ENDPOINT PROTECTOR | by CoSoSys
NOW PART OF netwrix

Endpoint Protector

사용자 매뉴얼

버전 5.9.3.0

날짜 2024년 2월 29일

목 차

1. 새로운 기능

최신 Endpoint Protector는 새로운 기능이 추가되고 향상된 사용자 경험을 제공합니다. 아래 릴리즈 노트에서 내용을 확인하시기 바랍니다:

https://cososys.kr/support/endpoint-protector-release-history/endpoint-protector-product-update-version-5.9.3.0

2. 이 매뉴얼에 대하여

2.1. 범위

이 문서는 Endpoint Protector를 설정하고 구성하는 방법을 설명합니다. 네트워크 토폴로지와 지속적인 유지보수를 포함해서 처음으로 시스템 배포를 완료하기 위한 설명을 제공합니다.

Endpoint Protector 사용자 인터페이스 사용 방법, 기본 사용 포트 번호 목록의 자세한 정보, 구성 제한 및 지원되는 기준을 기술합니다.

2.2. 대상

이 문서는 최종 사용자가 아니라 시스템 관리자를 위한 매뉴얼입니다.

Endpoint Protector로 보호되는 기기에 접근하고 이 매뉴얼이 제공하지 않는 질문이 있다면 연락을 주시기 바랍니다.

3. 소개

USB 플래시 드라이브, 외장 HDD, 디지털 카메라, MP3 플레이어/iPod 등 휴대용 저장 장치는 거의 모든 곳에서 몇 초 만에 Windows PC, Mac 또는 Linux 컴퓨터와 연결됩니다. 사실상 인터넷, 온라인 응용프로그램 및 협업 도구에 접근할 수 있는 컴퓨터는 데이터 절도 또는 실수로 인한 자료 유출은 너무나 쉽습니다.

단순한 인터넷 연결 또는 USB 장치로 인한 자료 유출 및 절도는 쉽고 몇 초도 걸리지 않습니다. 네트워크 관리자는 이러한 사건을 사전에 조치하거나 사용자의 책임을 가려내기가 힘들었습니다. 지금까지는 어려운 현실이었습니다.

매체 제어, 콘텐츠 인식 보호, eDiscovery 및 암호화 정책 모듈이 통합된 Endpoint Protector는 회사에서 이러한 위협을 멈출 수 있도록 도와줍니다. 엔드포인트의 모든 장치 활동을 제어할 뿐만 아니라 민감한 콘텐츠 탐지를 위해 모든 가능한 출구 지점들을 모니터하고 스캔합니다. 이것은 매우 중요한 비즈니스 데이터가 장치에 복사되거나 허가 없이 인터넷으로 보내지는 행위를 통해서 내부 네트워크를 빠져 나가지 못하도록 보장합니다. 모든 민감한 데이터의 사건이 보고가 됩니다. 게다가 엔드포인트에 존재하는 저장 데이터 (data at rest)에 민감한 콘텐츠가 있는지 검사하고 원격으로 바로 조치할 수가 있습니다. 또한 휴대용 USB 저장 장치의 암호화 강제 기능이 가능합니다. 이 모든 것을 웹 기반의 단일 인터페이스에서 수행할 수 있습니다.

Endpoint Protector는 완전한 DLP (Data Loss Prevention)이고 DLP 관련 기능은 아래에서 설명할 것입니다. Endpoint Protector와 관련된 추가 정보는 https://www.cososys.kr 의 자료실을 참조하시기 바랍니다.

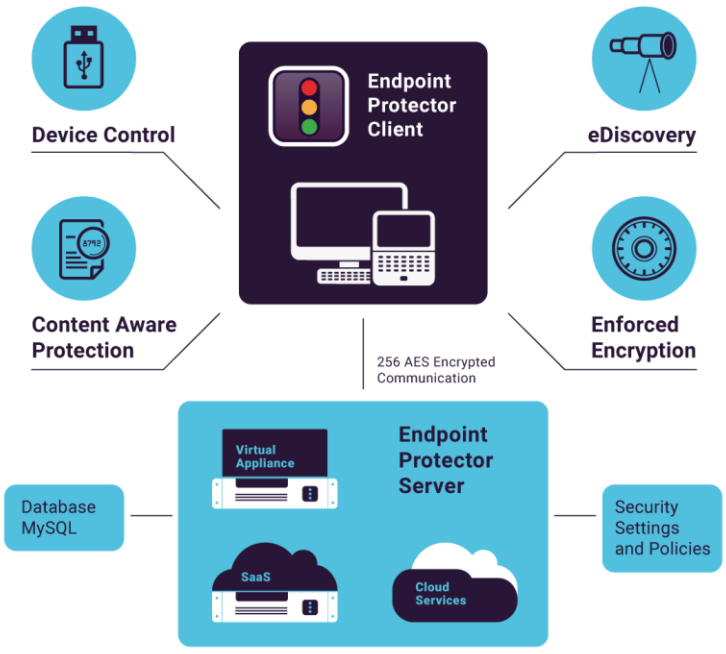
3.1. 주요 구성요소

Endpoint Protector는 여러 물리적 객체로 설계되었습니다.

- **컴퓨터** - Endpoint Protector 클라이언트가 설치된 Windows, Mac 및 Linux 워크스테이션
- **장치** - 현재 Endpoint Protector가 지원하는 장치 (예: USB 장치, PTP 장치, USB 메모리 카드 등)
- **사용자** - 장치와 컴퓨터를 다룰 사용자

Endpoint Protector의 서버는 밀접하게 같이 동작하는 다른 부분이 있습니다.

- **Endpoint Protector 하드웨어 또는 가상 어플라이언스** – 운영 시스템, 데이터 베이스 등을 포함
- **웹 서비스** – Endpoint Protector 클라이언트와 통신하고 받은 정보를 저장
- **Endpoint Protector 사용자 인터페이스** – 존재하는 장치, 컴퓨터, 사용자, 그룹 및 전체 시스템에서의 행동을 관리



4. 서버 기능

Endpoint Protector 하드웨어 또는 가상 어플라이언스 설정을 완료되면 할당된 IP 주소로 사용자 인터페이스에 접근합니다.

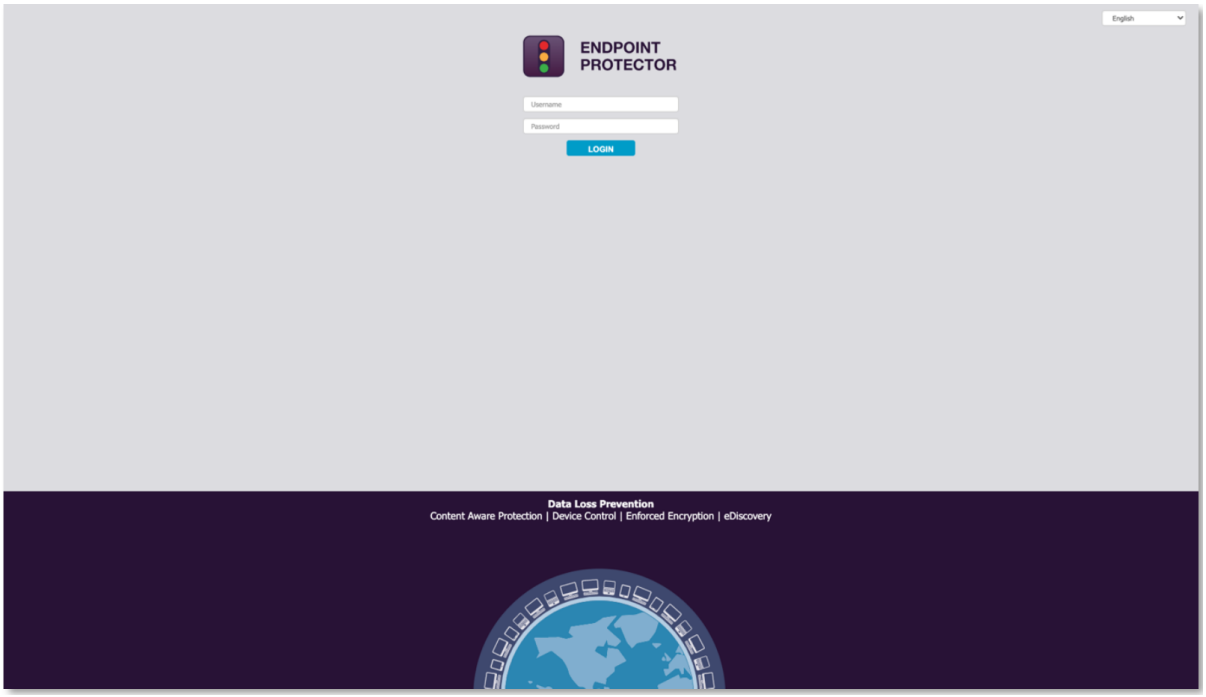
Endpoint Protector 기본 IP 주소는 https://192.168.0.201입니다.

참조: IP 주소는 항상 HTTPS (Hypertext Transfer Protocol Secure)를 사용합니다.

Endpoint Protector의 기본 로그인 계정입니다:

- **사용자 이름**: root
- **비밀번호**: epp2011

설정을 변경하거나 추가 관리자를 만들기 위해서는 **시스템 관리자** 섹션을 참조하시기 바랍니다.



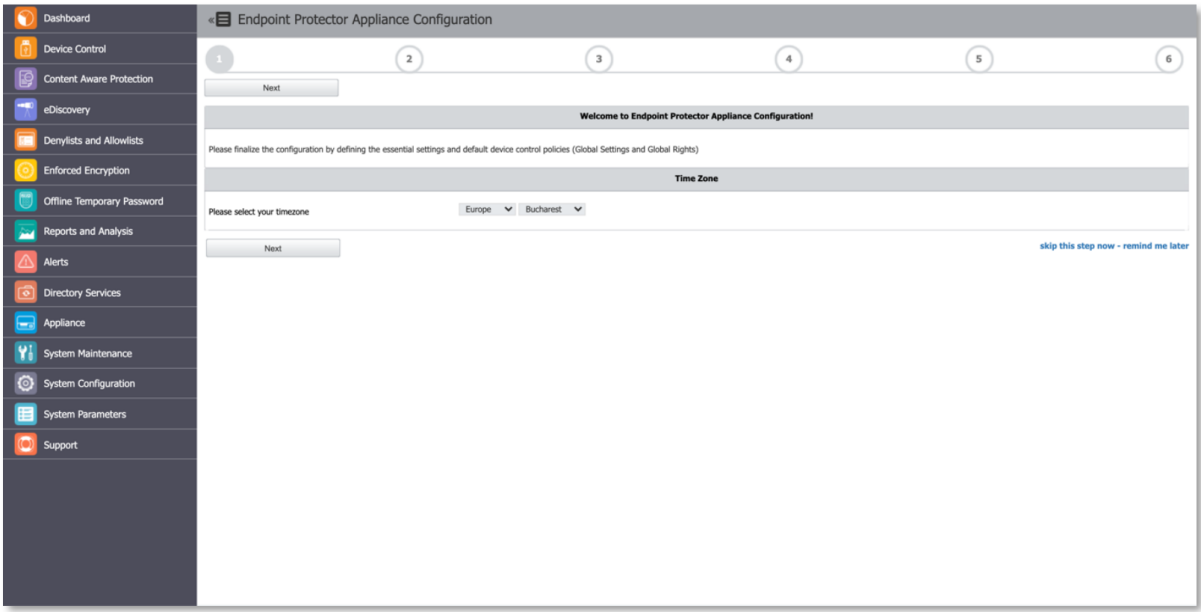
4.1. Endpoint Protector 설정 마법사

설정 마법사는 관리자가 기본 설정을 정의하기 위한 여러가지 절차를 제공합니다. 서버 시간 설정, 라이선스 가져오기, 서버 업데이트 또는 오프라인 패치 업로드, 전체 권한, 이메일 서버 설정, 주요 관리자 상세정보 등이 포함되어 있습니다. 이 설정은 차후에 언제든지 변경이 가능합니다.

설정 마법사는 Endpoint Protector가 한 번도 설정을 한 적이 없는 경우에만 사용할 수 있습니다.

보안 조치로 세션 타임아웃은 300초 (5분) 후에 비활성화 되도록 구현되어 있습니다. 이 시간 동안 동작이 없으면 세션은 타임아웃 되고 관리자는 로그아웃 됩니다.

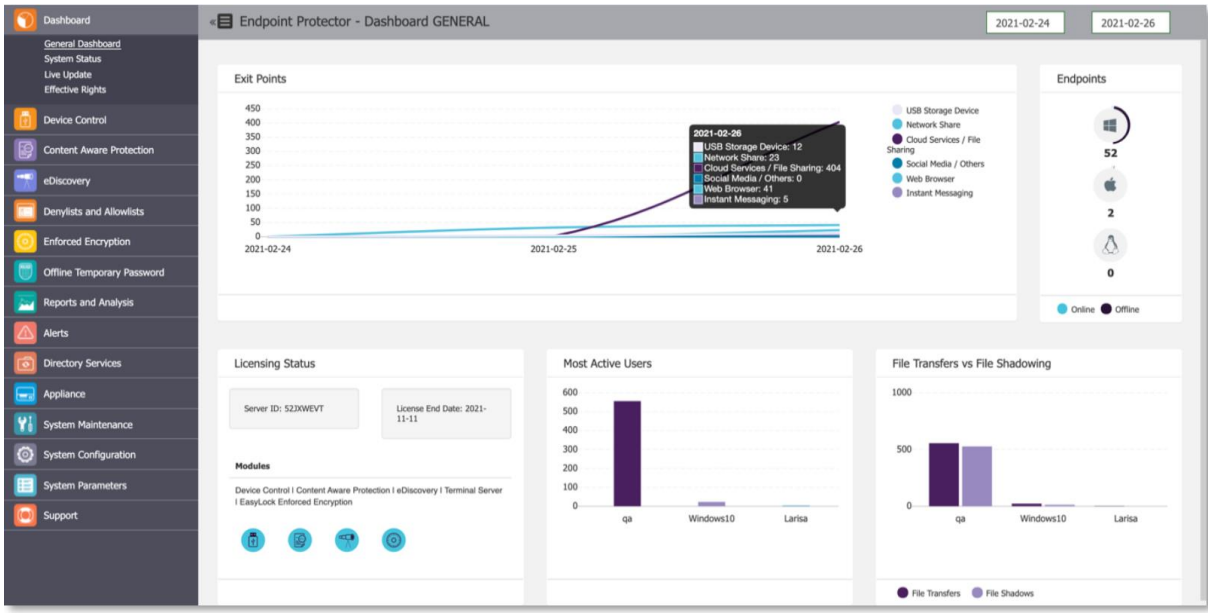
참조: 세션 설정 섹션에서 세션 타임아웃과 세션 카운터를 사용자 정의할 수 있습니다.



4.2. 통합 대시보드

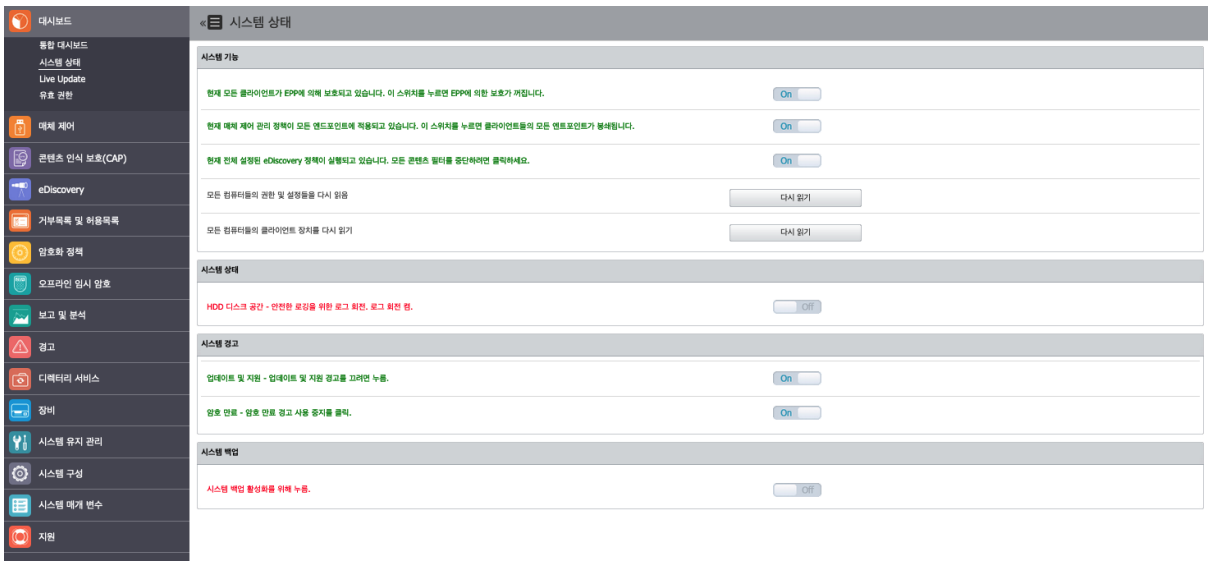
이 섹션에서 Endpoint Protector의 가장 중요한 활동 로그를 한 눈에 볼 수 있도록 시각화와 차트를 제공합니다.

매체 제어, 콘텐츠 인식 보호, eDiscovery 섹션에 대한 추가 정보가 표시 됩니다.



4.3. 시스템 상태

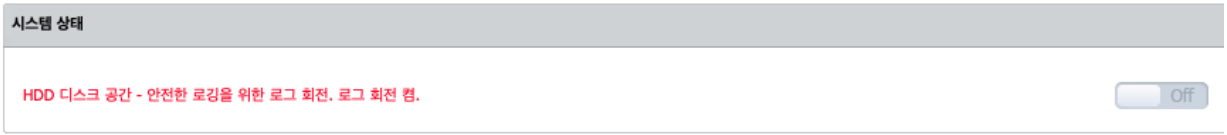
이 섹션에서 시스템 기능, 경고, 백업 상태를 한 눈에 확인할 수 있습니다. 여러 주요 기능을 단지 버튼을 클릭해서 ON 또는 OFF로 변경할 수 있습니다.



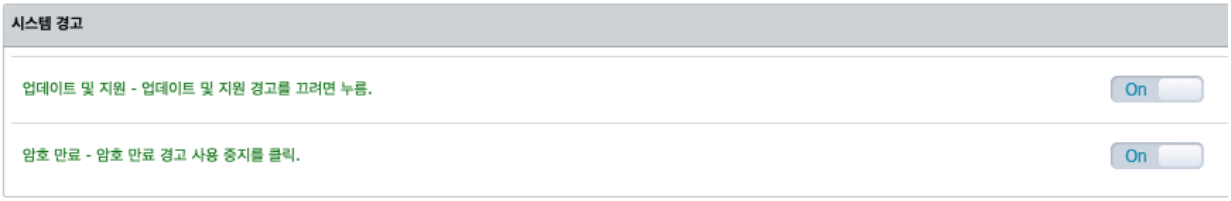
시스템 기능 섹션에서 Endpoint Protector의 특정 모듈 (매체 제어, 콘텐츠 인식 보호, eDiscovery)을 사용할 수 있습니다.

시스템 상태 하위 섹션에서 **HDD 디스크 공간 – 안전한 로깅을 위한 로그 회전**을 사용할 수 있습니다.

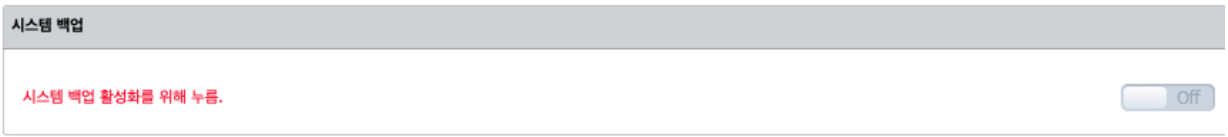
참조: 이 설정을 사용하면 서버 디스코 공간이 특정 퍼센트 (50%에서 최대 90%)가 될 때 오래된 로그는 자동으로 새로운 로그로 덮어쓰기 합니다.



시스템 경고 하위 섹션에서 APNS 인증서, 업데이트, 지원 또는 비밀번호의 만료를 알리는 중요한 경고를 사용할 수 있습니다.



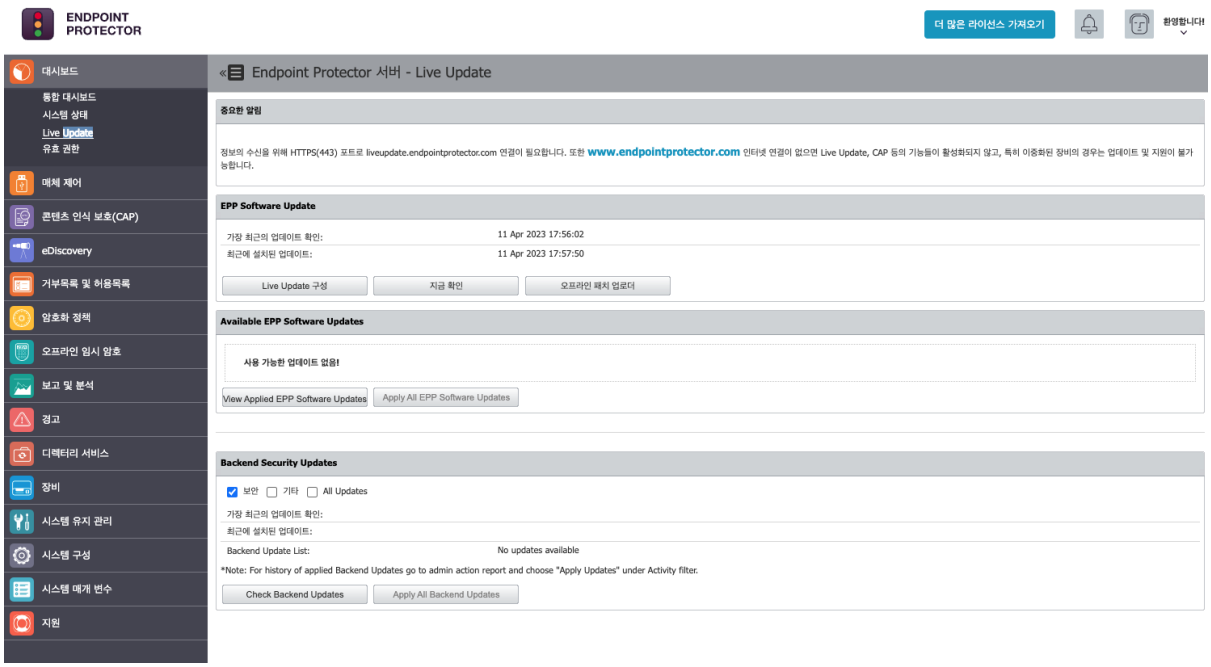
시스템 백업 하위 섹션에서 **시스템 백업**을 사용할 수 있습니다.



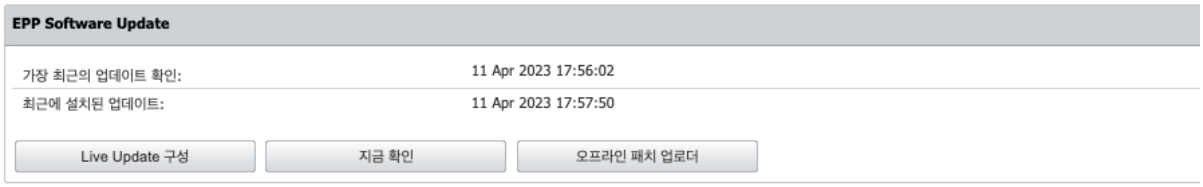
4.4. Live Update

이 섹션에서 Endpoint Protector 서버의 최신 업데이트를 확인하고 적용할 수 있습니다.

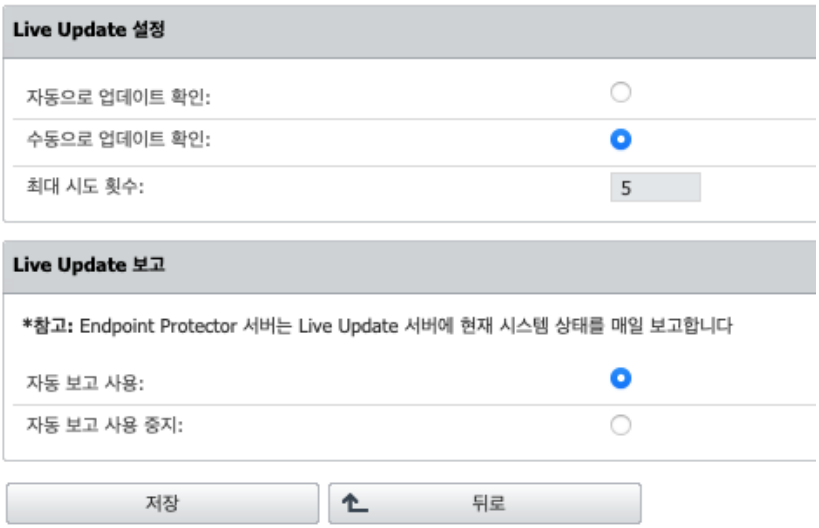
참조: 이 기능은 80번 포트를 통해서 통신합니다. liveupdate.endpointprotector.com (IP: 178.63.3.86) 도메인을 화이트리스트 합니다.



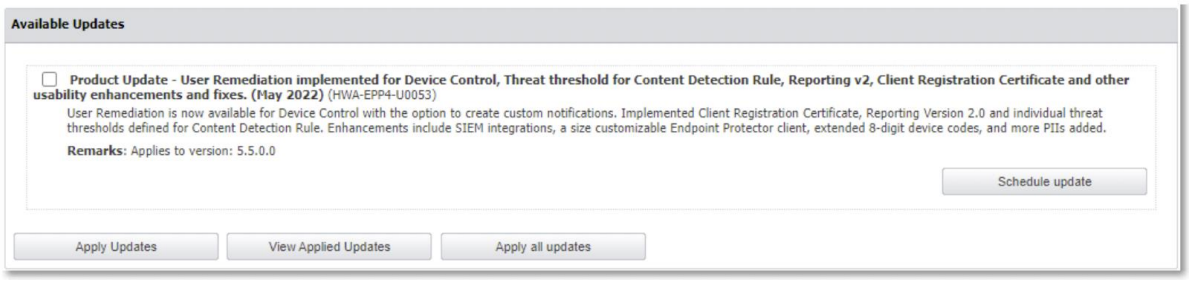
4.4.1. 소프트웨어 업데이트



수동 또는 자동으로 업데이트 선택, 최대 시도 횟수, Live Update 서버에 자동 보고 관리를 하려면 Live Update 구성을 클릭합니다.



Endpoint Protector 서버 업데이트를 검색하기 위해 **지금 확인**을 사용하면 **사용 가능한 업데이트 섹션**에 표시됩니다. **업데이트 적용**으로 업데이트를 선택하고 설치할 수 있고 또는 모든 업데이트 적용으로 모두 업데이트 할 수 있습니다. 설치된 최신 업데이트를 보려면 **적용된 업데이트 보기**를 클릭하시기 바랍니다.



컴퓨터에서 오프라인 패치를 선택하는 **오프라인 패치 업로더** 옵션을 사용해서 Endpoint Protector 최신 버전에 성공적으로 설치할 수 있습니다.

참조: 오프라인 패치는 각 총판사에 문의하시기 바랍니다.

중요: Endpoint Protector 서버를 5206 이전 버전과 근접 OS 이미지에서 5.7.0.0 서버 버전으로 업

그레이드하기 전에 데이터베이스 파티션을 사용할 필요가 있습니다. 각 총판사에 문의하시기 바랍니다.

4.4.2. 보안 업데이트

보안 업데이트의 다른 형식을 체크 및 적용하기, 최신 업데이트 체크 또는 설치 정보 보기, 가능한 업데이트 목록 보기에 이 섹션을 사용할 수 있습니다.

참고: 보안 업데이트 옵션은 고객이 호스트하는 인스턴스 (예: AWS, Google 등)에서만 사용 가능합니다. 운영 체제 및 커널 업그레이드는 예외입니다.

중요: 업데이트는 사전에 테스트되지는 않지만 공식 Linux 리포지토리에서 가져옵니다.

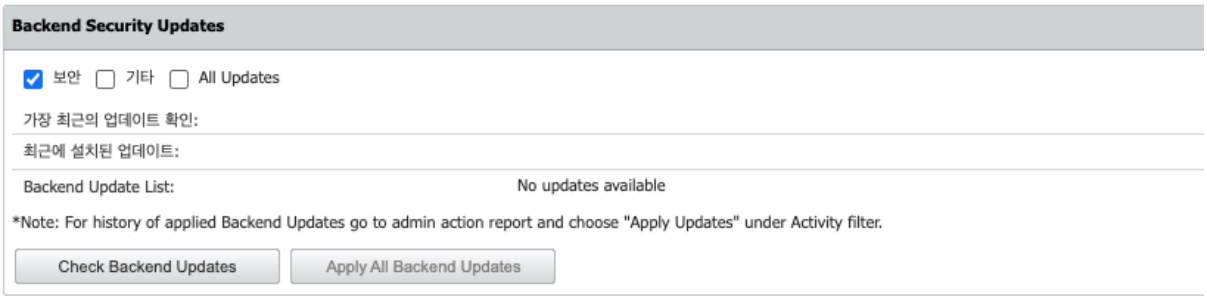
이 업데이트가 시스템을 손상시키지 않게 하려면 다음 액션을 따르시기 바랍니다:

- 먼저 테스트 환경에서 업데이트 테스트하기
- VM 스냅샷 만들기
- 시스템 유지관리 섹션에서 System Backup v2 백업 만들기

보안 업데이트 형식 중 하나를 선택하고 **Check Updates**를 클릭하시기 바랍니다:

- **보안** – 설치된 패키지의 모든 보안 관련 업데이트 (심각 및 높음)를 업데이트합니다.
- **기타** – 제 3 라이브러리, 커널, OS 패키지, MySQL 데이터베이스에서 사용 가능한 모든 업데이트를 다운로드하고 적용합니다.
- **모든 업데이트** – **정보** 및 **선택/미분류** 업데이트를 다운로드하고 적용합니다.

만약 업데이트가 가능하다면 **Apply Updates**를 클릭하시기 바랍니다:



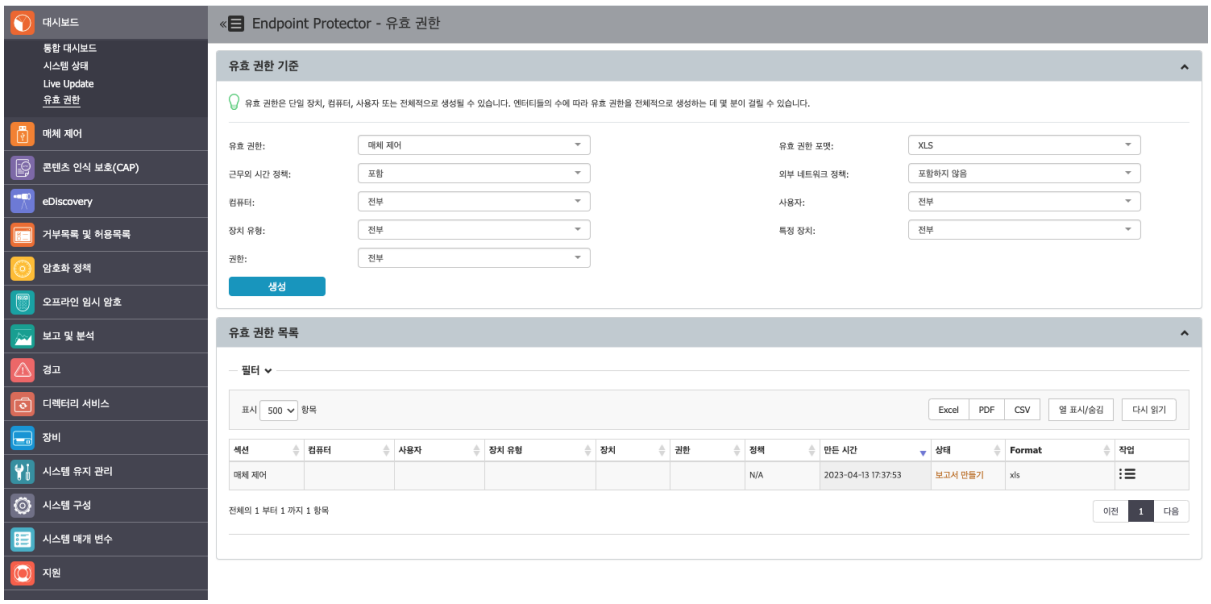
참고: 적용된 백엔드 업데이트 기록에 관련해서는 작업 관리자 보고서로 이동 후 필터에서 Apply Update를 선택합니다.

중요: 패치의 특성으로 일부 업데이트는 Endpoint Protector 서버 또는 백그라운드의 다른 하위 서비스를 자동으로 재시작할 수 있습니다.

4.5. 유효 권한

이 섹션은 현재 적용된 매체 제어 또는 콘텐츠 인식 보호 정책을 보여 줍니다. 여러분이 선택한 **유효 권한 기준**을 기반으로 권한, 사용자, 컴퓨터, 장치 유형, 특정 장치, 보고서 유형 (PDF 또는 XLS), 근무외 시간 정책, 외부 네트워크 정책 등의 정보를 볼 수 있습니다.

한 번 보고서가 만들어지면 **작업** 열에서 다운로드 또는 삭제 할 수 있습니다.

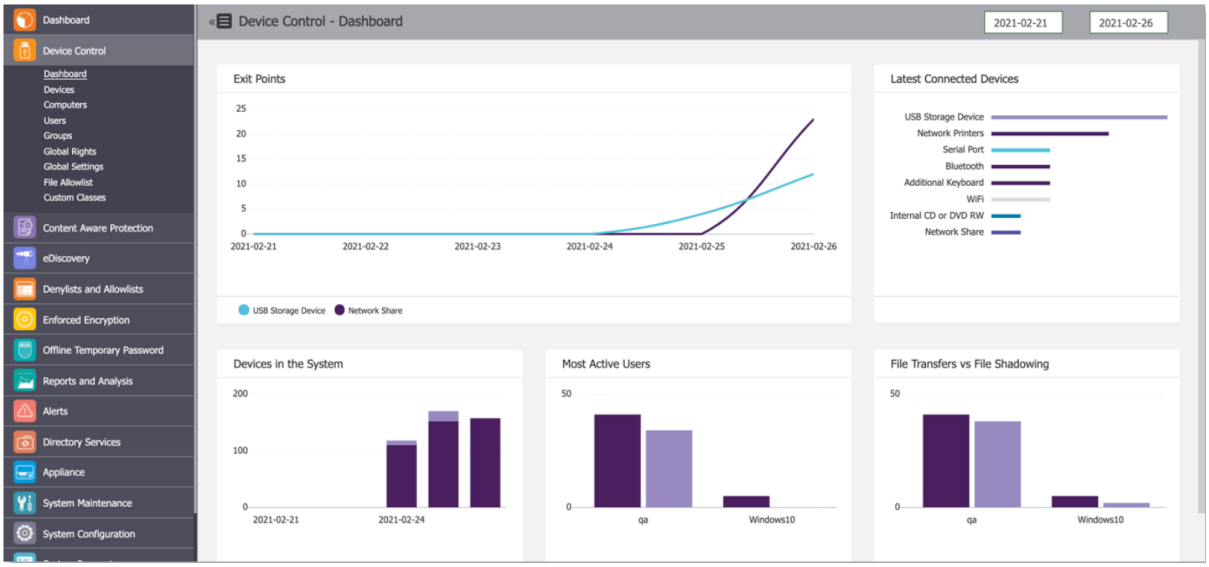


5. 매체 제어

이 섹션에서 여러분은 시스템의 모든 객체, 하위 권한 및 설정을 관리할 수 있습니다. Endpoint Protector 클라이언트와 심층 패킷 검사(DPI) 설정과 같은 매체 제어의 다른 설정 유형을 관리할 수 있습니다. Endpoint Protector의 첫 번째 보안 계층으로 제공된 모든 구성은 기본으로 활성화되어 있습니다.

5.1. 대시보드

이 섹션은 Endpoint Protector 객체에 관련된 내용을 그래픽과 차트의 형태로 전체적으로 빠르게 볼 수 있도록 제공합니다. 오른쪽 상단의 달력으로 시각화에 사용되는 시작 날짜와 끝나는 날짜를 선택할 수 있고 실시간으로 데이터를 볼 수 있습니다.



5.2. 장치

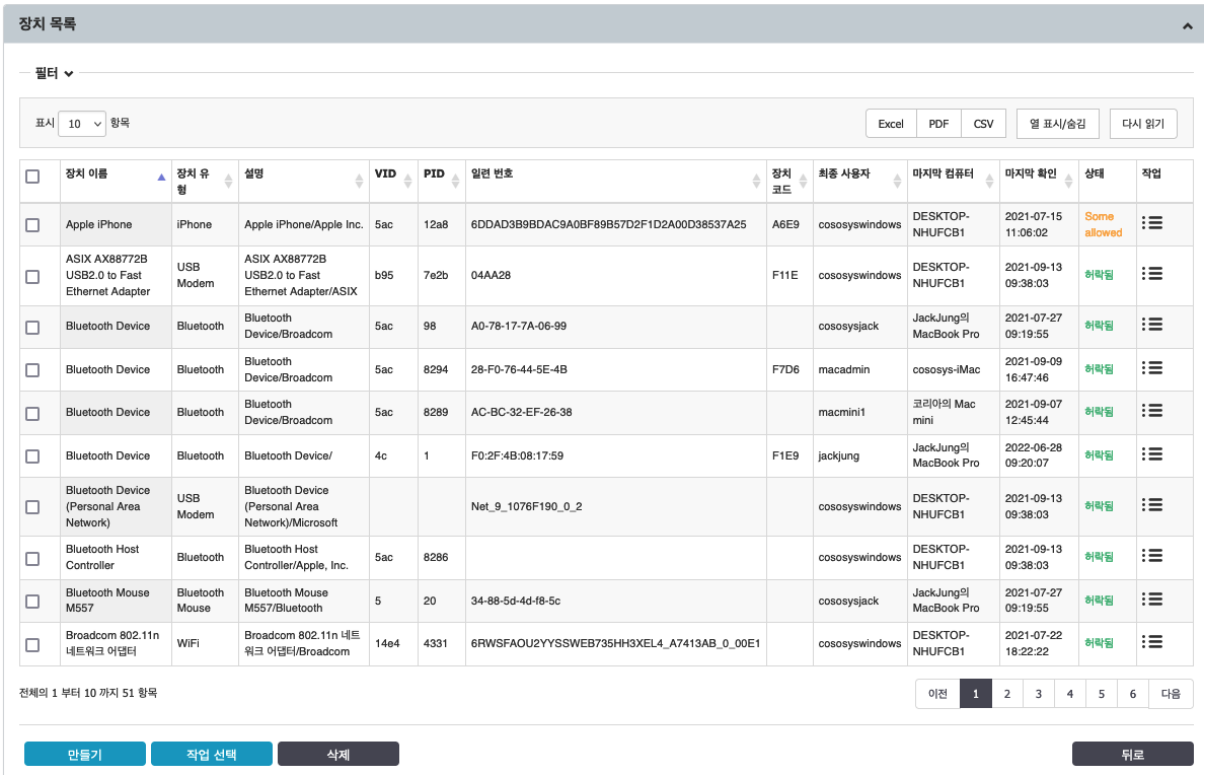
이 섹션에서 여러분은 시스템의 모든 장치를 필터링해서 볼 수 있고 Excel, PDF, CSV로 내보내기

할 수 있습니다. **작업** 열을 사용해서 편집, 권한 관리, 기록 보기 및 특정 장치를 삭제할 수 있습니다.

여러분은 **상태** 열에서 색을 기반으로 각 장치의 권한을 볼 수 있습니다.

- **빨강색**은 장치가 시스템에서 차단되었다는 의미입니다.
- **초록색**은 장치가 컴퓨터 또는 사용자에서 허용되었다는 의미입니다.
- **노란색**은 일부 제한된 컴퓨터 또는 사용자에서 허용되었다는 의미입니다.

참고: 보호되는 컴퓨터에 연결된 새로운 모든 장치는 데이터베이스에 자동으로 추가되고 나중에 변경될 수 있는 첫 번째 사용자에 할당됩니다.



장치 정보를 제공하는 목록에 새로운 장치를 수동으로 추가하기 위해서 **만들기**를 클릭합니다 – 장치 이름, 식별 이름, PID, 구분, 설명, VID, 일련 번호, 사용자 클래스.

장치 목록 내보내기, 목록 내보내기 예약, 장치 내보내기 (JSON), 장치 가져오기 (JSON), 기기 코드 갱신을 위해서 **작업 선택**을 사용합니다.

JSON 포맷으로 장치 내보내기/가져오기 기능은 Endpoint Protector 서버에서 또 다른 Endpont Protector 서버로 장치를 관리할 수 있도록 허용하고 장치 권한과 그룹을 연관시키기 위한 목적입니다.

- 두 서버에 같은 그룹이 존재하면 가져온 장치 또한 접근 권한을 유지할 것입니다.
- 그룹이 같지 않다면 장치는 여전히 가져온 상태이나 접근 권한은 무시될 것입니다.

여러분은 또한 Active Directory 에서 장치를 가져올 수 있습니다.

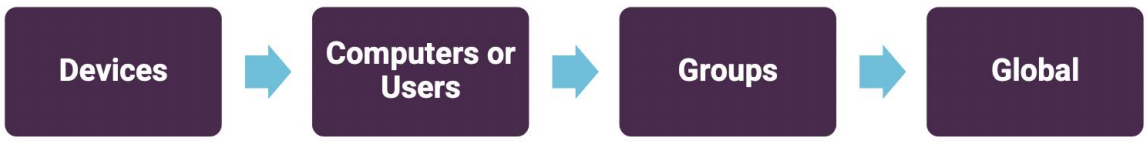
참고: Active Directory에 관련된 자세한 내용은 **디렉터리 서비스** 를 참조하시기 바랍니다.

5.2.1. 우선 순위

다른 장치 권한 설정이 없으면 권한은 장치 유형 (USB 저장 장치, 디지털 카메라, iPod, Thunderbolt, Chip Card 장치 등) 마다 설정된 기본 전체 권한을 상속 받습니다.

참고: 더 자세한 내용은 **장치 유형** 을 참조하시기 바랍니다.

모든 객체에 세부적으로 장치 권한을 구성하려면 우선 순위는 아래와 같습니다. 가장 높은 쪽부터 시작합니다.

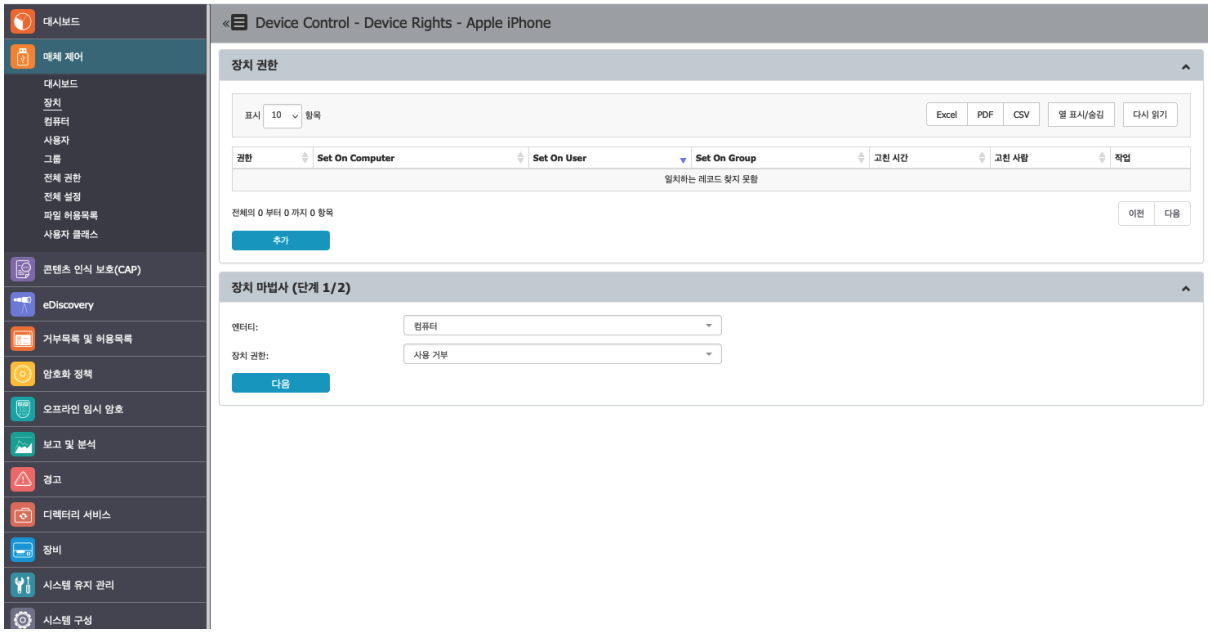


예제: 전체 권한이 모든 컴퓨터에 대해서 특정 장치에 차단으로 설정되어 있고 한 컴퓨터는 특정 장치를 허용하도록 설정이 되어 있으면 특정 장치에 허용으로 설정된 컴퓨터는 해당 장치를 허용합니다.

5.2.2. 장치 권한

특정 컴퓨터, 그룹, 사용자에 대한 장치 권한을 관리하기 위해서 **작업** 열에서 **권한 관리**를 선택합

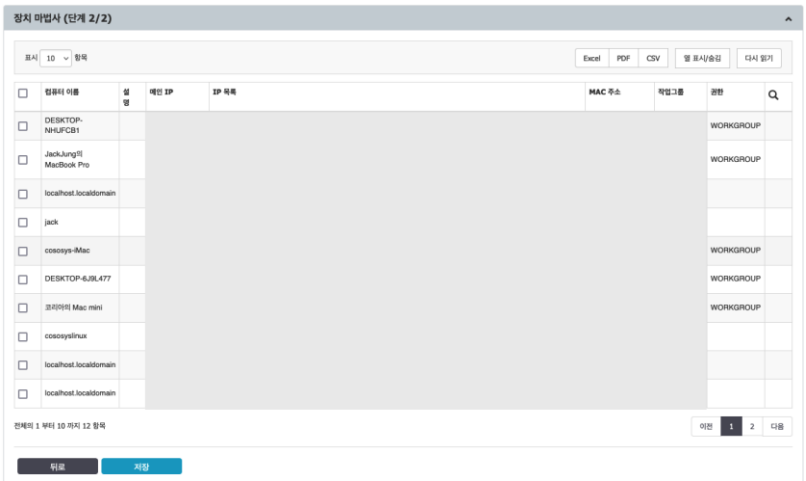
니다.



장치를 선택한 후에 원하는 사용자, 컴퓨터 또는 그룹에 특정 권한을 할당하기 위해서 다음 단계를 따릅니다.

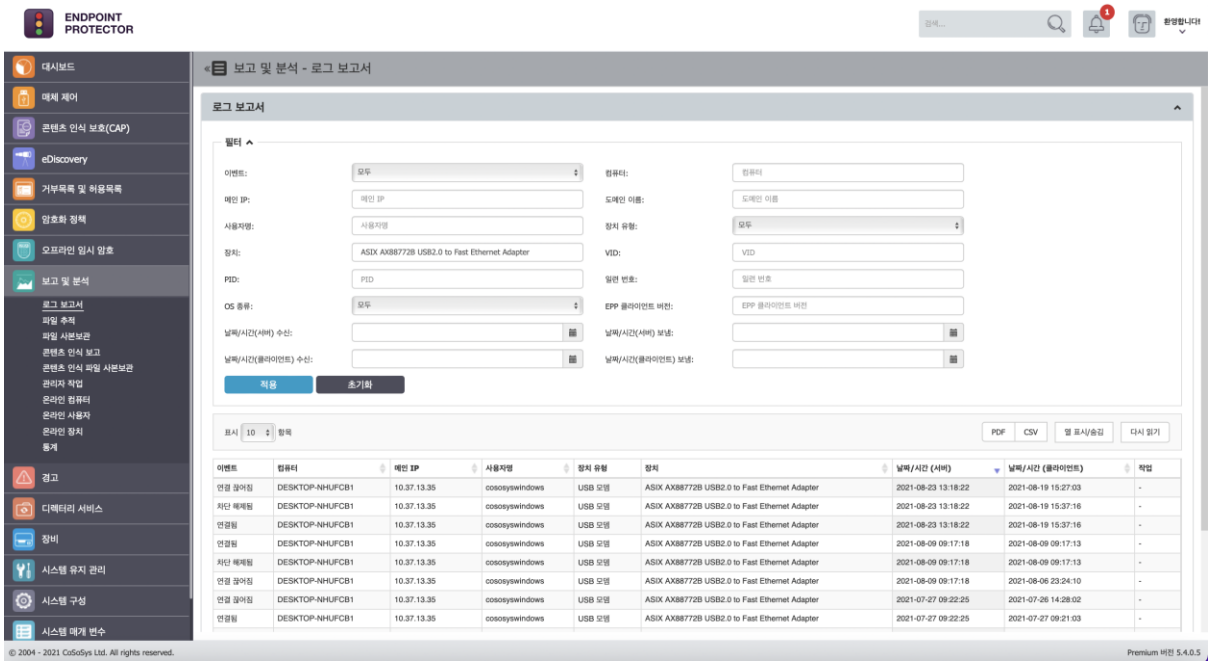
1. **엔터티** 및 **장치 권한** 선택

2. **엔터티** (컴퓨터, 그룹, 사용자) 선택



5.2.3. 보기 기록

이 세션에서 여러분은 보기 기록을 선택해서 장치 기록을 볼 수 있습니다. 각 장치로 필터링 되어 로그 보고서 페이지에 표시됩니다.

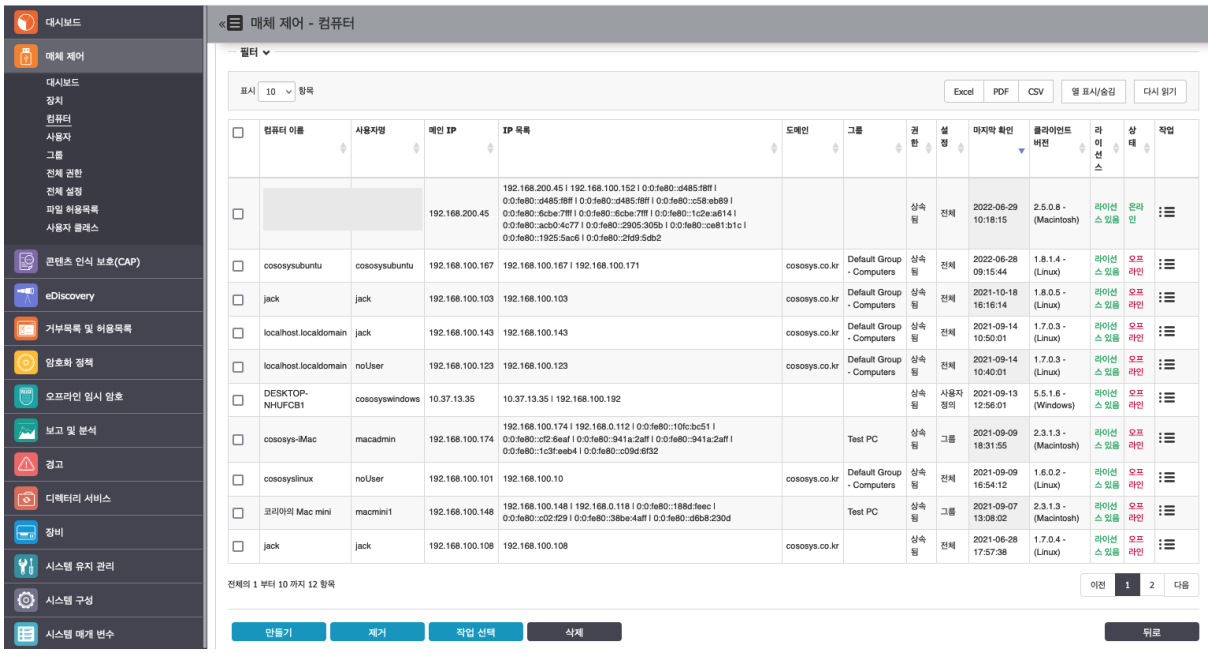


5.3. 컴퓨터

이 섹션에서 여러분은 시스템의 모든 컴퓨터를 관리할 수 있습니다. Endpoint Protector 클라이언트가 배포된 새로운 컴퓨터는 자동으로 데이터베이스에 추가되어 관리가 가능합니다.

시스템 유지 관리, 내보내기된 엔터티들 세션에서 각 엔터티 (컴퓨터/사용자/그룹)에 대한 심층 패킷 검사(DPI) 상태와 심층 패킷 분석(DPI)가 사용된 엔터티를 볼 수 있는 설정 보고서를 다운로드 받을 수 있습니다.

Endpoint Protector 클라이언트가 배포된 모든 새로운 컴퓨터는 자동으로 데이터베이스에 추가되어 관리가 가능합니다.



Endpoint Protector 클라이언트는 자체 등록 메커니즘을 가지고 있습니다. 이 프로세스는 클라이언트 소프트웨어가 클라이언트 컴퓨터에 설치된 후에 바로 동작합니다. 그리고 나서 클라이언트는 시스템에 존재하는 서버와 통신할 것입니다. 서버는 데이터베이스에 컴퓨터 관련 정보를 저장하고 라이선스를 할당합니다.

참고: 자체 등록 메커니즘은 컴퓨터 라이선스 모듈이 변경 될 때 마다 동작합니다. 그 때마다 응용프로그램 클라이언트는 재설치 됩니다. 컴퓨터 소유자는 자체 등록 프로세스에 저장되지 않습니다.

라이선스에 관련된 더 자세한 내용은 **시스템 라이선스** 챕터를 참조 하시기 바랍니다.

컴퓨터는 컴퓨터 매개 변수 (메인 IP, IP 목록, MAC, 도메인 또는 워크그룹)으로 식별되지만 이름과 설명 같은 정보 또한 필수적입니다.

컴퓨터는 컴퓨터를 다루는 첫 번째 사용자를 기본값으로 할당합니다. 그러나 이것은 차후에 변경할 수 있고 컴퓨터에 로그인하는 사용자를 기반으로 자동으로 업데이트됩니다.

참고: 시스템 제한으로 컴퓨터 시리얼 번호는 가상 머신에서 주어지지 않을 수 있습니다.

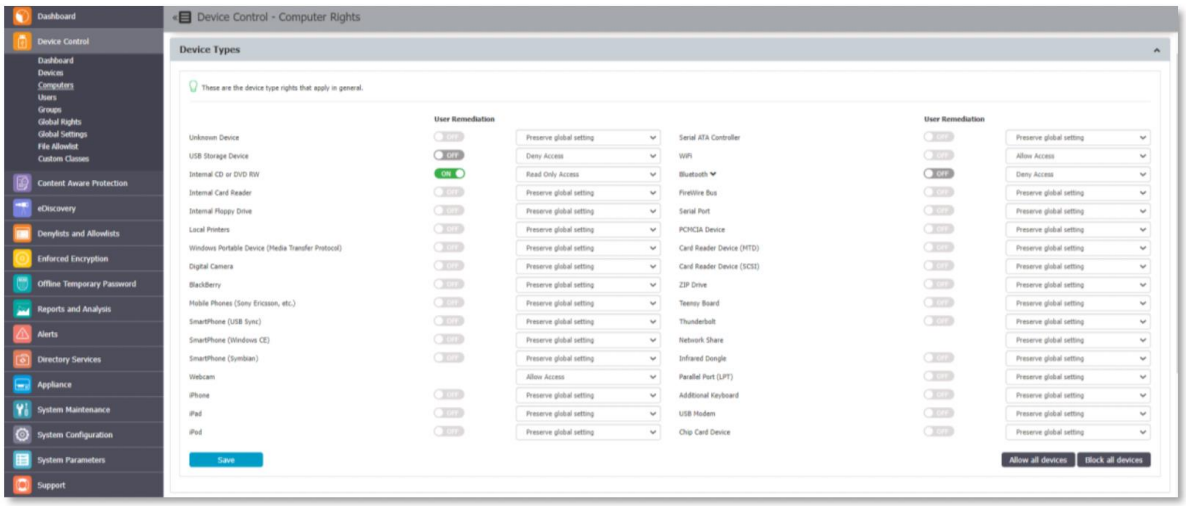
컴퓨터 매개 변수와 위에서 언급된 정보 또는 Active Directory 에서 가져온 컴퓨터를 제공하여 언제든 새로운 컴퓨터를 수동으로 만들 수 있습니다.

아래와 같이 컴퓨터를 할당할 수 있습니다.

- ❿ 그룹 예: 같은 사무실의 있는 여러 컴퓨터
- ❿ 구분 그룹의 대안 조직

5.3.1. 컴퓨터 권한

컴퓨터 권한은 특정 컴퓨터의 **작업** 열에서 **권한 관리**를 선택해서 컴퓨터 권한을 관리할 수 있습니다. 이 섹션은 컴퓨터에 구축이 되었고 어느 장치 유형 및 특정 장치가 허용될 수 있는지 명시합니다.



표준 매체 제어 권한은 장치 유형 및 이미 존재하는 장치 섹션을 포함합니다. 이는 일반적으로 장치 권한에만 사용됩니다.

표준 매체 제어 권한에 추가하여 전체 설정을 사용하면 근무외 시간 및 외부 네트워크 환경을 대비하는 정책을 만들 수 있습니다.

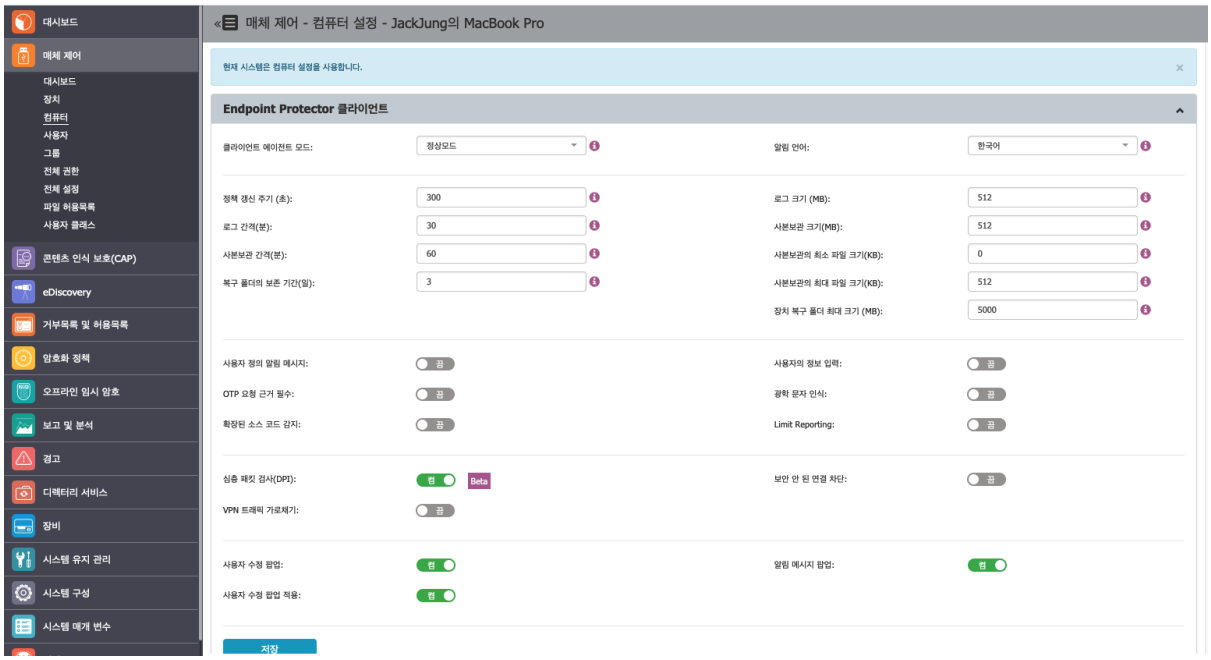
장치 유형과 특정 장치 (표준, 외부 네트워크, 근무외 시간)에 대한 자세한 내용은 **장치 유형** 챕터를 참조하시기 바랍니다.

참고: 전체 권한 복원 버튼은 하위 권한을 전체 권한으로 복원할 때 사용합니다. 한 번 이 버튼을 누르면 현재 단계의 권한이 모두 전체 권한을 따르고 시스템은 다음 단계의 권한에 사용됩니다. 복원을 사용하면 이 단계에 설정된 이미 존재하는 장치는 삭제됩니다.

5.3.2. 컴퓨터 설정

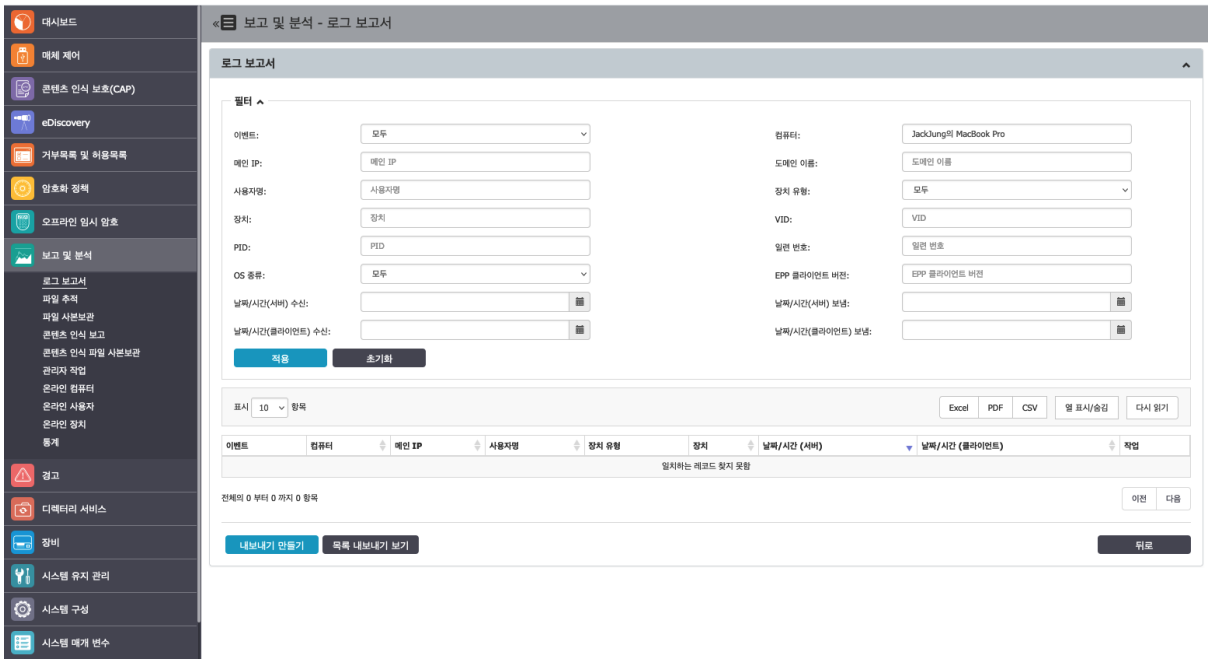
이 섹션은 각 컴퓨터 설정을 편집할 수 있습니다.

모든 컴퓨터에 대한 사용자 정의 설정은 컴퓨터가 수동 설정 정의 없이 완벽하고 정확하게 기능을 수행하기 때문에 불필요합니다. 그룹이 가지고 있는 설정을 받아오거나 아니면 시스템에 기본 값으로 되어 있는 전체 설정을 받아 올 수 있습니다. 전체 설정 역시 추후에 변경이 가능합니다.



5.3.3. 컴퓨터 기록

이 섹션에서 컴퓨터 기록 보기 작업을 선택해서 컴퓨터 기록을 볼 수 있습니다. 각 컴퓨터 별로 로그 보고서 페이지에 나타납니다.



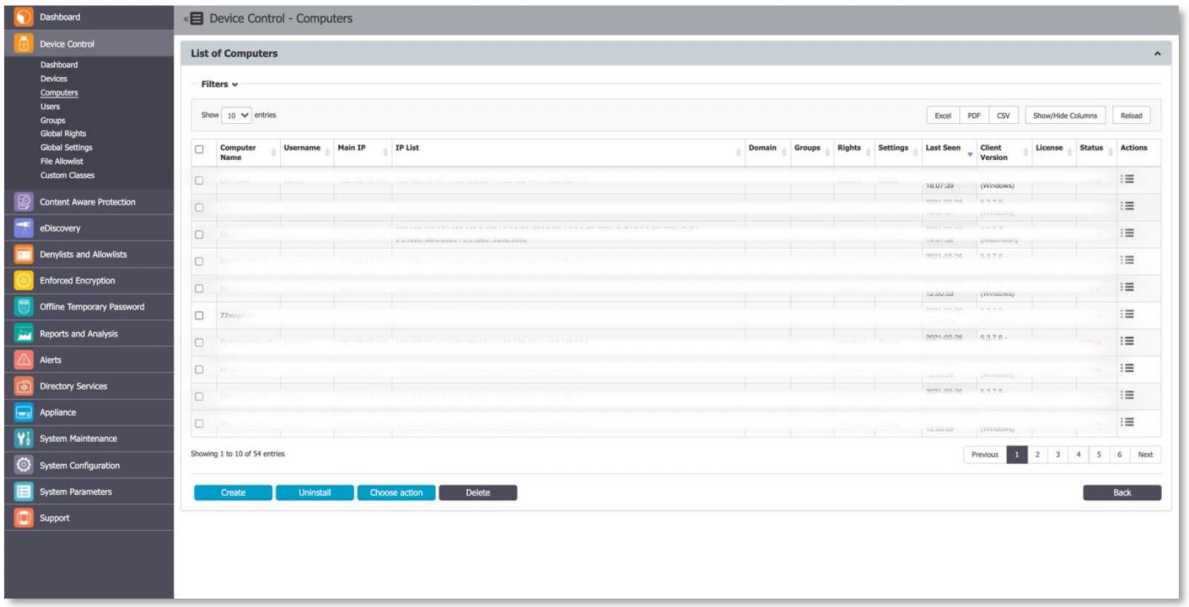
5.3.4. 터미널 서버 및 씬 클라이언트

씬 클라이언트와 Windows 터미널 서버 사이의 RDP 스토리지에 파일 전송을 제어가 Endpoint Protector를 통해서 가능합니다. 아래에서 세부 내용을 확인하시기 바랍니다.

5.3.4.1. 초기 설정

프로세스는 매체 제어 > 컴퓨터 에서 **터미널 서버로 지정** 으로 시작됩니다.

터미널 서버로 시스템의 컴퓨터를 선택한 후에 "Yes"가 식별이 쉽도록 표시될 것입니다. 아래 이미지를 참조 부탁드립니다.

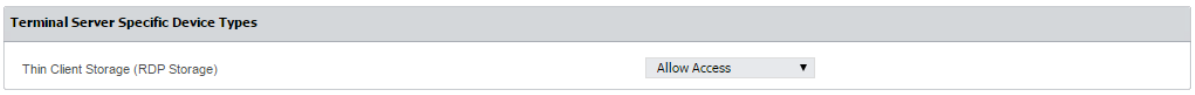


참고: 이 작업으로 대상이 될 수 있는 컴퓨터는 엄격하게 터미널 서버 역할을 수행할 수 있도록 적절하게 구성된 Windows 서버입니다.

터미널 서버로 이 작업이 지정되고 수행되려면 적어도 하나의 터미널 서버 라이선스가 있어야 합니다.

터미널 서버가 성공적으로 지정되면 새로운 장치 유형이 매체 제어, 컴퓨터, 컴퓨터 권한에서 편집을 선택할 때 나타날 것입니다.

터미널 서버 장치 유형의 설정은 '전체 설정 유지', '사용 허용', '사용 거부', '읽기 전용 사용' 으로 나뉩니다.

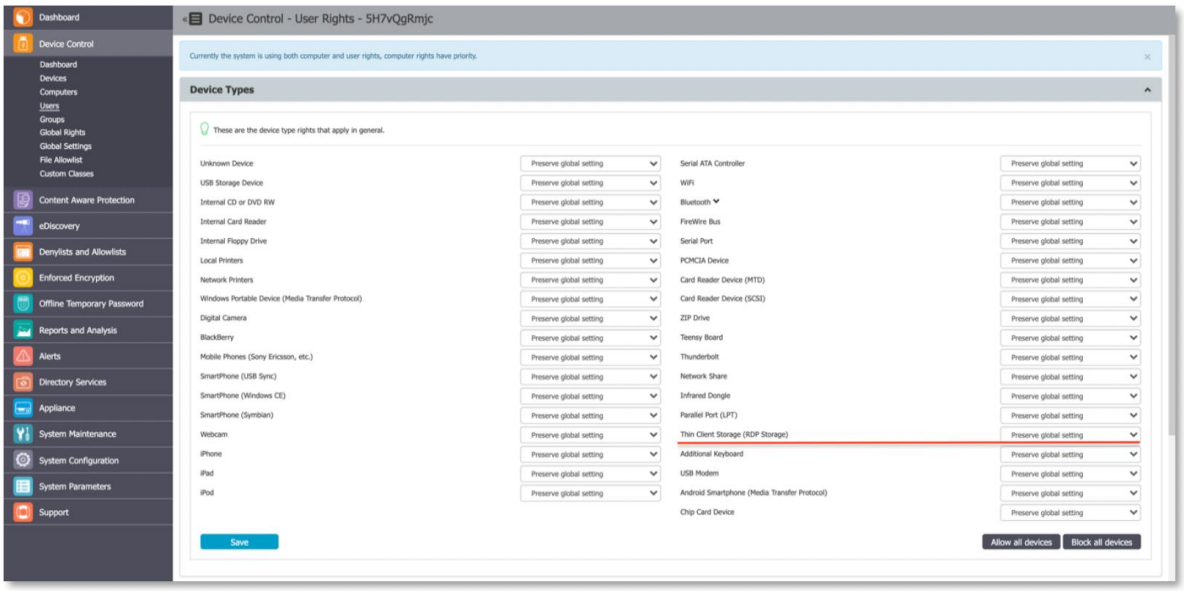


RDP 저장소 장치 유형의 '사용 허용'은 RDP 터미널 서버에 연결된 모든 사용자가 그들의 로컬 디스크 또는 USB와 같은 공유 저장장치에 파일을 전송할 수 있습니다.

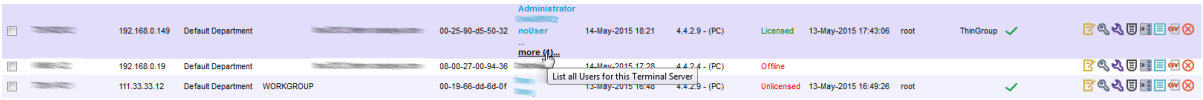
이와 반대로 RDP 저장소 장치 유형의 '사용 거부'는 RDP 터미널 서버에 연결된 어떤 사용자도 그들의 로컬 디스크 또는 USB와 같은 공유 저장장치에 파일을 전송할 수 없습니다.

참고: 사용자 우선순위로 권한 정책을 사용자 로그인에 적용하기 위해서 시스템 구성, 시스템 설정, Endpoint Protector 권한 기능의 설정 바에서 사용자 권한 사용을 사용합니다.

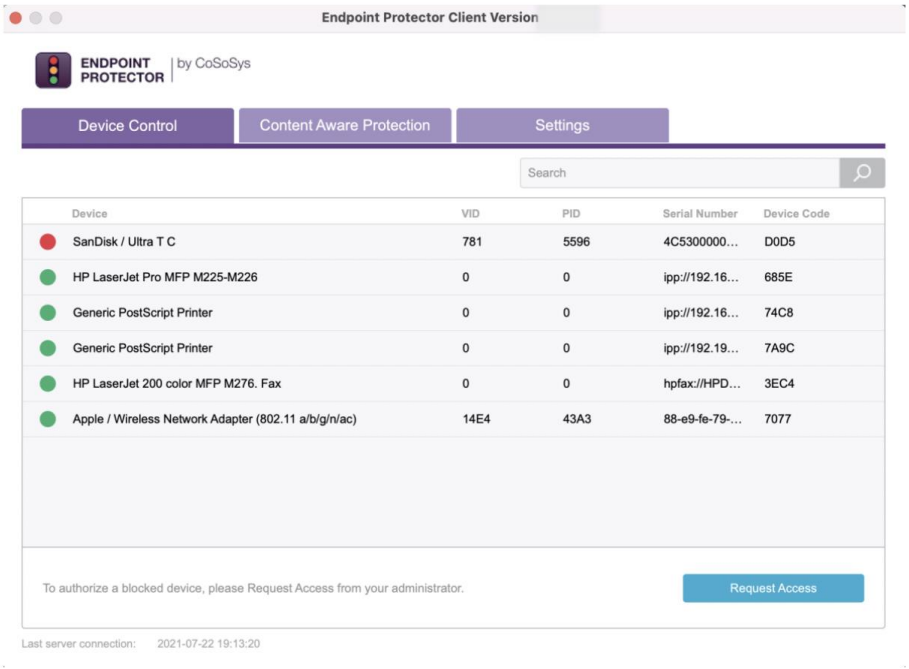
두 번째로 '매체 제어 > 사용자 > 권한 관리'에서 Endpoint Protector의 모든 사용자에 씬 클라이언트 (RDP 저장소)로 명명된 추가 장치 유형이 존재할 것입니다.



여러 사용자가 터미널 서버의 활성 사용자로 인식이 될 수 있습니다. 그래서 이 권한 설정은 특정 사용자의 접근 정책을 만드는 강력한 도구로 사용될 수 있습니다.

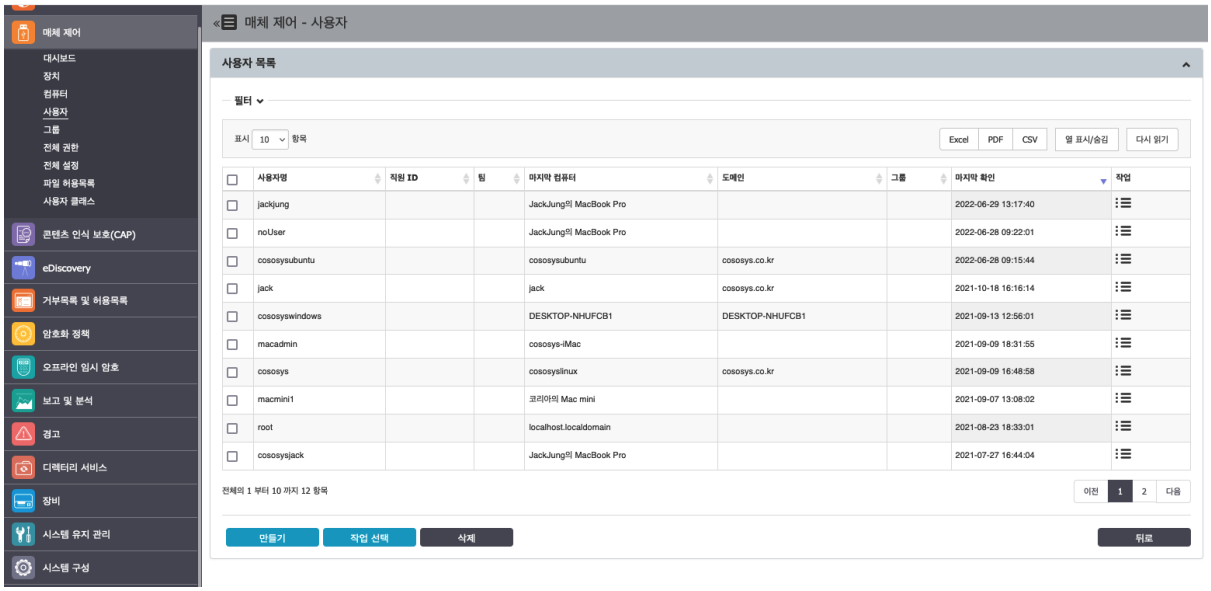


윈도우 터미널 서버에서 Endpoint Protector 클라이언트는 아래와 같이 하나 또는 여러 씬 클라이언트를 공유하는 RDP 스토리지 디스크로 표시될 것입니다.



5.4. 사용자

이 섹션에서는 시스템의 모든 사용자를 관리할 수 있습니다. 사용자는 Endpoint Protector 클라이언트 소프트웨어가 설치된 컴퓨터에 로그인한 마지막 사용자로 정의합니다. 새로운 사용자는 자동으로 데이터베이스에 추가되어서 관리가 가능합니다.



사용자는 이름 (사용자, 성, 이름), 부서, 연락처 (전화번호, 이메일) 및 기타 정보를 확인하고 자동

으로 컴퓨터에 등록이 됩니다.

관리자는 위에 언급된 사용자 매개 변수를 이용하여 언제든지 새로운 사용자를 수동으로 만들 수 있습니다. 사용자는 또한 Active Directory에서 Endpoint Protector로 가져올 수 있습니다.

Active Drirectory에 대한 더 자세한 정보는 **디렉터리 서비스** 챕터를 참조하시기 바랍니다.

Endpoint Protector의 설치 프로세스에서 기본 값으로 만들어진 두 가지 사용자가 있습니다.

- **noUser** – 컴퓨터에 로그인한 사용자가 없을 때 모든 이벤트를 수행하기 위해 연결된 사용자입니다. 컴퓨터에 접속한 원격 사용자의 이름은 기록되지 않으며 그들의 이벤트는 noUser 이벤트로 저장됩니다. noUser 이벤트의 또 다른 발생은 특정 컴퓨터에 접속한 사용자가 없을 때 장치에 접속한 자동 스크립트 / 소프트웨어가 있는 경우입니다.
- **autorunUser** – 특정 장치가 윈도우에서 시작하는 인스톨러를 가리킵니다. 운영 체제에서 자동 시작이 되었을 때 특정 장치에서 시작하는 프로그램이 만든 모든 이벤트에 관련된 사용자입니다.

중요: OS에 따라서 추가 시스템 사용자가 다음과 같이 나타날 수 있습니다:

- _mbsetupuser (macOS 업데이트 중)
- 65535, 62624 등 (Linux 화면 잠금 중)

작업 열은 편집, 권한 관리, 기록 및 삭제와 같은 사용자 관리와 관련된 여러 옵션을 제공합니다.

5.4.1. 사용자 권한

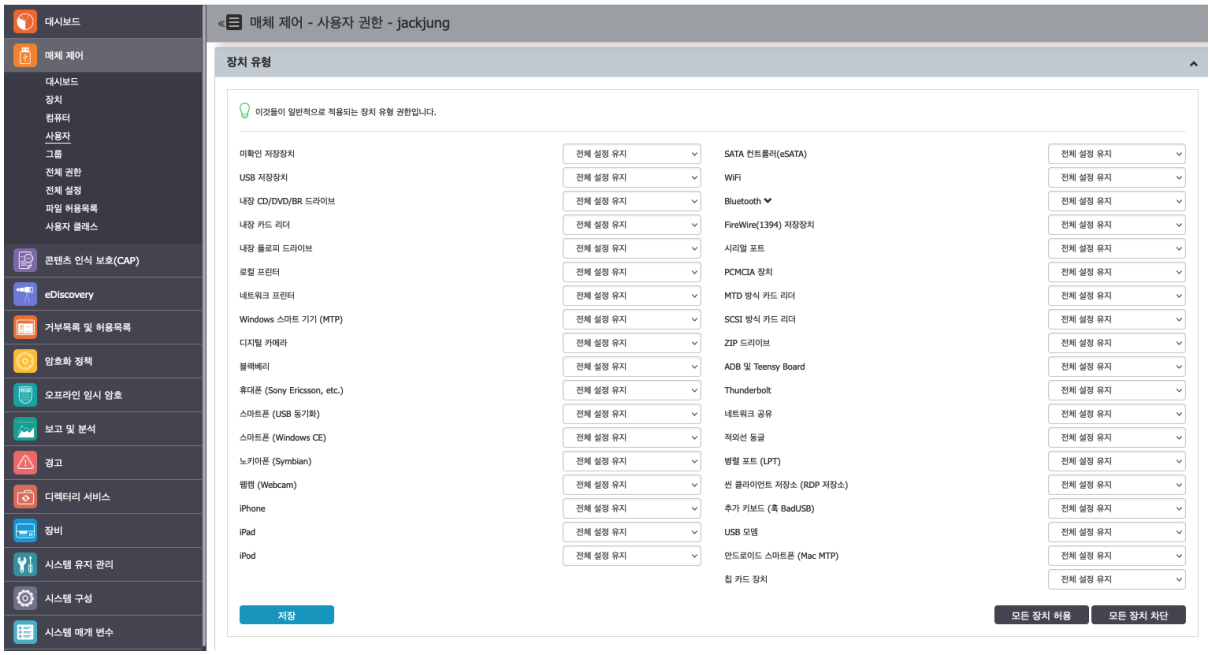
사용자 권한은 특정 컴퓨터의 작업 열에서 권한 관리를 선택해서 접근할 수 있습니다. 이 섹션은 관리자가 특정 장치 유형과 특정 장치의 권한을 설정하는 것을 허용합니다.

이 섹션은 사용자 위주로 구축되어 관리자는 장치 유형을 특정하고 또한 특정 장치에 접근할 수 있도록 허용합니다.

표준 매체 제어 권한은 장치 유형과 이미 존재하는 장치 섹션을 포함합니다. 일반적으로 유일한

장치 권한으로 사용됩니다.

표준 매체 제어 권한에 추가하여 전체 설정이 활성화되어 있으면 관리자는 외부 네트워크 및 근무외 시간 환경에 대응 정책을 만들 수 있습니다.

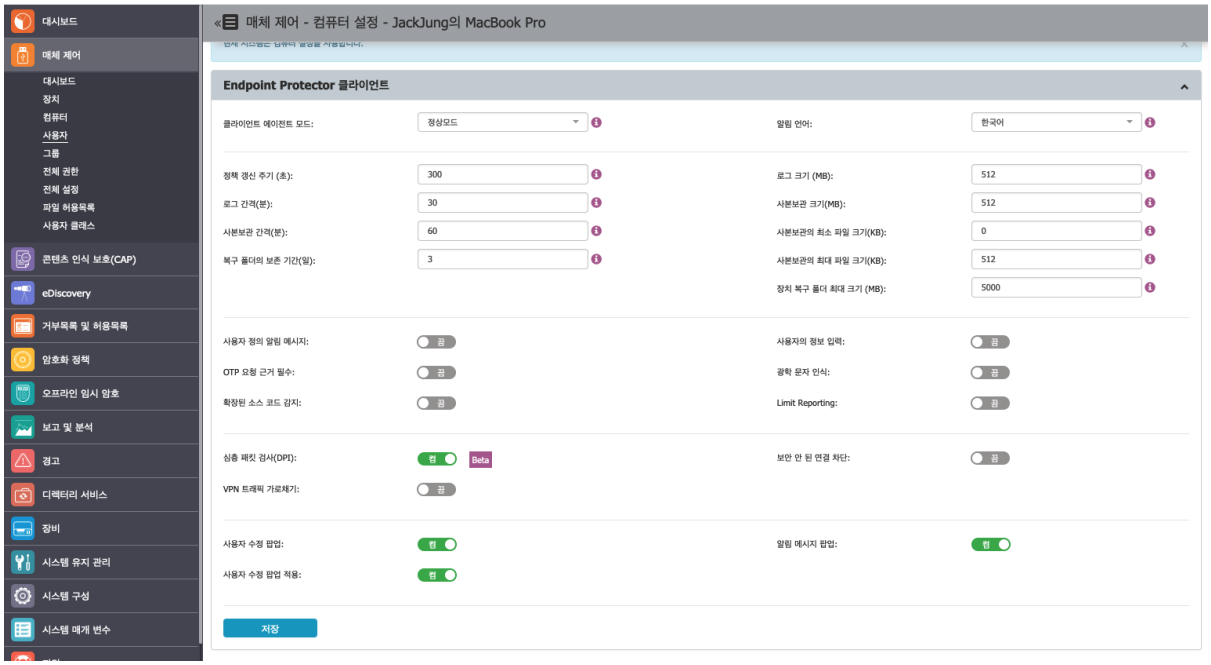


참고: 전체 권한 복원 버튼은 하위 계층 권한을 되돌릴 때 사용할 수 있습니다. 이 버튼을 누르면 해당 계층의 모든 권한은 전체 설정을 유지하도록 설정될 것이고 시스템은 권한의 다음 계층을 사용할 것입니다.

복원을 하면 해당 계층에 추가된 모든 이미 존재하는 장치는 삭제될 것입니다.

5.4.2. 사용자 설정

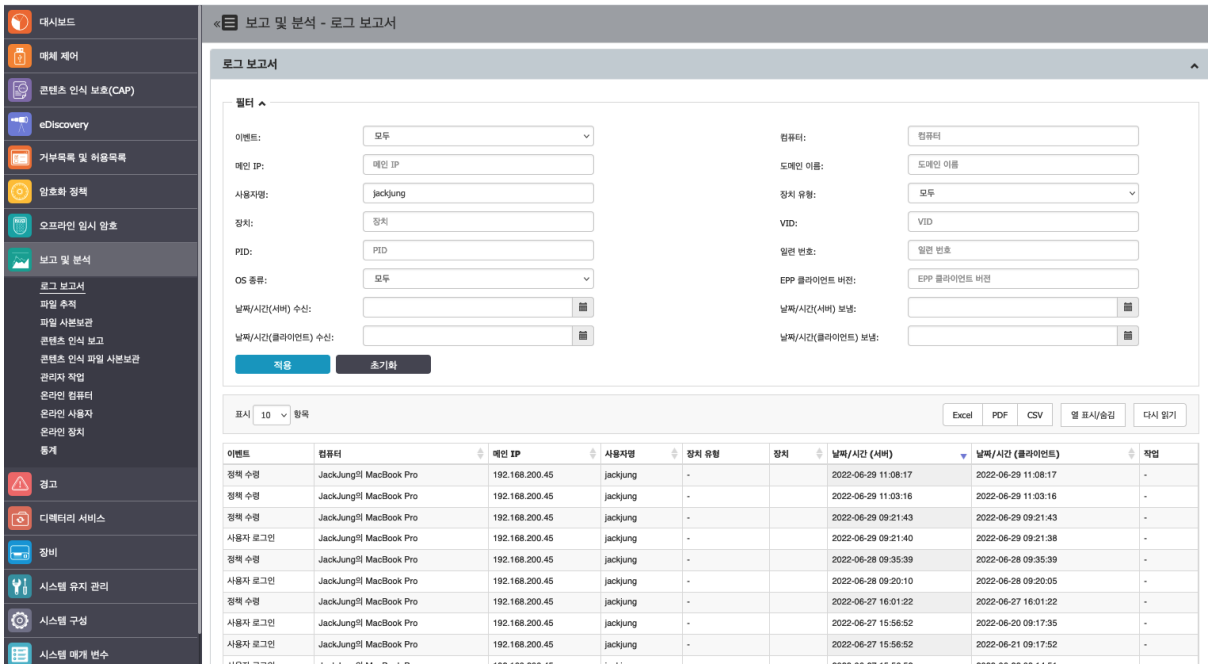
이 섹션에서 각 사용자 설정을 편집할 수 있습니다.



사용자가 어떤 수동 설정을 정의하지 않고도 정확하게 작동할 수 있기 때문에 모든 사용자에 대해서 설정을 정의할 필요는 없습니다. 이 작업은 기본적으로 자신이 속한 그룹의 설정을 상속하거나 설치 시 기본값을 사용하여 시스템에 존재하는 전체 설정을 상속하여 수행됩니다.

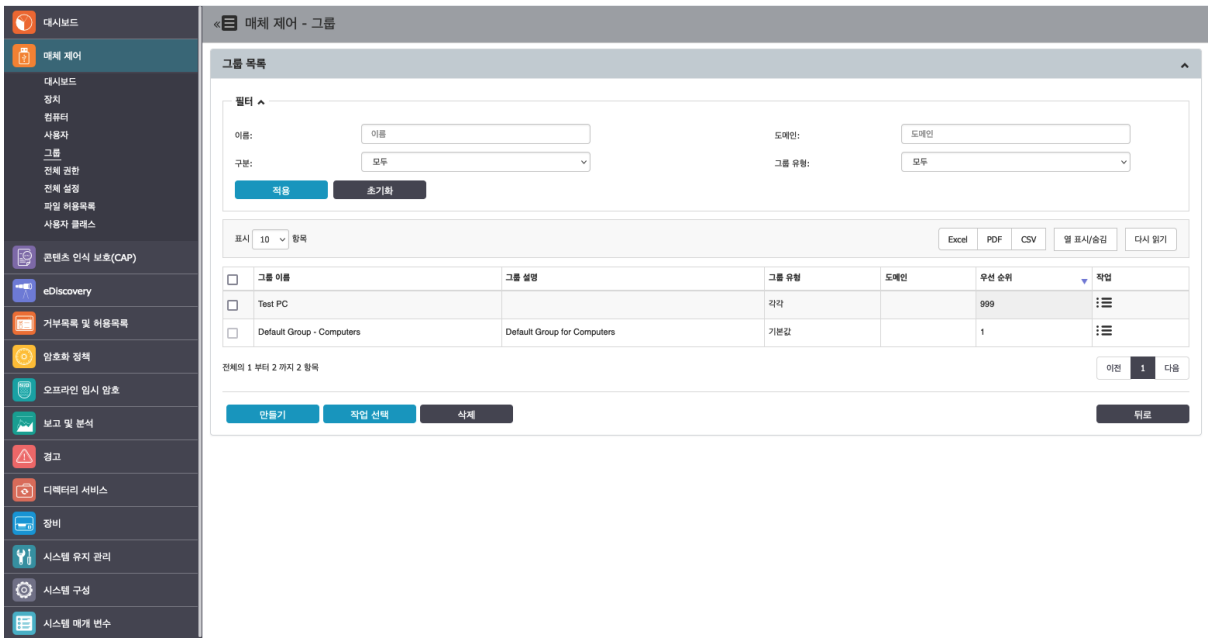
5.4.3. 사용자 기록

이 섹션에서 사용자 기록 활동 보기를 통해서 사용자 기록을 볼 수 있습니다. 각 사용자에 대한 로그 리포트를 보여줍니다.



5.5. 그룹

이 섹션에서 시스템의 모든 그룹을 관리할 수 있습니다. 컴퓨터 및 사용자의 그룹은 관리자가 권한을 관리하거나 효율적으로 각 객체의 설정을 만들 때 도움이 됩니다.



그룹은 객체 (컴퓨터 및 사용자) 기반 이외에 이름과 설명과 같은 정보로 확인됩니다.

관리자는 위에서 언급된 그룹 정보를 이용하여 새로운 그룹을 수동으로 만들 수 있습니다. 그룹은 또한 Active Directory에서 Endpoint Protector로 가져오기 할 수 있습니다.

참고: Active Directory의 더 자세한 내용은 디렉터리 서비스 챕터를 참조하시기 바랍니다.

작업 열은 편집, 권한 관리, 설정 관리, 기록 및 삭제 등 그룹 관리에 관련된 여러 옵션을 제공합니다.

5.5.1. 그룹 유형

5.5.1.1. 일반 그룹

일반 그룹은 관리자가 만들거나 AD에서 가져온 그룹으로 규칙을 기반으로 만들지 않습니다. 관리자는 원하는 컴퓨터와 사용자를 추가 또는 삭제할 수 있습니다.

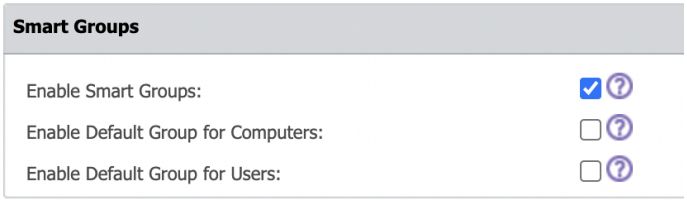
5.5.1.2. 스마트 그룹

스마트 그룹은 컴퓨터와 사용자 그룹의 역동적 범주로 그룹 구성은 구성의 이름 패턴을 기반으로 정의할 수 있습니다.

스마트 그룹을 사용하려면 아래 단계 진행하시기 바랍니다:

1. 스마트 그룹은 **시스템 구성, 시스템 설정, 스마트 그룹** 에서 사용할 수 있습니다. 페이지 하단을 스크롤 후 **저장**을 클릭하시기 바랍니다.

   참고: 스마트 그룹 기능을 사용하면 스마트 그룹을 만들지 않는 한 컴퓨터와 사용자는 자동으로 기본 그룹에 할당되지 않습니다.



2. **매체 제어, 그룹 섹션**에서 스마트 그룹을 만듭니다. **만들기**를 클릭하고 아래 내용을 확인

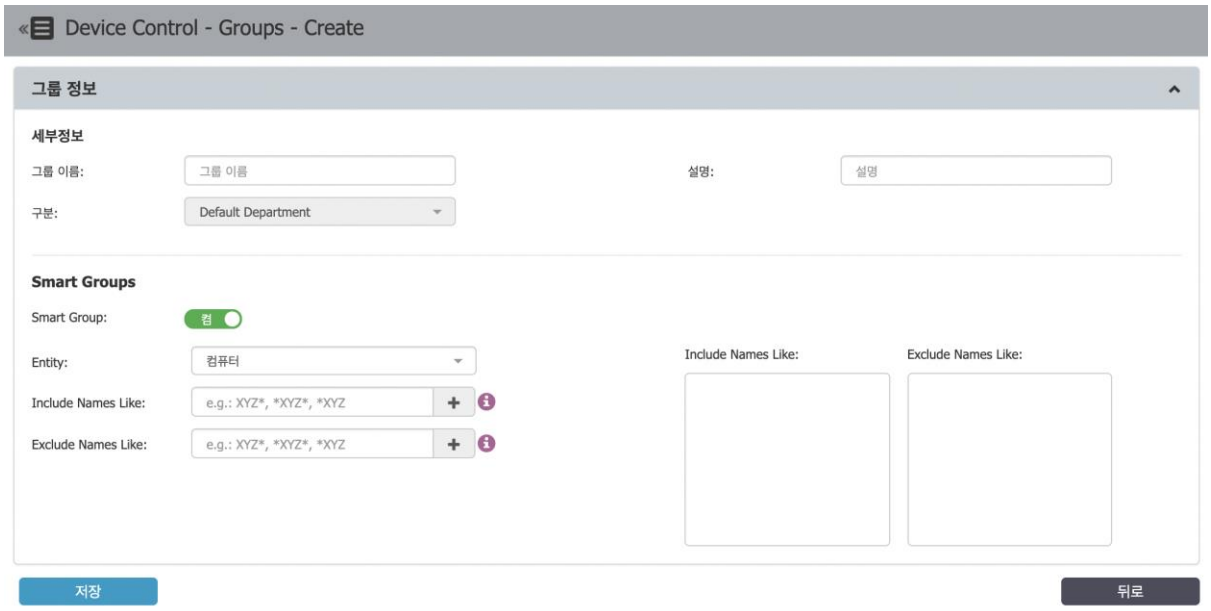
후 **저장**을 클릭합니다.

- 그룹 이름, 설명, 구분
- **스마트 그룹** 설정 활성화
- 엔터티, 컴퓨터, 사용자 선택
- 포함 및 제외 관련 컴퓨터 또는 사용자 규칙 설정

스마트 그룹을 사용할 때 관리자는 이름과 매칭이 되는 규칙을 정의할 수 있습니다. 이름 포함 및 이름 제외는 XYZ*, *XYZ*, *XYZ 로 설정이 가능합니다.

중요: 규칙 설정은 대소문자가 구분되어야 합니다.

참고: 만들어지면 드래그 앤 드롭 액션으로 그룹 우선 순위를 관리할 수 있습니다.



3. 스마트 그룹에 엔터티들을 동기화합니다.

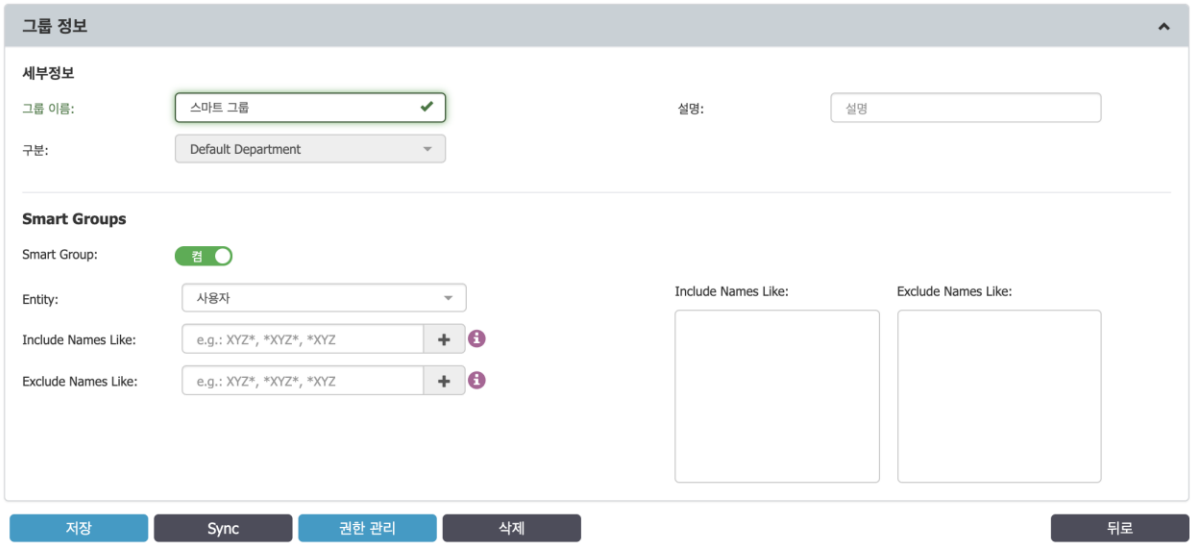
   스마트 그룹은 스마트 그룹에 할당된 일반 그룹의 항목을 삭제하지 않습니다. 엔터티는 동기화로 스마트 그룹에 추가됩니다. 스마트 그룹을 만든 후에 매 1분 간격으로 동기화가 시작되도록 **동기화**를 클릭합니다.

참고: 동기화 프로세스는 일반 그룹에 설정을 변경하지 않습니다.

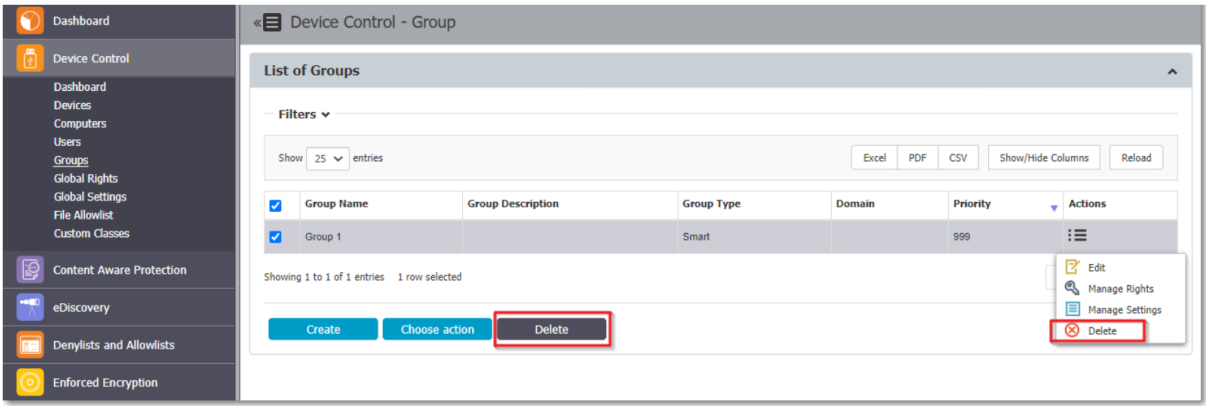
새로운 컴퓨터가 등록되고 설정한 규칙 중 하나와 매치가 되면 이 컴퓨터는 자동으로 그룹에

할당됩니다.

만약 매치가 되지 않고 기본 그룹 (Default Group)을 사용할 수 있으면 기본 그룹에 추가 됩니다.



4. **작업** 컬럼에서 스마트 그룹을 삭제하거나 목록에서 그룹을 선택 후 **삭제**를 클릭합니다.



스마트 그룹은 다음 **제한**을 가지고 있습니다:

- 할당된 컴퓨터 또는 사용자는 표시되지 않습니다.
- 스마트 그룹에 엔터티를 수동으로 추가할 수 없습니다.
- 스마트 그룹은 기본 구분의 부분이지만 구분을 사용하지 않습니다.

시스템 설정에서 스마트 그룹을 사용하지 않으면 스마트 그룹은 일반 그룹으로 변경됩니다. 이는

이러한 설정, 권한, 다른 설정을 보유하지만 그 엔터티는 잃게 됩니다. 그리고 컴퓨터의 기본 그룹과 사용자의 기본 그룹은 삭제됩니다.

사용자 엔터티만 컴퓨터 등록 시간이 아닌 동기화 스크립트가 구동될 때 스마트 그룹에 할당됩니다. 이는 사용자 정보가 Endpoint Protector 클라이언트에 의해서 전달되는 방식 때문입니다.

컴퓨터 정보만 갖고 있는 등록 시간에서 사용자 정보는 이벤트 (로그)나 정기적 ping/reprovision 요청으로 전달됩니다. 사용자 정보는 휘발성입니다: 요청 사이에서 변경될 수 있습니다 (같은 컴퓨터에 다른 사용자가 로그인 로그아웃; 로그아웃 이벤트/절전 모드로 기본 하드 코딩 사용자 객체가 활성/온라인으로 표시되는 결과를 가져옴).

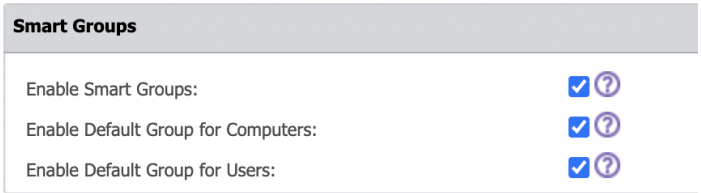
5.5.1.3. 기본 그룹

기본 그룹은 스마트 그룹에 속하지 않는 컴퓨터와 사용자의 그룹입니다. 이 그룹은 스마트 그룹에 설정된 이름 패턴을 따르지 않는 컴퓨터와 사용자입니다.

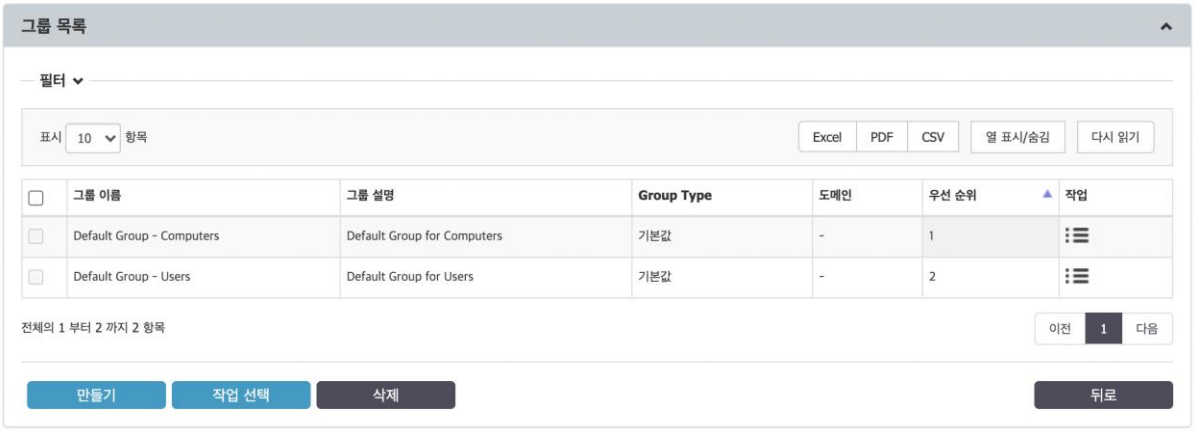
참고: 스마트 그룹이 활성화 될 때만 기본 그룹을 사용할 수 있습니다.

기본 그룹을 사용하기 위해서 다음 단계를 따르시기 바랍니다:

1. **시스템 구성, 시스템 설정, 스마트 그룹** 섹션에서 컴퓨터와 사용자의 기본 그룹을 사용할 수 있습니다. 페이지를 맨 아래로 스크롤 한 후 **저장**을 클릭합니다.



중요: 기본 그룹을 수동으로 생성하도록 요구하지 않습니다 – 활성화하면 사용자와 컴퓨터의 기본 그룹은 자동으로 만들어 집니다.



2. 기본 그룹에 엔터티들을 동기화합니다.

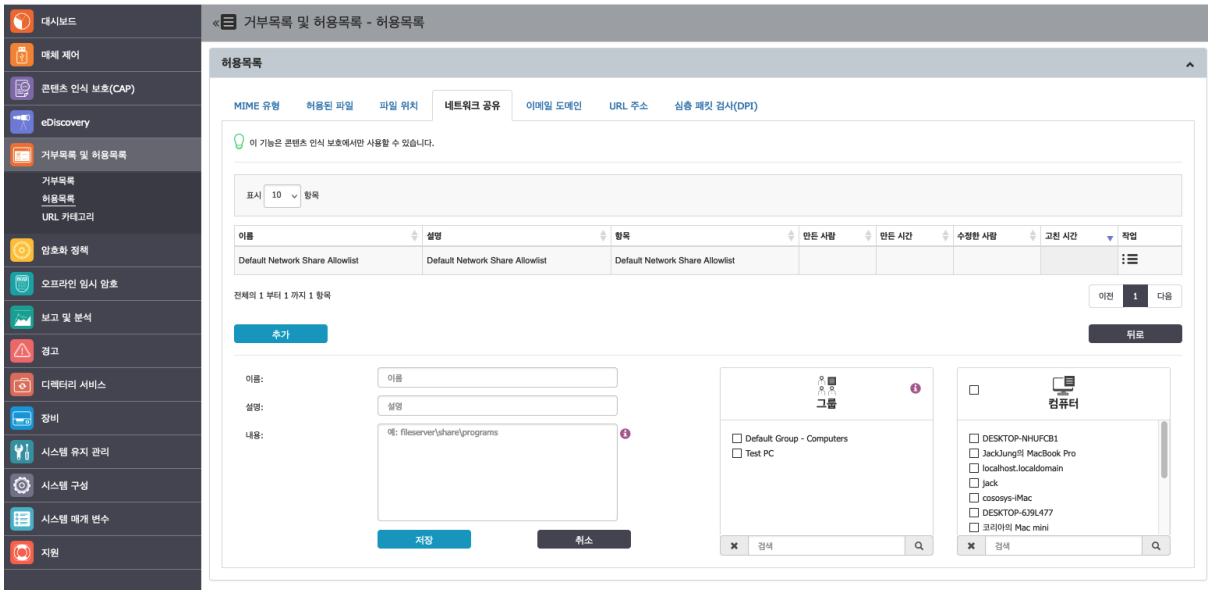
   기본 그룹에 할당된 컴퓨터와 사용자에 대해서 **매체제어, 그룹** 섹션의 그룹 목록에서 **작업** 컬럼을 선택하고 **편집** 그리고 **동기화**를 클릭합니다.

기본 그룹에는 **제한**이 있습니다:

- 기본 그룹 설명만 편집이 가능하고 기본 그룹 이름은 수정할 수 없습니다.
- 기본 그룹은 삭제할 수 없지만 **시스템 구성, 시스템 설정, 스마트 그룹** 섹션에서 비활성화 할 수 있습니다.
- 기본 그룹을 비활성화 하면 모든 의존성은 삭제됩니다.

5.5.1.4. 컴퓨터 그룹의 허용목록

파일 위치, 네트워크 공유 허용목록과 파일 위치 거부목록은 컴퓨터 그룹에서 설정할 수 있습니다.



그룹 선택 박스에는 모든 그룹이 노출됩니다.

선택된 그룹에서 허용목록 / 거부목록 규칙은 그룹의 컴퓨터에만 적용됩니다. 만약 그룹에 컴퓨터가 포함되어 있지 않으면 적용되지 않습니다. 관리자는 선택 박스에서 추가적으로 컴퓨터만 선택해야 합니다.

스마트 그룹은 정책에 적용되는 것처럼 거부목록에 포함된 모든 컴퓨터와 항상 동기화합니다. 허용목록 또는 거부목록에 선택된 그룹은 매 15분마다 동기화합니다.

5.5.2. 그룹 권한

그룹 권한은 특정 그룹의 작업 열에서 권한 관리를 선택해서 접근할 수 있습니다. 이 섹션은 관리자가 장치 유형과 특정 장치에 권한을 설정할 수 있도록 허용합니다.

이 섹션은 그룹을 위주로 구축되어 장치 유형을 특저하고 또한 특정 장치를 접근하도록 허용합니다.

이 섹션은 컴퓨터 권한 섹션과 비슷합니다. 차이점은 그룹에 속한 모든 컴퓨터에 적용되는 것입니다.

표준 매체 제어 권한은 매체 유형과 이미 존재하는 장치 섹션을 포함합니다. 이는 장치 권한에만

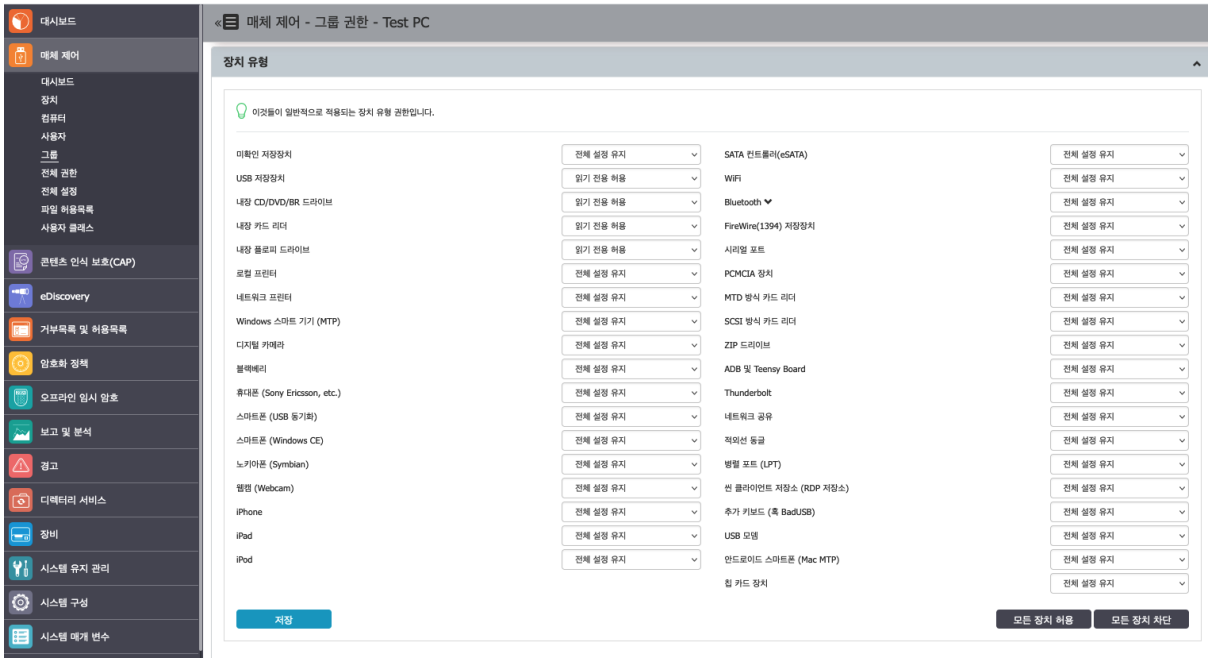
사용됩니다.

표준 매체 제어 권한에 추가하여 전체 설정이 사용하여 외부 네트워크와 업무 시간 환경에 대한 대응 정책을 만들 수 있습니다.

매체 유형과 특정 장치 (표준, 외부 네트워크, 근무외 시간)에 관련된 더 자세한 정보는 **장치 유형** 챕터를 참조하시기 바랍니다.

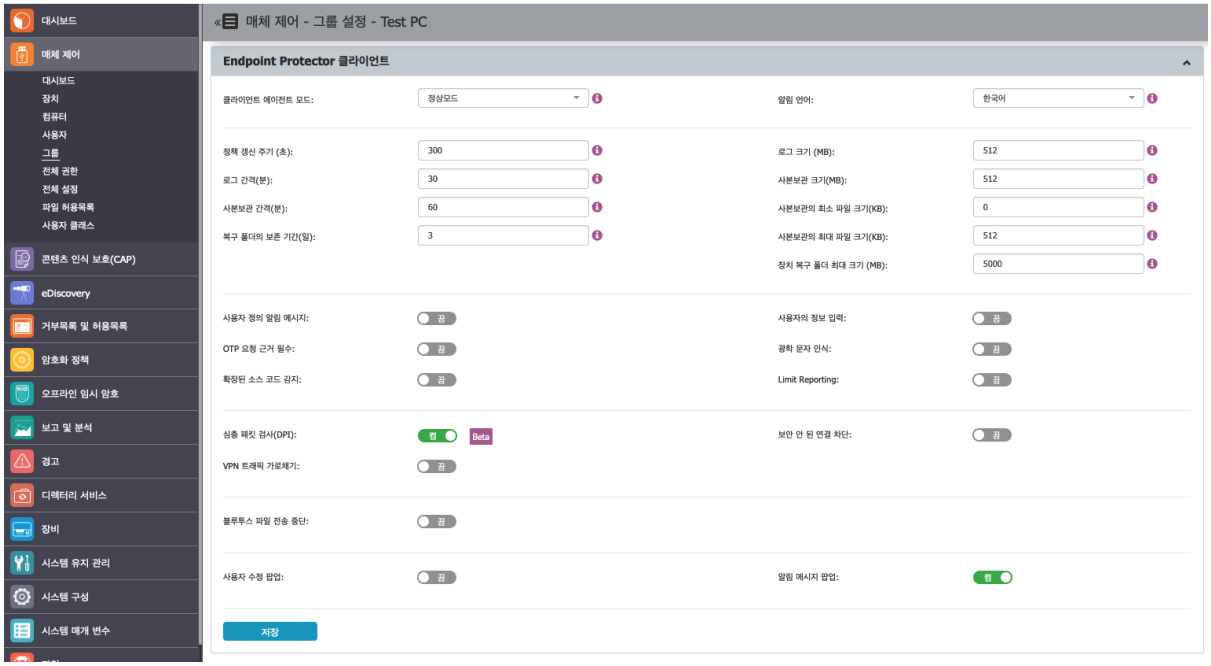
참고: 더 낮은 수준의 권한을 되돌리기 위해서 전체 권한 복원을 사용합니다. 사용하면 해당 수준의 모든 권한이 전체 설정을 보존하기 위해서 설정되고 시스템은 다음 수준의 권한을 사용할 것입니다.

참고: 해당 권한에 추가된 모든 기존 장치는 복원을 사용하면 삭제될 것입니다.



5.5.3. 그룹 설정

이 섹션에서 각 그룹의 설정을 편집할 수 있습니다.

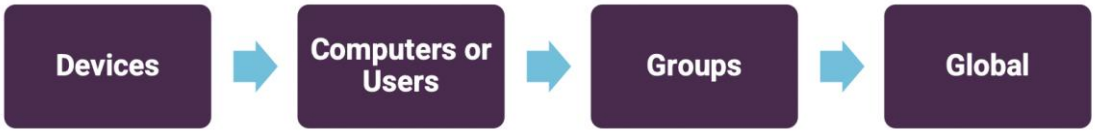


컴퓨터와 사용자를 그룹으로 만들면 설정을 더 쉽고 더 논리적으로 할 수 있다는 것을 위에서 언급했습니다. 모든 그룹의 사용자 정의 설정은 필수가 아닙니다. 컴퓨터는 어떤 세밀한 설정이 정의되지 않더라도 완벽하고 정확하게 기능을 수행합니다. 전체 설정에 되어 있는 값을 가져오거나 아니면 시스템 설치 시 기본 값을 가져와서 수행합니다.

5.6. 전체 권한

이 섹션에서 전체 시스템을 관리할 수 있습니다. 관리자는 전체 권한과 설정을 모든 Endpoint Protector 객체에 부여할 수 있습니다.

참고: 장치 권한 또는 다른 설정이 객체에 세밀하게 설정되어 있다면 우선 순위는 아래와 같습니다. 왼쪽이 가장 높은 우선 순위입니다:

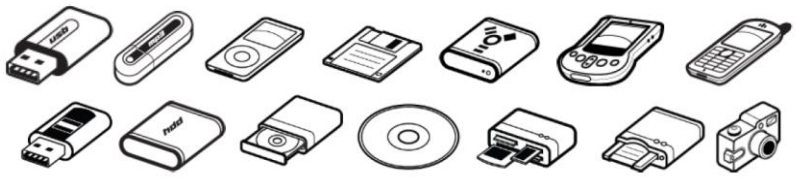


이 섹션은 전체 시스템과 관련이 있습니다. 장치 유형과 특정 장치의 허용 여부를 명시해 줍니다. 표준 권한 정책은 기본 정책이며 근무외 시간 또는 외부 네트워크 정책을 사용할 수 있습니

다. 전체 설정에서 첫번째로 활성화된 시스템을 따릅니다.

5.6.1. 장치 유형 (표준)

Endpoint Protector는 보안 침해의 주요 소스를 대표하는 넓은 범위의 장치 유형을 지원합니다. 이 장치들은 사용자가 콘텐츠를 보고 만들고 수정이 가능하도록 인가 받을 수 있고 관리자는 이렇게 인가된 장치의 데이터 전송을 볼 수 있습니다.



- **휴대용 저장 장치**
- **일반 USB 플래시 드라이브, U3 및 Autorun 드라이브, 디스크 키 등**
- **USB 1.1, USB 2.0, USB 3.0**
- **메모리 카드 – SD 카드, MMC 카드 및 콤팩트 플래시 카드 등**
- **카드 리더 – 내장 및 외장**
- **CD/DVD 플레이어/버너 – 내장 및 외장**
- **디지털 카메라**
- **스마트폰 / 포켓용 컴퓨터 / PDA (Nokia N 시리즈, Blackberry, Windows CE 호환 기기, 윈도우 모바일 기기 등 포함)**
- **iPods / iPhones / iPads**
- **MP3 플레이어 / 미디어 플레이 기기**

- **외장 HDD / 휴대용 하드 디스크**
- **FireWire 장치**
- **PCMCIA 장치**
- **생체 인식 장치**
- **Bluetooth**
- **프린터 (시리얼, USB 및 LTP 연결 적용)**
- **ExpressCard (SSD)**
- **무선 USB**
- **LPT/Parallel 포트 *스토리지 장치에만 적용**
- **플로피 디스크 드라이브**
- **시리얼 ATA 컨트롤러**
- **네트워크 프린터**

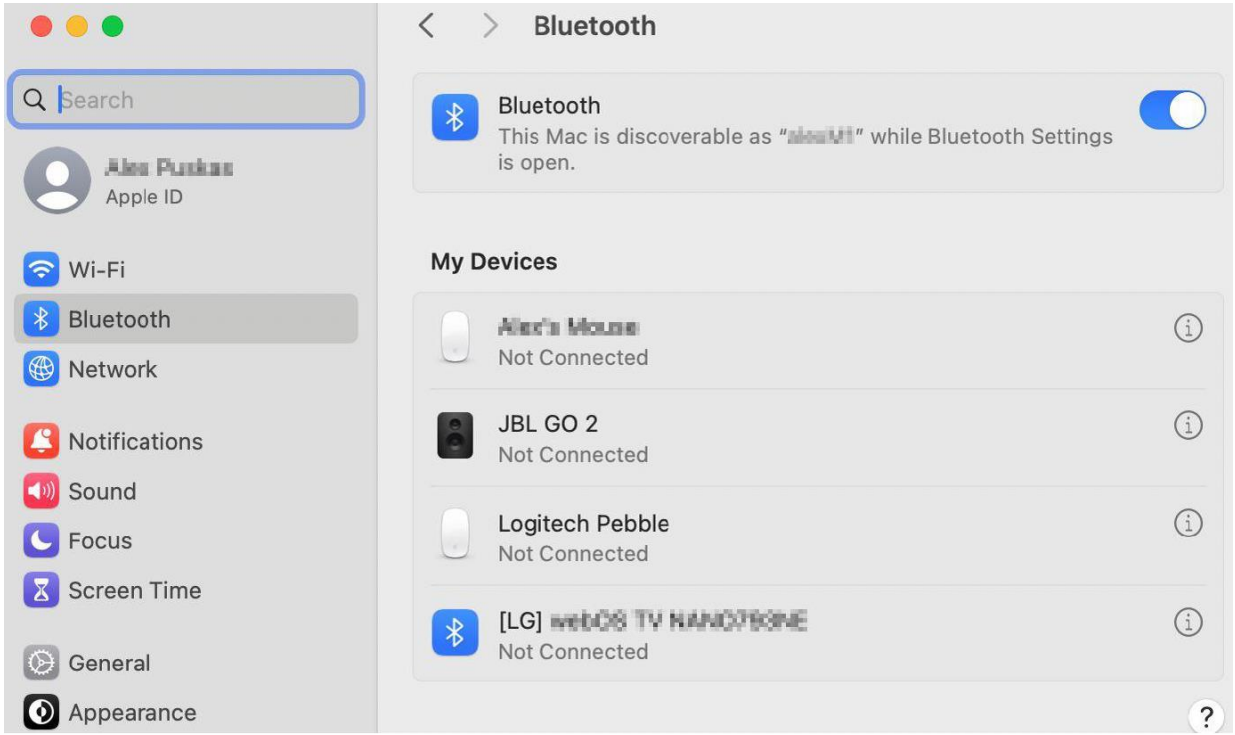
장치 유형에 따라 '사용 허용' 및 '사용 거부' 권한 이외의 추가 권한 사용이 가능합니다. 여기에는 '읽기 전용 사용' 또는 'CAP 스캐닝에서 엑세스 허용 및 제외' 또는 TD 레벨 1~4 사용 허용 등의 여러 조합의 사용 허용이 다양한 제한을 가지고 있습니다.

Endpoint Protector의 **TrustedDevices™** 기술은 4단계의 보안을 사용합니다. 이것은 장치에 제공된 보호 수준에 따릅니다. (EasyLockTM은 TD 레벨1 입니다.)

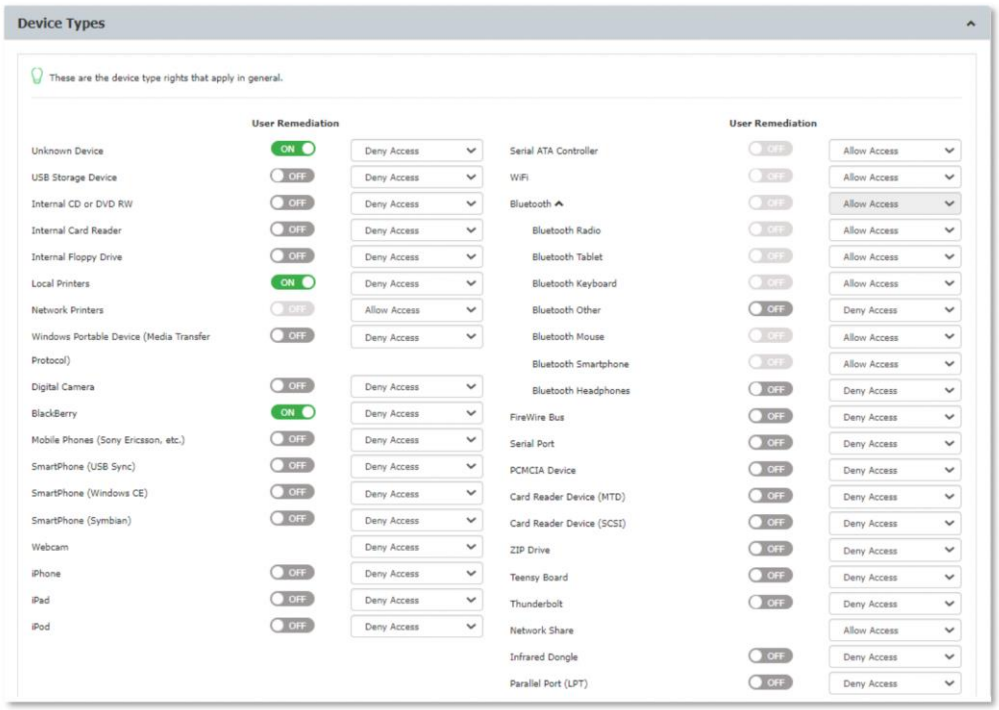
TrustedDevices™과 EasyLock™의 더 자세한 정보는 **Trusted Devices** 챕터를 참조하시기 바랍니다.

참고: '유선 네트워크가 있으면 WiFi 차단' 권한을 옵션이 있어서 유선 네트워크를 연결하고 WiFi 연결을 사용하지 않을 때 사용합니다. WiFi 연결은 유선 네트워크 연결이 없으면 사용할 수 있습니다.

참고: macOS version 14 (Sonoma) 또는 그 이상의 버전에서 Bluetooth 장치는 '시스템 설정' 의 Bluetooth 섹션의 '내 장치'에서 장치가 연결되고 보일 때만 관리됩니다.



기본 값으로 대부분의 장치 유형은 차단되어 있습니다. 그러나 설정 과정에서 인터넷 연결 또는 무선 키보드 등이 필요하기 때문에 일부 장치는 사용 허용으로 설정이 되어있습니다. WiFi, Bluetooth, 네트워크 공유, 추가 키보드 및 USB 모뎀은 사용 허용에 포함된 장치 유형입니다.



5.6.1.1. VM USB 장치 사용

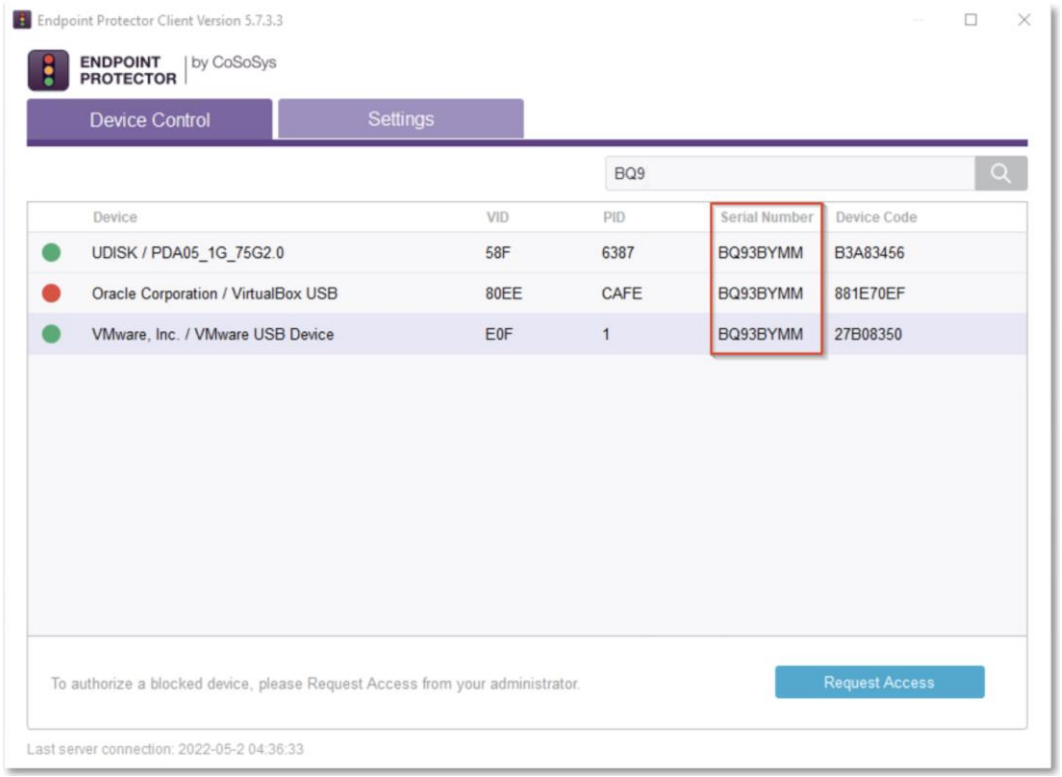
VM USB 장치 유형은 VMWare와 VirtualBox 가상 환경에 대한 Endpoint Protector 응용성을 확장했습니다.

가상 환경에서 USB 접근 관리를 위한 이 옵션을 사용할 수 있습니다.

가상 환경에서 사용할 때 USB 장치는 실제 이름, VID, PID 정보가 Endpoint Protector 알림에 표시되지 않습니다. 실제 정보는 일련번호 뿐입니다.

예: 아래 이미지에서 Endpoint Protector에 탐지된 3개의 장치를 볼 수 있습니다. 다른 VID, PID, 장치 코드를 가지고 있지만 이 장치는 모두 같은 일련번호를 가지고 있습니다.

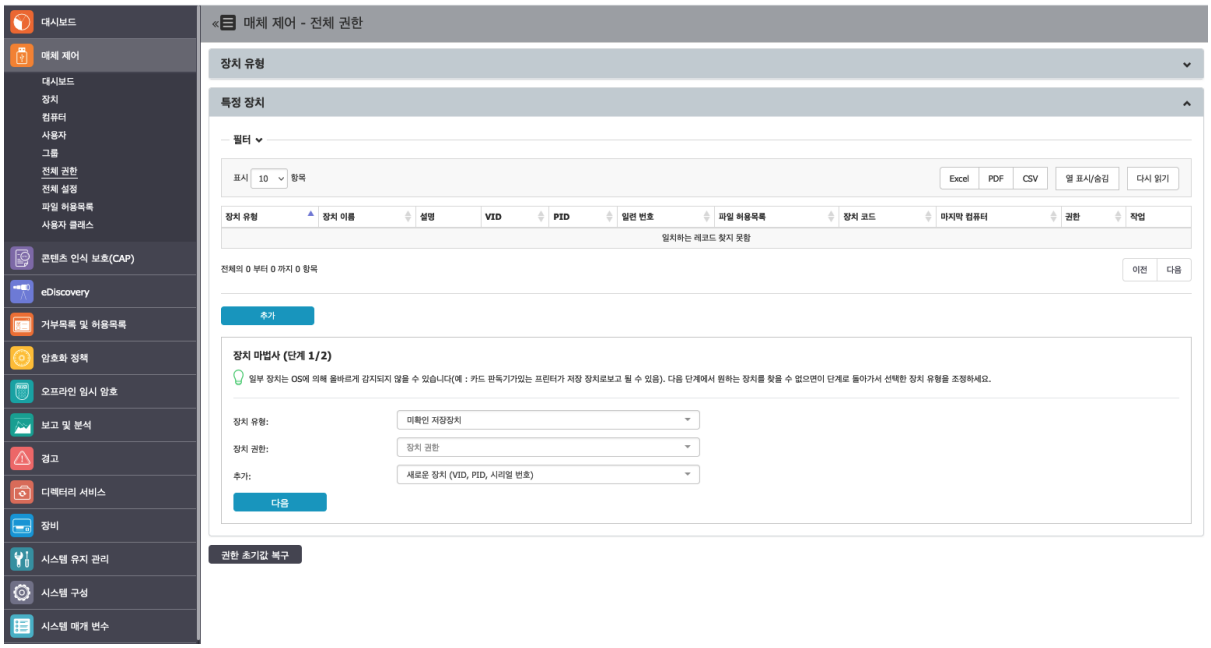
참고: Endpoint Protector 클라이언트는 장치 이름/VID/PID로 USB 장치 (예: USB 하드 드라이브 vs USB 웹 캠) 를 구별하지 않습니다.



5.6.2. 특정 장치 (표준)

이 섹션은 특정 장치에 대한 접근 권한을 관리할 수 있습니다.

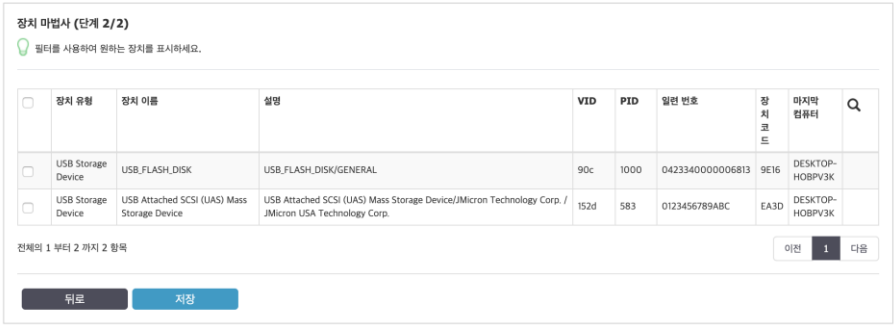
장치 권한은 각 섹션 및 엔터티에 권한 관리 작업을 사용하여 전체 또는 그룹, 사용자 또는 컴퓨터로 설정할 수 있습니다.



이 영역에 새로운 장치를 추가하려면 추가 버튼을 누르고 아래 장치 마법사의 단계를 따릅니다.

- **새로운 장치 (VID, PID, Serial Number)** – 2단계에서 벤더 ID, 제품 번호, 일련 번호 기반으로 새로운 장치를 추가할 수 있습니다.

- **특정 장치 (마법사)** – 2단계에서 이전에 보호되는 컴퓨터에 연결된 장치와 Endpoint Protector 데이터베이스에 있는 장치를 추가할 수 있습니다.



- **장치 시리얼 번호 범위** – 2단계에서 동시에 여러 장치를 추가할 수 있습니다. 시리얼 번호의 첫 번째와 마지막 숫자를 이용합니다. 패턴이 명확하고 연속 범위의 시리얼 번호를

쓰는 장치에 사용하는 것을 권장합니다.

참고: 실제로 이 기능은 시리얼 번호 범위가 눈에 띄는 패턴이 아니라도 동작하지만 권장하지는 않습니다. 이경우 일부 장치는 Endpoint Protector가 무시하고 원하는 정책 효과를 가져오지 않습니다.

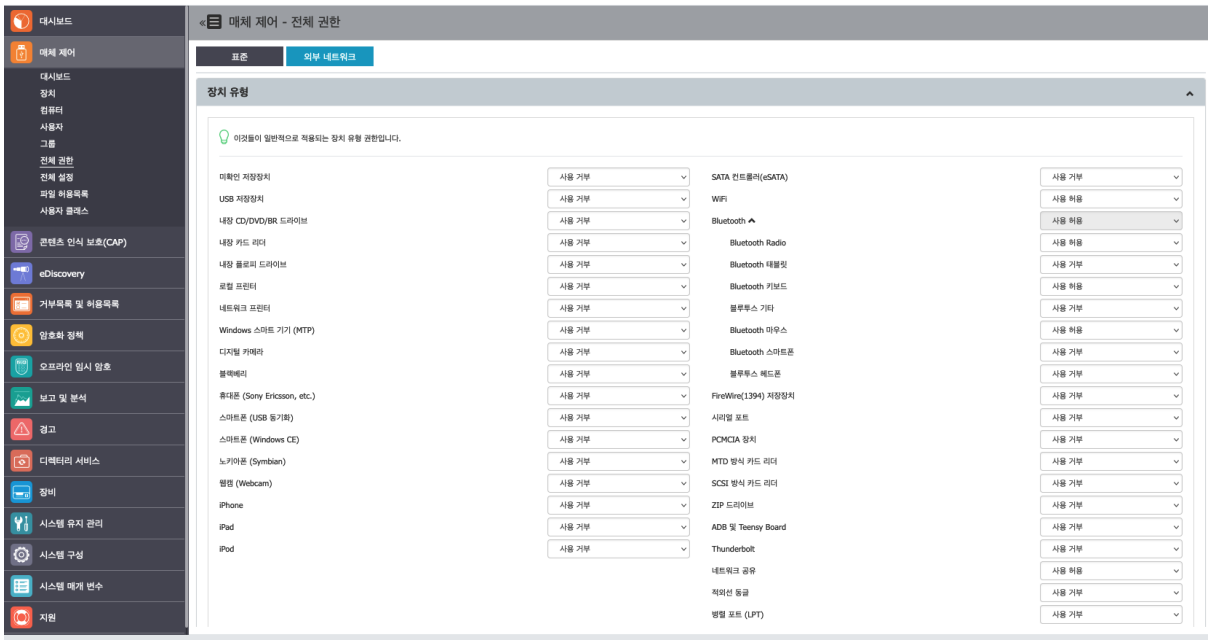
- **장치의 벌크 리스트** – 2단계에서 2개에서 1000까지의 장치를 동시에 입력할 수 있습니다. 가져오기와 단순히 붙여넣기 두 가지 방법을 사용할 수 있습니다.

파일 허용목록 기능은 USB 저장 장치의 사용 허용 권한에서 사용할 수 있습니다. 더 자세한 정보는 파일 허용목록 챕터를 참조하시기 바랍니다.

5.6.3. 외부 네트워크

참고: 이 기능을 사용하려면 전체 설정 섹션에서 설정이 필요합니다.

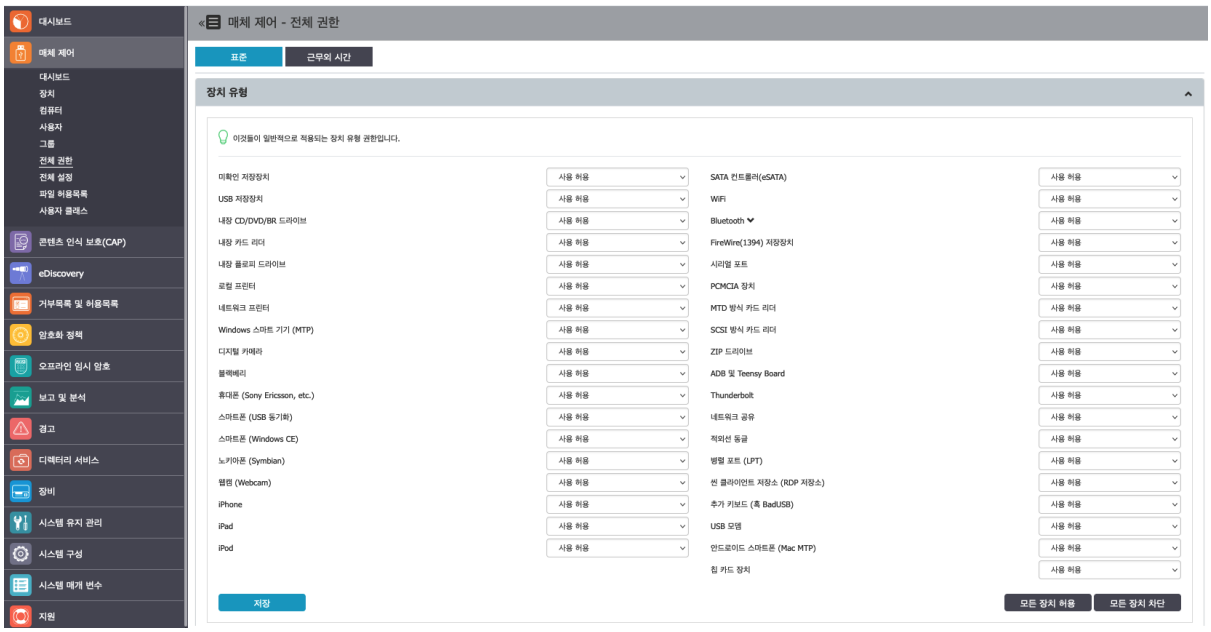
이 섹션에서 외부 네트워크에 적용할 수 있는 대응 정책을 정의 할 수 있습니다. 모든 기능은 전체 권한의 표준 영역에서 확인할 수 있습니다.



5.6.4. 근무외 시간

참고: 이 기능을 사용하려면 전체 설정 섹션에서 설정이 필요합니다.

이 섹션에서 업무 시간을 기반으로 적용할 수 있는 대응 정책을 정의 할 수 있습니다. 모든 기능은 전체 권한의 표준 영역에서 확인할 수 있습니다.



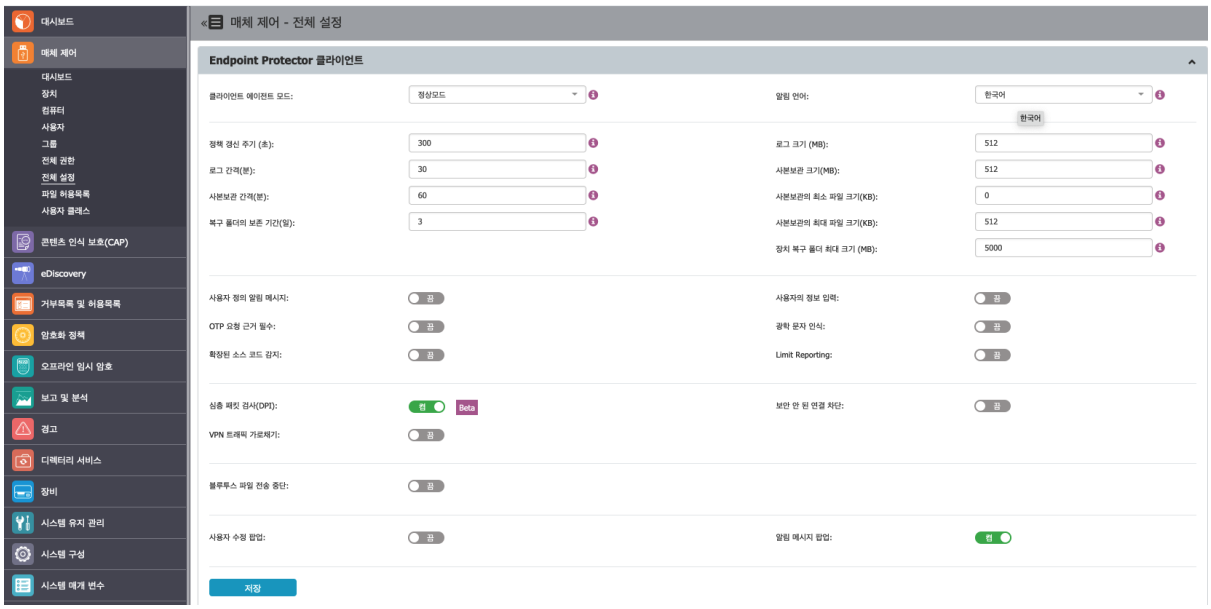
5.7. 전체 설정

이 섹션은 모든 Endpoint Protector 엔터티에 전체 설정을 적용할 수 있습니다.

❿ 컴퓨터에 세밀하게 정의된 설정이 없고 그룹에 속하지 않으면 이 설정을 상속받습니다.

❿ 컴퓨터가 그룹에 속해 있으면 그룹의 설정을 상속 받습니다.

참고: 이 섹션의 여러 설정은 또한 매체 제어 모듈이 아닌 (콘텐츠 인식 보호(CAP), eDiscovery 등) 다른 모듈에도 관련이 됩니다.



5.7.1. Endpoint Protector 클라이언트 설정

이 섹션에서 Endpoint Protector 클라이언트와 각각의 특정 엔터티 (전체, 그룹, 컴퓨터)에 대한 클라이언트 동작에 직접적으로 관련된 설정을 관리할 수 있습니다.

- **클라이언트 에이전트 모드** - Endpoint Protector 클라이언트 동작 변경 모드 선택

  참고: 클라이언트 모드 섹션에서 더 자세한 내용을 참조하시기 바랍니다.

- **알림 언어** – 알림에 대해 사용자의 OS 언어와 자동으로 일치하도록 Endpoint Protector 클라이언트를 구성합니다. "자동"으로 설정하면 클라이언트가 서버와 상호 작용 없이 사

용자의 OS 언어 기본 설정에 맞춰 언어를 선택하여 사용자 환경을 개선하고 혼란을 줄입니다.

EPP 알림 언어 구성 방법:

1. Endpoint Protector 콘솔의 **'매체 제어 > 전체 설정'**으로 이동합니다.
2. **'알림 언어'** 섹션에서 선호도에 따라 **'자동'** 또는 **'기본'** 중 하나를 선택합니다.
   2.1. '자동'은 언어가 서버의 상호 작용없이 OS에서 자동으로 탐지함을 의미합니다.
   2.2. '기본'은 서버에서 선택된 언어가 적용되는 것을 의미합니다. 만약 서버에서 '자동' 언어로 선택한다면 '자동' 언어가 사용됩니다.
3. 선택한 언어 선택 적용을 위해서 설정을 저장하시기 바랍니다.

이 강화된 언어 선택 기능으로 Endpoint Protector 사용자에게 더욱 편리한 환경을 제공하여 알림 및 경고에 대한 접근성을 높이고 사용자 중심 환경을 제공합니다.

- **Tamper Mode –** 인가되지 않은 종료 및 변경에서 Endpoint Protector 클라이언트를 보호하기 위해서 이 설정을 활성화

중요: 정확하게 작동시키려면 이 설정을 활성화한 후에 머신 또는 서비스 재시작을 반드시 해야 합니다.

- **정책 갱신 간격 (초) -** 최신 설정, 권한 정책 업데이트를 하는 클라이언트와 서버 사이의 시간 간격 입력

참고: 만약 Endpoint Protector 엔터티 동기화가 구성되어 있다면 정책 갱신 주기는 Azure Active Directory 동기화 간격 (또는 Active Directory 동기화)에 영향을 받을지도 모릅니다. 적절한 정책 갱신 간격을 결정할 때 Azure Active Directory 또는 Active Directory 동기화 프로세스의 동기화 간격을 고려하시기 바랍니다.

- **로그 간격 (분) -** 클라이언트가 로그를 서버로 보내는 시간 간격 입력

- **사본보관 간격 (분) –** Endpoint Protector 클라이언트가 Endpoint Protector 서버에 파일 사본을 보내는 간격을 0 – 720 분 사이에서 입력

  참고: 파일 사본을 즉시 보내기 위해서는 간격을 0으로 설정

- **복구 폴더의 보존 기간 (일)** - Mac과 Linux 컴퓨터에 해당됩니다. 전송되는 파일의 콘텐츠를 완전하게 검사하기 전에 폴더에 격리되는 것과 같은 액션입니다. 전송이 차단되어 일어나는 파일의 잠재적 손실을 피하기 위함입니다. 특정 시간 가격 후에 파일은 영원히 삭제됩니다.

- **사본보관의 최소 파일 크기 (KB)** - 파일 사본 보관을 만드는 최소 파일 크기 입력

- **복구 폴더의 보존 기간 (일)** - Mac과 Linux 컴퓨터에 해당됩니다. 전송되는 파일의 콘텐츠를 완전하게 검사하기 전에 폴더에 격리되는 것과 같은 액션입니다. 전송이 차단되어 일어나는 파일의 잠재적 손실을 피하기 위함입니다. 특정 시간 가격 후에 파일은 영원히 삭제됩니다.

- **로그 크기 (MB)** - 클라이언트에 저장되는 모든 로그의 최대 크기. 이 값에 도달하면 가장 오래된 로그는 삭제되고 새로운 로그로 덮어씁니다.. 클라이언트와 서버가 통신하지 않는 최대 시간 동안 사용이 됩니다.

- **사본보관 크기 (MB)** - 클라이언트의 모든 파일 사본 보관 최대 크기 입력. 이 값에 도달하면 가장 오래된 사본 보관은 삭제되고 새로운 사본 보관으로 덮어씁니다.. 클라이언트와 서버가 통신하지 않는 최대 시간 동안 사용이 됩니다.

- **사본 보관의 최대 파일 크기 (KB)** - 파일 사본 보관을 만드는 최대 파일 크기 입력

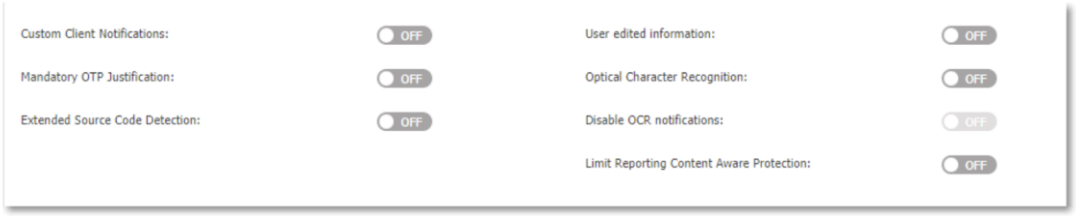
- **장치 복구 폴더의 최대 크기 (MB)** - Mac과 Linux 컴퓨터에 해당됩니다. 격리 폴더의 최대 크기입니다. 이 값에 도달하면 새로운 파일이 가장 오래된 파일을 덮어쓰기 합니다.

- **장치 복구 폴더 최대 크기 (MB) –** 이 설정은 Mac과 Linux 컴퓨터에 해당됩니다. 격리 폴더의 최대크기로 이 값에 도달하면 새로운 파일은 가장 오래된 파일을 덮어쓰기 합니다.

- **사용자 정의 알림 메시지** – 사용으로 되어 있으면 클라이언트 알림을 사용자 정의할 수 있습니다.
- **사용자의 정보 입력** - 사용으로 되어 있으면 사용자가 Endpoint Protector 클라이언트의 사용자와 컴퓨터 정보를 편집할 수 있습니다.
- **OTP 요청 근거 필수** - 사용으로 되어 있으면 사용자가 오프라인 임시 암호 요청 시 요청 이유를 반드시 입력해야 보내집니다.
- **광학 문자 인식 (OCR)** - 사용으로 되어 있으면 JPEG, PNG, GIF, BMP, TIFF 등의 파일 유형에서 콘텐츠를 검사합니다. 이 옵션은 또한 MIME 유형 허용목록에서 변경할 수 있습니다.
- **확장된 소스 코드 감지** - 사용으로 되어 있으면 PDF, docx 등과 같은 파일 유형 내부 탐지로 확장됩니다. **웹 메일 모니터** 설정이 사용하면 웹 브라우저를 사용하는 이메일의 제목과 본문의 소스 코드를 또한 탐지할 수 있습니다.

  참고: 소스 코드 탐지는 작은 코드 시니펫을 처리할 때 문제가 발생할 수 있습니다. 이는 다양한 프로그래밍 언어 간의 잠재적인 중복으로 발생할 수 있습니다. 최적의 결과를 얻으려면 소스 코드 감지를 구성하고 활용할 때 이러한 제한 사항을 고려가 중요합니다.
- **OCR 알림 사용 안함** – 사용으로 되어 있으면 광학 문자 인식 (OCR) 설정으로 생성되는 모든 알림을 사용하지 않습니다.

- **콘텐츠 인식 보호(CAP) 보고 제한 –** 사용으로 되어 있으면 임계값 도달 또는 콘텐츠 인식 보호(CAP)의 보고만 정책에 AND 연산자가 포함된 콘텐츠 탐지 규칙으로 일치로 발견된 모든 정보는 더 이상 로그를 생성하지 않도록 합니다. 이는 로그의 수를 줄여서 할당된 저장 공간을 최적화합니다.



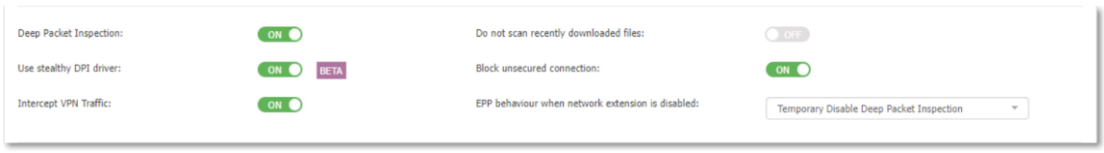
- **심층 패킷 검사 (DPI) -** 이 옵션을 사용하면 콘텐츠의 네트워크 트래픽을 검사할 수 있습니다. 이 옵션은 심층 패킷 검사 허용 목록과 URL 및 도메인 거부 목록을 수행합니다.
- **스텔스 DPI 드라이버 사용 –** 독립 소프트웨어 벤더와 상호 운용성을 개선하기 위해 이 드라이버를 사용합니다.
- **VPN 트래픽 가로채기 -** 이 옵션을 사용하면 Endpoint Protector 클라이언트는 네트워크 확장 프레임워크를 사용하여 macOS의 VPN 트래픽을 가로챕니다.

  참고: VPN 트래픽 가로채기 섹션에서 더 자세한 내용을 참조하시기 바랍니다.
- **최근에 다운로드한 파일 스캔하지 않음 –** 이 옵션을 사용하면 심층 패킷 검사 (DPI)를 사용하지 않을 때 민감한 데이터가 포함된 파일을 브라우저로 다운로드 및 업로드 할 수 있습니다.

  참고: 이 기능은 Endpoint Protector 5700 이후의 Windows 에이전트에서만 동작합니다.
- **보안 안 된 연결 차단 -** 이 옵션을 사용하면 HTTP를 통한 보안이 없는 접근은 차단되고 사용자 접근은 제한됩니다.

  참고: 보안 안 된 연결 차단 기능은 심층 패킷 검사 (DPI) 기능이 사용 중일 때만 동작합니다.

- **네트워크 확장 중단일 때 EPP 동작** - 사용 가능한 목록에서 동작 유형을 선택



- **블루투스 파일 전송 중단** - 이 옵션을 사용하면 이 설정은 엔드포인트의 페어링 여부에 관계없이 블루투스 전송을 차단합니다. **이 기능은 Windows 엔드포인트에만 적용됩니다.**

- **TD1+ 에서 휴대용 장치의 포맷/이름 변경 허용** – Windows 에서만 사용 가능하고 TD1+ 접근 허용인 USB 장치의 포맷 또는 이름 변경을 사용자가 할 수 있습니다.

  참고: 성공적으로 설정하려면 Minifilter 드라이버 설정을 사용합니다.

- **알림 메시지 팝업** - 기존 알림, 시스템 트레이 또는 팝업 알림 사이에서 선택이 가능합니다.

- **사용자 교정 팝업** – 이 설정은 **사용자 교정 기능**이 활성화되고 최종 사용자의 사용자 수정 팝업 알림이 사용되었을 때 사용이 가능합니다.

- **사용자 교정 팝업 적용** - 이 설정은 사용자 교정 팝업 설정을 사용할 때만 사용 가능합니다. 이 설정을 사용할 때 최종 사용자는 사용자 교정 팝업 알림 끄기를 할 수 없습니다.

- **미니필터 드라이버 사용** – Windows에서만 사용 가능하고 이 설정은 유지보수의 신뢰와 쉬움을 더 제공하는 보정된 드라이버의 사용을 허용합니다. 컴퓨터 / 사용자/ 그룹 / 전체 섹션의 작업 컬럼에서 관리 설정에서 사용할 수 있습니다.

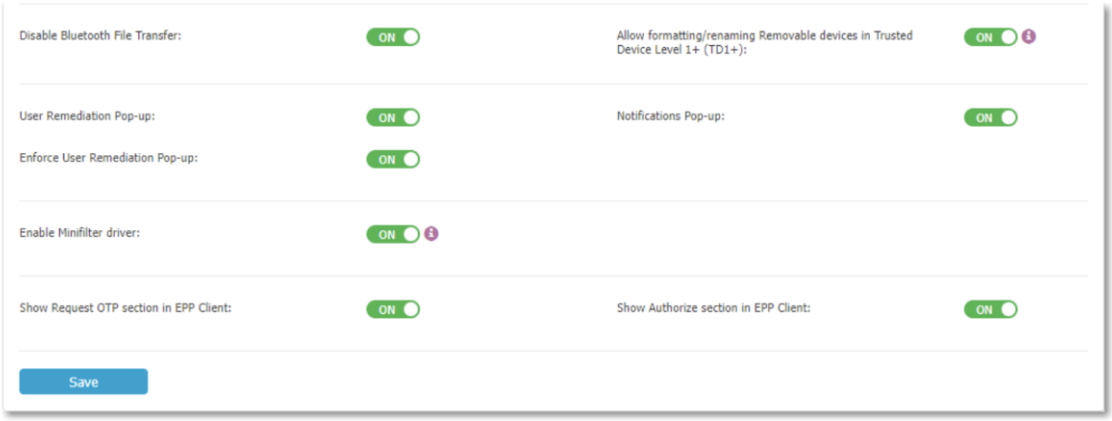
- **사용자 교정 알림 템플릿** – 사용자 정의 알림을 드롭 다운 목록에서 선택할 수 있습니다.

  참고: 사용자 교정 팝업 그리고 **사용자 교정 팝업 적용**은 프리미엄 라이선스에서만 사용 가능합니다.

- **EPP 클라이언트에서 OTP 섹션 요청 보이기** – Endpoint Protector 클라이언트에서 OTP

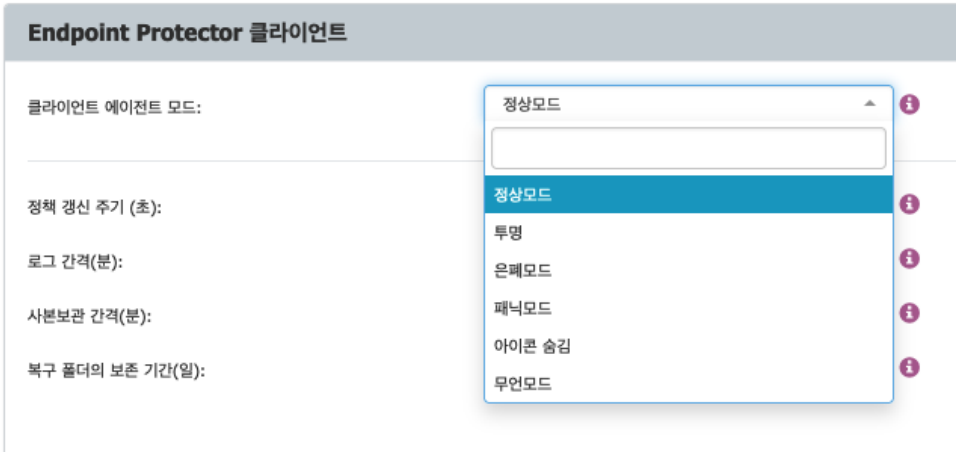
요청하기를 숨기는 설정을 사용할 수 없습니다.

- **EPP 클라이언트에서 인가 섹션 보이기** – Endpoint Protector 클라이언트에서 인가를 숨기는 설정을 사용할 수 없습니다.



5.7.1.1. 클라이언트 모드

동작이 정의된 클라이언트 모드 드롭다운 목록에서 선택할 수 있습니다.



1. **정상모드** – 이 설정은 다른 모드가 의미하는 바를 완전히 인식하기 전에 사용할 수 있는 기본 및 권장 설정입니다.

   참고: 만약 정상모드가 적당하지 않다면 **아이콘 숨김** 또는 **무언모드**가 최고의 대안이 될 수 있습니다.

2. **투명모드** – 모든 장치를 차단하는 동시에 사용자는 Endpoint Protector 클라이언트 존재나 제한을 인식하지 못합니다.

   이 모드를 선택하면:

   - 시스템 트레이 아이콘이 표시되지 않음
   - 시스템 트레이 알림이 표시되지 않음
   - 인가 여부에 관계없이 모든 것이 차단됨
   - 관리자는 모든 활동의 경고를 받음

3. **은폐모드** – 모든 사용자와 컴퓨터를 모니터링하는 동시에 사용자는 Endpoint Protector 클라이언트의 존재나 제한을 인식하지 못합니다.

   참고: 모든 것이 허용되지 때문에 사용자의 일상적인 업무 활동을 방해하지 않습니다.

   이 모드를 선택하면:

   - 시스템 트레이 아이콘이 표시되지 않음
   - 시스템 트레이 알림이 표시되지 않음
   - 인가 여부에 관계없이 모든 것이 허용됨
   - 모든 사용자 활동을 모니터링하고 볼 수 있는 파일 사본보관 및 파일 추적이 가능함
   - 관리자는 모든 활동의 경고를 받음

4. **패닉모드** – 사용자의 악의적인 의도 또는 활동이 탐지되는 심각한 상황에서 자동으로 시작됩니다.

   중요: 특별한 상황에서 수동으로 이 모드를 사용하여 모든 장치를 차단할 수 있지만 권장하지 않습니다.

이 모드를 사용하면:

- 시스템 트레이 아이콘이 표시되지 않음
- 시스템 트레이 알림이 표시되지 않음
- 인가 여부에 관계없이 모든 것이 차단됨
- 모든 사용자 활동을 모니터링하고 볼 수 있는 파일 사본보관 및 파일 추적이 가능함
- 관리자는 컴퓨터가 패닉모드로 들어가고 나갈 때 경고를 받습니다.

5. **아이콘 숨김 모드** – 이 모드는 정상모드와 비슷합니다. 다만 Endpoint Protector 클라이언트는 사용자에게 보이지 않습니다.

   이 모드를 사용하면:

   - 시스템 트레이 아이콘이 표시되지 않음
   - 시스템 트레이 알림이 표시되지 않음
   - 현재 정해진 구성에 따라 모든 권한 및 설정이 적용됨

6. **무언모드** – 이 모드는 정상모드와 비슷합니다. 다만 팝업 알림이 사용자에게 보이지 않습니다.

   이 모드를 사용하면:

   - 시스템 트레이 아이콘 표시
   - 시스템 트레이 알림이 표시되지 않음
   - 현재 정해진 구성에 따라 모든 권한 및 설정이 적용됨

5.7.2. DPI 구성

이 섹션에서 아래의 설정을 관리할 수 있습니다:

- **심층 패킷 검사(DPI)** – 이 옵션을 사용하면 네트워크 및 브라우저 트래픽에서 콘텐츠를 검사할 수 있습니다. 이 옵션은 심층 패킷 검사 허용 목록과 URL 및 도메인 거부 목록 모두 필요합니다.
- **스텔스 DPI 드라이버 사용** – 이 드라이버를 사용하면 독립 소프트웨어 공급업체와 상호 운용성을 향상시킬 수 있습니다.
- **VPN 트래픽 가로채기** – 이 설정을 사용하면 네트워크 확장 프레임워크를 사용해서 macOS에서 Endpoint Protector 클라이언트가 VPN 트래픽을 가로채도록 허용합니다.

  참고: 더 많은 정보는 VPN 트래픽 가로채기 섹션을 참조하시기 바랍니다.
- **네트워크 확장이 꺼진 상태의 EPP 동작** – 사용 가능한 항목에서 동작 유형을 선택합니다.
- **피어 인증서 유효성 검사** – 이 설정을 사용하면 DPI가 활성화 되어 있을 때 사용자가 액세스하는 웹사이트의 Endpoint Protector 인증서 유효성 검사를 켭니다.
  - ☐ 만료일 무시 – 체크하면 만료된 인증서를 무시하고 트래픽을 허용합니다.
  - ☐ 신뢰성 무시 – 체크하면 루트 인증서의 유효성 검사하지 않습니다.
  - ☐ 호스트 이름 무시 – 체크하면 인증서 호스트 이름 속성을 서버 호스트 이름에 대해 유효성 검사하지 않습니다.

  중요: '피어 인증서 유효성 검사' 설정을 사용하지 않아도 EPP 기능에 영향을 주지 않습니다. Secure Web Gateway 솔루션과 같은 대체 네트워크 트래픽 검사 제품이 웹사이트 인증서를 검증하는 경우에만 비활성화해야 합니다.
- **DPI 연결 끊김에 대한 대화 상자 표시** – 이 설정을 사용하면 엔드포인트 컴퓨터의 자세한 내용이 포함된 대화 상자를 표시합니다.
- **DPI 연결 끊김 알림 사용하지 않음** – 이 설정을 사용하면 시스템 트레이 근처의 알림 센터의 알림이 표시되지 않습니다.
- **보안되지 않는 연결 차단** – 이 설정을 사용하면 HTTP를 통한 보안되지 않은 액세스는 차단되고 사용자 액세스가 제한됩니다.

  참고: 보안되지 않는 연결 차단 기능은 DPI 검사 기능이 활성화된 경우에만 사용할 수 있습니다.

- **DPI 우회 트래픽** – 이 설정은 검사할 수 없는 트래픽을 자동으로 우회하고 허용된 트래픽에 대한 이벤트를 전송합니다.

  □ 우회 가능한 이유:

  - 타사 응용프로그램의 DPI 인증서 거부 우회
    - 웹 브라우저와 같은 소스 응용프로그램에서 다음과 같은 SSL 오류가 발생하면 이 설정을 사용합니다.
      - SSL_R_TLSV1_ALERT_UNKNOWN_CA
      - SSL_R_SSLV3_ALERT_CERTIFICATE_UNKNOWN
      - 이는 Endpoint Protector에서 발급한 서버 인증서 유효성에 실패했음을 의미합니다.
      - 시스템 키 체인에서 DPI 인증서가 없는 것도 이 시나리오의 원인이 될 수 있습니다.
      - '인증서 고정'도 이 범주에 속합니다.

  참고: 네트워크 트래픽 분석을 위한 Wireshark 사용에 대해 자세히 알아보시기 바랍니다.

  - 알 수 없는 TLS 핸드 셰이크 우회
    - 이 설정을 사용하면 보안 포트 연결이 TLS 대신 사용자 지정 암호화를 사용할 때 DPI 우회가 활성화됩니다.
      - 이 예시는 DPI 모니터링을 위해 Telegram.app을 구성하고 앱에 로그인하여 알 수 없는 TLS 핸드셰이크가 발생하는 경우로 볼 수 있습니다.
  - 웹 사이트 일시적 허용 목록 우회 (mTLS 연결 가능성 / SSL 설정 실패 / 지원되지 않는 TLS 프로토콜)
    - SSL 연결이 서버 측에서 SSL 설정 실패 또는 지원되지 않는 TLS 프로토콜 오류가 발생하는 경우 이 설정을 사용합니다. 웹 사이트를 일시적으로 허용 목록에 추가합니다.
      - 구체적인 예는 드물지만 이러한 경우 잠재적인 mTLS 연결과 관련이 있습니다.

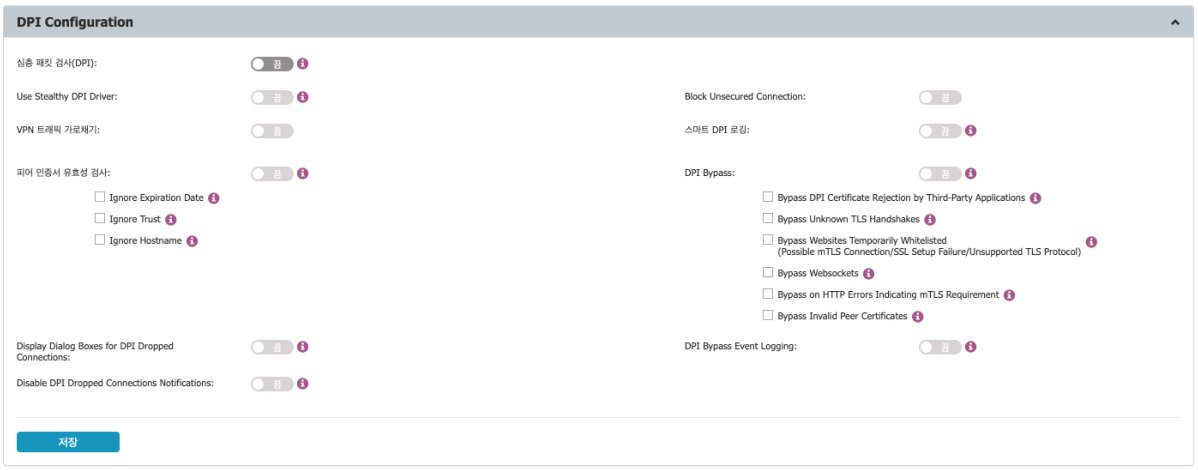
- 웹 소켓 우회
  - 웹사이트가 임의의 데이터 프로토콜의 웹 소켓을 사용하는 경우 이 설정을 활성화합니다.
    - EPP는 HTTP 연결이 웹 소켓으로 업그레이드되면 연결을 통과합니다.
    - 예를 들어 WhatsApp 웹, Firefox Send 등과 같은 응용프로그램이 있습니다.
- mTLS 요구 사항을 나타내는 HTTP 오류 시 바이패스
  - 서버가 클라이언트 인증서 (mTLS) 요구 사항을 나타내는 경우 이 설정을 사용합니다.
    - '400 Bad Response', '496 SSL Certificate Required' 등의 HTTP 오류에 대해 EPP가 우회를 시작합니다.
    - 필요한 클라이언트 인증서를 제공하지 않고 웹 브라우저에서 https://client.badssl.com/ 접속 요구가 이러한 상황을 설명합니다.
- 유효하지 않은 피어 인증서 우회
  - '피어 인증서 유효성 검사'가 활성화된 경우 유효하지 않은 피어 인증서와 연결을 허용하려면 이 설정을 사용합니다.
    - '유효하지 않은 피어 인증서 우회' 및 '피어 인증서 유효성 검사' 설정을 모두 활성화된 경우 '유효하지 않은 피어 인증서 우회'가 더 우선합니다.
    - '유효하지 않은 피어 인증서 우회' 및 '피어 인증서 유효성 검사' 설정을 모두 사용한 상태에서 웹 브라우저에서 https://expired.badssl.com/에 접속하면 이러한 상황을 보여줍니다 (웹 사이트에 접속할 수 있음).

중요: 현재 기본 DPI 목록과 새로운 기본 DPI 우회 목록은 CAP 정책 내에서 수동으로 확인했을 때만 사용된다는 점에 유의하시기 바랍니다.

참고: 우회된 웹 사이트의 타임아웃 기간과 우회된 도메인 및 응용프로그램 처리에 대해서 알아보시기 바랍니다.

- **DPI 우회 이벤트 로깅** – 이 설정은 엔드포인트에서 연결이 우회될 때 DPI 우회 이벤트/이유를 EPP 서버로 자동으로 전송합니다.

  참고: 우회 로그 보고 빈도에 대해서 알아보시기 바랍니다.



5.7.2.1. VPN 트래픽 가로채기

이 설정을 사용하면 Endpoint Protector 클라이언트는 네트워크 확장 프레임워크를 사용하는 macOS의 VPN 트래픽을 가로채기 합니다.

참고: VPN 트래픽 가로채기는 심층 패킷 검사 (DPI) 기능을 사용할 때만 사용이 가능합니다. macOS 11.0 이상 버전 그리고 심층 패킷 검사 (DPI) 인증서가 추가될 때만 동작합니다.

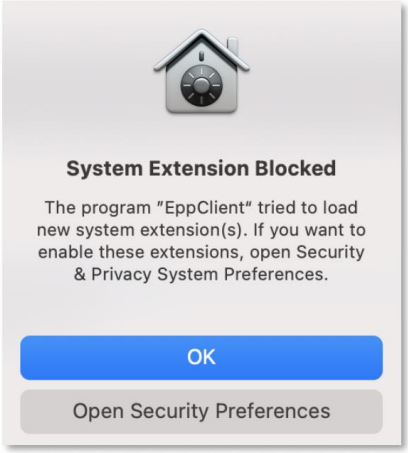
이 기능을 사용하려면 아래 단계를 따르시기 바랍니다:

1. **심층 패킷 검사 (DPI)** 사용
2. **VPN 트래픽 가로채기** 사용
3. **네트워크 확장 중단 일 때 EPP 동작**에 대한 옵션 선택
   - **심층 패킷 검사 (DPI) 임시 사용 중단** – 심층 패킷 검사 (DPI) 임시 사용을 중단합니다.
   - **인터넷 엑세스 차단** – 사용자가 Endpoint Protector 프록시 구성을 승인할 때 까지 인터넷 연결을 차단합니다. 또한 사용자는 PC를 재부팅 후에 구성을 허용할

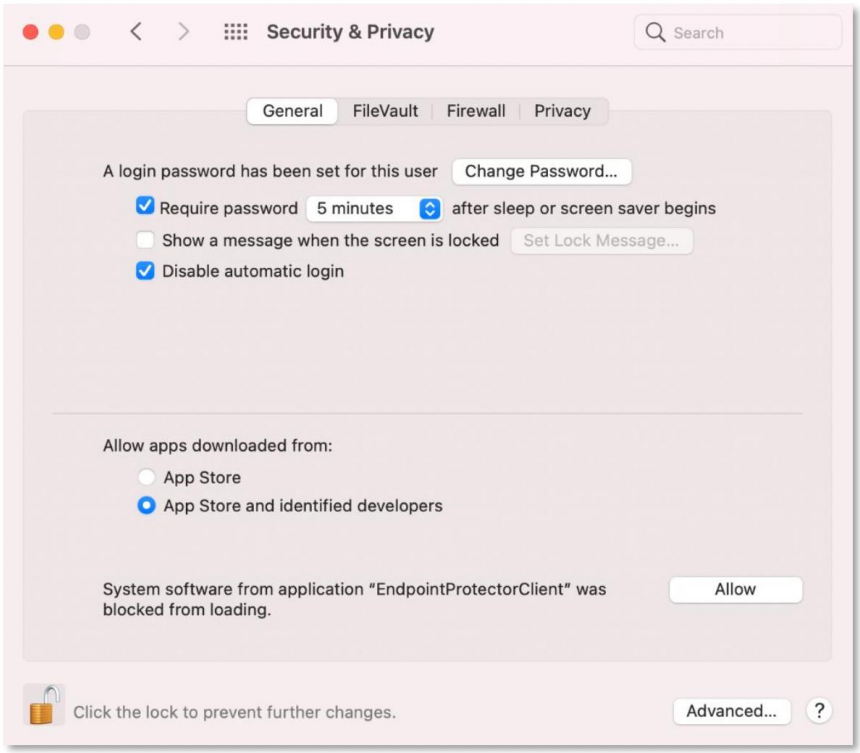
수 있습니다.

- **VPN 반복 알림** – 심지어 사용자가 이전에 허용을 거부한 후에도 VPN 팝업 창을 여러 차례 표시합니다.

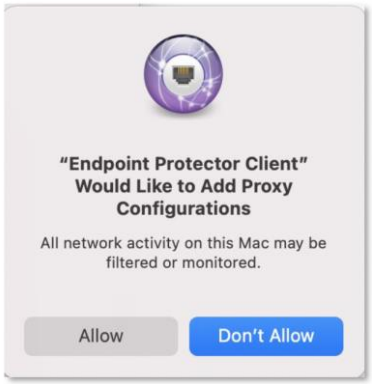
4. **저장**을 클릭합니다.
5. 시스템 확장이 차단되었다는 팝업 창이 사용자에게 나타나면 허용을 위해 **OK**를 클릭합니다;



6. **시스템 환경설정, 보안 및 개인 정보 보호, 일반**으로 이동한 후 Endpoint Protector 클라이언트 확장을 허용합니다.

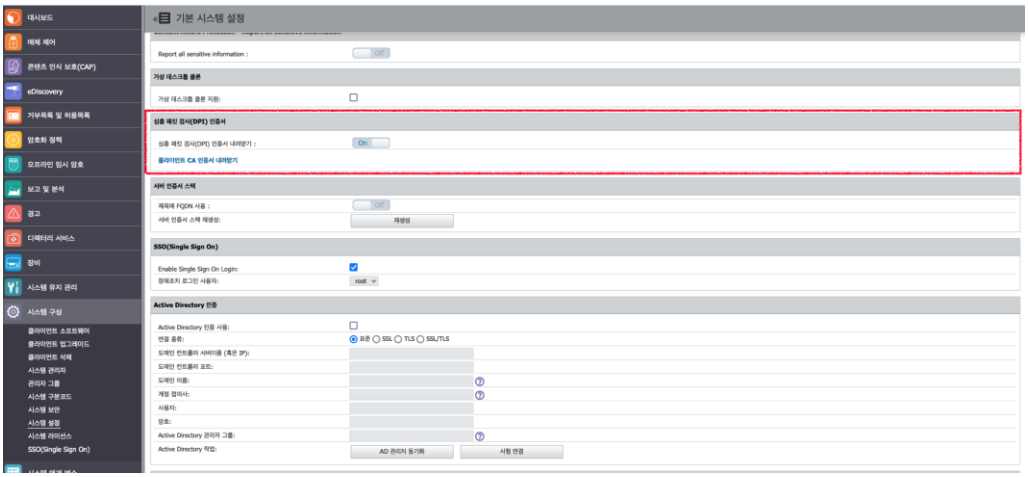


7. Endpoint Protector 프록시 구성 팝업 창에서 **Allow**를 클릭합니다.

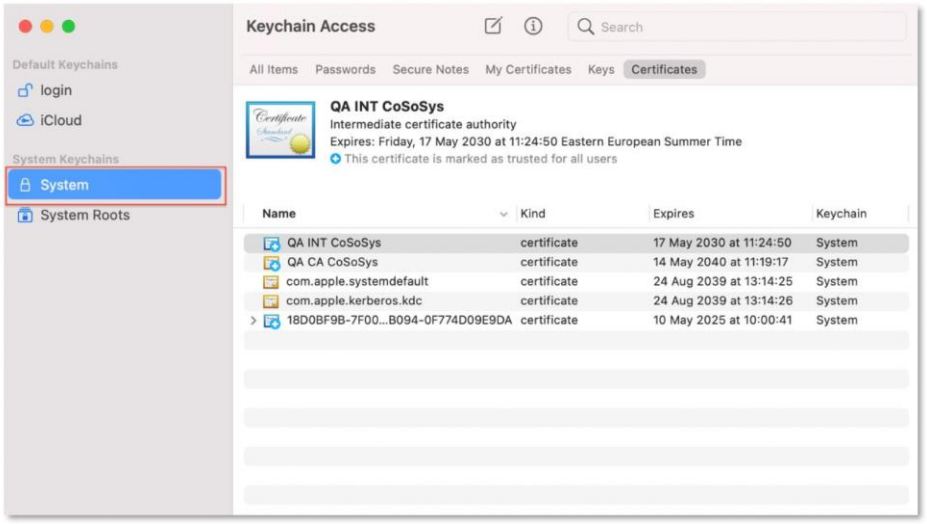


참고: 네트워크 확장이 성공적으로 사용되면 Client Integrity OK 로그가 생성됩니다.

8. **시스템 구성, 시스템 설정, 심층 패킷 검사 (DPI) 인증서**로 이동해서 CA 인증서를 다운로드합니다.

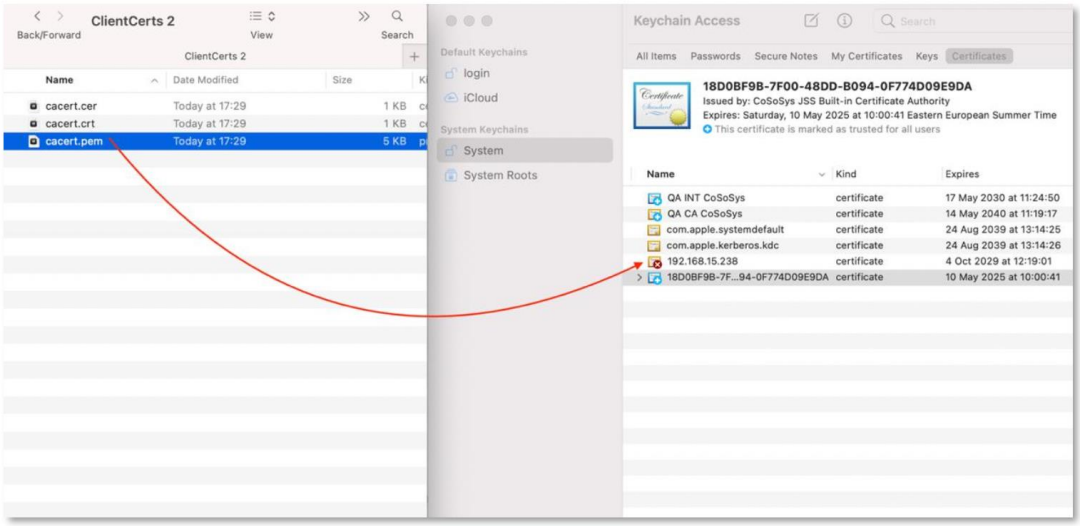


9. macOS에서 **키체인 접근** 응용프로그램을 열고 **시스템**으로 이동합니다.

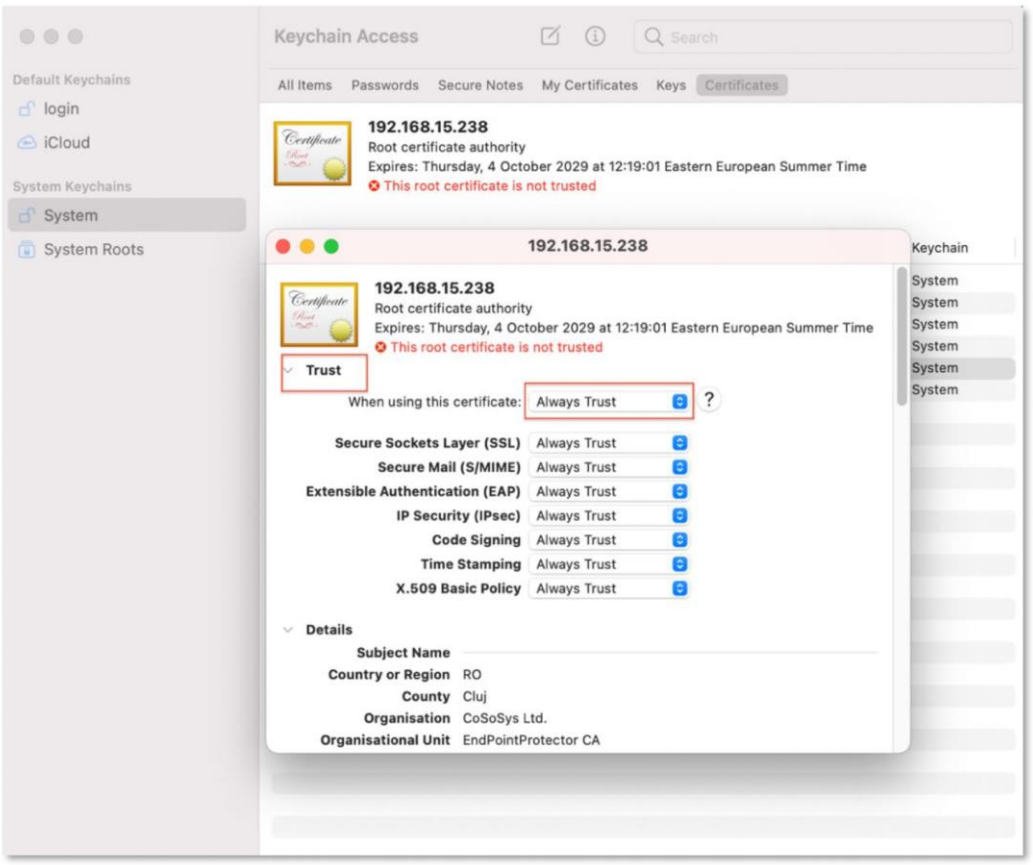


10. **ClientCerts** 파일 압축을 풉니다.

11. **cacert.pem** 파일을 선택하고 **키체인 접근, 시스템**에 드래그 앤 드롭합니다.



12. 새롭게 추가된 인증서에 **X**를 더블 클릭하고 신뢰 섹션에서 **항상 신뢰**를 선택합니다.



13. 변경을 **저장**합니다.

5.7.2.2. 스마트 DPI (로그 조절, Log Throttling)

이 설정을 활성화하면 URL 거부 목록에 대한 과도한 오탐 수를 해결할 수 있습니다. 이 개선 사항은 관련 없는 정보를 필터링하는 구성 옵션을 제공하여 실제 오탐에 초점을 맞춰서 보다 정확한 로그를 생성하고 불필요한 노이즈를 줄여 데이터베이스 저장 공간을 절약할 수 있습니다.

5.7.2.3. 우회 로그 보고 빈도

EPP 에이전트는 최대 2주에 한 번씩 각 도메인 이름과 응용프로그램 쌍을 보고하여 효율적인 리소스 활용을 보장합니다. 이 접근 방식은 더 자주 보고할 경우 과도한 수치를 기록할 수 있는 로그의 압도적인 유입을 방지합니다.

5.7.2.4. 우회된 웹 사이트의 타임아웃 기간

간소화된 프로세스를 유지하기 위해 EPP는 2주의 타임아웃 기간을 적용합니다. 이 기간 동안 우회된 웹 사이트 상태는 유지됩니다. 이 기간이 지나면 우회 상태가 자동으로 제거되어 리소스를 효과적으로 관리할 수 있습니다.

5.7.2.5. 우회된 도메인 및 응용프로그램 처리

EPP는 우회된 도메인과 응용프로그램 처리를 위해 미묘한 접근 방식을 사용합니다.

5.7.2.5.1. 메모리 및 디스크 보존

우회된 웹 사이트 정보는 메모리와 디스크에 모두 저장됩니다. 이 이중 저장으로 우회한 웹 사이트 목록에 쉽게 액세스할 수 있어서 나중에 효율적으로 참조할 수 있으며 이 정보를 유지함으로써 로그 생성 빈도를 제어하여 불필요한 리소스 부담을 피할 수 있습니다.

5.7.2.5.2. 우회 상태 삭제

우회 상태를 재설정하고 관련 기록을 지우려면 관리자가 간단한 프로세를 시작하면 됩니다. EPP 서버에서 우회 DPI 설정을 일시적으로 비활성화 했다가 다시 활성화하면 이 재설정이 완료됩니다.

5.7.2.6. 네트워크 트래픽 분석을 위한 Wireshark 사용

"DPI 인증서 거부" 이벤트가 발생하기 전에 Wireshark는 네트워크 트래픽 진단에 중요한 역할을 할 수 있습니다. Wireshark에서 "TLS 경고" 오류가 발생하면 이벤트가 임박했다는 신호입니다.

5.7.3. 파일 추적 및 사본보관

이 섹션에서는 아래 내용을 관리할 수 있습니다:

- **파일 추적** – 이 기능은 보호되는 엔드포인트와 이동식 저장 장치, 내장 eSATA HDD, 네트워크 공유 사이에 데이터 트래픽을 모니터링합니다. 또한 파일 이름, 삭제, 허용, 수정 등과 같이 일어나는 활동을 또한 보여줍니다.

이 기능을 사용하려면 **매체 제어**, **전체 설정** 또는 **그룹** 또는 **컴퓨터**에서 적용할 수 있습니다.

- **파일 사본보관** – 이 기능은 파일 추적으로 제공되는 정보의 확장입니다. 사용자가 접근한 파일의 정확한 사본을 생성합니다.

파일 사본 생성은 다음 이벤트가 일어나면 시작됩니다: 파일 복사, 파일 쓰기, 파일 읽기. 파일 삭제와 파일 이름 변경과 같은 이벤트는 해당되지 않습니다.

지원되는 모든 이동식 저장 장치에서 파일 사본보관이 가능합니다:

- **eSATA HDD 또는 타임머신**
- **네트워크 공유**
- **콘텐츠 인식 보호** – 온라인 응용프로그램, 프린터, 클립보드 등과 같은 다양한 포인트를 통한 파일 전송
- **이메일 본문**

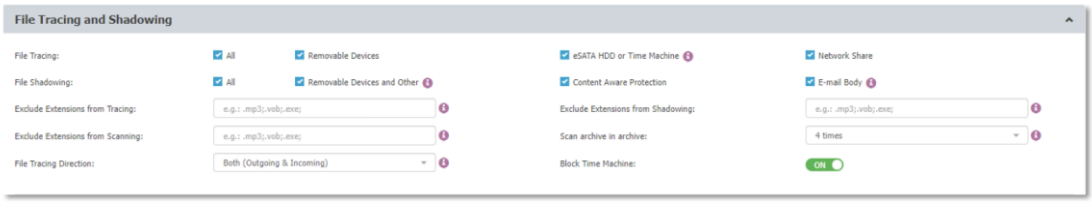
중요: 파일 추적없이 **파일 사본보관**은 사용할 수 없습니다.

파일 사본보관은 네트워크 트래픽 및 다른 컴퓨터 또는 파일 크기에 대한 Endpoint Protector 설정으로 연기될 수 있습니다. 사본보관 파일은 일반적으로 몇 분 후에 사용 가능합니다.

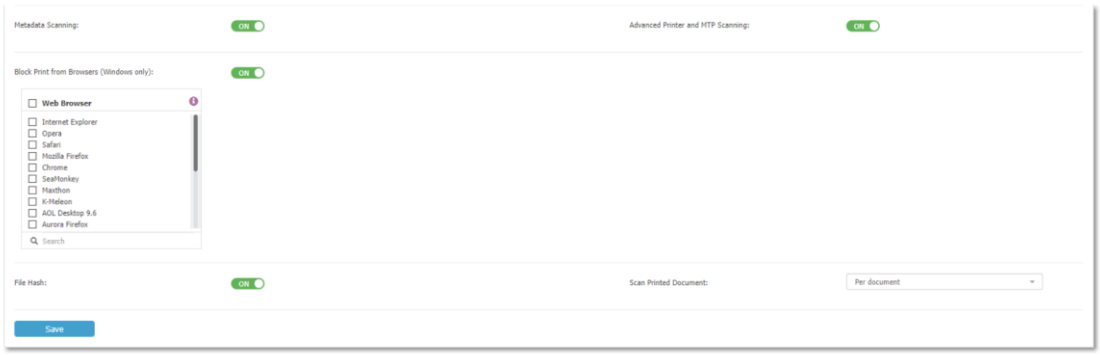
참고: 대규모 배포 (250-1000 엔드포인트)에서 가상 또는 하드웨어 어플라이언스의 총 수용량의 15% 까지만 파일 사본보관을 수행하는 것을 강력하게 권고합니다 (예: M1000 하드웨어 어플라이언스에서 파일 사본보관은 최적화된 성능을 위해서는 최대 150 엔드포인트만 할당해야 합니다.).

- **추적에서 제외된 확장자** – 특정 파일 유형에 대한 파일 추적을 하지 않을 수 있습니다.
- **검색에서 제외할 확장자** – 특정 파일 유형에 대한 검색을 하지 않을 수 있습니다.
- **파일 추적 방향** – 전송 방향을 기반으로 파일 전송을 모니터링 하도록 설정할 수 있습니다.
    - **발신 전송**은 로컬 머신에서 이동식 장치로 가는 전송입니다.
    - **수신 전송**은 이동식 장치에서 로컬 머신으로 가는 전송입니다.
    - **모두 (발신전송 및 수신전송)**은 이동식 장치와 로컬 머신 사이의 모든 유형의 전송을 모니터링 할 수 있습니다.

  참고: 파일 추적 방향 설정은 이동식 장치, 컴퓨터, 네트워크 공유 사이의 전송만 적용되고 Windows 와 macOS 11.0 이상에서만 동작합니다.
- **메타데이터 검색** – 이 설정을 사용하지 않으면 PDF, ZIP, 오피스 파일 (docx, xlsx, pptx, doc, xlx, ppt)에서 메타데이터는 검색되지 않습니다.
- **사본보관에서 제외된 확장자** – 이 설정은 특정 파일 유형에 대한 파일 사본보관을 하지 않습니다.
- **압축 파일 속의 압축 파일 검색** – 콘텐츠가 검색되는 압축 횟수를 정의하는 설정입니다.



- **타임머신 차단** – 이 설정을 사용하면 macOS에서 타임머신 백업을 차단합니다.
- **개선된 프린터 및 MTP 검색** – 이 설정을 사용하면 파일 차단 및 파일 사본보관에 대한 정확도를 늘리고 오탐을 줄일 수 있습니다. Windows에서만 사용 가능하고 컴퓨터는 재부팅이 되어야 합니다.
- **파일 해시** – 이 설정이 사용으로 되어 있으면 파일 해시가 생성되고 파일 전송 로그에 포함됩니다.
- **브라우저 인쇄 차단 –** Windows 에서만 사용 가능하고 다양한 브라우저 유형에서 웹 페이지 인쇄를 사용자가 못하도록 제한할 수 있습니다.
- **인쇄된 문서 스캔** – 특정 페이지 또는 전체 문서에서 위협이 제한되는 알림을 원할 때 선택합니다.



중요: 최신 Linux 우분투 버전에는 기본적으로 'snap' 기반 응용프로그램이 설치되어 있어 EPP 클라이언트에 영향을 줍니다. 이로 인해 파일 추적 및 파일 사본보관 아티팩트에서 파일 관련 이벤트가 누락될 수 있습니다. 'snap' 기반 응용프로그램에 대한 의존도는 파일 관련 웹 브라우저 활동에도 영향을 미쳐 이러한 제한을 더욱 악화시킵니다. 최적의 기능을 위한 대체 구성으로 'snap' 기반이 아닌 응용프로그램(가능한 경우)을 고려하시기

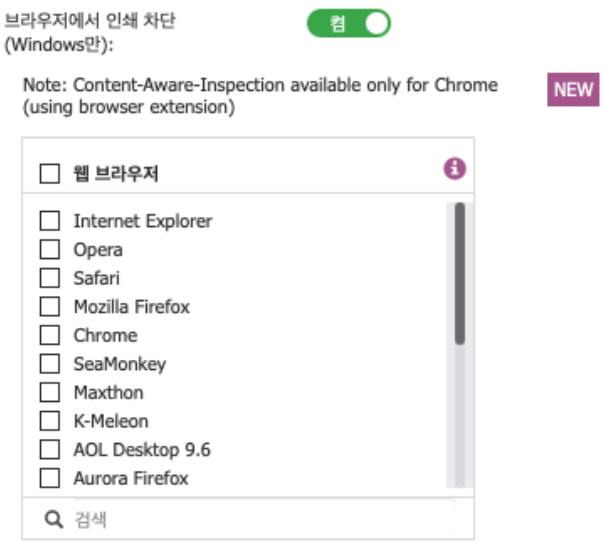
바랍니다.

5.7.3.1. 브라우저에서 인쇄 차단

이 설정은 사용자가 사용 가능한 다양한 브라우저 형식에서 웹 페이지 인쇄를 제한 하도록 만들 수 있습니다. 특정 브라우저를 정의하고 **정책 대상** 섹션의 **프린터**가 포함된 콘텐츠 인식 보호(CAP) 정책을 만들어 수행하도록 합니다.

참고: 이 설정은 Windows에서만 사용 가능합니다.

중요: "브라우저에서 인쇄 차단" 설정을 활성화하고 클라이언트에 이 구성을 적용한 후에 열려 있는 브라우저 탭을 다시 로드하거나 브라우저를 다시 시작해야 변경 사항이 적용되는 점을 유의하시기 바랍니다.



Google Chrome 웹 브라우저에서 문서가 프린터에 보내지면 정책 출구 지점 섹션의 프린터가 포함된 콘텐츠 인식 보호(CAP) 정책이 만들어지고 적용되어 콘텐츠 인식 탐지를 사용할 수 있습니다.

원활한 콘텐츠 인식 감지 및 보호를 위해 EPP 브라우저 연결 확장 프로그램은은 이 설정이 사용한 후 자동으로 설치가 됩니다. 이 확장 프로그램을 사용하면 Endpoint Protector가 정책에 따라

위협을 검사하고 탐지할 수 있습니다.

참고: 확장 프로그램은 '프라이빗/익명 모드에서는 동작하지 않습니다. 로드에 실패하면 인쇄를 포함한 전체 차단 모드로 전화되어 포괄적인 보호 기능을 제공합니다.

참고: 확장 프로그램의 안정성을 보장하고 사용자 간섭을 방지하려면 Google Chrome과 Microsoft Edge 모두 설치하는 독점적이고 권장되는 방법인 GPO(Group Policy Object)를 사용하시기 바랍니다.

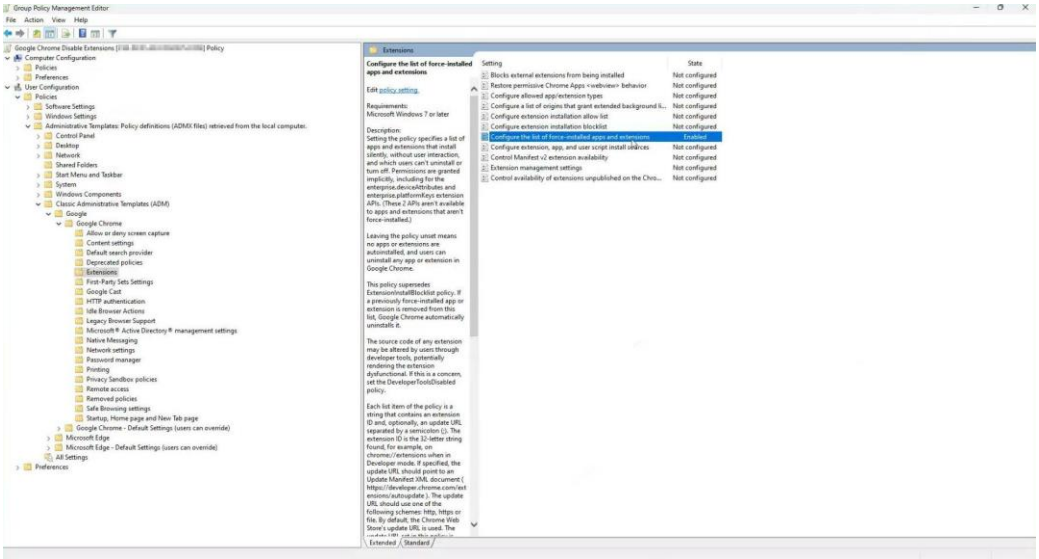
중요: 그룹 정책을 사용하여 웹 브라우저에서 PDF 파일이 열리지 않고 다운로드하도록 설정해야 브라우저에서 인쇄 차단이 정확하게 작동합니다.

중요: GPO(Group Policy Object)는 사용자가 Google Chrome 및 Microsoft Edge 확장 프로그램을 비활성화하거나 제거하지 못하도록 방지하는 유일한 지원 방법입니다.

5.7.3.2. 브라우저 확장을 위한 GPO 구성

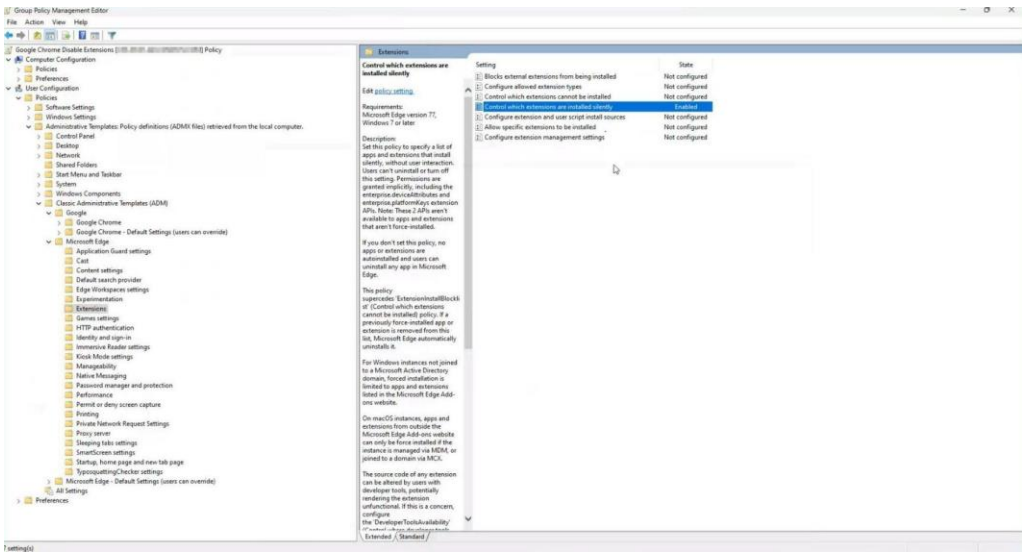
브라우저 확장 프로그램을 Windows 컴퓨터에 배포하고 사용자가 이를 제거하지 못하도록 GPO(Group Policy Object)를 구성하려면 아래 단계를 따르시기 바랍니다:

1. **Google Chrome**
    - 자세한 안내를 위해 공식 Google 지원 가이드를 참조 하시기 바랍니다.
    - Chrome Group Policy Template을 여기에서 다운로드 하시기 바랍니다.
    - 아래와 같이 Group Policy를 구성하시기 바랍니다.
        - EPP Browser Connector ID: **nnnaeanocbmnnjjlcfhcbpefmlgbcgoi**



2. Microsoft Edge

- Microsoft에서 제공된 가이드를 사용하시기 바랍니다: Microsoft Edge 구성
- 여기에서 Edge Group Policy Template를 다운로드 받으시기 바랍니다.
- 아래와 같이 Group Policy를 구성하시기 바랍니다.
    - EPP Browser Connector ID: **nnnaeanocbmnnjjlcfhcbpefmlgbcgoi**



중요: 통제된 환경에서 구성을 철저하게 테스트하여 의도한 대로 작동하는지 확인해야 합니다. 엔

드포인트 보안 정책을 항상 업데이트하고 조직의 보안 표준에 맞게 조정하시기 바랍니다.

5.7.4. 가상 프린터 무시

가상 프린터 이벤트를 무시하는 옵션이 도입되어 고객은 Microsoft의 PDF, PDFCreator 등과 같은 가상 프린터에 대해서 고객이 콘텐츠 인식 보호 (CAP)과 파일 추적의 가시성 제어를 강화했습니다. 이 강화된 기능은 주요 로그 공간을 절약하는데 도움이 될 뿐만 아니라 분석 및 관리 팀의 업무량을 줄입니다. 이 옵션으로 이제 PDF가 만들어지 시점 뿐만 아니라 조직 환경을 벗어날 때만 추적에 집중할 수 있어서 모니터링 작업이 간소화되고 효율성이 향상됩니다.

참고: 이 기능은 Windows에서만 동작합니다.

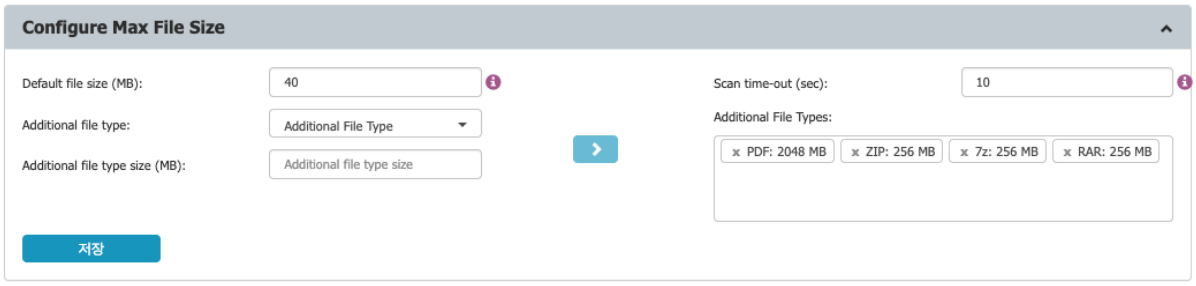
5.7.5. 파일 최대 크기 구성

이 섹션은 고객이 특정 사용 사례에 맞춰서 최대 파일 크기를 조정할 수 있습니다. 이 설정을 사용자 정의해서 Endpoint Protector는 조직의 요구 사항을 맞출 수 있습니다. 기본 최대 파일 크기는 40 MB로 설정되어 있고 최대 4096 MB로 제한되어 있습니다.

또한 기본적으로 다음과 같이 설정된 추가 파일 형식 크기를 유연하게 구성할 수 있습니다: PDF (2048 MB) 및 압축 파일 (256 MB). 이러한 파일 유형 크기는 특정 요구 사항에 맞게 1 KB에서 4 GB 범위 내에서 조정할 수 있습니다.

또한 Windows 환경에서는 10초의 기본 시간 제한이 적용됩니다. macOS의 경우 즉시 응답하지 않는 프로세스를 종료하는 Apple OS 아키텍처로 10초의 엄한 시간 제한이 적용됩니다. Linux는 현재 특정 시간 제한 없이 작동합니다.

참고: 이 설정은 콘텐츠 인시 정책(CAP)에만 적용되며 eDisocvery와 파일 사본보관의 최대 파일 크기에는 영향을 미치지 않습니다.



5.7.6. 근무외 시간 및 외부 네트워크

이 섹션에서 매체 제어와 콘텐츠 인식 보호 (CAP) 모듈에 대한 근무외 시간 및 외부 네트워크 관리를 할 수 있습니다.

⓾ **근무외 시간 정책** – 이 설정을 사용해서 **근무 요일**, **근무 시작 시간**, **근무 마침 시간**을 설정합니다.

⓾ **외부 네트워크 정책** – 이 설정을 사용해서 **DNS 내부망에만 있는 이름 (FQDN)**, **DNS IP 주소 목록**을 추가합니다.

이 설정이 만들어지면 대응 장치 유형 권한은 전체, 그룹, 사용자, 컴퓨터로 설정할 수 있습니다.

중요: 정책이 실행되면 대응 정책은 표준 장치 권한을 대체합니다. 대응 정책에서는 외부 네트워크 정책이 근무외 시간 정책을 대체합니다.

참고: 콘텐츠 인식 정책에 대해서 외부 네트워크 및 근무 외 시간 정책 또한 선택이 필요합니다.

5.7.7. 전송 제한

이 섹션에서 전송 제한 시간 주기 (시간)으로 전송 제한을 설정할 수 있습니다. 이 제한에 도달하면 응용프로그램 (콘텐츠 인식 보호) 제어를 위한 저장 장치 (매체 제어)의 파일 전송은 시간 주기 만료와 숫자가 초기화 될 때까지 더 이상 가능하지 않습니다. 비슷하게 네트워크 공유를 통한 파일 전송 또한 전송 제한에 포함됩니다.

전송 제한에 도달하는 시간을 확인하는 메커니즘은 컴퓨터 성능에 영향을 미치지 않도록 설계되었습니다.

그러므로 제한에 도달하는 정확한 시간과 전송 제한 실행 사이에 약간의 지연이 있을 수 있습니다. 일반적으로 몇 초 밖에 안 걸리지만 네트워크에 따라서는 몇 분 정도 걸릴 수도 있습니다.

전송 제한에 도달 할 때 세 가지 활동을 선택합니다:

- **모니터만** – 이 설정은 제한에 도달하면 보고합니다.
- **제한** – 이 설정은 매체 제어 정책에 정의된 장치와 응용프로그램을 차단합니다.
- **잠금** – 이 설정은 매체 제어 정책의 정의 여부와 관계없이 모든 장치를 차단합니다. 네트워크 인터페이스가 포함되어 모든 전송이 차단됩니다.

참고: 전송 제한 시간 주치 만료 전에 서버-클라이언트 통신을 재구축하면 전송 제한 리셋 오프라인 임시암호를 사용할 수 있습니다. 더 자세한 내용은 **오프라인 임시 암호** 챕터를 참조하시기 바랍니다.

전송 제한 도달 경고와 매일, 주별, 월별 기준으로 전송 제한 도달 보고서 스케줄을 사용할 수 있

습니다.

5.7.8. 디버그 로깅

특정 이슈에 대한 로그 수집과 고객 지원팀이 이슈 해결을 돕기 위한 결과 압축 파일을 보낼 때 이 기능을 사용할 수 있습니다.

이 기능을 사용해서 Endpoint Protector 클라이언트는 로그 파일을 생성하고 심층 패킷 검사 (DPI)가 사용 중이면 추가적으로 심층 패킷 검사 (DPI) 로그를 수집합니다.

참고: 디버그 설정은 심층 패킷 검사 (DPI)를 사용하지 않을 때 표준 진단 파일을 수집합니다.

5.7.8.1. 디버그 로깅 사용

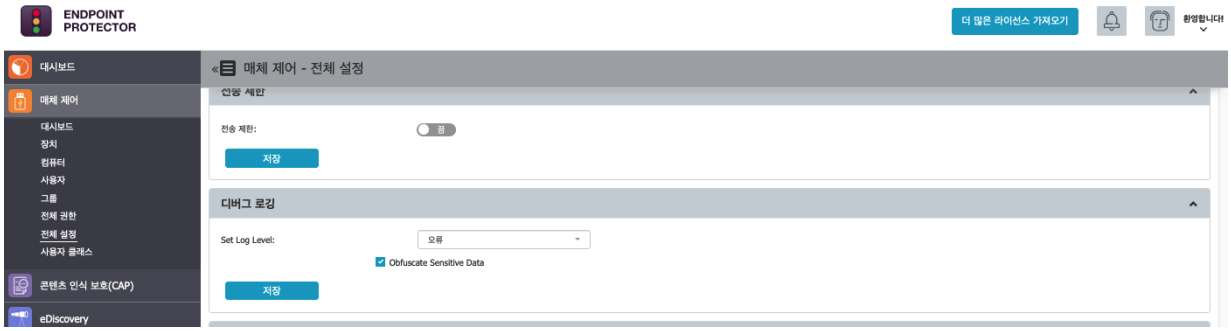
- 매뉴얼 로깅

디버그 기능을 사용하고 로그를 수집하기 위해서 다음 단계를 따르시기 바랍니다:

1. **전체 / 컴퓨터 / 사용자 설정** 페이지에서 다음 설정을 사용합니다.
    - **디버그 로깅** 섹션의 **디버그 모드**
    - 로그 레벨 선택 (없음, 오류, 경고, 정보, 디버그)

- 난해한 민감한 데이터 옵션을 선택하려면 오류, 경고, 정보, 디버그 로그를 선택
- **저장**

참고: 더 자세한 정보는 **난해한 데이터 규칙**을 읽으시기 바랍니다.



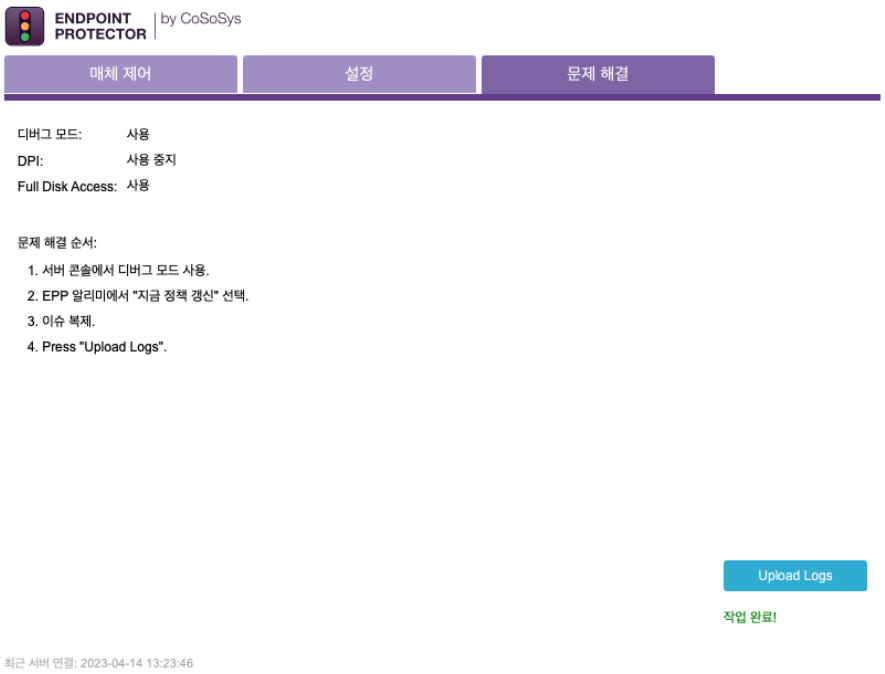
2. **Endpoint Protector 클라이언트** 아이콘을 오른쪽 클릭하고 **지금 정책 갱신**을 선택합니다;

3. 이슈를 복제해서 해당 로그를 생성합니다;

4. Endpoint Protector 클라이언트를 열고 **문제 해결** 탭으로 이동합니다;

5. **로그 업로드**를 클릭합니다 – Endpoint Protector 서버에 로그를 업로드 할 것입니다;

6. **전체 설정** 페이지로 이동해서 디버그 모드를 사용하지 않습니다.



- 자동 로깅

자동 로깅 옵션을 사용해서 수동 로깅 절차 (4번과 5번)에서 사용자 작업을 대체할 수도 있습니다.

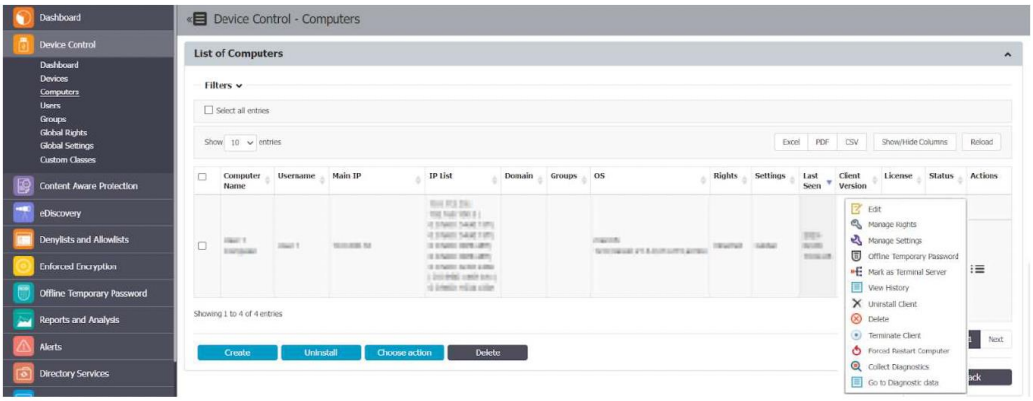
이 옵션은 **매체 제어, 컴퓨터** 페이지에서 사용할 수 있습니다.

컴퓨터를 호버링, 오른쪽 클릭 그리고 **진단 수집**을 선택합니다 – 컴퓨터 사용자의 입력 또는 지식 없이 특정 컴퓨터의 로그를 수집할 것입니다.

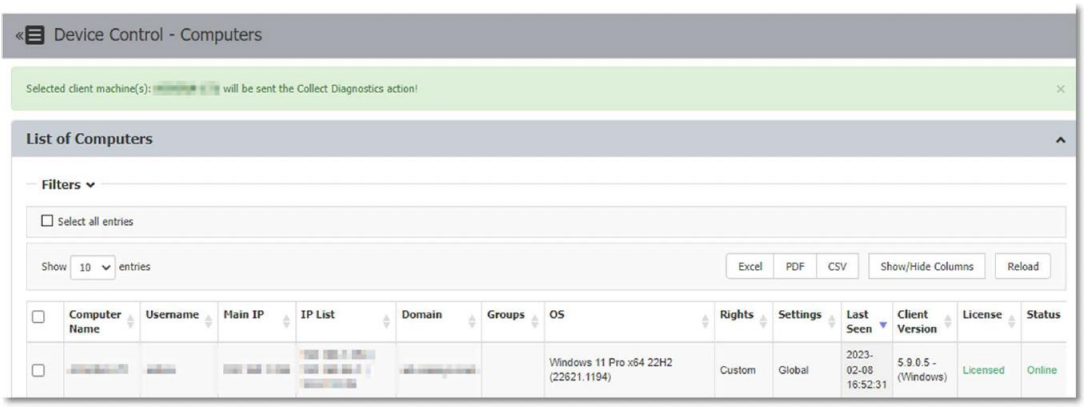
로그는 Endpoint Protector의 **로그 보고서** 페이지로 보내지고 진단 데이터를 받을 때 **아티팩트 받음** 이벤트가 등록됩니다.

5.7.8.2. 디버그 로깅 작업

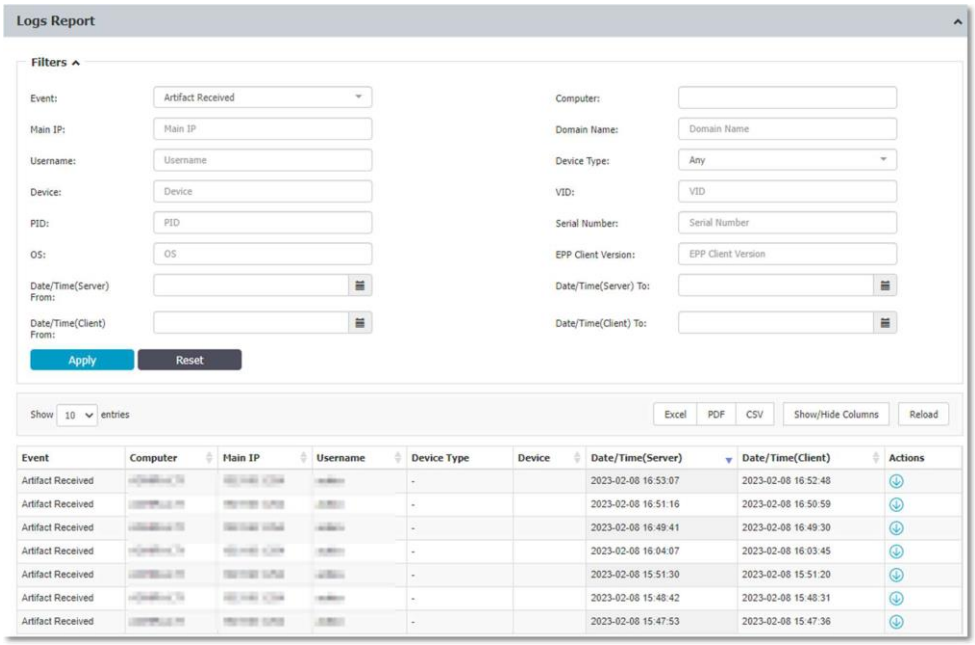
매체 제어, **컴퓨터** 페이지에서 **작업** 컬럼으로 이동해서 로그 작업을 봅니다.



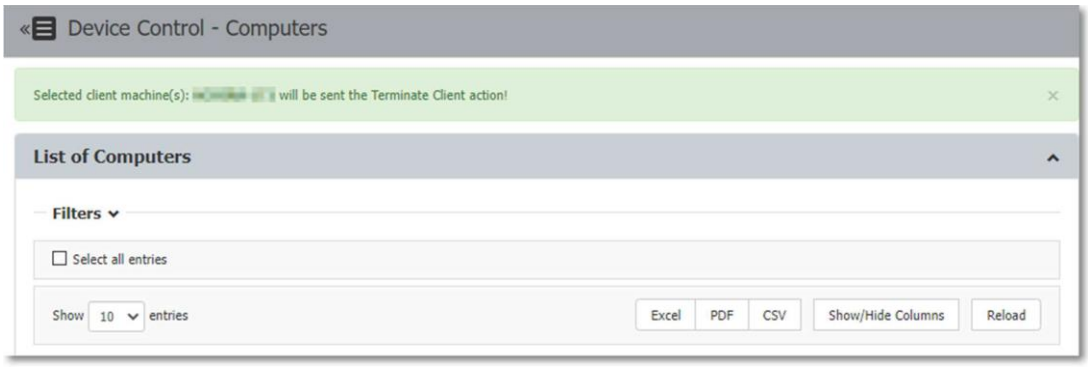
- **진단 수집** – 진단 데이터가 요청될 때 이벤트가 등록됩니다 (아티팩트 요청 이벤트)



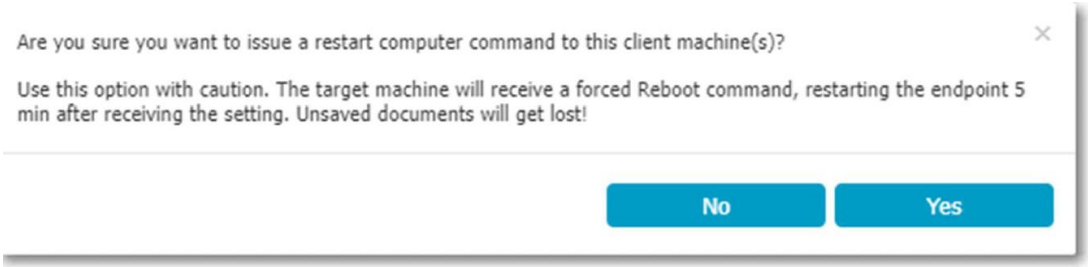
- **진단 데이터 이동** – 이 옵션은 **보고 및 분석**, **로그 보고서** 페이지, 디버그 모드 **로그 아티팩트 받음** 이벤트에서 사용자를 리디렉션합니다.

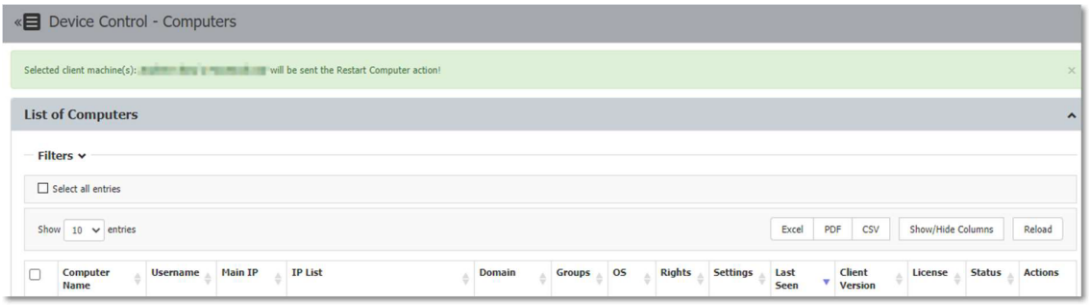


- **클라이언트 삭제** – 이 옵션은 Endpoint Protector 클라이언트를 삭제합니다.



- **강제 컴퓨터 재시작** – 이 옵션은 컴퓨터에 강제 재시작 명령을 보냅니다. 명령을 사용하고 10분 후에 컴퓨터는 재시작 됩니다. 사용자는 저장되지 않은 문서의 누락을 피하기 위한 경고 메시지를 받습니다.





5.7.8.3. 난해한 데이터 규칙

다음 규칙에 따르면 모든 데이터는 난해합니다.

- 위협의 길이가 12문자 이하이면 처음 4문자가 표시됩니다.

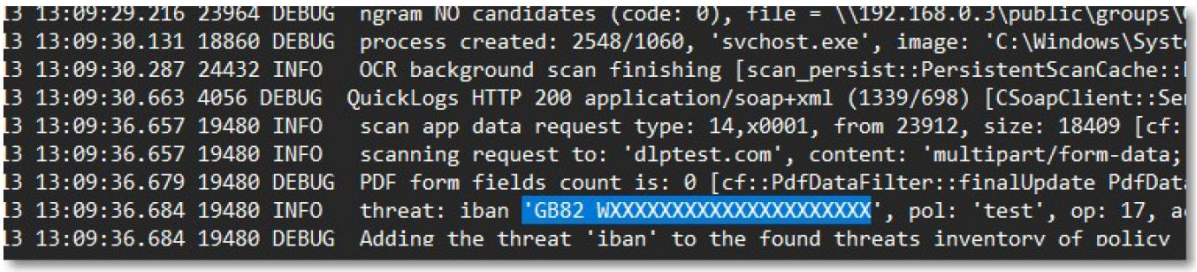
또는

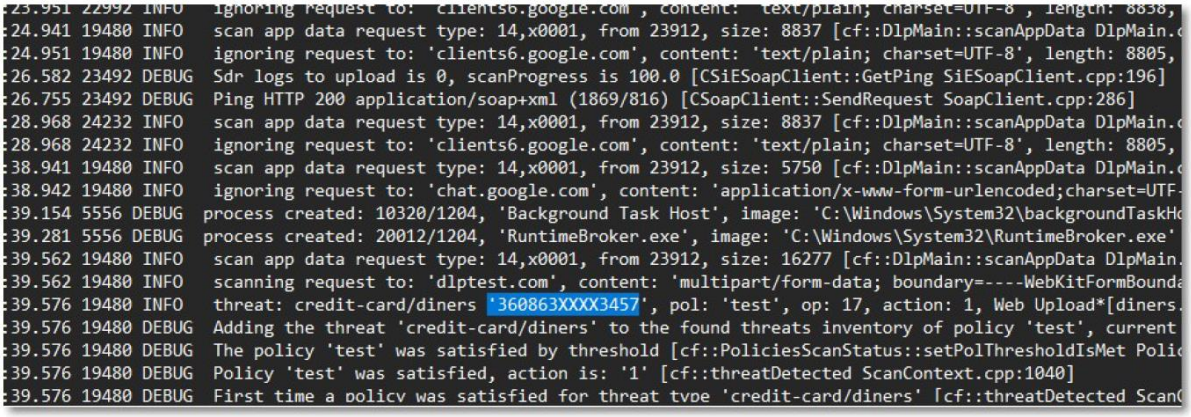
- 위협의 길이가 12문자 이상이면 처음 6문자가 표시됩니다.

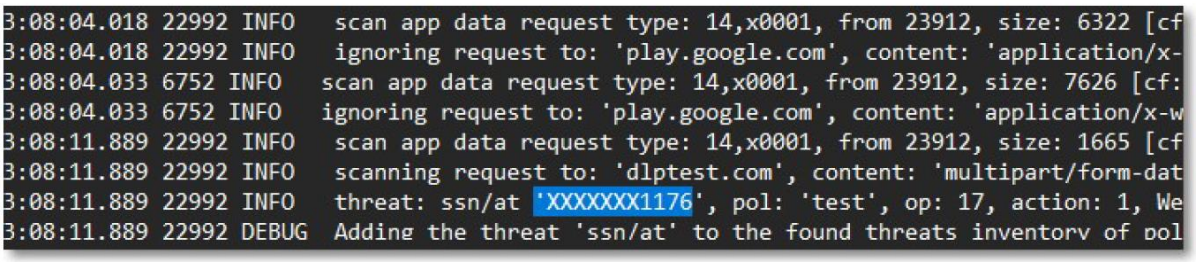
특정 사용 사례:

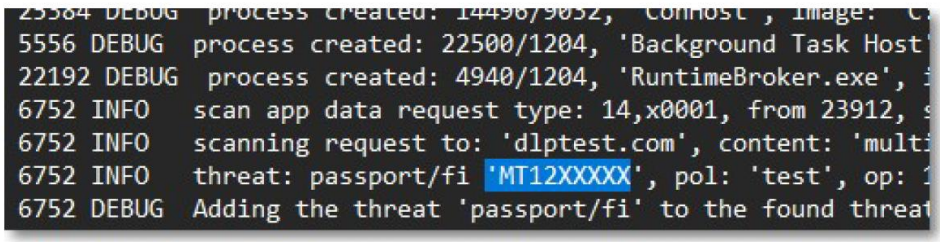
1. **신용카드**에서 PCI 보안 표준이 구현되었습니다.
2. **SSN**에서 마지막 4문자가 표시됩니다.
3. **브라질 ID** (CPF)에서 처음 3 그리고 마지가 2 문자가 난해합니다.

중요: 파일 유형 위협, 파일 크기 위협, 데이터 위협에서 데이터는 난해하지 않습니다.







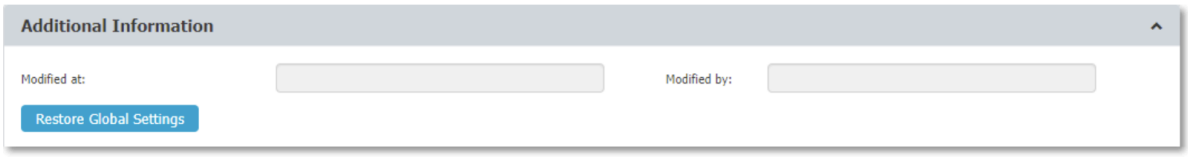


5.7.9. EasyLock 설정

이 섹션에서 EasyLock 설치를 허용하고 신뢰하는 Endpoint Protector 서버 목록 관련 또는 Endpoint Protector가 설치된 컴퓨터에서만 운영하도록 할 수 있습니다.

5.7.10. 추가적인 정보

이 설정에서 전체 설정을 복원하고 작업이 수행된 이름과 날짜를 볼 수 있습니다.

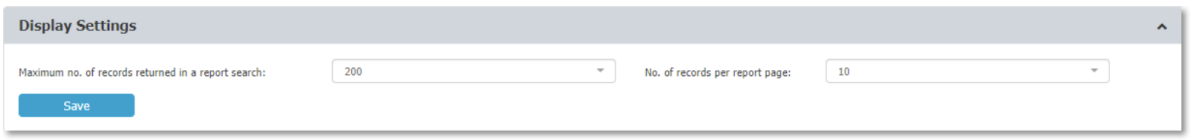


5.7.11. 화면 설정

이 섹션에서 Endpoint Protector 서버에 표시되는 최대 로그 수와 페이지 당 보고되는 수를 설정할 수 있습니다.

보고 당 표시되는 최대 10,000 로그를 설정할 수 있습니다. 로그 수가 최대 10,000 제한을 초과할 때 모든 엔터티를 내보내기 위해서 **내보내기 만들기** 옵션 또는 필터를 사용하여 검색을 범위를 줄입니다.

참고: 여기서 설정한 정보는 eDicovery에 또한 적용됩니다.

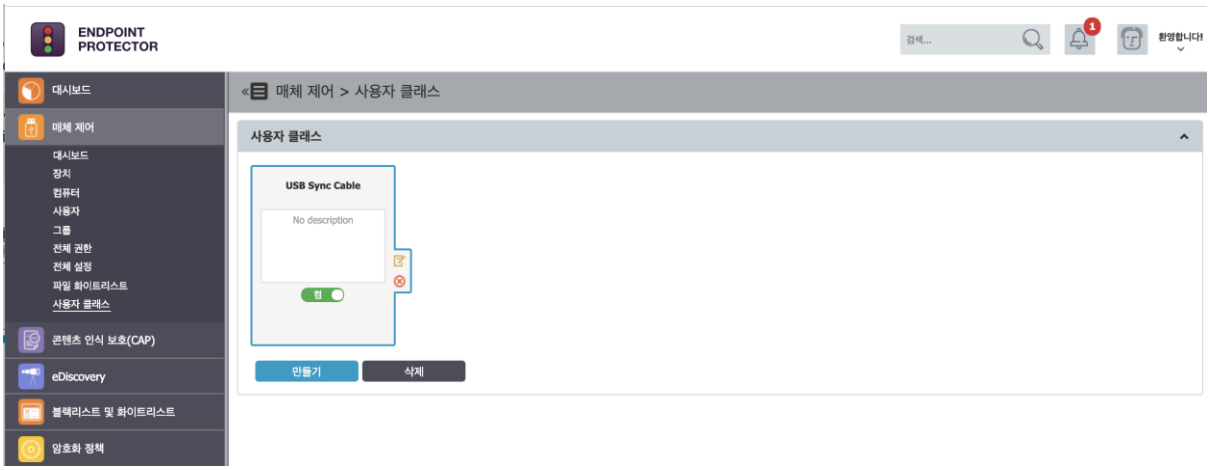


5.8. 사용자 클래스

이 섹션은 더 쉬운 관리를 위한 장치의 새로운 클래스를 만드는 옵션을 제공합니다. 특히 동일한 벤더와 제품 (동일한 VID 및 PID)를 가진 장치에서 매우 강력한 기능입니다.

새로운 사용자 클래스는 만들기 버튼을 클릭해서 만들 수 있습니다. 이미 존재하는 정책은 더블 클릭으로 편집할 수 있습니다.

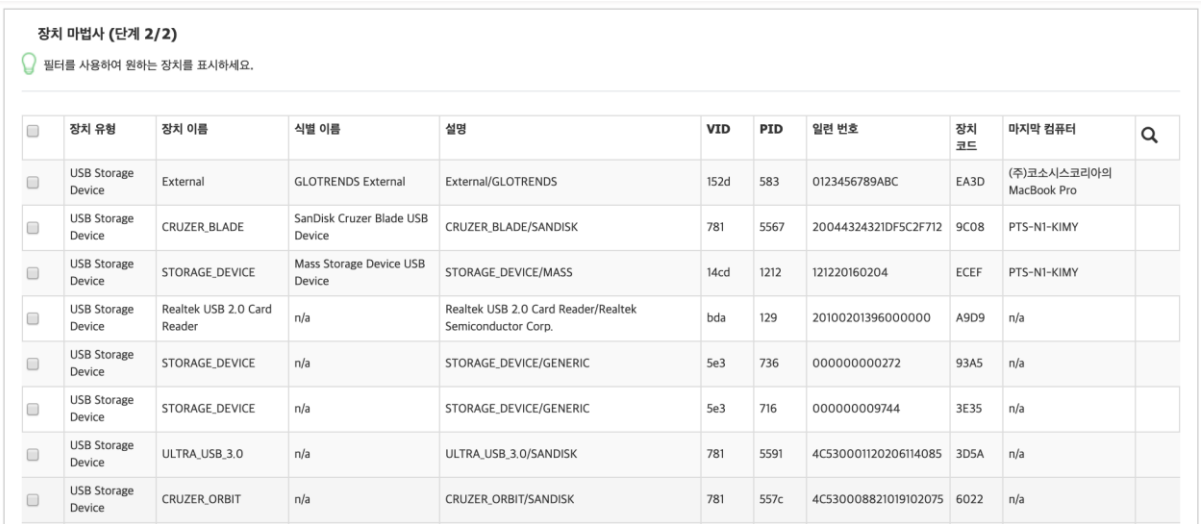
정책을 선택하면 편집, 복사, 삭제 할 수 있습니다.



사용자 클래스에 장치를 추가하기 전에 이름, 설명, 장치 종류 (USB 저장 장치, 카메라 등), 장치 권한 (사용 허용, 사용 거부 등)이 반드시 설정되어야 합니다. 한 번 설정되면 사용자 클래스에 장치 추가는 여러가지 방법으로 진행 할 수 있습니다.

- **새로운 장치 추가** – 팝업이 열리고 벤더 ID, 제품 ID, 일련 번호 기반으로 각 장치를 추가합니다. 우측의 녹색 +버튼을 누르면 장치를 계속 추가 할 수 있습니다.

- **기존 장치에 추가 (마법사)** – 팝업이 열리고 보호되는 컴퓨터에 전에 연결된 장치와 그 후에 Endpoint Protector 데이터베이스에서 이미 사용 가능한 장치들을 선택할 수 있습니다.



장치 유형	장치 이름	식별 이름	설명	VID	PID	일련 번호	장치 코드	마지막 컴퓨터
USB Storage Device	External	GLOTRENDS External	External/GLOTRENDS	152d	583	0123456789ABC	EA3D	(주)코소시스코리아의 MacBook Pro
USB Storage Device	CRUZER_BLADE	SanDisk Cruzer Blade USB Device	CRUZER_BLADE/SANDISK	781	5567	20044324321DF5C2F712	9C08	PTS-N1-KIMY
USB Storage Device	STORAGE_DEVICE	Mass Storage Device USB Device	STORAGE_DEVICE/MASS	14cd	1212	121220160204	ECEF	PTS-N1-KIMY
USB Storage Device	Realtek USB 2.0 Card Reader	n/a	Realtek USB 2.0 Card Reader/Realtek Semiconductor Corp.	bda	129	20100201396000000	A9D9	n/a
USB Storage Device	STORAGE_DEVICE	n/a	STORAGE_DEVICE/GENERIC	5e3	736	000000000272	93A5	n/a
USB Storage Device	STORAGE_DEVICE	n/a	STORAGE_DEVICE/GENERIC	5e3	716	000000009744	3E35	n/a
USB Storage Device	ULTRA_USB_3.0	n/a	ULTRA_USB_3.0/SANDISK	781	5591	4C530001120206114085	3D5A	n/a
USB Storage Device	CRUZER_ORBIT	n/a	CRUZER_ORBIT/SANDISK	781	557c	4C530008821019102075	6022	n/a

- **일련번호 범위 추가** – 팝업이 열리고 일련번호의 첫 번째와 마지막 번호를 지정해서한 번에 추가할 수 있습니다. 이 기능의 권장 사용은 연속되는 범위와 명확한 패턴의 일련번호를 가진 장치에 사용하는 것입니다.

참고: 이 기능은 명확한 패턴이 없는 시리얼 번호를 가진 상황에서도 동작을 하지만 권장하지는 않습니다. 이러한 경우 일부 장치는 Endpoint Protector가 무시할 수도 있어서 원하는 사용자 클래스 효과를 낼 수 없습니다.

- **대량 장치 추가** – 팝업이 열리고 동일한 유형의 장치 500개까지 등록할 수 있습니다. 목록을 가져오거나 단순히 붙여 넣기로 등록할 수 있습니다.

- **장치 클래스 (장치 유형)** – 이 옵션은 시스템의 모든 장치를 매우 빠르게 변경하고 특정 장치만 일부 사용자 또는 컴퓨터에 적용하는 상황에서 사용되도록 만들어 졌습니다.

예: 위의 경우에 커스텀 클래스 CD-ROM 허용을 만들고 CD-ROM / DVD-ROM 장치 유형의 접근 허용을 설정합니다. 클라이언트 PC CIP0에 설정된 CD-ROM 사용 거부 권한에 대해 알아보겠습니다. CD-ROM 사용 허용 커스텀 클래스가 만들어지고 사용으로 되어 있으면 심지어 클라이언트 PC CIP0이 사용 거부 권한을 가지고 있어도 모든 CD-ROM / DVD-ROM은 허용됩니다.

5.9. 장치 권한 우선순위

컴퓨터 권한, 그룹 권한, 정체 권한은 단일 설정이고 각각 다른 설정을 상속합니다. 이것은 하나가 변경되면 다른 설정에 영향을 미치는 것을 의미합니다.

전체 권한, 그룹 권한, 컴퓨터 권한 세 가지 계층 구조가 있습니다. 권한 관리를 결정하는 요소를 후에 알아보겠습니다.

장치 권한은 모든 컴퓨터, 그룹, 전체 권한보다 우선합니다.

사용자 권한은 컴퓨터 권한과 같은 레벨에 있습니다. 우선순위는 시스템 설정 섹션에서 설정할 수 있습니다.

참고: 더 자세한 내용은 **구분 사용** 섹션을 참조하시기 바랍니다.

구분 코드 기반으로 클라이언트에 허용하는 옵션을 선택합니다. 또한 **기본 구분 코드**인 – defdep를 볼 수 있습니다.

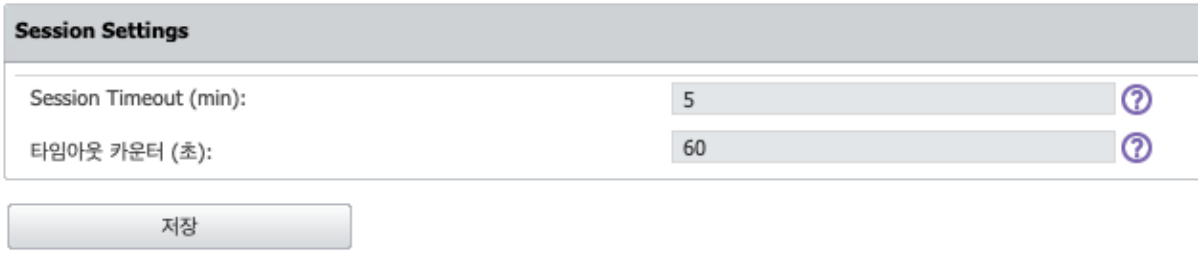
참고: 더 자세한 내용은 **시스템 구분** 섹션을 참조하시기 바랍니다.

5.9.1 세션 설정

세션 타임아웃 설정을 따라 수정할 수 있습니다:

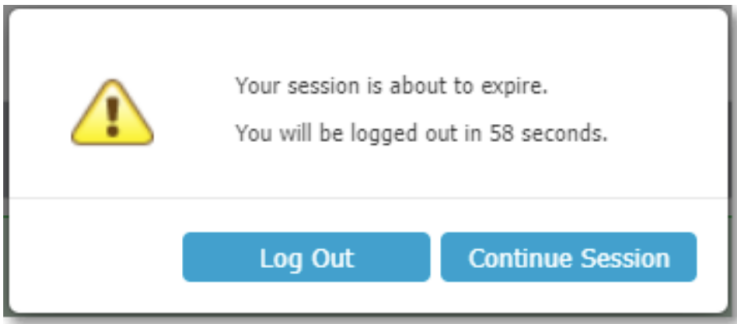
- **세션 타임아웃** – 5분에서 60분 사이에 세션이 만료될 때까지 사용자의 비활성화 시간을 설정합니다.
- **타임아웃 카운터** – 5분에서 (세션 타임아웃 – 1분) 시간 사이에 세션 타임아웃 카운트다운에 대한 시간을 설정합니다.

예: 세션 타임아웃이 5분으로 타임아웃 카운터가 60초로 정의되어 있으면 비활성화까지 4분이 지난 후에 60초 후에 로그아웃이 된다는 팝업 창의 알림을 받게 됩니다.

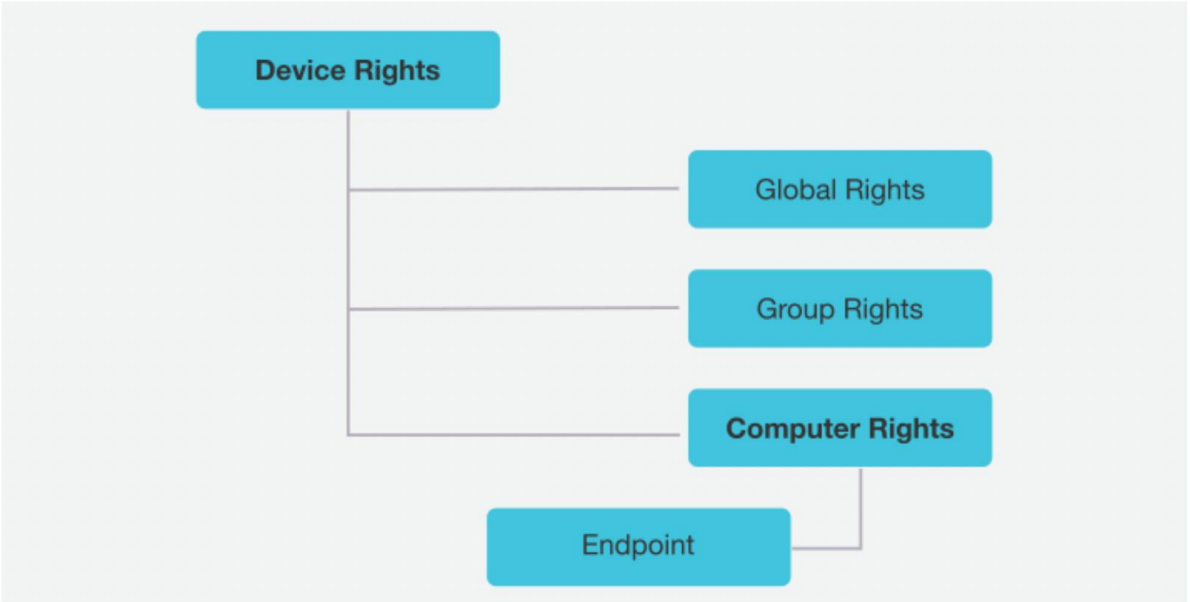


정의된 시간 동안 작업이 없으면 Endpoint Protector는 미리 정의된 카운트다운의 세션이 만료되는 메시지 표시와 응답을 멈추게 됩니다.

세션 타임아웃 간격을 재설정해서 세션을 계속 연결하거나 로그아웃을 선택할 수 있습니다.



Endpoint Protector 권한 기능



예: 장치 X 는 전체 권한으로 허용되어 있습니다. 만약 컴퓨터 권한으로 같은 장치를 허용 거부를 하면 장치는 사용할 수 없습니다. 같은 장치를 다음과 같이 반대로 적용합니다. 전체 권한을 사용 거부로 설정하고 컴퓨터에서 사용 허용 권한을 설정하면 장치를 사용할 수 있습니다. 같은 장치를 다음과 같이 그룹과 전체 권한을 설정합니다. 전체 권한을 사용 거부로 설정하고 그룹을 사용 허용으로 설정하면 장치를 사용할 수 있습니다.

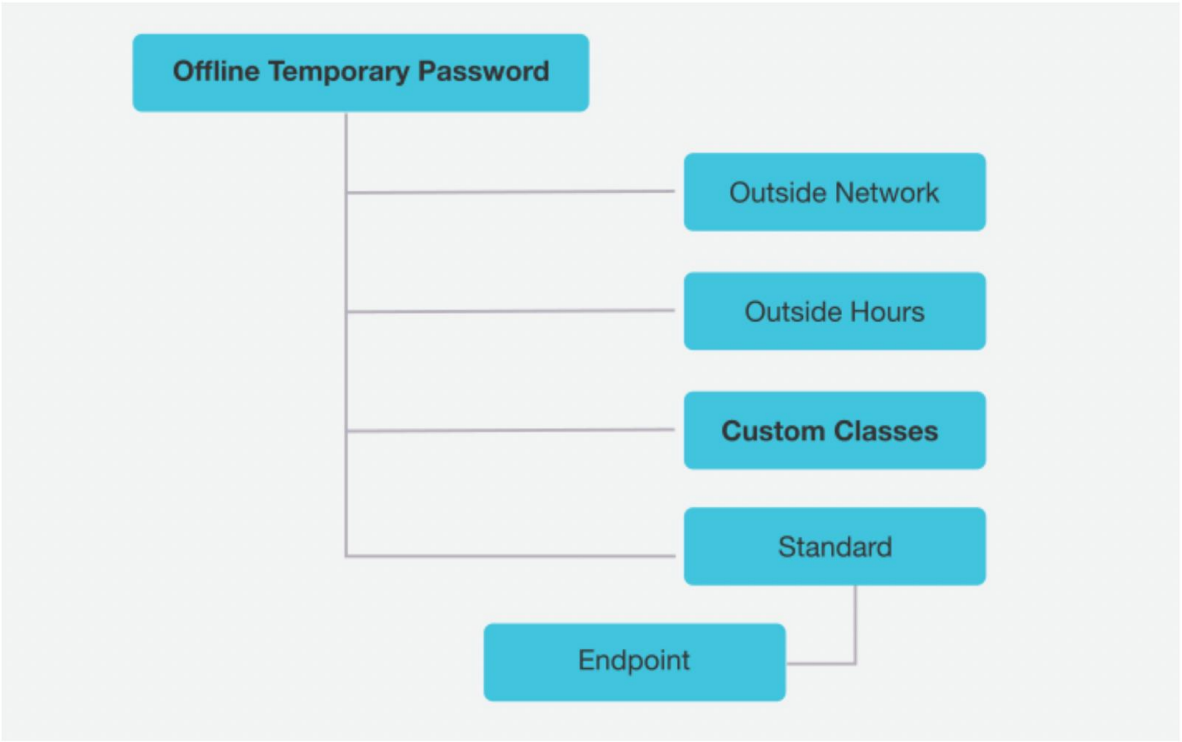
5.9.2. 매체 제어 정책 우선순위

매체 제어 정책은 기본적으로 사용할 수 있습니다. 여기에는 장치 유형과 이미 존재하는 장치 섹션이 포함되어 있습니다.

사용자 클래스를 정의할 수 있습니다. 전체 네트워크에 특정 접근 권한을 가진 그룹입니다. 사용자 클래스는 표준 매체 제어 권한보다 우선이 됩니다.

외부 네트워크와 업무 시간 장치 권한이 설정이 되어있다면 이 권한은 사용자 클래스보다 우선이 됩니다.

오프라인 임시 암호 권한으로 예외 처리를 할 수 있습니다. 이 권한은 모든 권한보다 우선이 됩니다.



6. 콘텐츠 인식 보호(CAP)

이 모듈에서 관리자는 선택된 사용자, 컴퓨터, 그룹 또는 구분에 대한 강력한 콘텐츠 필터링 정책을 강제화하고 설정하고 아래와 같이 민감한 회사 데이터의 의도적 또는 휴먼 에러를 통한 파일 전송에 노출된 위험을 제어합니다.

- **개인 식별 정보 (PII)**: 주민등록번호, 운전면허번호, 이메일 주소, 여권번호, 전화번호, 주소, 날짜 등.
- **금융 및 신용 카드 정보**: Visa, MasterCard, American Express, JCB, Discover Card, Dinners 신용 카드 번호 및 계좌 번호 등.
- **기밀 파일**: 세일즈 및 마케팅 보고서, 기술 문서, 회계 문서, 고객 데이터베이스 등.

중요: Endpoint Protector는 암호화된 파일 또는 보안 통신으로 암호화를 사용하는 응용프로그램을 스캔할 수 없습니다.

민감한 자료 유출을 예방하기 위해서 Endpoint Protector는 다양한 엔드포인트의 모든 활동을 면밀하게 모니터링합니다.

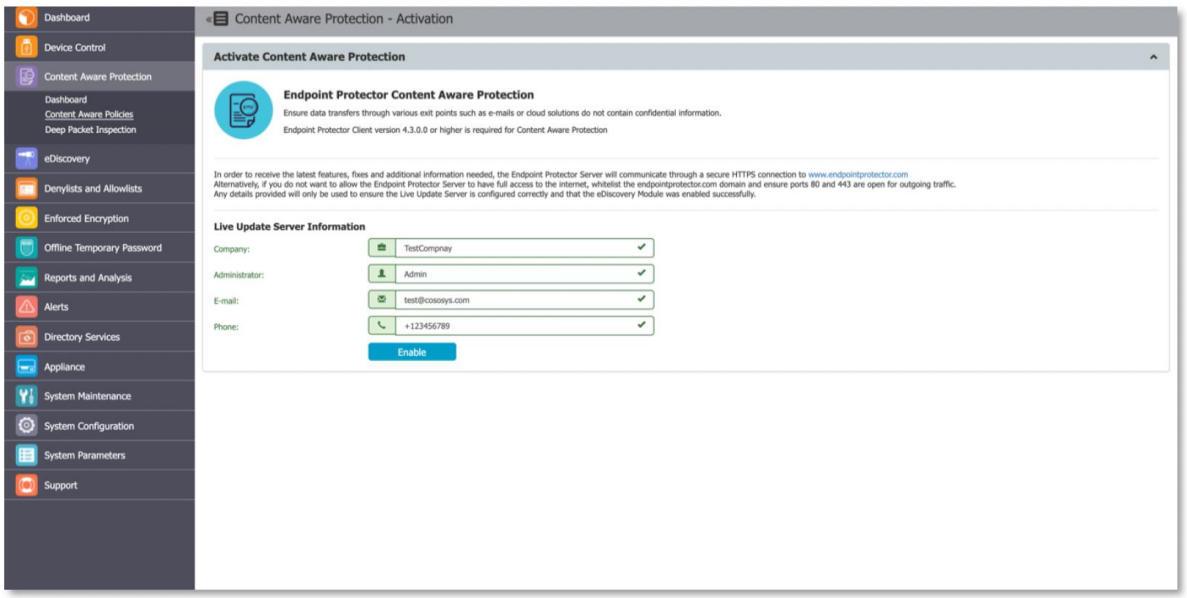
- 휴대용 저장 장치 및 다른 매체의 전송 (USB 드라이브, 외장 HDD, CD / DVD, SD 카드 등) 과 암호화 소프트웨어를 통한 예방 (예> EasyLock)
- 로컬 네트워크 전송 (네트워크 공유)
- 인터넷을 통한 전송 (이메일 클라이언트, 파일 공유 응용프로그램, 웹 브라우저, 인스턴트 메시징, 소셜 미디어 등)
- 클라우드를 통한 전송 (iCloud, Google Drive, Dropbox, Microsoft SkyDrive 등)

- 복사 / 붙여넣기 (클립보드)를 통한 전송
- 프린트 스크린
- 프린터 및 기타

6.1. 콘텐츠 인식 보호 활성화

콘텐츠 인식 보호는 Endpoint Protector의 선택 기능입니다. 모듈은 보이지만 '기능 사용 (Enable Feature)' 버튼을 누르는 것과 최고 관리자의 연락처 상세정보를 입력하여 간단하게 활성화하는 절차가 필요합니다.

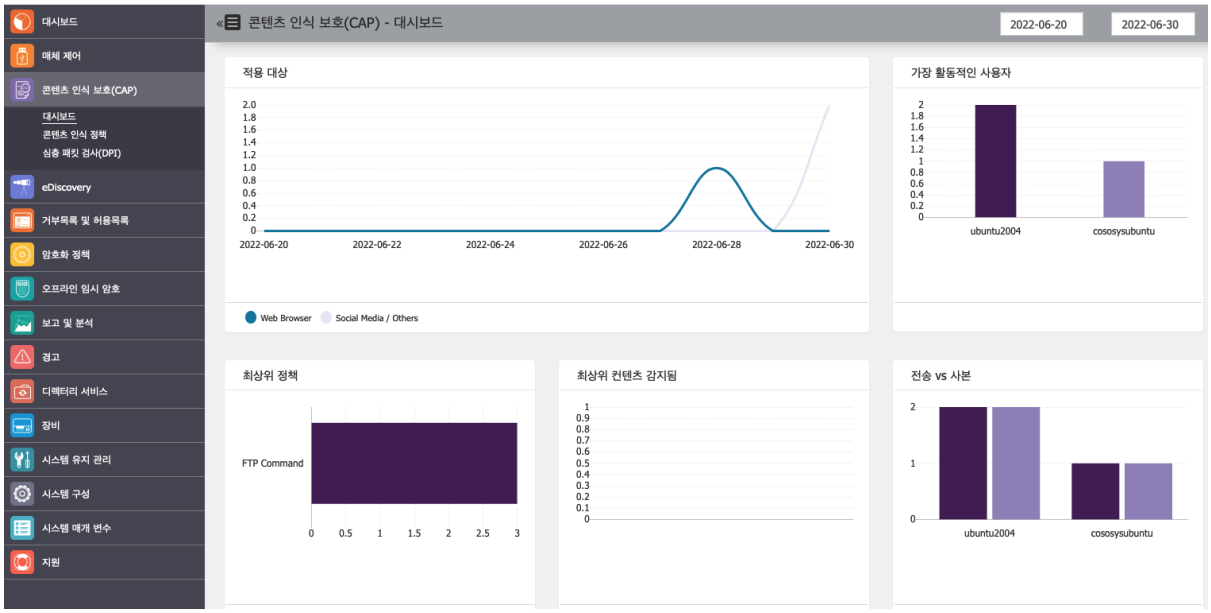
참고: 모든 상세 내용은 Live Update 서버 정확하게 설정이 되었는지 그리고 콘텐츠 인식 보호 모듈이 성공적으로 사용할 수 있는지 확인하는 용도로만 사용이 됩니다.



중요: 콘텐츠 인식 보호 모듈은 매체 제어 또는 eDiscovery 모듈과 분리되어 있습니다. 각각의 라이선스가 필요합니다.

6.2. 대시보드

이 섹션은 콘텐츠 인식 보호 모듈과 관련된 정보를 그래픽과 차트의 형태로 빠르게 현황을 볼 수 가 있도록 제공합니다.



6.3. 콘텐츠 인식 정책

콘텐츠 인식 정책은 선택된 엔터티 (사용자, 컴퓨터, 그룹, 구분)에서 파일 전송 관리 실행하는 민감한 콘텐츠 탐지에 대한 규칙입니다.

이 섹션에서 새로운 정책을 만들고 존재하는 정책을 편집 또는 삭제하거나 이미 정의된 정책을 만들고 적용할 수 있습니다.

예: 콘텐츠 인식 정책은 신용카드번호와 이메일을 AND 논리로 차단하도록 설정할 수 있습니다. 이 경우 신용카드번호와 이메일을 포함한 파일만 차단됩니다. 만약 신용카드번호 포함한 파일의 전송은 차단되지 않습니다.

각 회사들은 그들의 특정 활동 영역, 목표 산업, 역할에 맞는 사용자 키워드로 자신만의 민감한 콘텐츠 데이터를 정의할 수 있습니다.

이 작업을 쉽게 하기 위해서 콘텐츠 인식 모듈은 대부분 많이 사용하는 기밀 용어 및 표현 포함된 미리 정의된 사용자 키워드를 가지고 있습니다.

예: 회사 재무 부서에서 이메일로 보내는 엑셀 보고서를 차단하거나 개인 식별 및 재무 정보 (예: 신용카드번호, 이메일, 전화번호, 주민등록번호 등)가 포함된 모든 파일 전송에 대한 보고를 하도록 정책을 설정할 수 있습니다.

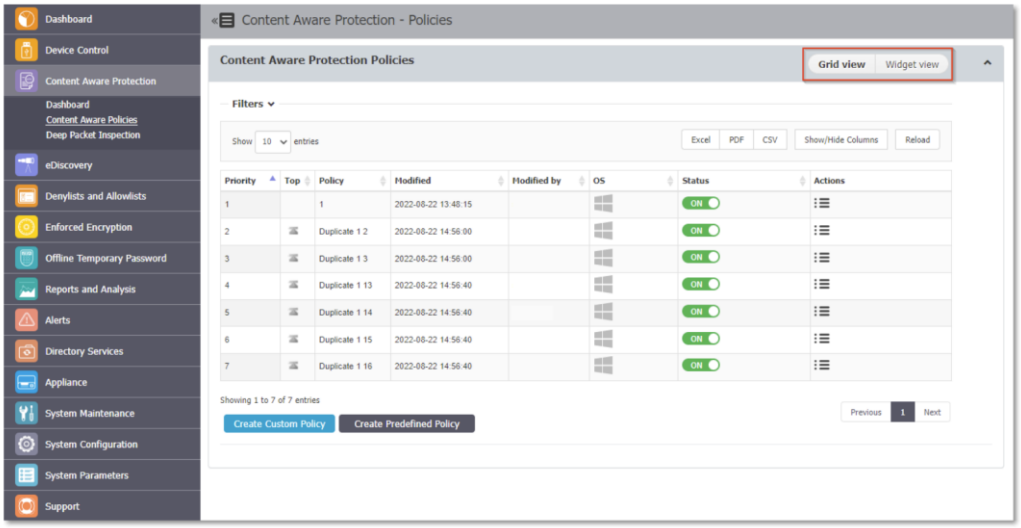
참고: 콘텐츠 인식 정책은 파일 허용목록 (매체 제어 > 파일 허용목록)에도 적용됩니다. 이전에 이렇게 허용 목록된 모든 파일은 민감한 콘텐츠 탐지로 검사가 될 것이고 정책에 따라 보고만 또는 보고 및 차단으로 적용되는 것을 의미합니다.

매체 제어 정책과 동일하게 콘텐츠 인식 정책도 회사 네트워크에서 컴퓨터 통신이 연결되지 않아도 계속 실행됩니다.

하나 또는 그 이상의 콘텐츠 인식 정책이 같은 컴퓨터, 사용자, 그룹, 구분에서 실행될 수 있습니다. 규칙 사이에 이러한 간섭을 피하기 위해서 정책 우선 순위는 왼쪽에서 오른쪽 순으로 수행됩니다. 가장 왼쪽의 정책이 가장 높은 우선 순위 (우선 순위 1)을 가지고 반면에 가장 오른쪽 정책이 가장 낮은 우선 순위를 가집니다. 하나 또는 그 이상 정책의 우선 순위에 대한 변경은 높은 우선 순위는 왼쪽 화살표 또는 낮은 우선 순위는 오른쪽 버튼을 클릭하여 정책을 오른쪽 또는 왼쪽으로 이동하여 수행할 수 있습니다.

더 쉽게 콘텐츠 인식 보호(CAP) 정책을 관리하려면 다음 옵션을 사용하시기 바랍니다:

- 오른쪽 상단에 **그리드** 또는 **위젯** 보기 옵션을 스위치
- 정책에 최우선 순위 할당을 위해 **탑** 버튼 사용
- 엔터티 편집을 위해 **우선순위** 컬럼의 정책을 더블 클릭



6.3.1. 정책 정보

48개까지 콘텐츠 인식 정책을 만들 수 있습니다.

콘텐츠 인식 정책을 만들기 위해서 다음 정보가 제공되어야 합니다:

참고: 특정 응용프로그램과 OS의 의존으로 일부 제한이 적용될 수 있습니다.

- **OS 종류** – 정책에 적용할 OS 종류를 선택 (Windows, Mac OS X, Linux)
- **정책 이름** – 정책 이름 제공
- **정책 설명** – 정책 설명 기술
- **정책 작업** – 수행되는 동작 유형 선택 (차단 및 보고, 보고만 , 차단만, 차단 및 수정)
    - **차단 및 보고** – 이 정책은 민감한 콘텐츠가 포함된 모든 데이터 전송을 차단하고 활동을 보고합니다.
    - **보고만** – 이 정책은 민감한 콘텐츠가 포함된 모든 데이터 전송을 허용하고 활동을 보고만 합니다.
    - **차단만** – 이 정책은 민감한 콘텐츠가 포함된 모든 데이터 전송을 차단하지만 활동은 보고하지 않습니다.

- **차단 및 교정** – 이 정책은 민감한 콘텐츠가 포함된 모든 데이터 전송을 차단하지만 사용자가 정당한 사유를 사용해서 차단을 수정할 수 있습니다.

참고: 초기 사용 시 네트워크의 데이터 흐름을 볼 수 있고 활동을 방해하지 않기 때문에 보고만 정책을 사용하는 것을 추천 드립니다.

- **정책 유형** – 정책 유형 선택 (표준, 외부 네트워크, 근무외 시간)

참고: 근무외 시간 및 외부 네트워크 옵션을 보정하기 위해서 정책을 저장한 후에 매체 제어, 전체 설정, 그룹 또는 컴퓨터에서 특정 장치 설정을 사용합니다.

- **정책 템플릿** – 드롭 다운 목록에서 커스텀 알림을 선택하거나 **시스템 파라미터, 장치 유형, 커스텀 콘텐츠 인식 보호 알림**에서 만듭니다.
- **전체 임계값** – 사용하지 않으면 일반 임계값으로 간주됨
- **위협 임계값** – 파일 전송에서 콘텐츠 위반을 허용하는 최대 개수
- **파일 크기 임계값** – 파일 전송의 차단 또는 보고를 시작하는 파일 크기 (MB) 입력

참고: 파일 크기 임계값을 설정하면 정책 안에서 파일 형식 또는 사용자 키워드에 관계없이 모든 정책에 적용됩니다. 파일 크기 임계값에 사용되는 값은 양의 정수가 되어야 합니다.

- **파일 크기 임계값이 일치하면 정책 적용** – 이 옵션을 사용하면 임계값과 정책이 함께 적용됩니다. 거부목록에서 확인된 모든 것은 임계값을 고려하여 차단될 것입니다. 이 설정은 파일 이름과 파일 위치에는 적용되지 않습니다.

중요: 이 설정은 파일 이름과 파일 위치에 적용되지 않습니다.

참고: 임계값 옵션은 미리 정의된 콘텐츠, 사용자 키워드, 정규식을 포함한 여러 필터에만 적용됩니다. 일반적인 규칙으로 임계값을 사용하는 차단 및 보고 정책은 보고만 정책보다 더 높은 우선순위에 두는 것을 권장합니다.

- **정책 상태** – 정책 상태 활성화 설정을 사용할 수 있습니다.

- **클라이언트 알림** – 클라이언트에 알림을 보내는 설정을 사용할 수 있습니다.

6.3.1.1. 일반 및 전체 임계값 사용 사례

① 차단 및 보고 정책으로 임계값을 4로 설정합니다. 여러 브라우저에 대해서 SSN (Social Security Numbers)의 전송에 대한 정책입니다.

4로 설정된 일반 임계값은 선택된 브라우저에서 SSN이 4개 이상인 콘텐츠가 포함된 모든 전송을 차단하지만 SSN 1개, 2개, 3개의 개별 전송은 차단하지 않습니다.

4개 이상의 같은 유형을 차단하는 일반 임계값과 반대로 전체 임계값은 서로 다른 유형의 위협이 합쳐서 4개 이상일 때 차단합니다.

② 차단 및 보고 정책으로 임계값을 2로 설정합니다. SSN 및 전화번호 전송입니다.

일반 임계값 정책에서 위의 2개 위협은 차단되지 않고 전체 임계값으로만 차단이 됩니다. 반면에 2개의 SSN 전송은 일반 및 전체 임계값으로 모두 차단됩니다.

6.3.2. 정책 대상

전송이 제어되는 출구 포인트 입니다:

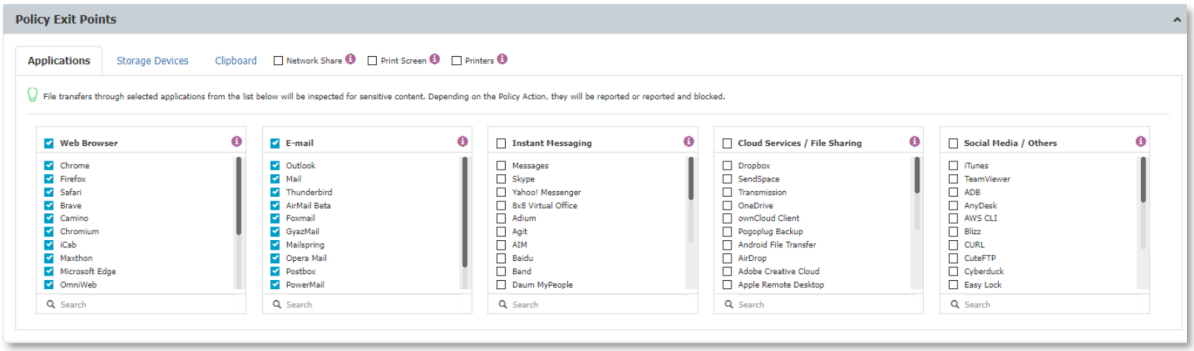
6.3.2.1. 응용프로그램

- **웹 브라우저** (예: Internet Explorer, Chrome, Firefox, Safari 등)
- **이메일 클라이언트** (예: Outlook, Thunderbird, Lotus Notes 등)

중요: Windows 10 Mail 응용프로그램을 포함한 유니버셜 Windows 플랫폼 응용프로그램은 add-on 사용이 제한된 고립된 환경에서 운영됩니다. 콘텐츠 인식 보호(CAP)에서 Windows Mail을 정책 대상으로 설정해서 제한된 파일 전송을 차단하여 데이터 유출을 예방합니다.

- **인스턴스 메시징** (예: Skype, Pidgin, Google Talk 등)
- **클라우드 서비스 / 파일 공유** (예: Google Drive 클라언트, iCloud, Dropbox, DC++ 등)
- **소셜 미디어/기타** (예: iTune, Total Commander, GoToMeeting 등)

참고: 웹 브라우저 범주에서 Adobe Flash Player를 선택하면 Adobe Flash Active X를 사용하는 사이트를 차단합니다.



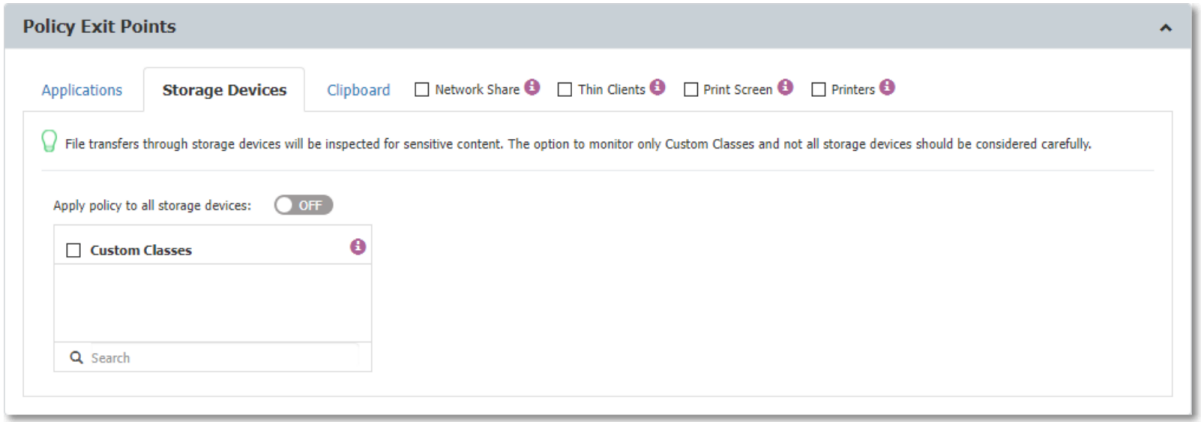
6.3.2.2. 저장 장치

저장 장치 탭에서 전송 모니터링을 선택할 수 있습니다:

- **커스텀 클래스만**
- **모든 저장 장치** – **모든 저장 장치에 정책 적용** 사용은 커스텀 클래스를 제외하고 모든 저장 장치의 콘텐츠 정책에 시행됩니다.

참고: Windows에서 이동식 매체로 들어가고 나가는 파일 전송은 모니터링 됩니다.

중요: Linux에서 붙여넣기 기능은 기본 gnome 세션이 Xorg 일 때만 동작합니다. 다른 gnome 세션에서 붙여넣기 기능은 사용할 수 없습니다 (예: wayland).



CD/DVD 버닝 차단

이 기능은 Windows에서만 사용 가능하고 내장 또는 제 3업체 버닝 기능 관련입니다.

사용자가 내장 Windows 기능을 사용해서 CD 또는 DVD에 민감한 콘텐츠 저장을 제한하기 위해서는 아래 단계를 따르시기 바랍니다:

1. **콘텐츠 인식 정책(CAP)** 만들기
2. **정책 대상** 섹션의 **저장 장치** 탭에서 **모든 저장 장치에 정책 적용** 설정
3. **거부목록** 정책 섹션에서 위협에 필요한 정책을 선택

제 3업체 응용프로그램을 사용해서 CD 또는 DVD에 민감한 콘텐츠 저장을 제한하기 위해서는 아래 단계를 따르시기 바랍니다.

1. **콘텐츠 인식 정책(CAP)** 만들기
2. **정책 대상** 섹션의 **저장 장치** 탭에서 **모든 저장 장치에 정책 적용** 설정
3. **응용프로그램** 섹션의 소셜 미디어/기타 탭에서 다음을 선택:
    - **CDBurnerXP**
    - **ImgBurn CD/DVD**
    - **InfraRecorder CD - DVD**

4. **거부목록** 정책 섹션에서 위협에 필요한 정책을 선택

참고: 이 기능은 USB 플래시 드라이버 및 CD/DVD 플레이어 옵션으로 드래그 앤 드롭 또는 복사 및 붙여넣기 작업으로 CD/DVD 버닝에 적용됩니다.

6.3.2.3. 클립보드

클립보드는 복사 및 붙여넣기 또는 잘라내기 및 붙여넣기 동작을 통한 모든 콘텐츠 캡쳐입니다.

참고: 클립보드 기능은 **소스코드**, **미리 정의된 콘텐츠**, **사용자 키워드** 또는 **정규식**에 대한 정책 거부목록에 정의된 기밀 콘텐츠에만 적용됩니다.

클립보드 기능은 상세한 세부 목록으로 제공됩니다:

- **클립보드** - 정의된 정책 대상에 관계없이 컴퓨터에서 모든 콘텐츠를 모니터링하기 위해서 **클립보드** 설정을 사용합니다.

  참고: 이 설정은 **복사** 운영에만 적용됩니다.

  복사 운영을 수행할 때 Endpoint Protector 클라이언트는 클립보드 콘텐츠를 검사하고 만약 민감한 정보가 탐지되면 **콘텐츠는 삭제됩니다**. 예를 들어 붙여넣기 운영은 클립보드 콘텐츠가 삭제되어서 동작하지 않습니다.

- **소스 코드 탐지** - 정책에 정의된 **소스코드**를 탐지하기 위해서 이 설정을 사용합니다.

  참고: 이 설정은 **복사** 또는 **붙여넣기** 운영에 적용됩니다.

  Endpoint Protector 클라이언트는 소스코드에 대한 클립보드 콘텐츠를 검사하고 만약 소스코드가 콘텐츠 인식 정책에서 탐지되고 모니터링되면 (예: C++이 콘텐츠 인식 정책에서 선택되고 탐지된 클립보드 콘텐츠는 C++ 입니다.) 콘텐츠는 **복사** 또는 **붙여넣기** 운영에서 차단됩니다 (**모든 감시되는 응용프로그램에 붙여넣기 제한 적용** 설정 사용 여부에 따라 다릅니다.).

- **이미지 탐지** – 이 설정은 클립보드로 이미지 복사를 탐지를 할 수 있도록 합니다.

  아래 이미지 유형이 대상이 됩니다:

  1. 프린트 스크린 유형 이미지 – 콘텐츠는 자동으로 차단됩니다.
  2. CTRL+C 로 복제하고 클립보드로 붙여넣기 하는 이미지 파일 (클립보드에 파일 URL 을 붙여넣기 할 것입니다.)

  참고: 만약 여러 파일이 복제되고 콘텐츠에 적어도 하나의 이미지가 포함되면 파일 콘텐츠는 차단될 것입니다.

  소스 코드 탐지와 유사하게 이미지 탐지 설정은 콘텐츠 인식 보호(CAP) 정책에서 파일 형식이 차단되는지 여부를 적용합니다 (만약 사용자가 PNG 파일을 복사하면 PNG 파일 형식이 콘텐츠 인식 보호(CAP) 정책에 체크가 되어 있다면 파일은 차단될 것입니다.).

  Endpoint Protector 에이전트는 스캔 후에 사본보관을 하거나 그렇지 않고 삭제하면 이동되는 임시 위치에 이미지 콘텐츠를 저장할 것입니다.

- **모든 감시되는 응용프로그램에 붙여넣기 제한 적용** - 특정 응용프로그램 검사와 붙여넣기 제한 설정을 위해서 **모든 감시되는 응용프로그램에 붙여넣기 제한 적용** 설정을 사용합니다.

  참고: 이 설정은 정의된 정책 대상의 **붙여넣기** 운영을 제한합니다.

  복사 운영을 수행할 때 Endpoint Protector 클라이언트는 클립보드 콘텐츠를 검사하고 만약 기밀 정보가 탐지되면 콘텐츠를 **허용하고** 대신에 콘텐츠 인식 정책에서 감시되는 응용프로그램이면 **붙여넣기 운영을 차단**합니다.

  중요: 붙여넣기 운영은 사용자가 창을 다른 응용프로그램으로 변경할 때 허용됩니다.

  예: 콘텐츠 인식 정책에서 Firefox가 감시되고 Chrome은 감시되지 않고 감시되는 응용프로그램의 붙여넣기 제한 적용이 사용됩니다. 사용자는 기밀 정보가 포함된 메모장에서 복사 운영을 수행하면 아래와 같은 결과가 나타납니다.

- Firefox에 붙여넣기 운영은 **차단됩니다.**
- Chrome에 붙여넣기 운영은 **허용됩니다.**

- **아래 응용프로그램에 확장된 붙여넣기 제한 확장** - 확장된 응용프로그램을 검사하고 붙여넣기 제한 설정을 위해서는 **아래 응용프로그램에 확장된 붙여넣기 제한 확장** 설정을 사용합니다.

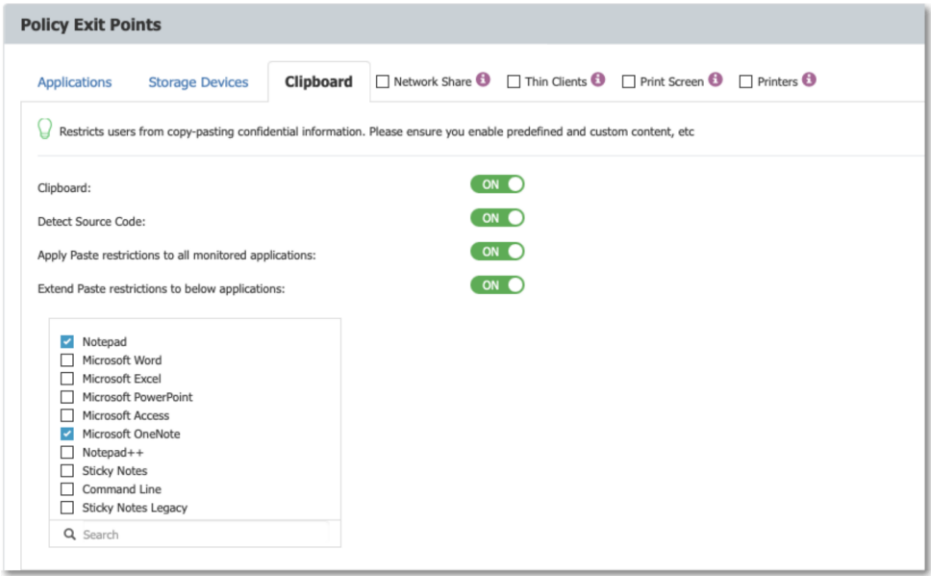
참고: 이 설정은 정의된 응용프로그램의 **붙여넣기** 운영을 제한합니다.

콘텐츠 인식 정책의 목록에 없는 응용프로그램을 확장하고 **붙여넣기** 운영을 **차단**하기 위해서 이 설정을 사용하시기 바랍니다.

예: Microsoft Word는 콘텐츠 인식 정책의 목록에 없지만 Microsoft Word 앱에서 **붙여넣기** 운영을 모니터링하기 위해서 목록에서 응용프로그램을 선택할 수 있습니다.

요구에 따라서 Endpoint Protector는 다른 응용프로그램을 추가할 수 있습니다.

중요: Wayland 프로토콜을 사용하는 특정 Linux 환경에서 Wayland로 초점이 맞춰진 창을 감지하지 못해서 붙여넣기 제어가 제한됩니다. 보안을 위해 복사 작업 중에 콘텐츠 차단이 이루어집니다.



중요: 최신 Linux Ubuntu 버전에는 기본적으로 'snap' 기반 응용프로그램이 설치되어 있어 EPP 클라이언트 기능에 영향을 미칩니다. 이로 인해 CAP 스캔에서 파일 관련 이벤트가 누락될 수 있습니다. '스냅' 기반 응용프로그램에 대한 의존도는 파일 관련 웹 브라우저 활동에도 영향을 미쳐 이러한 제한을 더욱 악화시킵니다. 최적의 기능을 위한 대체 구성으로 'snap' 기반이 아닌 응용프로그램 (가능한 경우)을 고려하시기 바랍니다.

1. **네트워크 공유**

Mac 네트워크 공유의 경우 Endpoint Protector의 보고만 정책에 대해서 모든 이벤트를 보고합니다. 차단 및 보고 정책에 대해서 로컬 디스크, 제어된 저장 장치 종류, 제어되는 응용프로그램으로 향하는 로컬 공유의 전송이 차단됩니다.

2. **씬 클라이언트**는 씬 클라이언트 드라이브의 파일 전송이 적용됩니다.

3. **화면 인쇄**는 스크린 캡쳐 옵션이 적용됩니다.

4. **프린터**는 로컬 프린터와 네트워크 공유 프린터 모두에 적용됩니다.

참고: 이 옵션을 사용할 때 **설정** (전체, 그룹, 컴퓨터 등)에서 **개선된 프린터 및 MTP 검색**을 사용할 것을 권장합니다.

6.3.3. 콘텐츠 감지 요약

콘텐츠 감지 요약은 콘텐츠 인식 보호에서 체크된 모든 미리 정의된 콘텐츠, 사용자 키워드, 정규식, HIPAA가 표시됩니다.

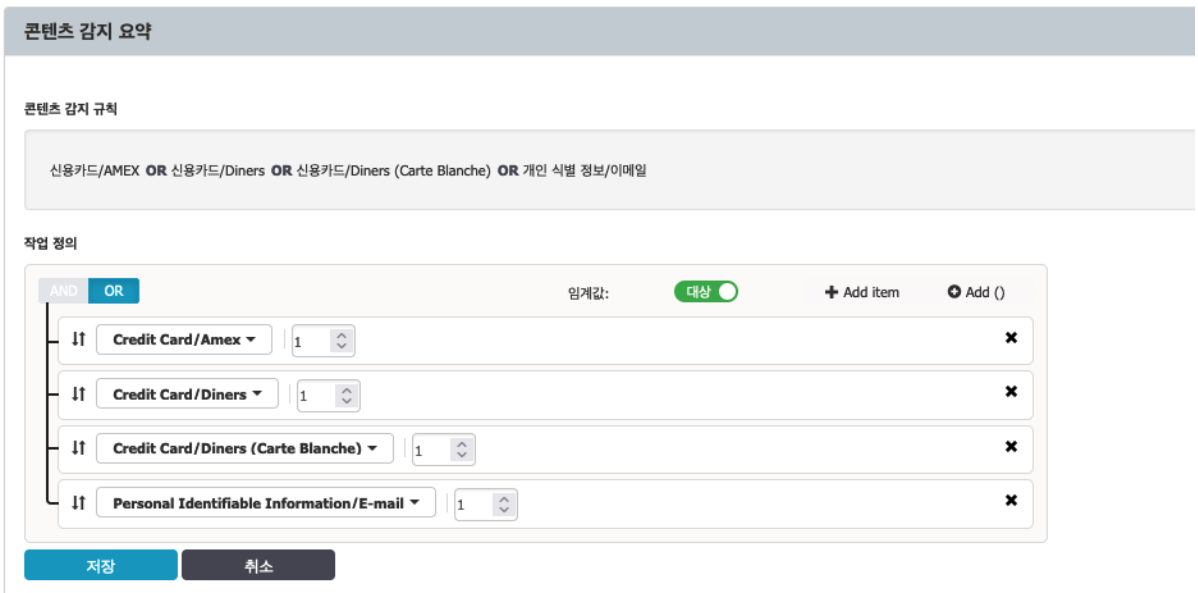
콘텐츠 감지 규칙은 **AND, OR** 운영을 사용하여 여러 기준 조합을 정의합니다.

참고: 이 기능은 프리미엄 라이선스에서만 사용할 수 있고 특정 파일 형식에 대한 **콘텐츠 감지 제한** 또한 사용할 수 있습니다.

콘텐츠 감지 규칙을 편집하려면 **수정**을 클릭하고 **작업 정의** 섹션에서 다음 정보를 제공합니다:

- **작업** 선택 – **OR** (기본값), **AND**
- **임계값**을 사용하고 1에서 1000까지 각 항목 옆에 숫자를 입력합니다; **정책 정보** 섹션에서 **전체 임계값** 설정을 사용하지 않습니다.
- **Add item** 후 드롭다운에서 PII 선택; 작업을 저장하기 전에 드롭다운 목록을 선택해서 PII를 변경할 수 있습니다. 목록에 항목을 제거하려면 각 PII 옆의 **x**를 클릭합니다.
- **그룹 추가**

작업 순서 변경을 위해서는 항목의 위아래 화살표 또는 드래그 앤 드롭을 사용합니다.



콘텐츠 탐지 제한을 위해서 콘텐츠 탐지 규칙에 적용하려는 파일 유형을 드롭다운 목록에서 선택합니다.

파일 유형을 설정하지 않으면 콘텐츠 탐지 규칙에 정의된 콘텐츠는 이 정책으로 차단되지 않는 모든 파일 유형을 검색할 것입니다.

문맥 탐지 규칙은 **프리미엄** 기능으로 **콘텐츠 탐지 규칙**에서 전에 정의된 하나 또는 여러 위협 유형에 대한 최소한 또는 최대한의 콘텐츠 일치 수를 특정 하도록 허용해서 오탐 탐지를 줄여줍니

다.

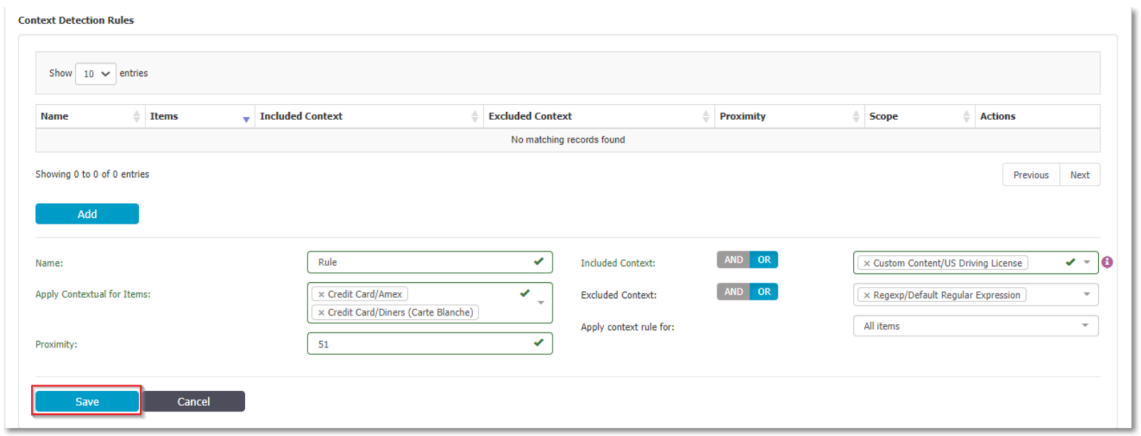
중요: 콘텐츠 탐지 규칙은 **OR** 운영자를 사용한 콘텐츠 탐지 규칙을 정의할 때만 만들 수 있습니다.

새로운 **콘텐츠 탐지 규칙**을 만들려면 **추가**를 클릭하고 아래 내용을 채운 후 저장합니다:

- **이름** – 문맥 탐지 규칙 이름 추가
- **아이템에 문맥 적용** – 콘텐츠 탐지 규칙에서 선택된 미리 정의된 콘텐츠를 드롭다운 목록에서 선택
- **주변 문자** – 50에서 3000 사이의 숫자 추가
- **문맥 포함** – AND/OR 운영자를 선택하고 규칙에 추가하려는 키워드, 정규식 또는 HIPPA를 드롭다운 목록에서 선택합니다.
- **문맥 제외** – AND/OR 운영자를 선택하고 규칙에 제외하려는 키워드, 정규식 또는 HIPPA를 드롭다운 목록에서 선택합니다.

  참고: 콘텐츠 탐지 규칙에 사용된 키워드는 문맥 포함 및 문맥 제외 드롭다운 목록에 표시되지 않습니다.
- **아이템을 문맥 규칙에 추가** – **모든 아이템** 또는 **최소 1 아이템으**로 규칙 적용을 선택

  참고: 최대 15개의 콘텐츠 탐지 규칙을 만들 수 있습니다.



중요: 정책 별 문맥 규칙과 글로벌 문맥 규칙의 충돌 해결을 위해 하나 이상의 정책에 개별 문맥 규칙이 설정되어 있는 경우 EPP클라이언트는 더 이상 글로벌 문맥 규칙의 영향을 받지 않습니다. 이는 개별 정책 구성의 우선순위를 강조하기 위해 글로벌 문맥 규칙이 더 이상 사용되지 않음을 의미합니다.

6.3.4. 정책 거부목록 및 허용목록

정책 거부목록 및 허용목록은 탐색된 콘텐츠를 특정합니다. 파일 형식, 미리 정의된 콘텐츠, 사용자 키워드, 파일 허용목록, 정규식, 도메인 허용목록, 심층 패킷 검사(DPI) 등이 포함됩니다.

6.3.4.1. 정책 거부목록

다음의 거부목록을 사용할 수 있습니다:

- **파일 형식** – 많은 파일 (예: 프로그래밍 파일)이 실제로는 .TXT 파일이기 때문에 기대하지 않은 결과를 피하기 위해서 파일 형식을 선택할 때 더 많은 예방책을 권장합니다.

  참고: 파일 유형 탐지는 일부 비밀번호로 보호되는 용량이 큰 Microsoft Office 파일에서는 항상 정확하게 동작하지 않습니다.

- **소스 코드** – N-gram 기반 탐지 방법은 이러한 파일 형식의 정확성을 증가시키는데 사용합니다. 그러나 다양한 소스코드가 근접하게 함께 연결이 되어 있기 때문에 (예: C, C++ 등) 이러한 상황을 또한 확인합니다. 더 쉽게 만들기 위해서 Endpoint Protector는 이러한 연관성을 자동으로 마크합니다.

심층 패킷 검사(DPI)가 사용될 때 Git 모니터링의 확장된 방법으로 사용할 수 있습니다. 만약 Git가 제한된 앱들로 선택되면 Git 응용프로그램의 사용에 관계없이 Git와 관련된 작업 (fetch, clone, push, pull)은 차단됩니다. 이는 완전하게 Git를 차단하는 결과입니다. 그러나 심층 패킷 검사(DPI) 허용목록은 특정 도메인 (예: internalgit.mydomain.com)에 연결된 특정 Git를 허용할 수 있습니다.

참고: 모든 Git 트래픽은 암호화됩니다. 그러므로 특정 도메인 허용은 콘텐츠 또는 다른 정책의

정의된 제한과 관계없이 결과적으로 모든 파일 전송을 허용합니다.

제한된 앱에서 Git가 선택되면 Endpoint Protector 알림과 로그는 Git 관련 작업 (fetch, clone, push, pull)에 대해서 만들어지지 않습니다.

- **미리 정의된 콘텐츠** – 미리 정의된 콘텐츠 항목의 대부분이 국가를 구분합니다 (예: 호주, 캐나다, 독일, 대한민국, 영국, 미국 등). 대량 로그 또는 오탐을 피하기 위해서 지역 또는 민감한 데이터 적용에 여권번호만 사용할 수 있습니다.

이탈리아 SSN 및 ID 사용

Endpoint Protector 5.7.0.0 버전을 시작으로 이탈리아 SSN이 PII 목록에 추가되었습니다. 이탈리아 ID와 비슷하여 PII 목록에서 선택하면 SSN과 같은 엔터티로 탐지될 것입니다.

이탈리아 SSN과 ID를 사용할 때 최신 Endpoint Protector 에이전트 버전으로 업그레이드하는 것을 권장합니다.

서버 업그레이드 후에 이전 에이전트 버전과 호환성을 유지하기 위해서 이탈리아 ID는 ID 섹션에 남아 있고 서버 업그레이드는 이탈리아 ID를 포함하여 이전 설정으로 남아 있을 것입니다.

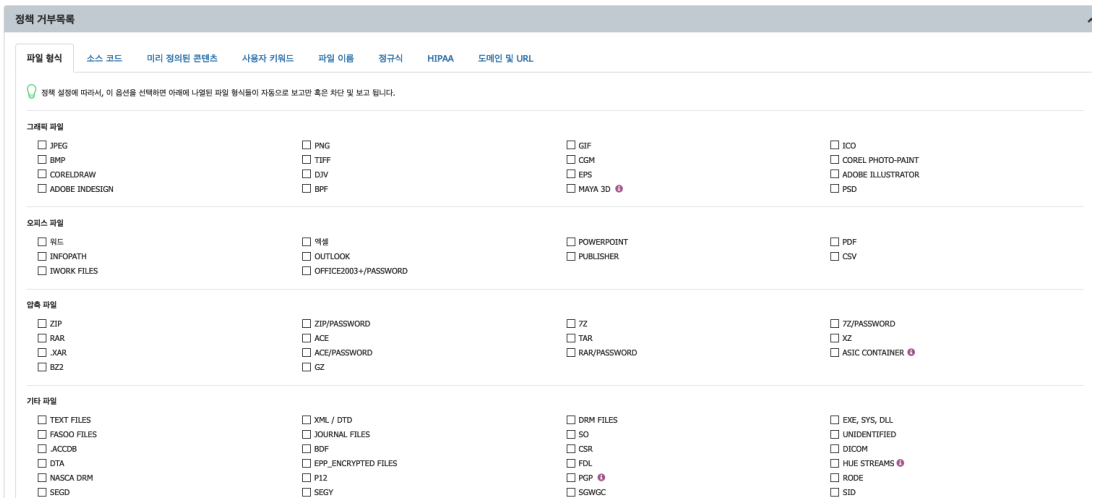
- 에이전트 버전 XXX 이후로 배포했을 때 이탈리아 SSN 사용
- 에이전트 버전 XXX 이전으로 배포했을 때 이탈리아 ID 사용
- 새로운 에이전트와 이전 에이전트의 혼합 환경에서 이탈리아 SSN과 ID 모두 사용

이탈리아 SSN과 ID는 모두 같은 엔터티로 탐지되기 때문에 여러 보고 결과를 피하기 위해서 이탈리아 ID를 선택하지 않습니다.

새로운 Endpoint Protector 에이전트 버전은 이탈리아 ID와 SSN을 모두 보고합니다.

- **사용자 키워드**
- **파일 이름**

- **파일 위치**
- **정규식**
- **HIPAA**
- **도메인 및 URL**



6.3.4.2. HIPAA 정책

HIPAA 탭 옵션이 선택되어 있다면 모든 콘텐츠 인식 보호 정책은 자동으로 HIPAA 정책이 됩니다. 사용할 수 있는 옵션은 FDA 인정한 목록과 ICD 코드입니다. HIPAA 정책을 적용하려면 미리 정의된 콘텐츠와 사용자 키워드를 또한 사용해야 합니다. 이 정책들은 자동으로 의료보험번호, 사회보장번호, 주소 등과 같은 PII가 포함된 파일 전송을 보고하거나 차단합니다.

참고: HIPAA 정책의 효과와 정확성을 높이려면 문맥 탐지 규칙을 미리 정의된 규칙 및 키워드 필

터와 함께 사용하면 좋습니다. 또한 정확도를 높이려면 미리 정의 콘텐츠에서 '전체 단어만' 활성화해야 해야 합니다. ICD 11 사전은 보험 코드가 아닌 특정 용어에만 초점을 맞추고 있습니다.

참고: 짧은 질병 설명에 대한 오탐을 최소화하려면 적절한 임계값과 인수 조합 설정이 좋습니다.

6.3.4.3. 정책 허용목록

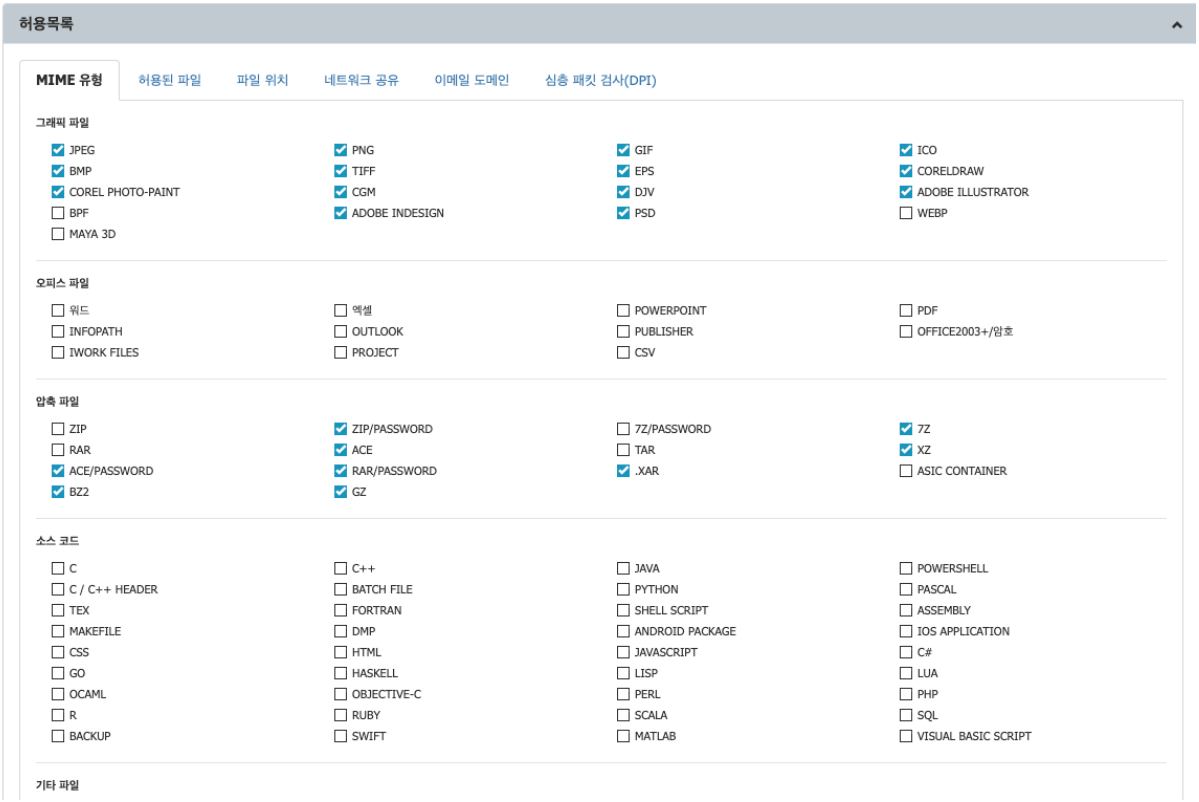
다음 허용목록을 사용할 수 있습니다:

- **MIME 유형**
- **허용된 파일들**
- **파일 위치**
- **네트워크 공유**
- **이메일 도메인**
- **URL 주소**
- **심층 패킷 검사(DPI)**

참고: 거부목록 및 허용목록의 더 자세한 내용은 거부목록 및 허용목록 챕터를 참조하시기 바랍니다.

중요: 콘텐츠 인식 보호 정책은 심지어 회사 네트워크 연결이 끊어진 후에도 보호되는 컴퓨터의 민감한 데이터 전송의 보고 및(또는) 차단을 지속적으로 수행합니다.

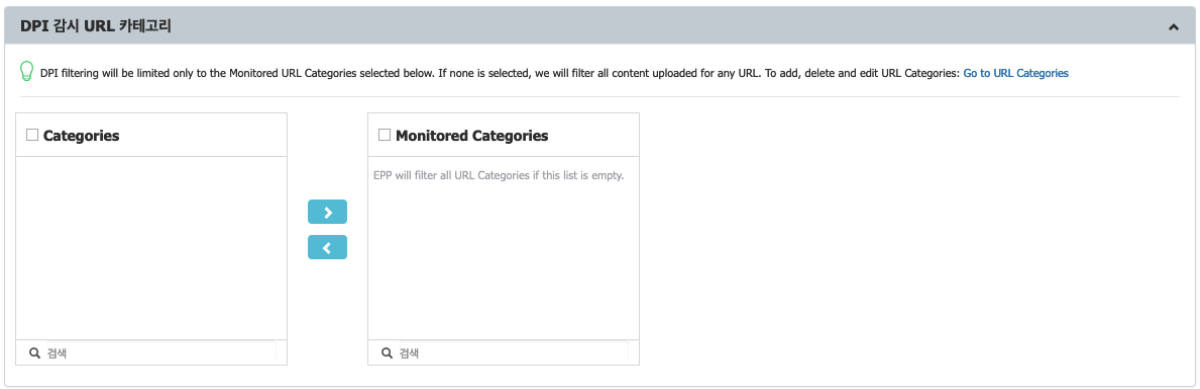
이 때 로그는 Endpoint Protector 클라이언트에 저장되고 연결이 재개되면 로그는 서버로 보냅니다.



6.3.5. DPI 감시 URL 카테고리

DPI 감시 URL 카테고리 필터를 정의할 수 있습니다. 아무것도 정의되지 않으면 모든 URL에 업로드된 모든 콘텐츠를 필터링 합니다.

거부목록 및 허용목록 섹션에서 URL 카테고리 추가, 삭제, 편집을 할 수 있습니다.



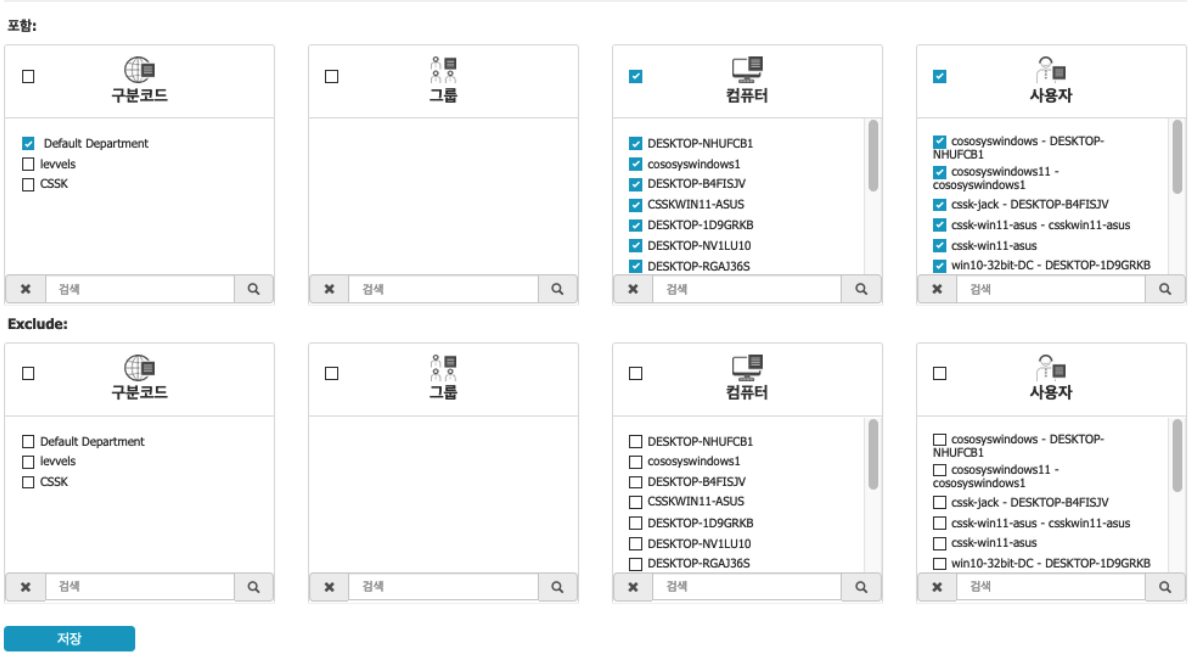
6.3.6. 정책 엔터티

정책을 만드는 마지막 단계는 적용 가능한 엔터티를 선택하는 것입니다:

- **구분**
- **그룹**
- **컴퓨터**
- **사용자**

참고: 콘텐츠 인식 정책이 이미 컴퓨터, 사용자, 그룹 또는 구분에서 시행되고 있다면 이것들 클릭했을 때 네트워크에 응답하는 엔터티는 하이라이트 될 것입니다.

제외된 섹션을 선택해서 정책에서 제외하는 엔터티 목록을 정의할 수 있습니다.



6.3.7. 차단 및 교정 정책

차단 및 교정 정책은 콘텐츠 인식 정책의 카테고리로 프리미엄 라이선스에서만 사용할 수 있습니다.

이 정책의 카테고리는 최종 사용자에게 근거를 사용해서 콘텐츠 인식 위협을 자체적으로 해결할 수 있는 가능성을 제공합니다.

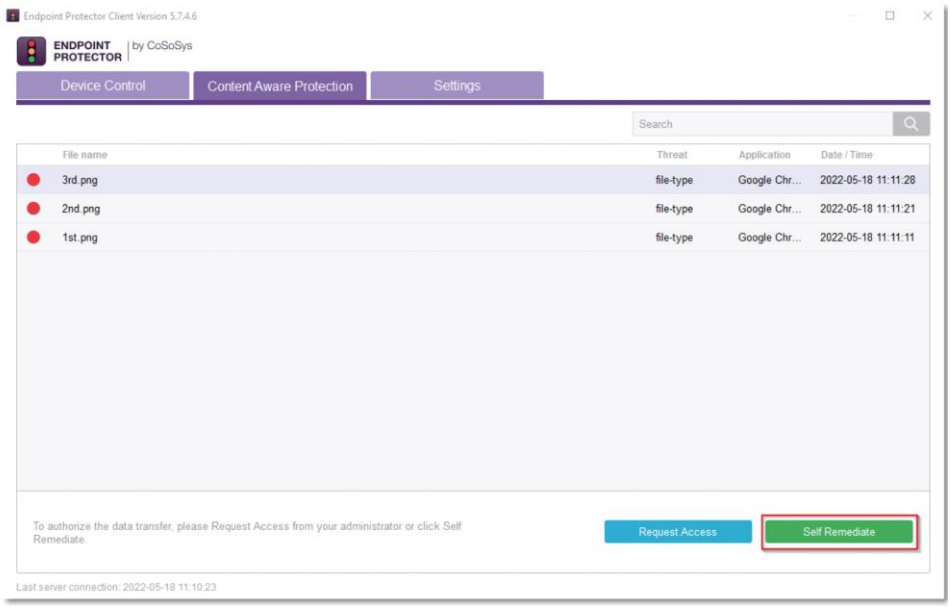
콘텐츠 인식 보호 섹션에서 차단 및 수정 콘텐츠 인식 정책을 쉽게 만들 수 있습니다.

탐지할 때 콘텐츠 인식 위협은 표시됩니다:

- Endpoint Protector 알림 창의 콘텐츠 인식 보호(CAP) 탭에서
- 설정 섹션에서 옵션이 사용되었다면 팝업 알림으로

위협 교정을 위해서 최종 사용자는 다음 단계를 확인합니다:

1. **Endpoint Protector 알림 창**을 열고 **콘텐츠 인식 보호(CAP)** 탭으로 이동합니다;
2. 교정 파일을 선택하고 **자가 교정**을 클릭합니다;



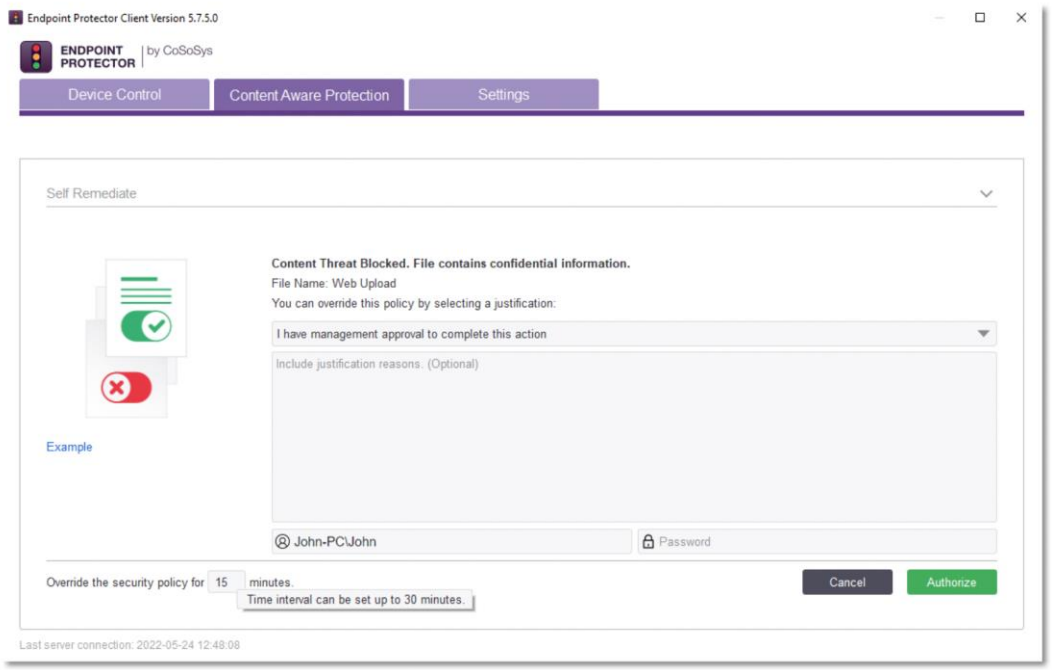
3. 자가 교정 섹션에서
   a. 드롭다운 목록에서 **근거**를 선택합니다.
   b. (필요하다면) 근거에 대한 **이유**를 추가합니다.
   c. 로고에 있는 **사용자 정의 URL**을 검색합니다.
   d. **계정 요구** 설정이 사용되었으면 계정을 추가합니다 (현재 사용자 이름을 새로고침 하

기 위해서 사용자 이름 아이콘을 클릭합니다.).

e. 기기 수정에 필요한 **시간 간격**을 추가합니다 (최대 시간 간격을 보려면 기본적으로 설정된 시간 간격을 호버링 할 수 있습니다.).

f. **확인**을 클릭합니다.

참고: 시스템 매개 변수의 사용자 수정 섹션에서 자가 교정 기능에 대한 자세한 설정을 관리할 수 있습니다.



콘텐츠 인식 보호의 사용자 수정은 웹 도메인을 통한 파일 전송을 완화할 수 있습니다.

특정 웹 도메인에 사용자 수정을 적용하려면 전체 / 컴퓨터 / 사용자 심층 패킷 검사(DPI)를 사용합니다. 이 기능은 브라우저와 데스크톱 이메일 응용프로그램에 기본으로 사용 가능합니다.

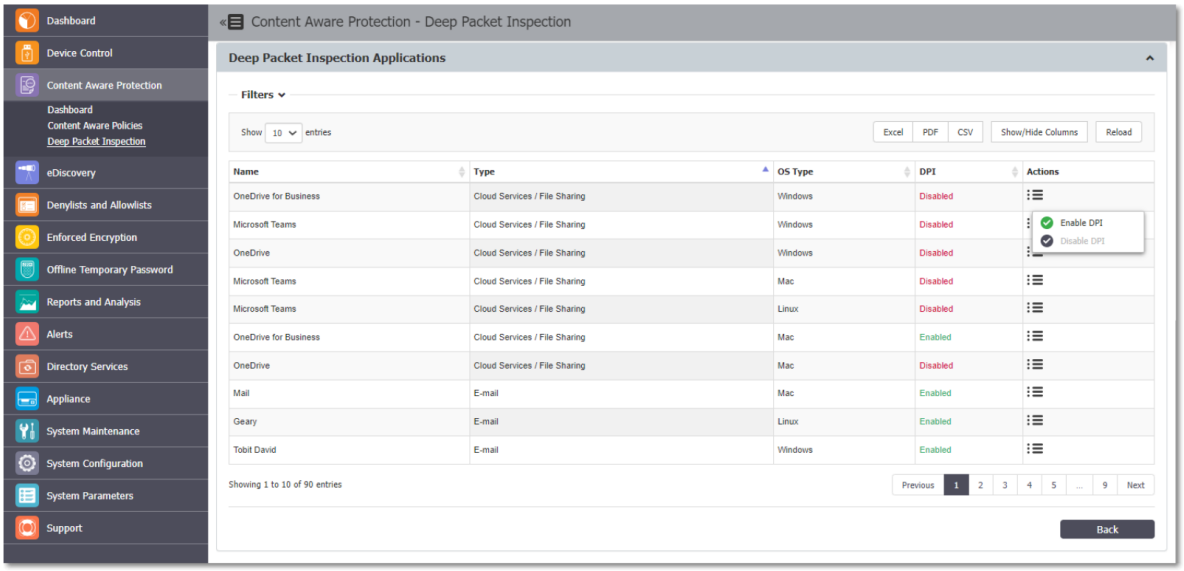
다른 응용프로그램에 해해서는 콘텐츠 인식 보호, 심층 패킷 검사, 작업 컬럼에서 심층 패킷 검사(DPI)를 사용합니다.

- **심층 패킷 검사(DPI) 사용** – 특정 웹 도메인에 전송되는 파일을 사용자 수정을 적용할

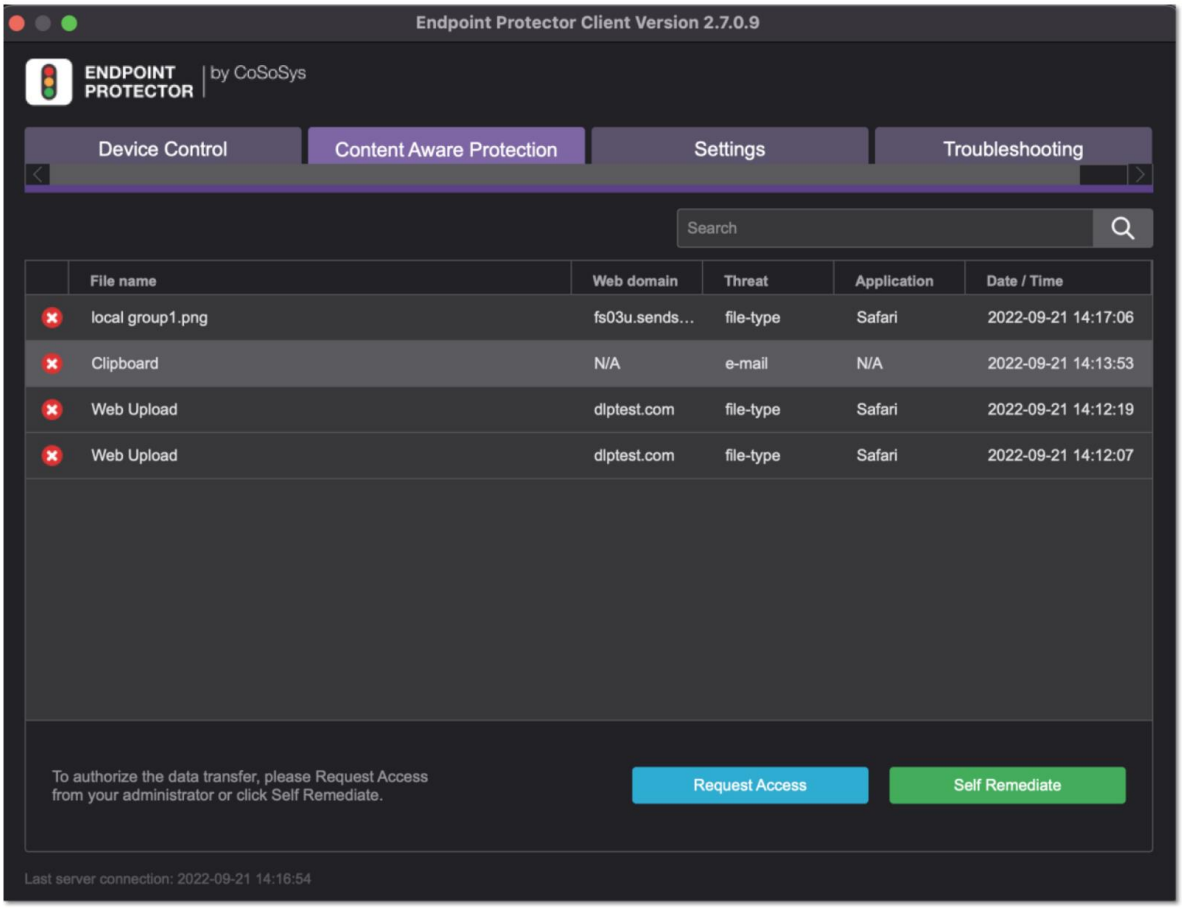
수 있습니다.

- **심층 패킷 검사(DPI) 사용 안함** – 특정 응용프로그램에 전송되는 파일의 사용자 수정만 적용할 수 있습니다.

예: Chrome에 파일을 업로드하고 사용자 수정을 적용하면 모든 Chrome URL에 파일을 업로드할 수 있습니다.



Endpoint Protector 클라이언트, 콘텐츠 인식 보호 탭에서 웹 도메인 컬럼에서 사용자 수정에 사용된 웹 도메인을 볼 수 있습니다.



6.3.8. 여러 콘텐츠 인식 정책 적용

콘텐츠 인식 보호는 매우 유용한 도구입니다. 보고만 또는 차단 및 보고와 관련된 원하는 액션을 섬세하게 설정하고 수행할 수 있습니다.

콘텐츠 인식 정책은 선택된 정보를 보고만 또는 차단 및 보고에 대한 규칙의 설정입니다. 체크되지 않은 모든 다른 옵션은 Endpoint Protector가 무시하는 것으로 간주됩니다.

같은 PC에 두 가지 정책이 적용될 때 Mozilla Firefox로 업로드 될 때 PNG 파일이 차단되고 반면에 Internet Explorer로 PNG 파일 보고만 두 번째 정책으로 설정되면 PNG 파일 유형은 차단됩니다.

같은 방법으로 첫 번째 정책을 통해서 Skype로 사용자 키워드 파일을 보고만으로 하고 두 번째 정책을 통해서 Yahoo로 같은 파일을 차단하면 이 파일은 보고만 됩니다.

다음은 개별적으로 선택된 목록 (예: 특정 파일 유형, 개인정보 콘텐츠 필터 또는 사용자 키워드 등)의 컴퓨터/사용자/그룹/구분에 설정된 하나 이상의 콘텐츠 인식 정책의 규칙입니다.

정책A (우선순위 1)	정책B (우선순위 2)	정책C (우선순위 3)	Endpoint Protector 동작
무시	무시	무시	차단/보고 안 됨
무시	무시	보고	보고됨
무시	보고	보고	보고됨
보고	보고	보고	보고됨
무시	무시	**차단**	차단됨
무시	**차단**	**차단**	차단됨
차단	**차단**	**차단**	차단됨
무시	보고	**차단**	보고됨
무시	**차단**	보고	차단됨
보고	무시	**차단**	보고됨
차단	무시	보고	차단됨
보고	**차단**	무시	보고됨
차단	보고	무시	차단됨

중요: 정책을 만들 때 체크되지 않은 상태로 남은 정보는 Endpoint Protector에서 무시되거나 허용되지 않음으로 간주됩니다.

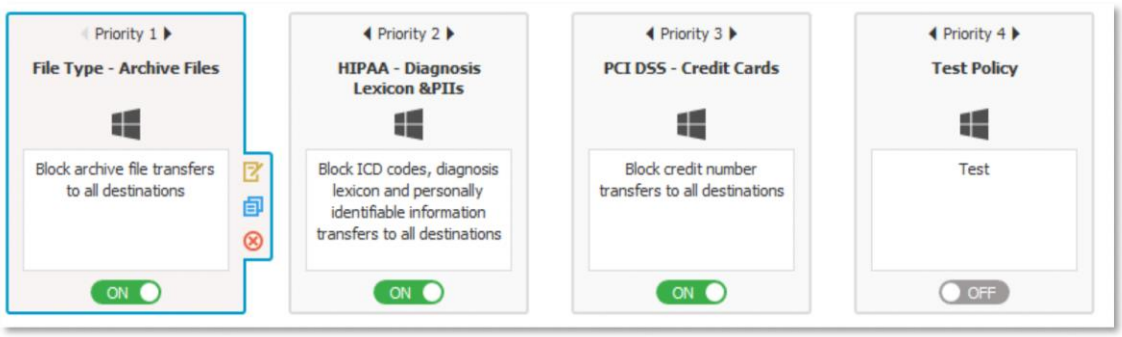
심층 패킷 검사(DPI) 기능은 도메인 허용기반의 이메일 검사로 확장되었습니다.

권장된 HIPAA는 콘텐츠 인식 정책이 고려되어야 합니다. HIPAA 탭 옵션 이외에도 아래 구성이 또한 필요합니다:

- 인식되는 모든 파일 형식이 포함되어야 합니다.
- 모든 PII (Personal Identifiable Information)은 미국 고유의 것이어야 합니다.

  (주소, 전화번호/팩스, 사회보장번호)
- 인터넷 프로토콜 주소가 모두 포함되어야 합니다.
- URL과 도메인 허용목록 옵션이 또한 체크되어야 합니다.

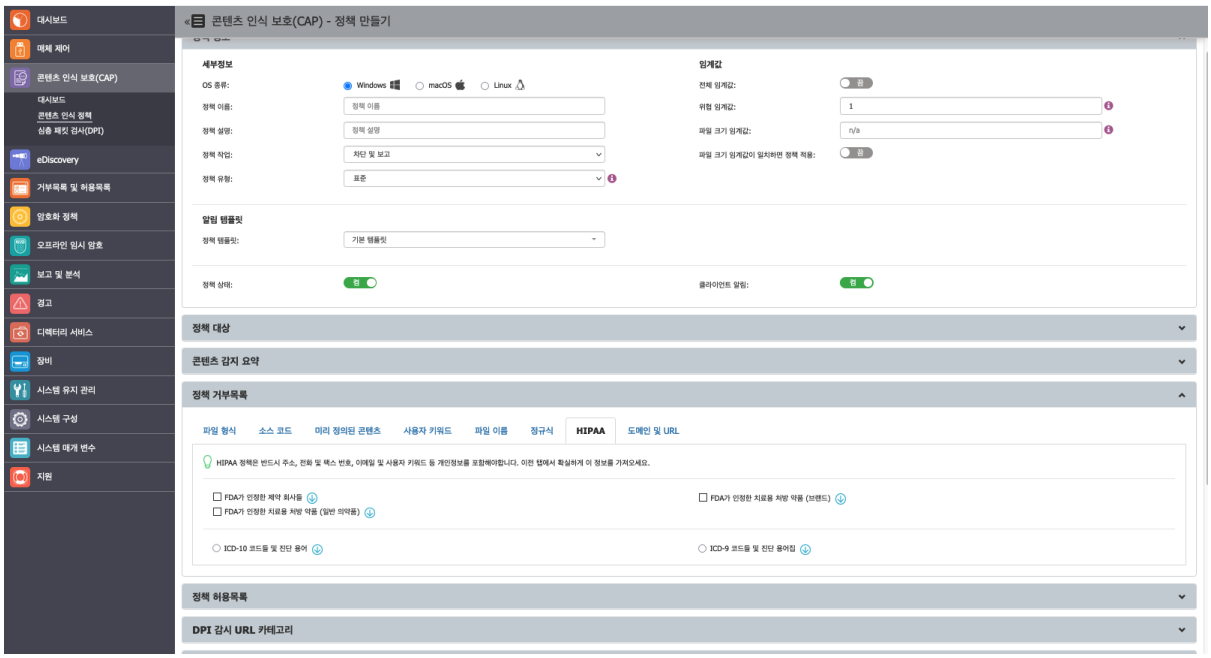
HIPAA 옵션은 네트워크 내부의 데이터를 더 잘 제어하기 위해 자체 또는 일반 정책과 함께 만들어 사용될 수 있습니다. 이러한 정책은 Windows, Mac OS X, Linux 컴퓨터에서 사용 가능합니다.



6.3.8.1. 사례 #1

회사A는 환자 의료 기록을 전산으로 취급하고 이 자료는 환자 이름, 주소, 생일, 전화번호, 사회보장번호 및 이메일 주소 등의 전반적인 정보를 포함한다고 가정합니다. 회사는 많이 사용하는 Windows 데스크톱 응용프로그램을 통한 파일 전송을 차단하기를 원합니다.

민감한 데이터는 환자 프로파일 포맷으로 되어 잇는 것을 알기 때문에 관리자는 아래와 같은 HIPAA 정책을 만들 수 있습니다.



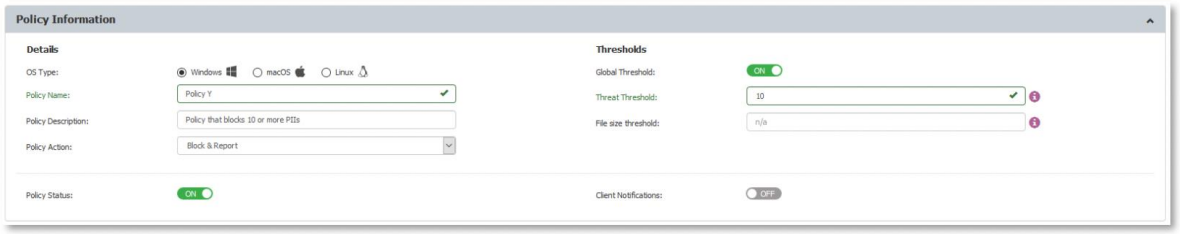
이 정책은 전체 임계값 4로 차단 및 보고 정책으로 설정되어 있습니다. 저장장치 (시스템 매개변수 > 매체 제어에서 탐지 목록 확인), 클립보드, 네트워크 공유 이외에 Endpoint Protector로 인식되는 응용프로그램의 모든 데이터베이스를 스캔합니다. 이 정책은 4개 이상의 서로 다른 정보 즉

주소 1개, 전화번호 2개, 이메일 2개가 포함된 콘텐츠를 차단합니다 (임계값 전체).

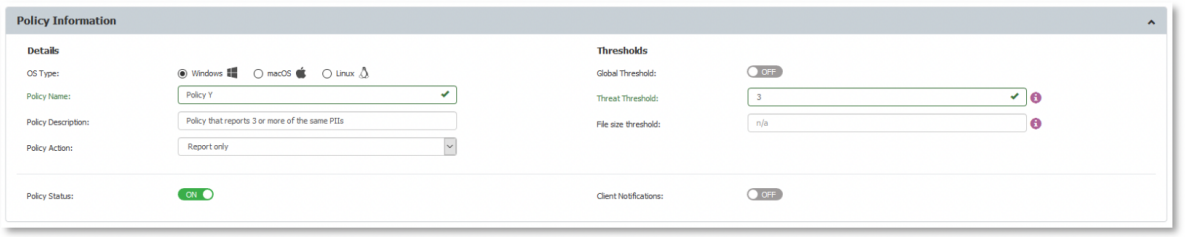
6.3.8.2. 사례 #2

회사B는 환자의 민감한 정보를 포함한 거대한 데이터베이스를 가지고 있습니다. 이 정보는 개별의 오피스 파일로 10개 이상의 환자 개인정보가 포함된 파일로 저장됩니다. 회사 직원은 정규적으로 파일 당 같은 개인정보 3개를 포함한 파일을 다룹니다. 회사B는 10개 이상의 개인정보가 포함된 데이터베이스의 파일 유출을 차단하고 3개의 개인정보 파일은 보고만하기를 원합니다.

관리자는 아래와 같이 전체 임계값 10을 사용하여 10개의 개인정보를 포함한 파일 전송차단을 설정할 수 있습니다.



또 다른 HIPAA 정책은 각각 임계값 3을 사용해서 같은 유형의 개인정보 3개를 포함한 파일의 보고를 할 수 있습니다.



차단 및 보고 정책은 보고만 정책이 두 번째로 오면 우선 순위를 가집니다.

6.4. 심층 패킷 검사(DPI)

심층 패킷 검사 기능은 관리자가 네트워크에 따라 미세하게 조정을 할 수 있어서 세분되어 적용할 수 있도록 제공됩니다.

참고: 심층 패킷 검사(DPI) 활성화는 검사된 파일의 업로드 속도에 영향을 줄 수 있습니다. 패킷 필터 대신 네트워크 확장을 사용하시기 바랍니다 (즉, VPN 트래픽 가로채기를 켜세요).

중요: 최신 Linux Ubuntu 버전에는 기본적으로 'snap' 기반 응용프로그램이 설치되어 있어 EPP 클라이언트 기능에 영향을 미칩니다. 이로 인해 DPI 파일 솔루션에서 파일 관련 이벤트가 누락될 수 있습니다. 'snap' 기반 응용프로그램에 대한 의존도는 파일 관련 웹 브라우저 활동에도 영향을 미쳐 이러한 제한을 더욱 악화시킵니다. 최적 기능을 위한 대체 구성으로 'snap' 기반이 아닌 응용프로그램 (가능한 경우)을 고려하시기 바랍니다.

6.4.1. 심층 패킷 검사(DPI) 인증서

심층 패킷 검사(DPI) 기능은 Endpoint Protector Root Certificate Authority에서 생성된 인증서를 사용합니다. 이는 DPI로 네트워크 트래픽을 가로채고 Endpoint Protector 클라이언트와 서버의 통신을 하기 위해서 입니다.

Endpoint Protector는 다양한 대안 스케줄로 인증서를 자동으로 새로 고치는 옵션을 제공합니다. 새로운 인증서가 생성된 후에 이 인증서는 클라이언트에 보내지고 기존 인증서를 대체합니다.

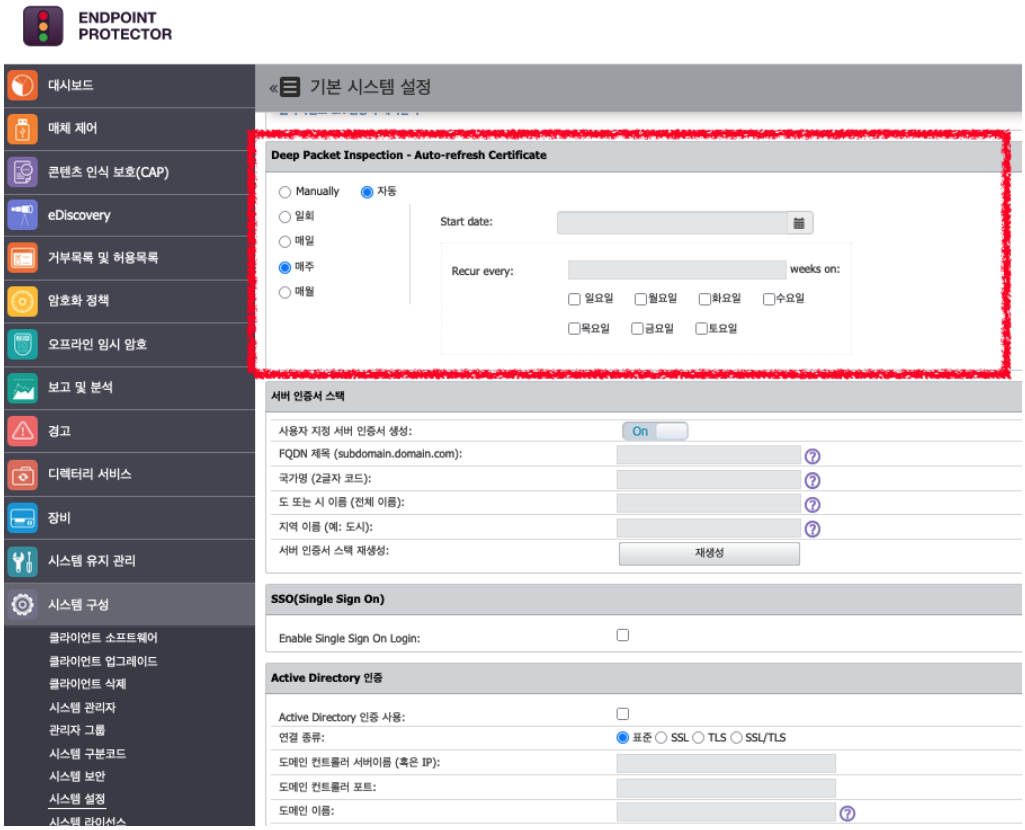
심층 패킷 검사(DPI) – 인증서 새로 고침 기능을 구성하려면 다음 단계를 참고하시기 바랍니다:

1. **시스템 구성, 시스템 설정, 심층 패킷 검사(DPI) – 인증서 새로 고침**으로 이동해서 **자동** 옵션을 선택합니다.

2. 가능한 스케줄 옵션을 하나 선택하고 변경 내용을 **저장**합니다.

3. 새로운 인증서는 만들어진 후에 엔드포인트에 자동으로 배포될 것입니다.

4. 엔드포인트의 재시작은 새로운 인증서를 강제로 사용하도록 요구합니다.



6.4.2. macOS에서 심층 패킷 검사(DPI) 인증서

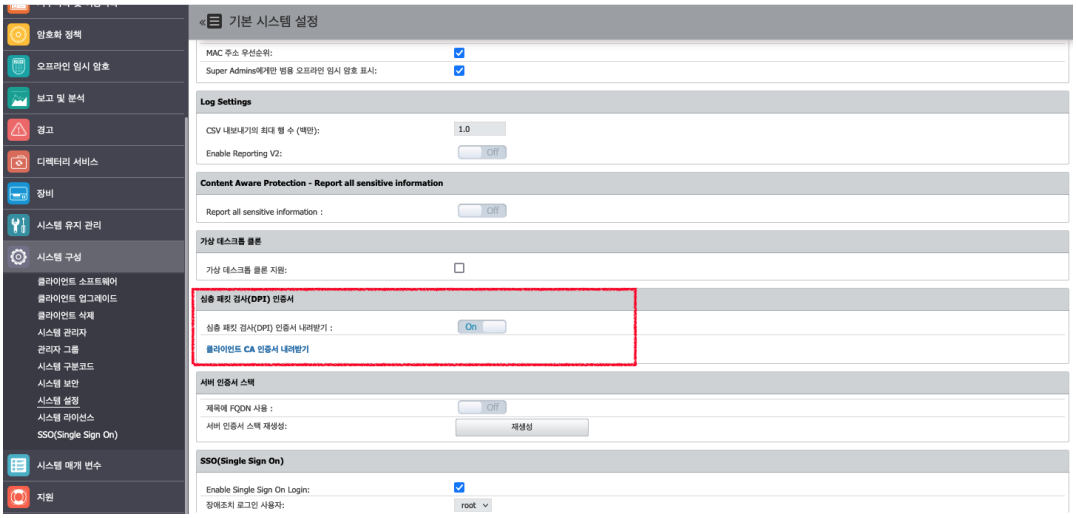
DPI (Deep Packet Inspection)에 영향을 주는 macOS 11.0 에서 최신 변경으로 DPI 기능이 macOS 11.0+ 에서 동작하기 위해서 새로운 인증서가 필요합니다.

참고: DPI 인증서가 Endpoint Protector 클라이언트에 추가되면 DPI 검사는 macOS 11.0+ 에서만 동작합니다.

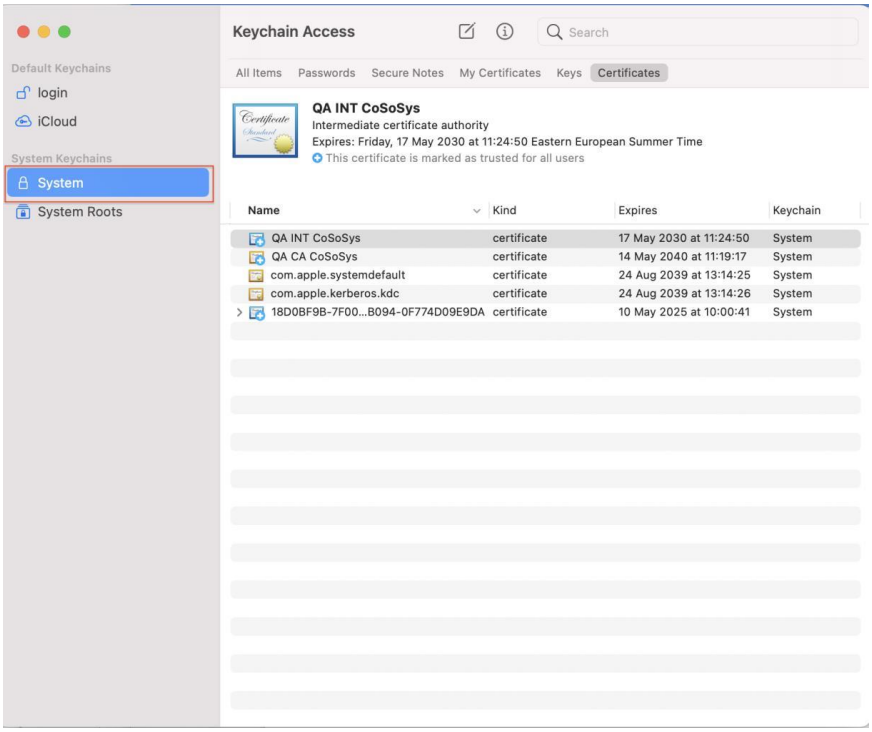
이 인증서는 '시스템 구성 > 시스템 설정 > DPI 인증서' 에서 다운로드 할 수 있습니다. 배포 솔루션을 통해서 수동 또는 자동으로 추가할 수 있습니다.

수동으로 추가하려면 아래 단계를 참조하시기 바랍니다:

1. **시스템 구성, 시스템 설정, DPI 인증서**로 이동해서 **CA 인증서**를 다운로드합니다.

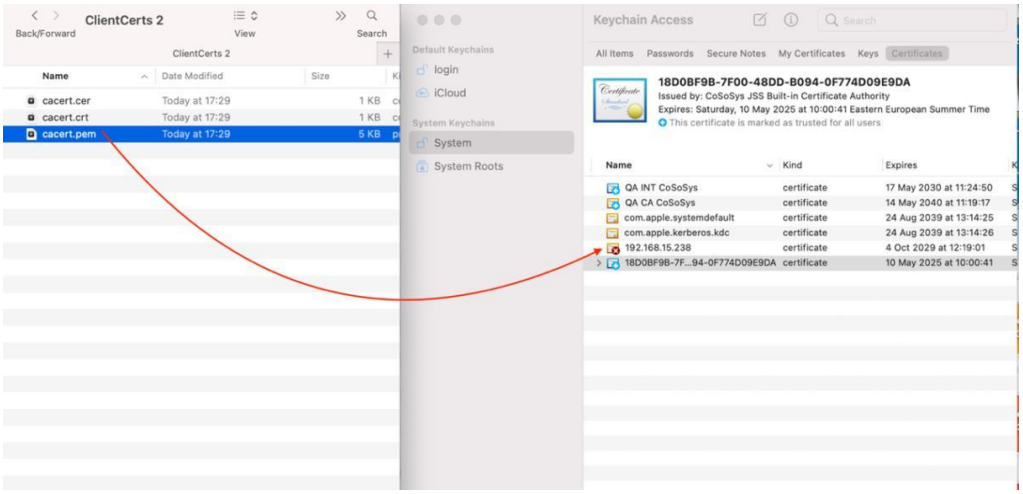


2. macOS에서 **키체인 접근** 응용프로그램을 열고 **시스템**을 선택합니다.

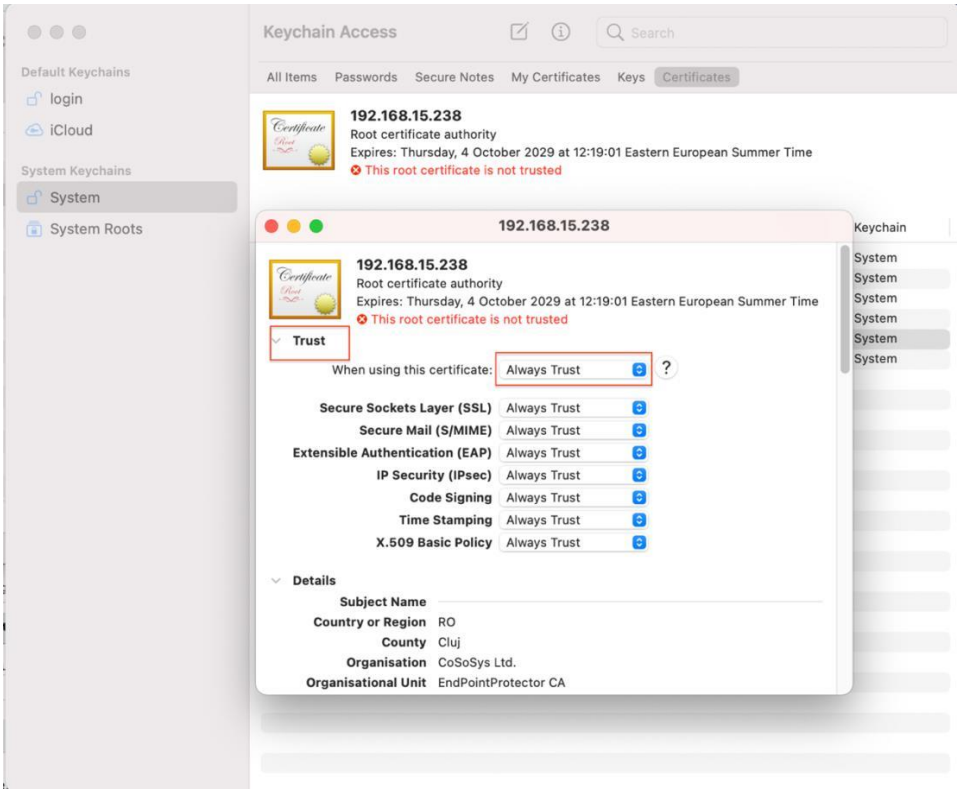


3. 다운로드한 **ClientCerts** 파일 압축을 해제합니다.

4. **cacert.pem** 파일을 선택하고 **키체인 접근, 시스템**에 드래그 앤 드롭합니다.



5. 새롭게 추가된 인증서에 **x** 표시가 됩니다. 더블 클릭 후에 **신뢰** 섹션에서 **항상 신뢰**를 선택합니다.



6. 변경을 **저장**합니다.

중요: 주의 하시기 바랍니다. 서버 인증 스택이 다시 만들어지는 것은 macOS 사용자가 키체인에 새로운 인증서를 강제로 추가하게 만듭니다 (Windows에서는 자동으로 업데이트합니다.).

6.4.3. 심층 패킷 검사(DPI) 포트 및 설정

이 섹션에서 각 네트워크에 사용되는 포트와 함께 모니터링되는 응용프로그램을 연관 시키고 설정을 관리하고 Gmail 제공 업체에 대한 도메인 허용을 추가 할 수 있습니다.

기본값으로 심층 패킷 검사 기능은 미리 정의된 포트 (80, 443, 8080 등) 목록이 설정되어 있습니다. 그러나 특정 네트워크에 사용자 정의 포트가 있다면 즉 콘텐츠 인식 보호 정책으로 정의된 감시되는 응용프로그램이 연결되어 있다면 이 포트는 이 섹션에서 추가 할 수 있습니다.

이 세션에서 다음 설정을 관리할 수 있습니다:

- **텍스트 검사** – 이 설정을 사용하면 Teams, Skype, Slack, Mattermost, Google Spreadsheet, Facebook 포스트, Facebook 코멘트, Instagram 코멘트 온라인 응용프로그램에서 타이핑되는 기밀 콘텐츠를 모니터링합니다.

  참고: Teams, Skype, Slack, Mattermost는 텍스트 검사 설정을 적용하기 위해서 심층 패킷 검사(DPI)를 사용해야 합니다. 이 목록은 개별적으로는 관리할 수 없습니다.

  중요: 차단 모드에서 Slack 및 Google Chat과 같은 플랫폼과 관련된 인스턴트 메시징 이벤트가 여러 번 생성될 수 있습니다. 이러한 동작은 메시지가 차단된 경우 도구의 고유한 재시도 메커니즘에 기인합니다. Endpoint Protector는 보안 강화를 위해 이러한 모든 재시도를 차단하도록 설계되었습니다.

- **상세한 Slack 보고** – **텍스트 검사**와 시스템 구성, 시스템 설정에서 **보고 V2**를 활성화 해야만 사용할 수 있습니다. 이 설정은 보고 및 분석 섹션에서 콘텐츠 인식 보고 페이지에

Slack 상세한 목적지를 보고합니다.

참고: 이 설정은 Endpoint Protector 클라이언트에 활성화된 인터넷 통신이 요구됩니다.

- **피어 인증서 유효성 검사** – DPI 기능이 활성화 되어 있을 때 사용자가 접근하는 웹 사이트의 Endpoint Protector 인증서 유효성 검사를 사용하지 않는 설정을 할 수 있습니다.

  중요: Secure Web Gateway Solution과 같은 웹 사이트 인증서의 유효성을 검사하는 또 다른 네트워크 트래픽 검사 제품이 있을 때만 이 설정을 사용하지 않음

- **웹 메일 감시** – 브라우저의 Gmail 및 Outlook에 대한 제목과 본문을 탐지를 위해 이 설정을 사용합니다. 이 설정에 관계없이 첨부 파일은 감시됩니다.

  중요: Yahoo 사용 시 첨부 파일에 화이트 리스팅 된 이메일 수신자는 수신자가 추가된 후에 첨부 파일이 업로드 될 때만 동작합니다. 첨부 파일을 업로드 후 수신자를 수정하면 파일은 다시 스캔을 하지 않고 새로운 수신자 목록에서 유효성을 검사합니다. Linux 시스템에서 일관성 없는 동작이 발생할 수 있습니다.

  웹 브라우저의 이메일 제목과 본문에 소스코드 탐지를 위해서 **웹 메일 모니터링** 기능을 사용할 수 있습니다. 이메일 응용프로그램에서 소스코드는 제목에서 탐지될 수 있고 본문에서 소스코드는 다른 기능이 배제 없이는 탐지하지 않습니다.

  참고: 확장된 소스코드 탐지 설정을 사용하여 항상 웹 메일 모니터링을 사용하시기 바랍니다.

- **새 Outlook 지원하지 않는 프로토콜 차단** – Outlook 레거시 기능과 상호 작용없이 새 Outlook에서 전자 메일 보내기 기능을 차단하기 위해 이 설정을 사용합니다.

- **Google 비즈니스 계정 도메인 허용**

심층 패킷 검사(DPI)를 사용할 때 전문적인 사용을 위한 특정 Google 도메인에 사용자 접근을 허용하기 위해서 이 설정을 사용합니다.

허용된 비즈니스 계정을 특정하기 위해서 **허용된 비즈니스 계정 추가**의 항목을 타이핑하고 **+** 를 클릭합니다.

허용된 비즈니스 계정 목록에 새로운 항목이 표시됩니다. **x** 를 클릭해서 삭제할 수 있습니다.

중요: Endpoint Protector는 해당 목록에 없는 Gmail, Google Drive, Google Docs 등에 사용된 모든 Google 도메인 (비즈니스 및 개인) 접근을 차단합니다. 만약 목록이 비워 있다면 Google 도메인은 차단되지 않습니다.

6.4.3.1 웹 메일 Json 포맷 파서 사용 모니터링

이 설정을 사용하려면 JSON 개념과 구조에 익숙해야 합니다.

사용된 값은 Endpoint Protector 서버 UI에서 사용한 기본 값 임을 고려해서 다음 문법 예를 살펴보시기 바랍니다:

- 괄호 안에 "," 콤마로 구분해서 여러 경로를 지정할 수 있습니다. 이 경로는 지정된 수서로 한 번에 하나씩 정보가 성공적으로 추출될 때까지 파서(parser)되고 사용됩니다.
- [:]는 배열에서 모든 엔트리를 가져오고 결과를 파싱하고 아래 예제 모두에서 사용될 수 있습니다.

1. Yahoo 서브젝트 추출 예제:

subject={requests[:].payloadParts[:].payload.message.headers.subject}

- 명명된 키 값 쌍 및 어레이 ([]) 사용

  [:] 예제: 어레이에 키가 3가지 요소를 가진 요청에 있다면 경로는 각 요소에 확장됩니다.

  - requests[0].payloadParts[:].payload.message.headers.subject
  - requests[1].payloadParts[:].payload.message.headers.subject
  - requests[2].payloadParts[:].payload.message.headers.subject

  이 후 프로세스는 payloadParts 어레이에 반복됩니다.

2. Gmail 서브젝트 추출 예제:

subject={[1][0][0][1][1][13][0][7]}

- 중첩 어레이만 사용합니다.
- 서브젝트는 특정 어레이의 모든 요소를 통과하지 않고 중첩 어레이 어레이의 특정 경로에 있고 [:]을 사용합니다.

중요: 클라우드 공급업체가 최근에 적용한 변경 사항으로 웹 메일 모니터가 동작하지 않는 한 JSON 파서(parser)의 변경 사항을 적용하지 않는 것이 좋습니다.

6.4.3.2. 피어 인증서 유효성 사용 참고

- **심층 패킷 검사(DPI) 사용** 그리고 **피어 인증서 유효성 사용**으로 되어 있으면 보안이 없는 웹 사이트에 접근할 수 없고 인증서 경고 메시지가 표시됩니다.
- **심층 패킷 검사(DPI) 사용** 그리고 **피어 인증서 유효성 사용 안함**으로 되어 있으면 보안이 없는 이메일에 접근할 수 없고 인증서 경고 메시지는 표시되지 않습니다.

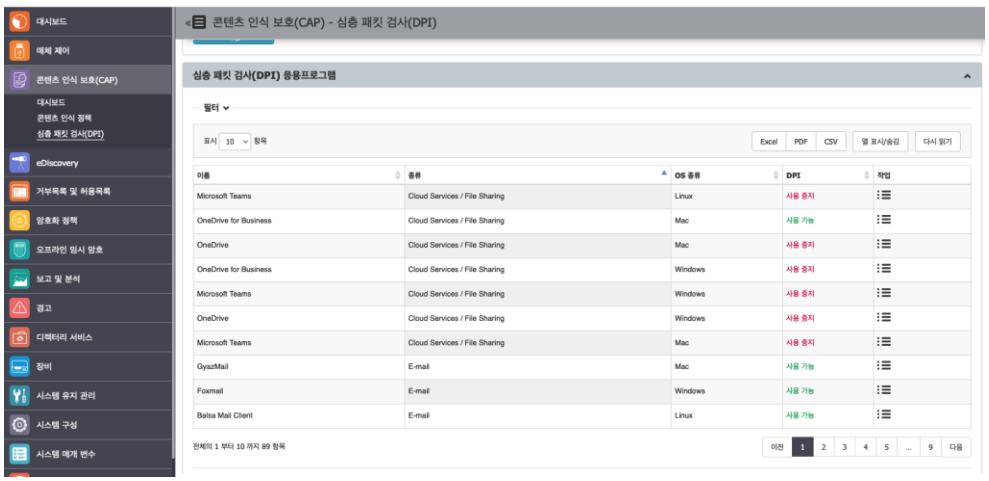
예: 여러분의 조직은 SSL 검사 프록시 또는 게이트웨이를 사용합니다. 프록시/게이트웨이로 검사되는 인증서는 엔드포인트에서 검증될 수 없습니다. 예제: 왜냐하면 이들은 잘못되었거나 발급자의 CA 인증서가 컴퓨터의 인증서 저장소에 "신뢰할 수 있는 루트 인증 기관"에 설치되어 있지 않기 때문입니다.

이러한 경우에 Endpoint Protector DPI 동작을 사용하려면 피어 인증서의 검증을 건너뛰게 하는 것입니다. Endpoint Protector 클라이언트는 이러한 경우에 피어 인증서 검증을 프록시 또는 게이트웨이에서 수행하는 것으로 가정해서 보안을 위협하지 않습니다.

6.4.4. 심층 패킷 검사(DPI) 응용프로그램

이 섹션에서 DPI가 적용되는 각각의 응용프로그램에 대한 활성화 또는 비활성화 설정을 할 수 있습니다.

참고: 심층 패킷 검사(DPI)를 지원하는 응용프로그램은 아래 목록에 있어야만 가능합니다.



중요: 심층 패킷 검사(DPI) 기능은 매체 제어, 설정 (전체, 그룹, 컴퓨터 등)에서 먼저 사용해야 합니다.

참고: 더 자세한 정보는 **전체 설정** 챕터를 참조하시기 바랍니다.

6.4.5. 인증서 상태 메트릭스

Endpoint Protector 서버가 특정 상태를 보고할 때 아래 표 목록을 참고 하시기 바랍니다.

OS	isAvailable	isTrusted	Server Side
macOS	N/A	N/A	N/A
	N/A	0	N/A
	N/A	1	N/A
	0	N/A	Not added
	0	0	Not added
	0	1	Not added
	1	N/A	Not trusted
	1	0	Not trusted
	1	1	Trusted
Linux	N/A	N/A	N/A
	N/A	0	N/A
	N/A	1	N/A
	0	N/A	N/A
	0	0	N/A
	0	1	N/A
	1	N/A	N/A
	1	0	N/A

	1	1	N/A
Windows	N/A		N/A
	0		Not added
	1		Trusted

참고: Linux는 전용 인증서 스토어가 있습니다.

참고: Windows에서는 인증서가 추가되면 자동으로 신뢰됩니다.

7. eDiscovery

이 모듈은 관리자가 보호되는 Windows, macOS, Linux 컴퓨터의 보존 데이터를 검사하는 정책을 만들 수 있습니다. 회사의 데이터 보호 전략을 적용하고 사고 또는 의도적인 데이터 유출의 위험을 관리할 수 있습니다. 관리자는 다음과 같은 민감한 자료를 발견해서 보전 데이터 (data at rest)에 존재하는 문제를 완화할 수 있습니다.

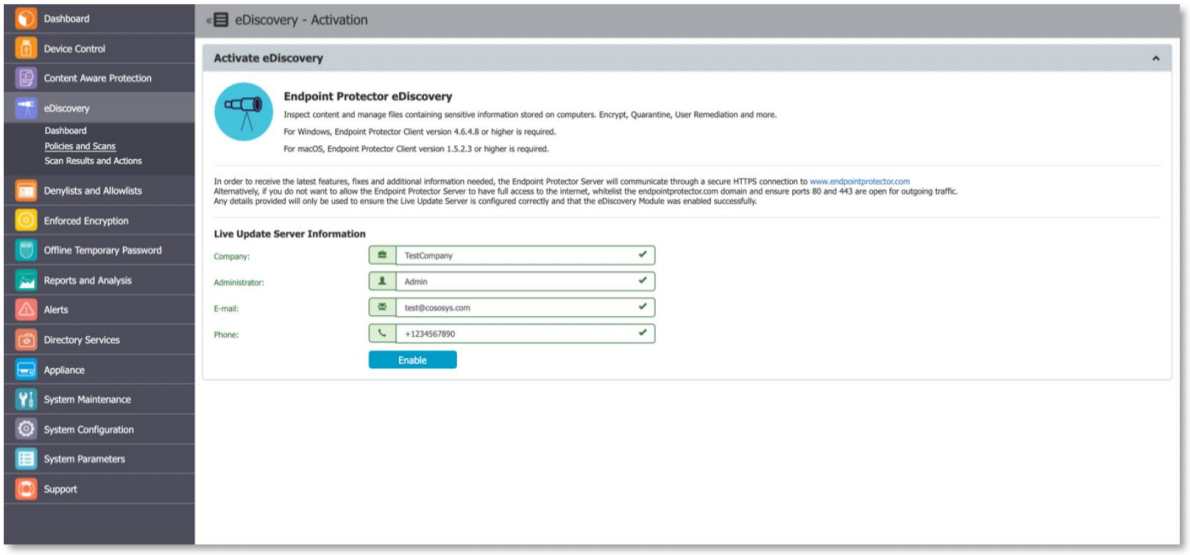
- **개인정보 (Personal Identifiable Information, PII):** 사회보장번호 (SSN), 주민등록번호, 운전면허번호, 이메일 주소, 여권번호, 전화번호, 주소, 날짜 등.
- **금융 및 신용카드 정보:** Visa, MasterCard, American Express, JCB, Discover Card, Dinners Club, 계좌번호 등.
- **기밀 파일:** 영업 및 마케팅 보고서, 기술 문서, 회계 문서, 고객 데이터베이스 등.

7.1. eDiscovery 활성화

eDiscovery는 Endpoint Protector에서 사용할 수 있는 데이터 보호 3단계입니다. 이 모듈 보이면 '사용하기' 버튼을 눌러서 활성화를 해야 사용이 가능합니다. 최고 관리자의 연락처 정보가 필요합니다.

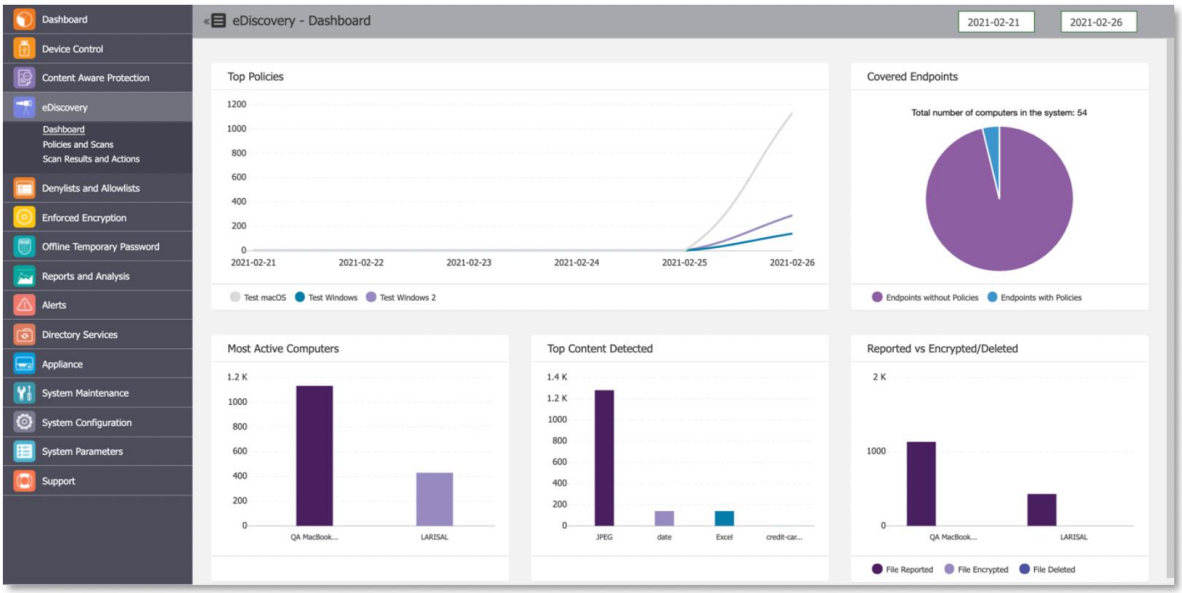
참고: 제공되는 상세 기능은 Live Update 서버가 정화하게 구성되고 eDiscovery 모듈이 성공적으로 사용되었을 때만 사용 가능합니다.

중요: eDiscovery 모듈은 매체 제어 또는 콘텐츠 인식 보호 모듈과 분리되어 있고 별도의 라이선스가 필요합니다.



7.2. 대시보드

이 섹션은 eDiscovery 모듈에 관련된 그래픽과 차트 형태로 빠르게 보여줍니다.



7.3. eDiscovery 정책 및 검색

eDiscovery 정책은 보호되는 컴퓨터에 저장된 데이터의 민감한 콘텐츠를 탐지하는 규칙을 설정합니다. eDiscovery 정책은 5가지 주요 구성 요소로 구성되어 있습니다.

- **OS 종류:** Windows, Mac, Linux 중 적용되는 OS
- **임계값:** 수용할 수 있는 위반의 수
- **정책 거부목록 정책**: 탐지되어지는 콘텐츠
- **정책 허용목록 정책:** 무시할 수 있는 콘텐츠
- **엔터티들:** 적용되는 구분, 그룹 또는 컴퓨터

참고: eDiscovery 정책이 만들어지면 eDiscovery 검색 유형을 선택합니다.

eDiscovery 검색은 정책에서 설정하고 데이터 디스커버리 시작할 때 정의됩니다. 아래 검색을 참조 바랍니다.

- **전체 검색 시작:** 처음부터 보존 데이터 검색을 시작
- **증분 검색 시작:** 이어서 보존 데이터 검색을 시작 (이전에 검색한 파일은 건너뜀)

eDiscovery 관리자는 증분 검색 설정을 통해서 자동 검색을 사용할 수 있습니다.

- **일회** – 특정 날짜와 시간에 한 번 검색
- **매주** – 특정 날짜와 시간에 매 7일마다 검색
- **매월** – 특정 날짜와 시간에 매 30일마다 검색

eDiscovery 검색은 원할 때 정지를 할 수 있고 결과는 자동으로 사라집니다.

아래 검색 정지를 참조 바랍니다.

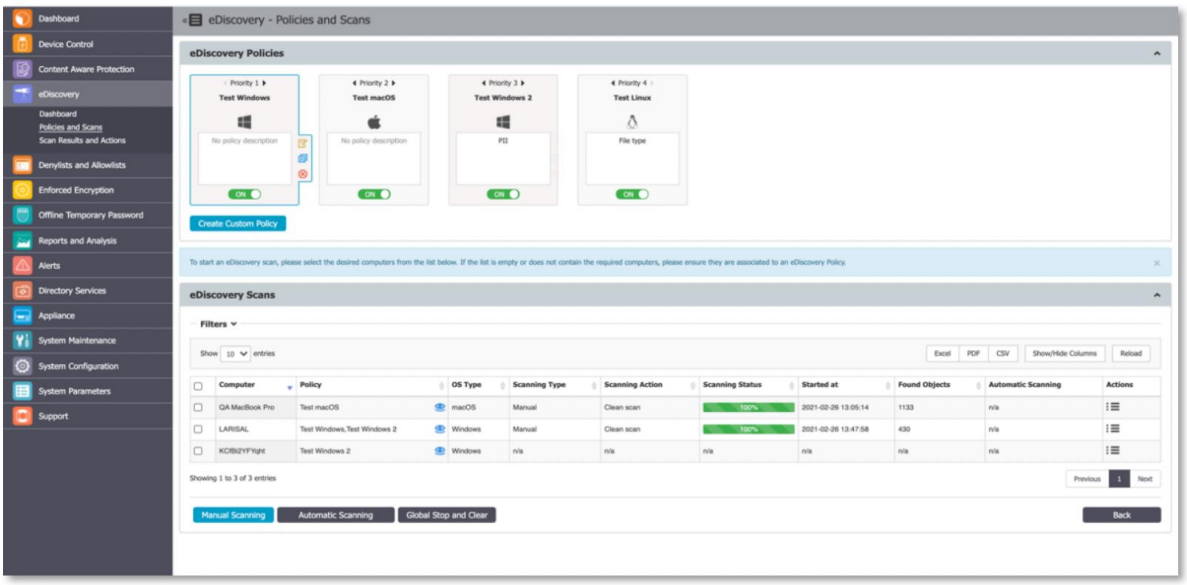
- **중단:** 검색을 중지 (하지만 로그에 영향을 주지 않음)

- **검색 중지 및 로그 삭제:** 검색을 중지하고 로그를 삭제

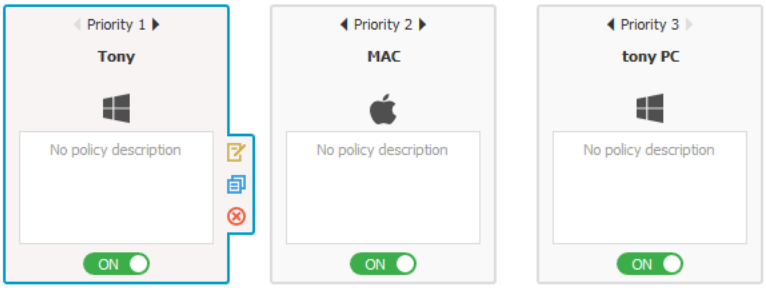
참고: 전체 정지 및 삭제 버튼은 모든 eDiscovery 검색을 정지하고 모든 로그를 삭제할 때 사용합니다.

7.3.1. eDiscovery 정책 및 검색 만들기

eDiscovery, 정책 및 검색 섹션에서 간단하게 eDiscovery 정책 및 검색을 만들고 관리할 수 있습니다.



새로운 정책은 사용자 정책 만들기 버튼을 클릭해서 만들 수 있고 이미 만들어진 정책은 더블 클릭해서 수정할 수 있습니다. 정책 수정, 복사, 삭제 옵션은 원하는 정책을 선택한 후에 사용 가능합니다.



새로운 정보를 만들 때 다음을 선택합니다:

- **정책 정보** (OS 종류, 정책 이름, 정책 설명, 액션, 유형)
- **정책 출구 포인트**
- **정책 거부목록, 정책 허용목록**
- **정책 엔터티들** (구분, 그룹, 컴퓨터)

다음 임계값을 사용할 수 있습니다.

- **보고하는 eD 제한**
- **위협 임계값**
- **파일 크기 임계값**

Endpoint Protector 사용자 인터페이스에서 직접 임계값의 더 자세한 내용을 찾을 수 있습니다.

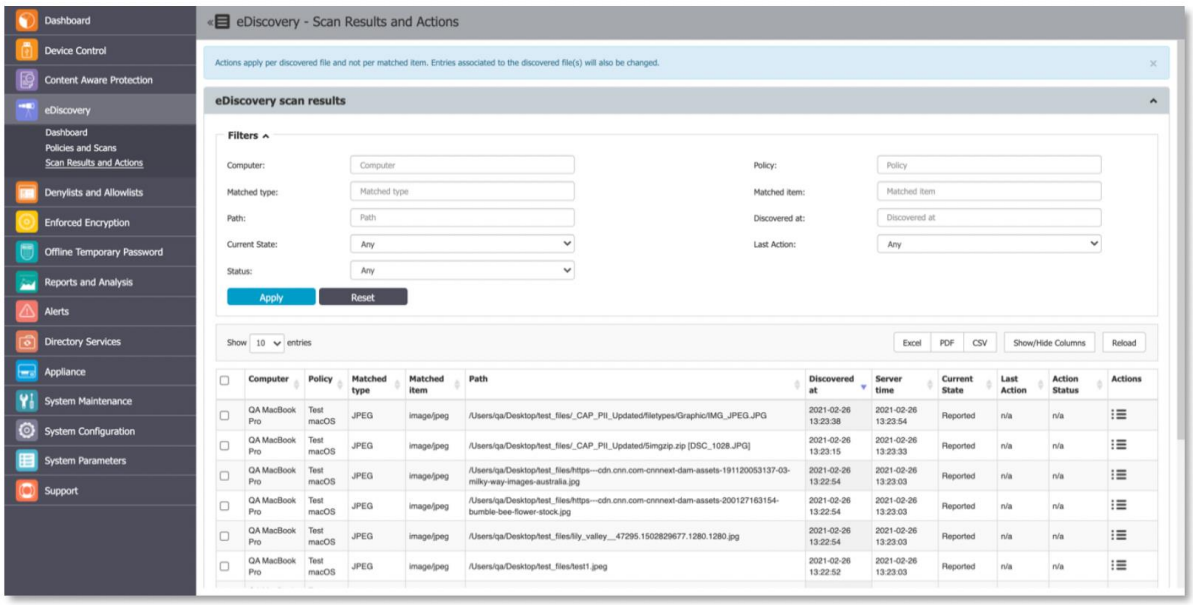
거부목록 및 허용목록의 자세한 내용은 거부목록 및 허용목록 챕터를 참조하시기 바랍니다.

eDIscovery 정책을 만든 후에 검색 액션을 선택할 수 있습니다. **전체 검색 시작, 증분 검색 시작, 중단, 검색 중지** 및 **로그 삭제**가 여기에 포함됩니다.

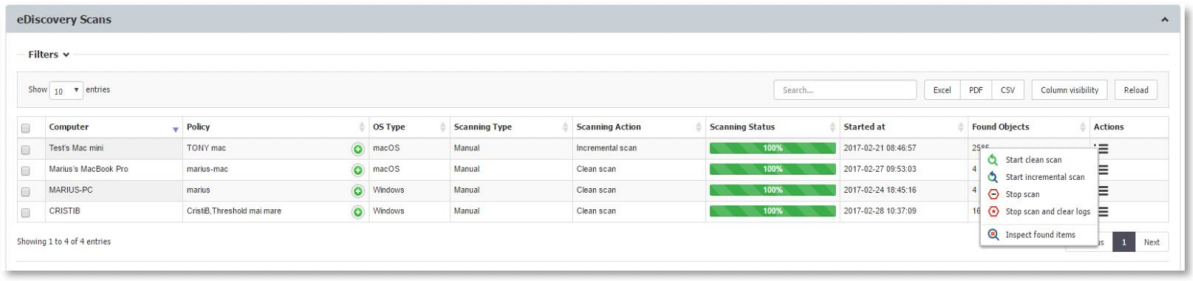
참고: 콘텐츠 인식 보호 정책과 같이 eDiscovery 정책 및 검색은 심지어 오프라인 상태에서도 보호되는 컴퓨터에 저장된 민감한 데이터 검색을 계속해서 수행합니다. 로그는 Endpoint Protector에 저장되고 서버와 연결되는 즉시 보내집니다.

7.4. eDiscovery 검색 결과 및 액션

eDiscovery 검색이 시작된 후에 발견된 항목을 검사하고 조치 (예: 타겟 삭제, 타겟 암호화, 타겟 복호화 등)를 취할 수 있습니다. 모든 결과는 eDiscovery, 검색 결과 및 액션 섹션에 나타납니다.

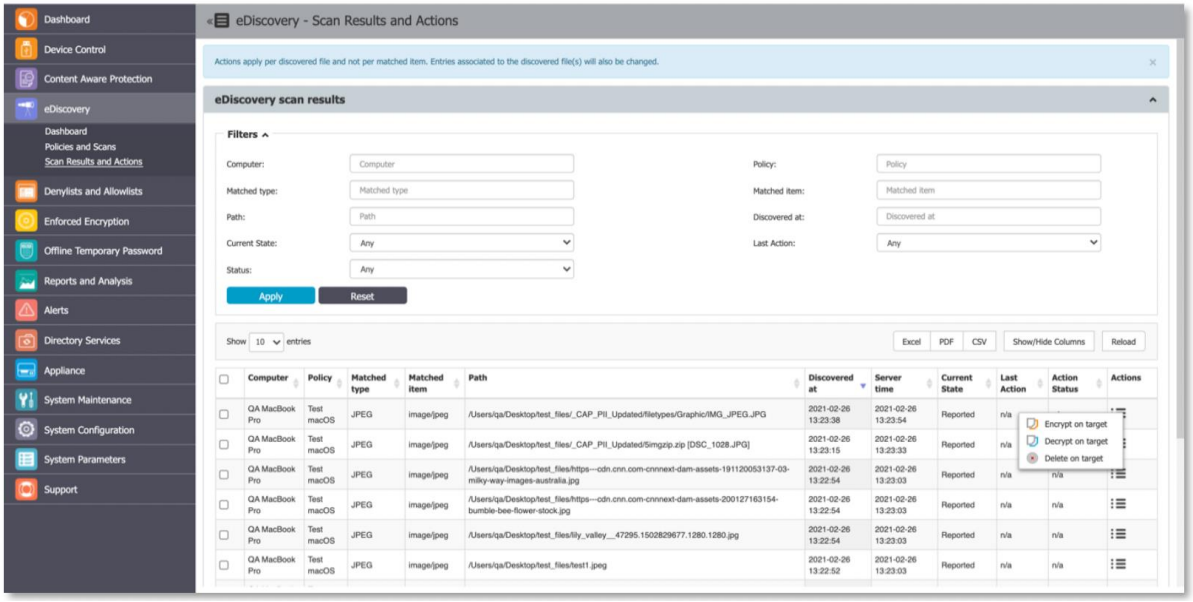


검색 결과 및 액션 섹션은 또한 eDiscovery 검색 목록에서 컴퓨터 선택 후 검사된 항목 찾기를 선택하여 "eDiscovery > 정책 및 검색"에서 바로 접근할 수 있습니다. 자동으로 검색 결과 목록을 필터링하고 특정 컴퓨터의 항목만 보입니다.



7.4.1. 검색 결과 보기 및 조치 하기

이 섹션에서 관리자는 스캔 결과를 관리할 수 있습니다. 스캔이 된 모든 컴퓨터의 목록 보기가 가능하고 삭제, 암호화, 복호화 조치를 할 수 있습니다.



관리자는 각 항목에 개별적으로 원하는 조치를 적용할 수 있고 여러 항목에 동시에 원하는 조치를 취할 수 있습니다.

8. 거부목록 및 허용목록

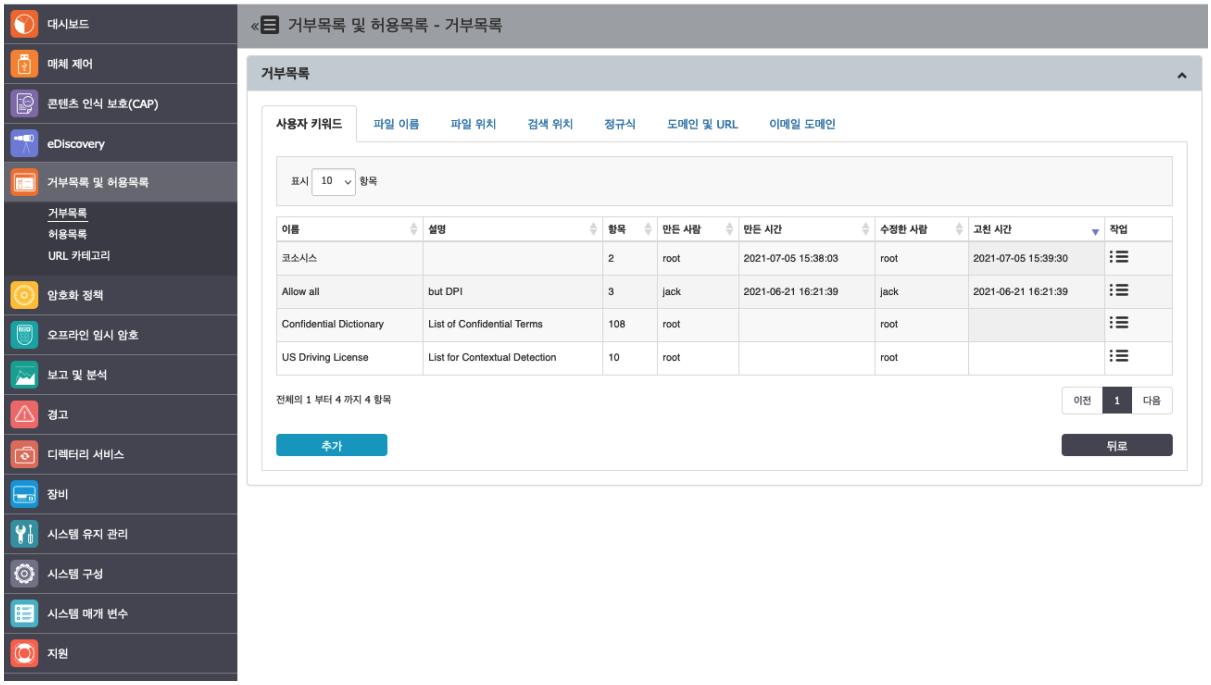
이 섹션에서 관리자는 콘텐츠 인식 보호 및 eDiscovery 모듈에서 사용할 수 있는 거부목록 및 허용목록을 만들 수 있습니다. 정의가 되면 바로 원하는 정책에서 거부목록 및 허용목록 사용이 가능합니다. 모든 거부목록 및 허용목록은 아래에서 자세히 설명하겠습니다.

거부목록 및 허용목록 사용						
대분류	소분류	OS			모듈	
		Windows	macOS	Linux	콘텐츠 인식 보호(CAP)	eDiscovery
거부목록	사용자 키워드	✓	✓	✓	✓	✓
	파일 이름	✓	✓	✓	✓	✓
	파일 위치	✓	✓	✓	✓	✓
	검색 위치	✓	✓	✓	x	✓
	정규식	✓	✓	✓	✓	✓
	도메인 및 URL	✓	✓	✓	✓	x
	이메일 도메인	✓	✓	✓	✓	x
허용목록	MIME 유형	✓	✓	✓	✓	✓
	허용된 파일	✓	✓	✓	✓	✓
	파일 위치	✓	✓	✓	✓	✓
	네트워크 공유	✓	✓	x	✓	x
	이메일 도메인	✓	✓	✓	✓	x
	URL 주소	✓ (Internet Explorer 만)	x	x	✓	x
	심층 패킷 검사(DPI)	✓	✓	✓	✓	x
URL 카테고리		✓	✓	✓	✓	x

8.1. 거부목록

8.1.1. 사용자 키워드

사용자 키워드 거부목록은 Endpoint Protector의 민감한 콘텐츠로 탐지되는 용어와 표현의 사용자 정의 목록입니다. 콘텐츠 인식 보호(CAP)와 eDiscovery 모듈 모두에서 사용 가능합니다.

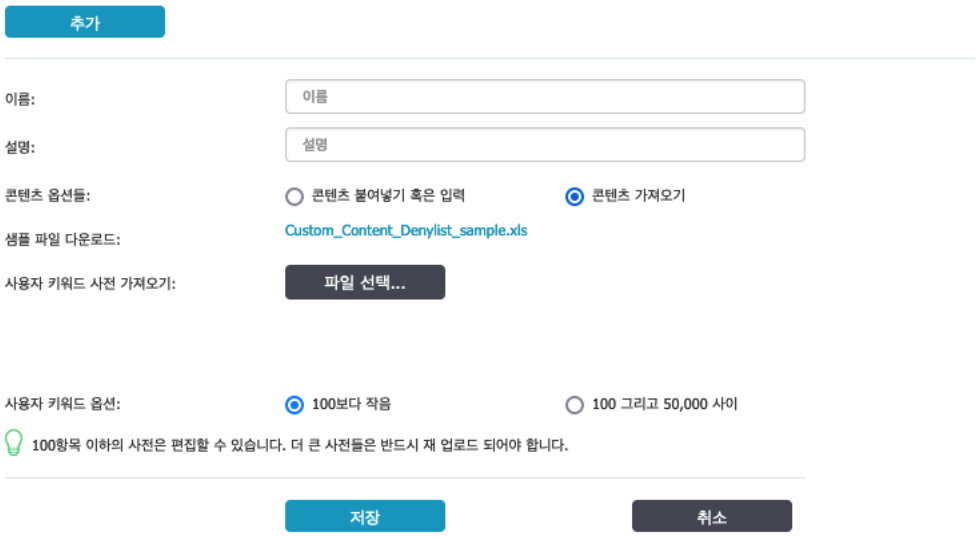


이 섹션에서 사용자 정의 콘텐츠 거부목록을 추가하거나 볼 수 있고 **작업** 컬럼에서 기존의 거부목록을 편집, 삭제, 내보내기 할 수 있습니다.

새로운 거부목록을 만들려면 사용 가능한 거부목록 항목에서 **추가**를 클릭하고 **이름**과 **설명**을 입력한 다음 적어도 3자 이상을 **직접 입력하거나 붙여넣기** 합니다. 각각의 내용은 줄 바꿈, 쉼표, 세미 콜론으로 구분합니다. 제공된 샘플 파일을 사용하여 **콘텐츠 가져오기**를 할 수 있습니다. 업로드된 키워드 개수를 기반으로 옵션을 선택합니다.

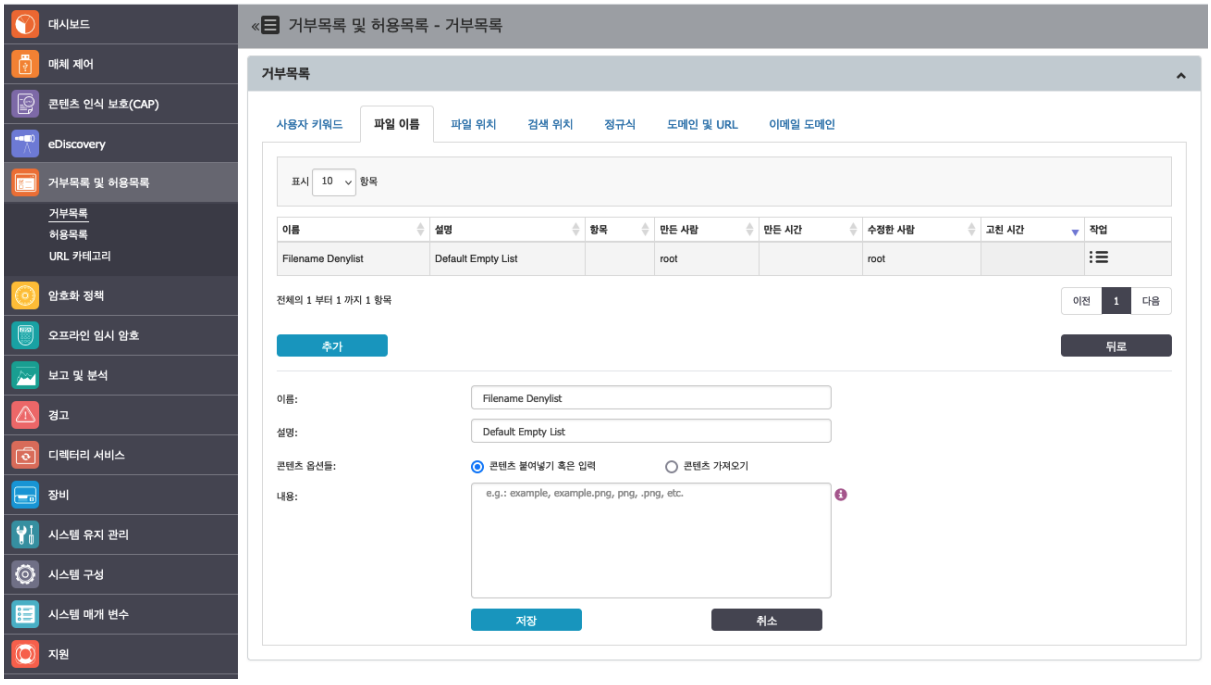
참고: 100보다 작은 키워드는 수정할 수 있습니다. 더 큰 수의 키워드는 다시 업로드해야 합니다.

거부목록은 만들면 사용자 키워드 목록에 표시되고 콘텐츠 인식 보호(CAP) 또는 eDiscovery 정책을 만들거나 편집할 때 사용할 수 있습니다.



8.1.2. 파일 이름

파일 이름 거부목록은 Endpoint Protector로 탐지되는 파일 이름의 사용자 정의 목록입니다. 콘텐츠 인식 보호(CAP)와 eDiscovery 모듈 모두에서 사용할 수 있습니다.



이 섹션에서 파일 이름 거부목록을 보거나 추가할 수 있고 **작업** 컬럼에서 기존 거부목록을 편집, 삭제, 내보내기 할 수 있습니다.

새로운 거부목록을 만들려면 사용 가능한 거부목록 항목에서 **추가**를 클릭하고 **이름**과 **설명**을 입

력한 다음 적어도 3자 이상을 **직접 입력하거나 붙여넣기** 합니다. 각각의 내용은 줄 바꿈, 쉼표, 세미 콜론으로 구분합니다. 제공된 **샘플 파일**을 사용하여 **콘텐츠 가져오기**를 할 수 있습니다

파일 이름, 파일 이름과 확장자 또는 확장자만 추가할 수 있도록 콘텐츠를 정의할 수 있습니다.

- **example.pdf** 파일이름 – example.pdf로 끝나는 모든 파일은 차단됩니다.

  _매치됨: example.pdf, my_exmple.pdf

  _매치되지 않음: example.txt, myexample.txt, test.pdf, example.pdf.txt, test_exmaple.pdf_test.zip

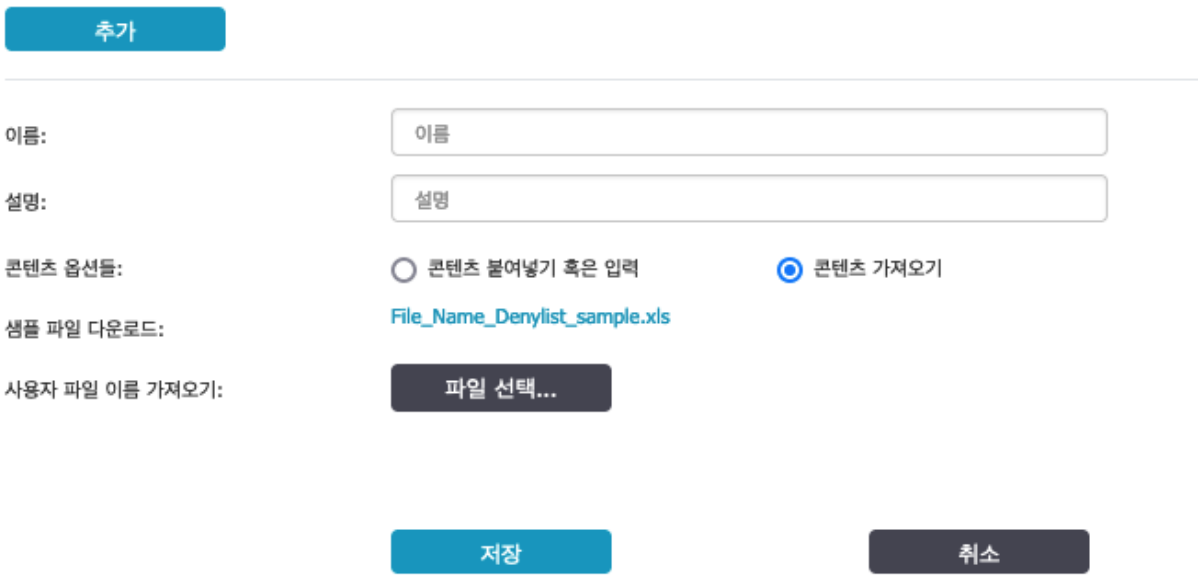
- **.epp** 확장자 - .epp 확장자를 가지는 모든 파일은 차단됩니다.

  _매치됨: test.epp, mail.epp, 123.epp

  _매치되지 않음: 123.epp.zip, mail.epp.txt

거부목록을 만들면 파일 이름 목록이 표시됩니다. 콘텐츠 인식 보호(CAP) 또는 eDiscovery 정책을 만들거나 수정할 때 사용할 수 있습니다.

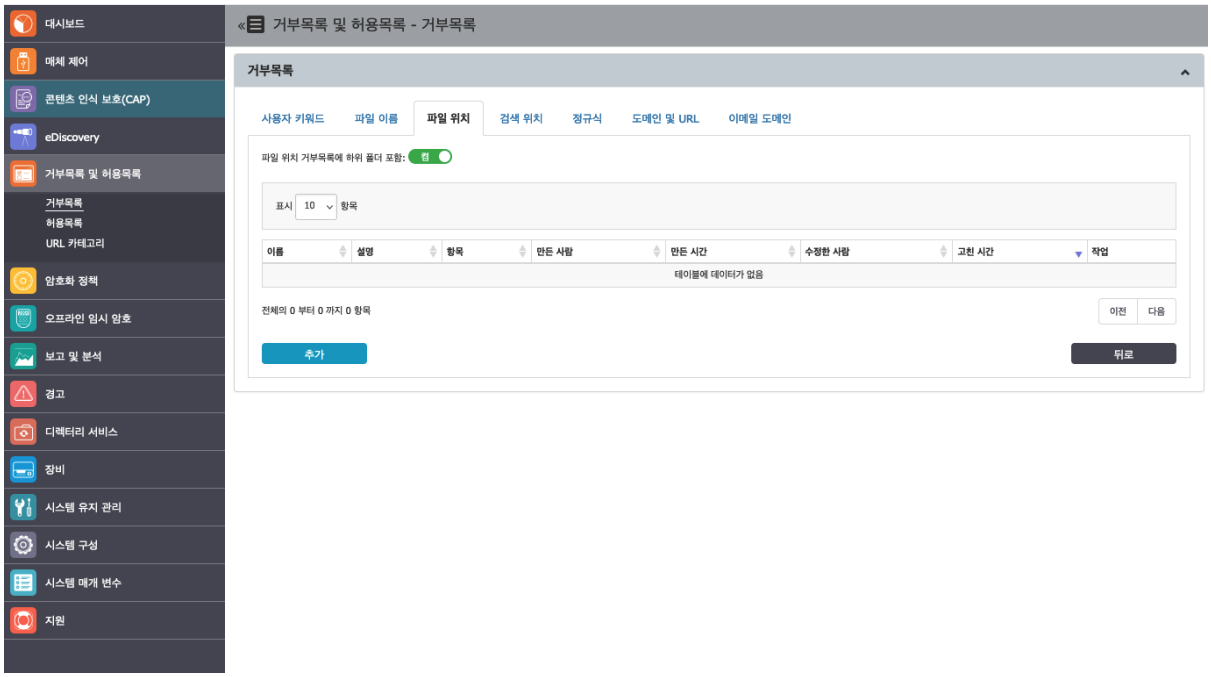
중요: 콘텐츠 인식 보호에서 파일 이름 거부목록은 차단 및 보고 정책에서만 동작합니다. 대소문자 구분 및 단어 단위 적용 옵션은 사용할 수 없습니다.



8.1.3. 파일 위치

파일 위치 거부목록은 Endpoint Protector로 식별되는 위치에 대한 사용자 정의 목록입니다. 이 위치에서 파일 전송은 다양한 정책에서 정의된 콘텐츠 검사 규칙 또는 허용에 관계없이 자동으로 차단됩니다.

파일 위치 거부목록은 콘텐츠 인식 보호(CAP)와 eDiscovery 모듈에서 모두 사용할 수 있습니다.



파일 위치 거부목록에 하위 폴더 포함 옵션 사용은 시스템을 통한 모든 다른 파일 위치 거부목록 및 허용목록에 영향을 줍니다. 기본적으로 파일 위치 거부목록은 특정 폴더에 위치한 모든 파일 뿐만 아니라 서브 폴더가 포함된 다른 파일에도 적용됩니다.

참고: 파일 위치 거부목록을 정의하는 것 이외에도 파일 전송에 사용되는 브라우저 또는 응용프로그램 또한 콘텐츠 인식 보호 정책에서 선택되어야 합니다.

이 섹션에서 파일 이름 거부목록을 보거나 추가할 수 있고 **작업** 컬럼에서 기존 거부목록을 편집, 삭제, 내보내기 할 수 있습니다.

새로운 거부목록을 만들려면 사용 가능한 거부목록 항목에서 **추가**를 클릭하고 **이름**과 **설명**을 입

력합니다. 각각의 내용은 줄 바꿈, 쉼표, 세미 콜론으로 구분합니다. **그룹**과 **컴퓨터**를 선택합니다.

중요: 파일 위치 거부목록은 사용자 그룹에는 적용되지 않고 컴퓨터 그룹에만 적용됩니다. 파일 위치 거부목록은 15분 후에 선택된 컴퓨터 그룹에만 적용됩니다.

파일 위치 거부에서 와일드 카드를 사용해서 와일드카드 매칭을 특정합니다. Windows의 Desktop 폴더를 매칭하기 위해서 다음 패턴을 사용합니다: "**?:₩Users₩*₩Desktop₩**".

파일 위치에 대한 와일드 카드 사용 예제			
와일드 카드 유형	**파일 위치**	**매칭된 결과**	**매칭되지 않은 결과**
암시적	C:₩temp	C:₩temp₩file.txt C:₩temp₩test₩file2.txt C:₩tempfile.txt	C:₩temp1₩file.txt C:₩Windows₩file.txt
명시적	C:₩Windows₩*	C:₩Windows₩regedit.exe C:₩Windows₩system32₩notepad.exe	C:₩Windows.old₩regedit.exe C:₩Windows.old₩system32₩notepad.exe

8.1.4. 검색 위치

검색 위치 거부목록은 eDiscovery 모듈로 식별되는 사용자 정의 위치 거부 목록입니다. 이 위치의 저장 데이터(Data at rest)는 다양한 정책으로 정의된 규칙에 따라서 자동으로 콘텐츠를 검사합니다.

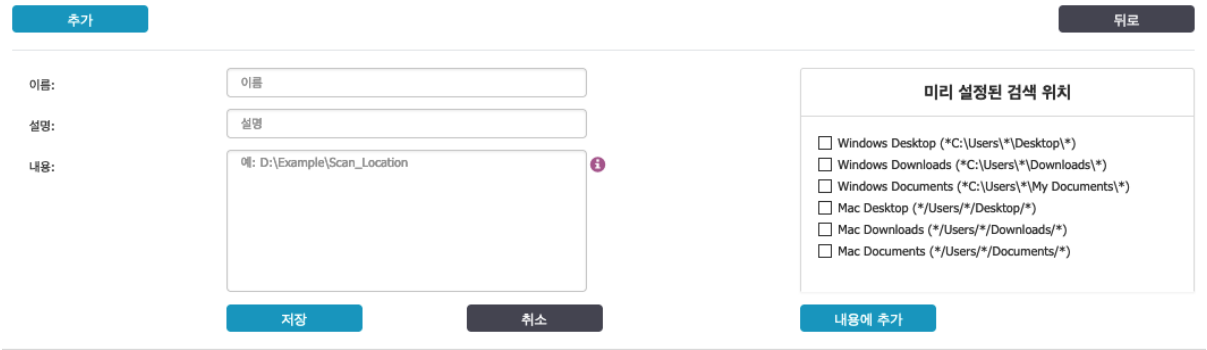
이 섹션에서 파일 이름 거부목록을 보거나 추가할 수 있고 **작업** 컬럼에서 기존 거부목록을 편집, 삭제, 내보내기 할 수 있습니다.

새로운 거부목록을 만들려면 사용 가능한 거부목록 항목에서 **추가**를 클릭하고 **이름**과 **설명**을 입력합니다. 각각의 내용은 줄 바꿈, 쉼표, 세미 콜론으로 구분하거나 **미리 설정된 검색 위치**에서 선택 후 **내용에 추가**를 합니다.

검색 위치를 정의할 때 경로에 아래 특수 문자를 사용합니다.

***** - 모든 단어 대체

? – 모든 문자 대체

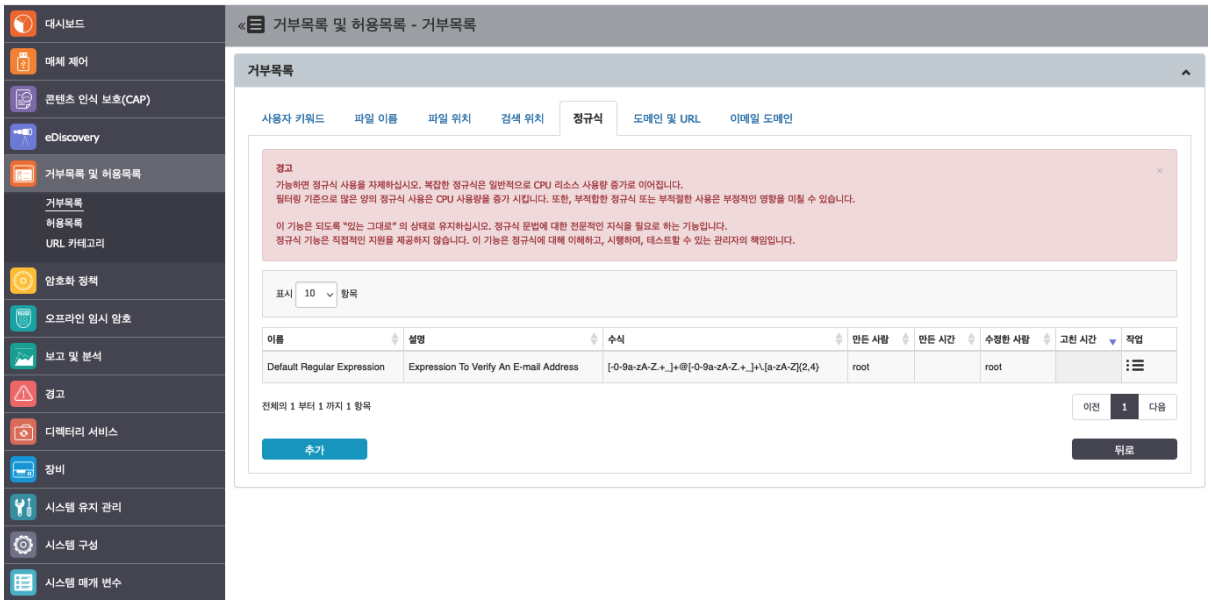


8.1.5. 정규식

정규식은 주로 문자열과 패턴 매칭에 사용하기 위한 검색 패턴을 형성하는 문자 시퀀스입니다.

보호되는 네트워크로 전송되는 데이터에서 특정 반복을 찾도록 정규식을 만들 수 있습니다. 정규식 거부목록은 콘텐츠 인식 보호(CAP)와 eDiscovery 모듈 모두에서 사용할 수 있습니다.

중요: 가능하면 정규식 표현 사용을 자제하시기 바랍니다. 일반적으로 리소스 사용이 증가하고 필터링 기준으로 많은 정규식을 사용하면 CPU 사용량이 급증합니다. 또한 부적절한 정규식 사용은 부적절한 영향을 가져올 수 있습니다.



이 섹션에서 정규식을 보거나 추가할 수 있고 **작업** 컬럼에서 기존 거부목록을 편집, 삭제, 내보내기 할 수 있습니다.

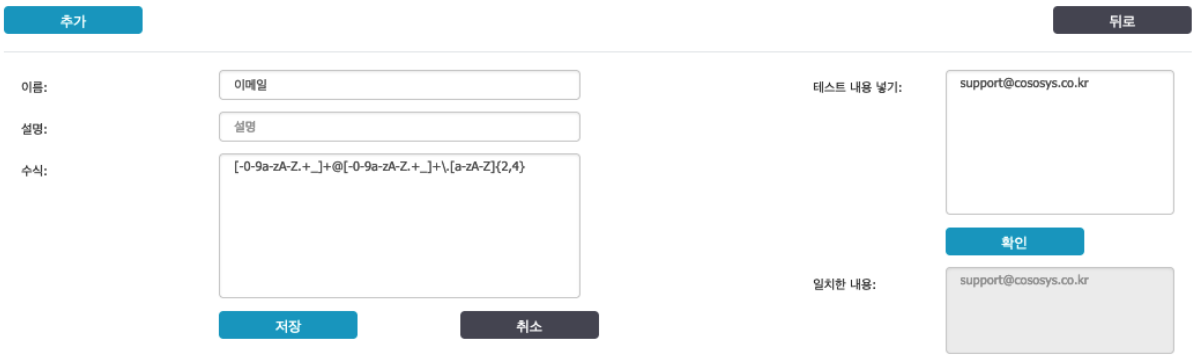
새로운 거부목록을 만들려면 사용 가능한 거부목록 항목에서 **추가**를 클릭하고 **이름**과 **설명**을 입력합니다. 정규식을 추가합니다.

오른쪽 옵션을 사용하여 정규식 정확성을 **테스트**할 수 있습니다. 콘텐츠를 추가하고 테스트를 클릭합니다. 정규식에 에러가 없다면 아래와 같이 일치한 내용 박스에 같은 콘텐츠가 나타날 것입니다.

이메일 매칭: [-0-9a-zA-Z.+_]+@[-0-9a-zA-Z.+_]+₩.[a-zA-Z]{2,4}

IP 매칭: (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)(₩.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)){3}

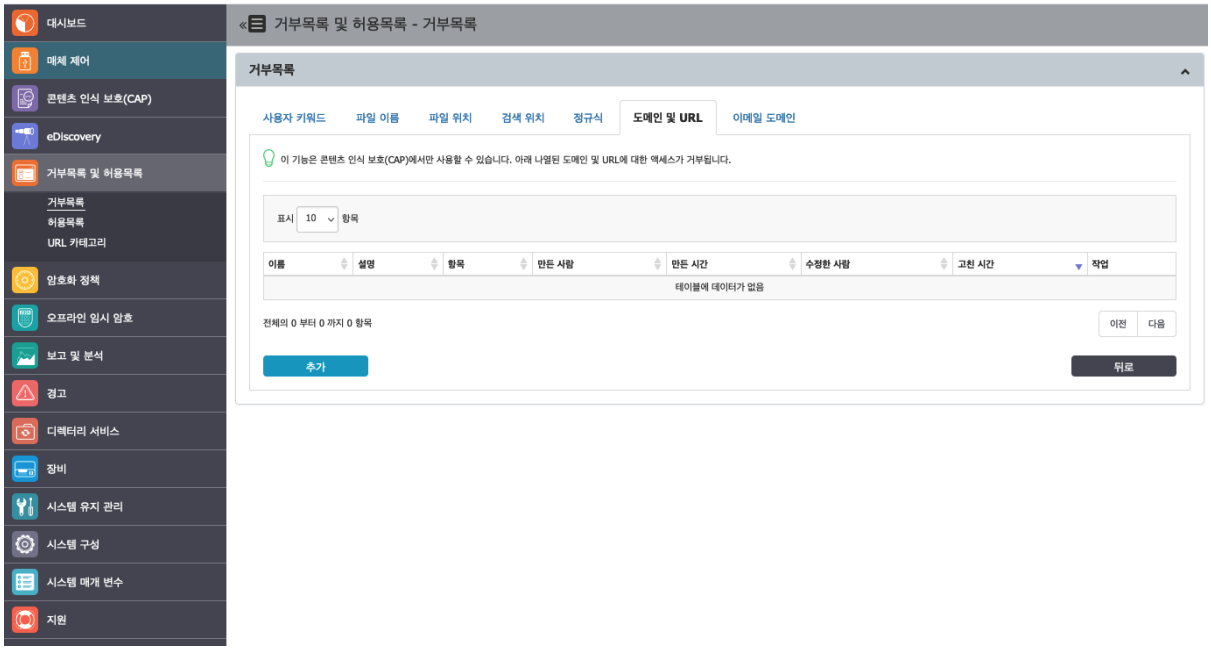
참고: 이 기능은 "있는 그대로 (as is)" 제공되며 정규식 문법에 대한 고급 지식이 필요합니다. 직접적인 지원은 제공되지 않으며 정규식 표현을 학습하고 구현하는 것은 고객의 책임입니다.



8.1.6. 도메인 및 URL

도메인 및 URL 거부목록은 Endpoint Protector로 식별되는 사용자 정의 웹 주소 거부목록 입니다. 이 목록에 있는 도메인 및 URL 접근은 거부됩니다.

참고: 도메인 및 URL 접근은 콘텐츠 인식 보호(CAP) 모듈에서만 사용할 수 있습니다.



이 섹션에서 도메인 및 URL 거부목록을 보거나 추가할 수 있고 **작업** 컬럼에서 기존 거부목록을 편집, 삭제, 내보내기 할 수 있습니다.

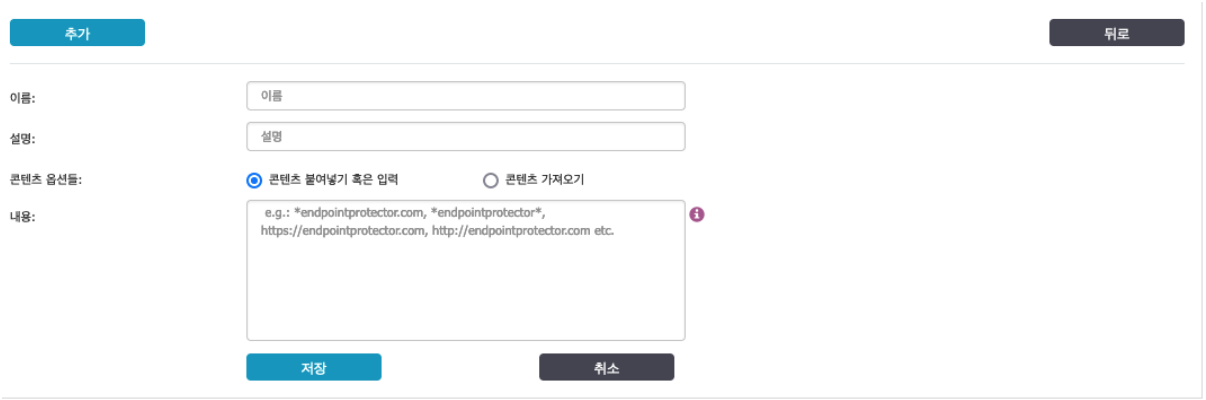
새로운 거부목록을 만들려면 사용 가능한 거부목록 항목에서 **추가**를 클릭하고 **이름**과 **설명**을 입력한 다음 **직접 입력하거나 붙여넣기** 합니다. 각각의 내용은 줄 바꿈, 쉼표, 세미 콜론으로 구분합니다. 제공된 **샘플 파일**을 사용하여 **콘텐츠 가져오기**를 할 수 있습니다.

목록을 100개까지 만들거나 가져올 수 있고 각 목록은 50,000개의 웹 도메인까지 구성할 수 있습니다.

참고: 100개의 웹 도메인으로 구성된 목록은 편집할 수 있지만 더 많은 도메인이 포함되어 있으면 다시 가져와야 합니다.

파일 이름, 파일 이름 및 확장자 또는 확장자만 추가해서 콘텐츠를 정의할 수 있습니다 – pdf, test1example.pdf, example.endpointprotector.com, *example.com, *example*example, https://website.com.

거부목록을 만들면 도메인 및 URL 목록에 표시되고 콘텐츠 인식 보호 정책을 만들거나 수정할 때 사용할 수 있습니다.

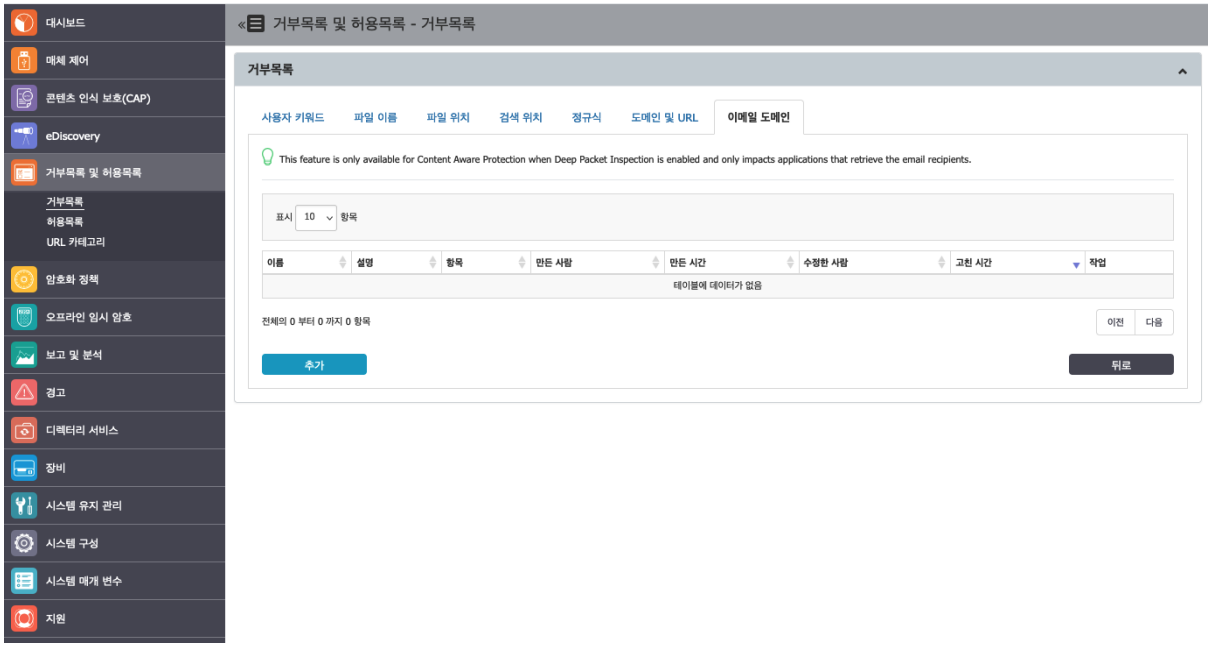


8.1.7. 이메일 도메인

이메일 도메인 거부목록은 사용자의 이메일 보내기를 차단하는 그룹과 컴퓨터에 적용되는 사용자 정의 이메일 주소와 도메인입니다.

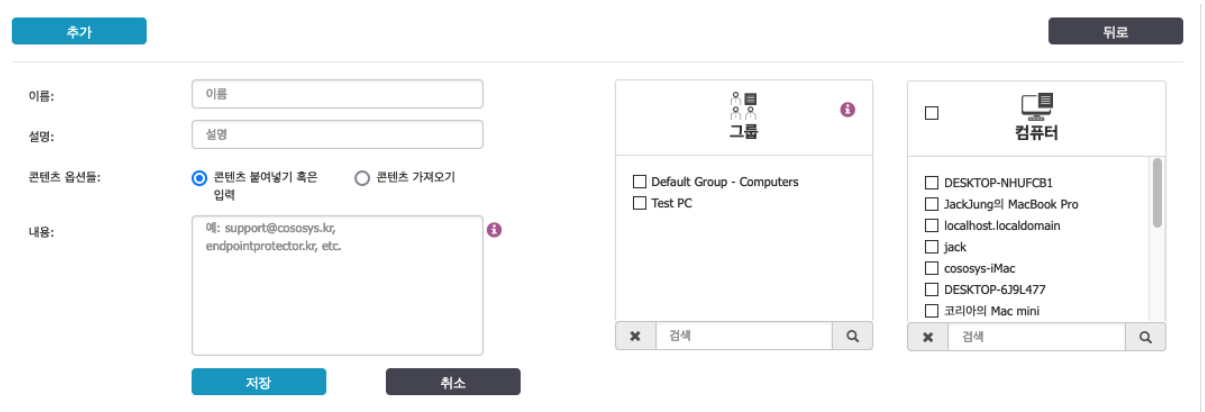
중요: 이 기능은 콘텐츠와 종류에 관계없이 사용자가 보내는 이메일을 차단합니다. 이 거부목록은 정책이 아니라 컴퓨터에 적용되어서 수정이 보고만 또는 차단 및 수정 정책에서 선택한 응용프로그램에서 이메일을 차단합니다. 사용자 수정은 가능하지 않습니다.

참고: 이 기능은 심층 패킷 검사(DPI)를 사용하는 콘텐츠 인식 보호(CAP)에서만 사용할 수 있습니다. 이메일 수신자를 찾는 응용프로그램에 영향을 주고 콘텐츠 인식 보호(CAP) 정책에서 선택됩니다.



이 섹션에서 이메일 도메인 거부목록을 보거나 추가할 수 있고 **작업** 컬럼에서 기존 거부목록을 편집, 삭제, 내보내기 할 수 있습니다.

새로운 거부목록을 만들려면 사용 가능한 거부목록 항목에서 **추가**를 클릭하고 **이름**과 **설명**을 입력합니다. 각각의 내용은 줄 바꿈, 쉼표, 세미 콜론으로 구분합니다. **그룹**과 **컴퓨터**를 선택합니다. 제공된 **샘플 파일**을 사용하여 **콘텐츠 가져오기**를 할 수 있습니다



8.1.8. 응용 프로그램

이 섹션은 CLI (Command Line Interface) 커맨드 거부목록 사용과 관련된 문서를 소개합니다. CLI

커맨드 거부 목록으로 고객에게 더 강력한 응용 프로그램 시작 이벤트를 통제하고 특정 응용 프로그램을 런칭하는데 사용되는 커맨드 라인 인수(arguments)를 면밀히 조사할 수 있는 기능을 제공합니다. 이 기능은 콘텐츠 인식 보호 (CAP) 정책의 정밀도를 향상시켜 사용자가 특정 응용 프로그램 사용에 대한 가시성을 확보하고 제어할 수 있습니다.

예제: 아래 Google Chrome의 예와 같이 응용 프로그램의 시작 모드를 제어하는 시나리오를 고려해 보시기 바랍니다.

chrome.exe --incognito

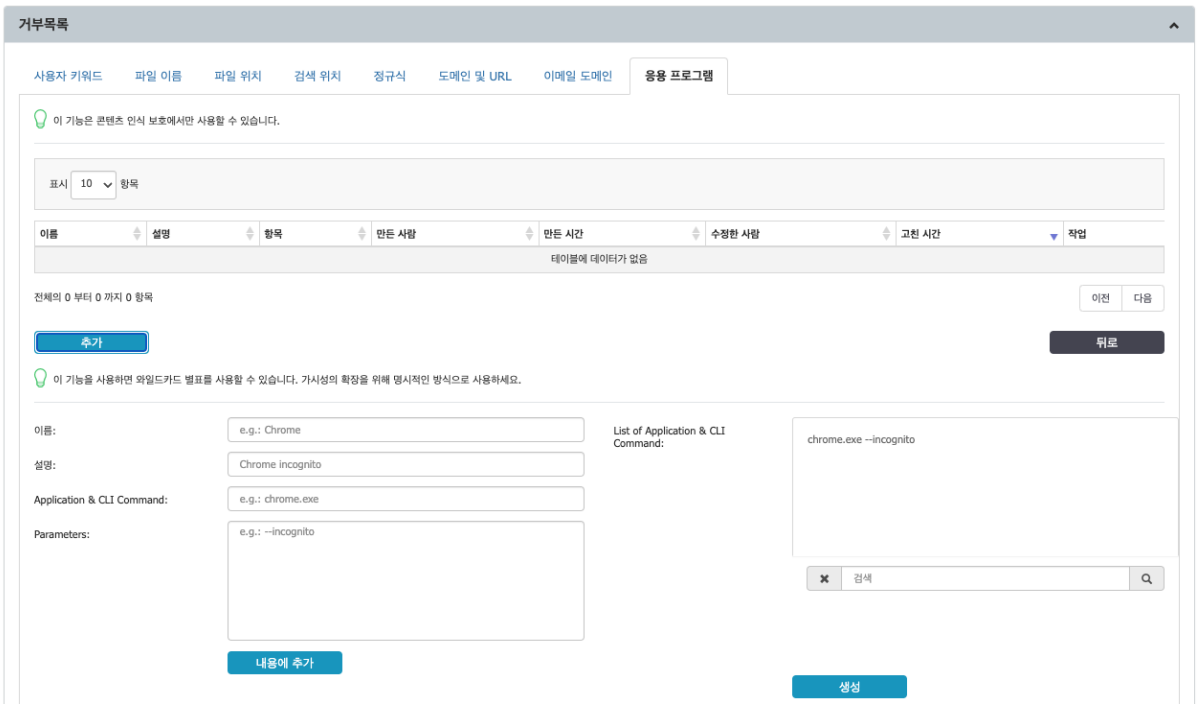
CLI 커맨드 거부목록으로 특정 응용 프로그램 동작과 일치하는 커맨드 라인 인수 (command line arguments)에 대한 기준을 정의 할 수 있습니다. 이를 통해서 조직은 필요한 CAP 정책을 생성하여 응용 프로그램 실행과 동작이 보안 및 규정 준수 요구사항에 부합하도록 만들 수 있습니다.

중요: 운영체제 코어 (Operating System Core)에 내장된 'ls', 'md', 'cd'와 같은 특정 기본 커맨드 라인 유틸리티는 CAP 가시성에 잡히지 않을 수 있습니다. 이러한 커맨드는 운영 체제 기능에 필수이며 일반적으로 CAP 정책에서 제외되고 나가는 채널이 아닙니다.

CLI 커맨드 정책을 정의하려면 아래 단계를 따르시기 바랍니다:

1. Endpoint Protector 콘솔의 '거부목록 > 응용 프로그램' 탭으로 이동
2. 제어가 필요한 응용 프로그램에서 사용되는 커맨드 라인 인수를 기반으로 기준을 정의
3. 위에서 설정한 기준을 CAP 정책 인수로 통합하여 응용 프로그램 사용량을 정확하게 제어 및 모니터링

위의 단계에 따라 CLI 커맨드 거부목록을 활용하여 조직의 보안을 강화하고 정책 및 규정을 준수하는 응용 프로그램을 사용하도록 보장하시기 바랍니다.



참고: 현재 EPP 클라이언트의 가시성은 PowerShell 및 PowerShell ISE로 인해서 제한되어 있습니다.

참고: 지금으로서는 macOS 및 Linux 기본 CLI 작업에 대한 가시성은 제공하지 않으며 여기에 touch, cp, cd, mv, mkdir 같은 작업이 포함됩니다.

8.2. 허용목록

8.2.1. MIME 유형

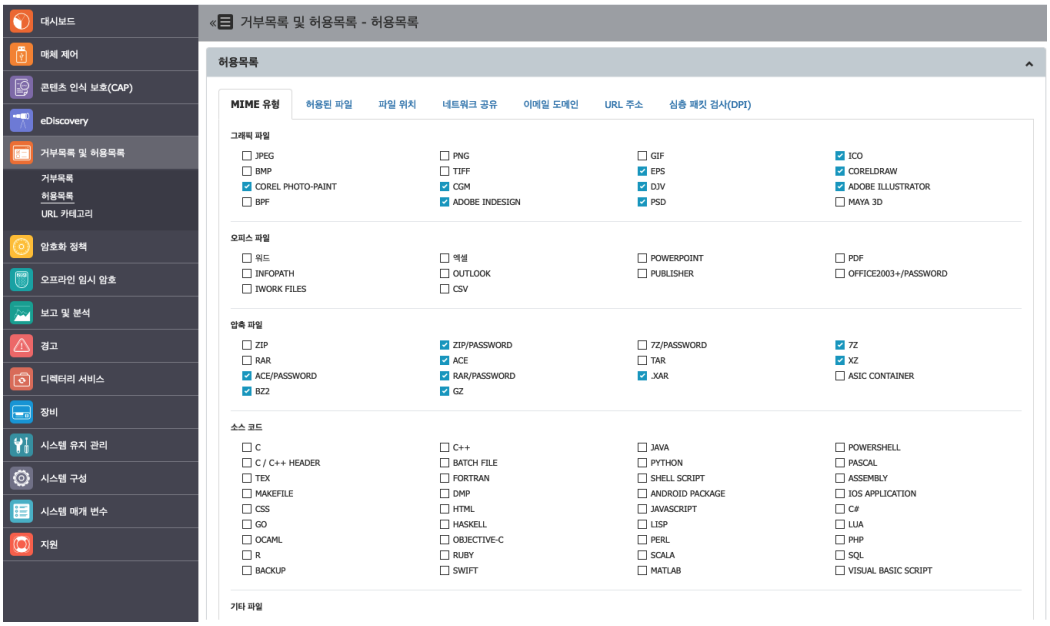
Endpoint Protector의 콘텐츠 탐지는 여러 파일 유형을 확인합니다. 일부 파일 (예: Word, Excel, PDF 등)은 기밀 정보 (예: 개인정보, SSN, 신용카드 등)를 포함할 수 있는 반면에 다른 파일 (예: .dll, .exe, .mp3, .avi 등)은 이러한 기밀 정보가 포함되지 않을 확률이 매우 높습니다.

MIME 유형 허용목록의 목적은 불필요한 파일 및 잉여 탐지 리소스를 제거하는 것 이외에 데이터 유출의 위험이 매우 낮은 파일의 메타 데이터 탐지 정보에 대한 오탐을 줄이는 것입니다.

예제: 음원 또는 비디오 파일은 신용카드번호 목록을 포할 수 없어서 콘텐츠 필터 사용으로 이러한 파일을 탐지하는 것은 불필요합니다.

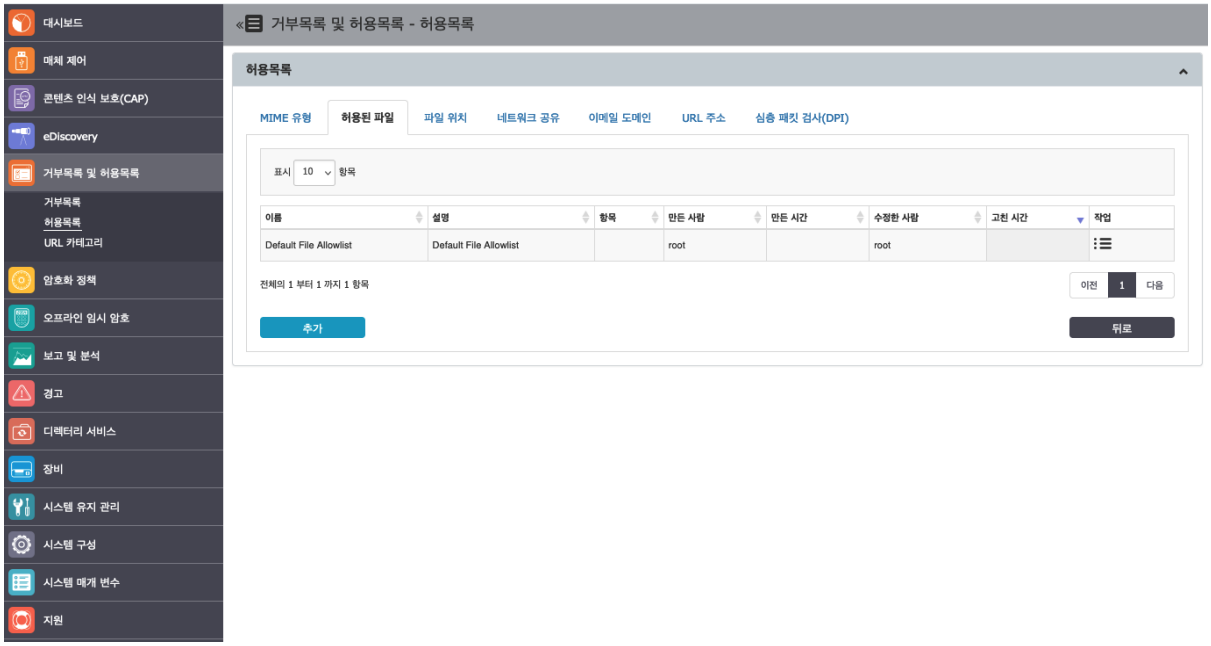
MIME 유형 허용목록은 콘텐츠 인식 보호(CAP)와 eDiscovery 모듈에서 모두 사용할 수 있습니다. 사용자 키워드, 미리 정의된 콘텐츠, 정규식에 적용합니다.

참고: 기본으로 그래픽 파일, 미디어 파일, 암호로 보호된 압축 파일, 일부 시스템 파일은 자동으로 MIME 유형 허용목록에 정의되어 있습니다. 쉽게 변경이 가능하지만 시스템 사용자가 사용하는 전송 데이터 종류, 시스템에서 사용자의 저장, Endpoint Protector 서버에서 로그 증가에 관련된 깊은 이해를 가진 후에 변경하시기를 권장합니다.



8.2.2. 허용된 파일

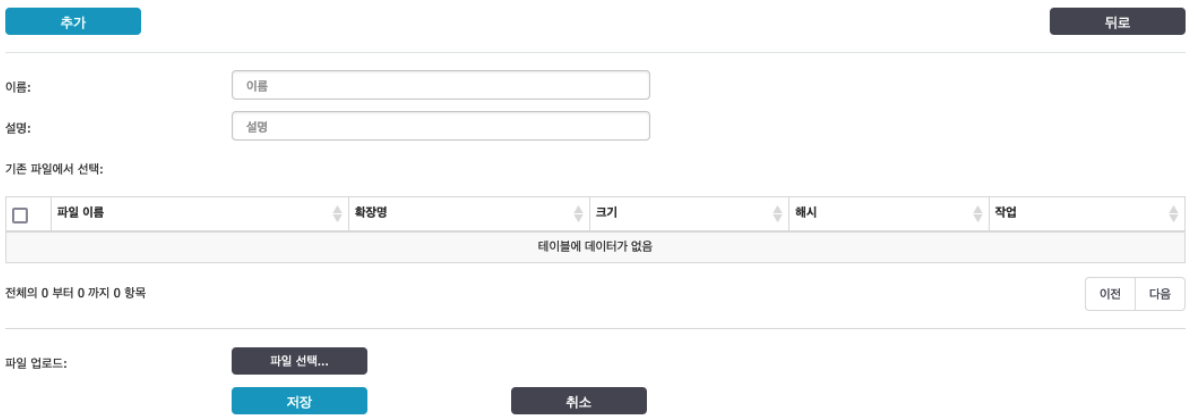
허용된 파일 허용목록은 Endpoint Protector의 민감한 콘텐츠 탐지에서 제외되는 사용자 정의 파일 그룹입니다. 콘텐츠 인식 보호(CAP)와 eDiscovery 모듈에서 모두 사용 가능합니다.



작업 컬럼에서 새로운 허용목록을 추가, 수정, 삭제할 수 있습니다.

새로운 허용목록을 만들기 위해서 가능한 허용목록에서 **추가**를 클릭하고 **이름**과 **설명**을 입력합니다. 목록에서 파일을 선택하거나 여러 허용목록에서 사용할 수 있는 새로운 파일을 업로드합니다.

허용목록을 만들면 허용된 파일 목록에 표시되고 콘텐츠 인식 보호(CAP) 또는 eDiscovery 정책을 만들거나 수정할 때 사용할 수 있습니다.



8.2.3. 파일 위치

파일 위치 허용목록은 Endpoint Protector로 식별되는 사용자 정의 위치 목록입니다. 이 위치의 파일 전송은 다양한 정책의 콘텐츠 검사 규칙 또는 허용에 관계없이 자동으로 허용됩니다.

파일 위치 허용목록은 콘텐츠 인식 보호(CAP)와 eDiscovery 모듈 모두에서 사용할 수 있습니다.

파일 위치 허용목록에 하위 폴더 포함 옵션 사용은 시스템을 통한 모든 다른 파일 위치 거부목록 및 허용목록에 영향을 줍니다. 기본적으로 파일 위치 거부목록은 특정 폴더에 위치한 모든 파일 뿐만 아니라 서브 폴더가 포함된 다른 파일에도 적용됩니다.

중요: 파일 위치 허용목록을 정의하는 것 이외에도 파일 전송에 사용되는 브라우저 또는 응용프로그램 또한 콘텐츠 인식 보호 정책에서 선택되어야 합니다.

파일 위치 허용 목록에서 와일드카드 매칭을 특정하는 와일드카드 패턴을 사용할 수 있습니다.

Windows에서 Desktop 폴더 매칭은 다음 패턴을 사용합니다 – "**?:₩Users₩*₩Desktop₩**".

파일 위치에 대한 와일드 카드 사용 예제

와일드 카드 유형	파일 위치	매칭된 결과	매칭되지 않은 결과
암시적	₩₩file-share₩public	₩₩file-share₩public₩jdoe₩file.txt ₩₩file-share₩public₩user512₩file2.txt	₩₩file-share₩c$₩file.txt ₩₩file-server₩puclic₩jdoe₩file.txt
명시적	₩₩*₩public₩*	₩₩localhost₩public₩payslip.xlsx ₩₩192.168.20.2₩public₩Windows₩system32₩notepad.exe	₩₩localhost₩c$₩system32₩notepad.exe C:₩Windows.old₩system32₩notepad.exe

작업 컬럼에서 새로운 허용목록을 추가, 수정, 삭제할 수 있습니다.

새로운 허용목록을 만들기 위해서 가능한 허용목록에서 **추가**를 클릭하고 **이름**과 **설명**을 입력합니다. 목록에서 파일을 선택하거나 여러 허용목록에서 사용할 수 있는 새로운 파일을 업로드합니다. **그룹**과 **컴퓨터**를 선택합니다.

파일 위치 허용목록은 사용자 그룹에는 적용되지 않고 컴퓨터 그룹에만 적용됩니다. 파일 위치 허용목록은 15분 후에 선택된 컴퓨터 그룹에서만 적용됩니다.

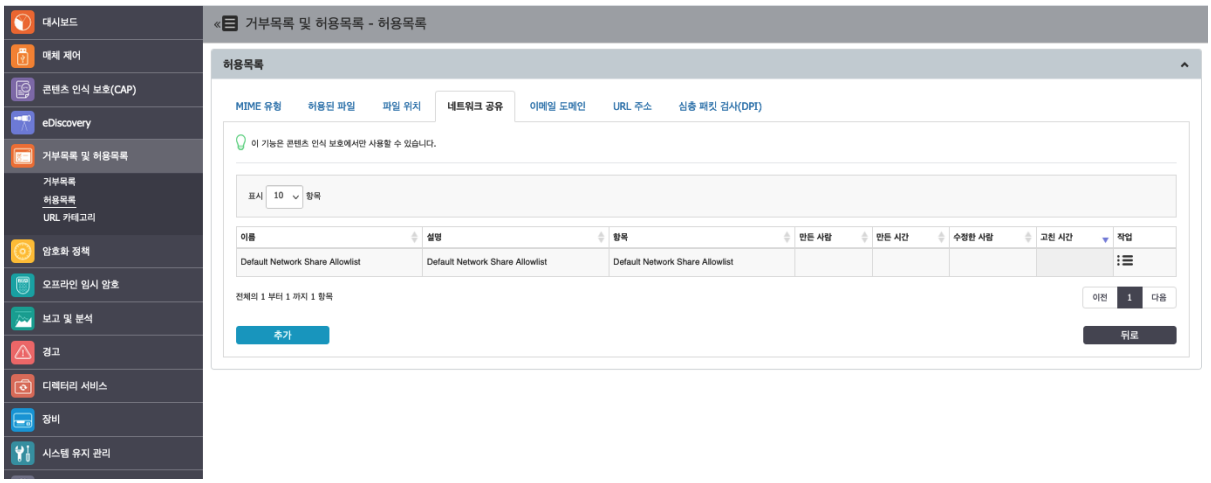
8.2.4. 네트워크 공유

네트워크 공유 허용목록은 기밀 정보의 전송이 Endpoint Protector에서 허용되는 사용자 정의 네트워크 공유 주소 목록입니다.

참고: 네트워크 공유 허용목록은 콘텐츠 인식 보호(CAP) 모듈에서만 사용 가능합니다.

와일드카드 매칭을 특정하기 위해서 네트워크 공유 허용목록에서 와일드카드 패턴을 사용할 수 있습니다. 네트워크 공유 허용목록은 전체 파일 이름 뿐만 아니라 와일드카드 패턴을 사용했을 때 디렉토리 이름에서 매칭을 수행 할 수 있습니다.

중요: 네트워크 공유는 매체 제어에서 사용 허용이 설정되어 있어야 하고 콘텐츠 인식 보호(CAP) 정책에서 네트워크 공유 스캔이 체크되어 있어야 합니다.

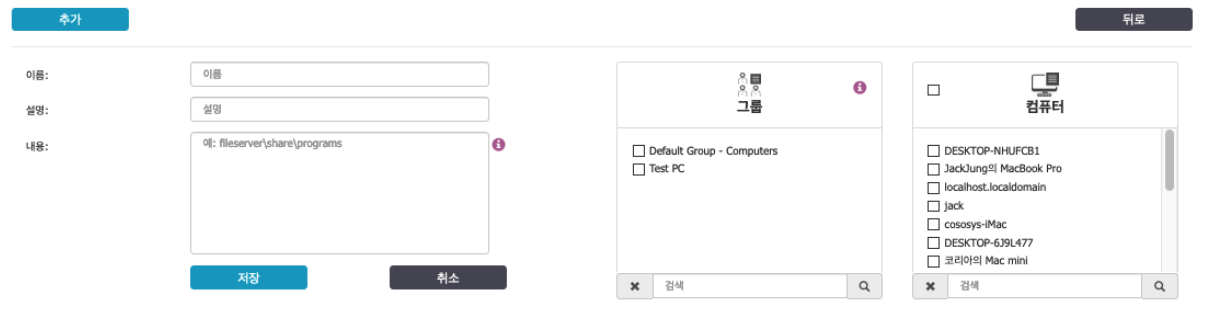


작업 컬럼에서 새로운 허용목록을 수정, 삭제 할 수 있습니다.

새로운 허용목록을 만들기 위해서 가능한 허용목록에서 **추가**를 클릭하고 **이름**과 **설명**을 입력합니다. 줄 바꿈, 쉼표, 세미 콜론으로 구분된 네트워크 공유 경로를 정의하기 위해서 서버 이름 또는 IP 주소를 추가합니다. **그룹**과 **컴퓨터**를 선택합니다.

네트워크 공유 허용목록은 사용자 그룹에는 적용되지 않고 컴퓨터 그룹에만 적용됩니다. 네트워크 공유 허용목록은 15분 후에 선택된 컴퓨터 그룹에서만 적용됩니다.

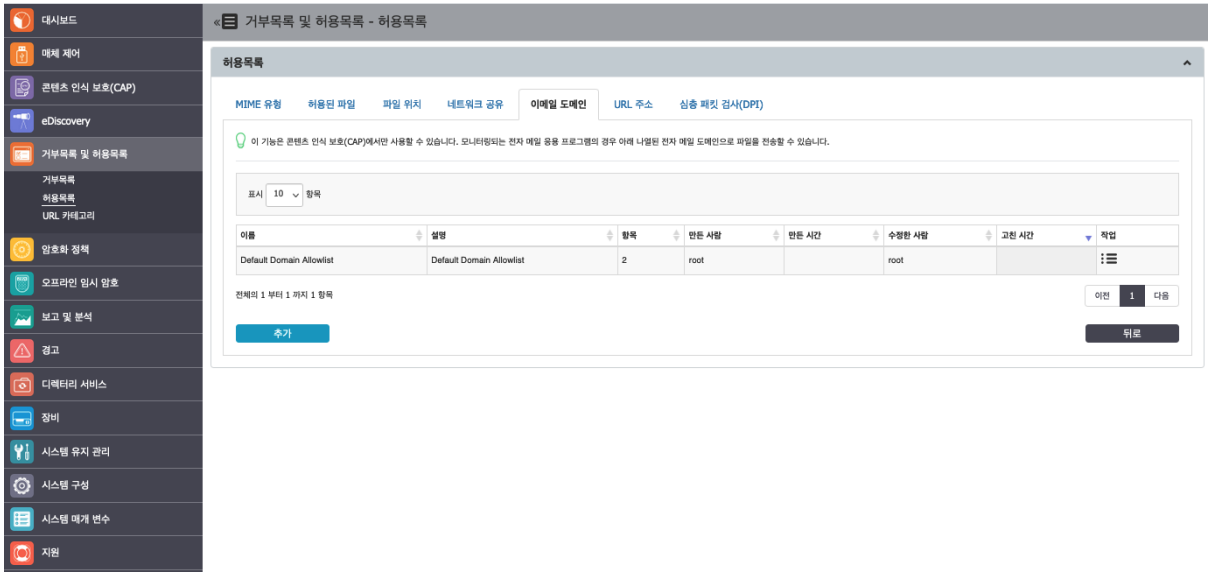
중요: 네트워크 공유 경로에 백슬래쉬(₩₩)를 입력하지 마시기 바랍니다 – 192.168.0.1₩public₩users₩test; fileserver₩documents₩example



8.2.5. 이메일 도메인

이메일 도메인 허용목록은 Endpoint Protector로 기밀 정보가 보내지는 것을 허용하는 사용자 정의 이메일 주소입니다.

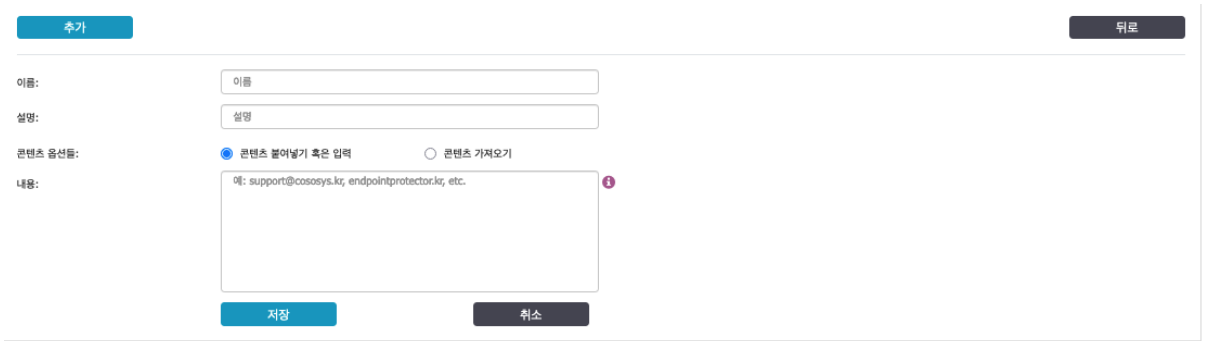
참고: 이메일 도메인 허용목록은 콘텐츠 인식 보호(CAP) 모듈에서만 사용 가능합니다.



작업 컬럼에서 허용목록의 수정, 삭제, 내보내기가 가능합니다.

새로운 허용목록을 만들기 위해서 가능한 허용목록에서 **추가**를 클릭하고 **이름**과 **설명**을 입력합니다. 목록은 줄 바꿈, 쉼표, 세미 콜론으로 구분되고 적어도 3자 이상을 **콘텐츠 붙여넣기 혹은 입력** 합니다. 폼에서 제공되는 **샘플 파일**을 사용하여 **콘텐츠 가져오기**를 할 수 있습니다.

허용목록을 만들면 이메일 도메인 목록이 표시되고 콘텐츠 인식 보호(CAP) 정책을 만들거나 수정할 때 사용할 수 있습니다.

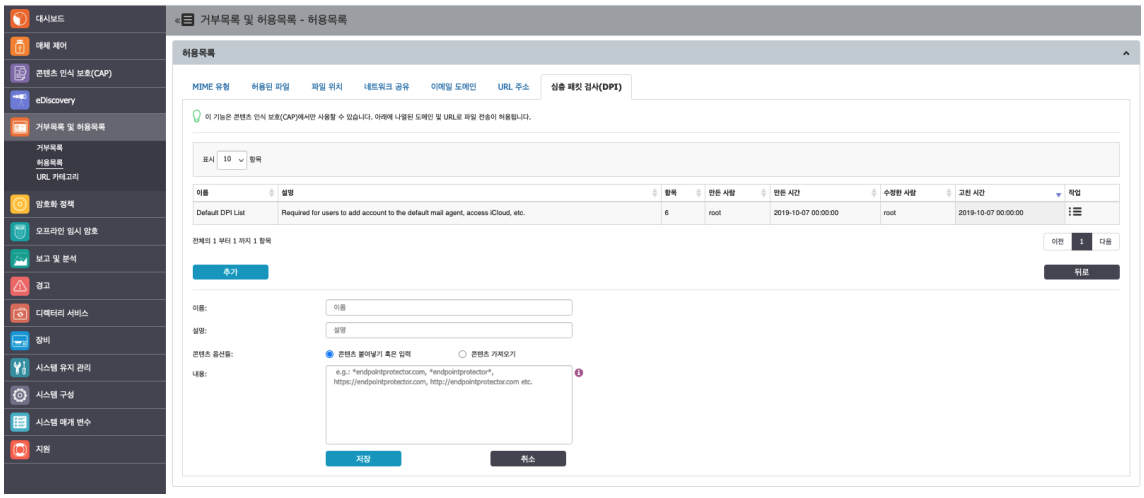


와일드카드 매칭을 특정하기 위해서 이메일 도메인에서 와일드카드 패턴을 사용할 수 있습니다. 아래를 참조하시기 바랍니다.

이메일 도메인의 와일드카드 사용 예제		
이메일 도메인 이름	**매치된 결과**	**매치되지 않는 결과**
@epp.com	robert@epp.com jdoe@epp.com jacmes@epp.com.ca	sara@eep.com jeff@ccs.com

8.2.6. 심층 패킷 검사(DPI)

심층 패킷 검사(DPI) 허용목록은 Endpoint Protector가 허용하는 기밀 정보 업로드의 사용자 정의 웹 주소 목록입니다.



작업 컬럼에서 허용목록의 수정, 삭제, 내보내기가 가능합니다.

목록을 100개까지 만들거나 가져올 수 있고 각 목록은 50,000개의 웹 도메인까지 구성할 수 있습니다.

참고: 100개의 웹 도메인으로 구성된 목록은 편집할 수 있지만 더 많은 도메인이 포함되어 있으면 다시 가져와야 합니다.

새로운 허용목록을 만들기 위해서 가능한 허용목록에서 **추가**를 클릭하고 **이름**과 **설명**을 입력합니다. 목록은 줄 바꿈, 쉼표, 세미 콜론으로 구분되고 적어도 3자 이상을 **콘텐츠 붙여넣기 혹은 입**

력 합니다. 폼에서 제공되는 **샘플 파일**을 사용하여 **콘텐츠 가져오기**를 할 수 있습니다.

허용목록이 한 번 만들어지면 URL 주소 목록에 표시되고 콘텐츠 인식 보호 정책이 만들어지거나 수정될 때 사용할 수 있습니다.

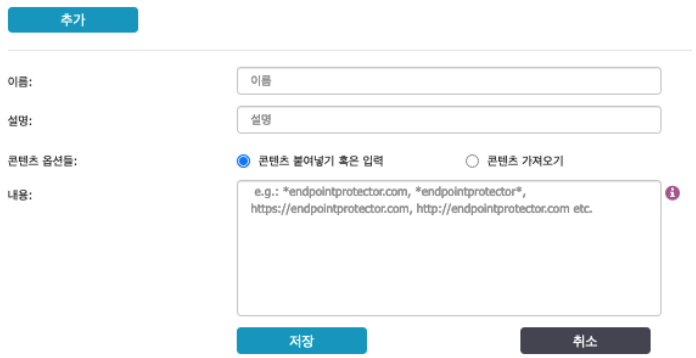
예: example.endpointprotector, *example.com, *example*, https://website.com 등

중요: "?" 는 문자를 대체할 수 없습니다.

참고: Gmail 사용으로 아래 사항을 고려하시기 바랍니다.

- 이메일 첨부 또는 파일의 드래그 앤 드롭 옵션 사용을 위해서 **mail.googl.com**을 허용해야 합니다.
- 이메일 본문에 이미지 추가를 위해 **doc.google.com**을 허용해야 합니다.

허용목록이 만들어지면 심층 패킷 검사(DPI) 목록에 표시되고 콘텐츠 인식 보호 정책을 만들거나 수정할 때 사용할 수 있습니다.



심층 패킷 검사(DPI)의 와일드카드 사용 예제		
도메인 이름	**매치된 결과**	**매치되지 않는 결과**

box.com	box.com	sub.box.com box1.com
***.box.com**	sub.box.com bad.box.com	fakebox.com mybox.com
box.*.com	box.co.com box.bad.com	sub.box.co.com box1.co.com box.co.uk
box.com.*	box.com.co box.com.us	sub.box.com.us box1.com.us
https://cisco.com	https://cisco.com/drives/downloads/ http://cisco.com/drives/downloads/ ftp://cisco.com/drives/downloads	https://sub.cisco.com/drives/downloads/ https://cisco.com.ca/downloads/
https://cisco.com*	https://cisco.com.ca/downloads/ http://cisco.com.ca/downloads/	https://subcisco.com.ca/downloads/ https://bad.cisco.com/downloads/

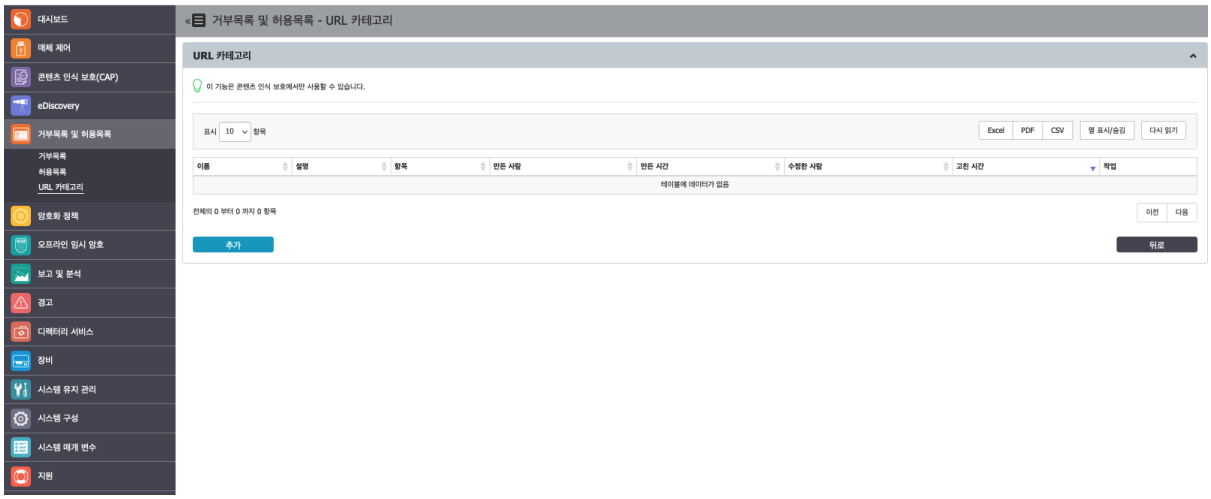
참고: 와일드카드 사용은 도메인 이름을 검색하지만 URL은 검색하지 않습니다.

8.3. URL 카테고리

URL 카테고리는 웹 트래픽을 모니터링하는 심층 패킷 검사(DPI)를 제한하기 위해 콘텐츠 인식 정책을 설정할 수 있는 사용자 정의 웹 주소 목록입니다. 정책에 심층 패킷 검사(DPI)로 모니터링되는 URL 카테고리가 설정되어 있지 않으면 Endpoint Protector 클라이언트는 기본값으로 모든 웹 주소를 모니터링합니다.

중요: URL 카테고리는 심층 패킷 검사(DPI)을 사용할 때만 적용이 됩니다.

URL 카테고리 기반으로 차단된 콘텐츠는 브라우저가 아닌 URL 기반으로 차단하기 때문에 보안 위반 요소가 있습니다. 정책은 새로운 카테고리가 발견되면 항상 업데이트가 필요합니다.



작업 컬럼에서 허용목록의 수정, 삭제, 내보내기가 가능합니다.

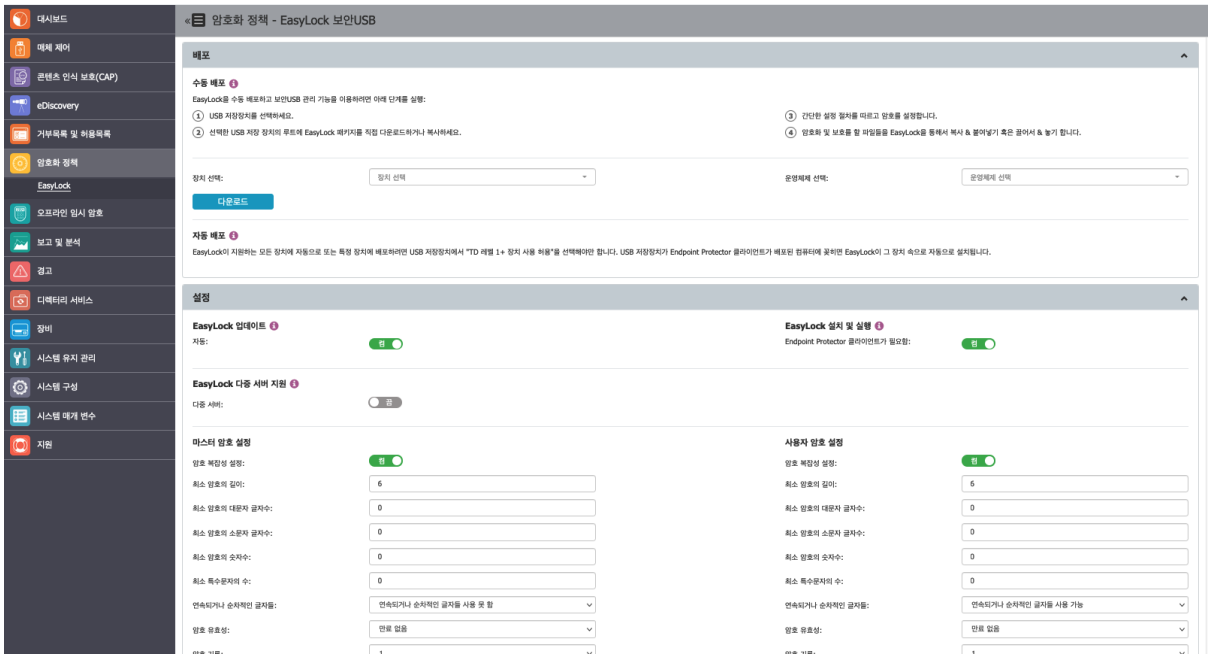
새로운 허용목록을 만들기 위해서 가능한 허용목록에서 **추가**를 클릭하고 **이름**과 **설명**을 입력합니다. 목록은 줄 바꿈, 쉼표, 세미 콜론으로 구분되고 적어도 3자 이상을 **콘텐츠 붙여넣기 혹은 입력** 합니다. 폼에서 제공되는 **샘플 파일**을 사용하여 **콘텐츠 가져오기**를 할 수 있습니다.

URL 카테고리가 한 번 만들어지면 URL 카테고리 목록에 표시되고 콘텐츠 인식 보호 정책을 만들거나 수정할 때 사용할 수 있습니다.

9. 암호화 정책

9.1. 암호화 정책[1]

EasyLock은 정부 승인 256bit AES CBC 모드 암호화로 데이터를 보호하는 크로스 플랫폼 솔루션입니다. USB 장치 용으로 root 디렉토리에 배포가 필요합니다. 직관적인 드래그 앤 드롭 인터페이스로 파일을 빠르게 장치에 암호화 및 복호화 할 수 있습니다.



참고: EasyLock 자체 사용에 대한 더 자세한 정보는 EasyLock 사용자 매뉴얼을 참조하시기 바랍니다.

Endpoint Protector와 함께 사용되는 EasyLock은 TD레벨 1으로 식별되는 USB 저장 장치를 허용합니다. 이는 보호되는 컴퓨터에서 USB 암호화 정책이 사용되는 것을 보장할 수 있습니다. 장치에 저장된 데이터 접근은 사용자가 설정한 패스워드 또는 Endpoint Protector 관리자가 설정한 마스터 패스워드를 통해서 가능합니다. 암호화된 데이터는 복호화 후에만 모든 사용자가 열 수 있습

니다. 그러므로 사용자에게 EasyLock 밖으로 정보 복사를 위해 요청합니다.

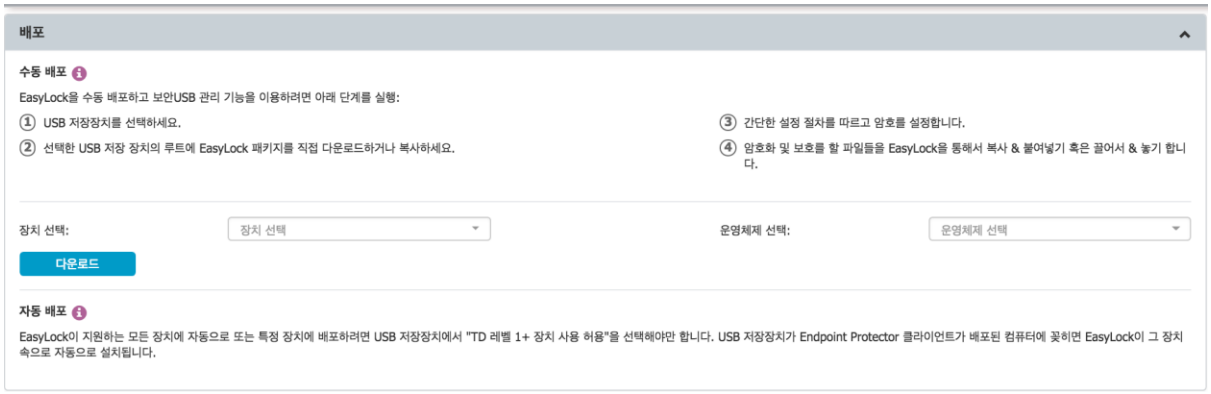
중요: EasyLock은 수정 또는 데이터 삭제를 예방하는 쓰기 보호 메커니즘을 가진 장치와 호환되지 않습니다. 쓰기 보호 메커니즘은 하드웨어 구성 (예: USB 장치의 스위치) 또는 소프트웨어 구성을 사용해서 실행할 수 있습니다.

참고: Endpoint Protector는 TD 레벨 1으로 식별되는 모든 EasyLock 암호화 장치를 탐지할 수 있습니다. 암호화 정책 사용을 위해서는 특정 EasyLock 버전을 사용해야 합니다. 이 기능은 Endpoint Protector 사용자 인터페이스에서 사용할 수 있습니다.

Windows에서 구성된 EasyLock, 장치가 Windows에서 포맷되었거나 일부 파일이 Windows에서 암호화되면 EasyLock은 읽기 전용 모드로 동작합니다. macOS에서 EasyLock과 호환이 되지 않는 NTFS를 제외하고 이러한 파일은 복호화 될 수 있습니다.

9.1.1. 암호화 정책 배포

EasyLock 암호화 정책은 Mac과 Windows 컴퓨터를 모두 지원합니다.



보호되는 컴퓨터에 매체 제어 권한에서 USB 저장 장치를 "**TD 레벨 1+이면 사용 허용**" 으로 설정하고 USB 저장 장치를 연결하면 자동으로 EasyLock이 배포됩니다. 이것은 "매체 제어 > 전체 권한"에서 확인 하거나 위의 이미지에서 제공하는 링크를 통해서 확인합니다.

수동 배포 또한 가능합니다. 이 섹션에서 Windows 및 macOS의 다운로드 사용이 가능합니다. 다운로드한 EasyLock 파일을 원하는 USB 저장 장치의 root 디렉토리에 복사 후 실행하면 됩니다.

수동 배포에 대한 보안 기능의 확장으로 새로운 USB 저장 장치에 EasyLock을 사용하려면 Endpoint Protector 인터페이스에서 다시 다운로드 받아야 합니다.

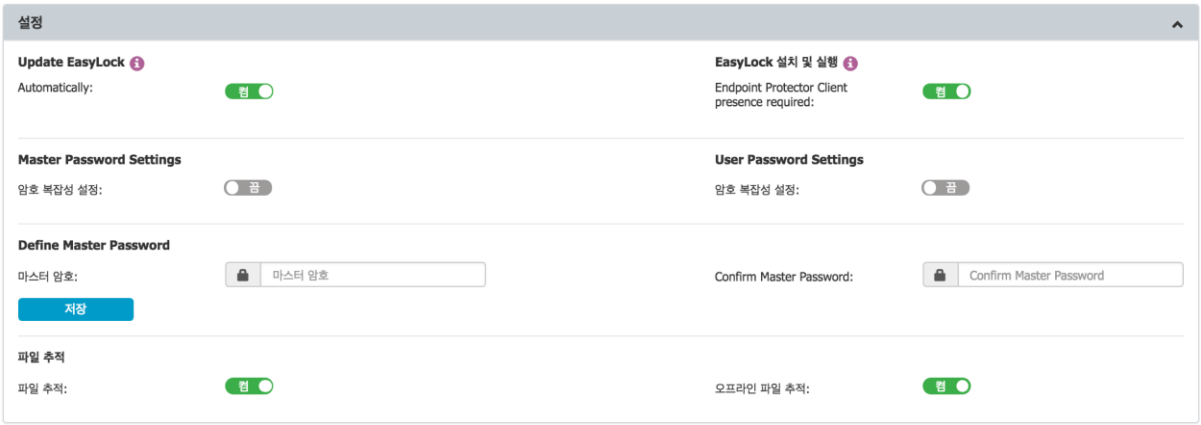
참고: Endpoint Protector 5.2.0.0 버전부터 수동 EasyLock 배포는 장치가 사용 허용으로 되어 있으면 클라이언트에 암호화 장치에 해당하는 작은 아이콘을 클릭해서 사용자가 설치할 수 있습니다 (TD 레벨 1+ 이면 사용 허용).

두 가지 방법은 모두 배포가 간단하고 사용자는 암호만 설정하면 됩니다.

참고: Mac에서 여러 파티션을 가진 USB 저장 장치는 EasyLock 및 TD 레벨 1이 지원하지 않습니다.

9.1.2. 암호화 정책 설정

이 섹션에서 관리자는 원격으로 EasyLock 암호화 장치를 관리합니다. 이 기능을 이용하기 전에 관리자는 마스터 암호를 설정해야 합니다.

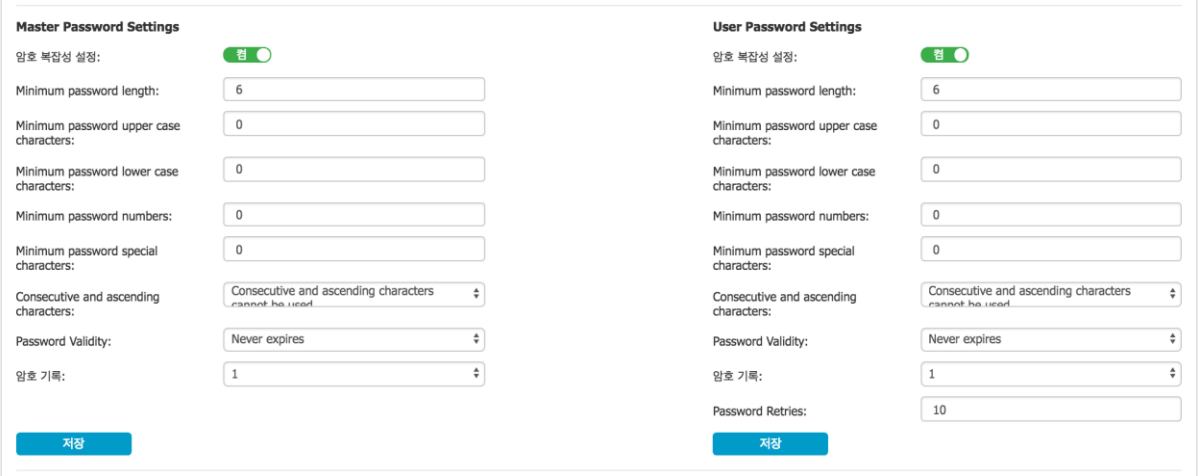


EasyLock이 Endpoint Protector 클라이언트가 설치된 컴퓨터에서만 실행할 수 있도록 설정이 가능합니다.

EasyLock 멀티 서버 기능으로 신뢰할 수 있는 다른 Endpoint Protector 서버 클라이언트가 설치된 컴퓨터에서 사용할 수 있도록 확장이 가능합니다

이 **설정** 섹션에서 **마스터 암호**, EasyLock 파일 추적 사용 이외에 Endpoint Protector 클라이언트가 설치된 컴퓨터에서만 EasyLock이 설치 및 실행되는 정의 구성이 가능합니다.

마스터 암호와 사용자 암호의 복잡성을 설정할 수 있습니다. 암호 길이, 최소 문자, 유효성, 기록 및 기타 설정을 할 수 있습니다.



Endpoint Protector는 EasyLock을 사용하는 휴대용 장치에 복사되고 암호화된 파일을 추적합니다. 이 옵션은 이 설정 창에서 활성화 시킬 수 있습니다.

파일 추적 옵션을 체크해서 EasyLock을 사용하는 장치로 전송된 모든 데이터가 기록되고 차후 감사를 위한 로그가 됩니다. 로그 정보는 Endpoint Protector 클라이언트가 컴퓨터에 설치되어 있으면 Endpoint Protector 서버로 자동으로 보냅니다. 이 액션은 파일 추적 옵션 사용에 관계없이 일어나고 매체 제어 모듈을 통해서 특정 컴퓨터에서만 해당되는 것은 아닙니다.

Endpoint Protector 클라이언트가 없는 경우에 정보는 로컬 장치의 암호화 포맷에 저장되고 후에 Endpoint Protector 클라이언트가 설치된 다른 컴퓨터에 연결되면 보냅니다.

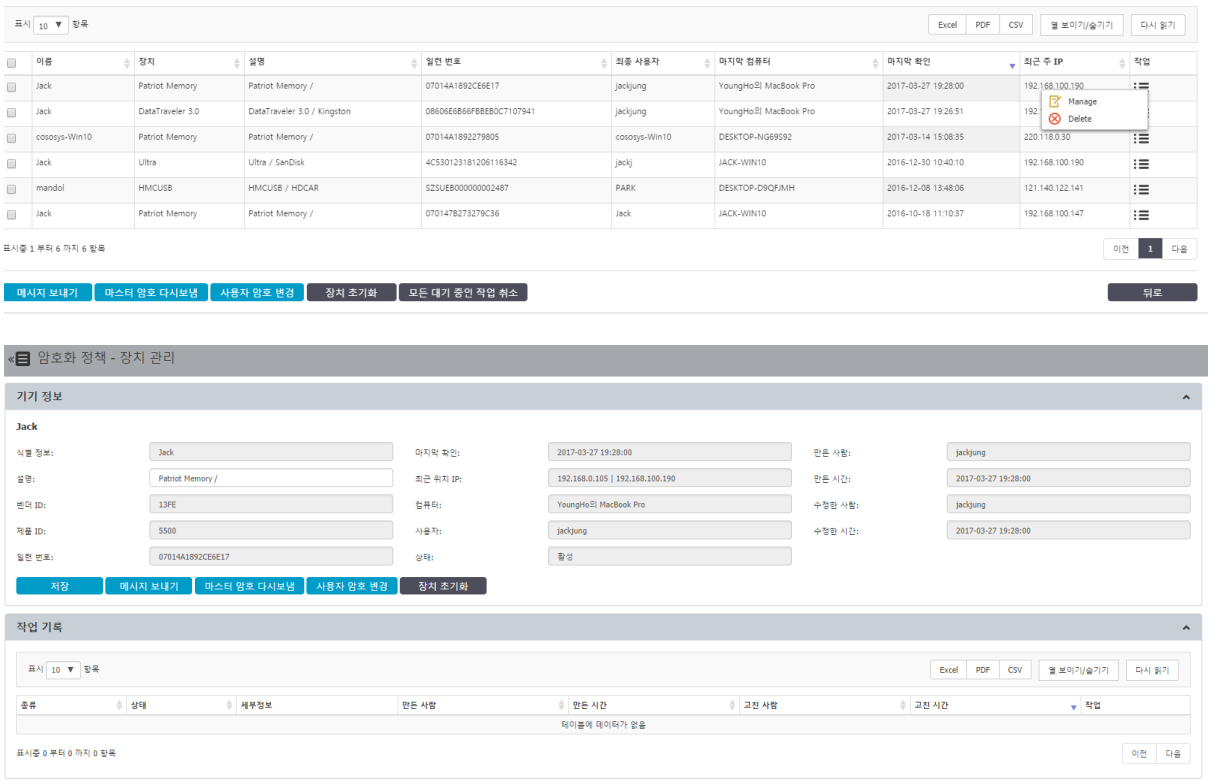
"오프라인 파일 추적"은 위 옵션의 확장입니다. Endpoint Protector 서버로 보내기 전에 바로 장치에 정보를 저장합니다. 복사된 파일 목록은 장치가 Endpoint Protector 서버와 통신하는 Endpoint Protector 클라이언트가 있는 컴퓨터에 연결되었을 때 보냅니다.

EasyLock은 파일 사본 보관 옵션이 사용 가능으로 설정된 Endpoint Protector 클라이언트가 있는 컴퓨터에서 파일을 전송할 때 사본 보관 기능을 지원합니다. 이벤트는 매체 제어 모듈을 통해서 일어납니다. 이것은 실시간 이벤트이고 사본 보관 정보는 장치에 저장되지 않습니다.

참고: 전체 설정에서 파일 추적 사용은 자동으로 EasyLock 파일 추적 기능을 활성화하지 않고 그 반대도 동일합니다.

9.1.3. 암호화 정책 클라이언트

클라이언트 목록에서 모든 EasyLock 사용 장치를 볼 수 있습니다. 메시지 보내기, 마스터 암호 다시 보내기, 사용자 암호 변경, 장치 초기화, 모든 대기 중인 작업 취소 등의 작업을 수행할 수 있습니다. 작업 열에서 관리를 클릭하면 클라이언트에 보낸 작업 기록을 확인할 수 있습니다.



9.1.4. TD (Trusted Devices)

이동 데이터를 보호는 장치가 분실 또는 도난 당한 경우에 제 3자가 데이터에 접근하지 못하게 보장하는 것이 필수적입니다. 암호화 정책 솔루션은 관리자에게 분실 또는 도난 당한 경우에 기밀 데이터를 보호할 수 있는 가능성을 제공합니다. Endpoint Protector가 설치된 컴퓨터에서 사용할 수 있는 암호화 장치인 TD (Trusted Devices) 이용하여 해결할 수 있습니다. TD는 반드시 Endpoint Protector 서버에 인가를 받아야 합니다. 그렇지 않으면 무용지물입니다. TD 보안의 4가

지 레벨이 있습니다:

- **레벨 1** – 데이터 보안에 대해서 소프트웨어 기반의 암호화에 중점을 둔 오피스와 개인 사용을 위한 최소한의 보안입니다. 모든 USB 저장 장치와 대부분의 휴대용 장치를 TD 레벨 1로 변환할 수 있습니다. 특정한 하드웨어가 필요하지는 않지만 EasyLock과 같은 암호화 솔루션이 필요합니다.
- **레벨 2** – 생체 데이터 보호 또는 고급 소프트웨어 기반 데이터 암호화를 사용한 중간 보안 레벨입니다. 보안 소프트웨어가 포함된 특별한 하드웨어가 필요하고 TD 레벨2에 대한 테스트가 되어야 합니다.
- **레벨 3** – SOX, HIPAA, GBLA, PIPED, Basel II, DPA, PCI 95/46/EC와 같은 규정 준수 의무호에 대한 강력한 하드웨어 기반의 암호화를 가진 높은 보안 레벨입니다. 고급 보안 소프트웨어와 TD 레벨3에 대한 테스트가 된 하드웨어 기반 암호화가 포함된 특별한 하드웨어가 필요합니다.
- **레벨 4** – 군대 및 정부에서 사용하는 최고 보안입니다. TD 레벨 4는 데이터 보호를 위한 강력한 하드웨어 기반 암호화가 포함되고 독립적인 인증이 되어야 합니다 (예: FIPS 140). 이러한 장치는 소프트웨어와 하드웨어에 대한 엄격한 테스트가 성공적으로 수행되어야 합니다. 보안에 중점을 둔 리셀러를 통해서 우선적으로 사용할 수 있는 특별한 하드웨어가 필요합니다.
- **레벨 1+** - 레벨 1에서 파생된 레벨로 Endpoint Protector 클라이언트가 설치된 컴퓨터에 USB 저장 장치를 연결하면 자동으로 마스터 비밀번호를 가진 EasyLock 2가 배포됩니다.

참고: TD 레벨 1을 사용하고 TD 레벨 2, 3, 4가 연결되면 권한은 다음에 따라 적용됩니다.

아래 표는 TD 목록을 제공합니다:

장치 이름	TD 레벨
EasyLock 암호화 장치	1
AT1177	2
UT169	2
UT176	2
Trek ThumbDrive	2
BitLocker Encrypted devices	3
FileVault Encrypted devices	3
Buffalo Secure Lock	3

CTWO SafeXs	3
Integral Crypto	3
Integral Crypto Dual	3
Integral Courier Dual	3
IronKey Secure Drive	3
iStorage datAshur	3
Kanguru Bio Drive	3
Kanguru Defender	3
Kanguru Elite (30, 200 & 300)	3
Kanguru Defender Elite	3
Kingston Data Traveler Locker+	3
Lexar 1 (Locked I Device)	3
Lexar Gemalto	3
SaferZone Token	3
ScanDisk Enterprise	3
Verbatim Professional	3
Verbatim Secure Data	3
Verbatim V-Secure	3
iStorage datAshur Pro	4
Kanguru Defender (2000 & 3000)	4
SafeStick BE	4
Stealth MXP Bio	4

10. 오프라인 임시 암호

이 섹션은 관리자가 오프라인 임시 암호 (OTP)를 만들고 임시적으로 접근 권한을 얻을 수 있습니다. 임시 접근 권한이 필요한 상황에서 보호되는 컴퓨터와 Endpoint Protector 서버 사이에 연결 네트워크가 없어도 또한 사용할 수 있습니다. 오프라인 임시 암호는 다음의 객체에서 설정이 가능합니다.

오프라인 임시 암호는 아래 엔터티에 대해서 만들어 질 수 있습니다:

- **장치** (특정 장치)
- **컴퓨터 및 사용자** (모든 장치)
- **컴퓨터 및 사용자** (모든 파일 전송)

암호는 접근 허용 기간과 연결되고 컴퓨터의 특정 장치마다 하나씩 부여됩니다. 이것은 같은 암호로 다른 장치 또는 컴퓨터에서 사용할 수 없습니다. 또한 두 번 사용할 수 없습니다 (범용 오프라인 임시 암호는 제외).

암호는 일정 기간동안 장치, 컴퓨터 또는 민감한 자료 전송 사용을 허용합니다. 시간 간격은 30분, 1시간, 2시간, 4시간, 8시간, 1일, 2일, 5일, 14일, 30일 또는 사용자가 지정으로 선택할 수 있습니다.

관리자는 암호를 만든 이유 설명을 추가하는 옵션을 가집니다. 이것은 후에 감사 목적 또는 전체 현황에 사용할 수 있습니다.

오프라인 임시 암호 기간은 사용자 정의 옵션을 제공합니다. '시작 날짜/시간'과 '종료 날짜/시간'을 사용해서 OTP 코드를 만들 수 있습니다.

다른 시간 대의 엔드포인트를 관리를 위해서 대기업 또는 다국적 기업은 Endpoint Protector의 서

버 시간 및 클라이언트 시간을 고려해야 합니다.

예: Endpoint Protector 서버가 독일에 있고 서버 시간은 UTC +01:00 입니다.

보호되는 엔드포인트는 루마니아에 위치해 있고 클라이언트 시간은 UTC +02:00 입니다.

엔드포인트 시간으로 내일 16:00에 적용되는 OTP 코드를 만들 때 서버에서 내일 15:00 으로 시간을 설정해야 합니다 (시간대가 1시간 차이가 있기 때문입니다.).

미리 정의된 기간에서는 위의 적용이 필요하지 않습니다. OTP 코드는 정해진 기간의 시간 만큼 유효합니다. 고려해야 할 점이 있다면 OTP 코드를 생성한 같은 날짜에만 적용됩니다.

참고: 범용 오프라인 임시 암호 기능 또한 사용할 수 있습니다. 이 기능을 사용하면 모든 장치 또는 파일 전송에 대해서 모든 사용자, 컴퓨터에서 보안 제한없이 1시간 동안 사용할 수 있습니다. 또한 모든 사용자에 대해서 여러 번 사용할 수 있습니다.

범용 오프라인 임시 암호는 최고 관리자에게만 보이게 할 수 있습니다. 이 설정을 사용하면 일반 및 오프라인 임시 암호 관리자에게는 보이지 않고 사용할 수도 없습니다. '시스템 구성 -> 시스템 설정 -> 사용자 설정' 에서 설정할 수 있습니다.

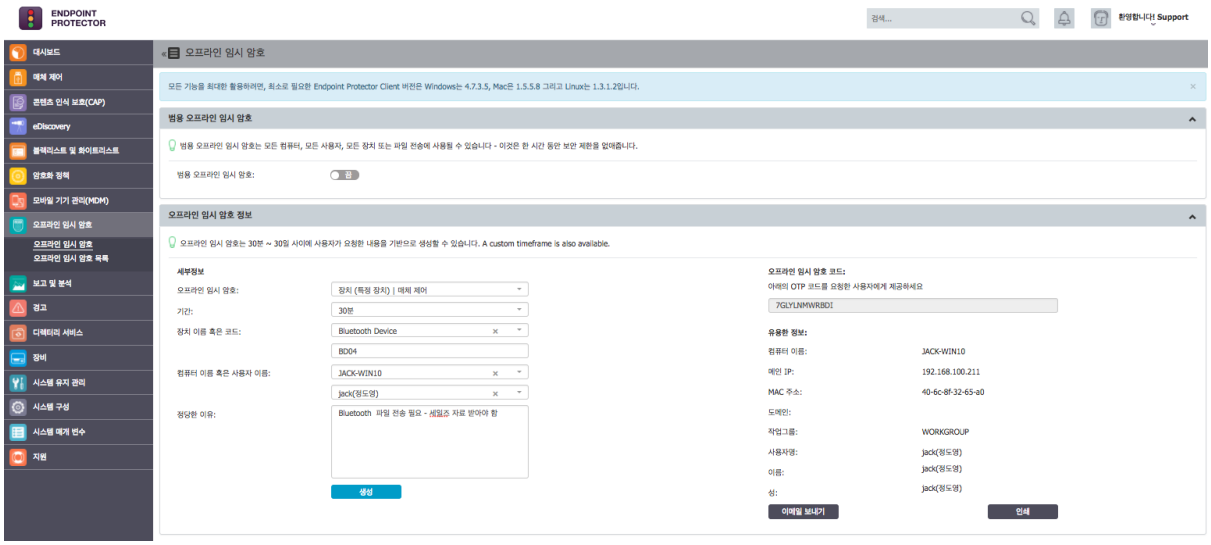
관리자는 추후에 감사를 위해서 각 오프라인 임시 암호에 정당한 이유를 추가할 수 있는 옵션을 가지고 있습니다. 즉 오프라인 임시 암호를 생성한 이유를 추가하는 것입니다.

한 번 오프라인 임시 암호를 인가하면 즉시 Endpoint Protector 서버에 저장된 설정 및 다른 권한의 효력이 사라집니다. 오프라인 임시 암호가 만료되면 다시 기존 설정 및 권한을 사용할 수 있습니다.

참고: 전송 제한 도달 오프라인 임시 암호는 전송 제한 도달 기능이 사용 중이거나 잠금으로 설정된 경우에만 사용이 가능합니다. 이 오프라인 임시 암호의 주요 목적은 전송 제한 도달 시간 주기가 만료되기 전에 서버-클라이언트 통신을 다시 연결하는 것입니다.

10.1. 오프라인 임시 암호 만들기

드롭다운 선택 메뉴 옵션으로 정확한 장치 또는 필요한 컴퓨터에 오프라인 임시 암호 (OTP)를 만들 수 있습니다.



장치에 대한 OTP를 만들 때 관리자는 사용자와 연락을 통해서 장치 코드를 받아서 입력하거나 Endpoint Protector 데이터베이스의 장치 검색을 위한 마법사를 사용할 수 있습니다. 오프라인 임시 암호를 설정하는 또 다른 방법은 매체 제어 > 컴퓨터 섹션의 액션 컬럼에서 오프라인 임시 암호 옵션을 선택하는 것입니다.

장치에 OTP 코드를 만들 때 장치 코드 또는 장치 이름을 입력해야 합니다. 이 중 하나는 자동으로 입력이 될 것입니다.

컴퓨터 이름과 사용자 이름 영역을 모두 채울 필요는 없습니다. 이 중 하나만 입력이 되어도 OTP 코드는 완벽하게 동작할 것입니다. 그러나 원하는 컴퓨터 사용자에 정확한 장치에 OTP 코드를 사용하려면 모든 관련 영역을 채울 필요가 있습니다.

OTP 코드를 생성하면 위의 이미지의 오른쪽과 같이 정보가 표시됩니다.

요청을 보낸 사람에게 이 코드를 전달해야 하기 때문에 Endpoint Protector는 이메일 또는 프린트 출력 두 가지 옵션을 제공합니다.

참고: 관리자 연락처 정보는 사용자에게 노출됩니다. 이것은 '시스템 구성 > 시스템 설정' 섹션에

서 변경할 수 있습니다. 여기에 주요 관리자 연락처를 입력하시면 됩니다.

특정 장치의 오프라인 임시 암호 생성과 똑같이 모든 장치 또는 모든 파일 전송에 대한 암호를 만들 때 컴퓨터 이름 및 사용자 이름 영역을 모두 채울 필요는 없습니다. OTP 코드는 둘 중 하나만 입력해도 완벽하게 동작합니다. 그러나 특정 컴퓨터의 특정 사용자의 장치에 OTP 코드를 만들 때 관련 영역이 모두 채워져야 합니다.

11. 보고 및 분석

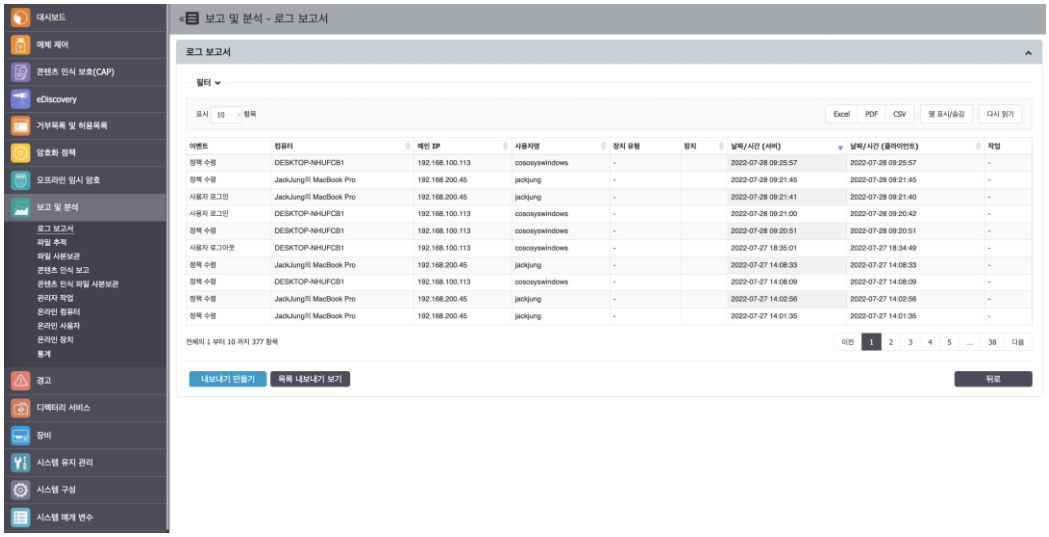
이 섹션은 관리자에게 시스템 로그, 매체 제어 로그 및 사본 보관, 콘텐츠 인식 보호 로그 및 사본 보관의 전체적인 정보를 제공합니다. 또한 권리자 액션, 통계 및 다른 유용한 정보를 이 섹션에서 찾을 수 있습니다.

eDiscovery 스캔 및 EasyLock 암호화 정책에 관련된 상세한 정보는 로그 및 분석 섹션에서 제공하지 않고 해당 섹션에서 찾을 수 있습니다.

추가적인 데이터 보안 조치로 이 섹션은 최고 관리자가 설정한 암호를 통해서 보호 할 수 있습니다. '시스템 구성 > 시스템 보안' 섹션에서 설정 할 수 있습니다. 시스템 보안에 대한 자세한 정보는 시스템 보안 챕터를 참조 하시기 바랍니다

11.1. 로그 보고서

이 섹션에는 관리자에게 시스템의 주요 로그 정보를 제공합니다. 사용자 로그인, 사용자 로그아웃, AD 가져오기, AD 동기화, 설치 삭제 시도 등 다양한 이벤트를 볼 수 있습니다. 매체 제어 로그를 이 섹션에서 확인 할 수 있습니다.



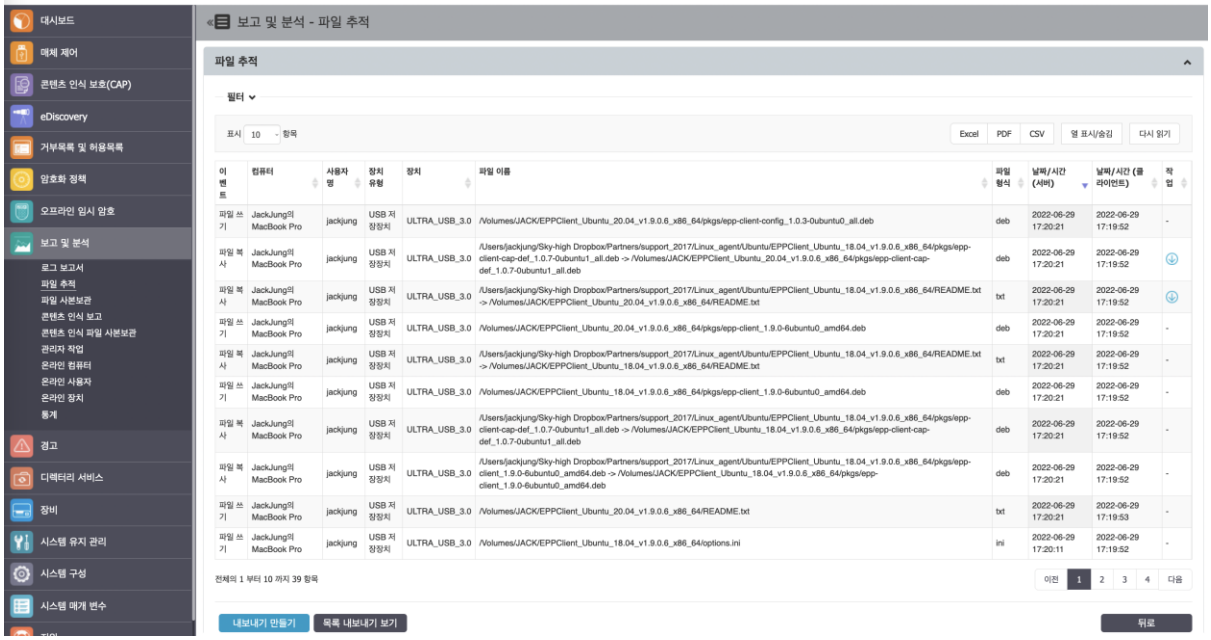
참고: 다른 로그 종류 보기와 분류를 위해 필터 옵션을 사용하고 결과 목록을 내보내기 할 수 있습니다.

11.2. 파일 추적

휴대용 장치 또는 네트워크에 있는 다른 컴퓨터로 클라이언트에서 전송 된 파일, 그 반대의 경우도 마찬가지로 파일들의 속성을 확인할 수 있습니다. 만약 복사 원본 감지 기능이 활성화 되어 있으면 파일의 원위치 또한 확인할 수 있습니다.

"파일 해시" 열을 보면 Endpoint Protector 응용프로그램은 파일 추적 기능이 적용된 대부분의 파일에 대해 MD5 해시 연산을 합니다. 이 방법으로 파일 내부의 콘텐츠 변경에 대한 위협을 완화할 수 있습니다.

관리자는 로그를 Excel, PDF 또는 CSV 파일로 내보내기 할 수 있습니다. 또는 전체 로그 보고서가 포함된 .CSV 파일로 만들어서 내보내기 할 수 있습니다.



11.2.1. 방향 별 파일 추적 이벤트

"방향 별 파일 추적 매트릭스" 표는 Endpoint Protector가 데이터 전송 방향에 따라 파일 추적 이벤트를 분류하는 방법을 이해하는데 유용한 참고 자료입니다. 이 표는 이벤트 처리에 대한 통찰력을 제공하고 사용자가 데이터 보호 정책의 효과적인 커스텀 설정에 도움이 됩니다. 로컬 전송을 추적하든 이동식 장치 및 네트워크 공유와 상호 작용을 추적하든 이 테이블은 명확한 개요를 제공합니다. 이 표는 강력한 보안과 규정 준수를 보장하는 Endpoint Protector 환경에서 데이터 보호 정책을 구성하는 필수적인 리소스입니다.

참고: 이 매트릭스는 5.9.0.0 릴리스 이후 버전의 클라이언트를 참조합니다.

이벤트의 자세한 내용은 아래 표를 참조하시기 바랍니다.

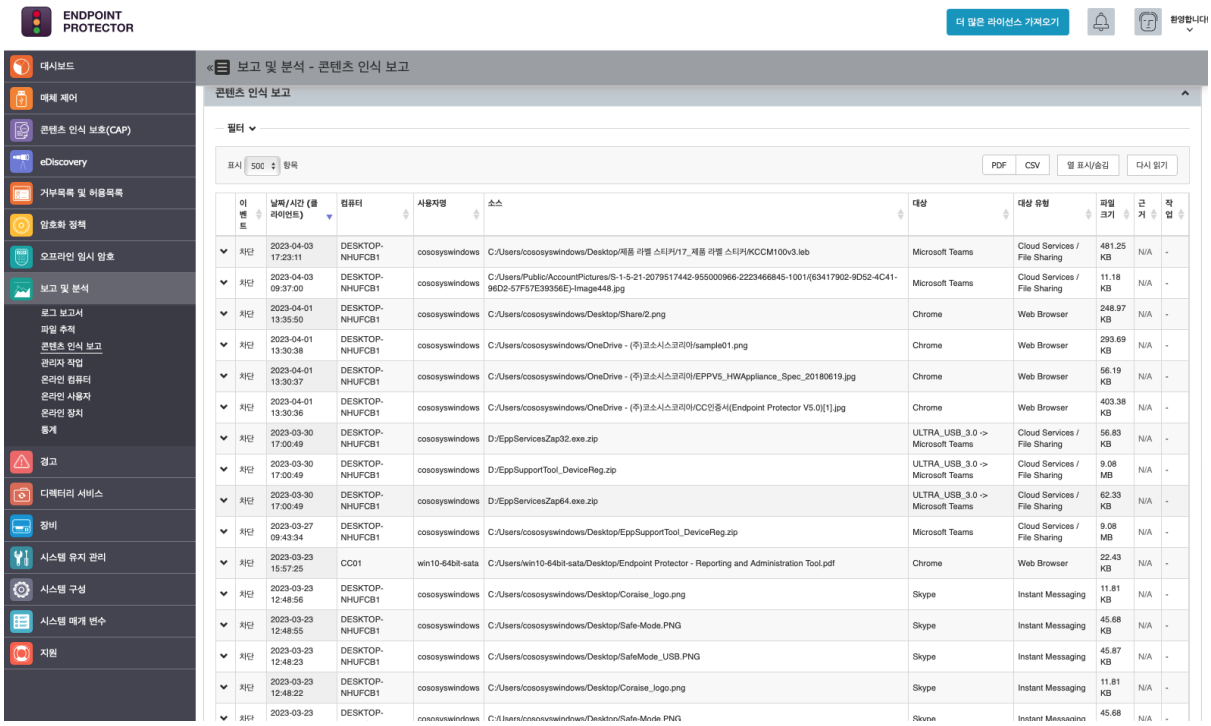
방향 별 파일 추적 이벤트 매트릭스			
방향	Windows	macOS	Linux
로컬 -> 로컬 (파티션 0)	N/A	N/A	N/A
로컬 -> 휴대용 장치	소스 및 목적지	소스 및 목적지	소스 및 목적지
로컬 -> 네트워크 공유	소스 및 목적지	소스 및 목적지	N/A
로컬 -> 파티션 1	소스 및 목적지	N/A	N/A
휴대용 장치 -> 로컬 (파티션 0)	소스 및 목적지	소스 및 목적지	소스 및 목적지
휴대용 장치 -> 휴대용 장치	소스 및 목적지	목적지	소스 및 목적지
휴대용 장치 -> 네트워크 공유	소스 및 목적지	목적지	N/A
휴대용 장치 -> 파티션 1	소스 및 목적지	소스 및 목적지	소스 및 목적지
네트워크 공유 -> 로컬 (파티션 0)	소스 및 목적지	소스 및 목적지	N/A
네트워크 공유 -> 휴대용 장치	소스 및 목적지	목적지	N/A
네트워크 공유 -> 네트워크 공유	소스 및 목적지	목적지	N/A
네트워크 공유 -> 파티션 1	소스 및 목적지	소스 및 목적지	N/A
파티션 1 -> 로컬 (파티션 0)	N/A	N/A	N/A
파티션 1 -> 휴대용 장치	소스 및 목적지	소스 및 목적지	소스 및 목적지
파티션 1 -> 네트워크 공유	소스 및 목적지	소스 및 목적지	N/A
파티션 1 -> 파티션 0	N/A	N/A	N/A

범례:

- *파티션 0 -> 부트 파티션 (OS)*
- *파티션 1 -> 2nd 파티션 (예: 2nd OS 또는 데이터 파티션)*

11.3. 콘텐츠 인식 보고

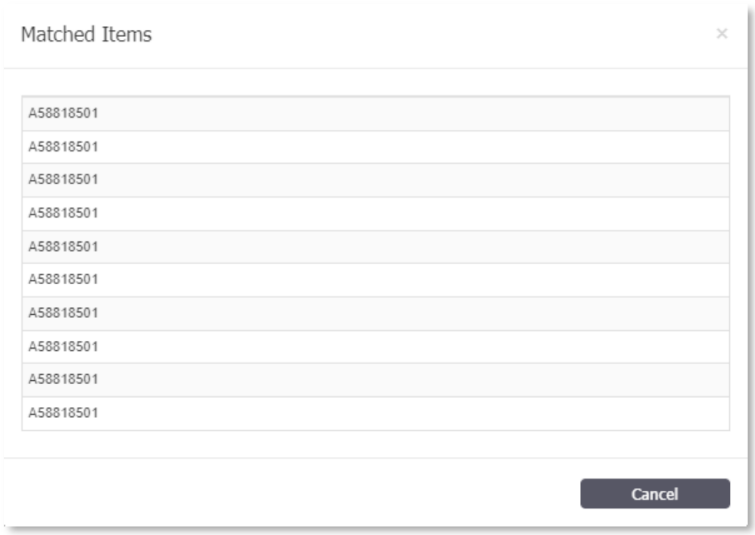
이 모듈은 모든 콘텐츠 인식 활동에 대한 상세 로그를 제공합니다. 언제 어떤 데이터 사고가 적용된 콘텐츠 인식 정책에 따라 탐지되었는지 관리자가 정확히 확인할 수 있습니다.



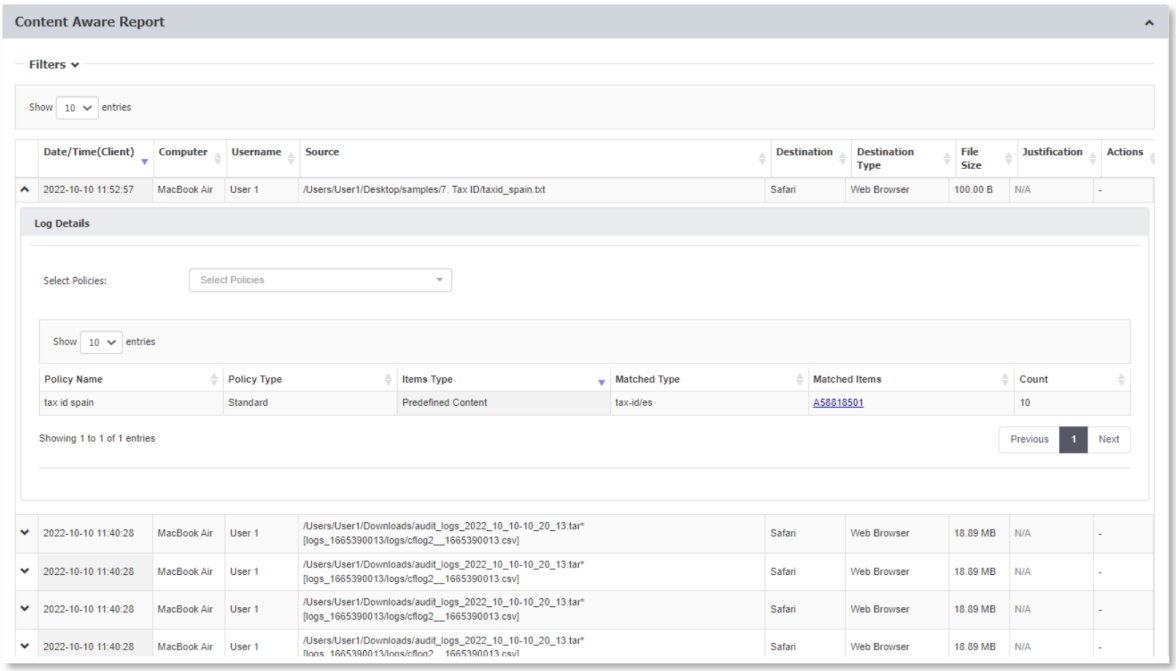
최신 Endpoint Protector 클라이언트를 사용할 때 스캔된 파일 당 구성된 자세한 로그를 볼 수 있습니다.

확장된 상세한 로그를 볼 수 있도록 아래 내용이 제공됩니다:

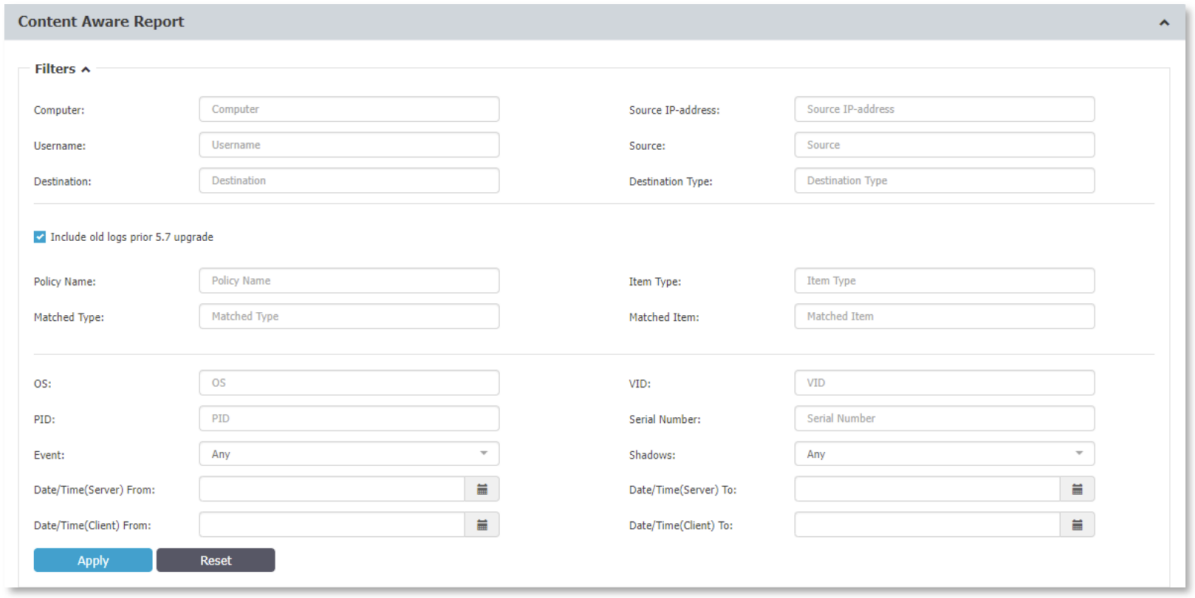
- **정책** – 드롭다운 목록에서 활성화된 정책 선택
- **정책 이름** – 선택된 정책 이름
- **정책 유형** – 선택된 정책 유형
- **아이템 유형** – 선택된 정책 거부목록 범주
- **일치된 유형** – 선택된 정책 거부목록 유형
- **일치된 아이템** – 일치된 아이템 목록에 팝업 윈도우를 볼 수 있도록 링크 클릭



- **카운트** – 일치된 아이템 숫자



필터 섹션에서 검색에 모든 로그가 포함되도록 필터 세션에서 **5.7 업그레이드 전에 이전 로그 포함** 옵션을 체크합니다. 이 옵션이 선택되지 않으면 필터는 새로운 로그만 적용됩니다.



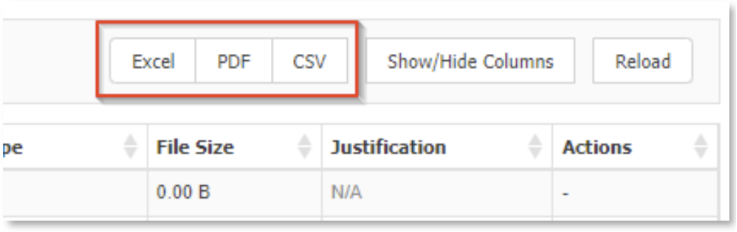
참고: Mac 사용자의 경우 Mac용 EPPClient에서 심층 패킷 검사(DPI) 기능이 활성화 된 경우 에이전트가 브라우저와 같이 모니터링되는 응용 프로그램을 통해 네트워크 공유에서 전송되는 파일의 전체 목적지 세부 정보를 제공하지 않는 특정 시나리오가 있을 수 있습니다. 이러한 경우 모니터링 프로세스에서 대상 정보가 완전히 캡쳐 되지 않을 수 있습니다.

참고: Linux 사용자의 경우 브라우저와 같이 DPI로 모니터링되는 응용 프로그램을 통해 네트워크 공유에서 파일이 전송되는 경우를 제외하고 EPPClient가 현재 네트워크 공유 가시성을 지원하지 않는다는 점에 유의해야 합니다. 다른 시나리오에서 네트워크 공유 가시성을 사용하지 못할 수도 있습니다.

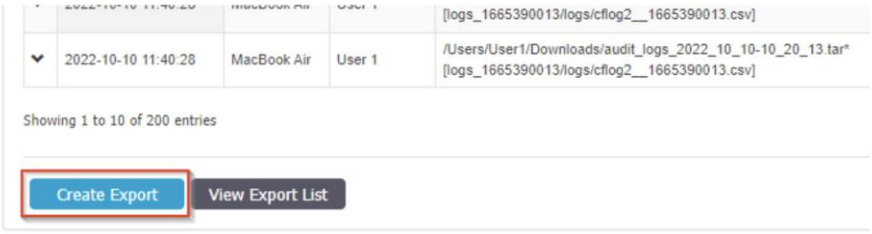
11.3.1. 콘텐츠 인식 보고 내보내기

Excel, PDF, CSV로 콘텐츠 인식 로그를 내보내기 하거나 CSV 또는 XLSX 파일로 전체 로그를 만들고 내보내기 할 수 있습니다.

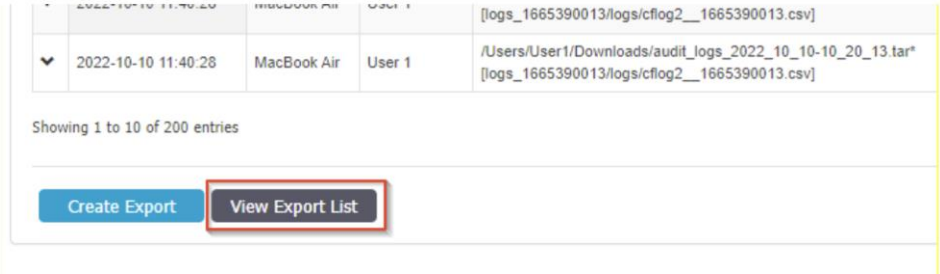
- **Excel/PDF/CSV** – 콘텐츠 인식 로그 목록 위에 위치해 있으며 기본 컬럼만 내보내기 합니다.

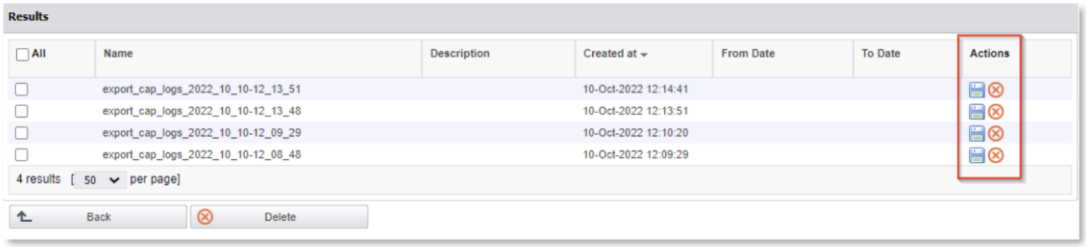


- **내보내기 만들기** – 콘텐츠 인식 보고 목록 아래에 위치해 있으며 정책 유형, 정책 이름, 아이템 유형, 일치된 유형, 일치된 아이템, 카운트 컬럼과 함께 확장된 로그 상세 섹션을 포함한 모든 데이터에 대한 내보내기를 만듭니다.



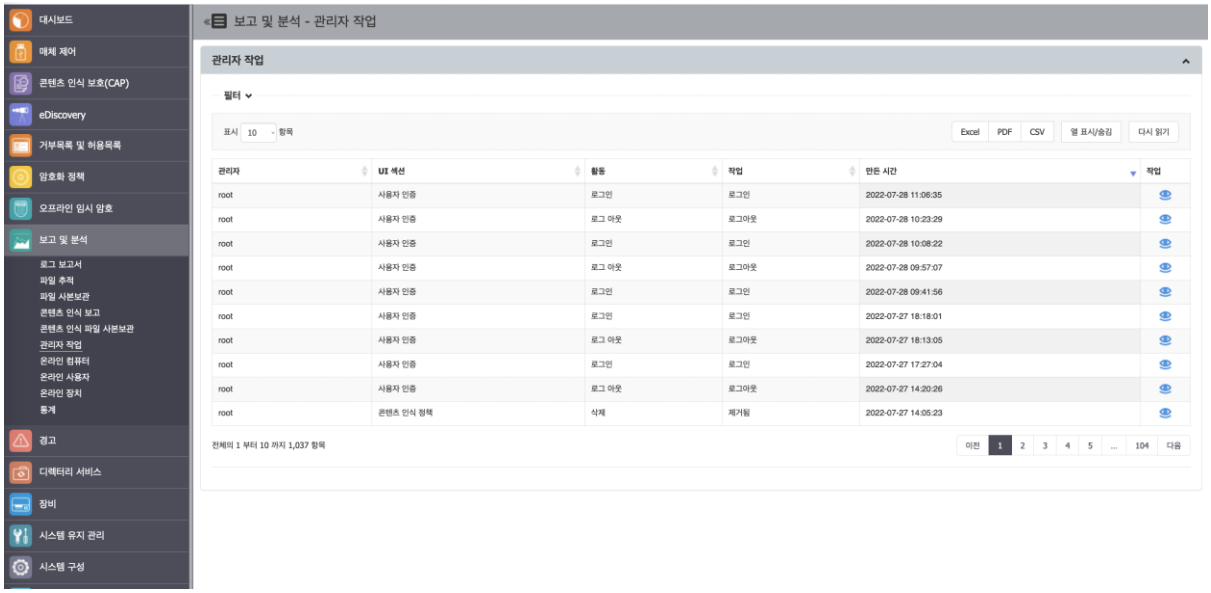
새로운 내보내기가 만들어지고 내보내기 목록을 사용할 수 있습니다 라는 메시지가 표시된 후에 **내보내기 목록 보기**를 클릭해서 보고 목록을 열면 보고서를 다운로드 또는 삭제할 수 있습니다.





11.4. 관리자 작업

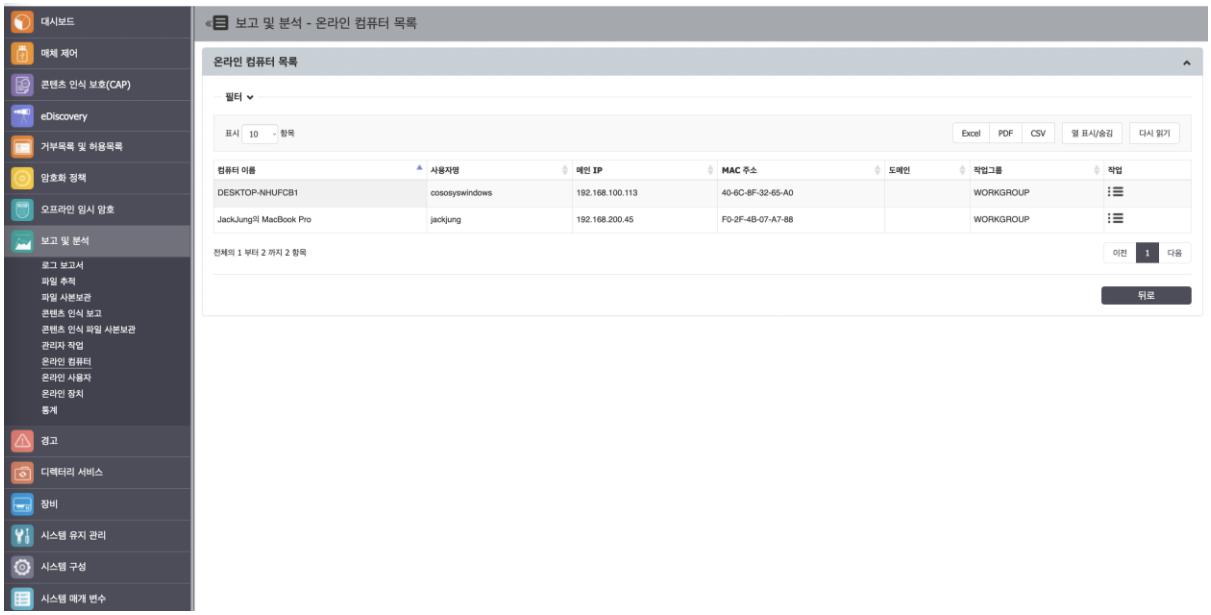
인터페이스에서 관리자가 수행하는 중요한 액션이 기록됩니다. "세부 정보 보기" 버튼을 클릭하면 특정 이벤트에 대해 더 자세한 정보를 보여주는 "관리자 액션 상세 정보" 페이지로 이동합니다.



11.5. 온라인 컴퓨터

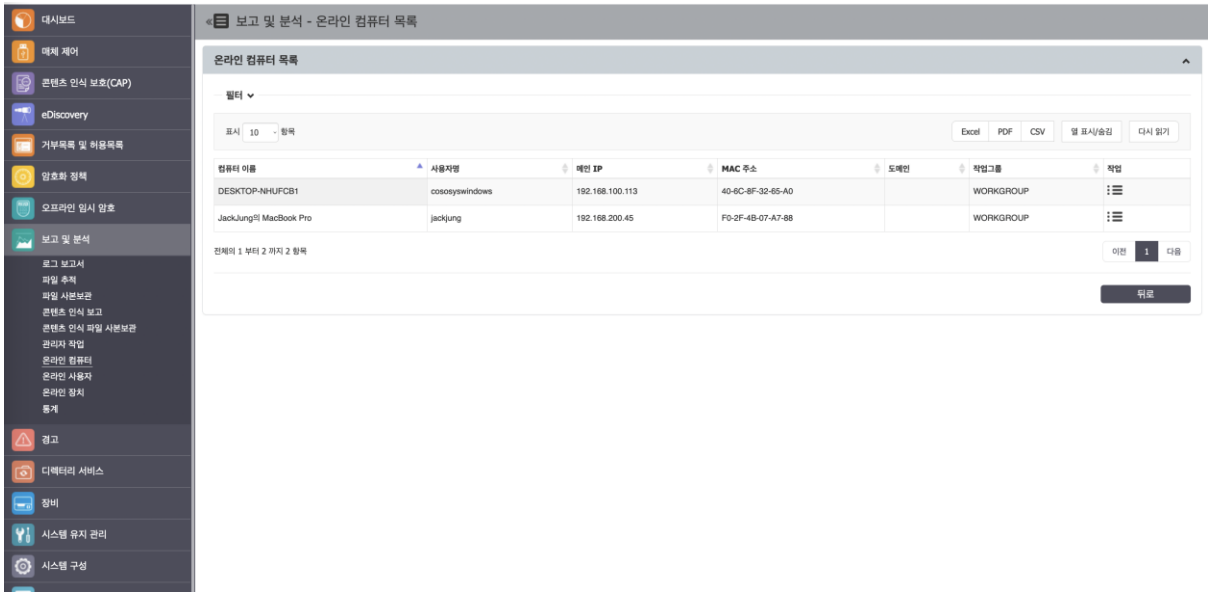
서버와 연결이 설정된 시스템에 등록된 클라이언트 컴퓨터를 모니터링할 수 있습니다.

컴퓨터 X의 새로 고침 간격이 1분이면 컴퓨터 X는 지난 1분 전에 서버와 통신 중이었습니다.



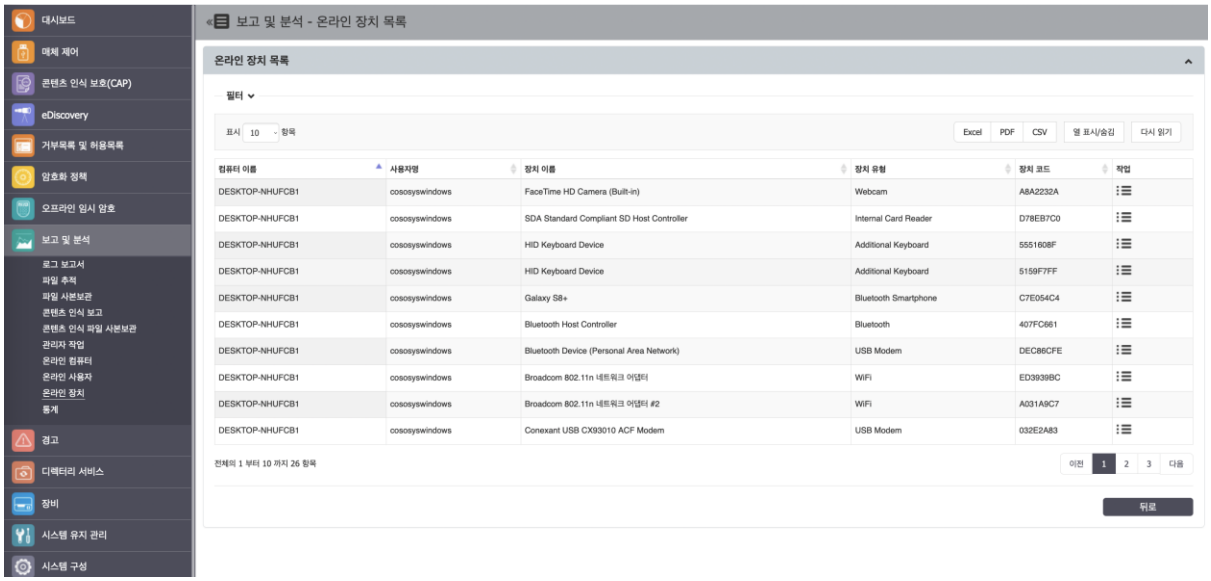
11.6. 온라인 사용자

이 섹션은 서버와 연결된 시스템에 등록된 사용자의 전체 보기를 제공합니다.



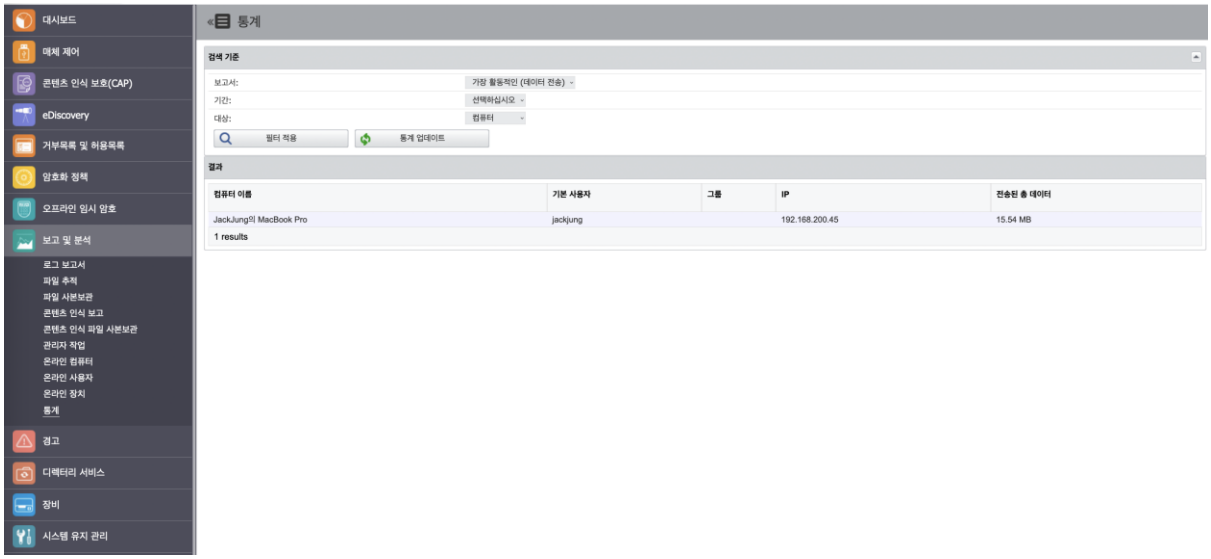
11.7. 온라인 장치

이 섹션은 서버와 연결된 시스템에 등록된 장치의 전체 보기를 제공합니다.



11.8. 통계

통계 모듈에서는 데이터 트래픽 및 장치 연결과 관련된 시스템 활동을 볼 수 있습니다. 통합 필터를 사용하여 쉽고 빠르게 보고서를 생성할 수 있습니다. 관심 분야를 선택한 다음 "필터 적용" 버튼을 클릭하기만 하면 됩니다.

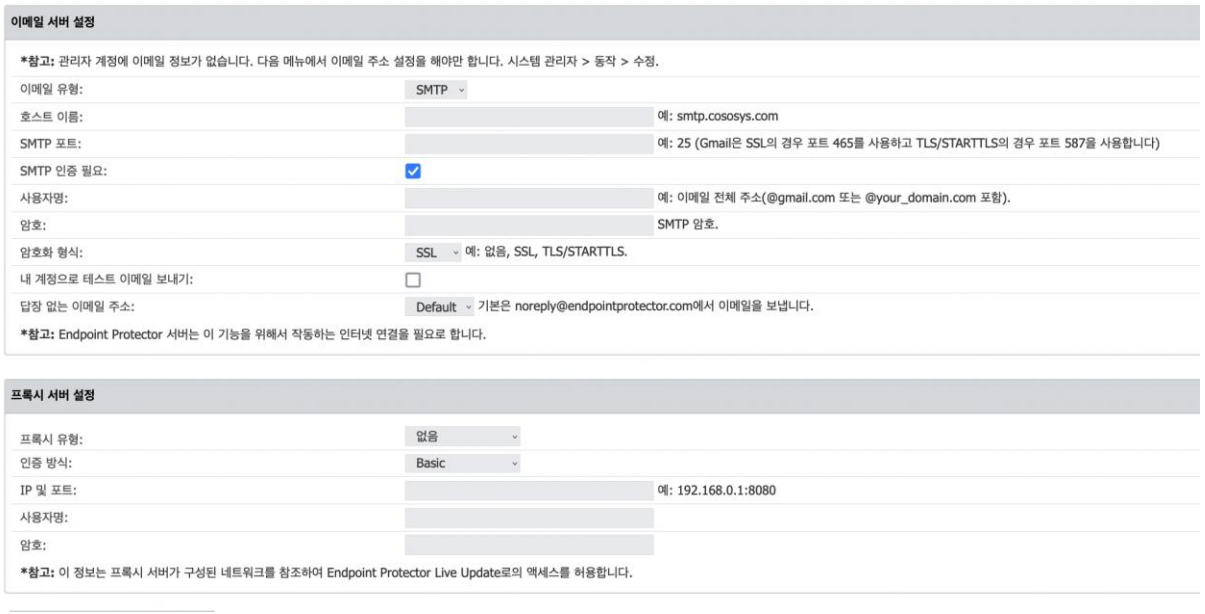


12. 경고

이 섹션에서 관리자는 Endpoint Protector가 탐지한 주요 이벤트의 이메일 경고를 정의할 수 있습니다. 시스템 경고, 매체 제어 경고, 콘텐츠 인식 경고, EasyLock 경고 및 모바일 기기 경고가 여기에 포함됩니다.

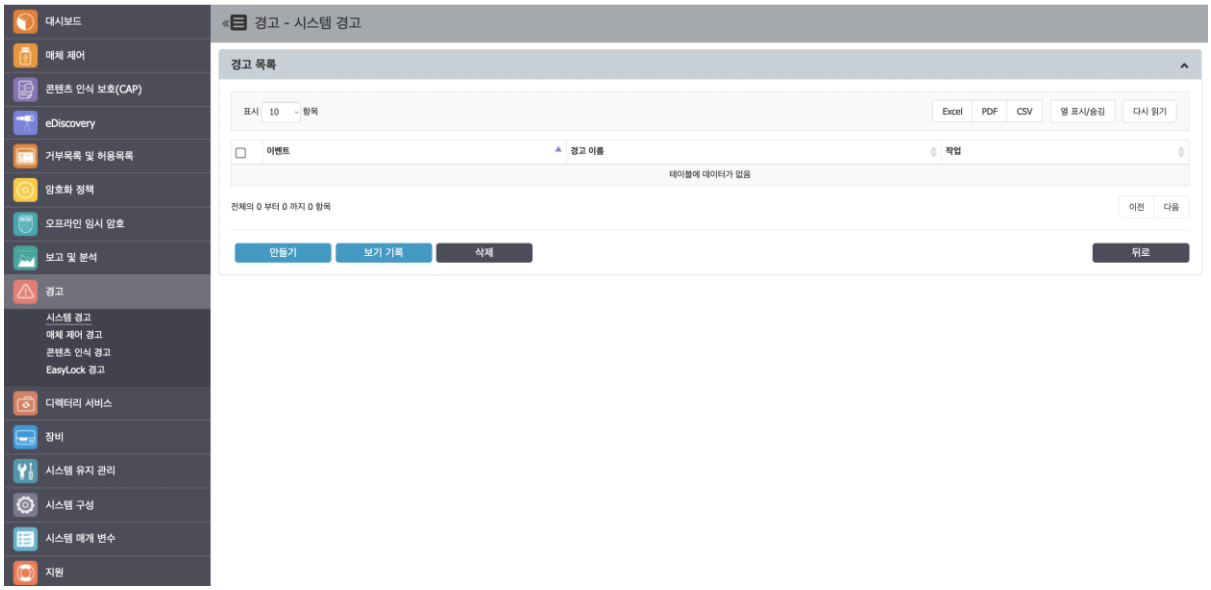
참고: 경고를 만들기 전에 Endpoint Protector 이메일 서버 세팅이 반드시 되어있어야 합니다. '시스템 구성 > 시스템 설정' 에서 확인 할 수 있습니다. 이 옵션을 확인하기 위해서 테스트 이메일 보내기를 할 수 있습니다.

경고 수신 목록에 각 관리자가 나타나려면 '시스템 구성 > 시스템 관리자' 섹션에 세부 정보를 입력해야 합니다.



12.1. 시스템 경고

이 섹션에서 APNS 인증서 만료, 업데이트 및 지원 만료, 엔드포인트 라이선스 등을 포함한 시스템 경고를 만들 수 있습니다.



12.1.1. 시스템 경고 만들기

시스템 경고를 새로 만들 때 아래 정보가 정의되어야 합니다.

1. **이벤트** – 경고를 만드는 이벤트 유형

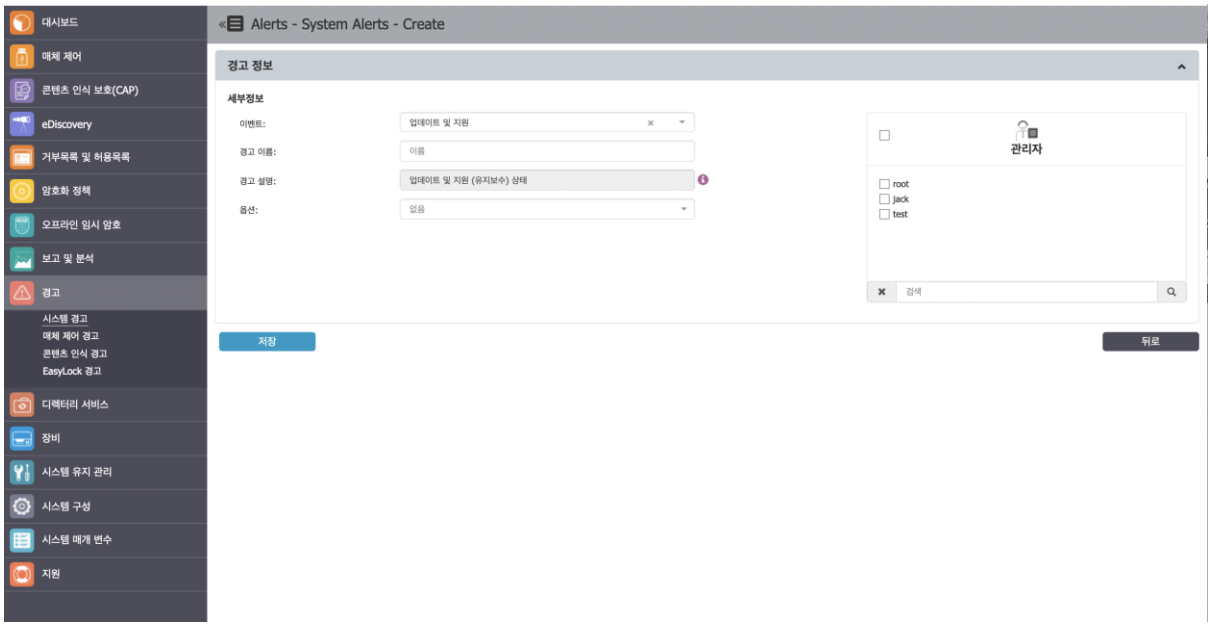
   - **업데이트 및 지원** – Endpoint Protector 어플라이언스가 최신 상태인지 확인하기 위해서 각각 모듈 유지보수 상태(매체 제어, 콘텐츠 인식 보호, 모바일 기기 관리)에 관련된 상기 메일을 보냅니다.

     참고: 업데이트 및 지원은 '대시보드 > 시스템 상태' 에서 사용하지 않음으로 변경 할 수 있습니다.

   - **엔드포인트 라이선스** – 각각의 네트워크는 보호받지 않는 엔드포인트의 위험을 없애기 위해 증가하고 경고를 생성합니다. 사용되고 있는 엔드포인트 라이선스가 70%, 80%, 90%에 도달하면 경고가 나가도록 정의되어 있습니다.

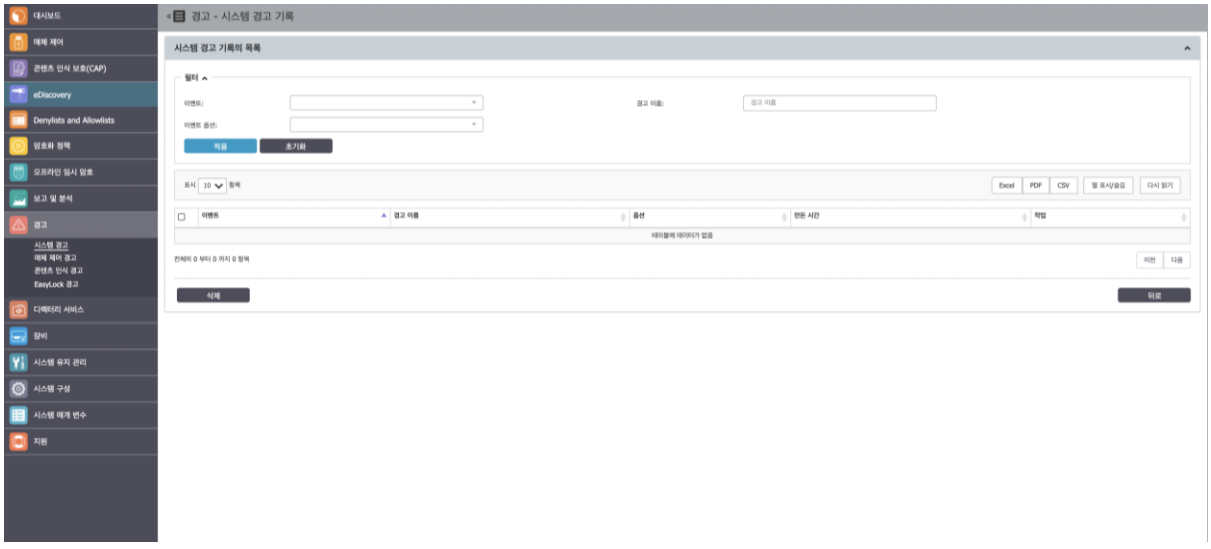
- **클라이언트 삭제** – 거대한 네트워크의 더 향상된 관리를 위해 Endpoint Protector 클라이언트가 삭제될 때 마다 경고가 보냅니다. 이 것은 특히 여러 관리자가 있을 때 더 도움이 됩니다.
- **서버 디스크 공간** – 로그를 저장하는 서버 디스크 공간이 남아있는지 정책이 적절하게 적용되어 있는지 확인 하기 위해 경고는 디스크 공간이 70%, 80%, 90%에 도달하면 보내도록 설정됩니다.
- **매체 제어 – 로그의 양** – 경고는 저장된 매체 제어 로그의 수가 지정된 양에 도달할 때마다 보냅니다. 간격을 10,000행 또는 10,000,000행 또는 원하는 값으로 정의해서 선택하는 옵션을 사용할 수 있습니다.
- **콘텐츠 인식 – 로그의 양** - 경고는 저장된 콘텐츠 인식 로그의 수가 지정된 양에 도달할 때마다 보냅니다. 간격을 10,000행 또는 10,000,000행 또는 원하는 값으로 정의해서 선택하는 옵션을 사용할 수 있습니다.
- **비밀번호 만료** – 비밀번호가 만료될 때 알림을 위한 경고를 설정합니다. 10일 5일 또는 1일 옵션을 사용하여 경고를 정의합니다.
- **온라인에서 안 보임** – 보호되는 엔드포이트가 특정 시간 동안 온라인에서 보이지 않으면 경고가 각 관리자에게 보내집니다. 이것은 또한 Endpoint Protector 클라이언트가 삭제될 수 있는 컴퓨터를 식별하는데 사용할 수 있습니다.
- **계획되지 않은 클라이언트 종료** – 사용자가 Endpoint Protector 프로세스 종료를 시도할 때 식별하기 위해서 경고를 설정합니다.

2. **경고 이름** – 경고에 이름을 추가합니다.
3. **옵션** – 선택한 경고 유형을 기반으로 추가적인 옵션을 사용한 경고를 정의합니다.
4. **관리자** – 경고를 받은 관리자를 선택합니다.



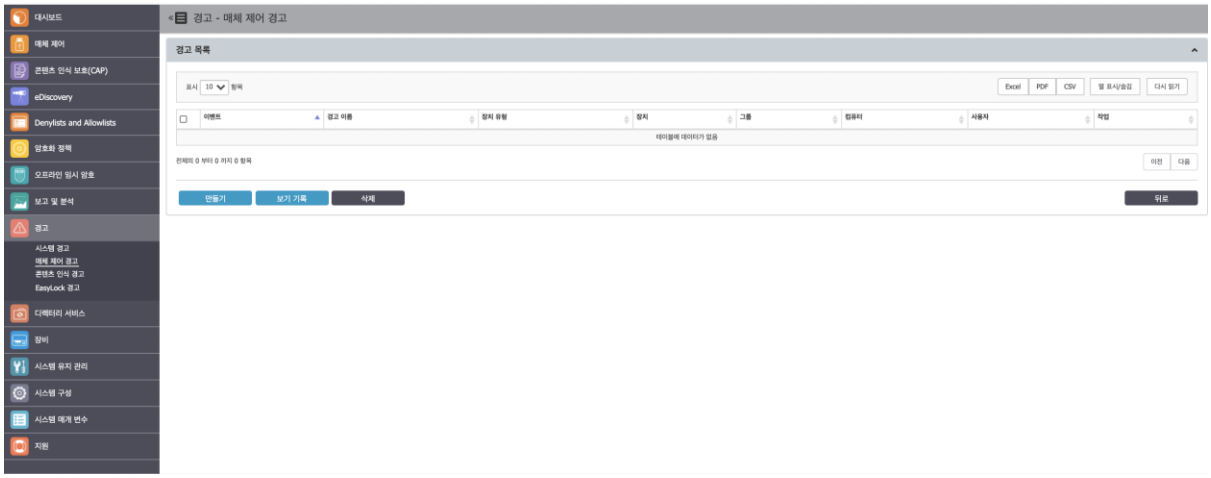
12.1.2. 시스템 경고 기록

이 섹션에서 시스템 경록 기록을 볼 수 있습니다. 더 이상 감사 목적으로 필요하지 않은 경고는 나중에 삭제 할 수 있습니다.



12.2. 매체 제어 경고

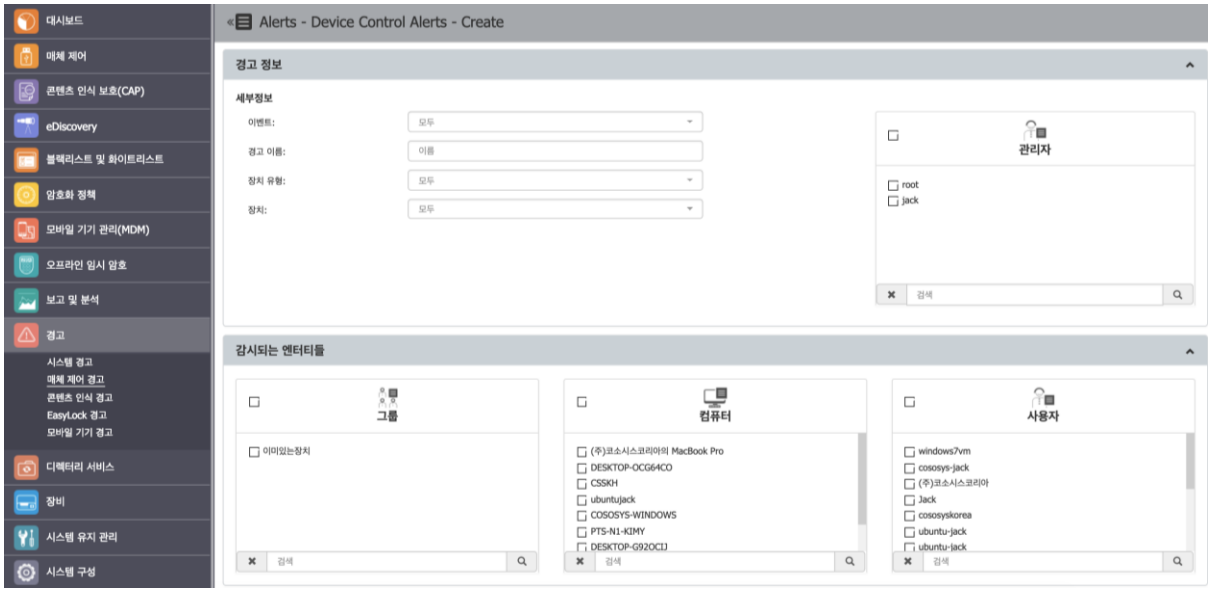
이 섹션에서는 관리자가 연결, 파일 읽기, 파일 쓰기, EasyLock 배포 성공 등과 같은 매체 제어 경고를 만들 수 있습니다.



12.2.1. 매체 제어 경고 만들기

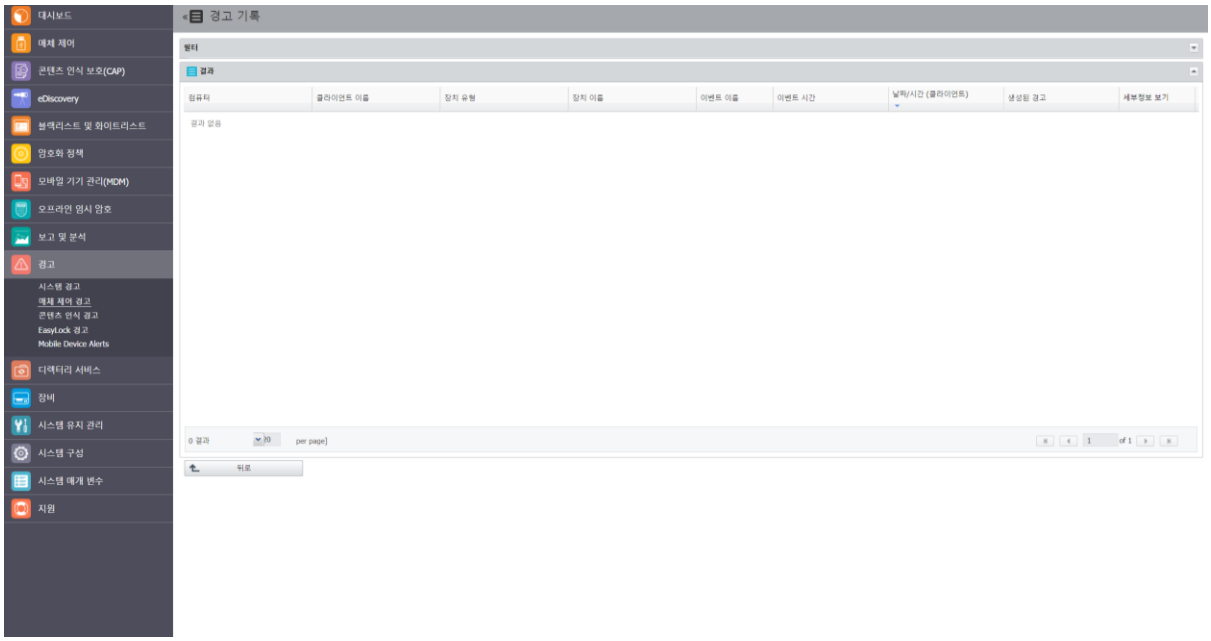
새로운 매체 제어 경고를 만들 때 아래 정보 정의가 필요합니다.

- **이벤트** – 경고를 만드는 이벤트 유형 (모두, 연결, 연결 끊어짐, 파일 읽기, 파일 쓰기, 파일 삭제 등)
- **경고 이름** – 경고의 이름
- **장치 유형** – 장치의 유형 (모두, USB 저장 장치, 블루투스, 스마트폰, iPhone, ZIP 드라이버 등)
- **장치** – 시스템에서 이미 사용 가능한 특정 장치
- **감시되는 엔터티들** – 이벤트를 만드는 그룹, 컴퓨터 또는 사용자
- **관리자** – 경고를 수신해야 하는 관리자



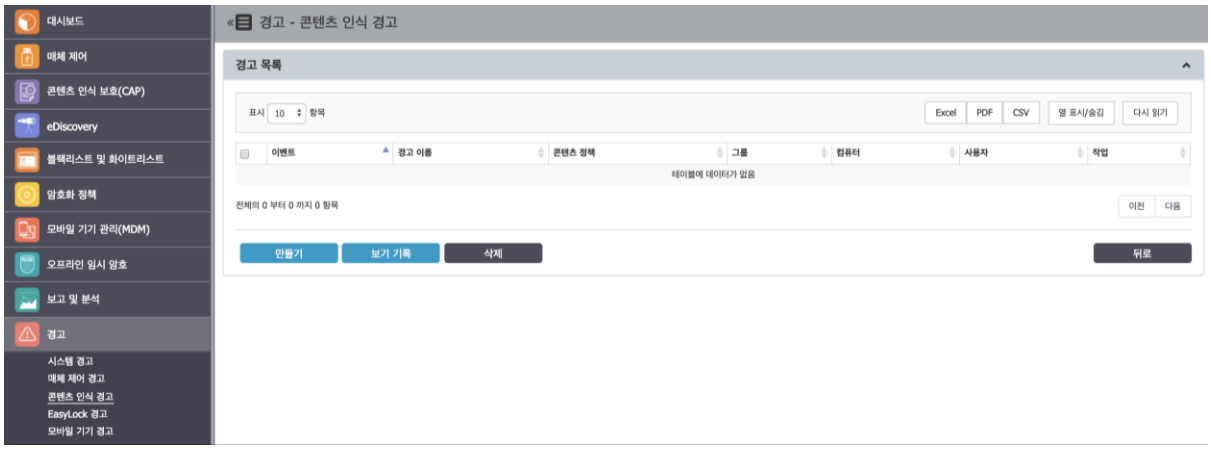
12.2.2. 매체 제어 경고 기록

이 섹션에서 매체 제어 경고 기록을 볼 수 있습니다. 더 이상 감사 목적으로 필요하지 않은 경고는 나중에 삭제할 수 있습니다.



12.3. 콘텐츠 인식 경고 정의

콘텐츠 인식 보호 모듈에 정의된 정책에 따라 새 콘텐츠 인식 경고를 생성하려면 콘텐츠 인식 경고 정의 하위 메뉴로 이동한 후 "만들기" 버튼을 클릭합니다.



12.3.1. 콘텐츠 인식 경고 만들기

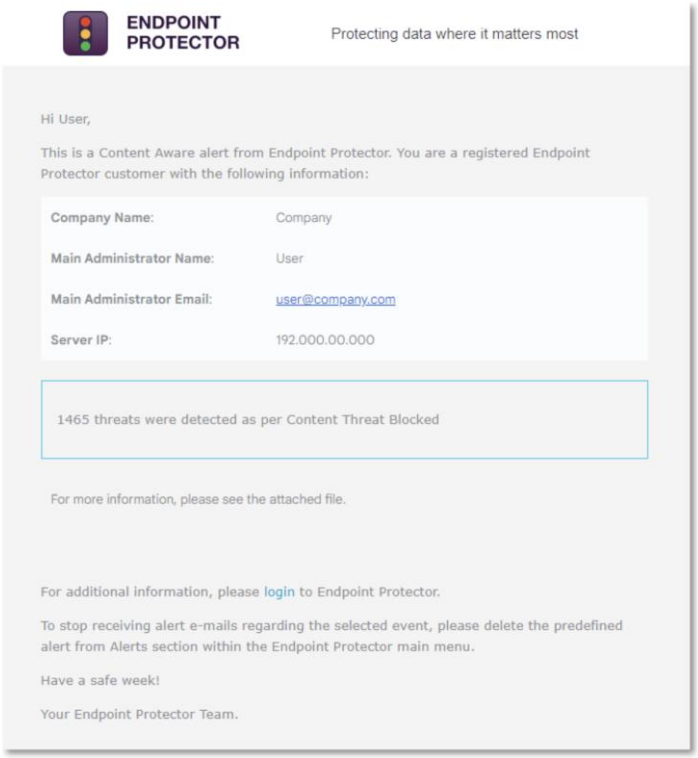
새로운 콘텐츠 인식 경고를 만들기 위해서는 아래 정보가 정의되어야 합니다.

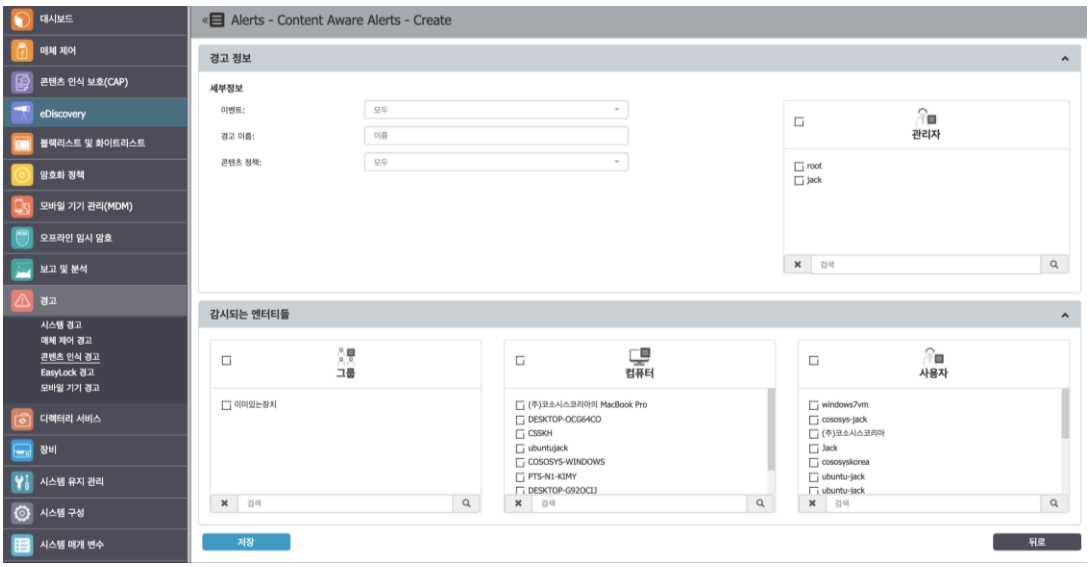
1. **이벤트** – 경고를 만드는 이벤트 유형 (콘텐츠 위협 탐지 또는 콘텐츠 위협 차단)
    - **탐지된 DPI 우회 허용목록 콘텐츠 위협**
    - **차단된 콘텐츠 위협**
    - **콘텐츠 수정 세션활동**
    - **사용자가 취소한 콘텐츠 수정 요청**
    - **DPI 우회 트래픽**
2. **경고 이름** – 경고 이름을 추가합니다.
3. **콘텐츠 정책** – 경고를 적용하는 정책을 선택합니다.
4. **감시되는 엔터티들** – 이벤트를 만드는 그룹, 컴퓨터 또는 사용자를 선택합니다.

5. **관리자** – 경고를 받는 관리자를 선택합니다.

이메일로 보낸 경고는 발견된 위협 보고로 CSV 파일이 포함됩니다.

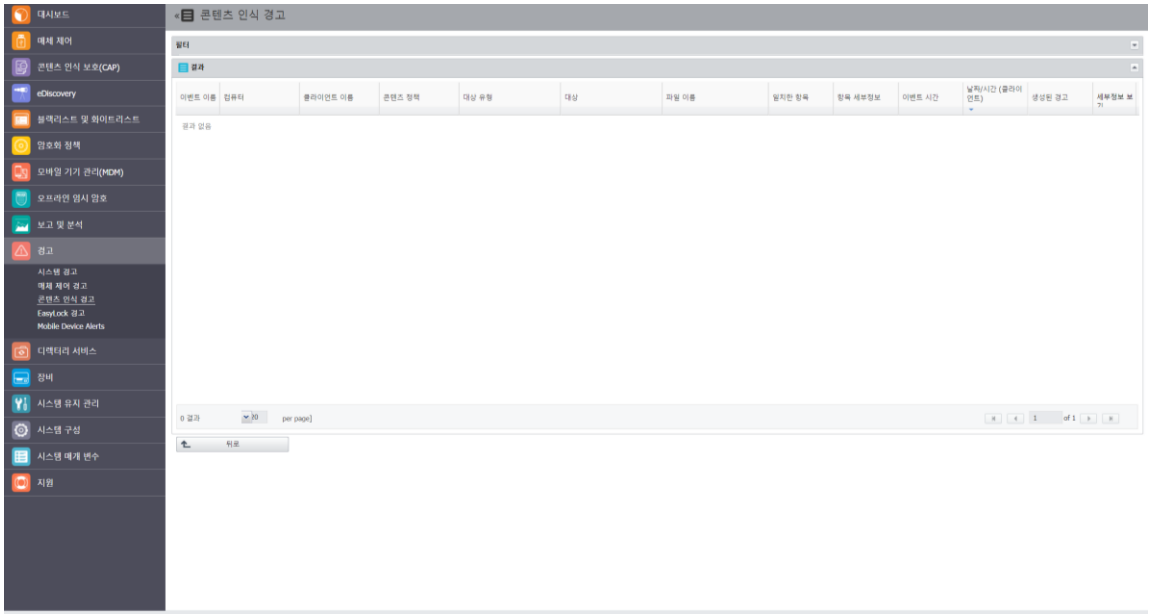
참고: 경고를 만들기 전에 선택된 콘텐츠 인식 정책이 선택된 컴퓨터, 사용자, 그룹 또는 구분에서 사용이 가능해야 합니다.





12.3.2. 콘텐츠 인식 경고 기록

이 섹션에서 콘텐츠 인식 경고 기록을 볼 수 있습니다. 더 이상 감사 목적으로 필요하지 않은 경고는 나중에 삭제할 수 있습니다.



12.4. EasyLock 경고

이 섹션에서는 관리자가 암호 변경, 메시지 전송 등과 같은 이벤트의 EasyLock 경고를 만들 수 있습니다.

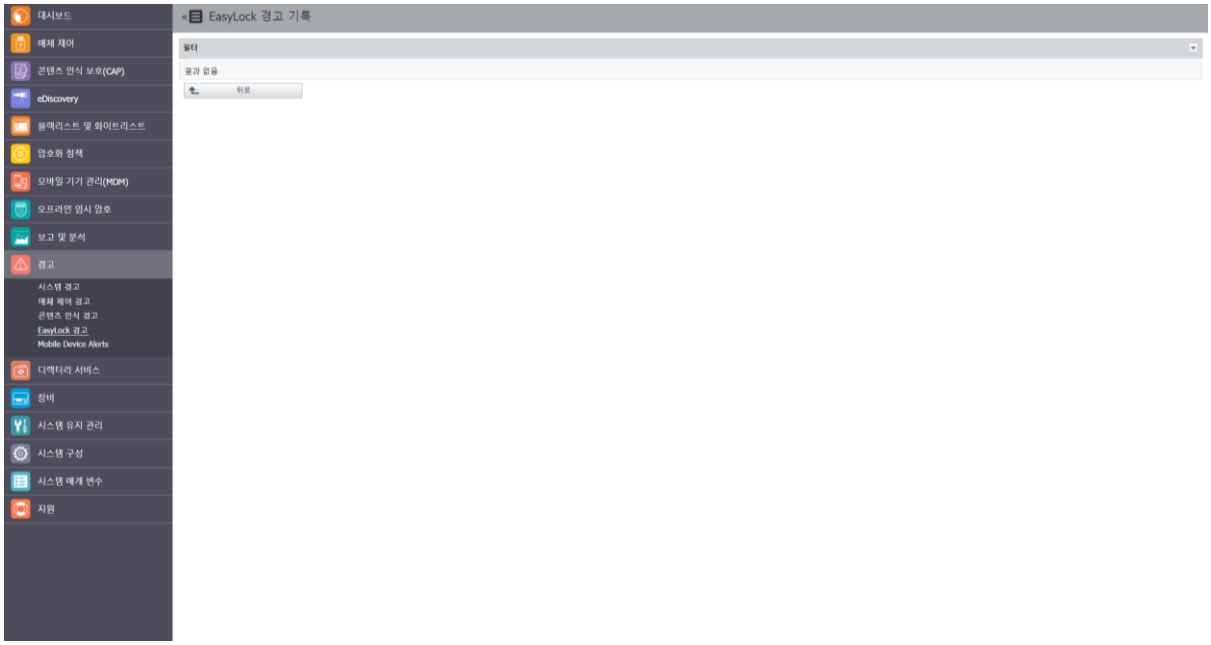
12.4.1 EasyLock 경고 만들기

새로운 EasyLock 경고를 만들 때 아래 정보 정의가 필요합니다.

1. **이벤트** – 경고가 만들어지는 이벤트 유형 선택
    - **메시지 보내기**
    - **마스터 패스워드 변경**
    - **사용자 패스워드 변경**
    - **장치 초기화**
    - **설정 변경 – 설치 및 실행**
    - **클라이언트 다시 배포**
    - **마스터 패스워드 로그인 성공**
    - **패스워드 로그인 실패**
    - **패스워드 로그인 시도 초과**
2. **경고 이름** – 경고 이름을 추가합니다.
3. **관리자** – 경고를 받는 관리자를 선택합니다.

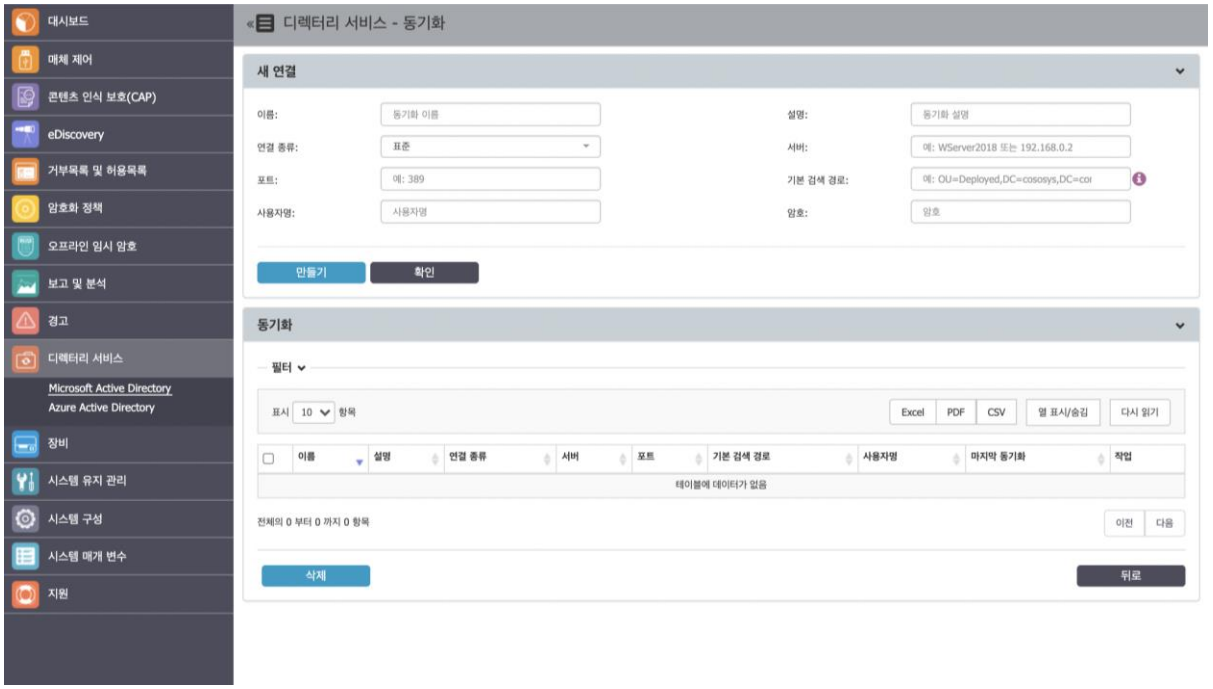
12.4.2 EasyLock 경고 기록

이 섹션에서 EasyLock 경고 기록을 볼 수 있습니다. 더 이상 감사 목적으로 필요하지 않은 경고는 나중에 삭제할 수 있습니다.



13. 디렉터리 서비스

이 섹션에서는 관리자가 회사의 Active Directory에서 객체 (사용자, 컴퓨터 및 그룹)을 가져오고 동기화 할 수 있습니다.



13.1. Microsoft Active Directory

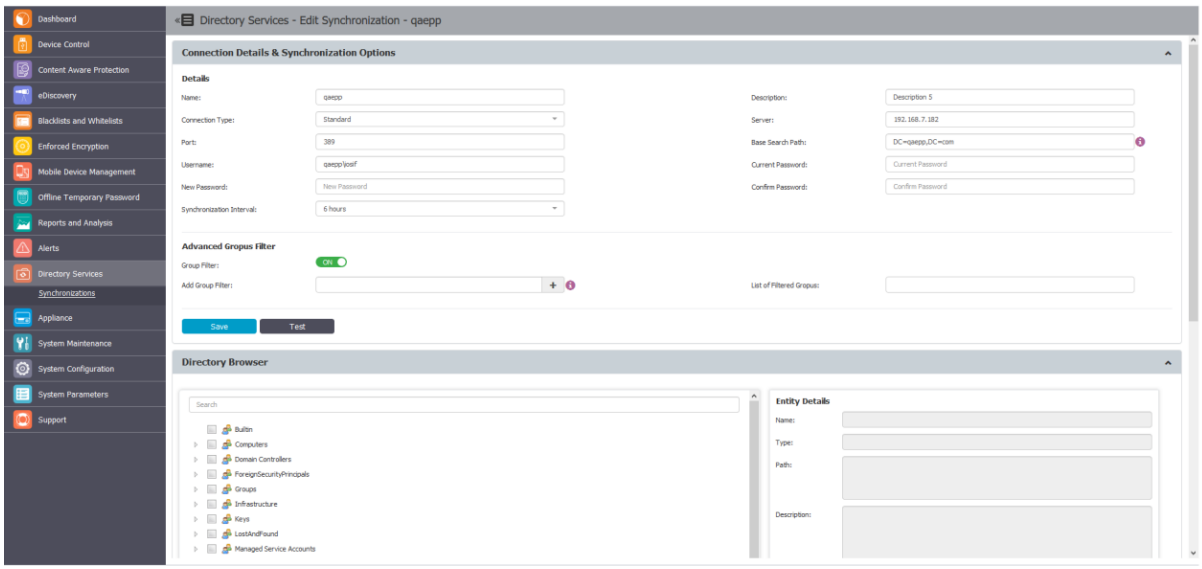
관리자는 디렉토리 서비스 > Microsoft Active Directory 섹션에서 연결을 만들고 관리할 수 있습니다. 연결 유형, 서버, 포트, 사용자 이름 및 암호의 정보가 필요합니다.

참고: 많은 객체를 가져올 때 관련 정보만 보이게 하기 위해서 기본 검색 경로를 사용하는 것을 권장합니다. 브라우저 제한으로 전체 AD 구조를 가져오는 것은 객체가 많다면 노출이 지연될 수도 있습니다.

정확한 정보 입력을 확인하기 위해서 새로운 연결은 테스트 버튼을 눌러서 확인할 수 있습니다.

새로운 연결이 만들어지면 동기화 목록에서 사용 가능하고 편집 그리고 필요한 객체를 가져올 수 있습니다.

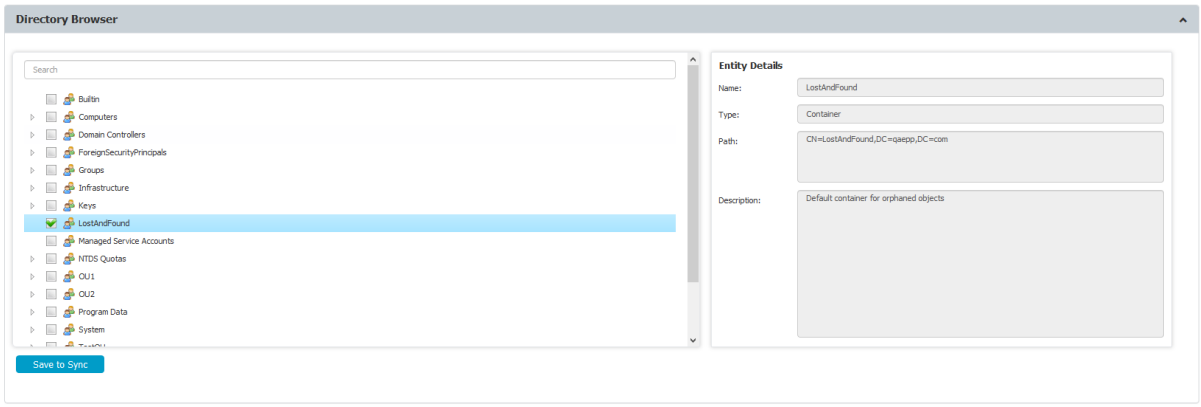
정의된 연결에서 여러가지 동기화 옵션을 사용할 수 있습니다. 이 섹션에서 연결 계정과 동기화 간격 또한 변경할 수 있습니다.



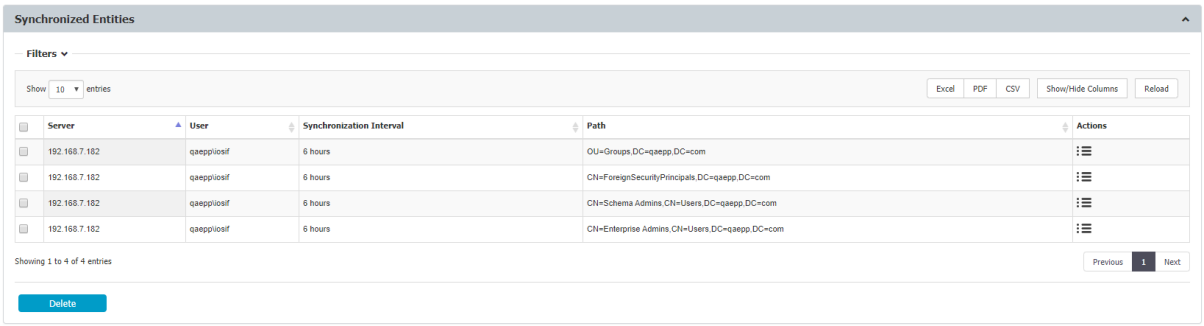
고급 그룹 필터는 특정 그룹만 가져오고 동기화 할 때 사용할 수 있습니다. 나머지 모든 객체는 무시합니다.

디렉터리 브라우저 섹션에서 관리자는 동기화에 필요한 모든 객체를 선택할 수 있습니다.

참고: 디렉터리 브라우저에서 OU (Organizational Units)과 그룹만 볼 수 있습니다.



객체를 선택하고 동기화 저장을 할 수 있습니다.



13.2. Azure Active Directory

관리자는 '디렉터리 서비스 > Azure Active Directory' 에서 연결을 만들고 관리할 수 있습니다. 이 섹션에서 Azure Active Directory 그룹은 Endpoint Protector 서버와 사용자를 동기화합니다. 그룹 멤버쉽은 API 플랫폼 자체에서 반복적으로 가져올 것입니다.

예:

- **그룹 1 -> 사용자 1, 사용자 2, 사용자 3;**
- **그룹 2 -> 그룹 1, 사용자 4;**
- **그룹 3 -> 그룹 2, 사용자 5;**

동기화 운영으로 그룹 3를 선택하면 Endpoint Protector 서버에서 그룹 3만 가져오고 만듭니다. 사용자 5는 또한 그룹 3의 멤버로써 추가될 것입니다. 그룹 2와 모든 서브 그룹은 분리되어서 사용자만 가져오고 실제 그룹은 서버에 추가되지 않을 것입니다.

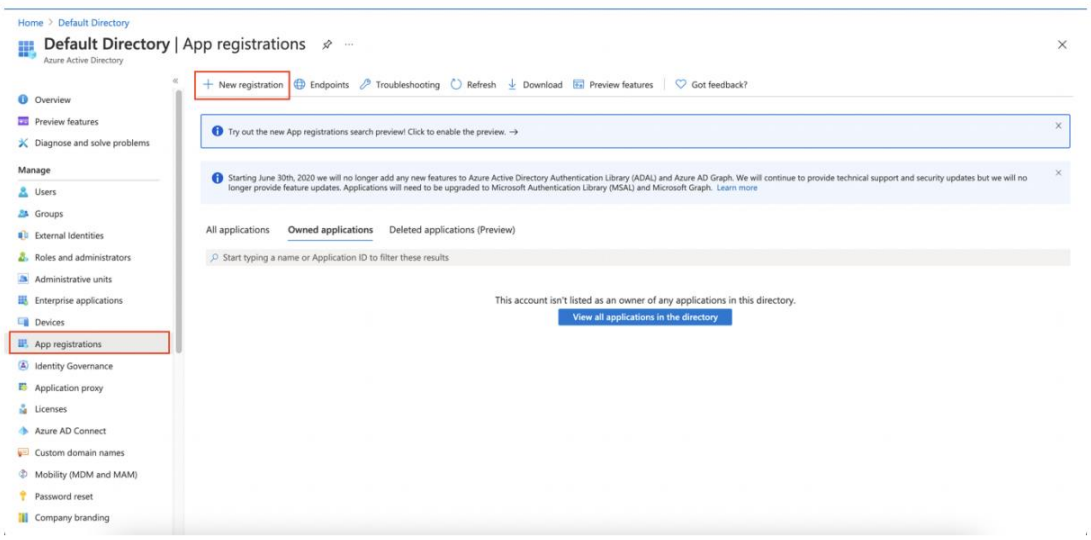
동기화가 끝난 후에 Endpoint Protector 서버에서 다음과 같이 보일 것입니다:

- **그룹 3 -> 사용자 5, 사용자 4, 사용자 3, 사용자 2, 사용자 1;**

13.2.1. Azure Active Directory 구성

13.2.1.1. Azure Active Directory에서 응용프로그램 만들기

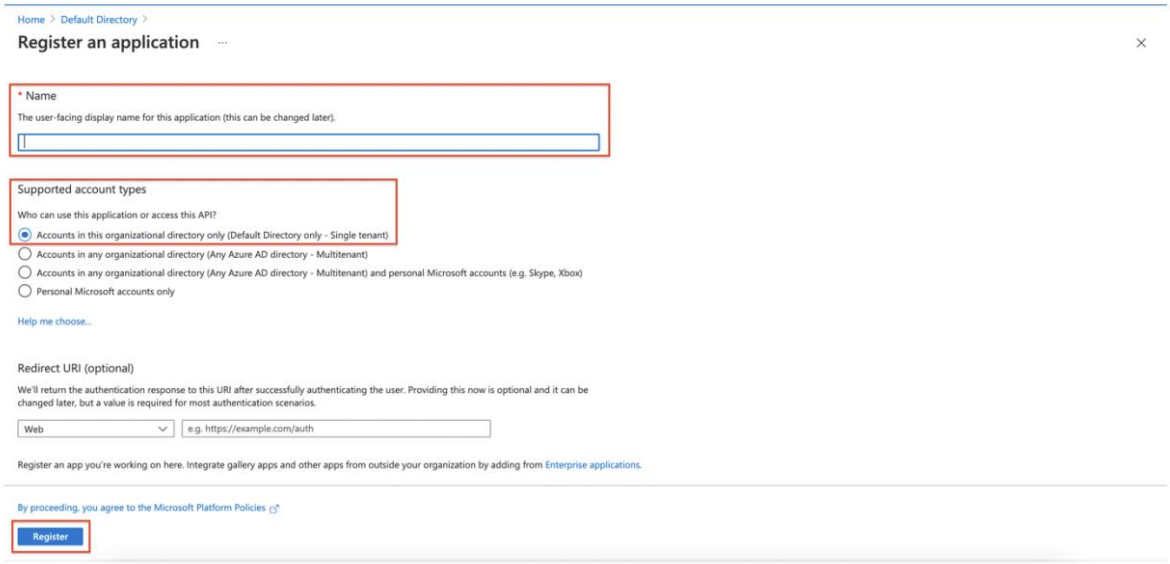
1. Azure Portal 로그인
2. Azure Active Directory 탐색
3. 왼쪽의 Active Directory 메뉴에서 **Manage** 섹션의 **App Registrations**을 클릭 후 **New Registration** 을 클릭합니다.



4. **Registration** 페이지에 **이름**을 입력합니다.
5. 지원되는 계정 유형에서 **Default Directory**를 선택합니다.

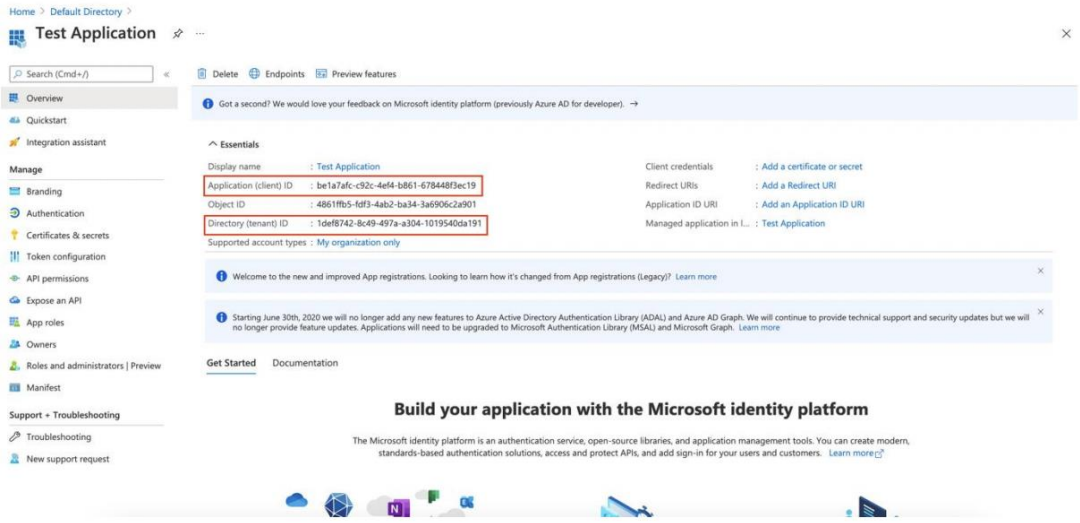
   중요: Redirect URI 필드에 입력하지 마시기 바랍니다.

6. **Register** 를 클릭합니다.



7. **Essentials** 섹션에서 다음 정보를 저장합니다:

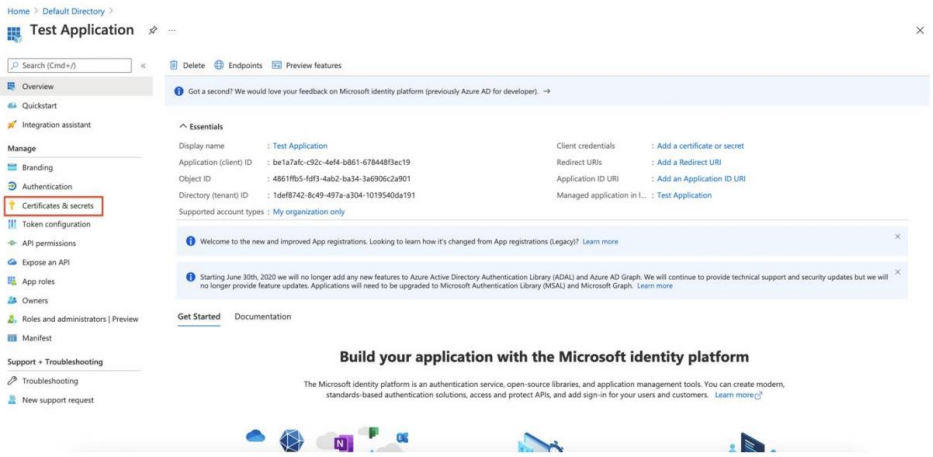
   - Application (client) ID는 Endpoint Protector 서버에서 Application (client) ID 항목에 추가할 때 필요할 것입니다.
   - Directory (tenant) ID는 Endpoint Protector 서버에서 Tenant ID 항목에 추가할 때 필요할 것입니다.



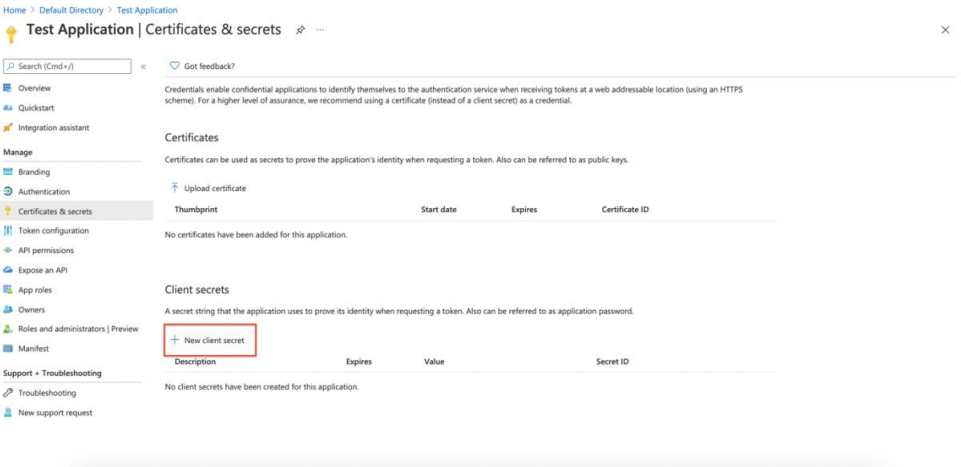
13.2.1.2. 응용프로그램에서 비밀 ID 만들기

비밀 ID는 Graph API에 응용프로그램에 접근하는 인가 방법으로 사용될 것입니다.

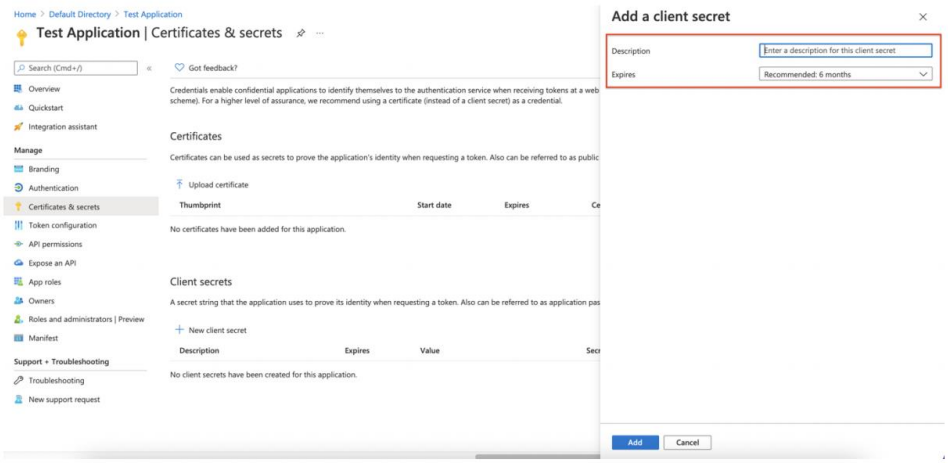
1. **Manage** 섹션의 측면 메뉴에 있는 **Certificates & Secrets** 클릭합니다.



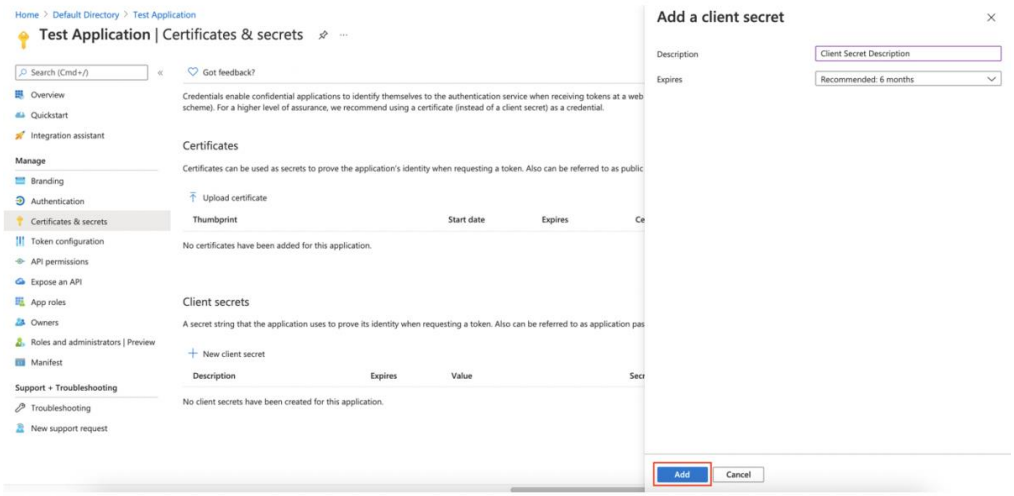
2. **Certificates & Secrets** 페이지에 **New client secret** 버튼을 클릭합니다.



3. secret ID의 **Description** 을 입력합니다.

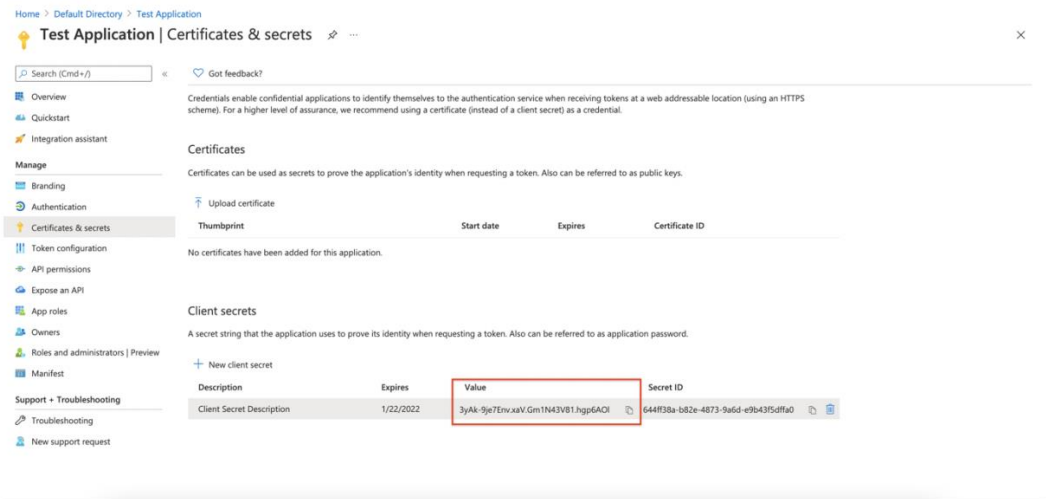


4. **Add** 및 **Add a client secret section** 클릭합니다.



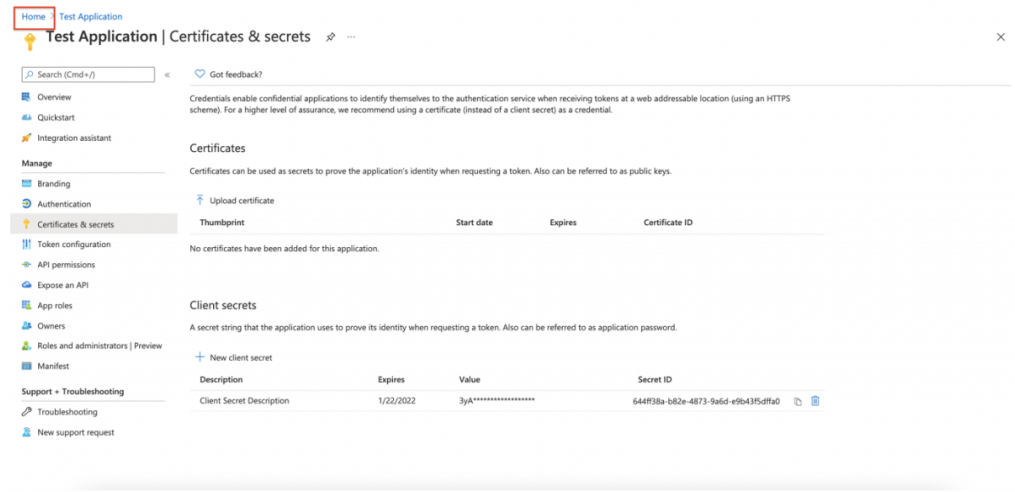
5. 나중에 더 필요하기 때문에 Secret ID 값을 기록하고 클립보드에 복사하고 안전하게 저장합니다.

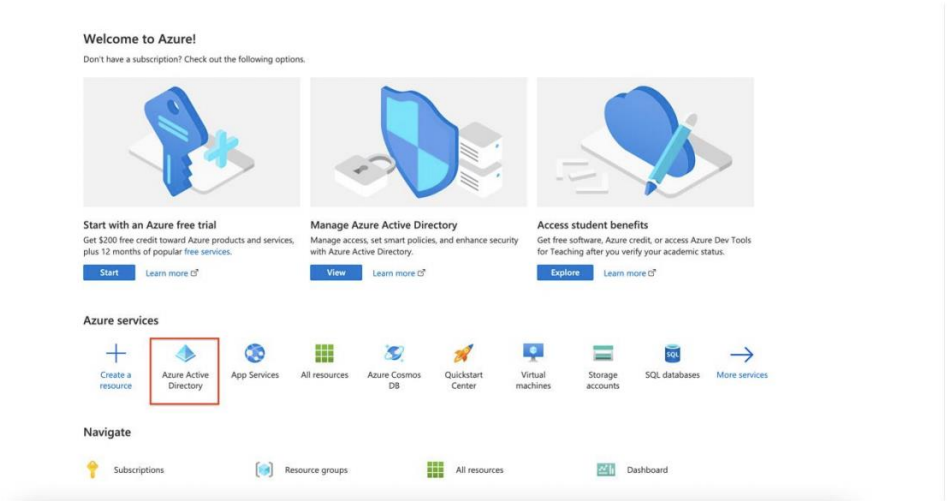
참고: 뒤로 가기를 하면 secret ID는 숨겨질 것입니다.



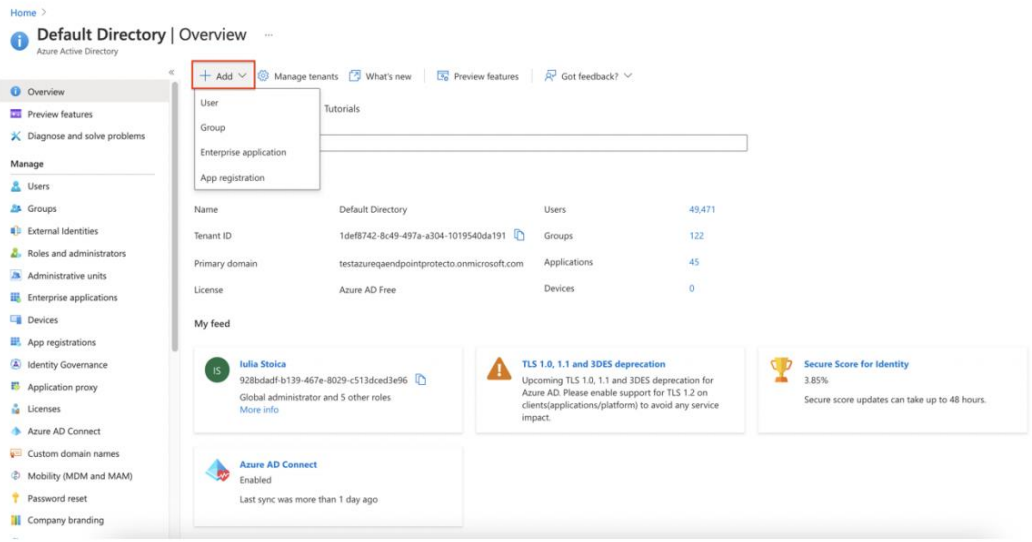
13.2.1.3. 그룹 API를 사용하여 사용자 / 그룹 만들기

1. **Home** 그리고 **Azure Active Directory**를 클릭합니다.

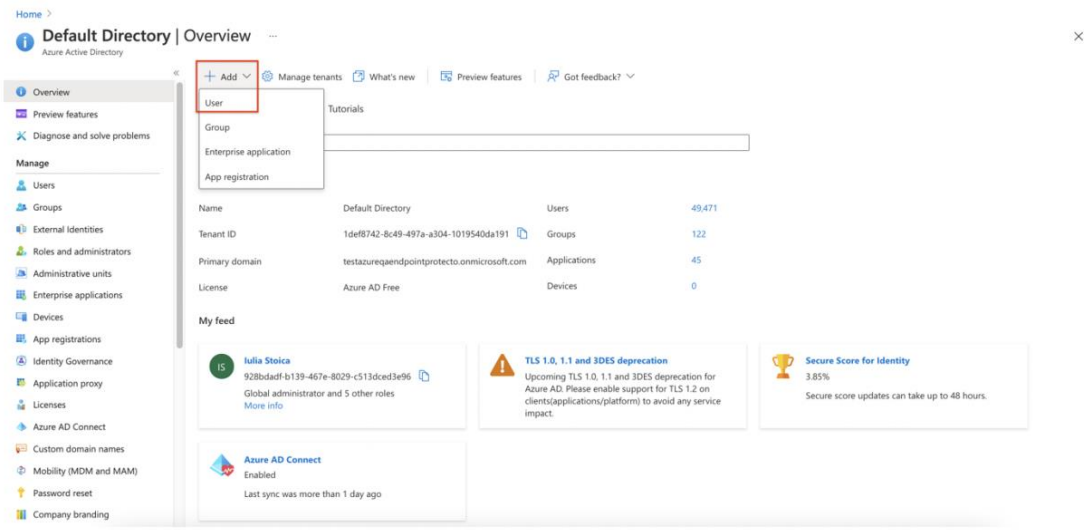




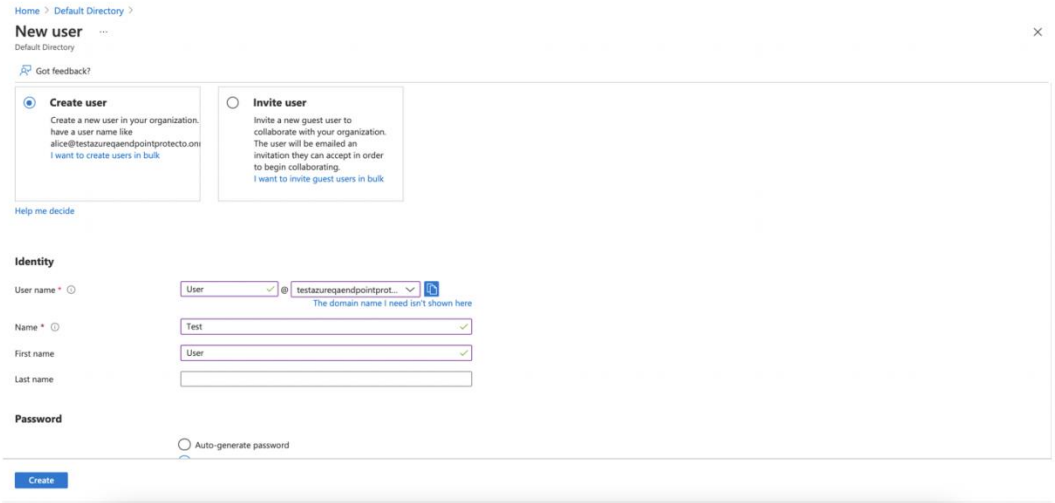
2. Default **Directory | Overview** 페이지에서 **Add** 버튼 클릭



3. **Add User** 클릭

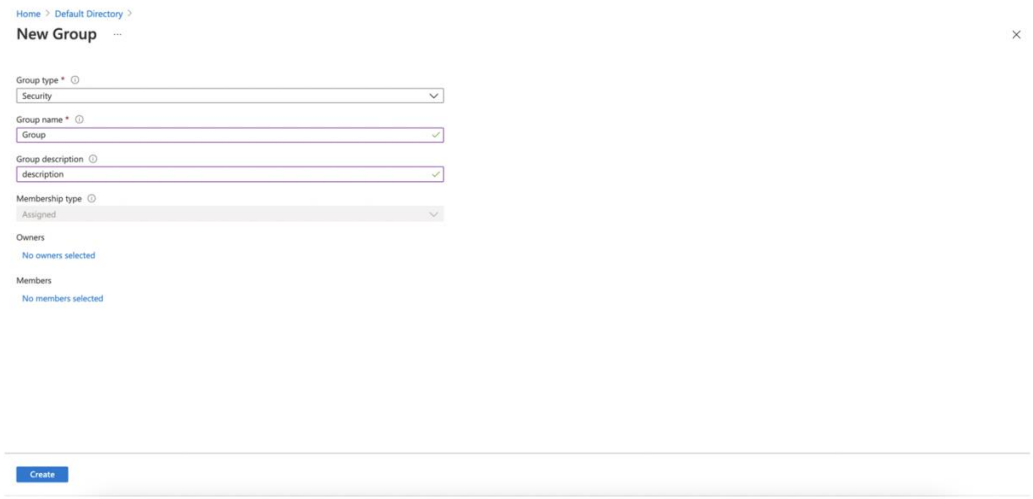


- **Create User** 선택
- **Username** 에서 **Domain** 선택
- **Name** 들어가기
- Auto-generate password 를 클릭하거나 직접 만들기
- **Department** 추가
- **Create** 클릭



4. 스텝 1과 2를 반복하고 **Group** 클릭

- **그룹 보안 유형** 선택
- 그룹 **이름**으로 가기
- 멤버쉽 추가를 위해 선택된 **멤버 없음** 클릭
- 새롭게 만들어진 사용자 검색 그리고 **Select** 클릭



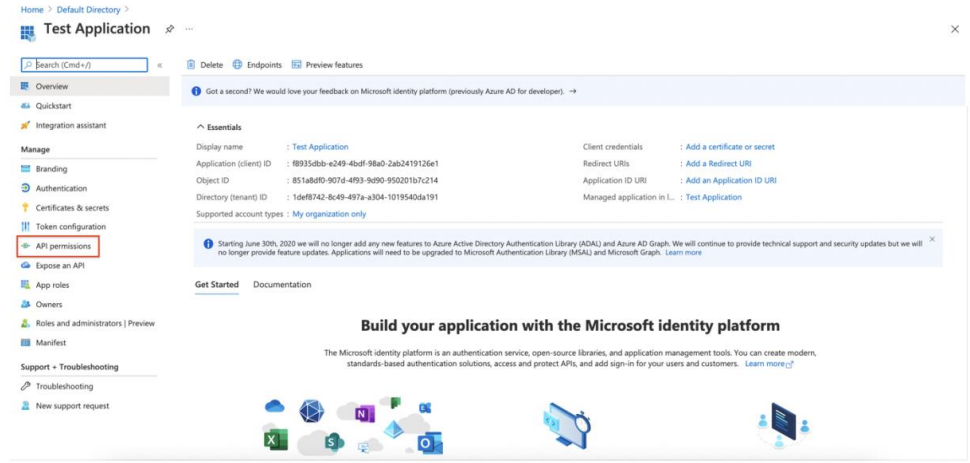
13.2.1.4. 응용프로그램에 승인 추가하기

응용프로그램에 추가되는 승인:

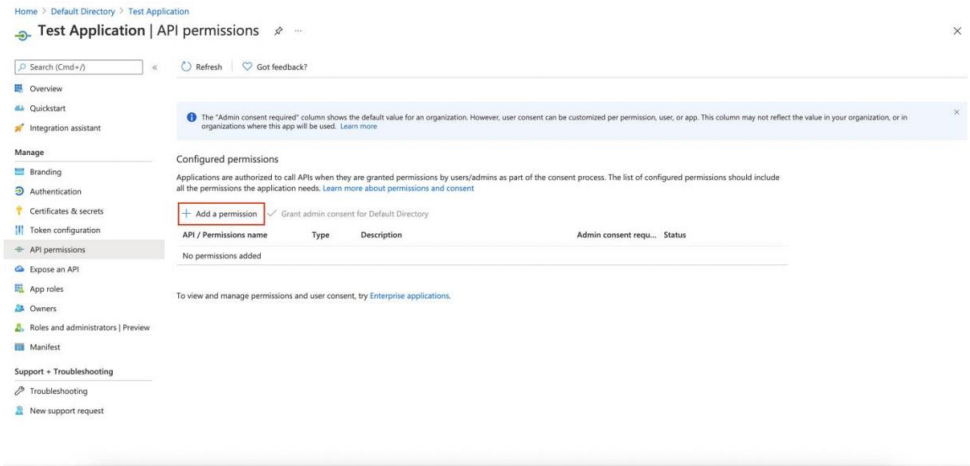
- ❿ **Directory.ReadWrite.All**
- ❿ **Group.ReadWrite.All**
- ❿ **User.ReadWrite.All**

만들어진 응용프로그램이 열리는지 확인하고 다음을 진행합니다:

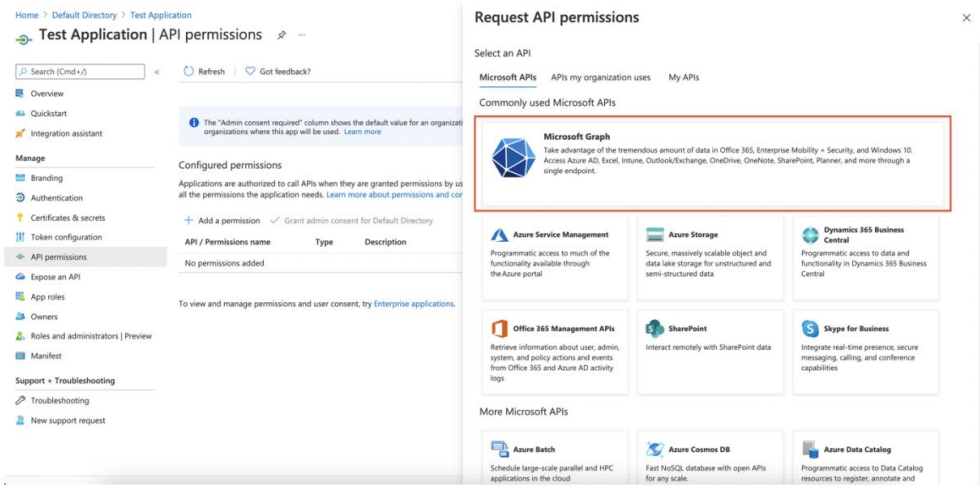
1. **API Permissions** 클릭합니다.



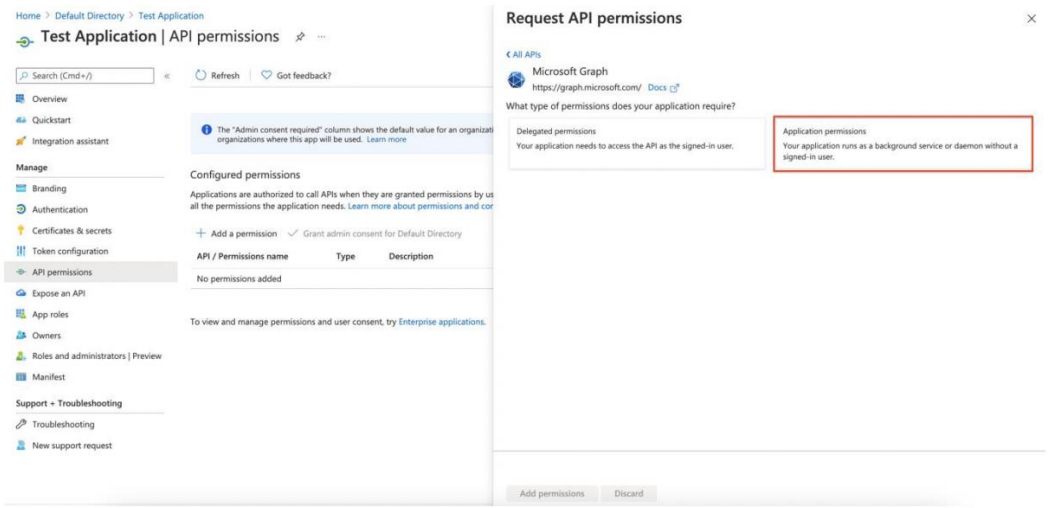
2. **Add a Permission** 클릭합니다.



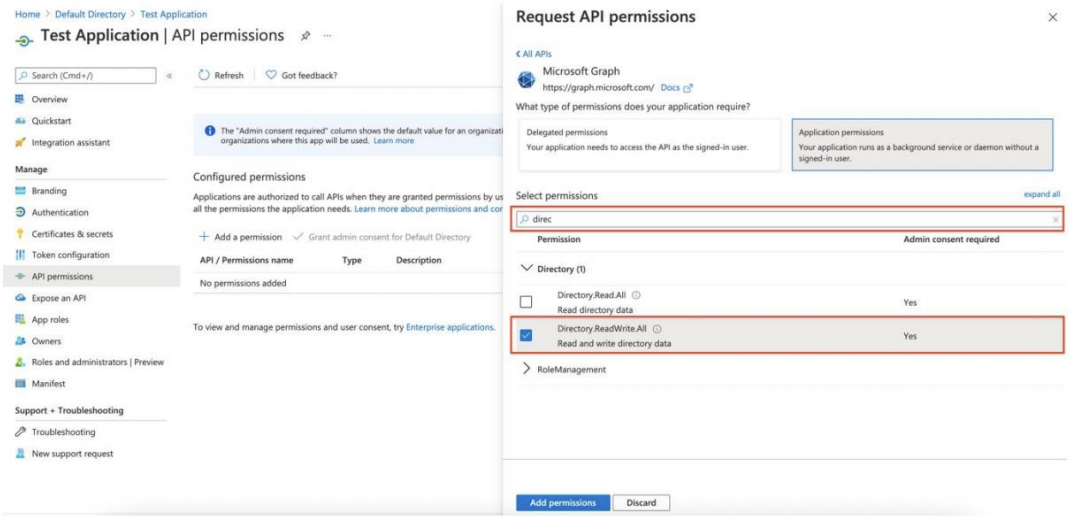
3. **Microsoft Graph** 클릭합니다.



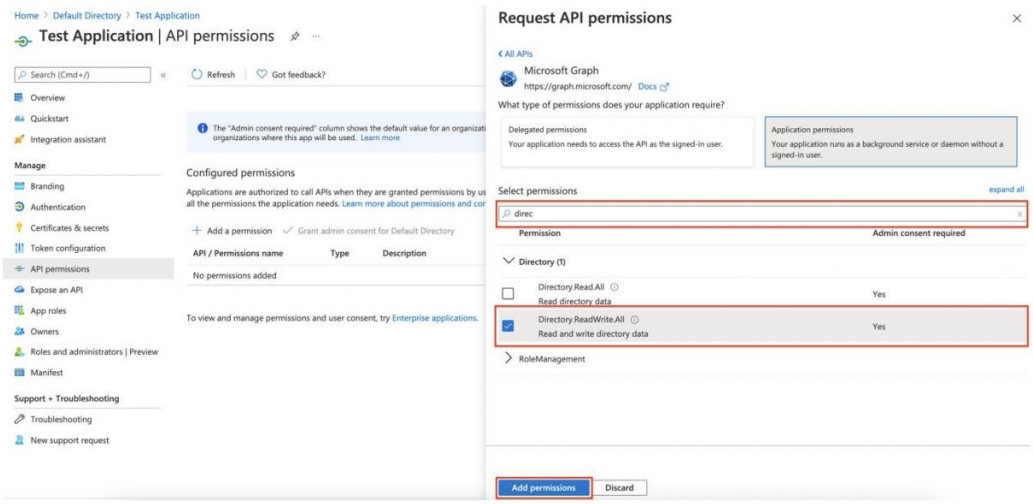
4. **Application Permissions** 클릭합니다.



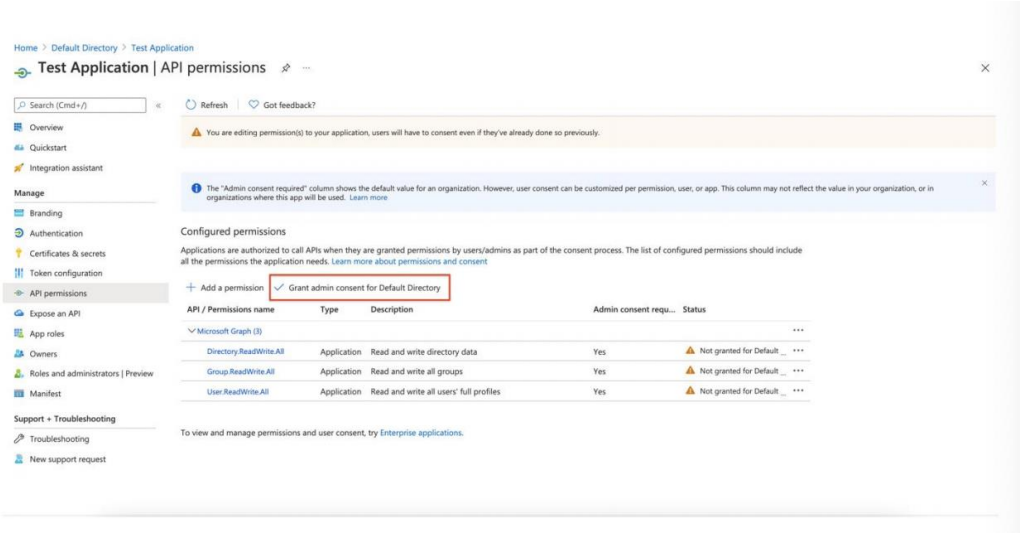
5. 위에서 언급된 승인을 검색하고 각각의 승인을 확인합니다. (Directory.ReadWrite.All, Group.ReadWrite.All, User.ReadWrite.All)



6. **Add Permissions** 클릭합니다.



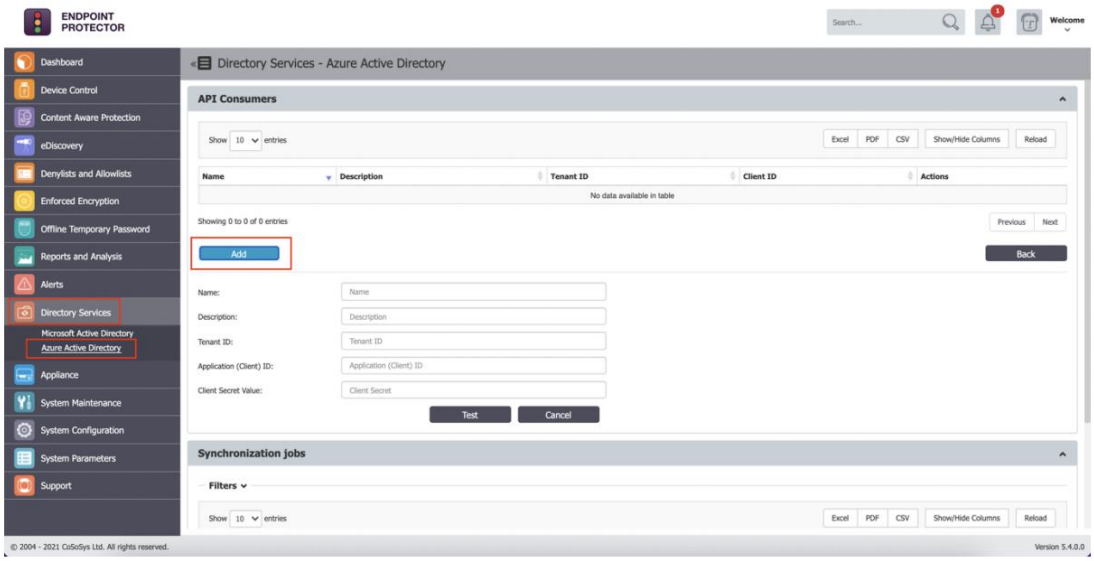
7. **API Permission** 페이지에서 **Grant admin consent for Default Directory** 버튼을 클릭



13.2.1.5. Endpoint Protector 서버에 Graph Application 추가하기

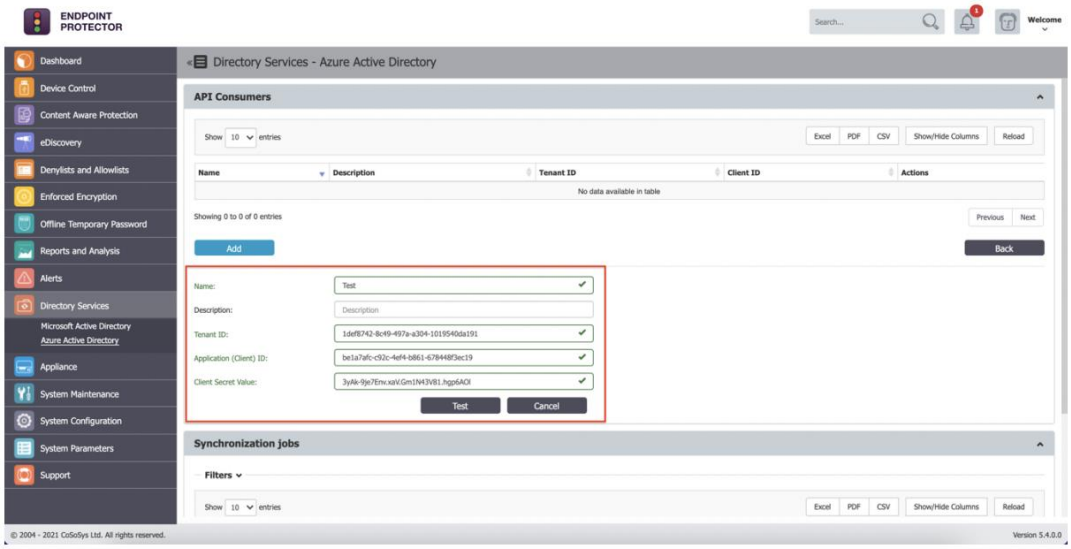
1. **'Endpoint Protector 서버 -> 디렉터리 서비스 -> Azure Active Directory'** 이동

2. API Consumer 추가를 위해 추가 버튼 클릭합니다 - 하나의 API Consumer는 다중 동기화 작업에 사용될 수 있습니다.

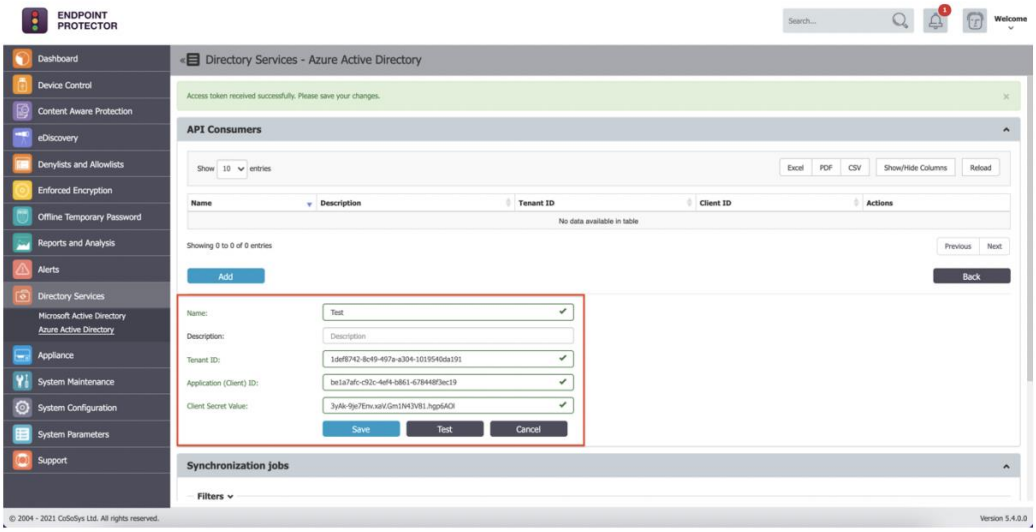


3. 상세 정보를 완성합니다.

   - **이름** 추가
   - **설명** 추가
   - Tenant ID 영역에 미리 저장한 **Directory (tenant) ID** 추가
   - 영역에 미리 저장한 **Application (client) ID** 추가
   - Client Secret Value 영역에 미리 저장한 **Secret ID** 추가

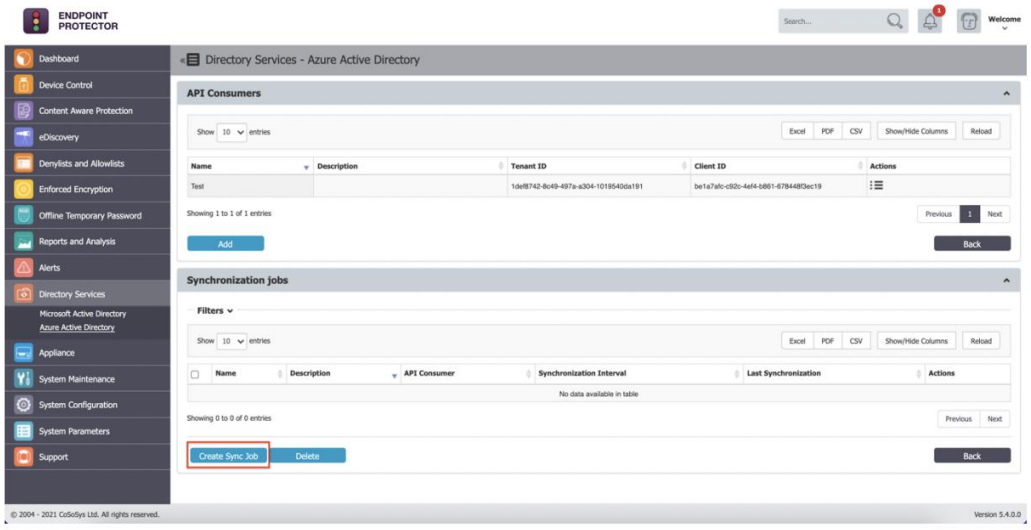


4. **테스트** 버튼 클릭 후 **저장**합니다.



13.2.1.6. Endpoint Protector 서버에서 동기화 작업 만들기

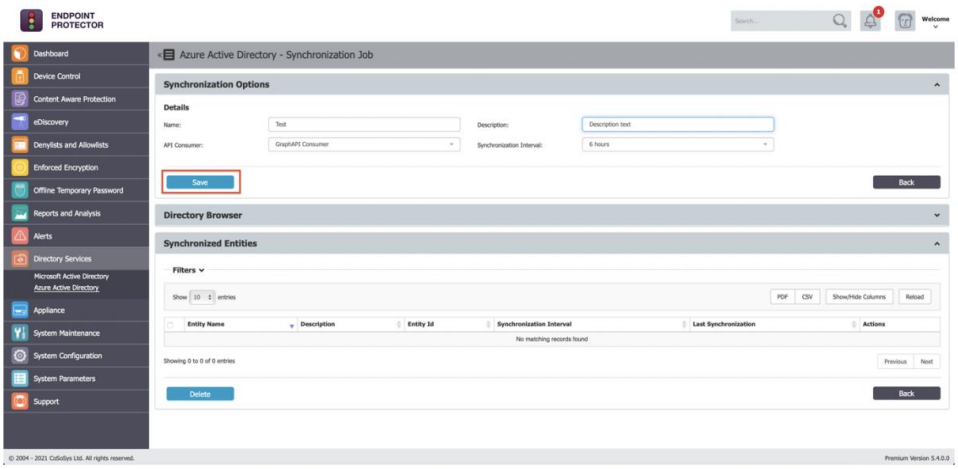
1. **동기화 작업 만들기** 클릭합니다.



2. 동기화 옵션 완성하기

- **이름** 입력
- **설명** 입력
- 만들어진 API Consumer 선택
- **동기화 간격** 선택

- **저장** 클릭



Azure Active Directory 커넥터의 "온-프레미스 사용자 매핑 (Map on-premises users)" 스위치는 Endpoint Protector가 로컬 Active Directory와 Azure AD (Active Directory)가 모두 있는 하이브리드 환경에서 사용자 이름을 검색하는 방법을 제어합니다. 이 스위치는 두 가지 상태가 있습니다:

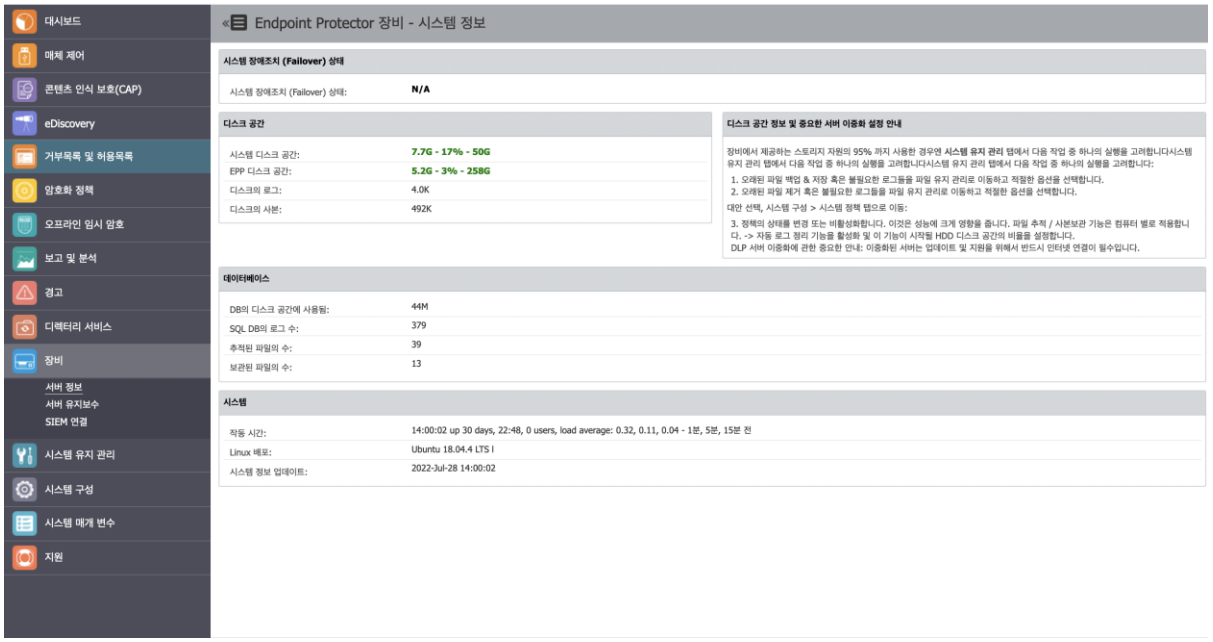
- **표시되지 않음 (기능 사용 안 함):** EPP는 사용자 이름 검색에 "userPrincipalName" Azure AD 속성을 사용합니다. 이 속정은 사용자 식별 및 계정 매핑의 기본 소스입니다.
- **표시됨 (기능 사용):** EPP는 사용자 이름 검색에 "onPremisesSamAccountName" Azure AD 속성을 사용합니다. 로컬 Active Directory와 Azure AD 사이에 정확한 동기화를 보장합니다.

이 기능을 활용하면 EPP는 사용자 이름의 원활한 동기화를 보장하여 사용자 이름 중복을 방지합니다. 특정 하이브리드 환경 설정과 요구사항을 기반으로 "Map on-premises users" 기능을 사용하거나 사용하지 않도록 설정하시기 바랍니다.

14. 장비

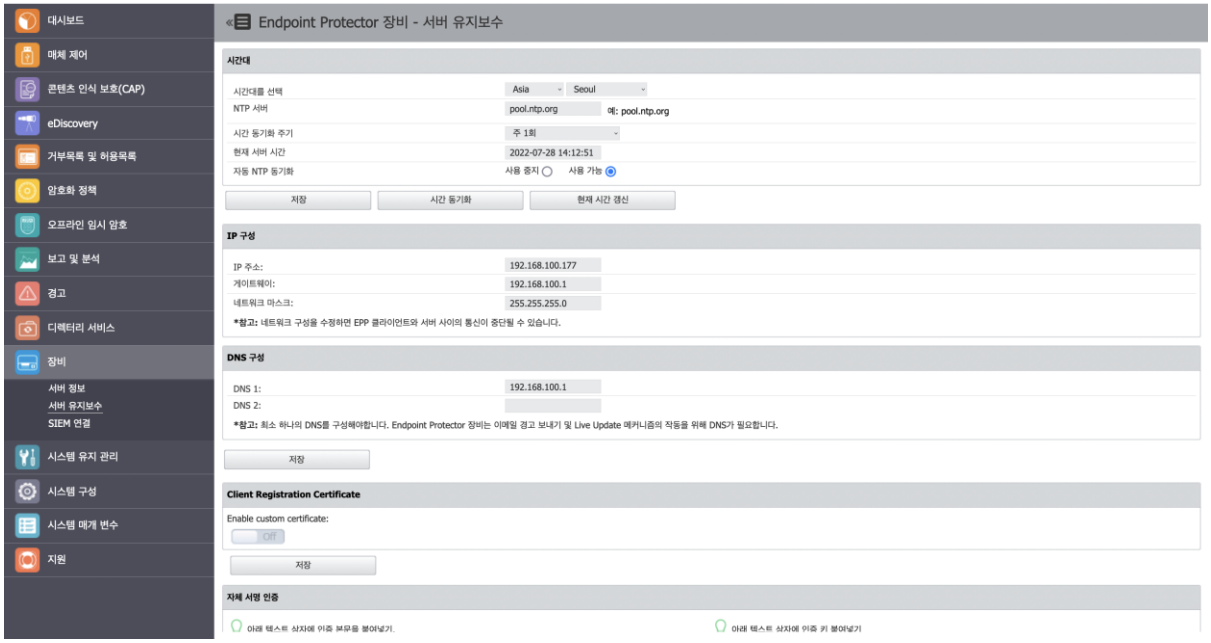
14.1. 서버 정보

이 화면은 관리자에게 서버, 장애 조치, 총 디스크 사용 및 동작 시간 등의 일반 정보를 제공 합니다.



14.2. 서버 유지보수

이 섹션에서 관리자는 선호 시간대와 NTP 동기화 서버를 설정, IP 및 DNS 구성, SSH 서버 접근 사용 / 사용 중지 뿐만 아니라 다시 부팅 / 종료 동작 수행까지 할 수 있습니다.

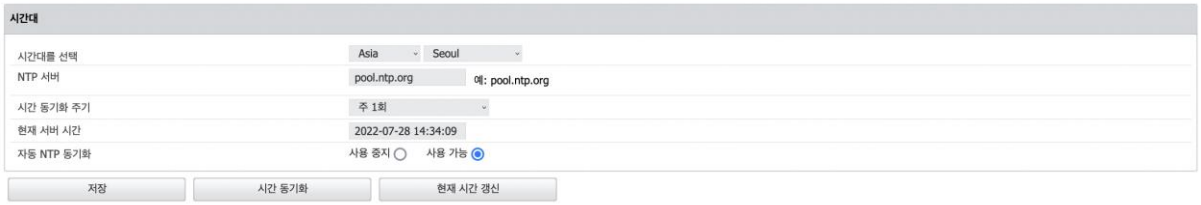


14.2.1. 시간대 설정

이 섹션에서 우선적인 시간대 또는 NTP 서버에 장비 동기화를 설정할 수 있습니다.

- **시간대를 선택** – 드롭다운 목록에서 지역과 위치를 선택
- **NTP 서버** – 서버 유형 또는 기본 입력으로 이동
- **시간 동기화 주기** – 기본값 선택으로 동기화 할 때 시간 주기는 드롭다운에서 선택

  참고: 장비는 pool.ntp.org 로 주 1회 동기화 설정이 미리 되어 있습니다.
- **현재 서버 시간** – 현재 서버 시간이 이 영역에 표시됩니다.
- **자동 NTP 동기화** – NTP 동기화를 사용 중지 또는 사용 가능으로 선택
- 동기화 프로세스 시작 없이 모든 변경을 유지하고 **저장**을 클릭
- 동기화 시작을 위해 **동기화 시간** 동기화를 클릭 – 5분 뒤에 동기화 시작됨. 경고 및 로그는 선택한 설정에 따라 5분 후에 보고됨
- **서버 현재 시간** 업데이트를 위해 **현재 시간 갱신** 클릭



14.2.2. IP 구성

이 섹션에서 네트워크에 정확하게 통신하는 장비를 위한 네트워크 설정을 변경할 수 있습니다.

중요: IP 주소를 변경한 후에 인터넷 브라우저를 닫고 새로운 창을 여시기 바랍니다. 그러면 Endpoint Protector 관리 및 보고 도구는 새로운 IP 주소로 액세스를 시도합니다.

14.2.3. DNS 구성

이 섹션에서 DNS 서버 주소를 변경 또는 추가할 수 있습니다. 변경 후 저장합니다.

14.2.4. 클라이언트 등록 인증서

이 섹션에서 Endpoint Protector 클라이언트 인증서 서명을 등록하고 검증할 수 있습니다. 클라이언트 인증서 등록은 추가적인 보안 조치로 인증서 기반 인증이 가능합니다.

중요: 클라이언트 등록 인증서 기능은 Linux에서는 사용할 수 없습니다.

1. 사용자 정의 인증서 설정을 실행하고 인증서 체인, Root CA, 중간 인증서를 업로드합니다;

   사용자 정의 인증서가 **사용 가능** 일 때:

   - **Endpoint Protector 서버**는 등록 단계에서 클라이언트 인증서를 승인할 것입니다.
   - **Endpoint Protector 클라이언트**는 서버 인증서를 승인하지 않을 것입니다.

   사용자 정의 인증서가 **사용 안함** 일 때"

   - **Endpoint Protector 서버**는 등록 단계에서 클라이언트 인증서를 승인하지 않을 것입니다.
   - **Endpoint Protector 클라이언트**는 서버 인증서를 승인하지 않을 것입니다.

2. 테스트 인증서 설정을 사용하고 **certificate singed by root CA just for testing the signature** (예: Endpoint Protector 인증서)를 업로드 합니다.

3. **저장**을 클릭하고 정보 인증을 위해 2분을 허용합니다. 사용자 정의 인증서가 추가가 성공적으로 확정되었다는 메시지를 볼 수 있습니다. 테스트 인증서는 승인됩니다.

   중요: 클라이언트 등록 승인 인증서와 Endpoint Protector 서버 인증서는 반드시 같은 CA에서 발급되어야 합니다.

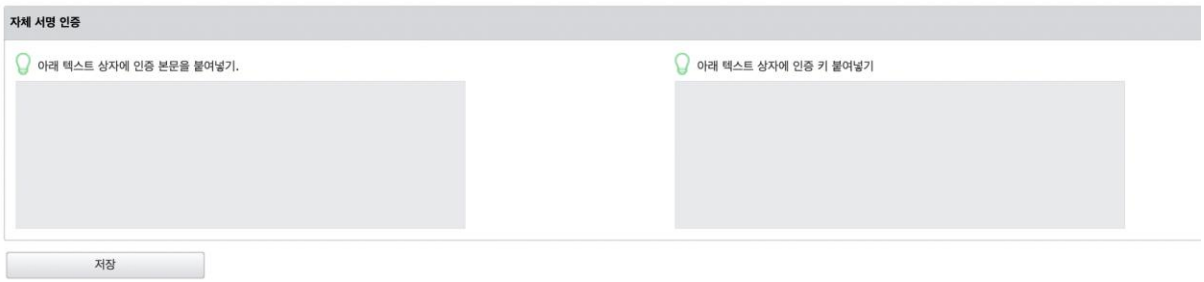
   이 기능 동작을 위해서 엔드포인트에 배포된 root CA로 서명된 암호화 식별이 되어야 합니다.

- **macOS**에서 이러한 식별은 "My Certificates" 섹션에 System Keychain에 추가되어야 합니다.
- **Windows**에서 이러한 식별은 Certificate Manger의 로컬 Computer₩Certificates₩Personal 섹션에 위치해야 합니다.

14.2.5. 자체 서명 인증

이 섹션에서 사용자 정의 인증서 설정을 할 수 있습니다.

이렇게 하기 위해서는 **본문**과 **키** 텍스트 상자에 **.pem** 인증서의 콘텐츠를 복사 및 붙여넣기 합니다.



14.2.6. 서버 인증서 유효성 검사

이 섹션에서 서버 인증서 유효성 검사를 구성하여 EPP 클라이언트의 모든 통신 요청에 사용되는 인증서의 유효성을 검사할 수 있습니다. 이 기능은 다양한 Endpoint Protector 제품 간의 보안 통신을 유지하는데 매우 중요합니다.

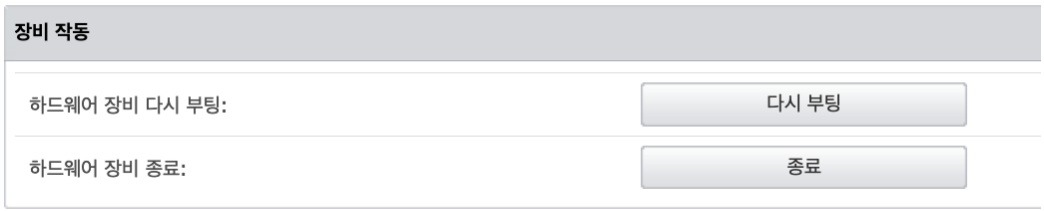
참고: 모든 인증서 유효성 검사 상태는 EPP 서버에 보고되고 디버깅 목적으로 EPP 클라이언트 로그에 저장됩니다.

중요: 인증 유효성 검사에 부적절한 인증서를 사용하면 EPP 클라이언트와 EPP 서버 간의 통신이 중단될 수 있으므로 이 기능은 책임감을 가지고 사용하시기 바랍니다.

중요: 5.9.0.0 릴리스 (Windows용 6.0.x.x; macOS용 2.8.3.x; Linux용 2.2.0.x) 버전 이상 부터 이 옵션을 활성화하면 EPP 클라이언트에서 모든 통신 요청에 대해 EPP 서버 인증서 유효성 검사를 활성화합니다. 통신에 사용되는 인증서가 유효하고 신뢰할 수 있는지 확인하여 EPP 환경의 보안을 강화할 수 있습니다.

14.2.7. 장비 작동

이 섹션에서 다시 부팅 또는 종료와 같은 장비 작동을 수행할 수 있습니다.



14.2.8. 개발사 원격지원

이 섹션에서 SSH 프로토콜을 통해서 장비에 사용자가 접근할 수 있도록 관리합니다.

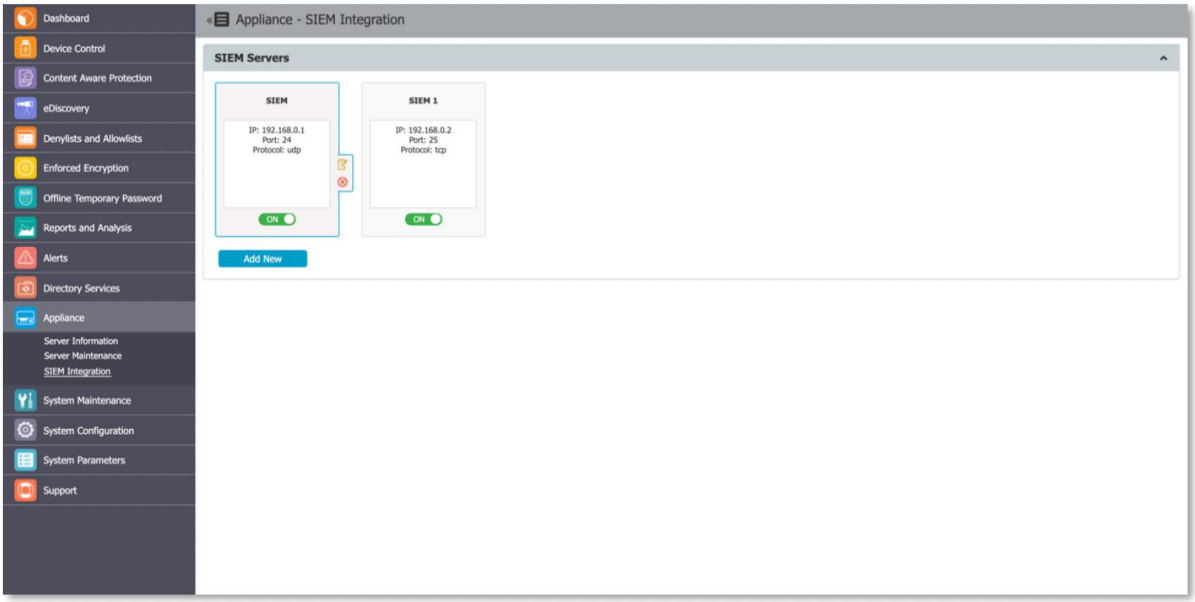
참고: 지원 요청 전에 이 설정을 사용으로 변경할 것을 권장합니다.

14.3. SIEM 연결

SIEM(Third-party security information and event management) 도구는 네트워크 장치 및 소프트웨어로 생성된 로깅 및 생성된 로그 분석을 할 수 있습니다. SIEM 연결은 보고 및 분석을 위해 Endpoint Protector가 활동 이벤트를 SIEM 서버로 전송할 수 있도록 합니다.

이 섹션에서 이미 존재하는 SIEM 서버 연동을 추가, 수정, 삭제할 수 있습니다. SIEM 서버 수정 또는 삭제를 위해서 사용 가능한 SIEM 서버 연결 선택이 필요합니다.

중요: SIEM 서버 연결은 최대 4대까지 구성할 수 있습니다.



SIEM 서버 클릭을 만들기 위해서 **새로 추가**를 클릭하고 다음 정보를 제공합니다.

- **SIEM 상태** – SIEM 서버 켬/끔 을 토글 스위치
- **로깅 사용 중지** – 로깅 켬/끔 을 토글 스위치

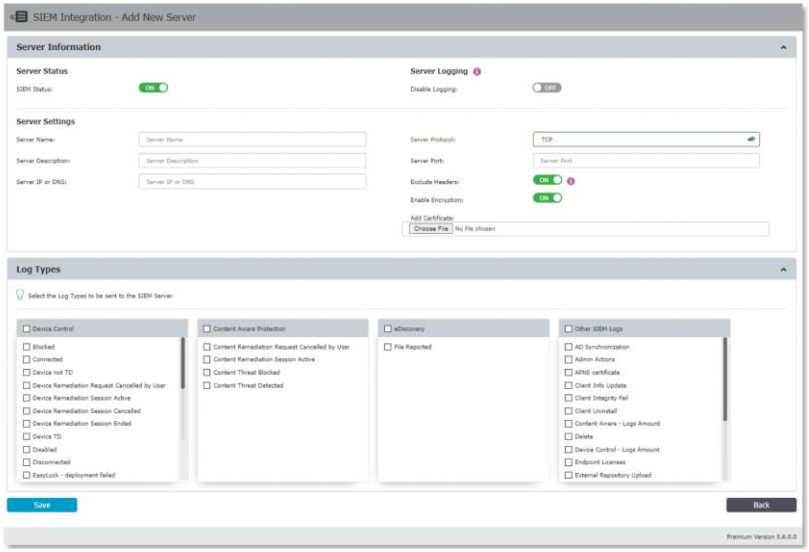
  참고: 로깅을 사용하지 않으면 로그는 Endpoint Protector 서버에 저장되고 사용하면 SIEM 서버에 저장합니다.

- **서버 이름** – 서버 이름 추가
- **서버 설명** – 설명 추가

- **서버 IP 또는 DNS** – IP 또는 DNS 추가
- **서버 프로토콜** – UDP 또는 TCP 서버 프로토콜 선택

  참고: 프로토콜 기반으로 SIEM 암호화 사용을 선택합니다.
- **서버 포트** – 포트 추가
- **헤더 제외** – 로그 헤드 켬/끔 토글 스위치

  참고: 로그 헤더를 사용하지 않으면 SIEM에 데이터만 내보내기 됩니다.
- **로그 종류** – 로그를 SIEM 서버에 보내는 사용 가능한 옵션에서 선택



중요: Endpoint Protector의 SIEM 연결 기능에 특정 제한이 있다는 점에 유의하시기 바랍니다. 이 SIEM 연결의 최신 기능을 사용하려면 사용자 환경이 특정 기준을 충족해야 합니다. EPP 버전 5.6.0.0 또는 최신 버전으로 설치되어 있어야 하며 활성화된 HTTPS 연결을 유지해야 합니다. 이러한 엄격한 전제 조건을 충족하는 환경에서만 SIEM 연결에 액세스할 수 있다는 점에 유의하시기 바랍니다.

14.3.1. SIEM 암호화

TCP 프로토콜을 사용할 때 각 SIEM 서버에 통신을 암호화하는 옵션을 가지고 있습니다. **암호화** 설정을 사용하고 .pem 포맷으로 SIEM 서버를 위한 서버 인증서 서명에 사용한 **root CA 업로드**

합니다.

중요: SIEM 서버에 사용된 인증서는 EPP 서버에 업로드 된 인증서로 같은 CA로 서명이 되어야 합니다. Endpoint Protector는 아래를 확인합니다:

- CA로 서명된 SIEM 인증서 그리고 CN 또는 SAN은 SIEM 머신 이름으로 일치됩니다.
- Root CA의 Basic Constraint CA 설정은 true 입니다.

인증서 승인 시 전체 인증서 체인은 CA 인증서를 포함해서 반드시 유효해야 합니다. 만약 인증서 체인 중 하나가 유효하지 않으면 연결은 거절됩니다.

만료될 때 인증서 파일을 업데이트 하시기 바랍니다.

참고: Live Update 옵션을 사용하여 최신 패치를 적용하면 SIEM 암호화 설정은 보이지 않을 수 있습니다. 지원팀에 연락하시기 바랍니다.

15. 시스템 유지 관리

15.1. 파일 유지 관리

이 모듈은 관리자가 Endpoint Protector 서버에 사용된 파일을 검색/구성 및 정리할 수 있습니다.

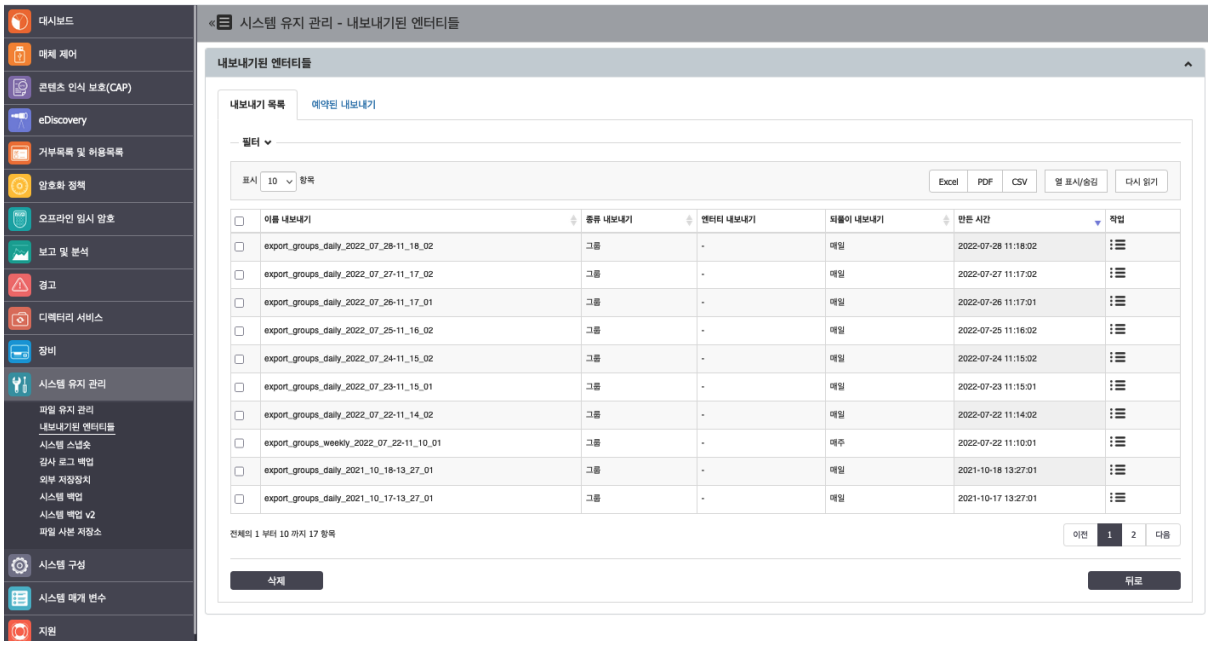
아래 옵션을 가지고 있습니다:

- **파일보관:** 선택된 컴퓨터에서 사본보고나 파일의 압축과 삭제를 허용합니다.
- **로그 백업 파일:** 이전에 백업된 로그 파일의 압축과 삭제를 허용합니다.

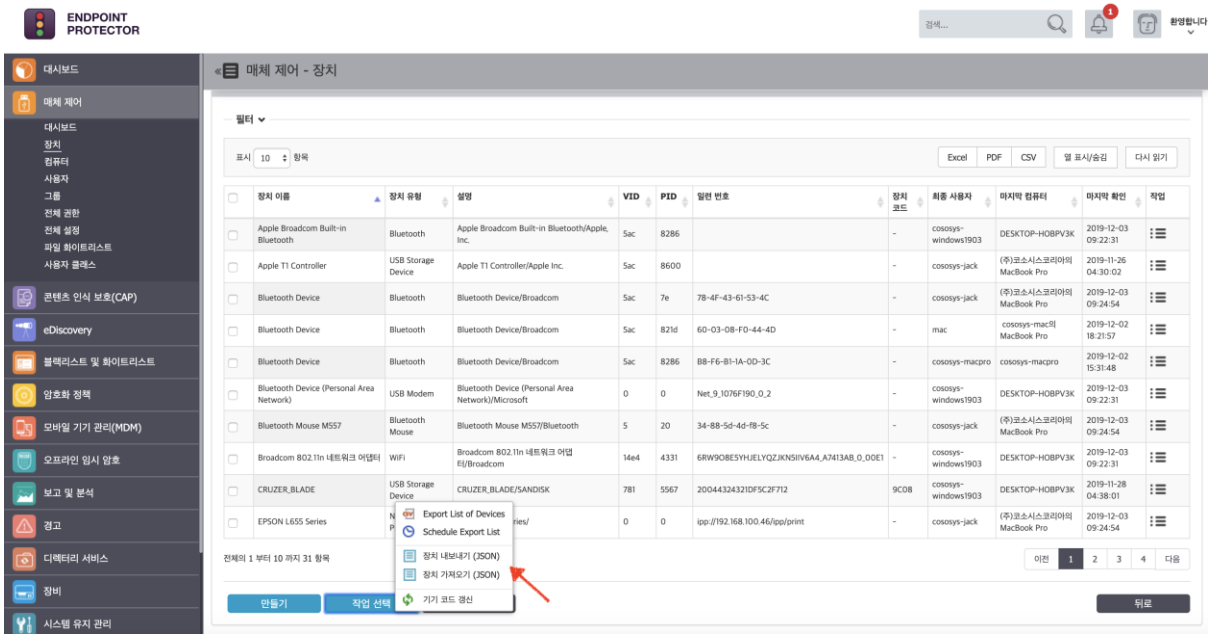
선택된 파일을 압축하려면 **Zip으로 저장**을 클릭하고 영구히 삭제하려면 **삭제**를 클릭합니다.

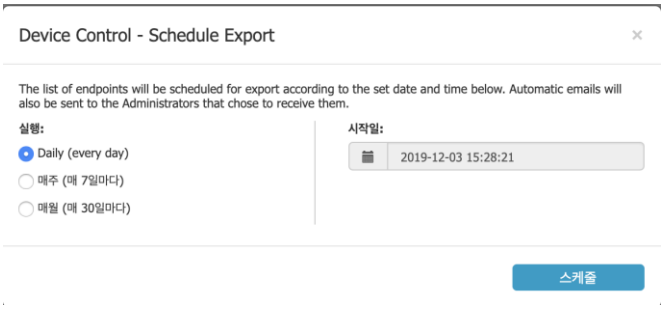
15.2. 내보내기 된 엔터티들

이 섹션에서 관리자는 내보내기 된 엔터티 목록을 볼 수 있고 다운로드 또는 삭제 할 수도 있을 뿐만 아니라 시스템에서 내보내기 목록을 예약할 수 있습니다.



'매체 제어 > 장치 목록 / 컴퓨터 목록 / 사용자 목록 / 그룹 목록' 을 수동으로 만들거나 예약 설정으로 만들 수 있습니다.





예약 내보내기는 **예약 내보내기 경고**가 설정된 모든 관리자의 이메일에 자동으로 보내집니다.

예약 내보내기는 매일, 매주, 매월 단위로 설정이 가능하고 Endpoint Protector 서버에 계속해서 저장됩니다.

성능을 유지하기 위해서 이러한 내보내기가 원하는 관리자에게 자동으로 이메일로 보낸다면 이미 만들어진 예약 내보내기는 14일 후에 서버에서 자동으로 삭제됩니다.

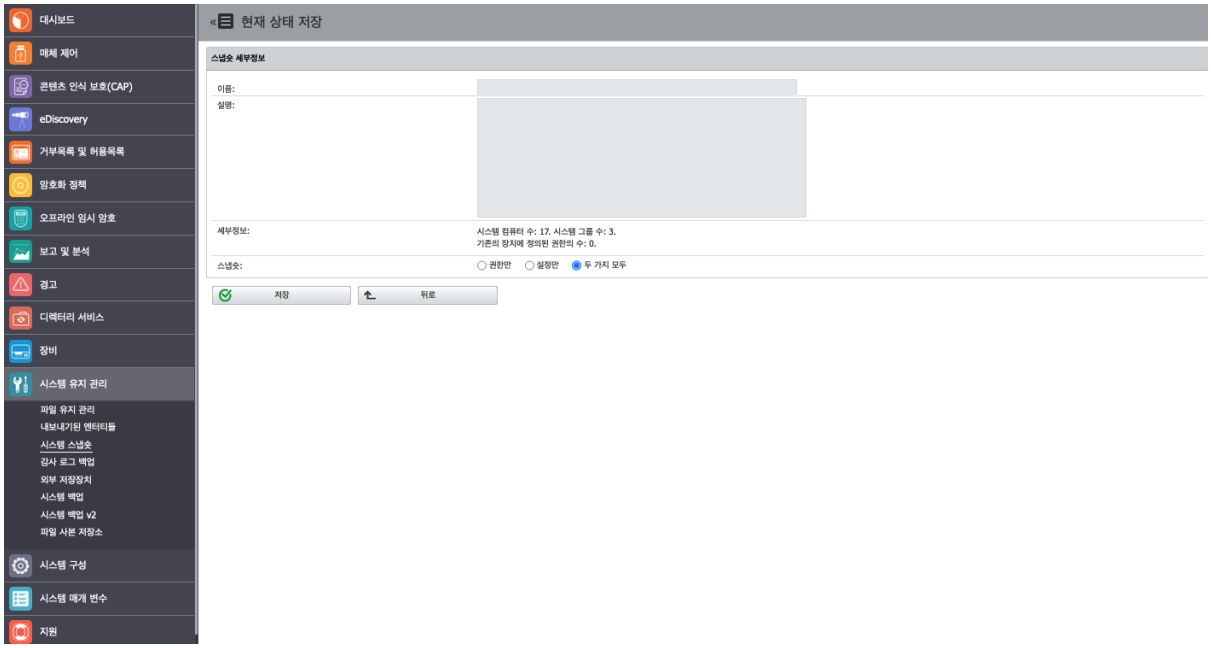
성능 관리 목적으로 예약된 내보내기와 로깅 사용 중지 옵션은 관리자가 Endpoint Protector 서버에 로그를 보관할 것인지 아니면 SIEM 서버에만 보관할지 결정할 수 있습니다.

15.3. 시스템 스냅숏

시스템 스냅숏 모듈에서는 모든 장치 제어 권한 및 설정을 시스템에 저장했다가 나중에 필요할 때 복원할 수 있습니다.

중요: Endpoint Protector 서버 설치 후 어떤 것이라도 수정하기 전에 시스템 스냅숏을 만들 것을 강력하게 권장합니다. 만약 서버가 잘못된 구성으로 변경이 되었을 때 원래 설정으로 되돌릴 수 있습니다.

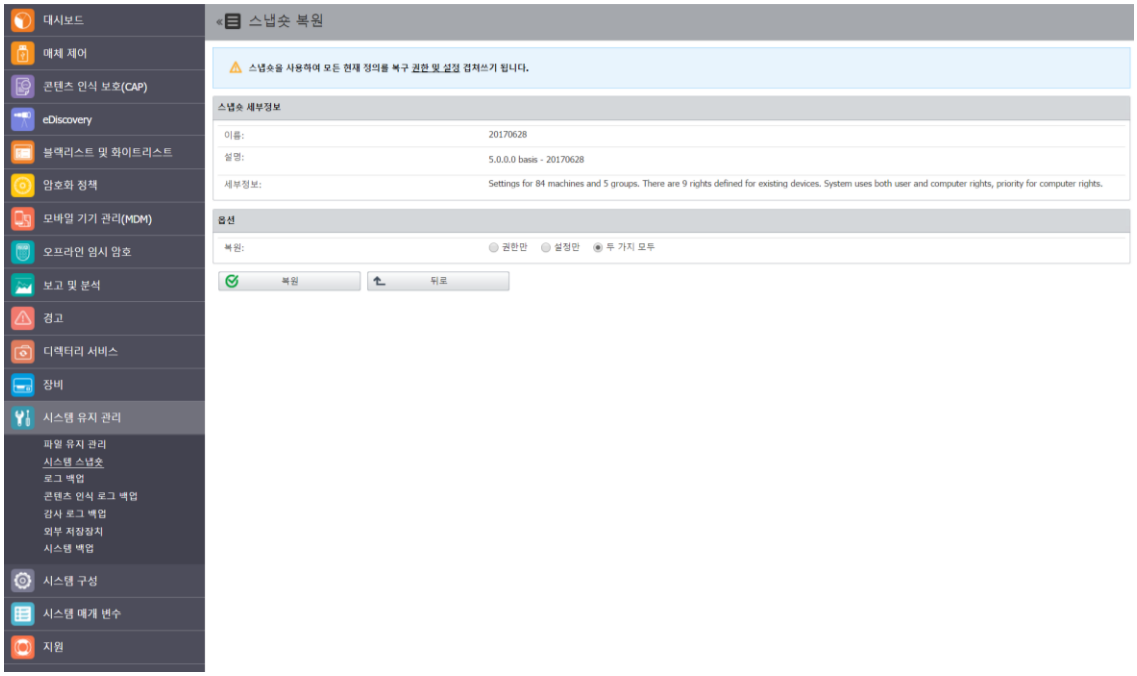
시스템 스냅숏을 만들기 위해서는 시스템 구성으로 이동한 후 **스냅숏 만들기**를 클릭합니다.



스냅숏 이름과 설명을 입력합니다. 또한 스냅샷에 저장할 항목을 **권한만**, **설정만** 또는 **두가지 모두** 중에서 선택하고 **저장**합니다.

시스템 스냅샷에 생성된 스냅샷이 나타납니다.

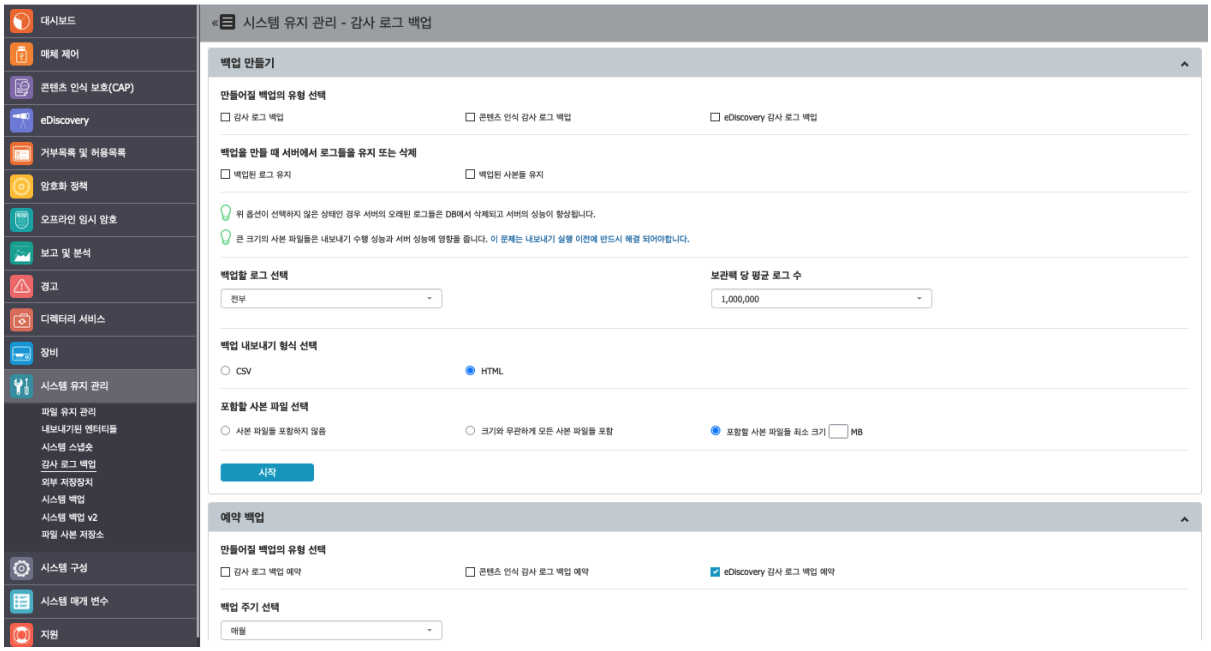
이전에 생성된 스냅샷을 복원하려면 원하는 스냅샷 옆에 있는 **복원** 버튼을 클릭합니다.



15.4. 감사 로그 백업

로그 백업과 콘텐츠 인식 로그 백업과 비슷하게 이 섹션은 오래된 로그를 저장하고 내보내기 할 수 있습니다. 이 옵션은 백업 목록 보기 또는 백업 스케줄러 보기 옵션 뿐만 아니라 내보내기 하는 로그의 수 및 파일 크기를 선택이 가능합니다.

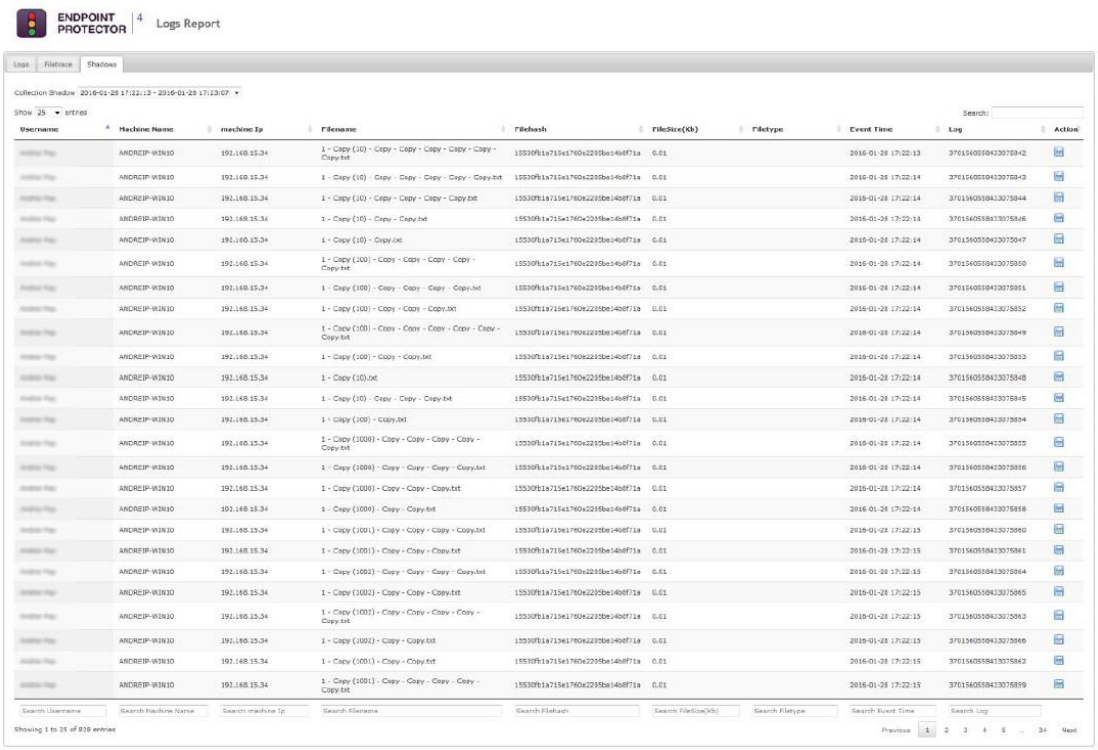
감사 로그 백업과 감사 백업 스케줄러 둘 다 얼마나 오래된 로그를 포함하는지 서버에 로그를 저장하는지 삭제하는지 파일 보관을 포함하는지 아닌지 등에 대한 여러가지 옵션을 제공합니다.



그러나 주요 다른 점은 내보낸 로그가 향상된 시각화 모드를 가진다는 사실 입니다. 이는 임원들이 쉽게 감사할 수 있는 리포트로 만듭니다.

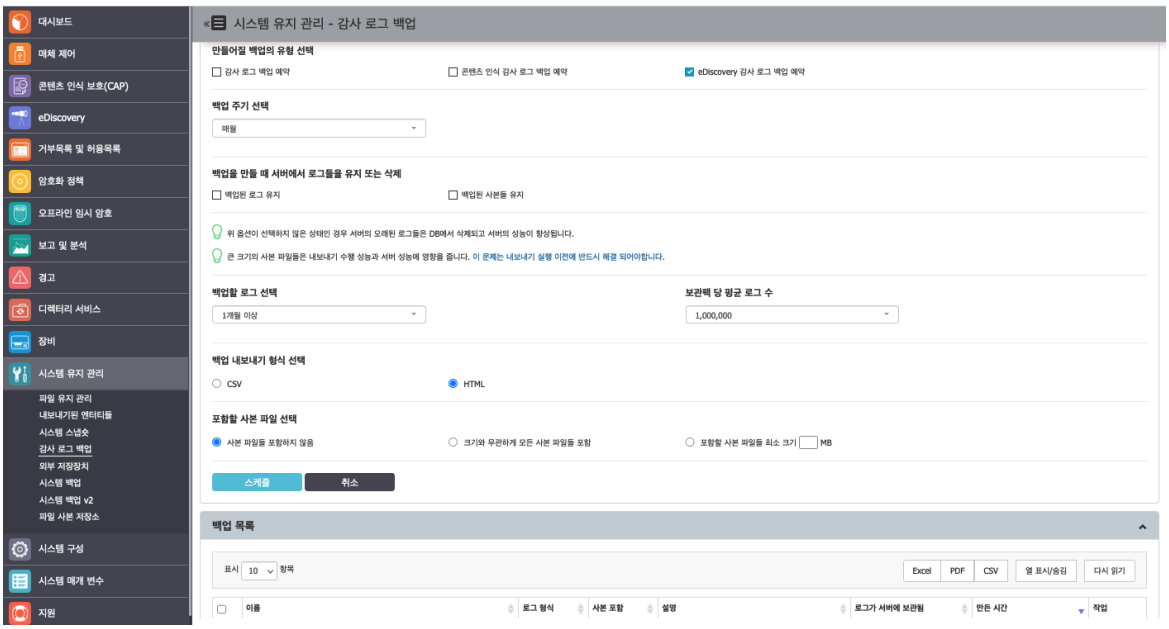
CSV 파일로 백업 내보내기는 사용하는 Endpoint Protector 서버 버전에 따라 다릅니다:

- Endpoint Protector 5.6.0.0 또는 이전 버전이라면 CSV 파일는 발견된 각 위협에 대한 파일을 보고합니다.
- Endpoint Protector 5.7.0.0 이면 발견된 모든 위협을 포함하는 하나의 파일만 있고 밑줄로 구분됩니다.



15.4.1. 감사 로그 백업 스케줄

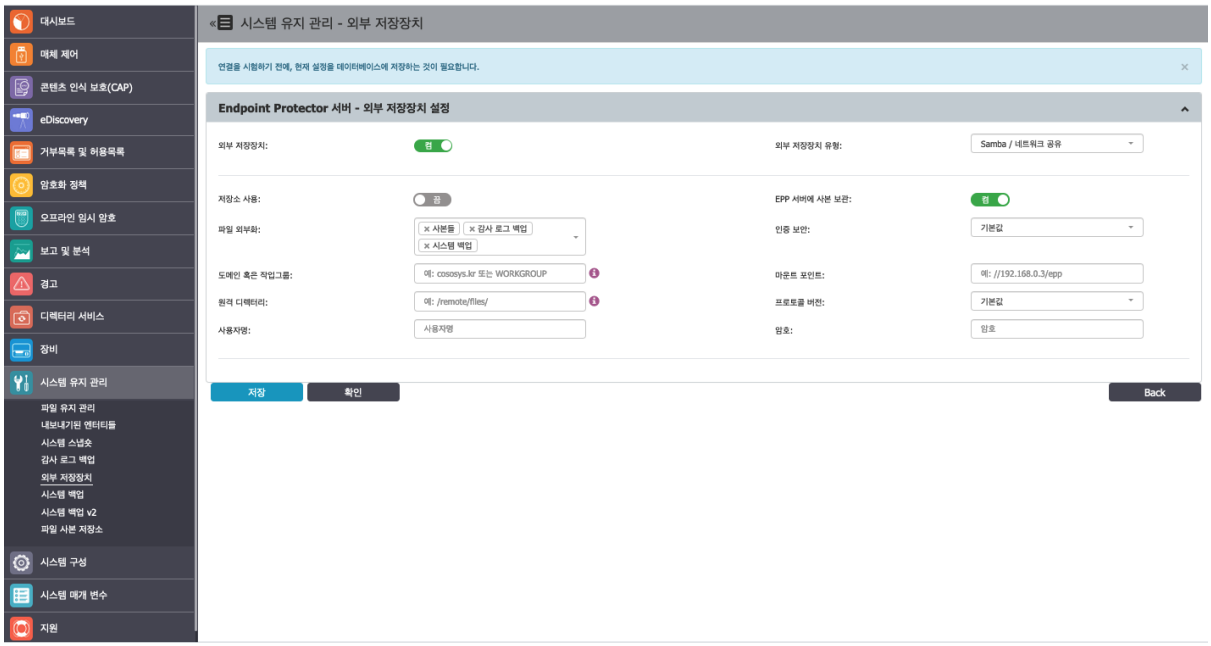
감사 로그 백업은 백업을 즉시 시작하는 반면에 감사 로그 백업 스케줄러는 특정 시간과 백업 주기 프로시저를 설정하는 옵션을 제공합니다. (매일, 매주, 매월, 6개월, 매년 등)



15.5. 외부 저장장치

외부 저장장치 옵션은 관리자가 Endpoint Protector로 만들어진 로그 백업 파일과 보관 파일을 네트워크를 통해서 특정 저장 디스크에 저장 할 수 있습니다. FTP, SFTP, Samba / 네트워크 공유 서버를 지원 합니다.

모든 외부 저장장치 유형에 Endpoint Protector에 파일 복사를 유지하는 옵션을 사용할 수 있습니다.

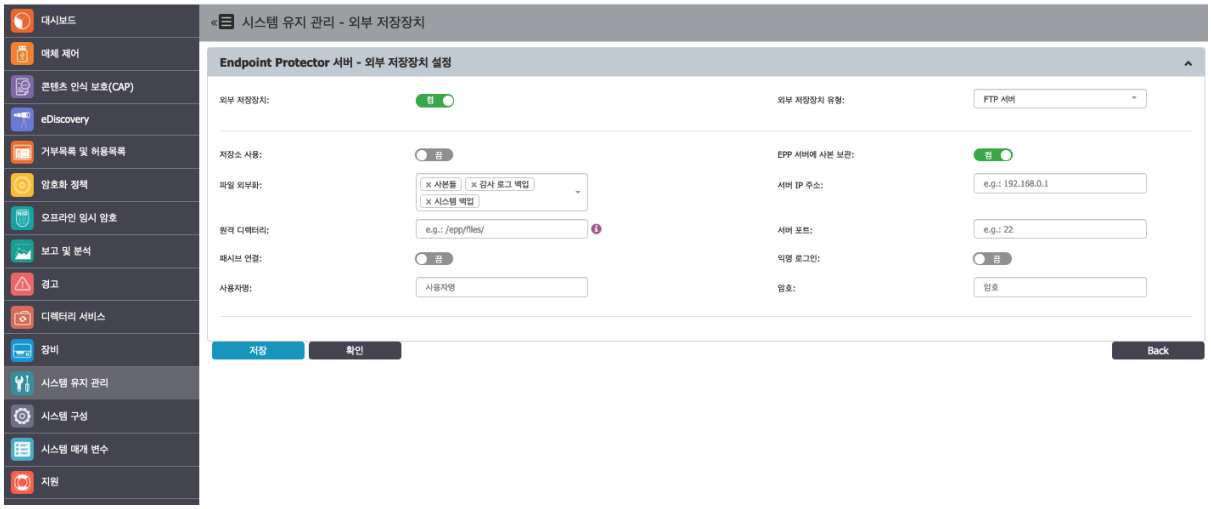


15.5.1. FTP 서버

FTP 서버를 설정하기 위해서 다음의 매개 변수가 필요합니다.

- **파일 외부화** – Endpoint Protector 파일: 사본들, 감사 로그 백업, 시스템 백업
- **서버 IP 주소** – 외부 서버의 IP
- **원격 디렉터리** – 외부 디렉터리의 특정 위치
- **사용자명** – 외부 서버의 사용자 이름

- **암호** – 관련 암호
- **외부 저장장치**
- **서버 포트**
- **패시브 연결**
- **익명 로그인**

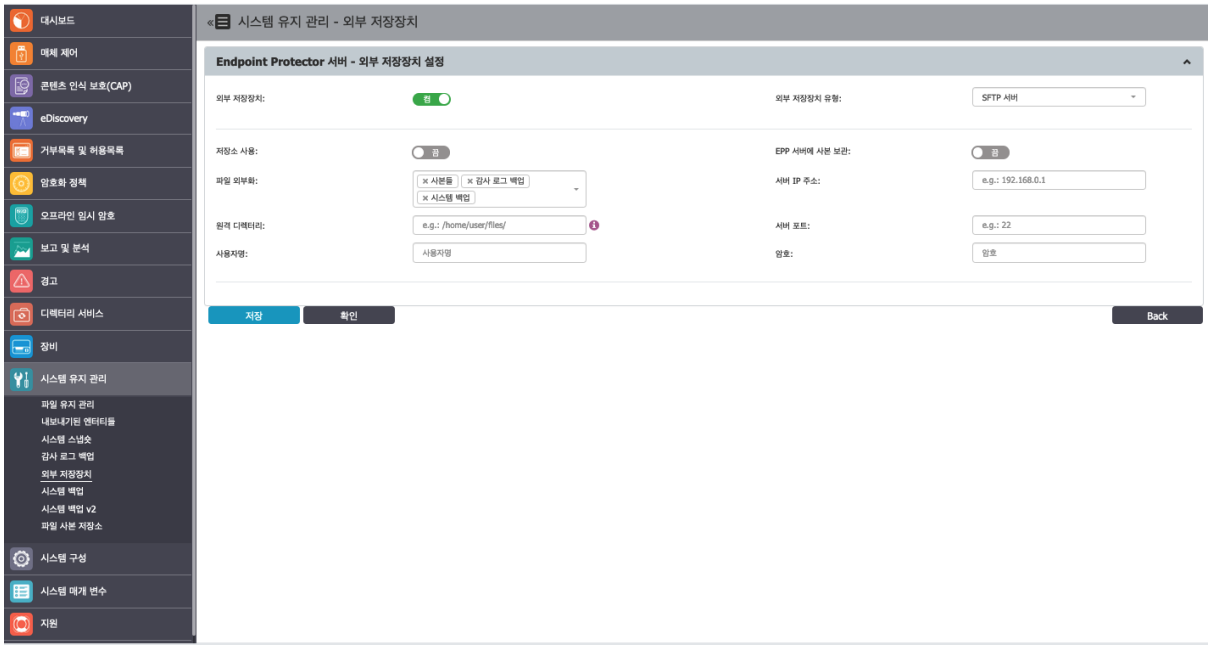


15.5.2. SFTP 서버

SFTP 서버를 설정하기 위해서 다음의 매개 변수가 필요합니다.

- **파일 외부화** – Endpoint Protector 파일: 사본들, 감사 로그 백업, 시스템 백업
- **서버 IP 주소** – 외부 서버의 IP
- **원격 디렉터리** – 외부 디렉터리의 특정 위치
- **서버 포트** – 외부 저장 서버의 포트
- **사용자명** – 외부 서버의 사용자 이름
- **암호** – 관련 암호

- **저장소 사용**

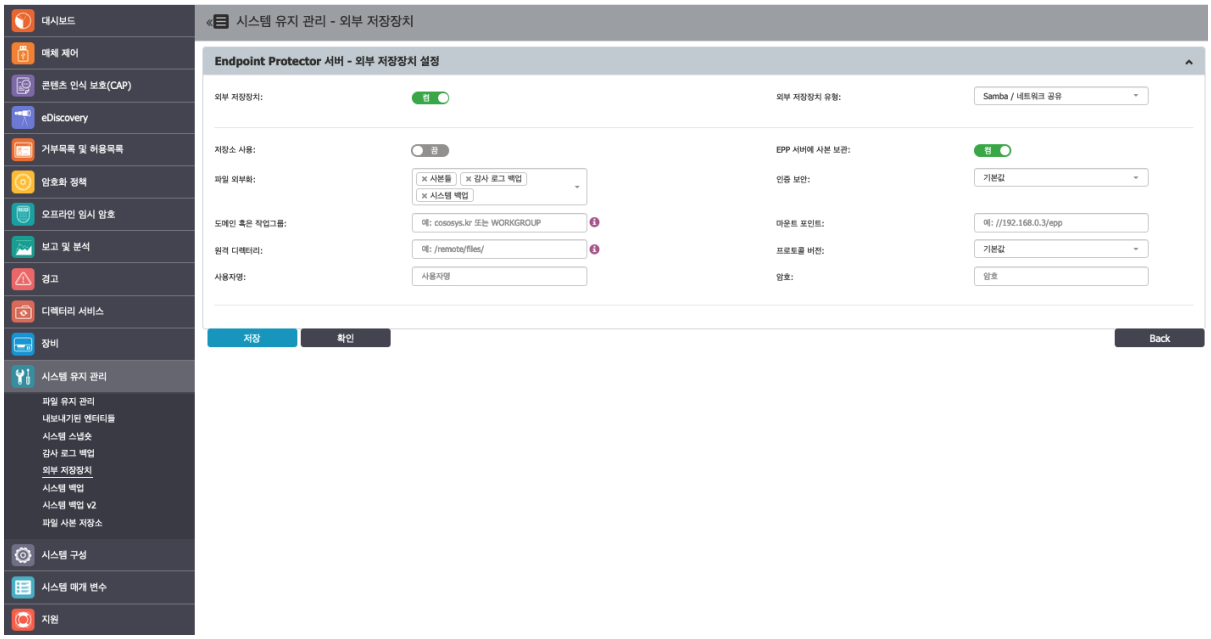


15.5.3. Samba / 네트워크 공유

Samba / 네트워크 공유 서버를 설정하기 위해서 다음의 매개 변수가 필요합니다.

- **저장소 사용**
- **EPP 서버에 사본 보관** – 이 설정을 사용하면 Endpoint Protector 서버에서 저장소 백업
- **파일 외부화** – Endpoint Protector 파일: 사본들, 감사 로그 백업, 시스템 백업
- **EPP 서버에 사본 보관** – 이 설정은 Endpoint Protector 서버의 스토리지 백업을 만들 수 있음
- **인증 보안** – 보안 프로토콜: 기본값, NTLM, NTLMv2, NTLMSSP
- **도메인 또는 작업그룹** – 적용될 때만 사용
- **마운트 포인트**

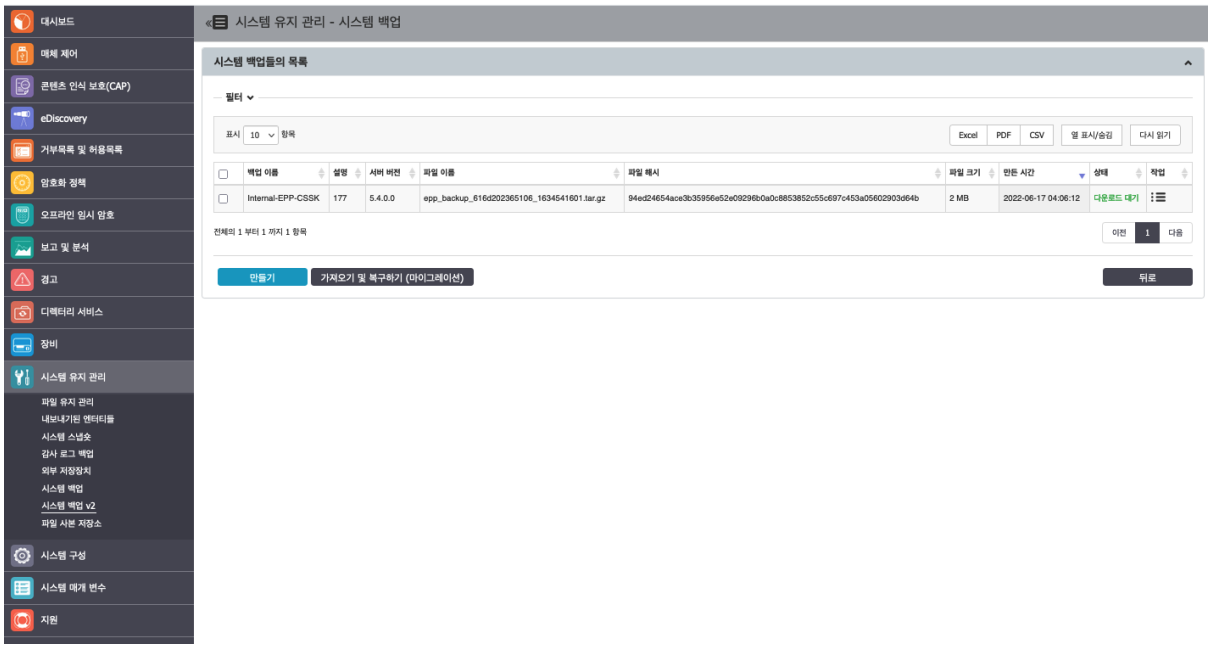
- **원격 디렉터리** – 외부 디렉터리의 특정 위치
- **서버 IP 주소** – 외부 서버 IP
- **원격 디렉토리** – 외부 디렉토리의 특정 위치
- **프로토콜 버전**
- **사용자 이름** – 외부 서버의 사용자 이름
- **암호** – 관련된 암호



15.6. 시스템 백업

15.6.1. 시스템 백업 (웹 인터페이스)

이 모듈은 관리자가 완전하게 시스템 백업을 수행하는 것을 허용합니다.

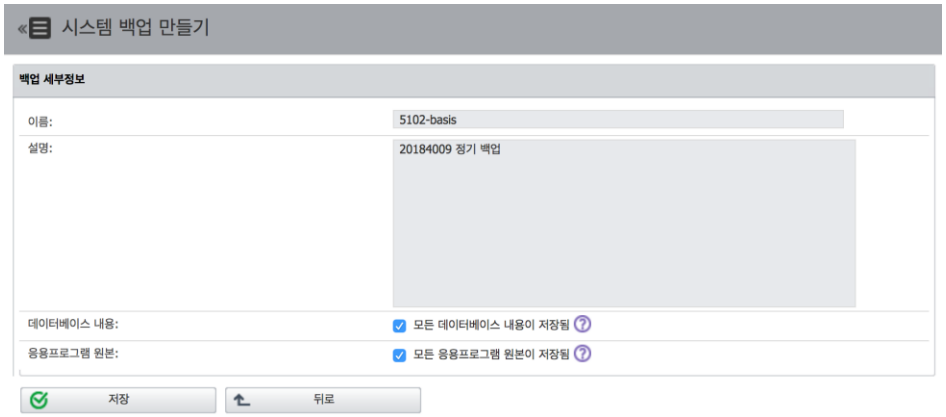


현재 시스템 백업 목록을 보기 위해서 **시스템 유지 관리 > 시스템 백업 v2** 로 이동합니다.

시스템 백업을 복원하려면 **복원**을 클릭하고 다음 동작을 확인합니다.

중요: 삭제하면 백업은 복구될 수 없습니다.

다운로드 버튼은 로컬 드라이브에 **.eppb** 백업 파일을 저장합니다. 파일이 저장을 기록하는 것을 권장합니다.

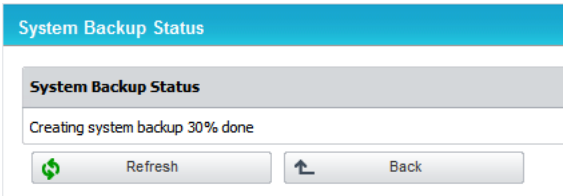


백업 만들기에서 아래 두 옵션을 선택할 수 있습니다:

- **데이터베이스 내용 저장** – 이 옵션은 EPP 서버있는 모든 장치, 권한, 로그, 설정, 정책의 백업 파일을 포함합니다.
- **응용프로그램 소스 저장** – 이 옵션은 EPP 클라이언트 및 서버의 적절한 다른 기능과 같은 파일을 포함하는 백업입니다.

참고: 시스템 백업은 IP 주소, 파일 사본보관, 임시 로그파일은 포함하지 않습니다.

두 번째 메뉴는 **상태**는 시스템의 현재 상태를 보여줍니다. 만약 백업이 생성 중이라면 아래와 같은 화면이 보입니다.



만약 시스템이 유휴 상태인 경우 버튼은 마지막으로 알려진 상태로 반환됩니다. 이 상태는 기본적으로 100% 완료로 설정됩니다.

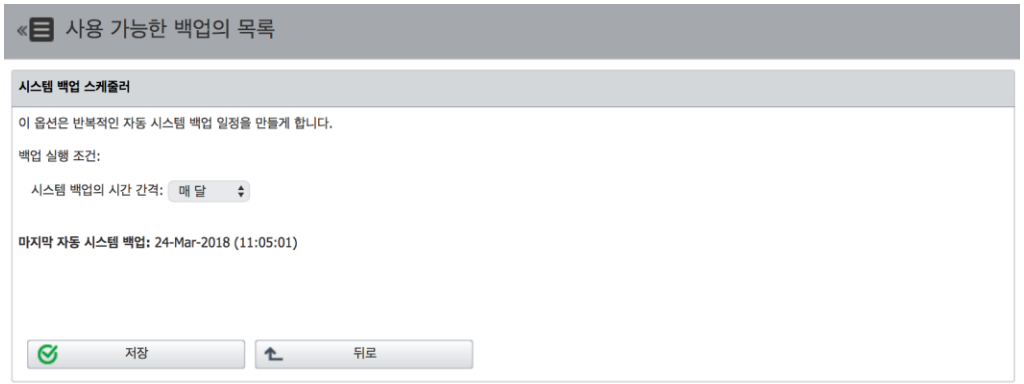
다음 메뉴인 **업로드**로 관리자는 로컬 파일 시스템에서 **.eppb** 파일을 올릴 수 있습니다. 이 기능은 **서버** 이관 또는 손상 복원에 매우 유용합니다. 아래와 같은 화면을 볼 수 있습니다.

중요: 200 MB 가 넘는 Endpoint Protector 백업 파일 (.eppb)은 어플라이언스 콘솔로만 업로드가 가능합니다. .eppb 파일이 200 MB 넘으면 담당 지원팀에 연락하시기 바랍니다.

이 섹션에서 **시스템 백업 시간 간격**을 설정할 수 있는 자동 백업 루틴의 시간을 정할 수 있습니다. 이 루틴은 매일, 매주, 매월 등으로 설정할 수 있습니다.

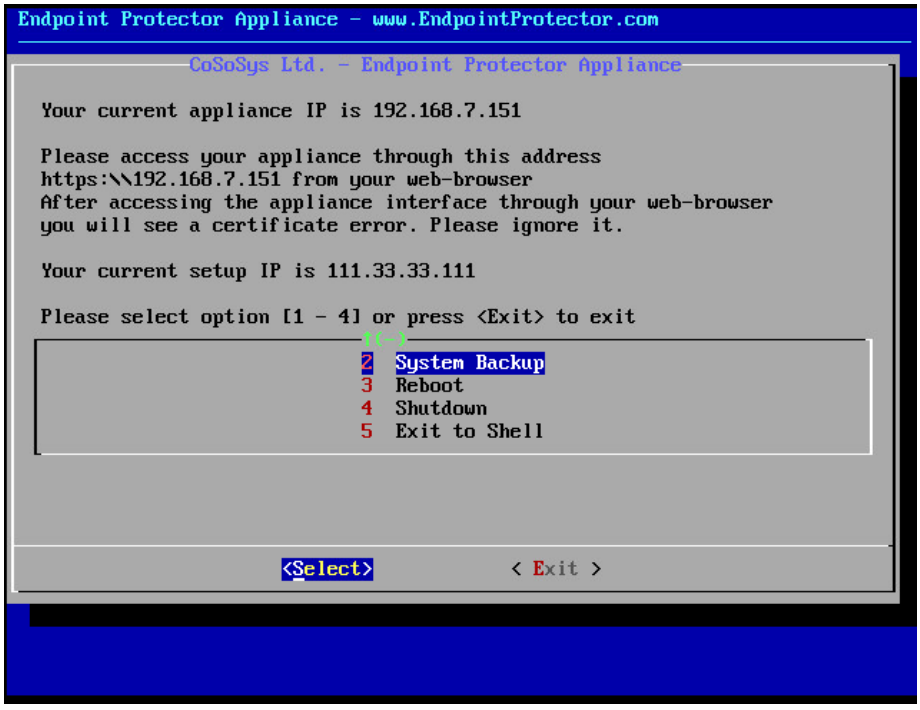
스케줄러는 **마지막 자동 시스템 백업 리마인더**로 관리자에게 알려 줍니다.

참고: 손실을 예방하기 위해서 스케줄 루틴을 권장합니다.



15.6.2. 시스템 백업 (콘솔)

Endpoint Protector는 초기 구성을 하는 관리자 콘솔에서 이전 상태로 시스템을 돌리는 옵션을 제공합니다.

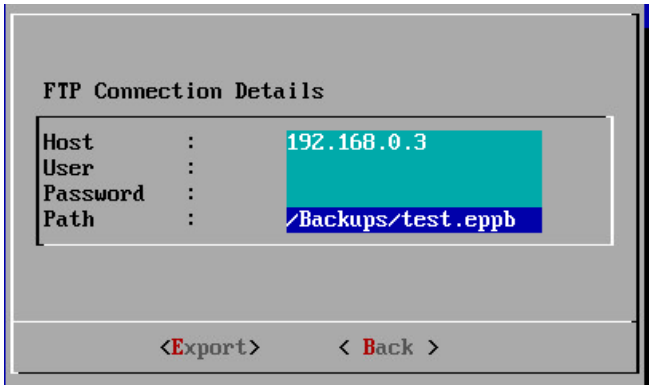


2번 메뉴를 통해 관리자는 다음 옵션을 사용할 수 있습니다.

1. **시스템 복원** – 웹 인터페이스를 이용하여 시스템 백업이 되어 있으면 수행할 수 있습니다.
2. **가져오기** - .epp 파일이 다운로드 되었거나 FTP 서버에 저장되어 있다면 수행할 수 있습니다.
3. **내보내기** – FTP 서버에 지금 백업을 저장하기 위해 수행할 수 있습니다.

.epp 파일을 가져오거나 내보내기 위해서 관리자는 FTP 서버 IP와 .eppb 파일의 파일 시스템 안의 경로를 가지고 있어야 합니다.

아래 예제를 보시기 바랍니다.



15.7. 시스템 백업 v2

이 섹션에서 관리자는 데이터베이스 (객체, 권한, 설정, 정책, 구성 등)을 오래된 Endpoint Protector 서버에서 새로운 서버로 마이그레이션 할 수 있습니다.

참고: 이 기능은 시스템 백업 기능을 대체하는 것이 아니라 오래된 Endpoint Protector 이미지를 5.2.0.6 버전으로 시작하는 새로운 서버에 마이그레이션하는 도구로 만들어졌습니다.

오래된 서버와 새로운 서버 버전이 같아야 합니다. 마이그레이션 전에 같은 버전이 되도록 맞추어야 합니다. (예: 5206으로 오래된 서버를 업그레이드해서 막 배포된 새로운 서버와 버전을 맞추

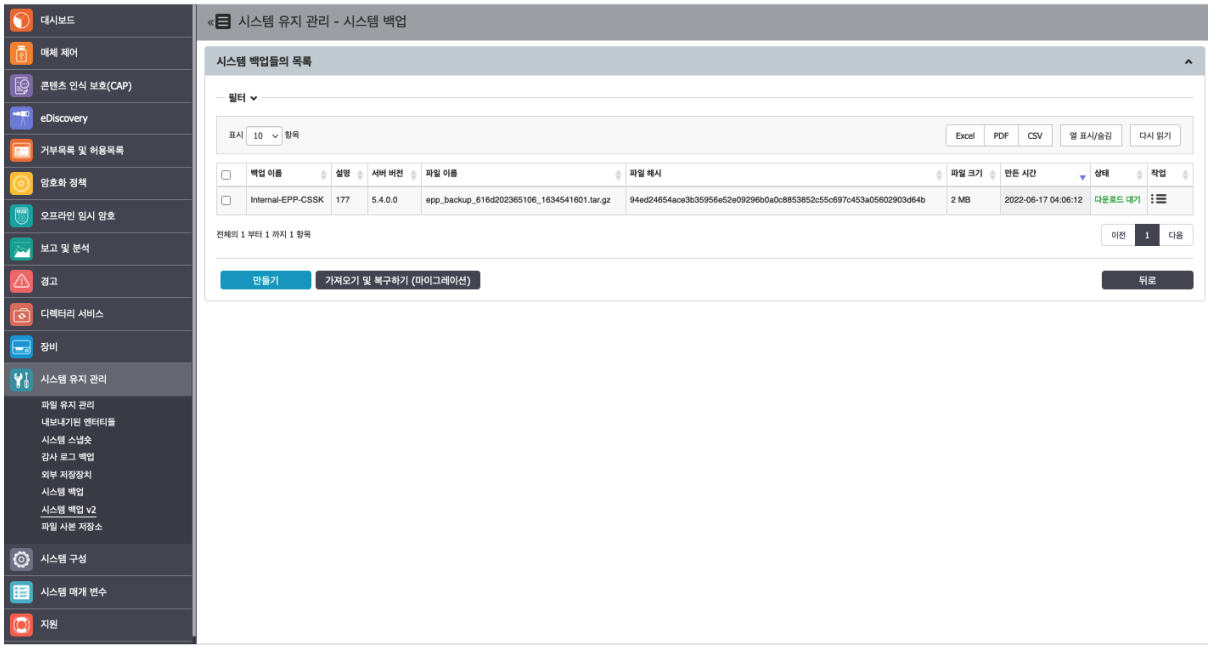
어야 합니다.).

로그, 감사 로그 또는 시스템 백업은 여기에 포함되지 않습니다. 필요하다면 시작하기 전에 다운로드 하시기 바랍니다.

예:

초기 Endpoint Protector 배포 버전은 4.4.0.7 이었습니다. 시간이 지나면서 라이브 업데이트 섹션을 통해서 업데이트가 적용되고 Endpoint Protector 버전 5.2.0.6으로 시작하는 어플라이언스가 되었습니다. 이러한 업데이트는 항상 패치와 보안 업데이트가 포함되지만 새로운 핵심 OS 버전의 완전한 롤아웃을 포함하지 않습니다 (예: 어플라이언스는 아직도 Ubuntu 14.04 LTS에서 운영됩니다.).

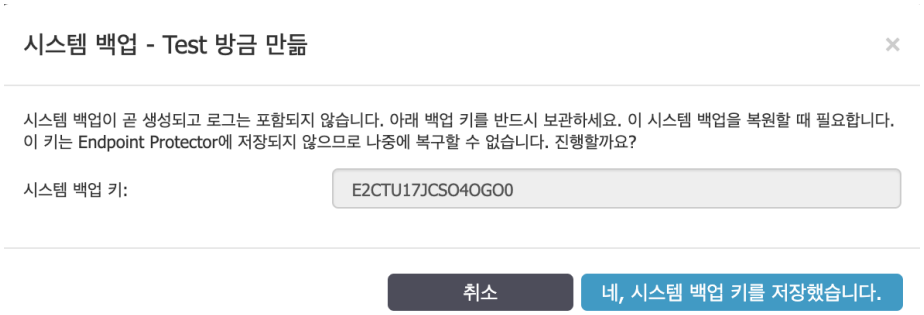
2019년에 Ubuntu 14.04는 더 이상 보안 패치를 받을 수 없기 때문에 최신 Ubuntu LTS 버전으로 운영되는 서버에 마이그레이션 작업을 할 때 이 기능을 활용하시면 됩니다.



15.7.1. 시스템 백업 v2 만들기 (마이그레이션)

관리자는 **시스템 유지 관리 > 시스템 백업 v2** 섹션에서 새로운 마이그레이션 백업을 만들 수 있습니다. 이름과 설명이 입력해야 합니다.

참고: 보안을 이유로 시스템 백업 키는 Endpoint Protector에 저장되지 않습니다. 시작하기 전에 적절한 곳에 저장하시기 바랍니다.



15.7.2. 가져오기 및 복원

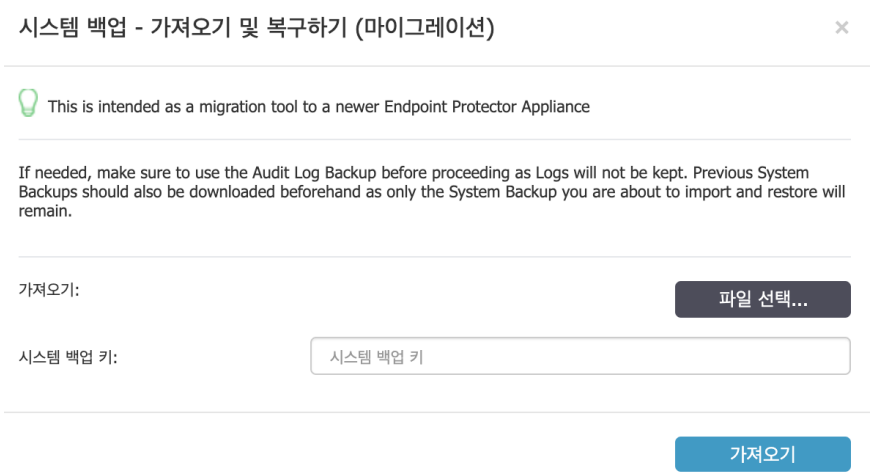
백업은 같은 Endpoint Protector 서버에서 복원할 수 있습니다. 그러나 이 기능의 주요 사용은 더 새로운 Endpoint Protector 서버에서 가져오기 및 복원이 될 것 입니다 (5.2.0.6 보다 높은 버전).

시스템 백업의 마이그레이션 프로세스는 백업 파일 과 시스템 백업 키가 필요합니다.

참고: 필요하다면 시작 전에 시스템 백업 또는 감사 로그 백업을 다운로드해야 합니다. 이 프로세스에서는 포함되지 않습니다.

새로운 어플라이언스에 가져오기 및 복원 (마이그레이션)을 만든 후에 오래된 어플라이언스 전원을 내려야 합니다. 배포된 Endpoint Protector 클라이언트가 새로운 어플라이언스와 통신을 시작

하기 위해서 IP가 새로운 어플라이언스에 재할당 되기를 기다려야 하기 때문입니다.



15.8. 사본 보관 저장소

이 섹션에서는 관리자가 사본 보관 저장소를 관리할 수 있습니다. 이 기능은 Endpoint Protector 클라이언트가 사본 보관 파일을 바로 외부 저장소에 보낼 수 있습니다.

멀티 파일 사본 보관 저장소를 만들 수 있고 구분을 기반으로 파일 사본 보관을 각 구분 코드를 통해서 관리하는 옵션이 있습니다.

참고: Endpoint Protector에서 구분은 같은 속성에서 같은 엔터티 모음으로 정의됩니다. 조직도의 부서와 혼동해서는 안됩니다.

Endpoint Protector 5.8.0.0 버전으로 시작하면 사본 보관은 이러한 파일 전송이 첫 째로 OS 기능에 의존해서 더 macOS와 Linux에 의존적입니다.

1. Mac / Linux

- 기본: LDAP (as-is)
- 대비: curl (as-is)

2. Windows

- 기본: LDAP
- 대비: curl

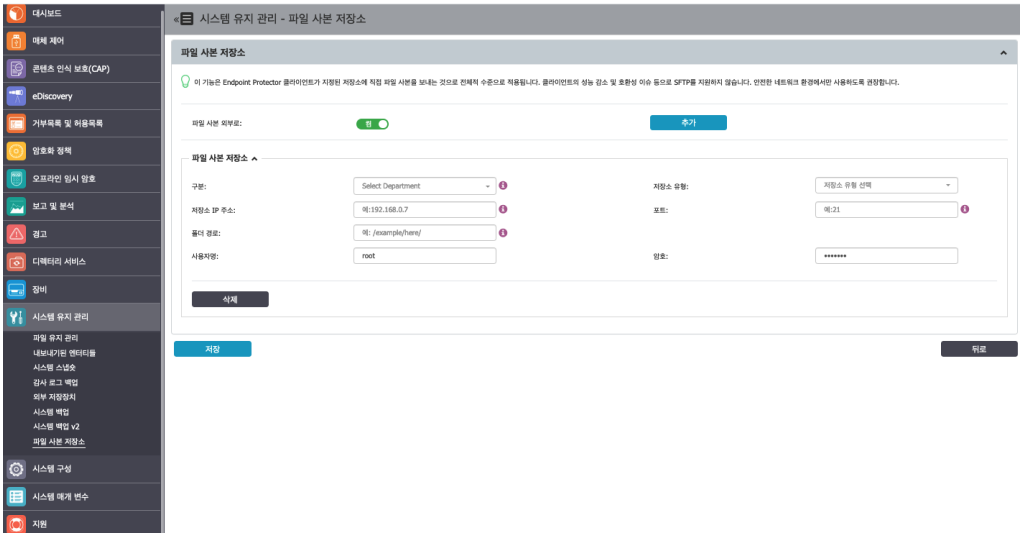
파일 사본 보관 저장소를 만들기 위해서 **추가**를 클릭하고 아래 정보를 입력합니다:

- **구분** – 파일 사본 보관 저장소에 하나 또는 여러 구분을 할당합니다.
- **저장소 유형** – FTP, Samba (smbv1), Azure File Storage, Samba (smbv2) 또는 S3 Bucket 저장소 유형을 선택합니다.

  참고: S3 Bucket 유형을 선택하면 사본 보관 저장소를 만들기 위해 요구되는 정보는 다르게 됩니다. 다음 섹션을 참조 하시기 바랍니다.

  참고: Samba 공유에 필요한 최소 권한은 750 입니다 (소유자는 전체 액세스 권한이 있고 그룹은 읽기 및 실행 권한만 있음)
- **저장소 IP 주소** – 파일 사본 저장소 IP 주소를 추가합니다.
- **포트** – 파일 사본 보관 저장소에 사용되는 포트를 추가합니다.

  참고: Samba (smbv1) 또는 Azure File Storage 및 Samba (smbv2) 저장소 포트는 정의할 필요가 없습니다.
- **폴더 경로** – 파일 사본이 저장된 폴더 경로를 추가합니다.
- **사용자 이름 및 암호** – 저장소 계정을 추가합니다.



15.8.1. 테스트 연결

"테스트" 버튼은 FTP 및 S3 Bucket 리포지토리(간접 아티팩트 검색)에 대한 확인 프로세스를 용이하게 합니다. 이 기능은 사용하면 제공된 자격 증명을 사용하여 더미 파일 업로드를 인증하고 실행할 수 있습니다.

1. **FTP 리포지토리**: '테스트' 버튼으로 인증 및 파일 업로드를 확인합니다.
2. **S3 버킷 리포지토리 (간접 아티팩트 검색)**: '테스트' 버튼은 키, 비밀키를 확인하고 인증 응답이 성공하면 버킷 영역과 이름을 확인합니다.

참고: S3 Bucket (직접 아티팩트 검색), Samba v1, Samba v2, Azure 파일 저장소 리포지토리 관련 테스트 연결은 IP 화이트리스트, smbclient 등과 같은 타사 요구 사항 때문에 지원되지 않습니다.

이 개선 사항은 각 리포지토리 유형의 특정 요구 사항을 고려하면서 FTP 및 S3 버킷 리포지토리에 대한 테스트 프로세스를 더욱 투명하고 효율적으로 만듦을 목표로합니다.

15.8.2. S3 Bucket 사본 보관 저장소

Amazon S3 bucket은 Amazon Web Services (AWS) Simple Storage Service (S3)에서 사용 가능한 퍼블릭 클라우드 오브젝트 스토리지 리소스입니다.

S3 Bucket 유형 파일 사본보관 저장소는 최대 5TB (AWS 사양)의 대용량 파일을 지원합니다.

Endpoint Protector에서 S3 Bucket 유형 파일 사본보관 저장소를 만들려면 아래 정보를 제공하시기 바랍니다:

- **저장소 유형** – 저장소 유형으로 S3 Bucket 선택
- **구분** – 파일 사본 보관 저장소에 하나 이상의 구분 할당
- **S3 Bucket Region** – 아티팩트 검색 방법에 따라서 드롭다운 목록의 옵션 또는 AWS S3 Bucket 설정에 해당하는 버킷 지역을 추가하거나 드롭다운 목록에서 옵션 중 하나를 선택
- **S3 Bucket Name** – AWS S3 Bucket 설정에 해당하는 버킷 저장소 이름을 추가
- **S3 Location** – AWS S3 Bucket에 특정 하위 폴더 위치 추가
- **Access Key ID** – AWS S3 Bucket 설정에 해당하는 S3 Bucket 키를 추가
- **Secret Access Key** – AWS S3 Bucket 설정에 해당하는 사용자가 생성한 Token Key를 추가

아티팩트 검색 방법 선택:

1. 간접적 아티팩트 검색 – 이 방법을 추천합니다. Endpoint Protector 서버를 통해서 아티팩트를 검색하는 가장 안전한 옵션입니다.

참고: 시스템 관리자는 Endpoint Protector 서버UI를 사용하는 아티팩트 검색을 요구합니다. Endpoint Protector 서버는 S3 버킷 저장소에서 아티팩트를 검색하고 시스템 관리자에게 아티팩트 파일을 제공할 것입니다.

SDK를 사용하여 오브젝트를 다운로드 또는 삭제할 수 있습니다. 아래에서 사용 가능한 지역을 제한합니다.

- us-west1 – Northern California
- us-west2 – Oregon
- eu-west1 – EU (Ireland)

- ap-southeast-1 – Asia Pacific (Singapore)
- ap-southeast-2 – Asia Pacific (Sydney)
- ap-northeast-1 – Asia Pacific (Japan)
- sa-east-1 – South America (Sao Paulo)
- us-gov1-west-1 – United States GovCloud
- fips-us-gov-west-1 – United States GovCloud FIPS 140-2

2. 직접 아티팩트 검색 – 이 옵션은 전체적으로 분산된 Endpoint Protector 배포 전용입니다. 이 방법은 시스템 관리자 컴퓨터에서 S3 Bucket Repository에 직접 연결을 구축하고 직접 아티팩트 다운로드를 개시합니다.

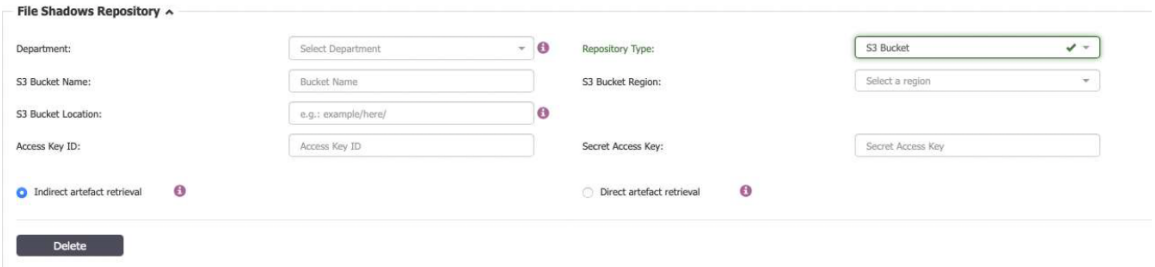
중요: 직접 방식과 간접 방식을 모두 사용하여 S3 버킷 리포지토리를 설정하려면 관리자가 AWS 관리를 통해 'Bucket Name'을 지정하고 'Access Key ID'와 'Secret Access Key'를 생성해야 합니다.

참고: 직접 아티팩트 검색 방법을 사용하기 위해서는 Endpoint Protector IP가 S3 Bucket whitelist에 아래 내용과 같이 추가되어야 합니다.

보고 및 분석 > 로그 보고서 그리고 관리자 액션을 사용하여 콘텐츠 인식 보고서 페이지에서 파일 사본 보관을 다운로드 또는 삭제할 수 있습니다.

파일이 업로드 될 때 외부 저장소 업로드 로그가 표시됩니다.

중요: S3 Bucket (파일 사본 보관 저장소)에 포함된 파일 사본 보관은 감사에 포함되지 않습니다.



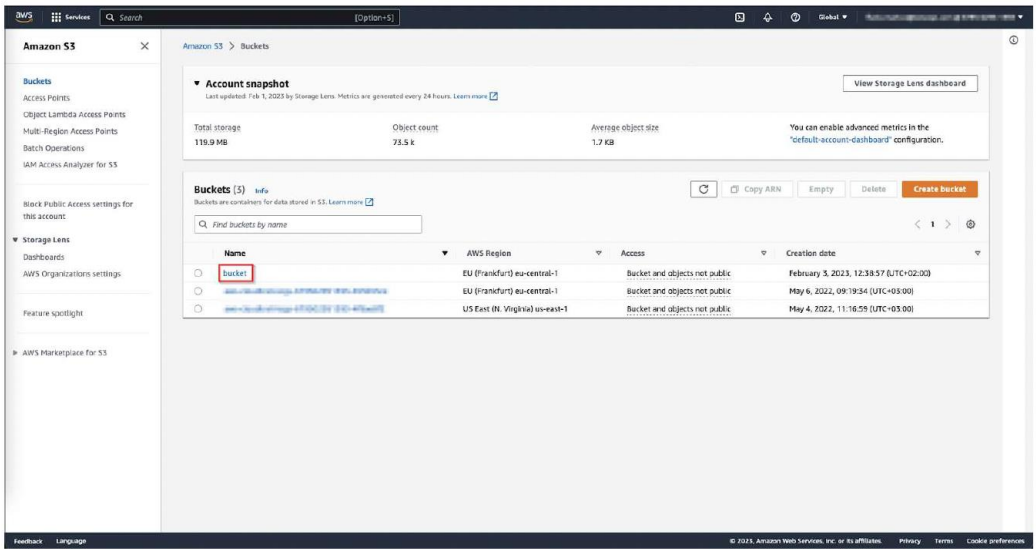
참고: 신뢰할 수 없는 네트워크가 있는 시나리오에서 guard-rail이 업로드 시도를 중지하기 전체 클라이언트는 아티팩트 업로드를 10번 시도할 것 입니다. 엔드포인트 성능, 디스크 공간 이용 및 모바일 전송 제한이 영향을 받지 않는 것을 보장하기 위에서 줄에서 파일 사본 보관을 삭제할 것 입니다.

15.8.2.1. 도메인 화이트리스팅

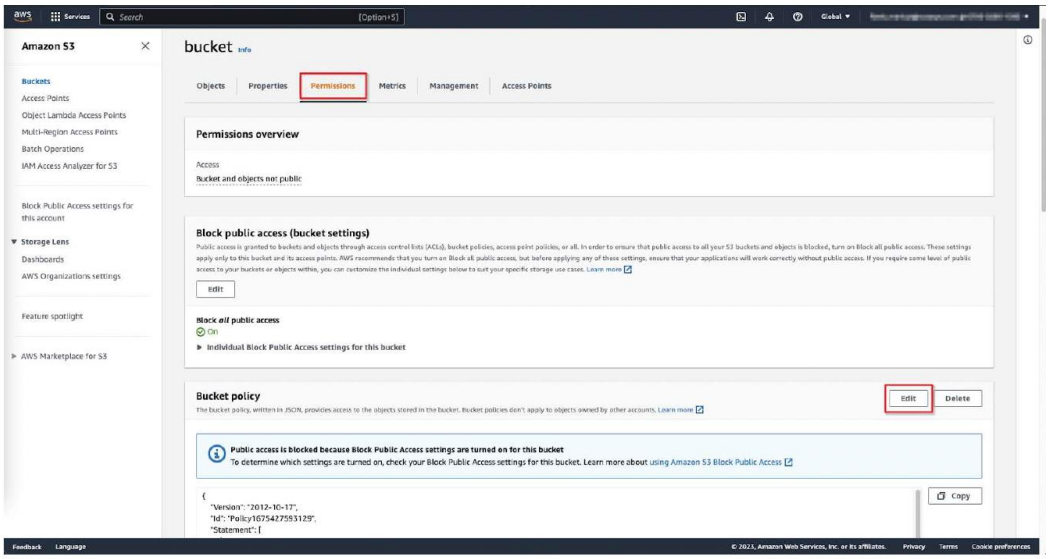
Endpoint Protector IP를 S3 Bucket 화이트리스트에 추가하려면 아래 단계를 따르시기 바랍니다:

1. **AWS** 로그인;

2. **S3 Bucket 목록**에서 엔트리 클릭;



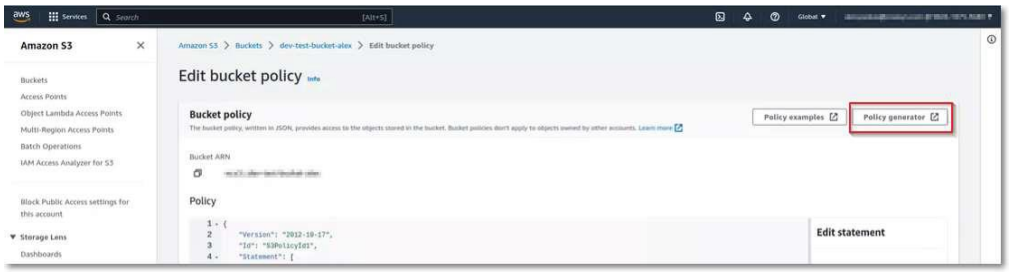
3. S3 Bucket에서 **Permission** 탭을 선택 후 스크롤을 **Bucket** 정책 섹션으로 내리고 **Edit**를 클릭



4. Bucket 정책에서 다음 IP를 추가:

- 다운로드를 위한 관리자 엔드포인트의 고정 IP 주소
- 삭제를 위한 EPP 외부 서버 IP 주소

5. 오른쪽 코너에 **Policy generator**를 사용하면 새로운 Bucket 정책을 편집 또는 만드는데 도움이 됩니다 – AWS Policy Generator는 새로운 페이지에서 열림.

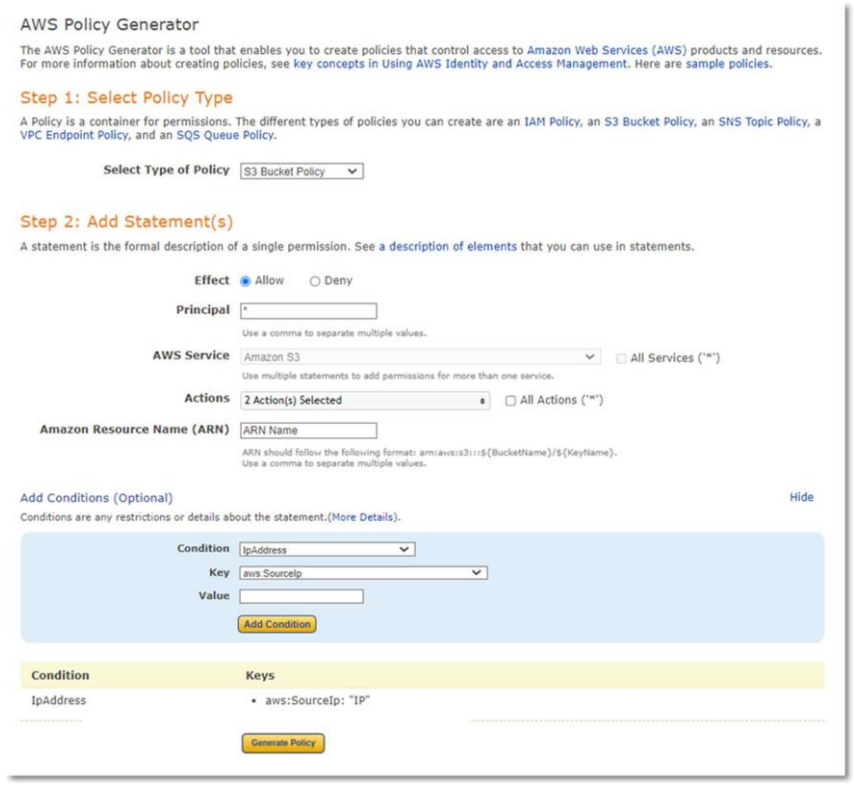


AWS Policy Generator에 다음 정보를 제공하시기 바랍니다:

- **Select Type of Policy** – S3 Bucket Policy
- **Effect** – Allow 선택
- **Principal** - * 추가
- **Actions** – **DeleteObject**와 **GetObject** 선택
- **Amazon Resource Name (ARN)** – ARN 이름 추가
- **Add Conditions** 클릭 후 드롭다운 목록에서 **Condition**에서 **IpAddress** 그리고 **Key**에서 **aws:SourceIP** 선택, **Value** 영역에서 콤마로 분리된 두 개의 IPs를 추가

위의 내용을 추가하고 **Generate Policy** 클릭 후 **Bucket Policy**를 사용하시기 바랍니다.

참고: 더 자세한 과정은 홈페이지의 AWS 문서를 참조하시기 바랍니다.



Example: S3 Bucket Policy (JSON)

```
{
 "Version": "2012-10-17",
 "Id": "S3PolicyId1",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": "*",
   "Action": [
        "s3:GetObject",
        "s3:DeleteObject"
   ],
   "Resource": "arn:aws:s3:::your-bucket-name/*",
   "Condition": {
    "IpAddress": {
     "aws:SourceIp": [
      "IP1", //the external  IP of the server; it's need it for Delete action
      "IP2", //public IP address; It's needed for the download method
     ]
    }
   }
  }
 ]
}
```

설명:

- "**Effect**": "Allow"는 허용된 권한을 의미함
- "**Principal**": "*"는 누구에게나 액세스를 확장함 (특정 계정에 대한 액세스를 제한하려면 * 를 AWS 계정 ID로 대체할 수 있음)
- "**Action**": ["s3:GetObject", "s3:DeleteObject"]는 "GetObject" 작업과 "DeleteObject" 작

업 (다운로드 및 삭제 메서드)을 모두 허용

- "**Resource**": "arn:aws:s3:::your-bucket-name/*"은 오브젝트의 ARN(Amazon Resource Name)을 지정. "your-bucket-name"을 실제 버킷 이름으로 변경 요청.

  중요: bucket ARN 끝에 / 를 추가가 매우 중요합니다. AWS 생성기는 기본으로 포함하지 않습니다.

- "**Condition**"은 IP 주소 조건을 지정
- "**GetObject**" 메서드 (EPP에서 다운로드 작업) 경우 – 이 메서드에서 공인 IP 주소 필요. 사본 보관을 다운로드하려면 Bucket Name, Bucket location, region, shadow name에 따라 적절한 AWS URL 구성
- "**DeleteObject**" 메서드 (EPP에서 삭제 작업) 경우 – 이 메서드에서는 서버의 외부 IP가 필요

이 접근 방식에서 cURL 요청을 사용하여 DELETE 요청을 AWS S3로 전송하여 버킷에서 개체를 쉽게 제거할 수 있습니다. 이 요청은 EPP 서버에서 시작되어 버킷 정책에서 해당 서버의 외부 IP 화이트리스트에 추가해야 합니다.

15.8.1.2. 인터넷 연결 요구사항

파일 사본 보관 저장소 유형으로 S3 Bucket을 사용할 때 다음 상황에서 직접 인터넷 연결이 필요합니다:

- 파일 사본을 AWS S3 Bucket 저장소에 전달하는 Endpoint Protector 클라이언트
- 간접 아티팩트 검색 방법을 사용하여 AWS S3 Bucket 저장소에서 파일 사본을 검색하는 Endpoint Protector 서버
- 직접 아티팩트 검색 방법을 사용하여 AWS S3 Bucket 저장소에서 파일 사본을 검색하는 관리자 엔드포인트

15.8.1.3. 파일 네이밍 및 구조

1. 파일 이름 컨벤션

파일 이름은 특수 문자 이슈를 피하기 위해 인코딩 된 URL로 S3 Bucket에 업로드 됩니다. Endpoint Protector 서버는 원래 이름을 표시하기 위해 디코딩 합니다.

예제:

File name

canada_&$@=;/+ ,?{^}%`]>[~<#|_山人é口ǒ刀ā木ù日ì月è女ǔ子ǐ馬/马鳥/鸟niǎ目ù水 .txt

File name displayed in AWS S3 Bucket

ln4w7yuqax-dev-client-bucket/2022-11-

23/ComputerName/canada_%26%24%40%3D%3B%3A%2B%20%2C%3F%5C%7B%5E%7D%25

%60%5D%3E%5B~%3C%23%7C_%E5%B1%B1%E4%BA%BAe%CC%81%E5%8F%A3o%CC%86%

E5%88%80a%CC%84%E6%9C%A8u%CC%80%E6%97%A5i%CC%80%E6%9C%88e%CC%80%E

5%A5%B3u%CC%88%CC%8C%E5%AD%90i%CC%86%E9%A6%AC%3A%E9%A9%AC%E9%B3%

A5%3A%E9%B8%9Fnia%CC%8C%E7%9B%AEu%CC%80%E6%B0%B4%20.txt

중요: 컴퓨터 이름과 위치에서 파일 이름과 특수 문자는 또한 인코딩 됩니다.

2. 파일 이름 구조

Default file name structure:

bucketName/CurrentDate/ComputerName

- **bucket name** (ln4w7yuqax-dev-client-bucket)
- **current date** in YYYY-MM-DD format (2022-11-23)
- **computer name** URL encoded

File name structure with S3 Bucket location field specified:

bucketName/location/CurrentDate/ComputerName

16. 시스템 구성

이 섹션은 시스템 기능과 안정성에 영향을 주는 Endpoint Protector 클라이언트, 시스템 라이선스, 다른 고급 설정을 포함합니다.

16.1. 클라이언트 소프트웨어

이 섹션에서 관리자는 사용 중인 운영 체제에 해당하는 Endpoint Protector 클라이언트를 다운로드 하여 설치할 수 있습니다.

참고: 서버와 클라이언트는 443 포트로 통신합니다.

커스텀 Web UI 포트를 사용하면 Nginx 구성 파일 조정을 위해 유상 원격지원이 필요합니다.

Windows 클라이언트 인스톨러는 add-on 이 있거나 없는 다운로드 패키지를 제공합니다. 이 옵션은 Endpoint Protector와 특정 솔루션 사이의 호환성 이슈를 해결합니다.

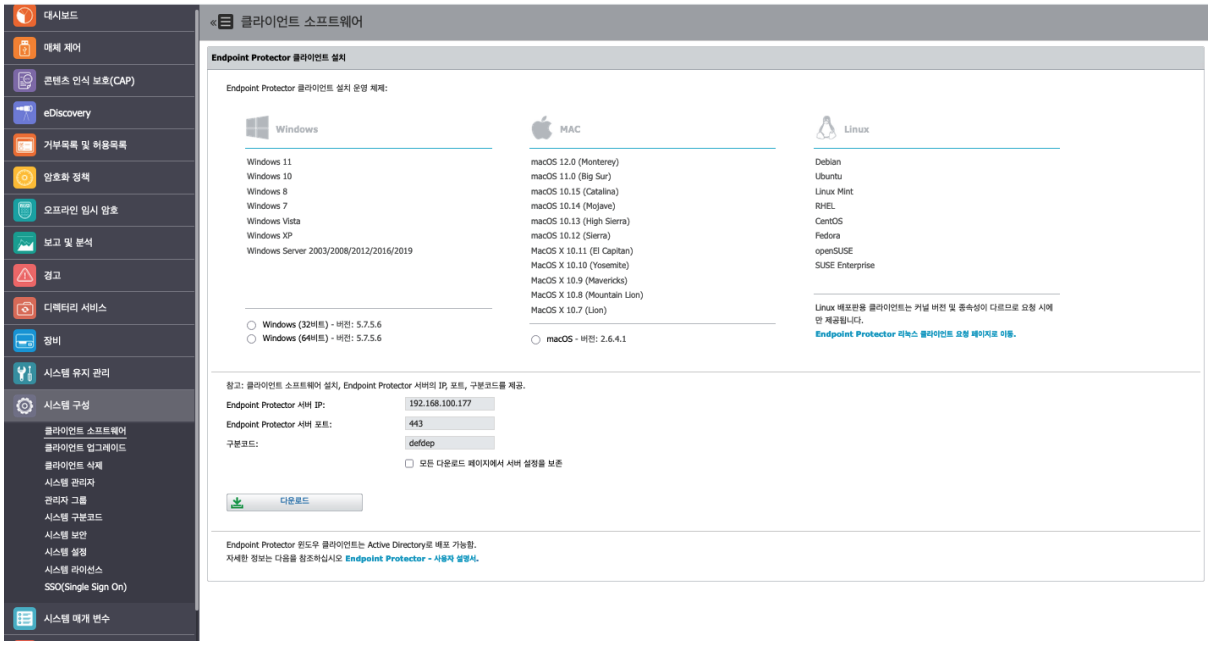
중요: 최신 Endpoint Protector 클라이언트만 다운로드할 수 있습니다. 클라이언트 소프트웨어 업그레이드 섹션에서 또 다른 기본 Endpoint Protector 클라이언트 버전을 설정할 수 없습니다.

Endpoint Protector 설치 과정 개선을 위해서 설치 관련 동작이 가능한 Endpoint Protector 도구를 사용하고 현재 Linux 배포판 식별 및 Endpoint Protector 릴리즈 노트를 보시기 바랍니다.

아래 커맨드를 사용하시기 바랍니다:

- i – install
- u – uninstall
- rn – release notes
- l – distribution list

참고: EPP 클라이언트 버전은 엔드포인트에서 X.X.X.XXXX 형식으로 표시됩니다. 이 버전은 EPP 서버 데이터베이스에 저장되지만 웹 콘솔에서 마지막 3자리 숫자는 잘립니다.



16.1.1. 우회 프록시 설정

모든 운영 체제에서 프록시 설정을 우회할 수 있습니다.

16.1.1.1. Windows 및 macOS

1. Endpoint Protector 마법사 설치

Endpoint Protector 마법사 설치에서 **수동 프록시 설정 사용**을 선택하고 아래 정보를 제공하시기 바랍니다:

- **Proxy IP:** 프록시 서버 IP
- **Proxy Port:** 프록시 포트
- **인증 사용** 체크박스 선택
- **Username:** 프록시 서버 사용자 이름 추가
- **Password:** 프록시 서버 비밀번호 추가

2. CLI 커맨드

CLI 커맨드를 사용하여 수동 프록시 설정을 적용할 수 있습니다.

예제:

msiexec.exe /i "C:₩Work₩Tools₩EPPClientSetup.5.7.1.5_x86_64.msi" /q

REBOOT=ReallySuppress RUNNOTIFIER=0 /log "C:₩Windows₩TEMP₩eppupgrade.

log" WSIP="192.168.18.125" WSPORT="8080" DEPT_CODE="defdep"

PROXYIP="127.0.0.1" PROXYPORT="80" AUTHUSR="user_name" AUTHPASS="password"

Where:

- **PROXY_IP** - IP of the proxy
- **PROXY_PORT** - Port of the proxy
- **AUTHUSR** - Username (if authentication for proxy is needed)
- **AUTHPASS** - Password (if authentication for proxy is needed)

아래 CLI 커맨드를 사용하여 특정 작업 모드에서 EPP 클라이언트를 설치할 수도 있습니다.

- WSIP – 서버 주소
- WSPORT – 서버 포트 번호
- DEPT_CODE – 구분 코드
- IPV6MAPPING – IPv4 주소를 매핑한 IPv6
- SUPPRESSRD – NS (네트워크 공유) 및 이동식 장치에 대한 파일 읽기 / 파일 삭제 이벤트 숨김
- DISABLECAP – CAP 드라이버 로딩 사용하지 않음 (CAP 동작하지 않음)

16.1.1.2. Linux

Linux에서는 .sh 파일에서 프록시 설정을 우회하기 위해서 옵션에서 CLI 아규먼트만 사용할 수 있습니다. 아래 단계를 따르시기 바랍니다:

1. 설치 폴더에 접근해서 터미널을 열고 다음 커맨드를 실행합니다:

cd Linux클라이언트폴더경로

2. root로 실행하기 위해서 다음 커맨드를 실행하고 비밀번호를 입력합니다;

sudo su

3. 다음 커맨드로 options.sh 구성 파일 파일을 오픈합니다;

gedit options.sh

4. 구성 파일에서 프록시 설정을 위한 다음 영역을 볼 수 있습니다;

#EPPCLIENT_HTTPS_PROXY=

#export EPPCLIENT_HTTPS_PROXY

5. 프록시 설정 적용을 위해서 각 줄에서 #를 제거합니다;

6. 첫 프록시 설정에서 EPPCLIENT_HTTPS_PROXY에 프록시 서버 정보를 **address:port:user:password** 포맷으로 추가합니다;

예제: EPPCLIENT_HTTPS_PROXY=**address:port:user:password**

7. 변경 내용을 저장하고 VPN 연결 없이 설치를 실행합니다:

bash install.sh

특정 모드에서 Linux용 추가 CLI 커맨드:

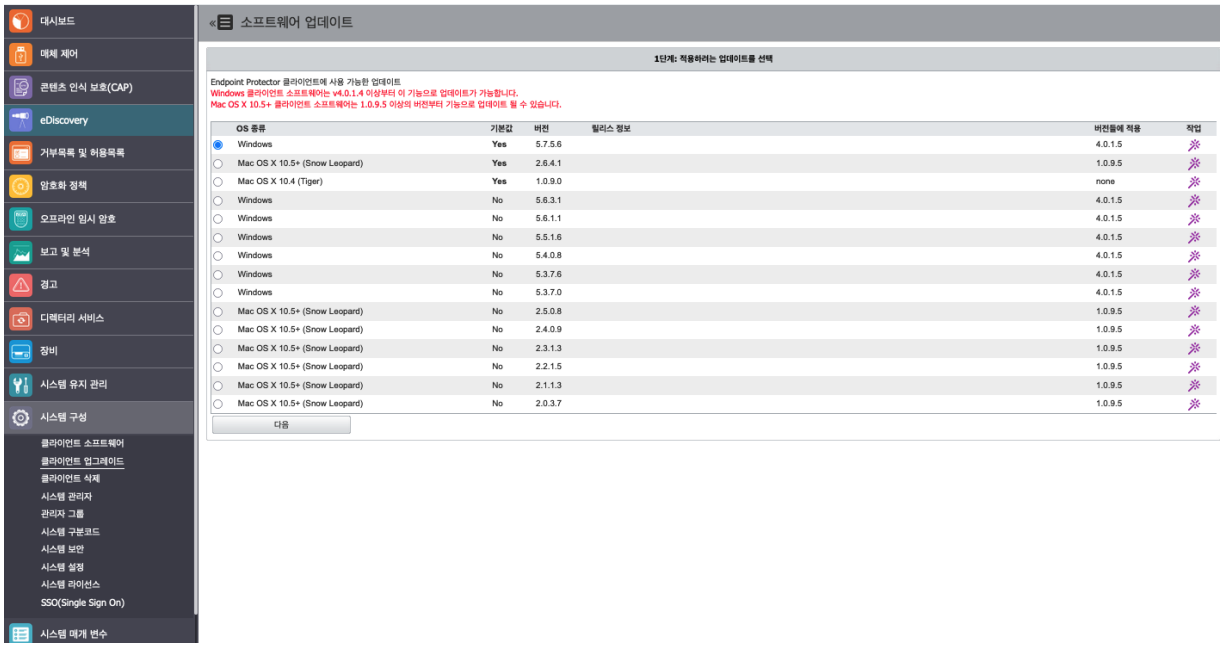
- #EPPCLIENT_SUPPRESSRW – NS (네트워크 공유) 및 이동식 장치에서 파일 읽기 / 파일 삭제 이벤트 숨김
- #EPPCLIENT_DISABLECAP – CAP 드라이버 로딩 사용하지 않음 (CAP 동작하지 않음)

16.2. 클라이언트 업그레이드

이 섹션에서는 설치된 Endpoint Protector 클라이언트 버전의 자동 업데이트를 선택하고 수행할 수 있습니다. 클라이언트 소프트웨어 업그레이드 기능은 Windows와 macOS 클라이언트에서만 사용할 수 있습니다. Linux 클라이언트 업그레이드는 총판사에 연락하시기 바랍니다.

참고: 최신 macOS Ventura로 운영체제를 업그레이드할 때 private/var/log에서 eppclient.log와 eppsslsplit.log는 삭제됩니다.

중요: 이 기능은 Windows 32bit 버전으로 운영되는 Endpoint Protector 인스턴스와 호환되지 않습니다.

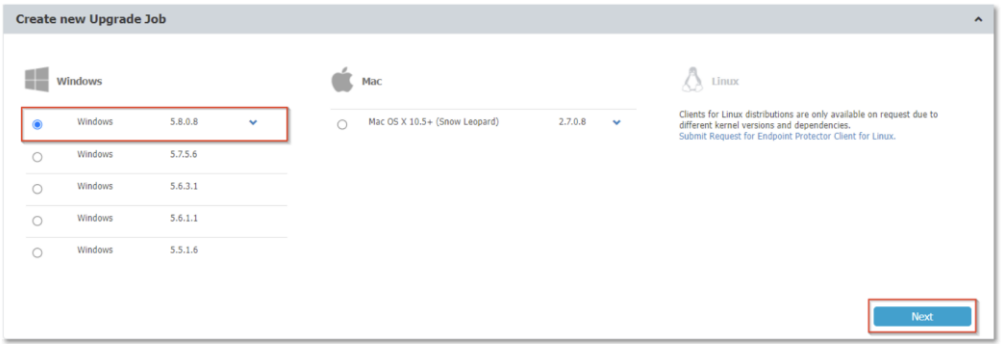


참고: EPP 클라이언트 버전은 엔드포인트에서 X.X.X.XXXX 형식으로 표시됩니다. 이 버전은 EPP 서버 데이터베이스에 저장되지만 웹 콘솔에서 마지막 3자리 숫자는 잘립니다. EPP 클라이언트 버전이 동일한 경우 (처음 4자리) EPP 서버는 여전히 전체 버전 번호를 서로 비교합니다. 전체 버전 번호를 서로 비교하여 가장 최신 버전을 식별합니다.

16.2.1. 새로운 업그레이드 작업 만들기

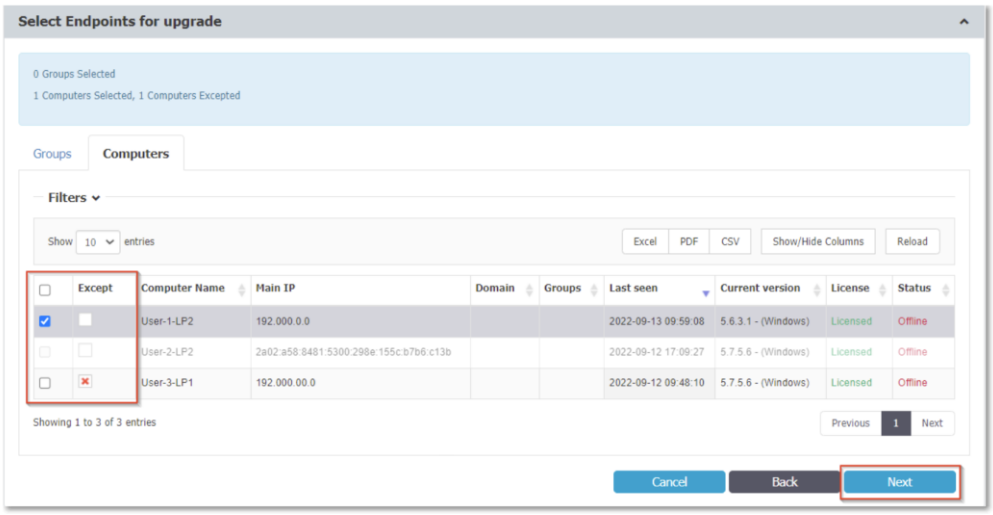
Endpoint Protector 클라이언트를 업그레이드하기 위해서 다음 단계를 따라서 새로운 업그레이드 작업을 만들 필요가 있습니다:

1. 드롭다운 목록에서 OS 버전을 선택하고 다음을 클릭합니다.



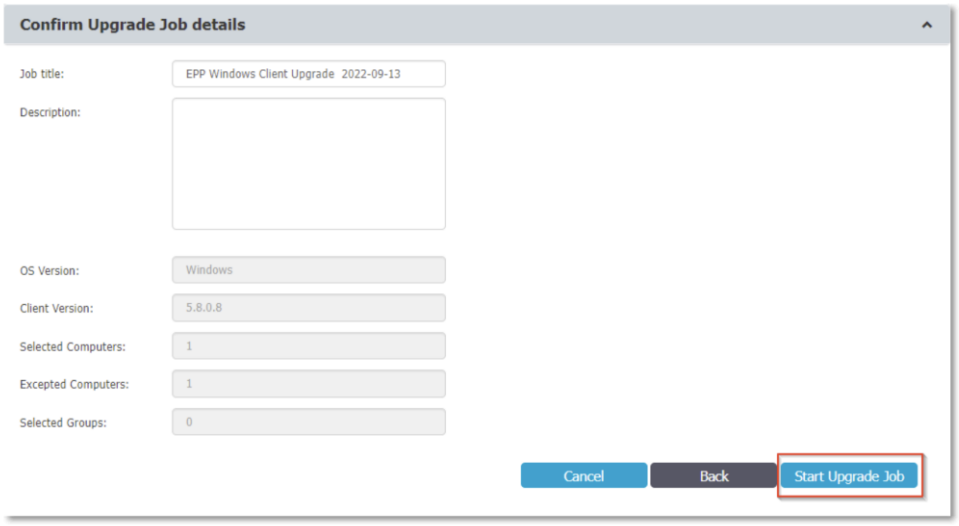
2. 업그레이드를 수행 또는 제외할 컴퓨터 그리고/또는 그룹을 선택하고 다음을 클릭합니다. 요약 정보를 볼 수 있습니다.

   참고: 이전에 선택된 운영체제를 사용하는 컴퓨터만 업그레이드됩니다. 다른 운영체제 시스템을 사용하는 엔드포인트를 가지는 그룹을 선택하면 업그레이드되지 않습니다. 혼합 그룹을 선택하면 컴퓨터와 사용자에서 컴퓨터만 업그레이드됩니다.



3. **업그레이드 작업 시작**을 클릭해서 기본 작업 제목 편집, 설명 추가, 업그레이드 작업 상세 정보 확인을 합니다. **업그레이드 작업** 섹션에서 업그레이드 엔트리가 보입니다.

   중요: Endpoint Protector 클라이언트의 업그레이드 프로세스는 전용 cron에 영향을 받습니다 매 5분마다 운영되고 cron은 **보류 중**으로 업그레이드 프로세스 상태를 설정하고 매 15분마다 **완료됨** 또는 **실패가 완료됨** 프로세스 상태를 확인하고 업데이트합니다.

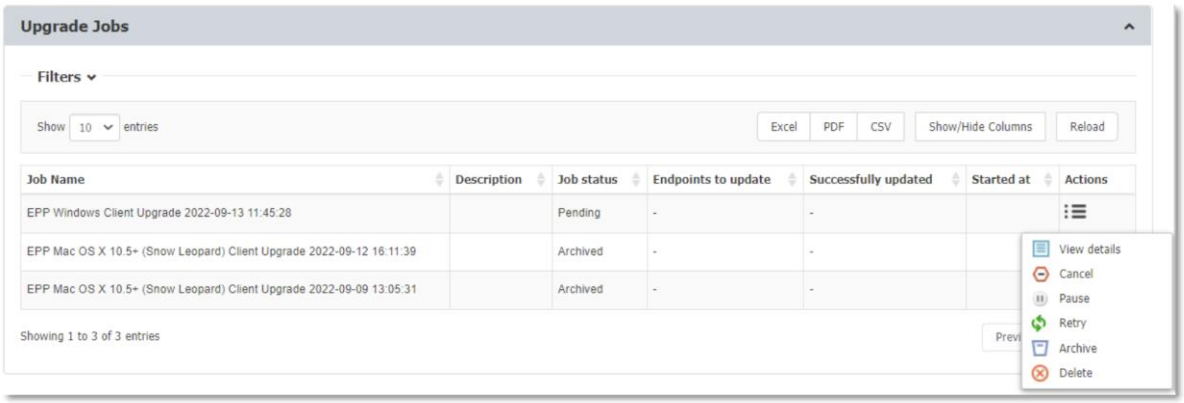


16.2.2. 업그레이드 작업 관리

이 섹션에서 업그레이드된 작업을 볼 수 있고 작업 상세정보, 취소, 일시 정지, 재시도, 압축 또는 목록의 엔트리 삭제를 보기위한 **작업** 컬럼을 사용할 수 있습니다.

취소된 클라이언트 업그레이드 작업을 업그레이드를 계속하려면 **작업** 컬럼에서 **재시도** 옵션을 사용하시기 바랍니다.

참고: 클라이언트 업그레이드 작업을 삭제 또는 아키브했다면 엔드포인트는 다른 작업에서 선택이 가능합니다.



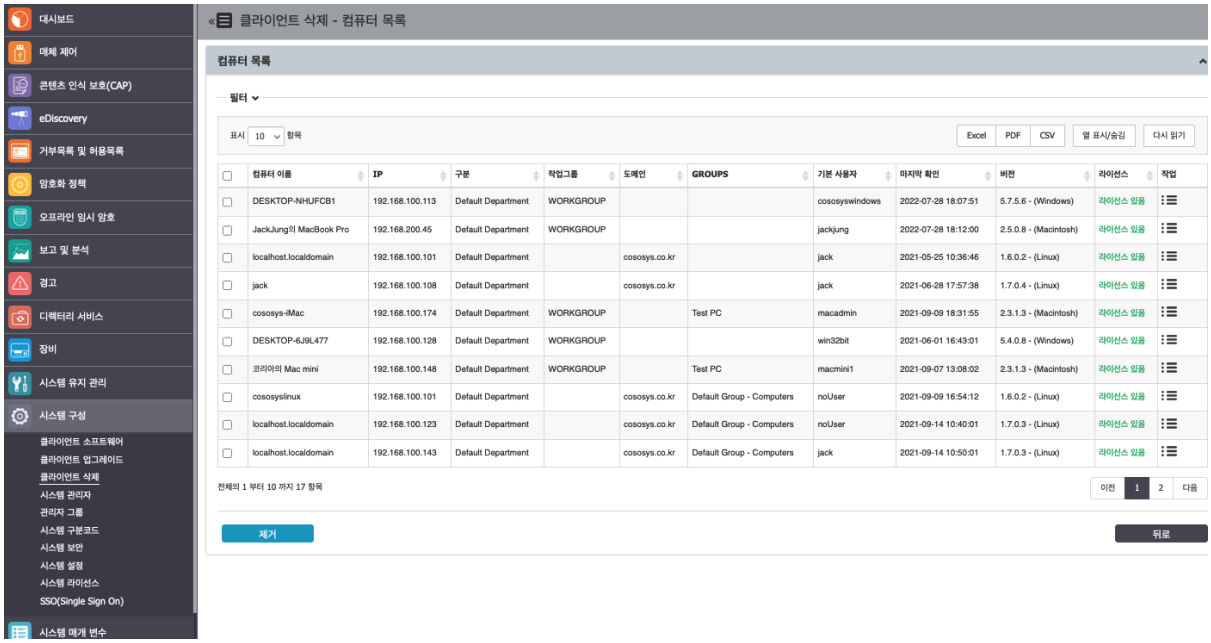
16.3. 클라이언트 삭제

설치된 EPP 클라이언트는 이 탭에서 원격으로 컴퓨터를 삭제할 수 있습니다. 컴퓨터는 서버에서

설정 명령을 받는 같은 시간에 삭제 명령을 받습니다.

만약 컴퓨터가 오프라인이면 첫 번째로 온라인으로 될 때 삭제 명령을 받습니다. 삭제 버튼을 누르면 컴퓨터는 동작이 수행 될 때까지 비활성화 처리됩니다.

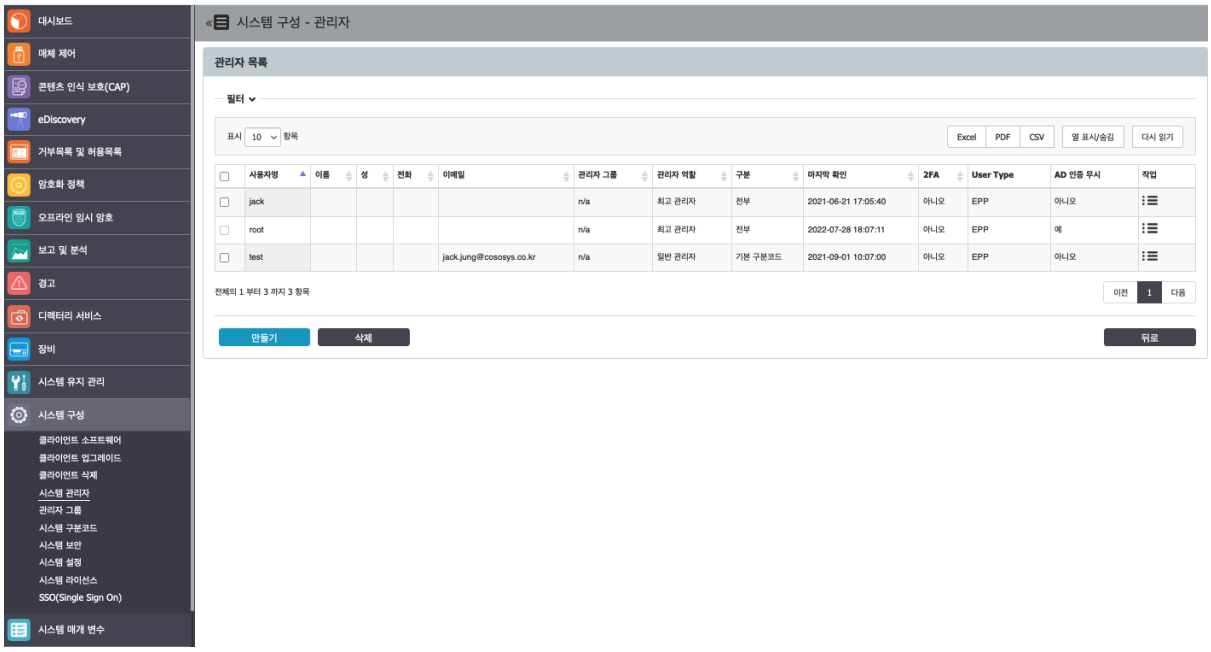
이미 실행된 것이 아니라면 삭제 명령은 취소 할 수 있습니다.



참고: 서버 인증 유효성 검사 누락으로 서버와 EPP 클라이언트가 통신할 수 없는 경우 (인증 유효성 검사 설정이 활성화된 경우), EPP 서버에서 제거 명령을 실행할 수 없습니다. 이러한 경우 EPP 클라이언트 컴퓨터에 인증서를 수동으로 설치할 수 없다면, EPP 서버에서 인증 유효성 검사 설정을 일시적으로 비활성화하고 EPP 클라이언트를 동기화하여 제거 명령을 검색할 수 있습니다.

16.4. 시스템 관리자

이 섹션에서 관리자를 보기, 만들기, 관리, 삭제 할 수 있습니다.



새로운 관리자를 만들기 위해서 기존의 관리자 테이블 아래에 있는 **만들기**를 클릭하고 다음 정보를 제공합니다.

1. **관리자 정보** – 사용자명과 암호, 이메일, 성과 이름, 전화번호를 입력하고 기본 UI 언어를 선택합니다.
2. **계정 설정**
   - **계정이 활성화 됨** – 계정 상태를 관리합니다.
   - **다음 로그인에 암호 변경 요구** – 첫 번째 로그인에 관리자 암호를 변경을 관리자에게 요청하고 암호를 변경하면 이 설정은 자동으로 비활성화 됩니다.
   - **로그인 시도 제한** – 새로운 로그인 시도전에 5에서 10으로 로그인 시도 실패에 대해서 5분에서 10분으로 타임아웃을 강제화 할 수 있습니다.
   - **로그인 IP 제한 적용** – 특정 IP 주소에서 로그인 시도를 할 수 있도록 제한합니다.

     중요: 다음 로그인에 암호 변경 요구 설정은 아래의 경우에 무시됩니다.

     a. **다음 로그인에 모든 관리자 암호 보안 강제화** 설정이 시스템 구성 > 시스템 보안에서 사용될 때 **다음 로그인에 암호 변경 요구**는 무시되고 암호가 변경되면 비활성화 됩니다.

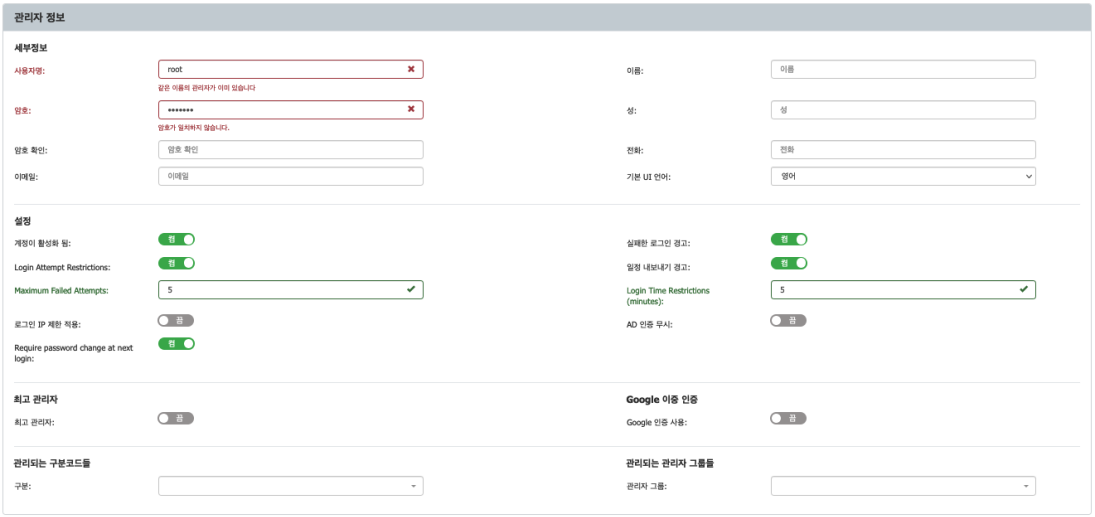
     b. Active Directory로 가져온 사용자

     c. SSO 사용자 (Azure 및 OKTA), 설정은 숨김으로 됩니다.

- **실패한 로그인 경고** – 모든 실패 로그인에 대한 경고를 받습니다.
- **일정 경고 보내기** – 모든 스케줄 내보내기에 대한 경고를 받습니다.
- **AD 인증 무시** – Endpoint Protector에 로그인을 위한 AD 계정을 사용하는 것을 허용합니다.

3. **최고 관리자 정보**

- **최고 관리자** – Endpoint Protector의 모든 구분과 섹션에 접근을 부여합니다.
- **Google 이중 인증** – 기기에 미리 설치된 Google Authenticator를 사용하여 2FA를 강제화 합니다.
- **관리되는 구분코드들** – 구분을 선택합니다.
- **관리되는 관리자 그룹들** – 그룹을 선택합니다.



16.5. 관리자 유형

최고 관리자는 전체 시스템을 완벽하게 제어할 수 있습니다. SSO (Single Sign On) 로그인 섹션에서 사용자를 최고 관리자로 가져오기로 설정하면 가져온 모든 Azure SSO (Single Sign On) 사용자에게 최고 관리자 권한을 부여할 수 있습니다.

최고 관리자는 대시보드 액세스, 라이브 업데이트 제어, 유효 권한 보고서를 실행, 매체 제어 관리, 심층 패킷 검사 (DPI) 기능이 포함된 콘텐츠 인식 보호 (CAP) 관리, eDiscovery 관리,

거부목록 및 허용 목록, URL 범주 관리, 암호화 정책 (EE) 관리, 오프라인 임시 암호 (OTP)관리, 보고 및 통계 보기, 관리자 액션 보기 및 관리, 경고 보기 및 관리, 디렉터리 서비스 관리 및 보기, 어플라이언스 및 SIEM 연결 관리 및 보기, 시스템 유지관리 관리 및 보기, 시스템 구성 관리 및 보기, 클라이언트 소프트웨어 (업그레이드 포함) 다운로드 및 보기, 시스템 파라미터 관리를 할 수 있습니다.

일반 관리자는 일반 권한이 있지만 몇 가지 제한이 있는 시스템 사용자입니다. 담당하는 시스템 구분에 속한 엔터티만 관리할 수 있습니다. 일반 관리자는 관리자 그룹 내에서 특정 책임을 할당하여 액세스를 더욱 제한할 수 있습니다. 예를 들어 오프라인 임시 암호 및 암호화 정책 같은 특정 업무가 있는 헬프 데스크 그룹에 배정되거나 콘텐츠 인식 보호 (CAP) 및 매체 제어와 같은 특정 모듈로 권한이 제한될 수 있습니다.

이러한 제한에도 불구하고 **일반 관리자**는 매체 제어, 콘텐츠 인식 보호 (CAP) 관리 (심층 패킷 검사 (DPI) 포함), eDiscovery 관리, 거부 목록 관리, 허용 목록 관리, 오프라인 임시 암호 관리, 암호화 정책 관리, 보고 및 통계 보기, 경고 보기 및 관리, 클라이언트 소프트웨어 다운로드 및 보기 (업그레이드 포함) 등의 다양한 시스템 관리 도구에 액세스 할 수 있습니다. 또한 시스템 매개변수를 제어할 수 있으며, 일반 관리자에게 특정 역할과 그룹을 할당함으로써 조직은 필요한 사용자만 민감한 데이터와 도구에 액세스할 수 있도록 보장하는 동시에 팀원들에게 시스템을 효율적으로 관리하는데 필요한 도구를 제공할 수 있습니다.

조직은 일반 관리자에게 특정 역할과 구분을 할당함으로써 민감한 데이터와 도구에 필요한 사용자만 액세스할 수 있도록 보장하고 팀원에게 시스템을 효율적으로 관하는 필요한 도구를 제공할 수 있습니다.

16.6. 관리자 그룹

이 섹션에서 관리자 그룹 만들기와 관리를 할 수 있습니다. 일반 관리자에게 다양한 접근 권한을

제공합니다.

그룹에 추가된 관리자는 역할에 할당된 섹션만 보고 관리할 수 있습니다.

기본으로 아래 관리자 그룹을 만들 수 있습니다:

- **오프라인 임시 암호 관리자** – 오프라인 임시 암호 섹션만 사용이 허용됨
- **보고 및 분석 관리자** – 보고 및 분석 섹션만 사용이 허용됨
- **암호화 정책 (EasyLock) 관리자** – 암호화 정책 섹션만 사용이 허용됨
- **유지 관리 관리자** – 디렉터리 서비스, 장비, 시스템 유지 관리 섹션 사용이 허용됨
- **헬프 데스크 관리자** – 암호화 정책 및 오프라인 임시 암호 섹션만 사용이 허용됨
- **매체 제어 관리자** – 매체 제어 섹션만 사용이 허용됨
- **보고만 관리자** – 모든 Endpoint Protector 섹션을 볼 수만 있도록 허용됨
- **콘텐츠 인식 보호(CAP) 관리자** – 콘텐츠 인식 보호(CAP) (심층 패킷 검사 (DPI))뿐만 아니라 거부 목록, 허용 목록, USR 카테고리 액세스가 허용됨
- **eDiscovery 관리자** – eDiscovery 섹션만 사용이 허용됨

새로운 관리자 그룹을 만들려면 **만들기**를 클릭하고 다음 정보를 입력합니다:

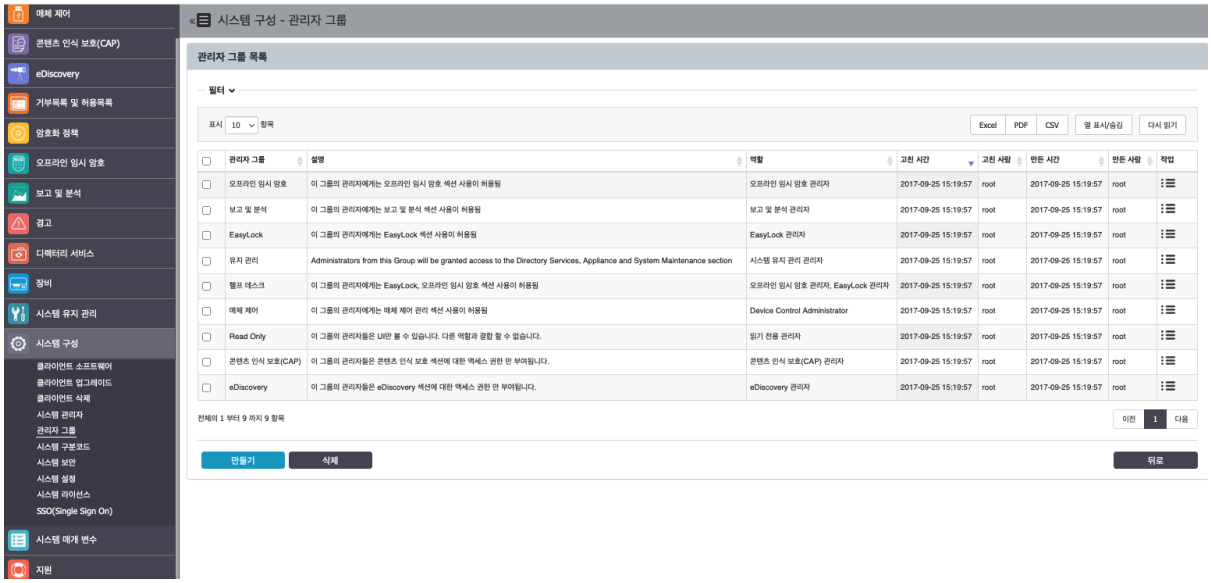
- **이름:** 새로운 관리자 그룹 이름 추가
- **역할:** 목록에서 하나 또는 그 이상을 선택

중요: 보고만 역할은 다른 역할과 함께 사용할 수 없습니다.

- **설명** – 새로운 관리자 그룹의 설명 추가
- **관리자 선택** – 이 그룹에서 하나 또는 그 이상의 관리자 추가

시스템 구성 > 시스템 관리자 > 관리되는 관리자 그룹 영역에서 관리자를 만들 때 관리자 그룹에 이 관리자들을 추가할 수도 있습니다.

참고: 지원 섹션은 관리자 그룹의 역할에 관계없이 모두에게 허용됩니다.



16.6.1. 사용자 역할 매트릭스

EPP 사용자 역할 매트릭스는 관리자의 역할에 따라 관리자의 다양한 기능과 권한을 정의합니다. 이 매트릭스를 통해 사용자는 업무 수행에 필요한 기능만 액세스 할 수 있어서 보안이 강화되고 의도치 않은 변경이나 데이터 유출 가능성이 낮아집니다.

User Role Matrix Table										
Feature	**Super Admin**	**Normal Admin**	**Reports & Analysis Admin**	**OTP Admin**	**EE Admin**	**Maintenance Admin**	**HelpDesk (OTP + EE)**	**Device Control Admin**	**CAP Admin**	**eDiscovery Admin**
View the General Dashboard	✓	X	X	X	X	X	X	X	X	X
Manage Live Updates	✓	X	X	X	X	X	X	X	X	X
Run Effective Rights reports	✓	X	X	X	X	X	X	X	X	X
Manage Device Control	✓	✓	X	X	X	X	X	✓	X	X
Manage Content-Aware Protection (CAP) including Deep Packet Inspection (DPI)	✓	✓	X	X	X	X	X	X	✓	X
Manage eDiscovery	✓	✓	X	X	X	X	X	X	X	✓
Manage Denylists, Allowlists, and URL Categories	✓	✓	X	X	X	X	X	X	✓	✓
Manage Enforced Encryption (EE)	✓	✓	X	X	✓	X	X	X	X	X
Manage Offline Temporary Password (OTP)	✓	✓	X	✓	X	X	✓	X	X	X
View Reporting and Statistics	✓	✓	✓	X	X	X	X	X	X	X
Manage and View Administrative Actions	✓	X	X	X	X	X	X	X	X	X
View and Manage Alerts	✓	✓	X	X	X	X	X	X	X	X
Manage and View Directory Services	✓	X	X	X	X	✓	X	X	X	X
Manage and View Appliance Configuration and SIEM Integration	✓	X	X	X	X	✓	X	X	X	X
Manage and View System Maintenance	✓	X	X	X	X	✓	X	X	X	X
Manage and View System Configuration	✓	X	X	X	X	X	X	X	X	X
Download and View Client Software (including Upgrade)	✓	✓	X	X	X	X	X	X	X	X
Manage System Parameters	✓	X	X	X	X	X	X	X	X	X
Except for Events, Manage System Parameters.	✓	✓	X	X	X	X	X	X	X	X

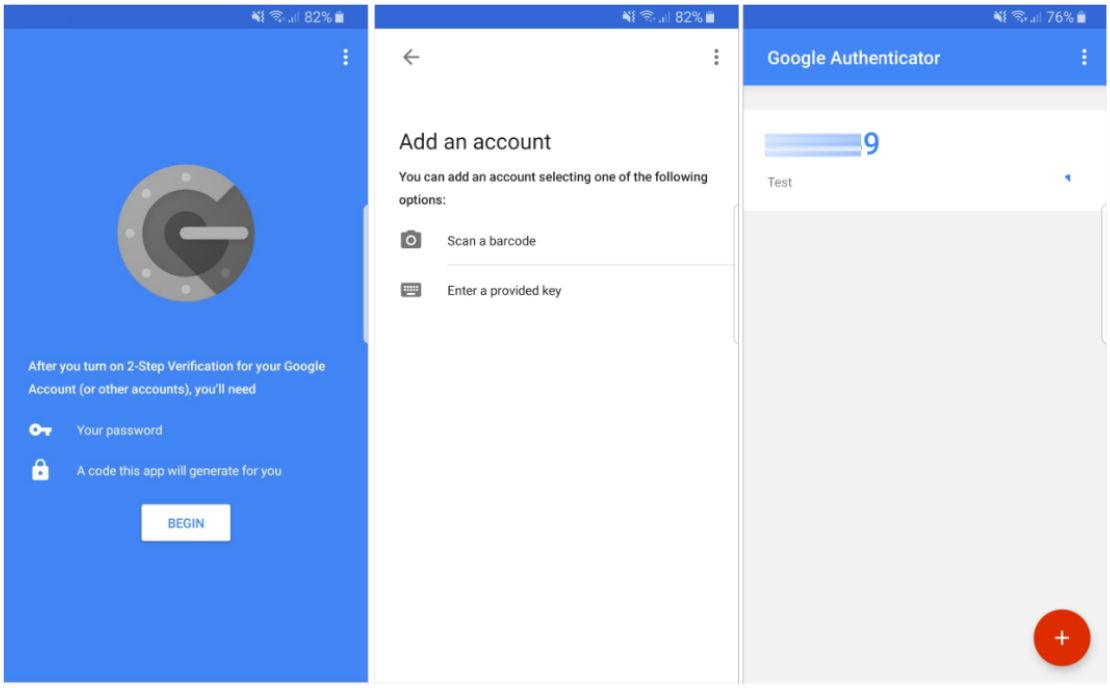
EPP에서 각각 고유한 권한이 있는 여러 사용자 역할이 있고 최고 관리자 역할은 가장 강력하고 모든 기능에 액세스할 수 있는 반면, 다른 역할은 업무에 따라 액세스 권한이 더 제한됩니다.

참고: 앞서 언급한 각 역할은 구분에 할당할 수 있습니다. 읽기 전용 모드에서 사용자는 보기 옵션만 제공되어 필수 정보는 얻을 수 있지만 시스템을 변경할 수 없습니다.

16.7. 이중 인증

이중 인증 (Two Factor Authentication, 2FA)는 Google 인증 앱을 통해서 생성된 임시 코드를 요청해서 로그인 프로세스에 추가적인 단계를 포함합니다. 만약 켬으로 되어있고 저장을 누르면 관리자는 인증 화면을 아래와 같이 볼 수 있습니다.

Google 인증 앱은 고유 코드 또는 QR 코드를 통해서 사용자가 등록하도록 요청합니다. 이 등록 프로세스를 따르면 계정이 목록에 추가되고 두 번째 인증 사용을 위한 고유 코드를 특정 시간 동안 사용할 수 있습니다.



16.8. 시스템 구분

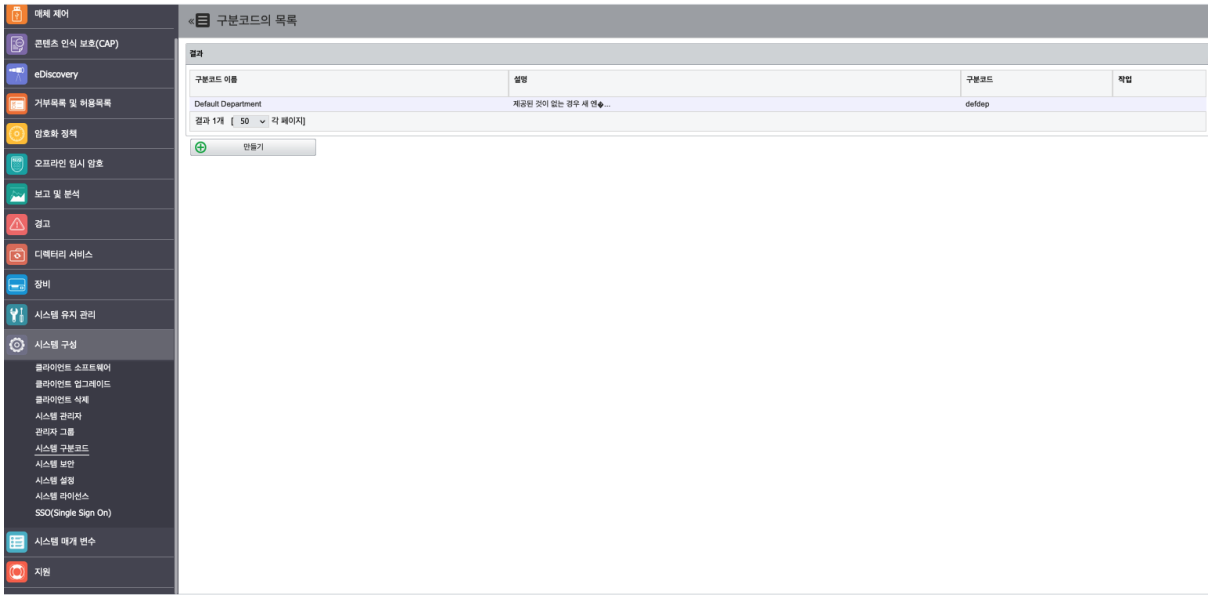
이 섹션에서 시스템 구분을 만들고 관리할 수 있습니다.

시스템 구분 사용은 옵션입니다. Endpoint Protector은 단지 기본 구분 (defdep)으로 완벽하게 동작합니다. 게다가 대부분의 시나리오는 장치, 컴퓨터, 사용자, 그룹 (또한 AD에서 사용 가능한

엔터티들)을 사용해서 커버가 됩니다.

이 기능은 관리자 수가 많고 엄격한 규정 준수가 필요한 대규모 배포에서 주로 사용될 것입니다. 이러한 환경에서 구분을 만들 수 있습니다. 일반 관리자는 그들의 엔터티들만 관리할 수 있도록 허용됩니다.

중요: 이 기능은 컴퓨터와 사용자의 그룹 그리고 관리자 역할과 다릅니다.



새로운 구분을 만들기 위해서 **만들기**를 클릭하고 이름, 설명, 고유의 구분코드를 입력합니다.

참고: 만약 잘못된 구분 코드 또는 입력이 되지 않았다면 구분 코드는 유효하지 않음으로 되고 컴퓨터는 기본 구분 (defdep)에 할당됩니다.

전문적인 명명과 관련해서 Endpoint Protector와 Active Directory (또는 다른 Director Service 소프트웨어) 사이의 유사성은 OU (Organization Unit)과 동등한 구분 (Department)을 만들 수 있습니다. 물론 OU는 구분 (Department)에서 식별하지 않고 다시 Endpoint Protector는 실제 최고 관리자에게 Endpoint Protector 구분에서 하나 또는 그 이상의 OU를 가상으로 연결하는 권한을 남겨

둡니다.

각 엔터티 (예: 컴퓨터)는 구분에 속해야 합니다. Endpoint Protector 클라이언트 배포 시 만약 설정된 구분이 발견되면 컴퓨터는 등록하고 구분에 속하게 됩니다.

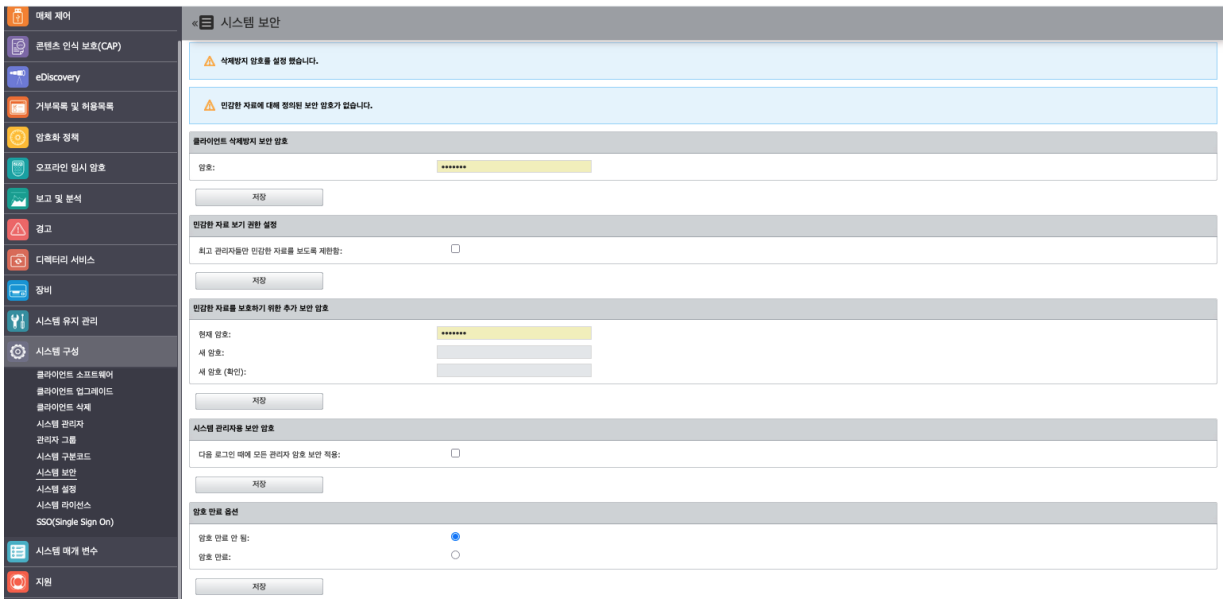
예: 컴퓨터 Test-PC는 "developers"라는 구분에 등록되었습니다. 이 경우 해당 컴퓨터에 로그인 된 사용자인 Test는 컴퓨터 Test-PC에 연결된 장치와 함께 같은 구분에 할당됩니다.

최고 관리자(예: root)는 구분에 상관없이 모든 주요 엔터티들에 접근합니다. 최고 관리자는 구분 이외에 일반 관리자 또는 다른 역할을 가진 관리자를 만들 수 있습니다. 최고 관리자는 구분을 관리하기 위해 관리자를 할당합니다.

일반 관리자는 할당된 구분만 관리할 수 있습니다. 또한 다른 구분에 연결된 엔터티들은 볼 수 없습니다.

16.9. 시스템 보안

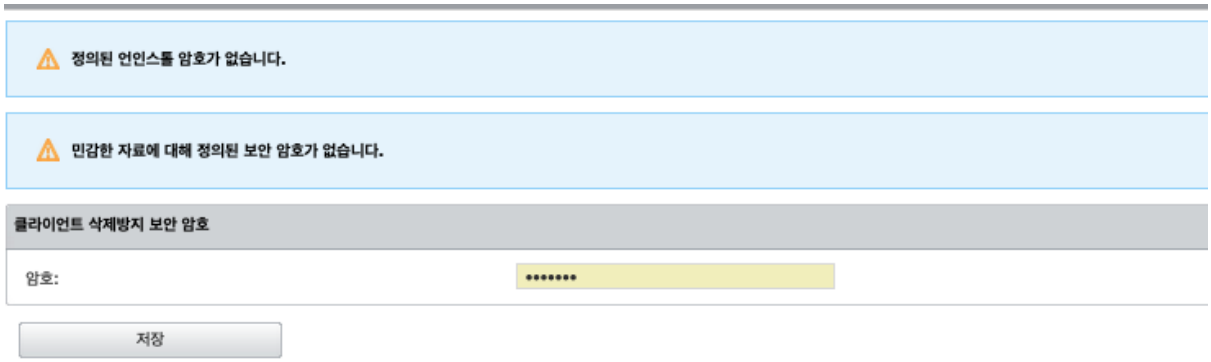
이 섹션에서 클라이언트 삭제방지 보안 암호, 최고 관리자들만 민감한 자료를 보도록 제한함, 민감한 자료를 보호하기 위한 추가 보안 암호, 다음 로그인 때에 모든 관리자 암호 보안 적용, 암호 만료 옵션과 같은 여러 보안 설정을 구성할 수 있습니다.



16.9.1. 클라이언트 삭제방지 보안 암호

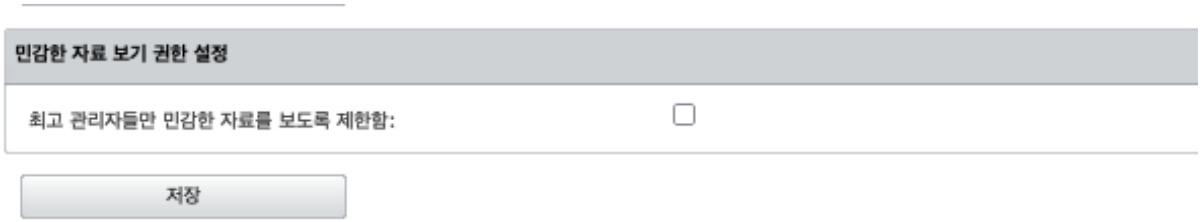
이 섹션에서 사용자가 Endpoint Protector 클라이언트 삭제 작업을 수행할 때 필요한 암호를 설정할 수 있습니다.

참고: 페이지 상단에서 이 작업의 암호가 설정되어 있는지 여부를 메시지로 보입니다.



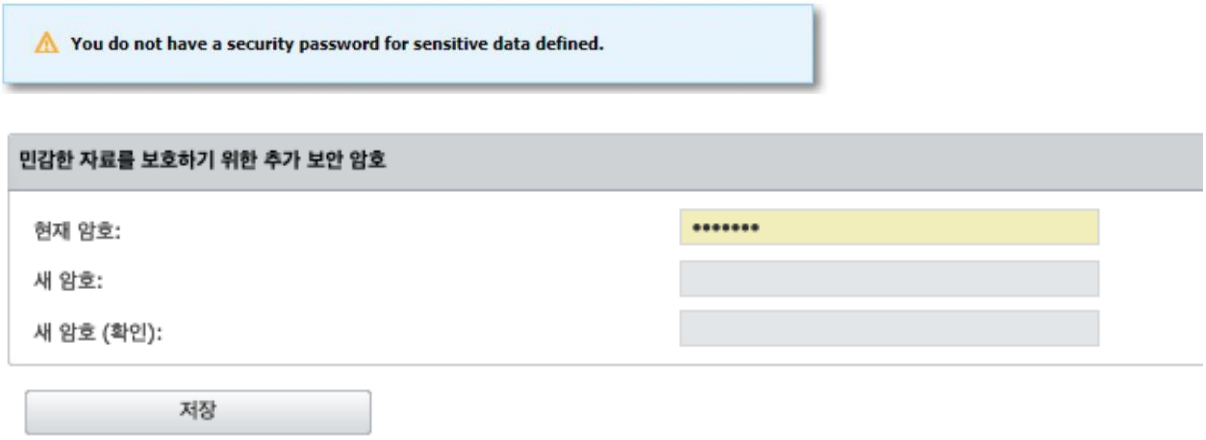
16.9.2. 민감한 자료 보기 권한 설정

이 섹션에서는 최고 관리자만 민감한 데이터에 접근을 허용할 수 있습니다.



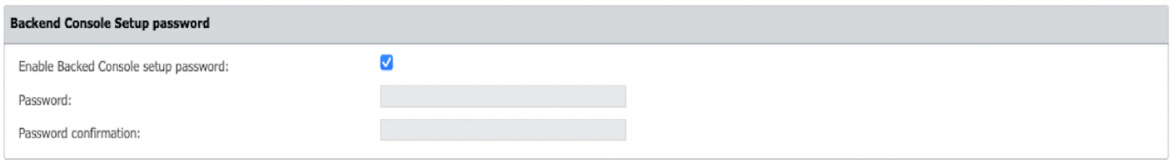
16.9.3. 민감한 자료를 보호하기 위한 추가 보안 암호

참고: 페이지 상단에서 이 작업의 암호가 설정되어 있는지 여부를 메시지로 보입니다.



16.9.4. 백엔드 콘솔 암호 설정

이 기능은 권한이 있는 사용자만 백엔드 콘솔에서 중요한 설정을 구성할 수 있도록 허용하여 보안을 강화합니다. 이 보호 기능을 활성화하려면 "시스템 구성 > 시스템 보안 > 백엔드 콘솔 암호 설정" 에서 백엔드 콘솔 암호 설정 사용을 체크합니다. 변경 사항을 저장하여 보안 계층을 추가하고 더욱 안전하고 통제된 환경을 만듭니다.



중요: 이 기능은 Ubuntu 22에 맞추어서 설계가 되었습니다. 아래와 같이 백엔드 비밀번호 설정 및 적용이 가능합니다:

- Ubuntu 14와 Ubuntu18에서는 '나가기'를 누르면 비밀번호를 다시 입력할 필요 없이 메뉴가 새로 고쳐집니다.
- Ubuntu 22에서는 '나가기'를 누르면 비밀번호를 다시 묻는 메시지가 표시됩니다.

참고: 암호 보호를 적용하려면 EPP 서버 어플라이언스를 재부팅해야 합니다. 유의하시기 바랍니다.

참고: 비밀번호는 ASCII 문자 집합이 지원됩니다.

16.9.5. 시스템 관리자용 보안 암호

이 섹션에서 다음 로그인 세션에서 모든 관리자가 보안 암호를 사용하도록 요구할 수 있습니다.

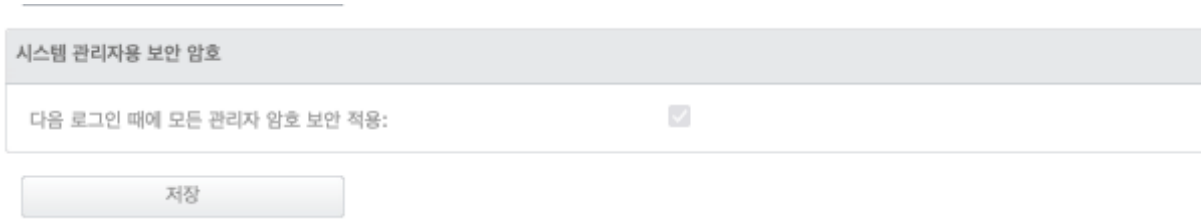
참고: "다음 로그인 때에 모든 관리자 암호 보안 적용" 설정을 한 번 사용하면 이 기능을 사용 안 함으로 할 수 없습니다.

한 번 사용되면 암호 복장성을 아래 규칙을 준수해서 정의할 수 있습니다:

- 최소 9자 사용
- 대소문자, 숫자, 특수문자 반드시 포함
- 오름차순으로 연속 문자 및 숫자를 사용할 수 없음

중요: 다음 로그인 때에 모든 관리자 암호 보안 적용 설정은 고급 사용자 암호 설정보다 우선합

니다. 이 설정은 또한 보고 및 분석, 읽기만 사용자 등 관리자가 아닌 사용자에 적용할 수 있습니다.



16.9.6. 고급 사용자 암호 설정

이 섹션에서 모든 사용자에게 고급 사용자 암호를 설정할 수 있습니다.

암호 복잡성을 사용할 수 있고 다음 정보를 제공합니다:

- 최소 암호의 길이: 8
- 최소 암호의 대문자 글자수: 1
- 최소 암호의 소문자 글자수: 1
- 최소 암호의 숫자 수: 1
- 최소 특수문자의 수: 1
- 연속되거나 순차적인 글자가 있다면 선택

만료된 암호가 시행될 때 다음 정보를 제공합니다:

- **암호 유효 기간**은 30 일까지 설정
- **새 암호는 이전 4개와 다르면 선택**

시스템 관리자 섹션에서 새로운 관리자를 만들 때 반드시 요구되는 사항입니다.

중요: 고급 사용자 암호 설정 섹션에 대한 모든 정보가 제공되면 관리자 뿐만 아니라 모든 사용자는 다음 로그인에 암호 변경이 요구됩니다.

16.10. 시스템 설정

이 섹션에서 관리자는 전체 시스템에 적용하는 일반 설정을 구성할 수 있습니다. 이러한 설정의 대부분은 이미 초기 Endpoint Protector 마법사에 포함이 되어있습니다.

16.10.1. 구분코드 사용

구분코드를 기반으로 클라이언트에 접근하는 옵션을 선택합니다.

기본 구분코드로 defdep를 볼 수 있습니다.

참고: 더 자세한 정보는 **시스템 구분코드** 섹션을 참조하시기 바랍니다.

16.10.2. 세션 설정

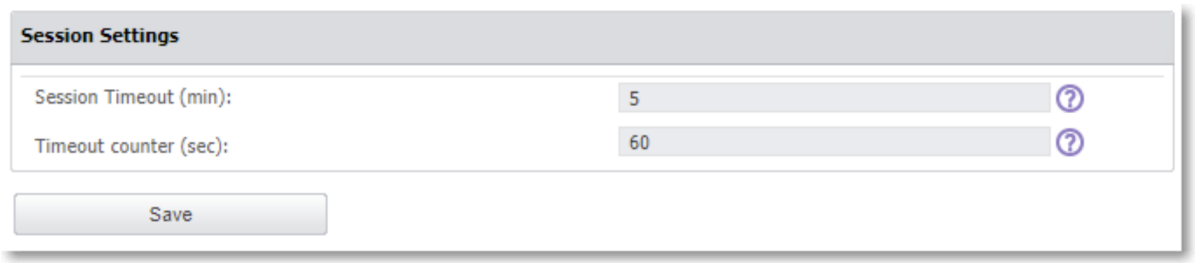
아래와 같이 세션 타임아웃 설정을 수정할 수 있습니다:

- **세션 타임아웃** – 5분에서 60분 사이로 세션이 만료될 때까지 사용자 비활성화되는 시간

을 설정합니다.

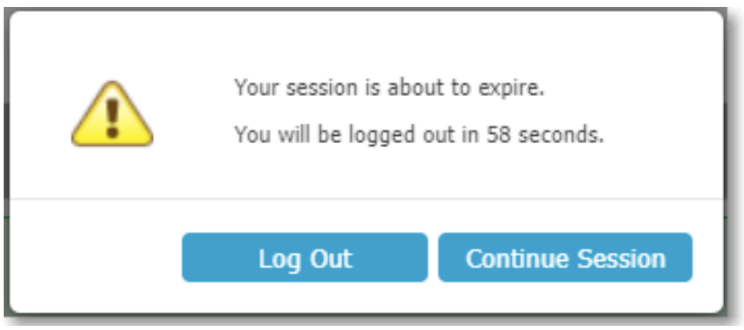
- **세션 카운터** – 5초와 세션 타임아웃 분에서 1분을 뺀 시간 사이에 세션 타임아웃 카운트다운 시간을 설정합니다.

예: 세션 타임아웃이 5분 그리고 타임아웃 카운터가 60초로 정의하면 사용자 비활성화 4분후에 60초 후에 로그아웃 된다는 팝업 창이 뜹니다.



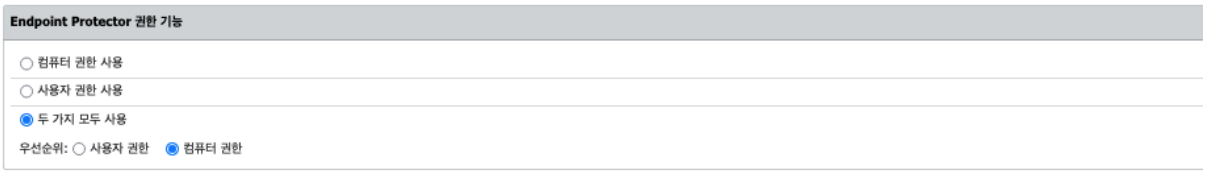
정의된 시간 동안 동작이 없으면 Endpoint Protector는 응답을 멈추고 미리 정의된 카운트다운에서 만료된 세션을 가리키는 메시지가 표시됩니다.

로그아웃을 선택하거나 세션을 유지할 수 있습니다. 이 때 세션 타임아웃 가격은 재설정됩니다.



16.10.3. Endpoint Protector 권한 기능

컴퓨터, 사용자, 두 가지 모두에 대한 기능 권한을 설정합니다. 두 가지 모두에 대해서 사용자 권한 또는 컴퓨터 권한 우선순위를 설정할 수 있습니다.



16.10.4. 스마트 그룹

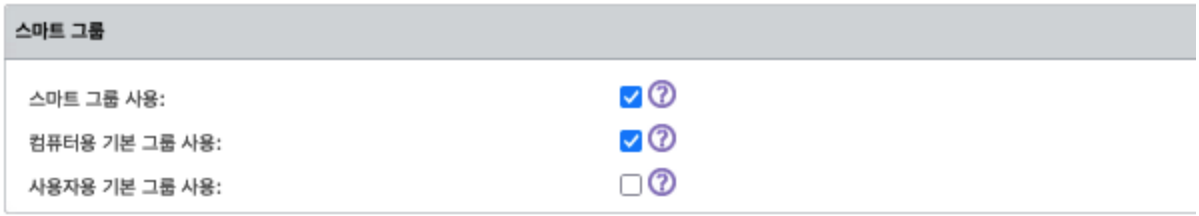
스마트 그룹, 컴퓨터 또는 사용자에 대한 기본 그룹에 관련된 설정을 관리합니다.

참고: 스마트 그룹은 이름 패턴 기반으로 구성원을 정의할 수 있는 동적인 그룹입니다.

- **스마트 그룹 사용** – 이 설정을 사용하지 않으면 스마트 그룹은 할당된 엔터티가 없는 일반 그룹으로 변환되고 컴퓨터용 기본 그룹과 사용자용 기본 그룹은 삭제됩니다.
- **컴퓨터용 기본 그룹 사용** – 스마트 그룹에 포함되지 않은 모든 컴퓨터를 기본 그룹으로 만듭니다.

  참고: 이 설정을 사용하지 않으면 컴퓨터용 기본 그룹은 삭제됩니다.
- **사용자용 기본 그룹 사용** – 스마트 그룹에 포함되지 않은 사용자를 기본 그룹으로 만듭니다.

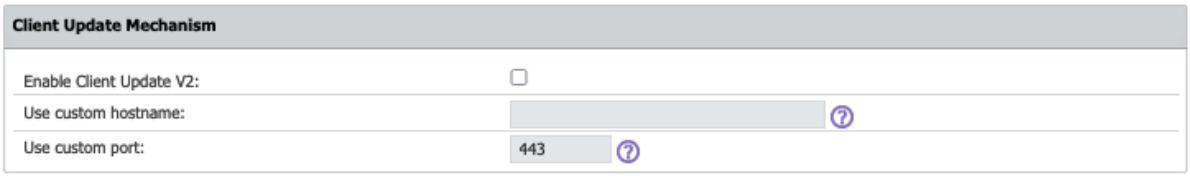
  참고: 이 설정을 사용하지 않으면 컴퓨터용 기본 그룹은 삭제됩니다.



16.10.5. 클라이언트 업데이트 메커니즘

클라이언트 업데이트 V2 설정을 사용하면 클라이언트 업데이트 성능을 향상시키고 **사용자 정의 호스 이름**과 **포트**를 추가합니다.

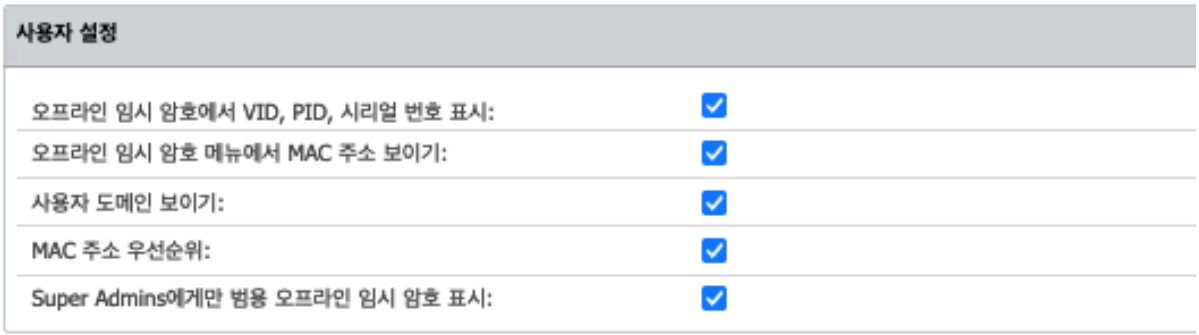
참고: 이 섹션에서 정의한 사용자 정의 포트는 기본 443 대신에 클라이언트 업데이트 다운로드 링크를 만들 때 사용됩니다.



16.10.6. 사용자 설정

Endpoint Protector의 더 자세한 정보 표시는 아래 내용을 사용합니다:

- **오프라인 임시 암호에서 VID, PID, 시리얼 번호 표시**
- **오프라인 임시 암호 메뉴에서 MAC 주소 보이기**
- **사용자 도메인 보이기**
- **MAC 주소 우선순위**
- **Super Admins에게만 범용 오프라인 임시 암호 표시**



16.10.7. 로그 설정

다음 로그 설정을 관리합니다.

- .csv 포맷으로 로그 보고서 내보내기를 위해 백만으로 **최대 행 수**를 설정합니다.

  참고: 1.0으로 최대 행 수를 설정하면 하나의 로그에 한 행으로 로그 보고서 .csv 내보내기에 1백만 로그가 내보내기 됩니다.

서버에 로그 파티션을 가지면 내보내기를 만들 때 날짜 또한 선택이 되도록 보장합니다.

- **보고서 V2 사용**은 콘텐츠 인식 보호 로그 구조를 수정하고 **목적지 상세**, **이메일 보낸 사람**, **이메일 주제** 정보가 컬럼에 표시됩니다.

  참고: Endpoint Protector 5.7.0.0 이전 버전에서는 보고서 V2 설정을 기본으로 사용하지 않습니다.

이 설정으로 사용된 구조는 SIEM에도 영향을 줍니다.

- 콘텐츠 인식 보고서 로그에 표시되는 **이벤트 당 보고된 위협의 최대 수**를 설정합니다. 확장된 로그 상세 정보 섹션의 카운트 컬럼에서 확인합니다.

  참고: 100에서 1000 사이의 보고된 위협 숫자를 설정할 수 있습니다.

16.10.7.1. 로그 설정 사용 사례 및 용어

로그 요청 – Endpoint Protector 클라이언트에서 보내집니다.

이벤트 – 스캔된 문서의 스캔 결과입니다.

위협 – 일치된 아이템 (예: U.S SSN)

로그 요청:

- 이벤트 1.0 (스캔된 문서의 스캔 결과) => 이벤트 나뉨 전 1,000개의 위협
- 이벤트 1.1 => 500개의 위협
- 이벤트 2.0 => 200개의 위협
- 100개 이벤트 까지

예: 값을 500으로 설정합니다. 1,500, 600, 200 개의 위협이 포함된 3개의 문서는 콘텐츠 인식 보호 정책에 종속됩니다.

Endpoint Protector 클라이언트는 단일 로그 요청을 보냅니다.

로그 요청:

- 이벤트 1.0 (스캔된 문서의 스캔 결과) => 500개의 위협 => 이벤트 나뉨
- 이벤트 1.1 (스캔된 문서의 스캔 결과) => 500개의 위협 => 이벤트 나뉨 (보고서에서 두 번째 로그 엔트리)
- 이벤트 1.2 (스캔된 문서의 스캔 결과) => 500개의 위협 (보고서에서 세 번째 로그 엔트리)
- 이벤트 2.0 (스캔된 문서의 스캔 결과) => 500개의 위협 => 이벤트 나뉨
- 이벤트 2.1 (스캔된 문서의 스캔 결과) => 100개의 위협 (보고서에서 두 번째 로그 엔트리)
- 이벤트 3.0 (스캔된 문서의 스캔 결과) => 200개의 위협
- 100개의 이벤트까지

16.10.8. 콘텐츠 인식 보호 – 모든 민감한 정보 보고

모든 민감한 정보 보고 설정 사용은 Endpoint Protector가 탐지된 파일에서부터 **보고된 임계값의 최대 수** 영역에 설정 제한까지 정책에 적용된 모든 민감한 정보의 로그를 허용합니다.

참고: 이 설정은 로그 양을 증가시켜 잠재적으로 클라이언트와 서버 성능에 영향을 줍니다.

중요: 보고 제한 설정은 **모든 민감한 정보 보고** 설정보다 우선합니다. 만약 **보고 제한**을 사용하면 보고는 임계값에 도달하면 정지합니다.

보고된 위협의 최대 수는 아래에 따라서 자동으로 수정됩니다:

User Input	Input Updated
0	1
1.000.000	100.000
>= 100.000	100.000

콘텐츠 인식 보호 보고 제한은 보고만 정책입니다.

- 이 기능을 사용하면 EPP 클라이언트는 보고 전용 정책이 만족하다고 판단할 만큼 충분한 위협이 발견되면 위협 고고를 중집합니다.

"콘텐츠 인식 보호 – 임계값 무시" 토글은 차단 및 정책을 나타냅니다.

- 이 토글을 켜짐으로 설정하면 차단으로 결정되어도 검사가 중지되지 않고 전송에서 발견된 추가 위협을 계속 보고합니다.
- 이 경우 보고되는 위협의 수를 제한하려면 '최대 보고 위협 수' 설정 값을 0보다 큰 값으로 설정할 수 있습니다. 설정 값은 보고된 위협의 수만 나타내며 실제 보고된 위협의 수는 이보다 약간 더 많을 수 있습니다.

CAP 정책의 Boolean 논리에 "AND" 연산자가 하나 이상 포함된 경우 "임계값 무시"를 설정하면 무시/무효화 됩니다. Boolean 논리(예: 아래 참조)가 식별자 당 하나 이상의 일치 항목으로 정책이 충족됩니다.

예: (이메일 AND SSN US) OR CC Visa

예제 – 시나리오 1:

- CAP 정책:
  - 차단 및 보고

- 위협 임계값: 4
- 콘텐츠 감지 규칙: (이메일 AND SSN US) 또는 CC Visa

- 임계값 무시: ON
  - 보고된 위협의 최대 수: 10
- 제한된 보고: OFF
- 테스트 파일 포함:
  - 이메일: 2
  - SSN US: 3
  - CC Visa: 6
  - IBAN: 22

이 예제에서 정책의 'AND' 연산자로 '위협 임계값'이 충족되는지 여부와 관계없이 정책이 총족되면 시작됩니다 (Boolean 논리). 테스트 파일의 데이터 구조에 따라 EPP 클라이언트는 EPP 서버에 서로 다른 10개의 위협을 보고할 수 있습니다.

- 2 이메일 + 2 SSN US + 6 CC Visa
- 또는 1 이메일 + 3 SSN US + 6 CC Visa
- 기타 등등

참고: CAP 정책에서 Boolean 논리의 부분이 아닌 식별자는 보고되지 않습니다.

일반적으로 CAP 정책 (차단 및 보고)는 정책의 Boolean 로직이 충족되면 시작됩니다. 그러나 '임계값 무시'가 활성화되어 있고 정책에 'AND' 연산자가 1개 이상인 경우, 스캔 엔진은 '보고 제한' (매체 제어 – 전체 설정)의 활성화 여부와 상관없이 '위협 임계값' 설정을 무시하고 총 위협이 10에 도달할 때까지 스캔을 계속합니다.

일반적으로 CAP 정책 (보고만)은 정책의 Boolean 로직이 충족되면 시작됩니다. 그러나 '임계값 무시'가 활성화되어 있고 정책에 'AND' 연산자가 1개 이상 있는 경우, 스캔 엔진은 '위협 임계값' 설정을 무시합니다. '보고 제한' (매체 제어 – 전체 설정)을 활성화한 경우, '임계값 무시'의 '보고된 최대 위협 수' 설정에서 총 위협 수가 10에 도달할 때까지 검사가 계속됩니다.

일반적으로 CAP 정책 (보고만)은 정책의 Boolean 로직이 충족되면 시작됩니다. 그러나 '임계값 무시'가 활성화되어 있고 정책에 'AND' 연산자가 1개 이상 있는 경우, 스캔 엔진은 '위협 임계값' 설정을 무시합니다. '보고 제한' (매체 제어 – 전체 설정)이 비활성화되어 있는 경우 검사 엔진은 전체 파일이 검사될 때까지 검사를 계속하지만 '임계값 무시'에서 '보고된 최대 위협 수'로 설정한 10개의 위협만 보고합니다.

예제 – 시나리오 2:

- CAP 정책:
  - 차단 및 보고
  - 위협 임계값: 4
  - 콘텐츠 감지 규칙: (이메일 AND SSN US) 또는 CC Visa
- 임계값 무시: ON
  - 보고된 위협의 최대 수: 4
- 보고된 제한: OFF
- 테스트 파일 포함:
  - 이메일: 2
  - SSN US: 3
  - CC Visa: 6
  - IBAN: 22

이 예제에서 정책의 'AND' 연산자로 인해 '위협 임계값'이 충족되는지 여부와 관계없이 정책이 충족되면 정책이 트리거 됩니다 (Boolean 논리). 테스트 파일의 데이터 구조에 따라 EPP 클라이언트는 EPP 서버에 서로 다른 4가지 위협을 보고할 수 있습니다.

- 1 이메일 + 1 SSN US + 2 CC Visa
- 또는 2 이메일 + 1 SSN US + 1 CC Visa
- 또는 1 이메일 + 2 SSN US + 1 CC Visa

일반적으로 CAP 정책 (차단 및 보고)는 정책의 Boolean 로직이 충족되면 시작됩니다. 그러나 '임계값 무시'가 활성화되어 있고 정책에 'AND' 연산자가 1개 이상인 경우, '보고 제한' (매체 제어 – 전체 설정)이 활성화되어 있더라도 스캔 엔진은 '위협 임계값' 설정을 무시하고 '최대 보고된 위협 수' 설정 총 위협이 4에 도달할 때까지 스캔을 계속합니다.

일반적으로 CAP 정책 (보고만)은 정책의 Boolean 로직이 충족되면 시작됩니다. 그러나 '임계값 무시'가 활성화되어 있고 정책에 'AND' 연산자가 1개 이상 있는 경우, 스캔 엔진은 '위협 임계값' 설정을 무시합니다. '보고 제한' (매체 제어 – 전체 설정)이 활성화된 경우, '임계값 무시'에서 '보고된 최대 위협 수'를 설정한 총 위협 수가 4에 도달할 때까지 검사가 계속됩니다.

일반적으로 CAP 정책 (보고만)은 정책의 Boolean 로직이 충족되면 시작됩니다. 그러나 '임계값 무시'가 활성화되어 있고 정책에 'AND' 연산자가 1개 이상 있는 경우, 스캔 엔진은 '위협 임계값' 설정을 무시합니다. '보고 제한' (매체 제어 – 전체 설정)이 비활성화되어 있는 경우, 검사 엔진은 전체 파일이 검사될 때까지 검사를 계속하지만 '임계값 무시'에서 '보고된 최대 위협 수'로 설정한 4개의 위협만 보고합니다.

예제 – 시나리오 3:

- CAP 정책:
  - 보고만
  - 위협 임계값: 4

    - 콘텐츠 감지 규칙: (이메일 AND SSN US) 또는 CC Visa

- 임계값 무시: ON
    - 보고된 위협의 최대 수: 10
- 제한된 보고: ON
- 테스트 파일 포함:
    - 이메일: 2
    - SSN US: 3
    - CC Visa: 6
    - IBAN: 22

이 예제에서 정책이 충족되면 (Boolean 논리), 즉 모든 식별자가 '위협 임계값'이 1이상에 도달하면 정책이 시작되며, '임계값 무시'의 '최대 보고 위협 수' 설정은 무시됩니다. 테스트 파일의 데이터 구조에 따라 EPP 클라이언트는 단일 위협을 EPP 서버에 다르게 보고할 수 있습니다.

- 1 이메일 + 1 SSN US
- 또는 1 CC Visa

일반적으로 CAP 정책 (보고만)은 모든 식별자가 '위협 임계값'이 1이상에 도달하는 등 정책의 Boolean 논리가 충족되면 시작됩니다. '보고 제한' (매체 제어 – 전체 설정)이 활성화되면 스캔 엔진은 '임계값 무시' 에서 ' 최대 보고된 위협 수'를 무시합니다. 정책이 충족되면 즉시 보고가 중지됩니다.

일반적으로 CAP 정책 (보고만)은 정책의 Boolean 논리가 충족 될 때, 즉 모든 식별자가 최소 1의 '위협 임계값'에 도달할 때 시작됩니다. '보고 제한' (매체 제어 – 전체 설정)이 비활성화되어 있으면 스캔 엔진은 '임계값 무시'의 '보고된 위협의 최대 수'를 고려합니다. 위협이 10개 발견되면 보고가 중지됩니다.

예제 – 시나리오 4:

- CAP 정책:
    - 차단 및 보고
    - 위협 임계값: 4
    - 콘텐츠 탐지 규칙: 이메일 또는 SSN US 또는 CC Visa
- 임계값 무시: ON
    - 보고된 위협의 최대 수: 10
- 제한된 보고: OFF
- 테스트 파일 포함
    - 이메일: 2
    - SSN US: 3
    - CC Visa: 6
    - IBAN: 22

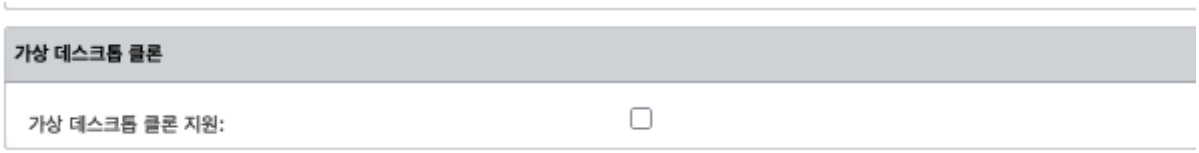
이 예제에서는 정책이 충족될 때 (Boolean 로직), 즉 하나 이상의 식별자 (예: 이메일)가 '위협 임계값' 4에 도달할 때 정책이 시작되지만 스캔 엔진은 '임계값 무시'에서 '최대 보고된 위협 수'를 설정한 총 위협이 10에 도달할 때까지 계속 스캔합니다. 테스트 파일의 데이터 구조에 따라 EPP 클라이언트는 EPP 서버에 서로 다른 10개의 위협을 보고할 수 있습니다.

- 2 이메일 + 2 SSN US + 6 CC Visa
- 또는 1 이메일 + 3 SSN US + 6 CC Visa
- 기타

일반적으로 CAP 정책 (차단 및 보고)는 정책의 Boolean 로직이 충족되면 시작됩니다. 그러나 '임계값 무시'가 활성화되어 있고 정책에 'AND' 연산자가 없는 경우, 스캔 엔진은 '임계값 무시'의 '최대 보고된 위협 수'를 설정한 총 위협 수 10에 도달할 때까지 검색합니다.

16.10.9. 가상 데스크톱 클론

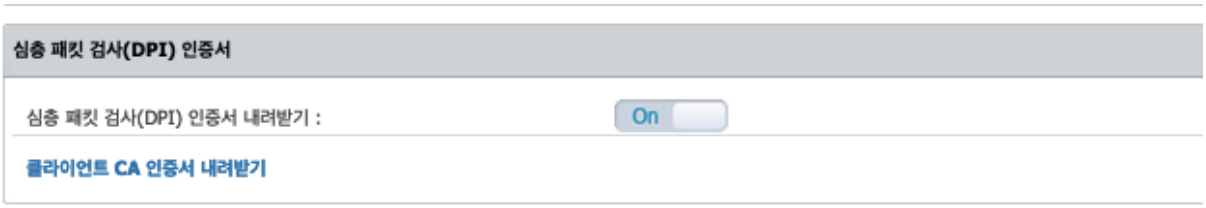
가상 데스크톱 클론 지원 설정을 사용하면 Endpoint Protector 서버가 가상 데스크톱 클론 식별하고 Endpoint Protector 클라이언트와 상호작용을 할 수 있도록 허용합니다.



16.10.10. 심층 패킷 검사 (DPI) 인증서

심층 패킷 검사 (DPI) 다운로드를 사용하지 않으면 Endpoint Protector 클라이언트는 기존 인증서 사용을 요구합니다. **클라이언트 CA 인증서**를 다운로드 할 수 있습니다.

이 기능의 더 자세한 내용은 심층 패킷 검사 (DPI) 섹션을 참조하시기 바랍니다.



16.10.11. 서버 인증 스택

이 세션은 사용자 정의 서버 인증서를 다시 만들기 위해 사용합니다.

옵션을 사용하고 다음 정보를 제공하시기 바랍니다:

- **FQDN (Fully Qualified Domain Name)** – 인증서, **서버 인증서 스택 다시 만들기**, macOS에서 심층 패킷 검사(DPI)에 사용되는 CA 인증서에 사용됩니다.
- **국가 이름** – 국가의 첫 번째 두 글자를 추가합니다.
- **주 또는 지방 이름** – 주 또는 지방 이름을 추가합니다.
- **로컬 이름** – 로컬 이름을 추가합니다.

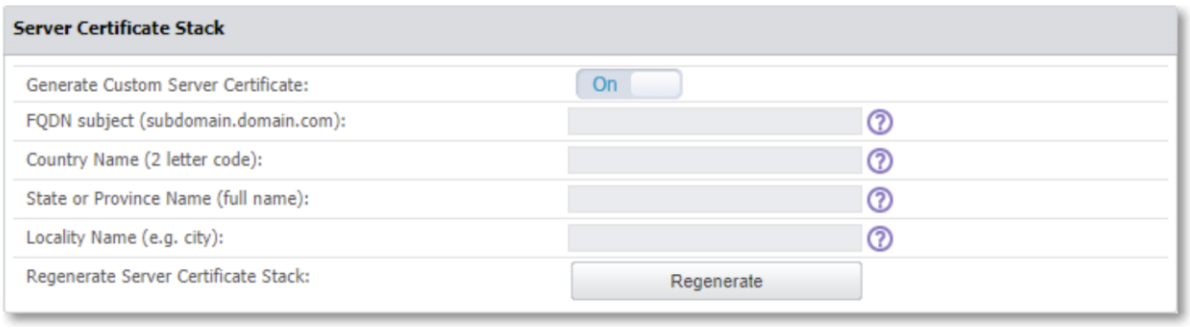
필수 정보를 모두 설정하면 이 설정 페이지 아래로 스크롤해서 **저장**을 클릭하고 서버 인증서 스택 세션으로 돌아와서 **서버 인증서 스택 다시 만들기**를 클릭합니다.

몇 분 후에 서버 인증서가 다시 만들어지고 사용자는 로그아웃 됩니다.

중요: macOS에서 심층 패킷 검사(DPI)를 다시 다운로드하고 키체인에서 신뢰를 받으시기 바랍니다.

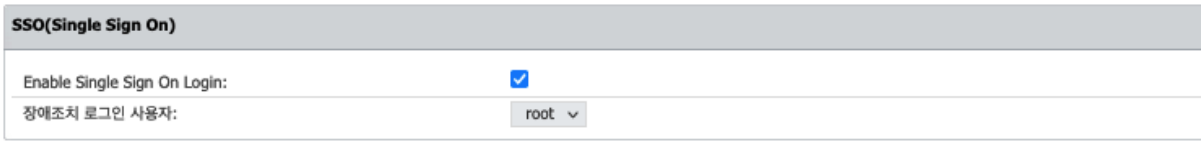
참고: 이 설정은 macOS 12.0+ 에서 유효합니다. 그러나 CA 인증서 재생성 할 때 macOS 11.0에서 대체합니다 – 인증서 다운로드 및 **시스템 > 키 체인 접근** 추가.

중요: Endpoint Protector 서버에 등록된 macOS 12.0+ 인스턴스가 없다면 이 설정을 사용하면 안 됩니다.



16.10.12. SSO (Single Sign On)

SSO (Single Sign On) 로그인 사용 설정은 Endpoint Protector에 로그를 남기고 SSO 기능이 작동하지 않을 때 **장애조치 로그인 사용자**를 선택합니다.



16.10.13. Active Directory 인증

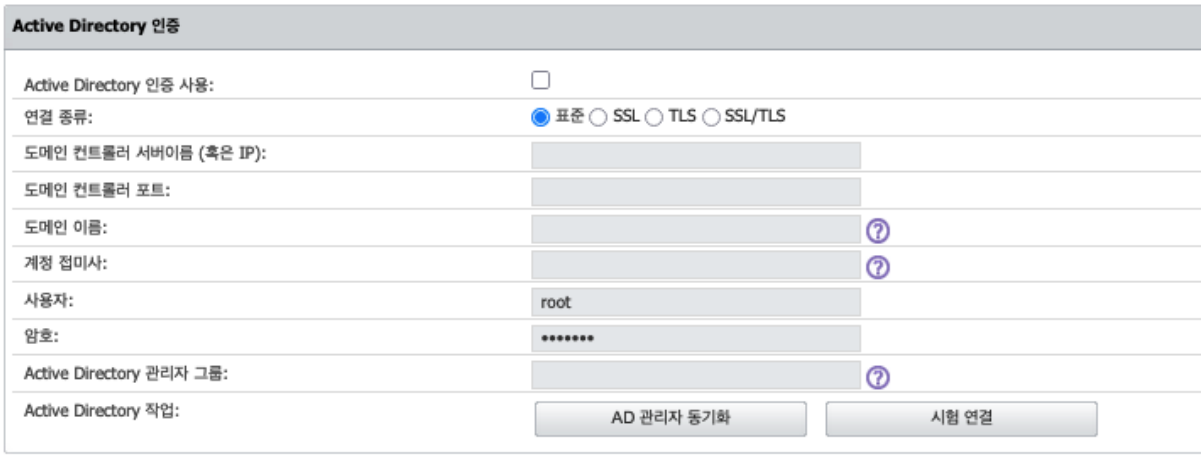
Active Directory 인증 사용 설정은 Endpoint Protector에 Active Directory의 관리자 그룹을 최고 관리자로 가져옵니다.

참고: Active Directory 인증을 사용하여 관리자가 Endpoint Protector에 로그인을 위해 Active Directory 계정을 사용하는 것을 허용합니다.

Active Directory 관리자 그룹을 가져오기 위한 단계는 아래와 같습니다:

1. 아래 사항을 고려해서 요구 정보 필드를 채웁니다.
    a. 일부의 경우에 **사용자 이름**(domain₩username) 앞에 도메인 추가가 필요합니다.
    b. **Active Directory 관리자 그룹**은 Microsoft에서 작업이 제한되는 **"primary groups"**을 제외한 다른 모든 사용자 그룹과 동기화 할 수 있습니다.
2. 페이지 버튼을 스크롤해서 변경을 저장합니다 – 페이지 상단에 성공 메시지를 볼 수 있습니다.
3. **Active Directory 인증**으로 돌아가서 **시험 연결**을 클릭해서 프로세스가 성공되었는지 확인합니다.
4. **AD 관리자 동기화**를 클릭합니다.

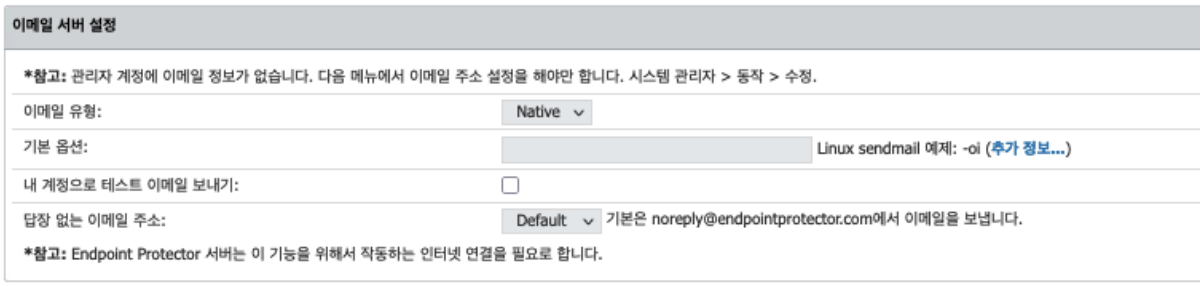
중요: Active Directory 관리자 그룹을 정의하면 이 AD 그룹의 사용자만 동기화되고 Endpoint Protector의 최고 관리자로 가져오기 됩니다. 추가 관리자 (다른 접근 레벨을 가진)는 **시스템 관리자** 섹션에서 수동으로 만들 수 있습니다.



16.10.14. 이메일 서버 설정

사용하는 이메일 유형을 기반으로 이메일 서버 설정을 관리합니다 – **native** 또는 **SMTP**.

참고: 이 기능을 사용하려면 인터넷 연결이 필요합니다.



이메일 유형에 따라 이메일 서버 설정을 관리하시기 바랍니다 (기본 또는 SMTP). TLS 1.3을 지원합니다.

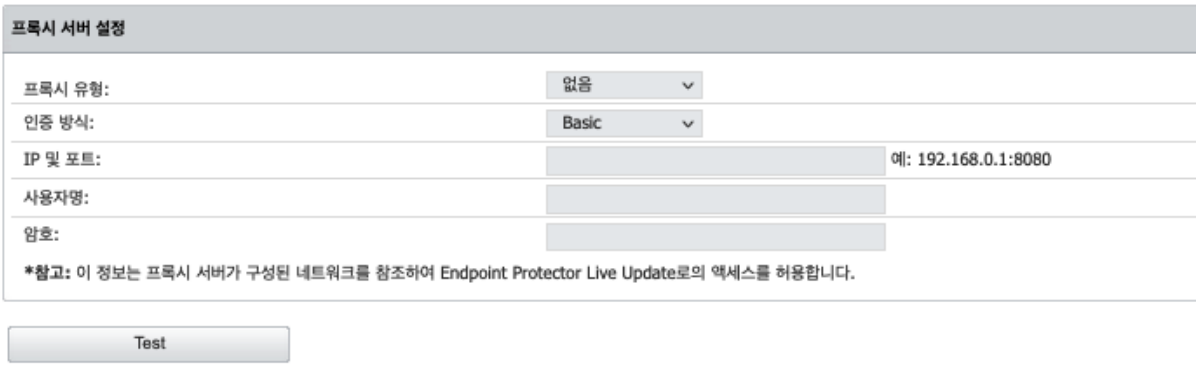
16.10.15. 프록시 서버 설정

아래 내용을 관리해서 프록시 서버 설정을 구성합니다.

- **프록시 유형**
- **인증 방식**
- **IP 및 포트**
- **프록시 접근 계정(사용자명/암호)**

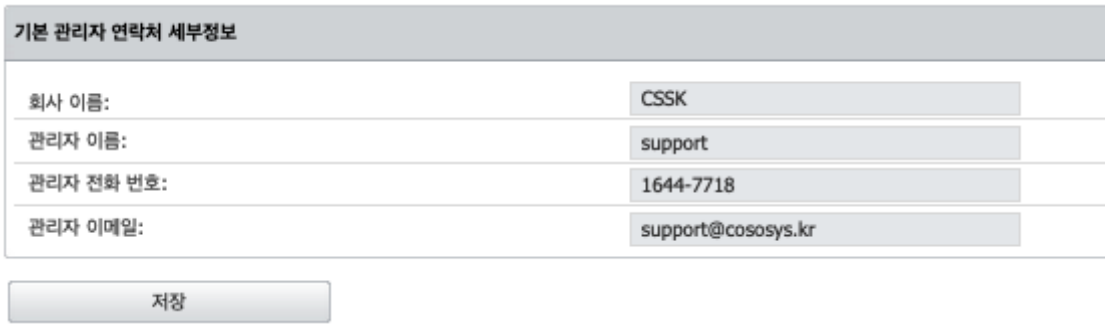
모든 정보가 입력되면 설정이 성공적으로 동작되는지 확인을 위해 **Test** 를 클릭합니다.

참고: 프록시 서버가 구성되지 않으면 Endpoint Protector는 liveupdate.endpointprotector.com에 직접 연결됩니다.



16.10.16. 기본 관리자 연락처 세부정보

주요 관리자의 상제 연락처를 편집하고 모든 변경을 유지하기 위해서 **저장**을 클릭합니다.

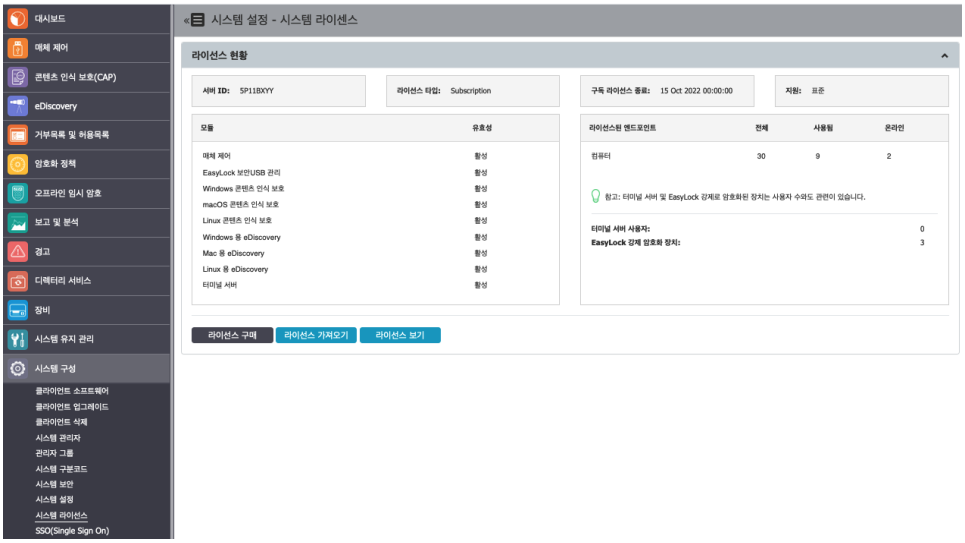


16.10.17. EPP 서버 이름 표시

EPP 사용자는 Endpoint Protector UI 내에서 환경을 시각적으로 구분하는 기능을 사용할 수 있습니다. 이 기능을 통해 사용자는 로그인 페이지의 Endpoint Protector 로고 위에 사용자 지정 텍스트를 추가할 수 있으며, Endpoint Protector 헤더의 로고 옆에 사용자 지정 로고를 추가할 수 있습니다. 개인화를 위해 텍스트와 로고를 사용자가 지정하고 업로드할 수 있습니다. 이러한 시각적 구분은 잘못된 환경에서 의도하지 않은 수정과 같은 사고를 방지하기 위해 설계되었습니다.

16.11. 시스템 라이선스

이 섹션에서 Endpoint Protector 라이선스 상태의 전체적으로 볼 수 있고 관리할 수 있습니다.



참고: Endpoint Protector 버전 5.9.0.0부터 새로운 구독 기반 라이선스 시스템이 도입되었습니다 – 해외 기준. 이 변경으로 프리미엄 기능에 대한 라이선스 제한이 제거되어 모든 고객에게 문맥 감지 같은 기능에 대한 무제한 액세스가 허용됩니다. 이러한 조정은 개정된 라이선스 모델에 따라 모든 기능을 표준으로 분류하여 모든 사용자가 액세스할 수 있습니다.

Endpoint Protector 라이선스는 두 가지 요소를 기반으로 합니다.

- **모듈** – 모든 모듈은 라이선스로 분리되고 (콘텐츠 인식 보호, eDiscovery 등) 매체 제어 모듈이 반드시 포함되어야 합니다.
- **엔드포인트** – 보호가 필요한 Windows, Mac, Linux 컴퓨터를 참조하고 이 컴퓨터에 설치된 Endpoint Protector 클라이언트가 있습니다.

선택된 모듈과 엔드포인트를 기반으로 라이선스 파일은 제공될 것입니다.

Endpoint Protector **서버 ID**는 각 서버의 고유 식별자이고 라이선스 파일과 연결됩니다. 라이선스 구매전에 서버 ID는 반드시 제공되어야 합니다.

시스템에 **구독 라이선스 종료**가 표시됩니다.

16.11.1. 무료 평가 라이선스

Endpoint Protector는 30일 무료 평가 라이선스를 한 번 제공합니다.

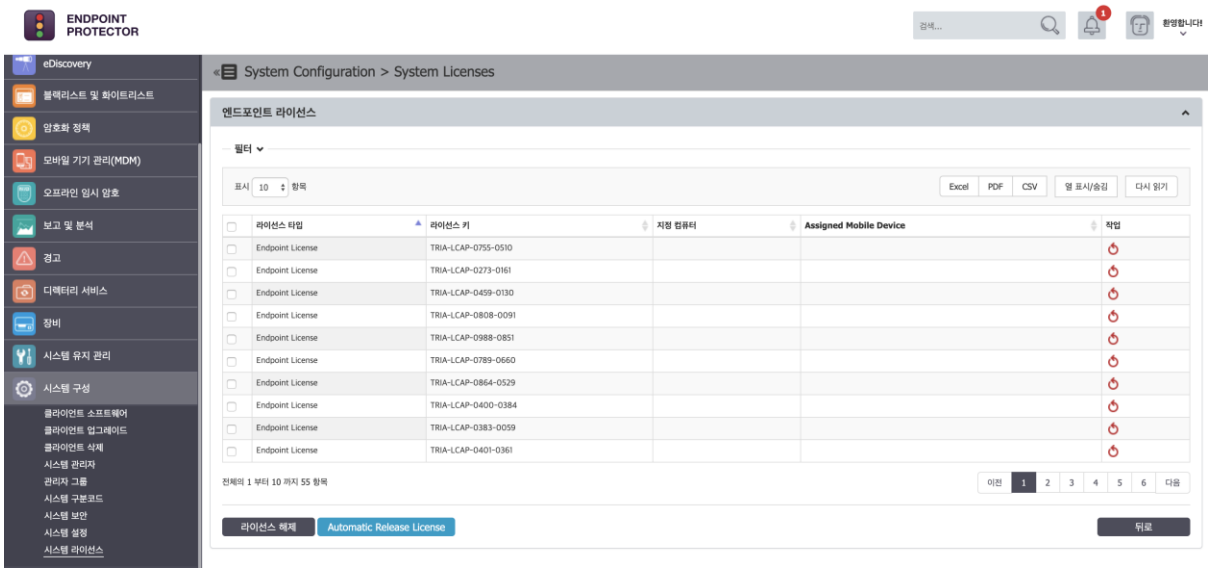
무료 평가판 버튼을 누르면 활성화 할 수 있습니다. 50대 컴퓨터 5대 모바일 기기에 대해서 모든 모듈을 자동으로 사용할 수 있습니다. 엔드포인트 라이선스는 **선착순** 기반으로 할당됩니다.

하나 또는 그 이상의 라이선스가 할당된 엔드포인트가 비활성화되고 재할당이 필요한 경우에 관리자는 이러한 라이선스를 다른 온라인 컴퓨터에 자동으로 재할당할 수 있습니다.

16.11.2. 라이선스 가져오기 및 관리

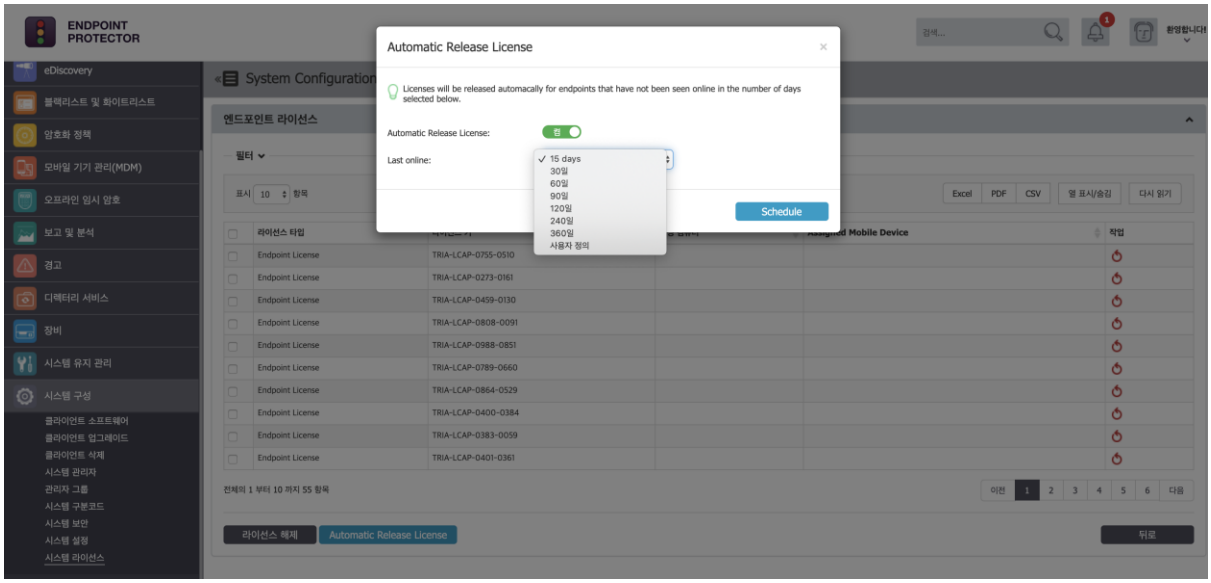
라이선스 가져오기 버튼은 라이선스 파일을 검색합니다. 이 파일은 모든 관련 정보가 포함되어 있습니다 (모듈, 엔드포인트 수, 만료일, 지원 유형 등).

라이선스 보기 버튼으로 엔드포인트 라이선스 관리를 할 수 있습니다.



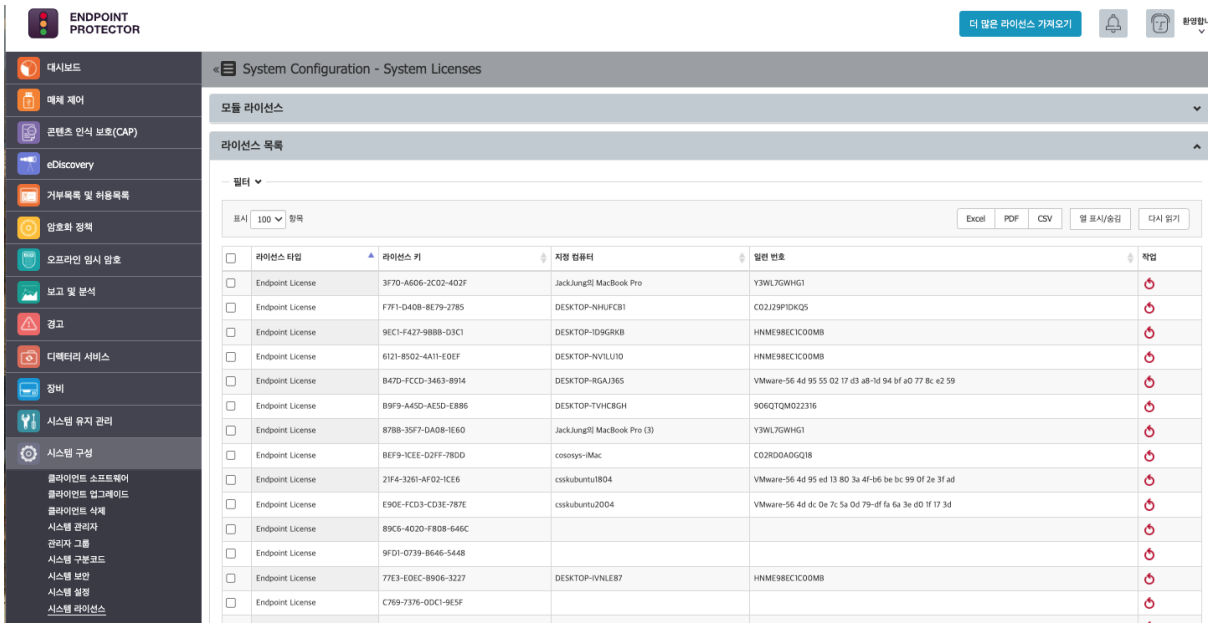
하나 또는 그 이상의 라이선스가 할당된 엔드포인트가 비활성화되고 재할당이 필요한 경우에 관리자는 이러한 라이선스를 다른 온라인 컴퓨터에 자동으로 재할당할 수 있습니다.

자동 라이선스 배포 기능을 사용하면 라이선스는 특정 기간 (15일, 30일, 90일 등 또는 사용자 정의) 동안 온라인으로 표시가 되지 않은 엔드포인트에 자동으로 배포될 것입니다.



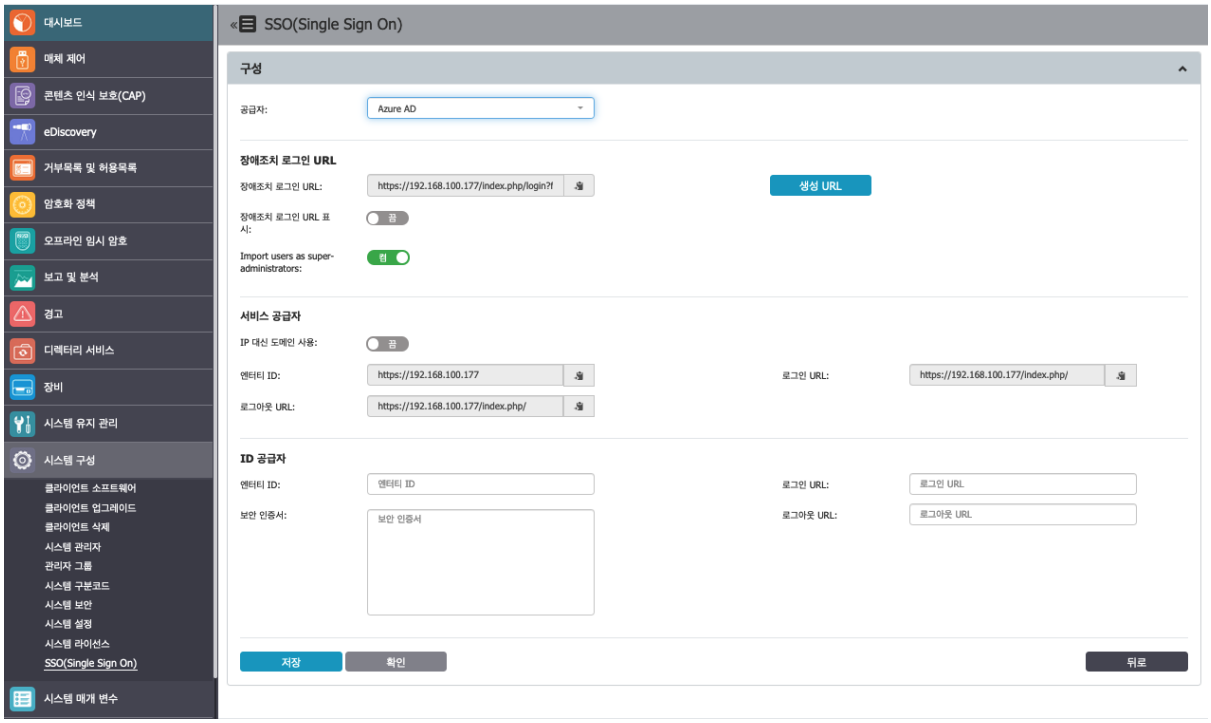
시스템 구성에서 라이선스 관리를 간소화하려면 **시스템 라이선스**으로 이동하여 **라이선스 보기** 섹션에서 일련 번호 필드를 찾습니다. 라이선스 테이블에서 일련 번호 열을 찾을 수 있습니다. 보기를 사용자 지정하려면 열 **표시/숨기기** 버튼을 사용하여 '**일련 번호**' (기본값은 '보기') 확인란을 선택하면 동일한 컴퓨터 이름의 문제를 해결하고 Machine UUID로 강화된 일련 번호 통합을 통해 보다 효과적으로 관리할 수 있습니다.

참고: 컴퓨터 일련 번호가 없는 경우, 엔드포인트 컴퓨터의 안전성 보장을 위해 이제 모든 OS 플랫폼에서 라이선스 페이지 열에 표시되는 Machine UUID로 대체됩니다.



16.12. SSO (Single Sign On)

SSO (Single Sign On) 기능은 관리자가 Azure AD 계정으로 Endpoint Protector 서버에 로그인 할 수 있도록 지원합니다. 만약 프리미엄 라이선스를 사용하면 OKTA의 SSO를 사용할 수 있습니다.



SSO 섹션은 아래 영역으로 구성되어 있습니다.

- **공급자** - 구성을 시작을 위해서 첫 번째로 선택되어야 합니다.
- **장애조치 로그인 URL** - Endpoint Protector 최고 관리자로 로컬 로그인이 허용되는 페이지의 링크를 제공하기 위해서 만들 수 있습니다. 이 URL 동작이 멈추는 상황에서 Azure SSO (Single Sign On) 로그인을 우회 합니다. URL을 보기 위해서 **장애조치 로그인 URL 표시** 설정을 사용합니다.

  참고: 최고 관리자로 사용자 가져오기 설정을 사용하면 모든 가져온 사용자는 최고 관리자 상태로 제공됩니다.

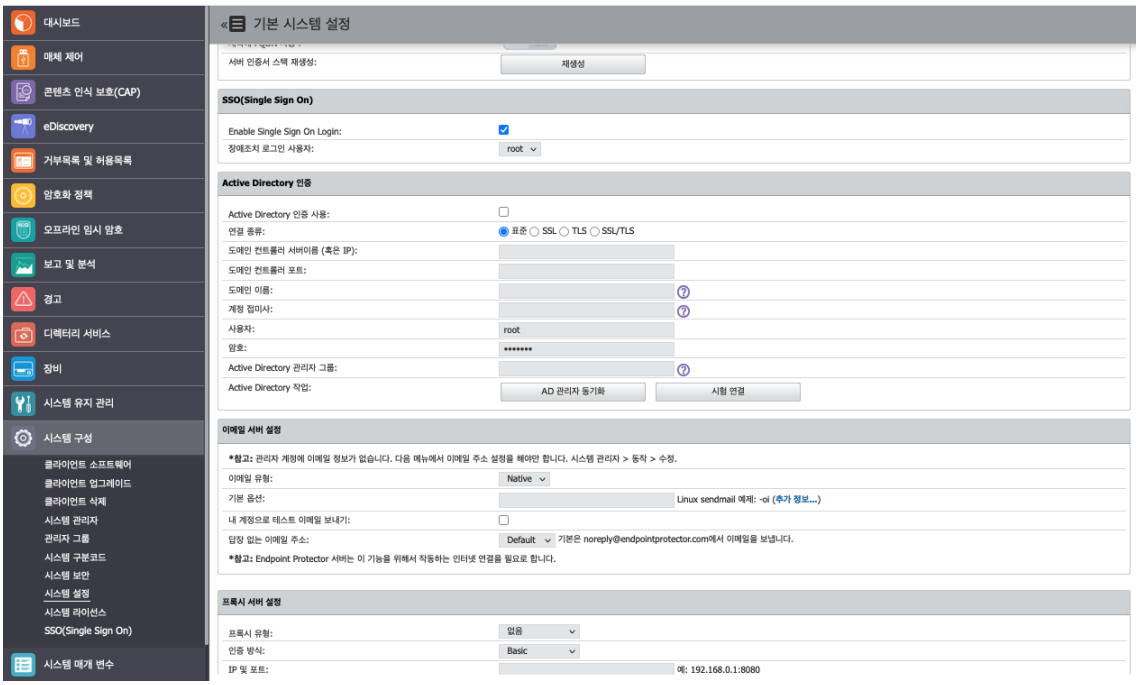
- **서비스 공급자** - Endpoint Protector 서버 식별을 나타냅니다. Azure에서 Endpoint Protector 응용프로그램을 구성할 때 정보가 필요합니다. **IP 또는 도메인**, **엔터티 ID**, **로그인** 및 **로그아웃 URL**을 기반으로 로그인을 선택합니다.

- **ID 공급자** - Azure 쪽을 나타냅니다. Azure에서 만들어진 데이터가 입력되어야 하는 영역이고 관리자는 Endpoint Protector 서버에 로그인할 수 있습니다.

16.12.1. Azure AD로 SSO (Single Sign One) 구성

Azure AD로 SSO 사용하려면 아래 단계를 따릅니다.

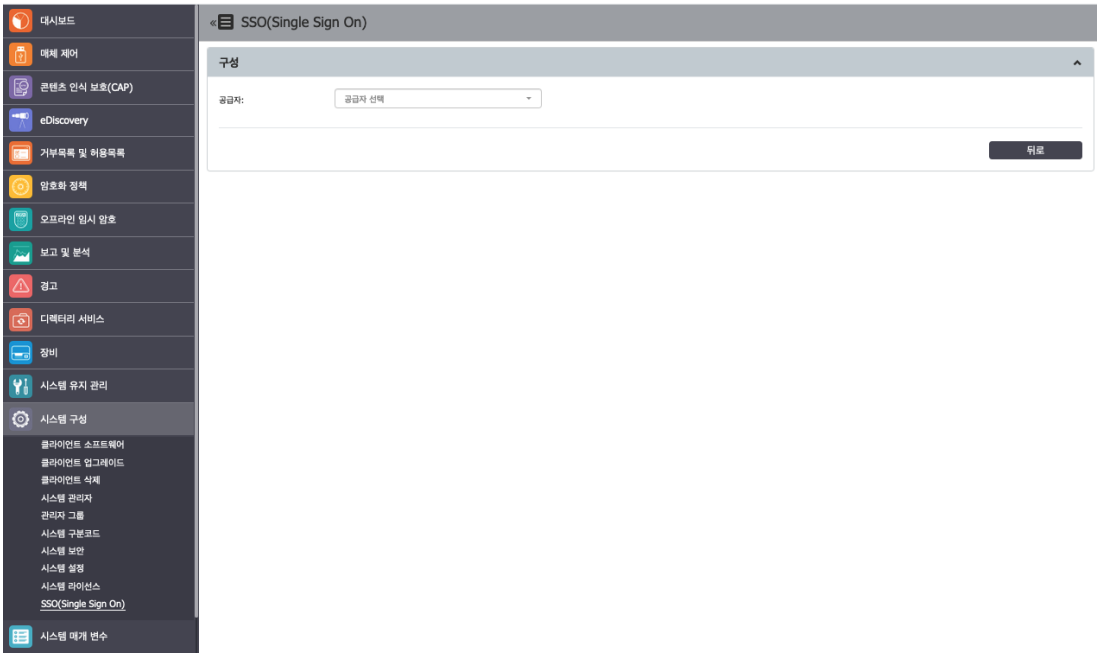
1. SSO를 사용하려면 **시스템 구성 > 시스템 설정 > SSO(Single Sign On)**로 이동합니다.
2. 사용하면 장애조치 로그인 사용자를 선택할 수 있도록 드롭다운 표시가 됩니다; root 사용자가 기본으로 선택됩니다.



위의 단계가 완료되면 SSO(Single Sign On) 하위 섹션이 시스템 구성 섹션에 표시됩니다.

참고: 선택된 장애조치 로그인 사용자는 선택된 동안 Endpoint Protector 서버에서 삭제할 수 없습니다. 장애조치 로그인 사용자가 없으면 SSO(Single Sign On)은 활성화되지 않습니다.

3. SSO (Single Sign On) 하위 섹션에서 공급자를 선택합니다.



4. **portal.azure.com** 이동 후 로그인합니다.

5. **Azure Active Directory**로 이동합니다.

6. 새로운 엔터프라이즈 애플리케이션을 만듭니다:

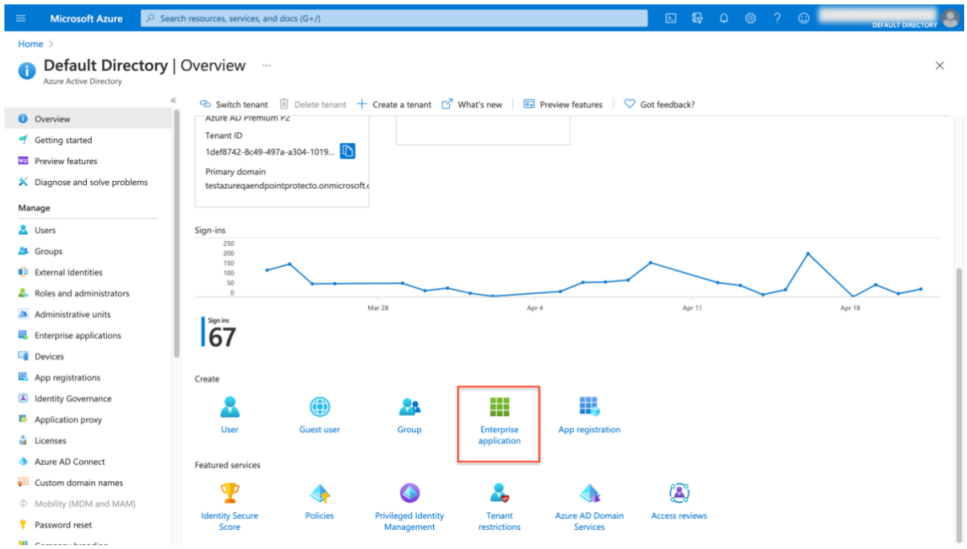
    a. **새로운 애플리케이션** 추가

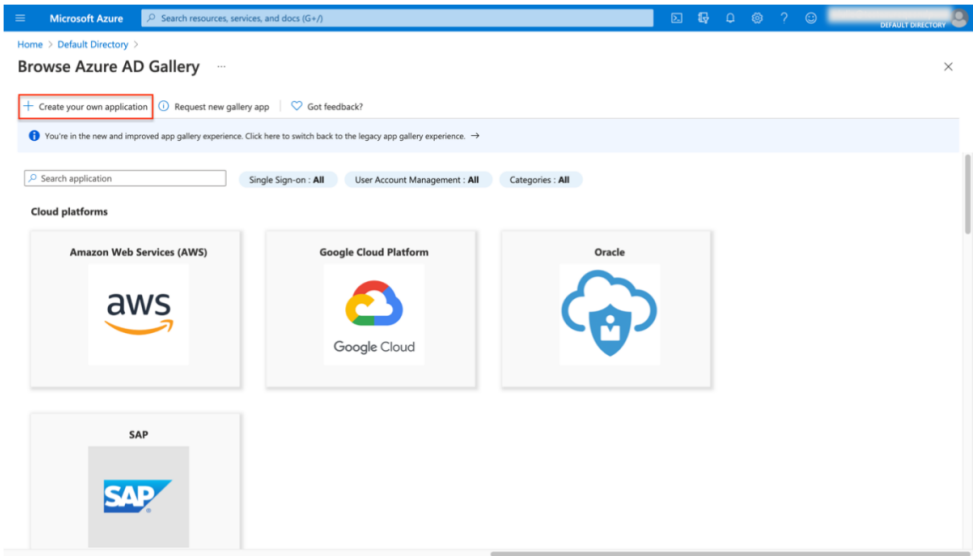
    b. **자신만의 애플리케이션 만들기** 클릭

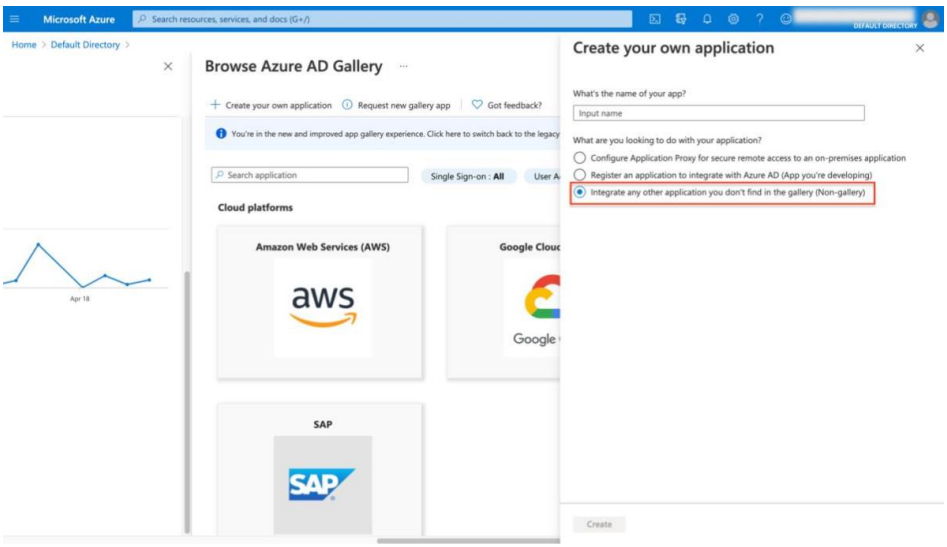
    c. 애플리케이션 이름 부여하기

    d. **갤러리에서 찾지 못하는 다른 모든 애플리케이션 통합** 선택

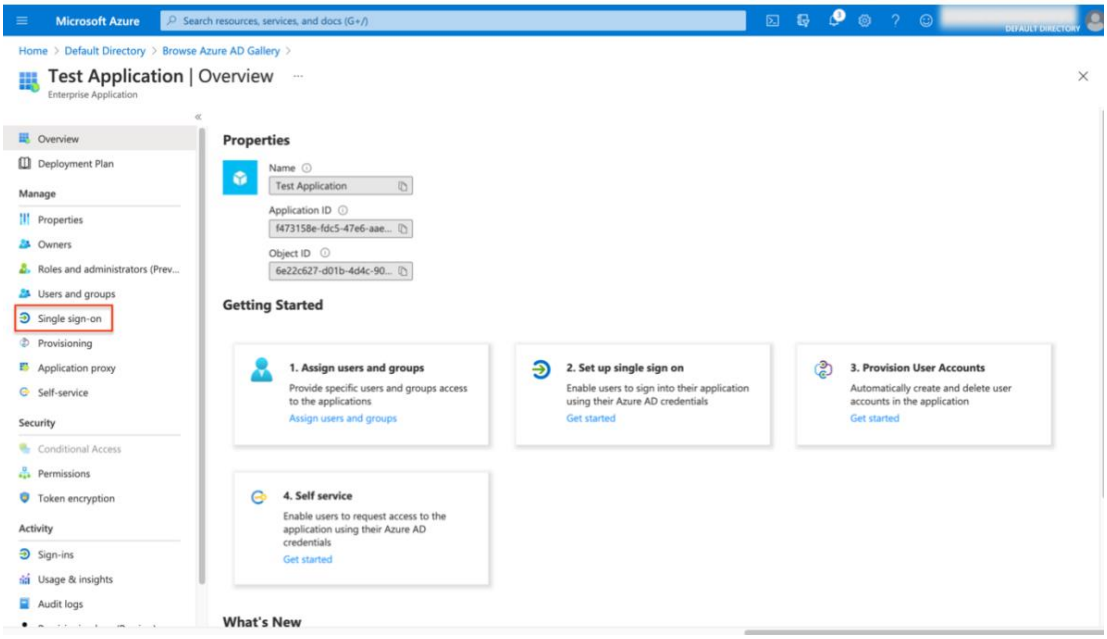
    e. **만들기** 클릭

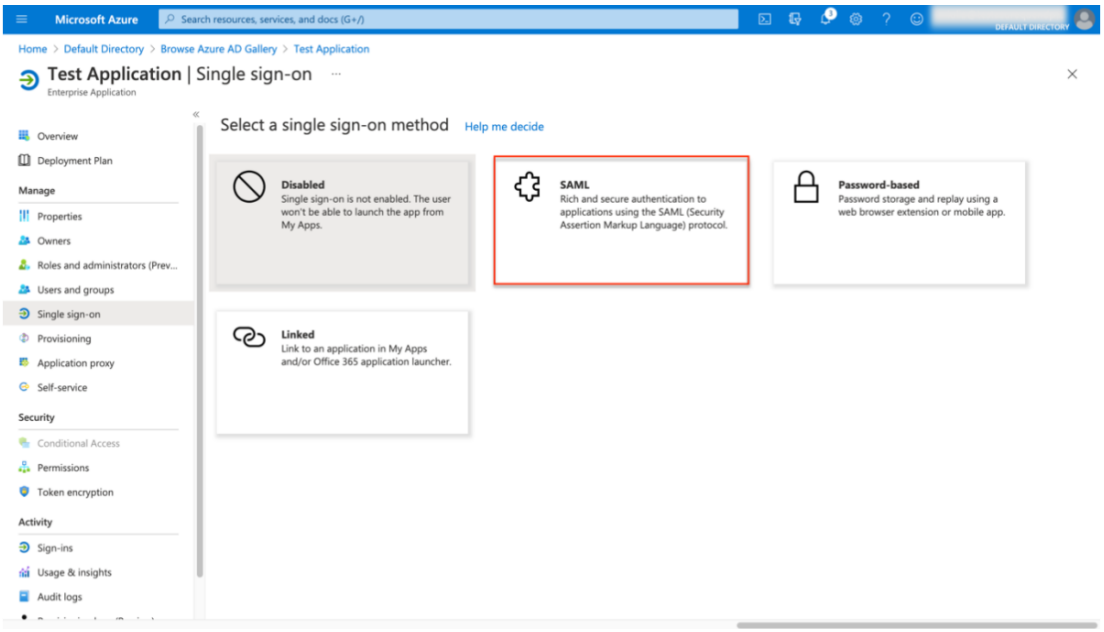






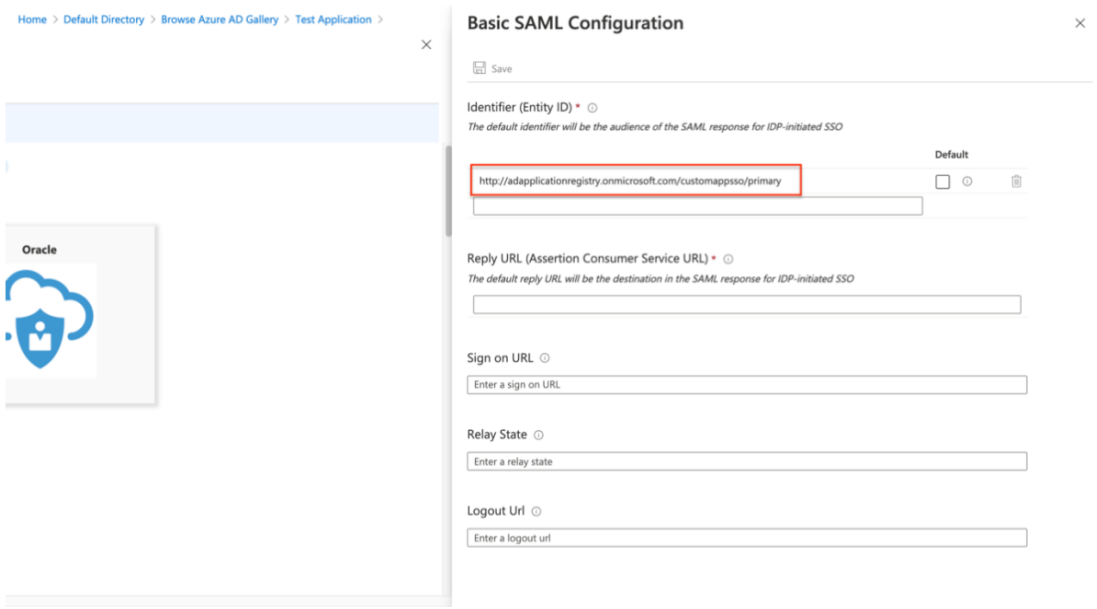
7. 왼쪽 메뉴에서 **Single Sign On** 으로 이동 후 **SAML** 방법을 선택합니다.





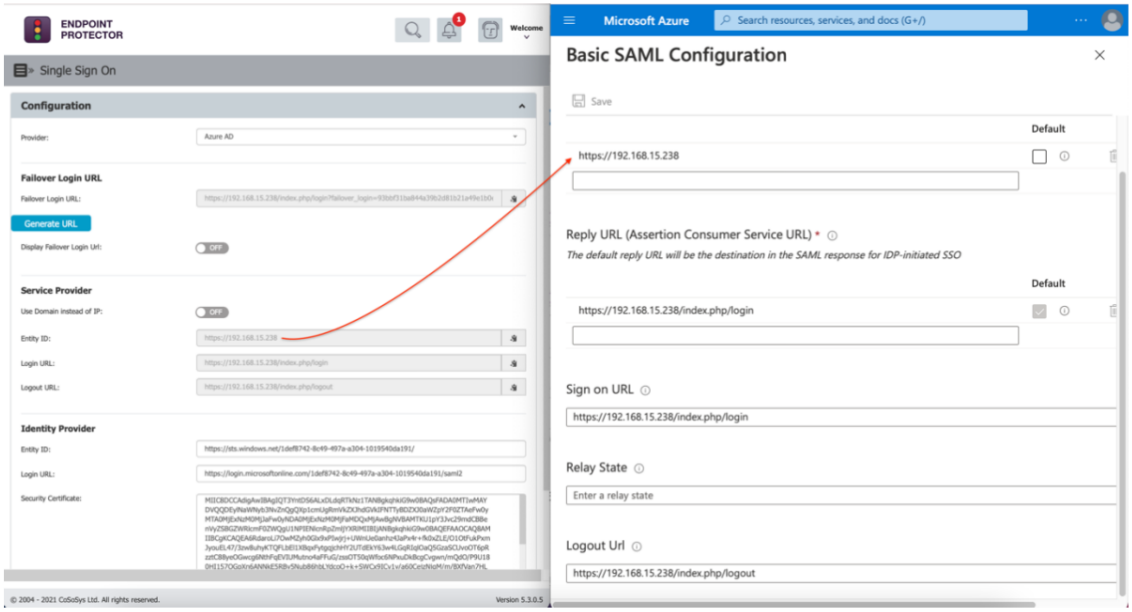
8. **기본 SAML 구성** 편집과 동시에 Endpoint Protector 서버에서 SSO (Single Sign On) 페이지로 들어갑니다. SSO 페이지의 데이터를 기본 SAML 구성 페이지에 복사 및 붙여 넣기 작업을 해야하기 때문입니다.

9. **기본 SAML 구성** 페이지에서 기본으로 식별 완성된 데이터를 삭제합니다 (객체 편집).



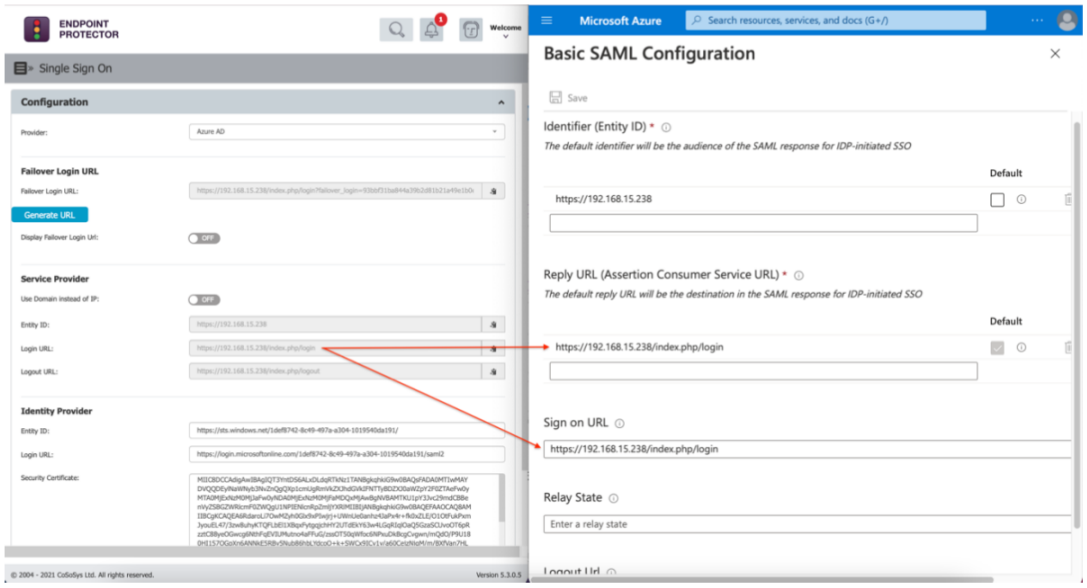
10. **Endpoint Protector 서버**의 **SSO(Single Sign On)** 페이지로 이동합니다:

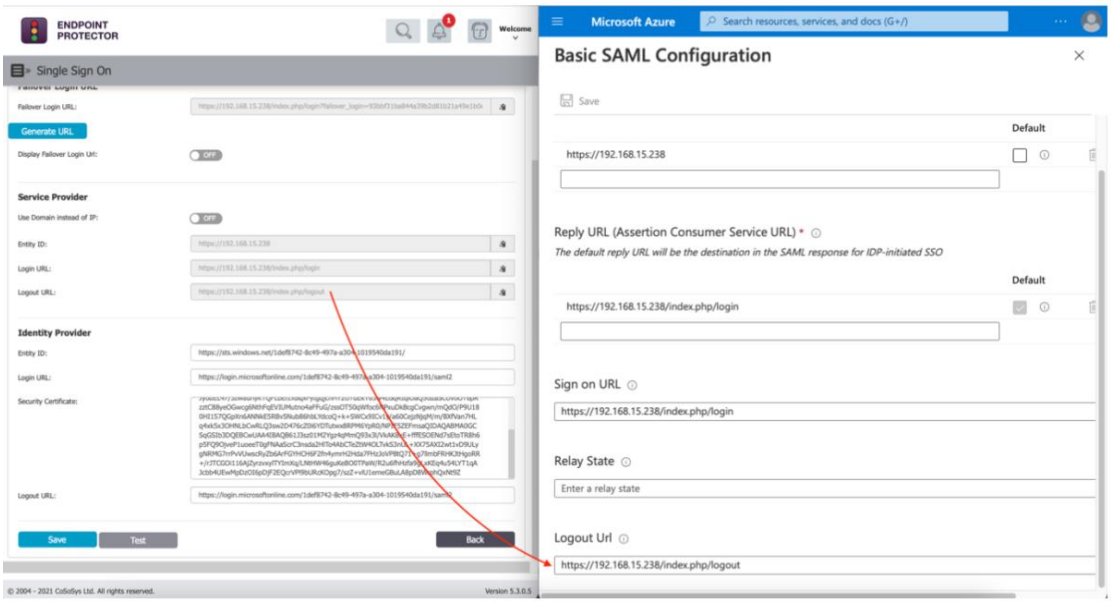
    a. **서비스 공급자**에서 **엔터티 ID** 데이터를 복사하고 기본 SAML 구성에서 식별자 (엔터티 ID) 영역과 URL 응답하기 (Assertion Consumer Service URL) 붙여 넣기를 하고 **기본** 설정(Default)에 체크합니다.



    b. **Endpoint Protector 서버**의 **SSO (Single Sign On)** 페이지에서 **서비스 공급자**의 **로그인 URL**을 복사하고 기본 SAML 구성 페이지의 **URL 서명**에 붙여넣기 합니다.

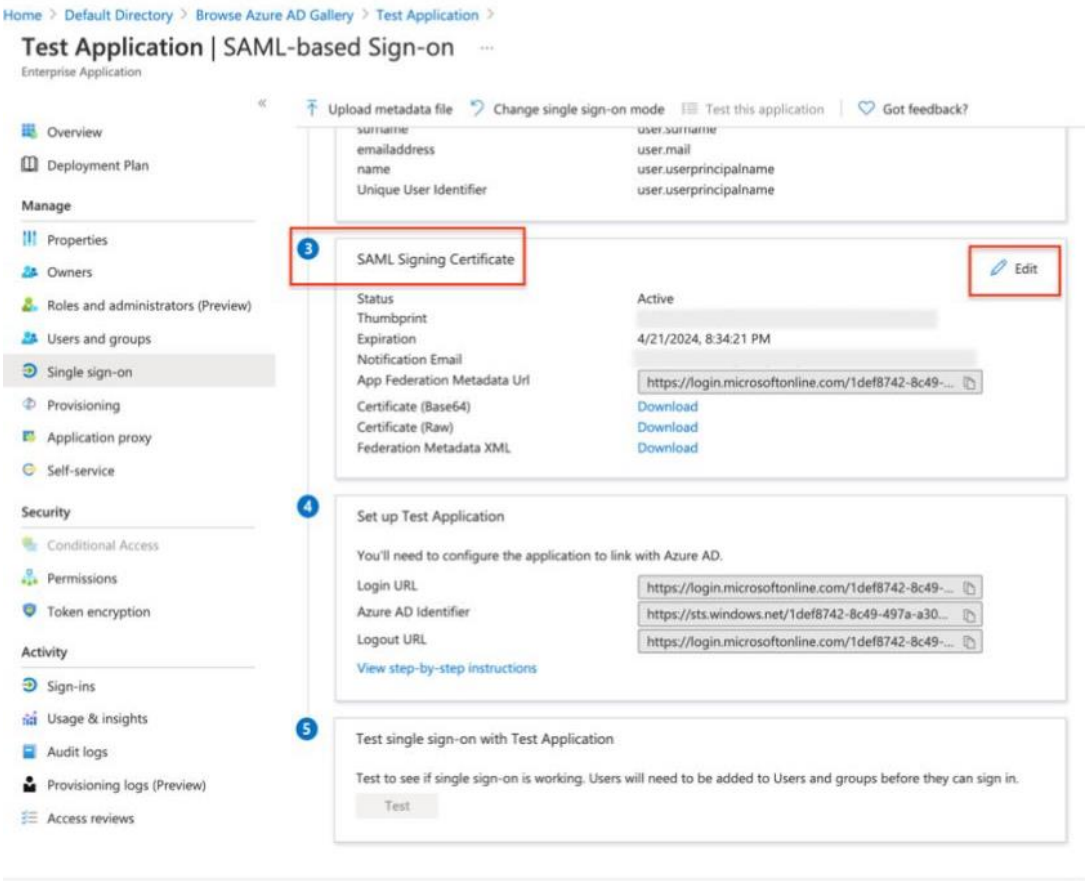
c. **Endpoint Protector 서버**의 **SSO (Single Sign On)** 페이지에서 **서비스 공급자**의 **로그아웃 URL**을 복사하고 기본 SAML 구성 페이지의 **로그아웃 URL**에 붙여넣기 합니다.



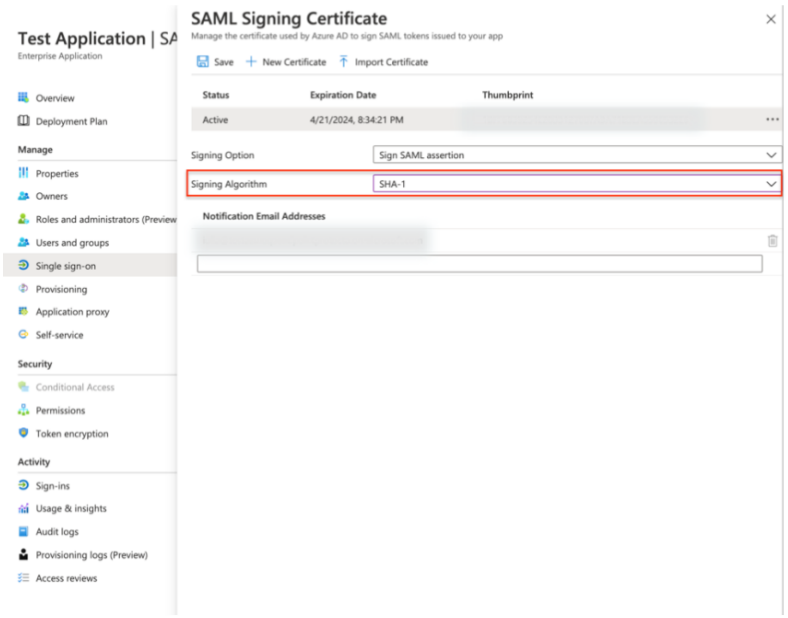


11. SSO (Single Sign On) 테스트 없이 설정을 저장합니다.

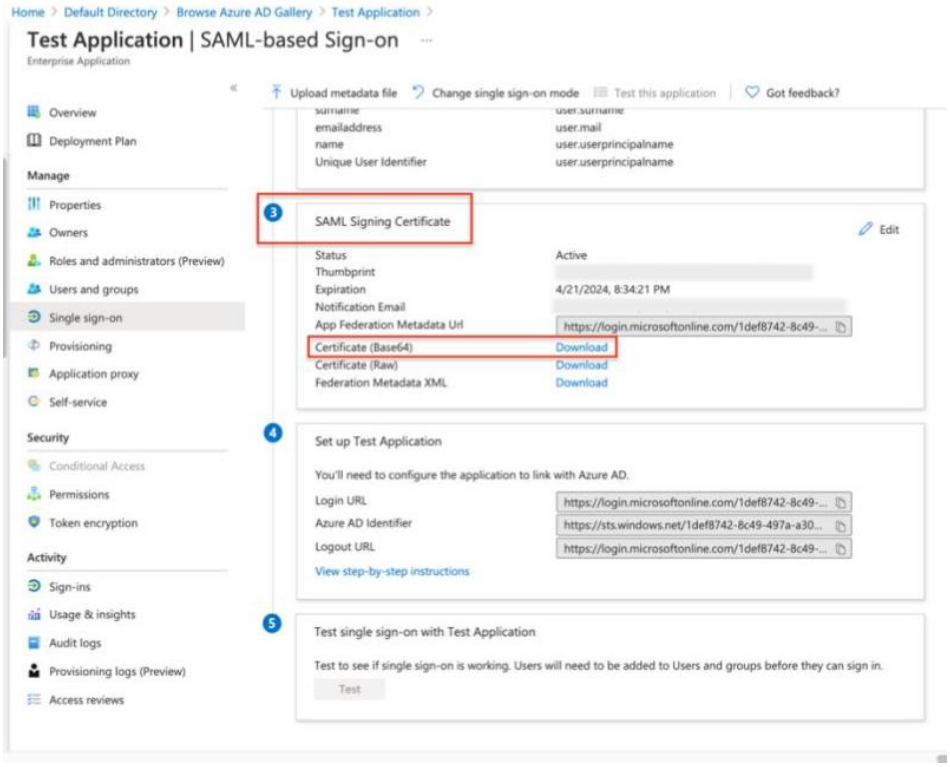
12. 페이지의 3번 단계인 **SAML 서명 인증서**로 이동해서 **편집**을 클릭합니다.



13. **서명 알고리즘**을 **SHA-1**으로 변경하고 **저장**을 클릭합니다.

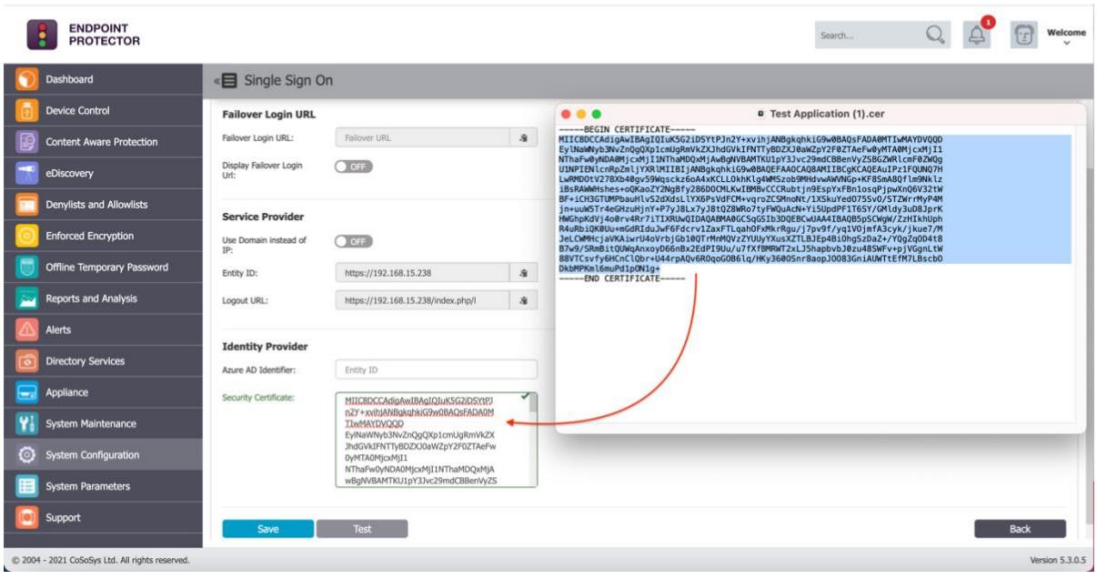


14. 3번 단계인 **SAML 서명 인증서**에서 **인증서 (Base64)**를 다운로드합니다.



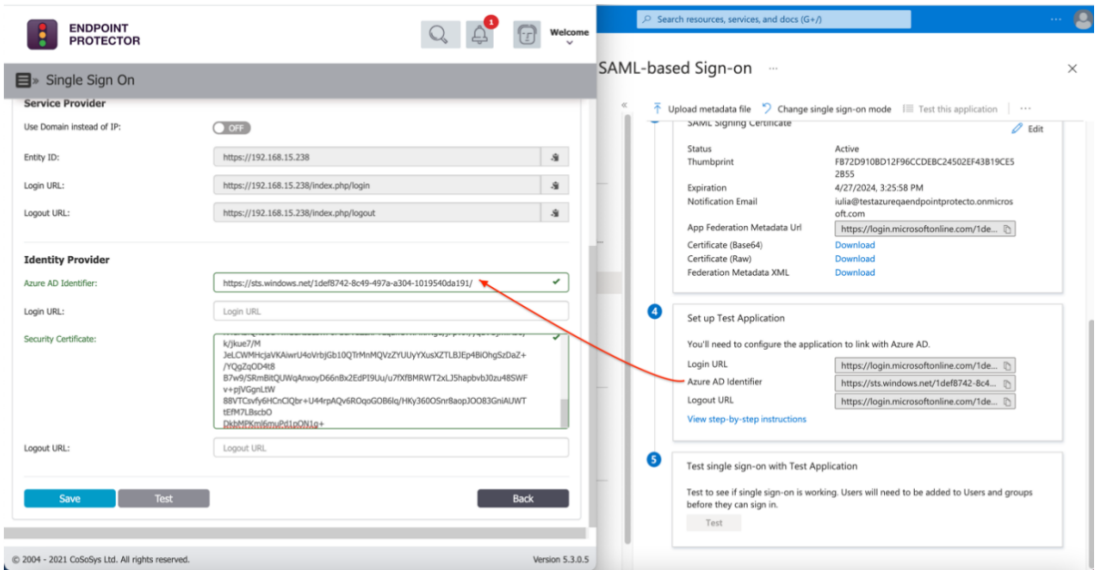
15. 텍스트 편집기에서 다운로드한 인증서를 열고 콘텐츠를 복사합니다.

16. **Endpoint Protector 서버**의 **시스템 구성** 섹션의 SSO (Single Sign On) > ID 공급자 > 보안 인증서에 콘텐츠를 붙여넣기 합니다.



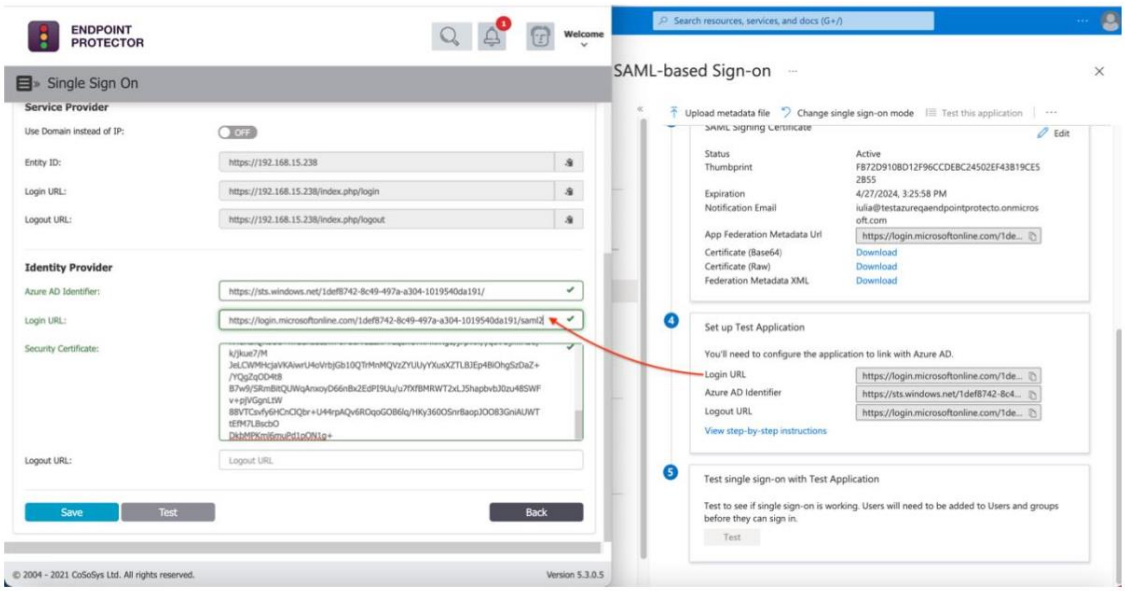
17. **Azure SAML 기반 서명** 페이지로 돌아와서 4번 단계 "당신의 애플리케이션" 설정으로 이동하고 Azure AD 식별자를 복사합니다.

18. Endpoint Protector 서버의 **시스템 구성 > SSO(Single Sign On) > ID 공급자 > Azure AD 식별자** 로 이동해서 이전에 복사한 데이터를 붙여 넣기 합니다.



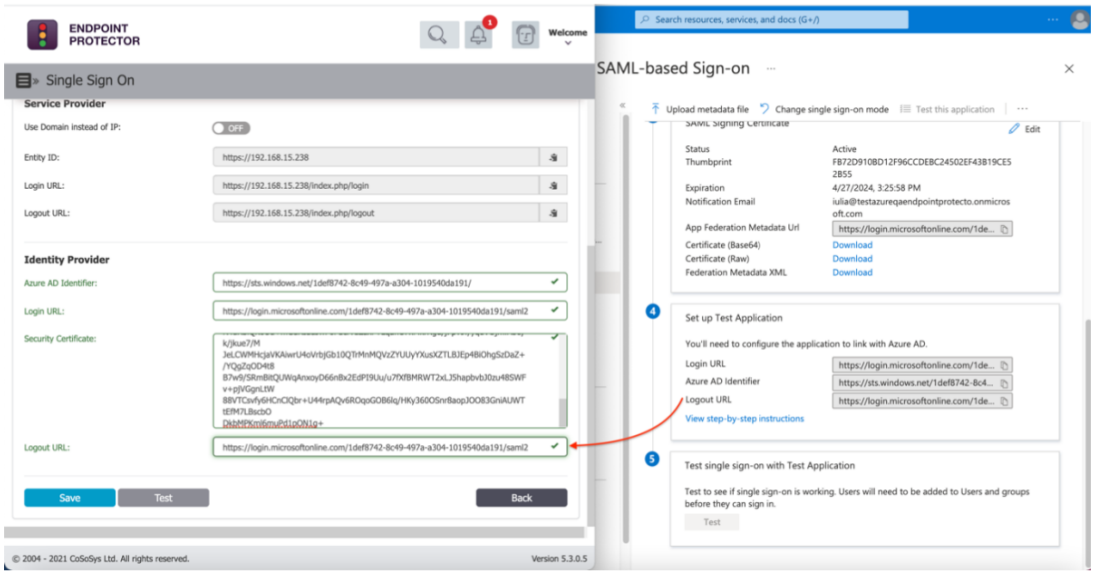
19. Azure SAML 기반 서명 페이지로 돌아와서 4번 단계인 "당신의 애플리케이션" 설정으로 가서 로그인 URL을 복사합니다.

20. Endpoint Protector 서버에서 시스템 구성 > SSO(Single Sign On) > ID 공급자 > 로그인 URL 로 이동 후 복사한 데이터를 붙여 넣기 합니다.

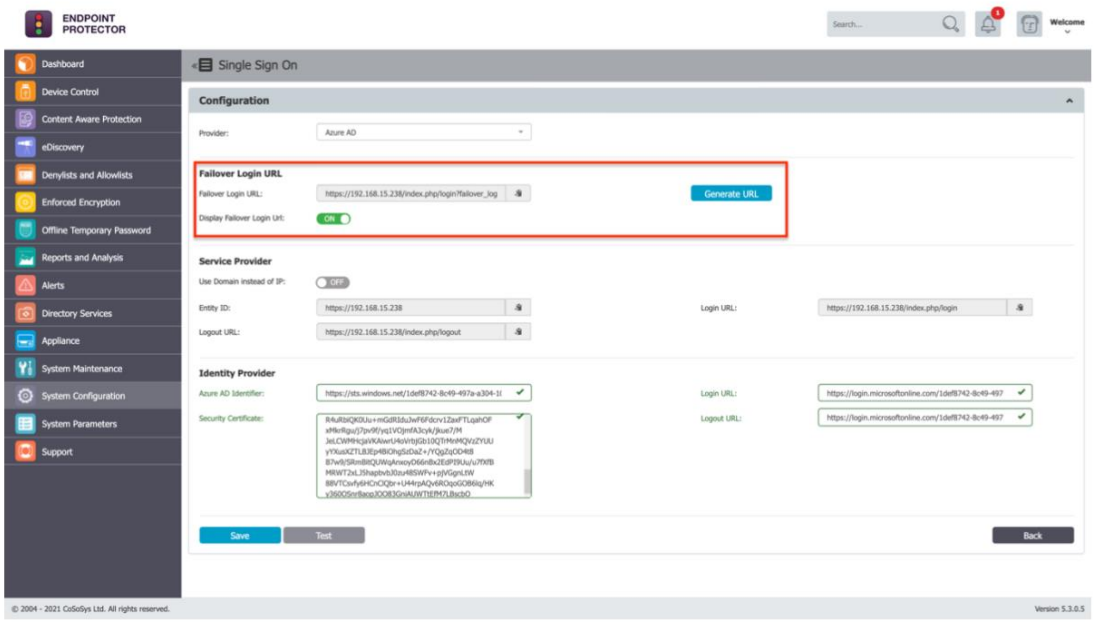


21. Azure SAML 기반 서명 페이지로 돌아와서 4번 단계인 "당신의 애플리케이션" 설정으로 이동해서 로그아웃 URL을 복사합니다.

22. Endpoint Protector 서버의 시스템 구성 > SSO(Single Sign On) > ID 공급자 > 로그아웃 URL 로 이동 후 복사한 데이터를 붙여 넣기 합니다.

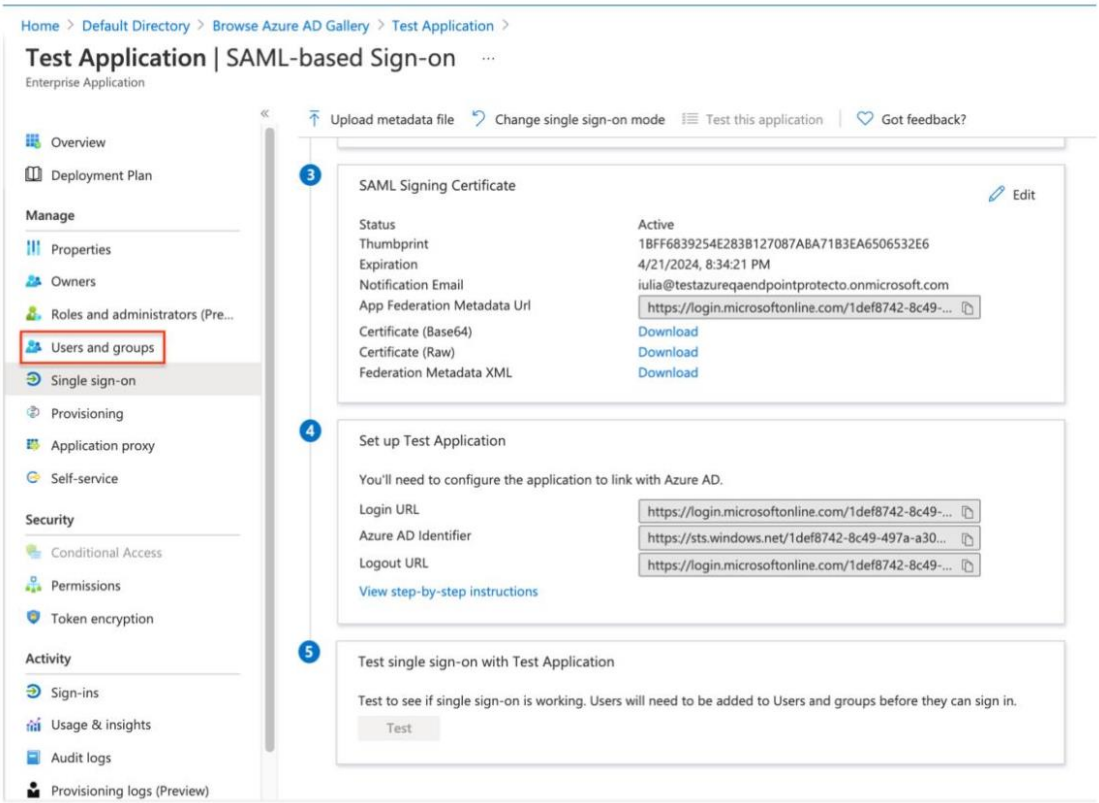


23. Endpoint Protector 서버의 시스템 구성 > SSO(Single Sign On) > 장애조치 로그인 URL 및 URL 저장 에서 장애조치 로그인 URL 만들기를 합니다.

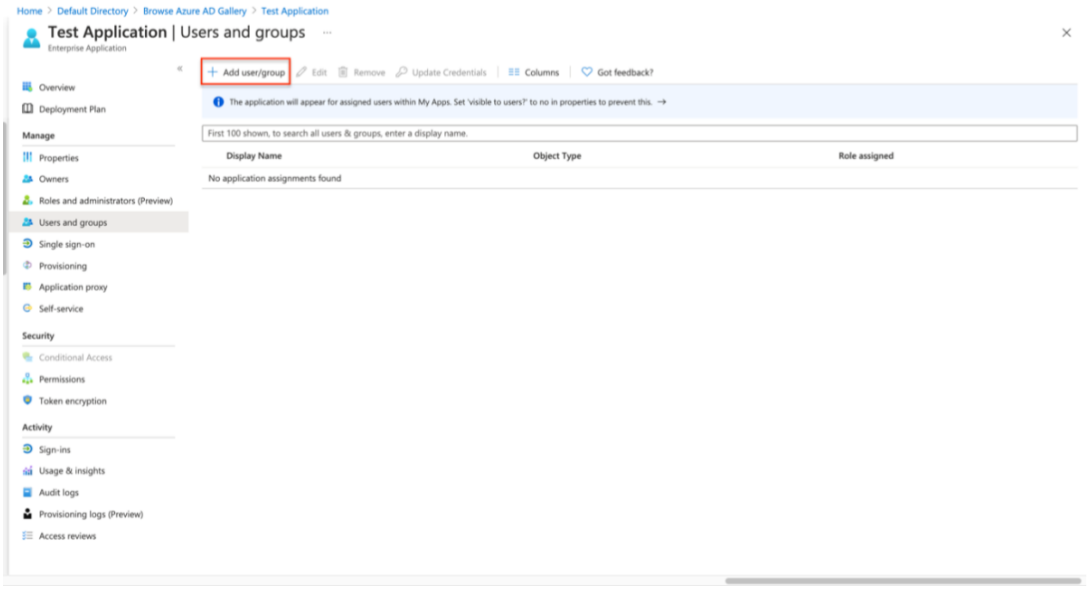


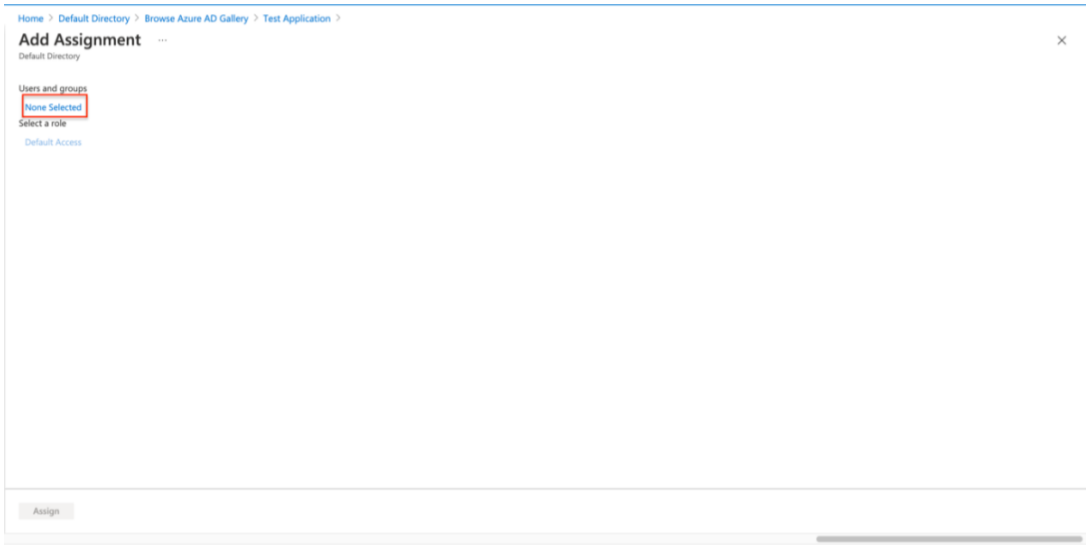
24. Endpoint Protector 서버의 SSO 페이지에서 설정을 저장합니다.

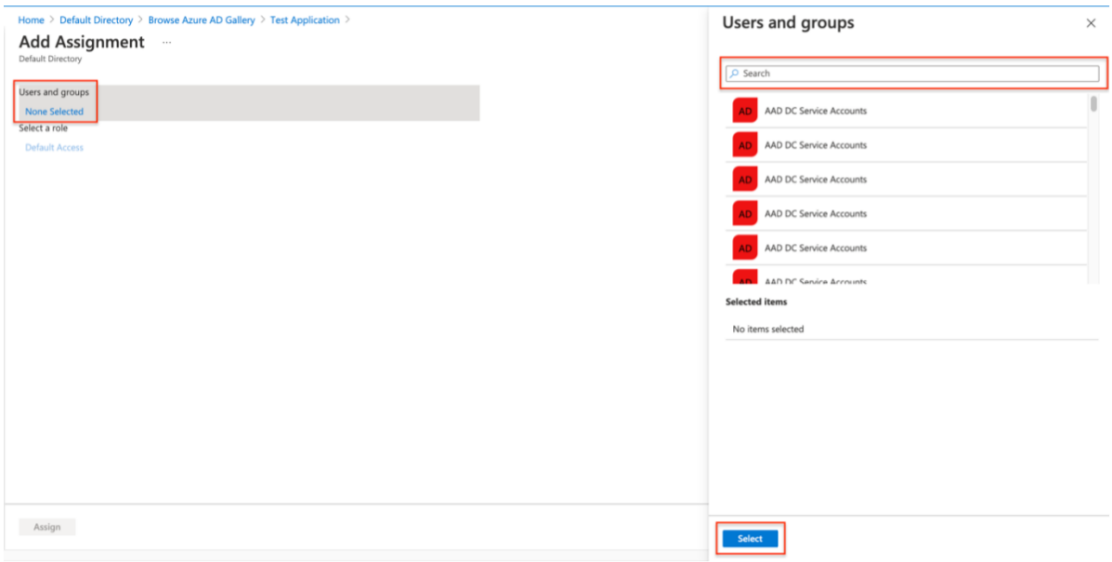
25. Azure > 왼쪽 메뉴의 사용자 및 그룹을 선택합니다.

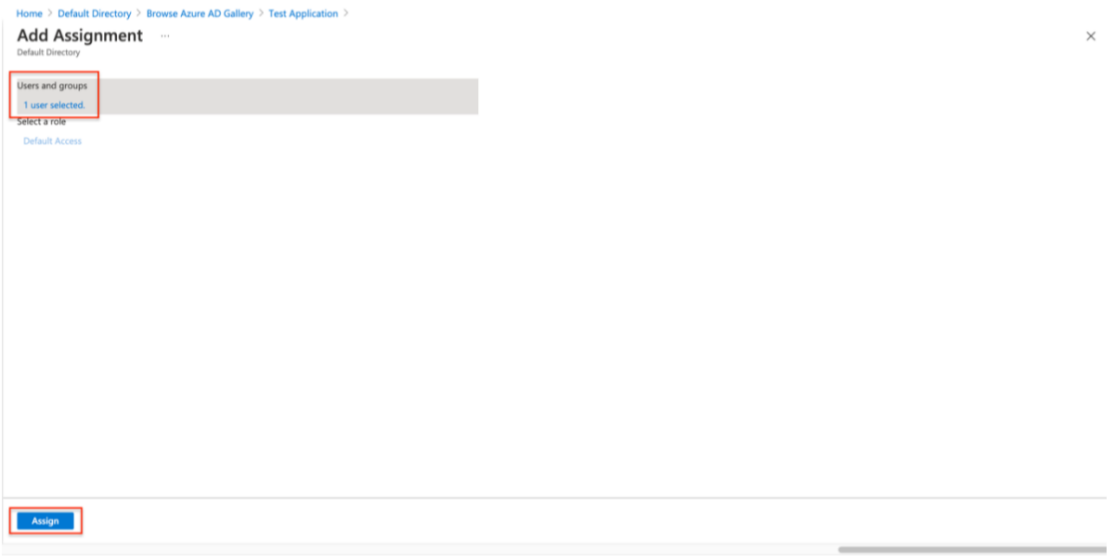


26. 사용자/그룹 추가 > 선택 없음 > 원하는 Azure 사용자 검색 > 선택 > 할당으로 이동합니다.









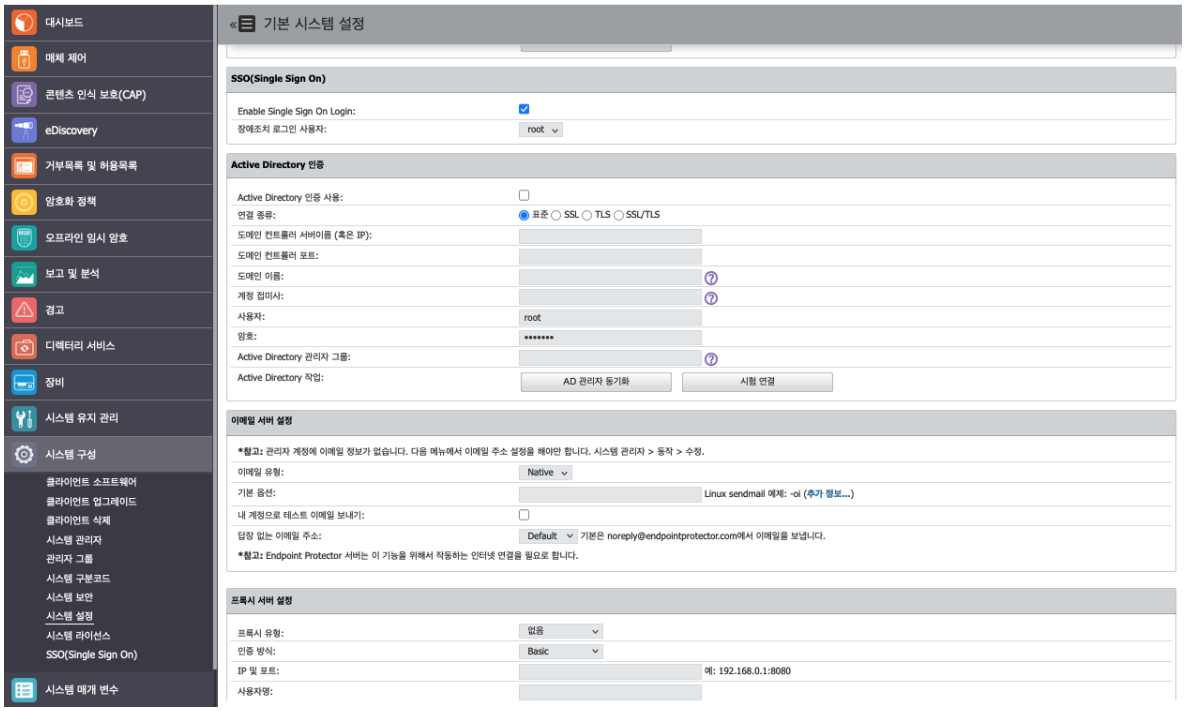
27. 사용자는 애플리케이션에 할당되고 Azure로 Endpoint Protector 로그인을 할 수 있습니다.

28. Endpoint Protector 서버에서 로그인하고 다시 접근하면 관리자는 Azure 로그인 프로세스를 위해서 http://login.microsoftonline.com으로 리 다이렉트 되어야 합니다.

OKTA로 SSO (Single Sign On) 구성

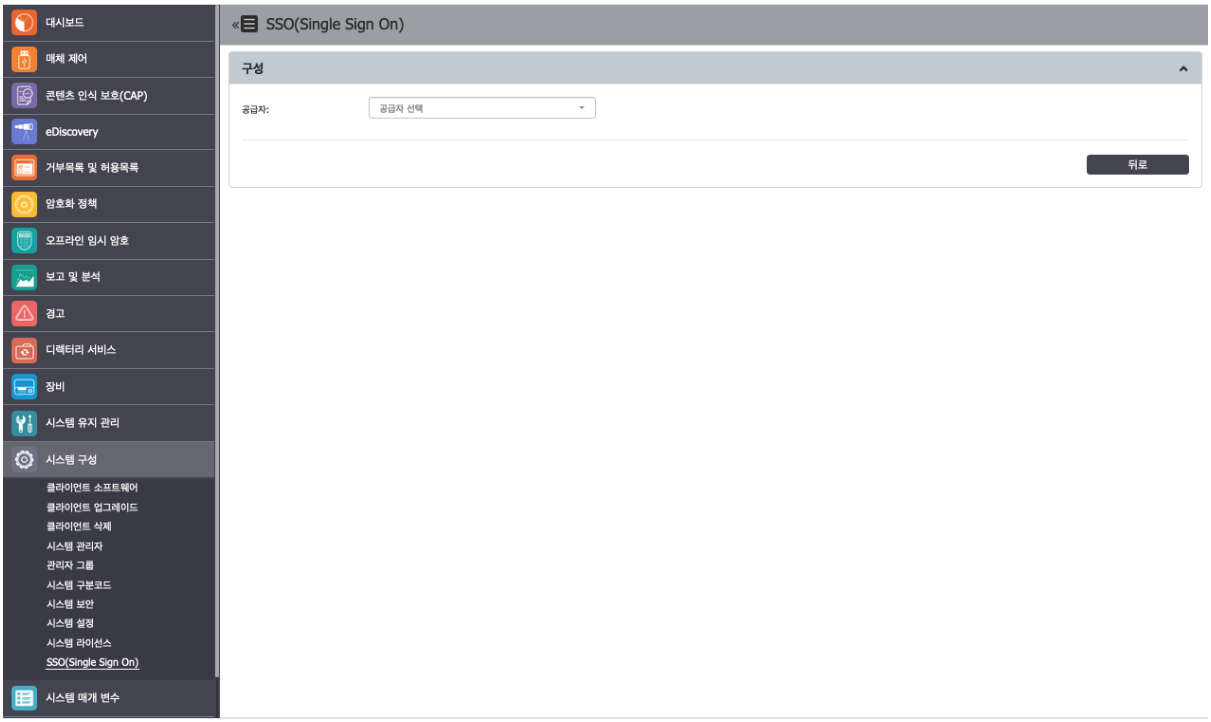
1. SSO를 사용하기 위해서 시스템 구성 > 시스템 설정 > SSO (Single Sign On)로 이동합니다.

활성화 후 드롭다운 메뉴가 표시되면 장애조치 로그인 사용자를 선택합니다. Root 사용자는 기본으로 설정되어 있습니다.

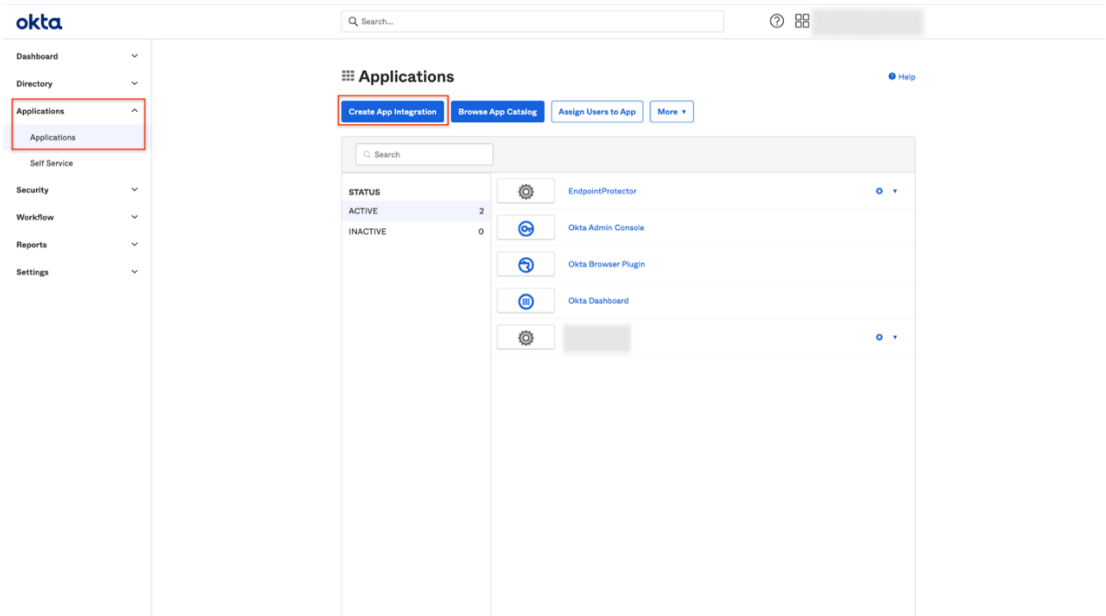


위 단계를 완료한 후에 시스템 구성 섹션에서 SSO (Single Sign On) 하위 섹션이 표시됩니다.

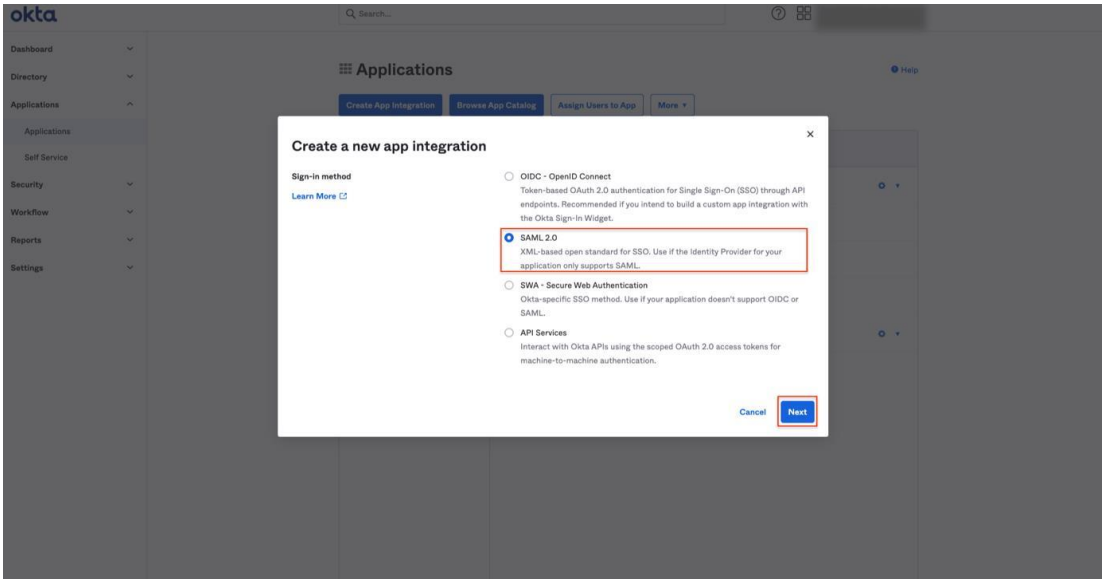
2. SSO (Single Sign On) 하위 메뉴 표시를 위해서 제공자를 선택합니다.



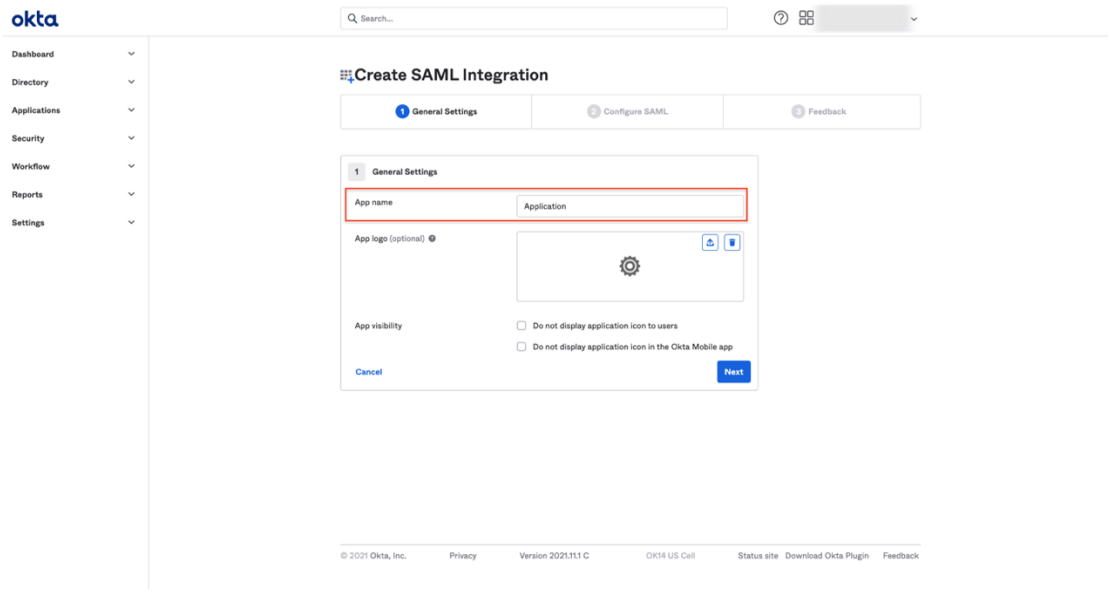
3. **yourcompany.okta.com** 에서 **Application > Create App Integration** 으로 이동합니다.



4. 아래 화면에서 **SAML 2.0** 을 선택하고 **다음** 버튼을 클릭합니다.

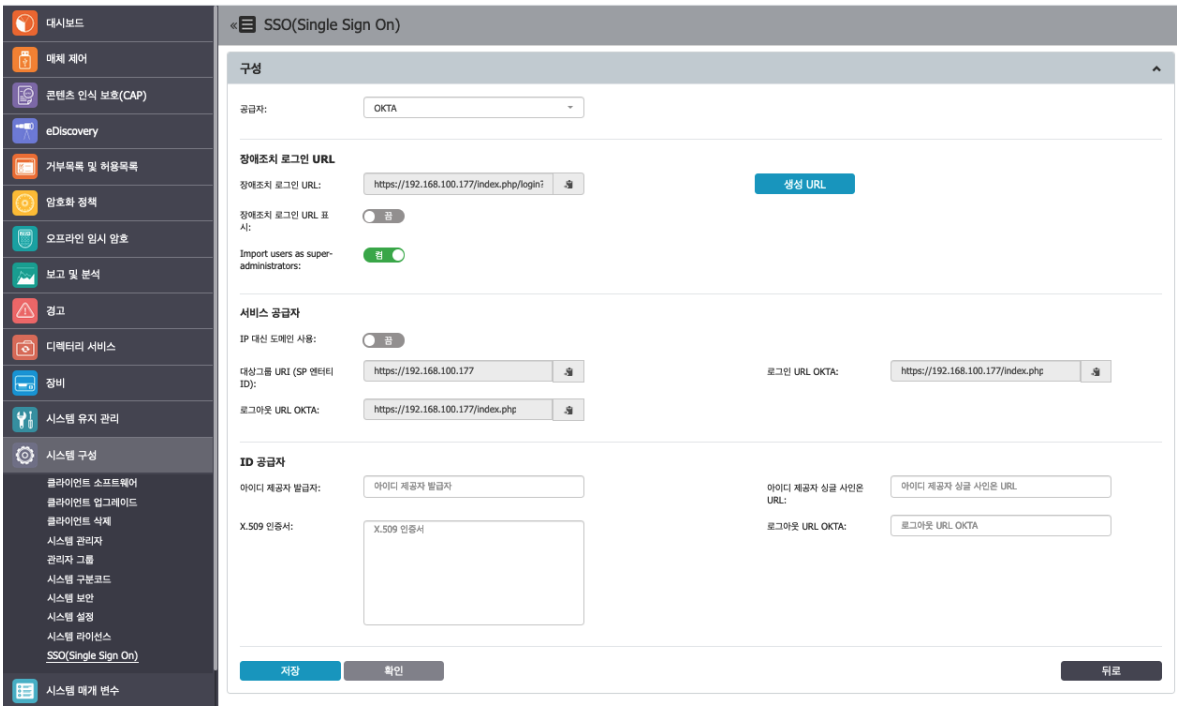


5. Application **이름**을 설정하고 **다음** 버튼을 클릭합니다.



6. **SAML 구성** 탭으로 이동합니다.

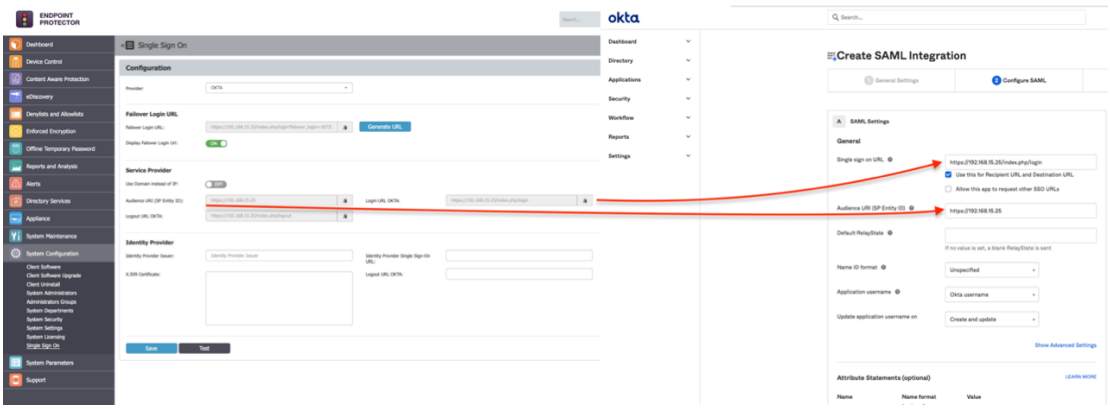
7. Endpoint Protector 서버에서 시스템 구성 > SSO (Single Sign On)로 이동합니다.



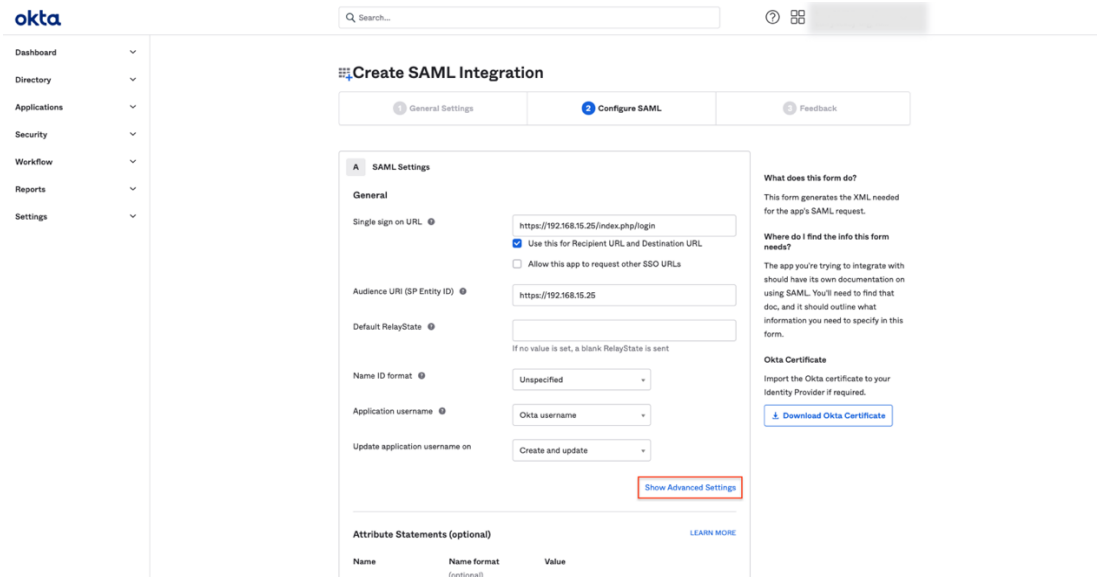
8. 정보를 복사합니다.

   - **Audience URI (SP Entity ID)**를 **OKTA 페이지의 Configure SAML**의 동일한 이름을 가진 필드에 붙여넣기

   - **Login URL OKTA**를 **OKTA 페이지의 Configure SAML**의 **Single Sign On URL** 필드에 붙여넣기

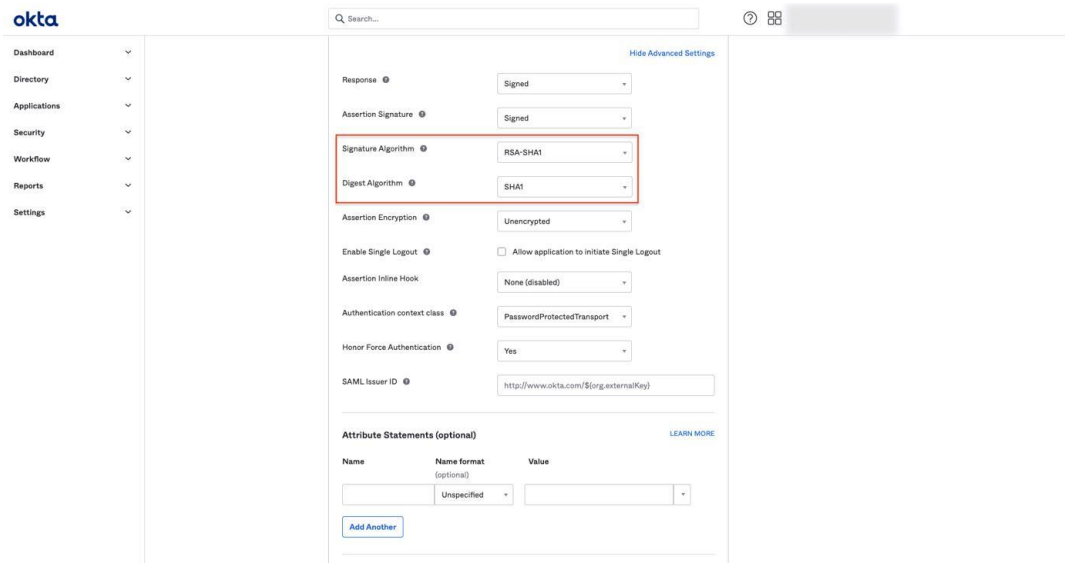


9. OKTA 페이지에서 **Show Advanced Settings**을 클릭합니다.



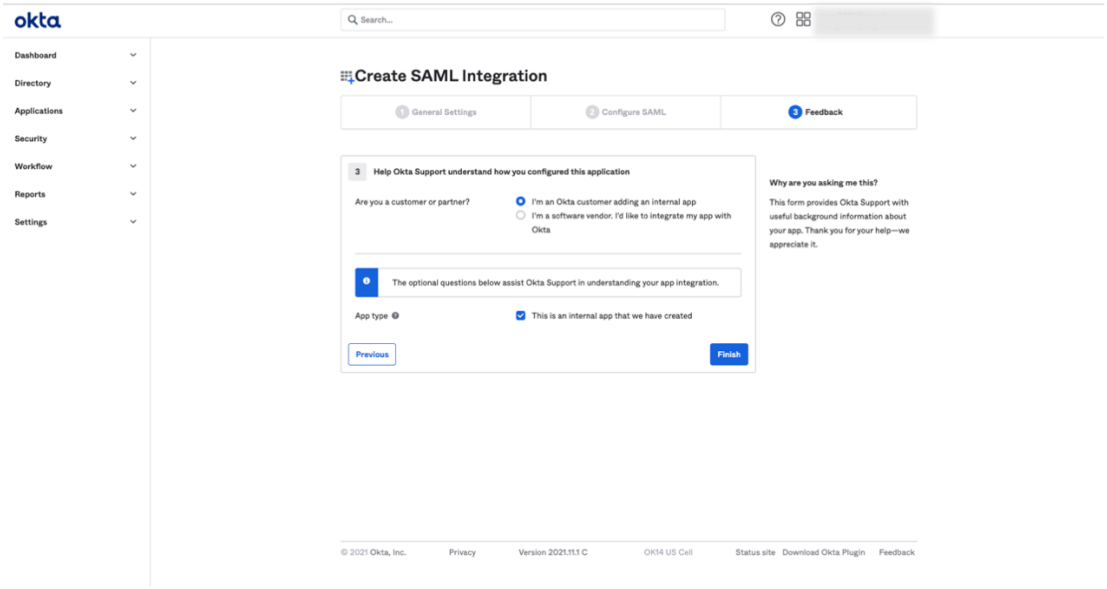
10. 아래 영역을 편집합니다.

    - **Signature Algorithm**에서 **RSA-SHA1** 선택
    - **Digest Algorithm**에서 **SHA1** 선택

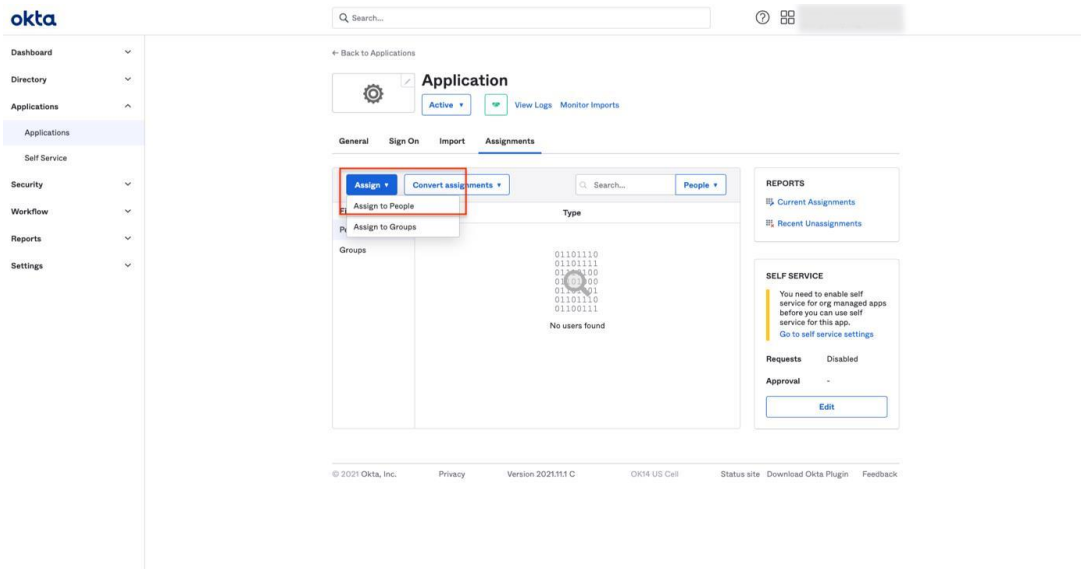


11. **Advanced Settings**을 숨기고 **다음**을 클릭합니다.

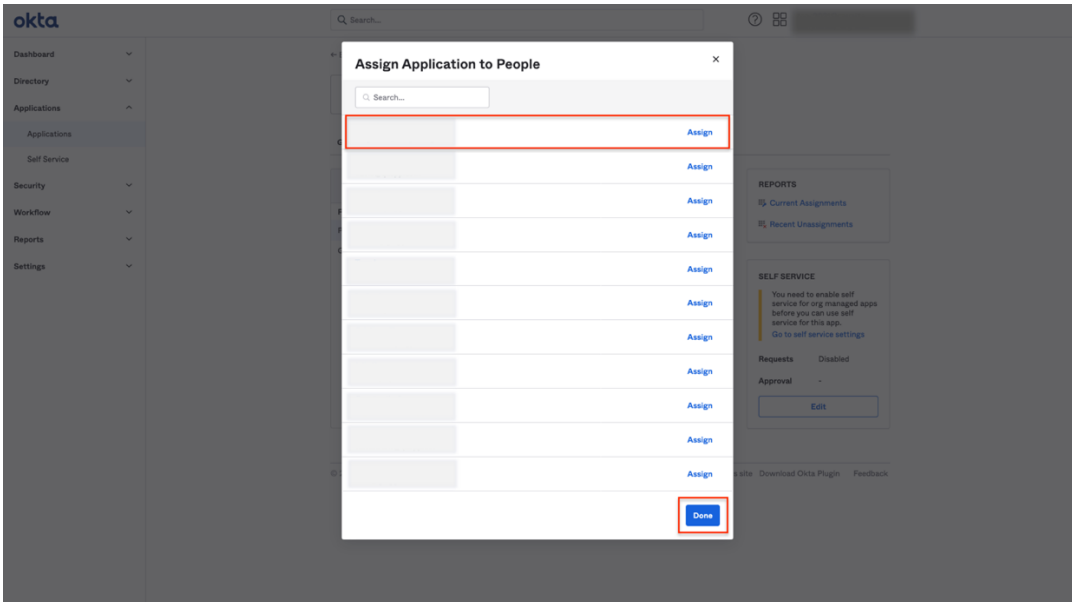
12. 3번째 단계에서 각 질문에 답을 선택하고 **마침** 버튼을 클릭합니다.



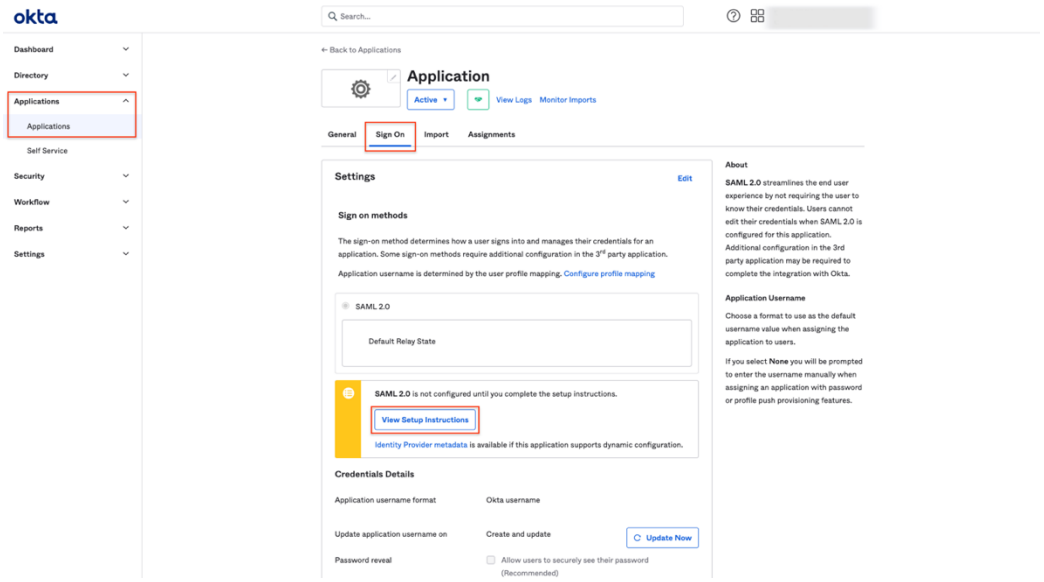
13. **Applications**으로 이동해서 Endpoint Protector 응용프로그램의 **Assignments** 로 이동 후 이 응용프로그램에 **People**을 할당합니다.



14. 필요한 계정을 할당한 후에 **완료**를 클릭합니다.



15. **Applications** 로 이동 후 만들어진 app으로 이동합니다. **Sign On** > **View Setup Instructions** 을 클릭합니다.

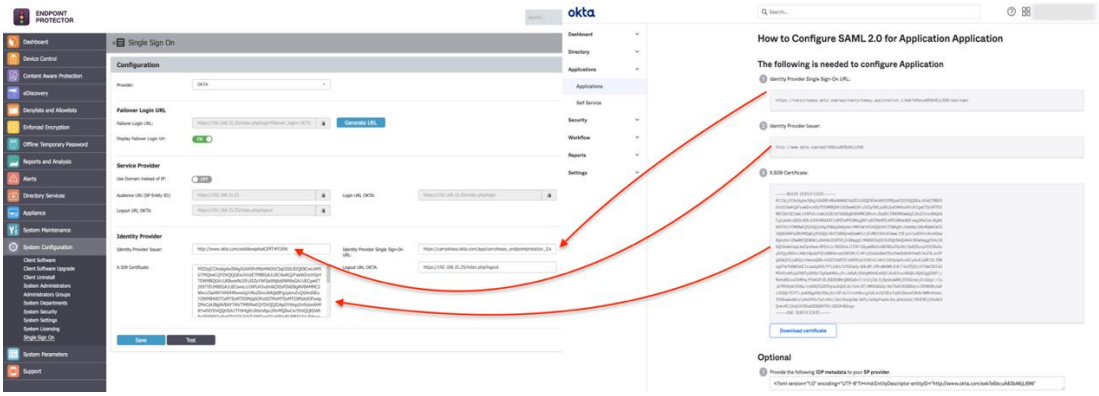


16. 새롭게 열린 섹션에서 필요한 정보를 복사한 후에 Endpoint Protector 서버에 붙여넣기 합니다.

- Endpoint Protector 서버에서 Single Sign-On URL 제공자 식별 > 시스템 구성 > Single Sign On > Single Sign-On URL 제공자 식별
- Endpoint Protector 서버에서 제공자 발행 식별 > 시스템 구성 > Single Sign On >

제공자 발행 식별

- Endpoint Protector 서버에서 X.509 인증 > 시스템 구성 > Single Sign On > X.509 인증

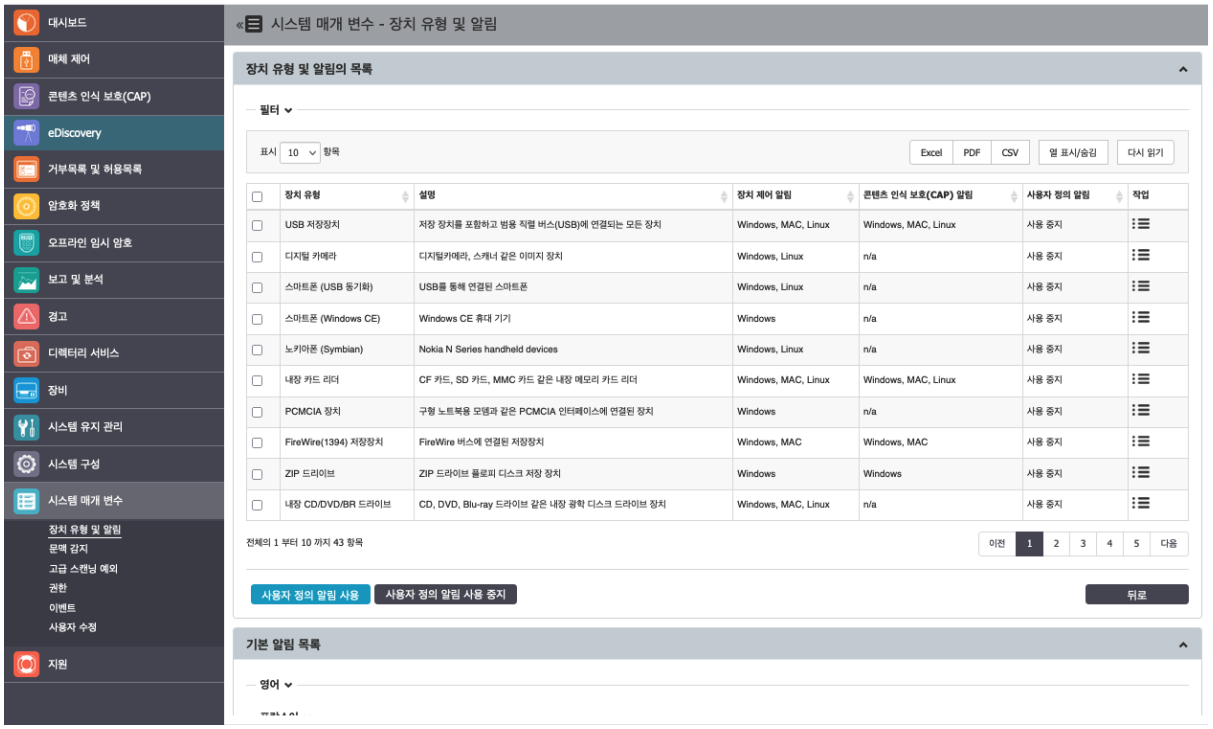


17. Endpoint Protector 서버에서 설정을 저장하고 구성 설정이 정확한지 인증 **테스트**를 클릭합니다.

17. 시스템 매개 변수

17.1. 장치 유형 및 알림

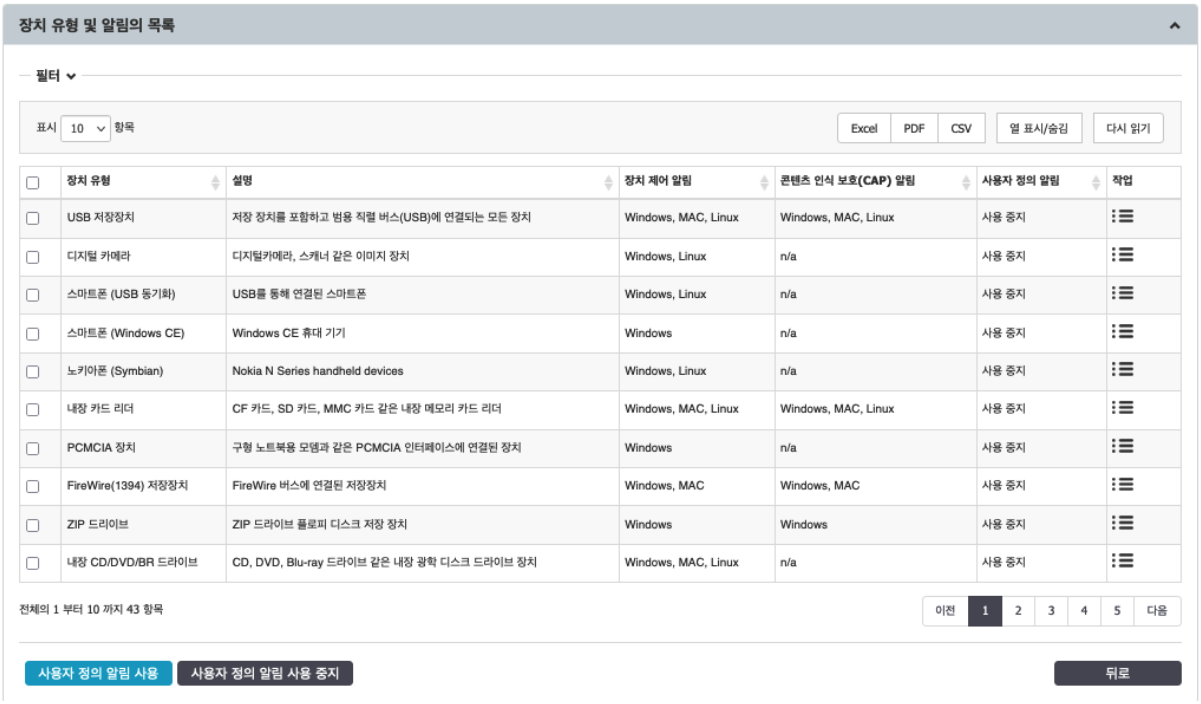
이 섹션에서 매체 유형 및 알림을 관리하고 볼 수 있습니다. 기본 알림과 번역 그리고 콘텐츠 인식 보호 정책과 매체 제어 사용자 수정에 대한 사용자 알림을 정의를 사용하고 볼 수 있습니다.



17.1.1. 장치 유형 및 알림의 목록

장치 유형 및 알림의 목록에서 각 운영 체제에서 사용할 수 있는 것 중에서 시스템에서 사용할 수 있는 매체 유형을 볼 수 있습니다. 이러한 장치는 콘텐츠 인식 보호 모듈로 검사될 수 있습니다.

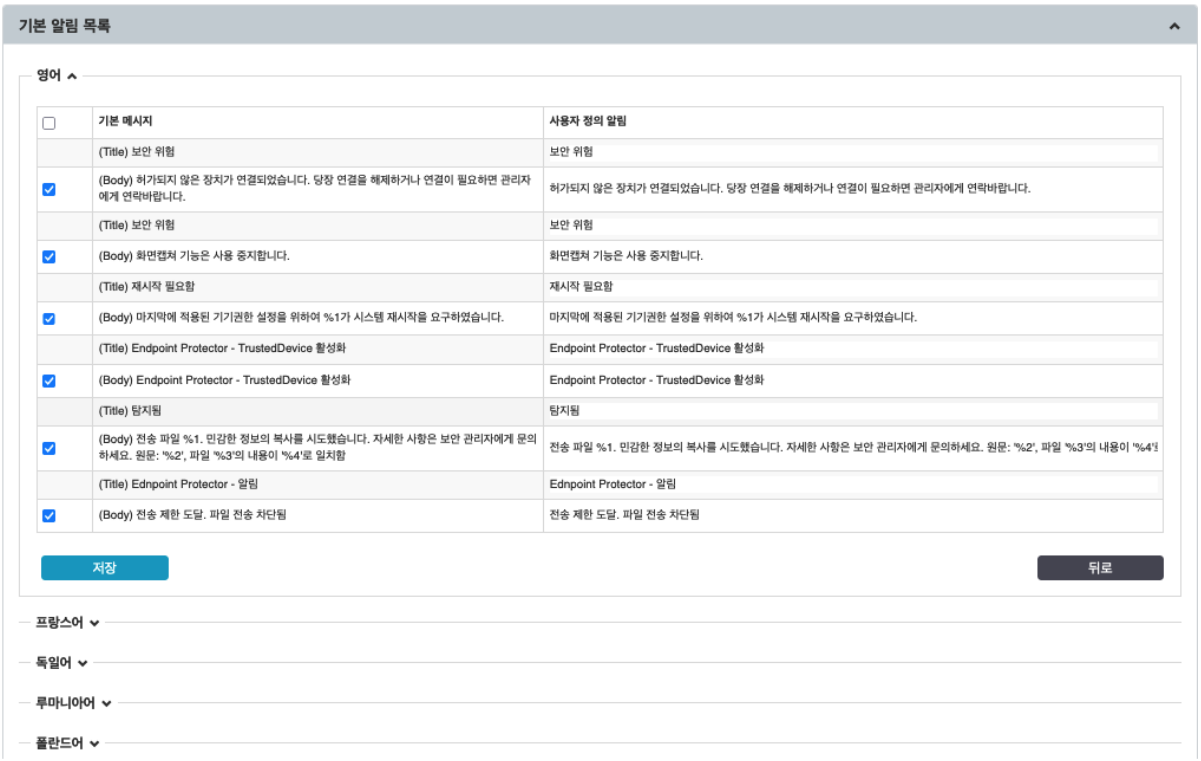
작업 컬럼에서 Endpoint Protector에 나타나는 알림 메시지를 사용 및 편집할 수 있습니다.



17.1.2. 기본 알림 목록

기본 알림 목록의 메시지를 볼 수 있고 사용 및 사용하지 않음으로 설정할 수 있습니다. 사용자 알림 번역을 편집할 수도 있습니다.

참고: 매체 제어의 **전체 설정**에서 **사용자 클라이언트 알림**을 전체적으로 사용할 수 있거나 특정 설정 섹션에서 컴퓨터 또는 그룹으로 개별 사용할 수 있습니다.



17.1.3. 사용자 콘텐츠 인식 보호(CAP) 알림

이 섹션에서 사용자 알림을 만들고 콘텐츠 인식 정책 당 이 알림을 설정할 수 있습니다. 그래서 특정 콘텐츠 인식 정책은 특정 클라이언트 알림을 가질 수 있습니다.

새로운 알림 추가를 위해 아래 단계를 따릅니다:

1. **만들기** 클릭
2. **템플릿 이름**, **이름**, **본문** 텍스트를 설정

   사용자 메시지를 만들기 위해 이 매개변수를 사용합니다:

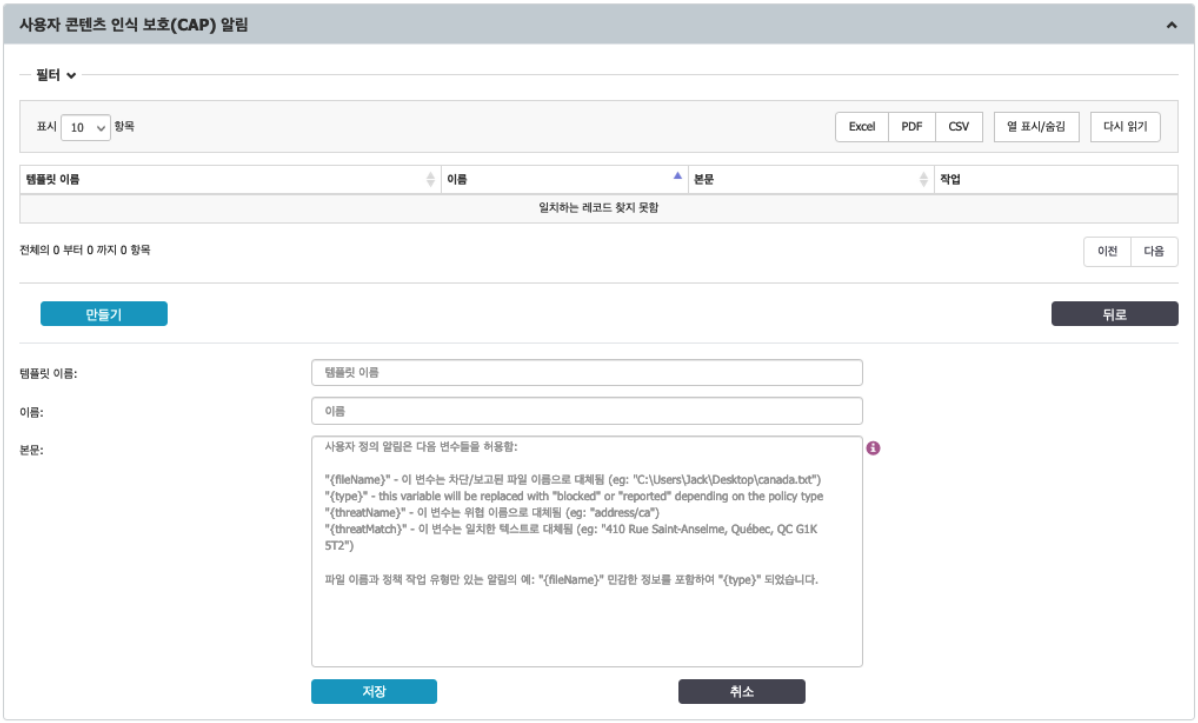
   - **{filename}** – 차단된 / 보고된 파일 이름;
   - **{type}** – 정책 유형에 따라 차단됨 또는 보고됨으로 대체;
   - **{threatName}** – 위협 이름으로 대체;

- **{threatMatch}** – 일치된 텍스트로 대체

3. **저장** 클릭

예: "{filename}"은 "{type}" 입니다. 왜냐하면 기밀 데이터를 포함하고 있습니다.

알림이 만들어지면 특정 콘텐츠 인식 정책의 **알림 템플릿** 드롭다운에서 사용자 알림을 선택할 수 있습니다.



17.1.4. 사용자 정의 매체 제어 사용자 교정 알림

참고: 이 세션은 **사용자 교정 섹션**에서 매체 제어 사용자 수정 설정을 사용했을 때만 사용 가능합니다.

이 섹션에서 매체 제어 사용자 교정에 대한 사용자 알림을 추가, 편집, 삭제할 수 있습니다.

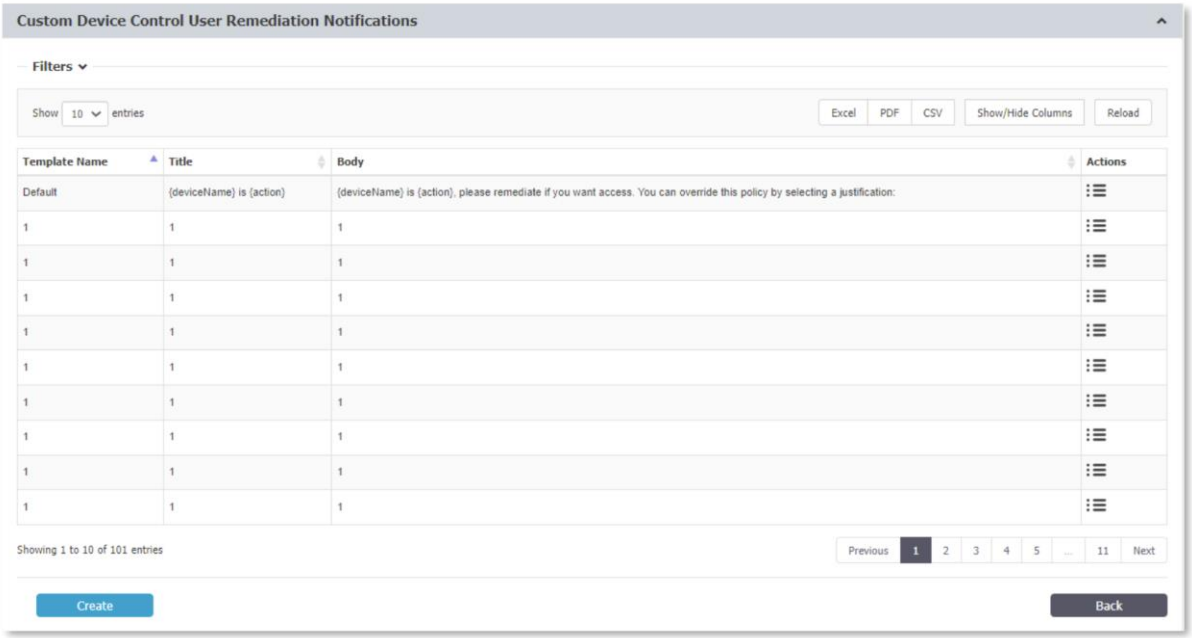
최대 100개의 사용자 알림을 추가할 수 있지만 기본 엔트리는 삭제할 수 없습니다.

새로운 사용자 알림을 추가하려면 아래 단계를 따르시기 바랍니다:

1. **만들기** 클릭
2. 사용자 메시지를 만들기 위해 매개 변수 사용
    - **{deviceName}**
    - **{action}**
3. **저장** 클릭

예: USB 저장 장치(deviceName)은 차단(action)되었습니다.

알림이 만들어지면 **전체 설정, 사용자, 컴퓨터, 그룹**에 있는 **매체 제어** 섹션에 위치한 드롭다운의 **사용자 수정 알림 템플릿**에서 사용자 알림을 선택할 수 있습니다.



17.2. 문맥 감지

이 섹션에서 관리자는 전체 시스템에 대한 문맥 감지를 관리할 수 있습니다. 사용하면 Endpoint Protector로 탐지된 기밀 정보를 콘텐츠와 문맥에 따라서 검사될 것입니다.

민감한 정보 (예: 신용카드, ID, 여권, 운전면허 등) 탐지 기능에 추가하여 문맥에 따른 추가 사항을 고려합니다. (근접한 다른 관련 키워드, 다른 관련 정규식 등).

추가적으로 탐지된 민감한 정보의 문맥을 제공하여 이 기능은 오탐을 줄여주는데 도움이 됩니다.

참고: 이 기능은 콘텐츠 인식 보호와 eDiscovery 정책에서 전체적으로 적용됩니다. 사용하면 문맥 감지는 시스템을 통해 탐지된 콘텐츠만 대체합니다. 이 기능을 사용하기 전에 규칙의 정확성과 시나리오의 관련성을 확인하시기 바랍니다.

문맥 감지 기능을 사용하면 문맥 XML에 정의된 규칙을 기반으로 전체로 적용됩니다 (또한 콘텐츠 인식 보호와 eDiscovery 정책에 연결됩니다).

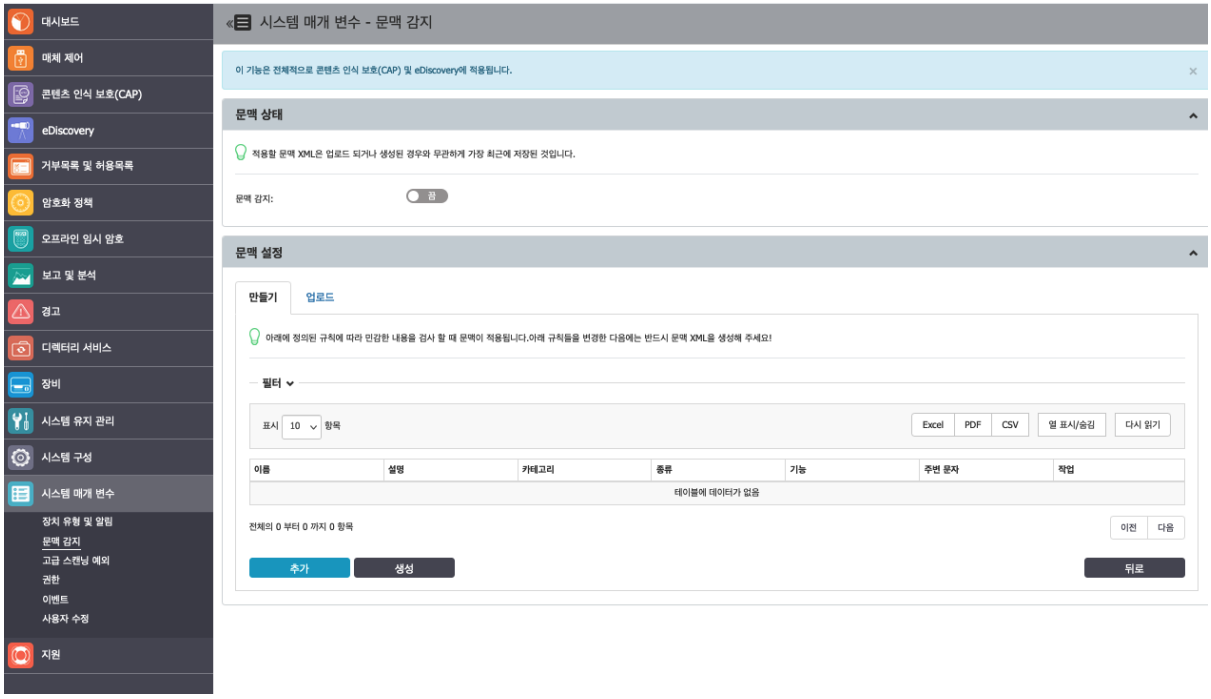
문맥 규칙을 만들기 위한 두 가지 옵션이 있습니다.

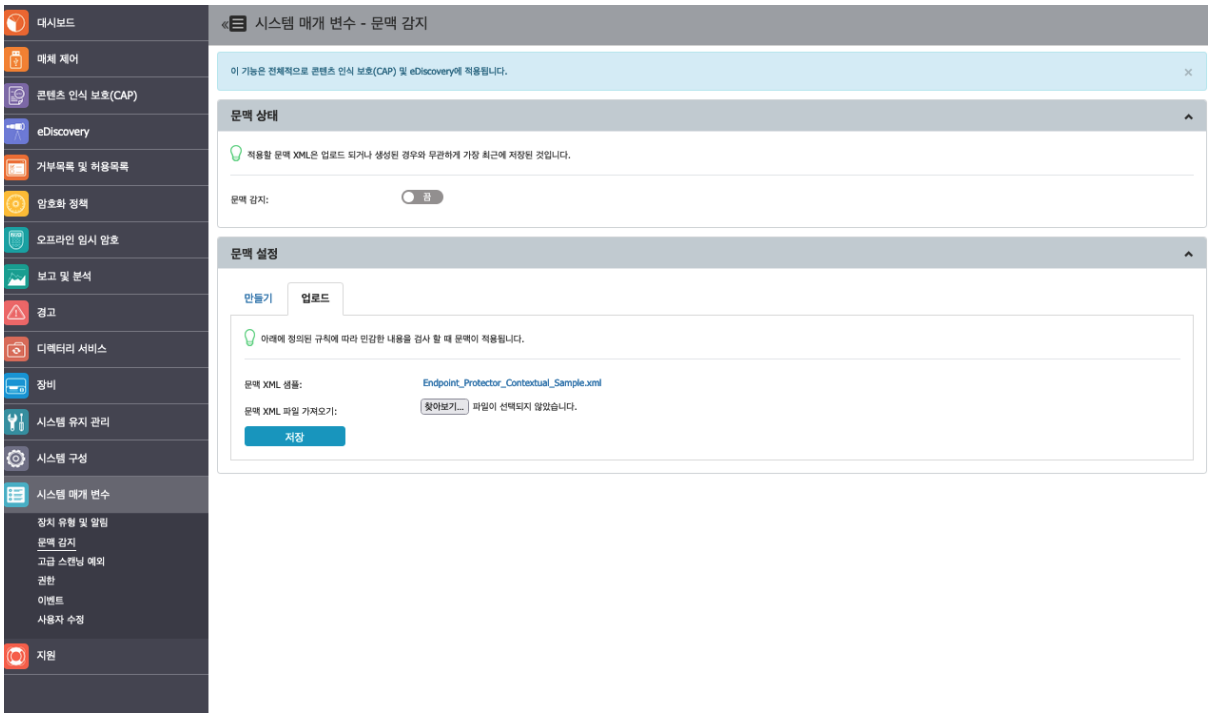
- Endpoint Protector 서버에서 직접 만들기
- 문맥 XML을 수동으로 편집하고 Endpoint Protector 서버에 업로드

중요: 전체 문맥 규칙과 정책 별 문맥 규칙 간의 충돌 해결을 위해, 하나 이상의 정책에 개별 문맥 규칙이 설정되어 있는 경우 EPP 클라이언트는 더 이상 전체 문맥 규칙의 영향을 받지 않습니다. 이는 개별 정책 구성의 우선순위를 강조하기 위해 글로벌 문맥 규칙이 더 이상 사용되지 않음을 의미합니다.

17.2.1. XML 만들기

이 방법은 가장 쉬운 방법으로 일반적인 사용에 대해 권장하고 대부분의 시나리오에서 사용할 수 있습니다.





미리 정의된 콘텐츠의 각각의 범주 (예: Credit Cards, IDs, Passports, Driving Licenses 등)에 대하여 '**추가**' 버튼을 클릭하고 아래의 목록을 선택해서 문맥 감지를 설정할 수 있습니다.

- **범주 및 유형** - 콘텐츠 인식 탐지 기능
- **주변 문자** - 문맥을 결정하는 검색 간격의 문자 수

- **관련된 사전** - PII (개인 식별 정보)에 관련된 키워드 목록
- **관련된 정규식** - 콘텐츠 인식 탐지 기능 중에 없는 추가 관련 정규식
- **관련된 파일 유형**- 관련된 파일 유형
- **관련된 파일 크기 (MB)**- 관련되 파일 크기, 메가 바이트
- **최소 일치 수** - 탐지를 할 수 있는 최소 일치 수
- **관련 없는 사전** - PII (개인 식별 정보)에 관련 없는 키워드 목록
- **관련 없는 정규식** - 콘텐츠 인식 탐지 중에 없는 추가 관련 없는 정규식
- **관련 없는 파일 유형** - 관련 없는 파일 유형
- **관련 없는 파일 크기 (MB)** - 관련 없는 파일 크기, 메가 바이트
- **최대 일치 수** - 탐지 하루 없는 최대 수 (0 사용 권장)

중요: 문맥 규칙을 만들거나 변경한 후에 Contextual XML 만들기 버튼을 누르는 것을 잊지 마시기 바랍니다.

17.2.2. XML 업로드

이 방법은 고급 관리자에게 권장합니다. 확장된 기능을 제공하지만 XML 문법에 대한 이해가 필요합니다.

고급 문맥 기능을 사용할 수 있습니다. 관리자가 수동으로 문맥 XML 파일을 편집한 후에 Endpoint Protector 서버에 업로드 합니다.

근접성, 키워드, 정규식 등 이 모든 것이 XML 문서에 정의가 되어 있어야 합니다. 신뢰 수준, 추가 함수 등의 더 복잡한 옵션을 사용할 수 있습니다. 15.2.1 XML 만들기 섹션에 기술된 것과 같이 다음의 더 복잡한 옵션이 가능합니다. **신뢰도 수준**, 주요 **함수**를 결정하는 추가적인 함수가 고려됩니다.

Contextual XML에 필요한 문법을 이해하는 가장 좋은 방법은 여러가지 예제가 포함된 Endpoint Protector에서 사용할 수 있는 샘플을 보는 것입니다.

예

<Rules>

<!-- SSN / Canada this is an example with multiple patterns -->

<Entity id="ssn/canada" patternsProximity="300" recommendedConfidence="75">

<Pattern confidenceLevel="75"> <Any minMatches="2">

<Match idRef="keywords_Canada_SSN_1" /> <Match idRef="keywords_Canada_SSN_2" />

<Match idRef="validate_date_fct" />

<Match idRef="regex_email_id" /> <!-- This is just an example -->

</Any>

<Any maxMatches="0">

<Match idRef="keywords_exclude_Canada_SSN" /> </Any>

</Pattern> </Entity>

<Function id="validate_date_fct" name="SEARCH_DATE_INTRL" /> <!-- name should be the same with the one on the client -->

<Function id="func_dlp_is_valid_ssn" name="SEARCH_SSN_Canada" /> <!-- name should be the same with the one on the client -->

Example

<Keyword id="keywords_Canada_SSN_1"> <Group matchStyle="word">

<Term>sin</Term>

<Term>social insurance</Term>

<Term>numero d'assurance sociale</Term> <Term>sins</Term>

<Term>ssn</Term>

<Term>ssns</Term>

<Term>social security</Term> <Term>numero d'assurance sociala</Term> <Term>national identification number</Term>

<Term>national id</Term> <Term>sin#</Term>

</Group> </Keyword>

<Keyword id="keywords_Canada_SSN_2"> <Group matchStyle="word">

<Term>driver's license</Term> <Term>drivers license</Term> <Term>driver's licence</Term> <Term>drivers licence</Term> <Term>DOB</Term> <Term>Birthdate</Term>

</Group> </Keyword>

<Keyword id="keywords_exclude_Canada_SSN"> <Group matchStyle="word">

<Term>random word</Term> </Group>

</Keyword>

<Regex id="regex_email_id">[-0-9a-zA-Z.+_]+@[-0-9a-zA-Z.+_]+₩.[a-zA-Z]{2,4}</Regex>

</Rules>

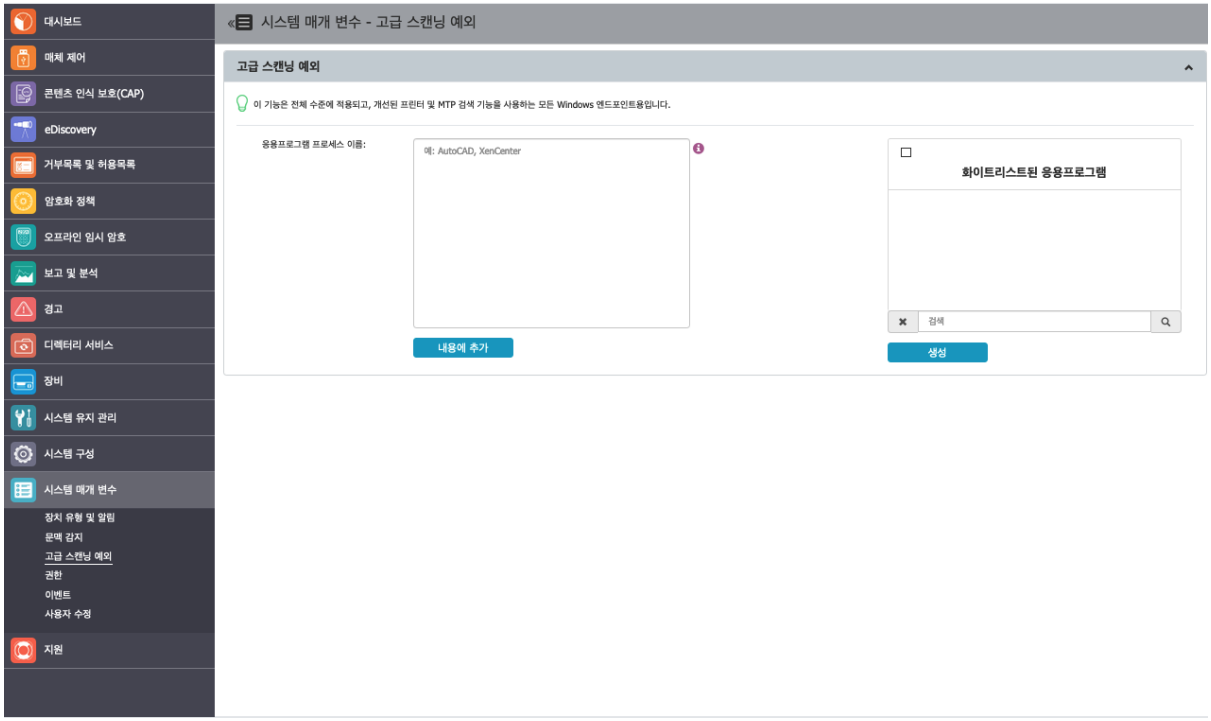
</RulePackage>

17.3. 고급 스캐닝 예외

Windows 환경은 고정적이고 보안 업데이트와 설치된 응용프로그램은 계속해서 발전합니다. Endpoint Protector 클라이언트 간섭을 피하기 위해서 응용프로그램과 프로세스의 허용목록가 가능합니다.

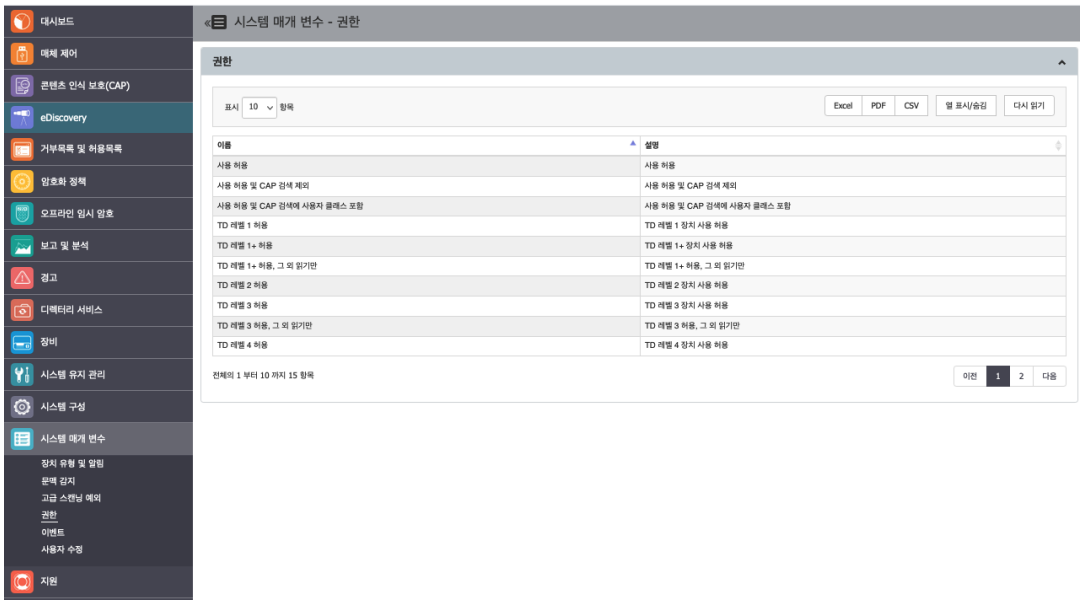
엔드포인트 컴퓨터에 향상된 프린터 및 MTP 검색 기능이 활성화 되어 있을 때 고급 스캐닝 예외 기능은 이러한 검색에서 원하는 응용프로그램을 예외처리 합니다.

참고: 이 기능은 글로벌 레벨로 '향상된 프린터 및 MTP 검색 기능' 이 활성화된 모든 Windows 엔드포인트 컴퓨터에 적용됩니다.



17.4. 권한

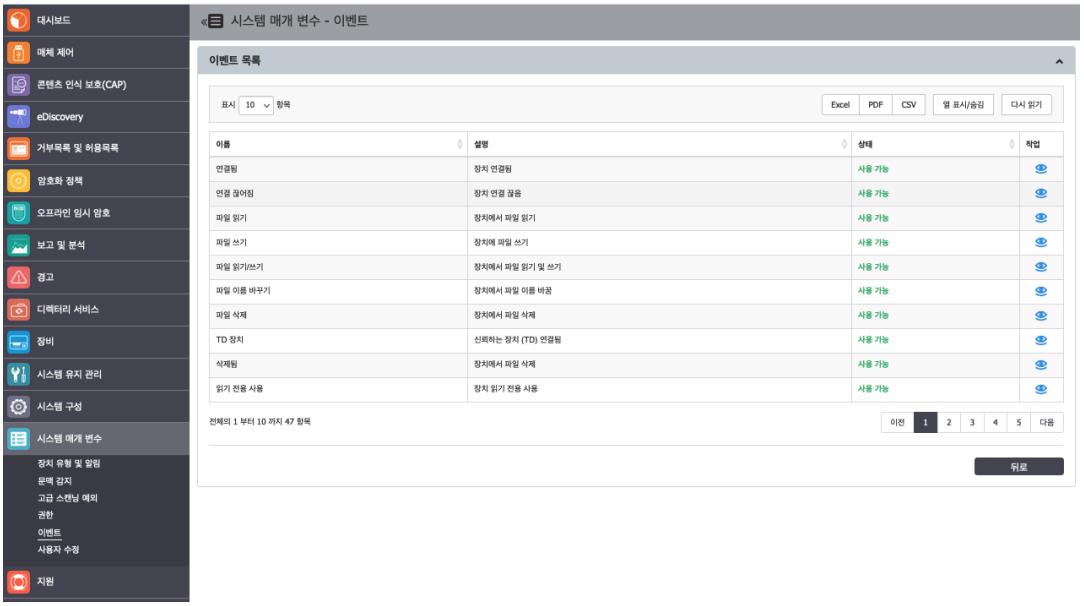
이 섹션은 장치에 적용할 수 있는 모든 접근 권한 목록을 보여줍니다.



17.5. 이벤트

이 섹션은 Endpoint Protector 로그의 이벤트 목록을 보여줍니다.

작업 컬럼은 이벤트 이름과 설명을 편집 또는 특정 이벤트 로그를 사용하지 못하게 하는 옵션을 제공합니다.



17.5.1. 이벤트 유형 및 설명

이 하위 섹션에 포괄적인 이벤트 목록이 표시되며 관리자는 데이터 보호 정책을 효과적으로 관리하고 모니터링할 수 있습니다. 또한 EasyLock 배포, 프린터 활동, 사용자 정보 업데이트, 전송 제한, 외부 저장소 업로드, 콘텐츠 교정, 강제 제거 시도, 장치 교정 세션, 인증서 관리, 계획되지 않은 클라이언트 종료, 아티팩트 수신 및 DPI 우회 트래픽과 관련된 이벤트 및 보다 구체적인 이벤트도 있습니다. 이러한 이벤트는 다양한 시스템 활동에 대한 세분화된 인사이트를 제공하여 조직이 강력한 보안 및 규정 준수 조치를 유지할 수 있도록 합니다. 모든 이벤트와 그 설명에 대한 자세한 내용은 아래 표를 참조 부탁드립니다.

이벤트 유형 및 설명	
이벤트 이름	**설명**

연결	장치 연결됨
연결 끊어짐	장치 연결 끊음
파일 읽기	장치에서 파일 일기
파일 쓰기	장치에 파일 쓰기
파일 읽기/쓰기	장치체서 파일 읽기 및 쓰기
파일 이름 바꾸기	장치에서 파일 이름 바꿈
파일 삭제	장치에서 파일 삭제
TD 장치	신뢰하는 장치 (TD) 연결됨
삭제됨	장치에서 파일 삭제
읽기 전용 사용	장치 읽기 전용 사용
TD 레벨 1 사용	TD 레벨 연결 시 장치 사용 (예: EasyLock 설치된 USB 저장 장치는 자동으로 런칭됨)
TD 레벨 2 사용	TD 레벨 2 장치 사용
TD 레벨 3 사용	TD 레벨 3 장치 사용
TD 레벨 4 사용	TD 레벨 4 장치 사용
AD 동기화	AD 동기화
차단됨	장치 또는 포트 차단됨
차단 해제됨	장치 또는 포트 차단 안 됨
오프라인 임시 암호 사용됨	오프라인 임시 암호 사용됨
사용자 로그인	사용자 로그인
파일 암호화	EasyLock을 사용 파일 암호화
파일 복호화	EasyLock을 사용 파일 복호화
파일 암호화(오프라인)	Endpoint Protector 서버와 통신하지 않을 때 EasyLock으로 암호화된 파일

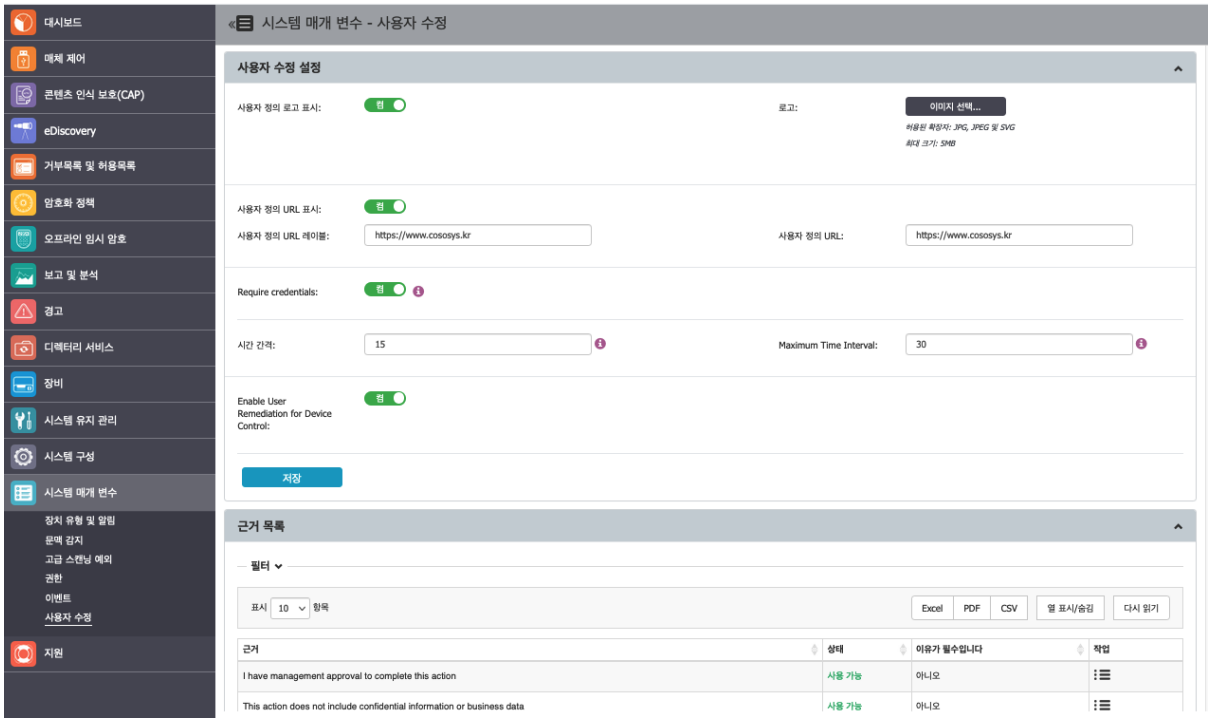
파일 복호화(오프라인)	Endpoint Protector 서버와 통신하지 않을 때 EasyLock으로 복호화된 파일
콘텐츠 위협 탐지됨	콘텐츠 인식 보호 – 위협 탐지됨
콘텐츠 위협 차단됨	콘텐츠 인식 보호 – 위협 차단됨
파일 복사	파일이 이동식 매체로 또는 이동식 매체로부터 복사 되었습니다.
콘텐츠 위협 발견됨	eDiscovery – 위협 발견됨
eDiscovery 클라이언트 액션	eDiscovery – 작업 수신 성공
사용자 로그아웃	사용자 로그아웃
클라이언트 무결성 OK	Endpoint Protector 클라이언트 무결성 OK
클라이언트 무결성 실패	Endpoint Protector 클라이언트 무결성 깨짐
정책 수령	Endpoint Protector 클라이언트 정책 수신 성공
삭제 시도	Endpoint Protector 클라이언트 삭제 시도
EasyLock – 성공적으로 배포됨	EasyLock – 성공적으로 배포됨
EasyLock – 배포 실패함	EasyLock – 배포 실패함
파일 인쇄됨	파일을 프린터에 성공적으로 보냄
사용자 정보 업데이트됨	사용자 정보 업데이트 성공
전송 제한 도달	전송 제한 도달
외부 저장소 업로드	파일 사본을 레포지토리에 업로드 성공
외부 저장소 업로드 실패	파일 사본을 레포지토리에 업로드 실패
콘텐츠 교정 세센 활성화	콘텐츠 인식 보호 (CAP) – 위협 교정
사용자가 콘텐츠 교정 요청을 취소됨	콘텐츠 인식 보호 (CAP) – 사용자가 사용자 교정 대화 상자 닫음
강제 삭제 시도	Endpoint Protector 클라이언트 강제로 삭제 시도

사용자가 장치 교정 요청을 취소함	매체 제어 – 사용자가 사용자 교정 대화 상자 닫음
장치 교정 세션 취소됨	사용자 교정 장치 일시적 잠금 해제 취소됨
장치 교정 세션 활성화	사용자 교정 장치 일시적 잠금 해제
장치 교정 세션 종료됨	사용자 교정 장치 일시적 잠금 해제 종료됨
키체인/저장소에 인증서가 추가됨	키체인/저장소에 인증서가 성공적으로 추가됨
계획하지 않은 클라이언트 중단	계획하지 않은 클라이언트 중단
받은 아티팩트	받은 아티팩드
DPI 우회한 트래픽	DPI 우회한 트래픽

17.6. 사용자 교정

사용자 수정은 최종 사용자가 정책 위반 또는 제한된 매체 접근을 자체적으로 수정 및 타당한 근거를 적용할 수 있도록 허용하는 기능입니다.

참고: 이 기능은 프리미엄 라이선스에서만 사용할 수 있습니다.



17.6.1. 사용자 교정 설정

이 섹션에서 사용자 교정 알림을 사용자 정의하고 설정 관리, 매체 제어의 사용자 교정을 사용할 수 있습니다.

- **사용자 정의 로고 보이기** - 이 설정에서 관리자는 팝업 알림에 나오는 원하는 로고를 업로드 할 수 있습니다.
- **사용자 정의 URL 보이기** - 최종 사용자의 특정 웹 페이지 URL을 이 하위 섹션에서 설정할 수 있습니다.

  참고: 다음 URL 포맷이 적용 가능합니다.

  - http://endpointprotector.com
  - https://endpointprotector.com
  - http://www.endpointprotector.com
  - https://www.endpointprotector.com

- **계정 요청** – 로컬 계정 또는 Active Directory 계정 사용을 위해 최종 사용자에게 요청합니다.

  참고: 로그인을 위해 다음 계정 포맷이 허용됩니다.

  - 로컬 사용자 – computer_name₩username (John-PC₩John)
  - LDAP/AD 사용자
  - domain_name₩username (epp.com₩John)
  - ip₩username (192.168.14.140₩John)

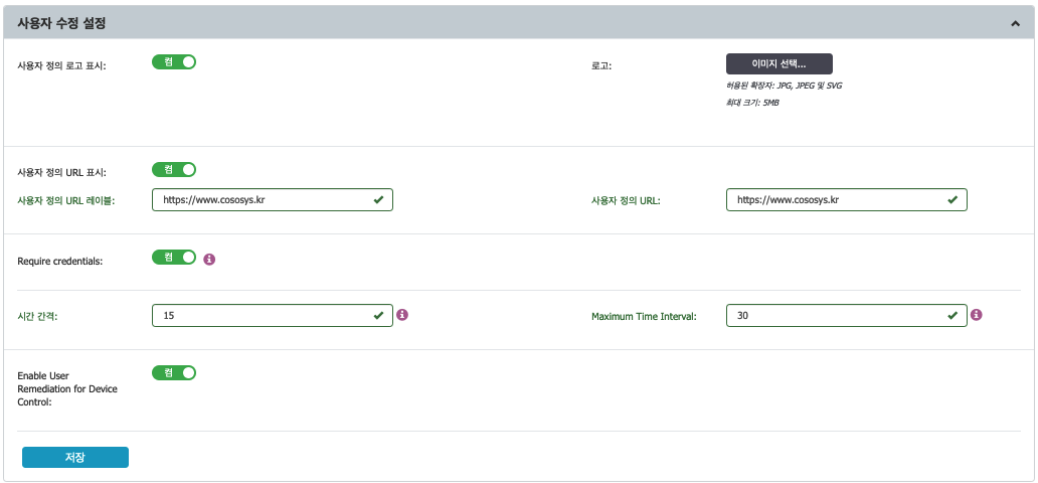
- **시간 간격** - 최종 사용자가 차단 및 수정된 위협 또는 제한된 장치 접근을 수정할 수 있는 시간 간격을 설정할 수 있습니다.

- **최대 시간 간격** – 최종 사용자가 차단 및 교정된 위협 또는 제한된 장치 접근을 수정할 수 있는 최대 시간 간격을 설정할 수 있습니다.

  참고: 입력할 수 있는 최댄 시간 간격은 1440분 (24시간) 입니다.

- **매체 제어의 사용자 교정 사용** – 매체 제어 모듈에 대한 사용자 교정 기능 사용을 설정할 수 있습니다.

  중요: 매체 제어의 사용자 교정 사용 설정은 기본으로 사용하지 않음으로 되어 있습니다. 이 기능을 사용하면 사용자 교정에 관련된 모든 설정은 콘텐츠 인식 보호와 매체 제어 모듈에 적용됩니다.

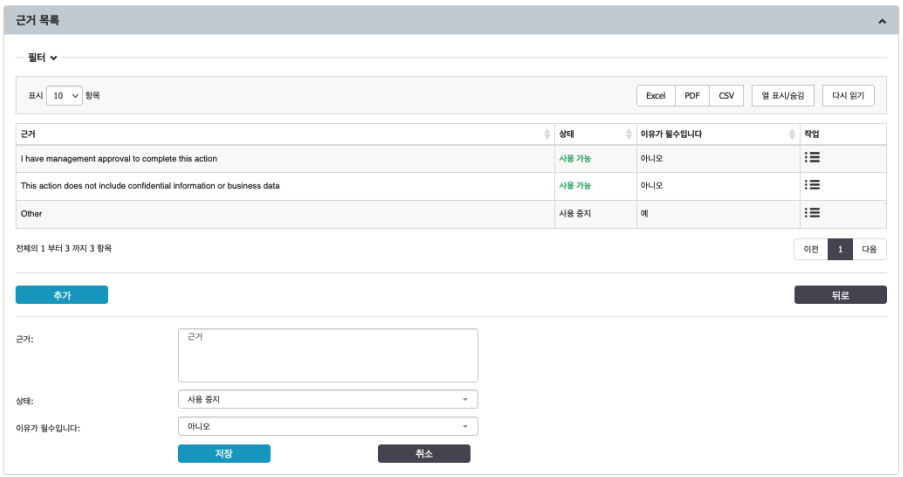


17.6.2. 근거 목록

이 섹션에서 근거를 확인, 추가, 편집, 내보내기, 삭제할 수 있습니다. 근거는 최종 사용자가 위협 또는 장치 수정을 정의하기 위해 선택한 이유입니다.

새로운 근거를 추가하기 위해서는 **추가**를 클릭하고 필드를 입력하고 **저장**을 클릭합니다. 최대 10 개의 근거를 추가할 수 있습니다. 기본값으로 여러 근거가 이미 추가되어 있습니다. 그러나 사용하려면 적어도 하나는 선택해야 합니다.

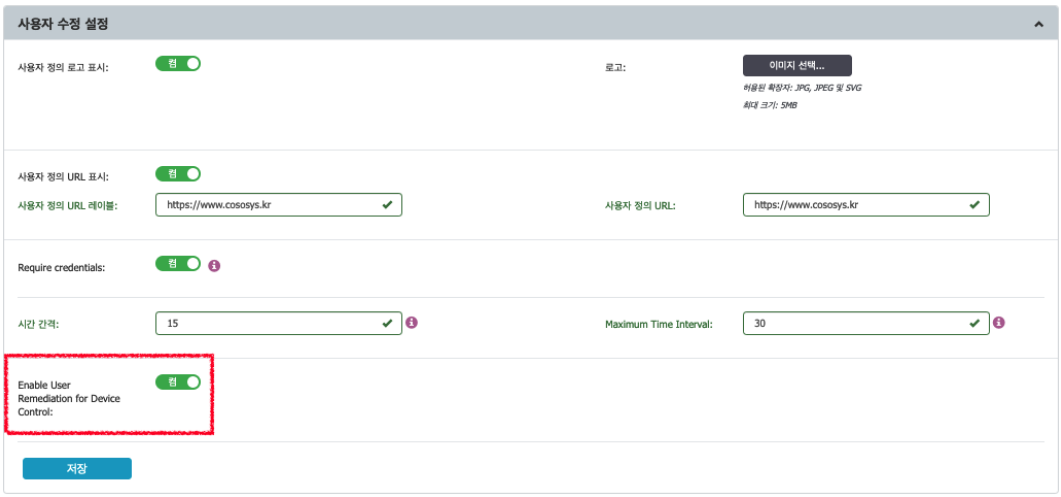
최종 사용자가 사용자 수정 팝업 알림을 보기를 강제화하고 사용하기 위해서 매체 제어의 전체 설정 Endpoint Protector 클라이언트 설정에서 옵션을 관리합니다.



17.6.3. 사용자 교정 사용하기

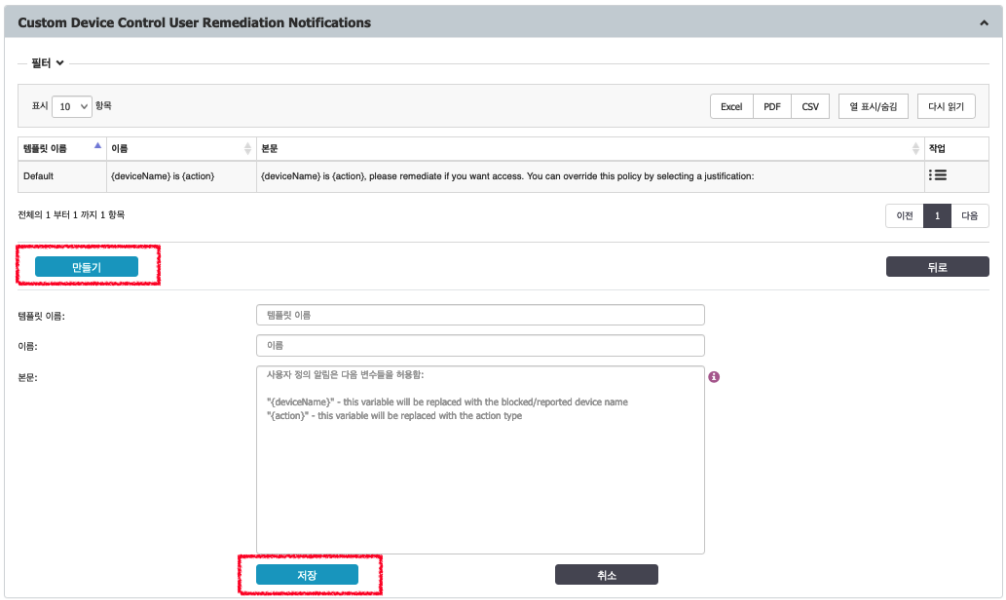
매체 제어의 사용자 교정을 사용하려면 아래의 단계를 따르시기 바랍니다:

1. 사용자 수정 설정에서 **매체 제어의 사용자 교정 사용**을 사용합니다.

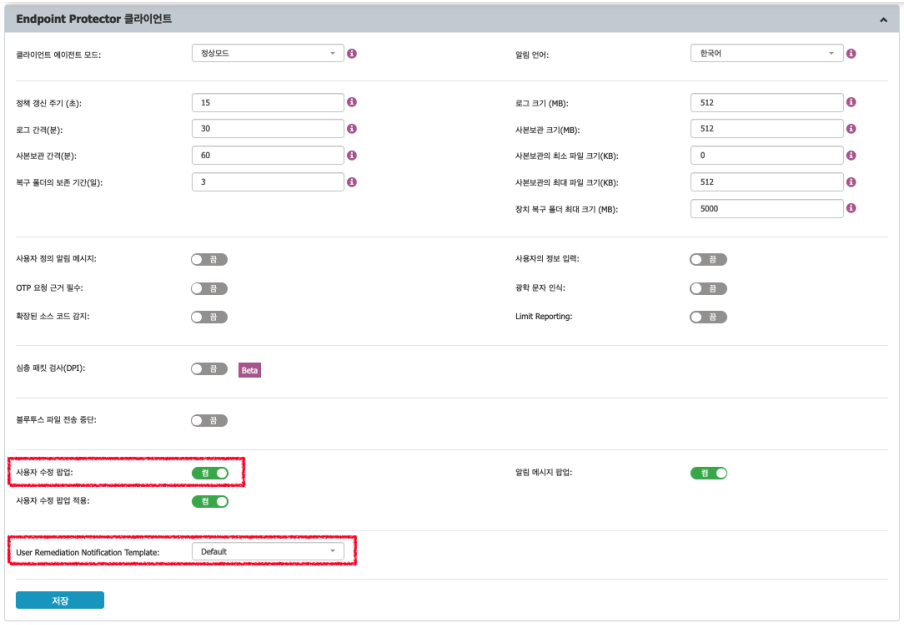


2. 매체 제어의 사용자 교정 알림을 정의합니다.

장치 유형 및 알림으로 이동해서 매체 제어의 사용자 수정 정의 섹션에서 **만들기**를 클릭하고 필드를 입력 후 **저장**합니다;

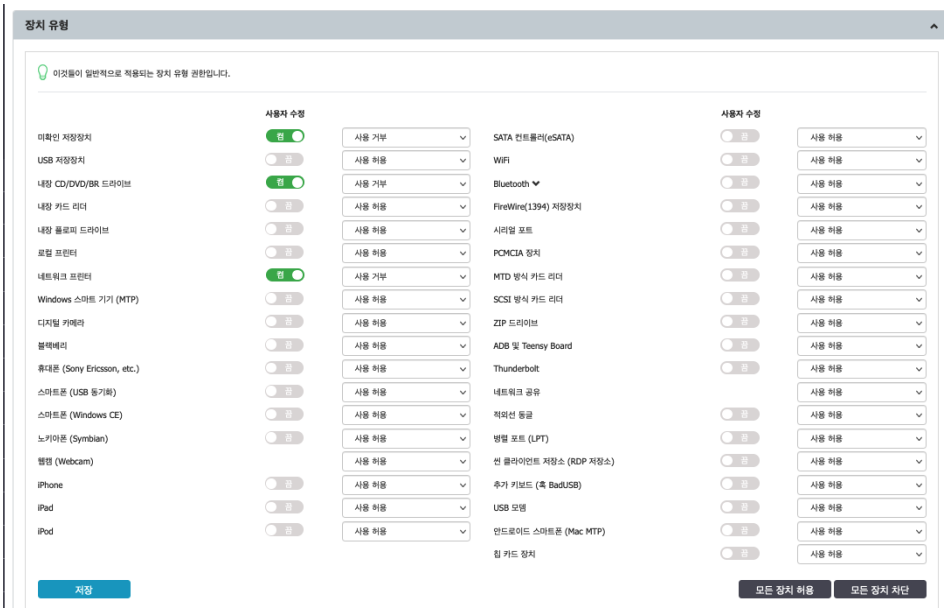


3. Endpoint Protector 클라이언트 설정에서 **사용자 교정 팝업** 설정을 사용하고 사용자 교정 알림 템플릿의 드롭다운 목록에서 **사용자 정의 알림**을 선택합니다.



4. 매체 제어 섹션의 전체 권한으로 이동하고 제한된 장치 접근에 대한 **사용자 교정**을 사용합니다 – 완전한 허용을 가진 장치는 사용자 교정 기능으로 활용하는 것은 무의미 합니다.

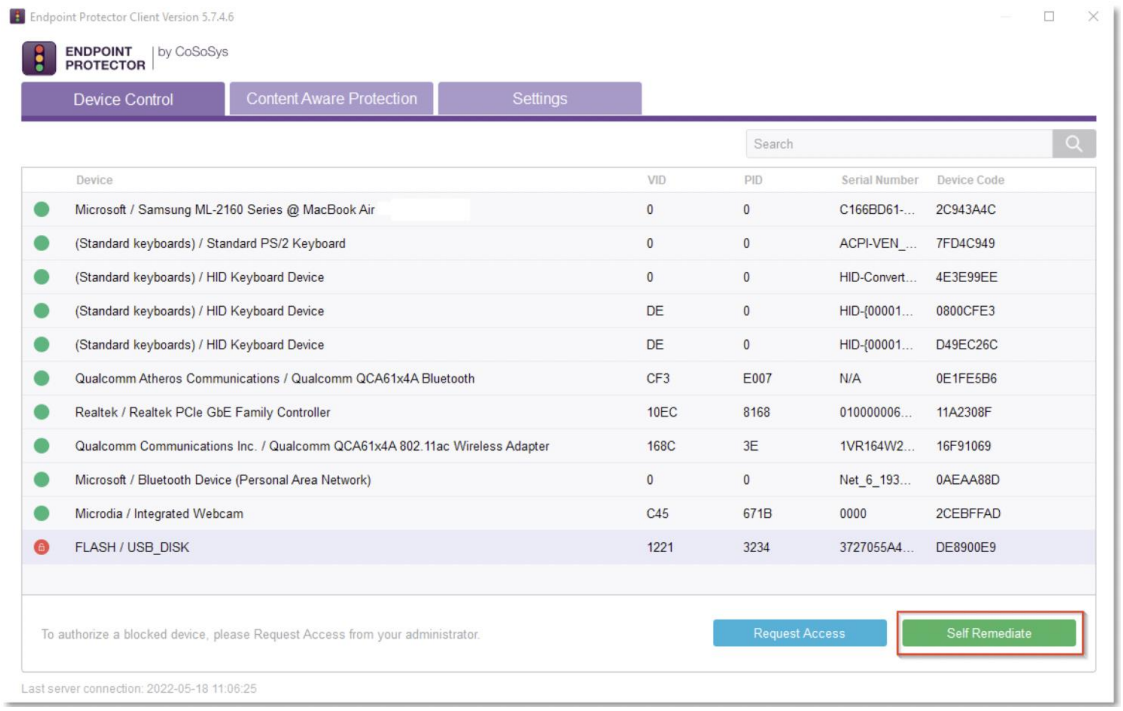
참고: 웹 캠과 네트워크 공유와 같은 내장 장치와 관련해서 사용자 교정 기능은 사용할 수 없습니다.



17.6.4. 사용자 교정 사용

장치 교정을 위해서 최종 사용자는 다음 단계를 따르시기 바랍니다:

1. **Endpoint Protector 알림창** 열고 **장치 제어** 탭으로 이동
2. 교정 장치 선택 후 **자체 교정** 클릭



3. **자체 교정** 섹션:
   a. 드롭다운 목록에서 **근거** 선택
   b. (필요하다면) 근거에 대한 **이유** 추가
   c. 로고 아래에 **사용자 URL** 검색
   d. 계정 요구 설정이 사용되어 있으면 **계정 추가** (현재 사용자 이름 새로 고침을 위해 사용자 이름 아이콘 클릭)

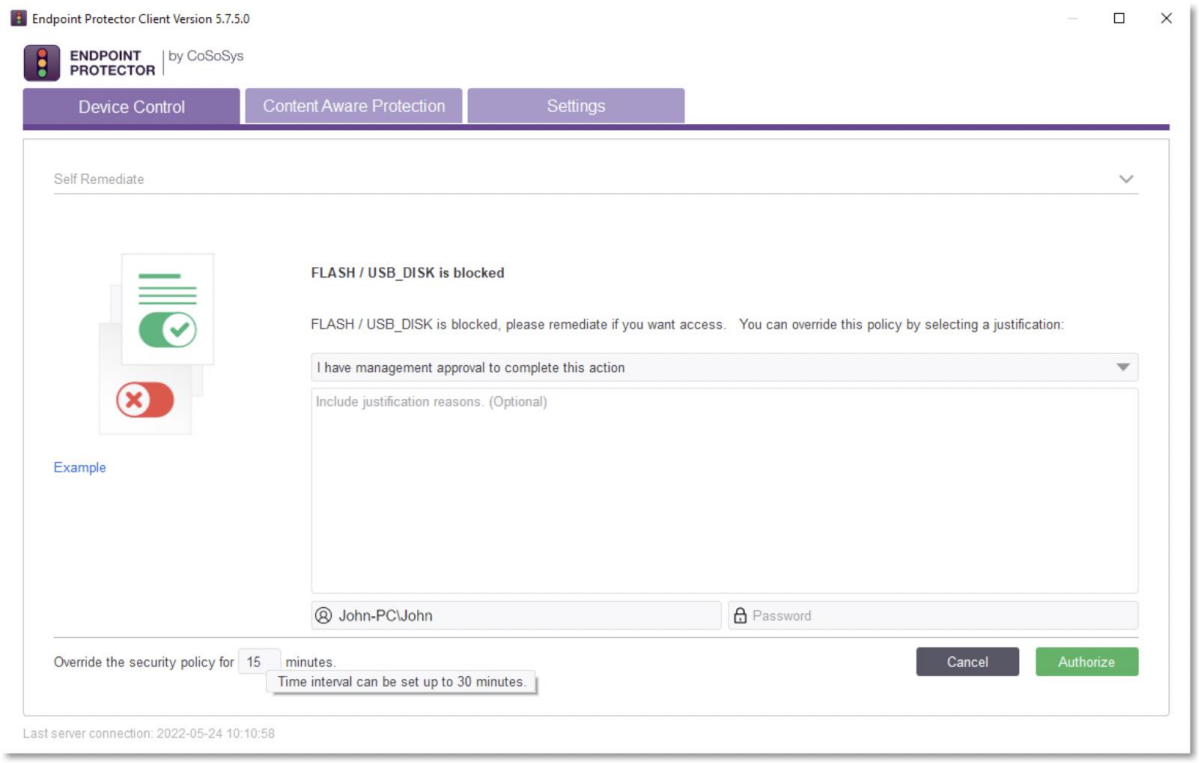
   i.참고: 대화 상자를 다시 열 때 인증에 다른 사용자 이름이 사용되면 EPP 알림은 현재 로그인한 사용자 아이디로 자동 전환됩니다.

ii.참고: 사용자 이름은 대소문자를 구분하지 않습니다.

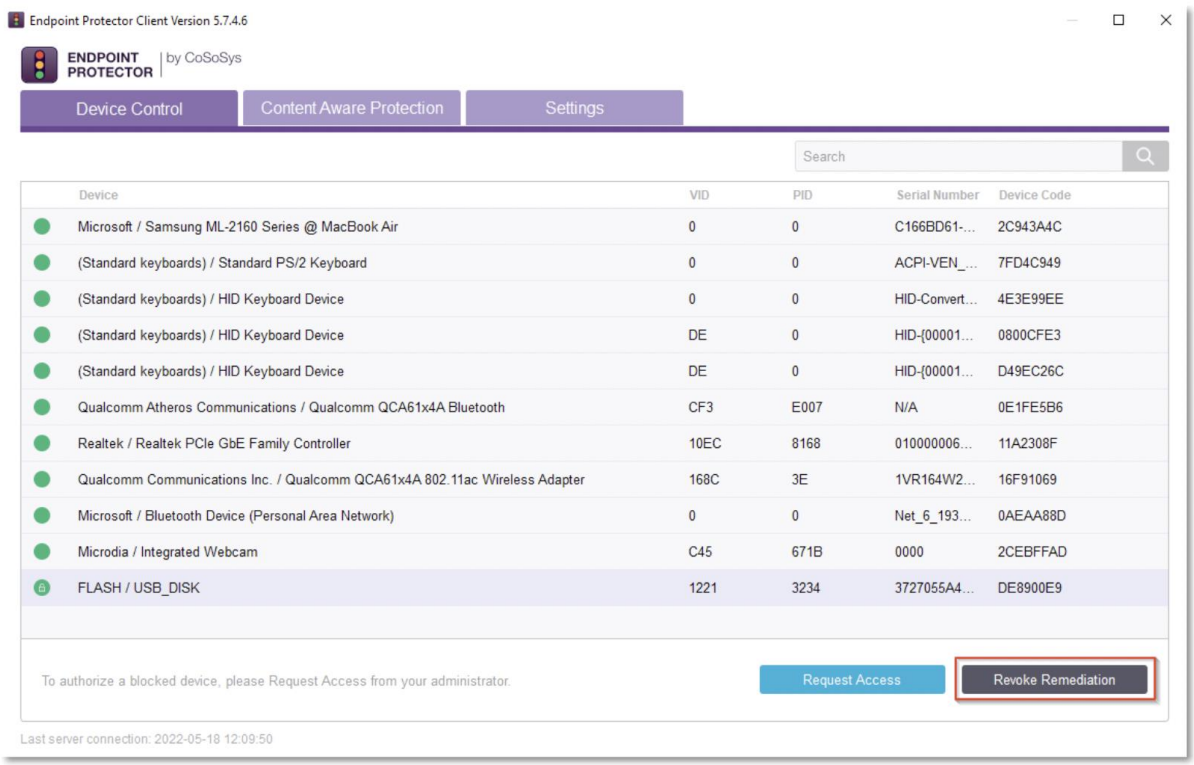
e. 장치 교정에 필요한 **시간(분)** 추가 (최대 시간 간격을 보기 위해서는 기본 숫자를 호버링)

f. **인증하기** 클릭

참고: 시스템 기본 설정과 **사용자 교정** 섹션에서 자체 수정 기능에 대한 더 많은 설정을 관리할 수 있습니다.



시간 간격 동안 언제든지 장치 수정 세션을 정지하려면 Endpoint Protector 알림 창에서 **장치 제어** 탭에서 장치 선택 후 **수정 취소**를 클릭합니다.



18. Endpoint Protector 클라이언트

Endpoint Protector 클라이언트는 보호되는 엔드포인트 (Windows, Mac, Linux)에서 Endpoint Protector 서버에서 받은 권한과 설정을 수행합니다.

Endpoint Protector 클라이언트는 Endpoint Protector UI에서 직접 다운로드 받을 수 있습니다. Endpoint Protector 클라이언트 다운로드에 대한 자세한 내용은 클라이언트 소트프웨어 챕터를 참조하시기 바랍니다.

참고: 대규모 네트워크에 Endpoint Protector 클라이언트를 배포하기 위해서 **Active Directory** 또는 **JAMF**와 같은 도구를 사용할 수 있습니다.

중요: Endpoint Protector 서버 5.8.0.0 을 시작으로 매체 제어 > 전체 설정 페이지 > Tamper Mode 설정이 가능하여 에이전트 무결성을 보호하는 추가적인 보호 조치가 가능합니다. 인가되지 않은 종료 또는 변조에서 Endpoint Protector 에이전트를 보호합니다.

18.1. 클라이언트 설치

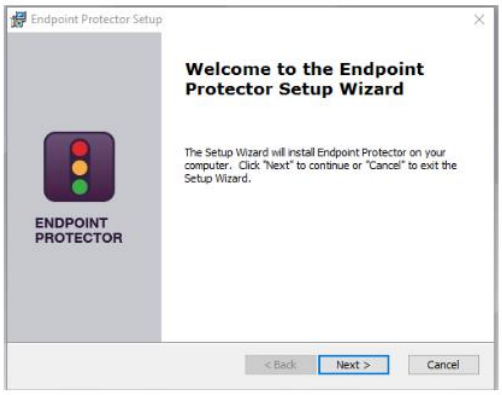
Windows와 **Mac**용 Endpoint Protector 클라이언트는 설치는 최소한의 노력만 들어갑니다. 설치 폴더와 서버 정보는 이미 미리 구성되어 있고 Endpoint Protector 서버에서 다운로드 할 수 있습니다.

Linux 설치를 위해서는 설치 파일에 있는 **readmeLinux.txt** 파일을 참조하시기 바랍니다.

참고: 1.4.0.4 버전으로 시작하는 Endpoint Protector Linux 클라이너트의 리포지포리에서 클라이언트를 설치할 수 있습니다. 아래 챕터에 기술되어 있습니다.

지원되는 배포판 예제는 아래를 따르시기 바랍니다 (최신 버전 지원을 우선으로 합니다).

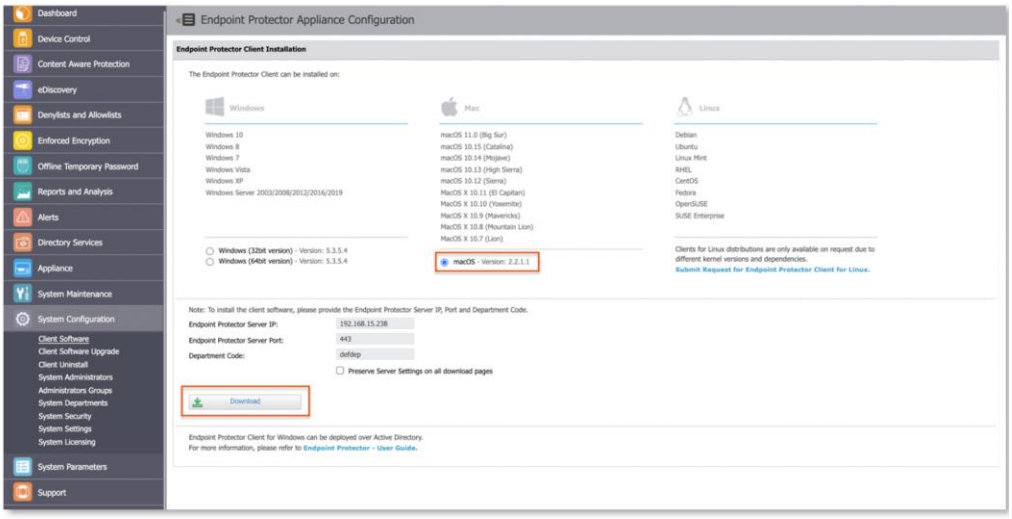
- **Ubuntu 14.04+**
- **Mint 18.x**
- **CentOS 7.x**
- **Fedora 29**
- **OpenSUSE 42.2 and 42.3**



18.1.1. DPI 및 VPN 트래픽 가로채기 사용을 위한 macOS Endpoint Protector 클라이언트 설치

1. Endpoint Protector 서버로 이동합니다.

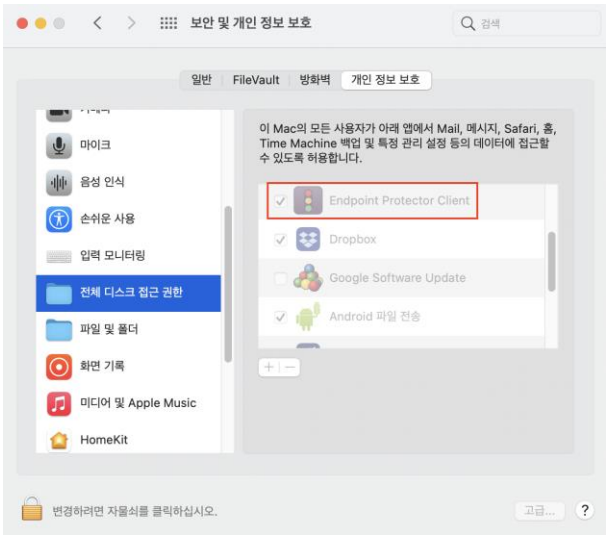
2. **시스템 구성** > **클라이언트 소프트웨어** 이동 후 macOS Endpoint Protector 클라이언트를 다운로드합니다.



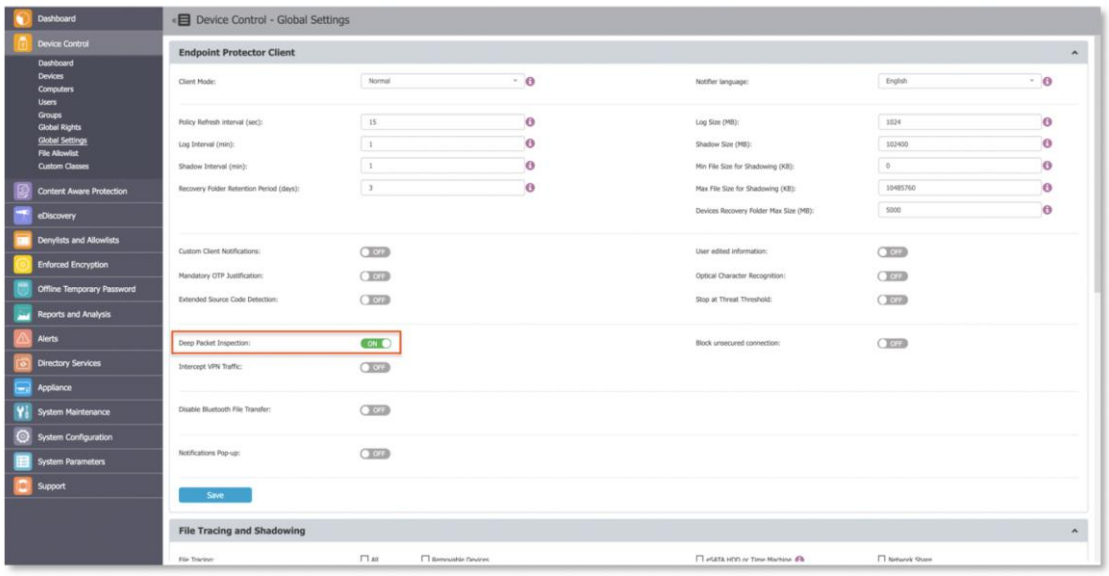
3. 다운로드 파일 압축을 해제합니다.

4. **.pkg** 파일을 열고 설치 단계를 따릅니다. 권한을 허용합니다.

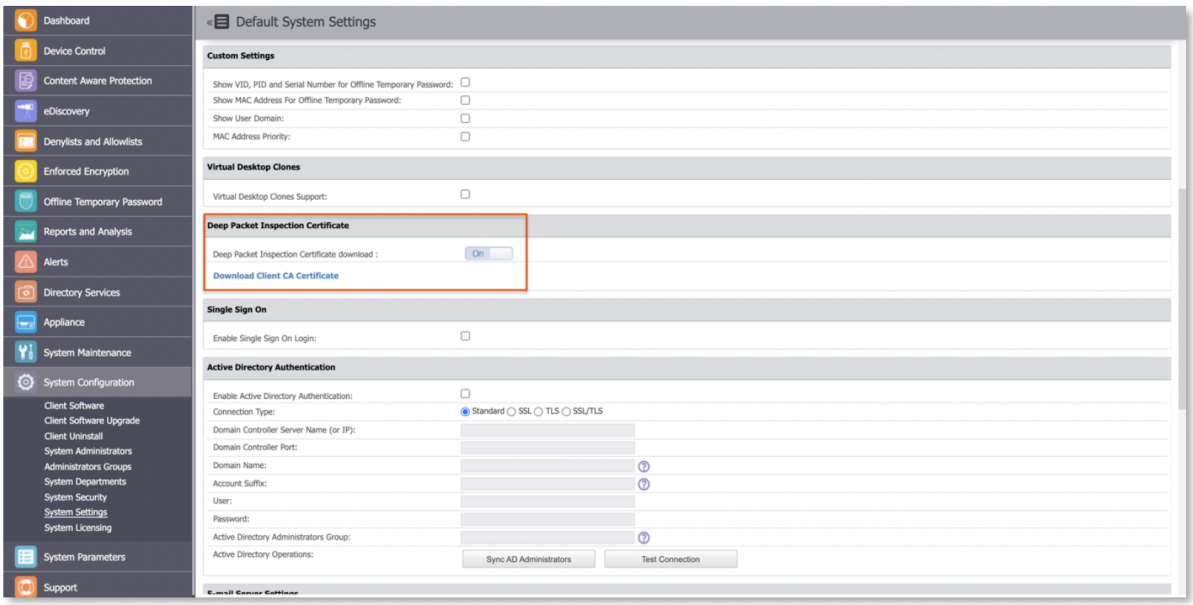
5. 설치가 성공적으로 완료된 후에 **시스템 환경 설정 > 보안 및 개인정보 > 개인 정보 보호 탭 > 전체 디스크 접근 권한** > Endpoint Protector 클라이언트 검색 및 응용프로그램 체크' 를 하고 변경을 저장합니다.



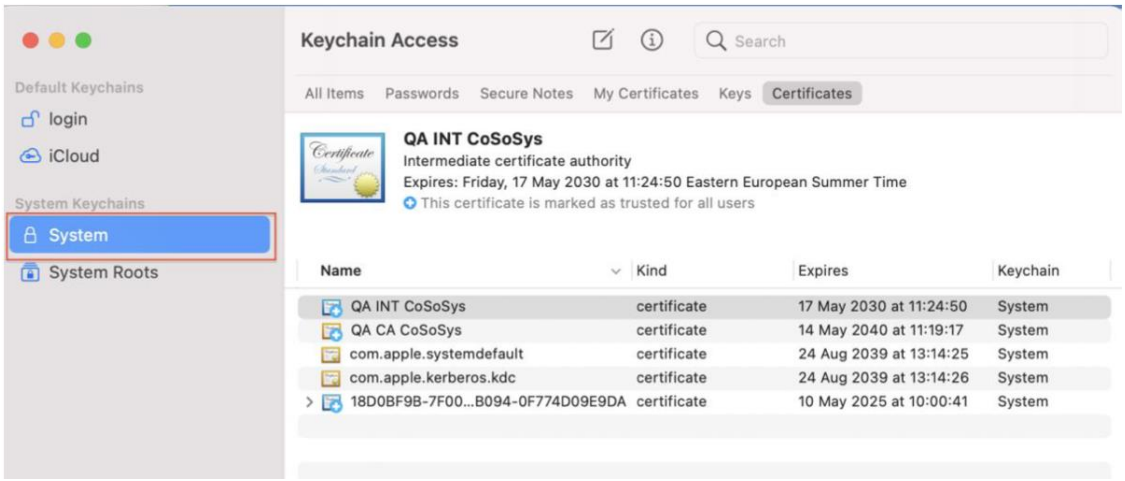
6. Endpoint Protector 서버로 이동해서 매체 제어 하위 섹션에서 **심층 패킷 검사(DPI)** 기능을 활성화합니다: **사용자/컴퓨터/그룹/전체 설정 > 설정 관리 > Endpoint Protector 클라이어트 > 심층 패킷 검사(DPI).**



7. **시스템 구성 > 시스템 설정 > DPI 인증서**에서 **CA 인증서**를 다운로드합니다.

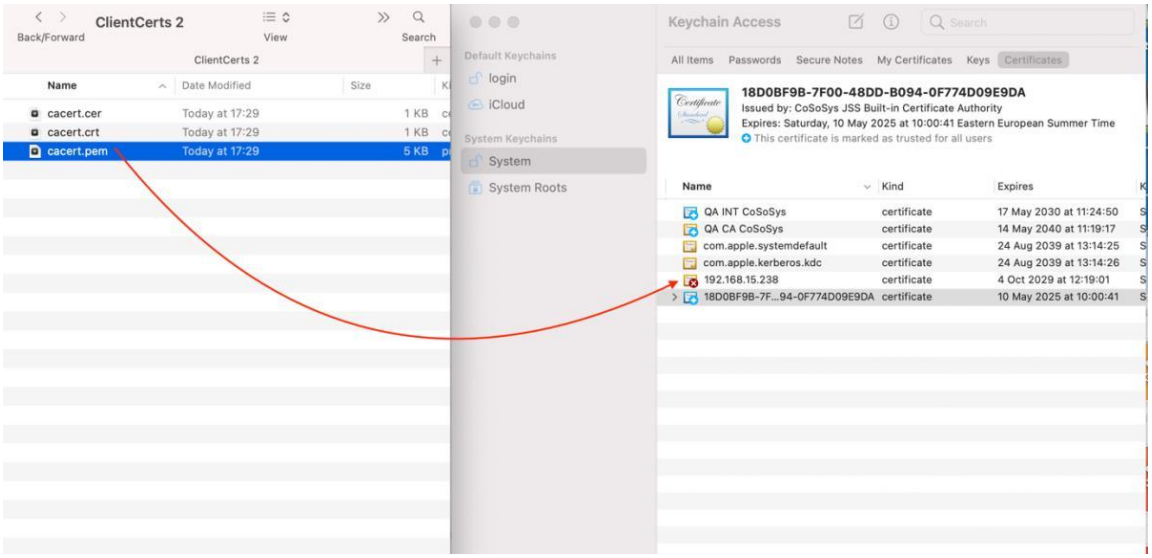


8. macOS에서 키 체인 접근 응용프로그램을 열고 시스템을 선택합니다.

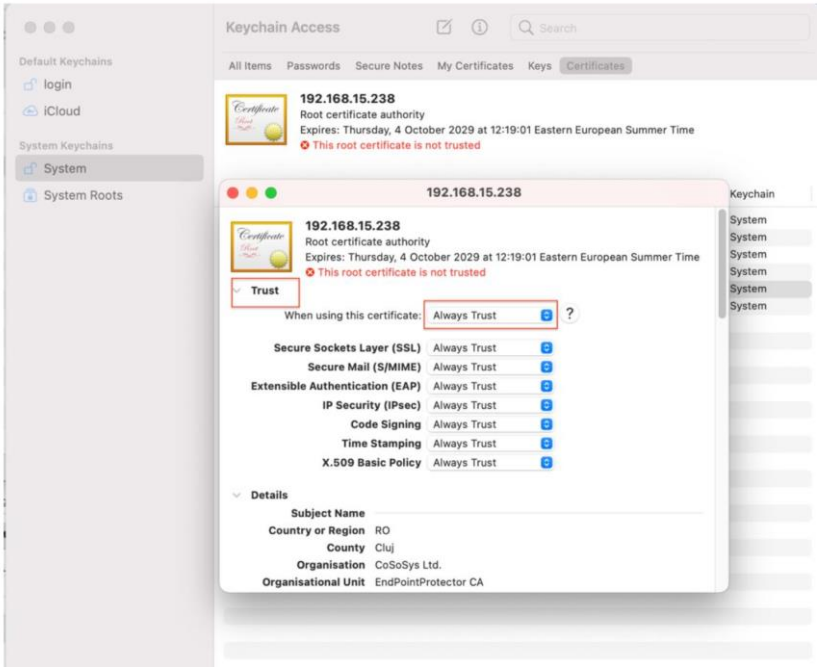


9. 다운로드된 **ClientCerts** 파일 압축을 해제합니다.

10. **cacert.pem** 파일을 선택하고 **키 체인 접근 > 시스템** 에 드래그 앤 드롭합니다.



11. 새롭게 추가된 인증서에 **x** 표시가 됩니다. 더블 클릭하고 **신뢰** 섹션에서 **항상 신뢰**를 선택합니다.

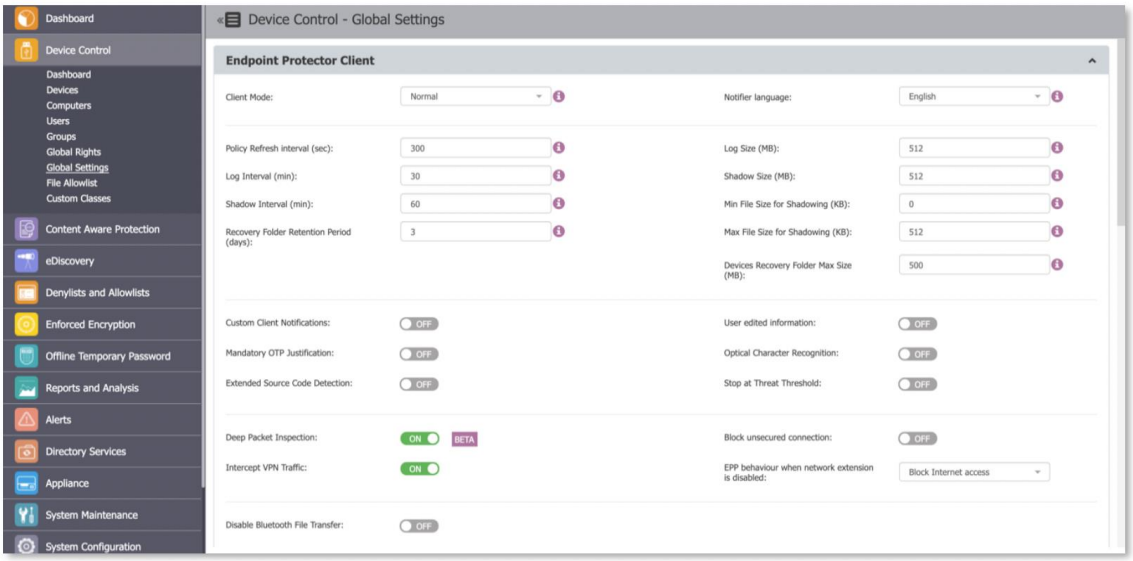


12. 변경 내용을 저장합니다.

13. **VPN 트래픽 가로채기**를 활성화합니다.

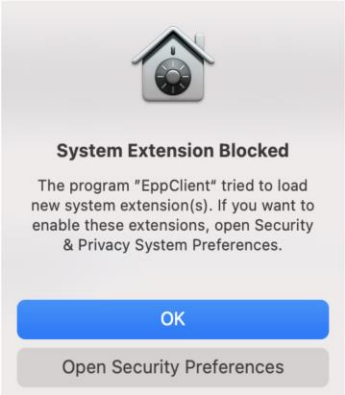
14. **네트워크 확장을 사용할 수 없을 때 EPP 동작** 옵션을 선택합니다.

- **임시적으로 DPI 기능 사용 안 함**: DPI (Deep Packet Inspection)을 임시적으로 사용하지 않습니다.
- **인터넷 접근 차단**: 최종 사용자가 Endpoint Protector 프록시 설정을 허용할 때까지 인터넷 연결을 차단합니다. 사용자는 PC를 재부팅 후에 허용이 가능합니다.

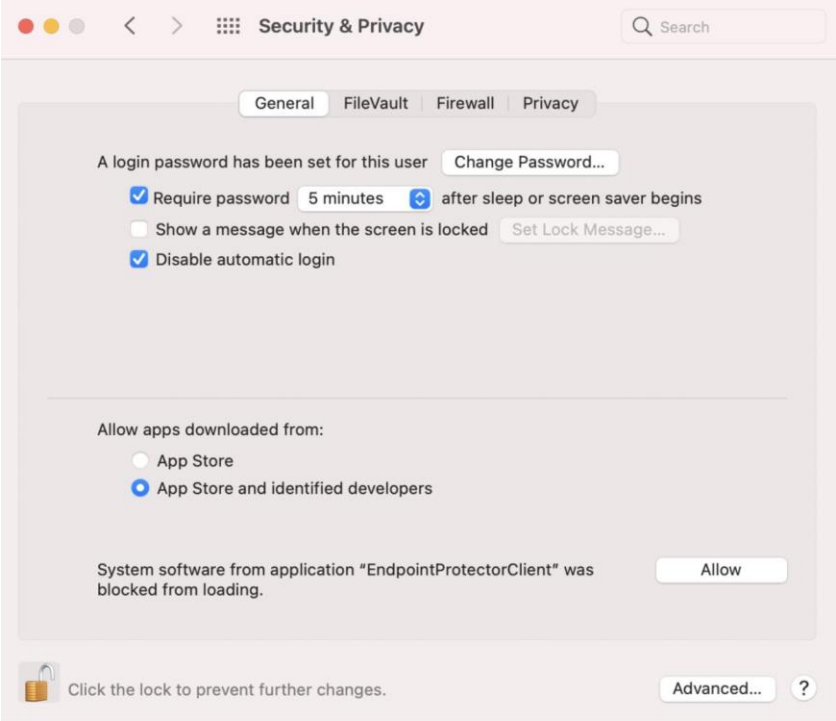


15. 변경 내용을 저장합니다.

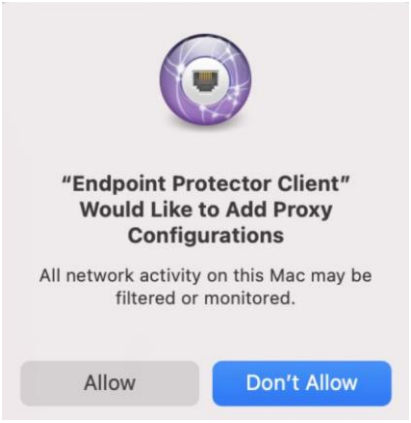
16. 시스템 확장 차단과 허용이 필요하다는 것을 최종 사용자에게 알려주는 다음 팝업이 표시됩니다.



17. **시스템 환경설정 > 보안 및 개인 정보 보호 > 일반 탭**에서 Endpoint Protector Client 확장 허용' 을 합니다.



18. 다음 화면이 표시되면 Endpoint Protector 프록시 설정을 허용합니다.



이 시점에서 macOS Endpoint Protector 클라이언트 설치가 완료됩니다.

참고: macOS에서 EPP클라이언트를 설치하거나 업그레이드한 후 EPP 알림이 표시되지 않는 경우, 컴퓨터를 재시작해서 이 문제를 해결하시기 바랍니다.

macOS에서 EPP클라이언트를 설치했다가 제거한 경우에도 EPP 알리밍 계속 표시될 수 있습니다. 목록에서 제거하려면 마우스 오른쪽 버튼을 클릭하고 "알림 재설정"을 선택하시면 됩니다.

18.1.2. Debian 기반 배포

설치 프로세스는 비슷하지만 각 배포판과 버전은 각 특징을 가지고 있습니다.

아래는 지원하는 배포판의 예제입니다:

- **Ubuntu 14.04**
- **Ubuntu 15.04**
- **Ubuntu 16.04**
- **Ubuntu 17.04**
- **Ubuntu 18.04**

- **Ubuntu 19.04**
- **Ubuntu 20.04**
- **Ubuntu 21.04**
- **Ubuntu 21.10**
- **Ubuntu 22.04**
- **LinuxMint**
- **Debian**

```
sudo apt update
sudo apt upgrade
wget
https://download.endpointprotector.com/linux_agent/EPPClient_v[X.X.X.X]/[Filename]
cd /Download
# unpack the archive
tar xvf [Filename.tar.xz]
# edit the options.ini file to contain the correct server address
cd [Extracted filename]
gedit options.ini
# run the installation script
bash install.sh
```

18.1.3. RedHat 기반 배포

설치 프로세스는 비슷하지만 각 배포판과 버전은 각 특징을 가지고 있습니다.

아래는 지원하는 배포판의 예제입니다:

- **CentOS 7.x**
- **RedHat 8.x**

- Fedora 32, 33, 34, 35
- AWS Linux 2

```
sudo yum update
sudo yum upgrade
wget
https://download.endpointprotector.com/linux_agent/EPPClient_v[X.X.X.X]/[Filen
ame]
cd /Download
# unpack the archive
tar xvf [Filename.tar.xz]
# edit the options.ini file to contain the correct server address
cd [Extracted filename]
gedit options.ini
# run the installation script
sudo bash install.sh
```

- OpenSuse 15.2
- SUSE 15+
- SLED Linux Enterprise Server 15 SP1
- SLED Linux Enterprise Server 15 SP2
- SLED Linux Enterprise Server 15 SP3

```
sudo zypper update
sudo zypper upgrade
wget
https://download.endpointprotector.com/linux_agent/EPPClient_v[X.X.X.X]/[Filename]
cd /Download
# unpack the archive
tar xvf [Filename.tar.xz]
# edit the options.ini file to contain the correct server address
cd [Extracted filename]
gedit options.ini
# run the installation script
sudo bash install.sh
```

18.1.4. Endpoint Protector 서버 IP 설정

모든 RedHat 기반 배포판은 Endpoint Protector 서버 IP 설정을 위해서 위의 명령어 실행 후 추가적인 단계가 필요합니다.

각 배포판 기반으로 다음 방법을 참조하시기 바랍니다:

Method 1

1. Define the Endpoint Protector Server IP

EPPCLIENT_WS_SERVER=[***the desired IP***]

export EPPCLIENT_WS_SERVER

2. Install the Endpoint Protector Client

- for SUSE and openSUSE: #zypper install epp-client
- for CentOS, RedHat, Fedora: #yum install epp-client

Method 2

1. Install the Endpoint Protector Client
 - for SUSE and openSUSE: #zypper install epp-client
 - for CentOS, RedHat, Fedora: #yum install epp-client

2. Run bash file to define the Endpoint Protector Server IP
bash '/opt/cososys/share/apps/epp-client/scripts/set_epp_client_server.sh'

19. Endpoint Protector 서버-클라이언트 통신

이 세션에서는 TLS 프로토콜 암호화로 Endpoint Protector 서버와 클라이언트 사이의 통신에 대한 자세한 정보를 제공합니다.

- Endpoint Protector 서버 5.7.0.0 버전에서 TLS V1.2를 기본으로 사용 가능하고 TLS V1.1은 5.7.0.0에서 요청 (오래된 에이전트 및 장비 호환)으로 사용할 수도 있습니다.
- Endpoint Protector 서버 5.8.0.0 버전에서 TLS V1.2 및 TLS V1.3을 기본으로 사용 가능하고 TLS V1.1은 5.8.0.0에서 요청 (오래된 에이전트 및 장비 호환)으로 사용할 수도 있습니다.

19.1. Endpoint Protector 클라이언트

TLS 1.3 호환성			
OS	**이전 버전**	**새 버전**	**Endpoint Protector 클라이언트 특징**
Windows	X Windows 7, XP 및 Windows 10 이전 버전	O Windows 10, 1903+ 버전	Windows 내장 TLS 암호 엔진 사용 (Schannel)
macOS	O	O	Endpoint Protector 클라이언트에서 제공하는 커스텀 OpenSSL 번들 패키지 사용
Linux	X	O	Linux 내장 OpenSSL 엔진 사용

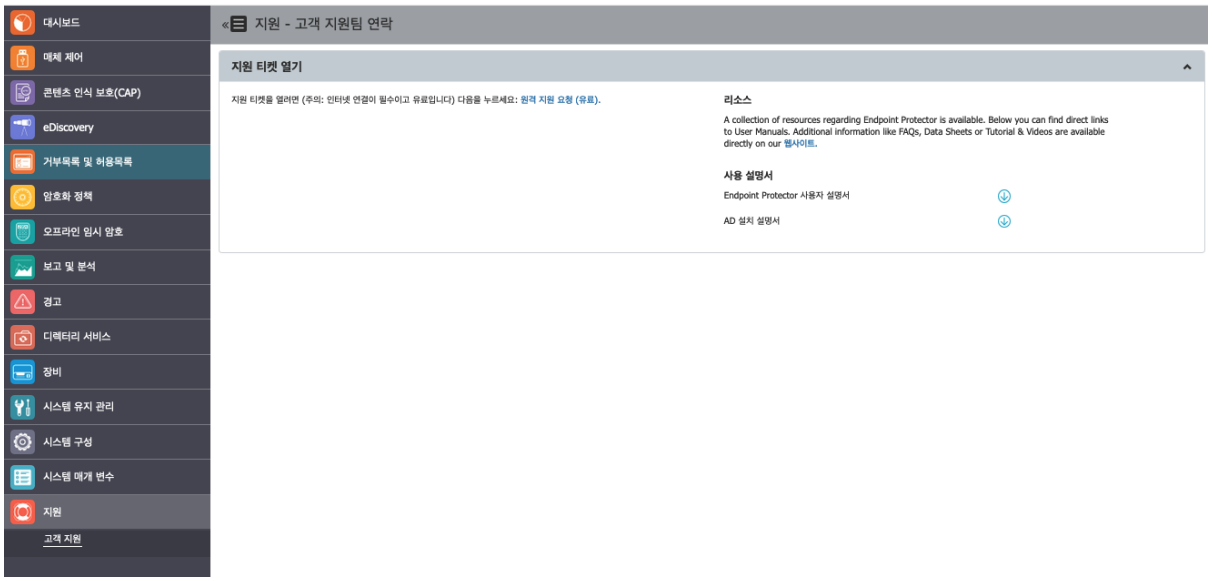
19.2. Endpoint Protector 서버

TLS 1.3 호환성	
5.7.0.0 이전 버전	Live Update 업그레이드로 TLS 1.3 사용할 수 없음
5.7.0.0 이후 버전	기본으로 TLS 1.3을 사용해서 현재 환경에서 내보내기/가져오기 시스템 구성을 사용하여 새로운 설치 및 마이그레이션 가능 Live Update 업그레이드에서 Linux OS 라이브러리는 지원팀에서 업그레이드해야 함

20. 지원

FAQ 나 전자 메일 지원과 같은 추가 지원이 필요한 경우 Cososys 지원 웹 사이트 (http://www.cososys.kr)를 방문하십시오.

고객 지원을 클릭하시면 해당 부서에 전자 메일을 보낼 수 있습니다.



21. 면책

Endpoint Protector 어플라이언스는 liveupdate.endpointprotector.com과 clould.endpointprotector.com을 제외하고 외부 네트워크와 통신하지 않습니다.

Endpoint Protector는 악성 소프트웨어를 포함하지 않고 모든 개인정보를 보내지 않습니다 (만약 자동 라이브 업데이트 보고가 사용하지 않음으로 되어있을 경우).

각 Endpoint Protector 서버는 서비스를 위해서 SSH 프로토콜 (22)이 열려있습니다. 거기에는 하나의 시스템 계정 (epproot)만 사용할 수 있고 비밀번호로 보호됩니다. SSH는 고객 요청으로 사용하지 않음으로 변경할 수 있습니다.

보안 제품들의 보호 기능은 그 특성상 우회가 가능할 수도 있습니다. CoSoSys 제품으로 보호되는 데이터 또는 저장 장치가 허락되지 않은 사람들에 의하여 접속되지 않음에 대하여 보증 할 수 없으며 또한 보증하지 않습니다. 그리고 CoSoSys는 법이 허용하는 최대한의 범위에서 그 효과에 대한 어떠한 보증도 제공하지 않는 점을 참고하여 주시기 바랍니다. 사용자의 이해를 부탁 드립니다.

EndpointProtector.com