브 보호를 허용하며 사용자에게도 PIN을 요청합니다.
시작 시 향상된 PIN 허용	해당 없음	사용함	이는 영숫자 PIN을 사용하여 TPM으로 시스템 드라이브를 보호할 수 있도록 설정된 값입니다. 이 값을 설정할 수 없는 경우, 숫자만 허용됩니다.

정책	설정	Sophos Central에 의해 설정된 값	주석
사전 부팅 복구 메시지 및 URL 구성	사전 부팅 복구 메시지에 대한 옵션 선택	기본 복구 메시지 및 URL 사용	이는 Sophos 기본 메시지 및 URL을 사용하도록 설정되었습니다.
사전 부팅 복구 메시지 및 URL 구성	사용자 지정 복구 메시지 옵션	복구 키가 없습니까? IT 헬프 데스크에 문의하거나 셀프 서비스 포털로 이동하십시오. https://sophos.com/ssp	
사전 부팅 복구 메시지 및 URL 구성	사용자 지정 복구 메시지 옵션		
고정 데이터 드라이브에 대한 하드웨어 기반 암호화 사용 구성	해당 없음	사용 안 함	이는 소프트웨어 기반 암호화를 적용하도록 설정되었습니다. 기존 BitLocker 그룹 정책 설정에 하드웨어 기반 암호화가 필요한 경우, 해당 정책 설정은 재정의되지 않습니다.
운영 체제 드라이브에 대한 하드웨어 기반 암호화 사용 구성	해당 없음	사용 안 함	이는 소프트웨어 기반 암호화를 적용하도록 설정되었습니다. 기존 BitLocker 그룹 정책 설정에 하드웨어 기반 암호화가 필요한 경우, 해당 정책 설정은 재정의되지 않습니다.

- 사용되는 암호화 알고리즘: 기본적으로 Sophos Central Device Encryption은 AES-256을 사용합니다. AES-128을 선택하는 데 사용할 수 있는 그룹 정책 설정이 있습니다.
- PIN/암호 요구 사항: 최소 PIN/암호 길이를 설정하고 복잡한 암호를 요구하는 데 사용할 수 있는 그룹 정책 설정이 있습니다.
- 모든 데이터 암호화 또는 사용된 공간만 해당: 부팅 볼륨 및/또는 데이터 볼륨에 대한 그룹 정책이 전체 데이터 암호화를 요구하도록 설정되어 있는 경우 사용 중인 공간의 암호화만 허용하는 Sophos Central 정책이 재정의됩니다.

일부 그룹 정책 설정은 Sophos Central과 충돌할 수 있으며 이 경우 암호화를 사용 설정할 수 없습니다. 이 경우, 이벤트가 Sophos Central에 전송됩니다.

- 스마트 카드 필요: 그룹 정책이 BitLocker에 스마트 카드를 사용해야 할 경우, Sophos Central에서는 이를 지원하지 않으며 오류 이벤트가 생성됩니다.
- 모든 데이터 암호화 또는 사용된 공간만 해당: 부팅 볼륨 및/또는 데이터 볼륨의 그룹 정책이 사용된 공간만 암호화하도록 설정되었으나 Sophos Central 정책에서는 전체 암호화가 필요한 경우, 오류 이벤트가 생성됩니다.

태블릿 장치(예: MS Surface Pro)를 암호화하려 하고 시작 인증을 사용할 경우 다음 그룹 정책 설정을 사용할 수 있도록 설정해야 합니다.

슬레이트에서 사전 부팅 키보드 입력이 필요한 BitLocker 인증 사용

자세한 내용은 기술 문서 자료 125772를 참조하십시오.

BitLocker 및 TPM 그룹 정책 설정에 대한 보다 일반적인 내용은 BitLocker 그룹 정책 설정 및 신뢰할 수 있는 플랫폼 모듈 서비스 그룹 정책 설정을 참조하십시오.

관련 개념

암호화 방법 및 보고 (페이지 10)
소프트웨어 기반 또는 하드웨어 기반 암호화로 볼륨을 암호화할 수 있습니다.

관련 정보

BitLocker 그룹 정책 설정
TPM 그룹 정책 설정
기술 문서 자료 125772

2.7 제한 사항

동적 디스크

BitLocker에서는 동적 디스크를 지원하지 않습니다. 끝점이 암호화에 실패했음을 알리기 위해 Sophos Central에 이벤트를 보냅니다. 동적 디스크의 시스템 볼륨은 암호화할 수 없기 때문입니다. 동적 디스크의 데이터 볼륨은 무시됩니다.

원격 데스크톱

Sophos Central 에이전트 소프트웨어가 설치된 원격 데스크톱을 통해 Windows 끝점을 사용하면 대화 상자가 표시되지 않으며, 암호화 정책이 배포될 경우 장치 암호화가 적용되지 않습니다. 암호화를 사용하도록 설정하면 결과적으로 재부팅 시퀀스가 하드웨어의 호환성을 확인합니다. 사용자는 사전 부팅 환경에서 PIN/패스프레이즈를 입력할 수 있어야 하며, 이는 원격 데스크톱을 통해 수행할 수 없습니다.

2.8 암호화 방법 및 보고

소프트웨어 기반 또는 하드웨어 기반 암호화로 볼륨을 암호화할 수 있습니다.

드라이브가 하드웨어 기반 암호화를 지원하는 경우에도, 장치 암호화는 새 볼륨에 대해 항상 소프트웨어 기반 암호화를 사용합니다.

드라이브가 하드웨어 기반 암호화로 이미 암호화되어 있는 경우, 이것은 변경되지 않습니다.

BitLocker 그룹 정책 설정에 하드웨어 기반 암호화가 필요한 경우, 이는 변경되지 않습니다.

컴퓨터페이지에서, 암호화 방법 또는 암호화되지 않은 컴퓨터와 같은 암호화 상태에 따라 컴퓨터를 필터링할 수 있습니다.

컴퓨터의 세부 정보 페이지에는 볼륨에 사용된 암호화 방법 및 알고리즘이 표시됩니다.

Windows 컴퓨터의 경우 다음 이후 암호화됨도 볼 수 있습니다. 표시되는 정보는 장치에 따라 다릅니다.

- Sophos Central Device Encryption으로 이미 암호화된 컴퓨터의 경우, 컴퓨터가 Sophos Central Device Encryption 버전 2.1로 업그레이드된 날짜와 시간이 표시됩니다.
- 다른 암호화 제품을 사용하여 암호화된 컴퓨터의 경우 Sophos Central Device Encryption이 설치된 날짜와 시간이 표시됩니다.
- Sophos Central Encryption 2.1 이상으로 암호화된 새 컴퓨터의 경우 암호화 날짜와 시간이 표시됩니다.

암호화 상태 보고서에는 컴퓨터의 암호화 상태가 표시됩니다.

어떤 컴퓨터가 암호화되는지, 어떤 볼륨 유형이 암호화되는지, 어떤 컴퓨터가 암호화 정책을 준수하는지 확인할 수 있습니다. 또한 컴퓨터가 인증하는 방법과 암호화 방식을 확인할 수도 있습니다.

관련 개념

BitLocker 그룹 정책 설정 (페이지 8)
Sophos Central에서는 일부 그룹 정책 설정을 자동으로 정의하므로, 관리자는 장치 암호화를 위해 컴퓨터를 준비해야 할 필요가 없습니다.

컴퓨터
컴퓨터 요약

2.9 암호 해독 정보

보통 암호 해독은 필요하지 않습니다. 암호화된 끝점을 암호화에서 제외해야 하는 경우 정책에서 모든 사용자를 제거한 후 암호화를 해제하면 됩니다.

끝점의 Windows Explorer에서 시스템 디스크를 마우스 오른쪽 단추로 클릭하고 BitLocker 관리를 선택합니다. BitLocker 드라이브 암호화 대화 상자에서 BitLocker 끄기를 클릭합니다. Windows 관리자만 이 작업을 수행할 수 있습니다.

사용자에게 암호화 정책이 적용된 경우 관리 권한을 가진 사용자가 수동으로 하드 디스크의 암호를 해독하려 시도하면 Sophos Central에서 사용자의 명령을 재정의하고 디스크가 암호화된 상태로 남아 있게 됩니다.

2.10 Windows 엔드포인트 복구

사용자가 BitLocker PIN 또는 암호를 잊어버린 경우 두 가지 방법으로 사용자 컴퓨터에 대한 액세스 권한을 다시 얻을 수 있습니다.

- 사용자는 Sophos 셀프 서비스 포털로 이동할 수 있습니다. 셀프 서비스 포털을 통해 복구 키 검색을 참조하십시오. Windows 10 사용자는 BitLocker recovery 화면에서 지침을 받습니다.
- 해당 사용자가 자신의 컴퓨터에 액세스하도록 도울 수 있습니다. 이러한 지침에는 사용자에게 표시되는 내용 및 사용자가 수행해야 할 작업이 설명되어 있습니다. 다음과 같이 하십시오.

1. 컴퓨터를 다시 시작하고 BitLocker 로그온 화면에서 Esc 키를 누릅니다.
2. BitLocker 복구 화면에서 복구 키 ID를 찾습니다.
3. 관리자에게 연락해 복구 키 ID를 알려 줍니다.
   사용자에게 복구 키를 제공할 수 있습니다. 사용자 중 한 명의 키를 검색하는 방법에 대한 도움말은 Sophos Central 도움말을 참조하십시오.
4. 사용자는 복구 키를 입력한 다음, 화면에 나타나는 지시 사항에 따라 새 PIN 또는 암호를 생성합니다.

   Windows 7을 실행하는 컴퓨터에서는 아무 지침도 표시되지 않습니다. 해당 PIN/암호를 수동으로 재설정해야 합니다.

사용자가 자신의 컴퓨터에 다시 액세스할 수 있습니다. 일반적으로, 사용자가 부팅 볼륨에 액세스하자 마다 데이터 볼륨은 자동으로 잠금 해제됩니다. 그렇지 않은 경우, 부팅 볼륨과 같은 방법으로 Sophos Central에서 데이터 볼륨에 대한 복구 키를 얻을 수 있습니다.

관련 작업

셀프 서비스 포털을 통해 복구 키 가져오기 (페이지 20)
사용자가 컴퓨터에 로그온할 수 없으면(BitLocker PIN, macOS 암호 등을 잊어버림) Sophos 셀프 서비스 포털을 사용해 복구 키를 검색할 수 있습니다.

관련 정보

셀프 서비스 포털

Sophos Central 도움말

3 FileVault Encryption 관리

Mac용 Sophos Central Device Encryption은 Mac에서 FileVault 전체 디스크 암호화 기능을 관리합니다.

사용자는 macOS 로그인 암호만 있으면 데이터를 암호화하고 여기에 액세스할 수 있습니다.

3.1 Sophos Central Device Encryption으로 마이그레이션(Mac)

Sophos Central을 사용하여 이미 FileVault로 암호화된 Mac 엔드포인트를 관리하려면 Sophos Central Device Encryption 정책을 이 엔드포인트에 적용해야 합니다.

참고
SafeGuard Enterprise와 함께 FileVault를 사용할 경우 먼저 Sophos SafeGuard Device Encryption 소프트웨어를 제거해야 합니다.

시작 전 사용자 참고 사항:

- Sophos Central 에이전트 소프트웨어를 엔드포인트에 설치해야 합니다.
- Sophos Central에서 Device Encryption 정책을 구성하고 켜야 합니다.
- 사용자는 자신의 엔드포인트에 로그온해야 합니다. 사용자는 Sophos Central에 연결되어 동기화되어야 합니다. 원격 로그온은 지원되지 않습니다.

이러한 지침에는 사용자에게 표시되는 내용 및 사용자가 수행해야 할 작업이 설명되어 있습니다.

1. 사용자가 로그온하거나 사용자가 로그온되어 있는 상태에서 Sophos Central Device Encryption 정책을 적용하면 Device Encryption이 컴퓨터를 보호하도록 설정되었다는 알림이 사용자에게 표시됩니다.
2. Sophos Central Device Encryption을 활성화하려면 사용자가 로그인 암호를 입력하고 키 생성을 클릭해야 합니다.
   새 복구 키가 생성되고 복구 목적을 위해 중앙에 저장됩니다. 암호화되지 않은 다른 내부 디스크가 있을 경우 해당 디스크도 암호화됩니다. 이를 위해 별도의 디스크 암호가 필요하지 않습니다.
3. 디스크 암호로 이미 암호화된 내부 디스크가 있을 경우 사용자는 디스크 암호를 입력하고 계속을 클릭해야 합니다.
   디스크 암호가 이제 Sophos Central에 의해 관리됩니다. 디스크는 시작 중에 자동으로 잠금 해제됩니다.

엔드포인트가 이제 Sophos Central Device Encryption에 의해 관리됩니다.

3.2 Device Encryption 단계별 안내(Mac)

Mac을 암호화하려면 다음 단계를 따르십시오.

시작 전 사용자 참고 사항:

- Sophos Central 에이전트 소프트웨어를 엔드포인트에 설치해야 합니다.
- Sophos Central에서 Device Encryption 정책을 구성하고 켜야 합니다.

- 사용자는 자신의 엔드포인트에 로그온해야 합니다. 사용자는 Sophos Central에 연결되어 동기화되어야 합니다. 원격 로그온은 지원되지 않습니다.

이러한 지침에는 사용자에게 표시되는 내용 및 사용자가 수행해야 할 작업이 설명되어 있습니다.

1. Mac을 시작한 후 로그인 암호를 입력합니다.

   그러면 Sophos Device Encryption이 켜집니다.
2. 암호화를 클릭하여 시스템 디스크의 암호화를 시작하거나 연기를 클릭하여 프로세스를 나중에 시작합니다.

   사용자가 로그인 암호를 입력하고 암호화를 클릭하면 복구 키가 키체인에 로컬로 저장되고 Sophos Central에도 저장됩니다.

   엔드포인트의 모든 기존 사용자가 FileVault에 자동으로 추가됩니다.

   macOS 10.12 이하를 실행하는 엔드포인트에서는 각 사용자가 개별적으로 로그인해야 FileVault에 추가됩니다.

시스템 디스크가 암호화되면 내부 데이터 볼륨이 자동으로 암호화됩니다. 컴퓨터기 시작되면 암호화 디스크가 자동으로 잠금 해제됩니다.

사용자는 알림을 통해 개별 디스크의 암호화 상태를 알 수 있습니다.

3.2.1 새 FileVault 사용자 추가

사용자가 FileVault에 자동으로 추가되지 않으면 이러한 지침에 새 사용자에게 표시되는 내용 및 사용자가 수행해야 하는 작업이 설명됩니다.

다음을 수행해야 합니다.

1. 로그인 암호를 입력하고 계속을 클릭합니다.
   사용자는 보통 macOS 로그인 암호를 사용하여 Mac에 액세스하고 FileVault를 사용할 수 있습니다.
2. Sophos Central에 아직 저장된 복구 키가 없으면 새 사용자가 이 작업에 권한을 부여해 줄 수 있는 기존 FileVault 사용자를 선택해야 합니다.
3. 그러면 기존 FileVault 사용자가 자신의 로그인 암호를 입력하고 계속을 클릭해야 합니다.

이제 사용자가 macOS 로그인 암호를 사용하여 Mac에 액세스하고 FileVault를 사용할 수 있습니다.

3.3 Mac 엔드포인트 복구

Mac을 복구하려면 다음 단계를 따르십시오.

사용자가 로그인 암호를 잊어버릴 경우 컴퓨터에 대한 액세스 권한을 되찾을 수 있는 방법이 여러 가지 있습니다.

- 해당 사용자가 컴퓨터에 마지막으로 로그인한 사람인 경우, Sophos 셀프 서비스 포털을 사용할 수 있습니다. 셀프 서비스 포털을 통해 복구 키 검색을 참조하십시오.
- 사용자는 대상 외부 Mac 시작 디스크로 컴퓨터를 시작한 뒤 터미널 명령을 사용해 디스크를 잠금 해제할 수 있습니다.
- 사용자는 대상 디스크 모드에서 컴퓨터를 시작한 뒤 터미널 명령을 사용해 디스크를 잠금 해제할 수 있습니다.
- 사용자는 대상 macOS 복구로 컴퓨터를 시작한 뒤 터미널 명령을 사용해 디스크를 잠금 해제할 수 있습니다.

  터미널 명령 작업에 대한 자세한 내용은 터미널 명령으로 HFS+ 볼륨 잠금 해제 및 터미널 명령으로 APFS 볼륨 잠금 해제를 참조하십시오.

사용자가 액세스 권한을 되찾도록 도울 수 있습니다. 이러한 지침에는 사용자에게 표시되는 내용 및 사용자가 수행해야 할 작업이 설명되어 있습니다. 다음과 같이 하십시오.

1. 엔드포인트 컴퓨터의 전원을 켜고 복구 키 ID가 표시될 때까지 기다립니다.
   복구 키 ID는 몇 분 정도밖에 표시되지 않습니다. 다시 표시하려면 사용자가 컴퓨터를 다시 시작해야 합니다.
2. 관리자에게 연락해 복구 키 ID를 알려 줍니다.
   사용자에게 복구 키를 제공할 수 있습니다. 사용자 중 한 명의 키를 검색하는 방법에 대한 도움말은 Sophos Central 도움말을 참조하십시오.
3. 암호 필드의 물음표 아이콘을 클릭합니다.
   메시지가 표시됩니다.
4. 메시지 옆의 화살표 아이콘을 클릭하여 복구 키 필드로 전환합니다.
5. 복구 키를 입력합니다.

   Active Directory에서 가져오기된 사용자의 경우 다음과 같은 추가 단계를 수행해야 합니다.

   - Active Directory에서 기존 암호를 다시 설정합니다. 그런 다음 임시 암호를 생성하고 사용자에게 제공합니다.
   - 사용자에게 암호 다시 설정 대화 상자에서 취소를 클릭하고 대신 임시 암호를 입력할 것을 알려줍니다.
6. 화면의 지침에 따라 새 암호를 만듭니다.
7. 메시지가 표시되면 새 키체인 생성을 클릭합니다.

사용자가 컴퓨터의 시작 볼륨에 다시 액세스할 수 있습니다.

macOS 10.12 또는 그 이전 버전을 실행 중인 엔드포인트에서는 새 복구 키가 생성되고 Sophos Central에 저장됩니다. 복구 키는 한 번만 사용할 수 있습니다. 컴퓨터를 나중에 다시 복구해야 하는 경우 새 복구 키를 검색해야 합니다.

macOS 10.13 및 APFS(Apple File System)를 실행 중인 엔드포인트에서는 새 복구 키가 생성되지 않습니다. 기존 복구 키가 유효한 상태로 유지됩니다.

관련 작업

셀프 서비스 포털을 통해 복구 키 가져오기 (페이지 20)
사용자가 컴퓨터에 로그온할 수 없으면(BitLocker PIN, macOS 암호 등을 잊어버림) Sophos 셀프 서비스 포털을 사용해 복구 키를 검색할 수 있습니다.

터미널 명령으로 HFS+ 볼륨 잠금 해제 (페이지 15)
터미널 명령을 사용하여 암호화된 볼륨을 잠금 해제할 수 있습니다. 이 섹션의 명령은 HFS+로 포맷된 볼륨으로 macOS 10.12 또는 그 이전 버전을 실행 중인 엔드포인트에 적용됩니다.

터미널 명령으로 APFS 볼륨 잠금 해제 (페이지 16)
터미널 명령을 사용하여 암호화된 볼륨을 잠금 해제할 수 있습니다. 이 섹션의 명령은 macOS 10.13 및 APFS(Apple File System)를 실행 중인 엔드포인트에 적용됩니다.

관련 정보

macOS 복구에 관하여
다른 시동 디스크를 선택하는 방법
Sophos Central 도움말

3.3.1 터미널 명령으로 HFS+ 볼륨 잠금 해제

터미널 명령을 사용하여 암호화된 볼륨을 잠금 해제할 수 있습니다. 이 섹션의 명령은 HFS+로 포맷된 볼륨으로 macOS 10.12 또는 그 이전 버전을 실행 중인 엔드포인트에 적용됩니다.

이러한 지침에는 사용자에게 표시되는 내용 및 사용자가 수행해야 할 작업이 설명되어 있습니다. 다음과 같이 하십시오.

1. 터미널 응용 프로그램을 열고 diskutil corestorage list를 실행합니다.
   연결된 모든 볼륨의 목록이 표시됩니다.
2. 복구하려는 볼륨 이름(LV 이름)을 검색하고 논리 볼륨 식별을 기억해 둡니다.
3. 관리자에게 연락하고 복구 키 ID로 논리 볼륨 식별을 사용해 복구 키를 요청합니다.
   사용자에게 복구 키를 제공합니다. 사용자 중 한 명의 키를 검색하는 방법에 대한 도움말은 Sophos Central 도움말을 참조하십시오.
4. 디스크 암호 대화 상자에 복구 키를 입력해 디스크의 잠금을 해제합니다.
   또는 사용자가 diskutil corestorage unlockVolume 명령을 사용하고 터미널 응용 프로그램에 복구 키를 입력해 디스크의 잠금을 해제할 수 있습니다.

이제 Finder에서 디스크에 액세스할 수 있습니다.

관련 정보
Sophos Central 도움말

3.3.2 터미널 명령으로 APFS 볼륨 잠금 해제

터미널 명령을 사용하여 암호화된 볼륨을 잠금 해제할 수 있습니다. 이 섹션의 명령은 macOS 10.13 및 APFS(Apple File System)를 실행 중인 엔드포인트에 적용됩니다.

이러한 지침에는 사용자에게 표시되는 내용 및 사용자가 수행해야 할 작업이 설명되어 있습니다. 다음과 같이 하십시오.

1. 터미널 응용 프로그램을 열고 diskutil apfs list를 실행합니다.
   연결된 모든 볼륨의 목록이 표시됩니다.
2. 복구하려는 볼륨 이름을 검색하고 볼륨 식별(예: Volume disk1s1)을 기록합니다.
3. 관리자에게 연락하고 복구 키 ID로 볼륨 식별을 사용해 복구 키를 요청합니다.
   사용자에게 복구 키를 제공합니다. 사용자 중 한 명의 키를 검색하는 방법에 대한 도움말은 Sophos Central 도움말을 참조하십시오.
4. 디스크 암호 대화 상자에 복구 키를 입력해 디스크의 잠금을 해제합니다.
   또는 사용자가 diskutil apfs unlockVolume 명령을 사용하고 터미널 응용 프로그램에 복구 키를 입력해 디스크의 잠금을 해제할 수 있습니다.

이제 Finder에서 디스크에 액세스할 수 있습니다.

관련 정보
Sophos Central 도움말

3.3.3 오류: 복구 키를 저장하지 못함

드물지만 시스템이 로컬(키체인)이나 Sophos Central에 복구 키를 저장하지 못하는 문제가 발생할 수도 있습니다.

이렇게 되면 사용자가 암호를 잊어버렸을 때 컴퓨터를 복구할 수 없게 됩니다. 이 위험을 완화하기 위해 복구 키와 함께 오류 메시지가 표시되고, 사용자에게 복구 키 복사본을 만들라는 메시지도 표시됩니다.

시스템이 Sophos Central에 복구 키를 저장하려 반복해서 시도합니다. 이 시도가 성공하는 즉시 사용자에게 Sophos Central에서 이제 새 복구 키를 관리하며 복구 키의 복사본을 폐기해도 된다는 사실을 알려 주는 메시지가 표시됩니다.

3.4 Device Encryption 상태(Mac)

사용자는 Sophos Device Encryption 응용 프로그램을 사용하여 암호화 상태에 대한 정보에 액세스할 수 있습니다. Applications 디렉터리에 설치되며, Finder, Launchpad 또는 Spotlight를 통해 실행할 수 있습니다.

Sophos Device Encryption 응용 프로그램은 다음 정보를 제공합니다.

- 정책 상태: 첫 번째 줄은 끝점이 Sophos Device Encryption에 의해 관리되는지 여부를 사용자에게 알려 줍니다.
- 사용자 상태: 두 번째 줄은 사용자에게 할 수 있는 작업과 그렇지 않은 작업을 알려 줍니다.
- 디스크 상태: 모든 내부 디스크의 목록이 표시됩니다. 디스크 이름이 회색으로 표시되면 디스크가 현재 탑재되어 있지 않은 것입니다. 디스크 이름 옆의 아이콘은 디스크의 상태를 나타냅니다. 다음과 같은 상태가 제공됩니다.
  - 녹색: 디스크가 완전하게 암호화되었으며 복구 키가 중앙에 저장되어 있습니다.
  - 노란색: 디스크가 완전하게 암호화되었지만 복구 키가 Sophos Central에 저장되어 있지 않습니다. 현재 Sophos Central에 연결할 수 없는 경우에 발생할 수 있습니다. 디스크의 암호화가 필요하지 않을 경우 복구 키가 아예 존재하지 않을 수도 있습니다. 보통 Sophos Central Device Encryption에 의해 디스크가 관리되지 않고 운영 체제 도구를 사용해 암호화되었을 경우에 발생합니다.
  - 노란색 + 느낌표: 디스크가 안전하게 암호화되었고 디스크를 암호화해야 한다는 정책이 존재하지만 사용할 수 있는 복구 키가 없습니다.
  - 빨간색: 디스크가 암호화되지 않았지만 디스크를 암호화해야 한다는 정책이 활성 상태입니다.
  - 회색: 디스크가 암호화되지 않았고 정책이 암호화를 요구하지 않거나 정책이 아예 없습니다.
  - 상태 표시줄 + 암호화 중: 디스크가 현재 암호화되고 있는 중입니다.
  - 상태 표시줄 + 암호 해독 중: 디스크가 현재 암호 해독되고 있는 중입니다.

    참고
    Mac 끝점에 대한 관리 권한이 있는 사용자가 암호화 정책이 적용된 하드 디스크를 수동으로 암호 해독하려고 시도하는 경우 Sophos Central에서 이를 재정의할 수 없으며, 디스크가 암호 해독됩니다. 암호 해독이 완료되면 FileVault를 설정하기 위해 암호를 묻는 메시지가 사용자에게 표시되고 디스크가 다시 암호화됩니다.

- 복구 상태: 창 맨 아래에 사용자에게 디스크에 복구 키를 사용할 수 있는지 여부를 알려 주는 메시지가 나타납니다.

또는 명령줄 도구를 사용하여 Device Encryption 상태에 대한 정보에 액세스할 수 있습니다. 도구는 /usr/local/bin/seadmin에 설치됩니다. 다음과 같은 명령이 제공됩니다.

- help: 사용 가능한 명령 목록을 표시합니다.
- status: 암호화 소프트웨어의 마지막 동기화와 동기화 간격을 표시합니다.
- --device-encryption: 현재 암호화 정책과 모든 내부 디스크의 암호화 및 복구 상태를 표시합니다.

4 보안 공유를 위해 파일을 암호로 보호

Device Encryption 정책에서 이 옵션을 설정할 수 있습니다.

참고
이 기능은 Central Device Encryption 2.0 이상에서만 사용할 수 있습니다. 이 기능은 Windows 컴퓨터에서만 사용할 수 있습니다.

최대 50MB의 파일을 보호할 수 있습니다.

오른쪽 클릭 상황에 맞는 메뉴 사용: 이 옵션을 켜면 암호로 보호된 파일 만들기 옵션이 오른쪽 클릭 메뉴에 나타납니다. 사용자는 민감한 데이터를 회사 네트워크 외부의 받는 사람에게 보낼 때 암호로 보호된 파일을 이메일에 첨부할 수 있습니다. 파일은 새 HTML 파일에 암호화된 내용으로 래핑됩니다.

받는 사람은 파일을 두 번 클릭하고 암호를 입력하여 파일을 열 수 있습니다. 받은 파일을 다시 보낼 때는 동일한 암호 또는 새 암호로 파일을 보호하거나 암호로 보호된 파일을 새로 만들 수 있습니다.

Outlook 추가 기능 사용: 이 옵션은 이메일 첨부 파일의 암호화를 Outlook에 추가합니다. 사용자는 Outlook 리본에서 첨부 파일 보호를 선택하여 첨부 파일을 보호할 수 있습니다. 보호되지 않은 모든 첨부 파일은 새 HTML 첨부 파일에 암호화된 내용으로 래핑되고 이메일이 전송됩니다.

첨부 파일 처리 방법 항상 확인: 이 옵션이 켜져 있으면, 사용자는 메시지에 파일을 첨부할 때마다 첨부 파일을 보내는 방법을 선택해야 합니다. 첨부 파일을 암호로 보호하거나 보호하지 않은 상태로 보낼 수 있습니다.

첨부 파일 처리 방법 항상 확인 옵션이 적용되지 않는 제외된 도메인을 입력할 수 있습니다(예: 귀하 조직의 도메인). 받는 사람이 그러한 도메인에 속해 있으면 보낸 사람에게 첨부 파일 처리 방법을 묻지 않습니다.

전체 도메인 이름만 입력하고 쉼표로 구분합니다.

관련 정보
Device Encryption 정책

5 사용자에게 암호/PIN 변경 메시지 표시

사용자에게 암호를 변경하도록 메시지를 표시하는 방법에는 두 가지가 있습니다.

참고
이 옵션은 Windows에는 제공되지 않습니다.

- 암호화 정책에서 사용자에게 새 인증 암호/PIN 요구 옵션을 사용합니다.

  이 옵션은 기본적으로 꺼져 있습니다. 이 옵션은 지정된 시간 후에 BitLocker 암호 또는 PIN을 강제로 변경합니다. 사용자가 암호 또는 PIN을 변경하면 이벤트가 기록됩니다.

  참고
  이 기능은 Central Device Encryption 2.0 이상에서만 사용할 수 있습니다.

- 컴퓨터 세부 정보 페이지의 요약 탭에 있는 암호/PIN 트리거 변경 옵션을 사용합니다.

  이를 위해서는 사용자가 즉시 BitLocker 암호 또는 PIN을 변경해야 합니다. 요청이 성공적으로 전송되면 메시지가 표시됩니다.

엔드포인트에서 새 BitLocker 암호 또는 PIN을 설정하라는 메시지가 나타납니다. 사용자가 새 암호 또는 PIN을 입력하지 않고 대화 상자를 닫으면 대화 상자는 30초 후에 다시 표시됩니다. 이는 입력을 하면 중지됩니다. 사용자가 암호 또는 PIN을 변경하지 않고 대화 상자를 다섯 번 닫으면 경고가 기록됩니다.

관련 정보
Device Encryption 정책
컴퓨터 요약

6 셀프 서비스 포털을 통해 복구 키 가져오기

사용자가 컴퓨터에 로그온할 수 없으면(BitLocker PIN, macOS 암호 등을 잊어버림) Sophos 셀프 서비스 포털을 사용해 복구 키를 검색할 수 있습니다.

복구 키가 있으면 컴퓨터에 다시 액세스할 수 있습니다.

셀프 서비스 포털에서 사용자가 컴퓨터를 복구할 수 있도록 설정하려면 Sophos Central > 사람 > 사용자로 이동하고 한 명 이상의 사용자를 선택한 후 이메일 설정 링크 단추를 클릭하십시오. 다음 대화 상자에서 Sophos Central 셀프 서비스 시작/시작 이메일을 선택해 사용자에게 활성화 링크를 이메일로 보내십시오. 사용자가 이메일의 지시 사항에 따를 경우 Sophos 셀프 서비스 포털을 사용하여 컴퓨터를 복구할 수 있습니다.

이러한 지침에는 사용자에게 표시되는 내용 및 사용자가 수행해야 할 작업이 설명되어 있습니다. 다음과 같이 하십시오.

1. 다른 컴퓨터를 사용하여 Sophos 셀프 서비스 포털에 로그온합니다.
2. Device Encryption 페이지로 이동합니다.
   사용자가 마지막으로 로그인한 모든 컴퓨터의 목록이 표시됩니다. 그동안 다른 사용자가 컴퓨터에 로그인한 경우 사용자가 셀프 서비스 포털을 통해 이 컴퓨터에 대한 액세스 권한을 다시 얻을 수 없습니다.
3. 목록에서 컴퓨터를 선택하고 복구 키 열에서 가져오기 단추를 클릭합니다.
   복구 키가 포함된 대화 상자가 표시됩니다.
4. 자신의 컴퓨터를 시작하고 복구 페이지로 이동합니다.
   - Windows: Esc 키를 눌러 BitLocker 복구 화면으로 전환합니다.
   - Mac: 암호 필드에서 물음표 아이콘을 클릭하여 FileVault 복구 페이지로 전환합니다.
5. 복구 키를 입력합니다.

사용자가 자신의 컴퓨터에 다시 액세스할 수 있습니다.

관련 정보
셀프 서비스 포털

7 추가 읽기

Windows

- FAQ: 기술 문서 자료 124819
- BitLocker에 대한 자주 묻는 질문(FAQ)
- BitLocker 그룹 정책 설정
- TPM 기본 항목
- TPM 그룹 정책 설정
- 신뢰할 수 있는 플랫폼 모듈 관리 기술 개요

Mac

- FAQ: 기술 문서 자료 125982
- FileVault 설정: Mac에서 FileVault를 사용하여 시동 디스크 암호화하기
- FileVault 복구 키: 기관에서 컴퓨터의 FileVault 복구 키 설정하기
- 암호 다시 설정: macOS 사용자 계정의 암호 변경 또는 재설정하기

관련 정보
BitLocker에 대한 자주 묻는 질문(FAQ)
BitLocker 그룹 정책 설정
TPM 그룹 정책 설정
TPM 기본 항목
신뢰할 수 있는 플랫폼 모듈 관리 기술 개요
Mac에서 FileVault를 사용하여 시동 디스크 암호화하기
기관에서 컴퓨터의 FileVault 복구 키 설정하기
macOS 사용자 계정의 암호 변경 또는 재설정하기
기술 문서 자료 124819
기술 문서 자료 125982

8 지원되는 웹 브라우저

현재 다음과 같은 브라우저가 지원됩니다.

- Microsoft Internet Explorer 11 및 Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Apple Safari(Mac 전용)

위의 목록에서 지원되는 버전을 설치하거나 이 버전으로 업그레이드하고, 항상 최신 버전을 유지하는 것이 좋습니다. Google Chrome, Mozilla Firefox, Apple Safari의 최신 버전과 이전 버전을 지원하는 것을 목표로 합니다. 지원되지 않는 브라우저가 발견되면 https://central.sophos.com/unsupported로 리디렉션됩니다.

참고
Sophos Central Admin은 모바일 장치에서 지원되지 않습니다.

9 추가 지원 받기

Sophos 지원으로부터 도움을 얻으려면 다음과 같이 하십시오.

1. 사용자 인터페이스의 오른쪽 상단에서 도움말을(를) 클릭하고 지원 티켓 만들기을(를) 선택합니다.
2. 양식을 작성합니다. 지원팀이 효과적으로 도와 드릴 수 있도록 최대한 정확하게 작성하십시오.
3. 이 옵션을 선택하면 지원 팀에서 Sophos Central 세션에 직접 액세스해 더 많은 도움을 드릴 수 있습니다.
4. 보내기를 클릭합니다.

Sophos가 24시간 안에 연락을 드립니다.

참고
지원팀에서 Sophos Central 세션에 액세스할 수 있도록 하는 옵션을 선택한 경우 보내기을(를) 클릭하면 이 기능이 활성화됩니다. 원격 지원은 72시간 후에 자동으로 사용할 수 없도록 설정됩니다. 더 일찍 사용할 수 없도록 설정하려면 계정 이름(사용자 인터페이스 오른쪽 위)을 클릭하고 계정 세부 정보을(를) 선택한 후 Sophos 지원 탭을 클릭합니다.

피드백 제출

Sophos Support에 피드백이나 제안을 제출하려면 다음과 같이 하십시오.

1. 사용자 인터페이스의 오른쪽 상단에서 도움말을(를) 클릭하고 피드백 제공을 선택합니다.
2. 양식을 작성합니다.
3. 제출를 클릭합니다.

추가 도움말

다음과 같은 기술 지원을 찾을 수도 있습니다.

- community.sophos.com/에서 Sophos Community를 방문하고 같은 문제를 겪고 있는 다른 사용자들을 검색합니다.
- www.sophos.com/en-us/support.aspx에서 Sophos 지원 지식 기반을 방문합니다.

10 법적 고지 사항