EasyLock

사용자 매뉴얼 버전 2.0.0.2

사용자 매뉴얼

COSOSYS

목 차

1. 서론

제 3자가 기밀 정보에 접근할 수 없도록 보장하는 이동 데이터 보호는 필수입니다. USB 저장 장치, CD/DVD, 로컬 폴더, 클라우드 솔루션 등 데이터가 어디에 저장되든 관계없이 암호화는 분실, 도난, 잘못된 곳에 보관하는 경우에 최고의 솔루션이 될 수 있습니다.

EasyLock은 엔터프라이즈 크로스 플랫폼 데이터 암호화 솔루션으로 기밀 데이터를 보호하기 위해서 디자인 되었습니다. 이 솔루션은 초보자에서 전문가 그리고 홈 사용자에서 다국적 직원에 이르기까지 모든 유형의 사용자에게 적합합니다.

여러가지 EasyLock 버전을 사용할 수 있습니다. 비록 이 버전들이 비슷하고 같은 암호화 등급과 쉬운 사용을 제공하지만 여러분의 시나리오에 따라서 올바른 선택을 위해서 고려해야 하는 부분이 있습니다.

- **EasyLock** – 컴퓨터 자체에 어떤 프로세스 설치도 필요하지 않은 독립실행형입니다. 강력한 256bit AES CBC-mode 암호화를 사용하여 USB 저장 장치를 보호합니다. *또한 로컬 폴더, CD/DVD, 클라우드 스토리지 솔루션에서 사용할 수 있습니다.

  Endpoint Protector에서 USB 저장 장치로 허용됩니다.

- **EasyLock 암호화 정책 –** 독립 실행형으로 USB 저장 장치에 같은 기능을 제공 합니다. 다른 점은 컴퓨터에 작은 설치가 필요합니다.

  USB 저장 장치를 TD(TrustedDevice) 1+ 로 인식됩니다. Endpoint Protector와 연동해서만 사용할 수 있습니다. Endpoint Protector 클라이언트가 설치된 컴퓨터에 연결되는 모든 USB 저장 장치를 보안USB 로 만들어 사용이 가능하고 암호 재설정, 메시지 보내기, 장치 재설정 등의 원격 관리 또한 할 수 있습니다.

직관적인 드래그 앤 드롭 인터페이스를 사용해서 파일을 장치에 빠르고 안전하고 효율적으로 복사할 수 있습니다.

2. 시스템 요구사항

EasyLock 과 EasyLock 암호화 정책은 거의 모든 Mac 또는 Windows에서 동작합니다.

지원하는 운영 시스템:

- Windows XP (최신 서비스 팩 및 업데이트 필요) 에서 최신 Windows 10 버전
- Mac OS 10.8 에서 최신 macOS 10.14 - Mojave

사용 가능한 USB 포트

USB 플래시 드라이브, 외장 하드 드라이브, 메모리 카드 등의 이동식 USB 저장 장치기

만약 휴대용 저장 장치가 수동으로 쓰기 보호 스위치 (Lock)를 가지고 있다면 반드시 쓰기가 가능하도록 풀어 주어야 EasyLock을 사용할 수 있습니다.

> **정보**
>
> 로컬 폴더, CD/DVD, 클라우드에 사용하는 EasyLock은 USB 포트가 필요하지 않습니다.

3. 배포

3.1. EasyLock 다운로드

EasyLock 응용프로그램 소프트웨어는 아래에서 다운로드 할 수 있습니다:
http://www.cososys.kr/products/easylock

EasyLock 암호화 정책 소프트웨어는 관련 Endpoint Protector 서버에서 다운로드가 필요합니다. 특정 서버와 그에 따른 특정 장치가 연관성을 가지고 있습니다. 각각의 장치는 새로운 인스톨러 다운로드가 필요합니다.

팁

EasyLock 설정이 Windows와 Mac 버전을 포함하고 있지만 초기 배포 단계에서는 다른 설치 파일을 사용합니다.

예: Windows 컴퓨터에서는 EasyLockSetup.exe 를 사용합니다.

예: Mac 컴퓨터에서는 EasyLockSetup.dmg 를 사용합니다.

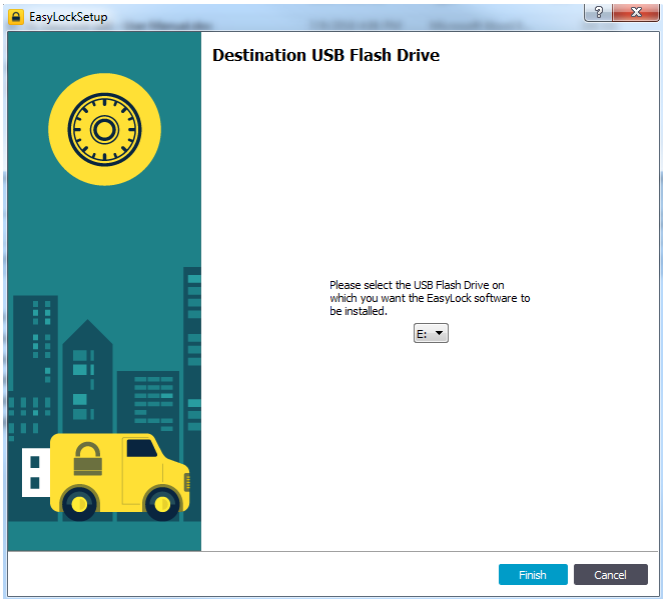
정보

EasyLock 암호화 정책의 경우 Endpoint Protector 서버 설정으로 클라이언트 컴퓨터에 USB 저장 장치를 연결하면 자동으로 EasyLock을 자동으로 배포할 수 있습니다.

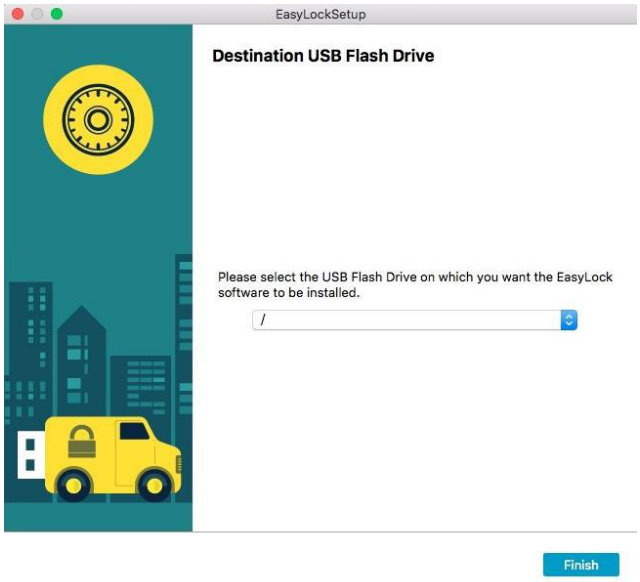
3.2. USB 저장 장치에 EasyLock 설치

USB 저장 장치에 EasyLock 설치:

- **Windows**: "EasyLockSetup.exe" 파일을 열고 USB 장치가 연결된 드라이브 선택 후 마침 버튼을 누릅니다. EasyLock 응용프로그램은 선택한 드라이브의 Root 폴더에 자동으로 설치 될 것입니다.



- **macOS**: "EasyLockSetup.dmg" 파일을 열고 USB 장치가 연결된 드라이브 선택 후 마침 버튼을 누릅니다. EasyLock 응용프로그램은 선택한 드라이브의 Root 폴더에 자동으로 설치 될 것입니다.



3.3. 로컬 폴더, 클라우드 등에 EasyLock 설치

CD/DVD, 로컬 폴더, 클라우드 스토리지 솔루션에 EasyLock을 설치하기 위해서는 3.2와 비슷한 단계의 프로세스를 거칩니다.

주요 차이점은 로컬 폴더의 초기 위치입니다. 설치된 후에 EasyLock은 클라우드 솔루션 또는 CD/DVD 로 이동할 수 있습니다.

3.4. USB 저장 장치에 EasyLock 암호화 정책 설치

USB 저장 장치에 EasyLock 암호화 정책을 설치하기 위해서는 3.2와 비슷한 단계의 프로세스를 거칩니다.

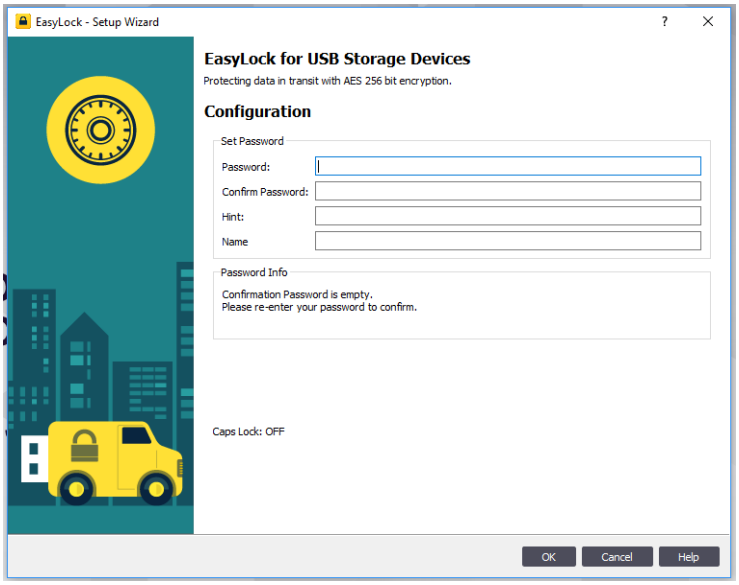
- 자동 배포를 이용하면 EasyLock은 장치의 Root 폴더에 자동으로 복사가 될 것입니다.
- 수동 배포를 이용하면 EasyLock을 장치의 Root 폴더에 복사해야 합니다.

3.5. EasyLock 설정 (모든 버전)

EasyLock 버전 (EasyLock 암호화 정책, USB 저장 장치 EasyLock, 클라우드 EasyLock 등)에 관계없이 주요 설정 요구사항은 암호입니다.

암호는 최소 6자리가 되어야 합니다. 보안상의 이유료 문자, 숫자, 특수문자 조합을 권장합니다.

또한 암호를 기억할 수 있는 리마인더 설정을 권장합니다. 암호는 복구가 불가능하고 코소시스는 어떠한 책임도 지지않습니다.



정보

EasyLock 암호화 정책에서 Endpoint Protector 관리자는 사용자가 암호를 잃어버린 경우에 추가적인 도구를 사용할 수 있습니다. 그러나 여러가지 경우가 존재하기 때문에 이러한 기능을 항상 사용할 수는 없습니다.

3.6. 암호 재시도

EasyLock 시작할 때마다 사용자는 암호를 입력해야 합니다. 보안상 이유로 10번의 재시도 기회가 주어집니다. 연속해서 10번 잘못된 암호를 입력하게 되면 EasyLcok의 모든 데이터는 안전하게 삭제됩니다.

이 보안 조치는 장치를 도난 또는 분실한 경우 데이터 보호를 보장합니다. 그러므로 휴대용 저장 장치의 데이터는 복구될 수 없고 영원히 완전하게 삭제됩니다.

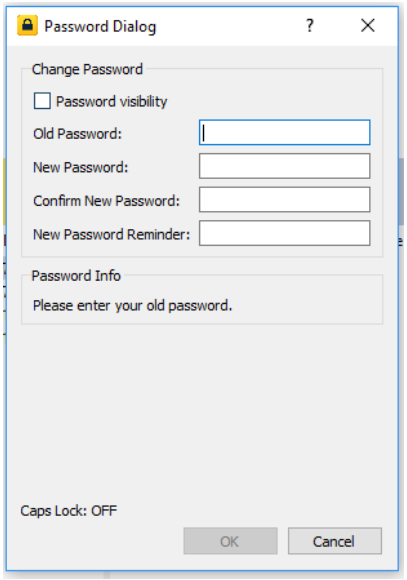
정보

EasyLock 암호화 정책에서 Endpoint Protector 관리자는 사용자 정의로 여러가지 암호 설정 옵션을 사용할 수 있습니다. 암호 재시도, 포맷, 기록, 만료 기간 등이 포함됩니다.

4. 특징 및 기능

4.1. 암호

로그인 후에 EasyLock은 언제든지 암호를 변경할 수 있습니다. 이 작업은 툴바의 옵션 > 보안 설정 또는 Ctrl + O 키를 눌러서 완료할 수 있습니다.

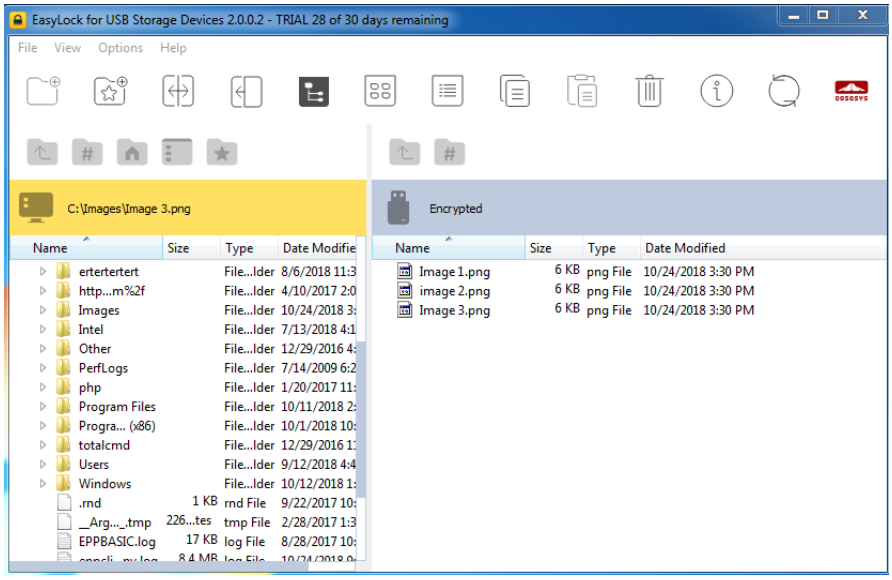


EasyLock 암호화 정책에서 이 작업은 옵션 > 암호 변경 에서 완료할 수 있습니다.

4.2. 화면 사용자 정의

툴바 영역에서 EasyLock 화면 위도우에 대한 여러가지 사용자 정의 옵션을 제공합니다. 주요 기능은 툴바 또는 주요 메뉴 > 보기 섹션에서 사용할 수 있습니다.

보기 > 툴바 에서 선택하기 또는 선택하지 않기를 통해서 툴바에서 노출 또는 숨길 수 있습니다.



4.3. 주요 기능

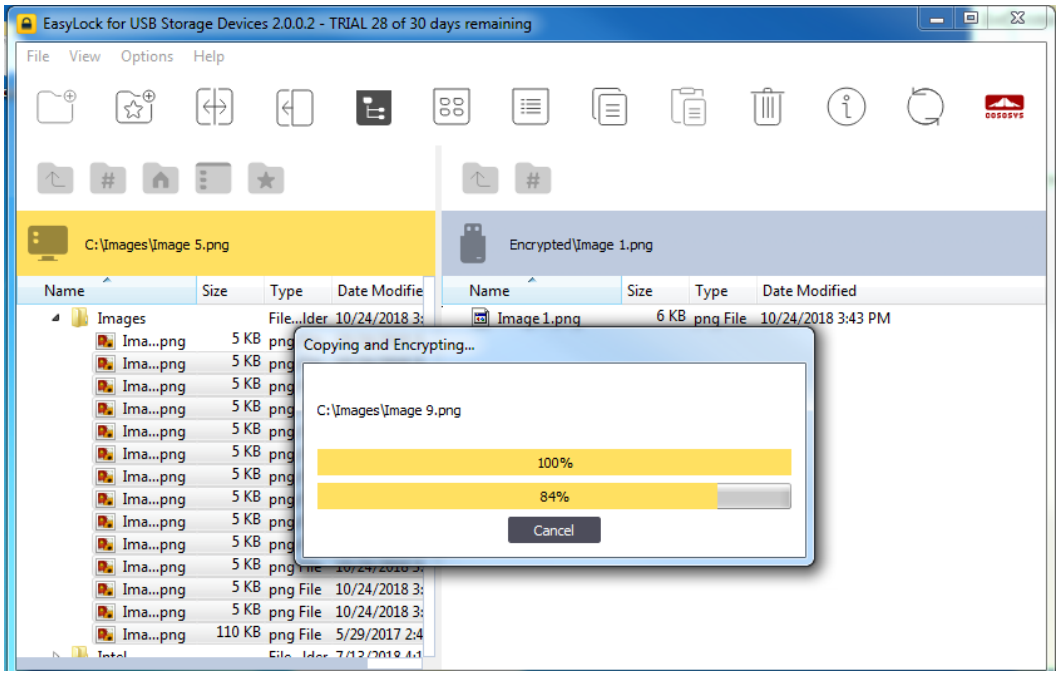
위에서 언급한 바와 같이 툴바 또는 주요 메뉴 > 보기 섹션으로 접근할 수 있습니다.

- **새로운 폴더** – 활성화 윈도우에서 새로운 디렉토리 생성
- **즐겨찾기** – 즐겨찾기 위치 관리
- **패널 스왑** – USB 드라이브 화면과 내 컴퓨터 패널 교환
- **내 컴퓨터 패널 보기 또는 숨기기** – 내 컴퓨터 패널 노출
- **트리 보기** – 트리 구조로 보여주기
- **자세히 보기** – 추가적인 파일 정보 보여주기
- **목록 보기** – 목록으로 아이템 보여주기
- **클립보드 복사** – 클립보드에 콘텐츠 복사
- **클립보드 삽입** – 클립보드 콘텐츠 삽입
- **삭제** – 아이템 삭제
- **정보** – EasyLock 버전 정보 보기
- **새로고침** – 파일 추가 정보 보여주기

4.4. 드래그 앤 드롭 기능

파일 작업 시 복사 및 붙여넣기 또는 드래그 앤 드롭 기능을 사용할 수 있습니다.

드래그 앤 드롭 기능은 파일 또는 폴더 작업을 간단하게 처리할 수 있습니다. 사용자는 EasyLock 윈도우에 복사가 필요한 아이템을 드롭하기만 하면 됩니다. 이 작업으로 파일과 폴더는 안전하게 보안 처리가 됩니다.

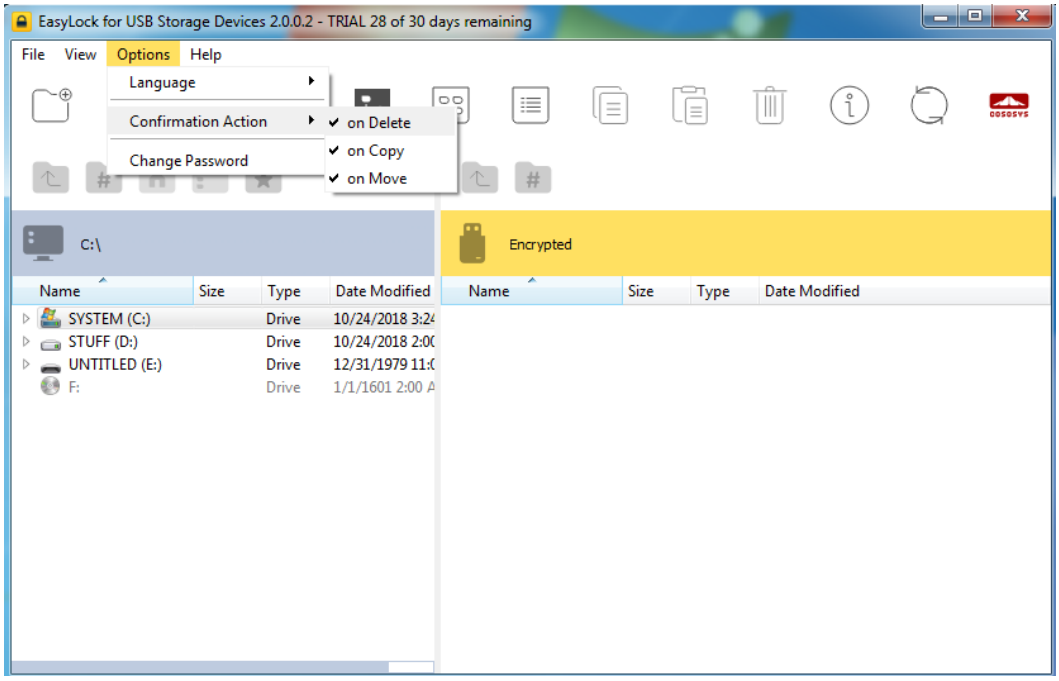


전송 상태는 프로그레스 바를 통해서 볼 수 있습니다.

4.5. 옵션 선택

암호 변경에 추가하여 이 섹션은 다른 옵션 뿐만 아니라 사용자 인터페이스 언어 변경을 제공합니다.

프리퍼런스 설정은 삭제, 복사 또는 이동과 같은 액션 확인 메시지 노출 또는 숨기기 허용을 할 수 있습니다. 암호화 정책 버전에서 이 섹션은 확인 액션으로 되어 있습니다.



4.6. 파일 열기 및 수정

이 응용프로그램 안에서 데이터를 보고 직접 수정할 수 있습니다. EasyLock은 사용자가 닫으면 바로 이 문서들을 닫으려고 할 것입니다. 만약 문서가 수정되었다면 (같은 이름으로 저장되거나 심지어 같은 폴더에 저장) 암호화 될 것입니다. 만약 문서가 수정되고 저장 되었지만 암호화에 실패한다면 (예: USB 장기가 갑자기 제거된 경우) 다음 EasyLock이 시작할 때 암호화 될 것입니다.

EasyLock 암호화 정책 버전에서 데이터는 이 응용프로그램 안에서 직접 보거나 편집 할 수 없습니다. 필요한 문서를 수정하려면 EasyLock 영역에서 다른 영역 (예: 사용자 로컬 영역)으로 복사해야 합니다.

팁

EasyLcok에서는 데이터를 직접 보거나 편집할 수 있습니다.

암호화 영역에 있는 파일에 접근하는 동안 EasyLock은 잠김으로 되어 있습니다.

5. Endpoint Protector와 EasyLock

독립 실행형 EasyLock과 EasyLock 암호화 정책 보안USB 버전 모두 Endpoint Protector와 함께 사용할 수 있습니다. USB 저장 장치를 TrustedDevice 레벨 1로 설정하면 됩니다.

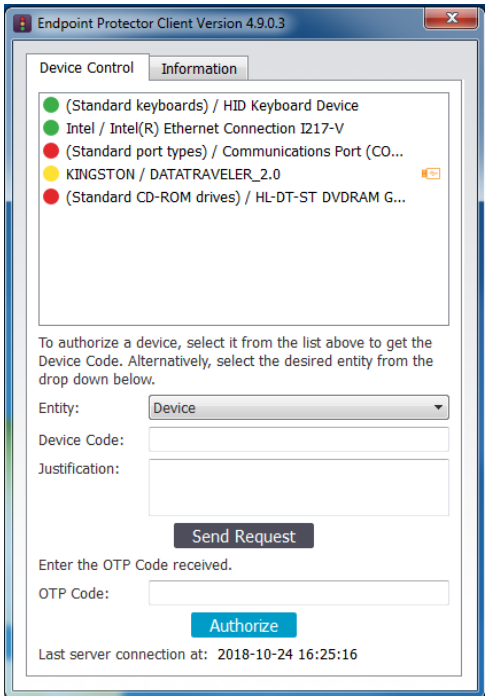
Endpoint Protector는 서버-클라이언트 방식의 DLP (Data Loss Prevention) 솔루션 입니다. 매체 제어 모듈은 USB와 주변 포트의 모니터링과 제어를 제공합니다.

전형적인 시나리오는 엔드포인트에 배포된 Endpoint Protector 클라이언트 배포가 포함된 것입니다. 데이터 분실 또는 도난을 피하기 위해서 장치 권한은 모든 USB 저장 장치 차단이 될 것입니다. 그러나 특정 장치에 EasyLock이 설치되어 있다면 모든 복사된 문서는 암호화되고 보호 상태로 그 접근이 허용되는 것을 의미합니다.

TrustedDevice 레벨 1은 EasyLock 응용프로그램이 이미 USB 저장 장치에 설치되어 있어서 Endpoint Protector를 통해서 허용되는 것을 의미합니다.

TrustedDevice 레벨 1+ 은 Endpoint Protector를 통해서 EasyLock 암호화 정책 또한 활성화되고 라이선스가 올라가 있다는 것입니다. 이 상황에서 EasyLock은 보호되는 엔드포인트에 USB 저장 장치가 연결되면 자동으로 배포됩니다.

TD 레벨 1+ 허용, 그 외 읽기만 권한 또한 사용할 수 있습니다. USB 저장 장치는 읽기만 권한이 허용되고 EasyLock은 Endpoint Protector 클라이언트로 자동으로 설치할 수 있습니다. Endpoint Protector 클라이언트에서 USB 장치에 할당된 노란색의 장치 아이콘을 클릭해서 배포할 수 있습니다.



만약 TrustedDevice가 Endpoint Protector의 인증에 실패한다면 사용자가 사용할 수 없을 것입니다. 장치는 차단되고 사용자는 그 장치에 접근할 수 없습니다.

5.1. EasyLock TrustedDevice 파일 추적

EasyLock TrustedDevice 파일 추적은 암호화된 USB 장치에 파일 복사 모니터링을 할 수 있습니다.

파일 추적 옵션을 활성화 함으로써 EasyLock을 사용한 장치에 전송되는 모든 데이터는 차후 감사 목적으로 기록되고 로그가 남습니다. 로그 정보는 자동으로 Endpoint Protector 서버에 보내집니다 (Endpoint Protector 클라이언트가 설치된 컴퓨터에 연결되고 인터넷 연결이 동작하는 경우).

Endpoint Protector 클라이언트 정보가 존재하지 않는 경우에 정보는 장치의 암호화 포맷 로컬 영역에 저장됩니다. 이 장치가 인터넷이 동작하고 보호되는 컴퓨터에 연결되면 후에 로그 정보는 Endpoint Protector 서버로 보내내집니다.

또 다른 측면으로 EasyLock 암호화 정책 버전은 Endpoint Protector 클라이언트가 존재하는 컴퓨터에서만 동작할 수 있습니다. 만약 클라이언트가 탐지되지 않는다면 EasyLock은 열리지 않습니다.

5.2. 마스터 암호

마스터 암호는 Endpoint Protector 서버에서 설정할 수 있습니다. 이는 관리자가 특정한 상황에서 EasyLock 장치에 접근할 수 있도록 허용합니다 (예: 직원이 회사를 나가고 그 직원의 장치에 있는 데이터 복구가 필요한 경우).

마스터 암호의 복잡성 설정이 가능하고 길이, 특수 문자, 대소문자, 유효 기간, 기록 등의 설정도 포함되어 있습니다.

팁

사용자 암호에 대해서도 똑같은 암호 복잡성 설정이 가능합니다. 이것은 Endpoint Protector 관리자의 내부 보안 정책 준수를 위해서 실행 할 수 있습니다.

5.3. Endpoint Protector 클라이언트 필요

추가 보안 조치를 위해서 EasyLock 암호화 정책은 Endpoint Protector 클라이언트가 설치된 컴퓨터에서만 사용하도록 제한 할 수 있습니다.

또한 또 다른 신뢰할 수 있는 Endpoint Protector 서버 목록에 추가할 수 있는 옵션이 있습니다.

6. 지원

추가적인 지원 자료를 받을 수 있습니다. 코소시스 웹사이트에 방문하면 더 많은 사용자 매뉴얼, FAQ, 동영상 등을 찾을 수 있습니다:

http://www.cososys.kr

7. 면책

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.